

Framework

# AWS Well-Architected Framework



# AWS Well-Architected Framework: Framework

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Die Handelsmarken und Handelsaufmachung von Amazon dürfen nicht in einer Weise in Verbindung mit nicht von Amazon stammenden Produkten oder Services verwendet werden, durch die Kunden irregeführt werden könnten oder Amazon in schlechtem Licht dargestellt oder diskreditiert werden könnte. Alle anderen Marken, die nicht im Besitz von Amazon sind, gehören den jeweiligen Besitzern, die möglicherweise mit Amazon verbunden sind oder von Amazon gesponsert werden.

---

# Table of Contents

Zusammenfassung und Einführung .....	1
Einführung .....	1
Definitionen .....	2
Architekturüberlegungen .....	5
Allgemeine Designprinzipien .....	7
Die Säulen des Frameworks .....	9
Operative Exzellenz .....	9
Designprinzipien .....	10
Definition .....	11
Bewährte Methoden .....	12
Ressourcen .....	23
Sicherheit .....	23
Designprinzipien .....	24
Definition .....	25
Bewährte Methoden .....	25
Ressourcen .....	35
Zuverlässigkeit .....	36
Designprinzipien .....	36
Definition .....	38
Bewährte Methoden .....	38
Ressourcen .....	44
Leistungseffizienz .....	44
Designprinzipien .....	44
Definition .....	45
Bewährte Methoden .....	46
Ressourcen .....	51
Kostensoptimierung .....	52
Designprinzipien .....	53
Definition .....	53
Bewährte Methoden .....	54
Ressourcen .....	61
Nachhaltigkeit .....	62
Designprinzipien .....	62
Definition .....	63

---

Bewährte Methoden .....	64
Ressourcen .....	71
Der Überprüfungsprozess .....	73
Schlussfolgerung .....	76
Mitwirkende .....	77
Weitere Informationen .....	78
Dokumentversionen .....	79
Anhang: Fragen und bewährte Methoden .....	83
Operative Exzellenz .....	83
Organisation .....	83
Vorbereitung .....	147
Betrieb .....	222
Weiterentwicklung .....	268
Sicherheit .....	288
Sicherheitsgrundlagen .....	289
Identity and Access Management .....	317
Erkennung .....	379
Schutz der Infrastruktur .....	395
Datenschutz .....	424
Vorfallreaktion .....	460
Anwendungssicherheit .....	486
Zuverlässigkeit .....	506
Grundlagen .....	507
Workload-Architektur .....	549
Änderungsmanagement .....	599
Fehlerverwaltung .....	644
Leistungseffizienz .....	752
Auswahl der Architektur .....	752
Computer und Hardware .....	769
Datenverwaltung .....	788
Netzwerk und Bereitstellung von Inhalten .....	814
Prozess und Kultur .....	846
Kostensoptimierung .....	865
Praxis für Cloud-Finanzmanagement .....	865
Ausgabenerkennung und Nutzungsbewusstsein .....	891
Kostengünstige Ressourcen .....	940

---

Verwaltung von Nachfrage und Bereitstellung von Ressourcen .....	985
Optimierung im Laufe der Zeit .....	999
Nachhaltigkeit .....	1008
Auswahl der Region .....	1009
Ausrichtung am Bedarf .....	1011
Software und Architektur .....	1028
Daten .....	1041
Hardware und Services .....	1062
Prozess und Kultur .....	1072
Hinweise .....	1082
AWS Glossar .....	1083
.....	mlxxxiv

# AWS Well-Architected Framework

Veröffentlichungsdatum: 27. Juni 2024 ([Dokumentversionen](#))

Das AWS Well-Architected Framework hilft Ihnen dabei, die Vor- und Nachteile von Entscheidungen zu verstehen, die Sie beim Aufbau von Systemen treffen. AWS Das Framework hilft Ihnen, bewährte Architekturmethoden für die Entwicklung und den Betrieb zuverlässiger, sicherer, effizienter, kostengünstiger und nachhaltiger Systeme in der Cloud zu ermitteln.

## Einführung

Das AWS Well-Architected Framework hilft Ihnen dabei, die Vor- und Nachteile von Entscheidungen zu verstehen, die Sie beim Aufbau von Systemen treffen. AWS Das Framework hilft Ihnen, bewährte Architekturmethoden für den Entwurf und Betrieb zuverlässiger, sicherer, effizienter, kostengünstiger und nachhaltiger Workloads in der AWS Cloud zu ermitteln. Es bietet Ihnen die Möglichkeit, Ihre Architekturen konsequent an bewährten Methoden zu messen und Verbesserungspotenzial zu identifizieren. Der Prozess zur Überprüfung einer Architektur ist ein konstruktives Gespräch über Architekturentscheidungen und kein Auditmechanismus. Wir sind davon überzeugt, dass eine durchdachte Systemarchitektur maßgeblich zu Ihrem künftigen geschäftlichen Erfolg beiträgt.

AWS Solutions Architects verfügen über jahrelange Erfahrung in der Architektur von Lösungen für eine Vielzahl von Geschäftsbereichen und Anwendungsfällen. Wir waren am Design und an der Überprüfung Tausender Kundenarchitekturen in AWS beteiligt. Daher kennen wir die bewährten Methoden und Kernstrategien für erfolgreiche Systemarchitekturen in der Cloud.

Das AWS Well-Architected Framework dokumentiert eine Reihe grundlegender Fragen, anhand derer Sie herausfinden können, ob eine bestimmte Architektur gut mit den Best Practices der Cloud übereinstimmt. 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. Da AWS es sich ständig weiterentwickelt und wir durch die Zusammenarbeit mit unseren Kunden immer mehr lernen, werden wir die Definition von „gut architektonisch“ weiter verfeinern.

Dieses Framework richtet sich an Personen in technologischer Position, wie z. B. Chief Technology Officers (CTOs), Architekten, Entwickler und Mitglieder des Betriebsteams. Es beschreibt AWS bewährte Verfahren und Strategien für die Entwicklung und den Betrieb eines Cloud-Workloads und bietet Links zu weiteren Implementierungsdetails und Architekturmustern. Weitere Informationen finden Sie auf der [Startseite des AWS Well-Architected Framework](#).

AWS bietet außerdem einen kostenlosen Service zur Überprüfung Ihrer Workloads. Das [AWS Well-Architected Tool](#) (AWS WA Tool) ist ein Service in der Cloud, der Ihnen einen konsistenten Prozess zur Überprüfung und Messung Ihrer Architektur mithilfe des AWS Well-Architected Framework bietet. Das AWS WA Tool bietet Empfehlungen, wie Sie Ihre Workloads zuverlässiger, sicherer, effizienter und kostengünstiger gestalten können.

Um Sie bei der Anwendung von bewährten Methoden zu unterstützen, haben wir [AWS Well-Architected Labs](#) entwickelt. Diese stellen Ihnen ein Repository mit Code und Dokumentation zur Verfügung, damit Sie praktische Erfahrungen mit der Implementierung von bewährten Methoden sammeln können. Wir haben uns auch mit ausgewählten Partnern im AWS Partnernetzwerk (APN) zusammengetan, die Mitglieder des [AWS Well-Architected](#) Partner-Programms sind. Diese AWS Partner verfügen über AWS fundiertes Wissen und können Ihnen helfen, Ihre Workloads zu überprüfen und zu verbessern.

## Definitionen

Jeden Tag AWS unterstützen Experten Kunden bei der Systemarchitektur, um die Vorteile der Best Practices in der Cloud zu nutzen. 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.

Auf der Grundlage unserer Erkenntnisse haben wir das AWS Well-Architected Framework entwickelt, das Kunden und Partnern einheitliche Best Practices zur Bewertung von Architekturen bietet und eine Reihe von Fragen enthält, anhand derer Sie beurteilen können, wie gut eine Architektur auf Best Practices abgestimmt ist. AWS

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

Tabelle 1. Die Säulen des AWS Well-Architected Framework

Name	Beschreibung
Operative Exzellenz	Die Fähigkeit, die Entwicklung zu unterstützen und Workloads effektiv auszuführen, Einblicke in die Betriebsabläufe zu erhalten und für geschäftlichen Mehrwert unterstüt

Name	Beschreibung
	zende Prozesse und Verfahren fortlaufend zu verbessern.
Sicherheit	Die Sicherheitssäule beschreibt, wie Sie Cloud-Technologien nutzen können, um Daten, Systeme und Komponenten so zu schützen, dass Ihre Sicherheitslage verbessert werden kann.
Zuverlässigkeit	Die Säule „Zuverlässigkeit“ umfasst die Fähigkeit einer Workload, die beabsichtigte Funktion erwartungsgemäß korrekt und konsistent auszuführen. Dies umfasst die Möglichkeit, die Workload während des gesamten Lebenszyklus zu betreiben und zu testen. Dieses paper enthält ausführliche Best-Practice-Anleitungen für die Implementierung zuverlässiger Workloads auf AWS.
Leistungseffizienz	Die Fähigkeit, Computerressourcen effizient zu nutzen, um Systemanforderungen zu erfüllen und diese Effizienz bei der Entwicklung von Nachfrageänderungen und Technologien aufrechtzuerhalten.
Kostenoptimierung	Die Fähigkeit, Systeme zu betreiben, um Unternehmenswert zum niedrigsten Preis zu liefern.



Name	Beschreibung
Nachhaltigkeit	Die Fähigkeit, die Auswirkungen auf die Nachhaltigkeit kontinuierlich zu verbessern, indem der Energieverbrauch reduziert und die Effizienz aller Komponenten einer Workload erhöht wird, indem der Nutzen der bereitgestellten Ressourcen maximiert und die insgesamt erforderlichen Ressourcen minimiert werden.

Im AWS Well-Architected Framework verwenden wir diese Begriffe:

- Eine Komponente ist der Code, die Konfiguration und die AWS Ressourcen, die zusammen eine Anforderung erfüllen. Eine Komponente ist häufig die Einheit technischen Eigentums und von anderen Komponenten losgelöst.
- Der Begriff Workload wird für zusammengehörige Komponenten, die geschäftlichen Mehrwert darstellen, verwendet. Eine Workload ist in vielen Fällen der Detaillierungsgrad, von dem Führungskräfte aus Wirtschaft und Technik häufig sprechen.
- Wir betrachten Architektur als das Zusammenwirken von Komponenten in einer Workload. Wie Komponenten kommunizieren und interagieren, ist häufig der Schwerpunkt von Architekturdiagrammen.
- Meilensteine markieren wichtige Änderungen im Laufe der Entwicklung einer Architektur im Produktlebenszyklus (Entwurf, Implementierung, Tests, Inbetriebnahme und Produktionsbetrieb).
- In Zusammenhang mit einer Organisation ist das Technologieportfolio die Sammlung an Workloads, die für den Geschäftsbetrieb erforderlich sind.
- Der Grad des Aufwands bezeichnet die Zeitspanne, den Aufwand und die Komplexität, die für die Implementierung einer Aufgabe benötigt werden. Jede Organisation muss die Größe und das Fachwissen des Teams sowie die Komplexität der Workload berücksichtigen, um den Grad des Aufwands für die Organisation richtig einzuordnen.
  - Hoch: Die Arbeit dauert möglicherweise mehrere Wochen oder Monate. Sie könnte in mehrere Abschnitte, Veröffentlichungen und Aufgaben aufgeteilt werden.
  - Mittel: Die Arbeit dauert möglicherweise mehrere Tage oder Wochen. Sie könnte in mehrere Veröffentlichungen und Aufgaben aufgeteilt werden.


- **Niedrig:** Die Arbeit dauert möglicherweise mehrere Stunden oder Tage. Sie könnte in mehrere Aufgaben aufgeteilt werden.

Beim Entwerfen von Workloads stellen Sie eine Kosten-Nutzen-Abwägung zwischen Säulen abhängig von Ihrem Geschäftskontext an. Diese Geschäftsentscheidungen können Ihre technischen Prioritäten beeinflussen. In Entwicklungsumgebungen könnten Sie im Hinblick auf eine Verbesserung der Nachhaltigkeitswirkung und eine Verringerung der Kosten zulasten der Zuverlässigkeit optimieren. Bei unternehmenskritischen Lösungen könnten Sie dagegen die Zuverlässigkeit optimieren und dafür höhere Kosten und stärkere Auswirkungen auf die Nachhaltigkeit in Kauf nehmen. Bei E-Commerce-Lösungen kann sich die Leistung auf die Einnahmen und die Kauflust der Kunden auswirken. Sicherheit und operative Exzellenz werden in der Regel nicht gegen die anderen Säulen abgewogen.

## Architekturüberlegungen

In On-Premises-Umgebungen setzen Kunden oft ein zentrales Technologiearchitektur-Team ein. Dies dient als Überlagerung für Produkt- oder Feature-Teams, um zu verifizieren, dass diese nach bewährten Methoden arbeiten. Technologiearchitektur-Teams setzen sich üblicherweise aus Fachleuten mit unterschiedlichen Aufgabengebieten zusammen, z. B.: Technical Architect (Infrastruktur), Solutions Architect (Software), Data Architect, Networking Architect und Security Architect. Oft verwenden diese Teams [TOGAF](#) oder das [Zachman Framework](#) als Teil einer Unternehmensarchitekturfunktion.

Bei ziehen wir es vor AWS, Fähigkeiten auf Teams zu verteilen, anstatt ein zentralisiertes Team mit diesen Fähigkeiten zu haben. Wenn die Entscheidungsbefugnis auf mehrere Teams verteilt wird, geht das mit Risiken einher. So muss beispielsweise bestätigt sein, dass die Teams internen Standards gerecht werden. Um diese Risiken aufzufangen, verwenden wir zwei Methoden. Zum einen arbeiten wir mit Methoden (Vorgehensweisen, Prozessen, Standards und gemeinhin anerkannte Normen), die darauf abzielen, jedes Team mit dieser Fähigkeit auszustatten. Dazu setzen wir Experten ein, die dafür sorgen, dass die Teams die vorgegebenen Standards übertreffen. Zweitens implementieren wir Mechanismen, die automatisch kontrollieren, ob Standards eingehalten werden.

 „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 (oftmals automatisierte) Mechanismen ersetzen, die kontrollieren, ob Regeln oder Prozesse 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. Vom Kunden aus zu denken, ist ein grundlegender Bestandteil unseres Innovationsprozesses. Unsere Arbeit richtet sich ganz nach dem Kunden und dessen Wünschen. 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 helfen, diese Fähigkeiten zu erwerben, oder bestehenden Teams dabei zu helfen, ihre Messlatte höher zu legen, ermöglichen wir den Zugang zu einer virtuellen Community von Principal Engineers, die ihre Entwürfe überprüfen und ihnen helfen können, zu verstehen, was AWS bewährte Verfahren sind. 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.

AWS Die besten Praktiken ergeben sich aus unserer Erfahrung mit dem Betrieb von Tausenden von Systemen auf Internetebene. 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 bestätigen, dass die Teams danach arbeiten. Im Laufe der Zeit werden diese bewährten Methoden in unsere internen Prüfprozesse sowie in Compliance-Mechanismen aufgenommen. Das Well-Architected Framework 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. Das Well-Architected Framework 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 Architekturständigkeiten), kann unserer Ansicht nach eine Well-Architected Enterprise-Architektur zustande kommen, die auf die Kundenwünsche ausgerichtet ist. Technologieführer (z. B. ein CTOs - oder Entwicklungsmanager), die Well-Architected-Prüfungen für all Ihre Workloads durchführen, ermöglichen es Ihnen, die Risiken in Ihrem Technologieportfolio besser zu verstehen. Sie identifizieren teamübergreifende Themen, die Ihre Organisation mit Hilfe von Mechanismen, Training oder Mittagsvorträgen angehen könnte. Allesamt Gelegenheiten für Ihre Principal Engineers, ihr Wissen zu bestimmten Themen an mehrere Teams weiterzugeben.

# Allgemeine Designprinzipien

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

- **Keine Ungewissheit mehr über die Kapazität:** Wenn Sie bei der Bereitstellung einer Workload eine schlechte 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 auf- und abskaliert.
- **Systeme auf Produktionsbetrieb testen:** Sie können in der Cloud bei Bedarf eine Testumgebung in Produktionsgröße einrichten, Ihre Tests abschließen und die Ressourcen dann wieder außer Betrieb nehmen. 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 On-Premises-Standort hätten.
- **Automatisieren unter Berücksichtigung architektonischer Experimente:** Wenn Sie automatisieren, können Sie Ihre Workloads kostengünstig erstellen und replizieren und vermeiden manuellen Aufwand. Sie können an der Automatisierung vorgenommene Änderungen nachverfolgen, die Auswirkungen nachprüfen und ggf. auf die vorherigen Parameter zurücksetzen.
- **Evolutionäre Architekturen berücksichtigen:** In herkömmlichen Umgebungen sind architekturelevante Entscheidungen oft als statische, einmalig auftretende Ereignisse implementiert. Dementsprechend gibt es während der Lebensdauer des Systems einige wenige Hauptversionen. Geschäftsvoraussetzungen und ihr Kontext entwickeln sich stetig weiter. 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. Systeme können sich somit 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 architekturelevanten Entscheidungen auf das Verhalten Ihrer Workload durchschlagen. Sie können also mit faktenbasierten Entscheidungen Ihre Workload verbessern. Ihre Cloud-Infrastruktur ist Code. Das bedeutet, dass Sie diese Daten im Laufe der Zeit in architekturelevante Entscheidungen und Verbesserungsmaßnahmen einfließen lassen können.
- **Verbesserung anhand von Gamedays:** Simulieren Sie an regelmäßigen Gamedays Vorfälle in der Produktion, um das Verhalten Ihrer Architektur und Prozesse zu simulieren. So können Sie

nachvollziehen, wo nachgebessert werden kann. Zudem üben Sie dabei ein, wie Ihre Organisation mit Ereignissen umgeht.

# Die Säulen des Frameworks

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 sechs Säulen „Operative Exzellenz“, „Sicherheit“, „Zuverlässigkeit“, „Leistungseffizienz“, „Kostenoptimierung“ und „Nachhaltigkeit“ 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.

## Säulen

- [Operative Exzellenz](#)
- [Sicherheit](#)
- [Zuverlässigkeit](#)
- [Leistungseffizienz](#)
- [Kostenoptimierung](#)
- [Nachhaltigkeit](#)

## Operative Exzellenz

Die Säule für die betriebliche Exzellenz beinhaltet die Fähigkeit, die Entwicklung zu unterstützen und Workloads effektiv auszuführen, Einblicke in die Betriebsabläufe zu erhalten und unterstützende Prozesse und Verfahren fortlaufend zu verbessern, um geschäftlichen Mehrwert zu schaffen.

Die Säule „Betriebliche Exzellenz“ gibt einen Überblick über konzeptionelle Grundsätze, bewährte Methoden und Fragen. Verbindliche Anleitungen zur Implementierung finden Sie im [Whitepaper „Säule der betrieblichen Exzellenz“](#).

## Themen

- [Designprinzipien](#)
- [Definition](#)
- [Bewährte Methoden](#)
- [Ressourcen](#)

## Designprinzipien

Nachfolgend finden Sie die konzeptionellen Grundsätze für die betriebliche Exzellenz in der Cloud:

- **Organisieren von Teams nach Geschäftsergebnissen:** Die Fähigkeit eines Teams, Geschäftsergebnisse zu erzielen, hängt von der Vision der Führung, effektiven Abläufen und einem geschäftsorientierten Betriebsmodell ab. Die Führung sollte voll investiert und sich für eine CloudOps Transformation mit einem geeigneten Cloud-Betriebsmodell einsetzen, das die Teams dazu anregt, so effizient wie möglich zu arbeiten und Geschäftsergebnisse zu erzielen. Ein geeignetes Betriebsmodell nutzt Personal-, Prozess- und Technologiekapazitäten, um zu skalieren, die Produktivität zu optimieren und durch Agilität, Reaktionsfähigkeit und Anpassung einen Wettbewerbsvorteil zu erlangen. Die langfristige Vision der Organisation wird in Ziele umgesetzt, die Stakeholdern und Verbrauchern Ihrer Cloud-Services unternehmensweit vermittelt werden. Ziele und Betriebsabläufe KPIs sind auf allen Ebenen aufeinander abgestimmt. Diese Vorgehensweise sorgt dafür, dass der langfristige Mehrwert, der sich aus der Umsetzung der folgenden Gestaltungsprinzipien ergibt, dauerhaft gewährleistet ist.
- **Implementieren von Beobachtbarkeit für umsetzbare Erkenntnisse:** Verschaffen Sie sich einen umfassenden Überblick über das Verhalten, die Leistung, die Zuverlässigkeit, die Kosten und den Zustand von Workloads. Legen Sie wichtige Leistungsindikatoren (KPIs) fest und nutzen Sie die Telemetrie zur Beobachtung, um fundierte Entscheidungen zu treffen und umgehend Maßnahmen zu ergreifen, wenn Geschäftsergebnisse gefährdet sind. Verbessern Sie proaktiv Leistung, Zuverlässigkeit und Kosten auf der Grundlage von verwertbaren Daten zur Beobachtbarkeit.
- **Sichere Automatisierung wo möglich:** In der Cloud können Sie die gleichen technischen Vorgehensweisen wie beim Anwendungscode in Ihrer gesamten Umgebung anwenden. Sie können Ihre gesamte Workload und deren Betrieb (Anwendungen, Infrastruktur, Konfiguration und Verfahren) als Code definieren und aktualisieren. Anschließend können Sie den Betrieb Ihrer Workloads automatisieren, indem Sie sie als Reaktion auf Ereignisse initiieren. In der Cloud können Sie Automatisierungssicherheit einsetzen, indem Sie einen Integritätsschutz wie Ratenkontrolle, Fehlerschwellenwerte und Genehmigungen einrichten. Durch eine effektive Automatisierung können Sie konsistente Reaktionen auf Ereignisse durchsetzen, menschliche Fehler begrenzen und den Arbeitsaufwand der Mitarbeiter reduzieren.
- **Vornehmen kleiner, häufiger und umkehrbarer Änderungen:** Entwerfen Sie skalierbare und lose verkoppelte Workloads, sodass Komponenten regelmäßig aktualisiert werden können. Automatisierte Bereitstellungstechniken in Verbindung mit kleineren, inkrementellen Änderungen verringern den „Blast Radius“ und ermöglichen eine schnellere Umkehrung bei Fehlern. Dadurch erhöht sich das Vertrauen, vorteilhafte Änderungen an Ihrer Workload vornehmen zu können,

während die Qualität erhalten bleibt und Sie sich schnell an veränderte Marktbedingungen anpassen können.

- Betriebliche Verfahren regelmäßig nachbessern: Wenn Sie Ihre Workloads weiterentwickeln, passen Sie auch Ihre Betriebsabläufe entsprechend an. Suchen Sie beim Einsatz betrieblicher Verfahren nach Möglichkeiten, diese zu verbessern. Führen Sie regelmäßige Überprüfungen durch und vergewissern Sie sich, dass alle Verfahren effektiv sind und dass die Teams mit ihnen vertraut sind. Wenn Lücken festgestellt werden, aktualisieren Sie die Verfahren entsprechend. Informieren Sie alle Beteiligten und Teams über Aktualisierungen der Verfahren. Gamifizieren Sie Ihren Betrieb zum Weitergeben von bewährten Methoden und zur Schulung von Teams.
- Fehlern vorbeugen: Maximieren Sie den betrieblichen Erfolg, indem Sie Ausfallszenarien entwickeln, um das Risikoprofil der Workload und ihre Auswirkungen auf Ihre Geschäftsergebnisse zu verstehen. Testen Sie die Wirksamkeit Ihrer Verfahren und die Reaktion Ihres Teams auf diese simulierten Fehler. Treffen Sie fundierte Entscheidungen, um offene Risiken zu auszuräumen, die anhand Ihrer Tests identifiziert wurden.
- Aus allen betrieblichen Ereignissen und Metriken 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. Die Erkenntnisse sollten Daten und Anekdoten enthalten, wie die Betriebsabläufe zu den Geschäftsergebnissen beitragen.
- Nutzen Sie Managed Services: Reduzieren Sie den betrieblichen Aufwand, indem Sie nach Möglichkeit AWS Managed Services nutzen. Erstellen Sie operative Verfahren für die Interaktion mit diesen Services.

## Definition

Die bewährten Methoden für betriebliche Exzellenz in der Cloud lassen sich in vier Bereiche einteilen:

- Organisation
- Vorbereitung
- Betrieb
- Weiterentwicklung

Die Leitung Ihrer Organisation definiert Geschäftsziele. Anforderungen und Prioritäten müssen in Ihrer Organisation bekannt sein, damit Aufgaben entsprechend organisiert und durchgeführt und die Geschäftsergebnisse erreicht werden können. Ihre Workload muss die Informationen ausgeben,



die für ihre Unterstützung erforderlich sind. Die Implementierung von Services zur Integration, Bereitstellung und Lieferung Ihrer Workload schafft einen erhöhten Fluss nützlicher Änderungen in die Produktion, indem wiederkehrende Prozesse automatisiert werden.

Es kann Risiken im Zusammenhang mit dem Betrieb Ihrer Workload geben. Verstehen Sie diese Risiken und treffen Sie eine fundierte Entscheidung dazu, ob der Übergang in die Produktion vollzogen werden sollte. Ihre Teams müssen in der Lage sein, Ihre Workload zu unterstützen. Geschäfts- und Betriebsmetriken, die von den gewünschten Geschäftsergebnissen abgeleitet werden, erlauben es Ihnen, den Zustand Ihrer Workload und Ihrer Betriebsaktivitäten nachzuvollziehen und auf Vorfälle zu reagieren. Ihre Prioritäten ändern sich, wenn sich Ihre geschäftlichen Anforderungen und die geschäftliche Umgebung ändern. Verwenden Sie diese als Feedback-Schleife, um Ihre Organisation und den Betrieb Ihrer Workload kontinuierlich zu verbessern.

## Bewährte Methoden

### Note

Alle Fragen zur betrieblichen Exzellenz haben das OPS Präfix als Abkürzung für die Säule.

### Themen

- [Organisation](#)
- [Vorbereitung](#)
- [Betrieb](#)
- [Weiterentwicklung](#)

## Organisation

Um die Prioritäten festlegen zu können, die den geschäftlichen Erfolg ermöglichen, müssen Ihre Teams gemeinsam in Erfahrung bringen, wie sämtliche Workloads aussehen, welche Rolle die einzelnen Teams dabei spielen und was für geschäftliche Ziele damit erreicht werden sollen. Mit gut definierten Prioritäten erzielen Ihre Bemühungen den größtmöglichen Nutzen. Bewerten Sie die Bedürfnisse interner und externer Kunden. Binden Sie dabei alle wichtigen Beteiligten ein, einschließlich der Geschäfts-, Entwicklungs- und Betriebsteams, um zu bestimmen, auf welche Bereiche die Anstrengungen konzentriert werden sollten. Durch das Bewerten von Kundenbedürfnissen wird sichergestellt, dass Sie den Support, der für die Erzielung der gewünschten

geschäftlichen Ergebnisse erforderlich ist, genau kennen und verstehen. Vergewissern Sie sich, dass Sie sich der Richtlinien oder Verpflichtungen bewusst sind, die von der Führung Ihres Unternehmens definiert wurden. Bewerten Sie externe Faktoren, z. B. gesetzliche Compliance-Anforderungen und Branchenstandards, die einen bestimmten Fokus erfordern oder verstärken können. Überprüfen Sie, ob Sie Mechanismen haben, um Änderungen an internen Governance- und externen Compliance-Anforderungen zu identifizieren. Wenn keine Anforderungen festgestellt werden, stellen Sie sicher, dass diese Prüfung sorgfältig durchgeführt wurde. Überprüfen Sie Ihre Prioritäten regelmäßig, damit sie bei Bedarf aktualisiert werden können.

Bewerten Sie Bedrohungen für das Unternehmen (z. B. Geschäftsrisiken und -verpflichtungen und Bedrohungen der Informationssicherheit) und pflegen Sie diese Informationen in einem Risikoregister. Bewerten Sie die Auswirkungen von Risiken und Kompromissen zwischen konkurrierenden Interessen oder alternativen Ansätzen. Beispielsweise kann eine beschleunigte Markteinführung neuer Features vor der Kostenoptimierung Vorrang haben, oder Sie können eine relationale Datenbank für nicht relationale Daten wählen, um die Migration eines Systems ohne Faktorwechsel zu vereinfachen. Wägen Sie die Vorteile und Risiken ab, um fundierte Entscheidungen zu treffen, wenn es darum geht, auf welche Bereiche die Anstrengungen konzentriert werden sollen. Einige Risiken oder Entscheidungen können eine bestimmte Zeit lang akzeptabel sein. Es gibt ggf. die Möglichkeit, die damit verbundenen Risiken zu minimieren, oder es ist zu einem bestimmten Zeitpunkt nicht mehr akzeptabel, dass ein Risiko weiterhin bestehen bleibt. In diesem Fall ergreifen Sie Maßnahmen, um das Risiko zu beheben.

Ihre Teams müssen ihre Rolle beim Erreichen von Geschäftsergebnissen verstehen. Teams müssen ihre Rolle für den Erfolg anderer Teams und die Rolle anderer Teams für ihren Erfolg verstehen und gemeinsame Ziele haben. Indem sie die Konzepte Verantwortlichkeit und Zuständigkeit verstehen und wissen, wie Entscheidung getroffen werden und wer dazu berechtigt ist, können ihre Anstrengungen fokussiert und der Nutzen Ihrer Teams maximiert werden. Die Anforderungen eines Teams werden durch den unterstützten Kunden, die Organisation, die Zusammensetzung des Teams und die Merkmale der jeweiligen Workloads beeinflusst. Es ist nicht sinnvoll, davon auszugehen, dass ein einziges Betriebsmodell alle Teams und Workloads in Ihrer Organisation unterstützen kann.

Stellen Sie sicher, dass für jede Anwendung, jede Workload, jede Plattform und jede Infrastrukturkomponente zuständige Besitzer vorhanden sind und dass jeder Prozess und jedes Verfahren einen festen Besitzer hat, der für die Definition verantwortlich ist, und Besitzer, die für die Leistung verantwortlich sind.

Durch das Verständnis für den geschäftlichen Nutzen der einzelnen Komponenten, Prozesse und Verfahren sowie dafür, weshalb diese Ressourcen vorhanden sind oder Aktivitäten ausgeführt

werden und warum diese Zuständigkeit besteht, basieren die Aktionen Ihrer Teammitglieder auf fundierten Informationen. Definieren Sie eindeutig die Verantwortlichkeiten der Teammitglieder, damit sie entsprechend handeln und Mechanismen zur Identifizierung von Verantwortlichkeit und Zuständigkeit besitzen. Nutzen Sie entsprechende Mechanismen zum Anfordern von Ergänzungen, Änderungen und Ausnahmen, damit Sie die Innovation nicht einschränken. Definieren Sie Vereinbarungen zwischen Teams, die beschreiben, wie sie für die gegenseitige und die Unterstützung der Geschäftsergebnisse zusammenarbeiten.

Unterstützen Sie Ihre Teammitglieder, damit sie effektiver handeln und positiv zu Ihrem Geschäftsergebnis beitragen können. Die beteiligten Führungskräfte sollten Erwartungen festlegen und den Erfolg messen. Die Geschäftsführung sollte Sponsor, Fürsprecher und treibende Kraft für die Übernahme bewährter Methoden und die Weiterentwicklung der Organisation sein. Lassen Sie die Teammitglieder Maßnahmen ergreifen, wenn Ergebnisse gefährdet sind, um Auswirkungen zu minimieren. Sie müssen dazu ermutigt werden, Entscheidungsträger und Interessenvertreter über ermittelte Risiken zu informieren, damit diese angegangen und Vorfälle vermieden werden können. Kommunizieren Sie bekannte Risiken und geplante Ereignisse zeitnah, klar und umsetzbar, damit Teammitglieder rechtzeitig entsprechende Maßnahmen ergreifen können.

Ermöglichen Sie das Ausprobieren neuer Ansätze, damit schneller Erkenntnisse erreicht werden, und sorgen Sie dafür, dass Teammitglieder interessiert und motiviert bleiben. Teams müssen ihre Fähigkeiten erweitern, um neue Technologien einzuführen und Änderungen bei Bedarf und Zuständigkeiten zu unterstützen. Dies sollten sie durch spezielle, strukturierte Lernzeiten unterstützen und ermutigen. Stellen Sie sicher, dass Ihre Teams über die nötigen Ressourcen verfügen (Tools und Teammitglieder), um positiv zu Ihren Geschäftsergebnissen beitragen zu können. Profitieren Sie von der Diversität in der gesamten Organisation, um verschiedene einzigartige Standpunkte zu erfahren. Nutzen Sie diese Perspektive, um Innovation zu fördern, Ihre Annahmen in Frage zu stellen und das Risiko einer Verzerrung durch automatische Bestätigung zu reduzieren. Stärken Sie die Inklusion, Diversität und Zugänglichkeit innerhalb Ihrer Teams, um nützliche Perspektiven zu gewinnen.

Wenn es externe gesetzliche Vorschriften oder Compliance-Anforderungen gibt, die für Ihre Organisation gelten, sollten Sie Ihre Teams mithilfe der von [AWS Cloud Compliance](#) bereitgestellten Ressourcen darin schulen, welche Auswirkungen es bei Ihren Prioritäten zu berücksichtigen gilt. Das Well-Architected Framework legt den Schwerpunkt auf Lernen, Messen und Verbessern. Es bietet Ihnen einen konsistenten Ansatz zur Bewertung von Architekturen und zur Implementierung von Designs, die sich im Laufe der Zeit skalieren lassen. AWS bietet die AWS Well-Architected Tool Möglichkeit, Ihren Ansatz vor der Entwicklung, den Status Ihrer Workloads vor der Produktion und den Status Ihrer Workloads in der Produktion zu überprüfen. Sie können Workloads mit den neuesten bewährten AWS Architekturpraktiken vergleichen, ihren Gesamtstatus überwachen und Einblicke in

potenzielle Risiken gewinnen. AWS Trusted Advisor ist ein Tool, das Zugriff auf eine Reihe zentraler Prüfungen bietet, die Optimierungen empfehlen, die Ihnen bei der Festlegung Ihrer Prioritäten helfen können. Kunden mit Business und Enterprise Support erhalten Zugriff auf weitere Prüfungen in den Bereichen Sicherheit, Zuverlässigkeit, Leistung, Kostenoptimierung und Nachhaltigkeit, die beim Festlegen von Prioritäten noch hilfreicher sind.

AWS kann Ihnen helfen, Ihre Teams über die Services AWS und deren Dienste aufzuklären, damit sie besser verstehen, wie sich ihre Entscheidungen auf Ihre Arbeitslast auswirken können. Nutzen Sie die von AWS Support (AWS Knowledge Center, AWS Diskussionsforen und AWS Support Center) bereitgestellten Ressourcen und die AWS Dokumentation, um Ihre Teams zu schulen. Wenden Sie sich an AWS Support das AWS Support Center, um Hilfe bei Ihren AWS Fragen zu erhalten. AWS teilt auch bewährte Verfahren und Muster, die wir durch den Betrieb von AWS The Amazon Builders' Library gelernt haben. Eine Vielzahl weiterer nützlicher Informationen ist im AWS Blog und im offiziellen AWS Podcast verfügbar. AWS Training and Certification bietet einige Schulungen in Form von digitalen Grundlagenkursen zum Selbststudium an AWS . Sie können sich auch für eine von einem Kursleiter geleitete Schulung anmelden, um die Weiterentwicklung der Fähigkeiten Ihrer Teams zu unterstützen. AWS

Verwenden Sie Tools oder Dienste, mit denen Sie Ihre Umgebungen kontenübergreifend zentral verwalten können, z. B. AWS Organizations um Ihre Betriebsmodelle zu verwalten. Services wie AWS Control Tower erweitern diese Verwaltungsfunktionen, indem sie es Ihnen ermöglichen, Blueprints (zur Unterstützung Ihrer Betriebsmodelle) für die Einrichtung von Konten zu definieren, fortlaufende Governance-Funktionen anzuwenden und die Bereitstellung neuer Konten zu automatisieren. AWS Organizations Managed Services-Anbieter wie AWS Managed Services AWS Managed Services Partner oder Managed Services Providers im AWS Partnernetzwerk bieten Fachwissen bei der Implementierung von Cloud-Umgebungen und unterstützen Sie bei Ihren Sicherheits- und Compliance-Anforderungen und Geschäftszielen. Durch die Erweiterung Ihres Betriebsmodells um verwaltete Services können Sie Zeit und Ressourcen sparen, Ihre internen Teams klein halten und sich auf strategische Ergebnisse konzentrieren, die Ihr Unternehmen auszeichnen, anstatt neue Fähigkeiten und Kompetenzen zu entwickeln.

In den folgenden Fragen geht es um Überlegungen zur betrieblichen Exzellenz. (Eine Liste der Fragen und bewährten Methoden zur betrieblichen Exzellenz finden Sie im [Anhang](#).)

### OPS1: Wie bestimmen Sie, was Ihre Prioritäten sind?

Jeder muss verstehen, welchen Beitrag er zum Geschäftserfolg leistet. Setzen Sie sich gemeinsame Ziele, damit Sie die Prioritäten für Ressourcen festlegen können. Dadurch erzielen Ihre Bemühungen den größtmöglichen Nutzen.

### OPS2: Wie strukturieren Sie Ihre Organisation, um Ihre Geschäftsergebnisse zu unterstützen?

Ihre Teams müssen ihre Rolle beim Erreichen von Geschäftsergebnissen verstehen. Teams müssen ihre Rolle für den Erfolg anderer Teams und die Rolle anderer Teams für ihren Erfolg verstehen und gemeinsame Ziele haben. Indem sie die Konzepte Verantwortlichkeit und Zuständigkeit verstehen und wissen, wie Entscheidungen getroffen werden und wer dazu berechtigt ist, können ihre Anstrengungen fokussiert und der Nutzen Ihrer Teams maximiert werden.

### OPS3: Wie unterstützt Ihre Unternehmenskultur Ihre Geschäftsergebnisse?

Lassen Sie Ihren Teammitgliedern Unterstützung zukommen, damit sie effektiver handeln und Ihr Geschäftsergebnis unterstützen können.

Manchmal kann es vorkommen, dass das Augenmerk zu stark auf eine kleine Auswahl von operativen Prioritäten gerichtet wird. Gehen Sie langfristig gut ausgewogen vor, um sicherzustellen, dass erforderliche Fähigkeiten entwickelt und Risiken verwaltet werden. Überprüfen Sie die Prioritäten regelmäßig und passen Sie sie an geänderte Anforderungen an. Wenn Verantwortlichkeit und Zuständigkeit undefiniert oder unbekannt sind, besteht das Risiko, dass erforderliche Aktionen nicht rechtzeitig ausgeführt werden und redundante und potenziell widersprüchliche Anstrengungen unternommen werden, um diese Anforderungen zu erfüllen. Die Organisationskultur wirkt sich direkt auf die Zufriedenheit und Bindung der Teammitglieder aus. Ermöglichen Sie die Interaktion und aktivieren Sie die Fähigkeiten Ihrer Teammitglieder für den Erfolg Ihres Unternehmens. Durch Experimente werden Innovationen möglich und Ideen zu Ergebnissen. Sie sollten anerkennen, dass unerwünschte Ergebnisse erfolgreiche Experimente sein können, durch die ein Pfad aufgezeigt wurde, der nicht zum Erfolg führt.

## Vorbereitung

Zur Vorbereitung auf die betriebliche Exzellenz müssen Sie in Erfahrung bringen, mit welchen Workloads zu rechnen ist und wie diese wahrscheinlich ausfallen werden. Dann können Sie diese so gestalten, dass Sie Einblick in deren Status erhalten und entsprechende Verfahren zu deren Unterstützung entwerfen.

Gestalten Sie Ihre Workload so, dass sie die Informationen bereitstellt, die Sie benötigen, um den internen Status (z. B. Metriken, Protokolle, Ereignisse und Ablaufverfolgungen) über alle Komponenten hinweg zu verstehen. Dies erhöht die Beobachtbarkeit und erleichtert die Untersuchung von Problemen. Beobachtbarkeit geht über die einfache Überwachung hinaus und bietet ein umfassendes Verständnis der internen Funktionsweise eines Systems auf der Grundlage seiner externen Ergebnisse. Beobachtbarkeit basiert auf Metriken, Protokollen und Ablaufverfolgungen und liefert tiefgreifende Erkenntnisse zum Verhalten und zur Dynamik von Systemen. Mit effektiver Beobachtbarkeit können Teams Muster, Anomalien und Trends erkennen, sodass sie potenzielle Probleme proaktiv angehen und einen optimalen Systemzustand aufrechterhalten können. Die Identifizierung wichtiger Leistungsindikatoren (KPIs) ist von entscheidender Bedeutung, um sicherzustellen, dass die Überwachungsaktivitäten und die Geschäftsziele aufeinander abgestimmt werden. Diese Abstimmung stellt sicher, dass Teams datengestützte Entscheidungen anhand von Metriken treffen, die wirklich wichtig sind, wodurch sowohl die Systemleistung als auch die Geschäftsergebnisse optimiert werden. Darüber hinaus ermöglicht Beobachtbarkeit Unternehmen, proaktiv statt reaktiv zu handeln. Teams können die cause-and-effect Zusammenhänge innerhalb ihrer Systeme verstehen und Probleme vorhersagen und verhindern, anstatt nur auf sie zu reagieren. Da sich Workloads weiterentwickeln, ist es wichtig, die Beobachtbarkeitsstrategie immer wieder neu aufzugreifen und zu verfeinern, um sicherzustellen, dass sie relevant und effektiv bleibt.

Verwenden Sie Strategien, die die Übertragung von Änderungen auf die Produktionsumgebung verbessern und einen Faktorwechsel, schnelles Feedback zur Qualität sowie eine schnelle Fehlerbehebung erreichen. 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 oder in Ihren Umgebungen erkannt werden, schnell aufgespürt und gelöst werden.

Verwenden Sie Ansätze, die schnelles Feedback zur Qualität liefern und eine schnelle Wiederherstellung bei Änderungen ermöglichen, die nicht zu den gewünschten Ergebnissen führen. Mit diesen Verfahren können Sie die Auswirkung von Problemen eindämmen, die durch Änderungen entstehen. Kalkulieren Sie nicht erfolgreiche Änderungen ein, damit Sie bei Bedarf

schneller reagieren und die vorgenommenen Änderungen testen und validieren können. Achten Sie auf geplante Aktivitäten in Ihren Umgebungen, damit Sie mit dem Risiko von Änderungen umgehen können, die sich auf geplante Aktivitäten auswirken. Nehmen Sie häufige, kleine und umkehrbare Änderungen vor, um den Umfang der Änderungen einzuschränken. Dies beschleunigt die Fehlersuche und ermöglicht eine schnellere Korrektur, da die Möglichkeit besteht, eine Änderung zurückzusetzen. Dies bedeutet auch, dass Sie häufiger von den Vorteilen wertvoller Änderungen profitieren.

Bewerten Sie die operative Bereitschaft Ihrer Workloads, der Prozesse und Verfahren sowie Ihrer Mitarbeiter, damit Sie die operativen Risiken im Zusammenhang mit Ihrer Workload genau kennen. Wenden Sie einen konsistenten Prozess (inklusive manueller und automatisierter Checklisten) an, damit Sie wissen, wann Sie bereit sind, Ihre Workload oder eine Änderung live zu schalten. Auf diese Weise können Sie auch alle Bereiche finden, um die Sie sich kümmern müssen. Ihre routinemäßigen Aktivitäten sollten in Runbooks notiert werden, und Playbooks helfen Ihnen bei der Lösung von Problemen. Machen Sie sich mit den Vorteilen und Risiken vertraut, um fundierte Entscheidungen treffen und Änderungen für die Produktion ermöglichen zu können.

AWS ermöglicht es Ihnen, Ihre gesamte Arbeitslast (Anwendungen, Infrastruktur, Richtlinien, Verwaltung und Betrieb) als Code anzuzeigen. Das bedeutet, dass Sie für jedes Element Ihres Stacks dieselbe technische Vorgehensweise anwenden können, die Sie für Anwendungscode nutzen. Diese können Sie über Teams oder Organisationen hinweg teilen und damit die Auswirkung der Entwicklungsbemühungen verstärken. Verwenden Sie Operations-as-Code in der Cloud und nutzen Sie die Möglichkeit, sicher zu experimentieren, Ihre Workload und betriebliche Verfahren zu entwickeln und Ausfälle zu üben. Die Verwendung AWS CloudFormation ermöglicht Ihnen konsistente Sandbox-Entwicklungs-, Test- und Produktionsumgebungen mit Vorlagen und einem höheren Maß an Betriebskontrolle.

In den folgenden Fragen geht es um Überlegungen zur betrieblichen Exzellenz.

#### OPS4: Wie implementieren Sie Observability in Ihren Workload?

Implementieren Sie Beobachtbarkeit in Ihre Workload, damit Sie deren Zustand verstehen und datengesteuerte Entscheidungen auf der Grundlage von Geschäftsanforderungen treffen können.

### OPS5: Wie können Sie Fehler reduzieren, deren Behebung vereinfachen und den Produktionsfluss verbessern?

Verwenden Sie Ansätze, die den Fluss von Änderungen in die Produktion verbessern, die einen Faktorwechsel ermöglichen, schnelles Feedback zur Qualität geben und Fehler beheben. 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.

### OPS6: Wie minimieren Sie Bereitstellungsrisiken?

Verwenden Sie Ansätze, die schnelles Feedback zur Qualität liefern und eine schnelle Wiederherstellung bei Änderungen ermöglichen, die nicht zu den gewünschten Ergebnissen führen. Mit diesen Verfahren können Sie die Auswirkung von Problemen eindämmen, die durch Änderungen entstehen.

### OPS7: Woher wissen Sie, dass Sie bereit sind, einen Workload zu unterstützen?

Bewerten Sie die Betriebsbereitschaft Ihrer Workloads, von Prozessen und Verfahren sowie Ihrer Mitarbeiter, damit Sie die betrieblichen Risiken im Zusammenhang mit Ihrer Workload genau kennen.

Investieren Sie in die Implementierung von Betriebsabläufen als Code, um die Produktivität von Betriebsmitarbeitern zu maximieren, Fehlerraten zu minimieren und automatisierte Reaktionen zu erreichen. Beugen Sie Fehlern nach Möglichkeit vor und stellen Sie entsprechende Abläufe auf. Wenden Sie Metadaten mithilfe von Ressourcen-Tags an und AWS Resource Groups folgen Sie einer konsistenten Tagging-Strategie, um Ihre Ressourcen zu identifizieren. Versehen Sie Ihre Ressourcen mit Tags für Organisation, Kostenkalkulation, Zugriffssteuerung und Zielrichtung der Ausführung von automatisierten Betriebsaktivitäten. Übernehmen Sie Bereitstellungsmethoden, die die Elastizität der Cloud ausnutzen, um Entwicklungsaktivitäten, die Vorabbereitstellung von Systemen und damit schnellere Implementierungen zu ermöglichen. Wenn Sie an Checklisten, mit denen Sie Ihre Workloads beurteilen, Änderungen vornehmen, bedenken Sie auch, was mit live geschalteten Systemen geschehen soll, die mit den Änderungen nicht mehr kompatibel sind.



## Betrieb

Beobachtbarkeit ermöglicht es Ihnen, sich auf aussagekräftige Daten zu konzentrieren und die Interaktionen und Ergebnisse Ihrer Workload zu verstehen. Indem Sie sich auf wichtige Erkenntnisse konzentrieren und unnötige Daten eliminieren, behalten Sie einen einfachen Ansatz zum Verständnis der Workload-Leistung bei. Es ist wichtig, Daten nicht nur zu erfassen, sondern sie auch richtig zu interpretieren. Definieren Sie klare Ausgangswerte, legen Sie geeignete Alarmschwellenwerte fest und überwachen Sie aktiv, ob Abweichungen vorliegen. Wenn eine wichtige Metrik abweicht, insbesondere wenn sie mit anderen Daten korreliert, kann dies spezifische Problembereiche aufzeigen. Mit Beobachtbarkeit sind Sie besser in der Lage, potenzielle Herausforderungen vorherzusehen und zu bewältigen sowie sicherzustellen, dass Ihre Workload reibungslos funktioniert und den Geschäftsanforderungen entspricht.

Der erfolgreiche Betrieb einer Workload wird daran gemessen, ob geschäftliche Ergebnisse erreicht und Kundenanforderungen erfüllt werden. Definieren Sie zu erwartende Ergebnisse, legen Sie fest, wie der Erfolg gemessen wird, und geben Sie an, welche Metriken in Berechnungen verwendet werden sollen, mit denen festgestellt wird, ob Workload und Betrieb erfolgreich sind. Der betriebliche Status beinhaltet sowohl den Status der Workload als auch den Status und Erfolg der betrieblichen Vorgänge, die zur Unterstützung der Workload ausgeführt werden (z. B. Bereitstellung und Vorfalldiagnose). Legen Sie Metrikausgangswerte für die Verbesserung, Untersuchung und Intervention fest. Erfassen 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 Untersuchung und Behebung von Problemen 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 eines zuständigen Besitzers festgelegt ist. Legen Sie vorab fest, welche Mitarbeiter für die Behebung eines Ereignisses zuständig sein sollen. Dazu gehören auch Prozesse für einen Eskalationsprozess, über den im Notfall auf der Grundlage der Dringlichkeit und Auswirkungen weitere Mitarbeiter herangezogen werden sollen. Für den Fall, dass eine nicht vorab festgelegte Vorfalldiagnose

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 auf die Zielgruppe (z. B. Kunde, Unternehmen, Entwickler, Betriebsteam) zugeschnitten sind, damit die jeweiligen Personen geeignete Maßnahmen durchführen können und wissen, wann der normale Betrieb wieder weitergeht.

In können Sie Dashboard-Ansichten Ihrer Messwerte generieren AWS, die aus Workloads und nativ aus Workloads erfasst wurden. AWS Sie können Anwendungen von Drittanbietern nutzen CloudWatch, um Ansichten der Betriebsaktivitäten auf Geschäfts-, Workload- und Betriebsebene zu aggregieren und zu präsentieren. AWS bietet Einblicke in die Arbeitslast mithilfe von Protokollierungsfunktionen wie AWS X-Ray CloudWatch, CloudTrail, und VPC Flow Logs, um Workload-Probleme zu identifizieren und so die Ursachenanalyse und -behebung zu unterstützen.

In den folgenden Fragen geht es um Überlegungen zur betrieblichen Exzellenz.

#### OPS8: Wie nutzen Sie die Workload-Beobachtbarkeit in Ihrem Unternehmen?

Sorgen Sie für einen optimalen Zustand der Workload, indem Sie die Beobachtbarkeit nutzen. Nutzen Sie relevante Metriken, Protokolle und Ablaufverfolgungen, um sich einen umfassenden Überblick über die Leistung Ihrer Workload zu verschaffen und Probleme effizient zu beheben.

#### OPS9: Wie beurteilen Sie den Zustand Ihrer Betriebsabläufe?

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

#### OPS10: Wie managen Sie Arbeitslast und Betriebsereignisse?

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

Alle von Ihnen erfassten Metriken sollten an die geschäftlichen Anforderungen und Ergebnisse angepasst werden, die sie unterstützen. Entwickeln Sie skriptbasierte Antworten auf bekannte Ereignisse und automatisieren Sie deren Leistung als Reaktion auf die Ereigniserkennung.

## Weiterentwicklung

Lernen Sie dazu und streben Sie kontinuierliche Verbesserungen an, um nachhaltige betriebliche Exzellenz zu erreichen. Planen Sie Arbeitszyklen ein, um nahezu kontinuierlich kleinere Verbesserungen vorzunehmen. Analysieren Sie nach einem Vorfall alle Ereignisse, die sich auf den Kunden auswirken. Identifizieren Sie die beitragenden Faktoren und Präventivmaßnahmen, um Wiederholungen zu begrenzen oder zu verhindern. Teilen Sie den betroffenen Communitys die beitragenden Faktoren nach Bedarf mit. 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.

Bei AWS aktivierter Option können Sie Ihre Protokolldaten nach Amazon S3 exportieren oder Protokolle zur Langzeitspeicherung direkt an Amazon S3 senden. Mithilfe AWS Glue können Sie Ihre Protokolldaten in Amazon S3 ermitteln und für Analysen aufbereiten und die zugehörigen Metadaten in der speichern AWS Glue Data Catalog. Amazon Athena kann dann durch seine native Integration mit verwendet werden AWS Glue, um Ihre Protokolldaten zu analysieren und sie standardmäßig abzufragen. SQL Mit einem Business Intelligence-Tool wie Amazon QuickSight können Sie Ihre Daten visualisieren, untersuchen und analysieren. Erkennen von Trends und Ereignissen, die zu einer Verbesserung führen können.

In der folgenden Frage geht es um Überlegungen zur betrieblichen Exzellenz.

OPS11: Wie entwickeln Sie Ihre Betriebsabläufe weiter?

Widmen Sie nahezu kontinuierlichen inkrementellen Verbesserungen Zeit und Ressourcen, um die Effektivität und Effizienz Ihrer Betriebsabläufe weiterzuentwickeln.

Die Voraussetzung für eine erfolgreiche Weiterentwicklung des Betriebs sind kontinuierliche kleinere Verbesserungen, das Bereitstellen sicherer Umgebungen und Zeitfenster zum Experimentieren, das Entwickeln und Testen von Verbesserungen sowie die Schaffung 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.

## Ressourcen

Weitere Informationen zu bewährten Methoden für betriebliche Exzellenz finden Sie in den folgenden Ressourcen.

### Dokumentation

- [DevOps und AWS](#)

### Whitepaper

- [Säule „Betriebliche Exzellenz“](#)

### Video

- [DevOps bei Amazon](#)

## Sicherheit

In der Säule der Sicherheit wird beschrieben, wie Sie Daten, Systeme und Komponenten so schützen, dass Sie Cloud-Technologien nutzen können, um Ihre Sicherheitslage zu verbessern.

Die Säule „Sicherheit“ gibt einen Überblick über konzeptionelle Grundsätze, bewährte Methoden und Fragen. Verbindliche Anleitungen zur Implementierung finden Sie im [Whitepaper „Säule der Sicherheit“](#).

### Themen

- [Designprinzipien](#)
- [Definition](#)
- [Bewährte Methoden](#)

- [Ressourcen](#)

## Designprinzipien

Die Cloud bietet zahlreiche Möglichkeiten zur Verbesserung Ihrer Workload-Sicherheit:

- Implementieren Sie ein starkes Identitätsfundament: Implementieren Sie das Prinzip der geringsten Rechte und setzen Sie die Aufgabentrennung durch, wobei für jede Interaktion mit Ihren AWS Ressourcen die entsprechende Autorisierung erforderlich ist. Zentralisieren Sie die Identitätsverwaltung und vermeiden Sie die Abhängigkeit von langfristigen statischen Anmeldeinformationen.
- Sicherstellen der Nachverfolgbarkeit: Überwachen, melden und prüfen Sie Aktionen und Änderungen in Ihrer Umgebung in Echtzeit. Integrieren Sie die Protokoll- und Metrikerfassung in Systeme, um automatisch zu untersuchen und Maßnahmen zu ergreifen.
- Sicherheit auf allen Ebenen: Etablieren Sie eine Abwehrstrategie mit mehreren Sicherheitsmechanismen. Auf alle Ebenen anwenden (z. B. NetzwerkrandVPC, Lastenausgleich, jede Instanz und jeden Rechendienst, Betriebssystem, Anwendung und Code).
- 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 Ihre Daten nach Sensibilität und nutzen sie Mechanismen wie Verschlüsselung, Tokenisierung der Daten und Zugriffskontrolle.
- Trennen von Benutzern und Daten: Nutzen Sie Mechanismen und Tools, um den direkten Zugriff auf Daten zu minimieren/verhindern und das manuelle Verarbeiten Ihrer Daten zu reduzieren. 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 zum Vorfalldmanagement sowie Richtlinien für die Überprüfung ein. Simulieren Sie Vorfalldreaktionen und nutzen Sie automatisierbare Tools, um die Erkennung, Untersuchung und Wiederherstellung zu beschleunigen.

## Definition

Es gibt sieben bewährte Methoden für die Sicherheit in der Cloud:

- Sicherheitsgrundlagen
- Identity and Access Management
- Erkennung
- Schutz der Infrastruktur
- Datenschutz
- Vorfallreaktion
- Anwendungssicherheit

Vor der Entwicklung von Workloads 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 Modell der AWS gemeinsamen Verantwortung hilft Unternehmen, die die Cloud einsetzen, dabei, ihre Sicherheits- und Compliance-Ziele zu erreichen. Da die Infrastruktur, die unsere Cloud-Dienste unterstützt, AWS physisch gesichert wird, können Sie sich als AWS Kunde darauf konzentrieren, Dienste zur Erreichung Ihrer Ziele zu nutzen. Die AWS Cloud bietet außerdem besseren Zugriff auf Sicherheitsdaten und einen automatisierten Ansatz zur Reaktion auf Sicherheitsereignisse.

## Bewährte Methoden

Themen

- [Sicherheit](#)
- [Identity and Access Management](#)
- [Erkennung](#)
- [Schutz der Infrastruktur](#)
- [Datenschutz](#)
- [Vorfallreaktion](#)

- [Anwendungssicherheit](#)

## Sicherheit

In der folgenden Frage geht es um Überlegungen zur Sicherheit. (Eine Liste der Fragen und bewährten Methoden zur Sicherheit finden Sie im [Anhang](#).)

### SEC1: Wie verwalten Sie Ihren Workload sicher?

Um Ihre Workload sicher zu betreiben, müssen Sie in allen Sicherheitsbereichen übergreifende bewährte Methoden anwenden. Wenden Sie die Anforderungen und Prozesse, die Sie im Bereich Operational Excellence auf Organisations- und Workload-Ebene definiert haben, auf alle Bereiche an.

Wenn Sie sich über Empfehlungen AWS, Branchenquellen und Bedrohungsinformationen auf dem Laufenden halten, können Sie Ihr Bedrohungsmodell und Ihre Kontrollziele weiterentwickeln. Durch die Automatisierung von Sicherheitsprozessen, Tests und Validierungen können Sie Ihre Sicherheitsabläufe skalieren.

Es wird empfohlen AWS, die verschiedenen Workloads nach Konten auf der Grundlage ihrer Funktion und ihrer Compliance- oder Datenvertraulichkeitsanforderungen zu trennen.

## Identity and Access Management

Das Identity and Access Management ist ein wichtiger Bestandteil eines Informationssicherheitsprogramms. Es stellt sicher, dass nur autorisierte und authentifizierte Benutzer in dem von Ihnen gewünschten Umfang auf Ihre Ressourcen zugreifen können. Definieren Sie beispielsweise Prinzipien (d. h. Konten, Benutzer, Rollen und Services, 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 wird die Rechteverwaltung hauptsächlich vom Dienst AWS Identity and Access Management (IAM) unterstützt, mit dem Sie den Benutzer- und programmgesteuerten Zugriff auf AWS Dienste und Ressourcen steuern können. Wenden Sie detaillierte Richtlinien an, um Benutzern, Gruppen, Rollen oder Ressourcen Berechtigungen zuzuweisen. Sie haben auch die Möglichkeit, strenge Kennwortpraktiken vorzuschreiben, z. B. den Grad der Komplexität, die Vermeidung der

Wiederverwendung und die Erzwingung einer Multi-Faktor-Authentifizierung (MFA). Sie haben die Möglichkeit, die Rechteverwaltung mit Ihrem Verzeichnisdienst zu verbinden. Für Workloads, auf die Systeme Zugriff haben müssen AWS, IAM ermöglicht es sicheren Zugriff über Rollen, Instanzprofile, Identitätsverbund und temporäre Anmeldeinformationen.

In den folgenden Fragen geht es um Überlegungen zur Sicherheit.

## SEC2: Wie verwaltet man Identitäten für Personen und Maschinen?

Es gibt zwei Arten von Identitäten, die Sie verwalten müssen, wenn Sie sichere AWS Workloads betreiben möchten. Wenn Sie verstehen, welche Arten von Identitäten Sie verwalten und Zugriff gewähren müssen, können Sie sicherstellen, dass die richtigen Identitäten unter den richtigen Bedingungen Zugriff auf die richtigen Ressourcen haben.

**Menschliche Identitäten:** Ihre Administratoren, Entwickler, Betreiber und Endbenutzer benötigen eine Identität, um auf Ihre AWS Umgebungen und Anwendungen zugreifen zu können. Dies sind Mitglieder Ihrer Organisation oder externe Benutzer, mit denen Sie zusammenarbeiten und die über einen Webbrowser, eine Client-Anwendung oder interaktive Befehlszeilentools mit Ihren AWS Ressourcen interagieren.

**Maschinenidentitäten:** Ihre Dienstanwendungen, Betriebstools und Workloads benötigen eine Identität, um Anfragen an AWS Dienste zu stellen, z. B. um Daten zu lesen. Zu diesen Identitäten gehören Maschinen, die in Ihrer AWS Umgebung ausgeführt werden, z. B. EC2 Amazon-Instances oder AWS Lambda -Funktionen. Sie können auch Maschinenidentitäten für externe Parteien verwalten, die Zugriff benötigen. Darüber hinaus benötigen möglicherweise auch Computer außerhalb AWS dieser Systeme Zugriff auf Ihre AWS Umgebung.

## SEC3: Wie verwalten Sie Berechtigungen für Personen und Maschinen?

Verwalten Sie Berechtigungen, um den Zugriff auf Personen- und Maschinenidentitäten zu kontrollieren, die Zugriff AWS auf Ihre Arbeitslast benötigen. Berechtigungen steuern, wer worauf und unter welchen Bedingungen zugreifen kann.

Anmeldeinformationen dürfen nicht zwischen Benutzern oder Systemen weitergegeben werden. Der Benutzerzugriff sollte nach dem Prinzip der geringsten Rechte gewährt werden, wobei bewährte Verfahren, einschließlich Kennwortanforderungen, berücksichtigt und durchgesetzt werden sollten.



MFA Der programmgesteuerte Zugriff, einschließlich der API Aufrufe von AWS Diensten, sollte mit temporären Zugangsdaten und Zugangsdaten mit eingeschränkten Rechten erfolgen, wie sie beispielsweise von der ausgestellt wurden. AWS Security Token Service

Benutzer benötigen programmatischen Zugriff, wenn sie mit AWS außerhalb des interagieren möchten. AWS Management Console Die Art und Weise, wie programmatischer Zugriff gewährt wird, hängt vom Benutzertyp ab, der zugreift. AWS

Um Benutzern programmgesteuerten Zugriff zu gewähren, wählen Sie eine der folgenden Optionen.

Welcher Benutzer benötigt programmgesteuerten Zugriff?	Bis	Von
<p>Mitarbeiteridentität</p> <p>(In IAM Identity Center verwaltete Benutzer)</p>	<p>Verwenden Sie temporäre Anmeldeinformationen, um programmatische Anfragen an AWS CLI AWS SDKs, oder AWS APIs zu signieren.</p>	<p>Befolgen Sie die Anweisungen für die Schnittstelle, die Sie verwenden möchten.</p> <ul style="list-style-type: none"> <li>• Informationen zu den AWS CLI finden Sie <a href="#">unter Konfiguration der AWS CLI zur Verwendung AWS IAM Identity Center</a> im AWS Command Line Interface Benutzerhandbuch.</li> <li>• Informationen zu AWS SDKs Tools und AWS APIs finden Sie unter <a href="#">IAM Identity Center-Authentifizierung</a> im Referenzhandbuch AWS SDKs und im Tools-Referenzhandbuch.</li> </ul>
<p>IAM</p>	<p>Verwenden Sie temporäre Anmeldeinformationen, um programmatische Anfragen an das AWS CLI AWS SDKs, oder AWS APIs zu signieren.</p>	<p>Folgen Sie den Anweisungen unter <a href="#">Verwenden temporärer Anmeldeinformationen mit AWS Ressourcen</a> im IAM Benutzerhandbuch.</p>

Welcher Benutzer benötigt programmgesteuerten Zugriff?	Bis	Von
IAM	<p>(Nicht empfohlen)</p> <p>Verwenden Sie langfristige Anmeldeinformationen, um programmatische Anfragen an das AWS CLI AWS SDKs, oder AWS APIs zu signieren.</p>	<p>Befolgen Sie die Anweisungen für die Schnittstelle, die Sie verwenden möchten.</p> <ul style="list-style-type: none"> <li>• Informationen dazu AWS CLI finden Sie unter <a href="#">Authentifizierung mithilfe von IAM Benutzeranmeldedaten</a> im AWS Command Line Interface Benutzerhandbuch.</li> <li>• Informationen zu AWS SDKs und Tools finden Sie unter <a href="#">Authentifizieren mit langfristigen Anmeldeinformationen</a> im Referenzhandbuch AWS SDKs und im Tools-Referenzhandbuch.</li> <li>• Weitere Informationen finden Sie unter <a href="#">Verwaltung von Zugriffsschlüsseln für IAM Benutzer</a> im IAM Benutzerhandbuch. AWS APIs</li> </ul>

AWS stellt Ressourcen bereit, die Sie bei der Identitäts- und Zugriffsverwaltung unterstützen können. Mehr zu den bewährten Methoden erfahren Sie in unseren praktischen Übungen zu den Themen [Verwaltung von Anmeldeinformationen und Authentifizierung](#), [Steuerung des Benutzerzugriffs](#) und [Steuerung des programmgesteuerten Zugriffs](#).

## Erkennung

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 Ihrer Organisation ermöglichen, den Umfang anomaler Aktivitäten zu ermitteln und zu verstehen.

In können Sie detektivische Kontrollen implementieren AWS, indem Sie Protokolle, Ereignisse und Überwachungen verarbeiten und so Prüfungen, automatische Analysen und Alarme ermöglichen. CloudTrail protokolliert, AWS API ruft auf und CloudWatch ermöglicht die Überwachung von Metriken mit Alarmfunktion und AWS Config stellt den Konfigurationsverlauf bereit. Amazon GuardDuty ist ein verwalteter Service zur Bedrohungserkennung, der kontinuierlich nach böartigem oder unberechtigtem Verhalten sucht, um Sie beim Schutz Ihrer AWS Konten und Workloads zu unterstützen. Mit Serviceprotokollen – etwa von Amazon Simple Storage Service (Amazon S3) – können Sie Zugriffsanfragen protokollieren.

In der folgenden Frage geht es um Überlegungen zur Sicherheit.

#### SEC4: Wie erkennen und untersuchen Sie Sicherheitsereignisse?

Erfassen und analysieren Sie Ereignisse anhand von Protokollen und Metriken, um mehr Transparenz zu erhalten. Reagieren Sie auf Sicherheitsereignisse und potenzielle Bedrohungen, um Ihre Workload zu schützen.

Die Protokollverwaltung ist für eine Well-Architected-Workload 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 On-Premises ausschlaggebend.

In AWS können Sie die statusbehaftete und zustandslose Paketinspektion implementieren, entweder mithilfe von AWS-nativen Technologien oder mithilfe von Partnerprodukten und -diensten, die über die erhältlich sind. AWS Marketplace Sie sollten Amazon Virtual Private Cloud (AmazonVPC) verwenden, um eine private, sichere und skalierbare Umgebung zu erstellen, in der Sie Ihre Topologie definieren können — einschließlich Gateways, Routing-Tabellen sowie öffentlichen und privaten Subnetzen.

In den folgenden Fragen geht es um Überlegungen zur Sicherheit.

### SEC5: Wie schützen Sie Ihre Netzwerkressourcen?

Alle Workloads, die über eine Art Netzwerkverbindung verfügen, unabhängig davon, ob es sich um das Internet oder ein privates Netzwerk handelt, erfordern mehrere Abwehrebene, um Schutz vor externen und internen Netzwerkbedrohungen sicherzustellen.

### SEC6: Wie schützen Sie Ihre Rechenressourcen?

Die Rechenressourcen in Ihrer Workload erfordern mehrere Verteidigungsebenen, um sie vor externen und internen Bedrohungen zu schützen. Zu den Rechenressourcen gehören EC2 Instanzen, Container, AWS Lambda Funktionen, Datenbankdienste, IoT-Geräte und mehr.

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

AWS Kunden sind in der Lage, die Konfiguration eines Amazon Elastic Compute Cloud (Amazon), Amazon Elastic Container Service (Amazon EC2ECS) -Containers oder AWS Elastic Beanstalk -

Instances maßzuschneidern oder zu härten und diese Konfiguration auf einem unveränderlichen Amazon Machine Image (AMI) beizubehalten. AMI Unabhängig davon, ob sie mit Auto Scaling oder manuell gestartet wurden, AMI erhalten alle neuen virtuellen Server (Instances), die damit gestartet werden, die gehärtete Konfiguration.

## 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.

AWS In erleichtern die folgenden Verfahren den Schutz von Daten:

- Als AWS Kunde behalten Sie die volle Kontrolle über Ihre Daten.
- AWS erleichtert Ihnen die Verschlüsselung Ihrer Daten und die Verwaltung von Schlüsseln, einschließlich der regelmäßigen Schlüsselrotation, die problemlos von Ihnen automatisiert AWS oder von Ihnen verwaltet werden kann.
- Sie haben Zugriff auf detaillierte Protokolle mit wichtigen Angaben etwa zu Dateizugriffen und -änderungen.
- AWS hat Speichersysteme für außergewöhnliche Ausfallsicherheit konzipiert. Amazon S3 Standard, S3 Standard-IA, S3 One Zone-IA und Amazon Glacier bieten beispielsweise eine einjährige Objektanglebigkeit von 99,999999999 %. Dies entspricht einem jährlichen erwarteten Verlust von 0,000000001 % der Objekte.
- Die Versionsverwaltung, die in ein umfassenderes Verfahren zur Datenlebenszyklusverwaltung eingebunden sein kann, bietet Schutz vor versehentlichen Überschreibungen, Löschungen und ähnlichen Gefahren.
- AWS initiiert niemals die Übertragung von Daten zwischen Regionen. Die in einer Region platzierten Inhalte bleiben in dieser Region, sofern Sie eine Verschiebung nicht ausdrücklich mithilfe einer Funktion oder eines Services durchführen.

In den folgenden Fragen geht es um Überlegungen zur Sicherheit.

## SEC7: Wie klassifizieren Sie Ihre Daten?

Die Datenklassifizierung bietet eine Möglichkeit, Daten basierend auf Wichtigkeit und Sensibilität zu kategorisieren, um Ihnen dabei zu helfen, angemessene Schutz- und Aufbewahrungskontrollen zu bestimmen.

## SEC8: Wie schützen Sie Ihre Daten im Ruhezustand?

Schützen Sie Ihre Daten im Ruhezustand, indem Sie mehrere Kontrollen implementieren und so das Risiko eines unbefugten Zugriffs oder einer falschen Handhabung verringern.

## SEC9: Wie schützen Sie Ihre Daten bei der Übertragung?

Schützen Sie Ihre Daten während der Übertragung, indem Sie mehrere Kontrollen implementieren und so das Risiko eines unbefugten Zugriffs oder eines Datenverlusts verringern.

AWS bietet mehrere Möglichkeiten zur Verschlüsselung von Daten im Ruhezustand und bei der Übertragung. Unsere Services enthalten Funktionen, die die Verschlüsselung Ihrer Daten erleichtern. Wir haben beispielsweise serverseitige Verschlüsselung (SSE) für Amazon S3 implementiert, um Ihnen das Speichern Ihrer Daten in verschlüsselter Form zu erleichtern. Sie können auch dafür sorgen, dass der gesamte HTTPS Verschlüsselungs- und Entschlüsselungsprozess (allgemein als SSL Terminierung bezeichnet) von Elastic Load Balancing (ELB) abgewickelt wird.

## 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 ermöglichen AWS die folgenden Methoden eine effektive Reaktion auf Vorfälle:

- Eine detaillierte Protokollierung wichtiger Informationen etwa zu Dateizugriffen und -änderungen.
- Ereignisse können automatisch verarbeitet werden und es können Tools gestartet werden, die automatische Reaktionen mithilfe von ermöglichen AWS APIs.
- Sie können vorab mit AWS CloudFormation entsprechende Tools und einen „Clean Room“ bereitstellen. Sie erhalten dadurch eine sichere, isolierte Umgebung für forensische Untersuchungen.

In der folgenden Frage geht es um Überlegungen zur Sicherheit.

**SEC10: Wie können Sie Vorfälle antizipieren, darauf reagieren und sich nach ihnen erholen?**

Die Vorbereitung ist entscheidend für eine rechtzeitige und effektive Untersuchung, Reaktion auf und Wiederherstellung nach Sicherheitsvorfällen, um Unterbrechungen der Geschäftsabläufe zu minimieren.

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

## Anwendungssicherheit

Anwendungssicherheit (AppSec) beschreibt den Gesamtprozess, bei dem Sie die Sicherheitseigenschaften der von Ihnen entwickelten Workloads entwerfen, erstellen und testen. Sie sollten die Personen in Ihrer Organisation entsprechend geschult haben und die Sicherheitseigenschaften Ihrer Entwicklung und der Infrastruktur Ihrer Softwareveröffentlichung verstehen. Sie sollten auch Automatisierung zum Identifizieren von Sicherheitsproblemen einsetzen.

Wenn Sie Anwendungssicherheitstests als regelmäßigen Bestandteil Ihres Softwareentwicklungszyklus (SDLC) und der Prozesse nach der Veröffentlichung einführen, können Sie überprüfen, ob Sie über einen strukturierten Mechanismus verfügen, mit dem Sie Sicherheitsprobleme von Anwendungen erkennen, beheben und verhindern können, dass sie in Ihre Produktionsumgebung gelangen.

Ihre Methodologie zur Anwendungsentwicklung sollte Sicherheitskontrollen enthalten, während Sie Ihre Workloads entwerfen, entwickeln, bereitstellen und ausführen. Während Sie das machen, passen Sie den Prozess für kontinuierliche Fehlerrückmeldung und Minimierung von technischen Schulden an. Das Verwenden von Bedrohungsmodellierung in der Designphase hilft Ihnen

beispielsweise dabei, Designfehler früh aufzudecken, wodurch sie einfacher und günstiger behoben werden können – im Gegensatz dazu, wenn Sie warten und die Fehler später beseitigen.

Die Kosten und der Aufwand für die Behebung von Fehlern sind in der Regel geringer, je früher Sie in der SDLC die einfachste Weise, Probleme zu lösen, ist keine zu haben. Daher hilft Ihnen ein Bedrohungsmodell, sich bereits in der Designphase auf die richtigen Ergebnisse zu konzentrieren. Mit zunehmender AppSec Reife Ihres Programms können Sie die Anzahl der Tests erhöhen, die mithilfe von Automatisierung durchgeführt werden, die Genauigkeit des Feedbacks an die Entwickler verbessern und den Zeitaufwand für Sicherheitsüberprüfungen reduzieren. All diese Aktionen erhöhen die Qualität der Software, die Sie entwickeln, und beschleunigen das Ausliefern von Funktionen in die Produktion.

Bei diesen Implementierungsrichtlinien gibt es vier Schwerpunktbereiche: Organisation und Kultur, Sicherheit der Pipeline, Sicherheit in der Pipeline und Verwaltung von Abhängigkeiten. Jeder Bereich bietet eine Reihe von Prinzipien, die Sie implementieren können, und bietet einen end-to-end Überblick darüber, wie Sie Workloads entwerfen, entwickeln, erstellen, bereitstellen und betreiben.

In gibt es eine Reihe von Ansätzen AWS, die Sie für Ihr Anwendungssicherheitsprogramm verwenden können. Einige dieser Ansätze basieren auf Technologie, während sich andere auf die menschlichen und betrieblichen Aspekte Ihres Anwendungssicherheitsprogramms konzentrieren.

In der folgenden Frage geht es um Überlegungen zur Anwendungssicherheit.

SEC11: Wie integrieren und validieren Sie die Sicherheitseigenschaften von Anwendungen während des gesamten Entwurfs-, Entwicklungs- und Bereitstellungszyklus?

Das Schulen von Personen, das Testen mithilfe von Automatisierung, ein Verständnis der Abhängigkeiten und die Validierung der Sicherheitseigenschaften von Tools und Anwendungen helfen dabei, die Wahrscheinlichkeit eines Sicherheitsproblems bei Produktions-Workloads zu verringern.

## Ressourcen

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

### Dokumentation

- [AWS Cloud-Sicherheit](#)



- [AWS -Compliance](#)
- [AWS Blog zum Thema Sicherheit](#)
- [AWS -Modell des Sicherheitsreifegrads](#)

## Whitepaper

- [Säule der Sicherheit](#)
- [AWS Überblick über die Sicherheit](#)
- [AWS Risiko und Einhaltung von Vorschriften](#)

## Video

- [AWS Sicherheitslage der Union](#)
- [Übersicht über die gemeinsame Verantwortlichkeit](#)

## Zuverlässigkeit

Die Säule „Zuverlässigkeit“ umfasst die Fähigkeit einer Workload, die beabsichtigte Funktion erwartungsgemäß korrekt und konsistent auszuführen. Dies umfasst die Möglichkeit, die Workload während des gesamten Lebenszyklus zu betreiben und zu testen. Dieses paper enthält ausführliche Best-Practice-Anleitungen für die Implementierung zuverlässiger Workloads auf AWS.

Die Säule „Zuverlässigkeit“ gibt einen Überblick über konzeptionelle Grundsätze, bewährte Methoden und Fragen. Verbindliche Anleitungen zur Implementierung finden Sie im [Whitepaper „Säule der Zuverlässigkeit“](#).

### Themen

- [Designprinzipien](#)
- [Definition](#)
- [Bewährte Methoden](#)
- [Ressourcen](#)

## Designprinzipien

Es gibt fünf Gestaltungsprinzipien für die Zuverlässigkeit in der Cloud:

- **Automatische Wiederherstellung nach einem Ausfall:** Durch die Überwachung eines Workloads auf wichtige Leistungsindikatoren (KPIs) können Sie die Automatisierung starten, wenn ein Schwellenwert überschritten wird. Diese KPIs sollten als Maßstab für den Geschäftswert und nicht für die technischen Aspekte des Betriebs des Dienstes dienen. Dies bietet eine automatische Benachrichtigung bei und Verfolgung von Fehlern sowie die Einleitung einer automatisierten Wiederherstellung, die eine Fehlerumgehung bietet oder den Fehler behebt. Bei einer ausgefeilteren Automatisierung ist es möglich, Fehler vor ihrem eigentlichen Auftreten zu antizipieren und zu beheben.
- **Testen von Wiederherstellungsverfahren:** In einer On-Premises-Umgebung werden häufig Tests durchgeführt, um nachzuweisen, dass die Workload in einem bestimmten Szenario funktioniert. Mit den Tests werden in der Regel keine Wiederherstellungsstrategien validiert. In der Cloud können Sie testen, in welchen Situationen die Workload Fehler produziert, und Sie können die Wiederherstellungsverfahren validieren. Mit der Automatisierung können Sie verschiedene Fehler simulieren oder Szenarien reproduzieren, die zuvor zu Fehlern geführt haben. Dieser Ansatz stellt Fehlerpfade bereit, die Sie testen und beheben können, bevor ein echtes Fehlerszenario auftritt, und reduziert so das Risiko.
- **Horizontale Skalierung zur Erhöhung der aggregierten Workload-Verfügbarkeit:** Ersetzen Sie eine große Ressource durch mehrere kleine Ressourcen, um die Auswirkung eines einzigen Fehlers auf die Gesamt-Workload zu reduzieren. Verteilen Sie Anfragen auf mehrere kleinere Ressourcen, um sicherzustellen, dass sie keine gemeinsame Fehlerquelle haben.
- **Genaue Analyse der verfügbaren Kapazität:** Eine häufige Fehlerursache bei On-Premises-Workloads ist die Ressourcensättigung. Ein solches Szenario liegt vor, wenn die Anforderungen an die Workload die Kapazität dieser Workload überschreiten (dies ist häufig das Ziel von Denial-of-Service-Angriffen). In der Cloud können Sie die Nachfrage und die Workload-Auslastung überwachen und das Hinzufügen oder Entfernen von Ressourcen automatisieren, um den Bedarf ohne Über- oder Unterbereitstellung stets effizient zu erfüllen. Es gibt weiterhin Grenzen, aber einige Kontingente können gesteuert und andere verwaltet werden (siehe Verwaltung von Service Quotas und Einschränkungen).
- **Änderungsmanagement per Automatisierung:** Änderungen an Ihrer Infrastruktur sollten über eine Automatisierung vorgenommen werden. Zu den Änderungen, die verwaltet werden müssen, gehören Änderungen an der Automatisierung, die anschließend nachverfolgt und überprüft werden können.

## Definition

Die bewährten Methoden für Zuverlässigkeit in der Cloud lassen sich in vier Bereiche einteilen:

- Grundlagen
- Workload-Architektur
- Änderungsmanagement
- Fehlerverwaltung

Um Zuverlässigkeit zu erreichen, müssen Sie mit den Grundlagen beginnen – einer Umgebung, in der Service Quotas und Netzwerktopologie der Workload entsprechen. Die Workload-Architektur des verteilten Systems muss so ausgelegt sein, dass Ausfälle verhindert und minimiert werden. Die Workload muss Änderungen in Bezug auf den Bedarf oder die Anforderungen verarbeiten und so konzipiert sein, dass sie Fehler erkennt und sie automatisch selbst behebt.

## Bewährte Methoden

Themen

- [Grundlagen](#)
- [Workload-Architektur](#)
- [Änderungsmanagement](#)
- [Fehlerverwaltung](#)

## Grundlagen

Grundlegende Anforderungen sind diejenigen, deren Umfang über eine einzelne Workload oder ein einzelnes Projekt hinausgeht. 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.

Die meisten dieser grundlegenden Anforderungen sind bereits enthalten oder können bei Bedarf erfüllt werden. AWS Die Cloud ist so konzipiert, dass sie nahezu unbegrenzt ist. Es liegt also in der Verantwortung, die Anforderungen AWS an ausreichende Netzwerk- und Rechenkapazität zu erfüllen, sodass Sie die Ressourcengröße und -zuweisung nach Bedarf ändern können.

In den folgenden Fragen geht es um Überlegungen zur Zuverlässigkeit. (Eine Liste der Fragen und bewährten Methoden zur Zuverlässigkeit finden Sie im [Anhang](#).)

## REL1: Wie verwalten Sie Servicequotas und Einschränkungen?

Für cloudbasierte Workload-Architekturen gibt es Service Quotas (auch als „Servicebeschränkungen“ bezeichnet). Diese Kontingente dienen dazu, zu verhindern, dass versehentlich mehr Ressourcen bereitgestellt werden, als Sie benötigen, und um die Anforderungsraten bei API Vorgängen zu begrenzen, um Dienste vor Missbrauch zu schützen. Es gibt auch Einschränkungen für Ressourcen, z. B. im Bezug auf die Rate, mit der Bits über ein Glasfaserkabel übertragen werden können, oder die Menge an Speicherplatz auf einer physischen Festplatte.

## REL2: Wie planen Sie Ihre Netzwerktopologie?

Workloads existieren oft in mehreren Umgebungen. Dazu gehören mehrere Cloud-Umgebungen (sowohl öffentlich zugänglich als auch privat) und möglicherweise Ihre bestehende Rechenzentrumsinfrastruktur. Die Pläne müssen Netzwerkaspekte wie systeminterne und systemübergreifende Konnektivität, Verwaltung öffentlicher IP-Adressen, Verwaltung privater IP-Adressen und Auflösung von Domainnamen beinhalten.

## Workload-Architektur

Ausgangspunkt für eine zuverlässige Workload sind vorab getroffene Designentscheidungen für Software und Infrastruktur. Ihre Auswahl in puncto Architektur wirkt sich in allen Well-Architected-Säulen auf das Verhalten der Workload aus. Zur Gewährleistung von Zuverlässigkeit sind bestimmte Muster zu befolgen.

Damit AWS haben Workload-Entwickler die Wahl zwischen Sprachen und Technologien, die sie verwenden können. AWS SDKs reduzieren Sie die Komplexität der Codierung, indem Sie sprachspezifische Dienste APIs bereitstellen. AWS Diese SDKs und die Auswahl der Sprachen ermöglichen es Entwicklern, die hier aufgeführten Best Practices für Zuverlässigkeit zu implementieren. Entwickler können sich auch in der [Amazon Builders' Library](#) darüber informieren, wie Software von Amazon erstellt und betrieben wird.

In den folgenden Fragen geht es um Überlegungen zur Zuverlässigkeit.

### REL3: Wie entwerfen Sie Ihre Workload-Servicearchitektur?

Erstellen Sie hoch skalierbare und zuverlässige Workloads mithilfe einer serviceorientierten Architektur (SOA) oder einer Microservices-Architektur. Serviceorientierte Architektur (SOA) ist die Praxis, Softwarekomponenten über Serviceschnittstellen wiederverwendbar zu machen. Die Microservices-Architektur geht noch weiter, um Komponenten kleiner und einfacher zu machen.

### REL4: Wie gestaltet man Interaktionen in einem verteilten System, um Ausfälle zu vermeiden?

Verteilte Systeme sind auf Kommunikationsnetzwerke angewiesen, um Komponenten wie Server oder Services miteinander zu verbinden. Ihre Workload muss trotz Datenverlust oder Latenz in diesen Netzwerken zuverlässig funktionieren. Die Komponenten des verteilten Systems müssen so funktionieren, dass sie sich nicht negativ auf andere Komponenten oder die Workload auswirken. Diese bewährten Methoden verhindern Ausfälle und verbessern die durchschnittliche Betriebsdauer zwischen Ausfällen (MTBF).

### REL5: Wie gestaltet man Interaktionen in einem verteilten System, um Ausfälle zu minimieren oder ihnen standzuhalten?

Verteilte Systeme nutzen Kommunikationsnetzwerke, um Komponenten (wie Server oder Services) miteinander zu verbinden. Ihre Workload muss trotz Datenverlust oder höherer Latenz in diesen Netzwerken zuverlässig ausgeführt werden. Die Komponenten des verteilten Systems müssen so funktionieren, dass sie sich nicht negativ auf andere Komponenten oder die Workload auswirken. Diese bewährten Methoden sorgen dafür, dass Workloads Belastungen oder Fehlern standhalten, sich schneller davon erholen und die Auswirkungen solcher Beeinträchtigungen abgeschwächt werden. Das Ergebnis ist eine kürzere durchschnittliche Zeit bis zur Wiederherstellung (MTTR).

## Änderungsmanagement

Änderungen an Ihrer Workload oder der Umgebung müssen vorausgesehen und berücksichtigt werden, um einen zuverlässigen Betrieb der Workload zu erreichen. Zu diesen Änderungen gehören z. B. Bedarfsspitzen sowie interne Änderungen wie Featurebereitstellungen und Sicherheitspatches, die sich auf Ihre Workloads auswirken.

Mit AWS dieser Option können Sie das Verhalten eines Workloads überwachen und die Reaktion darauf automatisieren KPIs. Beispielsweise kann die Workload bei einer zunehmenden Zahl von Benutzern zusätzliche Server hinzufügen. Sie können kontrollieren und steuern, welche Benutzer Änderungen an der Workload vornehmen dürfen, und die Historie dieser Änderungen überprüfen.

In den folgenden Fragen geht es um Überlegungen zur Zuverlässigkeit.

#### REL6: Wie überwachen Sie Workload-Ressourcen?

Protokolle und Metriken sind leistungsstarke Tools, mit denen Sie sich einen Überblick über den Zustand Ihrer Workload verschaffen können. Sie können Ihre Workload so konfigurieren, dass Protokolle und Metriken überwacht und Benachrichtigungen gesendet werden, wenn Schwellenwerte überschritten werden oder wichtige Ereignisse auftreten. Dank der Überwachung kann die Workload erkennen, wenn Schwellenwerte für eine niedrige Leistung unterschritten werden oder Ausfälle auftreten, sodass als Reaktion drauf eine automatische Wiederherstellung erfolgen kann.

#### REL7: Wie gestalten Sie Ihre Arbeitslast so, dass sie sich an Veränderungen der Nachfrage anpasst?

Eine skalierbare Workload bietet Elastizität, sodass Ressourcen automatisch hinzugefügt oder entfernt werden können, damit sie dem aktuellen Bedarf zu einem bestimmten Zeitpunkt genau entsprechen.

#### REL8: Wie implementieren Sie Veränderungen?

Kontrollierte Änderungen sind erforderlich, um neue Funktionen bereitzustellen und um sicherzustellen, dass die Workloads und die Betriebsumgebung bekannte Software ausführen und auf vorhersagbare Weise durch Patches aktualisiert oder ersetzt werden können. Wenn solche Änderungen nicht kontrolliert sind, ist es schwierig, die Auswirkungen der Änderungen vorherzusagen oder Probleme zu lösen, die sich aus ihnen ergeben.

Wenn Sie eine Workload so gestalten, dass Ressourcen als Reaktion auf Bedarfsänderungen automatisch hinzugefügt und entfernt werden, erhöht das nicht nur die Zuverlässigkeit. Vielmehr sorgt diese Vorgehensweise auch dafür, dass geschäftlicher Erfolg nicht zu einer Belastung

wird. Wenn die Überwachung eingerichtet ist, wird Ihr Team automatisch benachrichtigt, wenn von den erwarteten Normen KPIs abgewichen wird. 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 die Regeln durchsetzen, die für die benötigte Zuverlässigkeit sorgen.

## Fehlerverwaltung

In Systemen mit großer Komplexität ist es wahrscheinlich, dass Fehler auftreten. Zur Gewährleistung von Zuverlässigkeit muss Ihre Workload auftretende Fehler erkennen und Maßnahmen ergreifen, um Auswirkungen auf die Verfügbarkeit zu vermeiden. Workloads müssen Ausfälle verkraften sowie Probleme automatisch beheben können.

Mit können Sie die Vorteile der Automatisierung nutzen AWS, um auf Überwachungsdaten zu reagieren. Wenn eine bestimmte Kennzahl beispielsweise einen Schwellenwert überschreitet, können Sie eine automatische Maßnahme zur Behebung dieses Problems starten. 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 aufstellen können, können Sie automatisiertes Testen verwenden, um vollständige Wiederherstellungsprozesse zu überprüfen.

In den folgenden Fragen geht es um Überlegungen zur Zuverlässigkeit.

### REL9: Wie sichern Sie Daten?

Sichern Sie Daten, Anwendungen und Konfigurationen, um Ihre Anforderungen in Bezug auf Wiederherstellungszeitziele (RTO) und Wiederherstellungspunktziele (RPO) zu erfüllen.

### REL10: Wie verwenden Sie die Fehlerisolierung, um Ihre Workloads zu schützen?

Fehlerisolierte Grenzen beschränken die Auswirkungen eines Fehlers innerhalb einer Workload auf eine begrenzte Anzahl von Komponenten. Komponenten außerhalb der Grenze sind von dem Ausfall nicht betroffen. Durch die Verwendung mehrerer fehlerisolierter Grenzen können Sie die Auswirkungen auf Ihre Workload einschränken.

### REL11: Wie gestalten Sie Ihren Workload so, dass er Komponentenausfällen standhält?

Workloads, für die eine hohe Verfügbarkeit und eine geringe mittlere Wiederherstellungszeit (MTTR) erforderlich sind, müssen auf Ausfallsicherheit ausgelegt werden.

### REL12: Wie testet man die Zuverlässigkeit?

Nachdem Sie Ihre Workload so konzipiert haben, dass sie den Belastungen der Produktion standhält, sind Tests die einzige Möglichkeit, sie auf die erwartete Funktionalität und Ausfallsicherheit hin zu testen.

### REL13: Wie planen Sie Disaster Recovery (DR)?

Sicherungen und redundante Workload-Komponenten sind der Ausgangspunkt Ihrer Strategie für die Notfallwiederherstellung. [RTO und RPO sind Ihre Ziele](#) für die Wiederherstellung Ihrer Arbeitslast. Legen Sie diese entsprechend den geschäftlichen Anforderungen fest. Implementieren Sie eine Strategie, um diese Ziele zu erreichen. Berücksichtigen Sie dabei Standorte und Funktionen von Workload-Ressourcen und -Daten. Die Wahrscheinlichkeit von Unterbrechungen und die Kosten von Wiederherstellungen sind ebenfalls wichtige Faktoren bei der Ermittlung des Unternehmenswerts, den Notfallwiederherstellungen von Workloads bieten.

Sichern Sie Ihre Daten regelmäßig und stellen Sie anhand von Tests der Sicherungsdateien sicher, dass Sie nach logischen und physischen Fehlern eine Wiederherstellung durchführen können. Ein Schlüssel zur Verwaltung von Fehlern ist das regelmäßige und automatisierte Testen von Workloads, um Ausfälle hervorzurufen, und das anschließende Beobachten des Wiederherstellungsverhaltens. Führen Sie diese Tests regelmäßig durch, auch nach größeren Workload-Änderungen. Verfolgen Sie KPIs aktiv die Ziele für die Wiederherstellungszeit (RTO) und die Zielsetzung für den Wiederherstellungspunkt (RPO), um die Belastbarkeit eines Workloads zu beurteilen (insbesondere bei Fehlertestszenarien). KPIs Die Nachverfolgung hilft Ihnen dabei, einzelne Fehlerquellen zu identifizieren und zu minimieren. Hierbei geht es darum, Ihre Prozesse zur Wiederherstellung von Workloads gründlich zu testen, damit Sie darauf vertrauen können, dass Sie alle Daten wiederherstellen und Ihren Service Ihren Kunden unterbrechungsfrei anbieten können – selbst bei länger anhaltenden Problemen. Mit Ihren Wiederherstellungsprozessen sollten Sie sich genauso vertraut machen wie mit Ihren normalen Produktionsprozessen.



## Ressourcen

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

### Dokumentation

- [AWS -Dokumentation:](#)
- [AWS Weltweite Infrastruktur](#)
- [AWS Auto Scaling: Funktionsweise von Skalierungsplänen](#)
- [Was ist AWS Backup?](#)

### Whitepaper

- [Säule der Zuverlässigkeit: AWS Well-Architected](#)
- [Implementierung von Microservices auf AWS](#)

## Leistungseffizienz

Die Säule der Leistungseffizienz betrifft die Fähigkeit zur effizienten Nutzung von Cloud-Ressourcen, um die Leistungsanforderungen zu erfüllen, sowie die Möglichkeit zur Aufrechterhaltung dieser Effizienz bei Nachfrageänderungen und einer Weiterentwicklung der Technologien.

Die Säule „Leistungsexzellenz“ gibt einen Überblick über konzeptionelle Grundsätze, bewährte Methoden und Fragen. Verbindliche Anleitungen zur Implementierung finden Sie im [Whitepaper „Säule der Leistungseffizienz“](#).

### Themen

- [Designprinzipien](#)
- [Definition](#)
- [Bewährte Methoden](#)
- [Ressourcen](#)

## Designprinzipien

Es gibt fünf Gestaltungsprinzipien für die Leistungseffizienz in der Cloud:

- **Demokratisieren fortschrittlicher Technologien:** Vereinfachen Sie die Implementierung fortschrittlicher Technologien für Ihr Team, indem Sie komplexe Aufgaben an Ihren Cloud-Anbieter delegieren. Statt Ihr IT-Team aufzufordern, sich näher über das Hosten und Ausführen einer neuen Technologie zu informieren, sollten Sie die Technologie als Service nutzen. Zum Beispiel sind keine SQL Datenbanken, Medientranscodierung und maschinelles Lernen alles Technologien, für die spezielles Fachwissen erforderlich ist. In der Cloud kann Ihr Team diese Technologien als Service nutzen und sich auf die Produktentwicklung konzentrieren, ohne sich um die Bereitstellung und Verwaltung von Ressourcen kümmern zu müssen.
- **Werden Sie innerhalb weniger Minuten global:** Durch die Bereitstellung Ihrer Workloads in mehreren AWS Regionen auf der ganzen Welt können Sie Ihren Kunden bei minimalen Kosten eine geringere Latenz und ein besseres Erlebnis bieten.
- **Nutzung von Serverless-Architekturen:** Aufgrund der in der Cloud verwendeten Serverless-Architekturen brauchen Sie für herkömmliche Datenverarbeitungsaktivitäten keine physischen Server mehr auszuführen und zu verwalten. Serverless-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 physischer Server, sondern auch die Transaktionskosten sinken, da verwaltete Services in der Cloud-Umgebung ausgeführt werden.
- **Vermehrtes Experimentieren:** Mit virtuellen und automatisierbaren Ressourcen können Sie schnell unterschiedliche Konfigurationen, Instance- oder Speichertypen miteinander vergleichen.
- **Berücksichtigen des technischen Verständnisses:** Befassen Sie sich mit der Verwendungsweise von Cloud-Services und nutzen Sie stets den Technologieansatz, der für Ihre Workload-Ziele geeignet ist. Berücksichtigen Sie bei der Auswahl des passenden Datenbank- oder Speicherkonzepts beispielsweise die Datenzugriffsmuster.

## Definition

Es gibt fünf bewährte Methoden für die Leistungseffizienz in der Cloud:

- Auswahl der Architektur
- Computer und Hardware
- Datenverwaltung
- Netzwerk und Bereitstellung von Inhalten
- Prozess und Kultur

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.

Wenn Sie Ihre Optionen regelmäßig überprüfen, wird bestätigt, dass Sie die Vorteile der sich ständig weiterentwickelnden AWS Cloud nutzen. Durch Überwachung erkennen Sie Abweichungen von der erwarteten Leistung. Zur Leistungssteigerung der Architektur können Sie auch Kompromisse eingehen, beispielsweise durch Komprimierung oder Caching, oder indem Sie hinsichtlich der Konsistenz mehr Toleranz einräumen.

## Bewährte Methoden

### Themen

- [Auswahl der Architektur](#)
- [Computer und Hardware](#)
- [Datenverwaltung](#)
- [Netzwerk und Bereitstellung von Inhalten](#)
- [Prozess und Kultur](#)

### Auswahl der Architektur

Die optimale Lösung für eine bestimmte Workload variiert und Lösungen sind häufig eine Kombination mehrerer Ansätze. Well-Architected-Workloads nutzen mehrere Lösungen und ermöglichen verschiedene Funktionen zur Verbesserung der Leistung.

AWS Ressourcen sind in vielen Typen und Konfigurationen verfügbar, was es einfacher macht, einen Ansatz zu finden, der Ihren Bedürfnissen am besten entspricht. Sie können zudem Optionen nutzen, die sich in Ihrer On-Premises-Infrastruktur nicht ohne Weiteres umsetzen ließen. Ein verwalteter Service wie Amazon DynamoDB bietet beispielsweise eine vollständig verwaltete SQL Nein-Datenbank mit einer Latenz im einstelligen Millisekundenbereich in jeder Größenordnung.

In der folgenden Frage geht es um Überlegungen zur Leistungseffizienz. (Eine Liste der Fragen und bewährten Methoden zur Leistungseffizienz finden Sie im [Anhang](#)).

## PERF1: Wie wählen Sie geeignete Cloud-Ressourcen und Architekturmuster für Ihren Workload aus?

Oft sind mehrere Ansätze erforderlich, um eine effektivere Leistung für eine Workload zu erzielen. Well-Architected-Systeme nutzen mehrere Lösungen und Funktionen zur Verbesserung der Leistung.

### Computer und Hardware

Die optimale Datenverarbeitungsoption für eine bestimmte Workload kann sich je nach Anwendungsdesign, Nutzungsmustern und Konfigurationseinstellungen unterscheiden. Architekturen können verschiedene Datenverarbeitungsoptionen für verschiedene Komponenten verwenden und verschiedene Funktionen zur Verbesserung der Leistung bieten. Die Wahl der falschen Datenverarbeitungslösung für eine Architektur kann die Leistungseffizienz schmälern.

In AWS, Compute ist in drei Formen verfügbar: Instanzen, Container und Funktionen:

- Instanzen sind virtualisierte Server, die es Ihnen ermöglichen, ihre Funktionen mit einer Taste oder einem API Aufruf zu ändern. Da Ressourcenentscheidungen in der Cloud flexibel sind, können Sie mit verschiedenen Servertypen experimentieren. Bei AWS diesen virtuellen Serverinstanzen gibt es verschiedene Familien und Größen und sie bieten eine Vielzahl von Funktionen, darunter Solid-State-Laufwerke (SSDs) und Grafikprozessoren (GPU). GPUs
- Container sind eine Methode der Betriebssystemvirtualisierung, mit der Sie eine Anwendung und ihre Abhängigkeiten in ressourcenisolierten Prozessen ausführen können. AWS Fargate ist serverloses Computing für Container oder Amazon EC2 kann verwendet werden, wenn Sie Kontrolle über die Installation, Konfiguration und Verwaltung Ihrer Rechenumgebung benötigen. Sie können auch aus mehreren Plattformen für die Container-Orchestrierung wählen: Amazon Elastic Container Service (ECS) oder Amazon Elastic Kubernetes Service (EKS).
- Funktionen abstrahieren die Ausführungsumgebung vom anzuwendenden Code. AWS Lambda Ermöglicht es Ihnen beispielsweise, Code auszuführen, ohne eine Instance auszuführen.

In der folgenden Frage geht es um Überlegungen zur Leistungseffizienz.

## PERF2: Wie wählen und verwenden Sie Rechenressourcen in Ihrem Workload?

Welche Datenverarbeitungslösung für eine Workload effizienter ist, ist vom Anwendungsdesign sowie von Nutzungsmustern und Konfigurationseinstellungen abhängig. Architekturen können unterschiedliche Datenverarbeitungslösungen für verschiedene Komponenten verwenden und unterschiedliche Funktionen zur Leistungsverbesserung bieten. Die Wahl der falschen Datenverarbeitungslösung für eine Architektur kann die Leistungseffizienz schmälern.

## Datenverwaltung

Die optimale Datenverwaltungslösung für ein bestimmtes System hängt von der Art des Datentyps (Block, Datei oder Objekt), den Zugriffsmustern (zufällig oder sequentiell), dem erforderlichen Durchsatz, der Häufigkeit des Zugriffs (online, offline, archiviert), der Aktualisierungshäufigkeit (WORMdynamisch) sowie von Verfügbarkeits- und Haltbarkeitsbeschränkungen ab. Well-Architected-Workloads verwenden zweckgebundene Datenspeicher, die verschiedene Features zur Verbesserung der Leistung ermöglichen.

AWS In ist Speicher in drei Formen verfügbar: Objekt, Block und Datei:

- Objektspeicher bietet eine skalierbare, robuste Plattform, damit Daten überall im Internet zugänglich sind. Das gilt für benutzergenerierte Inhalte, aktive Archive, Serverless-Datenverarbeitung, Big Data-Speicher oder die Sicherung und Wiederherstellung. Amazon Simple Storage Service (Amazon S3) ist ein Objektspeicherservice, der branchenführende Skalierbarkeit, Datenverfügbarkeit, Sicherheit und Leistung bietet. Amazon S3 ist auf eine Verfügbarkeit von 99,999999999 % ausgelegt und speichert Daten für Millionen von Anwendungen für Unternehmen weltweit.
- Blockspeicher bietet hochverfügbaren, konsistenten Blockspeicher mit niedriger Latenz für jeden virtuellen Host und entspricht direkt angeschlossenem Speicher (DAS) oder einem Storage Area Network (SAN). Amazon Elastic Block Store (AmazonEBS) wurde für Workloads entwickelt, die persistenten Speicher benötigen, auf den EC2 Instances zugreifen können, sodass Sie Anwendungen mit der richtigen Speicherkapazität, Leistung und den richtigen Kosten optimieren können.
- Dateispeicher bietet auf mehreren Systemen Zugriff auf ein gemeinsam genutztes Dateisystem. Dateispeicherlösungen wie Amazon Elastic File System (AmazonEFS) eignen sich ideal für Anwendungsfälle wie große Inhaltsrepositorys, Entwicklungsumgebungen, Medienspeicher oder Benutzerverzeichnisse. Amazon FSx macht es effizient und kostengünstig, beliebte Dateisysteme

zu starten und auszuführen, sodass Sie die umfangreichen Funktionen und die schnelle Leistung weit verbreiteter Open-Source-Dateisysteme und kommerziell lizenzierter Dateisysteme nutzen können.

In der folgenden Frage geht es um Überlegungen zur Leistungseffizienz.

**PERF3: Wie speichern, verwalten und greifen Sie auf Daten in Ihrem Workload zu?**

Die effizientere Speicherlösung für ein System hängt von der Art des Zugriffsvorgangs (Block, Datei oder Objekt), den Zugriffsmustern (zufällig oder sequentiell), dem erforderlichen Durchsatz, der Zugriffshäufigkeit (online, offline, Archivierung), der Aktualisierungshäufigkeit (WORMdynamisch) sowie von Verfügbarkeits- und Haltbarkeitsbeschränkungen ab. Gut geplante Systeme nutzen mehrere Speicherlösungen und bieten unterschiedliche Möglichkeiten zur Leistungsoptimierung und effizienten Ressourcennutzung.

## Netzwerk und Bereitstellung von Inhalten

Welche Netzwerklösung für eine Workload optimal ist, richtet sich nach der Latenz, dem erforderlichen Durchsatz, dem Jitter und der Bandbreite. Die Standortoptionen sind von den physischen Einschränkungen abhängig, z. B. von Benutzer- oder On-Premises-Ressourcen. Diese Einschränkungen können durch Edge-Standorte oder die Ressourcenplatzierung wettgemacht werden.

On AWS ist das Netzwerk virtualisiert und in einer Reihe verschiedener Typen und Konfigurationen verfügbar. Dies macht es einfacher, Ihren Netzwerkanforderungen gerecht zu werden. AWS bietet Produktfunktionen (z. B. Enhanced Networking, Amazon EC2 Networking Optimized Instances, Amazon S3 Transfer Acceleration und Dynamic Amazon CloudFront) zur Optimierung des Netzwerkverkehrs. AWS bietet auch Netzwerkfunktionen (z. B. Amazon Route 53-Latenz-Routing, VPC Amazon-Endpunkte und AWS Global Accelerator) AWS Direct Connect, um Netzwerkdistanz oder Jitter zu reduzieren.

In der folgenden Frage geht es um Überlegungen zur Leistungseffizienz.

**PERF4: Wie wählen und konfigurieren Sie Netzwerkressourcen in Ihrem Workload?**

In dieser Frage werden Anleitungen und bewährte Methoden für die Entwicklung, Konfiguration und den Betrieb effizienter Netzwerk und Inhaltsbereitstellungslösungen in der Cloud bereitgestellt.

## Prozess und Kultur

Bei der Architektur von Workloads gibt es Prinzipien und Methoden, die Sie übernehmen können, um effiziente und leistungsstarke Cloud-Workloads besser zu betreiben. Um eine Kultur zu schaffen, die die Leistungseffizienz von Cloud-Workloads fördert, sollten Sie diese Schlüsselprinzipien und -methoden berücksichtigen.

Beachten Sie beim Aufbau dieser Kultur die folgenden Schlüsselprinzipien:

- **Infrastruktur als Code:** Definieren Sie Ihre Infrastruktur als Code mithilfe von Ansätzen wie AWS CloudFormation Vorlagen. Mit Vorlagen können Sie Ihre Infrastruktur zusammen mit Ihrem Anwendungscode und Ihren Konfigurationen per Quellcodeüberwachung verwalten. Dies ermöglicht es Ihnen, dieselben Methoden wie bei der Softwareentwicklung auch auf Ihre Infrastruktur anzuwenden, um von einer schnellen Iteration zu profitieren.
- **Bereitstellungspipeline:** Nutzen Sie zur Bereitstellung der Infrastruktur eine CI/CD-Pipeline (Continuous Integration/Continuous Deployment) wie etwa ein Quellcode-Repository, Build-Systeme sowie automatisierte Bereitstellungs- und Testverfahren. Dies lässt eine reproduzierbare, konsistente und kostengünstige Iteration zu.
- **Klar definierte Metriken:** Richten Sie Metriken ein und überwachen Sie sie, um wichtige Leistungsindikatoren zu erfassen (KPIs). Wir empfehlen die Verwendung technischer und geschäftlicher Metriken. Bei Websites oder mobilen Apps sind Erfassung time-to-first-byte oder Rendern die wichtigsten Kennzahlen. Zu den weiteren allgemein anwendbaren Metriken zählen die Thread-Anzahl, die Garbage Collection-Rate sowie Wartezustände. Anhand von geschäftlichen Metriken wie den aggregierten kumulativen Kosten pro Anforderung können Sie Möglichkeiten zur Kostensenkung ermitteln. Erwägen Sie sorgfältig, wie Metriken interpretiert werden sollen. Sie können beispielsweise anstelle von Durchschnittswerten Maximalwerte oder das 99. Perzentil wählen.
- **Automatische Leistungstests:** Sorgen Sie im Rahmen der Bereitstellung dafür, dass nach dem erfolgreichen Absolvieren der schnelleren Ausführungstests automatisch Leistungstests initiiert werden. Durch die Automatisierung sollte eine neue Umgebung mit entsprechenden Anfangsbedingungen, z. B. Testdaten, entstehen, in der anschließend einige Benchmark- und Lasttests ausgeführt werden. Die Ergebnisse dieser Tests sollten mit dem Build in Verbindung gebracht werden, um Leistungsänderungen verfolgen zu können. Für langwierige Tests können Sie diesen Teil der Pipeline gegenüber dem restlichen Build asynchron ausführen. Alternativ können Sie über Nacht Leistungstests mit Amazon EC2 Spot-Instances durchführen.
- **Lastgenerierung:** Erstellen Sie eine Reihe von Testskripts zum Replizieren synthetischer oder vorab aufgezeichneter Benutzerreisen. Diese Skripts sollten idempotent und nicht gekoppelt

sein. Um gültige Ergebnisse zu erzielen, sind möglicherweise zusätzliche vorbereitende Skripts erforderlich. Die Testskripts sollten das Nutzungsverhalten in der Produktion möglichst authentisch replizieren. Sie können Software oder software-as-a-service (SaaS-) Lösungen verwenden, um die Last zu generieren. Erwägen Sie die Verwendung von [AWS Marketplace](#)-Lösungen und [Spot Instances](#). Dies können kostengünstige Ansätze zum Generieren der Last sein.

- **Leistungstransparenz:** Wichtige Metriken sollten für das ganze Team sichtbar sein. Dies gilt insbesondere für die Metriken der einzelnen Build-Versionen. Damit lassen sich wichtige positive oder negative Trends erkennen. Wichtig sind auch Metriken zur Anzahl der Fehler oder Ausnahmen, um sicherzustellen, dass das System funktioniert.
- **Visualisierung:** Nutzen Sie Visualisierungstechniken, mit denen Leistungsprobleme, Hotspots, Wartezustände oder niedrige Auslastungen klar aufgezeigt werden. Zeigen Sie Leistungsmetriken in Architekturdiagrammen an. Aufrufgrafiken oder Code können die Problemerkennung beschleunigen.
- **Regelmäßiger Prüfungsprozess:** Wenn Architekturen eine schlechte Leistung aufweisen, liegt dies normalerweise daran, dass ein Prozess zur Überprüfung der Leistung fehlt oder fehlerhaft ist. Falls Sie derartige Probleme mit Ihrer Architektur haben, können Sie jederzeit ein Leistungsprüfverfahren implementieren und somit iterative Verbesserungen fördern.
- **Fortlaufende Optimierung:** Schaffen Sie eine Kultur fortlaufender Optimierung der Leistungseffizienz Ihrer Cloud-Workload.

In der folgenden Frage geht es um Überlegungen zur Leistungseffizienz.

PERF5: Welchen Prozess verwenden Sie, um die Leistungseffizienz Ihres Workloads zu erhöhen?

Bei der Architektur von Workloads gibt es Prinzipien und Methoden, die Sie übernehmen können, um effiziente und leistungsstarke Cloud-Workloads besser zu betreiben. Um eine Kultur zu schaffen, die die Leistungseffizienz von Cloud-Workloads fördert, sollten Sie diese Schlüsselprinzipien und -methoden berücksichtigen.

## Ressourcen

Weitere Informationen zu bewährten Methoden für die Leistungseffizienz finden Sie in den folgenden Ressourcen.



## Dokumentation

- [Leistungsoptimierung mit Amazon S3](#)
- [Leistung von Amazon EBS Volume](#)

## Whitepaper

- [Säule der Leistungseffizienz](#)

## Video

- [AWS re:Invent 2019: EC2 Amazon-Stiftungen \(-R2\) CMP211](#)
- [AWS re:Invent 2019: Sitzung für Führungskräfte: Der Zustand der Speicherbranche \(01-L\) STG2](#)
- [AWS re:Invent 2019: Sitzung für Führungskräfte: speziell entwickelte Datenbanken \(09-L AWS \) DAT2](#)
- [AWS re:Invent 2019: Konnektivität zu und hybride Netzwerkarchitekturen \(-R1\) AWSAWS NET317](#)
- [AWS re:Invent 2019: Unterstützung für Amazon der nächsten Generation EC2: Tiefer Einblick in das Nitro-System \(03-R2\) CMP3](#)
- [AWS re:Invent 2019: Skalierung bis zu Ihren ersten 10 Millionen Benutzern \(-R\) ARC211](#)

## Kostenoptimierung

Die Säule „Kostenoptimierung“ umfasst die Fähigkeit, Systeme so auszuführen, dass sie geschäftlichen Wert bei geringstmöglichen Kosten liefern.

Die Säule „Kostenoptimierung“ bietet einen Überblick über Designprinzipien, bewährte Methoden und Fragen. Verbindliche Anleitungen zur Implementierung finden Sie im [Whitepaper zur Säule „Kostenoptimierung“](#).

### Themen

- [Designprinzipien](#)
- [Definition](#)
- [Bewährte Methoden](#)
- [Ressourcen](#)

## Designprinzipien

Es gibt fünf Designprinzipien für die Kostenoptimierung in der Cloud:

- **Cloud Financial Management implementieren:** Um finanziellen Erfolg zu haben und die Wertschöpfung in der Cloud zu beschleunigen, müssen Sie in Cloud-Finanzmanagement und Kostenoptimierung investieren. Ihre Organisation muss Zeit und Ressourcen aufwenden, um Know-how in diesem neuen Bereich des Technologie- und Nutzungsmanagements aufzubauen. Wie bei Ihren Funktionen zur Sicherheit oder der operativen Exzellenz müssen Sie Fähigkeiten durch Wissen, Programme, Ressourcen und Prozesse entwickeln, damit Sie zu einer kosteneffizienten Organisation werden können.
- **Verbrauchsmodell einführen:** Zahlen Sie nur für die benötigten Datenverarbeitungsressourcen, 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 der Workload und die mit der Bereitstellung verknüpften Kosten. Verwenden Sie diese Kennzahlen, um die Gewinne zu ermitteln, die Sie durch die Erhöhung der Leistung und die Reduzierung der Kosten erzielen.
- **Hören Sie auf, Geld für undifferenzierte Schwerarbeit auszugeben:** AWS übernimmt die Schwerstarbeit des Rechenzentrumsbetriebs wie Rackierung, Stapelung und Stromversorgung von Servern. Außerdem entfällt der betriebliche Aufwand für die Verwaltung von Betriebssystemen und Anwendungen mit verwalteten Services. So können Sie sich auf Ihre Kunden und Geschäftsprojekte anstatt auf die IT-Infrastruktur konzentrieren.
- **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-Besitzer durchzuführen. Dies hilft bei der Messung der Investitionsrendite (ROI) und gibt Workload-Besitzern die Möglichkeit, ihre Ressourcen zu optimieren und Kosten zu senken.

## Definition

Es gibt fünf Bereiche für bewährte Methoden für die Kostenoptimierung in der Cloud:

- Cloud Financial Management betreiben

- Ausgabenerkennung und Nutzungsbewusstsein
- Kosteneffiziente Ressourcen
- Verwaltung von Nachfrage und Bereitstellung von Ressourcen
- Optimierung im Laufe der Zeit

Wie bei den anderen Säulen innerhalb des Well-Architected Framework gibt es Kompromisse, die berücksichtigt werden müssen, zum Beispiel, ob die Kosten oder die Kosten optimiert werden sollen. speed-to-market In manchen Fällen ist es sinnvoll, die Priorität auf Geschwindigkeit zu legen, z. B. verbunden mit einer raschen Markteinführung, der Bereitstellung neuer Features oder einer simplen Fristerfüllung, statt im Vorfeld in Kostenoptimierung zu investieren. Konzeptionelle Entscheidungen werden gelegentlich durch Eile statt auf Basis von Daten getroffen, und man ist immer der Versuchung ausgesetzt, einem potenziellen Szenario zu viel Bedeutung beizumessen, statt Zeit in die Bestimmung der kostengünstigsten Bereitstellung zu investieren. Dies führt häufig übermäßigen und mangelhaft optimierten Bereitstellungen. Es ist jedoch die richtige Wahl, wenn Sie Ressourcen aus Ihrer On-Premises-Umgebung per Lift and Shift in die Cloud verlagern und die Optimierung anschließend durchführen möchten. Wenn Sie vorab genügend Arbeit in eine Strategie zur Kostenoptimierung investieren, können Sie die wirtschaftlichen Vorteile der Cloud schneller nutzen, indem Sie eine konsistente Einhaltung bewährter Methoden sicherstellen und Überbereitstellungen vermeiden. In den folgenden Abschnitten finden Sie Techniken und bewährte Methoden sowohl für die erste als auch die fortlaufende Implementierung von Cloud-Finanzmanagement und Kostenoptimierung für Ihre Workloads.

## Bewährte Methoden

### Themen

- [Cloud Financial Management betreiben](#)
- [Ausgabenerkennung und Nutzungsbewusstsein](#)
- [Kosteneffiziente Ressourcen](#)
- [Verwaltung von Nachfrage und Bereitstellung von Ressourcen](#)
- [Optimierung im Laufe der Zeit](#)

### Cloud Financial Management betreiben

Mit der Einführung der Cloud können Technologieteams dank verkürzter Genehmigungs-, Beschaffungs- und Infrastrukturbereitstellungszyklen schneller innovieren. Ein neuer Ansatz für das

Finanzmanagement in der Cloud ist erforderlich, um geschäftlichen Nutzen und finanziellen Erfolg zu erzielen. Dieser Ansatz ist das Cloud-Finanzmanagement. Es baut Funktionen in Ihrer gesamten Organisation auf, indem organisationsweit Wissensaufbau, Programme, Ressourcen und Prozesse implementiert werden.

Viele Organisationen bestehen aus vielen verschiedenen Einheiten mit unterschiedlichen Prioritäten. Durch die Fähigkeit, Ihre Organisation an mehreren vereinbarten Finanzziele auszurichten und ihr die Mechanismen zur Erreichung der Ziele bereitzustellen, wird die Effizienz der Organisation gesteigert. Eine leistungsfähige Organisation innoviert und entwickelt schneller, ist agiler und passt sich einfacher an beliebige interne oder externe Faktoren an.

In können AWS Sie den Cost Explorer und optional Amazon Athena und Amazon QuickSight mit dem Kosten- und Nutzungsbericht (CUR) verwenden, um das Kosten- und Nutzungsbewusstsein in Ihrem gesamten Unternehmen zu erhöhen. AWS Budgets bietet proaktive Benachrichtigungen zu Kosten und Nutzung. Die AWS Blogs bieten Informationen zu neuen Diensten und Funktionen, um sicherzustellen, dass Sie über neue Serviceversionen auf dem Laufenden bleiben.

In der folgenden Frage geht es um Überlegungen zur Kostenoptimierung. (Eine Liste der Fragen und bewährten Methoden zur Kostenoptimierung finden Sie im [Anhang](#).)

#### COST1: Wie implementieren Sie Cloud-Finanzmanagement?

Durch die Implementierung von Cloud Financial Management können Unternehmen durch die Optimierung ihrer Kosten und Nutzung sowie die Skalierung ihren Geschäftswert und ihren finanziellen Erfolg steigern AWS.

Setzen Sie beim Aufbau einer Kostenoptimierungsfunktion Mitglieder ein und ergänzen Sie das Team durch Experten für Kostenoptimierung. CFM Bestehende Teammitglieder wissen, wie die Organisation derzeit funktioniert und Verbesserungen schnell implementiert werden können. Erwägen Sie auch, Personen mit ergänzenden oder speziellen Kenntnissen, wie im Bereich Analytik oder Projektmanagement, mit einzubinden.

Wenn Sie in Ihrer Organisation ein Kostenbewusstsein implementieren, verbessern Sie vorhandene Programme oder bauen auf diesen auf. Es geht viel schneller, bestehende Prozesse und Programme zu ergänzen, als sie neu zu erstellen. So werden die Ergebnisse viel schneller erreicht.

## Ausgabenerkennung und Nutzungsbewusstsein

Die erhöhte Flexibilität und Agilität der Cloud fördert Innovationen und schnelle Entwicklungen und Bereitstellungen. Diese Merkmale eliminieren die manuellen Prozesse und den Zeitaufwand für die Bereitstellung einer On-Premises-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 können fundiertere Entscheidungen in Bezug auf die Budgetaufteilung treffen.

In AWS erstellen Sie eine Kontostruktur mit AWS Organizations oder AWS Control Tower, die für eine Trennung sorgt und Sie bei der Verteilung Ihrer Kosten und Nutzung unterstützt. Sie können auch das Ressourcen-Tagging verwenden, um Geschäfts- und Organisationsinformationen auf Ihre Nutzung und Kosten anzuwenden. Verwenden Sie diese Option, AWS Cost Explorer um einen Überblick über Ihre Kosten und Nutzung zu erhalten, oder erstellen Sie maßgeschneiderte Dashboards und Analysen mit Amazon Athena und Amazon. QuickSight Die Kontrolle Ihrer Kosten und Nutzung erfolgt durch Benachrichtigungen über AWS Budgets und Kontrollen mithilfe von AWS Identity and Access Management (IAM) und Service Quotas.

In den folgenden Fragen geht es um Überlegungen zur Kostenoptimierung.

### COST2: Wie regeln Sie die Nutzung?

Legen Sie Richtlinien und Mechanismen fest, um zu überprüfen, ob angemessene Kosten anfallen und die Ziele erreicht werden. Durch die Anwendung eines checks-and-balances Ansatzes können Sie innovativ sein, ohne zu viel auszugeben.

### COST3: Wie überwachen Sie Nutzung und Kosten?

Definieren Sie Richtlinien und Verfahren, um Ihre Kosten überwachen und richtig zuordnen zu können. So können Sie die Kosteneffizienz einer Workload messen und verbessern.

### COST4: Wie werden Ressourcen außer Betrieb genommen?

Implementieren Sie Änderungskontrolle und Ressourcenmanagement von Projektbeginn bis. end-of-life Auf diese Weise können Sie ungenutzte Ressourcen herunterfahren oder beenden, um Verschwendungen zu minimieren.

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

Achten Sie darauf, dass Sie den richtigen Detail- und Granularitätsgrad für die Kosten- und Nutzungsberichterstattung und -überwachung verwenden. Um allgemeine Erkenntnisse zu gewinnen und Trends zu erkennen, verwenden Sie die tägliche Granularität mit AWS Cost Explorer. Für tiefere Analysen und Inspektionen verwenden Sie die stündliche Granularität in AWS Cost Explorer oder Amazon Athena und Amazon QuickSight mit dem Kosten- und Nutzungsbericht (CUR) mit stündlicher Granularität.

Durch die Kombination von mit Tags gekennzeichneten Ressourcen und Entitätslebenszyklus-Tracking (Mitarbeiter, Projekte) können Sie verwaiste Ressourcen oder Projekte identifizieren, die für das Unternehmen keinen Wert mehr generieren und außer Betrieb genommen werden sollten. Sie können Abrechnungsbenachrichtigungen einrichten, um sich über prognostizierte Budgetüberschreitungen zu informieren.

## Kosteneffiziente Ressourcen

Die Verwendung geeigneter Instances und Ressourcen für Ihre 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 Vielzahl flexibler und kostengünstiger Preisoptionen, mit denen Sie Instances von Amazon EC2 und anderen Diensten erwerben können, und zwar auf eine Weise, die Ihren Anforderungen besser entspricht. Mit On-Demand-Instances können Sie die genutzte Datenverarbeitungskapazität auf Stundenbasis und ohne Mindestverpflichtungen bezahlen. Savings Plans und Reserved Instances bieten Einsparungen von bis zu 75 % gegenüber On-Demand-Preisen. Mit Spot-Instances können Sie ungenutzte EC2 Amazon-Kapazitäten nutzen und Einsparungen von bis zu 90% gegenüber den On-Demand-Preisen erzielen. Spot-Instances eignen sich, wenn das System die Nutzung einer Serverflotte toleriert, bei der einzelne Server dynamisch ein- und ausgeschaltet werden können, z. B. statuslose Webserver, Batch-Verarbeitung oder bei Verwendung von HPC Big Data.

Durch die Auswahl geeigneter Dienste können auch die Nutzung und die Kosten reduziert werden, z. B. CloudFront zur Minimierung der Datenübertragung, oder zur Senkung der Kosten, z. B. durch die Verwendung von Amazon Aurora auf Amazon, RDS um teure Datenbanklizenzkosten zu vermeiden.

In den folgenden Fragen geht es um Überlegungen zur Kostenoptimierung.

#### COST5: Wie bewerten Sie die Kosten bei der Auswahl von Services?

Amazon EC2EBS, Amazon und Amazon S3 sind Baustein-Services AWS . Managed Services wie Amazon RDS und Amazon DynamoDB sind Services auf höherer Ebene oder Anwendungsebene. AWS Wenn Sie sich für die richtigen Bausteine und verwalteten Services entscheiden, können Sie die Kosten dieser Workload 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.

**COST6: Wie erreichen Sie die Kostenziele, wenn Sie Art, Größe und Anzahl der Ressourcen auswählen?**

Stellen Sie sicher, dass Sie den geeigneten Ressourcenumfang und die Anzahl der Ressourcen für die jeweilige Aufgabe auswählen. Durch die Auswahl des kostengünstigsten Typs, Umfangs und der kostengünstigsten Anzahl minimieren Sie die Verschwendung von Ressourcen.

**COST7: Wie nutzen Sie Preismodelle, um Kosten zu senken?**

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

**COST8: Wie planen Sie die Gebühren für die Datenübertragung?**

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.

Indem Sie die Kosten bei der Serviceauswahl berücksichtigen und Tools wie Cost Explorer verwenden und AWS Trusted Advisor Ihre AWS Nutzung regelmäßig überprüfen, können Sie Ihre Auslastung aktiv überwachen und Ihre Bereitstellungen entsprechend anpassen.

## Verwaltung von Nachfrage und Bereitstellung von Ressourcen

Wenn Sie in die Cloud wechseln, zahlen Sie nur für die genutzten Ressourcen. Sie können Ressourcen so bereitstellen, dass sie dem Workload-Bedarf zum jeweiligen Zeitpunkt entsprechen. Dadurch werden kostspielige Überbereitstellungen überflüssig. Sie können den Bedarf auch anpassen, indem Sie eine Drosselung, einen Puffer oder eine Warteschlange verwenden, um den Bedarf zu glätten und ihn mit weniger Ressourcen zu erfüllen, was zu niedrigeren Kosten führt. Außerdem können Sie ihn mit einem Batch-Service zu einem späteren Zeitpunkt verarbeiten.

In können Sie automatisch Ressourcen bereitstellen AWS, um dem Workload-Bedarf gerecht zu werden. Durch Auto Scaling mit bedarfs- oder zeitbasiertem Ansatz können Sie Ressourcen nach



Bedarf hinzufügen und entfernen. Wenn Sie in der Lage sind, Bedarfsänderungen zu antizipieren, können Sie mehr Kosten einsparen und zugleich sicherstellen, dass Ihre Ressourcen Ihren Workload-Anforderungen entsprechen. Sie können Amazon API Gateway verwenden, um Drosselung zu implementieren, oder Amazon, SQS um eine Warteschlange in Ihrem Workload zu implementieren. Mit beiden können Sie den Bedarf für Ihre Workload-Komponenten anpassen.

In der folgenden Frage geht es um Überlegungen zur Kostenoptimierung.

### COST9: Wie verwalten Sie Nachfrage und Bereitstellung von Ressourcen?

Stellen Sie bei einer Workload mit ausgewogenen Ausgaben und Leistungen sicher, dass alles, wofür Sie bezahlen, genutzt wird, und vermeiden Sie eine erhebliche Unterauslastung der Instances. Eine verzerrte Nutzungskennzahl in beide Richtungen hat negative Auswirkungen auf Ihr Unternehmen, entweder in Bezug auf Betriebskosten (Leistungseinbußen aufgrund von Überauslastung) oder verschwendete AWS Ausgaben (aufgrund übermäßiger Bereitstellung).

Wenn Sie planen, dass Ressourcen für Bedarf und Bereitstellung geändert werden können, denken Sie auch an die Nutzungsmuster, die Zeit für die Bereitstellung neuer Ressourcen und die Vorhersehbarkeit des Bedarfsmusters. Stellen Sie beim Verwalten des Bedarfs sicher, dass Ihre Warteschlange oder Ihr Puffer korrekt dimensioniert ist und Sie in der erforderlichen Zeit auf den Workload-Bedarf reagieren.

### Optimierung im Laufe der Zeit

Bei AWS der Veröffentlichung neuer Dienste und Funktionen empfiehlt es sich, Ihre bestehenden Architekturentscheidungen zu überprüfen, um sicherzustellen, dass sie auch weiterhin die kostengünstigsten sind. Wenn sich Ihre Anforderungen ändern, zögern Sie nicht, und nehmen Sie Ressourcen, ganze Services und Systeme, die Sie nicht mehr benötigen, außer Betrieb.

Durch die Implementierung neuer Features oder Ressourcentypen können Sie Ihre Workload inkrementell optimieren und gleichzeitig den Aufwand für die Implementierung der Änderung minimieren. Dadurch wird die Effizienz im Laufe der Zeit kontinuierlich verbessert und sichergestellt, dass Sie stets die aktuellste Technologie nutzen, um die Betriebskosten zu senken. Sie können mit neuen Services auch Komponenten der Workload ersetzen oder ihm neue Komponenten hinzufügen. Dies kann zu erheblichen Effizienzsteigerungen führen. Daher ist es wichtig, Ihre Workload regelmäßig zu überprüfen und neue Services und Features zu implementieren.

In den folgenden Fragen geht es um Überlegungen zur Kostenoptimierung.

## COST10: Wie bewerten Sie neue Services?

Bei AWS der Veröffentlichung neuer Dienste und Funktionen ist es eine bewährte Methode, Ihre bestehenden Architekturentscheidungen zu überprüfen, um sicherzustellen, dass sie weiterhin die kostengünstigsten sind.

Wenn Sie Ihre Bereitstellungen regelmäßig überprüfen, sollten Sie auch bewerten, wie Sie mit neueren Services möglicherweise Geld sparen können. Amazon Aurora on Amazon RDS kann beispielsweise die Kosten für relationale Datenbanken senken. Wenn Sie serverlose Technologie wie Lambda verwenden, müssen Sie Instances nicht mehr betreiben und verwalten, um Code auszuführen.

## COST11: Wie schätzen Sie die Kosten des Aufwands ein?

Bewerten Sie die Kosten für den Betrieb in der Cloud, überprüfen Sie Ihren zeitaufwändigen Cloud-Betrieb und automatisieren Sie ihn, um den Personalaufwand und die Kosten zu reduzieren, indem Sie verwandte AWS Dienste, Produkte von Drittanbietern oder maßgeschneiderte Tools einsetzen.

## Ressourcen

Weitere Informationen zu bewährten Methoden für die Kostenoptimierung finden Sie in den folgenden Ressourcen.

### Dokumentation

- [AWS -Dokumentation:](#)

### Whitepaper

- [Säule der Kostenoptimierung](#)

# Nachhaltigkeit

Bei der Säule „Nachhaltigkeit“ geht es um Auswirkungen auf die Umwelt, insbesondere um Energieverbrauch und -effizienz, da diese wichtige Faktoren für Architekten sind, die ihre direkten Aktionen zur Reduzierung des Ressourcenverbrauchs beeinflussen. Verbindliche Anleitungen zur Implementierung finden Sie im [Whitepaper zur Säule „Nachhaltigkeit“](#).

Themen

- [Designprinzipien](#)
- [Definition](#)
- [Bewährte Methoden](#)
- [Ressourcen](#)

## Designprinzipien

Es gibt sechs Designprinzipien für Nachhaltigkeit in der Cloud:

- **Verstehen Ihrer Auswirkungen:** Messen Sie die Auswirkungen Ihrer Cloud-Workloads und modellieren Sie diese Auswirkungen für die Zukunft. berücksichtigen Sie dabei alle relevanten Faktoren, darunter Auswirkungen durch die Verwendung Ihrer Produkte durch Kunden sowie solche durch deren Außerbetriebnahme und Entsorgung. Vergleichen Sie den produktiven Output mit den Gesamtauswirkungen Ihrer Cloud-Workloads, indem Sie die für jede Arbeitseinheit erforderlichen Ressourcen und die damit verbundenen Emissionen ermitteln. Verwenden Sie diese Daten, um wichtige Leistungsindikatoren (KPIs) festzulegen, Möglichkeiten zur Steigerung der Produktivität bei gleichzeitiger Verringerung der Auswirkungen zu bewerten und die Auswirkungen der vorgeschlagenen Änderungen im Laufe der Zeit abzuschätzen.
- **Festlegen von Nachhaltigkeitszielen:** Formulieren Sie für alle Cloud-Workloads langfristige Nachhaltigkeitsziele wie etwa die Reduzierung der pro Transaktion erforderlichen Datenverarbeitungs- und Speicherressourcen. Modellieren Sie den ROI von Verbesserungen in Bezug auf die Nachhaltigkeit vorhandener Workloads. Stellen Sie den Besitzern die nötigen Ressourcen zur Verfügung, um in Nachhaltigkeitsziele investieren zu können. Planen Sie wachstumsorientiert und gestalten Sie Ihre Workloads so, dass das Wachstum mit geringeren Auswirkungen einhergeht – gemessen in einer sinnvollen Einheit, etwa pro Benutzer oder pro Transaktion. Ziele helfen Ihnen, die allgemeinen Nachhaltigkeitsziele Ihres Unternehmens oder Ihrer Organisation zu erreichen, Rückschritte zu identifizieren und Bereiche mit Verbesserungsmöglichkeiten zu priorisieren.

- **Maximieren der Auslastung:** Sorgen Sie für Workloads angemessenen Umfangs und nutzen Sie effiziente Designprinzipien, um eine hohe Auslastung zu gewährleisten und die Energieeffizienz der zugrunde liegenden Hardware so zu maximieren. Zwei Hosts mit 30 % Auslastung sind aufgrund des grundlegenden Energieverbrauchs pro Host weniger effizient als ein Host mit 60 % Auslastung. Gleichzeitig sollten Sie nicht genutzte Ressourcen, Verarbeitungsvorgänge und Speicher reduzieren oder minimieren, um den Gesamtenergieverbrauch für Ihre Workloads zu senken.
- **Antizipieren und Einführen neuer und effizienterer Hardware- und Software-Angebote:** Unterstützen Sie die Verbesserungen, die Ihre Partner und Lieferanten in früheren Prozessphasen vornehmen, um die Auswirkungen Ihrer Cloud-Workloads zu reduzieren. Achten Sie stets auf neue und effizientere Hardware- und Software-Angebote. Planen Sie für Flexibilität, damit neue effiziente Technologien schnell eingeführt werden können.
- **Verwenden von verwalteten Services:** Die gemeinsame Nutzung von Services über eine breite Kundenbasis hinweg hilft dabei, die Ressourcennutzung zu maximieren und dadurch den Umfang der Infrastruktur zu verringern, der für die Unterstützung Ihrer Cloud-Workloads erforderlich ist. Kunden können beispielsweise die Auswirkungen gemeinsamer Rechenzentrumskomponenten wie Stromversorgung und Netzwerke gemeinsam nutzen, indem sie Workloads in die Umgebung migrieren AWS Cloud und Managed Services wie AWS Fargate für serverlose Container einsetzen, die skalierbar arbeiten und für deren effizienten AWS Betrieb verantwortlich sind. Nutzen Sie verwaltete Services, die Ihnen helfen können, Ihre Auswirkungen zu minimieren, wie z. B. die automatische Verschiebung selten aufgerufener Daten in Cold Storage mit Amazon S3 Lifecycle-Konfigurationen oder Amazon EC2 Auto Scaling, um die Kapazität an die Nachfrage anzupassen.
- **Reduzieren der nachgelagerten Auswirkungen Ihrer Cloud-Workloads:** Senken Sie den Energie- oder Ressourcenverbrauch für die Nutzung Ihrer Services. Reduzieren Sie die Erfordernis für Kunden, ihre Geräte zu aktualisieren, um Ihre Services nutzen zu können. Verwenden Sie in Ihren Tests Gerätefarmen, um die zu erwartenden Auswirkungen zu verstehen, und führen Sie Tests mit Kunden durch, um die tatsächlichen Auswirkungen der Nutzung Ihrer Services zu erkennen.

## Definition

Es gibt sechs Bereiche für bewährte Methoden für Nachhaltigkeit in der Cloud:

- Auswahl der Region
- Ausrichtung am Bedarf
- Software und Architektur

- Daten
- Hardware und Services
- Prozess und Kultur

Nachhaltigkeit in der Cloud ist ein nahezu kontinuierliches Bestreben, das sich in erster Linie auf die Reduzierung des Energieverbrauchs und die Effizienz aller Komponenten einer Workload konzentriert. Dazu muss der maximale Nutzen aus den bereitgestellten Ressourcen gezogen und die insgesamt erforderlichen Ressourcen müssen minimiert werden. Diese Bemühung kann von der anfänglichen Auswahl einer effizienten Programmiersprache, der Einführung moderner Algorithmen, der Nutzung effizienter Datenspeichertechniken, der Bereitstellung einer korrekt dimensionierten und effizienten Recheninfrastruktur bis hin zur Minimierung der Anforderungen an leistungsstarke Endbenutzerhardware reichen.

## Bewährte Methoden

### Themen

- [Auswahl der Region](#)
- [Ausrichtung am Bedarf](#)
- [Software und Architektur](#)
- [Datenverwaltung](#)
- [Hardware und Services](#)
- [Prozess und Kultur](#)

### Auswahl der Region

Die Wahl der Region für Ihren Workload wirkt sich erheblich auf dessen LeistungKPIs, Kosten und CO2-Fußabdruck aus. Um diese zu verbessernKPIs, sollten Sie Regionen für Ihre Workloads auswählen, die sowohl auf Geschäftsanforderungen als auch auf Nachhaltigkeitszielen basieren.

In der folgenden Frage geht es um Überlegungen zur Nachhaltigkeit. (Eine Liste der Fragen und bewährten Methoden zur Nachhaltigkeit finden Sie im [Anhang](#)).

## SUS1: Wie wählen Sie Regionen für Ihren Workload aus?

Die Wahl der Region für Ihren Workload wirkt sich erheblich auf dessen LeistungKPIs, Kosten und CO2-Fußabdruck aus. Um diese zu verbessernKPIs, sollten Sie Regionen für Ihre Workloads auswählen, die sowohl auf Geschäftsanforderungen als auch auf Nachhaltigkeitszielen basieren.

## Ausrichtung am Bedarf

Wenn Sie berücksichtigen, wie Benutzer und Anwendungen Ihre Workloads und andere Ressourcen nutzen, können Sie auf diese Weise Verbesserungsmöglichkeiten ermitteln, um Nachhaltigkeitsziele zu erreichen. Skalieren Sie Ihre Infrastruktur so, dass Sie den Bedarf kontinuierlich anpassen können. Sorgen Sie zudem dafür, dass zur Unterstützung Ihrer Benutzer nicht mehr Ressourcen verwendet werden als unbedingt nötig. Richten Sie Service-Levels an den Kundenanforderungen aus. Positionieren Sie Ressourcen so, dass die Netzwerkkapazitäten, die für Benutzer und Anwendungen erforderlich sind, begrenzt werden. Entfernen Sie ungenutzte Komponenten. Stellen Sie Teammitgliedern Geräte zur Verfügung, die ihre Anforderungen bei geringstmöglichen Auswirkungen auf die Nachhaltigkeit erfüllen.

Die folgende Frage konzentriert sich auf diese Überlegungen zur Nachhaltigkeit:

## SUS2: Wie passen Sie Cloud-Ressourcen an Ihren Bedarf an?

Wenn Sie berücksichtigen, wie Benutzer und Anwendungen Ihre Workloads und andere Ressourcen nutzen, können Sie auf diese Weise Verbesserungsmöglichkeiten ermitteln, um Nachhaltigkeitsziele zu erreichen. Skalieren Sie Ihre Infrastruktur so, dass Sie den Bedarf kontinuierlich anpassen können. Sorgen Sie zudem dafür, dass zur Unterstützung Ihrer Benutzer nicht mehr Ressourcen verwendet werden als unbedingt nötig. Richten Sie Service-Levels an den Kundenanforderungen aus. Positionieren Sie Ressourcen so, dass die Netzwerkkapazitäten, die für Benutzer und Anwendungen erforderlich sind, begrenzt werden. Entfernen Sie ungenutzte e Komponenten. Stellen Sie Teammitgliedern Geräte zur Verfügung, die ihre Anforderungen bei geringstmöglichen Auswirkungen auf die Nachhaltigkeit erfüllen.

Skalieren der Infrastruktur anhand der Benutzerlast: Identifizieren Sie Zeiträume mit geringer oder gar keiner Nutzung und skalieren Sie Ressourcen, um überschüssige Kapazitäten zu entfernen und die Effizienz zu verbessern.

Auf Nachhaltigkeitsziele ausrichten SLAs: Definieren und aktualisieren Sie Service Level Agreements (SLAs) wie Verfügbarkeits- oder Datenaufbewahrungsfristen, um die Anzahl der Ressourcen zu minimieren, die zur Unterstützung Ihrer Arbeitslast erforderlich sind, und gleichzeitig die Geschäftsanforderungen zu erfüllen.

Beenden der Erstellung und Wartung nicht verwendeter Komponenten: Analysieren Sie Anwendungskomponenten (wie vorab kompilierte Berichte, Datensätze und statische Bilder) sowie Zugriffsmuster für Komponenten, um Redundanzen, eine zu geringe Auslastung und mögliche Kandidaten für die Außerbetriebnahme zu identifizieren. Konsolidieren Sie generierte Komponenten mit redundanten Inhalten (z. B. monatliche Berichte mit sich überschneidenden oder gemeinsam genutzten Datensätzen und Ausgaben), um für duplizierte Ausgaben genutzte Ressourcen zu eliminieren. Deaktivieren Sie nicht verwendete Komponenten (z. B. Bilder von Produkten, die nicht mehr verkauft werden), um genutzte Ressourcen freizugeben und die Zahl der Ressourcen zu reduzieren, die zur Unterstützung von Workloads verwendet werden.

Optimieren der geografischen Platzierung von Workloads für Benutzerstandorte: Analysieren Sie Netzwerkzugriffsmuster, um zu erkennen, aus welchen geografischen Regionen Ihre Kunden Verbindungen herstellen. Wählen Sie Regionen und Services im Hinblick auf die Reduzierung der Distanz für den Netzwerkdatenverkehr aus, um die Zahl der Netzwerkressourcen zu verringern, die zur Unterstützung von Workloads benötigt werden.

Optimieren von Ressourcen für Teammitglieder im Hinblick auf die ausgeführten Aktivitäten: Optimieren Sie die Ressourcen, die Teammitgliedern zur Verfügung gestellt werden, um negative Auswirkungen auf die Nachhaltigkeit zu minimieren und gleichzeitig ihre Anforderungen zu erfüllen. Beispielsweise können Sie komplexe Vorgänge wie Rendering und Kompilierung auf intensiv genutzten, geteilten Cloud-Desktops statt auf weniger ausgelasteten Einzelbenutzersystemen mit hohem Energieverbrauch ausführen.

## Software und Architektur

Implementieren Sie Muster für den Lastausgleich und die Wahrung einer konsistent hohen Nutzung der bereitgestellten Ressourcen, um die Zahl der genutzten Ressourcen zu minimieren. Komponenten werden möglicherweise aufgrund von Änderungen des Benutzerverhaltens über die Zeit nicht mehr genutzt. Prüfen Sie Muster und Architekturen, um nicht ausreichend genutzte Komponenten zu konsolidieren und so die Nutzung insgesamt zu erhöhen. Nehmen Sie Komponenten außer Betrieb, die nicht mehr benötigt werden. Identifizieren Sie die Leistung Ihrer Workload-Komponenten und optimieren Sie die Komponenten, die die meisten Ressourcen verbrauchen. Achten Sie auf die Geräte, mit denen Ihre Kunden auf Ihre Services zugreifen, und implementieren Sie Muster, um den Bedarf für Geräte-Upgrades zu minimieren.

In den folgenden Fragen geht es um diese Überlegungen zur Nachhaltigkeit:

SUS3: Wie nutzen Sie Software- und Architekturmuster, um Ihre Nachhaltigkeitsziele zu erreichen ?

Implementieren Sie Muster für den Lastausgleich und die Wahrung einer konsistent hohen Nutzung der bereitgestellten Ressourcen, um die Zahl der genutzten Ressourcen zu minimieren. Komponenten werden möglicherweise aufgrund von Änderungen des Benutzerverhaltens über die Zeit nicht mehr genutzt. Prüfen Sie Muster und Architekturen, um nicht ausreichend genutzte Komponenten zu konsolidieren und so die Nutzung insgesamt zu erhöhen. Nehmen Sie Komponenten außer Betrieb, die nicht mehr benötigt werden. Identifizieren Sie die Leistung Ihrer Workload-Komponenten und optimieren Sie die Komponenten, die die meisten Ressourcen verbrauchen. Achten Sie auf die Geräte, mit denen Ihre Kunden auf Ihre Services zugreifen, und implementieren Sie Muster, um den Bedarf für Geräte-Upgrades zu minimieren.

Optimieren von Software und Architektur für asynchrone und geplante Aufträge: Verwenden Sie effiziente Softwaredesigns und Architekturen, um die Zahl der für einzelne Arbeitseinheiten im Durchschnitt benötigten Ressourcen zu minimieren. Implementieren Sie Mechanismen für die gleichmäßige Nutzung von Komponenten, um die Zahl der Ressourcen zu reduzieren, die zwischen Aufgaben nicht genutzt werden, und die Auswirkungen von Lastspitzen zu minimieren.

Entfernen von Workload-Komponenten mit geringer oder keiner Nutzung oder Faktorwechsel: Überwachen Sie die Workload-Aktivität, um Änderungen bei der Nutzung einzelner Komponenten über die Zeit zu erkennen. Entfernen Sie ungenutzte Komponenten, die nicht mehr benötigt werden. Führen Sie einen Faktorwechsel für wenig genutzte Ressourcen durch, um die Verschwendung von Ressourcen zu begrenzen.

Optimieren von Codebereichen, die die meiste Zeit oder die meisten Ressourcen verbrauchen: Überwachen Sie die Workload-Aktivität, um die Anwendungskomponenten zu identifizieren, die die meisten Ressourcen verbrauchen. Optimieren Sie den Code, der innerhalb dieser Komponenten ausgeführt wird, um die Ressourcennutzung zu minimieren und die Leistung zu maximieren.

Optimieren der Auswirkungen auf Geräte und Ausrüstung von Kunden: Identifizieren Sie die Geräte und Einrichtungen, mit denen Ihre Kunden Ihre Services nutzen, ihren voraussichtlichen Lebenszyklus und die finanziellen und nachhaltigkeitsbezogenen Auswirkungen der Ersetzung dieser Komponenten. Implementieren Sie Softwaremuster und Architekturen, die es für Kunden unnötig machen, Geräte zu ersetzen oder ihre Ausrüstung zu aktualisieren. Implementieren



Sie beispielsweise neue Features, die Code verwenden, der mit älterer Hardware und älteren Betriebssystemversionen abwärtskompatibel ist, oder gestalten Sie die Größe von Nutzlasten so, dass sie die Speicherkapazitäten der Zielgeräte nicht überschreiten.

Verwenden von Softwaremustern und Architekturen, die Datenzugriffs- und Speichermuster optimal unterstützen: Identifizieren Sie, wie Daten in Ihrer Workload verwendet, von Benutzern genutzt, übertragen und gespeichert werden. Wählen Sie Technologien aus, die die Anforderungen an Datenverarbeitung und -speicherung minimieren.

## Datenverwaltung

In den folgenden Fragen geht es um diese Überlegungen zur Nachhaltigkeit:

SUS4: Wie nutzen Sie Datenmanagementrichtlinien und -muster, um Ihre Nachhaltigkeitsziele zu unterstützen?

Implementieren Sie Verfahren für die Datenverwaltung, die den zur Unterstützung Ihrer Workload bereitgestellten Speicher und die für dessen Nutzung erforderlichen Ressourcen reduzieren. Verstehen Sie Ihre Daten und setzen Sie Speichertechnologien und -konfigurationen ein, die den geschäftlichen Mehrwert der Daten und deren Nutzung am besten fördern. Verschieben Sie die Daten während des Lebenszyklus zu effizienteren Speichern mit geringerer Leistung, wenn die Anforderungen abnehmen. Löschen Sie Daten, die nicht mehr benötigt werden.

Implementieren einer Richtlinie für die Klassifizierung von Daten: Klassifizieren Sie Daten, um ihre Bedeutung für geschäftliche Ergebnisse zu verstehen. Nutzen Sie diese Informationen, um festzulegen, wann Daten in einen energieeffizienteren Speicher übertragen oder auf sichere Weise gelöscht werden können.

Verwenden von Technologien, die Datenzugriff und Speichermuster unterstützen: Nutzen Sie einen Speicher, der den Zugriff auf Ihre Daten und ihre Speicherung jeweils optimal unterstützt, um die Zahl der bereitgestellten Ressourcen zu minimieren und gleichzeitig Ihre Workload zu unterstützen. Festkörpergeräte (SSDs) sind beispielsweise energieintensiver als Magnetlaufwerke und sollten nur für aktive Datenanwendungen verwendet werden. Verwenden Sie für Daten, auf die nicht häufig zugegriffen wird, einen energieeffizienten Archivierungsspeicher.

Verwenden von Lebenszyklusrichtlinien zum Löschen nicht notwendiger Daten: Verwalten Sie den Lebenszyklus aller Daten und setzen Sie automatisch Löschfristen durch, um die Speicheranforderungen Ihrer Workload insgesamt zu minimieren.

Minimieren übermäßiger Bereitstellungen im Blockspeicher: Erstellen Sie zur Minimierung des insgesamt bereitgestellten Speichers Blockspeicher mit Größenzuweisungen entsprechend der jeweiligen Workload. Verwenden Sie elastische Volumes, um den Speicher bei wachsenden Datenmengen erweitern zu können, ohne die Größe des an Datenverarbeitungsressourcen angefügten Speichers ändern zu müssen. Überprüfen Sie elastische Volumes regelmäßig und verkleinern Sie zu große Volumes, um sie an den aktuellen Datenumfang anzupassen.

Entfernen nicht benötigter oder redundanter Daten: Duplizieren Sie Daten nur wie notwendig, um den insgesamt genutzten Speicher zu minimieren. Verwenden Sie Sicherungstechnologien, die Daten auf Datei- und Blockebene deduplizieren. Beschränken Sie die Verwendung von Konfigurationen mit redundanten Arrays unabhängiger Laufwerke (RAID), es sei denn, dies ist erforderlich, um folgende Anforderungen zu erfüllen SLAs.

Verwenden geteilter Dateisysteme oder Objektspeicher für den Zugriff auf allgemeine Daten: Verwenden Sie geteilten Speicher und zentrale Datenquellen, um Datenduplizierungen zu vermeiden und den Gesamtspeicherbedarf Ihrer Workload zu reduzieren. Rufen Sie Daten nur bei Bedarf aus dem gemeinsam genutzten Speicher ab. Trennen Sie nicht genutzte Volumes, um Ressourcen freizugeben. Minimieren Sie Datenübertragungen über Netzwerke hinweg. Verwenden Sie stattdessen einen geteilten Speicher und greifen Sie über regionale Datenspeicher auf die Daten zu, um die Zahl der Netzwerkressourcen zu minimieren, die für Datenübertragungen für Ihre Workload benötigt werden.

Sichern von Daten nur in dem Fall, dass ihre erneute Erstellung schwierig ist: Sichern Sie zur Minimierung der Speichernutzung nur Daten, die einen Unternehmenswert besitzen oder zur Erfüllung von Compliance-Anforderungen benötigt werden. Prüfen Sie Sicherheitsrichtlinien und vermeiden Sie einen flüchtigen Speicher, der in einem Wiederherstellungsszenario keinen Wert bietet.

## Hardware und Services

Suchen Sie nach Möglichkeiten, die Auswirkungen auf die Nachhaltigkeit Ihrer Workloads durch Änderungen der Methoden für die Hardwareverwaltung zu reduzieren. Minimieren Sie den Umfang der für die Bereitstellung erforderlichen Hardware und wählen Sie die jeweils effizienteste Hardware und den effizientesten Service für die jeweilige Workload aus.

In den folgenden Fragen geht es um diese Überlegungen zur Nachhaltigkeit:

## SUS5: Wie wählen und nutzen Sie Cloud-Hardware und -Services in Ihrer Architektur, um Ihre Nachhaltigkeitsziele zu unterstützen?

Suchen Sie nach Möglichkeiten, die Auswirkungen auf die Nachhaltigkeit Ihrer Workloads durch Änderungen der Methoden für die Hardwareverwaltung zu reduzieren. Minimieren Sie den Umfang der für die Bereitstellung erforderlichen Hardware und wählen Sie die jeweils effizienteste Hardware und den effizientesten Service für die jeweilige Workload aus.

Verwenden der geringstmöglichen Menge an Hardware zur Erfüllung Ihrer Anforderungen: Mit den Möglichkeiten der Cloud können Sie häufige Änderungen für Ihre Workload-Implementierungen ausführen. Aktualisieren Sie bereitgestellte Komponenten, wenn sich Ihre Anforderungen ändern.

Verwendung von Instance-Typen mit den geringsten Auswirkungen: Überwachen Sie kontinuierlich die Einführung neuer Instance-Typen und nutzen Sie Verbesserungen bei der Energieeffizienz, einschließlich Instance-Typen, die zur Unterstützung spezifischer Workloads bestimmt sind, wie z. B. Machine-Learning-Trainings und -Inferenzen und Videotranskodierung.

Nutzen Sie Managed Services: Managed Services verlagern die Verantwortung für die Aufrechterhaltung einer hohen durchschnittlichen Auslastung und die Nachhaltigkeitsoptimierung der eingesetzten Hardware auf AWS. Mit verwalteten Services können Sie die nachhaltigkeitsbezogenen Auswirkungen des Service über alle Mandanten des Service verteilen und so Ihren Beitrag verringern.

Optimieren Sie Ihre Nutzung von GPUs: Grafikprozessoren (GPUs) können einen hohen Stromverbrauch verursachen, und viele GPU Workloads sind sehr variabel, wie z. B. Rendern, Transcodieren sowie Training und Modellierung für maschinelles Lernen. Führen Sie GPUs Instanzen nur für die benötigte Zeit aus und nehmen Sie sie automatisiert außer Betrieb, wenn sie nicht benötigt werden, um den Ressourcenverbrauch zu minimieren.

## Prozess und Kultur

Reduzieren Sie nachhaltigkeitsbezogene Auswirkungen, indem Sie Ihre Entwicklungs-, Test- und Bereitstellungsmethoden ändern.

In den folgenden Fragen geht es um diese Überlegungen zur Nachhaltigkeit:

## SUS6: Wie unterstützen Ihre organisatorischen Prozesse Ihre Nachhaltigkeitsziele?

Reduzieren Sie nachhaltigkeitsbezogene Auswirkungen, indem Sie Ihre Entwicklungs-, Test- und Bereitstellungsmethoden ändern.

Einführen von Methoden, die schnelle Verbesserungen für die Nachhaltigkeit ermöglichen: Testen und validieren Sie potenzielle Verbesserungen, bevor Sie sie für die Produktion bereitstellen. Berücksichtigen Sie die Testkosten bei der Berechnung des potenziellen zukünftigen Nutzens einer Verbesserung. Entwickeln Sie kostengünstige Testmethoden, um kleine Verbesserungen einzuführen.

Halten Sie Ihren Workload auf dem neuesten Stand: Up-to-date Betriebssysteme, Bibliotheken und Anwendungen können die Workload-Effizienz verbessern und die Einführung effizienterer Technologien fördern. Up-to-date Software kann auch Funktionen enthalten, mit denen Sie die Auswirkungen Ihrer Workloads auf die Nachhaltigkeit genauer messen können, da Anbieter Funktionen bereitstellen, mit denen sie ihre eigenen Nachhaltigkeitsziele erreichen können.

Höhere Auslastung von Entwicklungsumgebungen: Verwenden Sie Automatisierung und Infrastructure-as-Code, um Vorproduktionsumgebungen bei Bedarf in Betrieb und bei Nichtverwendung wieder außer Betrieb zu nehmen. Eine typische Vorgehensweise besteht in der Planung von Verfügbarkeitszeiten, die mit den Arbeitszeiten der Entwicklungsteams übereinstimmen. Der Ruhezustand ist ein nützliches Tool, um den Status beizubehalten und Instances nur bei Bedarf schnell online zu schalten. Verwenden Sie Instance-Typen mit Burst-Kapazität, Spot Instances, Services für elastische Datenbanken, Container und andere Technologien, um Entwicklungs- und Testkapazitäten an die Nutzung anzupassen.

Verwenden verwalteter Gerätefarmen für Tests verwenden: Verwaltete Gerätefarmen verteilen die nachhaltigkeitsbezogenen Auswirkungen der Hardwarefertigung und der Ressourcennutzung über zahlreiche Mandanten. Verwaltete Gerätefarmen stellen verschiedene Gerätetypen bereit, unterstützen auch ältere und weniger verbreitete Hardware und vermeiden nachhaltigkeitsbezogene Auswirkungen durch unnötige Geräte-Upgrades seitens Kunden.

## Ressourcen

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

## Whitepaper

- [Säule „Nachhaltigkeit“](#)

## Video

- [The Climate Pledge](#)

# Der Überprüfungsprozess

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 der Workload arbeitet, ein angenehmeres Erlebnis ermöglichen.

Wie bereits im Abschnitt „Architekturüberlegungen“ 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 nahezu fortlaufend statt, können Ihre Teammitglieder parallel mit der Entwicklung der Architektur Antworten aktualisieren und mit jedem neuen Feature die Architektur verbessern.

Das AWS Well-Architected Framework ist auf die Art und Weise ausgerichtet, wie Systeme und Dienste intern AWS überprüft werden. Es basiert auf einer Reihe von Entwurfsprinzipien, die den architektonischen Ansatz beeinflussen, sowie auf Fragen, die sicherstellen, dass Bereiche, die häufig in der Ursachenanalyse () behandelt werden, nicht vernachlässigt werden. RCA Immer wenn es ein schwerwiegendes Problem mit einem internen System, einem AWS Service oder einem Kunden gibt, prüfen wir, ob wir die RCA von uns verwendeten Überprüfungsprozesse verbessern können.

Die Überprüfungen müssen an wichtigen Meilensteinen des Produktzyklus erfolgen – früh in der Entwurfsphase, um Einbahnstraßen zu vermeiden, an denen schwer nachzubessern ist. Und zuletzt schließlich kurz vor dem Go-Live. (Viele Entscheidungen können rückgängig gemacht werden; es gibt zwei Möglichkeiten. Für diese Entscheidungen reicht ein schlanker Prozess. Gibt es nur eine Möglichkeit, kann diese nur schwer oder gar nicht rückgängig gemacht werden und muss genauer inspiziert werden, bevor sie gewählt wird.) Nachdem Sie in Produktion gehen, verändert sich Ihre Workload weiter, da neue Funktionen hinzukommen und Sie Technologieimplementierungen anpassen. Die Architektur einer Workload 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 sein. Häufig ist die Überprüfung der Punkt, an dem einem Team das erste Mal richtig klar wird, was es implementiert hat. Wird die Workload eines anderen Teams überprüft, ist es sinnvoll, mehrere informelle Konversationen über deren 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
- Maßnahmenliste mit Fragen, für out-of-band deren Beantwortung Nachforschungen erforderlich sind (z. B. „Haben wir die Verschlüsselung aktiviert oder nicht?“)

Nach der Überprüfung sollten Sie eine Liste mit Problemen vorliegen haben. Welche Sie priorisieren, hängt vom geschäftlichen Kontext ab. Sie sollten auch die Auswirkungen dieser Probleme auf die day-to-day Arbeit Ihres Teams berücksichtigen. Wenn Sie die Probleme frühzeitig angehen, 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 entgegen, 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 geschützte Informationen preisgibt.

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.



# Schlussfolgerung

Das AWS Well-Architected Framework bietet architektonische Best Practices in den sechs Säulen für die Entwicklung und den Betrieb zuverlässiger, sicherer, effizienter, kostengünstiger und nachhaltiger Systeme in der Cloud. Die Fragen aus dem Framework erlauben Ihnen, bestehende und geplante Architekturen zu überprüfen. Es bietet auch eine Reihe von AWS Best Practices für jede Säule. Als fester Bestandteil Ihres Architekturdesigns fördert das Framework stabile und effiziente Systeme. Anschließend können Sie sich auf Ihre funktionalen Anforderungen konzentrieren.

# Mitwirkende

Folgende Personen und Organisationen haben zu diesem Dokument beigetragen:

- Brian Carlson, Operations Lead Well-Architected, Amazon Web Services
- Ben Potter, Security Lead Well-Architected, Amazon Web Services
- Seth Eliot, Reliability Lead Well-Architected, Amazon Web Services
- Eric Pullen, Sr. Solutions Architect, Amazon Web Services
- Rodney Lester, Principal Solutions Architect, Amazon Web Services
- Jon Steele, Sr. Technical Account Manager, Amazon Web Services
- Max Ramsay, Principal Security Solutions Architect, Amazon Web Services
- Callum Hughes, Solutions Architect, Amazon Web Services
- Ben Mergen, Senior Cost Lead Solutions Architect, Amazon Web Services
- Chris Kozlowski, Senior Specialist Technical Account Manager, Enterprise Support, Amazon Web Services
- Alex Livingstone, Principal Specialist Solutions Architect, Cloud Operations, Amazon Web Services
- Paul Moran, Principal Technologist, Enterprise Support, Amazon Web Services
- Peter Mullen, Advisory Consultant, Professional Services, Amazon Web Services
- Chris Pates, Senior Specialist Technical Account Manager, Enterprise Support, Amazon Web Services
- Arvind Raghunathan, Principal Specialist Technical Account Manager, Enterprise Support, Amazon Web Services
- Sam Mokhtari, Senior Efficiency Lead Solutions Architect, Amazon Web Services

# Weitere Informationen

[AWS -Architekturzentrum](#)

[AWS Cloud-Compliance](#)

[AWS Well-Architected-Partnerprogramm](#)

[AWS Well-Architected Tool](#)

[AWS Well-Architected Homepage](#)

[Whitepaper zur Säule „Betriebliche Exzellenz“](#)

[Whitepaper zur Säule „Sicherheit“](#)

[Whitepaper zur Säule „Zuverlässigkeit“](#)

[Whitepaper zur Säule „Leistungseffizienz“](#)

[Whitepaper zur Säule „Kostenoptimierung“](#)

[Whitepaper zur Säule „Nachhaltigkeit“](#)

[Die Amazon Builders' Library](#)

# Dokumentversionen

Abonnieren Sie den Feed, um über Aktualisierungen dieses Whitepapers informiert zu werden. [RSS](#)


Änderung	Beschreibung	Datum
<a href="#">Leitfäden zu bewährten Methoden aktualisiert</a>	In den Säulen wurden umfangreiche Aktualisierungen der bewährten Methoden vorgenommen. Für Sicherheit und Kosten wurden neue bewährte Methoden hinzugefügt.	27. Juni 2024
<a href="#">Größere Aktualisierung</a>	Größere Aktualisierungen der Säulen.	3. Oktober 2023
<a href="#">Aktualisierungen für das neue Framework</a>	Bewährte Methoden mit verbindlichen Anleitungen aktualisiert und neue bewährte Methoden hinzugefügt. Neue Fragen zu den Säulen Sicherheit und Kostenoptimierung hinzugefügt.	10. April 2023
<a href="#">Kleines Update</a>	Eine Definition für Grad des Aufwands wurde hinzugefügt und bewährte Methoden im Anhang wurden aktualisiert.	20. Oktober 2022
<a href="#">Whitepaper aktualisiert</a>	Die Säule „Nachhaltigkeit“ wurde hinzugefügt und Links wurden aktualisiert.	2. Dezember 2021
<a href="#">Größere Aktualisierung</a>	Die Säule „Nachhaltigkeit“ wurde dem Framework hinzugefügt.	20. November 2021

---

<a href="#">Kleines Update</a>	Nicht inklusive Sprache entfernt.	22. April 2021
<a href="#">Kleines Update</a>	Zahlreiche Links wurden repariert.	10. März 2021
<a href="#">Kleines Update</a>	Kleinere redaktionelle Änderungen im gesamten Dokument.	15. Juli 2020
<a href="#">Aktualisierungen für das neue Framework</a>	Prüfung und Umformulierung der meisten Fragen und Antworten.	8. Juli 2020
<a href="#">Whitepaper aktualisiert</a>	AWS Well-Architected Tool Hinzufügung von Links zu AWS Well-Architected Labs und AWS Well-Architected Partners, kleinere Korrekturen zur Aktivierung mehrsprachiger Versionen des Frameworks.	1. Juli 2019
<a href="#">Whitepaper aktualisiert</a>	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.	1. November 2018

---

<a href="#">Whitepaper aktualisiert</a>	Fragentext ist nach mehreren Aktualisierungen einfacher formuliert, Antworten sind standardisiert und die Lesbarkeit wurde verbessert.	1. Juni 2018
<a href="#">Whitepaper aktualisiert</a>	Betriebliche Exzellenz wurde vor die anderen Säulen gesetzt und umgeschrieben. Umfasst jetzt die anderen Säulen. Andere Säulen wurden aktualisiert, um der Entwicklung von Rechnung zu tragen. AWS	1. November 2017
<a href="#">Whitepaper aktualisiert</a>	Aktualisierung des Framework . Dieses enthält jetzt die Säule „Betriebliche Exzellenz“. Die anderen Säulen wurden überarbeitet und aktualisiert. Dabei wurden Doppelungen ausgeräumt und Erkenntnisse aus Überprüfungen bei mehreren Tausend Kunden aufgenommen.	1. November 2016
<a href="#">Kleinere Updates</a>	Der Anhang wurde mit aktuellen Amazon CloudWatch Logs-Informationen aktualisiert.	1. November 2015
<a href="#">Erste Veröffentlichung</a>	AWS Well-Architected Framework veröffentlicht.	1. Oktober 2015

 Note

Um RSS Updates zu abonnieren, muss für den von Ihnen verwendeten Browser ein RSS Plugin aktiviert sein.

## Framework-Versionen:

- [2023-10-03](#) (aktuell)
- [2023-04-10](#)
- [31.03.2022](#)

# Anhang: Fragen und bewährte Methoden

Dieser Anhang fasst alle Fragen und bewährten Methoden im AWS Well-Architected Framework zusammen.

## Säulen

- [Operative Exzellenz](#)
- [Sicherheit](#)
- [Zuverlässigkeit](#)
- [Leistungseffizienz](#)
- [Kostenoptimierung](#)
- [Nachhaltigkeit](#)

## Operative Exzellenz

Die Säule „Operative Exzellenz“ beinhaltet die Fähigkeit, die Entwicklung zu unterstützen und Workloads effektiv auszuführen, Einblicke in die eigenen Betriebsabläufe zu erhalten und unterstützende Prozesse und Verfahren fortlaufend zu verbessern, um geschäftlichen Mehrwert zu schaffen. Verbindliche Anleitungen zur Implementierung finden Sie im [Whitepaper „Säule der betrieblichen Exzellenz“](#).

## Bereiche für bewährte Methoden

- [Organisation](#)
- [Vorbereitung](#)
- [Betrieb](#)
- [Weiterentwicklung](#)

## Organisation

### Fragen

- [OPS1. Wie bestimmen Sie, was Ihre Prioritäten sind?](#)
- [OPS2. Wie strukturieren Sie Ihr Unternehmen, um die gewünschten Geschäftsergebnisse zu erzielen?](#)



- [OPS3. Wie unterstützt Ihre Unternehmenskultur Ihre Geschäftsergebnisse?](#)

## OPS1. Wie bestimmen Sie, was Ihre Prioritäten sind?

Jeder muss verstehen, welchen Beitrag er zum Geschäftserfolg leistet. Setzen Sie sich gemeinsame Ziele, damit Sie die Prioritäten für Ressourcen festlegen können. Dadurch erzielen Ihre Bemühungen den größtmöglichen Nutzen.

### Bewährte Methoden

- [OPS01-BP01 Kundenbedürfnisse bewerten](#)
- [OPS01-BP02 Evaluieren Sie die internen Kundenbedürfnisse](#)
- [OPS01-BP03 Bewertung der Governance-Anforderungen](#)
- [OPS01-BP04 Evaluieren Sie die Compliance-Anforderungen](#)
- [OPS01-BP05 Bewerten Sie die Bedrohungslandschaft](#)
- [OPS01-BP06 Bewerten Sie Kompromisse und managen Sie gleichzeitig Vorteile und Risiken](#)

### OPS01-BP01 Kundenbedürfnisse bewerten

Binden Sie alle wichtigen Stakeholder ein, einschließlich Geschäfts-, Entwicklungs- und Betriebsteams, um zu bestimmen, welche Bereiche verstärkt auf die Bedürfnisse der externen Kunden ausgerichtet werden müssen. Dadurch wird sichergestellt, dass Sie mit der betrieblichen Unterstützung vertraut sind, die erforderlich ist, um die gewünschten geschäftlichen Ergebnisse zu erzielen.

### Gewünschtes Ergebnis:

- Sie arbeiten rückwärts von den Kundenergebnissen aus.
- Sie wissen, wie Ihre betrieblichen Praktiken Geschäftsergebnisse und -ziele unterstützen.
- Sie binden alle relevanten Parteien ein.
- Sie verfügen über Mechanismen, um Kundenbedürfnisse zu erfassen.

### Typische Anti-Muster:

- Sie haben sich entschieden, außerhalb der Kerngeschäftszeiten keinen Kundenservice zu bieten, aber Sie haben dazu keine historischen Supportanfragedaten analysiert. Daher wissen Sie nicht, ob diese Entscheidung Auswirkungen auf Ihre Kunden hat.

- Sie entwickeln ein neues Feature, haben aber Ihre Kunden nicht miteinbezogen, um herauszufinden, ob die Funktion erwünscht ist und wie sie genau aussehen sollte. Außerdem haben Sie keine Tests durchgeführt, um die Nachfrage und die Methode der Bereitstellung zu validieren.

Vorteile der Nutzung dieser bewährten Methode: Kunden, deren Anforderungen erfüllt sind, bleiben mit höherer Wahrscheinlichkeit als Kunden erhalten. Die Bewertung und das Verständnis externer Kundenbedürfnisse liefert die Grundlage dafür, wie Sie Ihre Anstrengungen zur Bereitstellung eines geschäftlichen Mehrwerts priorisieren.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Hoch

### Implementierungsleitfaden

Verstehen Sie die geschäftlichen Anforderungen: Der geschäftliche Erfolg basiert auf gemeinsamen Zielen und der Kommunikation zwischen allen Stakeholdern, zu denen auch die Teams aus den Bereichen Geschäft, Entwicklung und Betrieb gehören.

Besprechen der geschäftlichen Ziele, Anforderungen und Prioritäten externer Kunden: Führen Sie wichtige Beteiligte zusammen, einschließlich Geschäfts-, Entwicklungs- und Betriebsteams, um die Ziele, Anforderungen und Prioritäten externer Kunden zu besprechen.. Dadurch wird sichergestellt, dass Sie mit der betrieblichen Unterstützung vertraut sind, die erforderlich ist, um die gewünschten Geschäfts- und Kundenergebnisse zu erzielen.

Schaffen Sie ein gemeinsames Verständnis: Sorgen Sie dafür, dass alle Beteiligten die Geschäftsfunktionen des Workloads und die Rollen der einzelnen Teams bei den Workload-spezifischen betrieblichen Abläufen kennen. Außerdem sollte bekannt sein, wie diese Faktoren die gemeinsamen Geschäftsziele mit internen und externen Kunden beeinflussen.

### Ressourcen

Zugehörige bewährte Methoden:

- [OPS11-BP03 Implementieren Sie Feedback-Schleifen](#)

OPS01-BP02 Evaluieren Sie die internen Kundenbedürfnisse

Binden Sie alle wichtigen Stakeholder ein, einschließlich Geschäfts-, Entwicklungs- und Betriebsteams, um zu bestimmen, welche Bereiche verstärkt auf die Bedürfnisse der internen

Kunden ausgerichtet werden müssen. Dadurch wird sichergestellt, dass Sie mit der betrieblichen Unterstützung vertraut sind, die erforderlich ist, um geschäftliche Ergebnisse zu erzielen.

Gewünschtes Ergebnis:

- Anhand Ihrer etablierten Prioritäten können Sie erkennen, an welchen Stellen die Verbesserungsbemühungen konzentriert werden sollten (z. B. Teamfähigkeiten entwickeln, die Workload-Leistung verbessern, Kosten senken, Runbooks automatisieren oder die Überwachung ausbauen).
- Wenn sich Anforderungen ändern, aktualisieren Sie Ihre Prioritäten entsprechend.

Typische Anti-Muster:

- Sie haben sich entschieden, die Zuweisung von IP-Adressen für Ihre Produktteams zu ändern, um die Netzwerkverwaltung zu vereinfachen. Dabei haben Sie jedoch nicht mit den Mitarbeitern gesprochen. Sie wissen also nicht, welche Auswirkungen diese Änderung auf Ihre Produktteams haben wird.
- Sie implementieren ein neues Entwicklungstool, haben aber Ihre internen Kunden nicht einbezogen, um herauszufinden, ob das Tool benötigt wird oder mit den Abläufen der Kunden kompatibel ist.
- Sie implementieren ein neues Überwachungssystem, haben aber Ihre internen Kunden nicht kontaktiert, um herauszufinden, ob spezifische Überwachungs- oder Berichtsanforderungen vorliegen, die berücksichtigt werden sollten.

Vorteile der Nutzung dieser bewährten Methode: Die Bewertung und das Verständnis interner Kundenbedürfnisse liefert die Grundlage dafür, wie Sie Ihre Anstrengungen zur Bereitstellung eines geschäftlichen Mehrwerts priorisieren.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Hoch

Implementierungsleitfaden

- Verstehen Sie die geschäftlichen Anforderungen: Der geschäftliche Erfolg basiert auf gemeinsamen Zielen und der Kommunikation zwischen allen Stakeholdern, zu denen auch die Teams aus den Bereichen Geschäft, Entwicklung und Betrieb gehören.
- Überprüfen Sie die geschäftlichen Ziele, Anforderungen und Prioritäten interner Kunden: Führen Sie wichtige Stakeholder zusammen, einschließlich Geschäfts-, Entwicklungs- und Betriebsteams,

um die Ziele, Anforderungen und Prioritäten interner Kunden zu besprechen. Dadurch wird sichergestellt, dass Sie mit der betrieblichen Unterstützung vertraut sind, die erforderlich ist, um die gewünschten Geschäfts- und Kundenergebnisse zu erzielen.

- Schaffen Sie ein gemeinsames Verständnis: Sorgen Sie dafür, dass alle Beteiligten die Geschäftsfunktionen des Workloads und die Rollen der einzelnen Teams bei den Workload-spezifischen betrieblichen Abläufen kennen. Außerdem sollte bekannt sein, wie diese Faktoren die gemeinsamen Geschäftsziele mit internen und externen Kunden beeinflussen.

## Ressourcen

Zugehörige bewährte Methoden:

- [OPS11-BP03 Implementieren Sie Feedback-Schleifen](#)

## OPS01-BP03 Bewertung der Governance-Anforderungen

Governance bezeichnet die Richtlinien, Regeln oder Rahmen, die ein Unternehmen nutzt, um die geschäftlichen Ziele zu erreichen. Die Governance-Anforderungen werden innerhalb Ihrer Organisation erstellt. Sie können sich darauf auswirken, welche Arten von Technologien Sie nutzen oder wie Sie Ihre Workload ausführen. Integrieren Sie die Governance-Anforderungen Ihrer Organisation in Ihren Workload. Konformität ist die Fähigkeit, nachzuweisen, dass Sie die Governance-Anforderungen implementiert haben.

Gewünschtes Ergebnis:

- Die Governance-Anforderungen werden in das Architekturdesign und den Betrieb Ihres Workloads integriert.
- Sie können nachweisen, dass Sie den Governance-Anforderungen nachkommen.
- Die Governance-Anforderungen werden regelmäßig überprüft und aktualisiert.

Typische Anti-Muster:

- Ihre Organisation verlangt Multi-Faktor-Authentifizierung für das Stammkonto. Sie haben diese Anforderung nicht implementiert und das Stammkonto wurde kompromittiert.
- Während des Entwurfs Ihres Workloads wählen Sie einen Instance-Typ, der nicht von der IT-Abteilung genehmigt wurde. Sie können Ihren Workload nicht starten und müssen ihn überarbeiten.

- Sie sind verpflichtet, über einen Plan für die Notfallwiederherstellung zu verfügen. Sie haben keinen solchen Plan erstellt und Ihr Workload ist von einem längeren Ausfall betroffen.
- Ihr Team möchte neue Instances verwenden, Ihre Governance-Anforderungen wurden jedoch nicht aktualisiert, sodass die Instances nicht zulässig sind.

Vorteile der Nutzung dieser bewährten Methode:

- Durch das Erfüllen der Governance-Anforderungen wird Ihr Workload auf die größeren Organisationsrichtlinien abgestimmt.
- Die Governance-Anforderungen spiegeln Branchenstandards und bewährte Methoden für Ihre Organisation wider.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Hoch

Implementierungsleitfaden

Ermitteln Sie Governance-Anforderungen, indem Sie mit Stakeholdern und Governance-Organisationen zusammenarbeiten. Integrieren Sie die Governance-Anforderungen in Ihren Workload. Seien Sie in der Lage, nachzuweisen, dass Sie den Governance-Anforderungen nachkommen.

Kundenbeispiel

Bei AnyCompany Retail arbeitet das Cloud-Operations-Team mit Stakeholdern im gesamten Unternehmen zusammen, um die Governance-Anforderungen zu entwickeln. Sie verbieten beispielsweise den SSH Zugriff auf EC2 Amazon-Instances. Wenn Teams Systemzugriff benötigen, müssen sie AWS Systems Manager Session Manager verwenden. Das Cloud-Operations-Team aktualisiert die Governance-Anforderungen regelmäßig, sobald neue Services verfügbar sind.

Implementierungsschritte

1. Identifizieren Sie die Stakeholder für Ihren Workload, einschließlich zentralisierter Teams.
2. Arbeiten Sie mit den Stakeholdern zusammen, um Governance-Anforderungen zu ermitteln.
3. Nachdem Sie eine Liste erstellt haben, ordnen Sie die Verbesserungspunkte entsprechend der Priorität und beginnen Sie damit, sie in Ihren Workload zu implementieren.
  - a. Verwenden Sie Dienste wie [AWS Config](#) die Erstellung governance-as-code und Überprüfung der Einhaltung von Governance-Anforderungen.

- b. Wenn Sie [AWS Organizations](#) verwenden, können Sie Governance-Anforderungen mithilfe von Service-Kontrollrichtlinien (Service Control Policies, SCP) implementieren.
4. Stellen Sie Unterlagen bereit, die die Implementierung bestätigen.

Aufwand für den Implementierungsplan: Mittel. Die Implementierung fehlender Governance-Anforderungen kann dazu führen, dass Sie Ihren Workload überarbeiten müssen.

Ressourcen

Zugehörige bewährte Methoden:

- [OPS01-BP04 Evaluieren Sie die Compliance-Anforderungen](#) – Compliance ist ähnlich wie Unternehmensführung, kommt jedoch von außerhalb des Unternehmens.

Zugehörige Dokumente:

- [AWS Leitfaden für Verwaltung und Governance zur Cloud-Umgebung](#)
- [Bewährte Methoden für Richtlinien zur AWS Organizations Servicesteuerung in einer Umgebung mit mehreren Konten](#)
- [Unternehmensführung in der AWS Cloud: Das richtige Gleichgewicht zwischen Agilität und Sicherheit](#)
- [Was sind Unternehmensführung, Risiko und Compliance \(GRC\)?](#)

Zugehörige Videos:

- [AWS Management und Unternehmensführung: Konfiguration, Compliance und Prüfung — AWS Online Tech Talks](#)
- [AWS re:INFORCE 2019: Governance für das Cloud-Zeitalter \(-R1\) DEM12](#)
- [AWS re:Invent 2020: Konformität als Code erreichen mit AWS Config](#)
- [AWS re:Invent 2020: Agile Unternehmensführung auf AWS GovCloud \(US\)](#)

Zugehörige Beispiele:

- [AWS Config Beispiele für das Konformitätspaket](#)

## Zugehörige Services:

- [AWS Config](#)
- [AWS Organizations - Richtlinien zur Servicekontrolle](#)

## OPS01-BP04 Evaluieren Sie die Compliance-Anforderungen

Regulatorische, branchenspezifische und interne Compliance-Anforderungen sind ein wichtiger Faktor, wenn Sie die Prioritäten Ihrer Organisation definieren. Ihr Compliance-Regelwerk hindert Sie möglicherweise daran, spezifische Technologien oder geografische Standorte zu nutzen. Wenden Sie die erforderliche Sorgfalt an, wenn keine externen Compliance-Regelwerke identifiziert sind. Erstellen Sie Audits oder Berichte, die die Compliance bestätigen.

Wenn Sie damit werben, dass Ihr Produkt bestimmte Compliance-Standards erfüllt, benötigen Sie einen internen Prozess zur kontinuierlichen Gewährleistung der Compliance. Zu den Compliance-Standards gehören beispielsweise PCI DSS, AMP, Fed und HIPAA. Die geltenden Compliance-Standards werden durch verschiedene Faktoren bestimmt, beispielsweise dadurch, welche Datentypen von der Lösung gespeichert oder gesendet werden und welche geografischen Regionen die Lösung unterstützt.

## Gewünschtes Ergebnis:

- Die regulatorischen, branchenspezifischen und internen Compliance-Anforderungen werden bei der Auswahl der Architektur berücksichtigt.
- Sie können die Compliance bestätigen und Audit-Berichte erstellen.

## Typische Anti-Muster:

- Teile Ihres Workloads fallen unter das Payment Card Industry Data Security Standard (PCI-DSS) - Framework, aber Ihr Workload speichert Kreditkartendaten unverschlüsselt.
- Ihren Software-Entwicklern und -Architekten ist das Compliance-Regelwerk, das Ihre Organisation einhalten muss, nicht bekannt.
- Das jährliche System and Organizations Control (SOC2) Type II Audit findet bald statt, und Sie können nicht überprüfen, ob die Kontrollen vorhanden sind.

## Vorteile der Nutzung dieser bewährten Methode:

- Die Bewertung und das Verständnis der Compliance-Anforderungen für Ihren Workload liefern die Grundlage dafür, wie Sie Ihre Anstrengungen zur Bereitstellung eines geschäftlichen Mehrwerts priorisieren.
- Sie wählen die Ihrem Compliance-Regelwerk entsprechenden Standorte und Technologien.
- Indem Sie Ihren Workload so entwerfen, dass Überprüfungen möglich sind, können Sie leichter nachweisen, dass Sie das Compliance-Regelwerk einhalten.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Hoch

### Implementierungsleitfaden

Wenn Sie diese bewährte Methode implementieren, bedeutet dies, dass Sie Compliance-Anforderungen in den Entwurfsprozess für Ihre Architektur integrieren. Ihren Teammitgliedern ist das erforderliche Compliance-Regelwerk bekannt. Sie bestätigen Ihre Compliance mit diesem Regelwerk.

### Kundenbeispiel

AnyCompany Einzelhändler speichern Kreditkarteninformationen für Kunden. Die Entwickler des Kartenspeicher-Teams wissen, dass sie das PCI DSS -Framework einhalten müssen. Sie haben Schritte unternommen, um zu überprüfen, ob Kreditkarteninformationen gemäß dem PCI -DSS Framework sicher gespeichert und abgerufen werden. Jedes Jahr arbeiten sie mit dem Sicherheitsteam zusammen, um die Compliance zu bestätigen.

### Implementierungsschritte

1. Arbeiten Sie mit Ihrem Sicherheits- und Governance-Team zusammen, um zu ermitteln, welche branchenspezifischen, regulatorischen oder internen Compliance-Regelwerke Ihr Workload einhalten muss. Integrieren Sie die Compliance-Regelwerke in Ihren Workload.
  - a. Überprüfen Sie die kontinuierliche Konformität der AWS Ressourcen mit Diensten wie [AWS Compute Optimizer](#) und [AWS Security Hub](#).
2. Informieren Sie Ihre Teammitglieder über die Compliance-Anforderungen, damit diese den Workload in Übereinstimmung mit den Anforderungen betreiben und weiterentwickeln können. Die Compliance-Anforderungen sollten bei architektur- und technologiebezogenen Entscheidungen berücksichtigt werden.
3. Je nach Compliance-Regelwerk müssen Sie möglicherweise einen Audit- oder Compliance-Bericht erstellen. Arbeiten Sie mit Ihrer Organisation zusammen, um diesen Prozess so weit wie möglich zu automatisieren.



- a. Nutzen Sie Services wie [AWS Audit Manager](#), um die Compliance zu validieren und Auditberichte zu erstellen.
- b. Sie können AWS Sicherheits- und Compliance-Dokumente mit [AWS Artifact](#) herunterladen.

Aufwand für den Implementierungsplan: Mittel. Die Implementierung von Compliance-Regelwerken kann eine Herausforderung darstellen. Das Erstellen von Auditberichten oder Compliance-Dokumenten erfordert zusätzlichen Aufwand.

## Ressourcen

### Zugehörige bewährte Methoden:

- [SEC01-BP03 Identifizieren und validieren Sie Kontrollziele — Ziele](#) der Sicherheitskontrolle sind ein wichtiger Bestandteil der allgemeinen Einhaltung von Vorschriften.
- [SEC01-BP06 Automatisieren Sie das Testen und Validieren von Sicherheitskontrollen in Pipelines](#) — Validieren Sie Sicherheitskontrollen als Teil Ihrer Pipelines. Sie können auch eine Compliance-Dokumentation für neue Änderungen erstellen.
- [SEC07-BP02 Definieren Sie Datenschutzkontrollen — Viele Compliance-Frameworks basieren auf Datenverarbeitungen](#) - und Speicherrichtlinien.
- [SEC10-BP03 Vorbereitung forensischer Funktionen — Forensische Funktionen können manchmal bei der Prüfung der Einhaltung von Vorschriften eingesetzt werden.](#)

### Zugehörige Dokumente:

- [AWS Compliance-Zentrum](#)
- [AWS Ressourcen zur Einhaltung von Vorschriften](#)
- [AWS Whitepaper zu Risiko und Compliance](#)
- [AWS Modell der geteilten Verantwortung](#)
- [AWS Dienstleistungen im Rahmen von Compliance-Programmen](#)

### Zugehörige Videos:

- [AWS re:Invent 2020: Konformität als Code erreichen mit AWS Compute Optimizer](#)
- [AWS re:Invent 2021 — Cloud-Compliance, Sicherheit und Prüfung](#)

- [AWS Summit ATL 2022 — Umsetzung von Compliance, Sicherheit und Prüfung am AWS \(02\) COP2](#)

Zugehörige Beispiele:

- [PCIDSSund bewährte AWS grundlegende Sicherheitsverfahren zu AWS](#)

Zugehörige Services:

- [AWS Artifact](#)
- [AWS Audit Manager](#)
- [AWS Compute Optimizer](#)
- [AWS Security Hub](#)

OPS01-BP05 Bewerten Sie die Bedrohungslandschaft

Bewerten Sie Bedrohungen für das Unternehmen (z. B. Wettbewerb, Geschäftsrisiken und -verpflichtungen, operative Risiken und Bedrohungen der Informationssicherheit) und pflegen Sie aktuelle Informationen in einem Risikoregister. Berücksichtigen Sie die Auswirkungen von Risiken, wenn Sie bestimmen, auf welche Bereiche die Anstrengungen fokussiert werden sollen.

Das [Well-Architected Framework](#) legt den Schwerpunkt auf Lernen, Messen und Verbessern. Es bietet Ihnen einen konsistenten Ansatz zur Bewertung von Architekturen und zur Implementierung von Designs, die sich im Laufe der Zeit skalieren lassen. AWS bietet die [AWS Well-Architected Tool](#)Möglichkeit, Ihren Ansatz vor der Entwicklung, den Status Ihrer Workloads vor der Produktion und den Status Ihrer Workloads in der Produktion zu überprüfen. Sie können sie mit den neuesten bewährten AWS Architekturpraktiken vergleichen, den Gesamtstatus Ihrer Workloads überwachen und Einblicke in potenzielle Risiken gewinnen.

AWS Kunden haben Anspruch auf eine geführte Well-Architected-Überprüfung ihrer unternehmenskritischen Workloads, um ihre Architekturen anhand von Best Practices [zu](#) bewerten. AWS Für Kunden mit Enterprise Support wird eine [Betriebsüberprüfung \(Operations Review\)](#) angeboten. Damit haben sie die Möglichkeit, Lücken in ihrem Cloud-Ansatz aufzuzeigen.

Aufgrund der teamübergreifenden Natur dieser Überprüfungen erhalten Sie ein allgemeines Verständnis Ihrer Workloads und können erkennen, wie Team-Rollen zum Erfolg beitragen. Die bei den Überprüfungen gefundenen Punkte können Ihnen beim Festlegen Ihrer Prioritäten helfen.

[AWS Trusted Advisor](#) bietet als Tool Zugriff auf verschiedene wichtige Prüfungen, die Optimierungsempfehlungen ausgeben. Diese Informationen können Ihnen beim Festlegen Ihrer Prioritäten helfen. [Kunden mit Business und Enterprise Support](#) erhalten Zugriff auf weitere Prüfungen in den Bereichen Sicherheit, Zuverlässigkeit, Leistung und Kostenoptimierung, die beim Festlegen von Prioritäten noch hilfreicher sind.

Gewünschtes Ergebnis:

- Du überprüfst Well-Architected und die Ergebnisse regelmäßig und reagierst entsprechend Trusted Advisor
- Sie sind über den neuesten Patch-Status Ihrer Services informiert.
- Sie kennen das Risiko und die Auswirkungen bekannter Bedrohungen und handeln entsprechend.
- Sie implementieren bei Bedarf Abhilfemaßnahmen.
- Sie kommunizieren Aktionen und Kontext.

Typische Anti-Muster:

- Sie verwenden in Ihrem Produkt eine alte Version einer Softwarebibliothek. Ihnen ist nicht bewusst, dass für die Bibliothek Sicherheitsaktualisierungen vorliegen, mit denen Probleme behoben werden, die unbeabsichtigte Auswirkungen auf Ihren Workload haben können.
- Ein Mitbewerber hat soeben eine Version seines Produkts veröffentlicht, in der viele Probleme behoben werden, die Kunden an Ihrem Produkt bemängeln. Die Behebung dieser bekannten Probleme hatte für Sie bisher keine Priorität.
- Regulierungsbehörden nehmen Unternehmen wie Ihres, die nicht den gesetzlichen Compliance-Anforderungen entsprechen, verstärkt ins Visier. Sie haben Ihre ausstehenden Compliance-Anforderungen nicht priorisiert.

Vorteile der Nutzung dieser bewährten Methode: Sie identifizieren und verstehen die Bedrohungen für Ihr Unternehmen und Ihren Workload und können daher besser bestimmen, welche Bedrohungen angegangen werden müssen, wo die Prioritäten liegen und welche Ressourcen dafür erforderlich sind.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel

## Implementierungsleitfaden

- Bewerten der Bedrohungsszenarien: Bewerten Sie Bedrohungen für das Unternehmen (z. B. Konkurrenz, Geschäftsrisiken und -verpflichtungen, operative Risiken und Bedrohungen der Informationssicherheit), damit Sie die jeweiligen Auswirkungen berücksichtigen können, wenn Sie bestimmen, auf welche Bereiche die operativen Anstrengungen konzentriert werden sollten.
  - [Aktuelle AWS -Sicherheitsmitteilungen](#)
  - [AWS Trusted Advisor](#)
- Verwalten eines Bedrohungsmodells: Erstellen und verwalten Sie ein Bedrohungsmodell, in dem potenzielle Bedrohungen, geplante und vorhandene Maßnahmen und deren Priorität festgehalten werden. Untersuchen Sie, wie wahrscheinlich es ist, dass sich Bedrohungen als Vorfälle äußern, wie hoch die Kosten für die Wiederherstellung nach diesen Vorfällen sind, welche Schäden zu erwarten sind und wie viel es kostet, diese Vorfälle zu verhindern. Überarbeiten Sie die Prioritäten, wenn sich der Inhalt des Bedrohungsmodells ändert.

## Ressourcen

### Zugehörige bewährte Methode:

- [SEC01-BP07 Identifizieren Sie Bedrohungen und priorisieren Sie Abhilfemaßnahmen mithilfe eines Bedrohungsmodells](#)

### Zugehörige Dokumente:

- [AWS Cloud -Compliance](#)
- [Aktuelle AWS -Sicherheitsmitteilungen](#)
- [AWS Trusted Advisor](#)

### Zugehörige Videos:

- [AWS re:Inforce 2023 – Tool für eine bessere Bedrohungsmodellierung](#)

OPS01-BP06 Bewerten Sie Kompromisse und managen Sie gleichzeitig Vorteile und Risiken

Konkurrierende Interessen mehrerer Parteien können eine Herausforderung darstellen, wenn es darum geht, Anstrengungen zu priorisieren, Fähigkeiten aufzubauen und Ergebnisse zu erzielen,

die auf die Geschäftsstrategien abgestimmt sind. Beispielsweise werden Sie möglicherweise aufgefordert, die Einführung neuer Funktionen zu beschleunigen, anstatt die Kosten speed-to-market für die IT-Infrastruktur zu optimieren. Dies kann dazu führen, dass die Interessen zweier Parteien miteinander in Widerspruch stehen. In solchen Situationen muss eine höhere Stelle hinzugezogen werden, um eine Entscheidung zur Lösung des Konflikts zu treffen. Daten sind erforderlich, um den Entscheidungsprozess von emotionalen Komponenten zu befreien.

Ähnliche Herausforderungen können auf taktischer Ebene auftreten. Beispielsweise kann die Wahl zwischen relationalen oder nicht relationalen Datenbanktechnologien erhebliche Auswirkungen auf den Betrieb einer Anwendung haben. Daher ist es wichtig, die voraussichtlichen Ergebnisse verschiedener Entscheidungen zu verstehen.

AWS kann Ihnen helfen, Ihre Teams über die Services AWS und Services zu informieren, damit sie besser verstehen, wie sich ihre Entscheidungen auf Ihre Arbeitslast auswirken können. Nutzen Sie bei der Schulung Ihrer Teams die vom [AWS Support](#) ([AWS Knowledge Center](#), [AWS - Diskussionsforen](#) und [AWS Support Center](#)) bereitgestellten Ressourcen und [AWS -Dokumente](#). Bei weiteren Fragen wenden Sie sich an AWS Support.

AWS teilt auch bewährte Verfahren und Muster für den Betrieb in [der Amazon Builders' Library](#). Eine Vielzahl weiterer nützlicher Informationen ist im [AWS Blog](#) und im [offiziellen AWS](#) Podcast verfügbar.

Gewünschtes Ergebnis: Sie verfügen über ein klar definiertes Governance-Framework zur Entscheidungsfindung, um wichtige Entscheidungen auf jeder Ebene in Ihrem Cloud-Bereitstellungsunternehmen zu erleichtern. Dieses Framework umfasst Features wie ein Risikoregister, definierte Rollen mit Entscheidungsbefugnissen und definierte Modelle für die einzelnen Entscheidungsebenen. Dieses Framework legt im Voraus fest, wie Konflikte gelöst werden, welche Daten präsentiert werden müssen und wie Optionen priorisiert werden, sodass Sie einmal gefasste Beschlüsse sofort umsetzen können. Das Framework zur Entscheidungsfindung beinhaltet einen standardisierten Ansatz zur Überprüfung und Abwägung der Vorteile und Risiken einzelner Entscheidungen, um die Tragweite etwaiger Kompromisse abzuschätzen. Dazu können externe Faktoren gehören wie die Einhaltung gesetzlicher Vorschriften.

Typische Anti-Muster:

- Ihre Anleger verlangen von Ihnen den Nachweis, dass Sie die Datensicherheitsstandards der Zahlungskartenbranche einhalten (PCIDSS). Sie denken nicht über einen möglichen Kompromiss zwischen der Erfüllung dieser Anfrage und der Fortsetzung Ihrer derzeitigen Entwicklungsaktivitäten nach. Stattdessen fahren Sie mit der Entwicklung fort, ohne einen Compliance-Nachweis zu erbringen. Ihre Investoren beenden die Unterstützung Ihres

Unternehmens, da sie Bedenken bezüglich der Sicherheit Ihrer Plattform und ihrer Investitionen haben.

- Sie haben sich entschieden, eine Bibliothek einzubinden, die einer Ihrer Entwickler „im Internet entdeckt“ hat. Sie haben keine Bewertung der Risiken durchgeführt, die die Einführung dieser Bibliothek aus einer unbekanntem Quelle bergen kann, und wissen nicht, ob sie Schwachstellen oder schädlichen Code enthält.
- Die ursprüngliche geschäftliche Begründung für Ihre Migration basierte auf der Modernisierung von 60 % Ihrer Anwendungsworkloads. Aufgrund technischer Schwierigkeiten wurde jedoch beschlossen, nur 20 % zu modernisieren. Dies führte langfristig zu einer Reduzierung der geplanten Leistungen, zu einem erhöhten Aufwand für die Infrastrukturteams bei der manuellen Wartung von Legacy-Systemen und zu einer stärkeren Abhängigkeit von der Entwicklung neuer Fähigkeiten in Ihren Infrastrukturteams, die diese Änderung nicht geplant hatten.

Vorteile der Nutzung dieser bewährten Methode: Vollständige Abstimmung und Unterstützung der Geschäftsprioritäten auf Vorstandsebene, Verständnis der Erfolgsrisiken, Treffen fundierter Entscheidungen und angemessenes Handeln, wenn Risiken die Erfolgchancen beeinträchtigen. Indem Sie die Auswirkungen und Konsequenzen Ihrer Entscheidungen verstehen, können Sie Ihre Optionen priorisieren und Führungskräfte schneller zu einer Einigung bringen, was zu besseren Geschäftsergebnissen führt. Wenn Sie die Vorteile Ihrer Entscheidungen erkennen und sich der Risiken für Ihre Organisation bewusst sind, können Sie datengestützte Entscheidungen treffen, anstatt sich auf Anekdoten verlassen zu müssen.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel

### Implementierungsleitfaden

Die Abwägung von Nutzen und Risiken sollte von einem Leitungsorgan übernommen werden, das die Anforderungen für wichtige Entscheidungen festlegt. Sie möchten, dass Entscheidungen basierend auf ihrem Nutzen für die Organisation getroffen und priorisiert werden und die damit verbundenen Risiken bekannt sind. Präzise Informationen bilden die Grundlage für die Entscheidungen Ihrer Organisation. Diese sollten auf soliden Messungen beruhen und durch branchenübliche Verfahren der Kosten-Nutzen-Analyse definiert werden. Damit Entscheidungen auf diese Art getroffen werden können, müssen Sie ein Gleichgewicht zwischen zentralisierter und dezentralisierter Autorität herstellen. Es gibt immer einen Kompromiss. Daher ist es wichtig zu verstehen, wie sich jede Entscheidung auf definierte Strategien und angestrebte Geschäftsergebnisse auswirkt.

## Implementierungsschritte

1. Formalisieren Sie die Verfahren zur Leistungsmessung innerhalb eines ganzheitlichen Cloud-Governance-Frameworks.
  - a. Bringen Sie die zentrale Kontrolle der Entscheidungsfindung in Einklang mit konkreten dezentralen Entscheidungsbefugnissen.
  - b. Machen Sie sich bewusst, dass nicht für jeden Beschluss aufwendige Entscheidungsprozesse vonnöten sind, da sie Sie verlangsamen können.
  - c. Integrieren Sie externe Faktoren in Ihren Entscheidungsprozess (wie Compliance-Anforderungen).
2. Richten Sie ein gemeinsames Framework zur Entscheidungsfindung für verschiedene Entscheidungsebenen ein, in dem festgelegt ist, wer Entscheidungen bei widersprüchlichen Interessen trifft.
  - a. Zentralisieren Sie einseitige Entscheidungen, die irreversibel sein könnten.
  - b. Lassen Sie leicht revidierbare Entscheidungen von Führungskräften auf niedrigerer Ebene treffen.
3. Machen Sie sich mit den Nutzen und Risiken vertraut und wägen Sie sie ab. Wägen Sie den Nutzen von Entscheidungen gegen die damit einhergehenden Risiken ab.
  - a. Ermitteln von Vorteilen: Ermitteln Sie die Vorteile auf Basis der geschäftlichen Ziele, Anforderungen und Prioritäten. Beispiele hierfür sind Auswirkungen auf Geschäftsszenarien time-to-market, Sicherheit, Zuverlässigkeit, Leistung und Kosten.
  - b. Ermitteln von Risiken: Ermitteln Sie die Risiken auf Basis der geschäftlichen Ziele, Anforderungen und Prioritäten. Zu den Beispielen gehören Sicherheit time-to-market, Zuverlässigkeit, Leistung und Kosten.
  - c. Abwägen von Vorteilen und Risiken und Treffen fundierter Entscheidungen: Bestimmen Sie die Auswirkungen von Vorteilen und Risiken anhand der Ziele, Anforderungen und Prioritäten der wichtigsten Beteiligten, zu denen auch Geschäfts-, Entwicklungs- und Betriebsteams zählen. Bewerten Sie den Wert eines Vorteils anhand der Wahrscheinlichkeit, dass sich das Risiko tatsächlich bewahrheitet, sowie der Kosten der jeweiligen Auswirkungen. Wenn beispielsweise der Schwerpunkt auf Zuverlässigkeit gelegt speed-to-market wird, kann dies einen Wettbewerbsvorteil bieten. Wenn jedoch Probleme mit der Zuverlässigkeit auftreten, kann dies zu einer verringerten Betriebszeit führen.
4. Setzen Sie wichtige Entscheidungen programmatisch um, um die Einhaltung von Compliance-Anforderungen zu automatisieren.

5. Nutzen Sie bekannte branchenübliche Frameworks und Funktionen wie die Wertstromanalyse LEAN, um die aktuelle Leistung und Geschäftskennzahlen als Ausgangsbasis zu ermitteln und Iterationen der Fortschritte bei der Verbesserung dieser Kennzahlen zu definieren.

Aufwand für den Implementierungsplan: Mittel-Hoch

Ressourcen

Zugehörige bewährte Methoden:

- [OPS01-BP05 Bewerten Sie die Bedrohungslandschaft](#)

Zugehörige Dokumente:

- [Elemente der Day-1-Kultur von Amazon | Hochwertige und schnelle Entscheidungen treffen](#)
- [Cloud-Governance](#)
- [Verwaltungs- und Governance-Cloud-Umgebung](#)
- [Governance in der Cloud und im digitalen Zeitalter: Teil eins und Teil zwei](#)

Zugehörige Videos:

- [Podcast | Jeff Bezos | So trifft man Entscheidungen](#)

Zugehörige Beispiele:

- [Treffen Sie fundierte Entscheidungen anhand von Daten \(The DevOps Sagas\)](#)
- [Mithilfe der Abbildung von Wertströmen aus der Entwicklung zur Identifizierung von Ergebniseinschränkungen DevOps](#)

OPS2. Wie strukturieren Sie Ihr Unternehmen, um die gewünschten Geschäftsergebnisse zu erzielen?

Ihre Teams müssen ihre Rolle beim Erreichen von Geschäftsergebnissen verstehen. Teams sollten ihre Rolle für den Erfolg anderer Teams und die Rolle anderer Teams für ihren Erfolg verstehen und gemeinsame Ziele haben. Indem sie die Konzepte Verantwortlichkeit und Zuständigkeit



verstehen und wissen, wie Entscheidung getroffen werden und wer dazu berechtigt ist, können ihre Anstrengungen fokussiert und der Nutzen Ihrer Teams maximiert werden.

### Bewährte Methoden

- [OPS02-BP01 Ressourcen haben Eigentümer identifiziert](#)
- [OPS02-BP02 Prozesse und Verfahren haben Eigentümer identifiziert](#)
- [OPS02-BP03 Bei den operativen Aktivitäten wurden Eigentümer identifiziert, die für ihre Leistung verantwortlich sind](#)
- [OPS02-BP04 Es gibt Mechanismen zur Verwaltung von Verantwortlichkeiten und Eigenverantwortung](#)
- [OPS02-BP05 Es gibt Mechanismen, um Ergänzungen, Änderungen und Ausnahmen zu beantragen](#)
- [OPS02-BP06 Verantwortlichkeiten zwischen Teams sind vordefiniert oder ausgehandelt](#)

### OPS02-BP01 Ressourcen haben Eigentümer identifiziert

Die Ressourcen für Ihren Workload müssen für die Änderungskontrolle, die Fehlerbehebung und andere Funktionen feste Verantwortliche haben. Verantwortliche werden für Workloads, Konten, Infrastruktur, Plattformen und Anwendungen zugewiesen. Die Verantwortlichkeit wird mit Tools wie einem Zentralverzeichnis oder Metadaten zu Ressourcen erfasst. Der Unternehmenswert der Komponenten bestimmt, welche Prozesse und Verfahren auf diese angewendet werden.

### Gewünschtes Ergebnis:

- Mithilfe von Metadaten oder einem Zentralverzeichnis werden feste Verantwortliche für die Ressourcen identifiziert.
- Die Teammitglieder können erkennen, wer für eine bestimmte Ressource verantwortlich ist.
- Konten haben wenn möglich einen festen Verantwortlichen.

### Typische Anti-Muster:

- Die alternativen Kontakte für Sie AWS-Konten sind nicht eingetragen.
- Die Ressourcen sind nicht mit Tags markiert, die kennzeichnen, wer dafür verantwortlich ist.
- Sie haben eine ITSM Warteschlange ohne E-Mail-Zuordnung.
- Zwei Teams haben sich überschneidende Verantwortlichkeit für einen wichtigen Teil der Infrastruktur.

Vorteile der Nutzung dieser bewährten Methode:

- Dank der zugewiesenen Verantwortlichkeit ist die Änderungskontrolle ganz einfach.
- Wenn Probleme auftreten, können die richtigen Verantwortlichen einbezogen werden.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Hoch

### Implementierungsleitfaden

Definieren Sie, was Verantwortlichkeit für die Ressourcen-Anwendungsfälle in Ihrer Umgebung bedeutet. Verantwortlichkeit kann bedeuten, Änderungen an der Ressource zu beaufsichtigen, die Ressource während der Fehlerbehebung zu unterstützen oder die finanzielle Verantwortung zu tragen. Legen Sie Verantwortliche für Ressourcen fest und dokumentieren Sie diese. Die Angaben sollten den Namen, die Kontaktinformationen, die Organisation und das Team beinhalten.

### Kundenbeispiel

AnyCompany Der Einzelhandel definiert Eigenverantwortung als das Team oder die Einzelperson, die für Änderungen verantwortlich ist und Ressourcen unterstützt. Sie nutzen AWS Organizations , um ihre zu verwalten AWS-Konten. Die alternativen Kontakte für die Konten werden mit Gruppenpostfächern konfiguriert. Jede ITSM Warteschlange ist einem E-Mail-Alias zugeordnet. Mithilfe von Tags wird angegeben, wem AWS Ressourcen gehören. Für andere Plattformen und Infrastruktur gibt es eine Wiki-Seite, auf der die Verantwortlichkeiten und die Kontaktinformationen angegeben sind.

### Implementierungsschritte

1. Beginnen Sie damit, die Verantwortlichkeiten für Ihre Organisation zu definieren. Verantwortlichkeit kann bedeuten, wer für das Risiko für die Ressource oder für Änderungen an der Ressource verantwortlich ist oder wer die Ressource im Fall einer Fehlerbehebung unterstützt. Verantwortlichkeit kann auch die finanzielle oder administrative Verantwortlichkeit für die Ressource umfassen.
2. Nutzen Sie [AWS Organizations](#) zur Verwaltung von Konten. Sie können die alternativen Kontakte für Ihre Konten zentral verwalten.
  - a. Durch die Verwendung von E-Mail-Adressen und Telefonnummern des Unternehmens als Kontaktdaten können Sie auch dann auf sie zugreifen, wenn die Personen, zu denen sie gehören, nicht mehr Teil Ihrer Organisation sind. Erstellen Sie beispielsweise separate E-Mail-Verteilerlisten für die Abrechnung, die Produktion und die Sicherheit und konfigurieren Sie sie

- in jedem aktiven AWS-Konto als Abrechnungs-, Sicherheits- und Produktionskontakte. Mehrere Personen erhalten AWS Benachrichtigungen und können antworten, auch wenn jemand im Urlaub ist, die Rolle wechselt oder das Unternehmen verlässt.
- b. Wenn ein Konto nicht von [AWS Organizations](#) verwaltet wird, helfen alternative Kontaktkontakte AWS dabei, bei Bedarf Kontakt mit den entsprechenden Personen aufzunehmen. Konfigurieren Sie die alternativen Kontakte für ein Konto so, dass sie auf eine Gruppe verweisen, und nicht auf eine Einzelperson.
3. Verwenden Sie Tags, um Eigentümer von AWS Ressourcen zu identifizieren. Sie können die Verantwortlichen und ihre Kontaktdaten in verschiedenen Tags angeben.
    - a. Sie können [AWS Config](#)-Regeln verwenden, um durchzusetzen, dass Ressourcen über die erforderlichen Eigentümerkennungen verfügen.
    - b. Ausführliche Anleitungen zur Entwicklung einer Tagging-Strategie für Ihr Unternehmen finden Sie im [Whitepaper „Bewährte AWS -Tagging-Methoden“](#).
  4. Verwenden Sie [Amazon Q Business](#), einen Konversationsassistenten, der auf generativer KI basiert, um die Produktivität Ihrer Mitarbeiter zu steigern, Fragen zu beantworten und Aufgaben auf der Grundlage von Informationen in Ihren Unternehmenssystemen zu erledigen.
    - a. Verbinden Sie Amazon Q Business mit der Datenquelle Ihres Unternehmens. Amazon Q Business bietet vorgefertigte Konnektoren für über 40 unterstützte Datenquellen, darunter Amazon Simple Storage Service (Amazon S3), Microsoft SharePoint, Salesforce und Atlassian Confluence. Weitere Informationen finden Sie unter [Amazon Q Business-Konnektoren](#).
  5. Erstellen Sie für andere Ressourcen, Plattformen und Infrastruktur eine Dokumentation mit Informationen zur jeweiligen Verantwortlichkeit. Diese sollte für alle Teammitglieder zugänglich sein.

Aufwand für den Implementierungsplan: Niedrig. Nutzen Sie Kontaktkontaktinformationen und Tags, um die Inhaberschaft von Ressourcen zuzuweisen. AWS Für andere Ressourcen können Sie etwas so Einfaches wie eine Tabelle in einem Wiki verwenden, um Eigentums- und Kontaktinformationen aufzuzeichnen, oder ein ITSM Tool verwenden, um die Eigentumsverhältnisse zuzuordnen.

## Ressourcen

Zugehörige bewährte Methoden:

- [OPS02-BP02 Für Prozesse und Verfahren wurden die Verantwortlichen identifiziert](#)
- [OPS02-BP04 Es gibt Mechanismen zur Verwaltung von Verantwortlichkeiten und Eigenverantwortung](#)

## Zugehörige Dokumente:

- [AWS -Kontoverwaltung – Aktualisieren der Kontaktinformationen](#)
- [AWS Organizations - Aktualisierung alternativer Ansprechpartner in Ihrer Organisation](#)
- [Bewährte AWS -Tagging-Methoden \(Whitepaper\)](#)
- [Entwickeln Sie private und sichere generative KI-Apps für Unternehmen mit Amazon Q Business and AWS IAM Identity Center](#)
- [Amazon Q Business \(jetzt allgemein verfügbar\) ermöglicht die Steigerung der Produktivität der Mitarbeiter mithilfe von generativer KI](#)
- [AWS Cloud Operations & Migrations Blog — Implementierung automatisierter und zentralisierter Tagging-Steuerungen mit und AWS Config](#)
- [AWS Organizations](#)
- [AWS Sicherheitsblog — Erweitern Sie Ihre Pre-Commit-Hooks mit AWS CloudFormation Guard](#)
- [AWS DevOps Blog — Integration AWS CloudFormation Guard in CI/CD-Pipelines](#)

## Zugehörige Workshops:

- [AWS -Workshop – Tagging](#)

## Zugehörige Beispiele:

- [AWS-Config-Regeln - Amazon EC2 mit den erforderlichen Tags und gültigen Werten](#)

## Zugehörige Services:

- [AWS-Config-Regeln - erforderliche Tags](#)
- [AWS Organizations](#)

OPS02-BP02 Prozesse und Verfahren haben Eigentümer identifiziert

Verschaffen Sie sich einen Überblick darüber, wer für die Definition einzelner Prozesse und Verfahren zuständig ist, warum diese spezifischen Prozesse und Verfahren verwendet werden und warum diese Zuständigkeit besteht. Wenn Sie wissen, warum bestimmte Prozesse und Verfahren verwendet werden, können Sie Verbesserungsmöglichkeiten identifizieren.

Gewünschtes Ergebnis: Ihre Organisation verfügt über gut definierte und verwaltete Prozesse und Verfahren für betriebliche Aufgaben. Der Prozess und die Verfahren werden an einem zentralen

Ort gespeichert und stehen Ihren Teammitgliedern zur Verfügung. Prozesse und Verfahren werden regelmäßig aktualisiert, wobei die Zuständigkeit eindeutig zugewiesen wird. Wo möglich, werden Skripte, Vorlagen und Automatisierungsdokumente als Code implementiert.

Typische Anti-Muster:

- Prozesse sind nicht dokumentiert. Es können fragmentierte Skripte auf isolierten Bedienerarbeitsplätzen existieren.
- Das Wissen über den Umgang mit Skripten wird von wenigen Personen oder informell als Teamwissen vermittelt.
- Ein veralteter Prozess muss aktualisiert werden, aber die Zuständigkeit für die Aktualisierung ist unklar, und der ursprüngliche Autor gehört nicht mehr zur Organisation.
- Prozesse und Skripte sind nicht auffindbar und daher nicht sofort verfügbar, wenn sie benötigt werden (z. B. als Reaktion auf einen Vorfall).

Vorteile der Nutzung dieser bewährten Methode:

- Prozesse und Verfahren unterstützen Sie bei der Bewältigung Ihrer Workloads.
- Neue Teammitglieder werden schneller handlungsfähig.
- Die Zeit bis zur Behebung von Vorfällen wird reduziert.
- Verschiedene Teammitglieder (und Teams) können dieselben Prozesse und Verfahren auf einheitliche Weise verwenden.
- Teams können ihre Prozesse durch wiederholbare Prozesse skalieren.
- Standardisierte Prozesse und Verfahren tragen dazu bei, die Auswirkungen der Übertragung von Workload-Verantwortlichkeiten zwischen Teams abzumildern.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Hoch

Implementierungsleitfaden

- Prozesse und Verfahren haben feste Besitzer, die für ihre Definition verantwortlich sind.
  - Identifizieren Sie die Betriebsaktivitäten, die zur Unterstützung Ihrer Workloads durchgeführt werden. Dokumentieren Sie diese Aktivitäten an einem auffindbaren Ort.
  - Legen Sie die Person oder Personen fest, die für die Spezifikation einer Aktivität verantwortlich sind. Sie sind dafür verantwortlich, sicherzustellen, dass die Aktivität von einem ausreichend

qualifizierten Teammitglied durchgeführt wird, das die entsprechenden Berechtigungen, Zugriffsrechte und Tools hat. Wenn bei der Durchführung dieser Aktivität Probleme auftreten, sind die zuständigen Teammitglieder dafür verantwortlich, detailliertes Feedback bereitzustellen, das für die Verbesserung der Aktivität erforderlich ist.

- Erfassen Sie die Eigentumsrechte an den Metadaten des Aktivitätsartefakts mithilfe von Diensten wie AWS Systems Manager, Dokumenten und AWS Lambda. Erfassen Sie die Ressourcenzuständigkeit mithilfe von Tags oder Ressourcengruppen und geben Sie Zuständigkeits- und Kontaktinformationen an. Wird verwendet AWS Organizations, um Tagging-Richtlinien zu erstellen und Eigentums- und Kontaktinformationen zu erfassen.
- Mit der Zeit sollten diese Verfahren so weiterentwickelt werden, dass sie als Code ausgeführt werden können, sodass weniger menschliche Eingriffe erforderlich sind.
  - Denken Sie beispielsweise an AWS Lambda Funktionen, CloudFormation Vorlagen oder AWS Systems Manager Manager-Automatisierungsdokumente.
  - Führen Sie die Versionskontrolle in den entsprechenden Repositories durch.
  - Fügen Sie geeignetes Ressourcen-Tagging hinzu, damit Eigentümer und Dokumentation leicht identifiziert werden können.

## Kundenbeispiel

AnyCompany Im Einzelhandel wird Eigentum als das Team oder die Einzelperson definiert, dem die Prozesse für eine Anwendung oder Anwendungsgruppen (die gemeinsame architektonische Praktiken und Technologien aufweisen) gehören. Anfänglich werden der Prozess und die Verfahren in Form von step-by-step Anleitungen im Dokumentenverwaltungssystem dokumentiert, die anhand von Tags auf dem Host der AWS-Konto Anwendung und auf bestimmten Ressourcengruppen innerhalb des Kontos auffindbar sind. Sie nutzen AWS Organizations, um ihre zu verwalten. AWS-Konten Im Laufe der Zeit werden diese Prozesse in Code umgewandelt, und Ressourcen werden mithilfe von Infrastructure-as-Code (z. CloudFormation B. AWS Cloud Development Kit (AWS CDK) Vorlagen) definiert. Die betrieblichen Prozesse werden zu Automatisierungsdokumenten in AWS Systems Manager oder AWS Lambda Funktionen, die als geplante Aufgaben als Reaktion auf Ereignisse wie AWS CloudWatch Alarme oder AWS EventBridge Ereignisse initiiert oder durch Anfragen innerhalb einer IT-Service-Management-Plattform (ITSM) gestartet werden können. Alle Prozesse sind mit Tags versehen, um die Zuständigkeit zu identifizieren. Die Dokumentation für die Automatisierung und den Prozess wird auf den Wiki-Seiten verwaltet, die vom Code-Repository für den Prozess generiert werden.

## Implementierungsschritte

1. Dokumentieren Sie die bestehenden Prozesse und Verfahren.
  - a. Überprüfe sie und behalte sie up-to-date.
  - b. Identifizieren Sie einen Besitzer für jeden Prozess und jede Prozedur.
  - c. Stellen Sie sie unter Versionskontrolle.
  - d. Wenn möglich, nutzen Sie Prozesse und Verfahren für Workloads und Umgebungen mit gemeinsamen Architekturentwürfen.
2. Richten Sie Mechanismen für Feedback und Verbesserung ein.
  - a. Definieren Sie Richtlinien dafür, wie oft Prozesse überprüft werden sollten.
  - b. Definieren Sie Prozesse für Prüfende und Genehmigende.
  - c. Implementieren Sie Probleme oder eine Ticket-Warteschlange, um Feedback zu geben und zu verfolgen.
  - d. Wo immer möglich, sollten Prozesse und Verfahren vorab von einem Change Approval Board genehmigt und nach Risiken eingestuft werden (CAB).
3. Stellen Sie sicher, dass Prozesse und Verfahren für diejenigen, die sie ausführen müssen, zugänglich und auffindbar sind.
  - a. Verwenden Sie Tags, um anzugeben, wo der Prozess und die Verfahren für die Workload aufgerufen werden können.
  - b. Verwenden Sie aussagekräftige Fehler- und Ereignismeldungen, um die geeigneten Prozesse oder Verfahren zur Behebung eines Problems anzugeben.
  - c. Verwenden Sie Wikis und Dokumentenmanagement und machen Sie Prozesse und Verfahren organisationsweit durchsuchbar.
4. Automatisieren Sie gegebenenfalls.
  - a. Automatisierungen sollten entwickelt werden, wenn Dienste und Technologien dies ermöglichen. API
  - b. Informieren Sie sich angemessen über Prozesse. Entwickeln Sie die Benutzerszenarien und Anforderungen, um diese Prozesse zu automatisieren.
  - c. Messen Sie die erfolgreiche Nutzung Ihrer Prozesse und Verfahren und geben Sie dabei Probleme an, die eine iterative Verbesserung unterstützen.

Aufwand für den Implementierungsplan: Mittel

## Ressourcen

### Zugehörige bewährte Methoden:

- [OPS02-BP01 Ressourcen haben Eigentümer identifiziert](#)
- [OPS02-BP04 Es gibt Mechanismen zur Verwaltung von Verantwortlichkeiten und Eigenverantwortung](#)
- [OPS11-BP04 Führen Sie Wissensmanagement durch](#)

### Zugehörige Dokumente:

- [AWS Whitepaper — Einführung in DevOps AWS](#)
- [AWS Whitepaper — Bewährte Methoden für das Markieren von Ressourcen AWS](#)
- [AWS Whitepaper — Organisieren Sie Ihre AWS Umgebung mithilfe mehrerer Konten](#)
- [AWS Cloud Operations & Migrations Blog — Entwickeln Sie eine Cloud-Automatisierungspraxis für optimale betriebliche Abläufe: Bewährte Verfahren von AWS Managed Services](#)
- [AWS Cloud Operations & Migrations Blog — Implementierung automatisierter und zentraler Tagging-Steuererelemente mit und AWS ConfigAWS Organizations](#)
- [AWS Sicherheitsblog — Erweitern Sie Ihre Pre-Commit-Hooks mit AWS CloudFormation Guard](#)
- [AWS DevOps Blog — Integration AWS CloudFormation Guard in CI/CD-Pipelines](#)

### Zugehörige Workshops:

- [AWS Well-Architected-Workshop zur betrieblichen Exzellenz](#)
- [AWS -Workshop – Tagging](#)

### Zugehörige Videos:

- [Wie automatisiert man den IT-Betrieb auf AWS](#)
- [AWS re:Invent 2020 — Automatisieren Sie alles mit Systems Manager AWS](#)
- [AWS re:inForce 2022 — Automatisierung von Patch-Management und Compliance mithilfe von \(06\) AWS NIS3](#)
- [AWS Support s You — Tauchen Sie tief in AWS Systems Manager ein](#)

### Zugehörige Services:



- [AWS Systems Manager - Automatisierung](#)
- [AWS Service Management Connector](#)

OPS02-BP03 Bei den operativen Aktivitäten wurden Eigentümer identifiziert, die für ihre Leistung verantwortlich sind

Verschaffen Sie sich einen Überblick darüber, wer für spezifische Aktivitäten in festgelegten Workloads verantwortlich ist und warum diese Zuständigkeit besteht. Wenn Sie wissen, wer für die Durchführung von Aktivitäten verantwortlich ist, können Sie nachvollziehen, wer die Aktivität durchführen, das Ergebnis validieren und dem Besitzer der Aktivität Feedback geben wird.

Gewünschtes Ergebnis:

Ihre Organisation definiert klar die Verantwortlichkeiten, um bestimmte Aktivitäten anhand definierter Workloads durchzuführen und auf Ereignisse zu reagieren, die durch die Workloads verursacht werden. Die Organisation dokumentiert die Zuständigkeit für Prozesse und deren Erfüllung und macht diese Informationen auffindbar. Sie überprüfen und aktualisieren die Zuständigkeiten, wenn organisatorische Änderungen stattfinden, und die Teams verfolgen und messen die Leistung der Aktivitäten zur Identifizierung von Fehlern und Ineffizienzen. Sie implementieren Feedback-Mechanismen, um Fehler und Verbesserungen nachzuverfolgen und iterative Verbesserungen zu unterstützen.

Typische Anti-Muster:

- Sie dokumentieren keine Verantwortlichkeiten.
- Fragmentierte Skripte existieren auf isolierten Bedienerarbeitsplätzen. Nur wenige Personen wissen, wie man sie verwendet, oder bezeichnen sie informell als Teamwissen.
- Ein veralteter Prozess muss aktualisiert werden, aber niemand weiß, wer für den Prozess zuständig ist, und der ursprüngliche Autor gehört nicht mehr zur Organisation.
- Prozesse und Skripte sind nicht auffindbar und nicht sofort verfügbar, wenn sie benötigt werden (z. B. als Reaktion auf einen Vorfall).

Vorteile der Nutzung dieser bewährten Methode:

- Sie wissen, wer die verantwortliche Person für die Durchführung einer Aktivität ist, wer benachrichtigt werden muss, wenn eine Aktion erforderlich ist, und wer die Aktion ausführen, das Ergebnis validieren und dem Besitzer der Aktivität Feedback geben wird.

- Prozesse und Verfahren unterstützen Sie bei der Bewältigung Ihrer Workloads.
- Neue Teammitglieder werden schneller handlungsfähig.
- Sie reduzieren die Zeit, die zur Behebung von Vorfällen benötigt wird.
- Verschiedene Teams verwenden dieselben Prozesse und Verfahren, um Aufgaben auf einheitliche Weise auszuführen.
- Teams können ihre Prozesse durch wiederholbare Prozesse skalieren.
- Standardisierte Prozesse und Verfahren tragen dazu bei, die Auswirkungen der Übertragung von Workload-Verantwortlichkeiten zwischen Teams abzumildern.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Hoch

### Implementierungsleitfaden

Um mit der Definition von Verantwortlichkeiten zu beginnen, beginnen Sie mit der vorhandenen Dokumentation, wie Zuständigkeitsmatrizen, Prozessen und Verfahren, Rollen und Verantwortlichkeiten sowie Tools und Automatisierung. Überprüfen und besprechen Sie die Verantwortlichkeiten für dokumentierte Prozesse. Ermitteln Sie gemeinsam mit den Teams, ob Abweichungen zwischen den Verantwortlichkeiten und Prozessen für Dokumente vorliegen. Besprechen Sie die angebotenen Dienstleistungen mit internen Kunden dieses Teams, um unterschiedliche Erwartungen zwischen den Teams zu identifizieren.

Analysieren und beheben Sie die Diskrepanzen. Identifizieren Sie Verbesserungsmöglichkeiten und suchen Sie nach häufig nachgefragten, ressourcenintensiven Aktivitäten, bei denen es sich in der Regel um gute Kandidaten für Verbesserungen handelt. Informieren Sie sich über bewährte Methoden, Muster und verbindliche Anleitungen, um Verbesserungen zu vereinfachen und zu standardisieren. Erfassen Sie Verbesserungsmöglichkeiten und verfolgen Sie die Verbesserungen bis zur Fertigstellung.

Mit der Zeit sollten diese Verfahren so weiterentwickelt werden, dass sie als Code ausgeführt werden, sodass weniger menschliche Eingriffe erforderlich sind. Verfahren können beispielsweise als AWS Lambda Funktionen, AWS CloudFormation Vorlagen oder AWS Systems Manager Automatisierungsdokumente initiiert werden. Stellen Sie sicher, dass diese Verfahren in den entsprechenden Repositories versionskontrolliert sind und ein geeignetes Ressourcen-Tagging enthalten, sodass die Teams die Eigentümer und die Dokumentation leicht identifizieren können. Dokumentieren Sie die Verantwortung für die Durchführung der Aktivitäten und überwachen Sie dann die Automatisierungen, um sicherzustellen, dass sie erfolgreich initiiert und ausgeführt werden und dass die gewünschten Ergebnisse erzielt werden.

## Kundenbeispiel

AnyCompany Im Einzelhandel wird Eigentum als das Team oder die Einzelperson definiert, die für Prozesse für eine Anwendung oder für Gruppen von Anwendungen verantwortlich ist, die gemeinsame Architekturpraktiken und Technologien verwenden. Zunächst dokumentiert das Unternehmen die Prozesse und Verfahren als step-by-step Leitlinien im Dokumentenmanagementsystem. Sie machen die Verfahren auffindbar, indem sie Tags auf dem Server verwenden, der die Anwendung hostet AWS-Konto , und auf bestimmten Gruppen von Ressourcen innerhalb des Kontos, die AWS Organizations zur Verwaltung der Prozesse verwendet werden. AWS-Konten Im Laufe der Zeit wandelt AnyCompany Retail diese Prozesse in Code um und definiert Ressourcen mithilfe von Infrastruktur als Code (mithilfe von Diensten wie CloudFormation oder AWS Cloud Development Kit (AWS CDK) Vorlagen). Die betrieblichen Prozesse werden zu Automatisierungsdokumenten in AWS Systems Manager oder AWS Lambda Funktionen, die als geplante Aufgaben als Reaktion auf Ereignisse wie CloudWatch Amazon-Alarme oder EventBridge Amazon-Ereignisse oder durch Anfragen innerhalb einer IT-Servicemanagement-Plattform (ITSM) initiiert werden können. Alle Prozesse sind mit Tags versehen, um die Zuständigkeit zu identifizieren. Teams verwalten die Dokumentation für die Automatisierung und den Prozess auf den Wiki-Seiten, die vom Code-Repository für den Prozess generiert werden.

## Implementierungsschritte

1. Dokumentieren Sie die bestehenden Prozesse und Verfahren.
  - a. Überprüfe und vergewissere dich, dass sie es sind up-to-date.
  - b. Stellen Sie sicher, dass jeder Prozess oder jedes Verfahren einen Besitzer hat.
  - c. Stellen Sie die Verfahren unter Versionskontrolle.
  - d. Wenn möglich, nutzen Sie Prozesse und Verfahren für Workloads und Umgebungen mit gemeinsamen Architekturentwürfen.
2. Richten Sie Mechanismen für Feedback und Verbesserung ein.
  - a. Definieren Sie Richtlinien dafür, wie oft Prozesse überprüft werden sollten.
  - b. Definieren Sie Prozesse für Prüfende und Genehmigende.
  - c. Implementieren Sie Probleme oder eine Ticket-Warteschlange, um Feedback zu geben und zu verfolgen.
  - d. Stellen Sie, wo immer möglich, eine Vorabgenehmigung und Risikoklassifizierung für Prozesse und Verfahren durch einen Ausschuss für die Genehmigung von Änderungen bereit (CAB).
3. Machen Sie Prozesse und Verfahren für Benutzer zugänglich und auffindbar, die sie ausführen müssen.

- a. Verwenden Sie Tags, um anzugeben, wo der Prozess und die Verfahren für die Workload aufgerufen werden können.
  - b. Verwenden Sie aussagekräftige Fehler- und Ereignismeldungen, um die geeigneten Prozesse oder Verfahren zur Behebung des Problems anzugeben.
  - c. Verwenden Sie Wikis oder Dokumentenmanagement, um Prozesse und Verfahren unternehmensweit durchsuchbar zu machen.
4. Automatisieren Sie, wenn es angemessen ist.
- a. Wo Dienste und Technologien dies ermöglichen API, sollten Automatisierungen entwickelt werden.
  - b. Stellen Sie sicher, dass die Prozesse gut verstanden werden, und entwickeln Sie Benutzerberichte und Anforderungen, um diese Prozesse zu automatisieren.
  - c. Messen Sie die erfolgreiche Nutzung der Prozesse und Verfahren und unterstützen Sie eine iterative Verbesserung anhand der Problemverfolgung.

Aufwand für den Implementierungsplan: Mittel

Ressourcen

Zugehörige bewährte Methoden:

- [OPS02-BP01 Ressourcen haben Eigentümer identifiziert](#)
- [OPS02-BP02 Für Prozesse und Verfahren wurden Eigentümer identifiziert](#)
- [OPS02-BP04 Es gibt Mechanismen zur Verwaltung von Verantwortlichkeiten und Eigenverantwortung](#)
- [OPS02-BP05 Es gibt Mechanismen zur Identifizierung von Verantwortung und Eigenverantwortung](#)
- [OPS11-BP04 Führen Sie Wissensmanagement durch](#)

Zugehörige Dokumente:

- [AWS Whitepaper | Einführung in DevOps AWS](#)
- [AWS Whitepaper | Bewährte Methoden für das Markieren von Ressourcen AWS](#)
- [AWS Whitepaper | Organisieren Sie Ihre AWS Umgebung mithilfe mehrerer Konten](#)
- [AWS Cloud Blog zu Betrieb und Migrationen | Entwickeln Sie eine Cloud-Automatisierungspraxis für optimale betriebliche Abläufe: Bewährte Verfahren von AWS Managed Services](#)

- [AWS -Workshop – Tagging](#)
- [AWS Service Management-Konnektor](#)

#### Zugehörige Videos:

- [AWS Knowledge Center Live | Ressourcen taggen AWS](#)
- [AWS re:Invent 2020 | Automatisieren Sie alles mit Systems Manager AWS](#)
- [AWS re:inForce 2022 | Automatisieren von Patch-Management und Compliance mithilfe von \(06\) AWS NIS3](#)
- [AWS Support s You | Tauchen Sie tief in AWS Systems Manager ein](#)

#### Zugehörige Beispiele:

- [AWS Well-Architected-Workshop zur betrieblichen Exzellenz](#)

OPS02-BP04 Es gibt Mechanismen zur Verwaltung von Verantwortlichkeiten und Eigenverantwortung

Verstehen Sie die die Verantwortlichkeiten Ihrer Rolle und, wie Sie zu Geschäftsergebnissen beitragen, da Ihnen dieses Wissen ermöglicht, Ihre Aufgaben entsprechend zu priorisieren und die Bedeutung Ihrer Rolle nachzuvollziehen. Auf diese Weise können Teammitglieder Anforderungen erkennen und entsprechend reagieren. Wenn die Teammitglieder ihre Rolle kennen, können sie Verantwortung übernehmen, Verbesserungsmöglichkeiten erkennen und verstehen, wie sie Einfluss nehmen oder entsprechende Änderungen vornehmen können.

Gelegentlich kann es vorkommen, dass eine Verantwortlichkeit keinen eindeutigen Besitzer hat. Entwerfen Sie in diesen Situationen einen Mechanismus, um diese Lücke zu schließen. Erstellen Sie einen klar definierten Eskalationsweg zu jemandem, der die Befugnis hat, die Verantwortung zu übertragen, oder entwickeln Sie einen Plan zur Deckung des Bedarfs.

Gewünschtes Ergebnis: Teams in Ihrer Organisation haben klar definierte Verantwortlichkeiten, zu denen auch gehört, in welcher Beziehung sie zu Ressourcen, durchzuführenden Aktionen, Prozessen und Verfahren stehen. Diese Verantwortlichkeiten entsprechen den Verantwortlichkeiten und Zielen des Teams sowie den Verantwortlichkeiten anderer Teams. Sie dokumentieren die Eskalationswege auf konsistente und nachvollziehbare Weise und nehmen diese Entscheidungen in Dokumentationsartefakte wie Zuständigkeitsmatrizen, Teamdefinitionen oder Wiki-Seiten auf.

## Typische Anti-Muster:

- Die Verantwortlichkeiten des Teams sind mehrdeutig oder schlecht definiert.
- Das Team stimmt Rollen nicht mit Verantwortlichkeiten ab.
- Das Team stimmt seine Ziele und Verantwortlichkeiten nicht aufeinander ab, was es schwierig macht, den Erfolg zu messen.
- Die Verantwortlichkeiten der Teammitglieder sind nicht am Team und der gesamten Organisation ausgerichtet.
- Ihr Team behält sich keine Verantwortung up-to-date, weshalb sie nicht mit den vom Team ausgeführten Aufgaben vereinbar sind.
- Eskalationswege zur Festlegung von Zuständigkeiten sind nicht definiert oder unklar.
- Eskalationswege haben keinen eindeutigen Besitzer, um eine zeitnahe Reaktion zu gewährleisten.
- Rollen, Zuständigkeiten und Eskalationswege sind nicht auffindbar und bei Bedarf nicht sofort verfügbar (z. B. als Reaktion auf einen Vorfall).

## Vorteile der Nutzung dieser bewährten Methode:

- Wenn Sie wissen, wer verantwortlich oder zuständig ist, können Sie sich an das entsprechende Team oder Teammitglied wenden, um eine Anfrage zu stellen oder eine Aufgabe zu übergeben.
- Um das Risiko von Untätigkeit und ungedecktem Bedarf zu verringern, haben Sie eine Person festgelegt, die befugt ist, Verantwortung und Zuständigkeit zu übertragen.
- Wenn Sie den Umfang einer Verantwortlichkeit klar definieren, gewinnen Ihre Teammitglieder an Autonomie und Eigenverantwortung.
- Ihre Verantwortlichkeiten wirken sich auf Ihre Entscheidungen, Ihre Aktionen und die Übergabe von Aktivitäten an die ordnungsgemäßen Besitzer aus.
- Es ist einfach, aufgegebene Verantwortlichkeiten zu identifizieren, da Sie genau wissen, was außerhalb der Verantwortung Ihres Teams liegt, was die Eskalation zur Aufklärung erleichtert.
- Es kommt innerhalb der Teams zu weniger Verwirrung und Spannungen und sie können ihre Workloads und Ressourcen besser verwalten.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Hoch

## Implementierungsleitfaden

Legen Sie die Rollen und Verantwortlichkeiten von Teammitgliedern fest und vergewissern Sie sich, dass sie die Anforderungen ihrer Rolle kennen. Diese Informationen sollten leicht auffindbar sein, damit Mitglieder Ihrer Organisation herausfinden können, an wen sie sich für bestimmte Anforderungen wenden müssen (an ein Team oder eine Person). Wenn Unternehmen versuchen, die Möglichkeiten der Migration und Modernisierung zu nutzen AWS, können sich auch Rollen und Verantwortlichkeiten ändern. Sorgen Sie dafür, dass sich Ihre Teams und ihre Mitglieder ihrer Verantwortlichkeiten bewusst sind, und schulen Sie sie angemessen, damit sie ihre Aufgaben während dieser Veränderung erfüllen.

Legen Sie fest, an welche Rolle oder welches Team eskaliert werden soll, um die Verantwortlichkeit und Zuständigkeit zu bestimmen. Dieses Team kann mit verschiedenen Stakeholdern zusammenarbeiten, um eine Entscheidung zu treffen. Es sollte jedoch die Verantwortung für die Verwaltung des Entscheidungsprozesses tragen.

Stellen Sie Mitgliedern Ihrer Organisation zugängliche Mechanismen bereit, um Zuständigkeiten und Verantwortlichkeiten zu ermitteln und zuzuordnen. Diese Mechanismen vermitteln ihnen, an wen sie sich bei spezifischen Bedürfnissen wenden können.

### Kundenbeispiel

AnyCompany Der Einzelhandel hat vor Kurzem eine Migration von Workloads von einer lokalen Umgebung in seine landing zone AWS mit einem Lift-and-Shift-Ansatz abgeschlossen. Das Unternehmen führte eine Betriebsüberprüfung durch, um festzustellen, wie allgemeine betriebliche Aufgaben erfüllt werden, und verifizierte, dass seine bestehende Verantwortungsmatrix die Abläufe in der neuen Umgebung widerspiegelt. Bei der Migration von der lokalen Infrastruktur zur AWS lokalen Infrastruktur wurden die Verantwortlichkeiten der Infrastrukturtteams in Bezug auf Hardware und physische Infrastruktur reduziert. Dieser Schritt eröffnete auch neue Möglichkeiten, das Betriebsmodell für seine Workloads weiterzuentwickeln.

Es identifizierte, adressierte und dokumentierte die meisten Verantwortlichkeiten, definierte aber auch Eskalationswege für alle Verantwortlichkeiten, die übersehen wurden oder die sich im Zuge der Weiterentwicklung der betrieblichen Abläufe möglicherweise ändern müssen. Um neue Möglichkeiten zur Standardisierung und Steigerung der Effizienz Ihrer Workloads zu erkunden, bieten Sie Zugriff auf Betriebstools wie AWS Systems Manager und Sicherheitstools wie Amazon AWS Security Hub . GuardDuty AnyCompanyDer Einzelhandel erstellt einen Überblick über die Zuständigkeiten und die Strategie auf der Grundlage der Verbesserungen, die zuerst angegangen werden sollen.

Wenn das Unternehmen neue Arbeitsweisen und Technologiemuster einführt, passt es seine Verantwortungsmatrix entsprechend an.

### Implementierungsschritte

1. Beginnen Sie mit der vorhandenen Dokumentation. Zu den typischen Quelldokumenten gehören möglicherweise:
  - a. Verantwortlichkeit oder verantwortliche, rechenschaftspflichtige, konsultierte und informierte Matrizen (RACI)
  - b. Teamdefinitionen oder Wiki-Seiten
  - c. Servicedefinitionen und Angebote
  - d. Rollen- oder Stellenbeschreibungen
2. Überprüfen und besprechen Sie die dokumentierten Verantwortlichkeiten:
  - a. Führen Sie Besprechungen mit den Teams durch, um Abweichungen zwischen den dokumentierten Verantwortlichkeiten und den vom Team üblicherweise wahrgenommenen Verantwortlichkeiten zu identifizieren.
  - b. Erörtern Sie mögliche Services, die von internen Kunden angeboten werden, um unterschiedliche Erwartungen zwischen den Teams zu identifizieren.
3. Analysieren und beheben Sie die Diskrepanzen.
4. Identifizieren Sie Verbesserungsmöglichkeiten.
  - a. Identifizieren Sie häufig nachgefragte, ressourcenintensive Anfragen, bei denen es sich in der Regel um gute Verbesserungsmöglichkeiten handelt.
  - b. Informieren Sie sich über bewährte Methoden, Muster und verbindliche Anleitungen und vereinfachen und standardisieren Sie Verbesserungen anhand dieser Anleitungen.
  - c. Erfassen Sie Verbesserungsmöglichkeiten und verfolgen Sie sie bis zur Fertigstellung.
5. Wenn ein Team noch nicht die Verantwortung für die Verwaltung und die Verfolgung der Zuweisung von Verantwortlichkeiten trägt, benennen Sie jemanden im Team, der diese Verantwortung übernimmt.
6. Definieren Sie einen Prozess, nach dem Teams eine Klärung der Verantwortlichkeiten anfordern können.
  - a. Überprüfen Sie den Prozess und stellen Sie sicher, dass er klar und einfach umzusetzen ist.
  - b. Stellen Sie sicher, dass jemand die Verantwortung für die Eskalationen trägt und sie bis zu ihrem Ende verfolgt.
  - c. Legen Sie betriebliche Metriken fest, um die Effektivität zu messen.



- d. Schaffen Sie Feedback-Mechanismen, um sicherzustellen, dass Teams Verbesserungsmöglichkeiten hervorheben können.
  - e. Implementieren Sie einen Mechanismus für die regelmäßige Überprüfung.
7. Führen Sie Dokumente an einem auffindbaren und zugänglichen Ort.
- a. Wikis oder das Dokumentationsportal sind gängige Optionen.

Aufwand für den Implementierungsplan: Mittel

Ressourcen

Zugehörige bewährte Methoden:

- [OPS01-BP06 Bewerten Sie Kompromisse](#)
- [OPS03-BP02 Die Teammitglieder sind in der Lage, Maßnahmen zu ergreifen, wenn die Ergebnisse gefährdet sind](#)
- [OPS03-BP03 Eine Eskalation wird empfohlen](#)
- [OPS03-BP07 Stellen Sie die Teams angemessen zur Verfügung](#)
- [OPS09-BP01 Messen Sie Ihre Betriebsziele und nutzen Sie diese anhand von Kennzahlen KPIs](#)
- [OPS09-BP03 Überprüfen Sie die Betriebskennzahlen und priorisieren Sie Verbesserungen](#)
- [OPS11-BP01 Setzen Sie einen Prozess zur kontinuierlichen Verbesserung ein](#)

Zugehörige Dokumente:

- [AWS Whitepaper — Einführung in DevOps AWS](#)
- [AWS Whitepaper — Rahmenbedingungen für die AWS Cloud Einführung: Betriebsperspektive](#)
- [AWS Well-Architected-Framework – Betriebliche Exzellenz — Betriebsmodelltopologien auf Workload-Ebene](#)
- [AWS Prescriptive Guidance – Aufbau Ihres Cloud-Betriebsmodells](#)
- [AWS Präskriptive Leitlinien — Erstellen Sie eine RACI RASCI Oder-Matrix für ein Cloud-Betriebsmodell](#)
- [AWS Cloud Blog „Operations & Migrations“ — Mit Cloud-Plattform-Teams Mehrwert für Ihr Unternehmen schaffen](#)
- [AWS Cloud Blog zu Betrieb und Migrationen — Warum ein Cloud-Betriebsmodell?](#)

- [AWS DevOps Blog — Wie sich Unternehmen für den Cloud-Betrieb modernisieren](#)

Zugehörige Videos:

- [AWS Summit Online – Cloud-Betriebsmodelle für eine schnellere Transformation](#)
- [AWS re:Invent 2023 – Cloud-Sicherheit zukunftssicher machen: Ein neues Betriebsmodell](#)

OPS02-BP05 Es gibt Mechanismen, um Ergänzungen, Änderungen und Ausnahmen zu beantragen

Sie können Anfragen an Verantwortliche für Prozesse, Verfahren und Ressourcen stellen. Die Anfragen umfassen Ergänzungen, Änderungen und Ausnahmen. Diese Anfragen durchlaufen einen Änderungsverwaltungsprozess. Treffen Sie fundierte Entscheidungen, um angemessene Anfragen nach einer Bewertung der Vorteile und Risiken zu genehmigen.

Gewünschtes Ergebnis:

- Sie können Anfragen zum Ändern von Prozessen, Verfahren und Ressourcen basierend auf der zugewiesenen Verantwortlichkeit stellen.
- Änderungen werden nach einem sorgfältigen Abwägen der Vorteile und Risiken vorgenommen.

Typische Anti-Muster:

- Sie müssen die Art und Weise der Bereitstellung Ihrer Anwendung aktualisieren, es gibt jedoch keine Möglichkeit, eine Änderung am Bereitstellungsprozess beim Produktionsteam zu beantragen.
- Der Notfallwiederherstellungsplan muss aktualisiert werden, es ist jedoch kein Verantwortlicher kenntlich gemacht, an den Anträge auf Änderungen übermittelt werden können.

Vorteile der Nutzung dieser bewährten Methode:

- Prozesse, Verfahren und Ressourcen können sich weiterentwickeln, wenn sich die Anforderungen ändern.
- Die Verantwortlichen können fundierte Entscheidungen treffen, wann Änderungen vorgenommen werden sollten.
- Änderungen werden nach sorgfältigen Überlegungen vorgenommen.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel

## Implementierungsleitfaden

Um diese bewährte Methode zu implementieren, müssen Sie Änderungen an Prozessen, Verfahren und Ressourcen beantragen können. Der Änderungsverwaltungsprozess kann einfach sein. Dokumentieren Sie den Änderungsverwaltungsprozess.

### Kundenbeispiel

AnyCompany Der Einzelhandel verwendet eine Matrix zur Zuweisung von RACI Zuständigkeiten (), um zu ermitteln, wem Änderungen an Prozessen, Verfahren und Ressourcen zugewiesen sind. Es gibt einen dokumentierten Änderungsverwaltungsprozess, der einfach und leicht zu befolgen ist. Mithilfe der RACI Matrix und des Prozesses kann jeder Änderungsanträge einreichen.

### Implementierungsschritte

1. Ermitteln Sie die Prozesse, Verfahren und Ressourcen für Ihren Workload sowie die jeweiligen Verantwortlichen. Dokumentieren Sie sie in Ihrem Wissensmanagementsystem.
  - a. Wenn Sie [OPS02-BP01 Ressourcen haben Eigentümer identifiziert](#), [OPS02-BP02 Prozesse und Verfahren haben Eigentümer identifiziert](#) oder [OPS02-BP03 Bei den operativen Aktivitäten wurden Eigentümer identifiziert, die für ihre Leistung verantwortlich sind](#) nicht implementiert haben, beginnen Sie damit.
2. Arbeiten Sie mit den Stakeholdern in Ihrer Organisation zusammen, um einen Änderungsverwaltungsprozess zu entwickeln. Der Prozess sollte Ergänzungen, Änderungen und Ausnahmen für Ressourcen, Prozesse und Verfahren umfassen.
  - a. Sie können [AWS Systems Manager Change Manager](#) als Änderungsverwaltungsplattform für Workload-Ressourcen verwenden.
3. Dokumentieren Sie den Änderungsverwaltungsprozess in Ihrem Wissensmanagementsystem.

Aufwand für den Implementierungsplan: Mittel. Die Entwicklung eines Änderungsverwaltungsprozesses erfordert die Abstimmung mit mehreren Stakeholdern in Ihrer Organisation.

### Ressourcen

Zugehörige bewährte Methoden:

- [OPS02-BP01 Ressourcen haben Eigentümer identifiziert](#) – Bevor Sie einen Änderungsverwaltungsprozess entwickeln, müssen für Ressourcen die Besitzer identifiziert werden.

- [OPS02-BP02 Prozesse und Verfahren haben Eigentümer identifiziert](#) – Bevor Sie einen Änderungsverwaltungsprozess entwickeln, müssen für Prozesse die Besitzer identifiziert werden.
- [OPS02-BP03 Bei den operativen Aktivitäten wurden Eigentümer identifiziert, die für ihre Leistung verantwortlich sind](#) – Bevor Sie einen Änderungsverwaltungsprozess entwickeln, müssen für Betriebsaktivitäten die Besitzer identifiziert werden.

Zugehörige Dokumente:

- [AWS Prescriptive Guidance — Leitfaden für die Grundlagen bei AWS großen Migrationen: Matrizen erstellen RACI](#)
- [Whitepaper „Änderungsmanagement in der Cloud“](#)

Zugehörige Services:

- [AWS Systems Manager Manager ändern](#)

OPS02-BP06 Verantwortlichkeiten zwischen Teams sind vordefiniert oder ausgehandelt

Es gibt definierte oder ausgehandelte Vereinbarungen zwischen Teams, in denen die Zusammenarbeit und gegenseitige Unterstützung beschrieben wird (z. B. Reaktionszeiten, Service-Level-Ziele oder Service-Level-Agreements). Die Kanäle für die teamübergreifende Kommunikation werden dokumentiert. Wenn bekannt ist, welche Auswirkungen die Arbeit der Teams auf die Geschäftsergebnisse und die Ergebnisse anderer Teams und Organisationen hat, können die Teams ihre Aufgaben priorisieren und entsprechend handeln.

Wenn Verantwortlichkeit und Zuständigkeit nicht definiert oder unbekannt sind, besteht das Risiko, dass sowohl die erforderlichen Aktivitäten nicht rechtzeitig ausgeführt als auch redundante und potenziell widersprüchliche Anstrengungen unternommen werden, um diese Anforderungen zu erfüllen.

Gewünschtes Ergebnis:

- Es werden Vereinbarungen zur teamübergreifenden Zusammenarbeit oder Unterstützung getroffen und dokumentiert.
- Teams, die zusammenarbeiten oder sich gegenseitig unterstützen, verfügen über definierte Kommunikationskanäle und Erwartungen in Bezug auf die Reaktion.

## Typische Anti-Muster:

- Während der Produktion tritt ein Problem auf und zwei separate Teams beginnen unabhängig voneinander mit der Fehlersuche. Aufgrund der getrennten Bemühungen verlängert sich der Ausfall.
- Das Produktionsteam benötigt Unterstützung vom Entwicklungsteam, es gibt jedoch keine Vereinbarung in Bezug auf die Reaktionszeit. Die Anfrage wird zurückgestellt.

## Vorteile der Nutzung dieser bewährten Methode:

- Die Teams wissen, wie sie miteinander interagieren und sich gegenseitig unterstützen können.
- Die Erwartungen in Bezug auf die Reaktionszeit sind bekannt.
- Die Kommunikationskanäle sind klar definiert.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Niedrig

## Implementierungsleitfaden

Wenn Sie diese bewährte Methode implementieren, bedeutet dies, dass es in Bezug auf die Zusammenarbeit zwischen Teams keine Unklarheiten gibt. Mithilfe von formellen Vereinbarungen wird festgelegt, wie Teams zusammenarbeiten oder sich gegenseitig unterstützen. Die Kanäle für die teamübergreifende Kommunikation werden dokumentiert.

## Kundenbeispiel

AnyCompany Das SRE Einzelhandelsteam hat mit seinem Entwicklungsteam ein Service Level Agreement abgeschlossen. Wenn das Entwicklungsteam eine Anfrage über das Ticketing-System einreicht, kann es innerhalb von 15 Minuten eine Antwort erwarten. Bei einem Ausfall der Website übernimmt das SRE Team mit Unterstützung des Entwicklungsteams die Leitung der Untersuchung.

## Implementierungsschritte

1. Arbeiten Sie zusammen mit den Stakeholdern in Ihrer Organisation und auf Grundlage der Prozesse und Verfahren Vereinbarungen zwischen Teams aus.
  - a. Entwickeln Sie für gemeinsame Prozesse oder Verfahren von zwei Teams ein Runbook für die Zusammenarbeit.
  - b. Wenn zwischen den Teams Abhängigkeiten bestehen, stimmen Sie einer Antwort auf Anfragen SLA zu.

## 2. Dokumentieren Sie die Verantwortlichkeiten in Ihrem Wissensmanagementsystem.

Aufwand für den Implementierungsplan: Mittel. Wenn keine Vereinbarungen zwischen Teams vorhanden sind, kann es mühsam sein, eine Vereinbarung mit den Stakeholdern in Ihrer Organisation zu treffen.

### Ressourcen

Zugehörige bewährte Methoden:

- [OPS02-BP02 Prozesse und Verfahren haben Eigentümer identifiziert](#) – Die Verantwortlichkeiten für Prozesse müssen bestimmt werden, bevor Teams Vereinbarungen miteinander treffen.
- [OPS02-BP03 Bei den operativen Aktivitäten wurden Eigentümer identifiziert, die für ihre Leistung verantwortlich sind](#) – Die Verantwortlichkeiten für Betriebsaktivitäten müssen bestimmt werden, bevor Teams Vereinbarungen miteinander treffen.

Zugehörige Dokumente:

- [AWS Executive Insights — Innovation fördern mit dem Two-Pizza-Team](#)
- [Einführung in DevOps On-Two-Pizza-Teams AWS](#)

## OPS3. Wie unterstützt Ihre Unternehmenskultur Ihre Geschäftsergebnisse?

Lassen Sie Ihren Teammitgliedern Unterstützung zukommen, damit sie effektiver handeln und Ihr Geschäftsergebnis unterstützen können.

### Bewährte Methoden

- [OPS03-BP01 Unterstützen Sie Führungskräfte](#)
- [OPS03-BP02 Teammitglieder sind befugt, Maßnahmen zu ergreifen, wenn die Ergebnisse gefährdet sind](#)
- [OPS03-BP03 Eskalation wird gefördert](#)
- [OPS03-BP04 Die Kommunikation ist zeitnah, klar und umsetzbar](#)
- [OPS03-BP05 Experimentieren wird gefördert](#)
- [OPS03-BP06 Teammitglieder werden ermutigt, ihre Fähigkeiten zu erhalten und auszubauen](#)
- [OPS03-BP07 Ressourcenteams angemessen](#)

## OPS03-BP01 Unterstützen Sie Führungskräfte

Auf höchster Ebene fungiert die Geschäftsleitung als Executive Sponsor, um Erwartungen klar festzulegen und die Richtung für die Ergebnisse der Organisation vorzugeben sowie den Erfolg zu bewerten. Der Sponsor befürwortet und fördert die Einführung von bewährten Methoden und die Weiterentwicklung der Organisation.

Gewünschtes Ergebnis: Organisationen, die einen Cloud-Betrieb einführen, transformieren oder optimieren möchten, legen eine klare Führung und Rechenschaftspflicht zum Erreichen der gewünschten Ergebnisse fest. Die Organisation kennt jede Fähigkeit, die sie benötigt, um ein neues Ergebnis zu erzielen, und überträgt den Funktionsteams die Verantwortung für die Entwicklung dieser Fähigkeiten. Die Führung gibt aktiv diese Richtung vor, überträgt Verantwortung, übernimmt Verantwortung und definiert die Arbeit. Dadurch können Mitarbeiter in der gesamten Organisation mobilisieren, sich inspiriert fühlen und aktiv auf die gewünschten Ziele hinarbeiten.

Typische Anti-Muster:

- Workload-Besitzer sind aufgefordert, Workloads zu AWS zu migrieren – ohne klare Unterstützung oder einen Plan für den Cloud-Betrieb. Dies führt dazu, dass Teams nicht gezielt zusammenarbeiten, um ihre operativen Fähigkeiten zu verbessern und weiterzuentwickeln. Der Mangel an Betriebsstandards mit bewährten Methoden führt dazu, dass die Teams überfordert sind (z. B. durch Überarbeitung der Mitarbeiter, Bereitschaftsdienste und technische Schulden) und die Innovation ins Stocken gerät.
- Es wurde ein neues organisationsweites Ziel gesetzt, eine neue Technologie einzuführen, ohne die Führung, den Sponsor und die Strategie anzugeben. Die Teams interpretieren Ziele unterschiedlich, was zu Verwirrung darüber führt, worauf sie sich konzentrieren sollten, warum sie wichtig sind und wie Auswirkungen gemessen werden sollen. Folglich verliert die Organisation bei der Einführung der Technologie an Dynamik.

Vorteile der Nutzung dieser bewährten Methode: Wenn die Geschäftsführung Vision, Ausrichtung und Ziele klar kommuniziert und teilt, wissen die Teammitglieder, was von ihnen erwartet wird. Wenn sich die Führungskräfte aktiv einbringen, beginnen Einzelpersonen und Teams, ihre Bemühungen intensiv in dieselbe Richtung zu lenken, um festgelegte Ziele zu erreichen. Dadurch maximiert die Organisation ihre Erfolgsfähigkeit. Wenn Sie den Erfolg evaluieren, können Sie Barrieren besser identifizieren um anschließend von der Führung gezielt ausgeräumt werden können.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Hoch

## Implementierungsleitfaden

- In jeder Phase des Wegs in die Cloud (Migration, Einführung oder Optimierung) erfordert der Erfolg eine aktive Beteiligung auf höchster Führungsebene mit einem leitenden Unterstützer. Der leitende Unterstützer richtet die Denkweise, Fähigkeiten und Arbeitsweisen des Teams an der definierten Strategie aus.
  - Erläutern des Warums: Sorgen Sie für Klarheit und erläutern Sie die Gründe für die Vision und die Strategie.
  - Festlegen der Erwartungen: Definieren und veröffentlichen Sie Ziele für Ihre Organisationen, einschließlich der Art und Weise, wie Fortschritt und Erfolg gemessen werden.
  - Verfolgen der Zielerreichung: Messen Sie regelmäßig das schrittweise Erreichen von Zielen (nicht nur die Erledigung von Aufgaben). Teilen Sie die Ergebnisse mit, damit geeignete Maßnahmen ergriffen werden können, wenn die Ergebnisse gefährdet sind.
  - Bereitstellen der erforderlichen Ressourcen zum Erreichen Ihrer Ziele: Bringen Sie Menschen und Teams zusammen, um zusammenzuarbeiten und die richtigen Lösungen zu entwickeln, die zu den definierten Ergebnissen führen. Dies reduziert oder beseitigt Reibungspunkte in der Organisation.
  - Unterstützen Ihrer Teams: Bleiben Sie mit Ihren Teams in Kontakt, damit Sie deren Leistung verstehen und herausfinden können, ob diese durch externe Faktoren beeinflusst wird. Identifizieren Sie Hindernisse für den Fortschritt Ihrer Teams. Treten Sie für Ihre Teams ein und beseitigen Sie Hindernisse und unnötige Belastungen. Wenn sich äußere Faktoren negativ auf Ihre Teams auswirken, bewerten Sie die Ziele neu und passen Sie sie entsprechend an.
  - Fördern der Einführung von bewährten Methoden: Würdigen Sie bewährte Methoden, die messbare Vorteile bieten, und schenken Sie ihren Entwicklern und Anwendern Ihre Anerkennung. Ermutigen Sie Ihre Teams zur Annahme dieser Methoden, um die Vorteile zu maximieren.
  - Ermuntern Sie Ihre Teams zur Weiterentwicklung: Schaffen Sie eine Kultur der kontinuierlichen Verbesserung und lernen Sie proaktiv aus Fortschritten und Fehlschlägen. Fördern Sie Wachstum und Entwicklung sowohl im Persönlichen als auch im Betrieblichen. Entwickeln Sie die Vision und Strategie anhand von Daten und Anekdoten weiter.

## Kundenbeispiel

AnyCompany Der Einzelhandel befindet sich im Prozess der Geschäftstransformation durch die rasche Neuerfindung von Kundenerlebnissen, die Steigerung der Produktivität und die Beschleunigung des Wachstums durch generative KI.



## Implementierungsschritte

1. Ernennen Sie einen einzelnen Verantwortlichen und einen leitenden Unterstützer, der die Transformation leitet und vorantreibt.
2. Definieren Sie klare Geschäftsergebnisse für Ihre Transformation, weisen Sie Verantwortlichkeiten zu und fordern Sie Eigenverantwortung ein. Erteilen Sie der leitenden Führungskraft die Befugnis, wichtige Entscheidungen zu leiten und zu treffen.
3. Stellen Sie sicher, dass Ihre Transformationsstrategie sehr klar ist und vom leitenden Sponsor auf allen Ebenen der Organisation umfassend kommuniziert wird.
  - a. Legen Sie klar definierte Geschäftsziele für IT- und Cloud-Initiativen fest.
  - b. Dokumentieren Sie wichtige Geschäftsmetriken, um die IT- und Cloud-Transformation voranzutreiben.
  - c. Kommunizieren Sie die Vision konsequent an alle Teams und Personen, die für Teile der Strategie verantwortlich sind.
4. Entwickeln Sie Matrizen zur Kommunikationsplanung, die vorgeben, welche Botschaft bestimmten Führungskräften, Managern und einzelnen Mitarbeitern übermittelt werden muss. Legen Sie fest, welche Person oder welches Team diese Nachricht übermitteln soll.
  - a. Erfüllen Sie Kommunikationspläne konsistent und zuverlässig.
  - b. Setzen und steuern Sie Ihre Erwartungen regelmäßig in persönlichen Meetings.
  - c. Nehmen Sie Feedback zur Effektivität der Kommunikation an, passen Sie die Kommunikation an und planen Sie entsprechend.
  - d. Planen Sie Kommunikationsveranstaltungen, um die Herausforderungen der Teams proaktiv zur Kenntnis zu nehmen, und richten Sie eine konsistente Feedback-Schleife ein, um den Kurs bei Bedarf zu korrigieren.
5. Beschäftigen Sie sich aktiv mit jeder Initiative aus der Führungsperspektive, um sicherzustellen, dass alle betroffenen Teams die Ergebnisse verstehen, für deren Erreichung sie verantwortlich sind.
6. Bei jedem Status-Meeting sollten die leitenden Unterstützer nach Hindernissen Ausschau halten, etablierte Metriken, Anekdoten oder das Feedback der Teams überprüfen und die Fortschritte bei der Erreichung der Ziele messen.

Aufwand für den Implementierungsplan: Mittel

## Ressourcen

### Zugehörige bewährte Methoden:

- [OPS03-BP04 Die Kommunikation ist zeitnah, klar und umsetzbar](#)
- [OP11-BP01 Haben Sie einen Prozess zur kontinuierlichen Verbesserung](#)
- [OPS11-BP07 Führen Sie Überprüfungen der Betriebskennzahlen durch](#)

### Zugehörige Dokumente:

- [Entwirren Ihrer Organisation: Stark ausgerichtet](#)
- [Die lebendige Transformation: Veränderungen pragmatisch angehen](#)
- [Transformation zu einem zukunftsfähigen Unternehmen](#)
- [7 Fallstricke, die Sie beim Bau eines vermeiden sollten CCOE](#)
- [Navigation in der Cloud: Wichtige Leistungskennzahlen für den Erfolg](#)

### Zugehörige Videos:

- [AWS re:Invent 2023: Leitfaden für Führungskräfte zur generativen KI: Die future mithilfe der Geschichte gestalten \(04\) SEG2](#)

### Zugehörige Beispiele:

- [Prosci: Rolle und Bedeutung des leitenden Unterstützers](#)

OPS03-BP02 Teammitglieder sind befugt, Maßnahmen zu ergreifen, wenn die Ergebnisse gefährdet sind

Eine von der Führung vermittelte Kultur der Eigenverantwortung führt dazu, dass sich die Mitarbeiter bestärkt fühlen, im Namen des gesamten Unternehmens über ihren definierten Rollen- und Verantwortungsbereich hinaus zu handeln. Die Mitarbeiter können handeln, um auftretende Risiken proaktiv zu erkennen und geeignete Maßnahmen ergreifen. Eine solche Kultur ermöglicht es den Mitarbeitern, die Situation zu überblicken und wichtige Entscheidungen zu treffen.

Amazon verwendet beispielsweise [Führungsprinzipien](#) als Richtlinien, um das gewünschte Verhalten der Mitarbeiter zu fördern, damit sie in Situationen vorankommen, Probleme lösen, mit Konflikten umgehen und Maßnahmen ergreifen können.

Gewünschtes Ergebnis: Die Führung hat eine neue Kultur beeinflusst, die es Einzelpersonen und Teams ermöglicht, wichtige Entscheidungen zu treffen – selbst auf niedrigeren Ebenen der Organisation (sofern Entscheidungen mit überprüfbaren Genehmigungen und Sicherheitsmechanismen definiert sind). Misserfolge werden als Lernerfahrung angesehen, und Teams lernen schrittweise, ihre Entscheidungen und Maßnahmen zu optimieren, um in Zukunft ähnliche Situationen zu bewältigen. Wenn die Maßnahmen einer Person zu einer Verbesserung führen, von der andere Teams profitieren können, werden die aus solchen Maßnahmen gewonnenen Erkenntnisse proaktiv geteilt. Die Geschäftsführung misst betriebliche Verbesserungen und bietet dem Einzelnen sowie der Organisation Anreize für die Übernahme solcher Muster.

Typische Anti-Muster:

- In einer Organisation gibt es keine klaren Leitlinien oder Mechanismen dafür, was zu tun ist, wenn ein Risiko erkannt wird. Wenn ein Mitarbeiter beispielsweise einen Phishing-Angriff bemerkt und dies nicht dem Sicherheitsteam meldet, kann dies zur Folge haben, dass ein großer Teil der Organisation auf den Angriff hereinfällt. Dies führt zu einer Datenschutzverletzung.
- Ihre Kunden beschwerten sich über die Nichtverfügbarkeit von Services, die hauptsächlich auf fehlgeschlagene Bereitstellungen zurückzuführen ist. Ihr SRE Team ist für das Bereitstellungstool verantwortlich, und ein automatisiertes Rollback für Bereitstellungen steht auf der langfristigen Roadmap. Bei einer kürzlichen Anwendungseinführung entwickelte einer der Engineers eine Lösung, um das Rollback seiner Anwendung auf eine frühere Version zu automatisieren. Ihre Lösung kann zwar zum Muster für SRE Teams werden, andere Teams übernehmen sie jedoch nicht, da es keinen Prozess gibt, mit dem solche Verbesserungen nachverfolgt werden können. Die Organisation wird weiterhin durch fehlgeschlagene Bereitstellungen unter Druck gesetzt, die sich auf die Kunden auswirken und die Reputation des Unternehmens gefährden.
- Um die Einhaltung der Vorschriften zu gewährleisten, überwacht Ihr Infosec-Team einen seit langem etablierten Prozess, bei dem gemeinsam genutzte SSH Schlüssel im Namen von Betreibern, die eine Verbindung zu ihren Amazon EC2 Linux-Instances herstellen, regelmäßig rotiert werden. Die InfoSec-Teams brauchen mehrere Tage für die Schlüsselrotation. In dieser Zeit können Sie keine Verbindung zu diesen Instances herstellen. Niemand innerhalb oder außerhalb von Infosec schlägt vor, andere Optionen zu verwenden, um dasselbe Ergebnis AWS zu erzielen.

Vorteile der Nutzung dieser bewährten Methode: Indem Sie die Entscheidungsbefugnisse dezentralisieren und Ihre Teams in die Lage versetzen, wichtige Entscheidungen zu treffen, können Sie Probleme schneller lösen und die Erfolgsquoten steigern. Darüber hinaus beginnen die Teams, ein Gefühl der Eigenverantwortung zu entwickeln, und Misserfolge werden als Lernerfahrungen angesehen. Experimentieren wird zu einem Eckpfeiler der Unternehmenskultur. Manager und

Bereichsleiter haben nicht das Gefühl, dass sie in allen Aspekten bis ins kleinste Detail gemanagt werden.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel

### Implementierungsleitfaden

1. Entwickeln Sie eine Kultur, in der damit gerechnet wird, dass Fehler auftreten können.
2. Definieren Sie klare Verantwortlichkeiten und Zuständigkeiten für verschiedene Funktionsbereiche innerhalb der Organisation.
3. Vermitteln Sie Eigenverantwortung und Rechenschaftspflicht, damit alle wissen, wo sie bei dezentralen Entscheidungen Unterstützung erhalten können.
4. Definieren Sie unumkehrbare und leicht revidierbare Entscheidungen, damit die Mitarbeiter wissen, wann sie Beschlüsse an höhere Führungsebenen eskalieren müssen.
5. Schaffen Sie in der Organisation ein Bewusstsein dafür, dass alle Mitarbeiter in der Lage sind, auf verschiedenen Ebenen Maßnahmen zu ergreifen, wenn Ergebnisse gefährdet sind. Stellen Sie Ihren Teammitgliedern Unterlagen über Governance, Befugnisebenen, Tools sowie Möglichkeiten zur Verfügung, um die erforderlichen Fähigkeiten für eine effektive Reaktion zu üben.
6. Geben Sie Ihren Teammitgliedern die Möglichkeit, die notwendigen Fähigkeiten zu üben, um auf verschiedene Entscheidungen zu reagieren. Sobald die Entscheidungsebenen festgelegt sind, führen Sie GameDays durch, um sicherzustellen, dass alle Mitarbeiter den Prozess verstehen und umsetzen können.
  - a. Stellen Sie alternative sichere Umgebungen bereit, in denen Prozesse und Verfahren getestet und eingeübt werden können.
  - b. Erkennen Sie an und schaffen Sie ein Bewusstsein dafür, dass Teammitglieder befugt sind, Maßnahmen zu ergreifen, wenn das Ergebnis ein vordefiniertes Risikoniveau aufweist.
  - c. Verschaffen Sie den Teammitgliedern die erforderliche Autorität, um Maßnahmen zu ergreifen, indem Sie ihnen Berechtigungen und Zugriff auf ihre Workloads und Komponenten geben.
7. Bieten Sie Teams die Möglichkeit, ihre Erfahrungen (betriebliche Erfolge und Misserfolge) auszutauschen.
8. Ermöglichen Sie Teams, den Status quo in Frage zu stellen, und stellen Sie Mechanismen zur Verfügung, mit denen Verbesserungen sowie deren Auswirkungen auf die Organisation verfolgt und gemessen werden können.

Aufwand für den Implementierungsplan: Mittel

## Ressourcen

### Zugehörige bewährte Methoden:

- [OPS01-BP06 Bewerten Sie Kompromisse und managen Sie gleichzeitig die Vorteile und Risiken](#)
- [OPS02-BP05 Es gibt Mechanismen zur Identifizierung von Verantwortung und Eigenverantwortung](#)

### Zugehörige Dokumente:

- [AWS -Blog-Beitrag | Das agile Unternehmen](#)
- [AWS -Blog-Beitrag | Erfolg messen: Ein Paradoxon und ein Plan](#)
- [AWS -Blog-Beitrag | Loslassen: Autonomie in Teams ermöglichen](#)
- [Zentralisieren oder Dezentralisieren?](#)

### Zugehörige Videos:

- [re:Invent 2023 | Wie du deine Transformation nicht sabotierst \(01\) SEG2](#)
- [re:Invent 2021 | Die Amazon Builders' Library: Betriebliche Exzellenz von Amazon](#)
- [Zentralisierung und Dezentralisierung im Vergleich](#)

### Zugehörige Beispiele:

- [Verwendung von Aufzeichnungen über architektonische Entscheidungen zur Optimierung der technischen Entscheidungsfindung für ein Softwareentwicklungsprojekt](#)

## OPS03-BP03 Eskalation wird gefördert

Die Teammitglieder werden von der Führung ermutigt, Probleme und Bedenken an übergeordnete Entscheidungsträger und Stakeholder zu eskalieren, wenn sie der Meinung sind, dass die gewünschten Ergebnisse gefährdet sind und die erwarteten Standards nicht erfüllt werden. Dies ist ein Feature der Organisationskultur und wird auf allen Ebenen vorangetrieben. Die Eskalation sollte frühzeitig und lieber zu oft vorgenommen werden, damit Risiken identifiziert und Vorfälle verhindert werden können. Die Führung tadelt Mitarbeiter nicht dafür, wenn sie ein Problem eskalieren.

Gewünschtes Ergebnis: Personen in der gesamten Organisation sind vertraut damit, Probleme an ihre unmittelbaren und höheren Führungsebenen zu eskalieren. Die Führung hat bewusst und gezielt

die Erwartung aufgestellt, dass sich ihre Teams sicher fühlen sollen, Probleme zu eskalieren. Es wurde ein Mechanismus eingerichtet, um Probleme auf allen Organisationsebenen zu eskalieren. Wenn Mitarbeiter eine Angelegenheit an ihren Vorgesetzten eskalieren, entscheiden sie gemeinsam über das Ausmaß der Auswirkungen und eine mögliche Eskalation des Problems. Eine Eskalation setzt voraus, dass die Mitarbeiter einen empfohlenen Arbeitsplan zur Behebung des Problems beifügen. Wenn die nächsthöhere Führungsebene nicht rechtzeitig Maßnahmen ergreift, sind die Mitarbeiter angehalten, Probleme an die oberste Führungsebene weiterzuleiten, wenn sie der festen Überzeugung sind, dass die Risiken für die Organisation eine Eskalation rechtfertigen.

Typische Anti-Muster:

- Führungskräfte haken während Ihrer Statusbesprechung zum Cloud-Transformationsprogramm nicht ausreichend nach, um herauszufinden, wo Probleme und Hindernisse auftreten. Stattdessen werden nur gute Nachrichten präsentiert. Sie CIO hat deutlich gemacht, dass sie nur gerne gute Nachrichten hört, da sie aufgrund der aufgeworfenen Probleme CEO glauben, dass das Programm scheitert.
- Sie sind als Cloud-Betriebsentwickler tätig und stellen fest, dass das neue Wissensmanagementsystem von den Anwendungsteams kaum verwendet wird. Das Unternehmen investierte ein Jahr und mehrere Millionen Dollar in die Implementierung eines neuen Wissensmanagementsystems, aber die Mitarbeiter verfassen ihre Runbooks noch immer lokal und teilen sie in einer internen Cloud-Umgebung, was die Suche nach Wissen erschwert, das für unterstützte Workloads relevant ist. Sie versuchen, die Führungskräfte darauf aufmerksam zu machen, da die konsequente Verwendung dieses Systems die betriebliche Effizienz verbessern kann. Als Sie das Problem der Bereichsleiterin vorlegen, die für die Implementierung des Wissensmanagementsystems zuständig ist, werden Sie von ihr kritisiert, weil dadurch die Investition in Frage gestellt wird.
- Das für die Absicherung der Rechenressourcen zuständige Infosec-Team hat beschlossen, einen Prozess einzuführen, bei dem die erforderlichen Scans durchgeführt werden müssen, um sicherzustellen, dass die EC2 Instanzen vollständig gesichert sind, bevor das Compute-Team die Ressource zur Nutzung freigibt. Dadurch kam es zu einer Zeitverzögerung von einer zusätzlichen Woche für die Bereitstellung von Ressourcen, wodurch deren SLA Verfügbarkeit beeinträchtigt wird. Das Computing-Team hat Angst, dies über die Cloud an den VP zu eskalieren, da der VP für Informationssicherheit dadurch in ein schlechtes Licht gerückt werden könnte.

Vorteile der Nutzung dieser bewährten Methode:

Komplexe oder kritische Probleme werden angegangen, bevor sie sich auf das Geschäft auswirken. Es wird weniger Zeit verschwendet. Risiken werden minimiert. Teams werden bei der Lösung von Problemen proaktiver und ergebnisorientierter.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Hoch

### Implementierungsleitfaden

Die Bereitschaft und Fähigkeit, auf allen Organisationsebenen uneingeschränkt zu eskalieren, ist eine bedeutende Eigenschaft der Organisation und ihrer Kultur, die bewusst weiterentwickelt werden sollte, und zwar durch gezielte Schulungen, Kommunikationen der Führungsebene, Erwartungssetzung und den Einsatz von Mechanismen auf allen Organisationsebenen.

### Implementierungsschritte

1. Definieren Sie Richtlinien, Standards und Erwartungen für Ihre Organisation.
  - a. Sorgen Sie für eine breite Anwendung und Kenntnis der Richtlinien, Erwartungen und Standards.
2. Ermutigen, schulen und befähigen Sie die Mitarbeiter, damit sie frühzeitig und häufig eskalieren, wenn die Standards nicht eingehalten werden.
3. Bekräftigen Sie in der Organisation, dass die frühe und häufige Eskalation die bewährte Methode ist. Akzeptieren Sie im Unternehmen, dass sich Eskalationen zwar als unbegründet herausstellen können, es sich aber trotzdem insgesamt lohnt, wenn ein echter Vorfall dadurch verhindert wird.
  - a. Entwickeln Sie einen Mechanismus für Eskalationen (z. B. ein Andon-Cord-System).
  - b. Sorgen Sie für dokumentierte Verfahren, die definieren, wann und wie eine Eskalation erfolgen soll.
  - c. Definieren Sie die Abfolge der Personen mit zunehmenden Befugnissen, um Maßnahmen zu ergreifen oder zu genehmigen, sowie die Kontaktinformationen der einzelnen Stakeholder.
4. Im Falle einer Eskalation sollte sie so lange fortgesetzt werden, bis das Teammitglied davon überzeugt ist, dass das Risiko durch entsprechende Maßnahmen der Führung gemindert wurde.
  - a. Eskalationen sollten Folgendes beinhalten:
    - i. Beschreibung der Situation und Art des Risikos
    - ii. Kritikalität der Situation
    - iii. Wer oder was betroffen ist
    - iv. Umfang der Auswirkungen
    - v. Dringlichkeit, falls eine Auswirkung eintritt

- vi. Vorgeschlagene Abhilfemaßnahmen und Risikominderungsplan
  - b. Schützen Sie Mitarbeiter, die ein Problem eskalieren. Führen Sie eine Richtlinie ein, die Teammitglieder vor Konsequenzen schützt, wenn sie an einen ablehnend eingestellten Entscheidungsträger oder Stakeholder eskalieren. Schaffen Sie Mechanismen, um solche Szenarien zu erkennen, und leiten Sie entsprechende Maßnahmen ein.
5. Fördern Sie eine Kultur der kontinuierlichen Verbesserung durch Feedback-Schleifen in allen Bereichen der Organisation. Feedback-Schleifen fungieren als kleine Eskalationen an die verantwortlichen Personen und identifizieren Verbesserungsmöglichkeiten, auch wenn eine Eskalation nicht erforderlich ist. Eine Kultur der kontinuierlichen Verbesserung zwingt alle dazu, proaktiver zu werden.
  6. Die Führung sollte regelmäßig an die Richtlinien, Standards und Mechanismen erinnern sowie an den Wunsch nach offener Eskalation und kontinuierlichen Feedback-Schleifen ohne Vergeltungsmaßnahmen jedweder Art.

Aufwand für den Implementierungsplan: Mittel

Ressourcen

Zugehörige bewährte Methoden:

- [OPS02-BP05 Es gibt Mechanismen, um Ergänzungen, Änderungen und Ausnahmen zu beantragen](#)

Zugehörige Dokumente:

- [Wie fördert man eine Kultur der kontinuierlichen Verbesserung und des Lernens von Andon- und Eskalationssystemen?](#)
- [Das Andon-Cord \(IT-Revolution\)](#)
- [AWS DevOps Leitlinien | Etablieren Sie klare Eskalationspfade und fördern Sie konstruktive Meinungsverschiedenheiten](#)

Zugehörige Videos:

- [Jeff Bezos erklärt, wie man Entscheidungen trifft \(und die Geschwindigkeit erhöht\)](#)
- [Toyota Product System: Anhalten der Produktion, ein Knopf und einer Andon-Elektroplatine](#)
- [Andon Cord in der Fertigung LEAN](#)



## Zugehörige Beispiele:

- [Arbeiten mit Eskalationsplänen in Incident Manager](#)

### OPS03-BP04 Die Kommunikation ist zeitnah, klar und umsetzbar

Die Führung ist für eine überzeugende und effektive Kommunikation zuständig, insbesondere wenn die Organisation vor der Einführung neuer Strategien, Technologien oder Arbeitsweisen steht. Führungskräfte sollten Erwartungen an alle Mitarbeiter stellen, damit sie auf die Unternehmensziele hinarbeiten können. Entwickeln Sie Kommunikationsmechanismen für die Bildung und Aufrechterhaltung des geforderten Bewusstseins in Teams, die für die Durchführung von Plänen verantwortlich sind, die von der Führung finanziert und unterstützt werden. Machen Sie sich die organisationsübergreifende Vielfalt zunutze und hören Sie sich verschiedene einzigartige Perspektiven aufmerksam an. Nutzen Sie diese Perspektive, um Innovation zu fördern, Ihre Annahmen in Frage zu stellen und das Risiko einer Verzerrung durch automatische Bestätigung zu reduzieren. Stärken Sie Inklusion, Vielfalt und Zugehörigkeit innerhalb Ihrer Teams, um nützliche Perspektiven zu gewinnen.

Gewünschtes Ergebnis: Ihre Organisation entwickelt Kommunikationsstrategien, um den Auswirkungen von Veränderungen auf die Organisation Rechnung zu tragen. Die Teams werden informiert und motiviert, weiter miteinander statt gegeneinander zu arbeiten. Einzelpersonen kennen die Bedeutung ihrer Rolle, um die angegebenen Ziele zu erreichen. E-Mail ist nur ein passiver Kommunikationsmechanismus und wird als solcher behandelt. Das Management verbringt Zeit mit seinen einzelnen Mitarbeitern, um ihnen ihre Verantwortung, die zu erledigenden Aufgaben und die Bedeutung ihrer Arbeit für die Gesamtmission zu vermitteln. Bei Bedarf binden Führungskräfte ihre Mitarbeiter an kleineren Veranstaltungsorten direkt ein, um Botschaften zu kommunizieren, und sie stellen sicher, dass diese Botschaften effektiv übermittelt werden. Die Organisation erfüllt oder übertrifft die Erwartungen der Führung mithilfe geeigneter Kommunikationsstrategien. Die Führung begrüßt und fördert unterschiedliche Meinungen innerhalb und zwischen Teams.

### Typische Anti-Muster:

- Ihre Organisation hat einen Fünf-Jahres-Plan für die Migration aller Workloads in AWS. Der Business Case für die Cloud beinhaltet die Modernisierung von 25 % aller Workloads, um die Vorteile der Serverless-Technologie zu nutzen. Der CIO vermittelt diese Strategie direkt unterstellten Mitarbeitern und erwartet von jeder Führungskraft, dass sie diese Präsentation ohne persönliche Kommunikation an Manager, Direktoren und einzelne Mitwirkende weiterleitet. Der CIO tritt zurück und erwartet von seiner Organisation, dass sie die neue Strategie umsetzt.

- Die Führung bietet oder nutzt keine Feedback-Mechanismen, und die Erwartungslücke wächst, was dazu führt, dass einzelne Projekte ins Stocken geraten.
- Sie werden gebeten, eine Änderung an Ihren Sicherheitsgruppen vorzunehmen, ohne konkrete Informationen über die Änderung zu erhalten oder darüber, welche Auswirkungen sie auf alle Workloads haben könnte und bis wann sie umzusetzen ist. Der Manager leitet eine E-Mail vom VP von weiter InfoSec und fügt die Nachricht „Make this happen“ hinzu.
- An Ihrer Migrationsstrategie wurden Änderungen vorgenommen, die die Anzahl der geplanten Modernisierungen von 25 auf 10 % reduzieren. Dies hat nachgelagerte Auswirkungen auf die Betriebsorganisation. Sie wurden nicht über diese strategische Änderung informiert und verfügen daher nicht über genügend qualifizierte Mitarbeiter, um einen größeren Lift-and-Shift-Aufwand von Workloads in AWS zu bewältigen.

Vorteile der Nutzung dieser bewährten Methode:

- Ihre Organisation ist über neue oder geänderte Strategien hinreichend informiert und die Mitarbeiter sind hochmotiviert, um sich gegenseitig dabei zu unterstützen, die von der Führung festgelegten Gesamtziele und Metriken zu erreichen.
- Es gibt Mechanismen und sie werden angewandt, um Teammitglieder rechtzeitig über bekannte Risiken und geplante Ereignisse zu informieren.
- Neue Arbeitsweisen (einschließlich Änderungen bzgl. Belegschaft, Organisation, Prozessen oder Technologien) werden zusammen mit den erforderlichen Fähigkeiten von der Organisation effektiver übernommen. Darüber hinaus erreicht Ihre Organisation schneller Geschäftsvorteile.
- Die Teammitglieder verfügen über die notwendigen Hintergrundinformationen zu den eingehenden Kommunikationen und können ihre Arbeit effektiver erledigen.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Hoch

Implementierungsleitfaden

Zur Implementierung dieser bewährten Methode müssen Sie mit Beteiligten aus der gesamten Organisation zusammenarbeiten, um Kommunikationsstandards zu vereinbaren. Machen Sie diese Standards in der Organisation bekannt. Bei allen wichtigen IT-Umstellungen kann ein etabliertes Planungsteam die Auswirkungen der Änderungen auf seine Mitarbeiter erfolgreicher bewältigen als eine Organisation, die diese Methode nicht anwendet. In größeren Organisationen können Veränderungen schwieriger umzusetzen sein, da es auf eine hohe Zustimmung aller einzelnen Mitarbeiter zu einer neuen Strategie ankommt. In Ermangelung eines solchen

Umstellungsplanungsteams trägt die Führung zu 100 % die Verantwortung für eine effektive Kommunikation. Wenn Sie ein Umstellungsplanungsteam einrichten, weisen Sie die Teammitglieder an, mit der gesamten Organisationsführung zusammenzuarbeiten, um eine effektive Kommunikation auf allen Ebenen zu definieren und zu gewährleisten.

### Kundenbeispiel

AnyCompany Retail hat sich für AWS Enterprise Support angemeldet und ist für seinen Cloud-Betrieb auf andere Drittanbieter angewiesen. Das Unternehmen nutzt Chat und Chatops als zentrales Kommunikationsmedium für seine betrieblichen Aktivitäten. Für Warnmeldungen und andere Informationen werden spezielle Kanäle genutzt. Wenn eine Maßnahme erforderlich ist, wird das erwartete Ergebnis klar formuliert, und in vielen Fällen gibt es ein Runbook oder Playbook dafür. Das Unternehmen verwendet einen Änderungskalender für die Planung größerer Änderungen an Produktionssystemen.

### Implementierungsschritte

1. Richten Sie innerhalb der Organisation ein Kernteam ein, das für die Erstellung und Initiierung von Kommunikationsplänen für Änderungen verantwortlich ist, die auf mehreren Ebenen innerhalb der Organisation stattfinden.
2. Fordern Sie Eigenverantwortlichkeit, um ein hohes Maß an Übersicht zu fördern. Geben Sie den einzelnen Teams die Möglichkeit, unabhängig voneinander Innovationen zu entwickeln, und sorgen Sie für einen ausgewogenen Einsatz einheitlicher Mechanismen, die das richtige Maß an Einsicht und Zielgerichtetheit ermöglichen.
3. Arbeiten Sie mit allen Stakeholdern in Ihrer Organisation zusammen, um Kommunikationsstandards, -methoden und -pläne zu vereinbaren.
4. Stellen Sie sicher, dass das zentrale Kommunikationsteam mit der Organisations- und Programmleitung zusammenarbeitet, um im Namen der Führungskräfte Botschaften an die zuständigen Mitarbeiter zu verfassen.
5. Entwickeln Sie strategische Kommunikationsmechanismen, um Veränderungen mithilfe von Ankündigungen, gemeinsamen Kalendern, Besprechungen mit allen Beteiligten und persönlichen Gesprächen oder one-on-one Methoden zu bewältigen, sodass die Teammitglieder die richtigen Erwartungen an die zu ergreifenden Maßnahmen haben.
6. Stellen Sie den erforderlichen Kontext, Details und die nötige Zeit bereit (wenn möglich), um festzustellen, ob Maßnahmen erforderlich sind. Wenn Maßnahmen erforderlich sind, identifizieren Sie die erforderlichen Maßnahmen und deren Auswirkungen.

7. Implementieren Sie Tools, die eine taktische Kommunikation fördern, z. B. interne Chats, E-Mails und Wissensmanagement.
8. Implementieren Sie Mechanismen, um zu messen und zu überprüfen, ob mit allen Kommunikationen die gewünschten Ergebnisse erreicht werden.
9. Richten Sie eine Feedback-Schleife ein, die die Effektivität aller Kommunikationen misst, insbesondere wenn darin der Widerstand gegen Veränderungen in der Organisation thematisiert wird.
10. Richten Sie für alle AWS-Konten [alternative Ansprechpartner](#) für Abrechnung, Sicherheit und Betrieb ein. Idealerweise sollte es sich bei diesen Kontakten um E-Mail-Verteilerlisten und nicht um Einzelpersonen handeln.
11. Erstellen Sie einen Kommunikationsplan für die Eskalation und die umgekehrte Eskalation, um mit Ihren internen und externen Teams, einschließlich AWS Support und anderen Drittanbietern, in Kontakt zu treten.
12. Initiieren Sie Kommunikationsstrategien und setzen Sie sie während der gesamten Laufzeit jedes Transformationsprogramms konsequent um.
13. Priorisieren Sie Maßnahmen, die nach Möglichkeit wiederholbar sind, um sie sicher und in großem Maßstab zu automatisieren.
14. Wenn Kommunikation in Szenarien mit automatisierten Maßnahmen erforderlich ist, sollte die Kommunikation hauptsächlich der Information der Teams oder Audits dienen oder Teil des Änderungsverwaltungsprozesses sein.
15. Analysieren Sie die Kommunikation Ihrer Warnsysteme auf Fehlalarme oder Warnmeldungen, die ständig generiert werden. Entfernen Sie diese Warnmeldungen oder ändern Sie sie so, dass sie nur ausgelöst werden, wenn menschliches Eingreifen erforderlich ist. Stellen Sie ein Runbook oder Playbook bereit, wenn eine Warnmeldung ausgelöst wird.
  - a. Sie können [AWS Systems Manager-Dokumente](#) verwenden, um Playbooks und Runbooks für Warnmeldungen zu erstellen.
16. Es gibt Mechanismen zur Benachrichtigung über Risiken oder geplante Ereignisse auf eine klare und unterstützende Weise mit ausreichend Zeit für geeignete Maßnahmen. Verwenden Sie E-Mail-Listen oder Chat-Kanäle zum Senden von Benachrichtigungen vor geplanten Ereignissen.
  - a. [AWS Chatbot](#) kann verwendet werden, um Warnmeldungen zu senden und auf Ereignisse innerhalb der Messaging-Plattform Ihrer Organisation zu reagieren.
17. Stellen Sie eine zugängliche Informationsquelle bereit, der geplante Ereignisse zu entnehmen sind. Stellen Sie Benachrichtigungen zu geplanten Ereignissen vom gleichen System bereit.

- a. [AWS Systems Manager Manager-Änderungskalender](#) kann verwendet werden, um Änderungsfenster zu erstellen, in denen Änderungen vorgenommen werden können. Dadurch werden Teammitglieder benachrichtigt, wann sie in sicherer Weise Änderungen vornehmen können.
18. Überwachen Sie Benachrichtigungen zu Schwachstellen und Patch-Informationen, um bestehende Schwachstellen und potenzielle Risiken im Zusammenhang mit den Komponenten Ihrer Workloads zu verstehen. Stellen Sie Benachrichtigungen für die Teammitglieder bereit, damit sie Maßnahmen ergreifen können.
- a. Sie können [AWS -Sicherheitsmitteilungen](#) abonnieren, um über Schwachstellen in AWS benachrichtigt zu werden.
19. Berücksichtigen unterschiedlicher Meinungen und Perspektiven: Ermutigen Sie alle dazu, Beiträge zu leisten. Geben Sie unterrepräsentierten Gruppen die Möglichkeit, sich in die Kommunikation einzubringen. Rotieren Sie die Rollen und Zuständigkeiten in Meetings.
- a. Erweitern von Rollen und Zuständigkeiten: Bieten Sie Teammitgliedern die Möglichkeit, Rollen zu übernehmen, die ihnen fremd sind. Auf diese Weise können sie Erfahrung sammeln und neue Perspektiven durch die Rolle und den resultierenden Austausch mit neuen Teammitgliedern gewinnen, zu denen sie möglicherweise andernfalls keinen Kontakt hätten. Nicht zuletzt können sie die neue Rolle und die Teammitglieder mit ihren Erfahrungen und Perspektiven bereichern. Mit zunehmender Erfahrung werden Sie aufkommende Geschäftsmöglichkeiten oder neue Verbesserungsmöglichkeiten identifizieren. Rotieren Sie allgemeine Aufgaben zwischen den Mitgliedern innerhalb eines Teams, die normalerweise anderen Tätigkeiten nachgehen, damit sie deren Anforderungen und Auswirkungen verstehen.
  - b. Bereitstellen einer sicheren und freundlichen Umgebung: Richten Sie Richtlinien und Kontrollen zum Schutz der geistigen und physischen Sicherheit der Teammitglieder in Ihrer Organisation ein. Die Teammitglieder müssen ohne Angst vor Vergeltungsmaßnahmen zusammenarbeiten können. Wenn sich Teammitglieder sicher und willkommen fühlen, ist die Wahrscheinlichkeit höher, dass sie engagiert und produktiv bleiben. Je vielfältiger Ihre Organisation ist, desto besser verstehen Sie die Personen, die Sie unterstützen, einschließlich Ihrer Kunden. Wenn Ihre Teammitglieder zufrieden sind, ihre Meinung sagen können und sich ernst genommen fühlen, steigt die Wahrscheinlichkeit, dass sie wertvolle Erkenntnisse mitteilen (z. B. Marketingmöglichkeiten, erforderliche Maßnahmen zur Barrierefreiheit, unerschlossene Marktsegmente, unbehandelte Risiken in Ihrer Umgebung).
  - c. Ermuntern von Teammitgliedern zu vollständigen Teilnahme: Stellen Sie die Ressourcen bereit, die Ihre Mitarbeiter benötigen, um alle arbeitsbezogenen Tätigkeiten auszuführen. Teammitglieder haben Fähigkeiten entwickelt, mit denen sie ihre täglichen Herausforderungen

meistern. Diese einzigartigen Fähigkeiten können für Ihre Organisation von großem Vorteil sein. Wenn Sie die Teammitglieder mit den notwendigen Ressourcen ausstatten, können Sie den Nutzen ihrer Beiträge maximieren.

## Ressourcen

### Zugehörige bewährte Methoden:

- [OPS03-BP01 Unterstützen Sie Führungskräfte](#)
- [OPS07-BP03 Verwenden Sie Runbooks, um Verfahren durchzuführen](#)
- [OPS07-BP04 Verwenden Sie Playbooks, um Probleme zu untersuchen](#)

### Zugehörige Dokumente:

- [AWS -Blog-Post | Rechenschaftspflicht und Befähigung sind der Schlüssel zu leistungsstarken agilen Organisationen](#)
- [AWS Executive Insights | Lernen Sie, Innovation statt Komplexität zu skalieren | Single-Threaded Leaders](#)
- [AWS -Sicherheitsberichte](#)
- [Öffnen CVE](#)
- [AWS Support App in Slack zur Verwaltung von Support-Fällen](#)
- [Verwalte AWS Ressourcen in deinen Slack-Kanälen mit AWS Chatbot](#)

### Zugehörige Beispiele:

- [Well-Architected Labs: Bestands- und Patch-Verwaltung \(Ebene 100\)](#)

### Zugehörige Services:

- [AWS Chatbot](#)
- [AWS Systems Manager Manager-Änderungskalender](#)
- [AWS Systems Manager Manager-Dokumente](#)

## OPS03-BP05 Experimentieren wird gefördert

Experimente können Katalysatoren für die Umsetzung von Ideen in Produkte und Funktionen sein. Sie beschleunigen Lernprozesse und halten Teammitglieder interessiert und engagiert. Team-Mitglieder sollten oft experimentieren, um Innovationen voranzubringen. Selbst nicht erwünschte Ergebnisse bieten den Vorteil, dass man dadurch weiß, wie man nicht vorgehen sollte. Teammitglieder werden nicht für erfolgreiche Experimente mit unerwünschten Ergebnissen bestraft.

### Gewünschtes Ergebnis:

- Ihre Organisation ermutigt zum Experimentieren, um Innovationen voranzubringen.
- Experimente werden genutzt, um daraus zu lernen.

### Typische Anti-Muster:

- Sie möchten einen A/B-Test durchführen, es gibt jedoch keinen Mechanismus für das Experiment. Sie stellen eine UI-Änderung bereit, ohne diese testen zu können. Dies beeinträchtigt den Kundenkomfort.
- Ihr Unternehmen verfügt nur über eine Staging- und eine Produktionsumgebung. Es gibt keine Sandbox-Umgebung zum Experimentieren mit neuen Funktionen oder Produkten, weshalb Sie in der Produktionsumgebung experimentieren müssen.

### Vorteile der Nutzung dieser bewährten Methode:

- Experimente bringen Innovationen voran.
- Mithilfe von Experimenten können Sie schneller auf Feedback reagieren.
- Ihre Organisation entwickelt eine Lernkultur.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel

### Implementierungsleitfaden

Experimente sollten in sicherer Weise durchgeführt werden. Nutzen Sie mehrere Umgebungen für Experimente, ohne dabei Produktionsressourcen in Gefahr zu bringen. Nutzen Sie A/B-Tests und Feature-Flags für Testexperimente. Geben Sie Teammitgliedern die Möglichkeit, Experimente in einer Sandbox-Umgebung durchzuführen.

### Kundenbeispiel

AnyCompany Der Einzelhandel fördert das Experimentieren. Teammitglieder können 20 % ihrer wöchentlichen Arbeitszeit für Experimente oder zum Erlernen neuer Technologien nutzen. Es gibt eine Sandbox-Umgebung zum Ausprobieren von Innovationen. Für neue Funktionen werden A/B-Tests verwendet, um sie mit realem Benutzerfeedback zu prüfen.

### Implementierungsschritte

1. Arbeiten Sie mit Führungskräften aus dem gesamten Unternehmen zusammen, um Experimente zu unterstützen. Teammitglieder sollten aufgefordert werden, Experimente in sicherer Weise durchzuführen.
2. Stellen Sie Ihren Teammitgliedern eine Umgebung zur Verfügung, in der sie in sicherer Weise experimentieren können. Sie müssen Zugriff auf eine Umgebung haben, die der Produktionsumgebung stark ähnelt.
  - a. Sie können eine separate Sandbox-Umgebung zum Experimentieren verwenden AWS-Konto , um eine Sandbox-Umgebung zu erstellen. [AWS Control Tower](#) kann verwendet werden, um diese Konten bereitzustellen.
3. Verwenden Sie Feature-Flags und A/B-Tests, um in sicherer Weise zu experimentieren und Benutzer-Feedback einzuholen.
  - a. [AWS AppConfig Feature Flags](#) bietet die Möglichkeit, Feature-Flags zu erstellen.
  - b. [Amazon kann CloudWatch offensichtlich](#) verwendet werden, um A/B-Tests über einen begrenzten Einsatz durchzuführen.
  - c. Mithilfe von [AWS Lambda -Versionen](#) können Sie eine neue Version einer Funktion für Beta-Tests bereitstellen.

Aufwand für den Implementierungsplan: Hoch. Die Bereitstellung einer Umgebung für Teammitglieder, in der sie in sicherer Weise experimentieren können, kann erhebliche Investitionen erfordern. Möglicherweise muss auch der Anwendungscode modifiziert werden, um Feature-Flags verwenden oder A/B-Tests unterstützen zu können.

### Ressourcen

Zugehörige bewährte Methoden:

- [OPS11-BP02 Führen Sie eine Analyse nach dem Vorfall durch](#) – Das Lernen aus Vorfällen ist neben Experimenten ein wichtiger Motor für Innovation.
- [OPS11-BP03 Implementieren Sie Feedback-Schleifen](#) – Feedbackschleifen sind ein wichtiger Bestandteil von Experimenten.



## Zugehörige Dokumente:

- [Ein Einblick in die Amazon-Kultur: Experimente, Misserfolge und Kundenorientierung](#)
- [Bewährte Methoden für die Erstellung und Verwaltung von Sandbox-Konten in AWS](#)
- [Schaffen Sie eine Kultur des Experimentierens, die durch die Cloud ermöglicht wird](#)
- [Wir ermöglichen Experimente und Innovationen in der Cloud bei SulAm Érica Seguros](#)
- [Mehr experimentieren, weniger scheitern](#)
- [Organisieren Sie Ihre AWS Umgebung mithilfe mehrerer Konten — Sandbox OU](#)
- [Verwenden von AWS AppConfig Feature-Flags](#)

## Zugehörige Videos:

- [AWS Auf Air ft. Amazon CloudWatch Evidently | Veranstaltungen AWS](#)
- [AWS Auf dem Air San Fran Summit 2022 ft. AWS AppConfig Integration von Feature-Flags mit Jira](#)
- [AWS re:Invent 2022 — Ein Deployment ist kein Release: Steuern Sie Ihre Launches mit Feature-Flags \(05-R\) BOA3](#)
- [Programmgesteuertes Erstellen Sie ein mit AWS-KontoAWS Control Tower](#)
- [Richten Sie eine AWS Umgebung mit mehreren Konten ein, die Best Practices verwendet für AWS Organizations](#)

## Zugehörige Beispiele:

- [AWS Sandbox für Innovationen](#)
- [End-to-endPersonalisierung 101 für E-Commerce](#)

## Zugehörige Services:

- [Amazon CloudWatch offenbar](#)
- [AWS AppConfig](#)
- [AWS Control Tower](#)

OPS03-BP06 Teammitglieder werden ermutigt, ihre Fähigkeiten zu erhalten und auszubauen

Teams müssen ihre Fähigkeiten ausbauen, um neue Technologien nutzen und mit veränderten Anforderungen und Aufgaben Ihrer Workloads umgehen zu können. Neue Fähigkeiten im Umgang mit neuen Technologien erhöhen oftmals die Zufriedenheit der Teammitglieder und ermöglichen Innovationen. Unterstützen Sie Ihre Teammitglieder beim Erlangen und Bewahren von Branchenzertifizierungen, mit denen ihre wachsenden Fähigkeiten bestätigt und anerkannt werden. Führen Sie funktionsübergreifende Trainings durch, um den Wissenstransfer zu fördern und das Risiko signifikanter Auswirkungen zu reduzieren, wenn Sie qualifizierte und erfahrene Teammitglieder mit kritischem Wissen verlieren. Schaffen Sie spezielle strukturierte Lernzeiten.

AWS bietet Ressourcen, darunter das [AWS Getting Started Resource Center](#), [AWS Blogs](#), [AWS Online-Technikgespräche](#), [AWS Veranstaltungen und Webinare](#) sowie die [AWS Well-Architected Labs](#), die Anleitungen, Beispiele und detaillierte Anleitungen zur Schulung Ihrer Teams bieten.

Ressourcen wie [AWS Support](#), [AWS re:Post](#), [AWS Support Center](#) und die [AWS Dokumentation](#) helfen dabei, technische Hindernisse zu beseitigen und den Betrieb zu verbessern. Wenden Sie sich an das AWS Support Center, um AWS Support Hilfe bei Ihren Fragen zu erhalten.

AWS teilt auch bewährte Verfahren und Muster, die wir durch den Betrieb von [The Amazon Builders' Library](#) gelernt haben, sowie eine Vielzahl anderer nützlicher Lehrmaterialien AWS im [AWS Blog](#) und [im offiziellen AWS Podcast](#).

[AWS Training und Die Zertifizierung](#) umfasst kostenlose Schulungen in Form von digitalen Kursen zum Selbststudium sowie Lernpläne für Rollen oder Fachbereiche. Sie können sich auch für von Dozenten geleitete Schulungen anmelden, um die Entwicklung der Fähigkeiten Ihrer Teams weiter zu unterstützen. AWS

Gewünschtes Ergebnis: Ihre Organisation bewertet ständig Qualifikationslücken und schließt sie mit strukturierten Budgets und Investitionen. Die Teams ermutigen und unterstützen ihre Mitglieder durch Weiterbildungsaktivitäten wie den Erwerb führender Branchenzertifizierungen. Teams nutzen spezielle Programme zum gemeinsamen Wissensaustausch wie Immersionstage lunch-and-learns, Hackathons und Gamedays. Ihr Unternehmen behält seine Wissenssysteme up-to-date bei, die für schulungsübergreifende Teammitglieder relevant sind, einschließlich Onboarding-Schulungen für neue Mitarbeiter.

Typische Anti-Muster:

- Aufgrund eines fehlenden strukturierten Trainingsprogramms und Budgets entstehen in den Teams Unsicherheit und Zweifel, wenn sie versuchen, mit der technologischen Entwicklung Schritt zu halten, was letztlich zu einer erhöhten Personalabwanderung führt.
- Im Rahmen der Umstellung darauf AWS weist Ihr Unternehmen Qualifikationslücken und unterschiedliche Cloud-Kenntnisse der einzelnen Teams auf. Aufgrund fehlender Fortbildungsprogramme sehen sich die Teams mit der veralteten und ineffizienten Verwaltung der Cloud-Umgebung überfordert, was zu einer Mehrbelastung der Mitarbeiter führt. Diese erschwerten Arbeitsbedingungen erhöhen die Unzufriedenheit der Mitarbeiter.

Vorteile der Nutzung dieser bewährten Methode: Wenn Ihre Organisation bewusst in die Verbesserung der Fähigkeiten der Teams investiert, trägt dies auch dazu bei, die Einführung und Optimierung der Cloud zu beschleunigen und zu skalieren. Gezielte Lernprogramme fördern Innovationen und stärken die operativen Fähigkeiten der Teams, um auf Ereignisse vorbereitet zu sein. Teams investieren bewusst in die Implementierung und Weiterentwicklung von bewährten Methoden. Die Arbeitsmoral im Team ist hoch und die Teammitglieder sind stolz auf ihren Beitrag zum Unternehmen.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel

### Implementierungsleitfaden

Investieren Sie kontinuierlich in die berufliche Weiterentwicklung Ihrer Teams, um neue Technologien einzuführen, Innovationen voranzutreiben und mit den Veränderungen der Anforderungen und Verantwortlichkeiten Schritt zu halten, um Ihre Workloads zu unterstützen.

### Implementierungsschritte

1. Nutzen Sie strukturierte Cloud-Advocacy-Programme: [AWS Skills Guild](#) bietet beratende Schulungen an, um das Vertrauen in die eigenen Cloud-Fähigkeiten zu stärken und eine Kultur des kontinuierlichen Lernens zu fördern.
2. Bereitstellen von Ressourcen für die Weiterbildung: Sorgen Sie für eine spezielle strukturierte Lernzeit, Schulungsmaterialien und Laborressourcen. Unterstützen Sie die Teilnahme an Konferenzen und professionellen Organisationen, die Möglichkeiten zum Lernen von Lehrenden und anderen Fachleuten bieten. Stellen Sie für Ihre Junior-Teammitglieder den Kontakt zu erfahreneren Teammitgliedern als Mentoren her oder ermöglichen Sie Junior-Teammitgliedern, ihnen bei der Arbeit zuzusehen, um sich mit ihren Methoden und Fähigkeiten vertraut zu machen. Ermutigen Sie dazu, auch etwas über Inhalte zu lernen, die nicht direkt mit der Arbeit zusammenhängen, um den Horizont zu erweitern.

3. Ermuntern Sie zur Nutzung von technischen Ressourcen für Experten: Nutzen Sie Ressourcen wie [AWS re:Post](#), um Zugang zu kuratiertem Wissen und einer lebendigen Community zu erhalten.
4. Aufbau und Pflege eines up-to-date Wissensarchivs: Nutzen Sie Plattformen für den Wissensaustausch wie Wikis und Runbooks. Erstellen Sie mit [AWS re:Post Private](#) Ihre eigene wiederverwendbare Quelle für Expertenwissen, um die Zusammenarbeit zu optimieren, die Produktivität zu steigern und das Onboarding von Mitarbeitern zu beschleunigen.
5. Teamschulung und teamübergreifende Zusammenarbeit: Planen Sie den Weiterbildungsbedarf Ihrer Teammitglieder ein. Schaffen Sie Gelegenheiten für die Teammitglieder, (vorübergehend oder dauerhaft) in anderen Teams zu arbeiten, damit sie untereinander Fähigkeiten und bewährte Methoden austauschen können, wovon letztendlich die gesamte Organisation profitiert.
6. Unterstützen beim Erlangen und Bewahren von Branchenzertifizierungen: Unterstützen Sie Ihre Teammitglieder beim Erlangen und Bewahren von Branchenzertifizierungen, durch die das Gelernte bestätigt wird und die Erfolge anerkannt werden.

Aufwand für den Implementierungsplan: Hoch

Ressourcen

Zugehörige bewährte Methoden:

- [OPS03-BP01 Unterstützen Sie Führungskräfte](#)
- [OPS11-BP04 Führen Sie Wissensmanagement durch](#)

Zugehörige Dokumente:

- [AWS -Whitepaper | Cloud Adoption Framework: Die Mitarbeiterperspektive](#)
- [Investitionen in kontinuierliches Lernen, um die Zukunft Ihrer Organisation zu fördern](#)
- [AWS Skills Guild](#)
- [AWS Training und Zertifizierung](#)
- [AWS Support](#)
- [AWS Re:Post](#)
- [AWS -Ressourcencenter für erste Schritte](#)
- [AWS -Blogs](#)
- [AWS Cloud -Compliance](#)

- [AWS -Dokumentation:](#)
- [Der offizielle Podcast AWS.](#)
- [AWS Online Tech Talks](#)
- [AWS Veranstaltungen und Webinare](#)
- [AWS Well-Architected Labs](#)
- [Die Amazon Builders' Library](#)

Zugehörige Videos:

- [AWS re:Invent 2023 | Weiterbildung mit der Geschwindigkeit der Cloud: Aus Mitarbeitern Unternehmer machen](#)
- [WS re:Invent 2023 | Aufbau einer Kultur der Neugier durch Gamification](#)

OPS03-BP07 Ressourcenteams angemessen

Setzen Sie die richtige Anzahl kompetenter Teammitglieder ein und stellen Sie Tools und Ressourcen zur Verfügung, um Ihre Workload-Anforderungen zu erfüllen. Eine Überlastung der Teammitglieder erhöht das Risiko menschlicher Fehler. Investitionen in Tools und Ressourcen wie Automatisierung können die Effektivität Ihres Teams steigern und es dabei unterstützen, eine größere Anzahl von Workloads zu bewältigen, ohne zusätzliche Kapazitäten zu benötigen.

Gewünschtes Ergebnis:

- Sie haben Ihr Team entsprechend personell ausgestattet, um die Fähigkeiten zu erwerben, die es benötigt, um Workloads AWS gemäß Ihrem Migrationsplan zu verwalten. Da sich Ihr Team im Laufe Ihres Migrationsprojekts immer weiter vergrößert hat, hat es Kenntnisse in den AWS Kerntechnologien erworben, die das Unternehmen bei der Migration oder Modernisierung seiner Anwendungen einsetzen will.
- Sie haben Ihren Personalplan sorgfältig abgestimmt, um Ressourcen mithilfe von Automatisierung und Workflows effizient zu nutzen. Ein kleineres Team kann jetzt im Auftrag der Anwendungsentwicklungsteams mehr Infrastruktur verwalten.
- Angesichts sich ändernder betrieblicher Prioritäten werden Personalengpässe proaktiv erkannt, um den Erfolg von Geschäftsinitiativen zu sichern.
- Betriebsmetriken, die auf operative Schwierigkeiten (wie Ermüdung des Bereitschaftsdienstes oder übermäßiges Telefonieren) hinweisen, werden überprüft, um eine Überforderung der Mitarbeiter zu vermeiden.

## Typische Anti-Muster:

- Ihre Mitarbeiter haben ihre AWS Fähigkeiten nicht erweitert, als Sie sich Ihrem mehrjährigen Cloud-Migrationsplan nähern, was die Unterstützung der Arbeitslast gefährdet und die Arbeitsmoral der Mitarbeiter beeinträchtigt.
- Ihre gesamte IT-Organisation stellt sich auf agile Arbeitsweisen um. Das Unternehmen priorisiert das Produktportfolio und legt Metriken dafür fest, welche Features zuerst entwickelt werden müssen. Ihr agiler Prozess erfordert nicht, dass Teams ihren Arbeitsplänen Story Points zuweisen. Daher ist es unmöglich zu wissen, welche Kapazitäten für den nächsten Arbeitsschritt erforderlich sind oder ob Sie über die dafür notwendigen Fähigkeiten verfügen.
- Sie beauftragen einen AWS Partner, Ihre Workloads zu migrieren, und Sie haben keinen Plan zur Umstellung auf den Support für Ihre Teams, sobald der Partner das Migrationsprojekt abgeschlossen hat. Ihre Teams haben Schwierigkeiten, die Workloads effizient und effektiv zu unterstützen.

Vorteile der Nutzung dieser bewährten Methode: In Ihrer Organisation gibt es Teammitglieder, die für die Unterstützung der Workloads qualifiziert sind. Die Ressourcenzuweisung kann an sich ändernde Prioritäten angepasst werden, ohne die Leistung zu beeinträchtigen. Somit können die Teams die Workloads effizient unterstützen und gleichzeitig mehr Zeit mit Innovationen für Kunden aufwenden, was wiederum die Mitarbeiterzufriedenheit erhöht.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel

## Implementierungsleitfaden

Die Ressourcenplanung für Ihre Cloud-Migration sollte auf einer Organisationsebene erfolgen, die Ihrem Migrationsplan sowie dem gewünschten Betriebsmodell entspricht, das zur Unterstützung Ihrer neuen Cloud-Umgebung implementiert wird. Dies erfordert nicht zuletzt ein umfassendes Verständnis, welche Cloud-Technologien für die Geschäfts- und Anwendungsentwicklungsteams eingesetzt werden. Die Infrastruktur- und Betriebsleitung sorgt für eine Analyse von Qualifikationslücken, Schulungen und die Rollendefinition für Ingenieure, die die Cloud-Einführung leiten.

## Implementierungsschritte

1. Definieren Sie Erfolgskriterien für den Erfolg des Teams anhand relevanter Betriebsmetriken wie der Mitarbeiterproduktivität (z. B. Kosten für die Unterstützung einer Workload oder Arbeitsstunden, die Mitarbeiter bei Vorfällen aufgewendet haben).

2. Definieren Sie Mechanismen zur Planung und Überprüfung der Kapazität von Ressourcen, um sicherzustellen, dass bei Bedarf ausreichend qualifizierte Ressourcen verfügbar sind und deren Zahl im Laufe der Zeit angepasst werden kann.
3. Schaffen Sie Mechanismen (z. B. das Senden einer monatlichen Umfrage an Teams), um arbeitsbezogene Herausforderungen zu verstehen, die sich auf Teams auswirken (z. B. zunehmende Verantwortlichkeiten, technologische Veränderungen, Personalabwanderung oder wachsende Anzahl unterstützter Kunden).
4. Verwenden Sie diese Mechanismen, um mit Teams in Kontakt zu treten und Trends zu erkennen, die zu Problemen bei der Mitarbeiterproduktivität beitragen können. Wenn sich äußere Faktoren negativ auf Ihre Teams auswirken, bewerten Sie die Ziele neu und passen Sie sie entsprechend an. Identifizieren Sie Hindernisse für den Fortschritt Ihres Teams.
5. Prüfen Sie regelmäßig, ob Ihre derzeit vorhandenen Ressourcen noch ausreichen oder ob zusätzliche Ressourcen benötigt werden, und nehmen Sie entsprechende Anpassungen an den Support-Teams vor.

Aufwand für den Implementierungsplan: Mittel

Ressourcen

Zugehörige bewährte Methoden:

- [OPS03-BP06 Die Teammitglieder werden ermutigt, ihre Fähigkeiten beizubehalten und auszubauen](#)
- [OPS09-BP03 Überprüfen Sie die Betriebskennzahlen und priorisieren Sie Verbesserungen](#)
- [OPS10-BP01 Verwenden Sie einen Prozess für das Ereignis-, Vorfall- und Problemmanagement](#)
- [OPS10-BP07 Automatisieren Sie Reaktionen auf Ereignisse](#)

Zugehörige Dokumente:

- [AWS Cloud Adoptionsrahmen: Aus der Perspektive der Menschen](#)
- [Transformation zu einem zukunftsfähigen Unternehmen](#)
- [Priorisieren der Fähigkeiten Ihrer Mitarbeiter, um das Unternehmenswachstum voranzutreiben](#)
- [Leistungsstarke Organisation – das Zwei-Pizzen-Team von Amazon](#)
- [Wie Unternehmen mit umfassender Cloud-Erfahrung erfolgreich sind](#)

# Vorbereitung

## Fragen

- [OPS4. Wie implementieren Sie die Beobachtbarkeit in Ihrer Workload?](#)
- [OPS5. Wie können Sie Fehler reduzieren, die Fehlerbehebung erleichtern und den Ablauf bis zur Produktion verbessern?](#)
- [OPS6. Wie können Sie Bereitstellungsrisiken eindämmen?](#)
- [OPS7. Wie bringen Sie in Erfahrung, ob Sie für die Unterstützung eines Workloads bereit sind?](#)

## OPS4. Wie implementieren Sie die Beobachtbarkeit in Ihrer Workload?

Implementieren Sie Beobachtbarkeit in Ihre Workload, damit Sie deren Zustand verstehen und datengesteuerte Entscheidungen auf der Grundlage von Geschäftsanforderungen treffen können.

## Bewährte Methoden

- [OPS04-BP01 Identifizieren Sie die wichtigsten Leistungsindikatoren](#)
- [OPS04-BP02 Implementieren Sie Anwendungstelemetrie](#)
- [OPS04-BP03 Implementieren Sie Benutzererlebnis-Telemetrie](#)
- [OPS04-BP04 Implementieren Sie Abhängigkeitstelemetrie](#)
- [OPS04-BP05 Implementieren Sie verteiltes Tracing](#)

## OPS04-BP01 Identifizieren Sie die wichtigsten Leistungsindikatoren

Die Implementierung von Beobachtbarkeit in Ihrer Workload beginnt damit, ihren Status zu verstehen und datengestützte Entscheidungen auf der Grundlage der geschäftlichen Anforderungen zu treffen. Eine der wirksamsten Methoden, um sicherzustellen, dass die Überwachungstätigkeiten und die Unternehmensziele aufeinander abgestimmt werden, ist die Definition und Überwachung zentraler Leistungsindikatoren (KPIs).

Gewünschtes Ergebnis: Effiziente Beobachtbarkeitspraktiken, die eng an den Geschäftszielen ausgerichtet sind und sicherstellen, dass die Überwachungsanstrengungen stets greifbaren Geschäftsergebnissen dienen.

## Typische Anti-Muster:



- **UndefiniertKPIs:** Die Arbeit ohne klare Angaben KPIs kann dazu führen, dass zu viel oder zu wenig überwacht wird und wichtige Signale fehlen.
- **StatischKPIs:** Es wird nicht wiederholt oder verfeinertKPIs, wenn sich die Arbeitslast oder die Geschäftsziele ändern.
- **Fehlausrichtung:** Konzentration auf technische Metriken, die nicht direkt mit Geschäftsergebnissen korrelieren oder schwieriger mit realen Problemen zu korrelieren sind.

Vorteile der Nutzung dieser bewährten Methode:

- **Einfache Identifizierung von Problemen:** In Unternehmen KPIs treten Probleme häufig deutlicher zutage als bei technischen Kennzahlen. Ein Einbruch in einem Unternehmen KPI kann ein Problem effektiver lokalisieren als die Analyse zahlreicher technischer Kennzahlen.
- **Geschäftsausrichtung:** Es wird sichergestellt, dass die Überwachungsaktivitäten die Geschäftsziele direkt unterstützen.
- **Effizienz:** Es erfolgt eine Priorisierung der Ressourcen für die Überwachung und die Konzentration auf wichtige Metriken.
- **Proaktivität:** Probleme werden erkannt und gelöst, bevor sie weitreichende Auswirkungen auf das Geschäft haben.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Hoch

Implementierungsleitfaden

Um die Arbeitslast effektiv zu definieren: KPIs

1. **Beginnen Sie mit den Geschäftsergebnissen:** Bevor Sie sich mit Metriken befassen, sollten Sie sich mit den gewünschten Geschäftsergebnissen vertraut machen. Sind es höhere Umsätze, mehr Benutzerinteraktionen oder schnellere Reaktionszeiten?
2. **Stimmen Sie technische Metriken auf Geschäftsziele ab:** Nicht alle technischen Metriken wirken sich direkt auf die Geschäftsergebnisse aus. Identifizieren Sie diejenigen, die dies tun, aber es ist oft einfacher, ein Problem mithilfe eines Unternehmens zu identifizierenKPI.
3. **Verwenden Sie [Amazon CloudWatch](#):** CloudWatch Employ, um Kennzahlen zu definieren und zu überwachen, die Ihren entsprechenKPIs.
4. **Regelmäßige Überprüfung und AktualisierungKPIs:** Sorgen Sie dafür, dass Ihre Daten KPIs relevant sind, wenn sich Ihre Arbeitslast und Ihr Unternehmen weiterentwickeln.

5. Stakeholder einbeziehen: Beziehen Sie sowohl technische als auch geschäftliche Teams in die Definition und Überprüfung mit einKPIs.

Aufwand für den Implementierungsplan: Mittel

Ressourcen

Zugehörige bewährte Methoden:

- [the section called “OPS04-BP02 Implementieren Sie die Anwendungstelemetrie”](#)
- [the section called “OPS04-BP03 Implementieren Sie Telemetrie für die Benutzererfahrung”](#)
- [the section called “OPS04-BP04 Implementieren Sie Abhängigkeitstelemetrie”](#)
- [the section called “OPS04-BP05 Implementieren Sie die verteilte Ablaufverfolgung”](#)

Zugehörige Dokumente:

- [AWS Bewährte Verfahren zur Beobachtbarkeit](#)
- [CloudWatch Benutzerleitfaden](#)
- [AWS Kurs Observability Skill Builder](#)

Zugehörige Videos:

- [Entwicklung einer Beobachtbarkeitsstrategie](#)

Zugehörige Beispiele:

- [Workshop zur Beobachtbarkeit](#)

### OPS04-BP02 Implementieren Sie Anwendungstelemetrie

Anwendungstelemetrie dient als Grundlage für die Beobachtbarkeit Ihres Workloads. Die ausgegebene Telemetrie muss unbedingt umsetzbare Erkenntnisse zum Status Ihrer Anwendung und zum Erreichen sowohl technischer als auch geschäftlicher Ergebnisse liefern. Von der Problembehebung über die Messung der Auswirkungen einer neuen Funktion bis hin zur Sicherstellung der Abstimmung mit den wichtigsten Unternehmensleistungsindikatoren (KPIs) — die Anwendungstelemetrie gibt Aufschluss darüber, wie Sie Ihre Workloads aufbauen, betreiben und weiterentwickeln.

Metriken, Protokolle und Traces bilden die drei wichtigsten Säulen der Beobachtbarkeit. Sie dienen als Diagnosetools, die den Status Ihrer Anwendung beschreiben. Im Laufe der Zeit helfen sie bei der Erstellung von Baselines und der Identifizierung von Anomalien. Um jedoch sicherzustellen, dass die Überwachungsaktivitäten und die Geschäftsziele aufeinander abgestimmt sind, ist es von entscheidender Bedeutung, diese zu definieren und zu überwachen. KPIs Unternehmen machen es KPIs oft einfacher, Probleme zu identifizieren als nur technische Kennzahlen.

Andere Telemetriearten, wie die Überwachung realer Benutzer (RUM) und synthetische Transaktionen, ergänzen diese primären Datenquellen. RUM bietet Einblicke in Benutzerinteraktionen in Echtzeit, während synthetische Transaktionen potenzielles Benutzerverhalten simulieren und so helfen, Engpässe zu erkennen, bevor echte Benutzer darauf stoßen.

Gewünschtes Ergebnis: Sie erzielen umsetzbare Erkenntnisse zur Leistung Ihres Workloads. Diese Erkenntnisse ermöglichen es Ihnen, proaktive Entscheidungen zur Leistungsoptimierung zu treffen, eine höhere Workload-Stabilität zu erreichen, CI/CD-Prozesse zu rationalisieren und Ressourcen effektiv zu nutzen.

Typische Anti-Muster:

- Unvollständige Beobachtbarkeit: Wenn die Beobachtbarkeit nicht auf jeder Ebene der Workload berücksichtigt wird, führt dies zu blinden Flecken, die wichtige Erkenntnisse über Systemleistung und Verhalten verschleiern können.
- Fragmentierte Datenansicht: Wenn Daten über mehrere Tools und Systeme verteilt sind, wird es schwierig, einen ganzheitlichen Überblick über den Zustand und die Leistung Ihrer Workloads zu behalten.
- Von Benutzern gemeldete Probleme: Ein Zeichen dafür, dass eine proaktive Problemerkennung durch Telemetrie und KPI Unternehmensüberwachung fehlt.

Vorteile der Nutzung dieser bewährten Methode:

- Fundierte Entscheidungsfindung: Mit Erkenntnissen aus Telemetrie und Unternehmen können Sie KPIs datengestützte Entscheidungen treffen.
- Verbesserte betriebliche Effizienz: Datengesteuerte Ressourcennutzung führt zu Kosteneffektivität.
- Verbesserte Workload-Stabilität: Schnellere Erkennung und Lösung von Problemen führt zu einer verbesserten Verfügbarkeit.
- Optimierte CI/CD-Prozesse: Erkenntnisse aus Telemetriedaten erleichtern die Verfeinerung von Prozessen und sichern die Codebereitstellung.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Hoch

## Implementierungsleitfaden

Verwenden Sie AWS Dienste wie [Amazon CloudWatch](#) und, um Anwendungstelemetrie für Ihren Workload zu implementieren. [AWS X-Ray](#) Amazon CloudWatch bietet eine umfassende Suite von Überwachungstools, mit denen Sie Ihre Ressourcen und Anwendungen in AWS und vor Ort überwachen können. Der Service erfasst, verfolgt und analysiert Metriken, konsolidiert und überwacht Protokolldaten und reagiert auf Änderungen in Ihren Ressourcen, wodurch Sie besser verstehen, wie Ihre Workload funktioniert. Gleichzeitig AWS X-Ray können Sie Ihre Anwendungen verfolgen, analysieren und debuggen, sodass Sie ein tiefes Verständnis des Verhaltens Ihrer Workloads erhalten. Mit Funktionen wie Service Maps, Latenzverteilungen und Trace-Zeitplänen AWS X-Ray bietet es Einblicke in die Leistung Ihres Workloads und die Engpässe, die sich darauf auswirken.

## Implementierungsschritte

1. Identifizieren, welche Daten erfasst werden sollen: Ermitteln Sie die wichtigsten Metriken, Protokolle und Traces, die aussagekräftige Erkenntnisse zu Zustand, Leistung und Verhalten Ihres Workloads bieten.
2. Stellen Sie den [CloudWatchAgenten bereit: Der CloudWatch Agent](#) spielt eine wichtige Rolle bei der Beschaffung von System- und Anwendungsmetriken und Protokollen von Ihrem Workload und der zugrunde liegenden Infrastruktur. Der CloudWatch Agent kann auch verwendet werden, um Spuren zu sammeln OpenTelemetry oder zu röntgen und sie an X-Ray zu senden.
3. Implementieren Sie die Anomalieerkennung für Protokolle und Metriken: Verwenden Sie die Erkennung von [CloudWatch Protokollanomalien und die Erkennung von CloudWatchMetrikanomalien](#), um ungewöhnliche Aktivitäten im Betrieb Ihrer Anwendung automatisch zu identifizieren. Diese Tools verwenden Machine-Learning-Algorithmen, um Anomalien zu erkennen und sie zu melden. Dadurch werden Ihre Überwachungsfunktionen verbessert und die Reaktionszeit bei potenziellen Störungen oder Sicherheitsbedrohungen verkürzt. Richten Sie diese Features ein, um den Zustand und die Sicherheit von Anwendungen proaktiv zu verwalten.
4. Schützen Sie sensible Protokolldaten: Verwenden Sie den [Datenschutz von Amazon CloudWatch Logs](#), um vertrauliche Informationen in Ihren Protokollen zu maskieren. Dieses Feature trägt zur Wahrung von Datenschutz und Compliance bei, indem sensible Daten automatisch erkannt und maskiert werden, bevor auf sie zugegriffen wird. Implementieren Sie Datenmaskierung, um sensible Daten wie personenbezogene Daten sicher zu handhaben und zu schützen (PII).

5. Definieren und überwachen Sie Ihr GeschäftKPIs: Legen Sie [benutzerdefinierte Kennzahlen](#) fest, die auf Ihre [Geschäftsergebnisse](#) abgestimmt sind.
6. Instrumentieren Sie Ihre Anwendung mit AWS X-Ray: Neben der Bereitstellung des CloudWatch Agenten ist es wichtig, dass [Ihre Anwendung](#) so konfiguriert ist, dass sie Trace-Daten aussendet. Dieser Prozess kann weitere Erkenntnisse zum Verhalten und zur Leistung Ihrer Workload liefern.
7. Standardisierung der Datenerfassung in Ihrer gesamten Anwendung: Standardisieren Sie die Datenerfassungspraktiken für Ihre gesamte Anwendung. Einheitlichkeit hilft bei der Korrelation und Analyse von Daten und liefert einen umfassenden Überblick über das Verhalten Ihrer Anwendung.
8. Implementieren Sie kontenübergreifende Beobachtbarkeit: Verbessern Sie die Effizienz der Überwachung über mehrere Konten hinweg AWS-Konten mit der [CloudWatch kontenübergreifenden Observability von Amazon](#). Mit dieser Funktion können Sie Metriken, Protokolle und Alarmer von verschiedenen Konten in einer einzigen Ansicht konsolidieren, was die Verwaltung vereinfacht und die Reaktionszeiten bei identifizierten Problemen in der gesamten Unternehmensumgebung verbessert. AWS
9. Daten analysieren und entsprechend handeln: Sobald die Datenerfassung und Normalisierung abgeschlossen sind, können Sie [Amazon CloudWatch](#) für die Analyse von Kennzahlen und Protokollen sowie für die Trace-Analyse verwenden. [AWS X-Ray](#) Eine solche Analyse kann wichtige Erkenntnisse über den Zustand, die Leistung und das Verhalten Ihrer Workload liefern und so Ihren Entscheidungsprozess beeinflussen.

Aufwand für den Implementierungsplan: Hoch

Ressourcen

Zugehörige bewährte Methoden:

- [OPS04-BP01 Arbeitslast definieren KPIs](#)
- [OPS04-BP03 Implementieren Sie Telemetrie für Benutzeraktivitäten](#)
- [OPS04-BP04 Implementieren Sie Abhängigkeitstelemetrie](#)
- [OPS04-BP05 Implementieren Sie die Rückverfolgbarkeit von Transaktionen](#)

Zugehörige Dokumente:

- [Bewährte Methoden zur Beobachtbarkeit für AWS](#)
- [CloudWatch-Benutzerhandbuch](#)

- [AWS X-Ray Entwicklerhandbuch](#)
- [Instrumentieren verteilter Systeme für Einblicke in die Betriebsabläufe](#)
- [Skill Builder-Kurs zur Beobachtbarkeit in AWS](#)
- [Was ist neu bei Amazon CloudWatch](#)
- [Was ist neu bei AWS X-Ray](#)

#### Zugehörige Videos:

- [AWS re:Invent 2022 — Bewährte Methoden zur Beobachtbarkeit bei Amazon](#)
- [AWS re:Invent 2022 — Entwicklung einer Strategie zur Beobachtung](#)

#### Zugehörige Beispiele:

- [Workshop zur Beobachtbarkeit](#)
- [AWS Lösungsbibliothek: Anwendungsüberwachung mit Amazon CloudWatch](#)

### OPS04-BP03 Implementieren Sie Benutzererlebnis-Telemetrie

Ein entscheidender Erfolgsfaktor besteht darin, tiefe Einblicke in die Erfahrung Ihrer Kunden und deren Interaktionen mit Ihrer Anwendung zu gewinnen. Echte Benutzerüberwachung (RUM) und synthetische Transaktionen dienen zu diesem Zweck als leistungsstarke Tools. RUM liefert Daten über echte Benutzerinteraktionen und ermöglicht so eine ungefilterte Perspektive der Nutzerzufriedenheit. Synthetische Transaktionen simulieren Benutzerinteraktionen und helfen so dabei, potenzielle Probleme zu erkennen, noch bevor sie sich auf echte Nutzer auswirken.

Gewünschtes Ergebnis: Eine ganzheitliche Ansicht des Kundenerlebnisses, die proaktive Erkennung von Problemen und die Optimierung der Benutzerinteraktionen, um nahtlos digitale Erfahrungen zu ermöglichen.

#### Typische Anti-Muster:

- Anwendungen ohne reale Benutzerüberwachung (RUM):
  - Verzögerte Problemerkennung: Ohne diese RUM Option werden Sie möglicherweise erst dann auf Leistungsengpässe oder -probleme aufmerksam, wenn sich Benutzer beschweren. Dieser reaktive Ansatz kann bei Ihren Kunden zu Unzufriedenheit führen.

- **Fehlende Einblicke in die Benutzererfahrung:** Wenn Sie sie nicht verwenden RUM, verlieren Sie wichtige Daten, die zeigen, wie echte Benutzer mit Ihrer Anwendung interagieren, wodurch Ihre Möglichkeiten zur Optimierung der Benutzererfahrung eingeschränkt werden.
- **Anwendungen ohne synthetische Transaktionen:**
  - **Fehlende Grenzfälle:** Synthetische Transaktionen helfen Ihnen dabei, Pfade und Funktionen zu testen, die von den meisten Benutzern möglicherweise nicht häufig verwendet werden, aber für bestimmte Geschäftsfunktionen von entscheidender Bedeutung sind. Ohne sie könnten mögliche Fehler bei diesen Pfaden und Funktionen unbemerkt bleiben.
  - **Ausbleibende Überprüfung auf Probleme bei inaktiver Anwendung:** Regelmäßige synthetische Tests können Situationen simulieren, in denen echte Benutzer nicht aktiv mit Ihrer Anwendung interagieren, wodurch sichergestellt wird, dass das System immer korrekt funktioniert.

Vorteile der Nutzung dieser bewährten Methode:

- **Proaktive Problemerkennung:** Identifizieren und beheben Sie potenzielle Probleme, bevor sie sich auf echte Benutzer auswirken.
- **Optimierte Benutzererfahrung:** Kontinuierliches Feedback von RUM hilft dabei, das allgemeine Benutzererlebnis zu verfeinern und zu verbessern.
- **Erkenntnisse zur Geräte- und Browserleistung:** Verstehen Sie, wie gut Ihre Anwendung auf verschiedenen Geräten und Browsern funktioniert, um weitere Optimierungen zu ermöglichen.
- **Validierte Geschäftsabläufe:** Regelmäßige synthetische Transaktionen stellen sicher, dass Kernfunktionen und kritische Pfade stets betriebsbereit und effizient bleiben.
- **Verbesserte Anwendungsleistung:** Nutzen Sie Erkenntnisse aus echten Benutzerdaten, um die Reaktionsfähigkeit und Zuverlässigkeit Ihrer Anwendungen zu verbessern.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Hoch

Implementierungsleitfaden

[AWS Bietet Dienste wie Amazon RUM und Amazon CloudWatch RUM Synthetics an, um synthetische Transaktionen für die Telemetrie von Benutzeraktivitäten zu nutzen. CloudWatch](#)

In Verbindung mit Daten zur Benutzeraktivität bieten Metriken, Protokolle und Traces einen umfassenden Überblick über den Betriebsstatus der Anwendung und die Benutzererfahrung zugleich.

## Implementierungsschritte

1. Bereitstellen von Amazon CloudWatch RUM: Integrieren Sie Ihre Anwendung, CloudWatch RUM um echte Benutzerdaten zu sammeln, zu analysieren und zu präsentieren.
  - a. Verwenden Sie die [CloudWatch RUM JavaScript Bibliothek](#), um sie in Ihre Anwendung zu integrieren RUM.
  - b. Richten Sie Dashboards ein, um echte Benutzerdaten zu visualisieren und zu überwachen.
2. CloudWatch Synthetics konfigurieren: Erstellen Sie Canaries oder skriptbasierte Routinen, die Benutzerinteraktionen mit Ihrer Anwendung simulieren.
  - a. Definieren Sie kritische Anwendungsworkflows und -pfade.
  - b. Entwerfen Sie Kanarienvögel mithilfe von [CloudWatch Synthetics-Skripten](#), um Benutzerinteraktionen für diese Pfade zu simulieren.
  - c. Planen und überwachen Sie Canaries so, dass sie in bestimmten Intervallen ausgeführt werden, und sorgen Sie so für einheitliche Leistungsprüfungen.
3. Daten analysieren und darauf reagieren: Nutzen Sie Daten aus RUM und synthetische Transaktionen, um Erkenntnisse zu gewinnen und Korrekturmaßnahmen zu ergreifen, wenn Anomalien entdeckt werden. Verwenden Sie CloudWatch Dashboards und Alarme, um auf dem Laufenden zu bleiben.

Aufwand für den Implementierungsplan: Mittel

Ressourcen

Zugehörige bewährte Methoden:

- [OPS04-BP01 Identifizieren Sie die wichtigsten Leistungsindikatoren](#)
- [OPS04-BP02 Implementieren Sie Anwendungstelemetrie](#)
- [OPS04-BP04 Implementieren Sie Abhängigkeitstelemetrie](#)
- [OPS04-BP05 Implementieren Sie verteiltes Tracing](#)

Zugehörige Dokumente:

- [CloudWatch RUM Amazon-Leitfaden](#)
- [Leitfaden für Amazon CloudWatch Synthetics](#)



## Zugehörige Videos:

- [Optimieren Sie Anwendungen mithilfe von Erkenntnissen für Endbenutzer mit Amazon CloudWatch RUM](#)
- [AWS auf Air ft. Echte Benutzerüberwachung für Amazon CloudWatch](#)

## Zugehörige Beispiele:

- [Workshop zur Beobachtbarkeit](#)
- [Git-Repository für Amazon CloudWatch RUM Web Client](#)
- [Verwenden von Amazon CloudWatch Synthetics zur Messung der Seitenladezeit](#)

## OPS04-BP04 Implementieren Sie Abhängigkeitstelemetrie

Die Abhängigkeitstelemetrie ist für die Überwachung des Status und der Leistung der externen Services und Komponenten, auf die Ihre Workload angewiesen ist, unerlässlich. Es bietet wertvolle Einblicke in Erreichbarkeit, Timeouts und andere kritische Ereignisse im Zusammenhang mit Abhängigkeiten wie DNS Datenbanken oder Drittanbietern. APIs Wenn Sie Ihre Anwendung so instrumentieren, dass sie Metriken, Protokolle und Traces zu diesen Abhängigkeiten ausgibt, gewinnen Sie ein besseres Verständnis von potenziellen Engpässen, Leistungsproblemen oder Ausfällen, die sich auf Ihren Workload auswirken könnten.

Gewünschtes Ergebnis: Sicherstellen, dass die Abhängigkeiten, auf die Ihre Workload angewiesen ist, erwartungsgemäß funktionieren, sodass Sie Probleme proaktiv angehen und eine optimale Workload-Leistung gewährleisten können.

## Typische Anti-Muster:

- Nichtbeachtung externer Abhängigkeiten: sich nur auf interne Anwendungsmetriken konzentrieren und dabei Metriken im Zusammenhang mit externen Abhängigkeiten außer Acht lassen.
- Mangelnde proaktive Überwachung: warten, bis Probleme auftreten, statt den Status und die Leistung von Abhängigkeiten kontinuierlich zu überwachen.
- Isolierte Überwachung: Einsatz mehrerer, unterschiedlicher Überwachungstools, was zu fragmentierten und inkonsistenten Ansichten bezüglich des Überwachungsstatus führen kann.

## Vorteile der Nutzung dieser bewährten Methode:

- Verbesserte Zuverlässigkeit der Workloads: sicherstellen, dass externe Abhängigkeiten kontinuierlich verfügbar sind und optimal funktionieren.
- Schnellere Problemerkennung und -lösung: proaktives Identifizieren und Beheben von Problemen mit Abhängigkeiten, bevor sie sich auf die Workload auswirken.
- Umfassender Überblick: Erhalt eines ganzheitlichen Überblicks über interne und externe Komponenten, die den Workload-Status beeinflussen.
- Verbesserte Skalierbarkeit der Workloads: Verständnis der Skalierbarkeitsgrenzen und Leistungsmerkmale externer Abhängigkeiten.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Hoch

### Implementierungsleitfaden

Implementieren Sie die Abhängigkeitstelemetrie, indem Sie zunächst die Services, Infrastrukturen und Prozesse identifizieren, von denen Ihre Workload abhängt. Quantifizieren Sie, wie gute Bedingungen aussehen, wenn diese Abhängigkeiten wie erwartet funktionieren, und bestimmen Sie dann, welche Daten zum Messen dieser Bedingungen benötigt werden. Mit diesen Informationen können Sie Dashboards und Warnmeldungen erstellen, die Ihren Operations-Teams Erkenntnisse zum Status dieser Abhängigkeiten liefern. Verwenden Sie AWS Tools, um die Auswirkungen zu ermitteln und zu quantifizieren, wenn Abhängigkeiten nicht wie gewünscht wirken können. Überarbeiten Sie Ihre Strategie kontinuierlich, um Änderungen der Prioritäten, Ziele und gewonnenen Erkenntnisse Rechnung zu tragen.

### Implementierungsschritte

So implementieren Sie die Abhängigkeitstelemetrie auf effiziente Weise:

1. Identifizierung externer Abhängigkeiten: Arbeiten Sie mit Stakeholdern zusammen, um die externen Abhängigkeiten zu ermitteln, von denen Ihr Workload abhängt. Externe Abhängigkeiten können Dienste wie externe Datenbanken APIs, Netzwerkverbindungsrouen von Drittanbietern zu anderen Umgebungen und DNS Dienste umfassen. Der erste Schritt zu einer effektiven Abhängigkeitstelemetrie besteht darin, auf ganzer Ebene zu verstehen, welche diese Abhängigkeiten sind.
2. Erstellung einer Überwachungsstrategie: Sobald Sie sich ein klares Bild von Ihren externen Abhängigkeiten verschafft haben, entwerfen Sie eine darauf zugeschnittene Überwachungsstrategie. Dazu müssen Sie die Wichtigkeit jeder Abhängigkeit, ihr erwartetes Verhalten und alle damit verbundenen Service Level Agreements oder Ziele (SLA oder)

- verstehen. SLTs Richten Sie proaktive Warnmeldungen ein, die Sie über Statusänderungen oder Leistungsabweichungen informieren.
3. Verwendung der [Netzwerküberwachung](#): Verwenden Sie die Tools [Internet Monitor](#) und [Network Monitor](#), die umfassende Einblicke in die globalen Internet- und Netzwerkbedingungen bieten. Diese Tools helfen Ihnen dabei, Ausfälle, Unterbrechungen oder Leistungseinbußen, die sich auf Ihre externen Abhängigkeiten auswirken, zu verstehen und darauf zu reagieren.
  4. Bleiben Sie auf dem Laufenden [AWS Health Dashboard](#): Es bietet Warnmeldungen und Anleitungen zur Problembeseitigung, wenn Ereignisse auftreten, die AWS sich auf Ihre Services auswirken könnten.
    - a. Überwachen Sie [AWS Health Ereignisse mit EventBridge Amazon-Regeln](#) oder integrieren Sie sie programmatisch, AWS Health API um Aktionen zu automatisieren, wenn Sie AWS Health Ereignisse erhalten. Dies können allgemeine Aktionen sein, z. B. das Senden aller geplanten Lebenszyklus-Ereignisnachrichten an eine Chat-Oberfläche, oder spezifische Aktionen, wie das Initiieren eines Workflows in einem IT-Service-Management-Tool.
    - b. Falls Sie diese Option verwenden AWS Organizations, können Sie [AWS Health Ereignisse kontenübergreifend zusammenfassen](#).
  5. Instrumentieren Sie Ihre Anwendung mit [AWS X-Ray](#): AWS X-Ray bietet Einblicke in die Leistung von Anwendungen und den ihnen zugrunde liegenden Abhängigkeiten. Verfolgen Sie Anfragen von Anfang bis Ende nach, um Engpässe oder Ausfälle bei den externen Services oder Komponenten zu identifizieren, auf die sich Ihre Anwendung stützt.
  6. Verwenden Sie [Amazon DevOps Guru](#): Dieser auf maschinellem Lernen basierende Service identifiziert betriebliche Probleme, prognostiziert, wann kritische Probleme auftreten könnten, und empfiehlt spezifische Maßnahmen. Dadurch ist er von unschätzbarem Wert, wenn es darum geht, Erkenntnisse zu Abhängigkeiten zu gewinnen und festzustellen, dass sie nicht die Ursache von operativen Problemen sind.
  7. Regelmäßige Überwachung: Überwachen Sie kontinuierlich alle Metriken und Protokolle, die sich auf externe Abhängigkeiten beziehen. Richten Sie Warnmeldungen ein, die Sie über unerwartetes Verhalten oder Leistungseinbußen informieren.
  8. Validierung nach Änderungen: Überprüfen Sie nach jeder Aktualisierung oder Änderung einer externen Abhängigkeit deren Leistung und Ausrichtung auf die Anforderungen Ihrer Anwendung.

Aufwand für den Implementierungsplan: Mittel

## Ressourcen

### Zugehörige bewährte Methoden:

- [OPS04-BP01 Arbeitslast definieren KPIs](#)
- [OPS04-BP02 Implementieren Sie die Anwendungstelemetrie](#)
- [OPS04-BP03 Implementieren Sie Telemetrie für Benutzeraktivitäten](#)
- [OPS04-BP05 Implementieren Sie die Rückverfolgbarkeit von Transaktionen](#)
- [OP08-BP04 Erstellen umsetzbarer Warnmeldungen](#)

### Zugehörige Dokumente:

- [Persönliches AWS Health Dashboard Amazon-Benutzerhandbuch](#)
- [AWS Internet Monitor-Benutzerhandbuch](#)
- [AWS X-Ray Entwicklerhandbuch](#)
- [AWS DevOpsGuru-Benutzerhandbuch](#)

### Zugehörige Videos:

- [Wie sich Internetprobleme auf die Leistung von Apps auswirken](#)
- [Einführung in Amazon DevOps Guru](#)
- [Verwalten Sie Ereignisse im Ressourcenlebenszyklus in großem Umfang mit AWS Health](#)

### Zugehörige Beispiele:

- [AIOPsMit Amazon DevOps Guru betriebliche Einblicke gewinnen](#)
- [AWS Health Bewusst](#)
- [Verwenden von Tag-basierter Filterung zur Verwaltung von AWS Health Überwachungs- und Warnmeldungen in großem Umfang](#)

## OPS04-BP05 Implementieren Sie verteiltes Tracing

Die verteilte Nachverfolgung bietet eine Möglichkeit, Anfragen zu überwachen und zu visualisieren, während sie verschiedene Komponenten eines verteilten Systems durchlaufen. Durch die Erfassung von Trace-Daten aus mehreren Quellen und deren Analyse in einer zentralen Ansicht

können Teams besser verstehen, wie Anfragen ablaufen, wo Engpässe bestehen und worauf Optimierungsbemühungen abzielen sollten.

Gewünschtes Ergebnis: Sie verschaffen sich einen ganzheitlichen Überblick über die Anfragen, die durch Ihr verteiltes System fließen, und ermöglichen so präzises Debugging, optimierte Leistung und verbesserte Benutzererfahrungen.

Typische Anti-Muster:

- Inkonsistente Instrumentierung: Nicht alle Services in einem verteilten System sind für die Nachverfolgung instrumentiert.
- Latenz wird ignoriert: Sie konzentrieren sich nur auf Fehler und berücksichtigen nicht die Latenz oder allmähliche Leistungseinbußen.

Vorteile der Nutzung dieser bewährten Methode:

- Umfassender Systemüberblick: Visualisierung des gesamten Anfragenverlaufs, vom Eingang bis zum Ausgang.
- Verbessertes Debugging: Schnelle Identifizierung von Fehlern oder Leistungsproblemen.
- Verbessertes Benutzererlebnis: Überwachung und Optimierung auf der Grundlage von tatsächlichen Benutzerdaten, um sicherzustellen, dass das System den realen Anforderungen entspricht.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Hoch

Implementierungsleitfaden

Identifizieren Sie zunächst alle Elemente Ihrer Workload, für die eine Instrumentierung erforderlich ist. Sobald alle Komponenten berücksichtigt sind, können Sie Tools wie AWS X-Ray und OpenTelemetry zum Sammeln von Trace-Daten für die Analyse mit Tools wie X-Ray und Amazon CloudWatch ServiceLens Map nutzen. Nehmen Sie regelmäßig an Besprechungen mit Entwicklern teil und ergänzen Sie diese Diskussionen mit Tools wie Amazon DevOps Guru, X-Ray Analytics und X-Ray Insights, um tiefere Erkenntnisse zu gewinnen. Richten Sie Warnmeldungen anhand von Trace-Daten ein, damit Sie benachrichtigt werden, wenn die im Workload-Überwachungsplan definierten Ergebnisse gefährdet sind.

Implementierungsschritte

So implementieren Sie die verteilte Nachverfolgung auf effektive Weise:

1. Verwendung von [AWS X-Ray](#): Integrieren Sie X-Ray in Ihre Anwendung, um Erkenntnisse zu ihrem Verhalten zu gewinnen, ihre Leistung zu verstehen und Engpässe zu lokalisieren. Nutzen Sie X-Ray Insights für die automatische Trace-Analyse.
2. Instrumentieren Sie Ihre Dienste: Stellen Sie sicher, dass jeder Service, von einer [AWS Lambda](#)Funktion bis zu einer [EC2Instance](#), Trace-Daten sendet. Je mehr Dienste Sie instrumentieren, desto klarer ist die end-to-end Sicht.
3. Integrieren Sie [CloudWatch Real User Monitoring](#) und [synthetisches Monitoring](#): Integrieren Sie Real User Monitoring (RUM) und synthetisches Monitoring mit X-Ray. Auf diese Weise können reale Benutzererfahrungen erfasst und Benutzerinteraktionen simuliert werden, um potenzielle Probleme zu identifizieren.
4. Verwenden Sie den [CloudWatch Agenten](#): Der Agent kann Spuren entweder von X-Ray oder senden OpenTelemetry, wodurch die Tiefe der gewonnenen Erkenntnisse erweitert wird.
5. Verwenden Sie [Amazon DevOps Guru](#): DevOps Guru verwendet Daten von X-Ray, CloudWatch, und AWS Config, AWS CloudTrail um umsetzbare Empfehlungen zu geben.
6. Analyse von Traces: Überprüfen Sie die Trace-Daten regelmäßig, um Muster, Anomalien oder Engpässe zu erkennen, die sich auf die Leistung Ihrer Anwendung auswirken könnten.
7. Warnmeldungen einrichten: Konfigurieren Sie Alarme [CloudWatch](#)für ungewöhnliche Muster oder längere Latenzen, sodass Probleme proaktiv behoben werden können.
8. Kontinuierliche Verbesserung: Überarbeiten Sie Ihre Tracing-Strategie, wenn Services hinzugefügt oder geändert werden, um alle relevanten Datenpunkte zu erfassen.

Aufwand für den Implementierungsplan: Mittel

Ressourcen

Zugehörige bewährte Methoden:

- [OPS04-BP01 Identifizieren Sie die wichtigsten Leistungsindikatoren](#)
- [OPS04-BP02 Implementieren Sie Anwendungstelemetrie](#)
- [OPS04-BP03 Implementieren Sie Benutzererlebnis-Telemetrie](#)
- [OPS04-BP04 Implementieren Sie Abhängigkeitstelemetrie](#)

Zugehörige Dokumente:

- [AWS X-Ray Leitfaden für Entwickler](#)

- [Benutzerhandbuch für CloudWatch Amazon-Agenten](#)
- [Amazon DevOps Guru-Benutzerhandbuch](#)

Zugehörige Videos:

- [Nutzen Sie AWS X-Ray Insights](#)
- [AWS auf Air ft. Beobachtbarkeit: Amazon CloudWatch](#) und AWS X-Ray

Zugehörige Beispiele:

- [Instrumentierung Ihrer Anwendung für AWS X-Ray](#)

OPS5. 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 Faktorwechsel, 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

- [OPS05-BP01 Versionskontrolle verwenden](#)
- [OPS05-BP02 Änderungen testen und validieren](#)
- [OPS05-BP03 Verwenden Sie Konfigurationsmanagementsysteme](#)
- [OPS05-BP04 Verwenden Sie Build- und Deployment-Management-Systeme](#)
- [OPS05-BP05 Patchmanagement durchführen](#)
- [OPS05-BP06 Designstandards teilen](#)
- [OPS05-BP07 Implementieren Sie Praktiken zur Verbesserung der Codequalität](#)
- [OPS05-BP08 Verwenden Sie mehrere Umgebungen](#)
- [OPS05-BP09 Nehmen Sie häufige, kleine, reversible Änderungen vor](#)
- [OPS05- BP1 0 Vollständig automatisierte Integration und Bereitstellung](#)

## OPS05-BP01 Versionskontrolle verwenden

Aktivieren Sie die Verfolgung von Änderungen und Releases mithilfe einer Versionskontrolle.

Viele AWS Dienste bieten Funktionen zur Versionskontrolle. Verwenden Sie ein Revisions- oder Quellcodeverwaltungssystem wie [AWS CodeCommit](#), um Code und andere Artefakte (z. B. versionsgesteuerte [AWS CloudFormation](#)-Vorlagen Ihrer Infrastruktur) zu verwalten.

Gewünschtes Ergebnis: Ihre Teams arbeiten gemeinsam am Code. Bei der Zusammenführung ist der Code einheitlich und es gehen keine Änderungen verloren. Fehler können durch korrekte Versionsverwaltung leicht behoben werden.

Typische Anti-Muster:

- Sie haben Ihren Code auf Ihrer Workstation entwickelt und gespeichert. Es ist ein Speicherfehler bei der Workstation aufgetreten, der nicht rückgängig gemacht werden kann, und Sie haben den Code verloren.
- Nachdem Sie den vorhandenen Code mit Ihren Änderungen überschrieben haben, starten Sie Ihre Anwendung neu, doch sie funktioniert nicht mehr. Sie können die Änderung nicht rückgängig machen.
- Sie arbeiten an einer Berichtsdatei, deshalb ist sie für alle anderen schreibgeschützt, doch ein anderer Benutzer möchte sie bearbeiten. Der Benutzer kontaktiert Sie und bittet darum, die Arbeit daran zu beenden, damit er seine Aufgabe erledigen kann.
- Ihr Forschungsteam arbeitet an einer detaillierten Analyse, die Ihre zukünftige Arbeit prägt. Jemand hat versehentlich den endgültigen Bericht mit seiner Einkaufsliste überschrieben. Sie können die Änderung nicht rückgängig machen und müssen den Bericht neu erstellen.

Vorteile der Nutzung dieser bewährten Methode: Durch die Verwendung von Versionskontrollfunktionen können Sie problemlos einen bekanntermaßen funktionierenden Status bzw. frühere Versionen wiederherstellen und so das Risiko von verlorenen Assets begrenzen.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Hoch

Implementierungsleitfaden

Bewahren Sie Ressourcen in Repositorys mit Versionskontrolle auf. Dies ermöglicht die Nachvollziehung von Änderungen, die Bereitstellung neuer Versionen, die Erkennung von Änderungen an bestehenden Versionen und die Rückkehr zu vorherigen Versionen (zum Beispiel bei



einem Fehler die Zurücksetzung auf einen bekanntermaßen funktionierenden Zustand). Integrieren Sie die Versionskontrollfunktionen Ihrer Konfigurationsverwaltungssysteme in Ihre Verfahren.

Ressourcen

Zugehörige bewährte Methoden:

- [OPS05-BP04 Verwenden Sie Build- und Deployment-Management-Systeme](#)

Zugehörige Dokumente:

- [Was ist AWS CodeCommit?](#)

Zugehörige Videos:

- [Einführung in AWS CodeCommit](#)

OPS05-BP02 Änderungen testen und validieren

Jede bereitgestellte Änderung muss getestet werden, um Fehler in der Produktion zu vermeiden. Diese bewährte Methode konzentriert sich auf das Testen von Änderungen von der Versionskontrolle bis zur Erstellung von Artefakten. Neben Änderungen am Anwendungscode sollten die Tests auch die Infrastruktur, die Konfiguration, die Sicherheitskontrollen und die Betriebsverfahren umfassen. Das Testen nimmt viele Formen an, von Komponententests bis hin zur Analyse von Softwarekomponenten (SCA). Wenn Tests im Softwareintegrations- und -bereitstellungsprozess weiter nach links verschoben werden, führt dies zu einer höheren Gewissheit der Artefaktqualität.

Ihr Unternehmen muss Teststandards für alle Software-Artefakte entwickeln. Automatisierte Tests verringern den Arbeitsaufwand und vermeiden manuelle Testfehler. In einigen Fällen können aber auch manuelle Tests notwendig sein. Entwickler müssen Zugang zu automatisierten Testergebnissen haben, um Feedback-Schleifen zur Verbesserung der Softwarequalität zu schaffen.

Gewünschtes Ergebnis: Ihre Softwareänderungen werden vor der Bereitstellung getestet. Die Entwickler haben Zugang zu den Testergebnissen und den Validierungen. Ihre Organisation hat einen Teststandard, der für alle Softwareänderungen gilt.

Typische Anti-Muster:

- Sie stellen eine neue Softwareänderung ohne jegliche Tests bereit. Sie kann in der Produktion nicht ausgeführt werden, was zu einem Ausfall führt.

- Neue Sicherheitsgruppen werden bereitgestellt, AWS CloudFormation ohne dass sie in einer Vorproduktionsumgebung getestet wurden. Durch die Sicherheitsgruppen ist Ihre App für Ihre Kunden unerreichbar.
- Eine Methode wurde geändert, aber es gibt keine Tests der Einheiten. Die Software läuft nicht, wenn sie in der Produktion eingesetzt wird.

Vorteile der Nutzung dieser bewährten Methode: Die Fehlerquote bei Änderungen bei Softwarebereitstellungen wird reduziert. Die Qualität der Software wird verbessert. Die Entwickler haben ein größeres Bewusstsein für die Lebensfähigkeit ihres Codes. Sicherheitsrichtlinien können zuverlässig eingeführt werden, um die Compliance des Unternehmens zu unterstützen. Infrastrukturänderungen, wie automatische Aktualisierungen der Skalierungsrichtlinien, werden im Voraus getestet, um den Anforderungen des Datenverkehrs gerecht zu werden.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Hoch

### Implementierungsleitfaden

Alle Änderungen, vom Anwendungscode bis zur Infrastruktur, werden im Rahmen Ihrer kontinuierlichen Integrationspraxis getestet. Die Testergebnisse werden veröffentlicht, damit die Entwickler schnelles Feedback erhalten. Ihre Organisation hat einen Teststandard, den alle Änderungen erfüllen müssen.

Nutzen Sie die Leistungsfähigkeit generativer KI mit Amazon Q Developer, um die Entwicklerproduktivität und die Codequalität zu verbessern. Amazon Q Developer umfasst die Generierung von Codevorschlägen (basierend auf großen Sprachmodellen), die Erstellung von Komponententests (einschließlich Randbedingungen) und Verbesserungen der Codesicherheit durch die Erkennung und Behebung von Sicherheitsschwachstellen.

### Kundenbeispiel

Im Rahmen seiner kontinuierlichen Integrationspipeline führt AnyCompany Retail verschiedene Arten von Tests an allen Softwareartefakten durch. Das Unternehmen praktiziert eine testgesteuerte Entwicklung, sodass die gesamte Software über Tests von Einheiten verfügt. Sobald das Artefakt erstellt ist, führen end-to-end sie Tests durch. Nach Abschluss dieser ersten Testrunde wird ein statischer Anwendungssicherheitsscan durchgeführt, bei dem nach bekannten Schwachstellen gesucht wird. Die Entwickler erhalten Meldungen, sobald die einzelnen Prüfpunkte durchlaufen wurden. Sobald alle Tests abgeschlossen wurden, wird der Software-Artefakt in einem Artefakt-Repository gespeichert.

## Implementierungsschritte

1. Arbeiten Sie mit den Beteiligten in Ihrem Unternehmen zusammen, um einen Teststandard für Software-Artefakte zu entwickeln. Welche Standardtests sollten alle Artefakte bestehen? Gibt es Compliance- oder Governance-Anforderungen, die bei der Testabdeckung berücksichtigt werden müssen? Müssen Sie die Qualität des Codes testen? Wer muss informiert werden, sobald die Tests abgeschlossen sind?
  1. Die [Referenzarchitektur für AWS -Bereitstellungs-Pipelines](#) enthält eine maßgebliche Liste von Testtypen, die als Teil einer Integrationspipeline an Software-Artefakten durchgeführt werden können.
2. Instrumentieren Sie Ihre Anwendung mit den erforderlichen Tests auf der Grundlage Ihres Software-Teststandards. Jeder Testreihe sollte in weniger als zehn Minuten abgeschlossen sein. Tests sollten im Rahmen einer Integrationspipeline durchgeführt werden.
  - a. Verwenden Sie [Amazon Q Developer](#), ein generatives KI-Tool, mit dem Sie Modultestfälle (einschließlich Randbedingungen) erstellen, Funktionen mithilfe von Code und Kommentaren generieren und bekannte Algorithmen implementieren können.
  - b. Verwenden Sie [Amazon CodeGuru Reviewer](#), um Ihren Anwendungscode auf Fehler zu testen.
  - c. Sie können [AWS CodeBuild](#) verwenden, um Tests auf Software-Artefakten durchzuführen.
  - d. [AWS CodePipeline](#) kann Ihre Softwaretests in eine Pipeline orchestrieren.

## Ressourcen

Zugehörige bewährte Methoden:

- [OPS05-BP01 Verwenden Sie die Versionskontrolle](#)
- [OPS05-BP06 Teilen Sie die Designstandards](#)
- [OPS05-BP07 Implementieren Sie Praktiken zur Verbesserung der Codequalität](#)
- [OPS05- BP1 0 Automatisieren Sie die Integration und Bereitstellung vollständig](#)

Zugehörige Dokumente:

- [Einen testgetriebenen Entwicklungsansatz verwenden](#)
- [Beschleunigen Ihres Softwareentwicklungszyklus mit Amazon Q](#)
- [Amazon Q Developer \(jetzt allgemein verfügbar\) enthält Vorschauen neuer Funktionen, mit denen Sie das Entwicklererlebnis neu gestalten können](#)

- [Der ultimative Spickzettel für die Verwendung von Amazon Q Developer in Ihrem IDE](#)
- [Shift-Left-Workload, Nutzung von KI für die Testerstellung](#)
- [Amazon Q-Entwicklerzentrum](#)
- [10 Möglichkeiten, Anwendungen mit Amazon schneller zu erstellen CodeWhisperer](#)
- [Mit Amazon geht der Blick über die Codeabdeckung hinaus CodeWhisperer](#)
- [Bewährte Methoden für schnelles Engineering mit Amazon CodeWhisperer](#)
- [Automatisierte AWS CloudFormation Testpipeline mit TaskCat und CodePipeline](#)
- [Aufbau einer end-to-end AWS DevSecOps CI/CD-Pipeline mit Open Source SCASAST, und Tools DAST](#)
- [Erste Schritte beim Testen von Serverless-Anwendungen](#)
- [Meine CI/CD-Pipeline ist mein Release Captain](#)
- [Durchführung von Continuous Integration und Continuous Delivery in AWS \(Whitepaper\)](#)

#### Zugehörige Videos:

- [Implementieren Sie einen API mit Amazon Q Developer Agent für Softwareentwicklung](#)
- [Installation, Konfiguration und Verwendung von Amazon Q Developer mit JetBrains IDEs \(Anleitung\)](#)
- [Die Kunst von Amazon beherrschen CodeWhisperer — Playlist YouTube](#)
- [AWS re:Invent 2020: Testbare Infrastruktur: Integrationstests aktiviert AWS](#)
- [AWS Summit ANZ 2021 — Förderung einer Test-First-Strategie mit testgetriebener Entwicklung CDK](#)
- [Testen Sie Ihre Infrastruktur als Code mit AWS CDK](#)

#### Zugehörige Ressourcen:

- [Entwicklung von Anwendungen mithilfe generativer KI mit Amazon CodeWhisperer](#)
- [CodeWhisperer Amazon-Werkstatt](#)
- [Referenzarchitektur für AWS -Bereitstellungs-Pipelines – Anwendung](#)
- [AWS Kubernetes-Pipeline DevSecOps](#)
- [Richtlinie als Code – Workshop – Testgesteuerte Entwicklung](#)

- [Führen Sie Komponententests für eine Node.js -Anwendung aus GitHub , indem Sie AWS CodeBuild](#)
- [Serverspec für die testgesteuerte Entwicklung von Infrastrukturcode verwenden](#)

Zugehörige Services:

- [Amazon Q Developer](#)
- [CodeGuru Amazon-Rezensent](#)
- [AWS CodeBuild](#)
- [AWS CodePipeline](#)

### OPS05-BP03 Verwenden Sie Konfigurationsmanagementsysteme

Verwenden Sie Systeme zur Konfigurationsverwaltung, um Änderungen vorzunehmen und zu verfolgen. Diese Systeme reduzieren Fehler aufgrund von manuellen Prozessen und verringern den Testaufwand.

Bei der statischen Konfigurationsverwaltung werden Werte festgelegt, wenn eine Ressource initialisiert wird, die erwartungsgemäß während der Lebensdauer der Ressource konsistent bleibt. Bei der dynamischen Konfigurationsverwaltung werden bei der Initialisierung Werte festgelegt, die sich während der Lebensdauer einer Ressource ändern können oder voraussichtlich ändern werden. So können Sie zum Beispiel durch eine Konfigurationsänderung ein Feature in Ihrem Code aktivieren oder während eines Vorfalls den Detaillierungsgrad des Protokolls ändern.

Konfigurationen sollten in einem bekannten und konsistenten Zustand bereitgestellt werden. Sie sollten die automatisierte Inspektion verwenden, um die Ressourcenkonfigurationen in mehreren Umgebungen und Regionen kontinuierlich zu überwachen. Diese Kontrollen sollten als automatisierter Code und automatisierte Verwaltung definiert werden, um sicherzustellen, dass Regeln in allen Umgebungen einheitlich angewendet werden. Änderungen an Konfigurationen sollten im Rahmen vereinbarter Verfahren zur Kontrolle von Änderungen aktualisiert und konsistent angewendet werden, sodass die Versionskontrolle gewahrt bleibt. Die Anwendungskonfiguration sollte unabhängig vom Anwendungs- und Infrastrukturcode verwaltet werden. Dies ermöglicht eine konsistente Bereitstellung in mehreren Umgebungen. Konfigurationsänderungen führen nicht dazu, dass die Anwendung neu erstellt oder bereitgestellt wird.

Gewünschtes Ergebnis: Sie konfigurieren, validieren und implementieren als Teil Ihrer CI/CD-Pipeline (Continuous Integration, Continuous Delivery). Sie überwachen, um zu überprüfen, ob

die Konfigurationen korrekt sind. Dadurch werden die Auswirkungen auf Endbenutzer und Kunden minimiert.

Typische Anti-Muster:

- Sie aktualisieren die Konfigurationen aller Webserver manuell und eine Reihe von Servern reagiert aufgrund von Updatefehlern nicht mehr.
- Sie aktualisieren Ihre Anwendungsserver mehrere Stunden lang auf manuelle Weise. Die Inkonsistenz der Konfiguration während der Änderung führt zu unerwarteten Verhaltensweisen.
- Jemand hat Ihre Sicherheitsgruppen aktualisiert und auf Ihre Webserver kann nicht mehr zugegriffen werden. Sie wissen nicht, was geändert wurde, und verbringen viel Zeit mit der Suche nach dem Problem – die Zeit bis zur Wiederherstellung nimmt zu.
- Sie übertragen eine Vorproduktionskonfiguration ohne Validierung über CI/CD in die Produktion. Sie setzen Benutzer und Kunden falschen Daten und Services aus.

Vorteile der Nutzung dieser bewährten Methode: Die Einführung von Konfigurationsverwaltungssystemen reduziert den Aufwand für die Durchführung und Nachverfolgung von Änderungen sowie die Häufigkeit der durch manuelle Verfahren verursachten Fehler. Konfigurationsverwaltungssysteme liefern Garantien in Bezug auf Governance, Compliance und regulatorische Anforderungen.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel

Implementierungsleitfaden

Konfigurationsverwaltungssysteme werden verwendet, um Änderungen an Anwendungs- und Umgebungskonfigurationen zu verfolgen und zu implementieren. Konfigurationsverwaltungssysteme werden auch eingesetzt, um Fehler zu reduzieren, die durch manuelle Prozesse verursacht werden, Konfigurationsänderungen wiederholbar und überprüfbar zu machen und den Aufwand zu reduzieren.

Mit [AWS Config](#) dieser Option können Sie Ihre AWS Ressourcenkonfigurationen [über Konten und Regionen hinweg](#) kontinuierlich überwachen. So können Sie den Konfigurationsverlauf besser verfolgen, nachvollziehen, wie sich eine Konfigurationsänderung auf andere Ressourcen auswirkt, und sie im Hinblick auf die erwarteten oder gewünschten Konfigurationen mithilfe von [AWS-Config-Regeln](#) und [AWS Config -Konformitätspaketen](#) prüfen.

Für dynamische Konfigurationen in Ihren Anwendungen, die auf EC2 Amazon-Instances AWS Lambda, Containern, mobilen Anwendungen oder IoT-Geräten ausgeführt werden, können Sie

sie verwenden, [AWS AppConfig](#) um sie in Ihren Umgebungen zu konfigurieren, zu validieren, bereitzustellen und zu überwachen.

## Implementierungsschritte

1. Identifizieren Sie die Verantwortlichen der Konfiguration.
  - a. Informieren Sie die Verantwortlichen der Konfigurationen über alle Compliance-, Governance- oder regulatorischen Anforderungen.
2. Identifizieren Sie Konfigurationselemente und Leistungen.
  - a. Konfigurationselemente sind alle Anwendungs- und Umgebungskonfigurationen, die von einer Bereitstellung innerhalb Ihrer CI/CD-Pipeline betroffen sind.
  - b. Zu den Leistungen gehören Erfolgskriterien, Validierung und was überwacht werden muss.
3. Wählen Sie Tools für die Konfigurationsverwaltung basierend auf Ihren Geschäftsanforderungen und Ihrer Bereitstellungs-pipeline aus.
4. Ziehen Sie für signifikante Konfigurationsänderungen gewichtete Bereitstellungen wie Canary-Bereitstellungen in Betracht, um die Auswirkungen falscher Konfigurationen zu minimieren.
5. Integrieren Sie Ihre Konfigurationsverwaltung in Ihre CI/CD-Pipeline.
6. Bestätigen Sie alle übermittelten Änderungen.

## Ressourcen

Zugehörige bewährte Methoden:

- [OPS06-BP01 Plan für erfolglose Änderungen](#)
- [OPS06-BP02 Testbereitstellungen](#)
- [OPS06-BP03 Setzen Sie sichere Einsatzstrategien ein](#)
- [OPS06-BP04 Automatisieren Sie Tests und Rollback](#)

Zugehörige Dokumente:

- [AWS Control Tower](#)
- [AWS Landing Zone Accelerator](#)
- [AWS Config](#)
- [Was ist AWS Config?](#)

- [AWS AppConfig](#)
- [Was ist AWS CloudFormation?](#)
- [AWS -Entwicklungstools](#)

Zugehörige Videos:

- [AWS re:Invent 2022 — Proaktive Verwaltung und Einhaltung von Vorschriften für Workloads AWS](#)
- [AWS re:Invent 2020: Erreichen Sie Compliance als Code mithilfe von AWS Config](#)
- [Verwaltung und Bereitstellung von Anwendungskonfigurationen mit AWS AppConfig](#)

OPS05-BP04 Verwenden Sie Build- und Deployment-Management-Systeme

Verwenden Sie Systeme zur Build- und Bereitstellungsverwaltung. Diese Systeme reduzieren Fehler aufgrund von manuellen Prozessen und verringern den Testaufwand.

In AWS können Sie CI/CD-Pipelines (Continuous Integration/Continuous Deployment) mithilfe von Diensten wie [AWS Entwicklertools](#) (z. B., AWS CodeCommit und) erstellen. [AWS CodeBuild](#)[AWS CodePipeline](#)[AWS CodeDeploy](#)[AWS CodeStar](#)

Gewünschtes Ergebnis: Ihre Systeme zur Build- und Bereitstellungsverwaltung unterstützen das Continuous Integration Continuous Delivery (CI/CD)-System Ihrer Organisation, das Funktionen zur Automatisierung sicherer Rollouts mit den richtigen Konfigurationen bietet.

Typische Anti-Muster:

- Nachdem Sie Ihren Code auf Ihrem Entwicklungssystem kompiliert haben, kopieren Sie die ausführbare Datei auf Ihre Produktionssysteme und sie kann nicht gestartet werden. Die lokalen Protokolldateien zeigen an, dass die Ausführung aufgrund fehlender Abhängigkeiten fehlgeschlagen ist.
- Sie erstellen Ihre Anwendung erfolgreich mit neuen Funktionen in Ihrer Entwicklungsumgebung und stellen den Code der Quality Assurance (QA, Qualitätsprüfung) zur Verfügung. Die QA-Prüfung schlägt fehl, da statische Komponenten fehlen.
- Am Freitag haben Sie Ihre Anwendung nach großem Aufwand manuell in Ihrer Entwicklungsumgebung erstellt, einschließlich der neu geschriebenen Funktionen. Am Montag können Sie die Schritte, mit denen Sie Ihre Anwendung erfolgreich erstellen konnten, nicht wiederholen.



- Sie führen die Tests durch, die Sie für den neuen Release erstellt haben. Sie verbringen die nächste Woche damit, eine Testumgebung einzurichten und alle vorhandenen Integrationstests durchzuführen, gefolgt von den Leistungstests. Der neue Code bewirkt eine inakzeptable Leistungsbeeinträchtigung und muss neu entwickelt und dann erneut getestet werden.

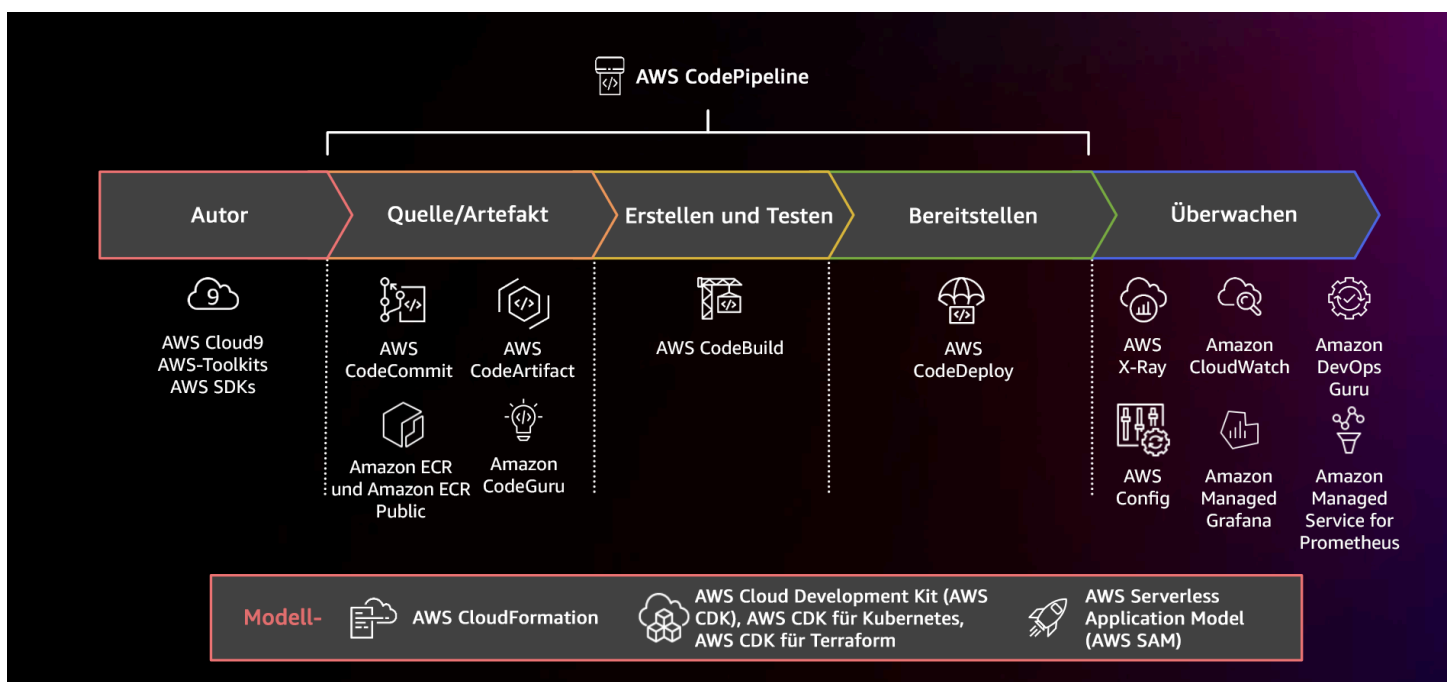
Vorteile der Nutzung dieser bewährten Methode: Mithilfe von Mechanismen zur Verwaltung von Erstellungs- und Bereitstellungsaktivitäten reduzieren Sie den Aufwand für wiederholte Aufgaben, verschaffen Ihren Teammitgliedern die Zeit, sich auf ihre wichtigen Aufgaben zu konzentrieren, und begrenzen die Entstehung von Fehlern durch manuelle Verfahren.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel

### Implementierungsleitfaden

Systeme zur Build- und Bereitstellungsverwaltung werden verwendet, um Änderungen nachzuverfolgen und zu implementieren, Fehler zu reduzieren, die durch manuelle Prozesse verursacht werden, und den Aufwand für sichere Implementierungen zu minimieren. Nutzen Sie eine vollständig automatisierte Integrations- und Bereitstellungs-Pipeline vom Einchecken des Codes über das Testen und die Bereitstellung bis hin zur Validierung. Dies reduziert die Vorlaufzeit, senkt die Kosten, ermöglicht häufigere Änderungen, minimiert den Aufwand und verbessert die Zusammenarbeit.

### Implementierungsschritte



## Diagramm, das eine CI/CD-Pipeline zeigt, die Dienste und verwandte Dienste nutzt AWS CodePipeline

1. Wird AWS CodeCommit zur Versionskontrolle, zum Speichern und Verwalten von Ressourcen (wie Dokumenten, Quellcode und Binärdateien) verwendet.
2. Wird verwendet, CodeBuild um Ihren Quellcode zu kompilieren, Komponententests auszuführen und Artefakte zu erzeugen, die sofort bereitgestellt werden können.
3. [Verwenden Sie CodeDeploy es als Bereitstellungsservice, der die Anwendungsbereitstellung auf EC2Amazon-Instances, lokalen Instances, serverlosen AWS Lambda Funktionen oder Amazon automatisiert. ECS](#)
4. Überwachen Sie Ihre Bereitstellungen.

### Ressourcen

#### Zugehörige bewährte Methoden:

- [OPS06-BP04 Automatisieren Sie Tests und Rollback](#)

#### Zugehörige Dokumente:

- [AWS -Entwicklungstools](#)
- [Was AWS CodeCommit ist?](#)
- [Was ist AWS CodeBuild?](#)
- [AWS CodeBuild](#)
- [Was ist AWS CodeDeploy?](#)

#### Zugehörige Videos:

- [AWS re:Invent 2022 — AWS Well-Architected Best Practices für DevOps AWS](#)

## OPS05-BP05 Patchmanagement 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 manueller Prozesse zu reduzieren, zu skalieren und den Aufwand für die Installation von Patches zu verringern.

Patch- und Schwachstellenmanagement sind Teil Ihrer Vorteile- und Risikomanagement-Aktivitäten. Es ist vorzuziehen, unveränderliche Infrastrukturen zu haben und Workloads in verifizierten bekannten guten Zuständen bereitzustellen. Wenn dies nicht realisierbar ist, ist das Patchen die verbleibende Option.

[Amazon EC2 Image Builder](#) stellt Pipelines zur Aktualisierung von Maschinenimages bereit. Ziehen Sie als Teil des Patch-Managements [Amazon Machine Images](#) (AMIs) in Betracht, das eine [AMI-Image-Pipeline](#) oder Container-Images mit einer [Docker-Image-Pipeline](#) verwendet und gleichzeitig Muster für [benutzerdefinierte Laufzeiten und zusätzliche Bibliotheken](#) zur Beseitigung von Sicherheitslücken AWS Lambda bereitstellt.

Sie sollten Updates für [Amazon Machine Images](#) für Linux- oder Windows Server-Images mit [Amazon EC2 Image Builder](#) verwalten. Sie können [Amazon Elastic Container Registry \(Amazon ECR\)](#) mit Ihrer bestehenden Pipeline verwenden, um ECS Amazon-Images und EKS Amazon-Images zu verwalten. Lambda enthält [Funktionen zur Versionsverwaltung](#).

Patches sollten nicht auf Produktionssystemen durchgeführt werden, ohne zuerst in einer sicheren Umgebung getestet zu werden. Patches sollten nur angewendet werden, wenn sie ein betriebliches oder geschäftliches Ergebnis unterstützen. Bei Aktivierung können Sie [AWS Systems Manager Patch Manager](#) verwenden AWS, um das Patchen verwalteter Systeme zu automatisieren und die Aktivität mithilfe von [Systems Manager Maintenance Windows](#) zu planen.

Gewünschtes Ergebnis: Ihre Images AMI und die Container-Images sind gepatcht und bereit für den Start. up-to-date Sie können den Status aller bereitgestellten Images nachverfolgen und wissen, dass die Patches konform sind. Sie können über den aktuellen Status berichten und verfügen über ein Verfahren, mit dem Sie Ihre Compliance-Anforderungen erfüllen können.

Typische Anti-Muster:

- Sie erhalten den Auftrag, alle neuen Sicherheits-Patches innerhalb von zwei Stunden anzuwenden, was zu mehreren Ausfällen aufgrund der Anwendungsinkompatibilität mit bestimmten Patches führt.
- Eine ungepatchte Bibliothek hat unbeabsichtigte Folgen, weil unbekannte Personen Schwachstellen darin ausnutzen, um auf Ihre Workload zuzugreifen.

- Sie patchen die Entwicklerumgebungen automatisch, ohne die Entwickler zu benachrichtigen. Sie erhalten mehrere Beschwerden von den Entwicklern, dass ihre Umgebung nicht mehr wie erwartet funktioniert.
- Sie haben die kommerzielle off-the-shelf Software nicht auf einer persistenten Instanz gepatcht. Als ein Problem mit der Software auftritt und Sie sich an den Anbieter wenden, werden Sie darüber informiert, dass die Version nicht unterstützt wird und Sie bestimmte Patches installieren müssen, um Unterstützung zu erhalten.
- Ein kürzlich veröffentlichter Patch für Ihre verwendete Verschlüsselungssoftware bietet signifikante Leistungsverbesserungen. Ihr ungepatchtes System weist Leistungsprobleme auf, die bestehen bleiben, weil es nicht gepatcht ist.
- Sie werden über eine Zero-Day-Schwachstelle informiert, die eine Notfalllösung erfordert, und Sie müssen alle Ihre Umgebungen manuell patchen.

Vorteile der Nutzung dieser bewährten Methode: Durch die Einrichtung eines Patch-Verwaltungsprozesses, einschließlich Ihrer Patching-Kriterien und Bereitstellungsmethodik für Ihre Umgebungen, können Sie die Patch-Ebenen skalieren und Berichte darüber erstellen. Das gibt Ihnen Sicherheit in Bezug auf Sicherheitspatches und gewährleistet einen klaren Überblick über den Status bekannter Problemlösungen. Dies wiederum fördert die Übernahme der gewünschten Merkmale und Funktionen, das Entfernen von Problemen und die kontinuierliche Compliance. Implementieren Sie Verwaltungssysteme und Automatisierung für Patches, um den Aufwand für die Bereitstellung von Patches zu reduzieren und Fehler zu begrenzen, die durch manuelle Prozesse verursacht werden.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel

### Implementierungsleitfaden

Installieren Sie auf Ihren Systemen Patches zur Behebung von Problemen, zur Erlangung der gewünschten Funktionen oder Fähigkeiten sowie zur kontinuierlichen Einhaltung der Governance-Richtlinien und der Anforderungen des Lieferantensupport. Nehmen Sie in unveränderlichen Systemen eine Bereitstellung mit einer geeigneten Patch-Gruppe vor, um das gewünschte Ergebnis zu erzielen. Automatisieren Sie den Mechanismus der Patch-Verwaltung, um die Patch-Zeit zu verkürzen, Fehler aufgrund von manuellen Prozessen zu vermeiden und den Aufwand für die Installation von Patches zu verringern.

### Implementierungsschritte

Für Amazon EC2 Image Builder:

1. Geben Sie mithilfe von Amazon EC2 Image Builder Pipeline-Details an:
  - a. Erstellen Sie eine Image-Pipeline und geben Sie ihr einen Namen.
  - b. Definieren Sie den Pipeline-Zeitplan und die Zeitzone.
  - c. Konfigurieren Sie alle Abhängigkeiten.
2. Wählen Sie ein Rezept:
  - a. Wählen Sie ein vorhandenes Rezept aus oder erstellen Sie ein neues.
  - b. Wählen Sie den Image-Typ aus.
  - c. Geben Sie Ihrem Rezept einen Namen und eine Versionsnummer.
  - d. Wählen Sie Ihr Basis-Image aus.
  - e. Fügen Sie Build-Komponenten zur Zielregistrierung hinzu.
3. Optional: Definieren Sie Ihre Infrastrukturkonfiguration.
4. Optional: Definieren Sie die Konfigurationseinstellungen.
5. Prüfen Sie die Einstellungen.
6. Achten Sie regelmäßig auf die Rezepthygiene.

Für Systems Manager Patch Manager:

1. Erstellen Sie eine Patch-Baseline.
2. Wählen Sie eine Methode für den Patch-Vorgang aus.
3. Aktivieren Sie Compliance-Berichte und -Scans.

Ressourcen

Zugehörige bewährte Methoden:

- [OPS06-BP04 Automatisieren Sie Tests und Rollback](#)

Zugehörige Dokumente:

- [Was ist Amazon EC2 Image Builder](#)
- [Erstellen Sie eine Image-Pipeline mit dem Amazon EC2 Image Builder](#)
- [Erstellen einer Container-Image-Pipeline](#)
- [AWS Systems Manager Patch Manager](#)

- [Arbeiten mit Patch Manager](#)
- [Arbeiten mit Patch-Compliance-Berichten](#)
- [AWS Tools für Entwickler](#)

Zugehörige Videos:

- [CI/CD für serverlose Anwendungen auf AWS](#)
- [Design mit Blick auf die Ops](#)

Zugehörige Beispiele:

- [Well-Architected Labs – Bestands- und Patch-Verwaltung](#)
- [AWS Systems Manager Tutorials zu Patch Manager](#)

OPS05-BP06 Designstandards teilen

Tauschen Sie teamübergreifend bewährte Methoden aus, um das Bewusstsein zu schärfen und den Nutzen der Entwicklungsarbeit zu maximieren. Dokumentieren Sie sie und halten Sie sie auf dem neuesten Stand, wenn sich Ihre Architektur weiterentwickelt. Wenn gemeinsame Standards in Ihrem Unternehmen durchgesetzt werden, ist es wichtig, dass Mechanismen vorhanden sind, um Ergänzungen, Änderungen und Ausnahmen von Standards abzubilden. Ohne diese Option werden Standards zu einer Einschränkung der Innovation.

Gewünschtes Ergebnis: Designstandards werden von allen Teams in Ihren Organisationen gemeinsam genutzt. Sie werden dokumentiert und entsprechend der Weiterentwicklung der bewährten Verfahren aufbewahrt up-to-date.

Typische Anti-Muster:

- Zwei Entwicklerteams haben jeweils einen Service zur Authentifizierung von Benutzern erstellt. Ihre Benutzer müssen für jeden Teil des Systems, auf den sie zugreifen möchten, eigene Anmeldeinformationen verwenden.
- Jedes Team verwaltet seine eigene Infrastruktur. Eine neue Compliance-Anforderung erzwingt eine Änderung Ihrer Infrastruktur. Jedes Team implementiert sie auf andere Weise.

Vorteile der Nutzung dieser bewährten Methode: Die Verwendung gemeinsamer Standards unterstützt die Umsetzung bewährter Methoden und maximiert den Nutzen der Entwicklungsarbeit.

Durch die Dokumentation und Aktualisierung von Designstandards wird Ihr Unternehmen stets up-to-date über bewährte Verfahren und Sicherheits- und Compliance-Anforderungen informiert.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Mittel

### Implementierungsleitfaden

Nutzen Sie bewährte Methoden, Designstandards, Checklisten, Arbeitsverfahren, Leitlinien und Governance-Anforderungen in allen Teams. Verwenden Sie Verfahren zur Anforderung von Änderungen, Ergänzungen und Ausnahmen von Designstandards, um Verbesserungen und Innovationen zu unterstützen. Stellen Sie sicher, dass die Teams über die veröffentlichten Inhalte informiert sind. Verfügen Sie über einen Mechanismus zur Beibehaltung von Designstandards up-to-date, wenn neue bewährte Verfahren auftauchen.

### Kundenbeispiel

AnyCompany Der Einzelhandel verfügt über ein funktionsübergreifendes Architekturteam, das Softwarearchitekturmuster erstellt. Dieses Team entwickelt die Architektur mit integrierter Compliance und Governance. Teams, die diese gemeinsamen Standards anwenden, profitieren davon, dass Compliance und Governance bereits integriert sind. Sie können schnell auf dem Designstandard aufbauen. Das Architekturteam trifft sich vierteljährlich, um die Architekturmuster zu bewerten und sie gegebenenfalls zu aktualisieren.

### Implementierungsschritte

1. Bestimmen Sie ein funktionsübergreifendes Team, das für die Entwicklung und Aktualisierung der Designstandards zuständig ist. Dieses Team sollte mit Stakeholdern in Ihrer gesamten Organisation zusammenarbeiten, um Designstandards, Arbeitsverfahren, Checklisten, Leitlinien und Governance-Anforderungen zu entwickeln. Dokumentieren Sie die Designstandards und geben Sie sie innerhalb Ihrer Organisation weiter.
  - a. Mit [AWS Service Catalog](#) können Sie Portfolios erstellen, die Designstandards als Infrastructure-as-Code abbilden. Sie können Portfolios über Konten hinweg gemeinsam nutzen.
2. Setzen Sie einen Mechanismus ein, um Designstandards beizubehalten, up-to-date sobald neue bewährte Verfahren identifiziert werden.
3. Wenn Designstandards zentral durchgesetzt werden, sollten Sie über ein Verfahren verfügen, um Änderungen, Aktualisierungen und Ausnahmen anzufordern.

Aufwand für den Implementierungsplan: Mittel. Die Entwicklung eines Prozesses zur Erstellung und gemeinsamen Nutzung von Designstandards kann die Koordination und Zusammenarbeit mit Stakeholdern in Ihrer gesamten Organisation erforderlich machen.

## Ressourcen

### Zugehörige bewährte Methoden:

- [OPS01-BP03 Bewertung der Governance-Anforderungen](#) – Governance-Anforderungen beeinflussen Designstandards.
- [OPS01-BP04 Evaluieren Sie die Compliance-Anforderungen](#) – Compliance ist ein wichtiger Faktor bei der Erstellung von Designstandards.
- [OPS07-BP02 Stellen Sie eine konsistente Überprüfung der Betriebsbereitschaft sicher](#) – Checklisten für die operative Einsatzbereitschaft sind ein Mechanismus zur Umsetzung von Designstandards bei der Gestaltung Ihrer Workload.
- [OPS11-BP01 Haben Sie einen Prozess zur kontinuierlichen Verbesserung](#) – Die Aktualisierung von Designstandards ist ein Teil der kontinuierlichen Verbesserung.
- [OPS11-BP04 Wissensmanagement durchführen](#) – Als Teil Ihres Wissensmanagements sollten Sie Designstandards dokumentieren und weitergeben.

### Zugehörige Dokumente:

- [Automatisieren Sie AWS Backup und mit AWS Service Catalog](#)
- [AWS Service Catalog Ab Werk erweitertes Konto](#)
- [Wie die Expedia Group das Database-as-a-Service \(\) -Angebot \(\) DBaaS mithilfe von AWS Service Catalog](#)
- [Überblick über die Nutzung von Cloud-Architekturmustern](#)
- [Vereinfachen Sie die gemeinsame Nutzung Ihrer AWS Service Catalog Portfolios in einem Setup AWS Organizations](#)

### Zugehörige Videos:

- [AWS Service Catalog — Erste Schritte](#)
- [AWS re:Invent 2020: Managen Sie Ihre AWS Service Catalog Portfolios wie ein Experte](#)

### Zugehörige Beispiele:



- [AWS Service Catalog Referenzarchitektur](#)
- [AWS Service Catalog Werkstatt](#)

Zugehörige Services:

- [AWS Service Catalog](#)

OPS05-BP07 Implementieren Sie Praktiken zur Verbesserung der Codequalität

Implementieren Sie Verfahren zur Verbesserung der Codequalität und Minimierung von Fehlern. Einige Beispiele sind die testbasierte Entwicklung, Code-Reviews, die Einführung von Standards und Pair-Programming. Integrieren Sie diese Verfahren in Ihren Continuous-Integration- und Continuous-Delivery-Prozess.

Gewünschtes Ergebnis: Ihre Organisation setzt bewährte Methoden wie Code-Reviews oder Pair-Programming ein, um die Codequalität zu verbessern. Entwickler und operative Mitarbeiter nutzen bewährte Methoden zur Codequalität als Teil des Softwareentwicklungslebenszyklus.

Typische Anti-Muster:

- Sie führen ohne Code-Review Commits zum Main-Branch Ihrer Anwendung durch. Die Änderung wird automatisch in der Produktion bereitgestellt und verursacht einen Ausfall.
- Eine neue Anwendung wird ohne Einheiten- oder end-to-end Integrationstests entwickelt. Es gibt keine Möglichkeit, die Anwendung vor der Bereitstellung zu testen.
- Ihre Teams nehmen manuelle Änderungen in der Produktion vor, um Fehler zu beheben. Die Änderungen durchlaufen keine Tests oder Code-Reviews und werden nicht durch kontinuierliche Integrations- und Bereitstellungsprozesse erfasst oder protokolliert.

Vorteile der Nutzung dieser bewährten Methode: Durch die Umsetzung von Methoden zur Verbesserung der Codequalität können Sie die Anzahl der Probleme minimieren, die bei der Produktion noch vorhanden sind. Die Codequalität erleichtert die Anwendung von bewährten Methoden wie Paarprogrammierung, Code-Reviews und Implementierung von KI-Produktivitätstools.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel

## Implementierungsleitfaden

Implementieren Sie Verfahren zur Verbesserung der Codequalität, um vor der Bereitstellung Fehler zu minimieren. Nutzen Sie Verfahren wie die testbasierte Entwicklung, Code-Reviews und Pair-Programming, um die Qualität Ihrer Entwicklung zu verbessern.

Nutzen Sie die Leistungsfähigkeit generativer KI mit Amazon Q Developer, um die Entwicklerproduktivität und die Codequalität zu verbessern. Amazon Q Developer umfasst die Generierung von Codevorschlägen (basierend auf großen Sprachmodellen), die Erstellung von Komponententests (einschließlich Randbedingungen) und Verbesserungen der Codesicherheit durch die Erkennung und Behebung von Sicherheitsschwachstellen.

### Kundenbeispiel

**AnyCompany** Der Einzelhandel wendet verschiedene Verfahren an, um die Codequalität zu verbessern. Die testbasierte Entwicklung ist der Standard für die Entwicklung von Anwendungen. Bei einigen neuen Funktionen arbeiten die Entwickler während eines Sprints zusammen. Jede Pull-Anforderung wird von einem erfahrenen Entwickler überprüft, bevor sie integriert und bereitgestellt wird.

### Implementierungsschritte

1. Setzen Sie bei Ihrem kontinuierlichen Integrations- und Bereitstellungsprozess auf Code-Qualitätsverfahren wie die testbasierte Entwicklung, Code-Reviews und Pair-Programming. Nutzen Sie diese Techniken, um die Softwarequalität zu verbessern.
  - a. Verwenden Sie [Amazon Q Developer](#), ein generatives KI-Tool, mit dem Sie Modultestfälle (einschließlich Randbedingungen) erstellen, Funktionen mithilfe von Code und Kommentaren generieren, bekannte Algorithmen implementieren, Verstöße gegen Sicherheitsrichtlinien und Schwachstellen in Ihrem Code erkennen, Geheimnisse aufdecken, Infrastructure as Code (IaC) scannen, Code dokumentieren und Codebibliotheken von Drittanbietern schneller erlernen können.
  - b. [Amazon CodeGuru Reviewer](#) kann Programmierempfehlungen für Java- und Python-Code mithilfe von maschinellem Lernen geben.
  - c. Sie können mit [AWS Cloud9](#) gemeinsame Entwicklungsumgebungen erstellen und Code in Teamarbeit entwickeln.

Aufwand für den Implementierungsplan: Mittel. Es gibt viele Möglichkeiten zur Umsetzung dieser bewährten Methode. Es kann jedoch schwierig sein, die Akzeptanz im Unternehmen zu erreichen.

## Ressourcen

### Zugehörige bewährte Methoden:

- [OPS05-BP02 Testen und validieren Sie Änderungen](#)
- [OPS05-BP06 Teilen Sie die Designstandards](#)

### Zugehörige Dokumente:

- [Einen testgetriebenen Entwicklungsansatz verwenden](#)
- [Beschleunigen Ihres Softwareentwicklungszyklus mit Amazon Q](#)
- [Amazon Q Developer \(jetzt allgemein verfügbar\) enthält Vorschauen neuer Funktionen, mit denen Sie das Entwicklererlebnis neu gestalten können](#)
- [Der ultimative Spickzettel für die Verwendung von Amazon Q Developer in Ihrem IDE](#)
- [Shift-Left-Workload, Nutzung von KI für die Testerstellung](#)
- [Amazon Q-Entwicklerzentrum](#)
- [10 Möglichkeiten, Anwendungen mit Amazon schneller zu erstellen CodeWhisperer](#)
- [Mit Amazon geht der Blick über die Codeabdeckung hinaus CodeWhisperer](#)
- [Bewährte Methoden für schnelles Engineering mit Amazon CodeWhisperer](#)
- [Leitfaden für agile Software](#)
- [Meine CI/CD-Pipeline ist mein Release Captain](#)
- [Automatisieren Sie Code-Reviews mit Amazon CodeGuru Reviewer](#)
- [Einen testgetriebenen Entwicklungsansatz verwenden](#)
- [Wie DevFactory entwickelt Amazon bessere Anwendungen CodeGuru](#)
- [Über Pair-Programming](#)
- [RENGAInc. automatisiert Code-Reviews mit Amazon CodeGuru](#)
- [Die Kunst der agilen Entwicklung: Testbasierte Entwicklung](#)
- [Warum Code-Reviews wichtig sind \(und tatsächlich Zeit sparen!\)](#)

### Zugehörige Videos:

- [Implementieren Sie einen API mit Amazon Q Developer Agent für Softwareentwicklung](#)

- [Installation, Konfiguration und Verwendung von Amazon Q Developer mit JetBrains IDEs \(Anleitung\)](#)
- [Die Kunst von Amazon beherrschen CodeWhisperer — Playlist YouTube](#)
- [AWS re:Invent 2020: Kontinuierliche Verbesserung der Codequalität mit Amazon CodeGuru](#)
- [AWS Summit ANZ 2021 — Förderung einer Test-First-Strategie mit testgetriebener Entwicklung CDK](#)

Zugehörige Services:

- [Amazon Q Developer](#)
- [CodeGuru Amazon-Rezensent](#)
- [Amazon CodeGuru Profiler](#)
- [AWS Cloud9](#)

OPS05-BP08 Verwenden Sie mehrere Umgebungen

Verwenden Sie mehrere Umgebungen, um Ihre Workload auszuprobieren, zu entwickeln und zu testen. Verwenden Sie zunehmende Kontrollstufen, wenn Umgebungen sich der Produktion nähern, um sicherzustellen, dass Ihre Workload bei der Bereitstellung wie beabsichtigt funktioniert.

Gewünschtes Ergebnis: Sie verfügen über mehrere Umgebungen, die Ihre Compliance- und Governance-Anforderungen widerspiegeln. Auf Ihrem Weg zur Produktion testen und promoten Sie Code in Umgebungen.

Typische Anti-Muster:

- Sie führen die Entwicklung in einer gemeinsamen Entwicklungsumgebung durch und ein weiterer Entwickler überschreibt Ihre Codeänderungen.
- Die restriktiven Sicherheitskontrollen Ihrer gemeinsamen Entwicklungsumgebung verhindern, dass Sie mit neuen Services und Funktionen experimentieren können.
- Sie führen Belastungstests auf Ihren Produktionssystemen durch und verursachen einen Ausfall für Ihre Benutzer.
- In der Produktion ist ein kritischer Fehler aufgetreten, der zum Verlust von Daten geführt hat. In Ihrer Produktionsumgebung versuchen Sie, die Bedingungen, die zum Datenverlust geführt haben, nachzustellen, damit Sie die Ursache feststellen und beseitigen können. Um einen weiteren

Datenverlust während des Testens zu verhindern, müssen Sie die Anwendung für Ihre Benutzer deaktivieren.

- Sie betreiben einen Mehrmandanten-Service und können eine Kundenanfrage nach einer eigenen Umgebung nicht erfüllen.
- Möglicherweise testen Sie nicht immer, aber wenn Sie dies tun, testen Sie in Ihrer Produktionsumgebung.
- Sie glauben, dass die Einfachheit einer einzelnen Umgebung die Auswirkungen von Änderungen innerhalb der Umgebung ausgleicht.

Vorteile der Nutzung dieser bewährten Methode: Sie können gleichzeitig mehrere Entwicklungs-, Test- und Produktionsumgebungen unterstützen, ohne Konflikte zwischen Entwicklern oder User-Communities zu erzeugen.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel

### Implementierungsleitfaden

Verwenden Sie mehrere Umgebungen und stellen Sie den Entwicklern Sandbox-Umgebungen mit weniger Kontrollen zur Verfügung, in denen sie experimentieren können. Richten Sie individuelle Entwicklungsumgebungen ein, damit parallele Arbeit möglich ist. Dadurch steigern Sie die Agilität der Entwicklung. Implementieren Sie strengere Kontrollen erst in den Umgebungen, die kurz vor der Produktionsaufnahme stehen, damit Entwickler Innovationen schaffen können. Nutzen Sie die Infrastruktur als Code sowie Konfigurationsverwaltungssysteme, um Umgebungen bereitzustellen, die mit den in der Produktion vorhandenen Kontrollen einheitlich konfiguriert sind. Auf diese Weise können Sie sicherstellen, dass die Systeme bei der Bereitstellung wie erwartet funktionieren. Wenn Umgebungen nicht in Gebrauch sind, schalten Sie sie ab, um Kosten für ungenutzte Ressourcen zu vermeiden (z. B. Entwicklungssysteme am Abend und am Wochenende). Stellen Sie beim Belastungstest produktionsgleiche Umgebungen bereit, um die Gültigkeit der Ergebnisse zu verbessern.

### Ressourcen

Zugehörige Dokumente:

- [Instance Scheduler aktiviert AWS](#)
- [Was ist AWS CloudFormation?](#)

## OPS05-BP09 Nehmen Sie häufige, kleine, reversible Änderungen vor

Häufige, kleine und reversible Änderungen verringern den Umfang und die Auswirkung einer Änderung. In Verbindung mit Change-Management-Systemen, Systemen zur Konfigurationsverwaltung und Build- und Liefersystemen reduzieren häufige, kleine und reversible Änderungen den Umfang und die Auswirkungen einer Änderung. Dies macht die Fehlersuche effizienter und ermöglicht eine schnellere Korrektur, da die Möglichkeit besteht, Änderungen zurückzusetzen.

Typische Anti-Muster:

- Sie stellen vierteljährlich eine neue Version Ihrer Anwendung mit einem Änderungsfenster bereit, was bedeutet, dass ein zentraler Dienst ausgeschaltet wird.
- Sie nehmen häufig Änderungen an Ihrem Datenbankschema vor, ohne Änderungen in Ihren Managementsystemen nachzuverfolgen.
- Sie führen direkte manuelle Updates durch, überschreiben damit bestehende Installationen und Konfigurationen und haben keinen klaren Rollback-Plan.

Vorteile der Nutzung dieser bewährten Methode: Sie profitieren schneller von den Entwicklungsarbeiten, wenn Sie häufig kleine Änderungen bereitstellen. Wenn die Änderungen klein sind, ist es viel einfacher zu erkennen, ob sie unbeabsichtigte Folgen haben, und sie lassen sich leichter rückgängig machen. Wenn die Änderungen rückgängig gemacht werden können, ist die Implementierung mit geringeren Risiken verbunden, da die Wiederherstellung einfacher ist. Der Änderungsprozess hat ein geringeres Risiko und die Auswirkungen einer fehlgeschlagenen Änderung werden reduziert.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Niedrig

Implementierungsleitfaden

Machen Sie häufige, kleine und reversible Änderungen und verringern Sie dadurch den Umfang und die Auswirkung einer Änderung. Dies erleichtert die Fehlersuche, trägt zur Beschleunigung der Fehlerbehebung bei und bietet die Möglichkeit, eine Änderung zurückzusetzen. Außerdem profitiert Ihr Unternehmen schneller von neuen Entwicklungen.

Ressourcen

Zugehörige bewährte Methoden:

- [OPS05-BP03 Verwenden Sie Konfigurationsmanagementsysteme](#)

- [OPS05-BP04 Verwenden Sie Build- und Deployment-Management-Systeme](#)
- [OPS06-BP04 Automatisieren Sie Tests und Rollback](#)

Zugehörige Dokumente:

- [Implementierung von Microservices auf AWS](#)
- [Microservices – Beobachtbarkeit](#)

## OPS05- BP1 0 Vollständig automatisierte Integration und Bereitstellung

Automatisieren Sie den Aufbau, die Bereitstellung und die Tests der Workloads. Dadurch werden Fehler aufgrund von manuellen Prozessen und der Aufwand für die Bereitstellung von Änderungen verringert.

Wenden Sie Metadaten mithilfe von [Ressourcen-Tags](#) und [AWS Resource Groups](#) nach einer konsistenten [Tagging-Strategie](#) an, um die Identifizierung Ihrer Ressourcen zu erleichtern. Versehen Sie Ihre Ressourcen mit Tags für Organisation, Kostenkalkulation, Zugriffssteuerung und Zielrichtung der Ausführung von automatisierten Betriebsaktivitäten.

Gewünschtes Ergebnis: Entwickler verwenden Tools, um Code bereitzustellen und bis zur Produktion zu unterstützen. Entwickler müssen sich nicht bei der anmelden AWS Management Console , um Updates bereitzustellen. Es gibt einen vollständigen Audit Trail für Änderungen und Konfigurationen, der die Governance- und Compliance-Anforderungen erfüllt. Prozesse sind wiederholbar und teamübergreifend standardisiert. Entwickler sind in der Lage, sich auf die Entwicklung und Code-Pushs zu konzentrieren, sodass die Produktivität steigt.

Typische Anti-Muster:

- Am Freitag schließen Sie die Erstellung des neuen Codes für Ihren Feature-Zweig ab. Am Montag, nach dem Ausführen Ihrer Skripts für die Codequalitätstests und einzelnen Komponententests, überprüfen Sie Ihren Code für den nächsten geplanten Release.
- Sie erhalten die Aufgabe, eine Korrektur für ein kritisches Problem zu schreiben, das sich auf eine große Anzahl von Kunden in der Produktion auswirkt. Nachdem Sie die Korrektur getestet haben, übermitteln Sie Ihren Code und fordern beim Änderungsmanagement die Bereitstellungsgenehmigung zur Produktion an.
- Als Entwickler melden Sie sich bei der AWS Management Console an, um eine neue Entwicklungsumgebung mit nicht standardmäßigen Methoden und Systemen zu erstellen.

Vorteile der Nutzung dieser bewährten Methode: Durch die Implementierung automatisierter Build- und Bereitstellungsverwaltungssysteme reduzieren Sie Fehler aus manuellen Prozessen und den Aufwand für die Bereitstellung von Änderungen, sodass sich Ihre Teammitglieder auf die Wertschöpfung konzentrieren können. Sie erhöhen die Liefergeschwindigkeit auf Ihrem Weg zur Produktion.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Niedrig

### Implementierungsleitfaden

Verwenden Sie Systeme zur Build- und Bereitstellungsverwaltung für die Verfolgung und Implementierung von Änderungen, die Reduzierung von Fehlern, die durch manuelle Prozesse entstehen, sowie zur Verringerung des Aufwands. Nutzen Sie eine vollständig automatisierte Integrations- und Bereitstellungs-Pipeline vom Einchecken des Codes über das Testen und die Bereitstellung bis hin zur Validierung. Dies reduziert die Vorlaufzeit, fördert häufigere Änderungen, reduziert den Aufwand, beschleunigt die Markteinführung, führt zu einer höheren Produktivität und erhöht die Sicherheit Ihres Codes bis hin zur Produktion.

### Ressourcen

Zugehörige bewährte Methoden:

- [OPS05-BP03 Verwenden Sie Konfigurationsmanagementsysteme](#)
- [OPS05-BP04 Verwenden Sie Build- und Deployment-Management-Systeme](#)

Zugehörige Dokumente:

- [Was ist AWS CodeBuild?](#)
- [Was ist AWS CodeDeploy?](#)

Zugehörige Videos:

- [AWS re\ :Invent 2022 — AWS Well-Architected Best Practices für DevOps AWS](#)

## OPS6. Wie können Sie Bereitstellungsrisiken eindämmen?

Verwenden Sie Ansätze, die schnelles Feedback zur Qualität liefern und eine schnelle Wiederherstellung bei Änderungen ermöglichen, die nicht zu den gewünschten Ergebnissen führen.



Mit diesen Verfahren können Sie die Auswirkung von Problemen eindämmen, die durch Änderungen entstehen.

### Bewährte Methoden

- [OPS06-BP01 Plan für erfolglose Änderungen](#)
- [OPS06-BP02 Testbereitstellungen](#)
- [OPS06-BP03 Setzen Sie sichere Einsatzstrategien ein](#)
- [OPS06-BP04 Automatisieren Sie Tests und Rollback](#)

### OPS06-BP01 Plan für erfolglose Änderungen

Planen Sie Maßnahmen für die Rückkehr zu einem bekanntermaßen funktionierenden Zustand oder die Korrektur in der Produktionsumgebung ein, falls bei der Bereitstellung ein nicht erwünschtes Ergebnis auftritt. Eine Richtlinie zur Festlegung eines solchen Plans hilft allen Teams, Strategien zum Umgang mit fehlgeschlagenen Änderungen zu entwickeln. Einige Beispiele für Strategien sind Bereitstellungs- und Rollback-Schritte, Änderungsrichtlinien, Feature-Flags sowie die Isolierung und Verlagerung von Datenverkehr. Ein einzelner Release kann mehrere zusammengehörige Komponentenänderungen enthalten. Die Strategie sollte die Möglichkeit bieten, dem Ausfall einer Komponentenänderung standzuhalten oder sich danach zu regenerieren.

Gewünschtes Ergebnis: Sie haben einen detaillierten Wiederherstellungsplan für Ihre Änderung erstellt, falls diese nicht erfolgreich sein sollte. Darüber hinaus haben Sie die Größe Ihres Releases reduziert, um die potenziellen Auswirkungen auf andere Workload-Komponenten zu minimieren. Infolgedessen haben Sie die Auswirkungen auf Ihr Unternehmen verringert, indem Sie die potenziellen Ausfallzeiten aufgrund einer fehlgeschlagenen Änderung reduziert und die Flexibilität und Effizienz der Wiederherstellungszeiten erhöht haben.

### Typische Anti-Muster:

- Sie haben Code bereitgestellt und Ihre Anwendung ist instabil geworden, aber es befinden sich aktive Benutzer im System. Sie müssen entscheiden, ob Sie die Änderung rückgängig machen und Auswirkungen auf die aktiven Benutzer in Kauf nehmen möchten, oder ob Sie die Änderung erst später rückgängig machen möchten, wodurch möglicherweise trotzdem Auswirkungen auf die Benutzer entstehen könnten.
- Nachdem Sie eine Routineänderung vorgenommen haben, kann auf Ihre neuen Umgebungen zugegriffen werden, aber eines Ihrer Subnetze ist nicht mehr erreichbar. Sie müssen entscheiden, ob Sie die gesamte Änderung rückgängig machen oder versuchen, die Nichtverfügbarkeit des

Subnetzes zu beheben. Während Sie diese Entscheidung abwägen, bleibt das Subnetz nicht erreichbar.

- Ihre Systeme sind nicht so konzipiert, dass sie mit kleineren Releases aktualisiert werden können. Daher haben Sie Schwierigkeiten, die Bulk-Änderungen während einer fehlgeschlagenen Bereitstellung rückgängig zu machen.
- Sie verwenden nicht Infrastructure as Code (IaC) und Sie haben manuelle Aktualisierungen an Ihrer Infrastruktur vorgenommen, die zu einer unerwünschten Konfiguration geführt haben. Sie sind nicht in der Lage, die manuellen Änderungen effektiv zu verfolgen und rückgängig zu machen.
- Da Sie die erhöhte Häufigkeit Ihrer Bereitstellungen nicht gemessen haben, hat Ihr Team keinen Anreiz, den Umfang seiner Änderungen zu reduzieren und seine Rollback-Pläne für jede Änderung zu verbessern. Dies führt zu höheren Risiken und höheren Ausfallraten.
- Sie messen nicht die Gesamtdauer eines Ausfalls, der durch erfolglose Änderungen verursacht wird. Ihr Team ist nicht in der Lage, den Bereitstellungsprozess und die Effektivität des Wiederherstellungsplans zu priorisieren und zu verbessern.

Vorteile der Einführung dieser bewährten Methode: Wenn Sie einen Plan für die Wiederherstellung nach erfolglosen Änderungen haben, wird die durchschnittliche Wiederherstellungszeit (MTTR) minimiert und die Auswirkungen auf Ihr Unternehmen verringert.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Hoch

### Implementierungsleitfaden

Mithilfe einer konsistenten, dokumentierten Richtlinie und Praxis, die von den Release-Teams angewendet wird, kann ein Unternehmen planen, was bei nicht erfolgreichen Änderungen passieren soll. Unter bestimmten Umständen sollte die Richtlinie ein Forward-Fixing berücksichtigen. In allen Fällen sollte ein Fix-Forward- oder Rollback-Plan vor der Bereitstellung in der Live-Produktion gut dokumentiert und getestet werden, um die benötigte Zeit zum Rückgängigmachen einer Änderung zu minimieren.

### Implementierungsschritte

1. Dokumentieren Sie die Richtlinien, nach denen Teams über wirksame Pläne verfügen müssen, wie Änderungen innerhalb eines bestimmten Zeitraums rückgängig gemacht werden können.
  - a. In den Richtlinien sollte festgelegt sein, wann eine Fix-Forward-Situation zulässig ist.
  - b. Erfordern Sie einen dokumentierten Rollback-Plan, auf den alle Beteiligten zugreifen können.

- c. Geben Sie die Anforderungen für das Rollback an (z. B. wenn festgestellt wird, dass nicht autorisierte Änderungen vorgenommen wurden).
2. Analysieren Sie den Grad der Auswirkungen aller Änderungen für jede Komponente einer Workload.
    - a. Ermöglichen Sie die Standardisierung, Vorlagenerstellung und Vorautorisierung wiederholbarer Änderungen, sofern sie einem konsistenten Workflow folgen, der Änderungsrichtlinien durchsetzt.
    - b. Reduzieren Sie die potenziellen Auswirkungen jeder Änderung, indem Sie den Umfang der Änderung verringern, damit die Wiederherstellung weniger Zeit in Anspruch nimmt und weniger Auswirkungen auf das Unternehmen hat.
    - c. Stellen Sie sicher, dass die Rollback-Verfahren den Code in einen bekannt funktionierenden Zustand zurückversetzen, um Zwischenfälle nach Möglichkeit zu vermeiden.
  3. Integrieren Sie Tools und Workflows, um Ihre Richtlinien programmgesteuert durchzusetzen.
  4. Machen Sie Daten zu Änderungen für andere Workload-Besitzer sichtbar, um die Diagnose bei fehlgeschlagenen Änderungen, für die kein Rollback möglich ist, zu beschleunigen.
    - a. Messen Sie den Erfolg dieser Methode anhand sichtbarer Änderungsdaten und identifizieren Sie iterative Verbesserungen.
  5. Verwenden Sie Überwachungstools, um den Erfolg oder Misserfolg einer Bereitstellung zu überprüfen und so die Entscheidungsfindung beim Rollback zu beschleunigen.
  6. Messen Sie die Dauer des Ausfalls bei einer erfolglosen Änderung, um Ihre Wiederherstellungspläne kontinuierlich zu verbessern.

Aufwand für den Implementierungsplan: Mittel

Ressourcen

Zugehörige bewährte Methoden:

- [OPS06-BP04 Automatisieren Sie Tests und Rollback](#)

Zugehörige Dokumente:

- [AWS Builders Library | Gewährleistung der Rollback-Sicherheit bei Bereitstellungen](#)
- [AWS Whitepaper | Änderungsmanagement in der Cloud](#)

## Zugehörige Videos:

- [re:Invent 2019 | Der Amazon-Ansatz für die Hochverfügbarkeitsbereitstellung](#)

## OPS06-BP02 Testbereitstellungen

Testen Sie Release-Verfahren in der Vorproduktion, indem Sie dieselbe Bereitstellungsconfiguration, dieselben Sicherheitskontrollen, Schritte und Verfahren wie in der Produktion verwenden. Stellen Sie sicher, dass alle bereitgestellten Schritte wie erwartet abgeschlossen wurden, z. B. das Überprüfen von Dateien, Konfigurationen und Services. Testen Sie alle Änderungen darüber hinaus mit Funktions-, Integrations- und Auslastungstests sowie Überwachungsverfahren, z. B. Zustandsprüfungen. Durch diese Tests können Sie Bereitstellungsprobleme frühzeitig erkennen und haben die Möglichkeit, sie vor der Produktion einzuplanen und zu beheben.

Sie können temporäre parallele Umgebungen erstellen, um jede Änderung zu testen. Automatisieren Sie die Bereitstellung der Testumgebungen mithilfe von Infrastructure as Code (IaC), um den Arbeitsaufwand zu reduzieren und Stabilität, Konsistenz und schnellere Feature-Bereitstellung zu gewährleisten.

Gewünschtes Ergebnis: Ihr Unternehmen führt eine testgestützte Entwicklungskultur ein, die Testbereitstellungen einschließt. Dadurch wird sichergestellt, dass sich die Teams darauf konzentrieren, Werte für das Unternehmen zu schaffen, anstatt Releases zu verwalten. Die Teams werden bei der Identifizierung von Bereitstellungsrisiken frühzeitig einbezogen, um die geeigneten Maßnahmen zur Risikominderung festzulegen.

## Typische Anti-Muster:

- Während Produktionseinführungen führen ungetestete Bereitstellungen häufig zu Problemen, die eine Fehlerbehebung und Eskalation erfordern.
- Ihr Release enthält Infrastructure as Code (IaC), wodurch vorhandene Ressourcen aktualisiert werden. Sie sind sich nicht sicher, ob IaC erfolgreich ausgeführt wird oder ob es Auswirkungen auf die Ressourcen gibt.
- Sie stellen ein neues Feature für Ihre Anwendung bereit. Sie funktioniert nicht wie beabsichtigt und dies fällt erst auf, als sie von betroffenen Benutzern gemeldet wird.
- Sie aktualisieren Ihre Zertifikate. Sie installieren versehentlich die Zertifikate für die falschen Komponenten, was unentdeckt bleibt und Auswirkungen auf Website-Benutzer hat, da keine sichere Verbindung zur Website hergestellt werden kann.

Vorteile der Nutzung dieser bewährten Methode: Durch umfangreiche Tests der Bereitstellungsverfahren und der durch sie eingeführten Änderungen in der Vorproduktion werden die potenziellen Auswirkungen der Bereitstellungsschritte auf die Produktion minimiert. Dies erhöht das Vertrauen bei der Produktionseinführung und minimiert den Support während des Betriebs, ohne die bereitgestellten Änderungen zu verlangsamen.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Hoch

### Implementierungsleitfaden

Das Testen Ihres Bereitstellungsprozesses ist genauso wichtig wie das Testen der Änderungen, die sich aus der Bereitstellung ergeben. Dies kann erreicht werden, indem Sie Ihre Bereitstellungsschritte in einer Vorproduktionsumgebung testen, die die Produktion so genau wie möglich widerspiegelt. Häufig auftretende Probleme, z. B. unvollständige oder falsche Bereitstellungsschritte oder Fehlkonfigurationen, können so vor der Bereitstellung in der Produktionsumgebung erkannt werden. Darüber hinaus können Sie Ihre Wiederherstellungsschritte testen.

### Kundenbeispiel

Im Rahmen seiner CI/CD-Pipeline (Continuous Integration and Continuous Delivery) führt AnyCompany Retail die definierten Schritte durch, die zur Veröffentlichung von Infrastruktur- und Softwareupdates für seine Kunden in einer Produktionsumgebung erforderlich sind. Die Pipeline besteht aus Vorabprüfungen zur Erkennung von Abweichungen (Erkennung von Änderungen an Ressourcen, die außerhalb von IaC vorgenommen wurden) bei Ressourcen vor der Bereitstellung sowie zur Validierung der Aktionen, die von IaC bei der Initiierung ausgeführt werden. Vor der erneuten Registrierung beim Load Balancer werden Bereitstellungsschritte validiert und z. B. sichergestellt, dass bestimmte Dateien und Konfigurationen vorhanden sind und Services ausgeführt werden und korrekt auf Zustandsprüfungen auf dem lokalen Host reagieren. Darüber hinaus führen alle Änderungen zu einer Reihe automatisierter Tests wie Funktions-, Sicherheits-, Regressions-, Integrations- und Auslastungstests.

### Implementierungsschritte

1. Führen Sie Prüfungen vor der Installation durch, um die Vorproduktionsumgebung in der Produktionsumgebung zu spiegeln.
  - a. Verwenden Sie die [Drift-Erkennung](#), um zu erkennen, wann Ressourcen außerhalb von geändert wurden. AWS CloudFormation

- b. Verwenden Sie [Änderungssätze](#), um zu überprüfen, ob die Absicht eines Stack-Updates mit den Aktionen übereinstimmt, die AWS CloudFormation bei der Initiierung des Änderungssatzes ausgeführt werden.
2. Dadurch wird ein manueller Genehmigungsschritt in [AWS CodePipeline](#) ausgelöst, um die Bereitstellung in der Vorproduktionsumgebung zu autorisieren.
3. Verwenden Sie Bereitstellungsconfigurationen wie [AWS CodeDeploy AppSpec](#) Dateien, um Bereitstellungs- und Validierungsschritte zu definieren.
4. [Integrieren Sie AWS CodeDeploy gegebenenfalls andere AWS Dienste](#) oder [integrieren Sie AWS CodeDeploy sie in Produkte und Services von Partnern](#).
5. [Überwachen Sie Bereitstellungen](#) mithilfe von Amazon CloudWatch, AWS CloudTrail, und SNS Amazon-Ereignisbenachrichtigungen.
6. Führen Sie nach der Bereitstellung automatisierte Tests durch, einschließlich Funktions-, Sicherheits-, Regressions-, Integrations- und Auslastungstests.
7. Führen Sie die [Fehlersuche](#) bei Problemen mit der Bereitstellung aus.
8. Eine erfolgreiche Validierung der zuvor genannten Schritte sollte einen manuellen Genehmigungsworkflow initiieren, um die Bereitstellung in der Produktion zu autorisieren.

Aufwand für den Implementierungsplan: Hoch

Ressourcen

Zugehörige bewährte Methoden:

- [OPS05-BP02 Änderungen testen und validieren](#)

Zugehörige Dokumente:

- [AWS Builders' Library | Automatisieren von sicheren, automatischen Bereitstellungen | Testbereitstellungen](#)
- [AWS Whitepaper | Praktische Umsetzung von Continuous Integration und Continuous Delivery am AWS](#)
- [Die Geschichte von Apollo – Die Deployment Engine von Amazon](#)
- [Wie können Sie AWS CodeDeploy lokal testen und debuggen, bevor Sie Ihren Code versenden](#)
- [Integration von Netzwerkkonnektivitätstests in die Bereitstellung der Infrastruktur](#)

## Zugehörige Videos:

- [re:Invent 2020 | Testen von Software und Systemen bei Amazon](#)

## Zugehörige Beispiele:

- [Tutorial | Bereitstellen und ECS Amazon-Service mit einem Validierungstest](#)

## OPS06-BP03 Setzen Sie sichere Einsatzstrategien ein

Sichere Produktionseinführungen steuern den Fluss vorteilhafter Änderungen mit dem Ziel, die von den Kunden wahrgenommenen Auswirkungen dieser Änderungen zu minimieren. Die Sicherheitskontrollen bieten Prüfmechanismen, um die gewünschten Ergebnisse zu validieren und den Umfang der Auswirkungen von Fehlern zu begrenzen, die durch die Änderungen oder durch Fehler bei der Bereitstellung verursacht werden. Zu sicheren Rollouts können Strategien wie Feature-Flags, One-Box, Rolling (Canary-Releases), Immutable, Aufteilung des Datenverkehrs und Blau/Grün-Bereitstellungen gehören.

Gewünschtes Ergebnis: Ihr Unternehmen verwendet ein CI/CD-System (Continuous Integration/Continuous Delivery, kontinuierliche Integration/kontinuierliche Bereitstellung), das Funktionen zur Automatisierung sicherer Rollouts bietet. Die Teams müssen angemessene sichere Rollout-Strategien anwenden.

## Typische Anti-Muster:

- Sie stellen eine nicht erfolgreiche Änderung für die gesamte Produktion gleichzeitig bereit. Infolgedessen sind alle Kunden gleichzeitig betroffen.
- Ein Fehler, der bei einer gleichzeitigen Bereitstellung in allen Systemen auftritt, erfordert ein Notfall-Release. Die Korrektur für alle Kunden dauert mehrere Tage.
- Die Verwaltung der Produktionseinführung erfordert die Planung und Beteiligung mehrerer Teams. Dies schränkt Ihre Fähigkeit ein, Features für Ihre Kunden häufig zu aktualisieren.
- Sie führen eine veränderbare Bereitstellung durch, indem Sie Ihre vorhandenen Systeme ändern. Nachdem Sie festgestellt haben, dass die Änderung nicht erfolgreich war, müssen Sie die Systeme erneut ändern, um die alte Version wiederherzustellen, was die Wiederherstellungsdauer verlängert.

Vorteile der Nutzung dieser bewährten Methode: Automatisierte Bereitstellungen sorgen für ein ausgewogenes Verhältnis zwischen der Geschwindigkeit der Bereitstellungen und der konsistenten Bereitstellung nützlicher Änderungen für die Kunden. Die Begrenzung der Auswirkungen verhindert kostspielige Bereitstellungsfehler und maximiert die Fähigkeit der Teams, effizient auf Ausfälle zu reagieren.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel

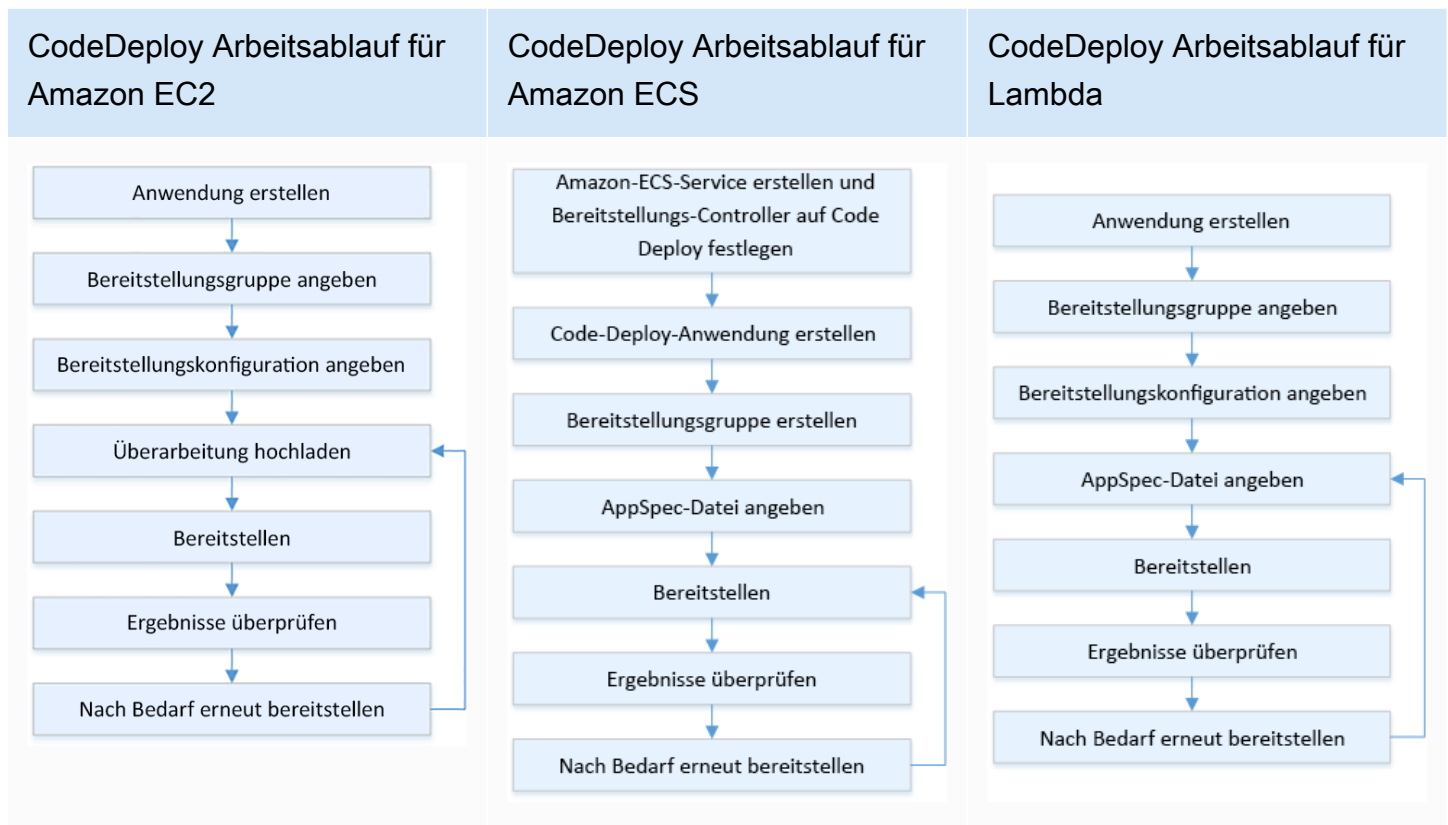
### Implementierungsleitfaden

Ausfälle bei der kontinuierlichen Bereitstellung können zu einer verringerten Serviceverfügbarkeit und schlechten Kundenerfahrungen führen. Um die Anzahl erfolgreicher Implementierungen zu maximieren, sollten Sie im end-to-end Release-Prozess Sicherheitskontrollen implementieren, um Bereitstellungsfehler zu minimieren, mit dem Ziel, Bereitstellungsfehler auf Null zu reduzieren.

### Kundenbeispiel

AnyCompany Der Einzelhandel hat es sich zur Aufgabe gemacht, Bereitstellungen mit minimalen bis gar keinen Ausfallzeiten zu erreichen, was bedeutet, dass während der Bereitstellung keine spürbaren Auswirkungen auf die Benutzer auftreten. Um dies zu erreichen, hat das Unternehmen Bereitstellungsmuster festgelegt, z. B. fortlaufende und Blau/Grün-Bereitstellungen (siehe nachfolgendes Workflow-Diagramm). Alle Teams übernehmen eines oder mehrere dieser Muster in ihre CI/CD-Pipeline.





## Implementierungsschritte

1. Verwenden Sie einen Genehmigungsworkflow, um die Reihenfolge der Produktionseinführungsschritte nach der Beförderung zur Produktion einzuleiten.
2. Verwenden Sie ein automatisiertes Bereitstellungssystem wie [AWS CodeDeploy](#). AWS CodeDeploy Zu den [Bereitlungsoptionen](#) gehören direkte Bereitstellungen für EC2 /On-Premises und Blue/Green-Bereitstellungen für EC2 /On-Premises AWS Lambda, und Amazon ECS (siehe vorheriges Workflow-Diagramm).
  - a. [Gegebenenfalls können Sie eine Integration AWS CodeDeploy mit anderen AWS Services oder mit Produkten und Services von Partnern durchführen. AWS CodeDeploy](#)
3. [Verwenden Sie blaue/grüne Bereitstellungen für Datenbanken wie Amazon Aurora und Amazon RDS](#)
4. [Überwachen Sie Bereitstellungen](#) mithilfe von Amazon CloudWatch AWS CloudTrail- und Amazon Simple Notification Service (AmazonSNS) -Ereignisbenachrichtigungen.
5. Führen Sie nach der Bereitstellung automatisierte Tests durch, einschließlich Funktions-, Sicherheits-, Regressions-, Integrations- und Auslastungstests.
6. Führen Sie die [Fehlersuche](#) bei Problemen mit der Bereitstellung aus.

## Aufwand für den Implementierungsplan: Mittel

### Ressourcen

#### Zugehörige bewährte Methoden:

- [OPS05-BP02 Änderungen testen und validieren](#)
- [OPS05-BP09 Nehmen Sie häufige, kleine, reversible Änderungen vor](#)
- [OPS05- BP1 0 Vollständig automatisierte Integration und Bereitstellung](#)

#### Zugehörige Dokumente:

- [AWS Builders Library | Automatisieren sicherer, automatisierter Bereitstellungen | Produktionsbereitstellungen](#)
- [AWS Builders Library | Meine CI/CD-Pipeline ist mein Release-Captain | Sichere, automatische Produktionsversionen](#)
- [AWS Whitepaper | Praktische Umsetzung von Continuous Integration und Continuous Delivery bei AWS | Bereitstellungsmethoden](#)
- [AWS CodeDeploy Benutzerhandbuch](#)
- [Arbeiten mit Bereitstellungsconfigurationen in AWS CodeDeploy](#)
- [Richten Sie eine API Gateway Canary Release-Bereitstellung ein](#)
- [ECSAmazon-Bereitlungstypen](#)
- [Vollständig verwaltete Blue/Green-Bereitstellungen in Amazon Aurora und Amazon RDS](#)
- [Blaue/grüne Bereitstellungen mit AWS Elastic Beanstalk](#)

#### Zugehörige Videos:

- [re:Invent 2020 | Vollständige Automatisierung: Automatisieren der Pipelines für kontinuierliche Bereitstellung bei Amazon](#)
- [re:Invent 2019 | Der Amazon-Ansatz für die Hochverfügbarkeitsbereitstellung](#)

#### Zugehörige Beispiele:

- [Testen Sie ein Beispiel für eine Blau/Grün-Bereitstellung in AWS CodeDeploy](#)
- [Workshop | Aufbau von CI/CD-Pipelines für Lambda-Canary-Implementierungen mit AWS CDK](#)

- [Workshop | Einsatz von Blue/Green und Canary für und EKS ECS](#)
- [Workshop | Erstellen einer kontenübergreifenden CI/CD-Pipeline](#)

## OPS06-BP04 Automatisieren Sie Tests und Rollback

Um die Geschwindigkeit, Zuverlässigkeit und Sicherheit Ihres Bereitstellungsprozesses zu erhöhen, sollten Sie eine Strategie für automatisierte Test- und Rollback-Funktionen in Vorproduktions- und Produktionsumgebungen entwickeln. Automatisieren Sie Tests bei der Bereitstellung in der Produktion, um Interaktionen zwischen Mensch und System zu simulieren und die bereitgestellten Änderungen zu überprüfen. Automatisieren Sie das Rollback, um schnell zu einem als funktionierend bekannten Zustand zurückkehren zu können. Das Rollback sollte unter vordefinierten Bedingungen automatisch eingeleitet werden, z. B. wenn das gewünschte Ergebnis einer Änderung nicht erreicht wird oder wenn der automatisierte Test fehlschlägt. Die Automatisierung dieser beiden Aktivitäten verbessert Ihre Erfolgsquote bei Bereitstellungen, minimiert die Wiederherstellungszeit und reduziert die potenziellen Auswirkungen auf das Unternehmen.

Gewünschtes Ergebnis: Ihre automatisierten Tests und Rollback-Strategien sind in Ihre CI/CD-Pipeline (Continuous Integration/Continuous Delivery, kontinuierliche Integration/kontinuierliche Bereitstellung) integriert. Ihre Überwachung kann Validierungen anhand Ihrer Erfolgskriterien ausführen und bei einem Fehler ein automatisches Rollback einleiten. Dadurch werden die Auswirkungen auf Endbenutzer und Kunden minimiert. Wenn beispielsweise alle Testergebnisse den Anforderungen entsprechen, übertragen Sie Ihren Code in die Produktionsumgebung, wo automatisierte Regressionstests unter Verwendung derselben Testfälle eingeleitet werden. Wenn die Ergebnisse der Regressionstests nicht den Erwartungen entsprechen, wird im Pipeline-Workflow ein automatisiertes Rollback eingeleitet.

### Typische Anti-Muster:

- Ihre Systeme sind nicht so konzipiert, dass sie mit kleineren Releases aktualisiert werden können. Daher haben Sie Schwierigkeiten, die Bulk-Änderungen während einer fehlgeschlagenen Bereitstellung rückgängig zu machen.
- Ihr Bereitstellungsprozess besteht aus einer Reihe manueller Schritte. Nachdem Sie Änderungen an Ihrer Workload bereitgestellt haben, beginnen Sie mit den Tests nach der Bereitstellung. Danach bemerken Sie, dass Ihre Workload nicht mehr funktioniert und die Verbindung der Kunden getrennt wird. Sie starten das Rollback zur vorherigen Version. All diese manuellen Schritte verzögern die allgemeine Systemwiederherstellung und wirken sich nachhaltig auf Ihre Kunden aus.

- Sie haben Zeit dafür aufgewendet, automatisierte Testfälle für Funktionen zu entwickeln, die in Ihrer Anwendung nicht häufig verwendet werden. Dadurch amortisiert sich die Investition in Ihre automatisierten Testfunktionen nur schlecht.
- Ihre Version besteht aus Anwendungs-, Infrastruktur-, Patch- und Konfigurations-Updates, die voneinander unabhängig sind. Sie haben jedoch nur eine CI/CD-Pipeline, die alle Änderungen gleichzeitig bereitstellt. Ein Fehler in einer Komponente zwingt Sie, alle Änderungen rückgängig zu machen, wodurch Ihr Rollback komplex und ineffizient wird.
- Ihr Team schließt die Programmierarbeiten im ersten Sprint ab und beginnt mit dem zweiten Sprint, aber Ihr Plan sieht Tests erst im dritten Sprint vor. Deshalb haben automatisierte Tests Fehler aus dem ersten Sprint aufgedeckt, die behoben werden müssen, bevor mit dem Testen der Ergebnisse von Sprint zwei begonnen werden kann. Der gesamte Release verzögert sich, wodurch der Wert Ihrer automatisierten Tests erheblich verringert wird.
- Ihre automatisierten Regressionstestfälle für die Produktionsversion sind abgeschlossen, aber Sie überwachen den Zustand der Workloads nicht. Da Sie nicht sehen können, ob der Dienst neu gestartet wurde oder nicht, sind Sie sich nicht sicher, ob ein Rollback erforderlich ist oder bereits stattgefunden hat.

Vorteile der Nutzung dieser bewährten Methode: Automatisierte Tests erhöhen die Transparenz Ihres Testprozesses und Ihre Fähigkeit, mehr Funktionen in kürzerer Zeit abzudecken. Durch das Testen und Validieren von Änderungen in der Produktionsphase können Sie Probleme sofort identifizieren. Die Verbesserung der Konsistenz mit automatisierten Testtools ermöglicht eine bessere Fehlererkennung. Durch das automatische Rollback zur vorherigen Version werden die Auswirkungen für Ihre Kunden minimiert. Ein automatisiertes Rollback sorgt letztendlich für mehr Vertrauen in Ihre Bereitstellungsfunktionen, da es die Auswirkungen auf Ihr Unternehmen verringert. Insgesamt verringern time-to-delivery sich diese Fähigkeiten bei gleichbleibender Qualität.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Mittel

### Implementierungsleitfaden

Automatisieren Sie die Tests von bereitgestellten Umgebungen, um schneller die gewünschten Ergebnisse zu erreichen. Automatisieren Sie den Rollback zu einem bekanntermaßen funktionierenden vorherigen Zustand, wenn die zuvor definierten Ergebnisse nicht erzielt werden. So können Sie die Wiederherstellungszeit minimieren und verringern Fehler, die durch manuelle Prozesse entstehen. Integrieren Sie Testtools in Ihren Pipeline-Workflow, um manuelle Eingaben konsistent zu testen und zu minimieren. Priorisieren Sie die Automatisierung von Testfällen, z. B. Tests, die die größten Risiken minimieren und die bei jeder Änderung häufig durchgeführt werden

müssen. Automatisieren Sie außerdem das Rollback auf Grundlage bestimmter Bedingungen, die in Ihrem Testplan vordefiniert sind.

## Implementierungsschritte

1. Richten Sie einen Testlebenszyklus für Ihren Entwicklungslebenszyklus ein, in dem jede Phase des Testprozesses definiert wird. Dies reicht von der Anforderungsplanung über die Testfallentwicklung, die Toolkonfiguration, das automatisierte Testen bis hin zum Abschluss des Testfalls.
  - a. Erstellen Sie anhand Ihrer gesamten Teststrategie einen Workload-spezifischen Testansatz.
  - b. Ziehen Sie eine Strategie für kontinuierliche Tests während des gesamten Entwicklungszyklus in Erwägung.
2. Wählen Sie in Abhängigkeit von Ihren Geschäftsanforderungen und Pipeline-Investitionen automatisierte Tools für Tests und Rollbacks aus.
3. Entscheiden Sie, welche Testfälle Sie automatisieren möchten und welche manuell durchgeführt werden sollen. Dies kann auf Grundlage des geschäftlichen Nutzens des getesteten Features definiert werden. Informieren Sie alle Teammitglieder über diesen Plan und legen Sie fest, wer für die Durchführung manueller Tests verantwortlich ist.
  - a. Wenden Sie automatisierte Testfunktionen auf bestimmte Testfälle an, die für die Automatisierung sinnvoll sind, z. B. wiederholbare oder häufig ausgeführte Fälle, Fälle, die sich wiederholende Aufgaben erfordern, oder solche, die für mehrere Konfigurationen erforderlich sind.
  - b. Definieren Sie Skripts für die Testautomatisierung sowie die Erfolgskriterien im Automatisierungstool, sodass eine kontinuierliche Workflow-Automatisierung initiiert werden kann, wenn bei bestimmten Fällen Fehler auftreten.
  - c. Definieren Sie spezifische Fehlerkriterien für das automatisierte Rollback.
4. Priorisieren Sie die Testautomatisierung, um konsistente Ergebnisse mit einer gründlichen Testfallentwicklung zu erzielen, bei der Komplexität und menschliche Interaktion ein höheres Ausfallrisiko darstellen.
5. Integrieren Sie Ihre automatisierten Test- und Rollback-Tools in Ihre CI/CD-Pipeline.
  - a. Entwickeln Sie klare Erfolgskriterien für Ihre Änderungen.
  - b. Überwachen und beobachten Sie Ihre Umgebung, um diese Kriterien zu erkennen und Änderungen automatisch rückgängig zu machen, wenn bestimmte Rollback-Kriterien erfüllt werden.
6. Führen Sie verschiedene Arten automatisierter Produktionstests durch, z. B.:

- a. A/B-Tests zur Anzeige von Ergebnissen im Vergleich zur aktuellen Version zwischen zwei Benutzertestgruppen.
  - b. Canary-Tests, mit denen Sie Ihre Änderung für eine Untergruppe von Benutzern bereitstellen können, bevor Sie sie für alle freigeben.
  - c. Testen mit Feature-Flags, wobei jeweils eine einzelne Funktion der neuen Version außerhalb der Anwendung ein- und ausgeschaltet werden kann, sodass alle neuen Funktionen einzeln validiert werden können.
  - d. Regressionstests zur Überprüfung neuer Funktionen mit bestehenden, miteinander verbundenen Komponenten.
7. Überwachen Sie die betrieblichen Aspekte der Anwendung, Transaktionen und Interaktionen mit anderen Anwendungen und Komponenten. Entwickeln Sie Berichte, um den Erfolg von Änderungen nach Workload aufzuzeigen, sodass Sie erkennen können, welche Teile der Automatisierung und des Workflows weiter optimiert werden können.
- a. Entwickeln Sie Testergebnisberichte, anhand derer Sie schnell entscheiden können, ob Rollback-Verfahren eingeleitet werden sollten oder nicht.
  - b. Implementieren Sie eine Strategie, die ein automatisiertes Rollback auf Grundlage vordefinierter Fehlerbedingungen ermöglicht, die sich aus einer oder mehreren Ihrer Testmethoden ergeben.
8. Entwickeln Sie Ihre automatisierten Testfälle so, dass sie bei zukünftigen wiederholbaren Änderungen wiederverwendet werden können.

Aufwand für den Implementierungsplan: Mittel

Ressourcen

Zugehörige bewährte Methoden:

- [OPS06-BP01 Plan für erfolglose Änderungen](#)
- [OPS06-BP02 Testbereitstellungen](#)

Zugehörige Dokumente:

- [AWS Builders Library | Gewährleistung der Rollback-Sicherheit bei Bereitstellungen](#)
- [Eine Bereitstellung erneut bereitstellen und rückgängig machen mit AWS CodeDeploy](#)
- [8 bewährte Methoden für die Automatisierung Ihrer Bereitstellungen mit AWS CloudFormation](#)

## Zugehörige Beispiele:

- [Testen von Benutzeroberflächen ohne Server mit Selenium, AWS Lambda, und Developer Tools AWS FargateAWS](#)

## Zugehörige Videos:

- [re:Invent 2020 | Vollständige Automatisierung: Automatisieren der Pipelines für kontinuierliche Bereitstellung bei Amazon](#)
- [re:Invent 2019 | Der Amazon-Ansatz für die Hochverfügbarkeitsbereitstellung](#)

OPS7. Wie bringen Sie in Erfahrung, ob Sie für die Unterstützung eines Workloads bereit sind?

Bewerten Sie die Betriebsbereitschaft Ihrer Workloads, von Prozessen und Verfahren sowie Ihrer Mitarbeiter, damit Sie die betrieblichen Risiken im Zusammenhang mit Ihrer Workload genau kennen.

## Bewährte Methoden

- [OPS07-BP01 Personalfähigkeit sicherstellen](#)
- [OPS07-BP02 Stellen Sie eine konsistente Überprüfung der Betriebsbereitschaft sicher](#)
- [OPS07-BP03 Verwenden Sie Runbooks, um Prozeduren durchzuführen](#)
- [OPS07-BP04 Verwenden Sie Playbooks, um Probleme zu untersuchen](#)
- [OPS07-BP05 Treffen Sie fundierte Entscheidungen zur Bereitstellung von Systemen und Änderungen](#)
- [OPS07-BP06 Supportpläne für Produktionsworkloads erstellen](#)

## OPS07-BP01 Personalfähigkeit sicherstellen

Stellen Sie einen Mechanismus bereit, mit dem Sie prüfen können, ob Sie über ausreichend trainierte Mitarbeiter zur Unterstützung der Workload verfügen. Sie müssen für die Plattform und die Services, die Ihre Workload ausmachen, trainiert sein. Stellen Sie ihnen die Informationen zur Verfügung, die sie zum Betrieb des Workloads benötigen. Sie müssen über genügend geschulte Mitarbeiter verfügen, um den normalen Betrieb der Workload zu unterstützen und auftretende Probleme zu beheben. Sorgen Sie für genügend Mitarbeiter, sodass Sie Bereitschaftsdienste und Urlaubsvertretungen abwechseln können, um Burnouts zu vermeiden.

## Gewünschtes Ergebnis:

- Es gibt genügend trainierte Mitarbeiter, um die Workload im Rahmen des Verfügbarkeitszeitraums zu unterstützen.
- Sie trainieren Ihre Mitarbeiter für die Software und Services, die Ihre Workload ausmachen.

## Typische Anti-Muster:

- Bereitstellen einer Workload ohne Teammitglieder, die für den Betrieb der Plattform und der genutzten Services trainiert sind.
- Sie haben nicht genug Mitarbeiter, um wechselnde Bereitschaftsdienste oder Urlaubszeiten abzudecken.

## Vorteile der Nutzung dieser bewährten Methode:

- Wenn Sie über qualifizierte Teammitglieder verfügen, können diese Ihre Workload effektiv unterstützen.
- Mit einer ausreichenden Anzahl von Teammitgliedern können Sie den Workload und die Rotation der Bereitschaftsdienste unterstützen und gleichzeitig das Risiko eines Burnouts verringern.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Hoch

## Implementierungsleitfaden

Validieren Sie, ob ausreichend trainierte Mitarbeiter für den Support des Workloads vorhanden sind. Vergewissern Sie sich, dass Sie über genügend Teammitglieder verfügen, um die normalen operativen Aktivitäten, einschließlich Einsatzbereitschaftsdienste, abzudecken.

## Kundenbeispiel

AnyCompany Der Einzelhandel stellt sicher, dass die Teams, die die Arbeitslast bewältigen, angemessen besetzt und geschult sind. Es gibt genügend Ingenieure, um wechselnde Bereitschaftsdienste zu unterstützen. Die Mitarbeiter erhalten Training, um die Software und die Workload-Plattform zu nutzen. Sie werden außerdem ermutigt, Zertifizierungen zu erwerben. Es gibt so viele Mitarbeiter, dass Urlaub möglich ist, ohne dass die Abdeckung der Workload und der rotierenden Bereitschaftsdienste unterbrochen werden muss.

## Implementierungsschritte



1. Weisen Sie eine ausreichende Anzahl von Mitarbeitern für den Betrieb und den Support Ihres Workloads zu – einschließlich der Bereitschaftsdienste.
2. Trainieren Sie die Mitarbeiter im Umgang mit der Software und den Plattformen, die Ihre Workload ausmachen.
  - a. [AWS Training and Certification](#) bietet eine Bibliothek mit Kursen zu AWS den Themen. Es gibt kostenlose und kostenpflichtige Kurse – online und vor Ort.
  - b. [AWS veranstaltet Veranstaltungen und Webinare](#), bei denen Sie von AWS Experten lernen.
3. Bewerten Sie regelmäßig die Größe und die Fähigkeiten des Teams, wenn sich die operativen Bedingungen und die Workload verändern. Passen Sie die Größe und Fähigkeiten des Teams an die operativen Anforderungen an.

Aufwand für den Implementierungsplan: Hoch. Das Einstellen und Trainieren eines Teams zur Unterstützung einer Workload kann einen erheblichen Aufwand darstellen, bietet aber langfristig einen bedeutenden Nutzen.

#### Ressourcen

Zugehörige bewährte Methoden:

- [OPS11-BP04 Wissensmanagement durchführen](#) – Die Teammitglieder müssen über die notwendigen Informationen verfügen, um die Workload zu betreiben und zu unterstützen. Der Schlüssel dazu ist das Wissensmanagement.

Zugehörige Dokumente:

- [AWS Veranstaltungen und Webinare](#)
- [AWS Schulung und Zertifizierung](#)

OPS07-BP02 Stellen Sie eine konsistente Überprüfung der Betriebsbereitschaft sicher

Überprüfen Sie anhand von Operational Readiness Readiness Readiness Reviews (ORRs), ob Sie Ihre Workloads bewältigen können. ORR ist ein Mechanismus, der bei Amazon entwickelt wurde, um zu überprüfen, ob Teams ihre Workloads sicher handhaben können. An ORR ist ein Überprüfungs- und Inspektionsprozess, bei dem eine Checkliste mit Anforderungen verwendet wird. An ORR ist ein Self-Service-Erlebnis, das Teams nutzen, um ihre Workloads zu zertifizieren. ORR beinhaltet bewährte Methoden, die wir aus unserer jahrelangen Erfahrung in der Softwareentwicklung gewonnen haben.

Eine ORR Checkliste besteht aus architektonischen Empfehlungen, betrieblichen Abläufen, Eventmanagement und der Qualität der Veröffentlichung. Unser Correction of Error (CoE)-Prozess ist dafür eine sehr wichtige Grundlage. Ihre eigene Analyse nach dem Vorfall sollte Ihre eigene Entwicklung vorantreiben. ORR Bei An ORR geht es nicht nur darum, bewährte Methoden zu befolgen, sondern auch zu verhindern, dass sich Ereignisse wiederholen, die Sie schon einmal erlebt haben. Schließlich können auch Sicherheits-, Governance- und Compliance-Anforderungen in eine ORR aufgenommen werden.

Wird ausgeführt, ORRs bevor ein Workload allgemein verfügbar ist, und dann während des gesamten Softwareentwicklungszyklus. Wenn Sie den ORR Befehl vor dem Start ausführen, können Sie den Workload sicherer ausführen. Führen Sie Ihren ORR Workload regelmäßig erneut aus, um catch von den bewährten Methoden zu erkennen. Sie können ORR Checklisten für die Einführung neuer Dienste und ORRs für regelmäßige Überprüfungen haben. So bleiben Sie hinsichtlich der neuen bewährten Methoden auf dem Laufenden und können Erfahrungen aus Analysen nach Vorfällen einarbeiten. Mit zunehmender Nutzung der Cloud können Sie ORR Anforderungen als Standardwerte in Ihre Architektur integrieren.

Gewünschtes Ergebnis: Sie haben eine ORR Checkliste mit bewährten Verfahren für Ihr Unternehmen. ORRs werden vor dem Start der Workloads durchgeführt. ORRs werden im Laufe des Workload-Lebenszyklus regelmäßig ausgeführt.

Typische Anti-Muster:

- Sie starten eine Workload, ohne zu wissen, ob Sie diese betreiben können.
- Governance- und Sicherheitsanforderungen gehören nicht zur Zertifizierung einer Workload für den Start.
- Workloads werden nicht regelmäßig erneut bewertet.
- Workloads werden gestartet, ohne dass erforderliche Verfahren eingerichtet sind.
- Sie erleben die Wiederholung von Ausfällen mit der gleichen Ursache bei mehreren Workloads.

Vorteile der Nutzung dieser bewährten Methode:

- Ihre Workloads beinhalten bewährte Methoden für Architektur, Prozess und Management.
- Die gewonnenen Erkenntnisse fließen in Ihren ORR Prozess ein.
- Workloads werden gestartet, wenn erforderliche Verfahren eingerichtet sind.
- ORRs werden während des gesamten Softwarelebenszyklus Ihrer Workloads ausgeführt.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Hoch

## Implementierungsleitfaden

An ORR besteht aus zwei Dingen: einem Prozess und einer Checkliste. Ihr ORR Prozess sollte von Ihrer Organisation übernommen und von einem leitenden Sponsor unterstützt werden. ORRs müssen mindestens durchgeführt werden, bevor ein Workload allgemein verfügbar ist. Führen Sie die Software ORR während des gesamten Lebenszyklus der Softwareentwicklung durch, um sie über bewährte Verfahren oder neue Anforderungen auf dem Laufenden zu halten. Die ORR Checkliste sollte Konfigurationselemente, Sicherheits- und Governance-Anforderungen sowie bewährte Verfahren aus Ihrem Unternehmen enthalten. Im Laufe der Zeit können Sie Dienste wie, und [AWS Control Tower Guardrails](#) verwenden [AWS Config](#) [AWS Security Hub](#), um bewährte Verfahren aus den Leitplanken zu entwickeln, ORR sodass bewährte Verfahren automatisch erkannt werden.

## Kundenbeispiel

Nach mehreren Produktionsvorfällen entschied sich AnyCompany Retail für die Implementierung eines Prozesses. ORR Das Unternehmen erstellte eine Checkliste mit bewährten Methoden sowie Governance- und Complianceanforderungen und Erfahrungen aus früheren Ausfällen. Neue Workloads werden ausgeführt, ORRs bevor sie auf den Markt kommen. Jeder Workload wird jährlich ORR mit einer Untergruppe von Best Practices durchgeführt, um neue bewährte Verfahren und Anforderungen zu berücksichtigen, die der Checkliste hinzugefügt werden. ORR Im Laufe der Zeit entdeckte der AnyCompany Einzelhandel einige bewährte Verfahren, wodurch der Prozess beschleunigt wurde. [AWS Config](#) ORR

## Implementierungsschritte

Weitere Informationen ORRs finden Sie im [Whitepaper Operational Readiness Reviews \(ORR\)](#). Es enthält ausführliche Informationen zur Geschichte des ORR Prozesses, dazu, wie Sie Ihre eigene ORR Praxis aufbauen und wie Sie Ihre ORR Checkliste erstellen können. Die folgenden Schritte sind eine verkürzte Version dieses Dokuments. Für ein tieferes Verständnis dessen, was das ORRs sind und wie Sie Ihre eigenen entwickeln können, empfehlen wir Ihnen, dieses Whitepaper zu lesen.

1. Bringen Sie die wichtigsten Stakeholder zusammen, darunter auch Vertreter aus den Bereichen Sicherheit, Operations und Entwicklung.
2. Lassen Sie alle Stakeholder mindestens eine Anforderung beisteuern. Versuchen Sie für den ersten Durchgang die Anzahl der Elemente auf höchstens dreißig zu beschränken.
  - [Anhang B: ORR Beispielfragen](#) aus dem Whitepaper Operational Readiness Reviews (ORR) enthält Beispielfragen, die Sie für den Einstieg verwenden können.

3. Fassen Sie Ihre Anforderungen in einer Tabelle zusammen.
  - Sie können [benutzerdefinierte Objekte](#) verwenden, um Ihre [AWS Well-Architected Tool](#) zu entwickeln ORR und sie in Ihren Konten und Ihrem AWS Unternehmen gemeinsam zu nutzen.
4. Identifizieren Sie einen Workload, der ORR ausgeführt werden soll. Ideal ist dafür eine Pre-Launch-Workload oder eine interne Workload.
5. Gehen Sie die ORR Checkliste durch und notieren Sie sich alle gemachten Entdeckungen. Diese sind möglicherweise nicht OK, wenn eine Behebung stattfindet. Fügen Sie alle Erkenntnisse ohne Behebung Ihrer Liste hinzu und implementieren Sie die Behebungen vor dem Start.
6. Fügen Sie Ihrer ORR Checkliste im Laufe der Zeit weiterhin bewährte Verfahren und Anforderungen hinzu.

AWS Support Kunden mit Enterprise Support können den [Operational Readiness Review Workshop](#) bei ihrem Technical Account Manager anfordern. Bei dem Workshop handelt es sich um eine interaktive Sitzung, in der Sie rückwärts arbeiten können, um Ihre eigene ORR Checkliste zu entwickeln.

Aufwand für den Implementierungsplan: Hoch. Die Einführung einer ORR Praxis in Ihrer Organisation erfordert die Unterstützung der Geschäftsleitung und die Zustimmung der Interessengruppen. Erstellen und aktualisieren Sie die Checkliste mit Beiträgen aus der gesamten Organisation.

## Ressourcen

Zugehörige bewährte Methoden:

- [OPS01-BP03 Bewertung der Governance-Anforderungen](#)— Anforderungen an die Unternehmensführung eignen sich hervorragend für eine Checkliste. ORR
- [OPS01-BP04 Evaluieren Sie die Compliance-Anforderungen](#)— Compliance-Anforderungen sind manchmal in einer ORR Checkliste enthalten. Ansonsten sind sie ein separater Prozess.
- [OPS03-BP07 Ressourcenteams angemessen](#)— Teamfähigkeit ist ein guter Kandidat für eine ORR Anforderung.
- [OPS06-BP01 Plan für erfolglose Änderungen](#) – Vor dem Start Ihrer Workload muss ein Rollback- oder Rollforward-Plan eingerichtet werden.
- [OPS07-BP01 Personalfähigkeit sicherstellen](#) – Zur Unterstützung einer Workload benötigen Sie das erforderliche Personal.
- [SEC01-BP03 Identifizieren und validieren Sie Kontrollziele — Ziele](#) der Sicherheitskontrolle stellen hervorragende ORR Anforderungen.

- [REL13-BP01 Definieren Sie Wiederherstellungsziele für Ausfallzeiten und Datenverlust](#) — Notfallwiederherstellungspläne sind eine gute Voraussetzung. ORR
- [COST02-BP01 Entwickeln Sie Richtlinien auf der Grundlage der Anforderungen Ihres Unternehmens](#) — Kostenmanagement-Richtlinien sollten in Ihre Checkliste aufgenommen werden. ORR

#### Zugehörige Dokumente:

- [AWS Control Tower - Leitplanken in AWS Control Tower](#)
- [AWS Well-Architected Tool - Kundenspezifische Objekte](#)
- [Operational Readiness Review Template von Adrian Hornsby](#)
- [Bewertungen der Betriebsbereitschaft \(ORR\) — Whitepaper](#)

#### Zugehörige Videos:

- [AWS Support Wie Sie | Aufbau einer effektiven Überprüfung der Betriebsbereitschaft \(\) ORR](#)

#### Zugehörige Beispiele:

- [Beispiel für eine Überprüfung der Betriebsbereitschaft \(ORR\)](#)

#### Zugehörige Services:

- [AWS Config](#)
- [AWS Control Tower](#)
- [AWS Security Hub](#)
- [AWS Well-Architected Tool](#)

#### OPS07-BP03 Verwenden Sie Runbooks, um Prozeduren durchzuführen

Ein Runbook ist ein dokumentierter Prozess für das Erreichen eines bestimmten Ergebnisses. Runbooks bestehen aus einer Reihe von Schritten, die befolgt werden sollen, um ein Ergebnis zu erzielen. Runbooks werden schon seit den frühen Tagen der Luftfahrt verwendet. Im Cloud-Bereich werden Runbooks verwendet, um die Risiken zu reduzieren und die gewünschten Ergebnisse zu erzielen. In der einfachsten Form ist ein Runbook eine Checkliste für die Durchführung einer Aufgabe.

Runbooks stellen einen kritischen Teil der Ausführung Ihrer Workload dar. Vom Onboarding eines neuen Teammitglieds bis zur Bereitstellung einer Hauptversion – Runbooks stellen kodifizierte Prozesse dar, mit denen unabhängig von der ausführenden Person konsistente Ergebnisse erzielt werden können. Runbooks sollten an einer zentralen Stelle veröffentlicht werden. Wenn sich der Prozess verändert, sollten sie aktualisiert werden; dies stellt eine zentrale Komponente des Änderungsmanagements dar. Sie sollten auch Anleitungen für Fehlerbehandlung, Tools, Berechtigungen, Ausnahmen und Eskalationen enthalten, falls ein Problem auftritt.

Wenn sich Ihre Organisation entwickelt, sollten Sie mit der Automatisierung von Runbooks beginnen. Sie sollten zunächst Runbooks automatisieren, die kurz sind und häufig verwendet werden. Verwenden Sie Skriptsprachen, um Schritte zu automatisieren oder ihre Ausführung zu vereinfachen. Nach der Automatisierung der ersten Runbooks können Sie komplexere Runbooks automatisieren. Mit der Zeit sollten die meisten Ihrer Runbooks auf die eine oder andere Art automatisiert werden.

Gewünschtes Ergebnis: Ihr Team verfügt über eine Sammlung von step-by-step Leitfäden für die Ausführung von Workload-Aufgaben. Die Runbooks enthalten Angaben zum gewünschten Ergebnis sowie zu notwendigen Tools und Berechtigungen. Darüber hinaus stellen sie Anleitungen für die Fehlerbehandlung bereit. Sie werden an einem zentralen Ort (Versionskontrollsystem) gespeichert und regelmäßig aktualisiert. Ihre Runbooks bieten Ihren Teams beispielsweise Funktionen zur Überwachung, Kommunikation und Reaktion auf AWS Health Ereignisse für kritische Accounts bei Anwendungsalarman, Betriebsproblemen und geplanten Lebenszyklusereignissen.

Typische Anti-Muster:

- Verlassen auf das Gedächtnis, um die einzelnen Schritte in einem Prozess durchzuführen.
- Manuelle Bereitstellung von Änderungen ohne Checkliste.
- Verschiedene Teammitglieder führen den gleichen Prozess aus, aber mit unterschiedlichen Schritten oder Ergebnissen.
- Runbooks sind nicht mehr mit Systemänderungen und Automatisierungen synchronisiert.

Vorteile der Nutzung dieser bewährten Methode:

- Reduzierung der Fehlerquoten für manuelle Aufgaben.
- Prozesse werden konsistent ausgeführt.
- Neue Teammitglieder können schneller mit der Ausführung von Aufgaben beginnen.
- Runbooks können automatisiert werden, um den Aufwand zu reduzieren.

## Risikostufe bei fehlender Befolgung dieser bewährten Methode: Mittel

### Implementierungsleitfaden

Runbooks können verschiedene Formen annehmen, abhängig vom Entwicklungsstand Ihrer Organisation. Sie sollten mindestens aus einem step-by-step Textdokument bestehen. Das gewünschte Ergebnis sollte klar angegeben werden. Dokumentieren Sie klar die notwendigen Berechtigungen oder Tools. Stellen Sie für den Fall, dass etwas nicht funktioniert, detaillierte Anleitungen für Fehlerbehandlung und Eskalation bereit. Nennen Sie die Person, die für das Runbook verantwortlich ist, und veröffentlichen Sie es an einer zentralen Stelle. Validieren Sie das Runbook, nachdem Sie es dokumentiert haben, indem Sie es von einem Teammitglied ausführen lassen. Mit der weiteren Entwicklung der Verfahren sollten Sie Ihre Runbooks entsprechend Ihrem Prozess für das Änderungsmanagement aktualisieren.

Ihre textbasierten Runbooks sollten mit zunehmender Entwicklung Ihrer Organisation automatisiert werden. Mit Services wie [AWS -Systems-Manager-Automatisierungen](#) können Sie Textdateien zu Automatisierungen transformieren, die Sie für Ihre Workload ausführen können. Diese Automatisierungen können als Reaktion auf Ereignisse ausgeführt werden, wodurch der Betriebsaufwand zur Aufrechterhaltung Ihrer Arbeitslast reduziert wird. AWS Systems Manager Automation bietet außerdem ein [visuelles Designerlebnis](#) mit geringem Code-Aufwand, sodass Automatisierungs-Runbooks einfacher erstellt werden können.

### Kundenbeispiel

AnyCompany Der Einzelhandel muss während der Softwarebereitstellung Datenbankschemaaktualisierungen durchführen. Das Cloud Operations-Team entwickelt gemeinsam mit dem Datenbankverwaltungsteam ein Runbook für die manuelle Bereitstellung dieser Änderungen. In diesem Runbook werden die einzelnen Prozessschritte in Form einer Checkliste aufgelistet. Es enthält für den Fall, dass es ein Problem gibt, auch einen Abschnitt zur Fehlerbehandlung. Das Runbook wird wie die übrigen Runbooks im internen Wiki veröffentlicht. Das Cloud Operations-Team plant, das Runbook in der Zukunft zu automatisieren.

### Implementierungsschritte

Wenn Sie noch kein Dokumenten-Repository besitzen, dann ist ein Repository für die Versionskontrolle hervorragend als Grundlage für Ihre Runbook-Bibliothek geeignet. Sie können Ihre Runbooks mithilfe von Markdown erstellen. Wir haben eine Runbook-Beispielvorlage bereitgestellt, die Sie für die Erstellung von Runbooks verwenden können.

```
# Runbook Title
```

```
## Runbook Info
| Runbook ID | Description | Tools Used | Special Permissions | Runbook Author | Last
Updated | Escalation POC |
|-----|-----|-----|-----|-----|-----|-----|
| RUN001 | What is this runbook for? What is the desired outcome? | Tools | Permissions
| Your Name | 2022-09-21 | Escalation Name |
## Steps
1. Step one
2. Step two
```

1. Wenn Sie noch kein Dokumentations-Repository oder -Wiki besitzen, sollten Sie in Ihrem Versionskontrollsystem ein neues Versionskontroll-Repository erstellen.
2. Identifizieren Sie einen Prozess, für den es kein Runbook gibt. Ein idealer Prozess hierfür ist ein Prozess, der halbregelmäßig ausgeführt wird, nur wenige Schritte enthält und bei Fehlern nur geringe Auswirkungen hat.
3. Erstellen Sie in Ihrem Dokument-Repository ein neues Markdown-Entwurfsdokument auf der Basis der Vorlage. Füllen Sie den Runbook-Titel und die Pflichtfelder unter Runbook-Informationen aus.
4. Füllen Sie ab dem ersten Schritt den Abschnitt Schritte im Runbook aus.
5. Geben Sie das Runbook einem Teammitglied. Lassen Sie das Teammitglied das Runbook ausführen, um die Schritte zu validieren. Aktualisieren Sie das Runbook, wenn etwas fehlt oder unklar ist.
6. Veröffentlichen Sie das Runbook in Ihrem internen Dokumentationsspeicher. Informieren Sie Ihr Team und die übrigen Stakeholder über das Runbook, nachdem es veröffentlicht wurde.
7. Mit der Zeit entsteht dadurch eine Bibliothek von Runbooks. Beginnen Sie mit der Automatisierung von Runbooks, wenn diese Bibliothek wächst.

Aufwand für den Implementierungsplan: Niedrig. Der Mindeststandard für ein Runbook ist ein step-by-step Texthandbuch. Die Automatisierung von Runbooks kann den Implementierungsaufwand erhöhen.

## Ressourcen

Zugehörige bewährte Methoden:

- [OPS02-BP02 Für Prozesse und Verfahren gibt es identifizierte Verantwortliche](#)
- [OPS07-BP04 Verwenden Sie Playbooks, um Probleme zu untersuchen](#)
- [OPS10-BP01 Verwenden Sie einen Prozess für das Ereignis-, Vorfall- und Problemmanagement](#)



- [OPS10-BP02 Führen Sie einen Prozess pro Warnung durch](#)
- [OPS11-BP04 Führen Sie Wissensmanagement durch](#)

#### Zugehörige Dokumente:

- [AWS Well-Architected Framework: Concepts: Runbook development](#)
- [Operative Kompetenz durch automatisierte Playbooks und Runbooks](#)
- [AWS Systems Manager: Arbeiten mit Runbooks](#)
- [Migrationsplan für AWS umfangreiche Migrationen — Aufgabe 4: Verbesserung Ihrer Migrations-Runbooks](#)
- [Use AWS Systems Manager Automation runbooks to resolve operational tasks](#)

#### Zugehörige Videos:

- [AWS re:Invent 2019: DIY Leitfaden für Runbooks, Incident-Reports und Incident-Response](#)
- [So automatisieren Sie den IT-Betrieb auf AWS | Amazon Web Services](#)
- [Integrieren Sie Skripte in AWS Systems Manager](#)

#### Zugehörige Beispiele:

- [Well-Architected Labs: Automatisieren von Vorgängen mit Playbooks und Runbooks](#)
- [AWS Blogbeitrag: Aufbau einer Cloud-Automatisierungspraxis für betriebliche Exzellenz: Best Practices von AWS Managed Services](#)
- [AWS Systems Manager: Komplettlösungen zur Automatisierung](#)
- [AWS Systems Manager: Stellen Sie ein Root-Volume aus dem neuesten Snapshot-Runbook wieder her](#)
- [Erstellen eines AWS Incident-Response-Runbooks mithilfe von Jupyter-Notebooks und Lake CloudTrail](#)
- [Gitlab – Runbooks](#)
- [Rubix – eine Python-Bibliothek für die Erstellung von Runbooks in Jupyter Notebooks](#)
- [Verwenden von Document Builder zum Erstellen eines benutzerdefinierten Runbooks](#)

#### Zugehörige Services:

- [AWS Systems Manager Automatisierung](#)

## OPS07-BP04 Verwenden Sie Playbooks, um Probleme zu untersuchen

Playbooks sind step-by-step Anleitungen zur Untersuchung eines Vorfalls. Wenn Vorfälle auftreten, werden Playbooks verwendet, um sie zu untersuchen, die Auswirkungen abzuschätzen und Ursachen zu identifizieren. Playbooks werden für verschiedene Szenarien eingesetzt, von fehlgeschlagenen Bereitstellungen bis hin zu Sicherheitsvorfällen. In vielen Fällen identifizieren Playbooks Ursachen, die dann mithilfe eines Runbooks beseitigt werden. Playbooks sind eine sehr wichtige Komponente der Vorfalldreaktionspläne Ihrer Organisation.

Ein gutes Playbook weist einige zentrale Merkmale auf. Es leitet den Benutzer Schritt für Schritt durch den Erkennungsprozess. Welche Schritte sollten befolgt werden, um einen Vorfall zu diagnostizieren? Legen Sie im Playbook klar fest, ob bestimmte Tools oder erhöhte Berechtigungen benötigt werden. Ein wichtiger Teil ist ein Kommunikationsplan, um alle Stakeholder über den Status der Untersuchung zu informieren. Für den Fall, dass die eigentliche Ursache des Vorfalls nicht identifiziert werden kann, sollte das Playbook einen Eskalationsplan enthalten. Wenn die Ursache identifiziert wurde, sollte das Playbook auf ein Runbook verweisen, das beschreibt, wie die Ursache zu beheben ist. Playbooks sollten zentral gespeichert und regelmäßig gepflegt werden. Wenn Playbooks für bestimmte Warnungsmeldungen verwendet werden, sollte Ihr Team in den Warnungsmeldungen auf das Playbook verwiesen werden.

Im Zuge der Weiterentwicklung Ihrer Organisation sollten Sie Ihre Playbooks automatisieren. Beginnen Sie mit Playbooks für Vorfälle mit geringem Risikograd. Automatisieren Sie die Erkennungsschritte mit Skripts. Stellen Sie sicher, dass Sie über begleitende Runbooks für die Behebung typischer Ursachen verfügen.

Gewünschtes Ergebnis: Ihre Organisation verfügt über Playbooks für typische Vorfälle. Die Playbooks werden an einem zentralen Ort gespeichert und sind für Ihre Teammitglieder verfügbar. Playbooks werden häufig aktualisiert. Für alle bekannten Ursachen werden begleitende Runbooks erstellt.

### Typische Anti-Muster:

- Es gibt kein Standardverfahren für die Untersuchung von Vorfällen.
- Teammitglieder verlassen sich auf ihr Gedächtnis oder allgemein vorhandenes Wissen, um eine fehlgeschlagene Bereitstellung zu beheben.
- Neue Teammitglieder lernen die Untersuchung von Problemen durch Ausprobieren.

- Es werden keine bewährten Methoden für die Untersuchung von Problemen zwischen Teams ausgetauscht.

Vorteile der Nutzung dieser bewährten Methode:

- Playbooks verbessern Ihre Fähigkeit zum Umgang mit Vorfällen.
- Verschiedene Teammitglieder können dasselbe Playbook verwenden, um Ursachen in konsistenter Weise zu ermitteln.
- Für bekannte Ursachen können Runbooks entwickelt werden, um die Wiederherstellungszeit zu verkürzen.
- Mit Playbooks können Teammitglieder schneller Beiträge leisten.
- Mit wiederholbaren Playbooks können Teams ihre Prozesse skalieren.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Mittel

### Implementierungsleitfaden

Wie Sie Ihre Playbooks aufbauen und verwenden, hängt vom Reifegrad Ihrer Organisation ab. Wenn Sie noch neu in der Cloud sind, erstellen Sie Playbooks in Textform in einem zentralen Dokumenten-Repository. Wenn sich Ihre Organisation weiterentwickelt, können Playbooks mit Skriptsprachen wie Python teilweise automatisiert werden. Diese Skripts können zur Beschleunigung der Untersuchung in einem Jupyter Notebook ausgeführt werden. Fortgeschrittene Organisationen haben vollständig automatisierte Playbooks für häufig auftretende Probleme, die dann mit Runbooks automatisch behoben werden.

Beginnen Sie die Arbeit an Ihren Playbooks mit der Auflistung typischer Vorfälle bei Ihren Workloads. Wählen Sie Playbooks zunächst für Vorfälle mit geringem Risiko, bei denen die Ursache eingegrenzt werden kann. Wenn Sie über Playbooks für einfachere Szenarien verfügen, gehen Sie zu Szenarien mit höheren Risiken oder zu Szenarien über, bei denen die Ursache nicht vollständig klar ist.

Ihre textbasierten Playbooks sollten mit zunehmender Entwicklung Ihrer Organisation automatisiert werden. Mit Services wie [AWS -Systems-Manager-Automatisierungen](#) können Textdateien in Automatisierungen transformiert werden. Diese Automatisierungen können dann für Ihre Workload ausgeführt werden, um die Untersuchungen zu beschleunigen. Sie können in Reaktion auf Ereignisse aktiviert werden, wodurch sich der durchschnittliche Zeitaufwand für die Untersuchung und Behebung von Vorfällen reduziert.

Kunden können [AWS Systems Manager Incident Manager](#) zur Reaktion auf Vorfälle verwenden. Dieser Service bietet eine einzige Oberfläche für die Untersuchung von Vorfällen, die Information der Stakeholder über Untersuchung und Abhilfemaßnahmen und die Zusammenarbeit während des gesamten Vorgangs. Es verwendet AWS Systems Manager Automations, um die Erkennung und Wiederherstellung zu beschleunigen.

## Kundenbeispiel

Ein Produktionsvorfall hatte Auswirkungen auf den Einzelhandel. AnyCompany Der zuständige Techniker untersuchte das Problem mithilfe eines Playbooks. Im Zuge der einzelnen Schritte wurden die Stakeholder, die im Playbook festgelegt waren, auf dem Laufenden gehalten. Der Techniker ermittelte einen Race-Zustand in einem Backend-Service als Ursache für den Vorfall. Mithilfe eines Runbooks hat der Techniker den Service neu gestartet und Retail wieder online gestellt. AnyCompany

## Implementierungsschritte

Wenn Sie noch kein Dokumenten-Repository besitzen, dann sollten Sie ein Versionskontroll-Repository für Ihre Playbook-Bibliothek erstellen. Sie können Ihre Playbooks mit Markdown erstellen, das mit den meisten Playbook-Automatisierungssystemen kompatibel ist. Wenn Sie neu beginnen, verwenden Sie die folgende Beispielvorgabe für ein Playbook.

```
# Playbook Title
## Playbook Info
| Playbook ID | Description | Tools Used | Special Permissions | Playbook Author | Last Updated | Escalation POC | Stakeholders | Communication Plan |
|-----|-----|-----|-----|-----|-----|-----|-----|-----|
| RUN001 | What is this playbook for? What incident is it used for? | Tools | Permissions | Your Name | 2022-09-21 | Escalation Name | Stakeholder Name | How will updates be communicated during the investigation? |
## Steps
1. Step one
2. Step two
```

1. Wenn Sie noch kein Dokumenten-Repository oder -Wiki besitzen, sollten Sie in Ihrem Versionskontrollsystem ein neues Versionskontroll-Repository für Ihre Playbooks erstellen.
2. Identifizieren Sie ein typisches Problem, das eine Untersuchung erfordert. Dies sollte ein Szenario sein, bei dem die Ursache auf wenige Probleme eingegrenzt werden kann und das Risiko insgesamt niedrig ist.

3. Füllen Sie mithilfe der Markdown-Vorlage den Abschnitt Playbook-Name und die Felder unter Playbook-Informationen aus.
4. Geben Sie die Schritte zur Fehlerbehebung ein. Benennen Sie die zu treffenden Maßnahmen bzw. die zu untersuchenden Bereiche so klar wie möglich.
5. Geben Sie das Playbook einem Teammitglied zur Prüfung. Wenn darin etwas fehlt oder nicht klar ist, aktualisieren Sie das Playbook.
6. Veröffentlichen Sie Ihr Playbook in Ihrem Dokumenten-Repository und informieren Sie Ihr Team und alle Stakeholder darüber.
7. Diese Playbook-Bibliothek wächst mit der Zeit an. Sobald Sie mehrere Playbooks haben, beginnen Sie, sie mithilfe von Tools wie AWS Systems Manager Automations zu automatisieren, um Automatisierung und Playbooks synchron zu halten.

Aufwand für den Implementierungsplan: Niedrig. Ihre Playbooks sollten an einem zentralen Ort gespeicherte Textdokumente sein. Ausgereifere Organisationen gehen zu automatisierten Playbooks über.

#### Ressourcen

#### Zugehörige bewährte Methoden:

- [OPS02-BP02 Für Prozesse und Verfahren wurden die Verantwortlichen identifiziert](#)
- [OPS07-BP03 Verwenden Sie Runbooks, um Verfahren durchzuführen](#)
- [OPS10-BP01 Verwenden Sie einen Prozess für das Ereignis-, Vorfall- und Problemmanagement](#)
- [OPS10-BP02 Führen Sie einen Prozess pro Warnung durch](#)
- [OPS11-BP04 Führen Sie Wissensmanagement durch](#)

#### Zugehörige Dokumente:

- [AWS Well-Architected Framework: Concepts: Playbook development](#)
- [Operative Kompetenz durch automatisierte Playbooks und Runbooks](#)
- [AWS Systems Manager: Arbeiten mit Runbooks](#)
- [Use AWS Systems Manager Automation runbooks to resolve operational tasks](#)

#### Zugehörige Videos:

- [AWS re:Invent 2019: DIY Leitfaden für Runbooks, Incident-Reports und Incident-Response \(-R1\) SEC318](#)
- [AWS Systems Manager Incident Manager — AWS Virtuelle Workshops](#)
- [Integrieren Sie Skripts in AWS Systems Manager](#)

Zugehörige Beispiele:

- [AWS Customer Playbook Framework](#)
- [AWS Systems Manager: Komplettlösungen zur Automatisierung](#)
- [Erstellung eines Runbooks zur Reaktion auf AWS Vorfälle mithilfe von Jupyter-Notebooks und Lake CloudTrail](#)
- [Rubix – Eine Python-Bibliothek für die Erstellung von Runbooks in Jupyter Notebooks](#)
- [Verwenden von Document Builder zum Erstellen eines benutzerdefinierten Runbooks](#)
- [Well-Architected Labs: Automatisieren von Vorgängen mit Playbooks und Runbooks](#)
- [Well-Architected Labs: Playbook für Vorfallreaktion mit Jupyter](#)

Zugehörige Services:

- [AWS Systems Manager Automatisierung](#)
- [AWS Systems Manager Incident Manager](#)

OPS07-BP05 Treffen Sie fundierte Entscheidungen zur Bereitstellung von Systemen und Änderungen

Sorgen Sie dafür, dass Prozesse für erfolgreiche und nicht erfolgreiche Änderungen an Ihrer Workload vorhanden sind. Eine Pre-mortem-Übung ist eine Übung, bei der ein Team einen Fehler simuliert, um Strategien zur Behebung zu entwickeln. Nutzen Sie diese „Pre-mortems“, um Fehlern vorzubeugen und legen Sie, wo erforderlich, entsprechende Abläufe fest. Bewerten Sie den Nutzen und die Risiken der Bereitstellung von Änderungen an Ihrer Workload. Überprüfen Sie, ob alle Änderungen mit der Governance übereinstimmen.

Gewünschtes Ergebnis:

- Sie treffen bei der Bereitstellung von Änderungen an Ihrer Workload fundierte Entscheidungen.
- Änderungen entsprechen der Governance.

## Typische Anti-Muster:

- Sie stellen eine Änderung an Ihrer Workload bereit, ohne einen Prozess für die Verarbeitung einer fehlgeschlagenen Bereitstellung zu haben.
- Sie nehmen Änderungen an Ihrer Produktionsumgebung vor, die nicht mit den Governance-Anforderungen vereinbar sind.
- Sie stellen eine neue Version Ihrer Workload bereit, ohne eine Baseline für die Ressourcenauslastung zu erstellen.

## Vorteile der Nutzung dieser bewährten Methode:

- Sie sind auf fehlgeschlagene Änderungen an Ihrer Workload vorbereitet.
- Änderungen an Ihrer Workload sind konform mit den Governance-Richtlinien.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Niedrig

## Implementierungsleitfaden

Verwenden Sie Pre-mortem-Übungen, um Prozesse für fehlgeschlagene Änderungen zu entwickeln. Dokumentieren Sie Ihre Prozesse für fehlgeschlagene Änderungen. Stellen Sie sicher, dass alle Änderungen mit der Governance übereinstimmen. Evaluieren Sie die Vorteile und Risiken der Bereitstellung von Änderungen an Ihrer Workload.

## Kundenbeispiel

AnyCompany Der Einzelhandel führt regelmäßig Vorsorgeuntersuchungen durch, um seine Prozesse auf erfolglose Änderungen hin zu überprüfen. Die Prozesse werden in einem gemeinsamen Wiki dokumentiert und regelmäßig aktualisiert. Alle Änderungen entsprechen den Governance-Anforderungen.

## Implementierungsschritte

1. Treffen Sie fundierte Entscheidungen, wenn Sie Änderungen an Ihrer Workload bereitstellen. Legen Sie Kriterien für eine erfolgreiche Bereitstellung fest und überprüfen Sie diese. Entwickeln Sie Szenarien oder Kriterien, die ein Rollback einer Änderung auslösen würden. Wägen Sie den Nutzen der Bereitstellung von Änderungen gegen die Risiken einer fehlgeschlagenen Änderung ab.
2. Überprüfen Sie, ob alle Änderungen mit den Governance-Richtlinien übereinstimmen.

3. Planen Sie anhand von Pre-Mortems fehlgeschlagene Änderungen und dokumentieren Sie Strategien zur Schadensbegrenzung. Führen Sie eine Table-Top-Übung durch, um eine fehlgeschlagene Änderung zu modellieren und Rollback-Verfahren zu validieren.

Aufwand für den Implementierungsplan: Mittel. Die Einführung von Pre-Mortems erfordert die Koordination und den Einsatz aller Stakeholder in Ihrer gesamten Organisation

Ressourcen

Zugehörige bewährte Methoden:

- [OPS01-BP03 Bewertung der Governance-Anforderungen](#) – Governance-Anforderungen sind ein Schlüssel bei der Entscheidung zur Bereitstellung einer Änderung.
- [OPS06-BP01 Plan für erfolglose Änderungen](#) – Erstellen Sie Pläne zur Eindämmung einer fehlgeschlagenen Bereitstellung und verwenden Sie Pre-Mortems, um diese zu validieren.
- [OPS06-BP02 Testbereitstellungen](#) – Jede Softwareänderung sollte vor der Bereitstellung ordnungsgemäß getestet werden, um Fehler in der Produktion zu reduzieren.
- [OPS07-BP01 Personalfähigkeit sicherstellen](#) – Ausreichend trainierte Mitarbeiter zur Unterstützung der Workload sind unerlässlich, um eine fundierte Entscheidung über die Bereitstellung einer Systemänderung zu treffen.

Zugehörige Dokumente:

- [Amazon Web Services: Risiko und Compliance](#)
- [AWS Modell der geteilten Verantwortung](#)
- [Unternehmensführung im AWS Cloud: Das richtige Gleichgewicht zwischen Agilität und Sicherheit](#)

OPS07-BP06 Supportpläne für Produktionsworkloads erstellen

Aktivieren Sie Support für sämtliche Software und Services, auf denen Ihre Produktions-Workload basiert. Wählen Sie ein geeignetes Support-Level für Ihre Servicelevel-Anforderungen in der Produktion. Supportpläne für diese Abhängigkeiten sind wichtig für den Fall von Serviceunterbrechungen oder Softwareproblemen. Dokumentieren Sie Supportpläne sowie die Verfahren zur Anfrage nach Support bei allen Service- und Softwareanbietern. Implementieren Sie Mechanismen zur Prüfung, ob Support-Kontaktpunkte stets aktuell sind.

Gewünschtes Ergebnis:



- Implementieren Sie Supportpläne für Software und Services, auf denen Ihre Produktions-Workloads basieren.
- Wählen Sie einen geeigneten Supportplan auf der Grundlage Ihrer Service-Level-Anforderungen.
- Dokumentieren Sie die Supportpläne, die Supportlevels und die Vorgehensweise bei Supportanfragen.

#### Typische Anti-Muster:

- Sie haben keinen Supportplan für einen kritischen Softwareanbieter. Dies beeinflusst Ihre Workload und Sie haben keine Möglichkeit, schnell einen Fix oder rechtzeitige Updates von dem Anbieter zu erhalten.
- Ein Entwickler, der der primäre Ansprechpartner bei einem Softwareanbieter war, hat das Unternehmen verlassen. Sie können den Support des Anbieters nicht direkt erreichen. Sie müssen Zeit aufwenden, um sich durch generische Kontaktsysteme zu arbeiten, was die Reaktionszeiten verlängert.
- Bei einem Softwareanbieter ereignet sich ein Produktionsausfall. Es gibt keine Dokumentation dazu, wie ein Supportfall einzureichen ist.

#### Vorteile der Nutzung dieser bewährten Methode:

- Mit dem richtigen Supportlevel können Sie schnell eine Reaktion erhalten, die dem Service-Level entspricht.
- Als Kunde mit Support stehen Ihnen bei Produktionsproblemen Eskalationsmöglichkeiten zur Verfügung.
- Software- und Serviceanbieter können Ihnen bei Vorfällen Unterstützung bei der Fehlerbehebung bieten.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Niedrig

#### Implementierungsleitfaden

Aktivieren Sie die Supportpläne für sämtliche Software- und Serviceanbieter, von denen Ihre Produktions-Workload abhängt. Richten Sie geeignete Supportpläne ein, um Service-Level einhalten zu können. Für AWS Kunden bedeutet dies, AWS Business Support oder höher für alle Konten zu aktivieren, für die Sie Produktionsworkloads haben. Treffen Sie sich regelmäßig mit Supportanbietern, um Neues zu Supportangeboten, -prozessen und -ansprechpartnern zu erfahren.

Dokumentieren Sie das Supportverfahren bei Software- und Serviceanbietern, einschließlich der Eskalationsmöglichkeiten bei Ausfällen. Implementieren Sie Mechanismen, um die Supportkontakte stets auf aktuellem Stand zu halten.

### Kundenbeispiel

Bei AnyCompany Retail gibt es für alle kommerziellen Software- und Serviceabhängigkeiten Supportpläne. Sie haben beispielsweise AWS Enterprise Support für alle Konten mit Produktionsworkloads aktiviert. Jeder Entwickler kann bei einem Problem einen Supportfall auslösen. Es gibt eine Wiki-Seite mit Informationen zum Verfahren bei Supportanfragen, zu den Ansprechpartnern und zu bewährten Methoden dafür.

### Implementierungsschritte

1. Arbeiten Sie mit den Stakeholdern in Ihrer Organisation, um Software- und Serviceanbieter zu identifizieren, von denen Ihre Workload abhängt. Dokumentieren Sie diese Abhängigkeiten.
2. Legen Sie die Service-Level-Anforderungen für Ihre Workload fest. Wählen Sie einen Supportplan, der dazu passt.
3. Richten Sie für kommerzielle Software und Services einen Supportplan bei den Anbietern ein.
  - a. Ein Abonnement von AWS Business Support oder höher für alle Produktionskonten bietet eine schnellere Reaktionszeit von AWS Support und wird dringend empfohlen. Wenn Sie keinen Premium-Support haben, benötigen Sie einen Aktionsplan zur Behebung von AWS Support Problemen, für die Sie Hilfe benötigen. AWS Support bietet eine Mischung aus Tools und Technologie, Mitarbeitern und Programmen, die Sie proaktiv dabei unterstützen sollen, die Leistung zu optimieren, Kosten zu senken und Innovationen schneller umzusetzen. AWS Business Support bietet zusätzliche Vorteile, darunter Zugriff auf das AWS Trusted Advisor AWS Personal Health Dashboard und schnellere Reaktionszeiten.
4. Dokumentieren Sie den Supportplan in Ihrem Wissensmanagement-Tool. Berücksichtigen Sie dabei, wie eine Supportanfrage durchgeführt wird, wer in einem solchen Fall zu benachrichtigen ist und wie Vorfälle eskaliert werden können. Ein Wiki ist ein gutes Hilfsmittel, das allen Beteiligten ermöglicht, erforderliche Aktualisierungen der Dokumentation vorzunehmen, wenn ihnen Änderungen bei Supportprozessen oder Ansprechpartnern bekannt werden.

Aufwand für den Implementierungsplan: Niedrig. Die meisten Software- und Serviceanbieter bieten Opt-in-Supportpläne an. Durch die Dokumentation und die Weitergabe bewährter Supportmethoden in Ihrem Wissensmanagementsystem können Sie sicherstellen, dass Ihr Team weiß, was bei einem Produktionsproblem zu tun ist.

## Ressourcen

Zugehörige bewährte Methoden:

- [OPS02-BP02 Prozesse und Verfahren haben Eigentümer identifiziert](#)

Zugehörige Dokumente:

- [AWS Support Pläne](#)

Zugehörige Services:

- [AWS Support für Unternehmen](#)
- [AWS Support für Unternehmen](#)

## Betrieb

Fragen

- [OPS8 Wie nutzen Sie die Beobachtbarkeit von Workloads in Ihrer Organisation?](#)
- [OPS9. Wie können Sie den Zustand Ihrer Operationen beurteilen?](#)
- [OPS10. Wie bewältigen Sie Workload- und operationsspezifische Ereignisse?](#)

### OPS8 Wie nutzen Sie die Beobachtbarkeit von Workloads in Ihrer Organisation?

Sorgen Sie für einen optimalen Zustand der Workload, indem Sie die Beobachtbarkeit nutzen. Nutzen Sie relevante Metriken, Protokolle und Ablaufverfolgungen, um sich einen umfassenden Überblick über die Leistung Ihrer Workload zu verschaffen und Probleme effizient zu beheben.

Bewährte Methoden

- [OPS08-BP01 Analysieren Sie Workload-Metriken](#)
- [OPS08-BP02 Analysieren Sie Workload-Protokolle](#)
- [OPS08-BP03 Analysieren Sie Workload-Traces](#)
- [OPS08-BP04 Erstellen Sie umsetzbare Benachrichtigungen](#)
- [OPS08-BP05 Dashboards erstellen](#)

## OPS08-BP01 Analysieren Sie Workload-Metriken

Analysieren Sie nach der Implementierung der Anwendungstelemetrie regelmäßig die gesammelten Metriken. Latenz, Anfragen, Fehler und Kapazität (oder Kontingente) liefern zwar Erkenntnisse zur Systemleistung, es ist jedoch wichtig, die Überprüfung der Metriken zu Geschäftsergebnissen zu priorisieren. Dadurch wird sichergestellt, dass Sie datengestützte Entscheidungen treffen, die auf Ihre Geschäftsziele abgestimmt sind.

Gewünschtes Ergebnis: Präzise Erkenntnisse zur Workload-Leistung, die als Grundlage für datengestützte Entscheidungen dienen und die Abstimmung mit den Geschäftszielen sicherstellen.

Typische Anti-Muster:

- Isolierte Analyse von Metriken, ohne deren Auswirkungen auf die Geschäftsergebnisse zu berücksichtigen.
- Übermäßiges Vertrauen in technische Metriken, während Geschäftsmetriken ignoriert werden.
- Seltene Überprüfung von Metriken, Entscheidungsmöglichkeiten in Echtzeit werden verpasst.

Vorteile der Nutzung dieser bewährten Methode:

- Verbessertes Verständnis des Zusammenhangs zwischen technischer Leistung und Geschäftsergebnissen.
- Verbesserter Entscheidungsprozess auf der Grundlage von Echtzeitdaten.
- Proaktive Identifizierung und Minderung von Problemen, bevor sie sich auf die Geschäftsergebnisse auswirken.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Mittel

Implementierungsleitfaden

Nutzen Sie Tools wie Amazon CloudWatch , um metrische Analysen durchzuführen. AWS Dienste wie CloudWatch Anomalieerkennung und Amazon DevOps Guru können zur Erkennung von Anomalien verwendet werden, insbesondere wenn statische Schwellenwerte unbekannt sind oder wenn Verhaltensmuster besser für die Erkennung von Anomalien geeignet sind.

Implementierungsschritte

1. Analysieren und überprüfen: Überprüfen Sie regelmäßig Ihre Workload-Metriken und werten Sie sie aus.

- a. Priorisieren Sie Metriken zu Geschäftsergebnissen gegenüber rein technischen.
  - b. Machen Sie sich mit der Bedeutung von Spitzen, Rückgängen oder Mustern in Ihren Daten vertraut.
2. Nutzen Sie Amazon CloudWatch: Verwenden Sie Amazon CloudWatch für eine zentrale Ansicht und detaillierte Analysen.
- a. Konfigurieren Sie CloudWatch Dashboards, um Ihre Kennzahlen zu visualisieren und sie im Laufe der Zeit zu vergleichen.
  - b. Verwenden Sie [Perzentile](#), CloudWatch um sich einen klaren Überblick über die Verteilung der Metriken zu verschaffen. Dies kann dazu beitragen, Ausreißer zu definieren SLAs und zu verstehen.
  - c. Richten Sie die [Erkennung von CloudWatch Anomalien](#) ein, um ungewöhnliche Muster zu identifizieren, ohne sich auf statische Schwellenwerte verlassen zu müssen.
  - d. Implementieren Sie [CloudWatch kontenübergreifende Beobachtbarkeit](#), um Anwendungen zu überwachen und Fehler zu beheben, die sich über mehrere Konten innerhalb einer Region erstrecken.
  - e. Verwenden Sie [CloudWatch Metric Insights](#), um Kennzahlen konten- und regionsübergreifend abzufragen und zu analysieren und Trends und Anomalien zu identifizieren.
  - f. Wenden Sie [CloudWatch Metric Math](#) an, um Ihre Kennzahlen zu transformieren, zu aggregieren oder zu berechnen, um tiefere Einblicke zu erhalten.
3. Nutzen Sie Amazon DevOps Guru: Integrieren Sie [Amazon DevOps Guru](#) für die durch maschinelles Lernen erweiterte Anomalieerkennung, um frühe Anzeichen von Betriebsproblemen Ihrer serverlosen Anwendungen zu erkennen und diese zu beheben, bevor sie sich auf Ihre Kunden auswirken.
4. Optimieren Sie auf der Grundlage von Erkenntnissen: Treffen Sie fundierte Entscheidungen auf der Grundlage Ihrer Metrikanalyse, um Ihre Workloads anzupassen und zu verbessern.

Aufwand für den Implementierungsplan: Mittel

Ressourcen

Zugehörige bewährte Methoden:

- [OPS04-BP01 Identifizieren Sie die wichtigsten Leistungsindikatoren](#)
- [OPS04-BP02 Implementieren Sie Anwendungstelemetrie](#)

## Zugehörige Dokumente:

- [The Wheel Blog – Die Bedeutung der kontinuierlichen Überprüfung von Metriken](#)
- [Perzentile sind wichtig](#)
- [Verwenden AWS Cost Anomaly Detection](#)
- [CloudWatch kontenübergreifende Beobachtbarkeit](#)
- [Fragen Sie Ihre Metriken mit Metrics Insights ab CloudWatch](#)

## Zugehörige Videos:

- [Kontoübergreifende Observability in Amazon aktivieren CloudWatch](#)
- [Einführung in Amazon DevOps Guru](#)
- [Analysieren Sie kontinuierlich Metriken mit AWS Cost Anomaly Detection](#)

## Zugehörige Beispiele:

- [Workshop zur Beobachtbarkeit](#)
- [AIOpsMit Amazon DevOps Guru Einblicke in den Betrieb gewinnen](#)

## OPS08-BP02 Analysieren Sie Workload-Protokolle

Die regelmäßige Analyse von Workload-Protokollen ist unerlässlich, um ein tieferes Verständnis der operativen Aspekte Ihrer Anwendung zu erlangen. Durch effizientes Durchsuchen, Visualisieren und Interpretieren von Protokolldaten können Sie die Leistung und Sicherheit von Anwendungen kontinuierlich optimieren.

Gewünschtes Ergebnis: Umfassende Erkenntnisse zum Anwendungsverhalten und zu Operationen, die aus einer gründlichen Protokollanalyse gewonnen wurden und für eine proaktive Problemerkennung und -behebung sorgen.

## Typische Anti-Muster:

- Die Analyse von Protokollen vernachlässigen, bis ein kritisches Problem auftritt.
- Die Suite verfügbarer Tools für die Protokollanalyse nicht nutzen und wichtige Erkenntnisse verpassen.

- Alleiniges Vertrauen auf die manuelle Überprüfung von Protokollen, ohne Automatisierungs- und Abfragefunktionen zu nutzen.

Vorteile der Nutzung dieser bewährten Methode:

- Proaktive Identifizierung von operativen Engpässen, Sicherheitsbedrohungen und anderen potenziellen Problemen.
- Effiziente Nutzung von Protokolldaten für die kontinuierliche Anwendungsoptimierung.
- Verbessertes Verständnis des Anwendungsverhaltens, Unterstützung beim Debuggen und bei der Problembehandlung.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Mittel

Implementierungsleitfaden

[Amazon CloudWatch Logs](#) ist ein leistungsstarkes Tool für die Protokollanalyse. Integrierte Funktionen wie CloudWatch Logs Insights und Contributor Insights machen das Ableiten aussagekräftiger Informationen aus Protokollen intuitiv und effizient.

Implementierungsschritte

1. CloudWatch Protokolle einrichten: Konfigurieren Sie Anwendungen und Dienste so, dass sie Protokolle an CloudWatch Logs senden.
2. Verwenden Sie die Erkennung von Protokollanomalien: Verwenden Sie die [Anomalieerkennung von Amazon CloudWatch Logs](#), um ungewöhnliche Protokollmuster automatisch zu identifizieren und darauf hinzuweisen. Mit diesem Tool können Sie Anomalien in Ihren Protokollen proaktiv verwalten und potenzielle Probleme frühzeitig erkennen.
3. CloudWatch Logs Insights einrichten: Verwenden Sie [CloudWatch Logs Insights](#), um Ihre Protokolldaten interaktiv zu suchen und zu analysieren.
  - a. Erstellen Sie Abfragen, um Muster zu extrahieren, Protokolldaten zu visualisieren und umsetzbare Erkenntnisse abzuleiten.
  - b. Verwenden Sie die [CloudWatch Logs Insights-Musteranalyse](#), um häufige Protokollmuster zu analysieren und zu visualisieren. Dieses Feature hilft Ihnen, allgemeine Betriebstrends und potenzielle Ausreißer in Ihren Protokolldaten nachzuvollziehen.
  - c. Verwenden Sie [CloudWatch Logs compare \(diff\)](#), um eine Differenzanalyse zwischen verschiedenen Zeiträumen oder zwischen verschiedenen Protokollgruppen durchzuführen.

Verwenden Sie diese Funktion, um Änderungen zu lokalisieren und deren Auswirkungen auf die Leistung oder das Verhalten Ihres Systems zu bewerten.

- Überwachen Sie Protokolle in Echtzeit mit Live Tail: Verwenden Sie [Amazon CloudWatch Logs Live Tail](#), um Protokolldaten in Echtzeit anzuzeigen. Sie können die Betriebsaktivitäten Ihrer Anwendung in Echtzeit aktiv überwachen, um sich einen unmittelbaren Einblick in die Systemleistung und potenzielle Probleme zu verschaffen.
- Nutzen Sie Contributor Insights: Verwenden Sie [CloudWatchContributor Insights](#), um Top-Talker in Dimensionen mit hoher Kardinalität wie IP-Adressen oder Benutzeragenten zu identifizieren.
- Implementieren Sie Metrikfilter für CloudWatch Logs: Konfigurieren Sie Metrikfilter für [CloudWatch Logs, um Protokolldaten in umsetzbare Metriken](#) umzuwandeln. Auf diese Weise können Sie Alarme einstellen oder Muster näher analysieren.
- Implementieren Sie [CloudWatchkontenübergreifende Beobachtbarkeit](#): Überwachen Sie Anwendungen, die sich über mehrere Konten innerhalb einer Region erstrecken, und beheben Sie Fehler.
- Regelmäßige Überprüfung und Verfeinerung: Überprüfen Sie regelmäßig Ihre Protokollanalysestrategien, um alle relevanten Informationen zu erfassen und die Anwendungsleistung kontinuierlich zu optimieren.

Aufwand für den Implementierungsplan: Mittel

Ressourcen

Zugehörige bewährte Methoden:

- [OPS04-BP01 Identifizieren Sie die wichtigsten Leistungsindikatoren](#)
- [OPS04-BP02 Implementieren Sie Anwendungstelemetrie](#)
- [OPS08-BP01 Analysieren Sie Workload-Metriken](#)

Zugehörige Dokumente:

- [Analysieren von Protokolldaten mit CloudWatch Logs Insights](#)
- [CloudWatch Contributor Insights verwenden](#)
- [CloudWatch Log-Metrikfilter erstellen und verwalten](#)

Zugehörige Videos:



- [Analysieren Sie Protokolldaten mit CloudWatch Logs Insights](#)
- [Verwenden Sie CloudWatch Contributor Insights, um Daten mit hoher Kardinalität zu analysieren](#)

Zugehörige Beispiele:

- [CloudWatch Protokolliert Beispielabfragen](#)
- [Workshop zur Beobachtbarkeit](#)

### OPS08-BP03 Analysieren Sie Workload-Traces

Die Analyse von Trace-Daten ist entscheidend, wenn es darum geht, einen umfassenden Überblick über den Betriebsverlauf einer Anwendung zu erhalten. Durch die Visualisierung und das Verständnis der Interaktionen zwischen verschiedenen Komponenten können die Leistung optimiert, Engpässe identifiziert und das Benutzererlebnis verbessert werden.

Gewünschtes Ergebnis: Sie verschaffen sich einen klaren Überblick über die verteilten Abläufe Ihrer Anwendung und erzielen dadurch eine schnellere Problemlösung und eine verbesserte Benutzererfahrung.

Typische Anti-Muster:

- Trace-Daten werden übersehen und man verlässt sich ausschließlich auf Protokolle und Metriken.
- Trace-Daten werden nicht mit zugehörigen Protokollen in Zusammenhang gebracht.
- Aus Traces abgeleitete Metriken wie Latenz und Fehlerraten werden ignoriert.

Vorteile der Nutzung dieser bewährten Methode:

- Verbessern Sie die Problembehandlung und reduzieren Sie die durchschnittliche Zeit bis zur Problemlösung ( ). MTTR
- Sie gewinnen Erkenntnisse über Abhängigkeiten und deren Auswirkungen.
- Sie können Leistungsprobleme rasch identifizieren und beheben.
- Sie nutzen von aus Trace abgeleitete Metriken für fundierte Entscheidungen.
- Sie erzielen ein besseres Benutzererlebnis durch optimierte Komponenteninteraktionen.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Mittel

## Implementierungsleitfaden

[AWS X-Ray](#) bietet eine umfassende Suite für die Analyse von Trace-Daten, die einen ganzheitlichen Überblick über Serviceinteraktionen, die Überwachung von Benutzeraktivitäten und die Erkennung von Leistungsproblemen bietet. Funktionen wie ServiceLens X-Ray Insights, X-Ray Analytics und Amazon DevOps Guru erweitern die Tiefe verwertbarer Erkenntnisse, die aus Trace-Daten gewonnen werden.

## Implementierungsschritte

Die folgenden Schritte bieten einen strukturierten Ansatz zur effektiven Implementierung der Analyse von Spurendaten mithilfe von AWS Services:

1. Integrieren AWS X-Ray: Stellen Sie sicher, dass X-Ray in Ihre Anwendungen integriert ist, um Trace-Daten zu erfassen.
2. Analyse von X-Ray-Metriken: Untersuchen Sie anhand von X-Ray-Traces abgeleitete Metriken wie Latenz, Anfrageraten, Fehlerraten und Antwortzeitverteilungen mithilfe der [Service-Übersicht](#), um den Status der Anwendung zu überwachen.
3. Verwendung ServiceLens: Nutzen Sie die [ServiceLensKarte](#), um die Sichtbarkeit Ihrer Dienste und Anwendungen zu verbessern. Dies ermöglicht eine integrierte Anzeige von Traces, Metriken, Protokollen, Alarmen und anderen Statusinformationen.
4. Aktivieren von X-Ray-Insights:
  - a. Aktivieren Sie [X-Ray-Insights](#) zur automatisierten Erkennung von Anomalien in Traces.
  - b. Untersuchen Sie Erkenntnisse, um Muster zu identifizieren und die Ursachen zu ermitteln, z. B. erhöhte Fehlerraten oder Latenzen.
  - c. Eine chronologische Analyse der erkannten Probleme finden Sie in der Insights-Timeline.
5. Verwenden von X-Ray Analytics: [X-Ray Analytics](#) ermöglicht es Ihnen, Trace-Daten gründlich zu untersuchen, Muster zu lokalisieren und Erkenntnisse zu gewinnen.
6. Verwenden von Gruppen in X-Ray: Erstellen Sie Gruppen in X-Ray, um Traces nach Kriterien wie hoher Latenz zu filtern und so eine gezieltere Analyse zu ermöglichen.
7. Integrieren Sie Amazon DevOps Guru: Nutzen Sie [Amazon DevOps Guru](#), um von Modellen für maschinelles Lernen zu profitieren, mit denen betriebliche Anomalien in Spuren lokalisiert werden können.
8. Verwenden Sie CloudWatch Synthetics: Verwenden Sie [CloudWatchSynthetics](#), um Kanarien für die kontinuierliche Überwachung Ihrer Endpunkte und Workflows zu erstellen. Sie können

diese Canaries in X-Ray integrieren, um Trace-Daten für eine eingehende Analyse der getesteten Anwendungen bereitzustellen.

9. Verwenden Sie Real User Monitoring (RUM): Mit [AWS X-Ray und CloudWatch RUM](#) können Sie den Anforderungspfad analysieren und debuggen, angefangen bei den Endbenutzern Ihrer Anwendung bis hin zu nachgeschalteten Managed Services. Auf diese Weise können Sie Latenzrends und Fehler identifizieren, die sich auf Ihre Endbenutzer auswirken.
10. Korrelieren von Daten mit Protokollen: Bringen Sie [Trace-Daten mit zugehörigen Protokollen](#) innerhalb der X-Ray-Trace-Ansicht in Zusammenhang, um eine detaillierte Perspektive auf das Anwendungsverhalten zu erhalten. Auf diese Weise können Sie Protokollereignisse anzeigen, die direkt mit verfolgten Transaktionen verknüpft sind.
11. Implementieren Sie [CloudWatchkontenübergreifende Beobachtbarkeit](#): Überwachen Sie Anwendungen, die sich über mehrere Konten innerhalb einer Region erstrecken, und beheben Sie Fehler.

Aufwand für den Implementierungsplan: Mittel

Ressourcen

Zugehörige bewährte Methoden:

- [OPS08-BP01 Analysieren Sie Workload-Metriken](#)
- [OPS08-BP02 Analysieren Sie Workload-Protokolle](#)

Zugehörige Dokumente:

- [Verwendung ServiceLens zur Überwachung des Anwendungszustands](#)
- [Erkunden von Trace-Daten mit X-Ray Analytics](#)
- [Mit X-Ray-Insights Anomalien in Traces erkennen](#)
- [Kontinuierliche Überwachung mit CloudWatch Synthetics](#)

Zugehörige Videos:

- [Analysieren und Debuggen von Anwendungen mit Amazon CloudWatch Synthetics & AWS X-Ray](#)
- [Nutzung von AWS X-Ray -Insights](#)

## Zugehörige Beispiele:

- [Workshop zur Beobachtbarkeit](#)
- [Implementierung von X-Ray mit AWS Lambda](#)
- [CloudWatchSynthetics Canary Schablonen](#)

## OPS08-BP04 Erstellen Sie umsetzbare Benachrichtigungen

Es ist entscheidend, Abweichungen im Verhalten Ihrer Anwendung umgehend zu erkennen und darauf zu reagieren. Besonders wichtig ist es, zu erkennen, wann Ergebnisse, die auf wichtigen Leistungsindikatoren (KPIs) basieren, gefährdet sind oder wann unerwartete Anomalien auftreten. Durch die Verwendung von Warnmeldungen KPIs wird sichergestellt, dass die Signale, die Sie erhalten, in direktem Zusammenhang mit geschäftlichen oder betrieblichen Auswirkungen stehen. Der Ansatz mit umsetzbaren Warnmeldungen fördert proaktive Reaktionen und trägt zur Aufrechterhaltung der Systemleistung und Zuverlässigkeit bei.

Gewünschtes Ergebnis: Erhalten Sie zeitnahe, relevante und umsetzbare Warnmeldungen, um potenzielle Probleme schnell zu erkennen und zu beheben, insbesondere wenn die KPI Ergebnisse gefährdet sind.

## Typische Anti-Muster:

- Es werden zu viele unkritische Warnmeldungen eingerichtet, was zu einer Alarmmüdigkeit führt.
- Keine Priorisierung von Warnmeldungen auf der Grundlage von KPIs Problemen, was es schwierig macht, die geschäftlichen Auswirkungen von Problemen zu verstehen.
- Die eigentlichen Ursachen werden vernachlässigt, was zu wiederholten Warnmeldungen für dasselbe Problem führt.

## Vorteile der Nutzung dieser bewährten Methode:

- Geringere Alarmermüdung durch Fokussierung auf umsetzbare und relevante Warnmeldungen.
- Verbesserte Systemverfügbarkeit und -zuverlässigkeit durch proaktive Problemerkennung und -behebung.
- Verbesserte Teamzusammenarbeit und schnellere Problemlösung durch die Integration in übliche Alarmierungs- und Kommunikationstools.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Hoch

## Implementierungsleitfaden

Um einen effektiven Warnmechanismus zu schaffen, ist es wichtig, Metriken, Protokolle und Rückverfolgungsdaten zu verwenden, die darauf hinweisen, wenn die Ergebnisse, die darauf basieren, gefährdet KPIs sind oder Anomalien entdeckt werden.

### Implementierungsschritte

1. Ermitteln Sie die wichtigsten Leistungsindikatoren (KPIs): Identifizieren Sie die Ihrer Anwendung. KPIs Warnmeldungen sollten mit diesen verknüpft werden, um die Auswirkungen KPIs auf das Unternehmen genau widerzuspiegeln.
2. Implementierung der Erkennung von Anomalien:
  - Verwenden Sie die CloudWatch Amazon-Anomalieerkennung: Richten Sie die [CloudWatch Amazon-Anomalieerkennung](#) so ein, dass ungewöhnliche Muster automatisch erkannt werden, sodass Sie nur Warnmeldungen für echte Anomalien generieren können.
  - AWS X-Ray Nutzen Sie Insights:
    - a. Richten Sie [X-Ray-Insights](#) ein, um Anomalien in Trace-Daten zu erkennen.
    - b. Konfigurieren Sie [Benachrichtigungen für X-Ray-Insights](#), um bei erkannten Problemen gewarnt zu werden.
  - Integrieren Sie mit Amazon DevOps Guru:
    - a. Nutzen Sie [Amazon DevOps Guru](#) für seine maschinellen Lernfunktionen zur Erkennung betrieblicher Anomalien anhand vorhandener Daten.
    - b. Navigieren Sie zu den [Benachrichtigungseinstellungen](#) in DevOps Guru, um Anomaliewarnungen einzurichten.
3. Implementieren umsetzbarer Warnmeldungen: Entwerfen Sie Warnmeldungen, die angemessene Informationen für sofortige Maßnahmen liefern.
  1. Überwachen Sie [AWS Health Ereignisse mit EventBridge Amazon-Regeln](#) oder integrieren Sie sie programmatisch, AWS Health API um Aktionen zu automatisieren, wenn Sie AWS Health Ereignisse erhalten. Dies können allgemeine Aktionen sein, z. B. das Senden aller geplanten Lebenszyklus-Ereignisnachrichten an eine Chat-Oberfläche, oder spezifische Aktionen, wie das Initiieren eines Workflows in einem IT-Service-Management-Tool.
4. Verringern der Alarmmüdigkeit: Minimieren Sie die Zahl der Warnmeldungen, die nicht kritisch sind. Wenn Teams mit zahllosen unbedeutenden Warnmeldungen überfordert werden, können sie den Überblick über kritische Probleme verlieren, was die Gesamteffektivität des Warnmechanismus beeinträchtigt.

5. Kombinierte Alarme einrichten: Verwenden Sie CloudWatch zusammengesetzte [Alarme von Amazon](#), um mehrere Alarme zu konsolidieren.
6. Integration mit Alarm-Tools: Integrieren Sie Tools wie [Ops Genie](#) und [PagerDuty](#).
7. Engage AWS Chatbot: Integrieren Sie [AWS Chatbot](#), um Benachrichtigungen an Amazon Chime, Microsoft Teams und Slack weiterzuleiten.
8. Auf Protokollen basierende Warnung: Verwenden Sie [Filter für Protokollmetriken](#) CloudWatch , um Alarme auf der Grundlage bestimmter Protokollereignisse zu erstellen.
9. Überprüfen und wiederholen: Überprüfen und verfeinern Sie die Warnkonfigurationen regelmäßig.

Aufwand für den Implementierungsplan: Mittel

Ressourcen

Zugehörige bewährte Methoden:

- [OPS04-BP01 Identifizieren Sie die wichtigsten Leistungsindikatoren](#)
- [OPS04-BP02 Implementieren Sie Anwendungstelemetrie](#)
- [OPS04-BP03 Implementieren Sie Benutzererlebnis-Telemetrie](#)
- [OPS04-BP04 Implementieren Sie Abhängigkeitstelemetrie](#)
- [OPS04-BP05 Implementieren Sie verteiltes Tracing](#)
- [OPS08-BP01 Analysieren Sie Workload-Metriken](#)
- [OPS08-BP02 Analysieren Sie Workload-Protokolle](#)
- [OPS08-BP03 Analysieren Sie Workload-Traces](#)

Zugehörige Dokumente:

- [CloudWatch Amazon-Alarme verwenden](#)
- [Erstellen eines zusammengesetzten Alarms](#)
- [Erstellen Sie einen CloudWatch Alarm, der auf der Erkennung von Anomalien basiert](#)
- [DevOpsGuru-Benachrichtigungen](#)
- [X-ray insights notifications](#)
- [Überwachen, verwalten und beheben Sie Ihre AWS Ressourcen interaktiv ChatOps](#)
- [CloudWatch Amazon-Integrationsleitfaden | PagerDuty](#)
- [Integrieren Sie Opsgenie mit Amazon CloudWatch](#)

## Zugehörige Videos:

- [Erstellen Sie zusammengesetzte Alarme in Amazon CloudWatch](#)
- [AWS Chatbot Übersicht](#)
- [AWS Auf Air ft. Mutative Befehle](#) in AWS Chatbot

## Zugehörige Beispiele:

- [Alarme, Vorfalmanagement und Problembehebung in der Cloud mit Amazon CloudWatch](#)
- [Tutorial: Eine EventBridge Amazon-Regel erstellen, die Benachrichtigungen sendet an AWS Chatbot](#)
- [Workshop zur Beobachtbarkeit](#)

## OPS08-BP05 Dashboards erstellen

Dashboards sind die anwenderorientierte Sicht auf die Telemetriedaten Ihrer Workloads. Sie stellen zwar eine wichtige visuelle Schnittstelle dar, sollten aber nicht als Ersatz, sondern als Ergänzung für Warnmechanismen dienen. Wenn sie sorgfältig zusammengestellt werden, liefern sie nicht nur schnelle Erkenntnisse zum Status und zur Leistung des Systems, sondern bieten Stakeholdern auch Echtzeitinformationen über Geschäftsergebnisse und die Auswirkungen von Problemen.

### Gewünschtes Ergebnis:

Klare, umsetzbare Erkenntnisse zur System- und Geschäftsstabilität mithilfe visueller Darstellungen.

### Typische Anti-Muster:

- Überkomplizierte Dashboards mit zu vielen Metriken.
- Sich auf Dashboards verlassen, ohne Warnmeldungen zur Erkennung von Anomalien zu nutzen.
- Fehlende Aktualisierung der Dashboards im Laufe des Workload-Fortschritts.

### Vorteile dieser bewährten Methode:

- Sofortiger Einblick in wichtige Systemmetriken und KPIs
- Verbesserte Kommunikation und mehr Verständnis unter den Stakeholdern.
- Rasche Erkenntnisse zu den Auswirkungen operativer Probleme.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Mittel

## Implementierungsleitfaden

### Geschäftsorientierte Dashboards

Auf Unternehmen KPIs zugeschnittene Dashboards sprechen ein breiteres Spektrum von Stakeholdern an. Auch wenn diese Personen vielleicht nicht an Systemmetriken interessiert sind, haben sie dennoch großes Interesse daran, die geschäftlichen Auswirkungen dieser Zahlen zu verstehen. Ein geschäftsorientiertes Dashboard stellt sicher, dass alle technischen und betrieblichen Metriken, die überwacht und analysiert werden, auf die übergeordneten Geschäftsziele ausgerichtet sind. Diese Ausrichtung sorgt für Klarheit und stellt sicher, dass alle gleich darüber informiert sind, was wichtig ist und was nicht. Darüber hinaus sind Dashboards, in denen Unternehmen hervorgehoben werden, in der KPIs Regel umsetzbarer. Sie bieten Stakeholdern die Möglichkeit, in kürzester Zeit den Status der Abläufe, die Bereiche, die Aufmerksamkeit erfordern, und die potenziellen Auswirkungen auf die Geschäftsergebnisse zu verstehen.

Vor diesem Hintergrund sollten Sie bei der Erstellung Ihrer Dashboards sicherstellen, dass ein Gleichgewicht zwischen technischen Kennzahlen und geschäftlichen Kennzahlen besteht. KPIs Beide sind wichtig, richten sich aber an unterschiedliche Zielgruppen. Idealerweise sollten Sie über Dashboards verfügen, die einen ganzheitlichen Überblick über den Status und die Leistung des Systems bieten und gleichzeitig wichtige Geschäftsergebnisse und deren Auswirkungen hervorheben.

CloudWatch Amazon-Dashboards sind anpassbare Homepages in der CloudWatch Konsole, mit denen Sie Ihre Ressourcen in einer einzigen Ansicht überwachen können, auch die Ressourcen, die auf verschiedene AWS-Regionen Konten verteilt sind.

## Implementierungsschritte

1. Erstellen Sie ein einfaches Dashboard: [Erstellen Sie ein neues Dashboard in CloudWatch](#) und geben Sie ihm einen aussagekräftigen Namen.
2. Verwenden von Markdown-Widgets: Bevor Sie sich mit den Metriken befassen, [verwenden Sie Markdown-Widgets](#), um Ihr Dashboard oben mit Kontext zu versehen. Dieser sollte den Inhalt des Dashboards beschreiben und angeben, welche Bedeutung den dargestellten Metriken zukommt. Er kann auch Links zu anderen Dashboards und Tools zur Fehlerbehebung enthalten.
3. Erstellen von Dashboard-Variablen: [Integrieren Sie gegebenenfalls Dashboard-Variablen](#), um dynamische und flexible Dashboard-Ansichten zu ermöglichen.



4. Erstellen von Metrik-Widgets: [Fügen Sie Metrik-Widgets hinzu](#), um verschiedene Metriken zu visualisieren, die Ihre Anwendung ausgibt, und passen Sie diese Widgets so an, dass sie den Systemstatus und die Geschäftsergebnisse effektiv darstellen.
5. Log Insights-Abfragen: Verwenden [CloudWatch Log Insights](#), um umsetzbare Kennzahlen aus Ihren Protokollen abzuleiten und diese Erkenntnisse auf Ihrem Dashboard anzuzeigen.
6. Alarme einrichten: Integrieren Sie [CloudWatch Alarme](#) in Ihr Dashboard, um einen schnellen Überblick über alle Messwerte zu erhalten, die ihre Schwellenwerte überschreiten.
7. Verwenden Sie Contributor Insights: Integrieren Sie [CloudWatch Contributor Insights](#), um Felder mit hoher Kardinalität zu analysieren und ein besseres Verständnis der wichtigsten Mitwirkenden Ihrer Ressource zu erhalten.
8. Entwerfen benutzerdefinierter Widgets: Für spezielle Anforderungen, die von Standard-Widgets nicht erfüllt werden, sollten Sie es in Betracht ziehen, [benutzerdefinierte Widgets](#) zu erstellen. Diese können Daten aus verschiedenen Datenquellen abrufen oder sie auf einzigartige Weise darstellen.
9. Verwendung AWS Health Dashboard: Verwenden Sie diese [AWS Health Dashboard](#) Option, um tiefere Einblicke in den Zustand Ihres Kontos, Ereignisse und bevorstehende Änderungen zu erhalten, die sich auf Ihre Dienste und Ressourcen auswirken könnten. Sie können auch eine zentrale Übersicht über Statusereignisse in AWS Organizations abrufen oder Ihre eigenen benutzerdefinierten Dashboards erstellen (weitere Informationen finden Sie unter „Verwandte Beispiele“).
10. Wiederholen und verfeinern: Im Laufe der Entwicklung Ihrer Anwendung sollten Sie Ihr Dashboard regelmäßig überprüfen, um sicherzustellen, dass es weiterhin relevant ist.

## Ressourcen

### Zugehörige bewährte Methoden:

- [OPS04-BP01 Identifizieren Sie die wichtigsten Leistungsindikatoren](#)
- [OPS08-BP01 Analysieren Sie Workload-Metriken](#)
- [OPS08-BP02 Analysieren Sie Workload-Protokolle](#)
- [OPS08-BP03 Analysieren Sie Workload-Traces](#)
- [OPS08-BP04 Erstellen Sie umsetzbare Benachrichtigungen](#)

### Zugehörige Dokumente:

- [Erstellung von Dashboards für operative Sichtbarkeit](#)
- [Verwenden von CloudWatch Amazon-Dashboards](#)

Zugehörige Videos:

- [Erstellen Sie konto- und regionsübergreifende Dashboards CloudWatch](#)
- [AWS re:Invent 2021 - Gain enterprise visibility with AWS Cloud operation dashboards\)](#)

Zugehörige Beispiele:

- [Workshop zur Beobachtbarkeit](#)
- [Anwendungsüberwachung mit Amazon CloudWatch](#)
- [AWS Health Dashboards und Einblicke zur Ereignisanalyse](#)
- [Visualisieren von AWS Health -Ereignissen mit Amazon Managed Grafana](#)

## OPS9. Wie können Sie den Zustand Ihrer Operationen beurteilen?

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

Bewährte Methoden

- [OPS09-BP01 Betriebsziele messen und mit Kennzahlen KPIs](#)
- [OPS09-BP02 Kommunizieren Sie Status und Trends, um einen Überblick über den Betrieb zu gewährleisten](#)
- [OPS09-BP03 Überprüfen Sie die Betriebskennzahlen und priorisieren Sie Verbesserungen](#)

### OPS09-BP01 Betriebsziele messen und mit Kennzahlen KPIs

Ermitteln Sie von Ihrem Unternehmen Ziele KPIs, die den betrieblichen Erfolg definieren, und stellen Sie fest, dass die Kennzahlen diese widerspiegeln. Legen Sie Baselines als Bezugspunkt fest und bewerten Sie diese regelmäßig neu. Entwickeln Sie Mechanismen, um diese Metriken von Teams zur Bewertung zu erfassen.

Gewünschtes Ergebnis:

- Die Ziele und die KPIs für die Betriebsteams der Organisation geltenden Ziele wurden veröffentlicht und gemeinsam genutzt.
- Metriken, die diese widerspiegeln KPIs, wurden festgelegt. Mögliche Beispiele:
  - Tiefe der Ticket-Warteschlange oder Durchschnittsalter der Tickets
  - Anzahl der Tickets, gruppiert nach Art des Problems
  - Zeit, die für die Bearbeitung von Problemen mit oder ohne standardisierte Betriebsprozedur aufgewendet wurde (SOP)
  - Zeit, die zur Wiederherstellung nach einem fehlgeschlagenen Code-Push aufgewendet wurde
  - Anruflautstärke

#### Typische Anti-Muster:

- Bereitstellungsfristen werden nicht eingehalten, weil Entwickler mit der Lösung von Problemen beauftragt werden. Entwicklerteams fordern mehr Personal, können aber nicht einschätzen, wie viele Personen benötigt werden, da der Zeitaufwand nicht gemessen werden kann.
- Für die Abwicklung von Kundenanrufen wurde ein Problem-Desk Stufe 1 eingerichtet. Im Laufe der Zeit kamen weitere Workloads hinzu, aber dem Problem-Desk Stufe 1 wurde kein zusätzliches Personal zugewiesen. Die Kundenzufriedenheit leidet, da immer mehr Anrufe nötig sind und Probleme länger ungelöst bleiben. Das Management sieht diese Anzeichen jedoch nicht und ermöglicht keine Gegenmaßnahmen.
- Eine problematische Workload wurde zur Bearbeitung an ein separates Operations-Team übergeben. Im Gegensatz zu anderen Workloads wurde diese neue Workload nicht mit ordnungsgemäßer Dokumentation und Runbooks geliefert. Daher verbringen Teams mehr Zeit damit, Fehler zu suchen und zu beheben. Es gibt jedoch keine Metriken, die dies dokumentieren, was die Rechenschaftspflicht erschwert.

Vorteile der Nutzung dieser bewährten Methode: Während die Workload-Überwachung den Status unserer Anwendungen und Services anzeigt, liefert die Überwachung von Operations-Teams den Verantwortlichen Erkenntnisse hinsichtlich Veränderungen bei den Benutzern dieser Workloads, wie z. B. sich ändernde Geschäftsanforderungen. Messen Sie die Effektivität dieser Teams und bewerten Sie sie im Hinblick auf Ihre operativen Ziele, indem Sie Metriken erstellen, die den operativen Status widerspiegeln können. Anhand von Metriken können Supportprobleme aufgezeigt oder Abweichungen von einem angestrebten Servicelevel erkannt werden.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Mittel

## Implementierungsleitfaden

Planen Sie Meetings mit der Geschäftsleitung und den Stakeholdern, um die allgemeinen Ziele des Services festzulegen. Ermitteln Sie, worin die Aufgaben der verschiedenen Operations-Teams bestehen sollten und mit welchen Herausforderungen sie beauftragt werden könnten. Führen Sie anhand dieser Daten ein Brainstorming der wichtigsten Leistungsindikatoren (KPIs) durch, die diese Betriebsziele widerspiegeln könnten. Dies können Faktoren wie Kundenzufriedenheit, Zeitspanne zwischen Entwurf und Bereitstellung von Features, durchschnittlicher Zeitaufwand für die Problemlösung und andere sein.

Identifizieren Sie auf dieser Grundlage die Kennzahlen und Datenquellen, die diese Ziele am besten widerspiegeln könnten. KPIs Kundenzufriedenheit kann eine Kombination aus verschiedenen Metriken wie Warte- oder Reaktionszeiten bei Anrufen, Zufriedenheitswerte und Art der dargelegten Probleme sein. Die Bereitstellungszeiten können die Summe des Zeitaufwands sein, der für Tests und Bereitstellungen benötigt wird, zuzüglich aller Korrekturen nach der Bereitstellung, die hinzugefügt werden mussten. Statistiken, aus denen hervorgeht, wie viel Zeit für verschiedene Arten von Problemen aufgewendet wurde (oder wie viele dieser Probleme auftraten), können Aufschluss darüber geben, wo gezielte Anstrengungen erforderlich sind.

### Ressourcen

#### Zugehörige Dokumente:

- [Amazon QuickSight — Verwenden KPIs](#)
- [Amazon CloudWatch — Metriken verwenden](#)
- [Erstellung von Dashboards](#)
- [So verfolgen Sie Ihre Kostenoptimierung KPIs mit dem KPI Dashboard](#)

OPS09-BP02 Kommunizieren Sie Status und Trends, um einen Überblick über den Betrieb zu gewährleisten

Wenn Sie in Erfahrung bringen wollen, wann Ergebnisse gefährdet sein könnten, ob zusätzliche Workloads unterstützt werden können oder nicht oder welche Auswirkungen Änderungen auf Ihre Teams hatten, müssen Sie unbedingt den Status Ihrer Betriebsabläufe und deren Trendrichtung kennen. Bei Betriebsereignissen können Statusseiten, auf denen Benutzer und Operations-Teams Informationen abrufen können, den Druck auf die Kommunikationskanäle verringern und Informationen proaktiv verbreiten.

#### Gewünschtes Ergebnis:

- Betriebsleiter erhalten auf einen Blick Erkenntnisse darüber, welches Anrufvolumen ihre Teams bewältigen müssen und welche Maßnahmen möglicherweise im Gange sind, z. B. Bereitstellungen.
- Wenn Auswirkungen auf den normalen Betrieb auftreten, werden Warnmeldungen an Stakeholder und Benutzergemeinschaften versendet.
- Unternehmensleitung und Stakeholder können als Reaktion auf eine Warnung oder Auswirkung eine Statusseite aufrufen und Informationen zu einem betrieblichen Ereignis abrufen, z. B. Kontaktstellen, Ticketinformationen und erwartete Wiederherstellungszeiten.
- Führungskräften und anderen Stakeholdern werden Berichte zur Verfügung gestellt, damit sie über Betriebsstatistiken wie das Anrufvolumen über einen bestimmten Zeitraum, Benutzerzufriedenheitswerte, Anzahl ausstehender Tickets und deren Alter informiert sind.

#### Typische Anti-Muster:

- Eine Workload fällt aus und ein Dienst wird nicht verfügbar. Das Anrufvolumen steigt, da Benutzer wissen möchten, was vor sich geht. Manager erhöhen dieses Volumen, da sie nachfragen, wer an dem Problem arbeitet. Verschiedene Operations-Teams bemühen sich doppelt, Untersuchungen durchzuführen.
- Der Wunsch nach neuen Funktionen führt dazu, dass mehrere Mitarbeiter umpositioniert werden, um an einem speziellen technischen Vorhaben zu arbeiten. Dadurch entstehende Lücken werden nicht aufgefüllt und die Problemlösungszeiten steigen. Diese Informationen werden nicht erfasst, und erst nach mehreren Wochen und viel negativem Feedback unzufriedener Benutzer wird die Unternehmensleitung auf das Problem aufmerksam.

Vorteile der Nutzung dieser bewährten Methode: Bei betrieblichen Ereignissen, die das Geschäft beeinträchtigen, wird manchmal viel Zeit und Energie damit verschwendet, Informationen von verschiedenen Teams abzufragen, die versuchen, die Situation zu verstehen. Durch die Einrichtung und Verbreitung von Statusseiten und Dashboards können Stakeholder rasch Informationen darüber abrufen, ob ein Problem festgestellt wurde oder nicht, wer mit der Lösung des Problems beschäftigt ist oder wann mit einer Rückkehr zum normalen Betrieb zu rechnen ist. Dadurch müssen die Teammitglieder nicht zu viel Zeit damit verbringen, anderen den Status mitzuteilen und haben mehr Zeit, Probleme zu lösen.

Darüber hinaus können Dashboards und Berichte Entscheidungsträgern und Stakeholdern Einblicke bieten, um zu sehen, wie Operations-Teams auf Geschäftsanforderungen reagieren können und wie ihre Ressourcen zugewiesen werden. Dies ist entscheidend, um festzustellen, ob angemessene Ressourcen zur Unterstützung des Unternehmens vorhanden sind.

## Risikostufe bei fehlender Befolgung dieser bewährten Methode: Mittel

### Implementierungsleitfaden

Erstellen Sie Dashboards, die die aktuellen Schlüsselmetriken für Ihre Operations-Teams anzeigen, und machen Sie sie sowohl für die Betriebsleitung als auch für das Management leicht zugänglich.

Erstellen Sie Statusseiten, die schnell aktualisiert werden können, um zu zeigen, wann sich ein Vorfall oder ein Ereignis abspielt, wer dafür verantwortlich ist und wer die Reaktion darauf koordiniert. Kommunizieren Sie auf dieser Seite alle Schritte oder Problemumgehungen, die Benutzer in Betracht ziehen sollten, und machen Sie sie für alle Beteiligten verfügbar. Bitten Sie Benutzer, zuerst diese Seite zu überprüfen, wenn sie mit einem unbekanntem Problem konfrontiert werden.

Erfassen Sie Daten und stellen Sie Berichte bereit, die den Zustand der Betriebsabläufe im Zeitverlauf aufzeigen, und verteilen Sie diese an Führungskräfte und Entscheidungsträger, um die Arbeit des Betriebs sowie die Herausforderungen und Bedürfnisse zu veranschaulichen.

Teilen Sie den Teams die Kennzahlen und Berichte mit, die die Ziele am besten widerspiegeln KPIs und wo sie den Wandel vorangetrieben haben. Nehmen Sie sich Zeit für diese Aktivitäten, um den Abläufen innerhalb und zwischen Teams mehr Bedeutung beizumessen.

### Ressourcen

#### Zugehörige Dokumente:

- [Fortschritt messen](#)
- [Erstellung von Dashboards für operative Sichtbarkeit](#)

#### Zugehörige Lösungen:

- [Datenoperationen](#)

## OPS09-BP03 Überprüfen Sie die Betriebskennzahlen und priorisieren Sie Verbesserungen

Durch die Bereitstellung von Zeit und Ressourcen für die Überprüfung des Betriebszustands wird sichergestellt, dass die day-to-day Betreuung des Geschäftsbereichs weiterhin Priorität hat. Bringen Sie Betriebsleiter und Stakeholder an einen Tisch, um regelmäßig Metriken zu überprüfen, Ziele und Vorgaben zu bestätigen oder zu ändern und Verbesserungen zu priorisieren.

### Gewünschtes Ergebnis:

- Betriebsleiter und Mitarbeiter treffen sich regelmäßig, um die Metriken für einen bestimmten Berichtszeitraum zu überprüfen. Herausforderungen werden kommuniziert, Erfolge gefeiert und gewonnene Erkenntnisse geteilt.
- Stakeholder und Unternehmensleiter werden regelmäßig über den Stand der Geschäftstätigkeit informiert und um Beiträge zu Zielen und future KPIs Initiativen gebeten. Kompromisse zwischen Servicebereitstellung, Betrieb und Wartung werden erörtert und in Zusammenhang gebracht.

#### Typische Anti-Muster:

- Ein neues Produkt wird auf den Markt gebracht, aber die Operations-Teams der Stufe 1 und 2 sind nicht ausreichend geschult, um Support zu leisten, oder bräuchten zusätzliches Personal. Metriken, die den Anstieg der Bearbeitungsdauer von Tickets und der Anzahl der Vorfälle belegen, werden von Führungskräften nicht berücksichtigt. Erst Wochen später werden Maßnahmen ergriffen, weil die Zahl der Abonnements zu sinken beginnt, da unzufriedene Benutzer die Plattform verlassen.
- Ein manuelles Verfahren zur Durchführung von Wartungsarbeiten an einer Workload gibt es schon lange. Der Wunsch nach Automatisierung war zwar vorhanden, hatte aber angesichts der geringen Bedeutung des Systems nur geringe Priorität. Im Laufe der Zeit hat das System jedoch an Bedeutung gewonnen und heute nehmen diese manuellen Prozesse einen Großteil der Betriebszeit in Anspruch. Es sind keine Ressourcen für die Bereitstellung von mehr Tools für den Betrieb vorgesehen, was zu einer Überlastung der Mitarbeiter führt, wenn die Workload zunimmt. Die Unternehmensleitung wird sich der Probleme bewusst, als sie erfährt, dass Mitarbeiter zu anderen Wettbewerbern wechseln.

Vorteile der Nutzung dieser bewährten Methode: In einigen Unternehmen kann es zu einer Herausforderung werden, für die Servicebereitstellung die gleiche Zeit und Aufmerksamkeit aufzuwenden, die neuen Produkten oder Angeboten entgegengebracht wird. Wenn dies zutrifft, kann der Geschäftsbereich darunter leiden und das erwartete Serviceniveau verschlechtert sich nach und nach. Dies liegt daran, dass sich der Betrieb nicht mit dem wachsenden Geschäft ändert und weiterentwickelt, wodurch er bald ins Hintertreffen gerät. Ohne eine regelmäßige Überprüfung der Erkenntnisse, die Operations erfasst, wird das Risiko für das Unternehmen möglicherweise erst sichtbar, wenn es zu spät ist. Wenn jedoch sowohl dem Betriebspersonal als auch den Führungskräften Zeit für die Überprüfung von Metriken und Verfahren eingeräumt wird, bleibt die entscheidende Rolle, die der Betrieb spielt, sichtbar und Risiken können erkannt werden, lange bevor sie ein kritisches Niveau erreichen. Operations-Teams erhalten einen besseren Überblick über bevorstehende Geschäftsänderungen und Initiativen, sodass proaktive Maßnahmen ergriffen werden können. Wenn Führungskräfte die Gelegenheit haben, die Betriebsmetriken zu prüfen, erkennen

sie, welche Rolle diese Teams für die Kundenzufriedenheit spielen –sowohl intern als auch extern. So können sie Operations die Möglichkeit geben, Entscheidungen im Hinblick auf Prioritäten besser abzuwägen oder sicherzustellen, dass die Teams über die Zeit und die Ressourcen verfügen, um mit neuen Geschäfts- und Workload-Initiativen zu wachsen und sich weiterzuentwickeln.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Mittel

### Implementierungsleitfaden

Nehmen Sie sich Zeit, um die Betriebsmetriken gemeinsam mit Stakeholdern und Operations-Teams zu überprüfen und die Berichtsdaten zu lesen. Stellen Sie diese Berichte in den Kontext der Ziele und Vorgaben der Organisation, um festzustellen, ob sie erreicht werden. Identifizieren Sie Unklarheiten, bei denen die Ziele nicht eindeutig sind oder wo Konflikte bestehen zwischen dem, was verlangt wird, und dem, was gegeben wird.

Identifizieren Sie, wo Zeit, Mitarbeiter und Tools zu Betriebsergebnissen beitragen können. Stellen Sie fest, welche Auswirkungen KPIs dies haben würde und welche Erfolgsziele angestrebt werden sollten. Greifen Sie Ihre Überlegungen regelmäßig wieder auf, um sicherzustellen, dass der Betrieb über ausreichende Ressourcen verfügt, um den Geschäftsbereich zu unterstützen.

### Ressourcen

Zugehörige Dokumente:

- [Amazon Athena](#)
- [Referenz zu CloudWatch Amazon-Kennzahlen und Dimensionen](#)
- [Amazon QuickSight](#)
- [AWS Glue](#)
- [AWS Glue Data Catalog](#)
- [Erfassen Sie mit dem Amazon Agent Metriken und Logs von EC2 CloudWatch Amazon-Instances und lokalen Servern](#)
- [Verwenden von CloudWatch Amazon-Metriken](#)

## OPS10. Wie bewältigen Sie Workload- und operationsspezifische Ereignisse?

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

### Bewährte Methoden



- [OPS10-BP01 Verwenden Sie einen Prozess für das Ereignis-, Vorfall- und Problemmanagement](#)
- [OPS10-BP02 Haben Sie einen Prozess pro Warnung](#)
- [OPS10-BP03 Priorisieren Sie betriebliche Ereignisse auf der Grundlage der Auswirkungen auf das Geschäft](#)
- [OPS10-BP04 Eskalationspfade definieren](#)
- [OPS10-BP05 Definieren Sie einen Kundenkommunikationsplan für Ereignisse, die sich auf den Service auswirken](#)
- [OPS10-BP06 Kommunizieren Sie den Status über Dashboards](#)
- [OPS10-BP07 Automatisieren Sie Reaktionen auf Ereignisse](#)

OPS10-BP01 Verwenden Sie einen Prozess für das Ereignis-, Vorfall- und Problemmanagement

Die Fähigkeit, Ereignisse, Vorfälle und Probleme effizient zu verwalten, ist der Schlüssel zur Aufrechterhaltung der Workload und der Leistung. Es ist wichtig, die Unterschiede zwischen diesen Elementen zu erkennen und zu verstehen, um eine effektive Reaktions- und Lösungsstrategie zu entwickeln. Die Einrichtung und Einhaltung eines klar definierten Prozesses für jeden Aspekt hilft Ihrem Team, alle auftretenden betrieblichen Herausforderungen schnell und effektiv zu bewältigen.

Gewünschtes Ergebnis: Ihr Unternehmen verwaltet betriebliche Ereignisse, Vorfälle und Probleme effektiv durch gut dokumentierte und zentral gespeicherte Prozesse. Diese Prozesse werden ständig aktualisiert, um Änderungen zu berücksichtigen, die Handhabung zu optimieren und eine hohe Servicezuverlässigkeit und Workload-Leistung aufrechtzuerhalten.

Typische Anti-Muster:

- Sie reagieren eher reaktiv als proaktiv auf Ereignisse.
- Bei verschiedenen Arten von Ereignissen oder Vorfällen werden inkonsistente Ansätze verfolgt.
- Ihr Unternehmen analysiert keine Vorfälle und lernt nicht aus ihnen, um zukünftige Vorfälle zu verhindern.

Vorteile der Nutzung dieser bewährten Methode:

- optimierte und standardisierte Reaktionsprozesse
- geringere Auswirkungen von Vorfällen auf Services und Kunden
- beschleunigte Problemlösung
- kontinuierliche Verbesserung der betrieblichen Abläufe

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Hoch

## Implementierungsleitfaden

Wenn Sie diese bewährte Methode implementieren, bedeutet dies, dass Sie Workload-Ereignisse nachverfolgen. Sie haben Prozesse für den Umgang mit Vorfällen und Problemen. Die Prozesse werden dokumentiert, geteilt und oft aktualisiert. Die Probleme werden identifiziert, priorisiert und behoben.

## Verstehen von Ereignissen, Vorfällen und Problemen

- **Ereignisse:** Bei einem Ereignis handelt es sich um eine Beobachtung einer Aktion, eines Vorkommens oder einer Statusänderung. Ereignisse können geplant oder ungeplant sein und sie können intern oder extern zur Workload entstehen.
- **Vorfälle:** Vorfälle sind Ereignisse, die eine Reaktion erfordern, wie ungeplante Unterbrechungen oder Beeinträchtigungen der Servicequalität. Sie stellen Störungen dar, die sofortige Aufmerksamkeit erfordern, um den normalen Workload-Betrieb wiederherzustellen.
- **Probleme:** Probleme sind die zugrundeliegenden Ursachen für einen oder mehrere Vorfälle. Bei der Identifizierung und Lösung von Problemen geht es darum, den Vorfällen auf den Grund zu gehen, um zukünftige Vorfälle zu verhindern.

## Implementierungsschritte

### Ereignisse

#### 1. Überwachen von Ereignissen:

- [Implementieren Sie Beobachtbarkeit](#) und [nutzen Sie Workload-Beobachtbarkeit](#).
- Überwachen Sie, dass Aktionen, die von einem Benutzer, einer Rolle oder einem AWS Dienst ausgeführt werden, als Ereignisse in aufgezeichnet werden. [AWS CloudTrail](#)
- Reagieren Sie mit [Amazon](#) in Echtzeit auf betriebliche Änderungen in Ihren Anwendungen EventBridge.
- Bewerten, überwachen und zeichnen Sie Änderungen der Ressourcenkonfiguration mit [AWS Config](#) kontinuierlich auf.

#### 2. Erstellen von Prozessen:

- Entwickeln Sie ein Verfahren zur Bewertung, welche Ereignisse signifikant sind und überwacht werden müssen. Dies beinhaltet die Festlegung von Schwellenwerten und Parametern für normale und abnormale Aktivitäten.

- Legen Sie Kriterien für die Eskalation eines Ereignisses in Bezug auf einen Vorfall fest. Dies kann auf Grundlage des Schweregrads, der Auswirkungen auf die Benutzer oder der Abweichung vom erwarteten Verhalten erfolgen.
- Überprüfen Sie regelmäßig die Prozesse zur Überwachung und Reaktion auf Ereignisse. Dazu gehören die Analyse früherer Vorfälle, die Anpassung von Schwellenwerten und die Verfeinerung von Warnmechanismen.

## Vorfälle

### 1. Reaktion auf Vorfälle:

- Nutzen Sie die Erkenntnisse aus den Tools zur Beobachtbarkeit, um Vorfälle schnell zu erkennen und darauf zu reagieren.
- Implementieren Sie [AWS Systems Manager Ops Center](#), um betriebliche Aufgaben und Vorfälle zu sammeln, zu organisieren und zu priorisieren.
- Nutzen Sie Dienste wie [Amazon CloudWatch](#) und [AWS X-Ray](#) für tiefere Analysen und Problembhebungen.
- Consider [AWS Managed Services \(AMS\)](#) bietet ein verbessertes Incident Management und nutzt die proaktiven, präventiven und detektiven Funktionen. AMS erweitert den betrieblichen Support um Dienste wie Überwachung, Erkennung und Reaktion auf Vorfälle sowie Sicherheitsmanagement.
- Kunden von Enterprise Support können [AWS -Vorfallerkennung und -reaktion](#) verwenden, wodurch eine kontinuierliche proaktive Überwachung und ein Vorfallmanagement für Produktions-Workloads ermöglicht wird.

### 2. Erstellen eines Vorfallmanagementprozesses:

- Richten Sie einen strukturierten Vorfallmanagementprozess ein, der klare Rollen, Kommunikationsprotokolle und Lösungsschritte umfasst.
- Integrieren Sie das Vorfallmanagement mit Tools wie [AWS Chatbot](#) für eine effiziente Reaktion und Koordination.
- Kategorisieren Sie Vorfälle nach Schweregrad mit vordefinierten [Vorfallreaktionsplänen](#) für jede Kategorie.

### 3. Lernen und Verbessern:

- Führen Sie [Analysen nach Vorfällen](#) aus, um die Grundursachen und die Effektivität der Lösung zu verstehen.

- Aktualisieren und verbessern Sie die Reaktionspläne kontinuierlich auf Grundlage von Überprüfungen und sich entwickelnden Praktiken.
- Dokumentieren Sie die gewonnenen Erkenntnisse und geben Sie sie an andere Teams weiter, um die betriebliche Widerstandsfähigkeit zu verbessern.
- Kunden mit Enterprise Support können den [Workshop zum Vorfallmanagement](#) bei ihrem Technical Account Manager anfordern. Dieser angeleitete Workshop testet Ihren vorhandenen Reaktionsplan für Vorfälle und hilft Ihnen, Verbesserungsmöglichkeiten zu identifizieren.

## Problems (Probleme)

### 1. Identifizieren von Problemen:

- Verwenden Sie Daten aus früheren Vorfällen, um wiederkehrende Muster zu erkennen, die auf tiefere systemische Probleme hinweisen könnten.
- Nutzen Sie Tools wie [AWS CloudTrail](#) und [Amazon CloudWatch](#), um Trends zu analysieren und grundlegende Probleme aufzudecken.
- Binden Sie funktionsübergreifende Teams ein, einschließlich Betriebs-, Entwicklungs- und Geschäftsbereiche, um unterschiedliche Sichtweisen auf die Grundursachen zu gewinnen.

### 2. Erstellen eines Problemmanagementprozesses:

- Entwickeln Sie einen strukturierten Prozess für das Problemmanagement, der sich auf langfristige Lösungen statt auf schnelle Lösungen konzentriert.
- Integrieren Sie Techniken zur Ursachenanalyse (RCA), um die zugrunde liegenden Ursachen von Vorfällen zu untersuchen und zu verstehen.
- Aktualisieren Sie Betriebsrichtlinien, Verfahren und Infrastruktur auf Grundlage der Erkenntnisse, um Wiederholungen zu verhindern.

### 3. Kontinuierliche Verbesserungen:

- Fördern Sie eine Kultur des ständigen Lernens und der Verbesserung und ermutigen Sie Ihre Teams, potenzielle Probleme proaktiv zu erkennen und anzugehen.
- Überprüfen und überarbeiten Sie regelmäßig die Problemmanagementprozesse und -tools, um sie an die sich entwickelnde Geschäfts- und Technologielandschaft anzupassen.
- Tauschen Sie Erkenntnisse und bewährte Methoden innerhalb des Unternehmens aus, um eine widerstandsfähigere und effizientere Betriebsumgebung zu schaffen.

### 4. Engagieren Sie sich AWS Support:

- Nutzen Sie AWS Support-Ressourcen, z. B. [AWS Trusted Advisor](#) für proaktive Beratung und Optimierungsempfehlungen.
- Kunden von Enterprise Support können auf spezielle Programme wie [AWS Countdown](#) zugreifen, um bei kritischen Ereignissen Unterstützung zu erhalten.

Aufwand für den Implementierungsplan: Mittel

Ressourcen

Zugehörige bewährte Methoden:

- [OPS04-BP01 Identifizieren Sie die wichtigsten Leistungsindikatoren](#)
- [OPS04-BP02 Implementieren Sie Anwendungstelemetrie](#)
- [OPS07-BP03 Verwenden Sie Runbooks, um Prozeduren durchzuführen](#)
- [OPS07-BP04 Verwenden Sie Playbooks, um Probleme zu untersuchen](#)
- [OPS08-BP01 Analysieren Sie Workload-Metriken](#)
- [OPS11-BP02 Führen Sie eine Analyse nach dem Vorfall durch](#)

Zugehörige Dokumente:

- [AWS Security Incident Response Guide](#)
- [AWS Erkennung und Reaktion auf Vorfälle](#)
- [AWS Framework für die Cloud-Einführung: Betriebsperspektive — Vorfall- und Problemmanagement](#)
- [Vorfallmanagement im Zeitalter von DevOps und SRE](#)
- [PagerDuty - Was ist Incident Management?](#)

Zugehörige Videos:

- [Die wichtigsten Tipps zur Reaktion auf Vorfälle von AWS](#)
- [AWS re:Invent 2022 — Die Amazon Builders' Library: 25 Jahre operative Exzellenz bei Amazon](#)
- [AWS re:Invent 2022 — AWS Erkennung und Reaktion auf Vorfälle \(01\) SUP2](#)
- [Wir stellen vor: Incident Manager von AWS Systems Manager](#)

## Zugehörige Beispiele:

- [AWS Proaktive Services — Workshop zum Incident-Management](#)
- [Wie automatisiert man die Reaktion auf Vorfälle mit PagerDuty und AWS Systems Manager Incident Manager](#)
- [Binden Sie Incident Responder mit den Bereitschaftszeitplänen in ein AWS Systems Manager Incident Manager](#)
- [Verbessern Sie die Sichtbarkeit und Zusammenarbeit bei der Bearbeitung von Vorfällen in AWS Systems Manager Incident Manager](#)
- [Berichte über Vorfälle und Serviceanfragen in AMS](#)

## Zugehörige Services:

- [Amazon EventBridge](#)

## OPS10-BP02 Haben Sie einen Prozess pro Warnung

Die Einrichtung eines klaren und definierten Prozesses für jede Warnmeldung in Ihrem System ist für ein effektives und effizientes Vorfalldmanagement unerlässlich. Diese Vorgehensweise stellt sicher, dass jede Warnmeldung zu einer spezifischen, umsetzbaren Reaktion führt, wodurch die Zuverlässigkeit und Reaktionsfähigkeit Ihrer Abläufe verbessert wird.

Gewünschtes Ergebnis: Jede Warnmeldung leitet einen bestimmten, genau definierten Reaktionsplan ein. Wenn möglich, werden die Antworten automatisiert, mit klaren Zuständigkeiten und einem definierten Eskalationspfad. Warnmeldungen sind mit einer up-to-date Wissensdatenbank verknüpft, sodass jeder Bediener konsistent und effektiv reagieren kann. Die Antworten sind schnell und einheitlich, was die betriebliche Effizienz und Zuverlässigkeit erhöht.

## Typische Anti-Muster:

- Für Warnmeldungen gibt es keinen vordefinierten Reaktionsprozess, was zu provisorischen und verzögerten Lösungen führt.
- Eine Überlastung mit Warnmeldungen führt dazu, dass wichtige Warnmeldungen übersehen werden.
- Warnmeldungen werden uneinheitlich gehandhabt, da es an klaren Zuständigkeiten und Verantwortlichkeiten mangelt.

Vorteile der Nutzung dieser bewährten Methode:

- Weniger Ermüdungserscheinungen, da nur umsetzbare Warnmeldungen ausgelöst werden.
- Verkürzte durchschnittliche Zeit bis zur Lösung betrieblicher Probleme (MTTR).
- Die durchschnittliche Zeit bis zur Untersuchung wurde verringert (MTTI), was zur Reduzierung beiträgt MTTR.
- Verbesserte Fähigkeit, operative Reaktionen zu skalieren.
- Verbesserte Konsistenz und Zuverlässigkeit bei der Behandlung von Betriebsereignissen.

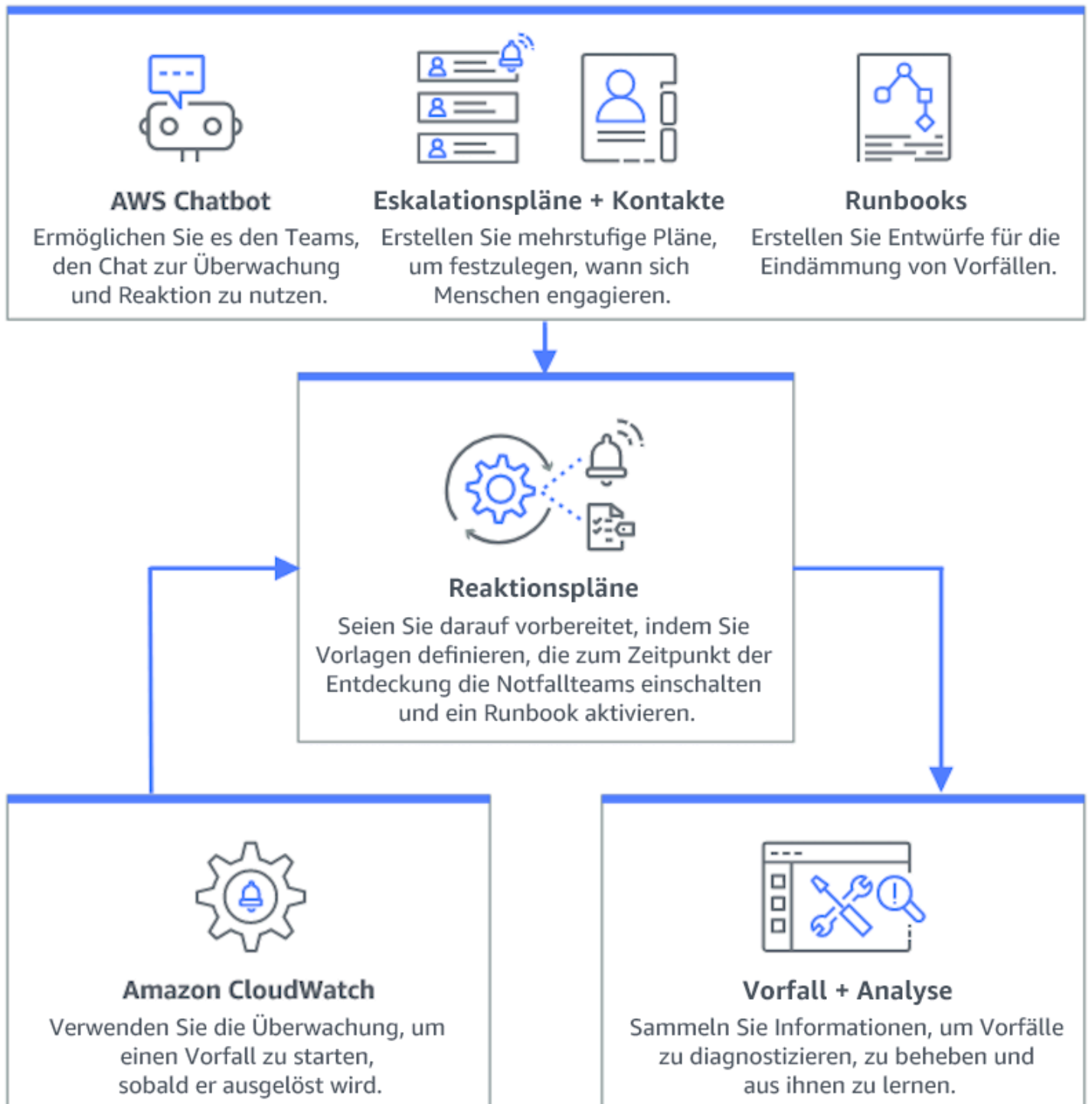
Risikostufe bei fehlender Befolgung dieser bewährten Methode: Hoch

Implementierungsleitfaden

Ein Prozess pro Warnmeldung beinhaltet die Erstellung eines klaren Reaktionsplans für jede Warnmeldung, die Automatisierung von Reaktionen (soweit dies möglich ist) und die kontinuierliche Optimierung dieser Prozesse auf Grundlage des betrieblichen Feedbacks und der sich entwickelnden Anforderungen.

Implementierungsschritte

Das folgende Diagramm veranschaulicht den Arbeitsablauf für das Vorfalmanagement in [AWS Systems Manager Incident Manager](#). Es wurde entwickelt, um schnell auf betriebliche Probleme zu reagieren, indem es automatisch Vorfälle als Reaktion auf bestimmte Ereignisse von Amazon CloudWatch oder Amazon erstellt. EventBridge Wenn ein Vorfall entweder automatisch oder manuell erstellt wird, zentralisiert Incident Manager die Verwaltung des Vorfalls, organisiert relevante AWS Ressourceninformationen und initiiert vordefinierte Reaktionspläne. Dazu gehören die Ausführung von Systems Manager Automation-Runbooks für sofortige Aktionen sowie die Erstellung eines übergeordneten operativen Arbeitselements OpsCenter zur Nachverfolgung verwandter Aufgaben und Analysen. Dieser optimierte Prozess beschleunigt und koordiniert die Reaktion auf Vorfälle in Ihrer AWS gesamten Umgebung.



1. Verwenden Sie zusammengesetzte Alarme: Erstellen Sie [zusammengesetzte Alarme](#), CloudWatch um zusammengehörige Alarme zu gruppieren. Dadurch werden Störgeräusche reduziert und aussagekräftigere Reaktionen ermöglicht.



2. Integrieren Sie CloudWatch Amazon-Alarme in Incident Manager. Konfigurieren Sie CloudWatch Alarme, um automatisch Vorfälle in zu erstellen [AWS Systems Manager Incident Manager](#).
3. Integrieren Sie Amazon EventBridge mit Incident Manager: Erstellen Sie [EventBridge Regeln](#), um auf Ereignisse zu reagieren, und erstellen Sie Vorfälle mithilfe definierter Reaktionspläne.
4. Vorbereitung auf Vorfälle in Incident Manager:
  - Richten Sie in Incident Manager detaillierte [Reaktionspläne](#) für jede Art von Warnmeldung ein.
  - Richten Sie über [AWS Chatbot](#) Chat-Kanäle ein, die mit Reaktionsplänen in Incident Manager verknüpft sind und die Echtzeitkommunikation bei Vorfällen über Plattformen wie Slack, Microsoft Teams und Amazon Chime ermöglichen.
  - Integrieren Sie [Systems-Manager-Automation-Runbooks](#) in Incident Manager, um automatisierte Reaktionen auf Vorfälle zu ermöglichen.

## Ressourcen

### Zugehörige bewährte Methoden:

- [OPS04-BP01 Identifizieren Sie die wichtigsten Leistungsindikatoren](#)
- [OPS08-BP04 Erstellen Sie umsetzbare Benachrichtigungen](#)

### Zugehörige Dokumente:

- [AWS Framework für die Cloud-Einführung: Betriebsperspektive — Vorfall- und Problemmanagement](#)
- [CloudWatch Amazon-Alarme verwenden](#)
- [Einrichtung AWS Systems Manager Incident Manager](#)
- [Preparing for incidents in Incident Manager](#)

### Zugehörige Videos:

- [Die wichtigsten Tipps zur Reaktion auf Vorfälle von AWS](#)

### Zugehörige Beispiele:

- [AWS Workshops — AWS Systems Manager Incident Manager — Automatisieren Sie die Reaktion auf Sicherheitsvorfälle](#)

## OPS10-BP03 Priorisieren Sie betriebliche Ereignisse auf der Grundlage der Auswirkungen auf das Geschäft

Eine schnelle Reaktion auf Betriebsereignisse ist von entscheidender Bedeutung, aber nicht alle Ereignisse sind gleich. Wenn Sie Ihre Prioritäten auf Grundlage der geschäftlichen Auswirkungen festlegen, müssen Sie sich auch vorrangig mit Ereignissen befassen, die erhebliche Folgen haben könnten, wie z. B. Sicherheit, finanzielle Verluste, Verstöße gegen Vorschriften oder Rufschädigung.

Gewünschtes Ergebnis: Die Reaktionen auf betriebliche Ereignisse werden auf Grundlage der potenziellen Auswirkungen auf die Geschäftsabläufe und -ziele priorisiert. Dadurch werden die Reaktionen effizient und effektiv.

### Typische Anti-Muster:

- Jedes Ereignis wird mit der gleichen Dringlichkeit behandelt, was zu Verwirrung und Verzögerungen bei der Behandlung kritischer Probleme führt.
- Sie unterscheiden nicht zwischen Ereignissen mit hoher und geringer Auswirkung, was zu einer Fehlallokation von Ressourcen führt.
- Ihrem Unternehmen fehlt ein klarer Rahmen für die Priorisierung, was zu inkonsistenten Reaktionen auf Betriebsereignisse führt.
- Ereignisse werden in der Reihenfolge ihrer Meldung priorisiert und nicht nach ihrer Auswirkung auf die Geschäftsergebnisse.

### Vorteile der Nutzung dieser bewährten Methode:

- Stellt sicher, dass wichtige Geschäftsfunktionen zuerst berücksichtigt werden, um mögliche Schäden zu minimieren.
- Verbessert die Ressourcenzuweisung bei mehreren gleichzeitigen Ereignissen.
- Verbessert die Fähigkeit der Organisation, das Vertrauen zu erhalten und die gesetzlichen Anforderungen zu erfüllen.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Hoch

### Implementierungsleitfaden

Wenn Sie mit mehreren betrieblichen Ereignissen konfrontiert sind, ist ein strukturierter Ansatz zur Priorisierung auf Grundlage von Auswirkungen und Dringlichkeit unerlässlich. Dieser Ansatz hilft

Ihnen, fundierte Entscheidungen zu treffen, Ihre Maßnahmen auf die Bereiche zu lenken, wo sie am dringendsten benötigt werden, und das Risiko für die Geschäftskontinuität zu mindern.

### Implementierungsschritte

1. Bewertung von Auswirkungen: Entwickeln Sie ein Klassifizierungssystem, um den Schweregrad von Ereignissen im Hinblick auf ihre potenziellen Auswirkungen auf den Geschäftsbetrieb und die Ziele zu bewerten. Das folgende Beispiel zeigt die Wirkungskategorien:

Auswirkungsgrad	Beschreibung
Hoch	Betrifft viele Mitarbeiter oder Kunden, hohe finanzielle Auswirkungen, hoher Reputationsschaden oder Verletzungen
Mittelschwer	Betrifft eine Gruppe von Mitarbeitern oder Kunden, mäßige finanzielle Auswirkungen oder mäßiger Reputationsschaden
Niedrig	Betrifft einzelne Mitarbeiter oder Kunden, geringe finanzielle Auswirkungen oder geringer Reputationsschaden

2. Beurteilen Sie die Dringlichkeit: Definieren Sie Dringlichkeitsstufen dafür, wie schnell auf ein Ereignis reagiert werden muss, und berücksichtigen Sie dabei Faktoren wie Sicherheit, finanzielle Auswirkungen und Leistungsvereinbarungen (SLAs). Das folgende Beispiel zeigt die Dringlichkeitskategorien:

Dringlichkeitsstufe	Beschreibung
Hoch	Exponentiell steigender Schaden, Beeinträchtigung zeitkritischer Aufgaben, drohende Eskalation oder betroffene Benutzer oder Gruppen. VIP
Mittelschwer	Der Schaden nimmt im Laufe der Zeit zu, oder es sind einzelne VIP Benutzer oder Gruppen betroffen.

Dringlichkeitsstufe	Beschreibung
Niedrig	Der geringfügige Schaden nimmt im Laufe der Zeit zu, oder die non-time-sensitive Arbeit wird beeinträchtigt.

### 3. Erstellen einer Priorisierungsmatrix:

- Verwenden Sie eine Matrix, um Auswirkungen und Dringlichkeit miteinander zu vergleichen, und weisen Sie verschiedenen Kombinationen Prioritätsstufen zu.
- Machen Sie die Matrix allen Teammitgliedern, die für die Reaktion auf betriebliche Ereignisse verantwortlich sind, zugänglich und verständlich.
- Die folgende Beispielmatrix zeigt den Schweregrad eines Vorfalls nach Dringlichkeit und Auswirkung an:

Dringlichkeit und Auswirkungen	Hoch	Mittelschwer	Niedrig
Hoch	Kritisch	Dringend	Hoch
Mittelschwer	Dringend	Hoch	Normal
Niedrig	Hoch	Normal	Niedrig

### 4. Trainieren und Kommunizieren: Schulen Sie die Response-Teams im Umgang mit der Prioritätenmatrix und der Wichtigkeit, diese während eines Ereignisses zu befolgen. Kommunizieren Sie den Priorisierungsprozess an alle Stakeholder, um klare Erwartungen zu schaffen.

### 5. Integration der Vorfalldreaktion:

- Integrieren Sie die Priorisierungsmatrix in Ihre Pläne und Tools zur Reaktion auf Vorfälle.
- Automatisieren Sie nach Möglichkeit die Klassifizierung und Priorisierung von Ereignissen, um die Reaktionszeiten zu verkürzen.
- Kunden von Enterprise Support können [AWS -Vorfallerkennung und -reaktion](#) nutzen, wodurch eine proaktive Überwachung rund um die Uhr und ein Vorfalldmanagement für Produktions-Workloads ermöglicht wird.

6. Überprüfen und Anpassen: Überprüfen Sie regelmäßig die Effektivität des Priorisierungsprozesses und nehmen Sie Anpassungen auf der Grundlage von Rückmeldungen und Änderungen im Geschäftsumfeld vor.

## Ressourcen

Zugehörige bewährte Methoden:

- [OPS03-BP03 Eskalation wird gefördert](#)
- [OPS08-BP04 Erstellen Sie umsetzbare Benachrichtigungen](#)
- [OPS09-BP01 Betriebsziele messen und mit Kennzahlen KPIs](#)

Zugehörige Dokumente:

- [Atlassian – Verständnis der Schweregrade von Vorfällen](#)
- [IT-Prozessplan – Checkliste der Vorfallopriorität](#)

## OPS10-BP04 Eskalationspfade definieren

Legen Sie in Ihren Protokollen zur Vorfallobreaktion klare Eskalationspfade fest, um rechtzeitige und effektive Maßnahmen zu ermöglichen. Dazu gehören die Angabe von Aufforderungen zur Eskalation, die detaillierte Beschreibung des Eskalationsprozesses und die vorherige Genehmigung von Maßnahmen zur Beschleunigung der Entscheidungsfindung und zur Verkürzung der mittleren Lösungszeit (M). MTTR

Gewünschtes Ergebnis: Ein strukturierter und effizienter Prozess, der Vorfälle an das entsprechende Personal weiterleitet und so die Reaktionszeiten und Auswirkungen minimiert.

Typische Anti-Muster:

- Mangelnde Klarheit über die Wiederherstellungsverfahren führt zu provisorischen Maßnahmen bei kritischen Vorfällen.
- Das Fehlen von definierten Berechtigungen und Zuständigkeiten führt zu Verzögerungen, wenn dringende Maßnahmen erforderlich sind.
- Stakeholder und Kunden werden nicht erwartungsgemäß informiert.
- Wichtige Entscheidungen verzögern sich.

## Vorteile der Nutzung dieser bewährten Methode:

- Optimierte Reaktion auf Vorfälle durch vordefinierte Eskalationsverfahren.
- Reduzierte Ausfallzeiten durch vorab genehmigte Maßnahmen und klare Zuständigkeiten.
- Verbesserte Ressourcenzuweisung und Anpassung der Support-Ebene an den Schweregrad des Vorfalls.
- Verbesserte Kommunikation mit Stakeholdern und Kunden.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Mittel

## Implementierungsleitfaden

Richtig definierte Eskalationspfade sind für eine schnelle Reaktion auf Vorfälle von entscheidender Bedeutung. AWS Systems Manager Incident Manager unterstützt die Erstellung strukturierter Eskalations- und Bereitschaftspläne, die das richtige Personal benachrichtigen, sodass es bei Vorfällen sofort reagieren kann.

## Implementierungsschritte

1. Eskalationsaufforderungen einrichten: Richten Sie [CloudWatch Alarme ein, um einen Vorfall](#) in zu verursachen. [AWS Systems Manager Incident Manager](#)
2. Erstellen von Bereitschaftsplänen: Erstellen Sie [Bereitschaftspläne](#) in Incident Manager, die auf Ihre Eskalationspfade abgestimmt sind. Statten Sie das Bereitschaftspersonal mit den erforderlichen Berechtigungen und Tools aus, um schnell handeln zu können.
3. Detaillierte Eskalationsverfahren:
  - Legen Sie bestimmte Bedingungen fest, unter denen ein Vorfall eskaliert werden sollte.
  - Erstellen Sie [Eskalationspläne](#) in Incident Manager.
  - Eskalationskanäle sollten aus einem Ansprechpartner oder einem Bereitschaftsplan bestehen.
  - Definieren Sie die Rollen und Verantwortlichkeiten des Teams auf jeder Eskalationsstufe.
4. Genehmigung von Schadensbegrenzungsmaßnahmen im Voraus: Arbeiten Sie mit Entscheidungsträgern zusammen, um Maßnahmen für erwartete Szenarien vorab zu genehmigen. Verwenden Sie die in Incident Manager integrierten [Systems-Manager-Automation-Runbooks](#), um die Behebung von Vorfällen zu beschleunigen.
5. Angabe der Zuständigkeit: Identifizieren Sie eindeutig die internen Besitzer für jeden Schritt des Eskalationspfads.

## 6. Details zu Eskalationen mit Drittanbietern:

- Dokumentieren Sie Service-Level-Vereinbarungen mit Drittanbietern (SLAs) und stimmen Sie sie mit internen Zielen ab.
- Legen Sie klare Protokolle für die Lieferantenkommunikation bei Vorfällen fest.
- Integrieren Sie Lieferantenkontakte in die Tools zum Vorfallmanagement, um direkten Zugriff zu erhalten.
- Führen Sie regelmäßige Übungen durch, die Reaktionsszenarien von Drittanbietern beinhalten.
- Sorgen Sie dafür, dass die Informationen zur Lieferanteneskalation gut dokumentiert und leicht zugänglich sind.

7. Trainieren und Testen von Eskalationsplänen: Schulen Sie Ihr Team im Eskalationsprozess und führen Sie regelmäßig Übungen zur Reaktion auf Vorfälle oder den Ernstfall durch. Kunden mit Enterprise Support können einen [Workshop zum Vorfallmanagement](#) anfordern.

8. Weitere Verbesserung: Überprüfen Sie regelmäßig die Wirksamkeit Ihrer Eskalationspfade. Aktualisieren Sie Ihre Prozesse auf Grundlage der Erkenntnisse aus den Nachuntersuchungen von Vorfällen und dem kontinuierlichen Feedback.

Aufwand für den Implementierungsplan: Mittel

Ressourcen

Zugehörige bewährte Methoden:

- [OPS08-BP04 Erstellen Sie umsetzbare Benachrichtigungen](#)
- [OPS10-BP02 Haben Sie einen Prozess pro Warnung](#)
- [OPS11-BP02 Führen Sie eine Analyse nach dem Vorfall durch](#)

Zugehörige Dokumente:

- [AWS Systems Manager Incident Manager Eskalationspläne](#)
- [Working with on-call schedules in Incident Manager](#)
- [Erstellen und Verwalten von Runbooks](#)
- [Temporäres Management erhöhter Zugriffe mit AWS IAM Identity Center](#)
- [Atlassian – Eskalationsrichtlinien für effektives Vorfallmanagement](#)

## OPS10-BP05 Definieren Sie einen Kundenkommunikationsplan für Ereignisse, die sich auf den Service auswirken

Eine effektive Kommunikation bei Ereignissen, die sich auf den Service auswirken, ist entscheidend, um das Vertrauen und die Transparenz gegenüber den Kunden aufrechtzuerhalten. Ein klar definierter Kommunikationsplan hilft Ihrem Unternehmen, bei Vorfällen schnell und klar Informationen sowohl intern als auch extern auszutauschen.

### Gewünschtes Ergebnis:

- Ein robuster Kommunikationsplan, der Kunden und Stakeholder bei Ereignissen, die sich auf den Service auswirken, effektiv informiert.
- Transparenz in der Kommunikation, um Vertrauen aufzubauen und Ängste der Kunden abzubauen.
- Minimierung der Auswirkungen von Ereignissen, die sich auf den Service in Bezug auf das Kundenerlebnis und den Geschäftsbetrieb auswirken.

### Typische Anti-Muster:

- Eine unzureichende oder verzögerte Kommunikation führt zu Verwirrung und Unzufriedenheit der Kunden.
- Allzu technische oder vage Nachrichten vermitteln nicht die tatsächlichen Auswirkungen auf die Benutzer.
- Es gibt keine vordefinierte Kommunikationsstrategie, was zu inkonsistenten und reaktiven Nachrichten führt.

### Vorteile der Nutzung dieser bewährten Methode:

- Mehr Vertrauen und Zufriedenheit bei den Kunden durch proaktive und klare Kommunikation.
- Entlastung der Support-Teams durch präventive Behandlung von Kundenanliegen.
- Verbesserte Fähigkeit, Vorfälle effektiv zu verwalten und zu bewältigen.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Mittel

### Implementierungsleitfaden

Die Erstellung eines umfassenden Kommunikationsplans für Ereignisse, die sich auf den Service auswirken, umfasst mehrere Facetten, von der Auswahl der richtigen Kanäle bis hin zur



Formulierung der Botschaft und des Tonfalls. Der Plan sollte anpassungsfähig und skalierbar sein und verschiedene Ausfallszenarien berücksichtigen.

## Implementierungsschritte

### 1. Definieren von Rollen und Zuständigkeiten:

- Beauftragen Sie einen Hauptzuständigen für die Vorfallreaktion mit der Überwachung der Maßnahmen.
- Benennen Sie einen Kommunikationsmanager, der für die Koordination der gesamten externen und internen Kommunikation verantwortlich ist.
- Beziehen Sie den Support-Manager ein, um eine konsistente Kommunikation über Support-Tickets zu gewährleisten.

2. Identifizieren Sie Kommunikationskanäle: Wählen Sie Kanäle wie Chat am Arbeitsplatz, E-Mail, soziale MedienSMS, In-App-Benachrichtigungen und Statusseiten aus. Diese Kanäle sollten robust und in der Lage sein, bei Ereignissen, die den Service beeinträchtigen, unabhängig zu arbeiten.

### 3. Schnelle, klare und regelmäßige Kommunikation mit Kunden:

- Entwickeln Sie Vorlagen für verschiedene Szenarien, bei denen Beeinträchtigungen des Serviceangebots vorliegen, und achten Sie dabei auf Einfachheit und wichtige Details. Fügen Sie Informationen über die Beeinträchtigung des Services, die erwartete Lösungszeit und die Auswirkungen hinzu.
- Verwenden Sie Amazon Pinpoint, um Kunden mithilfe von Push-Benachrichtigungen, In-App-Benachrichtigungen, E-Mails, Textnachrichten, Sprachnachrichten und Nachrichten über benutzerdefinierte Kanäle zu informieren.
- Verwenden Sie Amazon Simple Notification Service (AmazonSNS), um Abonnenten programmatisch oder per E-Mail, mobilen Push-Benachrichtigungen und Textnachrichten zu benachrichtigen.
- Kommunizieren Sie den Status über Dashboards, indem Sie ein CloudWatch Amazon-Dashboard öffentlich teilen.
- Förderung des Engagements in den sozialen Medien:
  - Verfolgen Sie aktiv die sozialen Medien, um die Stimmung der Kunden zu verstehen.
  - Posten Sie auf Social-Media-Plattformen, um die Öffentlichkeit auf dem Laufenden zu halten und die Community einzubeziehen.
  - Bereiten Sie Vorlagen für eine konsistente und klare Kommunikation in den sozialen Medien vor.

4. Koordinieren Sie die interne Kommunikation: Implementieren Sie interne Protokolle mithilfe von Tools wie AWS Chatbot Teamkoordination und Kommunikation. Verwenden Sie CloudWatch Dashboards, um den Status zu kommunizieren.
5. Organisation der Kommunikation mit speziellen Tools und Services:
  - Verwenden Sie AWS Systems Manager Incident Manager with AWS Chatbot , um spezielle Chat-Kanäle für die interne Kommunikation und Koordination bei Vorfällen in Echtzeit einzurichten.
  - Verwenden Sie AWS Systems Manager Incident Manager Runbooks, um Kundenbenachrichtigungen über Amazon PinpointSNS, Amazon oder Tools von Drittanbietern wie Social-Media-Plattformen bei Vorfällen zu automatisieren.
  - Integrieren Sie Genehmigungs-Workflows in Runbooks, um optional die gesamte externe Kommunikation vor dem Versand zu überprüfen und zu autorisieren.
6. Praktizieren und verbessern:
  - Führen Sie Trainingkurse zum Einsatz von Kommunikationsmitteln und -strategien durch. Ermöglichen Sie es Teams, bei Vorfällen rechtzeitig Entscheidungen zu treffen.
  - Testen Sie den Kommunikationsplan durch regelmäßige Übungen oder Ernstfallübungen. Mithilfe dieser Tests können Sie Ihre Botschaften präzisieren und die Effektivität der Kanäle bewerten.
  - Implementieren Sie Feedback-Mechanismen, um die Effektivität der Kommunikation bei Vorfällen zu bewerten. Entwickeln Sie den Kommunikationsplan auf Grundlage des Feedbacks und der sich ändernden Bedürfnisse kontinuierlich weiter.

Aufwand für den Implementierungsplan: Hoch

Ressourcen

Zugehörige bewährte Methoden:

- [OPS07-BP03 Verwenden Sie Runbooks, um Prozeduren durchzuführen](#)
- [OPS10-BP06 Kommunizieren Sie den Status über Dashboards](#)
- [OPS11-BP02 Führen Sie eine Analyse nach dem Vorfall durch](#)

Zugehörige Dokumente:

- [Atlassian – Bewährte Methoden der Kommunikation bei Vorfällen](#)

- [Atlassian – Verfassen eines guten Status-Updates](#)
- [PagerDuty - Ein Leitfaden zur Kommunikation bei Vorfällen](#)

Zugehörige Videos:

- [Atlassian – Erstellung eines eigenen Kommunikationsplans für Vorfälle: Vorlagen für Zwischenfälle](#)

Zugehörige Beispiele:

- [AWS Health Armaturenbrett](#)
- [Beispiel für AWS Statusaktualisierungen](#)

OPS10-BP06 Kommunizieren Sie den Status über Dashboards

Verwenden Sie Dashboards als strategisches Werkzeug, um den Betriebsstatus und wichtige Metriken in Echtzeit an verschiedene Zielgruppen zu vermitteln, darunter interne technische Teams, Führungskräfte und Kunden. Diese Dashboards bieten eine zentrale, visuelle Darstellung des Systemzustands und der Geschäftsleistung und erhöhen so die Transparenz und die Effizienz der Entscheidungsfindung.

Gewünschtes Ergebnis:

- Ihre Dashboards bieten einen umfassenden Überblick über das System und die Geschäftskennzahlen, die für verschiedene Stakeholder relevant sind.
- Stakeholder können proaktiv auf Betriebsinformationen zugreifen, sodass keine häufigen Statusanfragen mehr erforderlich sind.
- Die Entscheidungsfindung in Echtzeit wird während des normalen Betriebs und bei Vorfällen verbessert.

Typische Anti-Muster:

- Techniker, die an einem Vorfalldialog teilnehmen, benötigen Statusaktualisierungen, um sich auf dem Laufenden zu halten.
- Sie verlassen sich auf die manuelle Berichterstattung für das Management, was zu Verzögerungen und möglichen Ungenauigkeiten führt.
- Die Arbeit der Operations-Teams wird bei Vorfällen häufig für Statusaktualisierungen unterbrochen.

## Vorteile der Nutzung dieser bewährten Methode:

- Ermöglicht Stakeholdern den sofortigen Zugriff auf wichtige Informationen und fördert so fundierte Entscheidungen.
- Reduziert betriebliche Ineffizienzen, indem manuelle Berichte und häufige Statusabfragen minimiert werden.
- Erhöht die Transparenz und das Vertrauen durch Echtzeiteinblicke in die Systemleistung und Geschäftskennzahlen.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Mittel

## Implementierungsleitfaden

Dashboards vermitteln effektiv den Status Ihrer Systeme und Geschäftskennzahlen und können auf die Bedürfnisse verschiedener Zielgruppen zugeschnitten werden. Tools wie Amazon CloudWatch Dashboards und Amazon QuickSight helfen Ihnen dabei, interaktive Echtzeit-Dashboards für Systemüberwachung und Business Intelligence zu erstellen.

## Implementierungsschritte

1. Ermittlung der Bedürfnisse der Stakeholder: Ermitteln Sie den spezifischen Informationsbedarf verschiedener Zielgruppen, z. B. technische Teams, Führungskräfte und Kunden.
2. Wählen Sie die richtigen Tools: Wählen Sie geeignete Tools wie [CloudWatch Amazon-Dashboards](#) für die Systemüberwachung und [Amazon QuickSight](#) für interaktive Business Intelligence.
3. Entwicklung effektiver Dashboards:
  - Gestalten Sie Dashboards, um relevante Kennzahlen übersichtlich darzustellen und sicherzustellen, dass sie verständlich und umsetzbar sind.
  - Integrieren Sie bei Bedarf Ansichten auf System- und Unternehmensebene.
  - Inkludieren Sie sowohl Dashboards auf hoher Ebene (für umfassende Übersichten) als auch auf niedriger Ebene (für detaillierte Analysen).
  - Integrieren Sie automatische Alarme in Dashboards, um kritische Probleme hervorzuheben.
  - Kommentieren Sie Dashboards mit wichtigen Schwellenwerten und Zielen für Metriken für sofortige Sichtbarkeit.
4. Integration von Datenquellen:

- Verwenden Sie [Amazon CloudWatch](#), um Metriken aus verschiedenen AWS Diensten zu aggregieren und anzuzeigen und [Metriken aus anderen Datenquellen abzufragen](#). So erhalten Sie einen einheitlichen Überblick über den Zustand und die Geschäftskennzahlen Ihres Systems.
  - Verwenden Sie Funktionen wie [CloudWatch Logs Insights](#), um Protokolldaten aus verschiedenen Anwendungen und Diensten abzufragen und zu visualisieren.
5. Bereitstellung von Selfservice-Zugriff:
- Teilen Sie CloudWatch Dashboards mit relevanten Stakeholdern für den Self-Service-Zugriff auf Informationen mithilfe von Funktionen zum [Teilen von Dashboards](#).
  - Stellen Sie sicher, dass Dashboards leicht zugänglich sind und Informationen in Echtzeit bereitstellen. up-to-date
6. Regelmäßige Aktualisierungen und Verbesserungen:
- Aktualisieren und verbessern Sie die Dashboards kontinuierlich, um sie an die sich entwickelnden Geschäftsanforderungen und das Feedback der Stakeholder anzupassen.
  - Überprüfen Sie die Dashboards regelmäßig, um sicherzustellen, dass sie relevant und effektiv sind, um die erforderlichen Informationen zu vermitteln.

## Ressourcen

### Zugehörige bewährte Methoden:

- [OPS08-BP05 Dashboards erstellen](#)

### Zugehörige Dokumente:

- [Erstellung von Dashboards für operative Sichtbarkeit](#)
- [Verwenden von CloudWatch Amazon-Dashboards](#)
- [Flexible Dashboards mit Dashboard-Variablen erstellen](#)
- [Dashboards teilen CloudWatch](#)
- [Metriken aus anderen Datenquellen abfragen](#)
- [Fügen Sie einem Dashboard ein benutzerdefiniertes Widget hinzu CloudWatch](#)

### Zugehörige Beispiele:

- [Workshop zur Beobachtbarkeit – Dashboards](#)

## OPS10-BP07 Automatisieren Sie Reaktionen auf Ereignisse

Die Automatisierung von Reaktionen auf Ereignisse ist der Schlüssel für eine schnelle, konsistente und fehlerfreie operative Abwicklung. Erstellen Sie optimierte Prozesse und verwenden Sie Tools, um Ereignisse automatisch zu verwalten und darauf zu reagieren, um manuelle Eingriffe zu minimieren und die betriebliche Effizienz zu steigern.

### Gewünschtes Ergebnis:

- weniger menschliche Fehler und schnellere Lösungszeiten durch Automatisierung
- konsistente und zuverlässige Handhabung betrieblicher Ereignisse
- verbesserte betriebliche Effizienz und Systemzuverlässigkeit

### Typische Anti-Muster:

- Die manuelle Behandlung von Ereignissen führt zu Verzögerungen und Fehlern.
- Bei sich wiederholenden, kritischen Aufgaben wird die Automatisierung übersehen.
- Sich wiederholende, manuelle Aufgaben führen zu Ermüdungserscheinungen und zum Übersehen kritischer Probleme.

### Vorteile der Nutzung dieser bewährten Methode:

- beschleunigte Reaktionen auf Ereignisse, wodurch sich die Ausfallzeiten des Systems reduzieren
- zuverlässiger Betrieb mit automatisierter und konsistenter Ereignisbehandlung

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Mittel

### Implementierungsleitfaden

Integrieren Sie Automatisierung, um effiziente Arbeitsabläufe zu schaffen und manuelle Eingriffe zu minimieren.

## Implementierungsschritte

1. Identifizieren von Möglichkeiten zur Automatisierung: Bestimmen Sie sich wiederholende Aufgaben für die Automatisierung, wie beispielsweise Problembehebung, Ticketverbesserung, Kapazitätsmanagement, Skalierung, Bereitstellung und Tests.
2. Identifizieren von Automatisierungsaufforderungen:
  - Beurteilen und definieren Sie spezifische Bedingungen oder Kennzahlen, die automatische Reaktionen mithilfe von [CloudWatch Amazon-Alarmaktionen auslösen](#).
  - Verwenden Sie [Amazon EventBridge](#), um auf Ereignisse in AWS Services, benutzerdefinierten Workloads und SaaS-Anwendungen zu reagieren.
  - Berücksichtigen Sie Initiierungsereignisse wie [bestimmte Protokolleinträge](#), [Schwellenwerte für Leistungskennzahlen](#) oder [Statusänderungen](#) AWS von Ressourcen.
3. Implementieren der ereignisgesteuerten Automatisierung:
  - Verwenden Sie AWS Systems Manager Automation-Runbooks, um Wartungs-, Bereitstellungs- und Problembehebungsaufgaben zu vereinfachen.
  - [Beim Erstellen von Vorfällen in Incident Manager](#) werden automatisch Details zu den beteiligten AWS Ressourcen gesammelt und dem Vorfall hinzugefügt.
  - Überwachen Sie Kontingente proaktiv mit [Quota Monitor for AWS](#).
  - Passen Sie die Kapazität mit [AWS Auto Scaling](#) automatisch an, um Verfügbarkeit und Leistung aufrechtzuerhalten.
  - Automatisieren Sie Entwicklungspipelines mit [Amazon CodeCatalyst](#).
  - Testen Sie die Endgeräte oder überwachen Sie sie kontinuierlich und APIs [verwenden Sie synthetische](#) Überwachung.
4. Schadensbegrenzung durch Automatisierung:
  - Implementieren Sie [automatisierte Sicherheitsmaßnahmen](#), um schnell auf Risiken zu reagieren.
  - Verwenden Sie [State Manager von AWS Systems Manager](#), um Konfigurationsabweichungen zu reduzieren.
  - [Korrigieren Sie Ressourcen, die nicht den Vorschriften entsprechen](#), mit AWS-Config-Regeln

Aufwand für den Implementierungsplan: Hoch

Ressourcen

Zugehörige bewährte Methoden:

Betrieb

- [OPS08-BP04 Erstellen Sie umsetzbare Benachrichtigungen](#)
- [OPS10-BP02 Haben Sie einen Prozess pro Warnung](#)

#### Zugehörige Dokumente:

- [Verwendung von Systems-Manager-Automation-Runbooks mit Incident Manager](#)
- [Erstellen von Vorfällen in Incident Manager](#)
- [AWS Servicekontingenten](#)
- [Überwachen der Ressourcennutzung und Senden von Benachrichtigungen, wenn das Kontingent fast erreicht ist](#)
- [AWS Auto Scaling](#)
- [Was ist Amazon CodeCatalyst?](#)
- [CloudWatch Amazon-Alarme verwenden](#)
- [CloudWatch Amazon-Alarmaktionen verwenden](#)
- [Behebung nicht konformer Ressourcen mit AWS-Config-Regeln](#)
- [Erstellen von Metriken aus Protokollereignissen mithilfe von Filtern](#)
- [AWS Systems Manager State Manager](#)

#### Zugehörige Videos:

- [Erstellen Sie Automatisierungs-Runbooks mit AWS Systems Manager](#)
- [So automatisieren Sie den IT-Betrieb auf AWS](#)
- [AWS Security Hub Automatisierungsregeln](#)
- [Starten Sie Ihr Softwareprojekt schnell mit Amazon CodeCatalyst Blueprints](#)

#### Zugehörige Beispiele:

- [CodeCatalyst Amazon-Tutorial: Erstellen eines Projekts mit dem Blueprint für moderne dreistufige Webanwendungen](#)
- [Workshop zur Beobachtbarkeit](#)
- [Reaktion auf Vorfälle mit Incident Manager](#)



## Weiterentwicklung

### Frage

- [OPS11. Wie können Sie Arbeitsvorgänge weiterentwickeln?](#)

### OPS11. Wie können Sie Arbeitsvorgänge weiterentwickeln?

Widmen Sie nahezu kontinuierlichen inkrementellen Verbesserungen Zeit und Ressourcen, um die Effektivität und Effizienz Ihrer Betriebsabläufe weiterzuentwickeln.

### Bewährte Methoden

- [OPS11-BP01 Haben Sie einen Prozess zur kontinuierlichen Verbesserung](#)
- [OPS11-BP02 Führen Sie eine Analyse nach dem Vorfall durch](#)
- [OPS11-BP03 Implementieren Sie Feedback-Schleifen](#)
- [OPS11-BP04 Wissensmanagement durchführen](#)
- [OPS11-BP05 Definieren Sie die Treiber für Verbesserungen](#)
- [OPS11-BP06 Erkenntnisse validieren](#)
- [OPS11-BP07 Führen Sie Prüfungen der Betriebsmetriken durch](#)
- [OPS11-BP08 Die gewonnenen Erkenntnisse dokumentieren und teilen](#)
- [OPS11-BP09 Nehmen Sie sich Zeit, um Verbesserungen vorzunehmen](#)

### OPS11-BP01 Haben Sie einen Prozess zur kontinuierlichen Verbesserung

Bewerten Sie Ihre Workload mithilfe bewährter Methoden für interne und externe Architekturen. Führen Sie häufige, bewusste Workload-Überprüfungen durch. Räumen Sie Verbesserungsmöglichkeiten in Ihrem Softwareentwicklungsplan Priorität ein.

### Gewünschtes Ergebnis:

- Sie analysieren Ihre Workload regelmäßig anhand bewährter Methoden für die Architektur.
- Sie räumen den Features in Ihrem Softwareentwicklungsprozess die gleiche Priorität wie Verbesserungsmöglichkeiten ein.

### Typische Anti-Muster:

- Sie haben seit der Bereitstellung Ihrer Workload vor einigen Jahren keine Architekturüberprüfung durchgeführt.
- Verbesserungsmöglichkeiten haben geringere Priorität. Im Vergleich zu neuen Features bleiben diese Möglichkeiten im Backlog.
- In der Organisation gibt es keinen Standard für die Umsetzung von Änderungen an bewährten Methoden.

Vorteile der Nutzung dieser bewährten Methode:

- Ihre Arbeitslast richtet sich nach up-to-date den bewährten Architekturpraktiken.
- Sie entwickeln Ihre Workload gezielt weiter.
- Sie können die bewährten Methoden der Organisation nutzen, um alle Workloads zu verbessern.
- Sie erzielen marginale Gewinne, deren kumulative Wirkung jedoch zu einer höheren Effizienz führen.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Hoch

Implementierungsleitfaden

Führen Sie regelmäßig eine Überprüfung der Architektur Ihrer Workload durch. Bewerten Sie anhand interner und externer bewährter Methoden Ihre Workload und ermitteln Sie Verbesserungsmöglichkeiten. Räumen Sie Verbesserungsmöglichkeiten in Ihrem Softwareentwicklungsplan Priorität ein.

Implementierungsschritte

1. Führen Sie in vereinbarten Intervallen Überprüfungen der Architektur Ihrer Produktions-Workloads durch. Verwenden Sie einen dokumentierten Architekturstandard, der AWS spezifische Best Practices beinhaltet.
  - a. Verwenden Sie Ihre intern definierten Standards für diese Bewertungen. Wenn Sie nicht über einen internen Standard verfügen, verwenden Sie das AWS Well-Architected Framework.
  - b. Verwenden Sie den AWS Well-Architected Tool , um eine benutzerdefinierte Übersicht Ihrer internen Best Practices zu erstellen und Ihre Architektur zu überprüfen.
  - c. Wenden Sie sich an Ihren AWS Solution Architect oder Technical Account Manager, um eine geführte Well-Architected Framework-Überprüfung Ihres Workloads durchzuführen.

2. Räumen Sie den während der Überprüfung ermittelten Verbesserungsmöglichkeiten in Ihrem Softwareentwicklungsprozess Priorität ein.

Aufwand für den Implementierungsplan: Niedrig. Sie können das AWS Well-Architected Framework verwenden, um Ihre jährliche Architekturüberprüfung durchzuführen.

Ressourcen

Zugehörige bewährte Methoden:

- [OPS11-BP02 Führen Sie eine Analyse nach dem Vorfall durch](#)
- [OPS11-BP08 Dokumentieren Sie die gewonnenen Erkenntnisse und teilen Sie sie](#)
- [OPS04 Implementieren Sie Observability](#)

Zugehörige Dokumente:

- [AWS Well-Architected Tool - Kundenspezifische Objekte](#)
- [AWS Well-Architected Whitepaper – The review process](#)
- [Passen Sie Well-Architected Reviews mithilfe von Custom Lenses und dem AWS Well-Architected Tool](#)
- [Implementierung des AWS Well-Architected Custom Lens Lifecycle in Ihrem Unternehmen](#)

Zugehörige Videos:

- [Well-Architected Labs — Level 100: Maßgeschneiderte Objekte auf AWS Well-Architected Tool](#)
- [AWS re:Invent 2023 — Skalierung von Best Practices AWS Well-Architected in Ihrem gesamten Unternehmen](#)

Zugehörige Beispiele:

- [AWS Well-Architected Tool](#)

OPS11-BP02 Führen Sie eine Analyse nach dem Vorfall durch

Überprüfen Sie die Ereignisse mit Auswirkungen auf Kunden und bestimmen Sie die beitragenden Faktoren und Präventivmaßnahmen. Entwickeln Sie anhand dieser Informationen

Abhilfemaßnahmen, um Wiederholungen einzuschränken oder zu verhindern. Entwickeln Sie Verfahren für schnelle und effektive Reaktionen. Informieren Sie nach Bedarf auf zielgruppengerechte Weise über beitragende Faktoren und Korrekturmaßnahmen.

Gewünschtes Ergebnis:

- Sie haben Prozesse für das Vorfalldmanagement eingerichtet, die auch Analysen nach dem Vorfall beinhalten.
- Sie verfügen über Pläne zur Beobachtbarkeit, um Daten über Ereignisse zu sammeln.
- Anhand dieser Daten können Sie Metriken verstehen und erfassen, die Sie bei der Analyse nach einem Vorfall unterstützen.
- Sie lernen aus Vorfällen, um zukünftige Ergebnisse zu verbessern.

Typische Anti-Muster:

- Sie verwalten einen Anwendungsserver. Ungefähr alle 23 Stunden und 55 Minuten werden alle Ihre aktiven Sitzungen beendet. Sie haben versucht, festzustellen, wo der Fehler auf Ihrem Anwendungsserver liegt. Sie vermuten, dass es sich um ein Netzwerkproblem handeln könnte, das Netzwerkteam zeigt sich jedoch unkooperativ, da es für Ihr Anliegen zu beschäftigt ist. Sie haben keinen vordefinierten Prozess, den Sie befolgen könnten, um Support zu erhalten und die nötigen Informationen zu sammeln, um dem Problem auf den Grund zu gehen.
- Bei Ihrer Workload kam es zu Datenverlust. Dies ist das erste Mal, dass dieses Problem aufgetreten ist, und die Ursache ist nicht klar. Sie entscheiden, dass es nicht wichtig ist, da Sie die Daten wiederherstellen können. Datenverluste beginnen mit größerer Häufigkeit aufzutreten und wirken sich auf Ihre Kunden aus. Dadurch steigt auch der betriebliche Aufwand, wenn Sie die fehlenden Daten wiederherstellen.

Vorteile der Nutzung dieser bewährten Methode:

- Durch vordefinierte Prozesse zur Bestimmung der Komponenten, Bedingungen, Maßnahmen und Ereignisse, die zu einem Vorfall beigetragen haben, können Sie Verbesserungsmöglichkeiten ermitteln.
- Sie können Daten aus der Analyse nach einem Vorfall nutzen, um Verbesserungen vorzunehmen.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Hoch

## Implementierungsleitfaden

Verwenden Sie einen Prozess zur Ermittlung der Faktoren, die dazu beitragen. Überprüfen Sie alle Vorfälle, die sich auf Kunden auswirken. Erarbeiten Sie ein Verfahren, um die beitragenden Faktoren eines Vorfalls 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. Informieren Sie gegebenenfalls über die Ursachen von Vorfällen und passen Sie die Kommunikation an Ihre Zielgruppe an. Teilen Sie Ihre Erkenntnisse offen innerhalb Ihrer Organisation mit.

### Implementierungsschritte

1. Erfassen Sie Metriken wie Bereitstellungsänderungen, Konfigurationsänderungen, Startzeit des Vorfalls, Zeitpunkt des Alarms, Zeitpunkt des Einsatzes, Startzeit der Schadensbegrenzung und Zeitpunkt der Behebung des Vorfalls.
2. Beschreiben Sie wichtige Zeitpunkte auf der Zeitleiste, um die Ereignisse des Vorfalls zu verstehen.
3. Stellen Sie die folgenden Fragen:
  - a. Könnten Sie die Zeit bis zur Erkennung verkürzen?
  - b. Gibt es Aktualisierungen von Metriken und Alarmen, durch die der Vorfall früher erkannt würde?
  - c. Können Sie die Zeit bis zur Diagnose verkürzen?
  - d. Gibt es Aktualisierungen Ihrer Reaktions- oder Eskalationspläne, mit denen die richtigen Notfallteams früher eingeschaltet werden könnten?
  - e. Können Sie die Zeit bis zur Schadensbegrenzung verkürzen?
  - f. Gibt es Runbook- oder Playbook-Schritte, die Sie hinzufügen oder verbessern könnten?
  - g. Können Sie zukünftige Vorfälle verhindern?
4. Erstellen Sie Checklisten und Aktionen. Verfolgen und führen Sie alle Aktionen durch.

Aufwand für den Implementierungsplan: Mittel

Ressourcen

Zugehörige bewährte Methoden:

- [OPS11-BP01 Haben Sie einen Prozess zur kontinuierlichen Verbesserung](#)
- [OPS4 — Implementieren Sie Beobachtbarkeit](#)

## Zugehörige Dokumente:

- [Durchführen einer Analyse nach einem Vorfall im Incident Manager](#)
- [Überprüfung der Betriebsbereitschaft](#)

## OPS11-BP03 Implementieren Sie Feedback-Schleifen

Feedbackschleifen bieten umsetzbare Erkenntnisse zur Unterstützung der Entscheidungsfindung. Integrieren Sie Feedbackschleifen in Ihre Verfahren und Workloads. Damit können Sie Probleme und Bereiche identifizieren, für die Verbesserungen erforderlich sind. Diese validieren auch Investitionen für Verbesserungen. Diese Feedbackschleifen sind die Grundlage für die kontinuierliche Verbesserung Ihrer Workload.

Feedbackschleifen können in zwei Kategorien unterteilt werden: sofortiges Feedback und nachträgliche Analysen. Sofortiges Feedback wird durch Prüfung der Leistung und der Ergebnisse betrieblicher Aktivitäten eingeholt. Dieses Feedback kommt von Teammitgliedern, Kunden oder der automatisierten Ausgabe der Aktivität. Sofortiges Feedback kommt von Dingen wie A/B-Tests und der Auslieferung neuer Features und ist für das „Schnell scheitern“-Konzept von entscheidender Bedeutung.

Nachträgliche Analysen werden regelmäßig durchgeführt, um Feedback aus der Überprüfung betrieblicher Ergebnisse und Metriken in der Vergangenheit zu erhalten. Dies geschieht am Ende einer Phase, in regelmäßigem Rhythmus oder nach größeren Releases oder Veranstaltungen. Diese Art von Feedbackschleife validiert Investitionen in Betriebsabläufe oder Ihre Workload. Dies hilft Ihnen beim Messen des Erfolgs und bei der Validierung Ihrer Strategie.

Gewünschtes Ergebnis: Sie nutzen sofortiges Feedback und nachträgliche Analysen für weitere Verbesserungen. Es gibt einen Mechanismus zur Erfassung des Feedbacks von Benutzern und Teammitgliedern. Nachträgliche Analysen identifizieren Trends, die Verbesserungen unterstützen können.

## Typische Anti-Muster:

- Sie starten ein neues Feature, haben aber keine Möglichkeit, Feedback von den Kunden dazu zu erhalten.
- Nach einer Investition in verbesserte Betriebsabläufe führen Sie keine nachträgliche Analyse für deren Validierung durch.
- Sie holen das Feedback von Kunden ein, überprüfen dies jedoch nicht regelmäßig.

- Feedbackschleifen führen zu vorgeschlagenen Maßnahmen, werden jedoch nicht in den Softwareentwicklungsprozess einbezogen.
- Kunden erhalten kein Feedback zu Verbesserungen, die sie vorgeschlagen haben.

Vorteile der Nutzung dieser bewährten Methode:

- Sie können vom Kunden aus rückwärts arbeiten, um neue Features zu unterstützen.
- Ihre Organisationskultur kann schneller auf Änderungen reagieren.
- Trends dienen zur Identifizierung von Verbesserungsmöglichkeiten.
- Nachträgliche Analysen validieren in Ihre Workloads und Betriebsabläufe getätigte Investitionen.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Hoch

### Implementierungsleitfaden

Die Implementierung dieser bewährten Methode bedeutet, dass Sie sofortiges Feedback und nachträgliche Analysen verwenden. Diese Feedbackschleifen erleichtern Verbesserungen. Es gibt zahlreiche Mechanismen für sofortiges Feedback, z. B. Umfragen, Kundenbefragungen oder Feedbackformulare. Ihre Organisation nutzt nachträgliche Analysen auch, um Möglichkeiten für Verbesserungen zu identifizieren und Initiativen zu validieren.

### Kundenbeispiel

AnyCompany Retail hat ein Webformular erstellt, über das Kunden Feedback geben oder Probleme melden können. Bei der wöchentlichen Scrum-Sitzung evaluiert das Softwareentwicklungsteam das Benutzerfeedback. Das Feedback wird regelmäßig genutzt, um die Weiterentwicklung der Plattform zu steuern. Am Ende jeder Etappe wird eine nachträgliche Analyse durchgeführt, um Punkte zu identifizieren, bei denen Verbesserungsbedarf besteht.

### Implementierungsschritte

#### 1. Sofortiges Feedback

- Sie benötigen einen Mechanismus für den Erhalt von Feedback von Kunden und Teammitgliedern. Ihre betrieblichen Aktivitäten können auch so konfiguriert werden, dass Sie automatisiertes Feedback erhalten.
- Ihre Organisation benötigt einen Prozess zur Prüfung dieses Feedbacks, zum Feststellen der Verbesserungsbereiche und zur Planung der Verbesserungen.

- Das Feedback muss in Ihren Softwareentwicklungsprozess integriert werden.
- Wenn Sie Verbesserungen durchführen, informieren Sie die Personen, die dazu Feedback gegeben haben.
  - Sie können [AWS Systems Manager OpsCenter](#) verwenden, um diese Verbesserungen zu erstellen und nachzuverfolgen als [OpsItems](#).

## 2. Nachträgliche Analyse

- Führen Sie nachträgliche Analysen am Ende eines Entwicklungszyklus, in regelmäßigen Abständen oder nach einem größeren Release durch.
- Laden Sie an der Workload beteiligte Stakeholder zu einer Nachbesprechung ein.
- Erstellen Sie auf einem Whiteboard oder in einem Spreadsheet drei Spalten: Beenden, Starten und Beibehalten.
  - Beenden gilt für alles, mit dem Ihr Team aufhören soll.
  - Starten gilt für Ideen, die ab sofort umgesetzt werden sollen.
  - Beibehalten gilt für Elemente, die weiterhin durchgeführt werden sollen.
- Holen Sie das Feedback aller anwesenden Stakeholder ein.
- Priorisieren Sie das Feedback. Weisen Sie allen „Starten“- oder „Beibehalten“-Elementen Aktionen und Stakeholder zu.
- Fügen Sie die Aktionen Ihrem Softwareentwicklungsprozess hinzu und halten Sie die Stakeholder bei Ihren Verbesserungen über den Status auf dem Laufenden.

Aufwand für den Implementierungsplan: Mittel. Zur Implementierung dieser bewährten Methode benötigen Sie ein Verfahren zum Einholen und zur Analyse sofortigen Feedbacks. Dazu müssen Sie auch einen Prozess für die nachträgliche Analyse einrichten.

## Ressourcen

Zugehörige bewährte Methoden:

- [OPS01-BP01 Kundenbedürfnisse bewerten](#): Feedbackschleifen sind ein Mechanismus zum Ermitteln der Anforderungen externer Kunden.
- [OPS01-BP02 Evaluieren Sie die internen Kundenbedürfnisse](#): Interne Stakeholder können Feedbackschleifen nutzen, um Bedürfnisse und Anforderungen zu kommunizieren.
- [OPS11-BP02 Führen Sie eine Analyse nach dem Vorfall durch](#): Analysen nach einem Vorfall sind eine wichtige Form nachträglicher Analyse nach Vorfällen.



- [OPS11-BP07 Führen Sie Prüfungen der Betriebsmetriken durch](#): Durch die Prüfung betrieblicher Metriken können Sie Trends und Bereiche für Verbesserungen identifizieren.

#### Zugehörige Dokumente:

- [7 Fallstricke, die Sie beim Bau eines vermeiden sollten CCOE](#)
- [Atlassian Team Playbook – Retrospectives](#)
- [E-Mail-Definitionen: Feedbackschleifen](#)
- [Etablierung von Feedback-Schleifen auf der Grundlage des AWS Well-Architected Framework Review](#)
- [IBMGarage Methodology — Halten Sie einen Rückblick](#)
- [Investopedia — Der Zyklus PDCA](#)
- [Maximizing Developer Effectiveness von Tim Cochran](#)
- [Bewertungen der Betriebsbereitschaft \(ORR\) Whitepaper — Iteration](#)
- [ITILCSI- Kontinuierliche Serviceverbesserung](#)
- [Toyota und E-Commerce: Lean bei Amazon](#)

#### Zugehörige Videos:

- [Aufbau effektiver Kundenfeedbackschleifen](#)

#### Zugehörige Beispiele:

- [Astuto – Open-Source-Tool für Kundenfeedback](#)
- [AWS Lösungen — Q nABot auf AWS](#)
- [Fider – Eine Plattform zur Organisation von Kundenfeedback](#)

#### Zugehörige Services:

- [AWS Systems Manager OpsCenter](#)

## OPS11-BP04 Wissensmanagement durchführen

Durch ein Wissensmanagement erhalten Teammitglieder die Informationen, die sie für ihre Arbeit benötigen. In lernenden Organisationen werden Informationen frei geteilt, was jedem Einzelnen die nötigen Kompetenzen eröffnet. Die Informationen können entdeckt oder gesucht werden. Die Informationen sind korrekt und aktuell. Es gibt Mechanismen, um neue Informationen zu erstellen, bestehende Informationen zu aktualisieren und veraltete Informationen zu archivieren. Das gängigste Beispiel für eine Wissensmanagement-Plattform ist ein Content-Management-System wie ein Wiki.

### Gewünschtes Ergebnis:

- Teammitglieder haben Zugriff auf zeitnahe, präzise Informationen.
- Die Informationen sind durchsuchbar.
- Es gibt Mechanismen zum Hinzufügen, Aktualisieren und Archivieren von Informationen.

### Typische Anti-Muster:

- Es gibt keinen zentralen Wissensspeicher. Die Teammitglieder verwalten ihre eigenen Notizen auf ihren lokalen Rechnern.
- Sie haben ein selbst gehostetes Wiki, aber keine Mechanismen zum Verwalten von Informationen, was dazu führt, dass die Informationen veraltet sind.
- Jemand stellt fest, dass Informationen fehlen, aber es gibt keinen Prozess, um das Hinzufügen dieser Informationen zum Team-Wiki anzustoßen. Er fügt sie selbst hinzu, aber versäumt einen wichtigen Schritt, was zu einem Ausfall führt.

### Vorteile der Nutzung dieser bewährten Methode:

- Die Teammitglieder werden gestärkt, weil Informationen frei geteilt werden.
- Neue Teammitglieder werden schneller eingearbeitet, weil die Dokumentation aktuell und durchsuchbar ist.
- Die Informationen sind zeitnah, präzise und umsetzbar.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Hoch

## Implementierungsleitfaden

Das Wissensmanagement ist eine wichtige Facette von lernenden Organisationen. Zunächst benötigen Sie ein zentrales Repository, in dem Sie Ihr Wissen speichern (z. B. ein selbst gehostetes Wiki). Sie müssen Prozesse entwickeln, um Wissen hinzuzufügen, zu aktualisieren und zu archivieren. Entwickeln Sie Standards für das, was dokumentiert werden soll, und lassen Sie alle Beteiligten dazu beitragen.

### Kundenbeispiel

**AnyCompany** Der Einzelhandel hostet ein internes Wiki, in dem das gesamte Wissen gespeichert ist. Die Teammitglieder werden ermutigt, die Wissensdatenbank im Rahmen ihrer täglichen Arbeit zu ergänzen. Ein funktionsübergreifendes Team bewertet vierteljährlich, welche Seiten am wenigsten aktualisiert werden, und entscheidet, ob sie archiviert oder aktualisiert werden sollen.

### Implementierungsschritte

1. Beginnen Sie damit, das Content-Management-System zu bestimmen, in dem das Wissen gespeichert werden soll. Holen Sie die Zustimmung der Stakeholder in Ihrer Organisation ein.
  - a. Wenn Sie kein vorhandenes Content-Management-System haben, können Sie ein selbst gehostetes Wiki oder ein Versionsverwaltungssystem als Ausgangspunkt verwenden.
2. Entwickeln Sie Runbooks für das Hinzufügen, Aktualisieren und Archivieren von Informationen. Informieren Sie Ihr Team über diese Prozesse.
3. Bestimmen Sie, welches Wissen im Content-Management-System gespeichert werden soll. Beginnen Sie mit den täglichen Aktivitäten (Runbooks und Playbooks), die die Teammitglieder ausführen. Arbeiten Sie mit Stakeholdern zusammen, um Prioritäten für das hinzuzufügende Wissen festzulegen.
4. Arbeiten Sie regelmäßig mit Interessengruppen zusammen, um out-of-date Informationen zu identifizieren und zu archivieren oder auf den neuesten Stand zu bringen.

**Aufwand für den Implementierungsplan:** Mittel. Wenn Sie kein vorhandenes Content-Management-System haben, können Sie ein selbst gehostetes Wiki oder ein Dokumenten-Repository mit Versionsverwaltung einrichten.

### Ressourcen

Zugehörige bewährte Methoden:

- [OPS11-BP08 Die gewonnenen Erkenntnisse dokumentieren und teilen](#) – Das Wissensmanagement erleichtert den Austausch von Informationen über gewonnene Erkenntnisse.

Zugehörige Dokumente:

- [Atlassian - Knowledge Management](#)

Zugehörige Beispiele:

- [DokuWiki](#)
- [Gollum](#)
- [MediaWiki](#)
- [Wiki.js](#)

OPS11-BP05 Definieren Sie die Treiber für Verbesserungen

Identifizieren Sie Verbesserungsmöglichkeiten, damit Sie Chancen basierend auf Daten und Feedbackschleifen bewerten und priorisieren können. Erkunden Sie Verbesserungsmöglichkeiten in Ihren Systemen und Prozessen und automatisieren Sie bei Bedarf.

Gewünschtes Ergebnis:

- Sie verfolgen Daten aus Ihrer gesamten Umgebung.
- Sie korrelieren Ereignisse und Aktivitäten mit Geschäftsergebnissen.
- Sie können Umgebungen und Systeme vergleichen und gegenüberstellen.
- Sie führen einen detaillierten Aktivitätsverlauf Ihrer Bereitstellungen und Ergebnisse.
- Sie sammeln Daten, um Ihren Sicherheitsstatus zu stärken.

Typische Anti-Muster:

- Sie sammeln Daten aus Ihrer gesamten Umgebung, korrelieren jedoch keine Ereignisse und Aktivitäten.
- Sie sammeln detaillierte Daten aus Ihrem gesamten Nachlass, was zu hohen AWS CloudTrail Amazon-Aktivitäten CloudWatch und Kosten führt. Sie ziehen jedoch keinen sinnvollen Nutzen aus diesen Daten.
- Bei der Definition von Verbesserungsfaktoren berücksichtigen Sie nicht die Geschäftsergebnisse.

- Sie messen nicht die Auswirkungen neuer Features.

Vorteile der Nutzung dieser bewährten Methode:

- Sie minimieren die Auswirkungen ereignisbasierter Motivationen oder emotionaler Investitionen, indem Sie Verbesserungskriterien festlegen.
- Sie reagieren auf alle, nicht nur technische Geschäftsereignisse.
- Sie messen Ihre Umgebung, um Verbesserungsbereiche zu identifizieren.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Mittel

Implementierungsleitfaden

- Kenntnis der Verbesserungsfaktoren: Sie sollten ein System nur dann ändern, wenn das gewünschte Ergebnis auch unterstützt wird.
  - Gewünschte Fähigkeiten: Prüfen Sie bei der Bewertung von Verbesserungsmöglichkeiten die gewünschten Features und Fähigkeiten.
    - [Was ist neu bei AWS](#)
  - Nicht akzeptable Probleme: Prüfen Sie bei der Bewertung von Verbesserungsmöglichkeiten nicht akzeptable Probleme, Fehler und Schwachstellen. Informieren Sie sich über Dimensionierungsoptionen und suchen Sie nach Optimierungsmöglichkeiten.
    - [AWS Latest Security Bulletins](#)
    - [AWS Trusted Advisor](#)
    - [Cloud Intelligence Dashboards](#)
  - Complianceanforderungen: Prüfen Sie bei der Bewertung von Verbesserungsmöglichkeiten, welche Updates und Änderungen erforderlich sind, um Vorschriften bzw. Richtlinien einzuhalten oder weiterhin den Support eines Drittanbieters nutzen zu können.
    - [AWS -Compliance](#)
    - [AWS Compliance Programs](#)
    - [AWS Compliance Latest News](#)

Ressourcen

Zugehörige bewährte Methoden:

- [OPS01 Prioritäten der Organisation](#)
- [OPS02 Beziehungen und Besitzverhältnisse](#)
- [OPS04-BP01 Identifizieren Sie die wichtigsten Leistungsindikatoren](#)
- [OPS08 Nutzung der Workload-Beobachtbarkeit](#)
- [OPS09 Operational Health verstehen](#)
- [OPS11-BP03 Implementieren Sie Feedback-Schleifen](#)

#### Zugehörige Dokumente:

- [Amazon Athena](#)
- [Amazon QuickSight](#)
- [AWS -Compliance](#)
- [AWS Compliance Latest News](#)
- [AWS Compliance Programs](#)
- [AWS Glue](#)
- [AWS Latest Security Bulletins](#)
- [AWS Trusted Advisor](#)
- [Exportieren von Protokolldaten nach Amazon S3](#)
- [Neuerungen bei AWS](#)
- [The Imperatives of Customer-Centric Innovation](#)
- [Digital Transformation: Hype or a Strategic Necessity?](#)

#### Zugehörige Videos

- [AWS re:Invent 2023 — Verbessern Sie die betriebliche Effizienz und Widerstandsfähigkeit mit AWS Support \(0\) SUP31](#)

#### OPS11-BP06 Erkenntnisse validieren

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.

## Gewünschte Ergebnisse:

- Sie überprüfen regelmäßig Erkenntnisse mit Geschäftsbereichsleitern. Geschäftsinhaber bieten zusätzlichen Kontext für neu gewonnene Erkenntnisse.
- Sie überprüfen Erkenntnisse und bitten um Feedback von Fachkollegen, und Sie teilen Ihre Erkenntnisse mit allen Teams.
- Sie veröffentlichen Daten und Erkenntnisse, die andere technische und Geschäftsteams überprüfen können. Sie entwickeln aus Ihren Erkenntnisse neue Methoden für andere Abteilungen.
- Sie fassen neue Erkenntnisse zusammen und besprechen sie mit Führungskräften. Führungskräfte nutzen neue Erkenntnisse, um die Strategie zu definieren.

## Typische Anti-Muster:

- Sie veröffentlichen ein neues Feature. Dieses Feature verändert das Verhalten einiger Ihrer Kunden. Ihre Beobachtbarkeit berücksichtigt diese Änderungen nicht. Sie quantifizieren die Vorteile dieser Änderungen nicht.
- Sie veröffentlichen ein neues Update und vernachlässigen es, Ihr Update zu aktualisieren. CDN Der CDN Cache ist nicht mehr mit der neuesten Version kompatibel. Sie messen den Prozentsatz der Anforderungen mit Fehlern. Alle Ihre Benutzer melden HTTP 400 Fehler bei der Kommunikation mit Backend-Servern. Sie untersuchen die Kundenfehler und stellen fest, dass Sie die Zeit verschwendet haben, weil Sie die falsche Dimension gemessen haben.
- Ihr Service Level Agreement sieht eine Verfügbarkeit von 99,9 % vor und Ihr Wiederherstellungszeitpunkt liegt bei vier Stunden. Der Servicebesitzer behauptet, dass das System keine Ausfallzeiten hat. Sie implementieren eine teure und komplexe Replikationslösung, die Zeit und Geld verschwendet.

## Vorteile der Nutzung dieser bewährten Methode:

- Durch die Prüfung von Erkenntnissen zusammen mit Geschäftsinhabern und Fachexperten bauen Sie ein gemeinsames Verständnis auf und sorgen effektiver für Verbesserungen.
- Sie entdecken verborgene Probleme und berücksichtigen sie bei zukünftigen Entscheidungen.
- Ihr Fokus verlagert sich von technischen Ergebnissen hin zu Geschäftsergebnissen.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Mittel

## Implementierungsleitfaden

- Prüfen von Erkenntnissen: Wenden Sie sich an die Geschäftsinhaber und Fachexperten, um sicherzustellen, dass die Bedeutung der von Ihnen gesammelten Daten allgemein verstanden und vereinbart ist. Ermitteln Sie zusätzliche Bedenken, potenzielle Auswirkungen und bestimmen Sie eine Vorgehensweise.

## Ressourcen

### Zugehörige bewährte Methoden:

- [OPS01-BP06 Bewerten Sie Kompromisse und managen Sie gleichzeitig die Vorteile und Risiken](#)
- [OPS02-BP06 Die Verantwortlichkeiten zwischen den Teams sind vordefiniert oder werden ausgehandelt](#)
- [OPS11-BP03 Implementieren Sie Feedback-Schleifen](#)

### Zugehörige Dokumente:

- [Gestaltung eines Cloud-Exzellenzzentrums \(\) CCOE](#)

### Zugehörige Videos:

- [Building observability to increase resiliency](#)

## OPS11-BP07 Führen Sie Prüfungen der Betriebsmetriken durch

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. Berücksichtigen Sie bei Ihrer Suche nach Verbesserungsmöglichkeiten all Ihre Umgebungen (z. B. Entwicklungs-, Test- und Produktionsumgebung).

### Gewünschtes Ergebnis:

- Sie überprüfen häufig Metriken, die sich auf das Geschäft auswirken.
- Sie erkennen und überprüfen Anomalien mithilfe Ihrer Beobachtbarkeitsfunktionen.



- Sie verwenden Daten, um die Erreichung von Geschäftsergebnissen und Zielen zu unterstützen.

#### Typische Anti-Muster:

- Ihr Wartungsfenster unterbricht eine wichtige Verkaufsaktion. Das Unternehmen weiß weiterhin nicht, dass es ein Standard-Wartungsfenster gibt, das verzögert werden könnte, wenn sich andere wichtige Ereignisse auf das Geschäft auswirken.
- Sie hatten einen längeren Ausfall, weil in Ihrer Organisation häufig eine veraltete Bibliothek verwendet wird. Inzwischen sind Sie zu einer unterstützten Bibliothek migriert. Die anderen Teams in Ihrer Organisation wissen nicht, dass diese Gefahr besteht.
- Sie überprüfen den Kundenerfolg nicht regelmäßig. SLAs Sie tendieren dazu, Ihren Kunden nicht zu treffen. SLAs Wenn Sie Ihren Kunden SLAs nicht treffen, drohen finanzielle Sanktionen.

#### Vorteile der Nutzung dieser bewährten Methode:

- Indem Sie sich regelmäßig treffen, um Betriebsmetriken, Ereignisse und Vorfälle zu überprüfen, sorgen Sie für ein gemeinsames Verständnis aller Teams.
- Ihr Team trifft sich regelmäßig, um Kennzahlen und Vorfälle zu überprüfen. Auf diese Weise können Sie Maßnahmen gegen Risiken ergreifen und Kunden SLAs erkennen.
- Sie teilen Ihre gewonnenen Erkenntnisse, die Daten zur Priorisierung und zur gezielten Verbesserung der Geschäftsergebnisse liefern.

#### Risikostufe bei fehlender Befolgung dieser bewährten Methode: Mittel

#### Implementierungsleitfaden

- Führen Sie regelmäßig teamübergreifend mit Teilnehmern aus verschiedenen Unternehmensbereichen nachträgliche Analysen der operationsspezifischen Metriken durch.
- Binden Sie alle Stakeholder, einschließlich der Teams aus den Bereichen Betriebswirtschaft, Entwicklung und Operationen, ein, indem Sie Ihre Erkenntnisse aus dem sofortigen Feedback und der nachträglichen Analyse und gewonnene Erkenntnisse austauschen.
- Machen Sie sich deren Erkenntnisse zunutze, um Verbesserungspotenziale und mögliche Maßnahmen ausfindig zu machen.

## Ressourcen

Zugehörige bewährte Methoden:

- [OPS08-BP05 Dashboards erstellen](#)
- [OPS09-BP03 Überprüfen Sie die Betriebskennzahlen und priorisieren Sie Verbesserungen](#)
- [OPS10-BP01 Verwenden Sie einen Prozess für das Ereignis-, Vorfall- und Problemmanagement](#)

Zugehörige Dokumente:

- [Amazon CloudWatch](#)
- [Referenz zu CloudWatch Amazon-Kennzahlen und -Dimensionen](#)
- [Veröffentlichen von benutzerdefinierten Metriken](#)
- [Verwenden von CloudWatch Amazon-Metriken](#)
- [Dashboards und Visualisierungen mit CloudWatch](#)

OPS11-BP08 Die gewonnenen Erkenntnisse dokumentieren und teilen

Dokumentieren Sie die Erkenntnisse aus den betrieblichen Aktivitäten und geben Sie diese weiter, damit Sie sie sowohl intern als auch teamübergreifend nutzen können. Die Erkenntnisse Ihres Teams sollten Sie an andere in Ihrer Organisation weitergeben, damit alle davon profitieren. Teilen Sie Informationen und Ressourcen, um vermeidbare Fehler zu verhindern und Entwicklungsbemühungen zu unterstützen, und konzentrieren Sie sich auf die Bereitstellung der angestrebten Features.

Verwenden Sie AWS Identity and Access Management (IAM), um Berechtigungen zu definieren, die einen kontrollierten Zugriff auf die Ressourcen ermöglichen, die Sie innerhalb und zwischen Konten gemeinsam nutzen möchten.

Gewünschtes Ergebnis:

- Anschließend sollten Sie versionsgesteuerte Repositories verwenden, um Anwendungsbibliotheken, skriptbasierte Verfahren, Verfahrens- und andere Systemdokumentationen freizugeben.
- Sie teilen Ihre Infrastrukturstandards als versionskontrollierte AWS CloudFormation -Vorlagen.
- Sie überprüfen die Erkenntnisse, die Sie teamübergreifend gelernt haben.

Typische Anti-Muster:

- Sie erlitten einen längeren Ausfall, weil Ihre Organisation häufig eine fehlerhafte Bibliothek verwendet. Seitdem sind Sie zu einer zuverlässigen Bibliothek migriert. Die anderen Teams in Ihrer Organisation wissen nicht, dass diese Gefahr besteht. Niemand dokumentiert und teilt die Erfahrung mit dieser Bibliothek und sie sind sich des Risikos nicht bewusst.
- Sie haben einen Grenzfall in einem intern gemeinsam genutzten Microservice ermittelt, der dazu führt, dass Sitzungen unterbrochen werden. Sie rufen den Service jetzt anders auf, um diesen Grenzfall zu vermeiden. Die anderen Teams in Ihrer Organisation wissen nicht, dass diese Gefahr besteht.
- Sie haben einen Weg gefunden, die CPU Nutzungsanforderungen für einen Ihrer Microservices deutlich zu reduzieren. Sie wissen nicht, ob andere Teams auch von diesem Verfahren profitieren könnten.

Vorteile der Einführung dieser bewährten Methode: Teilen Sie die Erkenntnisse, um Verbesserungen zu unterstützen und erfahrungsbasierte Vorteile zu maximieren.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Niedrig

#### Implementierungsleitfaden

- Dokumentieren und Weitergeben von Erkenntnissen: Implementieren Sie Verfahren zur Dokumentation der aus der Durchführung von betrieblichen Aktivitäten und nachträglichen Analysen gewonnenen Erkenntnisse, damit auch andere Teams davon profitieren.
- Weitergeben von Erkenntnissen: Nutzen Sie Verfahren für den teamübergreifenden Austausch gewonnener Erkenntnisse und zugehöriger Artefakte. Veröffentlichen Sie beispielsweise aktualisierte Verfahren, Richtlinien, Governance und bewährte Methoden in einem allgemein zugänglichen Wiki. Teilen Sie Skripte, Code und Bibliotheken über ein gemeinsames Repository.
  - [Delegieren Sie den Zugriff auf Ihre Umgebung AWS](#)
  - [Teilen Sie ein Repository AWS CodeCommit](#)

#### Ressourcen

Zugehörige bewährte Methoden:

- [OPS02-BP06 Die Zuständigkeiten zwischen den Teams sind vordefiniert oder werden ausgehandelt](#)
- [OPS05-BP01 Verwenden Sie die Versionskontrolle](#)

- [OPS05-BP06 Teilen Sie die Designstandards](#)
- [OPS11-BP03 Implementieren Sie Feedback-Schleifen](#)
- [OPS11-BP07 Führen Sie Überprüfungen der Betriebsmetriken durch](#)

Zugehörige Dokumente:

- [Reduzieren Sie Projektverzögerungen mit einer Lösung docs-as-code](#)

Zugehörige Videos:

- [Delegieren Sie den Zugriff auf Ihre Umgebung AWS](#)
- [AWS Support s You | Exploring the Incident Management Tabletop Exercise](#)

OPS11-BP09 Nehmen Sie sich Zeit, um Verbesserungen vorzunehmen

Reservieren Sie Zeit und Ressourcen innerhalb Ihrer Prozesse, um kontinuierliche, schrittweise Verbesserungen zu ermöglichen.

Gewünschtes Ergebnis:

- Sie können temporäre Duplikate von Umgebungen erstellen. Das senkt die Risiken, den Aufwand und Kosten, die mit dem Experimentieren und Testen verbunden sind.
- Diese duplizierten Umgebungen können Sie nutzen, um die aus Ihren Analysen gezogenen Rückschlüsse zu testen, Verbesserungen zu entwickeln und geplante Verbesserungen zu testen.
- Sie veranstalten Spieltage und verwenden den Fault Injection Service (FIS), um die Kontrollen und Leitplanken bereitzustellen, die Teams für die Durchführung von Experimenten in einer Produktionsumgebung benötigen.

Typische Anti-Muster:

- Es besteht ein bekanntes Leistungsproblem auf Ihrem Anwendungsserver. Es wird im Backlog hinter jeder geplanten Feature-Implementierung priorisiert. Bleibt die Rate der hinzugefügten geplanten Features konstant, wird das Leistungsproblem niemals behoben.
- Genehmigen Sie den Administratoren und Entwicklern, dass sie ihre Überstunden zur Auswahl und Implementierung von Verbesserungen nutzen können, um kontinuierliche Verbesserungen zu unterstützen. Es werden niemals Verbesserungen vorgenommen.

- Die Betriebsabnahme ist abgeschlossen und Sie testen die betrieblichen Praktiken nicht erneut.

Vorteile der Einführung dieser bewährten Methode: Indem Sie Zeit und Ressourcen innerhalb Ihrer Prozesse reservieren, können Sie kontinuierliche, schrittweise Verbesserungen ermöglichen.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Niedrig

#### Implementierungsleitfaden

- Einplanen von Zeit für Verbesserungen: Reservieren Sie Zeit und Ressourcen innerhalb Ihrer Prozesse, um kontinuierliche, schrittweise Verbesserungen zu ermöglichen.
- Implementieren Sie Änderungen, die zu Verbesserungen führen sollen, und beurteilen Sie deren Ergebnisse.
- Versuchen Sie alternative Vorgehensweisen, wenn die Ergebnisse die Ziele nicht erfüllen und die Verbesserung immer noch Priorität hat.
- Simulieren Sie Produktionsworkloads durch GameDays, und nutzen Sie die Erkenntnisse aus diesen Simulationen, um sich zu verbessern.

#### Ressourcen

Zugehörige bewährte Methoden:

- [OPS05-BP08 Verwenden Sie mehrere Umgebungen](#)

Zugehörige Videos:

- [AWS re:Invent 2023 — Verbessern Sie die Ausfallsicherheit von Anwendungen mit dem Fault Injection Service AWS](#)

## Sicherheit

In der Säule der Sicherheit wird beschrieben, wie Sie Daten, Systeme und Komponenten so schützen, dass Sie Cloud-Technologien nutzen können, um Ihre Sicherheitslage zu verbessern. Verbindliche Anleitungen zur Implementierung finden Sie im [Whitepaper „Säule der Sicherheit“](#).

Bereiche für bewährte Methoden

- [Sicherheitsgrundlagen](#)

- [Identity and Access Management](#)
- [Erkennung](#)
- [Schutz der Infrastruktur](#)
- [Datenschutz](#)
- [Vorfalldreaktion](#)
- [Anwendungssicherheit](#)

## Sicherheitsgrundlagen

### Frage

- [SEC1. Wie wird Ihre Workload sicher verwaltet?](#)

### SEC1. Wie wird Ihre Workload sicher verwaltet?

Um Ihre Workload sicher zu betreiben, müssen Sie in allen Sicherheitsbereichen übergreifende bewährte Methoden anwenden. Wenden Sie die Anforderungen und Prozesse, die Sie im Bereich Operational Excellence auf Organisations- und Workload-Ebene definiert haben, auf alle Bereiche an. Wenn Sie über Branchenempfehlungen AWS und Bedrohungsinformationen auf dem Laufenden bleiben, können Sie Ihr Bedrohungsmodell und Ihre Kontrollziele weiterentwickeln. Die Automatisierung von Sicherheitsprozessen, Tests und Validierung ermöglicht es Ihnen, Ihre operativen Abläufe zu skalieren.

### Bewährte Methoden

- [SEC01-BP01 Separate Workloads mithilfe von Konten](#)
- [SEC01-BP02 Root-Benutzer und Eigenschaften für sicheres Konto](#)
- [SEC01-BP03 Kontrollziele identifizieren und validieren](#)
- [SEC01-BP04 Bleiben Sie über Sicherheitsbedrohungen und Empfehlungen auf dem Laufenden](#)
- [SEC01-BP05 Reduzieren Sie den Umfang des Sicherheitsmanagements](#)
- [SEC01-BP06 Automatisieren Sie die Implementierung von Standardsicherheitskontrollen](#)
- [SEC01-BP07 Identifizieren Sie Bedrohungen und priorisieren Sie Abhilfemaßnahmen mithilfe eines Bedrohungsmodells](#)
- [SEC01-BP08 Regelmäßige Evaluierung und Implementierung neuer Sicherheitsdienste und -funktionen](#)

## SEC01-BP01 Separate Workloads mithilfe von Konten

Sorgen Sie mit einer Mehrkonten-Strategie für wirksamen Integritätsschutz und Isolierungen zwischen Umgebungen (etwa Produktion, Entwicklung und Test) sowie Workloads. Die Trennung auf Kontoebene wird nachdrücklich angeraten, da diese für die wirksame Isolierung für Sicherheits-, Fakturierungs- und Zugriffszwecke sorgt.

Gewünschtes Ergebnis: eine Kontostruktur, die Cloud-Vorgänge, nicht zusammengehörige Workloads und Umgebungen in separaten Konten voneinander isoliert, sodass die Sicherheit in der gesamten Cloud-Infrastruktur verbessert wird.

Typische Anti-Muster:

- Platzierung mehrerer nicht zusammengehöriger Workloads mit unterschiedlicher Datensensitivität in einem einzigen Konto
- Schlecht definierte Organizational Unit (OU, Organisationseinheit)-Struktur

Vorteile der Nutzung dieser bewährten Methode:

- Geringere Auswirkungen bei versehentlichen Zugriffen auf eine Workload
- Zentrale Steuerung des Zugangs zu AWS Dienstleistungen, Ressourcen und Regionen.
- Wahrung der Sicherheit der Cloud-Infrastruktur durch Richtlinien und die zentralisierte Verwaltung von Sicherheitservices
- Automatisierte Kontoerstellung und Wartungsprozesse
- Zentralisierte Prüfung Ihrer Infrastruktur auf Compliance- und regulatorische Anforderungen

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Hoch

Implementierungsleitfaden

AWS-Konten sorgen für eine Sicherheitsisolierung zwischen Workloads oder Ressourcen, die auf unterschiedlichen Empfindlichkeitsstufen betrieben werden. AWS bietet Tools, mit denen Sie Ihre Cloud-Workloads mithilfe einer Strategie für mehrere Konten skalieren können, um diese Isolationsgrenze zu nutzen. Anleitungen zu den Konzepten, Mustern und der Implementierung einer Multi-Account-Strategie finden Sie unter [Organizing Your AWS Environment Using Multi-Accounts](#).  
AWS

Wenn mehrere Konten zentral AWS-Konten verwaltet werden, sollten Ihre Konten in einer Hierarchie organisiert werden, die durch Ebenen von Organisationseinheiten (OUs) definiert wird. Anschließend können Sicherheitskontrollen organisiert und auf die Mitgliedskonten OUs und die Mitgliedskonten angewendet werden, wodurch konsistente präventive Kontrollen für die Mitgliedskonten in der Organisation eingerichtet werden. Die Sicherheitskontrollen werden weitergegeben, sodass Sie nach verfügbaren Berechtigungen für Mitgliedskonten auf unteren Ebenen der OE-Hierarchie filtern können. Ein gutes Design macht sich diese Weitergabe zunutze, um die Anzahl und die Komplexität der Sicherheitsrichtlinien, die für die erwünschten Sicherheitskontrollen für jedes Mitgliedskonto erforderlich sind, zu reduzieren.

[AWS Organizations](#) und [AWS Control Towers](#) sind zwei Dienste, mit denen Sie diese Struktur mit mehreren Konten in Ihrer AWS Umgebung implementieren und verwalten können. AWS Organizations ermöglicht es Ihnen, Konten in einer Hierarchie zu organisieren, die durch eine oder mehrere Ebenen definiert wird OUs, wobei jede Organisationseinheit eine Reihe von Mitgliedskonten enthält. [Richtlinien zur Dienstkontrolle](#) (SCPs) ermöglichen es dem Organisationsadministrator, detaillierte präventive Kontrollen für Mitgliedskonten einzurichten. [AWS Config](#) Sie können auch verwendet werden, um proaktive und detektive Kontrollen für Mitgliedskonten einzurichten. Viele AWS Dienste [lassen sich integrieren AWS Organizations](#), um delegierte Verwaltungskontrollen bereitzustellen und dienstspezifische Aufgaben für alle Mitgliedskonten im Unternehmen auszuführen.

Darüber AWS Organizations hinaus [AWS Control Tower](#) bietet es eine Einrichtung von Best Practices mit nur einem Klick für eine AWS Umgebung mit mehreren Konten und einer [landing](#) zone. Die Landing Zone ist der Einstiegspunkt für die Mehrkonten-Umgebung, eingerichtet von Control Tower. Control Tower bietet mehrere [Vorteile](#) gegenüber AWS Organizations. Hier sind drei Vorteile, die die Kontoverwaltung verbessern:

- Integrierter verpflichtender Integritätsschutz, der automatisch auf für die Organisation zugelassene Konten angewendet wird
- Optionale Steuerungen, die für eine bestimmte Gruppe von ein- oder ausgeschaltet werden können. OUs
- [AWS Control Tower Account Factory](#) ermöglicht die automatisierte Bereitstellung von Konten mit vorab genehmigten Baselines und Konfigurationsoptionen in Ihrem Unternehmen.

## Implementierungsschritte



1. Entwurf einer Struktur für Organisationseinheiten: Eine ordnungsgemäß gestaltete Struktur für Organisationseinheiten reduziert den Verwaltungsaufwand für die Erstellung und Wahrung von Service-Kontrollrichtlinien und anderen Sicherheitskontrollen. Ihre Struktur für Organisationseinheiten sollte [an Ihre geschäftlichen Anforderungen, die Sensitivität der Daten und die Workload-Struktur angepasst sein](#).
2. Erstellen einer Landing Zone für Ihre Mehrkontenumgebung: Eine Landing Zone bietet eine konsistente Sicherheits- und Infrastrukturbasis, über die Ihre Organisation Workloads schnell entwickeln, starten und bereitstellen kann. Sie können eine [individuell erstellte Landing Zone AWS Control Tower oder](#) für die Orchestrierung Ihrer Umgebung verwenden.
3. Einrichtung von Integritätsschutz: Implementieren Sie konsistenten Integritätsschutz für Ihre Umgebung über Ihre Landing Zone. AWS Control Tower bietet eine Liste [verpflichtender](#) und [optionaler](#) Kontrollen, die bereitgestellt werden können. Verpflichtende Kontrollen werden automatisch bereitgestellt, wenn Control Tower implementiert wird. Überprüfen Sie die Liste nachdrücklich empfohlener sowie optionaler Kontrollen und implementieren Sie diejenigen, die Ihren Anforderungen entsprechen.
4. Beschränken Sie den Zugriff auf neu hinzugefügte Regionen: Bei neuen AWS-Regionen werden IAM Ressourcen wie Benutzer und Rollen nur an die von Ihnen angegebenen Regionen weitergegeben. Diese Aktion kann über die [Konsole ausgeführt werden, wenn Sie Control Tower verwenden](#), oder indem Sie die [IAM-Berechtigungsrichtlinien in](#) anpassen AWS Organizations.
5. AWS [CloudFormation StackSets](#) Erwägen Sie, Ihnen anhand einer genehmigten Vorlage dabei zu StackSets helfen, Ressourcen wie IAM Richtlinien, Rollen AWS-Konten und Gruppen in verschiedenen Regionen bereitzustellen.

## Ressourcen

### Zugehörige bewährte Methoden:

- [SEC02-BP04 Verlassen Sie sich auf einen zentralen Identitätsanbieter](#)

### Zugehörige Dokumente:

- [AWS Control Tower](#)
- [Richtlinien zur AWS -Sicherheitsprüfung](#)
- [IAM-Bewährte Verfahren](#)
- [Wird verwendet CloudFormation StackSets , um Ressourcen in mehreren AWS-Konten Regionen bereitzustellen](#)

- [Organizations FAQ](#)
- [AWS Organizations Terminologie und Konzepte](#)
- [Bewährte Methoden für Richtlinien zur Servicesteuerung in einer Umgebung AWS Organizations mit mehreren Konten](#)
- [AWS -Referenzhandbuch zur Kontoverwaltung](#)
- [Organisieren Sie Ihre AWS Umgebung mithilfe mehrerer Konten](#)

#### Zugehörige Videos:

- [Enable AWS adoption at scale with automation and governance](#)
- [Security Best Practices the Well-Architected Way](#)
- [Aufbau und Verwaltung mehrerer Konten mit AWS Control Tower](#)
- [Enable Control Tower for Existing Organizations](#)

#### Zugehörige Workshops:

- [Control Tower Immersion Day](#)

### SEC01-BP02 Root-Benutzer und Eigenschaften für sicheres Konto

Der Root-Benutzer ist der Benutzer mit den meisten Rechten in einem AWS-Konto. Er hat vollen Administratorzugriff auf alle Ressourcen innerhalb des Kontos und kann in einigen Fällen nicht durch Sicherheitsrichtlinien eingeschränkt werden. Die Deaktivierung des programmatischen Zugriffs auf den Root-Benutzer, die Einrichtung geeigneter Kontrollen für den Root-Benutzer und das Vermeiden der routinemäßigen Verwendung des Root-Benutzers senken die Risiken einer unbeabsichtigten Offenlegung der Anmeldeinformationen des Root-Benutzers und daraus resultierender ernsthafter Probleme für die Cloud-Umgebung.

Gewünschtes Ergebnis: Das Sichern des Root-Benutzers hilft dabei, die Gefahr zu verringern, dass versehentliche oder beabsichtigte Schäden durch den Missbrauch der Anmeldeinformationen des Root-Benutzers entstehen. Die Einrichtung erkennender Kontrollen kann auch für die Benachrichtigung der richtigen Personen sorgen, wenn Aktionen unter Verwendung des Root-Benutzers durchgeführt werden.

#### Typische Anti-Muster:

- Verwendung des Root-Benutzers für andere Aufgaben als die wenigen, für die Root-Benutzer-Anmeldeinformationen erforderlich sind
- Versäumnis, Notfallpläne regelmäßig zu testen, um das Funktionieren kritischer Infrastrukturen, Prozesse und des Personals während eines Notfalls zu überprüfen.
- ausschließliche Berücksichtigung des typischen Kontoanmeldungsprozesses und keine Berücksichtigung alternativer Kontowiederherstellungsverfahren
- E-Mail-Server und Telefonanbieter gehören nicht zum kritischen Sicherheitsbereich, da diese bei der Kontowiederherstellung verwendet werden. DNS

Vorteile der Nutzung dieser bewährten Methode: Der Schutz des Zugriffs auf den Root-Benutzer stärkt das Vertrauen dazu, dass Aktionen in Ihrem Konto kontrolliert und überwacht werden.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Hoch

### Implementierungsleitfaden

AWS bietet viele Tools zur Sicherung Ihres Kontos. Da einige dieser Maßnahmen aber nicht standardmäßig aktiviert sind, müssen Sie sie selbst implementieren. Betrachten Sie diese Empfehlungen als grundlegende Schritte für den Schutz Ihres AWS-Konto. Bei der Implementierung dieser Schritte ist es wichtig, dass Sie einen Prozess für die kontinuierliche Bewertung und Überwachung der Sicherheitskontrollen einrichten.

Wenn Sie zum ersten Mal ein erstellen AWS-Konto, beginnen Sie mit einer Identität, die vollständigen Zugriff auf alle AWS Dienste und Ressourcen im Konto hat. Diese Identität wird als AWS-Konto Root-Benutzer bezeichnet. Sie können sich als Stammbenutzer mit der E-Mail-Adresse und dem Passwort anmelden, die Sie bei der Erstellung des Kontos verwendet haben. Aufgrund der erhöhten Zugriffsrechte, die dem AWS Root-Benutzer gewährt werden, müssen Sie die Verwendung des AWS Root-Benutzers einschränken, um Aufgaben auszuführen, [für die er ausdrücklich erforderlich ist](#). Die Anmeldedaten des Root-Benutzers müssen sorgfältig geschützt werden, und für den AWS-Konto Root-Benutzer sollte immer die Multi-Faktor-Authentifizierung (MFA) verwendet werden.

Zusätzlich zum normalen Authentifizierungsablauf, bei dem Sie sich mit einem Benutzernamen, einem Passwort und einem Gerät mit Multi-Faktor-Authentifizierung (MFA) bei Ihrem Root-Benutzer anmelden, gibt es Verfahren zur Kontowiederherstellung, mit denen Sie sich bei Ihrem AWS-Konto Root-Benutzer anmelden können, wenn Sie Zugriff auf die E-Mail-Adresse und Telefonnummer haben, die mit Ihrem Konto verknüpft sind. Daher ist es ebenso wichtig, das E-Mail-Konto des Root-

Benutzers, an das die Wiederherstellungs-E-Mail gesendet wird, und die mit dem Konto verknüpfte Telefonnummer zu sichern. Denken Sie auch an mögliche zirkuläre Abhängigkeiten, bei denen die dem Root-Benutzer zugeordnete E-Mail-Adresse auf E-Mail-Servern oder Domain Name Service (DNS) -Ressourcen desselben AWS-Konto gehostet wird.

Bei der Verwendung gibt es mehrere AWS Organizations, von denen AWS-Konten jede einen Root-Benutzer hat. Ein Konto fungiert als Verwaltungskonto und mehrere Ebenen von Mitgliedskonten können dann darunter hinzugefügt werden. Priorisieren Sie den Schutz des Root-Benutzers Ihres Verwaltungskontos und kümmern Sie sich dann um diejenigen der Mitgliedskonten. Die Strategie zum Schutz des Root-Benutzers Ihres Verwaltungskontos kann sich von der für die Root-Benutzer der Mitgliedskonten unterscheiden und Sie können präventive Sicherheitskontrollen für die Root-Benutzer Ihrer Mitgliedskonten einrichten.

## Implementierungsschritte

Die folgenden Implementierungsschritte werden für die Einrichtung der Kontrollen für den Root-Benutzer empfohlen. Gegebenenfalls werden die Empfehlungen mit der [Benchmark-Version 1.4.0 der CIS AWS Foundation](#) verglichen. Konsultieren Sie zusätzlich zu diesen Schritten die [Richtlinien für AWS bewährte Verfahren](#) zum Schutz Ihrer Ressourcen AWS-Konto und Ihrer Ressourcen.

## Präventive Kontrollen

1. Richten Sie genaue [Kontaktinformationen](#) für das Konto ein.
  - a. Diese Informationen werden für die Wiederherstellung eines verlorenen Kennworts, für die Wiederherstellung eines verlorenen MFA Gerätekontos und für wichtige sicherheitsrelevante Mitteilungen mit Ihrem Team verwendet.
  - b. Verwenden Sie eine von ihrer Unternehmensdomain gehostete E-Mail-Adresse, vorzugsweise eine Verteilerliste, als E-Mail-Adresse des Root-Benutzers. Die Verwendung einer Verteilerliste anstelle einer einzelnen E-Mail-Adresse sorgt für zusätzliche Redundanz und Kontinuität beim Zugriff auf das Root-Konto über längere Zeiträume hinweg.
  - c. Die in den Kontaktinformationen angegebene Telefonnummer sollte eine für diesen Zweck speziell eingerichtete und sichere Telefonnummer sein. Diese Telefonnummer sollte nicht eingetragen sein oder an andere weitergegeben werden.
2. Erstellen Sie keine Zugriffsschlüssel für den Root-Benutzer. Falls Zugangsschlüssel vorhanden sind, entfernen Sie sie (CIS1.4).
  - a. Entfernen Sie alle langfristigen programmatischen Anmeldeinformationen (Zugriffs- und geheime Schlüssel) für den Root-Benutzer.

- b. Wenn Root-Benutzerzugriffsschlüssel bereits existieren, sollten Sie Prozesse, die diese Schlüssel verwenden, auf die Verwendung temporärer Zugriffsschlüssel aus einer AWS Identity and Access Management (IAM) -Rolle umstellen und dann [die Root-Benutzerzugriffsschlüssel löschen](#).
3. Ermitteln Sie, ob Sie Anmeldeinformationen für den Root-Benutzer speichern müssen.
    - a. Wenn Sie neue Mitgliedskonten erstellen, wird das anfängliche Passwort für den Root-Benutzer neuer Mitgliedskonten auf einen zufälligen Wert gesetzt, der Ihnen nicht zugänglich ist. AWS Organizations Erwägen Sie, den Ablauf zum Zurücksetzen des Passworts von Ihrem AWS Organisationsverwaltungs-konto aus zu verwenden, [um bei Bedarf Zugriff auf das Mitgliedskonto](#) zu erhalten.
    - b. Für ein eigenständiges Konto AWS-Konten oder das Verwaltungskonto der AWS Organisation sollten Sie erwägen, Anmeldeinformationen für den Root-Benutzer zu erstellen und sicher zu speichern. MFA für den Root-Benutzer verwenden.
  4. Verwenden Sie präventive Kontrollen für Root-Benutzer von Mitgliedskonten in Umgebungen AWS mit mehreren Konten.
    - a. Erwägen Sie die präventive Sicherheitsvorkehrung [Erstellung von Zugriffsschlüsseln für den Root-Benutzer nicht zulassen](#) für Mitgliedskonten.
    - b. Erwägen Sie die Aktivierung der präventiven Sicherheitsmaßnahme [Aktionen als Root-Benutzer nicht zulassen](#) für Mitgliedskonten.
  5. Wenn Sie Anmeldeinformationen für den Root-Benutzer benötigen:
    - a. Verwenden Sie ein komplexes Passwort.
    - b. Aktivieren Sie die Multi-Faktor-Authentifizierung (MFA) für den Root-Benutzer, insbesondere für AWS Organizations Verwaltungskonten (Zähler) (1.5). CIS
    - c. Ziehen Sie aus Gründen der Stabilität und Sicherheit MFA Hardwaregeräte in Betracht, da Einweggeräte die Wahrscheinlichkeit verringern können, dass Geräte, die Ihre MFA Codes enthalten, für andere Zwecke wiederverwendet werden. Stellen Sie sicher, dass batteriebetriebene MFA Hardwaregeräte regelmäßig ausgetauscht werden. (CIS1.6)
      - Folgen Sie zur Konfiguration MFA für den Root-Benutzer den Anweisungen zum Erstellen eines [virtuellen MFA Geräts MFA oder eines Hardwaregeräts](#).
    - d. Erwägen Sie, mehrere MFA Geräte für das Backup zu registrieren. [Pro Konto sind bis zu 8 MFA Geräte zulässig](#).
      - Beachten Sie, dass die Registrierung von mehr als einem MFA Gerät für den Root-Benutzer automatisch die [Wiederherstellung Ihres Kontos deaktiviert, falls das MFA Gerät verloren geht](#).

- e. Speichern Sie das Passwort in sicherer Weise, und beachten Sie zirkuläre Abhängigkeiten bei der elektronischen Speicherung des Passworts. Speichern Sie das Passwort nicht so, dass Sie Zugriff darauf benötigen, um es AWS-Konto zu erhalten.
6. Optional: Erwägen Sie die Einrichtung einer periodischen Passwortrotation für den Root-Benutzer.
- Bewährte Methoden für die Verwaltung von Anmeldeinformationen hängen von Ihren jeweiligen regulatorischen und Richtlinienanforderungen ab. Root-Benutzer, MFA die durch geschützt sind, sind nicht auf das Passwort als einzigen Authentifizierungsfaktor angewiesen.
  - [Die regelmäßige Änderung des Root-Benutzer-Passworts](#) senkt das Risiko, dass ein unbeabsichtigt offengelegtes Passwort missbraucht werden kann.

### Detektivische Kontrollen

- Erstellen Sie Alarme, um die Verwendung der Root-Anmeldeinformationen zu erkennen (CIS1.7). [Amazon GuardDuty](#) kann anhand der Ergebnisse die Verwendung von API Root-Benutzeranmeldedaten überwachen und [RootCredentialUsage](#) darauf hinweisen.
- Evaluieren und implementieren Sie die im [AWS Well-Architected Security Pillar-Konformitätspaket](#) enthaltenen detektiven Kontrollen oder AWS Config, falls Sie diese verwenden, die [dringend empfohlenen Kontrollen AWS Control Tower, die im Control Tower](#) verfügbar sind.

### Operative Anleitung

- Legen Sie fest, wer in der Organisation Zugriff auf die Root-Benutzer-Anmeldeinformationen haben sollte.
- Verwenden Sie eine Zwei-Personen-Regel, damit niemand Zugriff auf alle erforderlichen Anmeldeinformationen hat und um Root-Benutzerzugriff MFA zu erhalten.
- Stellen Sie sicher, dass die Organisation und nicht eine einzelne Person die Kontrolle über die Telefonnummer und den E-Mail-Alias behält, die dem Konto zugeordnet sind (die für das Zurücksetzen und MFA Zurücksetzen von Passwörtern verwendet werden).
- Verwenden Sie den Root-Benutzer nur ausnahmsweise (CIS1.7).
- Der AWS Root-Benutzer darf nicht für alltägliche Aufgaben verwendet werden, auch nicht für administrative. Melden Sie sich nur dann als Root-Benutzer an, wenn Sie [AWS -Aufgaben durchführen müssen, für die der Root-Benutzer erforderlich ist](#). Alle anderen Aktionen sollten von anderen Benutzern mit den entsprechenden Rollen durchgeführt werden.

- Prüfen Sie regelmäßig, ob der Zugriff auf den Root-Benutzer funktioniert, um Prozeduren vor dem Eintreten von Notsituationen zu testen, die die Verwendung der Root-Benutzer-Anmeldeinformationen erfordern.
- Prüfen Sie regelmäßig, ob die mit dem Konto verbundene E-Mail-Adresse und die unter [Alternative Kontakte](#) aufgeführten E-Mail-Adressen funktionieren. Überwachen Sie diese E-Mail-Posteingänge auf etwaige Sicherheitsmitteilungen von <abuse@amazon.com>. Stellen Sie auch sicher, dass alle mit dem Konto verbundenen Telefonnummern funktionieren.
- Bereiten Sie Notfallreaktionsprozeduren vor, um auf den Missbrauch des Root-Kontos reagieren zu können. Weitere Informationen zum Aufbau einer Sicherheitsstrategie für Ihr AWS-Konto finden Sie im [AWS -Reaktionsleitfaden für Sicherheitsvorfälle](#) und in den bewährten Methoden im [Abschnitt zu Vorfälleaktionen im Whitepaper zur Säule „Sicherheit“](#).

## Ressourcen

### Zugehörige bewährte Methoden:

- [SEC01-BP01 Separate Workloads mithilfe von Konten](#)
- [SEC02-BP01 Verwenden Sie starke Anmeldemechanismen](#)
- [SEC03-BP02 Least-Privilege-Zugriff gewähren](#)
- [SEC03-BP03 Notfallzugangsverfahren einrichten](#)
- [SEC10-BP05 Zugriff vor der Bereitstellung](#)

### Zugehörige Dokumente:

- [AWS Control Tower](#)
- [Richtlinien zur AWS -Sicherheitsprüfung](#)
- [IAM Bewährte Verfahren](#)
- [Amazon GuardDuty — Warnung zur Verwendung von Root-Anmeldeinformationen](#)
- [S tep-by-step Anleitung zur Überwachung der Verwendung von Root-Anmeldeinformationen durch CloudTrail](#)
- [MFAToken, die für die Verwendung mit zugelassen sind AWS](#)
- Implementierung von [Break Glass Access](#) auf AWS
- [Die 10 wichtigsten Sicherheitselemente, die Sie in Ihrem Bereich verbessern sollten AWS-Konto](#)

- [What do I do if I notice unauthorized activity in my AWS-Konto?](#)

Zugehörige Videos:

- [Enable AWS adoption at scale with automation and governance](#)
- [Security Best Practices the Well-Architected Way](#)
- [Beschränkung der Verwendung von AWS Root-Anmeldeinformationen](#) aus AWS re:inforce 2022 — Bewährte Sicherheitsmethoden mit AWS IAM

Zugehörige Beispiele und Labs:

- [Labor: AWS-Konto Einrichtung und Root-Benutzer](#)

SEC01-BP03 Kontrollziele identifizieren und validieren

Entsprechend Ihren Compliance-Anforderungen und Risiken, die aus Ihrem Bedrohungsmodell identifiziert werden, können Sie die Kontrollziele und Kontrollen ableiten und validieren, die Sie für Ihre Workload benötigen. Die laufende Validierung von Kontrollzielen und Kontrollen hilft Ihnen, die Effektivität der Risikominderung zu messen.

Gewünschtes Ergebnis: Die Kontrollziele Ihres Unternehmens sind klar definiert und auf Ihre Compliance-Anforderungen abgestimmt. Kontrollen werden durch Automatisierung und Richtlinien implementiert und durchgesetzt und kontinuierlich auf ihre Wirksamkeit bei der Erreichung Ihrer Ziele überprüft. Die Belege für die Wirksamkeit sowohl zu einem bestimmten Zeitpunkt als auch über einen bestimmten Zeitraum hinweg sind jederzeit für Prüfer abrufbar.

Typische Anti-Muster:

- Regulatorische Anforderungen, Markterwartungen und Branchenstandards für verlässliche Sicherheit sind in Ihrem Unternehmen nicht hinreichend vertraut.
- Ihr Framework für die Cybersicherheit und Ihre Kontrollziele sind nicht an den Anforderungen Ihres Unternehmens ausgerichtet.
- Die Implementierung der Kontrollen ist nicht messbar auf Ihre Kontrollziele ausgerichtet.
- Sie verwenden keine Automatisierung zur Berichterstattung über die Wirksamkeit Ihrer Kontrollen.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Hoch



## Implementierungsleitfaden

Es gibt zahlreiche gängige Frameworks für die Cybersicherheit, die die Grundlage für Ihre Sicherheitskontrollziele bilden können. Berücksichtigen Sie die regulatorischen Anforderungen, die Markterwartungen und die Branchenstandards für Ihr Unternehmen, um festzustellen, welches Framework Ihre Anforderungen am besten erfüllt. [Zu den Beispielen gehören AICPASOC2, HITRUST, PCI-DSS, ISO27001 und NIST SP 800-53.](#)

Machen Sie sich im Hinblick auf die von Ihnen festgelegten Kontrollziele ein Bild davon, wie die von Ihnen in Anspruch genommenen AWS Dienste Ihnen dabei helfen, diese Ziele zu erreichen. Hier finden [AWS Artifact](#) Sie Dokumentationen und Berichte, die auf Ihre Ziel-Frameworks abgestimmt sind und den Zuständigkeitsbereich beschreiben, für den Sie zuständig sind, AWS sowie Anleitungen für den verbleibenden Bereich, für den Sie verantwortlich sind. Weitere servicespezifische Anleitungen, die sich an verschiedenen Regelwerken orientieren, finden Sie unter [AWS Customer Compliance Guides](#).

Während Sie die Kontrollen zur Erreichung Ihrer Ziele definieren, kodifizieren Sie die Durchsetzung mithilfe von präventiven Kontrollen und automatisieren die Abschwächung mithilfe von detektivischen Kontrollen. Mithilfe von [Richtlinien zur Servicesteuerung \(SCP\)](#) können Sie verhindern, dass Ressourcenkonfigurationen und Aktionen in Ihrem AWS Organizations Unternehmen nicht den Vorschriften entsprechen. Implementieren Sie Regeln in [AWS Config](#) zur Überwachung und Berichterstattung über nicht konforme Ressourcen und wechseln Sie dann zu einem Durchsetzungsmodell, sobald Sie von deren Verhalten überzeugt sind. Wenn Sie vordefinierte und verwaltete Regeln bereitstellen möchten, die sich an Ihren Cybersicherheits-Rahmenbedingungen orientieren, sollten Sie die Verwendung von [AWS Security Hub -Standards](#) als erste Wahl in Betracht ziehen. Der Standard AWS Foundational Service Best Practices (FSBP) und der CIS AWS Foundations Benchmark sind gute Ausgangspunkte für Kontrollen, die auf viele Ziele ausgerichtet sind, die in mehreren Standard-Frameworks gemeinsam sind. In Fällen, in denen Security Hub nicht intrinsisch die gewünschten Kontrollmeldungen verfügt, kann es durch [AWS Config -Konformitätspakete](#) ergänzt werden.

Nutzen Sie die vom AWS Global Security and Compliance Acceleration (GSCA) -Team empfohlenen [APN Partnerpakete](#), um bei Bedarf Unterstützung von Sicherheitsberatern, Beratungsagenturen, Systemen zur Erfassung und Berichterstattung von Nachweisen, Auditoren und anderen ergänzenden Dienstleistungen zu erhalten.

## Implementierungsschritte

1. Bewerten Sie gängige Frameworks für Cybersicherheit und richten Sie Ihre Kontrollziele an den ausgewählten Frameworks aus.
2. Besorgen Sie sich relevante Unterlagen zu Anleitungen und Verantwortlichkeiten bei der Verwendung AWS Artifact Ihres Frameworks. Finden Sie heraus, für welche Aspekte der Einhaltung der AWS Vorschriften das Modell der gemeinsamen Verantwortung gilt und für welche Bereiche Sie verantwortlich sind.
3. Verwenden Sie SCPs Ressourcenrichtlinien, Rollenvertrauensrichtlinien und andere Schutzmaßnahmen, um unzulässige Ressourcenkonfigurationen und Aktionen zu verhindern.
4. Evaluieren Sie den Einsatz von Security Hub Hub-Standards und AWS Config Konformitätspaketen, die Ihren Kontrollzielen entsprechen.

## Ressourcen

### Zugehörige bewährte Methoden:

- [SEC03-BP01 Definieren Sie die Zugriffsanforderungen](#)
- [SEC04-BP01 Konfigurieren Sie die Dienst- und Anwendungsprotokollierung](#)
- [SEC07-BP01 Verstehen Sie Ihr Datenklassifizierungsschema](#)
- [OPS01-BP03 Bewerten Sie die Anforderungen an die Unternehmensführung](#)
- [OPS01-BP04 Bewerten Sie die Compliance-Anforderungen](#)
- [PERF01-BP05 Verwenden Sie Richtlinien und Referenzarchitekturen](#)
- [COST02-BP01 Entwickeln Sie Richtlinien auf der Grundlage der Anforderungen Ihres Unternehmens](#)

### Zugehörige Dokumente:

- [AWS Customer Compliance Guides](#)

### Zugehörige Tools:

- [AWS Artifact](#)

## SEC01-BP04 Bleiben Sie über Sicherheitsbedrohungen und Empfehlungen auf dem Laufenden

Bleiben Sie auf dem Laufenden über die neuesten Bedrohungen und Abhilfemaßnahmen, indem Sie Veröffentlichungen zu Bedrohungsdaten und Datenfeeds der Branche auf Aktualisierungen verfolgen. Prüfen Sie Angebote für verwaltete Services, die automatisch auf der Grundlage der neuesten Bedrohungsdaten aktualisiert werden.

Gewünschtes Ergebnis: Sie bleiben auf dem Laufenden, da die Branchenpublikationen mit den neuesten Bedrohungen und Empfehlungen aktualisiert werden. Sie nutzen die Automatisierung, um potenzielle Schwachstellen und Gefährdungen zu erkennen, während Sie neue Bedrohungen identifizieren. Sie ergreifen Maßnahmen zur Eindämmung dieser Bedrohungen. Sie AWS nutzen Dienste, die automatisch mit den neuesten Bedrohungsdaten aktualisiert werden.

Typische Anti-Muster:

- Kein zuverlässiger und wiederholbarer Mechanismus, um über die neuesten Bedrohungsdaten informiert zu sein
- Manuelle Bestandsführung Ihres Technologieportfolios, Ihrer Workloads und Abhängigkeiten, was menschliches Eingreifen im Hinblick auf potenzielle Schwachstellen und Gefährdungen erfordert
- Fehlende Mechanismen zur Aktualisierung Ihrer Workloads und Abhängigkeiten auf die neuesten verfügbaren Versionen, die bekannte Bedrohungsabwehrmaßnahmen bieten

Vorteile der Nutzung dieser bewährten Methode: Die Verwendung von Bedrohungsdatenquellen, um auf dem Laufenden zu bleiben, verringert das Risiko, wichtige Änderungen in der Bedrohungslandschaft zu verpassen, die sich auf Ihr Unternehmen auswirken können. Wenn Sie Ihre Workloads und deren Abhängigkeiten automatisiert auf potenzielle Schwachstellen oder Gefährdungen prüfen, diese erkennen und beheben, können Sie Risiken im Vergleich zu manuellen Alternativen schnell und vorhersehbar eindämmen. Dies trägt dazu bei, Zeit und Kosten im Zusammenhang mit der Behebung von Schwachstellen zu kontrollieren.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Hoch

Implementierungsleitfaden

Verfolgen Sie vertrauenswürdige Veröffentlichungen zu Bedrohungsdaten, um über die Bedrohungslandschaft auf dem Laufenden zu bleiben. Dokumentation zu bekannten gegnerischen Taktiken, Techniken und Verfahren finden Sie in der [MITRE ATT&CK Knowledge Base](#) (). TTPs Lesen Sie MITRE die Liste der [häufigsten Sicherheitslücken und Risiken](#) (CVE), um über bekannte

Sicherheitslücken in Produkten, auf die Sie sich verlassen, auf dem Laufenden zu bleiben. Machen Sie sich mit dem beliebten [OWASPTop-10-Projekt](#) des Open Worldwide Application Security Project (OWASP) ein Bild von kritischen Risiken für Webanwendungen.

Bleiben Sie mit AWS den [Sicherheitsbulletins AWS](#) für über Sicherheitsereignisse und empfohlene Maßnahmen zur Problembhebung auf dem Laufenden. CVEs

Um Ihren Gesamtaufwand und die Kosten für die Aktualisierung zu reduzieren, sollten Sie die Nutzung von AWS Diensten in Betracht ziehen, die im Laufe der Zeit automatisch neue Bedrohungsinformationen einbeziehen. [Amazon GuardDuty](#) hält sich beispielsweise über branchenspezifische Bedrohungsinformationen auf dem Laufenden, um ungewöhnliche Verhaltensweisen und Bedrohungssignaturen in Ihren Konten zu erkennen. [Amazon Inspector](#) hält automatisch eine Datenbank mit den CVEs für seine kontinuierlichen Scanfunktionen verwendeten Daten auf dem neuesten Stand. Sowohl [AWS WAF](#) als auch [AWS Shield Advanced](#) bieten verwaltete Regelgruppen, die automatisch aktualisiert werden, wenn neue Bedrohungen auftauchen.

Informationen zum automatisierten Flottenmanagement und Patching finden Sie unter [Säule „Operative Exzellenz“ – Well-Architected-Framework](#)

### Implementierungsschritte

- Abonnieren Sie Updates für Bedrohungsinformationen, die für Ihr Unternehmen und Ihre Branche relevant sind. Abonnieren Sie die AWS -Sicherheitsberichte.
- Erwägen Sie die Einführung von Diensten wie Amazon GuardDuty und Amazon Inspector, die neue Bedrohungsinformationen automatisch integrieren.
- Erstellen Sie eine Flottenmanagement- und Patching-Strategie, die sich an den bewährten Methoden der der Säule „Operative Exzellenz“ des Well-Architected-Framework“ orientiert.

### Ressourcen

Zugehörige bewährte Methoden:

- [SEC01-BP07 Identifizieren Sie Bedrohungen und priorisieren Sie Abhilfemaßnahmen mithilfe eines Bedrohungsmodells](#)
- [OPS01-BP05 Bewerten Sie die Bedrohungslandschaft](#)
- [OPS11-BP01 Haben Sie einen Prozess zur kontinuierlichen Verbesserung](#)

## SEC01-BP05 Reduzieren Sie den Umfang des Sicherheitsmanagements

Stellen Sie fest, ob Sie Ihren Sicherheitsbereich reduzieren können, indem Sie AWS Dienste verwenden, bei denen die Verwaltung bestimmter Kontrollen auf AWS (verwaltete Dienste) verlagert wird. Mit diesen Services können Sie Ihre Wartungsaufgaben im Bereich Sicherheit reduzieren, z. B. die Bereitstellung der Infrastruktur, die Einrichtung von Software, Patches oder Sicherungen.

Gewünschtes Ergebnis: Sie berücksichtigen den Umfang Ihres Sicherheitsmanagements, wenn Sie AWS Dienste für Ihren Workload auswählen. Die Kosten für Verwaltungsaufwand und Wartungsaufgaben (die Gesamtbetriebskosten oder TCO) werden zusätzlich zu anderen Well-Architected-Überlegungen gegen die Kosten der von Ihnen ausgewählten Services abgewogen. Sie beziehen die AWS Kontroll- und Compliance-Dokumentation in Ihre Kontrollbewertungs- und Überprüfungsverfahren ein.

Typische Anti-Muster:

- Bereitstellung von Workloads ohne gründliches Verständnis des Modells der geteilten Verantwortung für die von Ihnen ausgewählten Services
- Hosten von Datenbanken und anderen Technologien auf virtuellen Maschinen, ohne einen entsprechenden verwalteten Service evaluiert zu haben
- Nichtberücksichtigung von Sicherheitsverwaltungsaufgaben bei den Gesamtbetriebskosten des Hostings von Technologien auf virtuellen Maschinen im Vergleich zu verwalteten Serviceoptionen

Vorteile der Nutzung dieser bewährten Methode: Der Einsatz von verwalteten Services kann Ihren Gesamtaufwand für die Verwaltung der betrieblichen Sicherheitskontrollen verringern, was Ihre Sicherheitsrisiken und Gesamtbetriebskosten reduzieren kann. Die Zeit, die Sie sonst für bestimmte Sicherheitsaufgaben aufwenden müssten, können Sie in Aufgaben investieren, die Ihrem Unternehmen einen größeren Nutzen bringen. Verwaltete Services können auch den Umfang Ihrer Compliance-Anforderungen reduzieren, indem sie einige Kontrollanforderungen in AWS verlagern.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Mittel

Implementierungsleitfaden

Es gibt mehrere Möglichkeiten, wie Sie die Komponenten Ihrer Workload in AWS integrieren können. Die Installation und Ausführung von Technologien auf EC2 Amazon-Instances erfordert häufig, dass Sie den größten Teil der gesamten Sicherheitsverantwortung übernehmen. Um den Aufwand für die Durchführung bestimmter Kontrollen zu verringern, sollten Sie AWS Managed

Services identifizieren, die Ihren Teil des Modells der gemeinsamen Verantwortung einschränken, und sich darüber informieren, wie Sie sie in Ihrer bestehenden Architektur einsetzen können. [Beispiele hierfür sind die Verwendung des Amazon Relational Database Service \(AmazonRDS\) für die Bereitstellung von Datenbanken, Amazon Elastic Kubernetes Service \(AmazonEKS\) oder AmazonElastic Container Service \(AmazonECS\) für die Orchestrierung von Containern oder die Verwendung serverloser Optionen.](#) Überlegen Sie bei der Entwicklung neuer Anwendungen, welche Services dazu beitragen können, den Zeit- und Kostenaufwand für die Implementierung und Verwaltung von Sicherheitskontrollen zu reduzieren.

Auch Compliance-Anforderungen können bei der Auswahl von Services eine Rolle spielen. Managed Services können die Einhaltung einiger Anforderungen auf Folgendes verlagern. AWS Erkundigen Sie sich mit Ihrem Compliance-Team darüber, inwieweit es sich mit der Prüfung der Aspekte der von Ihnen betriebenen und verwalteten Dienste sowie mit der Annahme von Controllerklärungen in den entsprechenden AWS Prüfberichten auskennt. Sie können die gefundenen Prüfartefakte Ihren Prüfern oder Aufsichtsbehörden als Nachweis für AWS Sicherheitskontrollen zur Verfügung stellen. [AWS Artifact](#) Sie können bei der Gestaltung Ihrer Architektur auch die in einigen AWS Prüfartefakten enthaltenen Hinweise zur Verantwortung sowie die Richtlinien zur [Einhaltung der AWS Kundenvorschriften verwenden](#). Dieser Leitfaden hilft Ihnen, die zusätzlichen Sicherheitskontrollen zu bestimmen, die Sie einrichten sollten, um die spezifischen Anwendungsfälle Ihres Systems zu unterstützen.

Wenn Sie Managed Services verwenden, sollten Sie mit dem Prozess der Aktualisierung ihrer Ressourcen auf neuere Versionen vertraut sein (z. B. mit der Aktualisierung der Version einer von Amazon RDS verwalteten Datenbank oder einer Programmiersprachen-Runtime für eine AWS Lambda Funktion). Auch wenn der verwaltete Service diesen Vorgang für Sie durchführt, sind Sie für die Konfiguration des Zeitpunkts der Aktualisierung und die Auswirkungen auf Ihren Betrieb selbst verantwortlich. Tools wie [AWS Health](#) können Ihnen helfen, diese Updates in Ihren Umgebungen zu verfolgen und zu verwalten.

## Implementierungsschritte

1. Bewerten Sie die Komponenten Ihrer Workload, die durch einen verwalteten Service ersetzt werden können.
  - a. Wenn Sie einen Workload auf migrieren AWS, sollten Sie bei der Entscheidung, ob Sie Ihren Workload rehosten, refaktorisieren, plattformübergreifend, neu aufbauen oder ersetzen sollten, den geringeren Verwaltungsaufwand (Zeit und Kosten) und die Verringerung des Risikos berücksichtigen. Manchmal können zusätzliche Investitionen zu Beginn einer Migration auf lange Sicht erhebliche Einsparungen bringen.

2. Erwägen Sie die Implementierung von Managed Services wie AmazonRDS, anstatt Ihre eigenen Technologiebereitstellungen zu installieren und zu verwalten.
3. Finden Sie anhand der Leitlinien AWS Artifact zur Verantwortung heraus, welche Sicherheitskontrollen Sie für Ihren Workload einrichten sollten.
4. Führen Sie eine Bestandsaufnahme der verwendeten Ressourcen und bleiben Sie up-to-date bei neuen Services und Ansätzen, um neue Möglichkeiten zur Reduzierung des Umfangs zu identifizieren.

## Ressourcen

### Zugehörige bewährte Methoden:

- [PERF02-BP01 Wählen Sie die besten Rechenoptionen für Ihren Workload](#)
- [PERF03-BP01 Verwenden Sie einen speziell entwickelten Datenspeicher, der Ihre Datenzugriffs- und Speicheranforderungen am besten unterstützt](#)
- [SUS05-BP03 Verwenden Sie verwaltete Dienste](#)

### Zugehörige Dokumente:

- [Geplante Lebenszyklusereignisse für AWS Health](#)

### Zugehörige Tools:

- [AWS Health](#)
- [AWS Artifact](#)
- [AWS Customer Compliance Guides](#)

### Zugehörige Videos:

- [Wie migriere ich zu einer Amazon RDS - oder Aurora My SQL DB-Instance mit AWS DMS?](#)
- [AWS re:Invent 2023 — Verwalten Sie Ereignisse im Ressourcenlebenszyklus in großem Umfang mit AWS Health](#)

## SEC01-BP06 Automatisieren Sie die Implementierung von Standardsicherheitskontrollen

Wenden Sie bei der Entwicklung und Implementierung von Sicherheitskontrollen, die in Ihren Umgebungen zum Standard gehören, moderne DevOps Verfahren an. AWS Definieren Sie standardmäßige Sicherheitskontrollen und -konfigurationen mithilfe von Infrastructure as Code (IaC) -Vorlagen, erfassen Sie Änderungen in einem Versionskontrollsystem, testen Sie Änderungen als Teil einer CI/CD-Pipeline und automatisieren Sie die Implementierung von Änderungen in Ihren Umgebungen. AWS

Gewünschtes Ergebnis: IaC-Vorlagen erfassen standardisierte Sicherheitskontrollen und übergeben sie an ein Versionskontrollsystem. CI/CD-Pipelines befinden sich an Stellen, an denen Änderungen erkannt und das Testen und Bereitstellen Ihrer Umgebungen automatisiert werden. AWS Mechanismen zum Integritätsschutz erkennen und warnen vor Fehlkonfigurationen in Vorlagen, bevor die Bereitstellung erfolgt. Workloads werden in Umgebungen bereitgestellt, in denen Standardkontrollen vorhanden sind. Die Teams können genehmigte Servicekonfigurationen über einen Selfservice-Mechanismus bereitstellen. Die Strategien zur Gewährleistung der Sicherheit bei der Sicherung und Wiederherstellung von Kontrollkonfigurationen, Skripten und zugehörigen Daten sind etabliert.

Typische Anti-Muster:

- Manuelle Änderungen an Ihren Standard-Sicherheitskontrollen über eine Webkonsole oder eine Befehlszeilenschnittstelle.
- Sich darauf verlassen, dass die einzelnen Workload-Teams die von einem zentralen Team festgelegten Kontrollen manuell umsetzen.
- Sich auf ein zentrales Sicherheitsteam verlassen, das auf Anfrage eines Workload-Teams Kontrollen auf Workload-Ebene bereitstellt.
- Erlauben, dass dieselben Personen oder Teams Automatisierungsskripte für die Sicherheitskontrolle entwickeln, testen und bereitstellen, ohne dass eine angemessene Aufgabentrennung oder gegenseitige Kontrolle stattfindet.

Vorteile der Nutzung dieser bewährten Methode: Die Verwendung von Vorlagen zur Definition Ihrer Standard-Sicherheitskontrollen ermöglicht es Ihnen, Änderungen im Laufe der Zeit mithilfe eines Versionskontrollsystems zu verfolgen und zu vergleichen. Der Einsatz von Automatisierung zum Testen und Bereitstellen von Änderungen schafft Standardisierung und Vorhersehbarkeit, erhöht die Chancen auf eine erfolgreiche Bereitstellung und reduziert manuelle, sich wiederholende Aufgaben. Durch die Bereitstellung eines Selfservice-Mechanismus für Workload-Teams zur Bereitstellung



genehmigter Services und Konfigurationen wird das Risiko von Fehlkonfigurationen und Missbrauch verringert. Das hilft ihnen auch dabei, Kontrollen früher in den Entwicklungsprozess einzubauen.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Mittel

### Implementierungsleitfaden

Wenn Sie die unter [SEC01-BP01 Separate Workloads mithilfe von Konten](#) beschriebenen Verfahren befolgen, werden Sie am Ende mehrere AWS-Konten für verschiedene Umgebungen verwenden, die Sie verwalten. AWS Organizations Auch wenn jede dieser Umgebungen und Workloads unterschiedliche Sicherheitskontrollen erfordert, können Sie einige Sicherheitskontrollen in Ihrer Organisation standardisieren. Beispiele hierfür sind die Integration zentraler Identitätsanbieter, die Definition von Netzwerken und Firewalls und die Konfiguration von Standardorten für die Speicherung und Analyse von Protokollen. Analog zur Anwendung von Infrastructure as Code (IaC) zur Anwendung der gleichen strikten Vorgehensweise bei der Entwicklung von Anwendungscode auf die Bereitstellung der Infrastruktur können Sie IaC auch zur Definition und Bereitstellung Ihrer Standard-Sicherheitskontrollen verwenden.

Definieren Sie Ihre Sicherheitskontrollen nach Möglichkeit deklarativ, wie z. B. in [AWS CloudFormation](#), und speichern Sie sie in einem Versionskontrollsystem. Verwenden Sie DevOps Methoden, um die Implementierung Ihrer Steuerungen zu automatisieren, um besser vorhersehbare Versionen zu erzielen. Automatisieren Sie Tests mithilfe von Tools wie [AWS CloudFormation Guard](#) und erkennen Sie Abweichungen zwischen Ihren eingesetzten Steuerungen und Ihrer gewünschten Konfiguration. Sie können Services wie [AWS CodePipeline](#), [AWS CodeBuild](#) und [AWS CodeDeploy](#) verwenden, um eine CI/CD-Pipeline zu erstellen. Beachten Sie die Hinweise unter [Organisieren Ihrer AWS Umgebung mithilfe mehrerer Konten](#), um diese Dienste in eigenen Konten zu konfigurieren, die von anderen Bereitstellungspipelines getrennt sind.

Sie können auch Vorlagen definieren, um die Definition und Bereitstellung AWS-Konten, Dienste und Konfigurationen zu standardisieren. Diese Technik ermöglicht es einem zentralen Sicherheitsteam, diese Definitionen zu verwalten und sie den Workload-Teams über einen Selfservice-Ansatz zur Verfügung zu stellen. Eine Möglichkeit, dies zu erreichen, ist die Verwendung von [Service Catalog](#), wo Sie Vorlagen als Produkte veröffentlichen können, die Workload-Teams in ihre eigenen Pipeline-Bereitstellungen einbinden können. Wenn Sie [AWS Control Tower](#) verwenden, sind einige Vorlagen und Kontrollen als Ausgangspunkt verfügbar. Control Tower bietet zudem die Funktion [Account Factory](#), mit der Workload-Teams neue AWS-Konten -Konten unter Verwendung der von Ihnen definierten Standards erstellen können. Mit dieser Funktion sind Sie nicht mehr auf ein zentrales Team angewiesen, das neue Konten genehmigt und anlegt, wenn diese von Ihren Workload-Teams

als notwendig erachtet werden. Sie benötigen diese Konten möglicherweise, um verschiedene Workload-Komponenten zu isolieren, z. B. aufgrund ihrer Funktion, der Sensibilität der verarbeiteten Daten oder ihres Verhaltens.

### Implementierungsschritte

1. Legen Sie fest, wie Sie Ihre Vorlagen in einem Versionskontrollsystem speichern und pflegen wollen.
2. Erstellen Sie CI/CD-Pipelines zum Testen und Bereitstellen Ihrer Vorlagen. Definieren Sie Tests, um zu prüfen, ob Fehlkonfigurationen vorliegen und ob die Vorlagen den Standards Ihres Unternehmens entsprechen.
3. Erstellen Sie einen Katalog mit standardisierten Vorlagen, die Workload-Teams entsprechend Ihren Anforderungen bereitstellen AWS-Konten und Services bereitstellen können.
4. Implementieren Sie sichere Sicherungs- und Wiederherstellungsstrategien für die Konfiguration Ihrer Kontrollen, Skripte und zugehörigen Daten.

### Ressourcen

Zugehörige bewährte Methoden:

- [OPS05-BP01 Verwenden Sie die Versionskontrolle](#)
- [OPS05-BP04 Verwenden Sie Build- und Deployment-Management-Systeme](#)
- [REL08-BP05 Implementieren Sie Änderungen mit Automatisierung](#)
- [SUS06-BP01 Wenden Sie Methoden an, mit denen schnell Verbesserungen der Nachhaltigkeit eingeführt werden können](#)

Zugehörige Dokumente:

- [Organisieren Sie Ihre AWS Umgebung mithilfe mehrerer Konten](#)

Zugehörige Beispiele:

- [Automatisieren Sie die Kontoerstellung und die Bereitstellung von Ressourcen mithilfe von Service Catalog AWS Organizations, und AWS Lambda](#)
- [Stärken Sie die DevOps Pipeline und schützen Sie Daten mit AWS Secrets Manager, AWS KMS, und AWS Certificate Manager](#)

## Zugehörige Tools:

- [AWS CloudFormation Guard](#)
- [Landezone Accelerator aktiviert AWS](#)

SEC01-BP07 Identifizieren Sie Bedrohungen und priorisieren Sie Abhilfemaßnahmen mithilfe eines Bedrohungsmodells

Führen Sie eine Bedrohungsmodellierung durch, um ein up-to-date Verzeichnis potenzieller Bedrohungen und der damit verbundenen Abhilfemaßnahmen für Ihren Workload zu identifizieren und zu führen. Priorisieren Sie Ihre Bedrohungen und passen Sie Ihre Sicherheitskontrollen an, um zu verhindern, zu erkennen und zu reagieren. Überarbeiten und halten Sie diese Methoden im Kontext Ihrer Workload und der sich entwickelnden Sicherheitslandschaft aktuell.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Hoch

Implementierungsleitfaden

Was versteht man unter Bedrohungsmodellierung?

„Bedrohungsmodellierung dient der Identifizierung, Kommunikation und dem Verständnis von Bedrohungen und Abhilfemaßnahmen im Kontext des Schutzes von etwas Wertvollem.“ — [Bedrohungsmodellierung für Anwendungen des Open Web Application Security Project \(OWASP\)](#)

Wozu dient die Bedrohungsmodellierung?

Systeme sind komplex und werden mit der Zeit immer komplexer und leistungsfähiger. Gleichzeitig liefern sie immer mehr geschäftlichen Wert und verbessern die Kundenzufriedenheit und -bindung. Dies bedeutet, dass Entscheidungen zum IT-Design immer mehr Anwendungsfälle berücksichtigen müssen. Diese Komplexität und die zunehmende Zahl der Anwendungsfälle macht unstrukturierte Konzepte ineffektiv, wenn es um das Erkennen und Bekämpfen von Bedrohungen geht. Stattdessen wird ein systematisches Konzept benötigt, das die potenziellen Bedrohungen für ein System auflisten und Abhilfemaßnahmen benennen und priorisieren kann, um sicherzustellen, dass die begrenzten Ressourcen einer Organisation in maximaler Weise in der Lage sind, die Sicherheitslage des Systems insgesamt zu verbessern.

Die Bedrohungsmodellierung dient zum Aufbau eines solchen systematischen Konzepts, damit Probleme frühzeitig im Designprozess erkannt und angegangen werden können, so lange Abhilfemaßnahmen noch mit niedrigen relativen Kosten und geringem Aufwand verbunden

sind, was später im Lebenszyklus nicht mehr der Fall ist. Dieses Konzept entspricht dem Branchenprinzip des [Shift-Left-Sicherheitsansatzes](#). Letztendlich ist die Bedrohungsmodellierung in den Risikomanagementprozess einer Organisation integriert und hilft mit einem auf Bedrohungen ausgerichteten Konzept bei Entscheidungen dazu, welche Kontrollmechanismen zu implementieren sind.

Wann sollte eine Bedrohungsmodellierung durchgeführt werden?

Beginnen Sie mit der Bedrohungsmodellierung so früh wie möglich im Lebenszyklus Ihrer Workload. Dies gibt Ihnen die benötigte Flexibilität im Umgang mit den identifizierten Bedrohungen. Wie bei Softwarebugs gilt auch hier: Je früher Sie Bedrohungen identifizieren, desto kostengünstiger ist es, sie zu beheben. Ein Bedrohungsmodell ist ein lebendiges Dokument, das stetig weiterentwickelt werden sollte, während sich Ihre Workloads verändern. Überprüfen Sie regelmäßig Ihre Bedrohungsmodelle, vor allem bei größeren Änderungen, bei Änderungen der Bedrohungslandschaft, oder wenn Sie neue Funktionen oder Services einführen.

Implementierungsschritte

Wie wird die Bedrohungsmodellierung durchgeführt?

Es gibt viele verschiedene Möglichkeiten zur Durchführung von Bedrohungsmodellierungen. Ähnlich wie bei Programmiersprachen gibt es Vor- und Nachteile und Sie sollten den Ansatz wählen, der für Sie am besten funktioniert. Ein Konzept besteht darin, mit [Shostack's 4 Question Frame for Threat Modeling](#) zu beginnen, das aus offenen Fragen besteht, die Ihre Bedrohungsmodellierung strukturieren:

1. Woran arbeiten wir?

Diese Frage dient dazu, das von Ihnen aufgebaute System sowie die sicherheitsrelevanten Details zu diesem System zu verstehen. Für die Beantwortung dieser Frage ist es üblich, ein Modell oder Diagramm zur Visualisierung dessen aufzustellen, was aufgebaut wird, etwa in Gestalt eines [Datenflussdiagramms](#). Das Aufschreiben von Annahmen und wichtigen Details zum System hilft ebenfalls beim Verständnis des Umfangs. So können sich alle am Bedrohungsmodell beteiligten Personen auf dasselbe konzentrieren und zeitaufwändige Umwege zu bestimmten out-of-scope Themen (einschließlich veralteter Versionen Ihres Systems) vermeiden. Wenn Sie beispielsweise eine Web-Anwendung erstellen, ist es wahrscheinlich nicht relevant, sich um die Bedrohungsmodellierung im Zusammenhang mit der Bootsequenz für Browser-Clients in vertrauenswürdigen Betriebssystemen zu kümmern, da Sie darauf ohnehin keinen Einfluss haben.

2. Was kann schief gehen?

Hier identifizieren Sie die Bedrohungen für Ihr System. Bedrohungen sind versehentliche oder beabsichtigte Handlungen oder Ereignisse, die unerwünschte Folgen haben und die Sicherheit Ihres Systems beeinträchtigen können. Ohne ein klares Verständnis dessen, was schief gehen kann, haben Sie keine Möglichkeit, etwas dagegen zu unternehmen.

Es gibt keine kanonische Liste dessen, was schief gehen kann. Die Erstellung dieser Liste erfordert Brainstorming und die Zusammenarbeit all Ihrer Teammitglieder und der [relevanten Beteiligten](#) an der Bedrohungsmodellierung. Sie können Ihr Brainstorming unterstützen, indem Sie ein Modell zur Identifizierung von Bedrohungen verwenden [STRIDE](#), das beispielsweise verschiedene Kategorien zur Bewertung vorschlägt: Spoofing, Manipulation, Ablehnung, Offenlegung von Informationen, Denial of Service und Erhöhung von Rechten. [Darüber hinaus können Sie das Brainstorming unterstützen, indem Sie sich bestehende Listen und Recherchen ansehen, um sich inspirieren zu lassen, darunter die Top 10, den Bedrohungskatalog und den OWASP Bedrohungskatalog Ihres Unternehmens. HiTrust](#)

### 3. Wie gehen wir damit um?

Wie schon bei der vorherigen Frage gibt es auch hier keine kanonische Liste möglicher Abhilfemaßnahmen. Die Inputs für diesen Schritt sind die identifizierten Bedrohungen, Akteure und Verbesserungsbereiche aus dem vorherigen Schritt.

Sicherheit und Compliance unterliegen der [geteilten Verantwortung zwischen Ihnen und AWS](#). Der Frage „Wie gehen wir damit um?“ sollte unbedingt die Frage „Wer ist für die Maßnahmen verantwortlich?“ angeschlossen werden. Wenn Sie wissen, wie Ihre Zuständigkeiten ausgewogen sind, können Sie Ihre Bedrohungsmodellierung auf die Abhilfemaßnahmen ausdehnen, die Sie kontrollieren können. Dabei handelt es sich in der Regel um eine Kombination aus AWS Dienstkonfigurationsoptionen und Ihren eigenen systemspezifischen Abhilfemaßnahmen. AWS

Was den AWS Teil der gemeinsamen Verantwortung angeht, werden Sie feststellen, dass die [AWS Services in den Geltungsbereich vieler Compliance-Programme fallen](#). Diese Programme helfen Ihnen dabei, die robusten Kontrollen zu verstehen, die AWS zur Aufrechterhaltung der Sicherheit und Compliance in der Cloud gelten. Die Prüfberichte dieser Programme stehen AWS Kunden unter zum Download zur Verfügung [AWS Artifact](#).

Unabhängig davon, welche AWS Dienste Sie nutzen, besteht immer ein gewisses Maß an Kundenverantwortung. Daher sollten Sie in Ihrem Bedrohungsmodell Maßnahmen zur Gefahrenabwehr berücksichtigen, die auf diese Aufgaben abgestimmt sind. Um die Sicherheitsvorkehrungen für die AWS Services selbst zu verringern, sollten Sie die

Implementierung von Sicherheitskontrollen in allen Bereichen in Betracht ziehen, darunter Bereiche wie Identitäts- und Zugriffsmanagement (Authentifizierung und Autorisierung), Datenschutz (im Speicher und bei der Übertragung), Infrastruktursicherheit, Protokollierung und Überwachung. Die Dokumentation für jeden AWS Dienst enthält ein [eigenes Sicherheitskapitel, das Anleitungen zu den Sicherheitskontrollen](#) enthält, die als Risikominderung in Betracht gezogen werden sollten. Wichtig ist, dass Sie den Code, den Sie schreiben, und dessen Abhängigkeiten berücksichtigen und an Kontrollen denken, die Sie für den Umgang mit den damit verbundenen Bedrohungen implementieren können. Bei diesen Kontrollen könnte es sich um Dinge wie [Eingabevalidierung](#), [Sitzungsabwicklung](#) und [Umgang mit Grenzen](#) handeln. Oft ist der Löwenanteil der Bedrohungen mit benutzerdefiniertem Code verbunden, konzentrieren Sie sich also besonders darauf.

#### 4. Haben wir gute Arbeit geleistet?

Ihr Team und die Organisation verfolgen das Ziel, die Qualität der Bedrohungsmodelle und die Geschwindigkeit zu verbessern, mit der Sie die Bedrohungsmodellierung im Laufe der Zeit durchführen. Diese Verbesserungen werden durch eine Kombination von Praxis, Lernen, Lehren und Prüfen ermöglicht. Um dies zu vertiefen und praktisch umzusetzen, sollten Sie und Ihr Team den Trainingskurs zum Thema [Korrekte Bedrohungsmodellierung für Builder](#) oder den dazugehörigen [Workshop](#) absolvieren. Wenn Sie außerdem nach Anleitungen suchen, wie Sie die Bedrohungsmodellierung in den Lebenszyklus der Anwendungsentwicklung Ihres Unternehmens integrieren können, finden Sie im AWS Sicherheits-Blog den Beitrag [How to Approach Threat Modeling](#).

#### Threat Composer

Als Unterstützung und Anleitung bei der Erstellung von Bedrohungsmodellen sollten Sie den Einsatz des [Threat Composer-Tools](#) in Betracht ziehen, das darauf abzielt, time-to-value bei der Bedrohungsmodellierung weniger Zeit zu verlieren. Das Tool hilft Ihnen bei den folgenden Aufgaben:

- Verfassen nützlicher, an [Bedrohungsgrammatik](#) ausgerichtete Bedrohungsanweisungen, die in einem natürlichen, nicht-linearen Arbeitsablauf funktionieren.
- Generieren Sie ein für Menschen lesbares Bedrohungsmodell.
- Generieren Sie ein maschinenlesbares Bedrohungsmodell, damit Sie Bedrohungsmodelle wie Code behandeln können.
- Mit dem Insights-Dashboard können Sie schnell Bereiche identifizieren, in denen die Qualität und die Abdeckung verbessert werden müssen.

Für weitere Informationen rufen Sie Threat Composer auf und wechseln Sie zum systemdefinierten Beispielarbeitsbereich.

## Ressourcen

Zugehörige bewährte Methoden:

- [SEC01-BP03 Kontrollziele identifizieren und validieren](#)
- [SEC01-BP04 Bleiben Sie über Sicherheitsbedrohungen und Empfehlungen auf dem Laufenden](#)
- [SEC01-BP05 Reduzieren Sie den Umfang des Sicherheitsmanagements](#)
- [SEC01-BP08 Regelmäßige Evaluierung und Implementierung neuer Sicherheitsdienste und -funktionen](#)

Zugehörige Dokumente:

- [Wie gehen Sie mit der Bedrohungsmodellierung um \(AWS Security Blog\)](#)
- [NIST: Leitfaden zur datenzentrierten Modellierung von Systembedrohungen](#)

Zugehörige Videos:

- [AWS Summit ANZ 2021 — Wie geht man mit der Bedrohungsmodellierung um](#)
- [AWS Summit ANZ 2022 — Skalierung der Sicherheit — Optimieren Sie für eine schnelle und sichere Bereitstellung](#)

Zugehörige Schulungen:

- [Bedrohungsmodellierung ist der richtige Weg für Entwickler — virtuelles AWS Skill Builder-Training zum Selbststudium](#)
- [Bedrohungsmodellierung — der richtige Weg für Bauherren — Workshop AWS](#)

Zugehörige Tools:

- [Threat Composer](#)

## SEC01-BP08 Regelmäßige Evaluierung und Implementierung neuer Sicherheitsdienste und -funktionen

Evaluieren und implementieren Sie Sicherheitservices und -funktionen von AWS AWS Partnern, die Ihnen helfen, den Sicherheitsstatus Ihrer Workloads zu verbessern.

Gewünschtes Ergebnis: Sie verfügen über ein Standardverfahren, das Sie über neue Funktionen und Services informiert, die von AWS und AWS Partnern veröffentlicht wurden. Sie bewerten, wie sich diese neuen Funktionen auf das Design der aktuellen und neuen Kontrollen für Ihre Umgebungen und Workloads auswirken.

Typische Anti-Muster:

- Sie abonnieren keine AWS Blogs und RSS Feeds, um schnell von relevanten neuen Funktionen und Diensten zu erfahren
- Sie verlassen sich auf Nachrichten und Updates über Sicherheitservices und Features aus zweiter Hand
- Sie ermutigen AWS Benutzer in Ihrer Organisation nicht, sich über die neuesten Updates auf dem Laufenden zu halten

Vorteile der Nutzung dieser bewährten Methode: Indem Sie sich über neue Sicherheitservices und Features auf dem Laufenden halten, können Sie fundierte Entscheidungen über die Implementierung von Kontrollen in Ihren Cloud-Umgebungen und Workloads treffen. Diese Quellen tragen dazu bei, das Bewusstsein für die sich entwickelnde Sicherheitslandschaft zu schärfen und dafür, wie AWS Dienste zum Schutz vor neuen und aufkommenden Bedrohungen eingesetzt werden können.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Niedrig

Implementierungsleitfaden

AWS informiert Kunden über verschiedene Kanäle über neue Sicherheitsdienste und -funktionen:

- [AWS Was ist neu](#)
- [AWS Nachrichten-Blog](#)
- [AWS -Blog zum Thema Sicherheit](#)
- [AWS -Sicherheitsberichte](#)
- [Überblick über die AWS -Dokumentation](#)



Mit Amazon Simple Notification Service (AmazonSNS) können Sie ein Thema mit [AWS täglichen Feature-Updates](#) abonnieren, um eine umfassende tägliche Zusammenfassung der Updates zu erhalten. Einige Sicherheitsdienste, wie [Amazon GuardDuty](#) und [AWS Security Hub](#), bieten eigene SNS Themen an, um über neue Standards, Erkenntnisse und andere Updates für diese speziellen Dienste auf dem Laufenden zu bleiben.

Neue Services und Features werden auch auf [Konferenzen, Veranstaltungen und Webinaren](#), die jedes Jahr rund um den Globus stattfinden, angekündigt und im Detail beschrieben. Besonders interessant ist dabei die jährliche Sicherheitskonferenz [AWS re:Inforce](#) und die breiter angelegte Konferenz [AWS re:Invent](#). [Auf den zuvor genannten AWS Nachrichtenkanälen werden diese Konferenzankündigungen zu Sicherheit und anderen Diensten veröffentlicht. Sie können sich auch online im Veranstaltungskanal unter „Veranstaltungen“ die ausführlichen und informativen Breakout-Sessions ansehen.](#)[AWS YouTube](#)

Sie können auch Ihr [AWS-Konto -Team](#) nach den neuesten Updates und Empfehlungen für Sicherheitsservices fragen. Sie können Ihr Team über das [Verkaufssupport-Formular](#) erreichen, wenn Ihnen dessen direkte Kontaktinformationen nicht vorliegen. Wenn Sie [AWS Enterprise Support abonniert haben](#), erhalten Sie ebenfalls wöchentliche Updates von Ihrem Technical Account Manager (TAM) und können ein regelmäßiges Überprüfungsgespräch mit diesem vereinbaren.

### Implementierungsschritte

1. Abonnieren Sie die verschiedenen Blogs und Bulletins mit Ihrem RSS Lieblingsleser oder das Thema „Tägliche Updates“. SNS
2. Finden Sie heraus, an welchen AWS Veranstaltungen Sie teilnehmen sollten, um sich aus erster Hand über neue Funktionen und Dienste zu informieren.
3. Vereinbaren Sie Besprechungen mit Ihrem AWS-Konto Team für alle Fragen zur Aktualisierung von Sicherheitsdiensten und -funktionen.
4. Erwägen Sie, Enterprise Support zu abonnieren, um sich regelmäßig mit einem Technical Account Manager beraten zu lassen (TAM).

### Ressourcen

Zugehörige bewährte Methoden:

- [PERF01-BP01 Erfahren Sie mehr über die verfügbaren Cloud-Dienste und -Funktionen und machen Sie sich damit vertraut](#)
- [COST01-BP07 Bleiben Sie auf dem Laufenden up-to-date mit neuen Service-Releases](#)

# Identity and Access Management

## Fragen

- [SEC2. Was ist bei der Verwaltung der Authentifizierung für Personen und Rechner zu beachten?](#)
- [SEC3. Wie werden Berechtigungen für Personen und Computer verwaltet?](#)

## SEC2. Was ist bei der Verwaltung der Authentifizierung für Personen und Rechner zu beachten?

Es gibt zwei Arten von Identitäten, die Sie beim Betrieb sicherer Workloads verwalten müssen. AWS Wenn Sie verstehen, welche Arten von Identitäten Sie verwalten und Zugriff gewähren müssen, können Sie sicherstellen, dass die richtigen Identitäten unter den richtigen Bedingungen Zugriff auf die richtigen Ressourcen haben.

**Menschliche Identitäten:** Ihre Administratoren, Entwickler, Betreiber und Endbenutzer benötigen eine Identität, um auf Ihre AWS Umgebungen und Anwendungen zugreifen zu können. Dies sind Mitglieder Ihrer Organisation oder externe Benutzer, mit denen Sie zusammenarbeiten und die über einen Webbrowser, eine Client-Anwendung oder interaktive Befehlszeilentools mit Ihren AWS Ressourcen interagieren.

**Maschinenidentitäten:** Ihre Dienstanwendungen, Betriebstools und Workloads benötigen eine Identität, um Anfragen an AWS Dienste zu stellen, z. B. um Daten zu lesen. Zu diesen Identitäten gehören Maschinen, die in Ihrer AWS Umgebung ausgeführt werden, z. B. EC2 Amazon-Instances oder AWS Lambda -Funktionen. Sie können auch Maschinenidentitäten für externe Parteien verwalten, die Zugriff benötigen. Darüber hinaus benötigen möglicherweise auch Computer außerhalb AWS dieser Systeme Zugriff auf Ihre AWS Umgebung.

## Bewährte Methoden

- [SEC02-BP01 Verwenden Sie starke Anmeldemechanismen](#)
- [SEC02-BP02 Temporäre Anmeldeinformationen verwenden](#)
- [SEC02-BP03 Geheimnisse sicher speichern und verwenden](#)
- [SEC02-BP04 Verlassen Sie sich auf einen zentralen Identitätsanbieter](#)
- [SEC02-BP05 Regelmäßige Prüfung und Rotation der Anmeldedaten](#)
- [SEC02-BP06 Benutzergruppen und Attribute einsetzen](#)

## SEC02-BP01 Verwenden Sie starke Anmeldemechanismen

Anmeldungen (Authentifizierung mithilfe von Anmeldeinformationen) können Risiken bergen, wenn Mechanismen wie die Multi-Faktor-Authentifizierung (MFA) nicht verwendet werden, insbesondere in Situationen, in denen Anmeldeinformationen versehentlich offengelegt wurden oder leicht zu erraten sind. Verwenden Sie starke Anmeldemechanismen, um diese Risiken zu verringern, indem Sie strenge Kennwortrichtlinien vorschreiben. MFA

Gewünschtes Ergebnis: Reduzieren Sie das Risiko eines unbeabsichtigten Zugriffs auf Anmeldeinformationen, AWS indem Sie starke Anmeldemechanismen für [AWS Identity and Access Management \(IAM\)](#) Benutzer, den [AWS-Konto Root-Benutzer AWS IAM Identity Center](#) (Nachfolger von AWS Single Sign-On) und externe Identitätsanbieter verwenden. Das bedeutet MFA, strenge Passwortrichtlinien vorzuschreiben, durchzusetzen und ungewöhnliches Anmeldeverhalten zu erkennen.

Typische Anti-Muster:

- Keine Durchsetzung einer sicheren Passwortrichtlinie für Ihre Identitäten, einschließlich komplexer Passwörter und. MFA
- Gemeinsame Nutzung derselben Anmeldeinformationen durch mehrere Benutzer.
- Keine Verwendung von detektivischen Kontrollen für verdächtige Anmeldevorgänge.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Hoch

Implementierungsleitfaden

Es gibt viele Möglichkeiten zur Anmeldung für menschliche Identitäten bei AWS. Es hat sich AWS bewährt, sich bei der Authentifizierung auf einen zentralen Identitätsanbieter zu verlassen, der den Verbund (direkte Verbindung oder Verwendung AWS IAM Identity Center) verwendet. AWS In diesem Fall sollten Sie einen sicheren Anmeldeprozess mit Ihrem Identitätsanbieter oder Microsoft Active Directory einrichten.

Wenn Sie einen zum ersten Mal öffnen AWS-Konto, beginnen Sie mit einem AWS-Konto Root-Benutzer. Sie sollten den Root-Benutzer nur verwenden, um den Zugriff für Ihre Benutzer einzurichten (und für [Aufgaben, für die der Root-Benutzer erforderlich ist](#)). Es ist wichtig, dass Sie den MFA Root-Benutzer sofort nach dem Öffnen Ihres Kontos aktivieren AWS-Konto und den Root-Benutzer anhand des AWS [Best-Practice-Leitfadens](#) sichern.

Wenn Sie Benutzer in diesem Dienst erstellen AWS IAM Identity Center, sichern Sie den Anmeldevorgang in diesem Dienst. Für Verbraucheridentitäten können Sie [Amazon Cognito-Benutzerpools](#) verwenden und den Anmeldevorgang in diesem Service sichern, oder Sie können einen der Identitätsanbieter verwenden, die Amazon Cognito-Benutzerpools unterstützen.

Wenn Sie Benutzer [AWS Identity and Access Management \(IAM\)](#) verwenden, würden Sie den Anmeldevorgang mit sichern. IAM

Unabhängig vom Anmeldeverfahren ist es wichtig, eine strenge Anmelderichtlinie durchzusetzen.

### Implementierungsschritte

Es folgen allgemeine Empfehlungen für starke Anmeldeverfahren. Die tatsächlichen Einstellungen, die Sie konfigurieren, sollten Ihren Unternehmensrichtlinien entsprechen oder einen Standard wie [NIST800-63](#) verwenden.

- Erforderlich MFA. Es ist eine [IAM bewährte Methode, die MFA für menschliche Identitäten und Workloads erforderlich](#) ist. Die Aktivierung MFA bietet eine zusätzliche Sicherheitsebene, bei der Benutzer Anmeldeinformationen und ein Einmalpasswort (OTP) oder eine kryptografisch verifizierte und generierte Zeichenfolge von einem Hardwaregerät eingeben müssen.
- Verlangen Sie eine Mindestlänge für Passwörter als primären Faktor für die Passwortstärke.
- Verlangen Sie Passwortkomplexität, um das Erraten von Passwörtern zu erschweren.
- Ermöglichen Sie Benutzern, ihre eigenen Passwörter zu ändern.
- Erstellen Sie individuelle Identitäten anstelle gemeinsam genutzter Anmeldeinformationen. Da Sie individuelle Identitäten erstellen, können Sie jedem Benutzer eindeutige Anmeldeinformationen zuordnen. Individuelle Benutzer bieten die Möglichkeit, die Aktivität der einzelnen Benutzer zu prüfen.

### IAM Empfehlungen von Identity Center:

- IAM Identity Center bietet bei Verwendung des Standardverzeichnisses eine vordefinierte [Kennwortrichtlinie](#), die Anforderungen an die Länge, Komplexität und Wiederverwendung von Passwörtern festlegt.
- [Aktivieren MFA](#) und konfigurieren Sie die kontextsensitive oder Always-On-Einstellung für den Fall MFA, dass die Identitätsquelle das Standardverzeichnis oder AD Connector AWS Managed Microsoft AD ist.
- Erlauben Sie Benutzern, ihre eigenen Geräte zu [registrieren. MFA](#)

## Empfehlungen für Verzeichnisse der Amazon Cognito-Benutzerpools:

- Konfigurieren Sie die Einstellungen für die [Passwortstärke](#).
- MFA für Benutzer [erforderlich](#).
- Verwenden Sie die [erweiterten Sicherheitseinstellungen](#) der Amazon Cognito-Benutzerpools für Features wie die [adaptive Authentifizierung](#), mit der verdächtige Anmeldungen blockiert werden können.

## IAM Benutzerempfehlungen:

- Idealerweise verwenden Sie IAM Identity Center oder Direct Federation. Möglicherweise benötigen Sie jedoch IAM Benutzer. [Legen Sie in diesem Fall eine Kennwortrichtlinie](#) für IAM Benutzer fest. Sie können die Passwortrichtlinie verwenden, um Anforderungen wie die Mindestlänge zu definieren oder ob das Passwort nicht-alphanumerische Zeichen beinhalten sollte.
- Erstellen Sie eine IAM Richtlinie, um die [MFAAnmeldung zu erzwingen](#), sodass Benutzer ihre eigenen Passwörter und MFA Geräte verwalten können.

## Ressourcen

### Zugehörige bewährte Methoden:

- [SEC02-BP03 Geheimnisse sicher speichern und verwenden](#)
- [SEC02-BP04 Verlassen Sie sich auf einen zentralen Identitätsanbieter](#)
- [SEC03-BP08 Teilen Sie Ressourcen sicher innerhalb Ihrer Organisation](#)

### Zugehörige Dokumente:

- [AWS IAM Identity Center Passwort-Richtlinie](#)
- [IAM Passwortrichtlinie für Benutzer](#)
- [Einstellung des AWS-Konto Root-Benutzerpassworts](#)
- [Amazon Cognito-Passwortrichtlinie](#)
- [AWS Anmeldeinformationen](#)
- [IAM Bewährte Methoden im Bereich Sicherheit](#)

### Zugehörige Videos:

- [Verwaltung von Benutzerberechtigungen in großem Umfang mit AWS IAM Identity Center](#)
- [Beherrschen der Identität auf jeder Ebene](#)

## SEC02-BP02 Temporäre Anmeldeinformationen verwenden

Bei Authentifizierungen jeder Art, sollten am besten temporäre anstelle langfristiger Anmeldeinformationen verwendet werden, um Risiken zu reduzieren oder zu eliminieren, etwa durch die unbeabsichtigte Offenlegung, die Weitergabe oder den Diebstahl von Anmeldeinformationen.

Gewünschtes Ergebnis: Um das Risiko langfristiger Anmeldeinformationen zu verringern, sollten Sie nach Möglichkeit sowohl für menschliche als auch für maschinelle Identitäten temporäre Anmeldeinformationen verwenden. Langfristige Anmeldeinformationen bergen viele Risiken. Sie können beispielsweise als Code in öffentliche GitHub Repositorien hochgeladen werden. Durch die Verwendung temporärer Anmeldeinformationen können Sie die Gefahr, dass Anmeldeinformationen kompromittiert werden, deutlich senken.

Typische Anti-Muster:

- Entwickler verwenden langfristige Zugriffsschlüssel von IAM Benutzern, anstatt temporäre Anmeldeinformationen vom CLI verwendenden Verbund zu erhalten.
- Entwickler betten langfristige Zugriffsschlüssel in ihren Code ein und laden diese in öffentliche Git-Repositorys hoch.
- Entwickler betten langfristige Zugriffsschlüssel in Mobil-Apps ein, die dann in App-Stores verfügbar gemacht werden.
- Benutzer geben langfristige Zugriffsschlüssel an andere Benutzer weiter, oder Mitarbeiter verlassen das Unternehmen und besitzen weiterhin langfristige Zugriffsschlüssel.
- Es werden langfristige Zugriffsschlüssel für Maschinenidentitäten genutzt, obwohl temporäre Anmeldeinformationen verwendet werden könnten.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Hoch

## Implementierungsleitfaden

Verwenden Sie temporäre Sicherheitsanmeldedaten anstelle von langfristigen Anmeldeinformationen für alle AWS API CLI Anfragen. API und CLI Anfragen an AWS Dienste müssen in fast allen Fällen mit [AWS Zugriffsschlüsseln](#) signiert werden. Diese Anfragen können mit temporären oder langfristigen Anmeldeinformationen signiert werden. Sie sollten langfristige Anmeldeinformationen, auch als

langfristige Zugriffsschlüssel bezeichnet, nur verwenden, wenn Sie einen [IAMBenutzer](#) oder den [AWS-Konto Root-Benutzer](#) verwenden. Wenn Sie sich mit anderen Methoden verbinden AWS oder eine [IAMRolle](#) übernehmen, werden temporäre Anmeldeinformationen generiert. Selbst wenn Sie AWS Management Console mithilfe von Anmeldeinformationen auf das zugreifen, werden temporäre Anmeldeinformationen generiert, mit denen Sie Dienste aufrufen können. AWS Es gibt nur wenige Situationen, in denen Sie langfristige Anmeldeinformationen benötigen, und fast alle Aufgaben lassen sich mit temporären Anmeldeinformationen erledigen.

Die Vermeidung der Verwendung langfristiger Anmeldeinformationen zugunsten temporärer Anmeldeinformationen sollte mit einer Strategie einhergehen, die Nutzung von IAM Benutzern zugunsten von Verbund und IAM Rollen zu reduzieren. Während IAM Benutzer in der Vergangenheit sowohl für menschliche als auch für maschinelle Identitäten verwendet wurden, empfehlen wir jetzt, sie nicht zu verwenden, um die Risiken zu vermeiden, die mit der Verwendung langfristiger Zugriffsschlüssel verbunden sind.

### Implementierungsschritte

Für menschliche Identitäten wie Mitarbeiter, Administratoren, Entwickler, Bediener und Kunden:

- Sie sollten [sich auf einen zentralen Identitätsanbieter verlassen](#) und [verlangen, dass menschliche Benutzer einen Verbund mit einem Identitätsanbieter verwenden, um mit temporären Anmeldeinformationen auf Daten zugreifen zu AWS können](#). Der Verbund für Ihre Benutzer kann entweder in Form eines [direkten Verbunds mit jedem AWS-Konto](#) oder unter Verwendung von [AWS IAM Identity Center](#) und des Identitätsanbieters Ihrer Wahl erfolgen. Der Verbund bietet eine Reihe von Vorteilen gegenüber der Verwendung von IAM Benutzern und macht zudem langfristige Anmeldeinformationen überflüssig. Ihre Benutzer können temporäre Anmeldeinformationen auch über die Befehlszeile für den [direkten Verbund](#) oder mithilfe von [IAMIdentity Center](#) anfordern. Das bedeutet, dass es nur wenige Anwendungsfälle gibt, in denen IAM Benutzer oder langfristige Anmeldeinformationen für Ihre Benutzer erforderlich sind.
- Wenn Sie Dritten, z. B. Anbietern von Software as a Service (SaaS), Zugriff auf Ressourcen in Ihrem Unternehmen gewähren AWS-Konto, können Sie [kontenübergreifende Rollen](#) und [ressourcenbasierte](#) Richtlinien verwenden.
- Wenn Sie Anwendungen für Verbraucher oder Kunden Zugriff auf Ihre AWS Ressourcen gewähren müssen, können Sie [Amazon Cognito Cognito-Identitätspools oder Amazon Cognito Cognito-Benutzerpools](#) verwenden, um temporäre Anmeldeinformationen bereitzustellen. Die Berechtigungen für die Anmeldeinformationen werden über IAM Rollen konfiguriert. Sie können auch eine separate IAM Rolle mit eingeschränkten Rechten für Gastbenutzer definieren, die nicht authentifiziert sind.

Für Maschinenidentitäten müssen Sie möglicherweise langfristige Anmeldeinformationen verwenden. In diesen Fällen sollten Sie [verlangen, dass Workloads temporäre Anmeldeinformationen mit IAM Rollen für den Zugriff verwenden](#). AWS

- Für [Amazon Elastic Compute Cloud](#) (AmazonEC2) können Sie [Rollen für Amazon](#) verwenden EC2.
- [AWS Lambda](#) ermöglicht es Ihnen, eine [Lambda-Ausführungsrolle zu konfigurieren, um dem Dienst Berechtigungen zur Ausführung von AWS Aktionen mit temporären Anmeldeinformationen zu gewähren](#). Es gibt viele andere ähnliche Modelle für AWS Dienste, um temporäre Anmeldeinformationen mithilfe von IAM Rollen zu gewähren.
- Für IoT-Geräte können Sie den [AWS IoT Core -Anmeldeinformationsanbieter](#) verwenden, um temporäre Anmeldeinformationen anzufordern.
- Für lokale Systeme oder Systeme, die außerhalb von Systemen ausgeführt werden AWS, die Zugriff auf AWS Ressourcen benötigen, können Sie [IAM Roles Anywhere](#) verwenden.

Es gibt Szenarien, in denen temporäre Anmeldeinformationen nicht in Frage kommen und stattdessen langfristige Anmeldeinformationen verwendet werden müssen. In diesen Situationen [sollten Anmeldeinformationen regelmäßig überprüft und rotiert werden](#) und [Zugriffsschlüssel für Anwendungsfälle, die langfristige Anmeldeinformationen erfordern, rotiert werden](#). Zu den Beispielen, für die möglicherweise langfristige Anmeldeinformationen erforderlich sind, gehören WordPress Plug-ins und AWS Clients von Drittanbietern. In Situationen, in denen Sie langfristige Anmeldeinformationen oder für andere Anmeldeinformationen als AWS Zugriffsschlüssel verwenden müssen, wie z. B. Datenbankanmeldungen, können Sie einen Dienst verwenden, der für die Verwaltung von Geheimnissen konzipiert ist, wie [AWS Secrets Manager](#). Secrets Manager vereinfacht die Verwaltung, Änderung und sichere Speicherung verschlüsselter Secrets mit [unterstützten Services](#). Weitere Informationen zum Austauschen von langfristigen Anmeldeinformationen finden Sie unter [Rotieren der Zugriffsschlüssel](#)

Ressourcen

Zugehörige bewährte Methoden:

- [SEC02-BP03 Geheimnisse sicher speichern und verwenden](#)
- [SEC02-BP04 Verlassen Sie sich auf einen zentralen Identitätsanbieter](#)
- [SEC03-BP08 Teilen Sie Ressourcen sicher innerhalb Ihrer Organisation](#)



## Zugehörige Dokumente:

- [Temporäre Sicherheitsanmeldeinformationen](#)
- [AWS Erweitern Sie im angezeigten Detailbereich die Option](#)
- [Bewährte Methoden bei der IAM-Sicherheit](#)
- [IAMRollen](#)
- [IAMIdentitätszentrum](#)
- [Identitätsanbieter und Verbund](#)
- [Rotieren der Zugriffsschlüssel](#)
- [Partnerlösungen im Bereich Sicherheit: Zugriff und Zugriffssteuerung](#)
- [Der Stammbenutzer des AWS -Kontos](#)

## Zugehörige Videos:

- [Benutzerberechtigungen in großem Umfang verwalten mit AWS IAM Identity Center](#)
- [Beherrschen der Identität auf jeder Ebene](#)

## SEC02-BP03 Geheimnisse sicher speichern und verwenden

Eine Workload muss ihre Identität automatisch gegenüber Datenbanken, Ressourcen und Services von Drittanbietern authentifizieren können. Dies wird mithilfe geheimer Zugangsdaten wie API Zugriffsschlüsseln, Kennwörtern und OAuth Tokens erreicht. Die Verwendung eines dedizierten Services zur Speicherung, Verwaltung und Rotation der Anmeldeinformationen hilft dabei, die Gefahr der Kompromittierung dieser Anmeldeinformationen zu verringern.

Gewünschtes Ergebnis: Implementierung eines Mechanismus zur sicheren Verwaltung von Anmeldeinformationen für Anwendungen, mit dem die folgenden Ziele erreicht werden:

- Identifikation der für die Workload erforderlichen Secrets
- Reduzierung der Anzahl der erforderlichen langfristigen Anmeldeinformationen durch ihren Austausch gegen kurzfristige Anmeldeinformationen, wo dies möglich ist
- Einrichtung der sicheren Speicherung und der automatischen Rotation der verbleibenden langfristigen Anmeldeinformationen
- Überwachung des Zugriffs auf in der Workload vorhandene Secrets

- Kontinuierliche Beobachtung, um sicherzustellen, dass im Rahmen des Entwicklungsprozesses keine Secrets in den Quellcode eingebettet werden
- Reduzieren der Gefahr unbeabsichtigter Offenlegungen von Anmeldeinformationen

Typische Anti-Muster:

- Keine Rotation der Anmeldeinformationen
- Speichern langfristiger Anmeldeinformationen in Quellcode oder Konfigurationsdateien
- Speichern von Anmeldeinformationen im Ruhezustand ohne Verschlüsselung

Vorteile der Nutzung dieser bewährten Methode:

- Secrets werden im Ruhezustand und während der Übertragung verschlüsselt gespeichert.
- Der Zugriff auf Anmeldeinformationen erfolgt über einen API (stellen Sie sich das als Automaten mit Zugangsdaten vor).
- Der Zugriff (Lese- und Schreibzugriff) auf Anmeldeinformationen wird geprüft und protokolliert.
- Trennung möglicher Problemquellen: Die Rotation der Anmeldeinformationen wird von einer separaten Komponente vorgenommen, die vom Rest der Architektur isoliert werden kann.
- Secrets werden automatisch bei Bedarf an Softwarekomponenten verteilt und die Rotation erfolgt an einem zentralen Ort.
- Der Zugriff auf Anmeldeinformationen kann detailliert kontrolliert werden.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Hoch

Implementierungsleitfaden

In der Vergangenheit waren Anmeldeinformationen, die zur Authentifizierung bei Datenbanken, Drittanbieter-APIs, Token und anderen Geheimnissen verwendet wurden, möglicherweise in Quellcode oder in Umgebungsdateien eingebettet. AWS bietet mehrere Mechanismen, um diese Anmeldeinformationen sicher zu speichern, sie automatisch zu rotieren und ihre Verwendung zu überprüfen.

Das beste Verfahren für die Verwaltung von Secrets besteht darin, den Anweisungen zum Entfernen, Ersetzen und Rotieren zu folgen. Die sichersten Anmeldeinformationen sind diejenigen, die Sie nicht speichern, verwalten oder handhaben müssen. Möglicherweise gibt es Anmeldeinformationen, die für die Funktion der Workload nicht mehr benötigt werden und sicher entfernt werden können.

Bei Anmeldeinformationen, die für die korrekte Funktion der Workload weiterhin benötigt werden, besteht die Möglichkeit, langfristige Anmeldeinformationen durch temporäre oder kurzfristige zu ersetzen. Anstatt beispielsweise einen AWS geheimen Zugriffsschlüssel fest zu codieren, sollten Sie erwägen, diese langfristigen Anmeldeinformationen mithilfe von Rollen durch temporäre Anmeldeinformationen zu ersetzen. IAM

Manche langfristigen Secrets können möglicherweise nicht entfernt oder ersetzt werden. Diese Secrets können in einem Service wie [AWS Secrets Manager](#) gespeichert werden, wo sie zentral gespeichert, verwaltet und regelmäßig rotiert werden können.

Eine Prüfung des Quellcodes und der Konfigurationsdateien der Workload kann verschiedene Arten von Anmeldeinformationen zutage fördern. Die folgende Tabelle fasst Strategien für den Umgang mit gängigen Arten von Anmeldeinformationen zusammen:

Anmeldeinformationstyp	Beschreibung	Empfohlene Strategie
IAMZugriffstasten	AWS IAMZugriffs- und geheime Schlüssel, die verwendet werden, um IAM Rollen innerhalb eines Workloads zu übernehmen	Ersetzen: Verwenden Sie stattdessen <a href="#">IAMRollen</a> , die den Compute-Instances zugewiesen sind (z. B. <a href="#">Amazon EC2</a> oder <a href="#">AWS Lambda</a> ). Fragen Sie aus Gründen der Interoperabilität mit Drittanbietern, die Zugriff auf Ihre Ressourcen benötigen AWS-Konto, ob diese den <a href="#">AWS kontoübergreifenden Zugriff</a> unterstützen. Erwägen Sie für mobile Apps die Verwendung temporärer Anmeldeinformationen über <a href="#">Amazon-Cognito-Identitätspools (Verbundidentitäten)</a> . Für Workloads, die außerhalb von ausgeführt werden AWS, sollten Sie <a href="#">Hybrid-Aktivierungen von IAMRoles Anywhere</a>

Anmeldeinformationstyp	Beschreibung	Empfohlene Strategie
		<a href="#">oder AWS Systems Manager</a> in Betracht ziehen.
SSHSchlüssel	Private Secure-Shell-Schlüssel, mit denen Sie sich manuell oder im Rahmen eines automatisierten Prozesses bei EC2 Linux-Instanzen anmelden	Ersetzen: Verwenden Sie <a href="#">AWS Systems Manager</a> oder <a href="#">EC2Instance Connect</a> , um mithilfe von IAM Rollen programmatischen und menschlichen Zugriff auf EC2 Instanzen zu gewähren.
Anwendungs- und Datenbank anmeldeinformationen	Passwörter – einfache Textzeichenfolge	Rotation: Speichern Sie Anmeldeinformationen in <a href="#">AWS Secrets Manager</a> und richten Sie nach Möglichkeit eine automatische Rotation ein.
Anmeldeinformationen für die Amazon RDS - und Aurora-Administrator Datenbank	Passwörter – einfache Textzeichenfolge	Ersetzen: Verwenden Sie die <a href="#">Secrets Manager Manager-Integration mit Amazon RDS</a> oder <a href="#">Amazon Aurora</a> . Darüber hinaus können einige RDS Datenbanktypen in einigen Anwendungsfällen IAM Rollen anstelle von Passwörtern verwenden (weitere Informationen finden Sie unter <a href="#">IAMDatenbankauthentifizierung</a> ).
OAuthTokens	Geheime Token – einfache Textzeichenfolge	Rotation: Speichern Sie Token in <a href="#">AWS Secrets Manager</a> und konfigurieren Sie die automatische Rotation.

Anmeldeinformationstyp	Beschreibung	Empfohlene Strategie
APITokens und Schlüssel	Geheime Token – einfache Textzeichenfolge	Rotation: Speichern Sie diese Daten in <a href="#">AWS Secrets Manager</a> und richten Sie nach Möglichkeit eine automatische Rotation ein.

Ein gängiges Anti-Pattern ist das Einbetten von IAM Zugriffsschlüsseln in Quellcode, Konfigurationsdateien oder mobile Apps. Wenn für die Kommunikation mit einem AWS Dienst ein IAM Zugriffsschlüssel erforderlich ist, verwenden Sie [temporäre \(kurzfristige\) Sicherheitsanmeldedaten](#). Diese kurzfristigen Anmeldeinformationen können über [IAMRollen für EC2 Instances, Ausführungsrollen für Lambda-Funktionen, IAMCognito-Rollen](#) für den mobilen Benutzerzugriff und [IoT Core-Richtlinien für IoT-Geräte](#) bereitgestellt werden. Wenn Sie Schnittstellen zu Drittanbietern haben, [delegieren Sie lieber den Zugriff an eine IAM Rolle](#) mit dem erforderlichen Zugriff auf die Ressourcen Ihres Kontos, anstatt einen IAM Benutzer zu konfigurieren und dem Dritten den geheimen Zugriffsschlüssel für diesen Benutzer zu senden.

Es gibt viele Fälle, in denen die Arbeitslast die Speicherung von Geheimnissen erfordert, die für die Zusammenarbeit mit anderen Diensten und Ressourcen erforderlich sind. [AWS Secrets Manager](#) wurde speziell für die sichere Verwaltung dieser Anmeldeinformationen sowie für die Speicherung, Verwendung und Rotation von API Token, Passwörtern und anderen Anmeldeinformationen entwickelt.

AWS Secrets Manager bietet fünf wichtige Funktionen, um die sichere Speicherung und Handhabung vertraulicher Anmeldeinformationen zu gewährleisten: [Verschlüsselung im Ruhezustand](#), [Verschlüsselung bei der Übertragung](#), [umfassende Prüfung](#), [detaillierte Zugriffskontrolle](#) und [erweiterbare](#) Rotation von Anmeldeinformationen. Andere Secret-Verwaltungsservices von AWS - Partnern oder lokal entwickelte Lösungen mit ähnlichen Funktionen und Sicherungen sind ebenfalls akzeptabel.

## Implementierungsschritte

1. Identifizieren Sie mithilfe automatisierter Tools wie [Amazon CodeGuru](#) Codepfade mit hartcodierten Anmeldeinformationen.

- a. Verwenden Sie Amazon CodeGuru , um Ihre Code-Repositorys zu scannen. Sobald die Überprüfung abgeschlossen ist, können Sie CodeGuru nach problematischen Codezeilen filtern. Type=Secrets
2. Identifizieren Sie Anmeldeinformationen, die entfernt oder ersetzt werden können.
  - a. Identifizieren Sie Anmeldeinformationen, die nicht mehr benötigt werden, und markieren Sie sie zum Entfernen.
  - b. Ersetzen Sie AWS geheime Schlüssel, die im Quellcode eingebettet sind, durch IAM Rollen, die den erforderlichen Ressourcen zugeordnet sind. Wenn sich ein Teil Ihrer Arbeitslast außerhalb befindet, für den Zugriff auf AWS Ressourcen AWS jedoch IAM Anmeldeinformationen erforderlich sind, sollten Sie [Hybrid-Aktivierungen von IAMRoles Anywhere oder AWS Systems Manager](#) in Betracht ziehen.
3. Integrieren Sie für andere langfristige Secrets von Dritten, die die Rotationsstrategie erfordern, Secrets Manager in Ihren Code, um die externen Secrets zur Laufzeit abzurufen.
  - a. Die CodeGuru Konsole kann mithilfe der erkannten Anmeldeinformationen automatisch [ein Geheimnis in Secrets Manager erstellen](#).
  - b. Integrieren Sie den Secret-Abruf von Secrets Manager in Ihren Anwendungscode.
    - i. Serverless-Lambda-Funktionen können eine sprachunabhängige [Lambda-Erweiterung](#) verwenden.
    - ii. AWS Stellt [clientseitigen Beispielcode für EC2 Instances oder Container zum Abrufen von Geheimnissen aus Secrets Manager](#) in verschiedenen gängigen Programmiersprachen bereit.
4. Prüfen Sie Ihre Codebasis regelmäßig und wiederholen Sie dies, um sicherzustellen, dass dem Code keine neuen Secrets hinzugefügt wurden.
  - a. Erwägen Sie die Verwendung eines Tools wie [git-secrets](#), um zu verhindern, dass neue Secrets in Ihr Quellcode-Repository geladen werden.
5. [Überwachen Sie die Aktivitäten von Secrets Manager](#) auf Anzeichen für eine unerwartete Nutzung, unangemessenen Secret-Zugriff oder Versuche, Secrets zu löschen.
6. Reduzieren Sie menschliche Interaktionen mit Anmeldeinformationen. Beschränken Sie den Zugriff zum Lesen, Schreiben und Ändern von Anmeldeinformationen auf eine IAM Rolle, die für diesen Zweck vorgesehen ist, und gewähren Sie nur einer kleinen Gruppe von Benutzern, die diese Rolle übernehmen, Zugriff auf diese Rolle.

## Ressourcen

### Zugehörige bewährte Methoden:

- [SEC02-BP02 Temporäre Anmeldeinformationen verwenden](#)
- [SEC02-BP05 Regelmäßige Prüfung und Rotation der Anmeldedaten](#)

### Zugehörige Dokumente:

- [Erste Schritte mit AWS Secrets Manager](#)
- [Identitätsanbieter und Verbund](#)
- [Amazon CodeGuru stellt Secrets Detector vor](#)
- [Wie AWS Secrets Manager verwendet AWS Key Management Service](#)
- [Ver- und Entschlüsselung von Secrets in Secrets Manager](#)
- [Blogeinträge zu Secrets Manager](#)
- [Amazon RDS kündigt Integration mit AWS Secrets Manager](#)

### Zugehörige Videos:

- [Bewährte Methoden zum Verwalten, Abrufen und Rotieren von Secrets in großem Maßstab](#)
- [Finden Sie hartcodierte Geheimnisse mit Amazon Secrets CodeGuru Detector](#)
- [Sicherung von Geheimnissen für hybride Workloads mit AWS Secrets Manager](#)

### Zugehörige Workshops:

- [Speichern, abrufen und verwalten Sie vertrauliche Anmeldeinformationen in AWS Secrets Manager](#)
- [AWS Systems Manager Hybride Aktivierungen](#)

## SEC02-BP04 Verlassen Sie sich auf einen zentralen Identitätsanbieter

Verlassen Sie sich im Zusammenhang mit Identitäten für Ihre Belegschaft (Mitarbeiter und Auftragnehmer) auf einen Identitätsanbieter, mit dem Sie Identitäten zentral verwalten können. Dadurch ist es einfacher, den Zugriff über mehrere Anwendungen und Systeme hinweg zu verwalten, da Sie den Zugriff von einem einzigen Standort aus erstellen, zuweisen, verwalten, widerrufen und überwachen.

Gewünschtes Ergebnis: Sie verfügen über einen zentralen Identitätsanbieter, mit dem Sie die Benutzer Ihrer Belegschaft, die Authentifizierungsrichtlinien (z. B. die Anforderung einer mehrstufigen Authentifizierung (MFA)) und die Autorisierung von Systemen und Anwendungen (z. B. die Zuweisung von Zugriffen auf der Grundlage der Gruppenmitgliedschaft oder der Attribute eines Benutzers) zentral verwalten können. Die Benutzer in Ihrer Belegschaft melden sich beim zentralen Identitätsanbieter an und bilden einen Verbund (Single Sign-On) mit internen und externen Anwendungen, sodass sich die Benutzer nicht mehrere Anmeldeinformationen merken müssen. Ihr Identitätsanbieter ist in Ihre Personalverwaltungssysteme integriert, sodass Personaländerungen automatisch mit Ihrem Identitätsanbieter synchronisiert werden. Wenn beispielsweise jemand Ihr Unternehmen verlässt, können Sie automatisch den Zugriff auf föderierte Anwendungen und Systeme (einschließlich) widerrufen. AWS Sie haben die detaillierte Auditprotokollierung in Ihrem Identitätsanbieter aktiviert und überwachen diese Protokolle auf ungewöhnliches Benutzerverhalten.

Typische Anti-Muster:

- Sie verwenden keinen Verbund mit Single-Sign-On. Die Benutzer in Ihrer Belegschaft erstellen separate Benutzerkonten und Anmeldeinformationen für mehrere Anwendungen und Systeme.
- Sie haben den Lebenszyklus von Identitäten für Benutzer in Ihrer Belegschaft nicht automatisiert, indem Sie beispielsweise Ihren Identitätsanbieter in Ihre Personalverwaltungssysteme integriert haben. Wenn ein Benutzer Ihre Organisation verlässt oder die Position wechselt, folgen Sie einem manuellen Prozess, um seine Datensätze in mehreren Anwendungen und Systemen zu löschen oder zu aktualisieren.

Vorteile der Nutzung dieser bewährten Methode: Durch die Verwendung eines zentralen Identitätsanbieters haben Sie die Möglichkeit, Benutzeridentitäten und Richtlinien für Ihre Mitarbeiter von einem zentralen Ort aus zu verwalten, Benutzern und Gruppen Zugriff auf Anwendungen zuzuweisen und die Anmeldeaktivitäten der Benutzer zu überwachen. Wenn ein Benutzer die Position wechselt, werden durch die Integration in Ihre Personalverwaltungssysteme Änderungen mit dem Identitätsanbieter synchronisiert und die ihm zugewiesenen Anwendungen und Berechtigungen werden automatisch aktualisiert. Wenn ein Benutzer Ihre Organisation verlässt, wird seine Identität automatisch im Identitätsanbieter deaktiviert, wodurch ihm der Zugriff auf Anwendungen und Systeme im Verbund entzogen wird.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Hoch

Implementierungsleitfaden

Leitfaden für Benutzer im Unternehmen, die auf AWS zugreifen



Workforce-Benutzer wie Mitarbeiter und Auftragnehmer in Ihrem Unternehmen benötigen möglicherweise Zugriff auf die AWS Verwendung von AWS Management Console oder AWS Command Line Interface (AWS CLI), um ihre Aufgaben wahrnehmen zu können. [Sie können Ihren Workforce-Benutzern AWS Zugriff gewähren, indem Sie einen Verbund von Ihrem zentralen Identitätsanbieter aus AWS auf zwei Ebenen einrichten: direkter Verbund mit jedem Konto AWS-Konto oder Verbund mit mehreren Konten in Ihrer AWS Organisation.](#)

- Um Ihre Workforce-Benutzer direkt mit den einzelnen Benutzern zu verbinden AWS-Konto, können Sie einen zentralen Identitätsanbieter verwenden, um sich mit diesem Konto zu [AWS Identity and Access Management](#) verbinden. Die Flexibilität von IAM ermöglicht es Ihnen, für jeden einen separaten [SAML2.0](#) - oder einen [Open ID Connect \(OIDC\)](#) Identity Provider zu aktivieren AWS-Konto und föderierte Benutzerattribute für die Zugriffskontrolle zu verwenden. Die Benutzer Ihrer Belegschaft verwenden ihren Webbrowser, um sich beim Identitätsanbieter anzumelden, indem sie ihre Anmeldeinformationen (wie Passwörter und MFA Token-Codes) eingeben. Der Identitätsanbieter gibt eine SAML Assertion an seinen Browser aus, die bei der AWS Management Console Anmeldung eingereicht wird URL, damit der Benutzer sich einmalig anmelden kann, [AWS Management Console indem er eine IAM Rolle annimmt](#). Ihre Benutzer können auch temporäre AWS API Anmeldeinformationen für die Verwendung in [AWS CLI](#) oder [AWS SDKs](#) von abrufen, [AWS STS](#) indem sie [die IAM Rolle mithilfe einer SAML Assertion des Identitätsanbieters übernehmen](#).
- Um die Benutzer Ihrer Belegschaft mit mehreren Konten in Ihrer AWS Organisation [AWS IAM Identity Center](#) zu verbinden, können Sie den Zugriff Ihrer Mitarbeiter auf AWS-Konten und Anwendungen zentral verwalten. Sie aktivieren Identity Center für Ihre Organisation und konfigurieren Ihre Identitätsquelle. IAM Identity Center bietet ein standardmäßiges Identitätsquellenverzeichnis, mit dem Sie Ihre Benutzer und Gruppen verwalten können. Alternativ können Sie eine externe Identitätsquelle auswählen, indem Sie mithilfe von SAML 2.0 eine [Verbindung zu Ihrem externen Identitätsanbieter](#) herstellen und Benutzer [und Gruppen mithilfe SCIM automatisch bereitstellen](#) oder eine [Verbindung zu Ihrem Microsoft AD-Verzeichnis](#) herstellen. [AWS Directory Service Sobald eine Identitätsquelle konfiguriert ist, können Sie Benutzern und Gruppen Zugriff zuweisen, AWS-Konten indem Sie in Ihren Berechtigungssätzen Richtlinien mit den geringsten Rechten definieren](#). Die Benutzer Ihrer Belegschaft können sich über Ihren zentralen Identitätsanbieter authentifizieren, um sich beim [AWS -Zugriffsportal](#) anzumelden und sich per Single Sign-On bei AWS-Konten und den ihnen zugewiesenen Cloud-Anwendungen zu authentifizieren. Ihre Benutzer können [AWS CLI v2](#) so konfigurieren, dass sie sich bei Identity Center authentifizieren und Anmeldeinformationen für die Ausführung von Befehlen abrufen. AWS CLI Identity Center ermöglicht auch den Single-Sign-On-Zugriff auf AWS Anwendungen wie [Amazon SageMaker Studio](#) - und [AWS IoT Sitewise Monitor-Portale](#).

Nachdem Sie die oben genannten Hinweise befolgt haben, müssen die Benutzer Ihrer Belegschaft bei der Verwaltung von Workloads keine IAM Benutzer und Gruppen mehr für den normalen Betrieb verwenden. AWS Stattdessen werden Ihre Benutzer und Gruppen extern verwaltet, AWS und Benutzer können als föderierte AWS Identität auf Ressourcen zugreifen. Verbundidentitäten verwenden die von ihrem zentralen Identitätsanbieter definierten Gruppen. Sie sollten IAM Gruppen, IAM Benutzer und langlebige Benutzeranmeldeinformationen (Passwörter und Zugriffsschlüssel) identifizieren und entfernen, die in Ihrem System nicht mehr benötigt werden. AWS-Konten Sie können mithilfe von [IAMAnmeldedatenberichten nach ungenutzten Anmeldeinformationen suchen](#), [die entsprechenden IAM Benutzer löschen und Gruppen löschen IAM](#). Sie können auf Ihre Organisation eine [Service Control-Richtlinie \(SCP\)](#) anwenden, die die Erstellung neuer IAM Benutzer und Gruppen verhindert und erzwingt, dass der Zugriff auf diese über föderierte AWS Identitäten erfolgt.

## Leitfaden für Benutzer Ihrer Anwendungen

Sie können die Identitäten der Benutzer Ihrer Anwendungen, z. B. einer mobilen App, mithilfe von [Amazon Cognito](#) als zentralem Identitätsanbieter verwalten. Amazon Cognito ermöglicht die Authentifizierung, Autorisierung und Benutzerverwaltung für Ihre Web- und Mobil-Apps. Amazon Cognito bietet einen Identitätsspeicher, der auf Millionen von Benutzern skaliert werden kann, unterstützt den Identitätsverbund für soziale Netzwerke und Unternehmen und bietet erweiterte Sicherheitsfeatures zum Schutz Ihrer Benutzer und Ihres Unternehmens. Sie können Ihre benutzerdefinierte Web- oder Mobilanwendung in Amazon Cognito integrieren, um Ihren Anwendungen innerhalb von Minuten Benutzerauthentifizierung und Zugriffskontrolle hinzuzufügen. Amazon Cognito basiert auf offenen Identitätsstandards wie SAML Open ID Connect (OIDC), unterstützt verschiedene Compliance-Vorschriften und lässt sich in Frontend- und Backend-Entwicklungsressourcen integrieren.

## Implementierungsschritte

### Schritte für Benutzer im Unternehmen, die auf AWS zugreifen

- Binden Sie die Benutzer Ihrer Belegschaft AWS mit einem zentralen Identitätsanbieter zusammen und verwenden Sie dabei einen der folgenden Ansätze:
  - Verwenden Sie IAM Identity Center, um Single Sign-On für mehrere Benutzer AWS-Konten in Ihrem AWS Unternehmen zu ermöglichen, indem Sie eine Verbindung mit Ihrem Identitätsanbieter herstellen.
  - Verwenden Sie diese IAM Option, um Ihren Identitätsanbieter direkt mit jedem zu verbinden und so einen AWS-Konto differenzierten Verbundzugriff zu ermöglichen.

- Identifizieren und entfernen Sie IAM Benutzer und Gruppen, die durch föderierte Identitäten ersetzt wurden.

### Schritte für Benutzer Ihrer Anwendungen

- Verwenden Sie Amazon Cognito als zentralen Identitätsanbieter für Ihre Anwendungen.
- Integrieren Sie Ihre benutzerdefinierten Anwendungen mit Amazon Cognito mithilfe von OpenID Connect und OAuth. Sie können Ihre benutzerdefinierten Anwendungen mithilfe der Amplify-Bibliotheken entwickeln, die einfache Schnittstellen zur Integration mit einer Vielzahl von AWS-Diensten bieten, z. B. Amazon Cognito für die Authentifizierung.

### Ressourcen

Zugehörige bewährte Methoden für Well-Architected:

- [SEC02-BP06 Benutzergruppen und Attribute einsetzen](#)
- [SEC03-BP02 Least-Privilege-Zugriff gewähren](#)
- [SEC03-BP06 Zugriff basierend auf dem Lebenszyklus verwalten](#)

Zugehörige Dokumente:

- [Identitätsverbund in AWS](#)
- [Bewährte Methoden für die Sicherheit in IAM](#)
- [AWS Identity and Access Management Bewährte Methoden](#)
- [Erste Schritte mit der delegierten Verwaltung von IAM Identity Center](#)
- [Wie verwendet man vom Kunden verwaltete Richtlinien in IAM Identity Center für erweiterte Anwendungsfälle](#)
- [AWS CLI v2: IAM Identity Center-Anmeldeinformationsanbieter](#)

Zugehörige Videos:

- [AWS re:inForce 2022 — AWS Identity and Access Management \(\) tiefer Einblick IAM](#)
- [AWS re:Invent 2022 — Vereinfachen Sie den Zugang Ihrer bestehenden Belegschaft mit Identity Center IAM](#)
- [AWS re:Invent 2018: Beherrschung der Identität auf jeder Ebene des Kuchens](#)

## Zugehörige Beispiele:

- [Workshop: Einsatz AWS IAM Identity Center zur Erzielung eines starken Identitätsmanagements](#)
- [Workshop: Serverless-Identität](#)

## Zugehörige Tools:

- [AWS Kompetenzpartner für Sicherheit: Identity and Access Management](#)
- [AWS IAM Identity Center](#)

## SEC02-BP05 Regelmäßige Prüfung und Rotation der Anmeldedaten

Prüfen und rotieren Sie Anmeldeinformationen regelmäßig, um die Zeit zu begrenzen, für die diese zum Zugriff auf Ihre Ressourcen genutzt werden können. Langfristig gültige Anmeldeinformationen sind mit Risiken verbunden, die durch die regelmäßige Rotation dieser Informationen reduziert werden können.

Gewünschtes Ergebnis: Implementieren Sie die Rotation von Anmeldeinformationen, um die Risiken zu verringern, die mit der Nutzung von langfristigen Anmeldeinformationen verbunden sind. Prüfen und korrigieren Sie regelmäßig fehlende Compliance mit Richtlinien zur Rotation von Anmeldeinformationen.

## Typische Anti-Muster:

- Keine Prüfung der Verwendung von Anmeldeinformationen
- Unnötiges Verwenden langfristiger Anmeldeinformationen
- Verwendung langfristiger Anmeldeinformationen, ohne diese regelmäßig zu rotieren

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Hoch

## Implementierungsleitfaden

Wenn Sie sich nicht auf temporäre Anmeldeinformationen verlassen können und langfristige Anmeldeinformationen benötigen, überprüfen Sie die Anmeldeinformationen, um sicherzustellen, dass definierte Kontrollen wie die Multi-Faktor-Authentifizierung (MFA) durchgesetzt werden, regelmäßig rotiert werden und über die entsprechende Zugriffsebene verfügen.

Eine regelmäßige Validierung, vorzugsweise durch ein automatisiertes Tool, ist notwendig, um zu überprüfen, ob die richtigen Kontrollen angewendet werden. Für Personenidentitäten sollten Sie festlegen, dass Benutzer ihre Passwörter regelmäßig ändern und anstelle von Zugriffsschlüsseln temporäre Anmeldeinformationen verwenden. Wenn Sie von Benutzern AWS Identity and Access Management (IAM) zu zentralisierten Identitäten wechseln, können Sie [einen Bericht mit Anmeldeinformationen erstellen, um Ihre Benutzer zu überprüfen](#).

Wir empfehlen Ihnen außerdem, die Durchsetzung und Überwachung MFA in Ihrem Identitätsanbieter vorzunehmen. Sie können [AWS Security Hub Sicherheitsstandards](#) einrichten [AWS-Config-Regeln](#) oder verwenden, um zu überwachen, ob Benutzer konfiguriert haben MFA. Erwägen Sie die Verwendung von IAM Roles Anywhere, um temporäre Anmeldeinformationen für Maschinenidentitäten bereitzustellen. In Situationen, in denen die Verwendung von IAM Rollen und temporären Anmeldeinformationen nicht möglich ist, sind häufige Prüfungen und rotierende Zugriffsschlüssel erforderlich.

### Implementierungsschritte

- **Regelmäßige Überprüfung der Anmeldeinformationen:** Die Überprüfung der Identitäten, die in Ihrem Identitätsanbieter konfiguriert sind, IAM hilft dabei, sicherzustellen, dass nur autorisierte Identitäten Zugriff auf Ihren Workload haben. Zu diesen Identitäten können unter anderem Benutzer, IAM Benutzer, Active AWS IAM Identity Center Directory-Benutzer oder Benutzer eines anderen Upstream-Identitätsanbieters gehören. Entfernen sie beispielsweise Personen, die die Organisation verlassen. Entfernen Sie auch kontoübergreifende Rollen, die nicht mehr erforderlich sind. Richten Sie ein Verfahren ein, um die Berechtigungen für die Dienste, auf die eine IAM Entität zugreift, regelmäßig zu überprüfen. Dadurch können Sie die Richtlinien identifizieren, die Sie ändern müssen, um nicht genutzte Berechtigungen zu entfernen. Verwenden Sie Berichte über Anmeldeinformationen und überprüfen [AWS Identity and Access Management Access Analyzer](#) Sie IAM Anmeldeinformationen und Berechtigungen. Sie können [Amazon verwenden CloudWatch , um Alarme für bestimmte API Anrufe in Ihrer AWS Umgebung einzurichten](#). [Amazon GuardDuty kann Sie auch auf unerwartete Aktivitäten aufmerksam machen, die auf einen zu](#) freizügigen Zugriff oder einen unbeabsichtigten Zugriff auf Anmeldeinformationen hindeuten können. IAM
- **Wechseln Sie die Anmeldeinformationen regelmäßig:** Wenn Sie keine temporären Anmeldeinformationen verwenden können, wechseln Sie die Schlüssel für IAM den langfristigen Zugriff regelmäßig (maximal alle 90 Tage). Wenn ein Zugriffsschlüssel ohne Ihr Wissen kompromittiert wurde, wird dadurch begrenzt, für wie lange die Anmeldeinformationen zum Zugriff auf Ihre Ressourcen genutzt werden können. Informationen zur Rotation von Zugriffstasten für IAM Benutzer finden Sie unter [Rotierende Zugriffstasten](#).

- Überprüfen Sie die IAM Berechtigungen: Um die Sicherheit Ihrer Richtlinien zu verbessern AWS-Konto, überprüfen und überwachen Sie regelmäßig jede Ihrer IAM Richtlinien. Stellen Sie sicher, dass die Richtlinien dem Prinzip der geringsten Berechtigung entsprechen.
- Erwägen Sie, die Erstellung und Aktualisierung von IAM Ressourcen zu automatisieren: IAM Identity Center automatisiert viele IAM Aufgaben, wie z. B. die Rollen- und Richtlinienverwaltung. Alternativ AWS CloudFormation kann es verwendet werden, um die Bereitstellung von IAM Ressourcen, einschließlich Rollen und Richtlinien, zu automatisieren, um das Risiko menschlicher Fehler zu verringern, da die Vorlagen verifiziert und versionskontrolliert werden können.
- Verwenden Sie IAM Roles Anywhere, um IAM Benutzer durch Maschinenidentitäten zu ersetzen: Mit IAM Roles Anywhere können Sie Rollen in Bereichen verwenden, in denen dies bisher nicht möglich war, z. B. auf lokalen Servern. IAMRoles Anywhere verwendet ein vertrauenswürdigen X.509-Zertifikat für die Authentifizierung AWS und den Empfang temporärer Anmeldeinformationen. Durch die Verwendung von IAM Roles Anywhere müssen diese Anmeldeinformationen nicht mehr rotiert werden, da langfristige Anmeldeinformationen nicht mehr in Ihrer lokalen Umgebung gespeichert werden. Beachten Sie, dass Sie das X.509-Zertifikat beobachten und gegen Ende seiner Gültigkeitsdauer austauschen müssen.

## Ressourcen

### Zugehörige bewährte Methoden:

- [SEC02-BP02 Temporäre Anmeldeinformationen verwenden](#)
- [SEC02-BP03 Geheimnisse sicher speichern und verwenden](#)

### Zugehörige Dokumente:

- [Erste Schritte mit AWS Secrets Manager](#)
- [IAMBewährte Verfahren](#)
- [Identitätsanbieter und Verbund](#)
- [Partnerlösungen im Bereich Sicherheit: Zugriff und Zugriffssteuerung](#)
- [Temporäre Sicherheitsanmeldeinformationen](#)
- [Abrufen von Berichten über Anmeldeinformationen für Ihr AWS-Konto](#)

### Zugehörige Videos:

- [Bewährte Methoden zum Verwalten, Abrufen und Rotieren von Secrets in großem Maßstab](#)
- [Verwaltung von Benutzerberechtigungen in großem Umfang mit AWS IAM Identity Center](#)
- [Beherrschen der Identität auf jeder Ebene](#)

Zugehörige Beispiele:

- [Well-Architected Lab — Automatisierte Benutzerbereinigung IAM](#)
- [Well-Architected Lab — Automatisierte Bereitstellung von IAM Gruppen und Rollen](#)

## SEC02-BP06 Benutzergruppen und Attribute einsetzen

Die Definition von Berechtigungen nach Benutzergruppen und Attributen trägt dazu bei, die Anzahl und Komplexität von Richtlinien zu reduzieren, sodass das Prinzip der geringsten Berechtigung einfacher umgesetzt werden kann. Sie können Benutzergruppen verwenden, um die Berechtigungen für viele Personen an einem Ort zu verwalten, basierend auf der Funktion, die sie in Ihrer Organisation innehaben. Attribute, wie z. B. Abteilung oder Standort, können eine zusätzliche Ebene des Berechtigungsumfangs bieten, wenn Personen eine ähnliche Funktion ausüben, aber für unterschiedliche Teilmengen von Ressourcen.

Gewünschtes Ergebnis: Sie können Änderungen der Berechtigungen auf alle Benutzer anwenden, die eine bestimmte Funktion ausführen. Die Gruppenzugehörigkeit und -attribute regeln die Benutzerberechtigungen, sodass Sie die Berechtigungen nicht mehr auf der Ebene der einzelnen Benutzer verwalten müssen. Die Gruppen und Attribute, die Sie in Ihrem Identitätsanbieter (IDP) definieren, werden automatisch an Ihre AWS -Umgebungen weitergegeben.

Typische Anti-Muster:

- Verwaltung von Berechtigungen für einzelne Benutzer und Duplizierung für viele Benutzer.
- Definition von Gruppen auf einer zu hohen Ebene, Gewährung von zu weitreichenden Berechtigungen.
- Die Definition von Gruppen auf einer zu granularen Ebene, was zu Doppelarbeit und Verwirrung über die Mitgliedschaft führt.
- Verwendung von Gruppen mit doppelten Berechtigungen für Teilmengen von Ressourcen, wenn stattdessen Attribute verwendet werden können.
- Keine Verwaltung von Gruppen, Attributen und Mitgliedschaften über einen standardisierten Identitätsanbieter, der in Ihre AWS -Umgebungen integriert ist.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel

## Implementierungsleitfaden

AWS Berechtigungen werden in Dokumenten definiert, die als Richtlinien bezeichnet werden und einem Prinzipal zugeordnet sind, z. B. einem Benutzer, einer Gruppe, einer Rolle oder einer Ressource. So können Sie für Ihre Mitarbeiter Gruppen definieren, die auf der Funktion basieren, die Ihre Benutzer in Ihrer Organisation innehaben, und nicht auf den Ressourcen, auf die sie zugreifen. Einer `WebAppDeveloper` Gruppe kann beispielsweise eine Richtlinie für die Konfiguration eines Dienstes wie Amazon CloudFront innerhalb eines Entwicklungskontos angehängt sein. Eine `AutomationDeveloper` Gruppe kann einige CloudFront Berechtigungen mit der `WebAppDeveloper` Gruppe gemeinsam haben. Diese Berechtigungen können in einer separaten Richtlinie erfasst und beiden Gruppen zugeordnet werden. Dadurch ist es nicht erforderlich, dass Benutzer beider Funktionen zu einer `CloudFrontAccess`-Gruppe gehören.

Zusätzlich zu Gruppen können Sie Attribute verwenden, um den Zugriff festzulegen. Sie können beispielsweise ein `Project`-Attribut für Benutzer in Ihrer `WebAppDeveloper`-Gruppe nutzen, damit die Benutzer nur auf Ressourcen ihres Projekts zugreifen können. Mit dieser Technik entfällt die Notwendigkeit, für Anwendungsentwickler, die an verschiedenen Projekten arbeiten, unterschiedliche Gruppen einzurichten, wenn ihre Berechtigungen ansonsten identisch sind. Die Art und Weise, wie Sie in Berechtigungsrichtlinien auf Attribute verweisen, hängt von deren Quelle ab, unabhängig davon, ob sie als Teil Ihres Verbundprotokolls (wie SAML OIDC, oder SCIM), als benutzerdefinierte SAML Assertionen oder in IAM Identity Center definiert sind.

## Implementierungsschritte

1. Legen Sie fest, wo Sie Gruppen und Attribute definieren wollen.
  - a. Anhand der Anleitung unter können Sie festlegen [SEC02-BP04 Verlassen Sie sich auf einen zentralen Identitätsanbieter](#), ob Sie Gruppen und Attribute innerhalb Ihres Identitätsanbieters, innerhalb IAM von Identity Center oder mithilfe von IAM Benutzergruppen in einem bestimmten Konto definieren müssen.
2. Definieren Sie Gruppen.
  - a. Legen Sie Ihre Gruppen je nach Funktion und Umfang des erforderlichen Zugriffs fest.
  - b. Wenn Sie innerhalb von IAM Identity Center definieren, erstellen Sie Gruppen und ordnen Sie die gewünschte Zugriffsebene mithilfe von Berechtigungssätzen zu.
  - c. Wenn Sie die Definition innerhalb eines externen Identitätsanbieters vornehmen, stellen Sie fest, ob der Anbieter das SCIM Protokoll unterstützt, und erwägen Sie, die automatische Bereitstellung innerhalb von IAM Identity Center zu aktivieren. Diese Funktion synchronisiert



die Erstellung, Mitgliedschaft und Löschung von Gruppen zwischen Ihrem Anbieter und IAM Identity Center.

### 3. Attribute definieren.

- a. Wenn Sie einen externen Identitätsanbieter verwenden, bieten SCIM sowohl das Protokoll als auch das SAML 2.0-Protokoll standardmäßig bestimmte Attribute. Zusätzliche Attribute können mithilfe von SAML Assertionen unter Verwendung des `https://aws.amazon.com/SAML/Attributes/PrincipalTag` Attributnamens definiert und übergeben werden.
- b. Wenn Sie innerhalb von IAM Identity Center definieren, aktivieren Sie die Funktion für die attributebasierte Zugriffskontrolle (ABAC) und definieren Sie die Attribute wie gewünscht.

### 4. Umfangsberechtigungen basierend auf Gruppen und Attributen.

- a. Erwägen Sie, Bedingungen in Ihre Genehmigungsrichtlinien aufzunehmen, die die Attribute Ihres Prinzipals mit den Attributen der Ressourcen vergleichen, auf die zugegriffen wird. Sie können beispielsweise eine Bedingung so definieren, dass der Zugriff auf eine Ressource nur dann gewährt wird, wenn der Wert eines `PrincipalTag`-Bedingungsschlüssels mit dem Wert eines `ResourceTag`-Schlüssels mit demselben Namen übereinstimmt.

## Ressourcen

### Zugehörige bewährte Methoden:

- [SEC02-BP04 Verlassen Sie sich auf einen zentralen Identitätsanbieter](#)
- [SEC03-BP02 Least-Privilege-Zugriff gewähren](#)
- [COST02-BP04 Implementieren Sie Gruppen und Rollen](#)

### Zugehörige Dokumente:

- [IAM Bewährte Verfahren](#)
- [Identitäten im IAM Identity Center verwalten](#)
- [Wofür ist es ABAC? AWS](#)
- [ABAC im IAM Identity Center](#)

### Zugehörige Videos:

- [Verwaltung von Benutzerberechtigungen in großem Umfang mit AWS IAM Identity Center](#)
- [Beherrschen der Identität auf jeder Ebene](#)

## SEC3. Wie werden Berechtigungen für Personen und Computer verwaltet?

Verwalten Sie Berechtigungen, um den Zugriff auf Personen- und Maschinenidentitäten zu kontrollieren, die Zugriff auf Ihre AWS Workloads benötigen. Berechtigungen steuern, wer worauf und unter welchen Bedingungen zugreifen kann.

### Bewährte Methoden

- [SEC03-BP01 Zugangsvoraussetzungen definieren](#)
- [SEC03-BP02 Least-Privilege-Zugriff gewähren](#)
- [SEC03-BP03 Notfallzugangsverfahren einrichten](#)
- [SEC03-BP04 Berechtigungen kontinuierlich reduzieren](#)
- [SEC03-BP05 Definieren Sie Genehmigungsleitlinien für Ihre Organisation](#)
- [SEC03-BP06 Zugriff basierend auf dem Lebenszyklus verwalten](#)
- [SEC03-BP07 Analysieren Sie den öffentlichen und kontoübergreifenden Zugriff](#)
- [SEC03-BP08 Teilen Sie Ressourcen sicher innerhalb Ihrer Organisation](#)
- [SEC03-BP09 Ressourcen sicher mit Dritten teilen](#)

### SEC03-BP01 Zugangsvoraussetzungen definieren

Auf jede Komponente oder Ressource Ihrer Workload müssen Administratoren, Endbenutzer oder andere Komponenten zugreifen können. Definieren Sie klar, wer oder was Zugriff auf die einzelnen Komponenten haben soll, und wählen Sie den geeigneten Identitätstyp und die Methode für die Authentifizierung und Autorisierung aus.

### Typische Anti-Muster:

- Hartkodierung oder Speicherung von geheimen Daten in Ihrer Anwendung
- Gewähren individueller Berechtigungen für jeden Benutzer
- Verwendung langlebiger Anmeldeinformationen

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Hoch

### Implementierungsleitfaden

Auf jede Komponente oder Ressource Ihrer Workload müssen Administratoren, Endbenutzer oder andere Komponenten zugreifen können. Definieren Sie klar, wer oder was Zugriff auf die einzelnen

Komponenten haben soll, und wählen Sie den geeigneten Identitätstyp und die Methode für die Authentifizierung und Autorisierung aus.

Der reguläre Zugriff AWS-Konten innerhalb der Organisation sollte über einen [Verbundzugriff](#) oder einen zentralen Identitätsanbieter erfolgen. Sie sollten auch Ihr Identitätsmanagement zentralisieren und sicherstellen, dass es eine etablierte Praxis gibt, um den AWS Zugriff in den Lebenszyklus Ihres Mitarbeiterzugriffs zu integrieren. Wenn beispielsweise ein Mitarbeiter in eine Rolle mit einer anderen Zugriffsstufe wechselt, sollte sich auch dessen Gruppenmitgliedschaft so ändern, dass die neuen Zugriffsanforderungen berücksichtigt werden.

Legen Sie bei der Definition der Zugriffsanforderungen für nicht menschliche Identitäten fest, welche Anwendungen und Komponenten Zugriff benötigen und wie die Berechtigungen gewährt werden. Es wird empfohlen, IAM Rollen zu verwenden, die mit dem Zugriffsmodell mit den geringsten Rechten erstellt wurden. [AWS Verwaltete Richtlinien](#) bieten vordefinierte IAM Richtlinien, die die häufigsten Anwendungsfälle abdecken.

AWS Dienste wie [AWS Secrets Manager](#) [AWS Systems Manager Parameter Store](#) können dazu beitragen, Geheimnisse sicher von der Anwendung oder dem Workload zu entkoppeln, wenn die Verwendung IAM von Rollen nicht möglich ist. In Secrets Manager können Sie die automatische Rotation Ihrer Anmeldeinformationen einrichten. Sie können Systems Manager verwenden, um Parameter in Ihren Skripten, Befehlen, SSM Dokumenten, Konfigurationen und Automatisierungsworkflows zu referenzieren, indem Sie den eindeutigen Namen verwenden, den Sie bei der Erstellung des Parameters angegeben haben.

Sie können AWS Identity and Access Management Roles Anywhere verwenden, um [temporäre Sicherheitsanmeldeinformationen IAM](#) für Workloads zu erhalten, die außerhalb von AWS ausgeführt werden. Ihre Workloads können dieselben [IAM Richtlinien](#) und [IAM Rollen](#) verwenden, die Sie für AWS Anwendungen für den Zugriff auf AWS Ressourcen verwenden.

Verwenden Sie nach Möglichkeit kurzfristige temporäre anstelle langfristiger statischer Anmeldeinformationen. Für Szenarien, in denen Sie -Benutzer mit programmgesteuertem Zugriff und langfristigen Anmeldeinformationen benötigen, verwenden Sie die [Informationen über die letzte Nutzung von Zugriffsschlüsseln](#), um die Zugriffsschlüssel zu rotieren und zu entfernen.

Benutzer benötigen programmgesteuerten Zugriff, wenn sie mit AWS außerhalb des interagieren möchten. AWS Management Console Die Art und Weise, wie programmatischer Zugriff gewährt wird, hängt vom Benutzertyp ab, der zugreift. AWS

Um Benutzern programmgesteuerten Zugriff zu gewähren, wählen Sie eine der folgenden Optionen.

Welcher Benutzer benötigt programmgesteuerten Zugriff?	Bis	Von
<p>Mitarbeiteridentität</p> <p>(In IAM Identity Center verwaltete Benutzer)</p>	<p>Verwenden Sie temporäre Anmeldeinformationen, um programmatische Anfragen an AWS CLI AWS SDKs, oder AWS APIs zu signieren.</p>	<p>Befolgen Sie die Anweisungen für die Schnittstelle, die Sie verwenden möchten.</p> <ul style="list-style-type: none"> <li>• Informationen zu den AWS CLI finden Sie <a href="#">unter Konfiguration der AWS CLI zur Verwendung AWS IAM Identity Center</a> im AWS Command Line Interface Benutzerhandbuch.</li> <li>• Informationen zu AWS SDKs Tools und AWS APIs finden Sie unter <a href="#">IAM Identity Center-Authentifizierung</a> im Referenzhandbuch AWS SDKs und im Tools-Referenzhandbuch.</li> </ul>
<p>IAM</p>	<p>Verwenden Sie temporäre Anmeldeinformationen, um programmatische Anfragen an das AWS CLI AWS SDKs, oder AWS APIs zu signieren.</p>	<p>Folgen Sie den Anweisungen unter <a href="#">Verwenden temporärer Anmeldeinformationen mit AWS Ressourcen</a> im IAM Benutzerhandbuch.</p>
<p>IAM</p>	<p>(Nicht empfohlen)</p> <p>Verwenden Sie langfristige Anmeldeinformationen, um programmatische Anfragen an das AWS CLI AWS SDKs, oder AWS APIs zu signieren.</p>	<p>Befolgen Sie die Anweisungen für die Schnittstelle, die Sie verwenden möchten.</p> <ul style="list-style-type: none"> <li>• Informationen dazu AWS CLI finden Sie unter <a href="#">Authentifizierung mithilfe von IAM Benutzeranmeldedaten</a> im AWS</li> </ul>

Welcher Benutzer benötigt programmgesteuerten Zugriff?	Bis	Von
		<p>Command Line Interface Benutzerhandbuch.</p> <ul style="list-style-type: none"> <li>• Informationen zu AWS SDKs und Tools finden Sie unter <a href="#">Authentifizieren mit langfristigen Anmeldeinformationen</a> im Referenzhandbuch AWS SDKs und im Tools-Referenzhandbuch.</li> <li>• Weitere Informationen finden Sie unter <a href="#">Verwaltung von Zugriffsschlüsseln für IAM Benutzer</a> im IAM Benutzerhandbuch. AWS APIs</li> </ul>

## Ressourcen

### Zugehörige Dokumente:

- [Attributbasierte Zugriffskontrolle \(\) ABAC](#)
- [AWS IAM Identity Center](#)
- [IAM Roles Anywhere](#)
- [AWS Verwaltete Richtlinien für Identity Center IAM](#)
- [AWS IAM politische Bedingungen](#)
- [IAM Anwendungsfälle](#)
- [Entfernen unnötiger Anmeldeinformationen](#)
- [Arbeiten mit -Richtlinien](#)
- [Wie kann der Zugriff auf AWS Ressourcen je AWS-Konto nach Organisationseinheit oder Organisation gesteuert werden](#)
- [Identifizieren, ordnen und verwalten Sie Geheimnisse ganz einfach mithilfe der erweiterten Suche in AWS Secrets Manager](#)

## Zugehörige Videos:

- [Werden Sie in 60 Minuten oder weniger zum IAM Policy Master](#)
- [Trennung von Pflichten, geringste Berechtigung, Delegation und CI/CD](#)
- [Optimieren des Identitäts- und Zugriffsmanagements für Innovation](#)

## SEC03-BP02 Least-Privilege-Zugriff gewähren

Es hat sich bewährt, nur den Zugriff zu gewähren, den Identitäten benötigen, um bestimmte Aktionen auf bestimmten Ressourcen unter bestimmten Bedingungen durchzuführen. Nutzen Sie Gruppen und Identitätsattribute, um Berechtigungen dynamisch in großem Umfang festzulegen, anstatt Berechtigungen für einzelne Benutzer zu definieren. Sie können beispielsweise einer Gruppe von Entwicklern den Zugriff erlauben, nur die Ressourcen für ihr Projekt zu verwalten. So ist sichergestellt, dass einem Entwickler, der nicht mehr am Projekt arbeitet, automatisch der Zugriff entzogen wird, ohne dass die zugrunde liegenden Zugriffsrichtlinien geändert werden müssen.

Gewünschtes Ergebnis: Benutzer sollten nur über die Berechtigungen verfügen, die für ihre Arbeit erforderlich sind. Die Benutzer sollten nur Zugriff auf Produktionsumgebungen erhalten, um eine bestimmte Aufgabe in einem begrenzten Zeitraum auszuführen. Nach Abschluss der Aufgabe sollte der Zugriff widerrufen werden. Nicht mehr benötigte Berechtigungen sollten widerrufen werden. Dies gilt auch, wenn ein Benutzer zu einem anderen Projekt wechselt oder eine andere Tätigkeit übernimmt. Administratorberechtigungen sollten nur einer kleinen Gruppe von vertrauenswürdigen Administratoren erteilt werden. Die Berechtigungen sollten regelmäßig geprüft werden, um eine schleichende Ausweitung der Berechtigungen zu vermeiden. Maschinen- oder Systemkonten sollten die geringsten Berechtigungen erhalten, die zur Ausführung ihrer Aufgaben benötigt werden.

## Typische Anti-Muster:

- Standardmäßige Gewährung von Administratorberechtigungen für Benutzer
- Den Root-Benutzer für day-to-day Aktivitäten verwenden.
- Erstellung übermäßig großzügiger Richtlinien, jedoch ohne vollständige Administratorberechtigungen
- Keine Überprüfung der Berechtigungen, um festzustellen, ob sie einen Zugriff mit der geringsten Berechtigung gewähren

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Hoch

## Implementierungsleitfaden

Das Prinzip der [geringsten Berechtigung](#) besagt, dass Identitäten nur die kleinstmögliche Menge von Aktionen ausführen dürfen, die zur Durchführung einer bestimmten Aufgabe erforderlich sind. Dies schafft ein Gleichgewicht zwischen Benutzerfreundlichkeit, Effizienz und Sicherheit. Die Anwendung dieses Prinzips trägt dazu bei, den unbeabsichtigten Zugriff zu beschränken und nachzuverfolgen, wer auf welche Ressourcen zugreifen kann. IAM-Benutzer und Rollen haben standardmäßig keine Berechtigungen. Der Root-Benutzer hat standardmäßig vollen Zugriff und sollte streng kontrolliert, überwacht und nur für [Aufgaben verwendet werden, die Root-Zugriff erfordern](#).

IAM-Richtlinien werden verwendet, um IAM-Rollen oder bestimmten Ressourcen explizit Berechtigungen zu gewähren. Beispielsweise können identitätsbasierte Richtlinien an IAM-Gruppen angehängt werden, während S3-Buckets durch ressourcenbasierte Richtlinien gesteuert werden können.

Bei der Erstellung einer IAM-Richtlinie können Sie die Dienstaktionen, Ressourcen und Bedingungen angeben, die erfüllt sein müssen, um den Zugriff zu erlauben oder AWS zu verweigern. AWS unterstützt eine Vielzahl von Bedingungen, mit denen Sie den Zugriff einschränken können. Mithilfe des `PrincipalOrgID` [Bedingungsschlüssels](#) können Sie beispielsweise Aktionen ablehnen, wenn der Anforderer nicht zu Ihrer AWS-Organisation gehört.

Mithilfe des `CalledVia` [Bedingungsschlüssels](#) können Sie auch Anfragen steuern, die AWS-Dienste in Ihrem Namen stellen, z. B. das AWS CloudFormation Erstellen einer AWS Lambda-Funktion. Sie sollten verschiedene Richtlinientypen miteinander verknüpfen, um die Gesamtberechtigungen Ihrer Benutzer festzulegen, defense-in-depth und einzuschränken. Sie können auch Beschränkungen in Bezug darauf festlegen, welche Berechtigungen unter welchen Umständen erteilt werden können. Sie können Ihren Anwendungsteams beispielsweise gestatten, ihre eigenen IAM-Richtlinien für die von ihnen erstellten Systeme zu erstellen, müssen aber auch eine [Berechtigungsgrenze](#) festlegen, um die maximalen Berechtigungen zu begrenzen, die das System erhalten kann.

## Implementierungsschritte

- Implementieren Sie Richtlinien mit den geringsten Rechten: Weisen Sie IAM-Gruppen und Rollen Zugriffsrichtlinien mit den geringsten Rechten zu, um die von Ihnen definierte Rolle oder Funktion des Benutzers widerzuspiegeln.
- Grundlegende API-Nutzungsrichtlinien: Eine Möglichkeit, die benötigten Berechtigungen zu ermitteln, ist die Überprüfung von AWS CloudTrail-Protokollen. Diese Überprüfung ermöglicht es Ihnen, Berechtigungen zu erstellen, die auf die Aktionen zugeschnitten sind, die der Benutzer tatsächlich ausführt AWS. [IAM Access Analyzer kann automatisch eine IAM-Richtlinie auf der](#)

[Grundlage von Aktivitäten generieren](#). Sie können IAM Access Advisor auf Organisations- oder Kontoebene verwenden, um [die zuletzt abgerufenen Informationen für eine bestimmte Richtlinie nachzuverfolgen](#).

- Erwägen Sie die Verwendung von [verwalteten AWS -Richtlinien für Tätigkeiten](#). Wenn Sie mit der Erstellung detaillierter Berechtigungsrichtlinien beginnen, kann es schwierig sein, zu wissen, wo Sie beginnen sollen. AWS hat Richtlinien für allgemeine Aufgaben verwaltet, z. B. für Rechnungsstellung, Datenbankadministratoren und Datenwissenschaftler. Diese Richtlinien können helfen, den Zugriff der Benutzer einzuschränken und gleichzeitig festzulegen, wie die Richtlinien für die geringste Berechtigung implementiert werden sollen.
- Unnötige Berechtigungen entfernen: Entfernen Sie Berechtigungen, die nicht benötigt werden, und schränken Sie zu großzügige Richtlinien ein. IAM Die [Access Analyzer-Richtliniengenerierung kann zur](#) Feinabstimmung der Berechtigungsrichtlinien beitragen.
- Sicherstellen, dass Benutzer eingeschränkten Zugriff auf Produktionsumgebungen haben: Benutzer sollten nur Zugriff auf Produktionsumgebungen haben, wenn es sich um einen gültigen Anwendungsfall handelt. Nachdem der Benutzer die konkreten Aufgaben ausgeführt hat, für die Zugriff auf die Produktionsumgebung erforderlich war, sollte der Zugriff widerrufen werden. Die Beschränkung des Zugriffs auf Produktionsumgebungen hilft, unbeabsichtigte Vorkommnisse mit Auswirkungen auf die Produktion zu verhindern und das Ausmaß der Auswirkungen eines unbeabsichtigten Zugriffs zu verringern.
- Denken Sie an Berechtigungsgrenzen: Eine Berechtigungsgrenze ist eine Funktion für die Verwendung einer verwalteten Richtlinie, mit der die maximalen Berechtigungen festgelegt werden, die eine identitätsbasierte Richtlinie einer Entität gewähren kann. IAM Durch eine Berechtigungsgrenze kann eine Entität nur die Aktionen durchführen, die sowohl von den identitätsbasierten Richtlinien als auch den Berechtigungsgrenzen erlaubt werden.
- [Ressourcen-Tags](#) für Berechtigungen erwägen: Ein auf Attributen basierendes Zugriffskontrollmodell, das Ressourcen-Tags verwendet, ermöglicht es Ihnen, Zugriff auf Grundlage von Ressourcenzweck, Eigentümer, Umgebung oder anderen Kriterien zu gewähren. Mithilfe von Ressourcen-Tags können Sie beispielsweise zwischen Entwicklungs- und Produktionsumgebungen unterscheiden. Mit diesen Tags können Sie den Zugriff der Entwickler auf die Entwicklungsumgebung beschränken. Durch die Kombination von Tagging und Berechtigungsrichtlinien können Sie einen differenzierten Ressourcenzugriff erzielen, ohne komplizierte, benutzerdefinierte Richtlinien für jeden Tätigkeitsbereich definieren zu müssen.
- Verwenden Sie [Richtlinien zur Dienststeuerung für](#). AWS Organizations Service-Kontrollrichtlinien steuern zentral die maximal verfügbaren Berechtigungen für Mitgliedskonten in Ihrer Organisation. Wichtig ist, dass Sie mithilfe von Service-Kontrollrichtlinien die Root-Benutzerberechtigungen in



Mitgliedskonten einschränken können. Erwägen Sie auch die Verwendung AWS Control Tower, die präskriptive verwaltete Kontrollen bietet, die eine Bereicherung bieten. AWS Organizations Sie können auch Ihre eigenen Kontrollen in Control Tower definieren.

- Richten Sie eine Benutzerlebenszyklusrichtlinie für Ihr Unternehmen ein: Richtlinien für den Benutzerlebenszyklus definieren Aufgaben, die ausgeführt werden müssen, wenn Benutzer aufgenommen werden AWS, ihre berufliche Rolle oder ihren Aufgabenbereich ändern oder auf die sie keinen Zugriff mehr benötigen. AWS Bei jedem Schritt im Lebenszyklus eines Benutzers sollten Berechtigungsprüfungen erfolgen, um sicherzustellen, dass die Berechtigungen angemessen restriktiv sind und keine schleichenden Berechtigungserweiterungen stattfinden.
- Richten Sie einen regelmäßigen Zeitplan ein, um die Berechtigungen zu überprüfen und alle nicht benötigten Berechtigungen zu entfernen: Sie sollten den Benutzerzugriff regelmäßig überprüfen, um sicherzustellen, dass Benutzer keinen übermäßigen Zugriff haben. [AWS Config](#) und IAM Access Analyzer kann Ihnen bei der Prüfung von Benutzerberechtigungen helfen.
- Erstellen Sie eine Job-Rollen-Matrix: Eine Job-Rollen-Matrix visualisiert die verschiedenen Rollen und Zugriffsebenen, die in Ihrem Umfeld erforderlich sind AWS . Mithilfe einer Job-Rollen-Matrix können Sie Berechtigungen auf der Grundlage von Benutzerzuständigkeiten in Ihrer Organisation definieren und trennen. Verwenden Sie Gruppen, anstatt Berechtigungen direkt auf einzelne Benutzer oder Rollen anzuwenden.

## Ressourcen

### Zugehörige Dokumente:

- [Gewähren der geringsten Berechtigung](#)
- [Berechtigungen, Grenzen für Entitäten IAM](#)
- [Techniken für die Erstellung von IAM Richtlinien mit den geringsten Rechten](#)
- [IAMAccess Analyzer erleichtert die Implementierung von Berechtigungen mit den geringsten Rechten, indem IAM Richtlinien auf der Grundlage der Zugriffsaktivität generiert werden](#)
- [Delegieren Sie die Rechteverwaltung an Entwickler, indem Sie IAM Rechtegrenzen verwenden](#)
- [Verfeinern von Berechtigungen mithilfe der Informationen zum letzten Zugriff](#)
- [IAMRichtlinientypen und wann sie verwendet werden sollten](#)
- [Testen von IAM Richtlinien mit dem IAM Richtliniensimulator](#)
- [Leitplanken rein AWS Control Tower](#)
- [Zero-Trust-Architekturen: Eine Perspektive AWS](#)

- [Wie lässt sich das Prinzip der geringsten Rechte umsetzen mit CloudFormation StackSets](#)
- [Attributbasierte Zugriffskontrolle \(\) ABAC](#)
- [Reduzieren des Richtlinienbereichs durch Anzeigen der Benutzeraktivität](#)
- [Anzeigen des Rollenzugriffs](#)
- [Verwenden Sie Tagging, um Ihre Umgebung zu organisieren und die Verantwortlichkeit zu fördern](#)
- [AWS -Strategien für das Tagging](#)
- [Taggen von AWS -Ressourcen](#)

Zugehörige Videos:

- [Berechtigungsmanagement der nächsten Generation](#)
- [Zero Trust: Eine Perspektive AWS](#)

Zugehörige Beispiele:

- [Labor: IAM Rechtegrenzen beim Delegieren der Rollenerstellung](#)
- [Labor: IAM Tag-basierte Zugriffskontrolle für EC2](#)

### SEC03-BP03 Notfallzugangsverfahren einrichten

Erstellen Sie einen Prozess, der im unwahrscheinlichen Fall eines Problems mit Ihrem zentralen Identitätsanbieter den Notfallzugriff auf Ihre Workloads ermöglicht.

Sie müssen Prozesse für verschiedene Ausfallmodi entwerfen, die zu einem Notfallereignis führen können. Unter normalen Umständen verbinden sich die Benutzer Ihrer Belegschaft beispielsweise über einen zentralen Identitätsanbieter ([SEC02-BP04](#)) mit der Cloud, um ihre Workloads zu verwalten. Wenn der zentrale Identitätsanbieter jedoch ausfällt oder die Konfiguration für den Verbund in der Cloud geändert wird, können sich die Benutzer in Ihrem Unternehmen möglicherweise nicht mit der Cloud verbinden. Ein Prozess für den Notfallzugriff ermöglicht autorisierten Administratoren den Zugriff auf Ihre Cloud-Ressourcen über alternative Verfahren (z. B. eine alternative Form des Verbunds oder direkter Benutzerzugriff), um Probleme mit Ihrer Verbundkonfiguration oder Ihren Workloads zu beheben. Der Prozess für den Notfallzugriff wird verwendet, bis der normale Verbundmechanismus wiederhergestellt ist.

Gewünschtes Ergebnis:

- Sie haben die Ausfallmodi definiert und dokumentiert, die als Notfall gelten: Berücksichtigen Sie dabei Ihre normalen Abläufe und die Systeme, auf die Ihre Benutzer angewiesen sind, um ihre Workloads zu verwalten. Überlegen Sie, wie jede dieser Abhängigkeiten ausfallen und zu einer Notsituation führen kann. Möglicherweise finden Sie die Fragen und bewährten Methoden in der [Säule der Zuverlässigkeit](#) hilfreich, um Ausfallarten zu identifizieren und widerstandsfähigere Systeme zu entwickeln, bei denen die Wahrscheinlichkeit von Ausfällen geringer ist.
- Sie haben die Schritte dokumentiert, die befolgt werden müssen, um einen Ausfall als Notfall zu identifizieren. Sie können beispielsweise festlegen, dass Ihre Identitätsadministratoren den Status Ihrer primären und Standby-Identitätsanbieter überprüfen müssen und, falls beide nicht verfügbar sind, ein Notfallereignis für den Ausfall eines Identitätsanbieters feststellen.
- Sie haben einen Prozess für den Notfallzugriff definiert, der für jeden Notfall- oder Ausfallmodus spezifisch ist. Wenn Sie hier möglichst detaillierte Informationen angeben, kann dies der Neigung Ihrer Benutzer entgegenwirken, einen allgemeinen Prozess für alle Arten von Notfällen zu stark zu nutzen. Ihre Prozesse für den Notfallzugriff beschreiben die Umstände, unter denen ein Prozess jeweils verwendet werden sollte, und umgekehrt Situationen, in denen der Prozess nicht verwendet werden sollte. In diesem Fall wird auf alternative Prozesse hingewiesen, die zutreffen können.
- Ihre Prozesse sind mit detaillierten Anweisungen und Playbooks, die schnell und effizient befolgt werden können, gut dokumentiert. Denken Sie daran, dass ein Notfallereignis Stress für Ihre Benutzer bedeuten kann und dass sie unter extremem Zeitdruck stehen können. Gestalten Sie Ihren Prozess daher so einfach wie möglich.

#### Typische Anti-Muster:

- Sie verfügen nicht über gut dokumentierte und gut getestete Prozesse für den Notfallzugriff. Ihre Benutzer sind nicht auf einen Notfall vorbereitet und nutzen improvisierte Prozesse, wenn er eintritt.
- Ihre Prozesse für den Notfallzugriff hängen von denselben Systemen (z. B. einem zentralen Identitätsanbieter) ab wie Ihre normalen Zugriffsmechanismen. Das bedeutet, dass der Ausfall eines solchen Systems sowohl Ihre normalen Zugriffsmechanismen als auch Ihre Notfallzugriffsmechanismen betrifft und Ihre Fähigkeit zur Wiederherstellung nach dem Ausfall beeinträchtigen kann.
- Ihre Prozesse für den Notfallzugriff werden in Situationen verwendet, die keine Notfälle sind. Ein Beispiel könnte sein, dass Ihre Benutzer Prozesse für den Notfallzugriff häufig missbrauchen, da es für sie einfacher ist, Änderungen direkt vorzunehmen, als Änderungen über eine Pipeline einzureichen.

- Ihre Prozesse für den Notfallzugriff generieren nicht genügend Protokolle, um sie zu überwachen, oder die Protokolle werden nicht so überwacht, dass Sie bei einem möglichen Missbrauch der Prozesse gewarnt werden.

Vorteile der Nutzung dieser bewährten Methode:

- Durch gut dokumentierte und gut getestete Prozesse für den Notfallzugriff können Sie die Zeit reduzieren, die Ihre Benutzer benötigen, um auf ein Notfallereignis zu reagieren und es zu beheben. Dies kann zu kürzeren Ausfallzeiten und einer höheren Verfügbarkeit der Services führen, die Sie für Ihre Kunden bereitstellen.
- Sie können jede Notfallzugriffsanfrage verfolgen und unbefugte Versuche, den Prozess für Nicht-Notfallereignisse zu missbrauchen, erkennen und darauf hinweisen.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel

### Implementierungsleitfaden

Dieser Abschnitt enthält Anleitungen zur Erstellung von Notfallzugriffsprozessen für verschiedene Ausfallmodi im Zusammenhang mit Workloads AWS, auf denen bereitgestellt wird. Zunächst finden Sie allgemeine Leitlinien, die für alle Fehlermodi gelten, gefolgt von spezifischen Anleitungen, die auf der Art des Fehlermodus basieren.

### Allgemeine Leitlinien für alle Ausfallmodi

Beachten Sie beim Entwerfen eines Prozesses für den Notfallzugriff für einen Ausfallmodus Folgendes:

- Dokumentieren Sie die Voraussetzungen und Annahmen für den Prozess: Wann soll der Prozess verwendet werden und wann nicht? Es ist hilfreich, den Ausfallmodus detailliert zu beschreiben und Annahmen zu dokumentieren, z. B. den Zustand anderer verwandter Systeme. Der Prozess für den Fehlermodus 2 geht beispielsweise davon aus, dass der Identity Provider verfügbar ist, die Konfiguration für Failure Mode 2 jedoch geändert wurde oder abgelaufen AWS ist.
- Erstellen Sie vorab Ressourcen, die für den Notfallzugriffsprozess benötigt werden ([SEC10-BP05](#)). Erstellen Sie beispielsweise vorab den Notfallzugriff AWS-Konto mit IAM Benutzern und Rollen sowie die kontenübergreifenden IAM Rollen in allen Workload-Konten. So wird sichergestellt, dass diese Ressourcen bereit und verfügbar sind, wenn ein Notfallereignis eintritt. Wenn Sie Ressourcen vorab erstellen, sind Sie nicht von der AWS [Steuerungsebene](#) APIs (die zum Erstellen und Ändern von AWS Ressourcen verwendet wird) abhängig, die im Notfall möglicherweise nicht verfügbar

ist. Wenn Sie IAM Ressourcen vorab erstellen, müssen Sie außerdem [mögliche Verzögerungen aufgrund der eventuellen](#) Konsistenz nicht berücksichtigen.

- Nehmen Sie Notfallzugriffsprozesse in Ihre Pläne für das Notfallmanagement auf ([SEC10-BP02](#)). Dokumentieren Sie, wie Notfallereignisse nachverfolgt und an andere in Ihrem Unternehmen, z. B. an Peer-Teams, Führungskräfte und gegebenenfalls extern an Kunden und Geschäftspartner, kommuniziert werden sollen.
- Definieren Sie den Prozess für Notfallzugriffsanfragen in Ihrem bestehenden Workflow-System für Serviceanfragen, falls eines vorhanden ist. In der Regel können Sie mit solchen Workflow-Systemen Eingabeformulare erstellen, um Informationen zur Anfrage zu erfassen, die Anfrage in jeder Phase des Workflows zu verfolgen und sowohl automatisierte als auch manuelle Genehmigungsschritte hinzuzufügen. Ordnen Sie jede Anfrage einem entsprechenden Notfallereignis zu, das in Ihrem Vorfalmanagement-System verfolgt wird. Mit einem einheitlichen System für Notfallzugriffe können Sie diese Anfragen in einem zentralen System verfolgen, Nutzungstrends analysieren und Ihre Prozesse verbessern.
- Stellen Sie sicher, dass Ihre Notfallzugriffsprozesse nur von autorisierten Benutzern initiiert werden können, und legen Sie fest, dass Genehmigungen von Kollegen oder Führungskräften des Benutzers erforderlich sind. Der Genehmigungsprozess sollte sowohl während als auch außerhalb der Geschäftszeiten funktionieren. Definieren Sie, wie Genehmigungsanfragen sekundäre Genehmiger berücksichtigen, falls die primären Genehmiger nicht verfügbar sind, und wie sie in Ihrer Managementkette nach oben eskaliert werden, bis sie genehmigt wurden.
- Stellen Sie sicher, dass der Prozess detaillierte Auditprotokolle und Ereignisse sowohl für erfolgreiche als auch für fehlgeschlagene Versuche, Notfallzugriff zu erhalten, generiert. Überwachen Sie sowohl den Anforderungsprozess als auch den Notfallzugriffsmechanismus, um Missbrauch oder nicht autorisierte Zugriffe zu erkennen. Korrelieren Sie Aktivitäten mit laufenden Notfallereignissen aus Ihrem Vorfalmanagement-System und senden Sie Benachrichtigungen, wenn Aktionen außerhalb der erwarteten Zeiträume erfolgen. Sie sollten beispielsweise die Aktivitäten im AWS-Konto für den Notfallzugriff überwachen und entsprechende Benachrichtigungen senden, da es im normalen Betrieb nie verwendet werden sollte.
- Testen Sie die Notfallzugriffsprozesse regelmäßig, um sicherzustellen, dass die Schritte klar sind und die richtigen Zugriffsebenen schnell und effizient gewährt werden. [Ihre Notfallzugangsprozesse sollten im Rahmen von Simulationen zur Reaktion auf Vorfälle \(SEC10-BP07\) und Notfallwiederherstellungstests \(-BP03\) getestet werden. REL13](#)

Fehlermodus 1: Der für die Verbundverbindung verwendete Identitätsanbieter ist nicht verfügbar AWS

Wie in [SEC02-BP04 beschrieben](#) [Verlassen Sie sich auf einen zentralen Identitätsanbieter](#). Wir empfehlen, sich auf einen zentralen Identitätsanbieter zu verlassen, um Ihren Mitarbeitern den Zugriff zu ermöglichen. AWS-Konten Mithilfe von IAM Identity Center können Sie sich mit mehreren AWS-Konten Mitgliedern in Ihrer AWS Organisation zusammenschließen, oder Sie können einen Verbund für einzelne Benutzer einrichten. AWS-Konten IAM In beiden Fällen authentifizieren sich die Benutzer in Ihrer Belegschaft beim zentralen Identitätsanbieter, bevor sie zu einem AWS -Anmeldeendpunkt für das Single Sign-On weitergeleitet werden.

Im unwahrscheinlichen Fall, dass der zentrale Identitätsanbieter nicht verfügbar ist, können sich die Benutzer Ihrer Belegschaft nicht mit AWS-Konten verbinden oder ihre Workloads verwalten. In diesem Notfall können Sie einen Notfallzugriff für eine kleine Gruppe von Administratoren einrichten, damit sie wichtige Aufgaben ausführen können, die nicht warten können, bis Ihre zentralen Identitätsanbieter wieder online sind. AWS-Konten Ihr Identitätsanbieter ist beispielsweise für 4 Stunden nicht verfügbar und während dieses Zeitraums müssen Sie die Obergrenzen einer Amazon EC2 Auto Scaling Scaling-Gruppe in einem Produktionskonto ändern, um einen unerwarteten Anstieg des Kundenverkehrs zu bewältigen. Ihre Notfalladministratoren sollten den Notfallzugriffsprozess befolgen, um Zugriff auf die jeweilige Produktion zu erhalten AWS-Konto und die erforderlichen Änderungen vorzunehmen.

Der Notfallzugriffsprozess basiert auf einem vorab erstellten Notfallzugriff AWS-Konto , der ausschließlich für den Notfallzugriff verwendet wird und über AWS Ressourcen (wie IAM Rollen und IAM Benutzer) verfügt, um den Notfallzugriffsprozess zu unterstützen. Während des normalen Betriebs sollte niemand auf das Notfallzugriffskonto zugreifen. Sie müssen dieses Konto auf Missbrauch überwachen und ggf. Warnungen senden (weitere Informationen finden Sie im vorherigen Abschnitt mit allgemeinen Leitlinien).

Das Notfallzugriffskonto verfügt über IAM Notfallzugriffsrollen mit der Berechtigung, kontenübergreifende Rollen in denjenigen zu übernehmen, für AWS-Konten die ein Notfallzugriff erforderlich ist. Diese IAM Rollen sind vorab erstellt und mit Vertrauensrichtlinien konfiguriert, die den Rollen des Notfallkontos IAM vertrauen.

Der Notfallzugriffsprozess kann einen der folgenden Ansätze verwenden:

- Sie können eine Gruppe von [IAM Benutzern](#) für Ihre Notfalladministratoren im Notfallzugriffskonto mit zugehörigen sicheren Passwörtern und MFA Tokens vorab erstellen. Diese IAM Benutzer sind berechtigt, die IAM Rollen zu übernehmen, die dann den kontenübergreifenden Zugriff auf die Bereiche ermöglichen, AWS-Konto in denen Notfallzugriff erforderlich ist. Wir empfehlen, so wenige solcher Benutzer wie möglich zu erstellen und jeden Benutzer einem einzelnen Notfalladministrator zuzuweisen. Während eines Notfalls meldet sich ein Notfalladministrator mit seinem Passwort

- und seinem MFA Token-Code beim Notfallzugriffskonto an, wechselt zur IAM Notfallzugriffsrolle im Notfallkonto und schließlich zur IAM Notfallzugriffsrolle im Workload-Konto, um die Notfall-Änderungsaktion durchzuführen. Der Vorteil dieses Ansatzes besteht darin, dass jeder IAM Benutzer einem Notfalladministrator zugewiesen ist und Sie anhand der Ereignisse feststellen können, welcher Benutzer angemeldet ist. CloudTrail Der Nachteil besteht darin, dass Sie mehrere IAM Benutzer mit ihren zugehörigen langlebigen Kennwörtern und Tokens verwalten müssen. MFA
- Sie können den [AWS-Konto Root-Benutzer](#) für den Notfallzugriff verwenden, um sich beim Notfallzugriffskonto anzumelden, die IAM Rolle für den Notfallzugriff und die kontoübergreifende Rolle im Workload-Konto zu übernehmen. Wir empfehlen, ein sicheres Passwort und mehrere MFA Token für den Root-Benutzer festzulegen. Wir empfehlen außerdem, das Passwort und die MFA Token in einem sicheren Tresor für Unternehmensanmeldedaten zu speichern, der eine starke Authentifizierung und Autorisierung durchsetzt. Sie sollten die Faktoren für das Zurücksetzen von Passwort und MFA Token sichern: Geben Sie als E-Mail-Adresse für das Konto eine E-Mail-Verteilerliste ein, die von Ihren Cloud-Sicherheitsadministratoren überwacht wird, und geben Sie für die Telefonnummer des Kontos eine gemeinsame Telefonnummer ein, die auch von Sicherheitsadministratoren überwacht wird. Der Vorteil dieses Ansatzes besteht darin, dass nur ein Satz von Root-Benutzeranmeldeinformationen verwaltet werden muss. Der Nachteil ist, dass sich mehrere Administratoren als Root-Benutzer anmelden können, da es sich um einen gemeinsam genutzten Benutzer handelt. Sie müssen die Protokollereignisse für den Unternehmens-Vault überprüfen, um festzustellen, welcher Administrator das Passwort für den Root-Benutzer ausgecheckt hat.

Fehlermodus 2: Die Konfiguration des Identity Providers on wurde geändert oder AWS ist abgelaufen

Damit sich die Benutzer Ihrer Belegschaft zusammenschließen können AWS-Konten, können Sie das IAM Identity Center mit einem externen Identitätsanbieter konfigurieren oder einen IAM Identitätsanbieter erstellen ([SEC02-BP04](#)). In der Regel konfigurieren Sie diese, indem Sie ein von Ihrem Identitätsanbieter SAML bereitgestelltes XML Metadatendokument importieren. Das XML Metadatendokument enthält ein X.509-Zertifikat, das einem privaten Schlüssel entspricht, den der Identitätsanbieter zum Signieren seiner Assertions verwendet. SAML

Diese Konfigurationen auf der AWS Seite können versehentlich von einem Administrator geändert oder gelöscht werden. In einem anderen Szenario läuft das importierte X.509-Zertifikat AWS möglicherweise ab und es wurden noch keine neuen Metadaten XML mit einem neuen Zertifikat importiert. AWS In beiden Szenarien kann der Verbund AWS für die Benutzer Ihrer Belegschaft unterbrochen werden, was zu einem Notfall führen kann.

In einem solchen Notfall können Sie Ihren Identitätsadministratoren Zugriff gewähren, AWS um die Verbundprobleme zu beheben. Ihr Identitätsadministrator verwendet beispielsweise das Notfallzugriffsverfahren, um sich für den Notfallzugriff anzumelden AWS-Konto, wechselt zu einer Rolle im Identity Center-Administratorkonto und aktualisiert die Konfiguration des externen Identitätsanbieters, indem er das neueste SAML XML Metadatendokument von Ihrem Identitätsanbieter importiert, um den Verbund wieder zu aktivieren. Sobald der Verbund wiederhergestellt ist, verwenden die Benutzer in Ihrer Belegschaft weiter den normalen Betriebsprozess, um sich mit ihren Workload-Konten zu verbinden.

Sie können die oben für Ausfallmodus 1 beschriebenen Vorgehensweisen befolgen, um einen Notfallzugriffsprozess zu erstellen. Sie können Ihren Identitätsadministratoren Berechtigungen nach dem Prinzip der geringsten Berechtigung gewähren, sodass sie nur auf das Identity Center-Administratorkonto zugreifen und nur in diesem Konto Aktionen für Identity Center ausführen können.

### Ausfallmodus 3: Störung von Identity Center

Für den unwahrscheinlichen Fall eines IAM Identity Center oder einer AWS-Region Störung empfehlen wir Ihnen, eine Konfiguration einzurichten, mit der Sie temporären Zugriff auf das gewähren können. AWS Management Console

Der Notfallzugriffsprozess verwendet einen direkten Verbund von Ihrem Identitätsanbieter zu IAM einem Notfallkonto. Einzelheiten zu den Prozess- und Entwurfsüberlegungen finden Sie im [Artikel zum Einrichten des Notfallzugriffs auf die AWS Management Console](#).

### Implementierungsschritte

#### Allgemeine Schritte für alle Ausfallmodi

- Erstellen Sie einen AWS-Konto speziellen Notfallzugriffsprozess. Erstellen Sie vorab die für das Konto benötigten IAM Ressourcen wie IAM Rollen oder IAM Benutzer und optional IAM Identitätsanbieter. Erstellen Sie außerdem vorab kontenübergreifende IAM Rollen im Workload AWS-Konten mit Vertrauensbeziehungen zu den entsprechenden IAM Rollen im Notfallzugriffskonto. Sie können [AWS CloudFormation StackSets with](#) verwenden AWS Organizations, um solche Ressourcen in den Mitgliedskonten Ihrer Organisation zu erstellen.
- Erstellen Sie [Richtlinien zur AWS Organizations Dienststeuerung](#) (SCPs), um das Löschen und Ändern der kontoübergreifenden IAM Rollen des Mitglieds AWS-Konten zu verhindern.
- Aktivieren Sie CloudTrail den Notfallzugriff AWS-Konto und senden Sie die Trail-Ereignisse an einen zentralen S3-Bucket in Ihrer Protokollsammlung AWS-Konto. Wenn Sie Ihre Umgebung mit



- AWS Control Tower AWS mehreren Konten einrichten und verwalten, ist jedes Konto, das Sie mit AWS Control Tower oder für das Sie sich registrieren, standardmäßig CloudTrail aktiviert und an einen S3-Bucket in einem dedizierten Protokollarchiv gesendet. AWS Control Tower AWS-Konto
- Überwachen Sie die Aktivitäten des Notfallzugriffskontos, indem Sie EventBridge Regeln erstellen, die bei der Anmeldung auf der Konsole und den API Aktivitäten der IAM Notfallrollen übereinstimmen. Senden Sie Benachrichtigungen an Ihr Security Operations Center, wenn Aktivitäten außerhalb eines laufenden Notfallereignisses stattfinden, das in Ihrem Vorfallmanagement-System nachverfolgt wurde.

Zusätzliche Schritte für Fehlermodus 1: Der für den Verbund verwendete Identitätsanbieter AWS ist nicht verfügbar und Fehlermodus 2: Identity Provider-Konfiguration aktiviert wurde geändert oder AWS ist abgelaufen

- Erstellen Sie vorab Ressourcen, je nachdem, welchen Mechanismus Sie für den Notfallzugriff wählen:
  - IAMBenutzer verwenden: Erstellen Sie die IAM Benutzer vorab mit sicheren Passwörtern und zugehörigen MFA Geräten.
  - Root-Benutzer des Notfallkontos verwenden: Konfigurieren Sie den Root-Benutzer mit einem sicheren Passwort und speichern Sie das Passwort im Unternehmens-Vault für Anmeldeinformationen. Ordnen Sie dem Root-Benutzer mehrere physische MFA Geräte zu und speichern Sie die Geräte an Orten, auf die Mitglieder Ihres Notfalladministratorteam schnell zugreifen können.

Zusätzliche Schritte für den Ausfallmodus 3 (Störung von Identity Center)

- Wie unter [Notfallzugriff einrichten](#) beschrieben AWS Management Console, erstellen Sie im Notfallzugriff einen IAM Identitätsanbieter AWS-Konto, um einen direkten SAML Verbund von Ihrem Identitätsanbieter aus zu ermöglichen.
- Erstellen Sie Notfalleinsatzgruppen in Ihrem Identitätsanbieter ohne Mitglieder.
- Erstellen Sie IAM Rollen, die den Notfalleinsatzgruppen im Notfallzugriffskonto entsprechen.

Ressourcen

Zugehörige bewährte Methoden für Well-Architected:

- [SEC02-BP04 Verlassen Sie sich auf einen zentralen Identitätsanbieter](#)

- [SEC03-BP02 Gewähren Sie den Zugriff mit den geringsten Rechten](#)
- [SEC10-BP02 Entwickeln Sie Pläne für das Vorfalmanagement](#)
- [SEC10-BP07 Spieltage veranstalten](#)

Zugehörige Dokumente:

- [Richten Sie den Notfallzugang zum ein AWS Management Console](#)
- [Ermöglicht Verbundbenutzern der SAML Version 2.0 den Zugriff auf AWS Management Console](#)
- [„Break Glass“-Zugriff](#)

Zugehörige Videos:

- [AWS re:Invent 2022 — Vereinfachen Sie den Zugang Ihrer bestehenden Belegschaft mit Identity Center IAM](#)
- [AWS re:inForce 2022 — \(\) tiefer Einblick AWS Identity and Access Management IAM](#)

Zugehörige Beispiele:

- [AWS -Rolle „Break Glass“](#)
- [AWS Customer Playbook Framework](#)
- [AWS -Beispiele von Playbooks für die Vorfallsreaktion](#)

SEC03-BP04 Berechtigungen kontinuierlich reduzieren

Wenn Ihre Teams bestimmen, welchen Zugriff sie benötigen, entfernen Sie unnötige Berechtigungen und erstellen Sie Überprüfungsprozesse, damit jederzeit dem Prinzip der geringsten Berechtigung entsprochen wird. Überwachen Sie Ihre Identitäten kontinuierlich und entfernen Sie ungenutzte Identitäten und Berechtigungen für den Zugriff von Menschen und Maschinen.

Gewünschtes Ergebnis: Die Genehmigungsrichtlinien sollten dem Prinzip der geringsten Berechtigung entsprechen. Wenn Zuständigkeiten und Rollen immer besser definiert werden, müssen Sie Ihre Berechtigungsrichtlinien prüfen, um unnötige Berechtigungen zu entfernen. Dieses Konzept verringert die Auswirkungen, wenn Anmeldeinformationen versehentlich offengelegt werden oder wenn anderweitig ohne Genehmigung darauf zugegriffen wird.

Typische Anti-Muster:

- Standardmäßige Gewährung von Administratorberechtigungen für Benutzer
- Erstellung übermäßig großzügiger Richtlinien, jedoch ohne vollständige Administratorberechtigungen
- Aufbewahrung von Berechtigungsrichtlinien, nachdem sie nicht mehr benötigt werden

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel

### Implementierungsleitfaden

Wenn Teams und Projekte gerade erst mit der Arbeit beginnen, können lockere Richtlinien verwendet werden, um Innovationen und Agilität zu unterstützen. In einer Entwicklungs- oder Testumgebung können Entwickler beispielsweise Zugriff auf eine Vielzahl von AWS Diensten erhalten. Wir empfehlen, den Zugriff kontinuierlich zu prüfen und auf Services und Serviceaktionen einzuschränken, die für die anstehende Aufgabe wirklich benötigt werden. Wir empfehlen diese Evaluierung für menschliche und für maschinelle Identitäten. Maschinenidentitäten, manchmal auch System- oder Dienstkonto genannt, sind Identitäten, die den AWS Zugriff auf Anwendungen oder Server ermöglichen. Dieser Zugriff ist besonders in einer Produktionsumgebung wichtig, in der übermäßig lockere Zugriffsregeln weitreichende Auswirkungen haben und möglicherweise Kundendaten offen legen könnten.

AWS bietet mehrere Methoden zur Identifizierung ungenutzter Benutzer, Rollen, Berechtigungen und Anmeldeinformationen. AWS kann auch dabei helfen, die Zugriffsaktivitäten von IAM Benutzern und Rollen, einschließlich der zugehörigen Zugriffsschlüssel, und den Zugriff auf AWS Ressourcen wie Objekte in Amazon S3 S3-Buckets zu analysieren. AWS Identity and Access Management Access Analyzer Die Generierung von Richtlinien kann Ihnen dabei helfen, restriktive Berechtigungsrichtlinien zu erstellen, die auf den tatsächlichen Diensten und Aktionen basieren, mit denen ein Auftraggeber interagiert. Die [attributbasierte Zugriffskontrolle \(ABAC\)](#) kann dazu beitragen, die Berechtigungsverwaltung zu vereinfachen, da Sie Benutzern anhand ihrer Attribute Berechtigungen erteilen können, anstatt die Berechtigungsrichtlinien direkt an jeden Benutzer anzuhängen.

### Implementierungsschritte

- Verwendung [AWS Identity and Access Management Access Analyzer](#): IAM Access Analyzer hilft bei der Identifizierung von Ressourcen in Ihrer Organisation und Ihren Konten, z. B. Amazon Simple Storage Service (Amazon S3) -Buckets oder IAM Rollen, die [mit einer externen Entität gemeinsam genutzt](#) werden.

- Verwenden Sie die [IAMAccess Analyzer-Richtliniengenerierung](#): Mit der IAM Access Analyzer-Richtliniengenerierung können Sie [detaillierte Berechtigungsrichtlinien erstellen, die auf der Zugriffsaktivität eines IAM Benutzers oder einer Rolle basieren](#).
- Legen Sie einen akzeptablen Zeitrahmen und eine akzeptable Nutzungsrichtlinie für IAM Benutzer und Rollen fest: Verwenden Sie den [Zeitstempel des letzten Zugriffs](#), um [ungenutzte Benutzer und Rollen zu identifizieren und](#) sie zu entfernen. Überprüfen Sie die Informationen zum letzten Service- und Aktionszugriff überprüfen, um [Berechtigungen für bestimmte Benutzer und Rollen zu identifizieren und festzulegen](#). Sie können beispielsweise Informationen zum letzten Zugriff verwenden, um die spezifischen Amazon S3-Aktionen zu identifizieren, die Ihre Anwendungsrolle erfordert, und den Zugriff der Rolle auf diese Aktionen beschränken. Die Funktionen für Informationen, auf die zuletzt zugegriffen wurde, sind in verfügbar AWS Management Console und ermöglichen es Ihnen, sie programmgesteuert in Ihre Infrastruktur-Workflows und automatisierten Tools zu integrieren.
- [Erwägen Sie die Protokollierung von Datenereignissen in AWS CloudTrail](#): Standardmäßig werden CloudTrail keine Datenereignisse wie Amazon S3 S3-Aktivitäten auf Objektebene (z. B. GetObject undDeleteObject) oder Amazon DynamoDB-Tabellenaktivitäten (z. B. und) protokolliert. PutItem DeleteItem Erwägen Sie die Verwendung der Protokollierung dieser Ereignisse, um zu ermitteln, welche Benutzer und Rollen Zugriff auf bestimmte Amazon S3-Objekte oder DynamoDB-Tabellenelemente benötigen.

## Ressourcen

### Zugehörige Dokumente:

- [Gewähren der geringsten Berechtigung](#)
- [Entfernen unnötiger Anmeldeinformationen](#)
- [Was ist? AWS CloudTrail](#)
- [Arbeiten mit -Richtlinien](#)
- [Protokollierung und Überwachung in DynamoDB](#)
- [Verwenden der CloudTrail Ereignisprotokollierung für Amazon S3 S3-Buckets und -Objekte](#)
- [Abrufen von Berichten über Anmeldeinformationen für Ihr AWS-Konto](#)

### Zugehörige Videos:

- [Werden Sie in 60 Minuten oder weniger zum IAM Policy Master](#)

- [Trennung von Pflichten, geringste Berechtigung, Delegation und CI/CD](#)
- [AWS Re:inForce 2022 — AWS Identity and Access Management \(\) tiefer Einblick IAM](#)

### SEC03-BP05 Definieren Sie Genehmigungsleitlinien für Ihre Organisation

Verwenden Sie Maßnahmen zum Integritätsschutz, um den Umfang der verfügbaren Berechtigungen, die Prinzipalen gewährt werden können, einzuschränken. Die Bewertungskette für Genehmigungsrichtlinien umfasst Ihren Integritätsschutz, um bei Autorisierungsentscheidungen die effektiven Berechtigungen eines Prinzipals zu bestimmen. Sie können Maßnahmen zum Integritätsschutz mit einem ebenenbasierten Ansatz definieren. Wenden Sie einige Maßnahmen zum Integritätsschutz allgemein für Ihre gesamte Organisation an und andere granular auf Sitzungen mit temporärem Zugriff.

Gewünschtes Ergebnis: Die Umgebungen sind durch die Verwendung separater AWS-Konten klar voneinander abgegrenzt. Richtlinien zur Servicesteuerung (SCPs) werden verwendet, um unternehmensweite Genehmigungsrichtlinien zu definieren. Umfassender angelegte Maßnahmen zu Integritätsschutz werden auf den Hierarchieebenen festgelegt, die der Root Ihrer Organisation am nächsten sind, und strengerer Integritätsschutz wird näher an der Ebene der einzelnen Konten festgelegt. Sofern unterstützt, definieren Ressourcenrichtlinien die Bedingungen, die ein Prinzipal erfüllen muss, um Zugriff auf eine Ressource zu erhalten. Die Ressourcenrichtlinien schränken auch den Umfang der erlaubten Aktionen ein, wo dies angebracht ist. Berechtigungsgrenzen werden auf Prinzipale verteilt, die Workload-Berechtigungen verwalten und die Verwaltung von Berechtigungen an einzelne Workload-Besitzer delegieren.

Typische Anti-Muster:

- Mitglieder werden AWS-Konten innerhalb einer [AWS Organisation](#) erstellt, aber nicht SCPs dazu verwendet, die Nutzung und die für ihre Root-Anmeldeinformationen verfügbaren Rechte einzuschränken.
- Zuweisung von Berechtigungen auf der Grundlage der geringsten Berechtigung, aber kein Integritätsschutz für die maximale Anzahl von Berechtigungen, die gewährt werden können
- Sie verlassen sich auf die implizite Ablehnungsgrundlage der AWS IAM Einschränkung von Berechtigungen und vertrauen darauf, dass Richtlinien keine unerwünschte ausdrückliche Genehmigungsberechtigung gewähren.
- Mehrere Workload-Umgebungen in derselben AWS-Konto Umgebung ausführen und sich dann auf Mechanismen wie VPCs Tags oder Ressourcenrichtlinien verlassen, um Berechtigungsgrenzen durchzusetzen.

Vorteile der Nutzung dieser bewährten Methode: Durch den Integritätsschutz für Berechtigungen kann das Vertrauen gestärkt werden, dass keine unerwünschten Berechtigungen erteilt werden können, selbst wenn eine Berechtigungsrichtlinie dies versucht. Dies kann die Definition und Verwaltung von Berechtigungen vereinfachen, da der maximale Umfang der zu berücksichtigenden Berechtigungen reduziert wird.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel

### Implementierungsleitfaden

Wir empfehlen Ihnen, einen ebenenbasierten Ansatz zu verwenden, um für Maßnahmen für den Integritätsschutz für Ihre Organisation zu definieren. Dieser Ansatz reduziert systematisch die maximale Anzahl der möglichen Berechtigungen, wenn weitere Ebenen hinzugefügt werden. So können Sie den Zugriff nach dem Prinzip der geringsten Berechtigung gewähren und das Risiko eines unbeabsichtigten Zugriffs aufgrund einer falschen Konfiguration der Richtlinie verringern.

Der erste Schritt zur Einrichtung zum Integritätsschutz ist die Isolierung Ihrer Workloads und Umgebungen in getrennten AWS-Konten. Principals eines Kontos können ohne ausdrückliche Genehmigung nicht auf Ressourcen in einem anderen Konto zugreifen, selbst wenn sich beide Konten in derselben AWS Organisation oder derselben [Organisationseinheit \(OU\)](#) befinden. Sie können KontenOUs, die Sie als eine Einheit verwalten möchten, zu einer Gruppe zusammenfassen.

Der nächste Schritt besteht darin, die maximale Anzahl von Berechtigungen zu reduzieren, die Sie Prinzipalen innerhalb der Mitgliedskonten Ihrer Organisation erteilen können. Zu diesem Zweck können Sie [Dienststeuerungsrichtlinien \(SCPs\)](#) verwenden, die Sie entweder auf eine Organisationseinheit oder ein Konto anwenden können. SCPs kann allgemeine Zugriffskontrollen durchsetzen, z. B. die Beschränkung des Zugriffs auf bestimmte AWS-Regionen, verhindern, dass Ressourcen gelöscht werden, oder die Deaktivierung potenziell riskanter Serviceaktionen. SCPs die Sie auf das Stammkonto Ihrer Organisation anwenden, wirkt sich nur auf deren Mitgliedskonten aus, nicht auf das Verwaltungskonto. SCPs regeln nur die Prinzipale innerhalb Ihrer Organisation. Sie kontrollieren SCPs nicht die Prinzipale außerhalb Ihrer Organisation, die auf Ihre Ressourcen zugreifen.

Ein weiterer Schritt besteht darin, mithilfe von [IAMRessourcenrichtlinien](#) die verfügbaren Aktionen festzulegen, die Sie für die von ihnen verwalteten Ressourcen ergreifen können, sowie alle Bedingungen, die der amtierende Schulleiter erfüllen muss. Dies kann so umfassend sein, dass Sie alle Aktionen zulassen, solange der Prinzipal Teil Ihrer Organisation ist (unter Verwendung des PrincipalOrgId [Bedingungsschlüssels](#)), oder so detailliert sein, dass nur bestimmte Aktionen einer bestimmten IAM Rolle zugelassen werden. Sie können einen ähnlichen Ansatz verfolgen, wenn es

um Bedingungen in den Richtlinien für das Vertrauen in IAM Rollen geht. Wenn eine Ressourcen- oder Rollenvertrauensrichtlinie explizit einen Prinzipal in demselben Konto benennt wie die Rolle oder Ressource, für die er zuständig ist, benötigt dieser Prinzipal keine angehängte IAM Richtlinie, die dieselben Berechtigungen gewährt. Wenn sich der Prinzipal in einem anderen Konto als der Ressource befindet, benötigt der Prinzipal eine angehängte IAM Richtlinie, die diese Berechtigungen gewährt.

Oft möchte ein Workload-Team die für seine Workload erforderlichen Berechtigungen verwalten. Dazu müssen sie möglicherweise neue IAM Rollen und Berechtigungsrichtlinien erstellen. Sie können den maximalen Umfang der Berechtigungen, die das Team gewähren darf, in einer [IAMBerechtigungsgrenze](#) erfassen und dieses Dokument einer IAM Rolle zuordnen, die das Team dann zur Verwaltung seiner IAM Rollen und Berechtigungen verwenden kann. Durch diesen Ansatz können sie ihre Arbeit erledigen und gleichzeitig die Risiken minimieren, die mit IAM administrativem Zugriff verbunden sind.

Ein detaillierterer Schritt ist die Implementierung von Techniken zur Verwaltung privilegierter Zugriffe (PAM) und zur Verwaltung temporärer Zugriffsberechtigungen (TEAM). Ein Beispiel dafür PAM ist, dass Prinzipale eine Multi-Faktor-Authentifizierung durchführen müssen, bevor sie privilegierte Aktionen ausführen. Weitere Informationen finden Sie unter [Konfiguration des MFA API -geschützten Zugriffs](#). TEAM erfordert eine Lösung, die die Genehmigung und den Zeitrahmen verwaltet, innerhalb dessen ein Principal über erweiterte Zugriffsrechte verfügen darf. Ein Ansatz besteht darin, den Principal vorübergehend zur Rollenvertrauensrichtlinie für eine IAM Rolle mit erhöhtem Zugriff hinzuzufügen. Ein anderer Ansatz besteht darin, im Normalbetrieb die einem Prinzipal von einer IAM Rolle erteilten Berechtigungen mithilfe einer [Sitzungsrichtlinie einzuschränken](#) und diese Einschränkung dann während des genehmigten Zeitfensters vorübergehend aufzuheben. Weitere Informationen zu Lösungen, die AWS und ausgewählte Partner validiert haben, finden Sie unter [Temporärer erweiterter Zugriff](#).

## Implementierungsschritte

1. Isolieren Sie Ihre Workloads und Umgebungen in separaten AWS-Konten.
2. Wird verwendet SCPs, um die maximale Anzahl an Berechtigungen zu reduzieren, die Prinzipalen innerhalb der Mitgliedskonten Ihrer Organisation gewährt werden können.
  - a. Wir empfehlen Ihnen, beim Verfassen Ihrer Anfrage eine Zulassungsliste zu verwenden SCPs, bei der alle Aktionen mit Ausnahme der Aktionen, die Sie zulassen, und der Bedingungen, unter denen sie zulässig sind, verweigert werden. Beginnen Sie damit, die Ressourcen zu definieren, die Sie kontrollieren möchten, und setzen Sie den Effekt auf „Verweigern“. Verwenden Sie das NotAction Element, um alle Aktionen außer den von Ihnen angegebenen zu verweigern.

Kombinieren Sie dies gegebenenfalls mit einer NotLike Bedingung, um zu definieren, wann diese Aktionen zulässig sind, z. B. StringNotLike und ArnNotLike.

b. Weitere Informationen finden Sie unter [Beispiele für Service-Kontrollrichtlinie](#).

3. Verwenden Sie IAM Ressourcenrichtlinien, um den Umfang einzugrenzen und Bedingungen für zulässige Aktionen mit Ressourcen festzulegen. Verwenden Sie Bedingungen in Richtlinien zur IAM Rollenvertrauensstellung, um Beschränkungen für die Übernahme von Rollen festzulegen.
4. Weisen Sie IAM Rollen IAM Rechtegrenzen zu, die Workload-Teams dann verwenden können, um ihre eigenen IAM Workload-Rollen und -Berechtigungen zu verwalten.
5. Evaluieren Sie PAM und TEAM finden Sie Lösungen, die auf Ihre Bedürfnisse zugeschnitten sind.

## Ressourcen

### Zugehörige Dokumente:

- [Datenperimeter auf AWS](#)
- [Einrichten des Berechtigungs-Integritätsschutzes mithilfe von Datenperimetern](#)
- [Auswertungslogik für Richtlinien](#)

### Zugehörige Beispiele:

- [Beispiele für Service-Kontrollrichtlinie](#)

### Zugehörige Tools:

- [AWS -Lösung: Temporäre erweiterte Zugriffsverwaltung](#)
- [Validierte Sicherheitspartnerlösungen für TEAM](#)

## SEC03-BP06 Zugriff basierend auf dem Lebenszyklus verwalten

Überwachen Sie die Berechtigungen, die Ihren Prinzipalen (Benutzern, Rollen und Gruppen) während ihres gesamten Lebenszyklus in Ihrer Organisation gewährt werden, und passen Sie sie an. Passen Sie die Gruppenmitgliedschaften an, wenn Benutzer ihre Rolle ändern, und entfernen Sie den Zugriff, wenn ein Benutzer die Organisation verlässt.

Gewünschtes Ergebnis: Sie überwachen und passen die Berechtigungen während des gesamten Lebenszyklus der Prinzipale innerhalb der Organisation an und reduzieren so das Risiko unnötiger



Rechte. Sie gewähren den entsprechenden Zugriff, wenn Sie einen Benutzer anlegen. Sie ändern den Zugriff, wenn sich die Aufgaben des Benutzers ändern, und Sie entfernen den Zugriff, wenn der Benutzer nicht mehr aktiv ist oder die Organisation verlassen hat. Sie verwalten Änderungen an Ihren Benutzern, Rollen und Gruppen zentral. Sie verwenden Automatisierung, um Änderungen in Ihren Umgebungen zu verbreiten. AWS

Typische Anti-Muster:

- Sie gewähren Identitäten im Voraus übermäßige oder weitreichende Zugriffsrechte, die über das ursprünglich erforderliche Maß hinausgehen.
- Sie unterlassen die Überprüfung der Zugriffsprivilegien und passen sie an, wenn sich die Rollen und Verantwortlichkeiten der Identitäten im Laufe der Zeit ändern.
- Sie belassen inaktive oder beendete Identitäten mit aktiven Zugriffsrechten. Dies erhöht das Risiko eines unbefugten Zugriffs.
- Sie automatisieren die Verwaltung von Identitätslebenszyklen nicht.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel

Implementierungsleitfaden

Verwalten Sie die Zugriffsprivilegien, die Sie Identitäten (z. B. Benutzern, Rollen, Gruppen) gewähren, sorgfältig und passen Sie sie im Laufe ihres Lebenszyklus an. Dieser Lebenszyklus umfasst die anfängliche Onboarding-Phase, laufende Änderungen der Rollen und Verantwortlichkeiten und schließlich das Offboarding oder die Kündigung. Verwalten Sie den Zugriff proaktiv je nach Stadium des Lebenszyklus, um die richtige Zugriffsstufe zu erhalten. Halten Sie sich an das Prinzip der geringsten Berechtigung, um das Risiko übermäßiger oder unnötiger Zugriffsberechtigungen zu verringern.

Sie können den Lebenszyklus von IAM Benutzern direkt innerhalb des AWS-Konto Identity Center oder über einen Verbund zwischen Ihrem Personaldienstleister und AWS IAM Identity Center verwalten. Für IAM Benutzer können Sie Benutzer und die zugehörigen Berechtigungen innerhalb von erstellen, ändern und löschen AWS-Konto. Für Verbundbenutzer können Sie IAM Identity Center verwenden, um ihren Lebenszyklus zu verwalten, indem Sie Benutzer- und Gruppeninformationen vom Identitätsanbieter Ihrer Organisation mithilfe des Systems for Cross-Domain Identity Management ( ) SCIM -Protokolls synchronisieren.

SCIM ist ein offenes Standardprotokoll für die automatisierte Bereitstellung und Deprovisionierung von Benutzeridentitäten in verschiedenen Systemen. Durch die Integration Ihres Identitätsanbieters mit

IAM Identity Center können Sie Benutzer- und Gruppeninformationen automatisch synchronisieren und so überprüfen, ob Zugriffsberechtigungen aufgrund von Änderungen in der autoritativen Identitätsquelle Ihres Unternehmens gewährt, geändert oder widerrufen wurden. SCIM

Wenn sich die Rollen und Zuständigkeiten der Mitarbeiter in Ihrer Organisation ändern, passen Sie ihre Zugriffsrechte entsprechend an. Sie können die Berechtigungssätze von IAM Identity Center verwenden, um verschiedene Aufgabenrollen oder Verantwortlichkeiten zu definieren und sie den entsprechenden IAM Richtlinien und Berechtigungen zuzuordnen. Wenn sich die Rolle eines Mitarbeiters ändert, können Sie die ihm zugewiesenen Berechtigungen aktualisieren, um die neuen Verantwortlichkeiten zu berücksichtigen. Vergewissern Sie sich, dass sie über den erforderlichen Zugriff verfügen, und halten Sie sich dabei an das Prinzip der geringsten Berechtigung.

### Implementierungsschritte

1. Definieren und dokumentieren Sie einen Lebenszyklusprozess für die Zugriffsverwaltung, einschließlich Verfahren für die Gewährung des Erstzugriffs, regelmäßige Überprüfungen und das Offboarding.
2. Implementieren Sie IAM Rollen, Gruppen und Berechtigungsgrenzen, um den Zugriff gemeinsam zu verwalten und die maximal zulässigen Zugriffsebenen durchzusetzen.
3. Integrieren Sie mithilfe IAM von Identity Center einen föderierten Identitätsanbieter (wie Microsoft Active Directory, Okta, Ping Identity) als autoritative Quelle für Benutzer- und Gruppeninformationen.
4. Verwenden Sie das SCIM Protokoll, um Benutzer- und Gruppeninformationen vom Identity Provider mit dem Identity Store von IAM Identity Center zu synchronisieren.
5. Erstellen Sie in IAM Identity Center Berechtigungssätze, die unterschiedliche Aufgabenbereiche oder Verantwortlichkeiten innerhalb Ihrer Organisation repräsentieren. Definieren Sie die entsprechenden IAM Richtlinien und Berechtigungen für jeden Berechtigungssatz.
6. Führen Sie regelmäßige Zugriffsüberprüfungen, sofortigen Zugriffsentzug und eine kontinuierliche Verbesserung des Lebenszyklusprozesses der Zugriffsverwaltung ein.
7. Schulung und Sensibilisierung der Mitarbeiter für die bewährten Methoden der Zugriffsverwaltung.

### Ressourcen

Zugehörige bewährte Methoden:

- [SEC02-BP04 Verlassen Sie sich auf einen zentralen Identitätsanbieter](#)

## Zugehörige Dokumente:

- [Verwaltung Ihrer Identitätsquelle](#)
- [Identitäten im Identity Center verwalten IAM](#)
- [Verwenden von AWS Identity and Access Management Access Analyzer](#)
- [IAMGenerierung von Access Analyzer-Richtlinien](#)

## Zugehörige Videos:

- [AWS re:InForce 2023 — Verwalten Sie temporären erhöhten Zugriff mit Identity Center AWS IAM](#)
- [AWS re:Invent 2022 — Vereinfachen Sie Ihren bestehenden Personalzugriff mit Identity Center IAM](#)
- [AWS re:Invent 2022 — Nutzen Sie das Potenzial von IAM Richtlinien und beschränken Sie Ihre Berechtigungen mit Access Analyzer](#)

## SEC03-BP07 Analysieren Sie den öffentlichen und kontoübergreifenden Zugriff

Überwachen Sie kontinuierlich Ergebnisse, die den öffentlichen und kontoübergreifenden Zugriff betreffen. Beschränken Sie den öffentlichen und kontoübergreifenden Zugriff ausschließlich auf Ressourcen, die diese Art von Zugriff benötigen.

Gewünschtes Ergebnis: Finden Sie heraus, welche Ihrer AWS Ressourcen gemeinsam genutzt werden und mit wem. Überwachen und prüfen Sie kontinuierlich Ihre freigegebenen Ressourcen, um sicherzustellen, dass sie nur für autorisierte Prinzipale freigegeben sind.

## Typische Anti-Muster:

- Fehlendes Inventar gemeinsam genutzter Ressourcen
- Nichtbefolgung eines Prozesses zur Genehmigung von kontoübergreifendem oder öffentlichem Zugriff auf Ressourcen

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Niedrig

## Implementierungsleitfaden

Wenn Ihr Konto registriert ist AWS Organizations, können Sie der gesamten Organisation, bestimmten Organisationseinheiten oder einzelnen Konten Zugriff auf Ressourcen gewähren. Wenn

Ihr Konto nicht zu einer Organisation gehört, können Sie Ressourcen für einzelne Konten freigeben. Sie können direkten kontoübergreifenden Zugriff gewähren, indem Sie ressourcenbasierte Richtlinien verwenden — z. B. die [Bucket-Richtlinien von Amazon Simple Storage Service \(Amazon S3\)](#) — oder indem Sie einem Principal in einem anderen Konto erlauben, eine IAM Rolle in Ihrem Konto zu übernehmen. Verifizieren Sie bei der Verwendung von Ressourcenrichtlinien, dass der Zugriff nur autorisierten Prinzipalen gewährt wird. Definieren Sie einen Prozess für die Genehmigung aller Ressourcen, die öffentlich verfügbar sein müssen.

[AWS Identity and Access Management Access Analyzer](#) nutzt [nachweisbare Sicherheit](#), um alle Zugriffspfade zu einer Ressource von außerhalb ihres Kontos zu identifizieren. Es überprüft Ressourcenrichtlinien kontinuierlich und meldet Ergebnisse des öffentlichen und kontoübergreifenden Zugriffs, um Ihnen die Analyse potenziell umfassender Zugriffe zu erleichtern. Erwägen Sie, IAM Access Analyzer mit AWS Organizations zu konfigurieren, um sicherzustellen, dass Sie alle Ihre Konten einsehen können. IAM mit Access Analyzer können Sie auch eine [Vorschau der Ergebnisse anzeigen](#), bevor Sie Ressourcenberechtigungen bereitstellen. So können Sie sicherstellen, dass mit den Richtlinienänderungen nur der beabsichtigte öffentliche und kontoübergreifende Zugriff auf Ihre Ressourcen gewährt wird. Wenn Sie den Zugriff auf mehrere Konten planen, können Sie mithilfe von [Vertrauensrichtlinien](#) steuern, in welchen Fällen eine Rolle übernommen werden kann. Sie könnten beispielsweise den [PrincipalOrgId-Bedingungsschlüssel verwenden, um Versuche, eine Rolle von außerhalb Ihres AWS Organizations zu übernehmen, abzulehnen](#).

[AWS Config kann falsch konfigurierte Ressourcen melden](#) und mithilfe von AWS Config Richtlinienprüfungen Ressourcen erkennen, für die öffentlicher Zugriff konfiguriert ist. Dienste wie z. B. [AWS Control Tower](#) und [AWS Security Hub](#) vereinfachen den Einsatz von Detektivkontrollen und Leitplanken, um öffentlich gefährdete AWS Organizations Ressourcen zu identifizieren und zu beseitigen. AWS Control Tower hat beispielsweise eine verwaltete Leitplanke, die erkennen kann, ob [EBS Amazon-Snapshots von wiederhergestellt werden](#) können. AWS-Konten

## Implementierungsschritte

- Erwägen Sie [AWS Config die Verwendung von for AWS Organizations](#): AWS Config ermöglicht es Ihnen, Ergebnisse aus mehreren Konten innerhalb eines delegierten Administratorkontos AWS Organizations zu aggregieren. Dies bietet einen umfassenden Überblick und ermöglicht die [AWS-Config-Regeln kontenübergreifende Bereitstellung, um öffentlich zugängliche Ressourcen zu erkennen](#).
- Configure AWS Identity and Access Management Access Analyzer IAM Access Analyzer hilft Ihnen dabei, Ressourcen in Ihrer Organisation und Ihren Konten zu identifizieren, z. B. Amazon S3 S3-Buckets oder IAM Rollen, die [mit einer externen Entität gemeinsam genutzt](#) werden.

- Verwenden Sie automatische Problemlösung AWS Config , um auf Änderungen in der Konfiguration des öffentlichen Zugriffs von Amazon S3 S3-Buckets zu reagieren: [Sie können die Einstellungen zum Blockieren des öffentlichen Zugriffs für Amazon S3 S3-Buckets automatisch aktivieren.](#)
- Überwachung und Warnmeldungen implementieren, um festzustellen, ob Amazon S3-Buckets öffentlich geworden sind: [Überwachung und Warnmeldungen](#) müssen aktiviert sein, damit erkannt werden kann, wenn Amazon S3 Block Public Access deaktiviert wird und ob Amazon S3-Buckets öffentlich geworden sind. Wenn Sie verwenden AWS Organizations, können Sie außerdem eine [Service Control-Richtlinie](#) erstellen, die Änderungen an den Amazon S3 S3-Richtlinien für den öffentlichen Zugriff verhindert. AWS Trusted Advisor sucht nach Amazon S3 S3-Buckets, die über Open-Access-Berechtigungen verfügen. Bucket-Berechtigungen, die allen Benutzern den Zugriff zum Hochladen/Löschen einräumen, bergen ein hohes Potenzial für Sicherheitsrisiken, da alle Personen Elemente in einem Bucket hinzufügen, ändern oder löschen können. Bei der Trusted Advisor Prüfung werden explizite Bucket-Berechtigungen und zugehörige Bucket-Richtlinien untersucht, die die Bucket-Berechtigungen möglicherweise außer Kraft setzen. Sie können es auch verwenden AWS Config , um Ihre Amazon S3 S3-Buckets für den öffentlichen Zugriff zu überwachen. Weitere Informationen finden Sie unter [So verwenden AWS Config Sie Amazon S3 S3-Buckets, die öffentlichen Zugriff zulassen, zu überwachen und darauf zu reagieren.](#) Bei der Überprüfung des Zugriffs ist es wichtig zu berücksichtigen, welche Arten von Daten in Amazon S3-Buckets enthalten sind. [Amazon Macie](#) hilft dabei, sensible Daten wie PIIPHI, und Anmeldeinformationen wie private Daten oder AWS Schlüssel zu erkennen und zu schützen.

## Ressourcen

### Zugehörige Dokumente:

- [Verwenden von AWS Identity and Access Management Access Analyzer](#)
- [AWS Control Tower steuert die Bibliothek](#)
- [AWS Grundlegender Standard für bewährte Sicherheitsverfahren](#)
- [Von AWS Config verwaltete Regeln](#)
- [AWS Trusted Advisor -Referenz prüfen](#)
- [AWS Trusted Advisor Prüfergebnisse mit Amazon überwachen EventBridge](#)
- [AWS Config Regeln für alle Konten in Ihrer Organisation verwalten](#)
- [AWS Config und AWS Organizations](#)
- [Machen Sie Ihre AMI öffentlich verfügbar, um sie in Amazon zu verwenden EC2](#)

## Zugehörige Videos:

- [Bewährte Methoden für den Schutz Ihrer Mehrkonten-Umgebung](#)
- [Tauchen Sie tief in IAM Access Analyzer ein](#)

## SEC03-BP08 Teilen Sie Ressourcen sicher innerhalb Ihrer Organisation

Wenn die Anzahl der Workloads zunimmt, müssen Sie möglicherweise den Zugriff auf Ressourcen in diesen Workloads ausweiten oder diese Ressourcen mehrfach über mehrere Konten hinweg zugänglich machen. Möglicherweise haben Sie Konstrukte zur Untergliederung Ihrer Umgebung, etwa für Entwicklungs-, Test- und Produktionsumgebungen. Solche Trennungskonstrukte schränken Sie jedoch nicht in der Lage ein, sicher zu teilen. Durch die gemeinsame Nutzung sich überschneidender Ressourcen können Sie übermäßigen betrieblichen Aufwand reduzieren und eine konsistente Umgebung schaffen, ohne dass Sie raten müssen, was Sie vielleicht versäumt haben, wenn Sie eine Ressource mehrmals erstellen.

Gewünschtes Ergebnis: Vermeiden Sie den unbeabsichtigten Zugriff, indem Sie sichere Methoden verwenden, um Ressourcen innerhalb Ihrer Organisation zu teilen, und unterstützen Sie Ihre Initiative zur Verhinderung von Datenverlust. Reduzieren Sie Ihren organisatorischen Aufwand gegenüber der Verwaltung einzelner Komponenten, senken Sie die Zahl von Fehlern durch das manuelle mehrmalige Erstellen identischer Ressourcen, und steigern Sie die Skalierbarkeit Ihrer Workloads. Sie können von kürzeren Lösungszeiten in Szenarien mit mehreren Fehlerpunkten profitieren und Ihr Vertrauen in die Bestimmung erhöhen, wann eine Komponente nicht mehr benötigt wird. Verbindliche Anleitungen zur Analyse extern gemeinsam genutzter Ressourcen finden Sie unter [SEC03-BP07 Analysieren Sie den öffentlichen und kontoübergreifenden Zugriff](#).

## Typische Anti-Muster:

- Fehlen eines Prozesses für die kontinuierliche Überwachung und die automatische Benachrichtigung bei unerwarteten externen Freigaben
- Fehlen einer Basislinie dazu, was freigegeben werden sollte und was nicht
- Die standardmäßige Verwendung einer sehr offenen Richtlinie, anstatt Ressourcen explizit freizugeben, wenn sie benötigt werden
- Manuelle Erstellung grundlegender Ressourcen bei Bedarf, die sich überlappen

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel

## Implementierungsleitfaden

Gestalten Sie Ihre Zugriffskontrollen und -muster so, dass die Nutzung freigegebener Ressourcen kontrolliert wird und nur mit vertrauenswürdigen Entitäten möglich ist. Überwachen Sie freigegebene Ressourcen, prüfen Sie kontinuierlich den Zugriff darauf und erhalten Sie Benachrichtigungen bei unangemessenen oder unerwarteten Freigaben. Lesen Sie [Analysieren des öffentlichen und kontoübergreifenden Zugriffs](#), um eine Governance einzurichten, mit der Sie den externen Zugriff auf diejenigen Ressourcen beschränken können, die ihn benötigen, und um einen Prozess zur kontinuierlichen Überwachung und automatischen Warnung einzurichten.

Die kontoübergreifende gemeinsame Nutzung innerhalb AWS Organizations wird von [einer Reihe von AWS Diensten](#) unterstützt [AWS Security Hub](#), z. B. [Amazon GuardDuty](#) und [AWS Backup](#). Diese Services ermöglichen die Freigabe von Daten für ein zentrales Konto, ihre Zugänglichkeit von einem zentralen Konto aus sowie die Verwaltung von Ressourcen und Daten von einem zentralen Konto aus. AWS Security Hub Kann beispielsweise Ergebnisse von einzelnen Konten auf ein zentrales Konto übertragen, wo Sie alle Ergebnisse einsehen können. AWS Backup kann ein Backup für eine Ressource erstellen und es für mehrere Konten freigeben. Sie können [AWS Resource Access Manager](#)(AWS RAM) verwenden, um andere gemeinsame Ressourcen wie [VPCSubnetze und Transit Gateway Gateway-Anhänge](#) oder [SageMaker Amazon-Pipelines](#) gemeinsam zu nutzen. [AWS Network Firewall](#)

Um Ihr Konto so zu beschränken, dass nur Ressourcen innerhalb Ihrer Organisation gemeinsam genutzt werden, verwenden Sie [Richtlinien zur Servicesteuerung \(SCPs\)](#), um den Zugriff auf externe Principals zu verhindern. Kombinieren Sie bei der gemeinsamen Nutzung von Ressourcen identitätsbasierte Kontrollen und Netzwerkkontrollen, um [einen Datenperimeter für Ihre Organisation zu schaffen](#), der zum Schutz vor unbeabsichtigtem Zugriff beiträgt. Ein Datenperimeter ist ein Satz von präventiven Maßnahmen zum Integritätsschutz, die dabei helfen, sicherzustellen, dass nur vertrauenswürdige Identitäten aus erwarteten Netzwerken auf vertrauenswürdige Ressourcen zugreifen. Diese Kontrollen begrenzen, welche Ressourcen gemeinsam genutzt werden, und verhindern die gemeinsame Nutzung oder Offenlegung von Ressourcen, die nicht zugelassen werden sollten. Als Teil Ihres Datenperimeters können Sie beispielsweise VPC Endpunktrichtlinien und die `AWS:PrincipalOrgId` Bedingung verwenden, um sicherzustellen, dass die Identitäten, die auf Ihre Amazon S3 S3-Buckets zugreifen, Ihrer Organisation gehören. Es ist wichtig zu beachten, dass [SCPsdies nicht für dienstbezogene Rollen oder Dienstprinzipale gilt](#). AWS

Wenn Sie Amazon S3 verwenden, [schalten Sie es ACLs für Ihren Amazon S3 S3-Bucket](#) aus und verwenden Sie IAM Richtlinien, um die Zugriffskontrolle zu definieren. [Um den Zugriff auf einen Amazon S3-Ursprung von Amazon einzuschränken](#) CloudFront, migrieren Sie von Origin

Access Identity (OAI) zu Origin Access Control (OAC), die zusätzliche Funktionen wie serverseitige Verschlüsselung mit unterstützt. [AWS Key Management Service](#)

In manchen Fällen möchten Sie möglicherweise die Freigabe von Ressourcen außerhalb Ihrer Organisation zulassen oder einer Drittpartei den Zugriff auf Ihre Ressourcen gewähren. Verbindliche Anleitungen zur Verwaltung von Berechtigungen für die externe gemeinsame Nutzung von Ressourcen finden Sie unter [Verwaltung von Berechtigungen](#).

## Implementierungsschritte

### 1. Verwenden. AWS Organizations

AWS Organizations ist ein Kontoverwaltungsservice, mit dem Sie mehrere Konten zu einer Organisation AWS-Konten zusammenfassen können, die Sie erstellen und zentral verwalten. Sie können Ihre Konten in Organisationseinheiten (OUs) gruppieren und jeder Organisationseinheit unterschiedliche Richtlinien zuordnen, um Ihre Budget-, Sicherheits- und Compliance-Anforderungen zu erfüllen. Sie können auch steuern, wie Dienste für AWS künstliche Intelligenz (KI) und maschinelles Lernen (ML) Daten sammeln und speichern können, und die Verwaltung mehrerer Konten der in Organizations integrierten AWS Dienste nutzen.

### 2. Integrieren Sie in AWS Organizations AWS Dienste.

Wenn Sie einen AWS Dienst verwenden, um in Ihrem Namen Aufgaben in den Mitgliedskonten Ihrer Organisation auszuführen, AWS Organizations erstellt dieser Dienst in jedem Mitgliedskonto eine IAM dienstbezogene Rolle (SLR). Sie sollten den vertrauenswürdigen Zugriff mit dem AWS Management Console AWS APIs, dem oder dem AWS CLI verwalten. Anleitungen zur Aktivierung des vertrauenswürdigen Zugriffs finden Sie unter [Verwendung AWS Organizations mit anderen AWS Diensten und AWS Diensten, die Sie mit Organizations verwenden können](#).

### 3. Richten Sie einen Datenperimeter ein.

Der AWS Perimeter wird in der Regel als eine Organisation dargestellt, die von verwaltet wird. AWS Organizations Neben lokalen Netzwerken und Systemen wird der Zugriff auf AWS Ressourcen von vielen als Perimeter von My angesehen. AWS Das Ziel des Perimeters besteht darin, zu überprüfen, ob der Zugriff erlaubt ist, wenn die Identität und die Ressource vertrauenswürdig sind und es sich um ein erwartetes Netzwerk handelt.

#### a. Definieren und implementieren Sie die Perimeter.



Folgen Sie für jede Autorisierungsbedingung den im Whitepaper [Perimeter-Implementierung](#) im AWS Whitepaper Building a Perimeter on beschriebenen Schritte. Verbindliche Anleitungen zum Schutz der Netzwerkschicht finden Sie unter [Schutz von Netzwerken](#).

- b. Sorgen Sie für kontinuierliche Überwachung und Benachrichtigung.

[AWS Identity and Access Management Access Analyzer](#) hilft bei der Identifizierung von Ressourcen in Ihrer Organisation und Ihren Konten, die mit externen Entitäten geteilt werden. Sie können [IAM Access Analyzer integrieren AWS Security Hub](#), um Ergebnisse für eine Ressource von IAM Access Analyzer an Security Hub zu senden und zu aggregieren, um den Sicherheitsstatus Ihrer Umgebung zu analysieren. Um zu integrieren, aktivieren Sie sowohl IAM Access Analyzer als auch Security Hub in jeder Region in jedem Konto. Sie können es auch verwenden AWS-Config-Regeln, um die Konfiguration zu überprüfen und die entsprechende Partei zu benachrichtigen, indem Sie [AWS Chatbot with](#) verwenden AWS Security Hub. Anschließend können Sie [AWS Systems Manager -Automatisierungsdokumente](#) verwenden, um Ressourcen zu korrigieren, die den Anforderungen nicht entsprechen.

- c. Eine verbindliche Anleitung zur kontinuierlichen Überwachung und Meldung von extern gemeinsam genutzten Ressourcen finden Sie unter [Analysieren des öffentlichen und kontoübergreifenden Zugriffs](#).

4. Verwenden Sie die gemeinsame Nutzung von Ressourcen in AWS Diensten und schränken Sie sie entsprechend ein.

Viele AWS Dienste ermöglichen es Ihnen, Ressourcen mit einem anderen Konto zu teilen oder eine Ressource in einem anderen Konto als Ziel zu verwenden, z. B. [Amazon Machine Images \(AMIs\)](#) und [AWS Resource Access Manager \(AWS RAM\)](#). Beschränken Sie `ModifyImageAttribute` API die Angabe der vertrauenswürdigen Konten, AMI mit denen Sie die teilen möchten. Geben Sie die `ram:RequestedAllowsExternalPrincipals` Bedingung AWS RAM an, wenn Sie die gemeinsame Nutzung auf Ihre Organisation beschränken möchten, um den Zugriff durch nicht vertrauenswürdige Identitäten zu verhindern. Verbindliche Hinweise und Überlegungen finden Sie unter [Gemeinsame Nutzung von Ressourcen und externe Ziele](#).

5. Dient AWS RAM zum sicheren Teilen in einem Konto oder mit anderen. AWS-Konten

[AWS RAM](#) unterstützt die sichere Freigabe der Ressourcen, die Sie erstellt haben, an Rollen und Benutzer in Ihrem Konto sowie an andere AWS-Konten. AWS RAM Ermöglicht es Ihnen, in einer Umgebung mit mehreren Konten eine Ressource einmal zu erstellen und sie mit anderen Konten zu teilen. Dieser Ansatz trägt dazu bei, Ihren Betriebsaufwand zu reduzieren und sorgt gleichzeitig

für Konsistenz, Transparenz und Überprüfbarkeit durch Integrationen mit Amazon CloudWatch und AWS CloudTrail, die Sie nicht erhalten, wenn Sie den kontoübergreifenden Zugriff verwenden.

Wenn Sie über Ressourcen verfügen, die Sie zuvor mithilfe einer ressourcenbasierten Richtlinie gemeinsam genutzt haben, können Sie die [PromoteResourceShareCreatedFromPolicyAPI](#) oder eine gleichwertige Option verwenden, um die Ressourcenfreigabe auf eine vollständige Ressourcenfreigabe hinaufzustufen. AWS RAM

In manchen Fällen müssen Sie möglicherweise weitere Schritte unternehmen, um Ressourcen freizugeben. Um beispielsweise einen verschlüsselten Snapshot zu teilen, müssen Sie [einen AWS KMS Schlüssel gemeinsam](#) nutzen.

## Ressourcen

Zugehörige bewährte Methoden:

- [SEC03-BP07 Analysieren Sie den öffentlichen und kontoübergreifenden Zugriff](#)
- [SEC03-BP09 Ressourcen sicher mit Dritten teilen](#)
- [SEC05-BP01 Netzwerkschichten erstellen](#)

Zugehörige Dokumente:

- [Bucket-Besitzer gewährt kontoübergreifende Berechtigung für Objekte, die er nicht besitzt](#)
- [Wie verwendet man Trust Policies mit IAM](#)
- [Aufbau von Data Perimeter auf AWS](#)
- [So verwenden Sie eine externe ID, wenn Sie Dritten Zugriff auf Ihre AWS Ressourcen gewähren](#)
- [AWS Dienste, die Sie mit nutzen können AWS Organizations](#)
- [Einrichtung eines Datenperimeters für AWS: Erlauben Sie nur vertrauenswürdigen Identitäten den Zugriff auf Unternehmensdaten](#)

Zugehörige Videos:

- [Granulärer Zugriff mit AWS Resource Access Manager](#)
- [Schützen Sie Ihren Datenperimeter mit Endpunkten VPC](#)
- [Einrichtung eines Datenperimeters am AWS](#)

## Zugehörige Tools:

- [Beispiele für Richtlinien für Datenperimeter](#)

### SEC03-BP09 Ressourcen sicher mit Dritten teilen

Die Sicherheit Ihrer Cloud-Umgebung endet nicht bei Ihrer Organisation. Möglicherweise stützt sich Ihre Organisation auf eine Drittpartei, um einen Teil Ihrer Daten zu verwalten. Die Rechteverwaltung für das von einem Drittanbieter verwaltete System sollte der Praxis folgen, bei der der just-in-time Zugriff nach dem Prinzip der geringsten Rechte mit temporären Zugangsdaten erfolgt. Durch die enge Zusammenarbeit mit einer Drittpartei können Sie die möglichen Auswirkungen und das Risiko unbeabsichtigter Zugriffe gemeinsam senken.

Gewünschtes Ergebnis: Langfristige AWS Identity and Access Management (IAM)

Anmeldeinformationen, IAM Zugriffsschlüssel und geheime Schlüssel, die einem Benutzer zugeordnet sind, können von jedem verwendet werden, solange die Anmeldeinformationen gültig und aktiv sind. Durch die Verwendung einer IAM Rolle und temporärer Anmeldeinformationen können Sie Ihre allgemeine Sicherheitslage verbessern, indem Sie den Aufwand für die Aufbewahrung langfristiger Anmeldeinformationen reduzieren, einschließlich des Verwaltungs- und Betriebsaufwands für diese vertraulichen Daten. Indem Sie in der IAM Vertrauensrichtlinie eine universell eindeutige Kennung (UUID) für die externe ID verwenden und die mit der IAM Rolle verknüpften IAM Richtlinien unter Ihrer Kontrolle behalten, können Sie überprüfen und sicherstellen, dass der Zugriff, der dem Dritten gewährt wird, nicht zu freizügig ist. Verbindliche Anleitungen zur Analyse extern gemeinsam genutzter Ressourcen finden Sie unter [SEC03-BP07 Analysieren Sie den öffentlichen und kontoübergreifenden Zugriff](#).

### Typische Anti-Muster:

- Verwenden Sie die standardmäßige IAM Vertrauensrichtlinie ohne jegliche Bedingungen.
- Verwendung langfristiger IAM Anmeldeinformationen und Zugriffsschlüssel.
- Extern IDs wiederverwenden.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Mittel

### Implementierungsleitfaden

Möglicherweise möchten Sie die gemeinsame Nutzung von Ressourcen außerhalb Ihres Kontos zulassen AWS Organizations oder Dritten Zugriff darauf gewähren. So könnte etwa eine Drittpartei

eine Überwachungslösung bereitstellen, die auf Ressourcen in Ihrem Konto zugreifen muss. Erstellen Sie in diesen Fällen eine IAM kontoübergreifende Rolle mit nur den Rechten, die der Drittanbieter benötigt. Definieren Sie außerdem eine Vertrauensrichtlinie mithilfe der [externen ID-Bedingung](#). Wenn eine externe ID verwendet wird, können Sie oder die Drittpartei eine eindeutige ID für jede(n) Kunden, Drittpartei oder Tenancy generieren. Die eindeutige ID sollte nach ihrer Erstellung ausschließlich von Ihnen kontrolliert werden. Die Drittpartei muss einen Prozess implementieren, durch den die externe ID in sicherer, prüfbarer und reproduzierbarer Weise dem Kunden zugeordnet wird.

Sie können Roles [Anywhere auch verwenden, um IAM IAM Rollen](#) für Anwendungen zu verwalten, die nicht zu AWS diesem Zweck gehören. AWS APIs

Wenn die Drittpartei keinen Zugriff mehr auf Ihre Umgebung benötigt, entfernen Sie die Rolle. Vermeiden Sie die Weitergabe langfristiger Anmeldeinformationen an Dritte. Achten Sie auf andere AWS Dienste, die das Teilen von Inhalten unterstützen. Dies AWS Well-Architected Tool ermöglicht beispielsweise die [gemeinsame Nutzung eines Workloads](#) mit anderen und [AWS Resource Access Manager](#) hilft Ihnen AWS-Konten, eine AWS Ressource, die Sie besitzen, sicher mit anderen Konten zu teilen.

## Implementierungsschritte

1. Verwenden Sie kontoübergreifende Rollen, um Zugriff auf externe Konten zu gewähren.

[Kontoübergreifende Rollen](#) reduzieren die Menge vertraulicher Informationen, die von externen Konten und Dritten gespeichert werden, um ihre Kunden zu betreuen. Mit kontoübergreifenden Rollen können Sie Dritten, wie AWS Partner z. B. Konten oder anderen Konten in Ihrer Organisation, auf sichere Weise Zugriff auf AWS Ressourcen in Ihrem Konto gewähren und gleichzeitig die Möglichkeit behalten, diesen Zugriff zu verwalten und zu überprüfen.

Möglicherweise stellt Ihnen die Drittpartei Dienstleistungen aus einer hybriden Infrastruktur heraus bereit oder ruft Daten zu einem anderen Standort ab. IAM Mit [Roles Anywhere](#) können Sie Workloads von Drittanbietern sicher mit Ihren AWS Workloads interagieren lassen und so den Bedarf an langfristigen Anmeldeinformationen weiter reduzieren.

Sie sollten keine langfristigen Anmeldeinformationen oder mit Benutzern verbundene Zugriffsschlüssel für die externe Gewährung des Zugriffs auf Konten verwenden. Verwenden Sie stattdessen kontoübergreifende Rollen, um kontoübergreifenden Zugriff zu gewähren.

2. Verwenden Sie eine externe ID für Dritte.

Mithilfe einer [externen ID](#) können Sie festlegen, wer eine Rolle in einer IAM Vertrauensrichtlinie übernehmen kann. Die Vertrauensrichtlinie kann verlangen, dass der Benutzer, der die Rolle annimmt, die Bedingung und das Ziel seiner Aktivität bestätigt. Außerdem kann der Kontoinhaber die Umstände festlegen, unter denen die Rolle angenommen werden kann. Die Hauptfunktion des externen Ausweises besteht darin, das Problem des [verwirrten Stellvertreters](#) zu lösen und zu verhindern.

Verwenden Sie eine externe ID, wenn Sie AWS-Konto Eigentümer sind und eine Rolle für einen Drittanbieter konfiguriert haben, der AWS-Konten zusätzlich zu Ihrer auf andere zugreift, oder wenn Sie Rollen im Namen verschiedener Kunden übernehmen können. Arbeiten Sie mit Ihrem Drittanbieter zusammen oder legen AWS Partner Sie eine externe ID-Bedingung fest, die in die IAM Vertrauensrichtlinie aufgenommen werden soll.

### 3. Verwenden Sie ein universell einzigartiges externes IDs Gerät.

Implementieren Sie einen Prozess, der einen zufälligen eindeutigen Wert für eine externe ID generiert, z. B. einen universell eindeutigen Bezeichner ()UUID. Ein Drittanbieter, der externe Daten für IDs verschiedene Kunden wiederverwendet, löst das Problem des verwirrten Stellvertreters nicht, da Kunde A möglicherweise Daten von Kunde B einsehen kann, indem er die Rolle ARN von Kunde B zusammen mit der duplizierten externen ID verwendet. In einer Umgebung mit mehreren Mandanten, in der ein Drittanbieter mehrere Kunden mit unterschiedlichen Kunden unterstützt AWS-Konten, muss der Drittanbieter für jeden eine andere eindeutige ID als externe ID verwenden. AWS-Konto Der Drittanbieter ist dafür verantwortlich, doppelte externe Daten zu erkennen IDs und jeden Kunden sicher seiner jeweiligen externen ID zuzuordnen. Die Drittpartei muss durch Testen sicherstellen, dass sie die Rolle nur annehmen kann, wenn die externe ID angegeben wird. Der Drittanbieter sollte die Kundenrolle ARN und die externe ID nicht speichern, bis die externe ID benötigt wird.

Die externe ID wird nicht als Secret behandelt, ihr Wert darf aber nicht leicht zu erraten sein wie etwa eine Telefonnummer, ein Name oder eine Konto-ID. Machen Sie die externe ID zu einem schreibgeschützten Feld, damit sie nicht für illegitime Einrichtungen geändert werden kann.

Die externe ID kann von Ihnen oder von der Drittpartei generiert werden. Richten Sie einen Prozess ein, um festzulegen, wer für die Generierung der ID verantwortlich ist. Unabhängig von der Entität, die die externe ID erstellt, setzt die Drittpartei Eindeutigkeit und Formate in konsistenter Weise für alle Kunden durch.

### 4. Verwenden Sie vom Kunden bereitgestellte langfristige Anmeldeinformationen nicht mehr.

Verwerfen Sie die Verwendung langfristiger Anmeldeinformationen und verwenden Sie kontoübergreifende Rollen oder IAM Roles Anywhere. Wenn Sie langfristige Anmeldeinformationen verwendet müssen, formulieren Sie einen Plan für die Migration rollenbasierter Zugriffe. Einzelheiten zur Verwaltung von Schlüsseln finden Sie unter [Identitätsverwaltung](#). Arbeiten Sie außerdem mit Ihrem AWS-Konto Team und dem Drittanbieter zusammen, um ein Runbook zur Risikominderung zu erstellen. Verbindliche Anleitungen zur Reaktion auf Sicherheitsvorfälle und zur Minderung ihre potenziellen Auswirkungen finden Sie unter [Vorfallsreaktion](#).

5. Stellen Sie sicher, dass die Einrichtung über verbindliche Anleitungen verfügt oder automatisiert ist.

Die Richtlinie, die für den kontoübergreifenden Zugriff in Ihren Konten erstellt wurde, muss dem [Prinzip der geringsten Berechtigung](#) entsprechen. Der Drittanbieter muss ein Rollenrichtliniendokument oder einen automatisierten Einrichtungsmechanismus bereitstellen, der eine AWS CloudFormation Vorlage oder eine gleichwertige Vorlage für Sie verwendet. Dies reduziert die Gefahr von Fehlern durch die manuelle Erstellung von Richtlinien und bietet einen Überwachungspfad. Weitere Informationen zur Verwendung einer AWS CloudFormation Vorlage zum Erstellen kontenübergreifender Rollen finden Sie unter [Kontoübergreifende Rollen](#).

Die Drittpartei muss einen automatisierten und prüfbaren Einrichtungsmechanismus bereitstellen. Sie sollten jedoch die Einrichtung der Rolle automatisieren, indem Sie das Rollenrichtliniendokument verwenden, das den erforderlichen Zugriff angibt. Mithilfe einer AWS CloudFormation Vorlage oder einer gleichwertigen Vorlage sollten Sie im Rahmen der Prüfungspraxis stets auf Änderungen achten und Abweichungen erkennen.

6. Berücksichtigen Sie Änderungen.

Ihre Kontostruktur und Ihr Bedarf an einer Drittpartei bzw. deren Serviceangebots können sich über Nacht ändern. Sie sollten Änderungen und Ausfälle antizipieren und mit den richtigen Personen, Prozessen und Technologielösungen entsprechend planen. Prüfen Sie regelmäßig das von Ihnen bereitgestellte Zugriffsniveau und implementieren Sie Erkennungsverfahren, die Sie auf unerwartete Änderungen aufmerksam machen. Überwachen und prüfen Sie die Verwendung der Rolle und des externen Datenspeichers. IDs Sie sollten darauf vorbereitet sein, den Zugriff der Drittpartei temporär oder dauerhaft zu widerrufen, wenn sich unerwartete Änderungen oder Zugriffsmuster ergeben. Messen Sie auch die Auswirkungen Ihrer Widerrufaktion, einschließlich der dafür benötigten Zeit, der involvierten Personen, der Kosten und der Auswirkungen auf andere Ressourcen.

Verbindliche Anleitungen zu Erkennungsmethoden finden Sie unter [Bewährte Methoden zur Erkennung](#).

## Ressourcen

Zugehörige bewährte Methoden:

- [SEC02-BP02 Temporäre Anmeldeinformationen verwenden](#)
- [SEC03-BP05 Definieren Sie Genehmigungsleitlinien für Ihre Organisation](#)
- [SEC03-BP06 Zugriff basierend auf dem Lebenszyklus verwalten](#)
- [SEC03-BP07 Analysieren Sie den öffentlichen und kontoübergreifenden Zugriff](#)
- [SEC04 Erkennung](#)

Zugehörige Dokumente:

- [Bucket-Besitzer gewährt kontoübergreifende Berechtigung für Objekte, die er nicht besitzt](#)
- [Wie verwendet man Vertrauensrichtlinien mit IAM Rollen](#)
- [Delegieren Sie den Zugriff AWS-Konten mithilfe von Rollen IAM](#)
- [Wie greife ich auf Ressourcen in einer anderen AWS-Konto Nutzung IAM zu?](#)
- [Bewährte Sicherheitsmethoden in IAM](#)
- [Logik für die kontoübergreifende Richtlinienbewertung](#)
- [So verwenden Sie eine externe ID, wenn Sie Dritten Zugriff auf Ihre AWS Ressourcen gewähren](#)
- [Sammeln von Informationen aus AWS CloudFormation Ressourcen, die in externen Konten mit benutzerdefinierten Ressourcen erstellt wurden](#)
- [Sichere Verwendung einer externen ID für den Zugriff auf AWS Konten, die anderen gehören](#)
- [Erweitern Sie IAM Rollen auf Workloads außerhalb von IAM IAM Roles Anywhere](#)

Zugehörige Videos:

- [Wie erlaube ich Benutzern oder Rollen einen separaten AWS-Konto Zugriff auf meine? AWS-Konto](#)
- [AWS re:Invent 2018: Werden Sie in 60 Minuten oder weniger zum IAM Policy Master](#)
- [AWS Knowledge Center Live: IAM Bewährte Verfahren und Designentscheidungen](#)

## Zugehörige Beispiele:

- [Well-Architected Lab — Übernahme einer kontoübergreifenden IAM Rolle bei Lambda \(Stufe 300\)](#)
- [Kontoübergreifenden Zugriff auf Amazon DynamoDB konfigurieren](#)
- [AWS STS Tool zur Netzwerkabfrage](#)

## Erkennung

### Frage

- [SEC4. Wie werden Sicherheitsereignisse erkannt und untersucht?](#)

### SEC4. Wie werden Sicherheitsereignisse erkannt und untersucht?

Erfassen und analysieren Sie Ereignisse anhand von Protokollen und Metriken, um mehr Transparenz zu erhalten. Reagieren Sie auf Sicherheitsereignisse und potenzielle Bedrohungen, um Ihre Workload zu schützen.

### Bewährte Methoden

- [SEC04-BP01 Dienst- und Anwendungsprotokollierung konfigurieren](#)
- [SEC04-BP02 Erfassen von Protokollen, Ergebnissen und Kennzahlen an standardisierten Orten](#)
- [SEC04-BP03 Korrelieren und bereichern Sie Sicherheitswarnungen](#)
- [SEC04-BP04 Behebung nicht richtlinienkonformer Ressourcen einleiten](#)

### SEC04-BP01 Dienst- und Anwendungsprotokollierung konfigurieren

Bewahren Sie Protokolle zu Sicherheitsereignissen von Services und Anwendungen auf. Dabei handelt es sich um ein grundlegendes Sicherheitsprinzip für Prüfungen, Ermittlungen und betriebliche Anwendungsfälle sowie um eine allgemeine Sicherheitsanforderung, die auf Standards, Richtlinien und Verfahren in den Bereichen Unternehmensführung, Risiko und Compliance (GRC) basiert.

Gewünschtes Ergebnis: Ein Unternehmen sollte in der Lage sein, Sicherheitsereignisprotokolle von AWS Diensten und Anwendungen zuverlässig und konsistent und zeitnah abzurufen, wenn dies zur Erfüllung eines internen Prozesses oder einer Verpflichtung erforderlich ist, z. B. bei der Reaktion auf Sicherheitsvorfälle. Erwägen Sie die Zentralisierung von Protokollen für bessere betriebliche Ergebnisse.



## Typische Anti-Muster:

- Protokolle werden dauerhaft gespeichert oder zu früh gelöscht.
- Jeder kann auf die Protokolle zugreifen.
- Für die Verwaltung und Verwendung von Protokollen werden ausschließlich manuelle Prozesse genutzt.
- Alle Arten von Protokollen werden gespeichert, nur für den Fall, dass sie benötigt werden.
- Die Protokollintegrität wird nur bei Bedarf geprüft.

Vorteile der Einführung dieser bewährten Methode: Implementieren Sie einen Mechanismus zur Ursachenanalyse (RCA) für Sicherheitsvorfälle und eine Beweisquelle für Ihre Governance-, Risiko- und Compliance-Verpflichtungen.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Hoch

## Implementierungsleitfaden

Bei einer Sicherheitsuntersuchung oder in anderen bedarfsabhängigen Anwendungsfällen müssen Sie relevante Protokolle konsultieren können, um alle Aspekte und den Zeitrahmen des Vorfalls zu verstehen. Protokolle werden auch für die Generierung von Alarmen benötigt, die darauf hinweisen, dass bestimmte Ereignisse vorgekommen sind. Es ist sehr wichtig, Abfrage-, Abruf- sowie Benachrichtigungsmechanismen auszuwählen, zu aktivieren, zu speichern und einzurichten.

## Implementierungsschritte

- Wählen und aktivieren Sie Protokollquellen. Vor einer Sicherheitsuntersuchung müssen Sie relevante Protokolle erfassen, um die Aktivitäten in einem AWS-Konto retroaktiv rekonstruieren zu können. Wählen und aktivieren Sie für Ihre Workloads relevante Protokollquellen.

Die Kriterien für die Auswahl der Protokollquelle sollten auf den Anwendungsfällen Ihres Unternehmens basieren. Richten Sie für jede AWS-Konto Verwendung AWS CloudTrail oder einen AWS Organizations Trail einen Trail ein und konfigurieren Sie dafür einen Amazon S3 S3-Bucket.

AWS CloudTrail ist ein Protokollierungsdienst, der API getätigte Anrufe anhand von Aktivitäten des AWS-Konto AWS Erfassungsdienstes verfolgt. Er ist standardmäßig aktiviert und bietet eine 90-tägige Aufbewahrung von Verwaltungsereignissen, die [über den CloudTrail Ereignisverlauf mit dem AWS Management Console AWS CLI, oder einem AWS SDK abgerufen](#) werden können. Für eine längere Aufbewahrung und Sichtbarkeit von Datenereignissen [erstellen Sie einen CloudTrail Trail](#)

und verknüpfen ihn mit einem Amazon S3 S3-Bucket und optional mit einer CloudWatch Amazon-Protokollgruppe. Alternativ können Sie einen [CloudTrail Lake](#) erstellen, der CloudTrail Protokolle für bis zu sieben Jahre aufbewahrt und eine SQL basierte Abfragefunktion bietet

AWS empfiehlt Kunden, Netzwerk-Traffic und DNS Logs mit [VPCFlow Logs bzw. Amazon Route 53 Resolver Query Logs](#) zu VPC aktivieren und diese entweder in einen Amazon S3 S3-Bucket oder eine CloudWatch Protokollgruppe zu streamen. Sie können ein VPC Flussprotokoll für eine VPC, ein Subnetz oder eine Netzwerkschnittstelle erstellen. Bei VPC Flow Logs können Sie auswählen, wie und wo Sie Flow Logs verwenden, um die Kosten zu senken.

AWS CloudTrail Logs, VPC Flow Logs und Route 53-Resolver-Abfrageprotokolle sind die grundlegenden Protokollierungsquellen zur Unterstützung von Sicherheitsuntersuchungen in AWS. Sie können [Amazon Security Lake](#) auch verwenden, um diese Protokolldaten im Apache Parquet-Format und im Open Cybersecurity Schema Framework (OCSF) zu sammeln, zu normalisieren und zu speichern, das für Abfragen bereit ist. Security Lake unterstützt auch andere AWS Protokolle und Protokolle aus Quellen von Drittanbietern.

AWS Services können Protokolle generieren, die nicht von den grundlegenden Protokollquellen erfasst werden, wie z. B. Elastic Load Balancing AWS WAF Balancing-Logs, Logs, AWS Config Recorder-Logs, GuardDuty Amazon-Ergebnisse, Amazon Elastic Kubernetes Service (AmazonEKS) Audit-Logs und EC2 Amazon-Instance-Betriebssystem- und Anwendungsprotokolle. Eine vollständige Liste von Protokoll- und Überwachungslösungen finden Sie unter [Anhang A: Definitionen der Cloud-Funktionen – Protokollierung und Ereignisse](#) in der [Anleitung zur Reaktion auf AWS -Sicherheitsvorfälle](#).

- Recherchieren Sie die Protokollierungsfunktionen für jeden AWS Service und jede Anwendung: Jeder AWS Service und jede Anwendung bietet Ihnen Optionen für die Protokollspeicherung, von denen jede über eigene Aufbewahrungs- und Lebenszyklusfunktionen verfügt. Die beiden gängigsten Protokollspeicherdienste sind Amazon Simple Storage Service (Amazon S3) und Amazon CloudWatch. Für lange Aufbewahrungszeiten wird die Verwendung von Amazon S3 empfohlen, wegen seiner Kosteneffektivität und der flexiblen Lebenszyklus-Funktionen. Wenn Amazon CloudWatch Logs die primäre Protokollierungsoption ist, sollten Sie als Option die Archivierung von Protokollen, auf die weniger häufig zugegriffen wird, in Amazon S3 in Betracht ziehen.
- Wählen Sie den Protokollspeicher aus: Die Wahl des Protokollspeichers hängt generell vom verwendeten Abfragetool, den Aufbewahrungsfunktionen, der Vertrautheit damit und den Kosten ab. Die wichtigsten Optionen für die Protokollspeicherung sind ein Amazon S3 S3-Bucket oder eine CloudWatch Protokollgruppe.

Ein Amazon S3-Bucket bietet kosteneffektiven und dauerhaften Speicher mit optionaler Lebenszyklusrichtlinie. In Amazon S3-Buckets gespeicherte Protokolle können mit Services wie Amazon Athena abgefragt werden.

Eine CloudWatch Protokollgruppe bietet dauerhaften Speicherplatz und eine integrierte Abfragefunktion über CloudWatch Logs Insights.

- Identifizieren Sie die geeignete Protokollaufbewahrung: Wenn Sie einen Amazon S3 S3-Bucket oder eine CloudWatch Protokollgruppe zum Speichern von Protokollen verwenden, müssen Sie für jede Protokollquelle angemessene Lebenszyklen einrichten, um die Speicher- und Abrufkosten zu optimieren. Normalerweise haben Kunden Protokolle zwischen drei Monaten bis einem Jahr für Abfragen verfügbar, bei einer Gesamtaufbewahrungszeit von bis zu sieben Jahren. Die Wahl von Verfügbarkeit und Aufbewahrungszeit sollte sich nach Ihren Sicherheitsanforderungen und einer Kombination aus gesetzlichen, regulatorischen und unternehmensinternen Vorschriften richten.
- Verwenden Sie die Protokollierung für jeden AWS Service und jede Anwendung mit den richtigen Aufbewahrungs- und Lebenszyklusrichtlinien: Beachten Sie für jeden AWS Service oder jede Anwendung in Ihrem Unternehmen die spezifischen Anleitungen zur Konfiguration der Protokollierung:
  - [AWS CloudTrail Trail konfigurieren](#)
  - [VPCFlow-Logs konfigurieren](#)
  - [Amazon GuardDuty Finding Export konfigurieren](#)
  - [Konfigurieren Sie die AWS Config Aufnahme](#)
  - [Konfigurieren Sie den AWS WAF ACL Webverkehr](#)
  - [Konfigurieren Sie AWS Network Firewall Netzwerkverkehrsprotokolle](#)
  - [Konfigurieren der Zugriffsprotokolle von Elastic Load Balancing](#)
  - [Konfigurieren von Resolver-Abfrageprotokollen von Amazon Route 53](#)
  - [RDSAmazon-Logs konfigurieren](#)
  - [Amazon EKS Control Plane-Protokolle konfigurieren](#)
  - [Amazon CloudWatch Agent für EC2 Amazon-Instances und lokale Server konfigurieren](#)
- Wählen und implementieren Sie Abfragemechanismen für Protokolle: Für Protokollabfragen können Sie [CloudWatch Logs Insights](#) für in CloudWatch Protokollgruppen gespeicherte Daten und [Amazon Athena](#) und Amazon [OpenSearch Service für in Amazon](#) S3 gespeicherte Daten verwenden. Sie können auch Abfragetools von Drittanbietern verwenden, z. B. einen Dienst zur Verwaltung von Sicherheitsinformationen und Ereignissen (SIEM).

Bei der Auswahl eines Tools zur Protokollabfrage sollten Sie die Personen, die Prozesse und die Technologieaspekte Ihrer Sicherheitsoperationen berücksichtigen. Wählen Sie ein Tool, das betriebliche, geschäftliche und sicherheitsrelevante Aspekte berücksichtigt und langfristig sowohl zugänglich als auch wartbar ist. Denken Sie daran, dass Tools zur Protokollabfrage optimal funktionieren, wenn die Anzahl der zu durchsuchenden Protokolle im Rahmen der Limits des jeweiligen Tools liegt. Es ist nicht ungewöhnlich, aus Kostengründen oder aufgrund technischer Einschränkungen mehrere Abfragetools zu verwenden.

Sie könnten beispielsweise ein Drittanbieter-Tool für die Verwaltung von Sicherheitsinformationen und Ereignissen (SIEM) verwenden, um Abfragen für die Daten der letzten 90 Tage durchzuführen, aber Athena für Abfragen verwenden, die länger als 90 Tage dauern, da die Protokollaufnahme von Athena kostet. SIEM Prüfen Sie unabhängig von der Implementierung, ob Ihr Konzept die Anzahl der für die Maximierung der operationalen Effizienz erforderlichen Tools minimiert, besonders für Untersuchungen von Sicherheitsvorfällen.

- Protokolle für Warnmeldungen verwenden: AWS bietet Warnmeldungen über verschiedene Sicherheitsdienste:
  - [AWS Config](#) überwacht und zeichnet Ihre AWS Ressourcenkonfigurationen auf und ermöglicht es Ihnen, die Bewertung und Korrektur der gewünschten Konfigurationen zu automatisieren.
  - [Amazon GuardDuty](#) ist ein Service zur Bedrohungserkennung, der kontinuierlich nach böswilligen Aktivitäten und unberechtigtem Verhalten sucht, um Sie AWS-Konten und Ihre Workloads zu schützen. GuardDuty erfasst, aggregiert und analysiert Informationen aus Quellen wie AWS CloudTrail Verwaltungs- und Datenereignissen, DNS Protokollen, VPC Flow Logs und Amazon EKS Audit-Logs. GuardDuty ruft unabhängige Datenströme direkt von VPC Flow Logs CloudTrail, DNS Abfrageprotokollen und Amazon EKS ab. Sie müssen keine Amazon S3-Bucket-Richtlinien verwalten oder die Art und Weise der Erfassung und Speicherung von Protokollen verändern. Es wird jedoch empfohlen, diese Protokolle für Ihre eigenen Untersuchungs- und Compliance-Zwecke aufzubewahren.
  - [AWS Security Hub](#) bietet einen zentralen Ort, an dem Ihre Sicherheitswarnungen oder Ergebnisse aus mehreren AWS Diensten und optionalen Produkten von Drittanbietern zusammengefasst, organisiert und priorisiert werden, sodass Sie einen umfassenden Überblick über Sicherheitswarnungen und den Compliance-Status erhalten.

Sie können auch benutzerdefinierte Alarm-Engines für Sicherheitsalarme verwenden, die von diesen Services nicht abgedeckt werden, bzw. für bestimmte Alarme, die für Ihre Umgebung relevante sind. Informationen zur Erstellung dieser Warnmeldungen und Erkennungen finden Sie unter [Detection im Security Incident Response Guide](#). AWS

## Ressourcen

### Zugehörige bewährte Methoden:

- [SEC04-BP02 Erfassen von Protokollen, Ergebnissen und Kennzahlen an standardisierten Orten](#)
- [SEC07-BP04 Definieren Sie skalierbares Datenlebenszyklusmanagement](#)
- [SEC10-BP06 Tools vor der Bereitstellung](#)

### Zugehörige Dokumente:

- [AWS Leitfaden zur Reaktion auf Sicherheitsvorfälle](#)
- [Erste Schritte mit Amazon Security Lake](#)
- [Erste Schritte: Amazon CloudWatch Logs](#)
- [Partnerlösungen im Bereich Sicherheit: Protokollierung und Überwachung](#)

### Zugehörige Videos:

- [AWS re:Invent 2022 — Wir stellen vor: Amazon Security Lake](#)

### Zugehörige Beispiele:

- [Assisted Log Enabler für AWS](#)
- [AWS Security Hub Ergebnisse: Historischer Export](#)

### Zugehörige Tools:

- [Snowflake for Cybersecurity](#)

## SEC04-BP02 Erfassen von Protokollen, Ergebnissen und Kennzahlen an standardisierten Orten

Sicherheitsteams stützen sich auf Protokolle und Erkenntnisse, um Ereignisse zu analysieren, die auf unbefugte Aktivitäten oder unbeabsichtigte Änderungen hindeuten könnten. Um diese Analyse zu rationalisieren, sollten Sie Sicherheitsprotokolle und Ergebnisse an standardisierten Orten erfassen.

Dies macht Datenpunkte von Interesse für die Korrelation verfügbar und kann die Integration von Tools vereinfachen.

Gewünschtes Ergebnis: Sie verfügen über einen standardisierten Ansatz zum Sammeln, Analysieren und Visualisieren von Protokolldaten, Erkenntnissen und Metriken. Sicherheitsteams können Sicherheitsdaten über verschiedene Systeme hinweg effizient korrelieren, analysieren und visualisieren, um potenzielle Sicherheitsereignisse zu erkennen und Anomalien zu identifizieren. Systeme zur Verwaltung von Sicherheitsinformationen und Ereignissen (SIEM) oder andere Mechanismen sind integriert, um Protokolldaten abzufragen und zu analysieren, um rechtzeitig auf Sicherheitsereignisse reagieren, sie verfolgen und eskalieren zu können.

Typische Anti-Muster:

- Teams besitzen und verwalten eigenständig Protokolle und Metriksammlungen, die nicht mit der Protokollierungsstrategie der Organisation übereinstimmen.
- Teams verfügen nicht über angemessene Zugriffskontrollen, um die Sichtbarkeit und Veränderung der erfassten Daten einzuschränken.
- Teams regeln ihre Sicherheitsprotokolle, Erkenntnisse und Metriken nicht als Teil ihrer Richtlinie zur Datenklassifizierung.
- Teams vernachlässigen bei der Konfiguration von Datensammlungen die Anforderungen an die Datenhoheit und die Lokalisierung.

Vorteile der Nutzung dieser bewährten Methode: Eine standardisierte Protokollierungslösung zur Erfassung und Abfrage von Protokolldaten und -ereignissen verbessert die aus den darin enthaltenen Informationen gewonnenen Erkenntnisse. Die Konfiguration eines automatisierten Lebenszyklus für die gesammelten Protokolldaten kann die durch die Speicherung von Protokollen entstehenden Kosten reduzieren. Sie können eine fein abgestufte Zugriffskontrolle für die gesammelten Protokollinformationen einrichten, je nachdem, wie sensibel die Daten sind und welche Zugriffsmuster Ihre Teams benötigen. Sie können Tools integrieren, um die Daten zu korrelieren, zu visualisieren und Erkenntnisse daraus abzuleiten.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel

Implementierungsleitfaden

Die zunehmende AWS Nutzung innerhalb eines Unternehmens führt zu einer wachsenden Anzahl verteilter Workloads und Umgebungen. Jeder dieser Workloads und jede dieser Umgebungen generiert Daten über die darin stattfindenden Aktivitäten. Die Erfassung und lokale Speicherung dieser Daten stellt eine Herausforderung für den Sicherheitsbetrieb dar. Sicherheitsteams verwenden Tools wie Sicherheitsinformations- und Event-Management-Systeme (SIEM), um Daten aus verteilten Quellen zu sammeln und Workflows für Korrelation, Analyse und Reaktion zu durchlaufen.

Dies erfordert die Verwaltung komplexer Berechtigungen für den Zugriff auf die verschiedenen Datenquellen und zusätzlichen Aufwand beim Betrieb der Extraktions-, Transformations- und Ladeprozesse (ETL).

Um diese Herausforderungen zu bewältigen, sollten Sie erwägen, alle relevanten Quellen von Sicherheitsprotokolldaten in einem Log [Archive-Konto](#) zusammenzufassen, wie unter [Organizing Your AWS Environment Using Multiple Accounts](#) beschrieben. Dazu gehören alle sicherheitsrelevanten Daten aus Ihrem Workload und Protokolle, die AWS -Services erzeugen, wie [AWS CloudTrail](#), [AWS WAF](#), [Elastic Load Balancing](#) und [Amazon Route 53](#). Die Erfassung dieser Daten an standardisierten Speicherorten an einem separaten Speicherort AWS-Konto mit entsprechenden kontoübergreifenden Berechtigungen bietet mehrere Vorteile. Diese Vorgehensweise hilft, die Manipulation von Protokollen in gefährdeten Workloads und Umgebungen zu verhindern, bietet einen einzigen Integrationspunkt für zusätzliche Tools und bietet ein einfacheres Modell für die Konfiguration der Datenaufbewahrung und des Lebenszyklus. Bewerten Sie die Auswirkungen der Datenhoheit, der Compliance-Bereiche und anderer Vorschriften, um festzustellen, ob mehrere Speicherorte für Sicherheitsdaten und Aufbewahrungsfristen erforderlich sind.

Um die Erfassung und Standardisierung von Protokollen und Erkenntnissen zu erleichtern, bewerten Sie [Amazon Security Lake](#) in Ihrem Protokollarchiv-Konto. Sie können Security Lake so konfigurieren, dass Daten aus gängigen Quellen wie Route 53 CloudTrailEKS, [Amazon](#) und [VPCFlow Logs](#) automatisch aufgenommen werden. Sie können Security Lake auch AWS Security Hub als Datenquelle konfigurieren, sodass Sie Ergebnisse von anderen AWS Diensten wie [Amazon GuardDuty](#) und [Amazon Inspector](#) mit Ihren Protokolldaten korrelieren können. Ferner haben Sie die Möglichkeit, Datenquellen von Drittanbietern zu integrieren oder eigene Datenquellen zu konfigurieren. Alle Integrationen standardisieren Ihre Daten im Format [Open Cybersecurity Schema Framework](#) (OCSF) und werden in [Amazon S3 S3-Buckets](#) als Parquet-Dateien gespeichert, sodass keine Verarbeitung erforderlich ist. ETL

Das Speichern von Sicherheitsdaten an standardisierten Speicherorten bietet erweiterte Analysefunktionen. AWS empfiehlt, dass Sie Tools für Sicherheitsanalysen, die in einer AWS Umgebung funktionieren, in einem [Security Tooling-Konto](#) bereitstellen, das von Ihrem Log Archive-Konto getrennt ist. Dieser Ansatz ermöglicht es Ihnen, Kontrollen in der Tiefe zu implementieren, um die Integrität und Verfügbarkeit der Protokolle und des Protokollverwaltungsprozesses zu schützen, und zwar unabhängig von den Tools, die auf sie zugreifen. Erwägen Sie die Nutzung von Services wie [Amazon Athena](#), um On-Demand-Abfragen durchzuführen, die mehrere Datenquellen miteinander in Beziehung setzen. Sie können auch Visualisierungstools wie [Amazon](#) integrieren QuickSight. KI-gestützte Lösungen werden zunehmend verfügbar und können Funktionen wie die Übersetzung von Erkenntnissen in für Menschen lesbare Zusammenfassungen und Interaktion in

natürlicher Sprache übernehmen. Diese Lösungen lassen sich oft leichter integrieren, wenn ein standardisierter Datenspeicher für Abfragen zur Verfügung steht.

## Implementierungsschritte

1. Erstellen Sie die Konten „Protokollarchiv“ und „Security Tooling“
  - a. [Erstellen Sie mithilfe von AWS Organizations Log Archive und Security Tooling Konten](#) unter einer Sicherheits-Organisationseinheit. Wenn Sie Ihre Organisation verwalten AWS Control Tower , werden die Konten Log Archive und Security Tooling automatisch für Sie erstellt. Konfigurieren Sie bei Bedarf Rollen und Berechtigungen für den Zugriff auf diese Konten und deren Verwaltung.
2. Konfigurieren Sie Ihre standardisierten Speicherorte für Sicherheitsdaten
  - a. Legen Sie Ihre Strategie für die Erstellung standardisierter Sicherheitsdatenorte fest. Sie können dies durch Optionen wie gängige Data-Lake-Architekturansätze, Datenprodukte von Drittanbietern oder [Amazon Security Lake](#) erreichen. AWS empfiehlt, dass Sie Sicherheitsdaten von den Konten erfassen AWS-Regionen , für die [Sie sich angemeldet](#) haben, auch wenn diese nicht aktiv genutzt werden.
3. Konfigurieren Sie die Veröffentlichung von Datenquellen an Ihren standardisierten Standorten
  - a. Identifizieren Sie die Quellen für Ihre Sicherheitsdaten und konfigurieren Sie sie so, dass sie an Ihren standardisierten Speicherorten veröffentlicht werden. Prüfen Sie die Optionen für den automatischen Export von Daten im gewünschten Format, im Gegensatz zu denen, bei denen ETL Prozesse entwickelt werden müssen. Mit Amazon Security Lake können Sie [Daten aus unterstützten AWS Quellen und integrierten Systemen von Drittanbietern sammeln](#).
4. Konfigurieren Sie Tools für den Zugriff auf Ihre standardisierten Speicherorte
  - a. Konfigurieren Sie Tools wie Amazon Athena, Amazon oder Lösungen von Drittanbietern QuickSight, um den erforderlichen Zugriff auf Ihre standardisierten Standorte zu erhalten. Konfigurieren Sie diese Tools so, dass sie über das Security Tooling-Konto mit kontoübergreifendem Zugriff auf das Protokollarchiv-Konto arbeiten, sofern zutreffend. [Erstellen Sie Subscriber in Amazon Security Lake](#), um diesen Tools Zugriff auf Ihre Daten zu erteilen.

## Ressourcen

Zugehörige bewährte Methoden:

- [SEC01-BP01 Separate Workloads mithilfe von Konten](#)
- [SEC07-BP04 Definieren Sie das Datenlebenszyklusmanagement](#)



- [SEC08-BP04 Erzwingen Sie die Zugriffskontrolle](#)
- [OPS08-BP02 Analysieren Sie Workload-Protokolle](#)

#### Zugehörige Dokumente:

- [AWS Whitepapers: Organisieren Sie Ihre Umgebung mithilfe mehrerer Konten AWS](#)
- [AWS Präskriptive Leitlinien: AWS Sicherheitsreferenzarchitektur \(\)AWS SRA](#)
- [AWS Prescriptive Guidance: Logging and monitoring guide for application owners](#)

#### Zugehörige Beispiele:

- [Aggregieren, Durchsuchen und Visualisieren von Protokolldaten aus verteilten Quellen mit Amazon Athena und Amazon QuickSight](#)
- [So visualisieren Sie die Ergebnisse von Amazon Security Lake mit Amazon QuickSight](#)
- [Generieren Sie mithilfe von Amazon SageMaker Studio und Amazon Bedrock KI-gestützte Erkenntnisse für Amazon Security Lake](#)
- [Identifizieren Sie mithilfe von Amazon Cybersicherheitsanomalien in Ihren Amazon Security Lake-Daten SageMaker](#)
- [Erfassung, Transformation und Bereitstellung von Ereignissen, die von Amazon Security Lake veröffentlicht wurden, an Amazon Service OpenSearch](#)
- [Wie benutzt man AWS Security Hub einen Amazon OpenSearch Service für SIEM](#)

#### Zugehörige Tools:

- [Amazon Security Lake](#)
- [Amazon Security Lake-Partnerintegrationen](#)
- [Öffnen Sie das Cybersecurity Schema Framework \(OCSF\)](#)
- [Amazon Athena](#)
- [Amazon QuickSight](#)
- [Amazon Bedrock](#)

## SEC04-BP03 Korrelieren und bereichern Sie Sicherheitswarnungen

Unerwartete Aktivitäten können mehrere Sicherheitswarnmeldungen aus verschiedenen Quellen auslösen, die eine weitere Korrelation und Anreicherung erfordern, um den gesamten Kontext zu verstehen. Implementieren Sie die automatische Korrelation und Anreicherung von Sicherheitswarnmeldungen, um eine genauere Identifizierung von Vorfällen und eine bessere Reaktion darauf zu ermöglichen.

Gewünschtes Ergebnis: Da die Aktivitäten in Ihren Workloads und Umgebungen unterschiedliche Warnmeldungen erzeugen, korrelieren automatische Mechanismen die Daten und bereichern sie mit zusätzlichen Informationen an. Diese Vorverarbeitung ermöglicht ein detaillierteres Verständnis des Ereignisses, was Ihren Ermittlern hilft, die Kritikalität des Ereignisses zu bestimmen und festzustellen, ob es sich um einen Vorfall handelt, der eine formelle Reaktion erfordert. Dieses Verfahren entlastet Ihre Überwachungs- und Untersuchungsteams.

Typische Anti-Muster:

- Verschiedene Personengruppen untersuchen Erkenntnisse und Warnmeldungen, die von verschiedenen Systemen generiert werden, sofern nicht durch Anforderungen der Aufgabentrennung etwas anderes vorgeschrieben ist.
- Ihre Organisation leitet alle Sicherheitserkenntnisse und -warnmeldungen an Standardspeicherorte weiter, verlangt aber von den Ermittlern, dass sie diese manuell korrelieren und anreichern.
- Sie verlassen sich ausschließlich auf die Intelligenz von Bedrohungserkennungssystemen, um über Erkenntnisse zu berichten und die Kritikalität zu bestimmen.

Vorteile der Nutzung dieser bewährten Methode: Die automatische Korrelation und Anreicherung von Warnmeldungen trägt dazu bei, die gesamte kognitive Belastung und die manuelle Datenaufbereitung zu reduzieren, die Ihre Ermittler benötigen. Diese Methode kann die Zeit verkürzen, die benötigt wird, um festzustellen, ob es sich bei dem Ereignis um einen Vorfall handelt, und eine formelle Reaktion einzuleiten. Zusätzlicher Kontext hilft Ihnen auch, den wahren Schweregrad eines Ereignisses genau zu bewerten, da er höher oder niedriger sein kann, als eine einzelne Warnmeldung vermuten lässt.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Niedrig

Implementierungsleitfaden

Sicherheitswarnungen können aus vielen verschiedenen Quellen stammen, darunter: AWS

- Dienste wie [Amazon GuardDuty](#), [Amazon Macie](#), [AWS Security Hub](#), [Amazon Inspector](#), [AWS Config](#), [AWS Identity and Access Management Access Analyzer](#), und [Network Access Analyzer](#)
- Warnmeldungen aus automatisierten Analysen von AWS Service-, Infrastruktur- und Anwendungsprotokollen, z. B. von [Security Analytics for Amazon OpenSearch Service](#).
- Alarmer als Reaktion auf Änderungen Ihrer Abrechnungsaktivitäten aus Quellen wie [Amazon CloudWatch](#) EventBridge, [Amazon](#) oder [AWS Budgets](#).
- Quellen von Drittanbietern wie Threat Intelligence Feeds und [Security Partner Solutions](#) von AWS Partner Network
- [Kontakt durch AWS Trust & Safety](#) oder andere Quellen wie Kunden oder interne Mitarbeiter.

In ihrer grundlegendsten Form enthalten Warnmeldungen Informationen darüber, wer (Prinzipal oder Identität) was (die Aktion, die ergriffen wird) im Hinblick auf (Ressourcen, die betroffen sind) macht. Ermitteln Sie für jede dieser Quellen, ob es Möglichkeiten gibt, Zuordnungen zwischen den Identifikatoren für diese Identitäten, Aktionen und Ressourcen als Grundlage für die Durchführung von Korrelationen zu erstellen. Dabei kann es sich um die Integration von Warnquellen mit einem Tool zur Verwaltung von Sicherheitsinformationen und Ereignissen (SIEM) handeln, um eine automatische Korrelation für Sie durchzuführen, Ihre eigenen Daten-Pipelines und deren Verarbeitung zu erstellen oder eine Kombination aus beidem.

Ein Beispiel für einen Dienst, der eine Korrelation für Sie durchführen kann, ist [Amazon Detective](#). Detective erfasst fortlaufend Warnmeldungen aus verschiedenen Quellen und von Drittanbietern AWS und verwendet verschiedene Formen von Informationen, um ein visuelles Diagramm ihrer Beziehungen zu erstellen, um die Ermittlungen zu unterstützen.

Während die anfängliche Kritikalität eines Alarms eine Hilfe für die Priorisierung ist, bestimmt der Kontext, in dem der Alarm auftrat, seine wahre Kritikalität. Beispielsweise GuardDuty kann Amazon darauf hinweisen, dass eine EC2 Amazon-Instance innerhalb Ihres Workloads einen unerwarteten Domainnamen abfragt. GuardDuty könnte dieser Warnung von sich aus eine niedrige Priorität zuweisen. Durch die automatische Korrelation mit anderen Aktivitäten rund um den Zeitpunkt der Warnung könnte jedoch aufgedeckt werden, dass mehrere hundert EC2 Instances mit derselben Identität bereitgestellt wurden, was die Gesamtbetriebskosten in die Höhe treibt. In diesem Fall GuardDuty könnte dieser korrelierte Ereigniskontext als neue Sicherheitswarnung veröffentlicht und die Kritikalität auf hoch gesetzt werden, was weitere Maßnahmen beschleunigen würde.

## Implementierungsschritte

1. Identifizieren Sie Quellen für Informationen zu Sicherheitswarnmeldungen. Verstehen Sie, wie Warnmeldungen aus diesen Systemen Identität, Aktion und Ressourcen darstellen, um festzustellen, wo eine Korrelation möglich ist.
2. Richten Sie einen Mechanismus zur Erfassung von Warnmeldungen aus verschiedenen Quellen ein. Ziehen Sie Dienste wie Security Hub und EventBridge CloudWatch für diesen Zweck in Betracht.
3. Identifizieren Sie Quellen für die Korrelation und Anreicherung von Daten. Zu den Beispielquellen gehören CloudTrail VPC Flow Logs, Amazon Security Lake sowie Infrastruktur- und Anwendungsprotokolle.
4. Integrieren Sie Ihre Warnmeldungen mit Ihren Datenkorrelations- und -anreicherungsquellen, um detailliertere Kontexte für Sicherheitsereignisse zu erstellen und die Kritikalität zu ermitteln.
  - a. Amazon Detective, SIEM Tools oder andere Lösungen von Drittanbietern können ein gewisses Maß an Erfassung, Korrelation und Anreicherung automatisch durchführen.
  - b. Sie können AWS Dienste auch verwenden, um Ihre eigenen zu entwickeln. Sie können beispielsweise eine AWS Lambda Funktion aufrufen, um eine Amazon Athena Athena-Abfrage für AWS CloudTrail oder Amazon Security Lake auszuführen, und die Ergebnisse in veröffentlichen. EventBridge

## Ressourcen

### Zugehörige bewährte Methoden:

- [SEC10-BP03 Bereiten Sie forensische Funktionen vor](#)
- [OPS08-BP04 Erstellen Sie umsetzbare Warnmeldungen](#)
- [REL06-BP03 Benachrichtigungen senden \(Verarbeitung und Alarmierung in Echtzeit\)](#)

### Zugehörige Dokumente:

- [AWS Security Incident Response Guide](#)

### Zugehörige Beispiele:

- [Wie reichert man Ergebnisse mit Konto-Metadaten AWS Security Hub an](#)
- [Wie benutzt man AWS Security Hub einen Amazon OpenSearch Service für SIEM](#)

## Zugehörige Tools:

- [Amazon Detective](#)
- [Amazon EventBridge](#)
- [AWS Lambda](#)
- [Amazon Athena](#)

## SEC04-BP04 Behebung nicht richtlinienkonformer Ressourcen einleiten

Ihre detektivischen Kontrollen können Sie auf Ressourcen aufmerksam machen, die nicht mit Ihren Konfigurationsanforderungen übereinstimmen. Sie können programmatisch definierte Abhilfemaßnahmen einleiten, entweder manuell oder automatisch, um diese Ressourcen zu korrigieren und mögliche Auswirkungen zu minimieren. Wenn Sie Abhilfemaßnahmen programmatisch definieren, können Sie sofort und konsequent handeln.

Automatisierung kann zwar den Sicherheitsbetrieb verbessern, aber Sie sollten die Automatisierung sorgfältig implementieren und verwalten. Schaffen Sie geeignete Überwachungs- und Kontrollmechanismen, um zu überprüfen, ob die automatisierten Antworten effektiv und genau sind und mit den Organisationsrichtlinien und der Risikobereitschaft übereinstimmen.

Gewünschtes Ergebnis: Sie definieren Standards für die Ressourcenkonfiguration und die Schritte zur Behebung, wenn festgestellt wird, dass die Ressourcen nicht konform sind. Wo immer möglich, haben Sie Abhilfemaßnahmen programmatisch definiert, sodass sie entweder manuell oder durch Automatisierung eingeleitet werden können. Es gibt Erkennungssysteme, die nicht konforme Ressourcen identifizieren und Warnungen in zentralisierten Tools veröffentlichen, die von Ihrem Sicherheitspersonal überwacht werden. Diese Tools unterstützen die Durchführung Ihrer programmatischen Korrekturen, entweder manuell oder automatisch. Automatische Abhilfemaßnahmen verfügen über angemessene Überwachungs- und Kontrollmechanismen, um ihre Verwendung zu steuern.

## Typische Anti-Muster:

- Sie implementieren Automatisierung, versäumen es aber, Abhilfemaßnahmen gründlich zu testen und zu validieren. Dies kann unbeabsichtigte Folgen haben, wie z. B. die Unterbrechung legitimer Geschäftsabläufe oder die Instabilität des Systems.
- Sie verbessern die Reaktionszeiten und Verfahren durch Automatisierung, aber ohne angemessene Überwachung und Mechanismen, die bei Bedarf menschliches Eingreifen und Urteilsvermögen ermöglichen.

- Sie verlassen sich ausschließlich auf Abhilfemaßnahmen, anstatt Abhilfemaßnahmen als Teil eines umfassenderen Programms zur Reaktion auf Vorfälle und zur Wiederherstellung zu nutzen.

Vorteile der Nutzung dieser bewährten Methode: Automatische Abhilfemaßnahmen können schneller auf Fehlkonfigurationen reagieren als manuelle Prozesse. So können Sie potenzielle Auswirkungen auf Ihr Unternehmen minimieren und das Zeitfenster für unbeabsichtigte Nutzungen verringern. Wenn Sie Abhilfemaßnahmen programmatisch definieren, werden sie konsistent angewendet, was das Risiko menschlicher Fehler verringert. Die Automatisierung kann auch eine größere Anzahl von Alarmen gleichzeitig verarbeiten, was besonders in Umgebungen von großem Maßstab wichtig ist.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel

### Implementierungsleitfaden

Wie unter [SEC01-BP03 Kontrollziele identifizieren und validieren](#) beschrieben, können Services wie [AWS Config](#) Ihnen dabei helfen, die Konfiguration der Ressourcen in Ihren Konten auf die Einhaltung Ihrer Anforderungen hin zu überwachen. Wenn nicht konforme Ressourcen erkannt werden, empfehlen wir, das Senden von Warnmeldungen an eine Cloud-Lösung zur Verwaltung der Sicherheitslage (CSPM) zu konfigurieren, z. B. [AWS Security Hub](#) bei der Behebung zu helfen. Diese Lösungen bieten einen zentralen Ort für Ihre Sicherheitsbeauftragten, um Probleme zu überwachen und Korrekturmaßnahmen zu ergreifen.

Einige Situationen, in denen Ressourcen nicht konform sind, können zwar einzigartig sein und erfordern menschliches Urteilsvermögen, um Abhilfe zu schaffen. Für andere Fälle gibt es jedoch eine Standardreaktion, die Sie programmatisch definieren können. Eine Standardantwort auf eine falsch konfigurierte VPC Sicherheitsgruppe könnte beispielsweise darin bestehen, die unzulässigen Regeln zu entfernen und den Besitzer zu benachrichtigen. Antworten können in [AWS Lambda](#)-Funktionen, in [AWS -Systems-Manager-Automation](#)-Dokumenten oder durch andere von Ihnen bevorzugte Code-Umgebungen definiert werden. Stellen Sie sicher, dass die Umgebung in der Lage ist, sich für die AWS Verwendung einer IAM Rolle mit den geringsten Rechten zu authentifizieren, die zum Ergreifen von Korrekturmaßnahmen erforderlich ist.

Sobald Sie die gewünschte Problembhebung definiert haben, können Sie festlegen, wie Sie sie am liebsten einleiten möchten. AWS Config kann [Abhilfemaßnahmen für Sie einleiten](#). Wenn Sie Security Hub verwenden, können Sie dies über [benutzerdefinierte Aktionen](#) tun, wodurch die Ergebnisinformationen an [Amazon](#) veröffentlicht EventBridge werden. Eine EventBridge Regel kann dann Ihre Problembhebung einleiten. Sie können die benutzerdefinierte Aktion in Security Hub so konfigurieren, dass sie entweder automatisch oder manuell ausgeführt wird.

Für programmatische Abhilfemaßnahmen empfehlen wir Ihnen, umfassende Protokolle und Audits für die durchgeführten Maßnahmen sowie deren Ergebnisse zu führen. Prüfen und analysieren Sie diese Protokolle, um die Effektivität der automatisierten Prozesse zu bewerten und Verbesserungsmöglichkeiten zu identifizieren. Erfassen Sie Protokolle in [Amazon CloudWatch Logs](#) und die Ergebnisse der Problembeseitigung als [Suchnotizen](#) im Security Hub.

Als Ausgangspunkt sollten Sie [Automated Security Response on](#) in Betracht ziehen AWS, das vorgefertigte Abhilfemaßnahmen zur Behebung häufiger Sicherheitsfehlfunktionen enthält.

## Implementierungsschritte

1. Analysieren und priorisieren Sie Warnmeldungen.
  - a. Konsolidieren Sie Sicherheitswarnungen aus verschiedenen AWS Diensten in Security Hub für zentrale Transparenz, Priorisierung und Problembeseitigung.
2. Entwickeln Sie Abhilfemaßnahmen.
  - a. Verwenden Sie Dienste wie Systems Manager und AWS Lambda führen Sie programmatische Problembeseitigungen durch.
3. Konfigurieren Sie, wie Abhilfemaßnahmen eingeleitet werden.
  - a. Definieren Sie mithilfe von Systems Manager benutzerdefinierte Aktionen, mit denen Ergebnisse veröffentlicht werden EventBridge. Konfigurieren Sie diese Aktionen so, dass sie manuell oder automatisch ausgelöst werden.
  - b. Sie können [Amazon Simple Notification Service \(SNS\)](#) auch verwenden, um Benachrichtigungen und Warnmeldungen an relevante Beteiligte (wie Sicherheitsteam oder Incident-Response-Teams) zu senden, damit diese bei Bedarf manuell eingreifen oder eskalieren können.
4. Prüfen und analysieren Sie die Protokolle der Abhilfemaßnahmen auf Wirksamkeit und Verbesserung.
  - a. Sendet die Protokollausgabe an CloudWatch Logs. Erfassen Sie die Ergebnisse als Erkenntnisse in Security Hub.

## Ressourcen

Zugehörige bewährte Methoden:

- [SEC06-BP03 Reduzieren Sie die manuelle Verwaltung und den interaktiven Zugriff](#)

## Zugehörige Dokumente:

- [AWS Security Incident Response Guide - Detection](#)

## Zugehörige Beispiele:

- [Automatisierte Sicherheitsreaktion auf AWS](#)
- [Überwachen Sie EC2 Instanz-Schlüsselpaare mit AWS Config](#)
- [Create AWS Config custom rules by using AWS CloudFormation Guard policies](#)
- [Automatisches Korrigieren unverschlüsselter Amazon RDS DB-Instances und -Cluster](#)

## Zugehörige Tools:

- [AWS Systems Manager Automatisierung](#)
- [Automatisierte Sicherheitsreaktion auf AWS](#)

# Schutz der Infrastruktur

## Fragen

- [SEC5. Wie werden Ihre Netzwerkressourcen geschützt?](#)
- [SEC6. Wie werden Ihre Rechenressourcen geschützt?](#)

## SEC5. Wie werden Ihre Netzwerkressourcen geschützt?

Alle Workloads, die über eine Art Netzwerkverbindung verfügen, unabhängig davon, ob es sich um das Internet oder ein privates Netzwerk handelt, erfordern mehrere Abwehrebene, um Schutz vor externen und internen Netzwerkbedrohungen sicherzustellen.

## Bewährte Methoden

- [SEC05-BP01 Netzwerkschichten erstellen](#)
- [SEC05-BP02 Steuern Sie den Verkehrsfluss innerhalb Ihrer Netzwerkschichten](#)
- [SEC05-BP03 Implementieren Sie einen inspektionsbasierten Schutz](#)
- [SEC05-BP04 Automatisieren Sie den Netzwerkschutz](#)



## SEC05-BP01 Netzwerkschichten erstellen

Segmentieren Sie Ihre Netzwerktopologie in verschiedene Ebenen, die auf logischen Gruppierungen Ihrer Workload-Komponenten entsprechend ihrer Datensensibilität und Zugriffsanforderungen basieren. Unterscheiden Sie zwischen Komponenten, auf die vom Internet aus zugegriffen werden muss, wie z. B. öffentliche Web-Endpunkte, und solchen, die nur intern erreichbar sein müssen, wie z. B. Datenbanken.

Gewünschtes Ergebnis: Die Schichten Ihres Netzwerks sind Teil eines ganzheitlichen defense-in-depth Sicherheitsansatzes, der die Identitätsauthentifizierungs- und Autorisierungsstrategie Ihrer Workloads ergänzt. Je nach Sensibilität der Daten und den Zugriffsanforderungen werden Ebenen mit entsprechenden Verkehrsfluss- und Kontrollmechanismen eingerichtet.

Typische Anti-Muster:

- Sie erstellen alle Ressourcen in einem einzigen VPC oder Subnetz.
- Sie erstellen Ihre Netzwerkebenen ohne Rücksicht auf die Anforderungen an die Datensensibilität, das Verhalten der Komponenten oder die Funktionalität.
- Sie verwenden VPCs Subnetze als Standardwerte für alle Überlegungen zur Netzwerkschicht, und Sie berücksichtigen nicht, wie AWS verwaltete Dienste Ihre Topologie beeinflussen.

Vorteile der Nutzung dieser bewährten Methode: Die Einrichtung von Netzwerkebenen ist der erste Schritt, um unnötige Pfade durch das Netzwerk einzuschränken, insbesondere solche, die zu kritischen Systemen und Daten führen. Dadurch wird es für Unbefugte schwieriger, sich Zugriff auf Ihr Netzwerk zu verschaffen und zu weiteren Ressourcen darin zu navigieren. Diskrete Netzwerkebenen reduzieren den Umfang der Analyse für Inspektionssysteme, z. B. für die Erkennung von Eindringlingen oder die Verhinderung von Malware, vorteilhaft. Dadurch wird das Potenzial für Fehlalarme und unnötigen Verarbeitungsaufwand reduziert.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Hoch

### Implementierungsleitfaden

Beim Entwurf einer Workload-Architektur ist es üblich, die Komponenten je nach ihrer Verantwortlichkeit in verschiedene Ebenen aufzuteilen. Eine Webanwendung kann zum Beispiel eine Präsentationsebene, eine Anwendungsebene und eine Datenebene haben. Bei der Gestaltung Ihrer Netzwerktopologie können Sie einen ähnlichen Ansatz wählen. Die zugrunde liegenden Netzwerkkontrollen können dazu beitragen, die Anforderungen Ihres Workloads an den Datenzugriff

durchzusetzen. In einer dreistufigen Webanwendungsarchitektur können Sie beispielsweise Ihre statischen Presentation-Layer-Dateien auf [Amazon S3](#) speichern und sie über ein Content Delivery Network (CDN) wie [Amazon CloudFront](#) bereitstellen. Die Anwendungsschicht kann über öffentliche Endpunkte verfügen, die ein [Application Load Balancer \(ALB\)](#) in einem VPC öffentlichen [Amazon-Subnetz](#) (ähnlich einer demilitarisierten Zone oder DMZ) bedient, wobei Back-End-Dienste in privaten Subnetzen bereitgestellt werden. Die Datenebene, die Ressourcen wie Datenbanken und gemeinsam genutzte Dateisysteme hostet, kann sich in anderen privaten Subnetzen befinden als die Ressourcen Ihrer Anwendungsebene. An jeder dieser Ebenengrenzen (öffentliches Subnetz/CDN, privates Subnetz) können Sie Kontrollen einrichten, die es nur autorisierten Datenverkehr ermöglichen, diese Grenzen zu überschreiten.

Ähnlich wie bei der Modellierung von Netzwerkebenen auf der Grundlage des funktionalen Zwecks der Komponenten Ihres Workloads sollten Sie auch die Sensibilität der verarbeiteten Daten berücksichtigen. Wenn Sie das Beispiel der Webanwendung verwenden, kann es sein, dass alle Ihre Workload-Services innerhalb der Anwendungsebene angesiedelt sind, während verschiedene Services Daten mit unterschiedlichen Sensibilitätsstufen verarbeiten. In diesem Fall kann es je nach Ihren Kontrollanforderungen angemessen sein, die Anwendungsebene mithilfe mehrerer privater Subnetze zu unterteilen. AWS-Konto, die sich VPCs in demselben oder sogar in unterschiedlicher Weise AWS-Konten für jede Ebene der Datensensitivität unterscheiden. VPCs

Eine weitere Überlegung für Netzwerkebenen ist die Verhaltenskonsistenz der Komponenten Ihres Workloads. Um das Beispiel fortzusetzen: In der Anwendungsebene haben Sie möglicherweise Services, die Eingaben von Endbenutzern oder externen Systemintegrationen akzeptieren, die von Natur aus risikoreicher sind als die Eingaben für andere Services. Beispiele sind das Hochladen von Dateien, das Ausführen von Skripten, das Scannen von E-Mails und so weiter. Die Unterbringung dieser Services in einer eigenen Netzwerkebene hilft dabei, eine stärkere Isolationsgrenze um sie herum zu schaffen, und kann verhindern, dass ihr einzigartiges Verhalten falsche positive Alarme in Inspektionssystemen erzeugt.

Berücksichtigen Sie im Rahmen Ihres Entwurfs, wie sich die Verwendung von AWS Managed Services auf Ihre Netzwerktopologie auswirkt. Erfahren Sie, wie Services wie [Amazon VPC Lattice](#) dazu beitragen können, die Interoperabilität Ihrer Workload-Komponenten über Netzwerkschichten hinweg zu vereinfachen. Verwenden Sie die Lösung in Ihren VPC Subnetzen [AWS Lambda](#), es sei denn, es gibt bestimmte Gründe, dies nicht zu tun. Ermitteln Sie, wo sich VPC Endpunkte befinden, und [AWS PrivateLink](#) können Sie die Einhaltung von Sicherheitsrichtlinien, die den Zugriff auf Internet-Gateways einschränken, vereinfachen.

## Implementierungsschritte

1. Überprüfen Sie Ihre Workload-Architektur. Gruppieren Sie Komponenten und Services logisch nach den Funktionen, die sie erfüllen, nach der Sensibilität der verarbeiteten Daten und nach ihrem Verhalten.
2. Für Komponenten, die auf Anfragen aus dem Internet reagieren, sollten Sie Load Balancer oder andere Proxys verwenden, um öffentliche Endpunkte bereitzustellen. Erkunden Sie die sich ändernden Sicherheitskontrollen, indem Sie Managed Services wie CloudFront [Amazon API Gateway](#) und Elastic Load Balancing nutzen und [AWS Amplify](#) öffentliche Endgeräte hosten.
3. Für Komponenten, die in Rechenumgebungen ausgeführt werden, wie EC2 Amazon-Instances, [AWS Fargate](#) Container oder Lambda-Funktionen, stellen Sie diese vom ersten Schritt an in privaten Subnetzen bereit, die auf Ihren Gruppen basieren.
4. Für vollständig verwaltete AWS Dienste wie [Amazon DynamoDB](#), [Amazon Kinesis](#) oder [Amazon SQS](#) sollten Sie die Verwendung von VPC Endpunkten als Standard für den Zugriff über private IP-Adressen in Betracht ziehen.

## Ressourcen

Zugehörige bewährte Methoden:

- [REL02 Planen Sie Ihre Netzwerktopologie](#)
- [PERF04-BP01 Verstehen Sie, wie sich Netzwerke auf die Leistung auswirken](#)

Zugehörige Videos:

- [AWS re:Invent 2023 — Grundlagen der Netzwerktechnik AWS](#)

Zugehörige Beispiele:

- [VPCBeispiele](#)
- [Greifen Sie mit AWS Fargate, AWS PrivateLink und einem Network Load Balancer privat auf Container-Anwendungen auf Amazon ECS zu](#)
- [Statische Inhalte in einem Amazon S3 S3-Bucket mithilfe VPC von Amazon bereitstellen CloudFront](#)

## SEC05-BP02 Steuern Sie den Verkehrsfluss innerhalb Ihrer Netzwerkschichten

Verwenden Sie innerhalb der einzelnen Ebenen Ihres Netzwerks eine weitere Segmentierung, um den Datenverkehr auf die für die einzelnen Workloads erforderlichen Flüsse zu beschränken. Konzentrieren Sie sich zunächst auf die Kontrolle des Datenverkehrs zwischen dem Internet oder anderen externen Systemen eines Workloads und Ihrer Umgebung (Nord-Süd-Verkehr). Betrachten Sie anschließend die Ströme zwischen verschiedenen Komponenten und Systemen (Ost-West-Verkehr).

Gewünschtes Ergebnis: Sie lassen nur die Netzwerkflüsse zu, die für die Kommunikation der Komponenten Ihrer Workloads untereinander, mit ihren Clients und mit allen anderen Services, von denen sie abhängig sind, erforderlich sind. Ihr Design berücksichtigt Überlegungen wie öffentlichen im Vergleich zu privatem Ingress und Egress, Datenklassifizierung, regionale Vorschriften und Protokollanforderungen. Wo immer möglich, bevorzugen Sie point-to-point Datenflüsse gegenüber Netzwerk-Peering als Teil des Prinzips der geringsten Rechte.

Typische Anti-Muster:

- Sie verfolgen bei der Netzwerksicherheit einen Perimeter-basierten Ansatz und kontrollieren den Datenverkehr nur an den Grenzen Ihrer Netzwerkebenen.
- Sie gehen davon aus, dass der gesamte Verkehr innerhalb einer Netzwerkebene authentifiziert und autorisiert ist.
- Sie kontrollieren entweder den eingehenden oder den ausgehenden Datenverkehr, aber nicht beide.
- Sie verlassen sich bei der Authentifizierung und Autorisierung des Datenverkehrs ausschließlich auf Ihre Workload-Komponenten und Netzwerkkontrollen.

Vorteile der Nutzung dieser bewährten Methode: Diese Vorgehensweise trägt dazu bei, das Risiko unbefugter Bewegungen innerhalb Ihres Netzwerks zu verringern, und fügt Ihren Workloads eine zusätzliche Autorisierungsebene hinzu. Durch die Kontrolle des Datenverkehrs können Sie den Umfang der Auswirkungen eines Sicherheitsvorfalls begrenzen und die Erkennung und Reaktion beschleunigen.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Hoch

Implementierungsleitfaden

Netzwerkschichten helfen zwar dabei, die Grenzen zwischen Komponenten Ihres Workloads festzulegen, die eine ähnliche Funktion, Datensensitivität und ähnliches Verhalten erfüllen, aber Sie

können eine viel detailliertere Ebene der Datenverkehrskontrolle erreichen, indem Sie Techniken verwenden, um Komponenten innerhalb dieser Schichten weiter zu segmentieren, die dem Prinzip der geringsten Rechte folgen. Innerhalb AWS werden Netzwerkschichten hauptsächlich mithilfe von Subnetzen gemäß IP-Adressbereichen innerhalb eines Amazon VPC definiert. Ebenen können auch anhand verschiedener Methoden definiert werden VPCs, z. B. zur Gruppierung von Microservice-Umgebungen nach Geschäftsdomänen. Wenn Sie mehrere verwenden VPCs, vermitteln Sie das Routing mit einem [AWS Transit Gateway](#). Dies ermöglicht zwar die Steuerung des Datenverkehrs auf Layer-4-Ebene (IP-Adressen und Portbereiche) mithilfe von Sicherheitsgruppen und Routing-Tabellen, Sie können jedoch mithilfe zusätzlicher Services [AWS PrivateLink](#), wie [Amazon Route 53 Resolver DNS Firewall](#), und [AWS Network Firewall AWS WAF](#), weitere Kontrolle erlangen.

Machen Sie sich mit den Datenfluss- und Kommunikationsanforderungen Ihrer Workloads in Bezug auf verbindungsinitiierende Parteien, Ports, Protokolle und Netzwerkschichten vertraut und inventarisieren Sie diese. Prüfen Sie die Protokolle, die für den Verbindungsaufbau und die Übertragung von Daten zur Verfügung stehen, und wählen Sie diejenigen aus, die Ihren Schutzanforderungen entsprechen (z. B. HTTPS nicht). Erfassen Sie diese Anforderungen sowohl an den Grenzen Ihrer Netzwerke als auch innerhalb jeder Ebene. Sobald diese Anforderungen identifiziert sind, prüfen Sie die Möglichkeiten, um nur den erforderlichen Datenverkehr an jedem Verbindungspunkt zuzulassen. Ein guter Ausgangspunkt ist die Verwendung von Sicherheitsgruppen innerhalb Ihrer VPC, da sie an Ressourcen angehängt werden können, die ein Elastic Network Interface (ENI) verwenden, wie EC2 Amazon-Instances, ECS Amazon-Aufgaben, EKS Amazon-Pods oder RDS Amazon-Datenbanken. Im Gegensatz zu einer Layer-4-Firewall kann eine Sicherheitsgruppe eine Regel haben, die den Datenverkehr einer anderen Sicherheitsgruppe anhand ihrer Kennung zulässt, wodurch Aktualisierungen minimiert werden, wenn sich die Ressourcen innerhalb der Gruppe im Laufe der Zeit ändern. Sie können den Datenverkehr auch mithilfe von Sicherheitsgruppen nach eingehenden und ausgehenden Regeln filtern.

Wenn sich der Verkehr zwischen VPCs bewegt, ist es üblich, VPC Peering für einfaches Routing oder AWS Transit Gateway für komplexes Routing zu verwenden. Mit diesen Ansätzen erleichtern Sie den Datenverkehrsfluss zwischen dem Bereich der IP-Adressen des Quell- und des Zielnetzwerks. Wenn Ihre Arbeitslast jedoch nur Datenflüsse zwischen bestimmten Komponenten in verschiedenen Bereichen erfordert VPCs, sollten Sie die Verwendung einer point-to-point Verbindung mit in Betracht ziehen. [AWS PrivateLink](#) Bestimmen Sie dazu, welcher Service als Produzent und welcher als Verbraucher fungieren soll. Stellen Sie einen kompatiblen Load Balancer für den Producer bereit, schalten Sie PrivateLink ihn entsprechend ein und akzeptieren Sie dann eine Verbindungsanfrage des Verbrauchers. Dem Producer-Dienst wird dann eine private IP-Adresse des Verbrauchers zugewiesen VPC, die der Verbraucher für nachfolgende Anfragen verwenden kann.

Dieser Ansatz reduziert die Notwendigkeit, die Netzwerke zu peeren. Beziehen Sie die Kosten für Datenverarbeitung und Lastenausgleich in die Bewertung mit ein PrivateLink.

Sicherheitsgruppen PrivateLink helfen zwar dabei, den Fluss zwischen den Komponenten Ihrer Workloads zu kontrollieren, aber ein weiterer wichtiger Aspekt ist, wie Sie kontrollieren können, auf welche DNS Domänen Ihre Ressourcen zugreifen dürfen (falls vorhanden). Je nach DHCP Konfiguration Ihres VPCs können Sie zu diesem Zweck zwei verschiedene AWS Dienste in Betracht ziehen. Die meisten Kunden verwenden den standardmäßigen Route 53 DNS Resolver-Service (auch DNS Amazon-Server oder genannt AmazonProvidedDNS), der VPCs unter der +2-Adresse seines CIDR Bereichs verfügbar ist. Mit diesem Ansatz können Sie DNS Firewall-Regeln erstellen und diese Ihren Regeln zuordnen VPC, die festlegen, welche Aktionen für die von Ihnen bereitgestellten Domainlisten zu ergreifen sind.

Wenn Sie nicht den Route 53-Resolver verwenden, oder wenn Sie den Resolver mit tieferen Prüf- und Flusskontrollfunktionen als der Domain-Filterung ergänzen wollen, sollten Sie die Bereitstellung eines AWS Network Firewall erwägen. Dieser Service prüft einzelne Pakete anhand von zustandslosen oder zustandsbehafteten Regeln, um zu entscheiden, ob der Datenverkehr verweigert oder zugelassen werden soll. Einen ähnlichen Ansatz können Sie für die Filterung des eingehenden Internetdatenverkehrs zu Ihren öffentlichen Endpunkten mit AWS WAF verfolgen. Weitere Hinweise zu diesen Diensten finden Sie unter [SEC05-BP03 Implementieren von inspektionsgestütztem Schutz](#).

### Implementierungsschritte

1. Identifizieren Sie die erforderlichen Datenflüsse zwischen den Komponenten Ihrer Workloads.
2. Wenden Sie mehrere Kontrollen mit einem defense-in-depth Ansatz für eingehenden und ausgehenden Datenverkehr an, einschließlich der Verwendung von Sicherheitsgruppen und Routing-Tabellen.
3. Verwenden Sie Firewalls, um eine differenzierte Kontrolle über den eingehenden, ausgehenden und zwischen Ihnen eingehenden Netzwerkverkehr zu definieren VPCs, z. B. die Route 53 Resolver DNS Firewall, und. AWS Network Firewall AWS WAF Erwägen Sie den Einsatz von [AWS Firewall Manager](#) für die zentrale Konfiguration und Verwaltung Ihrer Firewall-Regeln in Ihrer Organisation.

### Ressourcen

Zugehörige bewährte Methoden:

- [REL03-BP01 Wählen Sie aus, wie Sie Ihren Workload segmentieren möchten](#)

- [SEC09-BP02 Verschlüsselung bei der Übertragung erzwingen](#)

Zugehörige Dokumente:

- [Bewährte Sicherheitsmethoden für Ihr VPC](#)
- [AWS Network Optimization Tips](#)
- [Leitlinien zur Netzwerksicherheit am AWS](#)
- [Schützen Sie Ihren VPC ausgehenden Netzwerkverkehr im AWS Cloud](#)

Zugehörige Tools:

- [AWS Firewall Manager](#)

Zugehörige Videos:

- [AWS Transit Gateway Referenzarchitekturen für viele VPCs](#)
- [Anwendungsbeschleunigung und Schutz mit Amazon CloudFront AWS WAF, und AWS Shield](#)
- [AWS re:Inforce 2023: Firewalls and where to put them](#)

Zugehörige Beispiele:

- [Labor: CloudFront für Webanwendungen](#)

## SEC05-BP03 Implementieren Sie einen inspektionsbasierten Schutz

Richten Sie Kontrollpunkte für den Datenverkehr zwischen Ihren Netzwerkebenen ein, um sicherzustellen, dass die Daten während der Übertragung den erwarteten Kategorien und Mustern entsprechen. Analysieren Sie Datenverkehrsströme, Metadaten und Muster, um Ereignisse effektiver zu identifizieren, zu erkennen und darauf zu reagieren.

Gewünschtes Ergebnis: Der Datenverkehr, der zwischen Ihren Netzwerkebenen verläuft, wird geprüft und autorisiert. Entscheidungen über das Zulassen oder Verweigern von Zugriffen beruhen auf expliziten Regeln, Informationen über Bedrohungen und Abweichungen vom Grundverhalten. Der Schutz wird strenger, je näher der Datenverkehr an sensible Daten heranrückt.

Typische Anti-Muster:

- Ausschließlich auf Firewall-Regeln vertrauen, die auf Ports und Protokollen basieren, und Vorteile intelligenter Systeme außer Acht lassen
- Firewall-Regeln auf der Grundlage bestimmter aktueller Bedrohungsmuster erstellen, die sich ändern können
- Überprüfung des Datenverkehrs auf den Übergang von privaten zu öffentlichen Subnetzen oder von öffentlichen Subnetzen zum Internet beschränken
- Keine Basisansicht Ihres Netzwerkdatenverkehrs haben, die Sie auf Verhaltensanomalien hin überprüfen können

Vorteile der Nutzung dieser bewährten Methode: Prüfungssysteme ermöglichen es Ihnen, intelligente Regeln zu erstellen, z. B. den Datenverkehr nur dann zuzulassen oder zu verweigern, wenn bestimmte Bedingungen in den Datenverkehrsdaten vorliegen. Profitieren Sie von verwalteten Regelsätzen von AWS und Partnern, die auf den neuesten Bedrohungsinformationen basieren, da sich die Bedrohungslandschaft im Laufe der Zeit ändert. Dadurch verringert sich der Aufwand für die Pflege von Regeln und die Suche nach Indikatoren für eine Gefährdung, wodurch das Potenzial für Fehlalarme reduziert wird.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel

Implementierungsleitfaden

[Verschaffen Sie sich mithilfe anderer Firewalls und Intrusion Prevention-Systeme \(IPS\) AWS Network Firewall, die Sie hinter einem Gateway Load Balancer \(\) einsetzen können, eine genaue Kontrolle über Ihren AWS Marketplace statusbehafteten und statusfreien Netzwerkverkehr. GWLB AWS Network Firewall unterstützt \[Suricata-kompatible\]\(#\) Open-Source-Spezifikationen, um Ihre Workloads zu schützen. IPS](#)

AWS Network Firewall Sowohl die Lösungen als auch die von Anbietern, die A verwenden, GWLB unterstützen unterschiedliche Bereitstellungsmodelle für Inline-Inspektionen. Sie können beispielsweise Inspektionen auf VPC Einzelbasis durchführen, sie in Form einer zentralen Inspektion durchführen oder sie in einem Hybridmodell einsetzen VPC, bei dem der Ost-West-Verkehr durch eine Inspektion fließt VPC und der Interneteingang einzeln geprüft wird. VPC Eine weitere Überlegung ist, ob die Lösung das Entpacken von Transport Layer Security (TLS) unterstützt, wodurch eine Deep Packet Inspection für Datenflüsse, die in beide Richtungen initiiert werden, ermöglicht wird. Weitere Informationen und ausführliche Details zu diesen Konfigurationen finden Sie im Leitfaden für [AWS Network Firewall Best Practices](#).



Wenn Sie Lösungen verwenden, die out-of-band Inspektionen durchführen, z. B. die PCAP-Analyse von Paketdaten von Netzwerkschnittstellen, die im Promiscuous-Modus arbeiten, können Sie die Verkehrsspiegelung konfigurieren. VPC Gespiegelter Datenverkehr wird auf die verfügbare Bandbreite Ihrer Schnittstellen angerechnet und unterliegt denselben Datenübertragungsgebühren wie nicht gespiegelter Datenverkehr. Sie können sehen, ob virtuelle Versionen dieser Appliances auf dem verfügbar sind [AWS Marketplace](#), was möglicherweise die Inline-Bereitstellung hinter einem unterstützt. GWLB

Schützen Sie Ihre Anwendung bei Komponenten, die über HTTP basierte Protokolle abgewickelt werden, mit einer Webanwendungs-Firewall (WAF) vor häufigen Bedrohungen. [AWS WAF](#) ist eine Firewall für Webanwendungen, mit der Sie Anfragen, die Ihren konfigurierbaren Regeln entsprechen, überwachen und blockieren HTTP können, bevor sie an Amazon API Gateway CloudFront, Amazon AWS AppSync oder einen Application Load Balancer gesendet werden. Ziehen Sie Deep Packet Inspection in Betracht, wenn Sie den Einsatz Ihrer Webanwendungs-Firewall evaluieren, da Sie bei einigen Anwendungen den Vorgang TLS vor der Datenverkehrsinspektion beenden müssen. Zu Beginn können Sie AWS WAF es [Von AWS verwaltete Regeln](#) in Kombination mit Ihren eigenen Integrationen verwenden oder bestehende [Partnerintegrationen](#) verwenden.

Mit können Sie AWS WAF, AWS Shield Advanced AWS Network Firewall, und VPC Amazon-Sicherheitsgruppen in Ihrer gesamten AWS Organisation zentral verwalten [AWS Firewall Manager](#).

### Implementierungsschritte

1. Stellen Sie fest, ob Sie die Inspektionsregeln breit fassen können VPC, z. B. durch eine Inspektion, oder ob Sie einen detaillierteren VPC Ansatz benötigen.
2. Für Inline-Prüfungslösungen:
  - a. Falls Sie diese verwenden AWS Network Firewall, erstellen Sie Regeln, Firewall-Richtlinien und die Firewall selbst. Sobald diese konfiguriert sind, können Sie den [Datenverkehr an den Endpunkt der Firewall leiten](#), um die Prüfung zu aktivieren.
  - b. Wenn Sie eine Appliance eines Drittanbieters mit einem Gateway Load Balancer (GWLB) verwenden, stellen Sie Ihre Appliance in einer oder mehreren Availability Zones bereit und konfigurieren Sie sie. Erstellen Sie dann Ihren GWLB Endpunktdienst und konfigurieren Sie das Routing für Ihren Datenverkehr.
3. Für out-of-band Inspektionslösungen:
  1. Aktivieren Sie VPC Traffic Mirroring auf Schnittstellen, an denen eingehender und ausgehender Datenverkehr gespiegelt werden soll. Sie können EventBridge Amazon-Regeln verwenden, um eine AWS Lambda Funktion aufzurufen, mit der die Verkehrsspiegelung auf Schnittstellen

aktiviert wird, wenn neue Ressourcen erstellt werden. Richten Sie die Sitzungen zur Datenverkehrsspiegelung auf den Network Load Balancer vor Ihrer Appliance, der den Datenverkehr verarbeitet.

#### 4. Für Lösungen für eingehenden Internetdatenverkehr:

- a. Um zu konfigurieren AWS WAF, konfigurieren Sie zunächst eine Web-Zugriffskontrollliste (WebACL). Das Web ACL ist eine Sammlung von Regeln mit einer seriell verarbeiteten Standardaktion (ALLOW oder DENY), die definiert, wie Sie mit dem Datenverkehr WAF umgehen. Sie können Ihre eigenen Regeln und Gruppen erstellen oder AWS verwaltete Regelgruppen in Ihrem Web ACL verwenden.
- b. Sobald Ihr Web konfiguriert ACL ist, verknüpfen Sie das Web ACL mit einer AWS Ressource (wie einem Application Load Balancer, einem API Gateway oder einer CloudFront Distribution) RESTAPI, um mit dem Schutz des Webverkehrs zu beginnen.

#### Ressourcen

##### Zugehörige Dokumente:

- [What is Traffic Mirroring?](#)
- [Implementing inline traffic inspection using third-party security appliances](#)
- [AWS Network Firewall Beispielarchitekturen mit Routing](#)
- [Zentralisierte Inspektionsarchitektur mit AWS Gateway Load Balancer und AWS Transit Gateway](#)

##### Zugehörige Beispiele:

- [Best practices for deploying Gateway Load Balancer](#)
- [TLS Inspektionskonfiguration für verschlüsselten Ausgangsverkehr und AWS Network Firewall](#)

##### Zugehörige Tools:

- [AWS Marketplace IDS/IPS](#)

#### SEC05-BP04 Automatisieren Sie den Netzwerkschutz

Automatisieren Sie die Implementierung Ihrer Netzwerkschutzmaßnahmen mithilfe von DevOps Methoden wie Infrastructure as Code (IaC) und CI/CD-Pipelines. Diese Praktiken können Ihnen helfen, Änderungen an Ihrem Netzwerkschutz über ein Versionskontrollsystem zu verfolgen, den

Zeitaufwand für die Bereitstellung von Änderungen zu reduzieren und zu erkennen, wenn Ihr Netzwerkschutz von der gewünschten Konfiguration abweicht.

Gewünschtes Ergebnis: Sie definieren Netzwerkschutzmaßnahmen mit Vorlagen und übertragen diese in ein Versionskontrollsystem. Automatisierte Pipelines werden initiiert, wenn neue Änderungen vorgenommen werden, die ihre Prüfung und Bereitstellung orchestrieren.

Richtlinienprüfungen und andere statische Tests dienen der Validierung von Änderungen vor der Bereitstellung. Sie stellen die Änderungen in einer Staging-Umgebung bereit, um zu überprüfen, ob die Kontrollen wie erwartet funktionieren. Die Bereitstellung in Ihrer Produktionsumgebung erfolgt ebenfalls automatisch, sobald die Kontrollen genehmigt sind.

Typische Anti-Muster:

- Darauf vertrauen, dass die einzelnen Workload-Teams ihren kompletten Netzwerkstack, Schutzmaßnahmen und Automatisierungen selbst definieren Keine zentrale Veröffentlichung von Standardaspekten des Netzwerkstacks und der Schutzmechanismen für Workload-Teams zur Nutzung
- Auf ein zentrales Netzwerkteam vertrauen, das alle Aspekte des Netzwerks, der Schutzmaßnahmen und der Automatisierungen definiert Verzicht auf die Delegation von Workload-spezifischen Aspekten des Netzwerkstacks und der Schutzmaßnahmen an das Team des Workloads
- Beibehalten eines ausgewogenen Verhältnisses zwischen Zentralisierung und Delegation zwischen einem Netzwerkteam und Workload-Teams, aber keine Anwendung konsistenter Test- und Bereitstellungsstandards über Ihre IaC-Vorlagen und CI/CD-Pipelines hinweg Unterlassen der Erfassung erforderlicher Konfigurationen in Tools, die Ihre Vorlagen auf Einhaltung überprüfen

Vorteile der Nutzung dieser bewährten Methode: Durch die Verwendung von Vorlagen zur Definition Ihres Netzwerkschutzes können Sie Änderungen im Laufe der Zeit mit einem Versionskontrollsystem verfolgen und vergleichen. Der Einsatz von Automatisierung zum Testen und Bereitstellen von Änderungen schafft Standardisierung und Vorhersehbarkeit, erhöht die Chancen auf eine erfolgreiche Bereitstellung und reduziert die sich wiederholenden manuellen Konfigurationen.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel

Implementierungsleitfaden

Eine Reihe von Netzwerkschutzmaßnahmen, die in [SEC05-BP02 Steuern Sie den Datenfluss innerhalb Ihrer Netzwerkschichten](#) und [SEC 05-BP03 Implementieren Sie inspektionsbasierten](#)

[Schutz](#) beschrieben sind, verfügen über verwaltete Regelsysteme, die automatisch auf der Grundlage der neuesten Bedrohungsinformationen aktualisiert werden können. [Beispiele für den Schutz Ihrer Web-Endgeräte sind AWS WAF verwaltete Regeln und automatische Abwehr auf Anwendungsebene.](#) [AWS Shield Advanced DDoS](#) Verwenden Sie [von AWS Network Firewall verwaltete Regelgruppen](#), um auch bei Domain-Listen mit geringer Reputation und Bedrohungssignaturen auf dem Laufenden zu bleiben.

Neben verwalteten Regeln empfehlen wir Ihnen, DevOps Methoden zur Automatisierung der Bereitstellung Ihrer Netzwerkressourcen, Schutzmaßnahmen und der von Ihnen festgelegten Regeln zu verwenden. Sie können diese Definitionen in [AWS CloudFormation](#) oder einem anderen Infrastructure as Code (IaC)-Tool Ihrer Wahl erfassen, sie an ein Versionskontrollsystem übergeben und sie über CI/CD-Pipelines bereitstellen. Nutzen Sie diesen Ansatz, um die traditionellen Vorteile der DevOps Verwaltung Ihrer Netzwerkkontrollen zu nutzen, z. B. vorhersehbarere Versionen, automatisierte Tests mit Tools wie [AWS CloudFormation Guard](#) und die Erkennung von Abweichungen zwischen Ihrer bereitgestellten Umgebung und der gewünschten Konfiguration.

Basierend auf den Entscheidungen, die Sie im Rahmen von [SEC05-BP01 Create Network Layers getroffen haben, verfolgen Sie möglicherweise einen zentralen Managementansatz für die Erstellung von Netzwerkschichten](#) VPCs, die für Eingangs-, Ausgangs- und Inspektionsabläufe vorgesehen sind. [Wie in der AWS Sicherheitsreferenzarchitektur \(AWS SRA\) beschrieben, können Sie diese VPCs in einem speziellen Netzwerkinfrastrukturkonto definieren.](#) Sie können ähnliche Techniken verwenden, um zentral die von Ihren Workloads in anderen Konten VPCs verwendeten Sicherheitsgruppen, AWS Network Firewall Bereitstellungen, Route 53-Resolver-Regeln und DNS Firewall-Konfigurationen sowie andere Netzwerkressourcen zu definieren. Sie können diese Ressourcen mit Ihren anderen Konten mit [AWS Resource Access Manager](#) teilen. Mit diesem Ansatz können Sie das automatisierte Testen und die Bereitstellung Ihrer Netzwerkkontrollen für das Netzwerkkonto vereinfachen, da Sie nur ein Ziel verwalten müssen. Sie können dies in einem hybriden Modell tun, bei dem Sie bestimmte Kontrollen zentral bereitstellen und gemeinsam nutzen und andere Kontrollen an die einzelnen Workload-Teams und ihre jeweiligen Konten delegieren.

### Implementierungsschritte

1. Legen Sie fest, welche Aspekte des Netzwerks und des Schutzes zentral definiert werden und welche Ihre Workload-Teams verwalten können.
2. Erstellen Sie Umgebungen zum Testen und Bereitstellen von Änderungen an Ihrem Netzwerk und dessen Schutzmaßnahmen. Verwenden Sie zum Beispiel ein Netzwerk-Testkonto und ein Netzwerk-Produktionskonto.

3. Legen Sie fest, wie Sie Ihre Vorlagen in einem Versionskontrollsystem speichern und pflegen wollen. Speichern Sie zentrale Vorlagen in einem Repository, das sich von den Workload-Repositories unterscheidet, während Workload-Vorlagen in Repositories gespeichert werden können, die speziell für diesen Workload gelten.
4. Erstellen Sie CI/CD-Pipelines zum Testen und Bereitstellen von Vorlagen. Definieren Sie Tests, um zu prüfen, ob Fehlkonfigurationen vorliegen und ob die Vorlagen den Standards Ihres Unternehmens entsprechen.

## Ressourcen

### Zugehörige bewährte Methoden:

- [SEC01-BP06 Automatisieren Sie die Implementierung von Standard-Sicherheitskontrollen](#)

### Zugehörige Dokumente:

- [AWS Security Reference Architecture - Network account](#)

### Zugehörige Beispiele:

- [AWS Deployment Pipeline Reference Architecture](#)
- [NetDevSecOps zur Modernisierung von Netzwerkinstallationen AWS](#)
- [Integration von AWS CloudFormation Sicherheitstests und Berichten AWS Security Hub AWS CodeBuild](#)

### Zugehörige Tools:

- [AWS CloudFormation](#)
- [AWS CloudFormation Guard](#)
- [cfn\\_nag](#)

## SEC6. Wie werden Ihre Rechenressourcen geschützt?

Die Rechenressourcen in Ihrer Workload erfordern mehrere Verteidigungsebenen, um sie vor externen und internen Bedrohungen zu schützen. Zu den Rechenressourcen gehören EC2 Instanzen, Container, AWS Lambda Funktionen, Datenbankdienste, IoT-Geräte und mehr.

## Bewährte Methoden

- [SEC06-BP01 Schwachstellenmanagement durchführen](#)
- [SEC06-BP02 Bereitstellen von Rechenleistung aus gehärteten Images](#)
- [SEC06-BP03 Reduzieren Sie die manuelle Verwaltung und den interaktiven Zugriff](#)
- [SEC06-BP04 Softwareintegrität validieren](#)
- [SEC06-BP05 Automatisieren Sie den Computerschutz](#)

### SEC06-BP01 Schwachstellenmanagement durchführen

Überprüfen und Patchen Sie Ihren Code, Ihre Abhängigkeiten und Ihre Infrastruktur häufig auf Schwachstellen, um sich vor neuen Bedrohungen zu schützen.

Gewünschtes Ergebnis: Erstellen und Verwalten eines Programms für das Schwachstellenmanagement. Scannen und patchen Sie regelmäßig Ressourcen wie EC2 Amazon-Instances, Amazon Elastic Container Service (AmazonECS) -Container (Amazon) und Amazon Elastic Kubernetes Service (AmazonEKS) -Workloads. Konfigurieren Sie Wartungsfenster für AWS verwaltete Ressourcen wie Amazon Relational Database Service (AmazonRDS) -Datenbanken. Verwenden Sie statisches Code-Scanning, um Anwendungsquellcode auf verbreitete Probleme zu überprüfen. Ziehen Sie Penetrationstests für Webanwendungen in Betracht, wenn Ihre Organisation über die entsprechenden Fähigkeiten verfügt oder externe Unterstützung erhalten kann.

#### Typische Anti-Muster:

- Fehlen eines Programms für das Schwachstellenmanagement
- Durchführung von System-Patches ohne Berücksichtigung des Schweregrads oder der Risikovermeidung
- Verwendung von Software, deren vom Hersteller bereitgestelltes Haltbarkeitsdatum () überschritten wurde. EOL
- Bereitstellung von Code für die Produktion, bevor dieser auf Sicherheitsprobleme untersucht wurde

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Hoch

#### Implementierungsleitfaden

Ein Programm für das Schwachstellenmanagement beinhaltet Sicherheitsbewertungen, die Identifizierung von Problemen sowie die Priorisierung und Durchführung von Patching-Vorgängen

im Rahmen der Behebung der Probleme. Automatisierung ist der Schlüssel zur kontinuierlichen Prüfung von Workloads auf Probleme und unbeabsichtigte Offenlegung in Netzwerken sowie für die Durchführung von Abhilfemaßnahmen. Die Automatisierung der Erstellung und Aktualisierung von Ressourcen spart Zeit und senkt die Gefahr von Konfigurationsfehlern, die zu weiteren Problemen führen können. Ein gut gestaltetes Programm für das Schwachstellenmanagement sollte auch Schwachstellentests in den Entwicklungs- und Bereitstellungsphasen des Softwarelebenszyklus beinhalten. Die Implementierung des Schwachstellenmanagements während der Entwicklung und der Bereitstellung verringert die Gefahr, dass eine Schwachstelle in Ihre Produktionsumgebung gelangt.

Die Implementierung eines Programms für das Schwachstellenmanagement erfordert ein gutes Verständnis des [AWS -Modells der geteilten Verantwortung](#) und seiner Beziehung zu Ihren spezifischen Workloads. Im Rahmen des Modells der geteilten Verantwortung AWS ist verantwortlich für den Schutz der Infrastruktur der. AWS Cloud Diese Infrastruktur besteht aus Hardware, Software, Netzwerken und Einrichtungen, die AWS Cloud Dienste ausführen. Sie sind für die Sicherheit in der Cloud verantwortlich, z. B. für die eigentlichen Daten, die Sicherheitskonfiguration und die Verwaltungsaufgaben von EC2 Amazon-Instances, und dafür, dass Ihre Amazon S3-Objekte ordnungsgemäß klassifiziert und konfiguriert sind. Ihr Konzept für das Schwachstellenmanagement kann auch je nach den von Ihnen genutzten Services variieren. AWS Verwaltet beispielsweise das Patchen für unseren verwalteten relationalen Datenbankservice AmazonRDS, aber Sie wären für das Patchen selbst gehosteter Datenbanken verantwortlich.

AWS bietet eine Reihe von Dienstleistungen an, die Sie bei Ihrem Schwachstellen-Management-Programm unterstützen. [Amazon Inspector](#) scannt AWS Workloads kontinuierlich auf Softwareprobleme und unbeabsichtigten Netzwerkzugriff. [AWS Systems Manager Patch Manager](#) hilft Ihnen bei der Verwaltung von Patches in Ihren EC2 Amazon-Instances. Amazon Inspector und Systems Manager können in eingesehen werden [AWS Security Hub](#), einem Cloud-Service zur Verwaltung des Sicherheitsstatus, der dabei hilft, AWS Sicherheitsprüfungen zu automatisieren und Sicherheitswarnungen zu zentralisieren.

[Amazon CodeGuru](#) kann mithilfe einer statischen Codeanalyse dabei helfen, potenzielle Probleme in Java- und Python-Anwendungen zu identifizieren.

### Implementierungsschritte

- [Amazon Inspector](#) konfigurieren: Amazon Inspector erkennt automatisch neu gestartete EC2 Amazon-Instances, Lambda-Funktionen und geeignete Container-Images, die an Amazon gesendet werden, ECR und scannt sie sofort auf Softwareprobleme, potenzielle Fehler und unbeabsichtigte Netzwerkgefährdung.

- Untersuchen Sie den Quellcode: Überprüfen Sie Bibliotheken und Abhängigkeiten auf Probleme und Fehler. [Amazon CodeGuru](#) kann sowohl für Java- als auch für Python-Anwendungen scannen und Empfehlungen zur Behebung [häufiger Sicherheitsprobleme](#) geben. [Die OWASP Foundation](#) veröffentlicht eine Liste von Tools zur Quellcode-Analyse (auch bekannt als SAST Tools).
- Implementieren Sie einen Mechanismus zur Untersuchung und zum Patching Ihrer bestehenden Umgebung sowie zur Untersuchung im Rahmen eines CI/CD-Pipeline-Erstellungsprozesses: Implementieren Sie einen Mechanismus zur Untersuchung und zum Patching von Problemen in Ihren Abhängigkeiten und Betriebssystemen, um Schutz gegen neue Bedrohungen zu bieten. Lassen Sie diesen Mechanismus regelmäßig laufen. Das Software-Schwachstellenmanagement ist wichtig, um zu verstehen, wo Patches angebracht oder Softwareprobleme behoben werden müssen. Priorisieren Sie die Abhilfemaßnahmen zu potenziellen Sicherheitsproblemen durch die frühzeitige Einbettung von Schwachstellenanalysen in Ihre Pipeline für kontinuierliche Integration und kontinuierliche Bereitstellung (Continuous Integration/Continuous Delivery, CI/CD). Ihr Ansatz kann je nach den AWS Diensten, die Sie in Anspruch nehmen, variieren. Um nach potenziellen Problemen mit Software zu suchen, die in EC2 Amazon-Instances ausgeführt wird, fügen Sie [Amazon Inspector](#) zu Ihrer Pipeline hinzu, um Sie zu benachrichtigen und den Erstellungsprozess zu beenden, wenn Probleme oder potenzielle Fehler erkannt werden. Amazon Inspector überwacht Ressourcen kontinuierlich. Sie können auch Open-Source-Produkte wie [OWASPDependency-Check](#), [Snyk](#), [Open VAS](#), Paketmanager und Tools für das Schwachstellenmanagement verwenden. AWS Partner
- Verwendung [AWS Systems Manager](#): Sie sind für das Patch-Management für Ihre AWS Ressourcen verantwortlich, einschließlich Amazon Elastic Compute Cloud (AmazonEC2) - Instances, Amazon Machine Images (AMIs) und anderer Rechenressourcen. [AWS Systems Manager Patch Manager](#) automatisiert das Patchen verwalteter Instances mit sicherheitsrelevanten und anderen Arten von Updates. Patch Manager kann verwendet werden, um Patches auf EC2 Amazon-Instances sowohl für Betriebssysteme als auch für Anwendungen anzuwenden, einschließlich Microsoft-Anwendungen, Windows-Service Packs und Nebenversions-Upgrades für Linux-basierte Instances. Neben Amazon EC2 kann Patch Manager auch zum Patchen von lokalen Servern verwendet werden.

Eine Liste der unterstützten Betriebssysteme finden Sie unter [Unterstützte Betriebssysteme](#) im Systems Manager-Benutzerhandbuch. Sie können Instances nur auf Patches hin durchsuchen und dann einen Bericht zu fehlenden Patches anzeigen oder automatisch alle fehlenden Patches installieren.

- Verwendung [AWS Security Hub](#): Security Hub bietet einen umfassenden Überblick über Ihren Sicherheitsstatus in AWS. Es sammelt Sicherheitsdaten über [mehrere AWS Dienste](#) hinweg und



stellt diese Ergebnisse in einem standardisierten Format bereit, sodass Sie Sicherheitserkenntnisse AWS dienstübergreifend priorisieren können.

- Verwenden Sie [AWS CloudFormation](#): [AWS CloudFormation](#) ist ein Infrastructure-as-Code (IaC)-Service, der das Schwachstellenmanagement durch die Automatisierung der Ressourcenbereitstellung und die Standardisierung der Ressourcenarchitektur über mehrere Konten und Umgebungen hinweg unterstützt.

## Ressourcen

### Zugehörige Dokumente:

- [AWS Systems Manager](#)
- [Überblick über die Sicherheit von AWS Lambda](#)
- [Amazon CodeGuru](#)
- [Improved, Automated Vulnerability Management for Cloud Workloads with a New Amazon Inspector](#)
- [Automatisieren Sie das Schwachstellenmanagement und die Behebung AWS von Sicherheitslücken mithilfe von Amazon Inspector und AWS Systems Manager — Teil 1](#)

### Zugehörige Videos:

- [Securing Serverless and Container Services](#)
- [Bewährte Sicherheitsmethoden für den EC2 Amazon-Instance-Metadatenservice](#)

## SEC06-BP02 Bereitstellen von Rechenleistung aus gehärteten Images

Bieten Sie weniger Möglichkeiten für einen unbeabsichtigten Zugriff auf Ihre Laufzeitumgebungen, indem Sie sie über gehärtete Images bereitstellen. Beziehen Sie Laufzeit-Abhängigkeiten wie Container-Images und Anwendungsbibliotheken nur von vertrauenswürdigen Registern und überprüfen Sie deren Signaturen. Erstellen Sie Ihre eigenen privaten Register, um vertrauenswürdige Images und Bibliotheken für die Verwendung in Ihren Build- und Bereitstellungsprozessen zu speichern.

**Gewünschtes Ergebnis:** Ihre Datenverarbeitungsressourcen werden über gehärtete Baseline-Images bereitgestellt. Sie rufen externe Abhängigkeiten, wie Container-Images und Anwendungsbibliotheken, nur aus vertrauenswürdigen Registern ab und überprüfen deren Signaturen. Diese werden in privaten

Registern gespeichert, auf die Ihre Build- und Bereitstellungsprozesse verweisen können. Sie überprüfen und aktualisieren Images und Abhängigkeiten regelmäßig, um sich vor neu entdeckten Schwachstellen zu schützen.

Typische Anti-Muster:

- Abrufen von Images und Bibliotheken aus vertrauenswürdigen Registern, ohne deren Signaturen zu überprüfen oder Schwachstellen zu scannen, bevor sie eingesetzt werden
- Härtung von Images, ohne sie regelmäßig auf neue Schwachstellen zu testen oder auf die neueste Version zu aktualisieren
- Installation oder Nichtentfernung von Softwarepaketen, die während des erwarteten Lebenszyklus des Images nicht benötigt werden
- Vertrauen auf Patches als einzige Methode, um Datenverarbeitungsressourcen in der Produktion auf dem neuesten Stand zu halten. Die alleinige Verwendung von Patches kann immer noch dazu führen, dass Datenverarbeitungsressourcen im Laufe der Zeit von dem gehärteten Standard abweichen. Patches sind außerdem nicht in der Lage, Malware zu entfernen, die möglicherweise von einem Bedrohungsakteur während eines Sicherheitsvorfalls installiert wurde.

Vorteile der Nutzung dieser bewährten Methode: Das Härten von Images trägt dazu bei, die Anzahl der in Ihrer Laufzeitumgebung verfügbaren Pfade zu reduzieren, die unbeabsichtigten Zugriff auf nicht autorisierte Benutzer oder Services ermöglichen können. Auch das Ausmaß der Auswirkungen eines unbeabsichtigten Zugriffs kann damit verringert werden.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Hoch

Implementierungsleitfaden

Um Ihre Systeme abzusichern, sollten Sie mit den neuesten Versionen von Betriebssystemen, Container-Images und Anwendungsbibliotheken beginnen. Wenden Sie Patches auf bekannte Probleme an. Reduzieren Sie das System auf ein Minimum, indem Sie nicht benötigte Anwendungen, Services, Gerätetreiber, Standardbenutzer und andere Anmeldeinformationen entfernen. Ergreifen Sie alle weiteren erforderlichen Maßnahmen, wie z. B. das Deaktivieren von Ports, um eine Umgebung zu schaffen, die nur über die von Ihren Workloads benötigten Ressourcen und Fähigkeiten verfügt. Von dieser Baseline aus können Sie dann Software, Agenten oder andere Prozesse installieren, die Sie für Zwecke wie die Überwachung des Workloads oder die Verwaltung von Schwachstellen benötigen.

Sie können die Belastung durch die Abhärtung von Systemen verringern, indem Sie sich an Anleitungen von vertrauenswürdigen Quellen wie dem [Center for Internet Security \(CIS\) und den Security Technical Implementation Guides](#) () der Defense Information Systems Agency (DISA) halten. Wir empfehlen Ihnen, mit einem [Amazon Machine Image](#) (AMI) zu beginnen, das von AWS oder einem APN Partner veröffentlicht wurde, und den AWS [EC2Image Builder](#) zu verwenden, um die Konfiguration gemäß einer geeigneten Kombination von CIS und STIG Kontrollen zu automatisieren.

Zwar sind gehärtete Images und EC2 Image Builder Builder-Rezepte verfügbar, die die CIS DISA STIG Oder-Empfehlungen anwenden, aber Sie stellen möglicherweise fest, dass Ihre Software aufgrund ihrer Konfiguration nicht erfolgreich ausgeführt werden kann. In diesem Fall können Sie von einem nicht gehärteten Basis-Image ausgehen, Ihre Software installieren und dann schrittweise CIS Kontrollen anwenden, um deren Wirkung zu testen. Testen Sie bei allen CIS Kontrollen, die die Ausführung Ihrer Software verhindern, ob Sie stattdessen die detaillierteren Empfehlungen zur Absicherung implementieren können. DISA Behalten Sie den Überblick über die verschiedenen CIS Steuerungen und DISA STIG Konfigurationen, die Sie erfolgreich anwenden können. Verwenden Sie diese, um Ihre Rezepte für die Bildhärtung in EC2 Image Builder entsprechend zu definieren.

[Für containerisierte Workloads sind gehärtete Images von Docker im öffentlichen Repository von Amazon Elastic Container Registry \(\) ECR verfügbar.](#) Sie können EC2 Image Builder verwenden, um Container-Images gleichzeitig AMIs zu härten.

Ähnlich wie bei Betriebssystemen und Container-Images können Sie Codepakete (oder Bibliotheken) mithilfe von Tools wie pip, npm, Maven und aus öffentlichen Repositories abrufen. NuGet Wir empfehlen Ihnen, Code-Pakete zu verwalten, indem Sie private Repositories, wie z. B. innerhalb von [AWS CodeArtifact](#), mit vertrauenswürdigen öffentlichen Repositories verbinden. Diese Integration kann das Abrufen, Speichern und Aufbewahren von Paketen für Sie übernehmen. up-to-date Ihre Anwendungsentwicklungsverfahren können dann die neueste Version dieser Pakete zusammen mit Ihrer Anwendung abrufen und testen. Dabei kommen Techniken wie Software Composition Analysis (SCA), Static Application Security Testing (SAST) und Dynamic Application Security Testing (DAST) zum Einsatz.

Vereinfachen Sie für serverlose Workloads, die verwenden AWS Lambda, die Verwaltung von Paketabhängigkeiten mithilfe von [Lambda-Schichten](#). Verwenden Sie Lambda-Ebenen, um einen Satz von Standardabhängigkeiten, die von verschiedenen Funktionen gemeinsam genutzt werden, in einem eigenständigen Archiv zu konfigurieren. Sie können Ebenen mithilfe eines eigenen Build-Prozesses erstellen und verwalten, sodass Ihre Funktionen auf zentrale Weise erhalten bleiben. up-to-date

## Implementierungsschritte

- Härten des Betriebssystems: Verwenden Sie Basis-Images aus vertrauenswürdigen Quellen als Grundlage für den Aufbau Ihres gehärteten SystemsAMIs. Verwenden Sie [EC2Image Builder](#), um die auf Ihren Images installierte Software anzupassen.
- Härten von containerisierten Ressourcen: Konfigurieren Sie containerisierte Ressourcen so, dass sie den bewährten Methoden im Bereich Sicherheit entsprechen. Wenn Sie Container verwenden, implementieren Sie [ECRImage Scanning](#) in Ihrer Build-Pipeline und regelmäßig anhand Ihres Image-Repositorys, um CVEs in Ihren Containern danach zu suchen.
- Wenn Sie die serverlose Implementierung mit verwenden AWS Lambda, verwenden Sie [Lambda-Schichten](#), um Anwendungsfunktionscode und gemeinsam genutzte abhängige Bibliotheken zu trennen. Konfigurieren Sie die [Codesignierung](#) für Lambda, um sicherzustellen, dass nur vertrauenswürdiger Code in Ihren Lambda-Funktionen ausgeführt wird.

## Ressourcen

### Zugehörige bewährte Methoden:

- [OPS05-BP05 Führen Sie das Patch-Management durch](#)

### Zugehörige Videos:

- [Tauchen Sie tief in die Sicherheit ein AWS Lambda](#)

### Zugehörige Beispiele:

- [AMIMit EC2 Image Builder schnell STIG baukonform erstellen](#)
- [Building better container images](#)
- [Using Lambda layers to simplify your development process](#)
- [Entwickeln und implementieren Sie AWS Lambda Ebenen mit dem Serverless Framework](#)
- [Aufbau einer end-to-end AWS DevSecOps CI/CD-Pipeline mit Open Source SCA und Tools SAST DAST](#)

## SEC06-BP03 Reduzieren Sie die manuelle Verwaltung und den interaktiven Zugriff

Nutzen Sie Automatisierung für die Bereitstellung, Konfiguration, Wartung und Untersuchung, wo immer dies möglich ist. Erwägen Sie den manuellen Zugriff auf Datenverarbeitungsressourcen in Notfällen oder in sicheren (Sandbox-)Umgebungen, wenn keine Automatisierung möglich ist.

Gewünschtes Ergebnis: Programmatische Skripte und Automatisierungsdokumente (Runbooks) erfassen autorisierte Aktionen in Ihren Datenverarbeitungsressourcen. Diese Runbooks werden entweder automatisch durch Systeme zur Erkennung von Änderungen oder manuell ausgelöst, wenn ein menschliches Urteilsvermögen erforderlich ist. Der direkte Zugriff auf Datenverarbeitungsressourcen wird nur in Notfällen gewährt, wenn keine Automatisierung verfügbar ist. Alle manuellen Aktivitäten werden protokolliert und in einen Überprüfungsprozess einbezogen, um Ihre Automatisierungsmöglichkeiten kontinuierlich zu verbessern.

Typische Anti-Muster:

- Interaktiver Zugriff auf EC2 Amazon-Instances mit Protokollen wie SSH oder RDP.
- Verwalten einzelner Benutzeranmeldungen wie `/etc/passwd` oder lokaler Windows-Benutzer.
- Gemeinsame Nutzung eines Passworts oder privaten Schlüssels für den Zugriff auf eine Instance durch mehrere Benutzer.
- Manuelles Installieren von Software und Erstellen oder Aktualisieren von Konfigurationsdateien.
- Manuelles Aktualisieren oder Patchen von Software.
- Einloggen in eine Instance, um Probleme zu beheben.

Vorteile der Nutzung dieser bewährten Methode: Die Durchführung automatisierter Aktionen hilft Ihnen, das betriebliche Risiko unbeabsichtigter Änderungen und Fehlkonfigurationen zu verringern. Wenn Sie die Verwendung von Secure Shell (SSH) und Remote Desktop Protocol (RDP) für den interaktiven Zugriff entfernen, wird der Umfang des Zugriffs auf Ihre Rechenressourcen reduziert. Damit wird ein gängiger Weg für unbefugte Aktionen abgeschnitten. Die Erfassung Ihrer Aufgaben zur Verwaltung von Datenverarbeitungsressourcen in Automatisierungsdokumenten und programmatischen Skripten bietet einen Mechanismus, mit dem Sie den gesamten Umfang der autorisierten Aktivitäten bis ins kleinste Detail definieren und überprüfen können.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel

## Implementierungsleitfaden

Das Protokollieren einer Instance ist eine klassische Methode der Systemverwaltung. Nach der Installation des Server-Betriebssystems würden sich die Benutzer normalerweise manuell anmelden, um das System zu konfigurieren und die gewünschte Software zu installieren. Während der Lebensdauer des Servers melden sich die Benutzer möglicherweise an, um Software-Updates durchzuführen, Patches anzuwenden, Konfigurationen zu ändern und Probleme zu beheben.

Der manuelle Zugriff birgt jedoch eine Reihe von Risiken. Dazu ist ein Server erforderlich, der Anfragen abhört, z. B. einen SSH RDP OR-Dienst, der einen potenziellen Weg zu unberechtigtem Zugriff bieten kann. Außerdem erhöht sich dadurch das Risiko menschlicher Fehler bei der Durchführung manueller Schritte. Diese können zu Störungen des Workloads, zur Beschädigung oder Zerstörung von Daten oder zu anderen Sicherheitsproblemen führen. Der menschliche Zugriff erfordert außerdem Schutzmaßnahmen gegen die Weitergabe von Anmeldeinformationen, was zusätzlichen Verwaltungsaufwand bedeutet.

Um diese Risiken zu minimieren, können Sie eine agentenbasierte Fernzugriffslösung wie [AWS Systems Manager](#) implementieren. AWS Systems Manager Der Agent (SSMAgent) initiiert einen verschlüsselten Kanal und ist daher nicht darauf angewiesen, extern initiierte Anfragen abzuhören. Erwägen Sie, den SSM Agenten so zu konfigurieren, dass [dieser Kanal über](#) einen Endpunkt eingerichtet wird. VPC

Systems Manager gibt Ihnen eine fein abgestufte Kontrolle darüber, wie Sie mit Ihren verwalteten Instances interagieren können. Sie legen fest, welche Automatisierungen ausgeführt werden sollen, wer sie ausführen darf und wann sie ausgeführt werden können. Systems Manager ist in der Lage, Patches anzuwenden, Software zu installieren und Konfigurationsänderungen ohne interaktiven Zugriff auf die Instance vorzunehmen. Systems Manager kann auch Zugriff auf eine Remote-Shell gewähren und jeden während der Sitzung aufgerufenen Befehl und seine Ausgabe in Protokollen und [Amazon S3](#) protokollieren. [AWS CloudTrail](#) zeichnet Aufrufe von Systems Manager APIs zur Inspektion auf.

## Implementierungsschritte

1. [Installieren Sie AWS Systems Manager Agent](#) (SSMAgent) auf Ihren EC2 Amazon-Instances. Prüfen Sie, ob SSM Agent in Ihrer AMI Basiskonfiguration enthalten ist und automatisch gestartet wird.
2. Stellen Sie sicher, dass die IAM Rollen, die Ihren EC2 Instanzprofilen zugeordnet sind, die AmazonSSMManagedInstanceCore [verwaltete IAM Richtlinie](#) enthalten.

3. Deaktivieren Sie SSHRDP, und andere Fernzugriffsdienste, die auf Ihren Instances ausgeführt werden. Sie können dies tun, indem Sie Skripts ausführen, die im Benutzerdatenbereich Ihrer Startvorlagen konfiguriert sind, oder indem Sie benutzerdefinierte Skripts AMIs mit Tools wie EC2 Image Builder erstellen.
4. Stellen Sie sicher, dass die für Ihre EC2 Instances geltenden Regeln für den Zugriff auf Sicherheitsgruppen keinen Zugriff auf Port 22/tcp (SSH) oder Port 3389/tcp (RDP) zulassen. Implementieren Sie die Erkennung und Alarmierung bei falsch konfigurierten Sicherheitsgruppen mit Services wie AWS Config.
5. Definieren Sie entsprechende Automatisierungen, Runbooks und Run Commands in Systems Manager. Definieren Sie mithilfe von IAM Richtlinien, wer diese Aktionen ausführen kann und unter welchen Bedingungen sie zulässig sind. Testen Sie diese Automatisierungen gründlich in einer nicht produktiven Umgebung. Rufen Sie diese Automatisierungen bei Bedarf auf, anstatt interaktiv auf die Instance zuzugreifen.
6. Verwenden Sie [AWS Systems Manager Session Manager](#), um bei Bedarf interaktiven Zugriff auf Instances zu ermöglichen. Aktivieren Sie die Protokollierung der Sitzungsaktivitäten, um einen Prüfpfad in [Amazon CloudWatch Logs](#) oder [Amazon S3](#) zu führen.

## Ressourcen

### Zugehörige bewährte Methoden:

- [REL08-BP04 Mithilfe einer unveränderlichen Infrastruktur bereitstellen](#)

### Zugehörige Beispiele:

- [Ersatz des SSH Zugriffs zur Reduzierung des Verwaltungs- und Sicherheitsaufwands durch AWS Systems Manager](#)

### Zugehörige Tools:

- [AWS Systems Manager](#)

### Zugehörige Videos:

- [Steuern des Zugriffs von Benutzersitzungen auf Instanzen im AWS Systems Manager Session Manager](#)

## SEC06-BP04 Softwareintegrität validieren

Verwenden Sie die kryptografische Überprüfung, um die Integrität von Software-Artefakten (einschließlich Images) zu überprüfen, die Ihr Workload verwendet. Signieren Sie Ihre Software kryptografisch, um sie vor unbefugten Änderungen in Ihren Computerumgebungen zu schützen.

Gewünschtes Ergebnis: Alle Artefakte werden aus vertrauenswürdigen Quellen bezogen. Die Zertifikate der Website des Anbieters sind validiert. Heruntergeladene Artefakte werden anhand ihrer Signaturen kryptografisch verifiziert. Ihre eigene Software ist kryptografisch signiert und wird von Ihren Computerumgebungen überprüft.

Typische Anti-Muster:

- Vertrauen auf die Websites seriöser Anbieter, um Software-Artefakte zu erhalten, aber Hinweise zum Ablauf von Zertifikaten ignorieren Fortfahren mit dem Herunterladen, ohne zu bestätigen, dass die Zertifikate gültig sind
- Validieren der Zertifikate von Anbieter-Websites, aber keine kryptografische Überprüfung der heruntergeladenen Artefakte von diesen Websites
- Prüfen der Integrität von Software ausschließlich anhand von Digests oder Hashes Hashes stellen sicher, dass Artefakte gegenüber der ursprünglichen Version nicht verändert wurden, aber sie bestätigen nicht ihre Quelle.
- Nicht signieren Ihrer eigene Software, Ihres eigenen Codes oder Ihrer eigenen Bibliotheken, selbst wenn Sie sie nur in Ihren eigenen Bereitstellungen verwenden.

Vorteile der Nutzung dieser bewährten Methode: Die Überprüfung der Integrität von Artefakten, von denen Ihr Workload abhängt, hilft zu verhindern, dass Malware in Ihre Computerumgebungen eindringt. Das Signieren Ihrer Software schützt Sie davor, dass sie von Unbefugten in Ihrer Computerumgebung ausgeführt wird. Sichern Sie Ihre Softwarelieferkette durch Signieren und Verifizieren von Code.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Mittel

Implementierungsleitfaden

Betriebssystem-Images, Container-Images und Code-Artefakte werden oft mit verfügbaren Integritätsprüfungen verteilt, z. B. durch einen Digest oder Hash. Diese ermöglichen es den Clients, die Integrität zu überprüfen, indem sie ihren eigenen Hash der Nutzdaten berechnen und überprüfen, ob er mit dem veröffentlichten Hash übereinstimmt. Diese Überprüfungen helfen zwar dabei, sicherzustellen, dass die Nutzdaten nicht manipuliert wurden, aber sie bestätigen nicht, dass die



Nutzdaten von der ursprünglichen Quelle (ihrer Herkunft) stammen. Zur Überprüfung der Herkunft ist ein Zertifikat erforderlich, das eine vertrauenswürdige Stelle ausstellt, um das Artefakt digital zu signieren.

Wenn Sie in Ihrem Workload eine heruntergeladene Software oder Artefakte verwenden, prüfen Sie, ob der Anbieter einen öffentlichen Schlüssel für die Überprüfung der digitalen Signatur bereitstellt. Hier sind einige Beispiele dafür, wie AWS einen öffentlichen Schlüssel und Verifizierungsanweisungen für die von uns veröffentlichte Software bereitstellt:

- [EC2Image Builder: Überprüfen Sie die Signatur des AWS TOE Installationsdownloads](#)
- [AWS Systems Manager: Überprüfung der Signatur des Agenten SSM](#)
- [Amazon CloudWatch: Überprüfung der Signatur des CloudWatch Agentenpakets](#)

Integrieren Sie die Überprüfung digitaler Signaturen in die Prozesse, die Sie zum Abrufen und Härten von Images verwenden, wie unter [SEC06-BP02 Bereitstellung von Rechenleistung](#) aus gehärteten Images beschrieben.

Sie können [AWS Signer](#) verwenden, um die Überprüfung von Signaturen sowie Ihren eigenen Lebenszyklus der Codesignatur für Ihre eigene Software und Artefakte zu verwalten. Sowohl [AWS Lambda](#) als auch [Amazon Elastic Container Registry](#) bieten Integrationen mit Signer, um die Signaturen Ihres Codes und Ihrer Images zu überprüfen. Mit den Beispielen im Abschnitt Ressourcen können Sie Signer in Ihre Continuous Integration und Delivery (CI/CD) Pipelines einbinden, um die Überprüfung von Signaturen und die Signierung Ihres eigenen Codes und Ihrer Images zu automatisieren.

## Ressourcen

### Zugehörige Dokumente:

- [Cryptographic Signing for Containers](#)
- [Bewährte Methoden zur Sicherung Ihrer Pipeline für die Erstellung von Container-Images mithilfe von AWS Signer](#)
- [Ankündigung von Container Image Signing with AWS Signer und Amazon EKS](#)
- [Codesignatur konfigurieren für AWS Lambda](#)
- [Best practices and advanced patterns for Lambda code signing](#)
- [Codesignatur mit AWS Certificate Manager privater CA und AWS Key Management Service asymmetrischen Schlüsseln](#)

## Zugehörige Beispiele:

- [Automatisieren Sie die Lambda-Code-Signierung mit Amazon CodeCatalyst und AWS Signer](#)
- [Signieren und Validieren von OCI Artefakten mit AWS Signer](#)

## Zugehörige Tools:

- [AWS Lambda](#)
- [AWS Signer](#)
- [AWS Certificate Manager](#)
- [AWS Key Management Service](#)
- [AWS CodeArtifact](#)

## SEC06-BP05 Automatisieren Sie den Computerschutz

Automatisieren Sie den Datenverarbeitungsschutz, um das Erfordernis menschlichen Eingreifens zu reduzieren. Nutzen Sie automatisierte Scans, um potenzielle Probleme in Ihren Datenverarbeitungsressourcen zu erkennen und mit automatisierten programmatischen Reaktionen oder Flottenmanagement-Vorgängen zu beheben. Integrieren Sie Automatisierung in Ihre CI/CD-Prozesse, um vertrauenswürdige Workloads mit Abhängigkeiten bereitzustellen. up-to-date

Gewünschtes Ergebnis: Automatisierte Systeme führen alle Scans und Patches von Datenverarbeitungsressourcen durch. Mithilfe der automatisierten Überprüfung überprüfen Sie, ob Software-Images und Abhängigkeiten aus vertrauenswürdigen Quellen stammen und nicht manipuliert wurden. Workloads werden automatisch auf up-to-date Abhängigkeiten überprüft und signiert, um die Vertrauenswürdigkeit in Computerumgebungen zu gewährleisten. AWS Automatisierte Abhilfemaßnahmen werden eingeleitet, wenn nicht konforme Ressourcen entdeckt werden.

## Typische Anti-Muster:

- Verfolgen des Ansatzes einer unveränderlichen Infrastruktur, aber ohne eine Lösung für Notfall-Patches oder den Austausch von Produktionssystemen
- Verwenden von Automatisierung, um falsch konfigurierte Ressourcen zu korrigieren, ohne dass ein manueller Überschreibungsmechanismus vorhanden ist Es können Situationen entstehen, in denen Sie die Anforderungen anpassen müssen, und es kann sein, dass Sie die Automatisierungen aussetzen müssen, bis Sie diese Änderungen vorgenommen haben.

Vorteile der Nutzung dieser bewährten Methode: Die Automatisierung kann das Risiko des unbefugten Zugriffs und der Nutzung Ihrer Datenverarbeitungsressourcen verringern. Sie hilft zu verhindern, dass Fehlkonfigurationen in Produktionsumgebungen gelangen, und Fehlkonfigurationen zu erkennen und zu beheben, wenn sie auftreten. Die Automatisierung hilft auch bei der Erkennung von unbefugtem Zugriff und der Nutzung von Datenverarbeitungsressourcen, um Ihre Reaktionszeit zu verkürzen. Dies wiederum kann den Gesamtumfang der Auswirkungen des Problems verringern.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel

### Implementierungsleitfaden

Sie können die in den Methoden der Sicherheitssäule beschriebenen Automatisierungen zum Schutz Ihrer Datenverarbeitungsressourcen anwenden. [SEC06-BP01 Perform Vulnerability Management](#) beschreibt, wie Sie [Amazon Inspector](#) sowohl in Ihren CI/CD-Pipelines als auch zum kontinuierlichen Scannen Ihrer Laufzeitumgebungen auf bekannte allgemeine Sicherheitslücken und Risiken () verwenden können. CVEs Sie können [AWS Systems Manager](#) verwenden, um Patches anzuwenden oder neue Images über automatisierte Runbooks bereitzustellen, damit Ihre Computerflotte stets mit der neuesten Software und den neuesten Bibliotheken ausgestattet ist. Nutzen Sie diese Techniken, um den Bedarf an manuellen Prozessen und interaktivem Zugriff auf Ihre Datenverarbeitungsressourcen zu reduzieren. Weitere Informationen finden Sie unter [SEC06-BP03](#) Reduzieren Sie die manuelle Verwaltung und den interaktiven Zugriff.

[Automatisierung spielt auch eine Rolle bei der Bereitstellung vertrauenswürdiger Workloads](#), wie in [SEC06-BP02 Bereitstellung von Rechenleistung anhand gehärteter Images](#) und [06-BP04 Softwareintegrität überprüfen](#) beschrieben. [SEC](#) Sie können Dienste wie [EC2Image Builder](#), [AWS Signer](#)[AWS CodeArtifact](#), und [Amazon Elastic Container Registry \(ECR\)](#) verwenden, um gehärtete und genehmigte Images und Codeabhängigkeiten herunterzuladen, zu verifizieren, zu erstellen und zu speichern. Neben Inspector kann jeder von ihnen eine Rolle in Ihrem CI/CD-Prozess spielen, sodass Ihr Workload nur dann in die Produktion gelangt, wenn bestätigt wird, dass seine Abhängigkeiten vertrauenswürdig sind up-to-date und von vertrauenswürdigen Quellen stammen. Ihr Workload ist auch signiert, sodass AWS Rechenumgebungen wie [AWS Lambda](#)[Amazon Elastic Kubernetes Service \(EKS\)](#) überprüfen können, ob er nicht manipuliert wurde, bevor er ausgeführt werden kann.

Über diese präventiven Kontrollen hinaus können Sie die Automatisierung auch bei den detektivischen Kontrollen für Ihre Datenverarbeitungsressourcen einsetzen. Als Beispiel [AWS Security Hub](#) bietet der Standard [NIST800-53 Rev. 5](#), der Prüfungen wie [\[EC2.8\] beinhaltet, dass EC2 Instances Instance Metadata Service Version 2 \(\) verwenden sollten](#). [IMDSv2](#) [IMDSv2](#) verwendet

die Techniken der Sitzungsauthentifizierung, blockiert Anfragen, die einen X-Forwarded-For HTTP Header enthalten, und verwendet ein 1-Netzwerk, um den Datenverkehr zu unterbinden, TTL der aus externen Quellen stammt und Informationen über die Instanz abrufen. EC2 Diese Überprüfung im Security Hub kann erkennen, wann EC2 Instances automatische Problemlösungen verwenden, IMDSv1 und diese einleiten. Weitere Informationen zur automatisierten Erkennung und Problemlösung finden Sie unter [SEC04-BP04 Initiate Remediation](#) für Ressourcen, die nicht richtlinientreu sind.

## Implementierungsschritte

1. Automatisieren Sie die Erstellung sicherer, konformer und AMIs robuster Produkte mit [EC2Image Builder](#). Sie können anhand von Basis AWS - und APN Partnerimages Images erstellen, die Steuerelemente aus den Standards des Center for Internet Security (CIS) Benchmarks oder Security Technical Implementation Guide (STIG) enthalten.
2. Automatische Konfigurationsverwaltung. Erzwingen und validieren Sie sichere Konfigurationen in Ihren Datenverarbeitungsressourcen automatisch. Verwenden Sie dazu einen Service oder ein Tool zur Konfigurationsverwaltung.
  - a. Automatisiertes Konfigurationsmanagement mit [AWS Config](#)
  - b. Automatisiertes Sicherheits- und Compliance-Management mit [AWS Security Hub](#)
3. Automatisieren Sie das Patchen oder Ersetzen von Amazon Elastic Compute Cloud (AmazonEC2) -Instances. AWS Systems Manager Patch Manager automatisiert den Prozess des Patchens verwalteter Instanzen mit sicherheitsrelevanten und anderen Arten von Updates. Sie können Patchmanager verwenden, um Patches sowohl für Betriebssysteme als auch für Anwendungen durchzuführen.
  - a. [AWS Systems Manager Patch Manager](#)
4. Automatisieren Sie das Scannen von Rechenressourcen nach häufigen Sicherheitslücken und Sicherheitsrisiken (CVEs) und integrieren Sie Sicherheitsscanning-Lösungen in Ihre Build-Pipeline.
  - a. [Amazon Inspector](#)
  - b. [ECRScannen von Bildern](#)
5. Ziehen Sie Amazon GuardDuty für die automatische Erkennung von Malware und Bedrohungen zum Schutz von Rechenressourcen in Betracht. GuardDuty kann auch potenzielle Probleme identifizieren, wenn eine [AWS Lambda](#)Funktion in Ihrer AWS Umgebung aufgerufen wird.
  - a. [Amazon GuardDuty](#)
6. Ziehen Sie AWS Partnerlösungen in Betracht. AWS Partner bieten branchenführende Produkte an, die den vorhandenen Steuerungen in Ihren lokalen Umgebungen entsprechen, diese identisch sind

oder sich in diese integrieren lassen. Diese Produkte ergänzen die vorhandenen AWS -Services, sodass Sie eine umfassende Sicherheitsarchitektur bereitstellen und eine nahtlosere Erfahrung in Ihren Cloud- und On-Premises-Umgebungen ermöglichen können.

a. [Sicherheit der Infrastruktur](#)

## Ressourcen

Zugehörige bewährte Methoden:

- [SEC01-BP06 Automatisieren Sie die Implementierung von Standard-Sicherheitskontrollen](#)

Zugehörige Dokumente:

- [Nutzen Sie alle Vorteile Ihrer Infrastruktur IMDSv2 und deaktivieren Sie IMDSv1 in AWS](#)

Zugehörige Videos:

- [Bewährte Sicherheitsmethoden für den EC2 Amazon-Instance-Metadatenservice](#)

## Datenschutz

### Fragen

- [SEC7. Wie klassifizieren Sie Ihre Daten?](#)
- [SEC8 Wie werden Ihre Daten im Ruhezustand geschützt?](#)
- [SEC9. Wie werden Ihre Daten während der Übertragung geschützt?](#)

### SEC7. Wie klassifizieren Sie Ihre Daten?

Die Datenklassifizierung bietet eine Möglichkeit, Daten basierend auf Wichtigkeit und Sensibilität zu kategorisieren, um Ihnen dabei zu helfen, angemessene Schutz- und Aufbewahrungskontrollen zu bestimmen.

### Bewährte Methoden

- [SEC07-BP01 Verstehen Sie Ihr Datenklassifizierungsschema](#)
- [SEC07-BP02 Wenden Sie Datenschutzkontrollen auf der Grundlage der Datensensitivität an](#)

- [SEC07-BP03 Automatisieren Sie die Identifizierung und Klassifizierung](#)
- [SEC07-BP04 Definieren Sie skalierbares Datenlebenszyklusmanagement](#)

## SEC07-BP01 Verstehen Sie Ihr Datenklassifizierungsschema

Machen Sie sich ein Bild von der Klassifizierung der Daten, die Ihr Workload verarbeitet, den Anforderungen an die Verarbeitung, den damit verbundenen Geschäftsprozessen, dem Ort, an dem die Daten gespeichert sind, sowie dem Eigentümer der Daten. Ihr Schema für die Klassifizierung und den Umgang mit Daten sollte die geltenden rechtlichen und Compliance-Anforderungen Ihres Workloads und die erforderlichen Datenkontrollen berücksichtigen. Das Verständnis der Daten ist der erste Schritt zur Datenklassifizierung.

Gewünschtes Ergebnis: Die in Ihrem Workload vorhandenen Datentypen sind gut verstanden und dokumentiert. Es gibt angemessene Kontrollen zum Schutz sensibler Daten auf der Grundlage ihrer Klassifizierung. Diese Kontrollen regeln z. B., wer auf die Daten zugreifen darf und zu welchem Zweck, wo die Daten gespeichert werden, die Verschlüsselungsrichtlinie für diese Daten und wie Verschlüsselungsschlüssel verwaltet werden, den Lebenszyklus der Daten und die Anforderungen an die Aufbewahrung, angemessene Vernichtungsprozesse, welche Sicherungs- und Wiederherstellungsprozesse vorhanden sind und die Überprüfung des Zugriffs.

### Typische Anti-Muster:

- Fehlen einer formalen Richtlinie zur Datenklassifizierung, um die Sensibilitätsebenen und die Anforderungen an die Handhabung von Daten zu definieren
- Mangel an Wissen über die Sensibilitätsebenen der Daten innerhalb Ihres Workloads und fehlende Erfassung dieser Informationen in der Architektur- und Betriebsdokumentation
- Versäumnis, angemessene Kontrollen für Ihre Daten anzuwenden, die auf deren Sensibilität und Anforderungen basieren, wie in Ihrer Richtlinie zur Datenklassifizierung und -verarbeitung festgelegt
- Unterlassen von Feedback über die Anforderungen an die Datenklassifizierung und -verarbeitung an die Eigentümer der Richtlinien

Vorteile der Nutzung dieser bewährten Methode: Diese Vorgehensweise beseitigt Unklarheiten über den angemessenen Umgang mit Daten innerhalb Ihres Workloads. Die Anwendung einer formellen Richtlinie, die die Sensibilitätsebenen der Daten in Ihrer Organisation und die erforderlichen Schutzmaßnahmen definiert, kann Ihnen helfen, gesetzliche Vorschriften und andere

Bescheinigungen und Zertifizierungen im Bereich der Cybersicherheit einzuhalten. Besitzer von Workloads können sich darauf verlassen, dass sie wissen, wo sensible Daten gespeichert sind und welche Schutzkontrollen vorhanden sind. Wenn Sie diese in der Dokumentation festhalten, können neue Team-Mitglieder sie besser verstehen und schon früh in ihrer Amtszeit Kontrollen durchführen. Diese Praktiken können auch dazu beitragen, die Kosten zu senken, indem die Kontrollen für jede Art von Daten richtig dimensioniert werden.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Hoch

### Implementierungsleitfaden

Wenn Sie einen Workload entwerfen, überlegen Sie vielleicht intuitiv, wie Sie sensible Daten schützen können. Bei einer mandantenfähigen Anwendung ist es beispielsweise intuitiv, die Daten jedes Mandanten als sensibel zu betrachten und Schutzmaßnahmen zu ergreifen, damit ein Mandant nicht auf die Daten eines anderen Mandanten zugreifen kann. Ebenso können Sie intuitiv Zugriffskontrollen so gestalten, dass nur Administratoren Daten ändern können, während andere Benutzer nur Lesezugriff oder gar keinen Zugriff haben.

Indem Sie diese Datensensibilitätsebenen zusammen mit den entsprechenden Datenschutzerfordernungen definieren und in Richtlinien festhalten, können Sie formell feststellen, welche Daten sich in Ihrem Workload befinden. Sie können dann feststellen, ob die richtigen Kontrollen vorhanden sind, ob die Kontrollen überprüft werden können und welche Reaktionen angemessen sind, wenn ein falscher Umgang mit Daten festgestellt wird.

Um die Kategorisierung von sensiblen Daten innerhalb Ihres Workloads zu erleichtern, sollten Sie, sofern verfügbar, [Ressourcen-Tags](#) verwenden. Sie können beispielsweise ein Tag mit dem Tag-Schlüssel *Classification* und dem Tag-Wert *PHI* für geschützte Gesundheitsinformationen (PHI) und ein anderes Tag mit dem Tag-Schlüssel und dem Tag-Wert von *Sensitivity* anwenden. High Mit Services wie [AWS Config](#) können Sie diese Ressourcen auf Änderungen überwachen und eine Warnung ausgeben, wenn sie so verändert werden, dass sie Ihren Schutzanforderungen nicht mehr genügen (z. B. durch Änderung der Verschlüsselungseinstellungen). Sie können die Standarddefinition Ihrer Tag-Schlüssel und zulässigen Werte mit [Tag-Richtlinien](#), einem Feature von AWS Organizations, erfassen. Es wird nicht empfohlen, dass der Tag-Schlüssel oder -Wert *private* oder *sensible* Daten enthält.

### Implementierungsschritte

1. Verstehen Sie das Datenklassifizierungsschema und die Schutzanforderungen Ihrer Organisation.
2. Identifizieren Sie die Arten von sensiblen Daten, die von Ihren Workloads verarbeitet werden.

3. Vergewissern Sie sich, dass sensible Daten in Ihrem Workload gemäß Ihrer Richtlinie gespeichert und geschützt werden. Nutzen Sie Techniken wie automatisierte Tests, um die Wirksamkeit Ihrer Kontrollen zu überprüfen.
4. Erwägen Sie die Verwendung von Markierungen auf Ressourcen- und Datenebene, sofern verfügbar, um Daten mit ihrer Sensibilitätsstufe und anderen operativen Metadaten zu versehen, die bei der Überwachung und der Reaktion auf Vorfälle helfen können.
  - a. AWS Organizations Tag-Richtlinien können verwendet werden, um Tagging-Standards durchzusetzen.

## Ressourcen

Zugehörige bewährte Methoden:

- [SUS04-BP01 Implementieren Sie eine Datenklassifizierungsrichtlinie](#)

Zugehörige Dokumente:

- [Data Classification Whitepaper](#)
- [Bewährte Methoden für die Kennzeichnung von Ressourcen AWS](#)

Zugehörige Beispiele:

- [AWS Organizations Syntax und Beispiele für Tag-Richtlinien](#)

Zugehörige Tools:

- [AWS Tag-Editor](#)

SEC07-BP02 Wenden Sie Datenschutzkontrollen auf der Grundlage der Datensensitivität an

Wenden Sie Datenschutzkontrollen an, die ein angemessenes Maß an Kontrolle für jede in Ihrer Klassifizierungsrichtlinie definierte Datenklasse bieten. Auf diese Weise können Sie sensible Daten vor unbefugtem Zugriff und unbefugter Nutzung schützen und gleichzeitig die Verfügbarkeit und Nutzung der Daten aufrechterhalten.

Gewünschtes Ergebnis: Sie verfügen über eine Klassifizierungsrichtlinie, die die verschiedenen Sensibilitätsstufen für Daten in Ihrer Organisation definiert. Für jede dieser Sensibilitätsebenen



haben Sie klare Richtlinien für zugelassene Speicher- und Bearbeitungsservices und -orte sowie deren erforderliche Konfiguration veröffentlicht. Sie implementieren die Kontrollen für jede Ebene entsprechend dem erforderlichen Schutzniveau und den damit verbundenen Kosten. Sie verfügen über Überwachungs- und Warnsysteme, um zu erkennen, wenn sich Daten an nicht autorisierten Orten befinden, in nicht autorisierten Umgebungen verarbeitet werden, nicht autorisierte Akteure darauf zugreifen oder die Konfiguration der zugehörigen Services nicht mehr konform ist.

Typische Anti-Muster:

- Anwenden des gleichen Maßes an Schutzkontrollen für alle Daten: Dies kann dazu führen, dass zu viele Sicherheitskontrollen für wenig sensible Daten bereitgestellt werden oder hochsensible Daten nicht ausreichend geschützt werden.
- Unterlassen, die relevanten Stakeholder aus Sicherheits-, Compliance- und Geschäftsteams bei der Definition von Datenschutzkontrollen einzubeziehen
- Vernachlässigen des betrieblichen Aufwands und der Kosten, die mit der Implementierung und Pflege von Datenschutzkontrollen verbunden sind
- Fehlen von regelmäßigen Überprüfungen der Datenschutzkontrollen, um die Übereinstimmung mit den Klassifizierungsrichtlinien zu gewährleisten

Vorteile der Nutzung dieser bewährten Methode: Indem Sie Ihre Kontrollen auf die Klassifizierungsstufe Ihrer Daten abstimmen, kann Ihre Organisation bei Bedarf in höhere Kontrollstufen investieren. Dies kann eine Aufstockung der Ressourcen für die Sicherung, Überwachung, Messung, Behebung und Berichterstattung beinhalten. Wo weniger Kontrollen angebracht sind, können Sie die Zugänglichkeit und Vollständigkeit der Daten für Ihre Mitarbeiter, Kunden oder Wähler verbessern. Dieser Ansatz bietet Ihrer Organisation die größtmögliche Flexibilität bei der Datennutzung, während gleichzeitig die Datenschutzerfordernisse eingehalten werden.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Hoch

Implementierungsleitfaden

Die Implementierung von Datenschutzkontrollen auf der Grundlage von Datensensibilitätsebenen umfasst mehrere wichtige Schritte. Ermitteln Sie zunächst die verschiedenen Datensensibilitätsebenen innerhalb Ihrer Workload-Architektur (z. B. öffentlich, intern, vertraulich und eingeschränkt) und bewerten Sie, wo Sie diese Daten speichern und verarbeiten. Als Nächstes definieren Sie Isolationsgrenzen um die Daten herum, basierend auf ihrer Sensibilitätsebene.

Wir empfehlen Ihnen, Daten in verschiedene Bereiche aufzuteilen und dabei [Richtlinien zur Dienstkontrolle](#) (SCPs) zu verwenden AWS-Konten, um die für jede Datensensibilitätsstufe zulässigen Dienste und Aktionen einzuschränken. Auf diese Weise können Sie starke Isolationsgrenzen schaffen und das Prinzip der geringsten Berechtigung durchsetzen.

Nachdem Sie die Isolationsgrenzen definiert haben, implementieren Sie geeignete Schutzkontrollen auf der Grundlage der Sensibilitätsebenen der Daten. Beachten Sie die bewährten Methoden zum [Schutz von Daten im Ruhezustand](#) und zum [Schutz von Daten während der Übertragung](#), um entsprechende Kontrollen wie Verschlüsselung, Zugriffskontrollen und Audits zu implementieren. Ziehen Sie Techniken wie Tokenisierung oder Anonymisierung in Betracht, um die Sensibilität Ihrer Daten zu verringern. Vereinfachen Sie die Anwendung konsistenter Datenrichtlinien in Ihrem Unternehmen mit einem zentralisierten System für Tokenisierung und De-Tokenisierung.

Überwachen und testen Sie fortlaufend die Wirksamkeit der implementierten Kontrollen. Überprüfen und aktualisieren Sie das Datenklassifizierungsschema, die Risikobewertungen und die Schutzkontrollen regelmäßig, wenn sich die Datenlandschaft und die Bedrohungen in Ihrer Organisation weiterentwickeln. Richten Sie die implementierten Datenschutzkontrollen an den einschlägigen Branchenvorschriften, Standards und gesetzlichen Anforderungen aus. Sorgen Sie außerdem für ein Sicherheitsbewusstsein und bieten Sie Schulungen an, damit die Mitarbeiter das Datenklassifizierungsschema und ihre Verantwortung im Umgang mit sensiblen Daten und deren Schutz verstehen.

### Implementierungsschritte

1. Identifizieren Sie die Klassifizierungs- und Sensibilitätsstufen der Daten innerhalb Ihres Workloads.
2. Definieren Sie Isolationsgrenzen für jede Ebene und legen Sie eine Durchsetzungsstrategie fest.
3. Bewerten Sie die von Ihnen definierten Kontrollen, die den Zugriff, die Verschlüsselung, die Prüfung, die Aufbewahrung und andere von Ihrer Datenklassifizierungsrichtlinie geforderte Punkte regeln.
4. Prüfen Sie gegebenenfalls Optionen zur Verringerung der Sensibilität der Daten, z. B. durch Tokenisierung oder Anonymisierung.
5. Überprüfen Sie Ihre Kontrollen durch automatische Tests und die Überwachung Ihrer konfigurierten Ressourcen.

### Ressourcen

Zugehörige bewährte Methoden:

- [PERF03-BP01 Verwenden Sie einen speziell entwickelten Datenspeicher, der Ihre Datenzugriffs- und Speicheranforderungen am besten unterstützt](#)
- [COST04-BP05 Setzen Sie Richtlinien zur Datenspeicherung durch](#)

Zugehörige Dokumente:

- [Data Classification Whitepaper](#)
- [Bewährte Methoden für Sicherheit, Identität und Compliance](#)
- [AWS KMS Bewährte Methoden](#)
- [Bewährte Methoden und Funktionen für die Verschlüsselung von Diensten AWS](#)

Zugehörige Beispiele:

- [Building a serverless tokenization solution to mask sensitive data](#)
- [How to use tokenization to improve data security and reduce audit scope](#)

Zugehörige Tools:

- [AWS Key Management Service \(AWS KMS\)](#)
- [AWS CloudHSM](#)
- [AWS Organizations](#)

SEC07-BP03 Automatisieren Sie die Identifizierung und Klassifizierung

Durch die Automatisierung der Identifizierung und Klassifizierung von Daten können Sie die richtigen Kontrollen implementieren. Der Einsatz von Automatisierung als Ergänzung zur manuellen Ermittlung verringert das Risiko menschlicher Fehler und das Risiko einer Gefährdung.

Gewünschtes Ergebnis: Sie sind in der Lage zu überprüfen, ob die richtigen Kontrollen auf der Grundlage Ihrer Klassifizierungs- und Bearbeitungsrichtlinien vorhanden sind. Automatisierte Tools und Services helfen Ihnen bei der Identifizierung und Klassifizierung der Sensibilitätsebene Ihrer Daten. Die Automatisierung hilft Ihnen auch bei der kontinuierlichen Überwachung Ihrer Umgebungen, um zu erkennen und zu melden, wenn Daten auf unzulässige Weise gespeichert oder verarbeitet werden, sodass schnell Abhilfemaßnahmen ergriffen werden können.

Typische Anti-Muster:

- Vertrauen auf ausschließlich manuelle Prozesse, die fehleranfällig und zeitaufwendig sein können, um Daten zu identifizieren und zu klassifizieren. Dies kann zu einer ineffizienten und inkonsistenten Datenklassifizierung führen, insbesondere wenn das Datenvolumen wächst.
- Fehlen von Mechanismen zur Verfolgung und Verwaltung von Datenbeständen in der gesamten Organisation
- Vernachlässigen der Notwendigkeit einer kontinuierlichen Überwachung und Klassifizierung von Daten, während sie sich innerhalb der Organisation bewegen und weiterentwickeln

Vorteile der Nutzung dieser bewährten Methode: Die Automatisierung der Identifizierung und Klassifizierung von Daten kann zu einer konsistenteren und präziseren Anwendung von Datenschutzkontrollen führen und das Risiko menschlicher Fehler verringern. Die Automatisierung kann auch den Zugriff auf und die Bewegung von sensiblen Daten transparent machen, sodass Sie unautorisierten Umgang mit diesen Daten erkennen und Korrekturmaßnahmen ergreifen können.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel

#### Implementierungsleitfaden

Auch wenn die Klassifizierung von Daten in den ersten Entwurfsphasen eines Workloads häufig nach menschlichem Ermessen erfolgt, sollten Sie zur Vorbeugung Systeme einsetzen, die die Identifizierung und Klassifizierung von Testdaten automatisieren. Beispielsweise können Entwickler ein Tool oder einen Dienst erhalten, um repräsentative Daten zu scannen und ihre Sensibilität zu bestimmen. Darin AWS können Sie Datensätze in [Amazon S3 hochladen und sie mit Amazon Macie, Amazon](#) [Comprehend](#) oder [Amazon Comprehend](#) Medical scannen. Ziehen Sie auch in Betracht, Daten im Rahmen von Modultests und Integrationstests zu scannen, um festzustellen, wo sensible Daten nicht erwartet werden. Eine Warnung vor sensiblen Daten in dieser Phase kann vor der Bereitstellung in der Produktion auf Schutzlücken hinweisen. Andere Funktionen wie die Erkennung sensibler Daten in [AWS Glue](#) [Amazon](#) und [Amazon CloudWatch](#) können ebenfalls verwendet werden, um zu erkennen PII und Gegenmaßnahmen zu ergreifen. Verstehen Sie bei jedem automatisierten Tool oder Dienst, wie es sensible Daten definiert, und ergänzen Sie es mit anderen menschlichen oder automatisierten Lösungen, um eventuelle Lücken zu schließen.

Nutzen Sie die kontinuierliche Überwachung Ihrer Umgebungen als detektivische Kontrolle, um festzustellen, ob sensible Daten auf nicht konforme Weise gespeichert werden.

Dies kann dazu beitragen, Situationen zu erkennen, in denen sensible Daten ohne ordnungsgemäße De-Identifizierung oder Schwärzung in Protokolldateien ausgegeben oder in eine Datenanalyseumgebung kopiert werden. Daten, die in Amazon S3 gespeichert sind, können mit Amazon Macie kontinuierlich auf sensible Daten überwacht werden.

## Implementierungsschritte

1. Führen Sie einen ersten Scan Ihrer Umgebungen zur automatischen Identifizierung und Klassifizierung durch.
  - a. Ein erster vollständiger Scan Ihrer Daten kann dazu beitragen, ein umfassendes Verständnis darüber zu erlangen, wo sich sensible Daten in Ihren Umgebungen befinden. Wenn ein vollständiger Scan nicht erforderlich ist oder aus Kostengründen nicht im Voraus durchgeführt werden kann, sollten Sie prüfen, ob Stichprobenverfahren geeignet sind, um Ihre Ziele zu erreichen. Zum Beispiel kann Amazon Macie so konfiguriert werden, dass eine umfassende automatische Erkennung sensibler Daten in Ihren S3 Buckets durchgeführt wird. Diese Funktion nutzt Stichprobenverfahren, um kosteneffizient eine Vorabanalyse darüber durchzuführen, wo sensible Daten gespeichert sind. Eine tiefere Analyse von S3 Buckets kann dann mit einem Auftrag zur Erkennung sensibler Daten durchgeführt werden. Auch andere Datenspeicher können in S3 exportiert werden, um von Amazon Macie durchsucht zu werden.
2. Konfigurieren Sie laufende Scans Ihrer Umgebungen.
  - a. Die automatische Erkennungsfunktion für sensible Daten von Amazon Macie kann für laufende Scans Ihrer Umgebungen verwendet werden. Bekannte S3 Buckets, die für die Speicherung sensibler Daten autorisiert sind, können mit einer Zulassen-Liste in Amazon Macie ausgeschlossen werden.
3. Integrieren Sie die Identifizierung und Klassifizierung in Ihre Build- und Testprozesse.
  - a. Identifizieren Sie Tools, mit denen Entwickler Daten auf Sensibilität prüfen können, während Workloads entwickelt werden. Verwenden Sie diese Tools als Teil der Integrationstests, um bei unerwarteten sensiblen Daten Alarm zu schlagen und eine weitere Bereitstellung zu verhindern.
4. Implementieren Sie ein System oder Runbook, um Maßnahmen zu ergreifen, wenn sensible Daten an nicht autorisierten Orten gefunden werden.

## Ressourcen

### Zugehörige Dokumente:

- [AWS Glue: Detect and process sensitive data](#)
- [Verwendung verwalteter Datenkennungen in Amazon SNS](#)
- [Amazon CloudWatch Logs: Helfen Sie mit Maskierung, sensible Protokolldaten zu schützen](#)

## Zugehörige Beispiele:

- [Aktivierung der Datenklassifizierung für die RDS Amazon-Datenbank mit Macie](#)
- [Detecting sensitive data in DynamoDB with Macie](#)

## Zugehörige Tools:

- [Amazon Macie](#)
- [Amazon Comprehend](#)
- [Amazon Comprehend Medical](#)
- [AWS Glue](#)

## SEC07-BP04 Definieren Sie skalierbares Datenlebenszyklusmanagement

Machen Sie sich mit den Anforderungen an den Lebenszyklus Ihrer Daten in Bezug auf die verschiedenen Ebenen der Datenklassifizierung und -verarbeitung vertraut. Dazu kann gehören, wie Daten behandelt werden, wenn sie zum ersten Mal in Ihre Umgebung gelangen, wie Daten umgewandelt werden und welche Regeln für ihre Vernichtung gelten. Berücksichtigen Sie Faktoren wie Aufbewahrungsfristen, Zugriff, Prüfung und Nachvollziehbarkeit der Herkunft.

Gewünschtes Ergebnis: Sie klassifizieren die Daten so nah wie möglich an dem Punkt und dem Zeitpunkt der Datenerfassung. Wenn die Klassifizierung von Daten eine Maskierung, Tokenisierung oder andere Prozesse zur Verringerung der Sensibilitätsebene erfordert, führen Sie diese Aktionen so nah wie möglich am Zeitpunkt der Datenerfassung durch.

Sie löschen Daten in Übereinstimmung mit Ihrer Richtlinie, wenn sie aufgrund ihrer Klassifizierung nicht mehr aufbewahrt werden sollten.

## Typische Anti-Muster:

- Implementierung eines one-size-fits-all Ansatzes für das Datenlebenszyklusmanagement, ohne unterschiedliche Sensibilitätsstufen und Zugriffsanforderungen zu berücksichtigen.
- Beschränken der Betrachtung des Lebenszyklusmanagements auf entweder nutzbare Daten oder gesicherte Daten, statt auf beide
- Annehmen, dass Daten, die in Ihren Workload eingegeben wurden, gültig sind, ohne ihren Wert oder ihre Herkunft zu ermitteln
- Vertrauen auf die Haltbarkeit von Daten als Ersatz für Datensicherungen und -schutz

- Beibehalten von Daten über ihre Nützlichkeit und die erforderliche Aufbewahrungsfrist hinaus

Vorteile der Nutzung dieser bewährten Methode: Eine gut definierte und skalierbare Strategie für die Verwaltung des Lebenszyklus von Daten hilft bei der Einhaltung gesetzlicher Vorschriften, verbessert die Datensicherheit, optimiert die Speicherkosten und ermöglicht einen effizienten Datenzugriff und -austausch unter Beibehaltung angemessener Kontrollen.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Hoch

### Implementierungsleitfaden

Daten innerhalb eines Workloads sind oft dynamisch. Die Form, in der die Daten in Ihre Workload-Umgebung gelangen, kann sich von der Form unterscheiden, in der sie gespeichert oder in der Geschäftslogik, der Berichterstattung, der Analyse oder dem Machine Learning verwendet werden. Außerdem kann sich der Wert der Daten im Laufe der Zeit ändern. Einige Daten sind zeitlich begrenzt und verlieren an Wert, wenn sie älter werden. Überlegen Sie, wie sich diese Änderungen an Ihren Daten auf die Bewertung nach Ihrem Datenklassifizierungsschema und die damit verbundenen Kontrollen auswirken. Verwenden Sie nach Möglichkeit einen automatisierten Lebenszyklus-Mechanismus wie [Amazon S3-Lebenszyklus-Richtlinien](#) und [Amazon Data Lifecycle Manager](#), um Ihre Datenaufbewahrung, Archivierung und Ablaufprozesse zu konfigurieren.

Unterscheiden Sie zwischen Daten, die zur Verwendung zur Verfügung stehen, und Daten, die als Backup gespeichert sind. Erwägen Sie den Einsatz [AWS Backup](#), um die Sicherung von Daten über verschiedene AWS Dienste hinweg zu automatisieren. [EBSAmazon-Snapshots](#) bieten die Möglichkeit, ein EBS Volume zu kopieren und mithilfe von S3-Funktionen wie Lebenszyklus, Datenschutz und Zugriff auf Schutzmechanismen zu speichern. Zwei dieser Mechanismen sind [S3 Object Lock](#) und [AWS Backup Vault Lock](#), die Ihnen zusätzliche Sicherheit und Kontrolle über Ihre Backups bieten können. Verwalten Sie eine klare Aufgabentrennung und Zugriffsrechte für Backups. Isolieren Sie Backups auf Kontoebene, um während eines Ereignisses eine Trennung von der betroffenen Umgebung zu gewährleisten.

Ein weiterer Aspekt des Lifecycle-Managements ist die Aufzeichnung des Datenverlaufs, während diese Ihren Workload durchlaufen. Dies wird als Nachverfolgung der Datenherkunft bezeichnet. Dadurch können Sie sicher sein, dass Sie wissen, woher die Daten stammen, welche Transformationen durchgeführt wurden, welcher Eigentümer oder Prozess diese Änderungen vorgenommen hat und wann. Dieser Verlauf hilft bei der Fehlersuche und bei der Untersuchung möglicher Sicherheitsvorfälle. Sie können zum Beispiel Metadaten über Transformationen in einer [Amazon DynamoDB](#)-Tabelle protokollieren. Innerhalb eines Data Lake können Sie Kopien der

transformierten Daten in verschiedenen S3-Buckets für jede Stufe der Datenpipeline aufbewahren. Speichern Sie Schema- und Zeitstempelinformationen in einem [AWS Glue Data Catalog](#).

Unabhängig von Ihrer Lösung sollten Sie die Anforderungen Ihrer Endbenutzer berücksichtigen, um die geeigneten Tools für die Berichterstattung über die Herkunft Ihrer Daten zu bestimmen. So können Sie feststellen, wie Sie Ihre Herkunft am besten verfolgen können.

### Implementierungsschritte

1. Analysieren Sie die Datentypen, Sensibilitätsebenen und Zugriffsanforderungen des Workloads, um die Daten zu klassifizieren und geeignete Strategien für das Lebenszyklusmanagement zu definieren.
2. Entwerfen und implementieren Sie Richtlinien für die Datenaufbewahrung und automatisierte Vernichtungsprozesse, die mit den rechtlichen, regulatorischen und organisatorischen Anforderungen übereinstimmen.
3. Etablieren Sie Prozesse und Automatisierungen für die kontinuierliche Überwachung, Prüfung und Anpassung von Strategien, Kontrollen und Richtlinien für die Verwaltung des Datenlebenszyklus, wenn sich die Anforderungen an den Workload und die Vorschriften weiterentwickeln.

### Ressourcen

Zugehörige bewährte Methoden:

- [COST04-BP05 Richtlinien zur Datenspeicherung durchsetzen](#)
- [SUS04-BP03 Verwenden Sie Richtlinien, um den Lebenszyklus Ihrer Datensätze zu verwalten](#)

Zugehörige Dokumente:

- [Data Classification Whitepaper](#)
- [AWS Blueprint for Ransomware Defense](#)
- [DevOpsLeitfaden: Verbessern Sie die Rückverfolgbarkeit durch die Nachverfolgung der Datenherkunft](#)

Zugehörige Beispiele:

- [How to protect sensitive data for its entire lifecycle in AWS](#)
- [Erstellen Sie Data Lineage für Data Lakes mit AWS Glue Amazon Neptune und Spline](#)



## Zugehörige Tools:

- [AWS Backup](#)
- [Amazon Data Lifecycle Manager](#)
- [AWS Identity and Access Management Access Analyzer](#)

## SEC8 Wie werden Ihre Daten im Ruhezustand geschützt?

Schützen Sie Ihre Daten im Ruhezustand, indem Sie mehrere Kontrollen implementieren und so das Risiko eines unbefugten Zugriffs oder einer falschen Handhabung verringern.

### Bewährte Methoden

- [SEC08-BP01 Implementieren Sie eine sichere Schlüsselverwaltung](#)
- [SEC08-BP02 Verschlüsselung im Ruhezustand erzwingen](#)
- [SEC08-BP03 Automatisieren Sie den Schutz ruhender Daten](#)
- [SEC08-BP04 Zugriffskontrolle erzwingen](#)

### SEC08-BP01 Implementieren Sie eine sichere Schlüsselverwaltung

Eine sichere Schlüsselverwaltung umfasst die Speicherung, Rotation, Zugriffskontrolle und Überwachung von Schlüsseldaten, die zum Schutz von Daten im Ruhezustand für Ihre Workloads erforderlich sind.

Gewünschtes Ergebnis: Ein skalierbarer, wiederholbarer und automatisierter Schlüsselverwaltungsmechanismus. Der Mechanismus sollte es ermöglichen, Zugriff mit geringsten Berechtigungen auf Schlüsseldaten zu erzwingen, und er sollte das richtige Gleichgewicht zwischen Schlüsselverfügbarkeit, Vertraulichkeit und Integrität bieten. Der Zugriff auf Schlüssel sollte überwacht werden und Schlüsseldaten sollten mit einem automatisierten Prozess rotiert werden. Schlüsseldaten sollten niemals für menschliche Identitäten zugänglich sein.

### Typische Anti-Muster:

- Personen haben Zugriff auf unverschlüsselte Schlüsseldaten.
- Es werden benutzerdefinierte kryptografische Algorithmen erstellt.
- Die Berechtigungen für den Zugriff auf Schlüsseldaten sind zu weit gefasst.

Vorteile der Nutzung dieser bewährten Methode: Indem Sie einen sicheren Mechanismus für die Schlüsselverwaltung für Ihre Workload einrichten, können Sie dazu beitragen, Ihre Inhalte vor unbefugtem Zugriff zu schützen. Darüber hinaus müssen möglicherweise regulatorische Anforderungen hinsichtlich der Verschlüsselung Ihrer Daten erfüllt werden. Eine effektive Schlüsselverwaltungslösung kann technische Mechanismen bereitstellen, die diesen Vorschriften zum Schutz von Schlüsseldaten entsprechen.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Hoch

### Implementierungsleitfaden

Viele regulatorische Anforderungen und bewährte Methoden beinhalten die Verschlüsselung von Daten im Ruhezustand als grundlegende Sicherheitskontrolle. Um diese Bedingung zu erfüllen, benötigt Ihre Workload einen Mechanismus, mit dem Schlüsseldaten, die zur Verschlüsselung Ihrer Daten im Ruhezustand verwendet werden, sicher gespeichert und verwaltet werden können.

AWS bietet AWS Key Management Service (AWS KMS) zur dauerhaften, sicheren und redundanten Aufbewahrung von Schlüsseln. AWS KMS [Viele AWS Dienste lassen sich integrieren AWS KMS](#), um die Verschlüsselung Ihrer Daten zu unterstützen. AWS KMS verwendet FIPS 140-2 validierte Hardware-Sicherheitsmodule der Stufe 3 zum Schutz Ihrer Schlüssel. Es gibt keinen Mechanismus zum Exportieren von AWS KMS Schlüsseln im Klartext.

Bei der Bereitstellung von Workloads mit einer Strategie für mehrere Konten gilt es als [bewährte Methode](#), AWS KMS Schlüssel in demselben Konto zu speichern wie der Workload, der sie verwendet. In diesem verteilten Modell liegt die Verantwortung für die Verwaltung der AWS KMS Schlüssel beim Anwendungsteam. In anderen Anwendungsfällen können sich Unternehmen dafür entscheiden, AWS KMS Schlüssel in einem zentralen Konto zu speichern. Diese zentralisierte Struktur erfordert zusätzliche Richtlinien, um den kontoübergreifenden Zugriff zu ermöglichen, der benötigt wird, damit das Workload-Konto auf Schlüssel zugreifen kann, die im zentralen Konto gespeichert sind. Dieses Verfahren kann jedoch in Anwendungsfällen, in denen ein einzelner Schlüssel von mehreren AWS-Konten gemeinsam genutzt wird, besser geeignet sein.

Unabhängig davon, wo das Schlüsselmaterial gespeichert ist, sollte der Zugriff auf den Schlüssel mithilfe [wichtiger Richtlinien und IAM Richtlinien](#) streng kontrolliert werden. Schlüsselrichtlinien sind die wichtigste Methode, um den Zugriff auf einen AWS KMS Schlüssel zu kontrollieren. Darüber hinaus können AWS KMS Schlüsselzuschüsse den Zugriff auf AWS Dienste ermöglichen, mit denen Daten in Ihrem Namen ver- und entschlüsselt werden können. Nehmen Sie sich Zeit, um sich mit den [bewährten Methoden für die Zugriffskontrolle auf Ihre AWS KMS Schlüssel vertraut zu](#) machen.

Es hat sich bewährt, die Verwendung von Verschlüsselungsschlüsseln zu überwachen, um ungewöhnliche Zugriffsmuster zu erkennen. Vorgänge, die mit AWS verwalteten Schlüsseln und gespeicherten, vom Kunden verwalteten Schlüsseln ausgeführt werden, AWS KMS können angemeldet werden AWS CloudTrail und sollten regelmäßig überprüft werden. Besondere Aufmerksamkeit sollte dabei der Überwachung von Schlüsselzerstörungsereignissen gelten. Um die versehentliche oder böswillige Zerstörung von Schlüsseldaten zu verhindern, werden Schlüsseldaten bei Schlüsselzerstörungsereignissen nicht sofort gelöscht. Versuche, Schlüssel zu löschen, AWS KMS unterliegen einer [Wartezeit](#), die standardmäßig 30 Tage beträgt, sodass Administratoren Zeit haben, diese Aktionen zu überprüfen und die Anfrage gegebenenfalls rückgängig zu machen.

AWS KMS Bei den meisten AWS Diensten erfolgt die Nutzung auf eine für Sie transparente Weise. Sie müssen lediglich entscheiden, ob Sie einen AWS verwalteten oder einen vom Kunden verwalteten Schlüssel verwenden möchten. Wenn Ihr Workload die direkte Verwendung von AWS KMS zum Verschlüsseln oder Entschlüsseln von Daten erfordert, empfiehlt es sich, zum Schutz Ihrer Daten die [Umschlagverschlüsselung](#) zu verwenden. Die [AWS Verschlüsselung SDK](#) kann Ihren Anwendungen clientseitige Verschlüsselungsprimitive zur Implementierung der Umschlagverschlüsselung und Integration zur Verfügung stellen. AWS KMS

## Implementierungsschritte

1. Ermitteln Sie die geeigneten [Schlüsselverwaltungsoptionen](#) (AWS verwaltet oder vom Kunden verwaltet) für den Schlüssel.
  - AWS Bietet aus Gründen der Benutzerfreundlichkeit AWS eigene und AWS verwaltete Schlüssel für die meisten Dienste, sodass encryption-at-rest Funktionen bereitgestellt werden können, ohne dass wichtige Materialien oder wichtige Richtlinien verwaltet werden müssen.
  - Wenn Sie kundenseitig verwaltete Schlüssel verwenden, sollten Sie den Standard-Schlüsselspeicher in Betracht ziehen, um das beste Gleichgewicht zwischen Agilität, Sicherheit, Datenhoheit und Verfügbarkeit zu erzielen. Andere Anwendungsfälle erfordern möglicherweise die Verwendung von benutzerdefinierten Schlüsselspeichern mit [AWS CloudHSM](#) oder mit dem [externen Schlüsselspeicher](#).
2. Sehen Sie sich die Liste der Dienste an, die Sie für Ihren Workload verwenden, um zu verstehen, wie sie AWS KMS sich in den Service integrieren lassen. EC2Instances können beispielsweise verschlüsselte EBS Volumes verwenden, um zu überprüfen, ob EBS Amazon-Snapshots, die aus diesen Volumes erstellt wurden, auch mit einem vom Kunden verwalteten Schlüssel verschlüsselt sind, und um die versehentliche Offenlegung unverschlüsselter Snapshot-Daten zu verhindern.
  - [Wie nutzen Dienste AWSAWS KMS](#)

- Ausführliche Informationen zu den Verschlüsselungsoptionen, die ein AWS Dienst bietet, finden Sie unter dem Thema Verschlüsselung im Ruhezustand im Benutzer- oder Entwicklerhandbuch für den Dienst.
3. Implementieren AWS KMS: AWS KMS macht es Ihnen einfach, Schlüssel zu erstellen und zu verwalten und die Verwendung von Verschlüsselung für eine Vielzahl von AWS Diensten und in Ihren Anwendungen zu kontrollieren.
    - [Erste Schritte: AWS Key Management Service \(AWS KMS\)](#)
    - Informieren Sie sich über die [bewährten Methoden für die Zugriffskontrolle auf Ihre AWS KMS Schlüssel](#).
  4. Bedenken Sie AWS Encryption SDK: Verwenden Sie die AWS Encryption SDK AWS KMS With-Integration, wenn Ihre Anwendung Daten clientseitig verschlüsseln muss.
    - [AWS Encryption SDK](#)
  5. Aktivieren Sie [IAMAccess Analyzer](#), um die wichtigsten Richtlinien automatisch zu überprüfen und zu benachrichtigen, wenn sie zu weit gefasst sind. AWS KMS
  6. Aktivieren Sie [Security Hub](#), um Benachrichtigungen zu erhalten, wenn falsch konfigurierte Schlüsselrichtlinien, Schlüssel mit geplanter Löschung oder Schlüssel ohne aktivierte automatische Rotation vorhanden sind.
  7. Ermitteln Sie die für Ihre AWS KMS Schlüssel geeignete Protokollierungsebene. Da Aufrufe von AWS KMS, einschließlich schreibgeschützter Ereignisse, protokolliert werden, AWS KMS können die zugehörigen CloudTrail Protokolle sehr umfangreich werden.
    - Einige Organisationen ziehen es vor, die AWS KMS Protokollierungsaktivitäten in einem separaten Protokoll zu unterteilen. Weitere Informationen finden Sie im CloudTrail Abschnitt [AWS KMS APIAnrufe protokollieren mit](#) im AWS KMS Entwicklerhandbuch.

## Ressourcen

### Zugehörige Dokumente:

- [AWS Key Management Service](#)
- [Kryptografische AWS -Services und -Tools](#)
- [Schützen von Amazon-S3-Daten durch Verschlüsselung](#)
- [Umschlagverschlüsselung](#)
- [Das Versprechen zu digitaler Souveränität](#)

- [Das Geheimnis von AWS KMS -Schlüsselvorgängen, Bring Your Own Key, benutzerdefiniertem Schlüsselspeicher und Portabilität von Geheimtext](#)
- [AWS Key Management Service kryptografische Details](#)

Zugehörige Videos:

- [Wie funktioniert Verschlüsselung in AWS](#)
- [Sicherung Ihres Blockspeichers auf AWS](#)
- [Datenschutz in AWS : Verwenden von Schlössern, Schlüsseln, Signaturen und Zertifikaten](#)

Zugehörige Beispiele:

- [Implementieren Sie erweiterte Zugriffskontrollmechanismen mit AWS KMS](#)

#### SEC08-BP02 Verschlüsselung im Ruhezustand erzwingen

Sie sollten die Verwendung der Verschlüsselung von Daten im Ruhezustand erzwingen. Durch die Verschlüsselung wird die Vertraulichkeit sensibler Daten im Falle eines unautorisierten Zugriffs oder einer unbeabsichtigten Offenlegung gewahrt.

Gewünschtes Ergebnis: Private Daten sollten standardmäßig im Ruhezustand verschlüsselt werden. Die Verschlüsselung wahrt die Vertraulichkeit der Daten und bietet eine zusätzliche Schutzebene gegen beabsichtigte oder unbeabsichtigte Datenoffenlegung oder Exfiltration. Verschlüsselte Daten können ohne vorherige Entschlüsselung nicht gelesen oder genutzt werden. Alle unverschlüsselt gespeicherten Daten sollten inventarisiert und kontrolliert werden.

Typische Anti-Muster:

- Konfigurationen werden nicht verwendet. encrypt-by-default
- Bereitstellung von Zugriffsmöglichkeiten mit zu vielen Berechtigungen für Entschlüsselungsschlüssel
- fehlende Überwachung der Ver- und Entschlüsselungsschlüssel
- Speichern von Daten ohne Verschlüsselung
- Verwendung desselben Verschlüsselungsschlüssels für alle Daten, ohne Berücksichtigung von Datennutzung, Typen und Klassifizierung

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Hoch

## Implementierungsleitfaden

Ordnen Sie Datenklassifizierungen in Ihren Workloads Verschlüsselungsschlüssel zu. Dieser Ansatz schützt vor Zugriff mit zu vielen Berechtigungen, wenn Sie entweder einen einzelnen Zugriffsschlüssel oder eine sehr kleine Anzahl von Verschlüsselungsschlüsseln für Ihre Daten verwenden (siehe [SEC07-BP01 Verstehen Sie Ihr Datenklassifizierungsschema](#)).

AWS Key Management Service (AWS KMS) lässt sich in viele AWS Dienste integrieren, um die Verschlüsselung Ihrer Daten im Ruhezustand zu vereinfachen. In Amazon Simple Storage Service (Amazon S3) können Sie beispielsweise die [Standardverschlüsselung](#) für einen Bucket festlegen, sodass neue Objekte automatisch verschlüsselt werden. Beachten Sie bei der Verwendung AWS KMS, wie stark die Daten eingeschränkt werden müssen. Standard- und dienstgesteuerte AWS KMS Schlüssel werden in Ihrem Namen von AWS verwaltet und verwendet. Bei sensiblen Daten, die einen detaillierten Zugriff auf den zugrunde liegenden Verschlüsselungsschlüssel erfordern, sollten Sie vom Kunden verwaltete Schlüssel ( ) in Betracht ziehen. CMKs Mithilfe von Schlüsselrichtlinien haben Sie die volle Kontrolle über CMKs die Rotation und die Zugriffsverwaltung.

Darüber hinaus unterstützen [Amazon Elastic Compute Cloud \(AmazonEC2\)](#) und [Amazon S3](#) die Durchsetzung der Verschlüsselung, indem sie die Standardverschlüsselung festlegen. Sie können [AWS-Config-Regel](#)ndamit automatisch überprüfen, ob Sie Verschlüsselung verwenden, z. B. für [Amazon Elastic Block Store \(AmazonEBS\) -Volumes](#), [Amazon Relational Database Service \(AmazonRDS\) -Instances](#) und [Amazon S3 S3-Buckets](#).

AWS bietet auch Optionen für die clientseitige Verschlüsselung, sodass Sie Daten verschlüsseln können, bevor Sie sie in die Cloud hochladen. [Das AWS Encryption SDK bietet eine Möglichkeit, Ihre Daten mithilfe der Umschlagverschlüsselung zu verschlüsseln](#). Sie geben den Umschließungsschlüssel an und der AWS Encryption SDK generiert einen eindeutigen Datenschlüssel für jedes Datenobjekt, das er verschlüsselt. Überlegen Sie AWS CloudHSM , ob Sie ein verwaltetes Hardware-Sicherheitsmodul für einen Mandanten benötigen ( )HSM. AWS CloudHSM ermöglicht Ihnen die Generierung, den Import und die Verwaltung kryptografischer Schlüssel auf einem FIPS 140-2-validierten Level 3-Standard. HSM Zu den Anwendungsfällen AWS CloudHSM gehören der Schutz privater Schlüssel für die Ausstellung einer Zertifizierungsstelle (CA) und die Aktivierung der transparenten Datenverschlüsselung (TDE) für Oracle-Datenbanken. Der AWS CloudHSM Client SDK bietet Software, mit der Sie Daten clientseitig mit Schlüsseln verschlüsseln können, die im Client gespeichert sind, AWS CloudHSM bevor Sie Ihre Daten hochladen. AWS Der Amazon DynamoDB Encryption Client ermöglicht darüber hinaus das Verschlüsseln und Signieren von Elementen vor dem Laden in eine DynamoDB-Tabelle.

## Implementierungsschritte

- Erzwingen der Verschlüsselung im Ruhezustand für Amazon S3: Implementieren Sie die [Standardverschlüsselung für einen Amazon-S3-Bucket](#).

[Standardverschlüsselung für neue EBS Amazon-Volumes](#) konfigurieren: Geben Sie an, dass alle neu erstellten EBS Amazon-Volumes in verschlüsselter Form erstellt werden sollen, mit der Option, den von bereitgestellten Standardschlüssel AWS oder einen von Ihnen erstellten Schlüssel zu verwenden.

Verschlüsselte Amazon Machine Images konfigurieren (AMIs): Beim Kopieren eines vorhandenen Images AMI mit konfigurierter Verschlüsselung werden Root-Volumes und Snapshots automatisch verschlüsselt.

[RDSAmazon-Verschlüsselung](#) konfigurieren: Konfigurieren Sie die Verschlüsselung für Ihre RDS Amazon-Datenbank-Cluster und Snapshots im Ruhezustand mithilfe der Verschlüsselungsoption.

Erstellen und konfigurieren Sie AWS KMS Schlüssel mit Richtlinien, die den Zugriff auf die entsprechenden Prinzipale für jede Datenklassifizierung einschränken: Erstellen Sie beispielsweise einen AWS KMS Schlüssel für die Verschlüsselung von Produktionsdaten und einen anderen Schlüssel für die Verschlüsselung von Entwicklungs- oder Testdaten. Sie können anderen auch Schlüsselzugriff gewähren. AWS-Konten Ziehen Sie die Nutzung verschiedener Konten für Ihre Entwicklungs- und Produktionsumgebungen in Betracht. Wenn Ihre Produktionsumgebung Artefakte im Entwicklungskonto entschlüsseln muss, können Sie die zum Verschlüsseln der Entwicklungsartefakte verwendete CMK Richtlinie so bearbeiten, dass das Produktionskonto diese Artefakte entschlüsseln kann. Die Produktionsumgebung kann dann die entschlüsselten Daten zur Verwendung in der Produktion einlesen.

Konfigurieren Sie die Verschlüsselung in zusätzlichen AWS Diensten: Lesen Sie für andere AWS Dienste, die Sie verwenden, in der [Sicherheitsdokumentation](#) für diesen Dienst nach, um die Verschlüsselungsoptionen des Dienstes zu ermitteln.

## Ressourcen

### Zugehörige Dokumente:

- [AWS Crypto Tools](#)
- [AWS Encryption SDK](#)
- [AWS KMS Whitepaper zu kryptografischen Details](#)

- [AWS Key Management Service](#)
- [Kryptografische AWS -Services und -Tools](#)
- [EBSAmazon-Verschlüsselung](#)
- [Standardverschlüsselung für EBS Amazon-Volumes](#)
- [RDSAmazon-Ressourcen verschlüsseln](#)
- [Wie aktiviere ich die Standardverschlüsselung für einen Amazon-S3-Bucket?](#)
- [Schützen von Amazon-S3-Daten durch Verschlüsselung](#)

Zugehörige Videos:

- [Wie funktioniert Verschlüsselung in AWS](#)
- [Sicherung Ihres Blockspeichers auf AWS](#)

SEC08-BP03 Automatisieren Sie den Schutz ruhender Daten

Nutzen Sie Automatisierung, um Daten im Ruhezustand zu validieren und zu kontrollieren. Nutzen Sie automatisierte Scans, um Fehlkonfigurationen Ihrer Datenspeicherlösungen zu erkennen, und führen Sie, wenn möglich, Abhilfemaßnahmen durch automatisierte programmatische Reaktionen durch. Integrieren Sie Automatisierung in Ihre CI/CD-Prozesse, um Fehlkonfigurationen des Datenspeichers zu erkennen, bevor sie in der Produktion bereitgestellt werden.

Gewünschtes Ergebnis: Automatisierte Systeme scannen und überwachen Datenspeicherorte auf falsch konfigurierte Steuerungen, unbefugten Zugriff und unerwartete Nutzung. Bei Erkennung falsch konfigurierter Speicherorte werden automatische Abhilfemaßnahmen initiiert. Automatisierte Prozesse erstellen Daten-Backups und speichern unveränderliche Kopien außerhalb der ursprünglichen Umgebung.

Typische Anti-Muster:

- Keine Berücksichtigung von Optionen zur Aktivierung der Verschlüsselung in den Standardeinstellungen, sofern unterstützt.
- Keine Berücksichtigung von Sicherheitsereignissen neben den betrieblichen Ereignissen bei der Formulierung einer automatisierten Backup- und Wiederherstellungsstrategie.
- Keine Erzwingung der Einstellungen für den öffentlichen Zugriff auf Speicher-Services.
- Keine Überwachung und Prüfung Ihrer Kontrollen zum Schutz von Daten im Ruhezustand.



Vorteile der Nutzung dieser bewährten Methode: Die Automatisierung trägt dazu bei, das Risiko falsch konfigurierter Datenspeicherorte zu vermeiden. Dadurch wird verhindert, dass Fehlkonfigurationen in Ihre Produktionsumgebungen gelangen. Diese bewährte Methode trägt außerdem dazu bei, gegebenenfalls vorhandene Fehlkonfigurationen zu erkennen und zu beheben.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel

### Implementierungsleitfaden

Die Automatisierung zieht sich wie ein roter Faden durch die Praktiken zum Schutz Ihrer Daten im Ruhezustand. [SEC01-BP06 Automatisierte Bereitstellung von Standardsicherheitskontrollen](#) beschreibt, wie Sie die Konfiguration Ihrer Ressourcen mithilfe von Infrastructure-as-Code-Vorlagen (IaC) erfassen können, z. B. mit [AWS CloudFormation](#). Diese Vorlagen sind an ein Versionskontrollsystem gebunden und werden verwendet, um Ressourcen AWS über eine CI/CD-Pipeline bereitzustellen. Diese Techniken gelten auch für die Automatisierung der Konfiguration Ihrer Datenspeicherlösungen (zum Beispiel für Verschlüsselungseinstellungen für Amazon-S3-Buckets).

Sie können die Einstellungen, die Sie in Ihren IaC-Vorlagen definieren, mithilfe von Regeln in [AWS CloudFormation Guard](#) auf Fehlkonfigurationen in Ihren CI/CD-Pipelines überprüfen. Sie können Einstellungen, die in CloudFormation oder anderen IaC-Tools noch nicht verfügbar sind, auf Fehlkonfigurationen mit überwachen. [AWS Config](#) Warnmeldungen, die Config für Fehlkonfigurationen generiert, können automatisch behoben werden, wie in [SEC04-BP04 Behebung für nicht konforme Ressourcen einleiten](#) beschrieben.

Der Einsatz von Automatisierung als Teil Ihrer Strategie zur Verwaltung von Berechtigungen ist ebenfalls ein wesentlicher Bestandteil des automatisierten Datenschutzes. [SEC03-BP02 Zugriff mit geringsten Rechten gewähren](#) und [SEC03-BP04 Berechtigungen kontinuierlich reduzieren beschreiben die Konfiguration von Richtlinien für den Zugriff mit den geringsten Rechten, die kontinuierlich](#) von der überwacht werden, um zu ermitteln, wann Berechtigungen eingeschränkt werden können. [AWS Identity and Access Management Access Analyzer](#) Neben der Automatisierung von Überwachungsberechtigungen können Sie [Amazon](#) so konfigurieren, GuardDuty dass es auf ungewöhnliches Datenzugriffsverhalten für Ihre [EBSVolumes](#) (über eine EC2 Instance), [S3-Buckets](#) und unterstützte [Amazon Relational Database Service](#) Service-Datenbanken achtet.

Automatisierung spielt auch eine Rolle bei der Erkennung, ob sensible Daten an nicht autorisierten Orten gespeichert sind. [SEC07-BP03 Automatisierte Identifizierung und Klassifizierung](#) beschreibt, wie [Amazon Macie](#) Ihre S3-Buckets auf unerwartete sensible Daten überwachen und Warnmeldungen generieren kann, die eine automatisierte Reaktion auslösen können.

Folgen Sie den Anleitungen unter [REL09 Daten sichern, um eine automatisierte Datensicherungs- und Wiederherstellungsstrategie zu entwickeln](#). Datensicherung und -wiederherstellung sind für die Wiederherstellung nach Sicherheitsereignissen ebenso wichtig wie für betriebliche Ereignisse.

### Implementierungsschritte

1. Erfassen Sie die Datenspeicherkonfiguration in IaC-Vorlagen. Verwenden Sie automatische Prüfungen in Ihren CI/CD-Pipelines, um Fehlkonfigurationen zu erkennen.
  - a. Sie können es für Ihre IaC-Vorlagen und [CloudFormationGuard](#) verwenden, um Vorlagen auf Fehlkonfigurationen zu überprüfen.
  - b. Verwenden Sie [AWS Config](#), um Regeln in einem proaktiven Auswertungsmodus auszuführen. Verwenden Sie diese Einstellung, um die Konformität einer Ressource vor der Erstellung als Schritt in Ihrer CI/CD-Pipeline zu prüfen.
2. Überwachen Sie Ressourcen auf Fehlkonfigurationen des Datenspeichers.
  - a. Konfigurieren Sie [AWS Config](#) so, dass Datenspeicherressourcen auf Änderungen der Kontrollkonfigurationen überwacht und Warnungen generiert werden, um Abhilfemaßnahmen aufzurufen, wenn eine Fehlkonfiguration erkannt wird.
  - b. Weitere Hinweise zu [SECautomatisierten Problembehebungen finden Sie unter 04-BP04 Problembehebung für Ressourcen initiieren, die nicht den Vorschriften entsprechen](#).
3. Überwachen und reduzieren Sie die Datenzugriffsberechtigungen kontinuierlich durch Automatisierung.
  - a. [IAMAccess Analyzer](#) kann kontinuierlich ausgeführt werden, um Warnmeldungen zu generieren, wenn Berechtigungen möglicherweise eingeschränkt werden können.
4. Überwachen Sie anomales Datenzugriffsverhalten und geben Sie entsprechende Warnungen aus.
  - a. [GuardDuty](#) überwacht sowohl bekannte Bedrohungssignaturen als auch Abweichungen vom grundlegenden Zugriffsverhalten für Datenspeicherressourcen wie EBS Volumes, S3-Buckets und RDS Datenbanken.
5. Überwachen Sie sensible Daten, die an unerwarteten Orten gespeichert sind, und geben Sie entsprechende Warnungen aus.
  - a. Verwenden Sie [Amazon Macie](#), um Ihre S3-Buckets kontinuierlich auf sensible Daten zu überprüfen.
6. Automatisieren Sie sichere und verschlüsselte Backups Ihrer Daten.
  - a. [AWS Backup](#) ist ein verwalteter Dienst, der verschlüsselte und sichere Backups verschiedener Datenquellen erstellt. AWS [Elastic Disaster Recovery](#) ermöglicht es Ihnen, komplette Server-Workloads zu kopieren und einen kontinuierlichen Datenschutz mit einem in Sekunden

gemessenen Recovery Point Objective (RPO) aufrechtzuerhalten. Sie können beide Services so konfigurieren, dass sie zusammenarbeiten, um die Erstellung von Daten-Backups und das Kopieren der Daten an Failover-Standorte zu automatisieren. Dies kann dazu beitragen, dass Ihre Daten auch dann verfügbar bleiben, wenn sie durch betriebliche oder sicherheitsrelevante Ereignisse beeinträchtigt werden.

## Ressourcen

### Zugehörige bewährte Methoden:

- [SEC01-BP06 Automatisieren Sie die Implementierung von Standard-Sicherheitskontrollen](#)
- [SEC03-BP02 Gewähren Sie den Zugriff mit den geringsten Rechten](#)
- [SEC03-BP04 Reduzieren Sie die Berechtigungen kontinuierlich](#)
- [SEC04-BP04 Initiieren Sie die Behebung nicht richtlinienkonformer Ressourcen](#)
- [SEC07-BP03 Automatisieren Sie die Identifizierung und Klassifizierung](#)
- [REL09-BP02 Backups sichern und verschlüsseln](#)
- [REL09-BP03 Führen Sie die Datensicherung automatisch durch](#)

### Zugehörige Dokumente:

- [AWS Präskriptive Anleitung: Automatisches Verschlüsseln vorhandener und neuer Amazon-Volumes EBS](#)
- [Ransomware-Risikomanagement bei der AWS Verwendung des NIST Cyber Security Frameworks \(CSF\)](#)

### Zugehörige Beispiele:

- [Wie kann man AWS Config proaktive Regeln und AWS CloudFormation Hooks einsetzen, um die Erstellung nicht richtlinienkonformer Cloud-Ressourcen zu verhindern](#)
- [Automatisieren und verwalten Sie den Datenschutz für Amazon S3 zentral mit AWS Backup](#)
- [AWS re:Invent 2023 — Implementieren Sie proaktiven Datenschutz mithilfe von Amazon-Snapshots EBS](#)
- [AWS re:Invent 2022 – Entwickeln und Automatisieren für Ausfallsicherheit mit modernem Datenschutz](#)

## Zugehörige Tools:

- [AWS CloudFormation Guard](#)
- [AWS CloudFormation Guard Registrierung von Regeln](#)
- [IAM Access Analyzer](#)
- [Amazon Macie](#)
- [AWS Backup](#)
- [Elastic Disaster Recovery](#)

## SEC08-BP04 Zugriffskontrolle erzwingen

Um Ihre Daten im Ruhezustand zu schützen, sollten Sie Zugriffskontrollen über Mechanismen wie Isolierung und Versionsverwaltung erzwingen und das Prinzip der geringsten Berechtigung anwenden. Verhindern Sie den öffentlichen Zugriff auf Ihre Daten.

Gewünschtes Ergebnis: Stellen Sie sicher, dass nur autorisierte Benutzer auf bestimmte Daten zugreifen können. need-to-know Schützen Sie Ihre Daten mit regelmäßigen Backups und Versionsverwaltung vor beabsichtigten oder unbeabsichtigten Änderungen oder Löschungen. Isolieren Sie wichtige Daten von anderen Daten, um deren Vertraulichkeit und Datenintegrität zu gewährleisten.

### Typische Anti-Muster:

- gemeinsame Speicherung von Daten mit unterschiedlichen Anforderungen hinsichtlich Vertraulichkeit oder verschiedenen Klassifizierungen
- Verwendung von übermäßigen Berechtigungen für Entschlüsselungsschlüssel
- nicht ordnungsgemäße Klassifizierung von Daten
- keine Aufbewahrung von Backups wichtiger Daten
- Gewährung von dauerhaftem Zugriff auf Produktionsdaten
- keine Prüfung des Datenzugriffs bzw. keine regelmäßige Prüfung der Berechtigungen

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Niedrig

### Implementierungsleitfaden

Mehrere Kontrollen können zum Schutz Ihrer Daten im Ruhezustand beitragen. Diese umfassen Zugriff (unter Verwendung des Prinzips der geringsten Berechtigung), Isolierung und

Versionsverwaltung. Der Zugriff auf Ihre Daten sollte mithilfe von Erkennungsmechanismen wie, und Service Level Logs AWS CloudTrail, wie Amazon Simple Storage Service (Amazon S3) - Zugriffsprotokollen, geprüft werden. Sie sollten inventarisieren, welche Daten öffentlich zugänglich sind, und einen Plan erstellen, wie Sie die Menge an öffentlich verfügbaren Daten im Laufe der Zeit reduzieren können.

Amazon S3 Glacier Vault Lock and Amazon S3 Object Lock bieten eine obligatorische Zugriffskontrolle für Objekte in Amazon S3. Sobald eine Tresorrichtlinie mit der Compliance-Option gesperrt wurde, kann sie bis zum Ablauf der Sperre selbst vom Root-Benutzer nicht mehr geändert werden.

### Implementierungsschritte

- Erzwingen der Zugriffskontrolle: Erzwingen Sie die Zugriffskontrolle nach dem Prinzip der geringsten Berechtigung, einschließlich des Zugriffs auf Verschlüsselungsschlüssel.
- Trennen von Daten anhand unterschiedlicher Klassifizierungsstufen: Verwenden Sie unterschiedliche AWS-Konten für Datenklassifizierungsstufen und verwalten Sie diese Konten mithilfe von [AWS Organizations](#).
- Richtlinien überprüfen AWS Key Management Service (AWS KMS): [Überprüfen Sie die in den AWS KMS Richtlinien gewährte Zugriffsebene](#).
- Überprüfen der Berechtigungen für Amazon-S3-Buckets und -Objekte: Überprüfen Sie regelmäßig den in S3-Bucket-Richtlinien gewährten Zugriff. Als bewährte Methode gilt, über keine öffentlich lesbaren oder schreibbaren Buckets zu verfügen. Erwägen Sie [AWS Config](#) die Verwendung zur Erkennung von Buckets, die öffentlich verfügbar sind, und Amazon CloudFront zur Bereitstellung von Inhalten aus Amazon S3. Vergewissern Sie sich, dass Buckets, die keinen öffentlichen Zugriff gewähren sollen, so konfiguriert sind, dass öffentliche Zugriffe verhindert werden. Standardmäßig sind alle S3-Buckets privat. Der Zugriff ist nur für Benutzer möglich, denen ausdrücklich Zugriff gewährt wurde.
- [AWS IAMAccess Analyzer](#) verwenden: IAM Access Analyzer analysiert Amazon S3 S3-Buckets und generiert einen Befund, wenn [eine S3-Richtlinie Zugriff auf eine externe Entität gewährt](#).
- Verwenden von [Amazon-S3-Versionsverwaltung](#) und [Objektsperre](#), sofern angemessen.
- Verwenden von [Amazon S3 Inventory](#): Amazon S3 Inventory kann verwendet werden, um den Replikations- und Verschlüsselungsstatus Ihrer S3-Objekte zu prüfen und zu melden.
- Überprüfen Sie die [Amazon EBS](#) - und [AMIFreigabeberechtigungen](#): Mit Freigabeberechtigungen können Sie Bilder und Volumes teilen AWS-Konten, die nicht zu Ihrem Workload gehören.

- Regelmäßiges Überprüfen der Freigaben von [AWS Resource Access Manager](#), um zu bestimmen, ob Ressourcen weiterhin freigegeben werden sollten. Resource Access Manager ermöglicht es Ihnen, Ressourcen wie AWS Netzwerk-Firewall-Richtlinien, Amazon Route 53-Resolver-Regeln und Subnetze innerhalb Ihres Amazon gemeinsam zu nutzen. VPCs Überprüfen Sie die freigegebenen Ressourcen regelmäßig und beenden Sie die Freigabe von Ressourcen, die keine Freigabe mehr erfordern.

## Ressourcen

### Zugehörige bewährte Methoden:

- [SEC03-BP01 Zugangsvoraussetzungen definieren](#)
- [SEC03-BP02 Least-Privilege-Zugriff gewähren](#)

### Zugehörige Dokumente:

- [AWS KMS Whitepaper zu kryptografischen Details](#)
- [Einführung in die Verwaltung von Zugriffsberechtigungen für Ihre Amazon-S3-Ressourcen](#)
- [Überblick über die Verwaltung des Zugriffs auf Ihre Ressourcen AWS KMS](#)
- [AWS-Config-Regeln](#)
- [Amazon S3 + Amazon CloudFront: Eine Kombination aus der Cloud](#)
- [Verwenden der Versionsverwaltung](#)
- [Sperren von Objekten mithilfe von Amazon S3 Object Lock](#)
- [Einen EBS Amazon-Snapshot teilen](#)
- [Geteilt AMIs](#)
- [Hosten einer Single-Page-Anwendung auf Amazon S3](#)

### Zugehörige Videos:

- [Sicherung Ihres Blockspeichers auf AWS](#)

## SEC9. Wie werden Ihre Daten während der Übertragung geschützt?

Schützen Sie Ihre Daten während der Übertragung, indem Sie mehrere Kontrollen implementieren und so das Risiko eines unbefugten Zugriffs oder eines Datenverlusts verringern.

## Bewährte Methoden

- [SEC09-BP01 Implementieren Sie eine sichere Schlüssel- und Zertifikatsverwaltung](#)
- [SEC09-BP02 Verschlüsselung bei der Übertragung erzwingen](#)
- [SEC09-BP03 Netzwerkkommunikation authentifizieren](#)

### SEC09-BP01 Implementieren Sie eine sichere Schlüssel- und Zertifikatsverwaltung

Transport Layer Security (TLS) -Zertifikate werden verwendet, um die Netzwerkkommunikation zu sichern und die Identität von Websites, Ressourcen und Workloads über das Internet sowie von privaten Netzwerken nachzuweisen.

Gewünschtes Ergebnis: Ein sicheres Zertifikatsverwaltungssystem, das Zertifikate in einer Public-Key-Infrastruktur bereitstellen, bereitstellen, speichern und erneuern kann (PKI). Ein sicherer Schlüssel- und Zertifikatsverwaltungsmechanismus verhindert die Offenlegung von Zertifikatsdaten mit privaten Schlüsseln und erneuert das Zertifikat automatisch in regelmäßigen Abständen. Er lässt sich auch in andere Services integrieren, um eine sichere Netzwerkkommunikation und Identität für Computerressourcen innerhalb Ihrer Workload zu gewährleisten. Schlüsseldaten sollten niemals für menschliche Identitäten zugänglich sein.

#### Typische Anti-Muster:

- Während der Bereitstellung oder Verlängerung von Zertifikaten werden manuelle Schritte ausgeführt.
- Beim Entwerfen einer privaten Zertifizierungsstelle (Certificate Authority, CA) wird die Hierarchie der Zertifizierungsstelle nicht ausreichend beachtet.
- Für öffentliche Ressourcen werden selbstsignierte Zertifikate verwendet.

#### Vorteile der Nutzung dieser bewährten Methode:

- Die Zertifikatsverwaltung wird durch automatisierte Bereitstellung und Verlängerung vereinfacht.
- Förderung der Verschlüsselung von Daten bei der Übertragung mithilfe von TLS Zertifikaten
- Sicherheit und Überprüfbarkeit der von der Zertifizierungsstelle ausgeführten Zertifikatsaktionen werden gesteigert.
- Verwaltungsaufgaben werden auf verschiedenen Ebenen der CA-Hierarchie strukturiert.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Hoch

## Implementierungsleitfaden

Moderne Workloads nutzen in großem Umfang verschlüsselte Netzwerkkommunikation mithilfe von PKI Protokollen wie TLS. Die Zertifikatsverwaltung kann komplex sein, aber die automatisierte Bereitstellung, Verwaltung und Erneuerung von Zertifikaten kann die Reibungsverluste im Zusammenhang mit der Zertifikatsverwaltung verringern.

AWS [bietet zwei Dienste zur Verwaltung von PKI Zertifikaten für allgemeine Zwecke: AWS Certificate Manager und AWS Private Certificate Authority \(PCA\)](#). AWS Private CA ist der Hauptdienst, den Kunden für die Bereitstellung, Verwaltung und Erneuerung von Zertifikaten sowohl für öffentliche als auch für private Workloads verwenden. AWS Private CA stellt Zertifikate mithilfe vieler anderer AWS verwalteter Dienste aus AWS Private CA und [lässt sich in diese integrieren](#), um sichere TLS Zertifikate für Workloads bereitzustellen.

AWS Private CA ermöglicht es Ihnen, Ihre eigene Stammzertifizierungsstelle oder untergeordnete Zertifizierungsstelle einzurichten und TLS Zertifikate über eine API auszustellen. Sie können diese Art von Zertifikaten in Szenarien verwenden, in denen Sie die Vertrauenskette auf der Clientseite der TLS Verbindung kontrollieren und verwalten. [Zusätzlich zu TLS Anwendungsfällen AWS Private CA können sie verwendet werden, um Zertifikate für Kubernetes-Pods, Matter-Geräteproduktbescheinigungen, Codesignaturen und andere Anwendungsfälle mit einer benutzerdefinierten Vorlage auszustellen](#). Sie können [IAM Roles Anywhere](#) auch verwenden, um temporäre IAM Anmeldeinformationen für lokale Workloads bereitzustellen, für die von Ihrer privaten CA signierte X.509-Zertifikate ausgestellt wurden.

Zusätzlich zu ACM und AWS Private CA [AWS IoT Core](#) bietet speziellen Support für die Bereitstellung, Verwaltung und Erneuerung von PKI Zertifikaten für IoT-Geräte. AWS IoT Core bietet spezielle Mechanismen für die [skalierbare Integration von IoT-Geräten](#) in Ihre Public-Key-Infrastruktur.

### Überlegungen zur Einrichtung einer privaten CA-Hierarchie

Wenn Sie eine private Zertifizierungsstelle einrichten müssen, ist es wichtig, dass Sie besonders darauf achten, die CA-Hierarchie im Voraus richtig zu entwerfen. Es hat sich bewährt, AWS-Konten bei der Erstellung einer privaten CA-Hierarchie jede Ebene Ihrer CA-Hierarchie separat bereitzustellen. Durch diesen gezielten Schritt wird die Oberfläche für jede Ebene in der CA-Hierarchie reduziert, wodurch es einfacher wird, Anomalien in den CloudTrail Protokolldaten zu erkennen und den Umfang des Zugriffs oder die Auswirkungen eines unbefugten Zugriffs auf eines der Konten zu verringern. Die Stammzertifizierungsstelle sollte sich in einem eigenen separaten Konto befinden und nur zur Ausstellung eines oder mehrerer Zertifikate für eine Zwischenzertifizierungsstelle verwendet werden.



Erstellen Sie anschließend ein oder mehrere CAs Zwischenkonten, die vom Konto der Stammzertifizierungsstelle getrennt sind, um Zertifikate für Endbenutzer, Geräte oder andere Workloads auszustellen. Stellen Sie abschließend Zertifikate von Ihrer Stammzertifizierungsstelle an die CAs Zwischenzertifizierungsstelle aus, die wiederum Zertifikate für Ihre Endbenutzer oder Geräte ausstellt. Weitere Informationen zur Planung Ihrer CA-Bereitstellung und zum Entwerfen Ihrer CA-Hierarchie, einschließlich Planung von Ausfallsicherheit, regionsübergreifender Replikation, CAs unternehmensübergreifender Freigabe und mehr, finden Sie unter [Planung Ihrer AWS Private CA Bereitstellung](#).

## Implementierungsschritte

1. Ermitteln Sie die relevanten AWS Dienste, die für Ihren Anwendungsfall erforderlich sind:

- In vielen Anwendungsfällen kann die bestehende AWS Public-Key-Infrastruktur genutzt [AWS Certificate Manager](#) werden. ACM kann verwendet werden, um TLS Zertifikate für Webserver, Load Balancer oder andere Zwecke für öffentlich vertrauenswürdige Zertifikate bereitzustellen.
- Ziehen Sie die Verwendung von [AWS Private CA](#) in Betracht, wenn Sie Ihre eigene private Zertifizierungsstellenhierarchie einrichten müssen oder Zugriff auf exportierbare Zertifikate benötigen. ACM kann dann verwendet werden, um [viele Arten von Endentitätszertifikaten mit dem auszustellen](#). AWS Private CA
- Für Anwendungsfälle, in denen in großem Umfang Zertifikate für eingebettete IoT-Geräte (Internet of Things, Internet der Dinge) bereitgestellt werden müssen, empfiehlt sich gegebenenfalls die Verwendung von [AWS IoT Core](#).

2. Implementieren Sie nach Möglichkeit eine automatisierte Zertifikatverlängerung:

- Verwenden Sie die [ACM verwaltete Verlängerung](#) für Zertifikate, die ACM zusammen mit integrierten AWS Managed Services ausgestellt wurden.

3. Richten Sie Protokollierung und Audit Trails ein:

- Aktivieren Sie [CloudTrail Protokolle](#), um den Zugriff auf die Konten der Zertifizierungsstellen nachzuverfolgen. Erwägen Sie, die Integritätsprüfung der Protokolldatei CloudTrail zu konfigurieren, um die Authentizität der Protokolldaten zu überprüfen.
- Generieren und überprüfen Sie regelmäßig [Auditberichte](#), in denen die Zertifikate aufgeführt werden, die Ihre private CA ausgestellt oder widerrufen hat. Diese Berichte können in einen S3-Bucket exportiert werden.
- Wenn Sie eine private Zertifizierungsstelle bereitstellen, müssen Sie außerdem einen S3-Bucket einrichten, in dem die Zertifikatssperlliste (CRL) gespeichert wird. Anleitungen zur Konfiguration

dieses S3-Buckets auf der Grundlage der Anforderungen Ihres Workloads finden Sie unter [Planung einer Zertifikatssperrliste \(CRL\)](#).

## Ressourcen

Zugehörige bewährte Methoden:

- [SEC02-BP02 Temporäre Anmeldeinformationen verwenden](#)
- [SEC08-BP01 Implementieren Sie eine sichere Schlüsselverwaltung](#)
- [SEC09-BP03 Netzwerkkommunikation authentifizieren](#)

Zugehörige Dokumente:

- [So hosten und verwalten Sie eine gesamte private Zertifikatsinfrastruktur in AWS](#)
- [So sichern Sie eine ACM private CA-Hierarchie auf Unternehmensebene für die Automobil- und Fertigungsindustrie](#)
- [Bewährte Private-CA-Methoden](#)
- [Wie verwenden Sie, AWS RAM um Ihr ACM privates CA-Konto gemeinsam zu nutzen](#)

Zugehörige Videos:

- [Aktivieren von AWS Certificate Manager Private CA \(Workshop\)](#)

Zugehörige Beispiele:

- [Private-CA-Workshop](#)
- [IOTWorkshop zur Geräteverwaltung](#) (einschließlich Gerätebereitstellung)

Zugehörige Tools:

- [Zu verwendendes Plugin für Kubernetes Cert-Manager AWS Private CA](#)

## SEC09-BP02 Verschlüsselung bei der Übertragung erzwingen

Erzwingen Sie Ihre definierten Verschlüsselungsanforderungen basierend auf den Richtlinien, regulatorischen Verpflichtungen und Standards Ihrer Organisation, damit Sie Ihre Organisations-,

Rechts- und Compliance-Anforderungen erfüllen können. Verwenden Sie nur verschlüsselte Protokolle, wenn Sie sensible Daten außerhalb Ihrer Virtual Private Cloud übertragen (VPC). Verschlüsselung trägt auch dann zur Wahrung der Datenvertraulichkeit bei, wenn die Daten nicht vertrauenswürdige Netzwerke durchqueren.

Gewünschtes Ergebnis: Alle Daten sollten bei der Übertragung mit sicheren TLS Protokollen und Verschlüsselungssammlungen verschlüsselt werden. Netzwerkdatenverkehr zwischen Ihren Ressourcen und dem Internet muss verschlüsselt werden, um nicht autorisierten Zugriff auf die Daten zu verhindern. Netzwerkverkehr ausschließlich innerhalb Ihrer internen AWS Umgebung sollte, TLS wo immer möglich, verschlüsselt werden. Das AWS interne Netzwerk ist standardmäßig verschlüsselt und der Netzwerkverkehr innerhalb eines VPC kann nicht gefälscht oder ausspioniert werden, es sei denn, eine nicht autorisierte Partei hat Zugriff auf die Ressource erlangt, die Traffic generiert (wie EC2 Amazon-Instances und Amazon-Container). ECS Erwägen Sie den Schutz des network-to-network Datenverkehrs mit einem IPsec virtuellen privaten Netzwerk (). VPN

Typische Anti-Muster:

- Verwenden Sie veraltete Versionen von SSL/TLS, und Cipher Suite-Komponenten (z. B. SSL v3.0, RSA 1024-Bit-Schlüssel und Cipher). RC4
- Zulassen von unverschlüsseltem () Datenverkehr zu oder von öffentlich zugänglichen Ressourcen. HTTP
- keine Überwachung und kein Ersatz von X.509-Zertifikaten, bevor sie ablaufen
- Verwendung von selbstsignierten X.509-Zertifikaten für. TLS

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Hoch

Implementierungsleitfaden

AWS Dienste stellen HTTPS Endpunkte zur Verfügung, die TLS für die Kommunikation verwendet werden, und bieten Verschlüsselung bei der Übertragung bei der Kommunikation mit dem. AWS APIs Unsichere Protokolle HTTP können beispielsweise VPC mithilfe von Sicherheitsgruppen geprüft und blockiert werden. HTTP-Anfragen können auch [automatisch HTTPS in Amazon CloudFront oder auf einem Application Load Balancer umgeleitet](#) werden. Sie haben uneingeschränkte Kontrolle über Ihre Datenverarbeitungsressourcen und können die Verschlüsselung während der Übertragung in allen Ihren Services implementieren. Darüber hinaus können Sie die VPN Konnektivität über ein externes Netzwerk [AWS Direct Connect](#) zu VPC Ihrem Netzwerk nutzen oder die Verschlüsselung des Datenverkehrs erleichtern. Stellen Sie sicher, dass Ihre Kunden mindestens TLS 1.2 AWS

APIs verwenden, da [AWS dies die Verwendung früherer Versionen von TLS Juni 2023](#) nicht mehr unterstützt. AWS empfiehlt die Verwendung von 1.3TLS. Lösungen von Drittanbietern sind in der verfügbar AWS Marketplace , falls Sie spezielle Anforderungen haben.

## Implementierungsschritte

- Erzwingen der Verschlüsselung bei der Übertragung: Die definierten Verschlüsselungsanforderungen sollten sich nach den neuesten Standards und bewährten Methoden richten und nur sichere Protokolle zulassen. Konfigurieren Sie beispielsweise eine Sicherheitsgruppe so, dass das HTTPS Protokoll nur für einen Application Load Balancer oder eine EC2 Amazon-Instance zulässig ist.
- Konfigurieren Sie sichere Protokolle in Edge-Services: [Konfigurieren Sie HTTPS mit Amazon CloudFront](#) und verwenden Sie ein [Sicherheitsprofil, das für Ihre Sicherheitslage und Ihren Anwendungsfall geeignet ist](#).
- Verwenden Sie a [VPN für externe Konnektivität](#): Erwägen Sie die Verwendung eines IPsec VPN für die Sicherung point-to-point von network-to-network Verbindungen, um sowohl Datenschutz als auch Integrität zu gewährleisten.
- Konfigurieren von sicheren Protokollen bei Load Balancern: Wählen Sie eine Sicherheitsrichtlinie aus, die die stärksten Verschlüsselungssammlungen bereitstellt, die von den Clients unterstützt werden, die eine Verbindung mit dem Listener herstellen. [Erstellen Sie einen HTTPS Listener für Ihren Application Load Balancer](#).
- Konfigurieren Sie sichere Protokolle in Amazon Redshift: Konfigurieren Sie Ihren Cluster so, dass eine [Secure Socket Layer \(SSL\) - oder Transport Layer Security \(TLS\) -Verbindung](#) erforderlich ist.
- Sichere Protokolle konfigurieren: Lesen Sie die AWS Servicedokumentation, um die encryption-in-transit Funktionen zu ermitteln.
- Konfigurieren von sicherem Zugriff beim Hochladen in Amazon-S3-Buckets: Verwenden Sie die Richtliniensteuerung für Amazon-S3-Buckets, um [sicheren Zugriff auf Daten zu erzwingen](#).
- Erwägen Sie die Verwendung von [AWS Certificate Manager](#): ACM ermöglicht Ihnen die Bereitstellung, Verwaltung und Bereitstellung öffentlicher TLS Zertifikate zur Verwendung mit AWS Diensten.
- Erwägen Sie [AWS Private Certificate Authority](#) die Verwendung für private PKI Zwecke: AWS Private CA Ermöglicht die Erstellung von Hierarchien privater Zertifizierungsstellen (CA) zur Ausstellung von X.509-Endzertifikaten, die zur Erstellung verschlüsselter Kanäle verwendet werden können. TLS

## Ressourcen

### Zugehörige Dokumente:

- [HTTPSVerwendung mit CloudFront](#)
- [Connect Sie VPC Ihre mit Remote-Netzwerken über AWS Virtual Private Network](#)
- [Erstellen Sie einen HTTPS Listener für Ihren Application Load Balancer](#)
- [Tutorial:SSL/TLSauf Amazon Linux 2 konfigurieren](#)
- [Verwenden vonSSL/TLS, um eine Verbindung zu einer DB-Instance zu verschlüsseln](#)
- [Konfigurieren von Sicherheitsoptionen für Verbindungen](#)

### SEC09-BP03 Netzwerkkommunikation authentifizieren

Überprüfen Sie die Identität der Kommunikation mithilfe von Protokollen, die die Authentifizierung unterstützen, wie Transport Layer Security (TLS) oderIPsec.

Gestalten Sie Ihre Workload so, dass bei der Kommunikation zwischen Services, Anwendungen oder Benutzern sichere, authentifizierte Netzwerkprotokolle verwendet werden. Die Verwendung von Netzwerkprotokollen, die Authentifizierung und Autorisierung unterstützen, ermöglicht eine bessere Kontrolle des Netzwerkflusses und reduziert die Auswirkungen von nicht autorisiertem Zugriff.

Gewünschtes Ergebnis: Eine Workload mit klar definierten Datenflüssen auf Daten- und Steuerebene zwischen Services. Die Datenflüsse verwenden authentifizierte und verschlüsselte Netzwerkprotokolle, sofern dies technisch möglich ist.

### Typische Anti-Muster:

- unverschlüsselte oder unauthentifizierte Datenflüsse innerhalb Ihrer Workload
- Wiederverwendung von Authentifizierungsdaten für mehrere Benutzer oder Entitäten
- alleinige Verwendung von Netzwerkkontrollen als Zugriffskontrolle
- Erstellung eines benutzerdefinierten Authentifizierungsmechanismus, anstatt sich auf branchenübliche Standard-Authentifizierungsmechanismen zu verlassen
- Übermäßig freizügiger Datenverkehr fließt zwischen Dienstkompnenten oder anderen Ressourcen in der VPC

### Vorteile der Nutzung dieser bewährten Methode:

- Schränkt den Umfang der Auswirkungen eines unberechtigten Zugriffs auf einen Teil des Workloads ein.
- Bietet ein höheres Maß an Sicherheit, dass Aktionen nur von authentifizierten Personen durchgeführt werden können.
- Verbessert die Entkopplung von Services, indem die vorgesehenen Schnittstellen für die Datenübertragung klar definiert und erzwungen werden.
- Verbessert die Überwachung und Protokollierung sowie die Reaktion auf Vorfälle durch Zuordnung von Anforderungen sowie durch klar definierte Kommunikationsschnittstellen.
- Sorgt defense-in-depth für Ihre Workloads, indem Netzwerkkontrollen mit Authentifizierungs- und Autorisierungskontrollen kombiniert werden.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Niedrig

### Implementierungsleitfaden

Die Netzwerkdatenverkehrsmuster Ihrer Workload lassen sich in zwei Kategorien einteilen:

- Der Ost-West-Verkehr steht für Datenflüsse zwischen Services, die eine Workload ausmachen.
- Der Nord-Süd-Verkehr stellt die Datenflüsse zwischen Ihrer Workload und den Consumern dar.

Während es üblich ist, den Nord-Süd-Verkehr zu verschlüsseln, ist der Schutz des Ost-West-Verkehrs mit authentifizierten Protokollen weniger verbreitet. In modernen Sicherheitspraktiken wird darauf hingewiesen, dass das Netzwerkdesign allein noch keine vertrauenswürdige Beziehung zwischen zwei Entitäten gewährleistet. Auch wenn sich zwei Services innerhalb einer gemeinsamen Netzwerkgrenze befinden, ist es immer noch die beste Methode, die Kommunikation zwischen diesen Services zu verschlüsseln, zu authentifizieren und zu autorisieren.

Beispielsweise APIs verwendet der AWS Dienst das Signaturprotokoll [AWS Signature Version 4 \(Sigv4\)](#), um den Anrufer zu authentifizieren, unabhängig davon, aus welchem Netzwerk die Anfrage stammt. Diese Authentifizierung stellt sicher, dass die Identität, die die Aktion angefordert hat, verifiziert werden AWS APIs kann. Diese Identität kann dann mit Richtlinien kombiniert werden, um eine Autorisierungsentscheidung zu treffen und zu bestimmen, ob die Aktion zulässig sein soll oder nicht.

Dienste wie [Amazon VPC Lattice](#) und [Amazon API Gateway](#) ermöglichen es Ihnen, dasselbe SigV4-Signaturprotokoll zu verwenden, um Authentifizierung und Autorisierung für den Ost-West-Verkehr in Ihren eigenen Workloads hinzuzufügen. Wenn Ressourcen außerhalb Ihrer AWS Umgebung

mit Diensten kommunizieren müssen, die eine SIGV4-basierte Authentifizierung und Autorisierung erfordern, können Sie [AWS Identity and Access Management \(IAM\) Roles Anywhere](#) auf der Nicht-Ressource verwenden, um temporäre Anmeldeinformationen abzurufen. AWS Diese Anmeldeinformationen können verwendet werden, um Anforderungen für Services zu signieren, die Zugriff mithilfe von SigV4 autorisieren.

Ein weiterer gängiger Mechanismus zur Authentifizierung von Ost-West-Verkehr ist TLS die gegenseitige Authentifizierung (m). TLS Viele Internet of Things (IoT), business-to-business Anwendungen und Microservices verwenden m, TLS um die Identität beider Seiten einer TLS Kommunikation mithilfe von client- und serverseitigen X.509-Zertifikaten zu überprüfen. Diese Zertifikate können von () ausgestellt werden AWS Private Certificate Authority .AWS Private CA Sie können Dienste wie [Amazon API Gateway](#) und [AWS App Mesh](#) die Bereitstellung der TLS M-Authentifizierung für die Kommunikation zwischen oder innerhalb von Workloads verwenden. m TLS stellt zwar Authentifizierungsinformationen für beide Seiten einer TLS Kommunikation bereit, bietet jedoch keinen Autorisierungsmechanismus.

Schließlich sind OAuth 2.0 und OpenID Connect (OIDC) zwei Protokolle, die typischerweise zur Steuerung des Zugriffs auf Dienste durch Benutzer verwendet werden, aber jetzt auch für den service-to-service Datenverkehr immer beliebter werden. APIGateway bietet einen [JSONWeb Token \(JWT\) -Authorizer](#), mit dem Workloads den Zugriff auf API Routen einschränken können, die von OIDC oder OAuth 2.0 JWTs ausgegebene Identitätsanbieter verwenden. OAuth2 Bereiche können als Quelle für grundlegende Autorisierungsentscheidungen verwendet werden, aber die Autorisierungsprüfungen müssen immer noch in der Anwendungsebene implementiert werden, und OAuth2 Bereiche allein können komplexere Autorisierungsanforderungen nicht erfüllen.

## Implementierungsschritte

- Definieren und dokumentieren Sie Ihre Workload-Netzwerkflüsse: Der erste Schritt bei der Implementierung einer defense-in-depth Strategie besteht darin, die Datenverkehrsflüsse Ihres Workloads zu definieren.
  - Erstellen Sie ein Datenflussdiagramm, das klar definiert, wie Daten zwischen den verschiedenen Services, aus denen sich Ihre Workload zusammensetzt, übertragen werden. Dieses Diagramm ist der erste Schritt zur Erzwingung dieser Datenflüsse über authentifizierte Netzwerkkanäle.
  - Nutzen Sie Ihre Workloads in der Entwicklungs- und Testphase, um zu überprüfen, ob das Datenflussdiagramm das Verhalten der Workloads zur Laufzeit korrekt wiedergibt.
  - Ein Datenflussdiagramm kann auch bei der Durchführung einer Bedrohungsmodellierung nützlich sein, wie in [SEC01-BP07 Identifizieren von Bedrohungen und Priorisieren von Abhilfemaßnahmen anhand eines Bedrohungsmodells](#) beschrieben.

- Einrichtung von Netzwerkkontrollen: Erwägen Sie AWS Möglichkeiten zur Einrichtung von Netzwerkkontrollen, die auf Ihre Datenflüsse abgestimmt sind. Netzwerkgrenzen sollten zwar nicht die einzige Sicherheitskontrolle sein, sie bieten jedoch eine Ebene in der defense-in-depth Strategie zum Schutz Ihrer Workloads.
- Verwenden Sie [Sicherheitsgruppen](#), um den Datenfluss zwischen Ressourcen zu definieren und einzuschränken.
- Erwägen Sie [AWS PrivateLink](#) die Verwendung für die Kommunikation AWS sowohl mit Diensten als auch mit Diensten von Drittanbietern, die dies unterstützen AWS PrivateLink. Daten, die über einen AWS PrivateLink Schnittstellenendpunkt gesendet werden, verbleiben innerhalb des AWS Netzwerk-Backbones und werden nicht über das öffentliche Internet übertragen.
- Implementieren Sie Authentifizierung und Autorisierung für alle Dienste in Ihrem Workload: Wählen Sie die AWS Dienste aus, die am besten geeignet sind, um authentifizierte, verschlüsselte Datenverkehrsflüsse in Ihrem Workload bereitzustellen.
- Ziehen Sie [Amazon VPC Lattice](#) in Betracht, um die service-to-service Kommunikation zu sichern. VPC Lattice kann die [SigV4-Authentifizierung in Kombination mit Authentifizierungsrichtlinien](#) verwenden, um den Zugriff zu kontrollieren. service-to-service
- Für die service-to-service Kommunikation mit m TLS sollten Sie [APIGateway](#) oder [App Mesh](#) in Betracht ziehen. [AWS Private CA](#) kann verwendet werden, um eine private CA-Hierarchie einzurichten, die Zertifikate für die Verwendung mit m ausstellen kann TLS.
- Bei der Integration mit Diensten, die OAuth 2.0 oder verwenden OIDC, sollten Sie erwägen, dass [APIGateway den JWT Authorizer verwendet](#).
- Für die Kommunikation zwischen Ihrer Workload und IoT-Geräten sollten Sie die Verwendung von [AWS IoT Core](#) in Betracht ziehen. Dadurch stehen Ihnen mehrere Optionen für die Verschlüsselung und Authentifizierung des Netzwerkverkehrs zur Verfügung.
- Überwachung auf nicht autorisierten Zugriff: Überwachen Sie kontinuierlich unbeabsichtigte Kommunikationskanäle, nicht autorisierte Prinzipale, die versuchen, auf geschützte Ressourcen zuzugreifen, und andere unzulässige Zugriffsmuster.
- Wenn Sie VPC Lattice verwenden, um den Zugriff auf Ihre Dienste zu verwalten, sollten Sie die [VPC Lattice-Zugriffsprotokolle](#) aktivieren und überwachen. Diese Zugriffsprotokolle enthalten Informationen über die anfragende Entität, Netzwerkinformationen einschließlich Quelle und Ziel sowie VPC Metadaten der Anfrage.
- Erwägen Sie, [VPC Flow-Logs](#) zu aktivieren, um Metadaten zu Netzwerkströmen zu erfassen und sie regelmäßig auf Anomalien zu überprüfen.



- Weitere Hinweise zur Planung, Simulation und [Reaktion auf AWS Sicherheitsvorfälle finden Sie im Security Incident Response Guide und im Abschnitt Incident Response der Sicherheitssäule AWS Well-Architected Framework.](#)

## Ressourcen

### Zugehörige bewährte Methoden:

- [SEC03-BP07 Analysieren Sie den öffentlichen und kontoübergreifenden Zugriff](#)
- [SEC02-BP02 Verwenden Sie temporäre Anmeldeinformationen](#)
- [SEC01-BP07 Identifizieren Sie Bedrohungen und priorisieren Sie Abhilfemaßnahmen mithilfe eines Bedrohungsmodells](#)

### Zugehörige Dokumente:

- [Evaluierung von Zugriffskontrollmethoden zur Sicherung von Amazon API Gateway APIs](#)
- [Konfiguration der gegenseitigen TLS Authentifizierung für ein REST API](#)
- [Wie sichert man API HTTP Gateway-Endpunkte mit einem Authorizer JWT](#)
- [Autorisieren von direkten Aufrufen von AWS Diensten mithilfe eines Anmeldeinformationsanbieters AWS IoT Core](#)
- [AWS Leitfaden zur Reaktion auf Sicherheitsvorfälle](#)

### Zugehörige Videos:

- [AWS re:invent 2022: Wir stellen vor: Lattice VPC](#)
- [AWS re:invent 2020: Serverlose Authentifizierung für API HTTP APIs AWS](#)

### Zugehörige Beispiele:

- [Amazon VPC Lattice Workshop](#)
- [Zero-Trust, Episode 1: Der Phantom-Service-Perimeter-Workshop](#)

## Vorfallreaktion

### Frage

- [SEC10. Wie können Sie Vorfälle voraussagen, darauf reagieren und diese beheben?](#)

## SEC10. Wie können Sie Vorfälle voraussagen, darauf reagieren und diese beheben?

Auch bei ausgereiften präventiven und Erkennungskontrollen, sollte Ihr Unternehmen Verfahren etablieren, um auf Sicherheitsvorfälle reagieren und mögliche Auswirkungen mindern zu können. Ihre Vorbereitung wirkt sich stark auf die Fähigkeit Ihrer Teams aus, während eines Vorfalls effektiv zu arbeiten, Probleme zu isolieren, einzudämmen und forensisch zu untersuchen sowie den Betrieb in einem bekannten guten Zustand wiederherzustellen. Durch die Bereitstellung von Tools und Zugriff vor einem Sicherheitsvorfall und die routinemäßige Reaktion auf Vorfälle im Alltag können Sie sicherstellen, dass Sie eine Wiederherstellung durchführen und die Betriebsunterbrechung minimieren können.

### Bewährte Methoden

- [SEC10-BP01 Identifizieren Sie wichtige Mitarbeiter und externe Ressourcen](#)
- [SEC10-BP02 Entwickeln Sie Pläne für das Vorfalmanagement](#)
- [SEC10-BP03 Forensische Fähigkeiten vorbereiten](#)
- [SEC10-BP04 Playbooks zur Reaktion auf Sicherheitsvorfälle entwickeln und testen](#)
- [SEC10-BP05 Zugriff vor der Bereitstellung](#)
- [SEC10-BP06 Tools vor der Bereitstellung](#)
- [SEC10-BP07 Simulationen ausführen](#)
- [SEC10-BP08 Schaffen Sie einen Rahmen, um aus Vorfällen zu lernen](#)

### SEC10-BP01 Identifizieren Sie wichtige Mitarbeiter und externe Ressourcen

Identifizieren Sie internes und externes Personal, Ressourcen und rechtliche Anforderungen, um Ihre Organisation bei der Reaktion auf einen Vorfall zu unterstützen.

Gewünschtes Ergebnis: Sie verfügen über eine Liste mit den wichtigsten Mitarbeitern, ihren Kontaktinformationen und ihrer Rolle bei der Reaktion auf ein Sicherheitsereignis. Sie überprüfen diese Informationen regelmäßig und aktualisieren sie, um personelle Veränderungen aus Sicht der internen und externen Tools zu berücksichtigen. Bei der Dokumentation dieser Informationen berücksichtigen Sie alle Drittanbieter und Anbieter, einschließlich Sicherheitspartner, Cloud-Anbieter und software-as-a-service (SaaS-) Anwendungen. Während eines Sicherheitsereignisses stehen Mitarbeiter mit dem entsprechenden Maß an Verantwortung, Kontext und Zugriff zur Verfügung, um zu reagieren und das Ereignis zu bewältigen.

## Typische Anti-Muster:

- Fehlen einer aktualisierten Liste der wichtigsten Mitarbeiter mit Kontaktinformationen, ihren Aufgaben und ihren Verantwortlichkeiten bei der Reaktion auf Sicherheitsvorfälle
- Voraussetzen, dass jeder die Personen, die Abhängigkeiten, die Infrastruktur und die Lösungen bei der Reaktion auf ein Ereignis und bei der Bewältigung eines Ereignisses versteht
- Fehlen eines Dokuments oder eines Wissens-Repositorys, das die wichtigsten Infrastruktur- oder Anwendungsdesigns darstellt
- Fehlen von angemessenen Einarbeitungsprozessen für neue Mitarbeiter, um effektiv zur Reaktion auf ein Sicherheitsereignis beizutragen (etwa die Durchführung von Ereignissimulationen)
- Fehlen eines Eskalationspfads für den Fall, dass wichtige Mitarbeiter vorübergehend nicht verfügbar sind oder bei Sicherheitsereignissen nicht reagieren

Vorteile der Nutzung dieser bewährten Methode Diese Praxis reduziert die Triage- und Reaktionszeit, die für die Identifizierung der richtigen Mitarbeiter und ihrer Rollen während eines Ereignisses aufgewendet wird. Minimieren Sie Zeitverluste während eines Ereignisses, indem Sie eine aktualisierte Liste der wichtigsten Mitarbeiter und ihrer Rollen führen, damit Sie die richtigen Personen für die Triage und die Bewältigung eines Ereignisses einsetzen können.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Hoch

## Implementierungsleitfaden

Identifizieren Sie wichtige Personen in Ihrer Organisation: Führen Sie eine Kontaktliste der Personen in Ihrer Organisation, die Sie einbeziehen müssen. Überprüfen und aktualisieren Sie diese Informationen regelmäßig bei personellen Veränderungen wie organisatorischen Änderungen, Beförderungen und Teamwechsell. Dies ist besonders wichtig für Schlüsselpositionen wie Incident Manager, Incident Responder und Communications Lead.

- Incident Manager: Incident Managers haben die Gesamtverantwortung für die Reaktion auf das Ereignis.
- Incident Responder: Incident Responders sind für Untersuchungen und Abhilfemaßnahmen zuständig. Diese Personen können sich je nach Art des Ereignisses unterscheiden, sind aber in der Regel Entwickler und Betriebs-Teams, die für die betroffene Anwendung verantwortlich sind.
- Communications Lead: Communications Leads sind für die interne und externe Kommunikation verantwortlich, insbesondere mit Behörden, Regulierungsbehörden und Kunden.

- **Fachexperten (SMEs):** Bei verteilten und autonomen Teams empfehlen wir Ihnen, SME für unternehmenskritische Workloads eine Lösung zu identifizieren. Sie bieten Einblicke in den Betrieb und die Datenklassifizierung von kritischen Workloads, die an dem Ereignis beteiligt sind.

Erwägen Sie die Verwendung des Features [AWS Systems Manager Incident Manager](#), um wichtige Kontakte zu erfassen, einen Reaktionsplan zu definieren, Bereitschaftspläne zu automatisieren und Eskalationspläne zu erstellen. Automatisieren und rotieren Sie alle Mitarbeiter durch einen Bereitschaftsdienstplan, sodass die Verantwortung für die Workload auf alle zuständigen Personen verteilt wird. Dies fördert gute Praktiken wie die Ausgabe relevanter Metriken und Protokolle sowie die Definition von Alarmschwellen, die für die Workload von Bedeutung sind.

Identifizieren Sie externe Partner: Unternehmen verwenden Tools, die von unabhängigen Softwareanbietern (ISVs), Partnern und Subunternehmern entwickelt wurden, um differenzierte Lösungen für ihre Kunden zu entwickeln. Binden Sie wichtige Mitarbeiter dieser Parteien ein, die Ihnen bei der Reaktion auf einen Vorfall und bei dessen Bewältigung helfen können. Wir empfehlen Ihnen, sich für die entsprechende Stufe von zu registrieren, um AWS Support im Rahmen eines Support-Falls umgehend AWS Kontakt zu Fachexperten zu erhalten. Erwägen Sie, ähnliche Vereinbarungen mit allen Anbietern kritischer Lösungen für die Workloads zu schließen. Einige Sicherheitsereignisse machen es erforderlich, dass börsennotierte Unternehmen die zuständigen Behörden und Aufsichtsbehörden über das Ereignis und dessen Auswirkungen informieren. Pflegen und aktualisieren Sie die Kontaktinformationen der relevanten Abteilungen und der zuständigen Personen.

### Implementierungsschritte

1. Richten Sie eine Lösung für das Vorfallmanagement ein.
  - a. Erwägen Sie die Bereitstellung von Incident Manager in Ihrem Security-Tooling-Konto.
2. Definieren Sie Kontakte in Ihrer Lösung für das Vorfallmanagement.
  - a. Definieren Sie mindestens zwei Arten von Kontaktkanälen für jeden Kontakt (z. B. SMS Telefon oder E-Mail), um die Erreichbarkeit während eines Vorfalls sicherzustellen.
3. Definieren Sie einen Reaktionsplan.
  - a. Ermitteln Sie die am besten geeigneten Ansprechpartner für einen Vorfall. Definieren Sie Eskalationspläne, die sich an den Rollen der einzuschaltenden Mitarbeiter orientieren (und nicht an einzelnen Ansprechpartnern). Erwägen Sie die Aufnahme von Kontakten, die gegebenenfalls für die Benachrichtigung externer Stellen zuständig sind, auch wenn diese nicht direkt an der Lösung des Vorfalls beteiligt sind.

## Ressourcen

### Zugehörige bewährte Methoden:

- [OPS02-BP03 Bei den operativen Aktivitäten wurden die Eigentümer identifiziert, die für ihre Leistung verantwortlich sind](#)

### Zugehörige Dokumente:

- [AWS Security Incident Response Guide](#)

### Zugehörige Beispiele:

- [AWS Customer Playbook Framework](#)
- [Vorbereiten und Reagieren auf Sicherheitsvorfälle in Ihrer AWS -Umgebung](#)

### Zugehörige Tools:

- [AWS Systems Manager Incident Manager](#)

### Zugehörige Videos:

- [Der Sicherheitsansatz von Amazon bei der Entwicklung](#)

## SEC10-BP02 Entwickeln Sie Pläne für das Vorfalmanagement

Das erste Dokument, das für die Vorfalreaktion entwickelt werden muss, ist der Vorfalreaktionsplan. Der Vorfalreaktionsplan ist als Grundlage für Ihr Vorfalreaktionsprogramm und Ihre Vorfalreaktionsstrategie konzipiert.

Vorteile der Nutzung dieser bewährten Methode: Die Entwicklung durchdachter und klar definierter Prozesse zur Vorfalreaktion ist der Schlüssel zu einem erfolgreichen und skalierbaren Vorfalreaktionsprogramm. Wenn ein Sicherheitsereignis eintritt, können Ihnen klare Schritte und Workflows dabei helfen, rechtzeitig zu reagieren. Möglicherweise verfügen Sie bereits über Prozesse zur Vorfalreaktion. Unabhängig von Ihrem aktuellen Status ist es wichtig, Ihre Prozesse zur Vorfalreaktion regelmäßig zu aktualisieren, zu wiederholen und zu testen.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Hoch

## Implementierungsleitfaden

Ein Vorfalmanagementplan ist von entscheidender Bedeutung, um auf Sicherheitsvorfälle zu reagieren, sie einzudämmen und ihre potenziellen Folgen zu beheben. Ein Vorfalmanagementplan ist ein strukturierter Prozess für die Identifizierung und Behebung von Sicherheitsvorfällen sowie die zeitnahe Reaktion darauf.

In der Cloud gibt es viele der betrieblichen Rollen und Anforderungen, die auch für eine On-Premises-Umgebung typisch sind. Bei der Erstellung eines Vorfalmanagementplans ist es wichtig, Reaktions- und Wiederherstellungsstrategien zu berücksichtigen, die optimal zu Ihren Anforderungen an geschäftliche Ergebnisse und Compliance passen. Wenn Sie beispielsweise Workloads in den USA betreiben, AWS die den Anforderungen der US-Notenbank RAMP entsprechen, ist es hilfreich, sich an den [NISTSP 800-61 Computer Security Handling Guide](#) zu halten. In ähnlicher Weise sollten Sie beim Betrieb von Workloads mit europäischen personenbezogenen Daten (PII) Szenarien in Betracht ziehen, z. B. wie Sie Probleme im Zusammenhang mit dem Datenspeicherort schützen und entsprechend den Bestimmungen der [Allgemeinen Datenschutzverordnung \(\) der EU \(\)](#) behandeln könnten. GDPR

Beginnen Sie bei der Erstellung eines Vorfalmanagementplans für Ihre Workloads mit dem [Modell der AWS gemeinsamen Verantwortung AWS](#), um einen defense-in-depth Ansatz für die Reaktion auf Vorfälle zu entwickeln. In diesem Modell wird die Sicherheit der Cloud AWS verwaltet, und Sie sind für die Sicherheit in der Cloud verantwortlich. Das bedeutet, dass Sie die Kontrolle behalten und für die Sicherheitskontrollen verantwortlich sind, für deren Implementierung Sie sich entscheiden. Der [Leitfaden für AWS Security Incident Response](#) enthält zentrale Konzepte und grundlegende Anleitungen für den Aufbau eines Cloud-basierten Vorfalmanagementplans.

Ein effektiver Vorfalmanagementplan muss kontinuierlich durchlaufen und stets an die Ziele Ihrer Cloud-Operationen angepasst werden. Erwägen Sie die Verwendung der nachfolgend erläuterten Implementierungspläne für die Erstellung und Weiterentwicklung Ihres Vorfalmanagementplans.

### Implementierungsschritte

#### Definieren von Rollen und Zuständigkeiten

Der Umgang mit Sicherheitsereignissen erfordert organisationsübergreifende Disziplin und Handlungsbereitschaft. Innerhalb Ihrer Organisationsstruktur sollte es viele Personen geben, die für einen Vorfall verantwortlich und rechenschaftspflichtig sind sowie konsultiert oder auf dem Laufenden gehalten werden. Beispiele wären etwa Vertreter der Personalabteilung (HR), des Führungsteams und der Rechtsabteilung. Berücksichtigen Sie diese Rollen und Verantwortlichkeiten sowie die Frage,

ob Dritte eingebunden werden müssen. Beachten Sie, dass in vielen Regionen lokale Gesetze gelten, die regeln, was getan werden sollte und was nicht. Auch wenn es bürokratisch erscheinen mag, ein Diagramm mit Verantwortung, Rechenschaftspflicht, Rücksprache und Information (RACI) für Ihre Pläne zur Reaktion auf die Sicherheit zu erstellen, erleichtert dies eine schnelle und direkte Kommunikation und beschreibt klar und deutlich, wie die Leitung in den verschiedenen Phasen der Veranstaltung abläuft.

Bei einem Vorfall ist es wichtig, die Eigentümer und Entwickler der betroffenen Anwendungen und Ressourcen einzubeziehen, da es sich um Fachexperten (SMEs) handelt, die Informationen und den Kontext bereitstellen können, um die Auswirkungen zu messen. Üben Sie und bauen Sie Beziehungen zu den Entwicklern und Anwendungsbesitzern auf, bevor Sie sich bei der Vorfalldiagnose auf deren Fachwissen verlassen. Anwendungseigentümer oder SMEs, wie z. B. Ihre Cloud-Administratoren oder Techniker, müssen möglicherweise in Situationen handeln, in denen die Umgebung unbekannt oder komplex ist oder in denen die Einsatzkräfte keinen Zugriff haben.

Zu guter Letzt können auch vertrauenswürdige Partner in die Untersuchung oder Reaktion einbezogen werden, da sie zusätzliches Fachwissen und wertvolle Einblicke bereitstellen können. Wenn Sie in Ihrem eigenen Team nicht über diese Fähigkeiten verfügen, sollten Sie eine externe Partei mit der Unterstützung beauftragen.

Machen Sie sich mit AWS Reaktionsteams und Support vertraut

- AWS Support
  - [AWS Support](#) bietet eine Reihe von Tarifen, die Zugriff auf Tools und Fachwissen bieten, die den Erfolg und die Funktionsfähigkeit Ihrer AWS Lösungen unterstützen. Wenn Sie technischen Support und mehr Ressourcen für die Planung, Bereitstellung und Optimierung Ihrer AWS Umgebung benötigen, können Sie einen Supportplan wählen, der am besten zu Ihrem AWS Anwendungsfall passt.
  - Betrachten Sie das [Support Center](#) AWS Management Console (Anmeldung erforderlich) als zentrale Anlaufstelle, um Support bei Problemen zu erhalten, die Ihre AWS Ressourcen betreffen. Der Zugriff auf AWS Support wird gesteuert von AWS Identity and Access Management. Weitere Informationen zum Zugriff auf AWS Support Funktionen finden Sie unter [Erste Schritte mit AWS Support](#).
- AWS Team zur Reaktion auf Kundenvorfälle (CIRT)
  - Das AWS Customer Incident Response Team (CIRT) ist ein spezialisiertes globales AWS Team, das rund um die Uhr verfügbar ist und Kunden bei aktiven Sicherheitsvorfällen auf Kundenseite im Rahmen des [Modells der AWS gemeinsamen Verantwortung](#) unterstützt.

- Wenn es Sie AWS CIRT unterstützt, bietet es Ihnen Unterstützung bei der Suche und Wiederherstellung bei einem aktiven Sicherheitsereignis am AWS. Mithilfe von AWS Serviceprotokollen können sie Sie bei der Ursachenanalyse unterstützen und Ihnen Empfehlungen für die Wiederherstellung geben. Sie können Ihnen auch Sicherheitsempfehlungen und bewährte Methoden an die Hand geben, mit denen Sie Sicherheitsereignisse in Zukunft vermeiden können.
- AWS Kunden können sie AWS CIRT anhand eines [AWS Support Falls kontaktieren](#).
- DDoSUnterstützung bei der Beantwortung
  - AWS bietet [AWS Shield](#) einen verwalteten Dienst zum Schutz vor verteilten Denial-of-Service (DDoS), der Webanwendungen schützt, auf denen ausgeführt wird. AWS Shield bietet eine ständig aktive Erkennung und automatische Inline-Abwehrmaßnahmen, mit denen Ausfallzeiten und Latenz von Anwendungen minimiert werden können, sodass kein Eingreifen erforderlich ist, um vom Schutz AWS Support zu profitieren. DDoS Es gibt zwei Stufen von Shield: AWS Shield Standard und AWS Shield Advanced. Weitere Informationen zu den Unterschieden zwischen diesen beiden Stufen finden Sie in der [Shield-Funktionsdokumentation](#).
- AWS Managed Services (AMS)
  - [AWS Managed Services \(AMS\)](#) ermöglicht die kontinuierliche Verwaltung Ihrer AWS Infrastruktur, sodass Sie sich auf Ihre Anwendungen konzentrieren können. Durch die Implementierung von Best Practices zur Wartung Ihrer Infrastruktur tragen Sie AMS dazu bei, Ihren betrieblichen Aufwand und Ihr Risiko zu reduzieren. AMSautomatisiert gängige Aktivitäten wie Änderungsanforderungen, Überwachung, Patch-Management, Sicherheit und Backup-Services und bietet Services über den gesamten Lebenszyklus für die Bereitstellung, den Betrieb und den Support Ihrer Infrastruktur.
  - AMSübernimmt die Verantwortung für die Implementierung einer Reihe von Sicherheitsfunktionen und bietet rund um die Uhr eine erste Reaktionslinie bei Warnmeldungen. Wenn eine Warnung ausgelöst wird, AMS folgt sie einem Standardsatz automatisierter und manueller Abläufe, um sicherzustellen, dass eine konsistente Reaktion gewährleistet ist. Diese Playbooks werden den AMS Kunden beim Onboarding zur Verfügung gestellt, sodass sie eine Reaktion entwickeln und mit ihnen abstimmen können. AMS

## Erstellen des Vorfallreaktionsplans

Der Vorfallreaktionsplan ist als Grundlage für Ihr Vorfallreaktionsprogramm und Ihre Vorfallreaktionsstrategie konzipiert. Er sollte immer formell schriftlich festgehalten werden. Ein Vorfallreaktionsplan enthält in der Regel folgende Abschnitte:



- Überblick über das Vorfalldreaktionsteam: Enthält die Ziele und Funktionen des Vorfalldreaktionsteams.
- Rollen und Zuständigkeiten: Hier werden die für die Vorfalldreaktion zuständigen Stakeholder aufgeführt und ihre Rollen im Falle eines Vorfalles beschrieben.
- Kommunikationsplan: Enthält Kontaktinformationen und gibt an, wie Sie während eines Vorfalles kommunizieren.
- Backup-Kommunikationsmethoden: Es hat sich bewährt, die out-of-band Kommunikation als Backup für die Kommunikation bei Zwischenfällen zu verwenden. Ein Beispiel für eine Anwendung, die einen sicheren out-of-band Kommunikationskanal bereitstellt, ist AWS Wickr.
- Phasen der Vorfalldreaktion und zu ergreifende Maßnahmen: Hier sind die Phasen der Vorfalldreaktion aufgeführt (beispielsweise Erkennung, Analyse, Beseitigung, Eindämmung und Wiederherstellung) – einschließlich der in diesen Phasen zu ergreifenden allgemeinen Maßnahmen.
- Definitionen des Schweregrads und der Priorisierung des Vorfalles: Hier wird erläutert, wie der Schweregrad eines Vorfalles klassifiziert wird, wie der Vorfall priorisiert wird und wie sich die Schweregraddefinitionen dann auf die Eskalationsverfahren auswirken.

Diese Abschnitte sind zwar in Unternehmen verschiedener Größen und Branchen üblich, der Vorfalldreaktionsplan ist jedoch für jede Organisation individuell. Erstellen Sie einen Vorfalldreaktionsplan, der für Ihre Organisation am besten geeignet ist.

## Ressourcen

Zugehörige bewährte Methoden:

- [SEC04 \(Wie erkennen und untersuchen Sie Sicherheitsereignisse?\)](#)

Zugehörige Dokumente:

- [AWS Leitfaden zur Reaktion auf Sicherheitsvorfälle](#)
- [NIST: Leitfaden zur Behandlung von Computersicherheitsvorfällen](#)

## SEC10-BP03 Forensische Fähigkeiten vorbereiten

Bevor es zu einem Sicherheitsvorfall kommt, empfiehlt es sich gegebenenfalls, forensische Funktionen zur Unterstützung der Untersuchung von Sicherheitsereignissen zu entwickeln.

## Risikostufe bei fehlender Befolgung dieser bewährten Methode: Mittel

Konzepte aus der traditionellen Forensik vor Ort gelten für AWS. Wichtige Informationen für den Aufbau forensischer Fähigkeiten in der finden Sie unter Strategien für [forensische AWS Cloud](#) Ermittlungsumgebungen in der AWS Cloud

Sobald Sie Ihre Umgebung und AWS-Konto Struktur für die Forensik eingerichtet haben, definieren Sie die Technologien, die zur effektiven Durchführung forensisch fundierter Methoden in den vier Phasen erforderlich sind:

- **Erfassung:** Sammeln Sie relevante AWS Protokolle wie,, VPC Flow Logs AWS CloudTrail und AWS Config Logs auf Hostebene. Sammeln Sie Snapshots, Backups und Speicherabbilder der betroffenen AWS Ressourcen, sofern verfügbar.
- **Prüfung:** Prüfen Sie die erfassten Daten, indem Sie die relevanten Informationen extrahieren und bewerten.
- **Analyse:** Analysieren Sie die erfassten Daten, um den Vorfall zu verstehen und Schlüsse daraus zu ziehen.
- **Berichterstellung:** Präsentieren Sie die Informationen, die sich aus der Analysephase ergeben.

## Implementierungsschritte

### Vorbereiten Ihrer forensischen Umgebung

[AWS Organizations](#) hilft Ihnen dabei, eine AWS Umgebung zentral zu verwalten und zu steuern, während Sie Ihre Ressourcen erweitern und skalieren. Eine AWS Organisation konsolidiert Ihre Daten, AWS-Konten sodass Sie sie als eine Einheit verwalten können. Sie können Organisationseinheiten (OUs) verwenden, um Konten zu gruppieren und sie als eine einzige Einheit zu verwalten.

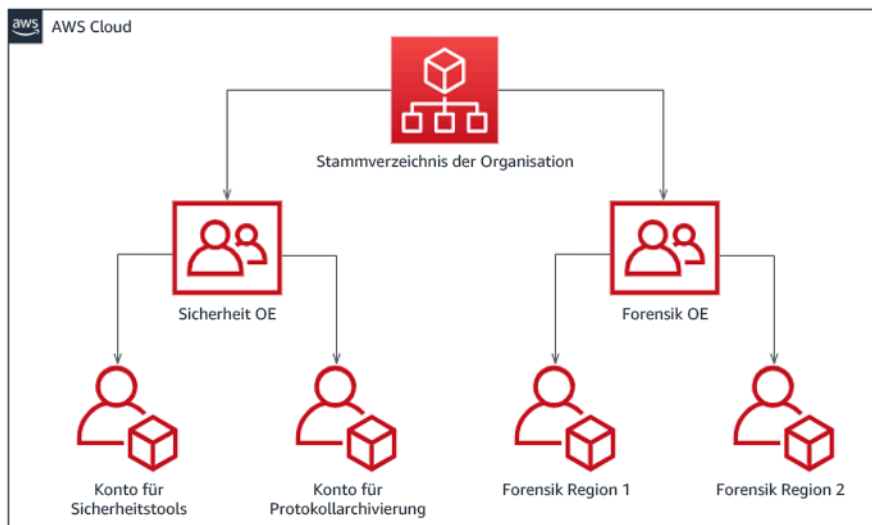
Für die Reaktion auf Vorfälle ist es hilfreich, über eine AWS-Konto Struktur zu verfügen, die die Funktionen der Incident-Response unterstützt. Dazu gehören eine Sicherheits-OU und eine Forensik-OU. Innerhalb der sicherheitsbezogenen Organisationseinheit sollten Sie über Konten für Folgendes verfügen:

- **Protokollarchivierung:** Aggregieren Sie Protokolle in einer Protokollarchivierung mit eingeschränkten Rechten AWS-Konto .
- **Sicherheitstools:** Zentralisieren Sie Sicherheitsdienste in einem Sicherheitstool. Dieses Konto fungiert als delegierter Administrator für Sicherheits-Services.

Innerhalb der forensischen Organisationseinheit haben Sie die Möglichkeit, für jede Region, in der Sie tätig sind, eines oder mehrere forensische Konten zu implementieren, je nachdem, was für Ihr Geschäfts- und Betriebsmodell am besten geeignet ist. Wenn Sie pro Region ein forensisches Konto erstellen, können Sie die Erstellung von AWS Ressourcen außerhalb dieser Region blockieren und so das Risiko verringern, dass Ressourcen in eine unbeabsichtigte Region kopiert werden. Wenn Sie beispielsweise nur in den Regionen „USA Ost (Nord-Virginia)“ (us-east-1) und „USA West (Oregon)“ (us-west-2) aktiv sind, würde die forensische Organisationseinheit zwei Konten umfassen: eins für us-east-1 und eins für us-west-2.

Sie können ein AWS-Konto forensisches System für mehrere Regionen erstellen. Sie sollten beim Kopieren von AWS Ressourcen auf dieses Konto Vorsicht walten lassen, um sicherzustellen, dass Sie Ihre Anforderungen an die Datenhoheit erfüllen. Da die Bereitstellung neuer Konten etwas dauert, ist es unerlässlich, die forensischen Konten rechtzeitig vor einem Vorfall einzurichten und zu instrumentieren, damit die Notfallteams vorbereitet sind und sie effektiv nutzen können.

Das folgende Diagramm zeigt eine Beispiel-Kontenstruktur mit einer forensischen Organisationseinheit mit regionsspezifischen forensischen Konten:



## Regionsspezifische Kontenstruktur für die Reaktion auf Vorfälle

### Erfassen von Backups und Snapshots

Die Einrichtung von Backups wichtiger Systeme und Datenbanken ist für die Wiederherstellung nach einem Sicherheitsvorfall und für forensische Zwecke von entscheidender Bedeutung. Mit vorhandenen Backups können Sie Ihre Systeme wieder in einen vorherigen sicheren Zustand versetzen. Bei AWS aktivierter Option können Sie Schnappschüsse verschiedener Ressourcen erstellen. Mit Snapshots erhalten Sie point-in-time Backups dieser Ressourcen. Es

gibt viele AWS Dienste, die Sie bei der Sicherung und Wiederherstellung unterstützen können. Einzelheiten zu diesen Services und Ansätzen für Backup und Wiederherstellung finden Sie unter [Präskriptive Leitlinien für Backup und Wiederherstellung](#) sowie unter [Verwendung von Backups zur Wiederherstellung nach Sicherheitsvorfällen](#).

Vor allem, wenn es um Situationen wie Ransomware geht, ist es wichtig, dass Ihre Backups gut geschützt sind. Hinweise zum Schutz Ihrer Backups finden Sie in den [10 besten Sicherheitsmethoden zum Schutz von Backups in AWS](#). Zusätzlich zum Schutz Ihrer Backups sollten Sie Ihre Backup- und Wiederherstellungsprozesse regelmäßig testen, um sicherzustellen, dass die vorhandenen Technologien und Prozesse wie erwartet funktionieren.

## Automatisieren der Forensik

Während eines Sicherheitsereignisses muss Ihr Incident-Response-Team in der Lage sein, schnell Beweise zu sammeln und zu analysieren und gleichzeitig die Genauigkeit für den Zeitraum, der das Ereignis umgibt, aufrechtzuerhalten (z. B. das Erfassen von Protokollen zu einem bestimmten Ereignis oder einer bestimmten Ressource oder das Sammeln eines Speicherabbilds einer EC2 Amazon-Instance). Für das Vorfalldreaktionsteam ist es sowohl schwierig als auch zeitaufwändig, die relevanten Nachweise manuell zu erfassen, insbesondere bei einer großen Anzahl von Instances und Konten. Darüber hinaus kann die manuelle Erfassung anfällig für menschliche Fehler sein. Daher sollten Sie die Automatisierung für die Forensik so weit wie möglich entwickeln und implementieren.

AWS bietet eine Reihe von Automatisierungsressourcen für die Forensik, die im folgenden Abschnitt „Ressourcen“ aufgeführt sind. Diese Ressourcen sind Beispiele für forensische Muster, die von entwickelt und von Kunden implementiert wurden. Obwohl sie für den Anfang eine nützliche Referenzarchitektur sein können, sollten Sie erwägen, sie zu ändern oder neue forensische Automatisierungsmuster zu erstellen, die auf Ihrer Umgebung, Ihren Anforderungen, Tools und forensischen Prozessen basieren.

## Ressourcen

### Zugehörige Dokumente:

- [AWS Leitfaden zur Reaktion auf Sicherheitsvorfälle — Entwickeln Sie forensische Fähigkeiten](#)
- [AWS Leitfaden zur Reaktion auf Sicherheitsvorfälle — Ressourcen für Forensik](#)
- [Strategien für forensische Untersuchungen im Umfeld der AWS Cloud](#)
- [So automatisieren Sie die forensische Festplattensammlung in AWS](#)
- [AWS Präskriptive Leitlinien — Automatisieren Sie die Reaktion auf Vorfälle und die Forensik](#)

## Zugehörige Videos:

- [Automatisieren der Vorfalldreaktion und Forensik](#)

## Zugehörige Beispiele:

- [Framework für die automatisierte Reaktion auf Vorfälle und für die Forensik](#)
- [Automatisierter Forensics Orchestrator für Amazon EC2](#)

## SEC10-BP04 Playbooks zur Reaktion auf Sicherheitsvorfälle entwickeln und testen

Ein wichtiger Teil der Vorbereitung Ihrer Prozesse zur Vorfalldreaktion ist die Entwicklung von Playbooks. Playbooks für die Vorfalldreaktion enthalten eine Reihe von präskriptiven Anleitungen und Schritten, die Sie befolgen müssen, wenn ein Sicherheitsereignis eintritt. Eine klare Struktur und klare Schritte vereinfachen die Reaktion und verringern die Wahrscheinlichkeit menschlicher Fehler.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel

## Implementierungsleitfaden

Playbooks sollten für Vorfalldszenarien wie die folgenden erstellt werden:

- Erwartete Vorfälle: Sie sollten Playbooks für zu erwartende Vorfälle erstellen. Dazu gehören Bedrohungen wie Denial of Service (DoS), Ransomware und die Kompromittierung von Anmeldeinformationen.
- Bekannte Sicherheitsfeststellungen oder Warnmeldungen: Playbooks sollten für Ihre bekannten Sicherheitsfeststellungen und -warnungen, wie z. B. Ergebnisse, erstellt werden. GuardDuty Möglicherweise erhalten Sie ein GuardDuty Ergebnis und denken: „Was nun?“ Um zu verhindern, dass ein Ergebnis falsch behandelt oder ignoriert wird, sollten Sie für jedes potenzielle GuardDuty Ergebnis ein Playbook erstellen. GuardDuty [Einige Einzelheiten und Anleitungen zur Problembehebung finden Sie in der Dokumentation. GuardDuty](#) Es ist erwähnenswert, dass dies standardmäßig nicht aktiviert GuardDuty ist und Kosten verursacht. Weitere Informationen dazu finden Sie in [Anhang A: Definitionen von Cloud-Funktionen — Sichtbarkeit und Warnmeldungen. GuardDuty](#)

Playbooks sollten technische Schritte enthalten, die ein Sicherheitsanalyst ausführen muss, um einen potenziellen Sicherheitsvorfall angemessen zu untersuchen und darauf zu reagieren.

## Implementierungsschritte

Zu den Elementen, die in ein Playbook aufgenommen werden sollten, gehören:

- **Playbook-Übersicht:** Welches Risiko- oder Vorfallszenario behandelt dieses Playbook? Was ist das Ziel des Playbooks?
- **Voraussetzungen:** Welche Protokolle, Erkennungsmechanismen und automatisierten Tools sind für dieses Vorfallszenario erforderlich? Wie lautet die erwartete Benachrichtigung?
- **Kommunikations- und Eskalationsinformationen:** Wer ist beteiligt und wie lauten die Kontaktinformationen? Welche Aufgaben haben die einzelnen Stakeholder?
- **Reaktionsschritte:** Welche taktischen Maßnahmen sollten in den einzelnen Phasen der Vorfalldiagnose ergriffen werden? Welche Abfragen sollte ein Analyst ausführen? Welcher Code sollte ausgeführt werden, um das gewünschte Ergebnis zu erzielen?
  - **Erkennen:** Wie wird der Vorfall erkannt?
  - **Analysieren:** Wie wird der Umfang der Auswirkungen bestimmt?
  - **Eindämmen:** Wie wird der Vorfall isoliert, um den Umfang zu begrenzen?
  - **Beseitigen:** Wie wird die Bedrohung aus der Umgebung entfernt?
  - **Wiederherstellen:** Wie wird das betroffene System oder die betroffene Ressource wieder in der Produktion bereitgestellt?
- **Erwartete Ergebnisse:** Was ist das erwartete Ergebnis des Playbooks, nachdem Abfragen und Code ausgeführt wurden?

## Ressourcen

Zugehörige bewährte Methoden für Well-Architected:

- [SEC10-BP02 — Entwickeln Sie Pläne für das Vorfalldiagnosemanagement](#)

Zugehörige Dokumente:

- [Framework für Playbooks für die Vorfalldiagnose](#)
- [Entwickeln eigener Playbooks für die Vorfalldiagnose](#)
- [Exemplarische Playbooks für die Vorfalldiagnose](#)
- [Erstellung eines Runbooks zur Reaktion auf AWS Vorfälle mithilfe von Jupyter-Playbooks und Lake CloudTrail](#)

## SEC10-BP05 Zugriff vor der Bereitstellung

Stellen Sie sicher, dass den Incident-Respondern vorab der richtige Zugriff zugewiesen wurde, um den Zeitaufwand für die Untersuchung AWS bis zur Wiederherstellung zu reduzieren.

Typische Anti-Muster:

- Verwendung des Root-Kontos für die Reaktion auf Vorfälle
- Veränderung bestehender Benutzerkonten
- Direktes Manipulieren von IAM Berechtigungen bei der Gewährung von Rechteerweiterungen just-in-time

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Mittel

### Implementierungsleitfaden

AWS empfiehlt, die Abhängigkeit von langlebigen Anmeldeinformationen, wo immer möglich, zu reduzieren oder ganz zu vermeiden und stattdessen temporäre Anmeldeinformationen und Mechanismen zur just-in-time Rechteerweiterung zu verwenden. Langlebige Anmeldeinformationen sind ein potenzielles Sicherheitsrisiko und erhöhen den Verwaltungsaufwand. Für die meisten Verwaltungsaufgaben und für die Reaktion auf Vorfälle empfehlen wir die Implementierung eines [Identitätsverbunds](#) zusammen mit einer [temporären Eskalierung für Administratorzugriff](#). In diesem Modell beantragt ein Benutzer eine höhere Berechtigungsstufe (etwa für eine Vorfalldarstellungsrolle). Anschließend wird, sofern der Benutzer grundsätzlich dafür infrage kommt, eine entsprechende Anforderung an einen Genehmiger gesendet. Wenn die Anforderung genehmigt wurde, erhält der Benutzer temporäre [AWS -Anmeldeinformationen](#) für die Durchführung seiner Aufgaben. Nach Ablauf dieser Anmeldeinformationen muss der Benutzer eine neue Erhöhungsanforderung übermitteln.

Wir empfehlen für die meisten Vorfalldarstellungsszenarien die Verwendung temporärer Berechtigungseskalierungen. Die korrekte Vorgehensweise ist die Verwendung von [AWS Security Token Service](#) und [Sitzungsrichtlinien](#) zur Festlegung der Zugriffsbereiche.

Es gibt Szenarien, in denen Verbundidentitäten nicht verfügbar sind. Hier ein paar Beispiele:

- Ausfall im Zusammenhang mit einem kompromittierten Identitätsanbieter (IdP)
- Durch fehlerhafte Konfiguration oder menschlichen Fehler beeinträchtigt Management-System für den Verbundzugriff

- Böswillige Aktivitäten wie ein Distributed-Denial-of-Service (DDoS) -Ereignis oder die Nichtverfügbarkeit des Systems.

Für diese Fälle sollte Notfallzugriff (Break-Glass-Zugriff) konfiguriert werden, um eine Untersuchung und schnelle Behandlung des Vorfalls zu ermöglichen. Wir empfehlen, dass Sie einen [Benutzer, eine Gruppe oder eine Rolle mit den entsprechenden Berechtigungen verwenden](#), um Aufgaben auszuführen und auf Ressourcen zuzugreifen AWS. Verwenden Sie den Root-Benutzer nur für [Aufgaben, die Root-Benutzeranmeldeinformationen erfordern](#). Um sicherzustellen, dass Incident Responder die richtigen Zugriffsrechte auf AWS und andere relevante Systeme haben, empfehlen wir die Vorabbereitstellung von dedizierten Konten. Die Konten benötigen privilegierten Zugriff und müssen streng kontrolliert und überwacht werden. Die Konten müssen mit den geringstmöglichen Berechtigungen versehen sein, die für die erforderlichen Aufgaben benötigt werden, und die Zugriffsstufe muss auf den Playbooks basieren, die im Rahmen des Vorfallmanagementplans erstellt werden.

Verwenden Sie als bewährte Methode zweckgerichtet erstellte und dedizierte Benutzer und Rollen. Durch die vorübergehende Ausweitung des Benutzer- oder Rollenzugriffs durch das Hinzufügen von IAM Richtlinien ist nicht klar, welchen Zugriff die Benutzer während des Vorfalls hatten, und es besteht auch die Gefahr, dass die eskalierten Rechte nicht entzogen werden.

Es ist wichtig, möglichst viele Abhängigkeiten zu entfernen, um sicherzustellen, dass in einem möglichst großen Spektrum von Ausfallszenarien zugegriffen werden kann. Um dies zu unterstützen, sollten Sie ein Playbook erstellen, das sicherstellt, dass Incident-Response-Benutzer als Benutzer mit einem eigenen Sicherheitskonto erstellt werden und nicht über eine bestehende Federation- oder Single Sign-On () -Lösung verwaltet werden. SSO Alle einzelnen Mitglieder von Notfallteams müssen über ein eigenes benanntes Konto verfügen. Bei der Kontokonfiguration müssen [strenge Kennwortrichtlinien](#) und eine mehrstufige Authentifizierung () durchgesetzt werden. MFA Wenn für die Playbooks zur Reaktion auf Incident Response nur Zugriff auf die erforderlich ist AWS Management Console, sollten für den Benutzer keine Zugriffsschlüssel konfiguriert sein und es sollte ihm ausdrücklich untersagt werden, Zugriffsschlüssel zu erstellen. Dies kann mit IAM Richtlinien oder Dienststeuerungsrichtlinien (SCPs) konfiguriert werden, wie unter Bewährte AWS Sicherheitsmethoden für beschrieben. [AWS Organizations SCPs](#) Mit Ausnahme der Möglichkeit zur Übernahme von Vorfallreaktionsrollen in anderen Konten sollten die Benutzer über keinerlei Berechtigungen verfügen.

Während eines Vorfalls kann es erforderlich sein, anderen internen oder externen Personen Zugriff zu gewähren, um Untersuchungs-, Korrektur- oder Wiederherstellungsaktivitäten zu unterstützen. Verwenden Sie in diesem Fall den vorher erwähnten Playbook-Mechanismus. Darüber hinaus



muss ein Prozess vorhanden sein, um sicherzustellen, dass jeglicher zusätzlicher Zugriff sofort nach Abschluss des Vorfalls widerrufen wird.

Um sicherzustellen, dass der Einsatz von Incident-Response-Rollen ordnungsgemäß überwacht und geprüft werden kann, ist es wichtig, dass die zu diesem Zweck erstellten IAM Konten nicht von Einzelpersonen gemeinsam genutzt werden und dass sie nur verwendet werden, wenn sie [für eine bestimmte Aufgabe erforderlich](#) sind. Root-Benutzer des AWS-Kontos Wenn der Root-Benutzer erforderlich ist (z. B. wenn der IAM Zugriff auf ein bestimmtes Konto nicht verfügbar ist), überprüfen Sie anhand eines separaten Verfahrens die Verfügbarkeit der Anmeldedaten und des Tokens des Root-Benutzers. MFA

Um die IAM Richtlinien für die Rollen zur Reaktion auf Vorfälle zu konfigurieren, sollten Sie in Erwägung ziehen, [IAMAccess Analyzer](#) zu verwenden, um Richtlinien auf AWS CloudTrail der Grundlage von Protokollen zu generieren. Gewähren Sie dazu der Vorfalldatenrolle in einem Nicht-Produktionskonto Administratorzugriff und durchlaufen Sie Ihre Playbooks. Anschließend kann eine Richtlinie erstellt werden, die nur die ausgeführten Aktionen zulässt. Diese Richtlinie kann dann auf alle Vorfalldatenrollen über alle Konten hinweg angewendet werden. Möglicherweise möchten Sie für jedes Playbook eine separate IAM Richtlinie erstellen, um die Verwaltung und Prüfung zu vereinfachen. Beispiel-Playbooks können Reaktionspläne für Ransomware-Angriffe, Datenschutzverletzungen, Verlust von produktionsrelevantem Zugriff oder andere Szenarien enthalten.

Verwenden Sie die Incident-Response-Konten, um spezielle [IAM Aufgaben im Bereich Incident Response in anderen AWS-Konten Bereichen](#) zu übernehmen. Diese Rollen müssen so konfiguriert werden, dass sie nur von Benutzern im Sicherheitskonto übernommen werden können, und die Vertrauensstellung muss voraussetzen, dass sich der aufrufende Prinzipal über authentifiziert hat. MFA Für die Rollen müssen eng begrenzte Richtlinien zur Zugriffskontrolle verwendet werden. Stellen Sie sicher, dass alle AssumeRole Anfragen für diese Rollen angemeldet sind und dass Benachrichtigungen angezeigt werden CloudTrail und dass alle Aktionen, die mit diesen Rollen ausgeführt werden, protokolliert werden.

Es wird dringend empfohlen, dass sowohl die IAM Konten als auch die IAM Rollen eindeutig benannt sind, damit sie in den CloudTrail Protokollen leicht auffindbar sind. Ein Beispiel hierfür wäre die Benennung der IAM Konten `<USER_ID>-BREAK-GLASS` und IAM Rollen `BREAK-GLASS-ROLE`.

[CloudTrail](#) wird verwendet, um API Aktivitäten in Ihren AWS Konten zu protokollieren und sollte verwendet werden, um [Benachrichtigungen zur Nutzung der Incident-Response-Rollen zu konfigurieren](#). Weitere Informationen finden Sie im Blog-Beitrag zur Konfiguration von Warnungen bei Verwendung von Root-Schlüsseln. Die Anweisungen können geändert werden, um die

[CloudWatchAmazon-Metrik](#) für AssumeRole Ereignisse filter-to-filter im Zusammenhang mit der IAM Rolle „Incident Response“ zu konfigurieren:

```
{ $.eventName = "AssumeRole" && $.requestParameters.roleArn =  
  "<INCIDENT_RESPONSE_ROLE_ARN>" && $.userIdentity.invokedBy NOT EXISTS && $.eventType !=  
  "AwsServiceEvent" }
```

Da die Vorfalldatenrollen sehr wahrscheinlich eine hohe Zugriffsstufe haben, ist es wichtig, dass diese Warnungen an eine weit gefasste Gruppe gesendet werden und dass umgehend auf sie reagiert wird.

Während eines Vorfalls ist es möglich, dass ein Responder Zugriff auf Systeme benötigt, die nicht direkt durch IAM gesichert sind. Dazu könnten Amazon Elastic Compute Cloud-Instances, Amazon Relational Database Service Service-Datenbanken oder software-as-a-service (SaaS) - Plattformen gehören. Es wird dringend empfohlen, für den gesamten administrativen Zugriff auf EC2 Amazon-Instances anstelle von systemeigenen Protokollen wie SSH oder RDP zu verwenden. [AWS Systems Manager Session Manager](#) Dieser Zugriff kann über IAM eine sichere und geprüfte Methode gesteuert werden. Gegebenenfalls ist es auch möglich, Teile Ihrer Playbooks mithilfe von [Run-Command-Dokumenten von AWS Systems Manager](#) zu automatisieren, um Benutzerfehler zu reduzieren und die Wiederherstellung zu beschleunigen. Für den Zugriff auf Datenbanken und Tools von Drittanbietern empfehlen wir, die Zugangsdaten in den Rollen der Incident-Responder zu speichern AWS Secrets Manager und ihnen Zugriff zu gewähren.

Schließlich sollte die Verwaltung der IAM Incident-Response-Konten zu Ihren [Joiners-, Movers- und Leavers-Prozessen hinzugefügt und regelmäßig überprüft und getestet werden](#), um sicherzustellen, dass nur der vorgesehene Zugriff erlaubt ist.

Ressourcen

Zugehörige Dokumente:

- [Verwaltung des temporären erhöhten Zugriffs auf Ihre Umgebung AWS](#)
- [AWS Leitfaden zur Reaktion auf Sicherheitsvorfälle](#)
- [AWS Elastic Disaster Recovery](#)
- [AWS Systems Manager Incident Manager](#)
- [Einrichtung einer Kontokennwortrichtlinie für IAM Benutzer](#)
- [Verwenden der Multi-Faktor-Authentifizierung \(MFA\) in AWS](#)
- [Konfiguration des kontoübergreifenden Zugriffs mit MFA](#)

- [Verwenden von IAM Access Analyzer zum Generieren von Richtlinien IAM](#)
- [Bewährte Methoden für AWS Organizations Service Control-Richtlinien in einer Umgebung mit mehreren Konten](#)
- [So erhalten Sie Benachrichtigungen, wenn die Root-Zugriffsschlüssel Ihres AWS Kontos verwendet werden](#)
- [Erstellen Sie mithilfe IAM verwalteter Richtlinien detaillierte Sitzungsberechtigungen](#)

Zugehörige Videos:

- [Automatisierung der Reaktion auf Vorfälle und der Forensik in AWS](#)
- [DIYLeitfaden zu Runbooks, Incident-Reports und Incident-Response](#)
- [Bereiten Sie sich auf Sicherheitsvorfälle in Ihrer AWS Umgebung vor und reagieren Sie darauf](#)

Zugehörige Beispiele:

- [Lab: AWS Kontoeinrichtung und Root-Benutzer](#)
- [Labor: Reaktion auf Vorfälle mit AWS Konsole und CLI](#)

SEC10-BP06 Tools vor der Bereitstellung

Stellen Sie sicher, dass Sicherheitspersonal über die richtigen Tools verfügt, um die Zeit von der Untersuchung bis zur Wiederherstellung zu verkürzen.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel

Implementierungsleitfaden

Zur Automatisierung von Sicherheits-, Reaktions- und Betriebsfunktionen können Sie eine umfassende Palette von Tools von APIs verwenden. AWS Sie können die Identitätsverwaltung, die Netzwerksicherheit, den Datenschutz und Überwachungsfunktionen vollständig automatisieren und mithilfe gängiger Softwareentwicklungsmethoden bereitstellen, die Sie bereits eingerichtet haben. Durch die Sicherheitsautomatisierung kann Ihr System Überwachungs- und Überprüfungsaufgaben übernehmen und eine Reaktion initiieren (im Gegensatz zur manuellen Überwachung der Sicherheitslage und manuellen Reaktion auf Ereignisse).

Wenn Ihre Vorfallreaktionsteams weiterhin auf die gleiche Weise auf Warnungen reagieren, werden Warnungen möglicherweise nicht mehr ernst genommen. Im Laufe der Zeit kann das Team für

Warnungen desensibilisiert werden und entweder Fehler bei der Verarbeitung normaler Situationen machen oder außergewöhnliche Warnungen übersehen. Automatisierung hilft, eine Abstumpfung gegenüber Warnungen zu vermeiden, indem Funktionen verwendet werden, die repetitive und gewöhnliche Warnungen verarbeiten, sodass Mitarbeiter die nötigen freien Kapazitäten haben, um sich um sensible und besondere Vorfälle zu kümmern. Durch die Integration von Systemen zur Erkennung von Anomalien wie Amazon GuardDuty, AWS CloudTrail Insights und Amazon CloudWatch Anomaly Detection kann die Belastung durch häufig auftretende schwellenwertbasierte Warnmeldungen reduziert werden.

Sie können manuelle Prozesse verbessern, indem Sie die Schritte im Prozess programmatisch automatisieren. Nachdem Sie das Korrekturmuster für ein Ereignis definiert haben, können Sie dieses Muster in umsetzbare Logik zerlegen und den Code schreiben, um diese Logik auszuführen. Notfallteams können anschließend diesen Code ausführen, um das Problem zu beheben. Mit der Zeit können Sie immer mehr Schritte automatisieren und schließlich häufige Vorfälle automatisch behandeln.

Bei einer Sicherheitsuntersuchung müssen Sie relevante Protokolle heranziehen können, um alle Aspekte und den Zeitrahmen des Vorfalls zu verstehen. Protokolle werden auch für die Generierung von Warnungen benötigt, die auf bestimmte Ereignisse aufmerksam machen. Es ist sehr wichtig, Abfrage- und Abrufmechanismen auszuwählen, zu aktivieren, zu speichern und einzurichten sowie die Alarmierung einzurichten. Darüber hinaus stellt [Amazon Detective](#) eine effektive Möglichkeit zur Bereitstellung von Tools zum Durchsuchen von Protokolldaten dar.

AWS bietet über 200 Cloud-Dienste und Tausende von Funktionen. Wir empfehlen Ihnen, die Services zu überprüfen, die Ihre Strategie zur Vorfalldiagnose unterstützen und vereinfachen können.

Zusätzlich zur Protokollierung sollten Sie eine [Markierungsstrategie](#) entwickeln und implementieren. Tagging kann dabei helfen, den Kontext rund um den Zweck einer Ressource bereitzustellen. AWS Die Markierung kann auch für die Automatisierung verwendet werden.

## Implementierungsschritte

### Auswählen und Einrichten von Protokollen für die Analyse und Alarmierung

In der folgenden Dokumentation finden Sie Informationen zur Konfiguration der Protokollierung für die Vorfalldiagnose:

- [Protokollierungsstrategien für die Reaktion auf Sicherheitsvorfälle](#)
- [SEC04-BP01 Dienst- und Anwendungsprotokollierung konfigurieren](#)

## Aktivieren von Sicherheits-Services zur Unterstützung von Erkennung und Reaktion

AWS bietet native Erkennungs-, Präventions- und Reaktionsfunktionen, und andere Dienste können zur Entwicklung maßgeschneiderter Sicherheitslösungen genutzt werden. Eine Liste der wichtigsten Services für die Reaktion auf Sicherheitsvorfälle finden Sie unter [Definitionen der Cloud-Funktionen](#).

## Entwickeln und Implementieren einer Markierungsstrategie

Es kann schwierig sein, Kontextinformationen zum geschäftlichen Anwendungsfall und zu relevanten internen Stakeholdern rund um eine AWS Ressource zu erhalten. Eine Möglichkeit, dies zu tun, sind Tags, die Ihren AWS Ressourcen Metadaten zuweisen und aus einem benutzerdefinierten Schlüssel und Wert bestehen. Sie können Tags erstellen, um Ressourcen nach Zweck, Besitzer, Umgebung, Art der verarbeiteten Daten und anderen Kriterien Ihrer Wahl zu kategorisieren.

Eine konsistente Tagging-Strategie kann die Reaktionszeiten beschleunigen und den Zeitaufwand für den Unternehmenskontext minimieren, da Sie kontextbezogene Informationen zu einer Ressource schnell identifizieren und erkennen können. AWS Tags können auch als Mechanismus zur Initiierung von Reaktionsautomatisierungen dienen. [Weitere Informationen darüber, was Sie taggen sollten, finden Sie unter Ressourcen taggen. AWS](#) Sie sollten zunächst die Tags definieren, die Sie in Ihrer Organisation implementieren möchten. Anschließend können Sie diese Markierungsstrategie implementieren und erzwingen. Weitere Informationen zur Implementierung und Durchsetzung finden Sie unter [Implementieren einer AWS Ressourcen-Tagging-Strategie mithilfe von AWS Tag-Richtlinien und Service Control-Richtlinien \(\) SCPs](#).

## Ressourcen

Zugehörige bewährte Methoden für Well-Architected:

- [SEC04-BP01 Dienst- und Anwendungsprotokollierung konfigurieren](#)
- [SEC04-BP02 Erfassen von Protokollen, Ergebnissen und Kennzahlen an standardisierten Orten](#)

Zugehörige Dokumente:

- [Protokollierungsstrategien für die Reaktion auf Sicherheitsvorfälle](#)
- [Definitionen der Cloud-Funktionen für die Vorfalldreaktion](#)

Zugehörige Beispiele:

- [Erkennung und Reaktion auf Bedrohungen mit Amazon GuardDuty und Amazon Detective](#)

- [Security-Hub-Workshop](#)
- [Management von Schwachstellen mit Amazon Inspector](#)

## SEC10-BP07 Simulationen ausführen

Organisationen wachsen und entwickeln sich weiter. Gleiches gilt auch für die Bedrohungslandschaft. Daher ist es wichtig, Ihre Fähigkeiten zur Vorfalldreaktion kontinuierlich zu überprüfen. Die Durchführung von Simulationen (auch bekannt als Gamedays) ist eine Methode, mit der diese Bewertung durchgeführt werden kann. Simulationen verwenden reale Sicherheitsereignis-Szenarien, die darauf ausgelegt sind, die Taktiken, Techniken und Verfahren eines Bedrohungsakteurs nachzuahmen (TTPs) und es einer Organisation zu ermöglichen, ihre Fähigkeiten zur Reaktion auf Vorfälle auszuüben und zu bewerten, indem sie auf diese simulierten Cyberereignisse so reagieren, wie sie in der Realität auftreten könnten.

Vorteile der Nutzung dieser bewährten Methode: Simulationen haben eine Vielzahl von Vorteilen:

- Validierung der Cybersicherheit und Stärkung des Vertrauens Ihres Vorfalldreaktionsteams
- Testen der Genauigkeit und Effizienz von Tools und Workflows
- Optimierung der Kommunikations- und Eskalationsmethoden Ihres Vorfalldreaktionsplans
- Möglichkeit, auf weniger verbreitete Vektoren zu reagieren

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel

## Implementierungsleitfaden

Es gibt drei Hauptarten von Simulationen:

- **Tabletop-Übungen:** Beim Tabletop-Ansatz für Simulationen handelt es sich um eine Diskussionsrunde, an der die verschiedenen, mit der Vorfalldreaktion betrauten Stakeholder teilnehmen, um Rollen und Verantwortlichkeiten zu üben und etablierte Kommunikationstools und Playbooks zu verwenden. Die Übung kann in der Regel an einem ganzen Tag sowie an einem virtuellen und/oder physischen Ort durchgeführt werden. Da sie auf Diskussionen basiert, konzentriert sich die Tabletop-Übung auf Prozesse, Menschen und Zusammenarbeit. Technologie ist ein integraler Bestandteil der Diskussion, aber der tatsächliche Einsatz von Tools oder Skripten für die Vorfalldreaktion ist in der Regel kein Teil der Tabletop-Übung.
- **Übungen des lila Teams:** Übungen des lila Teams verbessern die Zusammenarbeit zwischen dem Vorfalldreaktionsteam (blaues Team) und den simulierten Bedrohungsakteuren (rotes Team).

Das blaue Team besteht aus Mitgliedern des Security Operations Center (SOC), kann aber auch andere Beteiligte einbeziehen, die während eines tatsächlichen Cyberereignisses involviert wären. Das rote Team besteht aus einem Penetrationstest-Team oder wichtigen Stakeholdern, die in offensiver Sicherheit geschult sind. Das rote Team arbeitet bei der Planung eines Szenarios mit den Übungsleitern zusammen, damit das Szenario korrekt und durchführbar ist. Bei den Übungen im violetten Team liegt das Hauptaugenmerk auf den Erkennungsmechanismen, den Tools und den Standardarbeitsanweisungen (SOPs), mit denen die Maßnahmen zur Reaktion auf Vorfälle unterstützt werden.

- **Übungen des roten Teams:** Bei einer Übung des roten Teams führt das Offensivteam (rotes Team) eine Simulation durch, um ein bestimmtes Ziel oder eine Reihe von Zielen aus einem vorher festgelegten Bereich zu erreichen. Die Verteidiger (blaues Team) kennen nicht unbedingt den Umfang und die Dauer der Übung, was eine realistischere Einschätzung darüber ermöglicht, wie sie auf einen tatsächlichen Vorfall reagieren würden. Da es sich bei den Übungen des roten Teams um invasive Tests handeln kann, sollten Sie vorsichtig sein und Kontrollen implementieren, um sicherzustellen, dass die Übung Ihrer Umgebung nicht tatsächlich schadet.

Erwägen Sie, in regelmäßigen Abständen Cybersimulationen durchzuführen. Jeder Übungstyp kann den Teilnehmern und der gesamten Organisation einzigartige Vorteile bieten. Sie können also etwa mit weniger komplexen Simulationstypen beginnen (beispielsweise mit Tabletop-Übungen) und dann zu komplexeren Simulationstypen übergehen (Übungen des roten Teams). Wählen Sie auf der Grundlage Ihres Sicherheitsreifegrads, Ihrer Ressourcen und der gewünschten Ergebnisse einen Simulationstyp aus. Einige Kunden entscheiden sich aufgrund der Komplexität und der Kosten möglicherweise gegen Übungen des roten Teams.

### Implementierungsschritte

Unabhängig von der Art der gewählten Simulation folgen diese im Allgemeinen den folgenden Implementierungsschritten:

1. **Definieren Sie die wichtigsten Übungselemente:** Definieren Sie das Simulationsszenario und die Ziele der Simulation. Beide sollten von der Führungsebene akzeptiert werden.
2. **Identifizieren Sie die wichtigsten Stakeholder:** Für eine Übung sind mindestens Übungsleiter und Teilnehmer erforderlich. Je nach Szenario können gegebenenfalls weitere Stakeholder einbezogen werden – etwa aus der Rechts- oder Kommunikationsabteilung oder aus der Geschäftsleitung.
3. **Erstellen und testen Sie das Szenario:** Das Szenario muss möglicherweise während der Erstellung neu definiert werden, falls bestimmte Elemente nicht realisierbar sind. Als Ergebnis dieser Phase wird ein fertiges Szenario erwartet.

4. Führen Sie die Simulation durch: Die Art der Simulation bestimmt die Durchführung (ein Szenario auf Papier im Vergleich zu einem hochtechnischen, simulierten Szenario). Die Übungsleiter sollten ihre Taktiken an den Übungsobjekten ausrichten und alle Übungsteilnehmer nach Möglichkeit einbeziehen, um den größtmöglichen Nutzen zu erzielen.
5. Entwickeln Sie den Bericht über die Folgemaßnahmen (AAR): Identifizieren Sie Bereiche, die gut gelaufen sind, Bereiche, in denen Verbesserungen erforderlich sind, und mögliche Lücken. Sie AAR sollten die Effektivität der Simulation sowie die Reaktion des Teams auf das simulierte Ereignis messen, sodass der Fortschritt im Laufe der Zeit mit future Simulationen verfolgt werden kann.

## Ressourcen

### Zugehörige Dokumente:

- [AWS Leitfaden zur Reaktion auf Vorfälle](#)

### Zugehörige Videos:

- [AWS GameDay - Sicherheitsausgabe](#)

## SEC10-BP08 Schaffen Sie einen Rahmen, um aus Vorfällen zu lernen

Die Implementierung eines Erkenntnis-Frameworks und einer Ursachenanalyse kann nicht nur zur Verbesserung der Reaktion auf Vorfälle, sondern auch zur Verhinderung einer Wiederholung des Vorfalls beitragen. Durch das Lernen aus Vorfällen können Sie verhindern, dass sich die gleichen Fehler, Risiken oder Fehlkonfigurationen wiederholen. Dies verbessert nicht nur Ihre Sicherheitslage, sondern minimiert auch den Zeitverlust durch vermeidbare Situationen.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel

## Implementierungsleitfaden

Es ist wichtig, ein Erkenntnis-Framework zu implementieren, das ganz allgemein Folgendes ermittelt und erreicht:

- Wann kommt es zu Erkenntnissen?
- Was beinhaltet der Erkenntnisprozess?
- Wie werden Erkenntnisse gewonnen?



- Wer ist auf welche Weise an dem Prozess beteiligt?
- Wie werden verbesserungswürdige Bereiche identifiziert?
- Wie stellen Sie sicher, dass Verbesserungen effektiv verfolgt und implementiert werden?

Das Framework sollte sich nicht auf Einzelpersonen konzentrieren oder ihnen die Schuld geben, sondern stattdessen den Fokus auf die Verbesserung der Tools und Prozesse legen.

### Implementierungsschritte

Abgesehen von den zuvor aufgeführten Ergebnissen auf hoher Ebene ist es wichtig, sicherzustellen, dass Sie die richtigen Fragen stellen, um den größtmöglichen Nutzen (Informationen, die zu umsetzbaren Verbesserungen führen) aus dem Prozess zu ziehen. Berücksichtigen Sie die folgenden Fragen, um Ihre Diskussionen über Erkenntnisse zu fördern:

- Was ist vorgefallen?
- Wann wurde der Vorfall zum ersten Mal identifiziert?
- Wie wurde er identifiziert?
- Von welchen Systemen wurde eine Warnung im Zusammenhang mit der Aktivität ausgegeben?
- Welche Systeme, Services und Daten waren beteiligt?
- Was ist konkret passiert?
- Was hat gut funktioniert?
- Was hat nicht gut funktioniert?
- Welcher Prozess oder welche Verfahren haben versagt oder konnten nicht skaliert werden, um auf den Vorfall zu reagieren?
- Was kann in den folgenden Bereichen verbessert werden:
  - Personen
    - Waren die Mitarbeiter, die kontaktiert werden mussten, tatsächlich verfügbar und war die Kontaktliste auf dem neuesten Stand?
    - Fehlten den Mitarbeitern Schulungen oder Fähigkeiten, die erforderlich waren, um effektiv auf den Vorfall reagieren und ihn untersuchen zu können?
    - Waren die erforderlichen Ressourcen bereit und verfügbar?
  - Prozess
    - Wurden Prozesse und Verfahren eingehalten?

- Waren Prozesse und Verfahren für diesen Vorfall bzw. für diese Art von Vorfall dokumentiert und verfügbar?
- Fehlten erforderliche Prozesse und Verfahren?
- Konnten die Notfallteams rechtzeitig auf die erforderlichen Informationen zugreifen, um auf das Problem zu reagieren?
- Technologie
  - Haben die bestehenden Warnsysteme die Aktivität effektiv identifiziert und gemeldet?
  - Wie hätten wir das um 50 time-to-detection% reduzieren können?
  - Müssen bestehende Warnungen verbessert oder neue Warnungen für diesen Vorfall bzw. für diese Art von Vorfall erstellt werden?
  - War mit den vorhandenen Tools eine effektive Untersuchung (Suche/Analyse) des Vorfalls möglich?
  - Was kann getan werden, um diesen Vorfall bzw. diese Art von Vorfall früher zu erkennen?
  - Was kann getan werden, um zu verhindern, dass sich dieser Vorfall bzw. diese Art von Vorfall wiederholt?
  - Wer ist für den Verbesserungsplan zuständig und wie testen Sie, ob er implementiert wurde?
  - Wie sieht der Zeitplan für die Implementierung und das Testen zusätzlicher Überwachungen oder präventiver Kontrollen und Prozesse aus?

Diese Liste ist nicht vollständig. Sie soll jedoch als Ausgangspunkt dienen, um zu ermitteln, was die Organisations- und Geschäftsanforderungen sind und wie Sie diese analysieren können, um am effektivsten aus Vorfällen zu lernen und Ihre Sicherheitslage kontinuierlich zu verbessern. Am wichtigsten ist, damit zu beginnen und Erkenntnisse standardmäßig in Ihren Prozess zur Vorfallreaktion, in die Dokumentation und in die Erwartungen der Stakeholder zu integrieren.

## Ressourcen

### Zugehörige Dokumente:

- [AWS -Leitfaden für die Reaktion auf Sicherheitsvorfälle – Entwickeln eines Frameworks, um aus Vorfällen zu lernen](#)
- [NCSCCAFBeratung — gewonnene Erkenntnisse](#)

# Anwendungssicherheit

## Frage

- [SEC11. Wie beziehen Sie die Sicherheitseigenschaften von Anwendungen während des gesamten Entwurfs-, Entwicklungs- und Bereitstellungslebenszyklus ein und validieren sie?](#)

SEC11. Wie beziehen Sie die Sicherheitseigenschaften von Anwendungen während des gesamten Entwurfs-, Entwicklungs- und Bereitstellungslebenszyklus ein und validieren sie?

Das Schulen von Personen, das Testen mithilfe von Automatisierung, ein Verständnis der Abhängigkeiten und die Validierung der Sicherheitseigenschaften von Tools und Anwendungen helfen dabei, die Wahrscheinlichkeit eines Sicherheitsproblems bei Produktions-Workloads zu verringern.

## Bewährte Methoden

- [SEC11-BP01 Train für Anwendungssicherheit](#)
- [SEC11-BP02 Automatisieren Sie Tests während des gesamten Entwicklungs- und Release-Lebenszyklus](#)
- [SEC11-BP03 Führen Sie regelmäßige Penetrationstests durch](#)
- [SEC11-BP04 Manuelle Code-Bewertungen](#)
- [SEC11-BP05 Dienste für Pakete und Abhängigkeiten zentralisieren](#)
- [SEC11-BP06 Software programmgesteuert bereitstellen](#)
- [SEC11-BP07 Beurteilen Sie regelmäßig die Sicherheitseigenschaften der Pipelines](#)
- [SEC11-BP08 Entwickeln Sie ein Programm, das die Verantwortung für Sicherheitsfragen in Workload-Teams einbettet](#)

## SEC11-BP01 Train für Anwendungssicherheit

Bieten Sie den Entwicklern in Ihrer Organisation Schulungsmöglichkeiten zu allgemeinen Praktiken für die sichere Entwicklung und den sicheren Betrieb von Anwendungen. Die Einführung sicherheitsbezogener Entwicklungsmethoden trägt dazu bei, die Wahrscheinlichkeit von Problemen zu verringern, die erst während der Phase der Sicherheitsüberprüfung erkannt werden.

Gewünschtes Ergebnis: Beim Entwerfen und Entwickeln von Software sollten Sicherheitsaspekte berücksichtigt werden. Wenn Entwickler in einer Organisation hinsichtlich sicherer Entwicklungspraktiken, die mit einem Bedrohungsmodell beginnen, geschult sind, wird die gesamte Qualität und Sicherheit der entwickelten Software verbessert. Mithilfe dieses Ansatzes kann die Zeit bis zur Auslieferung von Software oder Funktionen verringert werden, da der Überarbeitungsaufwand nach Sicherheitsüberprüfungen geringer ist.

Für die Zwecke dieser bewährten Methode bezieht sich sichere Entwicklung auf die Software, die gerade geschrieben wird, und auf die Tools oder Systeme, die den Softwareentwicklungszyklus unterstützen (SDLC).

Typische Anti-Muster:

- Auf eine Sicherheitsüberprüfung warten und dann die Sicherheitseigenschaften eines Systems berücksichtigen
- Alle sicherheitsbezogenen Entscheidungen dem Sicherheitsteam überlassen
- Versäumnis, zu kommunizieren, wie SDLC sich die im Rahmen der getroffenen Entscheidungen auf die allgemeinen Sicherheitserwartungen oder -richtlinien der Organisation beziehen.
- Den Sicherheitsüberprüfungsprozess zu spät nutzen

Vorteile der Nutzung dieser bewährten Methode:

- Bessere Kenntnis der Unternehmensanforderungen hinsichtlich der Sicherheit frühzeitig im Entwicklungszyklus
- Schnellere Auslieferung von Funktionen durch schnelles Identifizieren und Lösen potenzieller Sicherheitsprobleme
- Verbesserte Qualität von Software und Systemen

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel

Implementierungsleitfaden

Stellen Sie Schulungen für Entwickler in Ihrer Organisation bereit. Ein Kurs über [Bedrohungsmodellierung](#) ist ein guter Start, um einen Grundstein für Sicherheitsschulungen zu legen. Im Idealfall sollten Entwickler selbständig auf die Informationen zugreifen können, die für ihre Workloads relevant sind. Dieser Zugriff hilft ihnen dabei, fundierte Entscheidungen im Zusammenhang mit den Sicherheitseigenschaften der Systeme zu treffen, die sie entwickelt

haben, ohne ein anderes Team kontaktieren zu müssen. Der Prozess für die Einbindung des Sicherheitsteams in Überprüfungen sollte klar definiert und einfach umsetzbar sein. Die Schritte des Überprüfungsprozesses sollten Inhalt der Sicherheitsschulung sein. Wenn bekannte Implementierungsmuster oder Vorlagen verfügbar sind, sollten sie einfach zu finden und mit den allgemeinen Sicherheitsanforderungen verknüpft sein. Erwägen Sie, [AWS CloudFormation](#), [AWS Cloud Development Kit \(AWS CDK\) -Konstrukte](#), [Service Catalog](#) oder andere Vorlagen-Tools zu verwenden, um weniger benutzerspezifische Konfigurationen zu benötigen.

### Implementierungsschritte

- Stellen Sie einen Kurs über [Bedrohungsmodellierung](#) für Entwickler bereit. Dies ist eine gute Grundlage und trägt dazu bei, sie für Sicherheitsüberlegungen zu schulen.
- Bieten Sie Zugang zu [Zertifizierungs AWS Training](#) -, Branchen- oder AWS Partnerschulungen an.
- Bieten Sie Schulungen zum Sicherheitsüberprüfungsprozess Ihrer Organisation an, die die Aufteilung von Verantwortlichkeiten zwischen Sicherheitsteams, Workload-Teams und anderen Beteiligten deutlich machen.
- Veröffentlichen Sie Self-Service-Anweisungen zur Erfüllung von Sicherheitsanforderungen, einschließlich Codebeispielen und Vorlagen, wenn verfügbar.
- Holen Sie regelmäßig Feedback von Entwicklerteams zu ihrer Erfahrung mit dem Sicherheitsüberprüfungsprozess und den Schulungen ein und verwenden Sie dieses Feedback, um Verbesserungen zu implementieren.
- Führen Sie Simulationen (Gamedays) oder Kampagnen zur Beseitigung von Bugs durch, um die Anzahl von Fehlern zu verringern und die Fähigkeiten Ihrer Entwickler auszuweiten.

### Ressourcen

Zugehörige bewährte Methoden:

- [SEC11-BP08 Entwickeln Sie ein Programm, das die Verantwortung für Sicherheitsfragen in Workload-Teams einbettet](#)

Zugehörige Dokumente:

- [AWS Training und Zertifizierung](#)
- [Betrachtung der Cloud-Sicherheits-Governance](#)
- [Konzepte für Bedrohungsmodellierung](#)

- [Schnellere Ausbildung — The AWS Skills Guild](#)

Zugehörige Videos:

- [Proaktive Sicherheit: Überlegungen und Ansätze](#)

Zugehörige Beispiele:

- [Workshop zur Bedrohungsmodellierung](#)
- [Branchenbewusstsein für Entwickler](#)

Zugehörige Services:

- [AWS CloudFormation](#)
- [AWS Cloud Development Kit \(AWS CDK\) \(AWS CDK\) Konstrukte](#)
- [Service Catalog](#)
- [AWS BugBust](#)

SEC11-BP02 Automatisieren Sie Tests während des gesamten Entwicklungs- und Release-Lebenszyklus

Automatisieren Sie das Testen der Sicherheitseigenschaften während des Entwicklungs- und Veröffentlichungslebenszyklus. Automatisierung vereinfacht die kontinuierliche und wiederholbare Identifizierung potenzieller Probleme. Dadurch wird das Risiko von Sicherheitsproblemen in der bereitgestellten Software verringert.

Gewünschtes Ergebnis: Das Ziel von automatisiertem Testen ist, eine programmatische Möglichkeit zur frühen Erkennung von potenziellen Problemen – häufig im Laufe des Entwicklungslebenszyklus – zu bieten. Wenn Sie Regressionstests automatisieren, können Sie funktionale und nicht funktionale Tests erneut durchführen, um zu überprüfen, ob zuvor getestete Software nach einer Änderung weiterhin wie erwartet funktioniert. Wenn Sie Sicherheitstests für Komponenten definieren, um nach häufigen Fehlkonfigurationen zu suchen, wie einer fehlerhaften oder fehlenden Authentifizierung, können Sie diese Fehler früh im Entwicklungsprozess identifizieren und beheben.

Testautomatisierung verwendet speziell entwickelte Testfälle zur Anwendungsvalidierung auf Basis der Anforderungen und der gewünschten Funktionalität der Anwendung. Das Ergebnis

von automatisiertem Testen basiert auf dem Vergleich zwischen der erstellten Testausgabe und der erwarteten Ausgabe, wodurch der gesamte Lebenszyklus des Testens beschleunigt wird. Testmethoden wie Regressionstests und Modultest-Suites eignen sich am besten zur Automatisierung. Durch die Automatisierung des Testens von Sicherheitseigenschaften können Entwickler automatisiertes Feedback erhalten, ohne auf eine Sicherheitsüberprüfung warten zu müssen. Automatisierte Tests in Form von statischer oder dynamischer Codeanalyse können die Qualität von Code erhöhen und dabei helfen, potenzielle Softwareprobleme früh im Entwicklungslebenszyklus zu erkennen.

Typische Anti-Muster:

- Testfälle und Testergebnisse des automatisierten Testens werden nicht kommuniziert.
- Automatisiertes Testen wird erst unmittelbar vor einer Veröffentlichung durchgeführt.
- Testfälle werden mit sich häufig ändernden Anforderungen automatisiert.
- Es wird keine Anleitung für den Umgang mit den Ergebnissen von Sicherheitstests bereitgestellt.

Vorteile der Nutzung dieser bewährten Methode:

- Verringerte Abhängigkeit von Menschen, die die Sicherheitseigenschaften eines Systems evaluieren
- Konsistente Erkenntnisse bei mehreren Arbeitsabläufen für mehr Konsistenz
- Geringere Wahrscheinlichkeit, dass Sicherheitsprobleme in Produktionssoftware gelangen
- Kürzeres Zeitfenster zwischen der Erkennung und Behebung von Softwareproblemen, da sie früher entdeckt werden
- Erhöhte Sichtbarkeit von systemischem oder wiederholtem Verhalten bei mehreren Arbeitsabläufen, dank derer organisationsweite Verbesserungen vorangetrieben werden können

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel

Implementierungsleitfaden

Setzen Sie während der Entwicklung Ihrer Software unterschiedliche Mechanismen für das Testen von Software ein, um sicherzustellen, dass Sie Ihre Anwendung sowohl auf funktionale Anforderungen (basierend auf Ihrer Geschäftslogik) als auch auf nicht funktionale Anforderungen testen, die sich auf die Zuverlässigkeit, Leistung und Sicherheit der Anwendung konzentrieren.

Static Application Security Testing (SAST) analysiert Ihren Quellcode auf ungewöhnliche Sicherheitsmuster und liefert Hinweise auf fehleranfälligen Code. SASTstützt sich auf statische Eingaben wie Dokumentation (Anforderungsspezifikation, Entwurfsdokumentation und Entwurfsspezifikationen) und Anwendungsquellcode, um auf eine Reihe bekannter Sicherheitsprobleme zu testen. Statische Code-Analyzer helfen dabei, die Analyse großer Codemengen zu beschleunigen. Die [NISTQuality Group](#) bietet einen Vergleich von [Source Code Security Analyzers](#), der Open-Source-Tools für [Bytecodescanner](#) und [Binärcodescanner](#) umfasst.

Ergänzen Sie Ihre statischen Tests mit Methoden zur dynamischen Analyse von Sicherheitstests (DAST), bei denen Tests mit der laufenden Anwendung durchgeführt werden, um potenziell unerwartetes Verhalten zu identifizieren. Dynamisches Testen kann verwendet werden, um potenzielle Probleme zu erkennen, die über die statische Analyse nicht gefunden werden können. Das Testen in der Code-Repository-, Build- und Pipeline-Phase ermöglicht es Ihnen, nach unterschiedlichen Arten potenzieller Fehler in Ihrem Code zu suchen. [Amazon CodeWhisperer](#) bietet Codeempfehlungen, einschließlich Sicherheitsscans, im BuilderIDE. [Amazon CodeGuru Reviewer](#) kann kritische Probleme, Sicherheitsprobleme und hard-to-find Bugs während der Anwendungsentwicklung identifizieren und gibt Empfehlungen zur Verbesserung der Codequalität.

Der [Workshop „Sicherheit für Entwickler“](#) verwendet AWS Entwicklertools wie [AWS CodeBuild](#), [AWS CodeCommit](#), [AWS CodePipeline](#), und für die Automatisierung der Release-Pipeline, einschließlich SAST DAST Testmethoden.

Richten Sie im weiteren Verlauf einen iterativen Prozess einSDLC, der regelmäßige Überprüfungen der Anwendungen durch Ihr Sicherheitsteam umfasst. Aus diesen Sicherheitsüberprüfungen gewonnenes Feedback sollte behandelt und im Rahmen der Bereitschaftsüberprüfung Ihrer Softwareversion validiert werden. Diese Überprüfungen schaffen einen robusten Sicherheitsstatus der Anwendungen und bieten Entwicklern umsetzbares Feedback, um Maßnahmen zum Beheben von Problemen zu ergreifen.

### Implementierungsschritte

- Implementieren Sie konsistente IDE Tools zur Codeüberprüfung und CI/CD, die Sicherheitstests beinhalten.
- Überlegen Sie, an welcher Stelle SDLC es angebracht ist, Pipelines zu blockieren, anstatt die Entwickler nur darüber zu informieren, dass Probleme behoben werden müssen.
- Der Workshop [Security for Developers](#) bietet ein Beispiel für die Integration von statischem und dynamischem Testen in eine Veröffentlichungs-Pipeline.



- Die Durchführung von Tests oder Codeanalysen mithilfe automatisierter Tools wie [Amazon](#), die in den Entwickler CodeWhisperer integriert sind IDEs, und [Amazon CodeGuru Reviewer](#) zum Scannen von Code beim Commit, hilft Entwicklern dabei, zum richtigen Zeitpunkt Feedback zu erhalten.
- Beim Erstellen mit AWS Lambda können Sie [Amazon Inspector](#) verwenden, um den Anwendungscode in Ihren Funktionen zu scannen.
- Wenn automatisiertes Testen in CI/CD-Pipelines enthalten ist, sollten Sie ein Ticket-System verwenden, um die Meldung und Behebung von Softwareproblemen nachzuverfolgen.
- Bei Sicherheitstests, die möglicherweise Erkenntnisse liefern, sollten Sie Lösungsanweisungen bereitstellen, damit Entwickler die Codequalität verbessern können.
- Analysieren Sie regelmäßig die Erkenntnisse automatisierter Tools, um die nächste Automatisierung, Entwicklerschulung oder Sensibilisierungskampagne zu planen.

## Ressourcen

### Zugehörige Dokumente:

- [Continuous Delivery und Continuous Deployment](#)
- [AWS DevOps Kompetenzpartner](#)
- [AWS -Kompetenzpartner für Sicherheit](#) für Anwendungssicherheit
- [Auswählen eines Well-Architected-CI/CD-Ansatzes](#)
- [CodeCommit Ereignisse in Amazon EventBridge und Amazon CloudWatch Events überwachen](#)
- [Entdeckung von Geheimnissen in Amazon CodeGuru Review](#)
- [Beschleunigen Sie Implementierungen AWS mit effektiver Steuerung](#)
- [Umgang von AWS mit der Automatisierung sicherer, vollautomatischer Bereitstellungen](#)

### Zugehörige Videos:

- [Vollständige Automatisierung: Automatisieren der Pipelines für kontinuierliche Bereitstellung bei Amazon](#)
- [Automatisieren von kontoübergreifenden CI/CD-Pipelines](#)

### Zugehörige Beispiele:

- [Branchenbewusstsein für Entwickler](#)
- [AWS CodePipeline Verwaltung](#) () GitHub
- [Workshop zur Sicherheit für Entwickler](#)

## SEC11-BP03 Führen Sie regelmäßige Penetrationstests durch

Führen Sie regelmäßige Penetrationstests für Ihre Software durch. Dieser Mechanismus hilft bei der Identifizierung potenzieller Softwareprobleme, die bei automatisierten Tests oder einer manuellen Überprüfung des Codes nicht erkannt werden können. Er kann Ihnen außerdem dabei helfen, die Wirksamkeit Ihrer Erkennungskontrollen zu verstehen. Penetrationstests sollen ermitteln, ob es möglich ist, die Software so zu beeinflussen, dass sie sich unerwartet verhält – etwa, indem sie Daten verfügbar macht, die geschützt sein sollten, oder umfassendere Berechtigungen gewährt als erwartet.

Gewünschtes Ergebnis: Penetrationstests werden zur Erkennung und Behandlung sowie zur Validierung der Sicherheitseigenschaften Ihrer Anwendung verwendet. Im Rahmen des Softwareentwicklungszyklus sollten regelmäßige und geplante Penetrationstests durchgeführt werden (SDLC). Die aus Penetrationstests gewonnenen Erkenntnisse sollten vor der Veröffentlichung der Software behandelt werden. Analysieren Sie die Erkenntnisse von Penetrationstests, um zu ermitteln, ob es sich um Probleme handelt, die mithilfe von Automatisierung gefunden werden können. Ein regelmäßiger und wiederholbarer Prozess für Penetrationstests mit einem aktiven Feedback-Mechanismus fließt in die Anweisungen für Entwickler ein und verbessert die Softwarequalität.

### Typische Anti-Muster:

- Penetrationstests werden nur für bekannte oder weit verbreitete Sicherheitsprobleme verwendet.
- Penetrationstests werden für Anwendungen ohne abhängige Drittanbieter-Tools und -Bibliotheken durchgeführt.
- Penetrationstests werden nur für Paketsicherheitsprobleme durchgeführt und die implementierte Geschäftslogik wird nicht evaluiert.

### Vorteile der Nutzung dieser bewährten Methode:

- Gesteigertes Vertrauen in die Sicherheitseigenschaften der Software vor der Veröffentlichung
- Möglichkeit, bevorzugte Anwendungsmuster zu identifizieren, wodurch die Softwarequalität erhöht wird

- Verbesserte Sicherheitseigenschaften von Software durch eine Feedbackschleife, die früher im Entwicklungszyklus ermittelt, wo Automatisierungen oder zusätzliche Schulungen hilfreich sind

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Hoch

### Implementierungsleitfaden

Penetrationstests sind eine strukturierte Sicherheitstestübung, bei der Szenarien mit geplanten Sicherheitsverstößen zur Erkennung und Behandlung sowie zur Validierung von Sicherheitskontrollen durchgespielt werden. Penetrationstests starten mit einer Erkundung, bei der Daten basierend auf dem aktuellen Design der Anwendung und ihrer Abhängigkeiten gesammelt werden. Eine kuratierte Liste mit sicherheitsspezifischen Testszenarien wird entwickelt und durchlaufen. Der wesentliche Zweck dieser Tests besteht darin, Sicherheitsprobleme in Ihrer Anwendung aufzudecken, die dazu genutzt werden können, unbeabsichtigten Zugriff auf Ihre Umgebung oder unautorisierten Zugriff auf Daten zu erhalten. Sie sollten Penetrationstests durchführen, wenn Sie neue Funktionen einführen oder wenn sich die Funktion oder technische Implementierung Ihrer Anwendung erheblich geändert hat.

Sie sollten in Ihrem Entwicklungslebenszyklus die am besten geeignete Phase bestimmen, um Penetrationstests durchzuführen. Diese Tests sollten so spät stattfinden, dass sich das System nahe am vorgesehenen Veröffentlichungszustand befindet, aber es sollte noch genügend Zeit vorhanden sein, damit Probleme behoben werden können.

### Implementierungsschritte

- Implementieren Sie einen strukturierten Prozess für den Umfang der Penetrationstests. Dieser Prozess sollte auf dem [Bedrohungsmodell](#) basieren, um den Kontext zu wahren.
- Bestimmen Sie den geeigneten Zeitpunkt im Entwicklungszyklus zum Durchführen von Penetrationstests. Penetrationstests sollten dann erfolgen, wenn nur noch minimale Anwendungsänderungen zu erwarten sind, aber noch ausreichend Zeit für die Fehlerbehebung übrig ist.
- Schulen Sie Ihre Entwickler hinsichtlich der zu erwartenden Erkenntnisse aus Penetrationstests sowie dahingehend, wie sie Informationen zu deren Behandlung erhalten können.
- Verwenden Sie Tools zur Beschleunigung von Penetrationstests durch Automatisierung gängiger oder wiederholbarer Tests.
- Analysieren Sie Erkenntnisse aus Penetrationstests, um systemische Sicherheitsprobleme zu identifizieren, und verwenden Sie diese Daten, um sie in zusätzliche automatisierte Tests und fortlaufende Entwicklerschulungen einfließen zu lassen.

## Ressourcen

Zugehörige bewährte Methoden:

- [SEC11-BP01 Train für Anwendungssicherheit](#)
- [SEC11-BP02 Automatisieren Sie Tests während des gesamten Entwicklungs- und Release-Lebenszyklus](#)

Zugehörige Dokumente:

- [AWS Penetrationstests](#) bieten detaillierte Anleitungen für Penetrationstests zu AWS
- [Beschleunigen Sie Implementierungen AWS mit effektiver Steuerung](#)
- [AWS -Kompetenzpartner für Sicherheit](#)
- [Modernisieren Sie Ihre Architektur für Penetrationstests auf AWS Fargate](#)
- [AWS Simulator zur Fehlerinjektion](#)

Zugehörige Beispiele:

- [Automatisieren Sie das API Testen mit AWS CodePipeline](#) (GitHub)
- [Automatisierter Sicherheitshelfer](#) (GitHub)

## SEC11-BP04 Manuelle Code-Bewertungen

Führen Sie eine manuelle Codeüberprüfung für die von Ihnen produzierte Software durch. Dieser Prozess stellt sicher, dass die Person, die den Code geschrieben hat, dessen Qualität nicht allein überprüft.

Gewünschtes Ergebnis: Das Hinzufügen einer manuellen Codeüberprüfung während der Entwicklung erhöht die Qualität der geschriebenen Software, hilft dabei, weniger erfahrene Teammitglieder weiterzubilden, und ermöglicht es, Automatisierungsmöglichkeiten zu identifizieren. Manuelle Codeüberprüfungen können von automatisierten Tools und Tests unterstützt werden.

Typische Anti-Muster:

- Vor der Bereitstellung werden keine Codeüberprüfungen durchgeführt.
- Der Code wird von der gleichen Person überprüft, die ihn auch geschrieben hat.

- Es wird keine Automatisierung zur Unterstützung und Orchestrierung von Codeüberprüfungen verwendet.
- Entwickler werden nicht in Anwendungssicherheit geschult, bevor sie Code überprüfen.

Vorteile der Nutzung dieser bewährten Methode:

- Verbesserte Codequalität
- Erhöhte Konsistenz bei der Codeentwicklung durch erneute Verwendung gängiger Ansätze
- Verringerte Anzahl von Schwierigkeiten, die bei Penetrationstests und in späteren Phasen entdeckt werden
- Verbesserter Wissenstransfer innerhalb des Teams

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel

Implementierungsleitfaden

Der Überprüfungsschritt sollte als Teil des allgemeinen Codeverwaltungs-Flows implementiert werden. Die Details hängen von dem Ansatz ab, der für Verzweigen, Pull-Anforderungen und Zusammenführen verwendet wird. Möglicherweise verwendest du AWS CodeCommit oder Lösungen von Drittanbietern wie GitHub, GitLab, oder Bitbucket. Unabhängig von der verwendeten Methode ist es wichtig, sicherzustellen, dass Ihre Prozesse eine Überprüfung von Code erfordern, bevor dieser in einer Produktionsumgebung bereitgestellt wird. Die Verwendung von Tools wie [Amazon CodeGuru Reviewer](#) kann die Orchestrierung des Code-Review-Prozesses erleichtern.

Implementierungsschritte

- Implementieren Sie einen Schritt zur manuellen Überprüfung als Teil Ihres Codeverwaltungs-Flows und führen Sie diese Überprüfung durch, bevor Sie fortfahren.
- Ziehen Sie [Amazon CodeGuru Reviewer](#) für die Verwaltung und Unterstützung von Code-Reviews in Betracht.
- Implementieren Sie einen Genehmigungs-Workflow, bei dem eine Codeüberprüfung erforderlich ist, bevor Code in die nächste Phase übergehen kann.
- Vergewissern Sie sich, dass es einen Prozess gibt, um Probleme zu identifizieren, die bei manuellen Codeüberprüfungen gefunden werden und automatisch erkannt werden könnten.
- Integrieren Sie den Schritt zur manuellen Codeüberprüfung auf eine Weise, die mit Ihren Codeentwicklungspraktiken in Einklang steht.

## Ressourcen

Zugehörige bewährte Methoden:

- [SEC11-BP02 Automatisieren Sie Tests während des gesamten Entwicklungs- und Release-Lebenszyklus](#)

Zugehörige Dokumente:

- [Arbeiten mit Pull-Requests in Repositories AWS CodeCommit](#)
- [Arbeiten mit Vorlagen für Genehmigungsregeln in AWS CodeCommit](#)
- [Informationen zu Pull-Requests in GitHub](#)
- [Automatisieren Sie Code-Reviews mit Amazon CodeGuru Reviewer](#)
- [Automatisierte Erkennung von Sicherheitslücken und Bugs in CI/CD-Pipelines mithilfe von Amazon Reviewer CodeGuru CLI](#)

Zugehörige Videos:

- [Kontinuierliche Verbesserung der Codequalität mit Amazon CodeGuru](#)

Zugehörige Beispiele:

- [Workshop zur Sicherheit für Entwickler](#)

## SEC11-BP05 Dienste für Pakete und Abhängigkeiten zentralisieren

Stellen Sie zentralisierte Services für Entwicklungsteams bereit, sodass sie Softwarepakete und andere Abhängigkeiten erhalten können. Dadurch können Pakete validiert werden, bevor sie in die von Ihnen geschriebene Software integriert werden, und es kann eine Datenquelle für die Analyse der Software bereitgestellt werden, die in Ihrer Organisation verwendet wird.

Gewünschtes Ergebnis: Software umfasst zusätzlich zum geschriebenen Code eine Reihe weiterer Softwarepakete. Dies macht es einfach, Implementierungen von Funktionen zu nutzen, die wiederholt verwendet werden, wie z. B. ein JSON Parser oder eine Verschlüsselungsbibliothek. Das logische Zentralisieren der Quellen und Abhängigkeiten für diese Pakete bietet einen Mechanismus für Sicherheitsteams, mit dem sie die Eigenschaften der Pakete validieren können, bevor sie verwendet werden. Dieser Ansatz verringert auch das Risiko, dass ein unerwartetes Problem durch die

Änderung eines vorhandenen Pakets verursacht wird oder dass Entwicklungsteams willkürlich Pakete direkt aus dem Internet einschließen. Verwenden Sie diesen Ansatz zusammen mit manuellen und automatischen Tests, um das Vertrauen in die Qualität der entwickelten Software zu steigern.

Typische Anti-Muster:

- Pakete werden willkürlich aus Repositorys im Internet abgerufen.
- Neue Pakete werden nicht getestet, bevor sie für Entwickler verfügbar gemacht werden.

Vorteile der Nutzung dieser bewährten Methode:

- Besseres Verständnis, welche Pakete in der entwickelten Software verwendet werden
- Benachrichtigung von Workload-Teams, wenn ein Paket aktualisiert werden muss (basierend auf dem Verständnis davon, wer was verwendet)
- Geringeres Risiko, dass ein Paket mit Problemen in Ihre Software eingeschlossen wird

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel

Implementierungsleitfaden

Stellen Sie zentralisierte Services für Pakete und Abhängigkeiten so bereit, dass sie von Entwicklern einfach verwendet werden können. Zentralisierte Services können logisch zentral sein, anstatt als monolithisches System implementiert zu werden. Mit diesem Ansatz können Sie Services anbieten, die die Anforderungen Ihrer Entwickler erfüllen. Sie sollten eine effiziente Methode zum Hinzufügen von Paketen zum Repository implementieren, wenn Aktualisierungen vorgenommen werden oder neue Anforderungen auftauchen. AWS Dienste wie [AWS CodeArtifact](#) oder ähnliche AWS Partnerlösungen bieten eine Möglichkeit, diese Funktion bereitzustellen.

Implementierungsschritte:

- Implementieren Sie einen logisch zentralisierten Repository-Service, der in allen Umgebungen, in denen die Software entwickelt wird, verfügbar ist.
- Schließen Sie Zugriff auf das Repository als Komponente des AWS-Konto -Vergabeprozesses ein.
- Entwickeln Sie eine Automatisierung zum Testen von Paketen, bevor diese in einem Repository veröffentlicht werden.
- Pflegen Sie Metriken der am häufigsten verwendeten Pakete, Sprachen und Teams mit den häufigsten Änderungen.

- Stellen Sie einen automatisierten Mechanismus für Entwicklerteams bereit, damit sie neue Pakete anfordern und Feedback geben können.
- Scannen Sie regelmäßig Pakete in Ihrem Repository, um die Auswirkungen kürzlich entdeckter Probleme zu identifizieren.

## Ressourcen

### Zugehörige bewährte Methoden:

- [SEC11-BP02 Automatisieren Sie Tests während des gesamten Entwicklungs- und Release-Lebenszyklus](#)

### Zugehörige Dokumente:

- [Beschleunigen Sie Implementierungen AWS mit effektiver Steuerung](#)
- [Erhöhen Sie Ihre Paketsicherheit mit dem CodeArtifact Package Origin Control Toolkit](#)
- [Erkennen von Sicherheitsproblemen bei der Protokollierung mit Amazon CodeGuru Reviewer](#)
- [Ebenen der Lieferkette für Softwareartefakte \(SLSA\)](#)

### Zugehörige Videos:

- [Proaktive Sicherheit: Überlegungen und Ansätze](#)
- [Die AWS -Philosophie zu Sicherheit \(re:Invent 2017\)](#)
- [Wenn Sicherheit und Dringlichkeit von Bedeutung sind: Umgang mit Log4Shell](#)

### Zugehörige Beispiele:

- [Pipeline zur Paketveröffentlichung in mehreren Regionen](#) (GitHub)
- [Veröffentlichen von Node.js -Modulen bei AWS CodeArtifact Verwendung von AWS CodePipeline](#) (GitHub)
- [AWS CDK CodeArtifact Java-Pipeline-Beispiel](#) (GitHub)
- [Privat verteilen. NET NuGet Pakete mit AWS CodeArtifact](#) (GitHub)



## SEC11-BP06 Software programmgesteuert bereitstellen

Führen Sie Bereitstellungen von Software nach Möglichkeit programmatisch durch. Dieser Ansatz verringert die Wahrscheinlichkeit eines Bereitstellungsfehlers oder der Einführung eines unerwarteten Problems aufgrund eines menschlichen Fehlers.

Gewünschtes Ergebnis: Menschen von Daten fernzuhalten ist eines der Prinzipien für sicheres Entwickeln in der AWS Cloud. Dieses Prinzip beinhaltet, wie Sie Ihre Software bereitstellen.

Wenn Sie sich bei der Softwarebereitstellung nicht auf Menschen verlassen, hat das den Vorteil, dass Sie stärker darauf vertrauen können, dass das, was getestet wird, auch das ist, was bereitgestellt wird, und dass die Bereitstellung jedes Mal konsistent durchgeführt wird. Die Software sollte nicht geändert werden müssen, damit sie in unterschiedlichen Umgebungen funktioniert. Mithilfe der Prinzipien der 12-Faktor-Anwendungsentwicklung, insbesondere dem Externalisieren der Konfiguration, können Sie den gleichen Code ohne Änderungen in mehreren Umgebungen bereitstellen. Durch kryptografisches Signieren von Softwarepaketen können Sie sich vergewissern, dass sich zwischen den Umgebungen nichts geändert hat. Das Gesamtergebnis dieses Ansatzes ist die Risikoverringung bei Ihrem Änderungsprozess und die Verbesserung der Konsistenz von Softwareveröffentlichungen.

Typische Anti-Muster:

- Software wird manuell in der Produktion bereitgestellt.
- An Software werden manuell Änderungen vorgenommen, um unterschiedlichen Umgebungen gerecht zu werden.

Vorteile der Nutzung dieser bewährten Methode:

- Gesteigertes Vertrauen in den Prozess der Softwareveröffentlichung
- Verringertes Risiko, dass eine fehlgeschlagene Änderung die Geschäftsfunktionen beeinträchtigt
- Erhöhte Veröffentlichungsfrequenz aufgrund eines geringeren Änderungsrisikos
- Automatische Rollback-Funktion für unerwartete Ereignisse während der Bereitstellung
- Möglichkeit, kryptografisch nachzuweisen, dass es sich bei der getesteten Software um die bereitgestellte Software handelt

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Hoch

## Implementierungsleitfaden

Bauen Sie Ihre AWS-Konto Struktur so auf, dass permanenter menschlicher Zugriff aus Umgebungen entfernt wird, und verwenden Sie CI/CD-Tools zur Durchführung von Bereitstellungen. Entwerfen Sie Ihre Anwendungen so, dass umgebungsspezifische Konfigurationsdaten aus externen Quellen wie [AWS Systems Manager Parameter Store](#) abgerufen werden. Signieren Sie Pakete, nachdem sie getestet wurden, und validieren Sie diese Signaturen während der Bereitstellung. Konfigurieren Sie Ihre CI/CD-Pipelines, um den Anwendungscode zu übertragen, und verwenden Sie Canaries, um die erfolgreiche Bereitstellung zu bestätigen. Verwenden Sie Tools wie [AWS CloudFormation](#) oder [AWS CDK](#), um Ihre Infrastruktur zu definieren, und verwenden Sie dann [AWS CodeBuild](#) und [AWS CodePipeline](#), um CI/CD-Vorgänge durchzuführen.

## Implementierungsschritte

- Entwickeln Sie klar definierte CI/CD-Pipelines, um den Bereitstellungsprozess zu optimieren.
- Die Verwendung von [AWS CodeBuild](#) und [AWS Code Pipeline](#) zur Bereitstellung von CI/CD-Funktionen vereinfacht die Integration von Sicherheitstests in Ihre Pipelines.
- Folgen Sie den Anweisungen zur Trennung von Umgebungen im Whitepaper [Organizing Your AWS Environment Using Multiple Accounts](#).
- Verifizieren Sie, dass es keinen dauerhaften menschlichen Zugriff auf Umgebungen gibt, in denen Produktions-Workloads ausgeführt werden.
- Entwickeln Sie Ihre Anwendungen so, dass sie die Externalisierung von Konfigurationsdaten unterstützen.
- Ziehen Sie die Verwendung eines Modells für die Blau/Grün-Bereitstellung in Betracht.
- Implementieren Sie Canaries, um die erfolgreiche Bereitstellung der Software zu validieren.
- Verwenden Sie kryptografische Tools wie [AWS Signer](#) oder [AWS Key Management Service \(AWS KMS\)](#), um die Softwarepakete, die Sie bereitstellen, zu signieren und zu verifizieren.

## Ressourcen

Zugehörige bewährte Methoden:

- [SEC11-BP02 Automatisieren Sie Tests während des gesamten Entwicklungs- und Release-Lebenszyklus](#)

Zugehörige Dokumente:

- [AWS -CI/CD-Workshop](#)
- [Beschleunigen Sie Implementierungen AWS mit effektiver Governance](#)
- [Automatisierung sicherer, vollautomatischer Bereitstellungen](#)
- [Codesignatur mit AWS Certificate Manager Private CA und AWS Key Management Service asymmetrischen Schlüsseln](#)
- [Codesignatur, eine Vertrauens- und Integritätskontrolle für AWS Lambda](#)

Zugehörige Videos:

- [Vollständige Automatisierung: Automatisieren der Pipelines für kontinuierliche Bereitstellung bei Amazon](#)

Zugehörige Beispiele:

- [Blaue/grüne Bereitstellungen mit AWS Fargate](#)

SEC11-BP07 Beurteilen Sie regelmäßig die Sicherheitseigenschaften der Pipelines

Wenden Sie die Prinzipien der Well-Architected-Säule „Sicherheit“ bei Ihren Pipelines an und achten Sie dabei besonders auf die Trennung von Berechtigungen. Bewerten Sie die Sicherheitseigenschaften Ihrer Pipeline-Infrastruktur regelmäßig. Durch eine effektive Verwaltung der Pipeline-Sicherheit können Sie die Sicherheit der Software sicherstellen, die diese Pipelines durchläuft.

Gewünschtes Ergebnis: Für die Pipelines, die zum Entwickeln und Bereitstellen Ihrer Software verwendet werden, sollten die gleichen empfohlenen Praktiken verwendet werden wie für jede andere Workload in Ihrer Umgebung. Die in den Pipelines implementierten Tests sollten nicht von Entwicklern bearbeitet werden können, die sie verwenden. Die Pipelines sollten nur über Berechtigungen für die Bereitstellungen verfügen, die sie durchführen, und sie sollten Sicherheitsmaßnahmen implementieren, um Bereitstellungen in den falschen Umgebungen zu verhindern. Pipelines sollten sich nicht auf langfristige Anmeldeinformationen verlassen und sie sollten so konfiguriert sein, dass sie den Zustand ausgeben, um die Integrität der Entwicklungsumgebung validieren zu können.

Typische Anti-Muster:

- Sicherheitstests können von Entwicklern umgangen werden.

- Berechtigungen für Bereitstellungs-Pipelines sind übermäßig weit gefasst.
- Pipelines sind nicht für die Validierung von Eingaben konfiguriert.
- Berechtigungen im Zusammenhang mit Ihrer CI/CD-Infrastruktur werden nicht regelmäßig überprüft.
- Langfristige oder fest codierte Anmeldeinformationen werden verwendet.

Vorteile der Nutzung dieser bewährten Methode:

- Größeres Vertrauen in die Integrität der Software, die über die Pipelines entwickelt und bereitgestellt wird.
- Eine Bereitstellung kann angehalten werden, wenn es verdächtige Aktivitäten gibt.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Hoch

### Implementierungsleitfaden

Wenn Sie mit verwalteten CI/CD-Diensten beginnen, die IAM Rollen unterstützen, wird das Risiko eines Verlusts von Anmeldeinformationen reduziert. Durch Anwendung der Prinzipien der Säule „Sicherheit“ auf Ihre CI/CD-Pipeline-Infrastruktur können Sie bestimmen, wo Sicherheitsverbesserungen durchgeführt werden können. Die [Referenzarchitektur für AWS - Bereitstellungs-Pipelines](#) ist ein guter Ausgangspunkt für die Erstellung eigener CI/CD-Umgebungen. Regelmäßige Überprüfungen der Pipeline-Implementierung und Untersuchungen von Protokollen auf unerwartetes Verhalten können Ihnen dabei helfen, die Verwendungsmuster der Pipelines, die zum Bereitstellen der Software verwendet werden, besser zu verstehen.

### Implementierungsschritte

- Beginnen Sie mit der [Referenzarchitektur für AWS -Bereitstellungs-Pipelines](#).
- Erwägen Sie die Verwendung von [AWS IAMAccess Analyzer](#), um programmatisch Richtlinien mit den geringsten Rechten für die Pipelines zu generieren. IAM
- Integrieren Sie Ihre Pipelines in Überwachungs- und Warnmeldungen, sodass Sie über unerwartete oder ungewöhnliche Aktivitäten informiert werden. Für AWS verwaltete Dienste EventBridge ermöglicht Ihnen [Amazon](#), Daten an Ziele wie [AWS LambdaAmazon Simple Notification Service \(AmazonSNS\) weiterzuleiten](#).

## Ressourcen

### Zugehörige Dokumente:

- [Referenzarchitektur für AWS -Bereitstellungs-Pipelines](#)
- [Überwachung von AWS CodePipeline](#)
- [Bewährte Sicherheitsmethoden für AWS CodePipeline](#)

### Zugehörige Beispiele:

- [DevOpsÜberwachungs-Dashboard](#) (GitHub)

SEC11-BP08 Entwickeln Sie ein Programm, das die Verantwortung für Sicherheitsfragen in Workload-Teams einbettet

Entwickeln Sie ein Programm oder einen Mechanismus, das bzw. der es Entwicklerteams ermöglicht, Entscheidungen bezüglich der Sicherheit der von ihnen erstellten Software zu treffen. Zwar muss Ihr Sicherheitsteam diese Entscheidungen immer noch während einer Überprüfung validieren, die Übertragung der Sicherheitsverantwortlichkeit auf Entwicklerteams ermöglicht jedoch eine schnellere und sicherere Workload-Entwicklung. Zudem fördert dieser Mechanismus eine Kultur der Verantwortlichkeit, die einen positiven Einfluss auf den Betrieb der von Ihnen entwickelten Systeme hat.

Gewünschtes Ergebnis: Um Verantwortung und Entscheidungsfindung auf Entwicklerteams zu übertragen, können Sie entweder Sicherheitsschulungen für Entwickler anbieten oder ihre Schulung durch Sicherheitsexperten verbessern, die in das Entwicklerteam eingebettet sind oder mit ihm in Kontakt stehen. Beide Ansätze sind geeignet und ermöglichen es dem Team, früher im Entwicklungszyklus bessere Sicherheitsentscheidungen zu treffen. Dieses Verantwortungsmodell basiert auf Schulungen in Anwendungssicherheit. Wenn Sie mit einem Bedrohungsmodell für die bestimmte Workload beginnen, hilft Ihnen das dabei, das Design Thinking auf den entsprechenden Kontext zu konzentrieren. Ein weiterer Vorteil einer Community von sicherheitsorientierten Entwicklern oder einer Gruppe von Sicherheitstechnikern, die mit Entwicklungsteams zusammenarbeiten, besteht darin, dass Sie besser verstehen, wie Software geschrieben wird. Dieses Verständnis hilft Ihnen dabei, die nächsten verbesserungswürdigen Bereiche bei Ihrem Automatisierungsunterfangen zu bestimmen.

### Typische Anti-Muster:

- Einem Sicherheitsteam werden alle Entscheidungen bezüglich des Sicherheitsdesigns überlassen.
- Sicherheitsanforderungen werden nicht früh genug im Entwicklungsprozess behandelt.
- Es wird kein Feedback von Entwicklern und Sicherheitsexperten zum Betrieb des Programms eingeholt.

Vorteile der Nutzung dieser bewährten Methode:

- Beschleunigung von Sicherheitsüberprüfungen.
- Verringerung von Sicherheitsproblemen, die erst in der Phase der Sicherheitsüberprüfung erkannt werden.
- Verbesserung der gesamten Qualität der Software, die geschrieben wird.
- Möglichkeit, systemische Probleme oder Bereiche mit hoher Wertverbesserung zu identifizieren und zu verstehen.
- Verringerung der erforderlichen Überarbeitung aufgrund von Erkenntnissen aus der Sicherheitsüberprüfung.
- Verbesserung bei der Wahrnehmung der Sicherheitsfunktion.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Niedrig

### Implementierungsleitfaden

Beginnen Sie mit der Anleitung unter [SEC11-BP01 Train für Anwendungssicherheit](#). Bestimmen Sie danach das Betriebsmodell für das Programm, von dem Sie denken, dass es am besten für Ihre Organisation geeignet ist. Die zwei Hauptmuster sind, Entwickler zu schulen oder Sicherheitsexperten in Entwicklungsteams einzubetten. Nachdem Sie sich für eine anfängliche Verfahrensweise entschieden haben, sollten Sie eine Pilotphase mit einem einzelnen Team oder einer kleinen Gruppe von Workload-Teams durchführen, um sich zu vergewissern, dass das Modell für Ihre Organisation funktioniert. Unterstützung der Führungskräfte aus dem Entwicklungs- und Sicherheitsbereich der Organisation hilft bei der Durchführung und trägt zum Erfolg des Programms bei. Bei der Entwicklung dieses Programms ist es wichtig, Metriken auszuwählen, die Aufschluss über den Wert des Programms geben. Von der Art und Weise zu lernen, wie dieses Problem AWS angegangen ist, ist eine gute Lernerfahrung. Diese bewährte Methode konzentriert sich auf die Veränderung und Kultur der Organisation. Die von Ihnen eingesetzten Tools sollten die Zusammenarbeit zwischen der Entwickler- und Sicherheits-Community unterstützen.

## Implementierungsschritte

- Beginnen Sie damit, Ihre Entwickler im Bereich der Anwendungssicherheit zu schulen.
- Schaffen Sie eine Community und ein Onboarding-Programm zur Schulung von Entwicklern.
- Geben Sie dem Programm einen Namen. Häufig wird etwas wie Guardians, Champions oder Advocates verwendet.
- Bestimmen Sie das Modell, das verwendet werden soll: Schulen Sie Entwickler, betten Sie Sicherheitstechniker ein oder verwenden Sie andere verwandte Sicherheitsrollen.
- Identifizieren Sie Projektsponsoren aus dem Sicherheits- und Entwicklungsbereich sowie gegebenenfalls aus anderen relevanten Gruppen.
- Verfolgen Sie Metriken für die Anzahl der am Programm beteiligten Personen, die für Überprüfungen erforderliche Zeit und das Feedback von Entwicklern und Sicherheitsexperten. Nutzen Sie diese Metriken für Verbesserungen.

## Ressourcen

Zugehörige bewährte Methoden:

- [SEC11-BP01 Train für Anwendungssicherheit](#)
- [SEC11-BP02 Automatisieren Sie Tests während des gesamten Entwicklungs- und Release-Lebenszyklus](#)

Zugehörige Dokumente:

- [Konzepte für Bedrohungsmodellierung](#)
- [Betrachtung der Cloud-Sicherheits-Governance](#)

Zugehörige Videos:

- [Proaktive Sicherheit: Überlegungen und Ansätze](#)

## Zuverlässigkeit

Die Säule „Zuverlässigkeit“ umfasst die Fähigkeit einer Workload, die beabsichtigte Funktion erwartungsgemäß korrekt und konsistent auszuführen. Verbindliche Anleitungen zur Implementierung finden Sie im [Whitepaper „Säule der Zuverlässigkeit“](#).

## Bereiche für bewährte Methoden

- [Grundlagen](#)
- [Workload-Architektur](#)
- [Änderungsmanagement](#)
- [Fehlerverwaltung](#)

## Grundlagen

### Fragen

- [REL1. Wie werden Service Quotas und Serviceeinschränkungen verwaltet?](#)
- [REL2. Wie wird die Netzwerktopologie geplant?](#)

### REL1. Wie werden Service Quotas und Serviceeinschränkungen verwaltet?

Für cloudbasierte Workload-Architekturen gibt es Service Quotas (auch als „Servicebeschränkungen“ bezeichnet). Diese Kontingente dienen dazu, zu verhindern, dass versehentlich mehr Ressourcen bereitgestellt werden, als Sie benötigen, und um die Anforderungsraten bei API Vorgängen zu begrenzen, um Dienste vor Missbrauch zu schützen. Es gibt auch Einschränkungen für Ressourcen, z. B. im Bezug auf die Rate, mit der Bits über ein Glasfaserkabel übertragen werden können, oder die Menge an Speicherplatz auf einer physischen Festplatte.

### Bewährte Methoden

- [REL01-BP01 Kenntnis der Servicequoten und Einschränkungen](#)
- [REL01-BP02 Servicekontingente über Konten und Regionen hinweg verwalten](#)
- [REL01-BP03 Berücksichtigung fester Servicequoten und Einschränkungen durch die Architektur](#)
- [REL01-BP04 Kontingente überwachen und verwalten](#)
- [REL01-BP05 Automatisieren Sie die Quotenverwaltung](#)
- [REL01-BP06 Stellen Sie sicher, dass zwischen den aktuellen Kontingenten und der maximalen Nutzung eine ausreichende Lücke besteht, um ein Failover zu ermöglichen](#)



## REL01-BP01 Kenntnis der Servicequoten und Einschränkungen

Sie wissen über die Standardkontingente Bescheid und verwalten Anfragen zur Kontingenterhöhung für Ihre Workload-Architektur. Außerdem wissen Sie, welche Ressourceneinschränkungen, z. B. bezüglich Datenträgern oder Netzwerken, potenziell große Auswirkungen haben.

Angestrebtes Ergebnis: Kunden können eine Verschlechterung oder Unterbrechung ihrer Dienste verhindern, AWS-Konten indem sie geeignete Richtlinien für die Überwachung wichtiger Kennzahlen, Infrastrukturüberprüfungen und Maßnahmen zur automatischen Behebung implementieren, um sicherzustellen, dass Servicequoten und Einschränkungen nicht erreicht werden, die zu einer Verschlechterung oder Unterbrechung des Dienstes führen könnten.

Typische Anti-Muster:

- Bereitstellung eines Workloads ohne Kenntnis der harten oder weichen Quoten und ihrer Grenzen für die verwendeten Services.
- Bereitstellung eines Ersatz-Workloads, ohne die erforderlichen Quoten zu analysieren und neu zu konfigurieren oder den Support im Voraus zu kontaktieren.
- Annehmen, dass Cloud-Services keine Grenzen haben und die Service ohne Berücksichtigung von Tarifen, Grenzen, Zählungen und Mengen genutzt werden können.
- Annehmen, dass die Quoten automatisch erhöht werden.
- Keine Kenntnis des Prozesses und der Zeitleiste von Quotenanforderungen.
- Annehmen, dass das Standardkontingent für Cloud-Services für jeden Service im regionalen Vergleich identisch ist.
- Annehmen, dass die Servicebeschränkungen überschritten werden können und die Systeme automatisch skalieren oder das Limit über die Beschränkungen der Ressource hinaus erhöhen.
- Die Anwendung nicht bei Spitzenbelastungen testen, um die Auslastung der Ressourcen zu strapazieren.
- Bereitstellung der Ressource ohne Analyse der erforderlichen Ressourcengröße.
- Überbereitstellung von Kapazitäten durch Auswahl von Ressourcentypen, die weit über den tatsächlichen Bedarf oder die erwarteten Spitzen hinausgehen.
- Keine Bewertung des Kapazitätsbedarfs für neue Datenverkehrsniveaus im Vorfeld eines neuen Kundenereignisses und keine Einführung einer neuen Technologie.

Vorteile der Nutzung dieser bewährten Methode: Durch die Überwachung und automatisierte Verwaltung von Service Quotas und Ressourcenbeschränkungen können Ausfälle proaktiv reduziert

werden. Änderungen in den Datenverkehrsmustern für den Service eines Kunden können zu einer Unterbrechung oder Verschlechterung führen, wenn die bewährten Methoden nicht befolgt werden. Durch die Überwachung und Verwaltung dieser Werte in allen Regionen und auf allen Konten können die Anwendungen bei ungünstigen oder ungeplanten Ereignissen besser geschützt werden.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Hoch

### Implementierungsleitfaden

Service Quotas ist ein AWS Service, mit dem Sie Ihre Kontingente für über 250 AWS Dienste von einem Standort aus verwalten können. Sie können nicht nur die Kontingentwerte nachschlagen, sondern auch Kontingenterhöhungen über die Konsole Service Quotas oder mithilfe von anfordern und verfolgen AWS SDK. AWS Trusted Advisor bietet eine Überprüfung der Servicekontingente, bei der Ihre Nutzung und Kontingente für einige Aspekte einiger Dienste angezeigt werden. Die Standard-Servicekontingente pro Service finden Sie auch in der AWS Dokumentation für den jeweiligen Service (siehe beispielsweise [VPCAmazon-Kontingente](#)).

Einige Servicebeschränkungen, wie z. B. gedrosselte Ratenbegrenzungen, APIs werden im Amazon API Gateway selbst festgelegt, indem ein Nutzungsplan konfiguriert wird. Zu den Beschränkungen, die als Konfiguration für die jeweiligen Dienste festgelegt wurden, gehören BereitgestelltelOPS, RDS Amazon-Speicherzuweisungen und EBS Amazon-Volumenzuweisungen. Amazon Elastic Compute Cloud verfügt über ein eigenes Service Limits-Dashboard, mit dem Sie Ihre Limits für Instances, Amazon Elastic Block Store und Elastic IP-Adressen verwalten können. Wenn Sie einen Anwendungsfall haben, bei dem Servicekontingente die Leistung Ihrer Anwendung beeinträchtigen und diese nicht an Ihre Bedürfnisse angepasst werden können, wenden Sie sich AWS Support an uns, um zu erfahren, ob es Abhilfemaßnahmen gibt.

Service Quotas können spezifisch für eine Region oder auch global sein. Die Nutzung eines AWS Dienstes, der sein Kontingent erreicht, verhält sich bei normaler Nutzung nicht erwartungsgemäß und kann zu Dienstunterbrechungen oder -beeinträchtigungen führen. Ein Servicekontingent begrenzt beispielsweise die Anzahl der DL EC2 Amazon-Instances, die in einer Region verwendet werden. Dieses Limit kann während eines Traffic-Skalierungsereignisses mit Auto Scaling Scaling-Gruppen (ASG) erreicht werden.

Service Quotas für die einzelnen Konten sollten regelmäßig auf ihre Nutzung hin überprüft werden, um festzustellen, welche Servicelimits für das jeweilige Konto angemessen sind. Diese Service Quotas dienen als betrieblicher Integritätsschutz, um zu verhindern, dass versehentlich mehr Ressourcen bereitgestellt werden, als Sie benötigen. Sie dienen auch dazu, die Anforderungsraten bei API Vorgängen zu begrenzen, um Dienste vor Missbrauch zu schützen.

Serviceeinschränkungen und Service Quotas unterscheiden sich voneinander.

Serviceeinschränkungen stellen die Limits einer bestimmten Ressource dar, wie sie durch diesen Ressourcentyp definiert sind. Dabei kann es sich um Speicherkapazität (GP2 hat beispielsweise eine Größenbeschränkung von 1 GB bis 16 TB) oder um den Festplattendurchsatz handeln. Es ist von entscheidender Bedeutung, dass die Beschränkung eines Ressourcentyps konstruiert und ständig auf eine Nutzung geprüft wird, durch die das Limit erreicht werden könnte. Wenn eine Beschränkung unerwartet erreicht wird, können die Anwendungen oder Services des Kontos beeinträchtigt oder unterbrochen werden.

Wenn es einen Anwendungsfall gibt, in dem Servicekontingente die Leistung einer Anwendung beeinträchtigen und sie nicht an die erforderlichen Anforderungen angepasst werden können, wenden Sie sich an uns, AWS Support um zu erfahren, ob es Abhilfemaßnahmen gibt. Weitere Einzelheiten zur Anpassung fester Kontingente finden Sie unter [REL01-BP03 Berücksichtigung fester Servicequoten und Einschränkungen durch die Architektur](#).

Es gibt eine Reihe von AWS Diensten und Tools zur Überwachung und Verwaltung von Service Quotas. Der Service und die Tools sollten genutzt werden, um automatische oder manuelle Überprüfungen der Kontingente zu ermöglichen.

- AWS Trusted Advisor bietet eine Überprüfung der Servicekontingenten, bei der Ihre Nutzung und Kontingente für einige Aspekte einiger Dienste angezeigt werden. Es kann dabei helfen, Services zu identifizieren, die ihr Kontingent fast erreicht haben.
- AWS Management Console bietet Methoden zum Anzeigen von Kontingentwerten für Dienste, zum Verwalten und Anfordern neuer Kontingente, zum Überwachen des Status von Kontingentanfragen und zum Anzeigen des Kontingentverlaufs.
- AWS CLI und CDKs bietet programmgesteuerte Methoden zur automatischen Verwaltung und Überwachung von Servicequotas und deren Nutzung.

## Implementierungsschritte

Für Service Quotas:

- [Überprüfen Sie die AWS Service Quotas](#).
- Um sich über Ihre bestehenden Servicekontingenten zu informieren, ermitteln Sie, welche Dienste (wie IAM Access Analyzer) verwendet werden. Es gibt ungefähr 250 AWS Dienste, die durch Dienstkontingente gesteuert werden. Bestimmen Sie dann den spezifischen Service-Quota-Namen, der für jedes Konto und jede Region verwendet werden kann. Pro Region gibt es etwa 3 000 Service-Quota-Namen.

- Erweitern Sie diese Kontingentanalyse AWS Config um, um alle [AWS Ressourcen](#) zu finden, die in Ihrem AWS-Konten verwendet werden.
- Verwenden Sie [AWS CloudFormation Daten](#), um Ihre verwendeten AWS Ressourcen zu ermitteln. Sehen Sie sich die Ressourcen an, die entweder in der AWS Management Console oder mit dem [list-stack-resources](#) AWS CLI Befehl erstellt wurden. Sie können zudem Ressourcen anzeigen, die für die Bereitstellung in der Vorlage selbst konfiguriert sind.
- Ermitteln Sie alle für die Workload erforderlichen Services durch Untersuchung des Bereitstellungscode.
- Ermitteln Sie die geltenden Service Quotas. Verwenden Sie die programmgesteuert zugänglichen Informationen von Trusted Advisor und Service Quotas.
- Richten Sie eine automatisierte Überwachungsmethode ein (siehe [REL01-BP02 Servicekontingente über Konten und Regionen hinweg verwalten](#) und [REL01-BP04 Kontingente überwachen und verwalten](#)), um zu warnen und zu informieren, wenn die Service Quotas fast erschöpft sind oder ihr Limit erreicht haben.
- Richten Sie eine automatische, programmatische Methode ein, um zu überprüfen, ob ein Service Quota in einer Region, aber nicht in anderen Regionen desselben Kontos geändert wurde (siehe [REL01-BP02 Servicekontingente über Konten und Regionen hinweg verwalten](#) und [REL01-BP04 Kontingente überwachen und verwalten](#)).
- Automatisieren Sie das Scannen von Anwendungsprotokollen und Metriken, um festzustellen, ob Fehler beim Kontingent oder bei Serviceeinschränkungen vorliegen. Falls Fehler vorhanden sind, senden Sie Warnmeldungen an das Überwachungssystem.
- Führen Sie technische Verfahren zur Berechnung der erforderlichen Kontingentänderung ein (siehe [REL01-BP05 Automatisieren Sie die Quotenverwaltung](#)), wenn festgestellt wird, dass für bestimmte Services größere Kontingente erforderlich sind.
- Erstellen Sie einen Bereitstellungs- und Genehmigungs-Workflow, um Änderungen am Service Quota anzufordern. Dies sollte einen Ausnahme-Workflow für den Fall umfassen, dass ein Antrag abgelehnt oder nur teilweise genehmigt wird.
- Entwickeln Sie eine technische Methode zur Überprüfung von Servicekontingenten vor der Bereitstellung und Nutzung neuer AWS Dienste, bevor Sie sie in Produktionsumgebungen oder Umgebungen mit hoher Auslastung bereitstellen. (zum Beispiel ein Lasttestkonto).

Bei Serviceeinschränkungen:

- Führen Sie Überwachungs- und Messmethoden ein, um auf Ressourcen aufmerksam zu machen, die ihre Ressourceneinschränkungen fast erreicht haben. Nutzen Sie CloudWatch sie je nach Bedarf für die Überwachung von Metriken oder Protokollen.
- Legen Sie Warnschwellenwerte für jede Ressource fest, die eine für die Anwendung oder das System bedeutsame Einschränkung hat.
- Erstellen Sie Verfahren für die Verwaltung von Workflows und Infrastrukturen, um den Ressourcentyp zu ändern, wenn die Nutzungseinschränkung fast erreicht ist. Dieser Workflow sollte Lasttests beinhalten, um zu überprüfen, ob der neue Typ der richtige Ressourcentyp mit den neuen Einschränkungen ist.
- Migrieren Sie die identifizierte Ressource unter Verwendung bestehender Verfahren und Prozesse auf den empfohlenen neuen Ressourcentyp.

## Ressourcen

### Zugehörige bewährte Methoden:

- [REL01-BP02 Servicekontingente über Konten und Regionen hinweg verwalten](#)
- [REL01-BP03 Berücksichtigung fester Servicequoten und Einschränkungen durch die Architektur](#)
- [REL01-BP04 Kontingente überwachen und verwalten](#)
- [REL01-BP05 Automatisieren Sie die Quotenverwaltung](#)
- [REL01-BP06 Stellen Sie sicher, dass zwischen den aktuellen Kontingenten und der maximalen Nutzung eine ausreichende Lücke besteht, um ein Failover zu ermöglichen](#)
- [REL03-BP01 Wählen Sie, wie Sie Ihre Arbeitslast segmentieren möchten](#)
- [REL10-BP01 Stellen Sie den Workload an mehreren Standorten bereit](#)
- [REL11-BP01 Überwachen Sie alle Komponenten des Workloads, um Fehler zu erkennen](#)
- [REL11-BP03 Automatisieren Sie die Heilung auf allen Ebenen](#)
- [REL12-BP05 Testen Sie die Resilienz mithilfe von Chaos Engineering](#)

### Zugehörige Dokumente:

- [AWS Die Zuverlässigkeitssäule von Well-Architected Framework: Verfügbarkeit](#)
- [AWS Service Quotas \(früher als Service Limits bezeichnet\)](#)
- [AWS Trusted Advisor Prüfungen bewährter Verfahren \(siehe Abschnitt Service Limits\)](#)

- [AWS Beschränken Sie den Monitor auf AWS Antworten](#)
- [EC2Amazon-Servicebeschränkungen](#)
- [Was ist Service Quotas?](#)
- [How to Request Quota Increase](#)
- [Service endpoints and quotas](#)
- [Service Quotas-Benutzerhandbuch](#)
- [Kontingentmonitor für AWS](#)
- [AWS Grenzen der Fehlerisolierung](#)
- [Availability with redundancy](#)
- [AWS für Daten](#)
- [What is Continuous Integration?](#)
- [What is Continuous Delivery?](#)
- [APNPartner: Partner, die beim Konfigurationsmanagement helfen können](#)
- [Verwaltung des Kontolebenszyklus in account-per-tenant SaaS-Umgebungen auf AWS](#)
- [Verwaltung und Überwachung der API Drosselung Ihrer Workloads](#)
- [Sehen Sie sich AWS Trusted Advisor Empfehlungen in großem Umfang an mit AWS Organizations](#)
- [Automatisierung von Service-Limit-Erhöhungen und Unternehmenssupport mit AWS Control Tower](#)

#### Zugehörige Videos:

- [AWS Live re:inForce 2019 — Service Quotas](#)
- [Kontingente für AWS Dienste mithilfe von Service Quotas anzeigen und verwalten](#)
- [AWS IAMDemo der Kontingente](#)

#### Zugehörige Tools:

- [CodeGuru Amazon-Rezensent](#)
- [AWS CodeDeploy](#)
- [AWS CloudTrail](#)
- [Amazon CloudWatch](#)
- [Amazon EventBridge](#)

- [DevOpsAmazon-Guru](#)
- [AWS Config](#)
- [AWS Trusted Advisor](#)
- [AWS CDK](#)
- [AWS Systems Manager](#)
- [AWS Marketplace](#)

REL01-BP02 Servicekontingente über Konten und Regionen hinweg verwalten

Wenn Sie mehrere Konten oder Regionen verwenden, fordern Sie die entsprechenden Kontingente in allen Umgebungen an, in denen die Produktions-Workloads ausgeführt werden.

Gewünschtes Ergebnis: Services und Anwendungen sollten bei Konfigurationen, die sich über Konten oder Regionen erstrecken oder die über ein Ausfallsicherheitsdesign mit Zonen-, Regions- oder Konto-Failover verfügen, nicht von der Erschöpfung des Service Quota betroffen sein.

Typische Anti-Muster:

- Es wird zugelassen, dass die Ressourcennutzung in einer Isolationsregion zunimmt, ohne dass es einen Mechanismus zur Aufrechterhaltung der Kapazität in den anderen Zonen gibt.
- Alle Kontingente werden manuell und in jeder Isolationsregion einzeln festgelegt.
- Nichtberücksichtigung der Auswirkungen von Ausfallsicherheitsarchitekturen (wie aktiv oder passiv) auf den künftigen Kontingentbedarf bei einer Verschlechterung in der nicht primären Region.
- Keine regelmäßige Bewertung der Kontingente und Durchführung der erforderlichen Änderungen in jeder Region und jedem Konto, in dem die Workload ausgeführt wird.
- Keine Nutzung von [Vorlagen für Kontingentanforderungen](#), um Erhöhungen für mehrere Regionen und Konten zu beantragen.
- Keine Aktualisierung von Service Quotas, weil man fälschlicherweise davon ausgeht, dass eine Erhöhung der Kontingente Kosten nach sich zieht, wie z. B. Anforderungen von Rechenkapazitäten.

Vorteile der Einführung dieser bewährten Methode: Überprüfen, ob Sie Ihre aktuelle Last in sekundären Regionen oder Konten bewältigen können, falls regionale Services nicht mehr verfügbar sind. Dies kann dazu beitragen, die Anzahl von Fehlern oder Verschlechterungen zu verringern, die beim Verlust von Regionen auftreten.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Hoch

## Implementierungsleitfaden

Service Quotas werden pro Konto aufgezeichnet. Sofern nicht anders angegeben, ist AWS-Region jedes Kontingent -spezifisch. Zusätzlich zu den Produktionsumgebungen verwalten Sie auch Kontingente in allen anwendbaren Nicht-Produktionsumgebungen, damit Tests und Entwicklung nicht behindert werden. Die Aufrechterhaltung eines hohen Maßes an Ausfallsicherheit setzt voraus, dass die Service Quotas ständig überprüft werden (entweder automatisch oder manuell).

Da durch die Implementierung von Designs mit den Ansätzen Aktiv/Aktiv, Aktiv/Passiv – Hot, Aktiv/Passiv – Cold und Aktiv/Passiv – Pilot Light immer mehr Workloads auf die Regionen verteilt werden, ist es wichtig, alle Kontingente für Regionen und Konten zu kennen. Frühere Datenverkehrsmuster sind nicht immer ein guter Indikator dafür, ob das Service Quota korrekt eingestellt ist.

Ebenso wichtig ist, dass das Namenslimit für das Service Quota nicht immer für alle Regionen gleich ist. In einer Region kann der Wert fünf sein, in einer anderen zehn. Die Verwaltung dieser Kontingente muss sich auf dieselben Services, Konten und Regionen erstrecken, um eine gleichmäßige Ausfallsicherheit unter Last zu gewährleisten.

Stimmen Sie alle Unterschiede zwischen den Service Quotas in den verschiedenen Regionen (aktive oder passive Region) ab und schaffen Sie Prozesse, um diese Unterschiede kontinuierlich abzugleichen. Die Testpläne für passive Regions-Failover sind selten auf die aktive Spitzenkapazität skaliert, was bedeutet, dass es im Ernstfall oder bei Tabletop-Übungen nicht gelingen kann, Unterschiede bei den Service Quotas zwischen den Regionen festzustellen und die korrekten Limits einzuhalten.

Service-Quota-Abweichung, d. h. der Umstand, dass die Service-Quota-Limits für ein bestimmtes benanntes Kontingent in einer Region und nicht in allen Regionen geändert werden, müssen unbedingt verfolgt und bewertet werden. Es sollte erwogen werden, die Kontingente in Regionen mit Datenverkehr oder potenziellem Datenverkehr zu ändern.

- Wählen Sie relevante Konten und Regionen anhand von Serviceanforderungen, regulatorischen Anforderungen sowie Anforderungen für die Latenz und die Notfallwiederherstellung aus.
- Ermitteln Sie Service Quotas für alle relevanten Konten, Regionen und Availability Zones. Die Limits gelten für ein Konto und eine Region. Diese Werte sollten auf Unterschiede hin verglichen werden.

## Implementierungsschritte



- Überprüfen Sie die Service Quotas-Werte, die über eine Risikostufe der Nutzung hinausgehen. AWS Trusted Advisor bietet Warnungen bei Überschreitung der Schwellenwerte von 80 % und 90 %.
- Überprüfen Sie die Werte für Service Quotas in allen passiven Regionen (in einem Aktiv/Passiv-Design). Stellen Sie sicher, dass die Last in den sekundären Regionen bei einem Ausfall in der primären Region erfolgreich ausgeführt werden kann.
- Automatisieren Sie die Bewertung, ob es zu einer Verschiebung der Service Quotas zwischen den Regionen desselben Kontos gekommen ist, und handeln Sie entsprechend, um die Limits zu ändern.
- Wenn die Organisationseinheiten (OU) des Kunden in der unterstützten Weise strukturiert sind, sollten die Vorlagen für Service Quotas aktualisiert werden, um Änderungen an Kontingenten widerzuspiegeln, die auf mehrere Regionen und Konten angewendet werden sollen.
  - Erstellen Sie eine Vorlage und weisen Sie der Kontingentänderung Regionen zu.
  - Überprüfen Sie alle bestehenden Vorlagen für Service Quotas auf erforderliche Änderungen (Region, Limits und Konten).

## Ressourcen

### Zugehörige bewährte Methoden:

- [REL01-BP01 Kenntnis der Servicequoten und Einschränkungen](#)
- [REL01-BP03 Berücksichtigung fester Servicequoten und Einschränkungen durch die Architektur](#)
- [REL01-BP04 Kontingente überwachen und verwalten](#)
- [REL01-BP05 Automatisieren Sie die Quotenverwaltung](#)
- [REL01-BP06 Stellen Sie sicher, dass zwischen den aktuellen Kontingenten und der maximalen Nutzung eine ausreichende Lücke besteht, um ein Failover zu ermöglichen](#)
- [REL03-BP01 Wählen Sie, wie Sie Ihre Arbeitslast segmentieren möchten](#)
- [REL10-BP01 Stellen Sie den Workload an mehreren Standorten bereit](#)
- [REL11-BP01 Überwachen Sie alle Komponenten des Workloads, um Fehler zu erkennen](#)
- [REL11-BP03 Automatisieren Sie die Heilung auf allen Ebenen](#)
- [REL12-BP05 Testen Sie die Resilienz mithilfe von Chaos Engineering](#)

### Zugehörige Dokumente:

- [AWS Die Zuverlässigkeitssäule von Well-Architected Framework: Verfügbarkeit](#)
- [AWS Service Quotas \(früher als Service Limits bezeichnet\)](#)
- [AWS Trusted Advisor Prüfungen bewährter Verfahren \(siehe Abschnitt Service Limits\)](#)
- [AWS Beschränken Sie den Monitor auf AWS Antworten](#)
- [EC2Amazon-Servicebeschränkungen](#)
- [Was ist Service Quotas?](#)
- [How to Request Quota Increase](#)
- [Service endpoints and quotas](#)
- [Service Quotas-Benutzerhandbuch](#)
- [Kontingentmonitor für AWS](#)
- [AWS Grenzen der Fehlerisolierung](#)
- [Availability with redundancy](#)
- [AWS für Daten](#)
- [What is Continuous Integration?](#)
- [What is Continuous Delivery?](#)
- [APNPartner: Partner, die beim Konfigurationsmanagement helfen können](#)
- [Verwaltung des Kontolebenszyklus in account-per-tenant SaaS-Umgebungen auf AWS](#)
- [Verwaltung und Überwachung der API Drosselung Ihrer Workloads](#)
- [Sehen Sie sich AWS Trusted Advisor Empfehlungen in großem Umfang an mit AWS Organizations](#)
- [Automatisierung von Service-Limit-Erhöhungen und Unternehmenssupport mit AWS Control Tower](#)

#### Zugehörige Videos:

- [AWS Live re:inForce 2019 — Service Quotas](#)
- [Kontingente für AWS Dienste mithilfe von Service Quotas anzeigen und verwalten](#)
- [AWS IAMDemo der Kontingente](#)

#### Zugehörige Services:

- [CodeGuru Amazon-Rezensent](#)
- [AWS CodeDeploy](#)

- [AWS CloudTrail](#)
- [Amazon CloudWatch](#)
- [Amazon EventBridge](#)
- [DevOpsAmazon-Guru](#)
- [AWS Config](#)
- [AWS Trusted Advisor](#)
- [AWS CDK](#)
- [AWS Systems Manager](#)
- [AWS Marketplace](#)

REL01-BP03 Berücksichtigung fester Servicequoten und Einschränkungen durch die Architektur

Achten Sie auf nicht änderbare Service Quotas, Servicebeschränkungen und physische Ressourcen-Limits. Entwerfen Sie Architekturen für Anwendungen und Services, um zu verhindern, dass sich diese Limits auf die Zuverlässigkeit auswirken.

Beispiele hierfür sind die Netzwerkbandbreite, die Größe der Nutzlast für den Aufruf serverloser Funktionen, die Drosselungsrate eines API Gateways und gleichzeitige Benutzerverbindungen zu einer Datenbank.

Gewünschtes Ergebnis: Die Anwendung oder der Service erbringt unter normalen Bedingungen und bei hohem Datenverkehr die erwartete Leistung. Sie wurden so konzipiert, dass sie innerhalb der für diese Ressource festgelegten Beschränkungen oder Service-Kontingente arbeiten.

Typische Anti-Muster:

- Auswahl eines Designs, das eine Ressource eines Service verwendet, ohne zu wissen, dass es Design-Einschränkungen gibt, die dazu führen, dass dieses Design beim Skalieren versagt.
- Sie führen ein Benchmarking durch, das unrealistisch ist und mit dem während der Tests die festen Kontingente für den Service erreicht werden. Sie führen beispielsweise Tests mit einem Burst-Limit durch, diese aber für einen längeren Zeitraum.
- Sie wählen ein Design aus, das nicht skaliert oder geändert werden kann, wenn feste Service-Kontingente überschritten werden müssen. Zum Beispiel eine SQS Payload-Größe von 256 KB.
- Die Überwachungsfunktion wurde nicht zur Überwachung und Benachrichtigung von/für Schwellenwerte/n für Service-Kontingente entwickelt und implementiert, die bei hohem Datenverkehr gefährdet sein könnten.

Vorteile der Nutzung dieser bewährten Methode: Es wird sichergestellt, dass die Anwendung unter allen prognostizierten Last-Levels der Services ohne Unterbrechung oder Beeinträchtigung läuft.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Mittel

### Implementierungsleitfaden

Im Gegensatz zu Soft-Service-Kontingenten oder Ressourcen, die durch Einheiten mit höherer Kapazität ersetzt werden, können feste Kontingente AWS von Diensten nicht geändert werden. Das bedeutet, dass all diese Arten von AWS Diensten auf mögliche harte Kapazitätsgrenzen hin untersucht werden müssen, wenn sie in einem Anwendungsdesign verwendet werden.

Feste Beschränkungen werden in der Service Quotas-Konsole angezeigt. Wenn in den Spalten ADJUSTABLE = No angezeigt wird, gibt es eine feste Beschränkung für den Service. Auch auf einigen Konfigurationsseiten für Ressourcen werden feste Beschränkungen angezeigt. Für Lambda gibt es zum Beispiel bestimmte feste Beschränkungen, die nicht angepasst werden können.

Wenn Sie beispielsweise eine Python-Anwendung entwerfen, die in einer Lambda-Funktion ausgeführt werden soll, sollte die Anwendung daraufhin geprüft werden, ob die Möglichkeit besteht, dass Lambda länger als 15 Minuten läuft. Wenn die Codeausführung länger als dieses Service-Kontingent dauert, müssen alternative Technologien oder Designs in Betracht gezogen werden. Wird diese Beschränkung nach der Bereitstellung in der Produktion erreicht, wird die Anwendung beeinträchtigt und gestört, bis sie wiederhergestellt werden kann. Im Gegensatz zu Soft-Kontingenten gibt es keine Möglichkeit, diese Beschränkungen zu ändern – selbst wenn ein Ereignis des Schweregrads 1 eintritt.

Sobald die Anwendung in einer Testumgebung bereitgestellt wurde, sollten Strategien eingesetzt werden, um herauszufinden, ob feste Beschränkungen erreicht werden könnten. Stresstests, Lasttests und Chaostests sollten Teil des Einführungstestplans sein.

### Implementierungsschritte

- Sehen Sie sich die vollständige Liste der AWS Dienste an, die in der Phase des Anwendungsentwurfs verwendet werden könnten.
- Sehen Sie sich die Soft-Kontingentbeschränkungen und Hard-Kontingentbeschränkungen der Services an. Nicht alle Beschränkungen werden in der Service Quotas-Konsole angezeigt. Einige Services [zeigen die Beschränkungen an anderen Stellen an](#).
- Prüfen Sie bei der Entwicklung Ihrer Anwendung die geschäftlichen und technologischen Faktoren Ihres Workloads, wie z. B. Geschäftsergebnisse, Anwendungsfälle, abhängige Systeme,

Verfügbarkeitsziele und Objekte für die Notfallwiederherstellung. Lassen Sie sich von Ihren geschäftlichen und technologischen Faktoren leiten, um das richtige verteilte System für Ihren Workload zu finden.

- Analysieren Sie die Last des Services über Regionen und Konten hinweg. Viele feste Beschränkungen für Services basieren auf Regionen. Einige Beschränkungen sind jedoch kontobasiert.
- Analysieren Sie die Architekturen zur Ausfallsicherheit der Ressourcen bei einem zonenbezogenen Fehler und einem Fehler in einer Region. Bei der Entwicklung von Multi-Regionen-Designs mit Aktiv/Aktiv-, Aktiv/Passiv-Hot-, Aktiv/Passiv-Cold- und Aktiv/Passiv-Pilot-Light-Ansätzen werden diese Fehlerfälle eine höhere Auslastung verursachen. Dies schafft einen potenziellen Anwendungsfall für feste Beschränkungen.

## Ressourcen

Zugehörige bewährte Methoden:

- [REL01-BP01 Kenntnis der Servicequoten und Einschränkungen](#)
- [REL01-BP02 Servicekontingente über Konten und Regionen hinweg verwalten](#)
- [REL01-BP04 Kontingente überwachen und verwalten](#)
- [REL01-BP05 Automatisieren Sie die Quotenverwaltung](#)
- [REL01-BP06 Stellen Sie sicher, dass zwischen den aktuellen Kontingenten und der maximalen Nutzung eine ausreichende Lücke besteht, um ein Failover zu ermöglichen](#)
- [REL03-BP01 Wählen Sie, wie Sie Ihre Arbeitslast segmentieren möchten](#)
- [REL10-BP01 Stellen Sie den Workload an mehreren Standorten bereit](#)
- [REL11-BP01 Überwachen Sie alle Komponenten des Workloads, um Fehler zu erkennen](#)
- [REL11-BP03 Automatisieren Sie die Heilung auf allen Ebenen](#)
- [REL12-BP05 Testen Sie die Resilienz mithilfe von Chaos Engineering](#)

Zugehörige Dokumente:

- [AWS Die Zuverlässigkeitssäule von Well-Architected Framework: Verfügbarkeit](#)
- [AWS Service Quotas \(früher als Service Limits bezeichnet\)](#)
- [AWS Trusted Advisor Prüfungen bewährter Verfahren \(siehe Abschnitt Service Limits\)](#)

- [AWS Beschränken Sie den Monitor auf AWS Antworten](#)
- [EC2Amazon-Servicebeschränkungen](#)
- [Was ist Service Quotas?](#)
- [How to Request Quota Increase](#)
- [Service endpoints and quotas](#)
- [Service Quotas-Benutzerhandbuch](#)
- [Kontingentmonitor für AWS](#)
- [AWS Grenzen der Fehlerisolierung](#)
- [Availability with redundancy](#)
- [AWS für Daten](#)
- [What is Continuous Integration?](#)
- [What is Continuous Delivery?](#)
- [APNPartner: Partner, die beim Konfigurationsmanagement helfen können](#)
- [Verwaltung des Kontolebenszyklus in account-per-tenant SaaS-Umgebungen auf AWS](#)
- [Verwaltung und Überwachung der API Drosselung Ihrer Workloads](#)
- [Sehen Sie sich AWS Trusted Advisor Empfehlungen in großem Umfang an mit AWS Organizations](#)
- [Automatisierung von Service-Limit-Erhöhungen und Unternehmenssupport mit AWS Control Tower](#)
- [Aktionen, Ressourcen und Bedingungsschlüssel für Service Quotas](#)

#### Zugehörige Videos:

- [AWS Live re:inForce 2019 — Service Quotas](#)
- [Kontingente für AWS Dienste mithilfe von Service Quotas anzeigen und verwalten](#)
- [AWS IAMDemo der Kontingente](#)
- [AWS re:Invent 2018: Kreisläufe schließen und neue Denkanstöße geben: So übernehmen Sie die Kontrolle über große und kleine Systeme](#)

#### Zugehörige Tools:

- [AWS CodeDeploy](#)
- [AWS CloudTrail](#)

- [Amazon CloudWatch](#)
- [Amazon EventBridge](#)
- [DevOpsAmazon-Guru](#)
- [AWS Config](#)
- [AWS Trusted Advisor](#)
- [AWS CDK](#)
- [AWS Systems Manager](#)
- [AWS Marketplace](#)

## REL01-BP04 Kontingente überwachen und verwalten

Überprüfen Sie die potenzielle Nutzung und erhöhen Sie Ihre Kontingente entsprechend, um einen geplanten Nutzungsanstieg zu ermöglichen.

Gewünschtes Ergebnis: Es wurden aktive und automatisierte Verwaltungs- und Überwachungssysteme bereitgestellt. Diese operativen Lösungen reagieren, wenn die Schwellenwerte für die Kontingentnutzung fast erreicht werden. Sie lösen die Situation durch die proaktiven Änderungen des Kontingents.

Typische Anti-Muster:

- Keine Konfigurationsüberwachung zur Prüfung von Schwellenwerten für das Service-Kontingent.
- Keine Konfigurationsüberwachung für feste Beschränkungen, auch wenn diese Werte nicht geändert werden können.
- Sie gehen davon aus, dass eine Änderung des Soft-Kontingents direkt stattfindet oder nur wenig Zeit erfordert.
- Es werden Warnungen für den Fall konfiguriert, dass Servicekontingente erreicht werden, aber es gibt keinen Prozess für die Reaktion auf eine entsprechende Warnung.
- Nur Alarmer für Dienste konfigurieren, die von AWS Service Quotas unterstützt werden, und keine Überwachung anderer AWS Dienste.
- Keine Berücksichtigung der Verwaltung von Kontingenten für die Ausfallsicherheit mehrerer Regionen, wie z. B. Aktiv/Aktiv-, Aktiv/Passiv-Hot-, Aktiv/Passiv-Cold- und Aktiv/Passiv-Pilot-Light-Ansätze.
- Keine Bewertung der Kontingentunterschiede zwischen den Regionen.

- Keine Bewertung des Bedarfs in jeder Region für eine bestimmte Kontingenterhöhung.
- Keine Nutzung von [Vorlagen für die Verwaltung von Kontingenten für mehrere Regionen](#).

Vorteile der Einführung dieser bewährten Methode: Durch die automatische Verfolgung der AWS Service Quotas und die Überwachung Ihrer Nutzung anhand dieser Kontingente können Sie erkennen, wann Sie sich einer Kontingentbegrenzung nähern. Sie können diese Überwachungsdaten außerdem nutzen, um Verschlechterungen aufgrund einer Kontingentausschöpfung zu begrenzen.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Mittel

### Implementierungsleitfaden

Bei unterstützten Services können Sie Ihre Kontingente überwachen, indem Sie verschiedene Services zur Bewertung und anschließenden Versendung von Warnungen konfigurieren. Auf diese Weise können Sie die Nutzung überwachen und werden auf sich nähernde Kontingentgrenzen aufmerksam gemacht. Diese Alarmer können von Lambda-Funktionen AWS Config CloudWatch, Amazon oder von aufgerufen werden. AWS Trusted Advisor Sie können auch Metrikfilter für CloudWatch Protokolle verwenden, um Muster in Protokollen zu suchen und zu extrahieren, um festzustellen, ob sich die Nutzung den Kontingentschwellenwerten nähert.

### Implementierungsschritte

Für die Überwachung:

- Erfassen Sie den aktuellen Ressourcenverbrauch (z. B. Buckets oder Instances). Verwenden Sie API Servicebetriebe wie Amazon EC2 DescribeInstancesAPI, um den aktuellen Ressourcenverbrauch zu ermitteln.
- Erfassen Sie Ihre aktuellen Kontingente, die für die Services wesentlich und anwendbar sind. Nutzen Sie dazu:
  - AWS Service Quotas
  - AWS Trusted Advisor
  - AWS Dokumentation
  - AWS dienstspezifische Seiten
  - AWS Command Line Interface (AWS CLI)
  - AWS Cloud Development Kit (AWS CDK)
- Verwenden Sie AWS Service Quotas, einen AWS Service, mit dem Sie Ihre Kontingente für über 250 AWS Dienste von einem Standort aus verwalten können.



- Verwenden Sie Trusted Advisor Servicelimits, um Ihre aktuellen Servicelimits bei verschiedenen Schwellenwerten zu überwachen.
- Prüfen Sie anhand der Historie der Servicekontingenten (Konsole oder AWS CLI), ob regionale Erhöhungen vorliegen.
- Vergleichen Sie die Änderungen der Service-Kontingente in jeder Region und jedem Konto, um bei Bedarf auszugleichen.

Für die Verwaltung:

- Automatisiert: Richten Sie eine AWS Config benutzerdefinierte Regel ein, um Servicekontingente in verschiedenen Regionen zu scannen und Unterschiede zu vergleichen.
- Automatisiert: Richten Sie eine geplante Lambda-Funktion ein, um Service-Kontingente in den Regionen zu scannen und Abweichungen zu ermitteln.
- Manuell: Scannen Sie die Service-Kontingente über AWS CLI API, oder die AWS Konsole, um Servicekontingente in verschiedenen Regionen zu scannen und auf Unterschiede zu vergleichen. Erstellen Sie einen Bericht zu den Abweichungen.
- Wenn Abweichungen in den Kontingenten zwischen den Regionen festgestellt werden, fordern Sie bei Bedarf eine Kontingentänderung an.
- Überprüfen Sie das Ergebnis aller Anforderungen.

Ressourcen

Zugehörige bewährte Methoden:

- [REL01-BP01 Kenntnis der Servicequoten und Einschränkungen](#)
- [REL01-BP02 Servicekontingente über Konten und Regionen hinweg verwalten](#)
- [REL01-BP03 Berücksichtigung fester Servicequoten und Einschränkungen durch die Architektur](#)
- [REL01-BP05 Automatisieren Sie die Quotenverwaltung](#)
- [REL01-BP06 Stellen Sie sicher, dass zwischen den aktuellen Kontingenten und der maximalen Nutzung eine ausreichende Lücke besteht, um ein Failover zu ermöglichen](#)
- [REL03-BP01 Wählen Sie, wie Sie Ihre Arbeitslast segmentieren möchten](#)
- [REL10-BP01 Stellen Sie den Workload an mehreren Standorten bereit](#)
- [REL11-BP01 Überwachen Sie alle Komponenten des Workloads, um Fehler zu erkennen](#)
- [REL11-BP03 Automatisieren Sie die Heilung auf allen Ebenen](#)

- [REL12-BP05 Testen Sie die Resilienz mithilfe von Chaos Engineering](#)

#### Zugehörige Dokumente:

- [AWS Die Zuverlässigkeitssäule von Well-Architected Framework: Verfügbarkeit](#)
- [AWS Service Quotas \(früher als Service Limits bezeichnet\)](#)
- [AWS Trusted Advisor Prüfungen bewährter Verfahren \(siehe Abschnitt Service Limits\)](#)
- [AWS Beschränken Sie den Monitor auf AWS Antworten](#)
- [EC2Amazon-Servicebeschränkungen](#)
- [Was ist Service Quotas?](#)
- [How to Request Quota Increase](#)
- [Service endpoints and quotas](#)
- [Service Quotas-Benutzerhandbuch](#)
- [Kontingentmonitor für AWS](#)
- [AWS Grenzen der Fehlerisolierung](#)
- [Availability with redundancy](#)
- [AWS für Daten](#)
- [What is Continuous Integration?](#)
- [What is Continuous Delivery?](#)
- [APNPartner: Partner, die beim Konfigurationsmanagement helfen können](#)
- [Verwaltung des Kontolebenszyklus in account-per-tenant SaaS-Umgebungen auf AWS](#)
- [Verwaltung und Überwachung der API Drosselung Ihrer Workloads](#)
- [Sehen Sie sich AWS Trusted Advisor Empfehlungen in großem Umfang an mit AWS Organizations](#)
- [Automatisierung von Service-Limit-Erhöhungen und Unternehmenssupport mit AWS Control Tower](#)
- [Aktionen, Ressourcen und Bedingungsschlüssel für Service Quotas](#)

#### Zugehörige Videos:

- [AWS Live re:inForce 2019 — Service Quotas](#)
- [Kontingente für AWS Dienste mithilfe von Service Quotas anzeigen und verwalten](#)
- [AWS IAMDemo der Kontingente](#)

- [AWS re:Invent 2018: Kreisläufe schließen und neue Denkansätze eröffnen: Wie man die Kontrolle über große und kleine Systeme übernimmt](#)

Zugehörige Tools:

- [AWS CodeDeploy](#)
- [AWS CloudTrail](#)
- [Amazon CloudWatch](#)
- [Amazon EventBridge](#)
- [DevOpsAmazon-Guru](#)
- [AWS Config](#)
- [AWS Trusted Advisor](#)
- [AWS CDK](#)
- [AWS Systems Manager](#)
- [AWS Marketplace](#)

REL01-BP05 Automatisieren Sie die Quotenverwaltung

Implementieren Sie Tools, um vor dem Erreichen von Schwellenwerten benachrichtigt zu werden. Mithilfe von AWS Service Quotas können Sie Anfragen zur Erhöhung des Kontingents automatisieren APIs.

Wenn Sie Ihre Configuration Management Database (CMDB) oder Ihr Ticketsystem mit Service Quotas integrieren, können Sie die Nachverfolgung von Anfragen zur Erhöhung der Kontingente und der aktuellen Kontingente automatisieren. Zusätzlich zu den AWS SDK bietet Service Quotas Automatisierung mithilfe von AWS Command Line Interface (AWS CLI).

Typische Anti-Muster:

- Die Kontingente und die Nutzung werden in Tabellen verfolgt.
- Es werden Berichte zur täglichen, wöchentlichen oder monatlichen Nutzung ausgeführt und anschließend wird die Nutzung mit den Kontingenten verglichen.

Vorteile der Einführung dieser bewährten Methode: Durch die automatische Verfolgung der AWS Servicekontingente und die Überwachung Ihrer Nutzung anhand dieses Kontingents können Sie erkennen, wann Sie sich einem Kontingent nähern. Sie können die Automatisierung einrichten,

damit Sie beim Anfordern eine Kontingenterhöhung bei Bedarf unterstützt werden. Wenn sich Ihre Nutzung in die entgegengesetzte Richtung entwickelt, sollten Sie einige Kontingente reduzieren, um von den verringerten Risiken (im Falle von kompromittierten Anmeldeinformationen) und von Kosteneinsparungen zu profitieren.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Mittel

### Implementierungsleitfaden

- Richten Sie eine automatisierte Überwachung ein. Implementieren Sie ToolsSDKs, mit denen Sie benachrichtigt werden, wenn Schwellenwerte erreicht werden.
  - Verwenden Sie Service Quotas und erweitern Sie den Service mit einer automatisierten Kontingentüberwachungslösung wie AWS Limit Monitor oder einem Angebot von AWS Marketplace.
    - [Was ist Service Quotas?](#)
    - [Quota Monitor aktiviert AWS — Lösung AWS](#)
- Richten Sie automatisierte Antworten auf der Grundlage von Kontingentschwellenwerten ein und verwenden Sie Amazon- SNS und AWS Service APIs Quotas.
- Testen Sie die Automatisierung.
  - Konfigurieren Sie Limit-Schwellenwerte.
  - Integrieren Sie Änderungen von AWS Config Bereitstellungspipelines EventBridge, Amazon oder Drittanbietern.
  - Legen Sie unnatürlich niedrige Schwellenwerte für Kontingente fest, um die Reaktionen zu testen.
  - Richten Sie Trigger ein, damit bei Benachrichtigungen geeignete Maßnahmen ergriffen werden und bei Bedarf der AWS Support kontaktiert wird.
  - Lösen Sie Änderungsereignisse manuell aus.
  - Führen Sie eine Ernstfallübung aus, um den Prozess für die Kontingenterhöhung zu testen.

### Ressourcen

Zugehörige Dokumente:

- [APNPartner: Partner, die beim Konfigurationsmanagement helfen können](#)
- [AWS Marketplace: CMDDB Produkte, die helfen, Grenzen zu verfolgen](#)
- [AWS Service Quotas \(früher als Service Limits bezeichnet\)](#)

- [AWS Trusted Advisor Prüfungen bewährter Verfahren \(siehe Abschnitt „Service Limits“\)](#)
- [Quota Monitor aktiviert AWS — AWS Lösung](#)
- [EC2Amazon-Servicebeschränkungen](#)
- [Was ist Service Quotas?](#)

Zugehörige Videos:

- [AWS Live re:inForce 2019 — Service Quotas](#)

REL01-BP06 Stellen Sie sicher, dass zwischen den aktuellen Kontingenten und der maximalen Nutzung eine ausreichende Lücke besteht, um ein Failover zu ermöglichen

In diesem Artikel wird erläutert, wie Sie den Abstand zwischen dem Ressourcenkontingent und Ihrer Nutzung beibehalten können und wie Ihr Unternehmen davon profitieren kann. Wenn Sie eine Ressource nicht mehr nutzen, wird diese Ressource möglicherweise noch auf ein Kontingent angerechnet. Dies kann zu einer fehlgeschlagenen oder nicht mehr erreichbaren Ressource führen. Überprüfen Sie, ob Ihre Kontingente die Überschneidung von ausgefallenen oder nicht zugreifbaren Ressourcen und deren Ersatz abdecken. Bei der Berechnung dieser Lücke sollten Sie Anwendungsfälle wie Netzwerkfehler, Fehler in der Availability Zone oder Fehler in einer Region berücksichtigen.

Gewünschtes Ergebnis: Kleine oder große Fehler bei Ressourcen oder der Ressourcenzugänglichkeit können innerhalb der aktuellen Service-Schwellenwerte abgedeckt werden. Zonenfehler, Netzwerkfehler oder sogar regionale Fehler wurden bei der Ressourcenplanung berücksichtigt.

Typische Anti-Muster:

- Es werden Servicekontingente auf Grundlage des aktuellen Bedarfs eingerichtet, ohne dass Failover-Szenarien berücksichtigt werden.
- Keine Berücksichtigung des Prinzips der statischen Stabilität bei der Berechnung des Spitzenkontingents für einen Service.
- Keine Berücksichtigung des Potenzials nicht zugreifbarer Ressourcen bei der Berechnung des für jede Region benötigten Gesamtkontingents.
- Ohne Berücksichtigung der Grenzen zur Isolierung von AWS Dienstfehlern für einige Dienste und ihrer potenziell abnormalen Nutzungsmuster.

Vorteile der Nutzung dieser bewährten Methode: Wenn die Verfügbarkeit von Anwendungen durch eine Service-Störung beeinträchtigt wird, bietet Ihnen die Cloud die Möglichkeit zur Implementierung von Strategien zur Abschwächung dieser Ereignisse oder der Wiederherstellung. Zu solchen Strategien gehört oft die Erstellung zusätzlicher Ressourcen, um ausgefallene oder unzugängliche Ressourcen zu ersetzen. Ihre Kontingent-Strategie muss diese Failover-Bedingungen berücksichtigen und würde nicht zu einer zusätzlichen Verschlechterung aufgrund des Erreichens von Service-Beschränkungen führen.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Mittel

### Implementierungsleitfaden

Berücksichtigen Sie bei der Bewertung der Kontingente auch Failover-Fälle, die aufgrund einer Verschlechterung auftreten können. Die folgenden Arten von Failover-Fällen sollten in Betracht gezogen werden:

- Ein unterbrochener oder VPC unzugänglicher Zugriff.
- Ein Subnetz, auf das nicht mehr zugegriffen werden kann.
- Eine Availability Zone wurde so stark beeinträchtigt, dass die Erreichbarkeit vieler Ressourcen beeinträchtigt ist.
- Verschiedene Netzwerk-Routen oder Ingress- und Egress-Punkte sind blockiert oder verändert.
- Eine Region ist so stark gestört, dass die Erreichbarkeit vieler Ressourcen beeinträchtigt ist.
- Es gibt mehrere Ressourcen, aber nicht alle sind von einem Fehler in einer Region oder einer Availability Zone betroffen.

Die Entscheidung für einen Failover ist für jede Situation und jeden Kunden individuell, da die Auswirkungen auf den Geschäftsbetrieb sehr unterschiedlich sein können. Wenn Sie sich jedoch operativ für einen Failover von Anwendungen oder Services entscheiden, müssen Sie sich vor dem Ereignis mit der Kapazitätsplanung der Ressourcen am Failover-Standort und den entsprechenden Kontingenten befassen.

Überprüfen Sie die Service-Kontingente für jeden Service und berücksichtigen Sie dabei die möglichen Spitzenwerte. Diese Spitzen können mit Ressourcen zusammenhängen, die über Netzwerkproblemen oder Berechtigungen zwar noch aktiv, aber nicht erreichbar sind. Nicht beendete aktive Ressourcen werden weiterhin auf das Kontingent des Service angerechnet.

### Implementierungsschritte

- Vergewissern Sie sich, dass zwischen Ihrem Service-Kontingent und Ihrer maximalen Nutzung genügend Spielraum besteht, um einen Failover oder den Verlust der Erreichbarkeit aufzufangen.
- Ermitteln Sie die Servicekontingente unter Berücksichtigung von Bereitstellungsmustern, der Verfügbarkeitsanforderungen und des Nutzungsanstiegs.
- Fordern Sie bei Bedarf Kontingenterhöhungen an. Planen Sie den erforderlichen Zeitraum bis zur Bewilligung von Kontingenterhöhungen.
- Bestimmen Sie Ihre Anforderungen an die Zuverlässigkeit (Anzahl der Neunen).
- Legen Sie Fehlerszenarien fest (z. B. Verlust einer Komponente, Availability Zone oder Region).
- Führen Sie eine Bereitstellungsmethode ein (z. B. Canary, Blau/Grün-Bereitstellung, Rot/Schwarz-Bereitstellung oder schrittweise).
- Berücksichtigen Sie einen angemessenen Puffer (z. B. 15 %) in aktuellen Limits.
- Berücksichtigen Sie gegebenenfalls Berechnungen zur statischen Stabilität (zonenbezogen und regional).
- Planen Sie den Nutzungsanstieg (z. B. durch Überwachen des Nutzungstrends).
- Berücksichtigen Sie die Auswirkungen der statischen Stabilität für Ihre kritischsten Workloads. Bewerten Sie Ressourcen entsprechend eines statisch stabilen Systems in allen Regionen und Availability Zones.
- Ziehen Sie den Einsatz von On-Demand-Kapazitätsreservierungen in Betracht, um vor einem Failover Kapazitäten zu reservieren. Diese Strategie kann während kritischer Geschäftszeiten sinnvoll sein, um potenzielle Risiken bei der Beschaffung der richtigen Menge und Art von Ressourcen während eines Failovers zu verringern.

## Ressourcen

### Zugehörige bewährte Methoden:

- [REL01-BP01 Kenntnis der Servicequoten und Einschränkungen](#)
- [REL01-BP02 Servicekontingente über Konten und Regionen hinweg verwalten](#)
- [REL01-BP03 Berücksichtigung fester Servicequoten und Einschränkungen durch die Architektur](#)
- [REL01-BP04 Kontingente überwachen und verwalten](#)
- [REL01-BP05 Automatisieren Sie die Quotenverwaltung](#)
- [REL03-BP01 Wählen Sie, wie Sie Ihre Arbeitslast segmentieren möchten](#)
- [REL10-BP01 Stellen Sie den Workload an mehreren Standorten bereit](#)
- [REL11-BP01 Überwachen Sie alle Komponenten des Workloads, um Fehler zu erkennen](#)

- [REL11-BP03 Automatisieren Sie die Heilung auf allen Ebenen](#)
- [REL12-BP05 Testen Sie die Resilienz mithilfe von Chaos Engineering](#)

#### Zugehörige Dokumente:

- [AWS Die Zuverlässigkeitssäule von Well-Architected Framework: Verfügbarkeit](#)
- [AWS Service Quotas \(früher als Service Limits bezeichnet\)](#)
- [AWS Trusted Advisor Prüfungen bewährter Verfahren \(siehe Abschnitt Service Limits\)](#)
- [AWS Beschränken Sie den Monitor auf AWS Antworten](#)
- [EC2Amazon-Servicebeschränkungen](#)
- [Was ist Service Quotas?](#)
- [How to Request Quota Increase](#)
- [Service endpoints and quotas](#)
- [Service Quotas-Benutzerhandbuch](#)
- [Kontingentmonitor für AWS](#)
- [AWS Grenzen der Fehlerisolierung](#)
- [Availability with redundancy](#)
- [AWS für Daten](#)
- [What is Continuous Integration?](#)
- [What is Continuous Delivery?](#)
- [APNPartner: Partner, die beim Konfigurationsmanagement helfen können](#)
- [Verwaltung des Kontolebenszyklus in account-per-tenant SaaS-Umgebungen auf AWS](#)
- [Verwaltung und Überwachung der API Drosselung Ihrer Workloads](#)
- [Sehen Sie sich AWS Trusted Advisor Empfehlungen in großem Umfang an mit AWS Organizations](#)
- [Automatisierung von Service-Limit-Erhöhungen und Unternehmenssupport mit AWS Control Tower](#)
- [Aktionen, Ressourcen und Bedingungsschlüssel für Service Quotas](#)

#### Zugehörige Videos:

- [AWS Live re:inForce 2019 — Service Quotas](#)
- [Kontingente für AWS Dienste mithilfe von Service Quotas anzeigen und verwalten](#)
- [AWS IAMDemo der Kontingente](#)



- [AWS re:Invent 2018: Kreisläufe schließen und neue Denkansätze eröffnen: Wie man die Kontrolle über große und kleine Systeme übernimmt](#)

#### Zugehörige Tools:

- [AWS CodeDeploy](#)
- [AWS CloudTrail](#)
- [Amazon CloudWatch](#)
- [Amazon EventBridge](#)
- [DevOpsAmazon-Guru](#)
- [AWS Config](#)
- [AWS Trusted Advisor](#)
- [AWS CDK](#)
- [AWS Systems Manager](#)
- [AWS Marketplace](#)

## REL2. Wie wird die Netzwerktopologie geplant?

Workloads existieren oft in mehreren Umgebungen. Dazu gehören mehrere Cloud-Umgebungen (sowohl öffentlich zugänglich als auch privat) und möglicherweise Ihre bestehende Rechenzentrumsinfrastruktur. Die Pläne müssen Netzwerkaspekte wie systeminterne und systemübergreifende Konnektivität, Verwaltung öffentlicher IP-Adressen, Verwaltung privater IP-Adressen und Auflösung von Domainnamen beinhalten.

#### Bewährte Methoden

- [REL02-BP01 Verwenden Sie hochverfügbare Netzwerkkonnektivität für Ihre öffentlichen Workload-Endpunkte](#)
- [REL02-BP02 Bereitstellung redundanter Konnektivität zwischen privaten Netzwerken in der Cloud und lokalen Umgebungen](#)
- [REL02-BP03 Stellen Sie sicher, dass die IP-Subnetzzuweisung Erweiterung und Verfügbarkeit berücksichtigt](#)
- [REL02-BP04 Bevorzugen Sie hub-and-spoke Topologien gegenüber Mesh many-to-many](#)
- [REL02-BP05 Erzwingen Sie nicht überlappende private IP-Adressbereiche in allen privaten Adressräumen, in denen sie verbunden sind](#)

## REL02-BP01 Verwenden Sie hochverfügbare Netzwerkkonnektivität für Ihre öffentlichen Workload-Endpunkte

Durch den Aufbau hochverfügbarer Netzwerkkonnektivität zu öffentlichen Endpunkten Ihrer Workloads können Sie Ausfallzeiten aufgrund von Verbindungsverlusten reduzieren und die Verfügbarkeit und Arbeitslast verbessern. SLA Verwenden Sie dazu hochverfügbare Content Delivery Networks (CDNs) DNS, API Gateways, Load Balancing oder Reverse-Proxys.

Gewünschtes Ergebnis: Es ist von entscheidender Bedeutung, eine hochverfügbare Netzwerkkonnektivität für Ihre öffentlichen Endpunkte zu planen, aufzubauen und in Betrieb zu nehmen. Wenn Ihr Workload aufgrund eines Konnektivitätsverlustes nicht mehr erreichbar ist, sehen Ihre Kunden Ihr System als ausgefallen an – selbst wenn Ihr Workload läuft und verfügbar ist. Durch die Kombination einer hochverfügbaren und stabilen Netzwerkkonnektivität für die öffentlichen Endpunkte Ihres Workloads mit einer stabilen Architektur für Ihren Workload selbst können Sie Ihren Kunden die bestmögliche Verfügbarkeit und das bestmögliche Serviceniveau bieten.

AWS Global Accelerator, Amazon CloudFront, Amazon API Gateway URLs AWS AppSync APIs, AWS Lambda Function und Elastic Load Balancing (ELB) bieten allesamt hochverfügbare öffentliche Endpunkte. Amazon Route 53 bietet einen hochverfügbaren DNS Service für die Auflösung von Domainnamen, um zu überprüfen, ob Ihre öffentlichen Endpunktadressen aufgelöst werden können.

Sie können auch AWS Marketplace Software-Appliances für Lastenausgleich und Proxying testen.

Typische Anti-Muster:

- Entwurf eines hochverfügbaren Workloads ohne vorherige Planung DNS und Netzwerkkonnektivität für hohe Verfügbarkeit.
- Verwendung öffentlicher Internetadressen auf einzelnen Instances oder Containern und Verwaltung der Konnektivität zu diesen Instanzen mit DNS.
- Verwendung von IP-Adressen anstelle von Domain-Namen zur Lokalisierung von Services.
- Keine Tests von Szenarien, in denen die Konnektivität zu Ihren öffentlichen Endpunkten verloren geht.
- Keine Analyse des Bedarfs für den Netzwerkdurchsatz und die Verteilungsmuster im Netzwerk.
- Keine Tests und Planungen für Szenarien, in denen die Internet-Netzwerkkonnektivität zu Ihren öffentlichen Endpunkten der Workloads unterbrochen werden könnte.
- Bereitstellen von Inhalten (z. B. Webseiten, statische Komponenten oder Mediendateien) für ein großes geografisches Gebiet ohne Verwendung eines Content-Delivery-Networks.

- Distributed-Denial-of-Service (DDoS) -Angriffe sind nicht geplant. DDoSBei Angriffen besteht die Gefahr, dass legitimer Datenverkehr gesperrt und die Verfügbarkeit für Ihre Benutzer beeinträchtigt wird.

Vorteile der Nutzung dieser bewährten Methode: Die Planung einer hochverfügbaren und stabilen Netzwerkkonnektivität stellt sicher, dass Ihr Workload für Ihre Benutzer zugreifbar und verfügbar ist.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Hoch

### Implementierungsleitfaden

Das Wichtigste beim Aufbau einer hochverfügbaren Netzwerkkonnektivität zu Ihren öffentlichen Endpunkten ist das Routing des Datenverkehrs. Um zu überprüfen, ob Ihr Datenverkehr die Endgeräte erreichen kann, DNS müssen diese in der Lage sein, die Domainnamen in die entsprechenden IP-Adressen aufzulösen. Verwenden Sie ein hochverfügbares und skalierbares [Domain Name System \(DNS\)](#) wie Amazon Route 53, um die DNS Datensätze Ihrer Domain zu verwalten. Sie können außerdem die von Amazon Route 53 bereitgestellten Zustandsprüfungen verwenden. Die Integritätsprüfungen stellen sicher, dass Ihre Anwendung erreichbar, verfügbar und funktionsfähig ist. Sie können auch so eingerichtet werden, dass sie das Verhalten Ihres Benutzers nachahmen, z. B. das Anfordern einer Webseite oder einer bestimmten URL Website. Im Falle eines Fehlers reagiert Amazon Route 53 auf DNS Lösungsanfragen und leitet den Datenverkehr nur an fehlerfreie Endpunkte weiter. Sie können auch die von Amazon Route 53 angebotenen geo DNS - und latenzbasierten Routing-Funktionen in Betracht ziehen.

Verwenden Sie Elastic Load Balancing (ELB), um zu überprüfen, ob Ihr Workload selbst hochverfügbar ist. Amazon Route 53 kann verwendet werdenELB, um den Traffic gezielt auf die Ziel-Compute-Instances zu verteilen. Sie können Amazon API Gateway auch zusammen mit AWS Lambda für eine serverlose Lösung verwenden. Kunden können Workloads auch in mehreren ausführen. AWS-Regionen Mit einem [Multi-Site Aktiv/Aktiv-Muster](#) kann der Workload den Datenverkehr aus mehreren Regionen bedienen. Bei einem Multi-Site Aktiv/Passiv-Muster bedient der Workload den Datenverkehr aus der aktiven Region, während die Daten in die sekundäre Region repliziert werden, die im Falle eines Fehlers in der primären Region aktiv wird. Route 53-Zustandsprüfungen können dann verwendet werden, um den DNS Failover von einem beliebigen Endpunkt in einer primären Region zu einem Endpunkt in einer sekundären Region zu kontrollieren und so zu überprüfen, ob Ihr Workload erreichbar und für Ihre Benutzer verfügbar ist.

Amazon CloudFront bietet eine einfache MöglichkeitAPI, Inhalte mit geringer Latenz und hohen Datenübertragungsraten zu verteilen, indem Anfragen über ein Netzwerk von Edge-Standorten

auf der ganzen Welt bearbeitet werden. Content Delivery Networks (CDNs) bedienen Kunden, indem sie Inhalte bereitstellen, die sich an einem Ort in der Nähe des Benutzers befinden oder dort zwischengespeichert werden. Dadurch wird auch die Verfügbarkeit Ihrer Anwendung verbessert, da die Last für Inhalte von Ihren Servern zu CloudFront den [Edge-Standorten](#) verlagert wird. Die Edge-Standorte und regionalen Edge-Caches halten zwischengespeicherte Kopien Ihrer Inhalte in der Nähe Ihrer Benutzer vor, was einen schnellen Abruf ermöglicht und die Erreichbarkeit und Verfügbarkeit Ihres Workloads erhöht.

Bei Workloads mit geografisch verteilten Benutzern können Sie AWS Global Accelerator so die Verfügbarkeit und Leistung der Anwendungen verbessern. AWS Global Accelerator stellt statische Anycast-IP-Adressen bereit, die als fester Einstiegspunkt für Ihre in einer oder mehreren gehosteten Anwendungen dienen. AWS-Regionen Dadurch kann der Datenverkehr so nah wie möglich an Ihren Benutzern in das AWS globale Netzwerk gelangen, was die Erreichbarkeit und Verfügbarkeit Ihrer Workloads verbessert. AWS Global Accelerator überwacht außerdem den Zustand Ihrer Anwendungsendpunkte mithilfe von TCPHTTP, und Integritätsprüfungen. HTTPS Jede Änderung im Zustand oder in der Konfiguration Ihrer Endpunkte leitet den Benutzerverkehr auf funktionierende Endpunkte weiter, die Ihren Benutzern die beste Leistung und Verfügbarkeit bieten. Darüber hinaus AWS Global Accelerator verfügt es über ein fehlerisolierendes Design, das zwei statische IPv4 Adressen verwendet, die von unabhängigen Netzwerkzonen bedient werden, wodurch die Verfügbarkeit Ihrer Anwendungen erhöht wird.

Um Kunden vor DDoS Angriffen zu schützen, bietet AWS AWS Shield Standard Shield Standard wird automatisch aktiviert und schützt vor gängigen Infrastrukturangriffen (Layer 3 und 4) wie SYN UDP /Floods und Reflection-Angriffen, um die Hochverfügbarkeit Ihrer Anwendungen zu gewährleisten AWS. Für zusätzlichen Schutz vor ausgefeilteren und größeren Angriffen (wie UDP Floods), State Exhaustion-Angriffen (wie TCP SYN Floods) und zum Schutz Ihrer Anwendungen, die auf Amazon Elastic Compute Cloud (AmazonEC2), Elastic Load Balancing (ELB) CloudFront AWS Global Accelerator, Amazon und Route 53 ausgeführt werden, können Sie die Verwendung von AWS Shield Advanced Verwenden Sie zum Schutz vor Angriffen auf Anwendungsebene wie HTTP POST GET Überschwemmungen. AWS WAF AWS WAF kann IP-Adressen, HTTP Header, HTTP Textkörper, URI Zeichenketten, SQL Injection und Cross-Site-Scripting-Bedingungen verwenden, um zu bestimmen, ob eine Anfrage blockiert oder zugelassen werden soll.

## Implementierungsschritte

1. Hochverfügbar einrichtenDNS: Amazon Route 53 ist ein hochverfügbarer und skalierbarer [Domain Name System \(DNS\)](#) -Webservice. Route 53 verbindet Benutzeranfragen mit

- Internetanwendungen, die vor Ort AWS oder vor Ort ausgeführt werden. Weitere Informationen finden Sie unter [Amazon Route 53 als Ihren DNS Service konfigurieren](#).
2. Richten Sie Zustandsprüfungen ein: Wenn Sie Amazon Route 53 verwenden, vergewissern Sie sich, dass nur korrekt funktionierende Ziele auflösbar sind. [Erstellen Sie zunächst Route 53-Zustandsprüfungen und konfigurieren Sie das DNS Failover](#). Bei der Einrichtung von Zustandsprüfungen sind die folgenden Aspekte zu beachten:
    - a. [So ermittelt Amazon Route 53, ob eine Zustandsprüfung fehlerfrei ist](#)
    - b. [Erstellen, Aktualisieren und Löschen von Zustandsprüfungen](#)
    - c. [Den Status von Zustandsprüfungen überwachen und Benachrichtigungen erhalten](#)
    - d. [Bewährte Methoden für Amazon Route 53 DNS](#)
  3. [Connect Sie Ihren DNS Service mit Ihren Endpunkten](#).
    - a. Wenn Sie Elastic Load Balancing als Ziel für Ihren Datenverkehr verwenden, erstellen Sie einen [Alias-Eintrag](#) mit Amazon Route 53, der auf den regionalen Endpunkt Ihres Load-Balancers verweist. Setzen Sie bei der Erstellung des Alias-Eintrags die Option „Zielzustand evaluieren“ auf „Ja“. Setzen Sie bei der Erstellung des Alias-Eintrags die Option „Zielzustand evaluieren“ auf „Ja“.
    - b. Verwenden Sie für serverlose oder private Workloads, APIs wenn API Gateway verwendet wird, [Route 53, um den Verkehr an Gateway weiterzuleiten](#). API
  4. Entscheiden Sie sich für ein Content Delivery Netzwerk.
    - a. Für die Bereitstellung von Inhalten über Edge-Standorte, die näher am Benutzer liegen, sollten Sie zunächst verstehen, [wie Inhalte bereitgestellt werden CloudFront](#).
    - b. Beginnen Sie mit einer [einfachen CloudFront Verteilung](#). CloudFront weiß dann, woher die Inhalte geliefert werden sollen, und weiß, wie die Bereitstellung von Inhalten nachverfolgt und verwaltet werden kann. Es ist wichtig, die folgenden Aspekte zu verstehen und zu berücksichtigen, wenn Sie die CloudFront Verteilung einrichten:
      - i. [So funktioniert das Caching mit CloudFront Edge-Standorten](#)
      - ii. [Erhöhung des Anteils der Anfragen, die direkt von den CloudFront Caches aus bedient werden \(Cache-Trefferquote\)](#)
      - iii. [Amazon CloudFront Origin Shield verwenden](#)
      - iv. [Optimierung der Hochverfügbarkeit mit CloudFront Origin-Failover](#)
  5. Schutz auf Anwendungsebene einrichten: AWS WAF Schützt Sie vor gängigen Web-Exploits und Bots, die die Verfügbarkeit beeinträchtigen, die Sicherheit gefährden oder übermäßig viele [Ressourcen verbrauchen können](#). Weitere Informationen dazu finden Sie unter [Erste Schritte](#)

mit. Erfahren Sie, [wie das AWS WAF funktioniert](#) und wann Sie bereit sind, Schutzmaßnahmen gegen HTTP POST AND GET Fluten auf Anwendungsebene zu implementieren. AWS WAF Sie können AWS WAF dies auch in der CloudFront Dokumentation zur [AWS WAF Funktionsweise mit CloudFront Amazon-Funktionen nachlesen](#).

6. Richten Sie zusätzlichen DDoS Schutz ein: Standardmäßig erhalten alle AWS Kunden ohne zusätzliche Kosten Schutz vor den häufigsten DDoS Angriffen auf Netzwerk- und Transportebene, die AWS Shield Standard auf Ihre Website oder Anwendung abzielen. Für zusätzlichen Schutz von mit dem Internet verbundenen Anwendungen, die auf AmazonEC2, Elastic Load Balancing CloudFront, Amazon und Amazon Route 53 ausgeführt werden AWS Global Accelerator, können Sie [Beispiele für DDoS belastbare](#) Architekturen in Betracht ziehen [AWS Shield Advanced](#) und überprüfen. [Informationen zum Schutz Ihres Workloads und Ihrer öffentlichen Endgeräte vor DDoS Angriffen finden Sie unter Erste Schritte mit. AWS Shield Advanced](#)

## Ressourcen

### Zugehörige bewährte Methoden:

- [REL10-BP01 Stellen Sie den Workload an mehreren Standorten bereit](#)
- [REL10-BP02 Wählen Sie die geeigneten Standorte für Ihren Einsatz an mehreren Standorten](#)
- [REL11-BP04 Verlassen Sie sich bei der Wiederherstellung auf die Datenebene und nicht auf die Steuerebene](#)
- [REL11-BP06 Benachrichtigungen senden, wenn Ereignisse die Verfügbarkeit beeinträchtigen](#)

### Zugehörige Dokumente:

- [APNPartner: Partner, die Ihnen bei der Planung Ihres Netzwerks helfen können](#)
- [AWS Marketplace für Netzwerkinfrastruktur](#)
- [Was ist AWS Global Accelerator?](#)
- [Was ist Amazon CloudFront?](#)
- [Was ist Amazon Route 53?](#)
- [Was ist Elastic Load Balancing?](#)
- [Network Connectivity capability - Establishing Your Cloud Foundations](#)
- [Was ist Amazon API Gateway?](#)
- [Was sind AWS WAF, AWS Shield, und AWS Firewall Manager?](#)

- [Was ist Amazon Application Recovery Controller?](#)
- [Konfigurieren Sie benutzerdefinierte Integritätsprüfungen für DNS Failover](#)

#### Zugehörige Videos:

- [AWS re:Invent 2022 — Verbessern Sie Leistung und Verfügbarkeit mit AWS Global Accelerator](#)
- [AWS re:Invent 2020: Globales Verkehrsmanagement mit Amazon Route 53](#)
- [AWS re:Invent 2022 — Betrieb hochverfügbarer Multi-AZ-Anwendungen](#)
- [AWS re:Invent 2022 — Tauchen Sie tief in die Netzwerkinfrastruktur ein AWS](#)
- [AWS re:Invent 2022 — Aufbau belastbarer Netzwerke](#)

#### Zugehörige Beispiele:

- [Notfallwiederherstellung mit Amazon Application Recovery Controller \(ARC\)](#)
- [Workshops zur Zuverlässigkeit](#)
- [AWS Global Accelerator Werkstatt](#)

REL02-BP02 Bereitstellung redundanter Konnektivität zwischen privaten Netzwerken in der Cloud und lokalen Umgebungen

Implementieren Sie Redundanz in Ihren Verbindungen zwischen privaten Netzwerken in der Cloud und On-Premises-Umgebungen, um die Stabilität der Konnektivität zu erreichen. Dies kann erreicht werden, indem zwei oder mehr Verbindungen und Datenverkehrspfade bereitgestellt werden, sodass die Konnektivität bei Netzwerkausfällen erhalten bleibt.

#### Typische Anti-Muster:

- Sie verlassen sich auf nur eine Netzwerkverbindung, was zu einer einzigen Fehlerquelle führt.
- Sie verwenden nur einen VPN Tunnel oder mehrere Tunnel, die in derselben Availability Zone enden.
- Sie verlassen sich ISP bei der VPN Konnektivität auf einen, was bei Ausfällen zu ISP Komplettausfällen führen kann.
- Sie implementieren keine dynamischen Routing-Protokolle wie BGP, die für die Umleitung des Datenverkehrs bei Netzwerkunterbrechungen von entscheidender Bedeutung sind.

- Sie ignorieren die Bandbreitenbeschränkungen von VPN Tunneln und überschätzen deren Backup-Fähigkeiten.

Vorteile der Nutzung dieser bewährten Methode: Durch die Implementierung redundanter Konnektivität zwischen Ihrer Cloud-Umgebung und Ihrer Unternehmens- bzw. On-Premises-Umgebung wird die sichere Kommunikation der abhängigen Services zwischen den beiden Umgebungen gewährleistet.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Hoch

### Implementierungsleitfaden

Wenn Sie Ihr lokales Netzwerk mit AWS Direct Connect verbinden AWS, können Sie eine maximale Netzwerkausfallsicherheit (SLA von 99,99%) erreichen, indem Sie separate Verbindungen verwenden, die auf unterschiedlichen Geräten an mehr als einem lokalen Standort und an mehr als einem Standort enden. AWS Direct Connect Diese Topologie bietet Widerstandsfähigkeit gegen Geräteausfälle, Verbindungsprobleme und komplette Standortausfälle. Alternativ können Sie eine hohe Ausfallsicherheit (SLA von 99,9%) erreichen, indem Sie zwei individuelle Verbindungen zu mehreren Standorten verwenden (jeder lokale Standort ist mit einem einzigen Direct Connect-Standort verbunden). Dieser Ansatz schützt vor Verbindungsunterbrechungen, die durch getrennte Glasfaserkabel oder Geräteausfälle verursacht werden, und trägt dazu bei, die Auswirkungen kompletter Standortausfälle zu mindern. Das AWS Direct Connect Resiliency Toolkit kann Sie beim Entwurf Ihrer Topologie unterstützen. AWS Direct Connect

Sie können auch erwägen AWS Site-to-Site VPN , eine AWS Transit Gateway als kostengünstiges Backup für Ihre primäre Verbindung zu verwenden. AWS Direct Connect Dieses Setup ermöglicht kostengünstiges Multipath (ECMP) -Routing über mehrere VPN Tunnel hinweg und ermöglicht so einen Durchsatz von bis zu 50 Gbit/s, obwohl jeder VPN Tunnel auf 1,25 Gbit/s begrenzt ist. Es ist jedoch wichtig zu beachten, dass dies immer noch die effektivste Wahl AWS Direct Connect ist, um Netzwerkunterbrechungen zu minimieren und eine stabile Konnektivität zu gewährleisten.

Wenn Sie Ihre Cloud-Umgebung VPNs über das Internet mit Ihrem lokalen Rechenzentrum verbinden, konfigurieren Sie zwei VPN Tunnel als Teil einer einzigen Verbindung. site-to-site VPN Jeder Tunnel sollte aus Gründen der Hochverfügbarkeit in einer anderen Availability Zone enden und redundante Hardware verwenden, um Ausfälle von On-Premises-Geräten zu verhindern. Ziehen Sie außerdem mehrere Internetverbindungen von verschiedenen Internetdienstanbietern (ISPs) an Ihrem Standort in Betracht, um eine vollständige VPN Verbindungsunterbrechung aufgrund eines einzigen ISP Ausfalls zu vermeiden. Durch die Auswahl ISPs unterschiedlicher Routing- und



Infrastrukturoptionen, insbesondere solcher mit separaten physischen Pfaden zu AWS Endpunkten, wird eine hohe Verfügbarkeit der Konnektivität gewährleistet.

Neben der physischen Redundanz mit mehreren AWS Direct Connect Verbindungen und mehreren VPN Tunneln (oder einer Kombination aus beidem) ist auch die Implementierung von dynamischem Routing mit dem Border Gateway Protocol (BGP) von entscheidender Bedeutung. Dynamic BGP ermöglicht die automatische Umleitung des Datenverkehrs von einem Pfad zum anderen auf der Grundlage von Netzwerkbedingungen in Echtzeit und konfigurierten Richtlinien. Dieses dynamische Verhalten ist besonders vorteilhaft zur Aufrechterhaltung der Netzwerkverfügbarkeit und Servicekontinuität bei Verbindungs- oder Netzwerkausfällen. Es wählt schnell alternative Pfade aus und verbessert so die Ausfallsicherheit und Zuverlässigkeit des Netzwerks.

### Implementierungsschritte

- Erwerben Sie hochverfügbare Konnektivität zwischen AWS und Ihrer lokalen Umgebung.
  - Verwenden Sie mehrere AWS Direct Connect Verbindungen oder VPN Tunnel zwischen separat bereitgestellten privaten Netzwerken.
  - Verwenden Sie mehrere AWS Direct Connect Standorte für eine hohe Verfügbarkeit.
  - Wenn Sie mehrere verwenden AWS-Regionen, sorgen Sie für Redundanz in mindestens zwei von ihnen.
- Verwenden Sie AWS Transit Gateway, wenn möglich, um Ihre [VPNVerbindung](#) zu beenden.
- Testen Sie AWS Marketplace Geräte, auf die [Sie Ihre SD-Verbindung beenden VPNs oder verlängern WAN möchten AWS](#). Wenn Sie AWS Marketplace Appliances verwenden, stellen Sie redundante Instanzen für hohe Verfügbarkeit in verschiedenen Availability Zones bereit.
- Stellen Sie auf Ihrer On-Premises-Umgebung eine redundante Verbindung her.
  - Möglicherweise benötigen Sie redundante Verbindungen zu mehreren, AWS-Regionen um Ihre Verfügbarkeitsanforderungen zu erfüllen.
  - Verwenden Sie das [AWS Direct Connect Resiliency Toolkit](#), um loszulegen.

### Ressourcen

#### Zugehörige Dokumente:

- [AWS Direct Connect Empfehlungen zur Ausfallsicherheit](#)
- [Verwendung redundanter Site-to-Site VPN Verbindungen zur Bereitstellung von Failover](#)
- [Routing-Richtlinien und Communities BGP](#)

- [Aktive/Aktive und Aktive/Passive Konfigurationen in AWS Direct Connect](#)
- [APNPartner: Partner, die Ihnen bei der Planung Ihres Netzwerks helfen können](#)
- [AWS Marketplace für Netzwerkinfrastruktur](#)
- Whitepaper [Amazon Virtual Private Cloud Connectivity Options](#)
- [Aufbau einer skalierbaren und sicheren VPC AWS Multi-Netzwerk-Infrastruktur](#)
- [Verwendung redundanter Site-to-Site VPN Verbindungen zur Bereitstellung von Failover](#)
- [Verwenden Sie das AWS Direct Connect Resiliency Toolkit für den Einstieg](#)
- [VPC-Endpunkte und VPC Endpunktdienste \(AWS PrivateLink\)](#)
- [Was ist Amazon VPC?](#)
- [What is a transit gateway?](#)
- [Was ist AWS Site-to-Site VPN?](#)
- [Working with Direct Connect gateways](#)

Zugehörige Videos:

- [AWS re:Invent 2018: Fortschrittliches VPC Design und neue Funktionen für Amazon VPC](#)
- [AWS re:Invent 2019: AWS Transit Gateway Referenzarchitekturen für viele VPCs](#)

REL02-BP03 Stellen Sie sicher, dass die IP-Subnetzzuweisung Erweiterung und Verfügbarkeit berücksichtigt

Die VPC IP-Adressbereiche von Amazon müssen groß genug sein, um den Workload-Anforderungen gerecht zu werden, einschließlich der Berücksichtigung future Erweiterungen und der Zuweisung von IP-Adressen zu Subnetzen in Availability Zones. Dazu gehören Load Balancer, EC2 Instances und containerbasierte Anwendungen.

Wenn Sie Ihre Netzwerktopologie planen, besteht der erste Schritt in der Definition des IP-Adressbereichs. Private IP-Adressbereiche (gemäß den Richtlinien von RFC 1918) sollten jedem Bereich zugewiesen werden. VPC Berücksichtigen Sie im Rahmen dieses Prozesses die folgenden Anforderungen:

- Erlauben Sie IP-Adressraum für mehr als einen VPC pro Region.
- Lassen Sie innerhalb einer VPC Platz für mehrere Subnetze frei, sodass Sie mehrere Availability Zones abdecken können.

- Erwägen Sie, ungenutzten CIDR Blockspeicher VPC für future Erweiterungen zu belassen.
- Stellen Sie sicher, dass ein IP-Adressraum vorhanden ist, um die Anforderungen aller vorübergehenden Flotten von EC2 Amazon-Instances zu erfüllen, die Sie möglicherweise verwenden, z. B. Spot-Flotten für maschinelles Lernen, EMR Amazon-Cluster oder Amazon Redshift-Cluster. Kubernetes-Cluster wie Amazon Elastic Kubernetes Service (AmazonEKS) sollten ebenfalls berücksichtigt werden, da jedem Kubernetes-Pod standardmäßig eine routbare Adresse aus dem Block zugewiesen wird. VPC CIDR
- Beachten Sie, dass die ersten vier IP-Adressen und die letzte IP-Adresse in jedem CIDR Subnetzblock reserviert und nicht für Sie verfügbar sind.
- Beachten Sie, dass der ursprüngliche VPC CIDR Block, der Ihnen zugewiesen wurde, VPC nicht geändert oder gelöscht werden kann. Sie können dem jedoch zusätzliche CIDR Blöcke hinzufügen, die sich nicht überschneiden. VPC Das Subnetz IPv4 CIDRs kann nicht geändert werden, kann es jedoch. IPv6 CIDRs
- Der größtmögliche VPC CIDR Block ist ein /16 und der kleinste ist ein /28.
- Ziehen Sie andere verbundene Netzwerke (VPClokale Netzwerke oder andere Cloud-Anbieter) in Betracht und achten Sie darauf, dass sich der IP-Adressraum nicht überschneidet. Weitere Informationen finden Sie unter [REL02-BP05 Erzwingen Sie sich nicht überlappende private IP-Adressbereiche in allen privaten Adressräumen](#), mit denen sie verbunden sind.

Gewünschtes Ergebnis: Ein skalierbares IP-Subnetz kann Ihnen helfen, zukünftiges Wachstum zu bewältigen und unnötige Verschwendung zu vermeiden.

Typische Anti-Muster:

- Wenn future Wachstum nicht berücksichtigt wird, was zu kleinen CIDR Blöcken führt, die neu konfiguriert werden müssen, was möglicherweise zu Ausfallzeiten führen kann.
- Es wird falsch eingeschätzt, wie viele IP-Adressen ein Elastic Load Balancer verwenden kann.
- Es werden viele Load Balancer mit hohem Datenverkehr in denselben Subnetzen bereitgestellt.
- Es werden automatische Skalierungsmechanismen verwendet, während der Verbrauch von IP-Adressen nicht überwacht wird.
- Definition übermäßig großer CIDR Bereiche, die weit über die future Wachstumserwartungen hinausgehen, was zu Schwierigkeiten beim Peering mit anderen Netzwerken mit überlappenden Adressbereichen führen kann.

Vorteile der Nutzung dieser bewährten Methode: So wird sichergestellt, dass Sie das Wachstum Ihrer Workloads bewältigen können und beim Hochskalieren weiterhin die entsprechende Verfügbarkeit bereitstellen.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel

### Implementierungsleitfaden

Berücksichtigen Sie bei der Planung Ihres Netzwerks Ihr zukünftiges Wachstum, die Einhaltung gesetzlicher Vorschriften sowie die Kompatibilität mit anderen Netzwerken. Das Wachstum kann unterschätzt werden, gesetzliche Vorschriften können sich ändern, und bei Unternehmensübernahmen oder privaten Netzwerkverbindungen kann die Implementierung ohne fundierte Planung zur Herausforderung werden.

- Wählen Sie die relevanten Regionen auf der Grundlage Ihrer Service AWS-Konten -, Latenz-, regulatorischen und Disaster Recovery (DR) -Anforderungen aus.
- Identifizieren Sie Ihren Bedarf an regionalen VPC Bereitstellungen.
- Identifizieren Sie die Größe der VPCs.
  - Stellen Sie fest, ob Sie VPC Multikonnektivität einsetzen werden.
    - [Was ist ein Transit-Gateway?](#)
    - [VPC Multikonnektivität in einer Region](#)
  - Ermitteln Sie, ob aufgrund von Compliance-Anforderungen getrennte Netzwerke erforderlich sind.
  - Stellen Sie CIDR Blöcke VPCs mit entsprechender Größe her, um Ihren aktuellen und future Bedürfnissen gerecht zu werden.
    - Wenn Sie unbekannte Wachstumsprognosen haben, möchten Sie vielleicht lieber größere CIDR Blöcke wählen, um das Potenzial für future Neukonfigurationen zu verringern.
  - Erwägen Sie, die [IPv6 Adressierung](#) für Subnetze als Teil eines Dual-Stacks zu verwenden. VPC IPv6 eignet sich gut für den Einsatz in privaten Subnetzen mit Flotten von kurzlebigen Instances oder Containern, für die andernfalls eine große Anzahl von Adressen erforderlich wäre. IPv4

### Ressourcen

Zugehörige bewährte Methoden für Well-Architected:

- [REL02-BP05 Erzwingen Sie, dass sich private IP-Adressbereiche nicht überschneiden, in allen privaten Adressräumen, mit denen sie verbunden sind](#)

## Zugehörige Dokumente:

- [APNPartner: Partner, die Ihnen bei der Planung Ihres Netzwerks helfen können](#)
- [AWS Marketplace für Netzwerkinfrastruktur](#)
- Whitepaper [Amazon Virtual Private Cloud Connectivity Options](#)
- [Multiple data center HA network connectivity](#)
- [VPCMultikonnektivität in einer Region](#)
- [Was ist AmazonVPC?](#)
- [IPv6auf AWS](#)
- [IPv6auf Referenzarchitekturen](#)
- [Amazon Elastic Kubernetes Service startet Unterstützung IPv6](#)
- [Empfehlungen für Ihren VPC — Classic Load Balancers](#)
- [Availability Zone-Subnetze — Application Load Balancers](#)
- [Verfügbarkeitszonen — Netzwerk-Load-Balancer](#)

## Zugehörige Videos:

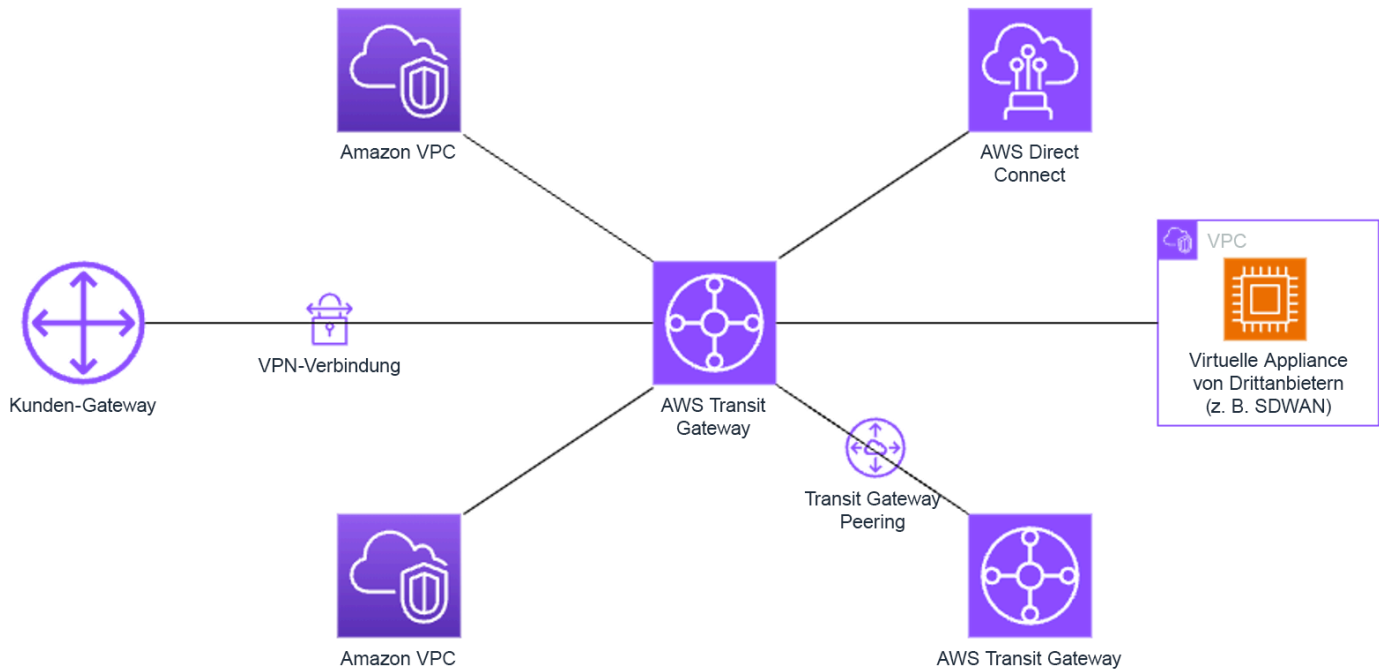
- [AWS re:Invent 2018: Fortschrittliches VPC Design und neue Funktionen für Amazon VPC \(03\) NET3](#)
- [AWS re:Invent 2019: AWS Transit Gateway Referenzarchitekturen für viele \(06-R1\) VPCs NET4](#)
- [AWS re:Invent 2023: Bereit für das, was als Nächstes kommt? AWS Gestaltung von Netzwerken für Wachstum und Flexibilität \(0\) NET31](#)

REL02-BP04 Bevorzugen Sie hub-and-spoke Topologien gegenüber Mesh many-to-many

Wenn Sie mehrere private Netzwerke wie Virtual Private Clouds (VPCs) und lokale Netzwerke verbinden, sollten Sie sich für eine hub-and-spoke Topologie anstelle einer Mesh-Topologie entscheiden. Im Gegensatz zu Mesh-Topologien, bei denen jedes Netzwerk direkt mit den anderen verbunden ist und die Komplexität und den Verwaltungsaufwand erhöht, zentralisiert die hub-and-spoke Architektur Verbindungen über einen einzigen Hub. Diese Zentralisierung vereinfacht die Netzwerkstruktur und verbessert deren Bedienbarkeit, Skalierbarkeit und Kontrolle.

AWS Transit Gateway ist ein verwalteter, skalierbarer und hochverfügbarer Dienst, der für den Aufbau von Netzwerken konzipiert ist. hub-and-spoke AWS Er dient als zentraler Knotenpunkt Ihres Netzwerks, der Netzwerksegmentierung, zentralisiertes Routing und die vereinfachte Verbindung zu

Cloud- und On-Premises-Umgebungen ermöglicht. Die folgende Abbildung zeigt, wie Sie damit Ihre AWS Transit Gateway hub-and-spoke Topologie erstellen können.



Typische Anti-Muster:

- Sie verkomplizieren die Routing-Richtlinien in einer hub-and-spoke Architektur, wodurch die Netzwerkeffizienz beeinträchtigt wird und sowohl die Fehlerbehebung als auch die proaktive Verwaltung erschwert werden.
- Eine unzureichende routingbasierte Segmentierung innerhalb des Hubs kann zu Sicherheitsschwachstellen führen, die das Netzwerk potenziell unbefugten Zugriffen aussetzen.
- Ohne sorgfältige Optimierung kann der über den Hub geleitete Verkehr zu höheren Datenübertragungskosten führen, insbesondere für den Verkehr, der Availability Zones und Regions passiert. Effektive Verkehrsmanagementstrategien sind für die Kostenkontrolle unerlässlich.

Vorteile der Einführung dieser bewährten Methode: Mit zunehmender Anzahl verbundener Netzwerke werden Verwaltung und Erweiterung der vernetzten Konnektivität immer schwieriger. AWS Transit Gateway bietet einen skalierbaren und zuverlässigen verwalteten Hub für den Aufbau und Betrieb Ihrer hub-and-spoke Topologien. Wenn Sie ihn verwenden, können Sie Verbindungen herstellen und das Routing des Datenverkehrs über mehrere Netzwerke zentralisieren.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Mittel

### Implementierungsleitfaden

- Planen Sie Ihr Netzwerk.
- Erstellen Sie Ihre AWS Transit Gateway
- Hängen Sie Ihre anVPCs.
- Erstellen Sie bei Bedarf VPN Verbindungen oder Direct Connect-Gateways und verknüpfen Sie sie mit dem Transit Gateway.
- Definieren Sie mithilfe der Konfiguration Ihrer Transit Gateway Gateway-Routentabellen, wie der Verkehr zwischen den verbundenen VPCs und anderen Verbindungen weitergeleitet wird.
- Verwenden Sie Amazon CloudWatch , um Konfigurationen zu überwachen und nach Bedarf anzupassen, um Leistung und Kosten zu optimieren.

### Ressourcen

#### Zugehörige Dokumente:

- [Was ist ein Transit-Gateway?](#)
- [Aufbau einer skalierbaren und sicheren VPC AWS Multi-Netzwerk-Infrastruktur](#)
- [Aufbau eines globalen Netzwerks mithilfe von AWS Transit Gateway regionsübergreifendem Peering](#)
- [Amazon Virtual Private Cloud Connectivity Options](#)
- [APNPartner: Partner, die Ihnen bei der Planung Ihres Netzwerkes helfen können](#)
- [AWS Marketplace für Netzwerkinfrastruktur](#)

#### Zugehörige Videos:

- [AWS re:Invent 2023 — AWS Grundlagen der Netzwerktechnik](#)
- [AWS re:Invent 2023 — Fortschrittliche VPC Designs und neue Funktionen](#)

REL02-BP05 Erzwingen Sie nicht überlappende private IP-Adressbereiche in allen privaten Adressräumen, in denen sie verbunden sind

Die IP-Adressbereiche jedes einzelnen von Ihnen VPCs dürfen sich nicht überschneiden, wenn sie miteinander verbunden, über Transit Gateway verbunden oder über VPN eine Verbindung hergestellt

werden. Vermeiden Sie IP-Adresskonflikte zwischen einer VPC und lokalen Umgebungen oder mit anderen Cloud-Anbietern, die Sie verwenden. Sie müssen bei Bedarf auch die Möglichkeit haben, private IP-Adressbereiche zuzuweisen. Ein IP-Adressverwaltungssystem (IPAM) kann dabei helfen, dies zu automatisieren.

Gewünschtes Ergebnis:

- Keine VPCs IP-Adressbereichskonflikte zwischen lokalen Umgebungen oder anderen Cloud-Anbietern.
- Eine angemessene IP-Adressverwaltung ermöglicht eine einfachere Skalierung der Netzwerkinfrastruktur, um wachsenden und sich wandelnden Netzwerkanforderungen gerecht zu werden.

Typische Anti-Muster:

- Sie verwenden denselben IP-Bereich VPC wie vor Ort, in Ihrem Unternehmensnetzwerk oder bei anderen Cloud-Anbietern
- IP-Bereiche, die für die Bereitstellung Ihrer Workloads VPCs verwendet wurden, werden nicht nachverfolgt.
- Alleinige Nutzung manueller IP-Adressverwaltungsprozesse wie Tabellenkalkulationen.
- CIDRBlöcke werden über- oder unterdimensioniert, was zu Verschwendung von IP-Adressen oder unzureichendem Adressraum für Ihre Arbeitslast führt.

Vorteile der Nutzung dieser bewährten Methode: Mit der aktiven Planung des Netzwerks stellen Sie sicher, dass dieselbe IP-Adresse in miteinander verbundenen Netzwerken nicht mehrmals vorkommt. So wird verhindert, dass Routing-Probleme in Teilen der Workload auftreten, die die verschiedenen Anwendungen verwenden.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel

Implementierungsleitfaden

Verwenden Sie einen IPAM, z. B. den [Amazon VPC IP Address Manager](#), um Ihre CIDR Nutzung zu überwachen und zu verwalten. Einige IPAMs sind auch bei der erhältlich AWS Marketplace. Bewerten Sie Ihre potenzielle Nutzung am AWS, fügen Sie CIDR Bereiche zu bestehenden hinzu und erstellen Sie VPCs, VPCs um ein geplantes Nutzungswachstum zu ermöglichen.



## Implementierungsschritte

- Erfassen Sie CIDR den aktuellen Verbrauch (z. B. VPCs und Subnetze).
  - Verwenden Sie API Serviceoperationen, um den aktuellen CIDR Verbrauch zu erfassen.
  - Verwenden Sie den [Amazon VPC IP Address Manager, um Ressourcen zu finden](#).
- Erfassen Sie die aktuelle Subnetzauslastung.
  - Verwenden Sie API Serviceoperationen, um [Subnetze pro VPC Region zu sammeln](#).
  - Verwenden Sie den [Amazon VPC IP Address Manager, um Ressourcen zu finden](#).
- Zeichnen Sie die aktuelle Auslastung auf.
- Prüfen Sie, ob sich IP-Bereiche überschneiden.
- Berechnen Sie die freie Kapazität.
- Identifizieren Sie sich überschneidende IP-Bereiche. Sie können entweder zu einem neuen Adressbereich migrieren oder die Verwendung von Techniken wie einem [privaten NAT Gateway](#) in Betracht ziehen oder [AWS PrivateLink](#) wenn Sie die sich überschneidenden Bereiche verbinden müssen.

## Ressourcen

Zugehörige bewährte Methoden:

- [Schutz von Netzwerken](#)

Zugehörige Dokumente:

- [APNPartner: Partner, die Ihnen bei der Planung Ihres Netzwerks helfen können](#)
- [AWS Marketplace für Netzwerkinfrastruktur](#)
- Whitepaper [Amazon Virtual Private Cloud Connectivity Options](#)
- [Multiple data center HA network connectivity](#)
- [Connecting Networks with Overlapping IP Ranges](#)
- [Was ist AmazonVPC?](#)
- [Was ist IPAM?](#)

Zugehörige Videos:

- [AWS re:Invent 2023 — Fortschrittliche VPC Designs und neue Funktionen](#)
- [AWS re:Invent 2019: AWS Transit Gateway Referenzarchitekturen für viele VPCs](#)
- [AWS re:Invent 2023 — Bereit für das, was als Nächstes kommt? Designing networks for growth and flexibility](#)
- [AWS re:Invent 2021 — {New Launch} Verwalten Sie Ihre IP-Adressen in großem Umfang AWS](#)

## Workload-Architektur

### Fragen

- [REL3. Wie entwerfen Sie Ihre Workload-Service-Architektur?](#)
- [REL4. Wie lassen sich Interaktionen in einem verteilten System so gestalten, dass Ausfälle vermieden werden?](#)
- [REL5. Wie lassen sich Interaktionen in einem verteilten System so gestalten, dass Ausfälle abgemildert oder bewältigt werden?](#)

### REL3. Wie entwerfen Sie Ihre Workload-Service-Architektur?

Erstellen Sie hoch skalierbare und zuverlässige Workloads mithilfe einer serviceorientierten Architektur (SOA) oder einer Microservices-Architektur. Serviceorientierte Architektur (SOA) ist die Praxis, Softwarekomponenten über Serviceschnittstellen wiederverwendbar zu machen. Die Microservices-Architektur geht noch weiter, um Komponenten kleiner und einfacher zu machen.

### Bewährte Methoden

- [REL03-BP01 Wählen Sie, wie Sie Ihre Arbeitslast segmentieren möchten](#)
- [REL03-BP02 Entwickeln Sie Services, die sich auf bestimmte Geschäftsbereiche und Funktionen konzentrieren](#)
- [REL03-BP03 Stellen Sie Serviceverträge bereit per API](#)

### REL03-BP01 Wählen Sie, wie Sie Ihre Arbeitslast segmentieren möchten

Die Workload-Segmentierung ist wichtig, wenn es um die Festlegung der Resilienzanforderungen Ihrer Anwendung geht. Eine monolithische Architektur sollte vermieden werden, wann immer möglich. Stattdessen sollten Sie sorgfältig überlegen, welche Anwendungskomponenten in Microservices aufgeteilt werden können. Je nach Ihren Anwendungsanforderungen kann es sich dabei, wenn

möglich, um eine Kombination aus einer serviceorientierten Architektur (SOA) und Microservices handeln. Workloads, die zustandslos sein können, können eher als Microservices bereitgestellt werden.

Gewünschtes Ergebnis: Workloads sollten unterstützbar, skalierbar und so lose miteinander verbunden sein wie möglich.

Wiegen Sie bei Entscheidungen zur Segmentierung von Workloads die Vorteile und die Komplexitäten miteinander ab. Was für ein neues Produkt richtig ist, das gerade auf dem Markt eingeführt wird, unterscheidet sich von den Anforderungen eines Workloads, der von Anfang an skalierbar sein muss. Bei einem Faktorwechsel für einen vorhandenen Monolith müssen Sie berücksichtigen, wie gut dieser aufgeteilt und in zustandslose Anwendungen transformiert werden kann. Die Aufteilung von Services in kleinere Teile ermöglicht kleinen, klar definierten Teams, diese weiterzuentwickeln und zu verwalten. Kleinere Services können jedoch Komplexitäten wie eine möglicherweise erhöhte Latenz, ein komplexeres Debugging und einen erhöhten operativen Aufwand einführen.

Typische Anti-Muster:

- Der [Microservice Death Star](#) ist eine Situation, in der die einzelnen Komponenten so stark voneinander abhängig werden, dass der Ausfall einer einzigen Komponente einen wesentlich größeren Ausfall bewirkt. Das bedeutet, dass die Komponenten so starr und anfällig wie ein Monolith sind.

Vorteile der Nutzung dieser bewährten Methode:

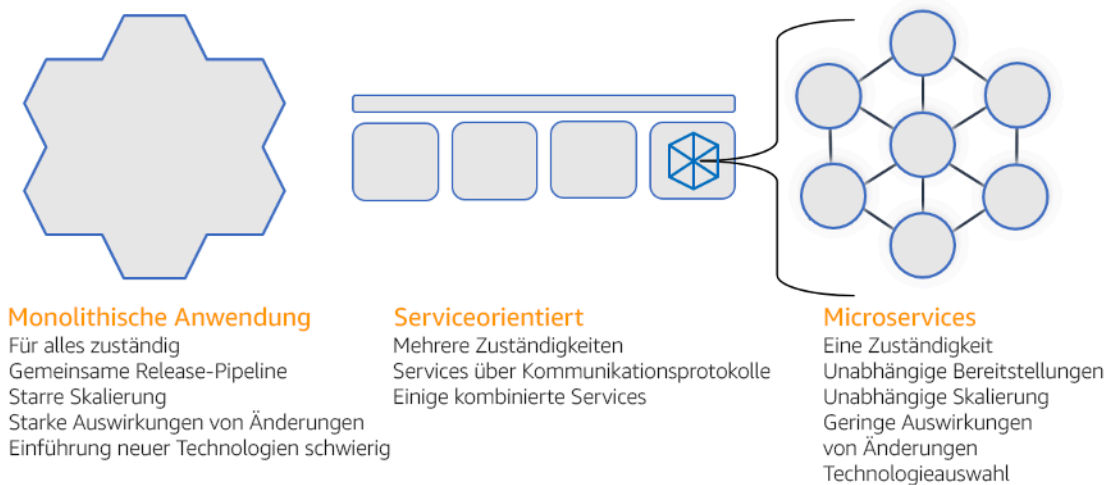
- Spezifischere Segmente führen zu einer größeren Agilität, zu organisatorischer Flexibilität und zu Skalierbarkeit.
- Die Auswirkungen von Service-Unterbrechungen werden reduziert.
- Die einzelnen Komponenten einer Anwendung besitzen möglicherweise unterschiedliche Anforderungen an die Verfügbarkeit, die von einer stärkeren Segmentierung besser unterstützt werden können.
- Die Verantwortlichkeiten der Teams, die den Workload unterstützen, sind klar definiert.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Hoch

## Implementierungsleitfaden

Wählen Sie Ihren Architekturtyp basierend auf der Segmentierung Ihres Workloads aus. Wählen Sie eine SOA oder eine Microservices-Architektur (oder in einigen seltenen Fällen eine monolithische Architektur). Selbst wenn Sie sich dafür entscheiden, mit einer Monolith-Architektur zu beginnen, müssen Sie sicherstellen, dass diese modular ist und sich letztendlich zu SOA Microservices weiterentwickeln kann, wenn Ihr Produkt mit der Benutzerakzeptanz skaliert. SOA und Microservices bieten jeweils eine geringere Segmentierung, was als moderne, skalierbare und zuverlässige Architektur bevorzugt wird. Allerdings müssen auch Kompromisse berücksichtigt werden, insbesondere bei der Implementierung einer Microservice-Architektur.

Aufgrund ihrer verteilten Computing-Architektur kann es schwieriger sein, die Latenzanforderungen von Benutzern zu erfüllen. Außerdem sind das Debugging und die Nachverfolgung von Benutzerinteraktionen komplexer. Zur Lösung dieses Problems können Sie AWS X-Ray verwenden. Ein weiterer Effekt ist die erhöhte operative Komplexität, da die Anzahl der von Ihnen verwalteten Anwendungen zunimmt. In der Folge müssen Sie eine größere Zahl voneinander unabhängiger Komponenten bereitstellen.



## Monolithische, serviceorientierte und Microservice-Architekturen

### Implementierungsschritte

- Ermitteln Sie die richtige Architektur für den Faktorwechsel oder die Entwicklung Ihrer Anwendung. SOA und Microservices bieten jeweils eine geringere Segmentierung, was als moderne, skalierbare und zuverlässige Architektur bevorzugt wird. SOA kann ein guter Kompromiss sein, um eine kleinere Segmentierung zu erreichen und gleichzeitig einige der Komplexitäten von Microservices zu vermeiden. Weitere Informationen finden Sie unter [Microservice Trade-Offs](#).

- Wenn Ihre Workload für sie zugänglich ist und Ihre Organisation sie unterstützen kann, sollten Sie eine Microservices-Architektur verwenden, um die beste Agilität und Zuverlässigkeit zu erzielen. [Weitere Informationen finden Sie unter Implementierung von Microservices auf AWS](#)
- Sie sollten das Muster mit der Bezeichnung [Strangler Fig \(„Würgefeige“\)](#) verwenden, um einen Faktorwechsel für einen Monolithen durchzuführen, bei dem Sie diesen in kleinere Komponenten aufteilen. Dies umfasst die schrittweise Ersetzung spezifischer Anwendungskomponenten durch neue Anwendungen und Services. [AWS Migration Hub Refactor Spaces](#) dient als Ausgangspunkt für den inkrementellen Faktorwechsel. Weitere Informationen finden Sie unter [Seamlessly migrate on-premises legacy workloads using a strangler pattern](#).
- Für die Implementierung von Microservices ist möglicherweise ein Service Discovery-Mechanismus erforderlich, der es diesen verteilten Diensten ermöglicht, miteinander zu kommunizieren. [AWS App Mesh](#) kann mit serviceorientierten Architekturen verwendet werden, um eine zuverlässige Erkennung und den zuverlässigen Zugriff auf Dienste zu ermöglichen. [AWS Cloud Map](#) kann auch für die dynamische, DNS basierte Serviceerkennung verwendet werden.
- Wenn Sie von einem Monolith zu Amazon MQ migrierenSOA, kann [Amazon MQ](#) Ihnen helfen, die Lücke als Service Bus bei der Neugestaltung älterer Anwendungen in der Cloud zu schließen.
- Im Fall vorhandener Monolithen mit einer einzigen, geteilten Datenbank müssen Sie entscheiden, wie Sie die Daten neu in kleineren Segmenten organisieren. Dabei kann es sich um Geschäftsbereiche, Zugriffsmuster oder Datenstrukturen handeln. An diesem Punkt des Refactoring-Prozesses sollten Sie sich dafür entscheiden, mit einem relationalen oder einem nicht-relationalen Datenbanktyp (Nein) fortzufahren. SQL [Weitere Informationen finden Sie unter Von bis Nein. SQL SQL](#)

Aufwand für den Implementierungsplan: Hoch

Ressourcen

Zugehörige bewährte Methoden:

- [REL03-BP02 Entwickeln Sie Services, die sich auf bestimmte Geschäftsbereiche und Funktionen konzentrieren](#)

Zugehörige Dokumente:

- [Amazon API Gateway: Konfiguration eines REST API mit Open API](#)
- [Was ist eine serviceorientierte Architektur?](#)

- [Bounded Context \(a central pattern in Domain-Driven Design\)](#)
- [Implementierung von Microservices auf AWS](#)
- [Microservice Trade-Offs](#)
- [Microservices - a definition of this new architectural term](#)
- [Microservices auf AWS](#)
- [Was ist AWS App Mesh?](#)

Zugehörige Beispiele:

- [Workshop für die iterative App-Modernisierung](#)

Zugehörige Videos:

- [Exzellenz mit Microservices erreichen AWS](#)

REL03-BP02 Entwickeln Sie Services, die sich auf bestimmte Geschäftsbereiche und Funktionen konzentrieren

Serviceorientierte Architekturen (SOA) definieren Dienste mit klar abgegrenzten Funktionen, die durch Geschäftsanforderungen definiert sind. Microservices verwenden Domain-Modelle und begrenzten Kontext, um Servicegrenzen entlang der Grenzen des Geschäftskontextes zu ziehen. Die Konzentration auf Geschäftsdomänen und Funktionen hilft Teams dabei, unabhängige Zuverlässigkeitsanforderungen für ihre Services zu definieren. Begrenzte Kontexte isolieren und kapseln die Geschäftslogik, sodass Teams besser überlegen können, wie mit Fehlern umzugehen ist.

Gewünschtes Ergebnis: Ingenieure und geschäftliche Interessenvertreter definieren gemeinsam begrenzte Kontexte und verwenden sie, um Systeme als Services zu entwerfen, die bestimmte Geschäftsfunktionen erfüllen. Diese Teams verwenden etablierte Praktiken wie Event Storming, um Anforderungen zu definieren. Neue Anwendungen sind als Services mit klar definierten Grenzen und losen Verkopplungen definiert. Bestehende Monolithen werden in [begrenzte Kontexte zerlegt, und Systemdesigns entwickeln sich hin](#) zu Microservice-Architekturen. SOA Bei der Refaktorisierung von Monolithen kommen etablierte Ansätze wie Bubble-Kontexte und Monolith-Zerlegung zur Anwendung.

Domain-orientierte Services werden als ein oder mehrere Prozesse ausgeführt, die keinen gemeinsamen Zustand haben. Sie reagieren selbstständig auf Nachfrageschwankungen und behandeln Störszenarien anhand Domain-spezifischer Anforderungen.

## Typische Anti-Muster:

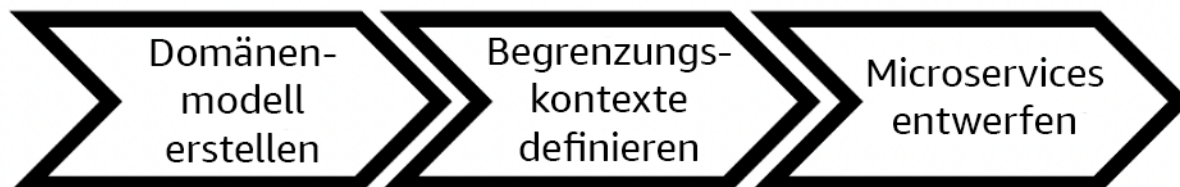
- Teams werden für bestimmte technische Bereiche wie UI und UX, Middleware oder Datenbank gebildet, anstatt für bestimmte Geschäftsdomänen.
- Anwendungen erstrecken sich über die Zuständigkeiten der einzelnen Domains. Services, die sich über begrenzte Kontexte erstrecken, können schwieriger zu verwalten sein, erfordern einen größeren Testaufwand und erfordern die Teilnahme mehrerer Domain-Teams an Softwareupdates.
- Domänenabhängigkeiten wie Domain-Entity-Bibliotheken werden von allen Services gemeinsam genutzt, sodass Änderungen für eine Servicedomäne Änderungen an anderen Service-Domänen erfordern.
- Serviceverträge und Geschäftslogik formulieren Entitäten nicht in einer gemeinsamen und konsistenten Domain-Sprache, was zu Übersetzungsebenen führt, die Systeme komplizieren und den Debugging-Aufwand erhöhen.

Vorteile der Nutzung dieser bewährten Methode: Anwendungen sind als unabhängige Services konzipiert, die durch Geschäftsdomänen begrenzt sind und eine gemeinsame Geschäftssprache verwenden. Services sind unabhängig voneinander testbar und einsetzbar. Services erfüllen die Domain-spezifischen Resilienzanforderungen für die implementierte Domain.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Hoch

## Implementierungsleitfaden

Domain-Driven Design (DDD) ist der grundlegende Ansatz beim Entwerfen und Entwickeln von Software für Geschäftsbereiche. Bei der Entwicklung von Services, die sich auf Geschäftsdomänen konzentrieren, ist es hilfreich, mit einem vorhandenen Framework zu arbeiten. Wenn Sie mit bestehenden monolithischen Anwendungen arbeiten, können Sie die Vorteile von Zerlegungsmustern nutzen, die etablierte Techniken zur Modernisierung von Anwendungen in Services bereitstellen.



## Domain-gesteuertes Design

## Implementierungsschritte

- Teams können [Event-Storming-Workshops](#) veranstalten, um rasch Ereignisse, Befehle, Mengen und Domänen in einem unkomplizierten Notizformat zu sammeln.
- Sobald Domain-Entitäten und -Funktionen in einem Domain-Kontext gebildet wurden, können Sie Ihre Domain mithilfe eines [begrenzten Kontexts](#), weiter in kleinere Modelle unterteilt, wobei Entitäten mit ähnlichen Funktionen und Attributen in Gruppen sortiert werden. Wenn das Modell in Kontexte unterteilt ist, entsteht eine Vorlage für die Begrenzung von Microservices.
  - Für die Website Amazon.com können Entitäten beispielsweise Pakete, Zustellung, Zeitplan, Preise, Rabatte und Währung enthalten.
  - Paket, Zustellung und Zeitplan werden dem Versandkontext zugeordnet, während Preis, Rabatt und Währung dem Preiskontext zugeordnet sind.
- Unter [Decomposing monoliths into microservices](#) wird das Muster für das Refactoring von Microservices skizziert. Die Verwendung von Mustern für die Unterteilung nach Geschäftsfähigkeit, Subdomäne oder Transaktion passt gut zu Domain-gesteuerten Ansätzen.
- Taktische Techniken wie der [Bubble-Kontext](#) ermöglichen die Einführung DDD in bestehende oder veraltete Anwendungen, ohne dass im Vorfeld Änderungen vorgenommen werden müssen und keine vollständigen Verpflichtungen eingegangen werden müssen. DDD Bei einem Bubble-Kontext-Ansatz wird mithilfe von Service-Mapping und -koordination ein kleiner begrenzter Kontext oder eine [Ebene zur Korruptionsbekämpfung](#) erstellt, die das neu definierte Domain-Modell vor äußeren Einflüssen schützt.

Nachdem die Teams eine Domänenanalyse durchgeführt und Entitäten und Serviceverträge definiert haben, können sie AWS Services nutzen, um ihr domänenorientiertes Design als cloudbasierte Dienste zu implementieren.

- Beginnen Sie Ihre Entwicklung, indem Sie Tests definieren, die die Geschäftsregeln Ihrer Domain anwenden. Testgetriebene Entwicklung (TDD) und verhaltensorientierte Entwicklung (BDD) helfen Teams dabei, ihre Services weiterhin auf die Lösung von Geschäftsproblemen zu konzentrieren.
- Wählen Sie [AWS -Services](#) die den Anforderungen Ihrer Geschäfts-Domain und Ihrer [Microservice-Architektur am besten entsprechen](#):
  - [AWS Serverless](#) ermöglicht es Ihrem Team, sich auf eine bestimmte Domänenlogik zu konzentrieren, anstatt Server und Infrastruktur zu verwalten.
  - [Container in AWS](#) vereinfachen die Verwaltung Ihrer Infrastruktur, sodass Sie sich auf Ihre Domain-Anforderungen konzentrieren können.



- [Speziell entwickelte Datenbanken](#) helfen Ihnen dabei, Ihre Domain-Anforderungen dem am besten geeigneten Datenbanktyp zuzuordnen.
- [Hexagonale Architekturen auf AWS](#) skizzieren ein Framework zur Integration von Geschäftslogik in Services. Dabei wird rückwärts von der Geschäfts-Domain aus gearbeitet, um funktionale Anforderungen zu erfüllen und dann Integrationsadapter zu implementieren. Muster, die Schnittstellendetails mit AWS Services von der Geschäftslogik trennen, helfen Teams dabei, sich auf die Domänenfunktionalität zu konzentrieren und die Softwarequalität zu verbessern.

## Ressourcen

### Zugehörige bewährte Methoden:

- [REL03-BP01 Wählen Sie, wie Sie Ihre Arbeitslast segmentieren möchten](#)
- [REL03-BP03 Stellen Sie Serviceverträge bereit per API](#)

### Zugehörige Dokumente:

- [AWS Mikroservices](#)
- [Implementierung von Microservices auf AWS](#)
- [How to break a Monolith into Microservices](#)
- [Erste Schritte, DDD wenn Sie von Legacy-Systemen umgeben sind](#)
- [Domain-Driven Design: Tackling Complexity in the Heart of Software](#)
- [Aufbau sechseckiger Architekturen auf AWS](#)
- [Decomposing monoliths into microservices](#)
- [Event Storming](#)
- [Messages Between Bounded Contexts](#)
- [Microservices](#)
- [Testgetriebene Entwicklung](#)
- [Verhaltensgetriebene Entwicklung](#)

### Zugehörige Beispiele:

- [Entwerfen von Cloud-Native-Microservices auf AWS \(von/\) DDD EventStormingWorkshop](#)

## Zugehörige Tools:

- [AWS Cloud Datenbanken](#)
- [Serverlos auf AWS](#)
- [Container bei AWS](#)

## REL03-BP03 Stellen Sie Serviceverträge bereit per API

Dienstleistungsverträge sind dokumentierte Vereinbarungen zwischen API Herstellern und Verbrauchern, die in einer maschinenlesbaren API Definition definiert sind. Eine Strategie zur Versionierung von Verträgen ermöglicht es den Verbrauchern, die vorhandenen weiterhin zu verwenden API und ihre Anwendungen auf eine neuere zu migrieren, API sobald sie bereit sind. Die Bereitstellung durch den Produzenten kann jederzeit erfolgen, solange der Vertrag eingehalten wird. Serviceteams können den Technologie-Stack ihrer Wahl verwenden, um den API Vertrag zu erfüllen.

Gewünschtes Ergebnis: Anwendungen, die mit serviceorientierten Architekturen oder Microservice-Architekturen erstellt wurden, können unabhängig voneinander betrieben werden und verfügen gleichzeitig über eine integrierte Laufzeitabhängigkeit. Änderungen, die an einem API Verbraucher oder Hersteller vorgenommen werden, beeinträchtigen nicht die Stabilität des Gesamtsystems, wenn beide Seiten einen gemeinsamen Vertrag einhalten. API Komponenten, die über den Service kommunizieren, APIs können unabhängige funktionale Releases durchführen, Upgrades auf Laufzeitabhängigkeiten durchführen oder ein Failover zu einem Disaster Recovery (DR) -Standort durchführen, ohne sich gegenseitig zu beeinträchtigen. Darüber hinaus können spezialisierte Services unabhängig voneinander skaliert werden und können dabei den Ressourcenbedarf absorbieren, ohne dass andere Services ebenfalls skaliert werden müssen.

## Typische Anti-Muster:

- Ein Dienst wird APIs ohne stark typisierte Schemas erstellt. Dies führt dazu APIs, dass sie nicht zum Generieren von API Bindungen und Nutzlasten verwendet werden können, die nicht programmgesteuert validiert werden können.
- Es wird keine Versionierungsstrategie angewendet, die API Verbraucher dazu zwingt, Updates und Releases vorzunehmen, andernfalls scheitern sie, wenn sich die Serviceverträge weiterentwickeln.
- Fehlermeldungen, die Details der zugrundeliegenden Service-Implementierung preisgeben, anstatt Integrationsfehler im Kontext und in der Sprache der Domain zu beschreiben.
- Keine Nutzung von API Verträgen zur Entwicklung von Testfällen und API Scheinimplementierungen, um unabhängige Tests von Servicekomponenten zu ermöglichen.

Vorteile der Einführung dieser bewährten Methode: Verteilte Systeme, die aus Komponenten bestehen, die über API Serviceverträge miteinander kommunizieren, können die Zuverlässigkeit verbessern. Entwickler können potenzielle Probleme frühzeitig im Entwicklungsprozess catch, indem sie während der Kompilierung eine Typprüfung durchführen, um sicherzustellen, dass Anfragen und Antworten dem API Vertrag entsprechen und die erforderlichen Felder vorhanden sind. APIVerträge bieten eine klare, sich selbst dokumentierende Schnittstelle für eine bessere Interoperabilität zwischen verschiedenen Systemen APIs und Programmiersprachen und sorgen für eine bessere Interoperabilität.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Mittel

### Implementierungsleitfaden

Sobald Sie Geschäftsbereiche identifiziert und Ihre Workload-Segmentierung festgelegt haben, können Sie Ihren Service weiterentwickeln. APIs Definieren Sie zunächst maschinenlesbare Serviceverträge für APIs und implementieren Sie anschließend eine API Versionierungsstrategie. Wenn Sie bereit sind REST, Dienste über gängige Protokolle wie GraphQL oder asynchrone Ereignisse zu integrieren, können Sie AWS Dienste in Ihre Architektur integrieren, um Ihre Komponenten mit stark API typisierten Verträgen zu integrieren.

### AWS Dienste für Serviceverträge API

Integrieren Sie AWS Services wie [Amazon API Gateway](#) und [Amazon EventBridge](#) in Ihre Architektur [AWS AppSync](#), um API Serviceverträge in Ihrer Anwendung zu verwenden. Amazon API Gateway unterstützt Sie bei der direkten Integration mit nativen AWS Diensten und anderen Webdiensten. APIGateway unterstützt die [APIOpen-Spezifikation](#) und Versionierung. AWS AppSync ist ein verwalteter [GraphQL-Endpunkt](#), den Sie konfigurieren, indem Sie ein GraphQL-Schema definieren, um eine Serviceschnittstelle für Abfragen, Mutationen und Abonnements zu definieren. Amazon EventBridge verwendet Ereignisschemas, um Ereignisse zu definieren und Codebindungen für Ihre Ereignisse zu generieren.

### Implementierungsschritte

- Definieren Sie zunächst einen Vertrag für Ihren. API Ein Vertrag drückt die Fähigkeiten eines aus und API definiert stark typisierte Datenobjekte und Felder für die API Eingabe und Ausgabe.
- Bei der Konfiguration APIs in API Gateway können Sie Open API Specifications für Ihre Endgeräte importieren und exportieren.

- Der [Import einer offenen API Definition](#) vereinfacht die Erstellung Ihrer Definition API und kann als Codetools wie [AWS Serverless Application Model](#) und [AWS Cloud Development Kit \(AWS CDK\)](#) in die AWS Infrastruktur integriert werden.
- Das [Exportieren einer API Definition](#) vereinfacht die Integration mit API Testtools und bietet dem Servicenutzer eine Integrationspezifikation.
- Sie können APIs GraphQL definieren und verwalten, AWS AppSync indem Sie [eine GraphQL-Schemadatei definieren](#), um Ihre Vertragsschnittstelle zu generieren und die Interaktion mit komplexen REST Modellen, mehreren Datenbanktabellen oder älteren Diensten zu vereinfachen.
- [AWS Amplify](#) Projekte, die integriert sind, AWS AppSync generieren stark typisierte JavaScript Abfragedateien zur Verwendung in Ihrer Anwendung sowie eine AWS AppSync GraphQL-Clientbibliothek für [Amazon DynamoDB-Tabellen](#).
- Wenn Sie Serviceereignisse von Amazon nutzen EventBridge, entsprechen Ereignisse Schemas, die bereits in der Schemaregistrierung vorhanden sind oder die Sie mit der Open API Spec definieren. Mit einem in der Registrierung definierten Schema können Sie auch Client-Bindungen aus dem Schemavertrag generieren, um Ihren Code in Ereignisse zu integrieren.
- Erweiterung oder Versionierung Ihrer API Das Erweitern von API ist eine einfachere Option, wenn Felder hinzugefügt werden, die mit optionalen Feldern oder Standardwerten für Pflichtfelder konfiguriert werden können.
  - JSONbasierte Verträge für Protokolle wie REST GraphQL können sich gut für eine Vertragsverlängerung eignen.
  - XMLVerträge, die auf Protokollen basieren, SOAP sollten mit den Nutzern der Dienste getestet werden, um festzustellen, ob eine Vertragsverlängerung durchführbar ist.
- Bei der Versionierung einer sollten Sie die Implementierung einer Proxy-Versionierung in Betracht ziehen API, bei der eine Fassade zur Unterstützung von Versionen verwendet wird, sodass die Logik in einer einzigen Codebasis verwaltet werden kann.
  - Mit API Gateway können Sie [Anfragen- und Antwortzuordnungen](#) verwenden, um die Übernahme von Vertragsänderungen zu vereinfachen, indem Sie eine Fassade einrichten, um Standardwerte für neue Felder bereitzustellen oder entfernte Felder aus einer Anfrage oder Antwort zu entfernen. Mit diesem Ansatz kann der zugrunde liegende Service mit einer einzelnen Codebasis betrieben werden.

## Ressourcen

Zugehörige bewährte Methoden:

- [REL03-BP01 Wählen Sie, wie Sie Ihre Arbeitslast segmentieren möchten](#)
- [REL03-BP02 Entwickeln Sie Services, die sich auf bestimmte Geschäftsbereiche und Funktionen konzentrieren](#)
- [REL04-BP02 Lose gekoppelte Abhängigkeiten implementieren](#)
- [REL05-BP03 Steuerung und Begrenzung von Wiederholungsaufrufen](#)
- [REL05-BP05 Client-Timeouts festlegen](#)

#### Zugehörige Dokumente:

- [Was ist eine API \(Anwendungsprogrammierschnittstelle\)?](#)
- [Implementierung von Microservices auf AWS](#)
- [Microservice Trade-Offs](#)
- [Microservices - a definition of this new architectural term](#)
- [Microservices auf AWS](#)
- [Ich arbeite mit API Gateway-Erweiterungen für Open API](#)
- [APIOpen-Spezifikation](#)
- [GraphQL: Schemata und Typen](#)
- [EventBridge Amazon-Codebindungen](#)

#### Zugehörige Beispiele:

- [Amazon API Gateway: Konfiguration eines REST API mit Open API](#)
- [CRUDAnwendung Amazon API Gateway to Amazon DynamoDB mithilfe von Open API](#)
- [Moderne Anwendungsintegrationsmuster in einem serverlosen Zeitalter: API Gateway Service Integration](#)
- [Implementierung einer Header-basierten API Gateway-Versionierung mit Amazon CloudFront](#)
- [AWS AppSync: Building a client application](#)

#### Zugehörige Videos:

- [Verwenden von Open API in AWS SAM zur Verwaltung von Gateway API](#)

#### Zugehörige Tools:

- [APIAmazon-Gateway](#)
- [AWS AppSync](#)
- [Amazon EventBridge](#)

REL4. Wie lassen sich Interaktionen in einem verteilten System so gestalten, dass Ausfälle vermieden werden?

Verteilte Systeme sind auf Kommunikationsnetzwerke angewiesen, um Komponenten wie Server oder Services miteinander zu verbinden. Ihre Workload muss trotz Datenverlust oder Latenz in diesen Netzwerken zuverlässig funktionieren. Die Komponenten des verteilten Systems müssen so funktionieren, dass sie sich nicht negativ auf andere Komponenten oder die Workload auswirken. Diese bewährten Methoden verhindern Ausfälle und verbessern die durchschnittliche Betriebsdauer zwischen Ausfällen (MTBF).

Bewährte Methoden

- [REL04-BP01 Identifizieren Sie die Art der verteilten Systeme, auf die Sie angewiesen sind](#)
- [REL04-BP02 Lose gekoppelte Abhängigkeiten implementieren](#)
- [REL04-BP03 Arbeite ständig](#)
- [REL04-BP04 Alle Antworten idempotent machen](#)

REL04-BP01 Identifizieren Sie die Art der verteilten Systeme, auf die Sie angewiesen sind

Verteilte Systeme verwenden die synchrone, asynchrone oder Stapelverarbeitung. Synchrone Systeme müssen Anfragen so schnell wie möglich verarbeiten und miteinander kommunizieren, indem sie synchrone Anfrage- und Antwortrufe mithilfe der Protokolle HTTP /SREST, oder Remote Procedure Call () ausführen. RPC Asynchrone Systeme kommunizieren miteinander, indem sie Daten asynchron über einen Zwischenservice austauschen, ohne einzelne Systeme zu koppeln. Systeme mit Stapelverarbeitung empfangen eine große Menge an Eingabedaten, führen automatisierte Datenprozesse ohne menschliches Eingreifen aus und generieren Ausgabedaten.

Gewünschtes Ergebnis: Entwerfen Sie einen Workload, der effektiv mit synchronen, asynchronen und Batch-Abhängigkeiten interagiert.

Typische Anti-Muster:

- Der Workload wartet auf unbestimmte Zeit auf eine Antwort von seinen Abhängigkeiten, was dazu führen kann, dass Workload-Clients das Zeitlimit überschreiten und nicht wissen, ob ihre Anfrage eingegangen ist.
- Der Workload verwendet eine Kette von abhängigen Systemen, die sich gegenseitig synchron aufrufen. Der Erfolg der gesamten Kette hängt davon ab, dass jedes System verfügbar ist und Anfragen erfolgreich verarbeitet, was zu instabilem Verhalten und eingeschränkter Gesamtverfügbarkeit führen kann.
- Der Workload kommuniziert asynchron mit seinen Abhängigkeiten und stützt sich auf das Konzept der garantierten einmaligen Zustellung von Nachrichten, obwohl es oft immer noch möglich ist, doppelte Nachrichten zu empfangen.
- Der Workload verwendet keine geeigneten Tools zur Batchplanung und ermöglicht die gleichzeitige Ausführung desselben Batchjobs.

Vorteile der Nutzung dieser bewährten Methode: Es ist üblich, dass ein bestimmter Workload einen oder mehrere Kommunikationsstile der synchronen, asynchronen und Stapelverarbeitung implementiert. Diese bewährte Methode hilft Ihnen dabei, die verschiedenen Kompromisse zu identifizieren, die mit den einzelnen Kommunikationsstilen verbunden sind, damit Ihr Workload Störungen in allen Abhängigkeiten tolerieren kann.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Hoch

### Implementierungsleitfaden

Die folgenden Abschnitte enthalten sowohl allgemeine als auch spezifische Implementierungshinweise für jede Art von Abhängigkeit.

#### General guidance (Allgemeine Anleitung)

- Stellen Sie sicher, dass die Service-Level-Ziele (SLOs) für Leistung und Zuverlässigkeit, die Ihre Abhängigkeiten bieten, den Leistungs- und Zuverlässigkeitsanforderungen Ihres Workloads entsprechen.
- Verwenden Sie [AWS Observability Services](#), um [Reaktionszeiten und Fehlerraten zu überwachen](#), und so sicherzustellen, dass Ihre Abhängigkeit den von Ihrem Workload benötigten Service bietet.
- Identifizieren Sie die potenziellen Herausforderungen, mit denen Ihr Workload bei der Kommunikation mit seinen Abhängigkeiten konfrontiert sein könnte. Verteilte Systeme [sind mit einer Vielzahl von Herausforderungen verbunden](#), die die architektonische Komplexität, den Betriebsaufwand und die Kosten erhöhen können. Zu den häufigsten Herausforderungen

gehören Latenz, Netzwerkunterbrechungen, Datenverlust, Skalierung und Verzögerungen bei der Datenreplikation.

- Implementieren Sie eine robuste Fehlerbehandlung und [-protokollierung](#), um Probleme zu beheben, wenn es in Ihrer Abhängigkeit zu Problemen kommt.

## Synchrone Abhängigkeit

Bei synchroner Kommunikation sendet Ihr Workload eine Anfrage an seine Abhängigkeit und blockiert den Vorgang, der auf eine Antwort wartet. Wenn ihre Abhängigkeit die Anfrage erhält, versucht sie, sie so schnell wie möglich zu bearbeiten, und sendet eine Antwort zurück an den Workload. Eine große Herausforderung bei synchroner Kommunikation besteht darin, dass sie zu einer zeitlichen Kopplung führt, was erfordert, dass der Workload und dessen Abhängigkeiten gleichzeitig verfügbar sind. Beachten Sie die folgenden Hinweise, wenn der Workload synchron mit seinen Abhängigkeiten kommunizieren muss:

- Der Workload sollte sich nicht auf mehrere synchrone Abhängigkeiten stützen, um eine einzelne Funktion auszuführen. Diese Kette von Abhängigkeiten erhöht die allgemeine Instabilität, da alle Abhängigkeiten im Pfad verfügbar sein müssen, damit die Anfrage erfolgreich abgeschlossen werden kann.
- Wenn eine Abhängigkeit fehlerhaft oder nicht verfügbar ist, bestimmen Sie Ihre Strategie zur Fehlerbehandlung und versuchen Sie es erneut. Vermeiden Sie bimodales Verhalten. Bimodales Verhalten liegt vor, wenn sich der Workload im Normalmodus und im Fehlermodus unterschiedlich verhält. Weitere Informationen zum bimodalen Verhalten finden Sie unter [REL11-BP05 Verwenden Sie statische Stabilität, um bimodales Verhalten zu verhindern](#).
- Denken Sie daran, dass es besser ist, schnell zu scheitern, als Ihren Workload warten zu lassen. Im [AWS Lambda Entwicklerleitfaden](#) wird beispielsweise beschrieben, wie Wiederholungen und Fehlschläge beim Aufrufen von Lambda-Funktionen behandelt werden.
- Legen Sie Timeouts fest, wenn Ihr Workload seine Abhängigkeit aufruft. Dadurch wird vermieden, zu lange oder unbegrenzt auf eine Antwort zu warten. Eine hilfreiche Erläuterung dieses Problems finden Sie unter [Tuning von AWS SDK HTTP Java-Anforderungseinstellungen für latenzsensitive Amazon DynamoDB DynamoDB-Anwendungen](#).
- Reduzieren Sie die Anzahl der Aufrufe von Ihrem Workload an seine Abhängigkeit, um eine einzelne Anfrage zu erfüllen. Durch zahlreiche Aufrufe erhöht sich die Kopplung und Latenz.

## Asynchrone Abhängigkeit



Um den Workload zeitlich von dessen Abhängigkeiten zu entkoppeln, sollte die Kommunikation asynchron erfolgen. Bei einem asynchronen Ansatz kann der Workload mit jeder anderen Verarbeitung fortfahren, ohne auf eine Antwort der Abhängigkeit oder Kette von Abhängigkeiten warten zu müssen.

Beachten Sie die folgenden Hinweise, wenn der Workload asynchron mit seiner Abhängigkeit kommunizieren muss:

- Entscheiden Sie je nach Anwendungsfall und Anforderungen, ob Sie Messaging oder Ereignis-Streaming verwenden möchten. Beim [Messaging](#) kann der Workload mit seiner Abhängigkeit kommunizieren, indem er Nachrichten über einen Message Broker sendet und empfängt. Beim [Ereignis-Streaming](#) können der Workload und seine Abhängigkeiten einen Streaming-Dienst verwenden, um Ereignisse zu veröffentlichen und zu abonnieren, die als kontinuierliche Datenströme bereitgestellt werden und so schnell wie möglich verarbeitet werden müssen.
- Messaging und Ereignis-Streaming behandeln Nachrichten unterschiedlich, sodass Sie basierend auf den folgenden Faktoren Abwägungsentscheidungen treffen müssen:
  - Nachrichtenpriorität: Message Broker können Nachrichten mit hoher Priorität vor normalen Nachrichten verarbeiten. Beim Ereignis-Streaming haben alle Nachrichten dieselbe Priorität.
  - Nachrichtenverbrauch: Message Broker stellen sicher, dass die Verbraucher die Nachricht erhalten. Ereignis-Streaming-Verbraucher müssen den Überblick über die zuletzt gelesene Nachricht behalten.
  - Reihenfolge der Nachrichten: Bei Nachrichten ist der Empfang von Nachrichten in der exakten Reihenfolge, in der sie gesendet wurden, nicht garantiert, es sei denn, Sie verwenden einen () -Ansatz. first-in-first-out FIFO Beim Ereignis-Streaming wird immer die Reihenfolge beibehalten, in der die Daten erzeugt wurden.
  - Löschen von Nachrichten: Beim Messaging muss der Verbraucher die Nachricht nach der Verarbeitung löschen. Der Ereignis-Streaming-Dienst hängt die Nachricht an einen Stream an und verbleibt dort, bis die Aufbewahrungsfrist der Nachricht abläuft. Diese Löschroutine macht das Ereignis-Streaming für die Wiedergabe von Nachrichten geeignet.
- Definieren Sie, wie Ihr Workload weiß, wann seine Abhängigkeit seine Arbeit beendet hat. Wenn der Workload beispielsweise [asynchron eine Lambda-Funktion](#) aufruft, stellt Lambda das Ereignis in eine Warteschlange und gibt eine Erfolgsantwort ohne zusätzliche Informationen zurück. Nach Abschluss der Verarbeitung kann die Lambda-Funktion das [Ergebnis an ein Ziel senden](#), das je nach Erfolg oder Misserfolg konfiguriert werden kann.

- Entwickeln Sie Ihren Workload so, dass er doppelte Nachrichten verarbeiten kann, indem Sie Idempotenz nutzen. Idempotenz bedeutet, dass sich die Ergebnisse des Workloads nicht ändern, auch wenn der Workload mehrmals für dieselbe Nachricht generiert wird. Es ist wichtig, darauf hinzuweisen, dass [Messaging](#)- oder [Streaming](#)-Dienste eine Nachricht erneut übermitteln, wenn ein Netzwerkausfall auftritt oder wenn keine Bestätigung eingegangen ist.
- Wenn Ihr Workload keine Antwort von seiner Abhängigkeit erhält, muss er die Anfrage erneut einreichen. Erwägen Sie, die Anzahl der Wiederholungsversuche zu begrenzen, um Ihre Workload-CPU, Arbeitsspeicher- und Netzwerkressourcen für die Bearbeitung anderer Anfragen zu schonen. In der [AWS Lambda -Dokumentation](#) wird gezeigt, wie Fehler beim asynchronen Aufruf behandelt werden.
- Nutzen Sie geeignete Beobachtbarkeits-, Debugging- und Tracing-Tools, um die asynchrone Kommunikation des Workloads mit seinen Abhängigkeiten zu verwalten und zu betreiben. Sie können [Amazon](#) verwenden CloudWatch, um [Nachrichten](#)- und [Event-Streaming-Dienste](#) zu überwachen. Sie können auch Ihren Workload mit [AWS X-Ray](#) instrumentieren, um schnell [Erkenntnisse zur Problembeseitigung](#) zu gewinnen.

## Batch-Abhängigkeit

Batch-Systeme nehmen Eingabedaten auf, initiieren eine Reihe von Aufgaben, um sie zu verarbeiten, und erzeugen einige Ausgabedaten, ohne dass manuelles Eingreifen erforderlich ist. Je nach Datengröße können Aufgaben in wenigen Minuten oder in einigen Fällen sogar in mehreren Tagen ausgeführt werden. Beachten Sie die folgenden Hinweise, wenn der Workload mit seiner Batch-Abhängigkeit kommuniziert:

- Definieren Sie das Zeitfenster, in dem der Workload den Batchjob ausführen soll. Der Workload kann ein Wiederholungsmuster einrichten, um ein Batchsystem aufzurufen, beispielsweise jede Stunde oder am Ende eines jeden Monats.
- Ermitteln Sie den Ort der Dateneingabe und der verarbeiteten Datenausgabe. Wählen Sie einen Speicherservice wie [Amazon Simple Storage Services \(Amazon S3\)](#), [Amazon Elastic File System \(AmazonEFS\)](#) und [Amazon FSx for Lustre](#), der es Ihrem Workload ermöglicht, Dateien in großem Umfang zu lesen und zu schreiben.
- Wenn Ihr Workload mehrere Batch-Jobs aufrufen muss, können Sie dies nutzen, um die Orchestrierung von Batch-Jobs [AWS Step Functions](#) zu vereinfachen, die vor Ort oder vor Ort ausgeführt werden. AWS in diesem [Beispielprojekt](#) wird die Orchestrierung von Batchjobs mithilfe von Step Functions, [AWS Batch](#) und Lambda demonstriert.

- Überwachen Sie Batchjobs, um nach Auffälligkeiten zu suchen, z. B. wenn die Ausführung eines Jobs länger dauert, als sie sollte. Sie könnten Tools wie [CloudWatchContainer Insights](#) verwenden, um AWS Batch Umgebungen und Jobs zu überwachen. In diesem Fall würde Ihr Workload den Beginn des nächsten Jobs unterbrechen und die zuständigen Mitarbeiter über die Ausnahme informieren.

## Ressourcen

### Zugehörige Dokumente:

- [AWS Cloud Betrieb: Überwachung und Beobachtbarkeit](#)
- [Die Amazon Builders' Library: Herausforderungen für verteilte Systeme](#)
- [REL11-BP05 Verwenden Sie statische Stabilität, um bimodales Verhalten zu verhindern](#)
- [AWS Lambda Entwicklerhandbuch: Fehlerbehandlung und automatische Wiederholungsversuche in AWS Lambda](#)
- [Optimierung der AWS SDK HTTP Java-Anforderungseinstellungen für latenzsensitive Amazon DynamoDB DynamoDB-Anwendungen](#)
- [AWS -Messaging](#)
- [Was sind Streaming-Daten?](#)
- [AWS Lambda Entwicklerhandbuch: Asynchroner Aufruf](#)
- [Amazon Simple Queue ServiceFAQ: FIFO Warteschlangen](#)
- [Amazon Kinesis Data Streams Streams-Entwicklerhandbuch: Umgang mit doppelten Datensätzen](#)
- [Amazon Simple Queue Service Entwicklerhandbuch: Verfügbare CloudWatch Metriken für Amazon SQS](#)
- [Entwicklerhandbuch für Amazon Kinesis Data Streams: Überwachung des Amazon Kinesis Data Streams Service mit Amazon CloudWatch](#)
- [AWS X-Ray Entwicklerhandbuch: Konzepte AWS X-Ray](#)
- [AWS Beispiele zu GitHub: AWS Step Functions Complex Orchestrator App](#)
- [AWS Batch Benutzerhandbuch: AWS Batch CloudWatch Container Insights](#)

### Zugehörige Videos:

- [AWS Summit SF 2022 — Full-Stack-Beobachtbarkeit und Anwendungsüberwachung mit AWS \(0\) COP31](#)

## Zugehörige Tools:

- [Amazon CloudWatch](#)
- [CloudWatch Amazon-Protokolle](#)
- [AWS X-Ray](#)
- [Amazon Simple Storage Service \(Amazon S3\)](#)
- [Amazon Elastic File System \(AmazonEFS\)](#)
- [Amazon FSx für Lustre](#)
- [AWS Step Functions](#)
- [AWS Batch](#)

## REL04-BP02 Lose gekoppelte Abhängigkeiten implementieren

Abhängigkeiten etwa zwischen Warteschlangensystemen, Streaming-Systemen, Workflows und Load Balancern sind lose gekoppelt. Eine lose Verkoppelung hilft, das Verhalten einer Komponente von anderen Komponenten zu isolieren, die von ihr abhängig sind. Dies verbessert Resilienz und Agilität.

Die Entkopplung von Abhängigkeiten wie Warteschlangensystemen, Streaming-Systemen und Workflows trägt dazu bei, die Auswirkungen von Änderungen oder Ausfällen auf ein System zu minimieren. Durch diese Trennung wird das Verhalten einer Komponente von Auswirkungen auf andere, die von ihr abhängig sind, isoliert und so die Widerstandsfähigkeit und Agilität verbessert.

In eng gekoppelten Systemen können Änderungen an einer Komponente Änderungen an anderen Komponenten erforderlich machen, die von ihr abhängen, was die Leistung aller Komponenten beeinträchtigt. Die lose Verkoppelung unterbricht diese Abhängigkeit, sodass abhängige Komponenten nur die versionierte und veröffentlichte Schnittstelle kennen müssen. Die Implementierung einer losen Verkoppelung zwischen Abhängigkeiten isoliert einen Ausfall. So wird verhindert, dass er sich auf andere Komponenten auswirkt.

Die lose Verkoppelung ermöglicht Ihnen, einer Komponente zusätzlichen Code oder Features hinzuzufügen und gleichzeitig das Risiko für Komponenten zu minimieren, die von ihr abhängig sind. Sie ermöglicht auch eine granulare Ausfallsicherheit auf Komponentenebene, bei der Sie die zugrunde liegende Implementierung der Abhängigkeit aufskalieren oder sogar ändern können.

Um die Ausfallsicherheit durch lose Verkoppelung weiter zu verbessern, legen Sie Komponenten-Interaktionen nach Möglichkeit als asynchron fest. Dieses Modell eignet sich für jede Interaktion,

bei der keine sofortige Antwort benötigt wird, sondern die Bestätigung ausreicht, dass eine Anfrage registriert wurde. Es umfasst eine Komponente, die Ereignisse generiert, und eine andere Komponente, die sie konsumiert. Die beiden Komponenten werden nicht durch direkte point-to-point Interaktion integriert, sondern normalerweise über eine dauerhafte Zwischenschicht, z. B. eine SQS Amazon-Warteschlange, eine Streaming-Datenplattform wie Amazon Kinesis oder AWS Step Functions.

Abbildung 4: Abhängigkeiten etwa zwischen Warteschlangensystemen und Load Balancer sind lose gekoppelt

SQS Amazon-Warteschlangen und AWS Step Functions sind nur zwei Möglichkeiten, eine Zwischenschicht für lose Kopplung hinzuzufügen. Eventgesteuerte Architekturen können auch AWS Cloud mithilfe von Amazon erstellt werden EventBridge, wodurch Kunden (Event-Produzenten) von den Diensten, auf die sie angewiesen sind (Event-Konsumenten), abstrahieren können. Amazon Simple Notification Service (Amazon SNS) ist eine effektive Lösung, wenn Sie Push-basiertes Messaging mit hohem Durchsatz benötigen. many-to-many Mithilfe von SNS Amazon-Themen können Ihre Publisher-Systeme Nachrichten zur parallel Verarbeitung an eine große Anzahl von Abonnenten-Endpunkten fächern.

Warteschlangen bieten zwar mehrere Vorteile, doch Anfragen, die älter als ein Schwellenwert sind (oft Sekunden), sollten in den meisten harten Echtzeitsystemen als veraltet betrachtet (der Client hat aufgegeben und wartet nicht mehr auf eine Antwort) und nicht verarbeitet werden. Auf diese Weise können stattdessen neuere (und wahrscheinlich noch gültige Anfragen) verarbeitet werden.

Gewünschtes Ergebnis: Wenn Sie lose gekoppelte Abhängigkeiten implementieren, können Sie die Fehlerfläche auf Komponentenebene minimieren, was die Diagnose und Lösung von Problemen erleichtert. Außerdem vereinfacht es die Entwicklungszyklen, da die Teams Änderungen auf modularer Ebene implementieren können, ohne die Leistung anderer Komponenten, die davon abhängen, zu beeinträchtigen. Dieser Ansatz ermöglicht eine Aufskalierung auf Komponentenebene auf Grundlage des Ressourcenbedarfs sowie der Auslastung einer Komponente und trägt so zur Kosteneffizienz bei.

Typische Anti-Muster:

- Bereitstellen eines monolithischen Workloads.
- Direkter Aufruf APIs zwischen Workload-Stufen, ohne dass ein Failover oder eine asynchrone Verarbeitung der Anfrage möglich ist.

- Enge Verknüpfung mithilfe gemeinsam genutzter Daten. Lose gekoppelte Systeme sollten die gemeinsame Nutzung von Daten durch gemeinsam genutzte Datenbanken oder andere Formen der eng gekoppelten Datenspeicherung vermeiden, da dies wieder zu einer engen Verknüpfung führen und die Skalierbarkeit behindern kann.
- Gegendruck wird ignoriert. Ihr Workload sollte in der Lage sein, die eingehenden Daten zu verlangsamen oder zu stoppen, wenn eine Komponente sie nicht mit der gleichen Geschwindigkeit verarbeiten kann.

Vorteile der Nutzung dieser bewährten Methode: Eine lose Verkoppelung hilft dabei, das Verhalten einer Komponente von anderen Komponenten zu isolieren, die von ihr abhängen, wodurch die Resilienz und Agilität erhöht werden. Fehler in einer Komponente sind von anderen isoliert.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Hoch

### Implementierungsleitfaden

Implementieren lose gekoppelter Abhängigkeiten. Es gibt verschiedene Lösungen, mit denen Sie lose gekoppelte Anwendungen erstellen können. Dazu gehören Dienste für die Implementierung vollständig verwalteter Warteschlangen, automatisierter Workflows, die Reaktion auf Ereignisse und APIs vieles mehr, die dazu beitragen können, das Verhalten von Komponenten von anderen Komponenten zu isolieren und so die Widerstandsfähigkeit und Agilität zu erhöhen.

- Erstellen Sie ereignisgesteuerte Architekturen: [Amazon EventBridge](#) hilft Ihnen beim Aufbau lose gekoppelter und verteilter ereignisgesteuerter Architekturen.
- Implementieren Sie Warteschlangen in verteilten Systemen: Sie können [Amazon Simple Queue Service \(AmazonSQS\)](#) verwenden, um verteilte Systeme zu integrieren und zu entkoppeln.
- Komponenten als Microservices containerisieren: [Microservices](#) ermöglichen es Teams, Anwendungen zu erstellen, die aus kleinen unabhängigen Komponenten bestehen, die über klar definierte Kanäle kommunizieren. APIs [Amazon Elastic Container Service \(AmazonECS\)](#) und [Amazon Elastic Kubernetes Service \(AmazonEKS\)](#) können Ihnen helfen, schneller mit Containern zu beginnen.
- Verwalten Sie Workflows mit Step Functions: Mit [Step Functions](#) können Sie mehrere AWS Services zu flexiblen Workflows koordinieren.
- Nutzen Sie die Messaging-Architekturen Publish-Subscribe (Pub/Sub): [Amazon Simple Notification Service \(AmazonSNS\)](#) ermöglicht die Nachrichtenzustellung von Verlagen an Abonnenten (auch bekannt als Produzenten und Verbraucher).

## Implementierungsschritte

- Komponenten in einer ereignisgesteuerten Architektur werden durch Ereignisse ausgelöst. Ereignisse sind Aktionen, die in einem System stattfinden, z. B. wenn ein Benutzer einen Artikel in den Warenkorb legt. Wenn eine Aktion erfolgreich ist, wird ein Ereignis erzeugt, das die nächste Komponente des Systems auslöst.
  - [Entwicklung ereignisgesteuerter Anwendungen mit Amazon EventBridge](#)
  - [AWS re:Invent 2022 — Entwicklung ereignisgesteuerter Integrationen mit Amazon EventBridge](#)
- Verteilte Nachrichtensysteme haben drei Hauptbestandteile, die für eine warteschlangenbasierte Architektur implementiert werden müssen. Sie umfassen Komponenten des verteilten Systems, die Warteschlange, die für die Entkopplung verwendet wird (verteilt auf SQS Amazon-Servern), und die Nachrichten in der Warteschlange. Ein typisches System hat einen Produzenten, der die Nachricht in die Warteschlange einstellt, und einen Verbraucher, der die Nachricht aus der Warteschlange empfängt. Die Warteschlange speichert Nachrichten aus Redundanzgründen auf mehreren SQS Amazon-Servern.
  - [Grundlegende SQS Amazon-Architektur](#)
  - [Send Messages Between Distributed Applications with Amazon Simple Queue Service](#)
- Wenn Microservices gut genutzt werden, verbessern sie die Wartbarkeit und die Skalierbarkeit, da lose gekoppelte Komponenten von unabhängigen Teams verwaltet werden. Sie ermöglichen zudem die Isolierung von Verhaltensweisen auf eine einzelne Komponente im Falle von Änderungen.
  - [Implementierung von Microservices auf AWS](#)
  - [Let's Architect! Architektur von Microservices mit Containern](#)
- Mit können AWS Step Functions Sie unter anderem verteilte Anwendungen erstellen, Prozesse automatisieren und Microservices orchestrieren. Die Orchestrierung mehrerer Komponenten in einem automatisierten Workflow ermöglicht es Ihnen, Abhängigkeiten in Ihrer Anwendung zu entkoppeln.
  - [Erstellen Sie einen serverlosen Workflow mit und AWS Step FunctionsAWS Lambda](#)
  - [Erste Schritte mit AWS Step Functions](#)

## Ressourcen

### Zugehörige Dokumente:

- [AmazonEC2: Idempotenz sicherstellen](#)

- [Die Amazon Builders' Library: Herausforderungen für verteilte Systeme](#)
- [Die Amazon Builders' Library: Zuverlässigkeit, stetige Ausführung und eine gute Tasse Kaffee](#)
- [Was ist Amazon EventBridge?](#)
- [Was ist Amazon Simple Queue Service?](#)
- [Break up with your monolith](#)
- [Orchestrieren Sie warteschlangenbasierte Microservices mit und Amazon AWS Step Functions SQS](#)
- [Grundlegende SQS Amazon-Architektur](#)
- [Warteschlangenbasierte Architektur](#)

Zugehörige Videos:

- [AWS New York Summit 2019: Einführung in ereignisgesteuerte Architekturen und Amazon \(05\) EventBridge MAD2](#)
- [AWS re:Invent 2018: Closed Loops and Opening Minds: Wie man die Kontrolle über große und kleine Systeme übernimmt ARC337 \(beinhaltet lockere Kopplung, konstante Arbeit, statische Stabilität\)](#)
- [AWS re:Invent 2019: Umstellung auf ereignisgesteuerte Architekturen \(08\) SVS3](#)
- [AWS re:Invent 2019: Skalierbare, serverlose, ereignisgesteuerte Anwendungen mit Amazon und Lambda SQS](#)
- [AWS re:Invent 2022 — Entwicklung ereignisgesteuerter Integrationen mit Amazon EventBridge](#)
- [AWS re:Invent 2017: Elastic Load Balancing im Detail und Best Practices](#)

REL04-BP03 Arbeite ständig

Bei größeren, schnellen Lastveränderungen können Systeme ausfallen. Wenn Ihr Workload beispielsweise eine Zustandsprüfung ausführt, die den Zustand vieler tausend Server überwacht, sollte er jedes Mal die gleiche Nutzlast senden (einen vollständigen Snapshot des aktuellen Status). Unabhängig davon, ob keine Server oder alle Server ausfallen, führt das System für die Zustandsprüfung die Aufgaben stetig und ohne große, schnelle Änderungen aus.

Wenn das Zustandsprüfungssystem beispielsweise 100 000 Server überwacht, ist die Last darauf angesichts der normalerweise geringen Serverausfallrate nominal. Wenn jedoch ein großes Ereignis die Hälfte dieser Server fehlerhaft macht, wäre das Zustandsprüfungssystem überfordert, wenn es versucht, Benachrichtigungssysteme zu aktualisieren und den Status an seine Clients



zu kommunizieren. Stattdessen sollte das Zustandsprüfungssystem jedes Mal den vollständigen Snapshot des aktuellen Status senden. 100 000 Server-Zustände, die jeweils durch ein Bit dargestellt werden, entsprechen nur eine Nutzlast von 12,5 KB. Unabhängig davon, ob keine oder alle Server ausfallen – das System für die Zustandsprüfung erledigt seine Arbeit konstant und große, schnelle Änderungen stellen keine Bedrohung für die Systemstabilität dar. Auf diese Weise führt Amazon Route 53 Zustandsprüfungen für Endpunkte (wie z. B. IP-Adressen) durch, um zu ermitteln, wie Endbenutzer an diese weitergeleitet werden.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Niedrig

### Implementierungsleitfaden

- Führen Sie Aufgaben konstant aus, sodass auch bei großen, schnellen Lastveränderungen keine Fehler auf Systemen auftreten.
- Implementieren Sie lose gekoppelte Abhängigkeiten. Abhängigkeiten etwa zwischen Warteschlangensystemen, Streaming-Systemen, Workflows und Load Balancern sind lose gekoppelt. Eine lose Verkoppelung hilft, das Verhalten einer Komponente von anderen Komponenten zu isolieren, die von ihr abhängig sind. Dies verbessert Resilienz und Agilität.
- [Die Amazon Builders' Library: Zuverlässigkeit, stetige Ausführung und eine gute Tasse Kaffee](#)
- [AWS re:Invent 2018: Regelkreise schließen und neue Denkansätze eröffnen: Wie man die Kontrolle über große und kleine Systeme übernimmt ARC337 \(beinhaltet ständige Arbeit\)](#)
  - Beispiel: Zustandsprüfungssystem, das 100.000 Server überwacht: Entwickeln Sie die Workloads so, dass die Nutzlastgrößen unabhängig von der Anzahl der Erfolge oder Ausfälle konstant bleiben.

### Ressourcen

#### Zugehörige Dokumente:

- [AmazonEC2: Idempotenz sicherstellen](#)
- [Die Amazon Builders' Library: Herausforderungen für verteilte Systeme](#)
- [Die Amazon Builders' Library: Zuverlässigkeit, stetige Ausführung und eine gute Tasse Kaffee](#)

#### Zugehörige Videos:

- [AWS New York Summit 2019: Einführung in ereignisgesteuerte Architekturen und Amazon \(05\) EventBridge MAD2](#)

- [AWS re:Invent 2018: Close-Loops und offene Denkansätze: Wie man die Kontrolle über große und kleine Systeme übernimmt \(beinhaltet ständige Arbeit\) ARC337](#)
- [AWS re:Invent 2018: Close Loops und Opening Minds: So übernehmen Sie die Kontrolle über große und kleine Systeme ARC337 \(beinhaltet lockere Kopplung, konstante Arbeit, statische Stabilität\)](#)
- [AWS re:Invent 2019: Umstellung auf ereignisgesteuerte Architekturen \(08\) SVS3](#)

## REL04-BP04 Alle Antworten idempotent machen

Ein idempotenter Service garantiert, dass jede Anfrage genau einmal abgeschlossen wird. Das bedeutet, dass das Senden mehrerer identischer Anfragen den gleichen Effekt hat wie das Senden einer einzelnen Anfrage. Ein idempotenter Service erleichtert es einem Client, Wiederholungen zu implementieren. So muss nicht befürchtet werden, dass eine Anfrage fälschlicherweise mehrfach verarbeitet wird. Zu diesem Zweck können Clients API Anfragen mit einem Idempotenz-Token ausgeben — dasselbe Token wird verwendet, wenn die Anfrage wiederholt wird. Ein idempotenter Dienst API verwendet das Token, um eine Antwort zurückzugeben, die mit der Antwort identisch ist, die beim ersten Abschluss der Anfrage zurückgegeben wurde.

In einem verteilten System ist es einfach, eine Aktion höchstens einmal (der Client stellt nur eine Anforderung) oder mindestens einmal (Anforderung so lange, bis der Client erfolgreich ist) durchzuführen. Es ist jedoch schwer zu gewährleisten, dass eine Aktion idempotent ist, was bedeutet, dass sie genau einmal ausgeführt wird, sodass das Erstellen mehrerer identischer Anfragen den gleichen Effekt hat wie das Erstellen einer einzelnen Anfrage. Mithilfe von Idempotenz-Tokens können Dienste eine mutierende Anfrage ein- oder mehrmals empfangen, ohne dass doppelte Datensätze oder Nebenwirkungen entstehen. APIs

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Mittel

### Implementierungsleitfaden

- Legen Sie alle Reaktionen als idempotent fest. Ein idempotenter Service garantiert, dass jede Anfrage genau einmal abgeschlossen wird. Das bedeutet, dass das Senden mehrerer identischer Anfragen den gleichen Effekt hat wie das Senden einer einzelnen Anfrage.
  - Clients können API Anfragen mit einem Idempotenz-Token ausstellen — dasselbe Token wird verwendet, wenn die Anfrage wiederholt wird. Ein idempotenter Dienst API verwendet das Token, um eine Antwort zurückzugeben, die mit der Antwort identisch ist, die beim ersten Abschluss der Anfrage zurückgegeben wurde.
  - [AmazonEC2: Idempotenz sicherstellen](#)

## Ressourcen

### Zugehörige Dokumente:

- [AmazonEC2: Idempotenz sicherstellen](#)
- [Die Amazon Builders' Library: Herausforderungen für verteilte Systeme](#)
- [Die Amazon Builders' Library: Zuverlässigkeit, stetige Ausführung und eine gute Tasse Kaffee](#)

### Zugehörige Videos:

- [AWS New York Summit 2019: Einführung in ereignisgesteuerte Architekturen und Amazon \(05\) EventBridge MAD2](#)
- [AWS re:Invent 2018: Closed Loops and Opening Minds: Wie man die Kontrolle über große und kleine Systeme übernimmt ARC337 \(beinhaltet lockere Kopplung, konstante Arbeit, statische Stabilität\)](#)
- [AWS re:Invent 2019: Umstellung auf ereignisgesteuerte Architekturen \(08\) SVS3](#)

REL5. Wie lassen sich Interaktionen in einem verteilten System so gestalten, dass Ausfälle abgemildert oder bewältigt werden?

Verteilte Systeme nutzen Kommunikationsnetzwerke, um Komponenten (wie Server oder Services) miteinander zu verbinden. Ihre Workload muss trotz Datenverlust oder höherer Latenz in diesen Netzwerken zuverlässig ausgeführt werden. Die Komponenten des verteilten Systems müssen so funktionieren, dass sie sich nicht negativ auf andere Komponenten oder die Workload auswirken. Diese bewährten Methoden sorgen dafür, dass Workloads Belastungen oder Fehlern standhalten, sich schneller davon erholen und die Auswirkungen solcher Beeinträchtigungen abgeschwächt werden. Das Ergebnis ist eine verbesserte durchschnittliche Zeit bis zur Wiederherstellung (MTTR).

### Bewährte Methoden

- [REL05-BP01 Implementieren Sie eine graziöse Degradation, um anwendbare harte Abhängigkeiten in weiche Abhängigkeiten umzuwandeln](#)
- [REL05-BP02 Drosselungsanfragen](#)
- [REL05-BP03 Steuerung und Begrenzung von Wiederholungsaufrufen](#)
- [REL05-BP04 Schnelles Scheitern und begrenzte Warteschlangen](#)
- [REL05-BP05 Client-Timeouts festlegen](#)

- [REL05-BP06 Systeme soweit möglich zustandslos machen](#)
- [REL05-BP07 Nothebel einbauen](#)

REL05-BP01 Implementieren Sie eine graziöse Degradation, um anwendbare harte Abhängigkeiten in weiche Abhängigkeiten umzuwandeln

Anwendungskomponenten sollten weiterhin ihre Kernfunktion erfüllen, auch wenn Abhängigkeiten nicht mehr verfügbar sind. Sie liefern möglicherweise leicht veraltete Daten, alternative Daten oder sogar keine Daten. Dadurch wird sichergestellt, dass die Gesamtsystemfunktion nur minimal durch lokale Ausfälle beeinträchtigt wird, während gleichzeitig der zentrale Geschäftswert gewährleistet ist.

Gewünschtes Ergebnis: Wenn die Abhängigkeiten einer Komponente fehlerhaft sind, kann die Komponente selbst weiterhin funktionieren, wenn auch in eingeschränkter Weise.

Komponentenausfälle sollten als normaler Geschäftsbetrieb betrachtet werden. Arbeitsabläufe sollten so konzipiert sein, dass solche Ausfälle nicht zu einem vollständigen Ausfall oder zumindest zu vorhersehbaren und wiederherstellbaren Zuständen führen.

Typische Anti-Muster:

- Die erforderlichen Kerngeschäftsfunktionen wurden nicht identifiziert. Es wird nicht getestet, ob die Komponenten auch bei Abhängigkeitsfehlern funktionsfähig sind.
- Es werden keine Daten zu Fehlern bereitgestellt oder wenn nur eine von mehreren Abhängigkeiten nicht verfügbar ist und Teilergebnisse dennoch zurückgegeben werden können.
- Es entsteht ein inkonsistenter Zustand, wenn eine Transaktion teilweise fehlschlägt.
- Es gibt keine alternative Möglichkeit, auf einen zentralen Parameterspeicher zuzugreifen.
- Lokale Zustände werden aufgrund einer fehlgeschlagenen Aktualisierung ungültig oder geleert, ohne die Konsequenzen zu berücksichtigen.

Vorteile der Nutzung dieser bewährten Methode: Eine schrittweise Degradation verbessert die Verfügbarkeit des gesamten Systems und gewährleistet die Funktionsfähigkeit der wichtigsten Funktionen auch bei Ausfällen.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Hoch

Implementierungsleitfaden

Die Implementierung einer schrittweisen Degradation trägt dazu bei, die Auswirkungen von Abhängigkeitsfehlern auf die Komponentenfunktion zu minimieren. Im Idealfall erkennt eine

Komponente Abhängigkeitsfehler und umgeht sie so, dass sich dies nur minimal auf andere Komponenten oder Kunden auswirkt.

Eine Architektur, die auf eine schrittweise Degradation ausgerichtet ist, bedeutet, potenzielle Ausfallmodi beim Entwurf von Abhängigkeiten zu berücksichtigen. Sorgen Sie für jeden Ausfallmodus für eine Möglichkeit, aufrufenden Komponenten oder Kunden die meisten oder zumindest die wichtigsten Funktionen der Komponente bereitzustellen. Diese Überlegungen können zu zusätzlichen Anforderungen werden, die getestet und verifiziert werden können. Im Idealfall ist eine Komponente in der Lage, ihre Kernfunktion auf akzeptable Weise auszuführen, selbst wenn eine oder mehrere Abhängigkeiten ausfallen.

Dies ist sowohl eine geschäftliche als auch eine technische Diskussion. Alle Geschäftsanforderungen sind wichtig und sollten nach Möglichkeit erfüllt werden. Es ist jedoch immer noch sinnvoll, sich zu fragen, was passieren soll, wenn nicht alle erfüllt werden können. Ein System kann so konzipiert werden, dass es verfügbar und konsistent ist. Doch was davon ist wichtiger, wenn auf eines davon verzichtet werden muss? Bei der Zahlungsabwicklung könnte dies die Konsistenz sein. Bei einer Echtzeitanwendung ist es eher die Verfügbarkeit. Bei einer kundenseitigen Website kann die Antwort von den Kundenerwartungen abhängen.

Was das bedeutet, hängt von den Anforderungen der Komponente ab und davon, was als ihre Kernfunktion angesehen werden sollte. Beispielsweise:

- Eine E-Commerce-Website kann Daten aus verschiedenen Systemen wie personalisierte Empfehlungen, bestbewertete Produkte und den Status von Kundenbestellungen auf der Startseite anzeigen. Wenn ein Upstream-System ausfällt, ist es immer noch sinnvoll, alles andere anzuzeigen, anstatt einem Kunden eine Fehlerseite anzuzeigen.
- Eine Komponente, die Batch-Schreibvorgänge durchführt, kann einen Stapel trotzdem weiterverarbeiten, wenn eine der einzelnen Operationen fehlschlägt. Es sollte einfach sein, einen Wiederholungsmechanismus zu implementieren. Geben Sie dazu Informationen dazu zurück, welche Operationen erfolgreich, welche fehlgeschlagen und warum sie fehlgeschlagen sind. Oder stellen Sie fehlgeschlagene Anfragen in eine Warteschlange für unzustellbare Nachrichten, um asynchrone Wiederholungsversuche zu implementieren. Informationen über fehlgeschlagene Operationen sollten ebenfalls protokolliert werden.
- Ein System, das Transaktionen verarbeitet, muss überprüfen, ob entweder alle oder keine einzelnen Aktualisierungen ausgeführt werden. Bei verteilten Transaktionen kann das Saga-Muster verwendet werden, um vorherige Operationen rückgängig zu machen, falls ein späterer Vorgang derselben Transaktion fehlschlägt. Hier besteht die Kernfunktion darin, die Konsistenz aufrechtzuerhalten.

- Zeitkritische Systeme sollten in der Lage sein, mit Abhängigkeiten umzugehen, die nicht rechtzeitig reagieren. In diesen Fällen kann das Unterbrechermuster verwendet werden. Wenn bei Antworten aus einer Abhängigkeit eine Zeitüberschreitung auftritt, kann das System in einen geschlossenen Zustand wechseln, in dem keine weiteren Aufrufe getätigt werden.
- Eine Anwendung kann Parameter aus einem Parameterspeicher lesen. Es kann nützlich sein, Container-Images mit einem Satz von Standardparametern zu erstellen und diese zu verwenden, falls der Parameterspeicher nicht verfügbar ist.

Beachten Sie, dass die im Falle eines Komponentenausfalls eingeschlagenen Pfade getestet werden müssen und deutlich einfacher sein sollten als der primäre Pfad. Allgemein sollten Fallback-Strategien vermieden werden.

## Implementierungsschritte

Identifizieren Sie externe und interne Abhängigkeiten. Überlegen Sie, welche Arten von Fehlern bei ihnen auftreten können. Überlegen Sie, wie Sie die negativen Auswirkungen dieser Ausfälle auf vor- und nachgeschaltete Systeme und Kunden minimieren können.

Im Folgenden finden Sie eine Liste von Abhängigkeiten und wie Sie sie schrittweise degradieren können, wenn sie ausfallen:

1. Teilweiser Ausfall von Abhängigkeiten: Eine Komponente kann mehrere Anfragen an nachgelagerte Systeme stellen, entweder in Form mehrerer Anfragen an ein System oder in Form einer Anfrage an jeweils mehrere Systeme. Je nach Unternehmenskontext können unterschiedliche Vorgehensweisen angemessen sein (weitere Einzelheiten finden Sie in den vorherigen Beispielen in den Implementierungsleitfäden).
2. Ein nachgelagertes System kann Anfragen aufgrund der hohen Auslastung nicht verarbeiten: Wenn Anfragen an ein nachgelagertes System immer wieder fehlschlagen, ist es nicht sinnvoll, es erneut zu versuchen. Dies kann ein bereits überlastetes System zusätzlich belasten und die Wiederherstellung erschweren. Hier kann das Unterbrechermuster verwendet werden, das fehlgeschlagene Aufrufe an ein nachgelagertes System überwacht. Wenn eine große Anzahl von Aufrufen fehlschlägt, werden keine weiteren Anfragen mehr an das nachgelagerte System gesendet und nur gelegentlich Aufrufe durchgelassen, um zu testen, ob das nachgelagerte System wieder verfügbar ist.
3. Ein Parameterspeicher ist nicht verfügbar: Um einen Parameterspeicher umzuwandeln, können Soft Dependency Caching oder vernünftige Standardwerte verwendet werden, die in Container-

Images oder Machine Images enthalten sind. Beachten Sie, dass diese Standardwerte beibehalten up-to-date und in Testsuiten aufgenommen werden müssen.

4. Ein Überwachungsservice oder eine andere nicht funktionale Abhängigkeit ist nicht verfügbar: Wenn eine Komponente zeitweise nicht in der Lage ist, Protokolle, Metriken oder Spuren an einen zentralen Überwachungsservice zu senden, ist es oft am besten, Geschäftsfunktionen weiterhin wie gewohnt auszuführen. Es ist oft nicht akzeptabel, Metriken über einen längeren Zeitraum stillschweigend nicht zu protokollieren oder weiterzuleiten. In einigen Anwendungsfällen können auch vollständige Auditeinträge erforderlich sein, um die Compliance-Anforderungen zu erfüllen.
5. Eine primäre Instance einer relationalen Datenbank ist möglicherweise nicht verfügbar: Amazon Relational Database Service kann, wie fast alle relationalen Datenbanken, nur eine primäre Writer-Instance haben. Dies führt zu einem einzigen Fehlerpunkt für Schreib-Workloads und erschwert die Skalierung. Dies kann teilweise gemildert werden, indem eine Multi-AZ-Konfiguration für hohe Verfügbarkeit oder Amazon Aurora Serverless für eine bessere Skalierung verwendet wird. Bei sehr hohen Verfügbarkeitsanforderungen kann es sinnvoll sein, sich überhaupt nicht auf den primären Writer zu verlassen. Für Abfragen, die nur lesen, können Lesereplikate verwendet werden, die Redundanz und die Möglichkeit bieten, nicht nur hoch-, sondern auch aufzuskalieren. Schreibvorgänge können gepuffert werden, zum Beispiel in einer Amazon Simple Queue Service-Warteschlange, sodass Schreibanfragen von Kunden auch dann akzeptiert werden können, wenn das primäre Gerät vorübergehend nicht verfügbar ist.

## Ressourcen

### Zugehörige Dokumente:

- [Amazon API Gateway: Drosseln Sie API Anfragen für einen besseren Durchsatz](#)
- [CircuitBreaker\(fasst Circuit Breaker aus „Release It!“ zusammen Buch\)](#)
- [Fehler bei Wiederholungsversuchen und exponentieller Backoff in AWS](#)
- [Michael Nygard “Release It! Design and Deploy Production-Ready Software”](#)
- [Die Amazon Builders' Library: Vermeiden von Fallback in verteilten Systemen](#)
- [Die Amazon Builders' Library: Vermeiden von nicht mehr aufholbaren Warteschlangen-Rückständen](#)
- [Die Amazon Builders' Library: Herausforderungen und Strategien für das Caching](#)
- [Die Amazon Builders' Library: Timeouts, Wiederholungen und Backoff mit Jitter](#)

### Zugehörige Videos:

- [Wiederholung, Backoff und Jitter: AWS re:Invent 2019: Wir stellen vor: Die Amazon Builders' Library \(\) DOP328](#)

Zugehörige Beispiele:

- [Well-Architected lab: Level 300: Implementing Health Checks and Managing Dependencies to Improve Reliability](#)

## REL05-BP02 Drosselungsanfragen

Drosseln Sie Anfragen, um eine Ressourcenüberlastung aufgrund eines unerwarteten Nachfrageanstiegs zu verringern. Anfragen, die unter der Drosselungsrate liegen, werden bearbeitet, während Anfragen, die das definierte Limit überschreiten, mit einer Rückmeldung abgelehnt werden, dass die Anforderung gedrosselt wurde.

Gewünschtes Ergebnis: Stark ansteigendes Volumen, das entweder durch plötzliche Anstiege des Kundendatenverkehrs, Flooding-Angriffe oder Wiederholungstürme verursacht wird, wird durch Anfragedrosselung abgeschwächt, sodass Workloads die normale Verarbeitung des unterstützten Anforderungsvolumens fortsetzen können.

Typische Anti-Muster:

- APIDrosselungen für Endgeräte sind nicht implementiert oder werden auf den Standardwerten belassen, ohne dass die zu erwartenden Mengen berücksichtigt werden.
- API-Endpunkte werden nicht ausgelastet oder Drosselungsgrenzwerte wurden nicht getestet.
- Anforderungsraten werden ohne Berücksichtigung der Größe oder Komplexität der Anfrage gedrosselt.
- Es werden sowohl die maximalen Anforderungsraten als auch die maximale Anforderungsgröße getestet, aber nicht beides zusammen.
- Ressourcen werden nicht mit denselben Limits bereitgestellt, die beim Testen festgelegt wurden.
- Nutzungspläne wurden nicht konfiguriert oder für Verbraucher, die von der Anwendung bis zur Anwendung (A2A) verwendet werden, in Betracht gezogen. API
- Für Warteschlangenverbraucher, die horizontal skalieren, sind keine Einstellungen für maximale Parallelität konfiguriert.
- Eine Ratenbegrenzung pro IP-Adresse wurde nicht implementiert.



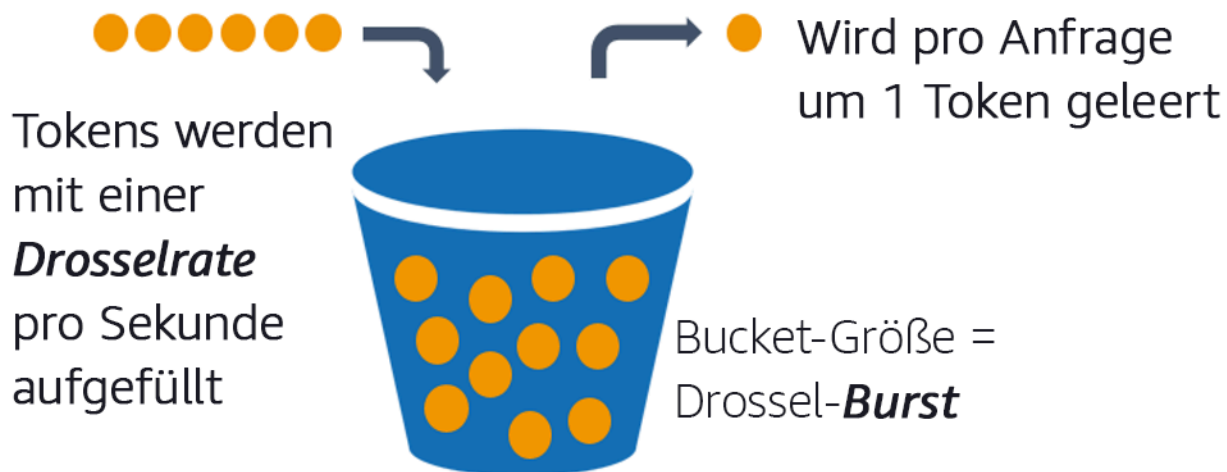
Vorteile der Nutzung dieser bewährten Methode: Workloads, die Drosselgrenzwerte festlegen, können normal arbeiten und akzeptierte Anfragen auch bei unerwarteten Volumenspitzen erfolgreich verarbeiten. Plötzliche oder anhaltende Spitzen von Anfragen an APIs und Warteschlangen werden gedrosselt, sodass die Ressourcen für die Anforderungsverarbeitung nicht ausgeschöpft werden. Durch Ratenbegrenzungen werden einzelne Anforderer gedrosselt, sodass ein hohes Datenvolumen von einer einzelnen IP-Adresse oder einem einzelnen Verbraucher die Ressourcen nicht erschöpft und sich auf andere API Verbraucher auswirkt.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Hoch

### Implementierungsleitfaden

Services sollten so konzipiert sein, dass sie eine bekannte Kapazität von Anfragen verarbeiten. Diese Kapazität kann durch Auslastungstests ermittelt werden. Wenn die Anzahl der Anfragen die Grenzwerte überschreitet, signalisiert die entsprechende Antwort, dass eine Anfrage gedrosselt wurde. Dies ermöglicht es dem Verbraucher, den Fehler zu beheben und es später erneut zu versuchen.

Wenn für Ihren Service eine Drosselungsimplementierung erforderlich ist, sollten Sie die Implementierung des Token-Bucket-Algorithmus in Betracht ziehen, bei dem ein Token für eine Anfrage zählt. Tokens werden mit einer Drosselrate pro Sekunde aufgefüllt und asynchron um ein Token pro Anfrage geleert.



### Der Token-Bucket-Algorithmus

[Amazon API Gateway](#) implementiert den Token-Bucket-Algorithmus gemäß Konto- und Regionsbeschränkungen und kann pro Kunde mit Nutzungsplänen konfiguriert werden. Darüber

hinaus können [Amazon Simple Queue Service \(AmazonSQS\)](#) und [Amazon Kinesis](#) Anfragen zwischenspeichern, um die Anforderungsrate auszugleichen, und höhere Drosselungsraten für Anfragen ermöglichen, die bearbeitet werden können. Schließlich können Sie eine Ratenbegrenzung implementieren, um bestimmte API Verbraucher [AWS WAF](#) zu drosseln, die eine ungewöhnlich hohe Last erzeugen.

## Implementierungsschritte

Sie können API Gateway mit Drosselungsgrenzen für Sie konfigurieren APIs und bei Überschreitung der Grenzwerte 429 Too Many Requests Fehler zurückgeben. Sie können es AWS WAF zusammen mit Ihren AWS AppSync und API Gateway-Endpunkten verwenden, um die Ratenbegrenzung pro IP-Adresse zu aktivieren. Wenn Ihr System asynchrone Verarbeitung toleriert, können Sie außerdem Nachrichten in eine Warteschlange oder einen Stream stellen, um die Antworten an Service-Clients zu beschleunigen und so höhere Drosselungsraten zu erreichen.

Bei asynchroner Verarbeitung können Sie, wenn Sie Amazon SQS als Ereignisquelle für konfiguriert haben, [maximale Parallelität konfigurieren AWS Lambda, um zu verhindern, dass hohe Ereignisraten das verfügbare Kontingent](#) für die gleichzeitige Ausführung des Kontos verbrauchen, das für andere Services in Ihrem Workload oder Konto erforderlich ist.

APIGateway bietet zwar eine verwaltete Implementierung des Token-Buckets, aber in Fällen, in denen Sie API Gateway nicht verwenden können, können Sie die Vorteile sprachspezifischer Open-Source-Implementierungen (siehe verwandte Beispiele unter Ressourcen) des Token-Buckets für Ihre Dienste nutzen.

- Machen Sie sich mit den [APIGateway-Drosselungslimits](#) auf Kontoebene, pro Region, pro Phase und auf API Schlüsselebene API pro Nutzungsplan vertraut und konfigurieren Sie sie.
- Wenden Sie [Regeln zur AWS WAF Ratenbegrenzung](#) auf API Gateways und AWS AppSync Endgeräte an, um sich vor Überschwemmungen zu schützen und bösartige Angriffe zu blockieren. IPs Regeln zur Ratenbegrenzung können auch für AWS AppSync API Schlüssel für A2A-Verbraucher konfiguriert werden.
- Überlegen Sie, ob Sie für die Drosselung mehr Kontrolle als für die Ratenbegrenzung benötigen AWS AppSync APIs, und konfigurieren Sie in diesem Fall ein API Gateway vor Ihrem Endpunkt. AWS AppSync
- Wenn SQS Amazon-Warteschlangen als Auslöser für Lambda-Warteschlangennutzer eingerichtet sind, legen Sie die [maximale Parallelität](#) auf einen Wert fest, der ausreichend verarbeitet wird, um Ihre Service-Level-Ziele zu erreichen, aber keine Parallelitätslimits verbraucht, die sich auf andere Lambda-Funktionen auswirken. Erwägen Sie, die reservierte Gleichzeitigkeit für andere Lambda-

Funktionen in demselben Konto und derselben Region festzulegen, wenn Sie Warteschlangen mit Lambda verbrauchen.

- Verwenden Sie API Gateway mit systemeigenen Serviceintegrationen zu Amazon SQS oder Kinesis, um Anfragen zu puffern.
- Wenn Sie API Gateway nicht verwenden können, schauen Sie sich sprachspezifische Bibliotheken an, um den Token-Bucket-Algorithmus für Ihren Workload zu implementieren. Sehen Sie sich den Abschnitt mit den Beispielen an und recherchieren Sie selbst, um eine geeignete Bibliothek zu finden.
- Testen Sie Grenzwerte, die Sie festlegen oder deren Erhöhung Sie zulassen möchten, und dokumentieren Sie die getesteten Grenzwerte.
- Erhöhen Sie die Grenzwerte nicht über das hinaus, was Sie beim Testen festgelegt haben. Wenn Sie einen Grenzwert erhöhen, stellen Sie sicher, dass die bereitgestellten Ressourcen bereits denen in Testszenarien entsprechen oder diese übertreffen, bevor Sie die Erhöhung anwenden.

## Ressourcen

Zugehörige bewährte Methoden:

- [REL04-BP03 Arbeite ständig](#)
- [REL05-BP03 Steuerung und Begrenzung von Wiederholungsaufrufen](#)

Zugehörige Dokumente:

- [Amazon API Gateway: Drosseln Sie API Anfragen für einen besseren Durchsatz](#)
- [AWS WAF: Rate-based rule statement](#)
- [Einführung einer maximalen Parallelität von AWS Lambda bei der Verwendung von Amazon SQS als Ereignisquelle](#)
- [AWS Lambda: Maximum Concurrency](#)

Zugehörige Beispiele:

- [Die drei wichtigsten AWS WAF ratenbasierten Regeln](#)
- [Java Bucket4j](#)
- [Python-Token-Bucket](#)

- [Node-Token-Bucket](#)
- [.NETBegrenzung der System-Threading-Rate](#)

Zugehörige Videos:

- [Implementierung von Best Practices für die API Sicherheit von GraphQL mit AWS AppSync](#)

Zugehörige Tools:

- [APIAmazon-Gateway](#)
- [AWS AppSync](#)
- [Amazon SQS](#)
- [Amazon Kinesis](#)
- [AWS WAF](#)

## REL05-BP03 Steuerung und Begrenzung von Wiederholungsaufrufen

Verwenden Sie das exponentielle Backoff, um Anfragen in zunehmend längeren Intervallen zwischen den einzelnen Wiederholungsversuchen zu wiederholen. Führen Sie Jitter zwischen den Wiederholungen ein, um die Wiederholungsintervalle zufällig zu bestimmen. Beschränken Sie die maximale Anzahl an Wiederholungen.

Gewünschtes Ergebnis: Zu den typischen Komponenten eines verteilten Softwaresystems gehören Server, Load Balancer, Datenbanken und Server. Während des normalen Betriebs können diese Komponenten auf Anfragen mit temporären oder begrenzten Fehlern sowie mit Fehlern antworten, die unabhängig von Wiederholungsversuchen dauerhaft bleiben würden. Wenn Clients Anfragen an Services stellen, verbrauchen die Anfragen Ressourcen wie Speicher, Threads, Verbindungen, Ports oder andere begrenzte Ressourcen. Die Steuerung und Einschränkung von Wiederholungsversuchen ist eine Strategie zur Freigabe und Minimierung des Ressourcenverbrauchs, sodass beanspruchte Systemkomponenten nicht überlastet werden.

Wenn Client-Anfragen eine Zeitüberschreitung oder Fehlerantworten erhalten, sollten sie entscheiden, ob sie es erneut versuchen möchten oder nicht. Wenn sie es erneut versuchen, tun sie dies mit exponentiellem Backoff mit Jitter und einem maximalen Wiederholungswert. Dadurch werden Backend-Services und -Prozesse entlastet und erhalten Zeit, um sich selbst zu reparieren, was zu einer schnelleren Wiederherstellung und einer erfolgreichen Bearbeitung von Anfragen führt.

## Typische Anti-Muster:

- Wiederholungsversuche werden ohne exponentielles Backoff, Jitter und maximale Wiederholungswerte implementiert. Backoff und Jitter helfen dabei, künstliche Datenverkehrsspitzen zu vermeiden, die durch ungewollt koordinierte Wiederholungsversuche in regelmäßigen Intervallen entstehen.
- Implementierung von Wiederholungsversuchen, ohne deren Auswirkungen zu testen oder davon auszugehen, dass Wiederholungsversuche bereits in Szenarien integriert sind, und SDK ohne Wiederholungsversuche zu testen.
- Veröffentlichte Fehlercodes aus Abhängigkeiten werden nicht richtig interpretiert, was dazu führt, dass bei allen Fehlern eine Wiederholung versucht wird, auch dann, wenn die Ursache auf eine fehlende Berechtigung, einen Konfigurationsfehler oder ein anderes Problem hindeutet, das vorhersehbar nicht ohne manuelles Eingreifen behoben werden kann.
- Beobachtbarkeits-Praktiken, einschließlich der Überwachung und Meldung von Warnmeldungen bei wiederholten Serviceausfällen, damit die zugrunde liegenden Probleme bekannt werden und behoben werden können, werden nicht beachtet.
- Es werden benutzerdefinierte Wiederholungsmechanismen entwickelt, wenn integrierte Wiederholungsfunktionen oder Wiederholungsfunktionen von Drittanbietern ausreichen.
- Es werden Wiederholungsversuche auf mehreren Ebenen eines Anwendungstapels auf eine Weise ausgeführt, die Wiederholungsversuche verstärkt, was die Ressourcen durch einen Wiederholungssturm weiter verbraucht. Vergewissern Sie sich, dass Sie verstehen, wie sich diese Fehler auf Ihre Anwendung und die Abhängigkeiten auswirken, auf die Sie sich verlassen, und führen Sie dann Wiederholungsversuche nur auf einer Ebene durch.
- Nicht idempotente Serviceaufrufe werden erneut versucht, was zu unerwarteten Nebeneffekten wie doppelten Ergebnissen führt.

Vorteile der Nutzung dieser bewährten Methode: Wiederholungsversuche helfen Clients dabei, die gewünschten Ergebnisse zu erzielen, wenn Anfragen fehlschlagen, verbrauchen aber auch mehr Zeit auf dem Server, um die gewünschten erfolgreichen Antworten zu erhalten. Wenn Fehler selten oder vorübergehend auftreten, funktionieren Wiederholungsversuche gut. Wenn Fehler durch Ressourcenüberlastung verursacht werden, können Wiederholungsversuche die Situation verschlimmern. Durch das Hinzufügen eines exponentiellen Backoffs mit Jitter zu den Client-Wiederholungsversuchen können Server sich erholen, wenn Ausfälle durch Ressourcenüberlastung verursacht werden. Jitter verhindert, dass Anfragen zu Datenverkehrsspitzen führen, und Backoff verringert die Lasteskalation, die durch das Hinzufügen von Wiederholungsversuchen zur

normalen Anforderungslast verursacht wird. Schließlich ist es wichtig, eine maximale Anzahl von Wiederholungsversuchen oder die verstrichene Zeit zu konfigurieren, um zu vermeiden, dass Rückstände entstehen, die zu metastabilen Ausfällen führen.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Hoch

### Implementierungsleitfaden

Steuern und begrenzen Sie Wiederholungsaufrufe. Verwenden Sie ein exponentielles Backoff, um Aufrufe nach zunehmend längeren Intervallen zu wiederholen. Nutzen Sie Jitter, um die Wiederholungsintervalle zu randomisieren, und legen Sie ein Limit für die Zahl der Wiederholungen fest.

Einige AWS SDKs implementieren standardmäßig Wiederholungsversuche und exponentielles Backoff. Verwenden Sie diese integrierten AWS Implementierungen, sofern dies für Ihren Workload relevant ist. Implementieren Sie eine ähnliche Logik in Ihrem Workload, wenn Sie Services aufrufen, die idempotent sind und bei denen Wiederholungsversuche die Verfügbarkeit Ihrer Clients verbessern. Legen Sie entsprechend Ihrem Anwendungsfall Zeitüberschreitungen fest und geben Sie an, wann Wiederholungsversuche gestoppt werden sollen. Erstellen Sie Testszenarien für diese Wiederholungsfälle und führen Sie sie aus.

### Implementierungsschritte

- Ermitteln Sie die optimale Ebene in Ihrem Anwendungsstack, um Wiederholungsversuche für die Services zu implementieren, auf die sich Ihre Anwendung stützt.
- Seien Sie sich bewusst SDKs, dass es für die Sprache Ihrer Wahl bewährte Wiederholungsstrategien mit exponentiellem Backoff und Jitter gibt, und ziehen Sie diese dem Schreiben Ihrer eigenen Wiederholungsimplementierungen vor.
- Stellen Sie sicher, dass [Services idempotent sind](#), bevor Sie Wiederholungen implementieren. Sobald Wiederholungsversuche implementiert wurden, stellen Sie sicher, dass sie sowohl getestet als auch regelmäßig in der Produktion ausgeführt werden.
- Verwenden Sie beim Aufrufen des AWS Dienstes die Option und APIs machen Sie sich mit den Konfigurationsoptionen für [AWS SDKs](#) Wiederholungen vertraut [AWS CLI](#). Finden Sie heraus, ob die Standardeinstellungen für Ihren Anwendungsfall geeignet sind, testen Sie sie und passen Sie sie nach Bedarf an.

### Ressourcen

Zugehörige bewährte Methoden:

- [REL04-BP04 Alle Antworten idempotent machen](#)
- [REL05-BP02 Drosselungsanfragen](#)
- [REL05-BP04 Schnelles Scheitern und begrenzte Warteschlangen](#)
- [REL05-BP05 Client-Timeouts festlegen](#)
- [REL11-BP01 Überwachen Sie alle Komponenten des Workloads, um Fehler zu erkennen](#)

#### Zugehörige Dokumente:

- [Fehler bei Wiederholungen und exponentiellem Backoff in AWS](#)
- [Die Amazon Builders' Library: Timeouts, Wiederholungen und Backoff mit Jitter](#)
- [Exponential Backoff and Jitter](#)
- [Machen Sie Wiederholungen mit idempotent sicher APIs](#)

#### Zugehörige Beispiele:

- [Spring Retry](#)
- [Resilience4j Retry](#)

#### Zugehörige Videos:

- [Wiederholung, Backoff und Jitter: AWS re:Invent 2019: Einführung in die Amazon Builders' Library \(\) DOP328](#)

#### Zugehörige Tools:

- [AWS SDKs und Tools: Verhalten bei Wiederholungen](#)
- [AWS Command Line Interface: Wiederholungen AWS CLI](#)

### REL05-BP04 Schnelles Scheitern und begrenzte Warteschlangen

Wenn ein Service nicht in der Lage ist, erfolgreich auf eine Anfrage zu antworten, sollte er schnell scheitern. Dies ermöglicht die Freigabe von mit einer Anfrage verbundenen Ressourcen und damit die Wiederherstellung eines Services, falls dieser nicht mehr über genügend Ressourcen verfügt. Schnelles Scheitern ist ein etabliertes Softwaredesignmuster, das genutzt werden kann, um hochzuverlässige Workloads in der Cloud aufzubauen. Warteschlangen sind ebenfalls ein

etabliertes Integrationsmuster für Unternehmen. Sie sorgen für eine ausgeglichene Auslastung und ermöglichen es den Clients, Ressourcen freizugeben, wenn eine asynchrone Verarbeitung toleriert wird. Wenn ein Service unter normalen Bedingungen erfolgreich antworten kann, aber fehlschlägt, wenn die Anforderungsrate zu hoch ist, verwenden Sie eine Warteschlange, um Anfragen zwischenspeichern. Lassen Sie jedoch keine langen Warteschlangen zu. Sie können dazu führen, dass veraltete Anfragen verarbeitet werden, die ein Client bereits aufgegeben hat.

Gewünschtes Ergebnis: Wenn bei Systemen Ressourcenknappheit, Timeouts, Ausnahmen oder Grauausfälle auftreten, die Service-Level-Ziele unerreichbar machen, ermöglichen Strategien für schnelles Scheitern eine schnellere Systemwiederherstellung. Systeme, die Traffic-Spitzen absorbieren müssen und asynchrone Verarbeitung ermöglichen, können die Zuverlässigkeit verbessern, indem sie es Clients ermöglichen, Anfragen schnell freizugeben, indem sie Warteschlangen verwenden, um Anfragen an Back-End-Services zu puffern. Beim Puffern von Anfragen in Warteschlangen werden Strategien zur Warteschlangenverwaltung implementiert, um nicht mehr aufzuholende Rückstände zu vermeiden.

Typische Anti-Muster:

- Implementierung von Nachrichtenwarteschlangen ohne Konfiguration von Warteschlangen (DLQ) oder Alarmen auf DLQ Volumes, um zu erkennen, wenn ein System ausfällt.
- Nichterfassung des Alters von Nachrichten in einer Warteschlange, einem Indikator für Latenz, um zu verstehen, wann Warteschlangenverbraucher mit der Verarbeitung nicht mehr hinterher kommen oder Fehler machen, was zu erneuten Versuchen führt.
- Kein Löschen von aufgestauten Nachrichten aus einer Warteschlange, wenn es keinen Sinn macht, diese Nachrichten zu verarbeiten, da kein Geschäftsbedarf mehr besteht.
- Die Konfiguration von FIFO First-in-First-Out-Warteschlangen bei Last-In-First-Out (LIFO) - Warteschlangen wäre besser auf die Bedürfnisse der Kunden zugeschnitten, z. B. wenn keine strikte Reihenfolge erforderlich ist und die Backlog-Verarbeitung alle neuen und zeitkritischen Anfragen verzögert, was dazu führt, dass bei allen Clients Service-Level-Verstöße auftreten.
- Interne Warteschlangen für Clients verfügbar zu machen, anstatt diese für die Verwaltung des Arbeitseingangs und APIs das Platzieren von Anfragen in interne Warteschlangen zu verwenden.
- Wenn zu viele Arbeitsanforderungstypen in einer einzigen Warteschlange zusammengefasst werden, kann dies die Backlog-Bedingungen verschärfen, da der Ressourcenbedarf auf die verschiedenen Anforderungstypen verteilt wird.
- Verarbeitung komplexer und einfacher Anfragen in derselben Warteschlange, obwohl unterschiedliche Überwachungs-, Timeout- und Ressourcenzuweisungen erforderlich sind.



- Keine Validierung von Eingaben oder Nutzung von Aussagen, um Mechanismen für schnelles Scheitern in Software zu implementieren, die Ausnahmen an übergeordnete Komponenten weiterleiten, die Fehler problemlos verarbeiten können.
- Keine Entfernung fehlerhafter Ressourcen aus der Anforderungswarteschlange, insbesondere bei Ausfällen ohne erkennbare Ursache mit sowohl erfolgreicher als auch fehlgeschlagener Verarbeitung aufgrund von Abstürzen und Neustarts, zeitweise auftretenden Abhängigkeitsfehlern, verringerter Kapazität oder Verlust von Netzwerkpaketen.

Vorteile der Nutzung dieser bewährten Methode: Systeme, die schnelles Scheitern nutzen, lassen sich leichter debuggen und korrigieren und weisen häufig Probleme im Code und in der Konfiguration auf, bevor Releases für die Produktion veröffentlicht werden. Systeme, die effektive Warteschlangenstrategien beinhalten, sind widerstandsfähiger und zuverlässiger bei Traffic-Spitzen und zeitweiligen Systemstörungen.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Hoch

### Implementierungsleitfaden

Strategien für schnelles Scheitern können sowohl in Softwarelösungen als auch in der Infrastruktur konfiguriert werden. Warteschlangen scheitern nicht nur schnell, sondern sind auch eine einfache und dennoch leistungsstarke Architekturtechnik zur Entkopplung von Systemkomponenten für eine ausgeglichene Auslastung. [Amazon CloudWatch](#) bietet Funktionen zur Überwachung von Ausfällen und zur Alarmierung bei Störungen. Sobald erkannt wird, dass ein System ausfällt, können Strategien zur Schadensbegrenzung umgesetzt werden, darunter auch der Wechsel weg von knapp werdenden Ressourcen. Wenn Systeme Warteschlangen mit [Amazon SQS](#) und anderen Warteschlangentechnologien implementieren, um das Laden zu erleichtern, müssen sie berücksichtigen, wie Warteschlangentrüger sowie Fehler beim Nachrichtenverbrauch verwaltet werden können.

### Implementierungsschritte

- Implementieren Sie programmatische Aussagen oder spezifische Metriken in Ihrer Software und verwenden Sie diese, um explizit Alarme bei Systemproblemen auszulösen. Amazon CloudWatch unterstützt Sie bei der Erstellung von Metriken und Alarmen auf der Grundlage des Anwendungsprotokollmusters und der SDK Instrumentierung.
- Verwenden Sie CloudWatch Metriken und Alarme, um beeinträchtigte Ressourcen auszulagern, die die Latenz bei der Verarbeitung erhöhen oder Anfragen wiederholt nicht bearbeiten können.

- Verwenden Sie asynchrone Verarbeitung, indem Sie mithilfe von Amazon Anfragen annehmen und Anfragen an interne Warteschlangen anhängen SQS und dann dem Kunden, der die Nachricht sendet, eine Erfolgsmeldung senden, sodass der Kunde Ressourcen freigeben und mit anderen Arbeiten fortfahren kann, während Backend-Warteschlangenverbraucher Anfragen verarbeiten. APIs
- Messen und überwachen Sie die Latenz bei der Warteschlangenverarbeitung, indem Sie jedes Mal, wenn Sie eine Nachricht aus einer Warteschlange nehmen, eine CloudWatch Metrik erstellen, indem Sie den aktuellen Wert mit dem Nachrichtenzeitstempel vergleichen.
- Wenn Fehler eine erfolgreiche Nachrichtenverarbeitung verhindern oder der Datenverkehr so stark ansteigt, dass er im Rahmen der Service Level Agreements nicht verarbeitet werden kann, wird älterer oder überschüssiger Datenverkehr in eine Überlaufwarteschlange ausgelagert. So können vorrangig neuere Aufträge verarbeitet werden. Ältere Aufträge werden verarbeitet, sobald Kapazitäten frei werden. Diese Technik ist eine Annäherung an die LIFO Verarbeitung und ermöglicht eine normale Systemverarbeitung für alle neuen Aufgaben.
- Verwenden Sie Warteschlangen für unzustellbare Nachrichten oder Redrive-Warteschlangen, um Nachrichten, die nicht verarbeitet werden können, aus dem Backlog an einen Ort zu verschieben, der später geprüft und verarbeitet werden kann.
- Versuchen Sie es entweder erneut oder, sofern dies tolerierbar ist, löschen Sie alte Nachrichten, indem Sie die tatsächliche Zeit mit dem Nachrichtenzeitstempel vergleichen und Nachrichten verwerfen, die für den anfragenden Client nicht mehr relevant sind.

## Ressourcen

### Zugehörige bewährte Methoden:

- [REL04-BP02 Lose gekoppelte Abhängigkeiten implementieren](#)
- [REL05-BP02 Drosselungsanfragen](#)
- [REL05-BP03 Steuerung und Begrenzung von Wiederholungsaufrufen](#)
- [REL06-BP02 Metriken definieren und berechnen \(Aggregation\)](#)
- [REL06-BP07 Überwachen Sie die end-to-end Nachverfolgung von Anfragen durch Ihr System](#)

### Zugehörige Dokumente:

- [Vermeiden von nicht mehr aufzuholenden Rückständen](#)
- [Fail Fast](#)

- [Wie kann ich verhindern, dass immer mehr Nachrichten in meiner SQS Amazon-Warteschlange zurückbleiben?](#)
- [Elastic Load Balancing: Zonal Shift](#)
- [Amazon Application Recovery Controller: Routing-Steuerung für Datenverkehrs-Failover](#)

Zugehörige Beispiele:

- [Enterprise Integration Patterns: Dead Letter Channel](#)

Zugehörige Videos:

- [AWS re:Invent 2022 — Betrieb hochverfügbarer Multi-AZ-Anwendungen](#)

Zugehörige Tools:

- [Amazon SQS](#)
- [Amazon MQ](#)
- [AWS IoT Core](#)
- [Amazon CloudWatch](#)

## REL05-BP05 Client-Timeouts festlegen

Legen Sie angemessene Zeitüberschreitungen für Verbindungen und Anfragen fest, überprüfen Sie sie systematisch und verlassen Sie sich nicht auf Standardwerte, da sie nicht Workload-spezifisch sind.

Gewünschtes Ergebnis: Client-Zeitüberschreitungen sollten die Kosten für Client, Server und Workload berücksichtigen, die mit dem Warten auf Anfragen verbunden sind, deren Bearbeitung ungewöhnlich lange dauert. Da es nicht möglich ist, die genaue Ursache einer Zeitüberschreitung zu ermitteln, müssen Clients ihr Wissen über Services nutzen, um Erwartungen hinsichtlich wahrscheinlicher Ursachen und geeigneter Zeitüberschreitungen zu entwickeln.

Bei Client-Verbindungen kommt es aufgrund der konfigurierten Werte zu einer Zeitüberschreitung. Nach einer Zeitüberschreitung entscheidet der Client entweder, die Anfrage abzurechnen und es erneut zu versuchen oder er öffnet einen [Unterbrecher](#). Durch diese Muster wird vermieden, dass Anfragen gestellt werden, die einen zugrunde liegenden Fehlerzustand verschlimmern könnten.

## Typische Anti-Muster:

- Systemzeitüberschreitungen oder standardmäßige Zeitüberschreitungen werden nicht beachtet.
- Normale Abschlusszeit für Anfragen ist nicht bekannt.
- Mögliche Ursachen, warum die Bearbeitung von Anfragen ungewöhnlich lange dauert, oder die Kosten für die Client-, Service- oder Workload-Leistung, die während des Wartens darauf, dass diese Anfragen abgeschlossen werden, anfallen, sind nicht bekannt.
- Die Wahrscheinlichkeit, dass ein gestörtes Netzwerk dazu führt, dass eine Anfrage erst dann fehlschlägt, wenn die Zeitüberschreitung erreicht ist, und die Kosten für die Client- und Workload-Leistung, die entstehen, wenn keine kürzere Zeitüberschreitung gewählt wird, sind nicht bekannt.
- Zeitüberschreitungsszenarien sowohl für Verbindungen als auch für Anfragen werden nicht getestet.
- Zu hohe Zeitüberschreitungen können zu langen Wartezeiten führen und die Ressourcenauslastung erhöhen.
- Zu niedrige Zeitüberschreitungen führen zu künstlichen Fehlschlägen.
- Muster zur Behandlung von Zeitüberschreitungsfehlern bei Remote-Aufrufen wie Unterbrecher und Wiederholungsversuchen werden übersehen.
- Die Überwachung der Fehlerraten bei Serviceaufrufen, der Service-Level-Ziele für die Latenz und der Latenzausreißer wird nicht in Betracht gezogen. Diese Metriken können Aufschluss über aggressive oder tolerante Zeitüberschreitungen geben.

Vorteile der Nutzung dieser bewährten Methode: Zeitüberschreitungen für Remote-Aufrufe sind konfiguriert und die Systeme sind so konzipiert, dass sie Zeitüberschreitungen ordnungsgemäß behandeln, sodass Ressourcen geschont werden, wenn Remote-Aufrufe ungewöhnlich langsam reagieren und Zeitüberschreitungsfehler von Service-Clients ordnungsgemäß behandelt werden.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Hoch

## Implementierungsleitfaden

Legen Sie eine Zeitüberschreitung für Verbindungen sowie Anfragen für alle Serviceabhängigkeitsaufrufe und generell für prozessübergreifende Aufrufe fest. Viele Frameworks bieten integrierte Zeitüberschreitungsfunktionen. Seien Sie jedoch vorsichtig, da einige Standardwerte unendlich oder höher als für Ihre Serviceziele akzeptabel sind. Ein zu hoher Wert reduziert die Nützlichkeit der Zeitbeschränkung, da Ressourcen weiterhin verbraucht werden, während der Client auf das Einsetzen der Zeitbeschränkung wartet. Ein zu niedriger Wert kann zu

erhöhtem Datenverkehr im Backend und zu erhöhter Latenz führen, da zu viele Anfragen wiederholt werden. In einigen Fällen kann dies zu vollständigen Ausfällen führen, da alle Anfragen wiederholt werden.

Beachten Sie bei der Festlegung von Zeitüberschreitungsstrategien Folgendes:

- Die Bearbeitung von Anfragen kann aufgrund ihres Inhalts, Beeinträchtigungen eines Zieldienstes oder eines Ausfalls einer Netzwerkpartition länger als normal dauern.
- Anfragen mit ungewöhnlich aufwändigem Inhalt könnten unnötige Server- und Client-Ressourcen verbrauchen. In diesem Fall können Ressourcen geschont werden, wenn für diese Anfragen eine Zeitüberschreitung konfiguriert wird und es nicht erneut versucht wird. Services sollten sich auch durch Drosselungen und serverseitige Zeitüberschreitungen vor ungewöhnlich aufwändigen Inhalten schützen.
- Anfragen, die aufgrund einer Servicebeeinträchtigung ungewöhnlich lange dauern, können mit einer Zeitüberschreitung abgebrochen und erneut versucht werden. Die Servicekosten für die Anfrage und den erneuten Versuch sollten berücksichtigt werden. Wenn die Ursache jedoch eine lokale Beeinträchtigung ist, ist ein erneuter Versuch wahrscheinlich nicht teuer und reduziert den Ressourcenverbrauch des Clients. Die Zeitüberschreitung kann je nach Art der Beeinträchtigung auch Serverressourcen freisetzen.
- Anfragen, deren Bearbeitung lange dauert, weil die Anfrage oder Antwort nicht vom Netzwerk zugestellt wurde, können mit einer Zeitüberschreitung abgebrochen und erneut versucht werden. Da die Anfrage oder Antwort nicht zugestellt wurde, würde sie unabhängig von der Länge der Zeitüberschreitung fehlschlagen. Durch eine Zeitüberschreitung werden in diesem Fall keine Serverressourcen, aber Client-Ressourcen freigegeben und die Workload-Leistung wird verbessert.

Nutzen Sie etablierte Entwurfsmuster wie Wiederholungsversuche und Schutzschalter, um Timeouts elegant zu handhaben und ausfallschnelle Ansätze zu unterstützen. [AWS SDKs](#) und [AWS CLI](#) ermöglichen die Konfiguration von Verbindungs- und Anforderungs-Timeouts sowie von Wiederholungsversuchen mit exponentiellem Backoff und Jitter. [AWS Lambda](#) Funktionen unterstützen die Konfiguration von Timeouts. Damit können Sie Low-Code-Schutzschalter bauen [AWS Step Functions](#), die die Vorteile der vorgefertigten Integrationen mit Diensten und nutzen. AWS SDKs [AWS App Mesh](#) Envoy bietet Funktionen für Zeitüberschreitungen und Unterbrecher an.

## Implementierungsschritte

- Konfigurieren Sie Zeitüberschreitungen für Remote-Serviceaufrufe und nutzen Sie die integrierten sprachspezifischen Zeitüberschreitungsfunktionen oder Open-Source-Bibliotheken für Zeitüberschreitungen.
- Wenn Ihr Workload Aufrufe mit einem tätigt AWS SDK, finden Sie in der Dokumentation Informationen zur sprachspezifischen Timeout-Konfiguration.
  - [Python](#)
  - [PHP](#)
  - [.NET](#)
  - [Ruby](#)
  - [Java](#)
  - [Go](#)
  - [Node.js](#)
  - [C++](#)
- Wenn Sie AWS SDKs AWS CLI Or-Befehle in Ihrem Workload verwenden, konfigurieren Sie Standard-Timeout-Werte, indem Sie die AWS [Konfigurationsstandardwerte](#) für und festlegen.  
`connectTimeoutInMillis` `tlsNegotiationTimeoutInMillis`
- Wenden Sie [Befehlszeilenoptionen](#) `cli-read-timeout` an `cli-connect-timeout` und steuern Sie einmalige AWS CLI Befehle auf Dienste. AWS
- Überwachen Sie Remote-Serviceanfragen auf Zeitüberschreitungen und richten Sie Alarme für anhaltende Fehler ein, sodass Sie proaktiv mit Fehlerszenarien umgehen können.
- Implementieren Sie [CloudWatch Metriken](#) und [CloudWatch Anomalieerkennung](#) zu Anrufehlerraten, Service-Level-Zielen für Latenz und Latenzausreißer, um Einblicke in den Umgang mit übermäßig aggressiven oder toleranten Timeouts zu gewinnen.
- Konfigurieren Sie Zeitüberschreitungen für [Lambda-Funktionen](#).
- APIGateway-Clients müssen bei der Behandlung von Timeouts ihre eigenen Wiederholungsversuche implementieren. APIGateway unterstützt ein [Integrations-Timeout von 50 Millisekunden bis 29 Sekunden für Downstream-Integrationen und versucht es nicht erneut, wenn die Integration ein Timeout](#) anfordert.
- Implementieren Sie das [Unterbrecher](#)-Muster, um zu vermeiden, dass Remote-Aufrufe getätigt werden, wenn Zeitüberschreitungen auftreten. Öffnen Sie die Leitung, um fehlschlagende Aufrufe zu vermeiden, und schließen Sie die Leitung, wenn die Aufrufe normal reagieren.

- Für containerbasierte Workloads können Sie die Funktionen von [App Mesh Envoy](#) nutzen, um von den integrierten Zeitüberschreitungen und Unterbrechern zu profitieren.
- Wird verwendet AWS Step Functions , um Low-Code-Schutzschalter für Remote-Serviceanrufe zu erstellen, insbesondere wenn AWS native SDKs und unterstützte Step Functions Functions-Integrationen aufgerufen werden, um Ihre Arbeitslast zu vereinfachen.

## Ressourcen

### Zugehörige bewährte Methoden:

- [REL05-BP03 Steuerung und Begrenzung von Wiederholungsaufrufen](#)
- [REL05-BP04 Schnelles Scheitern und begrenzte Warteschlangen](#)
- [REL06-BP07 Überwachen Sie die end-to-end Nachverfolgung von Anfragen durch Ihr System](#)

### Zugehörige Dokumente:

- [AWS SDK: Wiederholungsversuche und Timeouts](#)
- [Die Amazon Builders' Library: Timeouts, Wiederholungen und Backoff mit Jitter](#)
- [Amazon API Gateway-Kontingente und wichtige Hinweise](#)
- [AWS Command Line Interface: Command line options](#)
- [AWS SDK for Java 2.x: API Timeouts konfigurieren](#)
- [AWS Botocore verwendet das Konfigurationsobjekt und die Konfigurationsreferenz](#)
- [AWS SDK for .NET: Retries and Timeouts](#)
- [AWS Lambda: Configuring Lambda function options](#)

### Zugehörige Beispiele:

- [Verwenden des Circuit Breaker Patterns mit AWS Step Functions Amazon DynamoDB](#)
- [Martin Fowler: CircuitBreaker](#)

### Zugehörige Tools:

- [AWS SDKs](#)
- [AWS Lambda](#)

- [Amazon SQS](#)
- [AWS Step Functions](#)
- [AWS Command Line Interface](#)

REL05-BP06 Systeme soweit möglich zustandslos machen

Systeme sollten entweder keinen Zustand erfordern oder ihn so auslagern, dass zwischen verschiedenen Client-Anfragen keine Abhängigkeit von lokal gespeicherten Daten auf der Festplatte und im Arbeitsspeicher besteht. Auf diese Weise können Server nach Belieben ersetzt werden, ohne dass dies Auswirkungen auf die Verfügbarkeit hat.

Wenn Benutzer oder Services mit einer Anwendung interagieren, führen sie häufig eine Reihe von Interaktionen aus, die eine Sitzung bilden. Bei einer Sitzung handelt es sich um eindeutige Daten für Benutzer, die zwischen Anfragen bestehen bleiben, während sie die Anwendung verwenden. Eine zustandslose Anwendung ist eine Anwendung, die keine Informationen zu früheren Interaktionen benötigt und keine Sitzungsinformationen speichert.

Sobald das System so konzipiert ist, dass es zustandslos ist, können Sie serverlose Rechen Dienste wie oder verwenden. AWS Lambda AWS Fargate

Neben dem Austausch von Servern besteht ein weiterer Vorteil statusfreier Anwendungen darin, dass sie horizontal skaliert werden können, da alle verfügbaren Rechenressourcen (wie EC2 Instanzen und AWS Lambda Funktionen) jede Anforderung bearbeiten können.

Vorteile der Nutzung dieser bewährten Methode: Systeme mit zustandslosem Design lassen sich besser an die horizontale Skalierung anpassen, sodass Kapazitäten je nach vorhandenem Datenverkehr und bestehender Nachfrage hinzugefügt oder entfernt werden können. Sie sind auch inhärent widerstandsfähig gegenüber Ausfällen und bieten Flexibilität und Agilität bei der Anwendungsentwicklung.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel

Implementierungsleitfaden

Erstellen Sie zustandslose Anwendungen. Zustandslose Anwendungen ermöglichen eine horizontale Skalierung und sind widerstandsfähig gegenüber Ausfällen einzelner Knoten. Analysieren Sie die Komponenten Ihrer Anwendung, die ihren Status innerhalb der Architektur beibehalten. Auf diese Weise können Sie die potenziellen Auswirkungen der Umstellung auf ein zustandsloses Design bewerten. Eine zustandslose Architektur entkoppelt Benutzerdaten und entlädt die Sitzungsdaten.



Dies bietet die Flexibilität, jede Komponente unabhängig zu skalieren, um unterschiedlichen Workload-Anforderungen gerecht zu werden und die Ressourcenauslastung zu optimieren.

### Implementierungsschritte

- Identifizieren und analysieren Sie die zustandsbehafteten Komponenten in Ihrer Anwendung.
- Entkoppeln Sie Daten, indem Sie Benutzerdaten von der Kernanwendungslogik trennen und verwalten.
  - [Amazon Cognito](#) kann Benutzerdaten mithilfe von Features wie [Identitätspools](#), [Benutzerpools](#) und [Amazon Cognito Sync](#) von Anwendungscode entkoppeln.
  - Sie können [AWS Secrets Manager](#) verwenden, um Benutzerdaten zu entkoppeln, indem Sie Secrets an einem sicheren, zentralen Ort speichern. Das bedeutet, dass der Anwendungscode keine Secrets speichern muss, was seine Sicherheit erhöht.
  - Erwägen Sie die Verwendung von [Amazon S3](#), um große, unstrukturierte Daten wie Bilder und Dokumente zu speichern. Ihre Anwendung kann diese Daten bei Bedarf abrufen, sodass sie nicht im Arbeitsspeicher gespeichert werden müssen.
  - Verwenden Sie [Amazon DynamoDB](#), um Informationen wie Benutzerprofile zu speichern. Ihre Anwendung kann diese Daten nahezu in Echtzeit abfragen.
- Verlagern Sie Sitzungsdaten in eine Datenbank, einen Cache oder externe Dateien.
  - [Amazon ElastiCache](#), Amazon DynamoDB, [Amazon Elastic File System](#) (AmazonEFS) und [Amazon MemoryDB](#) sind Beispiele für AWS Dienste, die Sie zum Auslagern von Sitzungsdaten verwenden können.
- Entwerfen Sie eine zustandslose Architektur, nachdem Sie festgelegt haben, welche Zustands- und Benutzerdaten in Ihrer bevorzugten Speicherlösung abgelegt werden müssen.

### Ressourcen

Zugehörige bewährte Methoden:

- [REL11-BP03 Automatisieren Sie die Heilung auf allen Ebenen](#)

Zugehörige Dokumente:

- [Die Amazon Builders' Library: Vermeiden von Fallback in verteilten Systemen](#)
- [Die Amazon Builders' Library: Vermeiden von nicht mehr aufholbaren Warteschlangen-Rückständen](#)

- [Die Amazon Builders' Library: Herausforderungen und Strategien für das Caching](#)
- [Bewährte Methoden für Stateless Web Tier auf AWS](#)

## REL05-BP07 Nothebel einbauen

Nothebel sind schnelle Prozesse, die die Auswirkungen auf die Verfügbarkeit Ihres Workloads mindern können.

Nothebel bewirken, dass das Verhalten von Komponenten oder Abhängigkeiten mithilfe bekannter und getesteter Mechanismen deaktiviert, gedrosselt oder geändert wird. Dadurch können Beeinträchtigungen des Workloads, die durch die Erschöpfung von Ressourcen aufgrund unerwarteter Nachfragessteigerungen verursacht werden, gemildert und die Auswirkungen von Ausfällen bei nicht kritischen Komponenten innerhalb Ihres Workloads reduziert werden.

Gewünschtes Ergebnis: Durch die Implementierung von Nothebeln können Sie bewährte Prozesse einrichten, um die Verfügbarkeit kritischer Komponenten in Ihrem Workload aufrechtzuerhalten. Der Workload sollte sich problemlos reduzieren lassen und auch während der Aktivierung eines Nothebels weiterhin seine geschäftskritischen Funktionen ausführen. Weitere Informationen zur graziösen Degradation finden Sie unter [REL05-BP01 Implementieren Sie eine graziöse Degradation, um entsprechende harte Abhängigkeiten in weiche Abhängigkeiten umzuwandeln](#).

Typische Anti-Muster:

- Der Ausfall von nicht kritischen Abhängigkeiten wirkt sich auf die Verfügbarkeit Ihres Kern-Workloads aus.
- Das Verhalten kritischer Komponenten wird während der Beeinträchtigung unkritischer Komponenten nicht getestet oder überprüft.
- Es sind keine klaren und deterministischen Kriterien für die Aktivierung oder Deaktivierung eines Nothebels definiert.

Vorteile der Nutzung dieser bewährten Methode: Die Implementierung von Nothebeln kann die Verfügbarkeit der kritischen Komponenten Ihres Workloads verbessern, indem Ihre Resolver mit bewährten Prozessen ausgestattet werden, um auf unerwartete Nachfragespitzen oder Ausfälle von nicht kritischen Abhängigkeiten zu reagieren.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel

## Implementierungsleitfaden

- Ermitteln Sie die kritischen Komponenten in Ihrem Workload.
- Entwerfen und gestalten Sie die kritischen Komponenten Ihres Workloads so, dass sie Ausfällen von nicht kritischen Komponenten standhalten.
- Führen Sie Tests durch, um das Verhalten Ihrer kritischen Komponenten beim Ausfall von nicht kritischen Komponenten zu überprüfen.
- Definieren und überwachen Sie relevante Metriken oder Auslöser für die Einleitung von Nothebeln.
- Definieren Sie die Verfahren (manuell oder automatisiert), die Bestandteil des Nothebels sind.

## Implementierungsschritte

- Ermitteln Sie die kritischen Komponenten in Ihrem Workload.
  - Jede technische Komponente Ihres Workloads sollte der entsprechenden Geschäftsfunktion zugeordnet und als kritisch oder nicht kritisch eingestuft werden. Beispiele für wichtige und unkritische Funktionen bei Amazon finden Sie unter [Any Day Can Be Prime Day: How Amazon.com Search Uses Chaos Engineering to Handle Over 84K Requests Per Second](#).
  - Hierbei handelt es sich sowohl um eine technische als auch um eine geschäftliche Entscheidung, die je nach Organisation und Workload unterschiedlich ausfallen kann.
- Entwerfen und gestalten Sie die kritischen Komponenten Ihres Workloads so, dass sie Ausfällen von nicht kritischen Komponenten standhalten.
  - Berücksichtigen Sie bei der Abhängigkeitsanalyse alle potenziellen Fehlermodi und stellen Sie sicher, dass Ihre Notfallmechanismen die kritischen Funktionen an nachgelagerte Komponenten weitergeben.
- Führen Sie Tests durch, um das Verhalten Ihrer kritischen Komponenten bei der Aktivierung Ihrer Nothebel zu überprüfen.
  - Vermeiden Sie bimodales Verhalten. Weitere Informationen finden Sie unter [REL11-BP05 Verwenden Sie statische](#) Stabilität, um bimodales Verhalten zu verhindern.
- Definieren und überwachen Sie relevante Metriken und lassen Sie gegebenenfalls einen Alarm auslösen, um einen Nothebel einzuleiten.
  - Die richtigen Metriken zur Überwachung zu finden, hängt von Ihrem Workload ab. Einige Beispielmetriken sind die Latenzzeit oder die Anzahl der fehlgeschlagenen Anfragen an eine Abhängigkeit.
- Definieren Sie die manuellen oder automatisierten Verfahren, die Bestandteil des Nothebels sind.

- Dazu können Mechanismen wie [Lastabwurf](#), [Drosselung von Anfragen](#) oder die Implementierung einer [ordnungsgemäßen Funktionsminderung](#) gehören.

## Ressourcen

### Zugehörige bewährte Methoden:

- [REL05-BP01 Implementieren Sie eine schrittweise Degradation, um anwendbare harte Abhängigkeiten in weiche Abhängigkeiten umzuwandeln](#)
- [REL05-BP02 Drosseln Sie Anfragen](#)
- [REL11-BP05 Verwenden Sie statische Stabilität, um bimodales Verhalten zu verhindern](#)

### Zugehörige Dokumente:

- [Automating safe, hands-off deployments](#)
- [Any Day Can Be Prime Day: How Amazon.com Search Uses Chaos Engineering to Handle Over 84K Requests Per Second](#)

### Zugehörige Videos:

- [AWS re:Invent 2020: Zuverlässigkeit, Konsistenz und Vertrauen durch Unveränderlichkeit](#)

## Änderungsmanagement

### Fragen

- [REL6. Wie werden Ihre Workload-Ressourcen überwacht?](#)
- [REL7. Wie wird die Workload so gestaltet, dass sie sich an Veränderungen der Nachfrage anpasst?](#)
- [REL8 Wie werden Veränderungen implementiert?](#)

### REL6. Wie werden Ihre Workload-Ressourcen überwacht?

Protokolle und Metriken sind leistungsstarke Tools, mit denen Sie sich einen Überblick über den Zustand Ihrer Workload verschaffen können. Sie können Ihre Workload so konfigurieren, dass Protokolle und Metriken überwacht und Benachrichtigungen gesendet werden, wenn Schwellenwerte

überschritten werden oder wichtige Ereignisse auftreten. Dank der Überwachung kann die Workload erkennen, wenn Schwellenwerte für eine niedrige Leistung unterschritten werden oder Ausfälle auftreten, sodass als Reaktion drauf eine automatische Wiederherstellung erfolgen kann.

### Bewährte Methoden

- [REL06-BP01 Alle Komponenten für den Workload überwachen \(Generation\)](#)
- [REL06-BP02 Metriken definieren und berechnen \(Aggregation\)](#)
- [REL06-BP03 Benachrichtigungen senden \(Verarbeitung und Alarmierung in Echtzeit\)](#)
- [REL06-BP04 Automatisierte Antworten \(Verarbeitung und Alarmierung in Echtzeit\)](#)
- [REL06-BP05 Logs analysieren](#)
- [REL06-BP06 Regelmäßige Überprüfungen durchführen](#)
- [REL06-BP07 Überwachen Sie die end-to-end Nachverfolgung von Anfragen durch Ihr System](#)

### REL06-BP01 Alle Komponenten für den Workload überwachen (Generation)

Überwachen Sie die Komponenten des Workloads mit Tools von Amazon CloudWatch oder Drittanbietern. Überwachen Sie AWS Dienste mit dem AWS Health Dashboard.

Alle Komponenten Ihres Workloads sollten überwacht werden, einschließlich Frontend, Geschäftslogik und Speicherstufen. Definieren Sie Schlüsselmetriken, beschreiben Sie, wie Sie diese gegebenenfalls aus Protokollen extrahieren, und legen Sie Schwellenwerte für das Auslösen entsprechender Alarmereignisse fest. Stellen Sie sicher, dass die Metriken für die wichtigsten Leistungsindikatoren (KPIs) Ihres Workloads relevant sind, und verwenden Sie Metriken und Protokolle, um Frühwarnsignale für eine Verschlechterung des Services zu erkennen. Beispielsweise kann eine Kennzahl, die sich auf Geschäftsergebnisse bezieht, wie die Anzahl der erfolgreich bearbeiteten Bestellungen pro Minute, schneller auf Workload-Probleme hinweisen als technische Kennzahlen wie die CPU Auslastung. Verwenden Sie das AWS Health Dashboard für einen personalisierten Überblick über die Leistung und Verfügbarkeit der AWS Dienste, die Ihren AWS Ressourcen zugrunde liegen.

Die Überwachung in der Cloud bietet neue Möglichkeiten. Die meisten Cloud-Anbieter haben anpassbare Hooks entwickelt und können Ihnen Einblicke liefern, mit denen Sie Ihre Workloads auf mehreren Ebenen überwachen können. AWS Dienste wie Amazon CloudWatch verwenden statistische Algorithmen und Algorithmen für maschinelles Lernen, um kontinuierlich Metriken von Systemen und Anwendungen zu analysieren, normale Ausgangswerte zu ermitteln und Anomalien

mit minimalem Benutzereingriff aufzudecken. Anomalieerkennungsalgorithmen berücksichtigen saisonale und trendbasierte Änderungen von Metriken.

AWS stellt eine Fülle von Überwachungs- und Protokollinformationen zur Verfügung, die verwendet werden können, um workload-spezifische Metriken und change-in-demand Prozesse zu definieren und Techniken des maschinellen Lernens anzuwenden, unabhängig von ML-Kenntnissen.

Zudem können Sie auch all Ihre externen Endpunkte überwachen, um sicherzustellen, dass diese von Ihrer Basisimplementierung unabhängig sind. Diese aktive Überwachung kann anhand von synthetischen Transaktionen erfolgen (auch Benutzer-Canaries genannt, jedoch nicht zu verwechseln mit Canary-Bereitstellungen). Diese führen regelmäßig eine Reihe gängiger Aufgaben aus, die mit Aktionen übereinstimmen, die von Clients der Workload durchgeführt werden. Diese Aufgaben sollten nicht zu lang sein und Sie sollten darauf achten, Ihre Workload beim Testen nicht zu überlasten. Mit Amazon CloudWatch Synthetics können Sie [synthetische Kanarienvögel erstellen](#), um Ihre Endgeräte zu überwachen und. APIs Sie können die synthetischen Canary-Client-Knoten auch mit der AWS X-Ray -Konsole kombinieren, um zu bestimmen, bei welchen synthetischen Canaries im ausgewählten Zeitraum Probleme mit Fehlern, Störungen oder Drosselungsraten auftreten.

Gewünschtes Ergebnis:

Erfassen und Nutzen kritischer Metriken aus allen Komponenten der Workload, um die Workload-Zuverlässigkeit und eine optimale Benutzererfahrung sicherzustellen. Wenn Sie erkennen, dass mit einem Workload keine Geschäftsergebnisse erzielt werden, können Sie schnell einen Systemausfall deklarieren und das System nach einem Vorfall wiederzustellen.

Typische Anti-Muster:

- Es werden nur externe Schnittstellen zum Workload überwacht.
- Generieren Sie keine workload-spezifischen Metriken und verlassen Sie sich nur auf Metriken, die Ihnen von den Services zur Verfügung gestellt werden, die AWS Ihr Workload nutzt.
- Verwenden Sie in Ihrem Workload nur technische Kennzahlen und überwachen Sie keine Metriken, die sich auf nicht technische Daten beziehen, zu denen KPIs der Workload beiträgt.
- Sie verlassen sich auf den Produktionsdatenverkehr und einfache Zustandsprüfungen für die Überwachung und Bewertung des Workload-Status.

Vorteile der Nutzung dieser bewährten Methode: Durch die Überwachung aller Ebenen Ihrer Workload können Sie Probleme in den darin enthaltenen Komponenten schneller vorhersehen und beheben.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Hoch

## Implementierungsleitfaden

1. Aktivieren Sie die Protokollierung, wann immer verfügbar. Von allen Workload-Komponenten sollten Überwachungsdaten erzielt werden. Aktivieren Sie eine zusätzliche Protokollierung, wie etwa S3 Access Logs, und ermöglichen Sie es Ihrer Workload, die workload-spezifischen Daten zu protokollieren. Erfassen Sie Metriken für CPU Netzwerk-I/O und Festplatten-I/O-Durchschnittswerte von Diensten wie Amazon ECSEKS, AmazonEC2, Elastic Load Balancing und AmazonEMR. AWS Auto Scaling Eine Liste der [AWS Services, für die CloudWatch Metriken veröffentlicht](#) werden, finden Sie unter AWS Services, die Metriken veröffentlichen CloudWatch.
2. Sehen Sie sich alle Standardmetriken an, um mehr über mögliche Datenerfassungslücken zu erfahren. Jeder Service generiert Standardmetriken. Durch die Erfassung von Standardmetriken erhalten Sie ein besseres Verständnis über die Abhängigkeiten zwischen Workload-Komponenten und darüber, wie die Komponentenzuverlässigkeit und -leistung die Workload beeinträchtigen. Sie können auch [Ihre eigenen Metriken erstellen und veröffentlichen](#), CloudWatch indem Sie das AWS CLI oder ein verwendenAPI.
3. Bewerten Sie alle Metriken, um zu entscheiden, bei welchen AWS Services in Ihrem Workload eine Warnung angezeigt werden soll. Sie können eine Metriken-Untergruppe auswählen, die eine höhere Auswirkung auf die Workload-Zuverlässigkeit hat. Wenn Sie sich auf kritische Metriken und Schwellenwerte konzentrieren, können Sie die Anzahl an [Warnmeldungen](#) genauer definieren und so Falschmeldungen reduzieren.
4. Definieren Sie Warnungen und den Wiederherstellungsprozess für Ihre Workload nach dem Auslösen der Warnmeldung. Durch die Definition von Warnmeldungen können Sie schnell Benachrichtigungen senden, eskalieren und die erforderlichen Schritte ausführen, um sich nach einem Vorfall zu erholen und Ihr vorgeschriebenes Wiederherstellungszeitziel (RTO) zu erreichen. Sie können [Amazon CloudWatch Alarms](#) verwenden, um automatisierte Workflows aufzurufen und Wiederherstellungsverfahren auf der Grundlage definierter Schwellenwerte einzuleiten.
5. Erfahren Sie mehr über die Verwendung von synthetischen Transaktionen für das Erfassen relevanter Daten zum Workload-Status. Die synthetische Überwachung folgt denselben Routen und führt dieselben Aktionen aus wie ein Kunde. Dadurch haben Sie die Möglichkeit, die Kundenerfahrung kontinuierlich zu überprüfen, selbst, wenn Sie keinen Kundendatenverkehr auf Ihren Workloads haben. Durch die Verwendung von [synthetischen Transaktionen](#) können Sie Probleme erkennen, bevor Ihre Kunden dies tun.

## Ressourcen

### Zugehörige bewährte Methoden:

- [REL11-BP03 Automatisieren Sie die Heilung auf allen Ebenen](#)

### Zugehörige Dokumente:

- [Erste Schritte mit Ihrem AWS Health Dashboard — Ihr Kontostatus](#)
- [AWS Dienste, die CloudWatch Metriken veröffentlichen](#)
- [Access Logs for Your Network Load Balancer](#)
- [Access logs for your application load balancer](#)
- [Zugreifen auf Amazon CloudWatch Logs für AWS Lambda](#)
- [Amazon-S3-Server-Zugriffsprotokollierung](#)
- [Enable Access Logs for Your Classic Load Balancer](#)
- [Exporting log data to Amazon S3](#)
- [Installieren Sie den CloudWatch Agenten auf einer EC2 Amazon-Instance](#)
- [Veröffentlichen von benutzerdefinierten Metriken](#)
- [Verwenden von CloudWatch Amazon-Dashboards](#)
- [Amazon CloudWatch Metrics verwenden](#)
- [Kanaren verwenden \(Amazon CloudWatch Synthetics\)](#)
- [Was sind Amazon CloudWatch Logs?](#)

### Benutzerhandbücher:

- [Creating a trail](#)
- [Überwachung von Speicher- und Festplattenmetriken für Amazon EC2 Linux-Instances](#)
- [Verwendung von CloudWatch Protokollen mit Container-Instances](#)
- [VPC-Flow-Protokolle](#)
- [Was ist Amazon DevOps Guru?](#)
- [Was ist AWS X-Ray?](#)

### Verwandte Blogs:



- [Debuggen mit Amazon CloudWatch Synthetics und AWS X-Ray](#)

Verwandte Beispiele und Workshops:

- [AWS Well-Architected Labs: Operational Excellence - Dependency Monitoring](#)
- [The Amazon Builders' Library: Instrumentieren verteilter Systeme für Einblicke in die Betriebsabläufe](#)
- [Workshop zur Beobachtbarkeit](#)

## REL06-BP02 Metriken definieren und berechnen (Aggregation)

Speichern Sie Protokolldaten und wenden Sie gegebenenfalls Filter an, um Metriken zu berechnen. Dazu gehören z. B. die Anzahl eines bestimmten Protokollereignisses oder die Latenz, die aus den Zeitstempeln des Protokollereignisses berechnet wird.

Amazon CloudWatch und Amazon S3 dienen als primäre Aggregations- und Speicherebenen. Für einige Dienste, wie AWS Auto Scaling Elastic Load Balancing, werden standardmäßig Standardmetriken für die CPU Last oder die durchschnittliche Anforderungslatenz in einem Cluster oder einer Instance bereitgestellt. Bei Streaming-Diensten wie VPC Flow Logs und werden Ereignisdaten an CloudWatch Logs weitergeleitet AWS CloudTrail, und Sie müssen Metrikfilter definieren und anwenden, um Metriken aus den Ereignisdaten zu extrahieren. Auf diese Weise erhalten Sie Zeitreihendaten, die als Eingaben für CloudWatch Alarme dienen können, die Sie zum Auslösen von Alarmen definieren.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Hoch

### Implementierungsleitfaden

- Definieren und Berechnen von Metriken (Aggregation) Speichern Sie Protokolldaten und wenden Sie gegebenenfalls Filter an, um Metriken zu berechnen. Dazu gehören z. B. die Anzahl eines bestimmten Protokollereignisses oder die Latenz, die aus den Zeitstempeln des Protokollereignisses berechnet wird.
  - Metrische Filter definieren die Begriffe und Muster, nach denen in Protokolldaten gesucht werden muss, wenn sie an CloudWatch Logs gesendet werden. CloudWatch Logs verwendet diese Metrikfilter, um Protokolldaten in numerische CloudWatch Messwerte umzuwandeln, die Sie grafisch darstellen oder einen Alarm auslösen können.
- [Suchen und Filtern von Protokolldaten](#)

- Verwenden Sie einen vertrauenswürdigen Drittanbieter für die Protokollaggregation.
- Befolgen Sie die Anweisungen des Drittanbieters. Die meisten Produkte von Drittanbietern lassen sich CloudWatch in Amazon S3 integrieren.
- Einige AWS Dienste können Protokolle direkt in Amazon S3 veröffentlichen. Wenn die Speicherung von Protokollen in Amazon S3 die wichtigste Anforderung ist, kann der Protokoll-Service die Protokolle direkt an Amazon S3 senden, ohne dass eine zusätzliche Infrastruktur eingerichtet werden muss.
  - [Senden von Protokollen direkt an Amazon S3](#)

## Ressourcen

### Zugehörige Dokumente:

- [Beispielabfragen für Amazon CloudWatch Logs Insights](#)
- [Debuggen mit Amazon CloudWatch Synthetics und AWS X-Ray](#)
- [Workshop zur Beobachtbarkeit](#)
- [Suchen und Filtern von Protokolldaten](#)
- [Senden von Protokollen direkt an Amazon S3](#)
- [Die Amazon Builders' Library: Verteilte Systeme instrumentieren, um betriebliche Transparenz zu erzielen](#)

## REL06-BP03 Benachrichtigungen senden (Verarbeitung und Alarmierung in Echtzeit)

Wenn Organisationen potenzielle Probleme erkennen, senden sie Benachrichtigungen und Warnungen in Echtzeit an das entsprechende Personal und die entsprechenden Systeme, um schnell und effektiv auf diese Probleme reagieren zu können.

Gewünschtes Ergebnis: Durch die Konfiguration relevanter Alarme auf der Grundlage von Service- und Anwendungsmetriken ist eine schnelle Reaktion auf operative Ereignisse möglich. Bei Überschreitung der Alarmschwellen werden das entsprechende Personal und die entsprechenden Systeme benachrichtigt, damit sie die zugrunde liegenden Probleme beseitigen können.

### Typische Anti-Muster:

- Sie konfigurieren Alarme mit einem übermäßig hohen Schwellenwert, was dazu führt, dass wichtige Benachrichtigungen nicht gesendet werden können.

- Sie konfigurieren Alarme mit einem zu niedrigen Schwellenwert, was dazu führt, dass bei wichtigen Warnungen aufgrund des Lärms übermäßiger Benachrichtigungen keine Aktion erfolgt.
- Sie aktualisieren keine Alarme und ihre Schwellenwerte, wenn sich die Nutzung ändert.
- Bei Alarmen, die am besten durch automatische Aktionen behoben werden, führt das Senden der Benachrichtigung an das Personal, anstatt die automatische Aktion zu generieren, dazu, dass übermäßig viele Benachrichtigungen gesendet werden.

Vorteile der Nutzung dieser bewährten Methode: Das Senden von Benachrichtigungen und Warnungen in Echtzeit an das entsprechende Personal und die entsprechenden Systeme ermöglicht eine frühzeitige Erkennung von Problemen und eine schnelle Reaktion auf betriebliche Vorfälle.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Hoch

### Implementierungsleitfaden

Workloads sollten mit der Verarbeitung und Benachrichtigung in Echtzeit ausgestattet sein, um die Erkennbarkeit von Problemen zu verbessern, die sich auf die Verfügbarkeit der Anwendung auswirken und als Auslöser für automatische Reaktionen dienen könnten. Organisationen können die Verarbeitung und Benachrichtigung in Echtzeit durchführen, indem sie Warnungen mit definierten Metriken erstellen, um Benachrichtigungen zu erhalten, wenn wichtige Ereignisse eintreten oder eine Metrik einen Schwellenwert überschreitet.

[Amazon CloudWatch](#) ermöglicht es Ihnen, [metrische](#) und zusammengesetzte CloudWatch Alarme mithilfe von Alarmen zu erstellen, die auf statischen Schwellenwerten, Anomalieerkennung und anderen Kriterien basieren. Weitere Informationen zu den Alarmtypen, die Sie verwenden können CloudWatch, finden Sie im [Abschnitt Alarme der CloudWatch Dokumentation](#).

Mithilfe von [CloudWatch Dashboards](#) können Sie benutzerdefinierte Ansichten der Kennzahlen und Benachrichtigungen Ihrer AWS Ressourcen für Ihre Teams erstellen. Die anpassbaren Homepages in der CloudWatch Konsole ermöglichen es Ihnen, Ihre Ressourcen in einer einzigen Ansicht über mehrere Regionen hinweg zu überwachen.

Alarme können eine oder mehrere Aktionen ausführen, z. B. das Senden einer Benachrichtigung an ein [SNSAmazon-Thema](#), das Ausführen einer [EC2Amazon-Aktion oder einer Amazon EC2 Auto Scaling Scaling-Aktion](#) oder das [Erstellen eines OpsItem Oder-Vorfalls](#) in AWS Systems Manager.

Amazon CloudWatch verwendet [Amazon SNS](#), um Benachrichtigungen zu senden, wenn sich der Status des Alarms ändert, und ermöglicht die Nachrichtenzustellung von den Herausgebern

(Produzenten) an die Abonnenten (Verbraucher). Weitere Informationen zur Einrichtung von SNS Amazon-Benachrichtigungen finden Sie unter [Amazon konfigurieren SNS](#).

CloudWatch sendet [EventBridgeEreignisse](#), wenn ein CloudWatch Alarm erstellt, aktualisiert, gelöscht wird oder sich sein Status ändert. Sie können diese Ereignisse verwenden EventBridge, um Regeln zu erstellen, die Aktionen ausführen, z. B. Sie benachrichtigen, wenn sich der Status eines Alarms ändert, oder mithilfe der [Systems Manager Manager-Automatisierung](#) automatisch Ereignisse in Ihrem Konto auslösen.

Wann sollten Sie Amazon verwenden EventBridge SNS?

EventBridge Sowohl Amazon als auch Amazon SNS können zur Entwicklung ereignisgesteuerter Anwendungen verwendet werden, und Ihre Wahl hängt von Ihren spezifischen Anforderungen ab.

Amazon EventBridge wird empfohlen, wenn Sie eine Anwendung erstellen möchten, die auf Ereignisse aus Ihren eigenen Anwendungen, SaaS-Anwendungen und AWS Diensten reagiert. EventBridge ist der einzige ereignisbasierte Dienst, der direkt mit SaaS-Partnern von Drittanbietern integriert werden kann. EventBridge nimmt außerdem automatisch Ereignisse von über 200 AWS Diensten auf, ohne dass Entwickler Ressourcen in ihrem Konto erstellen müssen.

EventBridge verwendet eine definierte Struktur JSON für Ereignisse und hilft Ihnen bei der Erstellung von Regeln, die auf den gesamten Veranstaltungstext angewendet werden, um Ereignisse auszuwählen, die an ein [Ziel](#) weitergeleitet werden sollen. EventBridge unterstützt derzeit über 20 AWS Dienste als Ziele, darunter [Amazon AWS Lambda](#), Amazon SQSSNS, [Amazon Kinesis Data Streams](#) und [Amazon Data Firehose](#).

Amazon SNS wird für Anwendungen empfohlen, die eine hohe Lüfterleistung benötigen (Tausende oder Millionen von Endpunkten). Ein übliches Muster, das wir beobachten, ist, dass Kunden Amazon SNS als Ziel für ihre Regel verwenden, um die Ereignisse zu filtern, die sie benötigen, und sich dann auf mehrere Endpunkte ausbreiten.

Nachrichten sind unstrukturiert und können in jedem Format vorliegen. Amazon SNS unterstützt die Weiterleitung von Nachrichten an sechs verschiedene Arten von Zielen, darunter Lambda-, Amazon-SQS, HTTP /S-EndpunkteSMS, Mobile Push und E-Mail. Die SNS [typische Latenz von Amazon liegt unter 30 Millisekunden](#). Eine Vielzahl von AWS Diensten sendet SNS Amazon-Nachrichten, indem sie den Dienst entsprechend konfigurieren (mehr als 30, darunter AmazonEC2, [Amazon S3](#) und [Amazon RDS](#)).

Implementierungsschritte

1. Erstellen Sie einen Alarm mithilfe von [CloudWatch Amazon-Alarmen](#).

- a. Ein metrischer Alarm überwacht eine einzelne CloudWatch Metrik oder einen Ausdruck, der von CloudWatch Metriken abhängt. Der Alarm initiiert eine oder mehrere Aktionen auf der Grundlage des Werts der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert über eine Reihe von Zeitintervallen. Die Aktion kann darin bestehen, eine Benachrichtigung an ein [SNSAmazon-Thema](#) zu senden, eine [EC2Amazon-Aktion](#) oder eine [Amazon EC2 Auto Scaling Scaling-Aktion](#) durchzuführen OpsItem oder [einen OR-Vorfall in zu erstellen](#) AWS Systems Manager.
  - b. Ein zusammengesetzter Alarm besteht aus einem Regelausdruck, der die Alarmbedingungen anderer von Ihnen erstellter Alarme berücksichtigt. Der zusammengesetzte Alarm wechselt nur dann in den Alarmstatus, wenn alle Regelbedingungen erfüllt sind. Die im Regelausdruck eines zusammengesetzten Alarms angegebenen Alarme können metrische Alarme und zusätzliche zusammengesetzte Alarme enthalten. Zusammengesetzte Alarme können SNS Amazon-Benachrichtigungen senden, wenn sich ihr Status ändert, und sie können Systems Manager [OpsItems](#) oder [Incidents](#) auslösen, wenn sie in den Alarmzustand wechseln, aber sie können keine Amazon EC2 - oder Auto Scaling Scaling-Aktionen ausführen.
2. Richten Sie [SNSAmazon-Benachrichtigungen](#) ein. Wenn Sie einen CloudWatch Alarm erstellen, können Sie ein SNS Amazon-Thema hinzufügen, um eine Benachrichtigung zu senden, wenn sich der Status des Alarms ändert.
  3. [Erstellen Sie Regeln EventBridge](#), die bestimmten CloudWatch Alarmen entsprechen. Jede Regel unterstützt mehrere Ziele, einschließlich Lambda-Funktionen. Sie können beispielsweise einen Alarm definieren, der ausgelöst wird, wenn der verfügbare Speicherplatz knapp wird, wodurch über eine EventBridge Regel eine Lambda-Funktion ausgelöst wird, um den Speicherplatz zu bereinigen. [Weitere Informationen zu Zielen finden Sie unter EventBridge EventBridge Ziele.](#)

## Ressourcen

Zugehörige bewährte Methoden für Well-Architected:

- [REL06-BP01 Alle Komponenten für den Workload überwachen \(Generation\)](#)
- [REL06-BP02 Metriken definieren und berechnen \(Aggregation\)](#)
- [REL12-BP01 Verwenden Sie Playbooks, um Fehler zu untersuchen](#)

Zugehörige Dokumente:

- [Amazon CloudWatch](#)
- [CloudWatch Protokolliert Einblicke](#)

- [CloudWatch Amazon-Alarme verwenden](#)
- [CloudWatch Amazon-Dashboards verwenden](#)
- [Verwenden von CloudWatch Amazon-Metriken](#)
- [SNSAmazon-Benachrichtigungen einrichten](#)
- [CloudWatch Erkennung von Anomalien](#)
- [CloudWatch Protokolliert den Datenschutz](#)
- [Amazon EventBridge](#)
- [Amazon Simple Notification Service](#)

Zugehörige Videos:

- [reinvent 2022 observability videos](#)
- [AWS re:Invent 2022 — Bewährte Methoden zur Beobachtbarkeit bei Amazon](#)

Zugehörige Beispiele:

- [Workshop zur Beobachtbarkeit](#)
- [Amazon EventBridge to AWS Lambda mit Feedback-Steuerung durch Amazon CloudWatch Alarms](#)

REL06-BP04 Automatisierte Antworten (Verarbeitung und Alarmierung in Echtzeit)

Automatisieren Sie bei Erkennung von Ereignissen die erforderlichen Maßnahmen, wie etwa den Austausch fehlerhafter Komponenten.

Die automatische Echtzeitverarbeitung von Alarmen ist implementiert, sodass die Systeme bei Auslösung von Alarmen schnell korrigierend eingreifen und versuchen können, Ausfälle oder Beeinträchtigungen des Services zu verhindern. Zu den automatisierten Reaktionen auf Alarme könnten der Austausch ausgefallener Komponenten, die Anpassung der Rechenkapazität, die Umleitung des Datenverkehrs auf fehlerfreie Hosts, Availability Zones oder andere Regionen sowie die Benachrichtigung der Betreiber gehören.

Gewünschtes Ergebnis: Alarme werden in Echtzeit erkannt, und die automatische Verarbeitung von Alarmen wird eingerichtet, um die entsprechenden Maßnahmen zur Einhaltung der Servicelevel-Ziele und Service-Level-Agreements einzuleiten (). SLAs Die Automatisierung kann von der Selbstreparatur einzelner Komponenten bis hin zum Failover eines ganzen Standorts reichen.

## Typische Anti-Muster:

- Fehlen einer genauen Bestandsaufnahme oder eines Katalogs der wichtigsten Echtzeitalarme
- Keine automatischen Reaktionen auf kritische Alarme (z. B. automatische Skalierung, wenn die Rechenkapazität fast erschöpft ist)
- Widersprüchliche Alarmreaktionen
- Es gibt keine Standardarbeitsanweisungen (SOPs), die Bediener befolgen müssen, wenn sie Warnmeldungen erhalten.
- Keine Überwachung von Konfigurationsänderungen, da unentdeckte Konfigurationsänderungen zu Ausfallzeiten bei Workloads führen können
- Keine Strategie, um unbeabsichtigte Konfigurationsänderungen rückgängig zu machen

Vorteile der Nutzung dieser bewährten Methode: Die Automatisierung der Alarmverarbeitung kann die Ausfallsicherheit des Systems verbessern. Das System ergreift automatisch Korrekturmaßnahmen und reduziert so manuelle Tätigkeiten, bei denen es zu einem menschlichen, fehleranfälligen Eingreifen kommen kann. Der Workload-Betrieb erfüllt die Verfügbarkeitsziele und reduziert Serviceunterbrechungen.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Mittel

## Implementierungsleitfaden

Zur wirksamen Verwaltung von Alarmen und zur Automatisierung ihrer Beantwortung kategorisieren Sie die Alarme nach ihrer Kritikalität und Auswirkung, dokumentieren die Reaktionsverfahren und planen die Reaktionen, bevor Sie die Aufgaben einordnen.

Ermitteln Sie Aufgaben, die bestimmte Aktionen erfordern (oft in Runbooks detailliert beschrieben), und untersuchen Sie alle Runbooks und Playbooks, um festzustellen, welche Aufgaben automatisiert werden können. Lassen sich Aktionen definieren, können sie oft auch automatisiert werden. Wenn Aktionen nicht automatisiert werden können, dokumentieren Sie die manuellen Schritte in einer SOP und schulen Sie die Bediener darin. Hinterfragen Sie kontinuierlich manuelle Prozesse und suchen Sie nach Möglichkeiten zur Automatisierung, um einen Plan für die Automatisierung von Alarmreaktionen zu erstellen und zu verwalten.

## Implementierungsschritte

1. Erstellen Sie ein Inventar von Alarmen: Um eine Liste aller Alarme zu erhalten, können Sie den CloudWatch Befehl [Amazon](#) verwenden [describe-alarms](#). [AWS CLI](#) Je nachdem, wie viele

Alarme Sie eingerichtet haben, müssen Sie möglicherweise die Paginierung verwenden, um eine Teilmenge von Alarmen für jeden Anruf abzurufen, oder Sie können den verwenden, AWS SDK um die Alarme [mithilfe eines API](#) Anrufs abzurufen.

2. Dokumentieren aller Alarmaktionen: Aktualisieren Sie ein Runbook mit allen Alarmen und ihren Aktionen, unabhängig davon, ob sie manuell oder automatisiert sind. [AWS Systems Manager](#) bietet vordefinierte Runbooks. Ausführliche Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter [Working with runbooks](#). Ausführliche Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter [View runbook content](#).
3. Alarmaktionen einrichten und verwalten: Geben Sie für alle Alarme, für die eine Aktion erforderlich ist, die [automatisierte Aktion mithilfe von](#) an. CloudWatch SDK Sie können beispielsweise den Status Ihrer EC2 Amazon-Instances auf der Grundlage eines CloudWatch Alarms automatisch ändern, indem Sie Aktionen für einen Alarm erstellen und aktivieren oder Aktionen für einen Alarm deaktivieren.

Sie können [Amazon](#) auch verwenden EventBridge, um automatisch auf Systemereignisse wie Probleme mit der Anwendungsverfügbarkeit oder Ressourcenänderungen zu reagieren. Sie können Regeln erstellen, um anzugeben, an welchen Ereignissen Sie interessiert sind, und welche Aktionen auszuführen sind, wenn ein Ereignis mit einer Regel übereinstimmt. [Zu den Aktionen, die automatisch initiiert werden können, gehören das Aufrufen einer AWS LambdaFunktion, das Aufrufen von Amazon EC2Run Command, das Weiterleiten des Ereignisses an Amazon Kinesis Data Streams und die Verwendung von Automate Amazon. EC2 EventBridge](#)

4. Standardarbeitsanweisungen (SOPs): [Basierend auf Ihren Anwendungskomponenten empfiehlt es sich, AWS Resilience Hubmehrere Vorlagen zu verwenden. SOP](#) Sie können diese verwendenSOPs, um alle Prozesse zu dokumentieren, die ein Bediener befolgen sollte, falls eine Warnung ausgelöst wird. Sie können auch [eine auf Resilience Hub-Empfehlungen SOP basierende Analyse erstellen](#), für die Sie eine Resilience Hub-Anwendung mit einer zugehörigen Resilienz-Richtlinie sowie eine historische Resilienzbewertung für diese Anwendung benötigen. Die Empfehlungen für Sie ergeben SOP sich aus der Resilienzbewertung.

Resilience Hub arbeitet mit Systems Manager zusammen, um Ihre Schritte zu automatisieren, SOPs indem es eine Reihe von [SSMDokumenten](#) bereitstellt, die Sie als Grundlage für diese verwenden könnenSOPs. Resilience Hub kann beispielsweise eine Empfehlung SOP für das Hinzufügen von Speicherplatz auf der Grundlage eines vorhandenen SSM Automatisierungsdokuments empfehlen.

5. Führen Sie automatisierte Aktionen mit Amazon DevOps Guru durch: Sie können [Amazon DevOps Guru](#) verwenden, um Anwendungsressourcen automatisch auf ungewöhnliches Verhalten zu



überwachen und gezielte Empfehlungen zu geben, um die Problemerkennung und -behebung zu beschleunigen. Mit DevOps Guru können Sie Ströme von Betriebsdaten nahezu in Echtzeit aus verschiedenen Quellen überwachen, darunter CloudWatch Amazon-Metriken [AWS Config](#), [AWS CloudFormation](#), und [AWS X-Ray](#). Sie können DevOps Guru auch verwenden, um Ereignisse automatisch zu erstellen OpsCenter und [OpsItems](#) an diese zu senden, [EventBridge um sie weiter zu automatisieren](#).

## Ressourcen

### Zugehörige bewährte Methoden:

- [REL06-BP01 Alle Komponenten für den Workload überwachen \(Generation\)](#)
- [REL06-BP02 Metriken definieren und berechnen \(Aggregation\)](#)
- [REL06-BP03 Benachrichtigungen senden \(Verarbeitung und Alarmierung in Echtzeit\)](#)
- [REL08-BP01 Verwenden Sie Runbooks für Standardaktivitäten wie die Bereitstellung](#)

### Zugehörige Dokumente:

- [AWS Systems Manager Automation](#)
- [Eine EventBridge Regel erstellen, die bei einem Ereignis aus einer AWS Ressource ausgelöst wird](#)
- [Workshop zur Beobachtbarkeit](#)
- [Die Amazon Builders' Library: Verteilte Systeme instrumentieren, um betriebliche Transparenz zu erzielen](#)
- [Was ist Amazon DevOps Guru?](#)
- [Working with Automation Documents \(Playbooks\)](#)

### Zugehörige Videos:

- [AWS re:Invent 2022 — Bewährte Methoden zur Beobachtbarkeit bei Amazon](#)
- [AWS re:Invent 2020: Automatisieren Sie alles mit AWS Systems Manager](#)
- [Einführung in AWS Resilience Hub](#)
- [Erstellen Sie benutzerdefinierte Ticketsysteme für Amazon DevOps Guru-Benachrichtigungen](#)
- [Aktivieren Sie die Aggregation von Erkenntnissen für mehrere Konten mit Amazon Guru DevOps](#)

## Zugehörige Beispiele:

- [Workshops zur Zuverlässigkeit](#)
- [Workshop für Amazon CloudWatch und Systems Manager](#)

### REL06-BP05 Logs analysieren

Erfassen Sie Protokolldateien und Metrikverläufe und analysieren Sie diese, um allgemeine Trends zu erkennen und Workload-Einblicke zu erhalten.

Amazon CloudWatch Logs Insights unterstützt eine [einfache, aber leistungsstarke Abfragesprache](#), mit der Sie Protokolldaten analysieren können. Amazon CloudWatch Logs unterstützt auch Abonnements, die einen nahtlosen Datenfluss zu Amazon S3 ermöglichen, wo Sie die Daten oder Amazon Athena verwenden können, um die Daten abzufragen. Abfragen für eine große Auswahl von Formaten werden ebenfalls unterstützt. Weitere Informationen finden Sie im Amazon Athena Benutzerhandbuch unter [Unterstützte Formate SerDes und Datenformate](#). Für die Analyse großer Protokolldateisätze können Sie einen EMR Amazon-Cluster ausführen, um Analysen im Petabyte-Bereich durchzuführen.

Es gibt eine Reihe von Tools, die von AWS Partnern und Drittanbietern bereitgestellt werden und die Aggregation, Verarbeitung, Speicherung und Analyse ermöglichen. Zu diesen Tools gehören New Relic, Splunk, Loggly, Logstash und Nagios. CloudHealth Die Generierung außerhalb von System- und Anwendungsprotokollen weicht jedoch bei jedem Cloud-Anbieter und häufig sogar bei den einzelnen Services ab.

Ein häufig übersehener Teil des Überwachungsprozesses ist die Datenverwaltung. Sie müssen Aufbewahrungsanforderungen für die Überwachung von Daten definieren und anschließend entsprechende Lebenszyklusrichtlinien anwenden. Amazon S3 unterstützt die Lebenszyklusverwaltung auf der Ebene von S3-Buckets. Diese Lebenszyklusverwaltung kann auf unterschiedliche Weise auf verschiedene Pfade im Bucket angewendet werden. Gegen Ende des Lebenszyklus können Sie die Daten zur Langzeitspeicherung an Amazon S3 Glacier übertragen und die Speicherung nach Ablauf des Aufbewahrungszeitraums beenden. Die S3 Intelligent-Tiering-Speicherkategorie wurde entwickelt, um die Kosten zu optimieren. Daten werden automatisch in die kostengünstigste Zugriffsstufe verschoben, ohne Auswirkungen auf die Leistung oder höheren Betriebsaufwand.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Mittel

## Implementierungsleitfaden

- CloudWatch Logs Insights ermöglicht es Ihnen, Ihre Protokolldaten in Amazon CloudWatch Logs interaktiv zu suchen und zu analysieren.
  - [Analysieren von Protokolldaten mit CloudWatch Logs Insights](#)
  - [Beispielabfragen für Amazon CloudWatch Logs Insights](#)
- Verwenden Sie Amazon CloudWatch Logs, um Protokolle an Amazon S3 zu senden, wo Sie die Daten oder Amazon Athena verwenden können, um die Daten abzufragen.
  - [Wie verwende ich Amazon Athena, um meine Amazon-S3-Serverzugriffsprotokolle zu analysieren?](#)
    - Erstellen Sie eine S3-Lebenszyklusrichtlinie für Ihren Bucket mit den Serverzugriffsprotokollen. Konfigurieren Sie die Richtlinie so, dass Protokolldateien regelmäßig entfernt werden. Dadurch wird die Menge der Daten reduziert, die Athena in einer Abfrage analysiert.
      - [How Do I Create a Lifecycle Policy for an S3 Bucket?](#)

## Ressourcen

### Zugehörige Dokumente:

- [Beispielabfragen für Amazon CloudWatch Logs Insights](#)
- [Analysieren von Protokolldaten mit CloudWatch Logs Insights](#)
- [Debuggen mit Amazon CloudWatch Synthetics und AWS X-Ray](#)
- [How Do I Create a Lifecycle Policy for an S3 Bucket?](#)
- [Wie verwende ich Amazon Athena, um meine Amazon-S3-Serverzugriffsprotokolle zu analysieren?](#)
- [Workshop zur Beobachtbarkeit](#)
- [Die Amazon Builders' Library: Verteilte Systeme instrumentieren, um betriebliche Transparenz zu erzielen](#)

## REL06-BP06 Regelmäßige Überprüfungen durchführen

Prüfen Sie regelmäßig, wie die Workload-Überwachung implementiert ist, und aktualisieren Sie sie auf Grundlage wichtiger Ereignissen und Änderungen.

Eine effektive Überwachung basiert auf wichtigen Geschäftsmetriken. Stellen Sie sicher, dass diese Metriken in Ihrem Workload berücksichtigt werden, wenn sich geschäftliche Prioritäten ändern.

Durch die Prüfung Ihrer Überwachung stellen Sie sicher, dass Sie wissen, wann eine Anwendung die eigenen Verfügbarkeitsziele erfüllt. Für die Durchführung von Ursachenanalysen ist es erforderlich, bei Ausfällen ermitteln zu können, was passiert ist. AWS bietet Services, mit denen Sie den Status Ihrer Services während eines Vorfalls nachverfolgen können:

- Amazon CloudWatch Logs: Sie können Ihre Protokolle in diesem Service speichern und deren Inhalt überprüfen.
- Amazon CloudWatch Logs Insights: Ist ein vollständig verwalteter Service, mit dem Sie umfangreiche Logs in Sekundenschnelle analysieren können. Es bietet Ihnen schnelle, interaktive Abfragen und Visualisierungen.
- AWS Config: Sie können sehen, welche AWS -Infrastruktur zu verschiedenen Zeitpunkten verwendet wurde.
- AWS CloudTrail: Sie können sehen, welche zu welchem Zeitpunkt und von welchem Principal aufgerufen AWS APIs wurden.

Bei führen wir ein wöchentliches Treffen durch AWS, um die [betriebliche Leistung zu überprüfen](#) und Erkenntnisse zwischen den Teams auszutauschen. Da es so viele Teams gibt AWS, haben wir [The Wheel entwickelt, um nach dem](#) Zufallsprinzip eine Arbeitslast auszuwählen, die überprüft werden soll. Der Aufbau einer Struktur mit regelmäßigen Überprüfungen der betrieblichen Leistung und mit Wissensaustausch verbessert Ihre Fähigkeit, höhere Leistungen bei Ihren Betriebsteams zu erzielen.

Typische Anti-Muster:

- Es werden nur Standardmetriken erfasst.
- Es wird eine Überwachungsstrategie festgelegt, aber nie überprüft.
- Bei Bereitstellung größerer Änderungen wird die Überwachung nicht erörtert.

Vorteile der Nutzung dieser bewährten Methode: Durch die regelmäßige Prüfung der Überwachung können Sie mögliche Probleme vorhersehen, statt nur zu reagieren, wenn ein Problem tatsächlich auftritt.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel

Implementierungsleitfaden

- Erstellen Sie mehrere Dashboards für den Workload. Ein übergeordnetes Dashboard mit den wichtigsten Geschäftsmetriken ist unverzichtbar. Es sollte zudem die technischen Metriken

enthalten, die Sie für den prognostizierten Zustand des Workloads bei variabler Nutzung als die relevantesten eingestuft haben. Dashboards für verschiedene Anwendungsebenen und Abhängigkeiten, die untersucht werden können, sind ebenfalls empfehlenswert.

- [Verwenden von CloudWatch Amazon-Dashboards](#)
- Planen und prüfen Sie die Workload-Dashboards regelmäßig. Führen Sie regelmäßige Untersuchungen der Dashboards durch. Was die Gründlichkeit der Untersuchungen angeht, sind unterschiedliche Intervalle denkbar.
  - Spüren Sie Trends in den Metriken auf. Vergleichen Sie die Metrikwerte mit Werten aus der Vergangenheit, um Trends zu erkennen, die darauf hinweisen könnten, dass etwas untersucht werden muss. Beispiele hierfür: ansteigende Latenz, Nachlassen der primären Geschäftsfunktion und zunehmende Anzahl von Reaktionen auf Fehler.
  - Spüren Sie Ausreißer/Anomalien in den Metriken auf. Ausreißer sind anhand von Durchschnitts- oder Mittelwerten oder Anomalien nicht unbedingt erkennbar. Sehen Sie sich die höchsten und niedrigsten Werte in einem bestimmten Zeitraum an und untersuchen Sie die Ursachen für die extremen Werte. Beseitigen Sie nach und nach die Ursachen und legen Sie dabei einen engeren Maßstab für die Definition von Extremwerten an. So können Sie die Beständigkeit der Workload-Leistung weiter erhöhen.
  - Spüren Sie plötzliche Änderungen im Verhalten auf. Eine plötzliche Veränderung in der Menge oder Richtung einer Metrik kann auf eine Änderung in der Anwendung hindeuten. Sie kann aber auch ein Hinweis auf externe Faktoren sein, für deren Verfolgung sie möglicherweise weitere Metriken hinzufügen müssen.

## Ressourcen

### Zugehörige Dokumente:

- [Beispielabfragen für Amazon CloudWatch Logs Insights](#)
- [Debuggen mit Amazon CloudWatch Synthetics und AWS X-Ray](#)
- [Workshop zur Beobachtbarkeit](#)
- [Die Amazon Builders' Library: Verteilte Systeme instrumentieren, um betriebliche Transparenz zu erzielen](#)
- [Verwenden von CloudWatch Amazon-Dashboards](#)

## REL06-BP07 Überwachen Sie die end-to-end Nachverfolgung von Anfragen durch Ihr System

Verfolgen Sie Anfragen während der Bearbeitung durch die Servicekomponenten, damit Produktteams Probleme einfacher analysieren und beheben und die Leistung verbessern können.

Gewünschtes Ergebnis: Workloads mit umfassender Ablaufverfolgung über alle Komponenten hinweg lassen sich leicht debuggen. Dadurch werden die [durchschnittliche Zeit bis zur Behebung](#) (MTTR) von Fehlern und die Latenz verbessert, da die Ursachenerkennung vereinfacht wird. End-to-endDie Ablaufverfolgung reduziert die Zeit, die benötigt wird, um betroffene Komponenten zu erkennen und die Ursachen von Fehlern oder Latenzen detailliert zu ermitteln.

Typische Anti-Muster:

- Nachverfolgung wird für einige Komponenten verwendet, aber nicht für alle. Ohne Rückverfolgung für können Teams beispielsweise die Latenz AWS Lambda, die durch Kaltstarts bei einer hohen Arbeitslast verursacht wird, möglicherweise nicht genau nachvollziehen.
- Synthetic Canaries oder die Überwachung realer Benutzer (RUM) sind nicht mit Tracing konfiguriert. Ohne Canaries oder RUM wird die Klienteninteraktionstelemetrie bei der Trace-Analyse nicht berücksichtigt, was zu einem unvollständigen Leistungsprofil führt.
- Hybride Workloads umfassen sowohl cloudnative Nachverfolgungs-Tools als auch Tools von Drittanbietern, es wurden jedoch keine Schritte unternommen, um eine einzige Nachverfolgungs-Lösung auszuwählen und vollständig zu integrieren. Je nach gewählter Tracing-Lösung SDKs sollte Cloud-natives Tracing zur Instrumentierung von Komponenten verwendet werden, bei denen es sich nicht um Cloud-native Komponenten handelt, oder Tools von Drittanbietern sollten so konfiguriert werden, dass sie Cloud-native Trace-Telemetrie aufnehmen.

Vorteile der Nutzung dieser bewährten Methode: Wenn Entwicklungsteams über Probleme informiert werden, können sie sich ein vollständiges Bild der Interaktionen zwischen den Systemkomponenten machen, einschließlich der Beziehung zwischen Komponenten, Protokollierung, Leistung und Ausfällen. Da die Nachverfolgung die visuelle Identifizierung der Ursachen erleichtert, können diese schneller untersucht werden. Teams, die die Interaktionen der Komponenten im Detail verstehen, treffen bessere und schnellere Entscheidungen bei der Lösung von Problemen. Entscheidungen, z. B. wann ein Notfallwiederherstellung (DR)-Failover eingeleitet werden sollte oder wo Strategien zur Selbstreparatur am besten implementiert werden sollten, können durch die Analyse von Systemprotokollen verbessert werden, was letztlich die Kundenzufriedenheit mit Ihren Services erhöht.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel

## Implementierungsleitfaden

Teams, die verteilte Anwendungen betreiben, können mithilfe von Nachverfolgungs-Tools eine Korrelationskennung einrichten, Spuren von Anfragen erfassen und Service-Maps für verbundene Komponenten erstellen. Alle Anwendungskomponenten sollten in den Anforderungsspuren enthalten sein, einschließlich Service-Clients, Middleware-Gateways und Event Busse, Rechenkomponenten und Speicher, einschließlich Schlüssel-Wert-Speicher und -Datenbanken. Integrieren Sie synthetische Kanarien und die Überwachung realer Benutzer in Ihre end-to-end Tracing-Konfiguration, um Kundeninteraktionen und Latenz aus der Ferne zu messen, sodass Sie die Leistung Ihres Systems anhand Ihrer Service Level Agreements und Ziele genau bewerten können.

Sie können die Instrumentierungsservices von [Amazon CloudWatch Application Monitoring](#) verwenden [AWS X-Ray](#), um einen vollständigen Überblick über die Anfragen zu erhalten, während sie Ihre Anwendung durchlaufen. X-Ray sammelt Anwendungstelemetrie und ermöglicht es Ihnen, sie nach Payloads, Funktionen, Traces und Diensten zu visualisieren und zu filtern. X-Ray kann für Systemkomponenten mit No-Code oder Low-Code aktiviert werden. APIs CloudWatch Die Anwendungsüberwachung umfasst ServiceLens die Integration Ihrer Traces mit Metriken, Protokollen und Alarmen. CloudWatch Die Anwendungsüberwachung umfasst auch synthetische Funktionen zur Überwachung Ihrer Endgeräte sowie die Überwachung von echten Benutzern zur Instrumentierung Ihrer Webanwendungsclients. APIs

### Implementierungsschritte

- Verwenden Sie es AWS X-Ray auf allen unterstützten nativen Diensten wie [Amazon S3](#) [und Amazon API Gateway](#). AWS Lambda Diese AWS Dienste ermöglichen X-Ray mit Konfigurationsumschaltern, die Infrastruktur als Code verwenden AWS SDKs, oder die AWS Management Console.
- Instrumentenanwendungen [AWS Distro for Open Telemetry und X-Ray](#) oder Erfassungs-Agenten von Drittanbietern.
- Im [AWS X-Ray -Entwicklerhandbuch](#) finden Sie weitere Informationen für die programmiersprachenspezifische Implementierung. In diesen Abschnitten der Dokumentation wird detailliert beschrieben, wie HTTP Anfragen, SQL Abfragen und andere Prozesse, die für Ihre Anwendungsprogrammiersprache spezifisch sind, instrumentiert werden.
- Verwenden Sie X-Ray Tracing für [Amazon CloudWatch Synthetic Canaries](#) und [Amazon CloudWatch RUM](#), um den Anforderungspfad von Ihrem Endbenutzer-Client durch Ihre nachgelagerte AWS Infrastruktur zu analysieren.

- Konfigurieren Sie CloudWatch Metriken und Alarme auf der Grundlage von Resource Health und Canary-Telemetrie, sodass Teams schnell auf Probleme aufmerksam gemacht werden und sich anschließend eingehend mit Traces und Service Maps befassen können. ServiceLens
- Aktivieren Sie die X-Ray-Integration für Nachverfolgungs-Tools von Drittanbietern wie [Datadog](#), [New Relic](#) oder [Dynatrace](#), wenn Sie Tools von Drittanbietern als primäre Nachverfolgungslösung verwenden.

## Ressourcen

### Zugehörige bewährte Methoden:

- [REL06-BP01 Alle Komponenten für den Workload überwachen \(Generation\)](#)
- [REL11-BP01 Überwachen Sie alle Komponenten des Workloads, um Fehler zu erkennen](#)

### Zugehörige Dokumente:

- [Was ist? AWS X-Ray](#)
- [Amazon CloudWatch: Anwendungsüberwachung](#)
- [Debuggen mit Amazon CloudWatch Synthetics und AWS X-Ray](#)
- [Die Amazon Builders' Library: Verteilte Systeme instrumentieren, um betriebliche Transparenz zu erzielen](#)
- [Integration AWS X-Ray mit anderen Diensten AWS](#)
- [AWS Distribution für und OpenTelemetry AWS X-Ray](#)
- [Amazon CloudWatch: Synthetisches Monitoring verwenden](#)
- [Amazon CloudWatch: Verwenden CloudWatch RUM](#)
- [Richten Sie Amazon CloudWatch Synthetics Canary und Amazon CloudWatch Alarm ein](#)
- [Verfügbarkeit und mehr: Verständnis und Verbesserung der Widerstandsfähigkeit verteilter Systeme auf AWS](#)

### Zugehörige Beispiele:

- [Workshop zur Beobachtbarkeit](#)

### Zugehörige Videos:



- [AWS re:Invent 2022 — Wie überwacht man Anwendungen für mehrere Konten](#)
- [Wie überwachen Sie Ihre Anwendungen AWS](#)

Zugehörige Tools:

- [AWS X-Ray](#)
- [Amazon CloudWatch](#)
- [Amazon Route 53](#)

REL7. Wie wird die Workload so gestaltet, dass sie sich an Veränderungen der Nachfrage anpasst?

Eine skalierbare Workload bietet Elastizität, sodass Ressourcen automatisch hinzugefügt oder entfernt werden können, damit sie dem aktuellen Bedarf zu einem bestimmten Zeitpunkt genau entsprechen.

Bewährte Methoden

- [REL07-BP01 Verwenden Sie Automatisierung bei der Beschaffung oder Skalierung von Ressourcen](#)
- [REL07-BP02 Besorgen Sie sich Ressourcen, wenn eine Beeinträchtigung der Arbeitsbelastung festgestellt wird](#)
- [REL07-BP03 Ressourcen abrufen, wenn festgestellt wird, dass mehr Ressourcen für einen Workload benötigt werden](#)
- [REL07-BP04 Belastungstest Ihr Workload](#)

REL07-BP01 Verwenden Sie Automatisierung bei der Beschaffung oder Skalierung von Ressourcen

Wenn Sie kaputte Ressourcen ersetzen oder Ihre Arbeitslast skalieren, automatisieren Sie den Prozess mithilfe von Managed AWS Services wie Amazon S3 und AWS Auto Scaling. Sie können auch Tools von Drittanbietern verwenden und AWS SDKs die Skalierung automatisieren.

Zu den verwalteten AWS Services gehören Amazon S3 CloudFront, Amazon AWS Auto Scaling, AWS Lambda, Amazon DynamoDB und Amazon Route 53. AWS Fargate

AWS Auto Scaling ermöglicht es Ihnen, beeinträchtigte Instanzen zu erkennen und zu ersetzen. [Außerdem können Sie damit Skalierungspläne für Ressourcen wie EC2-Amazon-Instances und Spot-](#)

## Flotten, ECSAmazon-Aufgaben, AmazonDynamoDB-Tabellen und -Indizes sowie Amazon Aurora Replicas erstellen.

Stellen Sie bei der Skalierung von EC2 Instances sicher, dass Sie mehrere Availability Zones (vorzugsweise mindestens drei) verwenden und Kapazität hinzufügen oder entfernen, um das Gleichgewicht zwischen diesen Availability Zones aufrechtzuerhalten. ECSAufgaben oder Kubernetes-Pods (bei Verwendung von Amazon Elastic Kubernetes Service) sollten ebenfalls auf mehrere Availability Zones verteilt werden.

Bei der Verwendung skalieren Instanzen AWS Lambda automatisch. Jedes Mal, wenn eine Ereignisbenachrichtigung für Ihre Funktion eingeht, wird AWS Lambda schnell nach freier Kapazität innerhalb der Rechenflotte gesucht und Ihr Code bis zur zugewiesenen Parallelität ausgeführt. Sie müssen sicherstellen, dass die erforderliche Gleichzeitigkeit auf dem spezifischen Lambda und in Ihrem Service Quotas konfiguriert ist.

Amazon S3 wird automatisch skaliert, um hohe Anfrageraten zu verarbeiten. Ihre Anwendung kann beispielsweise mindestens 3.500PUT//DELETEoder 5.500 COPY POSTGET//HEADAnfragen pro Sekunde pro Präfix in einem Bucket erreichen. Es gibt keine Einschränkungen für die Anzahl der Präfixe in einem Bucket. Sie können Ihre Lese- und Schreibleistung steigern, indem Sie Lesevorgänge parallelisieren. Wenn Sie beispielsweise 10 Präfixe in einem Amazon S3-Bucket für parallele Lesevorgänge einrichten, können Sie damit die Leseleistung auf 55 000 Leseanfragen pro Sekunde skalieren.

Konfigurieren und verwenden Sie Amazon CloudFront oder ein vertrauenswürdigen Content Delivery Network (CDN). A CDN kann schnellere Antwortzeiten für Endbenutzer bieten und Anfragen nach Inhalten aus dem Cache bearbeiten, sodass Sie Ihre Arbeitslast nicht skalieren müssen.

Typische Anti-Muster:

- Es werden Auto Scaling-Gruppen für die automatisierte Reparatur implementiert, aber keine Elastizität.
- Als Reaktion auf stark ansteigenden Datenverkehr wird automatisch skaliert.
- Es werden hochgradig zustandsbehaftete Anwendungen bereitgestellt, wodurch die Option der Elastizität entfällt.

Vorteile der Nutzung dieser bewährten Methode: Durch die Automatisierung entfällt die Gefahr manueller Fehler bei der Bereitstellung und Außerbetriebnahme von Ressourcen. Durch die Automatisierung entfällt das Risiko von Kostenüberschreitungen und Dienstverweigerungen (Denial

of Service) aufgrund der langsamen Reaktion auf Bedürfnisse bezüglich der Bereitstellung oder Außerbetriebnahme von Ressourcen.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Hoch

## Implementierungsleitfaden

- Konfigurieren und nutzen Sie AWS Auto Scaling. Hiermit erfolgt eine Überwachung der Anwendungen und eine automatische Anpassung der Kapazität, um eine stabile, vorhersehbare Leistung zu möglichst niedrigen Kosten aufrechtzuerhalten. Mit AWS Auto Scaling lässt sich die Anwendungsskalierung für mehrere Ressourcen in mehreren Services einrichten.
- [Was ist AWS Auto Scaling?](#)
  - Konfigurieren Sie Auto Scaling für Ihre EC2 Amazon-Instances und Spot-Flotten, ECS Amazon-Aufgaben, Amazon DynamoDB-Tabellen und -Indizes, Amazon Aurora Replicas und Appliances, sofern zutreffend. AWS Marketplace
  - [Automatische Verwaltung der Durchsatzkapazität mit DynamoDB-Auto-Scaling](#)
    - Verwenden Sie API Serviceoperationen, um Alarme, Skalierungsrichtlinien, Aufwärm- und Abkühlzeiten festzulegen.
- Nutzen Sie Elastic Load Balancing. Load Balancer können die Last nach Pfaden oder Netzwerkkonnektivität verteilen.
- [Was ist Elastic Load Balancing?](#)
  - Application Load Balancer können Lasten nach Pfaden verteilen.
  - [Was ist ein Application Load Balancer?](#)
    - Konfigurieren Sie einen Application Load Balancer, um Datenverkehr basierend auf dem Pfad unter dem Domain-Namen auf verschiedene Workloads zu verteilen.
    - Application Load Balancer können verwendet werden, um Lasten so zu verteilen, dass sie integriert werden können, um den Bedarf AWS Auto Scaling zu steuern.
      - [Nutzen eines Load Balancer mit einer Auto-Scaling-Gruppe](#)
  - Network Load Balancer können Lasten nach Verbindungen verteilen.
  - [Was ist ein Network Load Balancer?](#)
    - Konfigurieren Sie einen Network Load Balancer, um den Datenverkehr mithilfe von IP-Adressen auf verschiedene Workloads zu verteilen TCP, oder um einen konstanten Satz von IP-Adressen für Ihren Workload zu verwenden.
    - Network Load Balancer können verwendet werden, um Lasten so zu verteilen, dass sie integriert werden können, um den Bedarf AWS Auto Scaling zu steuern.

- Verwenden Sie einen DNS Anbieter mit hoher Verfügbarkeit. DNSNamen ermöglichen es Ihren Benutzern, Namen anstelle von IP-Adressen einzugeben, um auf Ihre Workloads zuzugreifen, und verteilen diese Informationen in einem definierten Bereich, in der Regel global für Benutzer der Workloads.
  - Verwenden Sie Amazon Route 53 oder einen vertrauenswürdigen DNS Anbieter.
    - [Was ist Amazon Route 53?](#)
  - Verwenden Sie Route 53, um Ihre CloudFront Verteilungen und Load Balancer zu verwalten.
    - Ermitteln Sie die zu verwaltenden Domänen und Subdomänen.
    - Erstellen Sie mithilfe von OR-Datensätzen die ALIAS entsprechenden Datensätze. CNAME
      - [Arbeiten mit Datensätzen](#)
- Verwenden Sie das AWS globale Netzwerk, um den Pfad von Ihren Benutzern zu Ihren Anwendungen zu optimieren. AWS Global Accelerator überwacht kontinuierlich den Zustand Ihrer Anwendungsendpunkte und leitet den Datenverkehr in weniger als 30 Sekunden an fehlerfreie Endpunkte weiter.
  - AWS Global Accelerator ist ein Service, der die Verfügbarkeit und Leistung Ihrer Anwendungen bei lokalen oder globalen Benutzern verbessert. Es stellt statische IP-Adressen bereit, die als fester Einstiegspunkt zu Ihren Anwendungsendpunkten in einer oder mehreren dienen AWS-Regionen, z. B. Ihren Application Load Balancers, Network Load Balancers oder Amazon-Instances. EC2
    - [Was ist AWS Global Accelerator?](#)
- Konfigurieren und verwenden Sie Amazon CloudFront oder ein vertrauenswürdiges Content Delivery Network (CDN). Ein Content Delivery Network kann Antwortzeiten für Endbenutzer verkürzen und Anfragen für Inhalte verarbeiten, die zu einer unnötigen Skalierung Ihrer Workloads führen könnten.
  - [Was ist Amazon CloudFront?](#)
    - Konfigurieren Sie CloudFront Amazon-Distributionen für Ihre Workloads oder verwenden Sie einen Drittanbieter. CDN
      - Sie können den Zugriff auf Ihre Workloads einschränken, sodass sie nur von dort aus zugänglich sind, CloudFront indem Sie die IP-Bereiche verwenden, die CloudFront in Ihren Endpunktsicherheitsgruppen oder Zugriffsrichtlinien angegeben sind.

## Ressourcen

### Zugehörige Dokumente:

Änderungsmanagement

- [APNPartner: Partner, die Ihnen bei der Erstellung automatisierter Rechenlösungen helfen können](#)
- [AWS Auto Scaling: Funktionsweise von Skalierungsplänen](#)
- [AWS Marketplace: Für Auto Scaling geeignete Produkte](#)
- [Automatische Verwaltung der Durchsatzkapazität mit DynamoDB-Auto-Scaling](#)
- [Nutzen eines Load Balancer mit einer Auto-Scaling-Gruppe](#)
- [Was ist AWS Global Accelerator?](#)
- [Was ist Amazon EC2 Auto Scaling?](#)
- [Was ist AWS Auto Scaling?](#)
- [Was ist Amazon CloudFront?](#)
- [Was ist Amazon Route 53?](#)
- [Was ist Elastic Load Balancing?](#)
- [Was ist ein Network Load Balancer?](#)
- [Was ist ein Application Load Balancer?](#)
- [Arbeiten mit Datensätzen](#)

REL07-BP02 Besorgen Sie sich Ressourcen, wenn eine Beeinträchtigung der Arbeitsbelastung festgestellt wird

Skalieren Sie Ressourcen bei Bedarf reaktiv, wenn die Verfügbarkeit beeinträchtigt ist, um die Verfügbarkeit der Workload wiederherzustellen.

Sie müssen zunächst Zustandsprüfungen und die Kriterien für diese Prüfungen konfigurieren, um anzugeben, wann die Verfügbarkeit durch fehlende Ressourcen beeinträchtigt wird. Benachrichtigen Sie anschließend entweder die zuständigen Mitarbeiter, um die Ressource manuell zu skalieren, oder starten Sie die Automatisierung, um sie automatisch zu skalieren.

Die Skalierung kann manuell an Ihre Arbeitslast angepasst werden (z. B. durch Ändern der Anzahl der EC2 Instances in einer Auto Scaling Scaling-Gruppe oder durch Ändern des Durchsatzes einer DynamoDB-Tabelle durch das AWS Management Console Oder AWS CLI). Wann immer es möglich ist, sollte jedoch Automatisierung eingesetzt werden (siehe Automatisiertes Abrufen oder Skalieren von Ressourcen).

Gewünschtes Ergebnis: Skalierungsaktivitäten (entweder automatisch oder manuell) werden eingeleitet, um die Verfügbarkeit wiederherzustellen, sobald ein Ausfall oder eine Verschlechterung der Kundenerfahrung festgestellt wird.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel

## Implementierungsleitfaden

Implementieren Sie Beobachtbarkeit und Überwachung für alle Komponenten Ihres Workloads, um die Kundenerfahrung zu überwachen und Fehler zu erkennen. Definieren Sie die manuellen oder automatisierten Verfahren, mit denen die erforderlichen Ressourcen skaliert werden. o Weitere Informationen finden Sie unter [REL11-BP01 Alle Komponenten des Workloads überwachen](#), um Fehler zu erkennen.

## Implementierungsschritte

- Definieren Sie die manuellen oder automatisierten Verfahren, mit denen die erforderlichen Ressourcen skaliert werden.
- Die Skalierungsverfahren hängen davon ab, wie die verschiedenen Komponenten innerhalb Ihres Workloads gestaltet sind.
- Die Skalierungsverfahren variieren auch je nach der zugrunde liegenden Technologie, die verwendet wird.
- Die verwendeten Komponenten AWS Auto Scaling können Skalierungspläne verwenden, um eine Reihe von Anweisungen für die Skalierung Ihrer Ressourcen zu konfigurieren. Wenn Sie mit AWS Ressourcen arbeiten AWS CloudFormation oder ihnen Tags hinzufügen, können Sie Skalierungspläne für verschiedene Ressourcengruppen pro Anwendung einrichten. Auto Scaling bietet Empfehlungen für Skalierungsstrategien, die auf die einzelnen Ressourcen zugeschnitten sind. Nachdem Sie einen Skalierungsplan erstellt haben, kombiniert Auto Scaling zur Unterstützung Ihrer Skalierungsstrategie Methoden für die dynamische und prädiktive Skalierung. Weitere Informationen finden Sie unter [Funktionsweise von Skalierungsplänen](#).
- Amazon EC2 Auto Scaling überprüft, ob Ihnen die richtige Anzahl von EC2 Amazon-Instances zur Verfügung steht, um die Last für Ihre Anwendung zu bewältigen. Sie erstellen Sammlungen von EC2 Instances, die als Auto Scaling Scaling-Gruppen bezeichnet werden. Sie können die Mindest- und Höchstanzahl von Instances in jeder Auto Scaling-Gruppe angeben, und Amazon EC2 Auto Scaling stellt sicher, dass Ihre Gruppe diese Grenzwerte niemals unter- oder überschreitet. Weitere Informationen finden Sie unter [Was ist Amazon EC2 Auto Scaling?](#)
- Amazon DynamoDB-Auto-Scaling verwendet den -Application-Auto-Scaling-Service, um die bereitgestellte Durchsatzkapazität in Ihrem Namen als Reaktion auf tatsächliche Datenverkehrsmuster dynamisch anzupassen. Auf diese Weise kann eine Tabelle oder ein

globaler sekundärer Index die bereitgestellte Lese- und Schreibkapazität zum Verarbeiten eines plötzlichen Datenverkehrsanstiegs ohne Drosselung erhöhen. Weitere Informationen finden Sie unter [Automatische Verwaltung der Durchsatzkapazität mit DynamoDB-Auto-Scaling](#).

## Ressourcen

Zugehörige bewährte Methoden:

- [REL07-BP01 Verwenden Sie Automatisierung bei der Beschaffung oder Skalierung von Ressourcen](#)
- [REL11-BP01 Überwachen Sie alle Komponenten des Workloads, um Fehler zu erkennen](#)

Zugehörige Dokumente:

- [AWS Auto Scaling: Funktionsweise von Skalierungsplänen](#)
- [Automatische Verwaltung der Durchsatzkapazität mit DynamoDB-Auto-Scaling](#)
- [Was ist Amazon EC2 Auto Scaling?](#)

REL07-BP03 Ressourcen abrufen, wenn festgestellt wird, dass mehr Ressourcen für einen Workload benötigt werden

Skalieren Sie Ressourcen proaktiv, um den Bedarf zu erfüllen und Auswirkungen auf die Verfügbarkeit zu vermeiden.

Viele AWS Dienste werden automatisch skaliert, um der Nachfrage gerecht zu werden. Wenn Sie EC2 Amazon-Instances oder ECS Amazon-Cluster verwenden, können Sie deren automatische Skalierung so konfigurieren, dass sie auf der Grundlage von Nutzungsmetriken erfolgt, die der Nachfrage nach Ihrer Workload entsprechen. Bei Amazon EC2 können die durchschnittliche CPU Auslastung, die Anzahl der Load Balancer-Anfragen oder die Netzwerkbandbreite verwendet werden, um EC2 Instances zu skalieren (oder zu skalieren). Bei Amazon ECS können die durchschnittliche CPU Auslastung, die Anzahl der Load Balancer-Anfragen und die Speicherauslastung verwendet werden, um ECS Aufgaben zu skalieren (oder zu skalieren). Wenn Target Auto Scaling aktiviert ist AWS, verhält sich der Autoscaler wie ein Haushaltsthermostat. Er fügt Ressourcen hinzu oder entfernt sie, um den von Ihnen angegebenen Zielwert (z. B. 70% CPU Auslastung) beizubehalten.

Amazon EC2 Auto Scaling kann auch [Predictive Auto Scaling](#) durchführen, bei dem maschinelles Lernen verwendet wird, um die historische Arbeitslast jeder Ressource zu analysieren und regelmäßig die future Auslastung zu prognostizieren.

Little's Law hilft bei der Berechnung, wie viele EC2 Recheninstanzen (Instanzen, gleichzeitige Lambda-Funktionen usw.) Sie benötigen.

$$L = \lambda W$$

L = Anzahl der Instances (oder mittlere Gleichzeitigkeit im System)

$\lambda$  = mittlere Rate des Eingangs von Anfragen (Anfrage/Sekunde)

W = mittlere Zeit, die jede Anfrage im System verbringt (Sekunden)

Wenn beispielsweise bei 100 RPS die Verarbeitung jeder Anfrage 0,5 Sekunden dauert, benötigen Sie 50 Instances, um mit dem Bedarf Schritt zu halten.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel

#### Implementierungsleitfaden

- Rufen Sie Ressourcen ab, wenn Sie feststellen, dass für eine Workload mehr Ressourcen benötigt werden. Skalieren Sie Ressourcen proaktiv, um den Bedarf zu erfüllen und Auswirkungen auf die Verfügbarkeit zu vermeiden.
  - Berechnen Sie, wie viele Rechenressourcen Sie benötigen (Gleichzeitigkeit der Datenverarbeitung), um eine bestimmte Anfragerate zu verarbeiten.
    - [Berichte über das Gesetz von Little](#)
  - Wenn Sie ein historisches Nutzungsmuster haben, richten Sie die geplante Skalierung für Amazon EC2 Auto Scaling ein.
    - [Geplante Skalierung für Amazon EC2 Auto Scaling](#)
  - Verwenden Sie AWS vorausschauende Skalierung.
    - [Vorausschauende Skalierung für Amazon EC2 Auto Scaling](#)

#### Ressourcen

#### Zugehörige Dokumente:

- [AWS Marketplace: Für Auto Scaling geeignete Produkte](#)



- [Automatische Verwaltung der Durchsatzkapazität mit DynamoDB-Auto-Scaling](#)
- [Prädiktive Skalierung für EC2, unterstützt durch Machine Learning](#)
- [Geplante Skalierung für Amazon EC2 Auto Scaling](#)
- [Berichte über das Gesetz von Little](#)
- [Was ist Amazon EC2 Auto Scaling?](#)

## REL07-BP04 Belastungstest Ihr Workload

Messen Sie anhand von Lasttests, ob die Skalierung den Workload-Anforderungen gerecht wird.

Es ist wichtig, regelmäßige Lasttests durchzuführen. Auslastungstests sollten die Belastungsgrenze ermitteln und die Leistung Ihres Workloads testen. AWS macht es einfach, temporäre Testumgebungen einzurichten, die den Umfang Ihrer Produktionslast modellieren. 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 On-Premises-Standort hätten.

Lasttests in der Produktion sollten auch im Rahmen von Ernstfallübungen durchgeführt werden, bei denen das Produktionssystem in einem Zeitraum mit geringer Kundennutzung stark belastet wird. Alle Mitarbeiter sollten an dieser Übung beteiligt sein, die Ergebnisse gemeinsam interpretieren und auftretende Probleme beheben.

Typische Anti-Muster:

- Es werden Lasttests für Bereitstellungen durchgeführt, die nicht mit der Konfiguration der Produktionsumgebung übereinstimmen.
- Lasttests werden nur für einzelne Teile, nicht aber für den gesamten Workload durchgeführt.
- Es werden Lasttests mit einer Teilmenge von Anfragen durchgeführt, aber nicht mit einer repräsentativen Gruppe tatsächlicher Anfragen.
- Es werden Lasttests mit einem kleinen Sicherheitsfaktor durchgeführt, der über der erwarteten Last liegt.

Vorteile der Nutzung dieser bewährten Methode: Sie wissen, welche Komponenten in der Architektur unter Last ausfallen, und können die zu überwachenden Metriken festlegen, die rechtzeitig auf die Annäherung an die Belastungsgrenze hinweisen, damit Sie das Problem beheben und entsprechende Auswirkungen vermeiden können.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel

### Implementierungsleitfaden

- Bestimmen Sie anhand von Lasttests, welcher Aspekt der Workload angegeben soll, dass Kapazität hinzugefügt oder entfernt werden muss. Bei Lasttests sollte ein repräsentativer Datenverkehr zum Einsatz kommen, der dem in der Produktion ähnelt. Erhöhen Sie unter Beobachtung der instrumentierten Metriken die Last, um zu bestimmen, welche Metrik angibt, wann Ressourcen hinzugefügt oder entfernt werden müssen.
- [Distributed Load Testing auf AWS: Simulieren Sie Tausende verbundener Benutzer](#)
  - Ermitteln Sie die Zusammensetzung von Anfragen. Möglicherweise haben Sie unterschiedliche Zusammensetzungen von Anfragen. Daher sollten Sie sich bei der Ermittlung der Zusammensetzung des Datenverkehrs verschiedene Zeiträume ansehen.
  - Implementieren Sie einen Lasttreiber. Zum Implementieren eines Lasttreibers können Sie Software mit eigenem Code, Open-Source-Software oder kommerzielle Software verwenden.
  - Führen Sie Lasttests zunächst mit geringer Kapazität durch. Schon bei der Erhöhung der Last für eine Einheit mit geringerer Kapazität, etwa einer einzelnen Instance oder einem einzelnen Container, stellen Sie unmittelbare Auswirkungen fest.
  - Führen Sie Lasttests mit größerer Kapazität durch. Bei einer verteilten Last sehen die Auswirkungen anders aus. Daher müssen Sie bei Tests Bedingungen herstellen, die der Produktionsumgebung möglichst nahekommen.

### Ressourcen

#### Zugehörige Dokumente:

- [Distributed Load Testing aktiviert AWS: simulieren Sie Tausende verbundener Benutzer](#)
- [Anwendungen für Lasttests](#)

#### Zugehörige Videos:

- [AWS Summit ANZ 2023: Mit AWS Distributed Load Testing können Sie mit Zuversicht schneller vorankommen](#)

## REL8 Wie werden Veränderungen implementiert?

Kontrollierte Änderungen sind erforderlich, um neue Funktionen bereitzustellen und um sicherzustellen, dass die Workloads und die Betriebsumgebung bekannte Software ausführen und auf vorhersagbare Weise durch Patches aktualisiert oder ersetzt werden können. Wenn solche Änderungen nicht kontrolliert sind, ist es schwierig, die Auswirkungen der Änderungen vorherzusagen oder Probleme zu lösen, die sich aus ihnen ergeben.

### Bewährte Methoden

- [REL08-BP01 Verwenden Sie Runbooks für Standardaktivitäten wie die Bereitstellung](#)
- [REL08-BP02 Integrieren Sie Funktionstests als Teil Ihrer Bereitstellung](#)
- [REL08-BP03 Integrieren Sie Resilienztests als Teil Ihrer Bereitstellung](#)
- [REL08-BP04 Bereitstellen mithilfe einer unveränderlichen Infrastruktur](#)
- [REL08-BP05 Änderungen automatisiert bereitstellen](#)

### REL08-BP01 Verwenden Sie Runbooks für Standardaktivitäten wie die Bereitstellung

Runbooks sind vordefinierte Verfahren, die ein bestimmtes Ergebnis verfolgen. Verwenden Sie Runbooks, um Standardaktivitäten manuell oder automatisch durchzuführen. Beispiele hierfür sind die Bereitstellung eines Workloads, das Patchen eines Workloads oder das Vornehmen von DNS Änderungen.

Sie können z. B. Prozesse einrichten, [um bei Bereitstellungen die Rollback-Sicherheit zu gewährleisten](#). Wenn Sie eine Bereitstellung ohne Unterbrechung für Ihre Kunden zurücksetzen können, steigert das die Zuverlässigkeit Ihres Service.

Für Runbook-Verfahren sollten Sie mit einem gültigen, effektiven manuellen Prozess beginnen, diesen in Code implementieren und ggf. die automatische Ausführung auslösen.

Selbst bei anspruchsvollen Workloads mit umfassender Automatisierung sind Runbooks nützlich, um [Ernstfallübungen auszuführen](#) oder strenge Berichterstellungs- und Auditing-Anforderungen zu erfüllen.

Playbooks werden als Reaktion auf bestimmte Vorfälle verwendet und mit Runbooks sollen bestimmte Ergebnisse erzielt werden. Häufig werden Runbooks für Routineaktivitäten genutzt, während Playbooks für die Reaktion auf außerplanmäßige Ereignisse verwendet werden.

Typische Anti-Muster:

- Durchführen ungeplanter Änderungen an der Konfiguration in der Produktion.
- Überspringen von Schritten in Ihrem Plan, um eine schnellere Bereitstellung durchzuführen, was zu einer fehlgeschlagenen Bereitstellung führt.
- Vornehmen von Änderungen, ohne die Umkehrung der Änderung zu testen.

Vorteile der Nutzung dieser bewährten Methode: Die effektive Änderungsplanung erhöht Ihre Fähigkeit, die Änderung erfolgreich auszuführen, da Sie sich aller betroffenen Systeme bewusst sind. Die Validierung Ihrer Änderungen in Testumgebungen erhöht Ihre Sicherheit.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Hoch

### Implementierungsleitfaden

- Unterstützen Sie konsistente und schnelle Reaktionen auf gut bekannte Ereignisse, indem Sie Verfahren in Runbooks dokumentieren.
  - [AWS Well-Architected Framework: Konzepte: Runbook](#)
- Verwenden Sie zur Definition Ihrer Infrastruktur den Grundsatz „Infrastructure as Code“. Wenn Sie Ihre Infrastruktur AWS CloudFormation (oder einen vertrauenswürdigen Drittanbieter) definieren, können Sie Versionskontrollsoftware verwenden, um Änderungen zu versionieren und nachzuverfolgen.
  - Verwenden Sie AWS CloudFormation (oder einen vertrauenswürdigen Drittanbieter), um Ihre Infrastruktur zu definieren.
    - [Was ist AWS CloudFormation?](#)
  - Erstellen Sie unter Anwendung guter Grundsätze für das Softwaredesign Vorlagen, die getrennt und entkoppelt sind.
    - Ermitteln Sie die für die Implementierung erforderlichen Berechtigungen, Vorlagen und zuständigen Parteien.
      - [Steuerung des Zugriffs mit AWS Identity and Access Management](#)
    - Verwenden Sie zur Versionskontrolle die Quellcodeverwaltung AWS CodeCommit oder ein Tool eines vertrauenswürdigen Drittanbieters.
      - [Was ist AWS CodeCommit?](#)

### Ressourcen

Zugehörige Dokumente:

- [APNPartner: Partner, die Ihnen bei der Entwicklung automatisierter Bereitstellungslösungen helfen können](#)
- [AWS Marketplace: Produkte zur Automatisierung Ihrer Bereitstellungen](#)
- [AWS Well-Architected Framework: Konzepte: Runbook](#)
- [Was ist? AWS CloudFormation](#)
- [Was ist AWS CodeCommit?](#)

Zugehörige Beispiele:

- [Automating operations with Playbooks and Runbooks](#)

## REL08-BP02 Integrieren Sie Funktionstests als Teil Ihrer Bereitstellung

Funktionstests werden im Rahmen der automatisierten Bereitstellung ausgeführt. Wenn die Erfolgskriterien nicht erfüllt sind, wird die Pipeline angehalten oder rückgängig gemacht. Diese Tests werden in einer Vorproduktionsumgebung ausgeführt, die vor der Produktion in der Pipeline bereitgestellt wird. Idealerweise erfolgt dies im Rahmen einer Bereitstellungs-pipeline.

Gewünschtes Ergebnis: Sie verwenden Automatisierung, um Funktionstests durchzuführen, und die zugehörigen Testdaten reduzieren die Testdauer und die Kosten und verbessern die Genauigkeit der Testergebnisse. Sie integrieren Funktionstests als Teil Ihres Bereitstellungsprozesses, was Ihnen hilft, Ihre Veröffentlichungspipelines für schnelle und zuverlässige Anwendungs- und Infrastrukturupdates zu automatisieren.

Typische Anti-Muster:

- Sie führen Tests außerhalb der Bereitstellungs-pipeline manuell durch.
- Sie überspringen Testschritte in Ihrer Automatisierung durch manuelle Notfall-Workflows.
- Sie folgen nicht Ihren etablierten Testplänen und Prozessen zugunsten beschleunigter Zeitpläne.

Vorteile der Nutzung dieser bewährten Methode: Funktionstests bestätigen, dass das System gemäß den angegebenen Anforderungen funktioniert. Es wird verwendet, um die vorgesehene Funktionsreihenfolge von Komponenten wie BenutzeroberflächenAPIs, Datenbanken und Quellcode konsistent zu überprüfen. Wenn Sie diese Systemkomponenten untersuchen, stellen Funktionstests sicher, dass sich jedes Feature wie erwartet verhält, wodurch sowohl die Benutzererwartungen als auch die Integrität der Software geschützt werden. Integrieren Sie Funktionstests als Teil Ihrer

regulären Bereitstellung und nutzen Sie die Automatisierung, um alle Änderungen umzusetzen, wodurch das Risiko menschlicher Fehler reduziert wird.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Hoch

### Implementierungsleitfaden

Integrieren Sie Funktionstests in Ihre Bereitstellung. Funktionstests werden im Rahmen der automatisierten Bereitstellung ausgeführt. Wenn die Erfolgskriterien nicht erfüllt sind, wird die Pipeline angehalten oder ein Rollback durchgeführt. AWS CodePipeline bietet eine Continuous-Delivery-Pipeline für automatisierte Tests, die es Testern ermöglicht, den gesamten Test- und Bereitstellungsprozess zu automatisieren. Es lässt sich in AWS Dienste wie AWS CodeBuild und AWS CodeDeploy zur Automatisierung der Erstellungs-, Test- und Bereitstellungsphasen des Softwareentwicklungszyklus integrieren.

### Implementierungsschritte

- Konfigurieren Sie Ihre Pipeline: Richten Sie Ihre Quell-, Build-, Test- und Bereitstellungsphasen mithilfe der AWS CodePipeline Konsole oder AWS Command Line Interface (CLI) ein.
  - Definiere deine Quelle: Mit AWS CodePipeline kannst du automatisch Quellcode von Versionskontrollsystemen wie GitHub,, oder Bitbucket abrufen AWS CodeCommit, wodurch überprüft wird, ob immer der neueste Code für Tests verwendet wird.
  - Automatisiere Builds und Tests: AWS CodeBuild kann deinen Code automatisch erstellen und testen und Testberichte generieren. Es unterstützt beliebige Test-Frameworks wie JUnitNUnit, und TestNG.
  - Stellen Sie Ihren Code bereit: Sobald der Code erstellt und getestet wurde, AWS CodeDeploy können Sie ihn in Ihrer Testumgebung bereitstellen, einschließlich EC2 Amazon-Instances, AWS Lambda Funktionen oder lokalen Servern.
  - Überwachen Sie Pipelines: AWS CodePipeline kann den Fortschritt Ihrer Pipeline und den Status jeder Phase verfolgen. Sie können auch Qualitätsprüfungen verwenden, um die Pipeline gemäß dem Testausführungsstatus zu blockieren. Außerdem können Sie Benachrichtigungen über jeden Ausfall einer Pipeline-Phase oder den Abschluss einer Pipeline erhalten.

### Ressourcen

Zugehörige Dokumente:

- [Verwenden Sie AWS CodePipeline with AWS CodeBuild , um Code zu testen und Builds auszuführen](#)
- [Einloggen und Überwachen AWS CodeBuild](#)
- [Indicators for functional testing](#)

## REL08-BP03 Integrieren Sie Resilienztests als Teil Ihrer Bereitstellung

Integrieren Sie Resilienztests, indem Sie bewusst Fehler in Ihr System einleiten, um dessen Leistungsfähigkeit im Falle von Störszenarien zu messen. Resilienztests unterscheiden sich von Geräte- und Funktionstests, die normalerweise in Bereitstellungszyklen integriert werden, da sie sich auf die Identifizierung unerwarteter Ausfälle in Ihrem System konzentrieren. Es ist zwar sicher, in der Vorproduktion mit der Integration von Resilienztests zu beginnen, aber setzen Sie sich das Ziel, diese Tests im Rahmen Ihrer [GameDays](#) in der Produktion zu implementieren.

Gewünschtes Ergebnis: Resilienztests tragen dazu bei, Vertrauen in die Fähigkeit des Systems aufzubauen, Beeinträchtigungen in der Produktion standzuhalten. Experimente identifizieren Schwachstellen, die zu Ausfällen führen könnten. Auf diese Weise können Sie Ihr System verbessern, um Ausfälle und Beeinträchtigungen automatisch und effizient zu beheben.

### Typische Anti-Muster:

- Mangelnde Beobachtbarkeit und Überwachung in Bereitstellungsprozessen
- Verlass auf Menschen, um Systemausfälle zu beheben
- Analysemechanismen von schlechter Qualität
- Fokus auf bekannte Probleme in einem System und das Fehlen von Experimenten, um unbekannte Probleme zu identifizieren
- Identifizieren von Fehlern, aber keine Lösung
- Keine Dokumentation der Erkenntnisse und keine Runbooks

Vorteile der Nutzung dieser bewährten Methode: Resilienztests, die in Ihre Bereitstellungen integriert sind, helfen dabei, unbekannte Probleme im System zu identifizieren, die andernfalls unbemerkt bleiben und zu Produktionsausfällen führen können. Die Identifizierung dieser unbekannt Probleme in einem System hilft Ihnen, Ergebnisse zu dokumentieren, Tests in Ihren CI/CD-Prozess zu integrieren und Runbooks zu erstellen, die die Schadensbegrenzung durch effiziente, wiederholbare Mechanismen vereinfachen.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel

## Implementierungsleitfaden

Die gängigsten Formen von Resilienztests, die in die Bereitstellungen Ihres Systems integriert werden können, sind die Notfallwiederherstellung und Chaos-Engineering.

- Schließen Sie Aktualisierungen Ihrer Notfallwiederherstellungspläne und Standardarbeitsanweisungen (SOPs) bei jeder größeren Bereitstellung mit ein.
- Integrieren Sie Zuverlässigkeitstests in Ihre automatisierten Bereitstellungs Pipelines. Services wie [AWS Resilience Hub](#) können [in Ihre CI/CD-Pipeline integriert werden](#), um kontinuierliche Resilienzbewertungen zu erstellen, die im Rahmen jeder Bereitstellung automatisch bewertet werden.
- Definieren Sie Ihre Anwendungen in AWS Resilience Hub. Resilienzanalysen generieren Codefragmente, die Ihnen helfen, Wiederherstellungsverfahren als AWS Systems Manager Manager-Dokumente für Ihre Anwendungen zu erstellen, und bieten eine Liste der empfohlenen CloudWatch Amazon-Monitore und -Alarmer.
- Sobald Ihre DR-Pläne und Aktualisierungen abgeschlossen SOPs sind, führen Sie die Notfallwiederherstellungstests durch, um sicherzustellen, dass sie wirksam sind. Mithilfe von Notfallwiederherstellungstests können Sie feststellen, ob Sie Ihr System nach einem Ereignis wiederherstellen und zum normalen Betrieb zurückkehren können. Sie können verschiedene Notfallwiederherstellungsstrategien simulieren und feststellen, ob Ihre Planung ausreicht, um Ihre Verfügbarkeitsanforderungen zu erfüllen. Zu den gängigen Notfallwiederherstellungsstrategien gehören Backup und Wiederherstellung, Pilot Light, Cold Standby, Warm Standby, Hot Standby und Aktiv-Aktiv. Sie alle unterscheiden sich in Kosten und Komplexität. Wir empfehlen Ihnen, vor dem Disaster Recovery-Test Ihr Wiederherstellungszeitziel (RTO) und Ihr Wiederherstellungspunktziel (RPO) zu definieren, um die Wahl der zu simulierenden Strategie zu vereinfachen. AWS bietet Tools für die Notfallwiederherstellung [AWS Elastic Disaster Recovery](#), die Ihnen den Einstieg in Ihre Planung und Tests erleichtern.
- Experimente im Bereich des Chaos-Engineering führen zu Störungen im System, wie z. B. Netzwerk- und Serviceausfällen. Durch die Simulation mit kontrollierten Ausfällen können Sie die Sicherheitsschwachstellen Ihres Systems erkennen und gleichzeitig die Auswirkungen der eingeführten Fehler eindämmen. Führen Sie wie bei den anderen Strategien kontrollierte Ausfallsimulationen in Umgebungen außerhalb der Produktion durch, indem Sie beispielsweise Services wie [AWS Fault Injection Service](#) nutzen, um vor dem Einsatz in der Produktion Vertrauen zu gewinnen.



## Ressourcen

### Zugehörige Dokumente:

- [Experiment with failure using resilience testing to build recovery preparedness](#)
- [Kontinuierliche Bewertung der Widerstandsfähigkeit von Anwendungen mit AWS Resilience Hub und AWS CodePipeline](#)
- [Disaster Recovery \(DR\) -Architektur weiter AWS, Teil 1: Strategien für die Wiederherstellung in der Cloud](#)
- [Verify the resilience of your workloads using Chaos Engineering](#)
- [Principles of Chaos Engineering](#)
- [Chaos Engineering Workshop](#)

### Zugehörige Videos:

- [AWS re:Invent 2020: Testing Resilience using Chaos Engineering](#)
- [Verbessern Sie die Widerstandsfähigkeit von Anwendungen mit dem AWS Fault Injection Service](#)
- [Bereiten Sie Ihre Anwendungen vor und schützen Sie sie vor Störungen mit AWS Resilience Hub](#)

## REL08-BP04 Bereitstellen mithilfe einer unveränderlichen Infrastruktur

Eine unveränderliche Infrastruktur sieht vor, dass Updates, Sicherheits-Patches oder Konfigurationsänderungen nicht direkt in Produktions-Workloads durchgeführt werden. Wenn eine Änderung erforderlich ist, wird die Architektur auf einer neuen Infrastruktur eingerichtet und für die Produktion bereitgestellt.

Verfolgen Sie eine Strategie zur Bereitstellung einer unveränderlichen Infrastruktur, um die Zuverlässigkeit, Konsistenz und Reproduzierbarkeit Ihrer Workload-Bereitstellungen zu erhöhen.

Gewünschtes Ergebnis: Bei einer unveränderlichen Infrastruktur sind keine [direkten Änderungen](#) an den Infrastrukturrressourcen innerhalb eines Workloads erlaubt. Wenn eine Änderung erforderlich ist, wird stattdessen ein neuer Satz aktualisierter Infrastrukturrressourcen, der alle erforderlichen Änderungen enthält, parallel zu Ihren vorhandenen Ressourcen bereitgestellt. Diese Bereitstellung wird automatisch validiert und bei Erfolg wird der Datenverkehr schrittweise auf die neuen Ressourcen verlagert.

Diese Bereitstellungsstrategie gilt unter anderem für Softwareupdates, Sicherheits-Patches, Infrastrukturänderungen, Konfigurationsupdates und Anwendungsupdates.

Typische Anti-Muster:

- Implementieren von Änderungen an laufenden Infrastruktur-Ressourcen vor Ort.

Vorteile der Nutzung dieser bewährten Methode:

- Erhöhte Konsistenz zwischen verschiedenen Umgebungen: Da es keine Unterschiede bei den Infrastrukturressourcen zwischen den Umgebungen gibt, wird die Konsistenz erhöht und das Testen vereinfacht.
- Verringerung der Konfigurationsabweichungen: Durch das Ersetzen von Infrastrukturressourcen durch eine bekannte und versionskontrollierte Konfiguration wird die Infrastruktur in einen bekannten, getesteten und vertrauenswürdigen Zustand versetzt, wodurch Konfigurationsabweichungen vermieden werden.
- Zuverlässige atomare Bereitstellungen: Entweder werden die Verteilungen erfolgreich abgeschlossen oder es ändert sich nichts, was die Konsistenz und Zuverlässigkeit des Verteilungsprozesses erhöht.
- Vereinfachte Bereitstellungen: Bereitstellungen werden vereinfacht, da sie keine Upgrades unterstützen müssen. Upgrades sind einfach neue Bereitstellungen.
- Sicherere Bereitstellungen mit schnellen Rollback- und Wiederherstellungsprozessen: Bereitstellungen sind sicherer, da die vorherige funktionierende Version nicht geändert wird. Sie können einen Rollback zur vorherigen Version durchführen, wenn Fehler erkannt werden.
- Verbesserte Sicherheitslage: Wenn Änderungen an der Infrastruktur nicht zugelassen werden, können Fernzugriffsmechanismen (z. B. SSH) deaktiviert werden. Dadurch wird der Angriffsvektor reduziert und die Sicherheitslage Ihrer Organisation verbessert.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel

Implementierungsleitfaden

Automation

Bei der Definition einer Strategie zur Bereitstellung einer unveränderlichen Infrastruktur empfiehlt es sich, die [Automatisierung](#) so weit wie möglich zu nutzen, um die Reproduzierbarkeit zu erhöhen und das Potenzial für menschliche Fehler zu minimieren. Weitere Informationen finden Sie unter [REL08-](#)

## BP05 Automatisierte Implementierung von Änderungen und Automatisieren sicherer, automatischer Bereitstellungen.

Mit [Infrastructure as code \(IaC\)](#) werden Schritte zur Bereitstellung, Orchestrierung und Implementierung der Infrastruktur auf programmatische, beschreibende und deklarative Weise definiert und in einem Quellkontrollsystem gespeichert. Die Nutzung von Infrastructure as Code vereinfacht die Automatisierung der Infrastrukturbereitstellung und trägt zur Unveränderbarkeit der Infrastruktur bei.

### Bereitstellungsmuster

Wenn eine Änderung des Workloads erforderlich ist, schreibt die Strategie der unveränderlichen Infrastrukturbereitstellung vor, dass ein neuer Satz von Infrastrukturressourcen bereitgestellt wird, einschließlich aller erforderlichen Änderungen. Es ist wichtig, dass diese neuen Ressourcen nach einem Muster eingeführt werden, das die Auswirkungen auf die Benutzer minimiert. Für diese Bereitstellung gibt es zwei Hauptstrategien:

[Canary-Bereitstellung](#): Hierbei wird eine kleine Anzahl Ihrer Kunden auf die neue Version umgestellt, die in der Regel auf einer einzelnen Service-Instance (dem Canary) ausgeführt wird. Anschließend überprüfen Sie sämtliche Verhaltensänderungen oder Fehler, die generiert werden. Sie können Datenverkehr aus der Canary-Umgebung entfernen, wenn kritische Probleme auftreten, und die Benutzer auf die vorherige Version zurücksetzen. Wenn die Bereitstellung erfolgreich ist, können Sie die Bereitstellung mit der gewünschten Geschwindigkeit fortsetzen und gleichzeitig die Änderungen auf Fehler überwachen, bis Sie vollständig bereitgestellt sind. AWS CodeDeploy kann mit einer [Bereitstellungskonfiguration](#) konfiguriert werden, die eine Bereitstellung auf Canary-Computern ermöglicht.

[Blue/Green-Bereitstellung](#): Verhält sich ähnlich wie die Canary-Bereitstellung, nur dass eine komplette Flotte der Anwendung parallel bereitgestellt wird. Sie können Ihre Bereitstellungen über die zwei Stacks (blau und grün) alternieren. Auch hier können Sie Datenverkehr an die neue Version senden und einen Failback auf die alte Version durchführen, wenn bei der Bereitstellung Probleme auftreten. In der Regel wird der gesamte Datenverkehr auf einmal umgestellt. Sie können jedoch auch Bruchteile Ihres Datenverkehrs für jede Version verwenden, um die Einführung der neuen Version mithilfe der gewichteten DNS Routing-Funktionen von Amazon Route 53 voranzutreiben. AWS CodeDeploy und [AWS Elastic Beanstalk](#) kann mit einer Bereitstellungskonfiguration konfiguriert werden, die eine blaue/grüne Bereitstellung ermöglicht.

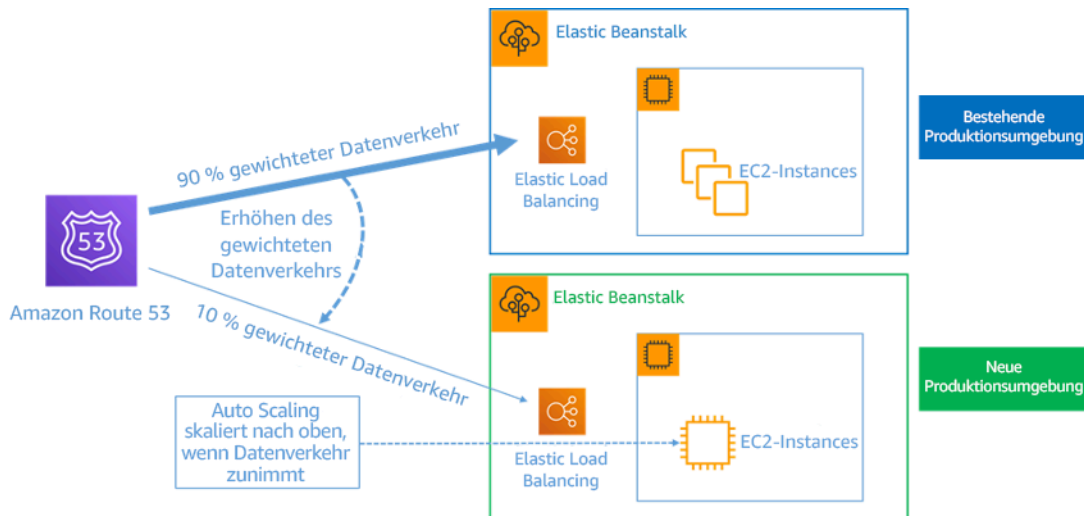


Abbildung 8: Blue/Green-Bereitstellung mit AWS Elastic Beanstalk und Amazon Route 53

## Erkennung von Abweichungen

Als Abweichung wird jede Änderung bezeichnet, die dazu führt, dass eine Infrastrukturressource einen anderen Zustand oder eine andere Konfiguration aufweist als erwartet. Jede Art von nicht verwalteter Konfigurationsänderung widerspricht dem Konzept der unveränderlichen Infrastruktur und sollte erkannt und behoben werden, um eine erfolgreiche Implementierung der unveränderlichen Infrastruktur zu gewährleisten.

## Implementierungsschritte

- Untersagen Sie die Änderung laufender Infrastruktur-Ressourcen an Ort und Stelle.
- Mit [AWS Identity and Access Management \(IAM\)](#) können Sie angeben, wer oder was auf Dienste und Ressourcen zugreifen kann AWS, detaillierte Berechtigungen zentral verwalten und den Zugriff analysieren, um die Zugriffsrechte zu verfeinern. AWS
- Automatisieren Sie die Bereitstellung von Infrastrukturressourcen, um die Reproduzierbarkeit zu erhöhen und das Potenzial für menschliche Fehler zu minimieren.
- Wie in der [Einführung in ein AWS Whitepaper](#) beschrieben, ist Automatisierung ein Eckpfeiler von AWS Services und wird intern in allen Services, Funktionen und Angeboten unterstützt. DevOps
- [Wenn Sie Ihr Amazon Machine Image \(AMI\) vorab](#) erstellen, kann dies die Startzeit verkürzen. [EC2Image Builder](#) ist ein vollständig verwalteter AWS Service, mit dem Sie die Erstellung, Wartung, Validierung, gemeinsame Nutzung und Bereitstellung von benutzerdefinierten, sicheren und up-to-date Linux- oder Windows-spezifischen Anwendungen automatisieren könnenAMI.

- Zu den Services, die die Automatisierung unterstützen, gehören:
  - [AWS Elastic Beanstalk](#) ist ein Service zur schnellen Bereitstellung und Skalierung von mit Java entwickelten Webanwendungen, .NET, Node.js, PHP, Python, Ruby, Go und Docker auf vertrauten Servern wie Apache NGINX, Passenger und IIS.
  - [AWS Proton](#) hilft Plattformteams dabei, alle die verschiedenen Tools zu verbinden und zu koordinieren, die Ihre Entwicklungsteams für die Bereitstellung von Infrastruktur, Codebereitstellung, Überwachung und Updates benötigen. AWS Proton ermöglicht automatisierte Infrastruktur als Codebereitstellung und Bereitstellung von serverlosen und containerbasierten Anwendungen.
- Die Nutzung von Infrastruktur als Code erleichtert die Automatisierung der Infrastrukturbereitstellung und trägt zur Unveränderlichkeit der Infrastruktur bei. AWS bietet Dienste, die die Erstellung, Bereitstellung und Wartung der Infrastruktur auf programmatische, beschreibende und deklarative Weise ermöglichen.
  - [AWS CloudFormation](#) hilft Entwicklern dabei, AWS Ressourcen auf geordnete und vorhersehbare Weise zu erstellen. Ressourcen werden im YAML Format JSON oder in Textdateien geschrieben. Die Vorlagen erfordern eine bestimmte Syntax und Struktur, die von den Arten der zu erstellenden und zu verwaltenden Ressourcen abhängt. Sie erstellen Ihre Ressourcen in JSON oder YAML mit einem beliebigen Code-Editor AWS Cloud9, z. B., checken sie in ein Versionskontrollsystem ein und erstellen CloudFormation dann die angegebenen Dienste auf sichere, wiederholbare Weise.
  - [AWS Serverless Application Model \(AWS SAM\)](#) ist ein Open-Source-Framework, auf dem Sie serverlose Anwendungen erstellen können. AWS SAM lässt sich in andere AWS Dienste integrieren und ist eine Erweiterung von AWS CloudFormation
  - [AWS Cloud Development Kit \(AWS CDK\)](#) ist ein Open-Source-Framework für die Softwareentwicklung zur Modellierung und Bereitstellung Ihrer Cloud-Anwendungsressourcen mit Hilfe gängiger Programmiersprachen. Sie können AWS CDK verwenden, um die Anwendungsinfrastruktur mithilfe von Python TypeScript, Java und zu modellieren. NET. AWS CDK verwendet AWS CloudFormation im Hintergrund, um Ressourcen auf sichere und wiederholbare Weise bereitzustellen.
  - [AWS Cloud Control API](#) führt einen gemeinsamen Satz von Create, Read, Update, Delete und List (CRUDL) APIs ein, mit dem Entwickler ihre Cloud-Infrastruktur auf einfache und konsistente Weise verwalten können. Die Cloud Control API Common APIs ermöglichen es Entwicklern, den Lebenszyklus von Diensten AWS und Diensten von Drittanbietern einheitlich zu verwalten.
- Implementieren Sie Bereitstellungsmuster, die die Auswirkungen auf die Benutzer minimieren.

- Canary-Bereitstellungen:
  - [Richten Sie ein API Gateway Canary Release-Deployment ein](#)
  - [Erstellen Sie eine Pipeline mit kanarischen Bereitstellungen für Amazon mithilfe von ECS AWS App Mesh](#)
- Blaue/grüne Bereitstellungen: Das [AWS Whitepaper Blue/Green Deployments on beschreibt Beispieltechniken zur Implementierung von blauen/grünen](#) Implementierungsstrategien.
- Erkennen Sie Konfigurations- oder Zustandsabweichungen. Weitere Informationen finden Sie unter [Detecting unmanaged configuration changes to stacks and resources](#).

## Ressourcen

### Zugehörige bewährte Methoden:

- [REL08-BP05 Automatisierte Implementierung von Änderungen](#)

### Zugehörige Dokumente:

- [Automatisierung sicherer, vollautomatischer Bereitstellungen](#)
- [Nutzung zur Schaffung einer AWS CloudFormation unveränderlichen Infrastruktur bei Nubank](#)
- [Infrastructure as Code](#)
- [Implementierung eines Alarms zur automatischen Erkennung von Abweichungen in Stapeln AWS CloudFormation](#)

### Zugehörige Videos:

- [AWS re:Invent 2020: Zuverlässigkeit, Konsistenz und Vertrauen durch Unveränderlichkeit](#)

## REL08-BP05 Änderungen automatisiert bereitstellen

Bereitstellungen und Patches werden automatisiert, um negative Auswirkungen zu vermeiden.

Änderungen an Produktionssystemen gehören in vielen Organisationen zu den größten Risikofaktoren. Neben den geschäftlichen Problemen, die durch die Software behoben werden, betrachten wir Bereitstellungen als vorrangiges Problem, das es zu lösen gilt. Heutzutage bedeutet das, wenn immer möglich und sinnvoll, Vorgänge zu automatisieren. Dazu gehören Tests und die

Bereitstellung von Änderungen, das Hinzufügen oder Entfernen von Kapazität und das Migrieren von Daten.

Gewünschtes Ergebnis: Sie integrieren automatische Bereitstellungssicherheit in den Veröffentlichungsprozess mit umfangreichen Tests vor der Produktion, automatischen Rollbacks und gestaffelten Produktionsbereitstellungen. Diese Automatisierung minimiert die potenziellen Auswirkungen auf die Produktion, die durch fehlgeschlagene Bereitstellungen verursacht werden, und Entwickler müssen die Bereitstellungen nicht mehr aktiv bis zur Produktion beobachten.

Typische Anti-Muster:

- Sie führen manuelle Änderungen durch.
- Sie überspringen Schritte in Ihrer Automatisierung durch manuelle Notfall-Workflows.
- Sie folgen nicht Ihren etablierten Plänen und Prozessen zugunsten beschleunigter Zeitpläne.
- Sie führen schnelle Folgebereitstellungen durch, ohne entsprechende Bake-Zeit einzuräumen.

Vorteile der Nutzung dieser bewährten Methode: Wenn Sie alle Änderungen mithilfe der Automatisierung implementieren, vermeiden Sie das Risiko menschlicher Fehler und bieten die Möglichkeit, Tests durchzuführen, bevor Sie die Produktion ändern. Wenn Sie diesen Vorgang vor dem Produktionsstart durchführen, wird sichergestellt, dass Ihre Pläne vollständig sind. Darüber hinaus kann ein automatisches Rollback in Ihren Veröffentlichungsprozess Produktionsprobleme identifizieren und Ihren Workload wieder in den ursprünglichen Betriebszustand versetzen.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel

Implementierungsleitfaden

Automatisieren Sie Ihre Bereitstellungs-Pipeline. Mit Bereitstellungs-Pipelines können Sie Tests und die Entdeckung von Anomalien automatisieren und die Pipeline an einem bestimmten Schritt vor der Bereitstellung in der Produktion anhalten oder eine Änderung automatisch zurückführen. Ein integraler Bestandteil davon ist die Einführung einer Kultur der [Continuous Integration und Continuous Delivery/Deployment](#) (CI/CD), bei der ein Commit oder eine Codeänderung verschiedene automatische Stage-Gates von der Build- und Testphase bis zur Bereitstellung in Produktionsumgebungen durchläuft.

Obwohl es immer noch als sinnvoll erachtet wird, Personen bei den komplexesten betrieblichen Abläufen einzubinden, empfehlen wir, diese Abläufe wegen ihrer Komplexität zu automatisieren.

## Implementierungsschritte

Sie können Bereitstellungen automatisieren, um manuelle Operationen zu vermeiden, indem Sie die folgenden Schritte ausführen:

- Einrichten eines Code-Repositorys zur Speicherung Ihres Codes: Verwenden Sie [AWS CodeCommit](#), um ein sicheres Git-basiertes Repository zu erstellen. .
- Konfigurieren Sie einen Continuous Integration Service, um Ihren Quellcode zu kompilieren, Tests durchzuführen und Bereitstellungsartefakte zu erstellen: Informationen zum Einrichten eines Build-Projekts für diesen Zweck finden Sie unter [Erste Schritte mit der AWS CodeBuild Verwendung](#) der Konsole.
- Richten Sie einen Bereitstellungsservice ein, der Anwendungsbereitstellungen automatisiert und die Komplexität von Anwendungsaktualisierungen bewältigt, ohne auf fehleranfällige manuelle Bereitstellungen angewiesen zu sein: [AWS CodeDeploy](#) automatisiert Softwarebereitstellungen für eine Vielzahl von Rechendiensten wie AmazonEC2, und Ihre lokalen Server. [AWS Fargate](#)[AWS Lambda Informationen zur Konfiguration dieser Schritte finden Sie unter Erste Schritte mit CodeDeploy](#)
- Konfigurieren eines Continuous-Integration-Services zur Automatisierung der Veröffentlichungspipelines für schnellere und zuverlässigere Anwendungs- und Infrastrukturupdates: Erwägen Sie die Verwendung von [AWS CodePipeline](#), um die Automatisierung Ihrer Veröffentlichungspipelines zu unterstützen. Weitere Informationen finden Sie in den [CodePipelineTutorials](#).

## Ressourcen

Zugehörige bewährte Methoden:

- [OPS05-BP04 Verwenden Sie Build- und Deployment-Management-Systeme](#)
- [OPS05- BP1 0 Automatisieren Sie die Integration und Bereitstellung vollständig](#)
- [OPS06-BP02 Testbereitstellungen](#)
- [OPS06-BP04 Automatisieren Sie Tests und Rollbacks](#)

Zugehörige Dokumente:

- [Kontinuierliche Bereitstellung verschachtelter Stacks mithilfe von AWS CloudFormation](#)[AWS CodePipeline](#)



- [Vollständiges CI/CD mit AWS CodeCommit,, und AWS CodeBuildAWS CodeDeployAWS CodePipeline](#)
- [APNPartner: Partner, die Ihnen bei der Erstellung automatisierter Bereitstellungslösungen helfen können](#)
- [AWS Marketplace: Produkte zur Automatisierung Ihrer Bereitstellungen](#)
- [Automate chat messages with webhooks.](#)
- [Die Amazon Builders' Library: Gewährleistung von Rollback-Sicherheit während der Bereitstellung](#)
- [Die Amazon Builders' Library: Schneller mit kontinuierlicher Lieferung](#)
- [Was ist AWS CodePipeline?](#)
- [Was ist CodeDeploy?](#)
- [AWS Systems Manager Patch Manager](#)
- [Was ist AmazonSES?](#)
- [Was ist Amazon Simple Notification Service?](#)

Zugehörige Videos:

- [AWS Summit 2019: CI/CD auf AWS](#)

## Fehlerverwaltung

Fragen

- [REL9. Wie werden Daten gesichert?](#)
- [REL10. Wie wird die Fehlerisolierung zum Schützen der Workload verwendet?](#)
- [REL11. Wie können Sie Workloads so gestalten, dass sie Komponentenausfällen gegenüber resilient sind?](#)
- [REL12. Wie lässt sich die Zuverlässigkeit testen?](#)
- [REL13. Was ist bei der Planung der Notfallwiederherstellung zu beachten?](#)

### REL9. Wie werden Daten gesichert?

Sichern Sie Daten, Anwendungen und Konfigurationen, um Ihre Anforderungen in Bezug auf Wiederherstellungszeitziele (RTO) und Wiederherstellungspunktziele (RPO) zu erfüllen.

## Bewährte Methoden

- [REL09-BP01 Identifizieren und sichern Sie alle Daten, die gesichert werden müssen, oder reproduzieren Sie die Daten aus Quellen](#)
- [REL09-BP02 Sicheres und Verschlüsseln von Backups](#)
- [REL09-BP03 Automatische Datensicherung durchführen](#)
- [REL09-BP04 Führen Sie eine regelmäßige Wiederherstellung der Daten durch, um die Integrität und die Prozesse des Backups zu überprüfen](#)

REL09-BP01 Identifizieren und sichern Sie alle Daten, die gesichert werden müssen, oder reproduzieren Sie die Daten aus Quellen

Sie sollten die Backup-Funktionen der von dem Workload genutzten Daten-Services und -Ressourcen verstehen und nutzen. Die meisten Services bieten Funktionen zur Sicherung von Workload-Daten.

Gewünschtes Ergebnis: Die Datenquellen wurden identifiziert und nach ihrer Bedeutung klassifiziert. Legen Sie anschließend eine Strategie für die Datenwiederherstellung fest, die auf dem basiert. RPO Diese Strategie involviert entweder die Sicherung dieser Datenquellen oder die Möglichkeit, Daten aus anderen Quellen zu reproduzieren. Im Falle eines Datenverlusts ermöglicht die implementierte Strategie die Wiederherstellung oder Reproduktion von Daten innerhalb des definierten RPO BereichsRTO.

„Cloud-Reife“-Phase: Grundlegend

Typische Anti-Muster:

- Nicht alle Datenquellen für die Workload und deren Kritikalität sind bekannt.
- Es erfolgen keine Backups kritischer Datenquellen.
- Es erfolgen nur Backups von manchen Datenquellen ohne die Verwendung von Kritikalität als Kriterium.
- Keine definierte oder RPO die Backup-Frequenz kann nicht eingehalten werdenRPO.
- Es erfolgt keine Bewertung, ob ein Backup erforderlich ist oder ob Daten aus anderen Quellen reproduziert werden können.

Vorteile der Nutzung dieser bewährten Methode: Die Identifizierung der Stellen, an denen Backups erforderlich sind, und die Implementierung eines Mechanismus zur Erstellung von Backups oder

die Möglichkeit, die Daten aus einer externen Quelle zu reproduzieren, verbessern die Fähigkeit zur Wiederherstellung und Wiederbeschaffung von Daten während eines Ausfalls.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Hoch

### Implementierungsleitfaden

Alle AWS Datenspeicher bieten Backup-Funktionen. Dienste wie Amazon RDS und Amazon DynamoDB unterstützen zusätzlich automatisiertes Backup, das point-in-time Recovery (PITR) ermöglicht, sodass Sie ein Backup jederzeit bis zu fünf Minuten oder weniger vor der aktuellen Uhrzeit wiederherstellen können. Viele AWS Dienste bieten die Möglichkeit, Backups auf andere zu kopieren. AWS-Region AWS Backup ist ein Tool, mit dem Sie den Datenschutz für alle AWS Dienste zentralisieren und automatisieren können. [AWS Elastic Disaster Recovery](#) ermöglicht es Ihnen, komplette Server-Workloads zu kopieren und einen kontinuierlichen Datenschutz vor Ort, in ganz AZ oder in verschiedenen Regionen aufrechtzuerhalten, wobei ein Recovery Point Objective (RPO) in Sekunden gemessen wird.

Amazon S3 kann als Backup-Ziel für selbstverwaltete und verwaltete Datenquellen verwendet werden. AWS Dienste wie Amazon EBS, Amazon ElastiCache und Amazon RDS DynamoDB verfügen über integrierte Funktionen zum Erstellen von Backups. Sicherungssoftware von Drittanbietern kann ebenfalls eingesetzt werden.

Lokale Daten können mithilfe von oder gesichert werden. AWS Cloud [AWS Storage Gateway](#) [AWS DataSync](#) Mit Amazon S3-Buckets können Sie diese Daten auf AWS speichern. Amazon S3 bietet mehrere Speicherebenen wie [Amazon S3 Glacier](#) oder [S3 Glacier Deep Archive](#), um die Kosten für den Datenspeicher zu senken.

Möglicherweise können Sie Ihre Datenwiederherstellungs-Anforderungen erfüllen, indem Sie Daten aus anderen Quellen reproduzieren. Zum Beispiel könnten [Amazon ElastiCache Replica Nodes](#) oder [Amazon RDS Read Replicas](#) verwendet werden, um Daten zu reproduzieren, falls der primäre Knoten verloren geht. In Fällen, in denen Quellen wie diese verwendet werden können, um Ihr [Recovery Point Objective \(RPO\) und Recovery Time Objective \(RTO\)](#) zu erreichen, benötigen Sie möglicherweise kein Backup. Ein weiteres Beispiel: Wenn Sie mit Amazon ElastiCache arbeiten, ist es möglicherweise nicht erforderlich, Ihren HDFS Datenspeicher zu sichern, solange Sie [die Daten von Amazon ElastiCache in Amazon S3 reproduzieren](#) können.

Bei der Auswahl einer Backup-Strategie sollten Sie die für die Datenwiederherstellung benötigte Zeit berücksichtigen. Diese hängt von der Art des Backups (im Falle einer Backup-Strategie) oder von der Komplexität des Datenreproduktions-Mechanismus ab. Diese Zeit sollte im Rahmen der RTO Arbeitslast liegen.

## Implementierungsschritte

1. Identifizieren Sie alle Datenquellen für die Workload. Daten können über verschiedene Ressourcen wie [Datenbanken](#), [Volumes](#), [Dateisysteme](#), [Protokollierungssysteme](#) und [Objektspeicher](#) gespeichert werden. Im Abschnitt Ressourcen finden Sie verwandte Dokumente zu den verschiedenen AWS Diensten, bei denen Daten gespeichert werden, und zu den Backup-Funktionen, die diese Dienste bieten.
2. Klassifizieren Sie Datenquellen basierend auf Kritikalität. Unterschiedliche Datensätze haben unterschiedliche Kritikalitäts-Niveaus für eine Workload und damit auch verschiedene Anforderungen an die Ausfallsicherheit. Beispielsweise können einige Daten kritisch sein und einen Wert RPO nahe Null erfordern, während andere Daten weniger kritisch sind und einen höheren RPO und einen gewissen Datenverlust tolerieren können. In ähnlicher Weise können auch für unterschiedliche Datensätze unterschiedliche RTO Anforderungen gelten.
3. Verwenden Sie AWS Dienste von Drittanbietern, um Backups der Daten zu erstellen. [AWS Backup](#) ist ein verwalteter Dienst, mit dem Backups verschiedener Datenquellen erstellt werden können. [AWS Elastic Disaster Recovery](#) verwaltet die automatische Datenreplikation in Sekundenbruchteilen auf eine AWS-Region. Die meisten AWS Dienste verfügen auch über native Funktionen zum Erstellen von Backups. The AWS Marketplace hat viele Lösungen, die diese Funktionen ebenfalls bieten. In den unten aufgeführten Ressourcen finden Sie Informationen darüber, wie Sie Backups von Daten aus verschiedenen AWS -Services erstellen können.
4. Für Daten, die nicht gesichert werden, sollten Sie einen Datenreproduktions-Mechanismus festlegen. Es gibt verschiedene Gründe dafür, Daten, die aus anderen Quellen reproduziert werden können, nicht zu sichern. Möglicherweise ergibt sich die Situation, dass es günstiger ist, Daten bei Bedarf aus Quellen zu reproduzieren als ein Backup zu erstellen, da mit der Speicherung von Backups gewisse Kosten verbunden sind. Ein anderes Beispiel ist, dass die Wiederherstellung aus einem Backup länger dauert als die Reproduktion der Daten aus Quellen, was zu einem Verstoß in führt. RTO In solchen Situationen sollten Sie sich einen Kompromiss überlegen und einen gut definierten Prozess festlegen, wie Daten aus diesen Quellen reproduziert werden können, wenn eine Datenwiederherstellung erforderlich ist. Wenn Sie beispielsweise Daten von Amazon S3 in ein Data Warehouse (wie Amazon Redshift) oder einen MapReduce Cluster (wie Amazon EMR) geladen haben, um diese Daten zu analysieren, kann dies ein Beispiel für Daten sein, die aus anderen Quellen reproduziert werden können. Solange die Ergebnisse dieser Analysen entweder irgendwo gespeichert oder reproduzierbar sind, würden Sie keinen Datenverlust aufgrund eines Fehlers im Data Warehouse oder Cluster erleiden. MapReduce Andere Beispiele, die aus Quellen reproduziert werden können, sind Caches (wie Amazon ElastiCache) oder RDS Read Replicas.

5. Legen Sie eine Kadenz für die Sicherung von Daten fest. Das Erstellen von Backups von Datenquellen ist ein periodischer Vorgang, und die Häufigkeit sollte davon abhängen. RPO

Aufwand für den Implementierungsplan: Mittel.

Ressourcen

Zugehörige bewährte Methoden:

[REL13-BP01 Definieren Sie Wiederherstellungsziele für Ausfallzeiten und Datenverlust](#)

[REL13-BP02 Verwenden Sie definierte Wiederherstellungsstrategien, um die Wiederherstellungsziele zu erreichen](#)

Zugehörige Dokumente:

- [Was ist AWS Backup?](#)
- [Was ist AWS DataSync?](#)
- [Was ist Volume Gateway?](#)
- [APNPartner: Partner, die beim Backup helfen können](#)
- [AWS Marketplace: Für die Sicherung geeignete Produkte](#)
- [EBSAmazon-Schnappschüsse](#)
- [Amazon sichern EFS](#)
- [Amazon FSx für Windows File Server sichern](#)
- [Backup und Wiederherstellung ElastiCache für Redis](#)
- [Creating a DB Cluster Snapshot in Neptune](#)
- [Creating a DB Snapshot](#)
- [Eine EventBridge Regel erstellen, die nach einem Zeitplan ausgelöst wird](#)
- [Cross-Region Replication with Amazon S3](#)
- [EFS-bis- EFS AWS Backup](#)
- [Exportieren von Protokolldaten nach Amazon S3](#)
- [Object lifecycle management](#)
- [On-Demand-Backup und Wiederherstellung für DynamoDB](#)
- [oint-in-timeP-Wiederherstellung für DynamoDB](#)
- [Arbeiten mit Amazon OpenSearch Service Index Snapshots](#)

- [Was ist AWS Elastic Disaster Recovery?](#)

Zugehörige Videos:

- [AWS re:Invent 2021 — Backup, Disaster Recovery und Ransomware-Schutz mit AWS](#)
- [AWS Backup Demo: Konto- und regionsübergreifendes Backup](#)
- [AWS re:Invent 2019: Tiefer Einblick in, ft. AWS Backup Rackspace \(\) STG341](#)

Zugehörige Beispiele:

- [Well-Architected Lab — Implementierung einer bidirektionalen regionsübergreifenden Replikation \(\) CRR für Amazon S3](#)
- [Well-Architected Lab: Testen von Backup und Wiederherstellung von Daten](#)
- [Well-Architected Lab: Backups und Wiederherstellung mit Failback für Analytics-Workload](#)
- [Well-Architected Lab: Notfallwiederherstellung – Backup und Wiederherstellung](#)

## REL09-BP02 Sicheres und Verschlüsseln von Backups

Kontrollieren und erkennen Sie den Zugriff auf Backups durch eine Authentifizierung und Autorisierung. Vermeiden und erkennen Sie mittels Verschlüsselung Beeinträchtigungen der Datenintegrität von Backups.

Typische Anti-Muster:

- Derselbe Zugriff auf die Sicherungen und die automatisierte Wiederherstellung wie auf die Daten.
- Keine Verschlüsselung der Sicherungen.

Vorteile der Nutzung dieser bewährten Methode: Die Absicherung Ihrer Backups verhindert die Manipulation der Daten und die Verschlüsselung der Daten verhindert den Zugriff auf diese Daten, wenn sie versehentlich offengelegt werden.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Hoch

## Implementierungsleitfaden

Steuern und erkennen Sie den Zugriff auf Backups mithilfe von Authentifizierung und Autorisierung, z. B. (). AWS Identity and Access Management IAM Vermeiden und erkennen Sie mittels Verschlüsselung Beeinträchtigungen der Datenintegrität von Backups.

Amazon S3 unterstützt mehrere Verschlüsselungsmethoden für Daten im Ruhezustand. Mithilfe der serverseitigen Verschlüsselung akzeptiert Amazon S3 Ihre Objekte als unverschlüsselte Daten und sorgt für ihre Verschlüsselung bei der Speicherung. Bei der clientseitigen Verschlüsselung ist Ihre Workload-Anwendung für die Verschlüsselung der Daten verantwortlich, bevor sie an Amazon S3 gesendet werden. Bei beiden Methoden können Sie AWS Key Management Service (AWS KMS) verwenden, um den Datenschlüssel zu erstellen und zu speichern, oder Sie können Ihren eigenen Schlüssel angeben, für den Sie dann verantwortlich sind. Mit dieser AWS KMS Methode können Sie Richtlinien festlegen, die festlegen, wer IAM auf Ihre Datenschlüssel und entschlüsselten Daten zugreifen kann und wer nicht.

Wenn Sie sich für Amazon entschieden haben RDS, Ihre Datenbanken zu verschlüsseln, werden auch Ihre Backups verschlüsselt. DynamoDB-Sicherungen werden immer verschlüsselt. Bei der Verwendung werden alle Daten AWS Elastic Disaster Recovery, die übertragen und gespeichert werden, verschlüsselt. Mit Elastic Disaster Recovery können Daten im Ruhezustand entweder mit dem standardmäßigen Amazon EBS Encryption Volume Encryption Key oder einem benutzerdefinierten, vom Kunden verwalteten Schlüssel verschlüsselt werden.

## Implementierungsschritte

1. Verwenden Sie eine Verschlüsselung für jeden Datenspeicher. Wenn Ihre Quelldaten verschlüsselt sind, wird die Sicherung ebenfalls verschlüsselt.
  - [Verwenden Sie Verschlüsselung in AmazonRDS.](#) . Sie können die Verschlüsselung im Ruhezustand AWS Key Management Service beim Erstellen einer RDS Instanz konfigurieren.
  - [Verwenden Sie Verschlüsselung auf EBS Amazon-Volumes.](#) . Während der Erstellung von Volumes können Sie eine Standardverschlüsselung konfigurieren oder einen eindeutigen Schlüssel angeben.
  - Verwenden Sie die erforderliche [Amazon DynamoDB-Verschlüsselung](#). DynamoDB verschlüsselt alle Daten im Ruhezustand. Sie können entweder einen AWS eigenen AWS KMS Schlüssel oder einen AWS verwalteten KMS Schlüssel verwenden und dabei einen Schlüssel angeben, der in Ihrem Konto gespeichert ist.
  - [Verschlüsseln Sie Ihre bei Amazon EFS gespeicherten Daten.](#) Konfigurieren Sie die Verschlüsselung beim Erstellen des Dateisystems.

- Konfigurieren Sie die Verschlüsselung in den Quell- und Zielregionen. Sie können die Verschlüsselung im Ruhezustand in Amazon S3 mithilfe von Schlüsseln konfigurieren KMS, die Schlüssel sind jedoch regionsspezifisch. Sie können die Zielschlüssel angeben, während Sie die Replikation konfigurieren.
  - Wählen Sie, ob Sie die standardmäßige oder die benutzerdefinierte [EBS Amazon-Verschlüsselung für Elastic Disaster Recovery](#) verwenden möchten. Mit dieser Option werden Ihre replizierten Daten im Ruhezustand auf den Staging-Area Subnetz-Datenträgern und den replizierten Datenträgern verschlüsselt.
2. Implementieren Sie Rechte mit geringsten Berechtigungen für den Zugriff auf Ihre Backups. Begrenzen Sie den Zugriff auf die Backups, Snapshots und Replikate anhand [bewährter Methoden im Bereich Sicherheit](#).

## Ressourcen

### Zugehörige Dokumente:

- [AWS Marketplace: Für die Sicherung geeignete Produkte](#)
- [EBS Amazon-Verschlüsselung](#)
- [Amazon S3: Daten durch Verschlüsselung schützen](#)
- [CRR Zusätzliche Konfiguration: Replizieren von Objekten, die mit serverseitiger Verschlüsselung \(SSE\) erstellt wurden, mithilfe von Verschlüsselungsschlüsseln, die in gespeichert sind AWS KMS](#)
- [DynamoDB-Verschlüsselung in Ruhezustand](#)
- [RDS Amazon-Ressourcen verschlüsseln](#)
- [Verschlüsseln von Daten und Metadaten in Amazon EFS](#)
- [Verschlüsselung für Backups in AWS](#)
- [Managing Encrypted Tables](#)
- [Säule der Sicherheit — AWS Well-Architected Framework](#)
- [Was ist? AWS Elastic Disaster Recovery](#)

### Zugehörige Beispiele:

- [Well-Architected Lab — Implementierung einer bidirektionalen regionsübergreifenden Replikation \(\) CRR für Amazon S3](#)



## REL09-BP03 Automatische Datensicherung durchführen

Konfigurieren Sie Backups so, dass sie automatisch auf der Grundlage eines regelmäßigen Zeitplans erstellt werden, der vom Recovery Point Objective (RPO) oder von Änderungen im Datensatz abhängig ist. Kritische Datensätze, bei denen Datenverlust vermieden werden sollte, müssen regelmäßig automatisch gesichert werden, wohingegen weniger kritische Daten, bei denen ein gewisser Verlust akzeptabel ist, weniger häufig gesichert werden können.

Gewünschtes Ergebnis: Ein automatisierter Prozess, der Backups von Datenquellen in einem festgelegten Rhythmus erstellt.

Typische Anti-Muster:

- Sicherungen werden manuell durchgeführt.
- Es werden Ressourcen mit Sicherungsfunktionen verwendet, die Sicherung wird aber nicht in die Automatisierung einbezogen.

Vorteile der Einführung dieser bewährten Methode: Durch die Automatisierung von Backups wird anhand Ihrer Daten überprüft, ob Backups regelmäßig erstellt werden RPO, und Sie werden benachrichtigt, wenn sie nicht erstellt werden.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Mittel

Implementierungsleitfaden

AWS Backup kann verwendet werden, um automatisierte Datensicherungen verschiedener AWS Datenquellen zu erstellen. RDS Amazon-Instances können fast ununterbrochen alle fünf Minuten gesichert werden, und Amazon S3-Objekte können fast ununterbrochen alle fünfzehn Minuten gesichert werden, sodass eine point-in-time Wiederherstellung (PITR) bis zu einem bestimmten Zeitpunkt im Backup-Verlauf möglich ist. Für andere AWS Datenquellen, wie EBS Amazon-Volumes, Amazon DynamoDB-Tabellen oder FSx Amazon-Dateisysteme, AWS Backup können automatische Backups bis zu stündlich ausgeführt werden. Diese Dienste bieten auch native Backup-Funktionen. AWS Zu den Services, die automatisiertes Backup mit point-in-time Wiederherstellung anbieten, gehören [Amazon DynamoDB](#), [RDS](#), [Amazon](#) und [Amazon Keyspaces \(für Apache Cassandra\)](#) — diese können zu einem bestimmten Zeitpunkt innerhalb des Backup-Verlaufs wiederhergestellt werden. Die meisten anderen AWS -Datenspeicher-Services bieten die Möglichkeit, stündliche periodische Backups einzuplanen.

Amazon RDS und Amazon DynamoDB bieten kontinuierliche Backups mit point-in-time Wiederherstellung. Die Amazon S3-Versionsverwaltung erfolgt nach der Aktivierung automatisch.

[Amazon Data Lifecycle Manager](#) kann verwendet werden, um das Erstellen, Kopieren und Löschen von EBS Amazon-Snapshots zu automatisieren. Es kann auch das Erstellen, Kopieren, Deaktivieren und Abmelden von Amazon Machine Images (AMIs) und den EBS ihnen zugrunde liegenden Amazon-Snapshots automatisieren. EBS

AWS Elastic Disaster Recovery ermöglicht eine kontinuierliche Replikation auf Blockebene von der Quellumgebung (vor Ort oder) bis zur Ziel-Wiederherstellungsregion. AWS Point-in-time EBS Amazon-Snapshots werden automatisch vom Service erstellt und verwaltet.

AWS Backup Bietet eine vollständig verwaltete, richtlinienbasierte Backup-Lösung für einen zentralen Überblick über Ihre Backup-Automatisierung und -Historie. Diese zentralisiert und automatisiert die Sicherung von Daten in mehreren AWS -Services in der Cloud sowie On-Premises mithilfe des AWS Storage Gateway.

Zusätzlich zur Versionsverwaltung bietet Amazon S3 eine Replikationsfunktion. Der gesamte S3-Bucket kann automatisch in einen anderen Bucket in einer anderen AWS-Region repliziert werden.

#### Implementierungsschritte

1. Identifizieren Sie Datenquellen, die derzeit manuell gesichert werden. Weitere Details erhalten Sie unter [REL09-BP01 Identifizieren und sichern Sie alle Daten, die gesichert werden müssen, oder reproduzieren Sie die Daten aus Quellen](#).
2. Ermitteln Sie das RPO für die Arbeitslast. Weitere Details erhalten Sie unter [REL13-BP01 Definieren Sie Wiederherstellungsziele für Ausfallzeiten und Datenverlust](#).
3. Verwenden Sie eine automatisierte Backup-Lösung oder einen verwalteten Service. AWS Backup ist ein vollständig verwalteter Service, der es einfach macht, den [Datenschutz AWS dienstübergreifend, in der Cloud und vor Ort zu zentralisieren und zu automatisieren](#). Mithilfe von Backup-Plänen in AWS Backup erstellen Sie Regeln, die die zu sichernden Ressourcen und die Häufigkeit, mit der diese Backups erstellt werden sollen, festlegen. Diese Häufigkeit sollte anhand der in Schritt 2 RPO festgelegten Daten angegeben werden. Praktische Anleitungen zum Erstellen automatisierter Backups mit AWS Backup finden Sie unter [Testen der Backup und Wiederherstellung von Daten](#). Die meisten AWS Dienste, die Daten speichern, bieten native Backup-Funktionen. RDS kann beispielsweise für automatisierte Backups mit point-in-time Recovery (PITR) genutzt werden.
4. Für Datenquellen, die nicht von einer automatisierten Backup-Lösung oder einem verwalteten Service unterstützt werden, wie z. B. On-Premises-Datenquellen oder Warteschlangen, sollten Sie eine zuverlässige Lösung eines Drittanbieters verwenden, um automatische Backups zu erstellen. Alternativ können Sie dafür eine Automatisierung erstellen, indem Sie das AWS CLI oder SDKs

verwenden. Sie können AWS Lambda Functions oder verwenden AWS Step Functions , um die Logik zu definieren, die bei der Erstellung einer Datensicherung erforderlich ist, und Amazon verwenden, EventBridge um sie mit einer Häufigkeit aufzurufen, die auf Ihrem RPO basiert.

Aufwand für den Implementierungsplan: Niedrig.

Ressourcen

Zugehörige Dokumente:

- [APNPartner: Partner, die bei der Datensicherung helfen können](#)
- [AWS Marketplace: Für die Sicherung geeignete Produkte](#)
- [Eine EventBridge Regel erstellen, die nach einem Zeitplan ausgelöst wird](#)
- [Was ist AWS Backup?](#)
- [Was ist AWS Step Functions?](#)
- [Was ist AWS Elastic Disaster Recovery?](#)

Zugehörige Videos:

- [AWS re:Invent 2019: Tiefer Einblick in AWS Backup, ft. Rackspace \(\) STG341](#)

Zugehörige Beispiele:

- [Well-Architected Lab: Testen von Backup und Wiederherstellung von Daten](#)

REL09-BP04 Führen Sie eine regelmäßige Wiederherstellung der Daten durch, um die Integrität und die Prozesse des Backups zu überprüfen

Stellen Sie sicher, dass Ihre Implementierung des Backup-Prozesses Ihre Ziele für die Wiederherstellungszeit (RTO) und die Zielvorgaben für den Wiederherstellungspunkt (RPO) erfüllt, indem Sie einen Wiederherstellungstest durchführen.

Gewünschtes Ergebnis: Daten aus Backups werden regelmäßig mithilfe genau definierter Mechanismen wiederhergestellt, um zu überprüfen, ob die Wiederherstellung innerhalb des festgelegten Wiederherstellungszeitziels (RTO) für den Workload möglich ist. Stellen Sie sicher, dass die Wiederherstellung aus einem Backup zu einer Ressource führt, die die Originaldaten enthält,

ohne dass diese beschädigt oder unzugänglich sind und dass Daten innerhalb des Ziels für den Wiederherstellungspunkt verloren gehen (RPO).

Typische Anti-Muster:

- Wiederherstellung eines Backups ohne Abfrage oder Abruf von Daten, um zu überprüfen, ob die Wiederherstellung funktionsfähig ist.
- Es wird angenommen, dass ein Backup existiert.
- Es wird angenommen, dass das Backup eines System voll funktionsfähig ist und Daten daraus wiederhergestellt werden können.
- Es wird davon ausgegangen, dass die Zeit für die Wiederherstellung oder Wiederherstellung von Daten aus einem Backup innerhalb der RTO für die Arbeitslast vorgesehenen Zeit liegt.
- Unter der Annahme, dass die in der Sicherung enthaltenen Daten in den RPO für die Arbeitslast vorgesehenen Bereich fallen
- Wiederherstellung bei Bedarf, ohne ein Runbook zu verwenden oder außerhalb eines etablierten automatisierten Verfahrens.

Vorteile der Einführung dieser bewährten Methode: Durch das Testen der Wiederherstellung der Backups wird überprüft, ob Daten bei Bedarf wiederhergestellt werden können, ohne dass man sich Sorgen machen muss, dass Daten fehlen oder beschädigt sein könnten, dass die Wiederherstellung und Wiederherstellung innerhalb der RTO für die Arbeitslast möglich ist und dass Datenverlust innerhalb der RPO für die Arbeitslast möglich ist.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Mittel

Implementierungsleitfaden

Das Testen der Sicherungs- und Wiederherstellungsfunktionen stärkt das Vertrauen in die Fähigkeit zur Durchführung dieser Aktionen während eines Ausfalls. Stellen Sie regelmäßig Backups an einem neuen Speicherort wieder her und führen Sie Tests aus, um die Datenintegrität zu überprüfen. Zu den häufigsten Tests, die durchgeführt werden sollten, gehört die Überprüfung, ob alle Daten verfügbar, nicht beschädigt oder zugänglich sind und ob Datenverlust in den Rahmen der RPO Arbeitslast fällt. Solche Tests können auch dabei helfen, festzustellen, ob die Wiederherstellungsmechanismen schnell genug sind, um den Anforderungen der Arbeitslast gerecht zu werden. RTO

Damit AWS können Sie eine Testumgebung einrichten und Ihre Backups wiederherstellen, um die RPO Funktionen zu bewerten RTO und Tests auf Dateninhalt und Integrität durchzuführen.

Darüber hinaus ermöglichen Amazon RDS und Amazon DynamoDB point-in-time Recovery (PITR). Durch die kontinuierliche Sicherung können Sie Ihren Datensatz in den Zustand zurücksetzen, in dem er sich an einem bestimmten Datum und zu einer bestimmten Uhrzeit befand.

Wenn alle Daten verfügbar sind, nicht beschädigt sind, zugänglich sind und jeder Datenverlust in den Rahmen der Arbeitslast RPO fällt. Solche Tests können auch dabei helfen, festzustellen, ob die Wiederherstellungsmechanismen schnell genug sind, um den Anforderungen der Arbeitslast gerecht zu werden. RTO

AWS Elastic Disaster Recovery bietet kontinuierliche point-in-time Wiederherstellungs-Snapshots von EBS Amazon-Volumes. Bei der Replikation der Quellserver werden die Status point-in-time auf der Grundlage der konfigurierten Richtlinie im Laufe der Zeit aufgezeichnet. Elastic Disaster Recovery hilft Ihnen, die Integrität dieser Snapshots zu überprüfen, indem Sie Instances zu Test- und Übungszwecken starten, ohne den Datenverkehr weiterzuleiten.

### Implementierungsschritte

1. Identifizieren Sie Datenquellen, die derzeit gesichert werden, und den Speicherort dieser Backups. Eine Anleitung zur Implementierung finden Sie unter [REL09-BP01 Identifizieren und sichern Sie alle Daten, die gesichert werden müssen, oder reproduzieren Sie die Daten aus Quellen](#).
2. Legen Sie für jede Datenquelle Kriterien für die Datenvalidierung fest. Verschieden Datentypen können unterschiedliche Eigenschaften aufweisen und somit auch unterschiedliche Validierungsmechanismen erfordern. Überlegen Sie, wie diese Daten validiert werden können, bevor Sie sie in der Produktion einsetzen. Häufig werden für die Datenvalidierung Daten- und Sicherheitseigenschaften wie Datentyp, Format, Prüfsumme, Größe oder eine Kombination dieser Eigenschaften mit einer benutzerdefinierten Validierungslogik verwendet. Ein Beispiel hierfür wäre der Vergleich der Prüfsummenwerte zwischen der wiederhergestellten Ressource und der Datenquelle zum Zeitpunkt der Erstellung des Backups.
3. Festlegung RTO und RPO Wiederherstellung der Daten auf der Grundlage der Datenkritikalität. Eine Anleitung zur Implementierung finden Sie unter [REL13-BP01 Definieren Sie Wiederherstellungsziele für Ausfallzeiten und Datenverlust](#).
4. Bewerten Sie Ihre Wiederherstellungsfunktion. Überprüfen Sie Ihre Sicherungs- und Wiederherstellungsstrategie, um herauszufinden, ob sie Ihren Anforderungen gerecht wird. RPO, RTO und passen Sie die Strategie gegebenenfalls an. Mithilfe von [AWS Resilience Hub](#) können Sie eine Bewertung Ihrer Workload durchführen. Bei der Bewertung wird Ihre Anwendungskonfiguration anhand der Stabilitätsrichtlinie bewertet und es wird berichtet, ob Ihre RTO RPO Ziele erreicht werden können.

5. Führen Sie eine Testwiederherstellung mit derzeit etablierten Prozessen durch, die in der Produktion für die Datenwiederherstellung verwendet werden. Diese Prozesse hängen davon ab, wie die ursprüngliche Datenquelle gesichert wurde sowie vom Format und der Speicherung des Backups selbst oder davon, ob die Daten aus anderen Quellen reproduziert werden. Wenn Sie beispielsweise einen verwalteten Service wie [AWS Backup verwenden, kann es sich einfach um das Wiederherstellen des Backups auf einer neuen Ressource handeln](#). Wenn Sie AWS Elastic Disaster Recovery verwendet haben, können Sie [eine Wiederherstellungsübung starten](#).
6. Überprüfen Sie die Datenwiederherstellung von der wiederhergestellten Ressource anhand von Kriterien, die Sie zuvor für die Datenvalidierung festgelegt haben. Enthalten die wiederhergestellten Daten den neuesten Datensatz bzw. das neueste Element zum Zeitpunkt des Backups? Fallen diese Daten in den Bereich RPO für den Workload?
7. Messen Sie die Zeit, die für Wiederherstellung und Wiederherstellung benötigt wird, und vergleichen Sie sie mit der von Ihnen festgestellten ZeitRTO. Fällt dieser Prozess unter RTO die Arbeitslast? Vergleichen Sie beispielsweise den Zeitstempel des Starts des Wiederherstellungsprozesses und des Abschlusses der Wiederherstellungsbewertung, um zu ermitteln, wie lange dieser Prozess dauert. Alle AWS API Anrufe sind mit einem Zeitstempel versehen und diese Informationen sind in verfügbar. [AWS CloudTrail](#) Während diese Informationen Details dazu liefern können, wann der Wiederherstellungsprozess gestartet wurde, sollte der End-Zeitstempel für den Abschluss der Validierung von der Validierungslogik aufgezeichnet werden. Wenn Sie einen automatisierten Prozess verwenden, können Services wie [Amazon DynamoDB](#) verwendet werden, um diese Informationen zu speichern. Darüber hinaus bieten viele AWS Dienste einen Ereignisverlauf, der Informationen mit Zeitstempel enthält, wann bestimmte Aktionen stattgefunden haben. Innerhalb AWS Backup werden Sicherungs- und Wiederherstellungsaktionen als Jobs bezeichnet. Diese Jobs enthalten Zeitstempelinformationen als Teil der Metadaten, anhand derer die für die Wiederherstellung und Wiederherstellung benötigte Zeit gemessen werden kann.
8. Informieren Sie die Beteiligten, wenn die Datenvalidierung fehlschlägt oder wenn die für die Wiederherstellung und Wiederherstellung erforderliche Zeit die RTO für die Arbeitslast festgelegte Zeit überschreitet. Bei der Implementierung von Automatisierung zu diesem Zweck, [wie in diesem Lab](#), können Dienste wie Amazon Simple Notification Service (AmazonSNS) verwendet werden, um Push-Benachrichtigungen wie E-Mails oder an Stakeholder SMS zu senden. [Diese Nachrichten können auch in Messaging-Anwendungen wie Amazon Chime, Slack oder Microsoft Teams veröffentlicht oder zum Erstellen von Aufgaben wie OpsItems mit AWS Systems Manager verwendet werden](#). OpsCenter
9. Automatisieren Sie diesen Prozess so, dass er regelmäßig ausgeführt wird. Beispielsweise AWS Step Functions können Dienste wie AWS Lambda oder eine State Machine in verwendet

werden, um die Wiederherstellungs- und Wiederherstellungsprozesse zu automatisieren, und Amazon EventBridge kann verwendet werden, um diesen Automatisierungs-Workflow regelmäßig aufzurufen, wie im Architekturdiagramm unten dargestellt. Erfahren Sie, wie Sie die [Validierung der Datenwiederherstellung mit AWS Backup automatisieren](#) können. Darüber hinaus bietet [dieses Well-Architected-Lab](#) praktische Erfahrungen mit einer Möglichkeit, mehrere der hier beschriebenen Schritte zu automatisieren.

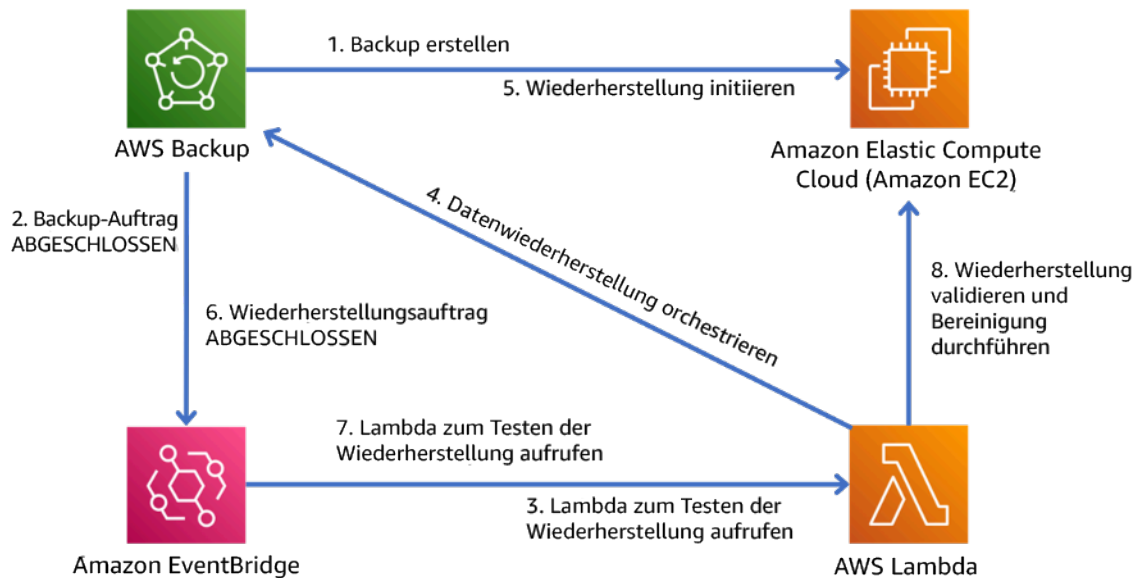


Abbildung 9. Ein automatisierter Sicherungs- und Wiederherstellungsprozess

Aufwand für den Implementierungsplan: Mittel bis hoch, abhängig von der Komplexität der Validierungskriterien.

Ressourcen

Zugehörige Dokumente:

- [Automatisieren Sie die Validierung der Datenwiederherstellung mit AWS Backup](#)
- [APNPartner: Partner, die bei der Datensicherung helfen können](#)
- [AWS Marketplace: Für die Sicherung geeignete Produkte](#)
- [Eine EventBridge Regel erstellen, die nach einem Zeitplan ausgelöst wird](#)
- [On-Demand-Backup und Wiederherstellung für DynamoDB](#)
- [Was ist AWS Backup?](#)
- [Was ist AWS Step Functions?](#)

- [Was ist AWS Elastic Disaster Recovery](#)
- [AWS Elastic Disaster Recovery](#)

Zugehörige Beispiele:

- [Well-Architected Lab: Testen von Backup und Wiederherstellung von Daten](#)

## REL10. Wie wird die Fehlerisolierung zum Schützen der Workload verwendet?

Fehlerisolierte Grenzen beschränken die Auswirkungen eines Fehlers innerhalb einer Workload auf eine begrenzte Anzahl von Komponenten. Komponenten außerhalb der Grenze sind von dem Ausfall nicht betroffen. Durch die Verwendung mehrerer fehlerisolierter Grenzen können Sie die Auswirkungen auf Ihre Workload einschränken.

Bewährte Methoden

- [REL10-BP01 Stellen Sie den Workload an mehreren Standorten bereit](#)
- [REL10-BP02 Wählen Sie die geeigneten Standorte für Ihren Einsatz an mehreren Standorten](#)
- [REL10-BP03 Automatisieren Sie die Wiederherstellung von Komponenten, die auf einen einzigen Standort beschränkt sind](#)
- [REL10-BP04 Verwenden Sie Schottarchitekturen, um den Wirkungsbereich zu begrenzen](#)

REL10-BP01 Stellen Sie den Workload an mehreren Standorten bereit

Verteilen Sie die Workload-Daten und -Ressourcen über mehrere Availability Zones oder ggf. über mehrere AWS-Regionen. Die Standorte können so vielfältig wie nötig sein.

Eines der Grundprinzipien für das Servicedesign AWS ist die Vermeidung einzelner Ausfallpunkte in der zugrunde liegenden physischen Infrastruktur. Dies treibt uns an, Software und Systeme zu entwickeln, die mehrere Availability Zones verwenden und Sicherheit gegen den Ausfall einer einzelnen Region bieten. Außerdem sollen Systeme sicher gegen den Ausfall einzelner Datenverarbeitungsknoten, einzelner Speicher-Volumes oder einzelner Instances einer Datenbank sein. Beim Aufbau eines Systems, das auf redundanten Komponenten basiert, muss sichergestellt werden, dass die Komponenten unabhängig voneinander und im Fall von AWS-Regionen autonom arbeiten. Die Vorteile theoretischer Verfügbarkeitsberechnungen mit redundanten Komponenten sind nur anwendbar, wenn diese Voraussetzung erfüllt ist.

Verfügbarkeitszonen ( ) AZs



AWS-Regionen bestehen aus mehreren Availability Zones, die so konzipiert sind, dass sie voneinander unabhängig sind. Die einzelnen Availability Zones sind durch eine deutliche physische Distanz voneinander getrennt, um so korrelierende Fehlerszenarios aufgrund von Umweltgefahren wie Feuer, Überflutungen und Tornados zu vermeiden. Jede Availability Zone verfügt auch über eine unabhängige physische Infrastruktur: spezielle Verbindungen zur Stromversorgung, zu unabhängigen Backup-Stromquellen, unabhängigen mechanischen Services und unabhängiger Netzwerkkonnektivität innerhalb der Availability Zone und darüber hinaus. Dieses Design beschränkt Fehler in einem dieser Systeme ausschließlich auf die betroffene AZ. Obwohl die Availability Zones geografisch getrennt sind, befinden sie sich in derselben Region, was Netzwerke mit hohem Durchsatz und niedriger Latenz ermöglicht. Die gesamte Anlage AWS-Region (über alle Availability Zones hinweg, bestehend aus mehreren physisch unabhängigen Rechenzentren) kann als ein einziges logisches Bereitstellungsziel für Ihren Workload behandelt werden, einschließlich der Fähigkeit, Daten synchron zu replizieren (z. B. zwischen Datenbanken). Und so können Sie Availability Zones in einer Aktiv/Aktiv- oder Aktiv/Standby-Konfiguration nutzen.

Availability Zones sind unabhängig und daher erhöht sich die Workload-Verfügbarkeit, wenn die Workload mehrere Zonen umfasst. Einige AWS Dienste (einschließlich der EC2 Amazon-Instance-Datenebene) werden als streng zonale Dienste bereitgestellt, wobei sie das Schicksal mit der Availability Zone, in der sie sich befinden, geteilt haben. EC2-Amazon-Instanzen in AZs den anderen sind jedoch nicht betroffen und funktionieren weiterhin. Wenn ein Ausfall in einer Availability Zone zum Ausfall einer Amazon Aurora-Datenbank führt, kann eine Aurora-Lesereplikat-Instance in einer nicht betroffenen AZ automatisch zur primären Instance hochgestuft werden. Regionale AWS - Services wie Amazon DynamoDB verwenden dagegen intern mehrere Availability Zones in einer Aktiv/Aktiv-Konfiguration, um die Verfügbarkeitsdesignziele für diesen Service zu erreichen, ohne dass Sie die AZ-Platzierung konfigurieren müssen.

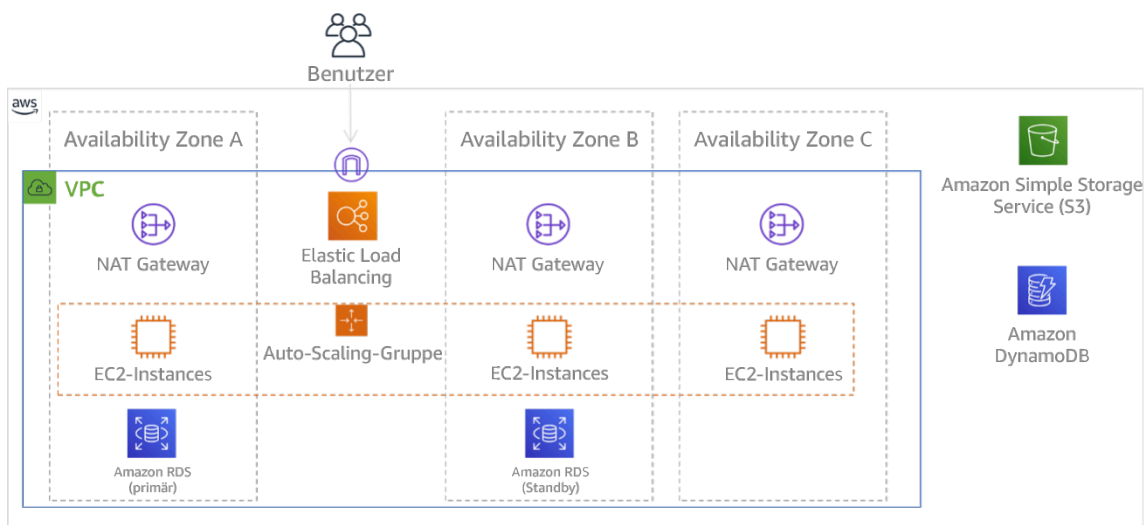


Abbildung 9: Mehrstufige Architektur, die in drei Availability Zones bereitgestellt wird. Amazon S3 und Amazon DynamoDB nutzen immer automatisch mehrere AZs. Die wird ELB auch in allen drei Zonen eingesetzt.

Während AWS Kontrollebenen in der Regel die Möglichkeit bieten, Ressourcen innerhalb der gesamten Region (mehrere Availability Zones) zu verwalten, haben bestimmte Kontrollebenen (einschließlich Amazon EC2 und AmazonEBS) die Möglichkeit, Ergebnisse nach einer einzigen Availability Zone zu filtern. Wenn dies erledigt ist, wird die Anfrage nur in der angegebenen Availability Zone verarbeitet; dies reduziert die Wahrscheinlichkeit von Ausfällen in anderen Availability Zones. Dieses AWS CLI Beispiel zeigt, wie EC2 Amazon-Instance-Informationen nur aus der Availability Zone us-east-2c abgerufen werden:

```
AWS ec2 describe-instances --filters Name=availability-zone,Values=us-east-2c
```

## AWS Lokale Zonen

AWS Local Zones verhalten sich insofern ähnlich wie Availability Zones AWS-Region in ihren jeweiligen Zonen, da sie als Platzierungsort für zonale AWS Ressourcen wie Subnetze und EC2 Instances ausgewählt werden können. Das Besondere an ihnen ist, dass sie sich nicht in den zugehörigen Zentren AWS-Region, sondern in der Nähe großer Bevölkerungsgruppen, Branchen und IT-Zentren befinden, wo es heute noch keine AWS-Region gibt. Sie sorgen dennoch für eine sichere Verbindung zwischen lokalen Workloads in der lokalen Zone und Workloads in der AWS-Region. Sie sollten AWS Local Zones verwenden, um Workloads mit geringen Latenzanforderungen näher an Ihren Benutzern bereitzustellen.

## Amazon Global Edge Network

Das Amazon Global Edge Network besteht aus Edge-Standorten in Städten auf der ganzen Welt. Amazon CloudFront nutzt dieses Netzwerk, um Endbenutzern Inhalte mit geringerer Latenz bereitzustellen. AWS Mit Global Accelerator können Sie Ihre Workload-Endpunkte an diesen Edge-Standorten einrichten, um das Onboarding in das AWS globale Netzwerk in der Nähe Ihrer Benutzer zu ermöglichen. Amazon API Gateway ermöglicht Edge-optimierte API Endgeräte mithilfe einer CloudFront Distribution, um den Kundenzugriff über den nächstgelegenen Edge-Standort zu erleichtern.

## AWS-Regionen

AWS-Regionen sind so konzipiert, dass sie unabhängig sind. Um also einen Ansatz für mehrere Regionen zu verwenden, würden Sie für jede Region spezielle Kopien der Services bereitstellen.

Bei Strategien zur Notfallwiederherstellung ist ein regionsübergreifender Ansatz üblich, um die Wiederherstellungsziele einzuhalten, wenn einmalige umfangreiche Ereignisse auftreten. Weitere Informationen zu diesen Strategien finden Sie unter [Planung der Notfallwiederherstellung](#). Hier konzentrieren wir uns jedoch stattdessen auf die Verfügbarkeit, das heißt, im Laufe der Zeit soll ein durchschnittliches Verfügbarkeitsziel erreicht werden. Um eine hohe Verfügbarkeit zu erzielen, wird eine Architektur mit mehreren Regionen im Allgemeinen so konzipiert, dass sie aktiv/aktiv ist, wobei jede Servicekopie (in ihrer jeweiligen Region) aktiv ist (Bearbeitung von Anfragen).

### Empfehlung

Die Zuverlässigkeitsziele für die meisten Workloads können mithilfe einer Multi-AZ-Strategie innerhalb einer einzelnen AWS-Region erfüllt werden. Architekturen, die sich über mehrere Regionen erstrecken, sollten nur in Betracht gezogen werden, wenn Workloads extreme Verfügbarkeitsanforderungen oder andere Geschäftsziele haben, die eine Architektur mit mehreren Regionen erfordern.

AWS bietet Ihnen die Möglichkeit, Dienste regionsübergreifend zu betreiben. AWS Bietet beispielsweise eine kontinuierliche, asynchrone Datenreplikation von Daten mithilfe von Amazon Simple Storage Service (Amazon S3) Replication, Amazon RDS Read Replicas (einschließlich Aurora Read Replicas) und Amazon DynamoDB Global Tables. Durch die kontinuierliche Replikation stehen Versionen Ihrer Daten in jeder Ihrer aktiven Regionen nahezu sofort zur Verfügung.

Mithilfe AWS CloudFormation können Sie Ihre Infrastruktur definieren und sie konsistent auf allen Ebenen einsetzen. AWS-Konten AWS-Regionen Und AWS CloudFormation StackSets erweitert diese Funktionalität, indem es Ihnen ermöglicht, AWS CloudFormation Stacks für mehrere Konten und Regionen mit einem einzigen Vorgang zu erstellen, zu aktualisieren oder zu löschen. Für EC2 Amazon-Instance-Bereitstellungen wird ein AMI (Amazon Machine Image) verwendet, um Informationen wie Hardwarekonfiguration und installierte Software bereitzustellen. Sie können eine Amazon EC2 Image Builder Builder-Pipeline implementieren, die die AMIs benötigten Daten erstellt und diese in Ihre aktiven Regionen kopiert. Dadurch wird sichergestellt, dass diese Golden AMIs über alles verfügen, was Sie für die Bereitstellung und Skalierung Ihrer Arbeitslast in jeder neuen Region benötigen.

Um den Verkehr weiterzuleiten, ermöglichen sowohl Amazon Route 53 als auch AWS Global Accelerator die Definition von Richtlinien, die festlegen, welche Benutzer zu welchem aktiven regionalen Endpunkt gehen. Mit Global Accelerator richten Sie eine Datenverkehrswahl ein, um den Prozentsatz des Datenverkehrs zu steuern, der an jeden Anwendungsendpunkt geleitet wird.

Route 53 unterstützt diesen prozentualen Ansatz sowie mehrere andere verfügbare Richtlinien, einschließlich Richtlinien, die auf geografischer Nähe und Latenz basieren. Global Accelerator nutzt automatisch das umfangreiche Netzwerk von AWS Edge-Servern, um den Datenverkehr so schnell wie möglich in den AWS Netzwerk-Backbone einzubinden, was zu geringeren Latenzen bei Anfragen führt.

Bei all diesen Funktionen bleibt die Autonomie der einzelnen Regionen gewahrt. Es gibt nur sehr wenige Ausnahmen von diesem Ansatz, einschließlich unserer Services, die globale Edge-Lieferung anbieten (wie Amazon CloudFront und Amazon Route 53), zusammen mit der Steuerungsebene für den AWS Identity and Access Management (IAM) -Service. Die meisten Services laufen vollständig innerhalb einer einzigen Region.

### On-Premises-Rechenzentrum

Für Workloads, die in einem lokalen Rechenzentrum ausgeführt werden, sollten Sie, wenn möglich, ein hybrides Erlebnis einrichten. AWS Direct Connect bietet eine dedizierte Netzwerkverbindung von Ihrem Standort aus, AWS sodass Sie in beiden Umgebungen arbeiten können.

Eine weitere Option besteht darin, AWS Infrastruktur und Dienste vor Ort mithilfe von AWS Outposts. AWS Outposts ist ein vollständig verwalteter Service, der AWS InfrastrukturAPIs, AWS Dienste und Tools auf Ihr Rechenzentrum ausdehnt. Dieselbe Hardware-Infrastruktur, die in der verwendet wurde, AWS Cloud ist in Ihrem Rechenzentrum installiert. AWS Outposts sind dann mit dem nächstgelegenen verbundenen AWS-Region. Sie können es dann AWS Outposts zur Unterstützung Ihrer Workloads mit geringer Latenz oder lokalen Datenverarbeitungsanforderungen verwenden.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Hoch

### Implementierungsleitfaden

- Verwenden Sie mehrere Availability Zones und AWS-Regionen. Verteilen Sie die Workload-Daten und -Ressourcen über mehrere Availability Zones oder ggf. über mehrere AWS-Regionen. Die Standorte können so vielfältig wie nötig sein.
  - Regionale Services werden von Haus aus in Availability Zones bereitgestellt.
    - Dazu gehören Amazon S3, Amazon DynamoDB und AWS Lambda (wenn nicht mit einem verbundenen) VPC
  - Stellen Sie Ihre Container-, Instance- und funktionsbasierten Workloads in mehreren Availability Zones bereit. Verwenden Sie Multi-AZ-Datenspeicher, einschließlich Cache. Nutzen Sie die Funktionen von Amazon EC2 Auto Scaling, Amazon ECS Task Placement, AWS Lambda Funktionskonfiguration bei der Ausführung in Ihrem VPC und ElastiCache Clustern.

- Verwenden Sie für die Bereitstellung von Auto-Scaling-Gruppen Subnetze in getrennten Availability Zones.
  - [Beispiel: Aufteilen von Instances in mehrere Availability Zones](#)
  - [Auswählen von Regionen und Availability Zones](#)
- Verwenden Sie Parameter für die ECS Aufgabenplatzierung und geben Sie DB-Subnetzgruppen an.
  - [Strategien zur ECS Aufgabenvergabe bei Amazon](#)
- Verwenden Sie Subnetze in mehreren Availability Zones, wenn Sie eine Funktion für die Ausführung in Ihrem VPC konfigurieren.
  - [Konfiguration einer AWS Lambda Funktion für den Zugriff auf Ressourcen in einem Amazon VPC](#)
- Verwenden Sie mehrere Availability Zones mit ElastiCache Clustern.
  - [Auswählen von Regionen und Availability Zones](#)
- Wenn Ihre Workload für mehrere Regionen bereitgestellt werden muss, sollten Sie sich für eine Strategie für mehrere Regionen entscheiden. Die meisten Zuverlässigkeitsanforderungen können AWS-Region mithilfe einer Strategie für mehrere Verfügbarkeitszonen innerhalb einer einzigen Lösung erfüllt werden. Verwenden Sie eine Multi-Regionen-Strategie, wenn notwendig, um Ihre Geschäftsanforderungen zu erfüllen.
  - [AWS re:Invent 2018: Architekturmuster für aktive/aktive Anwendungen mit mehreren Regionen \(09-R2\) ARC2](#)
    - Durch die Sicherung auf einem anderen System AWS-Region kann zusätzlich gewährleistet werden, dass Daten bei Bedarf verfügbar sind.
    - Für einige Workloads gibt es gesetzliche Anforderungen, die eine Multi-Regionen-Strategie erfordern.
- Bewerten AWS Outposts Sie Ihre Arbeitslast. Wenn Ihre Workload eine niedrige Latenz für Ihr On-Premises-Rechenzentrum erfordert oder lokale Datenverarbeitungsanforderungen hat. Führen Sie dann AWS Infrastruktur und Dienste vor Ort aus mit AWS Outposts
  - [Was ist AWS Outposts?](#)
- Stellen Sie fest, ob AWS Local Zones Ihnen hilft, Ihren Benutzern Service zu bieten. Wenn Sie Anforderungen mit niedriger Latenz haben, überprüfen Sie, ob sich AWS Local Zones in der Nähe Ihrer Benutzer befindet. Wenn dies der Fall ist, verwenden Sie es, um Workloads näher an diesen Benutzern bereitzustellen.
  - [AWS Local ZonesFAQ](#)

## Ressourcen

### Zugehörige Dokumente:

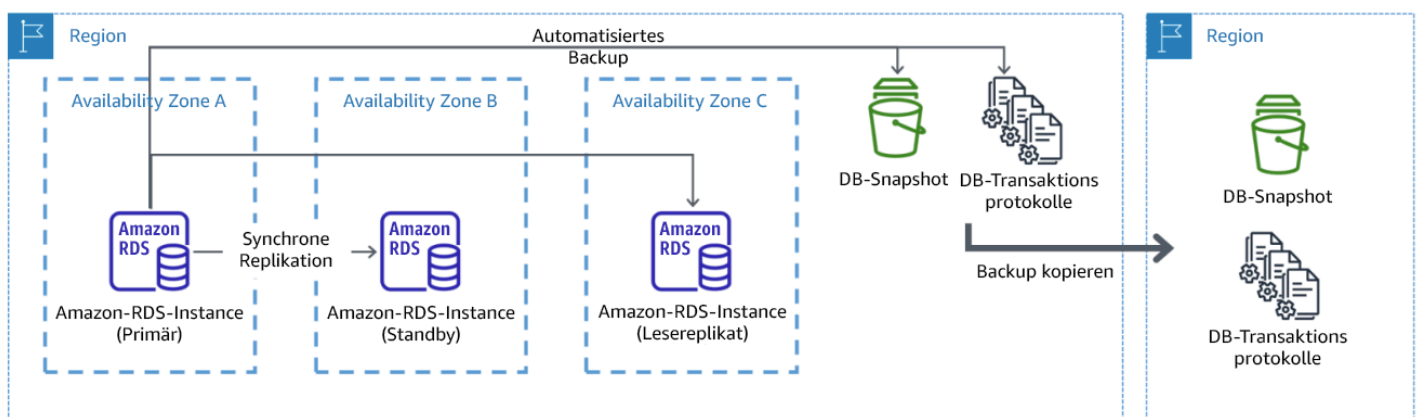
- [Globale AWS -Infrastruktur](#)
- [AWS Local ZonesFAQ](#)
- [Strategien zur ECS Aufgabenvergabe bei Amazon](#)
- [Auswählen von Regionen und Availability Zones](#)
- [Beispiel: Aufteilen von Instances in mehrere Availability Zones](#)
- [Globale Tabellen: Multiregionale Replikation mit DynamoDB](#)
- [Verwenden von Amazon Aurora Global Databases](#)
- [Blogserie „Erstellen einer regionsübergreifenden Anwendung mit AWS Services“](#)
- [Was ist AWS Outposts?](#)

### Zugehörige Videos:

- [AWS re:Invent 2018: Architekturmuster für aktiv-aktive Anwendungen mit mehreren Regionen \(09-R2\) ARC2](#)
- [AWS re:Invent 2019: Innovation und Betrieb der globalen Netzwerkinfrastruktur \(\) AWS NET339](#)

REL10-BP02 Wählen Sie die geeigneten Standorte für Ihren Einsatz an mehreren Standorten

Gewünschtes Ergebnis: Um eine hohe Verfügbarkeit zu erreichen, sollten Sie Ihre Workload-Komponenten immer (wenn möglich) in mehreren Availability Zones (AZs) bereitstellen. Überdenken Sie bei Workloads mit extremen Anforderungen an die Ausfallsicherheit die Optionen für eine Multi-Region-Architektur genau.



## Eine robuste Multi-AZ-Datenbankbereitstellung mit Backup in einer anderen AWS -Region

### Typische Anti-Muster:

- Entscheidung für das Design einer Architektur mit mehreren Regionen, wenn eine Multi-AZ-Architektur die Anforderungen erfüllen würde.
- Nichtberücksichtigung von Abhängigkeiten zwischen Anwendungskomponenten, wenn sich die Anforderungen an Ausfallsicherheit und mehrere Standorte zwischen diesen Komponenten unterscheiden.

Vorteile der Nutzung dieser bewährten Methode: Aus Gründen der Ausfallsicherheit sollten Sie einen Ansatz wählen, bei dem Schutzebenen aufgebaut werden. Eine Ebene schützt vor kleineren, häufigeren Störungen, indem eine hochverfügbare Architektur mit mehreren AZs Komponenten aufgebaut wird. Eine weitere Verteidigungsebene schützt vor seltenen Ereignissen wie Naturkatastrophen mit großer Reichweite und Unterbrechungen auf Regionsebene. Diese zweite Ebene beinhaltet die Architektur Ihrer Anwendung so, dass sie sich über mehrere Ebenen erstreckt. AWS-Regionen

- Der Unterschied zwischen einer Verfügbarkeit von 99,5 % und einer Verfügbarkeit von 99,99 % beträgt mehr als 3,5 Stunden pro Monat. Die erwartete Verfügbarkeit eines Workloads kann nur „vier Neunen“ erreichen, wenn es sich um mehrere Workloads handelt. AZs
- Wenn Sie Ihren Workload in mehreren Workloads ausführenAZs, können Sie Fehler in den Bereichen Stromversorgung, Kühlung und Netzwerk sowie die meisten Naturkatastrophen wie Feuer und Überschwemmungen isolieren.
- Wenn Sie eine Multi-Region-Strategie für Ihre Workload implementieren, ist sie vor weitreichenden Naturkatastrophen, die einen großen geografischen Bereich in einem Land betreffen, oder technischen Fehlern in einer ganzen Region geschützt. Beachten Sie dabei, dass das Implementieren einer Multi-Region-Architektur äußerst komplex sein kann und bei den meisten Workloads nicht erforderlich ist.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Hoch

### Implementierungsleitfaden

Bei einem Katastrophenfall, der auf einer Unterbrechung oder einem teilweisen Verlust einer Availability Zone beruht, trägt die Implementierung eines hochverfügbaren Workloads in mehreren Availability Zones innerhalb einer einzigen Availability Zones AWS-Region dazu bei, natürliche

und technische Katastrophen zu vermeiden. Jede AWS-Region besteht aus mehreren Availability Zones, die von Fehlern in den jeweils anderen Zonen isoliert und durch eine deutliche Entfernung voneinander getrennt sind. In Bezug auf Notfallereignisse, bei denen das Risiko besteht, dass mehrere Availability Zone-Komponenten, die weit voneinander entfernt sind, ausfallen, sollten Sie jedoch Optionen für die Notfallwiederherstellung implementieren, um die Auswirkungen von Ausfällen mit regionalem Ausmaß zu mindern. Für Workloads, die eine extreme Ausfallsicherheit erfordern (kritische Infrastruktur, gesundheitsbezogene Anwendungen, Finanzsysteminfrastruktur usw.), kann eine Strategie mit mehreren Regionen erforderlich sein.

## Implementierungsschritte

1. Bewerten Sie Ihren Workload und ermitteln Sie, ob die Anforderungen an die Ausfallsicherheit durch einen Multi-AZ-Ansatz (einzeln AWS-Region) erfüllt werden können oder ob ein regionsübergreifender Ansatz erforderlich ist. Die Implementierung einer Architektur mit mehreren Regionen zur Erfüllung dieser Anforderungen bringt zusätzliche Komplexität mit sich. Denken Sie daher sorgfältig über Ihren Anwendungsfall und die damit verbundenen Anforderungen nach. Anforderungen an die Ausfallsicherheit können fast immer mit einer einzigen AWS-Region erfüllt werden. Berücksichtigen Sie die folgenden möglichen Anforderungen, wenn Sie entscheiden, ob Sie mehrere Regionen verwenden müssen:
  - a. Disaster Recovery (DR): Bei einem Notfall, der auf einer Unterbrechung oder einem teilweisen Verlust einer Availability Zone beruht, AWS-Region trägt die Implementierung eines hochverfügbaren Workloads in mehreren Availability Zones innerhalb einer einzigen zur Minderung natürlicher und technischer Katastrophen bei. In Bezug auf Notfallereignisse, bei denen das Risiko besteht, dass mehrere Availability Zone-Komponenten, die weit voneinander entfernt sind, ausfallen, sollten Sie die Notfallwiederherstellung über mehrere Regionen hinweg implementieren, um die Auswirkungen von Naturkatastrophen oder technischen Fehlern mit regionalem Ausmaß zu mindern.
  - b. Hochverfügbarkeit (HA): Eine Architektur mit mehreren Regionen (mit mehreren AZs in jeder Region) kann verwendet werden, um eine Verfügbarkeit von mehr als vier 9 (> 99,99%) zu erreichen.
  - c. Stack-Lokalisierung: Wenn Sie einen Workload für ein globales Publikum bereitstellen, können Sie lokalisierte Stacks in verschiedenen Regionen bereitstellen, AWS-Regionen um Zielgruppen in diesen Regionen zu bedienen. Die Lokalisierung kann Sprache, Währung und Arten der gespeicherten Daten umfassen.



- d. Nähe zu Benutzern: Wenn Sie einen Workload für ein globales Publikum bereitstellen, können Sie die Latenz reduzieren, indem Sie Stacks in der AWS-Regionen Nähe der Endbenutzer einsetzen.
  - e. Datenresidenz: Einige Workloads unterliegen Anforderungen an die Datenresidenz, sodass Daten bestimmter Benutzer innerhalb der Grenzen eines bestimmten Landes bleiben müssen. Auf der Grundlage der jeweiligen Verordnung können Sie wählen, ob Sie einen ganzen Stack oder nur die Daten AWS-Region innerhalb dieser Grenzen bereitstellen möchten.
2. Hier finden Sie einige Beispiele für Multi-AZ-Funktionen, die von AWS -Services bereitgestellt werden:
- a. Um Workloads mit EC2 oder zu schützen ECS, stellen Sie einen Elastic Load Balancer vor den Rechenressourcen bereit. Elastic Load Balancing bietet dann die Lösung, um Instances in fehlerhaften Zonen zu erkennen und den Datenverkehr an die fehlerfreien Zonen weiterzuleiten.
    - i. [Erste Schritte mit Application Load Balancern](#)
    - ii. [Erste Schritte mit Network Load Balancern](#)
  - b. Bei EC2 Instances, auf denen kommerzielle off-the-shelf Software ausgeführt wird, die Load Balancing nicht unterstützt, können Sie eine Art von Fehlertoleranz erreichen, indem Sie eine Multi-AZ-Daster-Recovery-Methode implementieren.
    - i. [the section called “REL13-BP02 Verwenden Sie definierte Wiederherstellungsstrategien, um die Wiederherstellungsziele zu erreichen”](#)
  - c. Bei ECS Amazon-Aufgaben sollten Sie Ihren Service gleichmäßig auf drei verteilen AZs, um ein ausgewogenes Verhältnis zwischen Verfügbarkeit und Kosten zu erreichen.
    - i. [Bewährte Methoden zur ECS Verfügbarkeit von Amazon | Containers](#)
  - d. Für AmazonRDS, die nicht von Aurora stammen, können Sie Multi-AZ als Konfigurationsoption wählen. Bei einem Ausfall der primären Datenbank-Instance befördert Amazon RDS automatisch eine Standby-Datenbank, sodass sie Traffic in einer anderen Availability Zone empfängt. Außerdem können Lesereplikate für mehrere Regionen erstellt werden, um die Ausfallsicherheit zu verbessern.
    - i. [Amazon RDS Multi-AZ-Bereitstellungen](#)
    - ii. [Erstellen einer Read Replica in einem anderen AWS-Region](#)
3. Im Folgenden finden Sie einige Beispiele für regionsübergreifende Funktionen, die von AWS Diensten bereitgestellt werden:

- a. Für Amazon S3-Workloads, bei denen die Multi-AZ-Verfügbarkeit automatisch durch den Service bereitgestellt wird, sollten Sie multiregionale Zugangspunkte in Betracht ziehen, wenn eine Bereitstellung in mehreren Regionen erforderlich ist.
  - i. [Multi-Regions-Zugriffspunkte in Amazon S3](#)
- b. Bei DynamoDB-Tabellen, bei denen die Multi-AZ-Verfügbarkeit automatisch vom Service bereitgestellt wird, können Sie bestehende Tabellen problemlos in globale Tabellen konvertieren, um mehrere Regionen zu nutzen.
  - i. [Konvertieren von Amazon DynamoDB-Einzelegionstabellen in globale Tabellen](#)
- c. Wenn Ihr Workload von Application Load Balancern oder Network Load Balancern unterstützt wird, können Sie AWS Global Accelerator verwenden, um die Verfügbarkeit Ihrer Anwendung zu verbessern, indem Sie den Datenverkehr in mehrere Regionen mit fehlerfreien Endpunkten weiterleiten.
  - i. [Endpunkte für Standardbeschleuniger in Global Accelerator — AWS Global Accelerator \(amazon.com\) AWS](#)
- d. Für Anwendungen, die diese Nutzung nutzen AWS EventBridge, sollten Sie regionsübergreifende Busse in Betracht ziehen, um Ereignisse in andere von Ihnen ausgewählte Regionen weiterzuleiten.
  - i. [Senden und Empfangen von EventBridge Amazon-Events zwischen AWS-Regionen](#)
- e. Bei Amazon Aurora-Datenbanken sollten Sie die globalen Aurora-Datenbanken in Betracht ziehen, die sich über mehrere AWS -Regionen erstrecken. Auch bestehende Cluster können geändert werden, um neue Regionen hinzuzufügen.
  - i. [Erste Schritte mit Amazon Aurora Global Databases](#)
- f. Wenn Ihr Workload Verschlüsselungsschlüssel AWS Key Management Service (AWS KMS) enthält, sollten Sie prüfen, ob Schlüssel für mehrere Regionen für Ihre Anwendung geeignet sind.
  - i. [Schlüssel für mehrere Regionen in AWS KMS](#)
- g. Weitere AWS Servicefunktionen finden Sie in dieser Blogserie zur [Erstellung einer regionsübergreifenden Anwendung mit AWS](#) Diensten

Aufwand für den Implementierungsplan: Mittel bis hoch

Ressourcen

Zugehörige Dokumente:

- [Serie „Erstellen einer multiregionalen Anwendung mit AWS Services“](#)
- [Disaster Recovery \(DR\) -Architektur aktiviert AWS, Teil IV: Aktiv/Aktiv an mehreren Standorten](#)
- [Globale AWS -Infrastruktur](#)
- [AWS Local ZonesFAQ](#)
- [Disaster Recovery \(DR\) -Architektur weiter AWS, Teil I: Strategien für die Wiederherstellung in der Cloud](#)
- [Die Notfallwiederherstellung in der Cloud unterscheidet sich](#)
- [Globale Tabellen: Multiregionale Replikation mit DynamoDB](#)

#### Zugehörige Videos:

- [AWS re:Invent 2018: Architekturmuster für aktiv-aktive Anwendungen mit mehreren Regionen \(09-R2\) ARC2](#)
- [Auth0: multiregionale Architektur mit hoher Verfügbarkeit, die auf mehr als 1,5 Milliarden Anmeldungen pro Monat mit automatisiertem Failover skaliert werden kann.](#)

#### Zugehörige Beispiele:

- [Disaster Recovery \(DR\) -Architektur weiter AWS, Teil I: Strategien für die Wiederherstellung in der Cloud](#)
- [DTCCerreicht eine Resilienz, die weit über das hinausgeht, was sie vor Ort leisten können](#)
- [Die Expedia Group verwendet eine Architektur mit mehreren Regionen und mehreren Availability Zones mit einem eigenen DNS Service, um die Ausfallsicherheit der Anwendungen zu erhöhen](#)
- [Uber: Notfallwiederherstellung für multiregionales Kafka](#)
- [Netflix: Aktiv-Aktiv für multiregionale Resilienz](#)
- [Entwicklung von Data Residency für Atlassian Cloud](#)
- [Intuit läuft TurboTax in zwei Regionen](#)

REL10-BP03 Automatisieren Sie die Wiederherstellung von Komponenten, die auf einen einzigen Standort beschränkt sind

Wenn Komponenten der Workload nur in einer einzigen Availability Zone oder in einem On-Premises-Rechenzentrum ausgeführt werden können, implementieren Sie die Möglichkeit, die Workload innerhalb Ihrer definierten Wiederherstellungsziele komplett neu aufzusetzen.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel

## Implementierungsleitfaden

Wenn die bewährte Methode zur Bereitstellung der Workload an mehreren Standorten aufgrund technologischer Einschränkungen nicht möglich ist, müssen Sie einen alternativen Pfad zur Ausfallsicherheit implementieren. Sie müssen die Möglichkeit automatisieren, die erforderliche Infrastruktur neu zu erstellen, Anwendungen neu bereitzustellen und die erforderlichen Daten für diese Fälle neu zu erstellen.

Amazon EMR startet beispielsweise alle Knoten für einen bestimmten Cluster in derselben Availability Zone, weil der Betrieb eines Clusters in derselben Zone die Leistung der Auftragsabläufe verbessert, da er eine höhere Datenzugriffsrate bietet. Wenn diese Komponente für die Ausfallsicherheit von Workloads erforderlich ist, müssen Sie die Möglichkeit haben, den Cluster und seine Daten erneut bereitzustellen. Auch für Amazon EMR sollten Sie Redundanz auf andere Weise als mit Multi-AZ bereitstellen. Sie können [mehrere Knoten](#) bereitstellen. Mithilfe von [EMR File System \(EMRFS\)](#) EMR können Daten in Amazon S3 gespeichert werden, die wiederum über mehrere Availability Zones repliziert werden können oder AWS-Regionen.

Ähnlich stellt Amazon Redshift Ihren Cluster standardmäßig in einer zufällig ausgewählten Availability Zone innerhalb der AWS-Region von Ihnen ausgewählten Availability Zone bereit. Alle Knoten des Clusters werden in derselben Zone bereitgestellt.

Für statusbehaftete serverbasierte Workloads, die in einem lokalen Rechenzentrum bereitgestellt werden, können Sie diese AWS Elastic Disaster Recovery zum Schutz Ihrer Workloads in verwenden. Wenn Sie bereits gehostet werden, können Sie Elastic Disaster Recovery verwenden, um Ihren Workload in einer alternativen Availability Zone oder Region zu schützen. Elastic Disaster Recovery verwendet eine kontinuierliche Replikation auf Block-Ebene in eine schlanke Staging-Area, um eine schnelle, zuverlässige Wiederherstellung von On-Premises-Anwendungen und cloudbasierten Anwendungen zu gewährleisten.

## Implementierungsschritte

1. Implementieren Sie die Selbstreparatur. Stellen Sie Ihre Instances oder Container nach Möglichkeit mit automatischer Skalierung bereit. Wenn Sie die automatische Skalierung nicht verwenden können, verwenden Sie die automatische Wiederherstellung für EC2 Instances oder implementieren Sie eine automatische Selbstheilung auf der Grundlage von Amazon EC2 - oder ECS Container-Lifecycle-Ereignissen.

- Verwenden Sie [Amazon EC2 Auto Scaling Scaling-Gruppen](#) für Instances und Container-Workloads, für die keine einzelne Instance-IP-Adresse, private IP-Adresse, Elastic IP-Adresse und Instance-Metadaten erforderlich sind.
- Die Benutzerdaten der Startvorlage können zur Implementierung einer Automatisierung verwendet werden, die die meisten Workloads automatisch reparieren kann.
- Verwenden Sie die automatische [Wiederherstellung von EC2 Amazon-Instances](#) für Workloads, die eine einzelne Instance-ID-Adresse, private IP-Adresse, elastische IP-Adresse und Instance-Metadaten benötigen.
  - Automatic Recovery sendet Benachrichtigungen zum Wiederherstellungsstatus an ein SNS Thema, sobald der Instance-Fehler erkannt wird.
- Verwenden Sie [Lebenszyklusereignisse von EC2 Amazon-Instanzen](#) oder [ECSAmazon-Ereignisse](#), um die Selbstheilung zu automatisieren, wenn automatische Skalierung oder EC2 Wiederherstellung nicht verwendet werden können.
  - Verwenden Sie die Ereignisse, um die Automatisierung der Reparatur der Komponente entsprechend der erforderlichen Prozesslogik aufzurufen.
- Schützen Sie statusbehaftete Workloads, die auf einen einzelnen Standort beschränkt sind, mithilfe von [AWS Elastic Disaster Recovery](#).

## Ressourcen

### Zugehörige Dokumente:

- [ECSAmazon-Veranstaltungen](#)
- [Lebenszyklus-Hooks von Amazon EC2 Auto Scaling](#)
- [Wiederherstellen der Instance.](#)
- [Automatische Skalierung von Services](#)
- [Was ist Amazon EC2 Auto Scaling?](#)
- [AWS Elastic Disaster Recovery](#)

REL10-BP04 Verwenden Sie Schottarchitekturen, um den Wirkungsbereich zu begrenzen

Implementieren Sie Bulkhead-Architekturen (zellenbasierte Architekturen), um die Auswirkungen von Fehlern innerhalb einer Workload auf eine begrenzte Anzahl von Komponenten zu beschränken.

Gewünschtes Ergebnis: Eine zellenbasierte Architektur verwendet mehrere isolierte Instances einer Workload, wobei jede Instance als Zelle bezeichnet wird. Jede Zelle ist unabhängig. Sie teilt ihren Status nicht mit anderen Zellen und bearbeitet eine Teilmenge der gesamten Workload-Anfragen. Dadurch werden die möglichen Auswirkungen eines Fehlers, z. B. eines fehlerhaften Software-Updates, auf eine einzelne Zelle und die von ihr verarbeiteten Anfragen reduziert. Wenn in einer Workload 10 Zellen für die Beantwortung von 100 Anfragen verwendet werden, sind bei einem Fehler 90 % der gesamten Anfragen nicht davon betroffen.

Typische Anti-Muster:

- Es wird ein unbegrenztes Wachstum der Zellen zugelassen.
- Code-Updates oder Bereitstellungen werden auf alle Zellen gleichzeitig angewandt.
- Status oder Komponenten werden von den Zellen geteilt (mit Ausnahme der Router-Schicht).
- Es werden komplexe Geschäfts- oder Routing-Logiken in die Routing-Schicht eingefügt.
- Es gibt keine Minimierung der zellenübergreifenden Interaktionen.

Vorteile der Nutzung dieser bewährten Methode: Bei zellenbasierten Architekturen sind viele gängige Fehlertypen in der Zelle selbst enthalten, was eine zusätzliche Fehlerisolierung ermöglicht. Diese Fehlergrenzen können die Widerstandsfähigkeit gegenüber Fehlertypen erhöhen, die sonst schwer einzudämmen sind, wie z. B. erfolglose Codebereitstellungen oder Anfragen, die beschädigt sind oder einen bestimmten Fehlermodus aufrufen (auch bekannt als Poison-Pill-Anfragen).

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Hoch

Implementierungsleitfaden

Auf einem Schiff sorgen Schotten dafür, dass eine Beschädigung des Rumpfes auf einen Teil des Schiffes beschränkt bleibt. In komplexen Systemen wird dieses Muster oft kopiert, um eine Fehlerisolierung zu ermöglichen. Fehlerisolierte Grenzen beschränken die Auswirkungen eines Fehlers innerhalb einer Workload auf eine begrenzte Anzahl von Komponenten. Komponenten außerhalb der Grenze sind von dem Ausfall nicht betroffen. Durch die Verwendung mehrerer fehlerisolierter Grenzen können Sie die Auswirkungen auf Ihre Workload einschränken. Bei „On AWS“ können Kunden mehrere Availability Zones und Regionen verwenden, um Fehler zu isolieren. Das Konzept der Fehlerisolierung kann jedoch auch auf die Architektur Ihres Workloads ausgedehnt werden.

Die gesamte Workload wird durch einen Partitionsschlüssel in Zellen unterteilt. Dieser Schlüssel muss mit der Struktur des Service übereinstimmen oder mit der natürlichen Art und Weise, wie die

Workload eines Service mit minimalen zellenübergreifenden Interaktionen unterteilt werden kann. Beispiele für Partitionsschlüssel sind Kunden-ID, Ressourcen-ID oder andere Parameter, auf die bei den meisten API Aufrufen leicht zugegriffen werden kann. Eine Schicht für das Routing von Zellen verteilt Anfragen auf der Grundlage des Partitionsschlüssels an einzelne Zellen und präsentiert den Kunden einen einzigen Endpunkt.

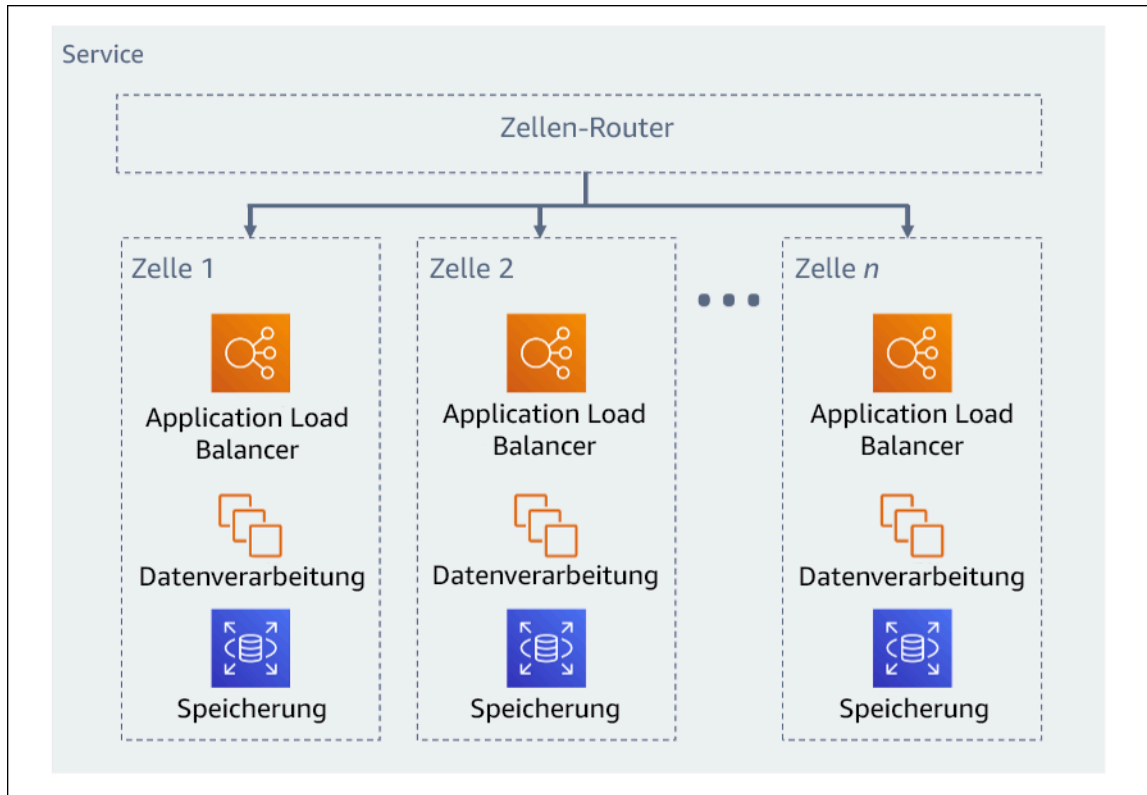


Abbildung 11: Zellenbasierte Architektur

### Implementierungsschritte

Bei der Entwicklung einer zellenbasierten Architektur sind mehrere Designüberlegungen zu berücksichtigen:

1. Partitionsschlüssel: Bei der Auswahl des Partitionsschlüssels sollten besondere Überlegungen angestellt werden.
  - Er sollte mit der Struktur des Service übereinstimmen oder mit der natürlichen Art und Weise, wie die Workload eines Service mit minimalen zellenübergreifenden Interaktionen unterteilt werden kann. Beispiele sind `customer ID` oder `resource ID`.
  - Der Partitionsschlüssel muss in allen Anfragen verfügbar sein – entweder direkt oder in einer Weise, die sich durch andere Parameter leicht deterministisch ableiten lässt.

2. Persistente Zellenzuordnung: Upstream-Services sollten während des gesamten Lebenszyklus ihrer Ressourcen nur mit einer einzelnen Zelle interagieren.
  - Je nach Workload kann eine Strategie zur Migration von Zellen erforderlich sein, um Daten von einer Zelle in eine andere zu migrieren. Ein mögliches Szenario, in dem eine Migration von Zellen erforderlich sein kann, ist, wenn ein bestimmter Benutzer oder eine bestimmte Ressource in Ihrer Workload zu groß wird und eine eigene Zelle benötigt.
  - Zellen sollten keinen Status und keine Komponenten gemeinsam nutzen.
  - Folglich sollten zellenübergreifende Interaktionen vermieden oder auf ein Minimum beschränkt werden, da diese Interaktionen Abhängigkeiten zwischen den Zellen schaffen und somit die Möglichkeiten zur Fehlerisolierung verringern.
3. Router-Schicht: Die Router-Schicht ist eine Komponente, die von Zellen gemeinsam genutzt wird, sodass nicht dieselbe Segmentierungsstrategie verfolgt werden kann wie bei Zellen.
  - Es wird empfohlen, dass die Routing-Schicht Anfragen auf einzelne Zellen verteilt, indem sie einen effizienten Algorithmus für die Zuordnung von Partitionen einsetzt – z. B. als die Kombination von kryptographischen Hash-Funktionen und einer modularen Arithmetik.
  - Um Auswirkungen auf mehrere Zellen zu vermeiden, muss die Routing-Schicht so einfach und horizontal skalierbar wie möglich bleiben, was den Verzicht auf eine komplexe Geschäftslogik innerhalb dieser Schicht erforderlich macht. Dies hat den zusätzlichen Nutzen, dass das erwartete Verhalten jederzeit leicht nachvollziehbar ist, was eine gründliche Testbarkeit ermöglicht. Wie Colm MacCárthaigh in [Zuverlässigkeit, stetige Ausführung und eine gute Tasse Kaffee](#) erklärt, sorgen einfache Designs und Muster mit konstanter Ausführung für zuverlässige Systeme und verringern die Widerstandsfähigkeit gegen Fragilität.
4. Zellgröße: Für Zellen sollte eine maximale Größe festgelegt sein, die sie nicht überschreiten dürfen.
  - Die maximale Größe sollte durch gründliche Tests ermittelt werden – bis Sollbruchstellen erreicht und sichere operative Margen etabliert sind. Weitere Details zur Implementierung von Testverfahren finden Sie unter [REL07-BP04 Belastungstest Ihr Workload](#).
  - Die gesamte Workload sollte durch Hinzufügen zusätzlicher Zellen wachsen, sodass die Workload mit der steigenden Nachfrage skalieren kann.
5. Multi-AZ- oder multiregionale Strategien: Zum Schutz vor unterschiedlichen Ausfall-Domains sollten mehrere Resilienzebenen genutzt werden.
  - Für die Ausfallsicherheit sollten Sie einen Ansatz wählen, bei dem verschiedene Verteidigungsebenen aufgebaut werden. Eine Ebene schützt vor kleineren, häufigeren Störungen, indem eine hochverfügbare Architektur mit mehreren AZs Komponenten erstellt wird.



Eine weitere Verteidigungsebene schützt vor seltenen Ereignissen wie Naturkatastrophen mit großer Reichweite und Unterbrechungen auf Regionsebene. Diese zweite Ebene beinhaltet die Architektur Ihrer Anwendung so, dass sie sich über mehrere Ebenen erstreckt. AWS-Regionen Wenn Sie eine Multi-Region-Strategie für Ihre Workload implementieren, ist sie vor weitreichenden Naturkatastrophen, die einen großen geografischen Bereich in einem Land betreffen, oder technischen Fehlern in einer ganzen Region geschützt. Beachten Sie dabei, dass das Implementieren einer Multi-Region-Architektur äußerst komplex sein kann und bei den meisten Workloads nicht erforderlich ist. Weitere Details erhalten Sie unter [REL10-BP02 Wählen Sie die geeigneten Standorte für Ihren Einsatz an mehreren Standorten](#).

6. Codebereitstellung: Eine Strategie zur gestaffelten Codebereitstellung sollte der gleichzeitigen Bereitstellung von Codeänderungen in allen Zellen vorgezogen werden.
- Auf diese Weise werden mögliche Fehler in mehreren Zellen aufgrund einer fehlerhaften Bereitstellung oder menschlichen Versagens minimiert. Weitere Informationen finden Sie unter [Automatisierung sicherer, vollautomatischer Bereitstellungen](#).

## Ressourcen

### Zugehörige bewährte Methoden:

- [REL07-BP04 Belastungstest Ihr Workload](#)
- [REL10-BP02 Wählen Sie die geeigneten Standorte für Ihren Einsatz an mehreren Standorten](#)

### Zugehörige Dokumente:

- [Zuverlässigkeit, stetige Ausführung und eine gute Tasse Kaffee](#)
- [AWS und Kompartimentierung](#)
- [Workload-Isolation mit Shuffle Sharding](#)
- [Automatisierung sicherer, vollautomatischer Bereitstellungen](#)

### Zugehörige Videos:

- [AWS re:Invent 2018: Kreisläufe schließen und neue Denkansätze eröffnen: Wie man die Kontrolle über große und kleine Systeme übernimmt](#)
- [AWS re:Invent 2018: So wird der Explosionsradius von AWS Ausfällen minimiert \(\) ARC338](#)
- [Shuffle-Sharding: AWS re:Invent 2019: Wir stellen vor: Die Amazon Builders' Library \(\) DOP328](#)

- [AWS Summit ANZ 2021 — Alles scheitert, die ganze Zeit: Auf Resilienz ausrichten](#)

Zugehörige Beispiele:

- [Well-Architected Lab: Fehlerisolierung mit Shuffle Sharding](#)

REL11. Wie können Sie Workloads so gestalten, dass sie Komponentenausfällen gegenüber resilient sind?

Workloads, für die eine hohe Verfügbarkeit und eine geringe mittlere Wiederherstellungszeit (MTTR) erforderlich sind, müssen auf Ausfallsicherheit ausgelegt werden.

Bewährte Methoden

- [REL11-BP01 Überwachen Sie alle Komponenten des Workloads, um Fehler zu erkennen](#)
- [REL11-BP02 Failover zu gesunden Ressourcen](#)
- [REL11-BP03 Automatisieren Sie die Heilung auf allen Ebenen](#)
- [REL11-BP04 Verlassen Sie sich bei der Wiederherstellung auf die Datenebene und nicht auf die Steuerebene](#)
- [REL11-BP05 Verwenden Sie statische Stabilität, um bimodales Verhalten zu verhindern](#)
- [REL11-BP06 Benachrichtigungen senden, wenn Ereignisse die Verfügbarkeit beeinträchtigen](#)
- [REL11-BP07 Gestalten Sie Ihr Produkt so, dass es Verfügbarkeitsziele und Service Level Agreements für Verfügbarkeit erfüllt \(\) SLAs](#)

REL11-BP01 Überwachen Sie alle Komponenten des Workloads, um Fehler zu erkennen

Überwachen Sie den Zustand Ihrer Workload kontinuierlich, damit Sie und Ihre automatisierten Systeme auf Fehler oder Verschlechterungen aufmerksam werden, sobald diese auftreten. Achten Sie auf wichtige Leistungsindikatoren (KPIs), die auf dem Geschäftswert basieren.

Alle Wiederherstellungs- und Reparaturmechanismen müssen auf eine schnelle Erkennung von Problemen ausgelegt sein. Technische Fehler sollten zuerst erkannt werden, damit sie behoben werden können. Die Verfügbarkeit hängt jedoch von der Fähigkeit Ihres Workloads ab, einen geschäftlichen Nutzen zu erzielen. Daher müssen wichtige Leistungsindikatoren (KPIs), mit denen dies gemessen wird, Teil Ihrer Erkennungs- und Problembehebungsstrategie sein.

Gewünschtes Ergebnis: Wesentliche Komponenten einer Workload werden unabhängig überwacht, um Fehler zu erkennen und anzuzeigen, wann und wo sie auftreten.

Typische Anti-Muster:

- Es sind keine Alarme konfiguriert, sodass Ausfälle ohne Benachrichtigung auftreten.
- Alarme sind vorhanden, aber mit Schwellenwerten, die keine ausreichende Zeit für die Reaktion bieten.
- Metriken werden nicht oft genug erfasst, um das Ziel der Wiederherstellungszeit (RTO) zu erreichen.
- Nur die kundenorientierten Schnittstellen der Workload werden aktiv überwacht.
- Es werden nur technische Metriken erfasst, keine Metriken für Geschäftsfunktionen.
- Es gibt keine Metriken, die die Benutzererfahrung der Workload messen.
- Es werden zu viele Überwachungen erstellt.

Vorteile der Nutzung dieser bewährten Methode: Mit einer angemessenen Überwachung auf allen Ebenen können Sie die Wiederherstellungszeit reduzieren, indem Sie die Zeit bis zur Erkennung verkürzen.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Hoch

Implementierungsleitfaden

Identifizieren Sie alle Workloads, die für die Überwachung überprüft werden sollen. Sobald Sie alle zu überwachenden Komponenten der Workload identifiziert haben, müssen Sie das Überwachungsintervall festlegen. Das Überwachungsintervall wirkt sich direkt darauf aus, wie schnell eine Wiederherstellung eingeleitet werden kann (abhängig davon, wie lange die Erkennung eines Fehlers dauert). Die mittlere Zeit bis zur Erkennung (MTTD) ist die Zeitspanne zwischen dem Auftreten eines Fehlers und dem Beginn der Reparaturarbeiten. Die Liste der Services sollte umfassend und vollständig sein.

Die Überwachung muss alle Ebenen des Anwendungs-Stacks (inklusive Anwendung, Plattform, Infrastruktur und Netzwerk) abdecken.

Ihre Überwachungsstrategie sollte außerdem die Auswirkungen von grauen Fehlern berücksichtigen. Weitere Informationen zu grauen Fehlern finden Sie unter [Graue Fehler](#) im Whitepaper „Erweiterte Multi-AZ Resilience-Muster“.

## Implementierungsschritte

- Das Überwachungsintervall hängt davon ab, wie schnell Wiederherstellungen durchgeführt werden müssen. Ihre Wiederherstellungszeit hängt von der Zeit ab, die für die Wiederherstellung benötigt wird. Daher müssen Sie die Häufigkeit der Datenerfassung bestimmen, indem Sie diese Zeit und Ihr Ziel für die Wiederherstellung berücksichtigen (RTO).
- Konfigurieren Sie eine detaillierte Überwachung für Komponenten und verwaltete Services.
  - Stellen Sie fest, ob eine [detaillierte Überwachung für EC2 Instances](#) und [Auto Scaling](#) erforderlich ist. Eine detaillierte Überwachung liefert Metriken in einminütigen Intervallen, die Standardüberwachung liefert Metriken in fünfminütigen Intervallen.
  - Stellen Sie fest, ob [eine erweiterte Überwachung](#) für RDS erforderlich ist. Bei der erweiterten Überwachung wird ein Agent für RDS Instances verwendet, um nützliche Informationen über verschiedene Prozesse oder Threads zu erhalten.
  - Ermitteln Sie die Überwachungsanforderungen kritischer serverloser Komponenten für [Lambda](#), [APIGateway](#), [Amazon EKSECS](#), [Amazon](#) und alle Arten von [Load](#) Balancern.
  - Ermitteln Sie die Überwachungsanforderungen der Speicherkomponenten für [Amazon S3FSx](#), [AmazonEFS](#), [Amazon](#) und [Amazon EBS](#).
- Erstellen Sie [benutzerdefinierte Metriken](#) zur Messung der wichtigsten Unternehmensleistungsindikatoren (KPIs). Workloads implementieren wichtige Geschäftsfunktionen, die verwendet werden sollten, um zu erkennen KPIs, wann ein indirektes Problem auftritt.
- Überwachen Sie das Benutzererlebnis mithilfe von Benutzer-Canarys auf Fehler. [Synthetische Transaktionstests](#) (auch bekannt als Canary-Tests, aber nicht zu verwechseln mit Canary-Bereitstellungen), die das Kundenverhalten simulieren können, gehören zu den wichtigsten Testprozessen. Führen Sie diese Tests für Ihre Workload-Endpunkte konstant von verschiedenen Remote-Standorten aus.
- Erstellen Sie [benutzerdefinierte Metriken](#) zur Verfolgung des Benutzererlebnisses. Wenn Sie das Kundenerlebnis instrumentieren können, können Sie die Verschlechterung des Kundenerlebnisses feststellen.
- [Richten Sie Alarmer ein](#), um zu erkennen, wenn ein Teil Ihrer Workload nicht ordnungsgemäß funktioniert, und um anzuzeigen, wann die Ressourcen automatisch skaliert werden müssen. Alarmer können visuell auf Dashboards angezeigt werden, Benachrichtigungen über Amazon SNS oder E-Mail senden und mit Auto Scaling die Workload-Ressourcen nach oben oder unten skalieren.

- Erstellen Sie [Dashboards](#), um Ihre Metriken zu visualisieren. Dashboards können verwendet werden, um Trends, Ausreißer und andere Indikatoren für potenzielle Probleme zu visualisieren, und auf Probleme hinweisen, die Sie untersuchen sollten.
- Erstellen Sie eine [verteilte Ablaufverfolgungsüberwachung](#) für Ihre Services. Mit der verteilten Überwachung können Sie nachvollziehen, wie Ihre Anwendung und die ihr zugrunde liegenden Services arbeiten, um die Ursache von Leistungsproblemen und Fehlern zu identifizieren und zu beheben.
- Erstellen Sie Dashboards und Datenerfassung für Überwachungssysteme (mithilfe von [X-Ray CloudWatch oder X-Ray](#)) in einer separaten Region und einem separaten Konto.
- Erstellen Sie eine Integration für die [Amazon Health Aware-Überwachung](#), um die Überwachung von AWS Ressourcen zu ermöglichen, bei denen es zu Leistungseinbußen kommen könnte. Für geschäftskritische Workloads bietet diese Lösung Zugriff auf proaktive Benachrichtigungen in Echtzeit für Services. AWS

## Ressourcen

Zugehörige bewährte Methoden:

- [Definition der Verfügbarkeit](#)
- [REL11-BP06 Senden Sie Benachrichtigungen, wenn Ereignisse die Verfügbarkeit beeinträchtigen](#)

Zugehörige Dokumente:

- [Mit Amazon CloudWatch Synthetics können Sie Benutzer-Kanarien erstellen](#)
- [Aktivieren oder Deaktivieren der detaillierten Überwachung für Ihre Instance](#)
- [Verbesserte Überwachung](#)
- [Überwachen Sie Ihre Auto Scaling Scaling-Gruppen und -Instances mithilfe von Amazon CloudWatch](#)
- [Veröffentlichen von benutzerdefinierten Metriken](#)
- [Amazon CloudWatch Alarms verwenden](#)
- [CloudWatch Dashboards verwenden](#)
- [Verwendung von regionsübergreifenden, kontenübergreifenden Dashboards CloudWatch](#)
- [Verwenden der regionen- und kontoübergreifenden X-Ray-Nachverfolgung](#)
- [Verstehen der Verfügbarkeit](#)

- [Implementierung von Amazon Health Aware \(AHA\)](#)

Zugehörige Videos:

- [Beheben von grauen Fehlern](#)

Zugehörige Beispiele:

- [Well-Architected Lab: Level 300: Implementieren von Zustandsprüfungen und Verwalten von Abhängigkeiten zur Verbesserung der Zuverlässigkeit](#)
- [Workshop zur Beobachtbarkeit: X-Ray erkunden](#)

Zugehörige Tools:

- [CloudWatch](#)
- [CloudWatch X-Ray](#)

## REL11-BP02 Failover zu gesunden Ressourcen

Wenn ein Fehler bei einer Ressource auftritt, sollten intakte Ressourcen weiterhin Anfragen bedienen. Stellen Sie bei Standortbeeinträchtigungen (wie Availability Zone oder AWS-Region) sicher, dass Sie über Systeme verfügen, die ein Failover auf intakte Ressourcen an unbeeinträchtigten Standorten ermöglichen.

Wenn Sie einen Service entwerfen, verteilen Sie die Last auf Ressourcen, Availability Zones oder Regionen. So kann der Fehler einer einzelnen Ressource oder eine Beeinträchtigung durch die Verlagerung des Datenverkehrs auf die verbleibenden intakten Ressourcen aufgefangen werden. Überlegen Sie, wie Services im Falle eines Fehlers erkannt und geroutet werden.

Entwerfen Sie Ihre Services mit Blick auf die Fehlerbehebung. Wir bei entwickeln Services so AWS, dass die Zeit bis zur Wiederherstellung nach Ausfällen und Auswirkungen auf Daten minimiert wird. Unsere Services verwenden primär Datenspeicher, die Anfragen erst akzeptieren, nachdem sie dauerhaft auf mehreren Replikaten in einer Region gespeichert wurden. Sie sind so aufgebaut, dass sie eine zellenbasierte Isolation und die Fehlerisolierung von Availability Zones nutzen. In unseren betrieblichen Abläufen setzen wir sehr stark auf Automatisierung. Wir optimieren auch unsere replace-and-restart Funktionalität, um nach Unterbrechungen eine schnelle Wiederherstellung zu gewährleisten.

Die Muster und Entwürfe, die den Failover ermöglichen, variieren für jeden AWS -Plattform-Service. Viele AWS native verwaltete Dienste haben nativ mehrere Availability Zones (wie Lambda oder API Gateway). Andere AWS Dienste (wie EC2 und EKS) erfordern spezielle Best-Practice-Designs, um das Failover von Ressourcen oder Datenspeicher auf allen Ebenen zu unterstützen. AZs

Es sollte eine Überwachung eingerichtet werden, um zu überprüfen, ob die Failover-Ressource in Ordnung ist, den Fortschritt der Failover-Ressourcen zu verfolgen und die Wiederherstellung von Geschäftsprozessen zu überwachen.

Gewünschtes Ergebnis: Die Systeme sind in der Lage, automatisch oder manuell neue Ressourcen zu verwenden, um sich von Störungen zu erholen.

Typische Anti-Muster:

- Die Planung für Fehler ist nicht Teil der Planungs- und Designphase.
- RTO und RPO sind nicht etabliert.
- Unzureichende Überwachung, um ausfallende Ressourcen zu erkennen.
- Ordnungsgemäße Isolierung von fehlerhaften Domains.
- Multi-Region-Failover wird nicht berücksichtigt.
- Die Erkennung von Fehlern ist bei der Entscheidung für einen Failover zu empfindlich oder zu aggressiv.
- Failover-Design wird nicht getestet oder validiert.
- Durchführen automatischer Reparaturen ohne die Benachrichtigung, dass eine Reparatur erforderlich war.
- Fehlender Ausgleichszeitraum, um einen zu frühen Failover zu vermeiden.

Vorteile der Nutzung dieser bewährten Methode: Sie können widerstandsfähigere Systeme aufbauen, die auch bei Fehlern zuverlässig bleiben, indem sie ordnungsgemäß reduziert werden und sich schnell erholen.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Hoch

Implementierungsleitfaden

AWS Dienste wie [Elastic Load Balancing](#) und [Amazon EC2 Auto Scaling](#) helfen dabei, die Last auf Ressourcen und Availability Zones zu verteilen. Daher kann der Ausfall einer einzelnen Ressource (z. B. einer EC2 Instance) oder die Beeinträchtigung einer Availability Zone gemildert werden, indem der Datenverkehr auf die verbleibenden intakten Ressourcen verlagert wird.

Bei Workloads, die mehrere Regionen umfassen, sind Designs etwas komplizierter. Mit regionsübergreifenden Read Replicas können Sie Ihre Daten beispielsweise mehreren Benutzern zur Verfügung stellen. AWS-Regionen Der Failover ist jedoch immer noch erforderlich, um das Lesereplikat zum primären Endpunkt zu machen und den Datenverkehr auf den neuen Endpunkt zu lenken. Amazon Route 53, [Amazon Application Recovery Controller \(ARC\)](#), Amazon und AWS Global Accelerator können dabei helfen CloudFront, den Datenverkehr weiterzuleiten AWS-Regionen.

AWS Dienste wie Amazon S3, Lambda, API Gateway, Amazon, Amazon, Amazon SQSSNS, Amazon PinpointSES, Amazon, ECR AWS Certificate Manager EventBridge, oder Amazon DynamoDB werden automatisch in mehreren Availability Zones von bereitgestellt. AWS Im Falle eines Fehlers leiten diese AWS Dienste den Datenverkehr automatisch an fehlerfreie Standorte weiter. Die Daten werden redundant in mehreren Availability Zones gespeichert und bleiben verfügbar.

Für AmazonRDS, Amazon Aurora, Amazon RedshiftEKS, Amazon oder Amazon ECS ist Multi-AZ eine Konfigurationsoption. AWS kann den Datenverkehr an die fehlerfreie Instance weiterleiten, wenn ein Failover initiiert wird. Diese Failover-Maßnahme kann vom Kunden AWS oder auf Wunsch des Kunden ergriffen werden

Für EC2 Amazon-Instances, Amazon Redshift, ECS Amazon-Aufgaben oder EKS Amazon-Pods wählen Sie aus, in welchen Availability Zones die Bereitstellung erfolgen soll. Bei einigen Designs bietet Elastic Load Balancing die Lösung, um Instances in fehlerhaften Zonen zu erkennen und den Datenverkehr an die fehlerfreien Zonen weiterzuleiten. Elastic Load Balancing kann den Datenverkehr auch an Komponenten in Ihrem On-Premises-Rechenzentrum weiterleiten.

Für den Failover des Datenverkehrs in mehreren Regionen kann die Umleitung Amazon Route 53, Amazon Application Recovery Controller AWS Global Accelerator, Route 53 Private DNS for nutzen oder eine Möglichkeit bietenVPCs, Internetdomänen CloudFront zu definieren und Routing-Richtlinien, einschließlich Zustandsprüfungen, zuzuweisen, um den Verkehr in fehlerfreie Regionen weiterzuleiten. AWS Global Accelerator stellt statische IP-Adressen bereit, die als fester Zugangspunkt für Ihre Anwendung dienen und dann zu Endpunkten Ihrer Wahl weiterleiten, wobei das AWS globale Netzwerk anstelle AWS-Regionen des Internets verwendet wird, um eine bessere Leistung und Zuverlässigkeit zu erzielen.

### Implementierungsschritte

- Erstellen Sie Failover-Designs für alle entsprechenden Anwendungen und Services. Isolieren Sie jede Architekturkomponente und erstellen Sie Failover-Designs, die den einzelnen Komponenten RPO entsprechen. RTO



- Konfigurieren Sie weniger anspruchsvolle Umgebungen (wie Entwicklungs- oder Testumgebungen) mit allen Services, die für einen Failover-Plan erforderlich sind. Stellen Sie die Lösungen mit Infrastructure as Code (IaC) bereit, um die Reproduzierbarkeit sicherzustellen.
- Konfigurieren Sie einen Wiederherstellungsstandort, z. B. eine zweite Region, um die Failover-Designs zu implementieren und zu testen. Falls erforderlich, können die Ressourcen für die Tests vorübergehend konfiguriert werden, um die zusätzlichen Kosten zu begrenzen.
- Ermitteln Sie, welche Failover-Pläne automatisiert werden AWS, welche durch einen DevOps Prozess automatisiert werden können und welche möglicherweise manuell ausgeführt werden. Dokumentieren und messen Sie die Daten der RTO einzelnen Services. RPO
- Erstellen Sie ein Failover-Playbook, das alle Schritte zum Failover jeder Ressource, Anwendung und jedes Services enthält.
- Erstellen Sie ein Failback-Playbook, das alle Schritte zum Failback (mit Zeitangabe) für jede Ressource, jede Anwendung und jeden Service enthält.
- Erstellen Sie einen Plan, um das Playbook zu initiieren und zu proben. Verwenden Sie Simulationen und Chaostests, um die Schritte des Playbooks und die Automatisierung zu testen.
- Stellen Sie bei Standortbeeinträchtigungen (z. B. Availability Zone oder AWS-Region) sicher, dass Sie über Systeme verfügen, die ein Failover auf intakte Ressourcen an unbeeinträchtigten Standorten ermöglichen. Überprüfen Sie Kontingente, die automatische Skalierung und laufende Ressourcen vor dem Failover-Test.

## Ressourcen

Zugehörige bewährte Methoden für Well-Architected:

- [REL13- Plan für DR](#)
- [REL10 — Verwenden Sie Fehlerisolierung, um Ihre Arbeitslast zu schützen](#)

Zugehörige Dokumente:

- [Einstellung RTO und RPO Ziele](#)
- [Failover mithilfe von gewichtetem Route 53-Routing](#)
- [Notfallwiederherstellung mit Amazon Application Recovery Controller](#)
- [EC2mit Autoscaling](#)
- [EC2Bereitstellungen — Multi-AZ](#)

- [ECSBereitstellungen — Multi-AZ](#)
- [Wechseln Sie den Datenverkehr mithilfe des Amazon Application Recovery Controllers](#)
- [Lambda mit einem Application Load Balancer und Failover](#)
- [ACMReplikation und Failover](#)
- [Parameter Store-Replikation und -Failover](#)
- [ECRregionsübergreifende Replikation und Failover](#)
- [Konfigurieren der regionsübergreifenden Replikation von Secrets Manager](#)
- [Aktivieren Sie die regionsübergreifende Replikation für EFS und Failover](#)
- [EFSRegionsübergreifende Replikation und Failover](#)
- [Netzwerk-Failover](#)
- [S3-Endpunkt-Failover mit MRAP](#)
- [Erstellen einer regionsübergreifenden Replikation für S3](#)
- [Anleitung für regionsübergreifendes Failover und Graceful Failback bei AWS](#)
- [Failover mit Global Accelerator über mehrere Regionen](#)
- [Failover mit DRS](#)
- [Erstellen von Mechanismen für die Notfallwiederherstellung mit Amazon Route 53](#)

Zugehörige Beispiele:

- [Notfallwiederherstellung aktiviert AWS](#)
- [Elastic Disaster Recovery aktiviert AWS](#)

REL11-BP03 Automatisieren Sie die Heilung auf allen Ebenen

Verwenden Sie bei Erkennung eines Fehlers automatisierte Funktionen, um Maßnahmen zur Behebung durchzuführen. Beeinträchtigungen können automatisch durch interne Service-Mechanismen behoben werden. Es kann aber auch erforderlich sein, Ressourcen neu zu starten oder Abhilfemaßnahmen durchzuführen.

Für selbstverwaltete Anwendungen und regionenübergreifende Korrekturen können Wiederherstellungskonzepte und automatisierte Korrekturprozesse aus [bestehenden bewährten Methoden](#) verwendet werden.

Die Möglichkeit, eine Ressource neu zu starten oder zu entfernen, ist ein wichtiges Instrument zur Behebung von Fehlern. Eine bewährte Methode besteht darin, Services nach Möglichkeit zustandslos zu betreiben. Dies verhindert den Datenverlust oder den Verlust der Verfügbarkeit bei einem Neustart der Ressource. In der Cloud können Sie (und sollten Sie üblicherweise) die gesamte Ressource (z. B. eine Datenverarbeitungs-Instance oder eine Serverless-Funktion) im Rahmen des Neustarts ersetzen. Der Neustart selbst ist eine einfache und zuverlässige Methode zur Wiederherstellung nach einem Ausfall. Bei Workloads treten viele verschiedene Arten von Fehlern auf. Fehler können bei Hardware, Software, Kommunikation und Betrieb auftreten.

Der Neustart oder Wiederholungsversuch gilt auch für Netzwerkanfragen. Nutzen Sie denselben Wiederherstellungsansatz für eine Netzwerk-Zeitüberschreitung und einen Abhängigkeitsfehler, bei dem die Abhängigkeit einen Fehler ausgibt. Beide Ereignisse wirken sich in ähnlicher Weise auf das System aus. Statt also zu versuchen, aus den einzelnen Ereignissen einen „Sonderfall“ zu konstruieren, sollten Sie eine ähnliche Strategie anwenden und versuchen, ein exponentielles Backoff mit Jitter durchzuführen. Die Fähigkeit zum Neustart ist eine Funktion, die in wiederherstellungsorientierten Datenverarbeitungs- und Hochverfügbarkeits-Cluster-Architekturen empfohlen wird.

Gewünschtes Ergebnis: Automatisierte Aktionen werden durchgeführt, um die Erkennung eines Fehlers zu beheben.

Typische Anti-Muster:

- Bereitstellung von Ressourcen ohne automatische Skalierung.
- Einzelne Bereitstellung von Anwendungen in Instances oder Containern.
- Bereitstellen von Anwendungen, die nicht ohne automatische Wiederherstellung an mehreren Standorten bereitgestellt werden können.
- Manuelle Reparatur von Anwendungen, die sich mit Auto Scaling und einer automatischen Wiederherstellung nicht reparieren lassen.
- Keine Automatisierung beim Failover von Datenbanken.
- Keine automatisierten Methoden zur Umleitung des Datenverkehrs auf neue Endpunkte.
- Keine Speicherreplikation.

Vorteile der Nutzung dieser bewährten Methode: Eine automatisierte Korrektur kann die mittlere Zeit bis zur Wiederherstellung verkürzen und Ihre Verfügbarkeit verbessern.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Hoch

## Implementierungsleitfaden

Designs für Amazon EKS oder andere Kubernetes-Dienste sollten sowohl minimale als auch maximale Replikat- oder Stateful-Sets sowie die minimale Cluster- und Knotengruppengröße beinhalten. Diese Mechanismen sorgen für ein Minimum an kontinuierlich verfügbaren Verarbeitungsressourcen und beheben gleichzeitig automatisch alle Fehler über die Steuerebene von Kubernetes.

Entwurfsmuster, auf die über einen Load Balancer mit Datenverarbeitungs-Clustern zugegriffen wird, sollten Auto-Scaling-Gruppen nutzen. Elastic Load Balancing (ELB) verteilt den eingehenden Anwendungsdatenverkehr automatisch auf mehrere Ziele und virtuelle Appliances in einer oder mehreren Availability Zones (AZs).

Bei Cluster-Datenverarbeitungs-Instances, die kein Load Balancing nutzen, sollte die Größe für den Verlust von mindestens einem Knoten ausgelegt sein. Auf diese Weise kann der Service mit möglicherweise reduzierter Kapazität weiterlaufen, während er einen neuen Knoten wiederherstellt. Beispieldienste sind Mongo, DynamoDB Accelerator, Amazon Redshift, Amazon, CassandraEMR, Kafka, MSK -EC2, Couchbase und Amazon Service. ELK OpenSearch Viele dieser Services können mit zusätzlichen Features zur Selbstheilung ausgestattet werden. Einige Cluster-Technologien müssen beim Verlust eines Knotens einen Alarm generieren, der einen automatisierten oder manuellen Workflow zur Wiederherstellung eines neuen Knotens auslöst. Dieser Workflow kann automatisiert werden, um Probleme schnell zu beheben. AWS Systems Manager

Amazon EventBridge kann verwendet werden, um Ereignisse wie CloudWatch Alarme oder Statusänderungen in anderen AWS Diensten zu überwachen und zu filtern. Auf der Grundlage von Ereignisinformationen kann es dann Systems Manager Automation oder andere Ziele aufrufen AWS Lambda, um eine benutzerdefinierte Behebungslogik für Ihren Workload auszuführen. Amazon EC2 Auto Scaling kann so konfiguriert werden, dass es beispielsweise den Zustand der EC2 Instanz überprüft. Wenn sich die Instance in einem anderen Status als in Betrieb befindet oder wenn der Systemstatus beeinträchtigt ist, betrachtet Amazon EC2 Auto Scaling die Instance als fehlerhaft und startet eine Ersatz-Instance. Bei Large-Scale-Ersetzungen (z. B. dem Verlust einer ganzen Availability Zone) ist für eine Hochverfügbarkeit die statische Stabilität vorzuziehen.

## Implementierungsschritte

- Verwenden Sie Auto-Scaling-Gruppen, um Tiers in einem Workload bereitzustellen. [Auto Scaling](#) kann zustandslose Anwendungen selbst reparieren und Kapazitäten hinzufügen oder entfernen.
- Verwenden Sie [Load Balancing](#) für die zuvor genannten Datenverarbeitungs-Instances und wählen Sie den entsprechenden Load Balancer-Typ aus.

- Erwägen Sie Healing for AmazonRDS. Konfigurieren Sie bei Standby-Instances das [automatische Failover](#) zur Standby-Instance. Für Amazon RDS Read Replica ist ein automatisierter Workflow erforderlich, um eine Read Replica primär zu machen.
- Implementieren Sie die [automatische Wiederherstellung für EC2 Instances, auf denen](#) Anwendungen bereitgestellt werden, die nicht an mehreren Standorten bereitgestellt werden können, und tolerieren Sie bei Fehlern einen Neustart. Mithilfe der automatischen Wiederherstellung kann ausgefallene Hardware ersetzt und die Instance neu gestartet werden, wenn die Anwendung sich nicht an mehreren Standorten bereitstellen lässt. Die Instance-Metadaten und die zugehörigen IP-Adressen sowie die [EBSVolumes](#) und Mount-Points für [Amazon Elastic File System oder File Systems for Lustre](#) und [Windows](#) werden beibehalten. Mithilfe [AWS OpsWorks](#) können Sie die automatische Heilung von EC2 Instances auf Layer-Ebene konfigurieren.
- Implementieren Sie die automatische Wiederherstellung mit [AWS Step Functions](#) und [AWS Lambda](#), wenn Sie keine automatische Skalierung oder automatische Wiederherstellung verwenden können oder wenn die automatische Wiederherstellung fehlschlägt. Wenn Sie die automatische Skalierung nicht verwenden können und entweder die automatische Wiederherstellung nicht verwenden können oder die automatische Wiederherstellung fehlschlägt, können Sie die Wiederherstellung mit AWS Step Functions und automatisieren AWS Lambda.
- [Amazon EventBridge](#) kann verwendet werden, um Ereignisse wie [CloudWatchAlarmer](#) oder Statusänderungen in anderen AWS Diensten zu überwachen und zu filtern. Auf der Grundlage von Ereignisinformationen kann es dann AWS Lambda (oder andere Ziele) aufrufen, um eine angepasste Wiederherstellungslogik für Ihre Workload auszuführen.

## Ressourcen

### Zugehörige bewährte Methoden:

- [Definition der Verfügbarkeit](#)
- [REL11-BP01 Überwachen Sie alle Komponenten des Workloads, um Fehler zu erkennen](#)

### Zugehörige Dokumente:

- [Funktionsweise von AWS Auto Scaling](#)
- [EC2Automatische Wiederherstellung durch Amazon](#)
- [Amazon Elastic Block Store \(AmazonEBS\)](#)
- [Amazon Elastic File System \(AmazonEFS\)](#)

- [Was ist Amazon FSx for Lustre?](#)
- [Was ist Amazon FSx for Windows File Server?](#)
- [AWS OpsWorks: Verwenden von Auto Healing zum Austausch fehlgeschlagener Instances](#)
- [Was ist AWS Step Functions?](#)
- [Was ist AWS Lambda?](#)
- [Was ist Amazon EventBridge?](#)
- [Amazon CloudWatch Alarms verwenden](#)
- [RDSAmazon-Failover](#)
- [SSM- Systems Manager Automatisierung](#)
- [Bewährte Methoden für eine widerstandsfähige Architektur](#)

Zugehörige Videos:

- [Automatisches Bereitstellen und Skalieren von OpenSearch Services](#)
- [Automatisches RDS Amazon-Failover](#)

Zugehörige Beispiele:

- [Workshop zum Thema Auto Scaling](#)
- [Amazon RDS Failover-Workshop](#)

Zugehörige Tools:

- [CloudWatch](#)
- [CloudWatch X-Ray](#)

REL11-BP04 Verlassen Sie sich bei der Wiederherstellung auf die Datenebene und nicht auf die Steuerebene

Kontrollebenen stellen die administrativen APIs Funktionen bereit, die zum Erstellen, Lesen und Beschreiben, Aktualisieren, Löschen und Auflisten (CRUDL) von Ressourcen verwendet werden, während Datenebenen den day-to-day Dienstverkehr regeln. Konzentrieren Sie sich bei der Implementierung von Wiederherstellungs- oder Abhilfemaßnahmen für Ereignisse, die sich möglicherweise auf die Ausfallsicherheit auswirken, auf eine minimale Anzahl von Operationen auf

der Steuerebene, um den Service wiederherzustellen, zu skalieren, zu reparieren oder einen Failover durchzuführen. Aktionen auf der Datenebene sollten während dieser Beeinträchtigungen Vorrang vor allen anderen Aktivitäten haben.

Die folgenden Aktionen gehören beispielsweise alle zur Steuerebene: Starten einer neuen Datenverarbeitungs-Instance, Erstellen von Block-Speicher und Beschreiben von Warteschlangen-Services. Wenn Sie Datenverarbeitungs-Instances starten, muss die Steuerebene mehrere Aufgaben erfüllen, z. B. einen physischen Host mit Kapazität finden, Netzwerkschnittstellen zuweisen, lokale Block-Speicher-Volumes vorbereiten, Anmeldeinformationen generieren und Sicherheitsregeln hinzufügen. Steuerebenen neigen zu einer komplizierten Orchestrierung.

Gewünschtes Ergebnis: Wenn bei einer Ressource eine Störung auftritt, ist das System in der Lage, diese automatisch oder manuell zu beheben, indem es den Datenverkehr von gestörten auf intakte Ressourcen umleitet.

Typische Anti-Muster:

- Abhängigkeit von der Änderung von DNS Datensätzen zur Umleitung des Datenverkehrs.
- Abhängigkeit von Skalierungsoperationen auf Steuerebene, um beeinträchtigte Komponenten aufgrund einer unzureichenden Bereitstellung von Ressourcen zu ersetzen.
- Verlassen Sie sich auf umfangreiche Maßnahmen, die mehrere Dienste und mehrere API Kontrollebenen umfassen, um jede Art von Beeinträchtigung zu beheben.

Vorteile der Nutzung dieser bewährten Methode: Eine höhere Erfolgsquote bei der automatisierten Behebung kann Ihre mittlere Zeit bis zur Wiederherstellung verkürzen und die Verfügbarkeit des Workloads verbessern.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel: Bei bestimmten Arten von Service-Einschränkungen sind Steuerebenen betroffen. Abhängigkeiten von der umfassenden Nutzung der Kontrollebene zur Behebung können die Wiederherstellungszeit (RTO) und die durchschnittliche Zeit bis zur Wiederherstellung (MTTR) verlängern.

Implementierungsleitfaden

Um die Aktionen auf der Datenebene zu begrenzen, bewerten Sie für jeden Service, welche Aktionen zur Wiederherstellung des Services erforderlich sind.

Nutzen Sie Amazon Application Recovery Controller, um den DNS Datenverkehr zu verlagern. Diese Funktionen überwachen kontinuierlich die Fähigkeit Ihrer Anwendung, sich nach Ausfällen zu

erholen, und ermöglichen es Ihnen AWS-Regionen, Ihre Anwendungswiederherstellung in mehreren Availability Zones und vor Ort zu kontrollieren.

Route 53-Routingrichtlinien verwenden die Steuerebene. Verlassen Sie sich also bei der Wiederherstellung nicht auf diese Ebene. Die Route 53-Datenebenen beantworten DNS Anfragen und führen Integritätsprüfungen durch und werten diese aus. Sie werden weltweit vertrieben und sind für ein [Service Level Agreement \(SLA\) mit 100-prozentiger Verfügbarkeit](#) konzipiert.

Die Route 53-Verwaltung APIs und die Konsolen, in denen Sie Route 53-Ressourcen erstellen, aktualisieren und löschen, werden auf Steuerungsebenen ausgeführt, die darauf ausgelegt sind, die hohe Konsistenz und Beständigkeit zu gewährleisten, die Sie bei der Verwaltung DNS benötigen. Zu diesem Zweck befinden sich die Steuerebenen in einer einzelnen Region, USA Ost (Nord-Virginia). Beide Systeme sind zwar auf hohe Zuverlässigkeit ausgelegt, die Steuerungsebenen sind jedoch nicht in der SLA enthalten. In seltenen Fällen kann es vorkommen, dass das ausfallsichere Design der Datenebene es ermöglicht, die Verfügbarkeit aufrechtzuerhalten, während die Steuerebene dies nicht tut. Verwenden Sie für die Notfallwiederherstellung und Failover-Mechanismen Datenebenen-Funktionen, um die bestmögliche Zuverlässigkeit bereitzustellen.

Gestalten Sie Ihre Recheninfrastruktur so, dass sie statisch stabil ist, um zu vermeiden, dass die Steuerungsebene während eines Vorfalls verwendet wird. Wenn Sie beispielsweise EC2 Amazon-Instances verwenden, vermeiden Sie es, neue Instances manuell bereitzustellen oder Auto Scaling Groups anzuweisen, als Reaktion darauf Instances hinzuzufügen. Für ein Höchstmaß an Ausfallsicherheit stellen Sie ausreichende Kapazitäten in dem für den Failover verwendeten Cluster bereit. Wenn dieser Kapazitätsschwellenwert begrenzt werden muss, richten Sie Drosselungen für das gesamte end-to-end System ein, um den Gesamtverkehr, der die begrenzten Ressourcen erreicht, sicher zu begrenzen.

Für Dienste wie Amazon DynamoDB, Amazon API Gateway, Load Balancer und AWS Lambda Serverless nutzt die Nutzung dieser Dienste die Datenebene. Das Erstellen neuer Funktionen, Load Balancer, API Gateways oder DynamoDB-Tabellen ist jedoch eine Aktion auf der Kontrollebene und sollte vor der Degradation abgeschlossen werden, um ein Ereignis vorzubereiten und Failover-Aktionen zu proben. Für Amazon RDS ermöglichen Aktionen auf Datenebene den Zugriff auf Daten.

Weitere Informationen zu Datenebenen, Kontrollebenen und dazu, wie Services AWS entwickelt werden, um Hochverfügbarkeitsziele zu erreichen, finden Sie unter [Statische Stabilität mithilfe von Availability Zones](#).

Erfahren Sie, welche Operationen auf der Datenebene und welche Operationen auf der Steuerebene ausgeführt werden.



## Implementierungsschritte

Bewerten Sie für jede Workload, die nach einem Störfall wiederhergestellt werden muss, das Failover-Runbook, das Hochverfügbarkeitsdesign, das Auto Healing Design oder den Plan zur Wiederherstellung von HA-Ressourcen. Identifizieren Sie jede Aktion, die als Aktion auf der Steuerebene in Frage kommt.

Ziehen Sie in Erwägung, eine Aktion auf der Steuerebene in eine Aktion auf der Datenebene umzuwandeln:

- Auto Scaling (Kontrollebene) auf vorkalierte EC2 Amazon-Ressourcen (Datenebene)
- Skalierung von EC2 Amazon-Instances (Kontrollebene) auf AWS Lambda Skalierung (Datenebene)
- Bewerten Sie alle Entwürfe unter Verwendung von Kubernetes und der Art der Aktionen auf der Steuerebene. Das Hinzufügen von Pods ist eine Aktion auf der Datenebene von Kubernetes. Aktionen sollten sich auf das Hinzufügen von Pods und nicht von Knoten beschränken. Die Verwendung von [überdimensionierten Knoten](#) ist die bevorzugte Methode zur Begrenzung von Aktionen auf der Steuerebene.

Ziehen Sie alternative Ansätze in Betracht, bei denen Aktionen auf der Datenebene dieselbe Maßnahme bewirken können.

- Route 53 Änderung aufzeichnen (Kontrollebene) oder Amazon Application Recovery Controller (Datenebene)
- [Route 53-Zustandsprüfungen für weitere automatisierte Aktualisierungen](#)

Ziehen Sie einige Services in einer sekundären Region in Betracht, wenn der Service geschäftskritisch ist, um mehr Aktionen auf der Steuerebene und Datenebene in einer nicht betroffenen Region zu ermöglichen.

- Amazon EC2 Auto Scaling oder Amazon EKS in einer primären Region im Vergleich zu Amazon EC2 Auto Scaling oder Amazon EKS in einer sekundären Region und Weiterleitung des Datenverkehrs in eine sekundäre Region (Aktion auf Kontrollebene)
- Ein Lesereplikat in der sekundären primären Region erstellen oder Versuchen derselben Aktion in der primären Region (Aktion auf der Steuerebene)

## Ressourcen

### Zugehörige bewährte Methoden:

- [Definition der Verfügbarkeit](#)
- [REL11-BP01 Überwachen Sie alle Komponenten des Workloads, um Fehler zu erkennen](#)

### Zugehörige Dokumente:

- [APNPartner: Partner, die Ihnen bei der Automatisierung Ihrer Fehlertoleranz helfen können](#)
- [AWS Marketplace: Zur Erzielung von Fehlertoleranz geeignete Produkte](#)
- [Amazon Builders' Library: Vermeiden von Überlastungen verteilter Systeme durch Übernahme der Steuerung durch den kleineren Service](#)
- [Amazon DynamoDB API \(Steuerungsebene und Datenebene\)](#)
- [AWS Lambda Ausführungen](#) (aufgeteilt in die Steuerungsebene und die Datenebene)
- [AWS Elemental MediaStore Datenebene](#)
- [Aufbau hochbelastbarer Anwendungen mit Amazon Application Recovery Controller, Teil 1: Stack mit einer einzelnen Region](#)
- [Aufbau hochbelastbarer Anwendungen mit Amazon Application Recovery Controller, Teil 2: Multi-Region-Stack](#)
- [Erstellen von Mechanismen für die Notfallwiederherstellung mit Amazon Route 53](#)
- [Was ist Amazon Application Recovery Controller](#)
- [Kubernetes-Steuerungsebene und -Datenebene](#)

### Zugehörige Videos:

- [Zurück zu den Basics – Verwendung statischer Stabilität](#)
- [Aufbau robuster Workloads an mehreren Standorten mithilfe globaler Services AWS](#)

### Zugehörige Beispiele:

- [Wir stellen vor: Amazon Application Recovery Controller](#)
- [Amazon Builders' Library: Vermeiden von Überlastungen verteilter Systeme durch Übernahme der Steuerung durch den kleineren Service](#)

- [Aufbau hochbelastbarer Anwendungen mit Amazon Application Recovery Controller, Teil 1: Stack mit einer einzelnen Region](#)
- [Aufbau hochbelastbarer Anwendungen mit Amazon Application Recovery Controller, Teil 2: Multi-Region-Stack](#)
- [Statische Stabilität mithilfe von Availability Zones](#)

Zugehörige Tools:

- [Amazon CloudWatch](#)
- [AWS X-Ray](#)

REL11-BP05 Verwenden Sie statische Stabilität, um bimodales Verhalten zu verhindern

Workloads sollten statisch stabil sein und nur in einem einzigen Normalmodus ausgeführt werden. Bimodales Verhalten liegt vor, wenn sich die Workload im Normalmodus und im Fehlermodus unterschiedlich verhält.

Sie können beispielsweise versuchen, nach einem Ausfall der Availability Zone eine Wiederherstellung durchzuführen, indem Sie neue Instances in einer anderen Availability Zone starten. Dies kann zu einer bimodalen Reaktion während eines Ausfallmodus führen. Stattdessen sollten Sie Workloads erstellen, die statisch stabil sind und nur in einem Modus betrieben werden. In diesem Beispiel hätten diese Instances vor dem Ausfall in der zweiten Availability Zone bereitgestellt werden sollen. Dieses statische Stabilitätsdesign verifiziert, dass die Workload nur in einem einzigen Modus ausgeführt wird.

Gewünschtes Ergebnis: Workloads zeigen im Normalmodus und im Fehlermodus kein bimodales Verhalten.

Typische Anti-Muster:

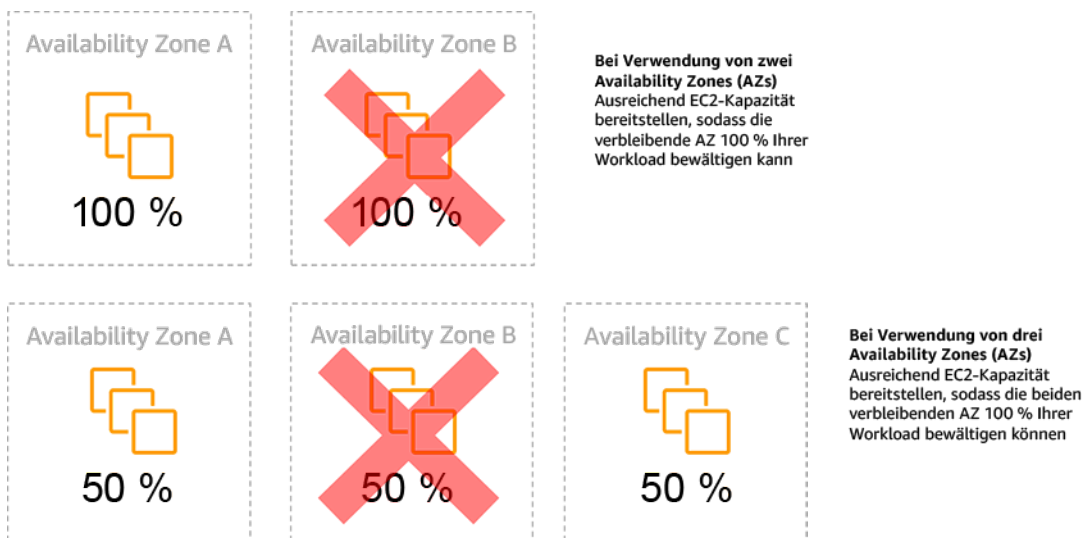
- Es wird davon ausgegangen, dass Ressourcen unabhängig vom Umfang des Fehlers immer bereitgestellt werden können.
- Während eines Fehlers wird versucht, dynamisch Ressourcen zu erwerben.
- Es werden keine ausreichenden Ressourcen für Zonen oder Regionen bereitgestellt, bis ein Fehler auftritt.
- Statische stabile Designs werden nur für Rechenressourcen in Erwägung gezogen.

Vorteile der Nutzung dieser bewährten Methode: Workloads, die mit statisch stabilen Designs ausgeführt werden, sind in der Lage, bei normalen Ereignissen und bei Ausfällen vorhersehbare Ergebnisse erzielen.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel

### Implementierungsleitfaden

Bimodales Verhalten bedeutet, dass eine Workload im normalen Modus und im Fehlermodus unterschiedliche Verhaltensweisen zeigt (z. B. Verlassen auf den Start neuer Instances bei Ausfall einer Availability Zone). Ein Beispiel für bimodales Verhalten ist, wenn stabile EC2 Amazon-Designs genügend Instances in jeder Availability Zone bereitstellen, um die Arbeitslast zu bewältigen, wenn eine AZ entfernt würde. Elastic Load Balancing oder Amazon Route 53 Health würde prüfen, ob eine Last von den beeinträchtigten Instances weg verlagert werden kann. Verwenden Sie diese Option, AWS Auto Scaling um nach der Verlagerung des Datenverkehrs asynchron Instances aus der ausgefallenen Zone zu ersetzen und sie in den fehlerfreien Zonen zu starten. Statische Stabilität bei der Bereitstellung von Rechenleistung (wie EC2 Instances oder Containern) sorgt für höchste Zuverlässigkeit.



### Statische Stabilität von EC2 Instanzen in allen Availability Zones

Dies muss gegen die Kosten für dieses Modell und den geschäftlichen Nutzen der Aufrechterhaltung der Workload in allen Ausfallsituationen abgewogen werden. Es ist kostengünstiger, weniger Rechenkapazität bereitzustellen und bei einem Ausfall neue Instances zu starten. Bei großen Ausfällen (z. B. bei Beeinträchtigung einer Availability Zone oder Region) ist dieser Ansatz jedoch weniger effektiv, da er sowohl auf einer Betriebsebene als auch auf der Verfügbarkeit ausreichender Ressourcen in den nicht betroffenen Zonen oder Regionen beruht.

Ihre Lösung sollte die Anforderungen an die Zuverlässigkeit und Kosten für Ihre Workload gegeneinander abwägen. Statische Stabilitätsarchitekturen gelten für eine Vielzahl von Architekturen, darunter Recheninstanzen, die über Availability Zones verteilt sind, Datenbank-Read-Replica-Designs, Kubernetes (AmazonEKS) -Cluster-Designs und Failover-Architekturen mit mehreren Regionen.

Es ist auch möglich, ein statisch stabileres Design zu implementieren, indem mehr Ressourcen in jeder Zone verwendet werden. Wenn Sie eine größere Anzahl von Zonen hinzufügen, verringert sich die Menge der zusätzlichen Rechenleistung, die Sie für die statische Stabilität benötigen.

Ein weiteres Beispiel für bimodales Verhalten ist eine Netzwerk-Zeitüberschreitung, die dazu führen kann, dass ein System versucht, den Konfigurationsstatus des gesamten Systems zu aktualisieren. Dies kann zur unerwarteten Auslastung einer anderen Komponente führen, die daraufhin ausfallen könnte, was möglicherweise weitere unerwartete Konsequenzen nach sich zieht. Diese negative Feedback-Schleife wirkt sich auf die Verfügbarkeit Ihrer Workload aus. Deshalb sollten Sie stattdessen Systeme erstellen, die statisch stabil sind und nur in einem Modus betrieben werden. Ein statisch stabiles Design arbeitet konstant und aktualisiert den Konfigurationsstatus in regelmäßigen Abständen. Wenn ein Aufruf fehlschlägt, verwendet der Workload den zuvor zwischengespeicherten Wert und löst einen Alarm aus.

Ein weiteres Beispiel für bimodales Verhalten: Sie lassen zu, dass Clients im Fehlerfall den Workload-Cache umgehen. Dies scheint eine Lösung zu sein, die Clientanforderungen erfüllt, sie kann aber die Belastung Ihrer Workload erheblich ändern und führt wahrscheinlich zu Fehlern.

Bewerten Sie kritische Workloads, um festzustellen, für welche Workloads diese Art von Resilienzdesign erforderlich ist. Für diejenigen, die als kritisch eingestuft werden, muss jede Anwendungskomponente überprüft werden. Beispiele für Services, für die statische Stabilitätsbewertungen erforderlich sind:

- Berechnung: AmazonEC2, EKS -EC2, ECS -EC2, EMR - EC2
- Datenbanken: Amazon Redshift, AmazonRDS, Amazon Aurora
- Speicher: Amazon S3 (Single Zone), Amazon EFS (Halterungen), Amazon FSx (Halterungen)
- Load Balancer: bei bestimmten Designs

### Implementierungsschritte

- Erstellen Sie Systeme, die statisch stabil sind und nur in einem einzigen Modus ausgeführt werden. Stellen Sie in diesem Fall in jeder Availability Zone oder Region genügend Instances bereit, um die

Workload-Kapazität zu bewältigen, falls eine Availability Zone oder Region entfernt würde. Eine Vielzahl von Services kann für das Routing zu intakten Ressourcen verwendet werden, z. B.:

- [Regionalübergreifendes Routing DNS](#)
- [MRAP Amazon S3 MultiRegion S3-Routing](#)
- [AWS Global Accelerator](#)
- [Amazon Application Recovery Controller](#)
- Konfigurieren Sie [Datenbank-Lesereplikate](#), um den Verlust einer einzelnen primären Instance oder eines Lesereplikats zu berücksichtigen. Wenn der Datenverkehr von Lesereplikaten bedient wird, sollte die Menge in jeder Availability Zone und jeder Region dem Gesamtbedarf im Fall eines Zonen- oder Regionsausfalls entsprechen.
- Konfigurieren Sie kritische Daten in einem Amazon S3-Speicher, der so konzipiert ist, dass er für die gespeicherten Daten beim Ausfall einer Availability Zone statisch stabil ist. Wenn die [Amazon S3 One Zone-IA](#)-Speicherklasse verwendet wird, sollte diese nicht als statisch stabil angesehen werden, da der Ausfall dieser Zone den Zugriff auf die zugehörigen gespeicherten Daten minimiert.
- [Load Balancer](#) sind manchmal falsch oder so konfiguriert, dass sie eine bestimmte Availability Zone bedienen. In diesem Fall könnte das statisch stabile Design darin bestehen, eine Arbeitslast AZs in einem komplexeren Design auf mehrere zu verteilen. Das ursprüngliche Design kann aus Sicherheits-, Latenz- oder Kostengründen verwendet werden, um den Verkehr zwischen den Zonen zu reduzieren.

## Ressourcen

Zugehörige bewährte Methoden für Well-Architected:

- [Definition der Verfügbarkeit](#)
- [REL11-BP01 Überwachen Sie alle Komponenten des Workloads, um Fehler zu erkennen](#)
- [REL11-BP04 Verlassen Sie sich bei der Wiederherstellung auf die Datenebene und nicht auf die Steuerebene](#)

Zugehörige Dokumente:

- [Minimierung der Abhängigkeiten bei der Planung der Notfallwiederherstellung](#)
- [Die Amazon Builders' Library: Statische Stabilität mithilfe von Availability Zones](#)
- [Grenzen für die Fehlerisolierung](#)
- [Statische Stabilität mithilfe von Availability Zones](#)

- [Mehrere Zonen RDS](#)
- [Minimierung der Abhängigkeiten bei der Planung der Notfallwiederherstellung](#)
- [Regionalübergreifendes Routing DNS](#)
- [MRAP Amazon S3 MultiRegion S3-Routing](#)
- [AWS Global Accelerator](#)
- [Amazon Application Recovery Controller](#)
- [Amazon S3 \(einzelne Zone\)](#)
- [Zonenübergreifendes Load Balancing](#)

Zugehörige Videos:

- [Statische Stabilität in AWS: AWS re:Invent 2019: Einführung in die Amazon Builders' Library \(\) DOP328](#)

REL11-BP06 Benachrichtigungen senden, wenn Ereignisse die Verfügbarkeit beeinträchtigen

Benachrichtigungen werden nach Erkennung von Schwellenwertüberschreitungen gesendet, auch wenn das durch das Ereignis verursachte Problem automatisch behoben wurde.

Auto Healing sorgt dafür, dass Ihre Workload zuverlässig ist. Allerdings können dadurch auch zugrunde liegende Probleme verschleiert werden, die behoben werden müssen. Implementieren Sie geeignete Überwachungsfunktionen und Ereignisse, damit Sie Problemmuster erkennen können, einschließlich solcher, die durch Auto Healing behoben werden. Auf diese Weise können Sie die Fehlerursachen beheben.

Resiliente Systeme sind so konzipiert, dass Verschlechterungsereignisse sofort an die entsprechenden Teams gemeldet werden. Diese Benachrichtigungen sollten über einen oder mehrere Kommunikationskanäle gesendet werden.

Gewünschtes Ergebnis: Bei Überschreitung von Schwellenwerten wie Fehlerraten, Latenz oder anderen wichtigen Leistungsindikatoren (Key Performance Indicator KPI) werden sofort Benachrichtigungen an die Betriebsteams gesendet, sodass diese Probleme so schnell wie möglich behoben werden und die Auswirkungen auf die Benutzer vermieden oder minimiert werden.

Typische Anti-Muster:

- Es werden zu viele Alarme gesendet.

- Es werden Alarme gesendet, die keine Maßnahmen erfordern.
- Die Schwellenwerte für den Alarm sind zu hoch (überempfindlich) oder zu niedrig (nicht empfindlich genug).
- Es werden keine Alarme für externe Abhängigkeiten gesendet.
- [Graue Fehler](#) werden bei der Planung von Überwachung und Alarmen nicht berücksichtigt.
- Es werden automatische Reparaturen ausgeführt, ohne das entsprechende Team darüber zu benachrichtigen, dass eine Reparatur erforderlich war.

Vorteile der Einführung dieser bewährten Methode: Durch Benachrichtigungen über die Wiederherstellung werden Betriebs- und Geschäftsteams über Serviceeinbußen informiert, sodass sie sofort reagieren können, um sowohl die mittlere Erkennungszeit (MTTD) als auch die durchschnittliche Reparaturzeit (MTTR) zu minimieren. Benachrichtigungen zu Wiederherstellungen stellen sicher, dass Sie selten auftretende Probleme nicht ignorieren.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel. Wenn keine geeigneten Überwachungsfunktionen und Mechanismen zur Benachrichtigung bei Ereignissen implementiert werden, kann dies dazu führen, dass Problemmuster nicht erkannt werden, einschließlich solcher, die durch Auto Healing behoben werden. Ein Team wird nur dann auf eine Verschlechterung des Systems aufmerksam gemacht, wenn Benutzer den Kundendienst kontaktieren oder der Fehler zufällig bemerkt wird.

### Implementierungsleitfaden

Bei der Definition einer Überwachungsstrategie ist ein ausgelöster Alarm ein häufiges Ereignis. Dieses Ereignis würde wahrscheinlich eine Kennung für den Alarm enthalten, den Alarmstatus (z. B. IN ALARM oder OK) und Einzelheiten darüber, was ihn ausgelöst hat. In vielen Fällen sollte ein Alarmereignis erkannt und eine E-Mail-Benachrichtigung gesendet werden. Dies ist ein Beispiel für eine Aktion bei einem Alarm. Die Alarmbenachrichtigung ist für die Beobachtbarkeit von entscheidender Bedeutung, da hiermit die richtigen Personen darüber informiert werden, dass ein Problem vorliegt. Wenn die Aktionen bei Ereignissen in Ihrer Lösung für die Beobachtbarkeit ausgereift sind, kann das Problem automatisch behoben werden, ohne dass menschliches Eingreifen erforderlich ist.

Sobald Alarme für die KPI Überwachung eingerichtet wurden, sollten Warnmeldungen an die entsprechenden Teams gesendet werden, wenn die Schwellenwerte überschritten werden. Diese Warnungen können auch verwendet werden, um automatisierte Prozesse auszulösen, die versuchen, die Verschlechterung zu beheben.



Für eine komplexere Schwellenwertüberwachung sollten zusammengesetzte Alarme in Betracht gezogen werden. Kombinierte Alarme verwenden eine Reihe von Alarmen KPI zur Überwachung, um eine Warnung auf der Grundlage der betrieblichen Geschäftslogik zu erstellen. CloudWatchAlarme können so konfiguriert werden, dass sie E-Mails senden oder Vorfälle mithilfe der SNS Amazon-Integration oder Amazon in Incident-Tracking-Systemen von Drittanbietern protokollieren EventBridge.

## Implementierungsschritte

Erstellen Sie verschiedene Arten von Alarmen, je nachdem, wie Workloads überwacht werden, z. B.:

- Anwendungsalarme werden verwendet, um zu erkennen, wenn ein Teil der Workload nicht ordnungsgemäß funktioniert.
- [Infrastrukturalarme](#) geben an, wann Ressourcen skaliert werden müssen. Alarme können visuell auf Dashboards angezeigt werden, Benachrichtigungen über Amazon SNS oder E-Mail senden und mithilfe von Auto Scaling Workload-Ressourcen nach innen oder außen skalieren.
- Einfache [statische Alarme](#) können erstellt werden, um zu überwachen, wann eine Metrik für eine bestimmte Anzahl von Bewertungszeiträumen einen statischen Schwellenwert überschreitet.
- [Zusammengesetzte Alarme](#) können komplexe Alarme aus mehreren Quellen berücksichtigen.
- Nachdem der Alarm erstellt wurde, erstellen Sie entsprechende Benachrichtigungsereignisse. Sie können [Amazon](#) direkt aufrufen, um Benachrichtigungen SNS API zu senden und alle Automatisierungen zur Problembehebung oder Kommunikation zu verknüpfen.
- Integrieren Sie die [Amazon Health Aware-Überwachung](#), um die Überwachung von AWS Ressourcen zu ermöglichen, bei denen es zu Leistungseinbußen kommen könnte. Für geschäftskritische Workloads bietet diese Lösung Zugriff auf proaktive Benachrichtigungen in Echtzeit für Services. AWS

## Ressourcen

Zugehörige bewährte Methoden für Well-Architected:

- [Definition der Verfügbarkeit](#)

Zugehörige Dokumente:

- [Einen CloudWatch Alarm auf der Grundlage eines statischen Schwellenwerts erstellen](#)
- [Was ist Amazon EventBridge?](#)

- [Was ist Amazon Simple Notification Service?](#)
- [Veröffentlichen von benutzerdefinierten Metriken](#)
- [Amazon CloudWatch Alarms verwenden](#)
- [Amazon Health Aware \(AHA\)](#)
- [CloudWatch Composite-Alarme einrichten](#)
- [Was gibt es Neues im Bereich AWS Observability auf der re:Invent 2022](#)

Zugehörige Tools:

- [CloudWatch](#)
- [CloudWatch X-Ray](#)

REL11-BP07 Gestalten Sie Ihr Produkt so, dass es Verfügbarkeitsziele und Service Level Agreements für Verfügbarkeit erfüllt ( ) SLAs

Gestalten Sie Ihr Produkt so, dass es die Verfügbarkeitsziele und die Service Level Agreements für die Verfügbarkeit erfüllt ( )SLAs. Wenn Sie Verfügbarkeitsziele oder Verfügbarkeitsziele veröffentlichen oder diesen privat zustimmen, stellen Sie sicherSLAs, dass Ihre Architektur und Ihre Betriebsprozesse darauf ausgelegt sind, diese Ziele zu unterstützen.

Gewünschtes Ergebnis: Jede Anwendung hat ein definiertes Ziel in Bezug auf Verfügbarkeit und SLA Leistungskennzahlen, die überwacht und verwaltet werden können, um die Geschäftsergebnisse zu erreichen.

Typische Anti-Muster:

- Entwerfen und Bereitstellen von Workloads, ohne irgendwelche festzulegenSLAs.
- SLADie Metriken sind ohne Begründung oder Geschäftsanforderungen zu hoch angesetzt.
- Festlegung SLAs ohne Berücksichtigung der Abhängigkeiten und der ihnen zugrunde liegenden SLA Abhängigkeiten.
- Anwendungsdesigns werden ohne Berücksichtigung des Modells der geteilten Verantwortung für die Ausfallsicherheit erstellt.

Vorteile der Nutzung dieser bewährten Methode: Die Entwicklung von Anwendungen auf der Grundlage wichtiger Ausfallsicherheitsziele hilft Ihnen dabei, Ihre Geschäftsziele und

Kundenerwartungen zu erfüllen. Diese Ziele sind die Grundlage für die Entwicklung von Anwendungen, bei der verschiedene Technologien bewertet und verschiedene Kompromisse in Betracht gezogen werden.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel

### Implementierungsleitfaden

Bei der Entwicklung von Anwendungen müssen Sie eine Reihe von Anforderungen berücksichtigen, die sich aus geschäftlichen, operativen und finanziellen Zielen ergeben. Im Rahmen der operativen Anforderungen müssen für Workloads spezifische Metriken für die Ausfallsicherheit festgelegt werden, damit sie angemessen überwacht und unterstützt werden können. Die Metriken für die Ausfallsicherheit sollten nicht nach der Bereitstellung der Workload festgelegt oder ermittelt werden. Sie sollten in der Entwurfsphase festgelegt werden und als Leitlinien für verschiedene Entscheidungen und Abwägungen dienen.

- Jede Workload sollte ihre eigenen Metriken für die Ausfallsicherheit haben. Diese Metriken können sich von anderen geschäftlichen Anwendungen unterscheiden.
- Die Reduzierung von Abhängigkeiten kann sich positiv auf die Verfügbarkeit auswirken. Jeder Workload sollte seine Abhängigkeiten und deren Abhängigkeiten berücksichtigen SLAs. Wählen Sie im Allgemeinen Abhängigkeiten mit Verfügbarkeitszielen aus, die den Zielen Ihrer Workload entsprechen oder höher sind.
- Ziehen Sie eine lose Verkoppelung in Betracht, damit Ihre Workload trotz der Beeinträchtigung durch Abhängigkeiten korrekt arbeiten kann, sofern dies möglich ist.
- Reduzieren Sie die Abhängigkeiten auf der Steuerebene, insbesondere während der Wiederherstellung oder einer Beeinträchtigung. Evaluieren Sie Designs, die für geschäftskritische Workloads statisch stabil sind. Nutzen Sie den sparsamen Umgang mit Ressourcen, um die Verfügbarkeit dieser Abhängigkeiten in einer Workload zu erhöhen.
- Beobachtbarkeit und Instrumentierung sind entscheidend, um dies zu erreichen, SLAs indem die mittlere Zeit bis zur Erkennung (MTTD) und die mittlere Zeit bis zur Reparatur (MTTR) reduziert werden.
- Weniger häufige Ausfälle (länger MTBF), kürzere Fehlererkennungszeiten (kürzer MTTD) und kürzere Reparaturzeiten (kürzer MTTR) sind die drei Faktoren, die zur Verbesserung der Verfügbarkeit in verteilten Systemen genutzt werden.
- Das Festlegen und Einhalten von Metriken für die Ausfallsicherheit einer Workload ist eine der Grundlagen für jedes effektive Design. Diese Designs müssen Kompromisse in Bezug auf Designkomplexität, Service-Abhängigkeiten, Leistung, Skalierung und Kosten berücksichtigen.

## Implementierungsschritte

- Überprüfen und dokumentieren Sie das Workload-Design unter Berücksichtigung der folgenden Fragen:
  - Wo werden die Steuerebenen in der Workload verwendet?
  - Wie implementiert die Workload die Ausfallsicherheit?
  - Wie sehen die Designmuster für die Skalierung, automatische Skalierung, Redundanz und hochverfügbare Komponenten aus?
  - Welche Anforderungen gibt es an die Datenkonsistenz und -verfügbarkeit?
  - Gibt es Überlegungen zur sparsamen Nutzung von Ressourcen oder zur statischen Stabilität von Ressourcen?
  - Welche Abhängigkeiten bestehen zwischen den Services?
- Definieren Sie SLA Metriken auf der Grundlage der Workload-Architektur und arbeiten Sie dabei mit den Beteiligten zusammen. SLAs berücksichtigen Sie alle Abhängigkeiten, die vom Workload verwendet werden.
- Sobald das SLA Ziel festgelegt wurde, optimieren Sie die Architektur, um das zu erreichen SLA.
- Sobald das Design festgelegt ist, das die Anforderungen erfüllen wird SLA, implementieren Sie betriebliche Änderungen, Prozessautomatisierung und Runbooks, wobei der Schwerpunkt auch auf der Reduzierung MTTD und MTTR liegt.
- Nach der Bereitstellung sollten Sie die überwachen und darüber Bericht erstatten. SLA

## Ressourcen

### Zugehörige bewährte Methoden:

- [REL03-BP01 Wählen Sie, wie Sie Ihre Arbeitslast segmentieren möchten](#)
- [REL10-BP01 Stellen Sie den Workload an mehreren Standorten bereit](#)
- [REL11-BP01 Überwachen Sie alle Komponenten des Workloads, um Fehler zu erkennen](#)
- [REL11-BP03 Automatisieren Sie die Heilung auf allen Ebenen](#)
- [REL12-BP05 Testen Sie die Resilienz mithilfe von Chaos Engineering](#)
- [REL13-BP01 Definieren Sie Wiederherstellungsziele für Ausfallzeiten und Datenverlust](#)
- [Grundlegendes zum Workload-Status](#)

### Zugehörige Dokumente:

- [Verfügbarkeit mit Redundanz](#)
- [Säule der Zuverlässigkeit – Verfügbarkeit](#)
- [Messung der Verfügbarkeit](#)
- [AWS Grenzen der Fehlerisolierung](#)
- [Modell der geteilten Verantwortung für Ausfallsicherheit](#)
- [Statische Stabilität mithilfe von Availability Zones](#)
- [AWS Servicelevel-Vereinbarungen \(SLAs\)](#)
- [Leitlinien für zellbasierte Architektur auf AWS](#)
- [AWS Infrastruktur](#)
- [Whitepaper „Erweiterte Multi-AZ Resilience-Muster“](#)

Zugehörige Services:

- [Amazon CloudWatch](#)
- [AWS Config](#)
- [AWS Trusted Advisor](#)

## REL12. Wie lässt sich die Zuverlässigkeit testen?

Nachdem Sie Ihre Workload so konzipiert haben, dass sie den Belastungen der Produktion standhält, sind Tests die einzige Möglichkeit, sie auf die erwartete Funktionalität und Ausfallsicherheit hin zu testen.

Bewährte Methoden

- [REL12-BP01 Verwenden Sie Playbooks, um Fehler zu untersuchen](#)
- [REL12-BP02 Führen Sie eine Analyse nach dem Vorfall durch](#)
- [REL12-BP03 Funktionale Anforderungen testen](#)
- [REL12-BP04 Skalierung und Leistungsanforderungen für Tests](#)
- [REL12-BP05 Testen Sie die Resilienz mithilfe von Chaos Engineering](#)
- [REL12-BP06 Regelmäßig Spieltage durchführen](#)

## REL12-BP01 Verwenden Sie Playbooks, um Fehler zu untersuchen

Gestatten Sie konsistente und schnelle Antworten auf noch unbekannte Fehlerszenarien, indem Sie den Untersuchungsprozess in Playbooks dokumentieren. Playbooks sind vordefinierte Abläufe zum Identifizieren der Faktoren, die zu einem Fehlerszenario beitragen. Die Ergebnisse aus jedem Prozessschritt sind die Grundlage für die nächsten Schritte. Nach diesem Muster wird vorgegangen, bis das Problem identifiziert oder eskaliert wird.

Das Playbook ist eine proaktive Planung, die für effektive Reaktionen erforderlich ist. Wenn nicht vom Playbook abgedeckte Fehlerszenarien in der Produktion auftreten, beheben Sie zunächst das Problem. Analysieren Sie danach die unternommenen Schritte und verwenden Sie diese, um einen neuen Eintrag im Playbook hinzuzufügen.

Beachten Sie, dass Playbooks als Reaktion auf bestimmte Vorfälle verwendet werden, während Runbooks verwendet werden, um bestimmte Ergebnisse zu erzielen. Häufig werden Runbooks für Routineaktivitäten verwendet, Playbooks hingegen, um auf außergewöhnliche Ereignisse zu reagieren.

Typische Anti-Muster:

- Planen der Bereitstellung einer Workload, ohne die Prozesse zur Diagnose von Problemen oder Reaktion auf Vorfälle zu kennen.
- Ungeplante Entscheidungen darüber, in welchen Systemen bei der Untersuchung von Ereignissen Protokolle und Metriken erfasst werden sollen.
- Metriken und Ereignisse werden nicht lange genug aufbewahrt, um die Daten abrufen zu können.

Vorteile der Nutzung dieser bewährten Methode: Durch die Erfassung von Playbooks wird sichergestellt, dass Prozesse konsistent befolgt werden können. Ihre Playbooks werden als Code festgehalten, um die Entstehung von Fehlern durch manuelle Aktivitäten zu reduzieren. Durch die Automatisierung von Playbooks kann schneller auf Ereignisse reagiert werden, weil Teammitglieder nicht eingreifen müssen oder ihnen vor dem Eingreifen zusätzliche Informationen zur Verfügung gestellt werden.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Hoch

Implementierungsleitfaden

- Ermitteln Sie Probleme mithilfe von Playbooks. Playbooks sind dokumentierte Prozesse für die Untersuchung von Problemen. Durch die Dokumentation der Prozesse in Playbooks werden die

Voraussetzungen für eine einheitliche und schnelle Reaktion auf Fehlerszenarien geschaffen. Playbooks müssen die Informationen und Anleitungen enthalten, die eine entsprechend qualifizierte Person zum Zusammentragen sachdienlicher Informationen, zum Identifizieren möglicher Fehlerursachen, zum Isolieren von Fehlern und zum Bestimmen beitragender Faktoren (zum Analysieren nach einem Vorfall) benötigt.

- Implementieren Sie Playbooks als Code. Führen Sie Ihre Operationen als Code aus, indem Sie Skripts für Ihre Playbooks erstellen, um Konsistenz sicherzustellen und Fehler zu reduzieren, die durch manuelle Prozesse verursacht werden. Playbooks können aus mehreren Skripts bestehen, die die verschiedenen Schritte darstellen, die erforderlich sein können, um die zu einem Problem beitragenden Faktoren zu identifizieren. Runbook-Aktivitäten können aufgerufen oder im Rahmen von Playbook-Aktivitäten ausgeführt werden. Sie können auch als Antwort auf identifizierte Ereignisse die Ausführung eines Playbooks auslösen.
  - [Automatisieren Sie Ihre operativen Playbooks mit AWS Systems Manager](#)
  - [AWS Systems Manager Befehl ausführen](#)
  - [AWS Systems Manager Automation](#)
  - [Was ist AWS Lambda?](#)
  - [Was ist Amazon EventBridge?](#)
  - [Amazon CloudWatch Alarms verwenden](#)

## Ressourcen

### Zugehörige Dokumente:

- [AWS Systems Manager Automatisierung](#)
- [AWS Systems Manager Befehl ausführen](#)
- [Automatisieren Sie Ihre operativen Playbooks mit AWS Systems Manager](#)
- [Amazon CloudWatch Alarms verwenden](#)
- [Kanaren verwenden \(Amazon CloudWatch Synthetics\)](#)
- [Was ist Amazon EventBridge?](#)
- [Was ist AWS Lambda?](#)

### Zugehörige Beispiele:

- [Automating operations with Playbooks and Runbooks](#)

## REL12-BP02 Führen Sie eine Analyse nach dem Vorfall durch

Überprüfen Sie die Ereignisse mit Auswirkungen auf Kunden und bestimmen Sie die beitragenden Faktoren und Präventivmaßnahmen. Entwickeln Sie anhand dieser Informationen Abhilfemaßnahmen, um Wiederholungen einzuschränken oder zu verhindern. Entwickeln Sie Verfahren für schnelle und effektive Reaktionen. Informieren Sie nach Bedarf auf zielgruppengerechte Weise über beitragende Faktoren und Korrekturmaßnahmen. Legen Sie eine Kommunikationsmethode fest, um andere bei Bedarf über die Ursachen zu informieren.

Bewerten Sie, warum bestehende Tests das Problem nicht gefunden haben. Fügen Sie Tests für diesen Fall hinzu, wenn noch keine Tests vorhanden sind.

Gewünschtes Ergebnis: Ihre Teams haben einen konsistenten und vereinbarten Ansatz für den Umgang mit Analysen nach einem Vorfall. Ein Mechanismus ist die [Korrektur des Fehlers \(\) COE](#) -Prozesses. Der COE Prozess hilft Ihren Teams dabei, die Hauptursachen für Vorfälle zu identifizieren, zu verstehen und zu beheben. Gleichzeitig werden Mechanismen und Leitplanken entwickelt, um die Wahrscheinlichkeit zu begrenzen, dass derselbe Vorfall erneut auftritt.

Typische Anti-Muster:

- Beitragende Faktoren werden ermittelt, es wird jedoch nicht weiter nach anderen potenziellen Problemen und Lösungsansätzen gesucht.
- Es werden nur menschliche Fehlerursachen ermittelt, es wird aber keine Schulung oder Automatisierung bereitgestellt, die menschliche Fehler verhindern könnte.
- Der Fokus liegt auf Schuldzuweisungen, anstatt die Ursache zu verstehen, wodurch eine Kultur der Angst entsteht und eine offene Kommunikation behindert wird.
- Es wird versäumt, Erkenntnisse weiterzugeben, wodurch die Ergebnisse der Ereignisanalyse in einer kleinen Gruppe bleiben und andere nicht von den gewonnenen Erkenntnissen profitieren können.
- Es gibt keine Mechanismen zur Erfassung des institutionellen Wissens, wodurch wertvolle Erkenntnisse verloren gehen, da die gewonnenen Erkenntnisse nicht in Form von aktualisierten bewährten Methoden festgehalten werden und es zu wiederholten Vorfällen mit derselben oder einer ähnlichen Ursache kommt.

Vorteile der Nutzung dieser bewährten Methode: Durch Analysen von Vorfällen und das Teilen von Ergebnissen können die Risiken für andere Workloads mit den gleichen beitragenden Faktoren die Risiken verringert werden. Außerdem können Abhilfemaßnahmen oder automatisierte Wiederherstellungen implementiert werden, bevor es zu einem Vorfall kommt.



Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Hoch

## Implementierungsleitfaden

Durch gute Analysen nach Vorfällen lassen sich allgemeine Lösungen für Probleme mit Architekturmustern ermitteln, die Sie bereits an anderer Stelle in den Systemen anwenden.

Ein Eckpfeiler des COE Prozesses ist die Dokumentation und Behebung von Problemen. Es wird empfohlen, ein standardisiertes Verfahren zur Dokumentation kritischer Ursachen festzulegen und sicherzustellen, dass diese überprüft und behoben werden. Weisen Sie die Verantwortung für den Analyseprozess nach einem Vorfall eindeutig zu. Benennen Sie ein verantwortliches Team oder eine Person, die die Untersuchungen von Vorfällen und die Folgemaßnahmen beaufsichtigt.

Fördern Sie eine Kultur, die sich auf Lernen und Verbesserung konzentriert, anstatt Schuldzuweisungen vorzunehmen. Betonen Sie, dass das Ziel darin besteht, zukünftige Vorfälle zu verhindern, und nicht darin, Einzelpersonen zu strafen.

Entwickeln Sie klar definierte Verfahren für die Durchführung von Analysen nach einem Vorfall. Diese Verfahren sollten die zu ergreifenden Schritte, die zu sammelnden Informationen und die Schlüsselfragen, die während der Analyse zu behandeln sind, darlegen. Untersuchen Sie Vorfälle gründlich und gehen Sie dabei über die unmittelbaren Ursachen hinaus, um die Grundursachen und die beitragenden Faktoren zu ermitteln. Verwenden Sie Techniken wie die [5-Why-Methode](#), um sich eingehend mit den zugrundeliegenden Problemen zu befassen.

Führen Sie eine Sammlung von Erkenntnissen, die Sie aus der Analyse von Vorfällen gewonnen haben. Dieses institutionelle Wissen kann als Referenz für zukünftige Vorfälle und Präventionsmaßnahmen dienen. Tauschen Sie die Ergebnisse und Erkenntnisse aus den Analysen nach dem Vorfall aus und erwägen Sie, offene Besprechungen nach dem Vorfall abzuhalten, um die gewonnenen Erkenntnisse zu diskutieren.

## Implementierungsschritte

- Achten Sie bei der Analyse nach einem Vorfall darauf, dass der Prozess frei von Schuldzuweisungen ist. Dies ermöglicht es den an dem Vorfall beteiligten Personen, die vorgeschlagenen Korrekturmaßnahmen sachlich zu beurteilen und fördert eine ehrliche Selbsteinschätzung und die Zusammenarbeit zwischen den Teams.
- Definieren Sie eine standardisierte Methode zur Dokumentation kritischer Probleme. Ein solches Dokument könnte beispielsweise folgendermaßen strukturiert sein:
  - Was ist passiert?

- Welche Auswirkungen gab es auf Kunden und Ihr Unternehmen?
- Was war die Ursache?
- Welche Daten haben Sie, um dies zu unterstützen?
  - Zum Beispiel Metriken und Grafiken
- Welches waren die kritischen Auswirkungen auf die Säulen, insbesondere in puncto Sicherheit?
  - Beim Entwerfen von Workloads sollten Sie je nach Geschäftskontext zwischen den einzelnen Säulen abwägen. 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. Sicherheit ist immer oberstes Gebot, da Sie Ihre Kunden schützen müssen.
- Welche Erkenntnisse haben Sie gewonnen?
- Welche Maßnahmen ergreifen Sie?
  - Aktionselemente
  - Verwandte Elemente
- Erstellen Sie klar definierte Standardverfahren für die Durchführung von Analysen nach einem Vorfall.
- Richten Sie ein standardisiertes Verfahren zur Meldung von Vorfällen ein. Dokumentieren Sie alle Vorfälle ausführlich, einschließlich des ersten Vorfallberichts, der Protokolle, der Kommunikation und der während des Vorfalls getroffenen Maßnahmen.
- Denken Sie daran, dass ein Vorfall nicht unbedingt einen Ausfall zur Folge haben muss. Es könnte sich um einen Beinahe-Unfall handeln oder um ein System, das auf unerwartete Weise funktioniert und dennoch seine Geschäftsfunktion erfüllt.
- Verbessern Sie Ihren Analyseprozess nach einem Vorfall kontinuierlich auf Grundlage von Rückmeldungen und gewonnenen Erkenntnissen.
- Halten Sie die wichtigsten Erkenntnisse in einem Wissensmanagementsystem fest und überlegen Sie, welche Muster in Entwicklerhandbücher oder Checklisten vor der Bereitstellung aufgenommen werden sollten.

## Ressourcen

### Zugehörige Dokumente:

- [Warum sollten Sie eine Fehlerkorrektur entwickeln \(\) COE](#)

## Zugehörige Videos:

- [Der Ansatz von Amazon: erfolgreiches Scheitern](#)
- [AWS re:Invent 2021 — Amazon Builders' Library: Operational Excellence bei Amazon](#)

## REL12-BP03 Funktionale Anforderungen testen

Verwenden Sie Techniken wie Modultests und Integrationstests, die die erforderliche Funktionalität validieren.

Im Idealfall sollten diese Tests automatisch als Teil von Build- und Bereitstellungsaktionen ausgeführt werden. Verwenden Sie AWS CodePipeline zum Beispiel, dass Entwickler Änderungen in ein Quell-Repository übertragen, wo die Änderungen CodePipeline automatisch erkannt werden. Diese Änderungen werden vorgenommen und Tests werden ausgeführt. Nach Abschluss der Tests wird der erstellte Code für weitere Tests auf Staging-Servern bereitgestellt. CodePipeline führt vom Staging-Server aus weitere Tests aus, z. B. Integrations- oder Auslastungstests. Nach erfolgreichem Abschluss dieser Tests wird der getestete und genehmigte Code auf Produktionsinstanzen CodePipeline bereitgestellt.

Darüber hinaus zeigt die Erfahrung, dass synthetische Transaktionstests (auch bekannt als Canary-Tests, aber nicht zu verwechseln mit Canary-Bereitstellungen), die das Kundenverhalten simulieren können, zu den wichtigsten Testprozessen gehören. Führen Sie diese Tests für Ihre Workload-Endpunkte konstant von verschiedenen Remote-Standorten aus. Mit Amazon CloudWatch Synthetics können Sie [Kanarien erstellen](#), um Ihre Endgeräte zu überwachen und APIs

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Hoch

## Implementierungsleitfaden

- Testen Sie funktionale Anforderungen. Dazu gehören Komponenten- und Integrationstests, mit denen die erforderliche Funktionalität validiert wird.
  - [Verwenden Sie CodePipeline with AWS CodeBuild , um Code zu testen und Builds auszuführen](#)
  - [AWS CodePipeline Fügt Support für Integrationstests und benutzerdefinierte Integrationstests hinzu mit AWS CodeBuild](#)
  - [Kontinuierliche Bereitstellung und kontinuierliche Integration](#)
  - [Kanaren verwenden \(Amazon CloudWatch Synthetics\)](#)
  - [Automatisierung von Softwaretests](#)

## Ressourcen

### Zugehörige Dokumente:

- [APNPartner: Partner, die bei der Implementierung einer kontinuierlichen Integrationspipeline helfen können](#)
- [AWS CodePipeline Fügt Support für Integrationstests und benutzerdefinierte Integrationstests hinzu mit AWS CodeBuild](#)
- [AWS Marketplace: Für die kontinuierliche Integration geeignete Produkte](#)
- [Kontinuierliche Bereitstellung und kontinuierliche Integration](#)
- [Automatisierung von Softwaretests](#)
- [Verwenden Sie CodePipeline with AWS CodeBuild , um Code zu testen und Builds auszuführen](#)
- [Kanaren verwenden \(Amazon CloudWatch Synthetics\)](#)

### REL12-BP04 Skalierung und Leistungsanforderungen für Tests

Nutzen Sie Techniken wie Lasttests, um zu prüfen, ob die Workload die Skalierungs- und Leistungsanforderungen erfüllt.

In der Cloud können Sie bei Bedarf eine Testumgebung in Produktionsgröße für Ihre Workload erstellen. Wenn Sie diese Tests auf einer herunterskalierten Infrastruktur ausführen, müssen Sie die Ergebnisse auf den Maßstab der Produktionsumgebung hochrechnen. Last- und Leistungstests können auch in der Produktion durchgeführt werden. Achten Sie dabei darauf, Benutzer nicht zu beeinträchtigen und Ihre Testdaten mit Tags zu versehen, sodass sie nicht mit Benutzerdaten vermischt werden und Nutzungsstatistiken oder Produktionsberichte verfälschen.

Stellen Sie mit Tests sicher, dass Ihre Basisressourcen, Skalierungseinstellungen, Service Quotas und die Ausfallsicherheit unter Auslastung wie erwartet funktionieren.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Hoch

### Implementierungsleitfaden

- Testen Sie Skalierungs- und Leistungsanforderungen. Führen Sie Lasttests durch, um zu prüfen, ob die Workload die Skalierungs- und Leistungsanforderungen erfüllt.
  - [Testen verteilter Lasten auf AWS: simulieren Sie Tausende verbundener Benutzer](#)
  - [Apache JMeter](#)

- Stellen Sie Ihre Anwendung in einer Umgebung bereit, die mit Ihrer Produktionsumgebung identisch ist, und führen Sie einen Lasttest durch.
- Erstellen Sie auf Grundlage von „Infrastructure as Code“-Konzepten eine Umgebung, die Ihrer Produktionsumgebung möglichst ähnlich ist.

## Ressourcen

### Zugehörige Dokumente:

- [Distributed Load Testing auf AWS: Simulieren Sie Tausende verbundener Benutzer](#)
- [Apache JMeter](#)

## REL12-BP05 Testen Sie die Resilienz mithilfe von Chaos Engineering

Führen Sie regelmäßig Chaos-Experimente in oder nahe an Produktionsumgebungen aus, um zu verstehen, wie Ihr System auf ungünstige Bedingungen reagiert.

### Gewünschtes Ergebnis:

Die Ausfallsicherheit der Workload wird regelmäßig durch die Anwendung von Chaos-Engineering in Form von Fehlerinjektionsexperimenten oder einer Injektion unerwarteter Last überprüft. Dazu kommen Tests der Ausfallsicherheit, um das bekannte erwartete Verhalten der Workload während eines Ereignisses zu validieren. Kombinieren Sie Chaos-Engineering mit Tests der Ausfallsicherheit, um sicher zu sein, dass Ihre Workload Komponentenausfällen standhalten und sich von unerwarteten Unterbrechungen erholen kann – mit minimalen oder gar keinen Auswirkungen.

### Typische Anti-Muster:

- Auslegung der Systeme auf Ausfallsicherheit, aber keine Überprüfung, wie die Workload als Ganzes funktioniert, wenn Fehler auftreten.
- Keine Experimente unter echten Bedingungen und der erwarteten Last.
- Keine Behandlung der Experimente als Code und fehlendes Aufrechterhalten während des Entwicklungszyklus.
- Keine Durchführung von Chaos-Experimenten als Teil Ihrer CI/CD-Pipeline und außerhalb von Bereitstellungen.
- Keine Nutzung früherer Analysen nach Vorfällen bei der Entscheidung über die Fehler, mit denen experimentiert werden soll.

Vorteile der Nutzung dieser bewährten Methode: Durch die Injektion von Fehlern zur Überprüfung der Resilienz Ihrer Workload gewinnen Sie die nötige Zuversicht, dass die Wiederherstellungsverfahren Ihres resilienten Entwurfs im Fall eines realen Fehlers funktionieren.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel

### Implementierungsleitfaden

Das Chaos-Engineering bietet Ihren Teams die nötigen Chancen, um auf kontrollierte Weise kontinuierlich reale Störungen (Simulationen) auf Serviceanbieter-, Infrastruktur-, Workload- und Komponentenebene zu injizieren – mit nur minimalen oder gar keinen Auswirkungen auf Ihre Kunden. Ihre Teams können so aus Fehlern lernen und die Resilienz Ihrer Workloads beobachten, messen und verbessern. Darüber hinaus können sie überprüfen, ob Warnungen ausgelöst werden und die Teams über Ereignisse benachrichtigt werden.

Bei kontinuierlicher Ausführung kann das Chaos-Engineering Mängel in Ihren Workloads aufzeigen, die sich negativ auf Verfügbarkeit und Ausführung auswirken könnten, wenn sie nicht behoben werden.

#### Note

Beim Chaos-Engineering geht es um das Experimentieren mit einem System, um sich davon zu überzeugen, dass das System in der Produktion auch außergewöhnlichen Bedingungen standhalten kann. – [Grundlagen des Chaos-Engineering](#)

Wenn ein System diesen Disruptionen standhalten kann, sollte das Chaos-Experiment weiter als automatisierter Regressionstest ausgeführt werden. Auf diese Weise sollten Chaos-Experimente als Teil Ihres Systementwicklungszyklus (SDLC) und als Teil Ihrer CI/CD-Pipeline durchgeführt werden.

Um sicherzustellen, dass Ihre Workload resilient gegenüber dem Ausfall von Komponenten ist, sollten Sie im Rahmen Ihrer Experimente Ereignisse aus der Praxis injizieren. Experimentieren Sie beispielsweise mit dem Verlust von EC2 Amazon-Instances oder dem Failover der primären RDS Amazon-Datenbank-Instance und stellen Sie sicher, dass Ihre Arbeitslast nicht (oder nur minimal) beeinträchtigt wird. Mit einer Kombination von Komponentenfehlern könnten Sie Ereignisse simulieren, die von einer Disruption in einer Availability Zone verursacht werden könnten.

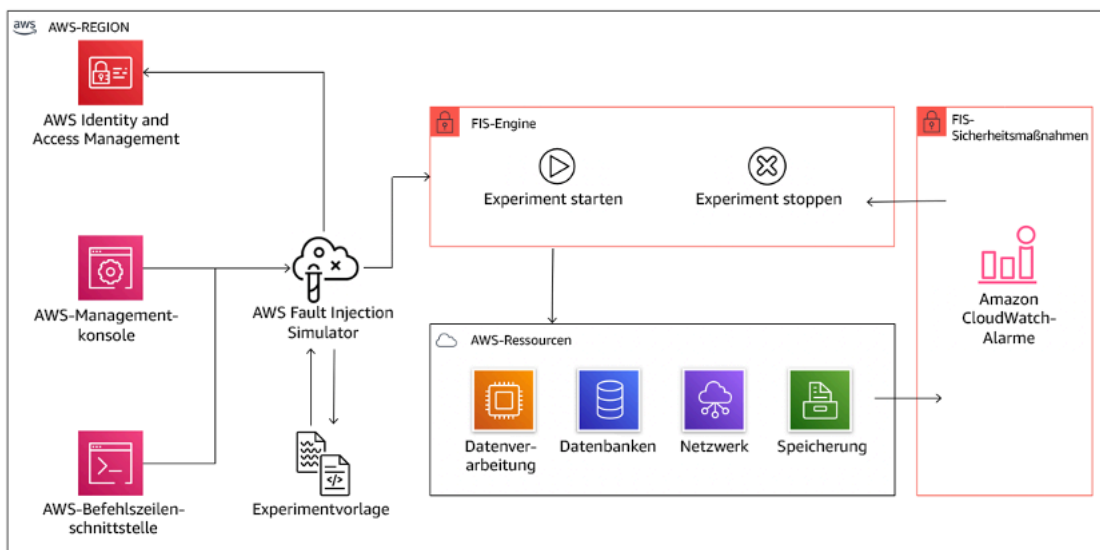
Bei Fehlern auf Anwendungsebene (wie Abstürzen) können Sie mit Stressfaktoren wie Arbeitsspeicher und Erschöpfung beginnen. CPU

Zur Validierung von [Fallback- oder Failover-Mechanismen](#) für externe Abhängigkeiten, die bei zeitweisen Netzwerkdisruptionen ausgelöst werden, sollten Ihre Komponenten diese Ereignisse durch das Blockieren des Zugriffs auf externe Anbieter über einen bestimmten Zeitraum simulieren, der von wenigen Sekunden bis zu mehreren Stunden dauern kann.

Andere Degradierungsmodi führen möglicherweise zu einer reduzierten Funktionalität und zu verzögerten Reaktionen, was eine Disruption Ihrer Services verursachen kann. Bekannte Quellen für diese Degradierung sind eine erhöhte Latenz bei kritischen Services und eine unzuverlässige Netzwerkkommunikation (Verlust von Paketen). Experimente mit diesen Fehlern, einschließlich Netzwerkeffekten wie Latenz, verworfenen Nachrichten und DNS Ausfällen, könnten die Unfähigkeit beinhalten, einen Namen aufzulösen, den DNS Dienst zu erreichen oder Verbindungen zu abhängigen Diensten herzustellen.

### Chaos-Engineering-Tools:

AWS Fault Injection Service (AWS FIS) ist ein vollständig verwalteter Dienst zur Durchführung von Fault-Injection-Experimenten, der als Teil Ihrer CD-Pipeline oder außerhalb der Pipeline verwendet werden kann. AWS FIS ist eine gute Wahl für Spieltage mit Chaos Engineering. Es unterstützt die gleichzeitige Einführung von Fehlern bei verschiedenen Ressourcentypen, darunter AmazonEC2, Amazon Elastic Container Service (AmazonECS), Amazon Elastic Kubernetes Service (AmazonEKS) und Amazon RDS. Zu diesen Fehlern gehören die Terminierung von Ressourcen, das Erzwingen von Failovers, Überlastung CPU oder Speicherauslastung, Drosselung, Latenz und Paketverlust. Da es in Amazon CloudWatch Alarms integriert ist, können Sie Stoppbedingungen als Leitplanken einrichten, um ein Experiment rückgängig zu machen, wenn es unerwartete Auswirkungen hat.



AWS Fault Injection Service lässt sich in AWS Ressourcen integrieren, sodass Sie Fault-Injection-Experimente für Ihre Workloads durchführen können.

Es gibt auch verschiedene Drittanbieteroptionen für Fehlerinjektionsexperimente. Dazu gehören Open-Source-Tools wie [Chaos Toolkit](#), [Chaos Mesh](#) und [Litmus Chaos](#) sowie kommerzielle Tools wie Gremlin. Es ist in [Chaos Mesh und Litmus Chaos AWS FIS integrierbar AWS](#), sodass Sie die Workflows zur Fehlerinjektion zwischen mehreren Tools koordinieren können, um den Umfang der Fehler zu erweitern, bei denen Fehler behoben werden können. Sie können beispielsweise CPU mithilfe von Chaos Mesh- oder Litmus-Fehlern einen Stresstest auf einem Pod ausführen und gleichzeitig einen zufällig ausgewählten Prozentsatz von Clusterknoten mithilfe von AWS FIS Fehleraktionen beenden.

## Implementierungsschritte

### 1. Ermitteln Sie die Fehler, mit denen experimentiert werden soll.

Bewerten Sie das Design Ihrer Workload in Bezug auf die Resilienz. Solche Designs (die unter Verwendung der bewährten Methoden des [Well-Architected Framework](#) erstellt wurden) berücksichtigen Risiken, die auf kritischen Abhängigkeiten, vergangenen Ereignissen, bekannten Problemen und Compliance-Anforderungen basieren. Listen Sie die einzelnen Elemente des Designs auf, die Resilienz zeigen sollen, und die Fehler, denen es standhalten soll. Weitere Informationen zur Erstellung solcher Listen finden Sie im [Whitepaper zur Überprüfung der betrieblichen Bereitschaft](#), in dem Sie auch erfahren, wie Sie einen Prozess erstellen können, um das Wiederauftreten früherer Vorfälle zu verhindern. Der Prozess zur Analyse der Fehlermodi und -auswirkungen (FMEA) bietet Ihnen ein Framework für die Durchführung einer Analyse von Ausfällen auf Komponentenebene und deren Auswirkungen auf Ihre Arbeitslast. FMEA wird von Adrian Cockcroft in [Failure Modes and Continuous Resilience](#) ausführlicher beschrieben.

### 2. Weisen Sie jedem Fehler eine Priorität zu.

Beginnen Sie mit einer groben Kategorisierung wie „Hoch“, „Mittel“ oder „Niedrig“. Berücksichtigen Sie bei der Festlegung der Priorität die Häufigkeit des Fehlers und die Auswirkungen des Fehlers auf die Workload insgesamt.

Analysieren Sie hinsichtlich der Häufigkeit eines bestimmten Fehlers frühere Daten für die betreffende Workload, wenn verfügbar. Wenn keine Daten verfügbar sind, verwenden Sie Daten zu anderen Workloads, die in einer ähnlichen Umgebung ausgeführt werden.

Bei der Betrachtung der Auswirkungen eines bestimmten Fehlers gilt, dass die Auswirkungen im Allgemeinen umso größer sind, je größer der vom Fehler betroffene Bereich ist. Sie sollten auch

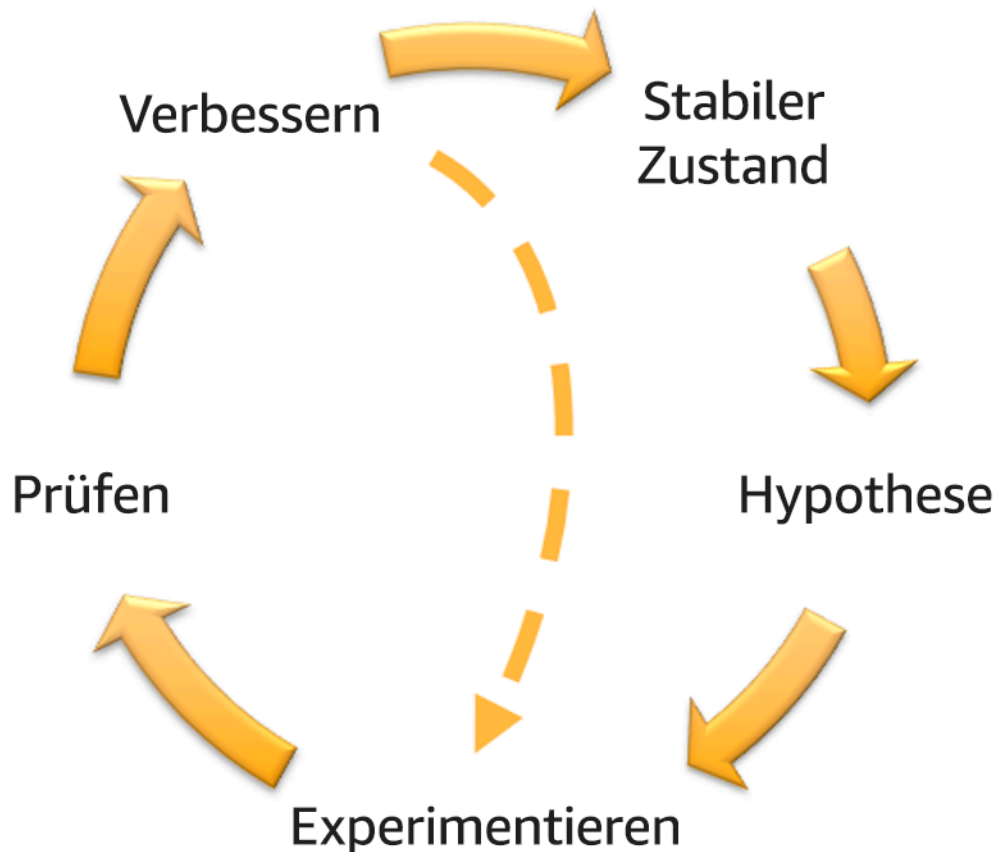


das Design und den Zweck der Workload berücksichtigen. Beispielsweise ist für eine Workload, die Daten transformiert und analysiert, der Zugriff auf die Quelldatenspeicher von kritischer Bedeutung. In diesem Fall würden Sie Experimente im Zusammenhang mit Zugriffsfehlern, Zugriffsdrosselungen und Latenzen priorisieren.

Nach Vorfällen durchgeführte Analysen stellen eine gute Datenquelle dar, um Häufigkeit und Auswirkungen von Fehlerarten besser zu verstehen.

Legen Sie anhand der zugewiesenen Priorität die Fehler fest, mit denen zuerst experimentiert werden soll, und die Reihenfolge, in der neue Fehlerinjektionsexperimente entwickelt werden sollen.

3. Für jedes von Ihnen ausgeführte Experiment sollten Sie sich am Schwungrad für Chaos-Engineering und kontinuierliche Resilienz in der folgenden Abbildung orientieren.



Schwungrad für Chaos-Engineering und kontinuierliche Resilienz unter Verwendung der wissenschaftlichen Methode von Adrian Hornsby.

- a. Definieren Sie den Steady-State als die messbare Ausgabe einer Workload, die ein normales Verhalten zeigt.


Ihre Workload befindet sich im Steady-State, wenn sie zuverlässig und wie erwartet ausgeführt wird. Daher sollten Sie die Integrität Ihrer Workload überprüfen, bevor Sie den Steady-State definieren. Steady-State bedeutet nicht notwendigerweise, dass sich ein Fehler nicht auf die Workload auswirkt, da ein bestimmter Prozentsatz an Fehlern innerhalb akzeptabler Grenzen liegen könnte. Der Steady-State ist die Basislinie, die Sie während des Experiments beobachten. Diese wird Anomalien aufweisen, wenn Ihre Hypothese, die Sie im nächsten Schritt definieren, nicht die erwarteten Ergebnisse zeigt.

Ein stabiler Zustand eines Zahlungssystems kann beispielsweise als die Verarbeitung von 300 Transaktionen TPS mit einer Erfolgsquote von 99% und einer Umlaufzeit von 500 ms definiert werden.

- b. Formulieren Sie eine Hypothese dazu, wie die Workload auf den Fehler reagieren wird.

Eine gute Hypothese basiert darauf, wie die Workload den Fehler voraussichtlich bewältigt, um den Steady-State zu wahren. Die Hypothese besagt, dass bei einem Fehler eines spezifischen Typs das System oder die Workload weiter im Steady-State bleibt, da die Workload mit bestimmten Resilienzmerkmalen entworfen wurde. Der spezifische Fehlertyp und die Fehlerbewältigung sollten in der Hypothese angegeben werden.

Sie können für die Hypothese die folgende Vorlage verwenden (andere Formulierungen sind jedoch auch akzeptabel):

 Note

Wenn *specific fault* tritt auf, der *workload name* Arbeitslast wird *describe mitigating controls* zu pflegen *business or technical metric impact*.

Beispielsweise:

- Wenn 20% der Knoten in der EKS Amazon-Knotengruppe abgeschaltet werden, bedient Transaction Create API weiterhin das 99. Perzentil der Anfragen in weniger als 100 ms (Steady State). Die EKS Amazon-Knoten werden innerhalb von fünf Minuten wiederhergestellt, und die Pods werden innerhalb von acht Minuten nach Beginn des

Experiments geplant und verarbeiten den Datenverkehr. Warnungen werden innerhalb von drei Minuten ausgelöst.


- Wenn eine einzelne EC2 Amazon-Instance ausfällt, veranlasst die Elastic Load Balancing-Zustandsprüfung des Bestellsystems, dass Elastic Load Balancing nur Anfragen an die verbleibenden fehlerfreien Instances sendet, während Amazon EC2 Auto Scaling die ausgefallene Instance ersetzt, wodurch ein Anstieg der serverseitigen (5xx) Fehler (Steady State) um weniger als 0,01% aufrechterhalten wird.
  - Wenn die primäre RDS Amazon-Datenbank-Instance ausfällt, führt der Supply-Chain-Datenerfassungs-Workload einen Failover durch und stellt eine Verbindung zur RDS Standby-Amazon-Datenbank-Instance her, um weniger als 1 Minute an Lese- oder Schreibfehlern der Datenbank aufrechtzuerhalten (Steady State).
- c. Führen Sie das Experiment aus, indem Sie den Fehler injizieren.

Ein Experiment sollte grundsätzlich nicht zu einem Ausfall führen und von der Workload toleriert werden. Wenn Sie wissen, dass die Workload ausfallen wird, sollten Sie das Experiment nicht durchführen. Das Chaos-Engineering sollte verwendet werden, um bekannt-unbekannte oder unbekannt-unbekannte Ereignisse zu untersuchen. Bekannt-unbekannte Ereignisse sind Dinge, derer Sie sich bewusst sind, die Sie aber nicht vollständig verstehen, und unbekannt-unbekannte Ereignisse sind Dinge, derer Sie sich nicht bewusst sind und die Sie auch nicht vollständig verstehen. Wenn Sie Experimente für eine Workload ausführen, von der Sie wissen, dass sie fehlerhaft ist, werden Sie keine neuen Erkenntnisse gewinnen. Ihr Experiment sollte sorgfältig geplant sein, einen klaren Wirkungsumfang besitzen und einen Rollback-Mechanismus besitzen, der bei unerwarteten Störungen angewendet werden kann. Wenn eine sorgfältige Überprüfung zeigt, dass Ihre Workload das Experiment überstehen sollte, können Sie das Experiment starten. Für die Injektion von Fehlern gibt es verschiedene Optionen. Für Workloads in AWS bietet [AWS FIS](#) viele vordefinierte Fehlersimulationen, die als [Aktionen](#) bezeichnet werden. Sie können auch benutzerdefinierte Aktionen definieren, die AWS FIS unter Verwendung von [AWS Systems Manager Dokumenten](#) ausgeführt werden.

Wir raten davon ab, angepasste Skripts für Chaos-Experimente zu verwenden, es sei denn, die Skripts können den aktuellen Zustand der Workload erkennen, können Protokolle ausgeben und stellen Rollback-Mechanismen und Stoppbedingungen bereit, soweit möglich.

Ein effektives Framework oder Toolset, das Chaos-Engineering unterstützt, sollte den aktuellen Status des Experiments nachverfolgen, Protokolle ausgeben und Rollback-Mechanismen bereitstellen, um eine kontrollierte Durchführung des Experiments zu unterstützen. Beginnen Sie mit einem etablierten Service wie AWS FIS diesem, der es Ihnen ermöglicht, Experimente

mit einem klar definierten Umfang und Sicherheitsmechanismen durchzuführen, die das Experiment rückgängig machen, wenn das Experiment zu unerwarteten Turbulenzen führt. Weitere Informationen zu einer Vielzahl von Experimenten mit AWS FIS Chaos Engineering finden Sie auch im Lab [Resilient and Well-Architected Apps with Chaos Engineering](#). Außerdem analysiert [AWS Resilience Hub](#) Ihre Workload und erstellt Experimente, die Sie in AWS FIS implementieren und ausführen können.

 Note

Sie sollten den Umfang und die Auswirkungen jedes Experiments genau verstehen. Wir empfehlen, Fehler zunächst in einer Nichtproduktionsumgebung zu simulieren, bevor sie in der Produktion ausgeführt werden.

Experimente sollten in der Produktion unter realer Last ausgeführt werden, wobei [Canary-Bereitstellungen](#) verwendet werden sollten, die sowohl eine Steuerung als auch eine experimentelle Systembereitstellung ermöglichen, sofern dies möglich ist. Die Ausführung von Experimenten außerhalb von Spitzenzeiten stellt ein empfehlenswertes Verfahren dar, um potenzielle Auswirkungen zu reduzieren, wenn ein Experiment zum ersten Mal in der Produktion durchgeführt wird. Wenn die Verwendung von tatsächlichem Kunden-Traffic ein zu großes Risiko darstellt, können Sie unter Verwendung der Kontroll- und Experimentbereitstellungen Experimente mit synthetischem Datenverkehr in der Produktionsinfrastruktur durchführen. Wenn ein Experiment nicht in der Produktion ausgeführt werden kann, führen Sie es in einer Präproduktionsumgebung aus, die der Produktionsumgebung so nahe wie möglich ist.

Sie müssen einen Integritätsschutz einrichten und überwachen, um sicherzustellen, dass sich das Experiment nicht jenseits akzeptabler Grenzen auf den Datenverkehr in der Produktionsumgebung oder andere Systeme auswirkt. Richten Sie Stoppbedingungen ein, um ein Experiment anhalten zu können, wenn es in einer Integritätsschutz-Metrik einen von Ihnen definierten Schwellenwert erreicht. Diese Metriken sollten die Metrik für den Steady-State der Workload und die Metrik für die Komponenten einschließen, in die Sie den Fehler injizieren. Die [synthetische Überwachung](#) (auch als Benutzer-Canary bezeichnet) gehört zu den Metriken, die Sie in der Regel als Benutzer-Proxy einschließen sollten. [Stoppbedingungen für AWS FIS](#) werden als Teil der Experimentvorlage unterstützt. Es sind bis zu fünf Stoppbedingungen pro Vorlage möglich.

Zu den Grundsätzen des Chaos-Engineering gehört die Minimierung von Umfang und Auswirkungen des Experiments:

Auch wenn einige kurzfristige negative Auswirkungen zulässig sein sollten, ist der Chaos-Engineer dafür verantwortlich, die Auswirkungen der Experimente zu minimieren und einzudämmen.

Eine Methode für die Überprüfung des Umfangs und der möglichen Auswirkungen besteht darin, das Experiment statt in der Produktionsumgebung zunächst in einer Nichtproduktionsumgebung durchzuführen. Dabei wird überprüft, ob die Schwellenwerte für Stoppbedingungen während des Experiments wie vorgesehen aktiviert werden und ob das Experiment beobachtet werden kann, um Ausnahmen abzufangen.

Wenn Sie Fehlerinjektionsexperimente durchführen, müssen alle verantwortlichen Beteiligten gut informiert sein. Teilen Sie den betroffenen Teams mit, wann die Experimente durchgeführt werden und was zu erwarten ist. Dies können Operations-Teams, die für die Servicezuverlässigkeit verantwortlichen Teams und der Kundensupport sein. Stellen Sie diesen Teams Kommunikationstools bereit, damit sie das Team, das das Experiment durchführt, über nachteilige Auswirkungen informieren können.

Sie müssen nach dem Experiment die Workload und die zugrunde liegenden Systeme wieder in den ursprünglichen, gut funktionierenden Zustand zurückversetzen. Häufig führt das resiliente Design der betreffenden Workload eine Selbstreparatur durch. Einige Fehlerdesigns oder fehlgeschlagenen Experimente können Ihre Workload jedoch in einem nicht erwarteten Fehlerzustand zurücklassen. Nach dem Ende des Experiments müssen Sie dies erkennen und die Workload und die Systeme wiederherstellen können. Mit können AWS FIS Sie innerhalb der Aktionsparameter eine Rollback-Konfiguration (auch Post-Aktion genannt) festlegen. Eine Post-Aktion führt das Ziel in den Zustand zurück, in dem es sich vor Ausführung der Aktion befunden hat. Diese Post-Aktionen sollten unabhängig davon, ob sie automatisiert (z. B. mithilfe AWS FIS) oder manuell ausgeführt werden, Teil eines Playbooks sein, in dem beschrieben wird, wie Fehler erkannt und behandelt werden können.

d. Prüfen Sie die Hypothese.

Unter [Grundlagen des Chaos-Engineering](#) wird die folgende Anleitung für die Verifizierung des Steady-State Ihrer Workload bereitgestellt:

Konzentrieren Sie sich auf die messbare Ausgabe des Systems und nicht auf seine internen Attribute. Messungen dieser Ausgabe über einen kurzen Zeitraum stellen einen Proxy für

den Steady-State des Systems dar. Der Gesamtdurchsatz, die Fehlerraten und die Latenz-Perzentile des Systems könnten Metriken sein, die das Steady-State-Verhalten beschreiben. Durch die Konzentration auf die Verhaltensmuster des Systems während Experimenten überprüft das Chaos-Engineering, ob das System funktioniert, statt zu versuchen, die Art der Funktion zu validieren.

In unseren beiden Beispielen oben verwenden wir die Steady-State-Metrik einer Erhöhung von weniger als 0,01 % bei serverseitigen Fehlern (5xx) und von weniger als einer Minute, in der Datenbankschreib- und Lesefehler auftreten.

Die 5xx-Fehler stellen eine gute Metrik dar, da sie die Folge des Fehlermodus sind, dem ein Client der Workload direkt unterliegen wird. Die Messung der Datenbankfehler ist als direkte Folge des Fehlers gut als Metrik geeignet, sollte jedoch durch eine Messung der Client-Auswirkungen ergänzt werden, beispielsweise in Form von fehlgeschlagenen Kundenanfragen oder Fehlern im Client. Fügen Sie außerdem einen synthetischen Monitor (auch als User Canary bezeichnet) auf einem beliebigen Workload APIs oder einem Client, auf den der Client URIs direkt zugreift, ein.

e. Verbessern Sie das Workload-Design hinsichtlich der Resilienz.

Wenn der Steady-State nicht bewahrt wurde, untersuchen Sie, wie das Workload-Design verbessert werden könnte, um den Fehler zu bewältigen. Wenden Sie dabei die bewährten Methoden der [AWS Well-Architected-Säule „Zuverlässigkeit“](#) an. Zusätzliche Anleitungen und Ressourcen finden Sie in der [AWS Builder's Library](#). Dort finden Sie unter anderem Artikel darüber, wie Sie Ihre [Zustandsprüfungen verbessern](#) oder [Wiederholungen mit Backoff in Ihrem Anwendungscode verwenden](#) können.

Führen Sie das Experiment nach der Implementierung dieser Änderungen erneut durch (angezeigt durch die gepunktete Linie im Flywheel für das Chaos-Engineering), um ihre Effektivität zu ermitteln. Wenn der Verifizierungsschritt zeigt, dass die Hypothese zutrifft, befindet sich die Workload im Steady-State und der Zyklus wird fortgesetzt.

4. Führen Sie regelmäßig Experimente durch.

Ein Chaos-Experiment ist ein Zyklus. Daher sollten Experimente regelmäßig als Teil des Chaos-Engineering durchgeführt werden. Wenn die Hypothese eines Experiments auf eine Workload zutrifft, sollte das Experiment automatisiert werden, um innerhalb Ihrer CI/CD-Pipeline kontinuierlich als Regression ausgeführt zu werden. Wie das geht, erfahren Sie in diesem Blog [zur Durchführung von AWS FIS Experimenten mit AWS CodePipeline](#). In diesem Lab

zu wiederkehrenden [AWS FIS -Experimenten in einer CI/CD-Pipeline](#) können Sie praktische Erfahrungen sammeln.

Fehlerinjektionsexperimente sind auch Bestandteil von Gamedays (siehe [REL12-BP06 Regelmäßig Spieltage durchführen](#)). Bei Gamedays wird ein Fehler oder Ereignis simuliert, um Systeme, Prozesse und die Reaktionen von Teams zu testen. Dabei sollen die auszuführenden Aktionen vom Team wie im Fall eines außergewöhnlichen Ereignisses tatsächlich ausgeführt werden.

#### 5. Erfassen und speichern Sie die Ergebnisse der Experimente.

Die Ergebnisse von Fehlerinjektionsexperimenten müssen erfasst und gespeichert werden. Erfassen Sie dabei alle notwendigen Daten (z. B. Zeit, Workload und Bedingungen), um die Ergebnisse und Trends von Experimenten später analysieren zu können. Beispiele für Ergebnisse können Screenshots von Dashboards, CSV Dumps aus der Datenbank Ihrer Metrik oder eine handgeschriebene Aufzeichnung von Ereignissen und Beobachtungen aus dem Experiment sein. Die [Protokollierung von Experimenten mit AWS FIS](#) kann Teil dieser Datenerfassung sein.

#### Ressourcen

Zugehörige bewährte Methoden:

- [REL08-BP03 Integrieren Sie Resilienztests als Teil Ihrer Bereitstellung](#)
- [REL13-BP03 Testen Sie die Disaster Recovery-Implementierung, um die Implementierung zu validieren](#)

Zugehörige Dokumente:

- [Was ist? AWS Fault Injection Service](#)
- [Was ist AWS Resilience Hub?](#)
- [Grundlagen des Chaos Engineering](#)
- [Chaos-Engineering: Planung Ihres ersten Experiments](#)
- [Resilience Engineering: Aus Fehlern lernen](#)
- [Chaos-Engineering-Geschichten](#)
- [Vermeiden von Fallback in verteilten Systemen](#)
- [Canary-Bereitstellung für Chaos-Experimente](#)

## Zugehörige Videos:

- [AWS re:Invent 2020: Resilienz mit Chaos Engineering testen \(\) ARC316](#)
- [AWS re:Invent 2019: Verbesserung der Widerstandsfähigkeit durch Chaos Engineering \(09-R1\) DOP3](#)
- [AWS re:Invent 2019: Chaos-Engineering in einer serverlosen Welt durchführen \(01\) CMY3](#)

## Zugehörige Beispiele:

- [Well-Architected Labor: Level 300: Testen der Widerstandsfähigkeit von AmazonEC2, Amazon und Amazon RDS S3](#)
- [Chaos-Engineering in AWS \(Lab\)](#)
- [Resiliente und Well-Architected-Apps mit Chaos-Engineering \(Lab\)](#)
- [Serverless-Chaos \(Lab\)](#)
- [Messen und verbessern Sie die Resilienz Ihrer Anwendungen mit Lab AWS Resilience Hub](#)

## Zugehörige Tools:

- [AWS Fault Injection Service](#)
- AWS Marketplace: [Gremlin Chaos Engineering Platform](#)
- [Chaos Toolkit](#)
- [Chaos Mesh](#)
- [Litmus](#)

## REL12-BP06 Regelmäßig Spieltage durchführen

Nutzen Sie Gamedays, um Ihre Verfahren für Reaktionen auf Ereignisse und Fehler unter möglichst produktionsnahen Bedingungen (einschließlich Produktionsumgebungen) regelmäßig mit den Personen zu testen, die auch bei tatsächlichen Fehlerszenarien beteiligt sind. Bei Gamedays werden Vorkehrungen getroffen, die sicherstellen, dass sich Produktionsereignisse nicht auf Benutzer auswirken.

Bei Gamedays wird ein Fehler oder Ereignis simuliert, um Systeme, Prozesse und die Reaktionen von Teams zu testen. Dabei sollen die auszuführenden Aktionen vom Team wie im Fall eines außergewöhnlichen Ereignisses tatsächlich ausgeführt werden. So können Sie nachvollziehen,



wo nachgebessert werden kann. Zudem üben Sie dabei ein, wie Ihre Organisation mit Ereignissen umgeht. Gamedays sollten regelmäßig ausgeführt werden, damit die Reaktion für Ihr Team zu einem Reflex wird.

Nachdem Sie Ihre Maßnahmen für Ausfallsicherheit implementiert und in Umgebungen abseits der Produktion getestet haben, können Sie an einem Gameday feststellen, ob in der Produktion alles wie geplant funktioniert. An einem Gameday, insbesondere am ersten, werden alle Entwickler und Betriebsteams miteinbezogen und über Zeitpunkt sowie Ablauf des Tests informiert. Runbooks sind vorhanden. Simulierte Ereignisse, einschließlich möglicher Ausfälle, werden in den Produktionssystemen in der vorgeschriebenen Weise ausgeführt, und die Auswirkungen werden bewertet. Wenn alle Systeme wie vorgesehen funktionieren, erfolgen Erkennung und Selbstreparatur mit minimalen oder gar keinen Auswirkungen. Wenn jedoch negative Auswirkungen festgestellt werden, wird der Test zurückgesetzt und die Workload-Probleme werden bei Bedarf manuell behoben (gemäß Runbook). Da Gamedays oft in der Produktion stattfinden, sollten alle Vorkehrungen getroffen werden, um Kunden vor Beeinträchtigungen der Verfügbarkeit zu schützen.

Typische Anti-Muster:

- Die eigenen Verfahren werden dokumentiert, jedoch nie trainiert.
- Entscheidungsträger werden bei den Tests außen vorgelassen.

Vorteile der Nutzung dieser bewährten Methode: Die regelmäßige Durchführung von Gamedays sorgt dafür, dass bei einem tatsächlichen Vorfall alle Mitarbeiter die Richtlinien und Verfahren befolgen. Außerdem wird überprüft, ob diese Richtlinien und Verfahren geeignet sind.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel

Implementierungsleitfaden

- Planen Sie Gamedays, um Ihre Runbooks und Playbooks regelmäßig zu trainieren. An Gamedays sollten alle Mitarbeiter beteiligt werden, die von Produktionsunterbrechungen betroffen sein können: Geschäftsinhaber, Entwickler, Produktionsmitarbeiter und die Teams, die auf Vorfälle reagieren.
  - Führen Sie Ihre Last- oder Leistungstests durch und simulieren Sie anschließend Fehler.
  - Prüfen Sie die Runbooks auf Anomalien und suchen Sie nach Möglichkeiten zur Ausführung der Playbooks.

- Wenn Sie von den Runbooks abweichen, optimieren Sie diese oder ändern Sie Ihre Vorgehensweise. Ermitteln Sie bei Ausführung eines Playbooks das Runbook, das hätte verwendet werden sollen, oder erstellen Sie ein neues.

## Ressourcen

### Zugehörige Videos:

- [AWS re:Invent 2019: Verbesserung der Widerstandsfähigkeit durch Chaos Engineering \(09-R1\) DOP3](#)

### Zugehörige Beispiele:

- [AWS Well-Architected Labs – Testen der Ausfallsicherheit](#)

## REL13. Was ist bei der Planung der Notfallwiederherstellung zu beachten?

Sicherungen und redundante Workload-Komponenten sind der Ausgangspunkt Ihrer Strategie für die Notfallwiederherstellung. [RTO und RPO sind Ihre Ziele](#) für die Wiederherstellung Ihrer Arbeitslast. Legen Sie diese entsprechend den geschäftlichen Anforderungen fest. Implementieren Sie eine Strategie, um diese Ziele zu erreichen. Berücksichtigen Sie dabei Standorte und Funktionen von Workload-Ressourcen und -Daten. Die Wahrscheinlichkeit von Unterbrechungen und die Kosten von Wiederherstellungen sind ebenfalls wichtige Faktoren bei der Ermittlung des Unternehmenswerts, den Notfallwiederherstellungen von Workloads bieten.

## Bewährte Methoden

- [REL13-BP01 Definieren Sie Wiederherstellungsziele für Ausfallzeiten und Datenverlust](#)
- [REL13-BP02 Verwenden Sie definierte Wiederherstellungsstrategien, um die Wiederherstellungsziele zu erreichen](#)
- [REL13-BP03 Testen Sie die Disaster Recovery-Implementierung, um die Implementierung zu validieren](#)
- [REL13-BP04 Konfigurationsabweichungen am DR-Standort oder in der Region verwalten](#)
- [REL13-BP05 Automatisieren Sie die Wiederherstellung](#)

## REL13-BP01 Definieren Sie Wiederherstellungsziele für Ausfallzeiten und Datenverlust

Für die Arbeitslast gibt es ein Ziel für die Wiederherstellungszeit (RTO) und ein Ziel für einen Erholungspunkt (RPO).

Das Wiederherstellungszeitziel (RTO) ist die maximal zulässige Verzögerung zwischen der Betriebsunterbrechung und der Wiederherstellung des Dienstes. Damit wird festgelegt, was als akzeptables Zeitfenster gilt, wenn der Service nicht verfügbar ist.

Recovery Point Objective (RPO) ist die maximal zulässige Zeitspanne seit dem letzten Datenwiederherstellungspunkt. Damit wird festgelegt, was als akzeptabler Datenverlust zwischen dem letzten Wiederherstellungspunkt und der Serviceunterbrechung gilt.

RTO und RPO Werte sind wichtige Überlegungen bei der Auswahl einer geeigneten Disaster Recovery (DR) -Strategie für Ihren Workload. Diese Ziele werden vom Unternehmen festgelegt und dann von den technischen Teams verwendet, um eine DR-Strategie auszuwählen und umzusetzen.

Gewünschtes Ergebnis:

Jedem Workload wird ein zugewiesener Workload zugewiesen RTO und RPO auf der Grundlage seiner Auswirkungen auf das Unternehmen definiert. Der Workload wird einer vordefinierten Stufe zugewiesen, die die Serviceverfügbarkeit und den akzeptablen Datenverlust definiert, mit einem zugehörigen RTO und RPO. Falls eine solche Staffelung nicht möglich ist, kann eine individuelle Zuweisung pro Workload durchgeführt werden – mit der Absicht, Stufen zu einem späteren Zeitpunkt zu erstellen. RTO und RPO werden als eine der wichtigsten Überlegungen bei der Auswahl einer Implementierung einer Disaster-Recovery-Strategie für den Workload verwendet. Zusätzliche Überlegungen bei der Auswahl einer solchen Strategie sind Kostenbeschränkungen, Workload-Abhängigkeiten und betriebliche Anforderungen.

Machen Sie sich anhand der Dauer eines Ausfalls ein Bild von den Auswirkungen. Sind sie linear oder gibt es nichtlineare Auswirkungen? (Beispiel: Nach vier Stunden schalten Sie eine Fertigungslinie bis zum Beginn der nächsten Schicht ab).

Eine Matrix der Notfallwiederherstellung wie die folgende kann Ihnen helfen zu verstehen, wie die Kritikalität der Workload mit den Wiederherstellungszielen zusammenhängt. (Beachten Sie, dass die tatsächlichen Werte für die X- und Y-Achsen an die Bedürfnisse Ihres Unternehmens angepasst werden sollten).

Matrix der Notfallwiederherstellung						
		Wiederherstellungszeitpunkt				
		< 1 Minute	< 1 Stunde	< 6 Stunden	< 1 Tag	+ 1 Tag
Wiederherstellungsdauer	< 10 Minuten	Kritisch	Kritisch	Hoch	Mittel	Mittel
	< 2 Stunden	Kritisch	Hoch	Mittel	Mittel	Niedrig
	< 8 Stunden	Hoch	Mittel	Mittel	Niedrig	Niedrig
	< 24 Stunden	Mittel	Mittel	Niedrig	Niedrig	Niedrig
	24 + Stunden	Mittel	Niedrig	Niedrig	Niedrig	Niedrig

Abbildung 16: Matrix der Notfallwiederherstellung

## Typische Anti-Muster:

- Keine definierten Wiederherstellungsziele.
- Auswählen beliebiger Wiederherstellungsziele.
- Auswählen von Wiederherstellungszielen, die nicht strikt genug sind und die Geschäftsziele nicht erfüllen.
- Mangelndes Verständnis für die Auswirkungen von Ausfallzeiten und Datenverlusten.
- Auswahl unrealistischer Wiederherstellungsziele (z. B. unverzügliche Wiederherstellung und kein Datenverlust), die für Ihre Workload-Konfiguration möglicherweise nicht erreichbar sind.
- Auswählen von Wiederherstellungszielen, die strikter sind als die tatsächlichen Geschäftsziele. Dies erzwingt Implementierungen für die Notfallwiederherstellung, die kostspieliger und komplizierter sind als die Anforderungen der Workload.
- Auswahl von Wiederherstellungszielen, die nicht mit denen einer abhängigen Workload vereinbar sind.
- Ihre Wiederherstellungsziele berücksichtigen nicht die Einhaltung gesetzlicher Vorschriften.
- RTO und für einen Workload RPO definiert, aber nie getestet.

Vorteile der Nutzung dieser bewährten Methode: Die Wiederherstellungsziele für Dauer und Datenverlust sind als Orientierungshilfe für die Implementierung der Notfallwiederherstellung erforderlich.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Hoch

## Implementierungsleitfaden

Sie müssen für die jeweilige Workload die Auswirkungen von Ausfallzeiten und Datenverlusten auf Ihr Unternehmen verstehen. Die Auswirkungen werden im Allgemeinen umso größer, je länger die Ausfallzeiten bzw. je größer der Datenverlust ist, aber die Form dieser Zunahme kann je nach Art der Workload unterschiedlich sein. Beispielsweise kann es sein, dass Sie Ausfallzeiten von bis zu einer Stunde mit geringen Auswirkungen tolerieren können, die Auswirkungen aber danach schnell zunehmen. Die Auswirkungen auf das Unternehmen zeigen sich auf vielerlei Art, etwa in Form von Kosten (z. B. Umsatzeinbußen), Kundenvertrauen (und Auswirkungen auf den Ruf), betrieblichen Problemen (z. B. verspätete Auszahlung von Gehältern oder verringerte Produktivität) und regulatorischen Risiken. Gehen Sie wie folgt vor, um sich mit diesen Auswirkungen vertraut zu machen und sie RPO für Ihren Workload festzulegen RTO.

### Implementierungsschritte

1. Ermitteln Sie die Stakeholder für diese Workload in Ihrem Unternehmen und setzen Sie sich mit ihnen in Verbindung, um diese Schritte umzusetzen. Die Wiederherstellungsziele für eine Workload sind eine Geschäftsentscheidung. Technische Teams arbeiten dann mit Stakeholdern im Unternehmen zusammen, um anhand dieser Ziele eine DR-Strategie auszuwählen.

#### Note

Für die Schritte 2 und 3 können Sie das [the section called "Arbeitsblatt zur Implementierung"](#) verwenden.

2. Sammeln Sie die erforderlichen Informationen, um eine Entscheidung zu treffen, indem Sie die folgenden Fragen beantworten.
3. Gibt es Kategorien oder Stufen der Kritikalität für die Workload-Auswirkungen in Ihrem Unternehmen?
  - a. Falls ja, weisen Sie diese Workload einer Kategorie zu.
  - b. Falls nein, legen Sie diese Kategorien fest. Erstellen Sie bis zu fünf Kategorien und verfeinern Sie den Bereich Ihres RTO für jede Kategorie. Zu den Beispielskategorien gehören „Kritisch“, „Hoch“, „Mittel“ und „Niedrig“. Um zu verstehen, wie Workloads Kategorien zugeordnet werden, sollten Sie sich überlegen, ob die Workload geschäftskritisch, wichtig für das Unternehmen oder für den Geschäftserfolg nicht maßgeblich ist.
  - c. Legen Sie die Arbeitslast fest RTO und RPO basieren Sie auf der Kategorie. Wählen Sie immer eine Kategorie, die strenger ist (niedriger RTO und RPO) als die in diesem Schritt berechneten

Rohwerte. Wenn sich der Wert dadurch zu stark ändert, sollten Sie erwägen, eine neue Kategorie zu erstellen.

4. Ordnen Sie RTO der Arbeitslast auf der Grundlage dieser Antworten RPO Werte zu. Dies kann direkt oder durch Zuweisen der Workload zu einer vordefinierten Serviceebene erfolgen.
5. Dokumentieren Sie den Notfallwiederherstellungsplan (DRP) für diesen Workload, der Teil des [Business Continuity Plans \(BCP\)](#) Ihres Unternehmens ist, an einem Ort, der für das Workload-Team und die Beteiligten zugänglich ist
  - a. Notieren Sie die RTO Werte und die Informationen RPO, die zur Bestimmung dieser Werte verwendet wurden. Beziehen Sie auch die Strategie ein, die zur Bewertung der Auswirkungen der Workload auf das Unternehmen verwendet wurde
  - b. Notieren Sie auch andere RPO Messwerte RTO und verfolgen Sie die Ziele der Notfallwiederherstellung oder planen Sie, diese nachzuverfolgen
  - c. Fügen Sie diesem Plan bei der Erstellung Einzelheiten zu Ihrer DR-Strategie und Ihrem Runbook hinzu.
6. Wenn Sie die Kritikalität der Workload in einer Matrix wie der in Abbildung 15 nachschlagen, können Sie damit beginnen, vordefinierte Serviceebenen festzulegen, die für Ihr Unternehmen definiert sind.
7. Nachdem Sie eine DR-Strategie (oder einen Machbarkeitsnachweis für eine DR-Strategie) gemäß den Vorgaben implementiert haben [the section called “REL13-BP02 Verwenden Sie definierte Wiederherstellungsstrategien, um die Wiederherstellungsziele zu erreichen”](#), testen Sie diese Strategie, um die tatsächliche Arbeitslast RTC (Recovery Time Capability) und RPC (Recovery Point Capability) zu ermitteln. Wenn diese nicht die angestrebten Wiederherstellungsziele erfüllen, passen Sie diese Ziele entweder gemeinsam mit Stakeholdern in Ihrem Unternehmen an oder nehmen Sie Änderungen an der DR-Strategie vornehmen, um die Zielvorgaben zu erreichen.

## Primäre Fragen

1. Wie lange kann die Workload maximal ausfallen, bevor dies schwerwiegende Auswirkungen auf das Unternehmen hat?
  - a. Ermitteln Sie die Kosten (direkte finanzielle Auswirkungen) für das Unternehmen pro Minute, in der die Workload unterbrochen ist.
  - b. Bedenken Sie, dass die Auswirkungen nicht immer linear sind. Die Auswirkungen können zunächst begrenzt sein und dann nach einem kritischen Zeitpunkt rasch zunehmen.

2. Wie viele Daten können maximal verlorengehen, bevor dies schwerwiegende Auswirkungen auf das Unternehmen hat?
  - a. Ziehen Sie diesen Wert für Ihren wichtigsten Datenspeicher in Betracht. Identifizieren Sie die jeweilige Kritikalität für andere Datenspeicher.
  - b. Können Workload-Daten wiederhergestellt werden, wenn sie verloren gehen? Wenn dies betrieblich einfacher ist als Sicherung und Wiederherstellung, sollten Sie die Wahl auf der RPO Grundlage der Wichtigkeit der Quelldaten treffen, die für die Neuerstellung der Workload-Daten verwendet wurden.
3. Was sind die Wiederherstellungsziele und Verfügbarkeitserwartungen für Workloads, von denen diese Workload abhängt (Downstream), bzw. für Workloads, die von dieser Workload abhängen (Upstream)?
  - a. Wählen Sie Wiederherstellungsziele, die es ermöglichen, dass diese Workload die Anforderungen der Upstream-Abhängigkeiten erfüllt.
  - b. Wählen Sie Wiederherstellungsziele, die angesichts der Wiederherstellungsfunktionen von Downstream-Abhängigkeiten erreichbar sind. Nichtkritische Downstream-Abhängigkeiten (solche, die Sie umgehen können) können ausgeschlossen werden. Oder arbeiten Sie mit kritischen Downstream-Abhängigkeiten zusammen, um ihre Wiederherstellungsfunktionen bei Bedarf zu verbessern.

### Zusätzliche Fragen

Denken Sie über diese Fragen nach und überlegen Sie, wie sie sich auf diese Workload auswirken können:

4. Haben Sie unterschiedliche RTO Ausfälle, die von der Art des Ausfalls RPO abhängen (Region oder AZ usw.)?
5. Gibt es einen bestimmten Zeitpunkt (Saisonalität, Verkaufsveranstaltungen, Produkteinführungen), zu dem sich Ihr RTO/ändern RPO kann? Falls ja, was sind die unterschiedlichen Mess- und zeitlichen Beschränkungen?
6. Wie viele Kunden sind betroffen, wenn die Workload unterbrochen wird?
7. Wie wirkt sich eine Unterbrechung der Workload auf den Ruf aus?
8. Welche anderen betrieblichen Auswirkungen können auftreten, wenn die Workload unterbrochen wird? Zum Beispiel Auswirkungen auf die Produktivität der Mitarbeiter, wenn E-Mail-Systeme nicht verfügbar sind oder wenn die Gehaltsabrechnungssysteme keine Transaktionen einreichen können.

9. Wie stehen Arbeitsaufwand RTO und RPO Ausrichtung auf die DR-Strategie des Geschäftsbereichs und der Organisation?

10. Gibt es interne vertragliche Verpflichtungen zur Erbringung eines Services? Gibt es Strafen für die Nichteinhaltung?

11. Welche regulatorischen oder behördlichen Auflagen gelten im Zusammenhang mit den Daten?

### Arbeitsblatt zur Implementierung

Sie können dieses Arbeitsblatt für die Implementierungsschritte 2 und 3 verwenden. Sie können dieses Arbeitsblatt an Ihre spezifischen Bedürfnisse anpassen, indem Sie beispielsweise zusätzliche Fragen hinzufügen.

Schritt 2: primäre Fragen	Gilt für Workload?	Workload-RTO	Workload-RPO	RTO anpassen	RPO anpassen	Anleitungen
[1] Maximale Zeit, in der der Workload ausfallen kann						Gemessen Zeit seit Beginn des Ausfalls bis zur Wiederherstellung
[2] Maximale Datenmenge, die verloren gehen kann						Gemessen in Zeit seit dem letzten bekannten gut wiederherstellbaren Datensatz
[3a] Vorgelagerte Abhängigkeiten						Strengste nachgelagerte Wiederherstellungsziele eingeben
[3b] Nachgelagerte Abhängigkeiten						Am wenigsten strenge nachgelagerte Wiederherstellungsziele eingeben
[3a] Abgegliche vorgelagerte Abhängigkeiten						Wenn der vorgelagerte Wert niedriger ist als aktuelle Werte und der nachgelagerte Wert größer ist,
[3b] Abgegliche nachgelagerte Abhängigkeiten						arbeiten Sie mit Abhängigkeiten, um auszugleichen und hier ausgeglichene Werte einzugeben.
[3] Abhängigkeiten						Werte senken, um vorgelagerte Abhängigkeiten zu erfüllen oder die basierend auf nachgelagerten Abhängigkeitsfähigkeiten zu erhöhen
<b>Schritt 2: zusätzliche Fragen</b>						Geben Sie an, ob die Frage zutrifft. Falls nicht, überspringen Sie sie.
Basis-RTO-/RPO						Übertragen Sie die RTO- und RPO-Werte von oben nach hier unten.
[4] Art des Ausfalls	[ ]/[ ]/[ ] N					Geben Sie Wiederherstellungsziele für Ereignisarten mit strengsten Anforderungen ein.
[5] Spezifische zeitbasierte Ziele	[ ]/[ ]/[ ] N					Geben Sie Wiederherstellungsziele für Zeiten mit strengsten Anforderungen ein.
[6] Unterbrechungen bei Kunden	[ ]/[ ]/[ ] N					Grafische Darstellung der betroffenen Kunden in Abhängigkeit von der Ausfallzeit oder dem Datenverlust. Verwenden Sie dies, um das maximal zulässige RTO und RPO auf der Grundlage der Kundenauswirkungen einzugeben.
[7] Auswirkungen auf den Ruf	[ ]/[ ]/[ ] N					Mit dem Unternehmen arbeiten, um die maximale RTO und den maximalen RPO basierend auf der Auswirkung auf die Reputation zu bestimmen
[8] Betriebliche Auswirkungen	[ ]/[ ]/[ ] N					Geben Sie das maximale RTO und RPO auf der Grundlage der betrieblichen Auswirkungen ein.
[9] Organisatorische Ausrichtung	[ ]/[ ]/[ ] N					Geben Sie das maximale RTO und RPO für Workloads dieses Typs gemäß den LOB- und Organisationsanforderungen ein.
[10] Vertragliche Verpflichtungen	[ ]/[ ]/[ ] N					Geben Sie das maximale RTO und RPO auf der Grundlage der vertraglichen Verpflichtungen ein.
[11] Gesetzliche Vorschriften	[ ]/[ ]/[ ] N					Geben Sie das maximale RTO und RPO auf der Grundlage der geltenden gesetzlichen Bestimmungen ein.
Ziel basierend auf zusätzlichen Fragen						Nehmen Sie den Mindestwert (strengerer Wert) aus den Fragen 4–11 und geben Sie ihn hier ein.
Angepasstes Ziel						Wenn die Ziele in der obigen Zeile nicht erreicht werden können, arbeiten Sie mit den Beteiligten zusammen, um die Beschränkungen zu lockern, und geben Sie hier ein neues Minimum ein.
RTO/RPO angepasst						Geben Sie die Basis-RPO-/RTO-Werte oder das angepasste Ziel ein, je nachdem, welcher Wert niedriger ist.
<b>Schritt 3</b>						
Zuordnung zu vordefinierter Kategorie oder Stufe						Senken Sie beide Werte (machen Sie sie strenger), um sie an die nächstgelegene definierte Stufe anzupassen.

### Arbeitsblatt

Aufwand für den Implementierungsplan: Niedrig

Ressourcen

Zugehörige bewährte Methoden:



- [the section called “REL09-BP04 Führen Sie eine regelmäßige Wiederherstellung der Daten durch, um die Integrität und die Backup-Prozesse zu überprüfen”](#)
- [the section called “REL13-BP02 Verwenden Sie definierte Wiederherstellungsstrategien, um die Wiederherstellungsziele zu erreichen”](#)
- [the section called “REL13-BP03 Testen Sie die Implementierung der Notfallwiederherstellung, um die Implementierung zu validieren”](#)

#### Zugehörige Dokumente:

- [AWS Architecture Blog: Notfallwiederherstellung](#)
- [Disaster Recovery von Workloads auf AWS: Wiederherstellung in der Cloud \(AWS Whitepaper\)](#)
- [Verwaltung von Resilienzrichtlinien mit Resilience Hub AWS](#)
- [APNPartner: Partner, die bei der Notfallwiederherstellung helfen können](#)
- [AWS Marketplace: Für die Notfallwiederherstellung geeignete Produkte](#)

#### Zugehörige Videos:

- [AWS re:Invent 2018: Architekturmuster für aktive/aktive Anwendungen in mehreren Regionen \(09-R2\) ARC2](#)
- [Notfallwiederherstellung von Workloads auf AWS](#)

REL13-BP02 Verwenden Sie definierte Wiederherstellungsstrategien, um die Wiederherstellungsziele zu erreichen

Definieren Sie eine Notfallwiederherstellungsstrategie (Disaster Recovery, DR), die den Wiederherstellungszielen Ihrer Workloads entspricht. Wählen Sie eine Strategie aus, z. B. Backup und Wiederherstellung, Standby (aktiv/passiv) oder Aktiv/Aktiv.

Gewünschtes Ergebnis: Für jede Workload gibt es eine definierte und implementierte DR-Strategie, mit der die Workload die DR-Ziele erreichen kann. DR-Strategien zwischen Workloads nutzen wiederverwendbare Muster (wie die zuvor beschriebenen Strategien),

#### Typische Anti-Muster:

- Implementierung von inkonsistenten Wiederherstellungsprozeduren für Workloads mit ähnlichen DR-Zielen.

- Die DR-Strategie muss im Notfall Ad-hoc umgesetzt werden.
- Es gibt keinen Plan für die Notfallwiederherstellung.
- Abhängigkeit von Vorgängen auf der Steuerebene während der Wiederherstellung.

Vorteile der Nutzung dieser bewährten Methode:

- Durch die Nutzung definierter Wiederherstellungsstrategien können Sie verbreitet verwendete Tools und Testverfahren verwenden.
- Die Verwendung definierter Wiederherstellungsstrategien verbessert den Wissensaustausch zwischen den Teams und die Implementierung der Notfallwiederherstellung für ihre Workloads.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Hoch. Ohne eine geplante, implementierte und getestete DR-Strategie ist es unwahrscheinlich, dass Sie Ihre Wiederherstellungsziele im Falle eines Notfalls erreichen.

### Implementierungsleitfaden

Eine DR-Strategie beruht auf der Fähigkeit, Ihre Workload an einem Wiederherstellungsstandort bereitzustellen, wenn Ihr primärer Standort nicht mehr in der Lage ist, die Workload auszuführen. Die gängigsten Wiederherstellungsziele sind RTO und RPO, wie unter beschrieben. [REL13-BP01 Definieren Sie Wiederherstellungsziele für Ausfallzeiten und Datenverlust](#)

Mit einer DR-Strategie, die sich über mehrere Availability Zones (AZs) innerhalb einer einzigen Zone erstreckt AWS-Region, können Katastrophenereignisse wie Brände, Überschwemmungen und größere Stromausfälle vermieden werden. Wenn es erforderlich ist, Schutz vor einem unwahrscheinlichen Ereignis zu implementieren, das verhindert, dass Ihr Workload in einer bestimmten Umgebung ausgeführt werden kann AWS-Region, können Sie eine DR-Strategie verwenden, die mehrere Regionen verwendet.

Wenn Sie eine DR-Strategie für mehrere Regionen entwickeln, sollten Sie eine der folgenden Strategien wählen. Sie sind in aufsteigender Reihenfolge der Kosten und Komplexität und in absteigender Reihenfolge aufgeführt RPO. RTO Die Wiederherstellungsregion bezieht sich auf eine AWS-Region andere als die primäre Region, die für Ihren Workload verwendet wird.

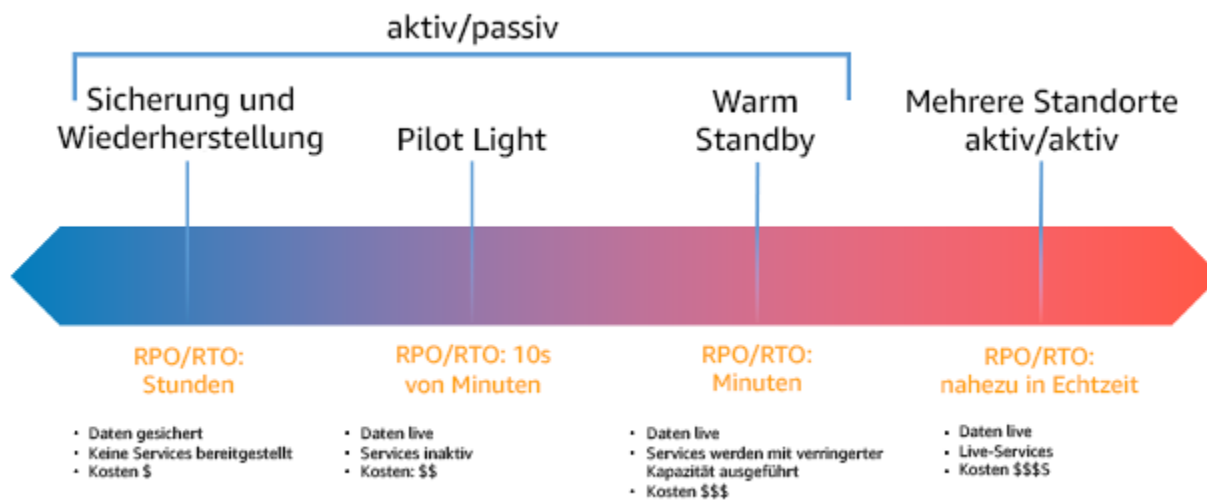


Abbildung 17: Strategien für die Notfallwiederherstellung (Disaster Recovery, DR)

- Backup und Wiederherstellung (RPO in Stunden, RTO innerhalb von 24 Stunden oder weniger): Sichern Sie Ihre Daten und Anwendungen in der Wiederherstellungsregion. Die Verwendung automatisierter oder kontinuierlicher Backups ermöglicht eine Point-in-Time-Wiederherstellung (PITR), die in einigen Fällen RPO auf bis zu 5 Minuten reduziert werden kann. Im Katastrophenfall stellen Sie Ihre Infrastruktur bereit (indem Sie Infrastruktur als Code zur Reduzierung verwenden RTO), Ihren Code bereitstellen und die gesicherten Daten wiederherstellen, um sie nach einem Notfall in der Wiederherstellungsregion wiederherzustellen.
- Pilotprojekt (RPO in Minuten, RTO in Dutzenden von Minuten): Stellen Sie eine Kopie Ihrer wichtigsten Workload-Infrastruktur in der Wiederherstellungsregion bereit. Replizieren Sie Ihre Daten in die Wiederherstellungsregion und erstellen Sie dort Sicherungskopien der Daten. Ressourcen, die zur Unterstützung der Datenreplikation und -sicherung erforderlich sind, wie Datenbanken und Objektspeicher, sind immer eingeschaltet. Andere Elemente wie Anwendungsserver oder Serverless-Datenverarbeitung werden nicht bereitgestellt, sondern können bei Bedarf mit der erforderlichen Konfiguration und dem Anwendungscode erstellt werden.
- Warm-Standby (RPO in Sekunden, RTO in Minuten): Behalten Sie eine verkleinerte, aber voll funktionsfähige Version Ihres Workloads bei, die immer in der Wiederherstellungsregion ausgeführt wird. Geschäftskritische Systeme sind vollständig dupliziert und ständig aktiv, aber mit herunterskalierter Flotte. Die Daten werden repliziert und sind in der Wiederherstellungsregion live. Wenn eine Wiederherstellung erforderlich ist, wird das System zur Bewältigung der Produktionslast schnell hochskaliert. Je höher der Warm-Standby-Modus ist, desto geringer RTO

ist die Abhängigkeit von der Steuerungsebene. Bei vollständiger Skalierung wird dies als Hot Standby bezeichnet.

- Regionsübergreifend (mehrere Standorte) aktiv-aktiv (RPO nahe Null, RTO potenziell Null): Ihr Workload wird auf mehrere verteilt und bedient aktiv Traffic von mehreren. AWS-Regionen Bei dieser Strategie müssen Sie die Daten zwischen den Regionen synchronisieren. Mögliche Konflikte, die durch Schreibvorgänge auf denselben Datensatz in zwei verschiedenen regionalen Repliken verursacht werden, müssen vermieden oder behandelt werden, was sehr komplex sein kann. Die Datenreplikation ist für die Datensynchronisierung nützlich und schützt Sie vor einigen Arten von Notfällen. Sie schützt Sie jedoch nicht vor Datenbeschädigung oder -zerstörung, sofern Ihre Lösung nicht auch Wiederherstellungsoptionen umfasst. point-in-time

#### Note

Der Unterschied zwischen Pilot Light und Warm Standby kann schwer zu überblicken sein. Beide beinhalten eine Umgebung in Ihrer Wiederherstellungsregion mit Kopien der Assets Ihrer Primärregion. Der Unterschied besteht darin, dass Pilot Light keine Anfragen bearbeiten kann, ohne dass zuvor zusätzliche Maßnahmen ergriffen werden, während Warm Standby den Datenverkehr (mit reduzierter Kapazität) sofort bearbeiten kann. Bei Pilot Light müssen Sie die Server einschalten, möglicherweise zusätzliche (nicht zum Kerngeschäft gehörende) Infrastruktur bereitstellen und die Leistung hochskalieren, während Sie bei Warm-Standby nur die Leistung hochskalieren müssen (alles ist bereits bereitgestellt und läuft). Wählen Sie je nach Ihren RPO Bedürfnissen RTO zwischen diesen Optionen.

Wenn es um Kosten geht und Sie ähnliche RPO RTO Ziele erreichen möchten, wie sie in der Warm-Standby-Strategie definiert sind, können Sie Cloud-native Lösungen in Betracht ziehen AWS Elastic Disaster Recovery, z. B. solche, die den Pilotansatz verfolgen RPO und verbesserte RTO Ziele bieten.

## Implementierungsschritte

1. Bestimmen Sie eine DR-Strategie, die die Wiederherstellungsanforderungen für diese Workload erfüllt.

Die Wahl einer DR-Strategie ist ein Kompromiss zwischen der Reduzierung von Ausfallzeiten und Datenverlusten (RTO und RPO) und den Kosten und der Komplexität der Umsetzung der Strategie. Sie sollten vermeiden, eine Strategie zu verfolgen, die strikter ist als nötig, da dies unnötige Kosten verursacht.

In der folgenden Abbildung hat das Unternehmen beispielsweise die zulässige Höchstmenge RTO sowie die Obergrenze für die Ausgaben für die Servicewiederherstellungsstrategie festgelegt. Angesichts der Unternehmensziele erfüllen die DR-Strategien Pilot Light oder Warm-Standby RTO sowohl die Kriterien als auch die Kostenkriterien.

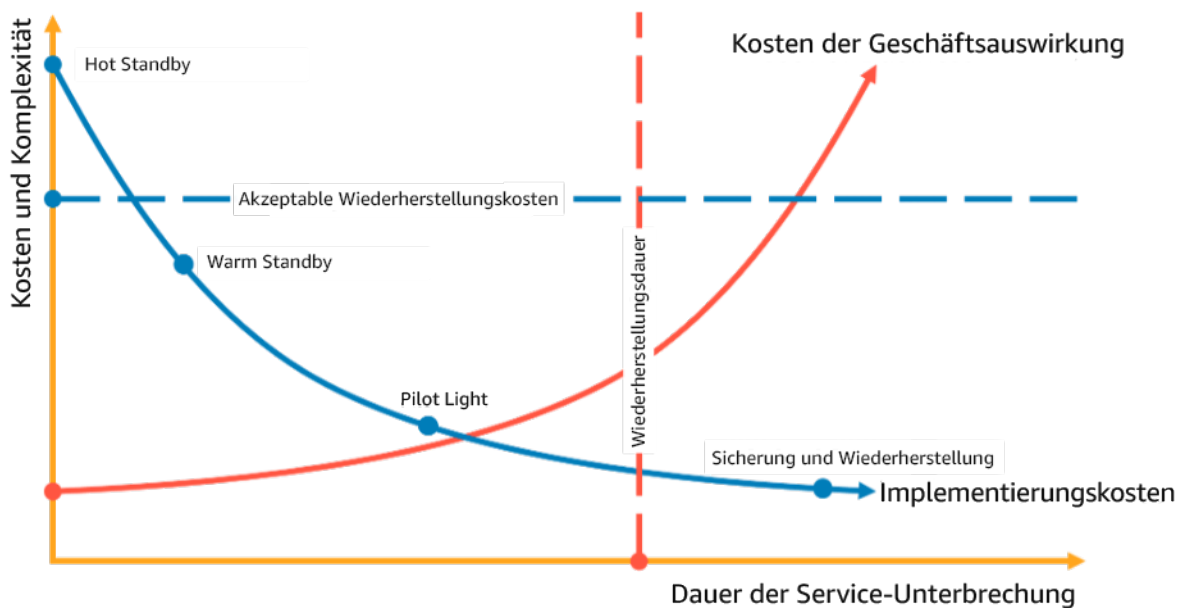


Abbildung 18: Auswahl einer DR-Strategie auf der RTO Grundlage von Kosten

Weitere Informationen finden Sie unter [Business Continuity Plan \(BCP\)](#).

## 2. Sehen Sie sich anhand der Muster an, wie die gewählte DR-Strategie umgesetzt werden kann.

In diesem Schritt geht es darum, zu verstehen, wie Sie die gewählte Strategie umsetzen wollen. Die Strategien werden anhand des primären AWS-Regionen Standorts und des Wiederherstellungsstandorts erläutert. Sie können jedoch auch Availability Zones innerhalb einer einzigen Region als DR-Strategie verwenden, die Elemente mehrerer dieser Strategien nutzt.

In den folgenden Schritten können Sie die Strategie auf Ihre spezifische Workload anwenden.

### Backup und Wiederherstellung

Backup und Wiederherstellung sind die am wenigsten komplexe Strategie, die implementiert werden muss, erfordert jedoch mehr Zeit und Mühe, um die Arbeitslast wiederherzustellen, was zu höheren RTO und führt RPO. Es empfiehlt sich, immer Backups Ihrer Daten zu erstellen und diese auf eine andere Site (z. B. eine andere AWS-Region) zu kopieren.

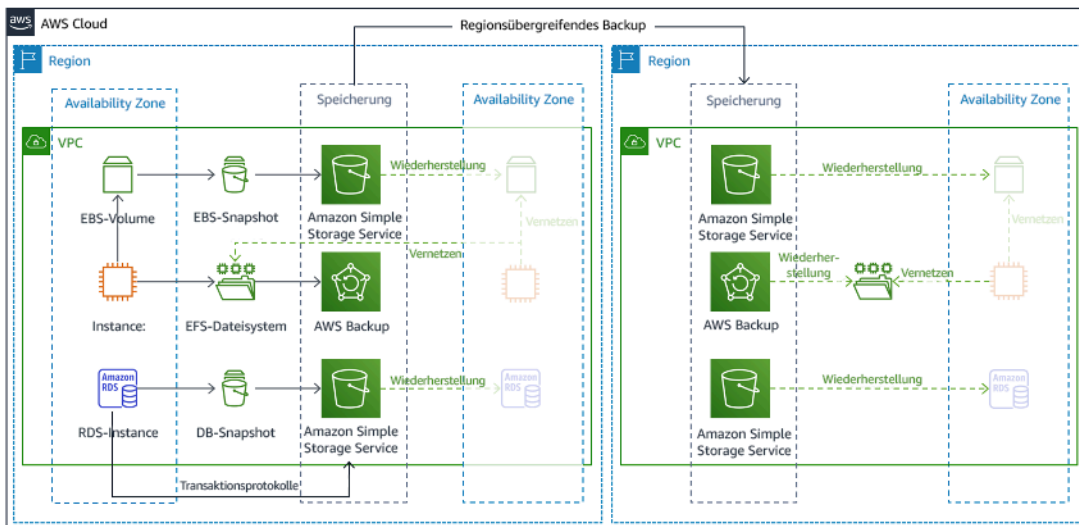


Abbildung 19: Backup- und Wiederherstellungsarchitektur

Weitere Informationen zu dieser Strategie finden Sie unter [Disaster Recovery \(DR\) -Architektur unter AWS, Teil II: Backup und Wiederherstellung mit Rapid Recovery](#).

### Pilot light

Beim Pilot-Light-Ansatz replizieren Sie die Daten von Ihrer primären Region in Ihre Wiederherstellungsregion. Die Kernressourcen, die für die Workload-Infrastruktur verwendet werden, werden in der Wiederherstellungsregion bereitgestellt, jedoch werden noch zusätzliche Ressourcen und Abhängigkeiten benötigt, um diesen Stack funktionsfähig zu machen. In Abbildung 20 werden zum Beispiel keine Datenverarbeitungs-Instances bereitgestellt.

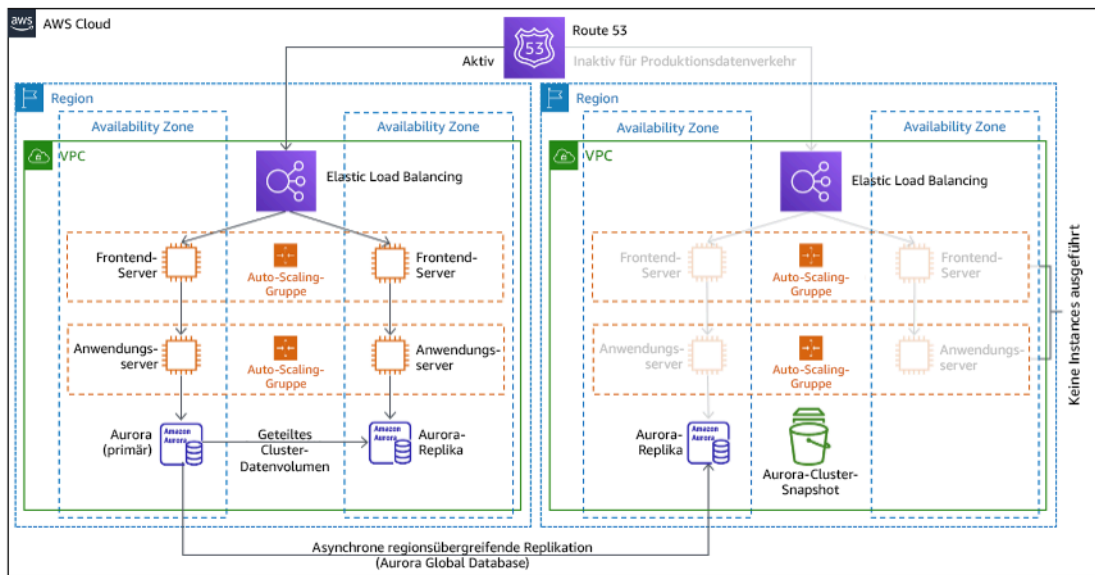


Abbildung 20: Pilot-Light-Architektur

Weitere Informationen zu dieser Strategie finden Sie unter [Disaster Recovery \(DR\) -Architektur unter AWS, TeilIII: Pilot Light und Warm Standby](#).

### Warmer Bereitschaftsmodus

Beim Warm-Standby-Ansatz wird sichergestellt, dass eine herunterskalierte, aber voll funktionsfähige Kopie Ihrer Produktionsumgebung in einer anderen Region vorhanden ist. Dieser Ansatz erweitert das Konzept des Pilot Light und verkürzt die Zeit bis zur Wiederherstellung, da die Workload in einer anderen Region ständig präsent ist. Wenn die Wiederherstellungsregion mit voller Kapazität bereitgestellt wird, wird dies als Hot Standby bezeichnet.

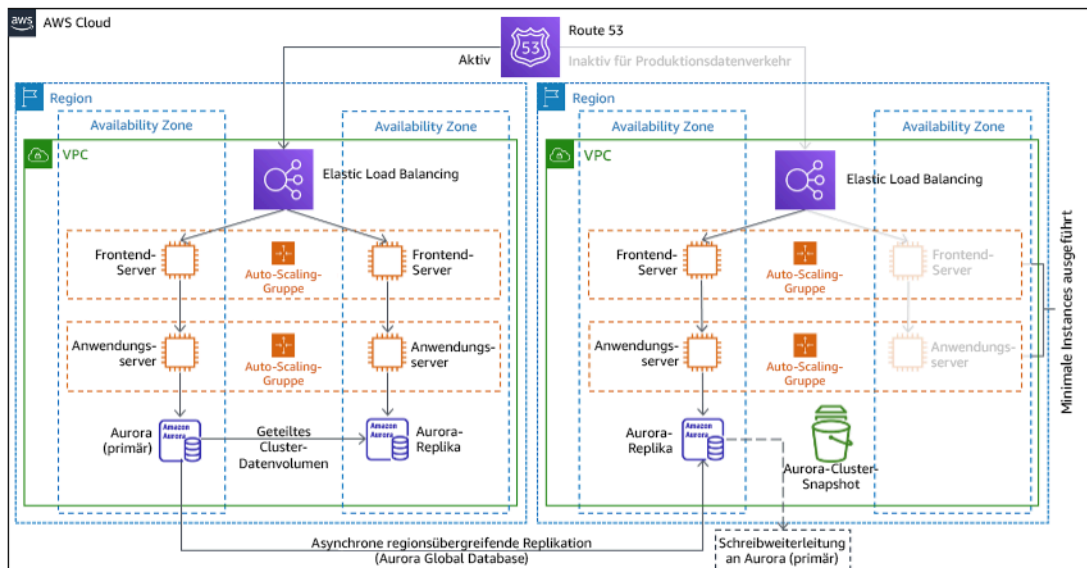


Abbildung 21: Warm-Standby-Architektur

Der Einsatz von Warm Standby oder Pilot Light erfordert ein Hochskalieren der Ressourcen in der Wiederherstellungsregion. Um sicherzustellen, dass Kapazität bei Bedarf verfügbar ist, sollten Sie die Nutzung von [Kapazitätsreservierungen](#) für EC2 Instances in Betracht ziehen. Bei Verwendung AWS Lambda der [bereitgestellten Parallelität](#) können Laufzeitumgebungen bereitgestellt werden, sodass diese bereit sind, sofort auf die Aufrufe Ihrer Funktion zu reagieren.

Weitere Informationen zu dieser Strategie finden Sie unter [Disaster Recovery \(DR\) -Architektur unter AWS, Teil III: Pilot Light](#) und Warm Standby.

### Multi-Site Aktiv/Aktiv

Im Rahmen einer Multi-Site Aktiv/Aktiv-Strategie können Sie Ihre Workload in mehreren Regionen gleichzeitig ausführen. Multi-Site Aktiv/Aktiv bedient den Datenverkehr aus allen Regionen, in denen es eingesetzt wird. Diese Strategie kann zur Erhöhung der Verfügbarkeit oder bei der Bereitstellung einer Workload für eine globale Zielgruppe verwendet werden (um den Endpunkt näher an die Benutzer zu bringen und/oder um Stacks bereitzustellen, die für die Zielgruppe in dieser Region lokalisiert sind). Als DR-Strategie gilt: Wenn der Workload in einer der AWS-Regionen Regionen, in denen er bereitgestellt wird, nicht unterstützt werden kann, wird diese Region evakuiert, und die verbleibenden Regionen werden verwendet, um die Verfügbarkeit aufrechtzuerhalten. Multi-Site Aktiv/Aktiv ist die betrieblich komplexeste der DR-Strategien und sollte nur dann gewählt werden, wenn die Geschäftsanforderungen dies erfordern.



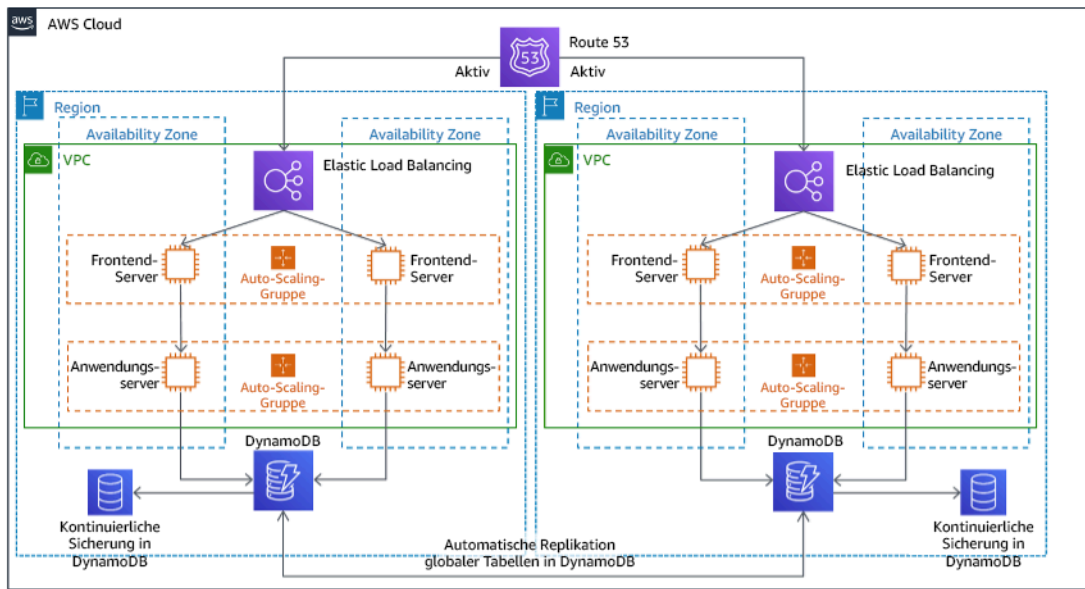


Abbildung 22: Multi-Site Aktiv/Aktiv-Architektur

Weitere Informationen zu dieser Strategie finden Sie unter [Disaster Recovery \(DR\) -Architektur unter AWS, Teil IV: Aktiv/Aktiv an mehreren Standorten.](#)

### AWS Elastic Disaster Recovery

Wenn Sie die Pilotphase- oder Warm-Standby-Strategie für die Notfallwiederherstellung in Betracht ziehen, AWS Elastic Disaster Recovery könnte dies ein alternativer Ansatz mit verbesserten Vorteilen sein. Elastic Disaster Recovery kann ein RPO RTO UND-Ziel bieten, das dem Warm-Standby-System ähnelt, wobei jedoch der kostengünstige Ansatz des Pilotbetriebs beibehalten wird. Elastic Disaster Recovery repliziert Ihre Daten von Ihrer primären Region in Ihre Wiederherstellungsregion und verwendet dabei kontinuierlichen Datenschutz, um eine in Sekunden RPO gemessene und eine in Minuten RTO messbare Leistung zu erzielen. In der Wiederherstellungsregion werden nur die für die Replikation der Daten erforderlichen Ressourcen bereitgestellt, was die Kosten ähnlich wie bei der Pilot-Light-Strategie niedrig hält. Bei Verwendung von Elastic Disaster Recovery koordiniert und orchestriert der Service die Wiederherstellung von Datenverarbeitungs-Ressourcen, wenn die Initiierung als Teil eines Failover oder Drills erfolgt.

## AWS Elastic Disaster Recovery (AWS DRS) – grundlegende Architektur

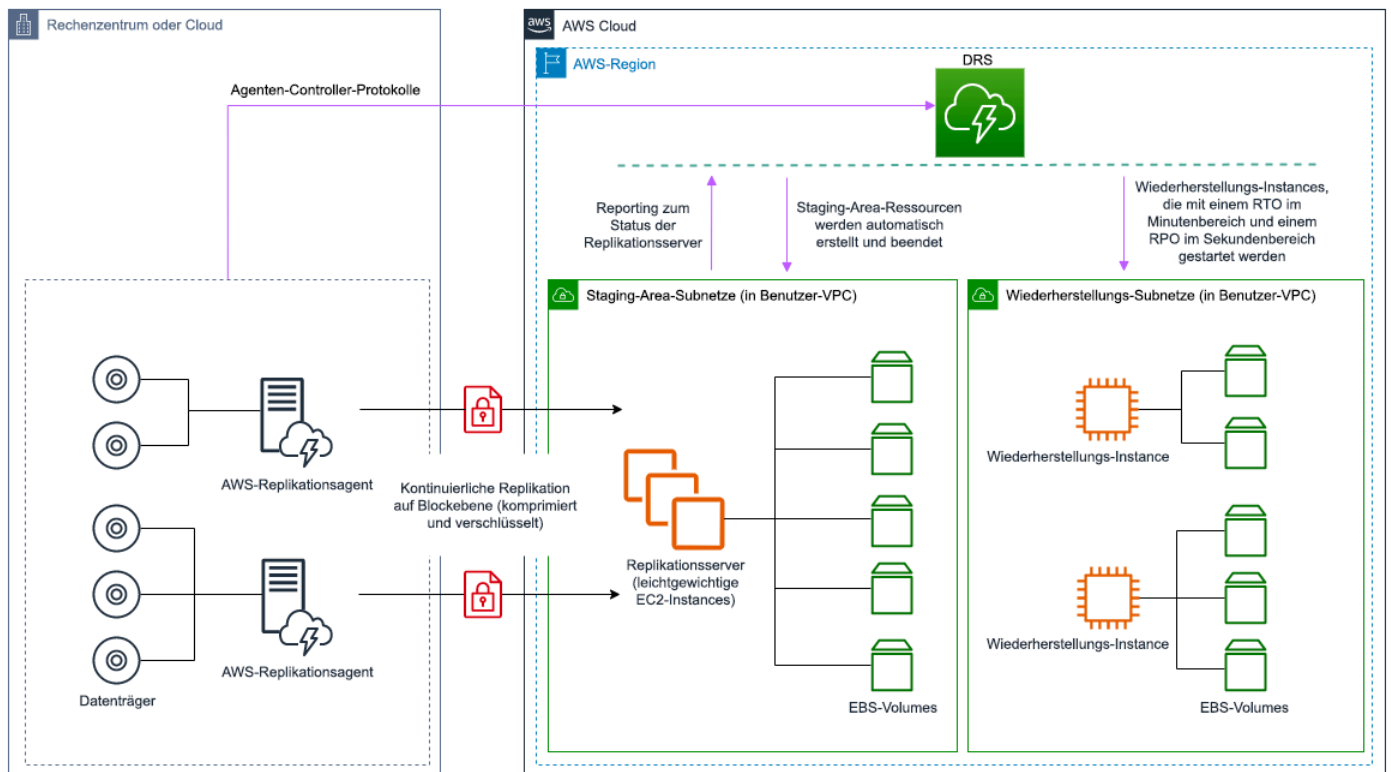


Abbildung 23: AWS Elastic Disaster Recovery Architektur

### Zusätzliche Methoden zum Schutz von Daten

Bei allen Strategien müssen Sie sich auch gegen einen Datennotfall wappnen. Die kontinuierliche Datenreplikation schützt Sie vor einigen Arten von Notfällen, aber sie schützt Sie möglicherweise nicht vor Datenbeschädigung oder -vernichtung, sofern Ihre Strategie nicht auch die Versionierung von gespeicherten Daten oder point-in-time Wiederherstellungsoptionen umfasst. Sie müssen auch die replizierten Daten auf der Wiederherstellungs-Site sichern, um zusätzlich zu den Replikaten point-in-time Backups zu erstellen.

### Verwenden mehrerer Availability Zones (AZs) innerhalb einer einzigen AWS-Region

Wenn Sie mehrere AZs innerhalb einer einzigen Region verwenden, verwendet Ihre DR-Implementierung mehrere Elemente der oben genannten Strategien. Zunächst müssen Sie eine Hochverfügbarkeitsarchitektur (HA) erstellen und mehrere verwenden, AZs wie in Abbildung 23 dargestellt. Diese Architektur verwendet einen aktiven/aktiven Ansatz für mehrere Standorte,

da die [EC2Amazon-Instances](#) und der [Elastic Load Balancer](#) über Ressourcen verfügenAZs, die in mehreren aktiven Anfragen bereitgestellt werden. Die Architektur demonstriert auch Hot-Standby, d. h. wenn die primäre [RDSAmazon-Instance](#) ausfällt (oder die AZ selbst ausfällt), wird die Standby-Instance zur primären Instance heraufgestuft.

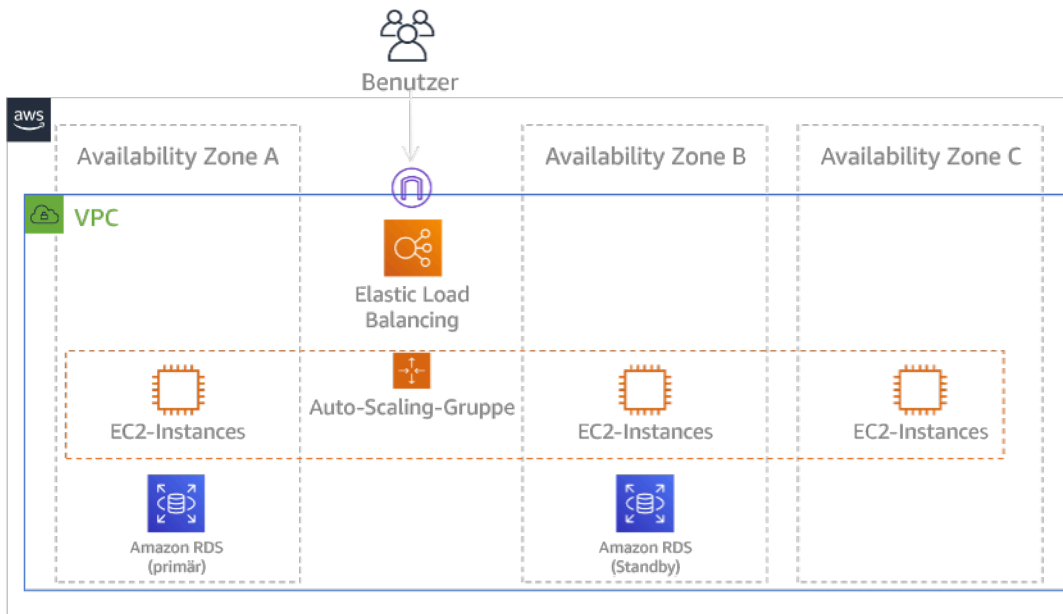


Abbildung 24: Multi-AZ-Architektur

Zusätzlich zu dieser HA-Architektur müssen Sie Backups aller Daten hinzufügen, die für die Ausführung Ihrer Workloads erforderlich sind. Dies ist besonders wichtig für Daten, die auf eine einzelne Zone beschränkt sind, wie z. B. [EBSAmazon-Volumes](#) oder [Amazon Redshift-Cluster](#). Wenn eine AZ ausfällt, müssen Sie diese Daten in einer anderen AZ wiederherstellen. Wenn möglich, sollten Sie AWS-Region als zusätzliche Schutzschicht auch Datensicherungen in eine andere kopieren.

Ein weniger verbreiteter alternativer Ansatz für einzelne Regionen, Multi-AZ-DR, wird im Blogbeitrag [Building highly resilient applications using Amazon Application Recovery Controller, Part 1: Single-Region-Stack](#) beschrieben. Hier besteht die Strategie darin, so viel Isolation wie möglich zwischen den AZs beider aufrechtzuerhalten, z. B. wie Regionen funktionieren. Bei dieser alternativen Strategie können Sie sich für einen Aktiv/Aktiv- oder Aktiv/Passiv-Ansatz entscheiden.

#### Note

Für einige Workloads gibt es gesetzliche Vorschriften im Hinblick auf die Datenresidenz. Wenn dies auf Ihre Arbeitslast an einem Standort zutrifft, an dem es derzeit nur eine

einzigste gibt AWS-Region, dann ist Multiregion nicht für Ihre Geschäftsanforderungen geeignet. Multi-AZ-Strategien bieten einen guten Schutz gegen die meisten Notfälle.

3. Bewerten Sie vor dem Failover (während des normalen Betriebs) die Ressourcen Ihrer Workloads und deren Konfiguration in der Wiederherstellungsregion.

Verwenden Sie für Infrastruktur und AWS Ressourcen Infrastruktur als Code [AWS CloudFormation](#) oder Tools von Drittanbietern wie Hashicorp Terraform. Um die Bereitstellung über mehrere Konten und Regionen mit einem einzigen Vorgang durchzuführen, können Sie Folgendes verwenden. [AWS CloudFormation StackSets](#) Bei Multi-Site-Aktiv/Aktiv- und Hot-Standby-Strategien verfügt die in Ihrer Wiederherstellungsregion bereitgestellte Infrastruktur über dieselben Ressourcen wie Ihre Primärregion. Bei den Strategien Pilot Light und Warm Standby sind zusätzliche Maßnahmen erforderlich, um die Infrastruktur produktionsreif zu machen. Mithilfe von CloudFormation [Parametern](#) und [bedingter Logik](#) können Sie mit einer [einzigsten Vorlage](#) steuern, ob ein bereitgestellter Stack aktiv oder im Standby-Modus ist. Wenn Sie Elastic Disaster Recovery verwenden, repliziert und orchestriert der Service die Wiederherstellung von Anwendungskonfigurationen und Datenverarbeitungs-Ressourcen.

Alle DR-Strategien erfordern, dass Datenquellen innerhalb der AWS-Region gesichert werden und diese Backups anschließend in die Wiederherstellungsregion kopiert werden. [AWS Backup](#) bietet eine zentrale Ansicht, in der Sie Backups für diese Ressourcen konfigurieren, planen und überwachen können. [Für Pilot Light, Warm Standby und Multi-Site active/active sollten Sie auch Daten aus der primären Region auf Datenressourcen in der Wiederherstellungsregion replizieren, z. B. Amazon Relational Database Service \(AmazonRDS\) -DB-Instances oder Amazon DynamoDB-Tabellen.](#) Diese Datenressourcen sind daher aktiv und bereit, Anfragen in der Wiederherstellungsregion zu bedienen.

[Weitere Informationen darüber, wie AWS Dienste in verschiedenen Regionen funktionieren, finden Sie in dieser Blogserie zum Thema Erstellen einer regionsübergreifenden Anwendung mit Services. AWS](#)

4. Ermitteln und implementieren Sie, wie Sie Ihre Wiederherstellungsregion bei Bedarf (im Notfall) auf ein Failover vorbereiten.

Bei Multi-Site Aktiv/Aktiv bedeutet Failover, dass eine Region evakuiert wird und die verbleibenden aktiven Regionen genutzt werden. Im Allgemeinen sind diese Regionen bereit, Datenverkehr aufzunehmen. Bei den Strategien Pilot Light und Warm Standby müssen Ihre Wiederherstellungsmaßnahmen die fehlenden Ressourcen wie die EC2 Instanzen in Abbildung 20 sowie alle anderen fehlenden Ressourcen bereitstellen.

Bei allen oben genannten Strategien müssen Sie möglicherweise schreibgeschützte Instances von Datenbanken zur primären Lese-/Schreib-Instance machen.

Für Sicherung und Wiederherstellung werden beim Wiederherstellen von Daten aus dem Backup Ressourcen für diese Daten wie EBS Volumes, RDS DB-Instances und DynamoDB-Tabellen erstellt. Außerdem müssen Sie die Infrastruktur wiederherstellen und Code bereitstellen. Sie können es verwenden AWS Backup , um Daten in der Wiederherstellungsregion wiederherzustellen. Weitere Details finden Sie unter [REL09-BP01 Identifizieren und sichern Sie alle Daten, die gesichert werden müssen, oder reproduzieren Sie die Daten aus Quellen](#). Der Wiederaufbau der Infrastruktur umfasst die Erstellung von Ressourcen wie EC2 Instanzen zusätzlich zur [Amazon Virtual Private Cloud \(AmazonVPC\)](#), den benötigten Subnetzen und Sicherheitsgruppen. Sie können einen Großteil des Wiederherstellungsprozesses automatisieren. Wie das geht, erfahren Sie in [diesem Blogbeitrag](#).

5. Ermitteln und implementieren Sie, wie Sie den Datenverkehr bei Bedarf (im Notfall) zum Failover umleiten.

Dieser Failover-Vorgang kann entweder automatisch oder manuell eingeleitet werden. Ein automatisch eingeleiteter Failover auf der Grundlage von Zustandsprüfungen oder Alarmen ist mit Vorsicht zu genießen, da ein unnötiger Failover (Fehlalarm) Kosten wie Nichtverfügbarkeit und Datenverlust verursacht. Daher wird häufig ein manuell initiiertes Failover verwendet. In diesem Fall sollten Sie die Schritte für den Failover dennoch automatisieren, sodass die manuelle Auslösung wie ein Knopfdruck wirkt.

Bei der Nutzung AWS von Diensten sind mehrere Optionen zur Verwaltung des Datenverkehrs zu berücksichtigen. Eine Option ist die Verwendung von [Amazon Route 53](#). Mit Amazon Route 53 können Sie mehrere IP-Endpunkte in einem oder mehreren AWS-Regionen mit einem Route 53-Domainnamen verknüpfen. Um ein manuell eingeleitetes Failover zu implementieren, können Sie [Amazon Application Recovery Controller](#) verwenden, der eine hochverfügbare Datenebene API zur Umleitung des Datenverkehrs in die Wiederherstellungsregion bereitstellt. Verwenden Sie bei der Implementierung von Failover Vorgänge auf der Datenebene und vermeiden Sie solche auf der Steuerebene, wie in [REL11-BP04 Verlassen Sie sich bei der Wiederherstellung auf die Datenebene und nicht auf die Steuerebene](#) beschrieben.

Weitere Informationen zu diesen und anderen Optionen finden Sie in [diesem Abschnitt des Whitepapers zur Notfallwiederherstellung](#).

6. Entwerfen Sie einen Plan für das Failback Ihrer Workload.

Failback bedeutet, dass Sie den Workload-Betrieb in der primären Region wieder aufnehmen, nachdem ein Notfallereignis abgeklungen ist. Die Bereitstellung von Infrastruktur und Code für die primäre Region erfolgt im Allgemeinen in denselben Schritten wie ursprünglich, wobei Infrastruktur als Code und Code-Bereitstellungspipelines verwendet werden. Die Herausforderung beim Failback ist die Wiederherstellung von Datenspeichern und die Sicherstellung ihrer Konsistenz mit der in Betrieb befindlichen Wiederherstellungsregion.

Im Status „Failover“ sind die Datenbanken in der Wiederherstellungsregion aktiv und verfügen über die up-to-date Daten. Das Ziel besteht dann darin, die Synchronisation von der Wiederherstellungsregion zur primären Region neu zu synchronisieren und sicherzustellen, dass dies der Fall ist up-to-date.

Bei einigen AWS Diensten erfolgt dies automatisch. Wenn Sie [globale Amazon DynamoDB-Tabellen](#) verwenden, setzt DynamoDB die Propagierung aller ausstehenden Schreibvorgänge fort, sobald die Tabelle wieder online ist, auch wenn sie in der primären Region nicht mehr verfügbar war. Wenn Sie [Amazon Aurora Global Database](#) und ein [verwaltetes geplantes Failover](#) verwenden, wird die vorhandene Replikationstopologie der globalen Aurora-Datenbank beibehalten. Daher wird die ehemalige Lese-/Schreib-Instance in der primären Region zu einem Replikat und erhält Aktualisierungen von der Wiederherstellungsregion.

In Fällen, in denen dies nicht automatisch geschieht, müssen Sie die Datenbank in der primären Region als Replikat der Datenbank in der Wiederherstellungsregion neu einrichten. In vielen Fällen bedeutet dies, dass die alte primäre Datenbank gelöscht und neue Replikate erstellt werden müssen.

Wenn Sie nach einem Failover in Ihrer Wiederherstellungsregion weiterarbeiten können, sollten Sie diese zur neuen Primärregion machen. Sie würden trotzdem alle oben genannten Schritte durchführen, um die ehemalige Primärregion in eine Wiederherstellungsregion zu verwandeln. Einige Unternehmen führen eine planmäßige Rotation durch und tauschen ihre Primär- und Wiederherstellungsregionen in regelmäßigen Abständen aus (z. B. alle drei Monate).

Alle für Failover und Failback erforderlichen Schritte sollten in einem Playbook festgehalten werden, das allen Teammitgliedern zur Verfügung steht und regelmäßig überprüft wird.

Wenn Sie Elastic Disaster Recovery verwenden, hilft der Service bei der Orchestrierung und Automatisierung des Failback-Prozesses. Weitere Informationen finden Sie unter [Durchführen eines Failbacks](#).

## Aufwand für den Implementierungsplan: Hoch

### Ressourcen

#### Zugehörige bewährte Methoden:

- [the section called “REL09-BP01 Identifizieren und sichern Sie alle Daten, die gesichert werden müssen, oder reproduzieren Sie die Daten aus Quellen”](#)
- [the section called “REL11-BP04 Verlassen Sie sich bei der Wiederherstellung auf die Datenebene und nicht auf die Steuerebene”](#)
- [the section called “REL13-BP01 Definieren Sie Wiederherstellungsziele für Ausfallzeiten und Datenverlust”](#)

#### Zugehörige Dokumente:

- [AWS Architecture Blog: Notfallwiederherstellung](#)
- [Disaster Recovery von Workloads auf AWS: Wiederherstellung in der Cloud \(AWS Whitepaper\)](#)
- [Optionen für die Notfallwiederherstellung in der Cloud](#)
- [Entwickeln einer Multi-Region-Serverless-Backend-Lösung, die aktiv/aktiv ist](#)
- [Multi-Region-Serverless-Backend – neu aufgelegt](#)
- [RDS: Read Replica regionsübergreifend replizieren](#)
- [Route 53: Failover konfigurieren DNS](#)
- [S3: Regionsübergreifende Replikation](#)
- [Was ist AWS Backup?](#)
- [Was ist Amazon Application Recovery Controller?](#)
- [AWS Elastic Disaster Recovery](#)
- [HashiCorpTerraform: Erste Schritte - AWS](#)
- [APNPartner: Partner, die bei der Notfallwiederherstellung helfen können](#)
- [AWS Marketplace: Für die Notfallwiederherstellung geeignete Produkte](#)

#### Zugehörige Videos:

- [Notfallwiederherstellung von Workloads auf AWS](#)
- [AWS re:Invent 2018: Architekturmuster für aktiv-aktive Anwendungen mit mehreren Regionen \(09-R2\) ARC2](#)

- [Erste Schritte mit AWS Elastic Disaster Recovery | Amazon Web Services](#)

Zugehörige Beispiele:

- [Well-Architected Lab – Notfallwiederherstellung](#) – Workshop-Reihe zur Veranschaulichung von DR-Strategien

REL13-BP03 Testen Sie die Disaster Recovery-Implementierung, um die Implementierung zu validieren

Testen Sie regelmäßig den Failover zu Ihrer Wiederherstellungs-Site, um sicherzustellen, dass er ordnungsgemäß funktioniert RTO und dass alle Anforderungen erfüllt RPO sind.

Typische Anti-Muster:

- Failover sollten nie in der Produktion getestet werden.

Vorteile der Nutzung dieser bewährten Methode: Durch regelmäßige Tests des Notfallwiederherstellungsplans ist gewährleistet, dass er bei Bedarf funktioniert und von Ihrem Team umgesetzt werden kann.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Hoch

Implementierungsleitfaden

Vom Erstellen selten durchgeführter Wiederherstellungspfade wird abgeraten. So könnten Sie beispielsweise einen zweiten Datenspeicher unterhalten, der nur für Leseabfragen verwendet wird. Wenn Sie Daten in einen Datenspeicher schreiben und der primäre Datenspeicher einen Fehler ausgibt, können Sie einen Failover auf den zweiten Datenspeicher durchführen. Wenn Sie diesen Failover nicht regelmäßig testen, werden Sie möglicherweise feststellen, dass Ihre Annahmen zu den Möglichkeiten des sekundären Datenspeichers unzutreffend sind. Die Kapazität des sekundären Datenspeichers, die bei den letzten Tests möglicherweise noch ausreichend war, genügt möglicherweise nicht mehr den Anforderungen dieses Szenarios. Unsere Erfahrungen haben gezeigt, dass bei einer Wiederherstellung nach einem Fehler nur der Pfad funktioniert, den Sie regelmäßig testen. Daher ist es ratsam, mehrere Wiederherstellungspfade zu pflegen. Sie können Wiederherstellungsmuster erstellen und diese regelmäßig testen. Auch komplexe oder kritische Wiederherstellungspfade müssen regelmäßig mittels Fehlersimulationen in der Produktion durchgeführt werden, um sicherzustellen, dass sie funktionieren. In dem gerade besprochenen



Beispiel sollten Sie regelmäßig und unabhängig von der Erfordernis einen Failover auf die Standby-Ressourcen durchführen.

## Implementierungsschritte

1. Legen Sie die Workloads für die Wiederherstellung aus. Testen Sie regelmäßig Ihre Wiederherstellungspfade Die Recovery-orientierte Datenverarbeitung identifiziert die Merkmale von Systemen, die die Wiederherstellung verbessern: Isolierung und Redundanz, systemweite Fähigkeit zur Rücknahme von Änderungen, Fähigkeit zur Überwachung und Bestimmung des Zustands, Fähigkeit zur Diagnose, automatisierte Wiederherstellung, modularer Aufbau und Fähigkeit zum Neustart. Testen Sie den Wiederherstellungspfad, um zu überprüfen, ob Sie die Wiederherstellung in der angegebenen Zeit und in dem angegebenen Zustand durchführen können. Dokumentieren Sie während dieser Wiederherstellung auftretende Probleme in Ihren Runbooks und suchen Sie vor dem nächsten Test nach Lösungen.
2. Verwenden Sie für EC2 Amazon-basierte Workloads [AWS Elastic Disaster Recovery](#) die Implementierung und den Start von Drill-Instances für Ihre DR-Strategie. AWS Elastic Disaster Recovery bietet die Möglichkeit, Drills effizient durchzuführen, sodass Sie sich auf ein Failover-Ereignis vorbereiten können. Sie können Ihre Instances mit Elastic Disaster Recovery außerdem regelmäßig zu Test- und Übungszwecken starten, ohne den Datenverkehr weiterleiten zu müssen.

## Ressourcen

### Zugehörige Dokumente:

- [APN Partner: Partner, die Ihnen bei der Notfallwiederherstellung helfen können](#)
- [AWS Architecture Blog: Notfallwiederherstellung](#)
- [AWS Marketplace: Für die Notfallwiederherstellung geeignete Produkte](#)
- [AWS Elastic Disaster Recovery](#)
- [Disaster Recovery von Workloads auf AWS: Wiederherstellung in der Cloud \(AWS Whitepaper\)](#)
- [AWS Elastic Disaster Recovery Vorbereitung auf den Failover](#)
- [The Berkeley/Stanford Recovery-Oriented Computing Project](#)
- [Was ist der AWS Fault Injection Simulator?](#)

### Zugehörige Videos:

- [AWS re:Invent 2018: Architekturmuster für aktiv-aktive Anwendungen in mehreren Regionen](#)

- [AWS re:Invent 2019: und Disaster-Recovery-Lösungen mit Backup-and-restore AWS](#)

Zugehörige Beispiele:

- [Well-Architected Lab – Testen der Ausfallsicherheit](#)

REL13-BP04 Konfigurationsabweichungen am DR-Standort oder in der Region verwalten

Stellen Sie sicher, dass die Infrastruktur, die Daten und die Konfiguration am Standort oder in der Region der Notfallwiederherstellung den Anforderungen entsprechen. Stellen Sie beispielsweise sicher, dass AMIs die Servicekontingente aktuell sind.

AWS Config überwacht und zeichnet Ihre AWS Ressourcenkonfigurationen kontinuierlich auf. Es kann Abweichungen erkennen und [AWS Systems Manager Automation](#) aufrufen, um sie zu beheben und Alarme auszulösen. AWS CloudFormation kann außerdem Abweichungen in Stacks erkennen, die Sie bereitgestellt haben.

Typische Anti-Muster:

- Fehlende Aktualisierungen an Ihren Wiederherstellungsstandorten, wenn Sie an Ihren primären Standorten Änderungen an der Konfiguration oder Infrastruktur vornehmen.
- Mögliche Einschränkungen (z. B. Serviceunterschiede) an primären Standorten und Wiederherstellungsstandorten werden nicht berücksichtigt.

Vorteile der Nutzung dieser bewährten Methode: Wenn Ihre Umgebung für die Notfallwiederherstellung mit der vorhandenen Umgebung konsistent ist, gewährleistet dies eine vollständige Wiederherstellung.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel

Implementierungsleitfaden

- Stellen Sie sicher, dass die Bereitstellung an Haupt- und Sicherheitsstandorte erfolgt. Pipelines für die Bereitstellung von Anwendungen in der Produktion müssen die Anwendungen an alle Standorte verteilen, die in der Strategie für die Notfallwiederherstellung angegeben sind. Dazu gehören auch Entwicklungs- und Testumgebungen.

- Ermöglicht AWS Config die Verfolgung potenzieller Driftstandorte. Verwenden Sie AWS Config Regeln, um Systeme zu erstellen, die Ihre Disaster-Recovery-Strategien durchsetzen und Warnmeldungen ausgeben, wenn Abweichungen erkannt werden.
  - [Behebung nicht konformer Ressourcen AWS durch AWS-Config-Regeln](#)
  - [AWS Systems Manager Automatisierung](#)
- Verwenden Sie AWS CloudFormation, um Ihre Infrastruktur bereitzustellen. AWS CloudFormation kann Abweichungen zwischen dem, was Ihre CloudFormation Vorlagen spezifizieren, und dem, was tatsächlich bereitgestellt wird, erkennen.
  - [AWS CloudFormation: Erkennen Sie Abweichungen auf einem gesamten CloudFormation Stack](#)

## Ressourcen

### Zugehörige Dokumente:

- [APNPartner: Partner, die bei der Notfallwiederherstellung helfen können](#)
- [AWS Architecture Blog: Notfallwiederherstellung](#)
- [AWS CloudFormation: Erkennen Sie Drift auf einem gesamten CloudFormation Stack](#)
- [AWS Marketplace: Für die Notfallwiederherstellung geeignete Produkte](#)
- [AWS Systems Manager Automatisierung](#)
- [Disaster Recovery von Workloads auf AWS: Wiederherstellung in der Cloud \(AWS Whitepaper\)](#)
- [Wie implementiere ich eine Lösung für die Verwaltung der Infrastrukturkonfiguration in AWS?](#)
- [Behebung nicht richtlinienkonformer Ressourcen durch AWS-Config-Regeln](#)

### Zugehörige Videos:

- [AWS re:Invent 2018: Architekturmuster für aktiv-aktive Anwendungen mit mehreren Regionen \(09-R2\) ARC2](#)

## REL13-BP05 Automatisieren Sie die Wiederherstellung

Verwenden Sie AWS Tools von Drittanbietern, um die Systemwiederherstellung zu automatisieren und den Datenverkehr an den DR-Standort oder die DR-Region weiterzuleiten.

Auf der Grundlage konfigurierter Zustandsprüfungen können AWS Dienste wie Elastic Load Balancing und AWS Auto Scaling die Last auf fehlerfreie Availability Zones verteilen, während

Dienste wie Amazon Route 53 und AWS Global Accelerator die Last an fehlerfreie Zonen weiterleiten können AWS-Regionen. Amazon Application Recovery Controller unterstützt Sie bei der Verwaltung und Koordination des Failovers mithilfe von Funktionen zur Bereitschaftsprüfung und Routingkontrolle. Diese Funktionen überwachen kontinuierlich die Fähigkeit Ihrer Anwendung, sich nach Ausfällen zu erholen, sodass Sie die Anwendungswiederherstellung in mehreren AWS-Regionen Availability Zones und vor Ort kontrollieren können.

Für Workloads in bestehenden physischen oder virtuellen Rechenzentren oder privaten Clouds ermöglicht [AWS Elastic Disaster Recovery](#) Unternehmen die Einrichtung einer automatisierten Notfallwiederherstellungsstrategie in AWS. Elastic Disaster Recovery unterstützt auch die regionsübergreifende und Availability-Zone-übergreifende Notfallwiederherstellung in AWS.

Typische Anti-Muster:

- Die Implementierung von identischem automatisiertem Failover und Failback kann bei einem Fehler zu Flapping führen.

Vorteile der Nutzung dieser bewährten Methode: Die automatisierte Wiederherstellung verkürzt die Wiederherstellungszeit, da manuelle Fehler nicht mehr möglich sind.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel

Implementierungsleitfaden

- Automatisieren Sie Wiederherstellungspfade. Für kurze Wiederherstellungszeiten sollten Sie sich an Ihren [Notfallwiederherstellungsplan](#) halten, damit Ihre IT-Systeme im Falle einer Störung schnell wieder online sind.
- Verwenden Sie Elastic Disaster Recovery für automatisiertes Failover und Failback. Elastic Disaster Recovery repliziert Ihre Maschinen (einschließlich Betriebssystem, Systemstatuskonfiguration, Datenbanken, Anwendungen und Dateien) kontinuierlich in einen kostengünstigen Staging-Bereich in Ihrer Ziel AWS-Konto - und bevorzugten Region. Nachdem Sie sich für die Wiederherstellung mit Elastic Disaster Recovery entschieden haben, automatisiert Elastic Disaster Recovery im Katastrophenfall die Konvertierung Ihrer replizierten Server in vollständig bereitgestellte Workloads in Ihrer Wiederherstellungsregion in AWS.
- [Verwenden von Elastic Disaster Recovery für Failover und Failback](#)
- [AWS Elastic Disaster Recovery Ressourcen](#)

## Ressourcen

### Zugehörige Dokumente:

- [APNPartner: Partner, die Ihnen bei der Notfallwiederherstellung helfen können](#)
- [AWS Architecture Blog: Notfallwiederherstellung](#)
- [AWS Marketplace: Für die Notfallwiederherstellung geeignete Produkte](#)
- [AWS Systems Manager Automatisierung](#)
- [AWS Elastic Disaster Recovery](#)
- [Disaster Recovery von Workloads auf AWS: Wiederherstellung in der Cloud \(AWS Whitepaper\)](#)

### Zugehörige Videos:

- [AWS re:Invent 2018: Architekturmuster für aktiv-aktive Anwendungen mit mehreren Regionen \(09-R2\) ARC2](#)

## Leistungseffizienz

Die Säule der Leistungseffizienz betrifft die Fähigkeit zur effizienten Nutzung von Cloud-Ressourcen, um die Leistungsanforderungen zu erfüllen, sowie die Möglichkeit zur Aufrechterhaltung dieser Effizienz bei Nachfrageänderungen und einer Weiterentwicklung der Technologien. Verbindliche Anleitungen zur Implementierung finden Sie im [Whitepaper „Säule der Leistungseffizienz“](#).

### Bereiche für bewährte Methoden

- [Auswahl der Architektur](#)
- [Computer und Hardware](#)
- [Datenverwaltung](#)
- [Netzwerk und Bereitstellung von Inhalten](#)
- [Prozess und Kultur](#)

## Auswahl der Architektur

### Fragen

- [PERF1. Wie wählen Sie geeignete Cloud-Ressourcen und -Architekturen für Ihren Workload aus?](#)

## PERF1. Wie wählen Sie geeignete Cloud-Ressourcen und -Architekturen für Ihren Workload aus?

Die optimale Lösung für eine bestimmte Workload variiert und Lösungen sind häufig eine Kombination mehrerer Ansätze. Well-Architected-Workloads nutzen mehrere Lösungen und ermöglichen verschiedene Funktionen zur Verbesserung der Leistung.

### Bewährte Methoden

- [PERF01-BP01 Erfahren Sie mehr über verfügbare Cloud-Dienste und -Funktionen und verstehen Sie sie](#)
- [PERF01-BP02 Lassen Sie sich von Ihrem Cloud-Anbieter oder einem geeigneten Partner beraten, um mehr über Architekturmuster und Best Practices zu erfahren](#)
- [PERF01-BP03 Kosten bei Architekturentscheidungen berücksichtigen](#)
- [PERF01-BP04 Bewerten Sie, wie sich Kompromisse auf Kunden und Architektureffizienz auswirken](#)
- [PERF01-BP05 Benutzungsrichtlinien und Referenzarchitekturen](#)
- [PERF01-BP06 Nutzen Sie Benchmarking, um Architekturentscheidungen zu treffen](#)
- [PERF01-BP07 Verwenden Sie einen datengesteuerten Ansatz für architektonische Entscheidungen](#)

PERF01-BP01 Erfahren Sie mehr über verfügbare Cloud-Dienste und -Funktionen und verstehen Sie sie

Informieren Sie sich kontinuierlich über verfügbare Services und Konfigurationen, die Ihnen helfen, bessere architektonische Entscheidungen zu treffen und die Leistungseffizienz Ihrer Workload-Architektur zu verbessern.

### Typische Anti-Muster:

- Sie verwenden die Cloud als gemeinsam genutztes Rechenzentrum.
- Sie modernisieren die Anwendung nach der Migration in die Cloud nicht.
- Sie verwenden nur einen Speichertyp für alle Objekte, die gespeichert werden müssen.
- Sie verwenden Instance-Typen, die am besten zu Ihren aktuellen Standards passen, bei Bedarf jedoch größer sind.
- Von Ihnen werden Technologien bereitgestellt und verwaltet, die als verwaltete Services verfügbar sind.

Vorteile der Nutzung dieser bewährten Methode: Wenn Sie neue Services und Konfigurationen in Betracht ziehen, können Sie möglicherweise die Leistung erheblich verbessern, die Kosten senken und den Aufwand für die Aufrechterhaltung der Workload optimieren. Es kann Ihnen auch dabei helfen, die Einführung von Cloud-fähigen Produkten time-to-value zu beschleunigen.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Hoch

### Implementierungsleitfaden

AWS veröffentlicht kontinuierlich neue Dienste und Funktionen, mit denen die Leistung verbessert und die Kosten von Cloud-Workloads gesenkt werden können. Die up-to-date Beibehaltung dieser neuen Dienste und Funktionen ist entscheidend für die Aufrechterhaltung der Leistungseffizienz in der Cloud. Die Modernisierung der Workload-Architektur hilft Ihnen auch dabei, die Produktivität zu beschleunigen, Innovationen voranzutreiben und mehr Wachstumschancen zu erschließen.

### Implementierungsschritte

- Inventarisieren Sie die Workload-Software und -Architektur für verwandte Services. Entscheiden Sie, über welche Produktkategorie Sie mehr erfahren möchten.
- Erkunden Sie die AWS Angebote, um die relevanten Dienste und Konfigurationsoptionen zu identifizieren und mehr darüber zu erfahren, mit denen Sie die Leistung verbessern und die Kosten und die betriebliche Komplexität reduzieren können.
  - [Amazon Web Services Cloud](#)
  - [AWS Akademie](#)
  - [Was ist neu bei AWS?](#)
  - [AWS Blog](#)
  - [AWS Skill Builder](#)
  - [AWS Veranstaltungen und Webinare](#)
  - [AWS Training und Zertifizierungen](#)
  - [AWS Youtube-Kanal](#)
  - [AWS Werkstätten](#)
  - [AWS -Communitys](#)
- Verwenden Sie [Amazon Q](#), um relevante Informationen und Tipps zu Services zu erhalten.
- Verwenden Sie Sandbox- bzw. Nicht-Produktionsumgebungen, um neue Services zu erlernen und mit ihnen zu experimentieren, ohne dass zusätzliche Kosten anfallen.
- Informieren Sie sich kontinuierlich über neue Cloud-Services und -Features.

## Ressourcen

### Zugehörige Dokumente:

- [Übersicht über Amazon Web Services](#)
- [EC2Amazon-Funktionen](#)
- [Lernen Sie step-by-step mit einem AWS Partner-Lernplan](#)
- [AWS Schulung und Zertifizierung](#)
- [Mein Lernweg zum AWS Lösungsarchitekten](#)
- [AWS Zentrum für Architektur](#)
- [AWS Partner Network](#)
- [AWS Bibliothek mit Lösungen](#)
- [AWS Wissenszentrum](#)
- [Erstellen Sie moderne Anwendungen auf AWS](#)

### Zugehörige Videos:

- [AWS re:Invent 2023 — Was ist neu bei Amazon EC2](#)
- [AWS re:Invent 2022 — Senken Sie Ihre Betriebs- und Infrastrukturkosten mit Amazon ECS](#)
- [AWS re:Invent 2023 — Bauen Sie mit der Effizienz, Agilität und Innovation der Cloud mit AWS](#)
- [AWS re:Invent 2022 — Implementieren Sie ML-Modelle für Inferenz mit hoher Leistung und niedrigen Kosten](#)
- [This is my Architecture](#)

### Zugehörige Beispiele:

- [AWS Beispiele](#)
- [AWS SDKBeispiele](#)

PERF01-BP02 Lassen Sie sich von Ihrem Cloud-Anbieter oder einem geeigneten Partner beraten, um mehr über Architekturmuster und Best Practices zu erfahren

Greifen Sie bei Ihren architektonischen Entscheidungen auf die Ressourcen von Cloud-Unternehmen, wie etwa Dokumentation, Lösungsarchitekten, professionelle Services oder einen geeigneten Partner



zurück. Diese Ressourcen helfen Ihnen dabei, Ihre Architektur zu überprüfen und zu verbessern, um so die Leistung zu optimieren.

Typische Anti-Muster:

- Sie verwenden AWS als gängiger Cloud-Anbieter.
- Sie nutzen AWS Dienste auf eine Weise, für die sie nicht konzipiert wurden.
- Sie befolgen alle Anweisungen, ohne Ihren Geschäftskontext zu berücksichtigen.

Vorteile der Nutzung dieser bewährten Methode: Wenn Sie sich Rat bei einem Cloud-Anbieter oder einem geeigneten Partner einholen, können Sie die richtige Architektur für die Workload wählen und Entscheidungen mit größerer Zuversicht treffen.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Mittel

Implementierungsleitfaden

AWS bietet eine breite Palette an Anleitungen, Dokumentationen und Ressourcen, die Sie beim Aufbau und der Verwaltung effizienter Cloud-Workloads unterstützen können. AWS Die Dokumentation enthält Codebeispiele, Tutorials und detaillierte Serviceerklärungen. Neben der Dokumentation AWS bietet sie Schulungs- und Zertifizierungsprogramme, Lösungsarchitekten und professionelle Dienstleistungen, die Kunden dabei unterstützen können, verschiedene Aspekte von Cloud-Diensten zu erkunden und eine effiziente Cloud-Architektur zu implementieren AWS.

Nutzen Sie diese Ressourcen, um Einblicke in wertvolles Wissen und bewährte Methoden zu gewinnen, Zeit zu sparen und bessere Ergebnisse in der AWS Cloud zu erzielen.

Implementierungsschritte

- Lesen Sie die AWS Dokumentation und Anleitungen und befolgen Sie die bewährten Methoden. Diese Ressourcen können Ihnen helfen, Services effektiv auszuwählen und zu konfigurieren und eine bessere Leistung zu erzielen.
  - [AWS Dokumentation](#) (wie Benutzerhandbücher und Whitepapers)
  - [AWS Blog](#)
  - [AWS Training und Zertifizierungen](#)
  - [AWS Youtube-Kanal](#)

- Nehmen Sie an AWS Partnerveranstaltungen (wie AWS Global Summits, AWS re:Invent, Benutzergruppen und Workshops) teil, um von AWS Experten mehr über bewährte Verfahren für die Nutzung von Diensten zu erfahren. AWS
  - [Lernen Sie step-by-step mit einem Partner-Lernplan AWS](#)
  - [AWS Veranstaltungen und Webinare](#)
  - [AWS Workshops](#)
  - [AWS Gemeinschaften](#)
- Wenden Sie sich an AWS uns, um Unterstützung zu erhalten, wenn Sie zusätzliche Anleitungen oder Produktinformationen benötigen. AWS Solutions Architects und [AWS Professional Services](#) beraten Sie bei der Implementierung von Lösungen. [AWS Partner](#) bieten AWS Fachwissen, um Ihnen dabei zu helfen, Agilität und Innovation für Ihr Unternehmen zu nutzen.
- Verwenden Sie [AWS Support](#), wenn Sie technischen Support benötigen, um einen Service effektiv nutzen zu können. [Unsere Supportpläne](#) sind darauf ausgelegt, Ihnen die richtige Kombination aus Tools und Zugang zu Fachwissen zu bieten, damit Sie erfolgreich sein und AWS gleichzeitig die Leistung optimieren, Risiken managen und die Kosten unter Kontrolle halten können.

## Ressourcen

### Zugehörige Dokumente:

- [AWS -Architekturzentrum](#)
- [AWS Partner Network](#)
- [AWS -Lösungsbibliothek](#)
- [AWS Knowledge Center](#)
- [AWS Enterprise Support](#)

### Zugehörige Videos:

- [This is my Architecture](#)
- [AWS re:Invent 2023 — Fortgeschrittene ereignisgesteuerte Muster mit Amazon EventBridge](#)
- [AWS re:Invent 2023 — Implementierung verteilter Entwurfsmuster auf AWS](#)
- [AWS re:Invent 2023 — Anwendungsarchitektur als Code](#)

### Zugehörige Beispiele:

- [AWS Beispiele](#)
- [AWS SDKBeispiele](#)
- [AWS Analytics-Referenzarchitektur](#)

## PERF01-BP03 Kosten bei Architekturentscheidungen berücksichtigen

Berücksichtigen Sie die Kosten bei Ihren architektonischen Entscheidungen, um die Ressourcennutzung und Leistungseffizienz der Cloud-Workloads zu verbessern. Wenn Sie sich der Kostenauswirkungen der Cloud-Workload bewusst sind, ist es wahrscheinlicher, dass Sie effiziente Ressourcen nutzen und verschwenderische Methoden reduzieren.

Typische Anti-Muster:

- Sie verwenden nur eine Instance-Familie.
- Sie bewerten keine lizenzierten Lösungen verglichen mit Open-Source-Lösungen.
- Sie definieren keine Speicher-Lebenszyklusrichtlinien.
- Sie überprüfen keine neuen Dienste und Funktionen von AWS Cloud
- Sie nutzen nur Blockspeicher.

Vorteile der Nutzung dieser bewährten Methode: Wenn Sie die Kosten bei Ihrer Entscheidungsfindung berücksichtigen, können Sie effizientere Ressourcen einsetzen und andere Investitionen in Betracht ziehen.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Mittel

### Implementierungsleitfaden

Die Kostenoptimierung von Workloads kann die Ressourcennutzung verbessern und Verschwendung bei einer Cloud-Workload vermeiden. Die Berücksichtigung der Kosten bei architektonischen Entscheidungen beinhaltet in der Regel die richtige Dimensionierung der Workload-Komponenten und die Schaffung von Elastizität. Dies führt zu einer verbesserten Leistungseffizienz von Cloud-Workloads.

### Implementierungsschritte

- Legen Sie Kostenziele wie Budgetlimits für die Cloud-Workload fest.

- Identifizieren Sie die wesentlichen Komponenten (wie Instances und Speicher), die die Kosten der Workload erhöhen. Sie können [AWS Pricing Calculator](#) und [AWS Cost Explorer](#) verwenden, um die wichtigsten Kostentreiber in Ihrer Workload zu identifizieren.
- Informieren Sie sich über die [Preismodelle](#) in der Cloud, z. B. On-Demand, Reserved Instances, Savings Plans und Spot Instances.
- Verwenden Sie die [bewährten Methoden zur Kostenoptimierung von Well-Architected](#), um diese Schlüsselkomponenten im Hinblick auf die Kosten zu optimieren.
- Überwachen und analysieren Sie kontinuierlich die Kosten, um Möglichkeiten zur Kostenoptimierung in der Workload zu identifizieren.
  - Nutzen Sie [AWS -Budgets](#), um bei nicht akzeptablen Kosten Warnungsmeldungen zu erhalten.
  - Verwenden Sie [AWS Compute Optimizer](#) oder [AWS Trusted Advisor](#), um Empfehlungen zur Kostenoptimierung zu erhalten.
  - Nutzen Sie [AWS Cost Anomaly Detection](#), um das automatisierte Erkennen von Kostenanomalien mit Ursachenanalyse zu erhalten.

## Ressourcen

### Zugehörige Dokumente:

- [Was ist AWS Billing and Cost Management?](#)
- [Kostenoptimierung mit AWS](#)
- [Wahl einer AWS Kostenmanagementstrategie](#)
- [Ein Leitfaden für Anfänger zum AWS Kostenmanagement](#)
- [Eine detaillierte Übersicht über das Cost Intelligence Dashboard](#)
- [AWS -Architekturzentrum](#)
- [AWS -Lösungsbibliothek](#)
- [AWS Knowledge Center](#)

### Zugehörige Videos:

- [This is my Architecture](#)
- [AWS re:Invent 2023 — Was ist neu bei AWS der Kostenoptimierung](#)
- [AWS re:Invent 2023 — Optimieren Sie Kosten und Leistung und verfolgen Sie die Fortschritte bei der Minderung](#)

- [AWS re:Invent 2023 — bewährte Methoden zur Optimierung der Speicherkosten AWS](#)
- [AWS re:Invent 2023 — Optimieren Sie die Kosten in Ihren Umgebungen mit mehreren Konten](#)

Zugehörige Beispiele:

- [AWS Compute Optimizer Demo-Code](#)
- [Workshop zur Kostenoptimierung](#)
- [Technische Playbooks zur Implementierung von Cloud Financial Management](#)
- [Startoptimierung: Optimierung der Anwendungsleistung für maximale Effizienz](#)
- [Workshop zur Serverless-Optimierung \(Leistung und Kosten\)](#)
- [Skalierung kostengünstiger Architekturen](#)

PERF01-BP04 Bewerten Sie, wie sich Kompromisse auf Kunden und Architektureffizienz auswirken

Ermitteln Sie beim Evaluieren von leistungsbezogenen Verbesserungen, welche gewählten Optionen sich auf Ihre Kunden und die Effizienz der Workloads auswirken. Wenn sich die Systemleistung beispielsweise bei Verwendung eines Schlüssel-Wert-Datenspeichers erhöht, sollten Sie unbedingt ermitteln, welche Auswirkungen sich bei einem dauerhaften Einsatz für die Kunden ergeben würden.

Typische Anti-Muster:

- Sie gehen davon aus, dass alle Leistungsgewinne implementiert werden sollten, auch wenn es Kompromisse für die Implementierung gibt.
- Änderungen an Workloads werden nur dann ausgewertet, wenn ein Leistungsproblem einen kritischen Punkt erreicht hat.

Vorteile der Nutzung dieser bewährten Methode: Wenn Sie potenzielle leistungsbezogene Verbesserungen bewerten, müssen Sie entscheiden, ob die Kompromisse für die Änderungen angesichts der Workload-Anforderungen akzeptabel sind. In einigen Fällen müssen Sie möglicherweise zusätzliche Kontrollen implementieren, um Kompromisse zu kompensieren.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Hoch

Implementierungsleitfaden

Identifizieren Sie kritische Bereiche in der Architektur in Bezug auf Leistung und Kundenauswirkung. Stellen Sie fest, welche Verbesserungen möglich und welche Kompromisse damit verbunden sind

und wie sich diese auf das System und das Benutzererlebnis auswirken. So lässt sich beispielsweise durch Caching von Daten die Leistung deutlich steigern. Es ist aber eine eindeutige Strategie erforderlich, mit der festgelegt wird, wie und wann Cache-Daten aktualisiert oder ungültig werden, um unerwünschtes Systemverhalten zu verhindern.

### Implementierungsschritte

- Verstehen Sie Ihre Workload-Anforderungen und SLAs
- Definieren Sie klare Bewertungsfaktoren. Faktoren können sich auf Kosten, Zuverlässigkeit, Sicherheit und Leistung der Workload beziehen.
- Wählen Sie die Architektur und Services, die Ihren Anforderungen entsprechen.
- Führen Sie Experimente und Machbarkeitsstudien (POCs) durch, um Kompromisse und Auswirkungen auf Kunden und Architektureffizienz zu bewerten. In der Regel verbrauchen hochverfügbare, leistungsstarke und sichere Workloads mehr Cloud-Ressourcen und bieten gleichzeitig ein besseres Kundenerlebnis. Machen Sie sich ein Bild von den Kompromissen in Bezug auf Komplexität, Leistung und Kosten Ihrer Workloads. In der Regel geht die Priorisierung von zwei der Faktoren auf Kosten des dritten.

### Ressourcen

#### Zugehörige Dokumente:

- [Amazon Builders' Library](#)
- [Amazon QuickSight KPIs](#)
- [Amazon CloudWatch RUM](#)
- [X-Ray-Dokumentation](#)
- [Resilienzmuster und Kompromisse verstehen, um eine effiziente Architektur in der Cloud zu entwickeln](#)

#### Zugehörige Videos:

- [Optimieren Sie Anwendungen über Amazon CloudWatch RUM](#)
- [AWS re:Invent 2023 — Kapazität, Verfügbarkeit, Kosteneffizienz: Wählen Sie drei](#)
- [AWS re:Invent 2023 — Fortschrittliche Integrationsmuster und Kompromisse für lose gekoppelte Systeme](#)

## Zugehörige Beispiele:

- [Messen Sie die Seitenladezeit mit Amazon CloudWatch Synthetics](#)
- [CloudWatch RUM Amazon-Webclient](#)

## PERF01-BP05 Benutzungsrichtlinien und Referenzarchitekturen

Verwenden Sie interne Richtlinien und vorhandene Referenzarchitekturen bei der Auswahl von Services und Konfigurationen, um die Workload effizienter zu gestalten und zu implementieren.

### Typische Anti-Muster:

- Sie erlauben eine Vielzahl von Technologien, was sich auf den Verwaltungsaufwand Ihres Unternehmens auswirken kann.

Vorteile der Nutzung dieser bewährten Methode: Durch Festlegung einer Richtlinie für die Architektur-, Technologie und Anbietersauswahl können Entscheidungen schnell getroffen werden.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Mittel

### Implementierungsleitfaden

Interne Richtlinien bei der Auswahl von Ressourcen und Architektur bieten Standards und Leitlinien, die bei Architekturentscheidungen zu beachten sind. Diese Richtlinien vereinfachen den Entscheidungsprozess bei der Auswahl des richtigen Cloud-Service und können zur Verbesserung der Leistungseffizienz beitragen. Stellen Sie die Workload mithilfe von Richtlinien oder Referenzarchitekturen bereit. Integrieren Sie die Services in Ihre Cloud-Bereitstellung. Überprüfen Sie anschließend anhand von Leistungstests, dass Sie die eigenen Leistungsanforderungen weiterhin erfüllen können.

### Implementierungsschritte

- Verstehen Sie die Anforderungen der Cloud-Workload genau.
- Überprüfen Sie die internen und externen Richtlinien, um die relevantesten zu ermitteln.
- Verwenden Sie die entsprechenden Referenzarchitekturen, die von AWS bereitgestellt werden, oder die branchenweit anerkannten bewährten Methoden.
- Schaffen Sie ein Kontinuum, das aus Richtlinien, Standards, Referenzarchitekturen und präskriptiven Richtlinien für häufig auftretende Situationen besteht. Auf diese Weise können Ihre Teams schneller vorankommen. Passen Sie die Komponenten gegebenenfalls an die Branche an.

- Prüfen Sie diese Richtlinien und Referenzarchitekturen für die Workload in Sandbox-Umgebungen.
- Halten Sie up-to-date sich an Industriestandards und AWS Updates, um sicherzustellen, dass Ihre Richtlinien und Referenzarchitekturen zur Optimierung Ihrer Cloud-Workloads beitragen.

## Ressourcen

### Zugehörige Dokumente:

- [AWS -Architekturzentrum](#)
- [AWS Partner Network](#)
- [AWS -Lösungsbibliothek](#)
- [AWS Knowledge Center](#)
- [AWS Architektur-Blog](#)

### Zugehörige Videos:

- [This is my Architecture](#)
- [AWS re:Invent 2022 — Steigern Sie den Wert Ihres Unternehmens mit SAP Referenzarchitektur AWS](#)

### Zugehörige Beispiele:

- [AWS Beispiele](#)
- [AWS SDKBeispiele](#)

PERF01-BP06 Nutzen Sie Benchmarking, um Architekturentscheidungen zu treffen

Führen Sie einen Benchmark-Vergleich für eine vorhandene Workload durch, um sich ein Bild über deren Leistung in der Cloud zu verschaffen, und treffen Sie architektonische Entscheidungen auf der Grundlage dieser Daten.

### Typische Anti-Muster:

- Sie verlassen sich auf gängige Benchmarks, die für die Workload-Merkmale nicht aufschlussreich sind.
- Sie verlassen sich auf Kundenfeedback und Kundenwahrnehmung als einzige Benchmark.



Vorteile der Einführung dieser bewährten Methode: Durch Benchmarking Ihrer aktuellen Implementierung können Sie Leistungsverbesserungen messen.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Mittel

### Implementierungsleitfaden

Kombinieren Sie Benchmarking mit synthetischen Tests, um die Leistung Ihrer Workload-Komponenten zu bewerten. Benchmarking lässt sich in der Regel schneller als Lasttests einrichten und dient zur Bewertung der Technologie einer bestimmten Komponente. Ein Benchmarking wird oft zu Beginn eines neuen Projekts durchgeführt, wenn Sie noch keine vollständige Lösung für einen Lasttest haben.

Sie können entweder Ihre eigenen benutzerdefinierten Benchmark-Tests erstellen oder einen Industriestandardtest wie [TPC-DS verwenden, um Ihre Workloads](#) zu bewerten. Branchen-Benchmarks sind zum Vergleich von Umgebungen nützlich. Benutzerdefinierte Benchmarks eignen sich zum Prüfen spezieller Arten von Vorgängen, die Sie in der Architektur ausführen möchten.

Beim Benchmarking ist es wichtig, die Testumgebung entsprechend vorzubereiten, um aussagekräftige Ergebnisse zu erzielen. Führen Sie denselben Benchmark-Test mehrmals aus, um sicherzustellen, dass alle Varianzen im Laufe der Zeit ermittelt wurden.

Da sich Benchmarks in der Regel schneller als Lasttests ausführen lassen, können Sie früher in der Bereitstellungs pipeline eingesetzt werden und schneller Feedback zu Leistungsabweichungen liefern. Wenn Sie eine wesentliche Veränderung einer Komponente oder eines Services bewerten, können Sie schnell ermitteln, ob der Aufwand für die Korrektur gerechtfertigt ist. Die Verwendung von Benchmarking in Verbindung mit Lasttests ist wichtig, da letztere Auskunft über die Leistung der Workload in der Produktion geben.

### Implementierungsschritte

- Planen und Definieren:
  - Definieren Sie die Ziele, den Ausgangswert, die Testszenarien, die Metriken (wie CPU Auslastung, Latenz oder Durchsatz) und KPIs für Ihren Benchmark.
  - Konzentrieren Sie sich auf die Benutzeranforderungen in Bezug auf das Benutzererlebnis und Faktoren wie Reaktionszeit und Barrierefreiheit.
  - Identifizieren Sie ein Benchmarking-Tool, das für Ihre Workload geeignet ist. Sie können AWS Dienste wie [Amazon CloudWatch](#) oder ein Drittanbieter-Tool verwenden, das mit Ihrem Workload kompatibel ist.

- **Konfiguration und Verwendung:**
  - Richten Sie Ihre Umgebung ein und konfigurieren Sie Ihre Ressourcen.
  - Implementieren Sie Überwachungs- und Protokollierungsfunktionen, um Testergebnisse zu erfassen.
- **Benchmarking und Überwachung:**
  - Führen Sie die Benchmark-Tests durch und überwachen Sie die Metriken während des Tests.
- **Analyse und Dokumentation:**
  - Dokumentieren Sie Ihren Benchmarking-Prozess und die entsprechenden Erkenntnisse.
  - Analysieren Sie die Ergebnisse, um Engpässe, Trends und Verbesserungsmöglichkeiten zu identifizieren.
  - Verwenden Sie die Testergebnisse, um die Architektur betreffende Entscheidungen zu fällen und die Workload anzupassen. Dies kann die Änderung von Services oder die Einführung neuer Features beinhalten.
- **Optimierung und Wiederholung:**
  - Passen Sie die Ressourcenkonfigurationen und -zuweisungen auf der Grundlage Ihrer Benchmarks an.
  - Testen Sie Ihre Workload nach der Anpassung erneut, um Ihre Verbesserungen zu überprüfen.
  - Dokumentieren Sie Ihre Erkenntnisse und wiederholen Sie den Prozess, um weitere Verbesserungsmöglichkeiten zu identifizieren.

## Ressourcen

### Zugehörige Dokumente:

- [AWS Architekturzentrum](#)
- [AWS Partner Network](#)
- [AWS Lösungsbibliothek](#)
- [AWS Wissenszentrum](#)
- [Amazon CloudWatch RUM](#)
- [Amazon CloudWatch Synthetics](#)
- [Genomics workflows, Part 5: automated benchmarking](#)
- [Benchmarking und Optimierung der Endgerätebereitstellung in Amazon SageMaker JumpStart](#)

## Zugehörige Videos:

- [AWS re:Invent 2023 — Benchmarking AWS Lambda von Kaltstarts](#)
- [Benchmarking stateful services in the cloud](#)
- [This is my Architecture](#)
- [Optimieren Sie Anwendungen über Amazon CloudWatch RUM](#)
- [Demo von Amazon CloudWatch Synthetics](#)

## Zugehörige Beispiele:

- [AWS Beispiele](#)
- [AWS SDKBeispiele](#)
- [Verteilte Lasttests](#)
- [Messen Sie die Seitenladezeit mit Amazon CloudWatch Synthetics](#)
- [CloudWatch RUMAmazon-Webclient](#)

PERF01-BP07 Verwenden Sie einen datengesteuerten Ansatz für architektonische Entscheidungen

Definieren Sie einen klaren, datengesteuerten Ansatz für architektonische Entscheidungen, um sicherzustellen, dass die richtigen Cloud-Services und -Konfigurationen verwendet werden, um Ihre spezifischen Geschäftsanforderungen zu erfüllen.

## Typische Anti-Muster:

- Sie gehen davon aus, dass die aktuelle Architektur statisch ist und im Laufe der Zeit nicht aktualisiert werden sollte.
- Ihre architektonischen Entscheidungen basieren auf Vermutungen und Annahmen.
- Sie führen im Laufe der Zeit Änderungen an der Architektur ein, ohne sie zu begründen.

Vorteile der Nutzung dieser bewährten Methode: Durch einen klar definierten Ansatz für architektonische Entscheidungen verwenden Sie Daten, um das Workload-Design zu beeinflussen und im Laufe der Zeit fundierte Entscheidungen zu treffen.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Mittel

## Implementierungsleitfaden

Nutzen Sie interne Erfahrungen und Kenntnisse im Zusammenhang mit der Cloud oder ziehen Sie externe Ressourcen heran, wie etwa veröffentlichte Anwendungsbeispiele oder Whitepapers, um Ressourcen und Services in der Architektur auszuwählen. Sie sollten über einen klar definierten Prozess verfügen, der das Experimentieren und Benchmarking mit den Services fördert, die in der Workload verwendet werden könnten.

Backlogs für kritische Workloads sollten nicht nur aus Benutzerszenarien bestehen, die für das Unternehmen und die Benutzer relevante Funktionen bereitstellen, sondern auch aus technischen Szenarien, die ein architektonisches System für die Workload bilden. Dieses System stützt sich auf neue technologische Fortschritte sowie neue Services und nimmt diese auf der Grundlage von Daten und entsprechender Begründung an. Dies stellt sicher, dass die Architektur zukunftssicher bleibt und nicht stagniert.

## Implementierungsschritte

- Arbeiten Sie mit wichtigen Stakeholdern zusammen, um die Workload-Anforderungen zu definieren, einschließlich Überlegungen zu Leistung, Verfügbarkeit und Kosten. Berücksichtigen Sie Faktoren wie die Anzahl der Benutzer und das Nutzungsmuster für die Workload.
- Erstellen Sie ein Architektursystem oder einen Technologie-Backlog, der zusammen mit dem funktionalen Backlog priorisiert wird.
- Bewerten und beurteilen Sie verschiedene Cloud-Services (weitere Informationen finden Sie unter [PERF01-BP01 Erfahren Sie mehr über verfügbare Cloud-Dienste und -Funktionen und verstehen Sie sie](#)).
- Erkunden Sie verschiedene Architekturmuster wie Microservices oder Serverless, die Ihren Leistungsanforderungen entsprechen (weitere Informationen finden Sie unter [PERF01-BP02 Lassen Sie sich von Ihrem Cloud-Anbieter oder einem geeigneten Partner beraten, um mehr über Architekturmuster und Best Practices zu erfahren](#)).
- Wenden Sie sich an andere Teams, Architekturdiagramme und Ressourcen wie AWS Solution Architects, [AWS Architecture Center](#) usw. [AWS Partner Network](#), um Ihnen bei der Auswahl der richtigen Architektur für Ihren Workload zu helfen.
- Definieren Sie Leistungsmetriken wie Durchsatz und Reaktionszeit, anhand derer Sie die Leistung der Workload bewerten können.

- Experimentieren Sie und verwenden Sie definierte Metriken, um die Leistung der ausgewählten Architektur zu validieren.
- Überwachen Sie kontinuierlich und nehmen Sie bei Bedarf Anpassungen vor, um die optimale Leistung der Architektur aufrechtzuerhalten.
- Dokumentieren Sie Ihre gewählte Architektur und Entscheidungen als Referenz für zukünftige Updates und Erkenntnisse.
- Überprüfen und aktualisieren Sie den Ansatz zur Architekturauswahl kontinuierlich auf der Grundlage von Erkenntnissen, neuen Technologien und Metriken, die auf eine notwendige Änderung oder ein Problem im aktuellen Ansatz hinweisen.

## Ressourcen

### Zugehörige Dokumente:

- [AWS -Lösungsbibliothek](#)
- [AWS Knowledge Center](#)
- [Architekturmuster, auf denen End-to-End datengesteuerte Anwendungen aufgebaut werden können AWS](#)

### Zugehörige Videos:

- [This is my Architecture](#)
- [AWS re:Invent 2021 — Datengesteuertes Unternehmen: Von der Vision zum Mehrwert](#)
- [AWS re:Invent 2022 — Bereitstellung nachhaltiger, leistungsstarker Architekturen](#)
- [AWS re:Invent 2023 — Optimieren Sie Kosten und Leistung und verfolgen Sie die Fortschritte bei der Eindämmung](#)
- [AWS re:Invent 2022 — AWS Optimierung: Umsetzbare Schritte für sofortige Ergebnisse](#)

### Zugehörige Beispiele:

- [AWS Beispiele](#)
- [AWS SDKBeispiele](#)

# Computer und Hardware

## Fragen

- [PERF2. Wie wählen und nutzen Sie Computing-Ressourcen für Ihre Workload?](#)

## PERF2. Wie wählen und nutzen Sie Computing-Ressourcen für Ihre Workload?

Die optimale Datenverarbeitungsoption für eine bestimmte Workload kann sich je nach Anwendungsdesign, Nutzungsmustern und Konfigurationseinstellungen unterscheiden. Architekturen können verschiedene Datenverarbeitungsoptionen für verschiedene Komponenten verwenden und verschiedene Funktionen zur Verbesserung der Leistung bieten. Die Wahl der falschen Datenverarbeitungslösung für eine Architektur kann die Leistungseffizienz schmälern.

## Bewährte Methoden

- [PERF02-BP01 Wählen Sie die besten Rechenoptionen für Ihren Workload](#)
- [PERF02-BP02 Verstehen Sie die verfügbare Rechenkonfiguration und die verfügbaren Funktionen](#)
- [PERF02-BP03 Erfassung rechnerbezogener Metriken](#)
- [PERF02-BP04 Rechenressourcen konfigurieren und dimensionieren](#)
- [PERF02-BP05 Skalieren Sie Ihre Rechenressourcen dynamisch](#)
- [PERF02-BP06 Verwenden Sie optimierte hardwarebasierte Rechenbeschleuniger](#)

## PERF02-BP01 Wählen Sie die besten Rechenoptionen für Ihren Workload

Wenn Sie die für die Workload am besten geeignete Datenverarbeitungsoption auswählen, können Sie die Leistung verbessern, unnötige Infrastrukturkosten reduzieren und den Betriebsaufwand für die Aufrechterhaltung der Workload senken.

## Typische Anti-Muster:

- Sie verwenden dieselbe Datenverarbeitungsoption, die On-Premises verwendet wurde.
- Ihnen fehlt es an Bewusstsein für Cloud-Datenverarbeitungsoptionen, -Features und -lösungen und wie diese Lösungen die Datenverarbeitungsleistung verbessern können.
- Sie stellen eine bestehende Datenverarbeitungsoption zu viel bereit, um Skalierungs- oder Leistungsanforderungen zu erfüllen, wenn eine alternative Datenverarbeitungsoption den Workload-Merkmalen besser entsprechen würde.

Vorteile der Nutzung dieser bewährten Methode: Durch die Ermittlung der Anforderungen an die Datenverarbeitung und deren Bewertung anhand der verfügbaren Optionen können Sie die Workload ressourceneffizienter gestalten.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Hoch

### Implementierungsleitfaden

Um Ihre Cloud-Workloads im Hinblick auf Leistungseffizienz zu optimieren, ist es wichtig, die für Ihren Anwendungsfall und Ihre Leistungsanforderungen am besten geeigneten Rechenoptionen auszuwählen. AWS bietet eine Vielzahl von Rechenoptionen, die auf unterschiedliche Workloads in der Cloud zugeschnitten sind. Sie können [Amazon](#) beispielsweise verwenden, EC2 um virtuelle Server zu starten und [AWS Lambda](#) dazu zu verwalten, Code auszuführen, ohne Server bereitstellen oder verwalten zu müssen, [Amazon ECS](#) oder [Amazon](#), EKS um Container auszuführen und zu verwalten oder [AWS Batch](#) um große Datenmengen parallel zu verarbeiten. Basierend auf Ihren Skalierungs- und Datenverarbeitungsanforderungen sollten Sie die optimale Datenverarbeitungslösung für Ihre Situation auswählen und konfigurieren. Sie können auch erwägen, mehrere Arten von Datenverarbeitungslösungen in einer einzigen Workload zu verwenden, da jede ihre eigenen Vor- und Nachteile hat.

Die folgenden Schritte führen Sie durch die Auswahl der richtigen Datenverarbeitungsoptionen, die Ihren Workload-Eigenschaften und Leistungsanforderungen entsprechen.

### Implementierungsschritte

- Verstehen Sie Ihre Workload-Datenverarbeitungsanforderungen. Die zu berücksichtigenden wesentlichen Anforderungen umfassen Anforderungen an Datenverarbeitung, Datenverkehrsmuster, Datenzugriffsmuster, Skalierung und Latenz.
- Erfahren Sie mehr über verschiedene [AWS -Datenverarbeitungsservices](#) für Ihre Workload. Weitere Informationen finden Sie unter [PERF01-BP01 Erfahren Sie mehr über verfügbare Cloud-Dienste und -Funktionen und verstehen Sie sie](#). Hier finden Sie einige wichtige AWS - Datenverarbeitungsoptionen, ihre Eigenschaften und gängige Anwendungsfälle:

AWS Service	Schlüsselmerkmale	Häufige Anwendungsfälle
<a href="#">Amazon Elastic Compute Cloud (AmazonEC2)</a>	Verfügt über eine spezielle Option für Hardware, Lizenzanforderungen, eine große Auswahl an	Lift-and-Shift-Migrationen, monolithische Anwendung, hybride Umgebungen, Enterprise-Anwendungen

AWS Service	Schlüsselmerkmale	Häufige Anwendungsfälle
	verschiedenen Instance-Familien, Prozessortypen und Beschleuniger der Datenverarbeitung	
<a href="#">Amazon Elastic Container Service (AmazonECS)</a> , <a href="#">Amazon Elastic Kubernetes Service (Amazon) EKS</a>	Einfache Bereitstellung, konsistente Umgebungen, skalierbar	Microservices, Hybrid-Umgebungen
<a href="#">AWS Lambda</a>	<a href="#">Serverless-Datenverarbeitungsservice</a> , der Code als Reaktion auf Ereignisse ausführt und die zugrunde liegenden Ressourcen für die Datenverarbeitung automatisch verwaltet.	Microservices, ereignisgesteuerte Anwendungen
<a href="#">AWS Batch</a>	Effiziente und dynamische Bereitstellung und Skalierung von <a href="#">Amazon Elastic Container Service (AmazonECS)</a> , <a href="#">Amazon Elastic Kubernetes Service (AmazonEKS)</a> und <a href="#">AWS Fargate</a> Rechenressourcen mit der Option, On-Demand- oder Spot-Instances je nach Ihren Jobanforderungen zu verwenden	HPC, trainieren Sie ML-Modelle
<a href="#">Amazon Lightsail</a>	Vorkonfigurierte Linux- und Windows-Anwendung für die Ausführung kleiner Workloads	Einfache Webanwendungen, benutzerdefinierte Website



- Bewerten Sie die Kosten (wie stündliche Gebühr oder Datenübertragung) und den Verwaltungsaufwand (wie Patching und Skalierung), die mit jeder Datenverarbeitungsoption verbunden sind.
- Führen Sie Experimente und Benchmarking in einer Nicht-Produktionsumgebung durch, um herauszufinden, welche Datenverarbeitungsoption Ihre Workload-Anforderungen am besten erfüllt.
- Nachdem Sie experimentiert und die neue Datenverarbeitungslösung ermittelt haben, planen Sie die Migration und überprüfen Sie die Leistungsmetriken.
- Verwenden Sie AWS Überwachungstools wie [Amazon CloudWatch](#) und Optimierungsdienste [AWS Compute Optimizer](#), um Ihre Rechenressourcen kontinuierlich auf der Grundlage realer Nutzungsmuster zu optimieren.

## Ressourcen

### Zugehörige Dokumente:

- [Cloud Computing mit AWS](#)
- [EC2Amazon-Instance-Typen](#)
- [EKSAmazon-Container: EKS Amazon-Worker-Knoten](#)
- [ECSAmazon-Container: ECS Amazon-Container-Instances](#)
- [Funktionen: Lambda-Funktionskonfiguration](#)
- [Prescriptive Guidance for Containers](#)
- [Prescriptive Guidance for Serverless](#)

### Zugehörige Videos:

- [AWS re:Invent 2023 — AWS Graviton: Das beste Preis-Leistungs-Verhältnis für Ihre Workloads](#)  
[AWS](#)
- [AWS re:Invent 2023 — Neue generative KI-Funktionen von Amazon Elastic Compute Cloud in](#)  
[AMS](#)
- [AWS re:Invent 2023 – What’s new with Amazon Elastic Compute Cloud](#)
- [AWS re:Invent 2023 – Smart savings: Amazon Elastic Compute Cloud cost-optimization strategies](#)
- [AWS re:Invent 2021 – Powering next-gen Amazon Elastic Compute Cloud: Deep dive on the Nitro](#)  
[System](#)

- [AWS re:Invent 2019 — Optimieren Sie die Leistung und die Kosten Ihrer Rechenleistung AWS](#)
- [AWS re:Invent 2.019 – Amazon Elastic Compute Cloud foundations](#)
- [AWS re:Invent 2022 — Implementieren Sie ML-Modelle für Inferenz mit hoher Leistung und niedrigen Kosten](#)
- [AWS re:Invent 2019 — Optimieren Sie die Leistung und die Kosten Ihrer Rechenleistung AWS](#)
- [EC2Amazon-Stiftungen](#)
- [Stellen Sie ML-Modelle für Inference mit hoher Leistung und niedrigen Kosten bereit](#)

Zugehörige Beispiele:

- [Migration der Webanwendung zu Containern](#)
- [Ausführen eines Serverless-„Hello World“](#)
- [EKSAmazon-Werkstatt](#)
- [EC2Amazon-Werkstatt](#)
- [Effiziente und belastbare Workloads mit Amazon Elastic Compute Cloud Auto Scaling](#)
- [Migration zu AWS Graviton mit Container Services](#)

PERF02-BP02 Verstehen Sie die verfügbare Rechenkonfiguration und die verfügbaren Funktionen

Informieren Sie sich über die verfügbaren Konfigurationsoptionen und Features für den Datenverarbeitungsservice, damit Sie die richtige Menge an Ressourcen bereitstellen und die Leistungseffizienz verbessern können.

Typische Anti-Muster:

- Sie bewerten keine Datenverarbeitungsoptionen oder verfügbaren Instance-Familien anhand der Workload-Merkmale.
- Sie stellen zu viele Datenverarbeitungsressourcen bereit, um Anforderungen von Nachfragespitzen zu erfüllen.

Vorteile der Einführung dieser bewährten Methode: Machen Sie sich mit den AWS Rechenfunktionen und -konfigurationen vertraut, sodass Sie eine Rechenlösung verwenden können, die für Ihre Workload-Merkmale und -anforderungen optimiert ist.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Mittel

## Implementierungsleitfaden

Jede Datenverarbeitungslösung verfügt über einzigartige Konfigurationen und Features, um unterschiedliche Workload-Merkmale und -Anforderungen zu unterstützen. Erfahren Sie, wie diese Optionen die Workload ergänzen, und finden Sie heraus, welche Konfigurationsoptionen am besten für Ihre Anwendung geeignet sind. Beispiele für diese Optionen sind Instanzfamilie, Größen, Funktionen (, I/O)GPU, Bursting, Timeouts, Funktionsgrößen, Container-Instances und Parallelität. Wenn Ihr Workload seit mehr als vier Wochen dieselbe Rechenoption verwendet und Sie davon ausgehen, dass die Eigenschaften auch in future gleich bleiben werden, können Sie anhand [AWS Compute Optimizer](#) dieser Methode herausfinden, ob Ihre aktuelle Rechenoption aus CPU Sicht des Speichers für die Workloads geeignet ist.

### Implementierungsschritte

- Machen Sie sich mit den Workload-Anforderungen (wie CPU Bedarf, Arbeitsspeicher und Latenz) vertraut.
- Lesen Sie die AWS Dokumentation und Best Practices, um mehr über empfohlene Konfigurationsoptionen zu erfahren, die zur Verbesserung der Rechenleistung beitragen können. Hier finden Sie einige wichtige Konfigurationsoptionen, die Sie in Betracht ziehen sollten:

Konfigurationsoption	Beispiele
Instance-Typ	<ul style="list-style-type: none"> <li>• <a href="#">Rechenoptimierte</a> Instances eignen sich ideal für Workloads, die ein hohes Verhältnis von V CPU zu Arbeitsspeicher erfordern.</li> <li>• <a href="#">Arbeitsspeicheroptimierte</a> Instances bieten große Mengen an Arbeitsspeicher, um arbeitsspeicherintensive Workloads zu unterstützen.</li> <li>• <a href="#">Speicheroptimierte</a> Instances sind für Workloads konzipiert, die einen hohen sequentiellen Lese- und Schreibzugriff () auf lokalen Speicher erfordern. IOPS</li> </ul>
Preismodell	<ul style="list-style-type: none"> <li>• Mit <a href="#">On-Demand-Instances</a> können Sie die Datenverarbeitungskapazität nach Sekunde oder Stunde ohne langfristige Verpflichtung</li> </ul>

Konfigurationsoption	Beispiele
	<p>tungen verwenden. Diese Instances eignen sich für Bursting über die Leistungsbasis hinaus.</p> <ul style="list-style-type: none"> <li>• <a href="#">Savings Plans</a> bieten erhebliche Einsparungen gegenüber On-Demand-Instances im Austausch gegen die Verpflichtung, eine bestimmte Menge an Rechenleistung für einen Zeitraum von ein oder drei Jahren zu nutzen.</li> <li>• <a href="#">Spot Instances</a> ermöglichen es Ihnen, ungenutzte Instance-Kapazitäten mit einem Rabatt für Ihre zustandslosen, fehlertoleranten Workloads zu nutzen.</li> </ul>
Auto Scaling	Nutzen Sie die <a href="#">Auto-Scaling</a> -Konfiguration zur Anpassung der Datenverarbeitungsressourcen an die Datenverkehrsmuster.
Dimensionierung	<ul style="list-style-type: none"> <li>• Nutzen Sie <a href="#">Compute Optimizer</a> zum Erhalt von Machine-Learning-gestützten Empfehlungen dazu, welche Datenverarbeitungskonfiguration am besten Ihren Datenverarbeitungsmerkmalen entspricht.</li> <li>• Mit <a href="#">AWS Lambda Power Tuning</a> können Sie die beste Konfiguration für Ihre Lambda-Funktion auswählen.</li> </ul>
Hardwarebasierte Computing-Beschleuniger	<ul style="list-style-type: none"> <li>• <a href="#">Beschleunigte Recheninstanzen</a> führen Funktionen wie Grafikverarbeitung oder Datenmusterabgleich effizienter aus als basierte Alternativen. CPU</li> <li>• <a href="#">Nutzen Sie für Machine-Learning-Workloads speziell für Ihre Arbeitslast entwickelte Hardware wie AWS Trainium, Inferentia und Amazon AWS EC2 DL1</a></li> </ul>

## Ressourcen

### Zugehörige Dokumente:

- [Cloud Computing mit AWS](#)
- [EC2Amazon-Instance-Typen](#)
- [Kontrolle des Prozessorstatus für Ihre EC2 Amazon-Instance](#)
- [EKSAamazon-Container: EKS Amazon-Worker-Knoten](#)
- [ECSAmazon-Container: ECS Amazon-Container-Instances](#)
- [Funktionen: Lambda-Funktionskonfiguration](#)

### Zugehörige Videos:

- [AWS re:Invent 2023 — AWS Graviton: Das beste Preis-Leistungs-Verhältnis für Ihre Workloads AWS](#)
- [AWS re:Invent 2023 — Neue EC2 generative KI-Funktionen von Amazon in AWS Management Console](#)
- [AWS re:Invent 2023 — Was ist neu bei Amazon EC2](#)
- [AWS re:Invent 2023 — Intelligentes Sparen: Strategien zur Kostenoptimierung von Amazon EC2](#)
- [AWS re:Invent 2021 — Unterstützung für Amazon der nächsten Generation EC2: Tiefer Einblick in das Nitro-System](#)
- [AWS re:Invent 2019 — Amazon-Stiftungen EC2](#)
- [AWS re:Invent 2022 — Optimierung von Amazon im Hinblick EKS auf Leistung und Kosten bei AWS](#)

### Zugehörige Beispiele:

- [Demo-Code für Compute Optimizer](#)
- [Workshop zu Amazon EC2 Spot-Instances](#)
- [Effiziente und belastbare Workloads mit Amazon EC2 AWS Auto Scaling](#)
- [Workshop für Graviton-Entwickler](#)
- [AWS für Microsoft Workloads Immersion Day](#)
- [AWS für den Immersionstag mit Linux-Workloads](#)
- [AWS Compute Optimizer Demo-Code](#)

- [EKSA Amazon-Werkstatt](#)

## PERF02-BP03 Erfassung rechnerbezogener Metriken

Erfassen und verfolgen Sie Datenverarbeitungsmetriken, um die Leistung der Rechenressourcen besser zu verstehen und deren Leistung und Auslastung zu verbessern.

Typische Anti-Muster:

- Sie suchen ausschließlich manuell mithilfe von Protokolldateien nach Metriken.
- Sie verwenden nur die Standardmetriken, die von der Überwachungssoftware aufgezeichnet wurden.
- Sie überprüfen Metriken nur dann, wenn ein Problem vorliegt.

Vorteile der Nutzung dieser bewährten Methode: Die Erfassung von Leistungsmetriken hilft Ihnen dabei, die Anwendungsleistung an den Geschäftsanforderungen auszurichten, um sicherzustellen, dass Sie Ihre Workload-Anforderungen erfüllen. Es kann Ihnen auch dabei helfen, die Ressourcenleistung und -nutzung in der Workload kontinuierlich zu verbessern.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Hoch

### Implementierungsleitfaden

Cloud-Workloads können große Mengen an Daten generieren, wie Metriken, Protokolle und Ereignisse. In der AWS Cloud ist das Sammeln von Metriken ein entscheidender Schritt zur Verbesserung von Sicherheit, Kosteneffizienz, Leistung und Nachhaltigkeit. AWS bietet eine breite Palette leistungsbezogener Kennzahlen mithilfe von Überwachungsdiensten wie [Amazon](#), CloudWatch um Ihnen wertvolle Einblicke zu bieten. Metriken wie CPU Auslastung, Speicherauslastung, Festplatten-I/O sowie eingehende und ausgehende Netzwerkdaten können Aufschluss über Auslastungsgrade oder Leistungsengpässe geben. Nutzen Sie diese Metriken im Rahmen eines datengestützten Ansatzes, der Ihnen die aktive Feinabstimmung und Optimierung der von der Workload genutzten Ressourcen ermöglicht. Im Idealfall sollten Sie alle Metriken zu Ihren Datenverarbeitungsressourcen auf einer einzigen Plattform erfassen und Aufbewahrungsrichtlinien implementieren, um Kosten- und Betriebsziele zu unterstützen.

## Implementierungsschritte

- Identifizieren Sie, welche Leistungsmetriken für Ihre Workload relevant sind. Sie sollten Metriken zur Ressourcennutzung und zum Betrieb der Cloud-Workload (wie Reaktionszeit und Durchsatz) erfassen.
  - [EC2Amazon-Standardmetriken](#)
  - [ECSAmazon-Standardmetriken](#)
  - [EKSAmazon-Standardmetriken](#)
  - [Lambda-Standardmetriken](#)
  - [EC2Speicher- und Festplattenmetriken von Amazon](#)
- Wählen Sie die richtige Protokollierungs- und Überwachungslösung für Ihre Workload aus und richten Sie sie ein.
  - [AWS -native Beobachtbarkeit](#)
  - [AWS Distribution für OpenTelemetry](#)
  - [Amazon Managed Service for Prometheus](#)
- Definieren Sie den erforderlichen Filter und die erforderliche Aggregation für die Metriken auf der Grundlage Ihrer Workload-Anforderungen.
  - [Quantifizieren Sie benutzerdefinierte Anwendungsmetriken mit Amazon CloudWatch Logs und Metrikfiltern](#)
  - [Sammeln Sie benutzerdefinierte Metriken mit CloudWatch strategischem Tagging von Amazon](#)
- Konfigurieren Sie Richtlinien zur Datenaufbewahrung für Ihre Metriken so, dass sie Ihren Sicherheits- und Betriebszielen entsprechen.
  - [Standardmäßige Datenspeicherung für Metriken CloudWatch](#)
  - [Standardmäßige Datenspeicherung für CloudWatch Protokolle](#)
- Erstellen Sie bei Bedarf Alarme und Benachrichtigungen für Ihre Metriken, damit Sie proaktiv auf leistungsbezogene Probleme reagieren können.
  - [Erstellen Sie mithilfe der CloudWatch Amazon-Anomalieerkennung Alarme für benutzerdefinierte Metriken](#)
  - [Erstellen Sie mit Amazon Metriken und Alarme für bestimmte Webseiten CloudWatch RUM](#)
- Verwenden Sie die Automatisierung, um die Kundendienstmitarbeiter für die Metrik- und Protokollaggregation einzusetzen.
  - [AWS Systems Manager Automatisierung](#)
  - [OpenTelemetrySammler](#)

## Ressourcen

### Zugehörige Dokumente:

- [Überwachung und Beobachtbarkeit](#)
- [Bewährte Methoden: Implementierung von Observability mit AWS](#)
- [CloudWatch Amazon-Dokumentation](#)
- [Erfassen Sie mit dem Agenten Metriken und Protokolle von EC2 Amazon-Instances und lokalen Servern CloudWatch](#)
- [Zugreifen auf Amazon CloudWatch Logs für AWS Lambda](#)
- [CloudWatch Logs mit Container-Instances verwenden](#)
- [Veröffentlichen von benutzerdefinierten Metriken](#)
- [AWS Answers: Zentralisierte Protokollierung](#)
- [AWS Dienste, die CloudWatch Metriken veröffentlichen](#)
- [Überwachung von Amazon EKS am AWS Fargate](#)

### Zugehörige Videos:

- [AWS re:Invent 2023 — \[LAUNCH\] Anwendungsüberwachung für moderne Workloads](#)
- [AWS re:Invent 2023 — Implementierung der Anwendungsbeobachtbarkeit](#)
- [AWS re:Invent 2023 — Aufbau einer effektiven Strategie für Beobachtbarkeit](#)
- [AWS re:Invent 2023 — Nahtlose Beobachtbarkeit mit Distro für AWS OpenTelemetry](#)
- [Leistungsmanagement für Anwendungen aktiviert AWS](#)

### Zugehörige Beispiele:

- [AWS Immersion Day für Linux-Workloads — Amazon CloudWatch](#)
- [Überwachung von ECS Amazon-Clustern und Containern](#)
- [Überwachung mit CloudWatch Amazon-Dashboards](#)
- [EKSAmazon-Werkstatt](#)



## PERF02-BP04 Rechenressourcen konfigurieren und dimensionieren

Konfigurieren und passen Sie die Größe der Datenverarbeitungsressourcen so an, dass sie den Leistungsanforderungen der Workloads entsprechen, und vermeiden Sie zu wenig oder zu stark ausgelastete Ressourcen.

Typische Anti-Muster:

- Sie ignorieren Ihre Workload-Leistungsanforderungen, was zu über- oder unterdimensionierten Datenverarbeitungsressourcen führt.
- Sie wählen nur die größte oder kleinste verfügbare Instance für alle Workloads aus.
- Sie verwenden nur eine Instance-Familie, um die Verwaltung zu vereinfachen.
- Sie ignorieren Empfehlungen von AWS Cost Explorer Compute Optimizer zur richtigen Dimensionierung.
- Sie bewerten die Workload nicht erneut auf die Eignung neuer Instance-Typen.
- Sie zertifizieren nur eine kleine Anzahl von Instance-Konfigurationen für Ihre Organisation.

Vorteile der Nutzung dieser bewährten Methode: Die richtige Dimensionierung der Datenverarbeitungsressourcen gewährleistet einen optimalen Betrieb in der Cloud, indem eine Über- und Unterdimensionierung von Ressourcen vermieden wird. Die richtige Dimensionierung der Datenverarbeitungsressourcen führt in der Regel zu einer besseren Leistung und einem besseren Kundenerlebnis bei gleichzeitiger Senkung der Kosten.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Mittel

### Implementierungsleitfaden

Die richtige Dimensionierung ermöglicht es Organisationen, ihre Cloud-Infrastruktur effizient und kostengünstig zu betreiben und gleichzeitig ihre Geschäftsanforderungen zu erfüllen. Eine übermäßige Bereitstellung von Cloud-Ressourcen kann zu zusätzlichen Kosten führen, während eine unzureichende Bereitstellung zu schlechter Leistung und einem negativen Kundenerlebnis führen kann. AWS bietet Tools wie [AWS Compute Optimizer](#) und [AWS Trusted Advisor](#) die Nutzung historischer Daten, um Empfehlungen zur richtigen Größe Ihrer Rechenressourcen zu geben.

### Implementierungsschritte

- Wählen Sie einen Instance-Typ, der am besten zu Ihren Anforderungen passt:

- [Wie wähle ich den passenden EC2 Amazon-Instance-Typ für meinen Workload aus?](#)
- [Attributbasierte Instance-Typauswahl für Amazon Fleet EC2](#)
- [Erstellen einer Auto-Scaling-Gruppe mit attributbasierter Auswahl des Instance-Typs](#)
- [Optimieren Ihrer Kubernetes-Datenverarbeitungskosten mit der Karpenter-Konsolidierung](#)
- Analysieren Sie die verschiedenen Leistungsmerkmale Ihres Workloads und wie sich diese Merkmale auf Speicher, Netzwerk und Nutzung auswirken. CPU Wählen Sie anhand dieser Daten die für das Profil und die Leistungsziele der Workloads am besten geeigneten Ressourcen aus.
- Überwachen Sie Ihren Ressourcenverbrauch mithilfe von AWS Überwachungstools wie Amazon CloudWatch.
- Wählen Sie die richtige Konfiguration für die Datenverarbeitungsressource aus.
  - Bei kurzlebigen Workloads sollten Sie die [CloudWatch Amazon-Instance-Kennzahlen](#) auswerten, CPUUtilization um festzustellen, ob die Instance zu wenig oder zu stark ausgelastet ist.
  - Für stabile Workloads sollten Sie sich in regelmäßigen Abständen die Tools zur AWS richtigen Dimensionierung ansehen, um Möglichkeiten zur AWS Trusted Advisor Optimierung AWS Compute Optimizer und zur richtigen Größe der Rechenressource zu ermitteln.
- Testen Sie Konfigurationsänderungen in einer Nicht-Produktionsumgebung, bevor Sie sie in einer Live-Umgebung implementieren.
- Bewerten Sie neue Datenverarbeitungsangebote und vergleichen Sie sie mit den Anforderungen Ihrer Workload.

## Ressourcen

### Zugehörige Dokumente:

- [Cloud-Computing mit AWS](#)
- [EC2Amazon-Instance-Typen](#)
- [ECSAmazon-Container: ECS Amazon-Container-Instances](#)
- [EKSAAmazon-Container: EKS Amazon-Worker-Knoten](#)
- [Funktionen: Lambda-Funktionskonfiguration](#)
- [Kontrolle des Prozessorstatus für Ihre EC2 Amazon-Instance](#)

### Zugehörige Videos:

- [EC2Amazon-Stiftungen](#)
- [AWS re:Invent 2023 — AWS Graviton: Das beste Preis-Leistungs-Verhältnis für Ihre Workloads AWS](#)
- [AWS re:Invent 2023 — Neue EC2 generative KI-Funktionen von Amazon in AWS Management Console](#)
- [AWS re:Invent 2023 — Was ist neu bei Amazon EC2](#)
- [AWS re:Invent 2023 — Intelligentes Sparen: Strategien zur Kostenoptimierung von Amazon EC2](#)
- [AWS re:Invent 2021 — Unterstützung für Amazon der nächsten GenerationEC2: Tiefer Einblick in das Nitro-System](#)
- [AWS re:Invent 2019 — Amazon-Stiftungen EC2](#)

Zugehörige Beispiele:

- [AWS Compute Optimizer Demo-Code](#)
- [EKSAamazon-Werkstatt](#)
- [Empfehlungen zur Dimensionierung](#)

PERF02-BP05 Skalieren Sie Ihre Rechenressourcen dynamisch

Nutzen Sie die Elastizität der Cloud, um die Datenverarbeitungsressourcen dynamisch nach oben oder unten zu skalieren, um Ihren Bedürfnissen zu entsprechen und eine Über- oder Unterdimensionierung von Kapazitäten für die Workload zu vermeiden.

Typische Anti-Muster:

- Sie reagieren auf Alarme, indem Sie die Kapazität manuell erhöhen.
- Sie verwenden dieselben Dimensionierungsrichtlinien (in der Regel statische Infrastruktur) wie bei On-Premises.
- Sie belassen die erhöhte Kapazität nach dem Hochskalieren, anstatt wieder herunterzuskalieren.

Vorteile der Nutzung dieser bewährten Methode: Durch das Konfigurieren und Testen der Elastizität von Datenverarbeitungsressourcen können Sie Geld sparen, Leistungsbenchmarks einhalten und die Zuverlässigkeit verbessern, wenn sich der Datenverkehr ändert.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Hoch

## Implementierungsleitfaden

AWS bietet die Flexibilität, Ihre Ressourcen mithilfe einer Vielzahl von Skalierungsmechanismen dynamisch nach oben oder unten zu skalieren, um Bedarfsänderungen gerecht zu werden. In Kombination mit Datenverarbeitungsmetriken ermöglicht eine dynamische Skalierung Workloads, automatisch auf Änderungen zu reagieren und die optimalen Datenverarbeitungsressourcen zu nutzen, um die Zielvorgabe zu erreichen.

Sie können verschiedene Ansätze nutzen, um das Angebot an Ressourcen auf die Nachfrage abzustimmen.

- **Ansatz zur Zielverfolgung:** Überwachen Sie Ihre Skalierungsmetriken und erhöhen oder verringern Sie die Kapazität automatisch Ihrem Bedarf entsprechend.
- **Prädiktive Skalierung:** Skalieren Sie in Erwartung täglicher und wöchentlicher Trends.
- **Zeitplanbasierter Ansatz:** Legen Sie Ihren eigenen Skalierungszeitplan entsprechend vorhersehbaren Laständerungen fest.
- **Skalierung von Services:** Wählen Sie Services (wie Serverless), die auf automatische Skalierung ausgelegt sind.

Sie müssen sicherstellen, dass Workload-Bereitstellungen sowohl Hoch- als auch Herunterskalierungsereignisse verarbeiten können.

## Implementierungsschritte

- Datenverarbeitungs-Instances, Container und Funktionen bieten Mechanismen für Elastizität, sei es in Kombination mit AutoScaling oder als Feature des Service. Hier finden Sie einige Beispiele für automatische Skalierungsmechanismen:

Autoscaling-Mechanismus	Aktion
<a href="#">Amazon EC2 Auto Scaling</a>	Um sicherzustellen, dass Ihnen die richtige Anzahl von <a href="#">EC2Amazon-Instances</a> zur Verfügung steht, um die Benutzerlast für Ihre Anwendung zu bewältigen.
<a href="#">Application Auto Scaling</a>	Um die Ressourcen für einzelne AWS Dienste außerhalb von Amazon automatisch zu skalieren, EC2 z. B. <a href="#">AWS Lambda</a> Funktion

Autoscaling-Mechanismus	Aktion
	n oder <a href="#">Amazon Elastic Container Service (AmazonECS)</a> -Services.
<a href="#">Kubernetes Cluster Autoscaler/Karpenter</a>	Zur automatischen Skalierung von Kubernetes-Clustern.

- Skalierung wird oft im Zusammenhang mit Rechendiensten wie EC2 Amazon-Instances oder AWS Lambda Funktionen diskutiert. Denken Sie auch daran, die Konfiguration von nicht Daten verarbeitenden Services in Betracht zu ziehen, z. B. [AWS Glue](#), um die Nachfrage zu decken.
- Stellen Sie sicher, dass die Metriken für die Skalierung den Merkmalen der bereitgestellten Workload entsprechen. Wenn Sie eine Anwendung zur Videotranskodierung einsetzen, wird eine CPU Auslastung von 100% erwartet, was nicht Ihre primäre Messgröße sein sollte. Verwenden Sie stattdessen die Tiefe der Aufgabenwarteschlange für die Transkodierung. Sie können bei Bedarf eine [benutzerdefinierte Metrik](#) für Ihre Skalierungsrichtlinie verwenden. Beachten Sie bei der Auswahl der richtigen Kennzahlen die folgenden Hinweise für AmazonEC2:
  - Es muss sich um eine gültige Nutzungsmetrik handeln, die beschreibt, wie stark eine Instance genutzt wird.
  - Der Wert der Metrik muss sich proportional zur Anzahl der Instances in der Auto-Scaling-Gruppe erhöhen oder verringern.
- Achten Sie darauf, für Ihre Auto-Scaling-Gruppe eine [dynamische Skalierung](#) anstelle einer [manuellen Skalierung](#) zu verwenden. Außerdem empfiehlt es sich, bei der dynamischen Skalierung [Skalierungsrichtlinien zur Zielverfolgung](#) zu verwenden.
- Prüfen Sie, ob Workload-Bereitstellungen mit beiden Skalierungen (nach oben und unten) umgehen können. Sie können beispielsweise den [Aktivitätsverlauf](#) verwenden, um eine Skalierungsaktivität für eine Auto-Scaling-Gruppe zu überprüfen.
- Evaluieren Sie Ihre Workload auf vorhersagbare Muster und skalieren Sie proaktiv, wenn Sie vorhergesagte und geplante Änderungen der Nachfrage erwarten. Mit der prädiktiven Skalierung können Sie die Notwendigkeit einer Überbereitstellung von Kapazitäten vermeiden. Weitere Informationen finden Sie unter [Predictive Scaling with Amazon EC2 Auto Scaling](#).

## Ressourcen

### Zugehörige Dokumente:

- [Cloud-Computing mit AWS](#)

- [EC2 Amazon-Instance-Typen](#)
- [ECS Amazon-Container: ECS Amazon-Container-Instances](#)
- [EKS Amazon-Container: EKS Amazon-Worker-Knoten](#)
- [Funktionen: Lambda-Funktionskonfiguration](#)
- [Kontrolle des Prozessorstatus für Ihre EC2 Amazon-Instance](#)
- [Tiefer Einblick in Amazon ECS Cluster Auto Scaling](#)
- [Vorstellung von Karpenter – Open-Source-Kubernetes-Cluster-Autoscaler mit hoher Leistung](#)

#### Zugehörige Videos:

- [AWS re:Invent 2023 — AWS Graviton: Das beste Preis-Leistungs-Verhältnis für Ihre Workloads](#)  
[AWS](#)
- [AWS re:Invent 2023 — Neue EC2 generative KI-Funktionen von Amazon in AWS der Management Console](#)
- [AWS re:Invent 2023 — Was ist neu bei Amazon EC2](#)
- [AWS re:Invent 2023 — Intelligentes Sparen: Strategien zur Kostenoptimierung von Amazon EC2](#)
- [AWS re:Invent 2021 — Unterstützung für Amazon der nächsten Generation EC2: Tiefer Einblick in das Nitro-System](#)
- [AWS re:Invent 2019 — Amazon-Stiftungen EC2](#)

#### Zugehörige Beispiele:

- [Beispiele EC2 für Amazon Auto Scaling-Gruppen](#)
- [EKSA Amazon-Werkstatt](#)
- [Skalieren Sie Ihre EKS Amazon-Workloads, indem Sie auf IPv6](#)

PERF02-BP06 Verwenden Sie optimierte hardwarebasierte Rechenbeschleuniger

Verwenden Sie Hardwarebeschleuniger, um bestimmte Funktionen effizienter auszuführen als CPU basierte Alternativen.

#### Typische Anti-Muster:

- Sie haben in der Workload keine Benchmark einer Allzweck-Instance verglichen mit einer speziell entwickelten Instance durchgeführt, die eine höhere Leistung und niedrigere Kosten bieten kann.

- Sie verwenden hardwarebasierte Rechenbeschleuniger für Aufgaben, die mit basierten Alternativen effizienter sein können. CPU
- Sie überwachen die Nutzung nicht. GPU

Vorteile der Einführung dieser bewährten Methode: Durch den Einsatz hardwarebasierter Beschleuniger wie Grafikprozessoren (GPUs) und Field Programmable Gate Arrays (FPGAs) können Sie bestimmte Verarbeitungsfunktionen effizienter ausführen.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Mittel

### Implementierungsleitfaden

Beschleunigte Recheninstanzen bieten Zugriff auf hardwarebasierte Rechenbeschleuniger wie und GPUs FPGAs Diese Hardwarebeschleuniger führen bestimmte Funktionen wie Grafikverarbeitung oder Datenmusterabgleich effizienter aus als basierte Alternativen. CPU Viele beschleunigte Workloads, wie Rendering, Transkodierung und Machine Learning, sind sehr variabel im Bezug auf die Ressourcennutzung. Betreiben Sie diese Hardware nur so lange wie nötig und nehmen Sie sie automatisch außer Betrieb, wenn sie nicht mehr benötigt wird, um die allgemeine Leistungseffizienz zu verbessern.

### Implementierungsschritte

- Ermitteln Sie, welche [beschleunigten Computing-Instances](#) für Ihre Anforderungen geeignet sind.
- [Nutzen Sie für Machine-Learning-Workloads speziell für Ihren Workload entwickelte Hardware wie AWS Trainium, AWS Inferentia und Amazon. EC2 DL1 AWS Inferentia-Instances wie Inf2-Instances bieten eine um bis zu 50% bessere Leistung pro Watt als vergleichbare Amazon-Instances. EC2](#)
- Erfassen Sie Nutzungsmetriken für Ihre beschleunigten Computing-Instances. Sie können den CloudWatch Agenten beispielsweise verwenden, um Metriken wie `utilization_gpu` und `utilization_memory` für Sie zu sammeln, GPUs wie in [NVIDIAGPUMetriken mit Amazon sammeln](#) gezeigt CloudWatch.
- Optimieren Sie Code, Netzwerkbetrieb und die Einstellungen von Hardwarebeschleunigern, um sicherzustellen, dass die zugrunde liegende Hardware optimal genutzt wird.
  - [GPUEinstellungen optimieren](#)
  - [GPUÜberwachung und Optimierung im Deep Learning AMI](#)
  - [I/O-Optimierung für die GPU Leistungsoptimierung von Deep-Learning-Trainings in Amazon SageMaker](#)
- Verwenden Sie die neuesten Hochleistungsbibliotheken und GPU Treiber.

- Verwenden Sie Automatisierung, um GPU Instanzen freizugeben, wenn sie nicht verwendet werden.

## Ressourcen

### Zugehörige Dokumente:

- [Arbeiten mit GPUs auf Amazon Elastic Container Service](#)
- [GPU Instanzen](#)
- [Instanzen mit AWS Trainium](#)
- [Instanzen mit Inferentia AWS](#)
- [Let's Architect! Erstellen von Architekturen mit benutzerdefinierten Chips und Beschleunigern](#)
  
- [Beschleunigte Datenverarbeitung](#)
- [EC2VT1 Amazon-Instances](#)
- [Wie wähle ich den passenden EC2 Amazon-Instance-Typ für meinen Workload aus?](#)
- [Wählen Sie mit Amazon den besten KI-Beschleuniger und die beste Modellkompilierung für Computer-Vision-Inferenz SageMaker](#)

### Zugehörige Videos:

- [AWS re:Invent 2021 — So wählen Sie Amazon Elastic Compute GPU Cloud-Instanzen für Deep Learning aus](#)
- [AWS re:Invent 2022 — \[!\] NEW LAUNCH Einführung in AWS Inferentia2-basierte Amazon Inf2-Instances EC2](#)
- [AWS re:Invent 2022 – Accelerate deep learning and innovate faster with AWS Trainium](#)
- [AWS re:Invent 2022 — Deep Learning weiter mit: Von der Schulung bis zur Bereitstellung AWS NVIDIA](#)

### Zugehörige Beispiele:

- [Amazon SageMaker und NVIDIA GPU Cloud \(NGC\)](#)
- [Verwenden Sie es SageMaker zusammen mit Trainium und Inferentia für optimierte Workloads für Deep-Learning-Training und Inferentia](#)



- [Optimierung von NLP Modellen mit Amazon Elastic Compute Cloud Inf1-Instances in Amazon SageMaker](#)

## Datenverwaltung

### Fragen

- [PERF3. Wie speichern und verwalten Sie die Daten in Ihrer Workload und wie greifen Sie darauf zu?](#)

PERF3. Wie speichern und verwalten Sie die Daten in Ihrer Workload und wie greifen Sie darauf zu?

Die optimale Datenverwaltungslösung für ein bestimmtes System hängt von der Art des Datentyps (Block, Datei oder Objekt), den Zugriffsmustern (zufällig oder sequentiell), dem erforderlichen Durchsatz, der Häufigkeit des Zugriffs (online, offline, archiviert), der Aktualisierungshäufigkeit (WORMdynamisch) sowie von Verfügbarkeits- und Haltbarkeitsbeschränkungen ab. Well-Architected-Workloads verwenden zweckgebundene Datenspeicher, die verschiedene Features zur Verbesserung der Leistung ermöglichen.

### Bewährte Methoden

- [PERF03-BP01 Verwenden Sie einen speziell entwickelten Datenspeicher, der Ihre Datenzugriffs- und Speicheranforderungen am besten unterstützt](#)
- [PERF03-BP02 Evaluieren Sie die verfügbaren Konfigurationsoptionen für den Datenspeicher](#)
- [PERF03-BP03 Leistungskennzahlen für Datenspeicher sammeln und aufzeichnen](#)
- [PERF03-BP04 Implementieren Sie Strategien zur Verbesserung der Abfrageleistung im Datenspeicher](#)
- [PERF03-BP05 Implementieren Sie Datenzugriffsmuster, die Caching nutzen](#)

PERF03-BP01 Verwenden Sie einen speziell entwickelten Datenspeicher, der Ihre Datenzugriffs- und Speicheranforderungen am besten unterstützt

Machen Sie sich mit Datenmerkmalen (wie Freigabe, Größe, Cache-Größe, Zugriffsmuster, Latenz, Durchsatz und Persistenz von Daten) vertraut, um die richtigen, speziell entwickelten Datenspeicher (Speicher oder Datenbank) für die Workload auszuwählen.

Typische Anti-Muster:

- Sie halten an einem Datenspeicher fest, da es interne Erfahrungen und Wissen über eine bestimmte Datenbanklösung gibt.
- Sie gehen davon aus, dass für alle Workloads ähnliche Datenspeicher- und Zugriffsanforderungen gelten.
- Sie haben keinen Datenkatalog zur Inventarisierung Ihrer Datenbestände eingeführt.

Vorteile der Nutzung dieser bewährten Methode: Wenn Sie die Datenmerkmale und -anforderungen verstehen, können Sie die effizienteste und leistungsfähigste Speichertechnologie ermitteln, die für Ihre Workload-Anforderungen geeignet ist.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Hoch

### Implementierungsleitfaden

Achten Sie bei der Auswahl und Implementierung des Datenspeichers darauf, dass die Abfrage-, Skalierungs- und Speichereigenschaften die Anforderungen an die Workload-Daten erfüllen. AWS bietet zahlreiche Datenspeicher- und Datenbanktechnologien, darunter Blockspeicher-, Objektspeicher-, Streaming-Speicher-, Dateisystem-, relationale, Schlüsselwert-, Dokument-, In-Memory-, Diagramm-, Zeitreihen- und Hauptbuchdatenbanken. Jede Datenverwaltungslösung hat verfügbare Optionen und Konfigurationen, um Ihre Anwendungsfälle und Datenmodelle zu unterstützen. Wenn Sie die Eigenschaften und Anforderungen von Daten verstehen, können Sie sich von monolithischen Speichertechnologien und restriktiven one-size-fits-all Ansätzen lösen und sich auf das angemessene Datenmanagement konzentrieren.

### Implementierungsschritte

- Führen Sie eine Bestandsaufnahme der verschiedenen Datentypen durch, die in Ihrer Workload vorhanden sind.
- Verstehen und dokumentieren Sie Datenmerkmale und -anforderungen, einschließlich:
  - Datentyp (strukturiert, semistrukturiert, relational)
  - Datenvolumen und -wachstum
  - Lebensdauer von Daten: anhaltend, flüchtig, vorübergehend
  - ACIDAnforderungen (Atomarität, Konsistenz, Isolierung, Haltbarkeit)
  - Datenzugriffsmuster (leseintensiv oder schreibintensiv)
  - Latency
  - Durchsatz

- IOPS(Eingabe-/Ausgabevorgänge pro Sekunde)
- Aufbewahrungszeitraum
- Erfahren Sie mehr über die verschiedenen Datenspeicher ([Speicher](#) - und [Datenbankdienste](#)), die für Ihren Workload verfügbar AWS sind und Ihre Dateneigenschaften erfüllen können, wie unter beschrieben. [PERF01-BP01 Erfahren Sie mehr über verfügbare Cloud-Dienste und -Funktionen und verstehen Sie sie](#) Einige Beispiele für AWS -Speichertechnologien und ihre Schlüsselmerkmale sind:

Typ	AWS Services	Schlüsselmerkmale
Objektspeicher	<a href="#">Amazon S3</a>	Unbegrenzte Skalierbarkeit, hohe Verfügbarkeit und mehrere Optionen für Barrierefreiheit. Für die Übertragung von Objekten in und aus Amazon S3 und den Zugriff auf diese Objekte können Sie einen Service wie z. B. <a href="#">Transfer Acceleration</a> oder <a href="#">Zugangspunkte</a> verwenden, um Ihren Standort, Ihre Sicherheitsanforderungen und Zugriffsmuster zu unterstützen.
Archivieren von Speichern	<a href="#">Amazon S3 Glacier</a>	Für die Datenarchivierung entwickelt.
Streaming-Speicher	<a href="#">Amazon Kinesis</a> <a href="#">Von Amazon Managed Streaming for Apache Kafka (AmazonMSK)</a>	Effiziente Erfassung und Speicherung von Streaming-Daten.
Gemeinsames Dateisystem	<a href="#">Amazon Elastic File System (AmazonEFS)</a>	Bereitstellbares Dateisystem, auf das mehrere Arten von

Typ	AWS Services	Schlüsselmerkmale
		Datenverarbeitungslösungen zugreifen können.
Gemeinsames Dateisystem	<a href="#">Amazon FSx</a>	Basiert auf den neuesten AWS Computerlösungen zur Unterstützung von vier häufig verwendeten Dateisystemen: Open NetApp ONTAPZFS, Windows File Server und Lustre. Die FSx <a href="#">Latenz, der Durchsatz und</a> der Durchsatz von Amazon IOPS variieren je nach Dateisystem und sollten bei der Auswahl des richtigen Dateisystems für Ihre Workload-Anforderungen berücksichtigt werden.
Blockspeicher	<a href="#">Amazon Elastic Block Store (AmazonEBS)</a>	Skalierbarer, leistungsstarker Blockspeicher-Service, der für Amazon Elastic Compute Cloud (AmazonEC2) entwickelt wurde. Amazon EBS bietet SSD-gestützten Speicher für IOPS transaktionsintensive Workloads und HDD-gestützten Speicher für durchsatzintensive Workloads.

Typ	AWS Services	Schlüsselmerkmale
Relationale Datenbank	<a href="#">Amazon Aurora</a> , <a href="#">Amazon RDS</a> , <a href="#">Amazon Redshift</a> .	Entwickelt, um Transaktionen ACID (Atomizität, Konsistenz, Isolierung, Haltbarkeit) zu unterstützen und die referenzielle Integrität und hohe Datenkonsistenz aufrechtzuerhalten. Viele traditionelle Anwendungen wie Enterprise Resource Planning (ERP), Customer Relationship Management (CRM) und E-Commerce verwenden relationale Datenbanken zum Speichern ihrer Daten.
Schlüssel-Werte-Datenbank	<a href="#">Amazon-DynamoDB</a>	Für gängige Zugriffsmuster optimiert, üblicherweise zum Speichern und Abrufen großer Datenmengen. Web-Apps mit hohem Datenverkehr, E-Commerce-Systeme und Gaming-Anwendungen sind typische Anwendungsfälle für Schlüssel-Werte-Datenbanken.

Typ	AWS Services	Schlüsselmerkmale
Dokumentdatenbank	<a href="#">Amazon DocumentDB</a>	Entwickelt, um halbstrukturierte Daten als JSON-ähnliche Dokumente zu speichern. Mit diesen Datenbanken können Entwickler Anwendungen wie Content Management, Kataloge und Benutzerprofile schnell erstellen und aktualisieren.
In-Memory-Datenbanken	<a href="#">Amazon ElastiCache</a> , <a href="#">Amazon MemoryDB</a> für Redis	Dies wird für Anwendungen eingesetzt, die einen Echtzeitzugriff auf Daten, die niedrigste Latenz und den höchsten Durchsatz erfordern. Sie können In-Memory-Datenbanken für Anwendungs-Caching, Sitzungsmanagement, Gaming-Bestenlisten, ML-Feature-Store mit niedriger Latenz, Microservices-Messaging-System und einen Streaming-Mechanismus mit hohem Durchsatz verwenden.

Typ	AWS Services	Schlüsselmerkmale
Graphdatenbank	<a href="#">Amazon Neptune</a>	Dies ist für Anwendungen gedacht, die in Millionen von Beziehungen zwischen hochgradig vernetzten Diagrammdatensätzen mit Millisekunden-Latenz navigieren und diese abfragen müssen. Viele Unternehmen verwenden Graphdatenbanken für Betrugserkennung, soziale Netzwerke und Empfehlung-Engines.
Zeitreihendatenbank	<a href="#">Amazon Timestream</a>	Diese erfasst, generiert und gewinnt auf effiziente Weise Einblicke aus Daten, die sich im Laufe der Zeit ändern. IoT-Anwendungen und industrielle Telemetrie können Zeitreihendatenbanken nutzen. DevOps

Typ	AWS Services	Schlüsselmerkmale
Wide-Column-Datenbanken	<a href="#">Amazon Keyspaces (für Apache Cassandra)</a>	Es werden Tabellen, Zeilen und Spalten verwendet, aber im Gegensatz zu einer relationalen Datenbank können sich die Namen und das Format der Spalten von Zeile zu Zeile in derselben Tabelle unterscheiden. In der Regel werden Wide Column-Speicher in umfangreichen Branchen-Apps für Gerätewartung, Flottenverwaltung und Routenoptimierung eingesetzt.
Ledger	<a href="#">Amazon Quantum Ledger-Datenbank (AmazonQLDB)</a>	Dies bietet eine zentrale und vertrauenswürdige Instanz für die Verwaltung einer skalierbaren, unveränderlichen und kryptografisch überprüfbaren Aufzeichnung von Transaktionen für jede Anwendung. Ledger-Datenbanken werden für Datensatzsysteme, Lieferketten, Registrierungen und sogar Banktransaktionen verwendet.

- Wenn Sie eine Datenplattform aufbauen, nutzen Sie die [moderne Datenarchitektur](#), AWS um Ihren Data Lake, Ihr Data Warehouse und speziell entwickelte Datenspeicher zu integrieren.
- Die wichtigsten Fragen, die Sie bei der Auswahl eines Datenspeichers für Ihre Workload berücksichtigen müssen, lauten wie folgt:



Frage	Worauf Sie achten sollten
Wie sind die Daten strukturiert?	<ul style="list-style-type: none"><li>• <a href="#">Wenn die Daten unstrukturiert sind, ziehen Sie einen Objektspeicher wie Amazon S3 oder eine SQL No-Datenbank wie Amazon DocumentDB in Betracht</a></li><li>• <a href="#">Ziehen Sie für Schlüsselwertdaten DynamoDB, Amazon ElastiCache (OSSRedis) oder Amazon MemoryDB in Betracht</a></li></ul>
Welches Maß an referentieller Integrität ist erforderlich?	<ul style="list-style-type: none"><li>• Bei Fremdschlüsseinschränkungen können relationale Datenbanken wie <a href="#">Amazon RDS</a> und <a href="#">Aurora</a> dieses Maß an Integrität bieten.</li><li>• In der Regel würden Sie bei einem SQL Modell ohne Daten die Normalisierung Ihrer Daten in ein einzelnes Dokument oder eine Sammlung von Dokumenten umwandeln, die dann in einer einzigen Anfrage abgerufen werden könnten, anstatt sie über mehrere Dokumente oder Tabellen hinweg zusammenzufügen.</li></ul>
Ist die Einhaltung von Vorschriften ACID (Atomität, Konsistenz, Isolierung, Haltbarkeit) erforderlich?	<ul style="list-style-type: none"><li>• <a href="#">Wenn die mit relationalen Datenbanken verknüpften ACID Eigenschaften erforderlich sind, sollten Sie eine relationale Datenbank wie Amazon RDS und Aurora in Betracht ziehen.</a></li><li>• Wenn für <a href="#">Keine SQL Datenbank</a> eine hohe Konsistenz erforderlich ist, können Sie Strongly Consistent Reads mit <a href="#">DynamoDB</a> verwenden.</li></ul>

Frage	Worauf Sie achten sollten
<p>Wie ändern sich die Speicheranforderungen im Laufe der Zeit? Wie beeinflusst dies die Skalierbarkeit?</p>	<ul style="list-style-type: none"> <li>• Serverlose Datenbanken wie <a href="#">DynamoDB</a> und <a href="#">Amazon Quantum Ledger Database (Amazon QLDB)</a> werden dynamisch skaliert.</li> <li>• Relationale Datenbanken haben oftmals Obergrenzen bei bereitgestelltem Speicher und müssen mithilfe von Mechanismen wie Sharding horizontal partitioniert werden, sobald sie diese Grenzen erreicht haben.</li> </ul>
<p>Wie hoch ist der Anteil der Leseabfragen im Verhältnis zu den Schreibabfragen? Könnte Caching die Leistung verbessern?</p>	<ul style="list-style-type: none"> <li>• Leseintensive Workloads können von einer Caching-Ebene profitieren, z. B. <a href="#">DAX</a> wenn es sich bei der Datenbank um <a href="#">ElastiCache</a> DynamoDB handelt.</li> <li>• <a href="#">Lesevorgänge können auch ausgelagert werden, um Repliken mit relationalen Datenbanken wie Amazon zu lesen. RDS</a></li> </ul>
<p>Haben Speicherung und Änderung (OLTP— Online-Transaktionsverarbeitung) oder Abruf und Berichterstattung (OLAP— Analytische Online-Verarbeitung) eine höhere Priorität?</p>	<ul style="list-style-type: none"> <li>• Für die unveränderte Transaktionsverarbeitung mit hohem Durchsatz sollten Sie eine SQL Nein-Datenbank wie DynamoDB in Betracht ziehen.</li> <li>• Verwenden Sie Amazon RDS für hohen Durchsatz und komplexe Lesemuster (wie Join) mit Konsistenz.</li> <li>• <a href="#">Ziehen Sie für analytische Abfragen eine spaltenförmige Datenbank wie Amazon Redshift in Betracht oder exportieren Sie die Daten nach Amazon S3 und führen Sie Analysen mit Athena oder Amazon durch. QuickSight</a></li> </ul>

Frage	Worauf Sie achten sollten
Welches Ausmaß an Stabilität erfordern die Daten?	<ul style="list-style-type: none"><li>• Aurora repliziert Ihre Daten automatisch in drei Availability Zones innerhalb einer Region, was bedeutet, dass Ihre Daten hochbeständig sind und eine geringere Wahrscheinlichkeit von Datenverlust besteht.</li><li>• DynamoDB wird automatisch in mehreren Availability Zones repliziert und bietet hohe Verfügbarkeit und Datenstabilität.</li><li>• Amazon S3 bietet eine Langlebigkeit mit 11 Neunen. Viele Datenbankdienste, wie Amazon RDS und DynamoDB, unterstützen den Export von Daten nach Amazon S3 zur langfristigen Aufbewahrung und Archivierung.</li></ul>
Besteht der Wunsch, sich von kommerziellen Datenbank-Engines oder Lizenzkosten zu entfernen?	<ul style="list-style-type: none"><li>• Denken Sie an Open-Source-Engines wie PostgreSQL und MySQL auf Amazon RDS oder Aurora.</li><li>• Nutzen Sie <a href="#">AWS Database Migration Service</a> und <a href="#">AWS Schema Conversion Tool</a> zum Migrieren von kommerziellen Datenbank-Engines zu Open Source-Lösungen.</li></ul>
Was ist die Betriebserwartung an die Datenbank? Ist der Umstieg zu verwalteten Services eine Priorität?	<ul style="list-style-type: none"><li>• Die Nutzung von Amazon RDS anstelle von Amazon DynamoDB oder Amazon DocumentDB EC2, anstatt eine SQL No-Datenbank selbst zu hosten, kann den Betriebsaufwand reduzieren.</li></ul>

Frage	Worauf Sie achten sollten
<p>Wie erfolgt derzeit der Zugriff auf die Datenbank? Geht es nur um Anwendungszugriff oder gibt es Business Intelligence (BI) -Benutzer und andere verbundene Anwendungen? off-the-shelf</p>	<ul style="list-style-type: none"> <li>• Wenn Sie von externen Tools abhängig sind, müssen Sie möglicherweise mit der Datenbank, die unterstützt wird, die Kompatibilität aufrecht erhalten. Amazon RDS ist vollständig kompatibel mit den verschiedenen Engine-Versionen, die es unterstützt, einschließlich Microsoft SQL Server, OracleSQL, My und PostgreSQL.</li> </ul>

- Führen Sie Experimente und Benchmarking in einer Nicht-Produktionsumgebung durch, um herauszufinden, welcher Datenspeicher Ihre Workload-Anforderungen erfüllen kann.

## Ressourcen

### Zugehörige Dokumente:

- [EBSAmazon-Volumetypen](#)
- [EC2Amazon-Speicher](#)
- [AmazonEFS: EFS Leistung von Amazon](#)
- [Amazon FSx für Lustre Performance](#)
- [Leistung von Amazon FSx für Windows-Dateiserver](#)
- [Amazon S3 Glacier: S3 Glacier Documentation](#)
- [Amazon S3: Überlegungen zu Anfragerate und Leistung](#)
- [Cloud-Speicher mit AWS](#)
- [Amazon EBS I/O-Eigenschaften](#)
- [Cloud-Datenbanken mit AWS](#)
- [AWS Datenbank-Caching](#)
- [DynamoDB Accelerator](#)
- [Bewährte Methoden mit Amazon Aurora](#)
- [Leistung von Amazon Redshift](#)
- [Die zehn besten Leistungstipps für Amazon Athena](#)
- [Bewährte Methoden für Amazon Redshift Spectrum](#)

- [Bewährte Methoden für Amazon DynamoDB](#)
- [Wählen Sie zwischen Amazon EC2 und Amazon RDS](#)
- [Bewährte Methoden für die Implementierung von Amazon ElastiCache](#)

#### Zugehörige Videos:

- [AWS re:Invent 2023: Verbessern Sie die Effizienz von Amazon Elastic Block Store und seien Sie kosteneffizienter](#)
- [AWS re:Invent 2023: Optimierung von Speicherpreis und -leistung mit Amazon Simple Storage Service](#)
- [AWS re:Invent 2023: Aufbau und Optimierung eines Data Lakes auf Amazon Simple Storage Service](#)
- [AWS re:Invent 2022: Aufbau moderner Datenarchitekturen auf AWS](#)
- [AWS re:Invent 2022: Aufbau von Data-Mesh-Architekturen auf AWS](#)
- [AWS re:Invent 2023: Tauchen Sie tief in Amazon Aurora und seine Innovationen ein](#)
- [AWS re:Invent 2023: Fortgeschrittene Datenmodellierung mit Amazon DynamoDB](#)
- [AWS re:Invent 2022: Modernisieren Sie Apps mit speziell entwickelten Datenbanken](#)
- [Ausführliche Beschreibung von Amazon DynamoDB: Erweiterte Entwurfsmuster](#)

#### Zugehörige Beispiele:

- [AWS Workshop zu speziell entwickelten Datenbanken](#)
- [Databases for Developers](#)
- [AWS Immersionstag zur modernen Datenarchitektur](#)
- [Bauen Sie ein Datennetz auf AWS](#)
- [Amazon S3-Beispiele](#)
- [Optimierung von Datenmustern mithilfe von Amazon Redshift Data Sharing](#)
- [Datenbankmigrationen](#)
- [MS SQL Server - AWS Database Migration Service \(AWS DMS\) Replikationsdemo](#)
- [Praktischer Workshop zur Datenbankmodernisierung](#)
- [Beispiele zu Amazon Neptune](#)

## PERF03-BP02 Evaluieren Sie die verfügbaren Konfigurationsoptionen für den Datenspeicher

Machen Sie sich mit den verschiedenen Features und Konfigurationsoptionen vertraut, die für Ihre Datenspeicher verfügbar sind, und bewerten Sie sie, um Speicherplatz und Leistung für Ihre Workload zu optimieren.

Typische Anti-Muster:

- Sie verwenden nur einen Speichertyp, z. B. AmazonEBS, für alle Workloads.
- Sie verwenden Provisioned IOPS für alle Workloads, ohne dass reale Tests für alle Speicherstufen erforderlich sind.
- Ihnen fehlt das Bewusstsein für die Wahl der Konfigurationsoptionen der Datenverwaltungslösung.
- Sie verlassen sich ausschließlich auf das Vergrößern der Instance-Größe, ohne andere verfügbare Konfigurationsoptionen in Betracht zu ziehen.
- Sie testen die Skalierungsoptionen Ihres Datenspeichers nicht.

Vorteile der Nutzung dieser bewährten Methode: Indem Sie Datenspeicherkonfigurationen erkunden und mit ihnen experimentieren, können Sie möglicherweise Infrastrukturkosten senken, die Leistung verbessern und den Aufwand zur Verwaltung Ihrer Workloads verringern.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Mittel

Implementierungsleitfaden

Für eine Workload können je nach Datenspeicher- und Zugriffsanforderungen ein oder mehrere Datenspeicher verwendet werden. Zur Optimierung der Leistungseffizienz und Kosten müssen Sie Datenzugriffsmuster auswerten, um die entsprechenden Datenspeicherkonfigurationen zu bestimmen. Während Sie die Datenspeicheroptionen erkunden, sollten Sie unterschiedliche Aspekte in Betracht ziehen. Dazu zählen Speicheroptionen, Arbeitsspeicher, Rechenvorgänge, Read Replica, Konsistenzanforderungen, Verbindungs-Pooling und Caching-Optionen. Experimentieren Sie mit diesen unterschiedlichen Konfigurationsoptionen, um Metriken zur Leistungseffizienz zu verbessern.

Implementierungsschritte

- Verstehen Sie die aktuellen Konfigurationen (wie Instance-Typ, Speichergröße oder Version der Datenbank-Engine) des Datenspeichers.
- Lesen Sie die AWS Dokumentation und die bewährten Methoden, um mehr über empfohlene Konfigurationsoptionen zu erfahren, mit denen Sie die Leistung Ihres Datenspeichers verbessern

können. Die wichtigsten Datenspeicheroptionen, die Sie in Betracht ziehen sollten, sind die folgenden:

Konfigurationsoption	Beispiele
Auslagern von Lesevorgängen (wie Read Replicas und Caching)	<ul style="list-style-type: none"><li>• Für DynamoDB-Tabellen können Sie Lesevorgänge mithilfe DAX von Caching auslagern.</li><li>• Sie können einen Amazon ElastiCache (RedisOSS) -Cluster erstellen und Ihre Anwendung so konfigurieren, dass sie zuerst aus dem Cache liest und auf die Datenbank zurückgreift, falls das angeforderte Element nicht vorhanden ist.</li><li>• Relationale Datenbanken wie Amazon RDS und Aurora und bereitgestellt Keine SQL Datenbanken wie Neptune und Amazon DocumentDB unterstützen alle das Hinzufügen von Read Replicas, um die gelesenen Teile der Arbeitslast auszulagern.</li><li>• Serverless-Datenbanken wie DynamoDB skalieren automatisch. Stellen Sie sicher, dass Sie über genügend Lesekapazitätseinheiten ( ) RCU verfügen, um die Arbeitslast zu bewältigen.</li></ul>

Konfigurationsoption	Beispiele
Skalieren von Schreibvorgängen (wie Partitionsschlüssel-Sharding oder Einführung einer Warteschlange)	<ul style="list-style-type: none"><li>• Bei relationalen Datenbanken können Sie die Größe der Instanz erhöhen, um einer erhöhten Arbeitslast gerecht zu werden, oder die bereitgestellte Instanz erhöhen, IOPs um einen höheren Durchsatz für den zugrunde liegenden Speicher zu ermöglichen.</li><li>• Sie können vor Ihrer Datenbank auch eine Warteschlange einrichten, anstatt direkt in die Datenbank zu schreiben. Mithilfe dieses Musters können Sie die Datenerfassung von der Datenbank entkoppeln und die Flow-Rate steuern, sodass die Datenbank nicht überwältigt wird.</li><li>• Das Batching Ihrer Schreibenforderungen, anstatt mehrere kurzlebige Transaktionen zu erstellen, kann Ihnen dabei helfen, den Durchsatz bei relationalen Datenbanken mit hohem Schreibvolumen zu verbessern.</li><li>• Serverlose Datenbanken wie DynamoDB können den Schreibdurchsatz automatisch oder durch Anpassung der bereitgestellten Schreibkapazitätseinheiten (WCU) je nach Kapazitätsmodus skalieren.</li><li>• Es können immer noch Probleme mit heißen Partitionen auftreten, wenn Sie die Durchsatzgrenzen für einen bestimmten Partitionsschlüssel erreichen. Dies kann verhindert werden, indem Sie einen Partitionsschlüssel auswählen, der gleichmäßiger verteilt ist, oder indem Sie die Schreibvorgänge des Partitionsschlüssels in Shards aufteilen.</li></ul>



Konfigurationsoption	Beispiele
Richtlinien zum Verwalten des Lebenszyklus von Datensätzen	<ul style="list-style-type: none"> <li>• Mit <a href="#">Amazon-S3-Lebenszyklen</a> können Sie Ihre Objekte während ihres gesamten Lebenszyklus verwalten. Wenn die Zugriffsmuster unbekannt oder nicht prognostizierbar sind oder sich ändern, können Sie <a href="#">Amazon S3 Intelligent-Tiering</a> verwenden. Hiermit werden Zugriffsmuster überwacht und Objekte, auf die nicht zugegriffen wurde, automatisch in kostengünstigere Zugriffsebenen verschoben. Anhand der Metriken von <a href="#">Amazon S3 Storage Lens</a> können Sie Optimierungsmöglichkeiten und Lücken im Lebenszyklusmanagement ermitteln.</li> <li>• <a href="#">Amazon EFS Lifecycle Management</a> verwaltet automatisch den Dateispeicher für Ihre Dateisysteme.</li> </ul>
Verbindungsmanagement und Pooling	<ul style="list-style-type: none"> <li>• Amazon RDS Proxy kann mit Amazon RDS und Aurora verwendet werden, um Verbindungen zur Datenbank zu verwalten.</li> <li>• Serverless-Datenbanken wie DynamoDB haben keine ihnen zugewiesenen Verbindungen, aber ziehen Sie die bereitgestellte Kapazität sowie automatische Skalierungsrichtlinien in Betracht, um Datenverkehrsspitzen zu bewältigen.</li> </ul>

- Führen Sie Experimente und Benchmarking in einer Nicht-Produktionsumgebung durch, um herauszufinden, welche Konfigurationsoption Ihre Workload-Anforderungen erfüllen kann.
- Nachdem Sie experimentiert haben, planen Sie die Migration und überprüfen Sie die Leistungsmetriken.

- Verwenden Sie Tools AWS zur Überwachung (wie [Amazon CloudWatch](#)) und Optimierung (wie [Amazon S3 Storage Lens](#)), um Ihren Datenspeicher kontinuierlich anhand von realen Nutzungsmustern zu optimieren.

## Ressourcen

### Zugehörige Dokumente:

- [Cloud-Speicher mit AWS](#)
- [EBSAmazon-Volumetypen](#)
- [EC2Amazon-Speicher](#)
- [AmazonEFS: EFS Leistung von Amazon](#)
- [Amazon FSx für Lustre Performance](#)
- [Leistung von Amazon FSx für Windows-Dateiserver](#)
- [Amazon S3 Glacier: S3 Glacier Documentation](#)
- [Amazon S3: Überlegungen zu Anfragerate und Leistung](#)
- [Amazon EBS I/O-Eigenschaften](#)
- [Cloud-Datenbanken mit AWS](#)
- [AWS Datenbank-Caching](#)
- [DynamoDB Accelerator](#)
- [Bewährte Methoden mit Amazon Aurora](#)
- [Leistung von Amazon Redshift](#)
- [Die zehn besten Leistungstipps für Amazon Athena](#)
- [Bewährte Methoden für Amazon Redshift Spectrum](#)
- [Bewährte Methoden für Amazon DynamoDB](#)

### Zugehörige Videos:

- [AWS re:Invent 2023: Improve Amazon Elastic Block Store efficiency and be more cost-efficient](#)
- [AWS re:Invent 2023: Optimize storage price and performance with Amazon Simple Storage Service](#)
- [AWS re:Invent 2023: Building and optimizing a data lake on Amazon Simple Storage Service](#)
- [AWS re:Invent 2023: Was ist neu bei der Dateispeicherung AWS](#)

- [AWS re:Invent 2023: Dive deep into Amazon DynamoDB](#)

Zugehörige Beispiele:

- [AWS Workshop zu speziell entwickelten Datenbanken](#)
- [Databases for Developers](#)
- [AWS Immersionstag zur modernen Datenarchitektur](#)
- [Amazon EBS Autoscale](#)
- [Amazon S3-Beispiele](#)
- [Amazon DynamoDB-Beispiele](#)
- [AWS Beispiele für Datenbankmigrationen](#)
- [Workshop zur Modernisierung von Datenbanken](#)
- [Arbeiten mit Parametern in Ihrer Amazon RDS for Postgress-Datenbank](#)

PERF03-BP03 Leistungskennzahlen für Datenspeicher sammeln und aufzeichnen

Verfolgen und zeichnen Sie relevante Leistungsmetriken für Ihren Datenspeicher auf, um zu verstehen, wie Ihre Datenverwaltungslösungen funktionieren. Mithilfe dieser Metriken können Sie Ihren Datenspeicher optimieren, überprüfen, ob Ihre Workload-Anforderungen erfüllt werden, und sich einen klaren Überblick über die Workload-Leistung verschaffen.

Typische Anti-Muster:

- Sie suchen ausschließlich manuell mithilfe von Protokolldateien nach Metriken.
- Sie veröffentlichen Metriken nur in internen Tools, die von Ihrem Team verwendet werden, und Sie haben kein umfassendes Bild Ihrer Workload.
- Sie verwenden nur die Standardmetriken, die von der Überwachungssoftware Ihrer Wahl aufgezeichnet wurden.
- Sie überprüfen Metriken nur dann, wenn ein Problem vorliegt.
- Sie überwachen Metriken nur auf Systemebene und erfassen keine Datenzugriffs- und Nutzungsmetriken.

Vorteile der Nutzung dieser bewährten Methode: Das Einrichten einer Leistungsbasislinie hilft Ihnen dabei, das normale Verhalten und die Anforderungen von Workloads zu verstehen. Abnorme

Muster können schneller identifiziert und behoben werden, was die Leistung und Zuverlässigkeit des Datenspeichers erhöht.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Hoch

### Implementierungsleitfaden

Um die Leistung der Datenspeicher zu überwachen, müssen Sie mehrere Leistungsmetriken über einen bestimmten Zeitraum aufzeichnen. Auf diese Weise können Sie Anomalien erkennen und die Leistung anhand von Geschäftsmetriken messen, um sicherzustellen, dass Sie die Anforderungen Ihrer Workload erfüllen.

Metriken sollten das zugrunde liegende System, das den Datenspeicher unterstützt, sowie die Datenbankmetriken enthalten. Zu den zugrunde liegenden Systemmetriken können CPU Auslastung, Arbeitsspeicher, verfügbarer Festplattenspeicher, Festplatten-E/A, Cache-Trefferquote sowie Metriken für eingehende und ausgehende Netzwerkdaten gehören, während die Datenspeicher-Metriken Transaktionen pro Sekunde, Top-Abfragen, durchschnittliche Abfrageraten, Antwortzeiten, Indexnutzung, Tabellensperren, Abfrage-Timeouts und Anzahl der geöffneten Verbindungen umfassen können. Diese Daten sind von entscheidender Bedeutung, um festzustellen, wie leistungsfähig die Workload ist und wie die Datenverwaltungslösung genutzt wird. Nutzen Sie diese Metriken im Rahmen eines datengestützten Ansatzes, der Ihnen die Feinabstimmung und Optimierung der von der Workload genutzten Ressourcen ermöglicht.

Nutzen Sie Tools, Bibliotheken und Systeme zum Aufzeichnen von Messungen zur Datenbankleistung.

### Implementierungsschritte

- Identifizieren Sie die wichtigsten Leistungsmetriken, die der Datenspeicher verfolgen soll.
  - [Metriken und Dimensionen von Amazon S3](#)
  - [Überwachen von Metriken für in einer RDS Amazon-Instance](#)
  - [Überwachen der Datenbanklast mit Performance Insights auf Amazon RDS](#)
  - [Überblick über „Erweiterte Überwachung“](#)
  - [DynamoDB-Metriken und -Dimensionen](#)
  - [Überwachen von DynamoDB Accelerator](#)
  - [Überwachen von Amazon MemoryDB mit Amazon CloudWatch](#)
  - [Welche Metriken sollte ich überwachen?](#)
  - [Überwachen der Amazon-Redshift-Cluster-Leistung](#)

- [Timestream-Metriken und Dimensionen](#)
- [CloudWatch Amazon-Metriken für Amazon Aurora](#)
- [Protokollierung und Überwachung in Amazon Keyspaces \(für Apache Cassandra\)](#)
- [Überwachen von Amazon-Neptune-Ressourcen](#)
- Verwenden Sie eine zugelassene Protokollierungs- und Überwachungslösung, um diese Metriken zu erfassen. [Amazon CloudWatch](#) kann Metriken für alle Ressourcen in Ihrer Architektur sammeln. Sie können auch benutzerdefinierte Metriken erfassen und in Oberflächen-, Geschäfts- oder abgeleiteten Metriken veröffentlichen. Verwenden Sie CloudWatch Lösungen von Drittanbietern, um Alarme einzurichten, die anzeigen, wenn Schwellenwerte überschritten werden.
- Prüfen Sie, ob die Datenspeicherüberwachung von einer Machine-Learning-Lösung profitieren kann, die Leistungsanomalien erkennt.
  - [Amazon DevOps Guru for Amazon RDS](#) bietet Einblick in Leistungsprobleme und gibt Empfehlungen für Korrekturmaßnahmen.
- Konfigurieren Sie die Datenaufbewahrung in Ihrer Überwachungs- und Protokollierungslösung so, dass sie Ihren Sicherheits- und Betriebszielen entspricht.
  - [Standardmäßige Datenspeicherung für Metriken CloudWatch](#)
  - [Standardmäßige Datenspeicherung für CloudWatch Protokolle](#)

## Ressourcen

### Zugehörige Dokumente:

- [AWS -Datenbank-Caching](#)
- [Die zehn besten Leistungstipps für Amazon Athena](#)
- [Bewährte Methoden mit Amazon Aurora](#)
- [DynamoDB Accelerator](#)
- [Bewährte Methoden für Amazon DynamoDB](#)
- [Bewährte Methoden für Amazon Redshift Spectrum](#)
- [Leistung von Amazon Redshift](#)
- [Cloud-Datenbanken mit AWS](#)
- [RDSPerformance Insights von Amazon](#)

### Zugehörige Videos:

- [AWS re:Invent 2022 — Leistungsüberwachung mit Amazon RDS und Aurora, mit Autodesk](#)
- [Überwachung und Optimierung der Datenbankleistung mit Amazon DevOps Guru für Amazon RDS](#)
- [AWS re:Invent 2023 — Was ist neu bei der Dateispeicherung AWS](#)
- [AWS re:Invent 2023 — Tauchen Sie tief in Amazon DynamoDB ein](#)
- [AWS re:Invent 2023 — Aufbau und Optimierung eines Data Lakes auf Amazon S3](#)
- [AWS re:Invent 2023 — Was ist neu bei der Dateispeicherung AWS](#)
- [AWS re:Invent 2023 — Tauchen Sie tief in Amazon DynamoDB ein](#)
- [Bewährte Methoden für die Überwachung von Redis-Workloads auf Amazon ElastiCache](#)

Zugehörige Beispiele:

- [Framework zur AWS -Datensatzerfassung und Sammlung von Metriken](#)
- [Workshop RDS zur Amazon-Überwachung](#)
- [AWS Workshop zu speziell entwickelten Datenbanken](#)

PERF03-BP04 Implementieren Sie Strategien zur Verbesserung der Abfrageleistung im Datenspeicher

Implementieren Sie Strategien zur Datenoptimierung und Verbesserung der Datenabfrage, um mehr Skalierbarkeit und eine effizientere Leistung für Ihre Workloads zu erzielen.

Typische Anti-Muster:

- Sie partitionieren keine Daten in Ihrem Datenspeicher.
- Sie speichern Daten in nur einem Dateiformat in Ihrem Datenspeicher.
- Sie verwenden keine Indizes in Ihrem Datenspeicher.

Vorteile der Nutzung dieser bewährten Methode: Die Optimierung der Daten- und Abfrageleistung führt zu mehr Effizienz, niedrigeren Kosten und einer verbesserten Benutzererfahrung.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Mittel

Implementierungsleitfaden

Daten- und Abfrageoptimierung sind wichtige Aspekte der Leistungseffizienz in einem Datenspeicher, da sie sich auf die Leistung und Reaktionsfähigkeit der gesamten Cloud-Workload auswirken.

Nicht optimierte Abfragen können zu einem höheren Ressourcenverbrauch und Engpässen führen, wodurch die Gesamteffizienz eines Datenspeichers beeinträchtigt wird.

Die Datenoptimierung umfasst mehrere Techniken, um eine effiziente Datenspeicherung und einen effizienten Datenzugriff zu gewährleisten. Dies trägt auch dazu bei, die Abfrageleistung in einem Datenspeicher zu verbessern. Zu den wichtigsten Strategien gehören Datenpartitionierung, Datenkomprimierung und Datendenormalisierung, mit denen Daten sowohl für die Speicherung als auch für den Zugriff optimiert werden können.

### Implementierungsschritte

- Verstehen und analysieren Sie die kritischen Datenabfragen, die in Ihrem Datenspeicher durchgeführt werden.
- Identifizieren Sie die langsamen Abfragen in Ihrem Datenspeicher und verwenden Sie Abfragepläne, um den aktuellen Status zu verstehen.
  - [Analysieren des Abfrageplans in Amazon Redshift](#)
  - [Verwenden von EXPLAIN und EXPLAIN ANALYZE in Athena](#)
- Implementieren Sie Strategien zur Verbesserung der Abfrageleistung. Einige der wichtigsten Strategien sind:
  - Verwendung eines [spaltenförmigen Dateiformats](#) (wie Parquet oder ORC).
  - Komprimieren von Daten im Datenspeicher, um Speicherplatz und E/A-Betrieb zu reduzieren.
  - Datenpartitionierung zur Aufteilung von Daten in kleinere Teile und zur Reduzierung der Zeit für das Scannen von Daten.
    - [Daten in Athena partitionieren](#)
    - [Partitionen und Datenverteilung](#)
  - Datenindizierung für die gemeinsamen Spalten in der Abfrage.
  - Verwenden Sie materialisierte Ansichten für häufige Abfragen.
    - [Materialisierte Ansichten verstehen](#)
    - [Erstellen von materialisierten Ansichten in Amazon Redshift](#)
  - Wählen Sie den richtigen Verknüpfungsvorgang für die Abfrage aus. Wenn Sie zwei Tabellen verknüpfen, geben Sie die größere Tabelle auf der linken Seite der Verknüpfung und die kleinere Tabelle auf der rechten Seite der Verknüpfung an.
  - Verteilte Caching-Lösung zur Verbesserung der Latenz und zur Reduzierung der Anzahl von Datenbank-E/A-Vorgängen.
  - Regelmäßige Wartung wie [Bereinigung](#), Neuindizierung und [Ausführen von Statistiken](#).

- Experimentieren und testen Sie Strategien in einer Nicht-Produktionsumgebung.

## Ressourcen

### Zugehörige Dokumente:

- [Bewährte Methoden mit Amazon Aurora](#)
- [Leistung von Amazon Redshift](#)
- [Die zehn besten Leistungstipps für Amazon Athena](#)
- [AWS -Datenbank-Caching](#)
- [Bewährte Methoden für die Implementierung von Amazon ElastiCache](#)
- [Daten in Athena partitionieren](#)

### Zugehörige Videos:

- [AWS re:Invent 2023 — bewährte Methoden zur Optimierung der AWS Speicherkosten](#)
- [AWS re:Invent 2022 — Leistungsüberwachung mit Amazon RDS und Aurora, mit Autodesk](#)
- [Optimize Amazon Athena Queries with New Query Analysis Tools](#)

### Zugehörige Beispiele:

- [Amazon S3 Select – Abfragen von Daten ohne Server oder Datenbanken](#)
- [AWS Workshop zu speziell entwickelten Datenbanken](#)

PERF03-BP05 Implementieren Sie Datenzugriffsmuster, die Caching nutzen

Implementieren Sie Zugriffsmuster, die vom Daten-Caching profitieren, damit häufig aufgerufene Daten schnell abgerufen werden können.

### Typische Anti-Muster:

- Sie speichern Daten, die sich häufig ändern.
- Sie verlassen sich auf zwischengespeicherte Daten, als ob sie dauerhaft gespeichert und immer verfügbar wären.
- Sie berücksichtigen nicht die Konsistenz Ihrer zwischengespeicherten Daten.



- Sie überwachen die Effizienz Ihrer Caching-Implementierung nicht.

Vorteile der Nutzung dieser bewährten Methode: Das Speichern von Daten in einem Cache kann die Leselatenz, den Lesedurchsatz, die Benutzererfahrung und die Gesamteffizienz verbessern sowie die Kosten senken.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Mittel

### Implementierungsleitfaden

Ein Cache ist eine Software- oder Hardwarekomponente zum Speichern von Daten, damit zukünftige Abfragen derselben Daten schneller oder effizienter verarbeitet werden können. Die in einem Cache gespeicherten Daten können bei Verlust rekonstruiert werden, indem eine frühere Berechnung wiederholt wird oder die Daten aus einem anderen Datenspeicher abgerufen werden.

Das Caching von Daten kann eine der effektivsten Strategien sein, um die allgemeine Anwendungsleistung zu verbessern und die Belastung Ihrer zugrunde liegenden primären Datenquellen zu verringern. Daten können auf mehreren Ebenen in der Anwendung zwischengespeichert werden, z. B. innerhalb der Anwendung durch Remote-Aufrufe (so genanntes clientseitiges Caching) oder durch Verwendung eines schnellen sekundären Services zur Speicherung der Daten (so genanntes Remote-Caching).

### Clientseitiges Caching

Beim clientseitigen Caching kann jeder Client (eine Anwendung oder ein Service, die bzw. der den Backend-Datenspeicher abfragt) die Ergebnisse seiner eindeutigen Abfragen lokal für einen bestimmten Zeitraum speichern. So kann die Anzahl der Anfragen an einen Datenspeicher im Netzwerk reduziert werden, da zuerst der lokale Client-Cache überprüft wird. Wenn die Ergebnisse nicht vorhanden sind, kann die Anwendung den Datenspeicher abfragen und diese Ergebnisse lokal speichern. Dieses Muster ermöglicht es jedem Client, Daten am nächstgelegenen Ort (dem Client selbst) zu speichern, was zur geringstmöglichen Latenz führt. Clients können auch weiterhin einige Abfragen bearbeiten, wenn der Backend-Datenspeicher nicht verfügbar ist, wodurch die Verfügbarkeit des Gesamtsystems erhöht wird.

Ein Nachteil dieses Ansatzes besteht darin, dass bei Beteiligung mehrerer Clients diese möglicherweise dieselben zwischengespeicherten Daten lokal speichern. Dies führt sowohl zu doppelten Speichervorgängen als auch zu Dateninkonsistenzen zwischen diesen Clients. So kann z. B. ein Client die Ergebnisse einer Abfrage zwischenspeichern und eine Minute später führt ein anderer Client dieselbe Abfrage aus und erhält ein anderes Ergebnis.

## Remote-Caching

Um das Problem der doppelten Daten zwischen den Clients zu lösen, kann ein schneller externer Service oder ein Remote-Cache verwendet werden, um die abgefragten Daten zu speichern. Anstatt einen lokalen Datenspeicher zu überprüfen, prüft jeder Client den Remote-Cache, bevor er den Backend-Datenspeicher abfragt. Diese Strategie ermöglicht konsistentere Antworten zwischen den Clients, eine bessere Effizienz der gespeicherten Daten und ein höheres Volumen an zwischengespeicherten Daten, da der Speicherplatz unabhängig von den Clients skaliert wird.

Der Nachteil eines Remote-Caches besteht darin, dass das Gesamtsystem möglicherweise eine höhere Latenz aufweist, da ein zusätzlicher Netzwerk-Hop erforderlich ist, um den Remote-Cache zu überprüfen. Das clientseitige Caching kann in Kombination mit dem Remote-Caching verwendet werden, um ein mehrstufiges Caching zu implementieren und die Latenz zu verbessern.

### Implementierungsschritte

- Identifizieren Sie Datenbanken APIs und Netzwerkdienste, die vom Caching profitieren könnten. Dienste, die eine hohe Leselast haben, ein hohes read-to-write Verhältnis aufweisen oder deren Skalierung teuer ist, kommen für das Caching in Frage.
  - [Datenbank-Caching](#)
  - [Aktivierung von API Caching zur Verbesserung der Reaktionsfähigkeit](#)
- Identifizieren Sie die geeignete Caching-Strategie, die am besten zu Ihrem Zugriffsmuster passt.
  - [Caching-Strategien](#)
  - [AWS -Caching-Lösungen](#)
- Befolgen Sie die [bewährten Methoden für das Caching](#) für Ihren Datenspeicher.
- Konfigurieren Sie eine Strategie zur Cache-Invalidierung, z. B. a time-to-live (TTL), für alle Daten, um ein Gleichgewicht zwischen der Aktualität der Daten und der Verringerung des Drucks auf den Backend-Datenspeicher herzustellen.
- Aktivieren Sie Features wie automatische Verbindungswiederholungen, exponentielles Backoff, clientseitige Timeouts und Verbindungspooling beim Client, sofern verfügbar, um die Leistung und Zuverlässigkeit zu verbessern.
  - [Bewährte Methoden: Redis-Kunden und Amazon ElastiCache \(OSSRedis\)](#)
- Überwachen Sie die Cache-Trefferrate mit einem Ziel von mindestens 80 %. Niedrigere Werte können auf eine unzureichende Cache-Größe oder ein Zugriffsmuster hinweisen, das nicht vom Caching profitiert.
  - [Welche Metriken sollte ich überwachen?](#)

- [Bewährte Methoden für die Überwachung von Redis-Workloads auf Amazon ElastiCache](#)
- [Überwachung von Best Practices mit Amazon ElastiCache \(RedisOSS\) mithilfe von Amazon CloudWatch](#)
- Implementieren Sie die [Datenreplikation](#), um Lesevorgänge auf mehrere Instances auszulagern und die Leseleistung und Verfügbarkeit von Daten zu verbessern.

## Ressourcen

### Zugehörige Dokumente:

- [Verwenden des Amazon ElastiCache Well-Architected-Objektivs](#)
- [Überwachung von Best Practices mit Amazon ElastiCache \(RedisOSS\) mithilfe von Amazon CloudWatch](#)
- [Welche Metriken sollte ich überwachen?](#)
- [ElastiCache Whitepaper „Leistung im großen Maßstab“ mit Amazon](#)
- [Caching-Herausforderungen und -Strategien](#)

### Zugehörige Videos:

- [ElastiCache Amazon-Lernpfad](#)
- [Erfolgreiches Design mit den ElastiCache Best Practices von Amazon](#)
- [AWS re:Invent 2020 — Erfolgreiches Design mit den Best Practices von Amazon ElastiCache](#)
- [AWS re:Invent 2023 — \[LAUNCH\] Wir stellen vor: Amazon Serverless ElastiCache](#)
- [AWS re:Invent 2022 — 5 großartige Möglichkeiten, Ihre Datenschicht mit Redis neu zu erfinden](#)
- [AWS re:Invent 2021 — Tiefer Einblick in Amazon ElastiCache \(Redis\) OSS](#)

### Zugehörige Beispiele:

- [Steigerung der Leistung meiner SQL Datenbank mit Amazon ElastiCache \(RedisOSS\)](#)

## Netzwerk und Bereitstellung von Inhalten

### Fragen

- [PERF4. Wie wählen und konfigurieren Sie Netzwerkressourcen in Ihrem Workload?](#)

## PERF4. Wie wählen und konfigurieren Sie Netzwerkressourcen in Ihrem Workload?

Welche Netzwerklösung für eine Workload optimal ist, richtet sich nach der Latenz, dem erforderlichen Durchsatz, dem Jitter und der Bandbreite. Die Standortoptionen sind von den physischen Einschränkungen abhängig, z. B. von Benutzer- oder On-Premises-Ressourcen. Diese Einschränkungen können durch Edge-Standorte oder die Ressourcenplatzierung wettgemacht werden.

### Bewährte Methoden

- [PERF04-BP01 Verstehen Sie, wie sich Netzwerke auf die Leistung auswirken](#)
- [PERF04-BP02 Evaluieren Sie die verfügbaren Netzwerkfunktionen](#)
- [PERF04-BP03 Wählen Sie die passende dedizierte Konnektivität oder VPN für Ihren Workload](#)
- [PERF04-BP04 Verwenden Sie Load Balancing, um den Verkehr auf mehrere Ressourcen zu verteilen](#)
- [PERF04-BP05 Wählen Sie Netzwerkprotokolle, um die Leistung zu verbessern](#)
- [PERF04-BP06 Wählen Sie den Standort Ihres Workloads basierend auf den Netzwerkanforderungen](#)
- [PERF04-BP07 Optimieren Sie die Netzwerkkonfiguration auf der Grundlage von Metriken](#)

### PERF04-BP01 Verstehen Sie, wie sich Netzwerke auf die Leistung auswirken

Analysieren und verstehen Sie, wie sich netzwerkbezogene Entscheidungen auf Ihre Workload auswirken, sodass Sie eine effiziente Leistung und ein verbessertes Benutzererlebnis erzielen können.

### Typische Anti-Muster:

- Der gesamte Datenverkehr fließt durch Ihre bestehenden Rechenzentren.
- Sie leiten den gesamten Datenverkehr durch zentrale Firewalls, anstatt cloudnative Netzwerksicherheitstools zu verwenden.
- Sie stellen AWS Direct Connect Verbindungen bereit, ohne die tatsächlichen Nutzungsanforderungen zu verstehen.
- Sie berücksichtigen beim Definieren Ihrer Netzwerklösungen die Workload-Eigenschaften und den Verschlüsselungsaufwand nicht.
- Sie verwenden On-Premises-Konzepte und -Strategien für Netzwerklösungen in der Cloud.

Vorteile der Nutzung dieser bewährten Methode: Indem Sie verstehen, wie das Netzwerk die Workload-Leistung beeinflusst, können Sie potenzielle Engpässe erkennen, die Benutzererfahrung verbessern, die Zuverlässigkeit erhöhen und den Betriebsaufwand verringern, während sich die Workload verändert.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Hoch

### Implementierungsleitfaden

Das Netzwerk ist für die Verbindung zwischen Anwendungskomponenten, Cloud-Services, Edge-Netzwerken und On-Premises-Daten verantwortlich und kann daher die Workload-Leistung wesentlich beeinflussen. Die Benutzererfahrung kann nicht nur durch die Workload-Leistung, sondern auch durch Netzwerklatenz, Bandbreite, Protokolle, Standort, Netzwerküberlastungen, Jitter, Durchsatz und Routingregeln beeinträchtigt werden.

Sie haben eine dokumentierte Liste an Netzwerkanforderungen der Workload, einschließlich Latenz, Paketgröße, Routingregeln, Protokolle und unterstützender Datenverkehrsmuster. Sie überprüfen alle verfügbaren Netzwerklösungen und identifizieren, welcher Service den Netzwerkmerkmalen Ihrer Workload entspricht. Da cloudbasierte Netzwerke schnell geändert werden können, müssen Sie Ihre Netzwerkarchitektur im Laufe der Zeit weiterentwickeln, um die effiziente Leistung zu verbessern.

### Implementierungsschritte:

- Definieren und dokumentieren Sie die Anforderungen an die Netzwerkleistung, einschließlich Metriken wie Netzwerklatenz, Bandbreite, Protokolle, Standorte, Datenverkehrsmuster (Spitzen und Frequenz), Durchsatz, Verschlüsselung, Überprüfung und Routingregeln.
- Erfahren Sie mehr über wichtige AWS Netzwerkdienste wie [VPCs](#), [AWS Direct Connect](#), [Elastic Load Balancing \(ELB\)](#) und [Amazon Route 53](#).
- Erfassen Sie die folgenden wichtigen Netzwerkmerkmale:

Merkmale	Tools und Metriken
Grundlegende Netzwerkmerkmale	<ul style="list-style-type: none"> <li>• <a href="#">VPCFlow-Protokolle</a></li> <li>• <a href="#">AWS Transit Gateway Flow Logs</a></li> <li>• <a href="#">AWS Transit Gateway Metriken</a></li> <li>• <a href="#">AWS PrivateLink Metriken</a></li> </ul>
Merkmale von Anwendungsnetzwerken	<ul style="list-style-type: none"> <li>• <a href="#">Elastic Fabric Adapter</a></li> </ul>

Merkmale	Tools und Metriken
	<ul style="list-style-type: none"> <li>• <a href="#">AWS App Mesh Metriken</a></li> <li>• <a href="#">Amazon API Gateway-Metriken</a></li> </ul>
Merkmale von Edge-Netzwerken	<ul style="list-style-type: none"> <li>• <a href="#">CloudFront Amazon-Metriken</a></li> <li>• <a href="#">Amazon-Route-53-Metriken</a></li> <li>• <a href="#">AWS Global Accelerator Metriken</a></li> </ul>
Merkmale hybrider Netzwerke	<ul style="list-style-type: none"> <li>• <a href="#">AWS Direct Connect Metriken</a></li> <li>• <a href="#">AWS Site-to-Site VPN Metriken</a></li> <li>• <a href="#">AWS Client VPN Metriken</a></li> <li>• <a href="#">AWS Cloud WANMetriken</a></li> </ul>
Merkmale von Sicherheitsnetzwerken	<ul style="list-style-type: none"> <li>• <a href="#">AWS ShieldAWS WAF, und AWS Network Firewall Metriken</a></li> </ul>
Nachverfolgungsmerkmale	<ul style="list-style-type: none"> <li>• <a href="#">AWS X-Ray</a></li> <li>• <a href="#">VPCReachability Analyzer</a></li> <li>• <a href="#">Network Access Analyzer</a></li> <li>• <a href="#">Amazon Inspector</a></li> <li>• <a href="#">Amazon CloudWatch RUM</a></li> </ul>

- Benchmarks für die Netzwerkleistung festlegen und testen:
  - [Vergleichen](#) Sie den Netzwerkdurchsatz, da einige Faktoren die EC2 Amazon-Netzwerkleistung beeinflussen können, wenn sich Instances in denselben befindenVPC. Messen Sie die Netzwerkbandbreite zwischen Amazon EC2 Linux-Instances auf dieselbe WeiseVPC.
  - Führen Sie [Lasttests](#) durch, um mit Netzwerklösungen und -optionen zu experimentieren.

## Ressourcen

### Zugehörige Dokumente:

- [Application Load Balancer](#)
- [EC2Verbessertes Networking unter Linux](#)
- [EC2Verbessertes Networking unter Windows](#)

- [EC2Platzierungsgruppen](#)
- [Aktivierung von Enhanced Networking mit dem Elastic Network Adapter \(ENA\) auf Linux-Instances](#)
- [Network Load Balancer](#)
- [Netzwerkprodukte mit AWS](#)
- [Transit-Gateway](#)
- [Umstellung auf latenzbasiertes Routing in Amazon Route 53](#)
- [VPC-Endpunkte](#)

#### Zugehörige Videos:

- [AWS re:Invent 2023 — Grundlagen der Vernetzung AWS](#)
- [AWS re:Invent 2023 — Was können Netzwerke für Ihre Anwendung tun?](#)
- [AWS re:Invent 2023 — Fortschrittliche VPC Designs und neue Funktionen](#)
- [AWS re:Invent 2023 — Ein Leitfaden für Entwickler zu Cloud-Netzwerken](#)
- [AWS re:Invent 2019 — Konnektivität zu und hybride AWS Netzwerkarchitekturen AWS](#)
- [AWS re:Invent 2019 — Optimierung der Netzwerkleistung für Amazon-Instances EC2](#)
- [AWS Summit Online — Verbessern Sie die globale Netzwerkleistung für Anwendungen](#)
- [AWS re:Invent 2020 — Bewährte Methoden und Tipps zum Netzwerken mit dem Well-Architected Framework](#)
- [AWS re:Invent 2020 — AWS Bewährte Netzwerkpraktiken bei groß angelegten Migrationen](#)

#### Zugehörige Beispiele:

- [AWS Transit Gateway und skalierbare Sicherheitslösungen](#)
- [AWS Netzwerk-Workshops](#)
- [Praktischer Workshop zur Netzwerk-Firewall](#)
- [Überwachung und Diagnose Ihres Netzwerks am AWS](#)
- [Suchen und Beheben von Netzwerkfehlfunktionen auf AWS](#)

PERF04-BP02 Evaluieren Sie die verfügbaren Netzwerkfunktionen

Prüfen Sie die Netzwerk-Features in der Cloud, mit denen die Leistung unter Umständen verbessert werden kann. Messen Sie die Auswirkungen der Features anhand von Tests, Metriken und Analysen.

Nutzen Sie beispielsweise die verfügbaren Features auf Netzwerkebene, um die Latenz, die Netzwerkentfernung oder den Jitter zu reduzieren.

Typische Anti-Muster:

- Sie bleiben innerhalb einer Region, da sich Ihre Firmenzentrale dort befindet.
- Sie verwenden Firewalls anstelle von Sicherheitsgruppen, um den Datenverkehr zu filtern.
- Sie verlassen sich auf TLS die Überprüfung des Datenverkehrs, anstatt sich auf Sicherheitsgruppen, Endpunktrichtlinien und andere Cloud-native Funktionen zu verlassen.
- Sie nutzen nur eine subnetzbasierte Segmentierung anstelle von Sicherheitsgruppen.

Vorteile der Nutzung dieser bewährten Methode: Wenn Sie alle Service-Features und Optionen evaluieren, kann dies die Workload-Leistung verbessern, die Infrastrukturkosten senken, den Verwaltungsaufwand für die Workload reduzieren und die allgemeine Sicherheit erhöhen. Sie können den globalen AWS Backbone nutzen, um Ihren Kunden ein optimales Netzwerkerlebnis zu bieten.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Hoch

Implementierungsleitfaden

AWS bietet Dienste wie [AWS Global Accelerator](#) an CloudFront, die zur Verbesserung der Netzwerkleistung beitragen können, während die meisten AWS Dienste über Produktfunktionen (wie die [Amazon S3 Transfer Acceleration Acceleration-Funktion](#)) zur Optimierung des Netzwerkverkehrs verfügen.

Sehen Sie sich die verfügbaren Konfigurationsoptionen für das Netzwerk an und finden Sie heraus, wie sich diese auf Ihre Workload auswirken. Die Leistungsoptimierung hängt davon ab, wie diese Optionen mit Ihrer Architektur interagieren und welche Auswirkungen sie auf die gemessene Leistung und auf die Benutzererfahrung haben.

Implementierungsschritte

- Erstellen Sie eine Liste der Workload-Komponenten.
  - Erwägen Sie [AWS Cloud WAN](#) den Einsatz zum Aufbau, zur Verwaltung und Überwachung Ihres Unternehmensnetzwerks, wenn Sie ein einheitliches globales Netzwerk aufbauen.
  - Überwachen Sie Ihre globalen Netzwerke und Kernnetzwerke mit [Amazon CloudWatch Logs-Metriken](#). Nutzen Sie [Amazon CloudWatch RUM](#), das Einblicke bietet, um das digitale Erlebnis der Nutzer zu identifizieren, zu verstehen und zu verbessern.



- Sehen Sie sich die aggregierte Netzwerklatenz zwischen AWS-Regionen und Availability Zones sowie innerhalb der einzelnen Availability Zones an, [AWS Network Manager](#) um einen Einblick in den Zusammenhang zwischen Ihrer Anwendungsleistung und der Leistung des zugrunde liegenden AWS Netzwerks zu erhalten.
- Verwenden Sie ein vorhandenes Tool für die Konfigurationsverwaltungsdatenbank (CMDB) oder einen Dienst [AWS Config](#), um beispielsweise eine Bestandsaufnahme Ihrer Arbeitslast und deren Konfiguration zu erstellen.
- Wenn es sich um eine bestehende Workload handelt, ermitteln und dokumentieren Sie die Benchmark für Ihre Leistungsmetriken. Konzentrieren Sie sich dabei auf Engpässe und Bereiche mit Verbesserungspotenzial. Leistungsbezogene Netzwerkmetriken werden je nach geschäftlichen Anforderungen und Workload-Merkmalen für die einzelnen Workloads unterschiedlich sein. Für den Anfang könnte die Prüfung folgender Metriken für Ihre Workload wichtig sein: Bandbreite, Latenz, Paketverlust, Jitter und erneute Übertragungen.
- Wenn es sich um eine neue Workload handelt, führen Sie [Lasttests](#) durch, um Leistungsengpässe zu ermitteln.
- Prüfen Sie für die ermittelten Leistungsengpässe die Konfigurationsoptionen Ihrer Lösungen, um Möglichkeiten zur Leistungsverbesserung zu finden. Informieren Sie sich über die folgenden wichtigen Netzwerkoptionen und -Features:

Verbesserungsmöglichkeit	Lösung
Netzwerkpfad oder -routen	Verwenden Sie <a href="#">Network Access Analyzer</a> , um Pfade oder Routen zu ermitteln.
Netzwerkprotokolle	Siehe <a href="#">PERF04-BP05 Wählen Sie Netzwerkprotokolle, um die Leistung zu verbessern</a>
Netzwerktopologie	Bewerten Sie Ihre betrieblichen und leistungsbezogenen Kompromisse zwischen <a href="#">VPC Peering</a> und <a href="#">AWS Transit Gateway</a> bei der Verbindung mehrerer Konten. AWS Transit Gateway vereinfacht die Art und Weise, wie Sie all Ihre Netzwerke miteinander verbinden VPCs, was sich über Tausende von AWS-Konten Netzwerken bis hin zu lokalen Netzwerken erstrecken kann. Teilen Sie

Verbesserungsmöglichkeit	Lösung
	<p>Ihre Daten AWS Transit Gateway zwischen mehreren Konten mithilfe von. <a href="#">AWS Resource Access Manager</a></p> <p>Siehe <a href="#">PERF04-BP03 Wählen Sie die passende dedizierte Konnektivität oder VPN für Ihren Workload</a></p>
Netzwerksservices	<p><a href="#">AWS Global Accelerator</a> ist ein Netzwerkdienst, der die Leistung des Datenverkehrs Ihrer Benutzer mithilfe der AWS globalen Netzwerkinfrastruktur um bis zu 60% verbessert.</p> <p><a href="#">Amazon CloudFront</a> kann die Leistung Ihrer Workloads, die Bereitstellung von Inhalten und die Latenz weltweit verbessern.</p> <p>Verwenden Sie <a href="#">Lambda @edge</a>, um Funktionen auszuführen, die den Inhalt so anpassen, CloudFront dass er den Benutzern näher kommt, die Latenz reduzieren und die Leistung verbessern.</p> <p>Amazon Route 53 bietet Optionen für <a href="#">latenzbasiertes Routing</a>, <a href="#">Geolocation-Routing</a>, <a href="#">Geoproximity-Routing</a> und <a href="#">IP-basiertes Routing</a>, mit denen Sie die Leistung Ihrer Workloads für eine globale Zielgruppe verbessern können. Ermitteln Sie, welche Routing-Option Ihre Workload-Leistung optimieren würde. Prüfen Sie dazu Ihren Workload-Datenverkehr und den Benutzers tandort bei der globalen Verteilung Ihrer Workload.</p>

Verbesserungsmöglichkeit	Lösung
Speicherressourcen-Features	<p><a href="#">Amazon S3 Transfer Acceleration</a> ist eine Funktion, mit der externe Benutzer von den Netzwerkoptimierungen profitieren können CloudFront , um Daten auf Amazon S3 hochzuladen. Dies erleichtert die Übertragung großer Datenmengen von Remotestandorten ohne spezielle Konnektivität zur AWS Cloud.</p> <p><a href="#">Multi-Region-Zugangspunkte in Amazon S3</a> replizieren Inhalte in mehreren Regionen und vereinfachen die Workload durch die Bereitstellung eines Zugangspunkts. Bei Verwendung eines Multi-Region-Zugangspunkts können Sie Daten anfordern oder in Amazon S3 schreiben, wobei der Service den Bucket mit der geringsten Latenz ermittelt.</p>

Verbesserungsmöglichkeit	Lösung
Compute-Ressourcen-Features	<p><a href="#">Elastic Network Interfaces (ENA)</a>, die von EC2 Amazon-Instances, Containern und Lambda-Funktionen verwendet werden, sind pro Flow begrenzt. Überprüfen Sie Ihre Platzierungsgruppen, um Ihren <a href="#">EC2Netzwe</a> <a href="#">rkdurchsatz</a> zu optimieren. Um Engpässe auf Pro-Fluss-Basis zu vermeiden, sollten Sie Ihre Anwendung so gestalten, dass mehrere Flüsse verwendet werden. Verwenden CloudWatch Sie Metrics und <a href="#">Ethtool</a>, um Ihre rechnerbezogenen Netzwerkmetriken zu überwachen und sich einen Überblick darüber zu verschaffen. Der <code>ethtool</code> Befehl ist im ENA Treiber enthalten und stellt zusätzliche netzwerkbezogene Metriken zur Verfügung, die als <a href="#">benutzerdefinierte</a> Metrik veröffentlicht werden können. CloudWatch</p> <p><a href="#">Amazon Elastic Network Adapters (ENA)</a> bieten weitere Optimierungen, indem sie einen besseren Durchsatz für Ihre Instances innerhalb einer <a href="#">Cluster-Platzierungsgruppe</a> bieten.</p> <p><a href="#">Elastic Fabric Adapter (EFA)</a> ist eine Netzwerkschnittstelle für EC2 Amazon-Instances, mit der Sie Workloads ausführen können, die ein hohes Maß an Kommunikation zwischen den Knoten erfordern, und zwar in großem Umfang. AWS</p> <p><a href="#">EBSAmazon-optimierte Instances verwenden einen optimierten Konfigurations-Stack</a> und bieten zusätzliche, dedizierte Kapazität, um die EBS Amazon-I/O zu erhöhen.</p>

## Ressourcen

### Zugehörige Dokumente:

- [Application Load Balancer](#)
- [EC2Verbessertes Networking unter Linux](#)
- [EC2Verbessertes Networking unter Windows](#)
- [EC2Platzierungsgruppen](#)
- [Aktivierung von Enhanced Networking mit dem Elastic Network Adapter \(ENA\) auf Linux-Instances](#)
- [Network Load Balancer](#)
- [Netzwerkprodukte mit AWS](#)
- [Umstellung auf latenzbasiertes Routing in Amazon Route 53](#)
- [VPC-Endpunkte](#)
- [VPC-Flow-Protokolle](#)

### Zugehörige Videos:

- [AWS re:Invent 2023 — Bereit für das, was als Nächstes kommt? Gestaltung von Netzwerken für Wachstum und Flexibilität](#)
- [AWS re:Invent 2023 — Fortschrittliche VPC Designs und neue Funktionen](#)
- [AWS re:Invent 2023 — Ein Leitfaden für Entwickler zum Thema Cloud-Netzwerke](#)
- [AWS re:Invent 2022 — Tauchen Sie tief in die Netzwerkinfrastruktur ein AWS](#)
- [AWS re:Invent 2019 — Konnektivität zu und hybride AWS Netzwerkarchitekturen AWS](#)
- [AWS re:Invent 2018 — Optimierung der Netzwerkleistung für Amazon-Instances EC2](#)
- [AWS Global Accelerator](#)

### Zugehörige Beispiele:

- [AWS Transit Gateway und skalierbare Sicherheitslösungen](#)
- [AWS Netzwerk-Workshops](#)
- [Überwachung und Diagnose Ihres Netzwerks](#)
- [Auffinden und Beheben von Netzwerkfehlkonfigurationen auf AWS](#)

## PERF04-BP03 Wählen Sie die passende dedizierte Konnektivität oder VPN für Ihren Workload

Wenn Hybrid-Konnektivität für die Verbindung von On-Premises- und Cloud-Ressourcen erforderlich ist, stellen Sie ausreichend Bandbreite bereit, um Ihre Leistungsanforderungen zu erfüllen. Schätzen Sie die Anforderungen an Bandbreite und Latenz für Ihre hybride Workload ab. Diese Zahlen dienen als Grundlage für die Größenanpassung.

Typische Anti-Muster:

- Sie evaluieren nur VPN Lösungen für Ihre Netzwerkverschlüsselungsanforderungen.
- Sie bewerten keine Optionen für Sicherung oder redundante Verbindungen.
- Sie identifizieren nicht alle Workload-Anforderungen (Verschlüsselung, Protokoll, Bandbreite und Traffic-Bedarf).

Vorteile der Nutzung dieser bewährten Methode: Durch die Auswahl und Konfiguration geeigneter Konnektivitätslösungen wird die Zuverlässigkeit Ihrer Workloads erhöht und die Leistung maximiert. Durch die Identifizierung der Workload-Anforderungen, die vorausschauende Planung und die Evaluierung von Hybridlösungen können Sie teure physische Netzwerkänderungen und den Betriebsaufwand minimieren und gleichzeitig Ihre Kosten erhöhen time-to-value.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Hoch

Implementierungsleitfaden

Entwickeln Sie eine hybride Netzwerkarchitektur, die auf Ihren Bandbreitenanforderungen basiert. [AWS Direct Connect](#) ermöglicht es Ihnen, Ihr On-Premises-Netzwerk privat mit AWS zu verbinden. Sie ist geeignet, wenn Sie eine hohe Bandbreite und eine geringe Latenz bei gleichbleibender Leistung benötigen. Eine VPN Verbindung stellt eine sichere Verbindung über das Internet her. Sie wird verwendet, wenn lediglich eine temporäre Verbindung erforderlich ist, wenn die Kosten eine Rolle spielen, oder wenn bei der Verwendung von AWS Direct Connect darauf gewartet wird, dass eine resiliente physische Netzwerkkonnektivität hergestellt wird.

Wenn Ihre Bandbreitenanforderungen hoch sind, könnten Sie mehrere AWS Direct Connect oder mehrere VPN Dienste in Betracht ziehen. Für den Datenverkehr kann ein Lastenausgleich zwischen Diensten vorgenommen werden, obwohl wir VPN aufgrund der Latenz AWS Direct Connect - und Bandbreitenunterschiede keinen Lastenausgleich zwischen und empfehlen.

Implementierungsschritte

- Schätzen Sie die Anforderungen an Bandbreite und Latenz für Ihre bestehenden Anwendungen ab.

- Nutzen Sie für bestehende Workloads, auf die umgestellt wird AWS, die Daten aus Ihren internen Netzwerküberwachungssystemen.
- Bei neuen oder bestehenden Workloads, für die Sie keine Monitoring-Daten haben, beraten Sie sich mit den Besitzern der Produkte, um angemessene Metriken für die Leistung zu bestimmen und ein gutes Benutzererlebnis zu gewährleisten.
- Wählen Sie eine dedizierte Verbindung oder VPN als Konnektivitätsoption. Basierend auf allen Workload-Anforderungen (Verschlüsselung, Bandbreite und Datenverkehrsanforderungen) können Sie entweder AWS Direct Connect oder [AWS VPN](#)(oder beides) wählen. Das folgende Diagramm kann Ihnen bei der Wahl der geeigneten Verbindungsart helfen.
- [AWS Direct Connect](#) liefert dedizierte Konnektivität für die AWS -Umgebung, von 50 Mbit/s bis zu 100 Gbit/s, entweder über dedizierte Verbindungen oder über gehostete Verbindungen. So erhalten Sie eine verwaltete und kontrollierte Latenz und bereitgestellte Bandbreite, damit sich Ihre Workload effizient mit anderen Umgebungen verbinden kann. Mithilfe von AWS Direct Connect Partnern können Sie end-to-end Konnektivität von mehreren Umgebungen aus nutzen und so ein erweitertes Netzwerk mit gleichbleibender Leistung bereitstellen. AWS ermöglicht die Skalierung der Bandbreite für Direktverbindungsverbindungen mit entweder systemeigenen 100 Gbit/s, Link Aggregation Group (LAG) oder BGP Equal-Cost Multipath (). ECMP
- Der AWS [Site-to-Site VPN](#)bietet einen verwalteten VPN Dienst, der die Internetprotokollsicherheit unterstützt (). IPsec Wenn eine VPN Verbindung hergestellt wird, umfasst jede VPN Verbindung zwei Tunnel für hohe Verfügbarkeit.
- Folgen Sie der AWS Dokumentation, um eine geeignete Verbindungsoption auszuwählen:
  - Wenn Sie sich für die Verwendung entscheiden AWS Direct Connect, wählen Sie die entsprechende Bandbreite für Ihre Konnektivität aus.
  - Wenn Sie an mehreren AWS Site-to-Site VPN Standorten eine Verbindung zu einer herstellen AWS-Region, verwenden Sie eine [beschleunigte Site-to-Site VPN Verbindung](#), um die Netzwerkleistung zu verbessern.
  - Wenn Ihr Netzwerkdesign aus einer IPsec VPN Verbindung über besteht [AWS Direct Connect](#), sollten Sie die Verwendung von Private IP in Betracht ziehen, VPN um die Sicherheit zu erhöhen und eine Segmentierung zu erreichen. [AWS Site-to-Site Private IP VPN](#) wird zusätzlich zur virtuellen Transitschnittstelle (VIF) bereitgestellt.
  - [AWS Direct Connect SiteLink](#)ermöglicht die Einrichtung redundanter Verbindungen mit niedriger Latenz zwischen Ihren Rechenzentren weltweit, indem Daten über den schnellsten Pfad zwischen [AWS Direct Connect Standorten](#) gesendet und umgangen AWS-Regionen werden.

- Überprüfen Sie Ihr Konnektivitäts-Setup, bevor Sie es in der Produktion einsetzen. Führen Sie Sicherheits- und Leistungstests durch, um sicherzustellen, dass das Setup Ihre Anforderungen an Bandbreite, Zuverlässigkeit, Latenz und Compliance erfüllt.
- Überwachen Sie regelmäßig die Leistung und Nutzung Ihrer Konnektivität und optimieren Sie sie bei Bedarf.

## Flussdiagramm zur deterministischen Leistung

### Ressourcen

#### Zugehörige Dokumente:

- [Netzwerkprodukte mit AWS](#)
- [AWS Transit Gateway](#)
- [VPC-Endpunkte](#)
- [Aufbau einer skalierbaren und sicheren VPC AWS Multi-Netzwerk-Infrastruktur](#)
- [Kunde VPN](#)

#### Zugehörige Videos:

- [AWS re:Invent 2023 — Aufbau hybrider Netzwerkkonnektivität mit AWS](#)
- [AWS re:Invent 2023 — Sichere Fernkonnektivität zu AWS](#)
- [AWS re:Invent 2022 — Leistung optimieren mit Amazon CloudFront](#)
- [AWS re:Invent 2019 — Konnektivität zu und hybride AWS Netzwerkarchitekturen AWS](#)
- [AWS re:Invent 2020 — Vernetzen AWS Transit Gateway](#)

#### Zugehörige Beispiele:

- [AWS Transit Gateway und skalierbare Sicherheitslösungen](#)
- [AWS Netzwerk-Workshops](#)



## PERF04-BP04 Verwenden Sie Load Balancing, um den Verkehr auf mehrere Ressourcen zu verteilen

Verteilen Sie den Datenverkehr auf mehrere Ressourcen oder Services, um von der Elastizität der Cloud zu profitieren. Sie können den Lastausgleich auch nutzen, um die Terminierung von Verschlüsselung auszulagern. So lässt sich die Leistung und Zuverlässigkeit optimieren und der Datenverkehr effektiv verwalten und weiterleiten.

Typische Anti-Muster:

- Sie berücksichtigen bei der Wahl des Load-Balancer-Typs nicht die Anforderungen Ihrer Workload.
- Sie nutzen die Features des Load Balancers nicht zur Optimierung der Leistung.
- Die Workload ist direkt mit dem Internet verbunden, ohne dass ein Load Balancer zum Einsatz kommt.
- Sie leiten den gesamten Internetverkehr über vorhandene Load Balancer weiter.
- Sie verwenden generischen TCP Lastenausgleich und sorgen dafür, dass jeder Rechenknoten die Verschlüsselung übernimmtSSL.

Vorteile der Nutzung dieser bewährten Methode: Ein Load Balancer verarbeitet die variierende Last des Anwendungsdatenverkehrs in einer einzigen oder in mehreren Availability Zones und ermöglicht eine hohe Verfügbarkeit, Auto Scaling sowie eine bessere Nutzung für Ihre Workload.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Hoch

Implementierungsleitfaden

Load Balancer fungieren als Eingangspunkt für Ihre Workload und verteilen den Datenverkehr von dort aus auf Ihre Backend-Ziele – wie Computing-Instances oder Container –, um die Nutzung zu verbessern.

Die Wahl des richtigen Load-Balancer-Typs ist der erste Schritt zur Optimierung Ihrer Architektur. Führen Sie zunächst Ihre Workload-Merkmale aufTCP, wie Protokoll (wie HTTP/TLS,, oder WebSockets), Zieltyp (wie Instances, Container oder Serverless), Anwendungsanforderungen (wie lang andauernde Verbindungen, Benutzerauthentifizierung oder Dauerhaftigkeit) und Platzierung (wie Region, Lokale Zone, Außenposten oder zonale Isolation).

AWS bietet mehrere Modelle für Ihre Anwendungen zur Nutzung des Lastenausgleichs. [Application Load Balancer](#) eignet sich am besten für den Lastenausgleich von HTTPS Datenverkehr

HTTP und bietet erweitertes Anforderungsrouting, das auf die Bereitstellung moderner Anwendungsarchitekturen, einschließlich Microservices und Containern, ausgerichtet ist.

[Network Load Balancer](#) eignet sich am besten für den Lastenausgleich von TCP Datenverkehr, bei dem extreme Leistung erforderlich ist. Hiermit lassen sich mit konstant geringer Latenz Millionen Anforderungen pro Sekunde und plötzliche Datenverkehrsspitzen oder schwankende Datenverkehrsmuster verarbeiten.

[Elastic Load Balancing](#) bietet integrierte Zertifikatsverwaltung SSL und/ TLS -entschlüsselung, sodass Sie die SSL Einstellungen des Load Balancers flexibel zentral verwalten und Ihren Workload von CPU intensiver Arbeit entlasten können.

Nachdem Sie sich für den richtigen Load Balancer entschieden haben, können Sie damit beginnen, seine Features zu nutzen, um die Belastung Ihres Backends durch den Datenverkehr zu verringern.

Wenn Sie beispielsweise sowohl Application Load Balancer (ALB) als auch Network Load Balancer (NLB) verwenden, können Sie die SSL TLS /-Verschlüsselung Offloading durchführen. Dies ist eine Möglichkeit, zu verhindern, dass der CPU -intensive TLS Handshake von Ihren Zielen ausgeführt wird, und auch die Zertifikatsverwaltung zu verbessern.

Wenn Sie SSL TLS /Offloading in Ihrem Load Balancer konfigurieren, ist er für die Verschlüsselung des Datenverkehrs von und zu den Clients verantwortlich, während der Datenverkehr unverschlüsselt an Ihre Backends weitergeleitet wird, wodurch Ihre Backend-Ressourcen freigesetzt und die Reaktionszeit für die Clients verbessert wird.

Application Load Balancer kann auch HTTP /2-Datenverkehr bereitstellen, ohne ihn auf Ihren Zielen unterstützen zu müssen. Diese einfache Entscheidung kann die Reaktionszeit Ihrer Anwendung verbessern, da HTTP /2 TCP Verbindungen effizienter nutzt.

Bei der Definition der Architektur sollten Sie die Anforderungen an die Latenz Ihrer Workload berücksichtigen. Wenn Sie beispielsweise eine latenzempfindliche Anwendung haben, können Sie sich für Network Load Balancer mit einer extrem niedrigen Latenz entscheiden. Alternativ können Sie Ihre Workload auch näher an Ihre Kunden heranbringen, indem Sie Application Load Balancer in [AWS Local Zones](#) oder sogar in [AWS Outposts](#) nutzen.

Eine weitere Überlegung für latenzempfindliche Workloads ist der zonenübergreifende Lastausgleich. Beim zonenübergreifenden Lastausgleich nimmt jeder Load-Balancer-Knoten eine Verteilung des Datenverkehrs auf die registrierten Ziele in allen zulässigen Availability Zones vor.

Verwenden Sie die Auto-Scaling-Integration für Ihren Load Balancer. Einer der Schlüssel für ein leistungsfähiges System ist die richtige Größenanpassung Ihrer Backend-Ressourcen. Zu diesem

Zweck können Sie Load-Balancer-Integrationen für Backend-Zielressourcen nutzen. Mithilfe der Load-Balancer-Integration mit Auto-Scaling-Gruppen werden Ziele je nach Bedarf als Reaktion auf den eingehenden Datenverkehr zum Load Balancer hinzugefügt oder aus ihm entfernt. Load Balancer können EKS für containerisierte Workloads auch in [Amazon ECS](#) und [Amazon](#) integriert werden.

- [Amazon ECS — Service-Lastenausgleich](#)
- [Lastenausgleich für Anwendungen bei Amazon EKS](#)
- [Netzwerklastenausgleich bei Amazon EKS](#)

### Implementierungsschritte

- Definieren Sie Ihre Anforderungen an den Lastenausgleich, einschließlich Datenverkehrsvolumen, Verfügbarkeit und Anwendungsskalierbarkeit.
- Wählen Sie den richtigen Load-Balancer-Typ für Ihre Anwendung.
  - Verwenden Sie den Application Load Balancer für HTTP HTTPS /-Workloads.
  - Verwenden Sie Network Load Balancer für HTTP Nicht-Workloads, die auf TCP oder ausgeführt werden. UDP
  - Verwenden Sie eine Kombination aus beiden ([ALB als Ziel von NLB](#)), wenn Sie die Funktionen beider Produkte nutzen möchten. Sie können dies beispielsweise tun, wenn Sie das statische IPs von NLB zusammen mit dem HTTP Header-basierten Routing von ALB verwenden möchten oder wenn Sie Ihre HTTP Arbeitslast einem aussetzen möchten [AWS PrivateLink](#).
  - Einen vollständigen Vergleich der Load Balancer finden Sie [im ELB Produktvergleich](#).
- Verwenden Sie nach SSL Möglichkeit/TLSOffloading.
  - Konfigurieren Sie HTTPS TLS /Listener mit integriertem [Application Load Balancer](#) und [Network Load Balancer](#). [AWS Certificate Manager](#)
  - Beachten Sie, dass einige Workloads aus Compliance-Gründen möglicherweise end-to-end verschlüsselt werden müssen. In diesem Fall ist es erforderlich, die Verschlüsselung an den Zielen zuzulassen.
  - Bewährte Sicherheitsmethoden finden Sie unter [SEC09-BP02 Verschlüsselung bei der Übertragung erzwingen](#).
- Wählen Sie den richtigen Routing-Algorithmus aus (nur). ALB

- Der Routing-Algorithmus kann einen entscheidenden Einfluss darauf haben, wie gut Ihre Backend-Ziele ausgelastet sind und wie sie die Leistung beeinflussen. ALB bietet beispielsweise [zwei Optionen für Routing-Algorithmen](#):
- Am wenigsten ausstehende Anfragen: Verwenden Sie diese Option, um eine bessere Verteilung der Last auf Ihre Backend-Ziele zu erreichen, wenn die Anfragen für Ihre Anwendung unterschiedlich komplex sind oder Ihre Ziele unterschiedliche Kapazitäten für die Verarbeitung haben.
- Round Robin: Verwenden Sie diese Option, wenn die Anfragen und Ziele ähnlich sind oder wenn Sie die Anfragen gleichmäßig auf die Ziele verteilen müssen.
- Ziehen Sie eine zonenübergreifende Verarbeitung oder Zonenisolierung in Betracht.
  - Verwenden Sie die deaktivierte zonenübergreifende Isolierung (Zonenisolierung), um die Latenz zu verbessern und Domains mit Zonenfehlern zu vermeiden. Es ist standardmäßig ausgeschaltet NLB und [ALB Sie können es pro Zielgruppe ausschalten](#).
  - Verwenden Sie die aktivierte zonenübergreifende Verarbeitung für eine höhere Verfügbarkeit und Flexibilität. Standardmäßig ist Cross-Zone für aktiviert ALB und innerhalb [können NLB Sie es pro Zielgruppe aktivieren](#).
- Aktivieren Sie HTTP Keep-Alives (nur) für Ihre HTTP Workloads. ALB Mit dieser Funktion kann der Load Balancer Backend-Verbindungen wiederverwenden, bis das Keep-Alive-Timeout abgelaufen ist, wodurch Ihre HTTP Anfrage- und Antwortzeit verbessert und auch die Ressourcenauslastung auf Ihren Backend-Zielen reduziert wird. Einzelheiten dazu, wie Sie dies für Apache und Nginx tun können, finden Sie unter [Was sind die optimalen Einstellungen für die Verwendung](#) von Apache oder als Backend-Server? NGINX ELB
- Aktivieren Sie die Überwachung für Ihren Load Balancer.
  - Aktivieren Sie die Zugriffsprotokolle für Ihren [Application Load Balancer](#) und [Network Load Balancer](#).
  - Die wichtigsten Felder, für die Sie in Betracht ziehen sollten request\_processing\_time, ALB sind, und request\_processing\_time. response\_processing\_time
  - Die wichtigsten Felder, die in Betracht gezogen werden sollten, NLB sind connection\_time und tls\_handshake\_time.
  - Bereiten Sie sich darauf vor, die Protokolle bei Bedarf abfragen zu können. [Sie können Amazon Athena verwenden, um sowohl ALB Protokolle als auch Protokolle abzufragen. NLB](#)
  - Erstellen Sie Alarme für leistungsbezogene Kennzahlen wie z. B. [TargetResponseTime für ALB](#).

## Ressourcen

### Zugehörige Dokumente:

- [ELBProduktvergleich](#)
- [AWS Globale Infrastruktur](#)
- [Verbesserung der Leistung und Senkung der Kosten durch Availability Zone-Affinität](#)
- [Step by step for Log Analysis with Amazon Athena](#)
- [Abfragen von Application-Load-Balancer-Protokollen](#)
- [Überwachen Ihrer Application Load Balancer](#)
- [Monitor your Network Load Balancer](#)
- [Um den Datenverkehr über die Instances in Ihrer Auto-Scaling-Gruppe zu verteilen, verwenden Sie Elastic-Load-Balancing](#)

### Zugehörige Videos:

- [AWS re:Invent 2023: Was können Netzwerke für Ihre Anwendung tun?](#)
- [AWS re:INFORCE 20: So nutzen Sie Elastic Load Balancing, um Ihre Sicherheitslage skalierbar zu verbessern](#)
- [AWS re:Invent 2018: Elastic Load Balancing: Detaillierte Informationen und bewährte Methoden](#)
- [AWS re:Invent 2021 — So wählen Sie den richtigen Load Balancer für Ihre Workloads AWS](#)
- [AWS re:Invent 2019: Holen Sie das Beste aus Elastic Load Balancing für verschiedene Workloads heraus](#)

### Zugehörige Beispiele:

- [Gateway Load Balancer](#)
- [CDKund AWS CloudFormation Beispiele für die Protokollanalyse mit Amazon Athena](#)

PERF04-BP05 Wählen Sie Netzwerkprotokolle, um die Leistung zu verbessern

Treffen Sie Entscheidungen über Protokolle für die Kommunikation zwischen Systemen und Netzwerken auf Grundlage der Auswirkungen, die sich für die Leistung der Workload ergeben.

In Bezug auf die Erzielung eines höheren Durchsatzes besteht eine Beziehung zwischen der Latenz und der Bandbreite. Wenn Ihre Dateiübertragung das Transmission Control Protocol (TCP) verwendet, verringern höhere Latenzen höchstwahrscheinlich den Gesamtdurchsatz. Es gibt Ansätze, dieses Problem durch TCP Optimierung und optimierte Übertragungsprotokolle zu beheben, aber eine Lösung ist die Verwendung des User Datagram Protocol (UDP).

Typische Anti-Muster:

- Sie verwenden es TCP für alle Workloads, unabhängig von den Leistungsanforderungen.

Vorteile der Nutzung dieser bewährten Methode: Wenn Sie sicherstellen, dass ein geeignetes Protokoll für die Kommunikation zwischen Benutzern und Workload-Komponenten verwendet wird, können Sie das Benutzererlebnis für Ihre Anwendungen insgesamt verbessern. Verbindungslose Verbindungen UDP ermöglichen beispielsweise eine hohe Geschwindigkeit, aber keine erneute Übertragung oder hohe Zuverlässigkeit. TCP ist ein Protokoll mit vollem Funktionsumfang, erfordert jedoch mehr Aufwand für die Verarbeitung der Pakete.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Mittel

Implementierungsleitfaden

Wenn Sie in der Lage sind, verschiedene Protokolle für Ihre Anwendung auszuwählen, und Sie über Fachwissen in diesem Bereich verfügen, optimieren Sie Ihre Anwendungs- und Endbenutzererfahrung, indem Sie ein anderes Protokoll verwenden. Beachten Sie, dass dieser Ansatz mit erheblichen Schwierigkeiten verbunden ist und nur versucht werden sollte, wenn Sie Ihre Anwendung zuvor auf andere Weise optimiert haben.

Um die Leistung Ihrer Workload zu verbessern, sollten Sie in erster Linie die Anforderungen an die Latenz und den Durchsatz kennen und dann Netzwerkprotokolle auswählen, die die Leistung optimieren.

Wann sollte die Verwendung in Betracht gezogen werden TCP

TCP bietet eine zuverlässige Datenlieferung und kann für die Kommunikation zwischen Workload-Komponenten verwendet werden, bei denen Zuverlässigkeit und garantierte Datenlieferung wichtig sind. Viele webbasierte Anwendungen basieren auf TCP-basierten Protokollen wie HTTP und HTTPS, um TCP Sockets für die Kommunikation zwischen Anwendungskomponenten zu öffnen. E-Mail- und Dateidatenübertragung sind gängige Anwendungen, die ebenfalls Gebrauch machen TCP, da es sich dabei um einen einfachen und zuverlässigen Übertragungsmechanismus zwischen Anwendungskomponenten handelt. Die Verwendung von TLS with TCP kann zu einem gewissen

Mehraufwand bei der Kommunikation führen, was zu einer erhöhten Latenz und einem geringeren Durchsatz führen kann, hat aber auch den Vorteil der Sicherheit. Der Overhead entsteht vor allem durch den zusätzlichen Aufwand des Handshake-Prozesses, der mehrere Roundtrips in Anspruch nehmen kann. Sobald der Handshake abgeschlossen ist, ist der Overhead für die Ver- und Entschlüsselung der Daten relativ gering.

Wann sollte die Verwendung in Betracht gezogen werden UDP

UDP ist ein connection-less-oriented Protokoll und eignet sich daher für Anwendungen, die eine schnelle und effiziente Übertragung benötigen, z. B. Protokoll-, Überwachungs- und VoIP-Daten. Erwägen Sie auch die Verwendung von Workload-Komponenten, die auf kleine Anfragen von einer großen Anzahl von Clients reagieren, UDP wenn Sie über Workload-Komponenten verfügen, um eine optimale Leistung der Arbeitslast sicherzustellen. Datagram Transport Layer Security (DTLS) UDP entspricht Transport Layer Security (TLS). Bei der Verwendung DTLS von UDP wird der Mehraufwand durch das Verschlüsseln und Entschlüsseln der Daten, da der Handshake-Prozess vereinfacht wird. DTLS fügt den UDP Paketen außerdem einen geringen Mehraufwand hinzu, da es zusätzliche Felder zur Angabe der Sicherheitsparameter und zur Erkennung von Manipulationen enthält.

Wann sollte man die Verwendung von SRD

Scalable Reliable Datagram (SRD) ist ein Netzwerktransportprotokoll, das für Workloads mit hohem Durchsatz optimiert ist, da es den Datenverkehr über mehrere Pfade verteilt und nach Paketverlusten oder Verbindungsausfällen schnell wiederhergestellt werden kann. SRD eignet sich daher am besten für High-Performance-Computing-Workloads (HPC), die eine Kommunikation zwischen Rechenknoten mit hohem Durchsatz und geringer Latenz erfordern. Dazu gehören z. B. parallele Verarbeitungsaufgaben wie Simulationen, Modellierung und Datenanalyse, bei denen eine große Menge an Daten zwischen den Knoten übertragen werden muss.

Implementierungsschritte

- Verwenden Sie die Services [AWS Global Accelerator](#) und [AWS Transfer Family](#), um den Durchsatz Ihrer Anwendungen für den File Transfer online zu verbessern. Der AWS Global Accelerator Service hilft Ihnen dabei, die Latenz zwischen Ihren Client-Geräten und Ihren Workloads zu AWS verringern. Mit AWS Transfer Family können Sie TCP basierte Protokolle wie Secure Shell File Transfer Protocol (SFTP) und File Transfer Protocol over SSL (FTPS) verwenden, um Ihre Dateiübertragungen an AWS Speicherdienste sicher zu skalieren und zu verwalten.
- Ermitteln Sie anhand der Netzwerklatenz, ob sie für die Kommunikation zwischen Workload-Komponenten geeignet TCP ist. Wenn die Netzwerklatenz zwischen Ihrer Client-Anwendung und

dem Server hoch ist, kann der TCP Drei-Wege-Handshake einige Zeit in Anspruch nehmen, was sich auf die Reaktionsfähigkeit Ihrer Anwendung auswirkt. Metriken wie die Zeit bis zum ersten Byte (TTFB) und die Round-Trip-Zeit (RTT) können zur Messung der Netzwerklatenz verwendet werden. Wenn Ihr Workload dynamische Inhalte für Benutzer bereitstellt, sollten Sie [Amazon CloudFront](#) in Betracht ziehen. Amazon stellt eine persistente Verbindung zu jedem Ursprung für dynamische Inhalte her, um die Verbindungsaufbauzeit zu vermeiden, die andernfalls jede Client-Anfrage verlangsamen würde.

- Die Verwendung TLS mit TCP oder UDP kann aufgrund der Auswirkungen der Verschlüsselung und Entschlüsselung zu einer erhöhten Latenz und einem verringerten Durchsatz für Ihren Workload führen. Für solche Workloads sollten Sie SSL TLS /offloading auf [Elastic Load Balancing](#) in Betracht ziehen, um die Workload-Leistung zu verbessern, indem Sie es dem Load Balancer ermöglichen, den SSL /- TLS Verschlüsselungs- und Entschlüsselungsprozess abzuwickeln, anstatt dies von Backend-Instances erledigen zu lassen. Dies kann dazu beitragen, die CPU Auslastung der Backend-Instances zu reduzieren, was die Leistung verbessern und die Kapazität erhöhen kann.
- Verwenden Sie den [Network Load Balancer \(NLB\)](#), um Dienste bereitzustellen, die auf dem UDP Protokoll basieren, z. B. Authentifizierung und Autorisierung, Protokollierung DNS, IoT und Streaming-Medien, um die Leistung und Zuverlässigkeit Ihres Workloads zu verbessern. Der NLB verteilt den eingehenden UDP Datenverkehr auf mehrere Ziele, sodass Sie Ihre Arbeitslast horizontal skalieren, die Kapazität erhöhen und den Overhead eines einzelnen Ziels reduzieren können.
- Für Ihre High Performance Computing (HPC) -Workloads sollten Sie die [Elastic Network Adapter \(ENA\) Express-Funktionalität](#) verwenden, die SRD das Protokoll verwendet, um die Netzwerkleistung zu verbessern, indem sie eine höhere Single-Flow-Bandbreite (25 Gbit/s) und eine geringere Tail-Latenz (99,9 Perzentile) für den Netzwerkverkehr zwischen Instances bereitstellt. EC2
- Verwenden Sie den [Application Load Balancer \(ALB\)](#), um Ihren G-Verkehr RPC (Remote Procedure Calls) zwischen Workload-Komponenten oder zwischen RPC G-Clients und -Diensten weiterzuleiten. g RPC verwendet das TCP basierte HTTP /2-Protokoll für den Transport und bietet Leistungsvorteile wie geringeren Netzwerkbedarf, Komprimierung, effiziente Binärserialisierung, Unterstützung für zahlreiche Sprachen und bidirektionales Streaming.

## Ressourcen

## Zugehörige Dokumente:



- [Wie leitet man den Verkehr nach Kubernetes UDP](#)
- [Application Load Balancer](#)
- [EC2Verbessertes Networking unter Linux](#)
- [EC2Verbessertes Networking unter Windows](#)
- [EC2Platzierungsgruppen](#)
- [Aktivierung von Enhanced Networking mit dem Elastic Network Adapter \(ENA\) auf Linux-Instances](#)
- [Network Load Balancer](#)
- [Netzwerkprodukte mit AWS](#)
- [Umstellung auf latenzbasiertes Routing in Amazon Route 53](#)
- [VPC-Endpunkte](#)

#### Zugehörige Videos:

- [AWS re:Invent 2022 — Skalierung der Netzwerkleistung auf Amazon Elastic Compute Cloud-Instanzen der nächsten Generation](#)
- [AWS re:Invent 2022 — Grundlagen von Anwendungsnetzwerken](#)

#### Zugehörige Beispiele:

- [AWS Transit Gateway und skalierbare Sicherheitslösungen](#)
- [Workshops zu AWS -Netzwerken](#)

PERF04-BP06 Wählen Sie den Standort Ihres Workloads basierend auf den Netzwerkanforderungen

Evaluieren Sie Optionen für die Platzierung von Ressourcen, um die Latenz im Netzwerk zu verringern und den Durchsatz zu verbessern und so ein optimales Benutzererlebnis durch kürzere Seitenlade- und Datentransferzeiten zu gewährleisten.

#### Typische Anti-Muster:

- Sie konsolidieren alle Workload-Ressourcen an einem geografischen Standort.
- Sie haben sich für die Region entschieden, die Ihrem Standort, aber nicht dem Workload-Endbenutzer, am nächsten liegt.

Vorteile der Nutzung dieser bewährten Methode: Die Benutzererfahrung wird stark von der Latenz zwischen dem Benutzer und Ihrer Anwendung beeinflusst. Durch die Verwendung eines geeigneten AWS-Regionen und AWS privaten globalen Netzwerks können Sie die Latenz reduzieren und Remote-Benutzern ein besseres Benutzererlebnis bieten.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Mittel

### Implementierungsleitfaden

Ressourcen, wie EC2 Amazon-Instances, werden in Availability Zones innerhalb [AWS-Regionen](#), [AWS Local Zones](#) oder [AWS Wavelength](#) Zonen platziert. [AWS Outposts](#) Die Auswahl dieses Standorts beeinflusst die Latenz des Netzwerks und den Durchsatz vom Standort des Benutzers aus. Edge-Services wie [Amazon CloudFront](#) [AWS Global Accelerator](#) können auch zur Verbesserung der Netzwerkleistung verwendet werden, indem sie entweder Inhalte an Edge-Standorten zwischenspeichern oder Benutzern einen optimalen Pfad zur Arbeitslast über das AWS globale Netzwerk bieten.

Amazon EC2 bietet Platzierungsgruppen zum Netzwerken an. Eine Platzierungsgruppe ist eine logische Gruppierung von Instances, um die Latenz zu verringern. Durch die Verwendung von Platzierungsgruppen mit unterstützten Instance-Typen und einem Elastic Network Adapter (ENA) können Workloads an einem 25-Gbit/s-Netzwerk mit geringer Latenz und reduziertem Jitter teilnehmen. Platzierungsgruppen werden für Workloads empfohlen, für die eine niedrige Netzwerklatenz bzw. ein hoher Durchsatz von Vorteil sind.

[Latenzempfindliche Dienste werden an Edge-Standorten über ein AWS globales Netzwerk wie Amazon bereitgestellt. CloudFront](#) Diese Edge-Standorte bieten in der Regel Dienste wie Content Delivery Network (CDN) und Domain Name System (DNS). Da sich diese Dienste an der Peripherie befinden, können Workloads mit geringer Latenz auf Anfragen nach Inhalten oder Lösungen reagieren. Es sind auch geografische Services wie das Geo-Targeting von Inhalten (Bereitstellung unterschiedlicher Inhalte gemäß dem Standort von Endbenutzern) oder die latenzbasierte Weiterleitung von Endbenutzern zur nächsten Region (minimale Latenz) verfügbar.

Verwenden Sie Edge-Services, um die Latenz zu reduzieren und das Caching von Inhalten zu ermöglichen. Konfigurieren Sie die Cachesteuerung DNS sowohl für als auch für HTTP/ korrekt HTTPS, um den größtmöglichen Nutzen aus diesen Ansätzen zu ziehen.

### Implementierungsschritte

- Erfassen Sie Informationen über den an den Netzwerkschnittstellen ein- und ausgehenden IP-Datenverkehr.

- [Protokollierung von IP-Verkehr mithilfe von VPC Flow Logs](#)
- [Wie wird die Client-IP-Adresse aufbewahrt in AWS Global Accelerator](#)
- Analysieren Sie die Netzwerkzugriffsmuster in Ihrer Workload, um zu ermitteln, wie die Benutzer Ihre Anwendung verwenden.
  - Verwenden Sie Überwachungstools wie [Amazon CloudWatch](#) und [AWS CloudTrail](#), um Daten zu Netzwerkaktivitäten zu sammeln.
  - Analysen Sie die Daten, um das Netzwerkzugriffsmuster zu identifizieren.
- Wählen Sie Regionen für Ihre Workload-Bereitstellung auf der Grundlage der folgenden zentralen Elemente aus:
  - Standort Ihrer Daten: Für datenintensive Anwendungen (wie etwa Big Data oder Machine Learning) sollte der Anwendungscode so nahe wie möglich zu den Daten ausgeführt werden.
  - Standort Ihrer Benutzer: Wählen Sie für benutzerseitige Anwendungen eine Region (oder Regionen) in der Nähe der Benutzer der Workload.
  - Weitere Einschränkungen: Berücksichtigen Sie Einschränkungen wie Kosten und Compliance, wie unter [Relevante Aspekte bei der Wahl einer Region für Ihre Workloads](#) erläutert.
- Verwenden Sie [AWS Local Zones](#), um Workloads wie Video-Rendern auszuführen. Mit Local Zones können Sie von allen Vorteilen profitieren, die sich durch die Platzierung der Datenverarbeitungs- und Speicherressourcen in der Nähe Ihrer Endbenutzer ergeben.
- Verwenden Sie [AWS Outposts](#) für Workloads, die On-Premises verarbeitet werden müssen und die Sie nahtlos mit Ihren restlichen Workloads in AWS ausführen möchten.
- ultra-low-latency Für Anwendungen wie hochauflösendes Live-Videostreaming, High-Fidelity-Audio und Augmented Reality oder Virtual Reality (AR/VR) sind 5G-Geräte erforderlich. Beachten Sie bei solchen Anwendungen Folgendes: [AWS Wavelength](#) AWS Wavelength bettet AWS Rechen- und Speicherdienste in 5G-Netzwerke ein und bietet so eine mobile Edge-Computing-Infrastruktur für die Entwicklung, Bereitstellung und Skalierung von ultra-low-latency Anwendungen.
- Verwenden Sie lokale Zwischenspeicherung oder [AWS -Zwischenspeicherung](#) für häufig genutzte Ressourcen zur Verbesserung der Leistung, zur Verringerung von Datenverschiebungen und zur Reduzierung der Umweltauswirkungen.

Service	Wann sollte dies verwendet werden?
<a href="#">Amazon CloudFront</a>	Wird verwendet, um statische Inhalte wie Bilder, Skripte und Videos sowie dynamische

Service	Wann sollte dies verwendet werden?
	Inhalte wie API Antworten oder Webanwendungen zwischenspeichern.
<a href="#">Amazon ElastiCache</a>	Verwenden Sie dies für die Zwischenspeicherung von Inhalten für Webanwendungen.
<a href="#">DynamoDB Accelerator</a>	Verwenden Sie dies für die Add-in-Speicher-Beschleunigung für Ihre DynamoDB-Tabellen.

- Nutzen Sie Services, die Ihnen dabei helfen können, Code näher an den Benutzern Ihrer Workload auszuführen:

Service	Wann sollte dies verwendet werden?
<a href="#">Lambda@Edge</a>	Verwenden Sie dies für rechenintensive Anwendungen, die initiiert werden, wenn sich Objekte nicht im Zwischenspeicher befinden.
<a href="#">CloudFront Amazon-Funktionen</a>	Wird für einfache Anwendungsfälle wie HTTP Anfragen oder Antwortmanipulationen verwendet, die durch kurzlebige Funktionen ausgelöst werden können.
<a href="#">AWS IoT Greengrass</a>	Verwenden Sie dies für die Ausführung lokaler Rechenoperationen, Messaging sowie die Datenzwischenspeicherung für verbundene Geräte.

- Einige Anwendungen benötigen feste Zugangspunkte oder eine höhere Leistung. Bei diesen müssen First-Byte-Latenz der Jitter verringert und der Durchsatz erhöht werden. Diese Anwendungen können von Netzwerkdiensten profitieren, die statische Anycast-IP-Adressen und TCP Terminierung an Edge-Standorten bereitstellen. [AWS Global Accelerator](#) kann die Leistung Ihrer Anwendungen um bis zu 60% verbessern und ein schnelles Failover für Architekturen mit mehreren Regionen ermöglichen. AWS Global Accelerator stellt Ihnen statische Anycast-IP-Adressen zur Verfügung, die als fester Einstiegspunkt für Ihre in einer oder mehreren gehosteten Anwendungen dienen. AWS-Regionen Diese IP-Adressen ermöglichen es, dass der

Datenverkehr so nah wie möglich an Ihren Benutzern in das AWS globale Netzwerk gelangt. AWS Global Accelerator reduziert die Zeit für den anfänglichen Verbindungsaufbau, indem eine TCP Verbindung zwischen dem Client und dem AWS Edge-Standort hergestellt wird, der dem Client am nächsten ist. Prüfen Sie die Verwendung von AWS Global Accelerator , um die Leistung Ihrer TCP UDP /-Workloads zu verbessern und ein schnelles Failover für Architekturen mit mehreren Regionen zu ermöglichen.

## Ressourcen

### Zugehörige bewährte Methoden:

- [COST07-BP02 Implementieren Sie Regionen auf der Grundlage der Kosten](#)
- [COST08-BP03 Implementieren Sie Dienste zur Senkung der Datenübertragungskosten](#)
- [REL10-BP01 Stellen Sie den Workload an mehreren Standorten bereit](#)
- [REL10-BP02 Wählen Sie die geeigneten Standorte für Ihre Bereitstellung an mehreren Standorten aus](#)
- [SUS01-BP01 Wählen Sie die Region auf der Grundlage von Geschäftsanforderungen und Nachhaltigkeitszielen](#)
- [SUS02-BP04 Optimieren Sie die geografische Verteilung von Workloads auf der Grundlage ihrer Netzwerkanforderungen](#)
- [SUS04-BP07 Minimierung der Datenbewegung zwischen Netzwerken](#)

### Zugehörige Dokumente:

- [AWS Globale Infrastruktur](#)
- [AWS Local Zones und AWS Outposts Auswahl der richtigen Technologie für Ihren Edge-Workload](#)
- [Platzierungsgruppen](#)
- [AWS Local Zones](#)
- [AWS Outposts](#)
- [AWS Wavelength](#)
- [Amazon CloudFront](#)
- [AWS Global Accelerator](#)
- [AWS Direct Connect](#)
- [AWS Site-to-Site VPN](#)

- [Amazon Route 53](#)

Zugehörige Videos:

- [AWS Erklärvideo zu Local Zones](#)
- [AWS Outposts: Overview and How it Works](#)
- [AWS re:Invent 2023 — Eine Migrationsstrategie für Edge-Workloads und lokale Workloads](#)
- [AWS re:Invent 2021 — AWS Outposts: Das Erlebnis vor Ort umsetzen AWS](#)
- [AWS re:Invent 2020: AWS Wavelength: Führen Sie Apps mit extrem niedriger Latenz am 5G-Edge aus](#)
- [AWS re:Invent 2022 — AWS Local Zones: Entwicklung von Anwendungen für eine verteilte Kante](#)
- [AWS re:Invent 2021 — Websites mit niedriger Latenz mit Amazon erstellen CloudFront](#)
- [AWS re:Invent 2022 — Verbessern Sie Leistung und Verfügbarkeit mit AWS Global Accelerator](#)
- [AWS re:Invent 2022 — Bauen Sie Ihr globales Wide Area Network auf mit AWS](#)
- [AWS re:Invent 2020: Globales Verkehrsmanagement mit Amazon Route 53](#)

Zugehörige Beispiele:

- [AWS Global Accelerator Workshop zu kundenspezifischem Routing](#)
- [Verarbeitung von Rewrites und Redirects mit Edge-Funktionen](#)

PERF04-BP07 Optimieren Sie die Netzwerkkonfiguration auf der Grundlage von Metriken

Treffen Sie anhand der erfassten und analysierten Daten fundierte Entscheidungen zum Optimieren Ihrer Netzwerkkonfiguration.

Typische Anti-Muster:

- Sie gehen davon aus, dass alle leistungsbezogenen Probleme auf Anwendungen zurückzuführen sind.
- Sie testen die Netzwerkleistung ausschließlich an einem Standort nahe der Stelle, an der Sie die Workload bereitgestellt haben.
- Sie verwenden Standardkonfigurationen für alle Netzwerkservices.
- Sie führen eine Überdimensionierung der Netzwerkressourcen durch, um eine ausreichende Kapazität zu gewährleisten.

Vorteile der Nutzung dieser bewährten Methode: Das Sammeln der erforderlichen Metriken Ihres AWS -Netzwerks und die Implementierung von Tools zur Überwachung des Netzwerks bieten Ihnen die Möglichkeit, die Leistung des Netzwerks zu ermitteln und die Netzwerkkonfigurationen zu optimieren.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Niedrig

### Implementierungsleitfaden

Die Überwachung des Datenverkehrs zu und von VPCs Subnetzen oder Netzwerkschnittstellen ist entscheidend, um zu verstehen, wie AWS Netzwerkressourcen genutzt und Netzwerkkonfigurationen optimiert werden können. Mithilfe der folgenden AWS Netzwerktools können Sie weitere Informationen zur Verkehrsnutzung, zum Netzwerkzugriff und zu den Protokollen einsehen.

### Implementierungsschritte

- Identifizieren Sie die wichtigsten Leistungskennzahlen wie Latenz oder Paketverlust, die erfasst werden sollen. AWS bietet mehrere Tools, die Ihnen bei der Erfassung dieser Messwerte helfen können. Mit den folgenden Tools können Sie Informationen über die Nutzung des Datenverkehrs, den Netzwerkzugriff und die Protokolle genauer untersuchen:

AWS Werkzeug	Aktion
<a href="#">Amazon VPC IP-Adressmanager</a> .	Wird verwendet, IPAM um IP-Adressen für Ihre und lokale Workloads zu planen, nachzuerfolgen AWS und zu überwachen. Dies ist eine bewährte Methode zur Optimierung der Nutzung und Zuweisung von IP-Adressen.
<a href="#">VPCFlow-Protokolle</a>	Verwenden Sie VPC Flow Logs, um detaillierte Informationen über den Verkehr zu und von Netzwerkschnittstellen in Ihrem zu erfassen VPCs. Mit VPC Flow Logs können Sie restriktive oder freizügige Sicherheitsgruppenregeln diagnostizieren und die Richtung des Datenverkehrs zu und von den Netzwerkschnittstellen bestimmen.

AWS Werkzeug	Aktion
<a href="#">AWS Transit Gateway Flow Logs</a>	Verwenden Sie AWS Transit Gateway Flow Logs, um Informationen über den IP-Verkehr zu und von Ihren Transit-Gateways zu erfassen.
<a href="#">DNSProtokollierung von Abfragen</a>	Protokollieren Sie Informationen über öffentliche oder private DNS Abfragen, die Route 53 empfängt. Mithilfe von DNS Protokollen können Sie DNS Konfigurationen optimieren, indem Sie herausfinden, welche Domain oder Subdomain angefordert wurde oder welche Route EDGE 53-Standorte auf DNS Anfragen geantwortet haben.
<a href="#">Reachability Analyzer</a>	Reachability Analyzer hilft Ihnen, die Erreichbarkeit von Netzwerken zu analysieren und zu debuggen. Reachability Analyzer ist ein Tool zur Konfigurationsanalyse, mit dem Sie Konnektivitätstests zwischen einer Quellressource und einer Zielressource in Ihrem durchführen können. VPCs Mit diesem Tool können Sie überprüfen, ob Ihre Netzwerkonfiguration der geplanten Konnektivität entspricht.



AWS Werkzeug	Aktion
<a href="#">Network Access Analyzer</a>	<p>Mit Network Access Analyzer können Sie den Netzwerkzugriff auf die eigenen Ressourcen analysieren. Mit Network Access Analyzer können Sie Ihre Anforderungen an den Netzwerkzugriff spezifizieren und potenzielle Netzwerkpfade identifizieren, die Ihren Anforderungen nicht entsprechen. Indem Sie Ihre entsprechende Netzwerkkonfiguration optimieren, können Sie den Zustand Ihres Netzwerks nachvollziehen und überprüfen sowie belegen, dass Ihr AWS -Netzwerk Ihre Complianceanforderungen erfüllt.</p>
<a href="#">Amazon CloudWatch</a>	<p>Verwenden Sie <a href="#">Amazon CloudWatch</a> und aktivieren Sie die entsprechenden Metriken für Netzwerkoptionen. Stellen Sie sicher, dass Sie die richtige Netzwerk-Metrik für Ihre Workload auswählen. Sie können beispielsweise Metriken für VPC Network Address Usage, VPC NAT Gateway, VPN Tunnel, AWS Transit Gateway, AWS Network Firewall, Elastic Load Balancing und aktivieren AWS Direct Connect. Die kontinuierliche Überwachung von Metriken ist eine gute Vorgehensweise, um den Status und die Nutzung Ihres Netzwerks zu beobachten und nachzuvollziehen. Sie hilft Ihnen, die Netzwerkkonfiguration auf der Basis Ihrer Beobachtungen zu optimieren.</p>

AWS Werkzeug	Aktion
<a href="#">AWS Network Manager</a>	<p>Mit dieser AWS Network Manager Option können Sie die Leistung des <a href="#">AWS globalen Netzwerks</a> in Echtzeit und in der Vergangenheit für betriebliche und planerische Zwecke überwachen. Network Manager bietet aggregierte Netzwerklatenz zwischen AWS-Regionen und Availability Zones sowie innerhalb jeder Availability Zone, sodass Sie besser verstehen können, wie Ihre Anwendungsleistung mit der Leistung des zugrunde liegenden AWS Netzwerks zusammenhängt.</p>
<a href="#">Amazon CloudWatch RUM</a>	<p>Verwenden Sie Amazon CloudWatch RUM, um die Kennzahlen zu sammeln, die Ihnen die Erkenntnisse liefern, die Ihnen helfen, die Benutzererfahrung zu identifizieren, zu verstehen und zu verbessern.</p>

- Identifizieren Sie mithilfe von AWS Transit Gateway Flow Logs die wichtigsten Gesprächspartner VPC und Muster des Anwendungsdatenverkehrs.
- Beurteilen und optimieren Sie Ihre aktuelle Netzwerkarchitektur VPCs, einschließlich Subnetze und Routing. Sie können beispielsweise bewerten, wie unterschiedlich VPC Peering ist, oder Sie AWS Transit Gateway können Ihnen helfen, das Netzwerk in Ihrer Architektur zu verbessern.
- Bewerten Sie die Routingpfade in Ihrem Netzwerk, um sicherzustellen, dass immer der kürzeste Pfad zwischen Zielen verwendet wird. Network Access Analyzer kann Ihnen dabei helfen.

## Ressourcen

### Zugehörige Dokumente:

- [Protokollierung öffentlicher DNS Abfragen](#)
- [Was ist IPAM?](#)
- [What is Reachability Analyzer?](#)
- [What is Network Access Analyzer?](#)

- [CloudWatchMetriken für deine VPCs](#)
- [Optimieren Sie die Leistung und senken Sie die Kosten für Netzwerkanalysen mit VPC Flow Logs im Apache Parquet-Format](#)
- [Überwachen Sie Ihre globalen Netzwerke und Kernnetzwerke mit CloudWatch Amazon-Metriken](#)
- [Kontinuierliches Überwachen von Netzwerkdatenverkehr und -ressourcen](#)

#### Zugehörige Videos:

- [AWS re:Invent 2023 — Ein Leitfaden für Entwickler zum Thema Cloud-Netzwerke](#)
- [AWS re:Invent 2023 — Bereit für das, was als Nächstes kommt? Gestaltung von Netzwerken für Wachstum und Flexibilität](#)
- [AWS re:Invent 2023 — Fortschrittliche VPC Designs und neue Funktionen](#)
- [AWS re:Invent 2022 — Tauchen Sie tief in die Netzwerkinfrastruktur ein AWS](#)
- [AWS re:Invent 2020 — Bewährte Methoden und Tipps zum Netzwerken mit dem AWS Well-Architected Framework](#)
- [AWS re:Invent 2020 — Überwachung und Fehlerbehebung im Netzwerkverkehr](#)

#### Zugehörige Beispiele:

- [Workshops zu AWS -Netzwerken](#)
- [AWS Network Monitoring](#)
- [Beobachten und diagnostizieren Sie Ihr Netzwerk am AWS](#)
- [Auffinden und Beheben von Netzwerkfehlfunktionen auf AWS](#)

## Prozess und Kultur

### Fragen

- [PERF5. Wie tragen Ihre Unternehmenspraktiken und Ihre Unternehmenskultur zur Leistungseffizienz Ihrer Workload bei?](#)

## PERF5. Wie tragen Ihre Unternehmenspraktiken und Ihre Unternehmenskultur zur Leistungseffizienz Ihrer Workload bei?

Bei der Architektur von Workloads gibt es Prinzipien und Methoden, die Sie übernehmen können, um effiziente und leistungsstarke Cloud-Workloads besser zu betreiben. Um eine Kultur zu schaffen, die die Leistungseffizienz von Cloud-Workloads fördert, sollten Sie diese Schlüsselprinzipien und -praktiken berücksichtigen:

### Bewährte Methoden

- [PERF05-BP01 Festlegung wichtiger Leistungsindikatoren \(KPIs\) zur Messung des Zustands und der Leistung der Arbeitslast](#)
- [PERF05-BP02 Verwenden Sie Überwachungslösungen, um die Bereiche zu verstehen, in denen Leistung am wichtigsten ist](#)
- [PERF05-BP03 Definieren Sie einen Prozess zur Verbesserung der Workload-Leistung](#)
- [PERF05-BP04 Belastungstest Ihr Workload](#)
- [PERF05-BP05 Verwenden Sie Automatisierung, um leistungsbezogene Probleme proaktiv zu beheben](#)
- [PERF05-BP06 Behalten Sie Ihren Workload und Ihre Services up-to-date](#)
- [PERF05-BP07 Überprüfen Sie die Kennzahlen in regelmäßigen Abständen](#)

PERF05-BP01 Festlegung wichtiger Leistungsindikatoren (KPIs) zur Messung des Zustands und der Leistung der Arbeitslast

Identifizieren Sie diejenigen KPIs, mit denen die Leistung der Arbeitslast quantitativ und qualitativ gemessen werden kann. KPIs helfen Ihnen dabei, den Zustand und die Leistung einer Arbeitslast im Zusammenhang mit einem Geschäftsziel zu messen.

### Typische Anti-Muster:

- Sie überwachen nur Metriken auf Systemebene, um Erkenntnisse über Ihre Workload zu gewinnen, und verstehen den geschäftlichen Einfluss dieser Metriken nicht.
- Sie gehen davon aus, KPIs dass Ihre Daten bereits als Standard-Metriken veröffentlicht und geteilt wurden.
- Sie definieren keinen quantitativen, messbaren Wert KPI.
- Sie orientieren sich nicht KPIs an Geschäftszielen oder -strategien.

Vorteile der Einführung dieser bewährten Methode: Die Identifizierung von spezifischen Merkmalen KPIs, die den Zustand und die Leistung der Arbeitslast widerspiegeln, hilft dabei, die Teams auf ihre Prioritäten auszurichten und erfolgreiche Geschäftsergebnisse zu definieren. Das Teilen dieser Metriken mit allen Abteilungen bietet Sichtbarkeit und die Ausrichtung an Grenzwerten, Erwartungen und Geschäftsauswirkungen.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Hoch

### Implementierungsleitfaden

KPIs ermöglichen es Geschäfts- und Technikteams, sich bei der Messung von Zielen und Strategien und der Art und Weise, wie diese Faktoren zusammenwirken, um Geschäftsergebnisse zu erzielen, abzustimmen. Beispielsweise könnte eine Website-Workload die Ladezeit der Seite als Indikator für die Gesamtleistung heranziehen. Diese Metrik wäre einer von mehreren Datenpunkten, mit denen das Benutzererlebnis gemessen wird. Zusätzlich zum Ermitteln der Grenzwerte für Seitenladezeiten sollten Sie das gewünschte Resultat dokumentieren bzw. das Geschäftsrisiko, wenn die ideale Leistung nicht erreicht wird. Die lange Ladezeit einer Seite betrifft Ihre Endbenutzer direkt, verringert die Bewertung ihres Benutzererlebnisses und kann zu einem Verlust von Kunden führen. Kombinieren Sie bei der Definition Ihrer KPI Schwellenwerte sowohl Branchen-Benchmarks als auch die Erwartungen Ihrer Endnutzer. Wenn der aktuelle Branchen-Benchmark beispielsweise eine Webseite innerhalb von zwei Sekunden lädt, Ihre Endnutzer jedoch erwarten, dass eine Webseite innerhalb eines Zeitraums von einer Sekunde geladen wird, sollten Sie diese beiden Datenpunkte bei der Festlegung der berücksichtigen. KPI

Ihr Team muss Ihre Arbeitslast KPIs anhand von detaillierten Echtzeitdaten und historischen Daten als Referenz bewerten und Dashboards erstellen, die metrische Berechnungen mit Ihren KPI Daten durchführen, um daraus Erkenntnisse zu Betrieb und Auslastung abzuleiten. KPIs sollten dokumentiert sein und Schwellenwerte enthalten, die die Geschäftsziele und -strategien unterstützen, und sollte den zu überwachenden Kennzahlen zugeordnet werden. KPIs sollten überprüft werden, wenn sich Geschäftsziele, Strategien oder Anforderungen der Endbenutzer ändern.

### Implementierungsschritte

- Identifizieren von Stakeholdern: Identifizieren und dokumentieren Sie wichtige Geschäfts-Stakeholder, einschließlich Entwicklungs- und Betriebsteams.
- Definition von Zielen: Arbeiten Sie mit diesen Stakeholdern zusammen, um die Ziele Ihrer Workload zu definieren und zu dokumentieren. Berücksichtigen Sie die kritischen Leistungsaspekte Ihrer Workloads, wie Durchsatz, Reaktionszeit und Kosten, sowie Geschäftsziele wie die Benutzerzufriedenheit.

- Überprüfen Sie die bewährten Verfahren der Branche: Überprüfen Sie die bewährten Verfahren der Branche, um herauszufinden, welche KPIs für Ihre Workload-Ziele relevant sind.
- Identifizieren von Metriken: Identifizieren Sie Metriken, die auf Ihre Workload-Ziele abgestimmt sind und Ihnen helfen können, Leistung und Geschäftsziele zu messen. Stellen Sie das KPIs System auf der Grundlage dieser Kennzahlen fest. Beispiele für Metriken sind Messungen wie die durchschnittliche Reaktionszeit oder die Anzahl gleichzeitiger Benutzer.
- Definieren und dokumentieren KPIs: Verwenden Sie branchenweit bewährte Verfahren und Ihre Workload-Ziele, um Ziele für Ihren Workload festzulegen KPI. Verwenden Sie diese Informationen, um KPI Schwellenwerte für den Schweregrad oder die Alarmstufe festzulegen. Identifizieren und dokumentieren Sie das Risiko und die Auswirkungen eines KPI Fehlers.
- Implementieren Sie die Überwachung: Verwenden Sie Überwachungstools wie [Amazon CloudWatch](#) oder [AWS Config](#) um Metriken zu sammeln und zu messen KPIs.
- Visuell kommunizieren KPIs: Verwenden Sie Dashboard-Tools wie [Amazon QuickSight](#), um Stakeholder zu visualisieren und KPIs mit ihnen zu kommunizieren.
- Analysieren und optimieren: Überprüfen und analysieren Sie regelmäßig KPIs, um Bereiche Ihres Workloads zu identifizieren, die verbessert werden müssen. Arbeiten Sie mit den Stakeholdern zusammen, um diese Verbesserungen umzusetzen.
- Überprüfung und Optimierung: Überprüfen Sie regelmäßig die Kennzahlen und KPIs bewerten Sie deren Effektivität, insbesondere wenn sich die Geschäftsziele oder die Leistung der Arbeitslast ändern.

## Ressourcen

### Zugehörige Dokumente:

- [CloudWatch Dokumentation](#)
- [Überwachung, Protokollierung und Leistung AWS Partner s](#)
- [AWS Tools zur Beobachtbarkeit](#)
- [Die Bedeutung von Key Performance Indicators \(KPIs\) für groß angelegte Cloud-Migrationen](#)
- [So verfolgen Sie Ihre Kostenoptimierung KPIs mit dem Dashboard KPI](#)
- [X-Ray-Dokumentation](#)
- [Verwenden von CloudWatch Amazon-Dashboards](#)
- [Amazon QuickSight KPIs](#)

## Zugehörige Videos:

- [AWS re:Invent 2023 — Optimieren Sie Kosten und Leistung und verfolgen Sie die Fortschritte bei der Risikominderung](#)
- [AWS re:Invent 2023 — Managen Sie Ereignisse im Ressourcenlebenszyklus in großem Umfang mit AWS Health](#)
- [AWS re:Invent 2023 — Leistung und Effizienz bei Pinterest: Optimierung der neuesten Instanzen](#)
- [AWS re:Invent 2022 — AWS Optimierung: Umsetzbare Schritte für sofortige Ergebnisse](#)
- [AWS re:Invent 2023 — Aufbau einer effektiven Strategie für Beobachtbarkeit](#)
- [AWS Summit SF 2022 — Full-Stack-Beobachtbarkeit und Anwendungsüberwachung mit AWS](#)
- [AWS re:Invent 2023 — Weitere Skalierung AWS für die ersten 10 Millionen Nutzer](#)
- [AWS re:Invent 2022 — Wie Amazon bessere Metriken für eine verbesserte Website-Performance verwendet](#)
- [Erstellung einer effektiven Metrik-Strategie für Ihr Unternehmen | Veranstaltungen AWS](#)

## Zugehörige Beispiele:

- [Ein Dashboard mit Amazon erstellen QuickSight](#)

PERF05-BP02 Verwenden Sie Überwachungslösungen, um die Bereiche zu verstehen, in denen Leistung am wichtigsten ist

Ermitteln Sie die Bereiche, in denen sich durch Steigern der Workload-Leistung positive Auswirkungen auf die Effizienz oder den Kundenkomfort realisieren lassen. Beispiel: Eine Website mit zahlreichen Kundeninteraktionen kann von der Nutzung von Edge-Services profitieren, indem Inhalte näher bei den Kunden bereitgestellt werden.

## Typische Anti-Muster:

- Sie gehen davon aus, dass Standard-Rechenmetriken wie CPU Auslastung oder Speicherauslastung ausreichen, um Leistungsprobleme zu erkennen.
- Sie verwenden nur die Standardmetriken, die von der Überwachungssoftware Ihrer Wahl aufgezeichnet wurden.
- Sie überprüfen Metriken nur dann, wenn ein Problem vorliegt.

Vorteile der Einführung dieser bewährten Methode: Das Verständnis kritischer Leistungsbereiche hilft Workload-Besitzern dabei, Verbesserungen mit großer Wirkung zu überwachen KPIs und zu priorisieren.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Hoch

### Implementierungsleitfaden

Richten Sie end-to-end die Ablaufverfolgung ein, um Verkehrsmuster, Latenz und kritische Leistungsbereiche zu identifizieren. Überwachen Sie Ihre Datenzugriffsmuster auf langsame Abfragen oder schlecht fragmentierte und partitionierte Daten. Identifizieren Sie problematische Workload-Bereiche mithilfe von Lasttests oder -überwachung.

Erhöhen Sie die Leistungseffizienz durch eingehendes Verständnis Ihrer Architektur, der Datenverkehrs- und der Datenzugriffsmuster und identifizieren Sie Ihre Latenz- und Verarbeitungszeiten. Identifizieren Sie potenzielle Engpässe, die sich bei zunehmenden Workloads auf den Kundenkomfort auswirken könnten. Nachdem Sie diese Bereiche untersucht haben, sollten Sie prüfen, welche Lösung Sie nutzen können, um diese Leistungsprobleme zu beseitigen.

### Implementierungsschritte

- Richten Sie die end-to-end Überwachung ein, um alle Workload-Komponenten und -Metriken zu erfassen. Hier finden Sie Beispiele für Überwachungslösungen auf AWS.

Service	Aktion
<a href="#">Amazon-Überwachung von CloudWatch echten Benutzern () RUM</a>	Zum Erfassen von Metriken zur Anwendung Leistung aus realen clientseitigen und Frontend-Sitzungen.
<a href="#">AWS X-Ray</a>	Zum Verfolgen des Datenverkehrs durch die Anwendungsebenen und zum Identifizieren der Latenz zwischen Komponenten und Abhängigkeiten. Verwenden Sie X-Ray-Service-Zuordnungen, um Beziehungen und Latenz zwischen Workload-Komponenten zu erkennen.



Service	Aktion
<a href="#">Amazon Relational Database Service – Performance Insights</a>	Zum Anzeigen von Metriken zur Datenbankleistung und zum Identifizieren von Möglichkeiten zur Leistungsverbesserung.
<a href="#">RDSVerbesserte Überwachung durch Amazon</a>	Zum Anzeigen von Datenbank-BS-Leistungsmetriken.
<a href="#">DevOpsAmazon-Guru</a>	Zum Erkennen ungewöhnlicher Betriebsmuster, damit Sie betriebliche Probleme identifizieren können, bevor sie sich auf Ihre Kunden auswirken.

- Führen Sie Tests durch, um Metriken zu generieren sowie Datenverkehrsmuster, Engpässe und kritische Leistungsbereiche zu identifizieren. Hier finden Sie einige Beispiele zum Durchführen von Tests:
  - Richten Sie [CloudWatchSynthetic Canaries](#) ein, um browserbasierte Benutzeraktivitäten mithilfe von Linux-Cronjobs oder Bewertungsausdrücken programmgesteuert nachzuahmen, um im Laufe der Zeit konsistente Metriken zu generieren.
  - Verwenden Sie die Lösung für [verteilte Lasttests auf AWS](#), um Spitzendatenverkehr zu generieren oder Workloads mit der erwarteten Wachstumsrate zu testen.
- Evaluieren Sie die Metriken und die Telemetriedaten, um Ihre kritischen Leistungsbereiche zu identifizieren. Prüfen Sie diese Bereiche zusammen mit Ihrem Team und besprechen Sie Überwachung und Lösung zur Vermeidung von Engpässen.
- Experimentieren Sie mit Leistungsverbesserungen und messen Sie diese Änderungen anhand von Daten. Sie können [CloudWatchEvidently beispielsweise verwenden, um neue Verbesserungen und Auswirkungen auf die Leistung](#) Ihres Workloads zu testen.

## Ressourcen

### Zugehörige Dokumente:

- [Was gibt es Neues im Bereich AWS Observability auf der re:Invent 2023](#)
- [Amazon Builders' Library](#)
- [X-Ray-Dokumentation](#)
- [Amazon CloudWatch RUM](#)

- [DevOpsAmazon-Guru](#)

#### Zugehörige Videos:

- [AWS re:Invent 2023 - \[LAUNCH\] Anwendungsüberwachung für moderne Workloads](#)
- [AWS re:Invent 2023 — Implementierung der Anwendungsbeobachtbarkeit](#)
- [AWS re:Invent 2023 — Aufbau einer effektiven Beobachtungsstrategie](#)
- [AWS Summit SF 2022 — Full-Stack-Beobachtbarkeit und Anwendungsüberwachung mit AWS](#)
- [AWS re:Invent 2022 — AWS Optimierung: Umsetzbare Schritte für sofortige Ergebnisse](#)
- [AWS re:Invent 2022 — Die Amazon Builders' Library: 25 Jahre operative Exzellenz bei Amazon](#)
- [AWS re:Invent 2022 — Wie Amazon bessere Metriken für eine verbesserte Website-Performance verwendet](#)
- [Visuelle Überwachung von Anwendungen mit Amazon CloudWatch Synthetics](#)

#### Zugehörige Beispiele:

- [Messen Sie die Seitenladezeit mit Amazon CloudWatch Synthetics](#)
- [CloudWatch RUMAmazon-Webclient](#)
- [X-Ray SDK für Python](#)
- [Testen verteilter Lasten auf AWS](#)

PERF05-BP03 Definieren Sie einen Prozess zur Verbesserung der Workload-Leistung

Definieren Sie einen Prozess, mit dem sich neu verfügbare Services, Designmuster, Ressourcentypen und Konfigurationen bewerten lassen. Führen Sie beispielsweise vorhandene Leistungstests für neue Instance-Angebote durch, um zu ermitteln, welche Verbesserungen sich für Ihre Workload ergeben.

#### Typische Anti-Muster:

- Sie gehen davon aus, dass Ihre aktuelle Architektur statisch ist und im Laufe der Zeit nicht aktualisiert wird.
- Sie führen im Laufe der Zeit Änderungen an der Architektur ein, ohne sie begründen.

Vorteile der Nutzung dieser bewährten Methode: Durch einen definierten Prozess zum Ändern der Architektur erhalten Sie die Möglichkeit, die gesammelten Daten langfristig in die Gestaltung Ihrer Workload einfließen zu lassen.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Mittel

### Implementierungsleitfaden

Für Ihre Workload gibt es einige wesentliche Einschränkungen. Dokumentieren Sie diese, damit Sie besser einschätzen können, durch welche Art von Innovation die Leistung Ihrer Workload gesteigert werden könnte. Ziehen Sie diese Informationen heran, wenn Sie von neuen verfügbaren Services oder Technologien erfahren, um Möglichkeiten zur Beseitigung von Einschränkungen oder Engpässen zu identifizieren.

Identifizieren Sie wesentliche Leistungseinschränkungen für Ihre Workload. Dokumentieren Sie die Leistungseinschränkungen Ihrer Workload, damit Sie besser einschätzen können, durch welche Art von Innovation die Leistung Ihrer Workload ggf. gesteigert werden kann.

### Implementierungsschritte

- **Identifizieren KPIs:** Identifizieren Sie Ihre Workload-Leistung, KPIs wie unter beschrieben, um Ihre Arbeitslast als Ausgangsbasis [PERF05-BP01 Festlegung wichtiger Leistungsindikatoren \(KPIs\) zur Messung des Zustands und der Leistung der Arbeitslast](#) zu definieren.
- **Implementieren Sie die Überwachung:** Verwenden Sie [AWS Beobachtungstools](#), um Leistungskennzahlen zu sammeln und zu messen KPIs.
- **Durchführen einer Analyse:** Führen Sie eine eingehende Analyse durch, um die Bereiche (wie Konfiguration und Anwendungscode) in Ihrer Workload zu identifizieren, die leistungsschwach sind, wie beschrieben unter [PERF05-BP02 Verwenden Sie Überwachungslösungen, um die Bereiche zu verstehen, in denen Leistung am wichtigsten ist](#). Verwenden Sie Analyse- und Leistungstools, um die Strategie zur Leistungsverbesserung zu identifizieren.
- **Validieren von Verbesserungen:** Verwenden Sie Sandbox- oder Vorproduktionsumgebungen, um die Effektivität von Verbesserungsstrategien zu überprüfen.
- **Implementieren von Änderungen:** Implementieren Sie die Änderungen in der Produktion und überwachen Sie kontinuierlich die Leistung der Workload. Dokumentieren Sie die Verbesserungen und teilen Sie die Änderungen den Stakeholdern mit.
- **Wiederaufgreifen und verfeinern:** Überprüfen Sie regelmäßig Ihren Prozess zur Leistungsverbesserung, um Bereiche mit Verbesserungspotenzial zu identifizieren.

## Ressourcen

### Zugehörige Dokumente:

- [AWS -Blog](#)
- [Was ist neu bei AWS](#)
- [AWS Skill Builder](#)

### Zugehörige Videos:

- [AWS re:Invent 2022 — Bereitstellung nachhaltiger, leistungsstarker Architekturen](#)
- [AWS re:Invent 2023 — Optimieren Sie Kosten und Leistung und verfolgen Sie die Fortschritte bei der Eindämmung](#)
- [AWS re:Invent 2022 — AWS Optimierung: Umsetzbare Schritte für sofortige Ergebnisse](#)
- [AWS re:Invent 2022 — Optimieren Sie Ihre Workloads mit Best-Practice-Anleitungen AWS](#)

### Zugehörige Beispiele:

- [AWS Github](#)

## PERF05-BP04 Belastungstest Ihr Workload

Führen Sie für die Workload Lasttests durch, um sicherzustellen, dass sie die Produktionslast bewältigen kann, und identifizieren Sie Leistungsengpässe.

### Typische Anti-Muster:

- Sie führen Lasttests für einzelne Teile der Workload durch, aber nicht für die gesamte Workload.
- Sie führen Lasttests in einer Infrastruktur durch, die sich von Ihrer Produktionsumgebung unterscheidet.
- Sie führen Lasttests nur für die erwartete Last durch und nicht für noch größere Lasten, um mögliche künftige Probleme besser vorherzusehen.
- Sie führen Belastungstests durch, ohne die [Amazon EC2 Testing Policy zu lesen](#) und ein Formular zur Einreichung von simulierten Ereignissen einzureichen. Dies führt dazu, dass Ihr Test nicht ausgeführt werden kann, da er wie ein denial-of-service Ereignis aussieht.

Vorteile der Nutzung dieser bewährten Methode: Die Messung der Leistung im Rahmen eines Lasttests gibt Aufschluss darüber, wo bei zunehmender Last mit Auswirkungen zu rechnen ist. Auf diese Weise können Sie erforderliche Änderungen vorhersehen, bevor sie sich auf Ihre Workload auswirken.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Niedrig

### Implementierungsleitfaden

Lasttests in der Cloud sind ein Prozess zur Messung der Leistung einer Cloud-Workload unter realistischen Bedingungen mit erwarteter Benutzerlast. Dieser Prozess beinhaltet die Bereitstellung einer produktionsähnlichen Cloud-Umgebung, die Verwendung von Lasttest-Tools zur Lastgenerierung und die Analyse von Metriken, um die Fähigkeit Ihrer Workload zu bewerten, mit einer realistischen Last umzugehen. Verwenden Sie für Lasttests synthetische oder bereinigte Produktionsdaten und entfernen Sie sensible oder personenbezogene Informationen. Führen Sie automatisch Lasttests als Teil Ihrer Bereitstellungs pipeline durch und vergleichen Sie die Ergebnisse mit vordefinierten Grenzwerten KPIs und Schwellenwerten. Dieser Prozess hilft Ihnen dabei, die erforderliche Leistung weiterhin zu erreichen.

### Implementierungsschritte

- **Testziele definieren:** Identifizieren Sie die Leistungsaspekte Ihrer Workload, die Sie bewerten möchten, wie Durchsatz und Reaktionszeit.
- **Testtool auswählen:** Wählen und konfigurieren Sie das Lasttest-Tool, das zu Ihrer Workload passt.
- **Umgebung einrichten:** Richten Sie die Testumgebung auf der Grundlage Ihrer Produktionsumgebung ein. Sie können AWS Services verwenden, um Produktionsumgebungen auszuführen und Ihre Architektur zu testen.
- **Implementieren Sie Überwachung:** Verwenden Sie Überwachungstools wie [Amazon CloudWatch](#), um Kennzahlen für alle Ressourcen in Ihrer Architektur zu sammeln. Sie können auch benutzerdefinierte Metriken erfassen und veröffentlichen.
- **Szenarien definieren:** Definieren Sie die Szenarien und Parameter der Lasttests (wie Testdauer und Anzahl der Benutzer).
- **Belastungstests durchführen:** Führen Sie Testszenarien in großem Maßstab durch. Nutzen Sie das AWS Cloud , um Ihren Workload zu testen und herauszufinden, wo er nicht skaliert werden kann oder ob er nicht linear skaliert wird. Nutzen Sie beispielsweise Spot Instances, um kostengünstig Lasten zu erzeugen und Engpässe zu identifizieren, bevor diese in der Produktionsumgebung auftreten.

- **Testergebnisse analysieren:** Analysieren Sie die Ergebnisse, um Leistungsengpässe und verbesserungswürdige Bereiche zu identifizieren.
- **Erkenntnisse dokumentieren und teilen:** Dokumentieren Sie Erkenntnisse und Empfehlungen und erstellen Sie Berichte darüber. Teilen Sie diese Informationen mit Stakeholdern, um ihnen zu helfen, fundierte Entscheidungen über Strategien zur Leistungsoptimierung zu treffen.
- **Kontinuierliche Iteration:** Lasttests sollten in regelmäßigen Abständen durchgeführt werden, insbesondere nach einer Systemänderung oder einem Systemupdate.

## Ressourcen

### Zugehörige Dokumente:

- [Amazon CloudWatch RUM](#)
- [Amazon CloudWatch Synthetics](#)
- [Testen verteilter Lasten auf AWS](#)

### Zugehörige Videos:

- [AWS Summit ANZ 2023: Mit AWS Distributed Load Testing mit Zuversicht beschleunigen](#)
- [AWS re:Invent 2022 — Weitere Skalierung AWS für Ihre ersten 10 Millionen Benutzer](#)
- [Problemlösung mit AWS Lösungen: Testen verteilter Lasten](#)
- [AWS re:Invent 2021 — Optimieren Sie Anwendungen mithilfe von Erkenntnissen für Endbenutzer mit Amazon CloudWatch RUM](#)
- [Demo von Amazon CloudWatch Synthetics](#)

### Zugehörige Beispiele:

- [Verteilte Belastungstests auf AWS](#)

PERF05-BP05 Verwenden Sie Automatisierung, um leistungsbezogene Probleme proaktiv zu beheben

Verwenden Sie wichtige Leistungsindikatoren (KPIs) in Kombination mit Überwachungs- und Warnsystemen, um leistungsbezogene Probleme proaktiv anzugehen.

## Typische Anti-Muster:

- Sie geben dem Betriebspersonal nur die Möglichkeit, betriebliche Änderungen an der Workload vorzunehmen.
- Sie lassen alle Alarme ohne proaktive Behebung zum Operations-Team filtern.

Vorteile der Nutzung dieser bewährten Methode: Die proaktive Behebung von Alarmaktionen ermöglicht es dem Support-Personal, sich auf die Elemente zu konzentrieren, die nicht automatisch umsetzbar sind. Dies hilft dem Betriebspersonal, alle Alarme zu bewältigen, ohne überfordert zu werden, und sich stattdessen auf die kritischen Alarme zu konzentrieren.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Niedrig

## Implementierungsleitfaden

Verwenden Sie Alarme, um automatisierte Aktionen auszulösen und auf diese Weise Probleme nach Möglichkeit zu beheben. Leiten Sie den Alarm an die Personen weiter, die die richtigen Maßnahmen einleiten können, falls keine automatisierte Reaktion möglich ist. Möglicherweise verfügen Sie über ein System, das erwartete Werte von Leistungskennzahlen (KPI) vorhersagen und bei Überschreitung bestimmter Schwellenwerte einen Alarm auslösen kann, oder ein Tool, das Bereitstellungen automatisch anhalten oder rückgängig machen kann, wenn KPIs die erwarteten Werte nicht eingehalten werden.

Implementieren Sie Prozesse, die Ihnen Einblick in die Leistung gewähren, während Ihre Workload ausgeführt wird. Entwickeln Sie Dashboards für die Überwachung und legen Sie Leistungsnormen in Form von Grundwerten fest, um zu bestimmen, ob die Workload optimal funktioniert.

## Implementierungsschritte

- Identifizierung eines Fehlerbehebungs-Workflows: Identifizieren und verstehen Sie das Leistungsproblem, das automatisch behoben werden kann. Verwenden Sie AWS Überwachungslösungen wie [Amazon CloudWatch](#) oder AWS X-Ray, um die Ursache des Problems besser zu verstehen.
- Definieren Sie den Automatisierungsprozess: Erstellen Sie einen step-by-step Behebungsprozess, mit dem das Problem automatisch behoben werden kann.
- Konfiguration des Initiierungseignisses: Konfigurieren Sie das Ereignis so, dass der Prozess zur Mängelbeseitigung automatisch eingeleitet wird. Sie können beispielsweise einen Trigger definieren, der eine Instance automatisch neu startet, wenn sie einen bestimmten CPU Nutzungsschwellenwert erreicht.

- Automatisieren Sie die Problembehebung: Verwenden Sie AWS Dienste und Technologien, um den Behebungsprozess zu automatisieren. Beispielsweise bietet [AWS Systems Manager Automation](#) eine sichere und skalierbare Möglichkeit, den Prozess zur Mängelbeseitigung zu automatisieren. Achten Sie darauf, die Selbstheilungslogik zu verwenden, um Änderungen rückgängig zu machen, wenn das Problem nicht gelöst wurde.
- Testen des Workflows: Testen Sie den automatisierten Prozess zur Mängelbeseitigung in einer Vorproduktionsumgebung.
- Implementieren des Workflows: Implementieren Sie die automatisierte Mängelbeseitigung in der Produktionsumgebung.
- Entwicklung eines Playbooks: Entwickeln und dokumentieren Sie ein Playbook, in dem die Schritte für den Mängelbeseitigungsplan beschrieben werden, einschließlich der Initiierungsereignisse, der Mängelbeseitigungslogik und der ergriffenen Maßnahmen. Stellen Sie sicher, dass alle Stakeholder entsprechend geschult werden, damit sie effektiv auf automatisierte Mängelbeseitigungsereignisse reagieren können.
- Überprüfen und verfeinern: Bewerten Sie regelmäßig die Effektivität des automatisierten Mängelbeseitigungsworkflows. Passen Sie bei Bedarf die Initiierungsereignisse und die Mängelbeseitigungslogik an.

## Ressourcen

### Zugehörige Dokumente:

- [CloudWatchDokumentation](#)
- [AWS Partner Network Partner für Überwachung, Protokollierung und Leistung](#)
- [X-Ray-Dokumentation](#)
- [Verwenden von Alarmen und Alarmaktionen in CloudWatch](#)
- [Entwickeln Sie eine Cloud-Automatisierungspraxis für betriebliche Exzellenz: Best Practices von AWS Managed Services](#)
- [Automate your Amazon Redshift performance tuning with automatic table optimization](#)

### Zugehörige Videos:

- [AWS re:Invent 2023 — Strategien für automatisierte Skalierung, Problembehebung und intelligente Selbstheilung](#)
- [AWS re:Invent 2023 — \[ \] LAUNCH Anwendungsüberwachung für moderne Workloads](#)



- [AWS re:Invent 2023 — Implementierung der Anwendungsbeobachtbarkeit](#)
- [AWS re:Invent 2021 — Cloud-Operationen intelligent automatisieren](#)
- [AWS re:Invent 2022 — Einrichtung von maßstabsgetreuen Steuerungen in Ihrer Umgebung AWS](#)
- [AWS re:Invent 2022 — Automatisierung des Patch-Managements und der Einhaltung von Vorschriften mithilfe AWS](#)
- [AWS re:Invent 2022 — Wie Amazon bessere Metriken für eine verbesserte Website-Performance verwendet](#)
- [AWS re:Invent 2023 — Entlasten: Leistungsprobleme mit Amazon diagnostizieren und lösen RDS](#)
- [AWS re:Invent 2021 — {New Launch} Automatische Erkennung und Lösung von Problemen mit Amazon Guru DevOps](#)
- [AWS re:Invent 2023 — Zentralisieren Sie Ihren Betrieb](#)

Zugehörige Beispiele:

- [CloudWatch Protokolle, individuelle Alarmer](#)

PERF05-BP06 Behalten Sie Ihren Workload und Ihre Services up-to-date

Bleiben Sie up-to-date auf der Suche nach neuen Cloud-Diensten und -Funktionen, um effiziente Funktionen einzuführen, Probleme zu beheben und die allgemeine Leistungseffizienz Ihres Workloads zu verbessern.

Typische Anti-Muster:

- Sie gehen davon aus, dass Ihre aktuelle Architektur statisch ist und im Laufe der Zeit nicht aktualisiert wird.
- Sie haben keine Systeme oder regelmäßigen Besprechungen zur Prüfung, ob aktualisierte Software und Pakete mit Ihrer Workload kompatibel sind.

Vorteile der Einführung dieser bewährten Methode: Durch die Einrichtung eines Prozesses up-to-date zur Beibehaltung neuer Services und Angebote können Sie neue Funktionen und Fähigkeiten einführen, Probleme lösen und die Workload-Leistung verbessern.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Niedrig

## Implementierungsleitfaden

Evaluieren Sie Möglichkeiten zur Verbesserung der Leistung, wenn neue Services, Entwurfsmuster und Produktfunktionen verfügbar sind. Ermitteln Sie anhand von Bewertungen, internen Diskussionen oder externen Analysen, wie sich diese neuen Optionen positiv auf die Leistung oder Effizienz der Workload auswirken können. Definieren Sie einen Prozess zum Bewerten von Updates, neuen Features und Services, die für Ihre Workload relevant sind. Erstellen Sie beispielsweise Machbarkeitsstudien, die auf neuen Technologien aufbauen, oder beraten Sie sich mit einer internen Gruppe. Führen Sie beim Ausprobieren neuer Ideen oder Services Leistungstests durch, um die Auswirkungen auf die Leistung der Workload zu messen.

## Implementierungsschritte

- Inventarisierung Ihrer Workload: Inventarisieren Sie Ihre Workload-Software und -Architektur und identifizieren Sie Komponenten, die aktualisiert werden müssen.
- Identifizierung von Quellen für Updates: Identifizieren Sie Quellen für Neuigkeiten und Updates im Zusammenhang mit Ihren Workload-Komponenten. Sie können beispielsweise den [AWS Blog What's New at](#) abonnieren, um die Produkte zu finden, die zu Ihrer Workload-Komponente passen. Sie können den RSS Feed abonnieren oder Ihre [E-Mail-Abonnements](#) verwalten.
- Definition eines Aktualisierungszeitplans: Definieren Sie einen Zeitplan zur Evaluierung neuer Services und Features für Ihre Workload.
  - Sie können [AWS Systems Manager Inventory](#) verwenden, um Betriebssystem- (OS), Anwendungs- und Instance-Metadaten von Ihren EC2 Amazon-Instances zu sammeln und so schnell zu verstehen, auf welchen Instances die Software und die Konfigurationen ausgeführt werden, die gemäß Ihrer Softwarerichtlinie erforderlich sind, und welche Instances aktualisiert werden müssen.
- Bewertung der neuen Aktualisierung: Erfahren Sie, wie die Komponenten Ihrer Workload aktualisiert werden. Nutzen Sie die Agilität in der Cloud, um schnell zu testen, wie neue Features Ihre Workload verbessern und so die Leistungseffizienz steigern können.
- Verwendung von Automatisierung: Verwenden Sie Automatisierung für den Aktualisierungsvorgang, um den Aufwand für die Bereitstellung neuer Features zu reduzieren und Fehler zu begrenzen, die durch manuelle Prozesse verursacht werden.
  - Sie können [CI/CD](#) verwenden AMIs, um Container-Images und andere Artefakte im Zusammenhang mit Ihrer Cloud-Anwendung automatisch zu aktualisieren.

- Sie können Tools wie den [AWS Systems Manager Patch Manager](#) verwenden, um den Systemaktualisierungsprozess zu automatisieren und die Aktivitäten mit [AWS Systems Manager Maintenance Windows](#) zu planen.
- Dokumentation des Prozesses: Dokumentieren Sie Ihren Prozess zur Evakuierung von Aktualisierungen und neuen Services. Geben Sie Ihren Eigentümern ausreichend Zeit und Raum zum Forschen, Testen, Experimentieren und zur Validierung von Aktualisierungen und neuen Services. Schauen Sie sich die dokumentierten Geschäftsanforderungen KPIs an und finden Sie heraus, welche Aktualisierung sich positiv auf Ihr Unternehmen auswirken wird.

## Ressourcen

### Zugehörige Dokumente:

- [AWS -Blog](#)
- [Was ist neu bei AWS](#)
- [Implementieren von up-to-date Images mit automatisierten EC2 Image Builder Builder-Pipelines](#)

### Zugehörige Videos:

- [AWS re:INFORCE 2022 — Automatisierung von Patch-Management und Compliance mithilfe AWS](#)
- [All Things Patch: | Veranstaltungen AWS Systems ManagerAWS](#)

### Zugehörige Beispiele:

- [Bestands- und Patch-Verwaltung](#)
- [Workshop zur Beobachtbarkeit](#)

PERF05-BP07 Überprüfen Sie die Kennzahlen in regelmäßigen Abständen

Überprüfen Sie im Rahmen der routinemäßigen Wartungsmaßnahme oder als Reaktion auf Ereignisse oder Vorfälle, welche Metriken erfasst werden. Ermitteln Sie anhand dieser Überprüfung, welche Metriken für die Behebung von Problemen wesentlich waren und welche zusätzlichen Metriken, sofern nachverfolgt, helfen könnten, Probleme zu identifizieren, zu beheben oder zu verhindern.

### Typische Anti-Muster:

- Sie lassen zu, dass Metriken für einen längeren Zeitraum im Alarmstatus bleiben.
- Sie erstellen Alarme, die von einem Automatisierungssystem nicht umsetzbar sind.

Vorteile der Nutzung dieser bewährten Methode: Überprüfen Sie kontinuierlich Metriken, die erfasst werden, um zu bestätigen, dass sie Probleme ordnungsgemäß identifizieren, beheben oder verhindern. Metriken können auch veralten, wenn sie für einen längeren Zeitraum im Alarmstatus bleiben.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Mittel

### Implementierungsleitfaden

Verbessern Sie kontinuierlich die Erfassung und Überwachung von Metriken. Bewerten Sie beim Reagieren auf Vorfälle oder Ereignisse diejenigen Metriken, die hilfreich für die Behebung des Problems waren, und überlegen Sie, welche derzeit noch nicht verfolgten Metriken förderlich sein könnten. Verbessern Sie auf diese Weise die Qualität der erfassten Metriken, damit Sie zukünftige Probleme verhindern oder schneller beheben können.

Bewerten Sie beim Reagieren auf Vorfälle oder Ereignisse diejenigen Metriken, die hilfreich für die Behebung des Problems waren, und überlegen Sie, welche derzeit noch nicht verfolgten Metriken förderlich sein könnten. Verbessern Sie auf diese Weise die Qualität der erfassten Metriken, damit Sie zukünftige Probleme verhindern oder schneller beheben können.

### Implementierungsschritte

- **Metriken definieren:** Definieren Sie wichtige Leistungsmetriken zur Überwachung, die auf Ihr Workload-Ziel abgestimmt sind, einschließlich Metriken wie Reaktionszeit und Ressourcenauslastung.
- **Ausgangswert festlegen:** Legen Sie für jede Metrik einen Ausgangswert und einen Zielwert fest. Der Ausgangswert sollte Referenzpunkte zur Identifizierung von Abweichungen oder Anomalien enthalten.
- **Takt festlegen:** Legen Sie einen Takt zur Überprüfung wichtiger Kennzahlen fest (z. B. wöchentlich oder monatlich).
- **Leistungsprobleme identifizieren:** Beurteilen Sie bei jeder Überprüfung Trends und Abweichungen von den Ausgangswerten. Suchen Sie nach Leistungsengpässen oder Anomalien. Führen Sie bei identifizierten Problemen eine eingehende Ursachenanalyse durch, um den Hauptgrund für das Problem zu ermitteln.

- **Korrekturmaßnahmen identifizieren:** Identifizieren Sie Korrekturmaßnahmen mithilfe Ihrer Analysen. Dies kann die Parameteroptimierung, das Beheben von Fehlern und das Skalieren von Ressourcen beinhalten.
- **Ergebnisse dokumentieren:** Dokumentieren Sie Ihre Erkenntnisse, einschließlich identifizierter Probleme, Ursachen und Korrekturmaßnahmen.
- **Iterieren und verbessern:** Beurteilen und verbessern Sie kontinuierlich den Prozess zur Überprüfung der Metriken. Nutzen Sie die Erkenntnisse aus der vorherigen Überprüfung, um den Prozess im Laufe der Zeit zu verbessern.

## Ressourcen

### Zugehörige Dokumente:

- [CloudWatchDokumentation](#)
- [Erfassen Sie mit dem Agenten Metriken und Protokolle von EC2 Amazon-Instances und lokalen Servern CloudWatch](#)
- [Fragen Sie Ihre Metriken mit CloudWatch Metrics Insights ab](#)
- [AWS Partner Network Partner für Überwachung, Protokollierung und Leistung](#)
- [X-Ray-Dokumentation](#)

### Zugehörige Videos:

- [AWS re:Invent 2022 — Einrichtung skalierbarer Steuerungen in Ihrer Umgebung AWS](#)
- [AWS re:Invent 2022 — Wie Amazon bessere Metriken für eine verbesserte Website-Performance verwendet](#)
- [AWS re:Invent 2023 — Aufbau einer effektiven Strategie für Beobachtbarkeit](#)
- [AWS Summit SF 2022 — Full-Stack-Beobachtbarkeit und Anwendungsüberwachung mit AWS](#)
- [AWS re:Invent 2023 — Entlasten: Leistungsprobleme mit Amazon diagnostizieren und lösen RDS](#)

### Zugehörige Beispiele:

- [Ein Dashboard mit Amazon erstellen QuickSight](#)
- [CloudWatch Dashboards](#)

# Kostenoptimierung

Die Säule „Kostenoptimierung“ umfasst die Fähigkeit, Systeme so auszuführen, dass sie geschäftlichen Wert bei geringstmöglichen Kosten liefern. Verbindliche Anleitungen zur Implementierung finden Sie im [Whitepaper zur Säule „Kostenoptimierung“](#).

Bereiche für bewährte Methoden

- [Praxis für Cloud-Finanzmanagement](#)
- [Ausgabenerkennung und Nutzungsbewusstsein](#)
- [Kostengünstige Ressourcen](#)
- [Verwaltung von Nachfrage und Bereitstellung von Ressourcen](#)
- [Optimierung im Laufe der Zeit](#)

## Praxis für Cloud-Finanzmanagement

Frage

- [COST1. Wie implementieren Sie das Cloud Financial Management?](#)

### COST1. Wie implementieren Sie das Cloud Financial Management?

Durch die Implementierung von Cloud Financial Management können Unternehmen durch die Optimierung ihrer Kosten, Nutzung und Skalierung ihren Geschäftswert und ihren finanziellen Erfolg erzielen AWS.

Bewährte Methoden

- [COST01-BP01 Übernehmen Sie die Verantwortung für die Kostenoptimierung](#)
- [COST01-BP02 Etablieren Sie eine Partnerschaft zwischen Finanzen und Technologie](#)
- [COST01-BP03 Legen Sie Cloud-Budgets und Prognosen fest](#)
- [COST01-BP04 Implementieren Sie Kostenbewusstsein in Ihren organisatorischen Prozessen](#)
- [COST01-BP05 Bericht und Benachrichtigung zur Kostenoptimierung](#)
- [COST01-BP06 Kosten proaktiv überwachen](#)
- [COST01-BP07 Bleiben Sie auf up-to-date dem Laufenden mit neuen Service Releases](#)
- [COST01-BP08 Schaffen Sie eine kostenbewusste Kultur](#)

- [COST01-BP09 Quantifizieren Sie den Geschäftswert der Kostenoptimierung](#)

## COST01-BP01 Übernehmen Sie die Verantwortung für die Kostenoptimierung

Bilden Sie ein Team (Cloud Business Office, Cloud Center of Excellence oder FinOps Team), das für die Schaffung und Aufrechterhaltung des Kostenbewusstseins in Ihrer gesamten Organisation verantwortlich ist. Für die Kostenoptimierung kann eine Einzelperson oder ein Team zuständig sein (mit Mitarbeitern aus dem Finanz-, Technologie- und Geschäftsbereich), Voraussetzung ist eine Übersicht über die gesamte Organisation und die Finanzierung der Cloud.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Hoch

### Implementierungsleitfaden

Dies ist die Einführung einer Funktion oder eines Teams im Bereich Cloud Business Office (CBO) oder Cloud Center of Excellence (CCOE), das für den Aufbau und die Aufrechterhaltung einer Kultur des Kostenbewusstseins im Cloud-Computing verantwortlich ist. Bei dieser Funktion kann es sich um eine bereits in der Organisation hierfür zuständige Person, ein Team innerhalb Ihrer Organisation oder um ein neues Team handeln, das sich aus den wichtigsten Finanz-, Technologie- und Organisationsbeteiligten aus der gesamten Organisation zusammensetzt.

Die Funktion (Einzelperson oder Team) priorisiert und verbraucht den erforderlichen Prozentsatz ihrer Zeit für Kostenmanagement- und Kostenoptimierungsaktivitäten. Bei kleinen Unternehmen kann die Funktion einen geringeren Prozentsatz der Zeit im Vergleich zu einer Vollzeitfunktion für ein größeres Unternehmen aufwenden.

Die Funktion erfordert einen multidisziplinären Ansatz, der Kompetenzen in den Bereichen Projektmanagement, Datenwissenschaft, Finanzanalyse und Software- oder Infrastrukturentwicklung voraussetzt. Die Mitarbeiter können die Effizienz von Workloads durch Kostenoptimierungen auf drei unterschiedlichen Verantwortlichkeitsebenen verbessern:

- Zentralisiert: Durch spezielle Teams wie FinOps Team, Cloud Financial Management (CFM) - Team, Cloud Business Office (CBO) oder Cloud Center of Excellence (CCoE) können Kunden Governance-Mechanismen entwerfen und implementieren und unternehmensweit bewährte Verfahren vorantreiben.
- Dezentralisiert: Hierbei werden Technologieteams mit der Durchführung von Kostenoptimierungen beauftragt.
- Hybrid: Zentralisierte und dezentralisierte Teams arbeiten gemeinsam an der Umsetzung von Kostenoptimierungen.

Die Funktion kann anhand ihrer Fähigkeit zur Durchführung und Implementierung im Hinblick auf Kostenoptimierungsziele gemessen werden (z. B. durch Workload-Effizienzmetriken).

Sie müssen sicherstellen, dass Führungskräfte diese Funktion als Sponsoren/Förderer unterstützen. Dies ist ein entscheidender Erfolgsfaktor. Der entsprechende Sponsor befürwortet eine kosteneffiziente Cloud-Nutzung und bietet Eskalationsunterstützung für das Team, um sicherzustellen, dass die Aktivitäten zur Kostenoptimierung mit der von der Organisation definierten Priorität behandelt werden. Andernfalls können Anweisungen nicht beachtet und Möglichkeiten für Kosteneinsparungen nicht priorisiert werden. Gemeinsam helfen der Sponsor und das Team Ihrer Organisation dabei, die Cloud effizient zu nutzen und Unternehmenswert zu schaffen.

Wenn Sie den Business Enterprise-On-Ramp - oder [Enterprise-Supportplan](#) haben und Hilfe beim Aufbau dieses Teams oder dieser Funktion benötigen, wenden Sie sich über Ihr Account-Team an Ihre Cloud Financial Management (CFM) -Experten.

### Implementierungsschritte

- **Definieren wichtiger Mitglieder:** Alle relevanten Bereiche Ihrer Organisation müssen ihren Beitrag leisten und ein Interesse an der Kostenverwaltung haben. Zu den üblichen Teams innerhalb von Organisationen gehören in der Regel: Finanz-, Anwendungs- oder Produktverantwortliche, Management- und Technikteams (DevOps). Einige Teams setzen ihre ganze Arbeitszeit hierfür ein (Finanz- und Technikbereich), während andere nach Bedarf eingebunden werden. Einzelne Personen oder Teams CFM benötigen die folgenden Fähigkeiten:
  - **Softwareentwicklung:** um Skripts und Automatisierungen entwickeln zu können.
  - **Infrastrukturentwicklung:** um Skripts bereitzustellen, Prozesse zu automatisieren und zu verstehen, wie Services oder Ressourcen bereitgestellt werden.
  - **Geschäftssinn:** Hier CFM geht es darum, effizient in der Cloud zu arbeiten, indem die effiziente Nutzung der Cloud gemessen, überwacht, geändert, geplant und skaliert wird.
- **Definieren von Zielen und Metriken:** Die Funktion muss der Organisation auf verschiedene Weise Mehrwert bieten. Diese Ziele werden definiert und mit der Entwicklung der Organisation kontinuierlich weiterentwickelt. Häufige Aktivitäten sind das Erstellen und Durchführen von Schulungsprogrammen zur Kostenoptimierung in der gesamten Organisation, Entwickeln von organisationsweiten Standards wie Überwachung und Berichterstellung zur Kostenoptimierung sowie Festlegen der Workload-Ziele bei der Optimierung. Außerdem muss diese Funktion der Organisation regelmäßig über ihre Möglichkeiten zur Kostenoptimierung Bericht erstatten.

Sie können wert- oder kostenbasierte Leistungsindikatoren definieren (KPIs). Wenn Sie die definieren KPIs, können Sie die erwarteten Kosten in Bezug auf Effizienz und erwartete



Geschäftsergebnisse berechnen. Wertbasiert KPIs verknüpfen Kosten- und Nutzungskennzahlen mit den Wertfaktoren des Unternehmens und helfen so, Ausgabenänderungen zu rationalisieren. AWS Der erste Schritt zur wertbasierten Ableitung KPIs besteht in der organisationsübergreifenden Zusammenarbeit, um ein Standardpaket auszuwählen und zu vereinbaren. KPIs

- Regelmäßigen Rhythmus etablieren: Die Gruppe (Teams aus den Bereichen Finanzen, Technologie und Geschäft) sollte sich regelmäßig treffen, um Ziele und Metriken zu überprüfen. Dazu gehört in der Regel die Überprüfung des Status der Organisation, der aktuell ausgeführten Programme und der gesamten Finanz- und Optimierungsmetriken. Anschließend werden detaillierte Berichte zu wichtigen Workloads erstellt.

Bei diesen regelmäßigen Überprüfungen können Sie die Workload-Effizienz (Kosten) und die geschäftlichen Ergebnisse bewerten. Eine Kostensteigerung von 20 % für eine Workload könnte beispielsweise mit einer erhöhten Nutzung durch Kunden zusammenhängen. In einem solchen Fall kann die Kostensteigerung von 20 % als Investition betrachtet werden. Diese regelmäßigen Telefongespräche können Teams dabei helfen, Werte zu identifizieren, die für KPIs das gesamte Unternehmen von Bedeutung sind.

## Ressourcen

### Zugehörige Dokumente:

- [AWS CCOE-Blog](#)
- [Einrichtung von Cloud Business Office](#)
- [CCOE- Cloud-Exzellenzzentrum](#)

### Zugehörige Videos:

- [CCOEErfolgsgeschichte von Vanguard](#)

### Zugehörige Beispiele:

- [Nutzung eines Cloud Center of Excellence \(CCOE\) zur Transformation des gesamten Unternehmens](#)
- [Aufbau eines CCOE, um das gesamte Unternehmen zu transformieren](#)
- [7 Fallstricke, die Sie beim Bauen vermeiden sollten CCOE](#)

## COST01-BP02 Etablieren Sie eine Partnerschaft zwischen Finanzen und Technologie

Beziehen Sie Finanz- und Technologieteams in Kosten- und Nutzungsgespräche in allen Phasen Ihres Wegs in die Cloud mit ein. Teams treffen sich regelmäßig, um Themen wie Organisationsziele, aktuellen Kosten- und Nutzungsstatus sowie Finanz- und Buchhaltungsmethoden zu besprechen.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Hoch

### Implementierungsleitfaden

Technologieteams können in der Cloud dank verkürzter Genehmigungs-, Beschaffungs- und Infrastrukturbereitstellungszyklen schneller Innovationen vorantreiben. Dies kann eine Anpassung für Finanzorganisationen sein, die zuvor an die Ausführung zeitaufwändiger und ressourcenintensiver Prozesse zur Beschaffung und Bereitstellung von Kapital in Rechenzentrums- und On-Premises-Umgebungen und die Kostenzuordnung nur nach Projektgenehmigung gewöhnt waren.

Was die Finanz- und Beschaffungsabteilungen betrifft, wurden die Prozesse in den Bereichen Budgetierung, Kapitalbedarf, Genehmigung, Beschaffung und Installation der physischen Infrastruktur über Jahrzehnte hinweg weiterentwickelt und standardisiert.

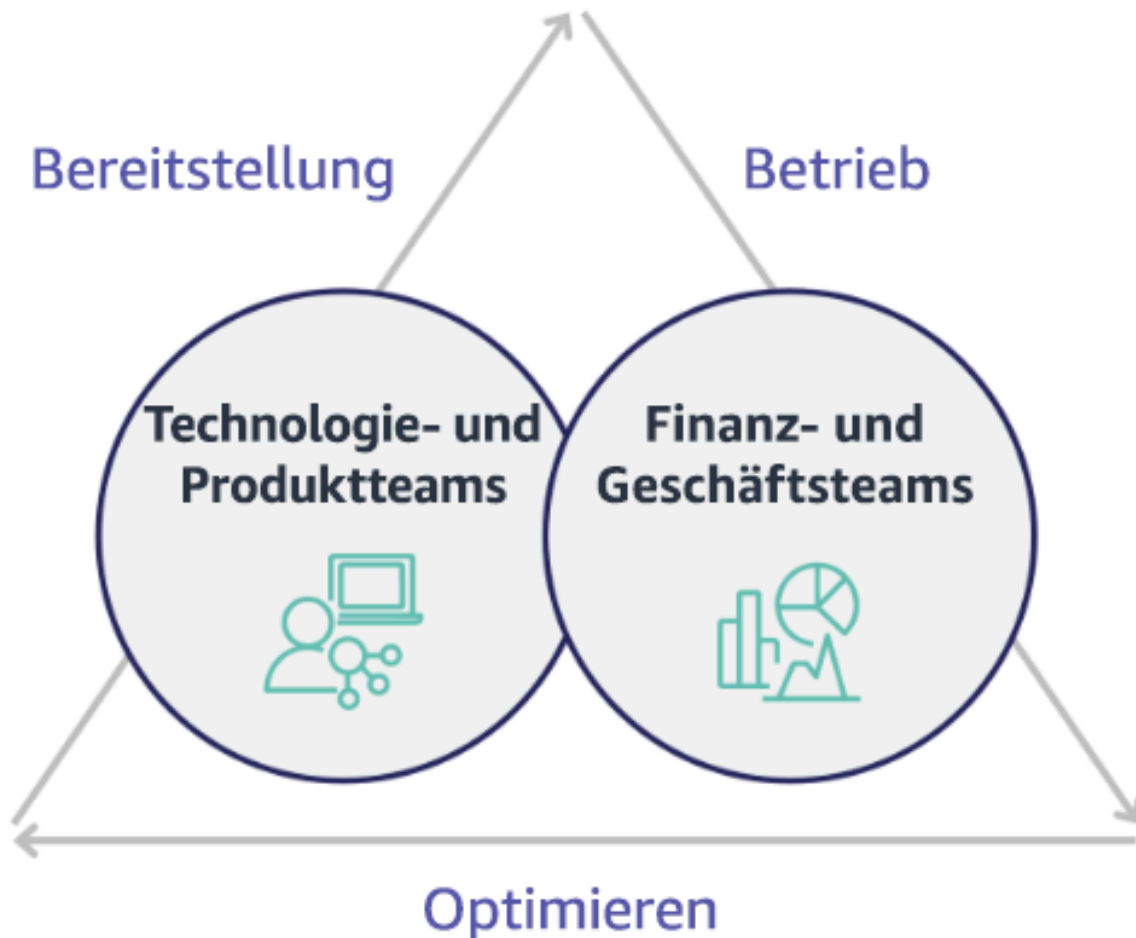
- In der Regel fordern die Entwicklungs- oder IT-Teams die Geldmittel an.
- Die Finanzteams genehmigen und beschaffen die Geldmittel.
- Betriebsteams stapeln, stapeln und übergeben die Infrastruktur ready-to-use



Mit der Einführung der Cloud werden Beschaffung und Nutzung der Infrastruktur nicht mehr als Kette von Abhängigkeiten betrachtet. Im Cloud-Modell entwickeln Technologie- und Produktteams ihre Produkte nicht nur, sondern führen sie auch selbst aus und sind für sie verantwortlich. Dabei führen sie die meisten Aktivitäten aus, die bisher als Domäne der Finanz- und Betriebsteams betrachtet wurden, einschließlich Beschaffung und Bereitstellung.

Zur Bereitstellung von Cloud-Ressourcen werden lediglich ein Konto und der richtige Satz von Berechtigungen benötigt. Dadurch werden auch die IT- und Finanzrisiken reduziert. Das bedeutet, dass Teams immer nur ein paar Klicks oder API Aufrufe davon entfernt sind, ungenutzte oder unnötige Cloud-Ressourcen zu beenden. Technologieteams können so auch schneller Innovationen einführen und erhalten die nötige Agilität und Flexibilität, um Experimente zu starten und zu beenden.

Auch wenn sich die variable Natur der Cloud-Nutzung auf die Planbarkeit der Budgetierung und die Genauigkeit von Prognosen auswirken kann, bietet sie Organisationen jedoch auch die Möglichkeit, sowohl die Kosten für Überbereitstellungen als auch die Opportunitätskosten für konservative Unterbereitstellungen zu reduzieren.



Bauen Sie eine Partnerschaft zwischen wichtigen Beteiligten aus dem Finanzwesen und der Technologie auf, um ein gemeinsames Verständnis der organisatorischen Ziele zu schaffen und Mechanismen zu entwickeln, um im variablen Ausgabenmodell von Cloud Computing einen finanziellen Erfolg zu erzielen. Relevante Teams innerhalb Ihrer Organisation müssen an Kosten- und Nutzungsdiskussionen in allen Phasen Ihres Wegs in die Cloud beteiligt sein, einschließlich:

- Finanzverantwortliche: CFOs Finanzkontrolleure, Finanzplaner, Geschäftsanalysten, Beschaffungs- und Kreditorenbuchhaltung müssen das Cloud-Nutzungsmodell, die Kaufoptionen und den monatlichen Rechnungsstellungsprozess verstehen. Die Teams in den Bereichen Finanzen und Technologie müssen zusammenarbeiten, um die IT-Wertschöpfung zu entwickeln und

darzustellen, damit die geschäftlichen Teams die Verbindung zwischen Technologieausgaben und Geschäftsergebnissen verstehen können. Auf diese Weise werden Technologieaufwendungen nicht als Kosten angesehen, sondern als Investitionen. Aufgrund der grundlegenden Unterschiede zwischen der Cloud (z. B. Änderungsrate der Nutzung, nutzungsabhängige Preisberechnung, gestaffelte Preise, Preismodelle und detaillierte Abrechnungs- und Nutzungsinformationen) im Vergleich zum On-Premises-Betrieb ist es für die Finanzorganisation von entscheidender Bedeutung, dass sie versteht, wie sich die Nutzung der Cloud auf geschäftliche Aspekte wie Beschaffungsprozesse, Anreizverfolgung, Kostenzuordnung und Finanzberichte auswirken kann.

- Verantwortliche im Technologiebereich: Technologieverantwortliche (einschließlich Produkt- und Anwendungsbesitzer) müssen die finanziellen Anforderungen (z. B. Budgeteinschränkungen) sowie die geschäftlichen Anforderungen (z. B. Service Level Agreements) kennen. Damit kann die Workload implementiert werden, um die gewünschten Ziele der Organisation zu erreichen.

Die Partnerschaft zwischen Finanzen und Technologie bietet folgende Vorteile:

- Finanz- und Technologieteams haben nahezu in Echtzeit Einblicke in Kosten und Nutzung.
- Finanz- und Technologieteams legen ein standardmäßiges Betriebsverfahren für die Bewältigung von Ausgabeunterschieden in der Cloud fest.
- Finanzakteure agieren als strategische Berater, wenn es darum geht, wie Kapital für den Kauf von Abbonnementrabatten (z. B. Reserved Instances oder AWS Savings Plans) verwendet wird und wie die Cloud für das Wachstum des Unternehmens genutzt wird.
- Vorhandene Kreditorenbuchhaltungs- und Beschaffungsprozesse werden mit der Cloud verwendet.
- Finanz- und Technologieteams arbeiten zusammen, um future AWS Kosten und Nutzung zu prognostizieren, um die Unternehmensbudgets aufeinander abzustimmen und zu erstellen.
- Bessere organisationsübergreifende Kommunikation durch eine gemeinsame Sprache und ein gemeinsames Verständnis von Finanzkonzepten.

Weitere Beteiligte innerhalb Ihrer Organisation, die an Kosten- und Nutzungsdiskussionen beteiligt sein sollten, sind:

- Besitzer von Geschäftseinheiten: Besitzer von Geschäftseinheiten müssen sich mit dem Cloud-Geschäftsmodell vertraut machen, sodass sie den Geschäftseinheiten und dem gesamten Unternehmen die Richtung vorweisen können. Dieses Cloud-Wissen ist wichtig, wenn es erforderlich ist, das Wachstum und die Workload-Nutzung zu prognostizieren oder verschiedene Kaufoptionen zu bewerten, z. B. Reserved Instances oder Savings Plans.

- **Entwicklungsteam:** Der Aufbau einer Partnerschaft zwischen Finanz- und Technologieteams ist für den Aufbau einer kostenbewussten Kultur unerlässlich, die Ingenieure dazu ermutigt, Maßnahmen im Bereich Cloud-Finanzmanagement zu ergreifen (CFM). Eines der häufigsten Probleme unserer Finanzexperten CFM und Finanzteams besteht darin, Techniker dazu zu bringen, das gesamte Cloud-Geschäft zu verstehen, bewährte Verfahren zu befolgen und empfohlene Maßnahmen zu ergreifen.
- **Dritte:** Wenn Ihr Unternehmen Drittanbieter einsetzt (z. B. Berater oder Tools), stellen Sie sicher, dass diese auf Ihre finanziellen Ziele ausgerichtet sind und sowohl durch ihre Engagement-Modelle als auch durch eine Kapitalrendite nachweisen können (ROI). In der Regel beteiligen sich Dritte an der Berichterstattung und Analyse der von ihnen verwalteten Systeme, und sie stellen Kostenanalysen für die von ihnen konzipierten Workloads bereit.

Die Implementierung CFM und der Erfolg erfordern die Zusammenarbeit der Finanz-, Technologie- und Geschäftsteams sowie eine Änderung der Art und Weise, wie Cloud-Ausgaben im gesamten Unternehmen kommuniziert und bewertet werden. Beziehen Sie die Entwicklungsteams in alle Phasen der Diskussion über Kosten- und Nutzung ein und motivieren Sie sie zur Befolgung von bewährten Methoden und zur Umsetzung vereinbarter Aktionen.

### Implementierungsschritte

- **Definieren wichtiger Mitglieder:** Stellen Sie sicher, dass sich alle relevanten Mitglieder Ihrer Finanz- und Technologieteams aktiv an der Partnerschaft beteiligen. Relevante Mitglieder im Bereich Finanzen sind Personen, die mit Cloud-Ausgaben interagieren. Dabei handelt es sich um CFOs in der Regel um Finanzkontrolleure, Finanzplaner, Geschäftsanalysten, Beschaffung und Beschaffung. Technologiemitarbeiter sind in der Regel Produkt- und Anwendungsbesitzer, technische Manager und Vertreter aller Teams, die in der Cloud aktiv sind. Weitere Mitglieder können Geschäftsbereiche mit Einfluss auf die Nutzung von Produkten sein, zum Beispiel das Marketing, und Dritte wie Berater, die Sie bei der Ausrichtung an Ihren Zielen und Mechanismen und bei Berichten unterstützen.
- **Definieren von Besprechungsthemen:** Definieren Sie die Themen, die in den Teams häufig auftreten, oder ein gemeinsames Verständnis erfordern. Verfolgen Sie die Kosten ab dem Zeitpunkt, an dem sie generiert werden, bis zur Bezahlung der Rechnung. Beachten Sie alle beteiligten Mitglieder und organisatorischen Prozesse, die angewendet werden müssen. Informieren Sie sich über jeden einzelnen Schritt oder Prozess, den sie durchlaufen, sowie die zugehörigen Informationen, wie z. B. verfügbare Preismodelle, gestaffelte Preise, Rabattmodelle, Budgetplanung und finanzielle Anforderungen.

- Regelmäßigen Rhythmus etablieren: Um eine Finanz- und Technologiepartnerschaft zu schaffen, sollte ein regelmäßiger Kommunikationsrhythmus festgelegt werden, um eine Abstimmung zu erreichen und aufrechtzuerhalten. Die Gruppe muss regelmäßig im Hinblick auf ihre Ziele und Metriken zusammenkommen. Dazu gehört in der Regel die Überprüfung des Status der Organisation, der aktuell ausgeführten Programme und der gesamten Finanz- und Optimierungsmetriken. Anschließend werden detaillierte Berichte zu wichtigen Workloads erstellt.

## Ressourcen

### Zugehörige Dokumente:

- [AWS Nachrichten-Blog](#)

## COST01-BP03 Legen Sie Cloud-Budgets und Prognosen fest

Passen Sie die bestehenden Budgetierungs- und Prognoseprozesse der Organisation an die hochgradig variablen Kosten und die Nutzung der Cloud an. Prozesse müssen dynamisch sein und Algorithmen anwenden, die auf Trends oder Geschäftsfaktoren oder einer Kombination aus beiden basieren.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Hoch

## Implementierungsleitfaden

Bei herkömmlichen On-Premises-IT-Setups stehen Kunden oft vor der Herausforderung, Fixkosten zu planen, die sich nur gelegentlich ändern, typischerweise beim Kauf neuer IT-Geräte und -Services, um die Spitzennachfrage zu decken. AWS Cloud verwendet dagegen einen anderen Ansatz, bei dem Kunden für die Ressourcen zahlen, die sie nutzen, je nach ihren tatsächlichen IT- und Geschäftsanforderungen. In der Cloud-Umgebung kann die Nachfrage monatlich, täglich oder sogar stündlich schwanken.

Die Nutzung der Cloud bringt Effizienz, Geschwindigkeit und Agilität, damit allerdings auch ein stark variables Kosten- und Nutzungsmuster. Die Kosten können als Reaktion auf eine höhere Workload-Effizienz oder die Bereitstellung neuer Workloads und Features sinken oder manchmal eben auch steigen. Wenn Workloads skaliert werden, um einen wachsenden Kundenstamm zu bedienen, steigen parallel dazu die Cloud-Nutzung und -Kosten aufgrund der besseren Verfügbarkeit von Ressourcen. Diese Flexibilität bei Cloud-Services erstreckt sich auch auf die Kosten und Prognosen, was zu einer gewissen Elastizität führt.

Es ist wichtig, sich eng an diesen sich ändernden Geschäftsanforderungen und Nachfragetreibern auszurichten und eine möglichst genaue Planung anzustreben. Traditionelle Budgetprozesse in Organisationen müssen angepasst werden, um dieser Variabilität Rechnung zu tragen.

Ziehen Sie bei der Prognose der Kosten für neue Workloads eine Kostenmodellierung in Betracht. Durch die Kostenmodellierung erhalten Sie ein grundlegendes Verständnis der zu erwartenden Cloud-Kosten. Auf diese Weise können Sie Gesamtbetriebskosten (TCO), Kapitalrendite (ROI) und andere Finanzanalysen durchführen, gemeinsam mit den Beteiligten Ziele und Erwartungen festlegen und Möglichkeiten zur Kostenoptimierung identifizieren.

Ihre Organisation muss die Kostendefinitionen und akzeptierten Gruppierungen kennen. Der Detaillierungsgrad, mit dem Sie Prognosen erstellen, kann je nach Struktur und internen Workflows Ihrer Organisation variieren. Wählen Sie eine Granularität, die Ihren spezifischen Anforderungen und Ihrer Organisationsstruktur entspricht. Es ist wichtig zu verstehen, auf welcher Ebene die Prognose durchgeführt wird:

- **Verwaltungskonto oder AWS Organizations -Ebene:** Das Verwaltungskonto ist das Konto, das Sie zum Erstellen von AWS Organizations verwenden. Organisationen haben standardmäßig ein Verwaltungskonto.
- **Verlinktes Konto oder Mitgliedskonto:** Ein Konto in Organizations ist ein Standard AWS-Konto, das Ihre AWS Ressourcen und die Identitäten enthält, die auf diese Ressourcen zugreifen können.
- **Umgebung:** Eine Umgebung ist eine Sammlung von AWS Ressourcen, auf der eine Anwendungsversion ausgeführt wird. Eine Umgebung kann mit mehreren verknüpften Konten oder Mitgliedskonten erstellt werden.
- **Projekt:** Ein Projekt ist eine Kombination aus festgelegten Zielen oder Aufgaben, die innerhalb eines bestimmten Zeitraums zu erfüllen sind. Es ist wichtig, den Projektlebenszyklus bei Ihrer Prognose zu berücksichtigen.
- **AWS Dienste:** Gruppen oder Kategorien wie Rechen- oder Speicherdienste, in denen Sie AWS Dienste für Ihre Prognose gruppieren können.
- **Benutzerdefinierte Gruppierung:** Sie können benutzerdefinierte Gruppen erstellen, die auf den Anforderungen Ihrer Organisation basieren, z. B. Geschäftseinheiten, Kostenstellen, Teams, Kostenzuordnungs-Tags, Kostenkategorien, verknüpfte Konten oder eine Kombination davon.

Identifizieren Sie die Geschäftsfaktoren, die sich auf Ihre Nutzungskosten auswirken können, und erstellen Sie für jeden dieser Faktoren separate Prognosen, um die erwartete Nutzung im Voraus zu berechnen. Einige der Faktoren fallen in den Verantwortungsbereich von IT- und



Produktteams innerhalb der Organisation. Andere Geschäftsfaktoren, wie Marketingveranstaltungen, Werbeaktionen, geografische Expansionen, Fusionen und Übernahmen, sind den Führungskräften in Vertrieb und Marketing und der Geschäftsleitung bekannt. Es ist wichtig, zusammenzuarbeiten und auch all diese Nachfragetreiber zu berücksichtigen.

Sie können es [AWS Cost Explorer](#) für trendbasierte Prognosen in einem definierten future Zeitraum verwenden, der auf Ihren vergangenen Ausgaben basiert. AWS Cost Explorer Die Prognose-Engine segmentiert Ihre historischen Daten auf der Grundlage von Gebührenarten (z. B. Reserved Instances) und verwendet eine Kombination aus maschinellem Lernen und regelbasierten Modellen, um Ausgaben für alle Gebührenarten individuell vorherzusagen.

Sobald Sie Ihren Prognoseprozess festgelegt und Modelle erstellt haben, können [AWS Budgets](#) Sie individuelle Budgets auf detaillierter Ebene festlegen, indem Sie den Zeitraum, die Häufigkeit oder den Betrag (fest oder variabel) angeben und Filter wie Service und Tags hinzufügen. AWS-Region Das Budget wird in der Regel für ein Jahr geplant und bleibt unverändert, sodass alle Stakeholder sich strikt daran halten müssen. Im Gegensatz dazu sind Prognosen flexibler, da sie erneute Anpassungen im Laufe des Jahres ermöglichen und dynamische Prognosen über einen Zeitraum von einem, zwei oder drei Jahren liefern. Sowohl die Budgetierung als auch Prognosen spielen eine entscheidende Rolle bei der Definition der Finanzerwartungen verschiedener Stakeholder aus dem technischen und geschäftlichen Bereich. Genaue Prognosen und deren Umsetzung sorgen zudem dafür, dass die Stakeholder, die direkt für die Bereitstellungskosten verantwortlich sind, zur Rechenschaft gezogen werden. Außerdem wird auf diese Weise das allgemeine Kostenbewusstsein gestärkt.

Um über die Leistung Ihrer bestehenden Budgets auf dem Laufenden zu bleiben, können Sie AWS Budgets -Berichte erstellen und planen, die Sie und Ihre Stakeholder in regelmäßigen Abständen per E-Mail erhalten. Sie können auch AWS Budgets -Warnmeldungen basierend auf tatsächlichen Kosten erstellen, also einen reaktiven Prozess. Budgetwarnungen zu prognostizierten Kosten geben Ihnen Zeit, Abhilfemaßnahmen gegen potenzielle Kostenüberschreitungen zu implementieren. Sie können sich benachrichtigen lassen, wenn Ihre Kosten oder Ihre Nutzung ein bestimmtes Niveau übersteigen oder in der Zukunft den budgetierten Betrag möglicherweise überschreiten werden.

Gestalten Sie vorhandene Budget- und Prognoseprozesse dynamischer. Hierzu können Sie trendbasierte Algorithmen (mit historischen Kosten als Eingabe) und auf Geschäftsfaktoren basierende Algorithmen verwenden (z. B. auf der Einführung neuer Produkte, auf einer regionalen Expansion oder neuen Umgebungen für Workloads), die besonders für Umgebungen mit dynamischen und variablen Ausgaben geeignet sind. Nachdem Sie Ihre trendbasierte Prognose mit dem Cost Explorer oder anderen Tools ermittelt haben, können Sie anhand des [AWS Pricing](#)

[Calculator](#) Ihren AWS Anwendungsfall und die future Kosten auf der Grundlage der erwarteten Nutzung (Traffic oder erforderliche EC2 Amazon-Instances) abschätzen. requests-per-second

Überprüfen Sie die Genauigkeit dieser Prognose, da Budgets auf Grundlage dieser Prognoseberechnungen und -schätzungen festgelegt werden sollten. Überwachen Sie die Genauigkeit und Effektivität der integrierten Cloud-Kostenprognosen. Überprüfen Sie regelmäßig die tatsächlichen Ausgaben im Vergleich zur Prognose und passen Sie sie bei Bedarf an, um die Prognosepräzision zu verbessern. Verfolgen Sie die Prognoseabweichung und führen Sie eine Ursachenanalyse der berichteten Abweichungen durch, um zu reagieren und die Prognosen anzupassen.

Wie in [COST01-BP02 Etablieren Sie eine Partnerschaft zwischen Finanzen und Technologie](#) erwähnt, ist es wichtig, eine Partnerschaft mit regelmäßigen Konsultationen zwischen IT, Finanzabteilung und anderen Stakeholdern zu schaffen, um zu bestätigen, dass alle in konsistenter Weise die gleichen Tools oder Prozesse anwenden. Wenn Budgets geändert werden müssen, führen Sie häufigere Besprechungen durch, um schneller darauf zu reagieren.

#### Implementierungsschritte

- Definieren Sie die Kostensprache innerhalb der Organisation: Erstellen Sie eine gemeinsame AWS Kostensprache innerhalb der Organisation mit mehreren Dimensionen und Gruppierungen. Stellen Sie sicher, dass die Stakeholder die Granularität der Prognosen, die Preismodelle und das Niveau Ihrer Kostenprognosen verstehen.
- Analysieren Sie trendbasierte Prognosen: Verwenden Sie trendbasierte Prognosetools wie AWS Cost Explorer und Amazon Forecast. Analysieren Sie Ihre Nutzungskosten anhand verschiedener Dimensionen wie Service, Konto, Tags und Kostenkategorien. Wenn erweiterte Prognosen erforderlich sind, importieren Sie Ihre AWS Kosten- und Nutzungsdaten (CUR) in Amazon Forecast (das lineare Regression als eine Form des maschinellen Lernens auf Prognosen anwendet).
- Analysieren Sie faktorbasierte Prognosen: Identifizieren Sie die Auswirkungen geschäftlicher Faktoren auf Ihre Cloud-Nutzung und erstellen Sie für jeden Faktor eine separate Prognose, um die erwarteten Nutzungskosten im Voraus zu berechnen. Arbeiten Sie eng mit Verantwortlichen von Geschäftseinheiten und Stakeholdern zusammen, um die Auswirkungen auf neue Faktoren zu verstehen und die erwarteten Kostenänderungen zu berechnen. So können Sie genaue Budgets definieren.
- Aktualisieren Sie die bestehenden Prognose- und Budgetprozesse: Definieren Sie Ihre Prozesse für die Prognose und Budgetierung auf Grundlage von bewährten Prognosemethoden, z. B. trendbasiert, geschäftsfaktorenbasiert oder einer Kombination aus beiden Ansätzen. Budgets sollten kalkuliert werden, realistisch sein und auf Ihren Prognosen basieren.

- Warnmeldungen und Benachrichtigungen konfigurieren: Verwenden Sie AWS Budgets Warnmeldungen und die Erkennung von Kostenanomalien, um Warnmeldungen und Benachrichtigungen zu erhalten.
- Führen Sie regelmäßige Prüfungen zusammen mit wichtigen Stakeholdern durch: Einigen Sie sich mit Stakeholdern in den Bereichen IT, Finanzen, Plattform usw. auf Änderungen der Unternehmensausrichtung und der Nutzung.

## Ressourcen

### Zugehörige Dokumente:

- [AWS Cost Explorer](#)
- [AWS Cost and Usage Report](#)
- [Prognosen mit Cost Explorer](#)
- [QuickSight Amazon-Prognosen](#)
- [Amazon Forecast](#)
- [AWS Budgets](#)

### Zugehörige Videos:

- [Wie kann ich AWS Budgets damit meine Ausgaben und Nutzung verfolgen](#)
- [AWS Serie zur Kostenoptimierung: AWS Budgets](#)

### Zugehörige Beispiele:

- [Faktorbasierte Prognosen verstehen und erstellen](#)
- [Eine Prognosekultur schaffen und fördern](#)
- [Prognosen für Cloud-Kosten optimieren](#)
- [Die richtigen Tools für Cloud-Kostenprognosen verwenden](#)

COST01-BP04 Implementieren Sie Kostenbewusstsein in Ihren organisatorischen Prozessen

Implementieren Sie Kostenbewusstsein und sorgen Sie für Transparenz und Verantwortlichkeit bei neuen oder bestehenden Prozessen, die sich auf die Nutzung auswirken, und greifen Sie

auf vorhandene Prozesse zur Steigerung des Kostenbewusstseins zurück. Implementieren Sie Kostenbewusstsein in die Mitarbeiterschulung.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Hoch

### Implementierungsleitfaden

Das Kostenbewusstsein muss in neuen und vorhandenen Organisationsprozessen implementiert werden. Dies ist eine der absoluten Grundlagen für weitere bewährte Methoden. Es wird empfohlen, vorhandene Prozesse nach Möglichkeit wiederzuverwenden und zu ändern. Dadurch werden die Auswirkungen auf Agilität und Geschwindigkeit minimiert. Melden Sie die Cloud-Kosten den Technologieteams und den Entscheidungsträgern in den Geschäfts- und Finanzteams, um das Kostenbewusstsein zu schärfen und wichtige Leistungsindikatoren (KPIs) für die Effizienz von Stakeholdern aus dem Finanz- und Geschäftsbereich festzulegen. Die folgenden Empfehlungen helfen Ihnen bei der Implementierung der Kostenerkennung in Ihrer Workload:

- Stellen Sie sicher, dass das Änderungsmanagement eine Kostenmessung umfasst, um die finanziellen Auswirkungen Ihrer Änderungen zu quantifizieren. Auf diese Weise können Sie kostenbezogene Probleme proaktiv lösen und Kosteneinsparungen hervorheben.
- Stellen Sie sicher, dass die Kostenoptimierung eine zentrale Komponente Ihrer Betriebsfunktionen ist. Sie können beispielsweise vorhandene Vorfalldmanagementprozesse nutzen, um die Ursache für Kosten- und Nutzungsanomalien (Kostenüberschreitungen) zu ermitteln und zu identifizieren.
- Beschleunigen Sie die Kosteneinsparungen und die Wertschöpfung des Unternehmens durch Automatisierung oder Tools. Wenn Sie über die Kosten der Implementierung nachdenken, sollten Sie das Gespräch so gestalten, dass eine Komponente der Kapitalrendite (ROI) berücksichtigt wird, um die Investition von Zeit oder Geld zu rechtfertigen.
- Weisen Sie Cloud-Kosten zu, indem Sie Showbacks oder Chargebacks für Cloud-Aufwendungen implementieren, einschließlich Aufwendungen für verpflichtungsbasierte Kaufoptionen, gemeinsam genutzte Services und Markteinkäufe, um die Cloudnutzung in möglichst kostenbewusster Weise zu gestalten.
- Erweitern Sie vorhandene Schulungs- und Entwicklungsprogramme, um Schulungen zum Kostenbewusstsein in Ihrer gesamten Organisation einzubeziehen. Es wird empfohlen, dass dies fortlaufende Schulungen und Zertifizierungen umfasst. Dadurch entsteht eine Organisation, die Kosten und Nutzung selbst verwalten kann.
- Nutzen Sie kostenlose AWS native Tools wie [AWS Cost Anomaly Detection](#), [AWS Budgets](#), und [AWS Budgets Reports](#).

Wenn Unternehmen konsequent [Cloud Financial Management](#) (CFM) -Praktiken anwenden, werden diese Verhaltensweisen in der Arbeitsweise und Entscheidungsfindung tief verwurzelt. Das Ergebnis ist eine kostenbewusstere Unternehmenskultur, angefangen von Entwicklern, die eine neue born-in-the-cloud Anwendung entwerfen, bis hin zu Finanzmanagern, die diese neuen Cloud-Investitionen ROI analysieren.

### Implementierungsschritte

- Bestimmen relevanter organisatorischer Prozesse: Jede Organisationseinheit überprüft ihre Prozesse und identifiziert Prozesse, die sich auf Kosten und Nutzung auswirken. Alle Prozesse, die zur Erstellung oder Beendigung einer Ressource führen, müssen zur Überprüfung einbezogen werden. Suchen Sie auch nach Prozessen, die das Kostenbewusstsein in Ihrem Unternehmen unterstützen können, wie z. B. Vorfallmanagement und Schulungen.
- Etablieren Sie eine sich selbst tragende, kostenbewusste Kultur: Stellen Sie sicher, dass sich alle relevanten Stakeholder an den Kosten orientieren cause-of-change und diese beeinflussen, damit sie die Cloud-Kosten verstehen. So kann Ihre Organisation eine sich selbst erhaltende, kostenbewusste Innovationskultur entwickeln.
- Aktualisieren von Prozessen mit Kostenbewusstsein: Jeder Prozess wird so geändert, dass er kostenbewusst wird. Der Prozess erfordert möglicherweise zusätzliche Vorabprüfungen, z. B. das Bewerten der Auswirkungen von Kosten oder nachträgliche Prüfungen, die bestätigen, dass die erwarteten Kosten- und Nutzungsänderungen stattgefunden haben. Unterstützungsprozesse wie Schulungs- und Vorfallmanagement können auf Kosten- und Nutzungselemente erweitert werden.

Wenn Sie Hilfe benötigen, wenden Sie sich über Ihr Account-Team an CFM Experten oder schauen Sie sich die unten stehenden Ressourcen und zugehörigen Dokumente an.

### Ressourcen

#### Zugehörige Dokumente:

- [AWS Cloud-Finanzmanagement](#)

#### Zugehörige Beispiele:

- [Strategie für effizientes Cloud-Kostenmanagement](#)
- [Blog-Serie zum Thema Kostenkontrolle Nr. 3: Umgang mit Kostenschocks](#)
- [Ein Leitfaden für Anfänger AWS Cost Management](#)

## COST01-BP05 Bericht und Benachrichtigung zur Kostenoptimierung

Richten Sie Cloud-Budgets ein und konfigurieren Sie Mechanismen zur Erkennung von Anomalien bei der Nutzung. Konfigurieren Sie zugehörige Tools für Kosten- und Nutzungswarnungen für vordefinierte Ziele und lassen Sie sich benachrichtigen, wenn eine Nutzung diese Ziele überschreitet. Halten Sie regelmäßig Meetings ab, um die Kosteneffektivität Ihrer Workloads zu analysieren und das Kostenbewusstsein zu stärken.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Niedrig

### Implementierungsleitfaden

Sie müssen regelmäßig Kosten- und Nutzungsoptimierungen in Ihrer Organisation melden. Sie können dedizierte Sitzungen implementieren, um die Kosteneffizienz zu besprechen, oder die Kostenoptimierung in Ihre regulären operativen Berichtszyklen für Ihre Workloads einschließen. Nutzen Sie Services und Tools, um die Kosteneffizienz regelmäßig zu überwachen und Möglichkeiten zur Kosteneinsparung zu nutzen.

Zeigen Sie Ihre Kosten und Nutzung mit mehreren Filtern und Granularität an, indem Sie [AWS Cost Explorer](#) verwenden, das Dashboards und Berichte wie Kosten pro Service oder Konto, Tageskosten oder Marktplatzkosten bereitstellt. Sie können Ihren Fortschritt bei Kosten und Nutzung mit [AWS Budgets -Berichten](#) anhand konfigurierter Budgets verfolgen.

Verwenden Sie diese Option [AWS Budgets](#), um benutzerdefinierte Budgets festzulegen, um Ihre Kosten und Nutzung zu verfolgen und schnell auf Benachrichtigungen per E-Mail oder Amazon Simple Notification Service (AmazonSNS) zu reagieren, wenn Sie Ihren Schwellenwert überschreiten. [Legen Sie Ihren bevorzugten Budgetzeitraum](#) auf täglich, monatlich, vierteljährlich oder jährlich fest und legen Sie spezifische Budgetlimits fest, damit Sie stets darüber informiert sind, wie sich die tatsächlichen oder prognostizierten Kosten und die Nutzung in Richtung Ihres Budgetschwellenwerts entwickeln. Sie können auch eine automatische Ausführung von [Warnungen](#) und [Aktionen](#) oder einen Genehmigungsprozess für den Fall einrichten, dass ein Budgetziel überschritten wird.

Implementieren Sie Benachrichtigungen zu Kosten und Nutzung, um sicherzustellen, dass bei unerwarteten Kosten- und Nutzungsänderungen schnell reagiert werden kann. [AWS Cost Anomaly Detection](#) ermöglicht es Ihnen, Kostenüberraschungen zu vermeiden und die Kontrolle zu verbessern, ohne die Innovation zu bremsen. AWS Cost Anomaly Detection identifiziert ungewöhnliche Ausgaben und deren Ursachen und trägt so dazu bei, das Risiko überraschender Rechnungsstellung zu verringern. In drei einfachen Schritten können Sie Ihre eigene kontextorientierte Überwachung einrichten und Benachrichtigungen erhalten, wenn anomale Ausgaben entdeckt werden.

Sie können [Amazon](#) auch QuickSight mit AWS Cost and Usage Report (CUR) -Daten verwenden, um hochgradig maßgeschneiderte Berichte mit detaillierteren Daten bereitzustellen. Amazon QuickSight ermöglicht es Ihnen, Berichte zu planen und regelmäßig E-Mails mit Kostenberichten zu erhalten, um historische Kosten und Nutzung oder Möglichkeiten zur Kosteneinsparung zu ermitteln. Schauen Sie sich unsere auf Amazon entwickelte Lösung [Cost Intelligence Dashboard](#) (CID) an QuickSight, die Ihnen erweiterte Transparenz bietet.

Verwenden Sie diese Option [AWS Trusted Advisor](#), mit der Sie überprüfen können, ob die bereitgestellten Ressourcen den AWS bewährten Methoden zur Kostenoptimierung entsprechen.

Vergleichen Sie Ihre Savings Plans-Empfehlungen anhand detaillierter grafischer Darstellungen zu Ihren Kosten und der Nutzung. Nach Stunden unterteilte Grafiken zeigen die On-Demand-Ausgaben zusammen mit den empfohlenen Savings Plans-Verpflichtungen und geben Aufschluss über die geschätzten Einsparungen, die Savings Plans-Abdeckung und Savings Plans-Nutzung. Auf diese Weise können Organisationen nachvollziehen, wie ihre Savings Plans auf jede aufgewendete Stunde angewendet werden, ohne Zeit und Ressourcen in die Erstellung von Modellen zur Analyse ihrer Ausgaben investieren zu müssen.

Erstellen Sie regelmäßig Berichte mit einer Übersicht über Savings Plans, Reserved Instances und Empfehlungen zur EC2 Anpassung von Amazon, um damit AWS Cost Explorer zu beginnen, die Kosten im Zusammenhang mit stationären Workloads, ungenutzten und nicht ausgelasteten Ressourcen zu senken. Identifizieren Sie unnötige Cloud-Ausgaben, die mit bereitgestellten Ressourcen verbunden sind, und gewinnen Sie diese zurück. Unnötige Cloud-Ausgaben entstehen, wenn Ressourcen mit der falschen Größe erstellt werden oder wenn andere als die erwarteten Nutzungsmuster beobachtet werden. Halten Sie sich an AWS bewährte Methoden, um Verschwendung zu reduzieren, oder bitten Sie Ihr Account-Team und Ihren Partner, Ihnen bei der [Optimierung](#) und Einsparung Ihrer Cloud-Kosten zu helfen.

Generieren Sie regelmäßig Berichte zu besseren Kaufoptionen für Ihre Ressourcen, um die Kosten pro Einheit für Ihre Workloads zu senken. Kaufoptionen wie Savings Plans, Reserved Instances oder Amazon EC2 Spot Instances bieten die größten Kosteneinsparungen bei fehlertoleranten Workloads und ermöglichen es allen Beteiligten (Geschäftsinhaber, Finanz- und Technikteams), an diesen Verpflichtungsgesprächen teilzunehmen.

Teilen Sie uns die Berichte mit Möglichkeiten oder Ankündigungen neuer Versionen mit, die Ihnen dabei helfen können, die Gesamtbetriebskosten (TCO) der Cloud zu senken. Führen Sie neue Services, Regionen, Funktionen, Lösungen oder neue Möglichkeiten für weitere Kostenreduzierungen ein.

## Implementierungsschritte

- Konfigurieren AWS Budgets: Konfigurieren Sie AWS Budgets auf allen Konten für Ihren Workload. Legen Sie ein Budget für die Gesamtkontoausgaben und ein Budget für die Workload mithilfe von Tags fest.
  - [Well-Architected Labs: Kosten und Steuerung der Nutzung](#)
- Bericht zur Kostenoptimierung: Richten Sie einen regelmäßigen Zyklus ein, um die Effizienz der Workload zu erörtern und zu analysieren. Melden Sie anhand der eingerichteten Metriken die erreichten Metriken und die Kosten für deren Erreichung. Identifizieren und beheben Sie negative Trends und suchen Sie nach positiven Trends, die Sie in der gesamten Organisation fördern können. Bei der Berichterstellung sollten Vertreter der Anwendungsteams und -Verantwortlichen, Finanzverantwortliche und wichtige Entscheidungsträger in Bezug auf Cloud-Ausgaben einbezogen werden.

## Ressourcen

### Zugehörige Dokumente:

- [AWS Cost Explorer](#)
- [AWS Trusted Advisor](#)
- [AWS Budgets](#)
- [AWS Cost and Usage Report](#)
- [AWS Budgets Bewährte Methoden](#)
- [Amazon-S3-Analytik](#)

### Zugehörige Beispiele:

- [Well-Architected Labs: Kosten und Steuerung der Nutzung](#)
- [Wichtige Möglichkeiten, um mit der Optimierung Ihrer AWS Cloud-Kosten zu beginnen](#)

## COST01-BP06 Kosten proaktiv überwachen

Implementieren Sie Tools und Dashboards, um die Kosten für die Workload proaktiv zu überwachen. Überprüfen Sie regelmäßig die Kosten mithilfe konfigurierter oder vorab erstellter Tools. Untersuchen Sie Kosten und Kategorien nicht erst, wenn Sie Benachrichtigungen erhalten. Die proaktive



Überwachung und Analyse der Kosten hilft Ihnen, positive Trends zu identifizieren und diese in der gesamten Organisation zu unterstützen.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Mittel

### Implementierungsleitfaden

Es wird empfohlen, die Kosten und die Nutzung innerhalb Ihrer Organisation proaktiv zu überwachen, nicht nur, wenn Ausnahmen oder Anomalien vorliegen. Hoch sichtbare Dashboards in Ihrem Büro oder Ihrer Arbeitsumgebung stellen sicher, dass relevante Mitarbeiter Zugriff auf benötigte Informationen haben, und signalisieren den Fokus der Organisation auf Kostenoptimierungen. Mit gut sichtbaren Dashboards können Sie den Erfolg aktiv unterstützen und positive Ergebnisse in der gesamten Organisation implementieren.

Erstellen Sie eine tägliche oder häufige Routine, die Sie verwenden können, [AWS Cost Explorer](#) oder ein anderes Dashboard wie [Amazon QuickSight](#), um die Kosten zu sehen und proaktiv zu analysieren. Analysieren Sie die AWS Servicenutzung und die Kosten auf AWS Kontoebene, Workload-Ebene oder auf einer bestimmten AWS Serviceebene durch Gruppierung und Filterung und überprüfen Sie, ob sie erwartet werden oder nicht. Nutzen Sie die Granularität und die Tags auf Stunden- und Ressourcenbasis, um für die wichtigsten Ressourcen wiederkehrende Kosten herauszufiltern und zu identifizieren. Mit dem [Cost Intelligence Dashboard](#), einer [QuickSightAmazon-Lösung](#) von AWS Solutions Architects, können Sie auch Ihre eigenen Berichte erstellen und Ihre Budgets mit den tatsächlichen Kosten und der tatsächlichen Nutzung vergleichen.

### Implementierungsschritte

- Bericht zur Kostenoptimierung: Richten Sie einen regelmäßigen Zyklus ein, um die Effizienz der Workload zu erörtern und zu analysieren. Melden Sie anhand der eingerichteten Metriken die erreichten Metriken und die Kosten für deren Erreichung. Identifizieren und beheben Sie negative Trends und suchen Sie nach positiven Trends, um diese in der gesamten Organisation zu unterstützen. Bei der Berichterstellung sollten Vertreter der Anwendungsteams und Besitzer, Finanz- und Geschäftsleitung einbezogen werden.
- Erstellen und aktivieren Sie die tägliche Granularität [AWS Budgets](#) für Kosten und Nutzung, um rechtzeitig Maßnahmen zur Vermeidung potenzieller Kostenüberschreitungen zu ergreifen: Sie AWS Budgets können Warnmeldungen konfigurieren, sodass Sie immer auf dem Laufenden bleiben, wenn einer Ihrer Budgettypen Ihre vorkonfigurierten Schwellenwerte überschreitet. Die beste Möglichkeit, dies zu nutzen, AWS Budgets besteht darin, Ihre zu erwartenden Kosten und Nutzung als Obergrenzen festzulegen, sodass alles, was über Ihrem Budget liegt, als zu viel ausgegeben angesehen werden kann.

- Create AWS Cost Anomaly Detection for Cost Monitor: [AWS Cost Anomaly Detection](#) nutzt fortschrittliche Machine-Learning-Technologie, um ungewöhnliche Ausgaben und deren Ursachen zu identifizieren, sodass Sie schnell Maßnahmen ergreifen können. Sie können auf diese Weise Tools für die Überwachung der Kosten von Ausgabensegmenten konfigurieren, die Sie überwachen möchten (z. B. einzelne AWS -Services, Mitgliederkonten, Kostenzuweisungs-Tags und Kostenkategorien). Sie können auch festlegen, wann, wo und wie Sie Warnungen erhalten. Jedem Überwachungstool können Sie mehrere Warnungsabonnements für Geschäftsbereichsleiter und Technologieteams anfügen, einschließlich Name, Kostenschwellenwert und Häufigkeit (einzelne Warnungen, tägliche Zusammenfassung, wöchentliche Zusammenfassung) für die einzelnen Abonnements.
- Verwenden AWS Cost Explorer oder integrieren Sie Ihre AWS Cost and Usage Report (CUR) - Daten in QuickSight Amazon-Dashboards, um die Kosten Ihres Unternehmens zu visualisieren: AWS Cost Explorer verfügt über eine easy-to-use Oberfläche, mit der Sie Ihre AWS Kosten und Nutzung im Laufe der Zeit visualisieren, verstehen und verwalten können. Das [Cost Intelligence Dashboard](#) ist ein anpassbares und zugängliches Dashboard, mit dem Sie die Grundlagen für Ihr eigenes Tool für Kostenmanagement und Optimierung legen können.

## Ressourcen

### Zugehörige Dokumente:

- [AWS Budgets](#)
- [AWS Cost Explorer](#)
- [Tägliche Kosten und Nutzungsbudgets](#)
- [AWS Cost Anomaly Detection](#)

### Zugehörige Beispiele:

- [Well-Architected Labs: Visualisierung](#)
- [Well-Architected Labs: Erweiterte Visualisierung](#)
- [Well-Architected Labs: Cloud Intelligence Dashboards](#)
- [Well-Architected Labs: Kostenvisualisierung](#)
- [AWS Cost Anomaly Detection Alarmieren Sie mit Slack](#)

## COST01-BP07 Bleiben Sie auf up-to-date dem Laufenden mit neuen Service Releases

Konsultieren Sie regelmäßig Experten oder AWS Partner, um herauszufinden, welche Dienste und Funktionen kostengünstiger sind. Lesen Sie AWS Blogs und andere Informationsquellen.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Mittel

### Implementierungsleitfaden

AWS fügt ständig neue Funktionen hinzu, sodass Sie die neuesten Technologien nutzen können, um schneller zu experimentieren und Innovationen zu entwickeln. Möglicherweise können Sie neue AWS Dienste und Funktionen implementieren, um die Kosteneffizienz Ihrer Workloads zu erhöhen. Lesen Sie regelmäßig [AWS Cost Management](#), den [AWS News Blog](#), den [AWS Cost Management-Blog](#) und [Neuerungen bei AWS](#), um Informationen zur Veröffentlichung neuer Services und Features zu erhalten. Neue Beiträge bieten einen kurzen Überblick über alle Ankündigungen zu AWS Diensten, Funktionen und Regionserweiterungen, sobald sie veröffentlicht werden.

### Implementierungsschritte

- Blogs abonnieren: Gehen Sie zu den AWS Blogseiten und abonnieren Sie den What's New Blog und andere relevante Blogs. Sie können sich auf der Seite für die [Kommunikationseinstellungen](#) mit Ihrer E-Mail-Adresse registrieren.
- AWS Neuigkeiten abonnieren: Informieren Sie sich regelmäßig im [AWS News-Blog](#) und unter [Neuigkeiten über AWS neue](#) Service- und Feature-Releases. Abonnieren Sie den RSS Feed oder mit Ihrer E-Mail-Adresse, um Ankündigungen und Veröffentlichungen zu verfolgen.
- AWS Preissenkungen folgen: Regelmäßige Preissenkungen bei all unseren Dienstleistungen waren eine Standardmethode, AWS um die wirtschaftliche Effizienz, die sich aus unserer Skalierung ergeben, an unsere Kunden weiterzugeben. Stand 20. September 2023, AWS hat die Preise seit 2006 134 Mal gesenkt. Wenn geschäftliche Entscheidungen aufgrund von Preisbedenken ausstehen, können Sie die Preise nach der Reduzierung und der Integration neuer Services erneut prüfen. In der [Kategorie Preissenkungen im AWS News-Blog](#) können Sie sich über die bisherigen Preissenkungsmaßnahmen, einschließlich Amazon Elastic Compute Cloud (AmazonEC2) -Instances, informieren.
- AWS Veranstaltungen und Treffen: Nehmen Sie an Ihrem lokalen AWS Gipfel und allen lokalen Treffen mit anderen Organisationen aus Ihrer Region teil. Wenn Sie nicht persönlich teilnehmen können, versuchen Sie, virtuelle Veranstaltungen zu besuchen, um mehr von AWS Experten und Geschäftsszenarien anderer Kunden zu erfahren.

- Treffen Sie sich mit Ihrem Account-Team: Planen Sie regelmäßige Treffen mit Ihrem Account-Team, um über Branchentrends und AWS -Services zu sprechen. Sprechen Sie mit Ihrem Account Manager, Solutions Architekt und Support-Team.

## Ressourcen

### Zugehörige Dokumente:

- [AWS Kostenmanagement](#)
- [Was ist neu bei AWS](#)
- [AWS Nachrichten-Blog](#)

### Zugehörige Beispiele:

- [Amazon EC2 — 15 Jahre Optimierung und Einsparung Ihrer IT-Kosten](#)
- [AWS News-Blog — Preissenkung](#)

## COST01-BP08 Schaffen Sie eine kostenbewusste Kultur

Implementieren Sie Änderungen oder Programme in Ihrer gesamten Organisation, um eine kostenbewusste Kultur zu schaffen. Es wird empfohlen, klein zu beginnen. Wenn Ihre Kompetenz und die Nutzung der Cloud in Ihrer Organisation zunehmen, implementieren Sie große und umfangreiche Programme.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Niedrig

### Implementierungsleitfaden

Eine kostenbewusste Kultur ermöglicht Ihnen die Skalierung von Kostenoptimierung und Cloud-Finanzmanagement (betriebliche Abläufe, Cloud-Kompetenzzentrum, Cloud-Betriebsteams usw.) mithilfe von bewährten Methoden, die in der gesamten Organisation auf organische und dezentralisierte Weise angewendet werden. Wenn Sie ein Kostenbewusstsein entwickeln, können Sie im Vergleich zu einem zentralisierten Top-Down-Approach in der gesamten Organisation mit minimalem Aufwand einen hohen Grad an Kompetenz erzielen.

Die Entwicklung eines Kostenbewusstseins im Bereich Cloud Computing, insbesondere bei primären Kostenfaktoren, ermöglicht Teams, die voraussichtlichen Ergebnisse von Änderungen aus Kostensicht zu verstehen. Teams, die auf Cloud-Umgebungen zugreifen, sollten die Preismodelle

kennen und den Unterschied zwischen herkömmlichen On-Premises-Rechenzentren und Cloud Computing verstehen.

Der Hauptvorteil einer Kultur des Kostenbewusstseins besteht darin, dass Technologieteams die Kosten proaktiv und kontinuierlich optimieren, statt bedarfsbasiert reaktive Kostenoptimierungen durchzuführen. (Die Kosten werden beispielsweise als eine nicht funktionale Anforderung betrachtet, wenn neue Workloads entwickelt oder vorhandene Workloads geändert werden.)

Kleine Veränderungen in der Kultur können große Auswirkungen auf die Effizienz Ihrer aktuellen und zukünftigen Workloads haben. Beispiele hierfür sind:

- Transparenz und Schaffung eines Bewusstseins bei Entwicklungsteams, damit diese verstehen, was sie tun und wie sich dies auf die Kosten auswirkt.
- Gamifizierung von Kosten und Nutzung in Ihrer gesamten Organisation. Dies kann über ein öffentlich sichtbares Dashboard oder einen Bericht geschehen, in dem die normalisierten Kosten und die Nutzung zwischen den Teams verglichen werden (z. B. und). cost-per-workload cost-per-transaction
- Kosteneffizienz erkennen. Belohnen Sie freiwillige oder unaufgeforderte Kostenoptimierungsleistungen öffentlich oder privat und lernen Sie aus Fehlern, um eine Wiederholung in Zukunft zu vermeiden.
- Erstellen Sie Top-Down-Organisationsanforderungen für die Ausführung von Workloads mit vordefinierten Budgets.
- Hinterfragen Sie die geschäftlichen Anforderungen in Bezug auf Änderungen und die Kostenauswirkungen von Änderungsanforderungen für die Architekturinfrastruktur oder die Workload-Konfiguration, um sicherzustellen, dass Sie nur für das bezahlen, was Sie benötigen.
- Stellen Sie sicher, dass sich Änderungsplaner voraussichtlicher Änderungen mit Auswirkungen auf die Kosten bewusst sind und dass diese Änderungen von den Stakeholdern genehmigt werden, um geschäftliche Ergebnisse auf kosteneffektive Weise zu erzielen.

### Implementierungsschritte

- Melden Sie Cloud-Kosten an Technologieteams, um das Kostenbewusstsein zu schärfen und die Effizienz der Beteiligten im Finanz KPIs - und Geschäftsbereich zu steigern.
- Informieren Sie Stakeholder oder Teammitglieder über geplante Änderungen: Erstellen Sie einen Tagesordnungspunkt zur Erörterung geplanter Änderungen und der Kosten-Nutzen-Auswirkungen auf die Arbeitsbelastung während der wöchentlichen Änderungsbesprechungen.

- Treffen Sie sich mit Ihrem Account-Team: Richten Sie regelmäßige Treffen mit Ihrem Account-Team ein, um über Branchentrends und AWS -Services zu sprechen. Sprechen Sie mit Ihrem Account Manager, Solutions Architect und Support-Team.
- Teilen Sie Erfolgsgeschichten: Teilen Sie Erfolgsgeschichten zur Kostensenkung für jede Arbeitslast oder Organisation AWS-Konto, um eine positive Einstellung und Ermutigung zur Kostenoptimierung zu schaffen.
- Schulung: Stellen Sie sicher, dass technische Teams oder Teammitglieder geschult werden, damit sie sich der Ressourcenkosten bewusst werden. AWS Cloud
- AWS Veranstaltungen und Treffen: Nehmen Sie an lokalen AWS Gipfeltreffen und allen lokalen Treffen mit anderen Organisationen aus Ihrer Region teil.
- Blogs abonnieren: Gehe zu den AWS Blogseiten und abonniere den [What's New Blog und andere relevante Blogs, um neue](#) Veröffentlichungen, Implementierungen, Beispiele und Änderungen zu verfolgen, die von geteilt wurden. AWS

## Ressourcen

### Zugehörige Dokumente:

- [AWS Blog](#)
- [AWS Kostenmanagement](#)
- [AWS Nachrichten-Blog](#)

### Zugehörige Beispiele:

- [AWS Cloud-Finanzmanagement](#)
- [AWS Well-Architected Labs: Cloud-Finanzmanagement](#)

## COST01-BP09 Quantifizieren Sie den Geschäftswert der Kostenoptimierung

Durch die Quantifizierung des Geschäftswerts von Kostenoptimierungen können Sie die gesamten Vorteile für Ihre Organisation verstehen. Da die Kostenoptimierung eine notwendige Investition ist, können Sie durch die Quantifizierung des Geschäftswerts den Beteiligten den ROI erklären. Die Quantifizierung des Geschäftswerts kann Ihnen helfen, mehr Unterstützung von Beteiligten für zukünftige Investitionen zur Kostenoptimierung zu gewinnen, und bietet einen Rahmen, um die Ergebnisse für die Kostenoptimierung Ihrer Organisation zu messen.

## Risikostufe bei fehlender Befolgung dieser bewährten Methode: Mittel

### Implementierungsleitfaden

Die Quantifizierung des Geschäftswerts bedeutet, dass der Nutzen gemessen wird, den Unternehmen aus ihren Maßnahmen und Entscheidungen ziehen. Bei dem Geschäftswert kann es sich um einen materiellen Wert (z. B. geringere Ausgaben oder höhere Gewinne) oder einen immateriellen Wert (z. B. ein besseres Markenimage oder eine höhere Kundenzufriedenheit) handeln.

Die Quantifizierung des geschäftlichen Nutzens der Kostenoptimierung bedeutet, dass Sie feststellen müssen, wie viel Wert oder Nutzen Sie aus Ihren Bemühungen um effizientere Ausgaben ziehen. Wenn ein Unternehmen beispielsweise 100.000\$ ausgibt, um einen Workload bereitzustellen AWS und ihn später zu optimieren, belaufen sich die neuen Kosten auf nur 80.000\$, ohne dass die Qualität oder der Output beeinträchtigt wird. In diesem Szenario würde der quantifizierte Geschäftswert aus der Kostenoptimierung eine Einsparung von 20.000 USD bedeuten. Aber über die reinen Einsparungen hinaus kann das Unternehmen den Wert auch in Form von kürzeren Lieferzeiten, verbesserter Kundenzufriedenheit oder anderen Metriken, die sich aus den Kostenoptimierungsbemühungen ergeben, quantifizieren. Die Beteiligten müssen Entscheidungen über den potenziellen Wert der Kostenoptimierung, die Kosten für die Optimierung der Workload und den Ertragswert treffen.

Zusätzlich zu den Einsparungen durch Kostenoptimierung wird empfohlen, den zusätzlichen Wert zu quantifizieren. Die Vorteile der Kostenoptimierung werden in der Regel in Bezug auf niedrigere Kosten pro Geschäftsergebnis quantifiziert. Sie können beispielsweise die Kosteneinsparungen Amazon Elastic Compute Cloud(AmazonEC2) quantifizieren, wenn Sie Savings Plans erwerben, die die Kosten senken und das Workload-Output-Niveau aufrechterhalten. Sie können die Kostensenkungen bei den AWS Ausgaben quantifizieren, wenn inaktive EC2 Amazon-Instances entfernt oder nicht verknüpfte Amazon Elastic Block Store (AmazonEBS) -Volumes gelöscht werden.

Die Vorteile der Kostenoptimierung gehen jedoch über die Kostensenkung oder -vermeidung hinaus. Ziehen Sie in Betracht, zusätzliche Daten zu erfassen, um Effizienzsteigerungen und Geschäftswert zu messen.

### Implementierungsschritte

- **Bewertung der geschäftlichen Vorteile:** Bei diesem Prozess werden die AWS Cloud Kosten analysiert und so angepasst, dass der Nutzen aus jedem ausgegebenen Dollar maximiert wird. Anstatt sich auf Kostensenkungen ohne geschäftlichen Nutzen zu konzentrieren, sollten Sie die Geschäftsvorteile und die Kapitalrendite für die Kostenoptimierung in Betracht ziehen, da diese

einen größeren Nutzen aus den von Ihnen ausgegebenen Mitteln ziehen können. Dabei geht es darum, Ausgaben umsichtig vorzunehmen und Investitionen und Ausgaben in Bereichen zu tätigen, die den besten Ertrag bringen.

- Analysieren Sie AWS Kostenprognosen: Mithilfe von Prognosen können Stakeholder aus der Finanzabteilung bei anderen internen und externen Stakeholdern der Organisation ihre Erwartungen festlegen. Außerdem können sie die finanzielle Planbarkeit Ihres Unternehmens verbessern. [AWS Cost Explorer](#) kann verwendet werden, um Prognosen für Ihre Kosten und Nutzung durchzuführen.

## Ressourcen

### Zugehörige Dokumente:

- [AWS Cloud Wirtschaftswissenschaften](#)
- [AWS Blog](#)
- [AWS Kostenmanagement](#)
- [AWS Nachrichten-Blog](#)
- [Well-Architected-Whitepaper zur Säule „Zuverlässigkeit“](#)
- [AWS Cost Explorer](#)

### Zugehörige Videos:

- [Erschließen Sie geschäftlichen Nutzen mit eingeschaltetem Windows AWS](#)

### Zugehörige Beispiele:

- [Measuring and Maximizing the Business Value of Customer 360](#)
- [The Business Value of Adopting Amazon Web Services Managed Databases](#)
- [The Business Value of Amazon Web Services for Independent Software Vendors](#)
- [Business Value of Cloud Modernization](#)
- [The Business Value of Migration to Amazon Web Services](#)

## Ausgabenerkennung und Nutzungsbewusstsein

### Fragen



- [COST2. Wie können Sie die Nutzung steuern?](#)
- [COST3. Wie überwachen Sie Ihre Kosten und die Nutzung?](#)
- [COST4. Wie können Sie Ressourcen außer Betrieb nehmen?](#)

## COST2. Wie können Sie die Nutzung steuern?

Legen Sie Richtlinien und Mechanismen fest, um zu überprüfen, ob angemessene Kosten anfallen und die Ziele erreicht werden. Durch die Anwendung eines checks-and-balances Ansatzes können Sie innovativ sein, ohne zu viel auszugeben.

### Bewährte Methoden

- [COST02-BP01 Entwickeln Sie Richtlinien auf der Grundlage der Anforderungen Ihres Unternehmens](#)
- [COST02-BP02 Ziele und Vorgaben umsetzen](#)
- [COST02-BP03 Implementieren Sie eine Kontostruktur](#)
- [COST02-BP04 Gruppen und Rollen implementieren](#)
- [COST02-BP05 Implementieren Sie Kostenkontrollen](#)
- [COST02-BP06 Projektlebenszyklus verfolgen](#)

### COST02-BP01 Entwickeln Sie Richtlinien auf der Grundlage der Anforderungen Ihres Unternehmens

Entwickeln Sie Richtlinien, die definieren, wie Ressourcen von Ihrer Organisation verwaltet werden, und überprüfen Sie sie regelmäßig. Die Richtlinien sollten sich auch mit den Kostenaspekten der Ressourcen und Workloads befassen, einschließlich Erstellung, Änderung und Außerbetriebnahme während der gesamten Lebensdauer der Ressourcen.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Hoch

### Implementierungsleitfaden

Die Kenntnis der Kostentreiber in Ihrer Organisation ist für die effektive Verwaltung Ihrer Ausgaben und Nutzung und die Identifizierung von Kostenreduzierungsmöglichkeiten von entscheidender Bedeutung. Organisationen betreiben in der Regel mehrere Workloads, die von mehreren Teams ausgeführt werden. Diese Teams können sich in verschiedenen Organisationseinheiten befinden, die jeweils über eigene Einnahmequellen verfügen. Die Möglichkeit, die Ressourcenkosten den

Workloads, der jeweiligen Organisation oder den Produkteigentümern zuzuordnen, fördert ein effizientes Nutzungsverhalten und hilft, die Verschwendung von Ressourcen einzudämmen. Eine genaue Kosten- und Nutzungsüberwachung hilft Ihnen zu verstehen, wie optimiert eine Workload ist und wie profitabel Geschäftsbereiche und Produkte sind. Mit diesem Wissen können Sie fundiertere Entscheidungen dazu treffen, wo Ressourcen in Ihrer Organisation eingesetzt werden sollen. Das Bewusstsein der Nutzung auf allen Organisationsebenen ist entscheidend für Veränderungen, da eine Änderung der Nutzung zu Kostenänderungen führt. Überlegen Sie sich, beim Ermitteln von Nutzungsmustern und Ausgaben einen mehrschichtigen Ansatz zu nutzen.

Der erste Schritt bei der Implementierung von Governance besteht darin, Richtlinien für die Cloud-Nutzung anhand der Anforderungen Ihrer Organisation zu entwickeln. Diese Richtlinien definieren, wie Ihre Organisation die Cloud verwendet und wie Ressourcen verwaltet werden. Richtlinien sollten alle Aspekte von Ressourcen und Workloads abdecken, die sich auf Kosten oder Nutzung beziehen, einschließlich Erstellung, Änderung und Außerbetriebnahme über die Lebensdauer der Ressource. Überprüfen Sie, ob die Richtlinien und Verfahren bei jeder Änderung in einer Cloud-Umgebung eingehalten und umgesetzt werden. Stellen Sie bei Ihren Meetings zum IT-Änderungsmanagement Fragen zu den Kostenauswirkungen geplanter Änderungen, ob die Kosten steigen oder sinken, zur geschäftlichen Rechtfertigung und zum erwarteten Ergebnis.

Richtlinien sollten einfach sein, damit sie leicht verständlich sind und in der gesamten Organisation effektiv implementiert werden können. Richtlinien müssen außerdem leicht zu befolgen und zu interpretieren sein (damit sie angewendet werden können) sowie spezifisch sein (keine Fehlinterpretationen zwischen den Teams). Darüber hinaus müssen sie (wie unsere Mechanismen) regelmäßig überprüft und aktualisiert werden, wenn sich die Geschäftsbedingungen oder Prioritäten der Kunden ändern, wodurch die Richtlinie veraltet wäre.

Beginnen Sie mit umfangreichen allgemeinen Richtlinien, z. B. welche geografische Region verwendet werden soll oder zu welchen Tageszeiten Ressourcen ausgeführt werden sollen. Verfeinern Sie schrittweise die Richtlinien für die verschiedenen Organisationseinheiten und Workloads. Zu den allgemeinen Richtlinien gehört, welche Services und Features verwendet werden können (z. B. Speicher mit niedrigerer Leistung in Test- und Entwicklungsumgebungen), welche Ressourcentypen von verschiedenen Gruppen verwendet werden können (z. B. ist die größte Ressource in einem Entwicklungskonto mittelgroß) und wie lange diese Ressourcen verwendet werden (ob vorübergehend, kurzfristig oder für einen bestimmten Zeitraum).

### Beispiele für Richtlinien

Im Folgenden finden Sie eine Beispielrichtlinie, die Sie überprüfen können, um Ihre eigenen Cloud-Governance-Richtlinien zur Kostenoptimierung zu erstellen. Stellen Sie sicher, dass Sie die

Richtlinien an die Anforderungen Ihrer Organisation und die Anforderungen Ihrer Interessenvertreter anpassen.

- **Richtliniename:** Definieren Sie einen eindeutigen Namen für die Richtlinie, z. B. Richtlinie zur Ressourcenoptimierung und Kostenreduzierung.
- **Zweck:** Erläutern Sie, warum diese Richtlinie angewendet werden sollte und was das erwartete Ergebnis ist. Mit dieser Richtlinie soll überprüft werden, ob für die Bereitstellung und Ausführung der gewünschten Workload Mindestkosten anfallen, um die Geschäftsanforderungen zu erfüllen.
- **Geltungsbereich:** Definieren Sie klar, wer diese Richtlinie verwenden soll und wann sie verwendet werden soll, z. B. DevOps X Team, um diese Richtlinie bei Kunden in den USA im Osten für eine X-Umgebung (Produktion oder Nichtproduktion) zu verwenden.

### Richtlinienanweisung

1. Wählen Sie basierend auf der Umgebung Ihrer Workload und den Geschäftsanforderungen (Entwicklung, Benutzerakzeptanztests, Vorproduktion oder Produktion) entweder us-east-1 oder mehrere us-east-Regionen aus.
2. Planen Sie Amazon EC2 - und RDS Amazon-Instances so, dass sie zwischen sechs Uhr morgens und acht Uhr abends (Eastern Standard Time (EST)) ausgeführt werden.
3. Stoppen Sie alle ungenutzten EC2 Amazon-Instances nach acht Stunden und ungenutzte RDS Amazon-Instances nach 24 Stunden Inaktivität.
4. Beenden Sie alle ungenutzten EC2 Amazon-Instances nach 24 Stunden Inaktivität in Produktionsumgebungen. Erinnern Sie den Besitzer der EC2 Amazon-Instances (basierend auf Tags) daran, seine gestoppten EC2 Amazon-Instances in der Produktion zu überprüfen, und teilen Sie ihm mit, dass seine EC2 Amazon-Instances innerhalb von 72 Stunden beendet werden, wenn sie nicht verwendet werden.
5. Verwenden Sie eine generische Instance-Familie und Größe wie m5.large und ändern Sie dann die Größe der Instance auf CPU der Grundlage der Speicherauslastung mithilfe von AWS Compute Optimizer
6. Priorisieren Sie mithilfe von Auto Scaling, um die Anzahl der ausgeführten Instances je nach Datenverkehr dynamisch anzupassen.
7. Verwenden Sie Spot Instances für unkritische Workloads.
8. Prüfen Sie die Kapazitätsanforderungen, um Savings Plans oder Reserved Instances für vorhersehbare Workloads festzulegen, und informieren Sie das Cloud-Financial-Management-Team.

9. Verwenden Sie Amazon-S3-Lebenszyklusrichtlinien, um Daten, auf die selten zugegriffen wird, auf günstigere Speicherebenen zu verschieben. Wenn keine Aufbewahrungsrichtlinie definiert ist, verwenden Sie Amazon S3 Intelligent-Tiering, um Objekte automatisch auf die Archivebene zu verschieben.
10. Überwachen Sie mithilfe von Amazon die Ressourcennutzung und richten Sie Alarme ein, um Skalierungsereignisse auszulösen CloudWatch.
11. Verwenden Sie diese AWS-Konto Option, AWS Budgets um Kosten- und Nutzungsbudgets für Ihr Konto auf der Grundlage der Kostenstelle und der Geschäftsbereiche festzulegen.
12. Indem AWS Budgets Sie Kosten- und Nutzungsbudgets für Ihr Konto festlegen, behalten Sie den Überblick über Ihre Ausgaben und vermeiden unerwartete Rechnungen, sodass Sie Ihre Kosten besser kontrollieren können.

Verfahren: Richten Sie detaillierte Verfahren für die Umsetzung dieser Richtlinie ein oder verweisen Sie auf andere Dokumente, in denen beschrieben wird, wie die einzelnen Grundsatzklärungen umgesetzt werden. Dieser Abschnitt sollte step-by-step Anweisungen zur Erfüllung der Richtlinienanforderungen enthalten.

Zur Implementierung dieser Richtlinie können Sie verschiedene Tools oder AWS Config Regeln von Drittanbietern verwenden, um die Einhaltung der Richtlinienklärung zu überprüfen und mithilfe von AWS Lambda Funktionen automatische Abhilfemaßnahmen auszulösen. Sie können sie auch verwenden AWS Organizations , um die Richtlinie durchzusetzen. Darüber hinaus sollten Sie Ihre Ressourcennutzung regelmäßig überprüfen und die Richtlinie bei Bedarf anpassen, um sicherzustellen, dass sie weiterhin Ihren Geschäftsanforderungen entspricht.

### Implementierungsschritte

- Treffen mit Interessenvertretern: Um Richtlinien zu entwickeln, bitten Sie die Interessenvertreter (Cloud-Geschäftsstellen, Techniker oder funktionale Entscheidungsträger für die Durchsetzung von Richtlinien) innerhalb Ihrer Organisation, ihre Anforderungen festzulegen und zu dokumentieren. Führen Sie einen iterativen Ansatz aus, indem Sie bei jedem Schritt umfassend beginnen und kontinuierlich auf die kleinsten Einheiten verfeinern. Zu den Teammitgliedern gehören Personen mit direktem Interesse an der Workload, z. B. Organisationseinheiten oder Anwendungsbesitzer sowie unterstützende Gruppen wie Sicherheits- und Finanzteams.
- Bestätigung einholen: Vergewissern Sie sich, dass sich diejenigen Teams auf Richtlinien einigen, die auf die AWS Cloud Zugriff haben und darin Bereitstellungen vornehmen können. Sorgen Sie dafür, dass sie die Richtlinien Ihrer Organisation befolgen und stellen Sie sicher, dass ihre Ressourcenerstellung mit den vereinbarten Richtlinien und Verfahren übereinstimmt.

- Onboarding-Trainings veranstalten: Fordern Sie neue Organisationmitglieder auf, Onboarding-Trainings zu absolvieren, um ein Kostenbewusstsein und ein Verständnis für die Organisationsanforderungen zu schaffen. Möglicherweise gehen neue Organisationmitglieder aufgrund ihrer bisherigen Erfahrungen von anderen Richtlinien aus oder denken überhaupt nicht daran.
- Festlegen der Speicherorte für Ihre Workload: Definieren Sie, wo Ihre Workload ausgeführt wird, einschließlich des Landes und der Region innerhalb des Landes. Diese Informationen werden für die Zuordnung zu Availability Zones AWS-Regionen und Availability Zones verwendet.
- Definieren und Gruppieren von Services und Ressourcen: Definieren Sie die Services, die für die Workloads erforderlich sind. Geben Sie für jeden Service die Typen, den Umfang und die Anzahl der erforderlichen Ressourcen an. Definieren Sie Gruppen für die Ressourcen nach Funktion, z. B. Anwendungsserver oder Datenbankspeicher. Ressourcen können mehreren Gruppen angehören.
- Definieren und Gruppieren der Benutzer nach Funktion: Definieren Sie die Benutzer, die mit der Workload interagieren, und konzentrieren Sie sich darauf, was sie tun und wie sie die Workload verwenden, nicht auf die Benutzer oder ihre Position in der Organisation. Fassen Sie ähnliche Benutzer oder Funktionen in einer Gruppe zusammen. Sie können die AWS verwalteten Richtlinien als Leitfaden verwenden.
- Definieren der Aktionen: Definieren Sie mithilfe der zuvor identifizierten Standorte, Ressourcen und Benutzer die Aktionen, die von jedem benötigt werden, um die Workload-Ergebnisse über die Lebensdauer (Entwicklung, Betrieb und Außerbetriebnahme) zu erzielen. Identifizieren Sie die Aktionen an jedem Standort basierend auf den Gruppen, nicht auf den einzelnen Elementen in den Gruppen. Beginnen Sie umfassend mit Lese- oder Schreibvorgängen und verfeinern Sie dann auf bestimmte Aktionen für jeden Service.
- Definieren des Überprüfungszeitraums: Workloads und Organisationsanforderungen können sich im Laufe der Zeit ändern. Definieren Sie den Zeitplan für die Überprüfung der Workload, um sicherzustellen, dass sie den Prioritäten der Organisation entspricht.
- Dokumentieren der Richtlinien: Stellen Sie sicher, dass auf die definierten Richtlinien zugegriffen werden kann, wie von Ihrer Organisation gefordert. Diese Richtlinien werden verwendet, um den Zugriff auf Ihre Umgebungen zu implementieren, zu verwalten und zu prüfen.

## Ressourcen

### Zugehörige Dokumente:

- [Änderungsmanagement in der Cloud](#)
- [AWS Verwaltete Richtlinien für Jobfunktionen](#)

- [AWS Abrechnungsstrategie für mehrere Konten](#)
- [Aktionen, Ressourcen und Zustandsschlüssel für AWS Dienste](#)
- [AWS Verwaltung und Unternehmensführung](#)
- [Steuern Sie den Zugriff AWS-Regionen mithilfe von IAM Richtlinien](#)
- [Globale Infrastrukturen, Regionen und AZs](#)

Zugehörige Videos:

- [AWS Management und Steuerung im großen Maßstab](#)

Zugehörige Beispiele:

- [VMware- Was sind Cloud-Richtlinien?](#)

## COST02-BP02 Ziele und Vorgaben umsetzen

Implementieren Sie Kosten- und Nutzungsziele sowie Vorgaben für Ihre Workload. Ziele geben Ihrer Organisation die Richtung für die erwarteten Ergebnisse vor, und Vorgaben geben spezifische, messbare Ergebnisse vor, die für Ihre Workloads erreicht werden sollen.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Hoch

### Implementierungsleitfaden

Entwickeln Sie Kosten- und Nutzungsziele sowie Vorgaben für Ihre Organisation. Als wachsendes Unternehmen ist es wichtig AWS, Ziele für die Kostenoptimierung festzulegen und zu verfolgen. Zu diesen Zielen oder [wichtigen Leistungsindikatoren \(KPIs\)](#) können Dinge wie der Prozentsatz der Ausgaben auf Abruf oder die Einführung bestimmter optimierter Dienste wie AWS Graviton-Instances oder EBS GP3-Volumetypen gehören. Legen Sie messbare und erreichbare Ziele fest, anhand derer Sie Effizienzverbesserungen bewerten können, was für den Geschäftsbetrieb wichtig ist. Ziele bieten Ihrer Organisation richtungsweisende Anleitungen hinsichtlich der erwarteten Ergebnisse.

Vorgaben bieten spezifische messbare Ergebnisse, die erreicht werden müssen. Kurz gesagt, ein Ziel ist die Richtung, in die Sie gehen möchten, und ein Ziel gibt an, wie weit Sie in diese Richtung gehen und wann dieses Ziel erreicht werden sollte (verwenden Sie spezifische, messbare, zuweisbare, realistische und zeitnahe Leitlinien oder). SMART Ein Beispiel für ein Ziel ist, dass die Nutzung der Plattform deutlich steigen soll, wobei die Kosten nur geringfügig (nicht linear) steigen sollen. Ein Beispiel für eine Vorgabe ist eine Steigerung der Plattformnutzung um 20 % bei

einem Kostenanstieg von weniger als fünf Prozent. Ein weiteres häufiges Ziel ist, dass Workloads alle sechs Monate effizienter werden müssen. Die damit verbundene Vorgabe wäre, dass die Kosten pro Geschäftsmetrik alle 6 Monate um 5 Prozent sinken müssen. Verwenden Sie die richtigen Kennzahlen und legen Sie sie KPIs für Ihr Unternehmen kalkuliert fest. Sie können mit den Grundlagen beginnen KPIs und sich später auf der Grundlage der Geschäftsanforderungen weiterentwickeln.

Ein Ziel der Kostenoptimierung besteht darin, die Workload-Effizienz zu erhöhen, also die Kosten pro Geschäftsergebnis der Workload im Laufe der Zeit zu senken. Implementieren Sie dieses Ziel für alle Workloads und legen Sie als Vorgabe beispielsweise eine 5-prozentige Steigerung der Effizienz alle 6 Monate bis zu 1 Jahr fest. In der Cloud können Sie dies durch den Aufbau von Funktionen zur Kostenoptimierung sowie durch neue Service- und Feature-Releases erreichen.

Vorgaben sind die quantifizierbaren Benchmarks, die Sie anstreben, um Ihre Ziele zu erreichen, und mithilfe von Benchmarks werden die tatsächlichen Ergebnisse mit einer Vorgabe verglichen. Legen Sie Benchmarks KPIs für die Kosten pro Einheit von Rechendiensten (wie Spot-Einführung, Graviton-Einführung, neueste Instance-Typen und On-Demand-Abdeckung), Speicherservices (wie EBS GP3 Einführung, veraltete EBS Snapshots und Amazon S3 S3-Standard Speicher) oder die Nutzung von Datenbankdiensten (wie RDS Open-Source-Engines, Einführung von Graviton und On-Demand-Abdeckung) fest. Mithilfe dieser Benchmarks KPIs können Sie überprüfen, ob Sie Dienste auf die kostengünstigste Art und Weise nutzen AWS .

Die folgende Tabelle enthält eine Liste von AWS Standardmetriken als Referenz. Jede Organisation kann für diese Ziele unterschiedliche Zielwerte festlegen KPIs.

Kategorie	KPI (%)	Beschreibung
Datenverarbeitung	EC2Umfang der Nutzung	EC2Instances (in Kosten oder Stunden), die SP+RI+Spot verwenden, im Vergleich zur Gesamtzahl (in Kosten oder Stunden) der Instances EC2
Datenverarbeitung	Berechnung der SP/RI-Auslastung	Die genutzten SP- oder RI-Stunden im Vergleich zur Gesamtzahl der verfügbaren SP- oder RI-Stunden

Kategorie	KPI (%)	Beschreibung
Datenverarbeitung	EC2/Kosten pro Stunde	EC2Kosten geteilt durch die Anzahl der EC2 Instances, die in dieser Stunde ausgeführt wurden
Datenverarbeitung	v CPU kostet	Kosten pro V CPU für alle Instanzen
Datenverarbeitung	Aktuelle Instance-Generation	Prozentsatz der Instances in Graviton (oder anderen Instance-Typen der modernen Generation)
Datenbank	RDSDeckung	RDSInstances (in Kosten oder Stunden), die RI nutzen, im Vergleich zur Gesamtzahl (in Kosten oder Stunden) der RDS Instances
Datenbank	RDSAuslastung	Die RI-Stunden im Vergleich zur Gesamtzahl der verfügbaren RI-Stunden
Datenbank	RDSBetriebszeit	RDSKosten geteilt durch die Anzahl der RDS Instances, die in dieser Stunde ausgeführt wurden
Datenbank	Aktuelle Instance-Generation	Prozentsatz der Instances in Graviton (oder anderen modernen Instance-Typen)



Kategorie	KPI (%)	Beschreibung
Speicher	Speichernutzung	Optimierte Speicherkosten (z. B. Glacier, Deep Archive oder Infrequent Access) geteilt durch die Gesamtspeicherkosten
Tagging	Ressourcen ohne Tags	<p>Cost Explorer:</p> <ol style="list-style-type: none"> <li>1. Filtern Sie Gutschriften, Rabatte, Steuern, Rückerstattungen und Marketplace heraus und kopieren Sie die aktuellen Monatskosten.</li> <li>2. Wählen Sie in Cost Explorer die Option Nur Ressourcen ohne Tag anzeigen aus.</li> <li>3. Teilen Sie den Betrag in Ressourcen ohne Tags durch Ihre monatlichen Kosten.</li> </ol>

Geben Sie anhand dieser Tabelle die Ziel- oder Benchmarkwerte an, die auf der Grundlage Ihrer Organisationsziele berechnet werden sollten. Sie müssen bestimmte Kennzahlen für Ihr Unternehmen messen und das Geschäftsergebnis für diesen Workload verstehen, um sie präzise und realistisch definieren zu können KPIs. Unterscheiden Sie bei der Bewertung von Leistungsmetriken innerhalb einer Organisation zwischen verschiedenen Arten von Metriken, die unterschiedlichen Zwecken dienen. Mit diesen Metriken werden in erster Linie die Leistung und Effizienz der technischen Infrastruktur und nicht direkt die allgemeinen Auswirkungen auf das Geschäft gemessen. Es können beispielsweise die Reaktionszeiten des Servers, die Netzwerklatenz oder die Systemverfügbarkeit verfolgt werden. Diese Metriken sind entscheidend, um zu bewerten, wie gut die Infrastruktur den technischen Betrieb der Organisation unterstützt. Sie bieten jedoch keinen direkten Einblick in umfassendere Geschäftsziele wie Kundenzufriedenheit, Umsatzwachstum oder Marktanteil. Um ein umfassendes Verständnis der Unternehmensleistung zu erhalten,

ergänzen Sie diese Effizienzmetriken durch strategische Geschäftsmetriken, die direkt mit den Geschäftsergebnissen korrelieren.

Verschaffen Sie sich nahezu in Echtzeit einen Überblick über Ihre KPIs und die damit verbundenen Einsparmöglichkeiten und verfolgen Sie Ihre Fortschritte im Laufe der Zeit. Für den Einstieg in die Definition und Nachverfolgung von KPI Zielen empfehlen wir das KPI Dashboard von [Cloud Intelligence Dashboards](#) (CID). Basierend auf den Daten aus dem Kosten- und Nutzungsbericht (CUR) bietet das KPI Dashboard eine Reihe von Empfehlungen zur Kostenoptimierung mit der Möglichkeit KPIs, benutzerdefinierte Ziele festzulegen und den Fortschritt im Laufe der Zeit zu verfolgen.

Wenn Sie über andere Lösungen zur Festlegung und Nachverfolgung von KPI Zielen verfügen, stellen Sie sicher, dass diese Methoden von allen Beteiligten im Cloud-Finanzmanagement in Ihrem Unternehmen übernommen werden.

### Implementierungsschritte

- Definieren der erwarteten Nutzungsgrade: Konzentrieren Sie sich zu Beginn auf die Nutzungsgrade. Sprechen Sie mit den Anwendungsbesitzern, der Marketingabteilung und größeren Geschäftsteams, um zu verstehen, wie die erwartete Nutzung für die Workload aussieht. Wie könnte sich die Kundennachfrage im Laufe der Zeit ändern und was kann sich aufgrund saisonaler Anstiege oder Marketingkampagnen ändern?
- Definieren von Ressourcen und Kosten für Workloads: Mit den definierten Nutzungsgraden quantifizieren Sie die Änderungen der Workload-Ressourcen, die erforderlich sind, um diese Nutzungsgrade zu erfüllen. Möglicherweise müssen Sie den Umfang oder die Anzahl der Ressourcen für eine Workload-Komponente und die Datenübertragung erhöhen oder Workload-Komponenten in einen anderen Service auf einer bestimmten Ebene ändern. Geben Sie die Kosten an jedem dieser Hauptpunkte an und prognostizieren Sie die Kostenänderung, wenn sich die Nutzung ändert.
- Definieren von Geschäftszielen: Nehmen Sie die Ergebnisse zu den erwarteten Änderungen bei Nutzung und Kosten, kombinieren Sie sie mit den erwarteten Änderungen bei der Technologie oder sonstigen Programmen, die Sie ausführen, und entwickeln Sie Ziele für die Workload. Die Ziele müssen Nutzung und Kosten sowie das Verhältnis zwischen beiden berücksichtigen. Die Ziele müssen einfach und allgemein gehalten sein und den Mitarbeitern helfen zu verstehen, was das Unternehmen an Ergebnissen erwartet (z. B. sicherzustellen, dass ungenutzte Ressourcen unter einem bestimmten Kostenniveau gehalten werden). Sie müssen nicht für jeden ungenutzten Ressourcentyp Ziele definieren oder Kosten festlegen, die Verluste für Ziele und Vorgaben verursachen können. Überprüfen Sie, ob es organisatorische Programme gibt (z. B.

Kompetenzaufbau wie Schulungen und Fortbildungen), wenn Kostenänderungen ohne veränderte Nutzung zu erwarten sind.

- Definieren der Ergebnisse: Geben Sie für jedes der definierten Ziele ein messbares Ergebnis an. Wenn das Ziel darin besteht, die Effizienz der Workload zu erhöhen, sollte mit der Vorgabe der Umfang der Verbesserung (in der Regel in Form von Geschäftsergebnissen für jeden ausgegebenen Dollar) und der Zeitpunkt der Erreichung dieses Ziels angegeben werden. Sie könnten sich zum Beispiel das Ziel setzen, Verschwendung aufgrund einer Überversorgung zu minimieren. Bei diesem Ziel kann Ihre Vorgabe darin bestehen, dass die Verschwendung aufgrund einer zu hohen Datenverarbeitungsleistung in der ersten Stufe der Produktionsworkloads 10 Prozent der Datenverarbeitungskosten auf dieser Stufe nicht überschreiten sollte. Darüber hinaus könnte eine zweite Vorgabe darin bestehen, dass die Verschwendung aufgrund einer zu hohen Datenverarbeitungsleistung in der zweiten Stufe der Produktionsworkloads 5 Prozent der Datenverarbeitungskosten auf dieser Stufe nicht überschreiten sollte.

## Ressourcen

### Zugehörige Dokumente:

- [Von AWS verwaltete Richtlinien für Auftragsfunktionen](#)
- [AWS -Fakturierungsstrategie mit mehreren Konten](#)
- [Steuern Sie den Zugriff AWS-Regionen mithilfe von IAM Richtlinien](#)
- [S.M.A.R.T.-Ziele](#)
- [So verfolgen Sie Ihre Kostenoptimierung KPIs mit dem CID KPI Dashboard](#)

### Zugehörige Videos:

- [Well-Architected Labs: Goals and Targets \(Level 100\)](#)

### Zugehörige Beispiele:

- [What is a unit metric?](#)
- [Selecting a unit metric to support your business](#)
- [Unit metrics in practice – lessons learned](#)
- [How unit metrics help create alignment between business functions](#)
- [Well-Architected Labs: Decommission resources \(Goals and Targets\)](#)

- [Well-Architected Labs: Resource Type, Size and Number \(Goals and Targets\)](#)

## COST02-BP03 Implementieren Sie eine Kontostruktur

Implementieren Sie eine Kontenstruktur, die für Ihre Organisation geeignet ist. Dadurch werden die Zuweisung und Verwaltung der Kosten in der gesamten Organisation erleichtert.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Hoch

### Implementierungsleitfaden

AWS Organizations ermöglicht es Ihnen, mehrere zu erstellen, mit AWS-Konten denen Sie Ihre Umgebung zentral verwalten können, während Sie Ihre Workloads skalieren. AWS Sie können Ihre Organisationshierarchie modellieren, indem Sie sie AWS-Konten in einer Organisationseinheitenstruktur (OU) gruppieren und AWS-Konten unter jeder Organisationseinheit mehrere erstellen. Um eine Kontostruktur zu erstellen, müssen Sie zuerst entscheiden, welches Ihrer AWS-Konten das Verwaltungskonto sein soll. Danach können Sie basierend auf der von Ihnen entworfenen Kontostruktur neue Konten erstellen AWS-Konten oder bestehende Konten als Mitgliedskonten auswählen, indem Sie die [bewährten Methoden für Verwaltungskonten](#) und [Mitgliedskonten befolgen](#).

Sie sollten immer mindestens ein Verwaltungs- mit einem verknüpften Mitgliedskonto haben, unabhängig von der Unternehmensgröße oder Nutzung. Alle Workload-Ressourcen sollten sich nur in Mitgliedskonten befinden. In Verwaltungskonten sollten keine Ressourcen erstellt werden. Es gibt keine allgemeingültige Antwort darauf, wie viele AWS-Konten Sie haben sollten. Beurteilen Sie Ihre aktuellen und future Betriebs- und Kostenmodelle, um sicherzustellen, dass Ihre Struktur den Zielen Ihres Unternehmens AWS-Konten entspricht. Einige Unternehmen erstellen mehrere aus geschäftlichen AWS-Konten Gründen, zum Beispiel:

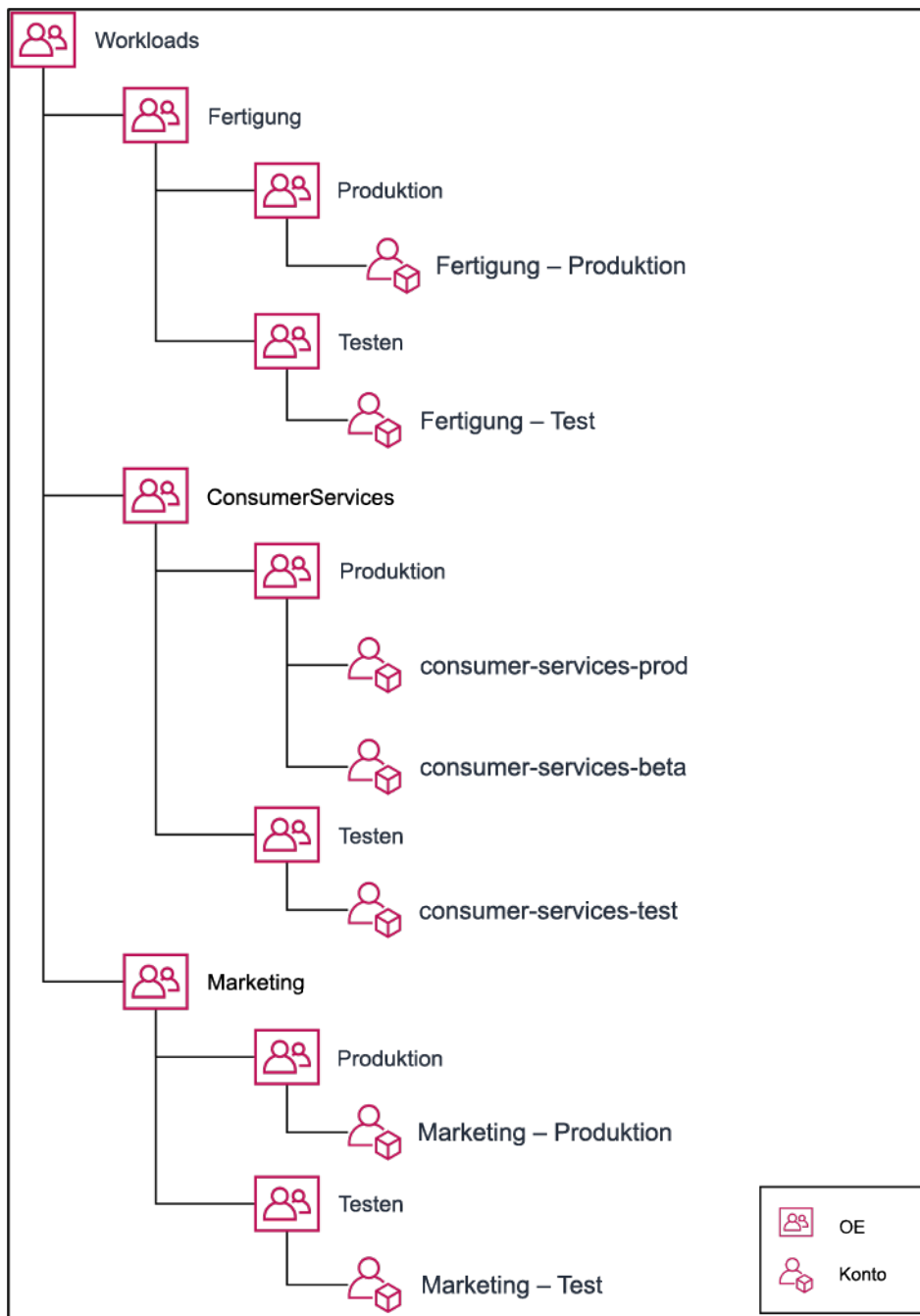
- Es ist eine administrative oder fiskale und fakturierungsbezogene Abgrenzung zwischen Organisationseinheiten, Kostenstellen oder spezifischen Workloads erforderlich.
- AWS Die Service-Limits sind so festgelegt, dass sie für bestimmte Workloads spezifisch sind.
- Es besteht eine Anforderung für Isolierung und Trennung zwischen Workloads und Ressourcen.

Innerhalb von [AWS Organizations](#) erstellt die [konsolidierte Fakturierung](#) das Konstrukt zwischen einem oder mehreren Mitgliedskonten und dem Verwaltungskonto. Mit Mitgliedskonten können Sie Ihre Kosten und Nutzung nach Gruppen isolieren und unterscheiden. In diesem Kontext hat es sich

bewährt, separate Mitgliedskonten für jede Organisationseinheit (z. B. Finanzen, Marketing und Vertrieb) oder für jeden Umgebungslebenszyklus (z. B. Entwicklung, Tests und Produktion) oder für jeden einzelnen Workload (Workload a, b und c) zu erstellen und diese verknüpften Konten dann über die konsolidierte Fakturierung zu aggregieren.

Mit der konsolidierten Fakturierung können Sie die Zahlung für mehrere AWS-Konten unter einem einzelnen Verwaltungskonto konsolidieren und dabei weiterhin die Sichtbarkeit für die Aktivitäten jedes verknüpften Kontos bereitstellen. Da Kosten und Nutzung im Verwaltungskonto aggregiert werden, können Sie sowohl Ihre Service-Volumenrabatte als auch die Nutzung Ihrer an feste Kapazität gebundene Rabatte (Savings Plans und Reserved Instances) maximieren und so die höchsten Vergünstigungen erzielen.

Das folgende Diagramm zeigt, wie Sie AWS Organizations mithilfe von Organisationseinheiten (OU) mehrere Konten gruppieren und jeder OU mehrere Konten AWS-Konten zuordnen können. Es wird empfohlen, es OUs für verschiedene Anwendungsfälle und Workloads zu verwenden. Es bietet Muster für die Organisation von Konten.



Beispiel für die Gruppierung mehrerer zu AWS-Konten Organisationseinheiten.

[AWS Control Tower](#) kann schnell mehrere AWS Konten einrichten und konfigurieren und so sicherstellen, dass die Unternehmensführung den Anforderungen Ihres Unternehmens entspricht.

### Implementierungsschritte

- Definieren von Trennungsanforderungen: Die Trennungsanforderungen sind eine Kombination aus mehreren Faktoren, darunter fallen Sicherheit, Zuverlässigkeit und finanzielle Konstrukte. Arbeiten

Sie die einzelnen Faktoren in der richtigen Reihenfolge durch und geben Sie an, ob der Workload oder die Workload-Umgebung von anderen Workloads getrennt sein sollte. Bei der Sicherheit steht die Einhaltung der Anforderungen an Zugriff und Daten im Vordergrund. Zuverlässigkeit bezieht sich auf die Verwaltung von Limits, sodass Umgebungen und Workloads keine Auswirkungen auf andere Elemente haben. Gehen Sie die Säulen Sicherheit und Zuverlässigkeit des Well-Architected Framework regelmäßig durch und halten Sie sich an die angegebenen bewährten Methoden. Finanzielle Konstrukte schaffen eine strikte Trennung im Bereich der Finanzen (verschiedene Kostenstellen, Verantwortlichkeiten für die Workloads und Rechenschaftspflicht). Häufige Beispiele für die Trennung sind Produktions- und Test-Workloads, die in separaten Konten ausgeführt werden, oder die Verwendung eines separaten Kontos, sodass die Rechnungs- und Fakturierungsdaten den verschiedenen Unternehmenseinheiten oder Abteilungen in der Organisation oder dem Stakeholder bereitgestellt werden können, dem das Konto gehört.

- Definieren von Gruppierungsanforderungen: Die Anforderungen für die Gruppierung überschreiben die Trennungsanforderungen nicht, sondern dienen zur Unterstützung der Verwaltung. Gruppieren Sie ähnliche Umgebungen oder Workloads, die keine Trennung erfordern. Ein Beispiel hierfür ist die Gruppierung mehrerer Test- oder Entwicklungsumgebungen aus einem oder mehreren Workloads.
- Definieren der Kontenstruktur: Geben Sie mit diesen Trennungen und Gruppierungen ein Konto für jede Gruppe an und stellen Sie sicher, dass die Trennungsanforderungen erfüllt werden. Diese Konten sind Ihre Mitgliedskonten oder verknüpfte Konten. Indem Sie diese Mitgliedskonten unter einem einzigen Verwaltungs-/Zahlungskonto gruppieren, kombinieren Sie die Nutzung. Dies ermöglicht höhere Volumenrabatte für alle Konten und Sie erhalten eine gemeinsame Rechnung für alle Konten. Es ist möglich, Fakturierungsdaten zu trennen und jedem Mitgliedskonto eine individuelle Ansicht ihrer Fakturierungsdaten bereitzustellen. Wenn die Nutzungs- oder Abrechnungsdaten eines Mitgliedskontos für kein anderes Konto sichtbar sein dürfen oder wenn eine separate Rechnungsadresse erforderlich ist, definieren Sie mehrere Verwaltungs- oder Zahlerkonten. In diesem Fall hat jedes Mitgliedskonto ein eigenes Verwaltungs-/Zahlungskonto. Ressourcen sollten immer in Mitgliedskonten oder verknüpften Konten platziert werden. Die Verwaltungs-/Zahlungskonten sollten nur für die Verwaltung verwendet werden.

## Ressourcen

### Zugehörige Dokumente:

- [Verwendung von Kostenzuordnungs-Tags](#)
- [Von AWS verwaltete Richtlinien für Auftragsfunktionen](#)

- [AWS -Fakturierungsstrategie mit mehreren Konten](#)
- [Steuern Sie den Zugriff AWS-Regionen mithilfe von Richtlinien IAM](#)
- [AWS Control Tower](#)
- [AWS Organizations](#)
- Bewährte Methoden für [Verwaltungskonten](#) und [Mitgliedskonten](#)
- [Organisieren Sie Ihre AWS Umgebung mithilfe mehrerer Konten](#)
- Aktivieren des Teilens der Rabatte für Reserved Instances und Savings Plans
- [Konsolidierte Fakturierung](#)
- [Konsolidierte Fakturierung](#)

Zugehörige Beispiele:

- [Den Zugriff aufteilen CUR und gemeinsam nutzen](#)

Zugehörige Videos:

- [Wir stellen vor AWS Organizations](#)
- [Richten Sie eine AWS Umgebung mit mehreren Konten ein, die Best Practices verwendet für AWS Organizations](#)

Zugehörige Beispiele:

- [Well-Architected Labs: Eine AWS Organisation erstellen \(Stufe 100\)](#)
- [Den Zugriff aufteilen und gemeinsam nutzen AWS Cost and Usage Report](#)
- [Definition einer AWS Multi-Account-Strategie für Telekommunikationsunternehmen](#)
- [Bewährte Methoden zur Optimierung AWS-Konten](#)
- [Bewährte Methoden für Organisationseinheiten mit AWS Organizations](#)

COST02-BP04 Gruppen und Rollen implementieren

Implementieren Sie Gruppen und Rollen, die Ihren Richtlinien entsprechen, und steuern Sie, wer Instances und Ressourcen in jeder Gruppe erstellen, ändern oder außer Betrieb nehmen kann. Implementieren Sie beispielsweise Entwicklungs-, Test- und Produktionsgruppen. Dies gilt für AWS Dienste und Lösungen von Drittanbietern.



Risikostufe bei fehlender Befolgung dieser bewährten Methode: Niedrig

## Implementierungsleitfaden

Benutzerrollen und -gruppen sind grundlegende Bausteine bei der Entwicklung und Implementierung sicherer und effizienter Systeme. Rollen und Gruppen helfen Organisationen dabei, den Bedarf an Kontrolle mit den Anforderungen an Flexibilität und Produktivität in Einklang zu bringen, um letztlich die Organisationsziele und die Bedürfnisse der Benutzer zu unterstützen. Wie im Abschnitt [Identitäts- und Zugriffsmanagement](#) von AWS Well-Architected Framework Security Pillar empfohlen, benötigen Sie ein robustes Identitätsmanagement und Berechtigungen, um den richtigen Personen unter den richtigen Bedingungen Zugriff auf die richtigen Ressourcen zu gewähren. Die Benutzer erhalten nur den Zugriff, den sie zur Erfüllung ihrer Aufgaben benötigen. Auf diese Weise wird das Risiko eines nicht autorisierten Zugriffs oder Missbrauchs minimiert.

Nachdem Sie Richtlinien entwickelt haben, können Sie logische Gruppen und Rollen von Benutzern innerhalb Ihrer Organisation erstellen. Auf diese Weise können Sie Berechtigungen zuweisen, die Nutzung kontrollieren und robuste Zugriffskontrollmechanismen implementieren, die den nicht autorisierten Zugriff auf sensible Informationen verhindern. Beginnen Sie mit allgemeinen Personengruppen. Dies entspricht in der Regel den Organisationseinheiten und beruflichen Rollen (z. B. ein Systemadministrator in der IT-Abteilung, ein Financial Controller oder ein Geschäftsanalyst). Den Gruppen treten Personen bei, die ähnliche Aufgaben ausführen und ähnlichen Zugriff benötigen. Rollen definieren, was eine Gruppe tun muss. Es ist einfacher, Berechtigungen für Gruppen und Rollen zu verwalten als für einzelne Benutzer. Rollen und Gruppen weisen allen Benutzern konsistent und systematisch Berechtigungen zu und verhindern so Fehler und Inkonsistenzen.

Wenn sich die Rolle eines Benutzers ändert, können Administratoren den Zugriff auf Rollen- oder Gruppenebene anpassen, anstatt einzelne Benutzerkonten neu zu konfigurieren. Beispielsweise benötigt ein Systemadministrator in der IT Zugriff, um alle Ressourcen zu erstellen, aber ein Analytikteammitglied muss nur Analytikressourcen erstellen.

## Implementierungsschritte

- Implementieren von Gruppen: Implementieren Sie bei Bedarf die entsprechenden Gruppen mithilfe der in Ihren Organisationsrichtlinien definierten Benutzergruppen. Bewährte Methoden für Benutzer, Gruppen und Authentifizierung finden Sie im [Security Pillar of the](#) AWS Well-Architected Framework.
- Implementieren von Rollen und Richtlinien: Erstellen Sie mithilfe der Aktionen, die in Ihren Organisationsrichtlinien definiert sind, die erforderlichen Rollen und Zugriffsrichtlinien. Bewährte

Methoden zu Rollen und Richtlinien finden Sie in der [Sicherheitssäule](#) des AWS Well-Architected Framework.

## Ressourcen

### Zugehörige Dokumente:

- [Von AWS verwaltete Richtlinien für Auftragsfunktionen](#)
- [AWS -Fakturierungsstrategie mit mehreren Konten](#)
- [AWS Sicherheitssäule eines gut konzipierten Frameworks](#)
- [AWS Identity and Access Management \(IAM\)](#)
- [AWS Identity and Access Management Richtlinien](#)

### Zugehörige Videos:

- [Why use Identity and Access Management](#)

### Zugehörige Beispiele:

- [Well-Architected Lab Basic Identity and Access](#)
- [Steuern Sie den Zugriff auf die AWS-Regionen Verwendung von IAM Richtlinien](#)
- [Starting your Cloud Financial Management journey: Cloud cost operations](#)

## COST02-BP05 Implementieren Sie Kostenkontrollen

Implementieren Sie Kontrollmechanismen, die auf den Organisationsrichtlinien sowie auf definierten Gruppen und Rollen basieren. Damit wird sichergestellt, dass nur Kosten im Rahmen der festgelegten Organisationsanforderungen anfallen, z. B. durch Steuerung des Zugriffs auf Regionen oder Ressourcentypen.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Mittel

## Implementierungsleitfaden

Ein häufiger erster Schritt bei der Implementierung von Kostenkontrollen ist die Einrichtung von Benachrichtigungen, wenn im Zusammenhang mit Kosten oder Nutzung Ereignisse auftreten, die

den Richtlinien nicht entsprechen. Auf diese Weise können Sie schnell agieren und überprüfen, ob Korrekturmaßnahmen erforderlich sind, ohne dass Workloads oder neue Aktivitäten eingeschränkt oder beeinträchtigt werden. Sobald Sie die Arbeitslast- und Umgebungsgrenzen kennen, können Sie die Steuerung durchsetzen. [AWS Budgets](#) ermöglicht es Ihnen, Benachrichtigungen einzurichten und monatliche Budgets für Ihre AWS Kosten, Nutzung und Abonnementrabatte (Savings Plans und Reserved Instances) zu definieren. Sie können Budgets auf aggregierter Kostenebene (z. B. alle Kosten) oder auf einer detaillierteren Ebene erstellen, in der Sie nur bestimmte Dimensionen wie verknüpfte Konten, Services, Tags oder Availability Zones einschließen.

Sobald Sie Ihre Budgetgrenzen mit eingerichtet haben AWS Budgets, verwenden Sie diese, [AWS Cost Anomaly Detection](#) um Ihre unerwarteten Kosten zu reduzieren. AWS Cost Anomaly Detection ist ein Kostenmanagement-Service, der maschinelles Lernen nutzt, um Ihre Kosten und Nutzung kontinuierlich zu überwachen und ungewöhnliche Ausgaben zu erkennen. So können Sie untypische Ausgaben und ihre Ursachen schnell identifizieren und so schnell Maßnahmen ergreifen. Erstellen Sie zunächst einen Kostenmonitor in und wählen Sie dann Ihre bevorzugte Warnmeldung aus AWS Cost Anomaly Detection, indem Sie einen Schwellenwert einrichten (z. B. eine Warnung bei Anomalien mit einer Auswirkung von mehr als 1.000 USD). Wenn Sie Warnungen erhalten, können Sie die Ursachen hinter den Unregelmäßigkeiten und deren wirtschaftliche Auswirkungen analysieren. Sie können Unregelmäßigkeiten in AWS Cost Explorer auch selbst überwachen und analysieren.

Setzen Sie Governance-Richtlinien AWS durch [AWS Identity and Access Management](#) und durch Richtlinien zur [AWS Organizations Servicesteuerung](#) () durch. SCP IAM ermöglicht es Ihnen, den Zugriff auf AWS Dienste und Ressourcen sicher zu verwalten. Mithilfe können Sie steuern IAM, wer AWS Ressourcen erstellen oder verwalten kann, welche Art von Ressourcen erstellt werden können und wo sie erstellt werden können. So wird die Möglichkeit eingeschränkt, Ressourcen außerhalb der definierten Richtlinie zu erstellen. Verwenden Sie die zuvor erstellten Rollen und Gruppen und weisen Sie [IAM Richtlinien](#) zu, um die korrekte Verwendung durchzusetzen. SCP bietet eine zentrale Kontrolle über die maximal verfügbaren Berechtigungen für alle Konten in Ihrer Organisation, sodass Ihre Konten Ihren Richtlinien für die Zugriffskontrolle entsprechen. SCP sind nur in einer Organisation verfügbar, in der alle Funktionen aktiviert sind. Sie können sie so konfigurieren, dass Aktionen für Mitgliedskonten standardmäßig entweder verweigert oder zugelassen werden. SCPs Weitere Informationen zur Implementierung des Zugriffsmanagements finden Sie im [Well-Architected-Whitepaper zur Säule „Sicherheit“](#).

Governance kann auch durch die Verwaltung von [AWS Service Quotas](#) implementiert werden. Indem Sie sicherstellen, dass Service Quotas mit minimalem Overhead definiert und ordnungsgemäß verwaltet werden, können Sie die Ressourcenerstellung über die Geschäftsanforderungen hinaus

minimieren. Dazu müssen Sie nachvollziehen, wie schnell sich Ihre Anforderungen ändern können, Sie müssen die derzeit ausgeführten Projekte kennen – in Bezug auf die Erstellung und die Deaktivierung von Ressourcen – und berücksichtigen, wie schnell Kontingentänderungen implementiert werden können. [Service Quotas](#) können bei Bedarf verwendet werden, um Ihre Kontingente zu erhöhen.

## Implementierungsschritte

- Implementieren von Benachrichtigungen zu Ausgaben: Erstellen Sie mithilfe Ihrer definierten Organisationsrichtlinien [AWS Budgets](#), um Benachrichtigungen zu erhalten, wenn Ausgaben außerhalb Ihrer Richtlinien liegen. Konfigurieren Sie mehrere Kostenbudgets, eines für jedes Konto, um über die allgemeinen Kontoausgaben informiert zu werden. Konfigurieren Sie zusätzliche Kostenbudgets innerhalb jedes Kontos für kleinere Einheiten innerhalb des Kontos. Diese Einheiten variieren je nach Kontostruktur. Einige gängige Beispiele sind AWS-Regionen Workloads (mithilfe von Tags) oder AWS Dienste. Konfigurieren Sie eine E-Mail-Verteilerliste als Empfänger für Benachrichtigungen, nicht das E-Mail-Konto einer Person. Sie können ein tatsächliches Budget für den Fall konfigurieren, dass ein Betrag überschritten wird, oder ein prognostiziertes Budget zur Benachrichtigung über die prognostizierte Nutzung verwenden. Sie können auch AWS Budgetaktionen vorkonfigurieren, mit denen bestimmte SCP Richtlinien durchgesetzt IAM oder Amazon- EC2 oder RDS Amazon-Ziel-Instances gestoppt werden können. Budgetaktionen werden entweder automatisch gestartet oder erfordern eine Workflow-Genehmigung.
- Implementieren von Benachrichtigungen zu ungewöhnlichen Ausgaben: Mit [AWS Cost Anomaly Detection](#) können Sie unerwartete Kosten in Ihrer Organisation reduzieren und die Ursachen potenzieller ungewöhnlicher Ausgaben analysieren. Sobald Sie den Kostenmonitor eingerichtet haben, um ungewöhnliche Ausgaben mit der von Ihnen angegebenen Granularität zu identifizieren, und Benachrichtigungen konfiguriert haben AWS Cost Anomaly Detection, erhalten Sie eine Benachrichtigung, wenn ungewöhnliche Ausgaben festgestellt werden. So können Sie die Ursache der Unregelmäßigkeit analysieren und erhalten Informationen zu den Auswirkungen auf Ihre Kosten. Verwenden Sie bei der Konfiguration AWS Cost Categories, AWS Cost Anomaly Detection um zu ermitteln, welches Projektteam oder welches Team der Geschäftseinheit die Ursache der unerwarteten Kosten analysieren und rechtzeitig die erforderlichen Maßnahmen ergreifen kann.
- Implementieren Sie Nutzungskontrollen: Implementieren Sie anhand Ihrer definierten IAM Unternehmensrichtlinien Richtlinien und Rollen, um festzulegen, welche Aktionen Benutzer ausführen können und welche nicht. Eine Richtlinie kann mehrere AWS Unternehmensrichtlinien enthalten. Gehen Sie auf die gleiche Art und Weise vor, wie Sie Richtlinien definiert haben. Beginnen Sie umfassend und wenden dann bei jedem Schritt detailliertere Kontrollen an. Service

Limits sind auch eine effektive Kontrolle der Nutzung. Implementieren Sie die richtigen Service Limits für alle Ihre Konten.

## Ressourcen

### Zugehörige Dokumente:

- [Von AWS verwaltete Richtlinien für Auftragsfunktionen](#)
- [AWS -Fakturierungsstrategie mit mehreren Konten](#)
- [Steuern Sie den Zugriff AWS-Regionen mithilfe von IAM Richtlinien](#)
- [AWS Budgets](#)
- [AWS Cost Anomaly Detection](#)
- [Kontrollieren Sie Ihre AWS Kosten](#)

### Zugehörige Videos:

- [Wie kann ich AWS Budgets damit meine Ausgaben und Nutzung verfolgen](#)

### Zugehörige Beispiele:

- [Beispiel für Richtlinien IAM zur Zugriffsverwaltung](#)
- [Example service control policies](#)
- [AWS Budgets und Aktionen](#)
- [IAM Richtlinie zur Steuerung des Zugriffs auf EC2 Amazon-Ressourcen mithilfe von Tags erstellen](#)
- [Beschränken Sie den Zugriff von IAM Identity auf bestimmte EC2 Amazon-Ressourcen](#)
- [Erstellen Sie eine IAM Richtlinie, um die EC2 Nutzung von Amazon nach Familien einzuschränken](#)
- [Well-Architected Labs: Cost and Usage Governance \(Level 100\)](#)
- [Well-Architected Labs: Cost and Usage Governance \(Level 200\)](#)
- [Slack-Integrationen zur Erkennung von Kostenanomalien mithilfe AWS Chatbot](#)

## COST02-BP06 Projektlebenszyklus verfolgen

Verfolgen, bewerten und überprüfen Sie den Lebenszyklus von Projekten, Teams und Umgebungen, damit Sie keine unnötigen Ressourcen nutzen, für die Sie zahlen müssen.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Niedrig

## Implementierungsleitfaden

Durch eine effektive Nachverfolgung des Projektlebenszyklus können Organisationen durch verbesserte Planung, Verwaltung und Ressourcenoptimierung eine bessere Kostenkontrolle erreichen. Die durch die Nachverfolgung gewonnenen Erkenntnisse sind von unschätzbarem Wert, um fundierte Entscheidungen zu treffen, die zur Kosteneffizienz und zum Gesamterfolg des Projekts beitragen.

Die Verfolgung des gesamten Lebenszyklus der Workload hilft Ihnen zu verstehen, wann Workloads oder Workload-Komponenten nicht mehr benötigt werden. Die vorhandenen Workloads und Komponenten scheinen in Gebrauch zu sein, aber wenn neue Dienste oder Funktionen AWS veröffentlicht werden, können sie außer Betrieb genommen oder übernommen werden. Prüfen Sie die vorherigen Phasen der Workloads. Nachdem eine Workload in Betrieb genommen wurde, können frühere Umgebungen außer Betrieb genommen oder in ihrer Kapazität stark reduziert werden, bis sie wieder erforderlich sind.

Sie können Ressourcen mit einem Zeitrahmen oder einer Erinnerung versehen, um zu markieren, wann die Workload überprüft wurde. Wenn die Entwicklungsumgebung beispielsweise zuletzt vor Monaten überprüft wurde, könnte es ein guter Zeitpunkt sein, sie erneut zu überprüfen, um festzustellen, ob neue Services eingeführt werden können oder ob die Umgebung verwendet wird. Sie können Ihre Anwendungen gruppieren und mit einem [myApplications](#) Tag versehen AWS, um Metadaten wie Kritikalität, Umgebung, zuletzt überprüft und Kostenstelle zu verwalten und nachzuverfolgen. Sie können sowohl den Lebenszyklus Ihrer Workload verfolgen als auch die Kosten, den Zustand, den Sicherheitsstatus und die Leistung Ihrer Anwendungen überwachen und verwalten.

AWS bietet verschiedene Verwaltungs- und Governance-Dienste, die Sie für die Nachverfolgung des Lebenszyklus von Entitäten verwenden können. Sie können unseren [AWS Systems Manager](#) verwenden [AWS Config](#), um eine detaillierte Bestandsaufnahme Ihrer AWS Ressourcen und Konfiguration zu erstellen. Es wird empfohlen, dass Sie diese mit Ihren vorhandenen Projekt- bzw. Komponentenverwaltungssystemen integrieren, um aktive Projekte und Produkte in Ihrer Organisation zu verfolgen. Durch die Kombination Ihres aktuellen Systems mit den zahlreichen Ereignissen und Kennzahlen von AWS können Sie sich einen Überblick über wichtige Ereignisse im Lebenszyklus verschaffen und Ressourcen proaktiv verwalten, um unnötige Kosten zu reduzieren.

Ähnlich wie beim [Application Lifecycle Management \(ALM\)](#) sollten bei der Nachverfolgung des Projektlebenszyklus mehrere Prozesse, Tools und Teams zusammenarbeiten, z. B. Design und Entwicklung, Tests, Produktion, Support und Workload-Redundanz.

Durch die sorgfältige Überwachung jeder Phase des Lebenszyklus eines Projekts erhalten Organisationen entscheidende Einblicke und eine bessere Kontrolle, was die erfolgreiche Planung, Implementierung und den Abschluss von Projekten erleichtert. Mit dieser sorgfältigen Überwachung wird sichergestellt, dass die Projekte nicht nur den Qualitätsstandards entsprechen, sondern auch pünktlich und innerhalb des Budgets fertiggestellt werden, was die Kosteneffizienz insgesamt fördert.

Weitere Informationen zur Implementierung der Verfolgung des Lebenszyklus von Entitäten finden Sie im [Whitepaper zur Säule „Operative Exzellenz“ des AWS Well-Architected Framework](#).

### Implementierungsschritte

- Einrichtung eines Prozesses zur Überwachung des Projektlebenszyklus: Das [Team des Cloud-Kompetenzzentrums](#) hat die Aufgabe, einen Prozess für die Überwachung des Projektlebenszyklus einzurichten. Entwickeln Sie einen strukturierten und systematischen Ansatz zur Überwachung der Workloads, um die Kontrolle, die Sichtbarkeit und die Leistung der Projekte zu verbessern. Sorgen Sie dafür, dass der Überwachungsprozess transparent und kooperativ ist und sich auf kontinuierliche Verbesserungen konzentriert, um seine Effektivität und seinen Wert zu maximieren.
- Durchführen von Workload-Überprüfungen: Richten Sie, wie in Ihren Organisationsrichtlinien festgelegt, einen regelmäßigen Rhythmus ein, um Audits Ihrer bestehenden Projekte und Überprüfungen von Workloads durchzuführen. Der Aufwand für die Prüfung sollte proportional zum ungefähren Risiko, dem Wert oder den Kosten für die Organisation sein. Wichtige Bereiche, die in die Prüfung aufgenommen werden sollen, sind das Risiko eines Vorfalls oder eines Ausfalls, der Wert oder Beitrag für die Organisation (gemessen am Umsatz oder Ruf der Marke), die Kosten der Workload (gemessen als Gesamtkosten für Ressourcen und Betriebskosten) und die Nutzung der Workload (gemessen an der Anzahl der Ergebnisse der Organisation pro Zeiteinheit). Wenn sich diese Bereiche im Laufe des Lebenszyklus ändern, sind Anpassungen der Workload erforderlich, z. B. die vollständige oder teilweise Außerbetriebnahme.

### Ressourcen

#### Zugehörige Dokumente:

- [Leitfaden für das Markieren von AWS](#)
- [Was ist ALM \(Application Lifecycle Management\)?](#)

- [Von AWS verwaltete Richtlinien für Auftragsfunktionen](#)

Zugehörige Beispiele:

- [Steuern Sie den Zugriff AWS-Regionen mithilfe von IAM Richtlinien](#)

Zugehörige Tools

- [AWS Config](#)
- [AWS Systems Manager](#)
- [AWS Budgets](#)
- [AWS Organizations](#)
- [AWS CloudFormation](#)

### COST3. Wie überwachen Sie Ihre Kosten und die Nutzung?

Definieren Sie Richtlinien und Verfahren, um Ihre Kosten überwachen und richtig zuordnen zu können. So können Sie die Kosteneffizienz einer Workload messen und verbessern.

Bewährte Methoden

- [COST03-BP01 Detaillierte Informationsquellen konfigurieren](#)
- [COST03-BP02 Fügen Sie Organisationsinformationen zu Kosten und Nutzung hinzu](#)
- [COST03-BP03 Identifizieren Sie Kategorien für die Kostenzuweisung](#)
- [COST03-BP04 Organisationskennzahlen festlegen](#)
- [COST03-BP05 Tools für Abrechnung und Kostenmanagement konfigurieren](#)
- [COST03-BP06 Zuweisung von Kosten auf der Grundlage von Workload-Metriken](#)

#### COST03-BP01 Detaillierte Informationsquellen konfigurieren

Richten Sie Kostenmanagement- und Berichtstools ein, um die Analyse und Transparenz von Kosten- und Nutzungsdaten zu verbessern. Konfigurieren Sie Ihre Workload so, dass Protokolleinträge erstellt werden, die die Nachverfolgung und Segmentierung von Kosten und Nutzung erleichtern.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Hoch



## Implementierungsleitfaden

Detaillierte Abrechnungsinformationen, z. B. durch Aufschlüsselung nach Stunden in Kostenmanagement-Tools, ermöglichen es Organisationen, ihre Ressourcennutzung anhand weiterer Details zu verfolgen und einige der Gründe für den Kostenanstieg zu identifizieren. Diese Datenquellen bieten die genaueste Ansicht der Kosten und Nutzung in Ihrer gesamten Organisation.

Sie können AWS Data Exports verwenden, um Exporte von AWS Cost and Usage Report (CUR) 2.0 zu erstellen. Dies ist die neue und empfohlene Methode, um Ihre detaillierten Kosten- und Nutzungsdaten von zu erhalten AWS. Sie bietet detaillierte Angaben zur täglichen oder stündlichen Nutzung, Tarife, Kosten und Nutzungsattribute für alle kostenpflichtigen AWS Dienste (dieselben Informationen wie CUR) sowie einige Verbesserungen. Alle möglichen Dimensionen CUR wie Tagging, Standort, Ressourcenattribute und Konto sind enthalten. IDs

Es gibt drei Exporttypen, die auf der Art des Exports basieren, den Sie erstellen möchten: einen Standarddatenexport, einen Export in ein Kosten- und Nutzung-Dashboard mit QuickSight Amazon-Integration oder einen Legacy-Datenexport.

- Standarddatenexport: Ein benutzerdefinierter Export einer Tabelle, der regelmäßig an Amazon S3 gesendet wird.
- Kosten- und Nutzungs-Dashboard: Ein Export und eine Integration nach Amazon, QuickSight um ein vorgefertigtes Kosten- und Nutzungs-Dashboard bereitzustellen.
- Export älterer Daten: Ein Export der älteren Version AWS Cost and Usage Report (CUR).

Sie können Datenexporte mit den folgenden Anpassungen erstellen:

- Ressource einbeziehen IDs
- Daten zur Zuordnung geteilter Kosten
- Stundenaufschlüsselung
- Versionsverwaltung
- Komprimierungstyp und Dateiformat

Aktivieren Sie für Ihre Workloads, die Container auf Amazon ECS oder Amazon EKS ausführen, Daten zur geteilten Kostenzuweisung, sodass Sie Ihre Containerkosten einzelnen Geschäftseinheiten und Teams zuordnen können, je nachdem, wie Ihre Container-Workloads gemeinsam genutzte Rechen- und Speicherressourcen verbrauchen. Mit Daten zur geteilten Kostenzuweisung werden

Kosten- und Nutzungsdaten für neue Ressourcen auf Containerebene hinzugefügt. AWS Cost and Usage Report Daten zur geteilten Kostenzuweisung werden berechnet, indem die Kosten einzelner ECS Dienste und Aufgaben berechnet werden, die auf dem Cluster ausgeführt werden.

Ein Kosten- und Nutzungs-Dashboard exportiert die Kosten- und Nutzungs-Dashboard-Tabelle in regelmäßigen Abständen in einen S3-Bucket und stellt ein vorgefertigtes Kosten- und Nutzungs-Dashboard für Amazon bereit. QuickSight Verwenden Sie diese Option, wenn Sie schnell ein Dashboard mit Ihren Kosten- und Nutzungsdaten bereitstellen möchten. Mit dieser Option sind keine Anpassungen möglich.

Falls gewünscht, können Sie weiterhin CUR im Legacy-Modus exportieren, wo Sie andere Verarbeitungsdienste integrieren können, z. B. [AWS Glue](#) um die Daten für die Analyse vorzubereiten und Datenanalysen mit [Amazon Athena](#) durchzuführen, SQL um die Daten abzufragen.

### Implementierungsschritte

- Datenexporte erstellen: Erstellen Sie benutzerdefinierte Exporte mit den gewünschten Daten und steuern Sie Ihr Exportschema. Erstellen Sie mit Basic SQL Exports von Abrechnungs- und Kostenmanagementdaten und visualisieren Sie Ihre Abrechnungs- und Kostenmanagementdaten durch die Integration mit Amazon QuickSight. Sie können Ihre Daten auch im Standardmodus exportieren, um Ihre Daten mit anderen Verarbeitungstools wie Amazon Athena zu analysieren.
- Konfiguration des Kosten- und Nutzungsberichts: Konfigurieren Sie über die Fakturierungskonsole mindestens einen Kosten- und Nutzungsbericht. Konfigurieren Sie einen Bericht mit stündlicher Granularität, der alle Kennungen und Ressourcen enthält. IDs Sie können auch andere Berichte mit unterschiedlichen Granularitäten erstellen, um zusammenfassende Informationen bereitzustellen.
- Konfiguration der stündlichen Granularität in Cost Explorer: Aktivieren Sie in der Fakturierungskonsole Daten auf Stundenbasis und auf Ressourcenebene, um auf Kosten- und Nutzungsdaten der letzten 14 Tage mit stündlicher Granularität zuzugreifen.
- Konfiguration der Anwendungsprotokollierung: Überprüfen Sie, dass Ihre Anwendung jedes Geschäftsergebnis protokolliert, das sie liefert, sodass es nachverfolgt und gemessen werden kann. Stellen Sie sicher, dass die Granularität dieser Daten mindestens stündlich ist, damit sie mit der Aufschlüsselung der Kosten- und Nutzungsdaten übereinstimmt. Weitere Informationen zur Protokollierung und Überwachung finden Sie unter der [Well-Architected-Säule „Operative Exzellenz“](#).

### Ressourcen

#### Zugehörige Dokumente:

- [AWS Data Exports](#)
- [AWS Glue](#)
- [Amazon QuickSight](#)
- [Preisberechnung des AWS -Kostenmanagements](#)
- [Taggen von AWS -Ressourcen](#)
- [Analysieren der Kosten mit Cost Explorer](#)
- [Verwalten von AWS Cost and Usage Report en](#)
- [Well-Architected-Säule „Operative Exzellenz“](#)

Zugehörige Beispiele:

- [AWS Account Setup](#)
- [Datenexporte für AWS Billing and Cost Management](#)
- [AWS Cost Explorer Häufige Anwendungsfälle](#)

COST03-BP02 Fügen Sie Organisationsinformationen zu Kosten und Nutzung hinzu

Definieren Sie ein auf Ihrer Organisation basierendes Markierungsschema, Workload-Attribute und Kostenzuordnungskategorien, damit Sie nach Ressourcen filtern und suchen oder die Kosten und Nutzung in Kostenverwaltungstools überwachen können. Implementieren Sie ein einheitliches Markieren aller Ressourcen, wenn möglich nach Zweck, Team, Umgebung oder anderen für Ihr Unternehmen relevanten Kriterien.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Mittel

Implementierungsleitfaden

Implementieren Sie das [Taggen in AWS AWS](#), um Organisationsinformationen zu Ihren Ressourcen hinzuzufügen, die dann zu Ihren Kosten- und Nutzungsinformationen hinzugefügt werden. Ein Tag ist ein Schlüssel-Wert-Paar – der Schlüssel ist definiert und muss innerhalb Ihrer Organisation eindeutig sein und der Wert ist für eine Gruppe von Ressourcen eindeutig. Ein Beispiel für ein Schlüssel-Wert-Paar ist der Schlüssel `Environment` mit dem Wert `Production`. Alle Ressourcen in der Produktionsumgebung verfügen über dieses Schlüssel-Wert-Paar. Mit Tags können Sie Ihre Kosten mit aussagekräftigen, relevanten Organisationsinformationen kategorisieren und nachverfolgen. Sie können Tags anwenden, die Organisationskategorien (z. B. Kostenstellen, Anwendungsnamen,

Projekte oder Besitzer) darstellen und Workloads und Merkmale von Workloads (z. B. Test oder Produktion) identifizieren, um Ihre Kosten und Nutzung in Ihrer gesamten Organisation zuzuordnen.

Wenn Sie Tags auf Ihre AWS Ressourcen (wie Amazon Elastic Compute Cloud Instances oder Amazon Simple Storage Service Buckets) anwenden und die Tags aktivieren, werden diese Informationen zu Ihren Kosten- und Nutzungsberichten AWS hinzugefügt. Sie können Berichte ausführen und Analysen für markierte und nicht markierte Ressourcen durchführen, um eine größere Compliance mit internen Kostenverwaltungsrichtlinien zu ermöglichen und eine genaue Zuordnung zu gewährleisten.

Durch die Erstellung und Implementierung eines AWS Tagging-Standards für alle Konten Ihres Unternehmens können Sie Ihre AWS Umgebungen konsistent und einheitlich verwalten und steuern. Verwenden Sie [Tag-Richtlinien](#) in AWS Organizations, um Regeln dafür zu definieren, wie Tags für AWS Ressourcen in Ihren Konten verwendet werden können. AWS Organizations Mit Tag-Richtlinien können Sie auf einfache Weise einen standardisierten Ansatz für die Kennzeichnung von Ressourcen AWS anwenden

AWS Mit [dem Tag-Editor](#) können Sie Tags mehrerer Ressourcen hinzufügen, löschen und verwalten. Mit Tag Editor können Sie nach den Ressourcen suchen, die Sie mit Tags markieren möchten, und dann die Tags für die Ressourcen in Ihren Suchergebnissen verwalten.

AWS Mithilfe von [Cost Categories](#) können Sie Ihren Kosten eine organisatorische Bedeutung zuweisen, ohne dass Ressourcen mit Tags versehen werden müssen. Sie können Ihre Kosten- und Nutzungsinformationen eindeutigen internen Organisationsstrukturen zuordnen. Sie definieren Kategorieregeln, um Kosten mithilfe von Fakturierungsdimensionen wie Konten und Tags zuzuordnen und zu kategorisieren. Dies bietet zusätzlich zum Tagging eine weitere Ebene der Verwaltungsfunktionen. Sie können auch bestimmte Konten und Tags mehreren Projekten zuordnen.

## Implementierungsschritte

- Definieren eines Tagging-Schemas: Versammeln Sie alle Beteiligten aus Ihrem gesamten Unternehmen, um ein Schema zu definieren. Dies umfasst in der Regel Mitarbeiter in technischen, finanziellen und leitenden Funktionen. Definieren Sie eine Liste der Tags, die alle Ressourcen haben müssen, sowie eine Liste der Tags, die Ressourcen haben sollten. Stellen Sie sicher, dass die Tag-Namen und -Werte in Ihrer Organisation konsistent sind.
- Taggen von Ressourcen: Platzieren Sie mithilfe Ihrer definierten Kostenzuordnungskategorien [Tags](#) für alle Ressourcen in Ihren Workloads entsprechend den Kategorien. Verwenden Sie Tools wie den CLI Tag-Editor oder, um die Effizienz AWS Systems Manager zu steigern.

- Implementieren von AWS Cost Categories: Sie können [Cost Categories](#) erstellen, ohne Tagging zu implementieren. Kostenkategorien verwenden die vorhandenen Kosten- und Nutzungsdimensionen. Erstellen Sie Kategorieregeln aus Ihrem Schema und implementieren Sie diese in Kostenkategorien.
- Automatisiertes Tagging: Automatisieren Sie das Tagging, um sicherzustellen, dass Sie ein hohes Maß an Tagging für alle Ressourcen aufrechterhalten, damit Ressourcen automatisch bei ihrer Erstellung getaggt werden. Nutzen Sie Services wie [AWS CloudFormation](#), um zu überprüfen, ob die Ressourcen bei der Erstellung mit Tags versehen wurden. Sie können auch eine benutzerdefinierte Lösung für das automatische Taggen mithilfe von Lambda-Funktionen erstellen oder einen Microservice verwenden, der die Workload regelmäßig überprüft und alle nicht getaggten Ressourcen entfernt, was ideal für Test- und Entwicklungsumgebungen ist.
- Überwachung von und Berichterstellung zu Tags: Um sicherzustellen, dass Sie in Ihrer Organisation ein hohes Maß an Tagging aufrechterhalten, melden und überwachen Sie die Tags in Ihren Workloads. Sie können [AWS Cost Explorer](#) verwenden, um die Kosten für getaggte und nicht getaggte Ressourcen anzuzeigen. Alternativ können Sie auch Services wie [Tag Editor](#) verwenden. Überprüfen Sie regelmäßig die Anzahl der nicht getaggten Ressourcen und ergreifen Sie Maßnahmen, um Tags hinzuzufügen, bis Sie die gewünschte Tagging-Stufe erreichen.

## Ressourcen

### Zugehörige Dokumente:

- [Tagging Best Practices](#)
- [AWS CloudFormation Ressourcen-Tag](#)
- [AWS Cost Categories](#)
- [Ressourcen taggen AWS](#)
- [Analysieren Sie Ihre Kosten mit Budgets AWS](#)
- [Analysieren der Kosten mit Cost Explorer](#)
- [Verwalten von AWS -Kosten- und -Nutzungsberichten](#)

### Zugehörige Videos:

- [Wie kann ich meine AWS Ressourcen taggen, um meine Rechnung nach Kostenstellen oder Projekten aufzuteilen](#)
- [Ressourcen taggen AWS](#)

## COST03-BP03 Identifizieren Sie Kategorien für die Kostenzuweisung

Identifizieren Sie Organisationskategorien wie Geschäftsbereiche, Abteilungen oder Projekte, anhand derer die Kosten innerhalb Ihres Unternehmens den internen Verbrauchern zugewiesen werden können. Verwenden Sie diese Kategorien, um ein Gefühl der Verantwortung für Ausgaben zu fördern, Bewusstsein für Kosten zu schaffen und ein effektives Nutzungsverhalten zu unterstützen.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Hoch

### Implementierungsleitfaden

Der Prozess der Kostenkategorisierung ist für Budgetierung, Buchhaltung, Finanzberichterstattung, Entscheidungsfindung, Benchmarking und Projektmanagement von entscheidender Bedeutung. Durch die Klassifizierung und Kategorisierung von Ausgaben können Teams die Arten von Kosten besser nachvollziehen, die auf dem Weg in die Cloud entstehen werden. So können sie fundierte Entscheidungen treffen und Budgets effektiv verwalten.

Die Rechenschaftspflicht bei den Cloud-Ausgaben ist ein starker Anreiz für ein diszipliniertes Nachfrage- und Kostenmanagement. Das Ergebnis sind deutlich höhere Cloud-Kosteneinsparungen für Unternehmen, die den größten Teil ihrer Cloud-Ausgaben für verbrauchende Geschäftsbereiche oder Teams aufwenden. Darüber hinaus hilft die Zuweisung von Cloud-Ausgaben Unternehmen dabei, mehr bewährte Methoden für die zentralisierte Cloud-Governance einzuführen.

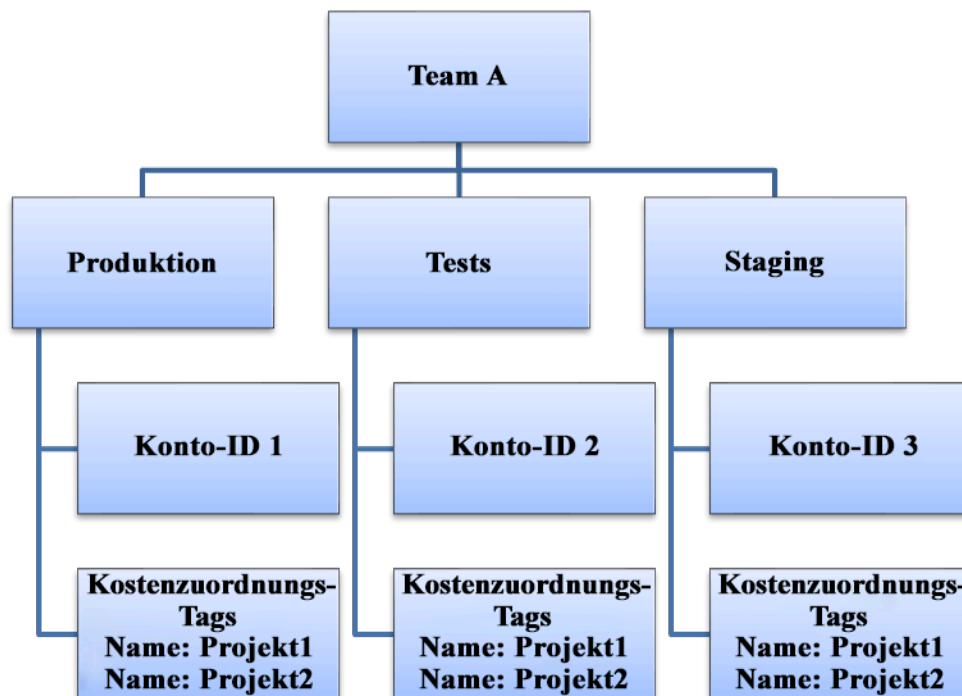
Arbeiten Sie in regelmäßigen Besprechungen mit Ihrem Finanzteam und anderen relevanten Stakeholdern zusammen, um zu verstehen, wie die Kosten innerhalb Ihres Unternehmens zugeordnet werden müssen. Workload-Kosten müssen über den gesamten Lebenszyklus hinweg zugeordnet werden, einschließlich Entwicklung, Tests, Produktion und Außerbetriebnahme. Analysieren Sie, welche Kosten durch Schulungen, Personalentwicklung und Ideenentwicklung im Unternehmen entstehen. Dies kann hilfreich sein, um Konten, die zu diesem Zweck verwendet werden, korrekt den Schulungs- und Entwicklungsbudgets zuzuordnen, anstatt allgemeinen IT-Kostenbudgets.

Nachdem Sie Ihre Kostenzuordnungskategorien mit den Beteiligten in Ihrer Organisation definiert haben, verwenden Sie [AWS Cost Categories](#), um Ihre Kosten- und Nutzungsinformationen in aussagekräftige Kategorien zu gruppieren AWS Cloud, z. B. Kosten für ein bestimmtes Projekt oder AWS-Konten für Abteilungen oder Geschäftsbereiche. Sie können benutzerdefinierte Kategorien erstellen und Ihre Kosten- und Nutzungsinformationen diesen Kategorien zuordnen, und zwar basierend auf Regeln, die Sie anhand verschiedener Dimensionen wie Konto, Tag, Service, oder Kostenart definieren. Sobald die Kostenkategorien eingerichtet sind, können Sie Ihre Kosten- und

Nutzungsinformationen nach diesen Kategorien aufgeschlüsselt anzeigen, sodass Ihr Unternehmen bessere Strategie- und Kaufentscheidungen treffen kann. Diese Kategorien sind auch in AWS Cost Explorer AWS Budgets, und AWS Cost and Usage Report sichtbar.

Erstellen Sie beispielsweise Kostenkategorien für Ihre Geschäftsbereiche (DevOps Team) und erstellen Sie unter jeder Kategorie mehrere Regeln (Regeln für jede Unterkategorie) mit mehreren Dimensionen (AWS-Konten, Kostenzuordnungskennzeichen, Dienstleistungen oder Gebührenart), die auf Ihren definierten Gruppierungen basieren. Sie können mit Cost Categories Ihre Kosten mithilfe einer regelbasierten Engine organisieren. Die von Ihnen konfigurierten Regeln unterteilen Ihre Kosten in Kategorien. Innerhalb dieser Regeln können Sie filtern, indem Sie für jede Kategorie mehrere Dimensionen verwenden, z. B. spezifische AWS-Konten, AWS Dienstleistungen oder Gebührenarten. Sie können diese Kategorien dann für mehrere Produkte in der [Konsole](#) von [AWS Billing and Cost Management and Cost Management](#) verwenden. Dazu gehören AWS Cost Explorer AWS Budgets, AWS Cost and Usage Report, und AWS Cost Anomaly Detection.

Das folgende Diagramm zeigt Ihnen beispielsweise, wie Ihre Kosten- und Nutzungsinformationen in Ihrem Unternehmen gruppiert werden können, z. B. mit mehreren Teams (Kostenkategorie) und mehreren Umgebungen (Regeln), wobei jede Umgebung mehrere Ressourcen oder Assets (Dimensionen) aufweist.



Organigramm für Kosten und Nutzung

Sie können mithilfe von Kostenkategorien auch Kostengruppierungen erstellen. Nachdem Sie die Kostenkategorien erstellt haben (es kann nach dem Erstellen einer Kostenkategorie bis zu 24 Stunden dauern, bis die Werte in Ihren Nutzungsdatensätzen aktualisiert sind), erscheinen sie in [AWS Cost Explorer](#), [AWS Budgets](#), [AWS Cost and Usage Report](#) und [AWS Cost Anomaly Detection](#). In AWS Cost Explorer und AWS Budgets wird eine Kostenkategorie als zusätzliche Fakturierungsdimension angezeigt. Damit können Sie Daten nach dem bestimmten Cost Category-Wert filtern oder nach Cost Category gruppieren.

## Implementierungsschritte

- **Definieren der Organisationskategorien:** Treffen Sie sich mit internen Stakeholdern und Vertretern aus verschiedenen Unternehmensbereichen, um Kategorien zu definieren, die die Struktur und Anforderungen Ihrer Organisation widerspiegeln. Diese werden direkt der Struktur vorhandener Finanzkategorien zugeordnet, z. B. Geschäftsbereich, Budget, Kostenstelle oder Abteilung. Sehen Sie sich die Ergebnisse an, die die Cloud für Ihr Unternehmen liefert, z. B. Schulungen oder Fortbildungen, da es sich auch um Organisationskategorien handelt.
- **Definieren der funktionalen Kategorien:** Treffen Sie sich mit internen Stakeholdern und Vertretern aus verschiedenen Unternehmensbereichen, um Kategorien zu definieren, die die Funktionen in Ihrer Organisation widerspiegeln. Dabei kann es sich um den Workload- oder Anwendungsnamen und die Art der Umgebung handeln, z. B. Produktion, Test oder Entwicklung.
- **Definieren Sie AWS Cost Categories:** Erstellen Sie Cost Categories, um Ihre Kosten- und Nutzungsinformationen mithilfe von [AWS Kostenkategorien](#) zu organisieren und Ihre AWS Kosten und Nutzung [aussagekräftigen Kategorien zuzuordnen](#). Einer Ressource können mehrere Kategorien zugewiesen werden und eine Ressource kann sich in mehreren verschiedenen Kategorien befinden. Definieren Sie daher so viele Kategorien wie nötig, um Ihre Kosten innerhalb der kategorisierten Struktur mithilfe von AWS Cost Categories zu [verwalten](#).

## Ressourcen

### Zugehörige Dokumente:

- [Taggen von AWS -Ressourcen](#)
- [Verwendung von Kostenzuordnungs-Tags](#)
- [Analysieren Sie Ihre Kosten mit AWS Budgets](#)
- [Analysieren der Kosten mit Cost Explorer](#)
- [Verwalten von AWS Cost and Usage Report](#)



- [AWS Cost Categories](#)
- [Verwaltung Ihrer AWS Kosten mit Cost Categories](#)
- Erstellen von Cost Categories
- Markieren von Cost Categories
- Aufteilen von Gebühren innerhalb von Cost Categories
- [AWS -Features für Kostenkategorien](#)

Zugehörige Beispiele:

- [Organisieren Sie Ihre Kosten- und Nutzungsdaten mit AWS Cost Categories](#)
- [Verwaltung Ihrer AWS Kosten mit Cost Categories](#)
- [Well-Architected Labs: Cost and Usage Visualization](#)
- [Well-Architected Labs: Cost Categories](#)

#### COST03-BP04 Organisationskennzahlen festlegen

Definieren Sie die Organisationsmetriken, die für diese Workload erforderlich sind. Beispiele für Metriken einer Workload sind erstellte Kundenberichte oder Webseiten, die den Kunden angezeigt werden.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Hoch

#### Implementierungsleitfaden

Entwickeln Sie ein Verständnis dafür, wie die Ausgabe Ihrer Workload im Vergleich zum Geschäftserfolg gemessen wird. Jede Workload verfügt in der Regel über einen kleinen Satz von Hauptausgaben, die auf die Leistung hinweisen. Wenn Sie eine komplexe Workload mit vielen Komponenten haben, können Sie die Liste priorisieren oder Metriken für jede Komponente definieren und nachverfolgen. Arbeiten Sie mit Ihren Teams zusammen, um zu verstehen, welche Metriken verwendet werden sollen. Diese Einheit wird verwendet, um die Effizienz der Workload oder die Kosten für die einzelnen Geschäftsausgaben zu verstehen.

#### Implementierungsschritte

- Definieren von Workload-Ergebnissen: Treffen Sie sich mit den Beteiligten im Unternehmen und definieren Sie die Ergebnisse für die Workload. Hierbei handelt es sich um eine primäre

Maßnahme für die Kundennutzung. Es müssen Geschäftsmetriken und keine technischen Metriken gemessen werden. Es sollte eine kleine Anzahl von allgemeinen Metriken (weniger als fünf) pro Workload geben. Wenn die Workload mehrere Ergebnisse für verschiedene Anwendungsfälle erzeugt, gruppieren Sie sie in einer einzigen Metrik.

- Definieren der Ergebnisse von Workload-Komponenten: Wenn Sie eine große und komplexe Workload haben oder Ihre Workload problemlos in Komponenten (z. B. Microservices) mit gut definierten Ein- und Ausgaben aufteilen können, definieren Sie optional Metriken für jede Komponente. Der Aufwand sollte den Wert und die Kosten der Komponente widerspiegeln. Beginnen Sie mit den größten Komponenten und arbeiten Sie sich zu den kleineren Komponenten vor.

## Ressourcen

### Zugehörige Dokumente:

- [Ressourcen taggen AWS](#)
- [Analysieren Sie Ihre Kosten mit Budgets AWS](#)
- [Analysieren der Kosten mit Cost Explorer](#)
- [Verwalten von AWS -Kosten- und -Nutzungsberichten](#)

## COST03-BP05 Tools für Abrechnung und Kostenmanagement konfigurieren

Konfigurieren Sie Kostenverwaltungstools in Übereinstimmung mit den Richtlinien Ihrer Organisation, um die Cloud-Ausgaben zu verwalten und zu optimieren. Dazu gehören Services, Tools und Ressourcen zur Organisation und Nachverfolgung von Kosten- und Nutzungsdaten, zur Verbesserung der Kontrolle durch konsolidierte Fakturierung und Zugriffsberechtigungen, zur Verbesserung der Planung durch Budgetierung und Prognosen, zum Erhalt von Benachrichtigungen oder Warnmeldungen und zur Kostensenkung durch Ressourcen- und Preisoptimierungen.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Hoch

## Implementierungsleitfaden

Um eine starke Rechenschaftspflicht zu gewährleisten, erörtern Sie im Rahmen Ihrer Kostenzuordnungsstrategie zunächst Ihre Kontostrategie. Wenn Sie das richtig machen, reicht das möglicherweise schon aus. Andernfalls fehlen wichtige Informationen und es kann zu weiteren Problemen kommen.

Um die Rechenschaftspflicht für Cloud-Ausgaben zu fördern, gewähren Sie Benutzern Zugriff auf Tools, die einen Überblick über ihre Kosten und Nutzung bieten. AWS empfiehlt, dass Sie alle Workloads und Teams für die folgenden Zwecke konfigurieren:

- **Organisation:** Legen Sie Ihre Basis für die Kostenzuordnung und Governance mit Ihrer eigenen Tagging-Strategie und -Taxonomie fest. Erstellen Sie mehrere AWS Konten mit Tools wie AWS Control Tower oder AWS Organization. Kennzeichnen Sie die unterstützten AWS Ressourcen und kategorisieren Sie sie anhand Ihrer Organisationsstruktur (Geschäftsbereiche, Abteilungen oder Projekte) sinnvoll. Kennzeichnen Sie Kontonamen für bestimmte Kostenstellen und ordnen Sie sie AWS Cost Categories zu, um Konten für Geschäftseinheiten ihren Kostenstellen zuzuordnen, sodass der Eigentümer der Geschäftseinheit den Verbrauch mehrerer Konten an einem Ort sehen kann.
- **Zugriff:** Verfolgen Sie organisationsweite Fakturierungsinformationen durch konsolidierte Abrechnungen nach. Stellen Sie sicher, dass die richtigen Stakeholder und Geschäftsinhaber Zugriff darauf haben.
- **Kontrolle:** Richten Sie effektive Governance-Mechanismen mit den richtigen Leitplanken ein, um unerwartete Szenarien bei der Verwendung von Service Control Policies (SCP), Tag-Richtlinien, IAM Richtlinien und Budgetwarnungen zu verhindern. Beispielsweise können Sie Teams erlauben, bestimmte Ressourcen nur in bevorzugten Regionen zu erstellen, indem Sie effektive Kontrollmechanismen verwenden und verhindern, dass Ressourcen ohne bestimmte Tags (z. B. Kostenstelle) erstellt werden.
- **Aktueller Status:** Konfigurieren Sie ein Dashboard mit aktuellen Kosten- und Nutzungsraten. Das Dashboard sollte an einem gut sichtbaren Ort innerhalb der Arbeitsumgebung verfügbar sein (wie bei einem Betriebs-Dashboard). Sie können Daten exportieren und für eine gute Sichtbarkeit das Kosten- und Nutzungs-Dashboard aus dem AWS Cost Optimization Hub oder einem beliebigen unterstützten Produkt verwenden. Möglicherweise müssen Sie verschiedene Dashboards für verschiedene Personengruppen erstellen. Beispielsweise kann sich das Manager-Dashboard von einem Engineering-Dashboard unterscheiden.
- **Benachrichtigungen:** Mithilfe von AWS Budgets oder der Erkennung von Kostenanomalien können Sie Benachrichtigungen senden, wenn Kosten oder Nutzung definierte Grenzwerte überschreiten und Anomalien auftreten. AWS
- **Berichte:** Fassen Sie alle Kosten- und Nutzungsinformationen zusammen. Erhöhen Sie das Bewusstsein und die Verantwortlichkeit für Ihre Cloud-Ausgaben mit detaillierten, zuordnungsfähigen Kostendaten. Erstellen Sie Berichte, die für das Team, das sie bearbeitet, relevant sind und Empfehlungen enthalten.

- Nachverfolgung: Zeigen Sie die aktuellen Kosten und Nutzung in Bezug zu konfigurierten Zielen oder Vorgaben an.
- Analyse: Ermöglichen Sie Teammitgliedern die Durchführung benutzerdefinierter und detaillierter Analysen mit stündlicher, täglicher oder monatlicher Granularität und verschiedenen Filtern (Ressource, Konto, Tag usw.).
- Prüfung: Bleiben Sie hinsichtlich Ihrer Ressourcenbereitstellung und Ihrer Möglichkeiten zur Kostenoptimierung auf dem Laufenden. Erhalten Sie Benachrichtigungen über Amazon CloudWatchSNS, Amazon oder Amazon SES für Ressourcenbereitstellungen auf Organisationsebene. Überprüfen Sie die Empfehlungen zur Kostenoptimierung mit AWS Trusted Advisor oder AWS Compute Optimizer.
- Trendberichte: Zeigen Sie die Variabilität von Kosten und Nutzung über den erforderlichen Zeitraum mit der erforderlichen Aufschlüsselung an.
- Prognosen: Zeigen Sie geschätzte zukünftige Kosten und schätzen Sie Ihre Ressourcennutzung und Ihre Ausgaben mit von Ihnen erstellten Prognose-Dashboards.

Sie können [AWS Cost Optimization Hub](#) verwenden, um potenzielle Kostenoptimierungsmöglichkeiten zu ermitteln, die von einem zentralen Standort aus konsolidiert werden, und Datenexporte für die Integration mit Amazon Athena erstellen. Sie können den AWS Cost Optimization Hub auch verwenden, um das Cost and Usage Dashboard bereitzustellen, das Amazon QuickSight für interaktive Kostenanalysen und den sicheren Austausch von Kosteninformationen verwendet.

Wenn Sie in Ihrer Organisation nicht über grundlegende Fähigkeiten oder Kapazitäten verfügen, können Sie mit [AWS ProServ](#), [AWS Managed Services \(AMS\)](#) oder [AWS Partnern](#) zusammenarbeiten. Sie können auch Tools von Drittanbietern verwenden. Stellen Sie jedoch sicher, dass Sie das Wertversprechen validieren.

### Implementierungsschritte

- Teambasierten Zugriff auf Tools ermöglichen: Konfigurieren Sie Ihre Konten und erstellen Sie Gruppen, die Zugriff auf die erforderlichen Kosten- und Nutzungsberichte für ihre Verbräuche haben, und verwenden Sie [AWS Identity and Access Management](#), um den Zugriff auf die Tools wie AWS Cost Explorer zu [kontrollieren](#). Diese Gruppen müssen Vertreter aller Teams umfassen, die für eine Anwendung zuständig sind oder diese verwalten. Auf diese Weise wird sichergestellt, dass jedes Team Zugriff auf seine Kosten- und Nutzungsinformationen hat, um seinen Verbrauch nachzuverfolgen.

- Organisieren von Kosten-Tags und -Kategorien: Organisieren Sie Ihre Kosten nach Teams, Geschäftseinheiten, Anwendungen, Umgebungen und Projekten. Verwenden Sie Ressourcen-Tags, um Kosten nach Kostenzuordnungs-Tags zu organisieren. Erstellen Sie Kostenkategorien auf der Grundlage der Dimensionen, indem Sie anhand von Tags, Konten, Diensten usw. Ihre Kosten abbilden.
- AWS Budgets konfigurieren: [Konfigurieren Sie AWS Budgets](#) für alle Konten für Ihre Workloads. Legen Sie mithilfe von Tags und Kostenkategorien Budgets für die Gesamtkontoausgaben und Budgets für die Workloads fest. Konfigurieren Sie Benachrichtigungen in AWS Budgets, sodass Sie Benachrichtigungen erhalten, wenn Sie Ihre budgetierten Beträge überschreiten oder wenn Ihre geschätzten Kosten Ihre Budgets überschreiten.
- Konfigurieren Sie die Erkennung von AWS Kostenanomalien: Verwenden Sie die [Erkennung von AWS Kostenanomalien](#) für Ihre Konten, Kerndienste oder Kostenkategorien, die Sie erstellt haben, um Ihre Kosten und Nutzung zu überwachen und ungewöhnliche Ausgaben zu erkennen. Sie können Benachrichtigungen einzeln in aggregierten Berichten und Benachrichtigungen in einer E-Mail oder einem SNS Amazon-Thema erhalten, sodass Sie die Ursache der Anomalie analysieren und ermitteln und den Faktor identifizieren können, der den Kostenanstieg verursacht.
- Verwenden von Kostenanalysetools: Konfigurieren Sie [AWS Cost Explorer](#) für Ihre Workload und Ihre Konten, um Ihre Kostendaten für die weitere Analyse zu visualisieren. Erstellen Sie ein Dashboard für die Workload, das die Gesamtausgaben, die wichtigsten Nutzungskennzahlen für die Workload und die Prognose künftiger Kosten auf der Grundlage Ihrer historischen Kostendaten nachverfolgt.
- Verwenden Sie kostensparende Analysetools: Verwenden Sie AWS Cost Optimization Hub, um Einsparmöglichkeiten mit maßgeschneiderten Empfehlungen zu identifizieren, darunter das Löschen ungenutzter Ressourcen, die richtige Dimensionierung, Sparpläne, Reservierungen und Empfehlungen für den Computeroptimierer.
- Konfigurieren von erweiterten Tools: Sie können optional Grafiken erstellen, um die interaktive Analyse und den Austausch von Kosteninformationen zu erleichtern. Mit Data Exports auf AWS Cost Optimization Hub können Sie ein von Amazon betriebenes Kosten- und Nutzungs-Dashboard QuickSight für Ihr Unternehmen erstellen, das zusätzliche Details und Detailgenauigkeit bietet. [Sie können auch erweiterte Analysefunktionen implementieren, indem Sie Datenexporte in Amazon Athena für erweiterte Abfragen verwenden und Dashboards auf Amazon erstellen. QuickSight](#) Arbeiten Sie mit [AWS -Partnern](#) zusammen, um Cloud-Management-Lösungen für die konsolidierte Überwachung und Optimierung von Cloud-Rechnungen einzuführen.

## Ressourcen

### Zugehörige Dokumente:

- [Was ist AWS Billing and Cost Management Kostenmanagement?](#)
- [Etablierung Ihrer AWS Best-Practice-Umgebung](#)
- [Bewährte Methoden für das Taggen von Ressourcen AWS](#)
- [Verschlagworten Sie Ihre Ressourcen AWS](#)
- [AWS Cost Categories](#)
- [Analysieren Sie Ihre Kosten mit Budgets AWS](#)
- [Analysieren Sie Ihre Kosten mit AWS Cost Explorer](#)
- [Was sind AWS Datenexporte?](#)

### Zugehörige Videos:

- [Deploying Cloud Intelligence Dashboards](#)
- [Erhalten Sie Benachrichtigungen zu beliebigen Kennzahlen FinOps oder Kennzahlen zur Kostenoptimierung oder KPI](#)

### Zugehörige Beispiele:

- [Kosten- und Nutzungs-Dashboard bereitgestellt](#) von Amazon QuickSight
- [AWS Cost and Usage Governance Workshop](#)

## COST03-BP06 Zuweisung von Kosten auf der Grundlage von Workload-Metriken

Teilen Sie die Kosten der betreffenden Workload anhand von Nutzungsmetriken oder Geschäftsergebnissen zu, um die Kosteneffizienz der Workload zu bewerten. Implementieren Sie einen Prozess zur Analyse der Kosten- und Nutzungsdaten mithilfe von Analytikservices, um von genaueren Einblicken und Rückbelastungsmöglichkeiten zu profitieren.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Niedrig

### Implementierungsleitfaden

Die Kostenoptimierung ermöglicht Geschäftsergebnisse zum niedrigsten Preis, was nur durch Zuweisung von Workload-Kosten nach Workload-Metriken (gemessen nach Workload-Effizienz)

erreicht werden kann. Überwachen Sie die definierten Workload-Metriken durch Protokolldateien oder andere Anwendungsüberwachung. Kombinieren Sie diese Daten mit den Workload-Kosten, die Sie erhalten können, indem Sie Kosten mit einem bestimmten Tag-Wert oder einer Konto-ID betrachten. Führen Sie diese Analyse stündlich durch. Ihre Effizienz ändert sich in der Regel, wenn Sie statische Kostenkomponenten haben (z. B. eine Backend-Datenbank, die dauerhaft ausgeführt wird) mit einer variierenden Anfragerate (z. B. Nutzungsspitzen von 9 bis 17 Uhr, mit wenigen Anfragen in der Nacht). Wenn Sie die Beziehung zwischen den statischen und variablen Kosten verstehen, können Sie Ihre Optimierungsaktivitäten besser fokussieren.

Die Erstellung von Workload-Metriken für gemeinsam genutzte Ressourcen kann im Vergleich zu Ressourcen wie containerisierten Anwendungen auf Amazon Elastic Container Service (Amazon ECS) und Amazon API Gateway eine Herausforderung sein. Es gibt jedoch bestimmte Möglichkeiten, die Nutzung zu kategorisieren und die Kosten zu verfolgen. Wenn Sie Amazon ECS und AWS Batch gemeinsam genutzte Ressourcen nachverfolgen müssen, können Sie Daten zur geteilten Kostenzuweisung in aktivieren AWS Cost Explorer. Mithilfe von Daten zur Aufteilung der Kosten können Sie die Kosten und die Nutzung Ihrer containerisierten Anwendungen nachvollziehen und optimieren und die Anwendungskosten auf Grundlage des Verbrauchs der gemeinsam genutzten Rechen- und Speicherressourcen einzelnen Geschäftsbereichen zuteilen.

### Implementierungsschritte

- Zuteilen von Kosten an Workload-Metriken: Erstellen Sie mit den definierten Metriken und konfigurierten Tags eine Metrik, die die Workload-Ausgabe und die Workload-Kosten kombiniert. Verwenden Sie Analysedienste wie Amazon Athena und Amazon, QuickSight um ein Effizienz-Dashboard für die gesamte Arbeitslast und alle Komponenten zu erstellen.

### Ressourcen

#### Zugehörige Dokumente:

- [Ressourcen taggen AWS](#)
- [Analysieren Sie Ihre Kosten mit Budgets AWS](#)
- [Analysieren der Kosten mit Cost Explorer](#)
- [Verwalten von AWS -Kosten- und -Nutzungsberichten](#)

#### Zugehörige Beispiele:

- [Verbessern Sie die Kostentransparenz von Amazon ECS und AWS Batch mit AWS Split Cost Allocation Data](#)

## COST4. Wie können Sie Ressourcen außer Betrieb nehmen?

Implementieren Sie Änderungskontrolle und Ressourcenmanagement von Projektbeginn bis end-of-life. So stellen Sie sicher, dass Sie ungenutzte Ressourcen abschalten oder beenden, um Verschwendung zu vermeiden.

### Bewährte Methoden

- [COST04-BP01 Ressourcen im Laufe ihrer Lebensdauer verfolgen](#)
- [COST04-BP02 Implementieren Sie einen Stilllegungsprozess](#)
- [COST04-BP03 Außerdienstliche Ressourcen](#)
- [COST04-BP04 Automatische Außerbetriebnahme von Ressourcen](#)
- [COST04-BP05 Richtlinien zur Datenspeicherung durchsetzen](#)

### COST04-BP01 Ressourcen im Laufe ihrer Lebensdauer verfolgen

Definieren und implementieren Sie eine Methode zur Verfolgung von Ressourcen und deren Verknüpfungen mit Systemen über ihre gesamte Lebensdauer hinweg. Mit entsprechenden Tags können Sie die Workload oder die Funktion der Ressource identifizieren.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Hoch

### Implementierungsleitfaden

Nicht mehr benötigte Workload-Ressourcen werden außer Betrieb genommen. Ein gängiges Beispiel sind Ressourcen, die zum Testen verwendet werden. Nach Abschluss des Tests können die Ressourcen entfernt werden. Das Nachverfolgen von Ressourcen mit Tags (und Ausführen von Berichten zu diesen Tags) kann Ihnen helfen, Komponenten zu identifizieren, die außer Betrieb genommen werden können, weil sie nicht genutzt werden oder ihre Lizenz abläuft. Die Verwendung von Tags ist eine effektive Möglichkeit, Ressourcen zu verfolgen, indem die Ressource mit ihrer Funktion oder einem bekannten Datum, an dem sie außer Betrieb genommen werden kann, gekennzeichnet wird. Berichte können dann zu diesen Tags ausgeführt werden. Beispielwerte für das Taggen von Features sind `feature-X testing`, um den Zweck der Ressource in Bezug auf den Workload-Lebenszyklus zu identifizieren. Ein anderes Beispiel ist die Verwendung von `LifeSpan`



oder TTL für Ressourcen, wie z. B. den Namen und den Wert des to-be-deleted Tag-Schlüssels, um den Zeitraum oder eine bestimmte Zeit für die Außerbetriebnahme zu definieren.

## Implementierungsschritte

- Implementieren eines Tagging-Schemas: Implementieren Sie ein Tagging-Schema, das die Workload identifiziert, zu der die Ressource gehört, und stellen Sie sicher, dass alle Ressourcen innerhalb der Workload entsprechend getaggt sind. Durch das Markieren mit Tags können Sie Ressourcen nach Zweck, Team, Umgebung oder anderen, für Ihr Unternehmen relevanten Kriterien kategorisieren. Detaillierte Informationen zu Anwendungsfällen, Strategien und Verfahren zum Taggen finden Sie in den [bewährten Methoden beim Tagging in AWS](#).
- Implementieren von Überwachung des Workload-Durchsatzes oder der Workload-Ausgabe: Implementieren Sie die Überwachung des Workload-Durchsatzes oder Alarme, die entweder bei Eingabebeanforderungen oder Ausgabeabschlüssen ausgelöst werden. Konfigurieren Sie die Überwachung so, dass Benachrichtigungen erstellt werden, wenn Workload-Anforderungen oder -Ausgaben auf Null fallen. Dies bedeutet, dass die Workload-Ressourcen nicht mehr verwendet werden. Integrieren Sie einen Zeitfaktor, wenn die Workload unter normalen Bedingungen regelmäßig auf Null fällt. Weitere Informationen zu ungenutzten oder nicht ausgelasteten Ressourcen finden Sie im [Artikel zu Checks für die Kostenoptimierung mit AWS Trusted Advisor](#).
- AWS Ressourcen gruppieren: Erstellen Sie Gruppen für AWS Ressourcen. Sie können [AWS Resource Groups](#) verwenden, um Ihre AWS Ressourcen zu organisieren und zu verwalten, die sich in derselben Gruppe befinden AWS-Region. Den meisten Ressourcen lassen sich Tags hinzufügen, um sie innerhalb der Organisation zu identifizieren und zu sortieren. Mit [Tag Editor](#) können Sie mehreren unterstützten Ressourcen gleichzeitig Tags hinzufügen. Ziehen Sie die Verwendung von [AWS Service Catalog](#) in Erwägung, um Portfolios mit genehmigten Produkten zu erstellen, zu verwalten und an Endnutzer zu verteilen und um den Produktlebenszyklus zu verwalten.

## Ressourcen

### Zugehörige Dokumente:

- [AWS Auto Scaling](#)
- [AWS Trusted Advisor](#)
- [AWS Trusted Advisor Prüfungen zur Kostenoptimierung](#)
- [Ressourcen kennzeichnen AWS](#)
- [Veröffentlichen von benutzerdefinierten Metriken](#)

## Zugehörige Videos:

- [Wie optimiert man die Kosten mit AWS Trusted Advisor](#)

## Zugehörige Beispiele:

- [AWS Ressourcen organisieren](#)
- [Optimieren Sie die Kosten mit AWS Trusted Advisor](#)

## COST04-BP02 Implementieren Sie einen Stilllegungsprozess

Implementieren Sie einen Prozess für die Identifizierung und Außerbetriebnahme nicht genutzter Ressourcen.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Hoch

### Implementierungsleitfaden

Implementieren Sie einen standardisierten Prozess in Ihrer gesamten Organisation, um ungenutzte Ressourcen zu identifizieren und zu entfernen. Der Prozess sollte definieren, wie häufig Suchvorgänge durchgeführt werden, und die Prozesse zum Entfernen der Ressource festlegen, um sicherzustellen, dass alle Organisationsanforderungen erfüllt sind.

### Implementierungsschritte

- Erstellen und Implementieren eines Prozesses für die Außerbetriebnahme: Erstellen Sie in Zusammenarbeit mit den Workload-Entwicklern und -Besitzern einen Prozess zur Außerbetriebnahme der Workloads und ihrer Ressourcen. Der Prozess sollte die Methode abdecken, um zu überprüfen, ob die Workload verwendet wird, und auch, ob jede der Workload-Ressourcen verwendet wird. Definieren Sie die erforderlichen Schritte, um die Ressource außer Betrieb zu nehmen und gleichzeitig die Einhaltung gesetzlicher Anforderungen sicherzustellen. Alle zugeordneten Ressourcen sollten dabei eingeschlossen werden, z. B. Lizenzen oder zugehöriger Speicher. Informieren Sie die Workload-Besitzer darüber, dass die Außerbetriebnahme gestartet wurde.

Die folgenden Schritte für die Außerbetriebnahme geben vor, was im Rahmen des Prozesses geprüft werden sollte:

- Identifizieren der Ressourcen, die außer Betrieb genommen werden sollen: Identifizieren Sie die Ressourcen, die in Ihrer AWS Cloud für die Außerbetriebnahme in Frage kommen. Erfassen

Sie alle erforderlichen Informationen und planen Sie die Außerbetriebnahme. Achten Sie bei der Zeitplanung darauf, unerwartete Probleme im Prozess zu berücksichtigen.

- Koordination und Kommunikation: Arbeiten Sie mit Workload-Besitzern zusammen, um zu bestätigen, dass die Ressource außer Betrieb genommen werden soll.
- Metadaten aufzeichnen und Backups erstellen: Erfassen Sie Metadaten (wie öffentlich IPs, Region, AZVPC, Subnetz und Sicherheitsgruppen) und erstellen Sie Backups (wie Amazon Elastic Block Store-Snapshots oder AufnahmenAMI, Schlüsselexport und Zertifikatsexport), wenn dies für die Ressourcen in der Produktionsumgebung erforderlich ist oder wenn es sich um kritische Ressourcen handelt.
- Validieren infrastructure-as-code: Stellen Sie fest AWS CloudFormation, ob Ressourcen mit Terraform oder einem anderen infrastructure-as-code Bereitstellungstool bereitgestellt wurden AWS Cloud Development Kit (AWS CDK), sodass sie bei Bedarf erneut bereitgestellt werden können.
- Verhindern des Zugriffs: Wenden Sie restriktive Kontrollen für einen bestimmten Zeitraum an, um zu verhindern, dass Ressourcen genutzt werden, während Sie bestimmen, ob diese benötigt werden. Stellen Sie sicher, dass die Ressourcenumgebung bei Bedarf in den ursprünglichen Zustand zurückversetzt werden kann.
- Folgen Sie Ihrem internen Außerbetriebnahmeprozess: Folgen Sie den administrativen Aufgaben und dem Außerbetriebnahmeprozess Ihrer Organisation, z. B. das Entfernen der Ressource aus Ihrer Unternehmensdomäne, das Entfernen des DNS Datensatzes und das Entfernen der Ressource aus Ihrem Konfigurationsmanagement-Tool, Überwachungstool, Automatisierungstool und Sicherheitstools.

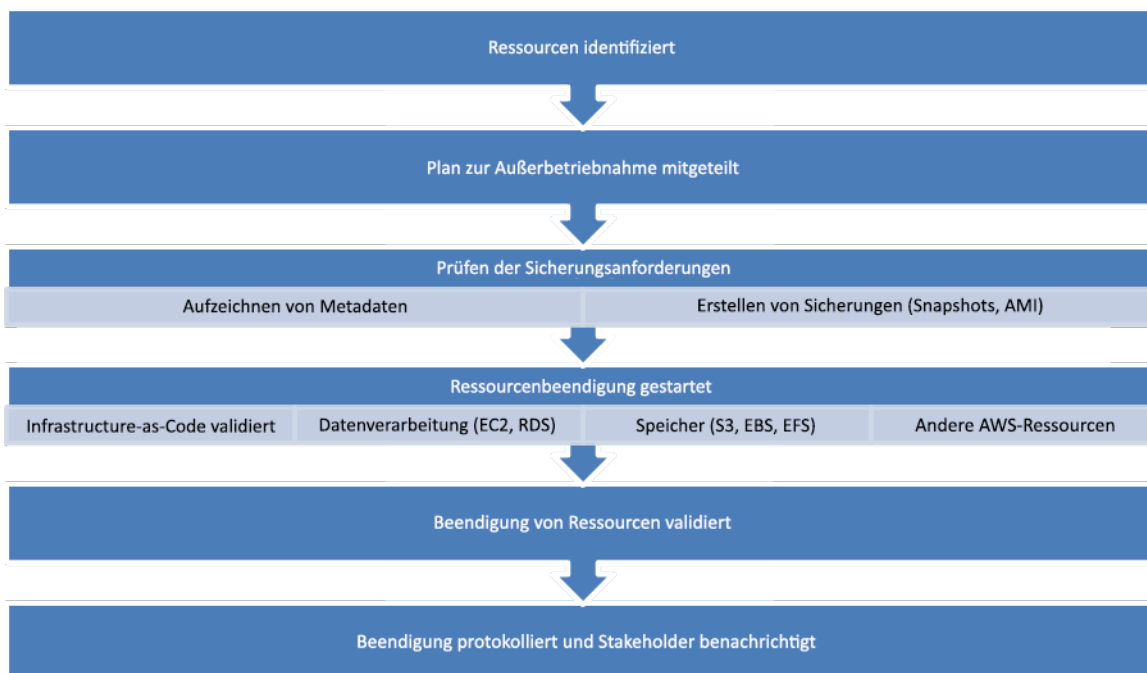
Wenn es sich bei der Ressource um eine EC2 Amazon-Instance handelt, schlagen Sie in der folgenden Liste nach. [Weitere Informationen finden Sie unter Wie lösche oder kündige ich meine EC2 Amazon-Ressourcen?](#)

- Stoppen oder beenden Sie alle Ihre EC2 Amazon-Instances und Load Balancer. EC2Amazon-Instances sind nach ihrer Beendigung für kurze Zeit in der Konsole sichtbar. Instances, die sich nicht im Ausführungsstatus befinden, werden Ihnen nicht in Rechnung gestellt.
- Löschen Sie Ihre Auto-Scaling-Infrastruktur.
- Geben Sie alle Dedicated Hosts frei.
- Löschen Sie alle EBS Amazon-Volumes und EBS Amazon-Snapshots.
- Geben Sie alle elastischen IP-Adressen frei.
- Melden Sie alle Amazon Machine Images ab ()AMIs.

- Beenden Sie alle Umgebungen AWS Elastic Beanstalk .

Wenn die Ressource ein Objekt in Amazon-S3-Glacier-Speicher ist und Sie ein Archiv löschen, bevor die Mindestspeicherdauer erreicht wurde, wird eine anteilige Gebühr für das frühzeitige Löschen in Rechnung gestellt. Die Mindestspeicherdauer für Amazon S3 Glacier ist abhängig von der verwendeten Speicherklasse. Eine Übersicht über die Mindestspeicherdauer der einzelnen Speicherklassen finden Sie in der Übersicht über die [Leistung für die verschiedenen Amazon-S3-Speicherklassen](#). Informationen zu Gebühren für vor Ablauf der Mindestspeicherdauer gelöschte Objekte finden Sie in der [Amazon-S3-Preisübersicht](#).

Das folgende Flussdiagramm eines einfachen Außerbetriebnahmeprozesses zeigt die einzelnen Schritte. Bestätigen Sie vor der Außerbetriebnahme von Ressourcen, dass die Ressourcen, die Sie für die Außerbetriebnahme identifiziert haben, von der Organisation nicht genutzt werden.



## Ablauf der Außerbetriebnahme von Ressourcen

### Ressourcen

### Zugehörige Dokumente:

- [AWS Auto Scaling](#)
- [AWS Trusted Advisor](#)
- [AWS CloudTrail](#)

## Zugehörige Videos:

- [Löschen Sie den CloudFormation Stack, behalten Sie aber einige Ressourcen bei](#)
- [Finden Sie heraus, welcher Benutzer die EC2 Amazon-Instance gestartet hat](#)

## Zugehörige Beispiele:

- [EC2Amazon-Ressourcen löschen oder beenden](#)
- [Finden Sie heraus, welcher Benutzer eine EC2 Amazon-Instance gestartet hat](#)

## COST04-BP03 Außerdienstliche Ressourcen

Außerbetriebnahme von Ressourcen, die durch Ereignisse wie regelmäßige Prüfungen oder Änderungen der Nutzung ausgelöst werden. Die Außerbetriebnahme erfolgt normalerweise regelmäßig und kann manuell oder automatisiert durchgeführt werden.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel

## Implementierungsleitfaden

Die Häufigkeit und der Aufwand für die Suche nach ungenutzten Ressourcen sollten die potenziellen Einsparungen widerspiegeln, sodass ein Konto mit geringen Kosten seltener analysiert werden sollte als ein Konto mit größeren Kosten. Suchanfragen und Außerbetriebnahmeereignisse können durch Statusänderungen in der Workload initiiert werden, z. B. ein Produkt, das sich dem Ende seiner Lebensdauer nähert oder ersetzt wird. Suchen und Außerbetriebnahme können auch durch externe Ereignisse initiiert werden, wie z. B. Änderungen der Marktbedingungen oder Produkteinstellung.

## Implementierungsschritte

- **Außerbetriebnahme von Ressourcen:** Dies ist die Phase, in der AWS -Ressourcen, die nicht mehr benötigt werden oder deren Lizenzvereinbarung abläuft, als veraltet deaktiviert werden. Führen Sie alle abschließenden Prüfungen durch und erstellen Sie Snapshots und Sicherungen, bevor Sie zur Außerbetriebnahmephase übergehen, um unerwünschte Unterbrechungen zu vermeiden. Befolgen Sie den Außerbetriebnahmeprozess, um jede der Ressourcen, die als nicht genutzt identifiziert wurde, außer Betrieb zu nehmen.

## Ressourcen

## Zugehörige Dokumente:

- [AWS Auto Scaling](#)
- [AWS Trusted Advisor](#)

Zugehörige Beispiele:

- [Well-Architected Labs: Decommission resources \(Level 100\)](#)

## COST04-BP04 Automatische Außerbetriebnahme von Ressourcen

Gestalten Sie Ihre Workload so, dass sie die Beendigung von Ressourcen reibungslos handhabt, wenn Sie unkritische Ressourcen, nicht benötigte Ressourcen oder Ressourcen mit geringer Auslastung identifizieren und außer Betrieb nehmen.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Niedrig

### Implementierungsleitfaden

Verwenden Sie die Automatisierung, um die damit verbundenen Kosten für die Außerbetriebnahme zu reduzieren oder zu entfernen. Wenn Sie Ihre Workload so konzipieren, dass die eine automatische Außerbetriebnahme durchführt, werden die gesamten Workload-Kosten während der Nutzungsdauer gesenkt. Sie können [Amazon EC2 Auto Scaling oder Application Auto Scaling](#) verwenden, um den Außerbetriebnahmeprozess durchzuführen. Sie können auch benutzerdefinierten Code mithilfe von [API Loder](#) implementieren, SDK um Workload-Ressourcen automatisch außer Betrieb zu nehmen.

[Moderne Anwendungen](#) basieren auf Serverless First, einer Strategie, die der Einführung serverloser Dienste Priorität einräumt. AWS entwickelte [serverlose Dienste](#) für alle drei Ebenen Ihres Stacks: Datenverarbeitung, Integration und Datenspeicher. Mit einer Serverless-Architektur können Sie in Phasen mit wenig Datenverkehr dank automatischer Skalierung Kosten sparen.

### Implementierungsschritte

- Implementieren Sie Amazon EC2 Auto Scaling oder Application Auto Scaling: Für Ressourcen, die unterstützt werden, konfigurieren Sie sie mit Amazon EC2 Auto Scaling oder Application Auto Scaling. Diese Services können Ihnen helfen, Ihre Nutzung zu optimieren und die Kosteneffizienz bei der Nutzung von AWS Services zu optimieren. Wenn die Nachfrage sinkt, entfernen diese Services automatisch überschüssige Ressourcenkapazitäten, damit keine unnötigen Kosten entstehen.
- CloudWatch So konfigurieren, dass Instanzen beendet werden: Instanzen können so konfiguriert werden, dass sie mithilfe von [CloudWatch Alarmen](#) beendet werden. Implementieren Sie

mithilfe der Metriken aus dem Außerbetriebnahmeprozess einen Alarm mit einer Aktion von Amazon Elastic Compute Cloud. Überprüfen Sie den Vorgang vor der Einführung in einer Nicht-Produktionsumgebung.

- Implementieren Sie Code innerhalb des Workloads: Sie können das AWS SDK oder verwenden AWS CLI , um Workload-Ressourcen außer Betrieb zu nehmen. Implementieren Sie Code innerhalb der Anwendung, der Ressourcen, die nicht mehr verwendet werden, integriert AWS und beendet oder entfernt.
- Verwenden Sie serverlose Dienste: Priorisieren Sie den Aufbau [serverloser Architekturen und ereignisgesteuerter Architekturen, um Ihre Anwendungen zu AWS erstellen und auszuführen](#). AWS bietet mehrere serverlose Technologiedienste, die von Haus aus eine automatisch optimierte Ressourcennutzung und automatische Außerbetriebnahme (Scale In und Scale Out) ermöglichen. Bei Serverless-Anwendungen wird die Ressourcennutzung automatisch optimiert und Ihnen entstehen nie Kosten für die Überbereitstellung.

## Ressourcen

### Zugehörige Dokumente:

- [Amazon EC2 Auto Scaling](#)
- [Erste Schritte mit Amazon EC2 Auto Scaling](#)
- [Application Auto Scaling](#)
- [AWS Trusted Advisor](#)
- [Serverlos an AWS](#)
- [Erstellen Sie Alarme, um eine Instance anzuhalten, zu beenden, neu zu starten oder wiederherzustellen.](#)
- [Abbruchaktionen zu CloudWatch Amazon-Alarmen hinzufügen](#)

### Zugehörige Beispiele:

- [Planung des automatischen Löschens von AWS CloudFormation Stacks](#)
- [Well-Architected Labs – Decommission resources automatically \(Level 100\)](#)
- [Servian Auto Cleanup AWS](#)

## COST04-BP05 Richtlinien zur Datenspeicherung durchsetzen

Definieren Sie Richtlinien zur Datenaufbewahrung auf unterstützten Ressourcen, um das Löschen von Objekten gemäß den Anforderungen Ihrer Organisation durchzuführen. Identifizieren und löschen Sie entbehrliche und verwaiste Ressourcen und Objekte, die nicht mehr benötigt werden.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Mittel

Mit Richtlinien zur Datenaufbewahrung und Lebenszyklusrichtlinien können Sie die mit der Außerbetriebnahme von Prozessen verbundenen Kosten sowie die Speicherkosten für die identifizierten Ressourcen reduzieren. Die Definition von Richtlinien zur Datenaufbewahrung und Lebenszyklusrichtlinien zur Durchführung einer automatischen Speicherklassenmigration und Löschung verringert die Gesamtspeicherkosten während des Lebenszyklus. Sie können Amazon Data Lifecycle Manager verwenden, um die Erstellung und Löschung von Amazon Elastic Block Store-Snapshots und Amazon EBS Machine Images (AMIs) zu automatisieren und Amazon S3 Intelligent-Tiering oder eine Amazon S3 S3-Lebenszykluskonfiguration verwenden, um den Lebenszyklus Ihrer Amazon S3 S3-Objekte zu verwalten. Sie können auch benutzerdefinierten Code mithilfe von [APLoder](#) implementieren, um Lebenszyklusrichtlinien und Richtlinienregeln für Objekte SDK zu erstellen, die automatisch gelöscht werden sollen.

### Implementierungsschritte

- Amazon Data Lifecycle Manager verwenden: Verwenden Sie Lebenszyklusrichtlinien in Amazon Data Lifecycle Manager, um das Löschen von EBS Amazon-Snapshots und EBS Amazon-Backups zu automatisieren. AMIs
- Einrichten der Lebenszykluskonfiguration für einen Bucket: Verwenden Sie die Amazon-S3-Lebenszykluskonfiguration für einen Bucket, um Aktionen für Amazon S3 zu definieren, die während des Lebenszyklus des Objekts ergriffen werden sollen, sowie die Löschung am Ende des Lebenszyklus des Objekts basierend auf Ihren geschäftlichen Anforderungen.

### Ressourcen

#### Zugehörige Dokumente:

- [AWS Trusted Advisor](#)
- [Amazon Data Lifecycle Manager](#)
- [How to set lifecycle configuration on Amazon S3 bucket](#)



## Zugehörige Videos:

- [Automatisieren Sie EBS Amazon-Snapshots mit Amazon Data Lifecycle Manager](#)
- [Empty an Amazon S3 bucket using a lifecycle configuration rule](#)

## Zugehörige Beispiele:

- [Empty an Amazon S3 bucket using a lifecycle configuration rule](#)
- [Well-Architected Lab: Decommission resources automatically \(Level 100\)](#)

# Kostengünstige Ressourcen

## Fragen

- [COST5. Wie können Sie die Kosten bei der Auswahl von Services einschätzen?](#)
- [COST6. Wie können Sie bei der Auswahl des Ressourcentyps, -umfangs und der Anzahl der Ressourcen Kostenziele erfüllen?](#)
- [COST7. Wie können Sie Kosten mithilfe von Preismodellen senken?](#)
- [COST8. Wie können Sie die Kosten für Datenübertragungen planen?](#)

## COST5. Wie können Sie die Kosten bei der Auswahl von Services einschätzen?

Amazon EC2/EBS, Amazon und Amazon S3 sind Baustein-Services AWS. Managed Services wie Amazon RDS und Amazon DynamoDB sind Services auf höherer Ebene oder Anwendungsebene. AWS Wenn Sie sich für die richtigen Bausteine und verwalteten Services entscheiden, können Sie die Kosten dieser Workload 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

- [COST05-BP01 Identifizieren Sie die organisatorischen Anforderungen an die Kosten](#)
- [COST05-BP02 Analysieren Sie alle Komponenten des Workloads](#)
- [COST05-BP03 Führen Sie eine gründliche Analyse jeder Komponente durch](#)
- [COST05-BP04 Wählen Sie Software mit kostengünstiger Lizenzierung aus](#)
- [COST05-BP05 Wählen Sie die Komponenten dieses Workloads aus, um die Kosten entsprechend den Prioritäten der Organisation zu optimieren](#)

- [COST05-BP06 Führen Sie eine Kostenanalyse für unterschiedliche Nutzungen im Laufe der Zeit durch](#)

COST05-BP01 Identifizieren Sie die organisatorischen Anforderungen an die Kosten

Definieren Sie gemeinsam mit den Teammitgliedern für diese Workload das Gleichgewicht zwischen Kostenoptimierung und anderen Säulen wie Leistung und Zuverlässigkeit.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Hoch

### Implementierungsleitfaden

In den meisten Organisationen besteht die Abteilung für Informationstechnologie (IT) aus mehreren kleinen Teams, von denen jedes seine eigene Agenda und seinen eigenen Schwerpunktbereich hat, der die Spezialgebiete und Fähigkeiten seiner Teammitglieder widerspiegelt. Sie müssen die allgemeinen Ziele, Prioritäten und Vorgaben Ihrer Organisation verstehen und wissen, wie jede Abteilung oder jedes Projekt zu diesen Zielen beiträgt. Die Kategorisierung aller wesentlichen Ressourcen, einschließlich Personal, Ausrüstung, Technologie, Material und externer Dienstleistungen, ist für die Erreichung der organisatorischen Ziele und eine umfassende Budgetplanung von entscheidender Bedeutung. Die Anwendung dieses systematischen Ansatzes zur Kostenermittlung und zum Kostenverständnis ist für die Erstellung eines realistischen und soliden Kostenplans für die Organisation von grundlegender Bedeutung.

Bei der Auswahl von Services für Ihre Workload ist es wichtig, dass Sie die Prioritäten Ihrer Organisation verstehen. Schaffen Sie ein Gleichgewicht zwischen Kostenoptimierung und anderen AWS Well-Architected Framework-Säulen wie Leistung und Zuverlässigkeit. Dieser Prozess sollte systematisch und regelmäßig durchgeführt werden, um Veränderungen in den Zielen der Organisation, den Marktbedingungen und der betrieblichen Dynamik zu berücksichtigen. Eine vollständig kostenoptimierte Workload ist die Lösung, die am meisten an den Anforderungen Ihrer Organisation ausgerichtet ist, nicht notwendigerweise an den niedrigsten Kosten. Treffen Sie sich mit allen Teams innerhalb Ihrer Organisation, um Informationen zu sammeln, z. B. mit den Produkt-, Geschäfts-, Technik- und Finanz-Teams. Bewerten Sie die Auswirkungen von Kompromissen zwischen konkurrierenden Interessen oder alternativen Ansätzen, um fundiert zu entscheiden, auf welche Bereiche die Anstrengungen konzentriert werden sollten, oder eine geeignete Handlungsweise zu wählen.

Beispielsweise kann die Beschleunigung der Markteinführung neuer Features einer Kostenoptimierung vorgezogen werden oder Sie können eine relationale Datenbank für nicht

relationale Daten wählen, um die Migration eines Systems zu vereinfachen, anstatt zu einer für Ihren Datentyp optimierten Datenbank zu migrieren und Ihre Anwendung zu aktualisieren.

### Implementierungsschritte

- Ermitteln der Organisationsanforderungen zur Kosteneinschätzung: Treffen Sie sich mit Teammitgliedern aus Ihrer Organisation, darunter Produktmanagement, Anwendungsbesitzern, Entwicklungs- und Betriebsteams, Management und Finanzen. Setzen Sie die Prioritäten hinsichtlich der Well-Architected-Säulen für diese Workload und seine Komponenten. Die Ausgabe sollte eine Liste der Säulen in der entsprechenden Reihenfolge sein. Sie können jeder Säule auch eine Gewichtung zuweisen, um anzugeben, wie viel zusätzlicher Fokus sie hat, oder wie ähnlich der Fokus zwischen zwei Säulen ist.
- Erfassen und Dokumentieren der technischen Schulden: Befassen Sie sich bei der Workload-Überprüfung mit den technischen Schulden. Dokumentieren Sie ein Backlog-Element, um die Workload in Zukunft wieder aufzugreifen und erneut zu überarbeiten oder neu zu strukturieren, mit dem Ziel, sie weiter zu optimieren. Es ist wichtig, dass Sie die Kompromisse, die Sie eingegangen sind, den anderen Beteiligten klar mitteilen.

### Ressourcen

Zugehörige bewährte Methoden:

- [REL11-BP07 Gestalten Sie Ihr Produkt so, dass es Verfügbarkeitsziele und Service Level Agreements für Verfügbarkeit erfüllt \(\) SLAs](#)
- [OPS01-BP06 Bewerten Sie Kompromisse](#)

Zugehörige Dokumente:

- [AWS Rechner für die Gesamtbetriebskosten \(\) TCO](#)
- [Amazon-S3-Speicherklassen](#)
- [Cloud-Produkte](#)

COST05-BP02 Analysieren Sie alle Komponenten des Workloads

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.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Hoch

### Implementierungsleitfaden

Workload-Komponenten, die der Organisation einen geschäftlichen Nutzen bringen sollen, können verschiedene Services umfassen. Für jede Komponente könnten spezifische AWS Cloud Dienste ausgewählt werden, um den Geschäftsanforderungen gerecht zu werden. Diese Auswahl könnte von Faktoren wie der Vertrautheit mit diesen Services oder früheren Erfahrungen mit ihnen beeinflusst sein.

Nachdem Sie die Anforderungen Ihres Unternehmens, wie in [COST05-BP01 Identifizieren Sie die organisatorischen Anforderungen in Bezug auf die Kosten](#) beschrieben, identifiziert haben, führen Sie eine gründliche Analyse aller Komponenten Ihres Workloads durch. Analysieren Sie jede Komponente unter Berücksichtigung der aktuellen und prognostizierten Kosten und Größen. Wägen Sie die Kosten der Analyse gegen die potenziellen Einsparungen bei der Workload während des Lebenszyklus ab. Der Aufwand, der für die Analyse aller Komponenten dieser Workloads betrieben wird, sollte den potenziellen Einsparungen oder Verbesserungen entsprechen, die durch die Optimierung dieser spezifischen Komponente zu erwarten sind. Wenn zum Beispiel die Kosten der vorgeschlagenen Ressource 10 USD/Monat betragen und bei prognostizierter Belastung 15 USD/Monat nicht überschreiten würden, könnte ein Tag Aufwand, um die Kosten um 50 % zu reduzieren (5 USD pro Monat), den potenziellen Nutzen über die Lebensdauer des Systems übersteigen. Verwenden Sie eine schnellere und effizientere datenbasierte Schätzung, um das beste Gesamtergebnis für diese Komponente zu erzielen.

Workloads können sich im Laufe der Zeit ändern. Die richtigen Services sind möglicherweise nicht optimal, wenn sich die Workload-Architektur oder -Nutzung ändert. Die Analyse für die Auswahl von Services muss aktuelle und zukünftige Workload-Zustände und Nutzungsebenen umfassen. Die Implementierung eines Service für den zukünftigen Workload-Status oder die Nutzung kann die Gesamtkosten senken, indem der Aufwand reduziert oder beseitigt wird, der für zukünftige Änderungen erforderlich ist. Beispielsweise könnte die Verwendung von EMR Serverless zunächst die richtige Wahl sein. Wenn die Nutzung für diesen Dienst jedoch zunimmt, EC2 könnte eine Umstellung EMR auf einen Dienst die Kosten für diese Komponente des Workloads senken.

[AWS Cost Explorer](#) und mit AWS Cost and Usage Reports ([CUR](#)) können die Kosten einer Machbarkeitsstudie (PoC) oder einer Betriebsumgebung analysiert werden. Sie können [AWS Pricing Calculator](#) auch verwenden, um die Workload-Kosten zu schätzen.

Schreiben Sie einen Workflow, an den sich die technischen Teams halten, um ihre Workloads zu überprüfen. Halten Sie diesen Workflow einfach, decken Sie aber auch alle notwendigen Schritte ab, um sicherzustellen, dass die Teams jede Komponente der Workload und ihre Preisgestaltung verstehen. Ihre Organisation kann diesen Workflow dann verfolgen und an die spezifischen Bedürfnisse jedes Teams anpassen.

1. Listen Sie jeden Dienst auf, der für Ihre Workload verwendet wird: Dies ist ein guter Ausgangspunkt. Identifizieren Sie alle Services, die derzeit genutzt werden und woher die Kosten stammen.
2. Verstehen Sie, wie die Preisgestaltung für diese Services funktioniert: Machen Sie sich mit dem [Preismodell](#) der einzelnen Services vertraut. Verschiedene AWS Dienste haben unterschiedliche Preismodelle, die auf Faktoren wie Nutzungsvolumen, Datenübertragung und funktionspezifischen Preisen basieren.
3. Konzentrieren Sie sich auf die Services, die mit unerwarteten Workload-Kosten verbunden sind und die nicht Ihrer erwarteten Nutzung und Ihrem Geschäftsergebnis entsprechen: Identifizieren Sie Ausreißer oder Services, bei denen die Kosten nicht proportional zum Wert oder zur Nutzung von AWS Cost Explorer oder s sind. AWS Cost and Usage Report Es ist wichtig, die Kosten mit den Geschäftsergebnissen zu korrelieren, um Optimierungsmaßnahmen zu priorisieren.
4. AWS Cost Explorer, CloudWatch Logs, VPC Flow Logs und Amazon S3 Storage Lens, um die Ursache dieser hohen Kosten zu verstehen: Diese Tools sind entscheidend für die Diagnose hoher Kosten. Jeder Service bietet einen anderen Blickwinkel, um die Nutzung und Kosten zu betrachten und zu analysieren. Cost Explorer hilft beispielsweise dabei, allgemeine Kostentrends zu ermitteln, CloudWatch Logs bietet betriebliche Einblicke, VPC Flow Logs zeigt IP-Verkehr an und Amazon S3 Storage Lens ist nützlich für Speicheranalysen.
5. Wird verwendet AWS Budgets , um Budgets für bestimmte Beträge für Dienste oder Konten festzulegen: Die Festlegung von Budgets ist eine proaktive Methode zur Kostenverwaltung. Wird verwendet AWS Budgets , um benutzerdefinierte Budgetschwellenwerte festzulegen und Benachrichtigungen zu erhalten, wenn die Kosten diese Schwellenwerte überschreiten.
6. Konfigurieren Sie CloudWatch Amazon-Alarme für das Senden von Abrechnungs- und Nutzungswarnungen: Richten Sie Überwachung und Benachrichtigungen für Kosten- und Nutzungskennzahlen ein. CloudWatch Alarme können Sie benachrichtigen, wenn bestimmte Schwellenwerte überschritten werden, was die Reaktionszeit bei Eingriffen verbessert.

Erzielen Sie im Laufe der Zeit bemerkenswerte Verbesserungen und finanzielle Einsparungen durch eine strategische Überprüfung aller Workload-Komponenten, unabhängig von ihren gegenwärtigen

Merkmale. Der Aufwand für diesen Überprüfungsprozess sollte bewusst und unter sorgfältiger Abwägung der möglichen Vorteile betrieben werden.

### Implementierungsschritte

- Erstellen einer Liste der Workload-Komponenten: Erstellen Sie eine Liste mit den Komponenten Ihrer Workload. Verwenden Sie diese Liste, um zu überprüfen, ob jede Komponente analysiert wurde. Der Aufwand sollte die Kritikalität für die Workload widerspiegeln, die durch die Prioritäten Ihrer Organisation definiert wird. Die Gruppierung von Ressourcen verbessert die Effizienz (z. B. die Speicherung von Produktionsdatenbanken, wenn es mehrere Datenbanken gibt).
- Priorisieren der Komponentenliste: Priorisieren Sie die Komponentenliste entsprechend dem Aufwand. In der Regel erfolgt die Priorisierung nach den Kosten der Komponente – von der teuersten zur günstigsten. Alternativ kann sie auch nach der von den Prioritäten Ihrer Organisation definierten Kritikalität erfolgen.
- Durchführen der Analyse: Überprüfen Sie für jede Komponente auf der Liste die verfügbaren Optionen und Services und wählen Sie die Option aus, die am besten mit Ihren Organisationsprioritäten übereinstimmt.

### Ressourcen

#### Zugehörige Dokumente:

- [AWS Pricing Calculator](#)
- [AWS Cost Explorer](#)
- [Amazon-S3-Speicherklassen](#)
- [AWS Cloud -Produkte](#)

#### Zugehörige Videos:

- [AWS Serie zur Kostenoptimierung: CloudWatch](#)

COST05-BP03 Führen Sie eine gründliche Analyse jeder Komponente durch

Nehmen Sie die Gesamtkosten, die der Organisation durch die einzelnen Komponenten entstehen, unter die Lupe. Berechnen Sie die Gesamtbetriebskosten unter Berücksichtigung der Betriebs- und Verwaltungskosten, insbesondere bei der Nutzung von verwalteten Services durch den Cloud-

Anbieter. Der Überprüfungsaufwand sollte in einem angemessenen Verhältnis zum potenziellen Nutzen stehen, z. B. muss die Zeit, die für die Analyse benötigt wird, den Komponentenkosten entsprechen.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Hoch

### Implementierungsleitfaden

Bedenken Sie die Zeitersparnis, die es Ihrem Team ermöglicht, sich auf das Aufholen technischen Rückstands, Innovation, wertschöpfende Features und die Herausarbeitung eines Alleinstellungsmerkmals zu konzentrieren. So könnten Sie beispielsweise Ihre Datenbank von Ihrer On-Premises-Umgebung so schnell wie möglich per Lift and Shift in die Cloud verlagern (auch als Hostwechsel bekannt) und die Optimierung im Nachgang ausführen. Es lohnt sich, die möglichen Einsparungen zu untersuchen, die Sie durch den Einsatz von verwalteten Services auf AWS erzielen könnten, die Lizenzkosten entfernen oder reduzieren. Mit Managed Services AWS entfällt der betriebliche und administrative Aufwand, der mit der Wartung eines Dienstes verbunden ist, wie z. B. das Patchen oder Aktualisieren des Betriebssystems, sodass Sie sich auf Innovation und Ihr Geschäft konzentrieren können.

Da verwaltete Services in der großen Cloud-Umgebung ausgeführt werden, profitieren Sie hier von geringeren Kosten pro Transaktion oder Service. Sie können potenzielle Optimierungen vornehmen, um konkrete Vorteile zu erzielen, ohne die Kernarchitektur der Anwendung zu ändern. Möglicherweise möchten Sie den Zeitaufwand für die Verwaltung von Datenbank-Instances reduzieren, indem Sie auf eine database-as-a-service Plattform wie [Amazon Relational Database Service \(AmazonRDS\)](#) migrieren oder Ihre Anwendung auf eine vollständig verwaltete Plattform wie migrieren. [AWS Elastic Beanstalk](#)

Verwaltete Services weisen in der Regel Attribute auf, die Sie festlegen können, um zu gewährleisten, dass ausreichend Kapazität bereitsteht. Sie müssen diese Attribute festlegen und überwachen, damit Ihre überschüssige Kapazität auf ein Minimum begrenzt und die Leistung maximiert werden. Sie können die Eigenschaften der AWS Managed Services Verwendung von AWS Management Console oder ändern AWS APIs und den Ressourcenbedarf SDKs an die sich ändernde Nachfrage anpassen. Sie können beispielsweise die Anzahl der Knoten in einem EMR Amazon-Cluster (oder einem Amazon Redshift-Cluster) erhöhen oder verringern, um nach oben oder unten zu skalieren.

Sie können auch mehrere Instances auf eine AWS Ressource packen, um eine Nutzung mit höherer Dichte zu aktivieren. Sie können beispielsweise mehrere kleine Datenbanken auf einer einzigen Amazon Relational Database Service (AmazonRDS) -Datenbank-Instance

bereitstellen. Bei steigender Nutzung können Sie eine der Datenbanken mithilfe eines Snapshot- und Wiederherstellungsprozesses auf eine dedizierte RDS Amazon-Datenbank-Instance migrieren.

Wenn Sie Workloads auf verwalteten Services bereitstellen, müssen Sie sich mit den Anforderungen für das Anpassen der Service-Kapazität vertraut machen. Diese Anforderungen sind in der Regel Zeit, Aufwand und die Auswirkungen auf den normalen Workload-Betrieb. Die bereitgestellte Ressource muss Zeit für Änderungen einräumen und den erforderlichen Overhead bereitstellen, damit dies möglich ist. Der laufende Aufwand, der zur Änderung von Diensten erforderlich ist, kann durch SDKs die Verwendung von System APIs - und Überwachungstools wie Amazon praktisch auf Null reduziert werden CloudWatch.

[Amazon RDS](#), [Amazon Redshift](#) und [Amazon ElastiCache](#) bieten einen verwalteten Datenbankservice an. [Amazon Athena](#)EMR, [Amazon](#) und [Amazon OpenSearch Service](#) bieten einen verwalteten Analysedienst.

[AMS](#) ist ein Service, der die AWS Infrastruktur im Auftrag von Unternehmenskunden und Partnern betreibt. Er bietet eine sichere und konforme Umgebung, in der Sie Ihre Workloads bereitstellen können. AMS verwendet automatisierte Cloud-Betriebsmodelle für Unternehmen, damit Sie die Anforderungen Ihres Unternehmens erfüllen, schneller in die Cloud wechseln und Ihre laufenden Verwaltungskosten senken können.

## Implementierungsschritte

- Durchführen einer gründlichen Analyse: Arbeiten Sie anhand der Komponentenliste jede Komponente von der höchsten Priorität bis zur niedrigsten Priorität ab. Führen Sie für die Komponenten mit höherer Priorität sowie für die teureren Komponenten zusätzliche Analysen durch und bewerten Sie alle verfügbaren Optionen und deren langfristige Auswirkungen. Bewerten Sie bei Komponenten mit niedrigerer Priorität, ob Änderungen in der Nutzung die Priorität der Komponente ändern. Führen Sie anschließend eine Analyse des angemessenen Aufwands durch.
- Vergleichen Sie verwaltete und nicht verwaltete Ressourcen: Berücksichtigen Sie die Betriebskosten der von Ihnen verwalteten Ressourcen und vergleichen Sie sie mit den AWS verwalteten Ressourcen. Überprüfen Sie beispielsweise Ihre Datenbanken, die auf EC2 Amazon-Instances laufen, und vergleichen Sie sie mit RDS Amazon-Optionen (einem AWS verwalteten Service) oder Amazon EMR mit der Ausführung von Apache Spark auf AmazonEC2. Wenn Sie von einem selbst verwalteten Workload zu einem AWS vollständig verwalteten Workload wechseln, sollten Sie Ihre Optionen sorgfältig prüfen. Berücksichtigen Sie dabei die drei wichtigsten Faktoren: die [Art des verwalteten Service](#), den Sie verwenden möchten, den Prozess, den Sie zur [Migration Ihrer Daten](#) verwenden, und ein Verständnis des [AWS -Modells der geteilten Verantwortung](#).



## Ressourcen

### Zugehörige Dokumente:

- [AWS Rechner für die Gesamtbetriebskosten \(TCO\)](#)
- [Amazon-S3-Speicherklassen](#)
- [AWS Cloud -Produkte](#)
- [AWS Modell mit geteilter Verantwortung](#)

### Zugehörige Videos:

- [Why move to a managed database?](#)
- [Was ist Amazon EMR und wie kann ich es für die Datenverarbeitung verwenden?](#)

### Zugehörige Beispiele:

- [Why move to a managed database](#)
- [Konsolidieren Sie Daten aus identischen SQL Server-Datenbanken in einer einzigen Amazon RDS für SQL Server-Datenbank mit AWS DMS](#)
- [Bereitstellung von Daten in großem Umfang an Amazon Managed Streaming for Apache Kafka \(AmazonMSK\)](#)
- [Migrieren Sie einASP.NETWebanwendung zu AWS Elastic Beanstalk](#)

COST05-BP04 Wählen Sie Software mit kostengünstiger Lizenzierung aus

Open-Source-Software eliminiert Softwarelizenzkosten, die erhebliche Kosten in Workloads verursachen können. Wenn lizenzierte Software erforderlich ist, sollten Sie Lizenzen vermeiden, die an willkürliche Eigenschaften gebunden sind CPUs, z. B. sollten Sie nach Lizenzen suchen, die an Leistung oder Ergebnisse gebunden sind. Die Kosten dieser Lizenzen lassen sich besser auf die von ihnen bereitgestellten Vorteile skalieren.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Niedrig

### Implementierungsleitfaden

Der Begriff „Open Source“ hat seinen Ursprung in der Softwareentwicklung und bedeutet, dass die Software bestimmte Kriterien für die freie Verteilung erfüllt. Open-Source-Software zeichnet sich

durch einen Quellcode aus, der von jedem eingesehen, verändert und verbessert werden kann. Auf der Grundlage der Geschäftsanforderungen, der Fähigkeiten der Techniker, der prognostizierten Nutzung oder anderer technologischer Abhängigkeiten können Unternehmen den Einsatz von Open-Source-Software in Betracht ziehen, AWS um ihre Lizenzkosten zu minimieren. Mit anderen Worten, die Kosten für Softwarelizenzen können durch den Einsatz von [Open-Source-Software](#) gesenkt werden. Dies kann erhebliche Auswirkungen auf die Workload-Kosten haben, da die Größe der Workload skaliert wird.

Wägen Sie die Vorteile lizenzierter Software gegen die Gesamtkosten ab, um Ihre Workload zu optimieren. Modellieren Sie Änderungen bei der Lizenzierung und wie sich diese auf Ihre Workload-Kosten auswirken würden. Wenn ein Anbieter die Kosten Ihrer Datenbanklizenz ändert, untersuchen Sie, wie sich dies auf die Gesamteffizienz Ihrer Workload auswirkt. Berücksichtigen Sie historische Preisankündigungen von Ihren Anbietern für Trends bei Lizenzänderungen in ihren Produkten. Die Lizenzkosten können auch unabhängig vom Durchsatz oder der Nutzung skaliert werden, z. B. bei Lizenzen, die je nach Hardware skaliert werden (CPUgebundene Lizenzen). Diese Lizenzen sollten vermieden werden, da sich die Kosten ohne entsprechende Ergebnisse schnell erhöhen können.

Wenn Sie beispielsweise eine EC2 Amazon-Instance in us-east-1 mit einem Linux-Betriebssystem betreiben, können Sie die Kosten im Vergleich zur Ausführung einer anderen EC2 Amazon-Instance, die unter Windows läuft, um ca. 45% senken.

Das [AWS Pricing Calculator](#) bietet eine umfassende Möglichkeit, die Kosten verschiedener Ressourcen mit unterschiedlichen Lizenzoptionen zu vergleichen, z. B. RDS Amazon-Instances und verschiedene Datenbank-Engines. Darüber hinaus AWS Cost Explorer bietet das einen unschätzbaren Überblick über die Kosten vorhandener Workloads, insbesondere solcher, die mit unterschiedlichen Lizenzen ausgestattet sind. Für die Lizenzverwaltung bietet [AWS License Manager](#) eine optimierte Methode zur Überwachung und Verwaltung von Softwarelizenzen. Kunden können ihre bevorzugte Open-Source-Software in der AWS Cloud bereitstellen und einsetzen.

### Implementierungsschritte

- **Analysieren der Lizenzoptionen:** Überprüfen Sie die Lizenzbedingungen der verfügbaren Software. Suchen Sie nach Open-Source-Versionen, die über die erforderliche Funktionalität verfügen, und stellen Sie fest, ob die Vorteile der lizenzierten Software die Kosten überwiegen. Bei günstigen Bedingungen stimmen die Kosten der Software mit ihren Vorteilen überein.
- **Analysieren des Softwareanbieters:** Überprüfen Sie alle bisherigen Preis- oder Lizenzänderungen des Anbieters. Suchen Sie nach Änderungen, die nicht im Einklang mit den Ergebnissen stehen,

wie z. B. Strafen für die Ausführung auf Hardware oder Plattformen bestimmter Anbieter. Achten Sie zudem darauf, wie mögliche Prüfungen und Strafen durchgeführt werden.

## Ressourcen

### Zugehörige Dokumente:

- [Open Source unter AWS](#)
- [AWS Rechner für die Gesamtbetriebskosten \(TCO\)](#)
- [Amazon-S3-Speicherklassen](#)
- [Cloud-Produkte](#)

### Zugehörige Beispiele:

- [Open-Source-Blogs](#)
- [AWS Open-Source-Blogs](#)
- [Optimierung und Lizenzierungsbewertung](#)

COST05-BP05 Wählen Sie die Komponenten dieses Workloads aus, um die Kosten entsprechend den Prioritäten der Organisation zu optimieren

Berücksichtigen Sie bei der Auswahl sämtlicher Komponenten für Ihre Workload die Kosten. Dies umfasst die Nutzung von verwalteten Services und Services auf Anwendungsebene oder einer Serverless-, Container- oder ereignisgesteuerten Architektur, um die Gesamtkosten zu verringern. Minimieren Sie Lizenzkosten mithilfe von Open-Source-Software, Software, für die keine Lizenzgebühren anfallen, oder Alternativen zur Verringerung der Ausgaben.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Mittel

## Implementierungsleitfaden

Berücksichtigen Sie die Kosten von Services und Optionen, wenn Sie alle Komponenten auswählen. Dazu gehört die Nutzung von Services auf Anwendungsebene und verwalteten Diensten wie [Amazon Relational Database Service](#) (AmazonRDS), [Amazon DynamoDB](#), Amazon [Simple Notification Service](#) (AmazonSNS) und Amazon [Simple Email Service \(AmazonSES\)](#), um die Gesamtkosten der Organisation zu senken.

Verwenden Sie Serverless-Lösungen und Container für die Datenverarbeitung, zum Beispiel [AWS Lambda](#) und [Amazon Simple Storage Service](#) (Amazon S3) für statische Websites. Containerisieren Sie Ihre Anwendung nach Möglichkeit und verwenden Sie AWS Managed Container Services wie [Amazon Elastic Container Service](#) (Amazon ECS) oder [Amazon Elastic Kubernetes Service](#) (Amazon EKS).

Minimieren Sie Lizenzkosten, indem Sie Open-Source-Software oder Software ohne Lizenzgebühren verwenden, wie z. B. Amazon Linux für Datenverarbeitungs-Workloads. Alternativ können Sie Datenbanken auch zu Amazon Aurora migrieren.

[Sie können serverlose Dienste oder Dienste auf Anwendungsebene wie Lambda, Amazon Simple Queue Service \(Amazon SQS\), Amazon und Amazon SNS verwenden. SES](#) Mit diesen Services müssen Sie keine Ressourcen mehr verwalten und sie stellen die Funktion der Codeausführung, Warteschlangenservices und Nachrichtenzustellung bereit. Der andere Vorteil besteht darin, dass die Leistung und Kosten entsprechend der Nutzung skaliert werden, was eine effiziente Kostenzuordnung ermöglicht.

Die Verwendung einer [ereignisgesteuerten Architektur](#) ist auch mit Serverless-Services möglich. Ereignisgesteuerte Architekturen sind Push-basiert, es geschieht also alles On-Demand, während das Ereignis im Router auftritt. So bezahlen Sie nicht für eine kontinuierliche Abfragung, um auf ein Ereignis zu prüfen. Das bedeutet weniger Netzwerkbandbreitenverbrauch, weniger CPU Auslastung, weniger ungenutzte Flottenkapazität und weniger Handshakes. SSL TLS

Weitere Informationen zu Serverless finden Sie im Whitepaper [Serverless Applications Lens - AWS Well-Architected Framework](#).

### Implementierungsschritte

- Auswahl der einzelnen Services zur Kostenoptimierung: Wählen Sie unter Verwendung Ihrer Prioritätenliste und Analyse jede Option aus, die am besten mit Ihren Organisationsprioritäten übereinstimmt. Statt die Kapazität zu erhöhen, um die Nachfrage zu erfüllen, denken Sie über andere Optionen nach, die eine bessere Leistung mit geringeren Kosten bedeuten können. Wenn Sie beispielsweise den erwarteten Traffic für Ihre Datenbanken überprüfen müssen, sollten Sie entweder die Instance-Größe erhöhen oder Amazon ElastiCache Services (Redis oder Memcached) verwenden, um Cache-Mechanismen für Ihre Datenbanken bereitzustellen.
- Bewerten der ereignisgesteuerten Architektur: Durch die Verwendung einer Serverless-Architektur können Sie auch eine ereignisgesteuerte Architektur für verteilte, auf Microservices basierende Anwendungen erstellen. So erhalten Sie skalierbare, resiliente, agile und kostengünstige Lösungen.

## Ressourcen

### Zugehörige Dokumente:

- [AWS Rechner für die Gesamtbetriebskosten \(\) TCO](#)
- [AWS Serverless](#)
- [Was ist ereignisgesteuerte Architektur \(EDA\)?](#)
- [Amazon-S3-Speicherklassen](#)
- [Cloud-Produkte](#)
- [Amazon ElastiCache \(RedisOSS\)](#)

### Zugehörige Beispiele:

- [Getting started with event-driven architecture](#)
- [Ereignisgesteuerte Architektur](#)
- [Wie Statsig mit Amazon ElastiCache \(Redis\) 100-mal kostengünstiger läuft OSS](#)
- [Bewährte Methoden für die Arbeit mit Funktionen AWS Lambda](#)

COST05-BP06 Führen Sie eine Kostenanalyse für unterschiedliche Nutzungen im Laufe der Zeit durch

Workloads können sich im Laufe der Zeit ändern. Einige Services oder Features sind auf unterschiedlichen Nutzungsebenen kostengünstiger. Wenn Sie jede Komponente im zeitlichen Verlauf und mit einer prognostizierten Nutzung analysieren, bleibt diese Workload über ihre gesamte Lebensdauer hinweg kostengünstig.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Mittel

### Implementierungsleitfaden

Mit der AWS Veröffentlichung neuer Dienste und Funktionen können sich die optimalen Dienste für Ihren Workload ändern. Der erforderliche Aufwand sollte potenzielle Vorteile widerspiegeln. Die Häufigkeit der Workload-Überprüfung hängt von den Anforderungen Ihrer Organisation ab. Wenn es sich um eine Workload mit erheblichen Kosten handelt, wird die Implementierung neuer Services früher die Kosteneinsparungen maximieren, sodass eine häufigere Überprüfung von Vorteil sein kann. Ein weiterer Auslöser für die Überprüfung ist die Änderung der Nutzungsmuster. Signifikante Änderungen bei der Nutzung können darauf hinweisen, dass alternative Services optimaler wären.

Wenn Sie Daten dorthin verschieben müssen AWS Cloud, können Sie eine Vielzahl von AWS Serviceangeboten und Partnertools auswählen, die Sie bei der Migration Ihrer Datensätze unterstützen, unabhängig davon, ob es sich dabei um Dateien, Datenbanken, Maschinenabbilder, Blockvolumes oder sogar Bandsicherungen handelt. Um beispielsweise große Datenmengen zu und von dort zu verschieben AWS oder Daten an der Peripherie zu verarbeiten, können Sie eines der AWS speziell entwickelten Geräte verwenden, um Petabyte an Daten kostengünstig offline zu verschieben. Ein anderes Beispiel: Bei höheren Datenübertragungsraten kann ein Direktverbindungsdienst günstiger sein als ein Dienst, der VPN die für Ihr Unternehmen erforderliche konsistente Konnektivität bietet.

Prüfen Sie Ihre Skalierungsaktivität basierend auf der Kostenanalyse für unterschiedliche Nutzungen im Laufe der Zeit. Analysieren Sie das Ergebnis, um herauszufinden, ob die Skalierungsrichtlinie so angepasst werden kann, dass Instances mit mehreren Instance-Typen und Kaufoptionen hinzugefügt werden können. Überprüfen Sie Ihre Einstellungen, um zu sehen, ob das Minimum zur Verarbeitung von Benutzeranfragen reduziert werden kann (jedoch mit einer kleineren Flottengröße), und fügen Sie mehr Ressourcen hinzu, um die erwartete hohe Nachfrage zu erfüllen.

Führen Sie eine Kostenanalyse für unterschiedliche Nutzungen im Lauf der Zeit durch, indem Sie mit Stakeholdern in Ihrer Organisation sprechen und das Prognosefeature von [AWS Cost Explorer](#) verwenden, um die potenziellen Auswirkungen von Serviceänderungen zu prognostizieren. Überwachen Sie den Nutzungsgrad von Markteinführungen mithilfe AWS Budgets von CloudWatch Abrechnungsalarmen und AWS Cost Anomaly Detection identifizieren und implementieren Sie die kostengünstigsten Dienste früher.

### Implementierungsschritte

- Definieren vorhergesagter Nutzungsmuster: Dokumentieren Sie in Zusammenarbeit mit Organisationbereichen, wie z. B. Marketing- und Produktbesitzern, wie die erwarteten und vorausgesagten Nutzungsmuster für die Workload aussehen werden. Sprechen Sie mit Business-Stakeholdern über historische und prognostizierte Kosten und gestiegene Nutzungen und stellen Sie sicher, dass solche Steigerungen mit den Geschäftsanforderungen übereinstimmen. Identifizieren Sie Kalendertage, Wochen oder Monate, an denen Sie davon ausgehen, dass mehr Benutzer Ihre AWS Ressourcen nutzen werden. Dies bedeutet, dass Sie die Kapazität der vorhandenen Ressourcen erhöhen oder zusätzliche Dienste einführen sollten, um die Kosten zu senken und die Leistung zu steigern.
- Durchführen einer Kostenanalyse bei vorhergesagter Nutzung: Führen Sie mithilfe der definierten Nutzungsmuster die Analyse an jedem dieser Punkte durch. Der Analyseaufwand sollte das potenzielle Ergebnis widerspiegeln. Wenn beispielsweise die Änderung der Nutzung groß ist, sollte

eine gründliche Analyse durchgeführt werden, um etwaige Kosten und Änderungen zu überprüfen. Mit anderen Worten: Wenn die Kosten steigen, sollte auch die Nutzung für Unternehmen zunehmen.

## Ressourcen

### Zugehörige Dokumente:

- [AWS Rechner für die Gesamtbetriebskosten \(TCO\)](#)
- [Amazon-S3-Speicherklassen](#)
- [Cloud-Produkte](#)
- [Amazon EC2 Auto Scaling](#)
- [Cloud-Datenmigration](#)
- [AWS Snow Family](#)

### Zugehörige Videos:

- [AWS OpsHub for Snow Family](#)

**COST6. Wie können Sie bei der Auswahl des Ressourcentyps, -umfangs und der Anzahl der Ressourcen Kostenziele erfüllen?**

Stellen Sie sicher, dass Sie den geeigneten Ressourcenumfang und die Anzahl der Ressourcen für die jeweilige Aufgabe auswählen. Durch die Auswahl des kostengünstigsten Typs, Umfangs und der kostengünstigsten Anzahl minimieren Sie die Verschwendung von Ressourcen.

## Bewährte Methoden

- [COST06-BP01 Kostenmodellierung durchführen](#)
- [COST06-BP02 Wählen Sie den Ressourcentyp, die Größe und die Anzahl anhand von Daten aus](#)
- [COST06-BP03 Wählen Sie den Ressourcentyp, die Größe und die Anzahl automatisch auf der Grundlage von Metriken](#)
- [COST06-BP04 Erwägen Sie die Verwendung gemeinsam genutzter Ressourcen](#)

## COST06-BP01 Kostenmodellierung durchführen

Identifizieren Sie die Anforderungen der Organisation (z. B. Geschäftsanforderungen und bestehende Verpflichtungen) und führen Sie eine Kostenmodellierung (Gesamtkosten) der Workload und aller ihrer Komponenten durch. Führen Sie Benchmark-Aktivitäten für die 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.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Hoch

### Implementierungsleitfaden

Führen Sie eine Kostenmodellierung für Ihre Workload und jede ihrer Komponenten durch, um das Gleichgewicht zwischen Ressourcen zu verstehen und die richtige Größe für jede Ressource in der Workload zu finden, unter Berücksichtigung eines bestimmten Leistungsgrads. Ein Verständnis der Kostenerwägungen kann den Geschäftsfall und die Entscheidungsfindung Ihrer Organisation bei der Bewertung der Ergebnisse der Wertrealisierung für die geplante Workload-Bereitstellung unterstützen.

Führen Sie Benchmark-Aktivitäten für die 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 proportional zu den Komponentenkosten oder prognostizierten Einsparungen sein. Bewährte Methoden finden Sie im [Abschnitt „Überprüfung“ der Säule „Leistungseffizienz“ des AWS Well-Architected Framework](#).

Beispiel: Zur Erstellung einer Kostenmodellierung für eine Workload, die aus Datenverarbeitungsressourcen besteht, kann [AWS Compute Optimizer](#) Sie bei der Kostenmodellierung für die Ausführung von Workloads unterstützen. Es bietet Empfehlungen zur richtigen Dimensionierung für Datenverarbeitungsressourcen basierend auf der bisherigen Nutzung. Stellen Sie sicher, dass CloudWatch Agenten auf den EC2 Amazon-Instances bereitgestellt werden, um Speichermetriken zu sammeln, die Ihnen dabei helfen, genauere Empfehlungen zu geben AWS Compute Optimizer. Dies ist die ideale Datenquelle für Datenverarbeitungsressourcen, da es sich um einen kostenlosen Service handelt, der Machine Learning nutzt, um je nach Risikograd mehrere Empfehlungen zu geben.

Es gibt [mehrere Dienste](#), die Sie mit benutzerdefinierten Protokollen als Datenquellen für die Anpassung von Vorgängen für andere Services und Workload-Komponenten wie [AWS Trusted](#)



[Advisor](#) [Amazon CloudWatch](#) und [Amazon CloudWatch Logs](#) verwenden können. AWS Trusted Advisor überprüft Ressourcen und kennzeichnet Ressourcen mit geringer Auslastung, was Ihnen helfen kann, Ihre Ressourcen richtig zu dimensionieren und Kostenmodelle zu erstellen.

Im Folgenden finden Sie Empfehlungen für die Kostenmodellierung von Daten und Metriken:

- Die Überwachung muss die Benutzererfahrung genau widerspiegeln. Wählen Sie die richtige Detaillierung für die Dauer aus, und wählen Sie das Maximum oder den 99. Perzentil statt des Durchschnitts aus.
- Wählen Sie die richtige Aufschlüsselung für die Dauer der Analyse aus, die für die Deckung der Workload-Zyklen erforderlich ist. Bei einer zweiwöchigen Analyse könnten Sie beispielsweise einen monatlichen Zyklus mit hoher Nutzung übersehen, der zu einer Unterbereitstellung führen könnte.
- Wählen Sie die richtigen AWS Services für Ihren geplanten Workload und berücksichtigen Sie dabei Ihre bestehenden Verpflichtungen, die ausgewählten Preismodelle für andere Workloads und die Fähigkeit, schneller zu innovieren und sich auf Ihr Kerngeschäft zu konzentrieren.

### Implementierungsschritte

- Durchführen einer Kostenmodellierung: Stellen Sie die Workload oder einen Machbarkeitsnachweis in einem separaten Konto mit den spezifischen zu testenden Ressourcentypen und -größen bereit. Führen Sie die Workload mit den Testdaten aus und zeichnen die Ergebnisse zusammen mit den Kostendaten zum Zeitpunkt der Testausführung auf. Anschließend stellen Sie die Workload erneut bereit oder ändern die Ressourcentypen und -umfänge und führen den Test noch einmal aus. Fügen Sie die Lizenzgebühren für alle Produkte, die Sie möglicherweise mit diesen Ressourcen verwenden, sowie die geschätzten Betriebskosten (Arbeits- oder Ingenieurkosten) für die Bereitstellung und Verwaltung dieser Ressourcen bei der Erstellung der Kostenmodelle hinzu. Erwägen Sie eine Kostenmodellierung für einen bestimmten Zeitraum (stündlich, täglich, monatlich, jährlich oder drei Jahre).

### Ressourcen

Zugehörige Dokumente:

- [AWS Auto Scaling](#)
- [Identifizieren von Möglichkeiten zur Größenanpassung](#)
- [CloudWatch Amazon-Funktionen](#)
- [Kostenoptimierung: Amazon EC2 Right Sizing](#)

- [AWS Compute Optimizer](#)
- [AWS Preisrechner](#)

Zugehörige Beispiele:

- [Perform a Data-Driven Cost Modelling](#)
- [Schätzen Sie die Kosten für geplante AWS Ressourcenkonfigurationen](#)
- [Wählen Sie die richtigen AWS Tools](#)

COST06-BP02 Wählen Sie den Ressourcentyp, die Größe und die Anzahl anhand von Daten aus

Wählen Sie die Ressourcengröße oder den -typ basierend auf Daten zur Workload und der Ressourcenmerkmale aus. Zu berücksichtigen sind hier beispielsweise Datenverarbeitung, Speicher, Durchsatz oder Schreibintensität. Diese Auswahl erfolgt in der Regel unter Verwendung einer früheren (On-Premises)-Version der Workload, der Dokumentation oder anderer Informationsquellen über die Workload.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Mittel

Implementierungsleitfaden

Amazon EC2 bietet eine große Auswahl an Instance-Typen mit unterschiedlichen Speicher-CPU, Speicher- und Netzwerkkapazitäten für unterschiedliche Anwendungsfälle. Diese Instance-Typen bieten unterschiedliche Kombinationen von Arbeitsspeicher-CPU, Speicher- und Netzwerkfunktionen, sodass Sie bei der Auswahl der richtigen Ressourcenkombination für Ihre Projekte vielseitig sind. Jeder Instance-Typ ist in mehreren Größen verfügbar, sodass Sie Ihre Ressourcen an die Anforderungen Ihrer Workload anpassen können. Um herauszufinden, welchen Instance-Typ Sie benötigen, informieren Sie sich über die Systemanforderungen der Anwendung oder Software, die Sie auf Ihrer Instance ausführen möchten. Diese Angaben sollten Folgendes umfassen:

- Betriebssystem
- Anzahl der CPU Kerne
- GPUkerne
- Größe des Systemspeichers (RAM)
- Speichertyp und Umgebung
- Anforderung an die Netzwerkbandbreite

Identifizieren Sie den Zweck der Rechenanforderungen und welche Instance benötigt wird, und erkunden Sie dann die verschiedenen EC2 Amazon-Instance-Familien. Amazon bietet die folgenden Instance-Typfamilien an:

- Allgemeine Zwecke
- Für Datenverarbeitung optimiert
- RAM-optimiert
- Speicheroptimiert
- Beschleunigte Datenverarbeitung
- HPCOptimiert

Ein tieferes Verständnis der spezifischen Zwecke und Anwendungsfälle, die eine bestimmte EC2 Amazon-Instance-Familie erfüllen kann, finden Sie unter [AWS Instance-Typen](#).

Die Erfassung der Systemanforderungen ist entscheidend, damit Sie die passende Instance-Familie und den geeigneten Instance-Typ für Ihre Anforderungen auswählen können. Die Namen der Instance-Typen setzen sich aus dem Familiennamen und der Größe der Instance zusammen. Die Instance „t2.micro“ zum Beispiel gehört zur T2-Familie und entspricht der Micro-Größe.

Wählen Sie die Ressourcengröße oder den -typ basierend auf der Workload und den Ressourcenmerkmalen aus (beispielsweise Datenverarbeitung, Speicher, Durchsatz oder Schreibintensität). Diese Auswahl erfolgt in der Regel unter Verwendung der Kostenmodellierung, einer früheren Version der Workload (z. B. einer On-Premises-Version), mithilfe der Dokumentation oder unter Verwendung anderer Informationsquellen über die Workload (Whitepaper, veröffentlichte Lösungen). AWS Die Verwendung von Preisrechnern oder Kostenmanagement-Tools kann dabei helfen, fundierte Entscheidungen über Instance-Typen, -Größen und -Konfigurationen zu treffen.

### Implementierungsschritte

- Auswahl von Ressourcen anhand von Daten: Verwenden Sie Ihre Kostenmodellierungsdaten, um den erwarteten Workload-Nutzungsgrad auszuwählen, und wählen Sie den angegebenen Ressourcentyp und die -größe aus. Ermitteln Sie anhand der Kostenmodellierungsdaten die Anzahl der virtuellen SpeicherCPUs, den Gesamtspeicher (GiB), das lokale Instance-Speichervolumen (GB), die EBS Amazon-Volumes und das Netzwerkleistungsniveau unter Berücksichtigung der für die Instance erforderlichen Datenübertragungsrate. Treffen Sie Ihre Auswahl stets auf Grundlage detaillierter Analysen und genauer Daten, um die Leistung zu optimieren und gleichzeitig die Kosten effektiv zu verwalten.

## Ressourcen

### Zugehörige Dokumente:

- [AWS Instance-Typen](#)
- [AWS Auto Scaling](#)
- [CloudWatch Amazon-Funktionen](#)
- [Kostenoptimierung: EC2 Richtige Dimensionierung](#)

### Zugehörige Videos:

- [Auswahl der richtigen EC2 Amazon-Instance für Ihre Workloads](#)
- [Right Size Your Services](#)

### Zugehörige Beispiele:

- [Es ist jetzt noch einfacher, EC2 Amazon-Instance-Typen zu entdecken und zu vergleichen](#)

COST06-BP03 Wählen Sie den Ressourcentyp, die Größe und die Anzahl automatisch auf der Grundlage von Metriken

Nutzen Sie Metriken aus der derzeit aktiven Workload für die Auswahl des richtigen Umfangs und Typs, um Kosten zu optimieren. Sorgen Sie für die richtige Bereitstellung von Durchsatz, Umfang und Speicher für Datenverarbeitungs-, Speicher-, Daten- und Netzwerkservices. Dies kann mit einer Feedback-Schleife wie automatische Skalierung oder durch benutzerdefinierten Code in der Workload erfolgen.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Niedrig

### Implementierungsleitfaden

Erstellen Sie eine Feedback-Schleife innerhalb der Workload, die aktive Metriken aus der laufenden Workload verwendet, um Änderungen an dieser Workload vorzunehmen. Sie können einen verwalteten Dienst verwenden, den Sie beispielsweise so konfigurieren [AWS Auto Scaling](#), dass er die für Sie richtigen Größenberechnungen durchführt. AWS bietet außerdem Funktionen [APIsSDKs](#), und, mit denen Ressourcen mit minimalem Aufwand geändert werden können. Sie können einen Workload für stop-and-start eine EC2 Amazon-Instance programmieren, um eine Änderung der

Instance-Größe oder des Instance-Typs zu ermöglichen. Dies bietet die Vorteile der richtigen Dimensionierung und eliminiert nahezu alle Betriebskosten, die für die Änderung erforderlich sind.

Einige AWS Dienste verfügen über eine integrierte automatische Typ- oder Größenauswahl, z. B. [Amazon Simple Storage Service Intelligent-Tiering](#). Amazon S3 Intelligent-Tiering verschiebt Ihre Daten basierend auf Ihren Nutzungsmustern automatisch zwischen den zwei Zugriffsebenen, häufiger Zugriff und seltener Zugriff.

## Implementierungsschritte

- Steigern der Beobachtbarkeit durch Konfigurieren von Workload-Metriken: Erfassen Sie wichtige Metriken für die Workload. Diese Kennzahlen geben Aufschluss über das Kundenerlebnis, z. B. die Workload-Leistung, und orientieren sich an den Unterschieden zwischen Ressourcentypen und -größen, z. B. CPU der Speicherauslastung. Analysieren Sie Leistungsdaten für Rechenressourcen, um Ihre EC2 Amazon-Instances richtig zu dimensionieren. Ermitteln Sie inaktive und nicht ausgelastete Instances. Die wichtigsten Kennzahlen, auf die Sie achten sollten, sind CPU Nutzung und Speicherauslastung (z. B. 40% CPU Auslastung in 90% der Fälle, wie unter [Rightsizing with AWS Compute Optimizer and Memory Utilization Enabled](#) beschrieben). Identifizieren Sie Instances mit einer maximalen CPU Nutzung und Speicherauslastung von weniger als 40% über einen Zeitraum von vier Wochen. Bei diesen Instances sollte die Größe angepasst werden, um die Kosten zu reduzieren. Für Speicherressourcen wie Amazon S3 können Sie [Amazon S3 Storage Lens](#) verwenden. Hiermit sehen Sie standardmäßig 28 Metriken aus unterschiedlichen Kategorien auf Bucket-Ebene sowie Verlaufsdaten aus 14 Tagen im Dashboard. Sie können das Dashboard von Amazon S3 Storage Lens nach Übersichtswerten und Kostenoptimierung oder nach Ereignissen sortieren, um bestimmte Metriken zu analysieren.
- Empfehlungen zur richtigen Dimensionierung anzeigen: Verwenden Sie die Empfehlungen zur richtigen Dimensionierung in AWS Compute Optimizer und das Amazon EC2 Rightsizing-Tool in der Kostenmanagement-Konsole, oder überprüfen Sie die richtige AWS Trusted Advisor Dimensionierung Ihrer Ressourcen, um Anpassungen an Ihrer Arbeitslast vorzunehmen. Es ist wichtig, bei der richtigen Dimensionierung verschiedener Ressourcen die [richtigen Tools](#) zu verwenden und die [Richtlinien zur richtigen Dimensionierung](#) zu befolgen, unabhängig davon, ob es sich um eine EC2 Amazon-Instance, AWS Speicherklassen oder RDS Amazon-Instance-Typen handelt. Bei Speicherressourcen können Sie Amazon S3 Storage Lens verwenden. Hiermit erhalten Sie Einblicke in die Objektspeichernutzung und Aktivitätstrends und finden Empfehlungen zur Kostenoptimierung und zum Anwenden von bewährten Methoden zum Schutz der Daten. Anhand der kontextbezogenen Empfehlungen, die [Amazon S3 Storage Lens](#) aus der Analyse von Metriken in Ihrer Organisation ableitet, können Sie direkt Schritte zur Speicheroptimierung ergreifen.

- Automatische Auswahl des Ressourcentyps und des Umfangs basierend auf Metriken: Mithilfe der Workload-Metriken können Sie Ihre Workload-Ressourcen manuell oder automatisch auswählen. Bei Datenverarbeitungsressourcen kann die Konfiguration von AWS Auto Scaling oder die Implementierung von Code in Ihrer Anwendung den Aufwand reduzieren, der bei häufigen Änderungen erforderlich ist. So lassen sich Änderungen möglicherweise früher implementieren, als dies mit einem manuellen Prozess der Fall wäre. Sie können eine Flotte von On-Demand-Instances und Spot-Instances innerhalb einer einzigen Auto-Scaling-Gruppe starten und automatisch skalieren. Zusätzlich zum Erhalt von Rabatten für die Verwendung von Spot-Instances können Sie mit Reserved Instances oder einem Savings Plan Rabatte auf die regulären On-Demand-Instance-Preise erhalten. All diese Faktoren zusammen helfen Ihnen dabei, Ihre Kosteneinsparungen für EC2 Amazon-Instances zu optimieren und den gewünschten Umfang und die gewünschte Leistung für Ihre Anwendung zu bestimmen. Sie können in [Auto Scaling Groups \(ASG\) auch eine auf Attributen basierende Strategie zur Auswahl des Instance-Typs \(ASG\)](#) verwenden, mit der Sie Ihre Instance-Anforderungen als eine Reihe von Attributen wie vCPU, Arbeitsspeicher und Speicher ausdrücken können. Sie können Instance-Typen der neueren Generation automatisch verwenden, wenn sie veröffentlicht werden, und mit Amazon EC2 Spot-Instances auf ein breiteres Kapazitätsspektrum zugreifen. Amazon EC2 Fleet und Amazon EC2 Auto Scaling wählen Instances aus und starten sie, die den angegebenen Attributen entsprechen, sodass die Instance-Typen nicht manuell ausgewählt werden müssen. Für Speicherressourcen können Sie die Funktionen [Amazon S3 Intelligent Tiering](#) und [Amazon EFS Infrequent Access](#) verwenden, mit denen Sie automatisch Speicherklassen auswählen können, die automatisch Speicherkosten sparen, wenn sich die Datenzugriffsmuster ändern, ohne dass sich dies auf die Leistung oder den Betriebsaufwand auswirkt.

## Ressourcen

### Zugehörige Dokumente:

- [AWS Auto Scaling](#)
- [AWS Die richtige Größe](#)
- [AWS Compute Optimizer](#)
- [CloudWatch Amazon-Funktionen](#)
- [CloudWatchEinrichtung](#)
- [CloudWatchVeröffentlichen benutzerdefinierter Metriken](#)
- [Erste Schritte mit Amazon EC2 Auto Scaling](#)
- [Amazon S3 Storage Lens](#)

- [Amazon S3 Intelligent-Tiering](#)
- [EFSSeltener Zugriff auf Amazon](#)
- [Starten Sie eine EC2 Amazon-Instance mit dem SDK](#)

Zugehörige Videos:

- [Right Size Your Services](#)

Zugehörige Beispiele:

- [Attributbasierte Instance-Typauswahl für Auto Scaling für Amazon EC2 Fleet](#)
- [Optimizing Amazon Elastic Container Service for cost using scheduled scaling](#)
- [Vorausschauende Skalierung mit Amazon EC2 Auto Scaling](#)
- [Optimieren Sie Kosten und erhalten Sie Einblick in die Nutzung mit Amazon S3 Storage Lens](#)
- [Well-Architected Labs: Rightsizing Recommendations \(Level 100\)](#)

COST06-BP04 Erwägen Sie die Verwendung gemeinsam genutzter Ressourcen

Bei bereits auf Organisationsebene für mehrere Geschäftseinheiten bereitgestellten Services sollten Sie erwägen, gemeinsam genutzte Ressourcen zu nutzen, um die Auslastung zu erhöhen und die Gesamtbetriebskosten zu senken (TCO). Die Verwendung gemeinsam genutzter Ressourcen kann eine kosteneffiziente Option sein, um Verwaltung und Kosten zu zentralisieren, indem bestehende Lösungen oder gemeinsam genutzte Komponenten oder beides verwendet werden. Verwalten Sie allgemeine Funktionen wie Überwachung, Sicherungen und Konnektivität entweder innerhalb einer Kontogrenze oder in einem dedizierten Konto. Sie können auch die Kosten senken, indem Sie Standardisierung implementieren und Duplizierung sowie Komplexität reduzieren.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Mittel

Implementierungsleitfaden

Wenn mehrere Workloads dieselbe Funktion ausführen, verwenden Sie vorhandene Lösungen und gemeinsam genutzte Komponenten, um Verwaltung und Kosten zu optimieren. Erwägen Sie die Nutzung vorhandener Ressourcen (insbesondere gemeinsam genutzter Ressourcen), z. B. Datenbankserver oder Verzeichnisservices, die nicht zur Produktion verwendet werden, um die Cloud-Kosten zu senken, indem Sie bewährte Sicherheitsmethoden und Organisationsvorschriften

befolgen. Für eine optimale Wertschöpfung und Effizienz ist entscheidend, die Kosten (mithilfe von Kostenauflistung und Rückbuchung) den relevanten Geschäftsbereichen zuzuordnen, die den Verbrauch antreiben.

Kostenauflistung bezieht sich auf Berichte, in denen die Cloud-Kosten in zuteilbare Kategorien wie Verbraucher, Geschäftseinheiten, Hauptbuchkonten oder andere verantwortliche Entitäten unterteilt werden. Mit Kostenaufstellungen sollen Teams, Geschäftseinheiten oder Einzelpersonen die Kosten ihrer verbrauchten Cloud-Ressourcen mitgeteilt werden.

Rückbuchung bedeutet, zentrale Serviceausgaben den Kostenträgern zuzuordnen, und zwar auf der Grundlage einer Strategie, die für einen bestimmten Finanzmanagementprozess geeignet ist. Für Kunden werden bei einer Rückbuchung die Kosten, die von einem Shared-Services-Konto anfallen, verschiedenen Finanzkostenkategorien zugeordnet, die für einen Kundenberichtsprozess geeignet sind. Durch die Einrichtung von Rückbuchungsmechanismen können Sie die Kosten melden, die verschiedenen Geschäftseinheiten, Produkten und Teams entstanden sind.

Workloads können als kritisch und unkritisch eingestuft werden. Verwenden Sie auf der Grundlage dieser Klassifizierung gemeinsam genutzte Ressourcen mit allgemeinen Konfigurationen für weniger kritische Workloads. Reservieren Sie dedizierte Server ausschließlich für kritische Workloads, um die Kosten weiter zu optimieren. Teilen Sie Ressourcen oder stellen Sie sie für mehrere Konten bereit, um sie effizient zu verwalten. Selbst in unterschiedlichen Entwicklungs-, Test- und Produktionsumgebungen ist eine sichere gemeinsame Nutzung möglich, ohne die Organisationsstruktur zu beeinträchtigen.

Verwenden Sie Daten zur Zuordnung geteilter Kosten, mit deren Hilfe Sie die Kosten einzelner Geschäftsentitäten basierend auf der Verwendung gemeinsam genutzter Datenverarbeitungs- und Speicherressourcen durch die Anwendung zuordnen können, um Ihr Verständnis zu verbessern und die Kosten und Nutzung für containerisierte Anwendungen zu optimieren. Daten zur geteilten Kostenzuweisung helfen Ihnen dabei, Showback und Chargeback auf Aufgabenebene bei Container-Workloads zu erreichen, die auf Amazon Elastic Container Service (AmazonECS) oder Amazon Elastic Kubernetes Service (Amazon) ausgeführt werden. EKS

Für verteilte Architekturen sollten Sie Shared Services erstellen, die einen zentralen Zugriff auf gemeinsam genutzte Dienste bieten. VPCs, die für die Workloads in den einzelnen Architekturen erforderlich sind. Diese gemeinsamen Dienste können Ressourcen wie Verzeichnisdienste oder VPC Endpunkte umfassen. Um den Verwaltungsaufwand und die Kosten zu reduzieren, sollten Sie Ressourcen von einem zentralen Standort aus gemeinsam nutzen, anstatt sie in jedem VPC zu bündeln.



Durch die Verwendung gemeinsam genutzter Ressourcen können Sie Betriebskosten sparen, die Ressourcenauslastung maximieren und die Konsistenz verbessern. Bei einem Design mit mehreren Konten können Sie einige AWS Dienste zentral hosten und über mehrere Anwendungen und Konten in einem Hub auf sie zugreifen, um Kosten zu sparen. Sie können [AWS Resource Access Manager \(AWS RAM\)](#) verwenden, um andere gemeinsame Ressourcen wie [VPCSubnetze und AWS Transit Gateway Anlagen](#) oder [SageMaker Amazon-Pipelines](#) gemeinsam zu nutzen. [AWS Network Firewall](#) Verwenden Sie in einer Umgebung mit mehreren Konten, AWS RAM um eine Ressource einmal zu erstellen und sie mit anderen Konten zu teilen.

Organisationen sollten die geteilten Kosten effektiv markieren und sicherstellen, dass kein erheblicher Teil ihrer Kosten unmarkiert oder nicht zugewiesen ist. Wenn Sie die gemeinsamen Kosten nicht effektiv verteilen und niemand die Verantwortung für die Verwaltung gemeinsamer übernimmt, können die Kosten für eine gemeinsame Cloud in die Höhe schießen. Sie müssen sich bewusst sein, wo Kosten auf Ressourcen-, Workload-, Team- oder Organisationsebene entstanden sind, da dieses Wissen Ihr Verständnis für den auf der jeweiligen Ebene geschaffenen Mehrwert im Vergleich zu den erzielten Geschäftsergebnissen verbessert. Letztlich profitieren Organisationen von Kosteneinsparungen, die sich aus der gemeinsamen Nutzung der Cloud-Infrastruktur ergeben. Fördern Sie die Kostenzuordnung für gemeinsam genutzte Cloud-Ressourcen, um die Cloud-Ausgaben zu optimieren.

### Implementierungsschritte

- **Vorhandene Ressourcen bewerten:** Prüfen Sie bestehende Workloads, die ähnliche Services für Ihre Workload verwenden. Ziehen Sie abhängig von den Komponenten der Workload vorhandene Plattformen in Betracht, sofern die Geschäftslogik oder die technischen Anforderungen dies zulassen.
- **Verwenden Sie die gemeinsame Nutzung von Ressourcen in AWS RAM** und schränken Sie sie entsprechend ein: Verwenden Sie diese Option AWS RAM , um Ressourcen mit anderen AWS Konten innerhalb Ihrer Organisation gemeinsam zu nutzen. Wenn Sie Ressourcen gemeinsam nutzen, müssen Sie Ressourcen nicht in mehreren Konten duplizieren, wodurch der betriebliche Aufwand der Ressourcenverwaltung minimiert wird. Dieser Prozess unterstützt die sichere Freigabe der Ressourcen, die Sie erstellt haben, an Rollen und Benutzer in Ihrem Konto sowie an andere AWS-Konten.
- **Ressourcen taggen:** Taggen Sie Ressourcen, die für die Kostenberichterstattung infrage kommen, und kategorisieren Sie sie in Kostenkategorien. Aktivieren Sie diese kostenbezogenen Ressourcen-Tags für die Kostenzuweisung, um einen Überblick über die AWS Ressourcennutzung zu erhalten. Konzentrieren Sie sich darauf, ein angemessenes Maß an Granularität in Bezug auf

Kosten- und Nutzungstransparenz zu schaffen und beeinflussen Sie das Verhalten der Cloud-Nutzung durch Berichte und Nachverfolgung der Kostenzuweisung. KPI

## Ressourcen

Zugehörige bewährte Methoden:

- [SEC03-BP08 Teilen Sie Ressourcen sicher innerhalb Ihrer Organisation](#)

Zugehörige Dokumente:

- [Was ist? AWS Resource Access Manager](#)
- [AWS Dienste, die Sie mit nutzen können AWS Organizations](#)
- [Gemeinsam nutzbare Ressourcen AWS](#)
- [AWS Fragen zu Kosten und Nutzung \(CUR\)](#)

Zugehörige Videos:

- [AWS Resource Access Manager - Granulare Zugriffskontrolle mit verwalteten Berechtigungen](#)
- [Wie gestalten Sie Ihre Strategie zur AWS Kostenverteilung](#)
- [AWS Cost Categories](#)

Zugehörige Beispiele:

- [So führen Sie Chargeback Shared Services durch: Ein Beispiel AWS Transit Gateway](#)
- [So erstellen Sie ein Chargeback-/Showback-Modell für Savings Plans mit dem CUR](#)
- [Nutzung von VPC Sharing für eine kostengünstige Microservice-Architektur mit mehreren Konten](#)
- [Verbessern Sie die Kostentransparenz von Amazon EKS mit AWS Split Cost Allocation Data](#)
- [Verbessern Sie die Kostentransparenz von Amazon ECS und AWS Batch mit AWS Split Cost Allocation Data](#)

## COST7. 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

- [COST07-BP01 Führen Sie eine Preismodellanalyse durch](#)
- [COST07-BP02 Wählen Sie Regionen nach Kosten](#)
- [COST07-BP03 Wählen Sie Verträge mit Drittanbietern mit kostengünstigen Konditionen aus](#)
- [COST07-BP04 Implementieren Sie Preismodelle für alle Komponenten dieses Workloads](#)
- [COST07-BP05 Führen Sie eine Preismodellanalyse auf Verwaltungskontoebene durch](#)

### COST07-BP01 Führen Sie eine Preismodellanalyse durch

Analysieren Sie die einzelnen Komponenten der Workload. Stellen Sie fest, ob die Komponente und die Ressourcen über einen längeren Zeitraum (für Bindungsrabatte) oder dynamisch und kurz ausgeführt werden (für Spot- oder On-Demand-Zwecke). Analysieren Sie die Workload mithilfe der Empfehlungen in Tools für die Kostenverwaltung und wenden Sie Geschäftsregeln auf diese Empfehlungen an, um hohe Erträge zu erzielen.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Hoch

### Implementierungsleitfaden

AWS verfügt über mehrere [Preismodelle](#), mit denen Sie Ihre Ressourcen auf die kostengünstigste Weise bezahlen können, die den Bedürfnissen Ihres Unternehmens und je nach Produkt entspricht. Arbeiten Sie mit Ihren Teams zusammen, um das am besten geeignete Preismodell zu bestimmen. Häufig besteht das Preismodell aus einer Kombination aus verschiedenen Optionen, die sich nach Ihrer Verfügbarkeit richtet.

Mit On-Demand-Instances zahlen Sie für die Datenverarbeitungs- oder Datenbankkapazitäten auf Stunden- oder Sekundenbasis (mindestens 60 Sekunden), abhängig von den Instances, die Sie ausführen. Es sind keine langfristigen Verpflichtungen oder Vorauszahlungen erforderlich.

Savings Plans sind ein flexibles Preismodell, das niedrige Preise für AmazonEC2, Lambda und AWS Fargate Nutzung bietet und im Gegenzug eine Verpflichtung zu einer gleichbleibenden Nutzungsdauer (gemessen in Dollar pro Stunde) über eine Laufzeit von einem Jahr oder drei Jahren bietet.

Spot-Instances sind ein EC2 Amazon-Preismechanismus, mit dem Sie freie Rechenkapazität zu einem vergünstigten Stundensatz (bis zu 90% Rabatt auf den On-Demand-Preis) ohne vorherige Verpflichtung anfordern können.

Mit Reserved Instances zahlen Sie im Voraus für die Kapazität und erhalten bis zu 75 Prozent Rabatt. Weitere Informationen finden Sie unter [Kostenoptimierung mit Reservierungen](#).

Sie könnten einen Savings Plan für die mit der Produktion, der Qualität und den Entwicklungsumgebungen verbundenen Ressourcen hinzufügen. Da Sandbox-Ressourcen nur bei Bedarf aktiviert werden, könnten Sie alternativ ein On-Demand-Modell für die Ressourcen in dieser Umgebung wählen. Verwenden Sie Amazon [Spot-Instances](#), um die EC2 Amazon-Kosten zu senken, oder verwenden Sie [Compute Savings Plans](#), um die Kosten für AmazonEC2, Fargate und Lambda zu senken. Das Empfehlungstool [AWS Cost Explorer](#) stellt Möglichkeiten für an feste Kapazität gebundene Rabatte mit Savings Plans vor.

Wenn Sie EC2 in der Vergangenheit [Reserved Instances](#) für Amazon gekauft haben oder innerhalb Ihres Unternehmens Verfahren zur Kostenverteilung eingeführt haben, können Sie Amazon EC2 Reserved Instances vorerst weiterhin verwenden. Wir empfehlen jedoch, eine Strategie für die zukünftige Verwendung von Savings Plans als flexibleren Mechanismus zur Kostenreduzierung zu entwickeln. Sie können die Empfehlungen für Savings Plans (SP) aktualisieren AWS Cost Management, um jederzeit neue Sparplanempfehlungen zu generieren. Verwenden Sie Reserved Instances (RI), um die Kosten für AmazonRDS, Amazon Redshift ElastiCache, Amazon und Amazon OpenSearch Service zu senken. Es stehen drei Optionen für Savings Plans und Reserved Instances zur Verfügung: vollständige Vorauszahlung, teilweise Vorauszahlung und keine Vorauszahlung. Verwenden Sie die Empfehlungen in den Kaufempfehlungen von AWS Cost Explorer RI und SP.

Um Möglichkeiten für Spot-Workloads zu finden, verwenden Sie eine stündliche Ansicht Ihrer Gesamtnutzung und suchen Sie nach regelmäßigen Zeiträumen mit sich ändernder Nutzung oder Elastizität. Sie können Spot-Instances für verschiedene fehlertolerante und flexible Anwendungen verwenden. Beispiele hierfür sind statusfreie Webserver, API Endpunkte, Big-Data- und Analyseanwendungen, containerisierte Workloads, CI/CD und andere flexible Workloads.

Analysieren Sie Ihre Amazon EC2 - und RDS Amazon-Instances, ob sie ausgeschaltet werden können, wenn Sie sie nicht verwenden (außerhalb der Geschäftszeiten und am Wochenende). Dadurch können Sie die Kosten verglichen mit einem Einsatz rund um die Uhr um 70 % oder mehr reduzieren. Wenn Sie über Amazon-Redshift-Cluster verfügen, die nur zu bestimmten Zeiten verfügbar sein müssen, können Sie den Cluster anhalten und zu einem späteren Zeitpunkt neu starten. Wenn der Amazon Redshift Redshift-Cluster oder Amazon EC2 and Amazon RDS Instance gestoppt wird, wird die Rechenabrechnung gestoppt und es fallen nur die Speichergebühren an.

Beachten Sie, dass [Kapazitätsreservierungen auf Abruf](#) (ODCR) kein Preisnachlass sind. Für Kapazitätsreservierungen wird Ihnen der entsprechende On-Demand-Tarif in Rechnung gestellt, unabhängig davon, ob Sie Instances mit der reservierten Kapazität ausführen oder nicht. Sie sollten

in Betracht gezogen werden, wenn Sie ausreichend Kapazität für die Ressourcen bereitstellen müssen, die Sie ausführen möchten. ODCRsmüssen nicht an langfristige Verpflichtungen gebunden sein, da sie gekündigt werden können, wenn Sie sie nicht mehr benötigen. Sie können aber auch von den Rabatten profitieren, die Savings Plans oder Reserved Instances bieten.

## Implementierungsschritte

- Analysieren der Workload-Elastizität: Verwenden Sie die stündliche Granularität in Cost Explorer oder ein benutzerdefiniertes Dashboard, um die Elastizität Ihrer Workloads zu analysieren. Suchen Sie nach regelmäßigen Änderungen hinsichtlich der Anzahl der Instances, die ausgeführt werden. Instances mit kurzer Dauer sind Kandidaten für Spot Instances oder Spot-Flotte.
  - [Well-Architected Lab: Cost Explorer](#)
  - [Well-Architected Lab: Cost Visualization](#)
- Überprüfen bestehender Preisverträge: Überprüfen Sie laufende Verträge oder Verpflichtungen für langfristige Anforderungen. Analysieren Sie, was Sie aktuell haben und inwiefern diese Verpflichtungen genutzt werden. Nutzen Sie bereits vorhandene vertragliche Rabatte oder Unternehmensverträge. [Unternehmensverträge](#) bieten Kunden die Möglichkeit, Verträge so zu gestalten, dass sie ihren Bedürfnissen am besten entsprechen. Bei langfristigen Verpflichtungen sollten Sie Preisnachlässe für Reserved, Reserved Instances oder Savings Plans für den jeweiligen Instance-Typ, die Instance-Familie und Availability Zones in Betracht ziehen. AWS-Region
- Durchführen einer Analyse des Bindungsrabatts: Sehen Sie sich unter Verwendung von Cost Explorer in Ihrem Konto die Empfehlungen für Savings Plans und Reserved Instances an. Um sicherzustellen, dass Sie die richtigen Empfehlungen mit den erforderlichen Rabatten und Risiken implementieren, befolgen Sie die [Well-Architected Labs](#).

## Ressourcen

### Zugehörige Dokumente:

- [Zugriff auf Empfehlungen für Reserved Instances](#)
- [Instance-Kaufoptionen](#)
- [AWS Unternehmen](#)

### Zugehörige Videos:

- [Save up to 90% and run production workloads on Spot](#)

## Zugehörige Beispiele:

- [Well-Architected Lab: Cost Explorer](#)
- [Well-Architected Lab: Cost Visualization](#)
- [Well-Architected Lab: Pricing Models](#)

## COST07-BP02 Wählen Sie Regionen nach Kosten

Ressourcenpreise können je nach Region abweichen. Ermitteln Sie regionale Kostenunterschiede und stellen Sie nur in Regionen mit höheren Kosten bereit, um die Anforderungen an Latenzzeiten, Datenresidenz und Datensouveränität zu erfüllen. Die Berücksichtigung der Regionalkosten sorgt dafür, dass Sie den niedrigsten Gesamtpreis für diese Workload zahlen.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Mittel

## Implementierungsleitfaden

Die [AWS Cloud Infrastruktur](#) ist global, wird [an mehreren Standorten weltweit](#) gehostet und basiert auf Availability Zones AWS-Regionen, Local Zones, AWS Outposts und Wavelength Zones. Eine Region ist ein physischer Standort auf der Welt, und jede Region ist ein separates geografisches Gebiet AWS mit mehreren Availability Zones. Availability Zones sind mehrere isolierte Standorte innerhalb jeder Region. Sie bestehen aus mindestens einem eigenständigen Rechenzentrum mit einer redundanten Stromversorgung, einem Netzwerk sowie Konnektivität.

Jede Region AWS-Region arbeitet innerhalb der lokalen Marktbedingungen, und die Preise für Ressourcen sind in jeder Region unterschiedlich, beispielsweise aufgrund von Unterschieden bei den Kosten für Land, Glasfaser, Strom und Steuern. Wählen Sie eine spezifische Region aus, in der Sie eine Komponente oder Ihre gesamte Lösung ausführen möchten, sodass Sie weltweit einen Betrieb zu den geringstmöglichen Kosten gewährleisten. Mit [AWS Calculator](#) können Sie die Kosten Ihrer Workload in verschiedenen Regionen einschätzen. Suchen Sie dazu Services nach Standorttyp (Region, Wavelength Zone und Local Zone) und Region.

Wenn Sie die Architektur Ihrer Lösungen aufbauen, hat es sich bewährt zu versuchen, Computing-Ressourcen zugunsten einer geringeren Latenz und einer stärkeren Datensouveränität näher an die Benutzer zu bringen. Wählen Sie den geografischen Standort auf der Grundlage Ihrer Geschäfts-, Datenschutz-, Leistungs- und Sicherheitsanforderungen. Verwenden Sie für Anwendungen mit globalen Endbenutzern mehrere Standorte.

Verwenden Sie Regionen, die niedrigere Preise für AWS Dienste anbieten, um Ihre Workloads bereitzustellen, wenn Sie keine Verpflichtungen in Bezug auf Datenschutz, Sicherheit und Geschäftsanforderungen haben. Wenn Ihre Standardregion beispielsweise Asien-Pazifik (Sydney) (ap-southwest-2) ist und es keine Einschränkungen (z. B. Datenschutz, Sicherheit) für die Nutzung anderer Regionen gibt, kostet Sie die Bereitstellung unkritischer EC2 Amazon-Instances (Entwicklung und Test) in USA Ost (Nord-Virginia-east-1) () weniger.

	<i>Compliance</i>	<i>Latenz</i>	<i>Kosten</i>	<i>Services/Funktionen</i>
<i>Region 1</i>	✓	15 ms	\$\$	✓
<i>Region 2</i>	✓	20 ms	\$\$\$	X
<i>Region 3</i>	✓	80 ms	\$	✓
<i>Region 4</i>	✓	15 ms	\$\$	✓
<i>Region 5</i>	✓	20 ms	\$\$\$	X
<b>Region 6</b>	✓	15 ms	\$	✓
<i>Region 7</i>	✓	80 ms	\$	✓
<i>Region 8</i>	✓	15 ms	\$	X

### Matrixtabelle für Regionsfeatures

Die obige Matrixtabelle zeigt uns, dass Region 6 die beste Option für dieses gegebene Szenario ist, da die Latenz im Vergleich zu anderen Regionen gering ist, der Service verfügbar ist und es sich um die kostengünstigste Region handelt.

### Implementierungsschritte

- **AWS-Region Preisgestaltung überprüfen:** Analysieren Sie die Workload-Kosten in der aktuellen Region. Berechnen Sie die Kosten in anderen verfügbaren Regionen, beginnend mit den höchsten Kosten nach Service und Verwendungstyp. Migrieren Sie in die neue Region, wenn die prognostizierte Einsparung die Kosten für das Verschieben der Komponente oder der Workload überwiegt.
- **Überprüfen der Anforderungen für Bereitstellungen in mehreren Regionen:** Analysieren Sie Ihre geschäftlichen Anforderungen und Verpflichtungen (Datenschutz, Sicherheit oder Leistung),

um herauszufinden, ob für Sie Beschränkungen gelten, sodass Sie nicht mehrere Regionen verwenden können. Wenn Sie sich nicht auf eine einzelne Region beschränken müssen, verwenden Sie mehrere Regionen.

- Analysieren der erforderlichen Datenübertragungen: Berücksichtigen Sie bei der Auswahl von Regionen die Datenübertragungskosten. Halten Sie Ihre Daten in der Nähe des Kunden und in der Nähe der Ressourcen. Wählen Sie aus AWS-Regionen, wo Daten weniger kostspielig fließen und wo nur minimale Datenübertragungen stattfinden. Je nach Ihren Geschäftsanforderungen an die Datenübertragung können Sie [Amazon](#),, und verwenden CloudFront [AWS PrivateLink](#)[AWS Direct Connect](#), um Ihre Nettwerkkosten [AWS Virtual Private Network](#) zu senken, die Leistung zu verbessern und die Sicherheit zu erhöhen.

## Ressourcen

### Zugehörige Dokumente:

- [Zugriff auf Empfehlungen für Reserved Instances](#)
- [EC2 Amazon-Preisgestaltung](#)
- [Instance-Kaufoptionen](#)
- [Tabelle „Region“](#)

### Zugehörige Videos:

- [Save up to 90% and run production workloads on Spot](#)

### Zugehörige Beispiele:

- [Überblick über die Datenübertragungskosten für gängige Architekturen](#)
- [Kostenerwägungen für globale Bereitstellungen](#)
- [What to Consider when Selecting a Region for your Workloads](#)
- [Well-Architected Labs: Restrict service usage by Region \(Level 200\)](#)

COST07-BP03 Wählen Sie Verträge mit Drittanbietern mit kostengünstigen Konditionen aus

Kosteneffiziente Vereinbarungen und Bedingungen stellen sicher, dass die Kosten dieser Services mit den von ihnen bereitgestellten Vorteilen skaliert werden. Wählen Sie Vereinbarungen und Preise aus, die skaliert werden, wenn sie Ihrer Organisation zusätzliche Vorteile bieten.



## Risikostufe bei fehlender Befolgung dieser bewährten Methode: Mittel

### Implementierungsleitfaden

Es gibt mehrere Produkte auf dem Markt, die Ihnen helfen, die Kosten für Ihre Cloud-Umgebungen zu verwalten. Sie unterscheiden sich teilweise in Bezug auf die Features, die von den Bedürfnissen der Kunden abhängen. So konzentrieren sich einige auf die Kostenkontrolle oder Kostentransparenz und andere auf die Kostenoptimierung. Ein Schlüsselfaktor für eine effektive Kostenoptimierung und Governance ist die Verwendung des richtigen Tools mit den erforderlichen Features und dem richtigen Preismodell. Diese Produkte unterscheiden sich in ihren Preismodellen. Bei manchen wird ein bestimmter Prozentsatz Ihrer monatlichen Rechnung berechnet, bei anderen ein Prozentsatz Ihrer erzielten Einsparungen. Im Idealfall sollten Sie nur für das bezahlen, was Sie benötigen.

Wenn Sie Lösungen oder Services von Drittanbietern in der Cloud nutzen, ist es wichtig, dass die Preisstrukturen an Ihren gewünschten Ergebnissen ausgerichtet sind. Preise sollten mit den Ergebnissen und dem Wert skaliert werden, den sie bieten. Beispielsweise kostet Software, deren Preis auf einem Prozentsatz der erzielten Einsparungen basiert, umso mehr, je mehr Sie sparen (Ergebnis). Lizenzvereinbarungen, bei denen Sie mit steigenden Ausgaben mehr bezahlen, sind möglicherweise nicht immer in Ihrem Interesse, um die Kosten zu optimieren. Wenn der Anbieter jedoch klare Vorteile für alle Bestandteile Ihrer Rechnung bietet, könnte diese Preisstaffelung gerechtfertigt sein.

Beispielsweise kann eine Lösung, die Empfehlungen für Amazon enthält EC2 und einen Prozentsatz Ihrer gesamten Rechnung berechnet, teurer werden, wenn Sie andere Dienste nutzen, die keinen Nutzen bieten. Ein weiteres Beispiel ist ein verwalteter Service, der zu einem Prozentsatz der Kosten für verwaltete Ressourcen in Rechnung gestellt wird. Eine höhere Instance-Größe erfordert möglicherweise nicht notwendigerweise mehr Verwaltungsaufwand, kann aber teurer werden. Stellen Sie sicher, dass diese Service-Preisvereinbarungen ein Kostenoptimierungsprogramm oder entsprechende Features in ihrem Service enthalten, um die Effizienz zu steigern.

Die Kunden finden diese auf dem Markt befindlichen Produkte vielleicht fortschrittlicher oder benutzerfreundlicher. Sie müssen die Kosten für diese Produkte berücksichtigen und über mögliche langfristige Kostenoptimierungen nachdenken.

### Implementierungsschritte

- Analyse von Vereinbarungen und Bedingungen Dritter: Überprüfen Sie die Preise in Drittanbietervereinbarungen. Führen Sie die Modellierung für verschiedene Nutzungsebenen durch und berücksichtigen Sie neue Kosten, wie z. B. die Nutzung neuer Services oder Erweiterungen

der aktuellen Services aufgrund des Workload-Wachstums. Entscheiden Sie, ob die zusätzlichen Kosten Ihrem Unternehmen die erforderlichen Vorteile bieten.

## Ressourcen

### Zugehörige Dokumente:

- [Zugriff auf Empfehlungen für Reserved Instances](#)
- [Instance-Kaufoptionen](#)

### Zugehörige Videos:

- [Save up to 90% and run production workloads on Spot](#)

COST07-BP04 Implementieren Sie Preismodelle für alle Komponenten dieses Workloads

Dauerhaft ausgeführte Ressourcen sollten reservierte Kapazität wie Savings Plans oder Reserved Instances nutzen. Die kurzfristige Kapazität wird für die Verwendung von Spot Instances 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 Zeitraums, je nach Ressourcentyp.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Niedrig

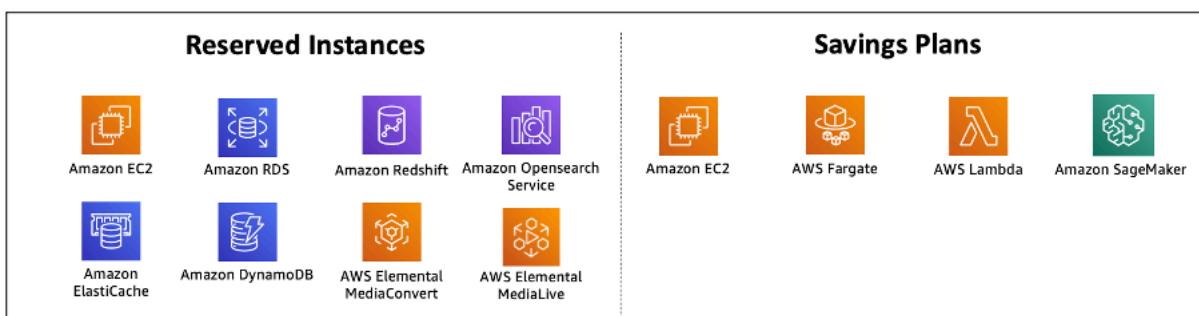
## Implementierungsleitfaden

Zur Verbesserung der Kosteneffizienz AWS gibt es mehrere verbindliche Empfehlungen, die auf Ihrer bisherigen Nutzung basieren. Anhand dieser Empfehlungen können Sie nachvollziehen, was Sie einsparen können und wie die Verpflichtung verwendet wird. Sie können diese Dienste als On-Demand-Dienste oder Spot-Dienste nutzen oder eine Verpflichtung für einen bestimmten Zeitraum eingehen und Ihre On-Demand-Kosten mit Reserved Instances (RIs) und Savings Plans (SPs) senken. Um Ihren Workload zu optimieren, müssen Sie nicht nur die einzelnen Workload-Komponenten und die verschiedenen AWS Services kennen, sondern auch die Tarife, Kaufoptionen und Spot-Instances für diese Services kennen.

Beachten Sie die Anforderungen der jeweiligen Workload-Komponenten sowie die verschiedenen Preismodelle für diese Services. Definieren Sie die Verfügbarkeitsanforderungen dieser Komponenten. Stellen Sie fest, ob mehrere unabhängige Ressourcen vorhanden sind, die die Funktion in der Workload ausführen, und welche Workload-Anforderungen im Laufe der Zeit

gelten. Vergleichen Sie die Kosten der Ressourcen unter Verwendung des standardmäßigen On-Demand-Preismodells und anderer anwendbarer Modelle. Beziehen Sie potenzielle Änderungen in Ressourcen oder Workload-Komponenten in Ihre Überlegungen ein.

Sehen wir uns zum Beispiel diese Webanwendungsarchitektur in AWS an. Dieser Beispiel-Workload besteht aus mehreren AWS Services wie Amazon Route 53, Amazon AWS WAF, EC2 Amazon-Instances CloudFront, RDS Amazon-Instances, Load Balancers, Amazon S3-Speicher und Amazon Elastic File System (AmazonEFS). Sie müssen jeden dieser Services überprüfen und mögliche Kosteneinsparungen durch die verschiedenen Preismodelle ermitteln. Einige von ihnen kommen möglicherweise für RIs oder in FrageSPs, während andere möglicherweise nur auf Abruf verfügbar sind. Wie die folgende Abbildung zeigt, können einige AWS Dienste mithilfe von RIs oder aktiviert werdenSPs.



AWS Dienste, die mithilfe von Reserved Instances und Savings Plans zugesagt wurden

### Implementierungsschritte

- Implementieren von Preismodellen: Kaufen Sie anhand Ihrer Analyseergebnisse Savings Plans, Reserved Instances oder implementieren Sie Spot Instances. Wenn es sich um Ihren ersten Abonnementkauf handelt, wählen Sie die fünf oder zehn wichtigsten Empfehlungen in der Liste aus und beobachten und analysieren Sie dann die Ergebnisse in den nächsten ein bis zwei Monaten. AWS Cost Management Console führt Sie durch den Prozess. Überprüfen Sie die RI- oder SP-Empfehlungen von der Konsole aus, passen Sie die Empfehlungen an (Typ, Zahlung und Laufzeit) und überprüfen Sie die stündliche Verpflichtung (z. B. 20 USD pro Stunde) und legen Sie sie dann in den Warenkorb. Die Rabatte gelten automatisch für die berechnete Nutzung. Erwerben Sie in regelmäßigen Zyklen eine geringe Anzahl von Bindungsrabatten, (z. B. alle 2 Wochen oder monatlich). Implementieren Sie Spot Instances für Workloads, die unterbrochen werden können oder zustandslos sind. Wählen Sie abschließend EC2 On-Demand-Amazon-Instances aus und weisen Sie Ressourcen für die verbleibenden Anforderungen zu.
- Workload-Überprüfungszyklus: Implementieren Sie einen Überprüfungszyklus für die Workload, der speziell die Abdeckung des Preismodells analysiert. Sobald der Workload den erforderlichen

Umfang erreicht hat, können Sie teilweise (alle paar Monate) oder wenn sich die Nutzung Ihrer Organisation ändert, zusätzliche Bindungsrabatte erwerben.

## Ressourcen

### Zugehörige Dokumente:

- [Understanding your Savings Plans recommendations](#)
- [Zugriff auf Empfehlungen für Reserved Instances](#)
- [Erwerb von Reserved Instances](#)
- [Instance-Kaufoptionen](#)
- [Spot Instances](#)
- [Reservierungsmodelle für andere Dienste AWS](#)
- [Savings Plans Supported Services](#)

### Zugehörige Videos:

- [Save up to 90% and run production workloads on Spot](#)

### Zugehörige Beispiele:

- [Was sollte ich vor dem Kauf eines Savings Plan beachten?](#)
- [Wie kann ich den Cost Explorer verwenden, um meine Ausgaben und Nutzung zu analysieren?](#)

COST07-BP05 Führen Sie eine Preismodellanalyse auf Verwaltungskontoebene durch

Prüfen Sie die Tools für die Fakturierung und Kostenverwaltung und informieren Sie sich über empfohlene Rabatte bei Bindung und Reservierungen, um regelmäßige Analysen auf Ebene des Verwaltungskontos auszuführen.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Niedrig

## Implementierungsleitfaden

Durch die regelmäßige Kostenmodellierung können Sie Möglichkeiten zur Optimierung über mehrere Workloads hinweg implementieren. Wenn beispielsweise mehrere Workloads On-Demand-Instances

verwenden, ist das Änderungsrisiko insgesamt niedriger und die Nutzung eines auf fester Kapazität basierenden Rabatts kann zu niedrigeren Gesamtkosten führen. Es wird empfohlen, Analysen in regelmäßigen Zyklen von zwei Wochen bis zu einem Monat durchzuführen. Auf diese Weise können Sie kleine Anpassungskäufe tätigen, sodass sich die Abdeckung Ihrer Preismodelle mit Ihren sich ändernden Workloads und ihren Komponenten weiter entwickelt.

Verwenden Sie das Empfehlungstool [AWS Cost Explorer](#), um Möglichkeiten für an feste Kapazität gebundene Rabatte in Ihrem Verwaltungskonto zu finden. Empfehlungen auf Ebene des Verwaltungskontos werden unter Berücksichtigung der Nutzung aller Konten in Ihrer AWS - Organisation berechnet, die über Reserved Instances (RI) oder Savings Plans (SP) verfügen. Sie werden auch berechnet, wenn die Rabattteilung aktiviert ist, um eine Festlegung zu empfehlen, mit der die Ersparnisse auf allen Konten maximiert werden.

Beim Kauf auf Verwaltungskontoebene werden in vielen Fällen maximale Einsparungen erzielt. Es kann jedoch Situationen geben, in denen Sie den Kauf SPs auf der Ebene des verknüpften Kontos in Betracht ziehen könnten, z. B. wenn Sie möchten, dass die Rabatte zuerst für die Nutzung in diesem bestimmten verknüpften Konto gelten. Empfehlungen für Mitgliedskonten werden auf Ebene der einzelnen Konten berechnet, um die Einsparungen für das jeweilige Konto zu maximieren. Wenn Ihr Konto sowohl RI- als auch SP-Bindungen umfasst, werden diese in der folgenden Reihenfolge angewendet:

1. Zonen-RI
2. Standard-RI
3. Konvertierbare RI
4. Instance Savings Plan
5. Compute Savings Plan

Wenn Sie einen SP auf Verwaltungskontoebene erwerben, werden die Einsparungen auf der Grundlage des höchsten bis niedrigsten Rabattprozentsatzes berechnet. SPs Schauen Sie sich auf der Ebene des Verwaltungskontos alle verknüpften Konten an und wenden Sie die Ersparnisse dort an, wo der discount am höchsten ist. Wenn Sie einschränken möchten, wo die Ersparnisse verwendet werden, können Sie auf der verknüpften Kontoebene einen Savings Plan erwerben. Jedes Mal, wenn auf diesem Konto berechnete Computing-Services ausgeführt werden, wird der Rabatt zuerst dort angewendet. Wenn auf dem Konto keine berechtigten Datenverarbeitungsservices ausgeführt werden, wird der Rabatt auf die anderen verknüpften Konten unter demselben Verwaltungskonto aufgeteilt. Die gemeinsame Nutzung von Rabatten ist standardmäßig aktiviert, kann aber bei Bedarf deaktiviert werden.

In einer konsolidierten Abrechnungsfamilie werden Savings Plans zuerst auf die Nutzung des Inhaberkontos und dann auf die Nutzung anderer Konten angewendet. Dies ist nur dann der Fall, wenn Sie das Teilen aktiviert haben. Ihre Savings Plans werden zuerst auf Ihren höchsten Sparprozentsatz angewendet. Wenn es mehrere Nutzungen mit denselben Sparprozentsätzen gibt, werden Savings Plans auf die erste Nutzung mit der niedrigsten Savings-Plans-Rate angewendet. Savings Plans gelten so lange, bis keine Restnutzungen mehr zur Verfügung stehen oder Ihre Bindung ausgeschöpft ist. Jede verbleibende Nutzung wird zu den On-Demand-Tarifen abgerechnet. Sie können die Sparplanempfehlungen in AWS Cost Management aktualisieren, um jederzeit neue Sparplanempfehlungen zu generieren.

Nach der Analyse der Flexibilität der Instances können Sie sich entsprechend den Empfehlungen festlegen. Erstellen Sie eine Kostenmodellierung, indem Sie die kurzfristigen Kosten der Arbeitslast mit potenziellen verschiedenen Ressourcenoptionen analysieren, AWS Preismodelle analysieren und sie an Ihren Geschäftsanforderungen ausrichten, um die Gesamtbetriebskosten und Möglichkeiten [zur Kostenoptimierung](#) zu ermitteln.

### Implementierungsschritte

Durchführen einer Analyse des Bindungsrabatts: Sehen Sie sich unter Verwendung von Cost Explorer in Ihrem Konto die Empfehlungen für Savings Plans und Reserved Instances an. Stellen Sie sicher, dass Sie die Empfehlungen zu Savings Plans verstehen, und schätzen Sie Ihre monatlichen Ausgaben und Einsparungen. Sehen Sie sich die Empfehlungen auf Ebene des Verwaltungskontos an, die unter Berücksichtigung der Nutzung aller Mitgliedskonten in Ihrer AWS -Organisation berechnet werden, für die das Teilen der Rabatte für RI oder Savings Plans aktiviert ist, um maximale Einsparungen über alle Konten hinweg zu ermöglichen. Sie können sicherstellen, dass Sie die richtigen Empfehlungen mit den erforderlichen Rabatten und Risiken implementieren, indem Sie die Well-Architected Labs befolgen.

### Ressourcen

#### Zugehörige Dokumente:

- [Wie funktioniert die AWS Preisgestaltung?](#)
- [Instance-Kaufoptionen](#)
- [Übersicht über Savings Plans](#)
- [Empfehlungen zu Savings Plans](#)
- [Zugriff auf Empfehlungen für Reserved Instances](#)
- [Understanding your Saving Plans recommendation](#)

- [So gelten Savings Plans für Ihre AWS Nutzung](#)
- [Savings Plans mit konsolidierter Fakturierung](#)
- [Aktivieren von geteilten reservierten Instances und Savings Plans-Rabatten](#)

Zugehörige Videos:

- [Save up to 90% and run production workloads on Spot](#)

Zugehörige Beispiele:

- [AWS Well-Architected Lab: Pricing Models \(Level 200\)](#)
- [AWS Well-Architected Labs: Pricing Model Analysis \(Level 200\)](#)
- [Was sollte ich vor dem Kauf eines Savings Plan beachten?](#)
- [How can I use rolling Savings Plans to reduce commitment risk?](#)
- [Verwendung von Spot-Instances](#)

## COST8 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

- [COST08-BP01 Datenübertragungsmodellierung durchführen](#)
- [COST08-BP02 Wählen Sie Komponenten aus, um die Datenübertragungskosten zu optimieren](#)
- [COST08-BP03 Implementieren Sie Dienste zur Senkung der Datenübertragungskosten](#)

### COST08-BP01 Datenübertragungsmodellierung durchführen

Stellen Sie die Organisationsanforderungen zusammen und führen Sie eine Datenübertragungsmodellierung der Workload und ihrer einzelnen Komponenten durch. Dadurch wird der niedrigste Kostenpunkt für die jeweiligen aktuellen Datenübertragungsanforderungen ermittelt.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Hoch

## Implementierungsleitfaden

Wenn eine Lösung in der Cloud entworfen wird, werden die Gebühren für die Datenübertragung in der Regel vernachlässigt, da die Architektur üblicherweise in On-Premises-Rechenzentren entworfen wird oder es an Kenntnissen mangelt. Die Gebühren für die Datenübertragung in AWS hängen von der Quelle, dem Ziel und dem Volumen des Datenverkehrs ab. Die Berücksichtigung dieser Gebühren in der Entwicklungsphase kann zu Kosteneinsparungen führen. Für eine genaue Schätzung der Gesamtbetriebskosten (TCO) ist es sehr wichtig zu wissen, wo die Datenübertragung in Ihrem Workload stattfindet, welche Kosten mit der Übertragung verbunden sind und welche Vorteile damit verbunden sind. Auf diese Weise können Sie eine fundierte Entscheidung treffen, die Architekturentscheidung zu ändern oder zu akzeptieren. Sie können beispielsweise über eine Multi-Availability-Zone-Konfiguration verfügen, in der Sie Daten zwischen den Availability Zones replizieren.

Sie modellieren die Komponenten der Services, die die Daten in Ihrer Workload übertragen, und entscheiden, dass dies akzeptable Kosten sind (ähnlich wie bei der Zahlung für Datenverarbeitung und Speicher in beiden Availability Zones), um die erforderliche Zuverlässigkeit und Ausfallsicherheit zu erreichen. Modellieren Sie die Kosten über verschiedene Nutzungsstufen. Die Workload-Nutzung kann sich im Laufe der Zeit ändern und verschiedene Services können auf verschiedenen Ebenen kostengünstiger sein.

Denken Sie bei der Modellierung Ihrer Datenübertragung daran, wie viele Daten aufgenommen werden und woher diese Daten stammen. Berücksichtigen Sie außerdem, wie viele Daten verarbeitet werden und wie viel Speicher- oder Datenverarbeitungskapazität benötigt wird. Befolgen Sie bei der Modellierung bewährte Methoden für Ihre Workload-Architektur, um Ihre potenziellen Datenübertragungskosten zu optimieren.

Auf diese AWS Pricing Calculator Weise können Sie sich einen Überblick über die geschätzten Kosten für bestimmte AWS Dienste und die zu erwartende Datenübertragung verschaffen. Wenn bei Ihnen bereits ein Workload ausgeführt wird (zu Testzwecken oder in einer Vorproduktionsumgebung), verwenden Sie [AWS Cost Explorer](#) oder [AWS Cost and Usage Report](#) (CUR), um Ihre Datenübertragungskosten zu ermitteln und zu modellieren. Konfigurieren Sie einen Machbarkeitsnachweis (PoC) oder testen Sie Ihre Workload und führen Sie einen Test mit einer realistischen simulierten Last aus. Sie können Ihre Kosten bei verschiedenen Workload-Nachfragen modellieren.

## Implementierungsschritte

- Ermitteln der Anforderungen: Was ist das primäre Ziel und was sind die geschäftlichen Anforderungen für die geplante Datenübertragung zwischen Quelle und Ziel? Was ist das erwartete



Geschäftsergebnis am Ende? Ermitteln Sie die Geschäftsanforderungen und definieren Sie das erwartete Ergebnis.

- Identifizieren Sie Quelle und Ziel: Was ist die Datenquelle und das Ziel für die Datenübertragung, z. B. innerhalb AWS-Regionen, zu AWS Diensten oder aus dem Internet?
  - [Datenübertragung innerhalb eines AWS-Region](#)
  - [Datenübertragung zwischen AWS-Regionen](#)
  - [Datenübertragung ins Internet](#)
- Ermittlung der Datenklassifizierungen: Welche Datenklassifizierung gilt für diese Datenübertragung? Um welche Art von Daten handelt es sich? Um wie viele Daten handelt es sich? Wie häufig müssen die Daten übertragen werden? Handelt es sich um sensible Daten?
- Identifizieren Sie die zu verwendenden AWS Dienste oder Tools: Welche AWS Dienste werden für diese Datenübertragung verwendet? Ist es möglich, einen bereits bereitgestellten Service für eine andere Workload zu verwenden?
- Berechnen der Datenübertragungskosten: Verwenden Sie [AWS Pricing](#), die Datenübertragungsmodellierung, die Sie zuvor erstellt haben, um die Datenübertragungskosten für die Workload zu berechnen. Berechnen Sie die Datenübertragungskosten bei verschiedenen Nutzungsstufen, sowohl bei erhöhter als auch bei verringerter Workload-Nutzung. Wenn es mehrere Optionen für die Workload-Architektur gibt, berechnen Sie die Kosten für jede Option zum Vergleich.
- Verknüpfen von Kosten mit Ergebnissen: Geben Sie für alle anfallenden Datenübertragungskosten das Ergebnis an, das damit für die Workload erreicht wird. Erfolgt der Transfer zwischen Komponenten, kann dies für die Entkopplung verwendet werden. Erfolgt der Transfer zwischen Availability Zones, kann dies zur Redundanz verwendet werden.
- Erstellen der Datenübertragungsmodellierung: Nachdem Sie alle Informationen zusammengetragen haben, erstellen Sie eine konzeptionelle Basisdatenübertragungsmodellierung für mehrere Anwendungsfälle und unterschiedliche Workloads.

## Ressourcen

### Zugehörige Dokumente:

- [AWS Caching-Lösungen](#)
- [AWS Preise](#)
- [EC2Amazon-Preisgestaltung](#)

- [VPCAmazon-Preisgestaltung](#)
- [Understanding data transfer charges](#)

Zugehörige Videos:

- [Monitoring and Optimizing Your Data Transfer Costs](#)
- [S3 Transfer Acceleration](#)

Zugehörige Beispiele:

- [Überblick über die Datenübertragungskosten für gängige Architekturen](#)
- [AWS Präskriptive Leitlinien für Netzwerke](#)

COST08-BP02 Wählen Sie Komponenten aus, um die Datenübertragungskosten zu optimieren

Alle Komponenten sind ausgewählt und die Architektur ist so konzipiert, dass die Datenübertragungskosten gesenkt werden. Dazu gehört die Verwendung von Komponenten wie wide-area-network (WAN) -Optimierung und Multi-Availability Zone (AZ) -Konfigurationen

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Mittel

Implementierungsleitfaden

Eine Architektur für die Datenübertragung minimiert die Kosten für die Datenübertragung. Dies kann auch die Nutzung von CDNs bedeuten, um die Daten näher an den Benutzern zu platzieren, oder die Verwendung spezieller Netzwerklinks von Ihrem Standort zu AWS. Sie können auch WAN Optimierung und Anwendungsoptimierung verwenden, um die Datenmenge zu reduzieren, die zwischen Komponenten übertragen wird.

Bei der Übertragung von Daten in oder innerhalb von ist es wichtig AWS Cloud, das Ziel anhand verschiedener Anwendungsfälle, der Art der Daten und der verfügbaren Netzwerkressourcen zu kennen, um die richtigen AWS Dienste zur Optimierung der Datenübertragung auswählen zu können. AWS bietet eine Reihe von Datenübertragungsdiensten, die auf unterschiedliche Datenmigrationsanforderungen zugeschnitten sind. Wählen Sie die richtigen Optionen für die [Datenspeicherung](#) und [Datenübertragung](#) auf Grundlage der geschäftlichen Anforderungen in Ihrer Organisation.

Beachten Sie bei der Planung oder Überprüfung Ihrer Workload-Architektur die folgenden Punkte:

- Verwenden Sie VPC Endpunkte innerhalb AWS: VPC Endpunkte ermöglichen private Verbindungen zwischen Ihren VPC und den unterstützten AWS Diensten. So vermeiden Sie die Nutzung des öffentlichen Internets, was zu Kosten für die Datenübertragung führen kann.
- Verwenden Sie ein NAT Gateway: Verwenden Sie ein [NATGateway](#), damit Instances in einem privaten Subnetz eine Verbindung zum Internet oder zu Diensten außerhalb Ihres Subnetzes herstellen können. Prüfen Sie, ob sich die Ressourcen hinter dem NAT Gateway, die den meisten Verkehr senden, in derselben Availability Zone wie das NAT Gateway befinden. Ist dies nicht der Fall, erstellen Sie neue NAT Gateways in derselben Availability Zone wie die Ressource, um die AZ-übergreifenden Datenübertragungsgebühren zu senken.
- Use AWS Direct Connect AWS Direct Connect umgeht das öffentliche Internet und stellt eine direkte, private Verbindung zwischen Ihrem lokalen Netzwerk und her. Dies kann kostengünstiger und konsistenter sein als die Übertragung großer Datenmengen über das Internet.
- Vermeiden Sie die Übertragung von Daten über regionale Grenzen hinweg: Für Datenübertragungen zwischen AWS-Regionen (von einer Region zur anderen) fallen in der Regel Gebühren an. Die Entscheidung, einen multiregionalen Weg einzuschlagen, sollte gut überlegt sein. Weitere Informationen finden Sie unter [Szenarien mit mehreren Regionen](#).
- Überwachen Sie die Datenübertragung: Verwenden Sie Amazon CloudWatch und [VPCFlow-Logs](#), um Details zu Ihrer Datenübertragung und Netzwerknutzung zu erfassen. Analysieren Sie die erfassten Netzwerkverkehrsinformationen in Ihrem VPCs System, z. B. die IP-Adresse oder den Bereich, der zu und von Netzwerkschnittstellen gesendet wird.
- Analysieren Sie Ihre Netzwerknutzung: Verwenden Sie Mess- und Berichtstools wie AWS Cost Explorer CUDOS Dashboards oder CloudWatch um die Datenübertragungskosten Ihrer Workloads zu ermitteln.

## Implementierungsschritte

- Auswählen der Komponenten für die Datenübertragung: Konzentrieren Sie sich anhand der in [COST08-BP01 Datenübertragungsmodellierung durchführen](#) erläuterten Datenübertragungsmodellierung darauf, wo die größten Datenübertragungskosten anfallen oder anfallen würden, wenn sich die Workload-Nutzung ändert. Suchen Sie nach alternativen Architekturen oder zusätzlichen Komponenten, die den Datenübertragungsbedarf beseitigen oder reduzieren (oder die Kosten senken).

## Ressourcen

Zugehörige bewährte Methoden:

- [COST08-BP01 Datenübertragungsmodellierung durchführen](#)
- [COST08-BP03 Implementieren Sie Dienste zur Senkung der Datenübertragungskosten](#)

Zugehörige Dokumente:

- [Cloud-Datenmigration](#)
- [AWS -Caching-Lösungen](#)
- [Schnellere Bereitstellung von Inhalten mit Amazon CloudFront](#)

Zugehörige Beispiele:

- [Überblick über die Datenübertragungskosten für gängige Architekturen](#)
- [AWS Tipps zur Netzwerkoptimierung](#)
- [Optimieren Sie die Leistung und senken Sie die Kosten für Netzwerkanalysen mit VPC Flow Logs im Apache Parquet-Format](#)

COST08-BP03 Implementieren Sie Dienste zur Senkung der Datenübertragungskosten

Implementieren Sie Services zur Verringerung der Datenübertragung. Verwenden Sie beispielsweise Edge-Standorte oder Content Delivery Networks (CDN), um Inhalte für Endbenutzer bereitzustellen, erstellen Sie Caching-Ebenen vor Ihren Anwendungsservern oder Datenbanken und verwenden Sie dedizierte Netzwerkverbindungen statt VPN für die Konnektivität zur Cloud.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Mittel

Implementierungsleitfaden

Es gibt verschiedene AWS Dienste, die Ihnen helfen können, die Nutzung der Netzwerkdatenübertragung zu optimieren. Abhängig von den Komponenten, dem Typ und der Cloud-Architektur Ihrer Workload können diese Services Sie bei der Komprimierung, beim Caching sowie der gemeinsamen Nutzung und Verteilung Ihres Datenverkehrs in der Cloud unterstützen.

- [Amazon CloudFront](#) ist ein globales Netzwerk zur Bereitstellung von Inhalten, das Daten mit geringer Latenz und hohen Übertragungsgeschwindigkeiten bereitstellt. Es stellt Daten an Edge-Standorten rund um die Welt in den Cache und reduziert damit die Belastung Ihrer Ressourcen. Durch die Verwendung CloudFront können Sie den administrativen Aufwand bei der Bereitstellung von Inhalten für eine große Anzahl von Benutzern weltweit mit minimaler Latenz reduzieren. Mit

dem [Sicherheitssparpaket](#) können Sie bis zu 30% bei Ihrer CloudFront Nutzung sparen, wenn Sie planen, Ihre Nutzung im Laufe der Zeit zu erhöhen.

- [AWS Direct Connect](#) ermöglicht es Ihnen, eine dedizierte Netzwerkverbindung zu AWS aufzubauen. Damit können Sie Netzwerkkosten reduzieren, die Bandbreite erhöhen und eine im Vergleich zu Internet-basierten Verbindungen gleichbleibendere Netzwerkerfahrung bieten.
- [AWS VPN](#) ermöglicht es Ihnen, eine sichere und private Verbindung zwischen Ihrem privaten Netzwerk und dem globalen AWS -Netzwerk aufzubauen. Dies ist ideal für kleine Niederlassungen oder Geschäftspartner, da es vereinfachte Konnektivität bietet und ein vollständig verwalteter und elastischer Service ist.
- [VPCEndgeräte](#) ermöglichen die Konnektivität zwischen AWS Diensten über private Netzwerke und können verwendet werden, um die Kosten für öffentliche Datenübertragungen und [NATGateways](#) zu senken. Für [VPCGateway-Endpunkte](#) fallen keine Stundengebühren an und sie unterstützen Amazon S3 und Amazon DynamoDB. [VPCSchnittstellenendpunkte](#) werden von bereitgestellt [AWS PrivateLink](#) und haben eine stündliche Gebühr sowie Nutzungskosten pro GB.
- [NATGateways](#) bieten im Gegensatz zu einer eigenständigen Instanz integrierte Skalierung und Verwaltung zur Kostensenkung. NAT Platzieren Sie NAT Gateways in denselben Availability Zones wie Instances mit hohem Traffic und erwägen Sie die Verwendung von VPC Endpunkten für die Instances, die auf Amazon DynamoDB oder Amazon S3 zugreifen müssen, um die Datenübertragungs- und Verarbeitungskosten zu senken.
- Verwenden Sie [AWS Snow Family](#)Geräte, die über Rechenressourcen verfügen, um Daten am Netzwerkrand zu sammeln und zu verarbeiten. AWS Snow Family Geräte ([Snowcone](#), [Snowball und Snowmobile](#)) ermöglichen es Ihnen, Petabyte an Daten kostengünstig und offline in das AWS Cloud Internet zu übertragen.

## Implementierungsschritte

- Implementieren Sie Dienste: Wählen Sie anhand der Datenübertragungsmodellierung und der Überprüfung der Flow-Logs die entsprechenden AWS Netzwerkdienste auf der Grundlage Ihres Service-Workload-Typs aus. VPC Sehen Sie sich an, wo sich die höchsten Kosten und Volumenströme befinden. Überprüfen Sie die AWS Dienste und beurteilen Sie, ob es einen Dienst gibt, der die Übertragung reduziert oder verhindert, insbesondere Netzwerke und Inhaltsbereitstellung. Suchen Sie auch nach Caching-Services, bei denen wiederholt auf Daten oder große Datenmengen zugegriffen wird.

## Ressourcen

### Zugehörige Dokumente:

- [AWS Direct Connect](#)
- [AWS Erkunden Sie unsere Produkte](#)
- [AWS -Caching-Lösungen](#)
- [Amazon CloudFront](#)
- [AWS Snow Family](#)
- [Amazon-Sparpaket CloudFront für Sicherheitslösungen](#)

### Zugehörige Videos:

- [Monitoring and Optimizing Your Data Transfer Costs](#)
- [AWS Serie zur Kostenoptimierung: CloudFront](#)
- [Wie kann ich die Datenübertragungsgebühren für mein NAT Gateway senken?](#)

### Zugehörige Beispiele:

- [How-to chargeback shared services: An AWS Transit Gateway example](#)
- [Verstehen Sie die Details der AWS Datenübertragung anhand des Kosten- und Nutzungsberichts mithilfe von Athena Query eingehend und QuickSight](#)
- [Überblick über die Datenübertragungskosten für gängige Architekturen](#)
- [Using AWS Cost Explorer to analyze data transfer costs](#)
- [Kostenoptimierung Ihrer AWS Architekturen durch die Nutzung von Amazon-Funktionen CloudFront](#)
- [Wie kann ich die Datenübertragungsgebühren für mein NAT Gateway senken?](#)

## Verwaltung von Nachfrage und Bereitstellung von Ressourcen

### Frage

- [COST9. Wie verwalten Sie die Nachfrage und stellen Ressourcen bereit?](#)

## COST9. Wie verwalten Sie die Nachfrage und stellen Ressourcen bereit?

Stellen Sie bei einer Workload mit ausgewogenen Ausgaben und Leistungen sicher, dass alles, wofür Sie bezahlen, genutzt wird, und vermeiden Sie eine erhebliche Unterauslastung der Instances. Eine verzerrte Nutzungskennzahl in beide Richtungen wirkt sich negativ auf Ihr Unternehmen aus, und zwar entweder in Bezug auf die Betriebskosten (Leistungseinbußen aufgrund von Überauslastung) oder auf verschwendete Ausgaben (aufgrund von zu viel Bereitstellung). AWS

### Bewährte Methoden

- [COST09-BP01 Führen Sie eine Analyse des Workload-Bedarfs durch](#)
- [COST09-BP02 Implementieren Sie einen Puffer oder eine Drosselung, um die Nachfrage zu steuern](#)
- [COST09-BP03 Ressourcen dynamisch bereitstellen](#)

### COST09-BP01 Führen Sie eine Analyse des Workload-Bedarfs durch

Analysieren Sie den Bedarf der Workload im gesamten Zeitverlauf. Stellen Sie sicher, dass die Analyse saisonale Trends berücksichtigt und die Betriebsbedingungen über die gesamte Lebensdauer der Workload genau wiedergibt. Der Analyseaufwand sollte in einem angemessenen Verhältnis zum potenziellen Nutzen stehen, z. B. muss der Zeitaufwand den Workload-Kosten entsprechen.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Hoch

### Implementierungsleitfaden

Die Analyse des Workload-Bedarfs für Cloud Computing erfordert ein Verständnis der Muster und Eigenschaften von Computing-Aufgaben, die in der Cloud-Umgebung initiiert werden. Diese Analyse hilft Benutzern, die Ressourcenzuweisung zu optimieren, Kosten zu verwalten und sicherzustellen, dass die Leistung den Anforderungen entspricht.

Informieren Sie sich über die Anforderungen der Workload. Die Anforderungen Ihrer Organisation sollten die Workload-Reaktionszeiten für Anforderungen angeben. Anhand der Reaktionszeit kann bestimmt werden, ob der Bedarf gut gesteuert wird oder ob das Ressourcenangebot geändert werden sollte, um der Nachfrage gerecht zu werden.

Die Analyse sollte die Vorhersehbarkeit und Wiederholbarkeit der Nachfrage, die Änderungsrate der Nachfrage und die Menge der Nachfrageänderungen umfassen. Führen Sie die Analyse über

einen Zeitraum durch, der lang genug ist, um saisonale Abweichungen, wie z. B. end-of-month Verarbeitungs- oder Feiertagsspitzen, zu berücksichtigen.

Der Analyseaufwand sollte die potenziellen Vorteile der Implementierung einer Skalierung widerspiegeln. Betrachten Sie die erwarteten Gesamtkosten der Komponente sowie etwaige Erhöhungen oder Verringerungen der Nutzung und der Kosten während der Workload-Lebensdauer.

Im Folgenden sind einige wichtige Aspekte aufgeführt, die bei der Durchführung der Workload-Bedarfsanalyse für Cloud Computing zu berücksichtigen sind:

1. **Kennzahlen zur Ressourcennutzung und Leistung:** Analysieren Sie, wie AWS Ressourcen im Laufe der Zeit genutzt werden. Ermitteln Sie Nutzungsmuster während und außerhalb der Spitzenzeiten, um die Ressourcenzuweisung und Skalierungsstrategien zu optimieren. Überwachen Sie Leistungsmetriken wie Reaktionszeiten, Latenz, Durchsatz und Fehlerraten. Diese Metriken helfen bei der Bewertung des Gesamtzustands und der Effizienz der Cloud-Infrastruktur.
2. **Skalierungsverhalten von Benutzern und Anwendungen:** Verstehen Sie das Benutzerverhalten und wie es sich auf den Workload-Bedarf auswirkt. Das Untersuchen von Mustern beim Benutzerdatenverkehr trägt dazu bei, die Bereitstellung von Inhalten und die Reaktionsfähigkeit von Anwendungen zu verbessern. Analysieren Sie, wie Workloads mit steigender Nachfrage skaliert werden. Bestimmen Sie, ob die Parameter für Auto Scaling korrekt und effektiv für den Umgang mit Auslastungsschwankungen konfiguriert sind.
3. **Workload-Typen:** Identifizieren Sie die verschiedenen Typen von Workloads, die in der Cloud ausgeführt werden, wie Batch-Verarbeitung, Echtzeitdatenverarbeitung, Webanwendungen, Datenbanken oder Machine Learning. Jeder Workload-Typ kann unterschiedliche Ressourcenanforderungen und Leistungsprofile aufweisen.
4. **Service Level Agreements (SLAs):** Vergleichen Sie die tatsächliche Leistung mit SLAs, um die Einhaltung der Vorschriften sicherzustellen und Bereiche zu identifizieren, in denen Verbesserungen erforderlich sind.

Sie können [Amazon](#) verwenden, CloudWatch um Kennzahlen zu sammeln und zu verfolgen, Protokolldateien zu überwachen, Alarme einzustellen und automatisch auf Änderungen Ihrer AWS Ressourcen zu reagieren. Sie können Amazon auch verwenden CloudWatch , um systemweite Einblicke in die Ressourcennutzung, die Anwendungsleistung und den Betriebszustand zu erhalten.

Mit [AWS Trusted Advisor](#) können Sie Ihre Ressourcen gemäß bewährten Methoden bereitstellen und so die Systemleistung und -zuverlässigkeit verbessern, die Sicherheit erhöhen und nach



Einsparungsmöglichkeiten suchen. Sie können auch Instances deaktivieren, die nicht zur Produktion gehören, und Amazon CloudWatch und Auto Scaling verwenden, um dem Anstieg oder Rückgang der Nachfrage gerecht zu werden.

Schließlich können Sie [Amazon QuickSight](#) mit der Datei AWS Cost and Usage Report (CUR) [AWS Cost Explorer](#) oder Ihren Anwendungsprotokollen verwenden, um eine erweiterte Analyse des Workload-Bedarfs durchzuführen.

Insgesamt ermöglicht eine umfassende Analyse des Workload-Bedarfs es Organisationen, fundierte Entscheidungen zur Bereitstellung, Skalierung und Optimierung von Ressourcen zu treffen, was zu einer besseren Leistung, Kosteneffizienz und Benutzerzufriedenheit führt.

### Implementierungsschritte

- **Vorhandene Workload-Daten analysieren:** Analysieren Sie Daten aus der vorhandenen Workload, früheren Versionen der Workload oder vorhergesagten Nutzungsmustern. Nutzen Sie Amazon CloudWatch, Protokolldateien und Monitoring-Daten, um sich einen Überblick darüber zu verschaffen, wie der Workload genutzt wurde. Analysieren Sie einen vollständigen Zyklus der Arbeitslast und sammeln Sie Daten über saisonale Veränderungen wie end-of-month end-of-year Ereignisse. Der in der Analyse reflektierte Aufwand sollte die Workload-Merkmale widerspiegeln. Der größte Aufwand sollte für hochwertige Workloads mit den größten Nachfrageänderungen betrieben werden. Der geringste Aufwand sollte für Workloads mit niedrigem Wert und geringfügigen Nachfrageänderungen betrieben werden.
- **Vorhersage externer Einflüsse:** Treffen Sie Teammitglieder aus der gesamten Organisation, die die Nachfrage in der Workload beeinflussen oder ändern können. Häufig betroffene Teams sind Vertrieb, Marketing oder Business Development. Arbeiten Sie mit ihnen zusammen, um die Zyklen kennenzulernen, in denen sie arbeiten, und um zu erfahren, ob es Ereignisse gibt, die die Nachfrage der Workload ändern könnten. Erstellen Sie eine Prognose des Workload-Bedarfs anhand dieser Daten.

### Ressourcen

#### Zugehörige Dokumente:

- [Amazon CloudWatch](#)
- [AWS Trusted Advisor](#)
- [AWS X-Ray](#)
- [AWS Auto Scaling](#)

- [AWS Instance Scheduler](#)
- [Erste Schritte mit Amazon SQS](#)
- [AWS Cost Explorer](#)
- [Amazon QuickSight](#)

Zugehörige Videos:

Zugehörige Beispiele:

- [Monitor, Track and Analyze for cost optimization](#)
- [Beim Suchen und Analysieren von Logs CloudWatch](#)

COST09-BP02 Implementieren Sie einen Puffer oder eine Drosselung, um die Nachfrage zu steuern

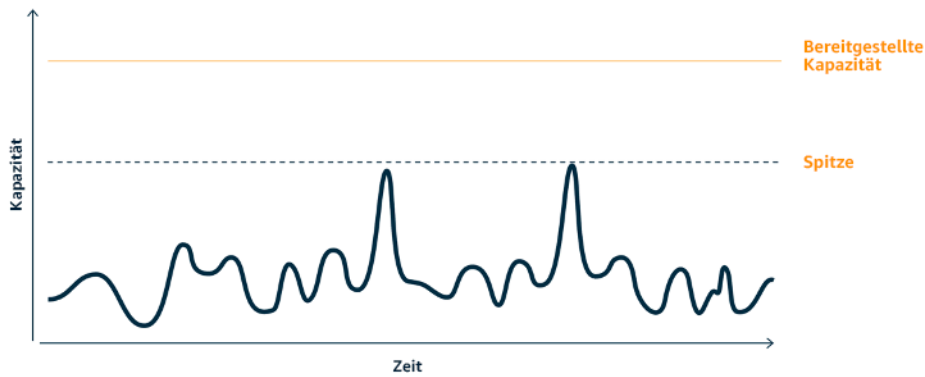
Pufferung und Drosselung ändern den Bedarf Ihrer Workload und glätten alle Spitzen.

Implementieren Sie die Drosselung, wenn Ihre Clients Wiederholungen durchführen. Implementieren Sie die Pufferung, um die Anforderung zu speichern und die Verarbeitung auf einen späteren Zeitpunkt zu verschieben. Stellen Sie sicher, dass Ihre Drosselungen und Puffer so konzipiert sind, dass Clients in der erforderlichen Zeit eine Antwort erhalten.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Mittel

Implementierungsleitfaden

Die Implementierung einer Pufferung oder Drosselung ist beim Cloud Computing von entscheidender Bedeutung, um die Nachfrage zu steuern und die für die Workload benötigte bereitgestellte Kapazität zu reduzieren. Für eine optimale Leistung ist es unerlässlich, die Gesamtnachfrage, einschließlich der Spitzen, sowie die Geschwindigkeit, mit der sich die Anfragen ändern, und die erforderliche Reaktionszeit zu messen. Wenn Clients die Möglichkeit haben, ihre Anfragen erneut zu senden, ist es praktisch, eine Drosselung vorzunehmen. Umgekehrt ist für Clients ohne Wiederholungsfunktionen die Implementierung einer Pufferlösung der ideale Ansatz. Solche Puffer rationalisieren den Eingang von Anfragen und optimieren die Interaktion von Anwendungen mit unterschiedlichen Betriebsgeschwindigkeiten.



Bedarfskurve mit zwei deutlichen Spitzen, die hohe bereitgestellte Kapazität erfordern

Nehmen wir eine Workload mit der nachfolgend gezeigten Bedarfskurve. Diese Workload hat zwei Spitzen und um damit umzugehen, wird die Ressourcenkapazität bereitgestellt, die hier durch die orangefarbene Linie angezeigt wird. Die für diese Workload aufgewendeten Ressourcen und die eingesetzte Energie werden nicht durch die Fläche unter der Bedarfskurve, sondern von der Linie für die bereitgestellte Kapazität angezeigt, da die bereitgestellte Kapazität zur Bewältigung dieser beiden Spitzen benötigt wird. Die Verflachung der Bedarfskurve kann Ihnen dabei helfen, die bereitgestellte Kapazität für eine Workload zu verringern und dessen Umweltauswirkungen zu reduzieren. Um die Spitzen abzuflachen, sollten Sie eine Lösung zur Drosselung oder Pufferung in Betracht ziehen.

Um dies besser zu verstehen, werden wir uns kurz die Drosselung und Pufferung ansehen.

**Drosselung:** Wenn die Quelle der Nachfrage über eine Wiederholungsfunktion verfügt, können Sie die Drosselung implementieren. Die Drosselung teilt der Quelle mit, dass wenn sie die Anfrage zum aktuellen Zeitpunkt nicht bedienen kann, sie es später erneut versuchen sollte. Die Quelle wartet einen bestimmten Zeitraum und wiederholt die Anfrage. Die Implementierung der Drosselung hat den Vorteil, dass die maximale Menge an Ressourcen und Kosten der Workload begrenzt wird. In können Sie [Amazon API Gateway](#) verwenden AWS, um Drosselung zu implementieren.

**Pufferbasiert:** Ein pufferbasierter Ansatz verwendet Produzenten (Komponenten, die Nachrichten an die Warteschlange senden), Verbraucher (Komponenten, die Nachrichten aus der Warteschlange empfangen) und eine Warteschlange (die Nachrichten enthält), um die Nachrichten zu speichern. Nachrichten können dadurch von Verbrauchern in der für ihre Geschäftsanforderungen passenden Geschwindigkeit gelesen und verarbeitet werden. Durch die Verwendung einer pufferbasierten Methodik werden die Nachrichten von den Produzenten in Warteschlangen oder Streams gespeichert und können von den Verbrauchern in einem Tempo abgerufen werden, das sich an deren betrieblichen Anforderungen orientiert.

In können Sie aus mehreren Services wählen AWS, um einen Pufferansatz zu implementieren. [Amazon Simple Queue Service \(AmazonSQS\)](#) ist ein verwalteter Service, der Warteschlangen bereitstellt, die es einem einzelnen Verbraucher ermöglichen, einzelne Nachrichten zu lesen. [Amazon Kinesis](#) stellt einen Stream bereit, mit dem viele Verbraucher dieselben Nachrichten lesen können.

Durch Pufferung und Drosselung können Spitzenwerte abgeflacht werden, indem die Anforderungen an Ihre Workload angepasst werden. Verwenden Sie die Drosselung, wenn Clients Aktionen wiederholen, und nutzen Sie die Pufferung, um Anfragen zurückzuhalten und später zu verarbeiten. Stellen Sie bei der Architektur mit einem pufferbasierten Ansatz sicher, dass Sie Ihre Workload so gestalten, dass er die Anfrage in der erforderlichen Zeit erfüllt, und dass Sie doppelte Arbeitsanfragen verarbeiten können. Analysieren Sie den Gesamtbedarf, die Änderungsrate und die erforderliche Reaktionszeit, um die korrekte Größe der erforderlichen Drosselung oder des Puffers zu bestimmen.

### Implementierungsschritte

- **Analysieren der Client-Anforderungen:** Analysieren Sie die Client-Anforderungen, um zu bestimmen, ob sie Wiederholungen durchführen können. Für Clients, die keine Wiederholungen durchführen können, müssen Puffer implementiert werden. Analysieren Sie den Gesamtbedarf, die Änderungsrate und die erforderliche Reaktionszeit, um die Größe der erforderlichen Drosselung oder des Puffers zu bestimmen.
- **Implementieren eines Puffers oder einer Drosselung:** Implementieren Sie einen Puffer oder eine Drosselung in der Workload. Eine Warteschlange wie Amazon Simple Queue Service (AmazonSQS) kann einen Puffer für Ihre Workload-Komponenten bereitstellen. Amazon API Gateway kann die Drosselung Ihrer Workload-Komponenten bereitstellen.

### Ressourcen

Zugehörige bewährte Methoden:

- [SUS02-BP06 Implementieren Sie Pufferung oder Drosselung, um die Nachfragekurve abzuflachen](#)
- [REL05-BP02 Drosselungsanfragen](#)

Zugehörige Dokumente:

- [AWS Auto Scaling](#)
- [AWS Instance Scheduler](#)
- [APIAmazon-Gateway](#)

- [Amazon Simple Queue Service](#)
- [Erste Schritte mit Amazon SQS](#)
- [Amazon Kinesis](#)

Zugehörige Videos:

- [Choosing the Right Messaging Service for Your Distributed App](#)

Zugehörige Beispiele:

- [Verwaltung und Überwachung der API Drosselung Ihrer Workloads](#)
- [Drosselung einer mehrstufigen Lösung mit mehreren Mandanten im großen Maßstab mithilfe von Gateway REST API](#)
- [Aktivierung von Tiering und Drosselung in einer Amazon EKS SaaS-Lösung mit mehreren Mandanten mithilfe von Amazon Gateway API](#)
- [Application integration Using Queues and Messages](#)

### COST09-BP03 Ressourcen dynamisch bereitstellen

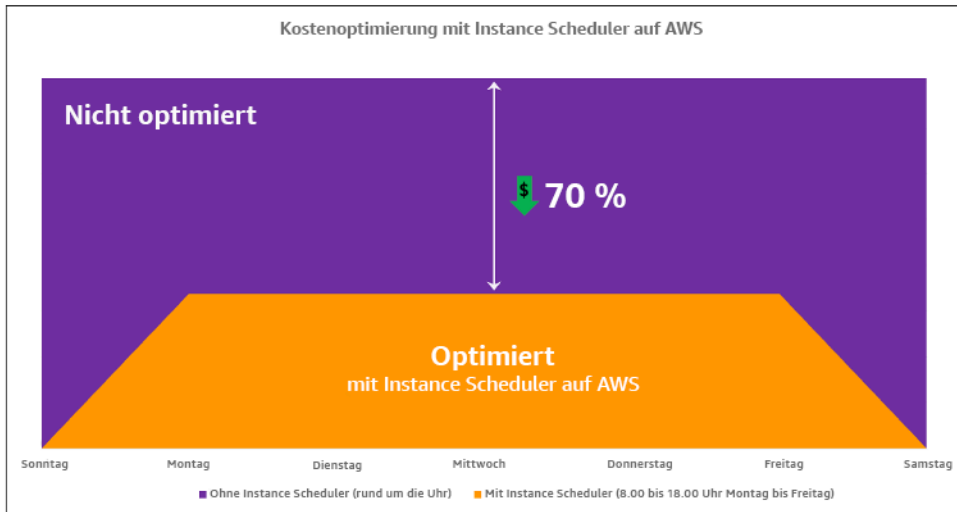
Ressourcen werden geplant bereitgestellt. Dies kann bedarfsbasiert sein, z. B. durch automatische Skalierung, oder zeitbasiert, wobei der Bedarf vorhersehbar ist und Ressourcen basierend auf der Zeit bereitgestellt werden. Diese Methoden führen zur geringsten Über- oder Unterversorgung.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Niedrig

### Implementierungsleitfaden

AWS Kunden haben verschiedene Möglichkeiten, die für ihre Anwendungen verfügbaren Ressourcen zu erhöhen und Ressourcen bereitzustellen, um der Nachfrage gerecht zu werden. Eine dieser Optionen ist die Verwendung von AWS Instance Scheduler, der das Starten und Stoppen von Amazon Elastic Compute Cloud (AmazonEC2) und Amazon Relational Database Service (AmazonRDS) -Instances automatisiert. Die andere Option ist die Verwendung AWS Auto Scaling, mit der Sie Ihre Rechenressourcen automatisch auf der Grundlage der Anforderungen Ihrer Anwendung oder Ihres Dienstes skalieren können. Wenn Sie Ressourcen bedarfsgerecht bereitstellen, zahlen Sie nur für die Ressourcen, die Sie tatsächlich nutzen. So senken Sie die Kosten, indem Sie Ressourcen bereitstellen, wenn sie benötigt werden, und sie beenden, wenn sie nicht mehr benötigt werden.

AWS Mit [Instance Scheduler](#) können Sie das Stoppen und Starten Ihrer Amazon EC2 - und RDS Amazon-Instances zu definierten Zeiten konfigurieren, sodass Sie den Bedarf an denselben Ressourcen innerhalb eines konsistenten Zeitmusters decken können, z. B. jeden Tag, an dem Benutzer um acht Uhr morgens auf EC2 Amazon-Instances zugreifen, die sie nach sechs Uhr nicht mehr benötigen. Durch diese Lösung lassen sich die Betriebskosten senken, indem sie nicht genutzte Ressourcen stoppt und sie bei Bedarf wieder startet.



Kostenoptimierung mit AWS Instance Scheduler.

Mit AWS Systems Manager Quick Setup können Sie auch ganz einfach Zeitpläne für Ihre EC2 Amazon-Instances für Ihre Konten und Regionen über eine einfache Benutzeroberfläche (UI) konfigurieren. Sie können Amazon EC2 - oder RDS Amazon-Instances mit AWS Instance Scheduler planen und bestehende Instances stoppen und starten. Sie können jedoch keine Instances beenden und starten, die Teil Ihrer Auto Scaling Scaling-Gruppe (ASG) sind oder Dienste wie Amazon Redshift oder Amazon OpenSearch Service verwalten. Auto-Scaling-Gruppen haben ihre eigene Planung für die Instances in der Gruppe und diese Instances werden erstellt.

Mit [AWS Auto Scaling](#) können Sie Ihre Kapazität anpassen, um eine stabile, vorhersehbare Leistung zu möglichst niedrigen Kosten aufrechtzuerhalten. Es handelt sich um einen vollständig verwalteten und kostenlosen Service zur Skalierung der Kapazität Ihrer Anwendung, der in EC2 Amazon-Instances und Spot-Flotten, AmazonECS, Amazon DynamoDB und Amazon Aurora integriert werden kann. Auto Scaling bietet eine automatische Ressourcenerkennung, um zu helfen, Ressourcen in Ihrer Workload zu finden, die konfiguriert werden können. Es verfügt über integrierte Skalierungsstrategien zur Optimierung der Leistung, der Kosten oder eines Gleichgewichts zwischen beiden Ressourcen und bietet eine prädiktive Skalierung, um regelmäßig auftretende Spitzen zu unterstützen.

Für die Skalierung Ihrer Auto-Scaling-Gruppe haben Sie mehrere Skalierungsoptionen:

- Fortlaufende Nutzung derselben Anzahl an Instances
- Manuelles Skalieren
- Skalierung nach Zeitplan
- Skalierung nach Bedarf
- Verwendung prädiktiver Skalierung

Auto-Scaling-Richtlinien unterscheiden sich und können in dynamische und geplante Skalierungsrichtlinien unterteilt werden. Dynamische Richtlinien sind für manuelle oder dynamische Skalierung, die geplant oder prädiktiv sein kann. Sie können Skalierungsrichtlinien für dynamische, geplante und prädiktive Skalierung verwenden. Sie können auch Metriken und Alarme von [Amazon](#) verwenden CloudWatch, um Skalierungsereignisse für Ihren Workload auszulösen. Wir empfehlen Ihnen die Verwendung von [Startvorlagen](#), mit denen Sie auf die neuesten Features und Verbesserungen zugreifen können. Nicht alle Auto-Scaling-Features sind verfügbar, wenn Sie Startkonfigurationen verwenden. Sie können beispielsweise keine Auto-Scaling-Gruppe erstellen, die Spot- und On-Demand-Instances startet oder mehrere Instance-Typen angibt. Sie müssen eine Startvorlage verwenden, um diese Funktionen zu konfigurieren. Wenn Sie Startvorlagen verwenden, empfehlen wir Ihnen, jede einzelne davon zu versionieren. Mit dem Versioning von Startvorlagen können Sie eine Teilmenge des vollständigen Satzes an Parametern erstellen. Anschließend können Sie es erneut verwenden, um andere Versionen derselben Startvorlage zu erstellen.

[Sie können Skalierung mit AWS Auto Scaling AWS APIs oder verwenden oder in Ihren Code integrieren SDKs](#). Dies reduziert Ihre Gesamtkosten für die Workload, da die Betriebskosten durch manuelle Änderungen an Ihrer Umgebung wegfallen, und kann viel schneller durchgeführt werden. So können Sie sicherstellen, dass Ihre Workload-Ressourcen jederzeit mit Ihrem Bedarf übereinstimmen. Um dieser bewährten Methode zu folgen und Ressourcen dynamisch für Ihr Unternehmen bereitzustellen, sollten Sie die horizontale und vertikale Skalierung der AWS Cloud Anwendungen sowie die Art der auf EC2 Amazon-Instances ausgeführten Anwendungen verstehen. Ihr Team für Cloud Financial Management sollte am besten mit den technischen Teams zusammenarbeiten, um diese bewährte Methode zu befolgen.

[Elastic Load Balancing](#) unterstützt Sie bei der Skalierung durch die Verteilung der Nachfrage auf mehrere Ressourcen. Mithilfe von ASG Elastic Load Balancing können Sie eingehende Anfragen verwalten, indem Sie den Datenverkehr optimal weiterleiten, sodass keine Instanz in einer Auto Scaling Scaling-Gruppe überlastet wird. Die Anforderungen werden nacheinander auf alle Ziele einer Zielgruppe verteilt, ohne Rücksicht auf Kapazität oder Auslastung.

Typische Metriken können EC2 Standardkennzahlen von Amazon sein, z. B. CPU Auslastung, Netzwerkdurchsatz und beobachtete Latenz bei Anfragen und Antworten mit Elastic Load Balancing. Wenn möglich, sollten Sie eine Metrik verwenden, die auf das Kundenerlebnis hinweist. In der Regel handelt es sich um eine benutzerdefinierte Metrik, die aus Anwendungscode innerhalb Ihrer Workload stammen kann. Um in diesem Dokument zu erläutern, wie die Nachfrage dynamisch gedeckt werden kann, werden wir Auto Scaling in zwei Kategorien einteilen, nämlich nachfragebasierte und zeitbasierte Angebotsmodelle, und uns eingehend mit den einzelnen Modellen befassen.

**Nachfragebasiertes Angebot:** Nutzen Sie die Elastizität der Cloud, um Ressourcen bereitzustellen, die sich ändernden Anforderungen gerecht werden, indem Sie sich auf den Nachfragestatus nahezu in Echtzeit verlassen. Für bedarfsorientierte Angebots-, Nutzungs APIs - oder Servicefunktionen, mit denen Sie die Menge der Cloud-Ressourcen in Ihrer Architektur programmgesteuert variieren können. Auf diese Weise können Sie Komponenten in Ihrer Architektur skalieren und die Anzahl der Ressourcen in Bedarfsspitzenzeiten zur Aufrechterhalten der Leistung erhöhen und die Kapazität zur Reduzierung der Kosten herabsetzen, wenn der Bedarf abklingt.

## Bedarfsorientiertes Angebot (dynamische Skalierungsrichtlinien)



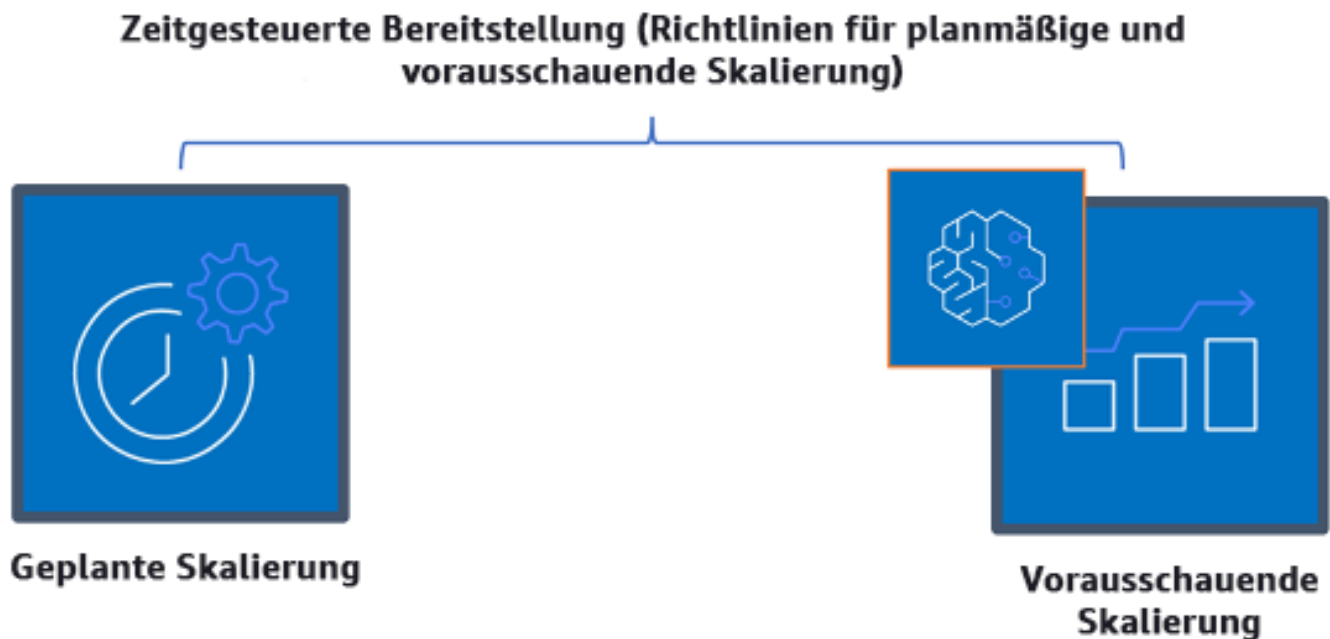
### Bedarfsbasierte dynamische Skalierungsrichtlinien

- **Einfache/schrittweise Skalierung:** Überwacht Metriken und fügt Instances gemäß den vom Kunden manuell definierten Schritten hinzu oder entfernt sie.
- **Zielverfolgung:** Ein thermostatähnlicher Steuermechanismus, der automatisch Instances hinzufügt oder entfernt, um die Metriken an einem vom Kunden definierten Ziel zu halten.



Beim Aufbau der Architektur mit einem bedarfsbasierten Ansatz sollten Sie die folgenden beiden wichtigen Aspekte berücksichtigen: 1. Machen Sie sich damit vertraut, wie schnell Sie neue Ressourcen bereitstellen müssen. 2. Machen Sie sich damit vertraut, dass sich die Größe der Marge zwischen Angebot und Nachfrage ändern wird. Sie müssen darauf vorbereitet sein, das Intervall der Änderung in Bezug auf die Nachfrage zu verarbeiten, und auch Ressourcenfehler einkalkulieren.

**Zeitbasiertes Angebot:** Ein zeitbasierter Ansatz richtet die Ressourcenkapazität an der Nachfrage aus, die vorhersehbar oder eindeutig durch die Zeit definiert ist. Dieser Ansatz ist in der Regel nicht abhängig vom Nutzungsgrad der Ressourcen. Mit einem zeitbasierten Ansatz können Sie sicherstellen, dass Ressourcen zu dem Zeitpunkt zur Verfügung stehen, zu dem sie benötigt werden, und ohne Verzögerung aufgrund von Startverfahren und System- oder Konsistenzprüfungen bereitgestellt werden können. Durch die Verwendung eines zeitbasierten Ansatzes können Sie zusätzliche Ressourcen hinzufügen oder die Kapazität in Spitzenzeiten erhöhen.



### Zeitbasierte Skalierungsrichtlinien

Sie können geplantes oder vorausschauendes Auto Scaling verwenden, um einen zeitbasierten Ansatz zu implementieren. Workloads können zu bestimmten Zeiten auf Basis eines Zeitplans auf- oder abskaliert werden, z. B. zu Beginn der Geschäftszeiten. Dadurch sind ausreichende Ressourcen verfügbar, wenn die Benutzer ankommen oder die Nachfrage steigt. Die vorausschauende Skalierung verwendet Muster zum Aufskalieren, während bei der geplanten Skalierung vordefinierte Zeiten

für die Aufskalierung verwendet werden. Sie können in Auto Scaling Scaling-Gruppen auch eine [attributbasierte Strategie zur Auswahl des Instanztyps \(ABS\)](#) verwenden, mit der Sie Ihre Instance-Anforderungen als eine Reihe von Attributen wie vCPU, Arbeitsspeicher und Speicher ausdrücken können. Auf diese Weise können Sie auch automatisch Instance-Typen der neueren Generation verwenden, wenn sie veröffentlicht werden, und mit Amazon EC2 Spot-Instances auf ein breiteres Kapazitätsspektrum zugreifen. Amazon EC2 Fleet und Amazon EC2 Auto Scaling wählen Instances aus und starten sie, die den angegebenen Attributen entsprechen, sodass die Instance-Typen nicht manuell ausgewählt werden müssen.

Sie können auch die Funktionen [AWS APIs und SDKs](#) und [AWS CloudFormation](#), um ganze Umgebungen nach Bedarf automatisch bereitzustellen und außer Betrieb zu nehmen. Dieser Ansatz eignet sich hervorragend für Entwicklungs- und Testumgebungen, die nur zu Geschäftszeiten oder in bestimmten Zeiträumen ausgeführt werden. Sie können APIs verwenden, um die Größe von Ressourcen innerhalb einer Umgebung zu skalieren (vertikale Skalierung). So könnten Sie beispielsweise eine Produktions-Workload hochskalieren, indem Sie die Instance-Größe oder -Klasse ändern. Stoppen und starten Sie dazu die Instance, und wählen Sie eine andere Instance-Größe oder -Klasse aus. Diese Technik kann auch auf andere Ressourcen angewendet werden, z. B. auf Amazon EBS Elastic Volumes, die während der Verwendung geändert werden können, um die Größe zu erhöhen, die Leistung anzupassen (IOPS) oder den Volumetyp zu ändern.

Beim Aufbau der Architektur mit einem zeitbasierten Ansatz sollten Sie die beiden folgenden wichtigen Aspekte berücksichtigen: 1: Wie konsistent ist das Nutzungsmuster? 2. Wie wirken sich Musteränderungen aus? Sie können die Treffergenauigkeit für Prognosen durch die Überwachung Ihrer Workloads und die Verwendung von Business Intelligence erhöhen. Wenn Sie signifikante Änderungen im Nutzungsmuster erkennen, können Sie die Zeiten ändern, um eine Deckung zu gewährleisten.

## Implementierungsschritte

- Konfigurieren der geplanten Skalierung: Für vorhersehbare Änderungen des Bedarfs kann die zeitbasierte Skalierung die richtige Anzahl an Ressourcen in einem angemessenen Zeitraum bereitstellen. Es ist auch nützlich, wenn die Ressourcenerstellung und -konfiguration nicht schnell genug ist, um bei Bedarf auf Änderungen zu reagieren. Mithilfe der Workload-Analyse konfigurieren Sie die geplante Skalierung mithilfe von AWS Auto Scaling. Um die zeitbasierte Planung zu konfigurieren, können Sie die vorausschauende Skalierung der geplanten Skalierung verwenden, um die Anzahl der EC2 Amazon-Instances in Ihren Auto Scaling Scaling-Gruppen im Voraus entsprechend den erwarteten oder vorhersehbaren Laständerungen zu erhöhen.

- **Predictive Scaling konfigurieren:** Mit Predictive Scaling können Sie die Anzahl der EC2 Amazon-Instances in Ihrer Auto Scaling Group erhöhen, bevor die täglichen und wöchentlichen Muster der Verkehrsflüsse berücksichtigt werden. Wenn Sie regelmäßige Spitzen beim Datenverkehr sowie Anwendungen haben, die lange brauchen, um zu starten, sollten Sie die vorausschauende Skalierung in Betracht ziehen. Die vorausschauende Skalierung kann Ihnen helfen, schneller zu skalieren, indem die Kapazität vor der prognostizierten Last initialisiert wird, im Gegensatz zur dynamischen Skalierung, die nur reaktiv ist. Wenn die Benutzer Ihre Workloads beispielsweise mit Beginn der Geschäftszeiten nutzen und sie nach Geschäftsschluss nicht mehr brauchen, kann die vorausschauende Skalierung die Kapazität vor den Geschäftszeiten erhöhen. Die Verzögerung, die bei der dynamischen Skalierung entsteht, bis sie auf den veränderten Datenverkehr reagiert, entfällt somit.
- **Konfigurieren von dynamischer automatischer Skalierung:** Verwenden Sie Auto Scaling, um die Skalierung auf der Grundlage von aktiven Workload-Metriken zu konfigurieren. Verwenden Sie die Analyse und konfigurieren Sie Auto Scaling so, dass es auf den richtigen Ressourcenebenen gestartet wird. Achten Sie darauf, dass die Workload in der erforderlichen Zeit skaliert wird. Sie können eine Flotte von On-Demand-Instances und Spot-Instances innerhalb einer einzigen Auto-Scaling-Gruppe starten und automatisch skalieren. Zusätzlich zum Erhalt von Rabatten für die Verwendung von Spot-Instances können Sie mit Reserved Instances oder einem Savings Plan Rabatte auf die regulären On-Demand-Instance-Preise erhalten. All diese Faktoren zusammen helfen Ihnen dabei, Ihre Kosteneinsparungen für EC2 Amazon-Instances zu optimieren und die gewünschte Skalierung und Leistung für Ihre Anwendung zu erzielen.

## Ressourcen

### Zugehörige Dokumente:

- [AWS Auto Scaling](#)
- [AWS Instance Scheduler](#)
- Skalieren der Größe Ihrer Auto-Scaling-Gruppe
- [Erste Schritte mit Amazon EC2 Auto Scaling](#)
- [Erste Schritte mit Amazon SQS](#)
- [Geplante Skalierung für Amazon EC2 Auto Scaling](#)
- [Vorausschauende Skalierung für Amazon EC2 Auto Scaling](#)

### Zugehörige Videos:

- [Target Tracking Scaling Policies for Auto Scaling](#)
- [AWS Instanzplaner](#)

Zugehörige Beispiele:

- [Attributbasierte Instance-Typauswahl für Auto Scaling für Amazon EC2 Fleet](#)
- [Optimizing Amazon Elastic Container Service for cost using scheduled scaling](#)
- [Vorausschauende Skalierung mit Amazon EC2 Auto Scaling](#)
- [Wie verwende ich Instance Scheduler, um EC2 Amazon-Instances AWS CloudFormation zu planen?](#)

## Optimierung im Laufe der Zeit

Fragen

- [COST10. Wie können Sie neue Services bewerten?](#)
- [COST11. Wie bewerten Sie die Kosten des Aufwands?](#)

### COST10. Wie können Sie neue Services bewerten?

Bei AWS der Veröffentlichung neuer Dienste und Funktionen empfiehlt es sich, Ihre bestehenden Architekturentscheidungen zu überprüfen, um sicherzustellen, dass sie auch weiterhin die kostengünstigsten sind.

Bewährte Methoden

- [COST10-BP01 Entwickeln Sie einen Prozess zur Überprüfung der Arbeitslast](#)
- [COST10-BP02 Überprüfen und analysieren Sie diesen Workload regelmäßig](#)

#### COST10-BP01 Entwickeln Sie einen Prozess zur Überprüfung der Arbeitslast

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, deren Wert mehr als 10 % der Rechnung ausmacht, vierteljährlich oder alle sechs Monate zu prüfen, während Workloads mit einem Wert von weniger als 10 % der Rechnung jährlich überprüft werden sollten.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Hoch

## Implementierungsleitfaden

Um sicherzustellen, dass Sie immer die kosteneffizienteste Workload haben, müssen Sie die Workload regelmäßig überprüfen, um zu wissen, ob es Möglichkeiten gibt, neue Services, Features und Komponenten zu implementieren. Damit Sie insgesamt niedrigere Kosten erzielen, muss der Prozess proportional zu den potenziellen Einsparungen sein. Beispielsweise sollten Workloads, die 50 % Ihrer Gesamtausgaben ausmachen, regelmäßiger und gründlicher überprüft werden als Workloads, die 5 % Ihrer Gesamtausgaben ausmachen. Lassen Sie auch externe Faktoren oder Volatilität in Ihre Überlegungen einfließen. Wenn die Workload eine bestimmte Geografie oder ein bestimmtes Marktsegment bedient und Änderungen in diesem Bereich vorhergesagt werden, können häufigere Überprüfungen zu Kosteneinsparungen führen. Ein weiterer Faktor bei der Überprüfung ist die Implementierung von Änderungen. Wenn es erhebliche Kosten für das Testen und Validieren von Änderungen gibt, sollten Überprüfungen seltener erfolgen.

Denken Sie an die langfristigen Kosten für die Wartung veralteter Komponenten und Ressourcen sowie die Unfähigkeit, neue Features in diese zu implementieren. Die aktuellen Kosten für Tests und Validierung können den vorgeschlagenen Vorteil übersteigen. Doch mit der Zeit können sich die Kosten für die Änderung erheblich erhöhen, da die Lücke zwischen der Workload und den aktuellen Technologien zunimmt, was zu noch größeren Kosten führt. Beispielsweise sind die Kosten für den Wechsel zu einer neuen Programmiersprache derzeit möglicherweise nicht günstig. In fünf Jahren können sich jedoch die Kosten für Personen, die in dieser Sprache qualifiziert sind, erhöhen. Aufgrund des Wachstums der Workload würden Sie ein noch größeres System in die neue Sprache verlagern, was noch mehr Aufwand erfordert als zuvor.

Unterteilen Sie Ihre Workload in Komponenten, weisen Sie die Kosten der Komponente zu (eine Schätzung reicht aus) und listen Sie dann die Faktoren (z. B. Aufwand und externe Märkte) neben den einzelnen Komponenten auf. Verwenden Sie diese Indikatoren, um eine Überprüfungshäufigkeit für jede Workload zu bestimmen. Zum Beispiel können bei Webservern hohe Kosten, geringer Änderungsaufwand und hohe externe Faktoren anfallen, was zu einer hohen Überprüfungshäufigkeit führt. Bei einer zentralen Datenbank können mittlere Kosten, hoher Änderungsaufwand und niedrige externe Faktoren anfallen, was zu einer mittleren Überprüfungshäufigkeit führt.

Definieren Sie einen Prozess, mit dem sich neu verfügbare Services, Designmuster, Ressourcentypen und Konfigurationen zur Optimierung Ihrer Workload-Kosten bewerten lassen. Ähnlich wie bei der [Prüfung der Säule „Leistungseffizienz“](#) und der [Prüfung der Säule „Zuverlässigkeit“](#) identifizieren, validieren und priorisieren Sie Optimierungs- und

Verbesserungsmaßnahmen. Führen Sie eine Problembehandlung durch und nehmen Sie diese in Ihr Backlog auf.

### Implementierungsschritte

- **Festlegen der Überprüfungshäufigkeit:** Legen Sie fest, wie häufig die Workload und ihre Komponenten überprüft werden sollen. Reservieren Sie Zeit und Ressourcen, um eine kontinuierliche Verbesserungen zu ermöglichen, und prüfen Sie die Häufigkeit, um Ihre Workload zu optimieren und effizienter zu gestalten. Dies ist eine Kombination von Faktoren und kann sich von Workload zu Workload innerhalb Ihrer Organisation und zwischen Komponenten in der Workload unterscheiden. Häufige Faktoren sind u. a. die Bedeutung für die Organisation, gemessen in Bezug auf Umsatz oder Marke, die Gesamtkosten für die Ausführung der Workload (einschließlich Betriebs- und Ressourcenkosten), die Komplexität der Workload, wie einfach es ist, eine Änderung zu implementieren, Softwarelizenzvereinbarungen sowie Änderungen, die aufgrund mangelhafter Lizenzen erhebliche Erhöhungen der Lizenzkosten verursachen würden. Komponenten können funktional oder technisch definiert werden, z. B. Webserver und Datenbanken oder Datenverarbeitungs- und Speicherressourcen. Gleichen Sie die Faktoren entsprechend aus und entwickeln Sie einen Zeitraum für die Workload und ihre Komponenten. Sie können sich entscheiden, die vollständigen Workload alle 18 Monate, die Webserver alle 6 Monate, die Datenbank alle 12 Monate, die Datenverarbeitungs- und Kurzzeitspeicherung alle 6 Monate und die Langzeitspeicherung alle 12 Monate zu überprüfen.
- **Festlegen der Prüfungsgründlichkeit:** Legen Sie den Aufwand für die Prüfung der Workload oder der Workload-Komponenten fest. Ähnlich wie bei der Überprüfungsfrequenz geht es hier um mehrere Faktoren, die ausgeglichen sein müssen. Bewerten und priorisieren Sie regelmäßig Verbesserungsmöglichkeiten, um die Maßnahmen dort zu intensivieren, wo sie den größten Nutzen bringen. So erfahren Sie auch, wie viel Aufwand für diese Aktivitäten erforderlich ist. Wenn die erwarteten Ergebnisse die Ziele nicht erfüllen und der Aufwand mehr kostet, wiederholen Sie den Versuch mit alternativen Vorgehensweisen. Bei Ihren Prüfungen sollten auch Zeit und Ressourcen genutzt werden, um kontinuierliche, schrittweise Verbesserungen zu ermöglichen. Sie können beispielsweise entscheiden, für die Analyse der Datenbankkomponente eine Woche, für die Analyse von Datenverarbeitungsressourcen eine Woche und für die Analyse von Speicherprüfungen vier Stunden aufzuwenden.

### Ressourcen

#### Zugehörige Dokumente:

- [AWS Nachrichten-Blog](#)

- [Arten von Cloud Computing](#)
- [Neuerungen bei AWS](#)

Zugehörige Beispiele:

- [AWS Support Sie proaktive Services](#)
- [Regelmäßige Workload-Überprüfungen von SAP Workloads](#)

COST10-BP02 Überprüfen und analysieren Sie diesen Workload regelmäßig

Bestehende Workloads werden basierend auf den einzelnen definierten Prozessen regelmäßig überprüft, um zu ermitteln, ob neue Services übernommen, vorhandene Services ersetzt oder die Architektur von Workloads geändert werden können.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Mittel

Implementierungsleitfaden

AWS fügt ständig neue Funktionen hinzu, sodass Sie mit der neuesten Technologie schneller experimentieren und Innovationen umsetzen können. [AWS Was AWS ist neu?](#) beschreibt, wie das funktioniert, und bietet einen schnellen Überblick über AWS Dienste, Funktionen und Ankündigungen regionaler Erweiterungen, sobald diese veröffentlicht werden. Sie können sich eingehender über die angekündigten Veröffentlichungen informieren und diese zur Prüfung und Analyse Ihrer bestehenden Workloads verwenden. Um die Vorteile neuer AWS Dienste und Funktionen zu nutzen, überprüfen Sie Ihre Workloads und implementieren bei Bedarf neue Dienste und Funktionen. Das bedeutet, dass Sie möglicherweise bestehende Dienste, die Sie für Ihre Workloads verwenden, ersetzen oder Ihren Workload modernisieren müssen, um diese neuen AWS Services einzuführen. Sie können beispielsweise Ihre Workloads überprüfen und die Messaging-Komponente durch Amazon Simple Email Service ersetzen. Dadurch entfallen die Kosten für den Betrieb und die Verwaltung einer Flotte von Instances, während die gesamte Funktionalität zu geringeren Kosten bereitgestellt wird.

Bei der Analyse Ihrer Workload und der Ermittlung potenzieller Chancen sollten Sie nicht nur neue Services, sondern auch neue Möglichkeiten zur Entwicklung von Lösungen berücksichtigen. Sehen Sie sich die Videos von [This is My Architecture](#) an AWS, um mehr über die Architekturentwürfe anderer Kunden, ihre Herausforderungen und Lösungen zu erfahren. Schauen Sie sich die [All-In-Serie an](#), um mehr über reale Anwendungen von AWS Diensten und Kundenberichte zu erfahren. Sie können sich auch die Videoreihe [Back to Basics](#) (Zurück zu den Grundlagen) ansehen, in der bewährte Methoden zum grundlegenden Cloud-Architekturmuster erklärt, untersucht und

aufgeschlüsselt werden. Eine weitere Quelle sind die Videos „[How to Build This](#)“, die Menschen mit großen Ideen dabei helfen sollen, ihr Produkt (MVP) mit Hilfe von AWS Dienstleistungen zum Leben zu erwecken. Auf diese Weise können sich Bauherren aus der ganzen Welt, die eine starke Idee haben, architektonische Beratung von erfahrenen AWS Solutions Architects einholen. In unseren Ressourcenmaterialien unter [Erste Schritte](#) finden Sie darüber hinaus ausführliche Tutorials.

Befolgen Sie vor dem Starten Ihres Überprüfungsprozesses die Anforderungen Ihres Unternehmens in Bezug auf die Workload, die Sicherheit und den Datenschutz, um einen spezifischen Service oder eine spezifische Region zu nutzen. Befolgen Sie während des vereinbarten Überprüfungsprozesses die Leistungsanforderungen.

### Implementierungsschritte

- **Regelmäßige Überprüfung der Workload:** Führen Sie mit Ihrem definierten Prozess Überprüfungen mit der angegebenen Häufigkeit durch. Stellen Sie sicher, dass Sie den richtigen Aufwand für jede Komponente aufwenden. Dieser Prozess ähnelt dem anfänglichen Designprozess, bei dem Sie Services für die Kostenoptimierung ausgewählt haben. Analysieren Sie die Services und die Vorteile, die sie mit sich bringen würden, sowie den Zeitfaktor bei den Änderungskosten. Analysieren Sie nicht nur die langfristigen Vorteile.
- **Implementieren neuer Services:** Wenn es das Ziel der Analyse ist, Änderungen zu implementieren, führen Sie zunächst eine Analyse der Basisanforderungen der Workload durch, um die aktuellen Kosten für jede Ausgabe festzustellen. Implementieren Sie die Änderungen und führen Sie dann eine Analyse durch, um die neuen Kosten für jede Ausgabe zu bestätigen.

### Ressourcen

#### Zugehörige Dokumente:

- [AWS Nachrichten-Blog](#)
- [Neuerungen bei AWS](#)
- [AWS Dokumentation](#)
- [AWS Erste Schritte](#)
- [AWS Allgemeine Ressourcen](#)

#### Zugehörige Videos:

- [AWS - Das ist meine Architektur](#)



- [AWS - Zurück zu den Grundlagen](#)
- [AWS - All-In-Serie](#)
- [How to Build This](#)

## COST11. Wie bewerten Sie die Kosten des Aufwands?

### Bewährte Methoden

- [COST11-BP01 Führen Sie eine Automatisierung für den Betrieb durch](#)

### COST11-BP01 Führen Sie eine Automatisierung für den Betrieb durch

Bewerten Sie die Betriebskosten in der Cloud und konzentrieren Sie sich dabei auf die Quantifizierung der Zeit- und Aufwandsersparnisse bei administrativen Aufgaben und Bereitstellungen, der Minimierung des Risikos menschlicher Fehler, Compliance und anderen Abläufen durch Automatisierung. Ermitteln Sie den Zeitaufwand und die damit verbundenen Kosten, die für den betrieblichen Aufwand erforderlich sind, und implementieren Sie die Automatisierung von Verwaltungsaufgaben, um den manuellen Aufwand zu minimieren, wo immer dies möglich ist.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Niedrig

### Implementierungsleitfaden

Die Automatisierung von Abläufen reduziert die Häufigkeit von manuellen Aufgaben, optimiert die Effizienz und bietet Kunden Vorteile, indem sie eine konsistente und zuverlässige Umgebung bei der Bereitstellung, Verwaltung oder dem Betrieb von Workloads ermöglicht. Sie können Infrastrukturressourcen von manuellen Betriebsaufgaben entlasten und für hochwertigere Aufgaben sowie Innovationen einsetzen, was den Unternehmenswert verbessert. Unternehmen benötigen eine bewährte, getestete Möglichkeit, ihre Workloads in der Cloud zu verwalten. Diese Lösung muss sicher, schnell und kostengünstig sein, mit minimalem Risiko und maximaler Zuverlässigkeit.

Beginnen Sie damit, Ihre Betriebsabläufe basierend auf dem erforderlichen Aufwand zu priorisieren, indem Sie sich die Gesamtbetriebskosten ansehen. Beispiel: Wie lange dauert es, neue Ressourcen in der Cloud bereitzustellen, vorhandene Ressourcen zu optimieren oder die notwendigen Konfigurationen zu implementieren? Sehen Sie sich die Gesamtkosten für die menschliche Arbeitskraft an und berücksichtigen Sie dabei die Kosten für Betriebsabläufe und Verwaltung. Priorisieren Sie die Automatisierung von Verwaltungsaufgaben, um die menschliche Arbeitskraft zu reduzieren.

Der Überprüfungsaufwand sollte in einem angemessenen Verhältnis zum potenziellen Nutzen stehen. Beispiel: Untersuchen Sie den Zeitaufwand für das manuelle im Vergleich zum automatischen Ausführen von Aufgaben. Priorisieren Sie die Automatisierung sich wiederholender, hochwertiger, zeitaufwändiger und komplexer Aktivitäten. Aufgaben mit hohem Wert oder einem hohen Risiko von menschlichen Fehlern sind in der Regel der bessere Ausgangspunkt für Automatisierungen, da das Risiko oft unerwünschte zusätzliche Betriebskosten (z. B. für Überstunden des Betriebsteams) mit sich bringt.

Verwenden Sie Automatisierungstools wie AWS Systems Manager oder AWS Config zur Optimierung von Betriebs-, Compliance-, Überwachungs-, Lebenszyklus- und Kündigungsprozessen. Mit AWS Services, Tools und Produkten von Drittanbietern können Sie die von Ihnen implementierten Automatisierungen an Ihre spezifischen Anforderungen anpassen. Die folgende Tabelle zeigt einige der zentralen Betriebsfunktionen der AWS -Services, mit denen Sie die Verwaltung und die Betriebsabläufe automatisieren können:

- [AWS Audit Manager](#): Überprüfen Sie Ihre AWS Nutzung kontinuierlich, um die Risiko- und Compliance-Bewertung zu vereinfachen
- [AWS Backup](#): Zentrale Verwaltung und Automatisierung des Datenschutzes
- [AWS Config](#): Konfiguration von Datenverarbeitungsressourcen, Bewertung, Prüfung und Auswertung von Konfigurationen und Ressourceninventar
- [AWS CloudFormation](#): Starten von hochverfügbaren Ressourcen mit Infrastructure as Code
- [AWS CloudTrail](#): IT-Änderungsmanagement, Compliance und Kontrolle
- [Amazon](#) Ereignisse EventBridge planen und auslösen AWS Lambda , um Maßnahmen zu ergreifen.
- [AWS Lambda](#): Automatisieren Sie sich wiederholende Prozesse, indem Sie sie mit Ereignissen auslösen oder sie nach einem festen Zeitplan mit ausführen. AWS EventBridge
- [AWS Systems Manager](#): Starten und Stoppen von Workloads, Patchen von Betriebssystemen, Automatisierung der Konfiguration und fortlaufende Verwaltung.
- [AWS Step Functions](#): Planen von Aufträgen und Automatisieren von Workflows
- [AWS Service Catalog](#): Vorlagennutzung und Infrastructure as Code mit Compliance und Kontrolle

Wenn Sie bei der Nutzung von AWS Produkten und Services sofort Automatisierungen einführen möchten und in Ihrem Unternehmen noch nicht über entsprechende Fähigkeiten verfügen, wenden Sie sich an [AWS Managed Services \(AMS\)](#), [AWS Professional Services](#) oder [AWS Partner](#), um die Akzeptanz von Automatisierung zu erhöhen und Ihre operative Exzellenz in der Cloud zu verbessern.

AWS Managed Services (AMS) ist ein Service, der die AWS Infrastruktur im Auftrag von Unternehmenskunden und Partnern betreibt. Er bietet eine sichere und konforme Umgebung, in der Sie Ihre Workloads bereitstellen können. AMS verwendet automatisierte Cloud-Betriebsmodelle für Unternehmen, damit Sie die Anforderungen Ihres Unternehmens erfüllen, schneller in die Cloud wechseln und Ihre laufenden Verwaltungskosten senken können.

AWS Professional Services können Ihnen auch dabei helfen, Ihre gewünschten Geschäftsergebnisse zu erzielen und Abläufe zu AWS automatisieren. Sie unterstützen die Kunden bei der Bereitstellung von automatisierten, robusten und agilen IT-Abläufen sowie für die Cloud optimierten Governance-Funktionen. Detaillierte Überwachungsbeispiele und empfohlene bewährte Methoden finden Sie im Whitepaper zur Säule für die betriebliche Effizienz.

### Implementierungsschritte

- Einmal erstellen und viele bereitstellen: Verwenden Sie „infrastructure-as-code“ CloudFormation, oder AWS SDK, AWS CLI um die Bereitstellung einmal durchzuführen und dann mehrfach für ähnliche Umgebungen oder für Notfallwiederherstellungsszenarien zu verwenden. Nutzen Sie während der Bereitstellung Tags, um die Nutzung wie in anderen bewährten Methoden beschrieben zu verfolgen. Wird verwendet [AWS Launch Wizard](#), um die Zeit für die Bereitstellung vieler beliebter Unternehmens-Workloads zu reduzieren. AWS Launch Wizard führt Sie anhand von AWS bewährten Methoden durch die Dimensionierung, Konfiguration und Bereitstellung von Unternehmens-Workloads. Sie können auch den [Service Catalog](#) verwenden, mit dem Sie infrastructure-as-code genehmigte Vorlagen erstellen und verwalten können, AWS damit jeder auf genehmigte Self-Service-Cloud-Ressourcen zugreifen kann.
- Automatisieren von kontinuierlicher Compliance: Erwägen Sie, die Bewertung und Korrektur aufgezeichneter Konfigurationen anhand vordefinierter Standards zu automatisieren. In Kombination AWS Organizations mit den Funktionen von AWS Config und [AWS CloudFormation](#) können Sie die Einhaltung der Konfigurationsbestimmungen für Hunderte von Mitgliedskonten effizient und in großem Umfang verwalten und automatisieren. Sie können Änderungen an Konfigurationen und Beziehungen zwischen AWS Ressourcen überprüfen und in den Verlauf einer Ressourcenkonfiguration eintauchen.
- Automatisieren von Überwachungsaufgaben: AWS bietet verschiedene Tools, mit denen Sie Services überwachen können. Sie können diese Tools so konfigurieren, dass sie Überwachungsaufgaben automatisieren. Erstellen und implementieren Sie einen Überwachungsplan, der Überwachungsdaten aus allen Teilen Ihrer Workload erfasst, sodass Sie einen Mehrpunktausfall, falls ein solcher auftritt, einfacher debuggen können. Beispielsweise können Sie die automatisierten Überwachungstools verwenden, um Amazon zu beobachten EC2

und Ihnen zu melden, wenn bei Systemstatusprüfungen, Instanzstatusprüfungen und CloudWatch Amazon-Alarmen etwas nicht stimmt.

- Automatisieren von Wartung und Betrieb: Führen Sie Routineaufgaben automatisch ohne menschliche Eingriffe aus. Mithilfe von AWS Services und Tools können Sie auswählen, welche AWS Automatisierungen implementiert und an Ihre spezifischen Anforderungen angepasst werden sollen. Verwenden Sie [EC2Image Builder](#) beispielsweise zum Erstellen, Testen und Bereitstellen von virtuellen Maschinen- und Container-Images zur Verwendung vor Ort AWS oder zum Patchen Ihrer EC2 Instanzen mit. AWS SSM Wenn Ihre gewünschte Aktion mit AWS Diensten nicht durchgeführt werden kann oder Sie komplexere Aktionen zum Filtern von Ressourcen benötigen, automatisieren Sie Ihre Abläufe mithilfe von [AWS Command Line Interface](#)(AWS CLI) oder AWS SDK Tools. AWS CLI bietet die Möglichkeit, den gesamten Prozess der Steuerung und Verwaltung von AWS Diensten mithilfe von Skripten zu automatisieren, ohne die AWS Management Console. Wählen Sie Ihre bevorzugte Option AWS SDKs für die Interaktion mit AWS Diensten aus. Weitere Codebeispiele finden Sie im [Repository für AWS SDK Codebeispiele](#).
- Schaffen eines kontinuierlichen Lebenszyklus mit Automatisierungen: Es ist wichtig, dass Sie ausgereifte Lebenszyklusrichtlinien einrichten und beibehalten, nicht nur für Vorschriften oder Redundanz, sondern auch für die Kostenoptimierung. Sie können es verwenden AWS Backup , um den Datenschutz von Datenspeichern, wie z. B. Ihren Buckets, Volumes, Datenbanken und Dateisystemen, zentral zu verwalten und zu automatisieren. Sie können Amazon Data Lifecycle Manager auch verwenden, um die Erstellung, Aufbewahrung und Löschung von EBS Snapshots und Backups zu automatisierenEBS. AMIs
- Löschen Sie nicht benötigte Ressourcen: Es ist durchaus üblich, ungenutzte Ressourcen in einer Sandbox oder in der Entwicklung anzuhäufen. AWS-Konten Entwickler erstellen und experimentieren im Rahmen des normalen Entwicklungszyklus mit verschiedenen Services und Ressourcen, und dann löschen sie diese Ressourcen nicht, wenn sie nicht mehr benötigt werden. Ungenutzte Ressourcen können unnötige und manchmal hohe Kosten für die Organisation verursachen. Durch das Löschen dieser Ressourcen können die Kosten für den Betrieb dieser Umgebungen gesenkt werden. Vergewissern Sie sich im Zweifelsfall, dass diese Daten nicht benötigt werden oder gesichert sind. Sie können AWS CloudFormation verwenden, um bereitgestellte Stapel zu bereinigen, wodurch die meisten in der Vorlage definierten Ressourcen automatisch gelöscht werden. Alternativ können Sie mithilfe von Tools wie [aws-nuke](#) eine Automatisierung für das Löschen von AWS Ressourcen erstellen.

Ressourcen

Zugehörige Dokumente:

- [Modernisierung des Betriebs in der AWS Cloud](#)
- [AWS Services for Automation](#)
- [Integration & Automation](#)
- [AWS Systems Manager Automatisierung](#)
- [Automated and manual monitoring](#)
- [AWS Automatisierungen für SAP Verwaltung und Betrieb](#)
- [AWS Managed Services](#)
- [AWS Professional Services](#)

Zugehörige Videos:

- [Automatisieren Sie die kontinuierliche Einhaltung von Vorschriften in großem Umfang AWS](#)
- [AWS Backup Demo: Konto- und regionsübergreifendes Backup](#)
- [Patches für Ihre Amazon-Instances EC2](#)

Zugehörige Beispiele:

- [Reinventing automated operations \(Part I\)](#)
- [Reinventing automated operations \(Part II\)](#)
- [Automatisieren Sie das Löschen von AWS Ressourcen mithilfe von aws-nuke](#)
- [Löschen Sie ungenutzte EBS Amazon-Volumes mit AWS Config und AWS SSM](#)
- [Automatisieren Sie die kontinuierliche Einhaltung von Vorschriften in großem Umfang AWS](#)
- [IT-Automatisierungen mit AWS Lambda](#)

## Nachhaltigkeit

Bei der Säule „Nachhaltigkeit“ geht es darum, die Auswirkungen der genutzten Services zu verstehen, diese über den gesamten Workload-Lebenszyklus hinweg zu quantifizieren sowie konzeptionelle Grundsätze und bewährte Methoden einzusetzen, die dabei helfen, diese Auswirkungen zu reduzieren, wenn Cloud-Workloads erstellt werden. Verbindliche Anleitungen zur Implementierung finden Sie im [Whitepaper „Säule der Nachhaltigkeit“](#).

Bereiche für bewährte Methoden

- [Auswahl der Region](#)
- [Ausrichtung am Bedarf](#)
- [Software und Architektur](#)
- [Daten](#)
- [Hardware und Services](#)
- [Prozess und Kultur](#)

## Auswahl der Region

### Frage

- [SUS1 Wie wählen Sie Regionen für Ihren Workload aus?](#)

### SUS1 Wie wählen Sie Regionen für Ihren Workload aus?

Die Wahl der Region für Ihren Workload wirkt sich erheblich auf dessen LeistungKPIs, Kosten und CO2-Fußabdruck aus. Um diese effektiv zu verbessernKPIs, sollten Sie Regionen für Ihre Workloads auswählen, die sowohl auf Geschäftsanforderungen als auch auf Nachhaltigkeitszielen basieren.

### Bewährte Methoden

- [SUS01-BP01 Wählen Sie die Region auf der Grundlage von Geschäftsanforderungen und Nachhaltigkeitszielen](#)

SUS01-BP01 Wählen Sie die Region auf der Grundlage von Geschäftsanforderungen und Nachhaltigkeitszielen

Wählen Sie eine Region für Ihren Workload aus, die sowohl auf Ihren Geschäftsanforderungen als auch auf Ihren Nachhaltigkeitszielen basiert, um diese Region zu optimierenKPIs, einschließlich Leistung, Kosten und CO2-Fußabdruck.

### Typische Anti-Muster:

- Sie wählen die Region der Workload auf der Grundlage Ihres eigenen Standorts aus.
- Sie konsolidieren alle Workload-Ressourcen an einem einzelnen geografischen Standort.

Vorteile der Nutzung dieser bewährten Methode: Wenn Sie eine Workload in der Nähe von Amazon-Projekten für erneuerbare Energien oder in Regionen mit nachweislich niedrigen Kohlendioxidemissionen platzieren, kann die CO<sub>2</sub>-Bilanz einer Clouds-Workload gesenkt werden.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel

### Implementierungsleitfaden

Dabei AWS Cloud handelt es sich um ein ständig wachsendes Netzwerk von Regionen und Präsenzpunkten (PoP) mit einer globalen Netzwerkinfrastruktur, die diese miteinander verbindet. Die Wahl der Region für Ihren Workload wirkt sich erheblich auf dessen LeistungKPIs, Kosten und CO<sub>2</sub>-Fußabdruck aus. Um diese effektiv zu verbessernKPIs, sollten Sie Regionen für Ihren Workload auswählen, die sowohl Ihren Geschäftsanforderungen als auch Ihren Nachhaltigkeitszielen entsprechen.

### Implementierungsschritte

- Befolgen Sie diese Schritte, um potenzielle Regionen für Ihre Workload zu bewerten und in die engere Auswahl zu nehmen. Berücksichtigen Sie dabei die Anforderungen Ihres Unternehmens, unter anderem in Bezug auf Compliance, verfügbare Funktionen, Kosten und Latenz:
  - Vergewissern Sie sich, dass die Regionen konform sind (basierend auf Ihren erforderlichen lokalen Vorschriften).
  - Prüfen Sie anhand der [Liste der verfügbaren AWS -Services nach Regionen](#), ob die Regionen über die für Ihre Workload erforderlichen Services und Funktionen verfügen.
  - Berechnen Sie die Kosten der Workload in jeder Region mithilfe des [AWS Pricing Calculator](#).
  - Testen Sie die Netzwerklatenz zwischen Ihren Endbenutzerstandorten und den einzelnen Standorten AWS-Region.
- Wählen Sie Regionen in der Nähe von Amazon-Projekten für erneuerbare Energien aus. Es sollte sich um Regionen handeln, in denen das Stromnetz nachweislich geringere Kohlendioxidemissionen generiert als an anderen Standorten (oder in anderen Regionen).
  - Identifizieren Sie Ihre relevanten Nachhaltigkeitsrichtlinien, um die year-to-year CO<sub>2</sub>-Emissionen auf der Grundlage des [Greenhouse Gas Protocol](#) (marktorientierte und standortbasierte Methoden) zu verfolgen und zu vergleichen.
  - Wählen Sie die Region entsprechend der Methode aus, mit der Sie CO<sub>2</sub>-Emissionen nachverfolgen. Weitere Informationen zum Auswählen einer Region anhand von Nachhaltigkeitsrichtlinien finden Sie im [Artikel zum Auswählen einer Region für Ihre Workload auf der Grundlage von Nachhaltigkeitszielen](#).

## Ressourcen

### Zugehörige Dokumente:

- [Grundlegendes zu CO2-Emissionsschätzungen](#)
- [Amazon weltweit](#)
- [Methodik für erneuerbare Energien](#)
- [„Relevante Aspekte bei der Wahl einer Region für Ihre Workloads“ erläutert](#)

### Zugehörige Videos:

- [AWS re:Invent 2023 — Nachhaltigkeitsinnovation in der globalen Infrastruktur AWS](#)
- [AWS re:INVENT 2023 — Nachhaltige Architektur: Vergangenheit, Gegenwart und future](#)
- [AWS re:Invent 2022 — Bereitstellung nachhaltiger, leistungsstarker Architekturen](#)
- [AWS re:Invent 2022 — Nachhaltig gestalten und Ihren CO2-Fußabdruck reduzieren AWS](#)
- [AWS re:Invent 2022 — Nachhaltigkeit in der globalen Infrastruktur AWS](#)

## Ausrichtung am Bedarf

### Frage

- [SUS2 Wie passen Sie Cloud-Ressourcen an Ihren Bedarf an?](#)

### SUS2 Wie passen Sie Cloud-Ressourcen an Ihren Bedarf an?

Wenn Sie berücksichtigen, wie Benutzer und Anwendungen Ihre Workloads und andere Ressourcen nutzen, können Sie auf diese Weise Verbesserungsmöglichkeiten ermitteln, um Nachhaltigkeitsziele zu erreichen. Skalieren Sie Ihre Infrastruktur so, dass Sie den Bedarf kontinuierlich anpassen können. Sorgen Sie zudem dafür, dass zur Unterstützung Ihrer Benutzer nicht mehr Ressourcen verwendet werden als unbedingt nötig. Richten Sie Service-Levels an den Kundenanforderungen aus. Positionieren Sie Ressourcen so, dass die Netzwerkkapazitäten, die für Benutzer und Anwendungen erforderlich sind, begrenzt werden. Entfernen Sie ungenutzte Komponenten. Stellen Sie Teammitgliedern Geräte zur Verfügung, die ihre Anforderungen bei geringstmöglichen Auswirkungen auf die Nachhaltigkeit erfüllen.

### Bewährte Methoden



- [SUS02-BP01 Dynamisches Skalieren der Workload-Infrastruktur](#)
- [SUS02-BP02 An den Nachhaltigkeitszielen SLAs ausrichten](#)
- [SUS02-BP03 Stoppen Sie die Erstellung und Wartung ungenutzter Ressourcen](#)
- [SUS02-BP04 Optimieren Sie die geografische Verteilung von Workloads auf der Grundlage ihrer Netzwerkanforderungen](#)
- [SUS02-BP05 Optimieren Sie die Ressourcen der Teammitglieder für die durchgeführten Aktivitäten](#)
- [SUS02-BP06 Implementieren Sie Pufferung oder Drosselung, um die Nachfragekurve abzuflachen](#)

## SUS02-BP01 Dynamisches Skalieren der Workload-Infrastruktur

Nutzen Sie die Elastizität der Cloud und skalieren Sie Ihre Infrastruktur dynamisch, um das Angebot an Cloud-Ressourcen an den Bedarf anzupassen und eine Überbereitstellung von Kapazitäten in Ihrer Workload zu vermeiden.

Typische Anti-Muster:

- Sie skalieren Ihre Infrastruktur nicht mit der Benutzerlast.
- Sie skalieren Ihre Infrastruktur immer manuell.
- Sie behalten die erhöhte Kapazität nach dem Hochskalieren bei, anstatt sie wieder herunterzuskalieren.

Vorteile der Nutzung dieser bewährten Methode: Das Konfigurieren und Testen der Workload-Elastizität trägt dazu bei, das Angebot an Cloud-Ressourcen effizient an den Bedarf anzupassen und eine Überbereitstellung von Kapazitäten zu vermeiden. Sie können die Vorteile der Elastizität in der Cloud nutzen, um die Kapazität während und nach Bedarfsspitzen automatisch zu skalieren und so sicherzustellen, dass Sie nur die Menge an Ressourcen nutzen, die für die Erfüllung Ihrer Geschäftsanforderungen erforderlich ist.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel

## Implementierungsleitfaden

Die Cloud bietet Ihnen die Flexibilität, Ressourcen dynamisch durch verschiedene Mechanismen zu erweitern oder zu reduzieren, um einem veränderten Bedarf gerecht zu werden. Eine optimale Abstimmung von Angebot und Bedarf führt zu den geringsten Auswirkungen auf die Umgebung für eine Workload.

Der Bedarf kann fest oder variabel sein und erfordert Metriken und Automatisierung, um sicherzustellen, dass die Verwaltung nicht zur Last wird. Anwendungen können vertikal (hoch oder herunter) und/oder horizontal (ab oder auf) skaliert werden. Bei der vertikalen Skalierung wird die Instance-Größe geändert, bei der horizontalen Skalierung die Anzahl von Instances.

Sie können verschiedene Ansätze nutzen, um das Angebot an Ressourcen auf den Bedarf abzustimmen.

- Zielverfolgungsansatz: Überwachen Sie Ihre Skalierungsmetriken und erhöhen oder verringern Sie die Kapazität automatisch nach Bedarf.
- Prädiktives Skalieren: Skalieren Sie auf der Grundlage erwarteter täglicher und wöchentlicher Trends.
- Zeitplanbasierter Ansatz: Legen Sie einen eigenen Skalierungszeitplan auf der Grundlage vorhersehbarer Laständerungen fest.
- Service-Skalierung: Wählen Sie Services (beispielsweise Serverless) aus, die nativ von Natur aus skalierbar sind oder Auto Scaling als Feature bieten.

Identifizieren Sie Zeiträume mit geringer oder gar keiner Nutzung und skalieren Sie Ressourcen, um überschüssige Kapazitäten zu entfernen und die Effizienz zu verbessern.

### Implementierungsschritte

- Elastizität ermöglicht die Anpassung der verfügbaren Ressourcen an den Bedarf. Instanzen, Container und Funktionen bieten Elastizitätsmechanismen, entweder in Kombination mit automatischer Skalierung oder als Funktion des Dienstes. AWS bietet eine Reihe von Auto-Scaling-Mechanismen, um sicherzustellen, dass Workloads in Zeiten geringer Benutzerlast schnell und einfach herunterskaliert werden können. Hier sind einige Beispiele für Auto-Scaling-Mechanismen:

Auto-Scaling-Mechanismus	Verwendung
<a href="#">Amazon EC2 Auto Scaling</a>	Wird verwendet, um zu überprüfen, ob Ihnen die richtige Anzahl von EC2 Amazon-Instances zur Verfügung steht, um die Benutzerlast für Ihre Anwendung zu bewältigen.

Auto-Scaling-Mechanismus	Verwendung
<a href="#">Application Auto Scaling</a>	Wird verwendet, um die Ressourcen für einzelne AWS Dienste außerhalb von Amazon automatisch zu skalieren EC2, z. B. Lambda-Funktionen oder Amazon Elastic Container Service (AmazonECS) -Services.
<a href="#">Kubernetes Cluster Autoscaler</a>	Wird verwendet, um Kubernetes-Cluster automatisch zu skalieren. AWS

- Skalierung wird häufig im Zusammenhang mit Rechendiensten wie EC2 Amazon-Instances oder AWS Lambda -Funktionen diskutiert. Ziehen Sie die Konfiguration von nicht Daten verarbeitenden Services wie Lese- und Schreibkapazitätseinheiten von [Amazon DynamoDB](#) oder Shards von [Amazon Kinesis Data Streams](#) in Betracht, um den Bedarf zu decken.
- Vergewissern Sie sich, dass die Metriken zum Hoch- oder Herunterskalieren für die jeweilige Art der bereitgestellten Workload überprüft werden. Wenn Sie eine Anwendung zur Videotranskodierung einsetzen, wird eine CPU Auslastung von 100% erwartet, was nicht Ihre primäre Messgröße sein sollte. Sie können bei Bedarf eine [benutzerdefinierte Metrik](#) (etwa die Speicherauslastung) für Ihre Skalierungsrichtlinie verwenden. Beachten Sie bei der Auswahl der richtigen Kennzahlen die folgenden Hinweise für AmazonEC2:
  - Es muss sich um eine gültige Nutzungsmetrik handeln, die beschreibt, wie stark eine Instance genutzt wird.
  - Der Wert der Metrik muss sich proportional zur Anzahl der Instances in der Auto-Scaling-Gruppe erhöhen oder verringern.
- Verwenden Sie für Ihre Auto-Scaling-Gruppe eine [dynamische Skalierung](#) anstelle einer [manuellen Skalierung](#). Außerdem empfiehlt es sich, bei der dynamischen Skalierung [Skalierungsrichtlinien zur Zielverfolgung](#) zu verwenden.
- Vergewissern Sie sich, dass Workload-Bereitstellungen sowohl Hoch- als auch Herunterskalierungsereignisse behandeln können. Erstellen Sie Testszenarien für Herunterskalierungsereignisse, um sich zu vergewissern, dass sich die Workload wie erwartet verhält und die Benutzererfahrung nicht beeinträchtigt wird (etwa durch den Verlust von Sticky Sessions). Sie können den [Aktivitätsverlauf](#) verwenden, um eine Skalierungsaktivität für eine Auto-Scaling-Gruppe zu überprüfen.
- Überprüfen Sie Ihre Workload auf vorhersagbare Muster und skalieren Sie proaktiv, wenn Sie vorhergesagte und geplante Bedarfsänderungen erwarten. Mit der prädiktiven Skalierung können

Sie die Notwendigkeit einer Überbereitstellung von Kapazitäten vermeiden. Weitere Informationen finden Sie unter [Predictive Scaling with Amazon EC2 Auto Scaling](#).

## Ressourcen

### Zugehörige Dokumente:

- [Erste Schritte mit Amazon EC2 Auto Scaling](#)
- [Prädiktive Skalierung für EC2, unterstützt durch Machine Learning](#)
- [Analysieren Sie das Nutzerverhalten mit Amazon OpenSearch Service, Amazon Data Firehose und Kibana](#)
- [Was ist Amazon CloudWatch?](#)
- [Überwachen der Datenbanklast mit Performance Insights auf Amazon RDS](#)
- [Einführung der nativen Support für Predictive Scaling mit Amazon EC2 Auto Scaling](#)
- [Vorstellung von Karpenter – Open-Source-Kubernetes-Cluster-Autoscaler mit hoher Leistung](#)
- [Tiefer Einblick in Amazon ECS Cluster Auto Scaling](#)

### Zugehörige Videos:

- [AWS re:Invent 2023 — Weitere Skalierung AWS für die ersten 10 Millionen Benutzer](#)
- [AWS re:INVENT 2023 — Nachhaltige Architektur: Vergangenheit, Gegenwart und future](#)
- [AWS re:Invent 2022 — Schaffen Sie eine kosten-, energie- und ressourceneffiziente Computerumgebung](#)
- [AWS re:Invent 2022 — Skalierung von Containern von einem Benutzer auf Millionen](#)
- [AWS re:Invent 2023 — Skalierung der FM-Inferenz auf Hunderte von Modellen mit Amazon SageMaker](#)
- [AWS re:Invent 2023 — Nutzen Sie die Leistungsfähigkeit von Karpenter, um Kubernetes zu skalieren, zu optimieren und zu aktualisieren](#)

### Zugehörige Beispiele:

- [Auto Scaling](#)

## SUS02-BP02 An den Nachhaltigkeitszielen SLAs ausrichten

Überprüfen und optimieren Sie die Service-Level-Vereinbarungen (SLA) für die Arbeitslast auf der Grundlage Ihrer Nachhaltigkeitsziele, um den Ressourcenaufwand für Ihre Arbeitslast zu minimieren und gleichzeitig die Geschäftsanforderungen zu erfüllen.

Typische Anti-Muster:

- SLAs Die Arbeitslast ist unbekannt oder mehrdeutig.
- Sie definieren Ihren SLA nur aus Gründen der Verfügbarkeit und Leistung.
- Sie verwenden für alle Ihre Workloads die gleichen Designmuster (wie etwa Multi-AZ-Architektur).

Vorteile der Einführung dieser bewährten Methode: Die Ausrichtung an SLAs Nachhaltigkeitszielen führt zu einer optimalen Ressourcennutzung bei gleichzeitiger Erfüllung der Geschäftsanforderungen.

Risikostufe bei fehlender Befolgung dieser bewährten Methode: Niedrig

Implementierungsleitfaden

SLAs definieren Sie das Serviceniveau, das von einem Cloud-Workload erwartet wird, z. B. Reaktionszeit, Verfügbarkeit und Datenspeicherung. Sie beeinflussen die Architektur, die Ressourcennutzung und die Umweltauswirkungen einer Cloud-Workload. Prüfen Sie in regelmäßigen Abständen SLAs und gehen Sie Kompromisse ein, die den Ressourcenverbrauch deutlich reduzieren und im Gegenzug akzeptable Verringerungen der Serviceniveaus ermöglichen.

Implementierungsschritte

- Nachhaltigkeitsziele verstehen: Identifizieren Sie Nachhaltigkeitsziele in Ihrer Organisation – etwa eine Reduzierung des CO<sub>2</sub>-Ausstoßes oder eine bessere Ressourcennutzung.
- Überprüfung SLAs: Evaluieren Sie Ihre Produkte SLAs, um zu beurteilen, ob sie Ihren Geschäftsanforderungen entsprechen. Wenn Sie diese Werte überschreiten SLAs, führen Sie eine weitere Überprüfung durch.
- Kompromisse verstehen: Machen Sie sich ein Bild von den Kompromissen zwischen der Komplexität (zum Beispiel hohe Anzahl gleichzeitiger Benutzer), der Leistung (zum Beispiel Latenz) und den Auswirkungen auf die Nachhaltigkeit Ihrer Workloads (zum Beispiel Ressourcenbedarf). In der Regel geht die Priorisierung von zwei der Faktoren auf Kosten des dritten.
- Anpassung SLAs: Passen Sie Ihre Situation an, SLAs indem Sie Kompromisse eingehen, die die Auswirkungen auf die Nachhaltigkeit deutlich reduzieren, und im Gegenzug akzeptable Verringerungen des Serviceniveaus vornehmen.

- **Nachhaltigkeit und Zuverlässigkeit:** Workloads mit hoher Verfügbarkeit verbrauchen in der Regel mehr Ressourcen.
- **Nachhaltigkeit und Leistung:** Die Nutzung von mehr Ressourcen, um die Leistung zu steigern, führt unter Umständen zu einer höheren Umweltbelastung.
- **Nachhaltigkeit und Sicherheit:** Übermäßig sichere Workloads haben möglicherweise eine höhere Umweltbelastung zur Folge.
- **Definieren Sie Nachhaltigkeit, SLAs wenn möglich:** Beziehen Sie Nachhaltigkeit in Ihren Workload mit SLAs ein. Definieren Sie beispielsweise ein Mindestauslastungsniveau als Nachhaltigkeit SLA für Ihre Recheninstanzen.
- **Verwenden Sie effiziente Entwurfsmuster:** Verwenden Sie Entwurfsmuster wie Microservices AWS , die geschäftskritischen Funktionen Priorität einräumen und niedrigere Service-Levels (wie Reaktionszeit- oder Wiederherstellungszeitziele) für unkritische Funktionen ermöglichen.
- **Kommunizieren Sie und legen Sie Rechenschaftspflichten fest:** Teilen Sie diese Informationen SLAs mit allen relevanten Stakeholdern, einschließlich Ihrem Entwicklungsteam und Ihren Kunden. Verwenden Sie die Berichterstattung, um die zu verfolgen und zu überwachen. SLAs Weisen Sie Rechenschaftspflicht zu, um die Nachhaltigkeitsziele für Sie SLAs zu erreichen.
- **Nutzen Sie Anreize und Prämien:** Nutzen Sie Anreize und Prämien, um Nachhaltigkeitsziele zu erreichen oder zu übertreffenSLAs.
- **Überprüfen und wiederholen:** Überprüfen Sie Ihre Ziele regelmäßig und passen Sie sie anSLAs, um sicherzustellen, dass sie mit den sich entwickelnden Nachhaltigkeits- und Leistungszielen in Einklang stehen.

## Ressourcen

### Zugehörige Dokumente:

- [Grundlegendes zu Resilienzmustern und Kompromissen, um eine effiziente Architektur in der Cloud zu entwickeln](#)
- [Bedeutung von Service Level Agreements für SaaS-Anbieter](#)

### Zugehörige Videos:

- [AWS re:Invent 2023 — Kapazität, Verfügbarkeit, Kosteneffizienz: Wählen Sie drei](#)
- [AWS re:INVENT 2023 — Nachhaltige Architektur: Vergangenheit, Gegenwart und future](#)

- [AWS re:Invent 2023 — Fortschrittliche Integrationsmuster und Kompromisse für lose gekoppelte Systeme](#)
- [AWS re:Invent 2022 — Bereitstellung nachhaltiger, leistungsstarker Architekturen](#)
- [AWS re:Invent 2022 — Schaffen Sie eine kosten-, energie- und ressourceneffiziente Computerumgebung](#)

SUS02-BP03 Stoppen Sie die Erstellung und Wartung ungenutzter Ressourcen

Nehmen Sie nicht verwendete Ressourcen in Ihrer Workload außer Betrieb, um die Anzahl der Cloud-Ressourcen zu verringern, die zur Unterstützung Ihres Bedarfs und zur Minimierung von Verschwendung erforderlich sind.

Typische Anti-Muster:

- Sie analysieren Ihre Anwendung nicht auf Ressourcen, die redundant sind oder nicht mehr benötigt werden.
- Sie entfernen keine redundanten oder nicht mehr benötigten Ressourcen.

Vorteile der Nutzung dieser bewährten Methode: Das Entfernen nicht genutzter Ressourcen setzt Kapazitäten frei und verbessert die allgemeine Effizienz der Workload.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Niedrig

Implementierungsleitfaden

Nicht verwendete Ressourcen verbrauchen Cloud-Kapazitäten wie Speicherplatz oder Rechenleistung. Wenn Sie solche Ressourcen identifizieren und eliminieren, können Sie diese Kapazitäten freisetzen, was zu einer effizienteren Cloud-Architektur führt. Analysieren Sie Anwendungsressourcen (wie vorab kompilierte Berichte, Datensätze, statische Bilder) sowie Zugriffsmuster für Komponenten, um Redundanzen, eine zu geringe Auslastung und mögliche Kandidaten für die Außerbetriebnahme zu identifizieren. Entfernen Sie diese redundanten Ressourcen, um die Ressourcenverschwendung in Ihrer Workload zu reduzieren.

Implementierungsschritte

- Bestandsaufnahme durchführen: Führen Sie eine umfassende Bestandsaufnahme durch, um alle Komponenten innerhalb Ihrer Workload zu identifizieren.

- **Nutzung analysieren:** Verwenden Sie die kontinuierliche Überwachung, um statische Komponenten zu identifizieren, die nicht mehr benötigt werden.
- **Ungenutzte Komponenten entfernen:** Entwickeln Sie einen Plan, um Komponenten zu entfernen, die nicht mehr benötigt werden.
  - Prüfen Sie vor dem Entfernen einer Ressource die Auswirkungen dieser Maßnahme auf die Architektur.
  - Konsolidieren Sie sich überschneidende generierte Komponenten, um eine redundante Verarbeitung zu entfernen.
  - Aktualisieren Sie Ihre Anwendungen, damit diese nicht mehr benötigte Ressourcen nicht weiter produzieren und speichern.
- **Mit Dritten kommunizieren:** Weisen Sie Dritte an, die Erstellung und Speicherung von Komponenten einzustellen, die in Ihrem Auftrag verwaltet und nicht mehr benötigt werden. Bitten Sie darum, dass redundante Komponenten konsolidiert werden.
- **Lebenszyklusrichtlinien verwenden:** Verwenden Sie Lebenszyklusrichtlinien, damit ungenutzte Komponenten automatisch gelöscht werden.
  - Mit [Amazon-S3-Lebenszyklen](#) können Sie Ihre Objekte während ihres gesamten Lebenszyklus verwalten.
  - Sie können [Amazon Data Lifecycle Manager](#) verwenden, um die Erstellung, Aufbewahrung und Löschung von EBS Amazon-Snapshots und Amazon EBS zu automatisieren. AMIs
- **Überprüfen und optimieren:** Überprüfen Sie regelmäßig Ihre Workload, um ungenutzte Komponenten zu identifizieren und zu entfernen.

## Ressourcen

### Zugehörige Dokumente:

- [Optimieren Sie Ihre AWS Infrastruktur im Hinblick auf Nachhaltigkeit, Teil II: Speicher](#)
- [Wie kündige ich aktive Ressourcen, die ich auf meinem nicht mehr benötigte AWS-Konto?](#)

### Zugehörige Videos:

- [AWS re:INVENT 2023 — Nachhaltige Architektur: Vergangenheit, Gegenwart und future](#)
- [AWS re:Invent 2022 — Erhaltung und Maximierung des Werts digitaler Medienressourcen mithilfe von Amazon S3](#)
- [AWS re:Invent 2023 — Optimieren Sie die Kosten in Ihren Umgebungen mit mehreren Konten](#)



## SUS02-BP04 Optimieren Sie die geografische Verteilung von Workloads auf der Grundlage ihrer Netzwerkanforderungen

Wählen Sie Cloud-Standorte und -Services für Ihre Workload, die die Entfernungen reduzieren, über die Netzwerkdatenverkehr übertragen werden muss, um die Zahl der Netzwerkressourcen zu verringern, die zur Unterstützung Ihrer Workload erforderlich sind.

Typische Anti-Muster:

- Sie wählen die Region der Workload auf der Grundlage Ihres eigenen Standorts aus.
- Sie konsolidieren alle Workload-Ressourcen an einem geografischen Standort.
- Der gesamte Datenverkehr fließt durch Ihre bestehenden Rechenzentren.

Vorteile der Nutzung dieser bewährten Methode: Die Platzierung von Workloads in der Nähe der Benutzer bietet die geringstmögliche Latenz und verringert gleichzeitig die Bewegung der Daten durch das Netzwerk und damit die Umweltauswirkungen.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel

Implementierungsleitfaden

Die AWS Cloud Infrastruktur basiert auf Standortoptionen wie Regionen, Availability Zones, Platzierungsgruppen und Edge-Standorten wie [AWS Outposts](#) [AWS Local Zones](#). Diese Standortoptionen stellen die Konnektivität zwischen Anwendungskomponenten, Cloud-Services, Edge-Netzwerken und On-Premises-Rechenzentren sicher.

Analysieren Sie die Netzwerkzugriffsmuster in Ihrer Workload, um festzustellen, wie diese verwendet werden können, um die Entfernungen für den Netzwerkdatenverkehr zu reduzieren.

Implementierungsschritte

- Analysieren Sie die Netzwerkzugriffsmuster in Ihrer Workload, um zu ermitteln, wie die Benutzer Ihre Anwendung verwenden.
  - Verwenden Sie Überwachungstools wie [Amazon CloudWatch](#) und [AWS CloudTrail](#), um Daten zu Netzwerkaktivitäten zu sammeln.
  - Analysen Sie die Daten, um das Netzwerkzugriffsmuster zu identifizieren.
- Wählen Sie die Regionen für Ihre Workload-Bereitstellung auf der Grundlage der folgenden zentralen Elemente aus:

- Ihr Nachhaltigkeitsziel: wie unter [Regionsauswahl](#) erklärt.
- Standort Ihrer Daten: Für datenintensive Anwendungen (wie etwa Big Data oder Machine Learning) sollte der Anwendungscode so nahe wie möglich zu den Daten ausgeführt werden.
- Standort Ihrer Benutzer: Wählen Sie für benutzerseitige Anwendungen eine Region (oder Regionen) in der Nähe der Benutzer der Workload.
- Weitere Einschränkungen: Berücksichtigen Sie Einschränkungen wie Kosten und Compliance, wie unter [Relevante Aspekte bei der Wahl einer Region für Ihre Workloads](#) erläutert.
- Verwenden Sie lokale Zwischenspeicherung oder [AWS -Zwischenspeicherung](#) für häufig genutzte Ressourcen zur Verbesserung der Leistung, zur Verringerung von Datenverschiebungen und zur Reduzierung der Umweltauswirkungen.

Service	Wann sollte dies verwendet werden?
<a href="#">Amazon CloudFront</a>	Wird verwendet, um statische Inhalte wie Bilder, Skripte und Videos sowie dynamische Inhalte wie API Antworten oder Webanwendungen zwischenzuspeichern.
<a href="#">Amazon ElastiCache</a>	Verwenden Sie dies für die Zwischenspeicherung von Inhalten für Webanwendungen.
<a href="#">DynamoDB Accelerator</a>	Verwenden Sie dies für die Add-in-Speicher-Beschleunigung für Ihre DynamoDB-Tabellen.

- Nutzen Sie Services, die Ihnen dabei helfen können, Code näher an den Benutzern Ihrer Workload auszuführen:

Service	Wann sollte dies verwendet werden?
<a href="#">Lambda@Edge</a>	Verwenden Sie dies für rechenintensive Anwendungen, die initiiert werden, wenn sich Objekte nicht im Zwischenspeicher befinden.
<a href="#">CloudFront Amazon-Funktionen</a>	Wird für einfache Anwendungsfälle wie HTTP Bearbeitungen von Anfragen oder Antworten

Service	Wann sollte dies verwendet werden?
	verwendet, die durch kurzlebige Funktionen ausgelöst werden können.
<a href="#">AWS IoT Greengrass</a>	Verwenden Sie dies für die Ausführung lokaler Rechenoperationen, Messaging sowie die Datenzwischenspeicherung für verbundene Geräte.

- Nutzen Sie Verbindungspooling, um die erneute Nutzung von Verbindungen zu ermöglichen und die Zahl der erforderlichen Ressourcen zu reduzieren.
- Verwenden Sie verteilte Datenspeicher, die nicht auf persistente Verbindungen und synchrone Updates angewiesen sind, um regionale Benutzergruppen zu unterstützen.
- Ersetzen Sie vorab bereitgestellte statische Netzwerkkapazität durch geteilte dynamische Kapazitäten und teilen Sie die Auswirkungen von Netzwerkkapazitäten auf die Nachhaltigkeit mit anderen Abonnenten.

## Ressourcen

### Zugehörige Dokumente:

- [Optimierung Ihrer AWS Infrastruktur im Hinblick auf Nachhaltigkeit, Teil: Netzwerke III](#)
- [ElastiCache Amazon-Dokumentation](#)
- [Was ist Amazon CloudFront?](#)
- [Die CloudFront wichtigsten Funktionen von Amazon](#)
- [AWS Globale Infrastruktur](#)
- [AWS Local Zones und AWS Outposts Auswahl der richtigen Technologie für Ihren Edge-Workload](#)
- [Platzierungsgruppen](#)
- [AWS Local Zones](#)
- [AWS Outposts](#)

### Zugehörige Videos:

- [Entmystifizierung der Datenübertragung am AWS](#)
- [Skalierung der Netzwerkleistung auf EC2 Amazon-Instances der nächsten Generation](#)

- [AWS Erklärvideo zu Local Zones](#)
- [AWS Outposts: Overview and How it Works](#)
- [AWS re:Invent 2023 — Eine Migrationsstrategie für Edge-Workloads und lokale Workloads](#)
- [AWS re:Invent 2021 — AWS Outposts: Das Erlebnis vor Ort umsetzen AWS](#)
- [AWS re:Invent 2020 — AWS Wavelength: Führen Sie Apps mit extrem niedriger Latenz am 5G-Edge aus](#)
- [AWS re:Invent 2022 — AWS Local Zones: Entwicklung von Anwendungen für eine verteilte Kante](#)
- [AWS re:Invent 2021 — Websites mit niedriger Latenz mit Amazon erstellen CloudFront](#)
- [AWS re:Invent 2022 — Verbessern Sie Leistung und Verfügbarkeit mit AWS Global Accelerator](#)
- [AWS re:Invent 2022 — Bauen Sie Ihr globales Wide Area Network auf mit AWS](#)
- [AWS re:Invent 2020: Globales Verkehrsmanagement mit Amazon Route 53](#)

Zugehörige Beispiele:

- [AWS Netzwerk-Workshops](#)
- [Architecting for sustainability - Minimize data movement across networks](#)

SUS02-BP05 Optimieren Sie die Ressourcen der Teammitglieder für die durchgeführten Aktivitäten

Optimieren Sie die Ressourcen, die Teammitgliedern zur Verfügung gestellt werden, um negative Auswirkungen auf die Nachhaltigkeit zu minimieren und gleichzeitig ihre Anforderungen zu erfüllen.

Typische Anti-Muster:

- Sie berücksichtigen nicht die Auswirkungen der von Ihren Teammitgliedern verwendeten Geräte auf die Gesamteffizienz Ihrer Cloud-Anwendung.
- Sie verwalten und aktualisieren die von Teammitgliedern verwendeten Ressourcen manuell.

Vorteile der Nutzung dieser bewährten Methode: Die Optimierung der Teammitglieder-Ressourcen verbessert die allgemeine Effizienz Cloud-fähiger Anwendungen.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Niedrig

## Implementierungsleitfaden

Verstehen Sie die Ressourcen, mit denen Ihre Teammitglieder Ihre Services nutzen, deren erwartete Lebensdauer sowie die finanziellen und nachhaltigkeitsbezogenen Auswirkungen. Implementieren Sie Strategien zur Optimierung dieser Ressourcen. Beispielsweise können Sie komplexe Vorgänge wie Rendering und Kompilierung auf intensiv genutzter und skalierbarer Infrastruktur anstatt auf weniger ausgelasteten Einzelbenutzersystemen mit hohem Energieverbrauch ausführen.

### Implementierungsschritte

- **Energieeffiziente Workstations verwenden:** Stellen Sie den Teammitgliedern energieeffiziente Workstations und Peripheriegeräte zur Verfügung. Verwenden Sie effiziente Energiemanagementfeatures (wie den Energiesparmodus) auf diesen Geräten, um ihren Energieverbrauch zu reduzieren.
- **Virtualisierung verwenden:** Verwenden Sie virtuelle Desktops und Anwendungs-Streaming, um Upgrade- und Geräteanforderungen zu begrenzen.
- **Remote-Zusammenarbeit fördern:** Ermutigen Sie die Teammitglieder, Tools für die Remote-Zusammenarbeit wie [Amazon Chime](#) oder [AWS Wickr](#) zu verwenden, um den Reisebedarf und die damit verbundenen CO<sub>2</sub>-Emissionen zu reduzieren.
- **Energieeffiziente Software verwenden:** Stellen Sie den Teammitgliedern energieeffiziente Software zur Verfügung, indem Sie nicht benötigte Features und Prozesse entfernen oder deaktivieren.
- **Lebenszyklen verwalten:** Evaluieren Sie die Auswirkungen von Prozessen und Systemen auf die Lebenszyklen von Geräten. Wählen Sie Lösungen aus, die den Bedarf für Geräteauswchvorgänge minimieren und gleichzeitig die geschäftlichen Anforderungen erfüllen. Pflegen und aktualisieren Sie regelmäßig Workstations oder Software, um die Effizienz aufrechtzuerhalten und zu verbessern.
- **Remote-Verwaltung für Geräte:** Implementieren Sie die Remote-Verwaltung für Geräte, um die Anzahl der erforderlichen Geschäftsreisen zu reduzieren.
  - [AWS Systems Manager Fleet Manager](#) ist eine einheitliche Benutzeroberfläche (UI), mit der Sie Ihre Knoten, die vor Ort AWS oder vor Ort laufen, aus der Ferne verwalten können.

### Ressourcen

Zugehörige Dokumente:

- [Was ist Amazon WorkSpaces?](#)
- [Cost Optimizer für Amazon WorkSpaces](#)

- [Amazon AppStream 2.0-Dokumentation](#)
- [NICE DCV](#)

Zugehörige Videos:

- [Verwaltung der Kosten für Amazon WorkSpaces am AWS](#)

SUS02-BP06 Implementieren Sie Pufferung oder Drosselung, um die Nachfragekurve abzuflachen

Pufferung und Drosselung verflachen die Bedarfskurve und reduzieren die erforderliche bereitgestellte Kapazität für Ihre Workload.

Typische Anti-Muster:

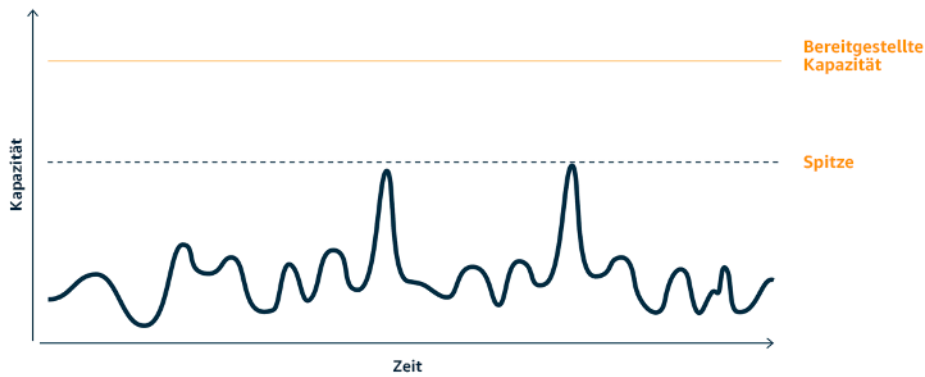
- Sie verarbeiten die Client-Anfragen sofort, obwohl dies nicht erforderlich ist.
- Sie analysieren die Anforderungen für Client-Anfragen nicht.

Vorteile der Nutzung dieser bewährten Methode: Das Verflachen der Bedarfskurve reduziert die erforderliche bereitgestellte Kapazität für die Workload. Die Reduzierung der bereitgestellten Kapazität bedeutet geringeren Energieverbrauch und geringere Umweltauswirkungen.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Niedrig

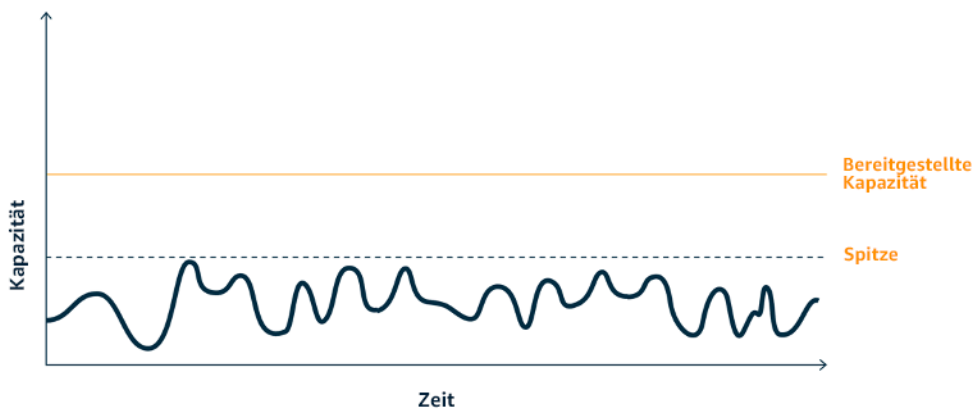
Implementierungsleitfaden

Die Verflachung der Bedarfskurve kann Ihnen dabei helfen, die bereitgestellte Kapazität für eine Workload zu verringern und dessen Umweltauswirkungen zu reduzieren. Nehmen wir eine Workload mit der nachfolgend gezeigten Bedarfskurve. Diese Workload hat zwei Spitzen und um damit umzugehen, wird die Ressourcenkapazität bereitgestellt, die hier durch die orangefarbene Linie angezeigt wird. Die für diese Workload aufgewendeten Ressourcen und die eingesetzte Energie werden nicht durch die Fläche unter der Bedarfskurve, sondern von der Linie für die bereitgestellte Kapazität angezeigt, da für den Umgang mit den beiden Spitzen bereitgestellte Kapazität erforderlich ist.



Bedarfskurve mit zwei deutlichen Spitzen, die hohe bereitgestellte Kapazität erfordern

Sie können Pufferung oder Drosselung verwenden, um die Bedarfskurve zu beeinflussen und die Spitzen abzumildern, was weniger bereitgestellte Kapazität und einen geringeren Energieverbrauch bedeutet. Implementieren Sie Drosselung, wenn Ihre Clients wiederholte Versuche durchführen können. Implementieren Sie die Pufferung, um die Anforderung zu speichern und die Verarbeitung auf einen späteren Zeitpunkt zu verschieben.



Auswirkung der Drosselung auf die Nachfragekurve und die bereitgestellte Kapazität

### Implementierungsschritte

- Analysieren Sie die Client-Anfragen, um festzulegen, wie darauf zu reagieren ist. Wichtige Faktoren dabei sind:
  - Kann diese Anfrage in asynchroner Weise verarbeitet werden?
  - Kann der Client die Anfrage erneut versuchen?

- Wenn dies der Fall ist, können Sie Drosselung verwenden, die der Quelle mitteilt, dass wenn sie die Anfrage zum aktuellen Zeitpunkt nicht bedienen kann, es später erneut versucht werden sollte.
  - Sie können [Amazon API Gateway](#) verwenden, um Drosselung zu implementieren.
- Für Clients, die Anfragen nicht erneut versuchen können, muss zur Verflachung der Bedarfskurve ein Puffer implementiert werden. Ein Puffer verschiebt die Anforderungsverarbeitung, so dass Anwendungen, die mit unterschiedlichen Raten ausgeführt werden, effektiv kommunizieren können. Bei der Pufferung werden Nachrichten von Produzenten in eine Warteschlange oder einen Stream gestellt. Nachrichten können dadurch von Verbrauchern in der für ihre Geschäftsanforderungen passenden Geschwindigkeit gelesen und verarbeitet werden.
  - [Amazon Simple Queue Service \(AmazonSQS\)](#) ist ein verwalteter Service, der Warteschlangen bereitstellt, die es einem einzelnen Verbraucher ermöglichen, einzelne Nachrichten zu lesen.
  - [Amazon Kinesis](#) stellt einen Stream bereit, mit dem viele Verbraucher dieselben Nachrichten lesen können.
- Analysieren Sie den Gesamtbedarf, die Änderungsrate und die erforderliche Reaktionszeit, um die korrekte Größe der erforderlichen Drosselung oder des Puffers zu bestimmen.

## Ressourcen

### Zugehörige Dokumente:

- [Erste Schritte mit Amazon SQS](#)
- [Application integration Using Queues and Messages](#)
- [Verwaltung und Überwachung der API Drosselung Ihrer Workloads](#)
- [Drosselung einer mehrstufigen Lösung mit mehreren Mandanten im großen Maßstab mithilfe von Gateway REST API API](#)
- [Application integration Using Queues and Messages](#)

### Zugehörige Videos:

- [AWS re:Invent 2022 — Anwendungsintegrationsmuster für Microservices](#)
- [AWS re:Invent 2023 — Intelligentes Sparen: Strategien zur Kostenoptimierung von Amazon EC2](#)
- [AWS re:Invent 2023 — Fortschrittliche Integrationsmuster und Kompromisse für lose gekoppelte Systeme](#)



## Software und Architektur

### Frage

- [SUS3 Wie nutzen Sie Software- und Architekturmuster, um Ihre Nachhaltigkeitsziele zu unterstützen?](#)

SUS3 Wie nutzen Sie Software- und Architekturmuster, um Ihre Nachhaltigkeitsziele zu unterstützen?

Implementieren Sie Muster für den Lastausgleich und die Wahrung einer konsistent hohen Nutzung der bereitgestellten Ressourcen, um die Zahl der genutzten Ressourcen zu minimieren. Komponenten werden möglicherweise aufgrund von Änderungen des Benutzerverhaltens über die Zeit nicht mehr genutzt. Prüfen Sie Muster und Architekturen, um nicht ausreichend genutzte Komponenten zu konsolidieren und so die Nutzung insgesamt zu erhöhen. Nehmen Sie Komponenten außer Betrieb, die nicht mehr benötigt werden. Identifizieren Sie die Leistung Ihrer Workload-Komponenten und optimieren Sie die Komponenten, die die meisten Ressourcen verbrauchen. Achten Sie auf die Geräte, mit denen Ihre Kunden auf Ihre Services zugreifen, und implementieren Sie Muster, um den Bedarf für Geräte-Upgrades zu minimieren.

### Bewährte Methoden

- [SUS03-BP01 Optimieren Sie Software und Architektur für asynchrone und geplante Jobs](#)
- [SUS03-BP02 Workload-Komponenten mit geringer oder keiner Nutzung entfernen oder umgestalten](#)
- [SUS03-BP03 Optimieren Sie Codebereiche, die am meisten Zeit oder Ressourcen verbrauchen](#)
- [SUS03-BP04 Optimieren Sie die Auswirkungen auf Geräte und Anlagen](#)
- [SUS03-BP05 Verwenden Sie Softwaremuster und Architekturen, die Datenzugriffs- und Speichermuster am besten unterstützen](#)

SUS03-BP01 Optimieren Sie Software und Architektur für asynchrone und geplante Jobs

Verwenden Sie effiziente Software- und Architekturmuster wie warteschlangenbasierte Systeme, um eine durchgängig hohe Auslastung von bereitgestellten Ressourcen zu erzielen.

Typische Anti-Muster:

- Sie stellen zu viele Ressourcen in der Cloud-Workload bereit, um auf unerwartete Nachfragesteigerungen reagieren zu können.
- In Ihrer Architektur werden Absender und Empfänger von asynchronen Nachrichten nicht durch eine Messaging-Komponente entkoppelt.

Vorteile der Nutzung dieser bewährten Methode:

- Durch effiziente Software- und Architekturmuster werden ungenutzte Ressourcen in Ihrer Workload minimiert und die allgemeine Effizienz gesteigert.
- Sie können die Verarbeitung unabhängig vom Empfang asynchroner Nachrichten skalieren.
- Durch eine Messaging-Komponente gelten weniger strenge Verfügbarkeitsanforderungen, die mit weniger Ressourcen erfüllt werden können.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel

### Implementierungsleitfaden

Verwenden Sie effiziente Architekturmuster wie eine [ereignisgesteuerte Architektur](#), die zu einer gleichmäßigen Nutzung der Komponenten führen und die Überbereitstellung in Ihrer Workload minimieren. Durch die Verwendung effizienter Architekturmuster werden ungenutzte Ressourcen, die aufgrund von Änderungen der Nachfrage im Laufe der Zeit nicht genutzt werden, minimiert.

Analysieren Sie die Anforderungen Ihrer Workload-Komponenten und führen Sie Architekturmuster ein, mit denen die allgemeine Auslastung der Ressourcen gesteigert wird. Nehmen Sie Komponenten außer Betrieb, die nicht mehr benötigt werden.

### Implementierungsschritte

- Analysieren Sie die Nachfrage für Ihre Workload, um zu bestimmen, wie diese erfüllt werden kann.
- Verwenden Sie für Anfragen oder Aufträge, für die keine synchronen Antworten erforderlich sind, warteschlangenbasierte Architekturen und Worker mit Auto Scaling, durch die die Auslastung maximiert wird. Hier finden Sie einige Beispiele für Situationen, in denen Sie eine warteschlangenbasierte Architektur in Erwägung ziehen sollten:

Warteschlangenmechanismus	Beschreibung
<a href="#">AWS Batch Job-Warteschlangen</a>	AWS Batch Jobs werden in eine Auftragswarteschlange gestellt, wo sie gespeichert werden, bis ihre Ausführung in einer Rechenumgebung geplant werden kann.
<a href="#">Amazon Simple Queue Service und Amazon EC2 Spot-Instances</a>	Kombinieren von Amazon SQS - und Spot-Instances zum Aufbau einer fehlertoleranten und effizienten Architektur.

- Verwenden Sie für Anfragen oder Aufträge, die jederzeit verarbeitet werden können, Planungsmechanismen zur Auftragsverarbeitung in Batches, um die Effizienz zu steigern. Hier sind einige Beispiele für Planungsmechanismen in folgenden Bereichen: AWS

Zeitplanungsmechanismus	Beschreibung
<a href="#">Amazon EventBridge Scheduler</a>	Eine Funktion von <a href="#">Amazon EventBridge</a> , mit der Sie geplante Aufgaben in großem Umfang erstellen, ausführen und verwalten können.
<a href="#">AWS Glue zeitbasierter Zeitplan</a>	Definieren Sie einen zeitbasierten Zeitplan für Ihre Crawler und Jobs in. AWS Glue
<a href="#">Geplante Aufgaben von Amazon Elastic Container Service (AmazonECS)</a>	Amazon ECS unterstützt die Erstellung von geplanten Aufgaben. Geplante Aufgaben verwenden EventBridge Amazon-Regeln, um Aufgaben entweder nach einem Zeitplan oder als Reaktion auf ein EventBridge Ereignis auszuführen.
<a href="#">Instance Scheduler</a>	Konfigurieren Sie Start- und Stoppzeitpläne für Ihre Amazon EC2 - und Amazon Relational Database Service Service-Instances.

- Wenn Sie Abfrage- und Webhook-Mechanismen in Ihrer Architektur verwenden, ersetzen Sie diese durch Ereignisse. Erstellen Sie mit [ereignisgesteuerten Architekturen](#) hocheffiziente Workloads.

- Nutzen Sie [Serverless in AWS](#), um eine übermäßige Bereitstellung in einer Infrastruktur zu eliminieren.
- Wählen Sie die richtige Größe für Ihre Architektur, um zu vermeiden, dass ungenutzte Ressourcen auf Eingaben warten.
  - Sie können die [Empfehlungen zur Dimensionierung in AWS Cost Explorer](#) oder [AWS Compute Optimizer](#) zur Identifizierung von Dimensionierungsmöglichkeiten verwenden.
  - Weitere Informationen finden Sie unter [Größenanpassung: Bereitstellung von an Workloads angepassten Instances](#).

## Ressourcen

### Zugehörige Dokumente:

- [What is Amazon Simple Queue Service?](#)
- [What is Amazon MQ?](#)
- [Skalierung auf Basis von Amazon SQS](#)
- [Was ist AWS Step Functions?](#)
- [Was ist AWS Lambda?](#)
- [Verwendung AWS Lambda mit Amazon SQS](#)
- [Was ist Amazon EventBridge?](#)
- [Verwaltung asynchroner Workflows mit einem REST API](#)

### Zugehörige Videos:

- [AWS re:Invent 2023 — Auf dem Weg zur serverlosen, ereignisgesteuerten Architektur](#)
- [AWS re:Invent 2023 — Einsatz von Serverless für ereignisgesteuerte Architektur und domänengesteuertes Design](#)
- [AWS re:Invent 2023 — Fortgeschrittene ereignisgesteuerte Muster mit Amazon EventBridge](#)
- [AWS re:INVENT 2023 — Nachhaltige Architektur: Vergangenheit, Gegenwart und future](#)
- [Asynchrone Nachrichtenmuster | Ereignisse AWS](#)

### Zugehörige Beispiele:

- [Ereignisgesteuerte Architektur mit AWS Graviton-Prozessoren und Amazon Spot-Instances EC2](#)

## SUS03-BP02 Workload-Komponenten mit geringer oder keiner Nutzung entfernen oder umgestalten

Entfernen Sie ungenutzte Komponenten, die nicht mehr benötigt werden, und führen Sie einen Faktorwechsel für Komponenten mit geringer Nutzung durch, um die Verschwendung von Ressourcen in Ihrer Workload zu begrenzen.

Typische Anti-Muster:

- Sie prüfen den Nutzungsgrad der einzelnen Komponenten Ihrer Workload nicht regelmäßig.
- Sie überprüfen und analysieren keine Empfehlungen von AWS Rightsizing-Tools wie [AWS Compute Optimizer](#)

Vorteile der Nutzung dieser bewährten Methode: Das Entfernen nicht genutzter Komponenten minimiert Ausschuss und verbessert die allgemeine Effizienz Ihrer Workload.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel

Implementierungsleitfaden

Prüfen Sie Ihre Workload, um nicht oder wenig genutzte Komponenten zu identifizieren. Dies ist ein sich wiederholender Verbesserungsprozess, der von Änderungen beim Bedarf oder der Einführung eines neuen Cloud-Services ausgelöst werden kann. Beispielsweise kann ein deutliches Zurückgehen der Laufzeit der [AWS Lambda](#)-Funktion darauf hindeuten, dass die Speichergröße reduziert werden muss. Außerdem können sich mit AWS der Veröffentlichung neuer Dienste und Funktionen die optimalen Dienste und die optimale Architektur für Ihren Workload ändern.

Überwachen Sie kontinuierlich die Workload-Aktivität und suchen Sie nach Möglichkeiten zur Verbesserung des Nutzungsgrads einzelner Komponenten. Wenn Sie nicht genutzte Komponenten entfernen und Dimensionierungsaktivitäten durchführen, erreichen Sie Ihre geschäftlichen Ziele mit der geringstmöglichen Menge von Cloud-Ressourcen.

Implementierungsschritte

- Führen Sie eine Bestandsaufnahme Ihrer AWS Ressourcen durch. In können Sie einschalten AWS, [AWS Ressourcen Explorer](#) um Ihre AWS Ressourcen zu erkunden und zu organisieren. Weitere Informationen finden Sie unter [AWS re:Invent 2022 — So verwalten Sie Ressourcen und Anwendungen in großem Umfang](#). AWS
- Überwachen und erfassen Sie die Nutzungsmetriken für wichtige Komponenten Ihrer Arbeitslast (wie CPU Auslastung, Speicherauslastung oder Netzwerkdurchsatz in [CloudWatch Amazon-Metriken](#)).

- Identifizieren Sie ungenutzte oder zu wenig genutzte Komponenten in Ihrer Architektur.
  - Um stabile Workloads zu gewährleisten, sollten Sie die Tools zur AWS richtigen Dimensionierung überprüfen, z. B. [AWS Compute Optimizer](#) in regelmäßigen Abständen, um ungenutzte, ungenutzte oder nicht ausgelastete Komponenten zu identifizieren.
  - Prüfen Sie für kurzzeitige Workloads die Nutzungsmetriken, um nicht oder wenig genutzte Komponenten zu identifizieren.
- Außerbetriebnahme von Komponenten und zugehörigen Ressourcen (wie ECR Amazon-Images), die nicht mehr benötigt werden.
  - [Automatisierte Bereinigung unbenutzter Bilder in Amazon ECR](#)
  - [Löschen Sie ungenutzte Amazon Elastic Block Store \(AmazonEBS\) -Volumes mit AWS Config und AWS Systems Manager](#)
- Führen Sie einen Faktorwechsel für nicht ausreichend genutzte Ressourcen durch oder konsolidieren Sie sie mit anderen Ressourcen, um die Nutzungseffizienz zu verbessern. Sie können beispielsweise mehrere kleine Datenbanken auf einer einzigen [RDS Amazon-Datenbank-Instance](#) bereitstellen, anstatt Datenbanken auf einzelnen, nicht ausgelasteten Instances laufen zu lassen.
- Machen Sie sich mit den [Ressourcen vertraut, die durch Ihre Workload bereitgestellt werden, um eine Arbeitseinheit zu erledigen](#).

## Ressourcen

### Zugehörige Dokumente:

- [AWS Trusted Advisor](#)
- [Was ist Amazon CloudWatch?](#)
- [Größenanpassung: Bereitstellung von an Workloads angepassten Instances](#)
- [Optimizing your cost with Rightsizing Recommendations](#)

### Zugehörige Videos:

- [AWS re:Invent 2023 — Kapazität, Verfügbarkeit, Kosteneffizienz: Wählen Sie drei](#)

### Zugehörige Beispiele:

- [Optimieren Sie Hardwaremuster und achten Sie auf Nachhaltigkeit KPIs](#)

## SUS03-BP03 Optimieren Sie Codebereiche, die am meisten Zeit oder Ressourcen verbrauchen

Optimieren Sie den Code, der innerhalb der verschiedenen Komponenten Ihrer Architektur ausgeführt wird, um die Ressourcennutzung zu minimieren und die Leistung zu maximieren.

Typische Anti-Muster:

- Sie versäumen die Optimierung Ihres Codes für die Ressourcennutzung.
- Sie reagieren auf Leistungsprobleme normalerweise mit Erhöhung des Ressourceneinsatzes.
- Ihr Code-Prüfungs- und -Entwicklungsprozess verfolgt keine Leistungsänderungen.

Vorteile der Nutzung dieser bewährten Methode: Die Verwendung effizienten Codes minimiert die Ressourcennutzung und verbessert die Leistung.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel

### Implementierungsleitfaden

Es ist sehr wichtig, jeden funktionalen Bereich, einschließlich des Codes einer für die Cloud erstellten Anwendung, zu untersuchen, um ihre Ressourcennutzung und Leistung zu optimieren. Überwachen Sie kontinuierlich die Leistung Ihrer Workload in Build-Umgebungen und Produktionsbereichen und suchen Sie nach Möglichkeiten, Codeausschnitte zu verbessern, die einen besonders hohen Ressourcenverbrauch haben. Führen Sie einen regelmäßigen Prüfungsprozess ein, um Fehler oder Anti-Muster in Ihrem Code zu identifizieren, die Ressourcen in ineffizienter Weise nutzen. Nutzen Sie einfache und effiziente Algorithmen, die dieselben Ergebnisse für Ihre Anwendungsfälle liefern.

### Implementierungsschritte

- Effiziente Programmiersprache verwenden: Verwenden Sie das jeweils effizienteste Betriebssystem und die optimale Programmiersprache für die Workload. Weitere Informationen zu energieeffizienten Programmiersprachen (einschließlich Rust) finden Sie unter [Sustainability with Rust](#).
- Verwenden Sie einen KI-Codierbegleiter: Erwägen Sie, einen KI-Codierbegleiter wie [Amazon CodeWhisperer](#) zu verwenden, um effizient Code zu schreiben.
- Code-Überprüfungen automatisieren: Führen Sie bei der Entwicklung Ihrer Workloads einen automatischen Code-Prüfungsprozess ein, um die Qualität zu verbessern sowie Fehler und Anti-Muster zu identifizieren.
  - [Automatisieren Sie Code-Reviews mit Amazon CodeGuru Reviewer](#)

- [Erkennung von Parallelitätsfehlern mit Amazon CodeGuru](#)
- [Erhöhung der Codequalität für Python-Anwendungen mit Amazon CodeGuru](#)
- Code-Profiler verwenden: Verwenden Sie einen Code-Profiler für Code-Prüfungen, um die Codebereiche als Optimierungsziele zu identifizieren, die die meiste Zeit oder die meisten Ressourcen verwenden.
  - [Reduzieren Sie den CO2-Fußabdruck Ihres Unternehmens mit Amazon CodeGuru Profiler](#)
  - [Grundlegendes zur Speichernutzung in Ihrer Java-Anwendung mit Amazon CodeGuru Profiler](#)
  - [Verbessern Sie das Kundenerlebnis und senken Sie die Kosten mit Amazon CodeGuru Profiler](#)
- Überwachen und optimieren: Verwenden Sie Ressourcen für die kontinuierliche Überwachung, um Komponenten mit hohem Ressourcenbedarf oder suboptimaler Konfiguration zu identifizieren.
  - Ersetzen Sie rechenintensive Algorithmen durch einfachere und effizientere Versionen, die dieselben Ergebnisse liefern.
  - Entfernen Sie unnötigen Code und überflüssige Formatierungen.
- Code-Faktorwechsel oder -Transformation verwenden: Erkunden Sie die Möglichkeiten der [Amazon-Q-Codetransformation](#) für die Wartung und Aktualisierung von Anwendungen.
  - [Sprachversionen mit Amazon-Q-Codetransformation aktualisieren](#)
  - [AWS re:Invent 2023 — Automatisieren Sie App-Upgrades und Wartung mithilfe von Amazon Q Code Transformation](#)

## Ressourcen

### Zugehörige Dokumente:

- [Was ist Amazon CodeGuru Profiler?](#)
- [FPGAInstanzen](#)
- [Die einzigen Tools, AWS SDKs auf denen Sie aufbauen können AWS](#)

### Zugehörige Videos:

- [Verbessern Sie die Code-Effizienz mit Amazon CodeGuru Profiler](#)
- [AWS re:Invent 2023 — Bewährte Methoden für Amazon CodeWhisperer](#)
- [Automatisieren Sie Codeprüfungen und Empfehlungen zur Anwendungsleistung mit Amazon CodeGuru](#)



## Zugehörige Beispiele:

- [Code mit Amazon optimieren CodeGuru](#)

## SUS03-BP04 Optimieren Sie die Auswirkungen auf Geräte und Anlagen

Verstehen Sie die in Ihrer Architektur verwendeten Geräte und nutzen Sie Strategien, um ihre Nutzung zu reduzieren. Dies kann die Umweltauswirkungen Ihrer Cloud-Workload insgesamt verringern.

### Typische Anti-Muster:

- Sie ignorieren die Umweltauswirkungen der Geräte, die Ihre Kunden verwenden.
- Sie verwalten und aktualisieren die von Kunden verwendeten Ressourcen manuell.

Vorteile der Nutzung dieser bewährten Methode: Die Implementierung von Softwaremustern und Features, die für Kundengeräte optimiert sind, können die Umweltauswirkungen von Cloud-Workloads insgesamt verringern.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel

### Implementierungsleitfaden

Die Implementierung für Kundengeräte optimierter Softwaremuster und Features können die Umweltauswirkungen auf unterschiedliche Weise reduzieren:

- Die Implementierung neuer abwärtskompatibler Features kann die Anzahl der Hardwareaustauschvorgänge verringern.
- Die Optimierung einer Anwendung, so dass sie effizient auf Geräten ausgeführt werden kann, kann bei der Reduzierung des Energieverbrauchs helfen und die Batterielaufzeit verlängern (falls Batterien zum Einsatz kommen).
- Die Optimierung einer Anwendung für Geräte kann auch Datenübertragungen über das Netzwerk verringern.

Verstehen Sie die in Ihrer Architektur verwendeten Geräte, ihre erwartete Lebensdauer und die Auswirkungen des Austauschs dieser Komponenten. Implementieren Sie Softwaremuster und Features, die dabei helfen, den Energieverbrauch von Geräten zu senken, und den Austausch von Geräten sowie manuelle Upgrades durch Kunden seltener erforderlich machen.

## Implementierungsschritte

- Bestandsaufnahme durchführen: Inventarisieren Sie die in ihrer Architektur verwendeten Geräte. Bei den Geräten kann es sich um IOT Mobilgeräte, Tablets, Geräte, intelligentes Licht oder sogar intelligente Geräte in einer Fabrik handeln.
- Energieeffiziente Geräte verwenden: Erwägen Sie den Einsatz energieeffizienter Geräte in Ihrer Architektur. Verwenden Sie Energieverwaltungsconfigurationen auf Geräten, um in den Energiesparmodus zu wechseln, wenn sie nicht verwendet werden.
- Effiziente Anwendungen ausführen: Optimieren Sie die Anwendung, die auf den Geräten ausgeführt wird:
  - Verwenden Sie Strategien wie die Ausführung von Aufgaben im Hintergrund, um den Energieverbrauch zu verringern.
  - Berücksichtigen Sie beim Erstellen von Nutzlasten Netzwerkbandbreite und Latenz und implementieren Sie Funktionen, mit denen Ihre Anwendungen auch über Verbindungen mit geringer Bandbreite und hoher Latenz gut funktionieren.
  - Wandeln Sie Nutzlasten und Dateien in von den Geräten benötigte optimierte Formate um. Sie können beispielsweise [Amazon Elastic Transcoder](#) oder [AWS Elemental MediaConvert](#) verwenden, um große, qualitativ hochwertige Digitalmediendateien in Formate umzuwandeln, die Benutzer auf Mobilgeräten abspielen können.
  - Führen Sie rechenintensive Aktivitäten (z. B. das Rendern von Bildern) serverseitig aus oder nutzen Sie Anwendungs-Streaming, um den Benutzerkomfort auf älteren Geräten zu verbessern.
  - Segmentieren und paginieren Sie Ausgaben, besonders für interaktive Sitzungen, um Nutzlasten zu verwalten und lokale Speicheranforderungen zu begrenzen.
- Anbieter einbeziehen: Arbeiten Sie mit Geräteanbietern zusammen, die nachhaltige Materialien verwenden und für Transparenz in ihren Lieferketten und Umweltzertifizierungen sorgen.
- Updates over-the-air (OTA) verwenden: Verwenden Sie den automatisierten Mechanismus over-the-air (OTA), um Updates für ein oder mehrere Geräte bereitzustellen.
  - Mit einer [CI/CD-Pipeline](#) können Sie mobile Anwendungen aktualisieren.
  - Mit [AWS IoT Device Management](#) können Sie verbundene Geräte in großem Umfang aus der Ferne verwalten.
- Verwaltung von Gerätefarmen verwenden: Verwenden Sie zum Testen neuer Features und Updates verwaltete Gerätefarmen mit repräsentativen Sätzen von Hardwaregeräten, um den Umfang der unterstützten Geräte zu maximieren. Weitere Details finden Sie unter [SUS06-BP04 Verwaltete Gerätefarmen zum Testen verwenden](#).

- Kontinuierliche Überwachung und Verbesserung: Verfolgen Sie den Energieverbrauch von Geräten, um Verbesserungsmöglichkeiten zu identifizieren. Verwenden Sie neue Technologien oder bewährte Methoden, um die Umweltauswirkungen dieser Geräte zu verbessern.

## Ressourcen

### Zugehörige Dokumente:

- [Was ist AWS Device Farm?](#)
- [AppStream 2.0 Dokumentation](#)
- [NICE DCV](#)
- [OTATutorial zum Aktualisieren der Firmware auf Geräten, auf denen Free ausgeführt wird RTOS](#)
- [Optimizing Your IoT Devices for Environmental Sustainability](#)

### Zugehörige Videos:

- [AWS re:Invent 2023 — Verbessern Sie die Qualität Ihrer Mobil- und Web-Apps mit AWS Device Farm](#)

SUS03-BP05 Verwenden Sie Softwaremuster und Architekturen, die Datenzugriffs- und Speichermuster am besten unterstützen

Identifizieren Sie, wie Daten in Ihrer Workload verwendet, von Benutzern genutzt, übertragen und gespeichert werden. Verwenden Sie Softwaremuster und Architekturen, die den Datenzugriff und die Speicherung optimal unterstützen, um die zur Unterstützung der Workload erforderlichen Datenverarbeitungs-, Netzwerk- und Speicherressourcen zu reduzieren.

### Typische Anti-Muster:

- Sie gehen davon aus, dass für alle Workloads ähnliche Datenspeicher- und Zugriffsmuster gelten.
- Sie verwenden nur eine Speicherebene, vorausgesetzt, dass alle Workloads in diese Ebene passen.
- Sie gehen davon aus, dass Datenzugriffsmuster im Laufe der Zeit konsistent bleiben.
- Ihre Architektur unterstützt potenzielle hohe Bursts beim Datenzugriff, was dazu führt, dass die Ressourcen die meiste Zeit ungenutzt bleiben.

Vorteile der Nutzung dieser bewährten Methode: Die Auswahl und Optimierung Ihrer Architektur auf der Grundlage von Datenzugriffs- und Speichermustern hilft bei der Reduzierung der Entwicklungskomplexität und der Steigerung der allgemeinen Nutzung. Das Verständnis, wann globale Tabellen, Datenpartitionen und Caching verwendet werden sollen, hilft Ihnen dabei, den Betriebsaufwand zu verringern und basierend auf Ihren Workload-Anforderungen zu skalieren.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel

## Implementierungsleitfaden

Verwenden Sie Software- und Architekturmuster, die optimal zu den Eigenschaften Ihrer Daten und den Zugriffsmustern passen. Verwenden Sie etwa eine [moderne Datenarchitektur in AWS](#), die die Nutzung speziell erstellter Services ermöglicht, die für Ihre ganz speziellen Analytikanwendungsfälle optimiert sind. Diese Architekturmuster ermöglichen die effiziente Datenverarbeitung und verringern die Ressourcennutzung.

## Implementierungsschritte

- Analysieren Sie die Eigenschaften ihrer Daten und Ihre Zugriffsmuster, um die korrekte Konfiguration für Ihre Cloud-Ressourcen zu identifizieren. Zu den berücksichtigenden Schlüsselmerkmalen gehören:
  - Datentyp: strukturiert, semistrukturiert, unstrukturiert
  - Datenwachstum: begrenzt, unbegrenzt
  - Lebensdauer von Daten: anhaltend, flüchtig, vorübergehend
  - Zugriffsmuster: Lese- oder Schreibzugriff, Häufigkeit von Aktualisierungen, schwankend oder konsistent
- Verwenden Sie Architekturmuster, die Datenzugriffs- und Speichermuster optimal unterstützen.
  - [Muster zur Aktivierung der Datenpersistenz](#)
  - [Let's Architect! Moderne Datenarchitekturen](#)
  - [Datenbanken zu AWS: Das richtige Tool für den richtigen Job](#)
- Nutzen Sie Technologien, die nativ mit komprimierten Daten funktionieren.
  - [Dateiformate von Athena Compression Support](#)
  - [Formatoptionen für ETL Eingaben und Ausgaben in AWS Glue](#)
  - [Laden komprimierter Datendateien aus Amazon S3 mit Amazon Redshift](#)

- Verwenden Sie zweckgerichtet erstellte [Analytikservices](#) für die Datenverarbeitung in Ihrer Architektur. Einzelheiten zu AWS speziell entwickelten Analysediensten finden Sie unter [AWS re:Invent 2022 — Building modern data architectures](#) on. AWS
- Verwenden Sie die Datenbank-Engine, die das dominierende Abfragemuster jeweils am besten unterstützt. Verwalten Sie Ihre Datenbankindizes so, dass sie die effiziente Ausführung von Abfragen unterstützen. Weitere Details finden Sie unter [AWS -Datenbanken](#) und [AWS re:Invent 2.022 - Modernize apps with purpose-built databases](#).
- Wählen Sie Netzwerkprotokolle aus, die die Menge der genutzten Netzwerkkapazitäten in Ihrer Architektur reduzieren.

## Ressourcen

### Zugehörige Dokumente:

- [COPYaus spaltenförmigen Datenformaten mit Amazon Redshift](#)
- [Converting Your Input Record Format in Firehose](#)
- [Improve query performance on Amazon Athena by Converting to Columnar Formats](#)
- [Monitoring DB load with Performance Insights on Amazon Aurora](#)
- [Überwachen der Datenbanklast mit Performance Insights auf Amazon RDS](#)
- [Speicherklasse Amazon S3 Intelligent-Tiering](#)
- [Erstellen Sie einen CQRS Event-Shop mit Amazon DynamoDB](#)

### Zugehörige Videos:

- [AWS re:Invent 2022 — Aufbau von Data-Mesh-Architekturen auf AWS](#)
- [AWS re:Invent 2023 — Tauchen Sie tief in Amazon Aurora und seine Innovationen ein](#)
- [AWS re:Invent 2023 — Verbessern Sie die EBS Effizienz von Amazon und seien Sie kosteneffizienter](#)
- [AWS re:Invent 2023 — Optimierung von Speicherpreis und -leistung mit Amazon S3](#)
- [AWS re:Invent 2023 — Aufbau und Optimierung eines Data Lakes auf Amazon S3](#)
- [AWS re:Invent 2023 — Fortgeschrittene ereignisgesteuerte Muster mit Amazon EventBridge](#)

### Zugehörige Beispiele:

- [AWS Workshop zu speziell entwickelten Datenbanken](#)
- [AWS Immersionstag zur modernen Datenarchitektur](#)
- [Bauen Sie ein Datennetz auf AWS](#)

## Daten

### Frage

- [SUS4 Wie nutzen Sie Datenmanagementrichtlinien und -muster, um Ihre Nachhaltigkeitsziele zu unterstützen?](#)

SUS4 Wie nutzen Sie Datenmanagementrichtlinien und -muster, um Ihre Nachhaltigkeitsziele zu unterstützen?

Implementieren Sie Verfahren für die Datenverwaltung, die den zur Unterstützung Ihrer Workload bereitgestellten Speicher und die für dessen Nutzung erforderlichen Ressourcen reduzieren. Verstehen Sie Ihre Daten und setzen Sie Speichertechnologien und -konfigurationen ein, die den geschäftlichen Mehrwert der Daten und deren Nutzung besser fördern. Verschieben Sie die Daten während des Lebenszyklus zu effizienteren Speichern mit geringerer Leistung, wenn die Anforderungen abnehmen. Löschen Sie Daten, die nicht mehr benötigt werden.

### Bewährte Methoden

- [SUS04-BP01 Implementieren Sie eine Datenklassifizierungsrichtlinie](#)
- [SUS04-BP02 Verwenden Sie Technologien, die Datenzugriffs- und Speichermuster unterstützen](#)
- [SUS04-BP03 Verwenden Sie Richtlinien, um den Lebenszyklus Ihrer Datensätze zu verwalten](#)
- [SUS04-BP04 Nutzen Sie Elastizität und Automatisierung, um den Blockspeicher oder das Dateisystem zu erweitern](#)
- [SUS04-BP05 Nicht benötigte oder redundante Daten entfernen](#)
- [SUS04-BP06 Verwenden Sie gemeinsam genutzte Dateisysteme oder Speicher, um auf gemeinsame Daten zuzugreifen](#)
- [SUS04-BP07 Datenbewegungen zwischen Netzwerken minimieren](#)
- [SUS04-BP08 Daten nur sichern, wenn sie schwer wiederhergestellt werden können](#)

## SUS04-BP01 Implementieren Sie eine Datenklassifizierungsrichtlinie

Klassifizieren Sie die Daten, um zu verstehen, wie wichtig sie für die Geschäftsergebnisse sind, und wählen Sie die richtige energieeffiziente Speicherebene zur Speicherung der Daten.

Typische Anti-Muster:

- Sie identifizieren keine Datenbestände mit ähnlichen Merkmalen (z. B. Sensibilität, Geschäftskritikalität oder gesetzliche Anforderungen), die verarbeitet oder gespeichert werden.
- Sie haben keinen Datenkatalog zur Inventarisierung Ihrer Datenbestände eingeführt.

Vorteile der Nutzung dieser bewährten Methode: Durch die Implementierung einer Datenklassifizierungsrichtlinie können Sie die energieeffizienteste Speicherebene für Daten bestimmen.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel

Implementierungsleitfaden

Bei der Datenklassifizierung wird identifiziert, welche Arten von Daten in einem Informationssystem verarbeitet und gespeichert werden, das einer Organisation gehört oder von ihr betrieben wird. Dazu gehört auch die Bestimmung der Kritikalität der Daten und der wahrscheinlichen Auswirkungen von Preisgaben, Verlusten oder Missbrauch von Daten.

Implementieren Sie Richtlinien zur Datenklassifizierung, indem Sie von der kontextuellen Verwendung der Daten ausgehen und ein Kategorisierungsschema erstellen, das den Grad der Kritikalität eines bestimmten Datensatzes für die Abläufe einer Organisation berücksichtigt.

Implementierungsschritte

- Bestandsaufnahme vornehmen: Führen Sie eine Bestandsaufnahme der verschiedenen Datentypen durch, die für Ihre Workload vorhanden sind.
- Daten gruppieren: Bestimmen Sie die Kritikalität, Vertraulichkeit, Integrität und Verfügbarkeit von Daten auf der Grundlage des Risikos für die Organisation. Verwenden Sie diese Anforderungen, um Daten in eine der von Ihnen gewählten Datenklassifizierungsebenen einzuteilen. Ein Beispiel finden Sie unter [Vier einfache Schritte zur Klassifizierung Ihrer Daten und zur Sicherung Ihres Startups](#).
- Datenklassifizierungsebenen und Richtlinien definieren: Definieren Sie für jede Datengruppe die Datenklassifizierungsebene (z. B. öffentlich oder vertraulich) und die Verarbeitungsrichtlinien.

Kennzeichnen Sie Daten entsprechend. Einzelheiten zu den Kategorien für die Datenklassifizierung finden Sie im Whitepaper zur Datenklassifizierung.

- **Regelmäßige Überprüfung:** Überprüfen und kontrollieren Sie Ihre Umgebung regelmäßig auf nicht markierte und nicht klassifizierte Daten. Verwenden Sie die Automatisierung, um diese Daten zu identifizieren und die Daten entsprechend zu klassifizieren und zu markieren. Ein Beispiel finden Sie unter [Data Catalog and crawlers in AWS Glue](#).
- **Datenkatalog einrichten:** Richten Sie einen Datenkatalog mit Prüfungs- und Governance-Funktionen ein.
- **Dokumentation:** Dokumentieren Sie Datenklassifizierungsrichtlinien und Verarbeitungsverfahren für jede Datenklasse.

## Ressourcen

### Zugehörige Dokumente:

- [Nutzung von AWS Cloud zur Unterstützung der Datenklassifizierung](#)
- [Kennzeichnen Sie Richtlinien von AWS Organizations](#)

### Zugehörige Videos:

- [AWS re:Invent 2022 — Agilität mit aktivierter Datenverwaltung ermöglichen AWS](#)
- [AWS re:Invent 2023 — Datenschutz und Resilienz mit Speicher AWS](#)

SUS04-BP02 Verwenden Sie Technologien, die Datenzugriffs- und Speichermuster unterstützen

Nutzen Sie Speichertechnologien, die den Zugriff auf Ihre Daten und ihre Speicherung jeweils optimal unterstützen, um die Zahl der bereitgestellten Ressourcen zu minimieren und gleichzeitig den Workload zu unterstützen.

### Typische Anti-Muster:

- Sie gehen davon aus, dass für alle Workloads ähnliche Datenspeicher- und Zugriffsmuster gelten.
- Sie verwenden nur eine Speicherebene, vorausgesetzt, dass alle Workloads in diese Ebene passen.
- Sie gehen davon aus, dass Datenzugriffsmuster im Laufe der Zeit konsistent bleiben.



Vorteile der Nutzung dieser bewährten Methode: Die Auswahl und Optimierung Ihrer Speichertechnologien auf der Grundlage von Datenzugriffs- und Speichermustern hilft Ihnen, die erforderlichen Cloud-Ressourcen zu reduzieren, um Ihre Geschäftsanforderungen zu erfüllen und die Gesamteffizienz der Cloud-Workload zu verbessern.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Niedrig

### Implementierungsleitfaden

Wählen Sie für maximale Leistungseffizienz die für Ihre Zugriffsmuster geeignete Speicherlösung, oder passen Sie Ihre Zugriffsmuster an die Speicherlösung an.

### Implementierungsschritte

- **Daten- und Zugriffsmerkmale bewerten:** Bewerten Sie Ihre Datenmerkmale und Zugriffsmuster, um die wichtigsten Merkmale Ihres Speicherbedarfs zu erfassen. Zu den berücksichtigenden Schlüsselmerkmalen gehören:
  - Datentyp: strukturiert, semistrukturiert, unstrukturiert
  - Datenwachstum: begrenzt, unbegrenzt
  - Lebensdauer von Daten: anhaltend, flüchtig, vorübergehend
  - Zugriffsmuster: Lese- oder Schreibzugriff, Häufigkeit, schwankend oder konsistent
- **Die richtige Speichertechnologie auswählen:** Migrieren Sie Daten zur geeigneten Speichertechnologie, die Ihre Datenmerkmale und Zugriffsmuster unterstützt. Hier sind einige Beispiele für AWS Speichertechnologien und ihre wichtigsten Merkmale:

Typ	Technologie	Schlüsselmerkmale
Objektspeicher	<a href="#">Amazon S3</a>	Ein Objektspeicherservice mit unbegrenzter Skalierbarkeit, hoher Verfügbarkeit und mehreren Zugriffsoptionen. Für die Übertragung von Objekten in und aus Amazon S3 und den Zugriff auf diese Objekte können Sie einen Service wie z. B. <a href="#">Transfer Acceleration</a> oder <a href="#">Zugangspunkte</a> verwenden

Typ	Technologie	Schlüsselmerkmale
		, um Ihren Standort, Ihre Sicherheitsanforderungen und Zugriffsmuster zu unterstützen.
Archivieren von Speichern	<a href="#">Amazon S3 Glacier</a>	Speicherklasse von Amazon S3 für die Datenarchivierung.
Gemeinsames Dateisystem	<a href="#">Amazon Elastic File System (AmazonEFS)</a>	Bereitstellbares Dateisystem, auf das mehrere Arten von Datenverarbeitungslösungen zugreifen können. Amazon vergrößert und verkleinert den Speicherplatz EFS automatisch und ist leistungsoptimiert, um gleichbleibend niedrige Latenzen zu gewährleisten.
Gemeinsames Dateisystem	<a href="#">Amazon FSx</a>	Basiert auf den neuesten AWS Computerlösungen zur Unterstützung von vier häufig verwendeten Dateisystemen: Open NetApp ONTAPZFS, Windows File Server und Lustre. Die FSx <a href="#">Latenz, der Durchsatz und</a> der Durchsatz von Amazon IOPS variieren je nach Dateisystem und sollten bei der Auswahl des richtigen Dateisystems für Ihre Workload-Anforderungen berücksichtigt werden.

Typ	Technologie	Schlüsselmerkmale
Blockspeicher	<a href="#">Amazon Elastic Block Store (AmazonEBS)</a>	Skalierbarer, leistungsstarker Blockspeicher-Service, der für Amazon Elastic Compute Cloud (AmazonEC2) entwickelt wurde. Amazon EBS bietet SSD-gestützten Speicher für IOPS transaktionsintensive Workloads und HDD-gestützten Speicher für durchsatzintensive Workloads.
Relationale Datenbank	<a href="#">Amazon Aurora</a> , <a href="#">Amazon RDS</a> , <a href="#">Amazon Redshift</a>	Konzipiert zur Unterstützung von Transaktionen ACID (Atomizität, Konsistenz, Isolierung, Haltbarkeit) und zur Wahrung der referenziellen Integrität und starken Datenkonsistenz. Viele traditionelle Anwendungen, Enterprise Resource Planning (ERP), Customer Relationship Management (CRM) und E-Commerce-Systeme verwenden relationale Datenbanken, um ihre Daten zu speichern.

Typ	Technologie	Schlüsselmerkmale
Schlüssel-Werte-Datenbank	<a href="#">Amazon-DynamoDB</a>	Für gängige Zugriffsmuster optimiert, üblicherweise zum Speichern und Abrufen großer Datenmengen. Web-Apps mit hohem Datenverkehr, E-Commerce-Systeme und Gaming-Anwendungen sind typische Anwendungsfälle für Schlüssel-Werte-Datenbanken.

- Automatisieren Sie die Speicherzuweisung: Überwachen Sie bei Speichersystemen mit fester Größe, wie Amazon EBS oder AmazonFSx, den verfügbaren Speicherplatz und automatisieren Sie die Speicherzuweisung bei Erreichen eines Schwellenwerts. [Sie können Amazon nutzen CloudWatch , um verschiedene Kennzahlen für Amazon und Amazon zu sammeln EBS und zu analysierenFSx.](#)
- Die richtige Speicherklasse wählen: Wählen Sie die passende Speicherklasse für Ihre Daten.
  - Amazon-S3-Speicherklassen können auf Objektebene konfiguriert werden. Ein einzelner Bucket kann Objekte enthalten, die in allen Speicherklassen gespeichert sind.
  - Sie können [Amazon-S3-Lebenszyklusrichtlinien](#) verwenden, um Objekte automatisch zwischen Speicherklassen zu wechseln oder Daten zu entfernen, ohne dass die Anwendung geändert werden muss. Im Allgemeinen müssen Sie bei diesen Speichermechanismen einen Kompromiss zwischen Ressourceneffizienz, Zugriffslatenz und Zuverlässigkeit eingehen.

## Ressourcen

### Zugehörige Dokumente:

- [EBSAmazon-Volumetypen](#)
- [EC2Amazon-Instance-Speicher](#)
- [Amazon S3 Intelligent-Tiering](#)
- [Eigenschaften von Amazon EBS I/O](#)
- [Verwenden von Amazon-S3-Speicherklassen](#)
- [Was ist Amazon S3 Glacier?](#)

## Zugehörige Videos:

- [AWS re:Invent 2023 — Verbessern Sie die EBS Effizienz von Amazon und seien Sie kosteneffizienter](#)
- [AWS re:Invent 2023 — Optimierung von Speicherpreis und -leistung mit Amazon S3](#)
- [AWS re:Invent 2023 — Aufbau und Optimierung eines Data Lakes auf Amazon S3](#)
- [AWS re:Invent 2022 — Aufbau moderner Datenarchitekturen auf AWS](#)
- [AWS re:Invent 2022 — Modernisieren Sie Apps mit speziell entwickelten Datenbanken](#)
- [AWS re:Invent 2022 — Aufbau von Data-Mesh-Architekturen auf AWS](#)
- [AWS re:Invent 2023 — Tauchen Sie tief in Amazon Aurora und seine Innovationen ein](#)
- [AWS re:Invent 2023 — Fortgeschrittene Datenmodellierung mit Amazon DynamoDB](#)

## Zugehörige Beispiele:

- [Amazon-S3-Beispiele](#)
- [AWS Workshop zu speziell entwickelten Datenbanken](#)
- [Databases for Developers](#)
- [AWS Immersionstag zur modernen Datenarchitektur](#)
- [Bauen Sie ein Datennetz auf AWS](#)

SUS04-BP03 Verwenden Sie Richtlinien, um den Lebenszyklus Ihrer Datensätze zu verwalten

Verwalten Sie den Lebenszyklus aller Daten und setzen Sie automatisch Löschen durch, um den für Ihre Workload benötigten Speicher insgesamt zu minimieren.

## Typische Anti-Muster:

- Sie löschen Daten manuell.
- Sie löschen keine Workload-Daten.
- Sie verschieben Daten nicht abhängig von den Aufbewahrungs- und Zugriffsanforderungen in energieeffizientere Speicherebenen.

Vorteile der Einführung dieser bewährten Methode: Durch Richtlinien für den Lebenszyklus wird die Effizienz des Datenzugriffs und der Datenaufbewahrung für eine Workload sichergestellt.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel

## Implementierungsleitfaden

Datensätze verfügen während ihres Lebenszyklus normalerweise über unterschiedliche Aufbewahrungs- und Zugriffsanforderungen. So kann eine Anwendung z. B. für einen bestimmten Zeitraum häufig Zugriff auf einige Datensätze benötigen. Danach wird nur noch unregelmäßig darauf zugegriffen.

Um Datensätze während ihres Lebenszyklus effizient zu verwalten, konfigurieren Sie Lebenszyklusrichtlinien, d. h. Regeln, die den Umgang mit den Datensätzen definieren.

Mit Lebenszyklus-Konfigurationsregeln können Sie einen bestimmten Speicherservice anweisen, einen Datensatz in energieeffizientere Speicherebenen zu verschieben, ihn zu archivieren oder zu löschen.

## Implementierungsschritte

- [Klassifizieren Sie Datensätze in Ihrer Workload.](#)
- Definieren Sie Bearbeitungsverfahren für jede Datenklasse.
- Legen Sie automatisierte Lebenszyklusrichtlinien zur Durchsetzung von Lebenszyklusregeln fest. Im Folgenden finden Sie einige Beispiele für die Einrichtung automatisierter Lebenszyklusrichtlinien für verschiedene AWS Speicherdienste:

Storage Service	Festlegen von automatisierten Lebenszyklusrichtlinien
<a href="#">Amazon S3</a>	<p>Mit <a href="#">Amazon-S3-Lebenszyklen</a> können Sie Ihre Objekte während ihres gesamten Lebenszyklus verwalten. Wenn die Zugriffsmuster unbekannt oder nicht prognostizierbar sind oder sich ändern, können Sie <a href="#">Amazon S3 Intelligent-Tiering</a> verwenden. Hiermit werden Zugriffsmuster überwacht und Objekte, auf die nicht zugegriffen wurde, automatisch in kostengünstigere Zugriffsebenen verschoben. Anhand der Metriken von <a href="#">Amazon S3 Storage Lens</a> können Sie Optimierungsmöglichkeiten</p>

Storage Service	Festlegen von automatisierten Lebenszyklusrichtlinien und Lücken im Lebenszyklusmanagement ermitteln.
<a href="#">Amazon Elastic Block Store</a>	Sie können <a href="#">Amazon Data Lifecycle Manager</a> verwenden, um die Erstellung, Aufbewahrung und Löschung von EBS Amazon-Snapshots und Amazon EBS zu automatisieren. AMIs
<a href="#">Amazon Elastic File System</a>	<a href="#">Amazon EFS Lifecycle Management</a> verwaltet automatisch den Dateispeicher für Ihre Dateisysteme.
<a href="#">Amazon Elastic Container Registry</a>	Die <a href="#">ECRLbenszyklusrichtlinien von Amazon</a> automatisieren die Bereinigung Ihrer Container-Images, indem sie Bilder je nach Alter oder Anzahl ablaufen lassen.
<a href="#">AWS Elemental MediaStore</a>	Sie können eine <a href="#">Objektlebenszyklus-Richtlinie</a> verwenden, die festlegt, wie lange Objekte im Container gespeichert werden sollen. MediaStore

- Löschen Sie nicht genutzte Volumes, Snapshots und Daten, deren Aufbewahrungszeitraum abgelaufen ist. Nutzen Sie native Servicefunktionen wie [Amazon DynamoDB Time To Live](#) oder die [Aufbewahrung von CloudWatch Amazon-Protokollen zum Löschen](#).
- Aggregieren und komprimieren Sie Daten wenn möglich auf der Basis von Lebenszyklusregeln.

## Ressourcen

### Zugehörige Dokumente:

- [Optimieren Ihrer Amazon-S3-Lebenszyklusregeln mit der Amazon-S3-Speicherklassenanalyse](#)
- [Evaluierung von Ressourcen mit AWS-Config-Regeln](#)

### Zugehörige Videos:

- [AWS re:Invent 2021 — Bewährte Methoden für Amazon S3 Lifecycle zur Optimierung Ihrer Speicherausgaben](#)
- [AWS re:Invent 2023 — Optimierung von Speicherpreis und -leistung mit Amazon S3](#)
- [Simplify Your Data Lifecycle and Optimize Storage Costs With Amazon S3 Lifecycle](#)
- [Reduce Your Storage Costs Using Amazon S3 Storage Lens](#)

SUS04-BP04 Nutzen Sie Elastizität und Automatisierung, um den Blockspeicher oder das Dateisystem zu erweitern

Verwenden Sie Elastizität und Automatisierung, um den Block-Speicher oder das Dateisystem zu erweitern, wenn das Datenvolumen zunimmt, um den bereitgestellten Gesamtspeicher zu minimieren.

Typische Anti-Muster:

- Sie unterhalten einen großen Block-Speicher oder ein großes Dateisystem für künftige Anforderungen.
- Sie stellen die Eingabe- und Ausgabeoperationen pro Sekunde (IOPS) Ihres Dateisystems zu viel bereit.
- Sie überwachen die Nutzung Ihrer Daten-Volumes nicht.

Vorteile der Nutzung dieser bewährten Methode: Die Minimierung der übermäßigen Bereitstellung für das Speichersystem reduziert ungenutzte Ressourcen und verbessert die Gesamteffizienz Ihrer Workload.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel

Implementierungsleitfaden

Erstellen Sie Block-Speicher und Dateisysteme mit Größenzuweisung, Durchsatz und Latenz, die den Anforderungen Ihrer Workloads entsprechen. Verwenden Sie Elastizität und Automatisierung, um den Block-Speicher oder das Dateisystem zu erweitern, wenn das Datenvolumen zunimmt, ohne dass diese Speicherservices übermäßig bereitgestellt werden.

Implementierungsschritte

- Stellen Sie bei Speichern mit fester Größe wie [Amazon](#) sicherEBS, dass Sie die Menge des verwendeten Speichers im Vergleich zur Gesamtspeichergröße überwachen, und erstellen



Sie nach Möglichkeit eine Automatisierung, um die Speichergröße zu erhöhen, wenn ein Schwellenwert erreicht wird.

- Verwenden Sie elastische Volumes und verwaltete Blockdaten-Services, um automatisch zusätzlichen Speicher zuzuweisen, wenn die Menge der persistenten Daten wächst. Beispielsweise können Sie [Amazon EBS Elastic Volumes](#) verwenden, um die Volume-Größe und den Volume-Typ zu ändern oder die Leistung Ihrer EBS Amazon-Volumes anzupassen.
- Wählen Sie die korrekte Speicherklasse sowie den korrekten Leistungs- und Durchsatz-Modus für Ihr Dateisystem für Ihre geschäftlichen Anforderungen und überschreiten Sie diese nicht.
  - [EFSLeistung von Amazon](#)
  - [EBSAmazon-Volumenleistung auf Linux-Instances](#)
- Legen Sie Zielstufen für die Nutzung Ihrer Daten-Volumes fest und passen Sie die Größe von Volumes an, die außerhalb der erwarteten Bereiche liegen.
- Passen Sie die Größe schreibgeschützter Volumes an die Datenmenge an.
- Migrieren Sie Daten zu Objektspeichern, um zu vermeiden, dass die überschüssige Kapazität aus Volumes mit fester Größe im Blockspeicher bereitgestellt wird.
- Überprüfen Sie elastische Volumes und Dateisysteme, beenden Sie nicht genutzte und verkleinern Sie zu große Volumes, um sie an den aktuellen Datenumfang anzupassen.

## Ressourcen

### Zugehörige Dokumente:

- [Erweitern Sie das Dateisystem, nachdem Sie die Größe eines EBS Volumes geändert haben](#)
- [Ändern Sie ein Volume mit Amazon EBS Elastic Volumes](#)
- [Amazon FSx – Dokumentation](#)
- [What is Amazon Elastic File System?](#)

### Zugehörige Videos:

- [Tiefer Einblick in Amazon EBS Elastic Volumes](#)
- [Optimierungsstrategien von Amazon EBS und Snapshot für bessere Leistung und Kosteneinsparungen](#)
- [Optimierung von Amazon im EFS Hinblick auf Kosten und Leistung mithilfe von Best Practices](#)

## SUS04-BP05 Nicht benötigte oder redundante Daten entfernen

Entfernen Sie nicht benötigte oder redundante Daten, um die zum Speichern Ihrer Datensätze benötigten Speicherressourcen zu minimieren.

Typische Anti-Muster:

- Sie duplizieren Daten, die leicht abgerufen oder erneut erstellt werden können.
- Sie sichern alle Daten, ohne ihre Kritikalität zu berücksichtigen.
- Sie löschen Daten nur unregelmäßig, nur bei bestimmten Ereignissen oder gar nicht.
- Sie speichern Daten redundant, unabhängig von der Stabilität des Speicherservices.
- Sie aktivieren die Amazon-S3-Versionsverwaltung, ohne dass dies geschäftlich gerechtfertigt ist.

Vorteile der Einführung dieser bewährten Methode: Durch das Entfernen nicht benötigter Daten werden die für Ihre Workload benötigte Speichergröße und die Umweltbelastungen durch die Workload reduziert.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel

Implementierungsleitfaden

Speichern Sie keine Daten, die Sie nicht benötigen. Automatisieren Sie das Löschen von nicht benötigten Daten. Verwenden Sie Technologien, die Daten auf Datei- und Blockebene deduplizieren. Nutzen Sie native Servicefeatures für Replikation und Redundanz.

Implementierungsschritte

- Bewerten Sie, ob Sie das Speichern von Daten vermeiden können, indem Sie vorhandene, öffentlich verfügbare Datensätze in [AWS Data Exchange](#) und [offene Daten in AWS](#) verwenden.
- Verwenden Sie Mechanismen, die Daten auf Block- und Objektebene deduplizieren können. Hier sind einige Beispiele für die Deduplizierung von Daten auf: AWS

Storage Service	Deduplizierungsmechanismus
<a href="#">Amazon S3</a>	Wird verwendet <a href="#">AWS Lake Formation FindMatches</a> , um mithilfe der neuen FindMatches ML-Transformation nach übereinstimmenden Datensätzen in einem

Storage Service	Deduplizierungsmechanismus
	Datensatz (einschließlich solcher ohne Identifikatoren) zu suchen.
<a href="#">Amazon FSx</a>	Verwenden Sie <a href="#">die Dateneduplizierung</a> auf Amazon FSx für Windows.
<a href="#">Snapshots von Amazon Elastic Block Store</a>	Snapshots sind inkrementelle Backups, d. h., es werden nur die Blöcke des Geräts gespeichert, die sich seit der letzten Snapshot-Speicherung geändert haben.

- Analysieren Sie den Datenzugriff, um nicht benötigte Daten zu identifizieren. Automatisieren Sie Lebenszyklusrichtlinien. Nutzen Sie native Servicefunktionen wie [Amazon DynamoDB Time To Live](#), [Amazon S3 Lifecycle](#) oder die [Aufbewahrung von CloudWatch Amazon-Protokollen zum Löschen](#).
- Verwenden Sie Datenvirtualisierungsfunktionen AWS , um Daten an der Quelle zu verwalten und Datenduplikationen zu vermeiden.
  - [Cloud-native Datenvirtualisierung aktiviert AWS](#)
  - [Optimierung von Datenmustern mithilfe von Amazon Redshift Data Sharing](#)
- Verwenden Sie Sicherungstechnologien, mit denen inkrementelle Sicherungen möglich sind.
- Nutzen Sie die Beständigkeit von [Amazon S3](#) und die [Replikation von Amazon EBS](#), um Ihre Stabilitätsziele zu erreichen, anstatt selbstverwaltete Technologien (wie ein redundantes Array unabhängiger Festplatten (RAID)) zu verwenden.
- Zentralisieren Sie Protokoll- und Nachverfolgungsdaten, deduplizieren Sie identische Protokolleinträge und richten Sie Mechanismen für die Anpassung der Ausführlichkeit ein, wenn notwendig.
- Füllen Sie Caches nur vorab aus, wenn dies begründet werden kann.
- Richten Sie Überwachung und Automatisierung für den Cache ein, um seine Größe entsprechend anzupassen.
- Entfernen Sie out-of-date Bereitstellungen und Ressourcen aus Objektspeichern und Edge-Caches, wenn Sie neue Versionen Ihres Workloads bereitstellen.

## Ressourcen

### Zugehörige Dokumente:

- [Ändern Sie die Aufbewahrung von Protokolldaten in Logs CloudWatch](#)
- [Datenduplizierung auf Amazon FSx für Windows File Server](#)
- [Funktionen von AmazonFSx, ONTAP einschließlich Datenduplizierung](#)
- [Dateien bei Amazon ungültig machen CloudFront](#)
- [Wird AWS Backup zum Sichern und Wiederherstellen von EFS Amazon-Dateisystemen verwendet](#)
- [Was ist Amazon CloudWatch Logs?](#)
- [Mit Backups bei Amazon arbeiten RDS](#)
- [Integrieren und deduplizieren Sie Datensätze mit AWS Lake Formation](#)

### Zugehörige Videos:

- [Amazon Redshift Data Sharing Use Cases](#)

### Zugehörige Beispiele:

- [Wie verwende ich Amazon Athena, um meine Amazon-S3-Serverzugriffsprotokolle zu analysieren?](#)

SUS04-BP06 Verwenden Sie gemeinsam genutzte Dateisysteme oder Speicher, um auf gemeinsame Daten zuzugreifen

Verwenden Sie geteilte Dateisysteme oder Speicher, um Datenduplizierungen zu vermeiden und eine effizientere Infrastruktur für Ihre Workload zu ermöglichen.

### Typische Anti-Muster:

- Sie stellen für jeden einzelnen Client Speicher bereit.
- Sie trennen Daten-Volumes von inaktiven Clients nicht ab.
- Sie ermöglichen keinen Zugriff auf Speicher über Plattformen und Systeme hinweg.

Vorteile der Nutzung dieser bewährten Methode: Die Verwendung geteilter Dateisysteme oder Speicher ermöglicht die gemeinsame Nutzung von Daten für mehrere Verbraucher, ohne dass diese

dazu kopiert werden müssen. Dies reduziert den Umfang der erforderlichen Speicherressourcen für die Workload.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel

### Implementierungsleitfaden

Wenn Sie mehrere Benutzer oder Anwendungen haben, die auf dieselben Datensätze zugreifen müssen, ist die Verwendung geteilter Speichertechnologien wichtig für eine effiziente Infrastruktur für Ihre Workload. Solche Technologien bieten einen zentralen Speicherort für die Speicherung und Verwaltung von Datensätzen und zur Vermeidung von Datenduplizierungen. Dazu wird die Konsistenz der Daten über verschiedene Systeme hinweg durchgesetzt. Hinzu kommt, dass geteilte Speicher die effizientere Nutzung der Datenverarbeitungsleistung ermöglichen, da mehr Datenverarbeitungsressourcen gleichzeitig auf Daten zugreifen und diese verarbeiten können.

Rufen Sie Daten von diesen geteilten Speicherservices nur bei Bedarf ab und trennen Sie nicht genutzte Volumes, um Ressourcen freizugeben.

### Implementierungsschritte

- Migrieren Sie Daten in einen geteilten Speicher, wenn die Daten mehrfach genutzt werden. Hier sind einige Beispiele für gemeinsam genutzte Speichertechnologien in folgenden Bereichen: AWS

Speicheroption	Wann sollte dies verwendet werden?
<a href="#">Amazon EBS Multi-Attach</a>	Mit Amazon EBS Multi-Attach können Sie ein einzelnes bereitgestelltes Volume IOPS SSD (io1 oder io2) mehreren Instances zuordnen, die sich in derselben Availability Zone befinden.
<a href="#">Amazon EFS</a>	Erfahren Sie, <a href="#">wann Sie sich für Amazon entscheiden sollten EFS</a> .
<a href="#">Amazon FSx</a>	Weitere Informationen finden <a href="#">Sie unter Auswahl eines FSx Amazon-Dateisystems</a> .
<a href="#">Amazon S3</a>	Anwendungen, die keine Dateisystemstruktur benötigen und zur Arbeit mit Objektspeichern gedacht sind, können Amazon S3

Speicheroption	Wann sollte dies verwendet werden?
	als massive, skalierbare, dauerhafte und kostengünstige Speicherlösung nutzen.

- Kopieren Sie Daten bzw. rufen Sie sie nur dann von geteilten Dateisystemen ab, wenn Sie sie benötigen. Sie können beispielsweise ein [Amazon FSx for Lustre-Dateisystem erstellen, das von Amazon S3 unterstützt wird](#), und nur die Teilmenge der Daten, die für die Verarbeitung von Aufträgen erforderlich sind, in Amazon laden. FSx
- Löschen Sie Daten entsprechend Ihren Nutzungsmustern, wie in [SUS04-BP03 Verwenden Sie Richtlinien, um den Lebenszyklus Ihrer Datensätze zu verwalten](#) erläutert.
- Trennen Sie Volumes von Clients, die sie nicht aktiv verwenden.

## Ressourcen

### Zugehörige Dokumente:

- [Linking your file system to an Amazon S3 bucket](#)
- [Verwenden Sie Amazon EFS for AWS Lambda in Ihren serverlosen Anwendungen](#)
- [Amazon EFS Intelligent-Tiering optimiert die Kosten für Workloads bei wechselnden Zugriffsmustern](#)
- [Amazon FSx mit Ihrem lokalen Daten-Repository verwenden](#)

### Zugehörige Videos:

- [Optimierung der Lagerkosten mit Amazon EFS](#)
- [AWS re:Invent 2023 — Was ist neu bei der Dateispeicherung AWS](#)
- [AWS re:Invent 2023 — Dateispeicher für Entwickler und Datenwissenschaftler auf Amazon Elastic File System](#)

## SUS04-BP07 Datenbewegungen zwischen Netzwerken minimieren

Verwenden Sie gemeinsam genutzte Dateisysteme oder Objektspeicher zum Zugriff auf häufig genutzte Daten und minimieren Sie die zur Unterstützung von Datenverschiebungen für Ihre Workload benötigten Netzwerkressourcen.

### Typische Anti-Muster:

- Sie speichern alle Daten in derselben Datenbank, AWS-Region unabhängig davon, wo sich die Datennutzer befinden.
- Sie optimieren Datenumfang und -format nicht vor der Verschiebung über das Netzwerk.

Vorteile der Nutzung dieser bewährten Methode: Die Optimierung der Datenverschiebung über das Netzwerk reduziert den Umfang der für die Workload benötigten Netzwerkressourcen und verringert die Umweltauswirkungen.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel

### Implementierungsleitfaden

Das Verschieben von Daten in der gesamten Organisation erfordert Datenverarbeitungs-, Netzwerk- und Speicherressourcen. Verwenden Sie Techniken zur Minimierung von Datenverschiebungen und verbessern Sie die Gesamteffizienz Ihrer Workloads.

### Implementierungsschritte

- Berücksichtigen Sie die Nähe zu den Daten oder Benutzer für die Entscheidung bei der [Auswahl einer Region für Ihre Workload](#).
- Partitionieren Sie regional genutzte Services so, dass regionsspezifische Daten in der Region gespeichert werden, in der sie genutzt werden.
- Verwenden Sie effiziente Dateiformate (wie Parquet oder ORC) und komprimieren Sie Daten, bevor Sie sie über das Netzwerk übertragen.
- Verschieben Sie keine nicht genutzten Daten. Einige Beispiele, die Ihnen helfen können, das Verschieben ungenutzter Daten zu vermeiden:
  - Reduzieren Sie API die Anzahl der Antworten nur auf relevante Daten.
  - Aggregieren Sie Daten, wenn keine detaillierten Informationen auf Datensatzebene benötigt werden.
  - Siehe [Well-Architected Lab - Optimize Data Pattern Using Amazon Redshift Data Sharing](#).
  - Erwägen Sie den [kontoübergreifenden Datenaustausch in AWS Lake Formation](#).
- Nutzen Sie Services, die Ihnen dabei helfen können, Code näher an den Benutzern Ihrer Workload auszuführen:

Service	Wann sollte dies verwendet werden?
<a href="#">Lambda@Edge</a>	Verwenden Sie dies für rechenintensive Anwendungen, die ausgeführt werden, wenn sich Objekte nicht im Zwischenspeicher befinden.
<a href="#">CloudFrontFunktionen</a>	Wird für einfache Anwendungsfälle verwendet , HTTP z. B. für Manipulationen von Anfragen und Antworten, die durch kurzlebige Funktionen ausgelöst werden können.
<a href="#">AWS IoT Greengrass</a>	Führen Sie lokale Datenverarbeitungsvorgänge, Messaging sowie die Datenzwischenspeicherung für verbundene Geräte aus.

## Ressourcen

### Zugehörige Dokumente:

- [Optimierung Ihrer AWS Infrastruktur im Hinblick auf Nachhaltigkeit, Teil: Netzwerke III](#)
- [AWS Globale Infrastruktur](#)
- [Die CloudFront wichtigsten Funktionen von Amazon, einschließlich des CloudFront Global Edge-Netzwerks](#)
- [HTTPAnfragen in Amazon OpenSearch Service komprimieren](#)
- [Zwischendatenkomprimierung mit Amazon EMR](#)
- [Loading compressed data files from Amazon S3 into Amazon Redshift](#)
- [Bereitstellen komprimierter Dateien mit Amazon CloudFront](#)

### Zugehörige Videos:

- [Entmystifizierung der Datenübertragung am AWS](#)

### Zugehörige Beispiele:



- [Architecting for sustainability - Minimize data movement across networks](#)

SUS04-BP08 Daten nur sichern, wenn sie schwer wiederhergestellt werden können

Vermeiden Sie das Sichern von Daten ohne geschäftlichen Wert, um die Anforderungen an Speicherressourcen für Ihre Workload zu minimieren.

Typische Anti-Muster:

- Sie haben keine Sicherungsstrategie für Ihre Daten.
- Sie sichern Daten, die problemlos erneut erstellt werden können.

Vorteile der Nutzung dieser bewährten Methode: Das Vermeiden der Sicherung nichtkritischer Daten reduziert den Umfang der benötigten Speicherressourcen für die Workload und verringert die Umweltauswirkungen.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel

Implementierungsleitfaden

Die Vermeidung der Sicherung nicht benötigter Daten kann Kosten senken und die von der Workload verwendeten Speicherressourcen verringern. Sichern Sie nur Daten, die einen geschäftlichen Wert haben oder zur Erfüllung von Compliance-Anforderungen benötigt werden. Prüfen Sie Sicherungsrichtlinien und vermeiden Sie einen flüchtigen Speicher, der in einem Wiederherstellungsszenario keinen Wert bietet.

Implementierungsschritte

- Implementieren Sie eine Richtlinie für die Klassifizierung von Daten wie in [SUS04-BP01 Implementieren Sie eine Datenklassifizierungsrichtlinie](#) erläutert.
- Nutzen Sie die Wichtigkeit Ihrer Datenklassifizierung und entwerfen Sie eine Backup-Strategie auf der Grundlage Ihrer Ziele für die [Wiederherstellungszeit \(RTO\) und die Zielsetzung für den Wiederherstellungspunkt \(\)](#). RPO Vermeiden Sie die Sicherung nichtkritischer Daten.
  - Schließen Sie Daten aus, die problemlos erneut erstellt werden können.
  - Schließen Sie flüchtige Daten von Sicherungen aus.
  - Schließen Sie lokale Kopien von Daten aus, es sei denn, der Zeitaufwand für die Wiederherstellung dieser Daten von einem gemeinsamen Speicherort überschreitet Ihre Service Level Agreements (SLAs).

- Verwenden Sie eine automatisierte Lösung oder einen verwalteten Service zur Sicherung geschäftskritischer Daten.
  - [AWS Backup](#) ist ein vollständig verwalteter Service, der es einfach macht, den Datenschutz AWS dienstübergreifend, in der Cloud und vor Ort zu zentralisieren und zu automatisieren. Praktische Anleitungen zur Erstellung automatisierter Backups mit AWS Backup finden Sie unter [Well-Architected Labs - Testing Backup and Restore of Data](#).
  - [Automatisieren Sie Backups und optimieren Sie die Backup-Kosten EFS für Amazon AWS Backup](#).

## Ressourcen

### Zugehörige bewährte Methoden:

- [REL09-BP01 Identifizieren und sichern Sie alle Daten, die gesichert werden müssen, oder reproduzieren Sie die Daten aus Quellen](#)
- [REL09-BP03 Führen Sie die Datensicherung automatisch durch](#)
- [REL13-BP02 Verwenden Sie definierte Wiederherstellungsstrategien, um die Wiederherstellungsziele zu erreichen](#)

### Zugehörige Dokumente:

- [Wird AWS Backup zum Sichern und Wiederherstellen von EFS Amazon-Dateisystemen verwendet](#)
- [EBSAmazon-Schnappschüsse](#)
- [Working with backups on Amazon Relational Database Service](#)
- [APNPartner: Partner, die beim Backup helfen können](#)
- [AWS Marketplace: Für die Sicherung geeignete Produkte](#)
- [Amazon sichern EFS](#)
- [Amazon FSx für Windows File Server sichern](#)
- [Backup und Wiederherstellung für Amazon ElastiCache \(RedisOSS\)](#)

### Zugehörige Videos:

- [AWS re:Invent 2023 — Backup- und Disaster Recovery-Strategien für mehr Resilienz](#)
- [AWS re:Invent 2023 — Was ist neu bei AWS Backup](#)

- [AWS re:Invent 2021 — Backup, Disaster Recovery und Ransomware-Schutz mit AWS](#)

Zugehörige Beispiele:

- [Well-Architected Lab - Backup data](#)

## Hardware und Services

Frage

- [SUS5 Wie wählen und nutzen Sie Cloud-Hardware und -Dienste in Ihrer Architektur, um Ihre Nachhaltigkeitsziele zu unterstützen?](#)

SUS5 Wie wählen und nutzen Sie Cloud-Hardware und -Dienste in Ihrer Architektur, um Ihre Nachhaltigkeitsziele zu unterstützen?

Suchen Sie nach Möglichkeiten, die Auswirkungen auf die Nachhaltigkeit Ihrer Workloads durch Änderungen der Methoden für die Hardwareverwaltung zu reduzieren. Minimieren Sie den Umfang der für die Bereitstellung erforderlichen Hardware und wählen Sie die jeweils effizienteste Hardware und den effizientesten Service für die jeweilige Workload aus.

Bewährte Methoden

- [SUS05-BP01 Verwenden Sie die Mindestmenge an Hardware, die Ihren Anforderungen entspricht](#)
- [SUS05-BP02 Verwenden Sie Instance-Typen mit den geringsten Auswirkungen](#)
- [SUS05-BP03 Managed Services nutzen](#)
- [SUS05-BP04 Optimieren Sie Ihren Einsatz von hardwarebasierten Rechenbeschleunigern](#)

SUS05-BP01 Verwenden Sie die Mindestmenge an Hardware, die Ihren Anforderungen entspricht

Verwenden Sie die geringstmögliche Menge an Hardware für Ihre Workload, um Ihre geschäftlichen Anforderungen in effizienter Weise zu erfüllen.

Typische Anti-Muster:

- Sie überwachen die Ressourcenauslastung nicht.
- Sie haben Ressourcen mit geringer Auslastung in Ihrer Architektur.

- Sie prüfen die Nutzung statischer Hardware nicht, um festzustellen, ob sie neu dimensioniert werden muss.
- Sie legen keine Ziele für die Hardwarenutzung für Ihre Computerinfrastruktur fest, die auf Ihrem Geschäft basieren. KPIs

Vorteile der Nutzung dieser bewährten Methode: Die korrekte Dimensionierung Ihrer Cloud-Ressourcen hilft dabei, die Umweltauswirkungen von Workloads zu reduzieren, Geld zu sparen und Leistungsbenchmarks einzuhalten.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel

### Implementierungsleitfaden

Wählen Sie die optimale Anzahl von Hardwaregeräten für Ihre Workload aus, um die allgemeine Effizienz zu verbessern. Das AWS Cloud bietet die Flexibilität, die Anzahl der Ressourcen dynamisch über eine Vielzahl von Mechanismen zu erweitern oder zu reduzieren, um beispielsweise [AWS Auto Scaling](#) Bedarfsänderungen gerecht zu werden. [Es bietet außerdem Funktionen APIs SDKs, die es ermöglichen, Ressourcen mit minimalem Aufwand zu ändern.](#) Verwenden Sie diese Möglichkeiten für häufige Änderungen an Ihren Workload-Implementierungen. Verwenden Sie außerdem die Richtlinien für die richtige Dimensionierung von AWS Tools, um Ihre Cloud-Ressourcen effizient zu nutzen und Ihre Geschäftsanforderungen zu erfüllen.

### Implementierungsschritte

- Auswahl des Instance-Typs: Wählen Sie den Instance-Typ aus, der Ihren Anforderungen am besten entspricht. Weitere Informationen zur Auswahl von Instances von Amazon Elastic Compute Cloud und zur Verwendung von Mechanismen wie der attributbasierten Auswahl des Instance-Typs finden Sie im Folgenden:
  - [Wie wähle ich den passenden EC2 Amazon-Instance-Typ für meinen Workload aus?](#)
  - [Attributbasierte Auswahl des Instance-Typs für Amazon Fleet. EC2](#)
  - [Erstellen einer Auto-Scaling-Gruppe mit attributbasierter Auswahl des Instance-Typs](#)
- Skalierung: Skalieren Sie variable Workloads in kleinen Schritten.
- Verwendung mehrerer Einkaufsoptionen für Datenverarbeitung: Kombinieren Sie Instance-Flexibilität, Skalierbarkeit und Kosteneinsparungen mit mehreren Einkaufsoptionen für Datenverarbeitung.
  - [Amazon EC2 On-Demand-Instances](#) eignen sich am besten für neue, statusbehaftete und stark beanspruchte Workloads, bei denen Instance-Typ, Standort oder Zeit nicht flexibel sein können.

- [Amazon EC2 Spot-Instances](#) sind eine hervorragende Möglichkeit, die anderen Optionen für fehlertolerante und flexible Anwendungen zu ergänzen.
- Nutzen Sie [Compute Savings Plans](#) für stabile Workloads, die Flexibilität ermöglichen, wenn sich Ihre Anforderungen (wie AZ, Region, Instance-Familien oder Instance-Typen) ändern.
- Nutzung der Vielfalt von Instances und Availability Zones: Maximieren Sie die Anwendungsverfügbarkeit und nutzen Sie überschüssige Kapazitäten, indem Sie Ihre Instances und Availability Zones diversifizieren.
- Instances richtig dimensionieren: Verwenden Sie die Empfehlungen der AWS Tools zur richtigen Dimensionierung, um Anpassungen an Ihrer Arbeitslast vorzunehmen. Weitere Informationen finden Sie unter [Kostenoptimierung mit Empfehlungen zur richtigen Dimensionierung](#) und [Richtige Dimensionierung: Bereitstellen von Instances entsprechend den Workloads](#).
- Verwenden Sie Empfehlungen zur richtigen Dimensionierung in AWS Cost Explorer oder, um Möglichkeiten zur richtigen Dimensionierung [AWS Compute Optimizer](#) zu identifizieren.
- Aushandeln von Service Level Agreements (SLAs): Verhandeln Sie Vereinbarungen SLAs, die eine vorübergehende Reduzierung der Kapazität ermöglichen, während die Automatisierung Ersatzressourcen bereitstellt.

## Ressourcen

### Zugehörige Dokumente:

- [Optimieren Sie Ihre AWS Infrastruktur im Hinblick auf Nachhaltigkeit, Teil I: Datenverarbeitung](#)
- [Attributbasierte Instance-Typauswahl für Auto Scaling für Amazon Fleet EC2](#)
- [AWS Compute Optimizer Dokumentation](#)
- [Ausführen von Lambda: Leistungsoptimierung](#)
- [Dokumentation zu Auto Scaling](#)

### Zugehörige Videos:

- [AWS re:Invent 2023 — Was ist neu bei Amazon EC2](#)
- [AWS re:Invent 2023 — Intelligentes Sparen: Strategien zur Kostenoptimierung mit Amazon Elastic Compute Cloud](#)
- [AWS re:Invent 2022 — Optimierung von Amazon Elastic Kubernetes Service im Hinblick auf Leistung und Kosten AWS](#)

- [AWS re:Invent 2023 — Nachhaltiges Rechnen: Reduzierung von Kosten und CO2-Emissionen mit AWS](#)

SUS05-BP02 Verwenden Sie Instance-Typen mit den geringsten Auswirkungen

Überwachen und nutzen Sie kontinuierlich neue Instance-Typen, um Verbesserungen bei der Energieeffizienz zu nutzen.

Typische Anti-Muster:

- Sie verwenden lediglich eine Familie von Instances.
- Sie verwenden nur x86-Instances.
- Sie geben einen Instance-Typ in Ihrer Amazon EC2 Auto Scaling Scaling-Konfiguration an.
- Sie verwenden AWS Instances auf eine Weise, für die sie nicht konzipiert wurden (z. B. verwenden Sie rechenoptimierte Instances für eine speicherintensive Arbeitslast).
- Sie evaluieren nicht regelmäßig neue Instance-Typen.
- [Sie überprüfen nicht die Empfehlungen von AWS Rightsizing-Tools wie AWS Compute Optimizer](#)

Vorteile der Nutzung dieser bewährten Methode: Durch die Verwendung energieeffizienter und korrekt dimensionierter Instances können Sie die Umweltauswirkungen und die Kosten Ihrer Workloads deutlich reduzieren.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel

Implementierungsleitfaden

Die Verwendung effizienter Instances für Cloud-Workloads ist von entscheidender Bedeutung für eine geringere Ressourcennutzung und die Kosteneffizienz. Überwachen Sie kontinuierlich die Einführung neuer Instance-Typen und nutzen Sie Verbesserungen bei der Energieeffizienz, einschließlich Instance-Typen, die zur Unterstützung spezifischer Workloads bestimmt sind, wie z. B. Machine-Learning-Trainings und -Inferenzen und Videotranskodierung.

Implementierungsschritte

- Kennenlernen der Instance-Typen: Finden Sie Instance-Typen, mit denen Sie die Umweltbelastung Ihrer Workloads verringern können.
  - Abonnieren Sie [What's New with AWS, um auf dem](#) neuesten Stand der AWS Technologien und Instanzen zu bleiben up-to-date.

- Erfahren Sie mehr über verschiedene AWS Instance-Typen.
- [Erfahren Sie mehr über AWS Graviton-basierte Instances, die die beste Leistung pro Watt Energieverbrauch in Amazon bieten, EC2 indem Sie sich re:Invent 2020 — Deep Dive on AWS Graviton2 prozessorbetriebene Amazon-Instances und Deep Dive in Graviton3- und Amazon EC2 C7g-Instances ansehen. AWS EC2](#)
- Verwendung von Instance-Typen mit den geringsten Auswirkungen: Planen Sie Ihre Workload und stellen Sie sie auf Instance-Typen mit den geringsten Auswirkungen um.
  - Definieren Sie einen Prozess zur Evaluierung neuer Features oder Instances für Ihre Workloads. Nutzen Sie die Agilität in der Cloud, um schnell zu testen, wie neue Instance-Typen die ökologische Nachhaltigkeit Ihrer Workloads verbessern können. Nutzen Sie Proxy-Metriken, um zu messen, wie viele Ressourcen Sie für eine Arbeitseinheit benötigen.
  - Wenn möglich, passen Sie Ihren Workload so an, dass er mit einer unterschiedlichen Anzahl vCPUs und unterschiedlichen Speichermengen arbeitet, um den Instance-Typ Ihrer Wahl zu maximieren.
  - Erwägen Sie die Übertragung Ihrer Workload zu auf Graviton basierenden Instances, um die Leistungseffizienz Ihrer Workload zu verbessern. Weitere Informationen zum Verschieben von Workloads nach AWS Graviton finden Sie unter [AWS Graviton Fast Start](#) und [Überlegungen bei der Umstellung von Workloads auf AWS Graviton-basierte Amazon Elastic Compute Cloud-Instances](#).
  - [Erwägen Sie, bei der Nutzung von Managed Services die Option AWS Graviton auszuwählen.AWS](#)
  - Migrieren Sie Ihre Workload zu Regionen mit Instances, die die geringsten nachhaltigkeitsbezogenen Auswirkungen bieten und dennoch Ihre geschäftlichen Anforderungen erfüllen.
  - [Nutzen Sie für Machine-Learning-Workloads speziell für Ihre Workloads entwickelte Hardware wie AWS Trainium,AWS Inferentia und Amazon. EC2 DL1](#) AWS Inferentia-Instances wie Inf2-Instances bieten eine um bis zu 50% bessere Leistung pro Watt als vergleichbare Amazon-Instances. EC2
  - Verwenden Sie [Amazon SageMaker Inference Recommender](#), um den ML-Inferenzendpunkt richtig zu dimensionieren.
  - Verwenden Sie für Workloads, bei denen es gelegentlich zu zusätzlichen Kapazitätsanforderungen kommt, [Instances mit Spitzenlastleistung](#).

- Verwenden Sie [Amazon EC2 Spot-Instances](#) für zustandslose und fehlertolerante Workloads, um die Gesamtauslastung der Cloud zu erhöhen und die Auswirkungen ungenutzter Ressourcen auf die Nachhaltigkeit zu reduzieren.
- Betrieb und Optimierung: Betreiben und optimieren Sie Ihre Workload-Instance.
- Bei kurzlebigen Workloads sollten Sie die [CloudWatch Amazon-Instance-Kennzahlen](#) auswerten, CPUUtilization um festzustellen, ob die Instance inaktiv oder nicht ausgelastet ist.
- Für stabile Workloads sollten Sie die Tools zur AWS richtigen Dimensionierung überprüfen, z. B. [AWS Compute Optimizer](#) in regelmäßigen Abständen, um Möglichkeiten zur Optimierung und zur richtigen Größe der Instances zu ermitteln. Weitere Beispiele und Empfehlungen finden Sie in den folgenden Labs:
  - [Well-Architected Lab - Rightsizing Recommendations](#)
  - [Well-Architected Lab - Rightsizing with Compute Optimizer](#)
  - [Well-Architected Lab — Hardwaremuster optimieren und Nachhaltigkeit beobachten KPIs](#)

## Ressourcen

### Zugehörige Dokumente:

- [Optimieren Sie Ihre AWS Infrastruktur im Hinblick auf Nachhaltigkeit, Teil I: Datenverarbeitung](#)
- [AWS Graviton](#)
- [Amazon EC2 DL1](#)
- [Flotten für EC2 Kapazitätsreservierungen bei Amazon](#)
- [Amazon EC2 Spot-Flotte](#)
- [Funktionen: Lambda-Funktionskonfiguration](#)
- [Attributbasierte Instance-Typauswahl für Amazon Fleet EC2](#)
- [Building Sustainable, Efficient, and Cost-Optimized Applications on AWS](#)
- [How the Contino Sustainability Dashboard Helps Customers Optimize Their Carbon Footprint](#)

### Zugehörige Videos:

- [AWS re:Invent 2023 — AWS Graviton: Das beste Preis-Leistungs-Verhältnis für Ihre Workloads](#)  
[AWS](#)



- [AWS re:Invent 2023 — Neue generative KI-Funktionen von Amazon Elastic Compute Cloud in AWS Management Console](#)
- [AWS re:Invent 2023 = Was ist neu bei Amazon Elastic Compute Cloud](#)
- [AWS re:Invent 2023 — Intelligentes Sparen: Strategien zur Kostenoptimierung mit Amazon Elastic Compute Cloud](#)
- [AWS re:Invent 2021 — Tiefer Einblick in AWS Graviton3- und Amazon C7g-Instances EC2](#)
- [AWS re:Invent 2022 — Schaffen Sie eine kosten-, energie- und ressourceneffiziente Computerumgebung](#)

Zugehörige Beispiele:

- [Lösung: Leitfaden zur Optimierung von Deep-Learning-Workloads im Hinblick auf Nachhaltigkeit auf AWS](#)
- [Datenbankmigration von Amazon Relational Database Service zu Graviton](#)

SUS05-BP03 Managed Services nutzen

Verwenden Sie verwaltete Services für effizientere Betriebsabläufe in der Cloud.

Typische Anti-Muster:

- Sie verwenden EC2 Amazon-Instances mit geringer Auslastung, um Ihre Anwendungen auszuführen.
- Ihr internes Team verwaltet nur die Workload, ohne Zeit zu haben, sich auf Innovation oder Vereinfachungen zu konzentrieren.
- Sie nutzen und verwalten Technologien für Aufgaben, die effizienter auf verwalteten Services ausgeführt werden können.

Vorteile der Nutzung dieser bewährten Methode:

- Durch den Einsatz von Managed Services verlagert sich die Verantwortung auf das Unternehmen AWS, das Einblicke in Millionen von Kunden hat, die dazu beitragen können, neue Innovationen und Effizienzsteigerungen voranzutreiben.
- Ein verwalteter Service verteilt die Umweltauswirkungen des Services durch Multi-Tenet-Steuerebenen auf mehrere Benutzer.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel

## Implementierungsleitfaden

Mit Managed Services verlagert sich die AWS Verantwortung auf die Aufrechterhaltung einer hohen Auslastung und die Optimierung der Nachhaltigkeit der eingesetzten Hardware. Verwaltete Services eliminieren dazu den betrieblichen und administrativen Aufwand für die Wartung eines Service, sodass Ihr Team mehr Zeit hat und sich auf Innovationen konzentrieren kann.

Überprüfen Sie Ihren Workload, um die Komponenten zu identifizieren, die durch AWS Managed Services ersetzt werden können. [AmazonRDS](#), [Amazon Redshift](#) und [Amazon ElastiCache](#) bieten beispielsweise einen verwalteten Datenbankservice an. [Amazon Athena](#)EMR, [Amazon](#) und [Amazon OpenSearch Service](#) bieten einen verwalteten Analysedienst.

## Implementierungsschritte

1. Inventarisieren Ihrer Workload: Inventarisieren Sie Ihre Workload für Services und Komponenten.
2. Identifizieren von Kandidaten: Bewerten und identifizieren Sie Komponenten, die durch verwaltete Services ersetzt werden können. Hier finden Sie einige Beispiele für Situationen, in denen Sie einen verwalteten Service in Erwägung ziehen sollten:

Aufgabe	Wofür soll ich es verwenden AWS
Hosten einer Datenbank	Verwenden Sie verwaltete <a href="#">Amazon Relational Database Service (AmazonRDS)</a> -Instances, anstatt Ihre eigenen RDS Amazon-Instances auf <a href="#">Amazon Elastic Compute Cloud (AmazonEC2)</a> zu verwalten.
Hosten einer Container-Workload	Verwenden Sie <a href="#">AWS Fargate</a> , anstatt Ihre eigene Container-Infrastruktur zu implementieren.
Hosten von Web-Apps	Verwenden Sie <a href="#">AWS Amplify Hosting</a> als vollständig verwalteten CI/CD- und Hosting-Service für statische Websites und serverseitig gerenderte Web-Apps.

3. Erstellen eines Migrationsplans: Identifizieren Sie Abhängigkeiten und erstellen Sie einen Migrationsplan. Aktualisieren Sie Runbooks und Playbooks entsprechend.
  - Der [AWS Application Discovery Service](#) erfasst und präsentiert automatisch detaillierte Informationen über Anwendungsabhängigkeiten und die Nutzung von Anwendungen. Damit treffen Sie bei der Planung Ihrer Migration fundiertere Entscheidungen.
4. Tests: Testen Sie den Service vor der Migration zum verwalteten Service.
5. Ersetzen selbst gehosteter Services: Verwenden Sie Ihren Migrationsplan, um selbst gehostete Services durch verwaltete Services zu ersetzen.
6. Überwachen und anpassen: Überwachen Sie den Service nach der Migration kontinuierlich, um erforderliche Anpassungen vorzunehmen und den Service zu optimieren.

## Ressourcen

### Zugehörige Dokumente:

- [AWS Cloud Produkte](#)
- [AWS Rechner für die Gesamtbetriebskosten \(TCO\)](#)
- [Amazon DocumentDB](#)
- [Amazon Elastic Kubernetes Service \(EKS\)](#)
- [Von Amazon Managed Streaming for Apache Kafka \(AmazonMSK\)](#)

### Zugehörige Videos:

- [AWS re:Invent 2021 — Cloud-Betrieb im großen Maßstab mit AWS Managed Services](#)
- [AWS re:Invent 2023 — Bewährte Methoden für den Betrieb auf AWS](#)

## SUS05-BP04 Optimieren Sie Ihren Einsatz von hardwarebasierten Rechenbeschleunigern

Sie können die Nutzung von beschleunigten Computing-Instances optimieren, um die Anforderungen Ihrer Workload an die physische Infrastruktur zu reduzieren.

### Typische Anti-Muster:

- Sie überwachen die Nutzung nicht. GPU
- Sie verwenden eine Allzweck-Instance für die Workload, während eine speziell erstellte Instance eine höhere Leistung, geringere Kosten und eine bessere Leistung pro Watt bieten kann.

- Sie verwenden hardwarebasierte Rechenbeschleuniger für Aufgaben, bei denen sie mit CPU-basierten Alternativen effizienter sind.

Vorteile der Nutzung dieser bewährten Methode: Durch den optimalen Einsatz hardwarebasierter Beschleuniger können Sie die Anforderungen an die physische Infrastruktur Ihrer Workload reduzieren.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel

### Implementierungsleitfaden

Wenn Sie eine hohe Verarbeitungskapazität benötigen, können Sie von beschleunigten Recheninstanzen profitieren, die Zugriff auf hardwarebasierte Rechenbeschleuniger wie Grafikprozessoren (GPUs) und feldprogrammierbare Gate-Arrays (FPGAs) bieten. Diese Hardwarebeschleuniger führen bestimmte Funktionen wie Grafikverarbeitung oder Datenmusterabgleich effizienter aus als CPU-basierte Alternativen. Viele beschleunigte Workloads, wie Rendering, Transkodierung und Machine Learning, sind sehr variabel im Bezug auf die Ressourcennutzung. Betreiben Sie diese Hardware nur so lange wie nötig und nehmen Sie sie automatisch außer Betrieb, wenn sie nicht mehr benötigt wird, um den Ressourcenverbrauch zu minimieren.

### Implementierungsschritte

- Ermitteln Sie, welche [beschleunigten Computing-Instances](#) für Ihre Anforderungen geeignet sind.
- [Nutzen Sie für Machine-Learning-Workloads speziell für Ihren Workload entwickelte Hardware wie AWS Trainium, AWS Inferentia und Amazon. EC2 DL1](#) AWS Inferentia-Instances wie Inf2-Instances bieten eine um bis zu [50% bessere Leistung pro Watt als vergleichbare](#) Amazon-Instances. EC2
- Erfassen Sie Nutzungsmetriken für Ihre beschleunigten Computing-Instances. Sie können den CloudWatch Agenten beispielsweise verwenden, um Metriken wie `utilization_gpu` und `utilization_memory` für Sie zu sammeln, GPUs wie in [NVIDIA GPUMetriken mit Amazon sammeln](#) gezeigt CloudWatch.
- Optimieren Sie Code, Netzwerkbetrieb und die Einstellungen von Hardwarebeschleunigern, um sicherzustellen, dass die zugrunde liegende Hardware optimal genutzt wird.
  - [GPU-Einstellungen optimieren](#)
  - [GPU-Überwachung und Optimierung im Deep Learning AMI](#)
  - [I/O-Optimierung für die GPU Leistungsoptimierung von Deep-Learning-Trainings in Amazon SageMaker](#)

- Verwenden Sie die neuesten Hochleistungsbibliotheken und GPU Treiber.
- Verwenden Sie Automatisierung, um GPU Instanzen freizugeben, wenn sie nicht verwendet werden.

## Ressourcen

### Zugehörige Dokumente:

- [Beschleunigte Datenverarbeitung](#)
- [Let's Architect! Architecting with custom chips and accelerators](#)
- [Wie wähle ich den passenden EC2 Amazon-Instance-Typ für meinen Workload aus?](#)
- [EC2VT1Amazon-Instances](#)
- [Wählen Sie mit Amazon den besten KI-Beschleuniger und die beste Modellkompilierung für Computer-Vision-Inferenz SageMaker](#)

### Zugehörige Videos:

- [AWS re:Invent 2021 — So wählen Sie EC2 GPU Amazon-Instances für Deep Learning aus](#)
- [AWS Online-Technikgespräche — Bereitstellung kostengünstiger Deep-Learning-Inferenz](#)
- [AWS re:Invent 2023 — Modernste KI mit und AWS NVIDIA](#)
- [AWS re:Invent 2022 - \[!\] NEW LAUNCH Einführung in AWS Inferentia2-basierte Amazon Inf2-Instances EC2](#)
- [AWS re:Invent 2022 — Beschleunigen Sie Deep Learning und innovieren Sie schneller mit AWS Trainium](#)
- [AWS re:Invent 2022 — Deep Learning weiter AWS mit: Von der Schulung bis zur Implementierung NVIDIA](#)

## Prozess und Kultur

### Frage

- [SUS6 Wie unterstützen Ihre organisatorischen Prozesse Ihre Nachhaltigkeitsziele?](#)

## SUS6 Wie unterstützen Ihre organisatorischen Prozesse Ihre Nachhaltigkeitsziele?

Reduzieren Sie nachhaltigkeitsbezogene Auswirkungen, indem Sie Ihre Entwicklungs-, Test- und Bereitstellungsmethoden ändern.

### Bewährte Methoden

- [SUS06-BP01 Wenden Sie Methoden an, mit denen schnell Verbesserungen der Nachhaltigkeit eingeführt werden können](#)
- [SUS06-BP02 Behalten Sie Ihr Arbeitspensum up-to-date](#)
- [SUS06-BP03 Steigern Sie die Nutzung von Build-Umgebungen](#)
- [SUS06-BP04 Verwaltete Gerätefarmen zum Testen verwenden](#)

SUS06-BP01 Wenden Sie Methoden an, mit denen schnell Verbesserungen der Nachhaltigkeit eingeführt werden können

Nutzen Sie Methoden und Prozesse zur Validierung potenzieller Verbesserung, zur Minimierung von Testkosten und zur Bereitstellung kleinerer Verbesserungen.

### Typische Anti-Muster:

- Die Prüfung Ihrer Anwendung auf Nachhaltigkeitsaspekte erfolgt nur einmal zu Beginn des Projekts.
- Ihre Workload stagniert, da der Freigabeprozess zu komplex ist, um kleinere Verbesserungen für die Ressourceneffizienz umzusetzen.
- Sie verfügen über keine Mechanismen zur Verbesserung Ihrer Workload unter Nachhaltigkeitsaspekten.

Vorteile der Nutzung dieser bewährten Methode: Durch die Einrichtung eines Prozesses für die Einführung und Nachverfolgung von Nachhaltigkeitsverbesserungen können Sie kontinuierlich neue Funktionen einführen, Probleme beseitigen und die Workload-Effizienz verbessern.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Mittel

### Implementierungsleitfaden

Testen und validieren Sie potenzielle Verbesserungen in Bezug auf die Nachhaltigkeit, bevor Sie sie in der Produktion bereitstellen. Berücksichtigen Sie die Testkosten bei der Berechnung des

potenziellen zukünftigen Nutzens einer Verbesserung. Entwickeln Sie kostengünstige Testmethoden, um kleinere Verbesserungen einzuführen.

### Implementierungsschritte

- Kenntnis und Kommunikation der Nachhaltigkeitsziele Ihrer Organisation: Machen Sie sich mit den Nachhaltigkeitszielen Ihrer Organisation vertraut, z. B. zur Reduzierung der CO<sub>2</sub>-Emissionen oder zum verantwortungsvollen Umgang mit Wasser. Übersetzen Sie diese Ziele in Nachhaltigkeitsanforderungen für Ihre Cloud-Workloads. Kommunizieren Sie diese Anforderungen an wichtige Stakeholder.
- Ergänzung des Backlogs mit Nachhaltigkeitsanforderungen: Fügen Sie Ihrem Entwicklungs-Backlog Anforderungen zur Verbesserung der Nachhaltigkeit hinzu.
- Iterieren und verbessern: Verwenden Sie einen [iterativen Verbesserungsprozess](#), um diese Verbesserungen zu identifizieren, zu bewerten, zu priorisieren, zu testen und bereitzustellen.
- Prüfung mit einem Produkt, das am wenigsten lebensfähig ist (MVP): Entwicklung und Erprobung potenzieller Verbesserungen unter Verwendung der repräsentativen Komponenten, um die Kosten und die Umweltbelastung durch Tests zu reduzieren.
- Verbessern und optimieren Sie Ihre Entwicklungsprozesse kontinuierlich. Sie können beispielsweise Ihren Softwarebereitstellungsprozess mit Pipelines für die Continuous Integration und Continuous Delivery (CI/CD) automatisieren, um potenzielle Verbesserungen zu testen und bereitzustellen und so den Aufwand zu reduzieren und Fehler durch manuelle Prozesse zu minimieren.
- Schulung und Sensibilisierung: Führen Sie Schulungsprogramme für Ihre Teammitglieder durch, um sie über Nachhaltigkeit und die Auswirkungen ihrer Aktivitäten auf die Nachhaltigkeitsziele Ihrer Organisation aufzuklären.
- Bewerten und anpassen: Bewerten Sie kontinuierlich die Auswirkungen von Verbesserungen und nehmen Sie bei Bedarf Anpassungen vor.

### Ressourcen

#### Zugehörige Dokumente:

- [AWS ermöglicht Nachhaltigkeitslösungen](#)
- [Skalierbare agile Entwicklungspraktiken auf der Grundlage von AWS CodeCommit](#)

#### Zugehörige Videos:

- [AWS re:INVENT 2023 — Nachhaltige Architektur: Vergangenheit, Gegenwart und future](#)
- [AWS re:Invent 2022 — Bereitstellung nachhaltiger, leistungsstarker Architekturen](#)
- [AWS re:Invent 2022 — Nachhaltige Architektur und Reduzierung Ihres CO2-Fußabdrucks AWS](#)
- [AWS re:Invent 2022 — Nachhaltigkeit in der globalen Infrastruktur AWS](#)
- [AWS re:Invent 2023 — Was ist neu im Bereich Observability und Operations AWS](#)

Zugehörige Beispiele:

- [Well-Architected Lab – Kosten- und Nutzungsberichte in Effizienzberichte umwandeln](#)

SUS06-BP02 Behalten Sie Ihr Arbeitspensum up-to-date

Behalten Sie Ihren Workload bei, up-to-date um effiziente Funktionen einzuführen, Probleme zu beheben und die Gesamteffizienz Ihres Workloads zu verbessern.

Typische Anti-Muster:

- Sie gehen davon aus, dass Ihre aktuelle Architektur statisch ist und im Laufe der Zeit nicht aktualisiert wird.
- Sie haben keine Systeme oder regelmäßigen Besprechungen zur Prüfung, ob aktualisierte Software und Pakete mit Ihrer Workload kompatibel sind.

Vorteile der Nutzung dieser bewährten Methode: Wenn Sie einen Prozess einrichten, um Ihre Workload auf neustem Stand zu halten, können Sie neue Features und Kapazitäten nutzen, Probleme lösen und die Workload-Effizienz verbessern.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Niedrig

Implementierungsleitfaden

Aktuelle Betriebssysteme, Laufzeiten, Middleware, Bibliotheken und Anwendungen können die Workload-Effizienz verbessern und die Nutzung effizienterer Technologien unterstützen. Aktuelle Software kann darüber hinaus Features für eine genauere Messung der Auswirkungen Ihrer Workload bereitstellen, da die Anbieter mit ihren Features ebenfalls Nachhaltigkeitsziele erfüllen müssen. Sorgen Sie für Regelmäßigkeit bei der Aktualisierung Ihrer Workload mit den neuesten Features und Versionen.

Implementierungsschritte



- Definieren eines Prozesses: Definieren Sie einen Prozess und einen Zeitplan, um neue Features oder Instances für Ihre Workloads zu evaluieren. Nutzen Sie die Agilität in der Cloud, um schnell zu testen, wie neue Features Ihre Workloads verbessern können:
  - Reduzierung von Auswirkungen auf die Nachhaltigkeit
  - Erzielen von Leistungseffizienzen
  - Beseitigen von Hindernissen für geplante Verbesserungen
  - Verbesserung Ihrer Fähigkeit für die Messung von und den Umgang mit Nachhaltigkeitsauswirkungen
- Inventarisierung: Inventarisieren Sie Ihre Workload-Software und -Architektur und identifizieren Sie Komponenten, die aktualisiert werden müssen.
  - Sie können [AWS Systems Manager Inventory](#) verwenden, um Betriebssystem- (OS), Anwendungs- und Instance-Metadaten von Ihren EC2 Amazon-Instances zu sammeln und so schnell zu verstehen, auf welchen Instances die Software und die Konfigurationen ausgeführt werden, die gemäß Ihrer Softwarerichtlinie erforderlich sind, und welche Instances aktualisiert werden müssen.
- Kennenlernen des Aktualisierungsverfahrens: Erfahren Sie, wie die Komponenten Ihrer Workload aktualisiert werden.

Workload-Komponente	Aktualisierung
Machine Images	Verwenden Sie <a href="#">EC2Image Builder</a> , um Updates für <a href="#">Amazon Machine Images (AMIs)</a> für Linux- oder Windows-Server-Images zu verwalten.
Container-Images	Verwenden Sie <a href="#">Amazon Elastic Container Registry (Amazon ECR)</a> mit Ihrer bestehenden Pipeline, um <a href="#">Amazon Elastic Container Service (Amazon ECS) -Images zu verwalten</a> .
AWS Lambda	AWS Lambda beinhaltet <a href="#">Funktionen zur Versionsverwaltung</a> .

- Verwendung von Automatisierung: Verwenden Sie Automatisierung für den Aktualisierungsvorgang, um den Aufwand für die Bereitstellung neuer Features zu reduzieren und Fehler zu begrenzen, die durch manuelle Prozesse verursacht werden.

- Sie können [CI/CD](#) verwenden AMIs, um Container-Images und andere Artefakte im Zusammenhang mit Ihrer Cloud-Anwendung automatisch zu aktualisieren.
- Sie können Tools wie den [AWS Systems Manager Patch Manager](#) verwenden, um den Systemaktualisierungsprozess zu automatisieren und die Aktivitäten mit [AWS Systems Manager Maintenance Windows](#) zu planen.

## Ressourcen

### Zugehörige Dokumente:

- [AWS Zentrum für Architektur](#)
- [Was ist neu bei AWS](#)
- [AWS Entwickler-Tools](#)

### Zugehörige Videos:

- [AWS re:Invent 2022 — Optimieren Sie Ihre AWS Workloads mit Best-Practice-Anleitungen](#)
- [All Things Patch: AWS Systems Manager](#)

### Zugehörige Beispiele:

- [Well-Architected Labs: Bestands- und Patch-Verwaltung](#)
- [Labor: AWS Systems Manager](#)

## SUS06-BP03 Steigern Sie die Nutzung von Build-Umgebungen

Erhöhen Sie die Ausnutzung von Ressourcen zum Entwickeln, Testen und Erstellen Ihrer Workloads.

### Typische Anti-Muster:

- Sie stellen Ihre Build-Umgebungen manuell bereit oder beenden sie manuell.
- Sie lassen Ihre Build-Umgebungen unabhängig von Test-, Build- oder Freigabeaktivitäten laufen (dazu gehört etwa der Betrieb einer Umgebung außerhalb der Arbeitszeit der Mitglieder Ihres Entwicklungsteams).
- Sie stellen übermäßig viele Ressourcen für Ihre Build-Umgebung bereit.

Vorteile der Nutzung dieser bewährten Methode: Durch die Steigerung der Ausnutzung von Build-Umgebungen können Sie die allgemeine Effizienz Ihrer Cloud-Workload verbessern, da die Ressourcen in effizienter Weise Entwicklungs-, Test- und Build-Aktivitäten zugewiesen werden.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Niedrig

### Implementierungsleitfaden

Nutzen Sie Automatisierung infrastructure-as-code, um Build-Umgebungen bei Bedarf hochzufahren und herunterzufahren, wenn sie nicht genutzt werden. Eine typische Vorgehensweise besteht in der Planung von Verfügbarkeitszeiten, die mit den Arbeitszeiten der Entwicklungsteams übereinstimmen. Ihre Testumgebungen sollten der Produktionskonfiguration sehr stark ähneln. Suchen Sie jedoch nach Möglichkeiten, Instance-Typen mit Burst-Kapazität, Amazon EC2 Spot-Instances, automatisch skalierende Datenbankdienste, Container und serverlose Technologien zu verwenden, um die Entwicklungs- und Testkapazität an die Nutzung anzupassen. Begrenzen Sie das Datenvolumen auf die Testanforderungen. Wenn Sie Produktionsdaten für einen Test verwenden, sollten Sie nach Möglichkeiten suchen, Daten aus der Produktion gemeinsam zu nutzen, anstatt Daten hin- und herzuschieben.

### Implementierungsschritte

- Infrastructure as Code verwenden: Verwenden Sie Infrastructure as Code, um Ihre Entwicklungsumgebungen bereitzustellen.
- Automatisierung verwenden: Nutzen Sie Automatisierungen, um den Lebenszyklus Ihrer Entwicklungs- und Testumgebungen zu verwalten und die Effizienz Ihrer Entwicklungsressourcen zu maximieren.
- Nutzung maximieren: Verwenden Sie Strategien zur Maximierung der Nutzung von Entwicklungs- und Testumgebungen.
  - Verwenden Sie die geringstmögliche Zahl repräsentativer Umgebungen, um mögliche Verbesserungen zu entwickeln und zu testen.
  - Nutzen Sie nach Möglichkeit Serverless-Technologien.
  - Verwenden Sie On-Demand-Instances, um Entwicklergeräte zu ergänzen.
  - Verwenden Sie Instance-Typen mit Burst-Kapazität, Spot Instances und andere Technologien, um die Entwicklungskapazität an der Nutzung auszurichten.
  - Nutzen Sie native Cloud-Services für den sicheren Instance-Shell-Zugriff, statt Bastion-Host-Flotten bereitzustellen.
  - Skalieren Sie Ihre Build-Ressourcen automatisch je nach Build-Aktivität.

## Ressourcen

### Zugehörige Dokumente:

- [AWS Systems Manager Sitzungsmanager](#)
- [EC2Leistungsinstanzen von Amazon Burstable](#)
- [Was ist AWS CloudFormation?](#)
- [Was ist AWS CodeBuild?](#)
- [Instance Scheduler aktiviert AWS](#)

### Zugehörige Videos:

- [AWS re:Invent 2023 — Kontinuierliche Integration und Bereitstellung für AWS](#)

## SUS06-BP04 Verwaltete Gerätefarmen zum Testen verwenden

Verwenden Sie verwaltete Gerätefarmen zum effektiven Testen neuer Features auf einer repräsentativen Auswahl von Hardwaregeräten.

### Typische Anti-Muster:

- Sie testen Ihre Anwendung manuell und stellen sie auf einzelnen physischen Geräten bereit.
- Sie verwenden keinen App-Testservice zum Testen und zum Interagieren mit Ihren Apps (beispielsweise Android, iOS und Web-Apps) auf realen physischen Geräten.

Vorteile der Nutzung dieser bewährten Methode: Die Verwendung verwalteter Gerätefarmen zum Testen cloud-fähiger Anwendungen bringt eine Reihe von Vorteilen mit sich:

- Dazu gehören effizientere Features zum Testen von Anwendungen auf einer breiten Palette von Geräten.
- Sie machen hausinterne Infrastruktur zum Testen überflüssig.
- Sie bieten unterschiedliche Gerätetypen, darunter ältere und weniger verbreitete Hardware, was unnötige Geräte-Upgrades eliminiert.

Risikostufe, wenn diese bewährte Methode nicht eingeführt wird: Niedrig

## Implementierungsleitfaden

Die Verwendung verwalteter Gerätefarmen kann Ihnen dabei helfen, Ihre Testprozesse für neue Features auf einer repräsentativen Auswahl von Hardwaregeräten zu optimieren. Verwaltete Gerätefarmen stellen verschiedene Gerätetypen bereit, unterstützen auch ältere und weniger verbreitete Hardware und vermeiden nachhaltigkeitsbezogene Auswirkungen auf Kunden durch unnötige Geräte-Upgrades.

### Implementierungsschritte

- Testanforderungen definieren: Definieren Sie Ihre Testanforderungen und Ihren Testplan (z. B. Testtyp, Betriebssysteme und Testzeitplan).
  - Sie können [Amazon](#) CloudWatch RUM, um Daten auf Kundenseite zu sammeln und zu analysieren und Ihren Testplan zu gestalten.
- Verwaltete Gerätefarm auswählen: Wählen Sie eine verwaltete Gerätefarm, die Ihre Testanforderungen unterstützen kann. Sie können beispielsweise die [AWS -Gerätefarm](#) verwenden, um die Auswirkungen Ihrer Änderungen auf eine repräsentative Auswahl von Hardwaregeräten zu testen und zu verstehen.
- Automatisierung verwenden: Verwenden Sie Automatisierung und kontinuierliche Integration/ Bereitstellung (CI/CD) für die Planung und Durchführung Ihrer Tests.
  - [Integration von AWS Device Farm in Ihre CI/CD-Pipeline zur Ausführung browserübergreifender Selenium-Tests](#)
  - [iOS- und iPad Betriebssystem-Apps mit mobilen Diensten AWS DevOps erstellen und testen](#)
- Prüfen und Anpassen: Prüfen Sie kontinuierlich Ihre Testergebnisse und nehmen Sie die erforderlichen Verbesserungen vor.

### Ressourcen

#### Zugehörige Dokumente:

- [AWS Device Farm Geräteliste](#)
- [Das CloudWatch RUM Dashboard anzeigen](#)

#### Zugehörige Videos:

- [AWS re:Invent 2023 — Verbessern Sie die Qualität Ihrer Mobil- und Web-Apps mit Device Farm AWS](#)

- [AWS re:Invent 2021 — Optimieren Sie Anwendungen mithilfe von Erkenntnissen für Endbenutzer mit Amazon CloudWatch RUM](#)

Zugehörige Beispiele:

- [AWS Device Farm Beispiel-App für Android](#)
- [AWS Device Farm Beispiel-App für iOS](#)
- [Appium Webtests für AWS Device Farm](#)

# Hinweise

Kunden sind dafür verantwortlich, Ihre eigene unabhängige Bewertung der Informationen in diesem Dokument vorzunehmen. Dieses Dokument: (a) dient nur zu Informationszwecken, (b) stellt aktuelle AWS Produktangebote und Praktiken dar, die ohne vorherige Ankündigung geändert werden können, und (c) stellt keine Verpflichtungen oder Zusicherungen von AWS und seinen verbundenen Unternehmen, Lieferanten oder Lizenzgebern dar. AWS Produkte oder Dienstleistungen werden „wie sie sind“ ohne ausdrückliche oder stillschweigende Garantien, Zusicherungen oder Bedingungen jeglicher Art bereitgestellt. Die Verantwortlichkeiten und Verbindlichkeiten AWS gegenüber seinen Kunden werden durch AWS Vereinbarungen geregelt, und dieses Dokument ist weder Teil einer Vereinbarung zwischen AWS und seinen Kunden noch ändert es diese.

Copyright © 2023 Amazon Web Services, Inc. bzw. Tochtergesellschaften des Unternehmens.

# AWS Glossar

Die neueste AWS Terminologie finden Sie im [AWS Glossar](#) in der AWS-Glossar Referenz.



Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.