Bericht

**Public Cloud Services HS23**

Dozent: Sebastian Graf

Studenten: Fabian Heuberger  
Etienne Frei  
Yannick Hohler

CI Pipeline on AWS

Ein Bild, das Rad, orange enthält.

Automatisch generierte Beschreibung

Inhaltsverzeichnis

[Use Case 3](#_Toc155608621)

[Architektur 4](#_Toc155608622)

[Umsetzung 5](#_Toc155608623)

[IaC 5](#_Toc155608624)

[AWS CodePipeline 5](#_Toc155608625)

[AWS S3 6](#_Toc155608626)

[AWS CodeBuild 6](#_Toc155608627)

[Amazon EventBridge 7](#_Toc155608628)

[AWS Lambda 7](#_Toc155608629)

[Erkenntnisse 9](#_Toc155608630)

[Fazit 9](#_Toc155608631)

# Use Case

In diesem Projekt dient GitHub als Repository für die Codebase. Das Deployment soll auf AWS realisiert werden.

Damit Änderungen getestet und direkt deployed werden soll eine CI/CD-Pipeline in integriert sein. Mit GitHub Actions könnte eine solche Pipeline umgesetzt werden, jedoch ist die Auslastung der von GitHub bereitgestellten Runner begrenzt und diese müssten bei einem grösseren Projekt mit vielen Änderungen durch einen eigenen Runner ersetzt werden. Einen eigenen Runner könnte durch eine EC2 Instanz bereitgestellt werden.

Um die Pipeline an einem zentralen Ort zu haben, soll die ganze Pipeline direkt in AWS umgesetzt werden. Dies führt zu einer besseren Kontrolle des gesamten Prozesses und führt zu einer nahtlosen Verbindung zu anderen AWS Services. Das Monitoring und Logging wird dadurch auch erleichtert.

# Architektur

Verargumentieren der Entscheidung anhand der gelernten Prinzipien

Ein Bild, das Text, Screenshot, Diagramm, Schrift enthält.

Automatisch generierte Beschreibung

Abbildung 1 Gesamte Architektur

* GitHub dient als Repository für die Codebase.
* CodePipeline orchestriert die Ausführung des Stages und dient als zentrales Element dieses Systems.
* CodeBuild welches von CodePipeline verwaltet wird erstellt die Artefakte der Applikation und speichert diese in einem S3 Bucket.
* Der SNS Dienst benachrichtigt per E-Mail über den Zustand von CodePipeline
* EventBridge beobachtet die Ereignisse welche von der CodePipeline generiert werden und leitet diese weiter.
* Lambda erstellt eine Rückmeldung auf GitHub basierend auf Ergebnissen der CodePipeline

# Umsetzung

In diesem Kapitel wird beschrieben wie die einzelne Services konfiguriert wurden und wie unser Service Stack erstellt wurde.

## IaC

Als Erstes haben wir versucht, Terraform als IaC-Tool zu verwenden. Es hat sich jedoch herausgestellt, dass es Funktionen gibt, die noch nicht unterstützt werden (Bug: [[Bug]: aws\_codebuild\_project queued\_timeout unsupported value when using lambda compute · Issue #34376 · hashicorp/terraform-provider-aws (github.com)](https://github.com/hashicorp/terraform-provider-aws/issues/34376)). Beim CodeBuild-Service haben wir AWS Lambda als "Compute Mode" gewählt. Dieser Modus unterstützt das Attribut "queued\_timeout" nicht. Beim Erstellen der Services wird ein Standardwert festgelegt, obwohl im Terraform-Template nichts definiert ist, was beim Bereitstellen der Services einen Fehler wirft.

Daher haben wir uns entschieden, AWS CloudFormation zu verwenden, um unsere Services zu erstellen. CloudFormation bietet folgende Vorteile:

* Es bietet eine tiefere Integration mit anderen AWS-Services und -Funktionen
* Die Syntax ist deklarativ, was bedeutet, dass Sie Ihre gewünschte Infrastruktur konfigurieren
* CloudFormation bietet eine grafische Benutzeroberfläche namens AWS CloudFormation Designer

## AWS CodePipeline

AWS CodePipeline ist ein Continuous-Delivery-Service, der zur Automatisierung von Software-Release-Prozessen eingesetzt wird. Unsere Pipeline besteht aus 3 Phasen:

* Source
* Build
* Deploy

Source Phase:

In dieser Phase greift der Pipeline-Prozess auf den neuesten Commit über eine Codestar-Verbindung, zieht die relevanten Dateien und speichert sie in die Artefakten-Bucket.

Build Phase:

Die Build-Phase holt sich die Artefakte aus dem Artefakten-Bucket und buildet das Projekt gemäss den in der Buildspec-Datei im Projekt-Repository spezifizierten Anweisungen. Dieser Prozess resultiert in der Erstellung eines Release-Dist-Verzeichnisses. Das generierte Release wird als ZIP-Datei im Artefakten-Bucket abgelegt.

Deploy Phase:

In der Deployment-Phase wird das erstellte Release-ZIP aus dem Artefakten-Bucket abgerufen. Dieses ZIP wird entpackt, und die enthaltenen Dateien werden als statische Website im Website-Bucket bereitgestellt. Die Webseite ist unter folgender URL erreichbar: <http://pipeline-stack-websitebucket-q4j5omdxwwn5.s3-website-eu-west-1.amazonaws.com>

Durch diese Release Pipeline wird sichergestellt, dass jede Änderung im Quellcode erfolgreich gebaut, veröffentlicht und bereitgestellt wird, wodurch ein effizienter Development- und Delivery-Prozess gewährleistet wird.

## AWS S3

In unserem CodePipeline Projekt wurden folgende 3 S3 Buckets erstellt und verwendet:

* WebsiteBucket: ein öffentlicher Bucket für das deployen einer statischen Webseite: <http://pipeline-stack-websitebucket-q4j5omdxwwn5.s3-website-eu-west-1.amazonaws.com>
* ArtifactBucket: der Bucket wird verwendet um alle Source und Build Artefakte zu speichern.
* LambdaSourceBucket: in diesem Bucket ist der Quellcode der Lambda Funktion angelegt.

## AWS CodeBuild

AWS CodeBuild wurde für die Build Phase verwendet. Für das CodeBuild Project haben wir statt einer EC2 Instanz AWS Lambda für das Ausführen unsere Builds verwendet. AWS Lambda ermöglicht schnellere Builds aufgrund einer geringeren Startlatenz. AWS Lambda skaliert auch automatisch, sodass Builds nicht in der Warteschlange warten, bis sie ausgeführt werden.

Der Build wird durch die Buildspec Datei im Angular Projekt definiert:

Buildspec.yaml:

A screen shot of a computer program

Description automatically generated

## Amazon EventBridge

Einen EventBridge ist ein zentraler Ereignisbus in der Ereignisse erfasst und weitergeleitet werden. Grundsätzlich besitzt jeder AWS Account eine Standard EventBridge. Auf dieser EventBridge können Regeln definiert werden die besagen welche Ereignisse an welche Services weitergeleitet werden. EventBridge ist serverlos und skalierbar. Folgendes Ereignismuster löst die Regel aus: Ein Bild, das Text, Screenshot, Schrift, Reihe enthält.

Automatisch generierte Beschreibung

Abbildung 2 Ereignismuster welches die definierte Regel auslöst

Sobald ein solches Ereignis aus der CodePipeline in EventBridge erscheint, wird die in der Regel verknüpfte Lambda Funktion damit aufgerufen. Wir haben uns entschieden die Zustände «suceeded» und «failed» der drei Phasen der CodePipeline für diese Case Study zu verarbeiten.

## AWS Lambda

Um direkt auf GitHub eine Rückmeldung zu generieren haben wir eine Lambda Funktion erstellt. Diese Funktion erstellt einen Kommentar unter dem Commit welche die Pipeline durchlaufen hat.   
Wie im Kapitel Amazon EventBridge beschrieben wird die Funktion durch ein Ereignis der CodePipeline ausgelöst welche von der Eventbridge weitergeleitet wird wie in Abbildung 2 dargestellt wird.

Ein Bild, das Text, Screenshot, Schrift, Reihe enthält.

Automatisch generierte Beschreibung

Abbildung 3 Verknüpfung zwischen EventBridge und Lambda Funktion

Die Lambda Funktion haben wir in JavaScript geschrieben und ist als Zip-Datei in einem S3-Bucket abgelegt. Benötigte Abhängigkeiten mussten innerhalb des Ordners installiert werden.

Folgendes Ereignis wird von der Lambda Funktion empfangen:   
Ein Bild, das Text, Screenshot, Schrift, Dokument enthält.

Automatisch generierte Beschreibung

Dieses Ereignis enthält jedoch nicht den Hash des Commits. Dies kann mit der AWS-SDK Bibliothek umgesetzt werden indem eine CodePipeline-Instanz erstellt wird und mit den Parametern wie Name und Execution-Id weitere Details abgerufen werden können:

Ein Bild, das Text, Schrift, Reihe, Screenshot enthält.

Automatisch generierte Beschreibung

Abbildung 4 Extrahieren von Details einer CodePipeline Ausführung mit AWS-SDK

Mit dem Hash des Commits kann nun über die GitHub-API der Commit erfasst und der Kommentar erstellt werden.

Ein Bild, das Text, Screenshot, Schrift, Zahl enthält.

Automatisch generierte Beschreibung

Abbildung 5 Erstellung des Kommentar unter spezifischem Commit

Damit die Lambda Funktion die Berechtigungen besitzt Kommentare im jeweiligen Repository zu schreiben wurde ein Access Token eines der Accounts benötigt. Somit werden die Kommentare im Namen eines Contributors geschrieben.

# Erkenntnisse & Fazit