Sicherheits- und Betriebsleitfaden für das Autonomous Driving Data Framework (ADDF)

AWS Präskriptive Leitlinien

AWS Präskriptive Leitlinien: Sicherheits- und Betriebsleitfaden für das Autonomous Driving Data Framework (ADDF)

Table of Contents

Sicherheits- und Betriebsleitfaden für das Autonomous Driving Data Framework (ADDF)

Andreas Falkenberg, Junjie Tang, Torsten Reitemeyer und Srinivas Reddy Cheruku, Amazon Web Services (AWS)

November 2022 (Dokumentverlauf)

Autonomous Driving Data Framework (ADDF) ist ein Open-Source-Projekt, das darauf ausgelegt ist, wiederverwendbare, modulare Codeartefakte für Automobilteams bereitzustellen, die allgemeine Aufgaben für fortschrittliche Fahrerassistenzsysteme (ADAS) implementieren möchten, wie z. B. die Konfiguration zentraler Datenspeicher, Datenverarbeitungspipelines, Visualisierungsmechanismen, Suchschnittstellen, Simulationsworkloads, Analyseschnittstellen und vorgefertigte Dashboards. Mit ADDF können Sie vollständig anpassbare Module gemeinsam nutzen, ändern oder erstellen, wodurch der Aufwand für die Erstellung und Bereitstellung dieser Lösungen reduziert wird.

Dieses Handbuch soll Ihnen helfen, bewährte Methoden für die sichere Bereitstellung und den Betrieb von ADDF in der AWS Cloud zu verstehen. Es behandelt die folgenden Themen:

- Architektur und Terminologie – Machen Sie sich mit der allgemeinen Architektur, den Arbeitsabläufen und wichtigen Begriffen vertraut.
- Modell der geteilten Verantwortung – Verstehen Sie Ihre Rolle und die Rolle von AWS bei der Sicherung Ihrer ADDF-Bereitstellung und Ihrer Cloud-Ressourcen.
- Prozess der Sicherheitsüberprüfung – Da es sich bei ADDF um ein Open-Source-Projekt handelt, sollten Sie überprüfen, wie AWS und die Mitwirkenden Sicherheitsüberprüfungen durchführen.
- Integrierte Sicherheitsfeatures – Erfahren Sie, wie bewährte Sicherheitsmethoden und Feature in das ADDF-Open-Source-Projekt und sein Bereitstellungs-Framework integriert sind.
- Sichere Einrichtung und Bedienung – Erfahren Sie, wie Sie ADDF in der AWS Cloud einsetzen und betreiben können.

Zielgruppe

Dieser Leitfaden richtet sich an Entwicklungsteams (DevOps), Infrastrukturingenieure, Administratoren, IT-Sicherheitspersonal und Incident-Response-Teams, die mit der Bewertung,

Bereitstellung, Anpassung und dem Betrieb von ADDF beauftragt sind. Sie können die Empfehlungen in diesem Leitfaden für Machbarkeitsstudien oder Produktionsumgebungen anwenden.

In diesem Handbuch wird davon ausgegangen, dass Sie keine Vorkenntnisse über ADDF haben. Wir empfehlen Ihnen jedoch, die ADDF-Readme-Datei (GitHub) zu lesen, bevor Sie fortfahren.

Gezielte Geschäftsergebnisse

Dieser Leitfaden soll Ihnen helfen, ADDF in Entwicklungs- und Produktionsumgebungen selbstbewusster und sicherer einzurichten und zu betreiben.

ADDF-Architektur und -Terminologie

Bevor Sie sich mit den Sicherheits- und Betriebsthemen in diesem Leitfaden vertraut machen können, ist es wichtig, dass Sie sich mit der Terminologie, den Komponenten und der Architektur des Autonomous Driving Data Framework (ADDF) vertraut machen. In diesem Abschnitt werden folgende Themen beschrieben:

ADDF-Terminologie

Die Schlüsselterminologie für ADDF lautet wie folgt:

- ADDF-Modul – Ein Modul ist Infrastructure as Code (IaC), das eine allgemeine Aufgabe in einem fortschrittlichen Fahrerassistenzsystem (ADAS) implementiert. Zu den häufigsten Aufgaben gehören die Konfiguration zentraler Datenspeicher, Datenverarbeitungspipelines, Visualisierungsmechanismen, Suchschnittstellen, Simulations-Workloads, Analyseschnittstellen und vorgefertigte Dashboards. Sie können ein Modul auf der Grundlage Ihrer Anforderungen erstellen oder ein vorhandenes Modul wiederverwenden oder anpassen.

  Sie können das AWS Cloud Development Kit (AWS CDK) verwenden, um ADDF-Module zu definieren, oder Sie können jedes gängige IaC-Framework verwenden, wie Hashicorp Terraform oder AWS CloudFormation, um die ADDF-Module zu implementieren. Ein Modul hat eine Reihe von Eingabeparametern. Eingabeparameter können von Ausgabewerten anderer Module abhängen. Ein ADDF-Modul ist die kleinste Bereitstellungseinheit für ein ADDF-Ziel-AWS-Konto.
- ADDF-Bereitstellungsmanifestdatei – Diese Datei definiert eine Orchestrierung von eigenständigen ADDF-Modulen. Orchestrierung bezieht sich auf die Bereitstellungsreihenfolge der Module. In der ADDF-Bereitstellungsmanifestdatei können Sie ADDF-Gruppen verwenden, um verwandte Module zu gruppieren. In dieser Datei definieren Sie auch den ADDF-Toolchain-AWS-Konto, die ADDF-Ziel-AWS-Konten und die Ziel-AWS-Regionen.
- ADDF-Bereitstellungsframework – Dieses Framework stellt ADDF-Module im ADDF-Ziel-AWS-Konten bereit, basierend auf der Orchestrierung, die in der ADDF-Bereitstellungsmanifestdatei definiert ist. Das ADDF-Bereitstellungsframework wird unter Verwendung der folgenden AWS-Open-Source-Projekte implementiert:

- SeedFarmer (GitHub) – SeedFarmer ist das CLI-Tool, das für ADDF-Bereitstellungen verwendet wird. Es verwaltet jeden Modulstatus, bereitet den Modulcode vor und verpackt ihn, erstellt Richtlinien mit den geringsten Berechtigungen für die ADDF-Bereitstellungs-Rollen und stellt semantische Anweisungen bereit, die CodeSeeder für die Bereitstellung verwendet. Sie können direkt mit SeedFarmer interagieren, um ADDF-Bereitstellungen auszuführen, oder Sie können es in eine Pipeline für kontinuierliche Integration und kontinuierliche Bereitstellung (CI/CD) integrieren.
- CodeSeeder (GitHub) – CodeSeeder stellt beliebige Infrastrukturen als Codepakete über eine AWS CodeBuild-Aufgabe bereit. SeedFarmer orchestriert und führt CodeSeeder automatisch aus. Nur SeedFarmer interagiert direkt mit CodeSeeder.

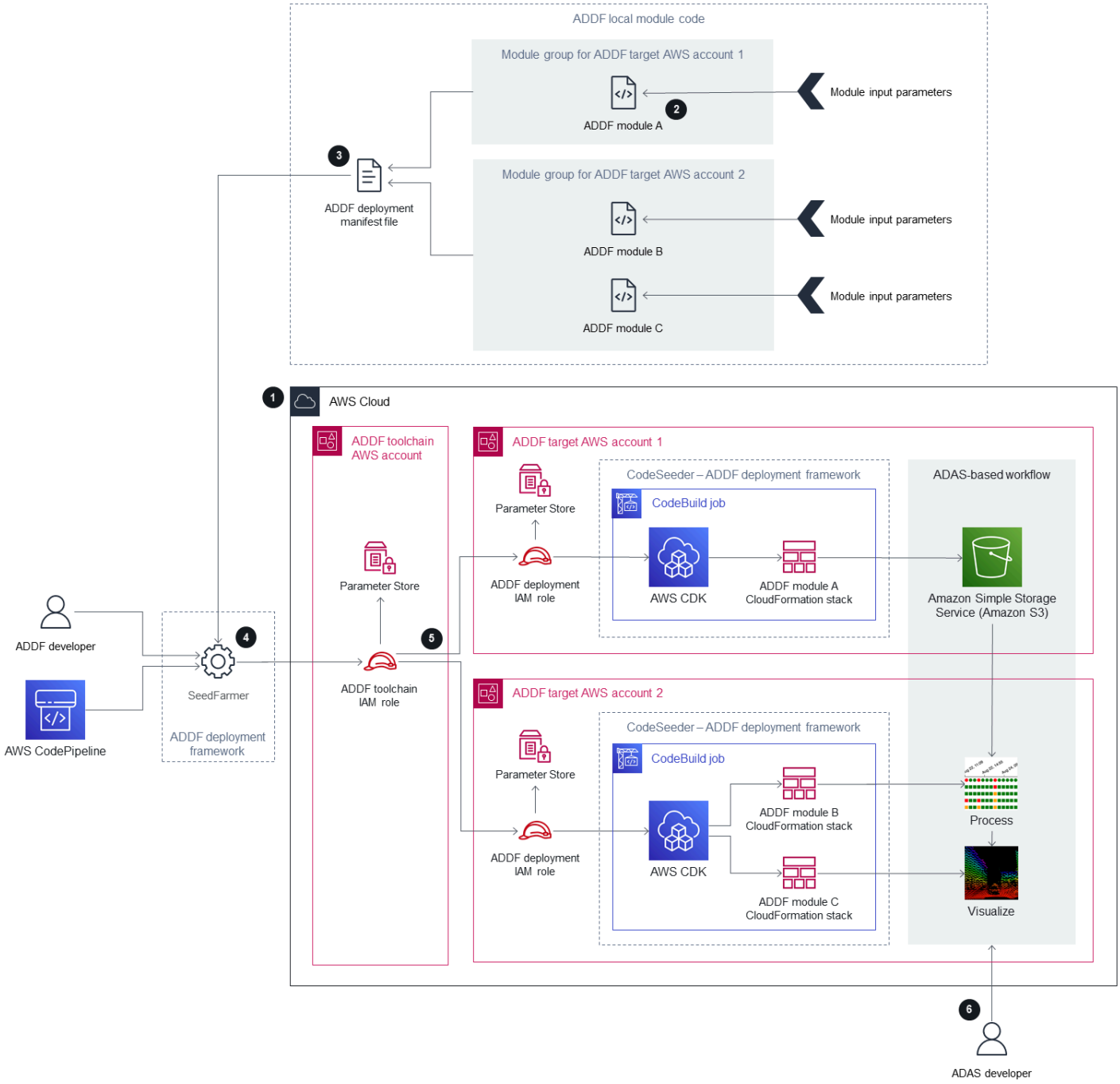
Das ADDF-Bereitstellungsframework wurde entwickelt, um Bereitstellungen in Architekturen mit einem oder mehreren Konten zu unterstützen. Auf der Grundlage der Anforderungen Ihrer Organisation entscheiden Sie, ob eine Architektur für ein oder mehrere Konten erforderlich ist.

- ADDF-Toolchain-AWS-Konto – Dieses Konto orchestriert und verwaltet die Bereitstellung von Modulen im ADDF-Ziel-AWS-Konten, basierend auf den Definitionen in der ADDF-Bereitstellungsmanifestdatei. Eine ADDF-Bereitstellung kann nur ein ADDF-Toolchain-AWS-Konto haben. In einer Architektur mit einem einzigen Konto ist das ADDF-Toolchain-AWS-Konto auch das ADDF-Ziel-AWS-Konto. Dieses Konto enthält eine AWS Identity and Access Management (IAM)-Rolle, genannt ADDF-Toolchain-IAM-Rolle, die von SeedFarmer während des ADDF-Bereitstellungsprozesses übernommen wird. In diesem Handbuch beziehen wir uns auf ein ADDF-Toolchain-AWS-Konto als ein Toolchain-Konto.
- ADDF-Ziel-AWS-Konten – Dies sind die Zielkonten, auf denen Sie ADDF-Module bereitstellen. Sie können ein oder mehrere Zielkonten haben. Diese Konten enthalten die Ressourcen und die Anwendungslogik, die in der ADDF-Bereitstellungsmanifestdatei und den zugehörigen Modulen beschrieben sind. In einer Architektur mit einem einzigen Konto ist das ADDF-Ziel-AWS-Konto auch das ADDF-Toolchain-AWS-Konto. Jedes ADDF-Zielkonto enthält eine IAM-Rolle, die sogenannte ADDF-Bereitstellungs-IAM-Rolle, die von CodeSeeder während des Bereitstellungsprozesses übernommen wird. In diesem Handbuch beziehen wir uns auf ein ADDF-Ziel-AWS-Konto als Zielkonto.
- ADDF-Instance – Wenn Sie ADDF und Ihre Module in der Cloud bereitstellen, wie in Ihrer ADDF-Bereitstellungsmanifestdatei definiert, wird daraus eine ADDF-Instance. Eine ADDF-Instance kann eine Architektur mit einem oder mehreren Konten haben, und Sie können mehrere ADDF-Instances bereitstellen. Weitere Informationen zur Auswahl der Anzahl von Instances und zum

Entwerfen einer Kontoarchitektur für Ihren Anwendungsfall finden Sie unter Definieren Sie Ihre ADDF-Architektur.

ADDF-Architektur

Das folgende Diagramm zeigt eine High-Level-Architektur für eine ADDF-Instance in der AWS Cloud. Es zeigt eine Architektur mit mehreren Konten, einschließlich einem dedizierten Toolchain-Konto und zwei Zielkonten. In diesem Leitfaden wird der gesamte Prozess der Verwendung von ADDF zur Bereitstellung von Ressourcen für die Zielkonten beschrieben.



1. Erstellen und bootstrappen Sie das ADDF-AWS-Konten.

   Um ordnungsgemäß zu funktionieren, muss für jedes Konto ein Bootstrapping zu ADDF AWS CDK durchgeführt werden. Wenn es sich um eine neue ADDF-Bereitstellung handelt oder Sie neue Zielkonten hinzufügen, machen Sie Folgendes:

a. Bootstrappen Sie AWS CDK im Toolchain-Konto und in jedem Zielkonto. Anweisungen finden Sie unter Bootstrappen (AWS CDK-Dokumentation). ADDF verwendet AWS CDK, um seine Infrastruktur bereitzustellen.

b. Bootstrappen Sie ADDF im Toolchain-Konto und in jedem Zielkonto. Anweisungen finden Sie unter Bootstrappen von AWS-Konto(en) im ADDF-Bereitstellungshandbuch. Dadurch werden alle ADDF-spezifischen IAM-Rollen eingerichtet, die von SeedFarmer und CodeSeeder benötigt werden.

> **Note**
>
> Sie müssen diesen Schritt nur ausführen, wenn Sie ADDF neu bereitstellen oder neue Zielkonten hinzufügen. Dieser Schritt ist nicht Teil von wiederkehrenden ADDF-Bereitstellungen für bereits eingerichtete ADDF-Instances.

2. Erstellen Sie die ADDF-Module oder passen Sie sie an.

   Erstellen Sie ADDF-Module oder passen Sie sie auf der Grundlage des spezifischen Problems an, das Sie lösen möchten. Ihr Modul sollte eine isolierte Aufgabe oder eine Gruppe von Aufgaben darstellen. Definieren Sie die Eingabeparameter für das Modul nach Bedarf und verwenden Sie die Modulausgabewerte als Eingabeparameter für andere Module.

3. Definition der Modulorchestrierung in der ADDF-Bereitstellungsmanifestdatei.

   Organisieren Sie Module in der ADDF-Manifestdatei in Gruppen und definieren Sie die Bereitstellungsreihenfolge und die Abhängigkeiten zwischen ihnen. In dieser Datei geben Sie auch das einzelne Toolchain-Konto und die Zielkonten an (einschließlich AWS-Regionen) für jede ADDF-Gruppe und ihre Module.

4. Bewerten Sie die ADDF-Bereitstellungsmanifestdatei und legen Sie den Bereitstellungsbereich fest.

   Der ADDF-Entwickler oder eine CI/CD-Pipeline, wie z. B. AWS CodePipeline, startet eine Bewertung der ADDF-Bereitstellungsmanifestdatei, indem das CLI-Tool SeedFarmer aufgerufen wird. Um die Bewertung zu starten:

   - SeedFarmer verwendet die ADDF-Bereitstellungsmanifestdatei als Eingabeparameter für die Bewertung.

- Um die IAM-Rolle der ADDF-Toolchain anzunehmen, erwartet SeedFarmer dieselben gültigen IAM-Rollen- oder Benutzer-Anmeldeinformationen, die während des ADDF-Bootstrap-Prozesses in Schritt 1 definiert wurden.

Wenn SeedFarmer nicht über die richtigen Anmeldeinformationen verfügt, um die IAM-Rolle der ADDF-Toolchain anzunehmen, oder nicht auf die ADDF-Bereitstellungsmanifestdatei zugreifen kann, startet die Bewertung nicht.

Wenn SeedFarmer die Bewertung starten kann, nimmt es die IAM-Rolle der ADDF-Toolchain im Toolchain-Konto an. Von dort aus kann SeedFarmer auf jedes Zielkonto zugreifen, indem es die IAM-Rolle für die ADDF-Bereitstellung in diesem Konto übernimmt. SeedFarmer versucht dann, alle ADDF-Metadaten im Toolchain-Konto und in den Zielkonten zu lesen. Es tritt einer der beiden folgenden Fälle ein:

- Wenn es keine ADDF-Metadaten zum Lesen gibt, deutet dies darauf hin, dass es sich um eine neue ADDF-Instance handelt. SeedFarmer stellt fest, dass der Bereitstellungsbereich die gesamte ADDF-Bereitstellungsmanifestdatei und ihren Inhalt umfasst.
- Wenn ADDF-Metadaten vorhanden sind, vergleicht SeedFarmer die ADDF-Bereitstellungsmanifestdatei und ihren Inhalt mit den MD5-Hashes der vorhandenen bereitgestellten Artefakte in den Zielkonten. Wenn bereitstellbare Änderungen erkannt werden, wird dieser Prozess fortgesetzt. Wenn keine bereitstellbaren Änderungen erkannt werden, ist der Vorgang abgeschlossen.

5. Stellen Sie die im Umfang enthaltenen ADDF-Module für die Zielkonten bereit.

CodeSeeder verfügt nun über eine geordnete Liste der auszuführenden Bereitstellungen, die gemäß der ADDF-Bereitstellungsmanifestdatei und den Bewertungsergebnissen aus dem vorherigen Schritt ausgeführt werden sollen. Basierend auf dieser sortierten Liste übernimmt CodeSeeder die IAM-Rolle für die ADDF-Bereitstellung in jedem zugehörigen Zielkonto. Anschließend wird CodeSeeder in einer AWS CodeBuild-Aufgabe ausgeführt zum Erstellen oder Aktualisieren der einzelnen IaC-Bereitstellungen, wie z. B. AWS CDK-Anwendungen für das ADDF-Modul. Standardmäßig verwendet ADDF AWS CDK als sein IaC-Framework, aber es werden auch andere gängige IaC-Frameworks unterstützt. Nachdem der Prozess für jedes Zielkonto abgeschlossen wurde, steht Ihnen ein vollständig bereitgestellter, kontenübergreifender, durchgängiger ADAS-basierter Workflow zur Verfügung, wie Sie ihn in der ADDF-Bereitstellungsmanifestdatei definiert haben.

Wenn Sie eine Architektur mit einem einzigen Konto verwenden, handelt es sich bei dem Toolchain-Konto und den Zielkonten um dasselbe Konto, und dieses eine Konto verfügt über alle beschriebenen Funktionen.

6. Verwenden Sie die von ADDF bereitgestellte Infrastruktur.

   Ein ADAS-Entwickler kann den bereitgestellten ADAS-basierten Workflow verwenden, wie er in Ihrem Anwendungsfall definiert ist.

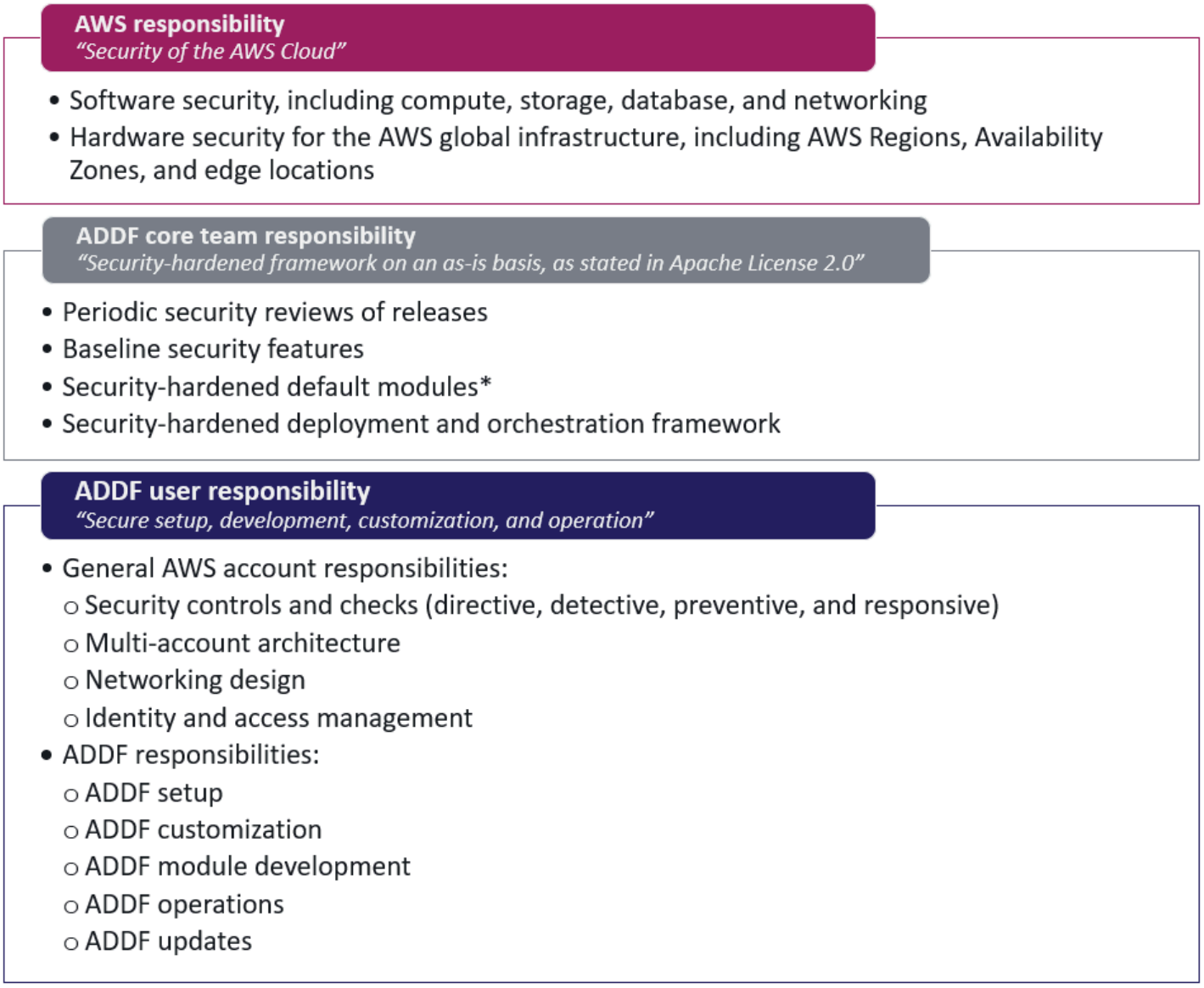
   Dieser Workflow beschreibt die Architektur einer einzelnen Instance einer ADDF-Umgebung mit mehreren Konten. Abhängig von Ihrem Entwicklungs-, Bereitstellungs- und Betriebsmodell empfehlen wir, dass Sie mehrere ADDF-Instances in einer mehrstufigen Umgebung ausführen. Ein typisches Setup könnte eine dedizierte ADDF-Instance mit dedizierten AWS-Konten für jede Bereitstellungsphase sein, z. B. Zweige für Entwicklung, Test und Produktion. Sie können auch mehrere ADDF-Instances in der gleichen Einzel-Konto- oder Multi-Konto-Umgebung in derselben AWS-Region ausführen, vorausgesetzt, Sie haben einen eindeutigen Ressourcennamensraum für jede ADDF-Instance erstellt. Weitere Informationen finden Sie unter Definieren Sie Ihre ADDF-Architektur.

Modell der geteilten Verantwortung in ADDF

Das Modell der geteilten Verantwortung, das für AWS-Services gilt, ist auch für das Autonomous Driving Data Framework (ADDF) gültig. Die folgenden Stellen tragen gemeinsam die Verantwortung für die Sicherung von ADDF, wie in der folgenden Abbildung dargestellt:

- AWS – Das Angebot an AWS-Services des Cloud-Infrastrukturanbieters.
- ADDF-Kernteam – Das ADDF-Kernteam ist die Einheit, die ADDF-Releases in ADDF-Repository (GitHub) veröffentlicht.
- ADDF-Benutzer – Zu den ADDF-Benutzern gehören, sind aber nicht darauf beschränkt:
  - ADDF-Entwickler – Jeder, der den Code für das ADDF-Modul ändert, anpasst oder neuen ADDF-Modulcode erstellt.
  - ADDF-Operator – Jeder, der eine ADDF-Instance einrichtet und betreibt.
  - ADAS-Entwickler – Der Endbenutzer oder Verbraucher der von ADDF bereitgestellten Ressourcen. Ein ADAS-Entwickler kann beispielsweise ein Visualisierungs-Frontend abfragen, das im Rahmen der ADDF-Bereitstellung erstellt wurde.

Das folgende Diagramm fasst die gemeinsame Verantwortung von AWS, dem ADDF-Kernteam und den ADDF-Benutzern.



* Excluding any modules in the ADDF **/modules/demo-only/** folder. Those modules exist only for proof-of-concept purposes and didn't receive security hardening.

AWS-Verantwortung

AWS ist für den Schutz der Infrastruktur zuständig, auf der alle angebotenen Services in der AWS Cloud laufen, wie im AWS-Modell der geteilten Verantwortung definiert. Diese Infrastruktur besteht aus der Hardware, Software, dem Netzwerk und den Einrichtungen, auf und in denen AWS Cloud-Services ausgeführt werden.

Verantwortung des ADDF-Kernteams

Das ADDF-Kernteam bietet ein Framework, das an sich sicher ist, und zwar nach bestem Wissen gemäss Apache License 2.0 (GitHub). Das ADDF-Kernteam ist für Folgendes verantwortlich:

- Regelmäßige Sicherheitsüberprüfungen von Veröffentlichungen
- Grundlegende Sicherheits-Feature
- Sicherheitsverstärkte Standardmodule (Dies schließt alle Module aus dem `/modules/demo-only/`-Ordner. Diese Module dienen nur dem Machbarkeitsnachweis und werden nicht sicherheitstechnisch gehärtet.)
- Framework für Bereitstellung und Orchestrierung mit verbesserter Sicherheit

Diese Sicherheitsverantwortung erstreckt sich nur auf das Framework, wie es im GitHub-Repository bereitgestellt wird, ohne dass Änderungen oder Anpassungen vorgenommen werden. Dies schließt alle ADDF-Module ein, mit Ausnahme der ADDF-Module im `modules/demo-only/`-Ordner. ADDF-Module im Ordner sind nicht sicherheitsgehärtet und sollten nicht in Produktionsumgebungen oder in Umgebungen mit sensiblen oder geschützten Daten eingesetzt werden. Diese Module sind enthalten, um die Systemfunktionen zu demonstrieren. Sie können sie als Grundlage für die Erstellung Ihrer eigenen maßgeschneiderten, sicherheitsgehärteten Module verwenden.

> **Note**
>
> ADDF als Framework wird ohne Mängelgewähr bereitgestellt. Es beinhaltet keine Haftung und Garantie, wie in der Apache License 2.0 (GitHub) definiert. Sie sollten Ihre eigene Sicherheitsbewertung von ADDF durchführen und sicherstellen, dass es den spezifischen Sicherheitsanforderungen Ihrer Organisation entspricht.

Verantwortung des ADDF-Benutzers

ADDF und seine Module sind nur sicher, wenn ADDF auf sichere Weise eingerichtet, angepasst und betrieben wird. Der ADDF-Benutzer trägt die volle Verantwortung für die Sicherheit der folgenden Komponenten:

- Allgemeine AWS-Konto-Verantwortlichkeiten:
  - Sicherheitskontrollen und -kontrollen (direktiv, detektiv, präventiv und reaktiv)

  - Architektur mit mehreren Konten
  - Netzwerkdesign
  - Identity and Access Management
- ADDF-spezifische Zuständigkeiten:
  - ADDF-Einrichtung
  - ADDF-Anpassung
  - Entwicklung von ADDF-Modulen
  - ADDF-Betrieb
  - ADDF-Aktualisierungen

Allgemeine AWS-Konto-Verantwortlichkeiten

Bevor Sie irgendwelche ADDF-bezogenen Ressourcen in AWS-Konten einsetzen, sollte Ihr AWS-Konten gemäß den bewährten Methoden im AWS Well-Architected Framework konfiguriert sein. Dazu gehören direktive, detektive, präventive und reaktive Sicherheitskontrollen. Sie sollten über detaillierte Abhilfemaßnahmen für den Fall von Sicherheitsverstößen oder Vorfällen verfügen. Die Richtlinien Ihrer Organisation sollten Anforderungen für die zentrale Identitäts-, Zugriffs- und Netzwerkverwaltung enthalten. In der Regel werden diese Anforderungen und Services von einem engagierten Landing-Zone-Team bearbeitet.

ADDF-spezifische Zuständigkeiten

Sicheres ADDF-Setup

Die Verantwortung eines ADDF-Benutzers beginnt mit der sicheren Einrichtung von ADDF gemäß der ADDF-Dokumentation. Wir empfehlen Ihnen dringend, die Anweisungen im ADDF-Bereitstellungshandbuch(GitHub) zu befolgen. Weitere Informationen zur sicheren Einrichtung von ADDF finden Sie unter Definieren Sie Ihre ADDF-Architektur und Erstes Einrichten.

Sichere ADDF-Anpassung

Im Falle einer Anpassung von ADDF-Kernfunktionen wie CodeSeeder-, SeedFarmer- und ADDF-Kernmodulen übernimmt der ADDF-Benutzer die volle Verantwortung für diese Änderungen. Weitere Informationen finden Sie unter Anpassen des Codes für das ADDF-Bereitstellungsframework.

Sichere Entwicklung von ADDF-Modulen

Der ADDF-Benutzer trägt die volle Verantwortung für jedes benutzerdefinierte Modul, das mit ADDF bereitgestellt wird. Darüber hinaus ist der ADDF-Benutzer für alle Codeänderungen an von ADDF bereitgestellten Modulen verantwortlich. Weitere Informationen finden Sie unter Schreiben von benutzerdefinierten Modulen in ADDF.

Sichere ADDF-Aktualisierungen und -Operationen

Im Zuge der Weiterentwicklung des Frameworks erhält ADDF Feature- und Sicherheitsupdates. Es liegt in der Verantwortung des ADDF-Benutzers, regelmäßig nach Updates zu suchen, die im GitHub-Repository veröffentlicht wurden, und ADDF langfristig sicher zu betreiben. Weitere Informationen dazu finden Sie unter Wiederkehrende ADDF-Bereitstellungen, Wiederkehrende Sicherheitsprüfungen, ADDF-Aktualisierungen und Außerbetriebnahme.

ADDF-Prozess der Sicherheitsüberprüfung

Das Autonomous Driving Data Framework (ADDF) wurde unter dem Aspekt der Sicherheit entwickelt. Vor der Veröffentlichung für die Öffentlichkeit führte AWS eine erste interne Sicherheitsüberprüfung von ADDF durch und löste alle festgestellten Sicherheitsprobleme. Sowohl AWS als auch die Open-Source-Community tragen zu laufenden Sicherheitsüberprüfungen des Frameworks bei.

Regelmäßige Sicherheitsüberprüfungen durch AWS

ADDF wird unter der GitHub-Organisation awslabs veröffentlicht, die AWS gehört. AWS führt regelmäßig automatische und manuelle Sicherheitsüberprüfungen des Codes in dieser Organisation durch, um die Sicherheit nach bestem Wissen und Gewissen zu überprüfen. Laut AWS-Richtlinie gibt AWS keine Informationen über die Häufigkeit der Sicherheitsüberprüfung, den Ansatz oder die verwendeten Werkzeuge bekannt. Darüber hinaus veröffentlicht AWS keine internen Prüfungsberichte über ADDF. Alle identifizierten Sicherheitserkenntnisse werden jedoch behoben und per Pull-Anfrage mit hoher Dringlichkeit veröffentlicht.

> **Note**
>
> ADDF als Framework wird „WIE GESEHEN“ BEREITGESTELLT, OHNE AUSDRÜCKLICHE ODER STILLSCHWEIGENDE GEWÄHRLEISTUNGEN ODER BEDINGUNGEN JEGLICHER ART, einschließlich, aber nicht beschränkt auf Gewährleistungen oder Bedingungen in Bezug auf Titel, Nichtverletzung von Rechten Dritter, Marktgängigkeit oder Eignung für einen bestimmten Zweck, wie in der Apache License 2.0 (GitHub) festgelegt. Sie sollten Ihre eigene Sicherheitsbewertung von ADDF durchführen und überprüfen, ob es den spezifischen Sicherheitsanforderungen Ihrer Organisation entspricht. Wie in der Apache License 2.0 dargelegt, sind Sie allein dafür verantwortlich, die Angemessenheit der Verwendung oder Weiterverbreitung von ADDF zu bestimmen und alle Risiken zu übernehmen, die mit Ihrer Ausübung oder Ihren Genehmigungen im Rahmen dieser Lizenz verbunden sind.

Open-Source-Sicherheitsüberprüfungen und -Beiträge

ADDF ist ein Open-Source-Projekt, das Beiträge begrüßt. Wir laden alle Benutzer ein, ihre eigene Sicherheitsüberprüfung des Frameworks durchzuführen und dazu beizutragen, indem sie alle

sicherheitsrelevanten Erkenntnisse melden. Wenn Sie ein Problem im Code erkennen, folgen Sie bitte den Richtlinien unterBenachrichtigungen über Sicherheitsprobleme (ADDF-Dokumentation).

In ADDF integrierte Sicherheitsfeatures

Das Autonomous Driving Data Framework (ADDF) verfügt über verschiedene eingebaute Sicherheitsfeatures. Standardmäßig sollen diese Features Ihnen bei der Einrichtung eines sicheren Frameworks helfen und Ihrer Organisation dabei unterstützen, die allgemeinen Sicherheitsanforderungen von Unternehmen zu erfüllen.

Im Folgenden sind die integrierten Sicherheitsfeatures aufgeführt:

- Geringste Berechtigung für ADDF-Modulcode
- Infrastructure as Code
- Automatisierte Sicherheitsprüfungen für IaC
- Benutzerdefinierte Richtlinie mit den geringsten Berechtigungen für die AWS CDK-Bereitstellungs-Rolle
- Richtlinie mit den geringsten Berechtigungen für die Deployspec-Datei des Moduls
- Datenverschlüsselung
- Speicherung von Anmeldeinformationen mit Secrets Manager
- Sicherheitsüberprüfungen von SeedFarmer und CodeSeeder
- Unterstützung der Berechtigungsgrenzen für die AWS CodeBuild-Rolle für CodeSeeder
- AWS-Architektur mit mehreren Konten
- Berechtigungen mit den geringsten Berechtigungen für Bereitstellungen mit mehreren Konten

Geringste Berechtigung für ADDF-Modulcode

Geringste Berechtigung ist die bewährte Methode, die für die Ausführung einer Aufgabe erforderlichen Mindestberechtigungen zu gewähren. Weitere Informationen finden Sie unter Anwendung von geringsten Berechtigungen. Von ADDF bereitgestellte Module folgen in ihrem Code und den bereitgestellten Ressourcen strikt dem Prinzip der geringsten Berechtigung, und zwar wie folgt:

- Alle für ein ADDF-Modul erstellten AWS Identity and Access Management (IAM)-Richtlinien haben die für den Anwendungsfall erforderlichen Mindestberechtigungen.

- AWS-Services sind nach dem Prinzip der geringsten Berechtigung konfiguriert und eingesetzt. Von ADDF bereitgestellte Module verwenden nur die Services und Service-Features, die für den jeweiligen Anwendungsfall erforderlich sind.

Infrastructure as Code

ADDF ist als Framework darauf ausgelegt, ADDF-Module als Infrastructure as Code (IaC) bereitzustellen. IaC macht manuelle Bereitstellungsprozesse überflüssig und hilft, Fehler und Fehlkonfigurationen zu vermeiden, die sich aus manuellen Prozessen ergeben können.

ADDF wurde für die Orchestrierung und Bereitstellung von Modulen mithilfe eines beliebigen gängigen IaC-Frameworks entwickelt. Dies enthält, ist aber nicht beschränkt auf:

- AWS Cloud Development Kit (AWS CDK)
- AWS CloudFormation
- Hashicorp Terraform

Sie können verschiedene IaC-Frameworks verwenden, um verschiedene Module zu schreiben, und dann ADDF verwenden, um sie bereitzustellen.

Das Standard-IaC-Framework, das von ADDF-Modulen verwendet wird, ist AWS CDK. AWS CDK ist eine objektorientierte Abstraktion auf hoher Ebene, die Sie verwenden können, um AWS-Ressourcen zwingend zu definieren. AWS CDK erzwingt bereits standardmäßig bewährte Methoden Sicherheit für verschiedene Services und Szenarien. Durch die Verwendung von AWS CDK wird das Risiko von Sicherheitsfehlkonfigurationen reduziert.

Automatisierte Sicherheitsprüfungen für IaC

Das Open-Source-Hilfsprogramm cdk-nag (GitHub) ist in ADDF integriert. Dieses Tool überprüft automatisch ADDF-Module, die auf AWS CDK basieren für die Einhaltung der allgemeinen und sicherheitstechnischen bewährten Methoden. Das Hilfsprogramm cdk-nag verwendet Regeln und Regelpakete, um Code zu erkennen und zu melden, der gegen bewährte Methoden verstößt. Weitere Informationen zu den Regeln und eine umfassende Liste finden Sie unter cdk-nag-Regeln (GitHub).

Benutzerdefinierte Richtlinie mit den geringsten Berechtigungen für die AWS CDK-Bereitstellungs-Rolle

ADDF nutzt in großem Umfang AWS CDK v2. Es ist erforderlich, dass Sie alle ADDF AWS-Konten zu AWS CDK bootstrappen. Weitere Informationen finden Sie unter Bootstrappen (AWS CDK-Dokumentation).

Standardmäßig weist AWS CDK die permissive AWS-verwaltete Richtlinie AdministratorAccess der AWS CDK-Bereitstellungsrolle zu, die in Bootstrap-Konten erstellt wurde. Der vollständige Name dieser Rolle lautet `cdk-[CDK_QUALIFIER]-cfn-exec-role-[AWS_ACCOUNT_ID]-[REGION]`. AWS CDK verwendet diese Rolle, um Ressourcen im Bootstrapped AWS-Konto bereitzustellen als Teil des AWS CDK-Bereitstellungsprozesses.

Abhängig von den Sicherheitsanforderungen Ihrer Organisation ist die `AdministratorAccess`-Richtlinie ist möglicherweise zu freizügig. Im Rahmen des AWS CDK-Bootstrap-Prozesses können Sie die Richtlinien und Berechtigungen an Ihre Bedürfnisse anpassen. Sie können die Richtlinie ändern, indem Sie das Konto mit einer neu definierten Richtlinie neu bootstrappen, indem Sie den `--cloudformation-execution-policies`-Parameter verwenden. Weitere Informationen finden Sie unter Bootstrapping anpassen (AWS CDK-Dokumentation).

> **Note**
>
> Obwohl dieses Sicherheitsfeature nicht spezifisch für ADDF ist, wird es in diesem Abschnitt aufgeführt, da es die allgemeine Sicherheit Ihrer ADDF-Bereitstellung erhöhen kann.

Richtlinie mit den geringsten Berechtigungen für die Deployspec-Datei des Moduls

Jedes Modul enthält eine Datei mit Bereitstellungsspezifikationen namens deployspec.yaml. Diese Datei definiert die Bereitstellungsanweisungen für das Modul. CodeSeeder verwendet sie, um das definierte Modul im Zielkonto unter Verwendung von AWS CodeBuild bereitzustellen. CodeSeeder weist CodeBuild eine Standard-Servicerolle zu, um die Ressourcen bereitzustellen, wie in der Datei mit den Bereitstellungsspezifikationen beschrieben. Diese Servicerolle ist nach dem Prinzip der geringsten Berechtigung konzipiert. Sie enthält alle erforderlichen Berechtigungen für die Bereitstellung von AWS CDK-Anwendungen, da alle von ADDF bereitgestellten Module als AWS CDK-Anwendungen erstellt werden.

Wenn Sie jedoch Stage-Befehle außerhalb von AWS CDK ausführen müssen, müssen Sie eine benutzerdefinierte IAM-Richtlinie erstellen, anstatt die Standard-Servicerolle für CodeBuild zu verwenden. Wenn Sie beispielsweise ein anderes IaC-Bereitstellungsframework verwenden als AWS CDK, wie z. B. Terraform, müssen Sie eine IAM-Richtlinie erstellen, die ausreichende Berechtigungen gewährt, damit dieses spezielle Framework funktioniert. Ein anderes Szenario, das eine spezielle IAM-Richtlinie erfordert, ist, wenn Sie AWS Command Line Interface (AWS CLI)-Aufrufe zu anderen AWS-Services in die `install`-, `pre_build`-, `build`-, oder `post_build`-Stage-Befehle einbeziehen. Sie benötigen zum Beispiel eine benutzerdefinierte Richtlinie, wenn Ihr Modul einen Amazon Simple Storage Service (Amazon S3)-Befehl zum Hochladen von Dateien in ein S3-Bucket enthält. Die benutzerdefinierte IAM-Richtlinie bietet eine detaillierte Kontrolle für jeden AWS-Befehl außerhalb der AWS CDK-Bereitstellung. Ein Beispiel für eine benutzerdefinierte IAM-Richtlinie finden Sie unter ModuleStack (SeedFarmer-Dokumentation). Wenn Sie eine benutzerdefinierte IAM-Richtlinie für Ihr ADDF-Modul erstellen, stellen Sie sicher, dass Sie geringste Berechtigungen anwenden.

Datenverschlüsselung

ADDF speichert und verarbeitet potenziell sensible Daten. Um diese Daten zu schützen, verschlüsseln die von SeedFarmer, CodeSeeder und von ADDF bereitgestellten Module Daten im Ruhezustand und bei der Übertragung für alle verwendeten AWS-Services (sofern nicht ausdrücklich anders angegeben für Module im `demo-only`-Ordner).

Speicherung von Anmeldeinformationen mit Secrets Manager

ADDF verwaltet verschiedene Geheimnisse für verschiedene Services wie Docker Hub, JupyterHub und Amazon Redshift. ADDF verwendet AWS Secrets Manager, um alle ADDF-bezogenen Geheimnisse zu speichern. Dies hilft Ihnen, sensible Daten aus dem Quellcode zu entfernen.

Secrets-Manager-Geheimnisse werden nur in den Zielkonten gespeichert, soweit dies für die ordnungsgemäße Funktion dieses Kontos erforderlich ist. Standardmäßig enthält das Toolchain-Konto keine Geheimnisse.

Sicherheitsüberprüfungen von SeedFarmer und CodeSeeder

SeedFarmer und CodeSeeder (GitHub-Repositorien) werden für die Bereitstellung von ADDF und seinen ADDF-Modulen verwendet. Diese Open-Source-Projekte durchlaufen denselben

regelmäßigen AWS-internen Sicherheitsüberprüfungsprozess wie ADDF, wie in ADDF-Prozess der Sicherheitsüberprüfung beschrieben.

Unterstützung der Berechtigungsgrenzen für die AWS CodeBuild-Rolle für CodeSeeder

IAM-Berechtigungsgrenzen sind ein allgemeiner Sicherheitsmechanismus, der die maximalen Berechtigungen definiert, die eine auf einer Identität basierende Richtlinie einer IAM-Entität erlauben kann. SeedFarmer und CodeSeeder unterstützen für jedes Zielkonto einen Anhang der IAM-Berechtigungsgrenze. Die Berechtigungsgrenze begrenzt die maximalen Berechtigungen aller Servicerollen, die von CodeBuild verwendet werden, wenn CodeSeeder Module bereitstellt. Die IAM-Berechtigungsgrenzen müssen außerhalb von ADDF von einem Sicherheitsteam erstellt werden. Anhänge für IAM-Berechtigungsgrenzen werden als Attribut in der ADDF-Bereitstellungsmanifestdatei akzeptiert, deployment.yaml. Weitere Informationen finden Sie unter Unterstützung von Berechtigungsgrenzen (SeedFarmer-Dokumentation).

Der Workflow ist wie folgt:

1. Ihr Sicherheitsteam definiert und erstellt eine IAM-Berechtigungsgrenze entsprechend Ihren Sicherheitsanforderungen. Die IAM-Berechtigungsgrenze muss in jedem ADDF-AWS-Konto individuell erstellt werden. Die Ausgabe ist eine Liste von Berechtigungsgrenzen-Richtlinien für Amazon-Ressourcennamen (ARN).
2. Das Sicherheitsteam teilt die ARN-Liste der Richtlinien mit Ihrem ADDF-Entwicklerteam.
3. Das ADDF-Entwicklerteam integriert die ARN-Liste der Richtlinien in die Manifestdatei. Ein Beispiel für diese Integration finden Sie unter sample-permissionboundary.yaml (GitHub) und Bereitstellungsmanifest (SeedFarmer-Dokumentation).
4. Nach erfolgreicher Bereitstellung wird die Berechtigungsgrenze allen Servicerollen zugewiesen, die CodeBuild zur Bereitstellung von Modulen verwendet.
5. Das Sicherheitsteam überwacht, ob die Berechtigungsgrenzen wie gewünscht angewendet werden.

AWS-Architektur mit mehreren Konten

Wie in der Sicherheitssäule des AWS Well-Architected Framework definiert, wird es als bewährte Methode angesehen, Ressourcen und Workloads in mehrere AWS-Konten aufzuteilen, basierend

auf den Anforderungen Ihrer Organisation. Das liegt daran, dass ein AWS-Konto als Isolationsgrenze fungiert. Weitere Informationen finden Sie unter AWS-Konto-Kontenverwaltung und Trennung. Die Umsetzung dieses Konzepts wird als Architektur mit mehreren Konten bezeichnet. Eine richtig konzipierte AWS-Multi-Konto-Architektur bietet eine Kategorisierung des Workloads und reduziert den Umfang der Auswirkungen im Falle eines Sicherheitsverstoßes im Vergleich zu einer Einzel-Konto-Architektur.

ADDF unterstützt nativ AWS-Multi-Konto-Architekturen. Sie können Ihre ADDF-Module auf beliebig viele AWS-Konten verteilen, je nach den Anforderungen Ihrer Organisation in Bezug auf Sicherheit und Aufgabentrennung. Sie können ADDF in einem einzigen AWS-Konto bereitstellen und die Funktionen der Toolchain und des Zielkontos kombinieren. Alternativ können Sie individuelle Zielkonten für ADDF-Module oder Modulgruppen erstellen.

Die einzige Einschränkung, die Sie berücksichtigen müssen, besteht darin, dass ein ADDF-Modul jeweils die kleinste Bereitstellungseinheit für jedes AWS-Konto darstellt.

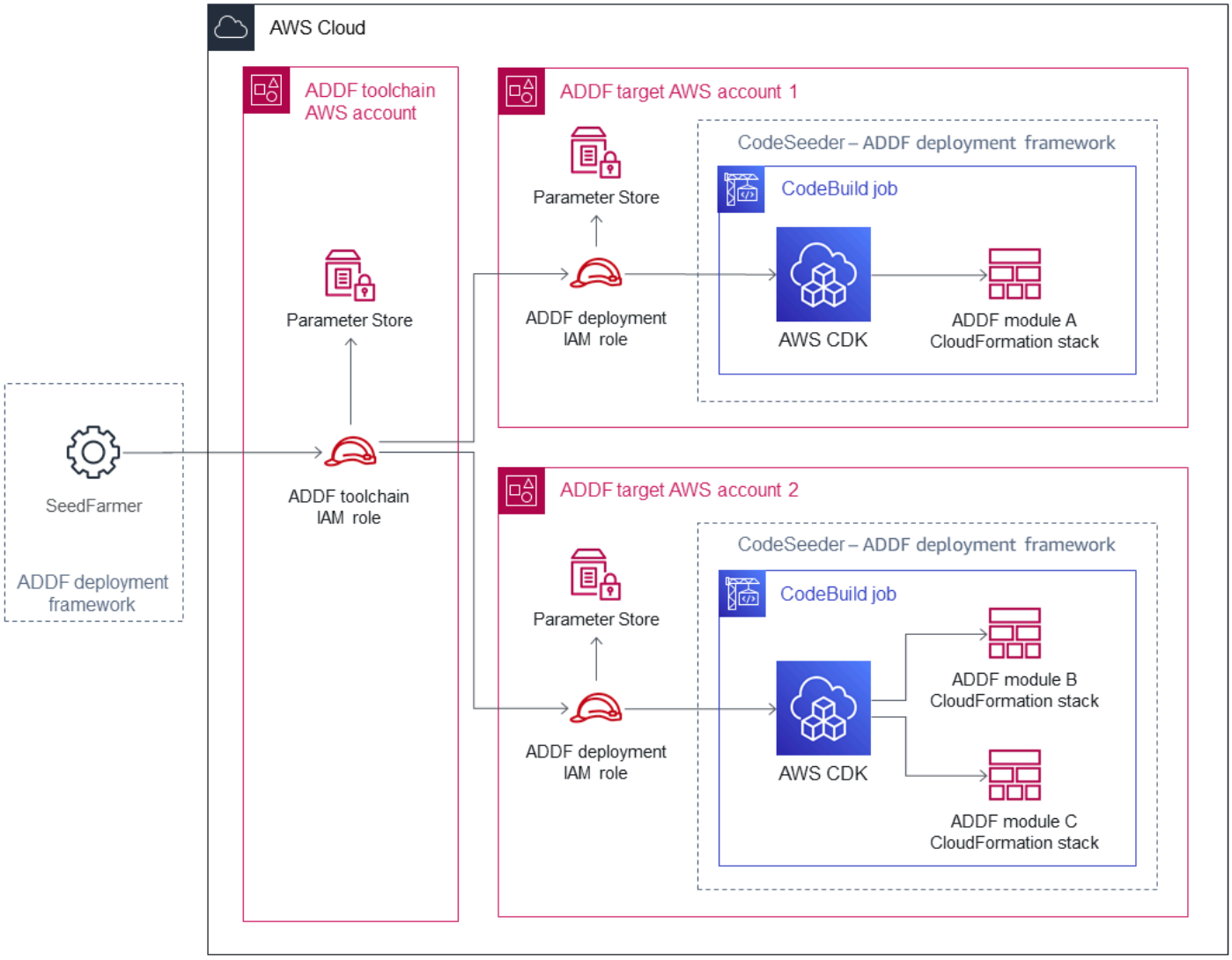
Für Produktionsumgebungen wird empfohlen, eine Architektur mit mehreren Konten zu verwenden, die aus einem Toolchain-Konto und mindestens einem Zielkonto besteht. Weitere Informationen finden Sie unter ADDF-Architektur.

Berechtigungen mit den geringsten Berechtigungen für Bereitstellungen mit mehreren Konten

Wenn Sie eine Architektur mit mehreren Konten verwenden, muss SeedFarmer auf die Zielkonten zugreifen, um die folgenden drei Aktionen durchzuführen:

1. Die Metadaten des ADDF-Moduls in das Toolchain-Konto und die Zielkonten schreiben.
2. Die aktuellen ADDF-Modul-Metadaten aus dem Toolchain-Konto und den Zielkonten lesen.
3. Initiierung von AWS CodeBuild-Aufträgen in den Zielkonten, um Module zu verteilen oder zu aktualisieren.

Die folgende Abbildung zeigt die kontenübergreifenden Beziehungen, einschließlich der Operationen, bei denen davon ausgegangen wird, dass sie ADDF-spezifische AWS Identity and Access Management (IAM)-Rollen sind.



Diese kontenübergreifenden Aktionen werden mithilfe klar definierter Operationen mit Rollenübernahme erreicht.

- Die IAM-Rolle der ADDF-Toolchain wird im Toolchain-Konto bereitgestellt. SeedFarmer übernimmt diese Rolle. Diese Rolle hat die Rechte zur Ausführung einer `iam:AssumeRole`-Aktion und kann in jedem Zielkonto die IAM-Rolle für die ADDF-Bereitstellung übernehmen. Darüber hinaus kann die ADDF-Toolchain-IAM-Rolle lokale AWS Systems Manager-Parameterspeichervorgänge ausführen.
- Die IAM-Rolle für die ADDF-Bereitstellung wird in jedem Zielkonto bereitgestellt. Diese Rolle kann nur von dem Toolchain-Konto übernommen werden, indem die ADDF-Toolchain-IAM-Rolle verwendet wird. Diese Rolle hat die Berechtigung, lokale AWS Systems Manager-

Parameterspeichervorgänge auszuführen und hat die Berechtigung, AWS CodeBuild-Aktionen auszuführen, die CodeBuild-Aufträge über CodeSeeder initiieren und beschreiben.

Diese ADDF-spezifischen IAM-Rollen werden im Rahmen des ADDF-Bootstrapping-Prozesses erstellt. Weitere Informationen finden Sie unter AWS-Konto(en) bootstrappen im Handbuch für ADDF-Bereitstellung (GitHub).

Alle kontoübergreifenden Berechtigungen sind nach dem Prinzip der geringste Berechtigungen eingerichtet. Wenn ein Zielkonto kompromittiert wird, hat dies nur minimale oder gar keine Auswirkungen auf andere ADDF-AWS-Konten.

Im Fall einer Einzel-Konto-Architektur für ADDF bleiben die Rollenbeziehungen gleich. Sie fallen einfach zu einem einzigen AWS-Konto zusammen.

Sichere Einrichtung und Bedienung von ADDF

Autonomous Driving Data Framework (ADDF) sollte als maßgeschneiderte Software behandelt werden, die eine kontinuierliche Wartung und Pflege durch ein engagiertes DevOps- und Sicherheitsteam in Ihrer Organisation erfordert. In diesem Abschnitt werden sicherheitsrelevante allgemeine Aufgaben beschriebe, die Sie bei der Einrichtung und dem Betrieb von ADDF während seines gesamten Lebenszyklus unterstützen.

Dieser Abschnitt beinhaltet die folgenden Aufgaben:

- Definieren Sie Ihre ADDF-Architektur
- Erstes Einrichten
- Anpassen des Codes für das ADDF-Bereitstellungsframework
- Schreiben von benutzerdefinierten Modulen in ADDF
- Wiederkehrende ADDF-Bereitstellungen
- Wiederkehrende Sicherheitsprüfungen
- ADDF-Aktualisierungen
- Außerbetriebnahme

Definieren Sie Ihre ADDF-Architektur

Eine ADDF-Instance ist nur so sicher wie die AWS-Konto-Umgebung, in der sie eingesetzt wird. Diese AWS-Konto-Umgebung muss so konzipiert sein, dass sie die Sicherheits- und Betriebsanforderungen Ihres spezifischen Anwendungsfalls erfüllt. Beispielsweise unterscheiden sich die sicherheits- und betriebsbezogenen Aufgaben und Überlegungen bei der Einrichtung einer ADDF-Instance in einer Proof-of-Concept-Umgebung (PoC) von denen für die Einrichtung von ADDF in einer Produktionsumgebung.

ADDF in einer PoC-Umgebung ausführen

Wenn Sie ADDF in einer PoC-Umgebung verwenden möchten, empfehlen wir die Erstellung eines AWS-Konto für ADDF, das keine anderen Workloads enthält. Dies trägt zur Sicherheit Ihres Kontos bei, während Sie ADDF und seine Features erkunden. Diese Herangehensweise bietet folgende Vorteile:

- Im Falle einer schwerwiegenden ADDF-Fehlkonfiguration würden keine anderen Workloads beeinträchtigt.
- Es besteht kein Risiko einer anderen Fehlkonfiguration von Workloads, die sich negativ auf die Einrichtung von ADDF auswirken könnten.

Selbst in einer PoC-Umgebung empfehlen wir Ihnen, möglichst viele der bewährten Methoden zu befolgen, die unter ADDF in einer Produktionsumgebung ausführen aufgeführt sind.

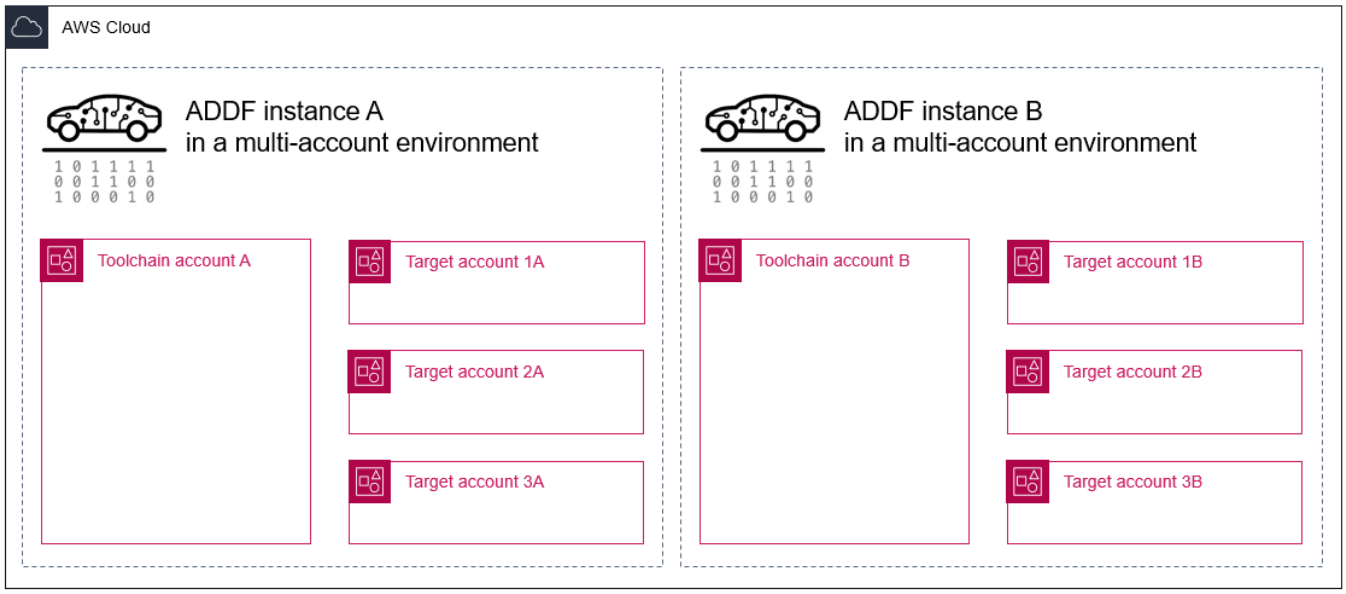
ADDF in einer Produktionsumgebung ausführen

Wenn Sie ADDF in einer Produktionsumgebung eines Unternehmens verwenden möchten, empfehlen wir Ihnen dringend, die bewährten Sicherheitsmethoden Ihrer Organisation zu berücksichtigen und ADDF entsprechend zu implementieren. Zusätzlich zu den bewährten Sicherheitsmethoden Ihrer Organisation empfehlen wir Ihnen, Folgendes zu implementieren:

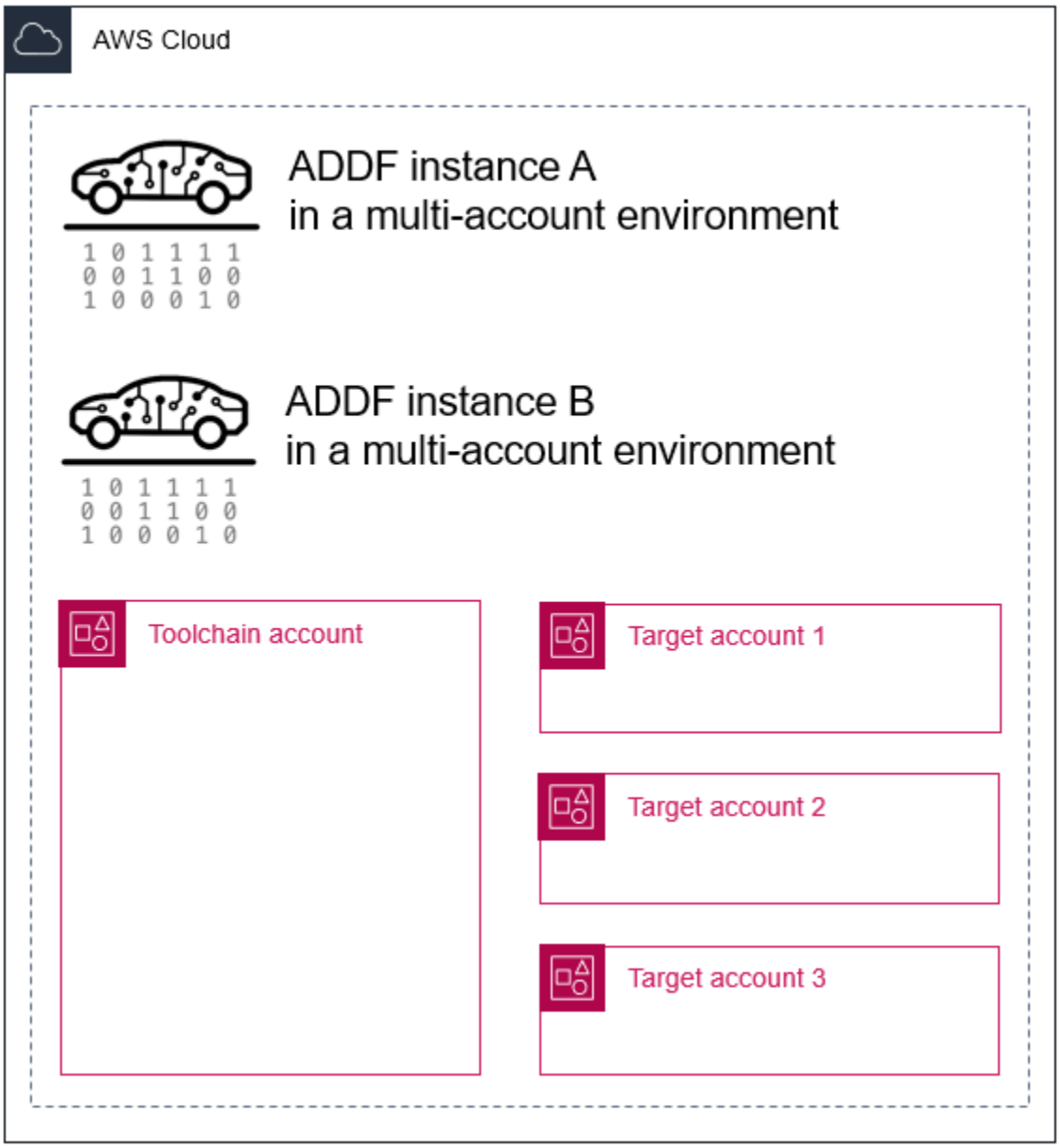
- Stellen Sie ein langfristiges, engagiertes ADDF-DevOps-Team zusammen – ADDF muss wie eine maßgeschneiderte Software behandelt werden. Es erfordert eine kontinuierliche Wartung und Pflege durch ein engagiertes DevOps-Team. Bevor mit der Ausführung von ADDF in einer Produktionsumgebung begonnen wird, sollte ein DevOps-Team mit ausreichender Größe und Kapazität mit vollem Ressourceneinsatz bis zum Ende der Lebensdauer der ADDF-Bereitstellung definiert werden.
- Verwenden Sie eine Architektur mit mehreren Konten – Jede ADDF-Instance sollte in einer eigenen AWS-Umgebung mit mehreren Konten bereitgestellt werden, ohne andere, nicht damit verbundene Workloads. Wie in AWS-Kontoverwaltung und -trennung (AWS Well-Architected Framework) definiert, gilt es als bewährte Methode, Ressourcen und Workloads je nach den Anforderungen Ihrer Organisation in mehrere AWS-Konten aufzuteilen. Das liegt daran, dass ein AWS-Konto als Isolationsgrenze fungiert. Eine richtig konzipierte AWS-Multi-Konto-Architektur bietet eine Kategorisierung des Workloads und reduziert den Umfang der Auswirkungen im Falle eines Sicherheitsverstoßes im Vergleich zu einer Einzel-Konto-Architektur. Die Verwendung einer Architektur mit mehreren Konten trägt auch dazu bei, dass Ihre Konten innerhalb ihrer AWS-Service-Quotas bleiben. Verteilen Sie Ihre ADDF-Module auf beliebig viele AWS-Konten wie nötig, um die Anforderungen Ihrer Organisation in Bezug auf Sicherheit und Aufgabentrennung zu erfüllen.
- Stellen Sie mehrere ADDF-Instances bereit – Richten Sie so viele separate ADDF-Instances ein, wie Sie benötigen, um ADDF-Module gemäß den Softwareentwicklungsprozessen Ihrer

Organisation ordnungsgemäß zu entwickeln, zu testen und bereitzustellen. Wenn Sie mehrere ADDF-Instances erstellen, können Sie einen der folgenden Ansätze verwenden:

- Mehrere ADDF-Instances in verschiedenen AWS-Umgebungen mit mehreren Konten – Sie können separate AWS-Konten verwenden, um verschiedene ADDF-Instances zu isolieren. Wenn Ihre Organisation beispielsweise über spezielle Entwicklungs-, Test- und Produktionsphasen verfügt, können Sie separate ADDF-Instances und dedizierte Konten für jede Phase erstellen. Dies bietet viele Vorteile, z. B. die Verringerung des Risikos, dass sich Fehler phasenübergreifend ausbreiten, hilft Ihnen bei der Implementierung eines Genehmigungsprozesses und beschränkt den Benutzerzugriff nur auf bestimmte Umgebungen. Die folgende Abbildung zeigt zwei ADDF-Instances, die in separaten Umgebungen mit mehreren Konten bereitgestellt werden.



- Mehrere ADDF-Instances in derselben AWS-Umgebung mit mehreren Konten – Sie können mehrere ADDF-Instances erstellen, die sich dieselbe AWS-Umgebung mit mehreren Konten teilen. Dadurch entstehen effektiv isolierte Zweige im selben AWS-Konten. Wenn beispielsweise verschiedene Entwickler parallel arbeiten, kann ein Entwickler eine dedizierte ADDF-Instance in derselben erstellenAWS-Konten. Dies hilft Entwicklern, zu Entwicklungs- und Testzwecken in isolierten Zweigen zu arbeiten. Wenn Sie diesen Ansatz verwenden, müssen Ihre ADDF-Ressourcen für jede ADDF-Instance eindeutige Ressourcennamen haben. Dies wird standardmäßig in vorinstallierten ADDF-Modulen unterstützt. Sie können diesen Ansatz verwenden, solange Sie die AWS-Service-Quotas nicht überschreiten. Die folgende Abbildung zeigt zwei ADDF-Instances, die in einer geteilten Umgebung mit mehreren Konten bereitgestellt werden.



- Mehrere ADDF-Instances in derselben AWS-Umgebung mit einem Konto – Diese Architektur ist dem vorherigen Beispiel sehr ähnlich. Der Unterschied besteht darin, dass mehrere ADDF-Instances in einer Umgebung mit einem Konto statt in einer Umgebung mit mehreren Konten bereitgestellt werden. Diese Architektur eignet sich für sehr einfache ADDF-Anwendungsfälle mit einem sehr begrenzten Umfang und mehreren Entwicklern, die gleichzeitig in verschiedenen Branchen arbeiten.

Da SeedFarmer das einzige Tool ist, das die Bereitstellungen für eine ADDF-Instance steuert, können Sie jede Umgebung und Kontoarchitektur erstellen, die zur Bereitstellungsstrategie und den CI/CD-Prozessen Ihrer Organisation passt.

- Passen Sie den AWS Cloud Development Kit (AWS CDK)-Bootstrap-Prozess entsprechend den Sicherheitsanforderungen Ihrer Organisation an – Standardmäßig weist AWS CDK die AWS-verwaltete Richtlinie AdministratorAccess während des Bootstrapping-Vorgangs zu. Diese Richtlinie gewährt volle Administratorrechte. Wenn diese Richtlinie für die Sicherheitsanforderungen Ihrer Organisation zu offen ist, können Sie die Richtlinien anpassen. Weitere Informationen finden Sie unter Benutzerdefinierte Richtlinie mit den geringsten Berechtigungen für die AWS CDK-Bereitstellungs-Rolle.
- Halten Sie sich bei der Einrichtung des Zugriffs in IAM an bewährte Methoden – Richten Sie eine strukturierte AWS Identity and Access Management (IAM)-Zugriffslösung ein, die Ihren Benutzern den Zugriff auf die ADDF-AWS-Konten ermöglicht. Das ADDF-Framework ist so konzipiert, dass es dem Prinzip der geringsten Berechtigung entspricht. Ihr IAM-Zugriffsmuster sollte außerdem dem

Prinzip der geringsten Berechtigung folgen, den Anforderungen Ihrer Organisation entsprechen und den Bewährten Methoden für die Sicherheit in IAM (IAM-Dokumentation) folgen.

- Das Netzwerk gemäß den bewährten Methoden Ihrer Organisation einrichten – ADDF beinhaltet einen optionalen Netzwerk-AWS CloudFormation-Stack, der eine einfache öffentliche oder Virtual Private Cloud (VPC) erstellt. Abhängig von der Konfiguration Ihrer Organisation kann diese VPC Ressourcen direkt dem Internet zugänglich machen. Wir empfehlen Ihnen, die bewährten Netzwerkpraktiken Ihrer Organisation zu befolgen und ein benutzerdefiniertes, sicherheitsverstärktes Netzwerkmodul zu erstellen.
- Bereitstellung von Maßnahmen zur Sicherheitsprävention, -erkennung und -minderung auf der AWS-Konto-Ebene – AWS bietet verschiedene Sicherheitsdienste wie Amazon GuardDuty, AWS Security Hub, Amazon Detective und AWS Config. Aktivieren Sie diese Services in Ihrer ADDF-AWS-Konto und integrieren Sie die Prozesse Ihrer Organisation zur Prävention, Erkennung, Minderung und Behandlung von Sicherheitsvorfällen. Wir empfehlen Ihnen bewährten Methoden für Sicherheit, Identität und Compliance (AWS Architecture Center) und allen servicespezifischen Empfehlungen, die in der Dokumentation für diesen Service enthalten sind, zu folgen. Weitere Informationen finden Sie unter AWS-Sicherheit auf Dokumentenebene.

ADDF behandelt keines dieser Themen, da die Implementierungs- und Konfigurationsdetails stark von den Anforderungen und Prozessen abhängen, die für Ihre Organisation spezifisch sind. Stattdessen liegt es in der Kernverantwortung Ihrer Organisation, sich mit diesen Themen zu befassen. In der Regel hilft das Team, das Ihre AWS Landing Zone verwaltet, Ihnen bei der Planung und Implementierung Ihrer ADDF-Umgebung.

Erstes Einrichten

Richten Sie ADDF gemäß dem ADDF-Bereitstellungshandbuch (GitHub) ein. Der Ausgangspunkt für jede Bereitstellung ist der `/manifest`-Ordner im Git Hub-Repository Framework für Daten zum autonomen Fahren. Der `/manifest/example-dev` Ordner enthält eine Beispielbereitstellung für Demo-Zwecke. Verwenden Sie dieses Beispiel als Ausgangspunkt für die Gestaltung Ihrer eigenen Bereitstellung. In diesem Verzeichnis befindet sich eine ADDF-Bereitstellungsmanifestdatei mit dem Namen deployment.yaml. Sie enthält alle Informationen, die SeedFarmer benötigt, um ADDF und seine Ressourcen zu verwalten, bereitzustellen oder zu löschen in der AWS Cloud. Sie können Gruppen von ADDF-Modulen in speziellen Dateien erstellen. Das core-modules.yaml ist ein Beispiel für die Kernmodulgruppe und umfasst alle von ADDF bereitgestellten Kernmodule. Zusammenfassend lässt sich sagen, dass die deployment.yaml-Datei alle Verweise auf die Gruppen

und Module, die für ihre Zielkonten bereitgestellt werden, enthält und die Bereitstellungsreihenfolge angibt.

Für eine sichere und konforme Konfiguration, insbesondere in einer Umgebung, in der es nicht um Machbarkeitsstudien geht, empfehlen wir Ihnen, den Quellcode jedes Moduls, das Sie bereitstellen möchten, zu überprüfen. Gemäß den bewährten Methoden zur Erhöhung der Sicherheit sollten Sie nur Module bereitstellen, die für Ihren beabsichtigten Anwendungsfall erforderlich sind.

> **Note**
>
> ADDF-Module im `modules/demo-only/`-Ordner sind nicht sicherheitsgehärtet und sollten nicht in Produktionsumgebungen oder in Umgebungen mit sensiblen oder geschützten Daten eingesetzt werden. Diese Module sind enthalten, um die Systemfunktionen zu demonstrieren. Sie können sie als Grundlage für die Erstellung Ihrer eigenen maßgeschneiderten, sicherheitsgehärteten Module verwenden.

Anpassen des Codes für das ADDF-Bereitstellungsframework

Das ADDF-Bereitstellungsframework und seine Orchestrierungs- und Bereitstellungslogik können vollständig an alle Anforderungen angepasst werden. Wir empfehlen Ihnen jedoch, entweder auf Anpassungen zu verzichten oder Ihre Änderungen aus den folgenden Gründen zu minimieren:

- Die Upstream-Kompatibilität beibehalten – Die Upstream-Kompatibilität erleichtert die Aktualisierung von ADDF auf die neuesten Features und Sicherheitsupdates. Durch eine Änderung des Frameworks wird die native Abwärtskompatibilität mit SeedFarmer, CodeSeeder und allen ADDF-Kernmodulen beeinträchtigt.
- Konsequenzen für die Sicherheit – Das Ändern des ADDF-Bereitstellungsframeworks kann eine komplexe Aufgabe sein, die unbeabsichtigte Auswirkungen auf die Sicherheit haben kann. Im schlimmsten Fall können Änderungen am Framework zu Schwachstellen führen.

Wenn möglich, sollten Sie Ihren eigenen Modulcode erstellen und anpassen, anstatt das ADDF-Deployment-Framework und den ADDF-Kernmodulcode zu ändern.

> **Note**
>
> Wenn Sie bei der Einrichtung und dem Betrieb von ADDF der Meinung sind, dass das Bereitstellungs-Framework verbessert oder die Sicherheit weiter verschärft werden muss, tragen Sie Ihre Änderungen bitte über eine Pull-Anforderung im ADDF-Repository bei. Weitere Informationen finden Sie unter Open-Source-Sicherheitsüberprüfungen und -Beiträge.

Schreiben von benutzerdefinierten Modulen in ADDF

Die Erstellung eines neuen ADDF-Moduls oder die Erweiterung eines vorhandenen Moduls ist ein Kernkonzept von ADDF. Bei der Erstellung oder Anpassung von Modulen empfehlen wir Ihnen, die allgemeinen bewährten AWS-Sicherheitsmethoden und die bewährten Methoden Ihrer Organisation für eine sichere Codierung zu befolgen. Darüber hinaus empfehlen wir Ihnen, erste und regelmäßige interne oder externe technische Sicherheitsüberprüfungen auf der Grundlage der Sicherheitsanforderungen Ihrer Organisation durchzuführen, um das Risiko von Sicherheitsproblemen weiter zu verringern.

Wiederkehrende ADDF-Bereitstellungen

Stellen Sie ADDF und seine Module wie im ADDF-Bereitstellungshandbuch (GitHub) beschrieben bereit. Um wiederkehrende ADDF-Bereitstellungen zu unterstützen, die Ressourcen in Ihren Zielkonten hinzufügen, aktualisieren oder entfernen, verwendet SeedFarmer MD5-Hashes, die im Parameterspeicher Ihrer Toolchain und Ihrer Zielkonten gespeichert sind, um die aktuell bereitgestellte Infrastruktur mit der Infrastruktur zu vergleichen, die in den Manifestdateien in Ihrer lokalen Codebasis definiert ist.

Dieser Ansatz folgt dem GitOps-Paradigma, bei dem Ihr Quell-Repository (die lokale Codebasis, in der Sie SeedFarmer betreiben) die Quelle der Wahrheit ist und die darin explizit deklarierte Infrastruktur das gewünschte Ergebnis Ihrer Bereitstellung ist. Weitere Informationen zu GitOps finden Sie unter Was ist GitOps (GitLab-Webseite).

Wiederkehrende Sicherheitsprüfungen

Integrieren Sie ADDF und Ihren benutzerdefinierten ADDF-Modulcode wie jede andere Software in Ihrer Organisation in Ihr Sicherheitsrisikomanagement, Ihre Sicherheitsüberprüfung und Ihren Sicherheitsprüfungszyklus.

ADDF-Aktualisierungen

ADDF wird im Rahmen seiner laufenden Entwicklungsanstrengungen regelmäßig aktualisiert. Dazu gehören Featureupdates sowie sicherheitsrelevante Verbesserungen und Korrekturen. Wir empfehlen Ihnen, regelmäßig nach neuen Framework-Versionen zu suchen und Aktualisierungen rechtzeitig zu installieren. Weitere Informationen finden Sie unter Schritte zur Aktualisierung von ADDF (ADDF-Dokumentation).

Außerbetriebnahme

Wenn ADDF nicht mehr benötigt wird, löschen Sie ADDF und alle zugehörigen Ressourcen aus Ihrem AWS-Konten. Jede unbeaufsichtigte und ungenutzte Infrastruktur verursacht unnötige Kosten und stellt ein potenzielles Sicherheitsrisiko dar. Weitere Informationen finden Sie unter Schritte zur Zerstörung von ADDF (ADDF-Dokumentation).

Nächste Schritte

In diesem Leitfaden wurden die bewährten Methoden und Überlegungen zu Sicherheit und Betrieb bei der Bereitstellung des Autonomous Driving Data Framework (ADDF) in Ihrer AWS Cloud-Umgebung. Dieser Leitfaden beschreibt das Modell der geteilten Verantwortung zwischen dem ADDF-Benutzer, dem ADDF-Kernteam und AWS, so dass Sie Ihre Rolle und Verantwortung für die Einrichtung und den sicheren Betrieb von ADDF verstehen. Er enthält auch Empfehlungen für den sicheren Betrieb von ADDF während seines gesamten Lebenszyklus, einschließlich umgebungsspezifischer Empfehlungen.

Wir empfehlen Ihnen, sich mit den Ressourcen im Ressourcen-Abschnitt vertraut zu machen. Wenn Sie bereit sind, können Sie ADDF gemäß den Anweisungen im ADDF-Bereitstellungshandbuch (GitHub) einrichten.

Wenn Sie bei der Einrichtung und dem Betrieb von ADDF der Meinung sind, dass das Bereitstellungs-Framework verbessert oder die Sicherheit weiter verschärft werden muss, tragen Sie Ihre Änderungen bitte über eine Pull-Anforderung in das ADDF-Repository ein. Weitere Informationen finden Sie unter Open-Source-Sicherheitsüberprüfungen und -Beiträge.

Ressourcen

AWS-Dokumentation

- Einen maßgeschneiderten Workflow mit ADDF in AWS entwickeln und bereitstellen (AWS-Blogbeitrag)
- AWS-Sicherheitsservicedokumentation
- Bewährte Methoden für die Sicherheit in IAM
- AWS-Kontoverwaltung und -Trennung
- Bootstrapping für AWS CDK
- AWS-Modell der geteilten Verantwortung
- AWS-Well-Architected-Framework

Open-Source-Ressourcen

- ADDF-Repository (GitHub)
- ADDF-Bereitstellungsleitfaden (GitHub)
- CodeSeeder-Repository (GitHub)
- SeedFarmer-Repository (GitHub)

Hinweise

Kunden sind dafür verantwortlich, Ihre eigene unabhängige Bewertung der Informationen in diesem Dokument vorzunehmen. Dieses Dokument: (a) dient nur zu Informationszwecken, (b) stellt die aktuellen AWS-Produktangebote und -praktiken dar, die ohne Vorankündigung geändert werden können, und (c) begründet keine Verpflichtungen oder Zusicherungen seitens AWS und der mit ihr verbundenen Unternehmen, Lieferanten oder Lizenzgeber. AWS-Produkte oder -Services werden ohne Mängelgewähr bereitgestellt, ohne ausdrückliche oder stillschweigende Garantien, Zusicherungen oder Bedingungen jeglicher Art.

Die Verantwortung und Haftung von AWS gegenüber seinen Kunden werden durch AWS-Vereinbarungen geregelt. Dieses Dokument gehört, weder ganz noch teilweise, nicht zu den Vereinbarung von AWS mit seinen Kunden und ändert diese Vereinbarungen auch nicht.

Dokumentverlauf

In der folgenden Tabelle werden wichtige Änderungen in diesem Leitfaden beschrieben. Um Benachrichtigungen über zukünftige Aktualisierungen zu erhalten, können Sie einen RSS-Feed abonnieren.

Änderung	Beschreibung	Datum
Erste Veröffentlichung	—	15. November 2022

AWS Glossar zu präskriptiven Leitlinien

Im Folgenden finden Sie häufig verwendete Begriffe in Strategien, Leitfäden und Mustern von AWS Prescriptive Guidance. Um Einträge vorzuschlagen, verwenden Sie bitte den Link Feedback geben am Ende des Glossars.

Zahlen

7 Rs

Sieben gängige Migrationsstrategien für die Verlagerung von Anwendungen in die Cloud. Diese Strategien bauen auf den 5 Rs auf, die Gartner 2011 identifiziert hat, und bestehen aus folgenden Elementen:

- Faktorwechsel/Architekturwechsel – Verschieben Sie eine Anwendung und ändern Sie ihre Architektur, indem Sie alle Vorteile cloudnativer Feature nutzen, um Agilität, Leistung und Skalierbarkeit zu verbessern. Dies beinhaltet in der Regel die Portierung des Betriebssystems und der Datenbank. Beispiel: Migrieren Sie Ihre lokale Oracle-Datenbank auf die Amazon Aurora PostgreSQL-kompatible Edition.
- Plattformwechsel (Lift and Reshape) – Verschieben Sie eine Anwendung in die Cloud und führen Sie ein gewisses Maß an Optimierung ein, um die Cloud-Funktionen zu nutzen. Beispiel: Migrieren Sie Ihre lokale Oracle-Datenbank zu Amazon Relational Database Service (Amazon RDS) für Oracle in der. AWS Cloud
- Neukauf (Drop and Shop) – Wechseln Sie zu einem anderen Produkt, indem Sie typischerweise von einer herkömmlichen Lizenz zu einem SaaS-Modell wechseln. Beispiel: Migrieren Sie Ihr CRM-System (Customer Relationship Management) zu Salesforce.com.
- Hostwechsel (Lift and Shift) – Verschieben Sie eine Anwendung in die Cloud, ohne Änderungen vorzunehmen, um die Cloud-Funktionen zu nutzen. Beispiel: Migrieren Sie Ihre lokale Oracle-Datenbank zu Oracle auf einer EC2-Instanz in der. AWS Cloud
- Verschieben (Lift and Shift auf Hypervisor-Ebene) – Verlagern Sie die Infrastruktur in die Cloud, ohne neue Hardware kaufen, Anwendungen umschreiben oder Ihre bestehenden Abläufe ändern zu müssen. Sie migrieren Server von einer lokalen Plattform zu einem Cloud-Dienst für dieselbe Plattform. Beispiel: Migrieren Sie eine Microsoft Hyper-V Anwendung zu AWS.
- Beibehaltung (Wiederaufgreifen) – Bewahren Sie Anwendungen in Ihrer Quellumgebung auf. Dazu können Anwendungen gehören, die einen umfangreichen Faktorwechsel erfordern und

die Sie auf einen späteren Zeitpunkt verschieben möchten, sowie ältere Anwendungen, die Sie beibehalten möchten, da es keine geschäftliche Rechtfertigung für ihre Migration gibt.

- Außerbetriebnahme – Dekommissionierung oder Entfernung von Anwendungen, die in Ihrer Quellumgebung nicht mehr benötigt werden.

A

ABAC

Siehe attributbasierte Zugriffskontrolle.

abstrahierte Dienste

Weitere Informationen finden Sie unter Managed Services.

ACID

Siehe Atomarität, Konsistenz, Isolierung und Haltbarkeit.

Aktiv-Aktiv-Migration

Eine Datenbankmigrationsmethode, bei der die Quell- und Zieldatenbanken synchron gehalten werden (mithilfe eines bidirektionalen Replikationstools oder dualer Schreibvorgänge) und beide Datenbanken Transaktionen von miteinander verbundenen Anwendungen während der Migration verarbeiten. Diese Methode unterstützt die Migration in kleinen, kontrollierten Batches, anstatt einen einmaligen Cutover zu erfordern. Es ist flexibler, erfordert aber mehr Arbeit als eine aktiv-passive Migration.

Aktiv-Passiv-Migration

Eine Datenbankmigrationsmethode, bei der die Quell- und Zieldatenbanken synchron gehalten werden, aber nur die Quelldatenbank Transaktionen von verbindenden Anwendungen verarbeitet, während Daten in die Zieldatenbank repliziert werden. Die Zieldatenbank akzeptiert während der Migration keine Transaktionen.

Aggregatfunktion

Eine SQL-Funktion, die mit einer Gruppe von Zeilen arbeitet und einen einzelnen Rückgabewert für die Gruppe berechnet. Beispiele für Aggregatfunktionen sind `SUM` und`MAX`.

AI

Siehe künstliche Intelligenz.

AIOps

Siehe Operationen mit künstlicher Intelligenz.

Anonymisierung

Der Prozess des dauerhaften Löschens personenbezogener Daten in einem Datensatz. Anonymisierung kann zum Schutz der Privatsphäre beitragen. Anonymisierte Daten gelten nicht mehr als personenbezogene Daten.

Anti-Muster

Eine häufig verwendete Lösung für ein wiederkehrendes Problem, bei dem die Lösung kontraproduktiv, ineffektiv oder weniger wirksam als eine Alternative ist.

Anwendungssteuerung

Ein Sicherheitsansatz, bei dem nur zugelassene Anwendungen verwendet werden können, um ein System vor Schadsoftware zu schützen.

Anwendungsportfolio

Eine Sammlung detaillierter Informationen zu jeder Anwendung, die von einer Organisation verwendet wird, einschließlich der Kosten für die Erstellung und Wartung der Anwendung und ihres Geschäftswerts. Diese Informationen sind entscheidend für den Prozess der Portfoliofindung und -analyse und hilft bei der Identifizierung und Priorisierung der Anwendungen, die migriert, modernisiert und optimiert werden sollen.

künstliche Intelligenz (KI)

Das Gebiet der Datenverarbeitungswissenschaft, das sich der Nutzung von Computertechnologien zur Ausführung kognitiver Funktionen widmet, die typischerweise mit Menschen in Verbindung gebracht werden, wie Lernen, Problemlösen und Erkennen von Mustern. Weitere Informationen finden Sie unter Was ist künstliche Intelligenz?

Operationen mit künstlicher Intelligenz (AIOps)

Der Prozess des Einsatzes von Techniken des Machine Learning zur Lösung betrieblicher Probleme, zur Reduzierung betrieblicher Zwischenfälle und menschlicher Eingriffe sowie zur Steigerung der Servicequalität. Weitere Informationen zur Verwendung von AIOps in der AWS -Migrationsstrategie finden Sie im Leitfaden zur Betriebsintegration.

Asymmetrische Verschlüsselung

Ein Verschlüsselungsalgorithmus, der ein Schlüsselpaar, einen öffentlichen Schlüssel für die Verschlüsselung und einen privaten Schlüssel für die Entschlüsselung verwendet. Sie können den öffentlichen Schlüssel teilen, da er nicht für die Entschlüsselung verwendet wird. Der Zugriff auf den privaten Schlüssel sollte jedoch stark eingeschränkt sein.

Atomizität, Konsistenz, Isolierung, Haltbarkeit (ACID)

Eine Reihe von Softwareeigenschaften, die die Datenvalidität und betriebliche Zuverlässigkeit einer Datenbank auch bei Fehlern, Stromausfällen oder anderen Problemen gewährleisten.

Attributbasierte Zugriffskontrolle (ABAC)

Die Praxis, detaillierte Berechtigungen auf der Grundlage von Benutzerattributen wie Abteilung, Aufgabenrolle und Teamname zu erstellen. Weitere Informationen finden Sie unter ABAC AWS in der AWS Identity and Access Management (IAM-) Dokumentation.

autoritative Datenquelle

Ein Ort, an dem Sie die primäre Version der Daten speichern, die als die zuverlässigste Informationsquelle angesehen wird. Sie können Daten aus der maßgeblichen Datenquelle an andere Speicherorte kopieren, um die Daten zu verarbeiten oder zu ändern, z. B. zu anonymisieren, zu redigieren oder zu pseudonymisieren.

Availability Zone

Ein bestimmter Standort innerhalb einer AWS-Region , der vor Ausfällen in anderen Availability Zones geschützt ist und kostengünstige Netzwerkkonnektivität mit niedriger Latenz zu anderen Availability Zones in derselben Region bietet.

AWS Framework für die Cloud-Einführung (AWS CAF)

Ein Framework mit Richtlinien und bewährten Verfahren, das Unternehmen bei der Entwicklung eines effizienten und effektiven Plans für den erfolgreichen Umstieg auf die Cloud unterstützt. AWS AWS CAF unterteilt die Leitlinien in sechs Schwerpunktbereiche, die als Perspektiven bezeichnet werden: Unternehmen, Mitarbeiter, Unternehmensführung, Plattform, Sicherheit und Betrieb. Die Perspektiven Geschäft, Mitarbeiter und Unternehmensführung konzentrieren sich auf Geschäftskompetenzen und -prozesse, während sich die Perspektiven Plattform, Sicherheit und Betriebsabläufe auf technische Fähigkeiten und Prozesse konzentrieren. Die Personalperspektive zielt beispielsweise auf Stakeholder ab, die sich mit Personalwesen (HR), Personalfunktionen und Personalmanagement befassen. Aus dieser Perspektive bietet AWS CAF Leitlinien für Personalentwicklung, Schulung und Kommunikation, um das Unternehmen auf eine erfolgreiche

Cloud-Einführung vorzubereiten. Weitere Informationen finden Sie auf der AWS -CAF-Webseite und dem AWS -CAF-Whitepaper.

AWS Workload-Qualifizierungsrahmen (AWS WQF)

Ein Tool, das Workloads bei der Datenbankmigration bewertet, Migrationsstrategien empfiehlt und Arbeitsschätzungen bereitstellt. AWS WQF ist in () enthalten. AWS Schema Conversion Tool AWS SCT Es analysiert Datenbankschemas und Codeobjekte, Anwendungscode, Abhängigkeiten und Leistungsmerkmale und stellt Bewertungsberichte bereit.

B

schlechter Bot

Ein Bot, der Einzelpersonen oder Organisationen stören oder ihnen Schaden zufügen soll.

BCP

Siehe Planung der Geschäftskontinuität.

Verhaltensdiagramm

Eine einheitliche, interaktive Ansicht des Ressourcenverhaltens und der Interaktionen im Laufe der Zeit. Sie können ein Verhaltensdiagramm mit Amazon Detective verwenden, um fehlgeschlagene Anmeldeversuche, verdächtige API-Aufrufe und ähnliche Vorgänge zu untersuchen. Weitere Informationen finden Sie unter Daten in einem Verhaltensdiagramm in der Detective-Dokumentation.

Big-Endian-System

Ein System, welches das höchstwertige Byte zuerst speichert. Siehe auch Endianness.

Binäre Klassifikation

Ein Prozess, der ein binäres Ergebnis vorhersagt (eine von zwei möglichen Klassen). Beispielsweise könnte Ihr ML-Modell möglicherweise Probleme wie „Handelt es sich bei dieser E-Mail um Spam oder nicht?“ vorhersagen müssen oder „Ist dieses Produkt ein Buch oder ein Auto?“

Bloom-Filter

Eine probabilistische, speichereffiziente Datenstruktur, mit der getestet wird, ob ein Element Teil einer Menge ist.

Blau/Grün-Bereitstellung

Eine Bereitstellungsstrategie, bei der Sie zwei separate, aber identische Umgebungen erstellen. Sie führen die aktuelle Anwendungsversion in einer Umgebung (blau) und die neue Anwendungsversion in der anderen Umgebung (grün) aus. Mit dieser Strategie können Sie schnell und mit minimalen Auswirkungen ein Rollback durchführen.

Bot

Eine Softwareanwendung, die automatisierte Aufgaben über das Internet ausführt und menschliche Aktivitäten oder Interaktionen simuliert. Manche Bots sind nützlich oder nützlich, wie z. B. Webcrawler, die Informationen im Internet indexieren. Einige andere Bots, die als bösartige Bots bezeichnet werden, sollen Einzelpersonen oder Organisationen stören oder ihnen Schaden zufügen.

Botnetz

Netzwerke von Bots, die mit Malware infiziert sind und unter der Kontrolle einer einzigen Partei stehen, die als Bot-Herder oder Bot-Operator bezeichnet wird. Botnetze sind der bekannteste Mechanismus zur Skalierung von Bots und ihrer Wirkung.

branch

Ein containerisierter Bereich eines Code-Repositorys. Der erste Zweig, der in einem Repository erstellt wurde, ist der Hauptzweig. Sie können einen neuen Zweig aus einem vorhandenen Zweig erstellen und dann Feature entwickeln oder Fehler in dem neuen Zweig beheben. Ein Zweig, den Sie erstellen, um ein Feature zu erstellen, wird allgemein als Feature-Zweig bezeichnet. Wenn das Feature zur Veröffentlichung bereit ist, führen Sie den Feature-Zweig wieder mit dem Hauptzweig zusammen. Weitere Informationen finden Sie unter Über Branches (GitHub Dokumentation).

Zugang durch Glasbruch

Unter außergewöhnlichen Umständen und im Rahmen eines genehmigten Verfahrens ist dies eine schnelle Methode für einen Benutzer, auf einen Bereich zuzugreifen AWS-Konto , für den er normalerweise keine Zugriffsrechte besitzt. Weitere Informationen finden Sie unter dem Indikator Implementation break-glass procedures in den AWS Well-Architected-Leitlinien.

Brownfield-Strategie

Die bestehende Infrastruktur in Ihrer Umgebung. Wenn Sie eine Brownfield-Strategie für eine Systemarchitektur anwenden, richten Sie sich bei der Gestaltung der Architektur nach den

Einschränkungen der aktuellen Systeme und Infrastruktur. Wenn Sie die bestehende Infrastruktur erweitern, könnten Sie Brownfield- und Greenfield-Strategien mischen.

Puffer-Cache

Der Speicherbereich, in dem die am häufigsten abgerufenen Daten gespeichert werden.

Geschäftsfähigkeit

Was ein Unternehmen tut, um Wert zu generieren (z. B. Vertrieb, Kundenservice oder Marketing). Microservices-Architekturen und Entwicklungsentscheidungen können von den Geschäftskapazitäten beeinflusst werden. Weitere Informationen finden Sie im Abschnitt Organisiert nach Geschäftskapazitäten des Whitepapers Ausführen von containerisierten Microservices in AWS.

Planung der Geschäftskontinuität (BCP)

Ein Plan, der die potenziellen Auswirkungen eines störenden Ereignisses, wie z. B. einer groß angelegten Migration, auf den Betrieb berücksichtigt und es einem Unternehmen ermöglicht, den Betrieb schnell wieder aufzunehmen.

C

CAF

Weitere Informationen finden Sie unter Framework für die AWS Cloud-Einführung.

Bereitstellung auf Kanaren

Die langsame und schrittweise Veröffentlichung einer Version für Endbenutzer. Wenn Sie sich sicher sind, stellen Sie die neue Version bereit und ersetzen die aktuelle Version vollständig.

CCoE

Weitere Informationen finden Sie im Cloud Center of Excellence.

CDC

Siehe Erfassung von Änderungsdaten.

Erfassung von Datenänderungen (CDC)

Der Prozess der Nachverfolgung von Änderungen an einer Datenquelle, z. B. einer Datenbanktabelle, und der Aufzeichnung von Metadaten zu der Änderung. Sie können CDC für

verschiedene Zwecke verwenden, z. B. für die Prüfung oder Replikation von Änderungen in einem Zielsystem, um die Synchronisation aufrechtzuerhalten.

Chaos-Technik

Absichtliches Einführen von Ausfällen oder Störungsereignissen, um die Widerstandsfähigkeit eines Systems zu testen. Sie können AWS Fault Injection Service (AWS FIS) verwenden, um Experimente durchzuführen, die Ihre AWS Workloads stress, und deren Reaktion zu bewerten.

CI/CD

Siehe Continuous Integration und Continuous Delivery.

Klassifizierung

Ein Kategorisierungsprozess, der bei der Erstellung von Vorhersagen hilft. ML-Modelle für Klassifikationsprobleme sagen einen diskreten Wert voraus. Diskrete Werte unterscheiden sich immer voneinander. Beispielsweise muss ein Modell möglicherweise auswerten, ob auf einem Bild ein Auto zu sehen ist oder nicht.

clientseitige Verschlüsselung

Lokale Verschlüsselung von Daten, bevor das Ziel sie AWS-Service empfängt.

Cloud-Kompetenzzentrum (CCoE)

Ein multidisziplinäres Team, das die Cloud-Einführung in der gesamten Organisation vorantreibt, einschließlich der Entwicklung bewährter Cloud-Methoden, der Mobilisierung von Ressourcen, der Festlegung von Migrationszeitplänen und der Begleitung der Organisation durch groß angelegte Transformationen. Weitere Informationen finden Sie in den CCoE-Beiträgen im AWS Cloud Enterprise Strategy Blog.

Cloud Computing

Die Cloud-Technologie, die typischerweise für die Ferndatenspeicherung und das IoT-Gerätemanagement verwendet wird. Cloud Computing ist häufig mit Edge-Computing-Technologie verbunden.

Cloud-Betriebsmodell

In einer IT-Organisation das Betriebsmodell, das zum Aufbau, zur Weiterentwicklung und Optimierung einer oder mehrerer Cloud-Umgebungen verwendet wird. Weitere Informationen finden Sie unter Aufbau Ihres Cloud-Betriebsmodells.

Phasen der Einführung der Cloud

Die vier Phasen, die Unternehmen bei der Migration in der Regel durchlaufen AWS Cloud:

- Projekt – Durchführung einiger Cloud-bezogener Projekte zu Machbarkeitsnachweisen und zu Lernzwecken
- Fundament – Grundlegende Investitionen tätigen, um Ihre Cloud-Einführung zu skalieren (z. B. Einrichtung einer Landing Zone, Definition eines CCoE, Einrichtung eines Betriebsmodells)
- Migration – Migrieren einzelner Anwendungen
- Neuentwicklung – Optimierung von Produkten und Services und Innovation in der Cloud

Diese Phasen wurden von Stephen Orban im Blogbeitrag The Journey Toward Cloud-First & the Stages of Adoption im AWS Cloud Enterprise Strategy-Blog definiert. Informationen darüber, wie sie mit der AWS Migrationsstrategie zusammenhängen, finden Sie im Leitfaden zur Vorbereitung der Migration.

CMDB

Siehe Datenbank für das Konfigurationsmanagement.

Code-Repository

Ein Ort, an dem Quellcode und andere Komponenten wie Dokumentation, Beispiele und Skripts gespeichert und im Rahmen von Versionskontrollprozessen aktualisiert werden. Zu den gängigen Cloud-Repositorys gehören GitHub oder AWS CodeCommit. Jede Version des Codes wird Zweig genannt. In einer Microservice-Struktur ist jedes Repository einer einzelnen Funktionalität gewidmet. Eine einzelne CI/CD-Pipeline kann mehrere Repositorien verwenden.

Kalter Cache

Ein Puffer-Cache, der leer oder nicht gut gefüllt ist oder veraltete oder irrelevante Daten enthält. Dies beeinträchtigt die Leistung, da die Datenbank-Instance aus dem Hauptspeicher oder der Festplatte lesen muss, was langsamer ist als das Lesen aus dem Puffercache.

Kalte Daten

Daten, auf die selten zugegriffen wird und die in der Regel historisch sind. Bei der Abfrage dieser Art von Daten sind langsame Abfragen in der Regel akzeptabel. Durch die Verlagerung dieser Daten auf leistungsschwächere und kostengünstigere Speicherstufen oder -klassen können Kosten gesenkt werden.

Computer Vision (CV)

Ein Bereich der KI, der maschinelles Lernen nutzt, um Informationen aus visuellen Formaten wie digitalen Bildern und Videos zu analysieren und zu extrahieren. AWS Panorama Bietet beispielsweise Geräte an, die CV zu lokalen Kameranetzwerken hinzufügen, und Amazon SageMaker stellt Bildverarbeitungsalgorithmen für CV bereit.

Drift in der Konfiguration

Bei einer Arbeitslast eine Änderung der Konfiguration gegenüber dem erwarteten Zustand. Dies kann dazu führen, dass der Workload nicht mehr richtlinienkonform wird, und zwar in der Regel schrittweise und unbeabsichtigt.

Verwaltung der Datenbankkonfiguration (CMDB)

Ein Repository, das Informationen über eine Datenbank und ihre IT-Umgebung speichert und verwaltet, inklusive Hardware- und Softwarekomponenten und deren Konfigurationen. In der Regel verwenden Sie Daten aus einer CMDB in der Phase der Portfolioerkennung und -analyse der Migration.

Konformitätspaket

Eine Sammlung von AWS Config Regeln und Abhilfemaßnahmen, die Sie zusammenstellen können, um Ihre Konformitäts- und Sicherheitsprüfungen individuell anzupassen. Mithilfe einer YAML-Vorlage können Sie ein Conformance Pack als einzelne Entität in einer AWS-Konto AND-Region oder unternehmensweit bereitstellen. Weitere Informationen finden Sie in der Dokumentation unter Conformance Packs. AWS Config

Kontinuierliche Bereitstellung und kontinuierliche Integration (CI/CD)

Der Prozess der Automatisierung der Quell-, Build-, Test-, Staging- und Produktionsphasen des Softwareveröffentlichungsprozesses. CI/CD wird allgemein als Pipeline beschrieben. CI/CD kann Ihnen helfen, Prozesse zu automatisieren, die Produktivität zu steigern, die Codequalität zu verbessern und schneller zu liefern. Weitere Informationen finden Sie unter Vorteile der kontinuierlichen Auslieferung. CD kann auch für kontinuierliche Bereitstellung stehen. Weitere Informationen finden Sie unterKontinuierliche Auslieferung im Vergleich zu kontinuierlicher Bereitstellung.

CV

Siehe Computer Vision.

D

Daten im Ruhezustand

Daten, die in Ihrem Netzwerk stationär sind, z. B. Daten, die sich im Speicher befinden.

Datenklassifizierung

Ein Prozess zur Identifizierung und Kategorisierung der Daten in Ihrem Netzwerk auf der Grundlage ihrer Kritikalität und Sensitivität. Sie ist eine wichtige Komponente jeder Strategie für das Management von Cybersecurity-Risiken, da sie Ihnen hilft, die geeigneten Schutz- und Aufbewahrungskontrollen für die Daten zu bestimmen. Die Datenklassifizierung ist ein Bestandteil der Sicherheitssäule im AWS Well-Architected Framework. Weitere Informationen finden Sie unter Datenklassifizierung.

Datendrift

Eine signifikante Abweichung zwischen den Produktionsdaten und den Daten, die zum Trainieren eines ML-Modells verwendet wurden, oder eine signifikante Änderung der Eingabedaten im Laufe der Zeit. Datendrift kann die Gesamtqualität, Genauigkeit und Fairness von ML-Modellvorhersagen beeinträchtigen.

Daten während der Übertragung

Daten, die sich aktiv durch Ihr Netzwerk bewegen, z. B. zwischen Netzwerkressourcen.

Datennetz

Ein architektonisches Framework, das verteilte, dezentrale Dateneigentum mit zentraler Verwaltung und Steuerung ermöglicht.

Datenminimierung

Das Prinzip, nur die Daten zu sammeln und zu verarbeiten, die unbedingt erforderlich sind. Durch Datenminimierung im AWS Cloud können Datenschutzrisiken, Kosten und der CO2-Fußabdruck Ihrer Analysen reduziert werden.

Datenperimeter

Eine Reihe präventiver Schutzmaßnahmen in Ihrer AWS Umgebung, die sicherstellen, dass nur vertrauenswürdige Identitäten auf vertrauenswürdige Ressourcen von erwarteten Netzwerken zugreifen. Weitere Informationen finden Sie unter Aufbau eines Datenperimeters auf. AWS

Vorverarbeitung der Daten

Rohdaten in ein Format umzuwandeln, das von Ihrem ML-Modell problemlos verarbeitet werden kann. Die Vorverarbeitung von Daten kann bedeuten, dass bestimmte Spalten oder Zeilen entfernt und fehlende, inkonsistente oder doppelte Werte behoben werden.

Herkunft der Daten

Der Prozess der Nachverfolgung des Ursprungs und der Geschichte von Daten während ihres gesamten Lebenszyklus, z. B. wie die Daten generiert, übertragen und gespeichert wurden.

betroffene Person

Eine Person, deren Daten gesammelt und verarbeitet werden.

Data Warehouse

Ein Datenverwaltungssystem, das Business Intelligence wie Analysen unterstützt. Data Warehouses enthalten in der Regel große Mengen an historischen Daten und werden in der Regel für Abfragen und Analysen verwendet.

Datenbankdefinitionssprache (DDL)

Anweisungen oder Befehle zum Erstellen oder Ändern der Struktur von Tabellen und Objekten in einer Datenbank.

Datenbankmanipulationssprache (DML)

Anweisungen oder Befehle zum Ändern (Einfügen, Aktualisieren und Löschen) von Informationen in einer Datenbank.

DDL

Siehe Datenbankdefinitionssprache.

Deep-Ensemble

Mehrere Deep-Learning-Modelle zur Vorhersage kombinieren. Sie können Deep-Ensembles verwenden, um eine genauere Vorhersage zu erhalten oder um die Unsicherheit von Vorhersagen abzuschätzen.

Deep Learning

Ein ML-Teilbereich, der mehrere Schichten künstlicher neuronaler Netzwerke verwendet, um die Zuordnung zwischen Eingabedaten und Zielvariablen von Interesse zu ermitteln.

defense-in-depth

Ein Ansatz zur Informationssicherheit, bei dem eine Reihe von Sicherheitsmechanismen und -kontrollen sorgfältig in einem Computernetzwerk verteilt werden, um die Vertraulichkeit, Integrität und Verfügbarkeit des Netzwerks und der darin enthaltenen Daten zu schützen. Wenn Sie diese Strategie anwenden AWS, fügen Sie mehrere Steuerelemente auf verschiedenen Ebenen der AWS Organizations Struktur hinzu, um die Ressourcen zu schützen. Ein defense-in-depth Ansatz könnte beispielsweise Multi-Faktor-Authentifizierung, Netzwerksegmentierung und Verschlüsselung kombinieren.

delegierter Administrator

In AWS Organizations kann ein kompatibler Dienst ein AWS Mitgliedskonto registrieren, um die Konten der Organisation und die Berechtigungen für diesen Dienst zu verwalten. Dieses Konto wird als delegierter Administrator für diesen Service bezeichnet. Weitere Informationen und eine Liste kompatibler Services finden Sie unter Services, die mit AWS Organizations funktionieren in der AWS Organizations -Dokumentation.

Bereitstellung

Der Prozess, bei dem eine Anwendung, neue Feature oder Codekorrekturen in der Zielumgebung verfügbar gemacht werden. Die Bereitstellung umfasst das Implementieren von Änderungen an einer Codebasis und das anschließende Erstellen und Ausführen dieser Codebasis in den Anwendungsumgebungen.

Entwicklungsumgebung

Siehe Umgebung.

Detektivische Kontrolle

Eine Sicherheitskontrolle, die darauf ausgelegt ist, ein Ereignis zu erkennen, zu protokollieren und zu warnen, nachdem ein Ereignis eingetreten ist. Diese Kontrollen stellen eine zweite Verteidigungslinie dar und warnen Sie vor Sicherheitsereignissen, bei denen die vorhandenen präventiven Kontrollen umgangen wurden. Weitere Informationen finden Sie unter Detektivische Kontrolle in Implementierung von Sicherheitskontrollen in AWS.

Abbildung des Wertstroms in der Entwicklung (DVSM)

Ein Prozess zur Identifizierung und Priorisierung von Einschränkungen, die sich negativ auf Geschwindigkeit und Qualität im Lebenszyklus der Softwareentwicklung auswirken. DVSM erweitert den Prozess der Wertstromanalyse, der ursprünglich für Lean-Manufacturing-Praktiken

konzipiert wurde. Es konzentriert sich auf die Schritte und Teams, die erforderlich sind, um durch den Softwareentwicklungsprozess Mehrwert zu schaffen und zu steigern.

digitaler Zwilling

Eine virtuelle Darstellung eines realen Systems, z. B. eines Gebäudes, einer Fabrik, einer Industrieanlage oder einer Produktionslinie. Digitale Zwillinge unterstützen vorausschauende Wartung, Fernüberwachung und Produktionsoptimierung.

Maßtabelle

In einem Sternschema eine kleinere Tabelle, die Datenattribute zu quantitativen Daten in einer Faktentabelle enthält. Bei Attributen von Dimensionstabellen handelt es sich in der Regel um Textfelder oder diskrete Zahlen, die sich wie Text verhalten. Diese Attribute werden häufig zum Einschränken von Abfragen, zum Filtern und zur Kennzeichnung von Ergebnismengen verwendet.

Katastrophe

Ein Ereignis, das verhindert, dass ein Workload oder ein System seine Geschäftsziele an seinem primären Einsatzort erfüllt. Diese Ereignisse können Naturkatastrophen, technische Ausfälle oder das Ergebnis menschlichen Handelns sein, z. B. unbeabsichtigte Fehlkonfigurationen oder Malware-Angriffe.

Notfallwiederherstellung (DR)

Die Strategie und der Prozess, die Sie zur Minimierung von Ausfallzeiten und Datenverlusten aufgrund einer Katastrophe anwenden. Weitere Informationen finden Sie unter Disaster Recovery von Workloads unter AWS: Wiederherstellung in der Cloud im AWS Well-Architected Framework.

DML

Siehe Sprache zur Datenbankmanipulation.

Domainorientiertes Design

Ein Ansatz zur Entwicklung eines komplexen Softwaresystems, bei dem seine Komponenten mit sich entwickelnden Domains oder Kerngeschäftszielen verknüpft werden, denen jede Komponente dient. Dieses Konzept wurde von Eric Evans in seinem Buch Domaingesteuertes Design: Bewältigen der Komplexität im Herzen der Software (Boston: Addison-Wesley Professional, 2003) vorgestellt. Informationen darüber, wie Sie domaingesteuertes Design mit dem Strangler-Fig-Muster verwenden können, finden Sie unter Schrittweises Modernisieren älterer Microsoft ASP.NET (ASMX)-Webservices mithilfe von Containern und Amazon API Gateway.

DR

Siehe Disaster Recovery.

Erkennung von Driften

Verfolgung von Abweichungen von einer Basiskonfiguration Sie können es beispielsweise verwenden, AWS CloudFormation um Abweichungen bei den Systemressourcen zu erkennen, oder Sie können AWS Control Tower damit Änderungen in Ihrer landing zone erkennen, die sich auf die Einhaltung von Governance-Anforderungen auswirken könnten.

DVSM

Siehe Abbildung des Wertstroms in der Entwicklung.

E

EDA

Siehe explorative Datenanalyse.

Edge-Computing

Die Technologie, die die Rechenleistung für intelligente Geräte an den Rändern eines IoT-Netzwerks erhöht. Im Vergleich zu Cloud Computing kann Edge Computing die Kommunikationslatenz reduzieren und die Reaktionszeit verbessern.

Verschlüsselung

Ein Rechenprozess, der Klartextdaten, die für Menschen lesbar sind, in Chiffretext umwandelt.

Verschlüsselungsschlüssel

Eine kryptografische Zeichenfolge aus zufälligen Bits, die von einem Verschlüsselungsalgorithmus generiert wird. Schlüssel können unterschiedlich lang sein, und jeder Schlüssel ist so konzipiert, dass er unvorhersehbar und einzigartig ist.

Endianismus

Die Reihenfolge, in der Bytes im Computerspeicher gespeichert werden. Big-Endian-Systeme speichern das höchstwertige Byte zuerst. Little-Endian-Systeme speichern das niedrigwertigste Byte zuerst.

Endpunkt

Siehe Service-Endpunkt.

Endpunkt-Services

Ein Service, den Sie in einer Virtual Private Cloud (VPC) hosten können, um ihn mit anderen Benutzern zu teilen. Sie können einen Endpunktdienst mit anderen AWS-Konten oder AWS Identity and Access Management (IAM AWS PrivateLink -) Prinzipalen erstellen und diesen Berechtigungen gewähren. Diese Konten oder Prinzipale können sich privat mit Ihrem Endpunktservice verbinden, indem sie Schnittstellen-VPC-Endpunkte erstellen. Weitere Informationen finden Sie unter Einen Endpunkt-Service erstellen in der Amazon Virtual Private Cloud (Amazon VPC)-Dokumentation.

Unternehmensressourcenplanung (ERP)

Ein System, das wichtige Geschäftsprozesse (wie Buchhaltung, MES und Projektmanagement) für ein Unternehmen automatisiert und verwaltet.

Envelope-Verschlüsselung

Der Prozess der Verschlüsselung eines Verschlüsselungsschlüssels mit einem anderen Verschlüsselungsschlüssel. Weitere Informationen finden Sie unter Envelope-Verschlüsselung in der AWS Key Management Service (AWS KMS) -Dokumentation.

Umgebung

Eine Instance einer laufenden Anwendung. Die folgenden Arten von Umgebungen sind beim Cloud-Computing üblich:

- Entwicklungsumgebung – Eine Instance einer laufenden Anwendung, die nur dem Kernteam zur Verfügung steht, das für die Wartung der Anwendung verantwortlich ist. Entwicklungsumgebungen werden verwendet, um Änderungen zu testen, bevor sie in höhere Umgebungen übertragen werden. Diese Art von Umgebung wird manchmal als Testumgebung bezeichnet.
- Niedrigere Umgebungen – Alle Entwicklungsumgebungen für eine Anwendung, z. B. solche, die für erste Builds und Tests verwendet wurden.
- Produktionsumgebung – Eine Instance einer laufenden Anwendung, auf die Endbenutzer zugreifen können. In einer CI/CD-Pipeline ist die Produktionsumgebung die letzte Bereitstellungsumgebung.

- Höhere Umgebungen – Alle Umgebungen, auf die auch andere Benutzer als das Kernentwicklungsteam zugreifen können. Dies kann eine Produktionsumgebung, Vorproduktionsumgebungen und Umgebungen für Benutzerakzeptanztests umfassen.

Epics

In der agilen Methodik sind dies funktionale Kategorien, die Ihnen helfen, Ihre Arbeit zu organisieren und zu priorisieren. Epics bieten eine allgemeine Beschreibung der Anforderungen und Implementierungsaufgaben. Zu den Sicherheitsthemen AWS von CAF gehören beispielsweise Identitäts- und Zugriffsmanagement, Detektivkontrollen, Infrastruktursicherheit, Datenschutz und Reaktion auf Vorfälle. Weitere Informationen zu Epics in der AWS - Migrationsstrategie finden Sie im Leitfaden zur Programm-Implementierung.

ERP

Siehe Enterprise Resource Planning.

Explorative Datenanalyse (EDA)

Der Prozess der Analyse eines Datensatzes, um seine Hauptmerkmale zu verstehen. Sie sammeln oder aggregieren Daten und führen dann erste Untersuchungen durch, um Muster zu finden, Anomalien zu erkennen und Annahmen zu überprüfen. EDA wird durchgeführt, indem zusammenfassende Statistiken berechnet und Datenvisualisierungen erstellt werden.

F

Faktentabelle

Die zentrale Tabelle in einem Sternschema. Sie speichert quantitative Daten über den Geschäftsbetrieb. In der Regel enthält eine Faktentabelle zwei Arten von Spalten: Spalten, die Kennzahlen enthalten, und Spalten, die einen Fremdschlüssel für eine Dimensionstabelle enthalten.

schnell scheitern

Eine Philosophie, die häufige und inkrementelle Tests verwendet, um den Entwicklungslebenszyklus zu verkürzen. Dies ist ein wichtiger Bestandteil eines agilen Ansatzes.

Grenze zur Fehlerisolierung

Dabei handelt es sich um eine Grenze AWS Cloud, z. B. eine Availability Zone AWS-Region, eine Steuerungsebene oder eine Datenebene, die die Auswirkungen eines Fehlers begrenzt und die

Widerstandsfähigkeit von Workloads verbessert. Weitere Informationen finden Sie unter Grenzen zur AWS Fehlerisolierung.

Feature-Zweig

Siehe Zweig.

Features

Die Eingabedaten, die Sie verwenden, um eine Vorhersage zu treffen. In einem Fertigungskontext könnten Feature beispielsweise Bilder sein, die regelmäßig von der Fertigungslinie aus aufgenommen werden.

Bedeutung der Feature

Wie wichtig ein Feature für die Vorhersagen eines Modells ist. Dies wird in der Regel als numerischer Wert ausgedrückt, der mit verschiedenen Techniken wie Shapley Additive Explanations (SHAP) und integrierten Gradienten berechnet werden kann. Weitere Informationen finden Sie unter Interpretierbarkeit von Modellen für maschinelles Lernen mit:AWS.

Featuretransformation

Daten für den ML-Prozess optimieren, einschließlich der Anreicherung von Daten mit zusätzlichen Quellen, der Skalierung von Werten oder der Extraktion mehrerer Informationssätze aus einem einzigen Datenfeld. Das ermöglicht dem ML-Modell, von den Daten profitieren. Wenn Sie beispielsweise das Datum „27.05.2021 00:15:37“ in „2021“, „Mai“, „Donnerstag“ und „15“ aufschlüsseln, können Sie dem Lernalgorithmus helfen, nuancierte Muster zu erlernen, die mit verschiedenen Datenkomponenten verknüpft sind.

FGAC

Weitere Informationen finden Sie unter detaillierter Zugriffskontrolle.

Feinkörnige Zugriffskontrolle (FGAC)

Die Verwendung mehrerer Bedingungen, um eine Zugriffsanfrage zuzulassen oder abzulehnen.

Flash-Cut-Migration

Eine Datenbankmigrationsmethode, bei der eine kontinuierliche Datenreplikation durch Erfassung von Änderungsdaten verwendet wird, um Daten in kürzester Zeit zu migrieren, anstatt einen schrittweisen Ansatz zu verwenden. Ziel ist es, Ausfallzeiten auf ein Minimum zu beschränken.

G

Geoblocking

Siehe geografische Einschränkungen.

Geografische Einschränkungen (Geoblocking)

Bei Amazon eine Option CloudFront, um zu verhindern, dass Benutzer in bestimmten Ländern auf Inhaltsverteilungen zugreifen. Sie können eine Zulassungsliste oder eine Sperrliste verwenden, um zugelassene und gesperrte Länder anzugeben. Weitere Informationen finden Sie in der Dokumentation unter Beschränkung der geografischen Verteilung Ihrer Inhalte. CloudFront

Gitflow-Workflow

Ein Ansatz, bei dem niedrigere und höhere Umgebungen unterschiedliche Zweige in einem Quellcode-Repository verwenden. Der Gitflow-Workflow gilt als veraltet, und der Trunk-basierte Workflow ist der moderne, bevorzugte Ansatz.

Greenfield-Strategie

Das Fehlen vorhandener Infrastruktur in einer neuen Umgebung. Bei der Einführung einer Neuausrichtung einer Systemarchitektur können Sie alle neuen Technologien ohne Einschränkung der Kompatibilität mit der vorhandenen Infrastruktur auswählen, auch bekannt als Brownfield. Wenn Sie die bestehende Infrastruktur erweitern, könnten Sie Brownfield- und Greenfield-Strategien mischen.

Integritätsschutz

Eine allgemeine Regel, die dabei hilft, Ressourcen, Richtlinien und die Einhaltung von Vorschriften in allen Organisationseinheiten (OUs) zu regeln. Präventiver Integritätsschutz setzt Richtlinien durch, um die Einhaltung von Standards zu gewährleisten. Sie werden mithilfe von Service-Kontrollrichtlinien und IAM-Berechtigungsgrenzen implementiert. Detektivischer Integritätsschutz erkennt Richtlinienverstöße und Compliance-Probleme und generiert Warnmeldungen zur Abhilfe. Sie werden mithilfe von AWS Config, AWS Security Hub, Amazon GuardDuty AWS Trusted Advisor, Amazon Inspector und benutzerdefinierten AWS Lambda Prüfungen implementiert.

H

HEKTAR

Siehe Hochverfügbarkeit.

Heterogene Datenbankmigration

Migrieren Sie Ihre Quelldatenbank in eine Zieldatenbank, die eine andere Datenbank-Engine verwendet (z. B. Oracle zu Amazon Aurora). Eine heterogene Migration ist in der Regel Teil einer Neuarchitektur, und die Konvertierung des Schemas kann eine komplexe Aufgabe sein. AWS bietet AWS SCT, welches bei Schemakonvertierungen hilft.

hohe Verfügbarkeit (HA)

Die Fähigkeit eines Workloads, im Falle von Herausforderungen oder Katastrophen kontinuierlich und ohne Eingreifen zu arbeiten. HA-Systeme sind so konzipiert, dass sie automatisch ein Failover durchführen, gleichbleibend hohe Leistung bieten und unterschiedliche Lasten und Ausfälle mit minimalen Leistungseinbußen bewältigen.

historische Modernisierung

Ein Ansatz zur Modernisierung und Aufrüstung von Betriebstechnologiesystemen (OT), um den Bedürfnissen der Fertigungsindustrie besser gerecht zu werden. Ein Historian ist eine Art von Datenbank, die verwendet wird, um Daten aus verschiedenen Quellen in einer Fabrik zu sammeln und zu speichern.

Homogene Datenbankmigration

Migrieren Sie Ihre Quelldatenbank zu einer Zieldatenbank, die dieselbe Datenbank-Engine verwendet (z. B. Microsoft SQL Server zu Amazon RDS für SQL Server). Eine homogene Migration ist in der Regel Teil eines Hostwechsels oder eines Plattformwechsels. Sie können native Datenbankserviceprogramme verwenden, um das Schema zu migrieren.

heiße Daten

Daten, auf die häufig zugegriffen wird, z. B. Echtzeitdaten oder aktuelle Translationsdaten. Für diese Daten ist in der Regel eine leistungsstarke Speicherebene oder -klasse erforderlich, um schnelle Abfrageantworten zu ermöglichen.

Hotfix

Eine dringende Lösung für ein kritisches Problem in einer Produktionsumgebung. Aufgrund seiner Dringlichkeit wird ein Hotfix normalerweise außerhalb des typischen DevOps Release-Workflows erstellt.

Hypercare-Phase

Unmittelbar nach dem Cutover, der Zeitraum, in dem ein Migrationsteam die migrierten Anwendungen in der Cloud verwaltet und überwacht, um etwaige Probleme zu beheben. In der Regel dauert dieser Zeitraum 1–4 Tage. Am Ende der Hypercare-Phase überträgt das Migrationsteam in der Regel die Verantwortung für die Anwendungen an das Cloud-Betriebsteam.

I

IaC

Sehen Sie sich Infrastruktur als Code an.

Identitätsbasierte Richtlinie

Eine Richtlinie, die einem oder mehreren IAM-Prinzipalen zugeordnet ist und deren Berechtigungen innerhalb der AWS Cloud Umgebung definiert.

Leerlaufanwendung

Eine Anwendung mit einer durchschnittlichen CPU- und Arbeitsspeicherauslastung zwischen 5 und 20 Prozent über einen Zeitraum von 90 Tagen. In einem Migrationsprojekt ist es üblich, diese Anwendungen außer Betrieb zu nehmen oder sie On-Premises beizubehalten.

IIoT

Siehe Industrielles Internet der Dinge.

unveränderliche Infrastruktur

Ein Modell, das eine neue Infrastruktur für Produktionsworkloads bereitstellt, anstatt die bestehende Infrastruktur zu aktualisieren, zu patchen oder zu modifizieren. Unveränderliche Infrastrukturen sind von Natur aus konsistenter, zuverlässiger und vorhersehbarer als veränderliche Infrastrukturen. Weitere Informationen finden Sie in der Best Practice Deploy using immutable infrastructure im AWS Well-Architected Framework.

Eingehende (ingress) VPC

In einer Architektur AWS mit mehreren Konten ist dies eine VPC, die Netzwerkverbindungen von außerhalb einer Anwendung akzeptiert, überprüft und weiterleitet. Die AWS -Referenzarchitektur für die Sicherheit empfiehlt, Ihr Netzwerkkonto mit eingehenden und ausgehenden VPCs und Inspektions-VPCs einzurichten, um die bidirektionale Schnittstelle zwischen Ihrer Anwendung und dem Internet zu schützen.

Inkrementelle Migration

Eine Cutover-Strategie, bei der Sie Ihre Anwendung in kleinen Teilen migrieren, anstatt eine einziges vollständiges Cutover durchzuführen. Beispielsweise könnten Sie zunächst nur einige Microservices oder Benutzer auf das neue System umstellen. Nachdem Sie sich vergewissert haben, dass alles ordnungsgemäß funktioniert, können Sie weitere Microservices oder Benutzer schrittweise verschieben, bis Sie Ihr Legacy-System außer Betrieb nehmen können. Diese Strategie reduziert die mit großen Migrationen verbundenen Risiken.

Industrie 4.0

Ein Begriff, der 2016 von Klaus Schwab eingeführt wurde und sich auf die Modernisierung von Fertigungsprozessen durch Fortschritte in den Bereichen Konnektivität, Echtzeitdaten, Automatisierung, Analytik und KI/ML bezieht.

Infrastruktur

Alle Ressourcen und Komponenten, die in der Umgebung einer Anwendung enthalten sind.

Infrastructure as Code (IaC)

Der Prozess der Bereitstellung und Verwaltung der Infrastruktur einer Anwendung mithilfe einer Reihe von Konfigurationsdateien. IaC soll Ihnen helfen, das Infrastrukturmanagement zu zentralisieren, Ressourcen zu standardisieren und schnell zu skalieren, sodass neue Umgebungen wiederholbar, zuverlässig und konsistent sind.

Industrielles Internet der Dinge (IIoT)

Einsatz von mit dem Internet verbundenen Sensoren und Geräten in Industriesektoren wie Fertigung, Energie, Automobilindustrie, Gesundheitswesen, Biowissenschaften und Landwirtschaft. Mehr Informationen finden Sie unter Aufbau einer digitalen Transformationsstrategie für das industrielle Internet der Dinge (IIoT).

Inspektions-VPC

In einer Architektur AWS mit mehreren Konten eine zentralisierte VPC, die Inspektionen des Netzwerkverkehrs zwischen VPCs (in derselben oder unterschiedlichen AWS-Regionen), dem Internet und lokalen Netzwerken verwaltet. Die AWS -Referenzarchitektur für die Sicherheit empfiehlt, Ihr Netzwerkkonto mit eingehenden und ausgehenden VPCs und Inspektions-VPCs einzurichten, um die bidirektionale Schnittstelle zwischen Ihrer Anwendung und dem Internet zu schützen.

Internet of Things (IoT)

Das Netzwerk verbundener physischer Objekte mit eingebetteten Sensoren oder Prozessoren, das über das Internet oder über ein lokales Kommunikationsnetzwerk mit anderen Geräten und Systemen kommuniziert. Weitere Informationen finden Sie unter Was ist IoT?

Interpretierbarkeit

Ein Merkmal eines Modells für Machine Learning, das beschreibt, inwieweit ein Mensch verstehen kann, wie die Vorhersagen des Modells von seinen Eingaben abhängen. Weitere Informationen finden Sie unter Interpretierbarkeit von Modellen für Machine Learning mit AWS.

IoT

Siehe Internet der Dinge.

IT information library (ITIL, IT-Informationsbibliothek)

Eine Reihe von bewährten Methoden für die Bereitstellung von IT-Services und die Abstimmung dieser Services auf die Geschäftsanforderungen. ITIL bietet die Grundlage für ITSM.

T service management (ITSM, IT-Servicemanagement)

Aktivitäten im Zusammenhang mit der Gestaltung, Implementierung, Verwaltung und Unterstützung von IT-Services für eine Organisation. Informationen zur Integration von Cloud-Vorgängen mit ITSM-Tools finden Sie im Leitfaden zur Betriebsintegration.

BIS

Weitere Informationen finden Sie in der IT-Informationsbibliothek.

ITSM

Siehe IT-Servicemanagement.

L

Labelbasierte Zugangskontrolle (LBAC)

Eine Implementierung der Mandatory Access Control (MAC), bei der den Benutzern und den Daten selbst jeweils explizit ein Sicherheitslabelwert zugewiesen wird. Die Schnittmenge zwischen der Benutzersicherheitsbeschriftung und der Datensicherheitsbeschriftung bestimmt, welche Zeilen und Spalten für den Benutzer sichtbar sind.

Landing Zone

Eine landing zone ist eine gut strukturierte AWS Umgebung mit mehreren Konten, die skalierbar und sicher ist. Dies ist ein Ausgangspunkt, von dem aus Ihre Organisationen Workloads und Anwendungen schnell und mit Vertrauen in ihre Sicherheits- und Infrastrukturumgebung starten und bereitstellen können. Weitere Informationen zu Landing Zones finden Sie unter Einrichtung einer sicheren und skalierbaren AWS -Umgebung mit mehreren Konten..

Große Migration

Eine Migration von 300 oder mehr Servern.

SCHWARZ

Weitere Informationen finden Sie unter Label-basierte Zugriffskontrolle.

Geringste Berechtigung

Die bewährte Sicherheitsmethode, bei der nur die für die Durchführung einer Aufgabe erforderlichen Mindestberechtigungen erteilt werden. Weitere Informationen finden Sie unter Geringste Berechtigungen anwenden in der IAM-Dokumentation.

Lift and Shift

Siehe 7 Rs.

Little-Endian-System

Ein System, welches das niedrigwertigste Byte zuerst speichert. Siehe auch Endianness.

Niedrigere Umgebungen

Siehe Umwelt.

M

Machine Learning (ML)

Eine Art künstlicher Intelligenz, die Algorithmen und Techniken zur Mustererkennung und zum Lernen verwendet. ML analysiert aufgezeichnete Daten, wie z. B. Daten aus dem Internet der Dinge (IoT), und lernt daraus, um ein statistisches Modell auf der Grundlage von Mustern zu erstellen. Weitere Informationen finden Sie unter Machine Learning.

Hauptzweig

Siehe Filiale.

Malware

Software, die entwickelt wurde, um die Computersicherheit oder den Datenschutz zu gefährden. Malware kann Computersysteme stören, vertrauliche Informationen durchsickern lassen oder sich unbefugten Zugriff verschaffen. Beispiele für Malware sind Viren, Würmer, Ransomware, Trojaner, Spyware und Keylogger.

verwaltete Dienste

AWS-Services für die die Infrastrukturebene, das Betriebssystem und die Plattformen AWS betrieben werden, und Sie greifen auf die Endgeräte zu, um Daten zu speichern und abzurufen. Amazon Simple Storage Service (Amazon S3) und Amazon DynamoDB sind Beispiele für Managed Services. Diese werden auch als abstrakte Dienste bezeichnet.

Manufacturing Execution System (MES)

Ein Softwaresystem zur Nachverfolgung, Überwachung, Dokumentation und Steuerung von Produktionsprozessen, bei denen Rohstoffe in der Fertigung zu fertigen Produkten umgewandelt werden.

MAP

Siehe Migration Acceleration Program.

Mechanismus

Ein vollständiger Prozess, bei dem Sie ein Tool erstellen, die Akzeptanz des Tools vorantreiben und anschließend die Ergebnisse überprüfen, um Anpassungen vorzunehmen. Ein Mechanismus ist ein Zyklus, der sich im Laufe seiner Tätigkeit selbst verstärkt und verbessert. Weitere Informationen finden Sie unter Aufbau von Mechanismen im AWS Well-Architected Framework.

Mitgliedskonto

Alle AWS-Konten außer dem Verwaltungskonto, die Teil einer Organisation in sind. AWS Organizations Ein Konto kann jeweils nur einer Organisation angehören.

DURCHEINANDER

Siehe Manufacturing Execution System.

Message Queuing-Telemetrietransport (MQTT)

Ein leichtes machine-to-machine (M2M) -Kommunikationsprotokoll, das auf dem Publish/Subscribe-Muster für IoT-Geräte mit beschränkten Ressourcen basiert.

Microservice

Ein kleiner, unabhängiger Service, der über klar definierte APIs kommuniziert und in der Regel kleinen, eigenständigen Teams gehört. Ein Versicherungssystem kann beispielsweise Microservices beinhalten, die Geschäftsfunktionen wie Vertrieb oder Marketing oder Subdomains wie Einkauf, Schadenersatz oder Analytik zugeordnet sind. Zu den Vorteilen von Microservices gehören Agilität, flexible Skalierung, einfache Bereitstellung, wiederverwendbarer Code und Ausfallsicherheit. Weitere Informationen finden Sie unter Integration von Microservices mithilfe serverloser Dienste. AWS

Microservices-Architekturen

Ein Ansatz zur Erstellung einer Anwendung mit unabhängigen Komponenten, die jeden Anwendungsprozess als Microservice ausführen. Diese Microservices kommunizieren über eine klar definierte Schnittstelle mithilfe einfacher APIs. Jeder Microservice in dieser Architektur kann aktualisiert, bereitgestellt und skaliert werden, um den Bedarf an bestimmten Funktionen einer Anwendung zu decken. Weitere Informationen finden Sie unter Implementierung von Microservices auf. AWS

Migration Acceleration Program (MAP)

Ein AWS Programm, das Beratung, Unterstützung, Schulungen und Services bietet, um Unternehmen dabei zu unterstützen, eine solide betriebliche Grundlage für die Umstellung auf die Cloud zu schaffen und die anfänglichen Kosten von Migrationen auszugleichen. MAP umfasst eine Migrationsmethode für die methodische Durchführung von Legacy-Migrationen sowie eine Reihe von Tools zur Automatisierung und Beschleunigung gängiger Migrationsszenarien.

Migration in großem Maßstab

Der Prozess, bei dem der Großteil des Anwendungsportfolios in Wellen in die Cloud verlagert wird, wobei in jeder Welle mehr Anwendungen schneller migriert werden. In dieser Phase werden die bewährten Verfahren und Erkenntnisse aus den früheren Phasen zur Implementierung einer Migrationsfabrik von Teams, Tools und Prozessen zur Optimierung der Migration von Workloads durch Automatisierung und agile Bereitstellung verwendet. Dies ist die dritte Phase der AWS - Migrationsstrategie.

Migrationsfabrik

Funktionsübergreifende Teams, die die Migration von Workloads durch automatisierte, agile Ansätze optimieren. Zu den Teams in der Migrationsabteilung gehören in der Regel Betriebsabläufe, Geschäftsanalysten und Eigentümer, Migrationsingenieure, Entwickler und DevOps Experten, die in Sprints arbeiten. Zwischen 20 und 50 Prozent eines Unternehmensanwendungsportfolios bestehen aus sich wiederholenden Mustern, die durch einen Fabrik-Ansatz optimiert werden können. Weitere Informationen finden Sie in Diskussion über Migrationsfabriken und den Leitfaden zur Cloud-Migration-Fabrik in diesem Inhaltssatz.

Migrationsmetadaten

Die Informationen über die Anwendung und den Server, die für den Abschluss der Migration benötigt werden. Für jedes Migrationsmuster ist ein anderer Satz von Migrationsmetadaten erforderlich. Beispiele für Migrationsmetadaten sind das Zielsubnetz, die Sicherheitsgruppe und AWS das Konto.

Migrationsmuster

Eine wiederholbare Migrationsaufgabe, in der die Migrationsstrategie, das Migrationsziel und die verwendete Migrationsanwendung oder der verwendete Migrationsservice detailliert beschrieben werden. Beispiel: Rehost-Migration zu Amazon EC2 mit AWS Application Migration Service.

Migration Portfolio Assessment (MPA)

Ein Online-Tool, das Informationen zur Validierung des Geschäftsszenarios für die Migration auf das bereitstellt. AWS Cloud MPA bietet eine detaillierte Portfoliobewertung (richtige Servergröße, Preisgestaltung, Gesamtbetriebskostenanalyse, Migrationskostenanalyse) sowie Migrationsplanung (Anwendungsdatenanalyse und Datenerfassung, Anwendungsgruppierung, Migrationspriorisierung und Wellenplanung). Das MPA-Tool (Anmeldung erforderlich) steht allen AWS Beratern und APN-Partnerberatern kostenlos zur Verfügung.

Migration Readiness Assessment (MRA)

Der Prozess, bei dem mithilfe des AWS CAF Erkenntnisse über den Cloud-Bereitschaftsstatus eines Unternehmens gewonnen, Stärken und Schwächen identifiziert und ein Aktionsplan zur Schließung festgestellter Lücken erstellt wird. Weitere Informationen finden Sie im Benutzerhandbuch für Migration Readiness. MRA ist die erste Phase der AWS - Migrationsstrategie.

Migrationsstrategie

Der Ansatz, der verwendet wurde, um einen Workload auf den AWS Cloud zu migrieren. Weitere Informationen finden Sie im Eintrag 7 Rs in diesem Glossar und unter Mobilisieren Sie Ihr Unternehmen, um umfangreiche Migrationen zu beschleunigen.

ML

Siehe maschinelles Lernen.

Modernisierung

Umwandlung einer veralteten (veralteten oder monolithischen) Anwendung und ihrer Infrastruktur in ein agiles, elastisches und hochverfügbares System in der Cloud, um Kosten zu senken, die Effizienz zu steigern und Innovationen zu nutzen. Weitere Informationen finden Sie unter Strategie zur Modernisierung von Anwendungen in der AWS Cloud.

Bewertung der Modernisierungsfähigkeit

Eine Bewertung, anhand derer festgestellt werden kann, ob die Anwendungen einer Organisation für die Modernisierung bereit sind, Vorteile, Risiken und Abhängigkeiten identifiziert und ermittelt wird, wie gut die Organisation den zukünftigen Status dieser Anwendungen unterstützen kann. Das Ergebnis der Bewertung ist eine Vorlage der Zielarchitektur, eine Roadmap, in der die Entwicklungsphasen und Meilensteine des Modernisierungsprozesses detailliert beschrieben werden, sowie ein Aktionsplan zur Behebung festgestellter Lücken. Weitere Informationen finden Sie unter Evaluierung der Modernisierungsbereitschaft von Anwendungen in der AWS Cloud.

Monolithische Anwendungen (Monolithen)

Anwendungen, die als ein einziger Service mit eng gekoppelten Prozessen ausgeführt werden. Monolithische Anwendungen haben verschiedene Nachteile. Wenn ein Anwendungs-Feature stark nachgefragt wird, muss die gesamte Architektur skaliert werden. Das Hinzufügen oder Verbessern der Feature einer monolithischen Anwendung wird ebenfalls komplexer, wenn die Codebasis wächst. Um diese Probleme zu beheben, können Sie eine Microservices-Architektur verwenden. Weitere Informationen finden Sie unter Zerlegen von Monolithen in Microservices.

MPA

Siehe Bewertung des Migrationsportfolios.

MQTT

Siehe Message Queuing-Telemetrietransport.

Mehrklassen-Klassifizierung

Ein Prozess, der dabei hilft, Vorhersagen für mehrere Klassen zu generieren (wobei eines von mehr als zwei Ergebnissen vorhergesagt wird). Ein ML-Modell könnte beispielsweise fragen: „Ist dieses Produkt ein Buch, ein Auto oder ein Telefon?“ oder „Welche Kategorie von Produkten ist für diesen Kunden am interessantesten?“

veränderbare Infrastruktur

Ein Modell, das die bestehende Infrastruktur für Produktionsworkloads aktualisiert und modifiziert. Für eine verbesserte Konsistenz, Zuverlässigkeit und Vorhersagbarkeit empfiehlt das AWS Well-Architected Framework die Verwendung einer unveränderlichen Infrastruktur als bewährte Methode.

O

OAC

Weitere Informationen finden Sie unter Origin Access Control.

OAI

Siehe Zugriffsidentität von Origin.

COM

Siehe organisatorisches Change-Management.

Offline-Migration

Eine Migrationsmethode, bei der der Quell-Workload während des Migrationsprozesses heruntergefahren wird. Diese Methode ist mit längeren Ausfallzeiten verbunden und wird in der Regel für kleine, unkritische Workloads verwendet.

OI

Siehe Betriebsintegration.

OLA

Siehe Vereinbarung auf operativer Ebene.

Online-Migration

Eine Migrationsmethode, bei der der Quell-Workload auf das Zielsystem kopiert wird, ohne offline genommen zu werden. Anwendungen, die mit dem Workload verbunden sind, können während der Migration weiterhin funktionieren. Diese Methode beinhaltet keine bis minimale Ausfallzeit und wird in der Regel für kritische Produktionsworkloads verwendet.

OPC-UA

Siehe Open Process Communications — Unified Architecture.

Offene Prozesskommunikation — Einheitliche Architektur (OPC-UA)

Ein machine-to-machine (M2M) -Kommunikationsprotokoll für die industrielle Automatisierung. OPC-UA bietet einen Interoperabilitätsstandard mit Datenverschlüsselungs-, Authentifizierungs- und Autorisierungsschemata.

Vereinbarung auf Betriebsebene (OLA)

Eine Vereinbarung, in der klargestellt wird, welche funktionalen IT-Gruppen sich gegenseitig versprechen zu liefern, um ein Service Level Agreement (SLA) zu unterstützen.

Überprüfung der Betriebsbereitschaft (ORR)

Eine Checkliste mit Fragen und zugehörigen bewährten Methoden, die Ihnen helfen, Vorfälle und mögliche Ausfälle zu verstehen, zu bewerten, zu verhindern oder deren Umfang zu reduzieren. Weitere Informationen finden Sie unter Operational Readiness Reviews (ORR) im AWS Well-Architected Framework.

Betriebstechnologie (OT)

Hardware- und Softwaresysteme, die mit der physischen Umgebung zusammenarbeiten, um industrielle Abläufe, Ausrüstung und Infrastruktur zu steuern. In der Fertigung ist die Integration von OT- und Informationstechnologie (IT) -Systemen ein zentraler Schwerpunkt der Industrie 4.0-Transformationen.

Betriebsintegration (OI)

Der Prozess der Modernisierung von Abläufen in der Cloud, der Bereitschaftsplanung, Automatisierung und Integration umfasst. Weitere Informationen finden Sie im Leitfaden zur Betriebsintegration.

Organisationspfad

Ein Pfad, der von erstellt wird und in AWS CloudTrail dem alle Ereignisse für alle AWS-Konten in einer Organisation protokolliert werden. AWS Organizations Diese Spur wird in jedem AWS-Konto , der Teil der Organisation ist, erstellt und verfolgt die Aktivität in jedem Konto. Weitere Informationen finden Sie in der CloudTrail Dokumentation unter Erstellen eines Pfads für eine Organisation.

Organisatorisches Veränderungsmanagement (OCM)

Ein Framework für das Management wichtiger, disruptiver Geschäftstransformationen aus Sicht der Mitarbeiter, der Kultur und der Führung. OCM hilft Organisationen dabei, sich auf neue Systeme und Strategien vorzubereiten und auf diese umzustellen, indem es die Akzeptanz von Veränderungen beschleunigt, Übergangsprobleme angeht und kulturelle und organisatorische Veränderungen vorantreibt. In der AWS Migrationsstrategie wird dieses Framework aufgrund der Geschwindigkeit des Wandels, der bei Projekten zur Cloud-Einführung erforderlich ist, als Mitarbeiterbeschleunigung bezeichnet. Weitere Informationen finden Sie im OCM-Handbuch.

Ursprungszugriffskontrolle (OAC)

In CloudFront, eine erweiterte Option zur Zugriffsbeschränkung, um Ihre Amazon Simple Storage Service (Amazon S3) -Inhalte zu sichern. OAC unterstützt alle S3-Buckets insgesamt AWS-Regionen, serverseitige Verschlüsselung mit AWS KMS (SSE-KMS) sowie dynamische `PUT` und `DELETE` Anfragen an den S3-Bucket.

Ursprungszugriffsidentität (OAI)

In CloudFront, eine Option zur Zugriffsbeschränkung, um Ihre Amazon S3 S3-Inhalte zu sichern. Wenn Sie OAI verwenden, CloudFront erstellt es einen Principal, mit dem sich Amazon S3 authentifizieren kann. Authentifizierte Principals können nur über eine bestimmte Distribution auf Inhalte in einem S3-Bucket zugreifen. CloudFront Siehe auch OAC, das eine detailliertere und verbesserte Zugriffskontrolle bietet.

ODER

Siehe Überprüfung der Betriebsbereitschaft.

NICHT

Siehe Betriebstechnologie.

Ausgehende (egress) VPC

In einer Architektur AWS mit mehreren Konten eine VPC, die Netzwerkverbindungen verarbeitet, die von einer Anwendung aus initiiert werden. Die AWS -Referenzarchitektur für die Sicherheit empfiehlt, Ihr Netzwerkkonto mit eingehenden und ausgehenden VPCs und Inspektions-VPCs einzurichten, um die bidirektionale Schnittstelle zwischen Ihrer Anwendung und dem Internet zu schützen.

P

Berechtigungsgrenze

Eine IAM-Verwaltungsrichtlinie, die den IAM-Prinzipalen zugeordnet ist, um die maximalen Berechtigungen festzulegen, die der Benutzer oder die Rolle haben kann. Weitere Informationen finden Sie unter Berechtigungsgrenzen für IAM-Entitys in der IAM-Dokumentation.

persönlich identifizierbare Informationen (PII)

Informationen, die, wenn sie direkt betrachtet oder mit anderen verwandten Daten kombiniert werden, verwendet werden können, um vernünftige Rückschlüsse auf die Identität einer Person zu ziehen. Beispiele für personenbezogene Daten sind Namen, Adressen und Kontaktinformationen.

Personenbezogene Daten

Siehe persönlich identifizierbare Informationen.

Playbook

Eine Reihe vordefinierter Schritte, die die mit Migrationen verbundenen Aufgaben erfassen, z. B. die Bereitstellung zentraler Betriebsfunktionen in der Cloud. Ein Playbook kann die Form von Skripten, automatisierten Runbooks oder einer Zusammenfassung der Prozesse oder Schritte annehmen, die für den Betrieb Ihrer modernisierten Umgebung erforderlich sind.

PLC

Siehe programmierbare Logiksteuerung.

PLM

Siehe Produktlebenszyklusmanagement.

policy

Ein Objekt, das Berechtigungen definieren (siehe identitätsbasierte Richtlinie), Zugriffsbedingungen spezifizieren (siehe ressourcenbasierte Richtlinie) oder die maximalen Berechtigungen für alle Konten in einer Organisation definieren kann AWS Organizations (siehe Dienststeuerungsrichtlinie).

Polyglotte Beharrlichkeit

Unabhängige Auswahl der Datenspeichertechnologie eines Microservices auf der Grundlage von Datenzugriffsmustern und anderen Anforderungen. Wenn Ihre Microservices über dieselbe Datenspeichertechnologie verfügen, kann dies zu Implementierungsproblemen oder zu Leistungseinbußen führen. Microservices lassen sich leichter implementieren und erzielen eine bessere Leistung und Skalierbarkeit, wenn sie den Datenspeicher verwenden, der ihren Anforderungen am besten entspricht. Weitere Informationen finden Sie unter Datenpersistenz in Microservices aktivieren.

Portfoliobewertung

Ein Prozess, bei dem das Anwendungsportfolio ermittelt, analysiert und priorisiert wird, um die Migration zu planen. Weitere Informationen finden Sie in Bewerten der Migrationsbereitschaft.

predicate

Eine Abfragebedingung, die `true` oder zurückgibt`false`, was üblicherweise in einer Klausel vorkommt. `WHERE`

Prädikat Pushdown

Eine Technik zur Optimierung von Datenbankabfragen, bei der die Daten in der Abfrage vor der Übertragung gefiltert werden. Dadurch wird die Datenmenge reduziert, die aus der relationalen Datenbank abgerufen und verarbeitet werden muss, und die Abfrageleistung wird verbessert.

Präventive Kontrolle

Eine Sicherheitskontrolle, die verhindern soll, dass ein Ereignis eintritt. Diese Kontrollen stellen eine erste Verteidigungslinie dar, um unbefugten Zugriff oder unerwünschte Änderungen an Ihrem Netzwerk zu verhindern. Weitere Informationen finden Sie unter Präventive Kontrolle in Implementierung von Sicherheitskontrollen in AWS.

Prinzipal

Eine Entität AWS , die Aktionen ausführen und auf Ressourcen zugreifen kann. Bei dieser Entität handelt es sich in der Regel um einen Root-Benutzer für eine AWS-Konto, eine IAM-Rolle oder

einen Benutzer. Weitere Informationen finden Sie unter Prinzipal in Rollenbegriffe und -konzepte in der IAM-Dokumentation.

Datenschutz durch Design

Ein Ansatz in der Systemtechnik, der den Datenschutz während des gesamten Engineering-Prozesses berücksichtigt.

Privat gehostete Zonen

Ein Container, der Informationen darüber enthält, wie Amazon Route 53 auf DNS-Abfragen für eine Domain und ihre Subdomains innerhalb einer oder mehrerer VPCs reagieren soll. Weitere Informationen finden Sie unter Arbeiten mit privat gehosteten Zonen in der Route-53-Dokumentation.

proaktive Steuerung

Eine Sicherheitskontrolle, die den Einsatz nicht richtlinienkonformer Ressourcen verhindern soll. Mit diesen Steuerelementen werden Ressourcen gescannt, bevor sie bereitgestellt werden. Wenn die Ressource nicht mit der Steuerung konform ist, wird sie nicht bereitgestellt. Weitere Informationen finden Sie im Referenzhandbuch zu Kontrollen in der AWS Control Tower Dokumentation und unter Proaktive Kontrollen unter Implementierung von Sicherheitskontrollen am AWS.

Produktlebenszyklusmanagement (PLM)

Das Management von Daten und Prozessen für ein Produkt während seines gesamten Lebenszyklus, vom Design, der Entwicklung und Markteinführung über Wachstum und Reife bis hin zur Markteinführung und Markteinführung.

Produktionsumgebung

Siehe Umgebung.

Speicherprogrammierbare Steuerung (SPS)

In der Fertigung ein äußerst zuverlässiger, anpassungsfähiger Computer, der Maschinen überwacht und Fertigungsprozesse automatisiert.

Pseudonymisierung

Der Prozess, bei dem persönliche Identifikatoren in einem Datensatz durch Platzhalterwerte ersetzt werden. Pseudonymisierung kann zum Schutz der Privatsphäre beitragen. Pseudonymisierte Daten gelten weiterhin als personenbezogene Daten.

veröffentlichen/abonnieren (pub/sub)

Ein Muster, das asynchrone Kommunikation zwischen Microservices ermöglicht, um die Skalierbarkeit und Reaktionsfähigkeit zu verbessern. In einem auf Microservices basierenden MES kann ein Microservice beispielsweise Ereignismeldungen in einem Kanal veröffentlichen, den andere Microservices abonnieren können. Das System kann neue Microservices hinzufügen, ohne den Veröffentlichungsservice zu ändern.

Q

Abfrageplan

Eine Reihe von Schritten, wie Anweisungen, die für den Zugriff auf die Daten in einem relationalen SQL-Datenbanksystem verwendet werden.

Abfrageplanregression

Wenn ein Datenbankserviceoptimierer einen weniger optimalen Plan wählt als vor einer bestimmten Änderung der Datenbankumgebung. Dies kann durch Änderungen an Statistiken, Beschränkungen, Umgebungseinstellungen, Abfrageparameter-Bindungen und Aktualisierungen der Datenbank-Engine verursacht werden.

R

RACI-Matrix

Siehe verantwortlich, rechenschaftspflichtig, konsultiert, informiert (RACI).

Ransomware

Eine bösartige Software, die entwickelt wurde, um den Zugriff auf ein Computersystem oder Daten zu blockieren, bis eine Zahlung erfolgt ist.

RASCI-Matrix

Siehe verantwortlich, rechenschaftspflichtig, konsultiert, informiert (RACI).

RCAC

Siehe Zugriffskontrolle für Zeilen und Spalten.

Read Replica

Eine Kopie einer Datenbank, die nur für Lesezwecke verwendet wird. Sie können Abfragen an das Lesereplikat weiterleiten, um die Belastung auf Ihrer Primärdatenbank zu reduzieren.

neu strukturieren

Siehe 7 Rs.

Recovery Point Objective (RPO)

Die maximal zulässige Zeitspanne seit dem letzten Datenwiederherstellungspunkt. Dies bestimmt, was als akzeptabler Datenverlust zwischen dem letzten Wiederherstellungspunkt und der Betriebsunterbrechung angesehen wird.

Wiederherstellungszeitziel (RTO)

Die maximal zulässige Verzögerung zwischen der Betriebsunterbrechung und der Wiederherstellung des Dienstes.

Refaktorierung

Siehe 7 Rs.

Region

Eine Sammlung von AWS Ressourcen in einem geografischen Gebiet. Jeder AWS-Region ist isoliert und unabhängig von den anderen, um Fehlertoleranz, Stabilität und Belastbarkeit zu gewährleisten. Weitere Informationen finden Sie unter Geben Sie an, was AWS-Regionen Ihr Konto verwenden kann.

Regression

Eine ML-Technik, die einen numerischen Wert vorhersagt. Zum Beispiel, um das Problem „Zu welchem Preis wird dieses Haus verkauft werden?“ zu lösen Ein ML-Modell könnte ein lineares Regressionsmodell verwenden, um den Verkaufspreis eines Hauses auf der Grundlage bekannter Fakten über das Haus (z. B. die Quadratmeterzahl) vorherzusagen.

rehosten

Siehe 7 Rs.

Veröffentlichung

In einem Bereitstellungsprozess der Akt der Förderung von Änderungen an einer Produktionsumgebung.

umziehen

Siehe 7 Rs.

neue Plattform

Siehe 7 Rs.

Rückkauf

Siehe 7 Rs.

Ausfallsicherheit

Die Fähigkeit einer Anwendung, Störungen zu widerstehen oder sich von ihnen zu erholen. Hochverfügbarkeit und Notfallwiederherstellung sind häufig Überlegungen bei der Planung der Ausfallsicherheit in der. AWS Cloud Weitere Informationen finden Sie unter AWS Cloud Resilienz.

Ressourcenbasierte Richtlinie

Eine mit einer Ressource verknüpfte Richtlinie, z. B. ein Amazon-S3-Bucket, ein Endpunkt oder ein Verschlüsselungsschlüssel. Diese Art von Richtlinie legt fest, welchen Prinzipalen der Zugriff gewährt wird, welche Aktionen unterstützt werden und welche anderen Bedingungen erfüllt sein müssen.

RACI-Matrix (verantwortlich, rechenschaftspflichtig, konsultiert, informiert)

Eine Matrix, die die Rollen und Verantwortlichkeiten aller an Migrationsaktivitäten und Cloud-Operationen beteiligten Parteien definiert. Der Matrixname leitet sich von den in der Matrix definierten Zuständigkeitstypen ab: verantwortlich (R), rechenschaftspflichtig (A), konsultiert (C) und informiert (I). Der Unterstützungstyp (S) ist optional. Wenn Sie Unterstützung einbeziehen, wird die Matrix als RASCI-Matrix bezeichnet, und wenn Sie sie ausschließen, wird sie als RACI-Matrix bezeichnet.

Reaktive Kontrolle

Eine Sicherheitskontrolle, die darauf ausgelegt ist, die Behebung unerwünschter Ereignisse oder Abweichungen von Ihren Sicherheitsstandards voranzutreiben. Weitere Informationen finden Sie unter Reaktive Kontrolle in Implementieren von Sicherheitskontrollen in AWS.

Beibehaltung

Siehe 7 Rs.

zurückziehen

Siehe 7 Rs.

Drehung

Der Vorgang, bei dem ein Geheimnis regelmäßig aktualisiert wird, um es einem Angreifer zu erschweren, auf die Anmeldeinformationen zuzugreifen.

Zugriffskontrolle für Zeilen und Spalten (RCAC)

Die Verwendung einfacher, flexibler SQL-Ausdrücke mit definierten Zugriffsregeln. RCAC besteht aus Zeilenberechtigungen und Spaltenmasken.

RPO

Siehe Recovery Point Objective.

RTO

Siehe Ziel der Wiederherstellungszeit.

Runbook

Eine Reihe manueller oder automatisierter Verfahren, die zur Ausführung einer bestimmten Aufgabe erforderlich sind. Diese sind in der Regel darauf ausgelegt, sich wiederholende Operationen oder Verfahren mit hohen Fehlerquoten zu rationalisieren.

S

SAML 2.0

Ein offener Standard, den viele Identitätsanbieter (IdPs) verwenden. Diese Funktion ermöglicht föderiertes Single Sign-On (SSO), sodass sich Benutzer bei den API-Vorgängen anmelden AWS Management Console oder die AWS API-Operationen aufrufen können, ohne dass Sie einen Benutzer in IAM für alle in Ihrer Organisation erstellen müssen. Weitere Informationen zum SAML-2.0.-basierten Verbund finden Sie unter Über den SAML-2.0-basierten Verbund in der IAM-Dokumentation.

SCADA

Siehe Aufsichtskontrolle und Datenerfassung.

SCP

Siehe Richtlinie zur Dienstkontrolle.

Secret

Interne AWS Secrets Manager, vertrauliche oder eingeschränkte Informationen, wie z. B. ein Passwort oder Benutzeranmeldeinformationen, die Sie in verschlüsselter Form speichern. Es besteht aus dem geheimen Wert und seinen Metadaten. Der geheime Wert kann binär, eine einzelne Zeichenfolge oder mehrere Zeichenketten sein. Weitere Informationen finden Sie unter Was ist in einem Secrets Manager Manager-Geheimnis? in der Secrets Manager Manager-Dokumentation.

Sicherheitskontrolle

Ein technischer oder administrativer Integritätsschutz, der die Fähigkeit eines Bedrohungsakteurs, eine Schwachstelle auszunutzen, verhindert, erkennt oder einschränkt. Es gibt vier Haupttypen von Sicherheitskontrollen: präventiv, detektiv, reaktionsschnell und proaktiv.

Härtung der Sicherheit

Der Prozess, bei dem die Angriffsfläche reduziert wird, um sie widerstandsfähiger gegen Angriffe zu machen. Dies kann Aktionen wie das Entfernen von Ressourcen, die nicht mehr benötigt werden, die Implementierung der bewährten Sicherheitsmethode der Gewährung geringster Berechtigungen oder die Deaktivierung unnötiger Feature in Konfigurationsdateien umfassen.

System zur Verwaltung von Sicherheitsinformationen und Ereignissen (security information and event management – SIEM)

Tools und Services, die Systeme für das Sicherheitsinformationsmanagement (SIM) und das Management von Sicherheitsereignissen (SEM) kombinieren. Ein SIEM-System sammelt, überwacht und analysiert Daten von Servern, Netzwerken, Geräten und anderen Quellen, um Bedrohungen und Sicherheitsverletzungen zu erkennen und Warnmeldungen zu generieren.

Automatisierung von Sicherheitsreaktionen

Eine vordefinierte und programmierte Aktion, die darauf ausgelegt ist, automatisch auf ein Sicherheitsereignis zu reagieren oder es zu beheben. Diese Automatisierungen dienen als detektive oder reaktionsschnelle Sicherheitskontrollen, die Sie bei der Implementierung bewährter AWS Sicherheitsmethoden unterstützen. Beispiele für automatisierte Antwortaktionen sind das Ändern einer VPC-Sicherheitsgruppe, das Patchen einer Amazon EC2 EC2-Instance oder das Rotieren von Anmeldeinformationen.

Serverseitige Verschlüsselung

Verschlüsselung von Daten am Zielort durch denjenigen AWS-Service , der sie empfängt.

Service-Kontrollrichtlinie (SCP)

Eine Richtlinie, die eine zentrale Kontrolle über die Berechtigungen für alle Konten in einer Organisation in AWS Organizations ermöglicht. SCPs definieren Integritätsschutz oder legen Grenzwerte für Aktionen fest, die ein Administrator an Benutzer oder Rollen delegieren kann. Sie können SCPs als Zulassungs- oder Ablehnungslisten verwenden, um festzulegen, welche Services oder Aktionen zulässig oder verboten sind. Weitere Informationen finden Sie in der AWS Organizations Dokumentation unter Richtlinien zur Dienststeuerung.

Service-Endpunkt

Die URL des Einstiegspunkts für einen AWS-Service. Sie können den Endpunkt verwenden, um programmgesteuert eine Verbindung zum Zielservice herzustellen. Weitere Informationen finden Sie unter AWS-Service -Endpunkte in der Allgemeine AWS-Referenz.

Service Level Agreement (SLA)

Eine Vereinbarung, in der klargestellt wird, was ein IT-Team seinen Kunden zu bieten verspricht, z. B. in Bezug auf Verfügbarkeit und Leistung der Services.

Service-Level-Indikator (SLI)

Eine Messung eines Leistungsaspekts eines Dienstes, z. B. seiner Fehlerrate, Verfügbarkeit oder Durchsatz.

Service-Level-Ziel (SLO)

Eine Zielkennzahl, die den Zustand eines Dienstes darstellt, gemessen anhand eines Service-Level-Indikators.

Modell der geteilten Verantwortung

Ein Modell, das die Verantwortung beschreibt, mit der Sie gemeinsam AWS für Cloud-Sicherheit und Compliance verantwortlich sind. AWS ist für die Sicherheit der Cloud verantwortlich, wohingegen Sie für die Sicherheit in der Cloud verantwortlich sind. Weitere Informationen finden Sie unter Modell der geteilten Verantwortung.

SIEM

Siehe Sicherheitsinformations- und Event-Management-System.

Single Point of Failure (SPOF)

Ein Fehler in einer einzelnen, kritischen Komponente einer Anwendung, der das System stören kann.

SLA

Siehe Service Level Agreement.

SLI

Siehe Service-Level-Indikator.

ALSO

Siehe Service-Level-Ziel.

split-and-seed Modell

Ein Muster für die Skalierung und Beschleunigung von Modernisierungsprojekten. Sobald neue Features und Produktversionen definiert werden, teilt sich das Kernteam auf, um neue Produktteams zu bilden. Dies trägt zur Skalierung der Fähigkeiten und Services Ihrer Organisation bei, verbessert die Produktivität der Entwickler und unterstützt schnelle Innovationen. Weitere Informationen finden Sie unter Schrittweiser Ansatz zur Modernisierung von Anwendungen in der AWS Cloud.

SPOTTEN

Siehe Single Point of Failure.

Sternschema

Eine Datenbank-Organisationsstruktur, die eine große Faktentabelle zum Speichern von Transaktions- oder Messdaten und eine oder mehrere kleinere dimensionale Tabellen zum Speichern von Datenattributen verwendet. Diese Struktur ist für die Verwendung in einem Data Warehouse oder für Business Intelligence-Zwecke konzipiert.

Strangler-Fig-Muster

Ein Ansatz zur Modernisierung monolithischer Systeme, bei dem die Systemfunktionen schrittweise umgeschrieben und ersetzt werden, bis das Legacy-System außer Betrieb genommen werden kann. Dieses Muster verwendet die Analogie einer Feigenrebe, die zu einem etablierten Baum heranwächst und schließlich ihren Wirt überwindet und ersetzt. Das Muster wurde eingeführt von Martin Fowler als Möglichkeit, Risiken beim Umschreiben

monolithischer Systeme zu managen. Ein Beispiel für die Anwendung dieses Musters finden Sie unter Schrittweises Modernisieren älterer Microsoft ASP.NET (ASMX)-Webservices mithilfe von Containern und Amazon API Gateway.

Subnetz

Ein Bereich von IP-Adressen in Ihrer VPC. Ein Subnetz muss sich in einer einzigen Availability Zone befinden.

Aufsichtskontrolle und Datenerfassung (SCADA)

In der Fertigung ein System, das Hardware und Software zur Überwachung von Sachanlagen und Produktionsabläufen verwendet.

Symmetrische Verschlüsselung

Ein Verschlüsselungsalgorithmus, der denselben Schlüssel zum Verschlüsseln und Entschlüsseln der Daten verwendet.

synthetisches Testen

Testen eines Systems auf eine Weise, die Benutzerinteraktionen simuliert, um potenzielle Probleme zu erkennen oder die Leistung zu überwachen. Sie können Amazon CloudWatch Synthetics verwenden, um diese Tests zu erstellen.

T

tags

Schlüssel-Wert-Paare, die als Metadaten für die Organisation Ihrer Ressourcen dienen. AWS Mit Tags können Sie Ressourcen verwalten, identifizieren, organisieren, suchen und filtern. Weitere Informationen finden Sie unter Markieren Ihrer AWS -Ressourcen.

Zielvariable

Der Wert, den Sie in überwachtem ML vorhersagen möchten. Dies wird auch als Ergebnisvariable bezeichnet. In einer Fertigungsumgebung könnte die Zielvariable beispielsweise ein Produktfehler sein.

Aufgabenliste

Ein Tool, das verwendet wird, um den Fortschritt anhand eines Runbooks zu verfolgen. Eine Aufgabenliste enthält eine Übersicht über das Runbook und eine Liste mit allgemeinen Aufgaben,

die erledigt werden müssen. Für jede allgemeine Aufgabe werden der geschätzte Zeitaufwand, der Eigentümer und der Fortschritt angegeben.

Testumgebungen

Siehe Umgebung.

Training

Daten für Ihr ML-Modell bereitstellen, aus denen es lernen kann. Die Trainingsdaten müssen die richtige Antwort enthalten. Der Lernalgorithmus findet Muster in den Trainingsdaten, die die Attribute der Input-Daten dem Ziel (die Antwort, die Sie voraussagen möchten) zuordnen. Es gibt ein ML-Modell aus, das diese Muster erfasst. Sie können dann das ML-Modell verwenden, um Voraussagen für neue Daten zu erhalten, bei denen Sie das Ziel nicht kennen.

Transit-Gateway

Ein Transit-Gateway ist ein Netzwerk-Transit-Hub, mit dem Sie Ihre VPCs und On-Premises-Netzwerke miteinander verbinden können. Weitere Informationen finden Sie in der AWS Transit Gateway Dokumentation unter Was ist ein Transit-Gateway.

Stammbasierter Workflow

Ein Ansatz, bei dem Entwickler Feature lokal in einem Feature-Zweig erstellen und testen und diese Änderungen dann im Hauptzweig zusammenführen. Der Hauptzweig wird dann sequentiell für die Entwicklungs-, Vorproduktions- und Produktionsumgebungen erstellt.

Vertrauenswürdiger Zugriff

Gewährung von Berechtigungen für einen Dienst, den Sie angeben, um Aufgaben in Ihrer Organisation AWS Organizations und in deren Konten in Ihrem Namen auszuführen. Der vertrauenswürdige Service erstellt in jedem Konto eine mit dem Service verknüpfte Rolle, wenn diese Rolle benötigt wird, um Verwaltungsaufgaben für Sie auszuführen. Weitere Informationen finden Sie in der AWS Organizations Dokumentation unter Verwendung AWS Organizations mit anderen AWS Diensten.

Optimieren

Aspekte Ihres Trainingsprozesses ändern, um die Genauigkeit des ML-Modells zu verbessern. Sie können das ML-Modell z. B. trainieren, indem Sie einen Beschriftungssatz generieren, Beschriftungen hinzufügen und diese Schritte dann mehrmals unter verschiedenen Einstellungen wiederholen, um das Modell zu optimieren.

Zwei-Pizzen-Team

Ein kleines DevOps Team, das Sie mit zwei Pizzen ernähren können. Eine Teamgröße von zwei Pizzen gewährleistet die bestmögliche Gelegenheit zur Zusammenarbeit bei der Softwareentwicklung.

U

Unsicherheit

Ein Konzept, das sich auf ungenaue, unvollständige oder unbekannte Informationen bezieht, die die Zuverlässigkeit von prädiktiven ML-Modellen untergraben können. Es gibt zwei Arten von Unsicherheit: Epistemische Unsicherheit wird durch begrenzte, unvollständige Daten verursacht, wohingegen aleatorische Unsicherheit durch Rauschen und Randomisierung verursacht wird, die in den Daten liegt. Weitere Informationen finden Sie im Leitfaden Quantifizieren der Unsicherheit in Deep-Learning-Systemen.

undifferenzierte Aufgaben

Diese Arbeit wird auch als Schwerstarbeit bezeichnet. Dabei handelt es sich um Arbeiten, die zwar für die Erstellung und den Betrieb einer Anwendung erforderlich sind, aber dem Endbenutzer keinen direkten Mehrwert bieten oder keinen Wettbewerbsvorteil bieten. Beispiele für undifferenzierte Aufgaben sind Beschaffung, Wartung und Kapazitätsplanung.

höhere Umgebungen

Siehe Umgebung.

V

Vacuuming

Ein Vorgang zur Datenbankwartung, bei dem die Datenbank nach inkrementellen Aktualisierungen bereinigt wird, um Speicherplatz zurückzugewinnen und die Leistung zu verbessern.

Versionskontrolle

Prozesse und Tools zur Nachverfolgung von Änderungen, z. B. Änderungen am Quellcode in einem Repository.

VPC-Peering

Eine Verbindung zwischen zwei VPCs, mit der Sie den Datenverkehr mithilfe von privaten IP-Adressen weiterleiten können. Weitere Informationen finden Sie unter Was ist VPC-Peering? in der Amazon-VPC-Dokumentation.

Schwachstelle

Ein Software- oder Hardwarefehler, der die Sicherheit des Systems gefährdet.

W

Warmer Cache

Ein Puffer-Cache, der aktuelle, relevante Daten enthält, auf die häufig zugegriffen wird. Die Datenbank-Instance kann aus dem Puffer-Cache lesen, was schneller ist als das Lesen aus dem Hauptspeicher oder von der Festplatte.

warme Daten

Daten, auf die selten zugegriffen wird. Bei der Abfrage dieser Art von Daten sind mäßig langsame Abfragen in der Regel akzeptabel.

Fensterfunktion

Eine SQL-Funktion, die eine Berechnung für eine Gruppe von Zeilen durchführt, die sich in irgendeiner Weise auf den aktuellen Datensatz beziehen. Fensterfunktionen sind nützlich für die Verarbeitung von Aufgaben wie die Berechnung eines gleitenden Durchschnitts oder für den Zugriff auf den Wert von Zeilen auf der Grundlage der relativen Position der aktuellen Zeile.

Workload

Ein Workload ist eine Sammlung von Ressourcen und Code, die einen Unternehmenswert bietet, wie z. B. eine kundenorientierte Anwendung oder ein Backend-Prozess.

Workstream

Funktionsgruppen in einem Migrationsprojekt, die für eine bestimmte Reihe von Aufgaben verantwortlich sind. Jeder Workstream ist unabhängig, unterstützt aber die anderen Workstreams im Projekt. Der Portfolio-Workstream ist beispielsweise für die Priorisierung von Anwendungen, die Wellenplanung und die Erfassung von Migrationsmetadaten verantwortlich. Der Portfolio-Workstream liefert diese Komponenten an den Migrations-Workstream, der dann die Server und Anwendungen migriert.

WURM

Sehen Sie einmal schreiben, viele lesen.

WQF

Weitere Informationen finden Sie unter AWS Workload Qualification Framework.

einmal schreiben, viele lesen (WORM)

Ein Speichermodell, das Daten ein einziges Mal schreibt und verhindert, dass die Daten gelöscht oder geändert werden. Autorisierte Benutzer können die Daten so oft wie nötig lesen, aber sie können sie nicht ändern. Diese Datenspeicherinfrastruktur gilt als unveränderlich.

Z

Zero-Day-Exploit

Ein Angriff, in der Regel Malware, der eine Zero-Day-Sicherheitslücke ausnutzt.

Zero-Day-Sicherheitslücke

Ein unfehlbarer Fehler oder eine Sicherheitslücke in einem Produktionssystem. Bedrohungsakteure können diese Art von Sicherheitslücke nutzen, um das System anzugreifen. Entwickler werden aufgrund des Angriffs häufig auf die Sicherheitsanfälligkeit aufmerksam.

Zombie-Anwendung

Eine Anwendung, deren durchschnittliche CPU- und Arbeitsspeichernutzung unter 5 Prozent liegt. In einem Migrationsprojekt ist es üblich, diese Anwendungen außer Betrieb zu nehmen.

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.