Auswahl des richtigen Zugriffsansatzes für Amazon QuickSight

# AWS Präskriptive Leitlinien

# AWS Präskriptive Leitlinien: Auswahl des richtigen Zugriffsansatzes für Amazon QuickSight

# Table of Contents

# Auswahl des richtigen Zugriffsansatzes für Amazon QuickSight

Henry Kong, Amazon Web Services (AWS)

Mai 2024 (Geschichte der Dokumente)

Amazon QuickSight ist ein Business Intelligence (BI) -Service auf Cloud-Ebene, der Sie dabei unterstützt, Ihre Daten in Dashboards zu visualisieren, zu analysieren und Berichte zu erstellen. Der Zugriff auf die meisten AWS-Services wird über AWS Identity and Access Management (IAM) und Richtlinien konfiguriert. Sie können den Zugriff auf mithilfe QuickSight von IAM konfigurieren, oder Sie können einen der anderen verfügbaren Ansätze verwenden, die direkt im Dienst konfiguriert werden können, z. B. lokale Benutzer, Verbund und Verzeichnisintegration. Für die meisten Anwendungsfälle AWS IAM Identity Center ist dies die empfohlene Methode zur Verwaltung des QuickSight Zugriffs. In diesem Handbuch werden die verfügbaren Optionen für die Bereitstellung des Zugriffs beschrieben, QuickSight sodass Sie die für Ihre Organisation geeignete Option auswählen können. Außerdem werden Anwendungsfälle sowie Faktoren der Konfiguration und des Betriebs erörtert, die diese Entscheidung beeinflussen können.

## Gezielte Geschäftsergebnisse

Dieser Leitfaden kann Ihnen und Ihrer Organisation dabei helfen, die folgenden Ziele zu erreichen:

- Machen Sie sich mit den verschiedenen Ansätzen zur Verwaltung des Benutzerzugriffs vertraut QuickSight
- Identifizieren Sie die verschiedenen Zugriffsfunktionen QuickSight , die für Ihr Unternehmen wichtig sind und die am besten auf Ihre Prozesse und Ihren Anwendungsfall abgestimmt sind
- Treffen Sie eine fundierte Entscheidung darüber, welcher QuickSight Zugriffsansatz für Ihr Unternehmen am besten geeignet ist

## Zielgruppe

Dieser Leitfaden richtet sich an Unternehmensarchitekten, Datenarchitekten sowie Identitäts- und Zugriffsarchitekten, die strategische technische Entscheidungen über den Einsatz von QuickSight in ihrem Unternehmen treffen.

# Die Ansätze im Überblick

Es gibt zwar viele verschiedene Ansätze, mit denen der Zugriff auf Amazon verwaltet werden kann QuickSight, aber der empfohlene Ansatz ist die AWS IAM Identity Center Integration. In einigen Fällen kann ein anderer Ansatz in Betracht gezogen werden, wenn Sie spezielle Anforderungen haben, auf die in diesem Leitfaden näher eingegangen wird.

Sie können die folgenden Methoden verwenden, um den Zugriff auf zu konfigurieren QuickSight:

- IAM Identity Center-Integration— Verwenden Sie die integrierte Serviceintegration zwischen QuickSight und IAM Identity Center, eine Funktion, die im August 2023 veröffentlicht wurde. Für diesen Ansatz ist die Enterprise Edition von QuickSight erforderlich.
- Verbundbenutzer— Verwalten Sie Benutzer mit einem Enterprise Identity Provider (IdP), um Benutzer zu authentifizieren, wenn sie sich anmelden. QuickSight
- Active Directory-Benutzer— Gewähren Sie Zugriff auf eine Verzeichnisgruppe in Microsoft Active Directory. Für diesen Ansatz ist die Enterprise Edition von erforderlich QuickSight. Die folgenden Optionen sind verfügbar:
  - AWS Directory Service for Microsoft Active Directory
  - AD Connector zeigt auf AWS Managed Microsoft AD
  - AD Connector, der auf ein selbstverwaltetes Verzeichnis verweist
- IAM-Benutzer— Gewähren Sie bestehenden AWS Identity and Access Management (IAM-) Benutzern Zugriff. Die folgenden Optionen sind verfügbar:
  - Senden Sie den IAM-Benutzern eine E-Mail-Einladung
  - Erteilen Sie IAM-Benutzern oder Benutzergruppen Berechtigungen zur Selbstbereitstellung
- QuickSight Benutzer— Erstellen Sie lokale Benutzer innerhalb von. QuickSight

Bei der Konfiguration des Benutzerzugriffs stehen viele Optionen zur Auswahl QuickSight. Wenn Sie die Vor- und Nachteile der einzelnen Ansätze verstehen, können Sie den richtigen Ansatz für Ihr Unternehmen ermitteln. Abhängig von bestimmten Umständen ist es auch möglich, mehr als einen Ansatz für Ihr Unternehmen zu wählen. Dies erhöht jedoch die Komplexität der Bereitstellungsvorgänge.

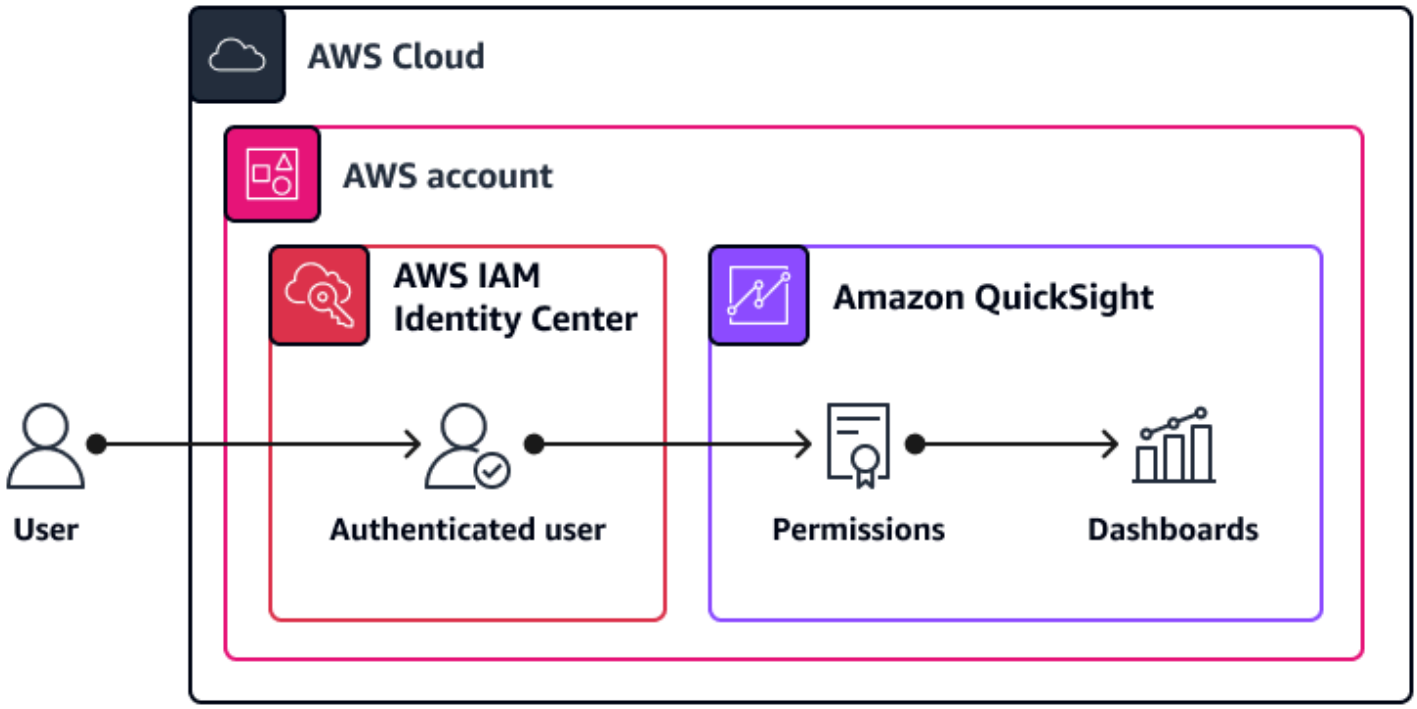
# Unterschiede zwischen den Editionen QuickSight

Die Optionen für die Zugriffsverwaltung variieren zwischen den Editionen Standard und Enterprise von QuickSight. In der folgenden Tabelle werden die jeweiligen Zugriffsoptionen verglichen. Weitere Informationen finden Sie in der QuickSight Dokumentation unter Benutzerverwaltung zwischen den Editionen.

| Zugriffsansatz | Standard Edition | Enterprise Edition |
|---|---|---|
| QuickSight Benutzer | Ja | Ja |
| IAM-Benutzer | Ja | Ja |
| Active Directory-Benutzer | Nein | Ja |
| IAM Identity Center-Integration | Nein | Ja |
| Verbundbenutzer | Ja | Ja |

# QuickSight Zugriff über die IAM Identity Center-Integration gewähren

> **Note**
>
> Dieser Zugriffsansatz ist nur für die Enterprise Edition von Amazon verfügbar QuickSight. Weitere Informationen finden Sie in der QuickSight Dokumentation unter Benutzerverwaltung für die Enterprise Edition.




Im Folgenden sind die Merkmale dieser Architektur und dieses Zugriffsansatzes aufgeführt:

- Benutzer und Gruppen werden AWS IAM Identity Center über eine der folgenden Identitätsquellen verwaltet:
  - Ein externer Identitätsanbieter
  - Ein Microsoft Active Directory-Verzeichnis
  - Ein IAM Identity Center-Verzeichnis
- Je nach Ihren Anforderungen können Sie entweder eine Organisationsinstanz oder eine Kontoinstanz von IAM Identity Center verwenden. Wenn externe Benutzer beispielsweise Zugriff

auf die Organisationsinstanz benötigen, diese QuickSight aber nicht verfügbar sind oder nicht in der Organisationsinstanz bereitgestellt werden dürfen, können Sie eine Kontoinstanz verwenden, die eine Identitätsquelle verwendet, die sowohl interne als auch externe Benutzer unterstützt.

- Sie weisen IAM Identity Center-Gruppen QuickSight Administrator-, Autoren- oder Leserzugriff zu.
- QuickSight Der Zugriff wird auf der Grundlage der zugewiesenen IAM Identity Center-Gruppenmitgliedschaften bereitgestellt.
- Sie können diesen QuickSight Zugriffsansatz nicht mit anderen Ansätzen kombinieren.

## Überlegungen und Anwendungsfälle

Es wird empfohlen, IAM Identity Center zu verwenden, um den Zugriff auf zu QuickSight verwalten. Es gibt zwei Ansätze, die Sie mit IAM Identity Center verwenden können. QuickSight ist eine IAM Identity Center-fähige Anwendung und unterstützt die native Integration, was der empfohlene Ansatz ist. Es ist auch möglich, den SAML 2.0-Verbund zu verwenden, wie Konfiguration des Verbundbenutzerzugriffs QuickSight über IAM Identity Center in diesem Handbuch beschrieben, aber dieser Ansatz wird für die meisten Anwendungsfälle nicht empfohlen.

Für die native Serviceintegration zwischen QuickSight und IAM Identity Center ist keine Einrichtung eines SAML-Verbunds zwischen den beiden Diensten erforderlich. Die native Integration verwendet IAM Identity Center-Gruppenmitgliedschaften, um den Zugriff auf zu verwalten. QuickSight

IAM Identity Center-Benutzergruppen werden automatisch mit synchronisiert. QuickSight In der QuickSight Konsole können Administratoren die IAM Identity Center-Gruppen den QuickSight Rollen zuordnen. Gruppen können die Rollen Admin, Author, Reader, Admin Pro, Author Pro oder Reader Pro zugewiesen werden.

Dieser Ansatz ist nützlich, da Sie dafür weder die Verbundkonfiguration noch irgendwelche Berechtigungssätze beibehalten müssen. Sobald dieser Ansatz implementiert ist, können Sie in future jedoch nicht mehr zu einem anderen Ansatz, z. B. einem Verbund, wechseln, ohne Ihr QuickSight Abonnement zu beenden. Sie können diesen Ansatz auch nicht mit anderen Ansätzen kombinieren.

Weitere Einschränkungen im Zusammenhang mit der Verwendung der QuickSight nativen Integration mit IAM Identity Center finden Sie in der QuickSightDokumentation. Beispielsweise wird die Verwendung der Namespaces-Funktion in QuickSight nicht unterstützt, wenn Sie die IAM Identity Center-Integration verwenden.

# Voraussetzungen

- Ein aktiver AWS-Konto
- Die folgenden Berechtigungen:
  - Administratorzugriff auf das AWS-Konto Where QuickSight ist abonniert
  - Zugriff auf die IAM Identity Center-Konsole, um Benutzer Gruppen zuzuweisen

# Konfiguration der IAM Identity Center-Integration und des Benutzerzugriffs

Beachten Sie bei der Konfiguration dieser Art von Zugriff Folgendes:

1. Stellen Sie vor dem Abonnieren sicher QuickSight, dass Sie IAM Identity Center bereits eingerichtet und konfiguriert haben. Anweisungen finden Sie in den Tutorials „Aktivierung“ AWS IAM Identity Center und „Erste Schritte“ in der IAM Identity Center-Dokumentation.
2. Folgen Sie den Anweisungen unter Registrierung für ein QuickSight Abonnement in der QuickSight Dokumentation. Wählen Sie Enterprise und anschließend IAM Identity Center-fähige Anwendung verwenden aus. Je nachdem, welche vorhandenen IAM Identity Center-Instanzen in Ihrer verfügbar sind AWS-Konto, können Sie zwischen einer Organisationsinstanz oder einer Kontoinstanz wählen.
3. Um IAM Identity Center-Gruppen QuickSight Rollen zuzuweisen, folgen Sie den Anweisungen unter Zugriff für IAM Identity Center-Benutzer verwalten in der Dokumentation. QuickSight

# QuickSight Zugriff für Verbundbenutzer gewähren

Wenn Sie föderierte Identitäten verwenden, können Sie Benutzer mit einem externen Identitätsanbieter (IdP) verwalten, um Benutzer zu authentifizieren, wenn sie sich bei Amazon anmelden. QuickSight QuickSight unterstützt den Identitätsverbund mit SAML 2.0. Viele externe Anbieter IdPs, wie Okta und Ping, verwenden diesen Standard. Sie können es auch AWS IAM Identity Center als externen IdP für einen SAML QuickSight 2.0-Verbundzugriffsansatz verwenden. Wir empfehlen jedoch die IAM Identity Center-Integration in diesem Handbuch beschriebene integrierte Serviceintegration anstelle des föderierten Benutzeransatzes. Wenn Sie IAM Identity Center verwenden, wird der Verbundbenutzeransatz nur empfohlen, wenn Sie die IAM Identity Center-Integration aufgrund der aktuellen Funktionseinschränkungen nicht verwenden können.

Verbundbenutzer verfügen über ein Single Sign-On-Erlebnis (SSO), und Sie können Zugriff gewähren, QuickSight ohne für jede Person in Ihrer Organisation einen AWS Identity and Access Management (IAM-) Benutzer oder QuickSight lokalen Benutzer zu erstellen. Darüber hinaus stellt der Verbund Benutzern temporäre Anmeldeinformationen zur Verfügung, was eine bewährte Sicherheitsmethode darstellt. Weitere Informationen zum Identitätsverbund sowie zu seinen Vorteilen und Anwendungsfällen finden Sie unter Identitätsverbund in AWS.

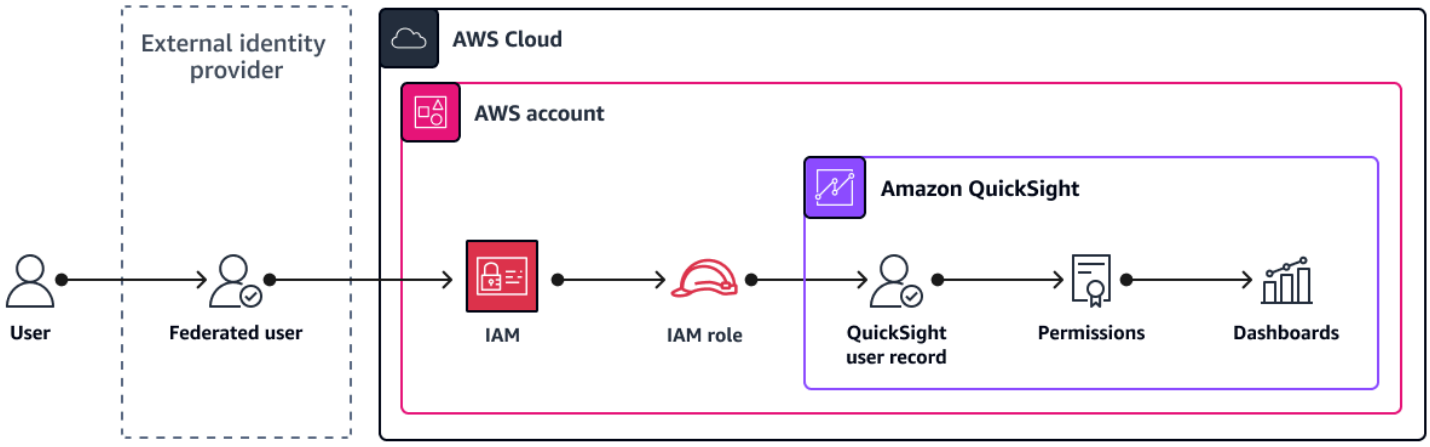
Bei der Konfiguration des Zugriffs auf QuickSight für Verbundbenutzer können Sie einen der folgenden Ansätze verwenden:

- Konfiguration des föderierten Benutzerzugriffs QuickSight über IAM und einen externen IdP
- Konfiguration des Verbundbenutzerzugriffs QuickSight über IAM Identity Center

Bei beiden Ansätzen können Verbundbenutzer den Zugriff auf selbst bereitstellen. QuickSight Die Ansätze variieren je nach Architektur und Diensten, die für den Verbund verwendet werden. In beiden Lösungen nimmt der Verbundbenutzer dann jedoch eine IAM-Rolle an, die bestimmt, über welche Berechtigungen er verfügt. QuickSight

Wenn Sie die QuickSight Enterprise Edition verwenden, können Sie Benutzer, die ihren Zugriff selbst bereitstellen, dazu zwingen, sich mit der im Identitätsanbieter definierten E-Mail-Adresse anzumelden. QuickSight Weitere Informationen finden Sie unter QuickSight E-Mail-Synchronisierung für Verbundbenutzer.

# Konfiguration des föderierten Benutzerzugriffs QuickSight über IAM und einen externen IdP




Im Folgenden sind die Merkmale dieser Architektur aufgeführt:

- Der QuickSight Amazon-Benutzerdatensatz ist mit einer AWS Identity and Access Management (IAM-) Rolle und dem Benutzernamen im IdP verknüpft, z. B. `QuickSightReader/DiegoRamirez@example.com`
- Benutzer können den Zugriff selbst bereitstellen.
- Benutzer melden sich bei ihrem externen Identitätsanbieter an.
- Wenn die E-Mail-Synchronisierung deaktiviert ist, können Benutzer bei der Anmeldung ihre bevorzugte E-Mail-Adresse angeben QuickSight. Wenn die E-Mail-Synchronisierung aktiviert ist, wird die im Unternehmens-IdP definierte E-Mail-Adresse QuickSight verwendet. Weitere Informationen finden Sie unter QuickSight E-Mail-Synchronisierung für Verbundbenutzer in diesem Handbuch.
- Die IAM-Rolle enthält eine Vertrauensrichtlinie, die es nur Verbundbenutzern Ihres externen IdP ermöglicht, die Rolle zu übernehmen.

## Überlegungen und Anwendungsfälle

Wenn Sie den Identitätsverbund bereits für den Zugriff auf Ihre verwenden AWS-Konten, können Sie diese bestehende Konfiguration verwenden, um auch den Zugriff auf zu erweitern QuickSight. Für QuickSight den Zugriff können Sie dieselben Prozesse wiederverwenden, die Sie für die Bereitstellung und Überprüfung des Zugriffs eingerichtet haben. AWS-Konten

### Voraussetzungen

- Administratorberechtigungen in QuickSight.
- Ihre Organisation verwendet bereits einen externen Identitätsanbieter, wie Okta or Ping.

### Konfigurieren des Zugriffs

Anweisungen finden Sie unter Einrichten eines IdP-Verbunds mithilfe von IAM und QuickSight in der QuickSight Dokumentation. Weitere Informationen zur Konfiguration der Berechtigungsrichtlinie für QuickSight finden Sie Konfigurieren von IAM-Richtlinien in diesem Handbuch.

## Konfiguration des Verbundbenutzerzugriffs QuickSight über IAM Identity Center

Wenn Ihr Unternehmen diesen Service bereits verwendet AWS IAM Identity Center, möchten Sie diesen Service möglicherweise zur Authentifizierung verbundener Benutzer verwenden. Sie können den SAML 2.0-Verbund oder die integrierte Dienstintegration zwischen IAM Identity Center verwenden. Weitere Informationen zur integrierten Serviceintegration finden Sie IAM Identity Center-Integration in diesem Handbuch.

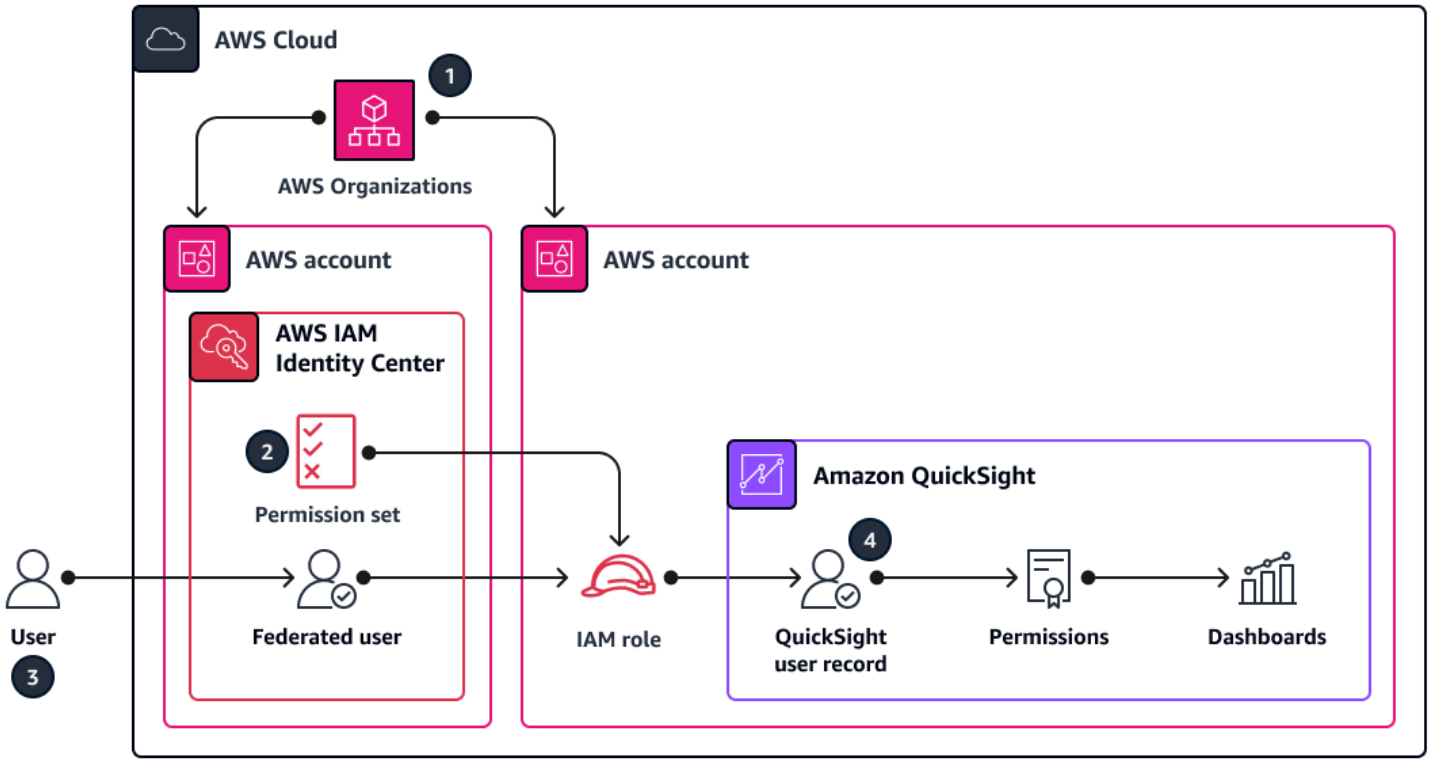
Wenn Sie den SAML 2.0-Verbund mit IAM Identity Center verwenden, gibt es zwei Methoden, um den Verbundbenutzerzugriff zu konfigurieren: QuickSight

- Konfiguration von Berechtigungen mithilfe von Berechtigungssätzen— Sie können diesen Ansatz nur verwenden, wenn Sie AWS-Konten für das IAM Identity Center zuständig QuickSight sind und Mitglieder derselben Organisation sind. AWS Organizations Ein Berechtigungssatz ist eine Vorlage, die eine Sammlung von einer oder mehreren AWS Identity and Access Management (IAM-) Richtlinien definiert. Berechtigungssätze können die Berechtigungsverwaltung in Ihrer Organisation vereinfachen.
- Konfiguration von Berechtigungen mithilfe von IAM-Rollen— Dieser Ansatz ist gut geeignet, wenn das AWS-Konto QuickSight Formular nicht Teil derselben Organisation wie IAM Identity Center ist. Bei diesem Ansatz erstellen Sie die IAM-Rollen direkt im selben Konto mit. QuickSight

Bei beiden Ansätzen können Benutzer ihren eigenen QuickSight Zugriff selbst bereitstellen. Wenn die QuickSight E-Mail-Synchronisierung deaktiviert ist, können Benutzer bei der Anmeldung ihre bevorzugte E-Mail-Adresse angeben. Wenn die E-Mail-Synchronisierung aktiviert ist, wird die im

Unternehmens-IdP definierte E-Mail-Adresse QuickSight verwendet. Weitere Informationen finden Sie unter QuickSight E-Mail-Synchronisierung für Verbundbenutzer in diesem Handbuch.

## Konfiguration von Berechtigungen mithilfe von Berechtigungssätzen




Im Folgenden sind die Merkmale dieser Architektur und dieses Zugriffsansatzes aufgeführt:

1. Sie sind AWS-Konten für IAM Identity Center und QuickSight befinden sich in derselben Organisation in AWS Organizations.
2. Der Berechtigungssatz, den Sie in IAM Identity Center definieren, verwaltet und steuert die IAM-Rolle.
3. Benutzer melden sich über IAM Identity Center an.
4. Der QuickSight Benutzerdatensatz ist mit der von IAM Identity Center verwalteten IAM-Rolle und dem Benutzernamen verknüpft, z. B. `AWSReservedSSO_QuickSightReader_7oe58cd620501f23/DiegoRamirez@example.com`

### Voraussetzungen

- Ein aktives Konto QuickSight

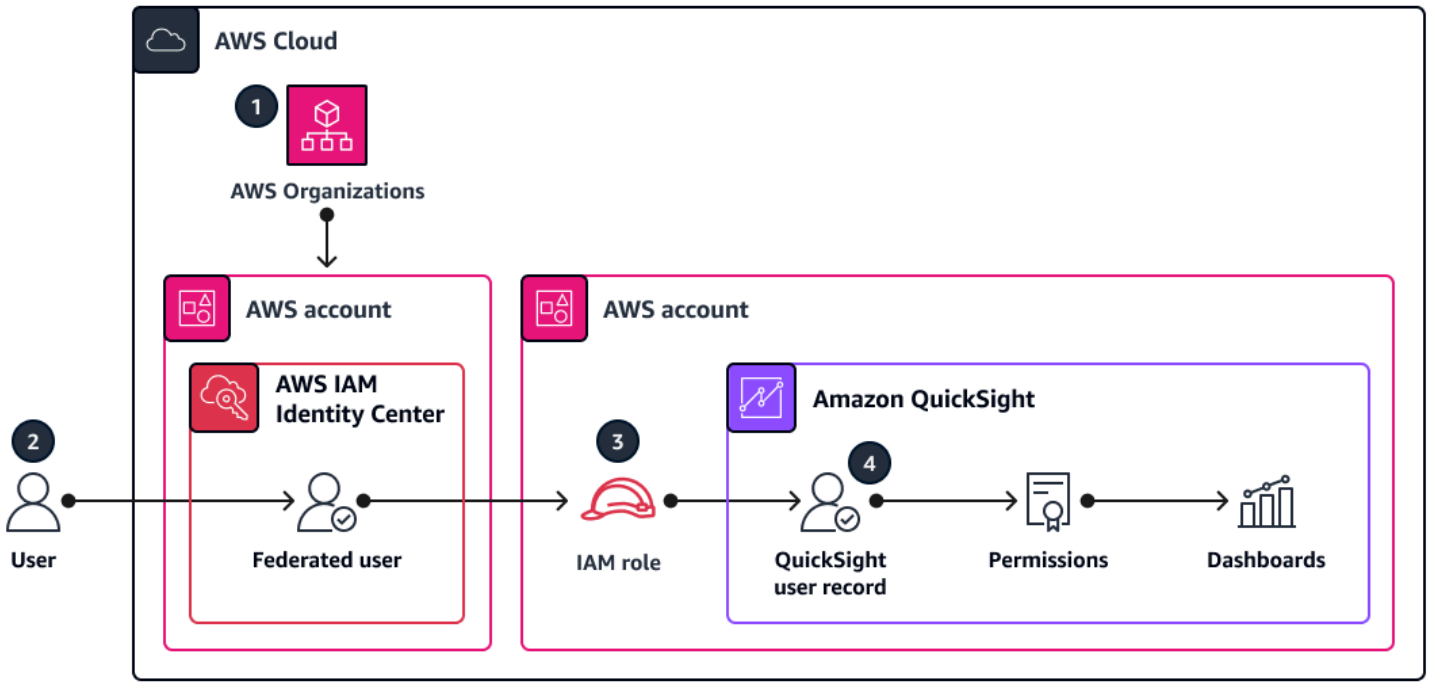
- Die folgenden Berechtigungen:
  - Administratorzugriff auf das AWS-Konto Where QuickSight ist abonniert
  - Zugriff auf die IAM Identity Center-Konsole und Berechtigungen zum Erstellen von Berechtigungssätzen

### Konfigurieren des Zugriffs

Stellen Sie vor dem Abonnieren sicher QuickSight, dass Sie IAM Identity Center bereits eingerichtet und konfiguriert haben. Anweisungen finden Sie in den Tutorials „Aktivierung“ AWS IAM Identity Center und „Erste Schritte“ in der IAM Identity Center-Dokumentation. Nachdem Sie IAM Identity Center in Ihrer Organisation konfiguriert haben, erstellen Sie in IAM Identity Center einen benutzerdefinierten Berechtigungssatz, der Verbundbenutzern den Zugriff ermöglicht. QuickSight Anweisungen finden Sie in der IAM Identity Center-Dokumentation unter Einen Berechtigungssatz erstellen. Weitere Informationen zur Konfiguration der Richtlinien, die Sie in den Berechtigungssatz aufnehmen, finden Sie Konfigurieren von IAM-Richtlinien in diesem Handbuch.

Nachdem Sie den Berechtigungssatz erstellt haben, stellen Sie ihn dem Ziel zur Verfügung, auf AWS-Konto dem er angemeldet QuickSight ist, und wenden Sie ihn dann auf die Benutzer und Gruppen an, die QuickSight Zugriff benötigen. Weitere Informationen zum Zuweisen von Berechtigungssätzen finden Sie AWS-Konten in der IAM Identity Center-Dokumentation unter Benutzerzugriff zuweisen.

## Konfiguration von Berechtigungen mithilfe von IAM-Rollen




Im Folgenden sind die Merkmale dieses Architektur- und Zugriffsansatzes aufgeführt:

1. Sie sind AWS-Konten für IAM Identity Center und QuickSight befinden sich nicht in derselben Organisation in AWS Organizations.
2. Benutzer melden sich über IAM Identity Center oder über den externen IdP an, den Sie in IAM Identity Center als Identitätsquelle konfiguriert haben.
3. Die IAM-Rolle enthält eine Vertrauensrichtlinie, die es nur Verbundbenutzern aus IAM Identity Center ermöglicht, die Rolle zu übernehmen.
4. Der QuickSight Benutzerdatensatz ist mit einer IAM-Rolle und dem Benutzernamen im IdP verknüpft, z. B. `QuickSightReader/DiegoRamirez@example.com`

## Voraussetzungen

- Ein aktives QuickSight Konto.
- Die folgenden Berechtigungen:
  - Administratorzugriff auf das AWS-Konto Where QuickSight ist abonniert.
  - Zugriff auf die IAM Identity Center-Konsole und Berechtigungen zur Verwaltung von Anwendungen.

- Sie haben IAM Identity Center eingerichtet und konfiguriert. Anweisungen finden Sie in den Tutorials „Aktivierung“ AWS IAM Identity Center und „Erste Schritte“ in der IAM Identity Center-Dokumentation.
- Sie haben IAM Identity Center als vertrauenswürdigen IdP in IAM konfiguriert. Anweisungen finden Sie in der IAM-Dokumentation unter Erstellen von IAM-Identitätsanbietern.

### Konfigurieren des Zugriffs

Anweisungen finden Sie im AWS IAM Identity Center Integrationsleitfaden für Amazon QuickSight. Nachdem Sie IAM Identity Center als vertrauenswürdigen Identitätsanbieter für konfiguriert haben AWS-Konto, erstellen Sie eine IAM-Rolle, auf die Verbundbenutzer zugreifen können. QuickSight Anweisungen finden Sie in der IAM-Dokumentation unter IAM-Rollen erstellen. Weitere Informationen zur Konfiguration der Richtlinien für QuickSight finden Sie Konfigurieren von IAM-Richtlinien in diesem Handbuch.

## QuickSight E-Mail-Synchronisierung für Verbundbenutzer

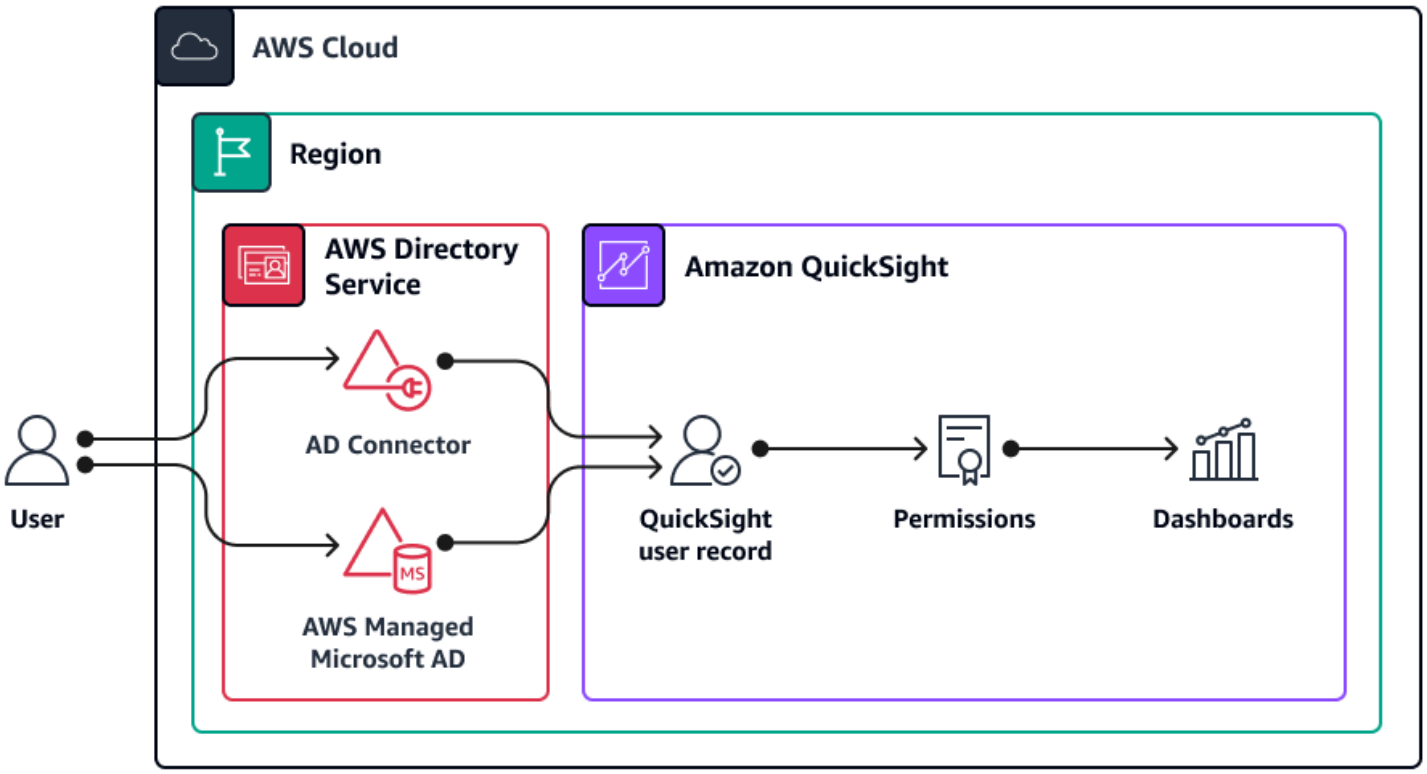
> **Note**
>
> Diese Funktion ist nur für die Enterprise Edition von Amazon verfügbar QuickSight.

Wenn IAM-Benutzer den Zugriff selbst bereitstellen QuickSight, können Administratoren nicht kontrollieren, an welche E-Mail-Adresse der Benutzer Daten weitergibt. QuickSight Benutzer könnten statt ihrer geschäftlichen E-Mail-Adresse eine persönliche E-Mail-Adresse eingeben. Dies ist für einige Organisationen möglicherweise nicht akzeptabel. Wenn Sie jedoch einen Identitätsanbieter für den Verbundzugriff auf die QuickSight Enterprise Edition verwenden, QuickSight verfügt diese Version über eine Funktion, die sicherstellt, dass die E-Mail-Adresse des Benutzers mit der E-Mail-Adresse des Benutzers im Identitätsanbieter QuickSight übereinstimmt.

Im IdP fügen Sie ein SAML-Attribut für die E-Mail-Adresse des Benutzers hinzu. Der Prozess zur Erstellung des Attributs oder Tokens ist für jeden IdP unterschiedlich. Lesen Sie die Anweisungen für Okta oder IAM Identity Center oder lesen Sie die Dokumentation für den IdP Ihrer Organisation. Der IdP übergibt die E-Mail-Adresse des Benutzers als `Principal` IAM-Sitzungs-Tag. QuickSight verwendet dieses Sitzungs-Tag, anstatt den Benutzer zur Angabe seiner E-Mail-Adresse aufzufordern. Anweisungen zur Aktivierung dieser Funktion finden Sie in der Dokumentation unter Konfiguration der E-Mail-Synchronisierung für Verbundbenutzer. QuickSight

# QuickSight Zugriff für Active Directory-Benutzer gewähren

> **Note**
>
> Dieser Zugriffsansatz ist nur für die Enterprise Edition von Amazon verfügbar QuickSight. Weitere Informationen finden Sie in der QuickSight Dokumentation unter Benutzerverwaltung für die Enterprise Edition.




Im Folgenden sind die Merkmale dieses Architektur- und Zugriffsansatzes aufgeführt:

- Der QuickSight Amazon-Benutzerdatensatz ist mit dem Benutzer in Active Directory verknüpft.
- Sie weisen Active Directory-Gruppen QuickSight Administrator-, Autoren- oder Leserzugriff zu.
- QuickSight Der Zugriff wird auf der Grundlage der zugewiesenen Active Directory-Gruppenmitgliedschaften bereitgestellt.
- Benutzerkennwörter werden in Active Directory verwaltet.
- Der Benutzer muss sich direkt über die QuickSight Konsole unter https://quicksight.aws.amazon.com/anmelden.

- Sie können diesen QuickSight Zugriffsansatz nicht mit anderen Ansätzen kombinieren.

## Überlegungen und Anwendungsfälle

Sie können Microsoft Active Directory-Benutzer und -Gruppen verwenden, um den Zugriff auf zu verwalten QuickSight. QuickSight unterstützt entweder den AWS Directory Service for Microsoft Active Directory (AWS Managed Microsoft AD) oder den Active Directory Connector (AD Connector).

AWS Managed Microsoft AD ist ein Active Directory-Host in der AWS Cloud , der die meisten Funktionen von Active Directory bietet. Wenn Sie über ein vorhandenes selbstverwaltetes Verzeichnis verfügen, das Sie für verwenden möchten QuickSight, können Sie AD Connector verwenden. Dieser Dienst leitet Verzeichnisanfragen an Ihr selbstverwaltetes Active Directory weiter — in einem anderen AWS-Region oder vor Ort —, ohne dass Informationen in der Cloud zwischengespeichert werden. Sowohl AD Connector als auch AWS Managed Microsoft AD sind Teil von AWS Directory Service.

Ihr Verzeichnis oder Ihre Verzeichnisverbindung AWS Directory Service muss sich in demselben Verzeichnis befinden AWS-Region , für das Sie sich anmelden QuickSight. Bei der Registrierung für QuickSight geben Sie die Active Directory-Domäne sowie die spezifischen Active Directory-Gruppen an, die für die Zugriffskontrolle verwendet werden.

Dieser Zugriffsansatz eignet sich am besten für Unternehmen, die ihre bestehenden Active Directory-Zugriffsverwaltungsprozesse nutzen möchten. Dieser Ansatz verwaltet QuickSight den Zugriff und die Rollen über Active Directory-Gruppenmitgliedschaften.

Ein wichtiger Aspekt bei der Verwendung dieses Ansatzes ist, dass er nicht mit anderen Ansätzen kombiniert werden kann. Sie können beispielsweise einen hybriden Zugriffsansatz mit IAM-Benutzern und QuickSight lokalen Benutzern erstellen. Überlegen Sie sich diesen Ansatz sorgfältig. Wenn Sie diesen Ansatz bei der Einrichtung wählen QuickSight, verpflichten Sie sich dazu. Sie können später nicht zu einem anderen Ansatz wechseln.

Dies ist nicht der einzige Zugriffsansatz, der Active Directory verwendet. Bei diesem Ansatz wird der QuickSight Zugriff auf der Grundlage der Gruppenmitgliedschaft in Active Directory bereitgestellt, und der QuickSight Benutzerdatensatz ist direkt mit dem Active Directory-Benutzer verknüpft. Sie können Active Directory auch als Identitätsquelle für den Benutzerverbund verwenden. Weitere Informationen finden Sie unter Verbundbenutzer in diesem Handbuch.

## Voraussetzungen

- Enterprise Edition von QuickSight
- Berechtigungen zum Abonnieren QuickSight, Erstellen von Benutzern und Verwalten von Active Directory (siehe identitätsbasierte IAM-Richtlinien für Amazon QuickSight: All Access for Enterprise Edition)

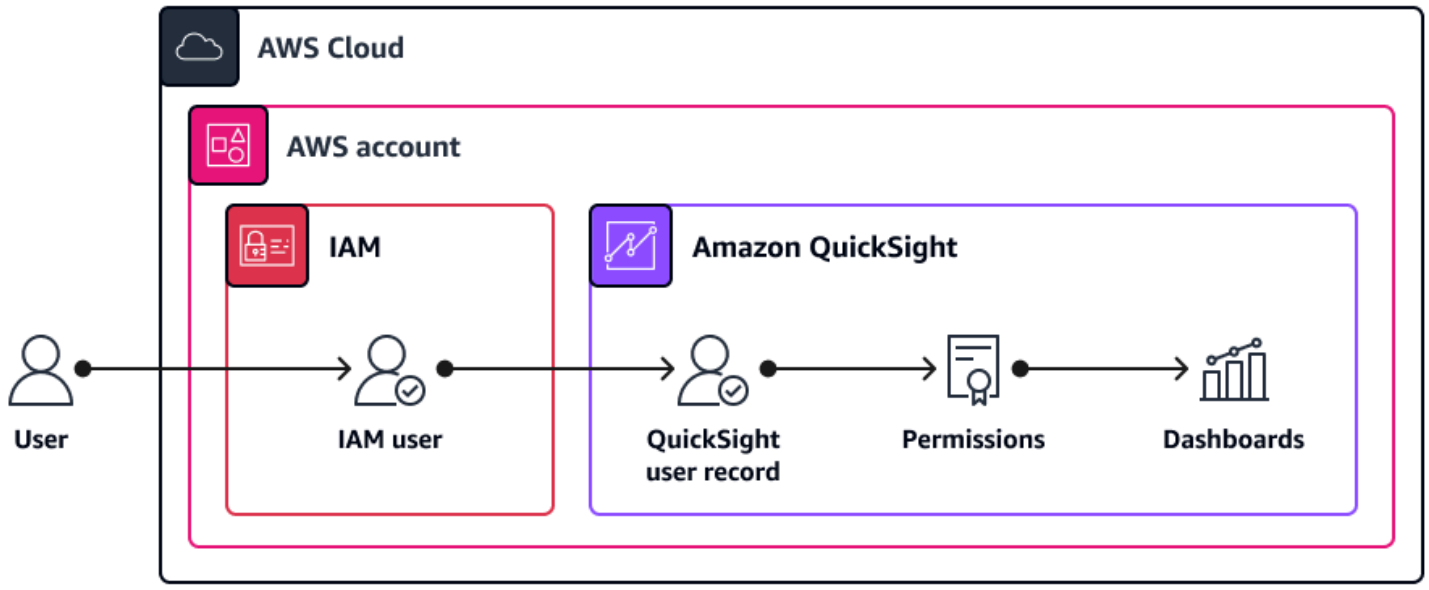
## Konfiguration des Zugriffs für Active Directory-Benutzer

Nachdem Sie die Details Ihres Verzeichnisses bestätigt haben, können Sie sich für registrieren QuickSight. Anweisungen finden Sie unter Für ein QuickSight Abonnement anmelden. Beachten Sie bei der Konfiguration dieser Art von Zugriff Folgendes:

1. Wählen Sie im QuickSight Anmeldeassistenten Enterprise und anschließend Use Active Directory aus.
2. Gehen Sie zur QuickSight Konsole und wählen Sie dann Zugriff verwalten auf QuickSight.
3. Wählen Sie die Active Directory-Gruppen aus, die QuickSight Zugriff haben sollen, und weisen Sie ihnen QuickSight Administrator-, Autor- oder Leserrollen zu. Anweisungen finden Sie unter Benutzerzugriff verwalten.

# QuickSight Zugriff für IAM-Benutzer gewähren

> **Note**
>
> Ein IAM-Benutzer ist eine Entität, die Sie in AWS Identity and Access Management (IAM) erstellen. Diese Art von Entität greift AWS-Konto mithilfe langfristiger Anmeldeinformationen auf Ihre zu. Als bewährte Methode AWS empfiehlt es sich, den Zugriff über temporäre Anmeldeinformationen zu gewähren, indem Sie Identitätsverbund- und IAM-Rollen verwenden. Weitere Informationen finden Sie unter Bewährte IAM-Methoden.




Im Folgenden sind die Merkmale dieses Architektur- und Zugriffsansatzes aufgeführt:

- Der QuickSight Amazon-Benutzerdatensatz ist mit dem Benutzer in IAM verknüpft.
- Benutzerkennwörter werden in IAM verwaltet.
- Sie können IAM-Benutzer direkt einladen oder eine identitätsbasierte IAM-Richtlinie erstellen, die es Benutzern ermöglicht, den Zugriff selbst bereitzustellen.
- Dieser Benutzertyp kann sich über die Konsole oder über die QuickSight anmelden. AWS Management Console

# Überlegungen und Anwendungsfälle

Es wird zwar AWS generell nicht empfohlen, den Zugriff über IAM-Benutzer zu konfigurieren, aber andere Zugriffsansätze, wie z. B. Verbundzugriff, sind in Ihrer Organisation derzeit möglicherweise nicht verfügbar. Viele Unternehmen, die gerade erst mit der Umstellung auf die Cloud beginnen, haben noch keine IAM-Rollen eingerichtet und arbeiten in einer Architektur mit einem einzigen Konto. Wenn Ihr Unternehmen IAM-Benutzer für den Zugriff auf Ihre AWS Umgebung verwendet, ist es QuickSight möglicherweise am einfachsten und sinnvollsten, diesen Ansatz erneut anzuwenden, bis Ihr Unternehmen andere Ansätze unterstützt.

# Voraussetzungen

- Für den Ansatz mit direkter Einladung benötigen Sie:
  - Administratorberechtigungen in QuickSight (siehe identitätsbasierte IAM-Richtlinien für die Standard - oder Enterprise-Editionen)
  - Die E-Mail-Adresse des IAM-Benutzers
- Für den selbstbereitgestellten Zugriffsansatz benötigt der Benutzer Berechtigungen zum Erstellen von Amazon QuickSight (siehe IAM-Richtlinien für identitätsbasierte IAM-Richtlinien für Amazon: Benutzer erstellen) QuickSight
- Der IAM-Benutzer muss über ein Passwort verfügen, das mit seinen IAM-Anmeldeinformationen verknüpft ist

# Konfiguration des Zugriffs für einen IAM-Benutzer

Sie können IAM-Benutzern Zugriff QuickSight gewähren, indem Sie eine der folgenden Optionen verwenden:

- Direkte Einladung — Sie laden den IAM-Benutzer zum Zugriff ein QuickSight, und der Benutzer kann die Einladung per E-Mail annehmen.
- Selbstbereitgestellter Zugriff — Sie erstellen eine IAM-Richtlinie, die es Benutzern ermöglicht, ihren eigenen Zugriff bereitzustellen. Wenn ein Benutzer QuickSight zum ersten Mal zugreift, erhält er Zugriff und definiert die E-Mail-Adresse, die mit seinem Benutzerdatensatz verknüpft wird. QuickSight

Das Ergebnis beider Optionen ist dasselbe: Der IAM-Benutzer kann darauf zugreifen. QuickSight Beide haben jedoch Vor- und Nachteile, wie in der folgenden Tabelle dargestellt. Beispielsweise könnte die direkte Einladung für Organisationen vorzuziehen sein, die die Verwendung genehmigter Unternehmens-E-Mail-Adressen erzwingen möchten.

| Ansatz | Vorteile | Nachteile |
| --- | --- | --- |
| Direkte Einladung | • Administratoren können steuern, welche E-Mail-Adresse mit dem Benutzerdatensatz verknüpft ist QuickSight<br>• Keine Aufgaben zur IAM-Richtlinienverwaltung | • Noch mehr Manuelles |
| Selbst bereitgestellter Zugriff | • Kann in bestehende IT-Betriebsprozesse integriert werden, um den Zugriff über IAM-Richtlinien bereitzustellen, wobei die Fähigkeit zur Selbstbereitstellung bereits Teil der bestehenden IAM-Richtlinien ist | • Administratoren können nicht kontrollieren, an welche E-Mail-Adresse der Benutzer sie weitergibt QuickSight |

## Direkte Einladung

Anweisungen zur Konfiguration des Zugriffs für einen IAM-Benutzer finden Sie unter Benutzer zum Zugriff auf Amazon QuickSight einladen. Beachten Sie bei der Konfiguration dieser Art von Benutzerzugriff Folgendes:

- Geben Sie als QuickSight Benutzernamen den Benutzernamen des IAM-Benutzers ein. Zulässige Zeichen sind Buchstaben, Zahlen und die folgenden Zeichen:. _ - (Bindestrich).
- Wählen Sie für IAM-Benutzer die Option Ja aus.
- Der Benutzer hat sieben Tage Zeit, um die Einladung anzunehmen. Wenn er innerhalb dieses Zeitraums nicht annimmt, können Sie die Einladungs-E-Mail erneut senden.

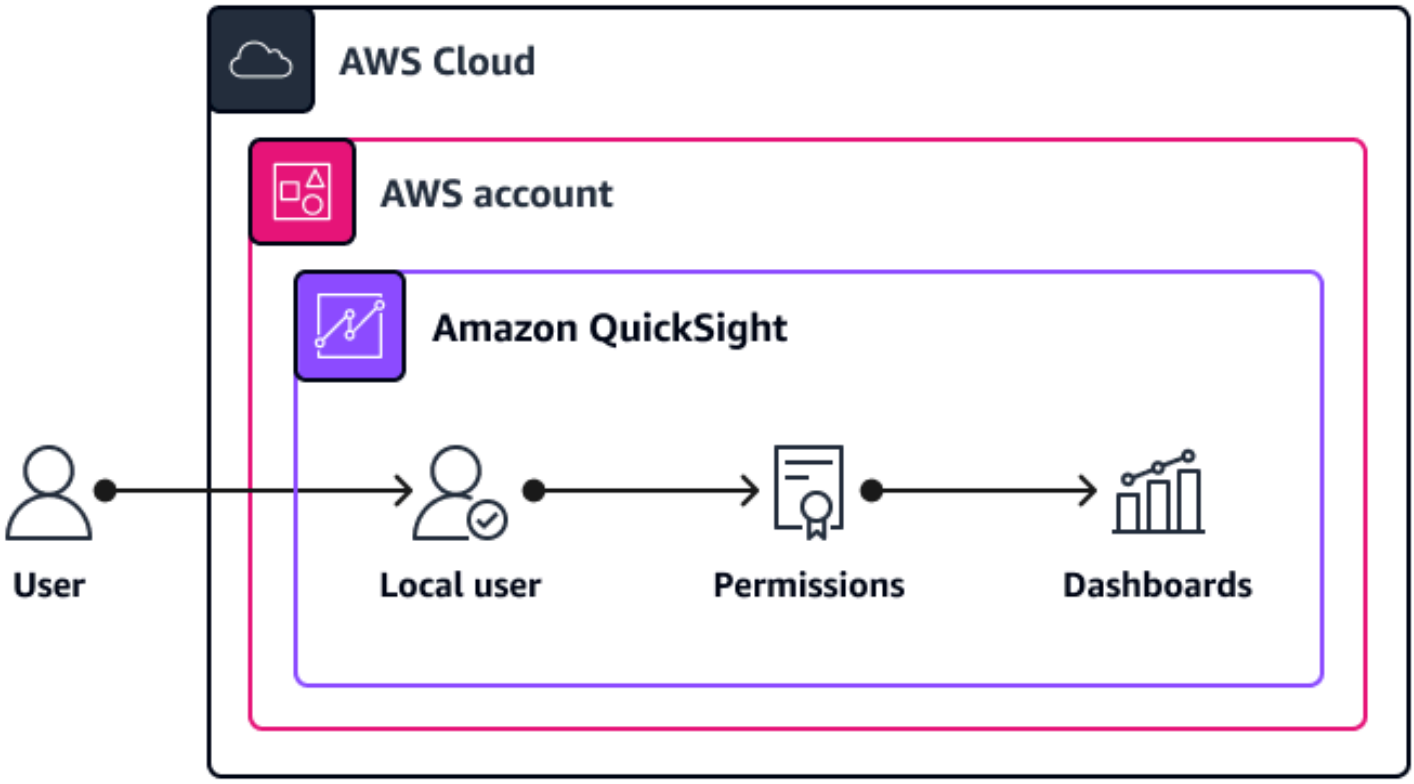
- Wenn der Benutzer die Einladung annimmt, muss er das Passwort eingeben, das seinen IAM-Anmeldeinformationen zugeordnet ist.

## Selbst bereitgestellter Zugriff

Wenn IAM-Benutzer den Zugriff selbst bereitstellen können, müssen sie nicht zu dem Konto eingeladen werden. QuickSight Wenn sie zum ersten Mal versuchen, auf die QuickSight Konsole zuzugreifen, müssen sie eine E-Mail-Adresse eingeben. Wenn der Benutzer Weiter auswählt, QuickSight wird ein Benutzerdatensatz für diesen IAM-Benutzer erstellt.

Um ihnen die Erlaubnis zu erteilen, ihren eigenen Zugriff bereitzustellen, erstellen Sie eine identitätsbasierte Richtlinie und wenden diese Richtlinie auf die IAM-Benutzer oder die IAM-Benutzergruppe an. Weitere Informationen finden Sie unter Konfigurieren von IAM-Richtlinien in diesem Handbuch.

# Lokale Benutzer erstellen in QuickSight




Im Folgenden sind die Merkmale dieses Architektur- und Zugriffsansatzes aufgeführt:

- Dieser Benutzer hat QuickSight nur Zugriff auf Amazon und kann nicht auf andere Dienste und Ressourcen in Ihrem zugreifen AWS-Konto.
- Das Passwort des Benutzers wird lokal in verwaltet QuickSight.
- Sie gewähren den Zugriff, indem Sie den Benutzer über seine E-Mail-Adresse einladen.
- Der Benutzer muss sich direkt über die QuickSight Konsole unter https://quicksight.aws.amazon.com/anmelden.

## Überlegungen und Anwendungsfälle

Dies ist die direkteste Methode, Zugriff auf zu gewähren, QuickSight da dadurch ein lokaler Benutzerdatensatz im QuickSight Benutzerspeicher erstellt wird und keine externen Abhängigkeiten bestehen. Dieser Benutzerdatensatz existiert nur in QuickSight und hat ein Passwort, das auch in verwaltet wird QuickSight.

Dieser Ansatz ist wahrscheinlich auch der flexibelste, da die einzige Voraussetzung darin besteht, eine E-Mail-Adresse für den Benutzer zu haben. Sie müssen keine Benutzer in einem anderen Dienst oder Verzeichnis erstellen und verwalten, und es kann eine schnelle Möglichkeit sein, Drittanbietern oder Partnern Zugriff zu gewähren, die auf Ihre QuickSight Dashboards zugreifen müssen. Dieser Zugriffsansatz eignet sich am besten für Benutzer, die QuickSight nur Zugriff auf andere Dienste und Ressourcen in der AWS-Konto benötigen und keinen Zugriff auf diese benötigen.

Da es sich um lokale Benutzer handelt QuickSight, müssen die IT-Betriebsteams spezielle Prozesse für die Verwaltung von Zugriffsanfragen, die Bereitstellung von Zugriff und die regelmäßige Überprüfung und Prüfung des Zugriffs einrichten. Beispielsweise können sie bestehende Verfahren zur Zugriffsprüfung nicht für Unternehmensidentitäten verwenden, da der Benutzerdatensatz unabhängig von anderen Identitätsmanagementsystemen ist.

## Voraussetzungen

- Administratorberechtigungen QuickSight oder Berechtigungen zum Erstellen von QuickSight Benutzern (siehe identitätsbasierte IAM-Richtlinien für Amazon QuickSight: Benutzer erstellen)
- E-Mail-Adresse des Benutzers

## Konfiguration des Zugriffs für einen lokalen Benutzer QuickSight

Anweisungen zur Konfiguration eines lokalen Benutzers finden Sie unter Benutzer zum Zugriff auf Amazon einladen QuickSight. Beachten Sie bei der Konfiguration dieser Art von Benutzerzugriff Folgendes:

- Sie können zwar jeden beliebigen Benutzernamen und jede E-Mail-Adresse definieren, wir empfehlen jedoch, Werte zu verwenden, die mit dem Mitarbeiterverzeichnis Ihrer Organisation übereinstimmen. Dies verbessert die Rechenschaftspflicht und Konsistenz.
- Wählen Sie für IAM-Benutzer Nein aus.
- Der Benutzer hat sieben Tage Zeit, um die Einladung anzunehmen. Wenn sie innerhalb dieses Zeitraums nicht annehmen, können Sie die Einladungs-E-Mail erneut senden.
- Wenn der Benutzer die Einladung annimmt, wird er aufgefordert, sein Passwort festzulegen und zu bestätigen.

# Konfiguration von IAM-Richtlinien für den Zugriff QuickSight

Weitere Informationen zur Funktionsweise von AWS Identity and Access Management (IAM-) Richtlinien finden Sie in der Dokumentation unter QuickSight Amazon-Richtlinien (identitätsbasiert) und in der QuickSight IAM-Dokumentation unter Richtlinien und Berechtigungen. Beispielrichtlinien für finden Sie QuickSight unter Beispiele für IAM-Richtlinien für Amazon QuickSight.

Beachten Sie bei der Konfiguration von Richtlinien, die es Benutzern ermöglichen, den Zugriff selbst bereitzustellen, die folgenden Aktionen:

- `quicksight:CreateReader`ermöglicht einem Benutzer die Selbstbereitstellung von schreibgeschütztem Zugriff in. QuickSight Weitere Informationen finden Sie unter Self-Provisioning an Amazon QuickSight Read-Only User.
- `quicksight:CreateUser`ermöglicht es einem Benutzer, den Autorenzugriff in selbst bereitzustellen. QuickSight Weitere Informationen finden Sie unter Self-Provisioning an QuickSight Amazon-Autoren.
- `quicksight:CreateAdmin`ermöglicht es einem Benutzer, Administratorzugriff in selbst bereitzustellen. QuickSight Weitere Informationen finden Sie unter Self-Provisioning an Amazon QuickSight Administrator.

# Schlussfolgerung

In diesem Leitfaden werden verschiedene Ansätze beschrieben, mit denen Sie Benutzerzugriff auf Amazon gewähren können QuickSight. In einigen Fällen können Sie sogar mehrere Ansätze kombinieren, um unterschiedliche Anwendungsfälle zu unterstützen. Jeder zusätzliche Ansatz erhöht jedoch die Komplexität.

Wenn alle Optionen für Ihre Bereitstellung möglich sind, empfiehlt es sich, die AWS IAM Identity Center integrierte Integration mit zu verwenden QuickSight. Um diesen Ansatz genauer zu überprüfen und festzustellen, ob eine der aktuellen Funktionseinschränkungen auf Ihre Situation zutrifft, finden Sie in der QuickSight Dokumentation unter Konfiguration Ihres QuickSight Amazon-Kontos mit IAM Identity Center.

Wenn Sie sich für einen Ansatz entscheiden, sollten Sie berücksichtigen, wie er sich auf die Benutzeranmeldung und die Sicherheit auswirkt und wie Sie ihn bei der Zugriffsverwaltung und den Prozessen in Ihrem Unternehmen unterstützen können. In future zu einem anderen Ansatz zu wechseln, könnte kostspielig oder gar nicht möglich sein. Nehmen Sie sich vor der Einrichtung die nötige Zeit QuickSight, um zu beurteilen, was für Ihr Unternehmen am besten ist.

# Ressourcen

## AWS-Service Dokumentation

- AWS IAM Identity Center Dokumentation
  - Erste Schritte
  - Erstellen Sie einen Berechtigungssatz
- QuickSightAmazon-Dokumentation
  - Konfigurieren Sie Ihr QuickSight Amazon-Konto mit IAM Identity Center
  - Amazon QuickSight mit IAM verwenden
  - Beispiele für IAM-Richtlinien für Amazon QuickSight
  - Self-Provisioning von Benutzern für Amazon QuickSight
  - Verwenden von Identity Federation und Single Sign-On mit Amazon QuickSight
  - Verwenden von Active Directory mit Amazon QuickSight Enterprise Edition
  - Konfiguration der E-Mail-Synchronisierung für Verbundbenutzer in Amazon QuickSight
  - Tutorial: Zugriff auf Amazon QuickSight mit Okta
- AWS Identity and Access Management (IAM) -Dokumentation
  - Überblick über das AWS Identitätsmanagement
  - Identitätsanbieter und Föderation
  - IAM-Identitätsanbieter erstellen
  - Eine Rolle für einen externen Identitätsanbieter (Verband) erstellen

## Andere AWS Ressourcen

- Identitätsverbund in AWS
- Vereinfachen Sie das Business Intelligence-Identitätsmanagement mit Amazon QuickSight und AWS IAM Identity Center (AWS Blogbeitrag)

# 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 |
| --- | --- | --- |
| AWS IAM Identity Center Integration | Wir haben den Abschnitt QuickSight Zugriff über die IAM Identity Center-Integration gewähren hinzugefügt. | 14. Mai 2024 |
| Erste Veröffentlichung | — | 18. Mai 2023 |

# AWS Glossar zu präskriptiven Leitlinien

Die folgenden Begriffe werden häufig in Strategien, Leitfäden und Mustern von AWS Prescriptive Guidance verwendet. 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 im Bereich künstliche 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 in der AWS Migrationsstrategie finden Sie im Operations Integration Guide. AIOps

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 die erfolgreiche Umstellung 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, sogenannte bösartige Bots, 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 in der Regel 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-Exzellenzzentrum (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 — Tätigen Sie grundlegende Investitionen, um Ihre Cloud-Einführung zu skalieren (z. B. Einrichtung einer landing zone, Definition eines CCo E, 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 oderBitbucket Cloud. 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. Amazon SageMaker AI bietet beispielsweise Bildverarbeitungsalgorithmen für CV.

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 is commonly described as a pipeline. CI/CDkann 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 Variation 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 historischer 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, wie z. B. unbeabsichtigte Fehlkonfigurationen oder ein Malware-Angriff.

Disaster Recovery (DR)

Die Strategie und der Prozess, die Sie verwenden, um Ausfallzeiten und Datenverluste aufgrund einer Katastrophe zu minimieren. 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.

EDI

Siehe elektronischer Datenaustausch.

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.

elektronischer Datenaustausch (EDI)

Der automatisierte Austausch von Geschäftsdokumenten zwischen Organisationen. Weitere Informationen finden Sie unter Was ist elektronischer Datenaustausch.

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.

Eingabeaufforderung mit wenigen Klicks

Bereitstellung einer kleinen Anzahl von Beispielen, die die Aufgabe und das gewünschte Ergebnis veranschaulichen, bevor das LLM aufgefordert wird, eine ähnliche Aufgabe auszuführen. Bei dieser Technik handelt es sich um eine Anwendung des kontextbezogenen Lernens, bei der Modelle anhand von Beispielen (Aufnahmen) lernen, die in Eingabeaufforderungen eingebettet sind. Bei Aufgaben, die spezifische Formatierungs-, Argumentations- oder Fachkenntnisse erfordern, kann die Eingabeaufforderung mit wenigen Handgriffen effektiv sein. Siehe auch Zero-Shot Prompting.

FGAC

Siehe detaillierte 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.

FM

Siehe Fundamentmodell.

Fundamentmodell (FM)

Ein großes neuronales Deep-Learning-Netzwerk, das mit riesigen Datensätzen generalisierter und unbeschrifteter Daten trainiert wurde. FMs sind in der Lage, eine Vielzahl allgemeiner Aufgaben zu erfüllen, z. B. Sprache zu verstehen, Text und Bilder zu generieren und Konversationen in natürlicher Sprache zu führen. Weitere Informationen finden Sie unter Was sind Foundation-Modelle.

# G

generative KI

Eine Untergruppe von KI-Modellen, die mit großen Datenmengen trainiert wurden und mit einer einfachen Textaufforderung neue Inhalte und Artefakte wie Bilder, Videos, Text und Audio erstellen können. Weitere Informationen finden Sie unter Was ist Generative KI.

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.

goldenes Bild

Ein Snapshot eines Systems oder einer Software, der als Vorlage für die Bereitstellung neuer Instanzen dieses Systems oder dieser Software verwendet wird. In der Fertigung kann ein Golden Image beispielsweise zur Bereitstellung von Software auf mehreren Geräten verwendet werden und trägt zur Verbesserung der Geschwindigkeit, Skalierbarkeit und Produktivität bei der Geräteherstellung bei.

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 dazu beiträgt, Ressourcen, Richtlinien und die Einhaltung von Vorschriften in allen Unternehmenseinheiten zu regeln (OUs). 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.

Holdout-Daten

Ein Teil historischer, beschrifteter Daten, der aus einem Datensatz zurückgehalten wird, der zum Trainieren eines Modells für maschinelles Lernen verwendet wird. Sie können Holdout-Daten verwenden, um die Modellleistung zu bewerten, indem Sie die Modellvorhersagen mit den Holdout-Daten vergleichen.

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 Security Reference Architecture empfiehlt, Ihr Netzwerkkonto mit eingehendem und ausgehendem Datenverkehr und Inspektion einzurichten, VPCs um die bidirektionale Schnittstelle zwischen Ihrer Anwendung und dem Internet im weiteren Sinne 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 (T) IIo

Einsatz von mit dem Internet verbundenen Sensoren und Geräten in Industriesektoren wie Fertigung, Energie, Automobilindustrie, Gesundheitswesen, Biowissenschaften und Landwirtschaft. Weitere 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 demselben oder unterschiedlichen AWS-Regionen), dem Internet und lokalen Netzwerken verwaltet. In der AWS Security Reference Architecture wird empfohlen, Ihr Netzwerkkonto mit eingehendem und ausgehendem Datenverkehr sowie Inspektionen einzurichten, VPCs um die bidirektionale Schnittstelle zwischen Ihrer Anwendung und dem Internet im weiteren Sinne 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 des Modells für maschinelles Lernen 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..

großes Sprachmodell (LLM)

Ein Deep-Learning-KI-Modell, das anhand einer riesigen Datenmenge vorab trainiert wurde. Ein LLM kann mehrere Aufgaben ausführen, z. B. Fragen beantworten, Dokumente zusammenfassen, Text in andere Sprachen übersetzen und Sätze vervollständigen. Weitere Informationen finden Sie unter Was sind. LLMs

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.

LLM

Siehe großes Sprachmodell.

Niedrigere Umgebungen

Siehe Umgebung.

# 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 Dienst, der über genau definierte Kanäle kommuniziert APIs 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 mithilfe von Lightweight über eine klar definierte Schnittstelle. 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

Siehe 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 Einen Trail für eine Organisation erstellen.

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.

ORR

Weitere Informationen finden Sie unter 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 Security Reference Architecture empfiehlt die Einrichtung Ihres Netzwerkkontos mit eingehendem und ausgehendem Datenverkehr sowie Inspektion, VPCs um die bidirektionale Schnittstelle zwischen Ihrer Anwendung und dem Internet im weiteren Sinne 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 von Natur aus

Ein systemtechnischer Ansatz, der den Datenschutz während des gesamten Entwicklungsprozesses berücksichtigt.

Privat gehostete Zonen

Ein Container, der Informationen darüber enthält, wie Amazon Route 53 auf DNS-Abfragen für eine Domain und deren Subdomains innerhalb einer oder mehrerer VPCs Domains antworten

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. Diese Steuerelemente scannen Ressourcen, 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.

schnelle Verkettung

Verwendung der Ausgabe einer LLM-Eingabeaufforderung als Eingabe für die nächste Aufforderung, um bessere Antworten zu generieren. Diese Technik wird verwendet, um eine komplexe Aufgabe in Unteraufgaben zu unterteilen oder um eine vorläufige Antwort iterativ zu verfeinern oder zu erweitern. Sie trägt dazu bei, die Genauigkeit und Relevanz der Antworten eines Modells zu verbessern und ermöglicht detailliertere, personalisierte Ergebnisse.

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.

publish/subscribe (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).

LAPPEN

Siehe Erweiterte Generierung beim Abrufen.

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. Damit wird festgelegt, was als akzeptabler Datenverlust zwischen dem letzten Wiederherstellungspunkt und der Serviceunterbrechung gilt.

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.

Retrieval Augmented Generation (RAG)

Eine generative KI-Technologie, bei der ein LLM auf eine maßgebliche Datenquelle verweist, die sich außerhalb seiner Trainingsdatenquellen befindet, bevor eine Antwort generiert wird. Ein RAG-Modell könnte beispielsweise eine semantische Suche in der Wissensdatenbank oder in benutzerdefinierten Daten einer Organisation durchführen. Weitere Informationen finden Sie unter Was ist RAG.

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 Benutzeranmeldedaten, 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.

Sicherheit durch Design

Ein systemtechnischer Ansatz, der die Sicherheit während des gesamten Entwicklungsprozesses berücksichtigt.

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 EC2 Amazon-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 Steuerung der Berechtigungen für alle Konten in einer Organisation in ermöglicht AWS Organizations. SCPs Definieren Sie Leitplanken oder legen Sie Grenzwerte für Aktionen fest, die ein Administrator an Benutzer oder Rollen delegieren kann. Sie können sie SCPs als Zulassungs- oder Ablehnungslisten verwenden, um festzulegen, welche Dienste 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, während 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.

Systemaufforderung

Eine Technik, mit der einem LLM Kontext, Anweisungen oder Richtlinien zur Verfügung gestellt werden, um sein Verhalten zu steuern. Systemaufforderungen helfen dabei, den Kontext festzulegen und Regeln für Interaktionen mit Benutzern festzulegen.

# 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 Netzwerk-Transit-Hub, über den Sie Ihre Netzwerke VPCs und Ihre lokalen Netzwerke miteinander verbinden können. Weitere Informationen finden Sie in der Dokumentation unter Was ist ein Transit-Gateway. AWS 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 , die es Ihnen ermöglicht, den Verkehr mithilfe privater IP-Adressen weiterzuleiten. Weitere Informationen finden Sie unter Was ist VPC-Peering? in der Amazon-VPC-Dokumentation.

Schwachstelle

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

# 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

Siehe AWS Workload-Qualifizierungsrahmen.

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.

Zero-Shot-Aufforderung

Bereitstellung von Anweisungen für die Ausführung einer Aufgabe an einen LLM, jedoch ohne Beispiele (Schnappschüsse), die ihm als Orientierungshilfe dienen könnten. Der LLM muss sein

vortrainiertes Wissen einsetzen, um die Aufgabe zu bewältigen. Die Effektivität von Zero-Shot Prompting hängt von der Komplexität der Aufgabe und der Qualität der Aufforderung ab. Siehe auch Few-Shot-Prompting.

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.