Umstellung auf mehrere AWS-Konten

AWS Präskriptive Leitlinien

AWS Präskriptive Leitlinien: Umstellung auf mehrere AWS-Konten

Table of Contents

Umstellung auf mehrere AWS-Konten

Amazon Web Services (Mitwirkende)

November 2024 (Verlauf der Dokumente)

Viele Unternehmen beginnen ihre Reise mit der Nutzung eines einzigen Amazon Web Services (AWS)-Kontos. Mehrere Rollen innerhalb eines Unternehmens verwenden dieses Konto, um das Geschäft zu betreiben. Ingenieure entwickeln Code, stellen ihn in Entwicklungs- und Testumgebungen bereit und fördern Änderungen in der Produktion. Produktmanager fragen Datenquellen ab, um Einblicke in die Unternehmensleistung zu gewinnen. Das Vertriebsteam führt Demos von der Produktionsumgebung durch, um neue Kunden zu gewinnen. Das Finanzteam überwacht die Cloud-Ausgaben von der AWS Billing Konsole aus.

Wenn all diese separaten Rollen eine einzige Rolle verwenden AWS-Konto, kann es schwierig werden, die bewährte Sicherheitsmethode durchzusetzen, d. h., dass Sie nur die für die Ausführung der Aufgabe erforderlichen Mindestberechtigungen gewähren. In einer bestimmten Phase der Entwicklung eines Startups wird jemand die Frage stellen Benötigen alle unsere Entwickler Zugang zur Produktion? Die Antwort lautet fast immer nein, aber viele Unternehmen tun sich schwer damit, ihre bestehende Einzelkontenumgebung in eine Umgebung mit mehreren Konten umzuwandeln, ohne dabei das Geschäft zu verlangsamen.

Dieser Leitfaden enthält bewährte Methoden, die Ihnen beim Übergang von einer Umgebung mit nur einem Konto zu einer Umgebung mit mehreren Konten helfen sollen. Es werden die Entscheidungen erörtert, die Sie in den Bereichen Kontomigration, Benutzerverwaltung, Netzwerke, Sicherheit und Architektur treffen müssen. Es wurde entwickelt, um Ihnen mit minimalen oder keinen Ausfallzeiten für Ihr Unternehmen und den täglichen Betrieb zum Erfolg zu verhelfen. Dieser Leitfaden konzentriert sich auf die folgenden Funktionen beim Übergang von einer Umgebung mit einem Konto AWS-Konto zu einer Umgebung mit mehreren Konten:

- Identitätsmanagement und Zugriffskontrolle
- Verwalten von Berechtigungen und Zugriff
- Netzwerkkonnektivität
- Reaktion auf Sicherheitsvorfälle
- Sicherungen
- Kontomigration

- Migration von Ressourcen
- Überlegungen zur Abrechnung

Weitere Informationen zu Funktionen finden Sie unter Cloud Foundation auf AWS.

Dieser Leitfaden orientiert sich an vorhandenen Ressourcen zu diesem Thema, darunter das Whitepaper Organizing Your AWS Environment Using Multiple Accounts, AWS Security Reference Architecture (AWS SRA) und das Whitepaper Establishing Your Cloud Foundation on. AWS Sie sollten diese Ressourcen weiterhin für spezifischere Anleitungen nutzen, die in diesem Leitfaden nicht behandelt werden.

Zielgruppe

Dieser Leitfaden eignet sich am besten für Unternehmen, die auf mehrere AWS-Konten umsteigen möchten oder müssen. Bei Startups entsteht dieser Bedarf in der Regel dann, wenn Sie ein Produkt für den Markt geeignet befunden haben, eine Finanzierungsrunde eingesammelt haben und beginnen, bestimmte technische Disziplinen einzustellen, wie Infrastruktur, Entwicklungsbetrieb (DevOps) oder Sicherheit.

Auch wenn Ihr Unternehmen für diesen Übergang noch nicht bereit ist, können Sie diesen Leitfaden verwenden, um zu verstehen, welche Entscheidungen während der Umstellung getroffen werden müssen, und mit den Vorbereitungen beginnen.

Ziele für den Übergang zu einer Multi-Account-Architektur

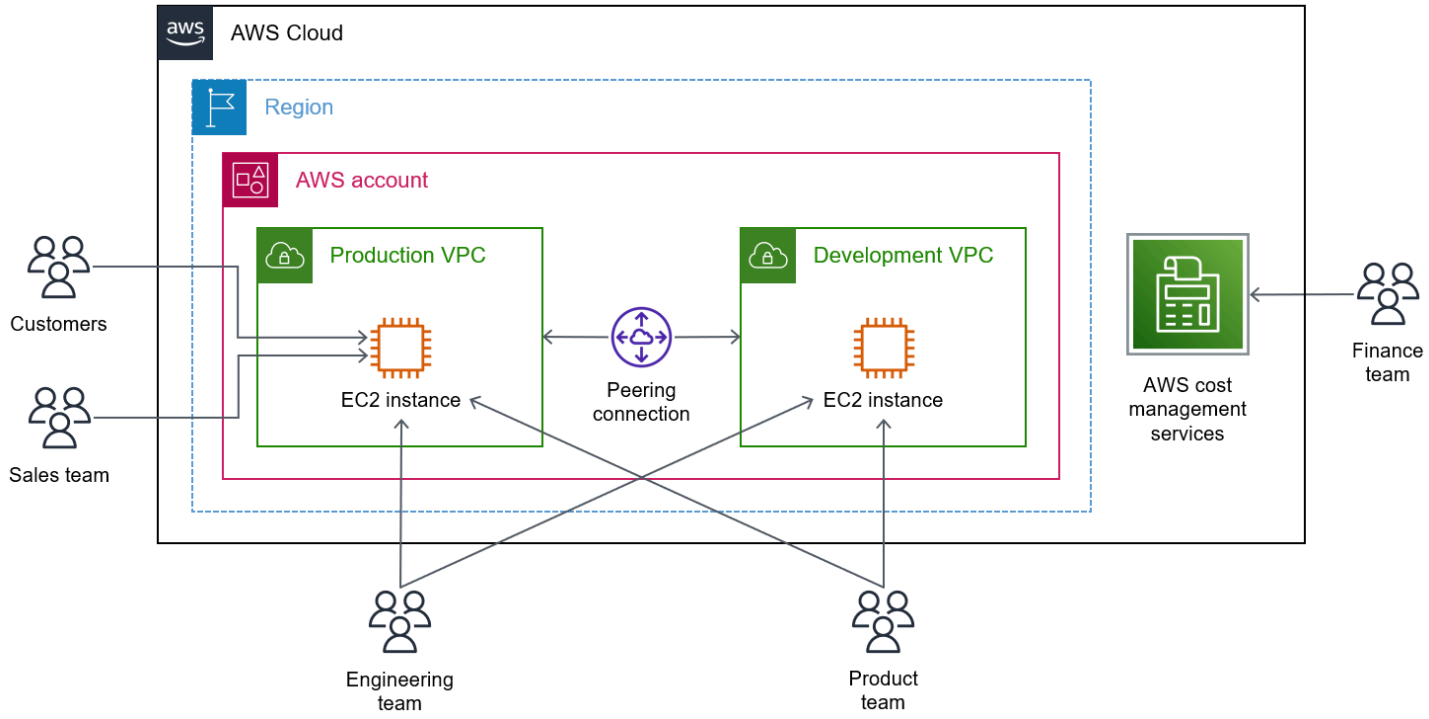
Der Übergang zu einer Architektur mit mehreren Konten ist in der Regel darauf zurückzuführen, dass ein Unternehmen einen oder mehrere der folgenden Vorteile benötigt:

- Gruppieren von Workloads nach Geschäftszweck oder Eigentümerschaft
- Anwenden unterschiedlicher Sicherheitskontrollen je nach Umgebung
- Beschränken des Zugriffs auf sensible Daten
- Fördern von Innovation und Agilität
- Begrenzen des Ausmaßes der Auswirkungen unerwünschter Ereignisse
- Unterstützen mehrerer IT-Betriebsmodelle
- Verwalten von Kosten
- Verteilung von AWS-Service Kontingenten und Beschränkungen der API-Anforderungsrate

Weitere Informationen zu den vielen Vorteilen einer Multi-Account-Architektur finden Sie unter Organizing Your AWS Environment Using Multi-Accounts (AWS Whitepaper) und Guidelines to Setup a well architecture environment (Dokumentation).AWS Control Tower

Beispiel für eine Einzel-Konto-Architektur

Als Ausgangspunkt ist es üblich, dass Startups oder kleine Unternehmen eine einzige verwenden AWS-Region und über zwei virtuelle private Clouds (VPCs) verfügen, die über VPC-Peering miteinander verbunden sind. Jede VPC enthält Rechenressourcen wie Amazon Elastic Compute Cloud (Amazon EC2)-Instances. Das Entwicklungteam entwickelt Code direkt in der VPC für die Entwicklung. Das Produktteam überprüft die Änderungen, und dann überträgt das Entwicklungsteam die Änderungen manuell auf die VPC für die Produktion. Das Finanzteam hat Zugriff auf die Konsole, AWS-Konto sodass es sie überprüfen kann. AWS Fakturierung und Kostenmanagement



Im Folgenden finden Sie einige Beispiele für Herausforderungen, denen ein Unternehmen in diesem Umfeld begegnen könnte:

- Ein Techniker hat versehentlich Produktionsdaten gelöscht, als er dachte, er würde auf eine Entwicklungsdatenbank zugreifen.
- Eine Verkaufsdemo wurde beeinträchtigt, als eine Produktionsbereitstellung länger als erwartet dauerte.
- Als der Entwicklungscode einem Belastungstest unterzogen wurde, wurde dieVPC für die Produktion langsam und generierte Fehlermeldungen über die Drosselung.
- Das Finanzteam kann die Kosten für Produktions- und Entwicklungsumgebungen nicht differenzieren.
- Der CEO ist besorgt darüber, dass einige neu eingestellte Fremdfirmen im Ausland über die VPC für die Produktion Zugang zu Kundendaten haben.
- Das Finanzteam darf den Zugriff auf bestimmte Daten, die hohe Kosten verursachen könnten AWS-Services , nicht verweigern.

Durch die Einführung einer Strategie für mehrere Konten werden all diese Herausforderungen bewältigt, indem Workloads und Zugriffe voneinander getrennt werden. AWS-Konten

Grundlegendes Framework und Sicherheitsverantwortlichkeiten für den Übergang zu einer Multi-Konto-Architektur

Die Informationen und bewährten Methoden in diesem Leitfaden sollen bestehende AWS -Empfehlungen für Infrastruktur und Sicherheit ergänzen. Bei der Umstellung von einem AWS-Konto auf mehrere Konten ist es wichtig AWS-Konten, sicherzustellen, dass Ihre neue Architektur mit mehreren Konten den Prinzipien des AWS Well-Architected Framework und der Cloud Foundation entspricht. Auf diese Weise können Sie eine Umgebung aufbauen und betreiben, die auf Sicherheit, Leistung und Stabilität ausgelegt ist und gleichzeitig die Governance-Anforderungen und Best Practices einhält. AWS

AWS Well-Architected Framework

AWS Well-Architected Framework hilft Ihnen beim Aufbau einer sicheren, leistungsstarken, belastbaren und effizienten Infrastruktur für Anwendungen und Workloads. Dieser Leitfaden orientiert sich an den Säulen Operative Exzellenz, Sicherheit, und Zuverlässigkeit dieses Rahmens. Dies hilft Ihnen, Ihre geschäftlichen und behördlichen Anforderungen zu erfüllen, indem Sie die aktuellen Empfehlungen befolgen. AWS

Sie können überprüfen, ob Sie sich an gut konzipierte bewährte Methoden halten, indem Sie die AWS Well-Architected Tool in Ihrem AWS-Konto verwenden.

Cloud Foundation auf AWS

Establishing Your Cloud Foundation on AWS (AWS Whitepaper) bietet Anleitungen, mit denen Sie Ihre AWS Umgebung an die Anforderungen Ihres Unternehmens anpassen können. Mithilfe eines auf Fähigkeiten basierenden Ansatzes können Sie eine Umgebung für die Bereitstellung, den Betrieb und die Verwaltung Ihrer Workloads erstellen. Sie können auch die Fähigkeiten erweitern, um Ihre Umgebung zu erweitern, wenn sich Ihre Anforderungen weiterentwickeln und Sie zusätzliche Workloads in der Cloud bereitstellen. Weitere Informationen zu den 30 Funktionen, die von definiert sind AWS, finden Sie unter Funktionen. Dieser Leitfaden enthält bewährte Methoden für die Implementierung der ursprünglichen Fähigkeiten in der vorgesehenen Reihenfolge.

Sie können Fähigkeiten entsprechend Ihren Betriebs- und Governance-Anforderungen einführen und implementieren. Wenn sich Ihre Geschäftsanforderungen weiterentwickeln, kann der

fähigkeitenbasierte Ansatz als Mechanismus verwendet werden, um zu überprüfen, ob Ihre Cloud-Umgebung bereit ist, Ihre Workloads zu unterstützen und nach Bedarf zu skalieren. Dieser Ansatz ermöglicht es Ihnen, zuversichtlich Ihre Cloud-Umgebung für Ihre Entwickler und Ihr Unternehmen einzurichten.

Identitätsmanagement und Zugriffskontrolle für den Übergang zu einer Multi-Konto-Architektur

Dieser erste Schritt beim Übergang zu einer Architektur mit mehreren Konten besteht darin, Ihre neue Kontostruktur innerhalb einer Organisation einzurichten. Anschließend können Sie Benutzer hinzufügen und ihren Zugriff auf die Konten konfigurieren. In diesem Abschnitt werden Ansätze zur Verwaltung des Benutzerzugriffs auf mehrere AWS-Konten beschrieben.

Dieser Abschnitt umfasst die folgenden Aufgaben:

- Eine Organisation einrichten
- Erstellen Sie eine Landing Zone
- Organisationseinheiten hinzufügen
- Erste Benutzer hinzufügen
- Mitgliedskonten verwalten

Eine Organisation einrichten

Wenn Sie mehrere haben AWS-Konten, können Sie diese Konten logisch über eine Organisation in AWS Organizationsverwalten. Ein Konto in AWS Organizations ist ein Standard AWS-Konto , der Ihre AWS Ressourcen und die Identitäten enthält, die auf diese Ressourcen zugreifen können. Eine Organisation ist eine Einheit, die Ihre Daten konsolidiert, AWS-Konten sodass Sie sie als eine Einheit verwalten können.

Wenn Sie ein Konto verwenden, um eine Organisation zu erstellen, wird dieses Konto das Verwaltungskonto (auch bekannt als Konto des Zahlers oder Root-Konto) für die Organisation. Eine Organisation kann nur ein Verwaltungskonto haben. Wenn Sie der Organisation weitere AWS-Konten hinzufügen, werden diese zu Mitgliedskonten.

> **Note**
>
> Jedes hat AWS-Konto außerdem eine einzige Identität, die als Root-Benutzer bezeichnet wird. Sie können sich als Root-Benutzer mit der E-Mail-Adresse und dem Passwort anmelden, die Sie bei der Erstellung des Kontos verwendet haben. Wir empfehlen jedoch dringend, den Root-Benutzer nicht für alltägliche Aufgaben zu verwenden, auch nicht für administrative Aufgaben. Weitere Informationen finden Sie unter AWS-Konto -Root-Benutzer.

Wir empfehlen außerdem, den Root-Zugriff für Mitgliedskonten zu zentralisieren und die Root-Benutzeranmeldeinformationen aus den Mitgliedskonten in Ihrer Organisation zu entfernen.

Sie organisieren Konten in einer hierarchischen, baumähnlichen Struktur, die aus dem Organisationsstamm, den Organisationseinheiten (OUs) und den Mitgliedskonten besteht. Root ist der übergeordnete Container für alle Konten in Ihrer Organisation. Eine organisatorische Einheit (OU) ist ein Container für Konten innerhalb des Roots. Eine Organisationseinheit kann andere Konten OUs oder Mitgliedskonten enthalten. Eine Organisationseinheit kann nur ein übergeordnetes Element haben und jedes Konto kann nur einer Organisationseinheit angehören. Weitere Informationen finden Sie unter Terminologie und Konzepte (AWS Organizations Dokumentation).

Eine Service Control Policy (SCP) spezifiziert die Dienste und Aktionen, die Benutzer und Rollen verwenden können. SCPs ähneln AWS Identity and Access Management (IAM-) Berechtigungsrichtlinien, mit dem Unterschied, dass sie keine Berechtigungen gewähren. SCPs Definieren Sie stattdessen die maximalen Berechtigungen. Wenn Sie eine Richtlinie an einen der Knoten in der Hierarchie anhängen, gilt sie für alle Konten OUs und innerhalb dieses Knotens. Wenn Sie beispielsweise eine Richtlinie auf das Stammverzeichnis anwenden, gilt sie für alle OUsKonten in der Organisation, und wenn Sie eine Richtlinie auf eine Organisationseinheit anwenden, gilt sie nur für die Konten OUs und in der Ziel-OU.

Eine Resource Control Policy (RCP) bietet eine zentrale Kontrolle über die maximal verfügbaren Berechtigungen für Ressourcen in Ihrer Organisation. RCPs hilft Ihnen dabei, sicherzustellen, dass die Ressourcen in Ihrem Konto den Richtlinien für die Zugriffskontrolle Ihrer Organisation entsprechen.

Sie können die AWS Organizations Konsole verwenden, um alle Ihre Konten innerhalb einer Organisation zentral einzusehen und zu verwalten. Einer der Vorteile einer Organisation besteht darin, dass Sie eine konsolidierte Rechnung erhalten können, in der alle mit den Verwaltungs- und Mitgliedskonten verbundenen Gebühren aufgeführt sind. Weitere Informationen finden Sie unter Konsolidierte Fakturierung (AWS Organizations Dokumentation).

Best Practices

- Verwenden Sie kein vorhandenes AWS-Konto , um eine Organisation zu erstellen. Beginnen Sie mit einem neuen Konto, das zu Ihrem Verwaltungskonto für die Organisation wird. Privilegierte Operationen können innerhalb des Verwaltungskontos einer Organisation ausgeführt werden SCPs

und gelten RCPs nicht für das Verwaltungskonto. Daher sollten Sie nur Cloud-Ressourcen und -Daten in das Verwaltungskonto aufnehmen, die dort verwaltet werden müssen.

- Beschränken Sie den Zugriff auf das Verwaltungskonto auf Personen, die neue Konten einrichten AWS-Konten und die Organisation verwalten müssen.
- Wird verwendet SCPs , um die maximalen Berechtigungen für das Stammkonto, die Organisationseinheiten und die Mitgliedskonten zu definieren. SCPs kann nicht direkt auf das Verwaltungskonto angewendet werden.
- Wird verwendet RCPs , um die maximalen Berechtigungen für Ressourcen in Mitgliedskonten zu definieren. RCPskann nicht direkt auf das Verwaltungskonto angewendet werden.
- Halten Sie sich an die Best Practices für AWS Organizations (AWS Organizations Dokumentation).

Erstellen Sie eine Landing Zone

Eine landing zone ist eine gut strukturierte AWS Umgebung mit mehreren Konten, von der aus Sie Workloads und Anwendungen bereitstellen können. Sie bietet eine Grundlage für den Einstieg in die Architektur mehrerer Konten, Identitäts- und Zugriffsmanagement, Governance, Datensicherheit, Netzwerkdesign und Protokollierung. AWS Control Tower ist ein Service, der die Wartung und Verwaltung einer Umgebung mit mehreren Konten vereinfacht, indem er automatisierten Integritätsschutz bereitstellt. In der Regel stellen Sie eine einzige AWS Control Tower landing zone bereit, die Ihre gesamte Umgebung verwaltet AWS-Regionen. AWS Control Tower funktioniert, indem es andere AWS-Services innerhalb Ihres Kontos orchestriert. Weitere Informationen finden Sie unter Was passiert, wenn Sie eine landing zone einrichten (AWS Control Tower Dokumentation).

Wenn Sie eine landing zone mit einrichten AWS Control Tower, identifizieren Sie drei gemeinsame Konten: das Verwaltungskonto, das Protokollarchivkonto und das Auditkonto. Weitere Informationen finden Sie unter Was sind gemeinsame Konten (AWS Control Tower Dokumentation). Für das Verwaltungskonto müssen Sie ein vorhandenes Konto verwenden, das keine Workloads hostet, um die Landing Zone einzurichten. Für das Protokollarchiv und die Auditkonten können Sie wählen, ob Sie vorhandene AWS-Konten Konten wiederverwenden oder sie für AWS Control Tower sich selbst erstellen möchten.

Anweisungen zur Einrichtung Ihrer AWS Control Tower landing zone finden Sie unter Erste Schritte (AWS Control Tower Dokumentation).

Best Practices

- Halten Sie sich an die Best Practices im Abschnitt Entwurfsprinzipien für Ihre Multi-Account-Strategie (AWS Whitepaper).
- Halten Sie sich an die Best Practices für AWS Control Tower Administratoren (AWS Control Tower Dokumentation).
- Erstellen Sie Ihre landing zone in der AWS-Region , in der die meisten Ihrer Workloads gehostet werden.

> **Important**
>
> Wenn du dich entscheidest, diese Region zu ändern, nachdem du deine landing zone eingerichtet hast, benötigst du die Unterstützung von AWS Support und du musst die landing zone außer Betrieb nehmen. Diese Vorgehensweise wird nicht empfohlen.

- Wählen Sie bei der Entscheidung, welche Regionen gelten AWS Control Tower sollen, nur die Regionen aus, in denen Sie davon ausgehen, dass Workloads sofort bereitgestellt werden. Sie können diese Regionen ändern oder später weitere hinzufügen. Wenn eine Region AWS Control Tower regiert, wird sie ihre detektivischen Leitplanken in dieser Region als einsetzen. AWS-Config-Regeln
- Nachdem festgelegt wurde, welche Regionen regieren AWS Control Tower sollen, wird allen Regionen, die keine Regierung besitzen, der Zugang verweigert. Auf diese Weise können Sie sicherstellen, dass Ihre Workloads und Entwickler nur zugelassene AWS-Regionen verwenden können. Dies wird in der Organisation als Service-Kontrollrichtlinie (SCP) implementiert. Weitere Informationen finden Sie unter Konfiguration der AWS-Region Verweigerungssteuerung (AWS Control Tower Dokumentation).
- Wenn du deine landing zone in AWS Control Tower einrichtest, empfehlen wir dir, die folgenden OUs Konten umzubenennen:
  - Wir empfehlen, die Sicherheit-OU zu Security_Prod umzubenennen, um zu signalisieren, dass diese Organisationseinheit für sicherheitsrelevante AWS-Konten in der Produktion verwendet wird.
  - Wir empfehlen Ihnen, die Erstellung einer zusätzlichen Organisationseinheit AWS Control Tower zuzulassen und diese dann von Sandbox in Workloads umzubenennen. Im nächsten Abschnitt erstellen Sie OUs innerhalb der Workloads OU weitere, mit denen Sie Ihre organisieren. AWS-Konten

  - Es wird empfohlen, die zentrale Protokollierung AWS-Konto von Log Archive in umzubenennen. log-archive-prod
  - Wir empfehlen, das Auditkonto von Audit in umzubenennen security-tooling-prod.
- Um Betrug zu verhindern, AWS ist es erforderlich, dass sie zuvor genutzt AWS-Konten wurden, bevor sie einer AWS Control Tower landing zone hinzugefügt werden können. Wenn Sie eine neue AWS-Konto ohne Nutzungshistorie verwenden, können Sie in dem neuen Konto eine Amazon Elastic Compute Cloud (Amazon EC2) -Instance starten, die nicht im AWS kostenlosen Kontingent enthalten ist. Lassen Sie die Instance einige Minuten laufen und beenden Sie sie dann.

Organisationseinheiten hinzufügen

Die Einrichtung der richtigen Organisationsstruktur ist entscheidend für die Einrichtung einer Umgebung mit mehreren Konten. Da Sie Richtlinien zur Servicesteuerung (SCPs) verwenden, um die maximalen Berechtigungen für eine Organisationseinheit und die darin enthaltenen Konten zu definieren, muss Ihre Organisationsstruktur aus Sicht der Verwaltung, der Berechtigungen und der Finanzberichterstattung logisch sein. Weitere Informationen zur Struktur einer Organisation, einschließlich der Organisationseinheiten (OUs), finden Sie unter Terminologie und Konzepte (AWS Organizations Dokumentation).

In diesem Abschnitt passen Sie die landing zone an, indem Sie verschachtelte Umgebungen erstellen, mit OUs denen Sie Ihre Umgebungen segmentieren und strukturieren können, z. B. Produktions- und Nichtproduktionsumgebungen. Diese empfohlenen bewährten Methoden dienen dazu, Ihre Landing Zone so zu segmentieren, dass produktive und nicht produktive Ressourcen getrennt werden und die Infrastruktur von den Workloads getrennt wird.

Weitere Informationen zur Erstellung OUs finden Sie unter Organisationseinheiten verwalten (AWS Organizations Dokumentation).

Best Practices

- Erstellen Sie in der Workloads-Organisationseinheit, in der Sie sie erstellt habenErstellen Sie eine Landing Zone, die folgenden OUs verschachtelten Elemente:
  - Prod – Verwenden Sie diese Organisationseinheit für AWS-Konten , die Produktionsdaten, einschließlich Kundendaten, speichern und darauf zugreifen.
  - NonProd— Verwenden Sie diese Organisationseinheit für den Speicher von Daten AWS-Konten , die nicht zur Produktion gehören, z. B. für Entwicklungs-, Staging- oder Testumgebungen

Erstellen Sie unter dem Organisationsroot eine Infrastruktur_Prod-DU. Verwenden Sie diese Organisationseinheit, um ein zentrales Netzwerkkonto zu hosten.

Erste Benutzer hinzufügen

Es gibt zwei Möglichkeiten, Menschen Zugang zu AWS-Konten zu gewähren:

- IAM-Identitäten, wie z. B. Benutzer, Gruppen und Rollen
- Identitätsverbund, z. B. durch AWS IAM Identity Center

In kleineren Unternehmen und Einzel-Konto-Umgebungen ist es üblich, dass Administratoren einen IAM-Benutzer erstellen, wenn eine neue Person dem Unternehmen beitritt. Der Zugriffsschlüssel und die geheimen Schlüsselanmeldeinformationen, die einem IAM-Benutzer zugeordnet sind, sind bekannt als langfristige Anmeldeinformationen weil sie nicht ablaufen. Dies ist jedoch keine empfohlene bewährte Sicherheitsmethode, denn wenn ein Angreifer diese Anmeldeinformationen kompromittiert hätte, müssten Sie neue Anmeldeinformationen für den Benutzer generieren. Ein anderer Ansatz für den Zugriff AWS-Konten sind IAM-Rollen. Sie können auch AWS -Security-Token-Service (AWS STS) verwenden, um vorübergehend kurzfristige Anmeldeinformationen anzufordern, die nach einer konfigurierbaren Zeit ablaufen.

Sie können den Zugriff von Personen auf Sie AWS-Konten über IAM Identity Center verwalten. Sie können individuelle Benutzerkonten für jeden Ihrer Mitarbeiter oder Auftragnehmer erstellen, sie können ihre eigenen Passwörter und Multi-Faktor-Authentifizierung (MFA)-Lösungen verwalten und Sie können sie gruppieren, um den Zugriff zu verwalten. Bei der Konfiguration von MFA können Sie Softwaretoken wie Authentifikatoranwendungen oder Hardwaretokens wie YubiKey Geräte verwenden.

IAM Identity Center unterstützt auch den Verbund mit externen Identitätsanbietern (IdPs) wie Okta und Ping Identity. JumpCloud Weitere Informationen finden Sie unter Unterstützte Identitätsanbieter (Dokumentation zu IAM Identity Center). Durch die Verbindung mit einem externen IdP können Sie die Benutzerauthentifizierung anwendungsübergreifend verwalten und dann IAM Identity Center verwenden, um den Zugriff auf bestimmte Anwendungen zu autorisieren. AWS-Konten

Best Practices

- Halten Sie sich an Bewährte Methoden für die Sicherheit (IAM-Dokumentation) für die Konfiguration des Benutzerzugriffs.

- Verwalten Sie den Kontozugriff nach Gruppen anstatt nach einzelnen Benutzern. Erstellen Sie in IAM Identity Center neue Gruppen, welche jede Ihrer Geschäftsfunktionen repräsentieren. Sie könnten beispielsweise Gruppen für Technik, Finanzen, Vertrieb und Produktmanagement erstellen.
- Oft werden Gruppen definiert, indem diejenigen getrennt werden, die Zugriff auf alle AWS-Konten benötigen (oft nur Lesezugriff) und diejenigen, die Zugriff auf ein einzelnes AWS-Konto benötigen. Wir empfehlen Ihnen, die folgende Benennungskonvention für Gruppen zu verwenden, damit Sie die mit der Gruppe verknüpften Rechte AWS-Konto und Berechtigungen leicht identifizieren können.

  `<prefix>-<account name>-<permission set>`
- Zum Beispiel für die Gruppe `AWS-A-dev-nonprod-DeveloperAccess`, ist `AWS-A` ein Präfix, das den Zugriff auf ein einzelnes Konto anzeigt, `dev-nonprod` ist der Name des Kontos und `DeveloperAccess` ist der dieser Gruppe zugewiesene Berechtigungssatz. Für die Gruppe `AWS-O-BillingAccess` indiziert der `AWS-O`-Präfix den Zugriff auf die gesamte Organisation, und `BillingAccess` gibt den Berechtigungssatz für die Gruppe an. In diesem Beispiel ist ein Kontoname nicht im Gruppennamen enthalten, da die Gruppe Zugriff auf die gesamte Organisation hat.
- Wenn Sie IAM Identity Center mit einem externen SAML-basierten IdP verwenden und MFA benötigen möchten, können Sie die Authentifizierungsmethode mithilfe der attributbasierten Zugriffskontrolle (ABAC) vom IdP an IAM Identity Center übergeben. Die Attribute werden über die SAML-Assertionen gesendet. Weitere Informationen finden Sie unter Attribute für die Zugriffskontrolle aktivieren und konfigurieren (Dokumentation von IAM Identity Center).

  Viele IdPs, wie Microsoft Azure Active Directory und Okta, können den Authentication Method Reference (`amr`) -Anspruch innerhalb einer SAML-Assertion verwenden, um den MFA-Status des Benutzers an IAM Identity Center weiterzuleiten. Der Anspruch, der zur Bestätigung des MFA-Status verwendet wird, und sein Format variieren je nach IdP. Weitere Informationen finden Sie in der Dokumentation zu Ihrem IdP.

  In IAM Identity Center können Sie dann Richtlinien für Berechtigungssätze erstellen, die festlegen, wer auf Ihre Ressourcen zugreifen kann. AWS Wenn Sie ABAC aktivieren und Attribute angeben, übergibt IAM Identity Center den Attributwert des authentifizierten Benutzers an IAM zur Verwendung bei der Richtlinienbewertung. Weitere Informationen finden Sie unter Erstellen Sie Berechtigungsrichtlinien für ABAC (Dokumentation von IAM Identity Center). Wie im folgenden Beispiel gezeigt, verwenden Sie die `aws:PrincipalTag`-Bedingungsschlüssel zum Erstellen einer Zugriffskontrollregel für MFA.

```
"Condition": {
  "StringLike": { "aws:PrincipalTag/amr": "mfa" }
}
```

Mitgliedskonten verwalten

In diesem Abschnitt laden Sie Ihr bereits bestehendes Konto in die Organisation ein und beginnen, neue Konten in Ihrer Organisation zu erstellen. Ein wichtiger Teil dieses Prozesses ist die Definition der Kriterien, anhand derer Sie bestimmen, ob Sie ein neues Konto einrichten müssen.

Dieser Abschnitt umfasst die folgenden Aufgaben:

- Einladen Ihres bereits bestehenden Kontos
- Passen Sie die VPC-Einstellungen an in AWS Control Tower
- Definieren Sie die Umfangskriterien

Einladen Ihres bereits bestehenden Kontos

Darin AWS Organizations können Sie das bereits bestehende Konto Ihres Unternehmens in Ihre neue Organisation einladen. Nur das Verwaltungskonto in der Organisation kann andere Konten zum Beitritt einladen. Wenn der Administrator des eingeladenen Kontos zustimmt, tritt das Konto umgehend der Organisation bei, und das Verwaltungskonto der Organisation wird für alle vom neuen Mitgliedskonto anfallenden Gebühren verantwortlich. Weitere Informationen finden Sie unter Einladen eines AWS-Konto , Ihrer Organisation beizutreten und Eine Einladung einer Organisation annehmen oder ablehnen (AWS Organizations -Dokumentation).

> **Note**
>
> Sie können ein Konto nur dann zum Beitritt zu einer Organisation einladen, wenn dieses Konto derzeit keiner anderen Organisation angehört. Wenn das Konto Mitglied einer bestehenden Organisation ist, müssen Sie es aus der Organisation entfernen. Wenn es sich bei dem Konto um das Verwaltungskonto für eine andere Organisation handelt, die fälschlicherweise erstellt wurde, müssen Sie die Organisation löschen.

> **Important**
>
> Wenn Sie Zugriff auf historische Kosten- oder Nutzungsinformationen aus Ihrem bestehenden Konto benötigen, können Sie diese Informationen in einen Amazon Simple Storage Service (Amazon S3) -Bucket exportieren. AWS Cost and Usage Report Tun Sie dies, bevor Sie die Einladung zum Beitritt der Organisation annehmen. Wenn ein Konto einer Organisation beitritt, verlieren Sie den Zugriff auf diese historischen Daten für das Konto. Weitere Informationen finden Sie unter Einen Amazon-S3-Bucket für Kosten- und Nutzungsberichte einrichten (AWS Cost and Usage Report -Dokumentation).

Best Practices

- Wir empfehlen Ihnen, Ihr bereits vorhandenes Konto, das wahrscheinlich Produktionsworkloads enthält, zur Workloads > Prod-Organisationseinheit hinzuzufügen, die Sie in Organisationseinheiten hinzufügen erstellt haben.
- Standardmäßig hat das Verwaltungskonto der Organisation keinen Administratorzugriff auf Mitgliedskonten, die zur Organisation eingeladen wurden. Wenn Sie möchten, dass das Verwaltungskonto die administrative Kontrolle hat, müssen Sie die OrganizationAccountAccessRoleIAM-Rolle im Mitgliedskonto erstellen und dem Verwaltungskonto die Erlaubnis erteilen, diese Rolle zu übernehmen. Weitere Informationen finden Sie unter Konto „ OrganizationAccountAccessRole In einem eingeladenen Mitglied“ erstellen (AWS Organizations Dokumentation).
- Lesen Sie für das bereits bestehende Konto, das Sie zu der Organisation eingeladen haben, die Informationen zu den Best Practices für Mitgliedskonten (AWS Organizations Dokumentation) und stellen Sie sicher, dass das Konto diesen Empfehlungen entspricht.

Passen Sie die VPC-Einstellungen an in AWS Control Tower

Wir empfehlen Ihnen, neue Produkte AWS-Konten über Account Factory in bereitzustellen AWS Control Tower. Wenn Sie Account Factory verwenden, können Sie die AWS Control Tower Integration mit Amazon nutzen EventBridge , um Ressourcen neu bereitzustellen, AWS-Konten sobald das Konto erstellt wurde.

Wenn Sie eine neue einrichten AWS-Konto, wird automatisch eine standardmäßige Virtual Private Cloud (VPC) bereitgestellt. Wenn Sie jedoch über Account Factory ein neues Konto einrichten, stellt AWS Control Tower automatisch eine zusätzliche VPC bereit. Weitere Informationen finden Sie unter

Überblick über AWS Control Tower und VPCs (AWS Control Tower Dokumentation). Das bedeutet, dass standardmäßig VPCs in jedem neuen Konto zwei Provisionen AWS Control Tower vorgesehen sind.

Es ist üblich, dass Unternehmen mehr Kontrolle über VPCs die Konten wünschen. Viele bevorzugen es, andere Dienste wie AWS CloudFormation Hashicorp Terraform oder Pulumi zu verwenden, um ihre einzurichten und zu verwalten. VPCs Sie sollten die Account-Factory-Einstellungen anpassen, um die Erstellung der zusätzlichen VPC zu verhindern, die von AWS Control Tower bereitgestellt werden. Anweisungen finden Sie unter Amazon VPC-Einstellungen konfigurieren (AWS Control Tower Dokumentation) und wenden Sie die folgenden Einstellungen an:

1. Deaktivieren Sie die Option Über das Internet zugängliches Subnetz.
2. Wählen Sie für Maximale Anzahl der öffentlichen Subnetze 0 aus.
3. Löschen Sie alle Regionen in Regionen für die Erstellung von VPC.
4. In Availability Zones wählen Sie 3.

Best Practices

- Löschen Sie die Standard-VPC, die automatisch in jedem neuen Konto bereitgestellt wird. Dadurch wird verhindert, dass Benutzer öffentliche EC2-Instances im Konto starten, ohne explizit eine dedizierte VPC zu erstellen. Weitere Informationen finden Sie unter Ihre Standardsubnetze und die Standard-VPC löschen (Dokumentation von Amazon Virtual Private Cloud). Sie können auch AWS Control Tower Account Factory für Terraform (AFT) konfigurieren, um die Standard-VPC in neu erstellten Konten automatisch zu löschen.
- Stellen Sie ein neues Objekt AWS-Konto namens dev-nonprod in der Organisationseinheit Workloads > bereit. NonProd Verwenden Sie dieses Konto für Ihre Entwicklungsumgebung. Anweisungen finden Sie unter Bereitstellen von Account Factory Factory-Konten mit AWS Service Catalog (AWS Control Tower Dokumentation).

Definieren Sie die Umfangskriterien

Sie müssen die Kriterien auswählen, anhand derer Ihr Unternehmen entscheidet, ob ein neues Konto bereitgestellt werden soll AWS-Konto. Sie können sich dafür entscheiden, Konten für jede Geschäftseinheit bereitzustellen, oder Sie entscheiden, Konten je nach Umgebung bereitzustellen, z. B. Produktion, Test oder Qualitätssicherung. Jedes Unternehmen hat seine eigenen Anforderungen

daran, wie groß oder klein es sein AWS-Konten sollte. Im Allgemeinen berücksichtigen Sie bei der Entscheidung über die Größe Ihrer Konten die folgenden drei Faktoren:

- Ausgleich von Servicekontingenten — Servicekontingenten sind die Höchstwerte für die Anzahl der Ressourcen, Aktionen und Elemente für die einzelnen Ressourcen, Aktionen und Elemente AWS-Service innerhalb eines AWS-Konto. Wenn sich viele Workloads dasselbe Konto teilen und ein Workload die meisten oder alle Servicekontingente beansprucht, kann sich dies negativ auf einen anderen Workload in demselben Konto auswirken. In diesem Fall müssen Sie diese Workloads möglicherweise auf verschiedene Konten aufteilen. Weitere Informationen finden Sie unter AWS-Service Quotas (Allgemeine AWS-Referenz).
- Kostenberichterstattung – Durch die Isolierung von Workloads auf separate Konten können Sie die Kosten in den Kosten- und Nutzungsberichten auf Kontoebene einsehen. Wenn Sie dasselbe Konto für verschiedene Workloads verwenden, können Sie Tags verwenden, um Ressourcen zu verwalten und zu identifizieren. Weitere Informationen zum Taggen finden Sie unter AWS Ressourcen taggen ()Allgemeine AWS-Referenz.
- Zugriffskontrolle – Wenn Workloads ein Konto gemeinsam nutzen, müssen Sie überlegen, wie Sie IAM-Richtlinien konfigurieren, um den Zugriff auf die Kontoressourcen zu beschränken, sodass Benutzer keinen Zugriff auf die Workloads haben, die sie nicht benötigen. Als Alternative können Sie mehrere Konten und Berechtigungssätze im IAM Identity Center verwenden, um den Zugriff auf einzelne Konten zu verwalten.

Best Practices

- Halten Sie sich an die Best Practices für die AWS Multi-Account-Strategie für Ihre AWS Control Tower landing zone (AWS Control Tower Dokumentation).
- Entwickeln Sie eine effektive Tagging-Strategie, die Ihnen bei der Identifizierung und Verwaltung von AWS -Ressourcen hilft. Mit Hilfe von Tags können Sie Ressourcen nach Zweck, Geschäftseinheit, Umgebung oder anderen Kriterien kategorisieren. Weitere Informationen finden Sie unter Bewährte Methoden für das Tagging (Allgemeine AWS-Referenz Dokumentation).
- Überlasten Sie ein Konto nicht mit zu vielen Workloads. Wenn der Workload den Servicekontingent überschreitet, kann dies zu Leistungsproblemen führen. Sie können die konkurrierenden Workloads in verschiedene aufteilen AWS-Konten oder eine Erhöhung der Servicequote beantragen. Weitere Informationen finden Sie unter Anfordern einer Erhöhung von Quotas (Dokumentation zu Service Quotas).

Verwaltung von Berechtigungen und Zugriff für eine Architektur mit mehreren Konten

In diesem Abschnitt werden folgende Themen beschrieben:

- Kulturtechnische Überlegungen
- Erstellen von Berechtigungssätzen
- Eine Berechtigungsgrenze erstellen
- Verwalten von Berechtigungen für Einzelpersonen

Kulturtechnische Überlegungen

Eine der Säulen des AWS Well-Architected Framework ist Operational Excellence. Teams müssen das Betriebsmodell und ihren Beitrag zum Erreichen Ihrer Geschäftsergebnisse verstehen. Teams können sich darauf konzentrieren, gemeinsame Ziele zu erreichen, wenn sie ihre Verantwortung verstehen, Verantwortung übernehmen und wissen, wie Entscheidungen getroffen werden.

Bei Unternehmen in der Anfangsphase, die sich schnell entwickeln, erfüllt jeder im Team mehrere Rollen. Es ist nicht ungewöhnlich, dass diese Benutzer sehr privilegierten Zugriff auf das gesamte AWS-Konto haben. Wenn Unternehmen wachsen, möchten sie oft dem Prinzip der geringsten Berechtigung folgen und nur Berechtigungen gewähren, die der Benutzer benötigt, um seine Arbeit zu erledigen. Um den Umfang einzuschränken, können Sie AWS Identity and Access Management Access Analyzer verwenden, um zu sehen, welche Berechtigungen ein Benutzer oder eine IAM-Rolle tatsächlich verwendet, sodass Sie alle überzähligen Berechtigungen entfernen können.

Es kann schwierig sein, zu entscheiden, wer in Ihrem Unternehmen über die Berechtigungen zum Erstellen von IAM-Rollen verfügt. Dies ist in der Regel ein Vektor für die Eskalation von Rechten. Bei der Eskalation von Rechten kann ein Benutzer seine eigenen Berechtigungen oder seinen eigenen Zugriffsumfang erweitern. Wenn ein Benutzer beispielsweise über eingeschränkte Berechtigungen verfügt, aber neue IAM-Rollen erstellen kann, kann er seine Berechtigungen erweitern, indem er eine neue IAM-Rolle erstellt und übernimmt, auf die die verwaltete Richtlinie `AdministratorAccess` angewendet wird.

Einige Unternehmen beschränken die Bereitstellung von IAM-Rollen auf ein zentralisiertes Team von vertrauenswürdigen Personen. Der Nachteil dieses Ansatzes ist, dass dieses Team schnell zu einem Engpass werden kann, da fast alle eine IAM-Rolle für den AWS-Services Betrieb benötigen.

Als Alternative können Sie Berechtigungsgrenzen verwenden, um den IAM-Zugriff nur an Benutzer zu delegieren, die Ihre Cloud-Infrastruktur entwickeln, testen, starten und verwalten. Beispiele für Richtlinien finden Sie unter Beispiel für Zugriffsgrenzen (). GitHub

Teams für den Entwicklungsbetrieb (DevOps), auch Plattformteams genannt, müssen häufig ein Gleichgewicht zwischen den Self-Service-Funktionen mehrerer interner Entwicklungsteams und der Betriebsstabilität von Anwendungen finden. Die Förderung einer Technikkultur, die Autonomie, Kompetenz und Zielstrebigkeit am Arbeitsplatz fördert, kann dazu beitragen, Teams zu motivieren. Ingenieure möchten ihre Arbeit selbstbestimmt erledigen, ohne sich darauf verlassen zu müssen, dass andere Dinge für sie erledigen. Wenn DevOps Teams Self-Service-Lösungen implementieren können, verringert sich dadurch auch die Zeit, in der andere auf sie angewiesen sind, um Aufgaben zu erledigen.

Erstellen von Berechtigungssätzen

Sie können AWS-Konto den Zugriff mithilfe von Berechtigungssätzen in AWS IAM Identity Center verwalten. Ein Berechtigungssatz ist eine Vorlage, mit der Sie eine oder mehrere IAM-Richtlinien für mehrere AWS-Konten bereitstellen können. Wenn Sie einen Berechtigungssatz einem AWS-Konto zuweisen, erstellt IAM Identity Center eine IAM-Rolle und fügt der Rolle die IAM-Richtlinien an. Weitere Informationen finden Sie unter Berechtigungsrichtlinien erstellen und verwalten (Dokumentation von IAM Identity Center).

AWS empfiehlt, Berechtigungssätze zu erstellen, die den verschiedenen Personas in Ihrem Unternehmen zugeordnet sind.

Beispielsweise könnten Sie die folgenden Berechtigungssätze erstellen:

- Fakturierungsberechtigungssatz
- Entwicklerberechtigungssatz
- Produktionsberechtigungssatz

Die folgenden Berechtigungssätze sind Auszüge aus einer Vorlage. AWS CloudFormation Sie sollten diesen Code als Ausgangspunkt verwenden und ihn an Ihr Unternehmen anpassen. Weitere Informationen zu CloudFormation Vorlagen finden Sie unter Grundlagen von Vorlagen lernen (CloudFormation Dokumentation).

Fakturierungsberechtigungssatz

Das Finanzteam verwendet BillingAccessPermissionSet, um sich das AWS Billing Konsolen-Dashboard und AWS Cost Explorer die einzelnen Konten anzusehen.

```
BillingAccessPermissionSet:
  Type: "AWS::SSO::PermissionSet"
  Properties:
    Description: Access to Billing and Cost Explorer
    InstanceArn: !Sub "arn:${AWS::Partition}:sso:::instance/ssoins-instanceId"
    ManagedPolicies:
      - !Sub "arn:${AWS::Partition}:iam::aws:policy/job-function/Billing"
    Name: BillingAccess
    SessionDuration: PT8H
    RelayStateType: https://console.aws.amazon.com/billing/home
```

Entwicklerberechtigungssatz

Das Entwicklungsteam verwendet, DeveloperAccessPermissionSetum auf Konten zuzugreifen, die nicht zur Produktion gehören.

```
DeveloperAccessPermissionSet:
  Type: "AWS::SSO::PermissionSet"
  Properties:
    Description: Access to provision resources through CloudFormation
    InlinePolicy: !Sub |-
      {
        "Version": "2012-10-17",
        "Statement": [
          {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:${AWS::Partition}:iam::*:role/CloudFormationRole",
            "Condition": {
              "StringEquals": {
                "aws:ResourceAccount": "${!aws:PrincipalAccount}",
                "iam:PassedToService": "cloudformation.${AWS::URLSuffix}"
              }
            }
          },
          {
            "Effect": "Allow",
```

```
            "Action": [
              "cloudformation:ContinueUpdateRollback",
              "cloudformation:CreateChangeSet",
              "cloudformation:CreateStack",
              "cloudformation:DeleteStack",
              "cloudformation:RollbackStack",
              "cloudformation:UpdateStack"
            ],
            "Resource": "arn:${AWS::Partition}:cloudformation:*:*:stack/app-*",
            "Condition": {
              "ArnLike": {
                "cloudformation:RoleArn": "arn:${AWS::Partition}:iam::${!
aws:PrincipalAccount}:role/CloudFormationRole"
              },
              "Null": {
                "cloudformation:ImportResourceTypes": true
              }
            }
          },
          {
            "Effect": "Allow",
            "Action": [
              "cloudformation:CancelUpdateStack",
              "cloudformation:DeleteChangeSet",
              "cloudformation:DetectStackDrift",
              "cloudformation:DetectStackResourceDrift",
              "cloudformation:ExecuteChangeSet",
              "cloudformation:TagResource",
              "cloudformation:UntagResource",
              "cloudformation:UpdateTerminationProtection"
            ],
            "Resource": "arn:${AWS::Partition}:cloudformation:*:*:stack/app-*"
          },
          {
           "Effect": "Allow",
            "Action": [
              "cloudformation:CreateUploadBucket",
              "cloudformation:ValidateTemplate",
              "cloudformation:EstimateTemplateCost"
            ],
            "Resource": "*"
          }
        ]
      }
```

```
    InstanceArn: !Sub "arn:${AWS::Partition}:sso:::instance/ssoins-instanceId"
    ManagedPolicies:
      - !Sub "arn:${AWS::Partition}:iam::aws:policy/AWSServiceCatalogEndUserFullAccess"
      - !Sub "arn:${AWS::Partition}:iam::aws:policy/AWSBillingReadOnlyAccess"
      - !Sub "arn:${AWS::Partition}:iam::aws:policy/AWSSupportAccess"
      - !Sub "arn:${AWS::Partition}:iam::aws:policy/ReadOnlyAccess"
    Name: DeveloperAccess
    SessionDuration: PT8H
```

Produktionsberechtigungssatz

Das Entwicklungsteam verwendet ProductionPermissionSet, um auf Produktionskonten zuzugreifen. Dieser Berechtigungssatz hat eingeschränkten Nur-Lesezugriff.

```
ProductionPermissionSet:
  Type: "AWS::SSO::PermissionSet"
  Properties:
    Description: Access to production accounts
    InlinePolicy: !Sub |-
      {
        "Version": "2012-10-17",
        "Statement": [
          {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:${AWS::Partition}:iam::*:role/CloudFormationRole",
            "Condition": {
              "StringEquals": {
                "aws:ResourceAccount": "${!aws:PrincipalAccount}",
                "iam:PassedToService": "cloudformation.${AWS::URLSuffix}"
              }
            }
          },
          {
            "Effect": "Allow",
            "Action": "cloudformation:ContinueUpdateRollback",
            "Resource": "arn:${AWS::Partition}:cloudformation:*:*:stack/app-*",
            "Condition": {
              "ArnLike": {
                "cloudformation:RoleArn": "arn:${AWS::Partition}:iam::${!
aws:PrincipalAccount}:role/CloudFormationRole"
              }
            }
```

```
          },
          {
            "Effect": "Allow",
            "Action": "cloudformation:CancelUpdateStack",
            "Resource": "arn:${AWS::Partition}:cloudformation:*:*:stack/app-*"
          }
        ]
      }
    InstanceArn: !Sub "arn:${AWS::Partition}:sso:::instance/ssoins-instanceId"
    ManagedPolicies:
      - !Sub "arn:${AWS::Partition}:iam::aws:policy/AWSBillingReadOnlyAccess"
      - !Sub "arn:${AWS::Partition}:iam::aws:policy/AWSSupportAccess"
      - !Sub "arn:${AWS::Partition}:iam::aws:policy/job-function/ViewOnlyAccess"
    Name: ProductionAccess
    SessionDuration: PT2H
```

Eine Berechtigungsgrenze erstellen

Nachdem Sie die Berechtigungssätze bereitgestellt haben, legen Sie eine Berechtigungsgrenze fest. Diese Berechtigungsgrenze ist ein Mechanismus, um den IAM-Zugriff nur an die Benutzer zu delegieren, die Ihre Cloud-Infrastruktur entwickeln, testen, einführen und verwalten. Diese Benutzer können nur die Aktionen ausführen, die gemäß der Richtlinie und der Berechtigungsgrenze zulässig sind.

Sie können die Berechtigungsgrenze in einer AWS CloudFormation Vorlage definieren und dann verwenden CloudFormation StackSets , um die Vorlage für mehrere Konten bereitzustellen. Auf diese Weise können Sie mit einem einzigen Vorgang standardisierte Richtlinien in Ihrer gesamten Organisation einrichten und beibehalten. Weitere Informationen und Anweisungen finden Sie unter Arbeiten mit AWS CloudFormation StackSets (CloudFormation Dokumentation).

Die folgende CloudFormation Vorlage stellt eine IAM-Rolle bereit und erstellt eine IAM-Richtlinie, die als Berechtigungsgrenze dient. Mithilfe eines Stack-Sets können Sie diese Vorlage für alle Mitgliedskonten in Ihrer Organisation bereitstellen.

```
CloudFormationRole:
  Type: "AWS::IAM::Role"
  Properties:
    AssumeRolePolicyDocument:
      Version: "2012-10-17"
      Statement:
        Effect: Allow
```

```
        Principal:
          Service: !Sub "cloudformation.${AWS::URLSuffix}"
        Action: "sts:AssumeRole"
        Condition:
          StringEquals:
            "aws:SourceAccount": !Ref "AWS::AccountId"
    Description: !Sub "DO NOT DELETE - Used by CloudFormation. Created by
 CloudFormation ${AWS::StackId}"
    ManagedPolicyArns:
      - !Sub "arn:${AWS::Partition}:iam::aws:policy/AdministratorAccess"
    PermissionsBoundary: !Ref DeveloperBoundary
    RoleName: CloudFormationRole

DeveloperBoundary:
  Type: "AWS::IAM::ManagedPolicy"
  Properties:
    Description: Permission boundary for developers
    ManagedPolicyName: PermissionsBoundary
    PolicyDocument:
      Version: "2012-10-17"
      Statement:
        - Sid: AllowModifyIamRolesWithBoundary
          Effect: Allow
          Action:
            - "iam:AttachRolePolicy"
            - "iam:CreateRole"
            - "iam:DeleteRolePolicy"
            - "iam:DetachRolePolicy"
            - "iam:PutRolePermissionsBoundary"
            - "iam:PutRolePolicy"
          Resource: !Sub "arn:${AWS::Partition}:iam::${AWS::AccountId}:role/app/*"
          Condition:
            ArnEquals:
              "iam:PermissionsBoundary": !Sub "arn:${AWS::Partition}:iam::
${AWS::AccountId}:policy/PermissionsBoundary"
        - Sid: AllowModifyIamRoles
          Effect: Allow
          Action:
            - "iam:DeleteRole"
            - "iam:TagRole"
            - "iam:UntagRole"
            - "iam:UpdateAssumeRolePolicy"
            - "iam:UpdateRole"
            - "iam:UpdateRoleDescription"
```

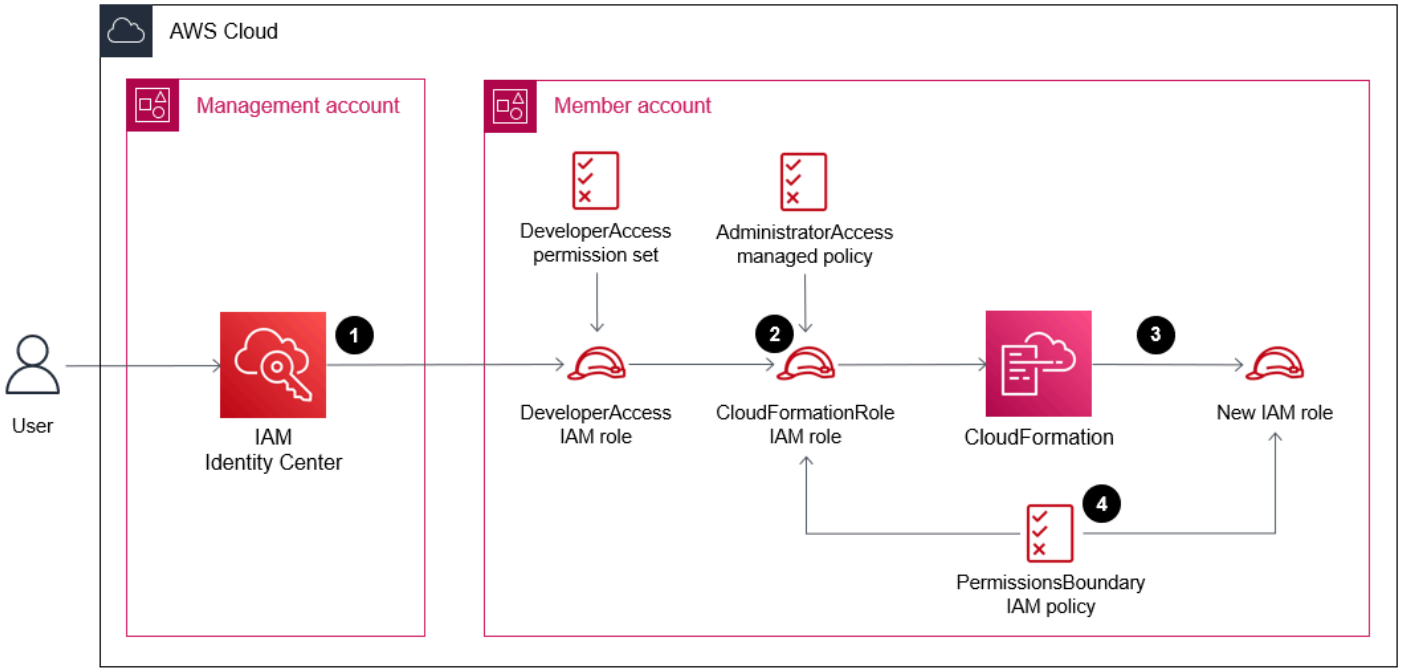
```
      Resource: !Sub "arn:${AWS::Partition}:iam::${AWS::AccountId}:role/app/*"
    - Sid: OverlyPermissiveAllowedServices
      Effect: Allow
      Action:
        - "lambda:*"
        - "apigateway:*"
        - "events:*"
        - "s3:*"
        - "logs:*"
      Resource: "*"
```

Die CloudFormationRoleRolle, die PermissionsBoundaryRichtlinie und der DeveloperAccessBerechtigungssatz gewähren zusammen die folgenden Berechtigungen:

- Benutzer haben über die ReadOnlyAccess AWS verwaltete Richtlinie nur Lesezugriff auf die meisten AWS-Services.
- Benutzer haben über die AWS verwaltete Access-Richtlinie AWSSupportZugriff auf offene Supportanfragen.
- Benutzer haben über die AWSBillingReadOnlyAccess AWS verwaltete Richtlinie nur Lesezugriff auf das AWS Billing Konsolen-Dashboard.
- Benutzer können über die AWSServiceCatalogEndUserFullAccess AWS verwaltete Richtlinie Produkte aus dem Service Catalog bereitstellen.
- Benutzer können mithilfe der Inline-Richtlinie die Kosten jeder CloudFormation Vorlage überprüfen und abschätzen.
- Mithilfe der CloudFormationRoleIAM-Rolle können Benutzer jeden CloudFormation Stack erstellen, aktualisieren oder löschen, der mit app/ beginnt.
- Benutzer können IAM-Rollen, CloudFormation die mit app/ beginnen, erstellen, aktualisieren oder löschen. Die PermissionsBoundaryIAM-Richtlinie verhindert, dass Benutzer ihre Rechte erweitern.
- Benutzer können Amazon AWS Lambda-, Amazon EventBridge - CloudWatch, Amazon Simple Storage Service (Amazon S3) - und Amazon API Gateway Gateway-Ressourcen nur mithilfe von bereitstellen CloudFormation.

Die folgende Abbildung zeigt, wie ein autorisierter Benutzer, z. B. ein Entwickler, mithilfe der in diesem Handbuch beschriebenen Berechtigungssätze, IAM-Rollen und Berechtigungsgrenzen eine neue IAM-Rolle in einem Mitgliedskonto erstellen kann:

1. Der Benutzer authentifiziert sich im IAM Identity Center und übernimmt die DeveloperAccessIAM-Rolle.
2. Der Benutzer initiiert die `cloudformation:CreateStack` Aktion und übernimmt die IAM-Rolle. CloudFormationRole
3. Der Benutzer initiiert die `iam:CreateRole` Aktion und erstellt CloudFormation damit eine neue IAM-Rolle.
4. Die PermissionsBoundaryIAM-Richtlinie wird auf die neue IAM-Rolle angewendet.



Der CloudFormationRoleRolle ist die AdministratorAccessverwaltete Richtlinie angehängt, aber aufgrund der PermissionsBoundaryIAM-Richtlinie entsprechen die effektiven Berechtigungen der CloudFormationRoleRolle der Richtlinie. PermissionsBoundary Die PermissionsBoundaryRichtlinie bezieht sich beim Zulassen der `iam:CreateRole` Aktion auf sich selbst, wodurch sichergestellt wird, dass Rollen nur erstellt werden können, wenn die Berechtigungsgrenze eingehalten wird.

Verwalten von Berechtigungen für Einzelpersonen

Mithilfe von Berechtigungssätzen, der Berechtigungsgrenze und der CloudFormationRoleIAM-Rolle können Sie die Anzahl der Berechtigungen einschränken, die Sie einzelnen Prinzipalen direkt zuweisen müssen. Auf diese Weise können Sie den Zugriff verwalten, wenn das Unternehmen wächst, und die bewährte Sicherheitsmethode, die Vergabe der geringsten Berechtigung, anwenden.

Sie können auch serviceverknüpfte Rollen verwenden, die einem AWS -Service Berechtigungen gewähren zur Bereitstellung von Ressourcen in Ihrem Namen. Anstatt dem IAM-Prinzipal (Benutzer, Benutzergruppe oder Rolle) Berechtigungen zu erteilen, können Sie die Berechtigungen auch dem Service gewähren. Mit der serviceverknüpften Rolle für AWS Service Catalogkönnen Sie beispielsweise Ihre eigenen Vorlagen, Ressourcen und Umgebungen bereitstellen, ohne dem IAM-Prinzipal Berechtigungen zuzuweisen. Weitere Informationen finden Sie unter AWS-Services , die mit IAM funktionieren und Verwenden von serviceverknüpften Rollen (IAM-Dokumentation).

Eine weitere bewährte Methode besteht darin, den Umfang des Zugriffs zu beschränken, den Einzelpersonen auf die AWS-Managementkonsole haben. Indem Sie den Zugriff auf die Konsole einschränken, können Sie festlegen, dass einzelne Personen Ressourcen mithilfe von Infrastructure-as-Code-Technologien (IaC) wie HashiCorp Terraform oder AWS CloudFormationPulumi bereitstellen. Durch die Verwaltung der Infrastruktur über IaC können Sie Änderungen an Ressourcen im Laufe der Zeit verfolgen und Mechanismen zur Genehmigung von Änderungen wie Pull-Requests einführen. GitHub

Netzwerkkonnektivität für eine Architektur mit mehreren Konten

Verbindung herstellen VPCs

Viele Unternehmen nutzen VPC-Peering in Amazon Virtual Private Cloud (Amazon VPC), um Entwicklung und Produktion zu verbinden. VPCs Mithilfe einer VPC-Peering-Verbindung können Sie den Verkehr zwischen zwei Verbindungen VPCs mithilfe einer privaten IP-Adressierung weiterleiten. Die Verbindung VPCs kann unterschiedlich AWS-Konten und unterschiedlich sein. AWS-Regionen Weitere Informationen finden Sie unter Was ist VPC-Peering (Amazon-VPC-Dokumentation). Wenn Unternehmen wachsen und die Anzahl der Unternehmen VPCs zunimmt, VPCs kann die Aufrechterhaltung von Peering-Verbindungen zwischen allen zu einer Wartungsbelastung werden. Möglicherweise sind Sie auch durch die maximale Anzahl von VPC-Peering-Verbindungen pro VPC begrenzt. Weitere Informationen finden Sie unter VPC-Peering-Verbindung-Quota (Amazon-VPC-Dokumentation).

Wenn Sie über mehrere Entwicklungs-, Test- und Staging-Umgebungen verfügen, in denen Daten außerhalb der Produktion gespeichert werden AWS-Konten, möchten Sie möglicherweise Netzwerkkonnektivität zwischen all diesen Umgebungen bereitstellen, VPCs aber jeglichen Zugriff auf Produktionsumgebungen verbieten. Sie können es verwenden AWS Transit Gateway, um mehrere Konten miteinander zu verbinden VPCs . Sie können die Routing-Tabellen trennen, um zu verhindern, dass die Entwicklung VPCs VPCs über das Transit-Gateway, das als zentraler Router fungiert, mit der Produktion kommuniziert. Weitere Informationen finden Sie unter Zentralisierter Router (Transit-Gateway-Dokumentation).

Transit-Gateway unterstützt auch Peering mit anderen Transit-Gateways, einschließlich solcher in verschiedenen AWS-Konten oder AWS-Regionen. Da es sich bei Transit-Gateway um einen vollständig verwalteten, hochverfügbaren Service handelt, müssen Sie für jede Region nur ein Transit-Gateway bereitstellen.

Weitere Informationen und detaillierte Netzwerkarchitekturen finden Sie unter Aufbau einer skalierbaren und sicheren AWS Multi-VPC-Netzwerkinfrastruktur (AWS Whitepaper).

Anwendungen verbinden

Wenn Sie die Kommunikation zwischen Anwendungen in verschiedenen Umgebungen in derselben Umgebung (z. B. AWS-Konten in der Produktion) einrichten müssen, können Sie eine der folgenden Optionen verwenden:

- VPC-Peering oder AWS Transit Gateway kann Konnektivität auf Netzwerkebene bereitstellen, wenn Sie einen breiten Zugriff auf mehrere IP-Adressen und Ports ermöglichen möchten.
- AWS PrivateLink erstellt Endpunkte in einem privaten Subnetz der VPC und diese Endpunkte werden als DNS-Einträge in Amazon Route 53 Resolver registriert. Mithilfe von DNS können Anwendungen die Endpunkte auflösen und eine Verbindung zu den registrierten Services herstellen, ohne dass NAT-Gateways oder Internet-Gateways in der VPC erforderlich sind.
- Amazon VPC Lattice ordnet Dienste wie Anwendungen mehreren Konten zu VPCs und fasst sie in einem Servicenetzwerk zusammen. Kunden, die mit dem Servicenetzwerk VPCs verbunden sind, können Anfragen an alle anderen Dienste senden, die dem Servicenetzwerk zugeordnet sind, unabhängig davon, ob sie sich im selben Konto befinden. VPC Lattice lässt sich in AWS Resource Access Manager (AWS RAM) integrieren, sodass Sie Ressourcen mit anderen Konten oder über gemeinsam nutzen können. AWS Organizations Sie können eine VPC nur einem Servicenetzwerk zuordnen. Diese Lösung erfordert kein VPC-Peering oder AWS Transit Gateway , um kontenübergreifend zu kommunizieren.

Bewährte Methoden für Netzwerkkonnektivität

- Erstellen Sie einen AWS-Konto , den Sie für das zentrale Netzwerk verwenden. Geben Sie diesem Konto den Namen network-prod und verwenden Sie es für AWS Transit Gateway Amazon VPC IP Address Manager (IPAM). Fügen Sie dieses Konto der Infrastructure_Prod Organisationseinheit hinzu.
- Verwenden Sie AWS Resource Access Manager (AWS RAM), um das Transit-Gateway, die VPC-Lattice-Servicenetzwerke und die IPAM-Pools mit dem Rest der Organisation zu teilen. Auf diese Weise kann jeder AWS-Konto in Ihrer Organisation mit diesen Diensten interagieren.
- Durch die Verwendung von IPAM-Pools zur zentralen Verwaltung IPv4 und IPv6 Adressierung von Zuweisungen können Sie es Ihren Endbenutzern ermöglichen, sich selbst VPCs bereitzustellen, indem Sie AWS Service Catalog Auf diese Weise können Sie IP-Adressräume angemessen dimensionieren VPCs und überlappende IP-Adressräume verhindern.

- Verwenden Sie einen zentralisierten Ausgangsansatz für Datenverkehr, der an das Internet gebunden ist, und verwenden Sie einen dezentralen Eingangsansatz für Datenverkehr, der aus dem Internet in Ihre Umgebung gelangt. Weitere Informationen erhalten Sie unter Zentralisierter Ausgang und Dezentraler Eingang.

Zentralisierter Ausgang

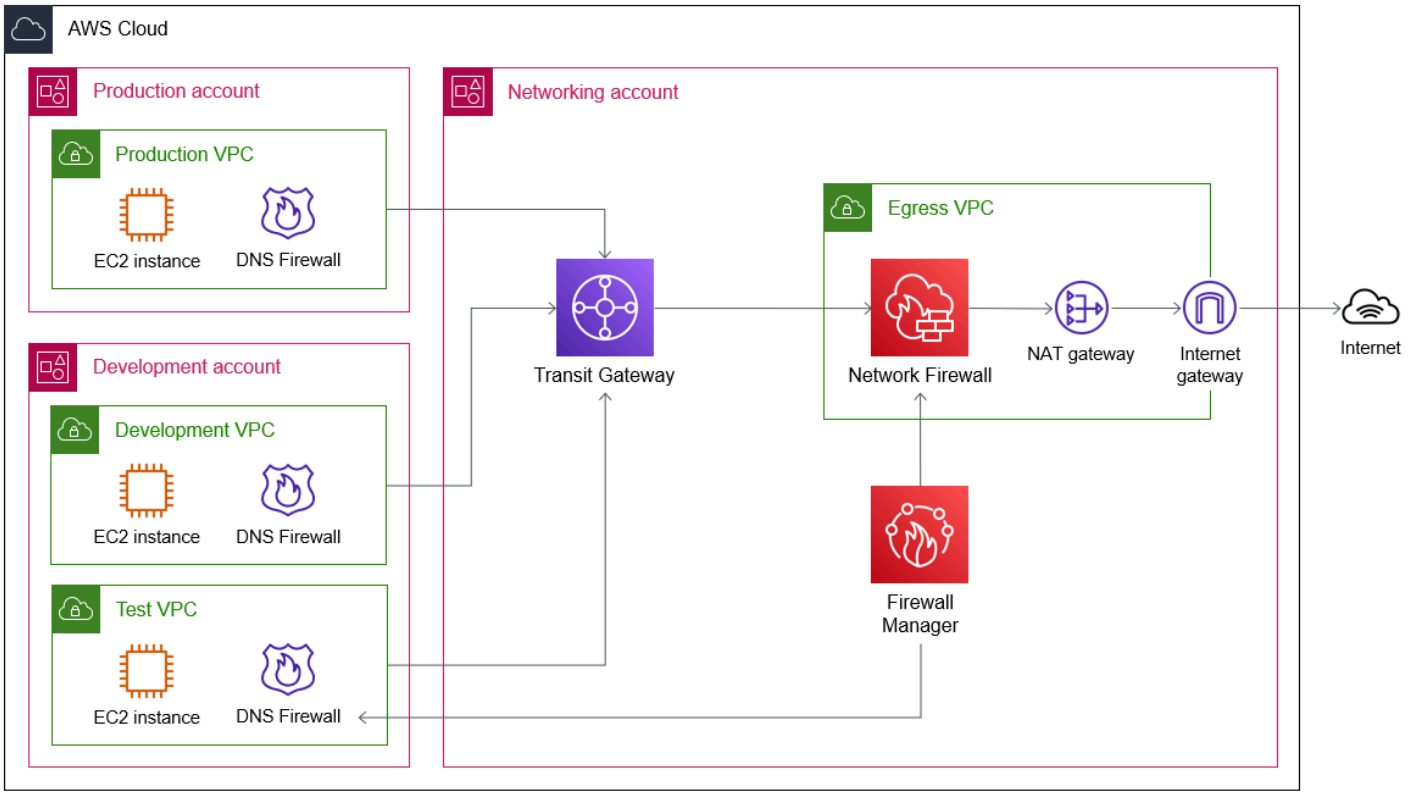
Zentralisierter Ausgang ist das Prinzip der Verwendung eines einzigen, gemeinsamen Eingangspunkts für den gesamten Netzwerkverkehr, der für das Internet bestimmt ist. Sie können die Inspektion an diesem Eingangspunkt einrichten und den Datenverkehr nur zu bestimmten Domänen oder nur über bestimmte Ports oder Protokolle zulassen. Durch die Zentralisierung von ausgehendem Datenverkehr können Sie auch Kosten senken, da Sie nicht mehr in jedem Ihrer VPCs Systeme NAT-Gateways einrichten müssen, um auf das Internet zuzugreifen. Aus Sicherheitsgründen ist dies von Vorteil, da dadurch die Gefahr von extern zugänglichen bösartigen Ressourcen, wie z. B. der C&C-Infrastruktur (Malware Command and Control – C&C), begrenzt wird. Weitere Informationen und Architekturoptionen für zentralisierten ausgehenden Datenverkehr finden Sie unter Zentralisierter Ausgang ins Internet (Whitepaper).AWS

Sie können AWS Network Firewall verwenden, wobei es sich um einen zustandsbehafteten, verwalteten Netzwerk-Firewall und Service zur Erkennung und Verhinderung von Eindringlingen handelt, der als zentraler Inspektionspunkt für ausgehenden Datenverkehr dient. Sie richten diese Firewall in einer dedizierten VPC für ausgehenden Datenverkehr ein. Die Network Firewall unterstützt statusbehaftete Regeln, mit denen Sie den Internetzugriff auf bestimmte Domains beschränken können. Weitere Informationen finden Sie unter Domainfilterung (Dokumentation zur Network Firewall).

Sie können auch die Amazon Route 53 Resolver -DNS-Firewall verwenden, um den ausgehenden Verkehr auf bestimmte Domainnamen zu beschränken, hauptsächlich um die unbefugte Exfiltration Ihrer Daten zu verhindern. In den DNS-Firewallregeln können Sie Domainlisten (Route-53-Dokumentation) anwenden, die den Zugriff auf bestimmte Domains zulassen oder verweigern.
Sie können AWS verwaltete Domänenlisten verwenden, die Domainnamen enthalten, die mit böswilligen Aktivitäten oder anderen potenziellen Bedrohungen in Verbindung stehen, oder Sie können benutzerdefinierte Domänenlisten erstellen. Sie erstellen DNS-Firewall-Regelgruppen und wenden sie dann auf Ihre an VPCs. Ausgehende DNS-Anfragen werden zur Domainnamenauflösung über einen Resolver in der VPC weitergeleitet, und die DNS-Firewall filtert die Anfragen auf der Grundlage der auf die VPC angewendeten Regelgruppen. Rekursive DNS-Anfragen, die an Resolver

gehen, werden nicht über den Transit-Gateway- und Netzwerkfirewall-Pfad geleitet. Route 53 Resolver und DNS-Firewall sollten als separate Ausgangspfade aus der VPC betrachtet werden.

Die folgende Abbildung zeigt eine Beispielarchitektur für zentralisierten Ausgang. Bevor die Netzwerkkommunikation beginnt, werden DNS-Anfragen an Route 53 Resolver gesendet, wo die DNS-Firewall die Auflösung der für die Kommunikation verwendeten IP-Adresse zulässt oder verweigert. Der für das Internet bestimmte Datenverkehr wird über ein zentrales Netzwerkkonto an ein Transit-Gateway weitergeleitet. Das Transit-Gateway leitet den Datenverkehr zur Überprüfung an die Network Firewall weiter. Wenn die Firewall-Richtlinie den ausgehenden Verkehr zulässt, wird der Datenverkehr über ein NAT-Gateway, über ein Internet-Gateway und ins Internet geleitet. Sie können AWS Firewall Manager damit DNS-Firewall-Regelgruppen und Netzwerk-Firewall-Richtlinien in Ihrer Infrastruktur mit mehreren Konten zentral verwalten.



Bewährte Methoden zur Absicherung des ausgehenden Datenverkehrs

- Fangen Sie an im Nur-Protokollierungs-Modus (Dokumentation zu Route 53). Wechseln Sie in den Blockmodus, nachdem Sie überprüft haben, dass legitimer Datenverkehr nicht beeinträchtigt wird.
- Blockieren Sie den DNS-Verkehr, der ins Internet geht, mithilfe von AWS Firewall Manager Richtlinien für Netzwerkzugriffskontrolllisten oder mithilfe AWS Network Firewall von Alle

DNS-Abfragen sollten über einen Route 53 Resolver geleitet werden, wo Sie sie mit Amazon überwachen GuardDuty (falls aktiviert) und mit der Route 53 Resolver DNS Firewall (falls aktiviert) filtern können. Weitere Informationen finden Sie unter Auflösen von DNS-Abfragen zwischen VPCs und Ihrem Netzwerk (Route 53-Dokumentation).

- Verwenden Sie die AWS -verwalteten Domainlisten (Dokumentation zu Route 53) in DNS-Firewall und Netzwerk-Firewall.
- Erwägen Sie, ungenutzte Top-Level-Domains mit hohem Risiko wie .info, .top, .xyz oder einige Ländercode-Domains zu blockieren.
- Erwägen Sie, ungenutzte Ports mit hohem Risiko zu blockieren, z. B. die Ports 1389, 4444, 3333, 445, 135, 139 oder 53.
- Als Ausgangspunkt können Sie eine Ablehnungsliste verwenden, die die AWS verwalteten Regeln enthält. Anschließend können Sie im Laufe der Zeit an der Implementierung eines Modells für Zulassungslisten arbeiten. Anstatt beispielsweise nur eine strikte Liste voll qualifizierter Domainnamen in die Zulassungsliste aufzunehmen, sollten Sie zunächst einige Platzhalter verwenden, z. B. *.example.com. Sie können sogar nur die Top-Level-Domains zulassen, die Sie erwarten, und alle anderen blockieren. Grenzen Sie diese dann im Laufe der Zeit auch ein.
- Verwenden Sie Route 53-Profile (Route 53-Dokumentation), um DNS-bezogene Route 53-Konfigurationen auf viele VPCs und unterschiedliche Arten anzuwenden. AWS-Konten
- Definieren Sie einen Prozess für den Umgang mit Ausnahmen von diesen bewährten Methoden.

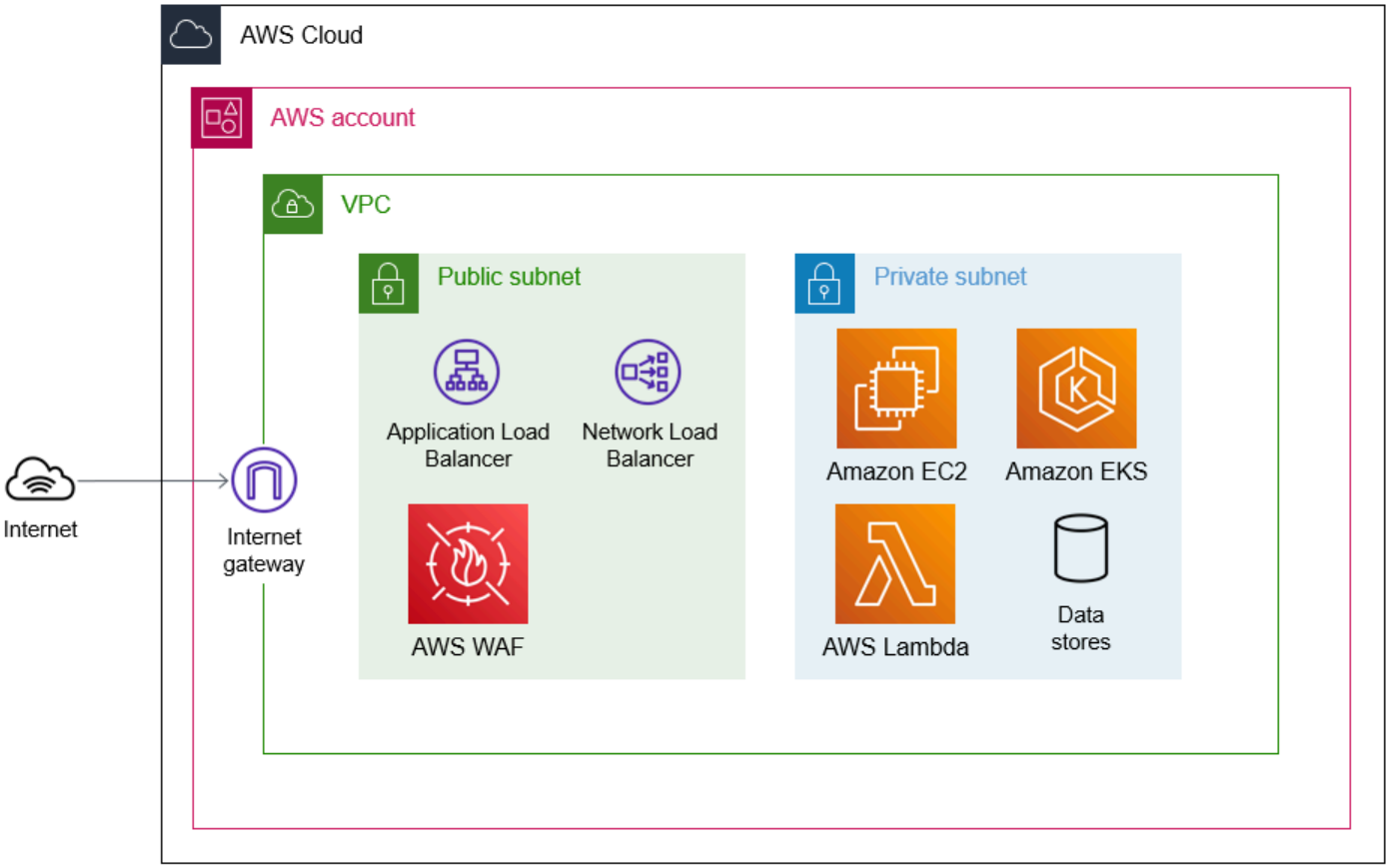
Dezentraler Eingang

Dezentraler Eingang ist das Prinzip, bei dem auf der Ebene eines einzelnen Kontos festgelegt wird, wie der Verkehr aus dem Internet die Workloads in diesem Konto erreicht. In Architekturen mit mehreren Konten besteht einer der Vorteile des dezentralen Eingangs darin, dass jedes Konto den für seine Workloads am besten geeigneten Eingangsservice oder die für seine Workloads am besten geeignete Eingangsressource verwenden kann, z. B. einen Application Load Balancer, Amazon API Gateway oder Network Load Balancer.

Dezentraler Eingang bedeutet zwar, dass Sie jedes Konto einzeln verwalten müssen, aber Sie können Ihre Konfigurationen mit AWS Firewall Manager zentral verwalten. Firewall Manager unterstützt Schutzmaßnahmen wie AWS WAF und Amazon-VPC-Sicherheitsgruppen. Sie können eine Verbindung AWS WAF zu einem Application Load Balancer, Amazon CloudFront, API Gateway oder AWS AppSync herstellen. Wenn Sie eine Eingangs-VPC und ein Transit-Gateway wie unter Zentralisierter Ausgang beschrieben verwenden, enthält jede Spoke-VPC öffentliche und private

Subnetze. Es ist jedoch nicht erforderlich, NAT-Gateways bereitzustellen, da der Datenverkehr über die Ausgangs-VPC im Netzwerkkonto geleitet wird.

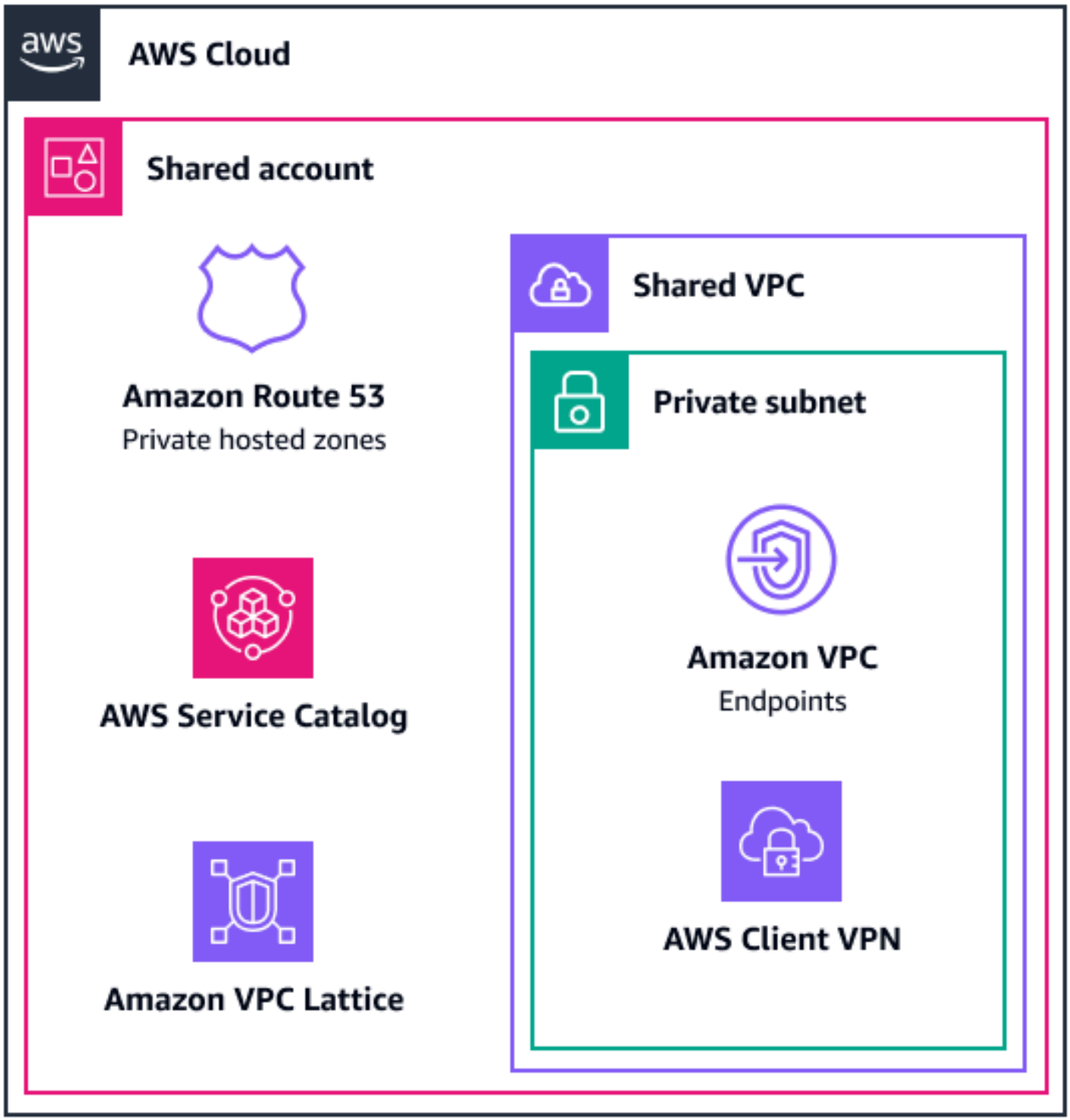
Die folgende Abbildung zeigt ein Beispiel für eine Person AWS-Konto , die über eine einzelne VPC verfügt, die einen über das Internet zugänglichen Workload enthält. Datenverkehr aus dem Internet greift über ein Internet-Gateway auf die VPC zu und erreicht Load–Balancing- und Sicherheits-Services, die in einem öffentlichen Subnetz gehostet werden. (Ein öffentliches Subnetz enthält eine Standardroute zu einem Internet-Gateway). Stellen Sie Load Balancer in öffentlichen Subnetzen bereit und hängen Sie AWS WAF Zugriffskontrolllisten (ACLs) an, um sich vor bösartigem Datenverkehr wie Cross-Site-Scripting zu schützen. Stellen Sie Workloads, die Anwendungen hosten, in privaten Subnetzen bereit, die keinen direkten Zugang zum und vom Internet haben.



Wenn Sie VPCs in Ihrer Organisation viele davon haben, möchten Sie möglicherweise gemeinsame Endpunkte nutzen, AWS-Services indem Sie VPC-Endpunkte mit Schnittstellen oder private gehostete Zonen in einer dedizierten und gemeinsam genutzten Zone erstellen. AWS-Konto Weitere Informationen finden Sie unter Zugreifen und AWS-Service Verwenden eines VPC-Endpunkts mit

einer Schnittstelle (AWS PrivateLink Dokumentation) und Arbeiten mit privaten gehosteten Zonen (Route 53-Dokumentation).

Die folgende Abbildung zeigt ein Beispiel für eine AWS-Konto , die Ressourcen hostet, die in der gesamten Organisation gemeinsam genutzt werden können. VPC-Endpunkte können von mehreren Konten gemeinsam genutzt werden, indem sie in einer dedizierten VPC erstellt werden. Wenn Sie einen VPC-Endpunkt erstellen, können Sie optional AWS die DNS-Einträge für den Endpunkt verwalten lassen. Um einen Endpunkt gemeinsam zu nutzen, deaktivieren Sie diese Option und erstellen Sie die DNS-Einträge in einer separaten privat gehosteten Zone (PHZ) von Route 53. Anschließend können Sie die PHZ allen VPCs in Ihrer Organisation zuordnen, um die zentrale DNS-Auflösung der VPC-Endpunkte zu gewährleisten. Sie müssen auch sicherstellen, dass die Routentabellen des Transit-Gateways Routen für die gemeinsam genutzte VPC zur anderen VPCs enthalten. Weitere Informationen finden Sie unter Zentralisierter Zugriff auf VPC-Schnittstellen-Endpunkte (AWS Whitepaper).



Ein geteiltes AWS-Konto Konto ist auch ein guter Ort, um AWS Service Catalog Portfolios zu hosten. Ein Portfolio ist eine Sammlung von IT-Services, die Sie für die Bereitstellung zur Verfügung stellen möchten AWS, und das Portfolio enthält Konfigurationsinformationen für diese Services. Sie können die Portfolios im gemeinsamen Konto erstellen, sie für die Organisation freigeben, und

dann importiert jedes Mitgliedskonto das Portfolio in seine eigene regionale Service Catalog-Instanz. Weitere Informationen finden Sie unter Teilen mit AWS Organizations (Dokumentation zum Service Catalog).

In ähnlicher Weise können Sie mit Amazon VPC Lattice das gemeinsame Konto verwenden, um Ihre Umgebung und Service-Vorlagen als Entitäten zentral zu verwalten und dann Kontoverbindungen mit den Mitgliedskonten der Organisation einzurichten. Weitere Informationen finden Sie unter Teilen Ihrer VPC Lattice-Entitäten (VPC Lattice-Dokumentation).

Reaktion auf Sicherheitsvorfälle für eine Architektur mit mehreren Konten

Bei der Umstellung auf mehrere ist es wichtig AWS-Konten, dass Sie den Überblick über Sicherheitsereignisse behalten, die in Ihrem Unternehmen auftreten können. In Identitätsmanagement und Zugriffskontrolle haben Sie AWS Control Tower benutzt, um Ihre Landing Zone einzurichten. Während dieses Einrichtungsprozesses AWS Control Tower wurde ein bestimmter AWS-Konto Sicherheitsaspekt festgelegt. Sie sollten die Verwaltung der Sicherheitsdienste an das Konto delegieren und dieses security-tooling-prodKonto verwenden, um diese Dienste zentral zu verwalten.

In diesem Leitfaden wird beschrieben, wie Sie sich AWS-Konten und Ihr Unternehmen AWS-Services mit folgenden Maßnahmen schützen können:

- Amazon GuardDuty
- Amazon Macie
- AWS Security Hub CSPM

Amazon GuardDuty

Amazon GuardDuty ist ein Dienst zur kontinuierlichen Sicherheitsüberwachung, der Datenquellen wie AWS CloudTrail Ereignisprotokolle analysiert. Eine vollständige Liste der unterstützten Datenquellen finden Sie unter So GuardDuty verwendet Amazon seine Datenquellen (GuardDuty Dokumentation). Er verwendet Bedrohungsdaten, z. B. Listen bösartiger IP-Adressen und Domains, ebenso wie Machine Learning, um unerwartete und potenziell nicht autorisierte bösartige Aktivitäten in Ihrer AWS -Umgebung zu identifizieren.

Wenn Sie GuardDuty mit verwenden AWS Organizations, kann das Verwaltungskonto in der Organisation jedes Konto in der Organisation als GuardDuty delegierten Administrator bestimmen. Der delegierte Administrator wird zum GuardDuty Administratorkonto für die Region. GuardDuty ist in folgenden Bereichen automatisch aktiviert:AWS-Region, und das delegierte Administratorkonto ist berechtigt, alle Konten in der Organisation in dieser Region zu aktivieren und zu verwalten GuardDuty . Weitere Informationen finden Sie unter GuardDuty Konten verwalten mit AWS Organizations (GuardDuty Dokumentation).

GuardDuty ist ein regionaler Dienst. Das bedeutet, dass Sie GuardDuty in jeder Region, die Sie überwachen möchten, die Aktivierung vornehmen müssen.

Best Practices

- GuardDuty In allen unterstützten Bereichen aktivieren AWS-Regionen. GuardDuty kann Erkenntnisse über unbefugte oder ungewöhnliche Aktivitäten generieren, auch in Regionen, die Sie nicht aktiv nutzen. Die Preisgestaltung für GuardDuty richtet sich nach der Anzahl der analysierten Ereignisse. Selbst in Regionen, in denen Sie keine Workloads ausführen, GuardDuty ist Enabling ein effektives und kostengünstiges Erkennungstool, das Sie vor potenziell bösartigen Aktivitäten warnt. Weitere Informationen zu den Regionen, in denen GuardDuty es verfügbar ist, finden Sie unter Amazon GuardDuty Service Endpoints (Allgemeine AWS-Referenz).
- Delegieren Sie innerhalb jeder Region das security-tooling-prodKonto an die Verwaltung Ihrer Organisation GuardDuty . Weitere Informationen finden Sie unter Benennen eines GuardDuty delegierten Administrators (Dokumentation). GuardDuty
- Konfigurieren Sie GuardDuty die Konfiguration so, dass neue Benutzer automatisch registriert werden AWS-Konten , sobald sie der Organisation hinzugefügt werden. Weitere Informationen finden Sie unter Schritt 3 — Automatisieren des Hinzufügens neuer Organisationskonten als Mitglieder unter Konten verwalten mit AWS Organizations (GuardDuty Dokumentation).

Amazon Macie

Amazon Macie ist ein vollständig verwalteter Service für Datensicherheit und Datenschutz, der Machine Learning und Musterabgleich verwendet, um Ihre sensiblen Daten in Amazon Simple Storage Service (Amazon S3) zu erkennen, zu überwachen und zu schützen. Sie können Daten von Amazon Relational Database Service (Amazon RDS) und Amazon DynamoDB in einen S3-Bucket exportieren und dann Macie verwenden, um die Daten zu scannen.

Wenn Sie Macie mit verwenden AWS Organizations, kann das Verwaltungskonto in der Organisation jedes Konto in der Organisation als Macie-Administratorkonto festlegen. Das Administratorkonto kann Macie für die Mitgliedskonten in der Organisation aktivieren und verwalten, auf Amazon-S3-Inventory-Daten zugreifen und Aufträge zur Erkennung sensibler Daten für die Konten ausführen. Weitere Informationen finden Sie unter Verwalten von Konten mit AWS Organizations (Macie-Dokumentation).

Macie ist ein regionaler Service. Das bedeutet, dass Sie Macie in jeder Region aktivieren müssen, die Sie überwachen möchten, und dass das Macie-Administratorkonto Mitgliedskonten nur innerhalb derselben Region verwalten kann.

Best Practices

- Folgen Sie sich den Überlegungen und Empfehlungen zur Verwendung von Macie mit AWS Organizations (Macie-Dokumentation).
- Delegieren Sie innerhalb jeder Region das security-tooling-prodKonto an die Verwaltung von Macie für Ihre Organisation. Um Macie-Konten in mehreren Ländern zentral zu verwalten AWS-Regionen, muss sich das Verwaltungskonto in jeder Region anmelden, in der die Organisation Macie derzeit verwendet oder verwenden wird, und dann das Macie-Administratorkonto für jede dieser Regionen festlegen. Das Macie-Administratorkonto kann dann die Organisation in jeder dieser Regionen konfigurieren. Weitere Informationen finden Sie unter Integrieren und Konfigurieren einer Organisation (Macie-Dokumentation).
- Macie bietet ein monatliches kostenloses Kontingent für die Suche nach sensiblen Daten. Wenn Sie möglicherweise sensible Daten in Amazon S3 gespeichert haben, verwenden Sie Macie, um Ihre S3-Buckets im Rahmen des monatlichen kostenlosen Kontingents zu analysieren. Wenn Sie das kostenlose Kontingent überschreiten, fallen für Ihr Konto Gebühren für die Erfassung sensibler Daten an.

AWS Security Hub CSPM

AWS Security Hub CSPMbietet Ihnen einen umfassenden Überblick über Ihren Sicherheitsstatus in. AWS Sie können damit Ihre Umgebung anhand von Industriestandards und bewährten Methoden der Sicherheit überprüfen. Security Hub CSPM sammelt Sicherheitsdaten aus all Ihren AWS-Konten Diensten (einschließlich Macie) GuardDuty und unterstützten Produkten von Drittanbietern. Security Hub CSPM hilft Ihnen dabei, Sicherheitstrends zu analysieren und Sicherheitsprobleme mit der höchsten Priorität zu identifizieren. Security Hub CSPM bietet verschiedene Sicherheitsstandards, die Sie aktivieren können, um in jedem Standard Konformitätsprüfungen durchzuführen. AWS-Konto

Wenn Sie Security Hub CSPM mit verwenden AWS Organizations, kann das Verwaltungskonto in der Organisation jedes Konto in der Organisation als Security Hub CSPM-Administratorkonto festlegen. Das Security Hub CSPM-Administratorkonto kann dann andere Mitgliedskonten in der Organisation aktivieren und verwalten. Weitere Informationen finden Sie unter AWS Organizations Zur Verwaltung von Konten verwenden (Security Hub CSPM-Dokumentation).

Security Hub CSPM ist ein regionaler Dienst. Das bedeutet, dass Sie Security Hub CSPM in jeder Region aktivieren müssen, die Sie analysieren möchten, und in AWS Organizations der Sie den delegierten Administrator für jede Region definieren müssen.

Best Practices

- Halten Sie sich an die Voraussetzungen und Empfehlungen (Security Hub CSPM-Dokumentation).
- Delegieren Sie das security-tooling-prodKonto in jeder Region, um Security Hub CSPM für Ihr Unternehmen zu verwalten. Weitere Informationen finden Sie unter Benennen eines Security Hub CSPM-Administratorkontos (Security Hub CSPM-Dokumentation).
- Konfigurieren Sie Security Hub CSPM so, dass neue Benutzer automatisch registriert werden AWS-Konten , wenn sie der Organisation hinzugefügt werden.
- Aktivieren Sie den Standard AWS Foundational Security Best Practices (Security Hub CSPM-Dokumentation), um zu erkennen, wenn Ressourcen von den bewährten Sicherheitsmethoden abweichen.
- Aktivieren Sie die regionsübergreifende Aggregation (Security Hub CSPM-Dokumentation), sodass Sie alle Ihre Security Hub-CSPM-Ergebnisse von einer einzigen Region aus anzeigen und verwalten können.

Konfigurieren von Backups für eine Architektur mit mehreren Konten

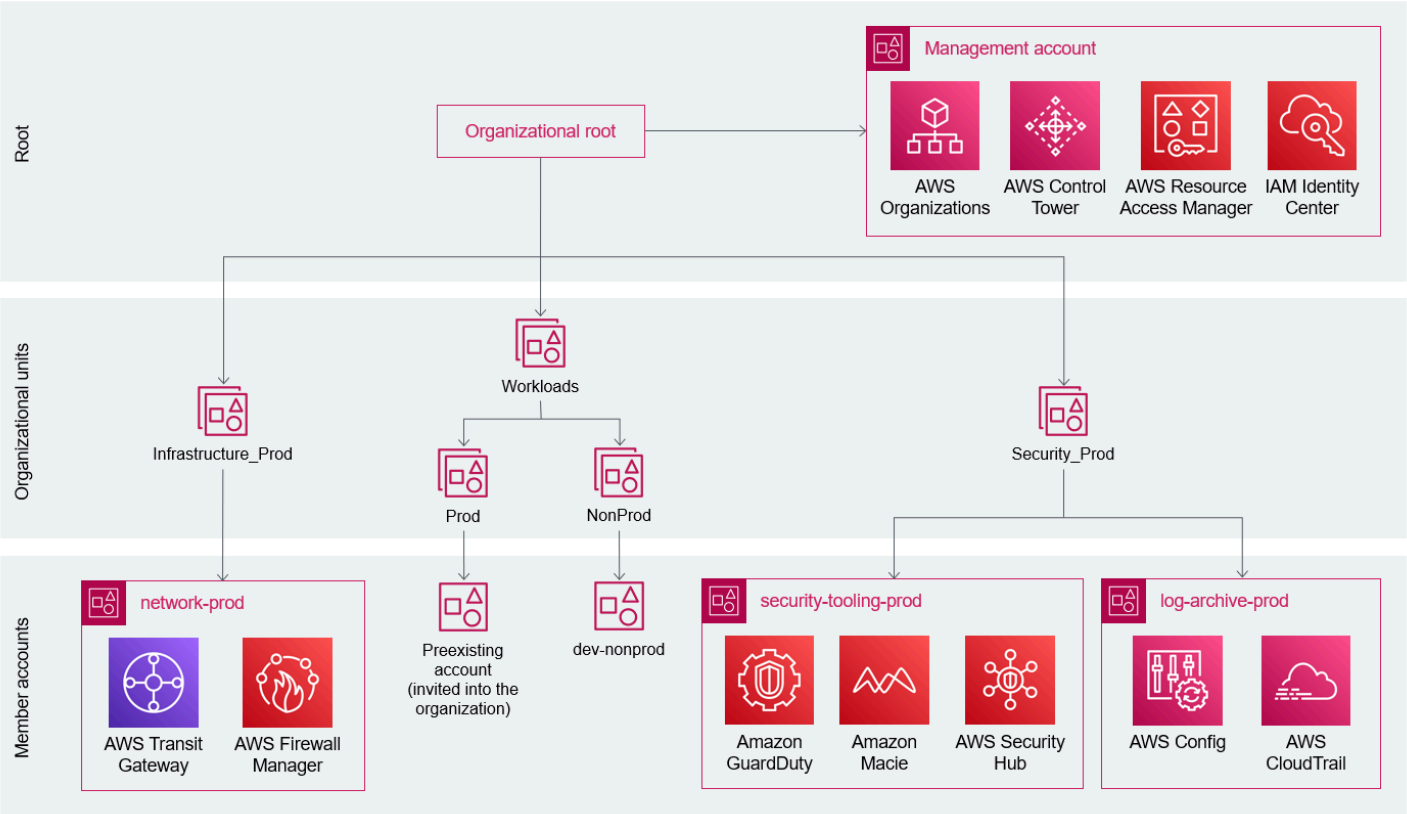
Eine umfassende Backup-Strategie ist ein wesentlicher Bestandteil des Datenschutzplans eines Unternehmens, um etwaigen Auswirkungen eines Sicherheitsvorfalls standzuhalten, sie zu verringern und sich zu erholen. Eine Backup-Richtlinie hilft Ihnen, eine Backup-Strategie für die Ressourcen über alle Konten in Ihrer Organisation zu standardisieren und zu implementieren. In einer Backup-Richtlinie können Sie Backup-Pläne für Ihre Ressourcen konfigurieren und bereitstellen. Weitere Informationen finden Sie unter Backup-Richtlinien (AWS Organizations Dokumentation). Weitere Informationen finden Sie unter Die 10 besten Sicherheitsmethoden zur Sicherung von Backups in AWS (AWS Prescriptive Guidance).

Kontomigration beim Übergang zu einer Multi-Konto-Architektur

In Einladen Ihres bereits bestehenden Kontos haben Sie Ihr bereits bestehendes Konto eingeladen, der Organisationseinheit Workloads > Prod beizutreten. Dieses Konto wird jetzt als Teil Ihrer Organisation verwaltet.

Sie haben auch ein neues dev-nonprod-Konto in der Organisationseinheit Workloads > bereitgestellt. NonProd Teammitglieder sollten nun über auf die entsprechenden Konten zugreifen können. AWS IAM Identity Center Entfernen Sie alle einzelnen Benutzerkonten in AWS Identity and Access Management (IAM).

Wenn Sie die Empfehlungen in diesem Leitfaden befolgt haben, hat Ihre Organisation nun die folgende Struktur.



Wenn innerhalb des bereits vorhandenen Kontos Workloads ausgeführt werden, migrieren Sie diese Workloads nun gemäß den Kriterien, die Sie in Definieren Sie die Umfangskriterien festgelegt haben, in unabhängige Konten. Migrieren Sie alle Workloads, die nicht zur Produktion gehören, auf die neue

Organisationseinheit dev-nonprod und migrieren Sie Produktionsworkloads auf das Konto network-prod. Weitere Informationen zur Migration gängiger AWS Ressourcen finden Sie im folgenden Abschnitt dieses Handbuchs. Migration von Ressourcen

Ressourcenreplikation oder Migration zwischen AWS-Konten

Nach der Migration von einer Architektur mit einem Konto AWS-Konto zu einer Architektur mit mehreren Konten ist es üblich, dass Produktions- und Nicht-Produktionsworkloads in dem bereits vorhandenen Konto ausgeführt werden. Die Migration dieser Ressourcen auf dedizierte Produktions- und Nicht-Produktionskonten oder Organisationseinheiten hilft Ihnen bei der Verwaltung des Zugriffs und des Netzwerks für diese Workloads. Im Folgenden sind einige Optionen für die Migration allgemeiner Ressourcen auf andere Ressourcen aufgeführt. AWS AWS-Konto

Dieser Abschnitt konzentriert sich auf Strategien zur Replikation von Daten zwischen AWS-Konten. Sie sollten sich bemühen, Ihre Workloads so zustandslos wie möglich zu gestalten, um zu vermeiden, dass Datenverarbeitungsressourcen zwischen Konten repliziert werden müssen. Es ist auch von Vorteil, Ihre Ressourcen über Infrastructure as Code (IaC) zu verwalten, sodass Sie eine Umgebung in einem separaten AWS-Konto erneut bereitstellen können.

In diesem Abschnitt werden Optionen für die Migration der folgenden Datenressourcen beschrieben:

- AWS AppConfig Konfigurationen und Umgebungen
- AWS Certificate Manager zertifikate
- CloudFront Amazon-Distributionen
- AWS CodeArtifact Domänen und Repositorys
- Amazon-DynamoDB-Tabellen
- Amazon-EBS-Volumes
- Amazon EC2 EC2-Instances oder AMIs
- Amazon-ECR-Register
- Amazon-EFS-Dateisysteme
- ElastiCache Amazon-Cluster (Redis OSS)
- AWS Elastic Beanstalk Umgebungen
- Elastic-IP-Adressen
- AWS Lambda Schichten
- Amazon-Lightsail-Instances
- Amazon Neptune-Cluster
- Amazon OpenSearch Service-Domänen

- Amazon-RDS-Snapshots
- Amazon-Redshift-Cluster
- Amazon-Route-53-Domains und gehostete Zonen
- Amazon-S3-Buckets
- SageMaker Amazon-KI-Modelle
- AWS WAF Web ACLs

AWS AppConfig Konfigurationen und Umgebungen

AWS AppConfig unterstützt nicht das direkte Kopieren seiner Konfiguration in eine andere AWS-Konto. Es hat sich jedoch bewährt, die AWS AppConfig Konfigurationen und Umgebungen getrennt von den Konfigurationen und Umgebungen zu verwalten, in AWS-Konten denen die Umgebungen gehostet werden. Weitere Informationen finden Sie unter Kontoübergreifende Konfiguration mit AWS AppConfig (AWS Blogbeitrag).

AWS Certificate Manager zertifikate

Sie können ein AWS Certificate Manager (ACM-) Zertifikat nicht direkt von einem Konto in ein anderes exportieren, da der Schlüssel AWS Key Management Service (AWS KMS), der zur Verschlüsselung des privaten Schlüssels des Zertifikats verwendet wird, für jedes AWS-Region Konto einzigartig ist. Sie können jedoch gleichzeitig mehrere Zertifikate mit demselben Domainnamen für mehrere Konten und Regionen bereitstellen. ACM unterstützt die Validierung des Domainbesitzes mithilfe von DNS (empfohlen) oder E-Mail. Wenn Sie die DNS-Validierung verwenden und ein neues Zertifikat erstellen, generiert ACM einen eindeutigen CNAME-Eintrag für jede Domain auf dem Zertifikat. Der CNAME-Eintrag ist für jedes Konto einzigartig und muss innerhalb von 72 Stunden der von Amazon Route 53 gehosteten Zone oder dem DNS-Anbieter hinzugefügt werden, damit das Zertifikat ordnungsgemäß validiert wird.

CloudFront Amazon-Distributionen

Amazon unterstützt CloudFront keine Migration von Distributionen von einer AWS-Konto zur anderen AWS-Konto. CloudFront Unterstützt jedoch die Migration eines alternativen Domainnamens, auch bekannt als CNAME, von einer Distribution zur anderen. Weitere Informationen finden Sie unter Wie behebe ich den CNAMEAlready Exists-Fehler, wenn ich einen CNAME-Alias für meine CloudFront Distribution einrichte? (AWS Knowledge Center).

AWS CodeArtifact Domänen und Repositorys

Eine Organisation kann zwar mehrere Domains haben, es wird jedoch empfohlen, eine einzige Produktionsdomain zu verwenden, die alle veröffentlichten Artefakte enthält. Dies hilft Entwicklungsteams dabei, Pakete innerhalb einer Organisation zu finden und gemeinsam zu nutzen. Das Konto AWS-Konto , dem die Domain gehört, kann sich von dem Konto unterscheiden, dem alle mit der Domain verknüpften Repositorys gehören. Sie können Pakete zwischen Repositorys kopieren, sie müssen jedoch zu derselben Domain gehören. Weitere Informationen finden Sie unter Pakete zwischen Repositorys kopieren (CodeArtifact Dokumentation).

Amazon-DynamoDB-Tabellen

Sie können einen der folgenden Services verwenden, um eine Amazon-DynamoDB-Tabelle in ein anderes AWS-Konto zu migrieren:

- AWS Backup
- DynamoDB-Import und -Export zu Amazon S3
- Amazon S3 und AWS Glue
- AWS Data Pipeline
- Amazon EMR

Weitere Informationen finden Sie unter Wie kann ich meine Amazon DynamoDB-Tabellen von einer AWS-Konto zur anderen migrieren (AWS Knowledge Center).

Amazon-EBS-Volumes

Sie können einen Snapshot eines vorhandenen Amazon Elastic Block Store (Amazon EBS)-Volumes erstellen, den Snapshot mit dem Zielkonto teilen und dann eine Kopie des Volumes im Zielkonto erstellen. Dadurch wird das Volume effektiv von einem Konto zum anderen migriert. Weitere Informationen finden Sie unter Wie kann ich einen verschlüsselten Amazon EBS-Snapshot oder ein verschlüsseltes Volume mit einem anderen teilen AWS-Konto (AWS Knowledge Center).

Amazon EC2 EC2-Instances oder AMIs

Es ist nicht möglich, bestehende Amazon Elastic Compute Cloud (Amazon EC2) -Instances oder Amazon Machine Images (AMIs) direkt auf eine andere AWS-Konto zu übertragen. Stattdessen

können Sie ein benutzerdefiniertes AMI im Quellkonto erstellen, das AMI mit dem Zielkonto teilen, eine neue EC2-Instance über das gemeinsam genutzte AMI im Zielkonto starten und dann das gemeinsam genutzte AMI abmelden.

Amazon-ECR-Register

Amazon Elastic Container Registry (Amazon ECR) unterstützt sowohl die konto- als auch die regionsübergreifende Replikation. Sie konfigurieren die Replikation in der Quellregistrierung und eine Registrierungsberechtigungsrichtlinie in der Zielregistrierung. Weitere Informationen finden Sie unter Konfigurieren der kontoübergreifenden Replikation (Amazon-ECR-Dokumentation) und Dem Root-Benutzer eines Quellkontos erlauben, alle Repositorys zu replizieren (Amazon-ECR-Dokumentation).

Amazon-EFS-Dateisysteme

Amazon Elastic File System (Amazon EFS) unterstützt die konto- und regionsübergreifende Replikation. Sie können die Replikation im Quelldateisystem konfigurieren. Weitere Informationen finden Sie unter Dateisysteme replizieren (Amazon EFS-Dokumentation).

ElastiCache Amazon-Cluster (Redis OSS)

Sie können ein Backup eines Amazon-Datenbank-Clusters ElastiCache (Redis OSS) verwenden, um ihn auf ein anderes Konto zu migrieren. Weitere Informationen finden Sie unter Was sind bewährte Methoden für die Migration meines ElastiCache (Redis OSS) -Clusters (AWS Knowledge Center).

AWS Elastic Beanstalk Umgebungen

Denn AWS Elastic Beanstalk Sie können gespeicherte Konfigurationen (Elastic Beanstalk Beanstalk-Dokumentation) verwenden, um eine Umgebung in eine andere zu migrieren. AWS-Konto Weitere Informationen finden Sie unter Wie migriere ich meine Elastic Beanstalk Beanstalk-Umgebung von einer AWS-Konto zur anderen AWS-Konto (AWS Knowledge Center).

Elastic-IP-Adressen

Sie können Elastic IP-Adressen zwischen AWS-Konten denen übertragen, die sich in derselben befinden. AWS-Region Weitere Informationen finden Sie unter Elastic-IP-Adressen übertragen (Amazon-VPC-Dokumentation).

AWS Lambda Schichten

Standardmäßig ist eine AWS Lambda Ebene, die Sie erstellen, nur für Sie reserviert AWS-Konto. Sie können die Ebene jedoch optional mit anderen teilen AWS-Konten oder sie öffentlich machen. Um eine Ebene zu kopieren, stellen Sie sie in einer anderen AWS-Konto erneut bereit. Weitere Informationen finden Sie unter Konfigurieren von Ebenenberechtigungen (Lambda-Dokumentation).

Amazon-Lightsail-Instances

Sie können einen Snapshot einer Amazon-Lightsail-Instance erstellen und den Snapshot in ein Amazon Machine Image (AMI) und einen verschlüsselten Snapshot eines Amazon-EBS-Volumes exportieren. Weitere Informationen finden Sie unter Amazon-Lightsail-Snapshots nach Amazon EC2 exportieren (Lightsail-Dokumentation). Standardmäßig wird der Snapshot mit einem verwalteten AWS-Schlüssel verschlüsselt, der in AWS Key Management Service (AWS KMS) erstellt wurde. Dieser KMS-Schlüsseltyp kann jedoch nicht gemeinsam genutzt werden AWS-Konten. Stattdessen verschlüsseln Sie manuell eine Kopie des AMI mit einem vom Kunden verwalteten Schlüssel, der vom Zielkonto aus verwendet werden kann. Weitere Informationen finden Sie unter Zulassen, dass Benutzer mit anderen Konten einen KMS-Schlüssel verwenden (AWS KMS Dokumentation). Anschließend können Sie das kopierte AMI mit dem Ziel teilen AWS-Konto und vom kopierten AMI aus eine neue EC2-Instance für Lightsail starten. Weitere Informationen finden Sie unter Starten einer Instance mit dem neuen Launch Instance Wizard (Amazon-EC2-Dokumentation).

Amazon Neptune-Cluster

Sie können einen automatisierten Snapshot des Amazon-Neptune-Datenbank-Clusters in ein anderes AWS-Konto kopieren. Weitere Informationen finden Sie unter Kopieren eines Datenbank-Cluster-Snapshots (DB) (Neptun-Dokumentation).

Sie können einen manuellen Snapshot auch mit bis zu 20 AWS-Konten teilen, die einen DB-Cluster direkt aus dem Snapshot wiederherstellen können. Weitere Informationen finden Sie unter Kopieren eines DB-Cluster-Snapshots (Neptune-Dokumentation).

Amazon OpenSearch Service-Domänen

Um Daten zwischen Amazon OpenSearch Service-Domains zu kopieren, können Sie Amazon S3 verwenden, um einen Snapshot der Quelldomain zu erstellen und den Snapshot dann in einer Zieldomain in einer anderen wiederherzustellen AWS-Konto. Weitere Informationen finden Sie unter

Wie stelle ich Daten von einer Amazon OpenSearch Service-Domain in einer anderen wieder her AWS-Konto (AWS Knowledge Center).

Wenn Sie eine Netzwerkverbindung zwischen den haben AWS-Konten, können Sie auch die Funktion zur clusterübergreifenden Replikation (OpenSearch Servicedokumentation) in OpenSearch Service verwenden.

Amazon-RDS-Snapshots

Für Amazon Relational Database Service (Amazon RDS) können Sie manuelle Snapshots von DB-Instances oder -Clustern mit bis zu 20 AWS-Konten teilen. Sie können dann die DB-Instance oder den DB-Cluster anhand des geteilten Snapshots wiederherstellen. Weitere Informationen finden Sie unter Wie teile ich manuelle Amazon RDS-DB-Snapshots oder Aurora-DB-Cluster-Snapshots mit anderen AWS-Konto (AWS Knowledge Center).

Sie können AWS Database Migration Service (AWS DMS) auch verwenden, um die kontinuierliche Replikation zwischen Datenbank-Instances in verschiedenen Konten zu konfigurieren. Dies erfordert jedoch Netzwerkkonnektivität zwischen den Konten, z. B. VPC-Peering oder ein Transit-Gateway.

Amazon-Redshift-Cluster

Um einen Amazon Redshift Redshift-Cluster auf einen anderen zu migrieren AWS-Konto, erstellen Sie einen manuellen Snapshot des Clusters im Quellkonto, teilen den Snapshot mit dem Ziel AWS-Konto und stellen dann den Cluster aus dem Snapshot wieder her. Weitere Informationen finden Sie unter Wie kopiere ich einen von Amazon Redshift bereitgestellten Cluster in einen anderen AWS-Konto (AWS Knowledge Center).

Amazon-Route-53-Domains und gehostete Zonen

Sie können Amazon-Route-53-Domains zwischen AWS-Kontenübertragen. Weitere Informationen finden Sie unter Übertragen einer Domain auf ein anderes AWS-Konto (Dokumentation zu Route 53).

Sie können eine von Route 53 gehostete Zone auch in eine andere migrieren. AWS-Konto Weitere Informationen darüber, wann dies empfohlen oder erforderlich ist, finden Sie unter Eine gehostete Zone in ein anderes AWS-Konto migrieren (Dokumentation zu Route 53). Wenn Sie eine gehostete Zone migrieren, erstellen Sie sie im Ziel- AWS-Konto neu. Eine Anleitung finden Sie unter Eine gehostete Zone in ein anderes AWS-Konto migrieren (Dokumentation zu Route 53).

Amazon-S3-Buckets

Sie können Amazon Simple Storage Service (Amazon S3) Same-Region-Replication verwenden, um Objekte zwischen S3-Buckets in derselben AWS-Region zu kopieren. Weitere Informationen finden Sie unter Objekte replizieren (Amazon-S3-Dokumentation). Beachten Sie Folgendes:

- Ändern Sie den Besitz des Replikats auf das Replikat AWS-Konto , dem der Ziel-Bucket gehört. Eine Anleitung finden Sie unter Ändern des Replikateigentümers(Amazon-S3-Dokumentation).
- Aktualisieren Sie die Bedingungen für den Bucket-Besitzer, sodass sie die AWS-Konto ID des Ziel-Buckets widerspiegeln. Weitere Informationen finden Sie unter Überprüfen der Bucket-Eigentümerschaft mit Bucket-Eigentümer-Bedingung (Amazon-S3-Dokumentation).
- Seit April 2023 ist die erzwungene Einstellung des Bucket-Besitzers für neu erstellte Buckets aktiviert, wodurch Bucket-Zugriffskontrolllisten (ACLs) und Objekte ACLs unwirksam werden. Weitere Informationen finden Sie unter Amazon S3 Security Changes Are Coming (AWS Blogbeitrag).
- Sie können S3-Batch-Replikation (Amazon-S3-Dokumentation) verwenden, um Objekte zu replizieren, die vor der Konfiguration der Replikation existierten.

SageMaker Amazon-KI-Modelle

SageMaker KI-Modelle werden während des Trainings in einem Amazon S3 S3-Bucket gespeichert. Indem Sie vom Zielkonto aus Zugriff auf den S3-Bucket gewähren, können Sie ein im Quellkonto gespeichertes Modell für das Zielkonto bereitstellen. Weitere Informationen finden Sie unter Wie kann ich ein Amazon SageMaker AI-Modell in einem anderen AWS-Konto(AWS Knowledge Center) bereitstellen.

AWS WAF Web ACLs

AWS WAF Web-Zugriffskontrolllisten (Web ACLs) müssen sich in demselben Konto befinden wie die Ressourcen, mit denen sie verknüpft sind, z. B. CloudFront Amazon-Distributionen, Application Load Balancers, Amazon API Gateway REST APIs und GraphQL. AWS AppSync APIs Sie können AWS Firewall Manager es verwenden, um das AWS WAF Web ACLs in Ihrer gesamten Organisation in AWS Organizations und zwischen Regionen zentral zu verwalten. Weitere Informationen finden Sie unter Erste Schritte mit AWS Firewall Manager-AWS WAF -Richtlinien (Dokumentation zu Firewall Manager).

Überlegungen zur Abrechnung beim Übergang zu einer Architektur mit mehreren Konten

Wenn Sie AWS Organizations für den Übergang zur Mehrfachabrechnung die Option verwenden AWS-Konten, können Sie die Funktion zur konsolidierten Fakturierung verwenden (AWS Organizations Dokumentation). Diese Funktion bietet eine einzige, kombinierte Rechnung, in der die Gebühren für mehrere Konten aufgeführt sind.

Im Folgenden finden Sie bewährte Methoden und Empfehlungen für die Abrechnung bei der Umstellung auf mehrere Konten:

- Wenn Sie Zugriff auf Ihre historischen Abrechnungsdaten benötigen, erstellen Sie, bevor Sie die Einladung zum Beitritt zu einer Organisation annehmen, einen Kosten- und Nutzungsbericht (AWS Cost and Usage Report Dokumentation), um die historischen Abrechnungsdaten des Kontos in einen Amazon Simple Storage Service (Amazon S3) -Bucket zu exportieren. Nachdem Sie die Einladung zum Beitritt zur Organisation angenommen haben, sind die historischen Abrechnungsdaten des Kontos nicht mehr zugänglich.
- Wenn Sie zwei Organisationen zusammenlegen müssen, z. B. im Rahmen einer Fusion oder Übernahme, können Sie die Kontobeurteilung für AWS Organizations (AWS Lösungsbibliothek) verwenden, um die ressourcenbasierten Richtlinien in den einzelnen Organisationen zu bewerten und mögliche Probleme zu identifizieren, bevor Sie sie kombinieren.

Schlussfolgerung

Der Übergang von einem einzelnen AWS-Konto zu mehreren Konten kann sich ohne eine Einführungsstrategie zunächst überwältigend anfühlen. Durch die Implementierung einer Strategie für mehrere Konten können Sie viele Herausforderungen bewältigen, mit denen Unternehmen konfrontiert sind, wenn sie ein einziges AWS-Konto verwenden:

- Produktionsdaten mit Entwicklungsdaten verwechseln — Sie können unterschiedliche Berechtigungen und Zugriffsrechte gewähren, indem Sie Produktions- und AWS IAM Identity Center Nicht-Produktionsorganisationseinheiten mit separaten Berechtigungssätzen verwenden. Nur Benutzer mit hohen Rechten sollten Zugriff auf die Produktionsdatenbank haben, und dieser Zugriff sollte zeitlich begrenzt sein und geprüft werden.
- Die Bereitstellung in der Produktion wirkt sich auf andere Geschäftsabläufe aus – Sie können die Stakeholder voneinander trennen, indem Sie mehrere Konten und mehrere Umgebungen verwenden. Sie könnten z. B. innerhalb eines Kontos, das nicht zur Produktion gehört, eine spezielle Demo-Umgebung für den Vertrieb einrichten, sodass Sie Bereitstellungen und Releases planen können, wenn keine Demos stattfinden.
- Geringere Leistung der Produktionsworkloads beim Testen von Entwicklungs-Workloads — Für jeden Dienst AWS-Konto gibt es unabhängige Servicequoten, die für jeden Dienst gelten. Durch die Verwendung mehrerer Konten können Sie die Auswirkungen einer Umgebung auf eine andere Umgebung begrenzen.
- Unterscheidung zwischen Produktionskosten und Entwicklungskosten – In der konsolidierten Abrechnung für die Organisation werden alle Kosten zusammengefasst auf der AWS-Konto -Ebene, sodass das Finanzteam sehen kann, wie hoch die Produktionskosten im Vergleich zu Umgebungen außerhalb der Produktion sind, wie z. B. Entwicklungs-, Test- und Demoumgebungen. Sie können auch Tags und Tagging-Richtlinien verwenden, um die Kosten innerhalb eines Kontos zu trennen.
- Beschränken Sie den Zugriff auf sensible Daten – Mit IAM Identity Center können Sie separate Zugriffsrichtlinien für eine Gruppe von Personen einrichten, die einem bestimmten Konto zugeordnet sind.
- Kostenkontrolle — Durch die Verwendung von Richtlinien zur Dienstkontrolle (SCPs) in einer Architektur mit mehreren Konten können Sie den Zugriff auf bestimmte Konten verbieten, was für Ihr AWS-Services Unternehmen zu hohen Kosten führen könnte. SCPs kann jeglichen Zugriff auf bestimmte Dienste verweigern oder die Nutzung eines Dienstes auf einen bestimmten Typ

beschränken, z. B. die Typen von Amazon Elastic Compute Cloud (Amazon EC2) -Instances einschränken, die erstellt werden können.

Mitwirkende

Zu den Mitwirkenden an diesem Dokument gehören:

- Justin Plock, Principal Solutions Architect, AWS (Hauptautor)
- Emily Arnautovic, Hauptarchitektin, AWS
- Jason DiDomenico, leitender Lösungsarchitekt, AWS
- Michael Leighty, Senior Security Specialist Solutions Architect, AWS
- Jesse Lepich, Senior Security Specialist Solutions Architect, AWS
- Rodney Lester, leitender Lösungsarchitekt, AWS
- Israel Lopez Moriano, Lösungsarchitekt, AWS
- George Rolston, leitender Lösungsarchitekt, AWS
- Alex Torres, leitender Lösungsarchitekt, AWS
- Dave Walker, Hauptarchitekt für Lösungen, AWS

Ressourcen

AWS Präskriptive Leitlinien

- AWS Sicherheitsreferenzarchitektur (SRA)AWS
- Die 10 besten Sicherheitsmethoden für die Sicherung von Backups in AWS

AWS Blog-Beiträge

- Wie die Einrichtung von IAM-Benutzern und IAM-Rollen dazu beitragen kann, Ihr Startup zu schützen
- Wie Sie es Entwicklern ermöglichen, IAM-Ressourcen zu erstellen und gleichzeitig die Sicherheit und Agilität für Ihre Organisation zu verbessern

AWS Whitepapers

- Organisieren Sie Ihre AWS Umgebung mithilfe mehrerer Konten
- Richten Sie Ihre Cloud-Grundlage ein auf AWS
- Aufbau einer skalierbaren und sicheren Multi-VPC-Netzwerkinfrastruktur AWS

AWS Codebeispiele

- Automatisieren Sie die Einrichtung von Sicherheitsservices mit AWS Control Tower (GitHub)

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
Richtlinien zur Ressourcenkontrolle	Dem Abschnitt Organisation einrichten wurden Informationen zu Richtlinien zur Ressourcenkontrolle hinzugefügt.	20. November 2024
Bewährte Methoden für zentralisierten ausgehenden Datenverkehr	Wir haben die bewährten Methoden zur Sicherung des ausgehenden Datenverkehrs aktualisiert.	6. Mai 2024
Bewährte Methoden für Organisationen	Wir haben die bewährten Methoden für das Erstellen einer Organisation in AWS Organizations aktualisiert.	4. Dezember 2023
Überlegungen zur Abrechnung	Wir haben den Abschnitt Überlegungen zur Abrechnung hinzugefügt.	20. September 2023
Ressourcenmigration, Anwendungskonnektivität und Amazon VPC Lattice	Wir haben die Abschnitte Migration von Ressourcen und Anwendungen verbinden hinzugefügt. Wir haben auch Informationen über einen neuen AWS-Service hinzugefügt, Amazon Virtual Private Cloud (Amazon VPC) Lattice.	27. April 2023

Kontoverlauf und ABAC	Wir haben den Abschnitt landing zone erstellen überarbeitet und nun Informationen darüber hinzugefügt, wie Sie sicherstellen können, dass Ihre neuen AWS-Konten Geräte über einen Nutzungsverlauf verfügen, sodass Sie sie zu Ihrer AWS Control Tower landing zone hinzufügen können. Wir haben auch den Abschnitt Hinzufügen erster Benutzer überarbeitet, um Informationen darüber hinzuzufügen, wie Sie die attributbasierte Zugriffskontrolle (ABAC) verwenden können, um die Authentifizierungsmethode von einem externen SAML-basierten IdP an AWS IAM Identity Center weiterzugeben.	06. Januar 2023
Netzwerke für ausgehenden Verkehr	Wir haben den Abschnitt Zentralisierter Ausgang überarbeitet und nun Informationen zur Verwendung der Amazon Route 53 Resolver DNS-Firewall hinzugefügt, um den ausgehenden Datenverkehr auf bestimmte Domainnamen zu beschränken.	13. Oktober 2022

Sicherheit des ausgehenden Datenverkehrs	Wir haben Bewährte Methoden zur Absicherung des ausgehenden Datenverkehrs hinzugefügt.	6. Oktober 2022
Berechtigungsgrenzen	Wir haben die Definition einer Berechtigungsgrenze verbessert und im Abschnitt Ressourcen einen neuen Link für weitere Informationen zu diesem Thema hinzugefügt.	22. September 2022
Erste Veröffentlichung	—	6. September 2022

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

Siehe 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 verarbeitet Transaktionen von verbindenden Anwendungen, 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.

maßgebliche 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 Einführung der Cloud (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 normalerweise keine Zugriffsrechte besitzt. Weitere Informationen finden Sie unter dem Indikator Implementation break-glass procedures in den AWS Well-Architected-Leitlinien.

Brownfield-Strategie

Die bestehende Infrastruktur in Ihrer Umgebung. Wenn Sie eine Brownfield-Strategie für eine Systemarchitektur anwenden, richten Sie sich bei der Gestaltung der Architektur nach den Einschränkungen der aktuellen Systeme und Infrastruktur. Wenn Sie die bestehende Infrastruktur erweitern, könnten Sie Brownfield- und Greenfield-Strategien mischen.

Puffer-Cache

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

Geschäftsfähigkeit

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

Planung der Geschäftskontinuität (BCP)

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

C

CAF

Weitere Informationen finden Sie unter Framework AWS für die 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 wird allgemein als Pipeline beschrieben. CI/CD kann Ihnen helfen, Prozesse zu automatisieren, die Produktivität zu steigern, die Codequalität zu verbessern und schneller zu liefern. Weitere Informationen finden Sie unter Vorteile der kontinuierlichen Auslieferung. CD kann auch für kontinuierliche Bereitstellung stehen. Weitere Informationen finden Sie unterKontinuierliche Auslieferung im Vergleich zu kontinuierlicher Bereitstellung.

CV

Siehe Computer Vision.

D

Daten im Ruhezustand

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

Datenklassifizierung

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

der Sicherheitssäule im AWS Well-Architected Framework. Weitere Informationen finden Sie unter Datenklassifizierung.

Datendrift

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

Daten während der Übertragung

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

Datennetz

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

Datenminimierung

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

Datenperimeter

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

Vorverarbeitung der Daten

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

Herkunft der Daten

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

betroffene Person

Eine Person, deren Daten gesammelt und verarbeitet werden.

Data Warehouse

Ein Datenverwaltungssystem, das Business Intelligence wie Analysen unterstützt. Data Warehouses enthalten in der Regel große Mengen 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.

Einsatz

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

Entwicklungsumgebung

Siehe Umgebung.

Detektivische Kontrolle

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

Abbildung des Wertstroms in der Entwicklung (DVSM)

Ein Prozess zur Identifizierung und Priorisierung von Einschränkungen, die sich negativ auf Geschwindigkeit und Qualität im Lebenszyklus der Softwareentwicklung auswirken. DVSM erweitert den Prozess der Wertstromanalyse, der ursprünglich für Lean-Manufacturing-Praktiken konzipiert wurde. Es konzentriert sich auf die Schritte und Teams, die erforderlich sind, um durch den Softwareentwicklungsprozess Mehrwert zu schaffen und zu steigern.

digitaler Zwilling

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

Maßtabelle

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

Katastrophe

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

Notfallwiederherstellung (DR)

Die Strategie und der Prozess, mit denen Sie Ausfallzeiten und Datenverluste aufgrund einer Katastrophe 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 Sicherheitsepen 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 CSPM, 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.

Daten zurückhalten

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 Infrastruktur als Code.

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

Siehe 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

Siehe Labelbasierte 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 Verfolgung, 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 Mitglied einer Organisation sein.

MES

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.

EICHE

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.

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. Diese Entität ist in der Regel ein 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 der Kontrolle entspricht, 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).

RAG

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 für die Erholungszeit.

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-Managementkonsole 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 Amazon EC2 EC2-Instance oder das Rotieren von Anmeldeinformationen.

Serverseitige Verschlüsselung

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

Service-Kontrollrichtlinie (SCP)

Eine Richtlinie, die eine zentrale 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.

Eingabeaufforderung ohne Zwischenfälle

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.