AWS Sicherheitsstandard für den Systemstart (SSB)AWS

AWS Präskriptive Leitlinien

AWS Präskriptive Leitlinien: AWS Sicherheitsstandard für den Systemstart (SSB)AWS

Table of Contents

AWS-Grundlagen für die Startup-Sicherheit. (AWS-SSB)

Jay Michael, Amazon Web Services (AWS)

Mai 2023 (Dokumentverlauf)

Die AWS Startup Security Baseline (SSB) besteht aus einer Reihe von Kontrollen, die eine Mindestgrundlage schaffen, auf der Unternehmen sicher in AWS aufbauen können, ohne ihre Agilität zu beeinträchtigen. Diese Kontrollen bilden die Grundlage für Ihre Sicherheitslage und konzentrieren sich auf die Sicherung von Anmeldeinformationen, die Bereitstellung von Protokollierung und Transparenz, die Verwaltung von Kontaktinformationen und die Implementierung grundlegender Datengrenzen.

Die Kontrollen in diesem Leitfaden wurden für frühe Startups konzipiert und minimieren die häufigsten Sicherheitsrisiken ohne großen Aufwand. Viele Startups beginnen ihren Weg in die AWS Cloud mit einem einzigen AWS-Konto. Wenn Organisationen wachsen, migrieren sie zu Architekturen mit mehreren Konten. Die Anleitungen in diesem Leitfaden sind für Einzelkontenarchitekturen konzipiert, helfen Ihnen jedoch bei der Einrichtung von Sicherheitskontrollen, die bei der Umstellung auf eine Architektur mit mehreren Konten einfach migriert oder geändert werden können.

Die Kontrollen in AWS SSB sind in zwei Kategorien unterteilt: Konto und Workload. Kontokontrollen tragen dazu bei, Ihr AWS Konto sicher zu halten. Es enthält Empfehlungen zur Einrichtung von Benutzerzugriffen, Richtlinien und Berechtigungen sowie Empfehlungen, wie Sie Ihr Konto auf unbefugte oder potenziell bösartige Aktivitäten überwachen können. Workload-Kontrollen helfen dabei, Ihre Ressourcen und Ihren Code in der Cloud zu sichern, z. B. Anwendungen, Backend-Prozesse und Daten. Es enthält Empfehlungen wie Verschlüsselung und Reduzierung des Zugriffsumfangs.

> **Note**
>
> Einige der in diesem Handbuch empfohlenen Steuerelemente ersetzen die bei der Ersteinrichtung konfigurierten Standardeinstellungen, während die meisten neue Einstellungen und Richtlinien konfigurieren. Dieses Dokument sollte in keiner Weise als umfassend betrachtet werden, wenn es um alle verfügbaren Kontrollen geht.

Zielgruppe

Dieser Leitfaden eignet sich am besten für Startups, die sich in der Anfangsphase der Entwicklung befinden und nur wenig Personal und Betrieb haben.

Startups oder andere Unternehmen, die sich in einer späteren Betriebs- und Wachstumsphase befinden, können immer noch erheblichen Nutzen daraus ziehen, diese Kontrollen anhand ihrer derzeitigen Praktiken zu überprüfen. Wenn Sie Lücken feststellen, können Sie die einzelnen Kontrollen in diesem Leitfaden implementieren und sie dann auf ihre Eignung als langfristige Lösung prüfen.

> **Note**
>
> Die in diesem Leitfaden empfohlenen Kontrollen sind grundlegender Natur. Startups oder andere Unternehmen, die in einer späteren Größenordnung oder Raffinesse tätig sind, sollten gegebenenfalls zusätzliche Kontrollen hinzufügen.

Grundlegender Rahmen und Sicherheitsaufgaben

Das AWS Well-Architected Framework hilft Cloud-Architekten beim Aufbau einer sicheren, leistungsstarken, belastbaren und effizienten Infrastruktur für ihre Anwendungen und Workloads. Die AWS Startup Security Baseline entspricht der Sicherheitssäule des AWS Well-Architected Framework. Die Sicherheitssäule beschreibt, wie Sie Cloud-Technologien nutzen können, um Daten, Systeme und Komponenten so zu schützen, dass Ihre Sicherheitslage verbessert werden kann. Dies hilft Ihnen, Ihre geschäftlichen und regulatorischen Anforderungen zu erfüllen, indem Sie die aktuellen AWS-Empfehlungen befolgen.

Sie können überprüfen, ob Sie die bewährte Methoden von Well-Architected einhalten, indem Sie den AWS Well-Architected Tool in Ihrem AWS-Konto verwenden.

Sicherheit und Compliance stellen eine übergreifende Verantwortlichkeit zwischen AWS und dem Kunden dar. Das Modell der geteilten Verantwortung wird oft so beschrieben, dass AWS zuständig ist für die Sicherheit der Cloud (das heißt für den Schutz der Infrastruktur, die alle in der Cloud angebotenen Services in der AWS Cloud ausführt), und Sie sind verantwortlich für die Sicherheit in der Cloud (je nach den von Ihnen gewählten AWS Cloud-Services). Beim Modell der geteilten Verantwortung fällt die Implementierung der Sicherheitskontrollen in diesem Dokument in Ihre Verantwortung als Kunde.

Ihr Konto sichern

Die Kontrollen und Empfehlungen in diesem Abschnitt tragen dazu bei, Ihr AWS Konto zu schützen. Es legt Wert auf die Verwendung von AWS Identity and Access Management (IAM)-Benutzern, -Gruppen und -Rollen (auch als Prinzipale bezeichnet) sowohl für den menschlichen als auch für den maschinellen Zugriff, wodurch die Verwendung des Root-Benutzers eingeschränkt wird und eine Multi-Faktor-Authentifizierung erforderlich ist. In diesem Abschnitt bestätigen Sie, dass über die Kontaktinformationen AWS verfügt, die Sie in Bezug auf Ihre Kontoaktivität und Ihren Status erreichen müssen. Sie richten auch Überwachungsservices wie AWS Trusted Advisor, Amazon und ein AWS Budgets, damit Sie über Aktivitäten in Ihrem Konto informiert werden und schnell reagieren können GuardDuty, wenn die Aktivität nicht autorisiert oder unerwartet ist.

In diesem Abschnitt werden folgende Themen behandelt:

- ACCT.01 – Einrichten der Kontakte auf Kontoebene zu gültigen E-Mail-Verteilerlisten
- ACCT.02 – Beschränken der Verwendung des Root-Benutzers
- ACCT.03 – Konfigurieren des Konsolenzugriffs für jeden Benutzer
- ACCT.04 – Berechtigungen zuweisen
- ACCT.05 – Für die Anmeldung ist eine Multi-Faktor-Authentifizierung (MFA) erforderlich
- ACCT.06 – Eine Passwortrichtlinie durchsetzen
- ACCT.07 – Bereitstellen von CloudTrail Protokollen an einen geschützten S3-Bucket
- ACCT.08 – Verhindern von öffentlichem Zugriff auf private S3-Buckets
- ACCT.09 – Löschen ungenutzter VPCs, Subnetze und Sicherheitsgruppen
- ACCT.10 – Konfigurieren von AWS Budgets zur Überwachung Ihrer Ausgaben
- ACCT.11 – Aktivieren und Beantworten von GuardDuty Benachrichtigungen
- ACCT.12 – Suchen Sie nach Problemen mit hohem Risiko und lösen Sie diese, indem Sie Trusted Advisor verwenden

ACCT.01 – Einrichten der Kontakte auf Kontoebene zu gültigen E-Mail-Verteilerlisten

Wenn Sie primäre und alternative Kontakte für Ihr AWS Konto einrichten, verwenden Sie eine E-Mail-Verteilerliste anstelle der E-Mail-Adresse einer Person. Durch die Verwendung einer E-Mail-Verteilerliste wird sichergestellt, dass Eigentum und Erreichbarkeit gewahrt bleiben, auch wenn

einzelne Personen in Ihrer Organisation kommen und gehen. Richten Sie alternative Kontakte für Fakturierungs-, Betriebs- und Sicherheitsbenachrichtigungen ein und verwenden Sie entsprechende E-Mail-Verteilerlisten. AWS verwendet diese E-Mail-Adressen, um Sie zu kontaktieren. Daher ist es wichtig, dass Sie weiterhin Zugriff auf sie haben.

Bearbeiten des Kontonamens, des Passworts des Root-Benutzers des und der E-Mail-Adresse des Stammbenutzers des

1. Melden Sie sich auf der Kontoeinstellungen-Seite in der Rechnungs– und Kostenverwaltungskonsole unter https://console.aws.amazon.com/billing/home?#/account an.
2. Klicken Sie auf der Seite Kontoeinstellungen neben Kontoeinstellungen auf Bearbeiten.
3. Wählen Sie Bearbeiten neben dem Feld aus, das Sie aktualisieren möchten.
4. Nachdem Sie Ihre Änderungen eingegeben haben, wählen Sie Änderungen speichern aus.
5. Nachdem Sie alle Änderungen durchgeführt haben, wählen Sie Fertig aus.

Ihre Kontaktinformationen bearbeiten

1. Auf der Kontoeinstellungen-Seite, unter Kontaktinformationen wählen Sie Bearbeiten.
2. Geben Sie in jedes Feld, das Sie ändern möchten, Ihre aktualisierten Daten ein und wählen Sie anschließend Aktualisieren aus.

Alternative Kontakte hinzufügen, aktualisieren oder entfernen

1. Auf der Kontoeinstellungen-Seite, unter Alternative Kontakte wählen Sie Bearbeiten.
2. Geben Sie in jedes Feld, das Sie ändern möchten, Ihre aktualisierten Daten ein und wählen Sie anschließend Aktualisieren aus.

ACCT.02 – Beschränken der Verwendung des Root-Benutzers

Der Root-Benutzer wird erstellt, wenn Sie sich für ein - AWS Konto registrieren, und dieser Benutzer verfügt über vollständige Eigentumsrechte und Berechtigungen für das Konto, die nicht geändert werden können. Verwenden Sie den Root-Benutzer nur für spezifische Aufgaben, die ihn erfordern. Weitere Informationen finden Sie unter Aufgaben, die die Anmeldeinformationen des Root-Benutzers erfordern (AWS Account Management). Führen Sie alle anderen Aktionen in Ihrem Konto durch, indem Sie andere Typen von IAM-Identitäten verwenden, z. B. Verbundbenutzer mit IAM-Rollen. Weitere Informationen finden Sie unterAWS -Sicherheitsanmeldedaten (IAM-Dokumentation).

Wie die Verwendung des Root-Benutzers beschränkt wird

1. Erfordern Sie die Multi-Faktor-Authentifizierung (MFA) für den Root-Benutzer an, wie unter ACCT.05 – Für die Anmeldung ist eine Multi-Faktor-Authentifizierung (MFA) erforderlich beschrieben.
2. Erstellen Sie einen Administrator, damit Sie für alltägliche Aufgaben nicht auf den Root-Benutzer zurückgreifen müssen. Weitere Informationen zur Konfiguration des Benutzerzugriffs finden Sie unter ACCT.03 – Konfigurieren des Konsolenzugriffs für jeden Benutzer.

ACCT.03 – Konfigurieren des Konsolenzugriffs für jeden Benutzer

Als bewährte Methode AWS empfiehlt die Verwendung temporärer Anmeldeinformationen, um Zugriff auf - AWS-Konten und -Ressourcen zu gewähren. Temporäre Anmeldeinformationen haben eine begrenzte Nutzungsdauer. Somit müssen Sie sie nicht rotieren oder explizit widerrufen, wenn Sie sie nicht mehr benötigen. Weitere Informationen finden Sie unter Temporäre Sicherheits-Anmeldeinformationen (IAM-Dokumentation).

Für menschliche Benutzer AWS empfiehlt die Verwendung von Verbundidentitäten von einem zentralen Identitätsanbieter (IdP), wie AWS IAM Identity Center, Okta, Active Directory oder Ping Identity. Durch den Verbund von Benutzern können Sie Identitäten an einem einzigen zentralen Ort definieren, und Benutzer können sich sicher bei mehreren Anwendungen und Websites authentifizieren, einschließlich AWS, indem sie nur einen Satz von Anmeldeinformationen verwenden. Weitere Informationen finden Sie unter Identitätsverbund in AWS und IAM Identity Center (AWS Website).

> **Note**
>
> Ein Identitätsverbund kann den Übergang von einer Einzelkontenarchitektur zu einer Architektur mit mehreren Konten erschweren. Es ist üblich, dass Startups die Implementierung eines Identitätsverbunds verzögern, bis sie eine Architektur mit mehreren Konten eingerichtet haben, die in AWS Organizations verwaltet wird.

So richten Sie einen Identitätsverbund ein

1. Wenn Sie IAM Identity Center verwenden, schauen Sie unter Erste Schritte (Dokumentation von IAM Identity Center).

Wenn Sie einen externen IdP oder einen Drittanbieter verwenden, finden Sie weitere Informationen unter Erstellen von IAM-Identitätsanbietern (IAM-Dokumentation).

2. Stellen Sie sicher, dass Ihr IdP die Multi-Faktor-Authentifizierung (MFA) durchsetzt.
3. Wenden Sie Berechtigungen gemäß ACCT.04 – Berechtigungen zuweisen an.

Für Startups, die nicht bereit sind, einen Identitätsverbund zu konfigurieren, können Sie Benutzer direkt in IAM erstellen. Dies ist keine empfohlene bewährte Sicherheitsmethode, da es sich um langfristige Anmeldeinformationen handelt, die nie ablaufen. Dies ist jedoch eine gängige Praxis für Startups, die sich in der Anfangsphase befinden, um Schwierigkeiten beim Übergang zu einer Architektur mit mehreren Konten zu vermeiden, wenn sie betriebsbereit sind.

Als Grundlage können Sie einen IAM-Benutzer für jede Person erstellen, die Zugriff auf AWS Management Console benötigt. Wenn Sie IAM-Benutzer konfigurieren, teilen Sie die Anmeldeinformationen nicht mit anderen Benutzern und rotieren Sie die langfristigen Anmeldeinformationen regelmäßig.

> ⚠ Warning
>
> IAM-Benutzer verfügen über langfristige Anmeldeinformationen, was ein Sicherheitsrisiko darstellt. Um dieses Risiko zu minimieren, empfehlen wir, dass Sie diesen Benutzern nur die Berechtigungen gewähren, die sie zur Ausführung der Aufgabe benötigen, und dass Sie diese Benutzer entfernen, wenn sie nicht mehr benötigt werden.

So erstellen Sie einen IAM-Benutzer

1. IAM-Benutzer erstellen (IAM-Dokumentation).
2. Wenden Sie Berechtigungen gemäß ACCT.04 – Berechtigungen zuweisen an.

ACCT.04 – Berechtigungen zuweisen

Konfigurieren Sie Benutzerberechtigungen im Konto, indem Sie Richtlinien zu ihrer IAM-Identität (Benutzergruppe oder Rolle) zuweisen. Sie können die Berechtigungen anpassen oder AWS verwaltete Richtlinien anfügen. Dabei handelt es sich um eigenständige Richtlinien, die von entwickelt wurden, AWS um Berechtigungen für viele häufige Anwendungsfälle bereitzustellen. Wenn Sie Berechtigungen anpassen, befolgen Sie die bewährten Sicherheitsmethoden von Gewährung der

geringsten Berechtigung. Geringste Berechtigung ist die Praxis, jedem Benutzer das Minimum an Berechtigungen zu gewähren, das er zur Ausführung seiner Aufgaben benötigt.

Wenn Sie verbundene Identitäten verwenden, greifen Benutzer auf das Konto zu, indem sie über den externen Identitätsanbieter eine IAM-Rolle übernehmen. Die IAM-Rolle definiert, welche Aktionen Benutzer, die vom IdP Ihrer Organisation authentifiziert wurden, in ausführen dürfen AWS. Sie wenden benutzerdefinierte oder AWS verwaltete Richtlinien auf diese Rolle an, um Berechtigungen zu konfigurieren.

Berechtigungen für verbundene Identitäten zuweisen

- Wenn Sie IAM Identity Center verwenden, lesen Sie Verwenden Sie IAM-Richtlinien in Berechtigungssätzen (Dokumentation von IAM Identity Center).

  Wenn Sie einen externen IdP oder einen Drittanbieter verwenden, lesen Sie Hinzufügen von IAM-Identitätsberechtigungen (IAM-Dokumentation).

Wenn Sie IAM-Benutzer verwenden, können Sie Benutzergruppen oder Rollen verwenden, um die Berechtigungen für mehrere IAM-Benutzer zu verwalten. Wir empfehlen Benutzergruppen für Startups, da sie einfacher zu verwalten sind und weniger anfällig für Fehlkonfigurationen sind, welche ein Sicherheitsrisiko für Ihr Konto darstellen könnten. Weisen Sie Benutzer zu Benutzergruppen zu, die ihren Aufgaben entsprechen. Beispiele für Benutzergruppen sind Anwendungs-, Daten-, Netzwerk- und Entwicklungsbetrieb (DevOps)-Techniker. Sie können die Benutzertypen auch je nach Entscheidungsbefugnis in kleinere Benutzergruppen unterteilen, z. B. für erfahrene oder nicht erfahrene Techniker.

Zuweisen von Berechtigungen für IAM-Benutzer

1. IAM-Benutzergruppen erstellen (IAM-Dokumentation).
2. Fügen Sie eine von AWS verwaltete Richtlinie an eine IAM-Benutzergruppe an (IAM-Dokumentation).

ACCT.05 – Für die Anmeldung ist eine Multi-Faktor-Authentifizierung (MFA) erforderlich

Mit MFA verfügen Benutzer über ein System, das eine Antwort auf eine Authentifizierungsaufgabe generiert. Die Anmeldeinformationen und die vom Gerät generierte Antwort jedes Benutzers

sind erforderlich, um den Anmeldevorgang abzuschließen. Aktivieren Sie als bewährte Sicherheitsmethode MFA für den AWS-Konto Zugriff, insbesondere für langfristige Anmeldeinformationen wie den Stammbenutzer des -Kontos und IAM-Benutzer.

So richten Sie MFA für den Root-Benutzer ein

1. Melden Sie sich bei der AWS Management Console unter anhttps://console.aws.amazon.com/.
2. Klicken Sie rechts in der Navigationsleiste auf den Kontonamen und wählen Sie dann Meine Sicherheitsanmeldeinformationen.
3. Sofern erforderlich, wählen Sie Continue to Security Credentials (Weiter zu Sicherheitsanmeldeinformationen).
4. Erweitern Sie den Bereich Multi-Factor Authentication (MFA) (Multifaktor-Authentifizierung).
5. Wählen Sie Activate MFA (MFA aktivieren).
6. Folgen Sie den Anweisungen des Assistenten, um Ihre MFA-Geräte entsprechend zu konfigurieren. Weitere Informationen finden Sie unter Aktivieren von MFA-Geräten für Benutzer in AWS (IAM-Dokumentation).

So richten Sie MFA im IAM Identity Center ein

- MFA aktivieren (Dokumentation zu IAM Identity Center)

So richten Sie MFA für Ihren eigenen IAM-Benutzer ein

1. Melden Sie sich mit Ihren IAM-Anmeldeinformationen bei der IAM-Konsole in https://console.aws.amazon.com/iam an.
2. Wählen Sie auf der Navigationsleiste rechts oben Ihren Benutzernamen und dann My Security Credentials (Meine Sicherheitsanmeldeinformationen).
3. Klicken Sie auf der AWS IAM-Anmeldeinformationen auf der Registerkarte Multifaktor-Authentifizierung wählen Sie im Abschnitt Verwalten von MFA Geräten.

So richten Sie MFA für IAM-Benutzer ein

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam.
2. Klicken Sie im Navigationsbereich auf Users (Benutzer).

3. Wählen Sie zuerst den Namen des Benutzers, für den Sie MFA aktivieren möchten, und dann die Registerkarte Security Credentials (Sicherheitsanmeldeinformationen).
4. Wählen Sie neben Assigned MFA device (Zugeordnetes MFA-Gerät) die Option Manage (Verwalten).
5. Folgen Sie den Anweisungen des Assistenten, um Ihre MFA-Geräte entsprechend zu konfigurieren. Weitere Informationen finden Sie unter Aktivieren von MFA-Geräten für Benutzer in AWS (IAM-Dokumentation).

ACCT.06 – Eine Passwortrichtlinie durchsetzen

Benutzer melden sich bei der an, AWS Management Console indem sie Anmeldeinformationen angeben, und MFA wird empfohlen. Erfordern Sie, dass Passwörter einer strengen Passwortrichtlinie entsprechen, um zu verhindern, dass Passwörter durch Brute-Force oder Social Engineering aufgedeckt werden.

Weitere Informationen zu den neuesten Empfehlungen für sichere Kennwörter finden Sie unter Leitfaden zu den Passwortrichtlinien auf der Website des Center for Internet Security (CIS).

Für IAM-Benutzer können Sie die Kennwortanforderungen in einer benutzerdefinierten IAM-Passwortrichtlinie konfigurieren. Weitere Informationen finden Sie unter Einrichten einer Kontopasswortrichtlinie (IAM-Dokumentation).

So erstellen Sie eine benutzerdefinierte Passwortrichtlinie

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam.
2. Wählen Sie im Navigationsbereich Account Settings (Kontoeinstellungen).
3. Klicken Sie im Abschnitt Passwortrichtlinie auf Passwortrichtlinie ändern.
4. Wählen Sie die Optionen aus, die Sie auf Ihre Passwortrichtlinie anwenden möchten, und wählen Sie dann Änderungen speichern.

ACCT.07 – Bereitstellen von CloudTrail Protokollen an einen geschützten S3-Bucket

Aktionen von Benutzern, Rollen und Services in Ihrem AWS Konto werden als Ereignisse in aufgezeichnet AWS CloudTrail. CloudTrail ist standardmäßig aktiviert und in der CloudTrail Konsole

können Sie auf Informationen zum Ereignisverlauf von 90 Tagen zugreifen. Informationen zum Anzeigen, Suchen, Herunterladen, Archivieren, Analysieren und Beantworten von Kontoaktivitäten in Ihrer gesamten AWS Infrastruktur finden Sie unter Anzeigen von Ereignissen mit CloudTrail Ereignisverlauf (CloudTrail Dokumentation).

Um den CloudTrail Verlauf mit zusätzlichen Daten über 90 Tage hinaus beizubehalten, erstellen Sie einen neuen Trail, der Protokolldateien an einen Amazon Simple Storage Service (Amazon S3)-Bucket für alle Ereignistypen liefert. Wenn Sie einen Trail in der CloudTrail Konsole erstellen, erstellen Sie einen multiregionalen Trail.

So erstellen Sie einen Trail, der Protokolle für alle AWS-Regionen an einen S3-Bucket übermittelt

1. Erstellen Sie einen Trail (CloudTrail Dokumentation). Führen Sie auf der Seite Protokollereignisse wählen die folgenden Schritte aus:

    a. Für API-Aktivität wählen Sie Lesen und Schreiben aus.

    b. Wählen Sie für Vorproduktionsumgebungen AWS KMS -Ereignisse ausschließen aus. Dies schließt alle AWS Key Management Service (AWS KMS)-Ereignisse aus Ihrem Trail aus. AWS KMS Leseaktionen wie `EncryptDecrypt`, und `GenerateDataKey` können eine große Anzahl von Ereignissen generieren.

    Wählen Sie für Produktionsumgebungen die Option Protokollierung von Schreiben-Verwaltungsereignissen und das Kontrollkästchen für Ausschließen von AWS KMS -Ereignissen aus. Dies schließt AWS KMS Leseereignisse mit hohem Volumen aus`Disable`, protokolliert aber dennoch relevante Schreibereignisse wie `Delete`, und `ScheduleKey`. Dies sind die empfohlenen AWS KMS Mindestprotokollierungseinstellungen für eine Produktionsumgebung.
2. Der neue Trail wird auf der Seite Trails angezeigt. In etwa 15 Minuten CloudTrail veröffentlicht Protokolldateien, die die AWS API-Aufrufe (Application Programming Interface) in Ihrem Konto anzeigen. Sie können die Protokolldateien in dem von Ihnen angegebenen S3-Bucket anzeigen.

So sichern Sie die S3-Buckets, in denen Sie CloudTrail Protokolldateien speichern

1. Überprüfen Sie die Amazon S3-Bucket-Richtlinie (CloudTrail Dokumentation) für alle Buckets, in denen Sie Protokolldateien speichern, und passen Sie sie nach Bedarf an, um unnötigen Zugriff zu entfernen.
2. Als bewährte Sicherheitsmethode gilt es, der Bucket-Richtlinie manuell einen`aws:SourceArn`-Bedingungsschlüssel hinzuzufügen. Weitere Informationen finden Sie unter Erstellen oder

Aktualisieren eines Amazon S3-Buckets zum Speichern der Protokolldateien für einen Organisations-Trail (CloudTrail Dokumentation).

3. MFA Delete aktivieren (Amazon-S3-Dokumentation).

ACCT.08 – Verhindern von öffentlichem Zugriff auf private S3-Buckets

Standardmäßig verfügen nur der Root-Benutzer des AWS-Konto und der IAM-Prinzipal, falls verwendet, über Lese- und Schreibberechtigungen für Amazon S3-Buckets, die von diesem Prinzipal erstellt wurden. Zusätzliche IAM-Prinzipale erhalten Zugriff mithilfe identitätsbasierter Richtlinien, und die Zugriffsbedingungen können mithilfe einer Bucket-Richtlinie durchgesetzt werden. Sie können Bucket-Richtlinien erstellen, die der generell öffentlichen Zugriff auf den Bucket gewähren, ein öffentlicher Bucket.

Buckets, die am oder nach dem 28. April 2023 erstellt wurden, haben die Einstellung Öffentlichen Zugriff blockieren standardmäßig aktiviert. Bei Buckets, die vor diesem Datum erstellt wurden, können Benutzer die Bucket-Richtlinie falsch konfigurieren und der Öffentlichkeit unbeabsichtigt Zugriff gewähren. Sie können diese Fehlkonfiguration verhindern, indem Sie die Einstellung Öffentlichen Zugriff blockieren für jeden Bucket aktivieren. Wenn Sie keine aktuellen oder zukünftigen Anwendungsfälle für einen öffentlichen S3-Bucket haben, aktivieren Sie diese Einstellung auf der -AWS-Konto Ebene. Diese Einstellung verhindert Richtlinien, die den öffentlichen Zugriff ermöglichen.

Den öffentlichen Zugriff auf S3-Buckets zu verhindern

- Konfigurieren Sie die Einstellungen zum Blockieren des öffentlichen Zugriffs zu Amazon-S3-Buckets (Amazon-S3-Dokumentation).

AWS Trusted Advisor generiert eine gelbe Erkenntnis für S3-Buckets, die Listen- oder Lesezugriff für die Öffentlichkeit ermöglichen, und generiert eine rote Erkenntnis für Buckets, die öffentliche Uploads oder Löschungen erlauben. Folgen Sie als Ausgangsbasis der Steuerung ACCT.12 – Suchen Sie nach Problemen mit hohem Risiko und lösen Sie diese, indem Sie Trusted Advisor verwenden, um falsch konfigurierte Buckets zu identifizieren und zu korrigieren. Öffentlich zugängliche S3-Buckets werden auch in der Amazon-S3-Konsole angezeigt.

ACCT.09 – Löschen ungenutzter VPCs, Subnetze und Sicherheitsgruppen

Um das Risiko von Sicherheitsproblemen zu verringern, löschen oder deaktivieren Sie alle Ressourcen, die nicht verwendet werden. In einem neuen AWS Konto wird standardmäßig automatisch in jeder eine Virtual Private Cloud (VPC) erstellt AWS-Region, mit der Sie öffentliche IP-Adressen in öffentlichen Subnetzen zuweisen können. Wenn diese VPCs jedoch nicht benötigt werden, besteht das Risiko einer unbeabsichtigten Gefährdung von Ressourcen.

Wenn sie nicht verwendet werden, löschen Sie die Standard-VPCs in allen Regionen, nicht nur in den Regionen, in denen Sie möglicherweise Workloads bereitstellen. Beim Löschen einer VPC werden auch ihre Komponenten wie Subnetze und Sicherheitsgruppen gelöscht.

> **Note**
>
> Sie können alle Regionen und VPCs in der Konsole Amazon EC2 Global View unter https://console.aws.amazon.com/ec2globalview/home anzeigen. Weitere Informationen finden Sie unter Auflisten und Filtern von Ressourcen in verschiedenen Regionen mithilfe von Amazon EC2 Global View (Amazon-EC2-Dokumentation).

Ungenutzte Standard-VPCs löschen

1. Löschen Ihrer VPC (Amazon-PC-Dokumentation).
2. Wiederholen Sie dies bei Bedarf für VPCs in anderen Regionen.

ACCT.10 – Konfigurieren von AWS Budgets zur Überwachung Ihrer Ausgaben

AWS Budgets ermöglichen die Überwachung der monatlichen Kosten und der Nutzung mit Benachrichtigungen, wenn die Kosten voraussichtlich die Zielschwellenwerte überschreiten. Benachrichtigungen über prognostizierte Kosten können auf unerwartete Aktivitäten hinweisen und zusätzlich zu anderen Überwachungssystemen wie AWS Trusted Advisor und Amazon zusätzliche Verteidigung bieten GuardDuty. Die Überwachung und das Verständnis Ihrer AWS -Kosten ist auch Teil einer guten Betriebsunterbrechung.

So richten Sie ein Budget in ein AWS Budgets

- Erstellen Sie ein Kostenbudget (AWS Budgets Dokumentation).

ACCT.11 – Aktivieren und Beantworten von GuardDuty Benachrichtigungen

Amazon GuardDuty ist ein Service zur Erkennung von Bedrohungen, der kontinuierlich auf böswilliges oder unbefugtes Verhalten überwacht, um Ihre AWS Konten, Workloads und Daten zu schützen. Wenn unerwartete und potenziell bösartige Aktivitäten erkannt werden, GuardDuty liefert detaillierte Sicherheitserkenntnisse für Transparenz und Abhilfe. GuardDuty kann Bedrohungen wie Kryptowährungs-Mining-Aktivitäten, Zugriff von Tor-Clients und -Relays, unerwartetes Verhalten und kompromittierte IAM-Anmeldeinformationen erkennen. Aktivieren GuardDuty und reagieren Sie auf Erkenntnisse, um potenziell böswilliges oder unbefugtes Verhalten in Ihrer - AWS Umgebung zu verhindern. Weitere Informationen zu den GuardDutyErkenntnissen in finden Sie unter Erkenntnistypen (GuardDuty Dokumentation).

Sie können Amazon CloudWatch Events verwenden, um automatisierte Benachrichtigungen einzurichten, wenn ein Ergebnis GuardDuty erstellt oder sich das Ergebnis ändert. Zunächst richten Sie ein Amazon Simple Notification Service (Amazon SNS)-Thema ein und fügen dem Thema Endpunkte oder E-Mail-Adressen hinzu. Anschließend richten Sie ein CloudWatch Ereignis für GuardDuty Erkenntnisse ein und die Ereignisregel benachrichtigt die Endpunkte im Amazon SNS-Thema.

So aktivieren Sie - GuardDuty und - GuardDuty Benachrichtigungen

1. Aktivieren Sie Amazon GuardDuty (GuardDuty Dokumentation).
2. Erstellen Sie eine CloudWatch Ereignisregel, um Sie über GuardDuty Erkenntnisse zu informieren (GuardDuty-Dokumentation).

ACCT.12 – Suchen Sie nach Problemen mit hohem Risiko und lösen Sie diese, indem Sie Trusted Advisor verwenden

AWS Trusted Advisor scannt passiv Ihre AWS Infrastruktur auf Probleme mit hohem Risiko oder hohen Auswirkungen im Zusammenhang mit Sicherheit, Leistung, Kosten und Zuverlässigkeit. Es bietet detaillierte Informationen zu den betroffenen Ressourcen und Empfehlungen zur Abhilfe.

Eine vollständige Liste der Prüfungen und Beschreibungen finden Sie in der -AWS Trusted Advisor Prüfungsreferenz (Trusted Advisor Dokumentation).

Überprüfen Sie die Trusted Advisor Ergebnisse regelmäßig und beheben Sie Probleme nach Bedarf. Wenn Sie über die AWS Business Support- oder Enterprise Support-Pläne verfügen, können Sie eine wöchentliche E-Mail mit den Erkenntnissen abonnieren. Weitere Informationen finden Sie unter Einrichten von Benachrichtigungseinstellungen (AWS Support -Dokumentation).

So zeigen Sie Probleme in an Trusted Advisor

- Überprüfen Sie jede Prüfungskategorie gemäß den Anweisungen unter Prüfungskategorien anzeigen (AWS Support Dokumentation). Wir empfehlen mindestens die Überprüfung der Probleme Maßnahme empfohlen, welche rot sind.

Ihren Workload absichern

Die Kontrollen und Empfehlungen in diesem Abschnitt helfen Ihnen dabei, Ihre Workloads zu schützen, die in AWS ausgeführt werden, während Sie sie erstellen. Sie legen Wert auf sichere Verfahren zur Verwaltung von Anwendungsgeheimnissen und Zugriffsumfang, zur Minimierung der Zugriffswege zu privaten Ressourcen und zum Schutz von Daten während der Übertragung und Speicherung von Daten mithilfe von Verschlüsselung.

In diesem Abschnitt werden folgende Themen beschrieben:

- WKLD.01 – Verwenden Sie IAM-Rollen für Berechtigungen in der Datenverarbeitungsumgebung
- WKLD.02 – Beschränken des Umfangs der Nutzung von Anmeldeinformationen mit ressourcenbasierten Richtlinienberechtigungen
- WKLD.03 – Verwenden Sie kurzlebige Geheimnisse oder einen Geheimnisverwaltungsservice
- WKLD.04 – Verhindern Sie, dass Anwendungsgeheimnisse offengelegt werden
- WKLD.05 – Enthüllte Geheimnisse erkennen und korrigieren
- WKLD.06 – Verwenden Sie Systems Manager anstelle von SSH oder RDP
- WKLD.07 – Protokollieren Sie Datenereignisse für S3-Buckets mit sensiblen Daten
- WKLD.08 – Amazon-EBS-Volumes verschlüsseln
- WKLD.09 – Verschlüsseln Sie Amazon-RDS-Datenbanken
- WKLD.10 – Bereitstellen von privaten Ressourcen in privaten Subnetzen
- WKLD.11 – Den Netzwerkzugriff mithilfe von Sicherheitsgruppen beschränken
- WKLD.12 – Verwenden von VPC-Endpunkten, um auf unterstützte Services zuzugreifen
- WKLD.13 – HTTPS für alle öffentlichen Web-Endpunkte erfordern
- WKLD.14 – Verwenden Sie Edge-Protection-Services für öffentliche Endpunkte
- WKLD.15 – Definieren von Sicherheitskontrollen in Vorlagen und Implementierung mithilfe von CI/CD-Methoden

WKLD.01 – Verwenden Sie IAM-Rollen für Berechtigungen in der Datenverarbeitungsumgebung

In AWS Identity and Access Management(IAM) steht eine Rolle für eine Reihe von Berechtigungen, die von einer Person oder einem Service für einen konfigurierbaren Zeitraum übernommen

werden können. Durch die Verwendung von Rollen entfällt die Notwendigkeit, langfristige Anmeldeinformationen zu speichern oder zu verwalten, wodurch die Wahrscheinlichkeit einer unbeabsichtigten Verwendung erheblich reduziert wird. Weisen Sie Amazon Elastic Compute Cloud (Amazon EC2)-Instances, AWS Fargate-Aufgaben und Services, AWS Lambda-Funktionen und anderen AWS-Datenverarbeitungsservices, sofern sie unterstützt werden, direkt eine IAM-Rolle zu. Anwendungen, die ein AWS-SDK verwenden und Ausführung in diesen Datenverarbeitungsumgebungen verwenden automatisch die IAM-Rollen-Anmeldeinformationen für die Authentifizierung.

Die Vorgehensweise und Anweisungen zur Verwendung von IAM-Rollen für die einzelnen Services finden Sie in der AWS-Dokumentation für den Service. Sehen Sie sich zum Beispiel Folgendes an:

- IAM-Rollen für Amazon EC2 (Amazon-EC2-Dokumentation)
- IAM-Rollen für Aufgaben (Dokumentation für Amazon Elastic Container Service)
- Lambda-Ausführungsrolle (Lambda-Dokumentation)

WKLD.02 – Beschränken des Umfangs der Nutzung von Anmeldeinformationen mit ressourcenbasierten Richtlinienberechtigungen

Richtlinien sind Objekte, mit denen Berechtigungen definiert oder Zugriffsbedingungen festgelegt werden können. Es gibt zwei primäre Typen von Richtlinien:

- Identitätsbasierte Richtlinien sind den Prinzipalen zugeordnet und definieren, welche Rechte der Prinzipal in der AWS-Umgebung hat.
- Ressourcenbasierte Richtlinien sind mit einer Ressource wie einem Amazon Simple Storage Service (Amazon S3)-Bucket oder einem Virtual Private Cloud (VPC)-Endpunkt verknüpft. Diese Richtlinien legen fest, welchen Prinzipalen der Zugriff gewährt wird, welche Aktionen unterstützt werden und welche anderen Bedingungen erfüllt sein müssen.

Damit einem Prinzipal Zugriff gewährt werden kann, um eine Aktion gegen eine Ressource durchzuführen, muss er in seiner identitätsbasierten Richtlinie über eine entsprechende Genehmigung verfügen und die Bedingungen der ressourcenbasierten Richtlinie erfüllen. Weitere Informationen finden Sie unter Identitätsbasierte Richtlinien und ressourcenbasierte Richtlinien (IAM-Dokumentation).

Zu den empfohlenen Bedingungen für ressourcenbasierte Richtlinien gehören:

- Beschränkung des Zugriffs auf nur Prinzipale in einer bestimmten Organisation (definiert in AWS Organizations) mithilfe der `aws:PrincipalOrgID`-Bedingung.
- Beschränkung des Zugriffs auf Verkehr, der von einer bestimmten VPC oder einem VPC-Endpunkt stammt, unter Verwendung der jeweiligen `aws:SourceVpc`- oder `aws:SourceVpce`-Bedingung.
- Zulassen oder Ablehnen von Datenverkehr auf der Grundlage der Quell-IP-Adresse mit einer `aws:SourceIp`-Bedingung.

Das Folgende ist ein Beispiel für eine ressourcenbasierte Richtlinie, mit der `aws:PrincipalOrgID`-Bedingung, dass nur Prinzipalen in der **<o-xxxxxxxxxxx>**-Organisation den Zugriff auf **<bucket-name>**-S3-Buckets gewährt:

```
{
   "Version":"2012-10-17",
   "Statement":[
     {
       "Sid":"AllowFromOrganization",
       "Effect":"Allow",
       "Principal":"*",
       "Action":"s3:*",
       "Resource":"arn:aws:s3:::<bucket-name>/*",
       "Condition": {
         "StringEquals": {"aws:PrincipalOrgID":"<o-xxxxxxxxxxx>"}
       }
     }
   ]
}
```

WKLD.03 – Verwenden Sie kurzlebige Geheimnisse oder einen Geheimnisverwaltungsservice

Anwendungsgeheimnisse bestehen größtenteils aus Anmeldeinformationen wie Schlüsselpaaren, Zugriffstoken, digitalen Zertifikaten und Anmeldeinformationen. Die Anwendung verwendet diese Geheimnisse, um Zugriff auf andere Services zu erhalten, von denen sie abhängig ist, z. B. eine Datenbank. Zum Schutz dieser Geheimnisse empfehlen wir, dass sie entweder kurzlebig sind (zum Zeitpunkt der Anfrage generiert und kurzlebig, z. B. bei IAM-Rollen) oder von einem Geheimnisverwaltungsservice abgerufen werden. Dadurch wird eine versehentliche Offenlegung

durch weniger sichere Mechanismen, wie z. B. das Speichern statischer Konfigurationsdateien, verhindert. Dies macht es auch einfacher, Anwendungscode von der Entwicklungs- in die Produktionsumgebung zu übertragen.

Für einen Service zur Verwaltung geheimer Daten empfehlen wir die Verwendung einer Kombination aus Parameter Store, einer Funktion von AWS Systems Manager, und AWS Secrets Manager:

- Verwenden Sie Parameter Store, um geheime Daten und andere Parameter zu verwalten, bei denen es sich um einzelne Schlüssel-Wert-Paare handelt, die auf Zeichenketten basieren, eine kurze Gesamtlänge haben und auf die häufig zugegriffen wird. Sie verwenden einen AWS Key Management Service (AWS KMS)-Schlüssel zur Verschlüsselung des Geheimnisses Das Speichern von Parametern in der Standardstufe von Parameter Store ist kostenlos. Weitere Informationen zu Parameterschichten finden Sie unter Parameterschichten verwalten (Systems-Manager-Dokumentation).
- Verwenden Sie Secrets Manager, um Geheimnisse zu speichern, die in Dokumentform vorliegen (z. B. mehrere verwandte Schlüssel-Wert-Paare), größer als 4 KB sind (z. B. digitale Zertifikate) oder von einer automatisierten Rotation profitieren würden.

Sie können Parameter-Store-APIs verwenden, um im Secrets Manager gespeicherte Geheimnisse abzurufen. Auf diese Weise können Sie den Code in Ihrer Anwendung standardisieren, wenn Sie eine Kombination aus beiden Services verwenden.

So verwalten Sie Geheimnisse im Parameter Store

1. Erstellen Sie einen symmetrischen AWS KMS-Schlüssel (AWS KMS-Dokumentation).
2. Erstellen Sie einen SecureString-Parameter (Systems-Manager-Dokumentation). Geheimnisse im Parameter Store verwenden den `SecureString`-Datentyp.
3. Rufen Sie in Ihrer Anwendung einen Parameter aus dem Parameterspeicher ab, indem Sie das AWS-SDK für Ihre Programmiersprache verwenden. Ein Beispiel in Java finden Sie unter GetParameter.java (AWS-Codebeispiel-Katalog).

So verwalten Sie Geheimnisse in Secrets Manager

1. Ein Secret erstellen (Secrets-Manager-Dokumentation).
2. Geheimnisse von AWS Secrets Manager in Code abrufen (Secrets-Manager-Dokumentation).

Es ist wichtig Verwendung AWS Secrets Manager-clientseitiger Caching-Bibliotheken, um die Verfügbarkeit und Latenz bei der Verwendung Ihrer Geheimnisse zu verbessern zu lesen (AWS-Blogbeitrag). Die Verwendung von clientseitigen SDKs, für die bereits bewährte Methoden implementiert wurden, sollte die Verwendung und Integration von Secrets Manager beschleunigen und vereinfachen.

WKLD.04 – Verhindern Sie, dass Anwendungsgeheimnisse offengelegt werden

Während der lokalen Entwicklung können Anwendungsgeheimnisse in lokalen Konfigurations- oder Codedateien gespeichert und versehentlich in Quellcode-Repositorys eingecheckt werden. Ungesicherte Repositorien, die bei öffentlichen Serviceanbietern gehostet werden, können unbefugten Zugriffen und der anschließenden Entdeckung dieser Geheimnisse unterliegen. Verwenden Sie die verfügbaren Tools, um zu verhindern, dass Geheimnisse eingecheckt werden. Integrieren Sie Prüfungen auf offengelegte Geheimnisse in Ihre manuellen Code-Review-Prozesse.

Einige gängige Tools, die verhindern können, dass Anwendungsgeheimnisse in Quellcode-Repositorys eingecheckt werden, sind:

- Gitleaks (GitHub-Repository)
- Whispers (GitHub-Repository)
- detect-secrets (GitHub-Repository)
- git-secrets (GitHub-Repository)
- TruffleHog (GitHub-Repository)

WKLD.05 – Enthüllte Geheimnisse erkennen und korrigieren

Im WKLD.03 – Verwenden Sie kurzlebige Geheimnisse oder einen Geheimnisverwaltungsservice und WKLD.04 – Verhindern Sie, dass Anwendungsgeheimnisse offengelegt werden ergreifen Sie Maßnahmen, um Geheimnisse zu schützen. Im Rahmen dieser Kontrolle stellen Sie eine Lösung bereit, mit der erkannt werden kann, ob geheime Daten diese Präventionsmaßnahmen umgangen haben, und Sie können entsprechende Abhilfemaßnahmen treffen.

Amazon CodeGuru Reviewer erkennt Anwendungsgeheimnisse im Quellcode und bietet einen Mechanismus zur Behebung und Veröffentlichung der erkannten Geheimnisse im Secrets Manager.

Der Anwendungscode zum Abrufen des Geheimnisses aus Secrets Manager wird ebenfalls bereitgestellt. Führen Sie eine Kosten-Nutzen-Analyse durch, um festzustellen, ob diese Lösung für Ihr Unternehmen geeignet ist. Als Alternative bieten einige der Open-Source-Lösungen in WKLD.04 – Verhindern Sie, dass Anwendungsgeheimnisse offengelegt werden Funktionen zur Erkennung vorhandener Geheimnisse.

So richten Sie die CodeGuru-Reviewer-Integration mit Secrets Manager ein

- Verwenden Sie CodeGuru Reviewer, um hartcodierte Geheimnisse zu identifizieren und AWS Secrets Manager, um sie zu sichern (AWS-Blogbeitrag und geführter Rundgang).

WKLD.06 – Verwenden Sie Systems Manager anstelle von SSH oder RDP

Öffentliche Subnetze, deren Standardroute auf ein Internet-Gateway verweist, stellen naturgemäß ein größeres Sicherheitsrisiko dar als private Subnetze, die keine Verbindung zum Internet haben. Sie können EC2-Instances in privaten Subnetzen ausführen und die Session Manager-Funktion von AWS Systems Manager verwenden, um remote auf die Instances zuzugreifen, entweder über AWS Command Line Interface (AWS CLI) oder AWS Management Console. Sie können dann die AWS CLI oder Konsole verwenden, um eine Sitzung zu starten, die über einen sicheren Tunnel eine Verbindung mit der Instance herstellt, sodass keine zusätzlichen Anmeldeinformationen für Secure Shell (SSH) oder Windows Remote Desktop Protocol (RDP) verwaltet werden müssen.

Verwenden Sie Session Manager, anstatt EC2-Instances in öffentlichen Subnetzen auszuführen, Jumpboxen auszuführen oder Bastion-Hosts auszuführen.

Session Manager einrichten

1. Stellen Sie sicher, dass die EC2-Instance das Amazon Machine Image (AMI) des neuesten Betriebssystems, wie Amazon Linux 2 oder Ubuntu verwendet. Der AWS Systems Manager-Agent (SSM Agent) ist auf dem AMI vorinstalliert.
2. Stellen Sie sicher, dass die Instance entweder über ein Internet-Gateway oder über VPC-Endpunkte mit diesen Adressen verbunden ist (ersetzen Sie **<region>** mit der entsprechenden AWS-Region):
    a. Ec2messages.<region>.amazonaws.com
    b. ssm.<region>.amazonaws.com

c. ssmmessages.<region>.amazonaws.com

3. Hängen Sie die AWS-verwaltete Richtlinie `AmazonSSMManagedInstanceCore` an die IAM-Rolle an, mit der Ihre Instances verknüpft sind.

Weitere Informationen finden Sie unter Session Manager einrichten(Systems-Manager-Dokumentation).

Eine Sitzung starten

- Starten Sie eine Sitzung (Systems-Manager-Dokumentation).

WKLD.07 – Protokollieren Sie Datenereignisse für S3-Buckets mit sensiblen Daten

Standardmäßig erfasst AWS CloudTrail Verwaltungsereignisse, Ereignisse, mit denen Ressourcen in Ihrem Konto erstellt, geändert oder gelöscht werden. Diese Verwaltungsereignisse erfassen keine Lese- oder Schreibvorgänge für einzelne Objekte in Buckets in Amazon Simple Storage Service. Während eines Sicherheitsereignisses ist es wichtig, unbefugten Datenzugriff oder unbefugte Datenverwendung auf individueller Datensatz- oder Objektebene zu erfassen. Verwenden Sie CloudTrail zur Protokollierung von Datenereignissen für alle S3-Buckets, in denen sensible oder geschäftskritische Daten gespeichert sind, zu Erkennungs- und Prüfungszwecken.

> **Note**
>
> Für die Protokollierung von Datenereignissen fallen zusätzliche Gebühren an. Weitere Informationen finden Sie unter AWS CloudTrail Preise.

Protokollierung von Datenereignissen für Trails

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die CloudTrail-Konsole unter https://console.aws.amazon.com/cloudtrail/
2. Wählen Sie im Navigationsbereich die Option Trails und dann den Namen des Pfades aus.
3. Wählen Sie unter Allgemeine Details „Bearbeiten“ aus, um die folgenden Einstellungen zu ändern. Sie können den Namen eines Trails nicht ändern.

a. Wählen Sie unter Datenereignisse Bearbeiten aus.

b. Wählen Sie für Daten-Ereignissquelle S3 aus.

c. Für Alle aktuellen und zukünftigen S3-Buckets, löschen Sie Lesen und Schreiben.

d. Suchen Sie unter Individuelle Bucket-Auswahl nach dem Bucket, in dem Datenereignisse protokolliert werden sollen. Sie können in diesem Fenster mehrere Buckets auswählen. Wählen Sie Bucket hinzufügen, um Datenereignisse für weitere Buckets zu protokollieren. Wählen Sie, ob Sie Read (Lesen)-Ereignisse wie `GetObject`, Write (Schreiben)-Ereignisse wie `PutObject` oder Ereignisse beider Typen protokolliert werden sollen.

e. Wählen Sie Trail aktualisieren aus.

WKLD.08 – Amazon-EBS-Volumes verschlüsseln

Erzwingen Sie die Verschlüsselung von Amazon Elastic Block Store (Amazon EBS)-Volumes als Standardverhalten in Ihrem AWS-Konto. Verschlüsselte Volumes haben die gleiche Leistung für Eingabe-/Ausgabevorgänge pro Sekunde (IOPS) wie unverschlüsselte Volumes und haben nur minimale Auswirkungen auf die Latenz. Dadurch wird verhindert, dass Volumes zu einem späteren Zeitpunkt aus Konformitäts- oder anderen Gründen neu erstellt werden müssen. Weitere Informationen finden Sie unter Die wichtigsten bewährten Methoden für die Amazon-EBS-Verschlüsselung (AWS-Blogbeitrag).

Verschlüsselung von Amazon-EBS-Volumes

- Verschlüsselung standardmäßig aktivieren (Amazon-EC2-Dokumentation).

WKLD.09 – Verschlüsseln Sie Amazon-RDS-Datenbanken

Ähnlich wie bei WKLD.08 – Amazon-EBS-Volumes verschlüsseln aktivieren Sie die Verschlüsselung von Amazon Relational Database Service (Amazon RDS). Diese Verschlüsselung wird auf der Ebene des zugrunde liegenden Volumes durchgeführt und hat dieselbe IOPS-Leistung wie unverschlüsselte Volumes mit minimaler Auswirkung auf die Latenz. Weitere Informationen finden Sie unter Übersicht über die Verschlüsselung von Amazon-RDS-Ressourcen (Amazon.RDS-Dokumentation).

Eine RDS-Datenbank-Instance verschlüsseln

- Verschlüsseln Sie eine Datenbankinstance (Amazon-RDS-Dokumentation).

WKLD.10 – Bereitstellen von privaten Ressourcen in privaten Subnetzen

Stellen Sie Ressourcen, die keinen direkten Internetzugang benötigen, wie EC2-Instances, Datenbanken, Warteschlangen, Caching oder andere Infrastrukturen, in einem privaten VPC-Subnetz bereit. Private Subnetze haben in ihrer Routing-Tabelle keine Route zu einem angeschlossenen Internet-Gateway deklariert und können keinen Internetverkehr empfangen. Datenverkehr, der aus einem privaten Subnetz stammt und für das Internet bestimmt ist, muss entweder über ein verwaltetes AWS-NAT-Gateway oder eine EC2-Instance, auf der NAT-Prozesse in einem öffentlichen Subnetz ausgeführt werden, eine Network Address Translation (NAT) durchlaufen. Weitere Informationen zur Netzwerkisolierung finden Sie unter Infrastruktursicherheit in Amazon VPC (Amazon-VPC-Dokumentation).

Gehen Sie beim Erstellen von privaten Ressourcen und Subnetzen wie folgt vor:

- Wenn Sie ein privates Subnetz erstellen, deaktivieren Sie Automatische Zuweisung einer öffentlichen IPv4-Adresse.
- Wenn Sie private EC2-Instances erstellen, deaktivieren Sie Öffentliche IP automatisch zuweisen. Dadurch wird verhindert, dass eine öffentliche IP zugewiesen wird, wenn die Instance versehentlich aufgrund einer Fehlkonfiguration in einem öffentlichen Subnetz bereitgestellt wird.

Bei Bedarf geben Sie das Subnetz für eine Ressource als Teil ihrer Konfiguration an. Sie können eine VPC bereitstellen, die bewährte Methoden befolgt, indem Sie Schnellstart für modulare und skalierbare VPC-Architektur verwenden (AWS-Schnellstarts).

WKLD.11 – Den Netzwerkzugriff mithilfe von Sicherheitsgruppen beschränken

Verwenden Sie Sicherheitsgruppen, um den Datenverkehr zu EC2-Instances, RDS-Datenbanken und anderen unterstützten Ressourcen zu steuern. Sicherheitsgruppen fungieren als virtuelle Firewall, die auf jede Gruppe verwandter Ressourcen angewendet werden kann, um konsistente Regeln für die Zulassung von eingehendem und ausgehendem Datenverkehr zu definieren. Zusätzlich zu Regeln, die auf IP-Adressen und Ports basieren, unterstützen Sicherheitsgruppen Regeln, die den Datenverkehr von Ressourcen zulassen, die anderen Sicherheitsgruppen zugeordnet sind. Eine Datenbanksicherheitsgruppe kann beispielsweise Regeln enthalten, die nur den Datenverkehr einer Anwendungsserver-Sicherheitsgruppe zulassen.

Standardmäßig lassen Sicherheitsgruppen den gesamten ausgehenden Datenverkehr, aber keinen eingehenden Datenverkehr zu. Die Regel für ausgehenden Verkehr kann entfernt werden, oder Sie können zusätzliche Regeln konfigurieren, um ausgehenden Verkehr einzuschränken und eingehenden Verkehr zuzulassen. Wenn die Sicherheitsgruppe keine Regeln für den ausgehenden Verkehr hat, ist kein ausgehender Verkehr von Ihrer Instance erlaubt. Weitere Informationen finden Sie unter Kontrollieren des Datenverkehrs zu Ressourcen mithilfe von Sicherheitsgruppen (Amazon-VPC-Dokumentation).

Im folgenden Beispiel gibt es drei Sicherheitsgruppen, die den Datenverkehr von einem Application Load Balancer zu EC2-Instances steuern, die eine Verbindung zu einer Datenbank von Amazon RDS für MySQL herstellen.

Sicherheitsgruppe	Regeln für eingehenden Datenverkehr	Regeln für ausgehenden Datenverkehr
Sicherheitsgruppe für Application Load Balancer	Beschreibung: HTTPS-Datenverkehr von überall zulassen Typ: HTTPS Quelle: Anywhere-IPv4 (0.0.0.0/0)	Beschreibung: Gesamten Datenverkehr überall hin zulassen Typ: Gesamter Datenverkehr Ziel: Anywhere-IPv4 (0.0.0.0/0)
EC2-Instance-Sicherheitsgruppe	Beschreibung: HTTP-Verkehr vom Application Load Balancer zulassen Typ: HTTP Quelle: Sicherheitsgruppe für Application Load Balancer	Beschreibung: Gesamten Datenverkehr überall hin zulassen Typ: Gesamter Datenverkehr Ziel: Anywhere-IPv4 (0.0.0.0/0)
RDS-Datenbank-Sicherheitsgruppe	Beschreibung: MySQL-Verkehr von der EC2-Instance zulassen Typ: MySQL	Keine Regeln für ausgehenden Datenverkehr

Sicherheitsgruppe	Regeln für eingehenden Datenverkehr	Regeln für ausgehenden Datenverkehr
	Quelle: EC2-Instance-Sicherheitsgruppe	

WKLD.12 – Verwenden von VPC-Endpunkten, um auf unterstützte Services zuzugreifen

In VPCs benötigen Ressourcen, die auf AWS oder andere externe Services zugreifen müssen, entweder eine Route zum Internet (`0.0.0.0/0`) oder an die öffentliche IP-Adresse des Zielservices. Verwenden Sie VPC-Endpunkte, um eine private IP-Route von Ihrer VPC zu unterstützten AWS oder andere Services zu aktivieren, mit denen die Verwendung eines Internet-Gateways, eines NAT-Geräts oder einer Virtual Private Network (VPN) vermieden wird, oder eine AWS Direct Connect-Verbindung.

VPC-Endpunkte unterstützen das Anhängen von Richtlinien und Sicherheitsgruppen, um den Zugriff auf einen Service weiter zu kontrollieren. Sie können beispielsweise eine VPC-Endpunktrichtlinie für Amazon DynamoDB schreiben, um nur Aktionen auf Elementebene zuzulassen und Aktionen auf Tabellenebene für alle Ressourcen in der VPC zu verhindern, unabhängig von deren eigenen Berechtigungsrichtlinien. Sie können auch eine S3-Bucket-Richtlinie schreiben, um nur Anfragen zuzulassen, die von einem bestimmten VPC-Endpunkt stammen, und jeden anderen externen Zugriff zu verweigern. Ein VPC-Endpunkt kann auch über eine Sicherheitsgruppenregel verfügen, die beispielsweise den Zugriff auf nur EC2-Instances beschränkt, die einer anwendungsspezifischen Sicherheitsgruppe zugeordnet sind, z. B. der Geschäftslogikebene einer Webanwendung.

Es gibt verschiedene Arten von VPC-Endpunkten. Sie greifen über einen VPC-Schnittstellenendpunkt auf die meisten Services zu. Auf DynamoDB wird über einen Gateway-Endpunkt zugegriffen. Amazon S3 unterstützt sowohl Gateway- als auch Schnittstellen-Endpunkte. Gateway-Endpunkte werden für Workloads empfohlen, die in einem einzigen AWS-Konto und einer einzigen Region enthalten sind, und sind ohne zusätzliche Kosten erhältlich. Schnittstellenendpunkte werden empfohlen, wenn ein erweiterbarer Zugriff erforderlich ist, z. B. auf einen S3-Bucket von anderen VPCs, On-Premises-Netzwerken oder von anderen AWS-Regionen. Für Schnittstellenendpunkte fallen eine stündliche Verfügbarkeitsgebühr und eine Datenverarbeitungsgebühr pro GB an, die beide niedriger sind als die jeweiligen Gebühren für das Senden der Daten an `0.0.0.0/0` durch AWS-NAT-Gateway.

Weitere Informationen zur Verwendung von VPC-Endpunkten finden Sie in den folgenden zusätzlichen Ressourcen:

- Weitere Informationen zur Auswahl zwischen Gateway- und Schnittstellen-Endpunkten für Amazon S3 finden Sie unter Wählen Sie Ihre VPC-Endpunkt-Strategie für Amazon S3 (AWS-Blogbeitrag).
- Erstellen eines Schnittstellen-Endpunkts (Amazon-VPC-Dokumentation).
- Einen Gateway-Endpunkt erstellen (Amazon-VPC-Dokumentation).
- Beispielhafte S3-Bucket-Richtlinien, mit denen der Zugriff auf eine bestimmte VPC oder VPC-Endpunkt eingeschränkt wird, finden Sie unter Beschränkung des Zugriffs auf eine bestimmte VPC (Amazon-S3-Dokumentation).
- Beispielhafte DynamoDB-Endpunktrichtlinien, die Aktionen einschränken, finden Sie unter Endpunktrichtlinien für DynamoDB (Amazon-VPC-Dokumentation).

WKLD.13 – HTTPS für alle öffentlichen Web-Endpunkte erfordern

Erfordern Sie HTTPS, um Ihren Web-Endpunkten zusätzliche Glaubwürdigkeit zu verleihen, Ihren Endpunkten die Verwendung von Zertifikaten zum Nachweis ihrer Identität zu ermöglichen und zu bestätigen, dass der gesamte Datenverkehr zwischen Ihrem Endpunkt und den verbundenen Clients verschlüsselt ist. Für öffentliche Websites bietet dies den zusätzlichen Vorteil eines höheren Suchmaschinen-Rankings.

Viele AWS-Services stellen öffentliche Web-Endpunkte für Ihre Ressourcen bereit, wie z. B. AWS Elastic Beanstalk, Amazon CloudFront, Amazon API Gateway, Elastic Load Balancing und AWS Amplify. Anweisungen dazu, wie HTTPS für jeden dieser Service erfordert wird, finden Sie im Folgenden:

- Elastic Beanstalk (Elastic-Beanstalk-Dokumentation)
- CloudFront (CloudFront-Dokumentation)
- Application Load Balancer (AWS Knowledge Center)
- Classic Load Balancer (AWS Knowledge Center)
- Amplify (Amplify-Dokumentation)

Auf Amazon S3 gehostete statische Websites unterstützen HTTPS nicht. Um HTTPS für diese Websites zu erfordern, können Sie CloudFront verwenden. Ein öffentlicher Zugriff auf S3-Buckets, die Inhalte über CloudFront bereitstellen, ist nicht erforderlich.

So verwenden Sie CloudFront zur Bereitstellung einer statischen Website, die auf Amazon S3 gehostet wird

1. Verwenden Sie CloudFront zum Bereitstellen einer statischen Website, die auf Amazon S3 gehostet wird (AWS Knowledge Center).
2. Wenn Sie den Zugriff auf einen öffentlichen S3-Bucket konfigurieren, erfordern Sie HTTPS zwischen Viewern und CloudFront (CloudFront-Dokumentation).

   Wenn Sie den Zugriff auf einen privaten S3-Bucket konfigurieren, schränken Sie den Zugriff auf Amazon-S3-Inhalte mithilfe einer Ursprungszugriffsidentität ein (CloudFront-Dokumentation).

Konfigurieren Sie außerdem HTTPS-Endpunkte so, dass sie moderne Transport Layer Security (TLS)-Protokolle und Chiffren benötigen, sofern keine Kompatibilität mit älteren Protokollen erforderlich ist. Verwenden Sie zum Beispiel die `ELBSecurityPolicy-FS-1-2-Res-2020-10` oder die neueste Richtlinie, die für HTTPS-Listener für Application Load Balancer verfügbar ist, anstelle der Standard-`ELBSecurityPolicy-2016-08`. Die aktuellsten Richtlinien erfordern mindestens TLS 1.2, Forward Secrecy und starke Verschlüsselungen, die mit modernen Webbrowsern kompatibel sind.

Weitere Informationen zu den verfügbaren Sicherheitsrichtlinien für öffentliche HTTPS-Endpunkte finden Sie unter:

- Vordefinierte SSL-Sicherheitsrichtlinien für Classic Load Balancer (Dokumentation zu Elastic Load Balancing)
- Sicherheitsrichtlinien für Ihren Application Load Balancer (Dokumentation zu Elastic Load Balancing)
- Unterstützte Protokolle und Verschlüsselungen zwischen Viewern und CloudFront (CloudFront-Dokumentation)

WKLD.14 – Verwenden Sie Edge-Protection-Services für öffentliche Endpunkte

Anstatt den Datenverkehr direkt von Datenverarbeitungsservices wie EC2-Instances oder Containern bereitzustellen, verwenden Sie einen Edge-Protection-Service. Dies bietet eine zusätzliche Sicherheitsebene zwischen dem eingehenden Datenverkehr aus dem Internet und Ihren Ressourcen, die diesen Datenverkehr bedienen. Diese Services können unerwünschten Datenverkehr filtern,

Verschlüsselung erzwingen und Routing oder andere Regeln wie Lastenausgleich anwenden, bevor der Datenverkehr Ihre internen Ressourcen erreicht.

AWS-Services, die öffentlichen Endpunktschutz bieten können, sind AWS WAF, CloudFront, Elastic Load Balancing, API Gateway und Amplify Hosting. Führen Sie VPC-basierte Services wie Elastic Load Balancing in einem öffentlichen Subnetz als Proxy für Webserviceressourcen aus, die in einem privaten Subnetz ausgeführt werden.

CloudFront, API Gateway und Amazon Route 53 bieten kostenlosen Schutz vor Distributed Denial of Service (DDos, verteilte Dienstblockade)-Angriffen der Ebenen 3 und 4 und AWS WAF kann vor Layer-7-Angriffen schützen.

Anweisungen für die ersten Schritte mit den einzelnen Services finden Sie hier:

- Erste Schritte mit AWS WAF (AWS-Webseite)
- Erste Schritte mit Amazon CloudFront (CloudFront-Dokumentation)
- Erste Schritte mit Elastic Load Balancing (Dokumentation zu Elastic Load Balancing)
- Erste Schritte mit API Gateway (API-Gateway-Dokumentation)
- Erste Schritte mit Amplify Hosting (Amplify-Dokumentation)

WKLD.15 – Definieren von Sicherheitskontrollen in Vorlagen und Implementierung mithilfe von CI/CD-Methoden

Infrastructure as Code (IaC) ist die Praxis, all Ihre AWS-Serviceressourcen und Konfigurationen in Vorlagen und Code, mit Pipelines für Continuous Integration und Continuous Delivery (CI/CD) bereitstellen, mit denen Softwareanwendungen bereitgestellt werden. IaC-Services, wie beispielsweise AWS CloudFormation, unterstützen sowohl identitätsbasierte als auch ressourcenbasierte IAM-Richtlinien und unterstützen AWS-Sicherheitsservices wie Amazon GuardDuty, AWS WAF und Amazon VPC. Erfassen Sie diese Artefakte als IaC-Vorlagen, übertragen Sie die Vorlagen in ein Quellcode-Repository und stellen Sie sie dann mithilfe von CI/CD-Pipelines bereit.

Sofern nicht anders vorgeschrieben, legen Sie Anwendungsberechtigungsrichtlinien mit Anwendungscode im selben Repository fest und verwalten Sie allgemeine Ressourcenrichtlinien und Sicherheitsservicekonfigurationen in separaten Code-Repositorys und Bereitstellungspipelines.

Weitere Informationen zu den ersten Schritten mit IaC auf AWS finden Sie in der AWS Cloud Development Kit (AWS CDK)-Dokumentation.

Beitragende Faktoren

Zu den Mitwirkenden an diesem Dokument gehören:

- Jay Michael, Principal Solutions Architect
- Cole Calistra, Principal Solutions Architect
- Justin Plock, Principal Solutions Architect
- Faisal Farooq, Solutions Architect
- Michael Nguyen, Sr. Solutions Architect
- Ritik Khatwani, Sr. Solutions Architect
- Paul Hawkins, Principal, Office of the Chief Information Security Officer (CISO)

Ein besonderer Dank geht an die folgenden Personen, die uns auch bei der Beratung und Überprüfung geholfen haben:

- Robert Put
- Mike Sullivan
- Bob Lee III

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
Einstellungen von Amazon-S3-Buckets	Wir haben den Abschnitt ACCT.08 – Verhindern Sie den öffentlichen Zugriff auf private S3-Buckets aktualisiert, um zu verdeutlichen, dass bei Amazon-S3-Buckets, die nach dem 28. April 2023 erstellt wurden, die Einstellung Block Public Access standardmäßig aktiviert ist.	18. Mai 2023
Bewährte IAM-Sicherheitsmethoden	Wir haben diesen Leitfaden aktualisiert, um ihn an den neuesten Stand zu bewährten Methoden für AWS Identity and Access Management (IAM) zu bringen. Weitere Informationen finden Sie unter Bewährte Sicherheitsmethoden in der IAM-Dokumentation.	1. Februar 2023
IAM-Rollen	Wir haben zusätzliche Links zur AWS-Service-Dokumentation im Abschnitt WKLD.01 – Verwenden Sie IAM-Rollen für Berechtigungen in der Datenverarbeitungsumgebung bereitgestellt.	22. September 2022

Passwortrichtlinie	Wir haben die Empfehlungen für sichere Passwörter aktualisiert, um die neuesten Leitlinien des Center for Internet Security (CIS) zu verwenden.	10. Mai 2022
Erste Veröffentlichung	—	13. April 2022

Glossar zu AWS Prescriptive Guidance

Die folgenden Begriffe werden häufig in Strategien, Leitfäden und Mustern verwendet, die von AWS Prescriptive Guidance bereitgestellt werden. 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 On-Premises-Oracle-Datenbank zu der PostgreSQL-kompatible Amazon-Aurora-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 On-Premises-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 On-Premises-Oracle-Datenbank zu Oracle auf einer EC2-Instance 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. Dieses Migrationsszenario ist spezifisch für VMware Cloud in AWS, welches die Kompatibilität mit virtuellen Maschinen (VM) und die Workload-Portabilität zwischen Ihrer On-Premises-Umgebung und AWS unterstützt. Sie können die VMware-Cloud-Foundation-Technologien von Ihren On-Premises-Rechenzentren aus verwenden, wenn

Sie Ihre Infrastruktur zu VMware Cloud in AWS migrieren. Beispiel: Verschieben Sie den Hypervisor, der Ihre Oracle-Datenbank hostet, auf VMware Cloud in 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 .

Abstrakte Services

Siehe -verwaltete Services.

ACID

Siehe Atomizität, Konsistenz, Isolation, 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. Sie ist flexibler, erfordert aber mehr Arbeit als die Aktiv-Passiv-Migration.

Aktiv-Passiv-Migration

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

Aggregatfunktion

Eine SQL-Funktion, die für eine 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 für künstliche Intelligenz.

Anonymisierung

Der Prozess des dauerhaften Löschens personenbezogener Daten in einem Datensatz. Anonymisierung kann dazu beitragen, den persönlichen Datenschutz zu schützen. Anonymisierte Daten werden nicht mehr als personenbezogene Daten betrachtet.

Anti-Muster

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

-Anwendungskontrolle

Ein Sicherheitsansatz, der nur die Verwendung genehmigter Anwendungen ermöglicht, um ein System vor Malware zu schützen.

Anwendungsportfolio

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

künstliche Intelligenz (KI)

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

Operationen mit künstlicher Intelligenz (AIOps)

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

Asymmetrische Verschlüsselung

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

Atomizität, Konsistenz, Isolierung, Haltbarkeit (ACID)

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

Attributbasierte Zugriffskontrolle (ABAC)

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

Autorisierende Datenquelle

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

Availability Zone

Ein eigener Standort in einer AWS-Region, der isoliert und somit vor Ausfällen in anderen Availability Zones geschützt ist und kostengünstige Netzwerkkonnektivität mit geringer Latenz zu anderen Availability Zones in der gleichen Region bereitstellt.

AWS Cloud Adoption Framework (AWS CAF)

Ein Rahmen von Leitlinien und bewährten Verfahren von AWS, um Organisationen bei der Entwicklung eines effizienten und effektiven Plans für eine erfolgreiche Umstellung auf die Cloud zu unterstützen. AWS CAF unterteilt die Beratung in sechs Schwerpunktbereiche, die

als Perspektiven bezeichnet werden: Geschäft, Menschen, 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. Für diese Perspektive bietet AWS-CAF Beratung für Personalentwicklung, Training und Kommunikation, um die Organisation auf eine erfolgreiche Cloud-Einführung vorzubereiten. Weitere Informationen finden Sie auf der AWS-CAF-Webseite und dem AWS-CAF-Whitepaper.

AWS Workload Qualification Framework (AWS WQF)

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

B

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 Endianität .

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.

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 Verzweigungen (GitHub Dokumentation).

Break-Glass-Zugriff

Unter außergewöhnlichen Umständen und durch einen genehmigten Prozess ist dies eine schnelle Möglichkeit für einen Benutzer, Zugriff auf einen zu erhaltenAWS-Konto, für den er normalerweise keine Zugriffsberechtigungen besitzt. Weitere Informationen finden Sie im Indikator Implement break-glass procedures in der AWS Well-Architected-Anleitung.

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

Siehe AWS Cloud Adoption Framework.

CCoE

Weitere Informationen finden Sie unter Cloud-Kompetenzzentrum.

CDC

Siehe Erfassung von Datenänderungen.

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-Engineering

Absichtliche Einführung von Ausfällen oder störenden Ereignissen, um die Ausfallsicherheit eines Systems zu testen. Sie können AWS Fault Injection Service (AWS FIS) verwenden, um Experimente durchzuführen, die Ihre AWSWorkloads belasten, und deren Antwort bewerten.

CI/CD

Siehe kontinuierliche Integration und kontinuierliche Bereitstellung.

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 der Ziel-AWS-Service sie empfängt.

Cloud-Kompetenzzentrum (CCoE)

Ein multidisziplinäres Team, das die Cloud-Einführung in der gesamten Organisation vorantreibt, einschließlich der Entwicklung bewährter Cloud-Methoden, der Mobilisierung von Ressourcen, der Festlegung von Migrationszeitplänen und der Begleitung der Organisation durch groß angelegte Transformationen. Weitere Informationen finden Sie hier: Beiträge von CCoE auf dem AWS-Blog zur Cloud-Unternehmensstrategie.

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 Erstellen, Reifen und Optimieren einer oder mehrerer Cloud-Umgebungen verwendet wird. Weitere Informationen finden Sie unter Erstellen Ihres Cloud-Betriebsmodells.

Phasen der Einführung der Cloud

Die vier Phasen, die Organisationen normalerweise durchlaufen, wenn sie auf die AWS-Cloud migrieren:

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

Diese Phasen wurden von Stephen Orban im Blogbeitrag Der Weg zu Cloud-First und die Phasen der Einführung im AWS-Blog zur Cloud-Unternehmensstrategie definiert. Informationen darüber, wie sie sich auf die AWS-Migrationsstrategie beziehen finden Sie im Leitfaden zur Vorbereitung der Migration.

CMDB

Siehe Konfigurationsverwaltungsdatenbank .

Code-Repository

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

Kalter Cache

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

Kalte Daten

Daten, auf die selten zugegriffen wird und die in der Regel historisch sind. Wenn Sie diese Art von Daten abfragen, sind langsame Abfragen in der Regel akzeptabel. Das Verschieben dieser Daten in Speicherebenen oder -klassen mit geringerer Leistung und geringeren Kosten kann die Kosten senken.

Computer Vision

Ein KI-Bereich, der von Maschinen verwendet wird, um Personen, Orte und Objekte in Bildern mit Genauigkeit auf oder über menschlichen Ebenen zu identifizieren. Oft mit Deep-Learning-Modellen erstellt, automatisiert es die Extraktion, Analyse, Klassifizierung und das Verständnis nützlicher Informationen aus einem einzelnen Bild oder einer Abfolge von Bildern.

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 Compliance- und Sicherheitsprüfungen individuell anzupassen. Mit Hilfe einer YAML-Vorlage können Sie ein Konformitätspaket als einzelne Einheit in einem AWS-Konto und Region oder in einer gesamten Organisation bereitstellen. Weitere Informationen finden Sie unter Konformitätspakete in der AWS Config-Dokumentation.

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.

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.

Datenabweichung

Eine bedeutende Variation zwischen den Produktionsdaten und den Daten, die zum Trainieren eines ML-Modells verwendet wurden, oder eine bedeutende Änderung der Eingabedaten im Laufe der Zeit. Datenabweichungen können die Gesamtqualität, Genauigkeit und Fairness bei ML-Modellvorhersagen reduzieren.

Daten während der Übertragung

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

Datenminimierung

Das Prinzip, nur die Daten zu erfassen und zu verarbeiten, die unbedingt erforderlich sind. Durch die Durchführung der Datenminimierung in der AWS Cloud können Datenschutzrisiken, Kosten und Ihren CO2-Fußabdruck für Analysen reduziert werden.

Datenumfang

Eine Reihe präventiver Integritätsschutz in Ihrer -AWSUmgebung, die dazu beitragen, sicherzustellen, dass nur vertrauenswürdige Identitäten von erwarteten Netzwerken aus auf vertrauenswürdige Ressourcen zugreifen. Weitere Informationen finden Sie unter Erstellen 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.

-Datenübereinstimmung

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

Betreff

Eine Person, deren Daten gesammelt und verarbeitet werden.

Data Warehouse

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

Datenbankdefinitionssprache (DDL)

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

Datenbankmanipulationssprache (DML)

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

DDL

Siehe Datenbankdefinitionssprache .

Deep-Ensemble

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

Deep Learning

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

defense-in-depth

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

delegierter Administrator

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

Bereitstellung

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

Entwicklungsumgebung

Siehe Umgebung .

Detektivische Kontrolle

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

Development Value Stream Mapping (DVSM)

Ein Prozess, der verwendet wird, um Einschränkungen zu identifizieren und zu priorisieren, die sich negativ auf Geschwindigkeit und Qualität in einem Lebenszyklus der Softwareentwicklung auswirken. DVSM erweitert den Prozess zur Zuordnung von Wertströmen, der ursprünglich für strenge Herstellungspraktiken entwickelt wurde. Es konzentriert sich auf die Schritte und Teams, die erforderlich sind, um den Wert im Softwareentwicklungsprozess zu schaffen und zu verschieben.

Digitale Telefonie

Eine virtuelle Darstellung eines realen Systems, z. B. eines Gebäudes, einer Fabrik, Industrieanlagen oder einer Produktionslinie. Digitale Komponenten unterstützen prädiktive Wartung, Remote-Überwachung und Produktionsoptimierung.

Dimensionstabelle

In einem Sternschema ist dies eine kleinere Tabelle, die Datenattribute zu quantitativen Daten in einer Faktentabelle enthält. Dimensionstabellenattribute sind in der Regel Textfelder oder diskrete Zahlen, die sich wie Text verhalten. Diese Attribute werden häufig für die Einschränkung, Filterung und Kennzeichnung von Ergebnissätzen verwendet.

Notfall

Ein Ereignis, das verhindert, dass ein Workload oder System seine Geschäftsziele an seinem primär bereitgestellten Standort erfüllt. Bei diesen Ereignissen kann es sich um Naturkatastrophen, technische Ausfälle oder das Ergebnis menschlicher Aktionen wie unbeabsichtigte Fehlkonfigurationen oder Malware-Angriffe handeln.

Notfallwiederherstellung (DR)

Die Strategie und der Prozess, die Sie verwenden, um Ausfallzeiten und Datenverluste zu minimieren, die durch einen Notfall verursacht werden. Weitere Informationen finden Sie unter Notfallwiederherstellung von Workloads auf AWS: Wiederherstellung in der Cloud im AWS Well-Architected Framework.

DML

Siehe Datenbankmanipulationssprache .

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 Notfallwiederherstellung .

Abweichungserkennung

Nachverfolgen von Abweichungen von einer Basiskonfiguration. Sie können beispielsweise verwenden, AWS CloudFormation um Abweichungen in Systemressourcen zu erkennen, oder Sie können verwenden, AWS Control Tower um Änderungen in Ihrer Landing Zone zu erkennen, die sich auf die Einhaltung der Governance-Anforderungen auswirken könnten.

DVSM

Weitere Informationen finden Sie unter Stream-Zuweisung von Entwicklungswerten.

E

EDA

Weitere Informationen finden Sie unter Explorative Datenanalyse.

Edge-Computing

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

Verschlüsselung

Ein Datenverarbeitungsprozess, der Klartextdaten, die für Menschen lesbar sind, in Geheimtext 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 Endpunktservice mit AWS PrivateLink erstellen und anderen AWS-Konten oder AWS Identity and Access Management (IAM)-Prinzipalen Berechtigungen erteilen. 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.

Envelope-Verschlüsselung

Der Prozess der Verschlüsselung eines Verschlüsselungsschlüssels mit einem anderen Verschlüsselungsschlüssel. Weitere Informationen finden Sie unter Umschlagverschlüsselung 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 AWS-CAF-Sicherheitsepics 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.

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 . Es speichert quantitative Daten über den Geschäftsbetrieb. In der Regel enthält eine Faktentabelle zwei Arten von Spalten: Spalten, die Messwerte enthalten, und Spalten, die einen Fremdschlüssel für eine Dimensionstabelle enthalten.

schnell fehlschlagen

Eine Variante, die häufige und inkrementelle Tests verwendet, um den Entwicklungslebenszyklus zu reduzieren. Es ist ein wichtiger Teil eines agilen Ansatzes.

Fehlerisolierungsgrenze

In der AWS Cloudeine Grenze wie eine Availability Zone, , AWS-RegionSteuerebene oder Datenebene, die die Auswirkungen eines Ausfalls begrenzt und die Ausfallsicherheit von Workloads verbessert. Weitere Informationen finden Sie unter AWS Fehlerisolierungsgrenzen.

Feature-Zweig

Siehe Verzweigung .

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 Machine-Learning-Modellen mit :AWS.

Featuretransformation

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

FGAC

Siehe differenzierte Zugriffskontrolle .

differenzierte Zugriffskontrolle (FGAC)

Die Verwendung mehrerer Bedingungen zum Zulassen oder Verweigern einer Zugriffsanforderung.

Flash-Cut-Migration

Eine Datenbankmigrationsmethode, die die kontinuierliche Datenreplikation über die Erfassung von Änderungsdaten verwendet, um Daten in der kürzestmöglichen Zeit zu migrieren, anstatt einen schrittweisen Ansatz zu verwenden. Ziel ist es, Ausfallzeiten auf ein Minimum zu beschränken.

G

Geoblockierung

Siehe geografische Einschränkungen.

Geografische Einschränkungen (Geoblocking)

In Amazon eine Option CloudFront, um Benutzer in bestimmten Ländern am Zugriff auf Inhaltsverteilungen zu hindern. Sie können eine Zulassungsliste oder eine Sperrliste verwenden, um zugelassene und gesperrte Länder anzugeben. Weitere Informationen finden Sie unter Einschränken der geografischen Verteilung Ihrer Inhalte in der - CloudFront Dokumentation.

Gitflow-Workflow

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

Greenfield-Strategie

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

Integritätsschutz

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

H

HA

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.

Hochverfügbarkeit (HA)

Die Fähigkeit eines Workloads, im Falle von Herausforderungen oder Katastrophen kontinuierlich und ohne Eingriff zu arbeiten. HA-Systeme sind so konzipiert, dass sie automatisch ein Failover durchführen, konsistent eine qualitativ hochwertige Leistung liefern und verschiedene Lasten und Ausfälle mit minimalen Leistungseinbußen behandeln.

Historische Modernisierung

Ein Ansatz, der zur Modernisierung und Aktualisierung von Systemen der Betriebstechnologie (OT) verwendet wird, um die Anforderungen der Fertigung besser zu erfüllen. Ein Historiker ist eine Art von Datenbank, die verwendet wird, um Daten aus verschiedenen Quellen in einer Fabrik zu sammeln und zu speichern.

Homogene Datenbankmigration

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

Hot Data

Daten, auf die häufig zugegriffen wird, wie Echtzeitdaten oder aktuelle Übersetzungsdaten. Diese Daten erfordern in der Regel eine Speicherebene oder Klasse mit hoher Leistung, um schnelle Abfrageantworten bereitzustellen.

Hotfix

Eine dringende Lösung für ein kritisches Problem in einer Produktionsumgebung. Aufgrund seiner Wichtigkeit 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

Siehe 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

Weitere Informationen finden Sie unter Industrielles Internet der Dinge.

unveränderliche Infrastruktur

Ein Modell, das eine neue Infrastruktur für Produktions-Workloads bereitstellt, anstatt die vorhandene Infrastruktur zu aktualisieren, zu patchen oder zu ändern. Unveränderliche Infrastrukturen sind von Natur aus konsistenter, zuverlässiger und vorhersehbarer als veränderbare Infrastrukturen. Weitere Informationen finden Sie unter Bereitstellung mit unveränderlicher Infrastruktur im AWS Well-Architected Framework.

Eingehende (ingress) VPC

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

Inkrementelle Migration

Eine Cutover-Strategie, bei der Sie Ihre Anwendung in kleinen Teilen migrieren, anstatt eine einziges vollständiges Cutover durchzuführen. Beispielsweise könnten Sie zunächst nur einige Microservices oder Benutzer auf das neue System umstellen. Nachdem Sie sich vergewissert haben, dass alles ordnungsgemäß funktioniert, können Sie weitere Microservices oder Benutzer

schrittweise verschieben, bis Sie Ihr Legacy-System außer Betrieb nehmen können. Diese Strategie reduziert die mit großen Migrationen verbundenen Risiken.

Infrastruktur

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

Infrastructure as Code (IaC)

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

Industrielles Internet der Dinge (IIoT)

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

Inspektions-VPC

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

Internet of Things (IoT)

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

Interpretierbarkeit

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

IoT

Siehe Internet der Dinge.

IT information library (ITIL, IT-Informationsbibliothek)

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

T service management (ITSM, IT-Servicemanagement)

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

ITIL

Siehe IT-Informationsbibliothek .

ITSM

Siehe IT-Servicemanagement.

L

Labelbasierte Zugriffskontrolle (LBAC)

Eine Implementierung der obligatorischen Zugriffskontrolle (MAC), bei der den Benutzern und den Daten selbst jeweils explizit ein Sicherheitsbezeichnungswert zugewiesen wird. Die Schnittmenge zwischen der Benutzersicherheitsbezeichnung und der Datensicherheitsbezeichnung bestimmt, welche Zeilen und Spalten vom Benutzer angezeigt werden können.

Landing Zone

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

Große Migration

Eine Migration von 300 oder mehr Servern.

LBAC

Siehe Label-basierte Zugriffskontrolle .

Geringste Berechtigung

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

Lift and Shift

Siehe 7 Rs.

Little-Endian-System

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

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 Verzweigung .

Von verwaltete Services

AWS-Services für die die Infrastrukturebene, das Betriebssystem und die Plattformen AWS betreibt und Sie auf die Endpunkte zugreifen, um Daten zu speichern und abzurufen. Amazon Simple Storage Service (Amazon S3) und Amazon DynamoDB sind Beispiele für verwaltete Services. Diese werden auch als abstrakte Services bezeichnet.

MAP

Weitere Informationen finden Sie unter Migration Acceleration Program.

Mechanismus

Ein vollständiger Prozess, in dem Sie ein Tool erstellen, die Einführung des Tools fördern und dann die Ergebnisse überprüfen, um Anpassungen vorzunehmen. Ein Mechanismus ist ein

Zyklus, der sich bei der Ausführung selbst verstärkt und verbessert. Weitere Informationen finden Sie unter Erstellen von Mechanismen im AWS Well-Architected Framework.

Mitgliedskonto

Alle AWS-Konten mit Ausnahme des Verwaltungskontos, die Teil einer Organisation in AWS Organizations sind. Ein Konto kann jeweils nur einer Organisation angehören.

Microservice

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

Microservices-Architekturen

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

Migration Acceleration Program (MAP)

Ein AWS-Programm, das Beratung, Unterstützung, Training und Services bietet, um Organisationen dabei zu unterstützen, eine solide betriebliche Grundlage für den Umstieg 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 der Migrationsfabrik gehören in der Regel Betrieb, 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 das AWS-Konto.

Migrationsmuster

Eine wiederholbare Migrationsaufgabe, in der die Migrationsstrategie, das Migrationsziel und die verwendete Migrationsanwendung oder der verwendete Migrationsservice detailliert beschrieben werden. Beispiel: Hostwechsel-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 in die AWS-Cloud. MPA bietet eine detaillierte Portfoliobewertung (richtige Servergröße, Preisgestaltung, Gesamtbetriebskostenanalyse, Migrationskostenanalyse) sowie Migrationsplanung (Anwendungsdatenanalyse und Datenerfassung, Anwendungsgruppierung, Migrationspriorisierung und Wellenplanung). Das MPA-Tool (erfordert Anmeldung) ist für alle AWS-Berater und APN-Partnerberater kostenlos verfügbar.

Migration Readiness Assessment (MRA)

Der Prozess der Gewinnung von Erkenntnissen über die Cloud-Bereitschaft einer Organisation, der Identifizierung von Stärken und Schwächen und der Erstellung eines Aktionsplans zur Schließung identifizierter Lücken unter Verwendung des AWS-CAF. Weitere Informationen finden Sie im Benutzerhandbuch für Migration Readiness. MRA ist die erste Phase der AWS-Migrationsstrategie.

Migrationsstrategie

Der Ansatz, der verwendet wird, um einen Workload in die AWS-Cloud zu migrieren. Weitere Informationen finden Sie im Eintrag 7 Rs in diesem Glossar und unter Mobilisieren Ihrer Organisation zur Beschleunigung umfangreicher Migrationen.

ML

Siehe Machine Learning.

MPA

Weitere Informationen finden Sie unter Bewertung des Migrationsportfolios.

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 Bewertung 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.

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?“

veränderliche Infrastruktur

Ein Modell, das die vorhandene Infrastruktur für Produktions-Workloads aktualisiert und ändert. Um Konsistenz, Zuverlässigkeit und Vorhersehbarkeit zu verbessern, empfiehlt das AWS Well-Architected Framework die Verwendung unveränderlicher Infrastruktur als bewährte Methode.

O

OAC

Siehe Ursprungszugriffskontrolle .

OAI

Siehe Ursprungszugriffsidentität .

COM

Siehe Organisations-Änderungsmanagement.

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 Betriebsebene .

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.

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, den Umfang von Vorfällen und möglichen Ausfällen zu verstehen, zu bewerten, zu verhindern oder zu reduzieren. Weitere Informationen finden Sie unter Operational Readiness Reviews (ORR) im AWS Well-Architected Framework.

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

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

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 heißt dieser Rahmen Beschleunigung der Menschen, aufgrund der Geschwindigkeit des Wandels, der bei Projekten zur Cloud-Einführung erforderlich ist. Weitere Informationen finden Sie im OCM-Handbuch.

Ursprungszugriffskontrolle (OAC)

In CloudFront, eine erweiterte Option zur Einschränkung des Zugriffs auf die Sicherung Ihrer Amazon Simple Storage Service (Amazon S3)-Inhalte. OAC unterstützt alle S3-Buckets in allen AWS-Regionen, serverseitige Verschlüsselung mit AWS KMS (SSE-KMS) und dynamische `PUT`- und `DELETE`-Anforderungen an den S3-Bucket.

Ursprungszugriffsidentität (OAI)

In CloudFront, eine Option zur Einschränkung des Zugriffs auf die Sicherung Ihrer Amazon S3-Inhalte. Wenn Sie OAI verwenden, CloudFront erstellt einen Prinzipal, mit dem sich Amazon S3 authentifizieren kann. Authentifizierte Prinzipale können nur über eine bestimmte CloudFront Verteilung auf Inhalte in einem S3-Bucket zugreifen. Siehe auch OAC, das eine detailliertere und verbesserte Zugriffskontrolle bietet.

ORR

Siehe Überprüfung der Betriebsbereitschaft.

Ausgehende (egress) VPC

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

P

Berechtigungsgrenze

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

persönlich identifizierbare Informationen (PII)

Informationen, die bei direkter Anzeige oder in Verbindung mit anderen zugehörigen Daten verwendet werden können, um die Identität einer Person verfolgbar abzuleiten. Beispiele für PII 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.

policy

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

Polyglotte Beharrlichkeit

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

Portfoliobewertung

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

predicate

Eine Abfragebedingung, die `true` oder zurückgibt`false`, die sich üblicherweise in einer -`WHERE`Klausel befindet.

Prädikat-Pushdown

Eine Datenbankabfrageoptimierungstechnik, die die Daten in der Abfrage vor der Übertragung filtert. Dies reduziert die Datenmenge, die aus der relationalen Datenbank abgerufen und verarbeitet werden muss, und verbessert die Abfrageleistung.

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 in AWS, die Aktionen durchführen und auf Ressourcen zugreifen kann. Diese Entität ist normalerweise ein Root-Benutzer für ein AWS-Konto, eine IAM-Rolle oder ein Benutzer.

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

Datenschutz nach Design

Ein Ansatz im System-Engineering, 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 ihre Subdomains innerhalb einer oder mehrerer VPCs reagieren soll. Weitere Informationen finden Sie unter Arbeiten mit privat gehosteten Zonen in der Route-53-Dokumentation.

Proaktive Kontrolle

Eine Sicherheitskontrolle, die die Bereitstellung nicht konformer Ressourcen verhindert. Diese Kontrollen scannen Ressourcen, bevor sie bereitgestellt werden. Wenn die Ressource nicht mit der Kontrolle konform ist, wird sie nicht bereitgestellt. Weitere Informationen finden Sie im Referenzhandbuch zu Kontrollen in der -AWS Control TowerDokumentation und unter Proaktive Kontrollen in Implementierung von Sicherheitskontrollen in AWS.

Produktionsumgebung

Siehe Umgebung .

Visualisierung

Der Prozess zum Ersetzen persönlicher Kennungen in einem Datensatz durch Platzhalterwerte. Die Pseudonymisierung kann dazu beitragen, den persönlichen Datenschutz zu schützen. Pseudonymisierte Daten werden weiterhin als personenbezogene Daten betrachtet.

Q

Abfrageplan

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

Abfrageplanregression

Wenn ein Datenbankserviceoptimierer einen weniger optimalen Plan wählt als vor einer bestimmten Änderung der Datenbankumgebung. Dies kann durch Änderungen an Statistiken,

Beschränkungen, Umgebungseinstellungen, Abfrageparameter-Bindungen und Aktualisierungen der Datenbank-Engine verursacht werden.

R

RACI-Matrix

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

Ransomware

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

RASCI-Matrix

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

RCAC

Siehe Zugriffskontrolle für Zeilen und Spalten .

Read Replica

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

Neuarchitektur

Siehe 7 Rs.

Recovery Point Objective (RPO)

Die maximal zulässige Zeit seit dem letzten Datenwiederherstellungspunkt. Dies bestimmt, was als akzeptabler Datenverlust zwischen dem letzten Wiederherstellungspunkt und der Unterbrechung des Services angesehen wird.

Recovery Time Objective (RTO)

Die maximal akzeptable Verzögerung zwischen der Unterbrechung des Services und der Wiederherstellung des Services.

Faktorwechsel

Siehe 7 Rs.

Region

Eine Sammlung von AWS-Ressourcen in einem geografischen Bereich. Jede AWS-Region ist isoliert und unabhängig von den anderen, um Fehlertoleranz, Stabilität und Belastbarkeit zu gewährleisten. Weitere Informationen finden Sie unter Verwalten von AWS-Regionen in der Allgemeine AWS-Referenz.

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.

Hostwechsel

Siehe 7 Rs.

Veröffentlichung

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

Verschiebung

Siehe 7 Rs.

Plattformwechsel

Siehe 7 Rs.

Neukauf

Siehe 7 Rs.

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, in der die Rollen und Verantwortlichkeiten aller an Migrationsaktivitäten und Cloud-Operationen beteiligten Parteien definiert werden. Der Matrixname wird aus den in der Matrix

definierten Verantwortungstypen abgeleitet: verantwortlich (R), rechenschaftspflichtig (A), konsultiert (C) und informiert (I). Der Support-Typ (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.

Außerbetriebnahme

Siehe 7 Rs.

Drehung

Der Prozess der regelmäßigen Aktualisierung eines Secrets, um es einem Angreifer zu erschweren, auf die Anmeldeinformationen zuzugreifen.

Zeilen- und Spaltenzugriffskontrolle (RCAC)

Die Verwendung grundlegender, flexibler SQL-Ausdrücke, für die Zugriffsregeln definiert sind. RCAC besteht aus Zeilenberechtigungen und Spaltenmasken.

RPO

Siehe Recovery Point Objective .

RTO

Siehe Recovery Time Objective .

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. Dieses Feature ermöglicht verbundenes Single Sign-On (SSO), sodass Benutzer sich bei der AWS Management Console anmelden oder die AWS-API-Operationen aufrufen können, ohne dass Sie in IAM einen Benutzer für jeden 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.

SCP

Siehe Service-Kontrollrichtlinie .

Secret

In vertrauliche AWS Secrets Manageroder eingeschränkte Informationen, wie ein Passwort oder Benutzeranmeldeinformationen, die Sie in verschlüsselter Form speichern. Sie besteht aus dem Secret-Wert und seinen Metadaten. Der Secret-Wert kann binär, eine einzelne Zeichenfolge oder mehrere Zeichenfolgen sein. Weitere Informationen finden Sie unter Secret in der Secrets-Manager-Dokumentation.

Sicherheitskontrolle

Ein technischer oder administrativer Integritätsschutz, der die Fähigkeit eines Bedrohungsakteurs, eine Schwachstelle auszunutzen, verhindert, erkennt oder einschränkt. Es gibt vier Haupttypen von Sicherheitskontrollen: präventive , detektivische , reaktive und proaktive .

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 der Sicherheitsantwort

Eine vordefinierte und geprogrammete Aktion, die darauf ausgelegt ist, automatisch auf ein Sicherheitsereignis zu reagieren oder es zu beheben. Diese Automatisierungen dienen als detektivische oder reaktive 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-Instance oder das Rotieren von Anmeldeinformationen.

Serverseitige Verschlüsselung

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

Service-Kontrollrichtlinie (SCP)

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

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.

Indikator auf Serviceebene (SLI)

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

Service Level Objective (SLO)

Eine Zielmetrik, die den Zustand eines Services darstellt, gemessen durch einen Indikator auf Serviceebene .

Modell der geteilten Verantwortung

Ein Modell, das die Verantwortung beschreibt, die Sie mit AWS für die Sicherheit der Cloud und die Einhaltung der Vorschriften teilen. AWS ist für die Sicherheit der Cloud zuständig, während Sie für die Sicherheit in der Cloud verantwortlich sind. Weitere Informationen finden Sie unter Modell der geteilten Verantwortung.

SIEM

Siehe Sicherheitsinformationen und Ereignisverwaltungssystem .

Single Point of Failure (SPOF)

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

SLA

Siehe Service Level Agreement .

SLI

Siehe Indikator auf Serviceebene .

SLO

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 im AWS Cloud.

SPOF

Siehe einzelne Fehlerquelle .

Sternschema

Eine Datenbankorganisationsstruktur, 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.

Symmetrische Verschlüsselung

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

synthetische Tests

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

T

tags

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

Zielvariable

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

Aufgabenliste

Ein Tool, das verwendet wird, um den Fortschritt anhand eines Runbooks zu verfolgen. Eine Aufgabenliste enthält eine Übersicht über das Runbook und eine Liste mit allgemeinen Aufgaben, die erledigt werden müssen. Für jede allgemeine Aufgabe werden der geschätzte Zeitaufwand, der Eigentümer und der Fortschritt angegeben.

Testumgebungen

Siehe Umgebung .

Training

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

Transit-Gateway

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

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

Erteilen von Berechtigungen für einen Service, den Sie für die Ausführung von Aufgaben in AWS Organizations und in ihren Konten und in Ihrem Namen in Ihrer Organisation angeben. 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 unter Verwenden von AWS Organizations mit anderen AWS-Services in der AWS Organizations-Dokumentation.

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 Pzzas 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

Arbeit, die auch als „schwere Arbeit“ bezeichnet wird, die erforderlich ist, um eine Anwendung zu erstellen und zu betreiben, aber dem Endbenutzer keinen direkten Wert bietet oder einen kompetitiven Vorteil bietet. Beispiele für undifferenzierte Aufgaben sind Beschaffung, Wartung und Kapazitätsplanung.

höhere Umgebungen

Siehe Umgebung .

V

Vacuuming

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

Versionskontrolle

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

VPC-Peering

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

Schwachstelle

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

Warm-Daten

Daten, auf die selten zugegriffen wird. Bei Abfragen 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, z. B. die Berechnung eines gleitenden Durchschnitts oder den Zugriff auf den Wert von Zeilen basierend auf 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.

WORM

Siehe einmal schreiben, viele lesen.

WQF

Weitere Informationen finden Sie unter AWS Workload Qualification Framework.

Einmal schreiben, viele lesen (WORM)

Ein Speichermodell, das Daten einmalig 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-Exploits

Ein Angriff, in der Regel Malware, der eine Zero-Day-Schwachstelle nutzt.

Zero-Day-Schwachstelle

Ein nicht behobener Fehler oder eine Schwachstelle in einem Produktionssystem. Bedrohungsakteure können diese Art von Schwachstelle verwenden, um das System anzugreifen. Entwickler werden häufig aufgrund des Angriffs auf die Schwachstelle aufmerksam.

Zombie-Anwendung

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

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.