AWS Sicherheitsgrundlagen beim Systemstart

AWS Präskriptive Leitlinien

AWS Präskriptive Leitlinien: AWS Sicherheitsgrundlagen beim Systemstart

Table of Contents

AWS Sicherheitsgrundlagen beim Start

Amazon Web Services (Mitwirkende)

Mai 2023 (Dokumentverlauf)

Die AWS Startup Security Baseline (AWS SSB) besteht aus einer Reihe von Kontrollen, die eine Mindestgrundlage schaffen, auf der Unternehmen sicher aufbauen können, AWS 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 ihre Reise im 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 im AWS SSB sind in zwei Kategorien unterteilt: Konto und Arbeitslast. Kontokontrollen tragen dazu bei, dass Sie AWS-Konto sicher sind. 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

AWS Well-Architected unterstützt Cloud-Architekten beim Aufbau einer sicheren, leistungsstarken, belastbaren und effizienten Infrastruktur für ihre Anwendungen und Workloads. Die AWS Startup Security Baseline orientiert sich an 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 behördlichen Anforderungen zu erfüllen, indem Sie die aktuellen Empfehlungen befolgen. AWS

Sie können überprüfen, ob Sie die Best Practices von Well-Architected einhalten, indem Sie die AWS Well-Architected Toolin Ihrem. AWS-Konto

Sicherheit und Compliance liegen in der gemeinsamen Verantwortung des Kunden AWS . Das Modell der gemeinsamen Verantwortung wird häufig so beschrieben, dass AWS es für die Sicherheit der Cloud verantwortlich ist (d. h. für den Schutz der Infrastruktur, auf der alle in der Cloud angebotenen Dienste ausgeführt werden AWS Cloud), und dass Sie für die Sicherheit in der Cloud verantwortlich sind (abhängig von den von Ihnen ausgewählten AWS Cloud Diensten). 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 zur Sicherheit Ihres AWS Kontos bei. Der Schwerpunkt liegt auf der Verwendung von AWS Identity and Access Management (IAM-) Benutzern, Benutzergruppen und Rollen (auch als Principals bezeichnet) sowohl für den menschlichen als auch für den Maschinenzugriff, wodurch die Verwendung des Root-Benutzers eingeschränkt wird und eine mehrstufige Authentifizierung erforderlich ist. In diesem Abschnitt bestätigen Sie, dass das Unternehmen über die Kontaktinformationen AWS verfügt, die erforderlich sind, um Sie bezüglich Ihrer Kontoaktivität und Ihres Kontostatus zu erreichen. Sie richten auch Überwachungsdienste wie Amazon GuardDuty und ein AWS Trusted Advisor AWS Budgets, sodass Sie über Aktivitäten in Ihrem Konto informiert werden und schnell reagieren können, wenn die Aktivität nicht autorisiert oder unerwartet ist.

In diesem Abschnitt werden folgende Themen behandelt:

ACCT.01 Richten Sie Kontakte auf Kontoebene für gültige E-Mail-Verteilerlisten ein

Verwenden Sie beim Einrichten von primären und alternativen Kontakten für Ihr AWS Konto eine E-Mail-Verteilerliste anstelle der E-Mail-Adresse einer Einzelperson. 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 Abrechnungs-, 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 darauf haben.

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

1. Melden Sie sich auf der Seite Kontoeinstellungen in der Billing and Cost Management-Konsole 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 Sie die Nutzung des Root-Benutzers

Der Root-Benutzer wird erstellt, wenn Sie sich für ein AWS Konto registrieren. Dieser Benutzer hat alle 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, für die Root-Benutzeranmeldedaten erforderlich sind (IAM-Dokumentation). 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 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 Sie den Konsolenzugriff für jeden Benutzer.

ACCT.03 Konfigurieren Sie den Konsolenzugriff für jeden Benutzer

AWS Empfiehlt als bewährte Methode, temporäre Anmeldeinformationen zu verwenden, um Zugriff auf und Ressourcen zu AWS-Konten 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).

AWS Empfiehlt menschlichen Benutzern, föderierte Identitäten von einem zentralen Identitätsanbieter (IdP) wie AWS IAM Identity Center Okta, Active Directory oder Ping Identity zu verwenden. Durch das Zusammenführen von Benutzern können Sie Identitäten an einem einzigen, zentralen Ort definieren, und Benutzer können sich sicher bei mehreren Anwendungen und Websites authentifizieren AWS, auch mit nur einem Satz von Anmeldeinformationen. Weitere Informationen finden Sie unter AWS Identitätsverbund in IAM Identity Center (Website).AWS

> **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 Identitätsanbieter und Verbund (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, diesen Benutzern nur die Berechtigungen zu gewähren, die sie für die Ausführung der Aufgabe benötigen, und diese Benutzer zu 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 anhängen. Dabei handelt es sich um eigenständige Richtlinien, die entwickelt wurden, AWS um Berechtigungen für viele gängige 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, was Benutzer, die vom IdP Ihrer Organisation authentifiziert wurden, tun 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 Entwicklungsingenieure (DevOps). 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. Ordnen Sie einer IAM-Benutzergruppe eine AWS verwaltete Richtlinie zu (IAM-Dokumentation).

ACCT.05 Für die Anmeldung ist eine Multi-Faktor-Authentifizierung erforderlich

Mit der Multi-Faktor-Authentifizierung (MFA) verfügen Benutzer über ein Gerät, das eine Antwort auf eine Authentifizierungsherausforderung generiert. Die Anmeldeinformationen und die vom Gerät generierte Antwort jedes Benutzers sind erforderlich, um den Anmeldevorgang abzuschließen.

Aktivieren Sie als bewährte Methode zur Sicherheit MFA für den AWS-Konto -Zugriff, insbesondere für langfristige Anmeldeinformationen wie Root-Benutzer und IAM-Benutzer.

So richten Sie MFA für den Root-Benutzer ein

1. Melden Sie sich an der AWS Management Console an.
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 AWS Multi-Faktor-Authentifizierung in IAM (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 Anmeldeinformationen bei der IAM-Konsole 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 IAM-Konsole an AWS Management Console und öffnen Sie sie.
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 AWS Multi-Faktor-Authentifizierung in IAM (IAM-Dokumentation).

ACCT.06 Eine Passwortrichtlinie durchsetzen

Benutzer melden sich bei der an, AWS Management Console indem sie Anmeldeinformationen angeben. 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 IAM-Konsole an AWS Management Console und öffnen Sie sie.
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 Übermitteln Sie CloudTrail Protokolle an einen geschützten S3-Bucket

Aktionen von Benutzern, Rollen und Diensten 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 Reagieren auf Kontoaktivitäten in

Ihrer gesamten AWS Infrastruktur finden Sie unter Ereignisse mit CloudTrail Ereignisverlauf anzeigen (CloudTrail Dokumentation).

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

Um einen Trail zu erstellen, der Logs 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. Dadurch werden alle AWS Key Management Service (AWS KMS) Ereignisse von deinem Trail ausgeschlossen. AWS KMS Leseaktionen wie`Encrypt`,`Decrypt`, und `GenerateDataKey` können eine große Anzahl von Ereignissen erzeugen.

    Wählen Sie für Produktionsumgebungen die Option Protokollierung von Schreiben-Verwaltungsereignissen und das Kontrollkästchen für Ausschließen von AWS KMS -Ereignissen aus. Dies schließt umfangreiche AWS KMS Leseereignisse aus, protokolliert aber dennoch relevante Schreibereignisse wie `DisableDelete`, und. `ScheduleKey` Dies sind die empfohlenen AWS KMS Mindestprotokollierungseinstellungen für eine Produktionsumgebung.

2. Der neue Trail wird auf der Seite Trails angezeigt. Veröffentlicht in etwa 15 Minuten Protokolldateien CloudTrail , in denen die API-Aufrufe (AWS Application Programming Interface) aufgeführt sind, die in Ihrem Konto getätigt wurden. Sie können die Protokolldateien in dem von Ihnen angegebenen S3-Bucket anzeigen.

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

1. Lesen Sie die Amazon S3 S3-Bucket-Richtlinie (CloudTrail Dokumentation) für alle Buckets, in denen Sie Protokolldateien speichern, und passen Sie sie nach Bedarf an, um unnötigen Zugriff zu verhindern.
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 S3-Buckets zum Speichern der Protokolldateien für einen Organization Trail (CloudTrail Dokumentation).

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

ACCT.08 Verhindern Sie den öffentlichen Zugriff auf private S3-Buckets

Standardmäßig haben nur der Root-Benutzer AWS-Konto und der IAM-Prinzipal, falls er verwendet wird, Lese- und Schreibberechtigungen für Amazon S3 S3-Buckets, die von diesem Principal 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 future 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 einen gelben Befund für S3-Buckets, die Listen- oder Lesezugriff für die Öffentlichkeit ermöglichen, und generiert einen roten Befund für Buckets, die öffentliche Uploads oder Löschungen zulassen. Folgen Sie als Ausgangsbasis der Steuerung ACCT.12 Überwachen Sie Probleme mit hohem Risiko und lösen Sie diese, indem Sie Trusted Advisor, um falsch konfigurierte Buckets zu identifizieren und zu korrigieren. Öffentlich zugängliche S3-Buckets werden auch in der Amazon-S3-Konsole angezeigt.

ACCT.09 Löscht ungenutzte Subnetze und Sicherheitsgruppen VPCs

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

Wenn sie nicht verwendet werden, löschen Sie die Standardeinstellung 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 auf der Amazon EC2 Global View-Konsole anzeigen. Weitere Informationen finden Sie unter Regionsübergreifendes Auflisten und Filtern von Ressourcen mithilfe von Amazon EC2 Global View (EC2Amazon-Dokumentation).

Um ungenutzte Standardwerte zu löschen VPCs

1. Löschen Ihrer VPC (Amazon-PC-Dokumentation).
2. Wiederholen Sie den Vorgang nach Bedarf für VPCs andere Regionen.

ACCT.10 So konfigurieren AWS Budgets , dass Ihre Ausgaben überwacht werden

AWS Budgets ermöglichen die Überwachung der monatlichen Kosten und der Nutzung mit Benachrichtigungen, wenn die Kosten voraussichtlich die Zielschwellenwerte überschreiten werden. Benachrichtigungen über prognostizierte Kosten können Hinweise auf unerwartete Aktivitäten geben AWS Trusted Advisor und bieten zusätzlichen Schutz zusätzlich zu anderen Überwachungssystemen wie Amazon GuardDuty. Zu einer guten Betriebshygiene gehört auch die Überwachung und das Verständnis Ihrer AWS Kosten.

Um ein Budget aufzustellen in AWS Budgets

- Erstellen Sie ein Kostenbudget (AWS Budgets Dokumentation).

ACCT.11 Benachrichtigungen aktivieren und darauf reagieren GuardDuty

Amazon GuardDuty ist ein Service zur Bedrohungserkennung, der kontinuierlich nach bösartigem oder unberechtigtem Verhalten sucht, um Ihre AWS Konten, Workloads und Daten zu schützen. Wenn der Service unerwartete und potenziell bösartige Aktivitäten entdeckt, GuardDuty liefert er detaillierte Sicherheitsinformationen, die für Transparenz und Problembehebung sorgen. GuardDuty kann Bedrohungen wie Cryptocurrency-Mining-Aktivitäten, Zugriffe von Tor-Clients und -Relays, unerwartetes Verhalten und kompromittierte IAM-Anmeldeinformationen erkennen. Aktiviere GuardDuty und reagiere auf Ergebnisse, um potenziell bösartiges oder unberechtigtes Verhalten in deiner Umgebung zu unterbinden. AWS Weitere Informationen zu Ergebnissen in GuardDuty finden Sie unter Suchtypen (GuardDuty Dokumentation).

Sie können Amazon CloudWatch Events verwenden, um automatische Benachrichtigungen einzurichten, wenn ein Ergebnis GuardDuty erstellt wird 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 Ergebnisse ein, und die Ereignisregel benachrichtigt die Endpunkte im Amazon SNS SNS-Thema.

Zur Aktivierung und Benachrichtigungen GuardDuty GuardDuty

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

ACCT.12 Überwachen Sie Probleme mit hohem Risiko und lösen Sie diese, indem Sie Trusted Advisor

AWS Trusted Advisor scannt Ihre AWS Infrastruktur passiv auf risikoreiche oder schwerwiegende Probleme in Bezug auf 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 AWS Trusted Advisor Sie in der Prüfreferenz (Dokumentation)Trusted Advisor .

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

Um Probleme zu sehen in Trusted Advisor

- Überprüfen Sie jede Prüfkategorie gemäß den Anweisungen unter Prüfkategorien anzeigen (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 behandelt:

- WKLD.01 Verwenden Sie IAM-Rollen für Berechtigungen in der Rechenumgebung
- WKLD.02 Beschränken Sie den Umfang der Nutzung von Anmeldeinformationen mit ressourcenbasierten Richtlinienberechtigungen
- WKLD.03 Verwenden Sie kurzlebige Geheimnisse oder einen Dienst zur Verwaltung von Geheimnissen
- WKLD.04 Verhindern Sie, dass Anwendungsgeheimnisse preisgegeben werden
- WKLD.05 Enthüllte Geheimnisse erkennen und korrigieren
- WKLD.06 Systems Manager anstelle von SSH oder RDP verwenden
- WKLD.07 Datenereignisse für S3-Buckets mit sensiblen Daten protokollieren
- WKLD.08 Amazon EBS-Volumes verschlüsseln
- WKLD.09 Amazon RDS-Datenbanken verschlüsseln
- WKLD.10 Stellen Sie private Ressourcen in privaten Subnetzen bereit
- WKLD.11 Beschränken Sie den Netzwerkzugriff mithilfe von Sicherheitsgruppen
- WKLD.12 Verwenden Sie VPC-Endpunkte, um auf unterstützte Dienste zuzugreifen
- WKLD.13 Erfordert HTTPS für alle öffentlichen Web-Endpunkte
- WKLD.14 Verwenden Sie Edge-Protection-Dienste für öffentliche Endgeräte
- WKLD.15 Definieren Sie Sicherheitskontrollen in Vorlagen und implementieren Sie sie mithilfe von CI/CD-Methoden

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

In AWS Identity and Access Management (IAM) stellt eine Rolle eine Reihe von Berechtigungen dar, die von einer Person oder einem Dienst 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 Rechendiensten, sofern diese unterstützt werden, direkt eine IAM-Rolle zu. Anwendungen, die ein AWS SDK verwenden und in diesen Rechenumgebungen ausgeführt werden, verwenden automatisch die Anmeldeinformationen der IAM-Rolle 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 (EC2 Amazon-Dokumentation)
- IAM-Rollen für Aufgaben (Dokumentation für Amazon Elastic Container Service)
- Lambda-Ausführungsrolle (Lambda-Dokumentation)

WKLD.02 Beschränken Sie den Umfang 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 Berechtigungen der Prinzipal in der Umgebung hat. AWS
- 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:

- Beschränken Sie den Zugriff nur auf Prinzipale in einer bestimmten Organisation (definiert in AWS Organizations), indem Sie die Bedingung verwenden. `aws:PrincipalOrgID`
- 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 Dienst zur Verwaltung von Geheimnissen

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 Dienst zur Verwaltung von Geheimnissen empfehlen wir die Verwendung einer Kombination aus Parameter Store, einer Funktion von und: AWS Systems Manager 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 Schlüssel AWS Key Management Service (AWS KMS), um das Geheimnis zu verschlüsseln. 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 verwenden APIs , 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 Manager-Dokumentation). Geheimnisse im Parameter Store verwenden den `SecureString`-Datentyp.

3. Rufen Sie in Ihrer Anwendung mithilfe des AWS SDK für Ihre Programmiersprache einen Parameter aus dem Parameter Store ab. Codebeispiele finden Sie unter GetParameter(AWS SDK-Codebibliothek).

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, den Artikel Verwenden Sie AWS Secrets Manager clientseitige Caching-Bibliotheken, um die Verfügbarkeit und Latenz bei der Verwendung Ihrer Geheimnisse zu verbessern (AWS Blogbeitrag) zu lesen. Die Verwendung von clientseitig SDKs, für die bereits Best Practices implementiert wurden, sollte die Verwendung und Integration von Secrets Manager beschleunigen und vereinfachen.

WKLD.04 Verhindern Sie, dass Anwendungsgeheimnisse preisgegeben 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 (Repository) GitHub
- Whispers (Repositorium) GitHub
- detect-secrets (Aufbewahrungsort) GitHub
- git-secrets (Repositorium) GitHub
- TruffleHog(Endlager) GitHub

WKLD.05 Enthüllte Geheimnisse erkennen und korrigieren

Im WKLD.03 Verwenden Sie kurzlebige Geheimnisse oder einen Dienst zur Verwaltung von Geheimnissen und WKLD.04 Verhindern Sie, dass Anwendungsgeheimnisse preisgegeben 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 in 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 preisgegeben werden Funktionen zur Erkennung vorhandener Geheimnisse.

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

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

WKLD.06 Systems Manager anstelle von SSH oder RDP verwenden

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 mithilfe der Session Manager-Funktion von AWS Systems Manager entweder über AWS Command Line Interface (AWS CLI) oder remote auf die Instanzen zugreifen. AWS Management Console Anschließend können Sie die Konsole AWS CLI oder verwenden, um eine Sitzung zu starten, die über einen sicheren Tunnel eine Verbindung mit der Instance herstellt, sodass Sie keine zusätzlichen Anmeldeinformationen verwalten müssen, die für Secure Shell (SSH) oder Windows Remote Desktop Protocol (RDP) verwendet werden.

Verwenden Sie den Sitzungsmanager, anstatt EC2 Instanzen in öffentlichen Subnetzen auszuführen, Jumpboxen auszuführen oder Bastion-Hosts auszuführen.

Session Manager einrichten

1. Stellen Sie sicher, dass die EC2 Instance das neueste Betriebssystem Amazon Machine Images (AMIs) verwendet, z. B. Amazon Linux oder Ubuntu. 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 **<Region>** mit diesen Adressen verbunden ist (ersetzen Sie sie durch die entsprechenden AWS-Region Adressen):
   a. `ec2messages.<Region>.amazonaws.com`
   b. `ssm.<Region>.amazonaws.com`
   c. `ssmmessages.<Region>.amazonaws.com`
3. Ordnen Sie die AWS verwaltete Richtlinie der IAM-Rolle `AmazonSSMManagedInstanceCore` zu, die Ihren Instances zugeordnet ist.

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

Eine Sitzung starten

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

WKLD.07 Datenereignisse für S3-Buckets mit sensiblen Daten protokollieren

AWS CloudTrail Erfasst standardmäßig Verwaltungsereignisse, Ereignisse, die Ressourcen in Ihrem Konto erstellen, ändern oder löschen. 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. Wird verwendet CloudTrail , um Datenereignisse für alle S3-Buckets zu protokollieren, 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 an AWS Management Console und öffnen Sie die Konsole 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 Bewährte Methoden für die Amazon EBS-Verschlüsselung, die Sie unbedingt kennen müssen (AWS Blogbeitrag).

Verschlüsselung von Amazon-EBS-Volumes

- Aktivieren Sie die Verschlüsselung standardmäßig (Amazon EBS-Dokumentation).

WKLD.09 Amazon RDS-Datenbanken verschlüsseln

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 Datenbank-Instance (Amazon-RDS-Dokumentation).

WKLD.10 Stellen Sie private Ressourcen in privaten Subnetzen bereit

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 NAT-Gateway oder eine EC2 Instanz, auf der NAT-Prozesse in einem öffentlichen Subnetz ausgeführt werden, einer Network AWS Address Translation (NAT) unterzogen werden. 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 die automatische Zuweisung einer öffentlichen IPv4 Adresse.
- Wenn Sie private EC2 Instanzen erstellen, deaktivieren Sie die automatische Zuweisung öffentlicher IP-Adressen. 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.

WKLD.11 Beschränken Sie den Netzwerkzugriff mithilfe von Sicherheitsgruppen

Verwenden Sie Sicherheitsgruppen, um den Datenverkehr zu EC2 Instances, RDS-Datenbanken und anderen unterstützten Ressourcen zu kontrollieren. 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 Amazon RDS for MySQL MySQL-Datenbank 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)

Sicherheitsgruppe	Regeln für eingehenden Datenverkehr	Regeln für ausgehenden Datenverkehr
EC2 Instanz-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 Instanz zulassen Typ: MySQL Quelle: Sicherheitsgruppe der EC2 Instanz	Keine Regeln für ausgehenden Datenverkehr

WKLD.12 Verwenden Sie VPC-Endpunkte, um auf unterstützte Dienste zuzugreifen

In: Ressourcen VPCs, die auf andere externe Dienste zugreifen AWS müssen, benötigen entweder eine Route zum Internet (`0.0.0.0/0`) oder zur öffentlichen IP-Adresse des Zieldienstes. Verwenden Sie VPC-Endpunkte, um eine private IP-Route von Ihrer VPC zu unterstützten AWS oder anderen Diensten zu aktivieren, sodass Sie kein Internet-Gateway, ein NAT-Gerät, eine VPN-Verbindung (Virtual Private Network) oder eine Verbindung verwenden müssen. AWS Direct Connect

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 nur auf 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 Region enthalten sind. Für sie fallen keine zusätzlichen Kosten an. Schnittstellenendpunkte werden empfohlen, wenn ein erweiterbarer Zugriff erforderlich ist, z. B. auf einen S3-Bucket von einem anderen VPCs, von lokalen Netzwerken oder von einem anderen aus. AWS-Regionen Für Schnittstellenendpunkte fallen stündliche Verfügbarkeitsgebühren und Datenverarbeitungsgebühren pro GB an, die beide niedriger sind als die jeweiligen Gebühren für das Senden der Daten über das NAT Gateway. `0.0.0.0/0` AWS

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

- Weitere Informationen zur Auswahl zwischen Gateway- und Schnittstellenendpunkten für Amazon S3 finden Sie unter Choosing Your VPC Endpoint Strategy for Amazon S3 (AWS Blogbeitrag).
- Zugriff und AWS-Service Verwendung eines VPC-Endpunkts mit Schnittstelle (Amazon VPC-Dokumentation).
- Gateway-Endpunkte (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 Erfordert HTTPS für alle öffentlichen Web-Endpunkte

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 Dienste stellen öffentliche Web-Endpunkte für Ihre Ressourcen bereit, z. B. Amazon AWS Elastic Beanstalk 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 Wissenszentrum)
- Classic Load Balancer (AWS Wissenszentrum)
- Amplify (Amplify-Dokumentation)

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

CloudFront Zur Bereitstellung einer statischen Website, die auf Amazon S3 gehostet wird

1. Wird verwendet CloudFront , um eine statische Website bereitzustellen, die auf Amazon S3 (AWS Knowledge Center) gehostet wird.
2. Wenn Sie den Zugriff auf einen öffentlichen S3-Bucket konfigurieren, benötigen Sie HTTPS zwischen Zuschauern und CloudFront (CloudFrontDokumentation).

   Wenn Sie den Zugriff auf einen privaten S3-Bucket konfigurieren, beschränken Sie den Zugriff auf Amazon S3 S3-Inhalte mithilfe einer ursprünglichen Zugriffsidentität (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 Chiffren zwischen Zuschauern und CloudFront (Dokumentation) CloudFront

WKLD.14 Verwenden Sie Edge-Protection-Dienste für öffentliche Endgeräte

Verwenden Sie einen Edge-Protection-Dienst, anstatt den Datenverkehr direkt von Computerdiensten wie EC2 Instances oder Containern aus bereitzustellen. 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 Zu den Diensten, die öffentlichen Endpunktschutz bieten können AWS WAF CloudFront, gehören 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 Layer-3- und Layer-4-Distributed-Denial-of-Service (DDoS) -Angriffen und AWS WAF können vor Layer-7-Angriffen schützen.

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

- Erste Schritte mit AWS WAF (AWS Website)
- 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 Sie Sicherheitskontrollen in Vorlagen und implementieren Sie sie 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-Dienste wie AWS CloudFormation, unterstützen sowohl identitätsbasierte als auch ressourcenbasierte IAM-Richtlinien und unterstützen AWS Sicherheitsdienste wie Amazon und Amazon GuardDuty VPC. AWS WAF 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 on finden Sie in der Dokumentation. AWSAWS Cloud Development Kit (AWS CDK)

Mitwirkende

Zu den Mitwirkenden an diesem Dokument gehören:

- Jay Michael, Principal Solutions Architect (Hauptautor)
- 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 Öffentlichen Zugriff auf private S3-Buckets verhindern aktualisiert, um zu berücksichtigen, dass Amazon S3 S3-Buckets, die nach dem 28. April 2023 erstellt wurden, die Einstellung Öffentlichen Zugriff blockieren standardmäßig aktiviert ist.	18. Mai 2023
Bewährte IAM-Sicherheitsmethoden	Wir haben diesen Leitfaden aktualisiert, um ihn an die neuesten Best Practices AWS Identity and Access Management (IAM) anzupassen. Weitere Informationen finden Sie unter Bewährte Sicherheitsmethoden in der IAM-Dokumentation.	1. Februar 2023
IAM-Rollen	Im Abschnitt WKLD.01 Verwenden von IAM-Rollen für Berechtigungen zur Rechenumgebung haben wir zusätzliche Links zur AWS-Service Dokumentation 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

AWS Glossar zu präskriptiven Leitlinien

Die folgenden Begriffe werden häufig in Strategien, Leitfäden und Mustern von AWS Prescriptive Guidance verwendet. Um Einträge vorzuschlagen, verwenden Sie bitte den Link Feedback geben am Ende des Glossars.

Zahlen

7 Rs

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

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

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

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

A

ABAC

Siehe attributbasierte Zugriffskontrolle.

abstrahierte Dienste

Weitere Informationen finden Sie unter Managed Services.

ACID

Siehe Atomarität, Konsistenz, Isolierung und Haltbarkeit.

Aktiv-Aktiv-Migration

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

Aktiv-Passiv-Migration

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

Aggregatfunktion

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

AI

Siehe künstliche Intelligenz.

AIOps

Siehe Operationen im Bereich künstliche Intelligenz.

Anonymisierung

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

Anti-Muster

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

Anwendungssteuerung

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

Anwendungsportfolio

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

künstliche Intelligenz (KI)

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

Operationen mit künstlicher Intelligenz (AIOps)

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

Asymmetrische Verschlüsselung

Ein Verschlüsselungsalgorithmus, der ein Schlüsselpaar, einen öffentlichen Schlüssel für die Verschlüsselung und einen privaten Schlüssel für die Entschlüsselung verwendet. Sie können den

öffentlichen Schlüssel teilen, da er nicht für die Entschlüsselung verwendet wird. Der Zugriff auf den privaten Schlüssel sollte jedoch stark eingeschränkt sein.

Atomizität, Konsistenz, Isolierung, Haltbarkeit (ACID)

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

Attributbasierte Zugriffskontrolle (ABAC)

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

autoritative Datenquelle

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

Availability Zone

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

AWS Framework für die Cloud-Einführung (AWS CAF)

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

AWS Workload-Qualifizierungsrahmen (AWS WQF)

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

B

schlechter Bot

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

BCP

Siehe Planung der Geschäftskontinuität.

Verhaltensdiagramm

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

Big-Endian-System

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

Binäre Klassifikation

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

Bloom-Filter

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

Blau/Grün-Bereitstellung

Eine Bereitstellungsstrategie, bei der Sie zwei separate, aber identische Umgebungen erstellen. Sie führen die aktuelle Anwendungsversion in einer Umgebung (blau) und die neue

Anwendungsversion in der anderen Umgebung (grün) aus. Mit dieser Strategie können Sie schnell und mit minimalen Auswirkungen ein Rollback durchführen.

Bot

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

Botnetz

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

branch

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

Zugang durch Glasbruch

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

Brownfield-Strategie

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

Puffer-Cache

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

Geschäftsfähigkeit

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

Planung der Geschäftskontinuität (BCP)

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

C

CAF

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

Bereitstellung auf Kanaren

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

CCoE

Weitere Informationen finden Sie im Cloud Center of Excellence.

CDC

Siehe Erfassung von Änderungsdaten.

Erfassung von Datenänderungen (CDC)

Der Prozess der Nachverfolgung von Änderungen an einer Datenquelle, z. B. einer Datenbanktabelle, und der Aufzeichnung von Metadaten zu der Änderung. Sie können CDC für verschiedene Zwecke verwenden, z. B. für die Prüfung oder Replikation von Änderungen in einem Zielsystem, um die Synchronisation aufrechtzuerhalten.

Chaos-Technik

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

CI/CD

Siehe Continuous Integration und Continuous Delivery.

Klassifizierung

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

clientseitige Verschlüsselung

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

Cloud-Exzellenzzentrum (CCoE)

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

Cloud Computing

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

Cloud-Betriebsmodell

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

Phasen der Einführung der Cloud

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

- Projekt – Durchführung einiger Cloud-bezogener Projekte zu Machbarkeitsnachweisen und zu Lernzwecken
- Fundament — Tätigen Sie grundlegende Investitionen, um Ihre Cloud-Einführung zu skalieren (z. B. Einrichtung einer landing zone, Definition eines CCo E, Einrichtung eines Betriebsmodells)

- Migration – Migrieren einzelner Anwendungen
- Neuentwicklung – Optimierung von Produkten und Services und Innovation in der Cloud

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

CMDB

Siehe Datenbank für das Konfigurationsmanagement.

Code-Repository

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

Kalter Cache

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

Kalte Daten

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

Computer Vision (CV)

Ein Bereich der KI, der maschinelles Lernen nutzt, um Informationen aus visuellen Formaten wie digitalen Bildern und Videos zu analysieren und zu extrahieren. Amazon SageMaker AI bietet beispielsweise Bildverarbeitungsalgorithmen für CV.

Drift in der Konfiguration

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

Verwaltung der Datenbankkonfiguration (CMDB)

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

Konformitätspaket

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

Kontinuierliche Bereitstellung und kontinuierliche Integration (CI/CD)

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

CV

Siehe Computer Vision.

D

Daten im Ruhezustand

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

Datenklassifizierung

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

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

Datendrift

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

Daten während der Übertragung

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

Datennetz

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

Datenminimierung

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

Datenperimeter

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

Vorverarbeitung der Daten

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

Herkunft der Daten

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

betroffene Person

Eine Person, deren Daten gesammelt und verarbeitet werden.

Data Warehouse

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

Datenbankdefinitionssprache (DDL)

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

Datenbankmanipulationssprache (DML)

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

DDL

Siehe Datenbankdefinitionssprache.

Deep-Ensemble

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

Deep Learning

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

defense-in-depth

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

delegierter Administrator

In AWS Organizations kann ein kompatibler Dienst ein AWS Mitgliedskonto registrieren, um die Konten der Organisation und die Berechtigungen für diesen Dienst zu verwalten. Dieses Konto

wird als delegierter Administrator für diesen Service bezeichnet. Weitere Informationen und eine Liste kompatibler Services finden Sie unter Services, die mit AWS Organizations funktionieren in der AWS Organizations -Dokumentation.

Bereitstellung

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

Entwicklungsumgebung

Siehe Umgebung.

Detektivische Kontrolle

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

Abbildung des Wertstroms in der Entwicklung (DVSM)

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

digitaler Zwilling

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

Maßtabelle

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

Katastrophe

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

Disaster Recovery (DR)

Die Strategie und der Prozess, die Sie verwenden, um Ausfallzeiten und Datenverluste aufgrund einer Katastrophe zu minimieren. Weitere Informationen finden Sie unter Disaster Recovery von Workloads unter AWS: Wiederherstellung in der Cloud im AWS Well-Architected Framework.

DML

Siehe Sprache zur Datenbankmanipulation.

Domainorientiertes Design

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

DR

Siehe Disaster Recovery.

Erkennung von Driften

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

DVSM

Siehe Abbildung des Wertstroms in der Entwicklung.

E

EDA

Siehe explorative Datenanalyse.

EDI

Siehe elektronischer Datenaustausch.

Edge-Computing

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

elektronischer Datenaustausch (EDI)

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

Verschlüsselung

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

Verschlüsselungsschlüssel

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

Endianismus

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

Endpunkt

Siehe Service-Endpunkt.

Endpunkt-Services

Ein Service, den Sie in einer Virtual Private Cloud (VPC) hosten können, um ihn mit anderen Benutzern zu teilen. Sie können einen Endpunktdienst mit anderen AWS-Konten oder AWS Identity and Access Management (IAM AWS PrivateLink -) Prinzipalen erstellen und diesen

Berechtigungen gewähren. Diese Konten oder Prinzipale können sich privat mit Ihrem Endpunktservice verbinden, indem sie Schnittstellen-VPC-Endpunkte erstellen. Weitere Informationen finden Sie unter Einen Endpunkt-Service erstellen in der Amazon Virtual Private Cloud (Amazon VPC)-Dokumentation.

Unternehmensressourcenplanung (ERP)

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

Envelope-Verschlüsselung

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

Umgebung

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

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

Epics

In der agilen Methodik sind dies funktionale Kategorien, die Ihnen helfen, Ihre Arbeit zu organisieren und zu priorisieren. Epics bieten eine allgemeine Beschreibung der Anforderungen und Implementierungsaufgaben. Zu den Sicherheitsthemen AWS von CAF gehören beispielsweise Identitäts- und Zugriffsmanagement, Detektivkontrollen, Infrastruktursicherheit,

Datenschutz und Reaktion auf Vorfälle. Weitere Informationen zu Epics in der AWS - Migrationsstrategie finden Sie im Leitfaden zur Programm-Implementierung.

ERP

Siehe Enterprise Resource Planning.

Explorative Datenanalyse (EDA)

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

F

Faktentabelle

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

schnell scheitern

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

Grenze zur Fehlerisolierung

Dabei handelt es sich um eine Grenze AWS Cloud, z. B. eine Availability Zone AWS-Region, eine Steuerungsebene oder eine Datenebene, die die Auswirkungen eines Fehlers begrenzt und die Widerstandsfähigkeit von Workloads verbessert. Weitere Informationen finden Sie unter Grenzen zur AWS Fehlerisolierung.

Feature-Zweig

Siehe Zweig.

Features

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

Bedeutung der Feature

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

Featuretransformation

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

Eingabeaufforderung mit wenigen Klicks

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

FGAC

Siehe detaillierte Zugriffskontrolle.

Feinkörnige Zugriffskontrolle (FGAC)

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

Flash-Cut-Migration

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

FM

Siehe Fundamentmodell.

Fundamentmodell (FM)

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

G

generative KI

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

Geoblocking

Siehe geografische Einschränkungen.

Geografische Einschränkungen (Geoblocking)

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

Gitflow-Workflow

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

goldenes Bild

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

Greenfield-Strategie

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

Integritätsschutz

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

H

HEKTAR

Siehe Hochverfügbarkeit.

Heterogene Datenbankmigration

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

hohe Verfügbarkeit (HA)

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

historische Modernisierung

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

Holdout-Daten

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

Homogene Datenbankmigration

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

heiße Daten

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

Hotfix

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

Hypercare-Phase

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

I

IaC

Sehen Sie sich Infrastruktur als Code an.

Identitätsbasierte Richtlinie

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

Leerlaufanwendung

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

IIoT

Siehe Industrielles Internet der Dinge.

unveränderliche Infrastruktur

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

Eingehende (ingress) VPC

In einer Architektur AWS mit mehreren Konten ist dies eine VPC, die Netzwerkverbindungen von außerhalb einer Anwendung akzeptiert, überprüft und weiterleitet. Die AWS Security Reference Architecture empfiehlt, Ihr Netzwerkkonto mit eingehendem und ausgehendem Datenverkehr und Inspektion einzurichten, VPCs um die bidirektionale Schnittstelle zwischen Ihrer Anwendung und dem Internet im weiteren Sinne zu schützen.

Inkrementelle Migration

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

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

Industrie 4.0

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

Infrastruktur

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

Infrastructure as Code (IaC)

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

industrielles Internet der Dinge (T) IIo

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

Inspektions-VPC

In einer Architektur AWS mit mehreren Konten eine zentralisierte VPC, die Inspektionen des Netzwerkverkehrs zwischen VPCs (in demselben oder unterschiedlichen AWS-Regionen), dem Internet und lokalen Netzwerken verwaltet. In der AWS Security Reference Architecture wird empfohlen, Ihr Netzwerkkonto mit eingehendem und ausgehendem Datenverkehr sowie Inspektionen einzurichten, VPCs um die bidirektionale Schnittstelle zwischen Ihrer Anwendung und dem Internet im weiteren Sinne zu schützen.

Internet of Things (IoT)

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

Interpretierbarkeit

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

IoT

Siehe Internet der Dinge.

IT information library (ITIL, IT-Informationsbibliothek)

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

T service management (ITSM, IT-Servicemanagement)

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

BIS

Weitere Informationen finden Sie in der IT-Informationsbibliothek.

ITSM

Siehe IT-Servicemanagement.

L

Labelbasierte Zugangskontrolle (LBAC)

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

Landing Zone

Eine landing zone ist eine gut strukturierte AWS Umgebung mit mehreren Konten, die skalierbar und sicher ist. Dies ist ein Ausgangspunkt, von dem aus Ihre Organisationen Workloads und Anwendungen schnell und mit Vertrauen in ihre Sicherheits- und Infrastrukturumgebung starten

und bereitstellen können. Weitere Informationen zu Landing Zones finden Sie unter Einrichtung einer sicheren und skalierbaren AWS -Umgebung mit mehreren Konten..

großes Sprachmodell (LLM)

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

Große Migration

Eine Migration von 300 oder mehr Servern.

SCHWARZ

Weitere Informationen finden Sie unter Label-basierte Zugriffskontrolle.

Geringste Berechtigung

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

Lift and Shift

Siehe 7 Rs.

Little-Endian-System

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

LLM

Siehe großes Sprachmodell.

Niedrigere Umgebungen

Siehe Umgebung.

M

Machine Learning (ML)

Eine Art künstlicher Intelligenz, die Algorithmen und Techniken zur Mustererkennung und zum Lernen verwendet. ML analysiert aufgezeichnete Daten, wie z. B. Daten aus dem Internet der

Dinge (IoT), und lernt daraus, um ein statistisches Modell auf der Grundlage von Mustern zu erstellen. Weitere Informationen finden Sie unter Machine Learning.

Hauptzweig

Siehe Filiale.

Malware

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

verwaltete Dienste

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

Manufacturing Execution System (MES)

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

MAP

Siehe Migration Acceleration Program.

Mechanismus

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

Mitgliedskonto

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

DURCHEINANDER

Siehe Manufacturing Execution System.

Message Queuing-Telemetrietransport (MQTT)

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

Microservice

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

Microservices-Architekturen

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

Migration Acceleration Program (MAP)

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

Migration in großem Maßstab

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

Migrationsfabrik

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

Migrationsmetadaten

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

Migrationsmuster

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

Migration Portfolio Assessment (MPA)

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

Migration Readiness Assessment (MRA)

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

Migrationsstrategie

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

ML

Siehe maschinelles Lernen.

Modernisierung

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

Bewertung der Modernisierungsfähigkeit

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

Monolithische Anwendungen (Monolithen)

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

MPA

Siehe Bewertung des Migrationsportfolios.

MQTT

Siehe Message Queuing-Telemetrietransport.

Mehrklassen-Klassifizierung

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

veränderbare Infrastruktur

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

O

OAC

Siehe Origin Access Control.

OAI

Siehe Zugriffsidentität von Origin.

COM

Siehe organisatorisches Change-Management.

Offline-Migration

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

OI

Siehe Betriebsintegration.

OLA

Siehe Vereinbarung auf operativer Ebene.

Online-Migration

Eine Migrationsmethode, bei der der Quell-Workload auf das Zielsystem kopiert wird, ohne offline genommen zu werden. Anwendungen, die mit dem Workload verbunden sind, können während

der Migration weiterhin funktionieren. Diese Methode beinhaltet keine bis minimale Ausfallzeit und wird in der Regel für kritische Produktionsworkloads verwendet.

OPC-UA

Siehe Open Process Communications — Unified Architecture.

Offene Prozesskommunikation — Einheitliche Architektur (OPC-UA)

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

Vereinbarung auf Betriebsebene (OLA)

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

Überprüfung der Betriebsbereitschaft (ORR)

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

Betriebstechnologie (OT)

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

Betriebsintegration (OI)

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

Organisationspfad

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

Organisatorisches Veränderungsmanagement (OCM)

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

Ursprungszugriffskontrolle (OAC)

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

Ursprungszugriffsidentität (OAI)

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

ORR

Weitere Informationen finden Sie unter Überprüfung der Betriebsbereitschaft.

NICHT

Siehe Betriebstechnologie.

Ausgehende (egress) VPC

In einer Architektur AWS mit mehreren Konten eine VPC, die Netzwerkverbindungen verarbeitet, die von einer Anwendung aus initiiert werden. Die AWS Security Reference Architecture empfiehlt die Einrichtung Ihres Netzwerkkontos mit eingehendem und ausgehendem Datenverkehr sowie Inspektion, VPCs um die bidirektionale Schnittstelle zwischen Ihrer Anwendung und dem Internet im weiteren Sinne zu schützen.

P

Berechtigungsgrenze

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

persönlich identifizierbare Informationen (PII)

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

Personenbezogene Daten

Siehe persönlich identifizierbare Informationen.

Playbook

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

PLC

Siehe programmierbare Logiksteuerung.

PLM

Siehe Produktlebenszyklusmanagement.

policy

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

Polyglotte Beharrlichkeit

Unabhängige Auswahl der Datenspeichertechnologie eines Microservices auf der Grundlage von Datenzugriffsmustern und anderen Anforderungen. Wenn Ihre Microservices über dieselbe

Datenspeichertechnologie verfügen, kann dies zu Implementierungsproblemen oder zu Leistungseinbußen führen. Microservices lassen sich leichter implementieren und erzielen eine bessere Leistung und Skalierbarkeit, wenn sie den Datenspeicher verwenden, der ihren Anforderungen am besten entspricht. Weitere Informationen finden Sie unter Datenpersistenz in Microservices aktivieren.

Portfoliobewertung

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

predicate

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

Prädikat Pushdown

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

Präventive Kontrolle

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

Prinzipal

Eine Entität AWS , die Aktionen ausführen und auf Ressourcen zugreifen kann. Bei dieser Entität handelt es sich in der Regel um einen Root-Benutzer für eine AWS-Konto, eine IAM-Rolle oder einen Benutzer. Weitere Informationen finden Sie unter Prinzipal in Rollenbegriffe und -konzepte in der IAM-Dokumentation.

Datenschutz von Natur aus

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

Privat gehostete Zonen

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

soll. Weitere Informationen finden Sie unter Arbeiten mit privat gehosteten Zonen in der Route-53-Dokumentation.

proaktive Steuerung

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

Produktlebenszyklusmanagement (PLM)

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

Produktionsumgebung

Siehe Umgebung.

Speicherprogrammierbare Steuerung (SPS)

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

schnelle Verkettung

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

Pseudonymisierung

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

publish/subscribe (pub/sub)

Ein Muster, das asynchrone Kommunikation zwischen Microservices ermöglicht, um die Skalierbarkeit und Reaktionsfähigkeit zu verbessern. In einem auf Microservices basierenden MES kann ein Microservice beispielsweise Ereignismeldungen in einem Kanal veröffentlichen,

den andere Microservices abonnieren können. Das System kann neue Microservices hinzufügen, ohne den Veröffentlichungsservice zu ändern.

Q

Abfrageplan

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

Abfrageplanregression

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

R

RACI-Matrix

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

LAPPEN

Siehe Erweiterte Generierung beim Abrufen.

Ransomware

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

RASCI-Matrix

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

RCAC

Siehe Zugriffskontrolle für Zeilen und Spalten.

Read Replica

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

neu strukturieren

Siehe 7 Rs.

Recovery Point Objective (RPO)

Die maximal zulässige Zeitspanne seit dem letzten Datenwiederherstellungspunkt. Damit wird festgelegt, was als akzeptabler Datenverlust zwischen dem letzten Wiederherstellungspunkt und der Serviceunterbrechung gilt.

Wiederherstellungszeitziel (RTO)

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

Refaktorierung

Siehe 7 Rs.

Region

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

Regression

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

rehosten

Siehe 7 Rs.

Veröffentlichung

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

umziehen

Siehe 7 Rs.

neue Plattform

Siehe 7 Rs.

Rückkauf

Siehe 7 Rs.

Ausfallsicherheit

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

Ressourcenbasierte Richtlinie

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

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

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

Reaktive Kontrolle

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

Beibehaltung

Siehe 7 Rs.

zurückziehen

Siehe 7 Rs.

Retrieval Augmented Generation (RAG)

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

Drehung

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

Zugriffskontrolle für Zeilen und Spalten (RCAC)

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

RPO

Siehe Recovery Point Objective.

RTO

Siehe Ziel der Wiederherstellungszeit.

Runbook

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

S

SAML 2.0

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

SCADA

Siehe Aufsichtskontrolle und Datenerfassung.

SCP

Siehe Richtlinie zur Dienstkontrolle.

Secret

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

Sicherheit durch Design

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

Sicherheitskontrolle

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

Härtung der Sicherheit

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

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

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

Automatisierung von Sicherheitsreaktionen

Eine vordefinierte und programmierte Aktion, die darauf ausgelegt ist, automatisch auf ein Sicherheitsereignis zu reagieren oder es zu beheben. Diese Automatisierungen dienen als

detektive oder reaktionsschnelle Sicherheitskontrollen, die Sie bei der Implementierung bewährter AWS Sicherheitsmethoden unterstützen. Beispiele für automatisierte Antwortaktionen sind das Ändern einer VPC-Sicherheitsgruppe, das Patchen einer EC2 Amazon-Instance oder das Rotieren von Anmeldeinformationen.

Serverseitige Verschlüsselung

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

Service-Kontrollrichtlinie (SCP)

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

Service-Endpunkt

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

Service Level Agreement (SLA)

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

Service-Level-Indikator (SLI)

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

Service-Level-Ziel (SLO)

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

Modell der geteilten Verantwortung

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

SIEM

Siehe Sicherheitsinformations- und Event-Management-System.

Single Point of Failure (SPOF)

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

SLA

Siehe Service Level Agreement.

SLI

Siehe Service-Level-Indikator.

ALSO

Siehe Service-Level-Ziel.

split-and-seed Modell

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

SPOTTEN

Siehe Single Point of Failure.

Sternschema

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

Strangler-Fig-Muster

Ein Ansatz zur Modernisierung monolithischer Systeme, bei dem die Systemfunktionen schrittweise umgeschrieben und ersetzt werden, bis das Legacy-System außer Betrieb

genommen werden kann. Dieses Muster verwendet die Analogie einer Feigenrebe, die zu einem etablierten Baum heranwächst und schließlich ihren Wirt überwindet und ersetzt. Das Muster wurde eingeführt von Martin Fowler als Möglichkeit, Risiken beim Umschreiben monolithischer Systeme zu managen. Ein Beispiel für die Anwendung dieses Musters finden Sie unter Schrittweises Modernisieren älterer Microsoft ASP.NET (ASMX)-Webservices mithilfe von Containern und Amazon API Gateway.

Subnetz

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

Aufsichtskontrolle und Datenerfassung (SCADA)

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

Symmetrische Verschlüsselung

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

synthetisches Testen

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

Systemaufforderung

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

T

tags

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

Zielvariable

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

Aufgabenliste

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

Testumgebungen

Siehe Umgebung.

Training

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

Transit-Gateway

Ein Netzwerk-Transit-Hub, über den Sie Ihre Netzwerke VPCs und Ihre lokalen Netzwerke miteinander verbinden können. Weitere Informationen finden Sie in der Dokumentation unter Was ist ein Transit-Gateway. AWS Transit Gateway

Stammbasierter Workflow

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

Vertrauenswürdiger Zugriff

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

finden Sie in der AWS Organizations Dokumentation unter Verwendung AWS Organizations mit anderen AWS Diensten.

Optimieren

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

Zwei-Pizzen-Team

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

U

Unsicherheit

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

undifferenzierte Aufgaben

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

höhere Umgebungen

Siehe Umgebung.

V

Vacuuming

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

Versionskontrolle

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

VPC-Peering

Eine Verbindung zwischen zwei VPCs , die es Ihnen ermöglicht, den Verkehr mithilfe privater IP-Adressen weiterzuleiten. Weitere Informationen finden Sie unter Was ist VPC-Peering? in der Amazon-VPC-Dokumentation.

Schwachstelle

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

W

Warmer Cache

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

warme Daten

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

Fensterfunktion

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

Workload

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

Workstream

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

WURM

Sehen Sie einmal schreiben, viele lesen.

WQF

Siehe AWS Workload-Qualifizierungsrahmen.

einmal schreiben, viele lesen (WORM)

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

Z

Zero-Day-Exploit

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

Zero-Day-Sicherheitslücke

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

Zero-Shot-Aufforderung

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

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

Zombie-Anwendung

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

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