Bewährte Methoden und Funktionen für die Verschlüsselung AWS-Services

AWS Präskriptive Leitlinien

AWS Präskriptive Leitlinien: Bewährte Methoden und Funktionen für die Verschlüsselung AWS-Services

Table of Contents

Bewährte Methoden und Feature für AWS-Services

Kurt Kumar, Amazon Web Services

September 2024 (Geschichte der Dokumente)

Verschlüsselung ist ein grundlegendes Cybersicherheitsinstrument zum Schutz sensibler Daten im digitalen Zeitalter. Da sich Unternehmen zunehmend auf Daten verlassen, um ihre Abläufe voranzutreiben, einschließlich generativer KI-Implementierungen, ist der Schutz dieser wertvollen Informationen durch robuste Verschlüsselungspraktiken ein wesentlicher Bestandteil einer umfassenden Datenschutzstrategie. Dieser Leitfaden kann Ihnen helfen, die Verschlüsselungsprinzipien und die damit AWS verbundenen Verschlüsselungsfunktionen zu verstehen.

Moderne Cybersicherheitsbedrohungen beinhalten das Risiko einer Datenschutzverletzung, bei der ein unbefugter Zugriff auf Ihre Informationsressourcen zum Verlust von Daten führt. Daten sind ein Geschäftsgut, das für jedes Unternehmen einzigartig ist. Sie können Kundeninformationen, Geschäftspläne, Konstruktionsdokumente oder Code enthalten. Das Unternehmen zu schützen bedeutet, seine Daten zu schützen.

Datenverschlüsselung kann dazu beitragen, Ihre Geschäftsdaten auch nach einem Verstoß zu schützen. Sie bietet eine Schutzschicht gegen unbeabsichtigte Offenlegung. Für den Zugriff auf verschlüsselte Daten in der AWS Cloud benötigen Benutzer Berechtigungen zur Verwendung des Schlüssels zum Entschlüsseln und benötigen Berechtigungen zur Nutzung des Services, in dem sich die Daten befinden. Ohne diese beiden Berechtigungen können Benutzer die Daten nicht entschlüsseln und anzeigen.

Im Allgemeinen gibt es drei Arten von Daten, die Sie verschlüsseln können. Daten während der Übertragung sind Daten, die sich aktiv durch Ihr Netzwerk bewegen, z. B. zwischen Netzwerkressourcen. Daten im Ruhezustand sind Daten, die stationär und inaktiv sind, z. B. Daten, die sich im Speicher befinden. Beispiele hierfür sind Blockspeicher, Objektspeicher, Datenbanken, Archive und Internet der Dinge (IoT)-Geräte. Verwendete Daten beziehen sich auf Daten, die Anwendungen oder Dienste aktiv verarbeiten oder nutzen. Durch die Sicherung von Daten am Verwendungsort können Unternehmen dazu beitragen, das Risiko einer unbeabsichtigten Offenlegung zu verringern.

In diesem Leitfaden werden Überlegungen und bewährte Verfahren zur Verschlüsselung von Daten während der Übertragung und Speicherung von Daten erörtert. Außerdem werden die

Verschlüsselungsfunktionen und -kontrollen beschrieben, die in vielen AWS-Services Programmen verfügbar sind. Sie können diese Verschlüsselungsempfehlungen auf Service-Ebene in Ihren AWS Cloud Umgebungen implementieren.

Zielgruppe

Dieser Leitfaden kann von kleinen, mittleren und großen Organisationen im öffentlichen und privaten Sektor verwendet werden. Ganz gleich, ob sich Ihre Organisation in der Anfangsphase der Bewertung und Umsetzung einer Datenschutzstrategie befindet oder ob es darum geht, bestehende Sicherheitskontrollen zu verbessern, die in diesem Leitfaden dargelegten Empfehlungen eignen sich am besten für die folgenden Zielgruppen:

- Führungskräfte, die Richtlinien für ihr Unternehmen formulieren, wie Geschäftsführer (CEOs), Chief Technology Officers (CTOs), Chief Information Officers (CIOs) und Chief Information Security Officers (CISOs)
- Technologiebeauftragte, die für die Festlegung technischer Standards verantwortlich sind, z. B. technische Vizepräsidenten und Direktoren
- Geschäfts-Stakeholder und Anwendungsinhaber, die verantwortlich sind für:
  - Bewertung der Risikosituation, Datenklassifizierung und Schutzanforderungen
  - Überwachung der Einhaltung etablierter organisatorischer Standards
- Beauftragte für Compliance, interne Revision und Unternehmensführung, die für die Überwachung der Einhaltung von Compliance-Richtlinien, einschließlich gesetzlicher und freiwilliger Compliance-Regelungen, zuständig sind

Über AWS-Kryptografieservices

Ein Verschlüsselungsalgorithmus ist eine Formel oder ein Verfahren, das eine Klartext-Nachricht in einen verschlüsselten Geheimtext umwandelt. Wenn Sie noch nicht mit der Verschlüsselung oder deren Terminologie vertraut sind, empfehlen wir Ihnen, Über Datenverschlüsselung und Konzepte der Kryptografie zu lesen, bevor Sie mit diesem Handbuch fortfahren.

AWS-Kryptografieservices basieren auf sicheren Open-Source-Verschlüsselungsalgorithmen. Diese Algorithmen werden von öffentlichen Normungsgremien und von der akademischen Forschung überprüft. Einige AWS-Tools und -Services erzwingen die Verwendung eines bestimmten Algorithmus. Bei anderen Services können Sie zwischen mehreren verfügbaren Algorithmen und Schlüssellängen wählen oder die empfohlenen Standardwerte verwenden.

In diesem Abschnitt werden einige der Algorithmen beschrieben, die AWS-Tools und -Services unterstützen. Sie lassen sich je nach der Funktionsweise ihrer Schlüssel in zwei Kategorien einteilen: symmetrisch und asymmetrisch:

- Symmetrische Verschlüsselung verwendet denselbe Schlüssel, um die Daten zu verschlüsseln und zu entschlüsseln. AWS-Services unterstützt Advanced Encryption Standard (AES) und Triple Data Encryption Standard (3DES oder TDES), zwei weit verbreitete symmetrische Algorithmen. Weitere Informationen finden Sie unter Symmetrische Algorithmen im AWS-Leitfaden für kryptografische Services und Tools.
- Asymmetrische Verschlüsselung verwendet ein Schlüsselpaar, einen öffentlichen Schlüssel zur Verschlüsselung und einen privaten Schlüssel zur Entschlüsselung. 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. AWS-Services unterstützt in der Regel RSA- und asymmetrische Algorithmen für Elliptic-Curve-Kryptografie (ECC). Weitere Informationen finden Sie unter Asymmetrische Algorithmen im AWS-Leitfaden für kryptografische Services und Tools.

AWS-Kryptografieservices entsprechen einer Vielzahl von kryptografischen Sicherheitsstandards, sodass Sie behördliche oder berufsrechtliche Vorschriften einhalten können. Eine vollständige Liste der Datensicherheitsstandards, die AWS-Services einhält, finden Sie unter AWS-Compliance-Programme. Weitere Informationen zu kryptografischen Tools und Services finden Sie unter kryptografische Services und Tools von AWS.

Allgemeine bewährte Methoden für die Verschlüsselung

Dieser Abschnitt enthält Empfehlungen, die für die Verschlüsselung von Daten in der AWS Cloud gelten. Diese allgemeinen bewährten Methoden zur Verschlüsselung sind nicht spezifisch für. AWS-Services In diesem Abschnitt werden folgende Themen behandelt:

- Datenklassifizierung
- Verschlüsseln von Daten während der Übertragung.
- Verschlüsselung gespeicherter Daten

Datenklassifizierung

Datenklassifizierung ist 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. Zu den Kategorien könnten gehören sehr vertraulich, vertraulich, nicht vertraulich, und öffentlich, aber die Klassifizierungsstufen und ihre Namen können von Organisation zu Organisation unterschiedlich sein. Weitere Informationen zum Datenklassifizierungsprozess, zu Überlegungen und Modellen finden Sie unter Datenklassifizierung (AWS Whitepaper).

Nachdem Sie Ihre Daten klassifiziert haben, können Sie eine Verschlüsselungsstrategie für Ihre Organisation erstellen, die auf dem für jede Kategorie erforderlichen Schutzniveau basiert. Beispielsweise könnte Ihre Organisation entscheiden, dass für streng vertrauliche Daten eine asymmetrische Verschlüsselung verwendet werden sollte und dass für öffentliche Daten keine Verschlüsselung erforderlich ist. Weitere Informationen zum Erstellen einer Verschlüsselungsstrategie finden Sie unter Erstellen einer unternehmensweiten Verschlüsselungsstrategie für Daten im Ruhezustand. Die technischen Überlegungen und Empfehlungen in diesem Handbuch beziehen sich zwar auf Daten im Ruhezustand, Sie können jedoch auch den schrittweisen Ansatz verwenden, um eine Verschlüsselungsstrategie für Daten während der Übertragung zu erstellen.

Verschlüsseln von Daten während der Übertragung.

Alle Daten, die AWS-Regionen über das AWS globale Netzwerk übertragen werden, werden auf der physischen Ebene automatisch verschlüsselt, bevor sie AWS gesicherte Einrichtungen verlassen. Der gesamte Verkehr zwischen Availability Zones ist verschlüsselt.

Im Folgenden finden Sie allgemeine bewährte Methoden für die Verschlüsselung von Daten während der Übertragung in AWS Cloud:

- Definieren Sie eine organisatorische Verschlüsselungsrichtlinie für Daten während der Übertragung, die auf Ihrer Datenklassifizierung, den organisatorischen Anforderungen und allen geltenden behördlichen oder Compliance-Standards basiert. Wir empfehlen dringend, Daten während der Übertragung als hochvertraulich oder vertraulich eingestufte Daten zu verschlüsseln. Ihre Richtlinie kann bei Bedarf auch die Verschlüsselung für andere Kategorien vorschreiben, z. B. für nicht vertrauliche oder öffentliche Daten.
- Bei der Verschlüsselung von Daten während der Übertragung empfehlen wir die Verwendung anerkannter Kryptografiealgorithmen, Blockverschlüsselungsmodi und Schlüssellängen, wie in Ihrer Verschlüsselungsrichtlinie definiert.
- Verschlüsseln Sie den Verkehr zwischen Informationsressourcen und Systemen innerhalb des Unternehmensnetzwerks und der AWS Cloud Infrastruktur mithilfe einer der folgenden Methoden:
  - AWS Site-to-Site VPN-Verbindungen
  - Eine Kombination aus AWS Direct ConnectVerbindungen AWS Site-to-Site VPN und, die eine IPsec verschlüsselte private Verbindung ermöglicht
  - AWS Direct Connect Verbindungen, die MAC Security (MACsec) unterstützen, um Daten von Unternehmensnetzwerken zum Standort zu verschlüsseln AWS Direct Connect
- Erstellen Sie für Ihre Verschlüsselungsschlüssel auf der Grundlage des Prinzips der geringsten Berechtigung. Geringste Berechtigung ist die bewährte Sicherheitsmethode, um Benutzern den Mindestzugriff zu gewähren, den sie zur Ausführung ihrer Aufgaben benötigen. Weitere Informationen zur Anwendung von Berechtigungen mit den geringsten Rechten finden Sie unter Bewährte Sicherheitsmethoden in IAM und Bewährte Methoden für Richtlinien. IAM

Verschlüsselung gespeicherter Daten

Alle AWS Datenspeicherdienste, wie Amazon Simple Storage Service (Amazon S3) und Amazon Elastic File System (AmazonEFS), bieten Optionen zum Verschlüsseln von Daten im Ruhezustand.

Die Verschlüsselung erfolgt mithilfe der 256-Bit-Blockverschlüsselungs- und AWS Kryptografiedienste Advanced Encryption Standard (AES-256) wie () oder.AWS Key Management ServiceAWS KMSAWS CloudHSM

Sie können Daten mit clientseitiger Verschlüsselung oder serverseitiger Verschlüsselung verschlüsseln. Dies hängt von Faktoren wie der Datenklassifizierung, dem Verschlüsselungsbedarf oder technischen Einschränkungen ab, die Sie daran hindern, end-to-end Verschlüsselung zu verwenden: end-to-end

- Clientseitige Verschlüsselung ist der Vorgang, bei dem Daten lokal verschlüsselt werden, bevor die Zielanwendung oder der Service sie empfängt. Der AWS-Service empfängt die verschlüsselten Daten lediglich und spielt keine Rolle bei ihrer Ver- oder Entschlüsselung. Für die clientseitige Verschlüsselung können Sie AWS KMS verwenden, das AWS Encryption SDK, oder andere Verschlüsselungstools oder -services von Drittanbietern.
- Serverseitige Verschlüsselung ist die Verschlüsselung von Daten am Zielort durch die Anwendung oder den Service, der sie erhält. Für serverseitige Verschlüsselung können Sie die Verschlüsselung des gesamten AWS KMS Speicherblocks verwenden. Sie können auch andere Verschlüsselungstools oder -dienste von Drittanbietern verwenden, z. B. LUKSzum Verschlüsseln eines Linux-Dateisystems auf Betriebssystemebene (OS).

Im Folgenden finden Sie allgemeine bewährte Methoden für die Verschlüsselung von Daten im Ruhezustand in AWS Cloud:

- Definieren Sie eine organisatorische Verschlüsselungsrichtlinie für Daten im Ruhezustand, die auf Ihrer Datenklassifizierung, den organisatorischen Anforderungen und allen geltenden behördlichen oder Compliance-Standards basiert. Weitere Informationen finden Sie unter Erstellen einer unternehmensweiten Verschlüsselungsstrategie für Daten im Ruhezustand. Wir empfehlen dringend, Daten im Ruhezustand als hochvertraulich oder vertraulich eingestufte Daten zu verschlüsseln. Ihre Richtlinie kann bei Bedarf auch die Verschlüsselung für andere Kategorien vorschreiben, z. B. für nicht vertrauliche oder öffentliche Daten.
- Bei der Verschlüsselung von Daten im Ruhezustand empfehlen wir die Verwendung anerkannter Kryptografiealgorithmen, Blockverschlüsselungsmodi und Schlüssellängen.
- Erstellen Sie für Ihre Verschlüsselungsschlüssel auf der Grundlage des Prinzips der geringsten Berechtigung.

Bewährte Methoden für die Verschlüsselung für AWS-Services

Dieser Abschnitt enthält bewährte Methoden und Empfehlungen für Folgendes: AWS-Services

- AWS CloudTrail
- Amazon-DynamoDB
- Amazon Elastic Compute Cloud (AmazonEC2) und Amazon Elastic Block Store (AmazonEBS)
- Amazon Elastic Container Registry (AmazonECR)
- Amazon Elastic Container Service (AmazonECS)
- Amazon Elastic File System (AmazonEFS)
- Amazon Elastic Kubernetes Service (Amazon) EKS
- AWS Encryption SDK
- AWS Key Management Service (AWS KMS)
- AWS Lambda
- Amazon Relational Database Service (AmazonRDS)
- AWS Secrets Manager
- Amazon-Simple-Storage-Service (Amazon-S3)
- Amazon Virtual Private Cloud (AmazonVPC)

Bewährte Methoden zur Verschlüsselung für AWS CloudTrail

AWS CloudTrail unterstützt die Aktivierung von Governance-, Compliance-, Betriebs- und Risikoprüfungen Ihres AWS-Konto.

Bedenken Sie die folgenden bewährten Verschlüsselungsmethoden für diesen Service:

- CloudTrail Protokolle sollten mithilfe eines vom Kunden verwalteten Systems verschlüsselt werden AWS KMS key. Wählen Sie einen KMS Schlüssel, der sich in derselben Region befindet wie der S3-Bucket, der Ihre Protokolldateien empfängt. Weitere Informationen finden Sie unter Einen Trail aktualisieren, um Ihren KMS Schlüssel zu verwenden.

- Aktivieren Sie als zusätzliche Sicherheitsebene die Überprüfung von Protokolldateien für Trails. Auf diese Weise können Sie feststellen, ob eine Protokolldatei nach der Übermittlung geändert, gelöscht oder CloudTrail unverändert wurde. Anweisungen finden Sie unter Aktivieren der Integritätsprüfung von Protokolldateien für CloudTrail.
- Verwenden Sie VPC Schnittstellenendpunkte, um die Kommunikation mit Ressourcen in anderen CloudTrail zu ermöglichen, VPCs ohne das öffentliche Internet zu durchqueren. Weitere Informationen finden Sie unter Verwendung AWS CloudTrail mit Schnittstellenendpunkten. VPC
- Fügen Sie der Schlüsselrichtlinie einen `aws:SourceArn` KMS Bedingungsschlüssel hinzu, um sicherzustellen, dass der KMS Schlüssel nur für einen oder mehrere bestimmte Pfade CloudTrail verwendet wird. Weitere Informationen finden Sie unter AWS KMS key Richtlinien konfigurieren für CloudTrail.
- Implementieren Sie unter die cloud-trail-encryption-enabled AWS verwaltete Regel AWS Config, um die Verschlüsselung von Protokolldateien zu validieren und durchzusetzen.
- Wenn CloudTrail es so konfiguriert ist, dass Benachrichtigungen über Amazon Simple Notification Service (AmazonSNS) -Themen gesendet werden, fügen Sie der CloudTrail Richtlinienerklärung einen `aws:SourceArn` (oder optional`aws:SourceAccount`) Bedingungsschlüssel hinzu, um unbefugten Kontozugriff auf das SNS Thema zu verhindern. Weitere Informationen finden Sie in den SNSAmazon-Themenrichtlinien für CloudTrail.
- Wenn Sie verwenden AWS Organizations, erstellen Sie einen Organisationspfad, der AWS-Konten alle Ereignisse für diese Organisation protokolliert. Dazu gehören das Verwaltungskonto und alle Mitgliedskonten der Organisation. Weitere Informationen finden unter Erstellen eines Trails für eine Organisation.
- Erstellen Sie einen Pfad, der für alle Bereiche gilt, in AWS-Regionen denen Sie Unternehmensdaten speichern, um AWS-Konto Aktivitäten in diesen Regionen aufzuzeichnen. AWS Schließt beim Start einer neuen Region CloudTrail automatisch die neue Region ein und protokolliert Ereignisse in dieser Region.

Bewährte Methoden zur Verschlüsselung für Amazon DynamoDB

Amazon DynamoDB ist ein vollständig verwalteter Service ohne SQL Datenbank, der eine schnelle, vorhersehbare und skalierbare Leistung bietet. Die DynamoDB-Verschlüsselung im Ruhezustand schützt Daten in einer verschlüsselten Tabelle — einschließlich des Primärschlüssels, der lokalen und globalen Sekundärindizes, Streams, globalen Tabellen, Backups und DynamoDB Accelerator (DAX) -Cluster, wenn die Daten auf dauerhaften Medien gespeichert werden.

Gemäß den Anforderungen an die Datenklassifizierung können die Vertraulichkeit und Integrität der Daten durch die Implementierung einer server- oder clientseitigen Verschlüsselung gewährleistet werden:

Für die serverseitige Verschlüsselung können Sie beim Erstellen einer neuen Tabelle AWS KMS keys verwenden, um die Tabelle zu verschlüsseln. Sie können AWS eigene Schlüssel, verwaltete Schlüssel oder vom Kunden verwaltete Schlüssel verwenden. AWS Wir empfehlen die Verwendung kundenverwalteten Schlüssel, da Ihre Organisation die volle Kontrolle über den Schlüssel hat und weil bei Verwendung dieses Schlüsseltyps der Verschlüsselungsschlüssel auf Tabellenebene, die DynamoDB-Tabelle, die lokalen und globalen sekundären Indizes und Streams alle mit demselben Schlüssel verschlüsselt werden. Weitere Informationen zu diesen Schlüsseltypen finden Sie unter Kundenschlüssel und AWS Schlüssel.

> **Note**
>
> Sie können jederzeit zwischen einem AWS eigenen Schlüssel, einem AWS verwalteten Schlüssel und einem vom Kunden verwalteten Schlüssel wechseln.

Für die clientseitige Verschlüsselung und den end-to-end Schutz von Daten, sowohl im Ruhezustand als auch bei der Übertragung, können Sie den Amazon DynamoDB Encryption Client verwenden. Zusätzlich zur Verschlüsselung, die die Vertraulichkeit des Elementattributwerts schützt, signiert der DynamoDB-Encryption-Client das Element. Das ermöglicht Ihnen, nicht autorisierte Änderungen am gesamten Element zu erkennen, einschließlich des Hinzufügens oder Löschens von Attributen oder des Ersetzens eines verschlüsselten Werts durch einen anderen.

Bedenken Sie die folgenden bewährten Verschlüsselungsmethoden für diesen Service:

- Beschränken Sie die Berechtigungen zur Deaktivierung oder zum geplanten Löschen des Schlüssels auf diejenigen Personen, die diese Aufgaben ausführen müssen. Diese Zustände verhindern, dass alle Benutzer und der DynamoDB-Service Daten ver- oder entschlüsseln und Lese- und Schreibvorgänge in der Tabelle durchführen können.
- DynamoDB verschlüsselt Daten bei der Übertragung zwar HTTPS standardmäßig, es werden jedoch zusätzliche Sicherheitskontrollen empfohlen. Sie können alle der folgenden Optionen verwenden:
  - AWS Site-to-Site VPN Verbindung, die zur Verschlüsselung verwendet IPsec wird.
  - AWS Direct Connect Verbindung, um eine private Verbindung herzustellen.

  - AWS Direct Connect Verbindung mit AWS Site-to-Site VPN Verbindung für eine IPsec -verschlüsselte private Verbindung.
  - Wenn der Zugriff auf DynamoDB nur von einer Virtual Private Cloud (VPC) aus erforderlich ist, können Sie einen VPC Gateway-Endpunkt verwenden und nur Ressourcen in der Zugriff VPC darauf gewähren. Dadurch wird verhindert, dass der Verkehr das öffentliche Internet durchquert.
- Wenn Sie VPC Endpunkte verwenden, beschränken Sie die Endpunktrichtlinien und IAM Richtlinien, die mit dem Endpunkt verknüpft sind, auf autorisierte Benutzer, Ressourcen und Dienste. Weitere Informationen finden Sie unter Steuern des Zugriffs auf DynamoDB-Endpunkte mithilfe von IAM Richtlinien und Steuern des Zugriffs auf Dienste mithilfe von Endpunktrichtlinien.
- Sie können die Datenverschlüsselung auf Spaltenebene auf Anwendungsebene für Daten implementieren, die gemäß Ihrer Verschlüsselungsrichtlinie verschlüsselt werden müssen.
- Konfigurieren Sie DAX Cluster so, dass sie Daten im Ruhezustand, z. B. Daten im Cache, Konfigurationsdaten und Protokolldateien, bei der Einrichtung des Clusters verschlüsseln. Sie können Verschlüsselung von Daten im Ruhezustand in einem vorhandenen Cluster nicht aktivieren. Diese serverseitige Verschlüsselung trägt dazu bei, Daten vor unbefugtem Zugriff durch den zugrunde liegenden Speicher zu schützen. DAXEncryption at Rest wird automatisch in die Verwaltung des Single-Service-Standardschlüssels integriert, der zur Verschlüsselung der Cluster verwendet wird. AWS KMS Wenn bei der Erstellung eines verschlüsselten DAX Clusters kein Dienst-Standardschlüssel vorhanden ist, wird AWS KMS automatisch ein neuer AWS verwalteter Schlüssel erstellt. Weitere Informationen finden Sie unter DAXVerschlüsselung im Ruhezustand.

  > **Note**
  >
  > Vom Kunden verwaltete Schlüssel können nicht mit DAX Clustern verwendet werden.

- Konfigurieren Sie DAX Cluster so, dass bei der Einrichtung des Clusters Daten während der Übertragung verschlüsselt werden. Sie können Verschlüsselung von Daten während der Übertragung in einem vorhandenen Cluster nicht aktivieren. DAXverwendetTLS, um Anfragen und Antworten zwischen der Anwendung und dem Cluster zu verschlüsseln, und verwendet das x509-Zertifikat des Clusters, um die Identität des Clusters zu authentifizieren. Weitere Informationen finden Sie unter DAXVerschlüsselung bei der Übertragung.
- Implementieren Sie unter die dax-encryption-enabled AWS verwaltete Regel AWS Config, um die Verschlüsselung von DAX Clustern zu validieren und aufrechtzuerhalten.

Bewährte Verschlüsselungsmethoden für Amazon EC2 und Amazon EBS

Amazon Elastic Compute Cloud (AmazonEC2) bietet skalierbare Rechenkapazität in der AWS Cloud. Sie können so viele virtuelle Server wie nötig nutzen und sie schnell nach oben oder unten skalieren. Amazon Elastic Block Store (AmazonEBS) bietet Speichervolumes auf Blockebene zur Verwendung mit EC2 Instances.

Bedenken Sie die folgenden bewährten Verschlüsselungsmethoden für diese Services:

- Kennzeichnen Sie alle EBS Volumes mit dem entsprechenden Datenklassifizierungsschlüssel und -wert. Auf diese Weise können Sie die geeigneten Sicherheits- und Verschlüsselungsanforderungen gemäß Ihrer Richtlinie ermitteln und implementieren.
- Konfigurieren Sie entsprechend Ihrer Verschlüsselungsrichtlinie und der technischen Machbarkeit die Verschlüsselung für Daten, die zwischen EC2 Instances oder zwischen EC2 Instances und Ihrem lokalen Netzwerk übertragen werden.
- Verschlüsseln Sie sowohl das Boot- als auch das EBS Datenvolume einer EC2 Instance. Ein verschlüsseltes EBS Volume schützt die folgenden Daten:
  - Die auf dem Volume gespeicherten Daten
  - Alle Daten, die zwischen dem Volume und der Instance verschoben werden
  - Alle Snapshots, die von dem Volume erstellt werden
  - Alle Volumes, die von diesen Snapshots erstellt werden

  Weitere Informationen finden Sie unter So funktioniert EBS Verschlüsselung.
- Aktivieren Sie in der aktuellen Version standardmäßig die Verschlüsselung für EBS Volumes für Ihr Konto AWS-Region. Dadurch wird die Verschlüsselung aller neuen EBS Volumes und Snapshot-Kopien erzwungen. Es hat keine Auswirkungen auf bestehende EBS Volumes oder Snapshots. Weitere Informationen finden Sie unter Verschlüsselung standardmäßig aktivieren.
- Verschlüsseln Sie das Root-Volume des Instance-Speichers für eine EC2 Amazon-Instance. Auf diese Weise können Sie die im Betriebssystem gespeicherten Konfigurationsdateien und Daten schützen. Weitere Informationen finden Sie unter So schützen Sie Daten im Ruhezustand mit Amazon EC2 Instance Store-Verschlüsselung (AWS Blogbeitrag)
- Implementieren Sie unter die Regel für verschlüsselte Volumes für automatisierte Prüfungen, die geeignete Verschlüsselungskonfigurationen validieren und durchsetzen. AWS Config

Bewährte Verschlüsselungsmethoden für Amazon ECR

Amazon Elastic Container Registry (AmazonECR) ist ein verwalteter Container-Image-Registry-Service, der sicher, skalierbar und zuverlässig ist.

Amazon ECR speichert Bilder in Amazon S3 S3-Buckets, die Amazon ECR verwaltet. Jedes ECR Amazon-Repository hat eine Verschlüsselungskonfiguration, die bei der Erstellung des Repositorys festgelegt wird. Standardmäßig ECR verwendet Amazon serverseitige Verschlüsselung mit von Amazon SSE S3 verwalteten (-S3) Verschlüsselungsschlüsseln. Weitere Informationen finden Sie unter Verschlüsselung im Ruhezustand (ECRAmazon-Dokumentation).

Bedenken Sie die folgenden bewährten Verschlüsselungsmethoden für diesen Service:

- Anstatt die serverseitige Standardverschlüsselung mit von Amazon SSE S3 verwalteten (-S3) Verschlüsselungsschlüsseln zu verwenden, verwenden Sie vom Kunden verwaltete KMS Schlüssel, die in gespeichert sind. AWS KMS Dieser Schlüsseltyp bietet die detailliertesten Steuerungsoptionen.

  > **Note**
  >
  > Der KMS Schlüssel muss sich im selben Verzeichnis befinden wie AWS-Region das Repository.

- Widerrufen Sie nicht die Zuschüsse, die Amazon standardmäßig ECR erstellt, wenn Sie ein Repository bereitstellen. Dies kann sich auf Funktionen auswirken, z. B. auf den Zugriff auf Daten, die Verschlüsselung neuer Bilder, die in das Repository übertragen werden, oder deren Entschlüsselung, wenn sie abgerufen werden.
- Wird verwendet AWS CloudTrail , um die Anfragen aufzuzeichnen, an die Amazon ECR sendet AWS KMS. Die Protokolleinträge enthalten einen Verschlüsselungskontextschlüssel, damit sie leichter identifizierbar sind.
- Konfigurieren Sie ECR Amazon-Richtlinien, um den Zugriff von bestimmten VPC Amazon-Endpunkten oder bestimmten VPCs zu kontrollieren. Dadurch wird der Netzwerkzugriff auf eine bestimmte ECR Amazon-Ressource effektiv isoliert, sodass nur von dieser bestimmten VPC Ressource aus zugegriffen werden kann. Indem Sie eine virtuelle private Netzwerkverbindung (VPN) mit einem VPC Amazon-Endpunkt herstellen, können Sie Daten während der Übertragung verschlüsseln.

- Amazon ECR unterstützt ressourcenbasierte Richtlinien. Mithilfe dieser Richtlinien können Sie den Zugriff auf der Grundlage der Quell-IP-Adresse oder der spezifischen IP-Adresse einschränken. AWS-Service

Bewährte Verschlüsselungsmethoden für Amazon ECS

Amazon Elastic Container Service (AmazonECS) ist ein schneller und skalierbarer Container-Management-Service, mit dem Sie Container in einem Cluster ausführen, stoppen und verwalten können.

Mit Amazon ECS können Sie Daten während der Übertragung verschlüsseln, indem Sie einen der folgenden Ansätze verwenden:

- Erstellen eines Service Meshs Konfigurieren Sie mithilfe von AWS App Mesh TLS Verbindungen zwischen den bereitgestellten Envoy-Proxys und Mesh-Endpunkten, z. B. virtuellen Knoten oder virtuellen Gateways. Sie können Zertifikate von oder vom Kunden bereitgestellte TLS Zertifikate verwenden. AWS Private Certificate Authority Weitere Informationen und exemplarische Vorgehensweisen finden Sie unter Aktivieren der Verschlüsselung des Datenverkehrs zwischen Diensten AWS App Mesh unter Verwendung von AWS Certificate Manager (ACM) oder vom Kunden bereitgestellten Zertifikaten (AWS Blogbeitrag).
- Falls unterstützt, verwenden AWS Sie Nitro Enclaves. AWS Nitro Enclaves ist eine EC2 Amazon-Funktion, mit der Sie isolierte Ausführungsumgebungen, sogenannte Enklaven, aus Amazon-Instances erstellen können. EC2 Es wurde entwickelt, um Ihre sensibelsten Daten zu schützen. Darüber hinaus können Sie mit ACMfor Nitro Enclaves öffentliche und private SSL TLS /-Zertifikate für Ihre Webanwendungen und Webserver verwenden, die auf EC2 Amazon-Instances mit AWS Nitro Enclaves ausgeführt werden. Weitere Informationen finden Sie unter AWS Nitro Enclaves — Isolierte EC2 Umgebungen zur Verarbeitung vertraulicher Daten (Blogbeitrag).AWS
- Verwenden Sie das Protokoll Server Name Indication (SNI) mit Application Load Balancers. Sie können mehrere Anwendungen hinter einem einzigen HTTPS Listener für einen Application Load Balancer bereitstellen. Jeder Listener hat sein eigenes Zertifikat. TLS Sie können Zertifikate verwenden, die von bereitgestellt werdenACM, oder Sie können selbstsignierte Zertifikate verwenden. Sowohl Application Load Balancer als auch Network Load Balancer werden unterstützt. SNI Weitere Informationen finden Sie unter Application Load Balancers Support jetzt mehrere TLS Zertifikate mit Smart Selection Using SNI (AWS Blogbeitrag).

- Verwenden Sie für mehr Sicherheit und Flexibilität, AWS Private Certificate Authority um ein TLS Zertifikat mit der ECS Amazon-Aufgabe bereitzustellen. Weitere Informationen finden Sie unter TLSWartung bis zum Container, Teil 2: Verwenden AWS Private CA (AWS Blogbeitrag).
- Implementieren Sie mutual TLS (m TLS) in App Mesh, indem Sie den Secret Discovery Service (Envoy) oder in ACM (GitHub) gehostete Zertifikate verwenden.

Bedenken Sie die folgenden bewährten Verschlüsselungsmethoden für diesen Service:

- Sofern technisch machbar, konfigurieren Sie zur Erhöhung der Sicherheit ECSVPCAmazon-Schnittstellenendpunkte in AWS PrivateLink. Beim Zugriff auf diese Endpunkte über eine VPN Verbindung werden Daten während der Übertragung verschlüsselt.
- Speichern Sie vertrauliche Materialien wie API Schlüssel oder Datenbankanmeldedaten sicher. Sie können diese als verschlüsselte Parameter im Parameter Store speichern, einer Funktion von AWS Systems Manager. Wir empfehlen Ihnen jedoch, diesen Dienst zu verwenden, AWS Secrets Manager da Sie mit diesem Dienst Geheimnisse automatisch rotieren, zufällige Geheimnisse generieren und Geheimnisse gemeinsam nutzen können AWS-Konten.
- Um das Risiko von Datenlecks durch Umgebungsvariablen zu verringern, empfehlen wir Ihnen, den AWS Secrets Manager und Config Provider for Secret Store CSI Driver (GitHub) zu verwenden. Mit diesem Treiber können Sie festlegen, dass im Secrets Manager gespeicherte Geheimnisse und im Parameter Store gespeicherte Parameter als in Kubernetes-Pods gemountete Dateien angezeigt werden.

> **Note**
>
> AWS Fargate wird nicht unterstützt.

- Wenn Benutzer oder Anwendungen in Ihrem Rechenzentrum oder ein externer Drittanbieter im Internet direkte HTTPS API Anfragen an richten AWS-Services, signieren Sie diese Anfragen mit temporären Sicherheitsanmeldedaten, die Sie von AWS Security Token Service (AWS STS) erhalten haben.

Bewährte Verschlüsselungsmethoden für Amazon EFS

Amazon Elastic File System (AmazonEFS) hilft Ihnen bei der Erstellung und Konfiguration gemeinsam genutzter Dateisysteme in der AWS Cloud.

Bedenken Sie die folgenden bewährten Verschlüsselungsmethoden für diesen Service:

- AWS Config Implementieren Sie in die efs-encrypted-check AWS verwaltete Regel. Diese Regel prüft, ob Amazon so konfiguriert EFS ist, dass die Dateidaten mit AWS KMS verschlüsselt werden.
- Erzwingen Sie die Verschlüsselung für EFS Amazon-Dateisysteme, indem Sie einen CloudWatch Amazon-Alarm erstellen, der CloudTrail Protokolle auf `CreateFileSystem` Ereignisse überwacht und einen Alarm auslöst, wenn ein unverschlüsseltes Dateisystem erstellt wird. Weitere Informationen finden Sie unter Exemplarische Vorgehensweise: Verschlüsselung auf einem EFS Amazon-Dateisystem im Ruhezustand erzwingen.
- Mounten Sie das Dateisystem mithilfe des EFSMount-Helpers. Dadurch wird ein TLS 1.2-Tunnel zwischen dem Client und dem EFS Amazon-Service eingerichtet und verwaltet und der gesamte Network File System (NFS) -Verkehr wird über diesen verschlüsselten Tunnel weitergeleitet. Der folgende Befehl implementiert die Verwendung von TLS für die Verschlüsselung bei der Übertragung.

  ```
  sudo mount -t efs  -o tls file-system-id:/ /mnt/efs
  ```

  Weitere Informationen finden Sie unter EFSMount Helper zum Mounten von EFS Dateisystemen verwenden.
- Verwenden AWS PrivateLink, implementieren Sie VPC Schnittstellenendpunkte, um eine private Verbindung zwischen VPCs und dem Amazon EFS API herzustellen. Daten, die über die VPN Verbindung zum und vom Endpunkt übertragen werden, werden verschlüsselt. Weitere Informationen finden Sie unter Zugreifen und AWS-Service Verwenden eines VPC Schnittstellenendpunkts.
- Verwenden Sie den `elasticfilesystem:Encrypted` Bedingungsschlüssel in IAM identitätsbasierten Richtlinien, um zu verhindern, dass Benutzer EFS Dateisysteme erstellen, die nicht verschlüsselt sind. Weitere Informationen finden Sie unter Verwenden, IAM um die Erstellung verschlüsselter Dateisysteme zu erzwingen.
- KMSSchlüssel, die für die EFS Verschlüsselung verwendet werden, sollten mithilfe ressourcenbasierter Schlüsselrichtlinien für den Zugriff mit den geringsten Rechten konfiguriert werden.
- Verwenden Sie den `aws:SecureTransport` Bedingungsschlüssel in der EFS Dateisystemrichtlinie, um die Verwendung von TLS für NFS Clients zu erzwingen, wenn sie eine Verbindung zu einem Dateisystem herstellen. EFS Weitere Informationen finden Sie unter

Verschlüsselung von Daten bei der Übertragung in Verschlüsseln von Dateidaten mit Amazon Elastic File System (AWS Whitepaper).

Bewährte Verschlüsselungsmethoden für Amazon EKS

Mit Amazon Elastic Kubernetes Service (AmazonEKS) können Sie Kubernetes ausführen, AWS ohne dass Sie Ihre eigene Kubernetes-Steuerebene oder Knoten installieren oder verwalten müssen. In Kubernetes helfen Ihnen Secrets dabei, vertrauliche Informationen wie Benutzerzertifikate, Passwörter oder Schlüssel zu verwalten. API Standardmäßig werden diese Geheimnisse unverschlüsselt im dem API Server zugrunde liegenden Datenspeicher gespeichert, der als etcd bezeichnet wird. Jeder Benutzer, der API Zugriff auf oder Zugriff auf hat, `etcd` kann ein Geheimnis abrufen oder ändern. Darüber hinaus kann jeder, der berechtigt ist, einen Pod in einem Namespace zu erstellen, diesen Zugriff verwenden, um jedes Geheimnis in diesem Namespace zu lesen. Sie können diese in Amazon gespeicherten Geheimnisse verschlüsseln AWS KMS keys, EKS indem Sie entweder AWS verwaltete Schlüssel oder vom Kunden verwaltete Schlüssel verwenden. Ein alternativer Ansatz zur Verwendung `etcd` ist die Verwendung von AWS Secrets und Config Provider (ASCP) (GitHub Repository). ASCPintegriert IAM ressourcenbasierte Richtlinien, um den Zugriff auf geheime Daten nur innerhalb bestimmter Kubernetes-Pods innerhalb eines Clusters einzuschränken und einzuschränken.

Sie können die folgenden AWS Speicherdienste mit Kubernetes verwenden:

- Für Amazon Elastic Block Store (AmazonEBS) können Sie den In-Tree-Speichertreiber oder den EBSCSIAmazon-Treiber verwenden. Beide beinhalten Parameter für die Verschlüsselung von Volumes und die Bereitstellung eines vom Kunden verwalteten Schlüssels.
- Für Amazon Elastic File System (AmazonEFS) können Sie den EFSCSIAmazon-Treiber mit Unterstützung für dynamische und statische Bereitstellung verwenden.

Bedenken Sie die folgenden bewährten Verschlüsselungsmethoden für diesen Service:

- Wenn Sie `etcd` verwenden, in dem geheime Objekte standardmäßig unverschlüsselt gespeichert werden, gehen Sie wie folgt vor, um Geheimnisse zu schützen:
  - Verschlüsseln Sie geheime Daten im Ruhezustand (Kubernetes-Dokumentation).
  - Aktivieren oder konfigurieren Sie die Autorisierung mithilfe von Regeln zur rollenbasierten Zugriffskontrolle (RBAC), die das Lesen und Schreiben des Geheimnisses einschränken. Schränken Sie die Berechtigungen ein, um neue Geheimnisse zu erstellen oder bestehende

zu ersetzen. Weitere Informationen finden Sie unter Autorisierungsübersicht (Kubernetes-Dokumentation).

- Wenn Sie mehrere Container in einem Pod definieren und nur einer dieser Container Zugriff auf ein Geheimnis benötigt, definieren Sie den Volume-Mount so, dass die anderen Container keinen Zugriff auf dieses Geheimnis haben. Geheimnisse, die als Volumes bereitgestellt werden, werden instanziiert als `tmpfs`-Volumes und werden automatisch vom Knoten entfernt, wenn der Pod gelöscht wird. Sie könnten auch Umgebungsvariablen verwenden, aber wir empfehlen diesen Ansatz nicht, da die Werte von Umgebungsvariablen in Protokollen erscheinen können. Weitere Informationen dazu finden Sie unter Geheimnisse (Kubernetes-Dokumentation).
- Vermeiden Sie nach Möglichkeit die Gewährung von Zugriff auf `watch`- und `list`-Anforderungen auf Geheimnisse innerhalb eines Namespaces. In Kubernetes sind diese Anfragen leistungsstarkAPI, da sie es dem Client ermöglichen, die Werte jedes Geheimnisses in diesem Namespace zu überprüfen.
- Erlauben Sie nur Clusteradministratoren den Zugriff auf `etcd`, einschließlich Lesezugriff.
- Wenn es mehrere `etcd` Instanzen gibt, stellen Sie sicher, dass `etcd` sie TLS für die Kommunikation zwischen Peers verwendet werden. `etcd`

- Wenn Sie verwendenASCP, gehen Sie wie folgt vor, um vertrauliche Daten zu schützen:
  - Verwenden Sie IAMRollen für Dienstkonten, um den geheimen Zugriff nur auf autorisierte Pods zu beschränken.
  - Aktivieren Sie die Verschlüsselung von Kubernetes-Geheimnissen, indem Sie den AWS Encryption Provider (GitHub Repository) verwenden, um die Envelope-Verschlüsselung mit einem vom Kunden verwalteten KMS Schlüssel zu implementieren.
- Erstellen Sie einen CloudWatch Amazon-Metrikfilter und einen Alarm, um Benachrichtigungen für vom Administrator festgelegte Vorgänge zu senden, z. B. das Löschen von Geheimnissen oder die Verwendung einer geheimen Version während der Wartezeit auf das Löschen. Weitere Informationen finden Sie unter Erstellen eines Alarms basierend auf Anomalieerkennung.

Bewährte Methoden zur Verschlüsselung für AWS Encryption SDK

Das AWS Encryption SDK ist eine clientseitige Open-Source-Verschlüsselungsbibliothek. Es verwendet Industriestandards und bewährte Verfahren, um die Implementierung und Interoperabilität in verschiedenen Programmiersprachen zu unterstützen. AWS Encryption SDK verschlüsselt Daten mithilfe eines sicheren, authentifizierten, symmetrischen Schlüsselalgorithmus und bietet

eine Standardimplementierung, die den bewährten Methoden der Kryptografie entspricht. Weitere Informationen finden Sie unter Unterstützte Algorithmus-Suiten im AWS Encryption SDK.

Eine der wichtigsten Funktionen von AWS Encryption SDK ist die Unterstützung für die Verschlüsselung von verwendeten Daten. Mit einem encrypt-then-use Ansatz können Sie sensible Daten verschlüsseln, bevor sie von Ihrer Anwendungslogik verarbeitet werden. Dies kann dazu beitragen, die Daten vor potenzieller Offenlegung oder Manipulation zu schützen, selbst wenn die Anwendung selbst von einem Sicherheitsereignis betroffen ist.

Bedenken Sie die folgenden bewährten Methoden für diesen Service:

- Halten Sie sich an alle Empfehlungen in Bewährte Methoden für die AWS Encryption SDK.
- Wählen Sie einen oder mehrere Umschlagschlüssel, um Ihre Datenschlüssel zu schützen. Weitere Informationen finden Sie unter Auswahl von Umschlagschlüsseln.
- Übergeben Sie den `KeyId` Parameter an den ReEncryptVorgang, um die Verwendung eines nicht vertrauenswürdigen KMS Schlüssels zu verhindern. Weitere Informationen finden Sie unter Verbesserte clientseitige Verschlüsselung: Explizite KeyIds und zentrale Verpflichtung (AWS Blogbeitrag).
- Verwenden Sie bei Verwendung von AWS Encryption SDK with AWS KMS die lokale `KeyId` Filterung. Weitere Informationen finden Sie unter Verbesserte clientseitige Verschlüsselung: Explizite KeyIds und zentrale Verpflichtung (AWS Blogbeitrag).
- Für Anwendungen mit großem Datenverkehrsvolumen, die eine Verschlüsselung oder Entschlüsselung erfordern, oder wenn Ihr Konto die AWS KMS Anforderungskontingente überschreitet, können Sie die Funktion zum Zwischenspeichern von für Datenschlüssel verwenden. AWS Encryption SDK Beachten Sie die folgenden bewährten Methoden für das Zwischenspeichern der Datenschlüssel:
  - Konfigurieren Sie Cache-Sicherheitsschwellenwerte, um zu begrenzen, wie lange jeder gecachte Datenschlüssel verwendet wird und wie viele Daten unter jedem Datenschlüssel geschützt sind. Empfehlungen zur Konfiguration dieser Schwellenwerte finden Sie unter Sicherheitsgrenzwerte für den Cache festlegen.
  - Beschränken Sie den lokalen Cache auf die kleinste Anzahl von Datenschlüsseln, die erforderlich ist, um die Leistungsverbesserungen für Ihren spezifischen Anwendungsfall zu erzielen. Anweisungen und ein Beispiel für die Konfiguration von Grenzwerten für den lokalen Cache finden Sie unter Verwenden der Zwischenspeicherung von Datenschlüsseln: S. tep-by-step

Weitere Informationen finden Sie unter AWS Encryption SDK: So entscheiden Sie, ob das Zwischenspeichern von Datenschlüsseln für Ihre Anwendung geeignet ist (AWS Blogbeitrag).

Bewährte Methoden zur Verschlüsselung für AWS Key Management Service

AWS Key Management Service (AWS KMS) hilft Ihnen dabei, kryptografische Schlüssel zu erstellen und zu kontrollieren, um Ihre Daten zu schützen. AWS KMS lässt sich in die meisten anderen Systeme integrieren AWS-Services , die Ihre Daten verschlüsseln können. Eine vollständige Liste finden Sie unter AWS-Services integriert mit AWS KMS. AWS KMS lässt sich auch integrieren AWS CloudTrail , um die Verwendung Ihrer KMS Schlüssel für Prüfungs-, behördliche und Compliance-Anforderungen zu protokollieren.

KMSSchlüssel sind die primäre Ressource in AWS KMS und sie sind logische Repräsentationen eines kryptografischen Schlüssels. Es gibt drei Haupttypen von KMS Schlüsseln:

- Vom Kunden verwaltete Schlüssel sind KMS Schlüssel, die Sie erstellen.
- AWS Verwaltete Schlüssel sind KMS Schlüssel, die in Ihrem Konto in Ihrem Namen AWS-Services erstellt werden.
- AWS Eigene Schlüssel sind KMS Schlüssel, die ein Benutzer AWS-Service besitzt und verwaltet und die in mehreren Schlüsseln verwendet AWS-Konten werden können.

Weitere Informationen zu diesen Schlüsseltypen finden Sie unter Kundenschlüssel und AWS - Schlüssel.

In der werden Richtlinien verwendet AWS Cloud, um zu kontrollieren, wer auf Ressourcen und Dienste zugreifen kann. In AWS Identity and Access Management (IAM) definieren identitätsbasierte Richtlinien beispielsweise Berechtigungen für Benutzer, Benutzergruppen oder Rollen, und ressourcenbasierte Richtlinien werden an eine Ressource, z. B. einen S3-Bucket, angehängt und definieren, welchen Prinzipalen Zugriff gewährt wird, welche Aktionen unterstützt werden und welche anderen Bedingungen erfüllt sein müssen. AWS KMS Verwendet ähnlich wie IAM Richtlinien wichtige Richtlinien, um den Zugriff auf einen Schlüssel zu kontrollieren. KMS Jeder KMS Schlüssel muss über eine Schlüsselrichtlinie verfügen, und jeder Schlüssel kann nur eine Schlüsselrichtlinie haben. Beachten Sie bei der Definition von Richtlinien, die den Zugriff auf KMS Schlüssel zulassen oder verweigern, Folgendes:

- Sie können die Schlüsselrichtlinie für vom Kunden verwaltete Schlüssel steuern, aber Sie können die Schlüsselrichtlinie für AWS verwaltete Schlüssel oder für AWS eigene Schlüssel nicht direkt steuern.
- Wichtige Richtlinien ermöglichen die Gewährung eines detaillierten Zugriffs auf AWS KMS API Anrufe innerhalb eines AWS-Konto. Sofern die Schlüsselrichtlinie dies nicht ausdrücklich zulässt, können Sie IAM Richtlinien nicht verwenden, um den Zugriff auf einen KMS Schlüssel zu gewähren. Ohne die Genehmigung durch die Schlüsselrichtlinie haben IAM Richtlinien, die Berechtigungen zulassen, keine Wirkung. Weitere Informationen finden Sie unter Zulassen, dass IAM Richtlinien den Zugriff auf den KMS Schlüssel zulassen.
- Sie können eine IAM Richtlinie verwenden, um den Zugriff auf einen vom Kunden verwalteten Schlüssel ohne die entsprechende Genehmigung der Schlüsselrichtlinie zu verweigern.
- Beachten Sie beim Entwerfen wichtiger IAM Richtlinien und Richtlinien für Schlüssel mit mehreren Regionen Folgendes:
  - Schlüsselrichtlinien sind nicht gemeinsam genutzte Eigenschaften von multiregionalen Schlüsseln und nicht kopiert oder synchronisiert zwischen verwandten multiregionalen Schlüsseln.
  - Wenn ein Schlüssel für mehrere Regionen mit dem `CreateKey` und `ReplicateKey`-Aktionen erstellt wird, wird die Standardschlüsselrichtlinie angewendet, sofern in der Anfrage keine Schlüsselrichtlinie angegeben ist.
  - Sie können Bedingungsschlüssel wie aws: implementierenRequestedRegion, um Berechtigungen auf einen bestimmten AWS-Region Bereich zu beschränken.
  - Sie können Erteilungen verwenden, um Berechtigungen für einen multiregionalen Primärschlüssel oder Replikatschlüssel zuzulassen. Eine einzelne Erteilung kann jedoch nicht verwendet werden, um Berechtigungen für mehrere KMS Schlüssel zu gewähren, selbst wenn es sich um verwandte Schlüssel für mehrere Regionen handelt.

Beachten Sie bei der Verwendung AWS KMS und Erstellung von Schlüsselrichtlinien die folgenden bewährten Verschlüsselungsmethoden und andere bewährte Sicherheitsmethoden:

- Halten Sie sich an die Empfehlungen in den folgenden Ressourcen für AWS KMS bewährte Methoden:
  - Bewährte Verfahren für AWS KMS Zuschüsse (AWS KMS Dokumentation)
  - Bewährte Verfahren für IAM politische Maßnahmen (AWS KMS Dokumentation)

- In Übereinstimmung mit der bewährten Praxis der Aufgabentrennung sollten Sie die Identitäten derjenigen, die Schlüssel verwalten, und derjenigen, die sie benutzen, getrennt halten:
  - Administratorrollen, die Schlüssel erstellen und löschen, sollten nicht in der Lage sein, den Schlüssel zu verwenden.
  - Einige Services müssen möglicherweise nur Daten verschlüsseln und sollten nicht berechtigt sein, die Daten mithilfe des Schlüssels zu entschlüsseln.
- Schlüsselrichtlinien sollten immer dem Modell der geringsten Berechtigung folgen. Verwenden Sie es nicht `kms:*` für Aktionen in IAM oder wichtige Richtlinien, da dadurch der Hauptbenutzer die Rechte erhält, den Schlüssel sowohl zu verwalten als auch zu verwenden.
- Beschränken Sie die Verwendung von vom Kunden verwalteten Schlüsseln auf bestimmte Schlüssel, AWS-Services indem Sie den ViaService Bedingungsschlüssel kms: in der Schlüsselrichtlinie verwenden.
- Wenn Sie zwischen Schlüsseltypen wählen können, werden vom Kunden verwaltete Schlüssel bevorzugt, da sie die detailliertesten Kontrolloptionen bieten, darunter die folgenden:
  - Verwaltung von Authentifizierung und Zugriffskontrolle
  - Aktivieren und Deaktivieren von Schlüsseln
  - Rotation von AWS KMS keys
  - Tagging von Schlüsseln
  - Erstellen von Aliases
  - AWS KMS keys löschen
- AWS KMS Administrations- und Änderungsberechtigungen müssen nicht genehmigten Prinzipalen ausdrücklich verweigert werden, und in einer Zulassungsanweisung für nicht autorisierte Prinzipale sollten keine AWS KMS Änderungsberechtigungen enthalten sein. Weitere Informationen finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für AWS Key Management Service.
- Implementieren Sie die Regeln -kms-actions und KMS iam-customer-policy-blocked-kms-actions, um die unbefugte Verwendung von Schlüsseln zu erkennen. AWS Config iam-inline-policy-blocked Dadurch wird verhindert, dass Prinzipale die Entschlüsselungsaktionen für alle Ressourcen verwenden. AWS KMS
- Implementieren Sie Richtlinien zur Dienststeuerung (SCPs) AWS Organizations , um zu verhindern, dass nicht autorisierte Benutzer oder Rollen KMS Schlüssel löschen, entweder direkt als Befehl oder über die Konsole. Weitere Informationen finden Sie unter Verwendung SCPs als präventive Kontrollen (AWS Blogbeitrag).

- AWS KMS APIAnrufe in einem Protokoll CloudTrail protokollieren. Dadurch werden die relevanten Ereignisattribute aufgezeichnet, z. B. welche Anfragen gestellt wurden, die Quell-IP-Adresse, von der die Anfrage stammt und wer die Anfrage gestellt hat. Weitere Informationen finden Sie unter AWS KMS APIAnrufe protokollieren mit AWS CloudTrail.
- Wenn Sie den Verschlüsselungskontext verwenden, sollte dieser keine vertraulichen Informationen enthalten. CloudTrail speichert den Verschlüsselungskontext in JSON Klartextdateien, die von jedem eingesehen werden können, der Zugriff auf den S3-Bucket hat, der die Informationen enthält.
- Konfigurieren Sie bei der Überwachung der Verwendung von kundenverwalteten Schlüsseln Ereignisse, um Sie zu benachrichtigen, wenn bestimmte Aktionen wie z. B. die Erstellung von Schlüsseln, die Aktualisierung von Richtlinien für kundenverwaltete Schlüssel oder der Import von Schlüsselmaterial erkannt werden. Es wird auch empfohlen, automatisierte Antworten zu implementieren, z. B. eine AWS Lambda -Funktion, die den Schlüssel deaktiviert oder andere Maßnahmen zur Reaktion auf Vorfälle durchführt, wie es in Ihren Organisationsrichtlinien vorgeschrieben ist.
- Schlüssel für mehrere Regionen werden für bestimmte Szenarien wie Compliance, Notfallwiederherstellung oder Backups empfohlen. Die Sicherheitseigenschaften von Schlüsseln für mehrere Regionen unterscheiden sich erheblich von denen für eine Region. Die folgenden Empfehlungen gelten für die Autorisierung der Erstellung, Verwaltung und Verwendung von Schlüsseln für mehrere Regionen:
  - Erlauben Sie Prinzipalen die Replikation eines multiregionalen Schlüssels nur in AWS-Regionen , die sie erfordern.
  - Erteilen Sie Berechtigungen für multiregionale Schlüssel nur an Prinzipale, die sie benötigen, und nur für Aufgaben, für die sie erforderlich sind.

Bewährte Methoden zur Verschlüsselung für AWS Lambda

AWS Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne dass Sie Server bereitstellen oder verwalten müssen. Sie können Ihre Umgebungsvariablen sichern, können Sie eine serverseitige Verschlüsselung nutzen, um Ihre Data-at-Rest zu schützen und eine clientseitige Verschlüsselung, um Ihre Daten während der Übertragung zu schützen.

Bedenken Sie die folgenden bewährten Verschlüsselungsmethoden für diesen Service:

- Lambda bietet im Ruhezustand immer serverseitiger Verschlüsselung mit einem AWS KMS key an. Standardmäßig verwendet Lambda einen AWS verwalteten Schlüssel. Wir empfehlen Ihnen, einen

vom Kunden verwalteten Schlüssel zu verwenden, da Sie die volle Kontrolle über den Schlüssel haben, einschließlich Verwaltung, Rotation und Prüfung.

- Aktivieren Sie Helpers für übertragene Daten, die verschlüsselt werden müssen. Dadurch wird sichergestellt, dass Umgebungsvariablen clientseitig verschlüsselt werden, um den Schutz bei der Übertragung zu gewährleisten, indem der bevorzugte Schlüssel verwendet wird. KMS Weitere Informationen finden Sie unter Sicherheit während der Übertragung in Sichern von Umgebungsvariablen.
- Umgebungsvariablen für Lambda-Funktionen, die sensible oder kritische Daten enthalten, sollten bei der Übertragung verschlüsselt werden, um die Daten, die dynamisch an die Funktionen weitergegeben werden (normalerweise Zugriffsinformationen), vor unbefugtem Zugriff zu schützen.
- Um zu verhindern, dass ein Benutzer Umgebungsvariablen anzeigt, fügen Sie den Benutzerberechtigungen in der IAM Richtlinie oder der Schlüsselrichtlinie eine Anweisung hinzu, die den Zugriff auf den Standardschlüssel, einen vom Kunden verwalteten Schlüssel oder alle Schlüssel verweigert. Weitere Informationen finden Sie unter Verwenden von AWS Lambda - Umgebungsvariablen.

Bewährte Verschlüsselungsmethoden für Amazon RDS

Amazon Relational Database Service (AmazonRDS) unterstützt Sie bei der Einrichtung, dem Betrieb und der Skalierung einer relationalen Datenbank (DB) in der. AWS Cloud Daten, die im Ruhezustand verschlüsselt werden, umfassen den zugehörigen Speicherplatz für DB-Instances, deren automatisierte Backups, Lesereplikate und Snapshots.

Mit den folgenden Ansätzen können Sie ruhende Daten in RDS DB-Instances verschlüsseln:

- Sie können Amazon RDS DB-Instances entweder mit AWS KMS keys einem AWS verwalteten Schlüssel oder einem vom Kunden verwalteten Schlüssel verschlüsseln. Weitere Informationen finden Sie unter AWS Key Management Service in diesem Handbuch.
- Amazon RDS for Oracle und Amazon RDS for SQL Server unterstützen die Verschlüsselung von DB-Instances mit Transparent Data Encryption (TDE). Weitere Informationen finden Sie unter Oracle Transparent Data Encryption oder Support for Transparent Data Encryption in SQL Server.

  Sie können TDE sowohl KMS Schlüssel als auch Schlüssel verwenden, um DB-Instances zu verschlüsseln. Dies kann jedoch die Leistung Ihrer Datenbank geringfügig beeinträchtigen, und Sie müssen diese Schlüssel separat verwalten.

Mit den folgenden Ansätzen können Sie Daten verschlüsseln, die zu oder von RDS DB-Instances übertragen werden:

- Für eine RDS Amazon-DB-Instance, auf der MariaDB, Microsoft SQL Server, MySQL, Oracle oder Postgre ausgeführt wirdSQL, können Sie die Verbindung SSL zum Verschlüsseln verwenden. Weitere Informationen finden Sie unter Eine Verbindung TLS zu einer DB-Instance mitSSL/verschlüsseln.
- Amazon RDS for Oracle unterstützt auch die native Netzwerkverschlüsselung von Oracle (NNE), die Daten verschlüsselt, wenn sie zu und von einer DB-Instance übertragen werden. NNEund die SSL Verschlüsselung kann nicht gleichzeitig verwendet werden. Weitere Informationen finden Sie unter Oracle native Netzwerkverschlüsselung.

Bedenken Sie die folgenden bewährten Verschlüsselungsmethoden für diesen Service:

- Wenn Sie eine Verbindung zu Amazon RDS for SQL Server- oder Amazon RDS for SQL Postgre-DB-Instances herstellen, um Daten zu verarbeiten, zu speichern oder zu übertragen, die verschlüsselt werden müssen, verwenden Sie die Funktion RDS Transport Encryption, um die Verbindung zu verschlüsseln. Sie können diese implementieren, indem Sie die `rds.force_ssl`-Parameter in der Parametergruppe auf 1 setzen. Weitere Informationen finden Sie unter Arbeiten mit Parametergruppen. Amazon RDS for Oracle verwendet die native Netzwerkverschlüsselung der Oracle-Datenbank.
- Vom Kunden verwaltete Schlüssel für die Verschlüsselung von RDS DB-Instances sollten ausschließlich für diesen Zweck und nicht zusammen mit anderen verwendet werden AWS-Services.
- Bevor Sie eine RDS DB-Instance verschlüsseln, legen Sie die KMS wichtigsten Anforderungen fest. Der von der Instance verwendete Schlüssel kann später nicht mehr geändert werden. Definieren Sie in Ihrer Verschlüsselungsrichtlinie beispielsweise die Nutzungs- und Verwaltungsstandards für AWS verwaltete Schlüssel oder vom Kunden verwaltete Schlüssel, die auf Ihren Geschäftsanforderungen basieren.
- Beachten Sie bei der Autorisierung des Zugriffs auf einen vom Kunden verwalteten KMS Schlüssel das Prinzip der geringsten Rechte, indem Sie Bedingungsschlüssel in Richtlinien verwenden. IAM Um beispielsweise zu ermöglichen, dass ein vom Kunden verwalteter Schlüssel nur für Anfragen verwendet wird, die von Amazon stammenRDS, verwenden Sie den ViaService Bedingungsschlüssel kms: mit dem `rds.<region>.amazonaws.com` Wert. Darüber hinaus können Sie Schlüssel oder Werte im RDSAmazon-Verschlüsselungskontext als Voraussetzung für die Verwendung des vom Kunden verwalteten Schlüssels verwenden.

- Es wird dringend empfohlen, Backups für verschlüsselte RDS DB-Instances zu aktivieren. Amazon RDS kann den Zugriff auf den KMS Schlüssel für eine DB-Instance verlieren, z. B. wenn der KMS Schlüssel nicht aktiviert ist oder wenn der RDS Zugriff auf einen KMS Schlüssel widerrufen wird. Wenn das auftritt, geht die verschlüsselte DB-Instance für sieben Tage in einen wiederherstellbaren Zustand. Wenn die DB-Instance nach sieben Tagen nicht wieder auf den Schlüssel zugreifen kann, ist der Zugriff auf die Datenbank endgültig unmöglich und sie muss aus einem Backup wiederhergestellt werden. Weitere Informationen finden Sie unter Verschlüsselung einer DB-Instance.
- Wenn sich eine Read Replica und ihre verschlüsselte DB-Instance in derselben befinden AWS-Region, müssen Sie denselben KMS Schlüssel verwenden, um beide zu verschlüsseln.
- Implementieren Sie in AWS Config die rds-storage-encrypted AWS verwaltete Regel zur Validierung und Durchsetzung der Verschlüsselung für RDS DB-Instances und die rds-snapshots-encryptedRegel zur Validierung und Durchsetzung der Verschlüsselung für RDS Datenbanksnapshots.
- Verwenden Sie AWS Security Hub es, um zu beurteilen, ob Ihre RDS Amazon-Ressourcen den bewährten Sicherheitsmethoden entsprechen. Weitere Informationen finden Sie unter Security Hub-Steuerelemente für Amazon RDS.

Bewährte Methoden zur Verschlüsselung für AWS Secrets Manager

AWS Secrets Managerhilft Ihnen dabei, hartcodierte Anmeldeinformationen in Ihrem Code, einschließlich Kennwörtern, durch einen API Aufruf von Secrets Manager zu ersetzen, um das Geheimnis programmgesteuert abzurufen. Secrets Manager lässt sich integrieren AWS KMS , um jede Version jedes geheimen Werts mit einem eindeutigen Datenschlüssel zu verschlüsseln, der durch einen AWS KMS key geschützt ist. Diese Integration schützt gespeicherte Geheimnisse mit Verschlüsselungsschlüsseln, die niemals AWS KMS unverschlüsselt bleiben. Sie können auch benutzerdefinierte Berechtigungen für den KMS Schlüssel definieren, um die Vorgänge zu überwachen, mit denen die Datenschlüssel generiert, verschlüsselt und entschlüsselt werden, die gespeicherte Geheimnisse schützen. Weitere Informationen finden Sie unter Verschlüsseln und Entschlüsseln von Geheimnissen in AWS Secrets Manager.

Bedenken Sie die folgenden bewährten Verschlüsselungsmethoden für diesen Service:

- Verwenden Sie in der Schlüsselrichtlinie den ViaService Bedingungsschlüssel kms:, um die Verwendung des Schlüssels auf Anfragen von Secrets Manager zu beschränken, indem Sie den Wert `secretsmanager.<region>.amazonaws.com` zuweisen.
- Für zusätzliche Sicherheit, basierend auf den Geschäftsanforderungen, verwenden Sie Schlüssel oder Werte im Secrets Manager Manager-Verschlüsselungskontext als Bedingung für die Verwendung des KMS Schlüssels, indem Sie Folgendes erstellen:
  - Ein String-Bedingungsoperator in einer IAM Oder-Schlüsselrichtlinie
  - Eine Vergabeeinschränkung in einer Vergabe
- Implementieren Sie in die secretsmanager-using-cmk AWS verwaltete Regel AWS Config, um zu überprüfen, ob alle Geheimnisse in Secrets Manager mit einem AWS verwalteten KMS Schlüssel oder einem vom Kunden verwalteten KMS Schlüssel verschlüsselt sind.
- Um sicherzustellen, dass Geheimnisse den definierten Rotationsrichtlinien entsprechen, implementieren Sie die folgenden AWS Config Regeln:
  - secretsmanager-rotation-enabled-check— Prüft, ob die Rotation für im Secrets Manager gespeicherte Geheimnisse konfiguriert ist.
  - secretsmanager-scheduled-rotation-success-check — Prüft, ob Geheimnisse erfolgreich rotiert wurden. AWS Config prüft auch, ob das Datum der letzten Rotation innerhalb der konfigurierten Rotationsfrequenz liegt.
  - secretsmanager-secret-periodic-rotation— Prüft, ob Geheimnisse innerhalb der angegebenen Anzahl von Tagen ausgetauscht wurden.
  - secretsmanager-secret-unused— Prüft, ob innerhalb der angegebenen Anzahl von Tagen auf Geheimnisse zugegriffen wurde.
- Wird verwendet AWS CloudTrail , um alle API Aufrufe von Secrets Manager und alle API Nichtereignisse aufzuzeichnen, z. B. den Start der Rotation, den Erfolg der Rotation, die Fehlschläge bei der Rotation und das geplante Löschen von Geheimnissen. Weitere Informationen finden Sie unter AWS Secrets Manager Ereignisse protokollieren mit AWS CloudTrail.
- Verwenden Sie Amazon EventBridge, um Warnmeldungen für einige Secrets Manager Manager-Operationen zu konfigurieren, z. B. das Löschen von Geheimnissen, das Rotieren von Geheimnissen oder den Versuch, einen geheimen Schlüssel zu verwenden, dessen Löschung geplant ist. Sie können wählen, welche Vorgänge eine Warnung auslösen. Bei der Warnung kann es sich um ein Thema von Amazon Simple Notification Service (AmazonSNS) handeln, das eine E-Mail oder Textnachricht an Abonnenten sendet, oder es kann sich um eine AWS Lambda Funktion handeln, die die Details des Vorgangs zur späteren Überprüfung protokolliert.

Bewährte Methoden zur Verschlüsselung für Amazon S3

Amazon Simple Storage Service (Amazon S3) ist ein cloudbasierter Objektspeicherservice, der Sie beim Speichern, Schützen und Abrufen beliebiger Datenmengen unterstützt.

Für die serverseitige Verschlüsselung in Amazon S3 gibt es drei Optionen:

- Serverseitige Verschlüsselung mit von Amazon S3 verwalteten Verschlüsselungsschlüsseln (-S3) SSE
- Serverseitige Verschlüsselung mit (-) AWS Key Management Service SSE KMS
- Serverseitige Verschlüsselung mit vom Kunden bereitgestellten Verschlüsselungsschlüsseln (-C) SSE

Amazon S3 wendet serverseitige Verschlüsselung mit von Amazon S3 verwalteten Schlüsseln (SSE-S3) als Basisverschlüsselungsebene für jeden Bucket in Amazon S3 an. Ab dem 5. Januar 2023 werden alle neuen Objekt-Uploads auf Amazon S3 ohne zusätzliche Kosten und ohne Auswirkungen auf die Leistung automatisch verschlüsselt. Der automatische Verschlüsselungsstatus für die Standardverschlüsselungskonfiguration des S3-Buckets und für das Hochladen neuer Objekte ist in den AWS CloudTrail Protokollen, im S3-Inventar, in der S3-Speicherlinse, in der Amazon S3 S3-Konsole und als zusätzlicher Amazon S3 API S3-Antwortheader in den Feldern AWS Command Line Interface (AWS CLI) und AWS SDKs verfügbar. Weitere Informationen finden Sie unter Standardverschlüsselung FAQ.

Wenn serverseitige Verschlüsselung verwendet wird, um ein Objekt zum Zeitpunkt des Uploads zu verschlüsseln, fügen Sie der Anfrage den `x-amz-server-side-encryption` Header hinzu, um Amazon S3 anzuweisen, das Objekt mit SSE -S3, SSE - KMS oder -C zu verschlüsseln. SSE Die folgenden Werte sind für den Header möglich: `x-amz-server-side-encryption`

- `AES256`, was Amazon S3 anweist, die Regeln für von Amazon S3 verwaltete Schlüssel zu nutzen.
- `aws:kms`, was Amazon S3 anweist, AWS KMS verwaltete Schlüssel zu verwenden.
- Wert als `True` oder `False` für SSE -C festlegen

Weitere Informationen finden Sie unter efense-in-depth D-Anforderung 1: Daten müssen im Ruhezustand und während der Übertragung verschlüsselt werden in How to Use Bucket Policies and Apply Defense-in-Depth to Help Help Help Your Amazon S3 Data (AWS Blogbeitrag).

Für die clientseitige Verschlüsselung in Amazon S3 gibt es zwei Optionen:

- Ein Schlüssel, gespeichert in AWS KMS
- Ein Schlüssel, der in der Anwendung gespeichert ist

Bedenken Sie die folgenden bewährten Verschlüsselungsmethoden für diesen Service:

- Implementieren Sie in AWS Config die bucket-server-side-encryptionS3-aktivierte AWS verwaltete Regel, um die S3-Bucket-Verschlüsselung zu validieren und durchzusetzen.
- Stellen Sie eine Amazon-S3-Bucket-Richtlinie bereit, die bestätigt, dass alle hochgeladenen Objekte mit der `s3:x-amz-server-side-encryption`-Bedingung verschlüsselt sind. Weitere Informationen finden Sie in der Beispiel-Bucket-Richtlinie unter Daten mit SSE -S3 schützen und in den Anweisungen unter Hinzufügen einer Bucket-Richtlinie.
- Erlauben Sie nur verschlüsselte Verbindungen über HTTPS (TLS), indem Sie die `aws:SecureTransport` Bedingung für S3-Bucket-Richtlinien verwenden. Weitere Informationen finden Sie unter Welche S3-Bucket-Richtlinie sollte ich verwenden, um die AWS Config Regel s3-einzuhaltenbucket-ssl-requests-only?
- Implementieren Sie in AWS Config die von S3 bucket-ssl-requests-only AWS verwaltete Regel, sodass Anfragen zur Verwendung erforderlich sindSSL.
- Verwenden Sie einen vom Kunden verwalteten Schlüssel, wenn Sie kontoübergreifenden Zugriff auf Ihre Amazon-S3-Objekte gewähren möchten. Konfigurieren Sie die Schlüsselrichtlinie so, dass der Zugriff von einem anderen AWS-Konto möglich ist.

Bewährte Verschlüsselungsmethoden für Amazon VPC

Amazon Virtual Private Cloud (AmazonVPC) hilft Ihnen dabei, AWS Ressourcen in einem von Ihnen definierten virtuellen Netzwerk bereitzustellen. Dieses virtuelle Netzwerk entspricht einem herkömmlichen Netzwerk, wie Sie es in Ihrem Rechenzentrum betreiben, kann jedoch die Vorzüge der skalierbaren Infrastruktur von AWS nutzen.

Bedenken Sie die folgenden bewährten Verschlüsselungsmethoden für diesen Service:

- Verschlüsseln Sie den Verkehr zwischen Informationsressourcen und Systemen innerhalb des Unternehmensnetzwerks und VPCs verwenden Sie eine der folgenden Methoden:
  - AWS Site-to-Site VPN Verbindungen
  - Eine Kombination aus AWS Direct Connect Verbindungen AWS Site-to-Site VPN und, die eine IPsec -verschlüsselte private Verbindung ermöglicht

  - AWS Direct Connect Verbindungen, die MAC Security (MACsec) unterstützen, um Daten von Unternehmensnetzwerken zum Standort zu verschlüsseln AWS Direct Connect
- Verwenden Sie VPC Endpunkte, um eine private Verbindung AWS PrivateLink VPCs zu Ihrem unterstützten Gerät herzustellen, AWS-Services ohne ein Internet-Gateway zu verwenden. Sie können unsere AWS VPN Dienste verwenden AWS Direct Connect , um diese Verbindung herzustellen. Der Verkehr zwischen Ihrem VPC und dem anderen Dienst verlässt das AWS Netzwerk nicht. Weitere Informationen finden Sie unter Zugriff AWS-Services über AWS PrivateLink.
- Konfigurieren Sie Sicherheitsgruppenregeln, die nur Datenverkehr von Ports zulassen, die sicheren Protokollen zugeordnet sind, z. B. HTTPS über TCP /443. Überwachen Sie Sicherheitsgruppen und ihre Regeln regelmäßig.

Ressourcen

- Entwicklung einer unternehmensweiten Verschlüsselungsstrategie für Daten im Ruhezustand (AWS Prescriptive Guidance)
- Bewährte Sicherheitsmethoden für AWS Key Management Service(Dokumentation)AWS KMS
- Wie AWS-Services benutzt man AWS KMS (AWS KMS Dokumentation)
- Sicherheitssäule: Datenschutz (AWS Well-Architected Framework)

Dokumentverlauf

In der folgenden Tabelle werden wichtige Änderungen in diesem Leitfaden beschrieben. Wenn Sie über future Updates informiert werden möchten, können Sie einen RSSFeed abonnieren.

Änderung	Beschreibung	Datum
AWS-Service Aktualisierungen	Wir haben die Informati onen und Empfehlungen für Amazon Elastic Kubernetes Service (AmazonEKS) AWS Encryption SDK, Amazon Relational Database Service (AmazonRDS) und Amazon Simple Storage Service (Amazon S3) aktualisiert.	4. September 2024
Erste Veröffentlichung	—	2. Dezember 2022

AWS Glossar zu präskriptiven Leitlinien

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

Zahlen

7 Rs

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

- Faktorwechsel/Architekturwechsel – Verschieben Sie eine Anwendung und ändern Sie ihre Architektur, indem Sie alle Vorteile cloudnativer Feature nutzen, um Agilität, Leistung und Skalierbarkeit zu verbessern. Dies beinhaltet in der Regel die Portierung des Betriebssystems und der Datenbank. Beispiel: Migrieren Sie Ihre lokale Oracle-Datenbank auf die Amazon Aurora SQL Postgre-Compatible 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 (AmazonRDS) 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 Kundenbeziehungsmanagementsystem (CRM) zu Salesforce.com.
- Hostwechsel (Lift and Shift) – Verschieben Sie eine Anwendung in die Cloud, ohne Änderungen vorzunehmen, um die Cloud-Funktionen zu nutzen. Beispiel: Migrieren Sie Ihre lokale Oracle-Datenbank zu Oracle auf einer EC2 Instanz in der. AWS Cloud
- Verschieben (Lift and Shift auf Hypervisor-Ebene) – Verlagern Sie die Infrastruktur in die Cloud, ohne neue Hardware kaufen, Anwendungen umschreiben oder Ihre bestehenden Abläufe ändern zu müssen. Sie migrieren Server von einer lokalen Plattform zu einem Cloud-Dienst für dieselbe Plattform. Beispiel: Migrieren Sie eine Microsoft Hyper-V Anwendung zu AWS.
- Beibehaltung (Wiederaufgreifen) – Bewahren Sie Anwendungen in Ihrer Quellumgebung auf. Dazu können Anwendungen gehören, die einen umfangreichen Faktorwechsel erfordern und

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

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

A

ABAC

Siehe attributbasierte Zugriffskontrolle.

abstrahierte Dienste

Siehe Managed Services.

ACID

Siehe Atomarität, Konsistenz, Isolierung und Haltbarkeit.

Aktiv-Aktiv-Migration

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

Aktiv-Passiv-Migration

Eine Datenbankmigrationsmethode, bei der die Quell- und Zieldatenbanken synchron gehalten werden, aber nur die Quelldatenbank 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 darüber, wie AIOps es in der AWS Migrationsstrategie verwendet wird, finden Sie im Operations Integration Guide.

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.

Atomarität, 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 ABACfür 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 AWS , das Unternehmen bei der Entwicklung eines effizienten und effektiven Plans für die erfolgreiche Umstellung auf die Cloud unterstützt. AWS CAFgliedert 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 AWS CAF bietet es Anleitungen zur Personalentwicklung, Schulung und Kommunikation, um das Unternehmen auf eine erfolgreiche

Cloud-Einführung vorzubereiten. Weitere Informationen finden Sie AWS CAFauf der Website und im AWS CAFWhitepaper.

AWS Rahmen für die Qualifizierung der Arbeitslast ()AWS WQF

Ein Tool, das Workloads bei der Datenbankmigration bewertet, Migrationsstrategien empfiehlt und Arbeitsschätzungen bereitstellt. AWS WQFist in AWS Schema Conversion Tool ()AWS SCT enthalten. 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 Anrufe und ähnliche Aktionen 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 Änderungsdaten (CDC)

Der Prozess der Nachverfolgung von Änderungen an einer Datenquelle, z. B. einer Datenbanktabelle, und der Aufzeichnung von Metadaten zu der Änderung. Sie können es CDC für verschiedene Zwecke verwenden, z. B. zur 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 CCoEBeiträgen 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 einerCCoE, Einrichtung eines Betriebsmodells)
- Migration – Migrieren einzelner Anwendungen
- Neuentwicklung – Optimierung von Produkten und Services und Innovation in der Cloud

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

CMDB

Siehe Datenbank für das Konfigurationsmanagement.

Code-Repository

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

Kalter Cache

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

Kalte Daten

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

Computer Vision (CV)

Ein Bereich der KI, der maschinelles Lernen nutzt, um Informationen aus visuellen Formaten wie digitalen Bildern und Videos zu analysieren und zu extrahieren. AWS Panorama Bietet

beispielsweise Geräte an, die CV zu lokalen Kameranetzwerken hinzufügen, und Amazon SageMaker stellt Bildverarbeitungsalgorithmen für CV bereit.

Drift in der Konfiguration

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

Datenbank für das Konfigurationsmanagement () 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 Phase der Migration, die sich CMDB in der Phase der Portfolioerkennung und -analyse befindet.

Konformitätspaket

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

Kontinuierliche Bereitstellung und kontinuierliche Integration (CI/CD)

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

CV

Siehe Computer Vision.

D

Daten im Ruhezustand

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

Datenklassifizierung

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

Datendrift

Eine signifikante 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 an historischen Daten und werden in der Regel für Abfragen und Analysen verwendet.

Datenbankdefinitionssprache (DDL)

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

Sprache zur Datenbankmanipulation (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. DVSMerweitert den Prozess der Wertstromanalyse, der ursprünglich für Lean-Manufacturing-

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

digitaler Zwilling

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

Maßtabelle

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

Katastrophe

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

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 dazu, wie Sie domänengesteuertes Design mit dem Strangler-Fig-Muster verwenden können, finden Sie unter Modernizing legacy Microsoft. ASP NET(ASMX) schrittweise 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 der Wertströme in der Entwicklung.

E

EDA

Siehe explorative Datenanalyse.

Edge-Computing

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

Verschlüsselung

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

Verschlüsselungsschlüssel

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

Endianismus

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

Endpunkt

Siehe Service-Endpunkt.

Endpunkt-Services

Ein Dienst, den Sie in einer virtuellen privaten 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) Prinzipalen erstellen AWS PrivateLink und diesen Berechtigungen gewähren. Diese Konten oder Prinzipale können sich privat mit Ihrem Endpunktdienst verbinden, indem sie VPC Schnittstellenendpunkte erstellen. Weitere Informationen finden Sie unter Create an Endpoint Service in der Dokumentation zu Amazon Virtual Private Cloud (AmazonVPC).

Unternehmensressourcenplanung (ERP)

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

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 AWS CAF Sicherheitsepen 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

Weitere Informationen finden Sie unter 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. EDAwird durchgeführt, indem zusammenfassende Statistiken berechnet und Datenvisualisierungen erstellt werden.

F

Faktentabelle

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

schnell scheitern

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

Grenze zur Fehlerisolierung

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

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

Feature-Zweig

Siehe Zweig.

Features

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

Bedeutung der Feature

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

Featuretransformation

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

FGAC

Siehe Feinkörnige Zugriffskontrolle.

feinkörnige Zugriffskontrolle () FGAC

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

Flash-Cut-Migration

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

G

Geoblocking

Siehe geografische Einschränkungen.

Geografische Einschränkungen (Geoblocking)

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

Gitflow-Workflow

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

Greenfield-Strategie

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

Integritätsschutz

Eine Regel auf hoher Ebene, die dabei hilft, Ressourcen, Richtlinien und die Einhaltung von Vorschriften in allen Organisationseinheiten zu regeln (). OUs Präventiver Integritätsschutz setzt Richtlinien durch, um die Einhaltung von Standards zu gewährleisten. Sie werden mithilfe von Dienststeuerungsrichtlinien 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, eine gleichbleibend hohe Leistung bieten und unterschiedliche Lasten und Ausfälle mit minimalen Leistungseinbußen bewältigen.

historische Modernisierung

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

Homogene Datenbankmigration

Migrieren Sie Ihre Quelldatenbank in eine Zieldatenbank, die dieselbe Datenbank-Engine verwendet (z. B. Microsoft SQL Server zu Amazon RDS for 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 Principals zugeordnet ist und deren Berechtigungen innerhalb der AWS Cloud Umgebung definiert.

Leerlaufanwendung

Eine Anwendung mit einer durchschnittlichen CPU Speicherauslastung 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.

eingehend (Eingang) VPC

In einer Architektur AWS mit mehreren Konten, VPC die Netzwerkverbindungen von außerhalb einer Anwendung akzeptiert, überprüft und weiterleitet. In der AWS Sicherheitsreferenzarchitektur wird empfohlen, Ihr Netzwerkkonto mit eingehenden und ausgehenden Daten sowie Inspektionen 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 () IIoT

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).

Inspektion VPC

In einer Architektur AWS mit mehreren Konten, eine zentrale Architektur, 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 von Modellen für maschinelles Lernen mit. AWS

IoT

Siehe Internet der Dinge.

IT-Informationsbibliothek (ITIL)

Eine Reihe von bewährten Methoden für die Bereitstellung von IT-Services und die Abstimmung dieser Services auf die Geschäftsanforderungen. ITILbietet die Grundlage fürITSM.

IT-Servicemanagement (ITSM)

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 Operations Integration Guide.

ITIL

Weitere Informationen finden Sie in der IT-Informationsbibliothek.

ITSM

Siehe IT-Servicemanagement.

L

Labelbasierte Zugriffskontrolle () LBAC

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

Landing Zone

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

Große Migration

Eine Migration von 300 oder mehr Servern.

LBAC

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 in der Dokumentation unter Anwenden von Berechtigungen mit den geringsten Rechten. IAM

Lift and Shift

Siehe 7 Rs.

Little-Endian-System

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

Niedrigere Umgebungen

Siehe Umwelt.

M

Machine Learning (ML)

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

Hauptzweig

Siehe Filiale.

Malware

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

verwaltete Dienste

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

Fertigungsleitsystem () 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.

MES

Siehe Manufacturing Execution System.

Message Queuing-Telemetrietransport () MQTT

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

Microservice

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

Microservices-Architekturen

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

Migration Acceleration Program (MAP)

Ein AWS Programm, das Beratung, Unterstützung, Schulungen und Services bietet, um Unternehmen dabei zu unterstützen, eine solide betriebliche Grundlage für die Umstellung auf die Cloud zu schaffen und die anfänglichen Kosten von Migrationen auszugleichen. MAPumfasst 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 von Migration Factory gehören in der Regel Betriebsanalysten 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.

Bewertung des Migrationsportfolios () MPA

Ein Online-Tool, das Informationen zur Validierung des Geschäftsszenarios für die Migration auf das bereitstellt. AWS Cloud MPAbietet eine detaillierte Portfoliobewertung (richtige Servergröße, Preisgestaltung, TCO Vergleiche, Analyse der Migrationskosten) sowie Migrationsplanung (Analyse und Datenerfassung von Anwendungen, Gruppierung von Anwendungen, Priorisierung der Migration und Wellenplanung). Das MPATool (Anmeldung erforderlich) steht allen AWS Beratern und APN Partnerberatern kostenlos zur Verfügung.

Bewertung der Eignung für die Migration (MRA)

Der Prozess der Gewinnung von Erkenntnissen über den Cloud-Bereitschaftsstatus eines Unternehmens, der Identifizierung von Stärken und Schwächen und der Erstellung eines Aktionsplans zur Schließung festgestellter Lücken unter Verwendung von AWS CAF. Weitere Informationen finden Sie im Benutzerhandbuch für Migration Readiness. MRAist die erste Phase der AWS Migrationsstrategie.

Migrationsstrategie

Der Ansatz, der verwendet wird, um einen Workload auf den zu migrieren AWS Cloud. 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.

OCM

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 betrieblicher 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 Offene Prozesskommunikation — Einheitliche Architektur.

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 betrieblicher Ebene () OLA

Eine Vereinbarung, in der klargestellt wird, welche funktionalen IT-Gruppen sich gegenseitig versprechen, um eine Vereinbarung auf Serviceniveau zu unterstützen (). SLA

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 Änderungsmanagement (OCM)

Ein Framework für das Management wichtiger, disruptiver Geschäftstransformationen aus Sicht der Mitarbeiter, der Kultur und der Führung. OCMunterstützt Unternehmen bei der Vorbereitung und Umstellung auf neue Systeme und Strategien, indem es die Einführung von Veränderungen beschleunigt, Übergangsprobleme angeht und kulturelle und organisatorische Veränderungen vorantreibt. In der AWS Migrationsstrategie wird dieses Framework als Mitarbeiterbeschleunigung bezeichnet, da bei Projekten zur Cloud-Einführung die Geschwindigkeit des Wandels erforderlich ist. Weitere Informationen finden Sie im OCMLeitfaden.

ursprüngliche Zugriffskontrolle (OAC)

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

ursprüngliche Zugriffsidentität () OAI

In CloudFront, eine Option zur Zugriffsbeschränkung, um Ihre Amazon S3 S3-Inhalte zu sichern. Wenn Sie es verwendenOAI, 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, welche eine detailliertere und erweiterte Zugriffskontrolle bietet.

ORR

Siehe Überprüfung der Betriebsbereitschaft.

NICHT

Siehe Betriebstechnologie.

ausgehend (Ausgang) VPC

In einer Architektur AWS mit mehreren Konten eine, VPC die Netzwerkverbindungen verarbeitet, die von einer Anwendung aus initiiert werden. In der AWS Security Reference Architecture wird empfohlen, Ihr Netzwerkkonto mit eingehenden und ausgehenden Daten und Inspektionen einzurichten, 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 zugewiesen wird, um die maximalen Berechtigungen festzulegen, die der Benutzer oder die Rolle haben kann. Weitere Informationen finden Sie in der IAM Dokumentation unter Grenzen von Berechtigungen.

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 hierfür PII sind Namen, Adressen und Kontaktinformationen.

PII

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 einen AWS-Konto, eine IAM Rolle oder

einen Benutzer. Weitere Informationen finden Sie in der IAM Dokumentation unter Principal in Roles (Begriffe und Konzepte).

Datenschutz durch Design

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

Privat gehostete Zonen

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

proaktive Steuerung

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

Produktlebenszyklusmanagement (PLM)

Das Management von Daten und Prozessen für ein Produkt während seines gesamten Lebenszyklus, von der Konstruktion, Entwicklung und Markteinführung über Wachstum und Reife bis hin zu Verkauf und Verkauf.

Produktionsumgebung

Siehe Umgebung.

programmierbare Logiksteuerung (PLC)

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

Pseudonymisierung

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

veröffentlichen/abonnieren (pub/sub)

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

RACIMatrix

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

Ransomware

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

RASCIMatrix

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.

Ziel des Wiederherstellungspunkts (RPO)

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

Ziel für die Wiederherstellungszeit (RTO)

Die maximal zulässige Verzögerung zwischen der Unterbrechung des Dienstes 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.

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

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 RASCIMatrix bezeichnet, und wenn Sie sie ausschließen, wird sie als RACIMatrix bezeichnet.

Reaktive Kontrolle

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

Beibehaltung

Siehe 7 Rs.

zurückziehen

Siehe 7 Rs.

Drehung

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

Zugriffskontrolle für Zeilen und Spalten (RCAC)

Die Verwendung einfacher, flexibler SQL Ausdrücke, die über definierte Zugriffsregeln verfügen. RCACbesteht 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

SAML2.0

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

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.

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 (SIEM)

Tools und Dienste, die Systeme zur Verwaltung von Sicherheitsinformationen (SIM) und zur Verwaltung 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.

Richtlinie zur Dienststeuerung (SCP)

Eine Richtlinie, die eine zentrale Kontrolle über die Berechtigungen für alle Konten in einer Organisation in AWS Organizations ermöglicht. SCPsDefinieren 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

Der 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.

Vereinbarung zum Servicelevel () SLA

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

Indikator für das Serviceniveau () SLI

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

Ziel auf Serviceniveau () 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

Weitere Informationen finden Sie unter System zur Verwaltung von Sicherheitsinformationen und Ereignissen.

zentraler Fehlerpunkt (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.

SLO

Siehe Service-Level-Ziel.

split-and-seed Modell

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

SPOF

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 Modernizing legacy MicrosoftASP. NET(ASMX) schrittweise Webservices mithilfe von Containern und Amazon API Gateway.

Subnetz

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

Aufsichtskontrolle und Datenerfassung (SCADA)

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

Symmetrische Verschlüsselung

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

synthetisches Testen

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

T

tags

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

Zielvariable

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

Aufgabenliste

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

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

Testumgebungen

Siehe Umgebung.

Training

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

Transit-Gateway

Ein 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.

VPCPeering

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

Schwachstelle

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

W

Warmer Cache

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

warme Daten

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

Fensterfunktion

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

Workload

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

Workstream

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

WORM

Sehen Sie einmal, schreiben Sie einmal, lesen Sie viele.

WQF

Siehe AWSWorkload-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 wird als unveränderlich angesehen.

Z

Zero-Day-Exploit

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

Zero-Day-Sicherheitslücke

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

Zombie-Anwendung

Eine Anwendung mit einer durchschnittlichen CPU Speicherauslastung von unter 5 Prozent. 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.