Erstellen einer unternehmensweiten Verschlüsselungsstrategie für Daten im Ruhezustand

AWS Präskriptive Leitlinien

AWS Präskriptive Leitlinien: Erstellen einer unternehmensweiten Verschlüsselungsstrategie für Daten im Ruhezustand

Table of Contents

Entwicklung einer unternehmensweiten Verschlüsselungsstrategie für ruhende Daten

Venki Srivatsav, Andrea Di Fabio und Vikramaditya Bhatnagar, Amazon Web Services (AWS)

September 2022 (Dokumentengeschichte)

Viele Unternehmen sind besorgt über die Bedrohung der Cybersicherheit durch eine Datenschutzverletzung. Bei einem Datenleck verschafft sich eine unbefugte Person Zugriff auf Ihr Netzwerk und stiehlt Unternehmensdaten. Firewalls und Anti-Malware-Dienste können zum Schutz vor dieser Bedrohung beitragen. Ein weiterer Schutz, den Sie implementieren können, ist die Datenverschlüsselung. Im Abschnitt Über Datenverschlüsselung dieses Handbuchs erfahren Sie mehr darüber, wie Datenverschlüsselung funktioniert und welche Typen verfügbar sind.

Wenn Sie über Verschlüsselung sprechen, gibt es im Allgemeinen zwei Arten von Daten. Transitdaten 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. Diese Strategie konzentriert sich auf Daten im Ruhezustand. Weitere Informationen zur Verschlüsselung von Daten während der Übertragung finden Sie unter Schutz von Daten bei der Übertragung (AWSWell-Architected Framework).

Eine Verschlüsselungsstrategie besteht aus vier Teilen, die Sie in aufeinanderfolgenden Phasen entwickeln. Die Verschlüsselungsrichtlinie wird von der Geschäftsleitung festgelegt und beschreibt die regulatorischen, Compliance-Anforderungen und Geschäftsanforderungen für die Verschlüsselung. Die Verschlüsselungsstandards helfen denjenigen, die die Richtlinie umsetzen, sie zu verstehen und einzuhalten. Standards können technologischer oder verfahrenstechnischer Natur sein. Das Framework besteht aus den Standardarbeitsanweisungen, Strukturen und Leitplanken, die die Umsetzung der Standards unterstützen. Schließlich ist die Architektur die technische Implementierung Ihrer Verschlüsselungsstandards, wie z. B. die Umgebung, Dienste und Tools, die Sie verwenden. Ziel dieses Dokuments ist es, Sie bei der Entwicklung einer Verschlüsselungsstrategie zu unterstützen, die Ihren Geschäfts-, Sicherheits- und Compliance-Anforderungen entspricht. Es enthält Empfehlungen zur Überprüfung und Implementierung von Sicherheitsstandards für gespeicherte Daten, damit Sie Ihre Compliance- und Geschäftsanforderungen auf ganzheitliche Weise erfüllen können.

Diese Strategie verwendetAWS Key Management Service (AWS KMS), um Sie bei der Erstellung und Verwaltung kryptografischer Schlüssel zu unterstützen, die zum Schutz Ihrer Daten beitragen.

AWS KMSlässt sich in vieleAWS Dienste integrieren, um all Ihre Daten im Ruhezustand zu verschlüsseln. Auch wenn Sie sich für einen anderen Verschlüsselungsdienst entscheiden, können Sie die Empfehlungen und Phasen in diesem Handbuch trotzdem anwenden.

Zielgruppe

Die Strategie zielt darauf ab, die folgenden Zielgruppen anzusprechen:

- Führungskräfte, die Richtlinien für ihr Unternehmen formulieren, wie 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
- Compliance- und Governance-Beauftragte, die für die Überwachung der Einhaltung der Compliance-Richtlinien, einschließlich gesetzlicher und freiwilliger Compliance-Regelungen, zuständig sind

Gezielte Geschäftsergebnisse

- Data-at-rest Verschlüsselungsrichtlinie — Entscheidungsträger und politische Entscheidungsträger können eine Verschlüsselungsrichtlinie erstellen und die kritischen Faktoren verstehen, die sich auf die Richtlinie auswirken.
- ata-at-rest D-Verschlüsselungsstandards — Technische Führungskräfte können Verschlüsselungsstandards entwickeln, die auf der Verschlüsselungsrichtlinie basieren.
- Framework für Verschlüsselung — Technische Führungskräfte und Implementierer können ein Framework schaffen, das als Brücke zwischen denjenigen, die die Richtlinie festlegen, und denen, die die Standards erstellen, fungiert. Framework bedeutet in diesem Zusammenhang, den geeigneten Prozess und Arbeitsablauf zu identifizieren, der Ihnen hilft, die Standards innerhalb der Richtlinien umzusetzen. Ein Framework ähnelt einer Standardarbeitsanweisung oder einem Change-Management-Prozess zur Änderung von Richtlinien oder Standards.
- Technische Architektur und Implementierung — Praktische Implementierer wie Entwickler und Architekten sind sich der verfügbaren Architekturreferenzen bewusst, die ihnen bei der Implementierung der Verschlüsselungsstrategie helfen können.

Einschränkungen

Dieses Dokument soll Ihnen helfen, eine benutzerdefinierte Verschlüsselungsstrategie zu formulieren, die den Anforderungen Ihres Unternehmens am besten entspricht. Es ist keine Verschlüsselungsstrategie selbst und es ist keine Compliance-Checkliste. Die folgenden Themen sind in diesem Dokument nicht enthalten:

- Verschlüsseln von Daten während der Übertragung
- Aufgliederung in Token
- Hashing
- Einhaltung von Vorschriften und Datenverwaltung
- Budgetierung für Ihr Verschlüsselungsprogramm

Weitere Informationen zu diesen Abschnitten enthalten die folgendenRessourcen Abschnitte.

Über Datenverschlüsselung

Dieser Abschnitt enthält einen allgemeinen Überblick über Verschlüsselungskonzepte und -terminologie. Nähere Informationen finden Sie unter Kryptografie-Konzepte (Leitfaden fürAWS kryptografische Dienste und Tools). Datenverschlüsselung hilft Ihnen, die Vertraulichkeit Ihrer Daten durchzusetzen. Durch die Implementierung von Verschlüsselung und Zugriffskontrollen können Sie dazu beitragen, die Daten in Ihrem Unternehmen zu schützen.

Über die Verschlüsselung

Verschlüsselungsdienste verwenden einen Verschlüsselungsschlüssel, um Daten zu verschlüsseln. Ein Verschlüsselungsschlüssel ist eine kryptografische Zeichenfolge von zufälligen Bits, die durch einen Verschlüsselungsalgorithmus generiert wird. Schlüssel können unterschiedlich lang sein, und jeder Schlüssel ist so konzipiert, dass er unberechenbar und einzigartig ist. Die Stärke der Verschlüsselung hängt typischerweise von zwei Faktoren ab: der Länge des Schlüssels und dem verwendeten Algorithmus. Im Allgemeinen sorgen längere Schlüssel für eine stärkere Verschlüsselung.

Über Verschlüsselungsalgorithmen

Es gibt zwei Arten von Algorithmen zur Generierung von Verschlüsselungsschlüsseln: symmetrische und asymmetrische.

Die symmetrische Verschlüsselung verwendet denselben Schlüssel zum Verschlüsseln und Entschlüsseln der Daten. Diese Art der Verschlüsselung ist in der Regel schneller und daher für große Datenmengen effizient. Diese Art der Verschlüsselung ist weit verbreitet und wird allgemein als sicher angesehen. Da ein einziger Schlüssel sowohl für die Verschlüsselung als auch für die Entschlüsselung verwendet wird, empfiehlt es sich, den Schlüssel häufig zu ändern, um zu verhindern, dass eine unbefugte Person ihn erhält. Weitere Informationen darüber, wann symmetrische Verschlüsselung empfohlen wird, finden SieWann benötige ich symmetrische Verschlüsselung? im FAQ-Bereich.

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

allgemein als sicherer angesehen als symmetrische Verschlüsselung, sie ist jedoch langsamer, da sie längere Schlüssellängen verwendet und komplexere Verschlüsselungsberechnungen erfordert. Weitere Informationen darüber, wann eine asymmetrische Verschlüsselung empfohlen wird, finden SieWann benötige ich eine asymmetrische Verschlüsselung? im FAQ-Bereich.

Über Envelope-Verschlüsselung

Wenn Sie Ihre Daten verschlüsseln, sind sie nur geschützt, solange Ihr Verschlüsselungsschlüssel geheim bleibt. Der Schlüssel, der zum Verschlüsseln der Daten verwendet wird, wird als Datenschlüssel bezeichnet. Bei der Umschlagverschlüsselung wird Ihr Datenschlüssel mit einem anderen Verschlüsselungsschlüssel verschlüsselt, der als Schlüsselverschlüsselungsschlüssel bezeichnet wird. Sie können diesen Schlüssel sogar mit einem anderen Verschlüsselungsschlüssel verschlüsseln usw. Schließlich muss ein Schlüssel im Klartext bleiben, damit Sie die Schlüssel und Ihre Daten entschlüsseln können. Dieser Top-Level-Klartext-Verschlüsselungsschlüssel zum Verschlüsseln von Schlüsseln wird als Stammschlüssel bezeichnet.

Envelope-Verschlüsselung bietet mehrere Vorteile:

- Komfort — Da Ihr Datenschlüssel verschlüsselt ist, können Sie ihn zusammen mit den verschlüsselten Daten speichern.
- Effizienz — Verschlüsselungsvorgänge können zeitaufwändig sein, insbesondere wenn es sich um eine große Datenmenge handelt. Statt Rohdaten mit verschiedenen Schlüsseln mehrmals neu zu verschlüsseln, können Sie einfach die Datenschlüssel, die die Rohdaten schützen, neu verschlüsseln. Auf diese Weise können Sie zwei oder mehr Verschlüsselungsebenen bereitstellen, ohne die Daten erneut zu verschlüsseln.
- Leistung — Sie können Verschlüsselungsalgorithmen kombinieren. Sie können beispielsweise die symmetrische Verschlüsselung für die Rohdaten verwenden, aber die asymmetrische Verschlüsselung für den Datenschlüssel verwenden, wodurch die Stärken beider Verschlüsselungsalgorithmen kombiniert werden.

Weitere Informationen zur Envelope-Verschlüsselung finden Sie unter Envelope-Verschlüsselung (AWS Key Management ServiceDokumentation). Weitere Informationen zur Entscheidung, ob Sie eine Briefumschlagverschlüsselung benötigen, finden SieWann benötige ich eine Briefumschlagverschlüsselung? im FAQ-Bereich.

Phasen der Entwicklung einer Verschlüsselungsstrategie

Die Entwicklung einer Verschlüsselungsstrategie auf Unternehmensebene erfordert einen mehrstufigen Ansatz. Jede Phase definiert eine Reihe von Kontrollen, mit denen Sie die gewünschten, greifbaren Ergebnisse erzielen können. Dieses Dokument führt Sie durch diese Phasen und stellt Ihnen spezifische Fragen, die Ihnen helfen, Ihre Verschlüsselungsstrategie anzupassen.

Die Entwicklung einer Verschlüsselungsstrategie für ruhende Daten besteht aus den folgenden aufeinanderfolgenden Phasen:

1. Verschlüsselungsrichtlinie— Erstellen Sie eine Richtlinie, die die data-at-rest Verschlüsselungsziele für Ihr Unternehmen definiert.
2. Verschlüsselungsstandards— Definieren Sie die technischen und verfahrenstechnischen Standards, die Ihnen bei der Umsetzung Ihrer Unternehmenspolitik helfen.
3. Verschlüsselungs-Framework— Entwickeln Sie das Framework, das allen Beteiligten hilft, Ihre Verschlüsselungsstandards zu verstehen, zu ändern und zu implementieren.
4. Implementierung— Stellen Sie Ihre Verschlüsselungsinfrastruktur bereit.

Verschlüsselungsrichtlinie

Der Zweck einer Verschlüsselungsrichtlinie besteht darin, auf Führungsebene die Geschäfts- und Compliance-Erwartungen festzulegen, die das Unternehmen erfüllen muss. Die Richtlinie dient als Ausgangspunkt für die Definition einer geeigneten Verschlüsselungsstrategie. Die Politik sollte abstrakt genug sein, um Freiheit und Flexibilität bei der Umsetzung zu bieten. Gleichzeitig muss es spezifisch genug sein, um die Grenzen einer akzeptablen Implementierung zu definieren, die den organisatorischen Zielen entspricht. Im Allgemeinen sind Richtlinien technologieunabhängig und werden nur sehr selten geändert, da sie die grundlegenden Merkmale Ihrer Unternehmensverschlüsselungsstrategie definieren.

In der Regel enthalten Verschlüsselungsrichtlinien Folgendes, sind aber nicht darauf beschränkt:

- Alle regulatorischen Vorschriften oder Compliance-Regelungen, die Ihr Unternehmen erfüllen muss
- Alle geschäftlichen Verpflichtungen oder Erwartungen in Bezug auf Datenverschlüsselung
- Die Art der Daten, die verschlüsselt werden müssen

- Kriterien dafür, wann andere Datenschutztechniken als Verschlüsselung verwendet werden sollten, wie Hashing oder Tokenisierung

In der Regel definiert und genehmigt die oberste Managementebene des Unternehmens, wie der CIO, der CTO und der CISO, die Verschlüsselungsrichtlinie.

Bitte beachten Sie beim Erstellen Ihrer Verschlüsselungsrichtlinie Folgendes:

- Ihr Geschäftsbereich bestimmt, welche Compliance- und Regulierungsvorschriften Sie einhalten müssen. Diese Regelungen schreiben die Anforderungen an die Datenverschlüsselung vor. Entscheidungen auf Führungsebene, das Geschäft in neue Regionen auszudehnen oder das Produktangebot zu erweitern, können sich darauf auswirken, welche Vorschriften für Ihre Daten gelten. Wenn eine Bank beispielsweise beschließt, ihren Kunden Kreditkarten anzubieten, müssen diese wahrscheinlich den Data Security Standard (PCI-DSS) der Zahlungskartenbranche einhalten, der eine Datenverschlüsselung erfordert.
- Ihre Richtlinie sollte angeben, welche Art von Daten verschlüsselt werden muss. Dies hängt von den Compliance-Anforderungen und den Datenverarbeitungszielen Ihres Unternehmens ab. Ihre Richtlinie könnte beispielsweise vorsehen, dass alle Daten, die das Unternehmen erfasst oder besitzt, im Speicher verschlüsselt werden müssen.
- Ihre Verschlüsselungsrichtlinie muss Ihren internen Datenkategorisierungsstandards entsprechen. Um eine effektive Verschlüsselungsrichtlinie zu formulieren, ist die Festlegung von Datenkategorien auf Metadatenebene erforderlich. Ihre Kategorien können beispielsweise öffentliche, interne, vertrauliche, geheime oder Kundendaten enthalten.
- Geben Sie Kriterien an, wie festgelegt werden kann, welche Daten verschlüsselt und welche Daten mit einer anderen Technik wie Tokenisierung oder Hashing geschützt werden sollten. In Ihrer Richtlinie könnte beispielsweise festgelegt werden, dass alle personenbezogenen Daten (PII), die in die Audit-, Trace- oder Anwendungsprotokolle aufgenommen werden, tokenisiert werden müssen.

Verschlüsselungsstandards

Standards werden aus Ihrer Richtlinie abgeleitet. Diese haben einen engeren Anwendungsbereich und helfen dabei, den Rahmen und die Architektur für die Implementierung zu definieren. Wenn die Richtlinie Ihres Unternehmens beispielsweise darin besteht, Ihre gespeicherten Daten zu verschlüsseln, würde ein Standard definieren, welche Art von Verschlüsselung erforderlich ist, und allgemeine Anweisungen zur Einhaltung der Richtlinie enthalten.

Verschlüsselungsstandards spezifizieren in der Regel Folgendes:

- Die Arten der Verschlüsselung, die verwendet werden sollten
- Mindestspezifikationen für die Verschlüsselung
- Wer hat Zugriff auf Verschlüsselungsschlüssel
- Wo Verschlüsselungsschlüssel gespeichert werden sollten
- Kriterien für die Auswahl einer geeigneten Schlüsselstärke bei der Auswahl von Verschlüsselungs- oder Hashing-Techniken
- Schlüsselrotation

Während Sie selten eine Verschlüsselungsrichtlinie aktualisieren müssen, können sich die Verschlüsselungsstandards ändern. Die Cybersicherheitsbranche entwickelt sich ständig weiter, um der sich ständig ändernden Bedrohungslandschaft gerecht zu werden. Daher sollten sich Ihre Standards ändern, um die neuesten Technologien und Best Practices zu übernehmen, um Ihren Unternehmensdaten den bestmöglichen Schutz zu bieten.

In einer Unternehmensorganisation definieren Vizepräsidenten, Direktoren oder Datenverwalter in der Regel Verschlüsselungsstandards, und ein Compliance-Beauftragter überprüft und genehmigt sie in der Regel.

Berücksichtigen Sie bei der Definition und Pflege von Verschlüsselungsstandards in Ihrem Unternehmen die folgenden Kategorien von Faktoren:

- Kosten- und Leistungsüberlegungen
- Schlüsselzugriffskontrolle
- Verschlüsselungstypen
- Verschlüsselungsschlüssel-Spezifikationen
- Wichtiger Lagerort

Kosten- und Leistungsüberlegungen

Berücksichtigen Sie bei der Festlegung von Verschlüsselungsstandards für gespeicherte Daten die folgenden Betriebsfaktoren:

- Die verfügbaren Hardwareressourcen müssen in der Lage sein, Ihre Standards in großem Maßstab zu unterstützen.

- Die Kosten für die Verschlüsselung hängen von der Länge des Schlüssels, der Datenmenge und der Zeit ab, die für die Verschlüsselung erforderlich ist. Im Vergleich zur symmetrischen Verschlüsselung verwendet die asymmetrische Verschlüsselung beispielsweise längere Schlüssel und benötigt mehr Zeit.
- Berücksichtigen Sie die Leistungsanforderungen Ihrer Unternehmensanwendungen. Wenn Ihre Anwendung eine niedrige Latenz und einen hohen Durchsatz erfordert, sollten Sie möglicherweise symmetrische Verschlüsselung verwenden.

Schlüsselzugriffskontrolle

Identifizieren Sie die Zugriffskontrollrichtlinien für Ihre Verschlüsselung, die auf dem Prinzip der geringsten Zugriffsrechte basiert. Least Privilege ist die bewährte Sicherheitsmethode, Benutzern den Mindestzugriff zu gewähren, den sie zur Erfüllung ihrer Aufgaben benötigen. Definieren Sie in Ihren Standards eine Zugriffskontrollrichtlinie, die:

- Identifiziert die Rollen, die die Schlüssel- und Datenschlüssel verwalten.
- Definiert wichtige Berechtigungen und ordnet sie Rollen zu. Es definiert beispielsweise, wer wichtige Administratorrechte hat und wer wichtige Benutzerrechte hat. Schlüsseladministratoren können Schlüssel zur Schlüsselverschlüsselung erstellen oder ändern, und wichtige Benutzer können Daten ver- und entschlüsseln und Datenschlüssel generieren.

Verschlüsselungstypen

Definieren Sie in Ihren Standards, welche Verschlüsselungstypen und -funktionen für Ihr Unternehmen geeignet sind:

- Dokumentieren Sie, wann symmetrische und asymmetrische Verschlüsselungsalgorithmen verwendet werden sollten. Weitere Informationen finden Sie unterWann benötige ich symmetrische Verschlüsselung? undWann benötige ich eine asymmetrische Verschlüsselung? im FAQ-Bereich.
- Entscheiden Sie, ob Sie die Umschlagverschlüsselung verwenden sollten, und definieren Sie die Umstände. Weitere Informationen finden SieWann benötige ich eine Briefumschlagverschlüsselung? im -Abschnitt unter — Häufig gestellte Fragen.
- Definieren Sie Kriterien für die Verwendung von Verschlüsselungsalternativen wie Tokenisierung und Hashing.

Verschlüsselungsschlüssel-Spezifikationen

Definieren Sie die erforderlichen Spezifikationen für Ihre Verschlüsselungsschlüssel, wie Schlüsselstärke und Algorithmen. Diese Spezifikationen müssen den in der Richtlinie festgelegten Vorschriften und Compliance-Regelungen entsprechen. Erwägen Sie, die folgenden Spezifikationen zu definieren:

- Definieren Sie die Mindestschlüsselstärke und die Mindestalgorithmen für symmetrische und asymmetrische Verschlüsselungstypen. Zu den Schlüsselfaktoren gehören Länge, Zufälligkeit und Einzigartigkeit.
- Definieren Sie, wann Sie neue Versionen von Verschlüsselungsalgorithmen implementieren möchten. Ihre Standards könnten beispielsweise lauten: Implementieren Sie die neueste Version des Algorithmus innerhalb von 30 Tagen nach der Veröffentlichung oder verwenden Sie immer eine Version, die älter ist als die neueste Version.
- Definieren Sie das Intervall für die Rotation Ihrer Verschlüsselungsschlüssel.

Wichtiger Lagerort

Beachten Sie in Ihren Standards Folgendes, wenn Sie entscheiden, wo Ihre Verschlüsselungsschlüssel gespeichert werden sollen:

- Konformität und gesetzliche Anforderungen können vorschreiben, wo Ihre Verschlüsselungsschlüssel gespeichert werden können.
- Entscheiden Sie, ob Sie Schlüssel an einem zentralen Ort oder mit den entsprechenden Daten speichern möchten. Weitere Informationen finden SieWarum sollte ich Verschlüsselungsschlüssel zentral verwalten? im -Abschnitt unter — Häufig gestellte Fragen.
- Wenn Sie sich für zentralisierten Speicher entscheiden, entscheiden Sie, ob Sie Schlüssel in einer vom Unternehmen verwalteten Infrastruktur speichern möchten, z. B. in einem Hardware-Sicherheitsmodul (HSM), oder in einem Managed Service Provider, z.AWS Key Management Service B. Weitere Informationen finden SieWann muss ich ein Hardwaresicherheitsmodul (HSM) verwenden? im -Abschnitt unter — Häufig gestellte Fragen.

Verschlüsselungs-Framework

Ein Framework bezieht sich in diesem Zusammenhang auf eine Reihe von Standardarbeitsanweisungen, die befolgt werden müssen, wenn Sie die Verschlüsselungsstandards

oder -richtlinien ändern. Das Framework ist das Gerüst, das Ihnen bei der Umsetzung der Standards hilft. Es hilft, Worte in Taten umzuwandeln. Das Framework verbindet die Personen, die Standards definieren, mit den Personen, die sie umsetzen.

Frameworks umfassen in der Regel die folgenden Themen:

- Datenklassifizierung
- Klassifizierung der Umwelt
- Veränderungsereignisse und -prozesse

Datenklassifizierung

Die Datenklassifizierung spielt eine wichtige Rolle bei der Entwicklung einer Verschlüsselungsstrategie. Bei der Datenklassifizierung werden Daten einer Kategorie zugewiesen, die auf der Sensitivität der Daten basiert. Die folgenden Kategorien sind gängige Datenklassifizierungskategorien, in aufsteigender Reihenfolge ihrer Sensibilität, aufgeführt: öffentlich, privat, intern, vertraulich und eingeschränkt.

Ihr Verschlüsselungsframework sollte die folgenden Informationen zur Datenklassifizierung enthalten:

- Die Datenklassifizierungskategorien für Ihr Unternehmen.
- Die Klassifizierungskriterien, die verwendet werden, um Daten in die entsprechende Kategorie einzuordnen. Beispielsweise könnte das Handelsrezept eines Unternehmens als eingeschränkt eingestuft werden, personenbezogene Daten von Mitarbeitern könnten vertraulich sein und die interne Kommunikation zwischen Mitarbeitern über offizielle Kanäle könnte intern erfolgen.
- Das Verfahren zur Heraufstufung und Herabstufung von Daten zwischen Kategorien.
- Die Zugriffskriterien für jede Datenklassifizierungskategorie.
- Die Art des Verschlüsselungsschlüssels, der für jede Kategorie erforderlich ist.

Klassifizierung der Umwelt

Ihr Unternehmen verfügt möglicherweise über mehrere Umgebungen wie Entwicklung, Testing, Sandbox, Vorproduktion und Produktion. Jede Umgebung kann unterschiedliche Datentypen enthalten und unterschiedliche Verschlüsselungsanforderungen haben.

Ihr Verschlüsselungs-Framework sollte die folgenden Informationen zu Ihren Umgebungen enthalten:

- Definieren Sie Ihre Unternehmensumgebungen.
- Definieren Sie die Verschlüsselungsanforderungen für jede Umgebung. Sie können beispielsweise einen einzigen Verschlüsselungsschlüssel für alle Datenkategorien in Ihrer Entwicklungsumgebung verwenden, und in Ihrer Produktionsumgebung können Sie für jede Geschäftsanwendung oder Datenklassifizierungskategorie unterschiedliche Verschlüsselungsschlüssel verwenden.

Veränderungsereignisse und -prozesse

Verschlüsselungsstandards unterliegen häufigen Änderungen, sodass Sie mit den neuesten Technologien, Best Practices und Innovationen Schritt halten können. Im Folgenden sind häufig auftretende Änderungsereignisse aufgeführt, die zu einer Überarbeitung Ihrer Verschlüsselungsstandards führen können:

- Änderungen der Mindestlänge von Verschlüsselungsschlüsseln
- Änderungen der Stärke eines Verschlüsselungsalgorithmus
- Änderungen daran, wer auf Verschlüsselungsschlüssel zugreifen kann und wie
- Änderungen der Rotationsintervalle für Ihre Tasten
- Änderungen am Prozess zum Löschen von Schlüsseln
- Änderungen des wichtigsten Speicherorts oder der Richtlinien
- Änderungen am Verfahren zum Sichern und Wiederherstellen von Schlüssels

Ihr Verschlüsselungsframework sollte Folgendes enthalten, um Ihr Unternehmen auf die Verwaltung, Implementierung und Kommunikation von Änderungen der Verschlüsselungsstandards oder -richtlinien vorzubereiten:

- Änderungskontrollprozess — Der Zweck dieses Prozesses besteht darin, die bevorstehende Änderung zu planen und sich darauf vorzubereiten. Wenn Sie Ihre Verschlüsselungsstandards oder -richtlinien ändern müssen, ist dieser wiederholbare und skalierbare Prozess darauf ausgelegt, Folgendes zu definieren:
  - Wie Ihr Unternehmen die Auswirkungen des Wandels bewertet
  - Wer kann Änderungen einleiten
  - Wer ist für die Umsetzung der Änderung verantwortlich
  - Wer ist für die Genehmigung der Änderung verantwortlich
  - Wie Ihre Organisation die Änderung gegebenenfalls rückgängig machen würde

- Überprüfbarkeit und Rückverfolgbarkeit von Änderungen — Dieser Prozess definiert, wie Ihr Unternehmen Änderungen prüft und nachverfolgt, sowohl auf Metadatenebene als auch auf Datenebene. Es sollte definieren, wie Sie Aufzeichnungen führen und auf diese zugreifen über:
  - Was hat sich geändert
  - Als es geändert wurde
  - Wer hat die Änderung initiiert, genehmigt und umgesetzt

  Wenn Ihr Unternehmen beispielsweise die Mindeststärke des Verschlüsselungsschlüssels ändert, sollten Sie in der Lage sein, die ursprünglichen und die neuen Anforderungen zu ermitteln, wann die Änderung wirksam war und wer am Änderungsprozess beteiligt war.
- Rollout-Prozess für Änderungen — Der Zweck dieses Prozesses besteht darin, zu definieren, wie Ihre Organisation die Änderung umsetzt, nachdem Sie sich dafür entschieden haben. Dieser Prozess definiert:
  - Wer sind die Stakeholder
  - Ob Sie ein Pilotprojekt oder einen Machbarkeitsnachweis absolvieren sollten
  - Wie und wann sollten Sie den Status der Änderung mitteilen
  - So machen Sie die Änderung rückgängig, falls erforderlich.
  - Wie lang sollte der Beobachtungszeitraum nach der Umsetzung der Änderung sein.
  - Wie wird der Beobachtungsprozess aussehen, um die Auswirkungen der Änderung zu beobachten, einschließlich der Art und Weise, wie Feedback zu der Änderung gesammelt und die Wirksamkeit bewertet werden kann
- Stilllegungsprozess — Mit diesem Prozess soll festgelegt werden, wie Ihr Unternehmen mit der Außerbetriebnahme verschlüsselungsbezogener Ressourcen und Informationen umgeht. Es enthält Anweisungen für den tatsächlichen Ruhestand sowie den Kommunikationsprozess für den Ruhestand.

Implementierung

In dieser Strategie bezieht sich Architektur auf die technische Umsetzung Ihrer Verschlüsselungsstandards. Dieser Abschnitt enthält Informationen darüberAWS-Services, wie AWS Key Management Service(AWS KMS) und AWS CloudHSMSie bei der Implementierung Ihrer data-at-rest Verschlüsselungsstrategie gemäß Ihren Richtlinien und Standards unterstützen können.

AWS KMSist ein verwalteter Dienst, mit dem Sie die kryptografischen Schlüssel erstellen und kontrollieren können, die zum Schutz Ihrer Daten verwendet werden. KMS-Schlüssel verlassen den Dienst niemals unverschlüsselt. Um Ihre KMS-Schlüssel zu verwenden oder zu verwalten, interagieren Sie mit ihnenAWS KMS, und viele davonAWS-Services sind integriertAWS KMS.

AWS CloudHSMist ein kryptografischer Dienst zur Erstellung und Wartung von Hardware-Sicherheitsmodulen (HSMs) in IhrerAWS Umgebung. HSMs sind Computergeräte, die kryptografische Operationen verarbeiten und einen sicheren Speicher für kryptografische Schlüssel bereitstellen. Wenn Ihre Standards vorschreiben, dass Sie FIPS 140-2 Level 3-validierte Hardware verwenden müssen oder wenn Ihre Standards die Verwendung von branchenüblichen APIs wie PKCS #11, Java Cryptography Extensions (JCE) und Microsoft CryptoNG (CNG) vorschreiben, sollten Sie erwägen, dies zu verwendenAWS CloudHSM.

Sie könnenAWS CloudHSM es als benutzerdefinierten Schlüsselspeicher für konfigurierenAWS KMS. Diese Lösung kombiniert den Komfort und die Serviceintegration vonAWS KMS mit den zusätzlichen Kontroll- und Compliance-Vorteilen der Verwendung einesAWS CloudHSM Clusters in IhremAWS-Konto. Weitere Informationen finden Sie unter Benutzerdefinierte Schlüsselspeicher (AWS KMSDokumentation).

In diesem Dokument werdenAWS KMS Funktionen auf hoher Ebene erörtert und erläutert, wie Sie Ihre Richtlinien und Standards berücksichtigenAWS KMS können.

Kosten, Komfort und Kontrolle

AWS KMSbietet verschiedene Arten von Schlüsseln. Einige gehören oder werden von Kunden verwaltetAWS, und andere werden von Kunden erstellt und verwaltet. Sie können je nach dem Grad der Kontrolle, den Sie über die Schlüssel- und Kostenüberlegungen haben möchten, zwischen diesen Optionen wählen:

- AWSeigene Schlüssel —AWS besitzt und verwaltet diese Schlüssel, und sie werden mehrfach verwendetAWS-Konten. EinigeAWS-Services unterstützenAWS eigene Schlüssel. Sie können diese Schlüssel kostenlos verwenden. Dieser Schlüsseltyp entlastet Sie von den Kosten und dem Verwaltungsaufwand für die Verwaltung des Schlüssellebenszyklus und des Zugriffs darauf. Weitere Informationen zu diesem Schlüsseltyp finden Sie unter AWSEigene Schlüssel (AWS KMSDokumentation).
- AWSverwaltete Schlüssel — Wenn ein in integriertAWS-Service istAWS KMS, kann er diese Art von Schlüsseln in Ihrem Namen erstellen, verwalten und verwenden, um Ihre Ressourcen in diesem Dienst zu schützen. Diese Schlüssel werden in IhremAWS-Konto erstellt undAWS-Services

können nur verwendet werden. Für einenAWS verwalteten Schlüssel fällt keine monatliche Gebühr an. Für die Nutzung, die über den kostenlosen Bereich hinausgeht, können Gebühren anfallen, aber einigeAWS-Services übernehmen diese Kosten für Sie. Sie können Identitätsrichtlinien verwenden, um den Zugriff auf diese Schlüssel zu kontrollieren und zu überprüfen, aber SieAWS verwalten den Schlüssellebenszyklus. Weitere Informationen zu diesem Schlüsseltyp finden Sie unter AWSVerwaltete Schlüssel (AWS KMSDokumentation). Eine umfassende Liste derAWS-Services Integrationsmöglichkeiten finden Sie unter AWS-ServiceIntegration (AWSMarketing).AWS KMS

- Vom Kunden verwaltete Schlüssel — Sie erstellen, besitzen und verwalten diesen Schlüsseltyp, und Sie haben die volle Kontrolle über den Schlüssellebenszyklus. Zur Aufgabentrennung können Sie identitäts- und ressourcenbasierte Richtlinien verwenden, um den Zugriff auf den Schlüssel zu steuern. Sie können auch eine automatische Schlüsselrotation einrichten. Für kundenverwaltete Schlüssel fällt eine monatliche Gebühr an, und wenn Sie das kostenlose Kontingent überschreiten, fällt auch eine Nutzungsgebühr für die Nutzung an. Weitere Informationen zu diesem Schlüsseltyp finden Sie unter Kundenverwaltete Schlüssel (AWS KMSDokumentation).

Weitere Informationen zur Speicherung und Verwendung von Schlüsseln finden Sie unter AWS Key Management ServicePreise (AWSMarketing).

Leistungs- und Verschlüsselungsarten

Basierend auf dem in den Standards ausgewählten Verschlüsselungstyp können Sie zwei Arten von KMS-Schlüsseln verwenden.

- Symmetrisch — AlleAWS KMS key Typen unterstützen symmetrische Verschlüsselung. Bei der Verschlüsselung von kundenverwalteten Schlüsseln können Sie einen Schlüssel mit einer einzigen Stärke für die Ver- und Entschlüsselung mit AES-256-GCM verwenden.
- Asymmetrisch — Kundenverwaltete Schlüssel unterstützen asymmetrische Verschlüsselung. Sie können je nach Verwendungszweck zwischen verschiedenen Schlüsselstärken und Algorithmen wählen. Asymmetrische Schlüssel können mit RSA ver- und entschlüsselt werden und Vorgänge mit RSA oder ECC signieren und verifizieren. Asymmetrische Schlüsselalgorithmen sorgen von Natur aus für eine Rollentrennung und vereinfachen die Schlüsselverwaltung. Wenn Sie asymmetrische Verschlüsselung mit verwendenAWS KMS, werden einige Operationen nicht unterstützt, z. B. das Rotieren von Schlüsseln und das Importieren von externem Schlüsselmaterial.

Weitere Informationen zu denAWS KMS Operationen, die symmetrische und asymmetrische Schlüssel unterstützen, finden Sie in der Schlüsseltypenreferenz (AWS KMSDokumentation).

Envelope-Verschlüsselung

Die Briefumschlagverschlüsselung ist integriertAWS KMS. InAWS KMS generieren Sie Datenschlüssel entweder im Klartext- oder im verschlüsselten Format. Verschlüsselte Datenschlüssel werden mit einem KMS-Schlüssel verschlüsselt. Sie können den KMS-Schlüssel in einem benutzerdefinierten Schlüsselspeicher in einemAWS CloudHSM Cluster speichern. Weitere Informationen zu den Vorteilen der Umschlagverschlüsselung finden Sie unterÜber Envelope-Verschlüsselung.

Wichtiger Lagerort

Sie verwenden Richtlinien, um den Zugriff aufAWS KMS Ressourcen zu verwalten. Richtlinien beschreiben, wer auf welche Ressourcen zugreifen kann. Richtlinien, die einemAWS Identity and Access Management (IAM-) Principal zugeordnet sind, werden als identitätsbasierte Richtlinien oder IAM-Richtlinien bezeichnet. Richtlinien, die anderen Arten von Ressourcen zugeordnet sind, werden als Ressourcenrichtlinien bezeichnet. AWS KMSRessourcenrichtlinien fürAWS KMS keys werden als Schlüsselrichtlinien bezeichnet. Jeder KMS-Schlüssel besitzt eine Schlüsselrichtlinie.

Wichtige Richtlinien bieten die Flexibilität, den Verschlüsselungsschlüssel an einem zentralen Ort zu speichern oder ihn näher an den Daten auf verteilte Weise zu speichern. Berücksichtigen Sie die folgendenAWS KMS Funktionen, wenn Sie entscheiden, wo KMS-Schlüssel in Ihrem gespeichert werden sollenAWS-Konto:

- Infrastrukturunterstützung für eine einzelne Region — Standardmäßig sind KMS-Schlüssel regionsspezifisch und werden niemalsAWS KMS unverschlüsselt gespeichert. Wenn Ihre Standards strenge Anforderungen für die Steuerung von Schlüsseln an einem bestimmten geografischen Standort enthalten, sollten Sie die Verwendung von Einzelregionsschlüsseln ausprobieren.
- Infrastrukturunterstützung für mehrere Regionen — unterstütztAWS KMS auch spezielle Schlüsseltypen, sogenannte Mehrregionsschlüssel. Das Speichern von Daten in mehrerenAWS-Regionen Dateien ist eine gängige Konfiguration für die Notfallwiederherstellung. Durch die Verwendung von Schlüsseln für mehrere Regionen können Sie Daten zwischen Regionen übertragen, ohne sie erneut zu verschlüsseln, und Sie können die Daten so verwalten, als ob Sie in jeder Region denselben Schlüssel gehabt hätten. Diese Funktion ist sehr nützlich, wenn Ihre Standards erfordern, dass Ihre Verschlüsselungsinfrastruktur mehrere Regionen in einer aktiven

Konfiguration umfasst. Weitere Informationen finden Sie unter Multiregionale Schlüssel (AWS KMSDokumentation).

- Zentrales Management — Wenn Ihre Standards erfordern, dass Sie Schlüssel an einem zentralen Ort speichern, können SieAWS KMS damit alle Ihre Verschlüsselungsschlüssel an einem einzigen Ort speichernAWS-Konto. Sie verwenden wichtige Richtlinien, um Zugriff auf andere Anwendungen zu gewähren, die sich auf verschiedenen Konten in derselben Region befinden können. Durch eine zentrale Schlüsselverwaltung kann der Verwaltungsaufwand für die Verwaltung des Schlüssellebenszyklus und der Schlüsselzugriffskontrolle reduziert werden.
- Externes Schlüsselmaterial — Sie können extern generiertes Schlüsselmaterial importierenAWS KMS. Support für diese Funktionalität ist für symmetrische Schlüssel mit einem und mehreren Regionen verfügbar. Da das Material des symmetrischen Schlüssels extern generiert wird, sind Sie für den Schutz der generierten Schlüsselmaterialien verantwortlich. Weitere Informationen finden Sie unter Importiertes Schlüsselmaterial (AWS KMSDokumentation).

Zugriffskontrolle

InAWS KMS können Sie die Zugriffskontrolle auf granularer Ebene implementieren, indem Sie die folgenden Richtlinienmechanismen verwenden: Schlüsselrichtlinien, IAM-Richtlinien und Zuschüsse. Mithilfe dieser Steuerelemente können Sie Ihre Aufgabentrennung auf der Grundlage von Rollen einrichten, z. B. Administratoren, Schlüsselbenutzer, die die Daten verschlüsseln können, Schlüsselbenutzer, die die Daten entschlüsseln können, und Schlüsselbenutzern, die die Daten sowohl verschlüsseln als auch entschlüsseln können. Weitere Informationen finden Sie unter Authentifizierung und Zugriffskontrolle (AWS KMSDokumentation).

Prüfung und Protokollierung

AWS KMSlässt sich zuAWS CloudTrail Protokollierungs- und Überwachungszwecken in Amazon EventBridge integrieren. AlleAWS KMS API-Operationen werden aufgezeichnet und können in CloudTrail Protokollen überprüft werden. Sie können Amazon verwenden CloudWatch EventBridge,AWS Lambda um benutzerdefinierte Überwachungslösungen einzurichten, um Benachrichtigungen und automatische Problembehebungen zu konfigurieren. Weitere Informationen finden Sie unter Protokollierung und Überwachung (AWS KMSDokumentation).

Häufig gestellte Fragen

In diesem Abschnitt finden Sie Antworten auf häufig gestellte Fragen bei der Definition Ihrer Verschlüsselungsstandards oder beim Aufbau Ihrer Verschlüsselungsinfrastruktur in der Implementierungsphase.

Wann benötige ich symmetrische Verschlüsselung?

Sie können symmetrische Verschlüsselung verwenden, wenn:

- Geschwindigkeit, Kosten und geringerer Rechenaufwand haben Priorität.
- Sie müssen eine große Datenmenge verschlüsseln.
- Die verschlüsselten Daten verlassen nicht die Grenzen des Unternehmensnetzwerks.

Wann benötige ich eine asymmetrische Verschlüsselung?

Sie können asymmetrische Verschlüsselung verwenden, wenn:

- Sie müssen die Daten außerhalb der Organisation teilen.
- Vorschriften oder Richtlinien verbieten die gemeinsame Nutzung des Schlüssels.
- Nichtbereitstellung ist erforderlich. (Die Nichtabweisung verhindert, dass ein Benutzer frühere Verpflichtungen oder Handlungen ablehnt.)
- Sie müssen den Zugriff auf Verschlüsselungsschlüssel auf der Grundlage der Unternehmensrollen strikt trennen.

Wann benötige ich eine Briefumschlagverschlüsselung?

Sie müssen die Umschlagverschlüsselung unterstützen und implementieren, wenn Ihre Verschlüsselungsrichtlinie eine Schlüsselrotation erfordert. Bei einigen Governance- und Compliance-Regelungen ist eine Schlüsselrotation erforderlich, oder Ihre Richtlinie könnte es vorschreiben, dass dies zur Erfüllung geschäftlicher Anforderungen erforderlich ist.

Wann muss ich ein Hardwaresicherheitsmodul (HSM) verwenden?

Möglicherweise benötigen Sie ein HSM, wenn Ihre Richtlinie die Einhaltung folgender Bestimmungen vorsieht:

- Der Federal Information Processing Standards (FIPS) 140-2 Level 3-Verschlüsselungsstandard. Weitere Informationen finden Sie unter FIPS-Validierung (AWS CloudHSMDokumentation).
- Industriestandard-APIs wie PKCS #11, Java Cryptography Extension (JCE) oder Microsoft Cryptography API: Next Generation (CNG)

Warum sollte ich Verschlüsselungsschlüssel zentral verwalten?

Im Folgenden sind die allgemeinen Vorteile einer zentralen Schlüsselverwaltung aufgeführt:

- Da Schlüssel an verschiedenen Standorten verwendet und verwaltet werden, können Sie Schlüssel wiederverwenden, was die Kosten senken kann.
- Sie haben mehr Kontrolle über den Zugriff auf die Verschlüsselungsschlüssel.
- Das Speichern von Schlüsseln an einem einzigen Ort erleichtert das Anzeigen, Prüfen und Aktualisieren von Schlüsseln im Falle einer Standardänderung.

Muss ich eine speziell entwickelte Verschlüsselungsinfrastruktur für gespeicherte Daten verwenden?

Ihr Unternehmen benötigt eine Verschlüsselungsinfrastruktur, wenn eine der folgenden Bedingungen erfüllt ist:

- Ihr Unternehmen verarbeitet und speichert Daten aller Kategorien, die nicht öffentlich sind.
- Ihr Unternehmen erfasst und speichert Daten über Mitarbeiter oder Kunden.
- Ihr Unternehmen verarbeitet PII-Daten.
- Ihr Unternehmen muss regulatorische oder behördliche Vorschriften einhalten, die eine Verschlüsselung von Daten erfordern.
- Die Unternehmensleitung hat die Verschlüsselung aller gespeicherten Daten vorgeschrieben.

Wie kann ich meinem UnternehmenAWS KMS helfen, seine Verschlüsselungsziele für gespeicherte Daten zu erreichen?

Zusätzlich zu vielen anderen FunktionenAWS Key Management Service kann es Ihnen helfen:

- Verwenden Sie Umschlagverschlüsselung.
- Steuern Sie den Zugriff auf Verschlüsselungsschlüssel, z. B. die Trennung der Schlüsselverwaltung von der Schlüsselnutzung.
- Teilen Sie Schlüssel auf mehrereAWS-Regionen undAWS-Konten.
- Zentralisieren Sie die Schlüsselverwaltung.
- Automatisieren und ordnen Sie die Schlüsselrotation an.

Ressourcen

AWS-Service-Dokumentation

- AWS KMSKryptografische Details
- AWS KMS-Entwicklerhandbuch
  - AWS KMS-Konzepte
  - Schlüssel für spezielle Zwecke
  - Authentifizierung und Zugriffskontrolle fürAWS KMS
  - Sicherheit vonAWS KMS
  - WieAWS-Services benutztAWS KMS
- AWS CloudHSM-Benutzerhandbuch
- AWSLeitfaden für kryptografische Dienste und Tools
  - So wählen Sie ein Verschlüsselungstool oder einen Verschlüsselungsdienst aus
  - Konzepte der Kryptographie

AWSMarketing

- AWS KMS-Preise
- AWS KMSIntegration mit anderenAWS-Services

AWSWell-Architected Framework

- Schutz von Daten bei der Übertragung
- Schutz ruhender Daten

Hashing und Tokenisierung

- Wie man Tokenisierung nutzt, um die Datensicherheit zu verbessern und den Prüfungsumfang zu reduzieren (AWSBlogbeitrag)
- Empfehlung für Anwendungen, die zugelassene Hash-Algorithmen verwenden (NIST-Publikation)

Videos

- So funktioniert Verschlüsselung inAWS
- Sichern Sie Ihren Blockspeicher aufAWS
- Erreichen von Sicherheitszielen mitAWS CloudHSM
- Bewährte Methoden für die ImplementierungAWS Key Management Service
- Ein tiefer Einblick inAWS Verschlüsselungsdienste

Dokumentverlauf

In der folgenden Tabelle werden die wichtigsten Änderungen an diesem Handbuch beschrieben. Wenn Sie über future Updates informiert werden möchten, können Sie einen RSS-Feed abonnieren.

Änderung	Beschreibung	Datum
Erstveröffentlichung	—	15. September 2022

AWS Glossar zu präskriptiven Leitlinien

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

Zahlen

7 Rs

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

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

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

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

A

ABAC

Siehe attributbasierte Zugriffskontrolle.

abstrahierte Dienste

Weitere Informationen finden Sie unter Managed Services.

ACID

Siehe Atomarität, Konsistenz, Isolierung und Haltbarkeit.

Aktiv-Aktiv-Migration

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

Aktiv-Passiv-Migration

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

Aggregatfunktion

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

AI

Siehe künstliche Intelligenz.

AIOps

Siehe Operationen mit künstlicher Intelligenz.

Anonymisierung

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

Anti-Muster

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

Anwendungssteuerung

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

Anwendungsportfolio

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

künstliche Intelligenz (KI)

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

Operationen mit künstlicher Intelligenz (AIOps)

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

Asymmetrische Verschlüsselung

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

Atomizität, Konsistenz, Isolierung, Haltbarkeit (ACID)

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

Attributbasierte Zugriffskontrolle (ABAC)

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

autoritative Datenquelle

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

Availability Zone

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

AWS Framework für die Cloud-Einführung (AWS CAF)

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

Cloud-Einführung vorzubereiten. Weitere Informationen finden Sie auf der AWS -CAF-Webseite und dem AWS -CAF-Whitepaper.

AWS Workload-Qualifizierungsrahmen (AWS WQF)

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

B

schlechter Bot

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

BCP

Siehe Planung der Geschäftskontinuität.

Verhaltensdiagramm

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

Big-Endian-System

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

Binäre Klassifikation

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

Bloom-Filter

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

Blau/Grün-Bereitstellung

Eine Bereitstellungsstrategie, bei der Sie zwei separate, aber identische Umgebungen erstellen. Sie führen die aktuelle Anwendungsversion in einer Umgebung (blau) und die neue Anwendungsversion in der anderen Umgebung (grün) aus. Mit dieser Strategie können Sie schnell und mit minimalen Auswirkungen ein Rollback durchführen.

Bot

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

Botnetz

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

branch

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

Zugang durch Glasbruch

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

Brownfield-Strategie

Die bestehende Infrastruktur in Ihrer Umgebung. Wenn Sie eine Brownfield-Strategie für eine Systemarchitektur anwenden, richten Sie sich bei der Gestaltung der Architektur nach den

Einschränkungen der aktuellen Systeme und Infrastruktur. Wenn Sie die bestehende Infrastruktur erweitern, könnten Sie Brownfield- und Greenfield-Strategien mischen.

Puffer-Cache

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

Geschäftsfähigkeit

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

Planung der Geschäftskontinuität (BCP)

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

C

CAF

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

Bereitstellung auf Kanaren

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

CCoE

Weitere Informationen finden Sie im Cloud Center of Excellence.

CDC

Siehe Erfassung von Änderungsdaten.

Erfassung von Datenänderungen (CDC)

Der Prozess der Nachverfolgung von Änderungen an einer Datenquelle, z. B. einer Datenbanktabelle, und der Aufzeichnung von Metadaten zu der Änderung. Sie können CDC für

verschiedene Zwecke verwenden, z. B. für die Prüfung oder Replikation von Änderungen in einem Zielsystem, um die Synchronisation aufrechtzuerhalten.

Chaos-Technik

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

CI/CD

Siehe Continuous Integration und Continuous Delivery.

Klassifizierung

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

clientseitige Verschlüsselung

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

Cloud-Kompetenzzentrum (CCoE)

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

Cloud Computing

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

Cloud-Betriebsmodell

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

Phasen der Einführung der Cloud

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

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

Diese Phasen wurden von Stephen Orban im Blogbeitrag 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.

Verwaltung der Datenbankkonfiguration (CMDB)

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

Konformitätspaket

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

Kontinuierliche Bereitstellung und kontinuierliche Integration (CI/CD)

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

CV

Siehe Computer Vision.

D

Daten im Ruhezustand

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

Datenklassifizierung

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

Datendrift

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

Daten während der Übertragung

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

Datennetz

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

Datenminimierung

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

Datenperimeter

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

Vorverarbeitung der Daten

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

Herkunft der Daten

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

betroffene Person

Eine Person, deren Daten gesammelt und verarbeitet werden.

Data Warehouse

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

Datenbankdefinitionssprache (DDL)

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

Datenbankmanipulationssprache (DML)

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

DDL

Siehe Datenbankdefinitionssprache.

Deep-Ensemble

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

Deep Learning

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

defense-in-depth

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

delegierter Administrator

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

Bereitstellung

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

Entwicklungsumgebung

Siehe Umgebung.

Detektivische Kontrolle

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

Abbildung des Wertstroms in der Entwicklung (DVSM)

Ein Prozess zur Identifizierung und Priorisierung von Einschränkungen, die sich negativ auf Geschwindigkeit und Qualität im Lebenszyklus der Softwareentwicklung auswirken. DVSM erweitert den Prozess der Wertstromanalyse, der ursprünglich für Lean-Manufacturing-Praktiken

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

digitaler Zwilling

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

Maßtabelle

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

Katastrophe

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

Notfallwiederherstellung (DR)

Die Strategie und der Prozess, die Sie zur Minimierung von Ausfallzeiten und Datenverlusten aufgrund einer Katastrophe anwenden. Weitere Informationen finden Sie unter Disaster Recovery von Workloads unter AWS: Wiederherstellung in der Cloud im AWS Well-Architected Framework.

DML

Siehe Sprache zur Datenbankmanipulation.

Domainorientiertes Design

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

DR

Siehe Disaster Recovery.

Erkennung von Driften

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

DVSM

Siehe Abbildung des Wertstroms in der Entwicklung.

E

EDA

Siehe explorative Datenanalyse.

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 Service, den Sie in einer Virtual Private Cloud (VPC) hosten können, um ihn mit anderen Benutzern zu teilen. Sie können einen Endpunktdienst mit anderen AWS-Konten oder AWS Identity and Access Management (IAM AWS PrivateLink -) Prinzipalen erstellen und diesen Berechtigungen gewähren. Diese Konten oder Prinzipale können sich privat mit Ihrem Endpunktservice verbinden, indem sie Schnittstellen-VPC-Endpunkte erstellen. Weitere Informationen finden Sie unter Einen Endpunkt-Service erstellen in der Amazon Virtual Private Cloud (Amazon VPC)-Dokumentation.

Unternehmensressourcenplanung (ERP)

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

Envelope-Verschlüsselung

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

Umgebung

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

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

- Höhere Umgebungen – Alle Umgebungen, auf die auch andere Benutzer als das Kernentwicklungsteam zugreifen können. Dies kann eine Produktionsumgebung, Vorproduktionsumgebungen und Umgebungen für Benutzerakzeptanztests umfassen.

Epics

In der agilen Methodik sind dies funktionale Kategorien, die Ihnen helfen, Ihre Arbeit zu organisieren und zu priorisieren. Epics bieten eine allgemeine Beschreibung der Anforderungen und Implementierungsaufgaben. Zu den Sicherheitsthemen AWS von CAF gehören beispielsweise Identitäts- und Zugriffsmanagement, Detektivkontrollen, Infrastruktursicherheit, Datenschutz und Reaktion auf Vorfälle. Weitere Informationen zu Epics in der AWS -Migrationsstrategie finden Sie im Leitfaden zur Programm-Implementierung.

ERP

Siehe Enterprise Resource Planning.

Explorative Datenanalyse (EDA)

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

F

Faktentabelle

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

schnell scheitern

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

Grenze zur Fehlerisolierung

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

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

Feature-Zweig

Siehe Zweig.

Features

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

Bedeutung der Feature

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

Featuretransformation

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

FGAC

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

H

HEKTAR

Siehe Hochverfügbarkeit.

Heterogene Datenbankmigration

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

hohe Verfügbarkeit (HA)

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

historische Modernisierung

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

Homogene Datenbankmigration

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

heiße Daten

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

Hotfix

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

Hypercare-Phase

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

I

IaC

Sehen Sie sich Infrastruktur als Code an.

Identitätsbasierte Richtlinie

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

Leerlaufanwendung

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

IIoT

Siehe Industrielles Internet der Dinge.

unveränderliche Infrastruktur

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

Eingehende (ingress) VPC

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

Inkrementelle Migration

Eine Cutover-Strategie, bei der Sie Ihre Anwendung in kleinen Teilen migrieren, anstatt eine einziges vollständiges Cutover durchzuführen. Beispielsweise könnten Sie zunächst nur einige Microservices oder Benutzer auf das neue System umstellen. Nachdem Sie sich vergewissert haben, dass alles ordnungsgemäß funktioniert, können Sie weitere Microservices oder Benutzer schrittweise verschieben, bis Sie Ihr Legacy-System außer Betrieb nehmen können. Diese Strategie reduziert die mit großen Migrationen verbundenen Risiken.

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. Mehr Informationen finden Sie unter Aufbau einer digitalen Transformationsstrategie für das industrielle Internet der Dinge (IIoT).

Inspektions-VPC

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

Internet of Things (IoT)

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

Interpretierbarkeit

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

IoT

Siehe Internet der Dinge.

IT information library (ITIL, IT-Informationsbibliothek)

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

T service management (ITSM, IT-Servicemanagement)

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

BIS

Weitere Informationen finden Sie in der IT-Informationsbibliothek.

ITSM

Siehe IT-Servicemanagement.

L

Labelbasierte Zugangskontrolle (LBAC)

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

Landing Zone

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

Große Migration

Eine Migration von 300 oder mehr Servern.

SCHWARZ

Weitere Informationen finden Sie unter Label-basierte Zugriffskontrolle.

Geringste Berechtigung

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

Lift and Shift

Siehe 7 Rs.

Little-Endian-System

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

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.

Manufacturing Execution System (MES)

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

MAP

Siehe Migration Acceleration Program.

Mechanismus

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

Mitgliedskonto

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

DURCHEINANDER

Siehe Manufacturing Execution System.

Message Queuing-Telemetrietransport (MQTT)

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

Microservice

Ein kleiner, unabhängiger Service, der über klar definierte APIs kommuniziert und in der Regel kleinen, eigenständigen Teams gehört. Ein Versicherungssystem kann beispielsweise Microservices beinhalten, die Geschäftsfunktionen wie Vertrieb oder Marketing oder Subdomains wie Einkauf, Schadenersatz oder Analytik zugeordnet sind. Zu den Vorteilen von Microservices gehören Agilität, flexible Skalierung, einfache Bereitstellung, wiederverwendbarer Code und Ausfallsicherheit. Weitere Informationen finden Sie unter 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 über eine klar definierte Schnittstelle mithilfe einfacher APIs. Jeder Microservice in dieser Architektur kann aktualisiert, bereitgestellt und skaliert werden, um den Bedarf an bestimmten Funktionen einer Anwendung zu decken. Weitere Informationen finden Sie unter Implementierung von Microservices auf. AWS

Migration Acceleration Program (MAP)

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

Migration in großem Maßstab

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

Migrationsfabrik

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

Migrationsmetadaten

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

Migrationsmuster

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

Migration Portfolio Assessment (MPA)

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

Migration Readiness Assessment (MRA)

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

Migrationsstrategie

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

ML

Siehe maschinelles Lernen.

Modernisierung

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

Bewertung der Modernisierungsfähigkeit

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

Monolithische Anwendungen (Monolithen)

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

MPA

Siehe Bewertung des Migrationsportfolios.

MQTT

Siehe Message Queuing-Telemetrietransport.

Mehrklassen-Klassifizierung

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

veränderbare Infrastruktur

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

O

OAC

Weitere Informationen finden Sie unter Origin Access Control.

OAI

Siehe Zugriffsidentität von Origin.

COM

Siehe organisatorisches Change-Management.

Offline-Migration

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

OI

Siehe Betriebsintegration.

OLA

Siehe Vereinbarung auf operativer Ebene.

Online-Migration

Eine Migrationsmethode, bei der der Quell-Workload auf das Zielsystem kopiert wird, ohne offline genommen zu werden. Anwendungen, die mit dem Workload verbunden sind, können während der Migration weiterhin funktionieren. Diese Methode beinhaltet keine bis minimale Ausfallzeit und wird in der Regel für kritische Produktionsworkloads verwendet.

OPC-UA

Siehe Open Process Communications — Unified Architecture.

Offene Prozesskommunikation — Einheitliche Architektur (OPC-UA)

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

Vereinbarung auf Betriebsebene (OLA)

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

Überprüfung der Betriebsbereitschaft (ORR)

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

Betriebstechnologie (OT)

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

Betriebsintegration (OI)

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

Organisationspfad

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

Organisatorisches Veränderungsmanagement (OCM)

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

Ursprungszugriffskontrolle (OAC)

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

Ursprungszugriffsidentität (OAI)

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

ODER

Siehe Überprüfung der Betriebsbereitschaft.

NICHT

Siehe Betriebstechnologie.

Ausgehende (egress) VPC

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

P

Berechtigungsgrenze

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

persönlich identifizierbare Informationen (PII)

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

Personenbezogene Daten

Siehe persönlich identifizierbare Informationen.

Playbook

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

PLC

Siehe programmierbare Logiksteuerung.

PLM

Siehe Produktlebenszyklusmanagement.

policy

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

Polyglotte Beharrlichkeit

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

Portfoliobewertung

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

predicate

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

Prädikat Pushdown

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

Präventive Kontrolle

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

Prinzipal

Eine Entität AWS , die Aktionen ausführen und auf Ressourcen zugreifen kann. Bei dieser Entität handelt es sich in der Regel um einen Root-Benutzer für eine AWS-Konto, eine IAM-Rolle oder

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

Datenschutz 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-Abfragen für eine Domain und ihre Subdomains innerhalb einer oder mehrerer VPCs reagieren soll. Weitere Informationen finden Sie unter Arbeiten mit privat gehosteten Zonen in der Route-53-Dokumentation.

proaktive 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, vom Design, der Entwicklung und Markteinführung über Wachstum und Reife bis hin zur Markteinführung und Markteinführung.

Produktionsumgebung

Siehe Umgebung.

Speicherprogrammierbare Steuerung (SPS)

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

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 auf Microservices basierenden MES kann ein Microservice beispielsweise Ereignismeldungen in einem Kanal veröffentlichen, den andere Microservices abonnieren können. Das System kann neue Microservices hinzufügen, ohne den Veröffentlichungsservice zu ändern.

Q

Abfrageplan

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

Abfrageplanregression

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

R

RACI-Matrix

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

Ransomware

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

RASCI-Matrix

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

RCAC

Siehe Zugriffskontrolle für Zeilen und Spalten.

Read Replica

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

neu strukturieren

Siehe 7 Rs.

Recovery Point Objective (RPO)

Die maximal zulässige Zeitspanne seit dem letzten Datenwiederherstellungspunkt. Dies bestimmt, was als akzeptabler Datenverlust zwischen dem letzten Wiederherstellungspunkt und der Betriebsunterbrechung angesehen wird.

Wiederherstellungszeitziel (RTO)

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

Refaktorierung

Siehe 7 Rs.

Region

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

Regression

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

rehosten

Siehe 7 Rs.

Veröffentlichung

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

umziehen

Siehe 7 Rs.

neue Plattform

Siehe 7 Rs.

Rückkauf

Siehe 7 Rs.

Ausfallsicherheit

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

Ressourcenbasierte Richtlinie

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

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

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

Reaktive Kontrolle

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

Beibehaltung

Siehe 7 Rs.

zurückziehen

Siehe 7 Rs.

Drehung

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

Zugriffskontrolle für Zeilen und Spalten (RCAC)

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

RPO

Siehe Recovery Point Objective.

RTO

Siehe Ziel der Wiederherstellungszeit.

Runbook

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

S

SAML 2.0

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

SCADA

Siehe Aufsichtskontrolle und Datenerfassung.

SCP

Siehe Richtlinie zur Dienstkontrolle.

Secret

Interne AWS Secrets Manager, vertrauliche oder eingeschränkte Informationen, wie z. B. ein Passwort oder Benutzeranmeldeinformationen, 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 (security information and event management – SIEM)

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

Automatisierung von Sicherheitsreaktionen

Eine vordefinierte und programmierte Aktion, die darauf ausgelegt ist, automatisch auf ein Sicherheitsereignis zu reagieren oder es zu beheben. Diese Automatisierungen dienen als detektive oder reaktionsschnelle Sicherheitskontrollen, die Sie bei der Implementierung bewährter AWS Sicherheitsmethoden unterstützen. Beispiele für automatisierte Antwortaktionen sind das Ändern einer VPC-Sicherheitsgruppe, das Patchen einer Amazon EC2 EC2-Instance oder das Rotieren von Anmeldeinformationen.

Serverseitige Verschlüsselung

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

Service-Kontrollrichtlinie (SCP)

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

Service-Endpunkt

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

Service Level Agreement (SLA)

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

Service-Level-Indikator (SLI)

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

Service-Level-Ziel (SLO)

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

Modell der geteilten Verantwortung

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

SIEM

Siehe Sicherheitsinformations- und Event-Management-System.

Single Point of Failure (SPOF)

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

SLA

Siehe Service Level Agreement.

SLI

Siehe Service-Level-Indikator.

ALSO

Siehe Service-Level-Ziel.

split-and-seed Modell

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

SPOTTEN

Siehe Single Point of Failure.

Sternschema

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

Strangler-Fig-Muster

Ein Ansatz zur Modernisierung monolithischer Systeme, bei dem die Systemfunktionen schrittweise umgeschrieben und ersetzt werden, bis das Legacy-System außer Betrieb genommen werden kann. Dieses Muster verwendet die Analogie einer Feigenrebe, die zu einem etablierten Baum heranwächst und schließlich ihren Wirt überwindet und ersetzt. Das Muster wurde eingeführt von Martin Fowler als Möglichkeit, Risiken beim Umschreiben

monolithischer Systeme zu managen. Ein Beispiel für die Anwendung dieses Musters finden Sie unter Schrittweises Modernisieren älterer Microsoft ASP.NET (ASMX)-Webservices mithilfe von Containern und Amazon API Gateway.

Subnetz

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

Aufsichtskontrolle und Datenerfassung (SCADA)

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

Symmetrische Verschlüsselung

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

synthetisches Testen

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

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

Stammbasierter Workflow

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

Vertrauenswürdiger Zugriff

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

Optimieren

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

Zwei-Pizzen-Team

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

U

Unsicherheit

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

undifferenzierte Aufgaben

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

höhere Umgebungen

Siehe Umgebung.

V

Vacuuming

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

Versionskontrolle

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

VPC-Peering

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

Schwachstelle

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

WURM

Sehen Sie einmal schreiben, viele lesen.

WQF

Weitere Informationen finden Sie unter AWS Workload Qualification Framework.

einmal schreiben, viele lesen (WORM)

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

Z

Zero-Day-Exploit

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

Zero-Day-Sicherheitslücke

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

Zombie-Anwendung

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

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