Bewährte Verfahren für die Entwicklung einer Multi-Cloud-Strategie

AWS Präskriptive Leitlinien

AWS Präskriptive Leitlinien: Bewährte Verfahren für die Entwicklung einer Multi-Cloud-Strategie

Table of Contents

Bewährte Methoden für die Entwicklung einer Multi-Cloud-Strategie

Tom Godden und Ellie Tamari, Amazon Web Services

September 2025 (Geschichte der Dokumente)

Organizations sehen sich heute mit widersprüchlichen Botschaften in Bezug auf die Einführung von Multiclouds konfrontiert. Einige raten gänzlich davon ab, während andere behaupten, dass jeder auf eine Multi-Cloud-Umgebung umsteigt. Die Realität liegt zwischen diesen Extremen: Es gibt sowohl legitime Gründe für als auch gegen Multi-Cloud-Strategien, und der Erfolg hängt davon ab, ob der potenzielle Geschäftswert gegen die inhärente Komplexität und das Risiko abgewogen wird.

Unser Engagement für Interoperabilität ist ein Hauptgrund, warum sich viele Kunden für unsere Plattform entscheiden. AWS Wir glauben daran, Ihnen die Freiheit zu geben, unabhängig von Ihren Workloads innovativ zu sein, und Ihnen die Möglichkeit zu geben, die Technologie zu wählen, die Ihren Anforderungen am besten entspricht. Bei AWS waren wir führend bei der Entwicklung von Lösungen, mit denen Sie Anwendungen in jeder Umgebung erstellen und bereitstellen können. Dieser kundenorientierte Ansatz ist von grundlegender Bedeutung für das AWS Cloud, dem Millionen von Kunden weltweit vertrauen.

Wir wissen, dass Kunden Cloud-Plattformen benötigen, die sowohl mit bestehenden Tools als auch mit future Technologieoptionen nahtlos zusammenarbeiten. Sie sollten nicht alles neu aufbauen müssen, wenn Sie Funktionen von einem anderen Anbieter hinzufügen. Ihre Cloud sollte Ihnen helfen, Workloads umgebungsübergreifend zu verbinden, zu sichern und zu verwalten, ohne dass Sie gezwungen sind, Experte für jede Plattform zu werden. AWS baut Verbindungspunkte direkt in ihre Dienste ein, um Ihnen zu helfen, effektiv zu arbeiten, unabhängig davon, ob Ihre Strategie darin besteht, AWS ausschließlich zu nutzen oder einen selektiven Multi-Cloud-Ansatz zu verfolgen.

Wir sind uns bewusst, dass jedes Unternehmen einzigartige Geschäftsanforderungen hat, die seine Cloud-Strategieentscheidungen beeinflussen. Ganz gleich, ob Sie Workloads hauptsächlich auf AWS, in mehreren Clouds ausführen oder sie AWS als Teil einer umfassenderen Multi-Cloud-Architektur verwenden, wir setzen uns dafür ein, Ihnen zum Erfolg zu verhelfen. AWS bietet die Tiefe und Breite an Tools und Funktionen, mit denen Sie einfacher und schneller erstellen, migrieren und betreiben können, unabhängig davon, wo sich Ihre Workloads befinden. AWS Tools vereinfachen die Verwaltung anbieterübergreifend und maximieren gleichzeitig die Leistung und den Wert Ihrer Cloud-Investitionen.

Dieses paper konzentriert sich auf bewährte Grundsätze für den Erfolg einer Multicloud-Strategie, einschließlich der Frage, wann und wo ein Multicloud-Ansatz sinnvoll ist und wie Unternehmen AWS dabei unterstützt werden, mit ihren Multi-Cloud-Strategien erfolgreich zu sein. Es enthält präskriptive Leitlinien, die Führungskräften helfen sollen, fundierte Strategie- und Entscheidungsentscheidungen im Zusammenhang mit der Einführung von Multi-Cloud-Systemen zu treffen. Dieses paper bietet keine technische, eingehende Erörterung von Multicloud-Implementierungen. Wenn Sie technische Unterstützung bei der Implementierung und Unterstützung bei Ihren spezifischen Herausforderungen benötigen, empfehlen wir Ihnen, mit Ihrem AWS Lösungsarchitekten zusammenzuarbeiten.

In diesem paper werden neun bewährte Grundsätze für den Erfolg von Multiclouds vorgestellt, die auf unseren Erfahrungen mit AWS Unternehmenskunden basieren. Jeder Grundsatz befasst sich mit einem wichtigen Aspekt der Multi-Cloud-Strategie, von der Ausrichtung der Geschäftsziele bis hin zur Sicherheitsimplementierung. Durch die Anwendung dieser Prinzipien können Unternehmen die Komplexität mehrerer Clouds souverän bewältigen.

- Grundsatz 1. Stimmen Sie Ihre Multi-Cloud-Ziele mit Ihrer Strategie ab
- Grundsatz 2. Seien Sie sich der Missverständnisse im Zusammenhang mit Multiclouds bewusst
- Grundsatz 3. Verfügen Sie über eine klare Strategie und Unternehmensführung, um dies zu unterstützen
- Grundsatz 4. Verteilen Sie zusammenhängende Workloads nicht auf mehrere Clouds
- Grundsatz 5. Haben Sie eine längerfristige Integrationsstrategie
- Grundsatz 6. Setzen Sie Container strategisch ein
- Grundsatz 7. Habe ein einziges CCo E, aber spezialisiere dich darauf
- Grundsatz 8. Stellen Sie sicher, dass Sicherheit immer oberste Priorität hat
- Grundsatz 9. Entscheiden Sie sich für einen 80/20-Ansatz und nicht für eine gleichmäßige Verteilung

Grundsatz 1. Stimmen Sie Ihre Multi-Cloud-Ziele mit Ihrer Strategie ab

Untersuchungen von Gartner und Branchentrends zeigen, dass Unternehmen zunehmend Multi-Cloud-Ansätze einsetzen, um spezifischen Geschäftsanforderungen gerecht zu werden. Die folgenden Szenarien zeigen, wann eine Multicloud-Infrastruktur strategisch vorteilhaft sein kann.

Fusionen und Übernahmen

Fusionen und Übernahmen (M&A) führen zu sofortigen Entscheidungen über die Cloud-Strategie. Der Betrieb mehrerer Clouds kann zwar die Kosten und die Komplexität erhöhen, eine schnelle Konsolidierung kann jedoch den Integrationswert verzögern und den Geschäftsbetrieb stören. Ihre Cloud-Entscheidungen werden für die Realisierung der Vorteile von Fusionen und Übernahmen von zentraler Bedeutung.

Die Integrationsplanung sollte die gesamte Technologielandschaft berücksichtigen. Jeder Workload muss im Kontext Ihres Integrationszeitplans und Ihrer Geschäftsprioritäten bewertet werden.

Unsere Beratung:

- Entwickeln Sie eine geschäftsorientierte Konsolidierungsstrategie, die unmittelbare Integrationsanforderungen mit langfristiger betrieblicher Effizienz in Einklang bringt. Halten Sie zunächst mehrere Clouds bereit, wenn eine übereilte Konsolidierung wichtige Geschäftsabläufe stören oder die Wertschöpfung durch Fusionen und Übernahmen verzögern könnte.
- Erstellen Sie klare Kriterien für die Verteilung der Workloads, die auf Ihren Integrationszeitplan abgestimmt sind. Priorisieren Sie umsatzgenerierende Anwendungen und Kerngeschäftsprozesse und berücksichtigen Sie dabei technische Abhängigkeiten und betriebliche Anforderungen.

Wunsch, die differenzierten Fähigkeiten eines anderen CSP langfristig zu nutzen

Die Angst, etwas zu verpassen, treibt einige Unternehmen dazu, von jeder Cloud ein bisschen zu wollen. Entscheidungen über die Verteilung von Workloads wirken sich auf das gesamte Unternehmen aus — von den Entwicklungsteams über die Finanzen bis hin zu den Sicherheitsabläufen.

Organizations müssen daher ihre Gründe für den Einsatz mehrerer Clouds überprüfen. Manche argumentieren, dass jeder Workload von dem Cloud-Dienstanbieter (CSP) verwaltet werden sollte, der seine Anforderungen am besten erfüllt. Die individuelle Workload-Optimierung muss jedoch gegen die umfassenderen organisatorischen Auswirkungen abgewogen werden. Jeder weitere Cloud-Anbieter riskiert, die betriebliche Komplexität zu erhöhen, neue Talentanforderungen zu schaffen und Sicherheitsaspekte einzuführen, die sich auf die gesamte Technologieorganisation auswirken.

Unsere Leitlinien:

- Folgen Sie einem 80/20-Ansatz: Wählen Sie für die meisten Workloads einen primären Anbieter aus und ziehen Sie zusätzliche Anbieter nur für spezifische, hochwertige Anwendungsfälle in Betracht. Diese Strategie maximiert die Effizienz und die Bindung von Talenten und reduziert gleichzeitig die Komplexität.
- Denken Sie an die Gesamtkosten für den Betrieb mehrerer Clouds. Beziehen Sie Sicherheitstools, Governance-Produkte, Finanzmanagementsysteme und betriebliche Gemeinkosten in Ihre Analyse mit ein.
- Bewerten Sie die Abhängigkeiten und Interaktionen der einzelnen Workloads. Workloads arbeiten selten isoliert; sie nutzen Daten, Sicherheitskontrollen und Betriebsprozesse gemeinsam.
- Führen Sie eine gründliche Analyse des Preis-Leistungs-Verhältnisses aller Anbieter durch. Vergleichen Sie nicht nur die direkten Kosten, sondern auch den Aufwand für die Verwaltung mehrerer Umgebungen.

Multicloud bei der Holdinggesellschaft und primäre Cloud bei der Betreibergesellschaft oder Branche

Private-Equity-Unternehmen und Holdinggesellschaften stehen vor einzigartigen Überlegungen zur Cloud-Strategie. Ihre Portfoliounternehmen verfolgen häufig unabhängige Cloud-Strategien, die häufig auf frühere M&A-Aktivitäten zurückzuführen sind. Diese Struktur reduziert die Komplexität, die typischerweise mit Multi-Cloud-Operationen verbunden ist, da jede Geschäftseinheit unabhängig arbeitet. Diese Unabhängigkeit kann jedoch die Möglichkeiten einschränken, unternehmensweite Mengenrabatte und Kaufanreize zu nutzen.

Die Wirksamkeit der Cloud-Strategie auf der Ebene der Holdinggesellschaft hängt von der Autonomie der Portfoliounternehmen und ihren individuellen Technologieanforderungen ab. Eine Konsolidierung

könnte zwar zu einer Hebelwirkung beim Kauf führen, sie könnte jedoch mit dem unabhängigen Geschäftsmodell kollidieren, das für Holdinggesellschaften und Private-Equity-Portfolios typisch ist.

Unsere Leitlinien:

- Machen Sie sich mit den CSP-Mengenrabattstrukturen vertraut. Jeder Anbieter bietet Mechanismen zum Hinzufügen oder Entfernen von Tochterunternehmen zu Unternehmensverträgen und zur Ausgliederung von Geschäftsbereichen in separate Einheiten. Dabei handelt es sich um wechselseitige Entscheidungen.
- Planen Sie Ihre Cloud-Einkaufsverpflichtungen sorgfältig. Wenden Sie sich frühzeitig an das Account-Team Ihres CSP oder wenden Sie sich an einen Experten AWS Partner mit der AWS Cloud-Operations-Kompetenz, um Unterstützung zu erhalten.
- Bringen Sie Unabhängigkeit und Effizienz in Einklang. Denken Sie an gemeinsame Dienste oder Einkaufsverträge, von denen Portfoliounternehmen profitieren, ohne ihre Geschäftstätigkeit einzuschränken.
- Konzentrieren Sie sich zunächst auf die Geschäftsziele. Entwickeln Sie Technologiestrategien, die Ihr Betriebsmodell unterstützen, anstatt eine Multi-Cloud-Strategie um ihrer selbst willen zu verfolgen.
- Evaluieren Sie Cloud-Strategien aus der Perspektive des Portfoliomanagements. Überlegen Sie, wie sich Cloud-Entscheidungen auf mögliche Veräußerungen oder future Akquisitionen auswirken.

Grundsatz 2. Seien Sie sich der Missverständnisse im Zusammenhang mit Multiclouds bewusst

Vermeiden Sie bei der Entwicklung Ihrer Multicloud-Strategie die häufigsten Missverständnisse, die in den folgenden Abschnitten behandelt werden.

Jeder setzt Multi-Cloud-Strategien ein

Beratungsunternehmen und Medienunternehmen zeichnen ein komplexes Bild der Multi-Cloud-Einführung. Untersuchungen zeigen ein breites Interesse an Multi-Cloud-Ansätzen, aber die Ausgabenmuster erzählen oft eine andere Geschichte. In der Praxis unterhalten viele Unternehmen entweder einzelne Cloud-Umgebungen oder klare primary/secondary CSP-Beziehungen. Diese Diskrepanz unterstreicht, wie wichtig es ist, über die Schlagzeilen hinauszuschauen und sich stattdessen auf die spezifischen Bedürfnisse Ihres Unternehmens zu konzentrieren.

Unsere Leitlinien:

- Treffen Sie Cloud-Entscheidungen auf der Grundlage Ihrer spezifischen Geschäftsanforderungen, anstatt Branchentrends zu folgen. Konzentrieren Sie sich auf messbare Kosten und Risiken für Ihr Unternehmen.
- Untersuchen Sie Multi-Cloud-Anwendungsfälle in Ihrem Branchenkontext. Cloud-Strategien, die für Unternehmen im Bereich Verbrauchertechnologie funktionieren, lassen sich möglicherweise nicht auf Finanzdienstleistungs-, Fertigungs- oder Spieleumgebungen übertragen.
- Betrachten Sie die Datengravitation als Hauptfaktor bei Entscheidungen über die Verteilung von Workloads. Der Standort und die Bewegung von Daten bestimmen häufig die effektivste Cloud-Architektur.
- Schauen Sie sich nicht nur die Statistiken zur Akzeptanz an, um die Ausgabenmuster zu verstehen. Hohe gemeldete Multi-Cloud-Nutzungsraten verbergen häufig die tatsächlichen Ausgabenmuster.
- Prüfen Sie die technischen Einschränkungen, bevor Sie sich für eine Multi-Cloud-Umgebung entscheiden. Einige Workloads funktionieren am besten, wenn ihre Komponenten in einer einzigen Cloud-Umgebung verbleiben.

Multicloud reduziert das Risiko einer Anbieterbindung

Die Flexibilität eines Anbieters ist ein legitimer Aspekt bei der Entwicklung einer Cloud-Strategie. Organizations schätzen die Fähigkeit, ihre Technologieauswahl an die sich ändernden Geschäftsanforderungen anzupassen. Dieses Problem spiegelt frühere Erfahrungen mit herkömmlichen IT-Investitionen wider, die zu verbindlichen, langfristigen Verpflichtungen führten. Cloud-Dienste bieten unterschiedliche Dynamiken in Bezug auf die Flexibilität der Anbieter. AWS bietet Open-Source-kompatible Dienste und Datenportabilitätsoptionen, die technische Migrationshürden verringern. Der Kompromiss zwischen Flexibilität und betrieblicher Effizienz bleibt jedoch wichtig. Organizations müssen den geschäftlichen Nutzen der Beibehaltung von Anbieteroptionen gegen die technischen Vorteile einer umfassenden Integration mit spezialisierten Diensten eines primären Anbieters abwägen.

Einige Kunden versuchen, eine Abhängigkeit zu vermeiden, indem sie Cloud-unabhängige Lösungen entwickeln, die Container verwenden. Dieser Ansatz beschränkt sie häufig auf grundlegende Rechen- und Speicherdienste und umgeht die Vorteile erweiterter Cloud-Funktionen. Unsere Erfahrung zeigt, dass diese Strategie aufgrund der erhöhten Entwicklungszeit und des höheren Ressourcenbedarfs im Vergleich zur Verwendung nativer Dienste zu einer erheblichen Komplexität führt.

Unsere Leitlinien:

- Berücksichtigen Sie die vollen Kosten Cloud-agnostischer Architekturen. Der zusätzliche technische Aufwand rechtfertigt möglicherweise keine Vorteile der Portabilität.
- Nutzen Sie Cloud-native Funktionen, um den größtmöglichen Nutzen zu erzielen. Alleine bei grundlegenden Rechen- und Speicherdiensten gehen oft erhebliche Vorteile in Bezug auf Sicherheit, Skalierbarkeit und Innovation verloren.
- Planen Sie Cloud-Strategien auf der Grundlage der Geschäftsanforderungen. Wenn eine Multi-Cloud-Implementierung einen klaren Mehrwert bietet, z. B. die Möglichkeit, Benutzer auf mehreren Plattformen zu bedienen, lohnt sich die zusätzliche technische Investition.
- Evaluieren Sie realistische Ausstiegsszenarien und Kosten. Vergleichen Sie die Wahrscheinlichkeit und die Kosten eines Anbieterwechsels mit den Vorteilen, die sich aus der Nutzung des gesamten Angebots von ergeben AWS-Services.
- Bauen Sie auf den Open-Source-Grundlagen von auf AWS. AWS Managed Services wie Amazon Relational Database Service (Amazon RDS) bieten Ihnen sowohl Flexibilität als auch operative Exzellenz und unterstützen die Datenbank-Engines, die Sie heute verwenden.

- Nutzen Sie die umfassenden Migrationstools von AWS. Wir helfen Ihnen dabei, Workloads in jede Richtung zu verschieben, und bieten kostenlosen Datenaustausch, falls AWS Sie andere Anbieter nutzen. Weitere Informationen finden Sie im AWS Blogbeitrag Kostenlose Datenübertragung ins Internet, wenn Sie das Internet verlassen. AWS

Multicloud verbessert die Verfügbarkeit und Belastbarkeit

Der Glaube an einen reibungslosen Workloadwechsel zwischen Cloud-Anbietern bei Ausfällen veranlasst einige Unternehmen zu Multi-Cloud-Strategien. Diese Denkweise führt zu einer stark vereinfachten Sicht auf die Widerstandsfähigkeit der Cloud-Infrastruktur, die grundlegende technische Realität ignoriert.

Basierend auf jahrelanger Erfahrung in der Zusammenarbeit mit Multicloud-Kunden haben wir festgestellt AWS, dass die Aufrechterhaltung einer vollständigen Workload-Portabilität zwischen Anbietern oft zu erheblicher Komplexität führt, ohne dass alle erwarteten Vorteile erzielt werden. Datenintensive Anwendungen stehen aufgrund der eingeschränkten Datendichte vor unüberwindbaren Herausforderungen. Unserer Ansicht nach ist es für Unternehmen sogar fast unmöglich, ein wirklich nahtloses Multi-Cloud-Failover für datenintensive Workloads erfolgreich zu implementieren.

Lydia Leong, angesehene VP Analyst bei Gartner, bekräftigt diese Sichtweise in einem Beitrag in den sozialen Medien: „Multicloud-Failover ist komplex und kostspielig, sodass es fast immer unpraktisch ist, und es ist kein besonders wirksames Mittel, um Risiken der Cloud-Resilienz zu begegnen.“ Die inhärente Differenzierung zwischen Anbietern in den Bereichen Netzwerk, Speicher, Datenbanken, maschinelles Lernen und Sicherheit macht eine echte Portabilität nahezu unmöglich. Die Verteilung der Workloads auf mehrere Anbieter kann das Risiko erhöhen, da ein Ausfall in einer der Umgebungen zu einem Ausfall in allen Umgebungen führen kann.

Unsere Leitlinien:

- Konzentrieren Sie sich darauf, die AWS Fähigkeiten für einzelne Workloads zu beherrschen, anstatt komplexe Multi-Cloud-Architekturen zu verfolgen.
- Bauen Sie Ausfallsicherheit durch AWS-Regionen Availability Zones auf, anstatt ein anbieterübergreifendes Failover zu versuchen. Ausführliche technische Informationen dazu, wie Workloads zwischen physischen Rechenzentren automatisch ausgefallen werden AWS können, finden Sie im AWS Blogbeitrag Zonal Autoshift — Automatisches Verschieben Ihres Datenverkehrs von Availability Zones weg, wenn wir potenzielle Probleme erkennen.

- Migrieren Sie Workloads strategisch zu einer Anwendung und konzentrieren Sie sich auf jeweils eine Anwendung AWS, um den Erfolg zu maximieren.

Multicloud bietet bessere Preise

Preisliche Wettbewerbsfähigkeit könnte das schwächste Argument für Multi-Cloud-Umgebungen sein. Organizations von Unternehmen mit komplizierten, teuren Software- oder Rechenzentrumsverträgen, die sie an mehrjährige Verträge binden, haben sie bei der Beschaffung von IT-Services vorsichtig gemacht. Herkömmliche Beschaffungsansätze haben sich nicht an pay-as-you-go Einkäufe, Mengenrabatte oder die Realität des Preiswettbewerbs in der Cloud angepasst. (Stand Januar 2025, AWS hat die Preise seit seiner Einführung 151 Mal gesenkt.)

Der größte Einzelfaktor zur Kostensenkung ist eine gut verwaltete und optimierte Cloud-Umgebung. Ein Unternehmen erzielt eine bessere Kostenoptimierung, wenn es in erster Linie mit einem Anbieter zusammenarbeitet, dessen Dienste Preis-/Leistungsvorteile bieten (z. B. Recheninstanzen, die auf maßgeschneiderten Chips wie AWS Graviton basieren) und der über erstklassige Cloud-Finanzmanagementlösungen verfügt. Laut einer Studie der Hackett Group aus dem Jahr 2022, an der mehr als 1.000 Unternehmen teilnahmen, waren die Infrastrukturausgaben als Prozentsatz der gesamten IT-Ausgaben bei AWS Kunden um 20% niedriger als bei Multi-Cloud-Organisationen.

Unserer Erfahrung nach rechnen Unternehmen nicht mit den zusätzlichen Kosten und der Komplexität, die der Betrieb in mehreren Clouds mit sich bringt, und sie wägen diese Kosten auch nicht angemessen gegen den wahrgenommenen Gewinn eines head-to-head Beschaffungsengagements ab.

Unsere Leitlinien:

- Bauen Sie Ihre Strategie zur Kostenoptimierung auf der Säule AWS Well-Architected Framework Cost Optimization auf. Es gibt fünf Gestaltungsprinzipien:
  - Implementieren Sie Cloud-Finanzmanagement: Um finanziellen Erfolg zu erzielen und die Realisierung von Geschäftswerten in der Cloud zu beschleunigen, müssen Sie in Cloud-Finanzmanagement investieren. Ihre Organisation muss die erforderliche Zeit und Ressourcen für die Entwicklung von Fähigkeiten in diesem neuen Bereich des Technologie- und Nutzungsmanagements aufwenden. Wie bei Ihren Sicherheits- oder Betriebsfähigkeiten müssen Sie Ihre Kapazitäten durch Wissensaufbau, Programme, Ressourcen und Prozesse ausbauen, um zu einem kosteneffizienten Unternehmen zu werden.

  - Verbrauchsmodell einführen: Zahlen Sie nur für die verbrauchten Computing-Ressourcen, und erhöhen oder verringern Sie die Nutzung auf Basis Ihrer Geschäftsanforderungen und nicht durch aufwändige Prognosen. Beispielsweise werden Entwicklungs- und Testumgebungen während der Arbeitswoche in der Regel nur acht Stunden am Tag genutzt. Sie können diese Ressourcen einstellen, wenn sie nicht genutzt werden, was zu potenziellen Kosteneinsparungen von 75% (40 Stunden gegenüber 168 Stunden) führt.
  - Messen Sie die Gesamteffizienz: Messen Sie die Geschäftsleistung Ihrer Arbeitslast und die mit der Bereitstellung verbundenen Kosten. Nutzen Sie diese Daten, um die Vorteile zu verstehen, die Sie durch die Erhöhung der Ausgabe, die Erweiterung der Funktionalität und die Reduzierung der Kosten erzielen.
  - Hören Sie auf, Geld für undifferenzierte Schwerarbeit auszugeben: CSPs Erledigen Sie die Schwerstarbeit der Rechenzentrumsabläufe wie Rackierung, Stapelung und Stromversorgung von Servern. Durch den Einsatz von Managed Services entfällt auch der betriebliche Aufwand, der mit der Verwaltung von Betriebssystemen und Anwendungen einhergeht. Auf diese Weise können Sie sich auf Ihre Kunden und Geschäftsprojekte konzentrieren, anstatt sich auf die IT-Infrastruktur zu konzentrieren.
  - Ausgaben analysieren und zuordnen: Mit der Cloud ist es einfacher, die Nutzung und die Kosten von Workloads genau zu ermitteln und auf Basis dieser Daten eine transparente Zuordnung der IT-Kosten auf Umsatzströme und einzelne Workload-Besitzer durchzuführen. Das hilft Ihnen bei der Ermittlung der Umsatzrendite (ROI) und Workload-Besitzer haben die Möglichkeit, ihre Ressourcen zu optimieren und die Kosten zu reduzieren.
- Angesichts des finanziellen Aufwands, der mit dem Betrieb über verschiedene Anbieter verbunden ist, empfehlen wir unseren Kunden, stark in Tools für Automatisierung und Kostenoptimierung zu investieren. Jeder CSP bietet umfangreiche native Tools in diesem Bereich, wie z. B. die. AWS Cost Optimization Hub Die meisten nativen Tools bieten Kunden in ihrer Cloud-Umgebung hervorragende Funktionen. Um jedoch die Ausgaben für mehrere zu verstehen CSPs, können Sie aus einer Vielzahl von ISV- und Software-as-a-Service (SaaS) -Produkten wählen, die diese Funktionen erweitern und ein einheitliches Erlebnis zur Kostenoptimierung bieten.
- Eine Verwässerung der Kaufkraft durch eine Spend-Equity-Strategie generiert keinen Geschäftswert. Dies kann potenzielle Mengenrabatte untergraben und möglicherweise das technische Design untergraben. Die effizienteste Art, Cloud-Dienste zu nutzen, besteht darin, einen primären Anbieter für den Großteil Ihrer Abläufe zu verwenden und andere Anbieter CSPs nur dann zu nutzen, wenn sie einen geschäftlichen Mehrwert bieten.

Grundsatz 3. Verfügen Sie über eine klare Strategie und Unternehmensführung, um dies zu unterstützen

Die Entscheidung, eine Multi-Cloud-Strategie zu verfolgen, reicht nicht aus. Sie müssen eine Strategie zur Erreichung Ihrer Ziele festlegen, einschließlich einer klaren Steuerung, für welche Workloads wo und warum verwendet werden. Bewertungskriterien sollten verwendet werden, um Workloads und ihre Abhängigkeiten zu optimieren. Wenn die Bewertung den einzelnen Personen überlassen wird, CSPs wird eine unkoordinierte Ausbreitung der Multi-Cloud-Strategie wahrscheinlich den Wert der Multi-Cloud-Strategie untergraben. Wir empfehlen Ihnen, die Leistung der CSP-Workloads regelmäßig zu bewerten und Ihre Bewertung als wichtigen Input für die Auswahl, die Kriterien und die future Nutzung des CSP zu verwenden.

Eine effektive Governance-Strategie erfordert einen Überblick über die Gesamtzahl der Dienste, Anwendungen und Komponenten, die im gesamten Unternehmen genutzt werden. Ein wesentlicher Bestandteil dieser Strategie ist eine robuste Tagging-Strategie, die klare Eigentumsverhältnisse, Nutzung und Umgebung (wie Entwicklung, Qualitätssicherung, Staging und Produktion) für alle eingesetzten Ressourcen umfasst CSPs und festlegt. Alles sollte einem Besitzer zugeordnet sein. Wenn es nicht markiert ist oder ein Besitzer nicht identifiziert werden kann, sollte es entfernt werden. Wir arbeiten eng mit einem großen Finanzdienstleistungsunternehmen zusammen, das automatisch alle Ressourcen ohne Tags findet und entfernt, und betrachten dies als bewährte Methode, unabhängig von den Unannehmlichkeiten, die es für Entwicklungsteams mit sich bringt. Dieser Tagging-Ansatz kodifiziert die Regeln der Unternehmensführung und automatisiert deren Durchsetzung, anstatt den Fortschritt zu blockieren (d. h. es werden Leitplanken und keine Tore eingeführt). Kosten, Betriebsabläufe und Sicherheit müssen auf die gleiche Weise verfolgt, überwacht und entsprechende Maßnahmen ergriffen werden, und zwar mit der gleichen Datentiefe und Transparenz. CSPs

Wenn Sie eine Multi-Cloud-Strategie implementieren, ist die Einrichtung einer klaren und konsistenten Kontostruktur für alle Cloud-Anbieter von entscheidender Bedeutung, um die betriebliche Kontrolle und Sicherheit aufrechtzuerhalten. Wir empfehlen die Einführung eines hub-and-spoke Modells, bei dem Sie separate Modelle AWS-Konten für verschiedene Geschäftsbereiche erstellen. Diese basieren auf zwei wichtigen zentralen Konten: einem security/audit Konto für die konsolidierte Compliance- und Sicherheitsüberwachung und einem zentralen Netzwerkkonto für die Verwaltung der Interkonnektivität. (Dieser Ansatz ist im Entwurf von kodifiziert. AWS Control Tower Die Prinzipien der geringsten Privilegien und der Aufgabentrennung gelten jedoch auch für andere Clouds. Das AWS Well-Architected Framework behandelt diese Konzepte ausführlich und ist für

technische Zielgruppen sehr zu empfehlen.) Dieser grundlegende Ansatz sollte sich bei allen Cloud-Anbietern widerspiegeln, um eine einheitliche Verwaltung und Betriebsabläufe zu gewährleisten. Workload-Konten sollten nach Umgebung (Entwicklung, Bereitstellung, Produktion) oder Funktion organisiert werden, wobei klare Prozesse für die Erstellung und Löschung von Konten festgelegt werden sollten.

Unsere Leitlinien:

- Implementieren Sie eine umfassende Tagging-Strategie, um klare Eigentums- und Nutzungsmuster für alle Cloud-Ressourcen aufrechtzuerhalten. Verfolgen Sie Umgebungen, Kostenstellen, Anwendungen und Geschäftsbereiche mithilfe einheitlicher Tagging-Richtlinien. Entfernen Sie Ressourcen, denen die richtigen Tags fehlen, um Governance-Standards durchzusetzen und die Transparenz der Umgebung zu wahren.
- Richten Sie ein einheitliches Compliance-Framework ein, das die regulatorischen Anforderungen in Ihrer Multi-Cloud-Umgebung abbildet. Sorgen Sie für eine klare Dokumentation darüber, wie die Kontrollen und Zertifizierungen der einzelnen Cloud-Anbieter Ihre Compliance-Verpflichtungen unterstützen.
- Automatisieren Sie die Durchsetzung der Unternehmensführung durch Automatisierung, anstatt manuelle Genehmigungsprozesse zu verwenden. Kodieren Sie Ihre Governance-Regeln in automatisierten Systemen, die Richtlinienverstöße verhindern, bevor sie auftreten. Dadurch werden menschliche Fehler vermieden und gleichzeitig die Entwicklungsgeschwindigkeit beibehalten.
- Strukturieren Sie Konten in einem hub-and-spoke Modell mit zentraler Sicherheits- und Netzwerksteuerung. Erstellen Sie spezielle Konten für Sicherheitsüberprüfungen und Netzwerkmanagement, um wichtige Funktionen zu zentralisieren. Diese Grundlage ermöglicht einheitliche Sicherheitsrichtlinien und Netzwerkkonnektivität im gesamten Unternehmen.
- Um betriebliche Grenzen zu wahren, sollten Sie separate Konten, Abonnements oder Projekte (abhängig von der Nomenklatur Ihres CSP) für verschiedene Umgebungen und Funktionen erstellen. Teilen Sie die Workloads nach Entwicklungs-, Staging- und Produktionsumgebungen auf. Diese Trennung verhindert, dass sich Sicherheitsvorfälle ausbreiten, und sorgt für klare Betriebsbereiche.
- Überwachen Sie Kosten, Abläufe und Sicherheit mithilfe einheitlicher Kennzahlen in der gesamten Umgebung. Implementieren Sie eine einheitliche Überwachung der Ressourcennutzung, Sicherheitsereignisse und Ausgabenmuster. Verwenden Sie diese Daten, um Entscheidungen zur Verteilung der Arbeitslast und zur Ressourcenzuweisung zu optimieren.
- Verhindern Sie unbefugte Cloud-Nutzung durch Unternehmensrichtlinien und automatisierte Kontrollen. Definieren Sie klare Prozesse für die Kontoerstellung und die Bereitstellung von

Ressourcen. Implementieren Sie Richtlinien zur Servicekontrolle (SCPs), um die Einhaltung der Unternehmensstandards für alle Konten durchzusetzen.

- Richten Sie detektive und präventive Kontrollen ein, um zu verhindern, dass Schatten-IT über nicht autorisierte Anbieterkonten nach außen gelangt. Halten Sie mithilfe von Spesenabrechnungen und Netzwerkverkehr Ausschau nach unbefugter Cloud-Nutzung. Blockieren Sie den Zugriff unberechtigter Anbieter und behalten Sie gleichzeitig bewährte Innovationspfade bei.

Grundsatz 4. Verteilen Sie zusammenhängende Workloads nicht auf mehrere Clouds

Die Verteilung zusammenhängender Workloads auf mehrere Cloud-Anbieter führt zu unnötiger Komplexität, Risiken und Kosten. Wenn Workloads, die Daten gemeinsam verarbeiten und analysieren, mehrere Anbieter umfassen, stehen Unternehmen vor Herausforderungen bei der Übertragung, Synchronisation und Konsistenz von Daten. Teams müssen sich für jeden Anbieter mit unterschiedlichen APIs Managementschnittstellen, Sicherheitsmodellen und Betriebsprozessen auseinandersetzen, was die Wahrscheinlichkeit von Fehlern erhöht und den betrieblichen Aufwand erhöht. Diese Komplexität erhöht die Wahrscheinlichkeit von Fehlern und den betrieblichen Aufwand und kann Agilität und Skalierbarkeit beeinträchtigen.

In einigen praktischen Szenarien müssen Unternehmen jedoch aufgrund spezifischer geschäftlicher oder technischer Anforderungen möglicherweise zusammenhängende Workloads auf mehrere Clouds verteilen. In diesen Fällen empfehlen wir Ihnen, klare Kriterien und Leitprinzipien festzulegen, um die Kompromisse zu bewerten und sicherzustellen, dass der Ansatz mit der allgemeinen Multi-Cloud-Strategie Ihres Unternehmens übereinstimmt.

Wenn Unternehmen sich dafür entscheiden, Workloads auf mehrere Clouds zu verteilen, kann die Einführung einer Architektur, die sich auf Messaging und lose Kopplung konzentriert, viele der damit verbundenen Herausforderungen verringern. Dies ist der beste Weg, um Bedenken zwischen Clouds zu trennen und das Ausmaß der Auswirkungen zu verringern, wenn ein Anbieter beeinträchtigt wird. Vorgänge, die am zeitaufwändigsten sind, wie z. B. Finanztransaktionen, sollten idealerweise in einer einzigen Umgebung abgewickelt werden. Ein Ausfall in einer Umgebung sollte niemals dazu führen, dass Workloads in einer anderen Umgebung gefährdet werden.

Unser Leitfaden:

- Entwerfen Sie Cloud-Workloads für betriebliche Unabhängigkeit, um Abhängigkeiten zwischen Anbietern in Echtzeit zu minimieren. Wenn eine Verteilung der Arbeitslast erforderlich ist, implementieren Sie effiziente Mechanismen für die Übertragung von Massendaten, anstatt konstante Cloud-übergreifende Verbindungen aufrechtzuerhalten.
- Bewerten Sie jeden vorgeschlagenen verteilten Workload anhand klarer Geschäftskriterien. Berücksichtigen Sie sowohl die strategischen Vorteile als auch die betriebliche Komplexität, die sich aus der Verteilung ergibt.

Grundsatz 5. Haben Sie eine längerfristige Integrationsstrategie

Seien Sie vorsichtig, wenn Sie große Datenmengen zwischen Anwendungen in verschiedenen Clouds verschieben, insbesondere wenn Ihre Rechenressourcen und Anwendungen in einem CSP und Ihre Datenspeicherressourcen in einem anderen bereitgestellt werden. Eine solche Situation kann zu mehr Komplexität und Latenz führen, was die vermeintlichen Vorteile zunichte machen könnte. Wir sprechen mit vielen Kunden, die über einen Data Lake in einer Cloud verfügen, aber maschinelles Lernen (ML) oder Analysen mit Tools eines anderen CSP durchführen möchten. Die Entscheidung, wo Workloads in einer Multi-Cloud-Umgebung platziert werden sollen, ist eine der wichtigsten — und oft schwierigsten — Entscheidungen, mit denen Unternehmen konfrontiert sind. Wir empfehlen, dass Sie jede Entscheidung zur Workload-Platzierung anhand von drei kritischen Aspekten bewerten: technische Anforderungen, Geschäftsanforderungen und Stärken des Anbieters.

Beginnen Sie mit der technischen Bewertung, indem Sie die wesentlichen Merkmale der einzelnen Workloads abbilden: Rechenleistung, Datenoperationen, Anforderungen an Reaktionszeiten und Wachstumsanforderungen. Anwendungen funktionieren naturgemäß am besten, wenn sie sich in der Nähe ihrer Daten befinden. Wenn Anwendungen von ihren Datenquellen wegbewegt werden, entstehen unnötige technische Hürden und die Leistung wird beeinträchtigt.

Bei Geschäftsentscheidungen müssen die Preise der Anbieter, die Anforderungen an den Datenstandort und die Lieferantenverträge berücksichtigt werden. Jede Workload-Platzierung wirkt sich auf den Betrieb, die Sicherheit und die Produktivität des gesamten Unternehmens aus. Eine isolierte Betrachtung von Workloads führt zu suboptimalen Entscheidungen.

Unsere Leitlinien:

- Implementieren Sie eine Massendatenübertragung zwischen Clouds anstelle von Echtzeitzugriff. Planen Sie regelmäßige Datenaktualisierungen, indem Sie effiziente Massenoperationen verwenden, anstatt ständige API-Aufrufe zwischen Clouds zu verwenden. Dieser Ansatz reduziert die Kosten, verbessert die Zuverlässigkeit und sorgt für eine gleichbleibende Leistung. Exportieren Sie beispielsweise zusammengefasste tägliche Verkaufsdaten, anstatt einzelne Transaktionen cloudübergreifend abzufragen.
- Berücksichtigen Sie bei der Gestaltung der Verteilung der Workloads die Schwerkraft der Daten. Halten Sie Anwendungen in der Nähe ihrer primären Datenquellen, um die Leistung aufrechtzuerhalten und die Kosten zu senken. ML-Modelle, Analyse-Engines und

Transaktionsverarbeitungssysteme profitieren alle vom direkten Zugriff auf ihre Daten. Die Verlagerung dieser Workloads von ihren Daten führt zu unnötiger Netzwerklatenz und Komplexität.

- Bewerten Sie Workload-Entscheidungen im Kontext Ihrer gesamten Cloud-Strategie, anstatt sie isoliert zu überprüfen. Überlegen Sie, wie sich die einzelnen Platzierungsentscheidungen auf betriebliche Prozesse, Sicherheitskontrollen und Teamkapazitäten in Ihrem Unternehmen auswirken. Eine Entscheidung, die für einen einzelnen Workload optimal erscheint, kann die Überwachung erschweren oder die Sicherheitsrisiken erhöhen, wenn sie ganzheitlich betrachtet wird.
- Definieren Sie klare Richtlinien für Dateneigentum und Datenverwaltung, die festlegen, wo sich verschiedene Datentypen befinden können. Erstellen Sie ein Framework zur Datenklassifizierung, das konsistente Entscheidungen über die Datenplatzierung bei allen Cloud-Anbietern ermöglicht.

Grundsatz 6. Setzen Sie Container strategisch ein

Container können eine wertvolle Rolle bei der Unterstützung einer Multi-Cloud-Strategie spielen, aber es ist wichtig, auch ihre Grenzen zu erkennen. Die Verwendung von Containern ist generell eine gute Idee für jede moderne, cloudnative Anwendung, da sie Vorteile in Bezug auf Portabilität und Konsistenz in verschiedenen Umgebungen bieten. Container sind plattformunabhängig, was bedeutet, dass sie auf jeder Cloud-Plattform oder Infrastruktur ausgeführt werden können, die Containerisierungstechnologie unterstützt, wie z. B. Kubernetes. Organizations, die Container verwenden, können ihre Anwendungen einmal entwickeln und verpacken und sie dann konsistent für mehrere Cloud-Anbieter oder lokale Umgebungen bereitstellen, ohne dass wesentliche Änderungen erforderlich sind. Durch die Kapselung von Anwendungscode, Abhängigkeiten und Laufzeitumgebung in einem Container können Sie ein hohes Maß an Portabilität erreichen, sodass Sie Workloads nahtlos zwischen Cloud-Anbietern oder zwischen der Cloud und lokalen Rechenzentren verschieben können.

Container lösen jedoch möglicherweise nicht jeden Anwendungsfall oder beseitigen nicht alle Herausforderungen, denen sich ein Unternehmen bei der Einführung einer Multi-Cloud-Strategie stellen könnte. Container funktionieren am besten mit modernen, auf Microservices basierenden Architekturen, eignen sich aber möglicherweise nicht so gut für große, monolithische Anwendungen. Darüber hinaus können Container zwar bestimmte Aspekte der Portabilität berücksichtigen, wie z. B. die Laufzeit von Anwendungen, aber sie lösen Probleme im Zusammenhang mit Datenmanagement, Sicherheitsrichtlinien und anderen Cloud-übergreifenden Abhängigkeiten nicht automatisch. Organizations müssen ihre Multi-Cloud-Lösungen immer noch sorgfältig planen und konzipieren, um ein konsistentes Datenmanagement, einheitliche Sicherheitskontrollen und eine nahtlose Integration zwischen in der Cloud gehosteten und lokalen Komponenten zu gewährleisten.

Unsere Leitlinien:

- Nutzen Sie die systemeigenen Container-Management-Funktionen der einzelnen Cloud-Anbieter, um den Geschäftswert zu maximieren und die Bereitstellung zu beschleunigen. Dieser Ansatz gewährleistet eine optimale Leistung und vermeidet gleichzeitig die Komplexität der Entwicklung von Cloud-unabhängigen Lösungen, die selten nennenswerte Renditen erzielen.
- Entwickeln Sie Container-Strategien, die das gesamte Betriebsbild berücksichtigen, einschließlich Datenmanagement, Sicherheit und cloudübergreifender Abhängigkeiten. Konzentrieren Sie sich auf die Geschäftsergebnisse, wenn Sie Entscheidungen zur Container-Architektur treffen.

Grundsatz 7. Habe ein einziges CCo E, aber spezialisiere dich darauf

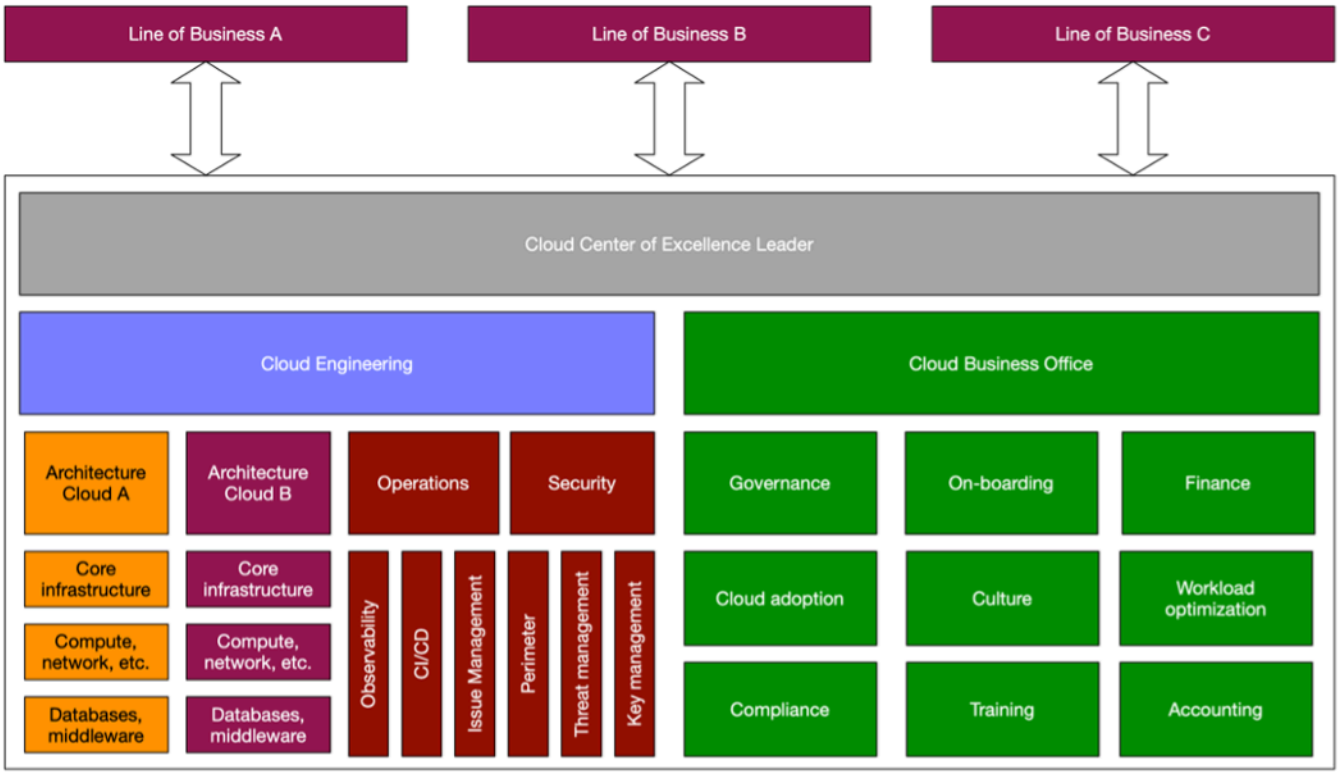
Wie wir vielen AWS Kunden empfehlen, sollten Sie in Ihrem Unternehmen ein Cloud Center of Excellence (CCoE) einrichten, das für eine führende Rolle, Standardisierung und Beschleunigung Ihrer Cloud-Reise sorgt. Wenn es um Multi-Cloud-Umgebungen geht, stellen wir fest, dass die erfolgreichsten Unternehmen einen ausgewogenen E-Ansatz verfolgen. CCo

Anstatt separate CCo Es für jeden CSP einzurichten, empfehlen wir, ein einziges, einheitliches CCo E einzurichten, das die Multi-Cloud-Strategie des Unternehmens überwacht. Dies trägt dazu bei, einen koordinierten, konsistenten Ansatz zu gewährleisten, anstatt isolierte Maßnahmen zu ergreifen, die zu Divergenzen, Neustrukturierungen und Verschwendung führen können. Stellen Sie sicher, dass die Teams in Ihrem Single CCo E über die erforderlichen Fachkenntnisse, Tools und Mechanismen für jeden CSP verfügen, den Ihr Unternehmen einsetzt. Dieses Fachwissen ermöglicht es dem CCo E, die Nutzung der verschiedenen Cloud-Plattformen effektiv zu steuern, zu unterstützen und zu beschleunigen.

Zum Beispiel sollte das CCo E über AWS spezifische Experten verfügen AWS Cloud, die sich mit den Services und bewährten Verfahren eingehend auskennen, sowie über Experten für andere, CSPs die das Unternehmen bei der Nutzung dieser Cloud-Technologien unterstützen können. Dieses spezialisierte Fachwissen innerhalb eines einzigen CCo E-Teams kann Ihrem Unternehmen helfen, von der Koordination und Standardisierung eines zentralisierten Ansatzes zu profitieren und gleichzeitig sicherzustellen, dass jede Cloud-Plattform optimal genutzt wird.

Das Single CCo E sollte als zentrales Leitungsgremium dienen, das Standards, Richtlinien und bewährte Verfahren für die Multi-Cloud-Strategie des Unternehmens festlegt. Die eigentliche Implementierung von Cloud-Workloads und -Projekten kann an spezialisierte Teams oder Geschäftsbereiche verteilt werden, während das CCOE die Aufsicht, Unterstützung und Koordination übernimmt. Dieser ausgewogene Ansatz trägt dazu bei, eine kohärente Multi-Cloud-Strategie sicherzustellen und gleichzeitig das erforderliche Maß an Flexibilität und Autonomie innerhalb der Organisation zu gewährleisten.

Das folgende Diagramm zeigt, wie ein CCo E einen zentralisierten Ansatz und eine zentrale Steuerung für mehrere Geschäftsbereiche (LOBs), Cloud-Engineering-Teams und Cloud Business Office (CBO) -Teams ermöglichen kann.



Unsere Beratung:

- Strukturieren Sie Ihr CCo E so, dass Sie den strategischen Überblick behalten und gleichzeitig spezialisiertes Fachwissen für jeden Cloud-Anbieter integrieren. Konzentrieren Sie sich darauf, fundiertes Fachwissen für einzelne Cloud-Plattformen zu rekrutieren, anstatt seltene Multi-Cloud-Spezialisten zu suchen, und fördern Sie den internen Wissensaustausch, um organisatorische Fähigkeiten aufzubauen.
- Geben Sie Ihrem CCo IT-Team die Möglichkeit, unternehmensweite Standards für bereichsübergreifende Themen wie Sicherheit und Beobachtbarkeit festzulegen, und geben Sie den einzelnen Teams gleichzeitig die Freiheit, diese Richtlinien mithilfe von Cloud-nativen Tools und Diensten umzusetzen.
- Entwickeln Sie eine umfassende Talentstrategie, die fundiertes Fachwissen über primäre Cloud-Plattformen mit umfassenderen Architekturkenntnissen in Einklang bringt. Konzentrieren Sie sich auf den Aufbau von Teams, die starke, Cloud-spezifische Fähigkeiten mit Erfahrung in der Unternehmensarchitektur kombinieren.

Grundsatz 8. Stellen Sie sicher, dass Sicherheit immer oberste Priorität hat

Ein Multicloud-Ansatz erschwert die Gewährleistung der Sicherheit, da er das Risiko eines unbefugten Zugriffs erhöht, da Ihr Sicherheitsstatus mehr Angriffsflächen berücksichtigen muss. Eine Multi-Cloud-Strategie zwingt Unternehmen häufig dazu, sich mit mehreren Sicherheitsmodellen CSPs in Bereichen wie Identitätsmanagement, Netzwerksicherheit, Asset Management und Auditprotokollierung auseinanderzusetzen. Diese Komplexität kann die Transparenz erschweren, die Belastung der Sicherheitsteams erhöhen und das Risiko erhöhen.

Die Automatisierung der Sicherheit ist in Multi-Cloud-Umgebungen unerlässlich. Das Identitätsmanagement muss in allen Umgebungen reibungslos funktionieren. Es muss bestehende Identitätsanbieter miteinander verbinden und gleichzeitig konsistente Zugriffsrichtlinien einhalten. Sicherheit erfordert integrierten Schutz auf Daten-, Netzwerk- und Endpunktebene. Datenklassifizierung, Verschlüsselung und Lebenszyklusmanagement bilden die Grundlage. Netzwerksicherheit basiert auf standardisierten Designs und Verbindungsmustern. Endpoint Protection vervollständigt das Framework durch konsistentes Patch-Management und hostbasierte Kontrollen.

Diese grundlegenden Elemente sind entscheidend für eine erfolgreiche und sichere Einführung mehrerer Cloud-Anbieter und müssen bei jeder Multi-Cloud-Strategieplanung frühzeitig berücksichtigt werden.

Unsere Leitlinien:

- Implementieren Sie in Ihrer Multi-Cloud-Umgebung ein integriertes Sicherheitsframework, das sich auf drei Kernelemente konzentriert: Datenschutz durch standardisierte Klassifizierung und Verschlüsselung, Netzwerksicherheit durch konsistente Entwurfsmuster und Endpunktschutz durch systematische Kontrollen und Patch-Management.
- Richten Sie ein einheitliches Sicherheitsmodell ein, das die systemeigenen Sicherheitsfunktionen der einzelnen Cloud-Anbieter nutzt und gleichzeitig die zentrale Transparenz und Kontrolle durch standardisierte Tools und Prozesse gewährleistet.
- Zentralisieren Sie die Erfassung und Analyse von Sicherheitsdaten mithilfe von Amazon Security Lake. Diese Plattform fasst Sicherheitsinformationen von anderen Cloud-Anbietern AWS, SaaS-Anwendungen und lokalen Systemen in einer einzigen Ansicht zusammen. Sie unterstützt das Open Cybersecurity Schema Framework (OCSF) und ermöglicht standardisierte Analysen in Ihrer

Hybrid- und Multi-Cloud-Umgebung. Dieser zentralisierte Ansatz verbessert die Erkennung und Reaktion auf Bedrohungen und vereinfacht gleichzeitig die Sicherheitsabläufe.

- Setzen Sie die systemeigenen Sicherheitstools jedes Anbieters ein, um Ihre Schutzfunktionen zu verbessern. Diese speziell entwickelten Dienste befassen sich mit anbieterspezifischen Funktionen und speisen gleichzeitig Daten an Ihre zentrale Sicherheitsplattform zurück. Eine Kombination aus systemeigenen Tools und zentraler Transparenz sorgt für einen umfassenden Sicherheitsschutz in Ihrer gesamten Infrastruktur.
- Implementieren Sie eine einheitliche Observability-Strategie, die von Grund auf umfassende Transparenz über Ihre gesamte Cloud-Landschaft, einschließlich Betriebs- und Sicherheitsdaten, sorgt. Standardisieren Sie sich auf branchenführende Überwachungsansätze, die eine konsistente Nachverfolgung von Unternehmensdiensten ermöglichen, unabhängig davon, wo sie betrieben werden.
- Etablieren Sie unternehmensweite Standards für die Erfassung und Visualisierung von Betriebsdaten, die eine schnelle Identifizierung und Lösung von Problemen in Ihrer Multi-Cloud-Umgebung ermöglichen. Konzentrieren Sie sich darauf, eine zentrale Informationsquelle für betriebliche Erkenntnisse zu schaffen, die sowohl technischen als auch geschäftlichen Stakeholdern dient.

Grundsatz 9. Entscheiden Sie sich für einen 80/20-Ansatz und nicht für eine gleichmäßige Verteilung

Die Art und Weise, wie Sie Workloads auf die Anbieter verteilen, ist entscheidend für Ihren Multi-Cloud-Erfolg. Viele Unternehmen streben fälschlicherweise nach Gleichheit bei ihrer Cloud-Verteilung und versuchen, die Workloads gleichmäßig auf die Anbieter zu verteilen. Dieser Ansatz erhöht die Komplexität, ohne proportionale Vorteile zu bieten. Eine gleichmäßige Verteilung fragmentiert Ihre technischen Fähigkeiten, verwässert Ihre Kaufkraft und verursacht unnötige betriebliche Gemeinkosten. Teams haben Schwierigkeiten, fundiertes Fachwissen zu entwickeln, wenn sie gezwungen sind, Kompetenzen auf mehreren Plattformen gleichzeitig aufrechtzuerhalten.

Der 80/20-Ansatz liefert nachweislich bessere Ergebnisse als eine gleichmäßige Verteilung über die Clouds. Wenn Sie 80% Ihrer Investitionen auf einen primären Anbieter konzentrieren und gleichzeitig gezielt andere Anbieter für bestimmte Funktionen einsetzen, entsteht eine ausgewogene Strategie, die sowohl Kosten als auch Komplexität reduziert. Dieser konzentrierte Ansatz beschleunigt die Innovation, da Ihre Teams fundiertes Fachwissen mit den fortschrittlichen Services Ihrer primären Plattform aufbauen können. Ihr technisches Personal kann zu Spezialisten für eine Architektur werden, anstatt sich über mehrere Umgebungen hinweg nur oberflächliches Wissen anzueignen. Wenn Techniker eine Plattform beherrschen, können sie effizienter bauen, Fehler schneller beheben und anspruchsvollere Lösungen implementieren.

Unternehmen, die den 80/20-Ansatz verfolgen, berichten in der Regel von einer besseren Mitarbeiterbindung, da ihre Teams wertvolles, marktfähiges Fachwissen entwickeln, anstatt auf mehrere Technologien verteilt zu sein. Diese konzentrierte Strategie trägt auch zur Vereinfachung des Sicherheitsmanagements bei, indem sie die Komplexität der verschiedenen Sicherheitsmodelle zwischen den Anbietern begrenzt. Der Großteil Ihrer Investitionen in Sicherheitstools, Überwachungslösungen und Betriebsprozesse fließt in die primäre Cloud. Dies schafft eine stärkere Sicherheitsgrundlage als das, was mit gleichmäßig verteilten Ressourcen möglich wäre.

Unsere Leitlinien:

- Wählen Sie einen primären Cloud-Anbieter, der den meisten Ihrer geschäftlichen und technischen Anforderungen entspricht. Dieser Anbieter sollte mindestens 80% Ihrer Workloads unterstützen und die Grundlage Ihrer Cloud-Strategie bilden. Konzentrieren Sie Ihre Investitionen in Schulungen, Architekturstandards und Betriebsprozesse darauf, den Nutzen dieser primären Plattform zu maximieren.

- Entwickeln Sie klare Kriterien für Workloads, die eine Platzierung in sekundären Clouds rechtfertigen. Diese Kriterien sollten sich auf einen bestimmten Geschäftswert konzentrieren, der mit Ihrem primären Anbieter nicht erzielt werden kann. Widerstehen Sie der Verlagerung von Workloads in sekundären Clouds, nur um Ausgabengerechtigkeit oder ein künstliches Gleichgewicht zwischen den Anbietern aufrechtzuerhalten.
- Strukturieren Sie Ihre Unternehmensvereinbarungen so, dass sie Ihrem 80/20-Ansatz entsprechen. Verhandeln Sie Mengenrabatte mit Ihrem Hauptanbieter auf der Grundlage konzentrierter Ausgaben und wahren Sie die Flexibilität bei sekundären Anbietern für bestimmte Anwendungsfälle. Dieser Ansatz maximiert Ihre Kaufkraft und führt in der Regel zu besseren Gesamtpreisen, als wenn Sie Ihre Ausgaben gleichmäßig verteilen würden.
- Passen Sie Ihre Talentstrategie an Ihrem 80/20-Ansatz an. Investieren Sie in die Entwicklung fundierter Fachkenntnisse mit den Services Ihres Hauptanbieters und behalten Sie gleichzeitig ausreichende Kenntnisse über sekundäre Plattformen zur Unterstützung bestimmter Workloads bei. Diese gezielte Talentstrategie verbessert die Produktivität, beschleunigt die Bereitstellung und verringert das Risiko kritischer Qualifikationslücken.
- Messen Sie regelmäßig die Geschäftsergebnisse Ihrer Multi-Cloud-Strategie. Verfolgen Sie Kennzahlen, die den Mehrwert der einzelnen Anbieter belegen, und passen Sie gegebenenfalls Ihren Vertrieb an. Das Ziel besteht nicht darin, Multicloud vollständig zu vermeiden, sondern sie strategisch dort zu implementieren, wo bestimmte Workloads wirklich von Funktionen profitieren, die es nur bei anderen Anbietern gibt.

Schlussfolgerung

In diesem paper wurden neun wichtige Grundsätze für die Entwicklung einer effektiven Multi-Cloud-Strategie dargelegt. Den größten Erfolg erzielen Organizations durch einen primären Cloud-Ansatz mit strategischem Einsatz zusätzlicher Anbieter, wenn spezifische Geschäftsanforderungen dies erfordern. Der von uns beschriebene 80/20-Ansatz bringt Fokus und Flexibilität in Einklang und ermöglicht es Unternehmen, tieferes Fachwissen zu entwickeln, engere Anbieterbeziehungen zu pflegen und wertvollere Talente zu gewinnen, während gleichzeitig legitime Multi-Cloud-Anforderungen erfüllt werden.

Eine erfolgreiche Multi-Cloud-Implementierung erfordert eine klare Bewertung der Geschäftsanforderungen, anstatt Branchentrends zu folgen. Unternehmen müssen eine solide Governance einrichten, der Sicherheit oberste Priorität einräumen, eine Verteilung der verbundenen Workloads auf mehrere Anbieter vermeiden, Anwendungen mit ihren Transaktionsdaten verwalten, Container-Beschränkungen erkennen und ein einheitliches, aber spezialisiertes Cloud Center of Excellence unterhalten.

Der AWS Cloud-Ansatz basiert im Wesentlichen auf der Wahlfreiheit und Interoperabilität der Kunden. Wir haben unsere Tools und Services so konzipiert, dass sie nahtlos in allen Umgebungen funktionieren, da wir wissen, dass Ihre Geschäftsanforderungen oft über einen einzelnen Anbieter hinausgehen. Von hybriden Konnektivitätslösungen bis hin zur Container-Orchestrierung, die sich über Umgebungen erstreckt und Funktionen AWS bietet, mit denen Sie in Ihrer gesamten Technologielandschaft effektiv arbeiten können.

Anstatt Sie zu zwingen, Experten für mehrere Plattformen zu werden, AWS vereinfacht das Multi-Cloud-Management mithilfe intuitiver Tools und einheitlicher Benutzeroberflächen. Wir konzentrieren uns darauf, Komplexität zu reduzieren, damit Sie sich auf Innovation konzentrieren können. Diese Funktionen helfen Ihnen dabei, Ihre Multi-Cloud-Strategie nach Ihren eigenen Vorstellungen umzusetzen — unabhängig davon, ob Sie diese AWS ausschließlich nutzen oder bestimmte AWS-Services Umgebungen zusammen mit anderen nutzen.

Die Cloud sollte Ihre Geschäftsstrategie stärken, nicht einschränken. Durch die Anwendung der in diesem paper beschriebenen Prinzipien und die Nutzung von AWS Interoperabilitätsfunktionen können Sie einen Cloud-Ansatz entwickeln, der den Wert maximiert, unnötige Komplexität minimiert und Ihr Unternehmen für langfristigen Erfolg im heutigen dynamischen Geschäftsumfeld positioniert.

Weitere Informationen zu AWS Lösungen, die zur Vereinfachung der Verwaltung in Hybrid- und Multi-Cloud-Umgebungen beitragen können, finden Sie unter AWS Lösungen für Multicloud-Umgebungen.

Ressourcen

Referenzen

- Nutzung eines Cloud Center of Excellence (CCOE) zur Transformation des gesamten Unternehmens (AWS Blogbeitrag)
- AWS Well-Architected Framework
- Identifizierung von Geschäftschancen mit Cost Optimization Hub (Dokumentation)AWS Cost Management
- Der geschäftliche Nutzen der Migration zu Amazon Web Services (The Hackett Group, Februar 2022)
- Kostenlose Datenübertragung ins Internet beim Umzug von AWS (AWS Blogbeitrag)

Tools

- Zonal Autoshift — Verlagern Sie Ihren Traffic automatisch von Availability Zones weg, wenn wir potenzielle Probleme erkennen (AWS Blogbeitrag)
- AWS Lösungen für Multicloud

AWS Partner

- AWS Cloud Kompetenz im Bereich Operations

Dokumentverlauf

In der folgenden Tabelle werden wichtige Änderungen in diesem Leitfaden beschrieben. Um Benachrichtigungen über zukünftige Aktualisierungen zu erhalten, können Sie einen RSS-Feed abonnieren.

Änderung	Beschreibung	Datum
Erste Veröffentlichung	—	3. September 2025

AWS Glossar zu präskriptiven Leitlinien

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

Zahlen

7 Rs

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

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

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

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

A

ABAC

Siehe attributbasierte Zugriffskontrolle.

abstrahierte Dienste

Siehe Managed Services.

ACID

Siehe Atomarität, Konsistenz, Isolierung und Haltbarkeit.

Aktiv-Aktiv-Migration

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

Aktiv-Passiv-Migration

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

Aggregatfunktion

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

AI

Siehe künstliche Intelligenz.

AIOps

Siehe Operationen im Bereich künstliche Intelligenz.

Anonymisierung

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

Anti-Muster

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

Anwendungssteuerung

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

Anwendungsportfolio

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

künstliche Intelligenz (KI)

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

Operationen mit künstlicher Intelligenz (AIOps)

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

Asymmetrische Verschlüsselung

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

Atomizität, Konsistenz, Isolierung, Haltbarkeit (ACID)

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

Attributbasierte Zugriffskontrolle (ABAC)

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

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 Einführung der Cloud (AWS CAF)

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

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

AWS Workload-Qualifizierungsrahmen (AWS WQF)

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

B

schlechter Bot

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

BCP

Siehe Planung der Geschäftskontinuität.

Verhaltensdiagramm

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

Big-Endian-System

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

Binäre Klassifikation

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

Bloom-Filter

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

Blau/Grün-Bereitstellung

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

Bot

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

Botnetz

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

branch

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

Zugang durch Glasbruch

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

Brownfield-Strategie

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

Puffer-Cache

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

Geschäftsfähigkeit

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

Planung der Geschäftskontinuität (BCP)

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

C

CAF

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

Bereitstellung auf Kanaren

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

CCoE

Weitere Informationen finden Sie im Cloud Center of Excellence.

CDC

Siehe Erfassung von Änderungsdaten.

Erfassung von Datenänderungen (CDC)

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

Chaos-Technik

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

CI/CD

Siehe Continuous Integration und Continuous Delivery.

Klassifizierung

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

clientseitige Verschlüsselung

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

Cloud-Exzellenzzentrum (CCoE)

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

Cloud Computing

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

Cloud-Betriebsmodell

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

Phasen der Einführung der Cloud

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

- Projekt – Durchführung einiger Cloud-bezogener Projekte zu Machbarkeitsnachweisen und zu Lernzwecken
- Fundament — Tätigen Sie grundlegende Investitionen, um Ihre Cloud-Einführung zu skalieren (z. B. Einrichtung einer landing zone, Definition eines CCo E, Einrichtung eines Betriebsmodells)
- Migration – Migrieren einzelner Anwendungen
- Neuentwicklung – Optimierung von Produkten und Services und Innovation in der Cloud

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

CMDB

Siehe Datenbank für das Konfigurationsmanagement.

Code-Repository

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

Kalter Cache

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

Kalte Daten

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

Computer Vision (CV)

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

Drift in der Konfiguration

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

Verwaltung der Datenbankkonfiguration (CMDB)

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

Konformitätspaket

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

Kontinuierliche Bereitstellung und kontinuierliche Integration (CI/CD)

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

CV

Siehe Computer Vision.

D

Daten im Ruhezustand

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

Datenklassifizierung

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

Datendrift

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

Daten während der Übertragung

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

Datennetz

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

Datenminimierung

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

Datenperimeter

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

Vorverarbeitung der Daten

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

Herkunft der Daten

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

betroffene Person

Eine Person, deren Daten gesammelt und verarbeitet werden.

Data Warehouse

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

Datenbankdefinitionssprache (DDL)

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

Datenbankmanipulationssprache (DML)

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

DDL

Siehe Datenbankdefinitionssprache.

Deep-Ensemble

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

Deep Learning

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

defense-in-depth

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

delegierter Administrator

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

Einsatz

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

Entwicklungsumgebung

Siehe Umgebung.

Detektivische Kontrolle

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

Abbildung des Wertstroms in der Entwicklung (DVSM)

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

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

digitaler Zwilling

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

Maßtabelle

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

Katastrophe

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

Notfallwiederherstellung (DR)

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

DML

Siehe Sprache zur Datenbankmanipulation.

Domainorientiertes Design

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

DR

Siehe Disaster Recovery.

Erkennung von Driften

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

DVSM

Siehe Abbildung des Wertstroms in der Entwicklung.

E

EDA

Siehe explorative Datenanalyse.

EDI

Siehe elektronischer Datenaustausch.

Edge-Computing

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

elektronischer Datenaustausch (EDI)

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

Verschlüsselung

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

Verschlüsselungsschlüssel

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

Endianismus

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

Endpunkt

Siehe Service-Endpunkt.

Endpunkt-Services

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

Unternehmensressourcenplanung (ERP)

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

Envelope-Verschlüsselung

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

Umgebung

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

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

- Produktionsumgebung – Eine Instance einer laufenden Anwendung, auf die Endbenutzer zugreifen können. In einer CI/CD Pipeline ist die Produktionsumgebung die letzte Bereitstellungsumgebung.
- Höhere Umgebungen – Alle Umgebungen, auf die auch andere Benutzer als das Kernentwicklungsteam zugreifen können. Dies kann eine Produktionsumgebung, Vorproduktionsumgebungen und Umgebungen für Benutzerakzeptanztests umfassen.

Epics

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

ERP

Siehe Enterprise Resource Planning.

Explorative Datenanalyse (EDA)

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

F

Faktentabelle

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

schnell scheitern

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

Grenze zur Fehlerisolierung

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

Feature-Zweig

Siehe Zweig.

Features

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

Bedeutung der Feature

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

Featuretransformation

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

Eingabeaufforderung mit wenigen Klicks

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

FGAC

Siehe detaillierte Zugriffskontrolle.

Feinkörnige Zugriffskontrolle (FGAC)

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

Flash-Cut-Migration

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

FM

Siehe Fundamentmodell.

Fundamentmodell (FM)

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

G

Generative KI

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

Geoblocking

Siehe geografische Einschränkungen.

Geografische Einschränkungen (Geoblocking)

Bei Amazon eine Option CloudFront, um zu verhindern, dass Benutzer in bestimmten Ländern auf Inhaltsverteilungen zugreifen. Sie können eine Zulassungsliste oder eine Sperrliste verwenden,

um zugelassene und gesperrte Länder anzugeben. Weitere Informationen finden Sie in der Dokumentation unter Beschränkung der geografischen Verteilung Ihrer Inhalte. CloudFront

Gitflow-Workflow

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

goldenes Bild

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

Greenfield-Strategie

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

Integritätsschutz

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

H

HEKTAR

Siehe Hochverfügbarkeit.

Heterogene Datenbankmigration

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

hohe Verfügbarkeit (HA)

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

historische Modernisierung

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

Daten zurückhalten

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

Homogene Datenbankmigration

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

heiße Daten

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

Hotfix

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

Hypercare-Phase

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

I

IaC

Sehen Sie Infrastruktur als Code.

Identitätsbasierte Richtlinie

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

Leerlaufanwendung

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

IIoT

Siehe Industrielles Internet der Dinge.

unveränderliche Infrastruktur

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

Eingehende (ingress) VPC

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

Inkrementelle Migration

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

Industrie 4.0

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

Infrastruktur

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

Infrastructure as Code (IaC)

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

industrielles Internet der Dinge (T) IIo

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

Inspektions-VPC

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

Internet of Things (IoT)

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

Interpretierbarkeit

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

IoT

Siehe Internet der Dinge.

IT information library (ITIL, IT-Informationsbibliothek)

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

T service management (ITSM, IT-Servicemanagement)

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

BIS

Siehe IT-Informationsbibliothek.

ITSM

Siehe IT-Servicemanagement.

L

Labelbasierte Zugangskontrolle (LBAC)

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

Landing Zone

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

großes Sprachmodell (LLM)

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

Große Migration

: Eine Migration von 300 oder mehr Servern.

SCHWARZ

: Siehe Labelbasierte Zugriffskontrolle.

Geringste Berechtigung

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

Lift and Shift

: Siehe 7 Rs.

Little-Endian-System

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

LLM

Siehe großes Sprachmodell.

Niedrigere Umgebungen

Siehe Umgebung.

M

Machine Learning (ML)

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

Hauptzweig

Siehe Filiale.

Malware

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

verwaltete Dienste

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

Manufacturing Execution System (MES)

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

MAP

Siehe Migration Acceleration Program.

Mechanismus

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

Mitgliedskonto

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

MES

Siehe Manufacturing Execution System.

Message Queuing-Telemetrietransport (MQTT)

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

Microservice

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

Microservices-Architekturen

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

Migration Acceleration Program (MAP)

Ein AWS Programm, das Beratung, Unterstützung, Schulungen und Services bietet, um Unternehmen dabei zu unterstützen, eine solide betriebliche Grundlage für die Umstellung auf

die Cloud zu schaffen und die anfänglichen Kosten von Migrationen auszugleichen. MAP umfasst eine Migrationsmethode für die methodische Durchführung von Legacy-Migrationen sowie eine Reihe von Tools zur Automatisierung und Beschleunigung gängiger Migrationsszenarien.

Migration in großem Maßstab

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

Migrationsfabrik

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

Migrationsmetadaten

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

Migrationsmuster

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

Migration Portfolio Assessment (MPA)

Ein Online-Tool, das Informationen zur Validierung des Geschäftsszenarios für die Migration auf das bereitstellt. AWS Cloud MPA bietet eine detaillierte Portfoliobewertung (richtige Servergröße, Preisgestaltung, Gesamtbetriebskostenanalyse, Migrationskostenanalyse) sowie Migrationsplanung (Anwendungsdatenanalyse und Datenerfassung, Anwendungsgruppierung,

Migrationspriorisierung und Wellenplanung). Das MPA-Tool (Anmeldung erforderlich) steht allen AWS Beratern und APN-Partnerberatern kostenlos zur Verfügung.

Migration Readiness Assessment (MRA)

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

Migrationsstrategie

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

ML

Siehe maschinelles Lernen.

Modernisierung

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

Bewertung der Modernisierungsfähigkeit

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

Monolithische Anwendungen (Monolithen)

Anwendungen, die als ein einziger Service mit eng gekoppelten Prozessen ausgeführt werden. Monolithische Anwendungen haben verschiedene Nachteile. Wenn ein Anwendungs-Feature stark nachgefragt wird, muss die gesamte Architektur skaliert werden. Das Hinzufügen oder

Verbessern der Feature einer monolithischen Anwendung wird ebenfalls komplexer, wenn die Codebasis wächst. Um diese Probleme zu beheben, können Sie eine Microservices-Architektur verwenden. Weitere Informationen finden Sie unter Zerlegen von Monolithen in Microservices.

MPA

Siehe Bewertung des Migrationsportfolios.

MQTT

Siehe Message Queuing-Telemetrietransport.

Mehrklassen-Klassifizierung

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

veränderbare Infrastruktur

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

O

OAC

Siehe Origin Access Control.

EICHE

Siehe Zugriffsidentität von Origin.

COM

Siehe organisatorisches Change-Management.

Offline-Migration

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

OI

Siehe Betriebsintegration.

OLA

Siehe Vereinbarung auf operativer Ebene.

Online-Migration

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

OPC-UA

Siehe Open Process Communications — Unified Architecture.

Offene Prozesskommunikation — Einheitliche Architektur (OPC-UA)

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

Vereinbarung auf Betriebsebene (OLA)

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

Überprüfung der Betriebsbereitschaft (ORR)

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

Betriebstechnologie (OT)

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

Betriebsintegration (OI)

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

Organisationspfad

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

Organisatorisches Veränderungsmanagement (OCM)

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

Ursprungszugriffskontrolle (OAC)

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

Ursprungszugriffsidentität (OAI)

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

ORR

Weitere Informationen finden Sie unter Überprüfung der Betriebsbereitschaft.

NICHT

Siehe Betriebstechnologie.

Ausgehende (egress) VPC

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

P

Berechtigungsgrenze

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

persönlich identifizierbare Informationen (PII)

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

Personenbezogene Daten

Siehe persönlich identifizierbare Informationen.

Playbook

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

PLC

Siehe programmierbare Logiksteuerung.

PLM

Siehe Produktlebenszyklusmanagement.

policy

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

Polyglotte Beharrlichkeit

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

Portfoliobewertung

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

predicate

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

Prädikat Pushdown

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

Präventive Kontrolle

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

Prinzipal

Eine Entität AWS , die Aktionen ausführen und auf Ressourcen zugreifen kann. Diese Entität ist in der Regel ein Root-Benutzer für eine AWS-Konto, eine IAM-Rolle oder einen Benutzer. Weitere Informationen finden Sie unter Prinzipal in Rollenbegriffe und -konzepte in der IAM-Dokumentation.

Datenschutz von Natur aus

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

Privat gehostete Zonen

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

proaktive Steuerung

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

Produktlebenszyklusmanagement (PLM)

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

Produktionsumgebung

Siehe Umgebung.

Speicherprogrammierbare Steuerung (SPS)

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

schnelle Verkettung

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

Pseudonymisierung

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

publish/subscribe (pub/sub)

Ein Muster, das asynchrone Kommunikation zwischen Microservices ermöglicht, um die Skalierbarkeit und Reaktionsfähigkeit zu verbessern. In einem auf Microservices basierenden MES kann ein Microservice beispielsweise Ereignismeldungen in einem Kanal veröffentlichen, den andere Microservices abonnieren können. Das System kann neue Microservices hinzufügen, ohne den Veröffentlichungsservice zu ändern.

Q

Abfrageplan

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

Abfrageplanregression

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

R

RACI-Matrix

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

RAG

Siehe Erweiterte Generierung beim Abrufen.

Ransomware

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

RASCI-Matrix

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

RCAC

Siehe Zugriffskontrolle für Zeilen und Spalten.

Read Replica

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

neu strukturieren

Siehe 7 Rs.

Recovery Point Objective (RPO)

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

Wiederherstellungszeitziel (RTO)

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

Refaktorierung

Siehe 7 Rs.

Region

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

Regression

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

rehosten

Siehe 7 Rs.

Veröffentlichung

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

umziehen

Siehe 7 Rs.

neue Plattform

Siehe 7 Rs.

Rückkauf

Siehe 7 Rs.

Ausfallsicherheit

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

Ressourcenbasierte Richtlinie

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

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

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

Reaktive Kontrolle

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

Beibehaltung

Siehe 7 Rs.

zurückziehen

Siehe 7 Rs.

Retrieval Augmented Generation (RAG)

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

Drehung

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

Zugriffskontrolle für Zeilen und Spalten (RCAC)

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

RPO

Siehe Recovery Point Objective.

RTO

Siehe Ziel für die Erholungszeit.

Runbook

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

S

SAML 2.0

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

SCADA

Siehe Aufsichtskontrolle und Datenerfassung.

SCP

Siehe Richtlinie zur Dienstkontrolle.

Secret

Interne AWS Secrets Manager, vertrauliche oder eingeschränkte Informationen, wie z. B. ein Passwort oder 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.

Sicherheit durch Design

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

Sicherheitskontrolle

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

Härtung der Sicherheit

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

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

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

Automatisierung von Sicherheitsreaktionen

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

Serverseitige Verschlüsselung

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

Service-Kontrollrichtlinie (SCP)

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

Service-Endpunkt

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

Service Level Agreement (SLA)

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

Service-Level-Indikator (SLI)

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

Service-Level-Ziel (SLO)

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

Modell der geteilten Verantwortung

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

SIEM

Siehe Sicherheitsinformations- und Event-Management-System.

Single Point of Failure (SPOF)

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

SLA

Siehe Service Level Agreement.

SLI

Siehe Service-Level-Indikator.

ALSO

Siehe Service-Level-Ziel.

split-and-seed Modell

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

SPOTTEN

Siehe Single Point of Failure.

Sternschema

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

Strangler-Fig-Muster

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

Subnetz

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

Aufsichtskontrolle und Datenerfassung (SCADA)

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

Symmetrische Verschlüsselung

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

synthetisches Testen

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

Systemaufforderung

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

T

tags

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

Zielvariable

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

Aufgabenliste

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

Testumgebungen

Siehe Umgebung.

Training

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

Transit-Gateway

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

Stammbasierter Workflow

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

Vertrauenswürdiger Zugriff

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

Optimieren

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

Zwei-Pizzen-Team

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

U

Unsicherheit

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

undifferenzierte Aufgaben

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

höhere Umgebungen

Siehe Umgebung.

V

Vacuuming

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

Versionskontrolle

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

VPC-Peering

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

Schwachstelle

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

W

Warmer Cache

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

warme Daten

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

Fensterfunktion

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

Workload

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

Workstream

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

WURM

Sehen Sie einmal schreiben, viele lesen.

WQF

Siehe AWS Workload-Qualifizierungsrahmen.

einmal schreiben, viele lesen (WORM)

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

Z

Zero-Day-Exploit

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

Zero-Day-Sicherheitslücke

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

Eingabeaufforderung ohne Zwischenfälle

Bereitstellung von Anweisungen für die Ausführung einer Aufgabe an einen LLM, jedoch ohne Beispiele (Schnappschüsse), die ihm als Orientierungshilfe dienen könnten. Der LLM muss sein vortrainiertes Wissen einsetzen, um die Aufgabe zu bewältigen. Die Effektivität von Zero-Shot Prompting hängt von der Komplexität der Aufgabe und der Qualität der Aufforderung ab. Siehe auch Few-Shot-Prompting.

Zombie-Anwendung

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

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