Entwicklung einer Strategie für Single-, Hybrid- und Multi-Cloud im Bildungswesen

AWS Präskriptive Leitlinien

AWS Präskriptive Leitlinien: Entwicklung einer Strategie für Single-, Hybrid- und Multi-Cloud im Bildungswesen

Table of Contents

Entwicklung einer Strategie für Single-, Hybrid- und Multi-Cloud im Bildungswesen

Amazon Web Services (Mitwirkende)

September 2023 (Verlauf der Dokumente)

Bildungseinrichtungen sind bestrebt, Funktionen wie Fernunterricht, Forschung, Studentenerfahrung, Dateneinblicke und Verwaltung mit der Agilität, Kosteneinsparungen, Sicherheit und Belastbarkeit zu unterstützen, die Cloud Computing bietet. Viele Unternehmen erwägen im Rahmen dieser digitalen Transformation Hybrid- und Multi-Cloud-Implementierungen.

Dieses paper enthält präskriptive Leitlinien zur Entwicklung einer Technologie- und Governance-Strategie für Single-, Hybrid- und Multi-Cloud-Technologien und -Governance-Strategien für Führungskräfte und Entscheidungsträger von Bildungseinrichtungen, die ihre Cloud-Optionen evaluieren. Diese Leitlinien basieren auf unserer Erfahrung in der AWS Zusammenarbeit mit über 14.000 Bildungseinrichtungen aller Größenordnungen auf der ganzen Welt — von Grund- und Sekundarschulen bis hin zu Hochschulen.

Übersicht

Im Zuge der digitalen Transformation von Bildungseinrichtungen, um ihren Schülern, Eltern, Dozenten, Mitarbeitern und der Gemeinschaft differenzierte Dienstleistungen und Erfahrungen zu bieten, stehen sie vor einer Vielzahl von technischen Entscheidungen. Viele Unternehmen haben sich bereits für die Einführung der Cloud entschieden, um mehr Agilität, Elastizität, Belastbarkeit, Sicherheit und Kosteneinsparungen zu erzielen. Aufgrund ihrer bestehenden Beziehungen und Investitionen innerhalb verschiedener Teams nutzen die meisten Unternehmen eine Kombination aus lokalen Rechenzentren, Colocation-Einrichtungen und Cloud-Anbietern. Angesichts der Verfügbarkeit mehrerer Cloud-Optionen müssen sich Bildungseinrichtungen häufig zwischen Single-, Hybrid- und Multi-Cloud-Bereitstellungsmodellen entscheiden (definiert im Abschnitt Cloud-Bereitstellungsstrategien).

Multicloud, also die Nutzung von Diensten von mindestens zwei Cloud-Dienstanbietern, ist für viele Institutionen heute keine Seltenheit. Ihr IT-Team bevorzugt möglicherweise einen Cloud-Anbieter, während sich andere Gruppen, Abteilungen oder einzelne Benutzer möglicherweise für alternative Anbieter entscheiden oder diese bereits nutzen. Bildungseinrichtungen, die keine klare Strategie haben, um sie zum geeigneten Cloud-Bereitstellungsmodell zu führen, stehen

vor vielen Herausforderungen. Dazu gehören unnötige Komplexität, steigender Personalbedarf, inkonsistente Unternehmensführung und Ansätze mit dem kleinsten gemeinsamen Nenner, die sie auf die Teilmenge der Basisfunktionen beschränken, die allen Anbietern gemeinsam sind. Jede Herausforderung behindert Innovationen und verlangsamt die digitale Transformation.

Umgekehrt können Sie mit einer Cloud-Strategie, die Sie zur Nutzung von Single-, Hybrid- und Multi-Clouds anleitet, Ihre Anforderungen im Bildungswesen erfüllen und gleichzeitig die Vorteile der Cloud auf eine Art und Weise nutzen, die betrieblich nachhaltig ist und einen langfristigen Erfolg gewährleistet. Für die Erstellung dieser Strategie empfehlen wir Folgendes:

- Wählen Sie einen primären, strategischen Cloud-Anbieter aus.
- Richten Sie ein Cloud Center of Excellence (CCoE) ein.
- Unterscheiden Sie zwischen Software-as-a-Service (SaaS) -Anwendungen und grundlegenden Cloud-Diensten.
- Legen Sie Sicherheits- und Governance-Anforderungen für jeden Cloud-Dienstanbieter fest.
- Setzen Sie Cloud-native, verwaltete Lösungen ein, wo immer dies möglich und praktikabel ist.
- Implementieren Sie Hybridarchitekturen, wenn bestehende Investitionen vor Ort Anreize für eine weitere Nutzung bieten.
- Reservieren Sie Multicloud nur für Workloads, die die technischen oder geschäftlichen Anforderungen nicht über einen einzigen Cloud-Anbieter erfüllen können.

Diese bewährten Verfahren werden im Abschnitt Empfehlungen dieses paper ausführlich erörtert. Jede Empfehlung ist wichtig, aber die Prioritäten Ihrer Institution hängen von der Phase der Cloud-Einführung ab. Wenn Sie beispielsweise gerade erst mit der Cloud-Einführung beginnen, konzentrieren Sie sich auf die Auswahl eines primären, strategischen Cloud-Anbieters, die Einrichtung eines CCo E-Anbieters und die Einführung cloudnativer, verwalteter Lösungen. Wenn Sie bereits einen einzigen Cloud-Anbieter verwenden, konzentrieren Sie sich auf die Festlegung der wichtigsten Sicherheits- und Governance-Anforderungen und ziehen Sie Hybridarchitekturen in Betracht, wenn Ihre bestehenden Investitionen in Rechenzentren Anreize für eine weitere Nutzung bieten. Wenn Ihr Unternehmen bereits mehrere Cloud-Anbieter nutzt, sollten Sie sich darauf konzentrieren, SaaS-Anwendungen zu differenzieren und Multi-Cloud-Bereitstellungen für die seltenen Workloads zu reservieren, die sie wirklich benötigen.

Inhalt

Strategien für die Cloud-Bereitstellung

AWS definiert Cloud Computing als die Bereitstellung von IT-Ressourcen auf Abruf über das Internet mit pay-as-you-go Preisgestaltung. Anstatt physische Rechenzentren und Server zu kaufen, zu besitzen und zu warten, können Sie bei Bedarf auf Technologiedienstleistungen wie Rechenleistung, Speicher und Datenbanken von einem Cloud-Anbieter zugreifen. Cloud-Computing ermöglicht es Bildungseinrichtungen, undifferenzierte Schwerstarbeit wie Hardwarebeschaffung, Wartung und Kapazitätsplanung zu vermeiden. Bei der Einführung und Bereitstellung von Cloud-Lösungen können Sie aus verschiedenen Modellen wählen: Single Cloud, Hybrid Cloud und Multicloud.

Eine einzige Cloud

Dieses Modell verwendet nur einen einzigen Cloud-Dienstanbieter. Single-Cloud-Anwendungen und -Workloads können direkt in der Cloud implementiert oder zuvor in einer anderen Umgebung gehostet und in die Cloud migriert werden. Diese Workloads können Infrastrukturdienste auf niedrigerer Ebene ihres Cloud-Anbieters oder auch verwaltete Dienste auf höherer Ebene nutzen. Unabhängig davon verwendet dieses Modell einen einzigen Cloud-Anbieter und verwendet nur Cloud-Dienste von diesem Anbieter.

Hybride Cloud

Ein Hybrid-Cloud-Modell verteilt Ressourcen auf das unternehmenseigene Rechenzentrum vor Ort und mindestens einen Cloud-Dienstanbieter. In der Regel besteht der Zweck dieses Modells darin, die Infrastruktur eines Unternehmens auf die Cloud auszudehnen und gleichzeitig die private Konnektivität mit bestehenden internen Systemen aufrechtzuerhalten, die sich vor Ort befinden.

Multicloud

Ein Multicloud-Modell verteilt Ressourcen auf mindestens zwei Cloud-Dienstanbieter und nutzt Dienste von diesen. Ein Unternehmen mag sich für Multicloud entscheiden, aber in den meisten Fällen ist dies eine unbeabsichtigte Folge davon, dass einzelne Teams, Abteilungen oder Mitarbeiter ihre eigenen Präferenzen für verschiedene Cloud-Anbieter haben.

Empfehlungen

Nachdem Sie nun ein grundlegendes Verständnis von Single Cloud, Hybrid Cloud und Multicloud erworben haben, enthält dieser Abschnitt detaillierte Empfehlungen für die Auswahl eines Modells.

- Wählen Sie einen primären, strategischen Cloud-Anbieter
- Richten Sie ein CCo E ein
- Unterscheiden Sie zwischen SaaS-Anwendungen und grundlegenden Cloud-Diensten
- Legen Sie Sicherheits- und Governance-Anforderungen für jeden Cloud-Dienstanbieter fest
- Setzen Sie Cloud-native, verwaltete Dienste ein, wo immer dies möglich und praktikabel ist
- Implementieren Sie Hybridarchitekturen, wenn bestehende Investitionen vor Ort Anreize für eine weitere Nutzung bieten
- Reservieren Sie Multicloud nur für Workloads, die ihre technischen oder geschäftlichen Anforderungen nicht über einen einzigen Cloud-Anbieter erfüllen können

Wählen Sie einen primären, strategischen Cloud-Anbieter

Die Einführung der Cloud bietet eine Fülle von Vorteilen, die für die Modernisierung, Kosteneffizienz und Innovation der IT unerlässlich sind. Die Einführung von Cloud-Technologien, die über begrenzte SaaS-Anwendungen hinausgehen, kann jedoch zu Herausforderungen führen, die Bildungseinrichtungen sorgfältig planen müssen, um unnötige Kosten und Komplexität zu vermeiden. Die technologischen und geschäftlichen Veränderungen, die mit der Implementierung von Workloads in der Cloud einhergehen, erfordern die Bereitstellung von Mitarbeitern und Anpassungen der Kerninfrastruktur, einschließlich Netzwerk, Sicherheit, Verwaltung und Betrieb.

Der beste Ansatz zur effektiven Bewältigung dieser Herausforderungen, insbesondere wenn sich Ihr Unternehmen in der Anfangsphase seiner Cloud-Umstellung befindet, besteht darin, einen primären, strategischen Cloud-Anbieter auszuwählen, der den Großteil Ihrer Workloads unterstützt. Beginnen Sie mit einer gezielten Einführung, die sich auf diesen Anbieter konzentriert, sodass Sie die Nutzung der Cloud-Vorteile vereinfachen und beschleunigen können. Die Auswahl eines primären Cloud-Anbieters ist keine ausschließliche, unumkehrbare Entscheidung. Es ermöglicht Ihrem Unternehmen, Ihre Cloud-Einführung iterativ weiterzuentwickeln. Sie können sich zunächst auf einige Dienste konzentrieren und dann bei Bedarf auf andere Cloud-Dienste ausweiten, ohne die Gesamtvorteile der Cloud zu beeinträchtigen. Dieser Ansatz maximiert die Fähigkeit Ihres Unternehmens, die Fähigkeiten eines Anbieters zu nutzen, die Fähigkeiten der Mitarbeiter zu

konzentrieren und weiterzuentwickeln und die Beziehungen zu Drittanbietern zu verbessern und das Lieferantenmanagement zu vereinfachen.

Wir haben gesehen, dass Kunden ihre Reise in die Cloud eingeschlagen haben, indem sie versucht haben, mehrere Cloud-Anbieter gleichzeitig zu nutzen, aber später diese Entscheidung und die damit verbundene Komplexität bereuen. Gartner teilt diese Erkenntnisse in seinem Artikel 6 Schritte zur Planung einer Cloud-Strategie, in dem Schritt 2 „Priorisieren Sie einen primären Anbieter in Multicloud-Architekturen“.

Jeder Cloud-Anbieter führt unterschiedliche Betriebs- und Supportmodelle, Identitäts- und Zugriffsmanagement, Netzwerke, Betriebsabläufe, Compliance-Funktionen und mehr ein. Es ist besser, das Betriebsmodell eines Cloud-Anbieters nach dem anderen zu beherrschen.Sie können dann schrittweise und schrittweise zusätzliche Cloud-Dienste integrieren, sofern dies rationalisiert ist. Viele Faktoren können Ihre Entscheidung, einen primären Cloud-Anbieter zu wählen, beeinflussen. Lassen Sie sich bei der Auswahl jedoch von den folgenden Schlüsselfragen leiten.

- Welche Breite und Tiefe der Dienstleistungen bietet der Anbieter an?

  Verschiedene Cloud-Anbieter bieten unterschiedliche Dienste an. Stellen Sie mindestens sicher, dass Ihr primärer Anbieter über die erforderlichen Fähigkeiten verfügt, um all Ihre funktionalen Anforderungen sowie Ihre bereichsübergreifenden betrieblichen Anforderungen wie Sicherheit, Verwaltung und Automatisierung zu erfüllen. Wählen Sie einen Anbieter, der diese Funktionen mit einer nachgewiesenen Erfolgsbilanz in Bezug auf Innovation und betriebliche Exzellenz bietet. Denken Sie nicht nur an Ihre Anwendungen, sondern auch an Ihre Daten. Denken Sie über future Datenintegrations- und Übertragungsmuster nach, um die Kosten, Latenz und Komplexität der Übertragung großer Datenmengen zwischen Anbietern zu begrenzen. Wählen Sie einen Anbieter, der über die größtmögliche Breite und Tiefe an Diensten verfügt, um Ihre aktuellen Anwendungs- und Datenanforderungen zu erfüllen und neue Anwendungsfälle zu erschließen, die den sich im Laufe der Zeit ändernden Anforderungen Ihrer Institution gerecht werden können.
- Kann der Anbieter all Ihre Sicherheits- und Compliance-Anforderungen erfüllen?

  Im Bildungswesen sind Sicherheit und Compliance für jeden Technologieeinsatz von entscheidender Bedeutung. Wählen Sie einen Cloud-Anbieter, der in der Lage ist, all Ihre Sicherheits- und Compliance-Anforderungen zu erfüllen. Tools wie AWS Artifactkönnen Ihnen bei der Bewertung von Anbietern helfen, indem sie eine zentrale Ressource für den On-Demand-Zugriff auf Sicherheits- und Compliance-Berichte bereitstellen. Denken Sie nicht nur an die Sicherheit und Konformität der Infrastruktur und der Dienste des Cloud-Anbieters, sondern auch daran, wie einfach es für Sie ist, mithilfe dieser Dienste sichere, konforme Lösungen zu entwickeln.

Bevorzugen Sie einen Anbieter, der eine Kombination aus vorgefertigten Lösungen, Schnellstarts und präskriptiven Anleitungen anbietet, um Ihre sichere Einführung der Cloud zu beschleunigen.

- Verfügt der Anbieter über ein robustes Partnernetzwerk?

  Kein Unternehmen durchläuft die Cloud-Transformation alleine. Um die Einführung zu beschleunigen, sollten Sie die Dienste und das Fachwissen des Cloud-Anbieters sowie dessen Partnernetzwerk nutzen. Zu diesem Netzwerk gehören Technologiepartner, die Software anbieten, die auf Cloud-Technologie läuft, sich in diese integriert oder diese unterstützt, sowie Beratungspartner, die Ihnen helfen können, Ihre eigenen Anwendungen in der Cloud zu entwerfen, zu erstellen, auszuführen und zu verwalten. Sie werden feststellen, dass viele Anbieter von Bildungstechnologie, unabhängige Softwareanbieter (ISVs), Berater und Wiederverkäufer, mit denen Sie bereits zusammenarbeiten, Mitglieder des Partnernetzwerks des Cloud-Anbieters sind. Bevorzugen Sie einen Cloud-Anbieter, der über das robusteste Netzwerk von Partnern mit geprüften Kompetenzen verfügt. Es ist von entscheidender Bedeutung, Partner mit nachgewiesener Branchen- und technischer Expertise zu haben.

- Welchen Support und welche Unterstützung bietet der Anbieter?

  Um eine neue Technologie erfolgreich einzuführen, benötigen Sie Mechanismen, mit denen Sie Schulungen und Hilfe anfordern können. Dazu gehören Empfehlungen für bewährte Verfahren, Anleitungen zur Konfiguration und Problembehebung. Wenn Sie sich für einen Cloud-Anbieter entscheiden, der umfassende Support- und Schulungsmöglichkeiten bietet, sind Sie auf Erfolgskurs. Informieren Sie sich über das offizielle Support-Modell und die Ressourcen des Anbieters sowie über alle verfügbaren Ressourcen von Drittanbietern oder Community-basierten Ressourcen wie Blogs, Foren, Videos und Anleitungen. Ziehen Sie nicht nur die technischen Supportprogramme des Anbieters in Betracht, sondern auch Programme, die sich auf die geschäftliche und kulturelle Transformation konzentrieren. Das AWS Cloud Adoption Framework (AWS CAF) unterstützt Unternehmen beispielsweise bei der digitalen Transformation, indem es sich auf Perspektiven konzentriert, die Geschäftsprozesse und Menschen einbeziehen, nicht nur Technologie. Bevorzugen Sie einen Cloud-Anbieter, der umfangreiche Schulungsmöglichkeiten sowie ein bewährtes, zuverlässiges Support-Modell und eine Community bietet.

Richten Sie ein CCo E ein

Erwägen Sie, Ihre Cloud-Führungsfunktion durch ein Transformationsbüro oder ein Cloud Center of Excellence (CCoE) weiterzuentwickeln. A CCo E entwickelt und verbreitet einen Ansatz für die Implementierung von Cloud-Technologie in großem Maßstab in einem Unternehmen. Für eine

erfolgreiche Cloud-Einführung sollten Sie Ihr CCo E so gestalten, dass es Vertreter einbezieht, die für die beteiligten Teams und Abteilungen sprechen können. Fangen Sie klein an und entwickeln Sie das CCo E schrittweise weiter, um es an Ihre Bedürfnisse anzupassen, während Sie die Transformation vorantreiben. Ihre wichtigsten Vertreter des Cloud-Anbieters, z. B. Ihr AWS Account Manager und Ihr Lösungsarchitekt, können Ihnen Ressourcen zur Verfügung stellen, die Sie bei der Erstellung Ihres CCo E unterstützen. Ein CCo E beschleunigt Ihre Fähigkeit, fachliches Fachwissen aufzubauen, Zustimmung zu erzielen, Vertrauen in Ihrem gesamten Unternehmen zu gewinnen und effektive Richtlinien für die Erfüllung Ihrer Unternehmensanforderungen festzulegen. Es gibt keine einheitliche Organisationsstruktur, die für jede Institution geeignet ist, aber die folgenden Fragen sollen Ihnen helfen, Ihr eigenes E zu entwerfen. CCo

- Wen sollten Sie in Ihr CCo E aufnehmen?

  Zu Beginn umfasst ein CCo E möglicherweise nur eine Handvoll Early Adopters und Cloud-Champions. Das CCo E mag klein bleiben, sollte sich aber weiterentwickeln und Champions einbeziehen, die sowohl für die Geschäftsfunktionen als auch für die technischen Funktionen sprechen können, die von der Cloud-Einführung betroffen sind. Zu den Geschäftsfunktionen gehören Change-Management, Anforderungen von Stakeholdern, Unternehmensführung, Schulung, Beschaffung und Kommunikation. Diese Funktionen werden in der Regel durch Mitglieder der Verwaltungs- und Lehrteams Ihrer Institution vertreten. Zu den technischen Funktionen gehören Infrastruktur, Automatisierung, Betriebstools, Sicherheit, Leistung und Verfügbarkeit. Diese Funktionen werden in der Regel von Mitgliedern der IT-Teams Ihrer Institution vertreten. Die CCo E sollte auch versuchen, bei Bedarf Anbieter und Partner einzubeziehen, um Fachwissen bereitzustellen. Das CCo E ist eine lebendige Organisation. Ihre Zusammensetzung, Form und Funktion werden sich wahrscheinlich im Laufe der Zeit ändern, und sie könnte sich zu einem future Zeitpunkt sogar auflösen.
- Wie interagiert die CCo EU mit ihren Interessengruppen?

  Das CCo E steht anderen Teams zur Verfügung und dient lediglich dazu, Informationen zu geben und eine erfolgreiche Cloud-Einführung zu ermöglichen. Schauen Sie sich die Einbettung von Teilen des CCo E in verschiedene Abteilungen, Schulen und Funktionen an. Dies ermöglicht den Zugriff auf ein breiteres Spektrum an Ressourcen und ein schnelleres internes Feedback. Konzentrieren Sie sich frühzeitig auf den Aufbau von Partnerschaften und offene Kommunikationswege zwischen den Interessengruppen, um Vertrauen innerhalb der Institution aufzubauen und organisatorische Silos aufzubrechen. Die EU CCo sollte Mechanismen für die Kommunikation mit Interessengruppen, das Sammeln von Feedback und die Schulung der Nutzer festgelegt haben. Die Erfolgskennzahlen der CCo E sollten diese Zusammenarbeit und

Kommunikation widerspiegeln. Wenn ein Team nur an der Gebäudetechnologie gemessen wird, wird mehr Technologie entwickelt, aber ihr Einsatz und ihre Ergebnisse werden erst im Hintergrund berücksichtigt. Ihre Kennzahlen sollten stattdessen Dinge wie die Anzahl der Teams messen, die durch die Arbeit des CCo E autark werden, wie oft sich das CCo E auf dem kritischen Weg für Initiativen befindet, die Anzahl der abgehaltenen Schulungsveranstaltungen oder die Breite der Akzeptanz der Ergebnisse des CCo E Ein gut aufgebautes, vertrauenswürdiges CCo E kann ein Sprungbrett zu einer umfassenderen Unternehmenstransformation sein, die auf Vertrauen basiert.

- Wie sollten Sie ein E einrichten? CCo

  Die meisten Unternehmen beginnen ihre Cloud-Einführung mit spezifischen, gezielten Pilotprojekten. Richten Sie im Rahmen dieser Projekte ein CCo E ein. Ein guter Start ist entscheidend für den Erfolg der gesamten Reise.

  - Beginnen Sie mit einem Geschäftsproblem. Technologie um der Technologie willen ist eine schlechte Strategie. Wenn Sie mit Cloud-Technologien experimentieren, identifizieren Sie einen überzeugenden Geschäftsanwendungsfall, egal wie klein er auch erscheinen mag. Gehen Sie dann von diesem Anwendungsfall aus und setzen Sie sich klare Ziele, wie Technologie Ihnen helfen kann. Implementieren Sie die Lösung nicht in einem Silo. Lassen Sie sich vor und während der Projektimplementierung ständig Anregungen von Interessengruppen aus dem Unternehmen geben. Alle erfolgreichen Cloud-Projekte sind auf eine enge Zusammenarbeit mit den institutionellen Einheiten angewiesen, die die Technologie nutzen werden.
  - Fangen Sie klein an. Wählen Sie ein Projekt mit geringem Risiko und wechselseitigem Zugang. Das bedeutet, dass das Projekt reversibel ist und etwaige Fehler schnell korrigiert werden können. Bei Pilotprojekten dreht sich alles ums Experimentieren. Durch die Vermeidung großer Projekte mit hohem Risiko haben Sie eine bessere Kontrolle über die Umsetzung und die Ergebnisse. Es hilft, spezifische, definierbare Probleme anzusprechen, anstatt sich auf breit angelegte Ziele zu konzentrieren. Wenn Automatisierung beispielsweise das ultimative Ziel ist, sollten Sie darauf abzielen, bestimmte Aufgaben statt ganzer Jobs zu automatisieren.
  - Definieren und messen Sie das Ergebnis. Legen Sie klare Kennzahlen fest, um den Fortschritt und die Leistung jedes Projekts zu bewerten. Definieren Sie den gewünschten Endzustand rechtzeitig, um widersprüchliche Erwartungen der Beteiligten zu vermeiden. Arbeiten Sie eng mit Geschäftsbeteiligten und anderen Führungskräften innerhalb der Organisation zusammen, um Erwartungen und messbare Gewinne zu definieren. Es ist auch wichtig, die Ergebnisse in eine nichttechnische Sprache zu übersetzen. Sprechen Sie über institutionelle Ziele, z. B. wie das Projekt die Kundenbindung verbessert und die Fluktuation verringert hat, wie es die Kosten senkte und die Geschwindigkeit der Umsetzung erhöhte und so weiter.

- Fangen Sie in der Komfortzone an. Wählen Sie ein Projekt in einem Bereich aus, mit dem Ihre Institution vertraut ist. Auf diese Weise können Sie sicherstellen, dass das Projekt aussagekräftige, verständliche Ziele mit echter Wirkung verfolgt. Ein solches Projekt schafft Vertrauen und führt zu besseren langfristigen Ergebnissen für Ihr Unternehmen. Wenn Sie beispielsweise bereits über Fachwissen im Bereich Datenanalyse verfügen, können Sie Ihre Cloud-Reise in Angriff nehmen und gleichzeitig Ihre vorhandenen Fähigkeiten nutzen, indem Sie mit einem Analyseprojekt beginnen. Jede Institution verfügt über unterschiedliche Fachkenntnisse und muss ihre einzigartigen Komponenten finden, um eine erfolgreiche Strategie für die digitale Transformation zu entwickeln.

Unterscheiden Sie zwischen SaaS-Anwendungen und grundlegenden Cloud-Diensten

Die meisten Bildungseinrichtungen haben bereits Software-as-a-Service (SaaS) -Anwendungen eingeführt. SaaS bietet Ihrer Institution eine Komplettlösung, die vom Dienstanbieter betrieben und verwaltet wird. Zu den gängigen SaaS-Anwendungen gehören Produktivitätsanwendungen wie Textverarbeitung und E-Mail, aber SaaS-Optionen gibt es auch für viele geschäftskritische Workloads wie Enterprise Resource Planning (ERP), Studenteninformationssysteme (SIS) und Lernmanagementsysteme (LMS). Wenn Ihre Institution ein SaaS-Angebot einführt, muss sich Ihr IT-Team keine Gedanken darüber machen, wie der Service gewartet oder die Infrastruktur verwaltet wird — Ihre Benutzer nutzen den Service einfach. Dieses Bereitstellungsmodell reduziert den Verwaltungsaufwand für Ihre IT-Mitarbeiter. Viele Institutionen entscheiden sich für einen „SaaS First“ -Ansatz in ihrer IT-Strategie, insbesondere wenn ihren IT-Teams die Zeit, die Ressourcen oder die Fähigkeiten fehlen, um dieselbe Anwendung ausreichend selbst zu hosten. Selbst wenn Sie über die Ressourcen verfügen, um selbst zu hosten, ist es möglicherweise kostengünstiger, eine SaaS-Lösung einzuführen und stattdessen in andere Projekte zu investieren.

Wenn Sie SaaS-Anwendungen verwenden, muss Ihr IT-Team die zugrunde liegende Infrastruktur nicht verwalten, sodass es weniger wichtig ist, wo der Anbieter die Anwendung hostet (lokales Rechenzentrum, Ihr primärer Cloud-Anbieter oder ein alternativer Cloud-Anbieter). Nachdem Sie sich für einen primären, strategischen Cloud-Anbieter entschieden haben, können Sie sich für ein SaaS-Angebot entscheiden, das bei einem anderen Cloud-Anbieter oder vor Ort im Rechenzentrum des Anbieters gehostet wird. Umgekehrt können Sie, selbst wenn Ihre SaaS-Anwendungen bei einem Cloud-Anbieter gehostet werden, je nach Stärke dieses Anbieters für Ihre Nicht-SaaS-Workloads einen anderen primären, strategischen Cloud-Anbieter wählen. Die Unterscheidung zwischen

Hosting-Umgebungen ist für SaaS weniger wichtig als für selbst gehostete Anwendungen. Sie sollten jedoch dennoch die folgenden wichtigen Fragen berücksichtigen, wenn Sie bewerten, wie SaaS im Rahmen Ihrer IT-Strategie zur Cloud passt.

- Ist die SaaS-Anwendung hochverfügbar und skalierbar?

  Viele Anbieter haben bereits die Entscheidung getroffen, die Cloud für ihre SaaS-Angebote einzusetzen. Auf diese Weise ist der Anbieter in der Lage, die Cloud-Vorteile einer erhöhten Verfügbarkeit und Skalierbarkeit zu nutzen. Da der Anbieter das Modell der gemeinsamen Verantwortung der Cloud übernehmen kann, anstatt die physische Infrastruktur zu verwalten und zu warten, kann er außerdem mehr Zeit und Ressourcen in die Bereitstellung neuer Funktionen investieren. Aufgrund dieser Vorteile sollten Sie Anbieter bevorzugen, die in der Cloud an erster Stelle stehen und in der Cloud gehostete Lösungen anbieten.
- Kann die SaaS-Anwendung Ihre Sicherheitsanforderungen erfüllen?

  Bei der Bewertung von SaaS ist es wichtig zu wissen, welche Daten die Anwendung speichert, wie diese Daten verwendet werden und welche Sicherheitskontrollen zum Schutz dieser Daten vorhanden sind. Auch wenn Sie möglicherweise keine direkte Kontrolle über den Datenspeicher haben, wie Sie es in Ihrer eigenen, selbst gehosteten Umgebung tun würden, sollten Sie sicherstellen, dass der Anbieter über Mechanismen und Kontrollen verfügt, um Ihre Daten angemessen zu handhaben. Beachten Sie, welche Sicherheitsfunktionen in die SaaS-Lösung integriert sind und welche Funktionen eine zusätzliche Konfiguration erfordern. Die Cloud ermöglicht es SaaS-Anbietern, verfügbarere und skalierbarere Lösungen zu entwickeln, und sie können aufgrund des Modells der gemeinsamen Verantwortung auch sicherere Lösungen entwickeln. Sie sollten Anbieter bevorzugen, die Cloud-Sicherheitstools und -dienste als Teil ihrer Lösungen nutzen.
- Wem gehören die SaaS-Anwendungsdaten und wie können Sie darauf zugreifen?

  Wenn Sie SaaS verwenden, vertrauen Sie darauf, dass der Anbieter die Daten Ihrer Institution ordnungsgemäß behandelt. Lesen Sie unbedingt die Nutzungsbedingungen und Service Level Agreements für SaaS-Anwendungen, um zu verstehen, welche Faktoren dazu beitragen, wie Datenbesitz, Verfügbarkeit und Haltbarkeit. Prüfen Sie die Mechanismen für die Sicherung oder den Export Ihrer Daten. Diese sind besonders wichtig, falls Sie den Anbieter wechseln möchten oder der Anbieter den Service einstellt.
- Können Ihre anderen Dienste und selbst gehosteten Anwendungen unabhängig von der Umgebung in die SaaS-Anwendung integriert werden?

Bei der Einführung einer SaaS-Lösung kann leicht davon ausgegangen werden, dass Dienste und Anwendungen, die dieselbe Hosting-Umgebung verwenden (d. h. Anwendungen, die denselben Cloud-Anbieter oder das Rechenzentrum desselben Anbieters verwenden), eine nahtlosere Integration aufweisen. Die meisten SaaS-Lösungen bieten heute jedoch eine breite Unterstützung für API- und Drittanbieter-Integrationen. Beschränken Sie sich also nicht auf Lösungen, die in derselben Umgebung gehostet werden. Wenn die erforderlichen Integrationen vorhanden sind, müssen sich die Lösungen nicht dieselbe zugrunde liegende Umgebung teilen. Nehmen wir zum Beispiel an, Sie verwenden eine SaaS-Lösung wie Google Drive oder Microsoft OneDrive für die Cloud-basierte Speicherung von Studentendateien. Um Ihren Schülern virtuelle Desktops und Anwendungsstreaming zur Verfügung zu stellen, könnten Sie feststellen, dass Amazon AppStream 2.0 am besten zu Ihren Anforderungen passt. Obwohl diese Dienste in unterschiedlichen Umgebungen ausgeführt werden, verfügt AppStream 2.0 über native Integrationen mit Google Drive und Microsoft OneDrive, sodass Ihre Schüler ihren vorhandenen Speicher weiterhin nutzen können.

- Unterstützt die SaaS-Anwendung zentralisiertes Identitätsmanagement?

  Um zu verhindern, dass Ihr IT-Team unterschiedliche Identitätsspeicher verwalten muss und Ihre Benutzer sich nicht mehrere Sätze von Anmeldeinformationen merken müssen, stellen Sie sicher, dass Ihre SaaS-Lösungen die Integration mit Ihren bestehenden Identitätsmanagement- oder Single Sign-On-Lösungen unterstützen. Ein fragmentiertes Identitätsmanagement verringert die Produktivität und kann zu schlechten Sicherheitspraktiken wie der Weitergabe von Zugriffsrechten und schwachen Passwörtern führen. Wenn Ihre gewünschte SaaS-Lösung Single Sign-On oder Ihren vorhandenen Identitätsspeicher nicht unterstützt, sollten Sie prüfen, ob der geschäftliche Nutzen der Einführung der Lösung die erhöhte Belastung für Benutzer und Mitarbeiter überwiegt.
- Wie können Sie die Netzwerkkommunikation mit der SaaS-Anwendung sichern?

  In einigen Fällen benötigen Sie möglicherweise eine selbst gehostete Anwendung, um mit einer SaaS-Anwendung zu kommunizieren. In der Regel erfolgt diese Kommunikation über Systeme APIs , die mit geeigneten Authentifizierungs- und Autorisierungsmechanismen gesichert sind. Je nach Hostumgebung der beiden Anwendungen können jedoch alternative oder zusätzliche Mechanismen erforderlich sein, um die Kommunikation zu vereinfachen oder zu sichern. Wenn Sie beispielsweise eine Anwendung selbst bei einem Cloud-Anbieter hosten und sie in eine SaaS-Anwendung integrieren müssen, die auf demselben Cloud-Anbieter gehostet wird, bietet der Anbieter möglicherweise mehrere Verbindungsoptionen. Möglicherweise können Sie cloudspezifische Peering-Verbindungen, private oder private Schnittstellen verwenden APIs, AWS PrivateLinkum zu verhindern, dass diese Kommunikation das öffentliche Internet durchquert.

Wenn Ihre lokale Anwendung über einen Dienst wie eine dedizierte Netzwerkverbindung zu einem Cloud-Anbieter verfügt AWS Direct Connect, können Sie dieselbe Verbindung auch für die Kommunikation mit SaaS-Anwendungen verwenden, die auf demselben Cloud-Anbieter gehostet werden.

Legen Sie Sicherheits- und Governance-Anforderungen für jeden Cloud-Dienstanbieter fest

Bildungseinrichtungen haben eine Vielzahl von Zielen in den Bereichen Compliance, Unternehmensführung und Cybersicherheit, die sie erreichen müssen. Zu den Risiken der Nichterfüllung dieser Ziele zählen der Verlust des Ansehens von Institutionen, Geldbußen, Lösegeld, Verletzungen vertraulicher Daten, Diebstahl geistigen Eigentums und der eingeschränkte oder vollständige Verlust geschäftskritischer Funktionen. Aufgrund des Modells der gemeinsamen Verantwortung können Institutionen, die Cloud-Dienste einsetzen, den Verwaltungsaufwand reduzieren, indem sie einen Teil der Verantwortung für die Infrastruktursicherheit auf den Cloud-Dienstanbieter übertragen. Darüber hinaus können Sie von speziell entwickelten, Cloud-nativen Sicherheitsdiensten profitieren, die Funktionen bieten, die bei einer lokalen Bereitstellung oft nicht verfügbar, schwer zu verwalten oder zu teuer sind. Beispiele hierfür sind Dienste wie AWS WAFzum Schutz von Webanwendungen, AWS Shieldzum Schutz vor verteilten Denial-of-Service (DDoS) und Amazon GuardDuty zur Bedrohungserkennung. Eine erfolgreiche Cloud-Sicherheits- und Governance-Strategie ermöglicht es IT- und Sicherheitsteams, sich auf die Entwicklung von Systemen zu konzentrieren, die von Haus aus sicher sind, hilft der Institution, sich schnell an die sich ändernden Aufgabenanforderungen anzupassen, und bietet Dozenten und Forschern sichere Umgebungen für bahnbrechendes Lernen und Innovation. Berücksichtigen Sie bei der Bewertung Ihrer Sicherheits- und Governance-Anforderungen die folgenden zentralen Fragen.

- An welchen Compliance-Frameworks müssen Ihre Workloads ausgerichtet sein?

  Bildungseinrichtungen müssen sich aufgrund der Vielzahl von Stakeholdern und Arbeitsbelastungen, die sie unterstützen, an viele Compliance-Rahmenbedingungen halten. Zu diesen Compliance-Rahmenbedingungen gehören der Family Educational Rights and Privacy Act (FERPA), der Health Insurance Portability and Accountability Act (HIPAA), das Federal Risk and Authorization Management Program (FedRAMP), die Cybersecurity Maturity Model Certification (CMMC), die International Traffic in Arms Regulations (ITAR), die Criminal Justice Information Services (CJIS) und der Payment Card Industry Data Security Standard (PCI DSS). In einigen Fällen, wie z. B. bei CMMC, werden Forschungsstipendien erst freigegeben, wenn

die entsprechenden Workloads als konform zertifiziert sind. Jedes Framework ist einzigartig und gilt möglicherweise nur für eine Teilmenge von Workloads. Stellen Sie sicher, dass Sie wissen, welche Workloads welchen Anforderungen entsprechen müssen, und dass Sie in der Lage sind, diese Anforderungen in der jeweiligen Workload-Umgebung zu erfüllen. Stellen Sie in Cloud-Umgebungen sicher, dass Sie Ihre Verantwortlichkeiten im Vergleich zu den Verantwortlichkeiten des Cloud-Anbieters verstehen. Sie sollten über das Wissen, die Ressourcen und die Fähigkeiten verfügen, die erforderlich sind, um die Einhaltung der Vorschriften zu erreichen und aufrechtzuerhalten.

- Welche Mechanismen haben Sie eingerichtet, um die Einhaltung der Vorschriften bei mehreren Cloud-Anbietern durchzusetzen, ohne Innovationen zu behindern?

  Wenn Ihre akademische Einrichtung noch nicht mit der Cloud vertraut ist, empfehlen wir Ihnen, einen primären strategischen Cloud-Dienstanbieter auszuwählen und sich darauf zu konzentrieren, zu verstehen, wie Cloud-Umgebungen konzipiert, entwickelt und betrieben werden, die von Haus aus sicher sind. Im Idealfall ermöglichen Sicherheitskontrollen, die automatisch in Self-Service-Systeme integriert werden, Benutzern die schnelle Bereitstellung sicherer Cloud-Umgebungen mit minimalem Aufwand durch IT-Teams. Die Konzentration auf einen einzigen Anbieter begrenzt die Menge an Ressourcen und Zeit, die Sie investieren müssen, um Sicherheit und Compliance zu gewährleisten. Die erfolgreichsten Institutionen entscheiden sich für einen Cloud-Dienstanbieter, der die meisten Compliance-Anforderungen erfüllen kann, über ein robustes Partnernetzwerk verfügt, vorgefertigte Compliance-Lösungen anbietet und sichere Self-Service-Automatisierung zur Verfügung stellt. Wenn Sie Sicherheit und Compliance bei mehreren Cloud-Anbietern sicherstellen müssen, sind zusätzliche Investitionen erforderlich, um die Fähigkeiten und Ressourcen aufzubauen, um die Einhaltung der Vorschriften für jede Umgebung zu gewährleisten. Wenn jeder Cloud-Anbieter eine andere grundlegende Umgebung oder landing zone verwendet, müssen Sie wissen, welche Compliance-Standards und Anforderungen jede landing zone unterstützen kann. Dies kann bestimmen, ob bestimmte Workloads bei diesem Anbieter gehostet werden können. Sie können die Einhaltung der Vorschriften für jeden Anbieter separat verwalten oder maßgeschneiderte Lösungen oder Partnerlösungen verwenden, mit denen die Verwaltung anbieterübergreifend zentralisiert werden kann. AWS Marketplacebietet schlüsselfertige Lösungen, die auch Ihre Compliance-Anforderungen erfüllen können.
- Wie können Sie Kosten und Nutzung bei mehreren Cloud-Anbietern bewerten und kontrollieren?

  Wenn Ihre akademische Einrichtung noch nicht mit der Cloud vertraut ist, empfehlen wir Ihnen, Mechanismen zur Kostentransparenz und -kontrolle einzurichten, um zu erfahren, welche Cloud-Dienste genutzt werden, wem die Cloud-Ressourcen gehören, welchem Zweck diese Cloud-

Ressourcen dienen und welche potenziellen Kosteneinsparungen durch eine Optimierung der Nutzung erzielt werden können. Institutionen können eine erhebliche Investitionsrendite erzielen, wenn sie bei der Migration und Modernisierung unternehmenskritischer Systeme mit ihrem Cloud-Dienstanbieter zusammenarbeiten, da sie Verträge auf Unternehmensebene aushandeln, von Volumenpreisen profitieren und das Fachwissen des Cloud-Dienstanbieters nutzen können. Wenn Sie Kosten und Nutzung bei mehreren Anbietern kontrollieren müssen, sollten Sie überlegen, wie Sie die Kosten und Nutzung der einzelnen Anbieter aggregieren und analysieren können, entweder mit internen Prozessen und Tools oder mithilfe von Partnerlösungen. Viele Unternehmen beginnen, Cloud-Finanzoperationen (FinOps) als Schlüsselfunktion zu identifizieren und Ressourcen für die Verbreitung und Implementierung von Funktionen für Cloud-Kostenmanagement und -optimierung bereitzustellen.

- Verfügen Sie über Mechanismen, mit denen Sie Benutzerberechtigungen im Laufe der Zeit einfach verwalten können?

  Wir empfehlen akademischen Einrichtungen, die wichtigsten Bedürfnisse der Interessengruppen zu verstehen, wenn sie sich zum ersten Mal der Cloud nähern. Zu den Nutzern institutioneller Systeme gehören Studierende, Dozenten, Forscher, IT-Mitarbeiter, Verwaltung, Sicherheit, die breite Öffentlichkeit und externe Mitarbeiter. Sie sollten die Kernbedürfnisse dieser Benutzer ermitteln und sicherstellen, dass Sie über geeignete Mechanismen verfügen, um ihnen Zugriff auf Cloud-Dienste zu gewähren. Verschiedene Benutzertypen benötigen unterschiedliche Arten des Zugriffs auf Cloud-Dienste. Studierende, Dozenten und die breite Öffentlichkeit benötigen beispielsweise Zugriff auf Anwendungen; IT-Mitarbeiter, Administratoren und Sicherheitsdienste benötigen Zugriff auf die Cloud-Infrastruktur; Forscher und ihre externen Mitarbeiter benötigen Zugang zu sicheren Forschungsumgebungen; Fakultäten benötigen Zugang zu sicheren Lehrumgebungen und möchten Studenten vielleicht sogar einen praktischen Zugang zu Cloud-Technologien bieten. Sie sollten über Tools verfügen, um diese Identitäten zentral und automatisiert zu verwalten und etablierte Prozesse zu verwenden, um Berechtigungen zu identifizieren, zu erteilen und zu widerrufen, wenn sich Rollen und Verantwortlichkeiten im Laufe der Zeit ändern.
- Verfügen Sie über Mechanismen, um neue Systeme angemessen in Ihre Identitätsmanagementlösung zu integrieren?

  Wir empfehlen akademischen Einrichtungen, die Integration neuer Systeme in ihre Identitätsmanagementsysteme zu vereinfachen. Dies gibt der Institution die Flexibilität, eine Vielzahl von geschäftskritischen Funktionen zu unterstützen, indem es den Interessengruppen ermöglicht wird, Systeme zu beschaffen und zu entwickeln, die einfach

in das Identitätsmanagementsystem integriert werden können. Durch die Vereinfachung des Integrationsprozesses wird es weniger wahrscheinlich sein, dass die Beteiligten ihre eigenen Zugriffskontrollmaßnahmen anwenden, wodurch bewährte Sicherheitsverfahren wie Single Sign-On, Hauptschlüssel und Multi-Faktor-Authentifizierung (MFA) möglicherweise nicht durchgesetzt werden. Stellen Sie sicher, dass Ihr Identitätsmanagementsystem mithilfe systemeigener Integrationen oder branchenüblicher Protokolle mit den erforderlichen Systemen zusammenarbeiten kann.

- Verfügen Sie über Mechanismen, die eine effektive Erkennung und Reaktion auf Vorfälle ermöglichen?

  Bildungseinrichtungen sind häufig das Ziel von Cyberangriffen und Ransomware. Um solche Vorfälle zu erkennen und effektiv darauf zu reagieren, empfehlen wir einen zweigeteilten Ansatz:

  - Konzentrieren Sie Ihre Bemühungen auf präventive Maßnahmen in Form von Sicherheitskontrollen, die automatisch in Cloud-Umgebungen integriert werden.
  - Implementieren Sie Erkennungsfunktionen, mit denen Einsatzkräfte bei Cybervorfällen Sicherheitsverletzungen rechtzeitig erkennen, eindämmen und abmildern können.

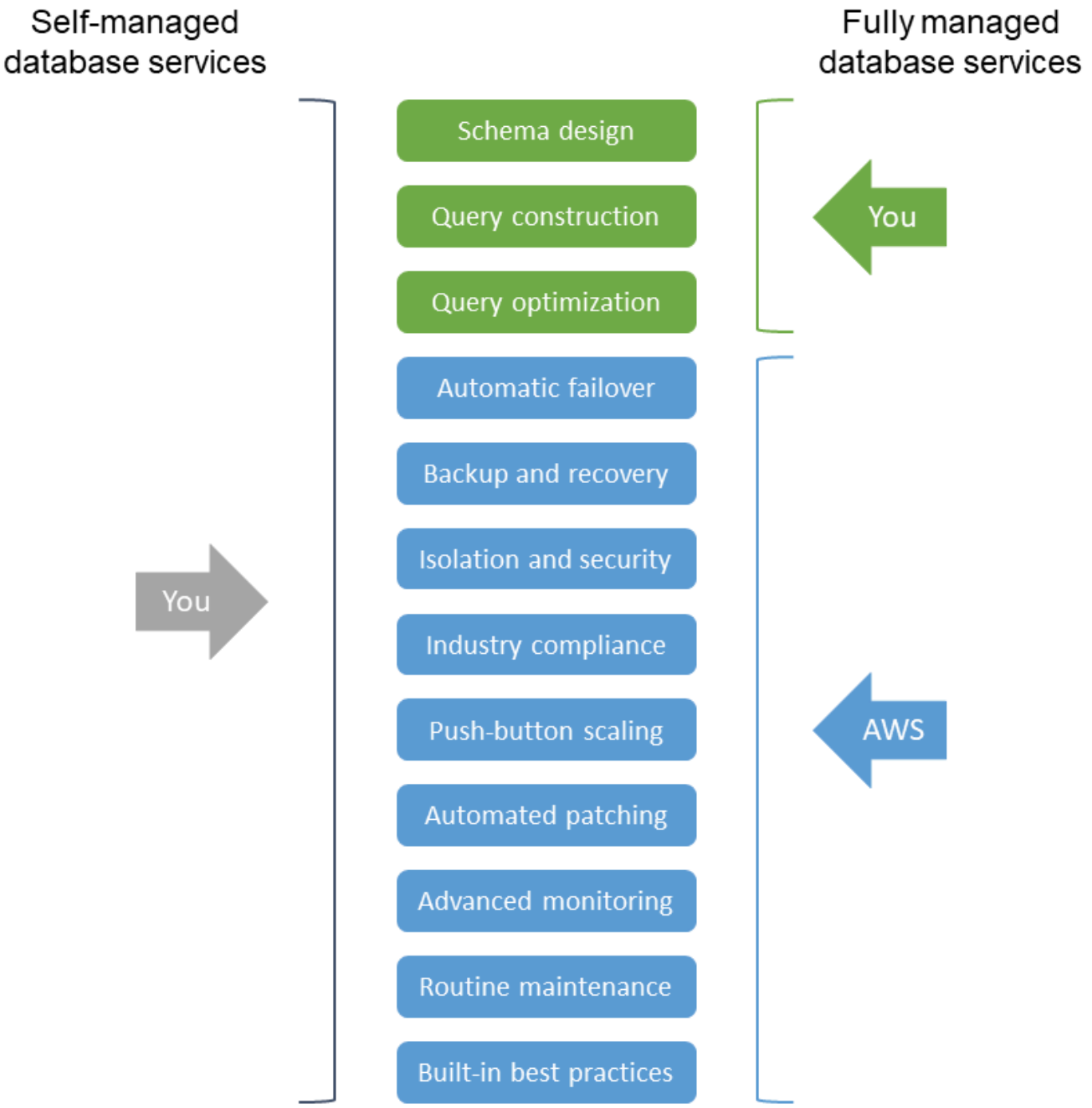
Wie bei der Einhaltung von Vorschriften müssen Sie sicherstellen, dass Sie über die Ressourcen, Fähigkeiten und Tools verfügen, um Ereignisse in jeder Umgebung zu erkennen, zu verhindern und darauf zu reagieren. Indem Sie sich auf einen einzigen, primären Cloud-Anbieter konzentrieren, können Sie die benötigten Ressourcen einschränken. Akademische Einrichtungen, die nicht über ein ausgereiftes Sicherheitsteam verfügen, sollten sich in diesen Bereichen an unabhängige Softwareanbieter, Anbieter von Managed Detection and Response und Cybersicherheitsberater wenden.

Setzen Sie Cloud-native, verwaltete Dienste ein, wo immer dies möglich und praktikabel ist

Wenn Sie zunächst überlegen, wie Sie die Vorteile von Cloud-Diensten nutzen können, scheint die Verwendung von Infrastrukturdiensten und Entwicklungstools, mit denen Ihre Teams vertraut sind, möglicherweise der beste Weg in die Zukunft zu sein. Die Auswahl cloudnativer verwalteter Dienste, insbesondere serverloser Optionen, kann jedoch Kosten, Aufwand und Komplexität erheblich reduzieren.

Cloud-native, verwaltete Services machen viele der undifferenzierten IT-Aufgaben überflüssig, die von Ihren Mitarbeitern Zeit und Mühe erfordern, die besser für geschäftsorientierte

Aktivitäten aufgewendet werden könnten. Wenn die Anbieter die Funktionen ihrer Services verbessern, profitieren Ihre Lösungen zudem von selbst von selbst von selbst von inkrementellen Verbesserungen in Bezug auf Effizienz, Sicherheit, Belastbarkeit, Leistung und andere Merkmale. Ein vollständig verwalteter Datenbankdienst ist beispielsweise ein relationales Datenbankverwaltungssystem mit vielen Funktionen, aber Sie müssen den zugrunde liegenden Server und das Betriebssystem, auf dem die Datenbank läuft, nicht bereitstellen und verwalten. Dadurch entfallen Verwaltungsaufgaben, die normalerweise erforderlich sind, wenn Sie eine relationale Datenbank in Ihrem eigenen Rechenzentrum oder auf einem selbst verwalteten virtuellen Server verwalten, den Sie in der Cloud bereitstellen. Das folgende Diagramm verdeutlicht diesen Unterschied.



Die Vorteile des Wegfalls der Infrastrukturverwaltung liegen auf der Hand, wenn Sie einen Cloud-nativen verwalteten Service mit einem vergleichbaren selbstverwalteten Ansatz vergleichen. Daher sollten Sie immer dann, wenn Sie Komponenten bereitstellen müssen, auf denen Ihre gekauften oder individuell entwickelten Anwendungen laufen, cloudnative, verwaltete Dienste verwenden, um Zeit und Aufwand zu reduzieren.

Wenn Ihr Team für die Entwicklung, Bereitstellung oder Verwaltung von Lösungen in der Cloud verantwortlich ist, nutzen Sie cloudnative, verwaltete Dienste, um die vielfältigen Funktionen und Innovationen Ihres Cloud-Anbieters voll auszuschöpfen. Diese Strategie ermöglicht es Ihnen, Cloud-Dienste so auszuwählen, zu integrieren und bereitzustellen, dass der Zeit- und Arbeitsaufwand für diese Projekte reduziert und gleichzeitig ihre Widerstandsfähigkeit und Sicherheit erhöht wird. Für eine erfolgreiche Cloud-Strategie sollten Sie erwägen, diese cloudnativen Bausteine zu übernehmen, wenn Sie benutzerdefinierte Lösungen in die Cloud migrieren, neue Lösungen in der Cloud entwickeln oder lizenzierte Software in der Cloud bereitstellen. Bei der Bewertung der Optionen für cloudnative, verwaltete Dienste sollten Sie die folgenden wichtigen Fragen berücksichtigen.

- Müssen Sie mehr Zeit und Mühe Ihrer Mitarbeiter auf Funktionen konzentrieren, die im Mittelpunkt Ihres Bildungsauftrags stehen?

  Die Verwaltung von Servern, auch virtueller Server, erfordert Zeit und Aufmerksamkeit, um sicherzustellen, dass sie mit Systemsoftware-Upgrades und Patches immer auf dem neuesten Stand sind. Durch den Einsatz von Managed Services, die diese Aufgaben für Sie übernehmen, können Sie die Zeit Ihrer IT-Mitarbeiter auf Aktivitäten konzentrieren, die sich besser an der Mission Ihrer Institution orientieren. Wenn Sie beispielsweise Container bereitstellen müssen, sollten Sie einen serverlosen, verwalteten Dienst in Betracht ziehen, AWS Fargatesodass Sie keine Server konfigurieren und warten müssen. Da die Beschaffung, Bereitstellung und Verwaltung der zugrunde liegenden Infrastruktur entfällt, können Sie sich stattdessen auf die Bereitstellung neuer Funktionen, die Optimierung der Leistung und die Verbesserung der Benutzererfahrung konzentrieren. Berücksichtigen Sie diesen Vorteil, wenn Sie verwaltete Dienste im Vergleich zu selbstverwalteten Optionen abwägen.
- Welchen Aufwand wird Ihr Team benötigen, um Cloud-native Managed Services einzuführen?

  Das Entwerfen und Implementieren von Lösungen mit cloudnativen, verwalteten Diensten kann eine Lernkurve mit sich bringen, aber diese Anstrengungen werden sich mit einer Verringerung der Kosten, des Zeitaufwands und der Komplexität während der gesamten Lebensdauer einer Lösung auszahlen. Aufgrund des pay-as-you-go On-Demand-Charakters von Cloud Computing ermöglichen Ihnen Cloud-native Services eine schnelle Iteration und flexiblere Experimentierbarkeit, ohne dass Vorabinvestitionen getätigt werden müssen. Dies führt zu mehr Innovation und kürzeren Projektzeitplänen. Um diese Vorteile effektiv nutzen zu können, sollten Sie jedoch überlegen, was für die Einführung und Nutzung des Dienstes erforderlich sein könnte, z. B. Schulungen der Mitarbeiter zu optimalen Nutzungsmustern und Code-Refactoring, um dienstspezifischen Anforderungen gerecht zu werden. APIs Selbst wenn der Service Industriestandards oder Open Source verwendet APIs, müssen Sie Ihre Anwendung

möglicherweise umgestalten oder konfigurieren, um Funktionsunterschiede oder Versionskonflikte zu beheben.

- Wie implementieren und verwalten Sie derzeit die Infrastruktur? Müssen Sie dieses Maß an Kontrolle aufrechterhalten?

  Es gibt eine Vielzahl von Möglichkeiten, die Infrastruktur in der Cloud zu hosten und zu verwalten, einschließlich der Verwendung von Bare-Metal-Hosts, virtuellen Maschinen, verwalteten Containerdiensten und serverlosen Angeboten. Auch wenn Sie derzeit eine ähnliche Infrastruktur wie virtuelle Maschinen oder Container in Ihrer lokalen Umgebung verwenden, sollten Sie in Betracht ziehen, ob ein alternativer Ansatz für bestimmte Workloads geeignet wäre. Anstatt beispielsweise alle Anwendungen auf virtuellen Maschinen auszuführen, sollten Sie erwägen, Ihre Anwendungen zu containerisieren und verwaltete Container-Services wie Amazon Elastic Container Service (Amazon ECS) zu nutzen. Dies erfordert möglicherweise ein Refactoring, aber Sie können ein Tool verwenden, um die Containerisierung AWS App2Containerzu vereinfachen und zu unterstützen. Gehen Sie noch einen Schritt weiter: Anstatt Server oder Container für alle Komponenten bereitzustellen, sollten Sie vollständig serverlose Optionen in Betracht ziehen. Serverlose Technologien zeichnen sich durch automatische Skalierung, integrierte Hochverfügbarkeit und ein pay-for-use Abrechnungsmodell aus, um die Flexibilität zu erhöhen und die Kosten zu optimieren. Gleichzeitig machen sie die Verwaltung von Servern und die Kapazitätsplanung überflüssig. Serverlose Computerdienste, wie sie zum Kern serverloser Architekturen AWS Lambdagehören. Lambda unterstützt gängige Programmiersprachen und ermöglicht es Entwicklern, sich auf den Anwendungscode zu konzentrieren, anstatt die Infrastruktur zu verwalten. Erkunden Sie diese Optionen für jeden Workload und berücksichtigen Sie Faktoren wie Lernkurve, Verwaltungsaufwand, Kosten und Lizenzierung.
- Müssen Sie die Infrastruktur für lizenzierte Software bereitstellen und verwalten?

  Wenn Sie lizenzierte Software von unabhängigen Softwareanbietern (ISVs) bereitstellen und verwalten, mag es logisch erscheinen, Ihre lokale Bereitstellung mit Cloud-Infrastruktur nachzuahmen. Sie könnten beispielsweise erwägen, lokale virtuelle Maschinen durch in der Cloud gehostete virtuelle Maschinen zu ersetzen. Obwohl dies eine praktikable Option ist, sollten Sie sich überlegen, ob Sie Komponenten der Architektur durch cloudnative, verwaltete Dienste ersetzen können. Beispielsweise könnten Sie einen selbstverwalteten Datenbankserver durch einen vollständig verwalteten Datenbankdienst ersetzen, der den Verwaltungsaufwand reduziert, während dieselbe Datenbank-Engine ausgeführt wird. Viele verwenden ISVs bereits Cloud-Architekturen, die die Vorteile von Managed Services nutzen, und bieten möglicherweise sogar vorgefertigte Vorlagen, um die Bereitstellung zu vereinfachen. Wenn möglich, sollten Sie

es vorziehen, ISVs dass präskriptive Anleitungen und Support für Cloud-Implementierungen angeboten werden. Bevor Sie lizenzierte Software in der Cloud bereitstellen, sollten Sie sich unbedingt an Ihren ISV wenden, um zu erfahren, wie sich die Lizenzierung für Cloud-Umgebungen von der lokalen Lizenzierung unterscheiden kann.

- Befürchten Sie, dass die Nutzung eines verwalteten Dienstes zu einer Anbieterbindung führen könnte?

  Viele Cloud-native, verwaltete Dienste sind so konzipiert, dass sie gängige Industriestandards unterstützen und. APIs Beispielsweise basieren Analysedienste wie Amazon EMR auf branchenüblichen Verarbeitungs AWS Glue- und Speicher-Frameworks wie Apache Spark und Apache Parquet. AWS Lambdaunterstützt nativ Java-, Go-, Microsoft- PowerShell, Node.js-, C#-, Python- und Ruby-Code. Amazon Relational Database Service (Amazon RDS) unterstützt mehrere Versionen gängiger Datenbank-Engines, darunter SQL Server, Oracle, PostgreSQL und MySQL. Wenn Dienste über eigene APIs, native Lösungen oder Partnerlösungen verfügen, stehen möglicherweise Lösungen zur Verfügung, mit denen über gängige, Cloud-unabhängige APIs Protokolle interagiert werden kann. Amazon Simple Storage Service (Amazon S3) verfügt beispielsweise über eine servicespezifische API für die direkte Integration, aber Sie können mit ihr auch interagieren, indem Sie Standardspeicherprotokolle wie Network File System (NFS), Server Message Block (SMB) und Internet Small Computer Systems Interface (iSCSI) verwenden, wenn Sie sie verwenden. AWS Storage Gateway Sie sollten sich weiterhin darauf konzentrieren, den Cloud-nativen, verwalteten Service auszuwählen, der Ihren Anforderungen am besten entspricht und gleichzeitig den Betriebsaufwand weitestgehend reduziert. Möglicherweise bevorzugen Sie jedoch Dienste, die gängige Industriestandards und -protokolle verwenden oder verfügbar machen.

Implementieren Sie Hybridarchitekturen, wenn bestehende Investitionen vor Ort Anreize für eine weitere Nutzung bieten

Die meisten Bildungseinrichtungen haben in lokale Rechenzentren unterschiedlicher Größe investiert, um Unternehmensanwendungen, Datenspeicherlösungen, Endbenutzer-Computerumgebungen (EUC) und gemeinsam genutzte Computerressourcen zu hosten. Alle Ressourcen in diesen Rechenzentren unterliegen unterschiedlichen Aktualisierungszyklen, bei denen Sie future Wachstum berücksichtigen und ausreichend Kapazität bereitstellen müssen, um Spitzenlasten zu bewältigen, die möglicherweise nur ein paar Mal pro Jahr erforderlich sind. Daher bleiben Ressourcen oft bis zum nächsten Aktualisierungszyklus ungenutzt. Die Planung, Budgetierung, Beschaffung und

Bereitstellung neuer Hardware kann Wochen, wenn nicht Monate oder länger dauern. Dieser langwierige Prozess behindert Innovationen und kann Lernen und Forschen verzögern.

Cloud Computing löst viele dieser Herausforderungen. Die Cloud stellt pay-as-you-go IT-Ressourcen auf Abruf bereit, sodass Sie die aktuelle Kapazität besser an den tatsächlichen Bedarf anpassen können, ohne große Vorabplanungen und Investitionen vornehmen zu müssen. Wenn Sie jedoch bereits erhebliche Investitionen in Hardware und Ressourcen vor Ort getätigt haben, sollten Sie versuchen, diese Ressourcen effizient zu nutzen und sie bei Bedarf mit Cloud-Technologie in einem Hybridmodell zu erweitern.

Eine erfolgreiche Hybrid-Cloud-Strategie nutzt die Vorteile vorhandener Investitionen und bietet gleichzeitig eine höhere Agilität, Skalierbarkeit und Zuverlässigkeit, als diese Investitionen allein unterstützen können. Die folgenden Überlegungen können Ihnen den Einstieg erleichtern.

- Wenn Sie einen neuen Workload hosten müssen, denken Sie zuerst an die Cloud?

  Wie Sie die öffentliche und private Cloud-Infrastruktur zusammen nutzen, definiert Ihre Hybrid-Cloud-Strategie. Ein Cloud-First-Ansatz bedeutet nicht, dass die Cloud die bessere Wahl für all Ihre Workloads ist. Wenn Sie jedoch neue Workloads planen, sollten Sie die Cloud als erste Option in Betracht ziehen, insbesondere für Workloads, die neue Technologien erfordern oder die vor Ort verfügbare Speicher- und Rechenkapazität überschreiten. Workloads mit vorübergehenden, inkonsistenten Nutzungsmustern, die schnelle Ergebnisse erfordern, leicht portierbar sind oder die neueste Hardware erfordern, sind ideale Kandidaten für die Skalierbarkeit und Elastizität der Cloud. Überlegen Sie auch, ob die Arbeitslast von Cloud-nativen, verwalteten Diensten profitieren würde, die vor Ort nicht verfügbar sind, auch wenn Sie über verfügbare Kapazitäten verfügen.
- Kennen Sie die Gesamtbetriebskosten Ihrer lokalen Umgebung und arbeiten Sie bei Neuinvestitionen mit Ihrem CFO zusammen?

  Wir empfehlen Ihnen, sich mit den tatsächlichen Gesamtbetriebskosten (TCO) der Wartung Ihres eigenen lokalen Rechenzentrums vertraut zu machen. Mit dem Besitz und Betrieb der Infrastruktur vor Ort sind viele versteckte Kosten verbunden, darunter nicht nur Hardware, Software und Support, sondern auch Einrichtungen, Nebenkosten, Versicherungen und Personalstunden. Diese Kosten können sich negativ auf die Produktivität der Mitarbeiter, die betriebliche Belastbarkeit und die geschäftliche Flexibilität auswirken. Prüfen Sie auch Ihre aktuellen Lizenzstrukturen und deren Verlängerungs- und Wartungszeiträume. Eine Partnerschaft mit Ihrem Finanzvorstand (CFO) kann Ihnen helfen, alle versteckten Kosten zu identifizieren, wenn Sie neue Investitionen tätigen möchten. Einige Lizenzen bieten möglicherweise BYOL-Optionen (Bring Your Own License) in der Cloud an, oder sie eignen sich möglicherweise mehr oder weniger für Cloud-Dienste. Wenn Sie die

tatsächlichen Gesamtbetriebskosten Ihrer aktuellen Infrastruktur kennen, können Sie die Cloud-Einführung für Workloads priorisieren, die den größten Einfluss auf die Gesamtbetriebskosten Ihres Unternehmens haben. Ihrem AWS Account-Team stehen sofort Tools zur Verfügung, mit denen Sie Ihre lokalen Gesamtbetriebskosten besser verstehen können.

- Welche Infrastruktur benötigen Sie, um hybride Bereitstellungen zu unterstützen?

  Um Hybridmodelle erfolgreich einzuführen, benötigen Sie grundlegende Netzwerk-, Sicherheits- und Infrastrukturtools. Stellen Sie sicher, dass Sie eine angemessene Netzwerkkonnektivität mit Ihrem Cloud-Anbieter aufrechterhalten können. Dies könnte durch eine Kombination aus vorhandener Internetverbindung, virtuellen privaten Netzwerken (VPNs), dedizierten Verbindungen wie AWS Direct Connect Konnektivitätsanbietern von Drittanbietern oder Internet2 - und regionalen Forschungs- und Bildungsnetzwerken geschehen. Stellen Sie sicher, dass Sie in Ihren lokalen und Cloud-Umgebungen über ein einheitliches Identitäts- und Zugriffsmanagement verfügen. Richten Sie Tools und Prozesse ein, um einheitliche Sicherheits-, Kosten- und Nutzungsrichtlinien durchzusetzen.

- Sind Ihre IT-Mitarbeiter bereit, hybride Implementierungen zu betreiben?

  Cloud-Dienste können spezifische Fähigkeiten erfordern, über die Ihr Team möglicherweise nicht verfügt. Um den Schulungs- und Schulungsaufwand zu begrenzen, der zur Weiterbildung Ihrer IT-Mitarbeiter für eine effektive Cloud-Einführung erforderlich ist, sollten Sie überlegen, ob der Cloud-Anbieter Dienste anbietet, die vorhandene Fähigkeiten vor Ort und in der Cloud wiederverwenden und darauf aufbauen. Wenn Sie beispielsweise Kubernetes verwenden und damit vertraut sind, könnten Sie die Verwendung von Amazon Elastic Kubernetes Service (Amazon EKS) oder Amazon EKS Anywhere in Betracht ziehen. Wenn Sie Amazon verwenden und damit vertraut sind NetApp, sollten Sie die Verwendung von Amazon FSx for NetApp ONTAP in Betracht ziehen. Denken Sie auch darüber nach, ob bestehende Partnerlösungen, die Sie verwenden, native Integrationen bieten oder Cloud-Umgebungen unterstützen.

- Können Sie Langzeitspeicher oder Rechenleistung mit geringer Auslastung von lokalen Standorten in die Cloud verlagern?

  Cloud-Speicher bietet mehrere kostengünstige Optionen für die langfristige Datenspeicherung. Amazon Simple Storage Service (Amazon S3) bietet beispielsweise verschiedene Speicherstufen, die für unterschiedliche Anwendungsfälle optimiert sind. Wenn Ihre Institution bestimmte Daten über einen längeren Zeitraum aufbewahren muss, sollten Sie Kühlspeicherlösungen wie Amazon S3 Glacier in Betracht ziehen. Durch das Auslagern dieser Daten in den Cloud-Speicher kann wertvoller Hochleistungsspeicher vor Ort freigesetzt werden. Dienste wie AWS

Storage Gatewayerleichtern lokalen Anwendungen den Zugriff auf Cloud-Speicherebenen über Standardprotokolle wie SMB, NFS und iSCSI. Erwägen Sie auch, alle Rechenaufgaben auszulagern, die selten oder wenig genutzt werden. Wenn Sie lokale Server haben, die für solche Aufgaben vorgesehen sind, können Sie stattdessen skalierbare Cloud-Rechendienste verwenden, bei denen Ressourcen nach Bedarf bereitgestellt werden und Sie nur für das bezahlen, was Sie tatsächlich nutzen. Diese kostengünstigen, langfristigen Speicher- und Rechenoptionen mit geringer Auslastung machen die Cloud auch ideal für Backup und Disaster Recovery. Sie können sicheren, dauerhaften und skalierbaren Speicher und Rechenleistung in der Cloud verwenden, um Ihre Daten zu schützen und im Notfall schnell wiederherzustellen, ohne die erforderliche Speicher- und Recheninfrastruktur selbst verwalten zu müssen.

- Verfügen Sie vor Ort über genügend Kapazitäten, um zu experimentieren und Innovationen zu entwickeln?

  Der Mangel an Elastizität und Agilität in lokalen Umgebungen mit fester Größe kann die Dienste und Technologien einschränken, die Ihren Benutzern zur Verfügung stehen. Wenn Sie strenge Aktualisierungszyklen haben, müssen neue Workloads möglicherweise bis zum nächsten Zyklus mit der Implementierung warten. Dieses Betriebsmodell kann Experimente einschränken und Innovationen verlangsamen. Wenn Sie einen neuen oder neuartigen Workload haben, der getestet werden muss, sollten Sie die Verwendung skalierbarer, elastischer Cloud-Services in Betracht ziehen. Cloud-Ressourcen können bei Bedarf bereitgestellt und deprovisioniert werden, und Sie zahlen nur für das, was Sie tatsächlich nutzen. So können Sie schnell experimentieren und scheitern und gleichzeitig das Unternehmensrisiko minimieren.
- Haben Sie spezielle Compliance- oder Leistungsanforderungen, die Sie dazu zwingen, Daten vor Ort aufzubewahren?

  Workloads mit strengen Anforderungen an die Datenresidenz oder Latenz erfordern möglicherweise, dass Sie Daten lokal oder so nah wie möglich an Ihren Benutzern speichern. Für diese Anwendungsfälle können Sie der Verwendung vorhandener, lokaler Ressourcen Priorität einräumen. Überlegen Sie jedoch, ob Ihr Cloud-Anbieter Edge-Services oder Mechanismen zur Nutzung von Cloud-basierter Technologie vor Ort anbietet. Edge-Services bieten Datenverarbeitung, Analyse und Speicherung näher an Ihren eigenen Endpunkten und ermöglichen Ihnen die Bereitstellung von Tools außerhalb der Rechenzentren von Standard-Cloud-Anbietern. AWS bietet beispielsweise Services wie AWS Local Zones und AWS Wavelengthdie Bereitstellung von Anwendungen an bestimmten Standorten in der Nähe der Endbenutzer. Mit Diensten wie Amazon ECS Anywhere und Amazon EKS Anywhere können Sie auch Cloud-

Services und -Funktionen in Ihr bestehendes Rechenzentrum integrieren. AWS OutpostsAWS Storage Gateway

Reservieren Sie Multicloud nur für Workloads, die ihre technischen oder geschäftlichen Anforderungen nicht über einen einzigen Cloud-Anbieter erfüllen können

Multicloud bezieht sich auf die Nutzung von Cloud-Diensten von mehreren (zwei oder mehr) Cloud-Dienstanbietern. Eine Multicloud-Strategie kann bestimmte Vorteile bieten, z. B. die Möglichkeit, die unterschiedlichen Fähigkeiten mehrerer Cloud-Anbieter zu nutzen, oder die Fähigkeit, Anforderungen an die Datenhoheit zu erfüllen, die ein einzelner Cloud-Anbieter möglicherweise nicht erfüllen kann. Stellen Sie jedoch für jeden Anbieter, den Sie nutzen, sicher, dass Sie über die richtigen Mitarbeiter, Fähigkeiten, Schulungen und Tools verfügen, um diesen Anbieter effektiv nutzen zu können. Wenn Sie eine Multicloud-Strategie für einen bestimmten Workload verwenden möchten, benötigen Sie außerdem zusätzliche Ressourcen, um die erforderlichen Dienste der einzelnen Cloud-Anbieter zu integrieren und miteinander zu verbinden. Wir empfehlen, Multicloud nur dann in Betracht zu ziehen, wenn die Vorteile die höheren Investitionen überwiegen. Um zu entscheiden, ob Sie sich für eine Multicloud-Strategie entscheiden sollten, sollten Sie sich die folgenden wichtigen Fragen stellen.

- Verfügen Sie über die Ressourcen und Fähigkeiten, um sich in den von verschiedenen Cloud-Anbietern angebotenen Diensten zurechtzufinden?

  Wenn mehrere Cloud-Anbieter verschiedene Produkte und Dienste anbieten, benötigen Ihre Mitarbeiter grundlegende Fähigkeiten, um sich mit den Fähigkeiten der einzelnen Anbieter vertraut zu machen. Die alleinige Nutzung der Dienste eines Cloud-Anbieters kann je nach den Diensten und Funktionen, die Sie nutzen, eine Weiterbildung und Schulung Ihrer Mitarbeiter erfordern. Wenn Sie eine Multi-Cloud-Strategie in Betracht ziehen, bewerten Sie Ihre vorhandenen Ressourcen, um festzustellen, welche zusätzlichen Fähigkeiten Sie benötigen, um Dienste mehrerer Cloud-Anbieter effektiv nutzen zu können. Möglicherweise müssen Sie Ihr Personal aufstocken oder zusätzliche Zeit und Geld in Weiterbildung und Schulung investieren, die über das hinausgehen, was für einen einzelnen Cloud-Anbieter erforderlich wäre. Wenn Sie bereits einzelne Teams oder Benutzer haben, die verschiedene Cloud-Anbieter nutzen, sollten Sie die organisatorischen Vorteile einer Konsolidierung dieser Teams auf Basis eines primären Cloud-Anbieters in Betracht ziehen. case-by-case
- Welchen zusätzlichen Overhead würde eine bestimmte Multi-Cloud-Architektur mit sich bringen?

Ein häufiger Grund für Multicloud ist der Wunsch, einen bestimmten verwalteten Dienst eines Anbieters zu nutzen, dessen Funktionen sich von den Diensten eines anderen Cloud-Anbieters unterscheiden lassen. Beispielsweise möchten Sie möglicherweise einen Cloud-Anbieter für Ihre Infrastrukturanforderungen und den Managed Service eines anderen Anbieters für Domain- und Verzeichnisdienste verwenden. Doch selbst wenn dieser einzelne verwaltete Dienst den Verwaltungsaufwand reduziert und die Verwaltung dieser Architekturkomponente vereinfacht, könnte er zusätzlichen Aufwand für andere Workloads mit sich bringen, wie Code-Refactoring, private Konnektivitätsanforderungen oder manuelle Integrationsarbeiten. Identifizieren Sie diesen zusätzlichen Aufwand im Voraus und stellen Sie sicher, dass er die Vorteile, die Ihr Team aus dem differenzierten Service ziehen kann, nicht ausgleichen oder in den Hintergrund drängen.

- Wie werden Sie die Überwachung und Verwaltung für alle Cloud-Anbieter zentralisieren?

  Wenn Sie beginnen, Anwendungen und Funktionen mithilfe von Ressourcen verschiedener Cloud-Anbieter bereitzustellen, sollten Sie sich überlegen, wie Sie diese Ressourcen taggen, überwachen und verwalten werden. Jeder Anbieter verfügt über eigene Tools, die Sie möglicherweise auf andere Umgebungen ausweiten können. Sie können Amazon beispielsweise verwenden, um wichtige Kennzahlen und Protokolle CloudWatch zu überwachen, Alarme zu erstellen und Ihre Anwendungen und Infrastruktur in Single-, Hybrid- und Multi-Cloud-Umgebungen zu visualisieren. Sie können es auch verwenden, AWS Systems Managerum die Transparenz und Kontrolle von Ressourcen zu verbessern, betriebliche Probleme schnell zu diagnostizieren und zu beheben und Prozesse wie das Aktualisieren und Patchen virtueller Maschinen umgebungsübergreifend zu automatisieren. Wenn Sie Anforderungen haben, die von den Tools eines Anbieters nicht unterstützt werden können, können Sie sich nach Partnerlösungen umsehen. Diese können jedoch zusätzliche Kosten oder zusätzlichen Integrationsaufwand mit sich bringen.

- Wie können Sie Infrastruktur als Code mit Automatisierung verwalten, wenn Sie verschiedene Cloud-Anbieter verwenden?

  Wenn Sie Ressourcen in der Cloud ausführen, hilft Ihnen die automatisierte Bereitstellung und Verwaltung von Ressourcen dabei, verschiedene Umgebungen effizient zu verwalten. Die APIs und nativen Automatisierungstools variieren je nach Cloud-Anbieter. Wenn möglich, sollten Sie die Verwendung eines gemeinsamen Satzes von Orchestrierungs- und Bereitstellungstools in Betracht ziehen, der die Ressourcen verschiedener Cloud-Anbieter berücksichtigen kann. Dies bietet mehr Flexibilität und vereinfacht den Betrieb über mehrere Clouds hinweg. Es könnte jedoch einfacher sein, die systemeigene Automatisierung jedes Anbieters separat zu verwenden und organisatorische Prozesse festzulegen, um eine angemessene Nutzung sicherzustellen.

- Haben Sie Compliance- und regulatorische Anforderungen, die jeder Cloud-Anbieter erfüllen muss?

  Möglicherweise haben Sie regulatorische Überlegungen, die vorschreiben, wie Daten gespeichert und behandelt werden sollen. Konzentrieren Sie sich auf die Standardisierung von Richtlinien (wie Netzwerkverkehr, Speicher und Sicherheit), die automatisch auf jede Cloud-Umgebung bei allen Cloud-Anbietern angewendet werden können. Überlegen Sie, wie Ihre Anwendungen mit ihren Daten kommunizieren, und hosten Sie sie bei demselben Anbieter. Wenn Ihre Anwendungen und ihre Daten anbieterübergreifend fragmentiert sind, wird es schwierig sein, sicherzustellen, dass Sie die Compliance- und behördlichen Anforderungen erfüllen. Oft ist es am besten, Anwendungen so nah wie möglich an den Daten zu platzieren, um die Netzwerklatenz zu minimieren, den Datendurchsatz zu maximieren und den Datenverlust zu begrenzen und gleichzeitig die Sicherheits- und Zugriffskontrollen zu vereinfachen.
- Sind Sie in der Lage, die Gesamtbetriebskosten zu minimieren und Preisnachlässe zu maximieren, wenn Sie Anwendungen bei verschiedenen Cloud-Anbietern bereitstellen?

  Es ist wichtig, die Gesamtbetriebskosten (TCO) zu berücksichtigen, wenn Multicloud in Betracht gezogen wird. Die Ausführung Ihrer Anwendungen über mehrere Cloud-Anbieter hinweg kann die Betriebskosten und den Verwaltungsaufwand für die Wartung und Verwaltung der Ressourcen in jeder Umgebung erhöhen. Darüber hinaus wird es durch die Verteilung der Nutzung auf mehrere Anbieter schwieriger, die Mengenrabatte oder Unternehmensvereinbarungen eines bestimmten Anbieters zu nutzen. Berücksichtigen Sie diese Faktoren, wenn Sie entscheiden, ob die Vorteile von Multicloud die höheren Gesamtbetriebskosten rechtfertigen.

Beispielanwendungsfälle

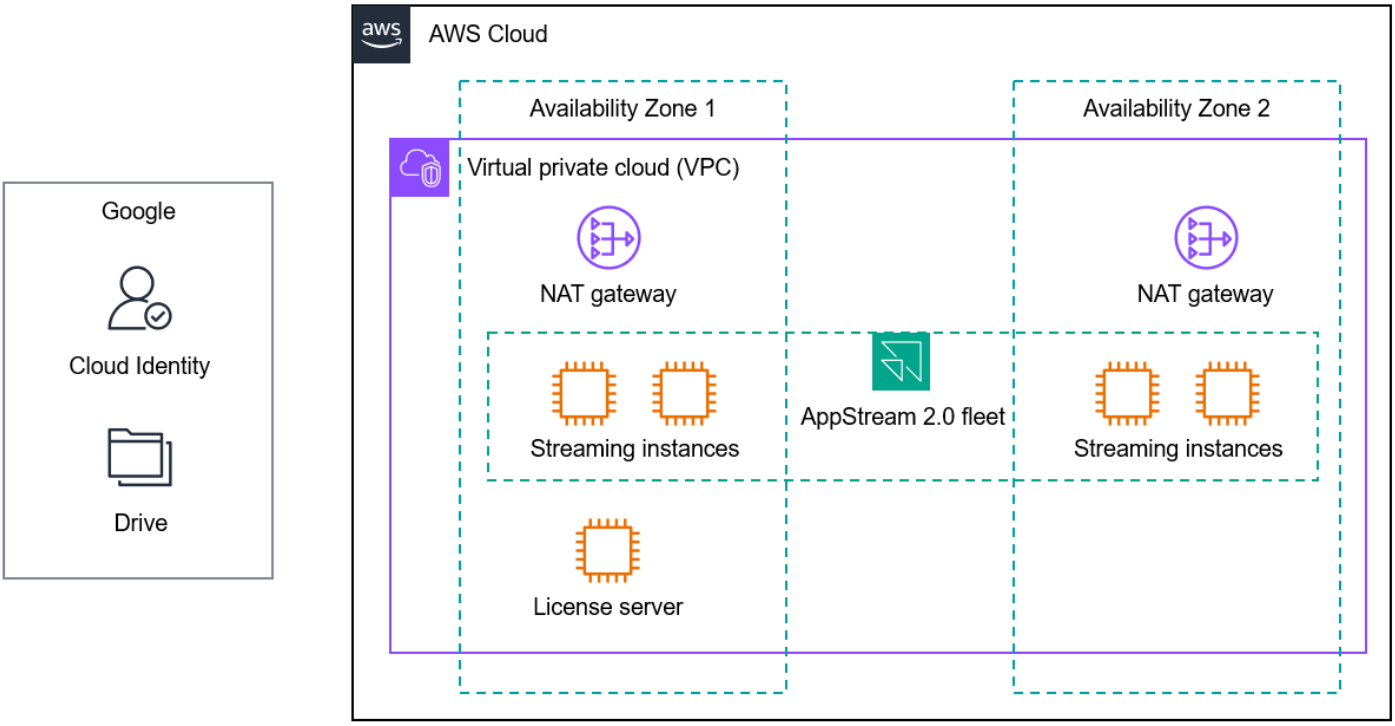
Um die Anwendung dieser Prinzipien in verschiedenen Szenarien besser zu verstehen, wollen wir einige Beispielanwendungsfälle besprechen. Diese Anwendungsfälle basieren darauf, wie Bildungseinrichtungen in der Praxis Cloud-Dienste einsetzen.

- Virtuelle Computerlabore
- Den Erfolg von Studierenden vorhersagen
- Identitätsverbund und Single Sign-On
- Cloud-Bursting für Forschungsrechnungen

Virtuelle Computerlabore

Trotz der Beliebtheit webbasierter Lerntools und der Fülle an Benutzergeräten wie Laptops, Chromebooks und Tablets unterhalten die meisten Bildungseinrichtungen physische Computerlabore für ressourcenintensive oder veraltete Anwendungen. Diese Computerräume sind häufig unverzichtbar für naturwissenschaftliche, technische, technische und mathematische Studiengänge (STEM), berufliche Bildung und technische Bildung (CTE), Medien und Kunst, Ingenieurwesen und ähnliche Lehrpläne. Schulen können physische Computerräume durch cloudbasierte virtuelle Desktops oder Anwendungsstreaming-Dienste erweitern oder ersetzen, um sicherzustellen, dass alle Schüler jederzeit, von jedem Ort und auf jedem Gerät Zugriff auf die benötigten Anwendungen haben. Dies verbessert die digitale Chancengleichheit, ermöglicht Fernunterricht, gewährleistet eine konsistente Benutzererfahrung, sichert den Fernzugriff und senkt gleichzeitig die Kosten.

In der Primar- und Sekundarstufe (K12) nutzen viele US-Schulen Amazon AppStream 2.0, einen vollständig verwalteten Desktop- und Anwendungs-Streaming-Dienst, um virtuelle Computerlabore bereitzustellen, die Zugriff auf Adobe Creative Cloud, Autodesk-Software, STEM- und CTE-Lehrpläne wie Project Lead the Way (PLTW) und mehr ermöglichen. Viele K12-Organisationen verwalten Single Sign-On und Dateispeicherung für Schüler bereits über Google Workspace und Google Drive, bei denen es sich um SaaS-Anwendungen handelt. Diese Einrichtungen können Single Sign-On zwischen Google Workspace und AppStream 2.0 über den SAML 2.0-Verbund einrichten. Sie können auch die native Integration zwischen AppStream 2.0 und Google Drive konfigurieren, sodass die Studierenden den vorhandenen Speicher nutzen können. Das folgende Diagramm veranschaulicht die AppStream 2.0-Bereitstellung für diesen Anwendungsfall.



Diese Architektur folgt den folgenden Empfehlungen:

- Wählen Sie einen primären, strategischen Cloud-Anbieter aus.Diese Architektur verwendet Cloud-Dienste von einem primären Cloud-Anbieter. Es beinhaltet zwar die Integration mit SaaS-Anwendungen, die nicht auf demselben Anbieter gehostet werden, diese Integrationen werden jedoch über einfache Konfigurationen durchgeführt. Cloud-Fachwissen und Fähigkeiten sind nur für die Bereitstellung und Verwaltung der Dienste des primären Cloud-Anbieters erforderlich.
- Unterscheiden Sie zwischen SaaS-Anwendungen und grundlegenden Cloud-Diensten.Google Workspace und Google Drive werden nicht auf demselben Cloud-Anbieter wie AppStream 2.0 gehostet. Dies ist jedoch akzeptabel, da diese Bereitstellung die erforderlichen Integrationen bietet. Single Sign-On ermöglicht ein zentrales Identitätsmanagement und wird über SAML 2.0 sicher konfiguriert. Die Aktivierung von persistentem Cloud-Speicher für Schüler erfordert einfache Konfigurationsänderungen in Google Drive und AppStream 2.0.
- Legen Sie Sicherheits- und Governance-Anforderungen für jeden Cloud-Dienstanbieter fest.Die in dieser Architektur verwendeten Dienste und Integrationen tragen dazu bei, die Sicherheits- und Governance-Anforderungen einer Institution zu erfüllen. Der Streaming-Verkehr ist verschlüsselt. Der Verbund über Google Workspace ermöglicht ein zentrales Identitätsmanagement. Netzwerkdienste wie Amazon Virtual Private Cloud (Amazon VPC) unterstützen die Konfiguration von Subnetzen, Routing und Firewalls. Sie können Inhalte filtern,

indem Sie die DNS-Konfiguration, Agenten, virtuelle Appliances oder verwaltete Dienste wie Amazon Route 53 Resolver die DNS-Firewall verwenden. Sie können Dienste nutzen, AWS Control Towerum beispielsweise sicherzustellen, dass das AWS-Konto, das AppStream 2.0 hostet, die standardmäßigen organisatorischen Richtlinien und Kontrollen einhält.

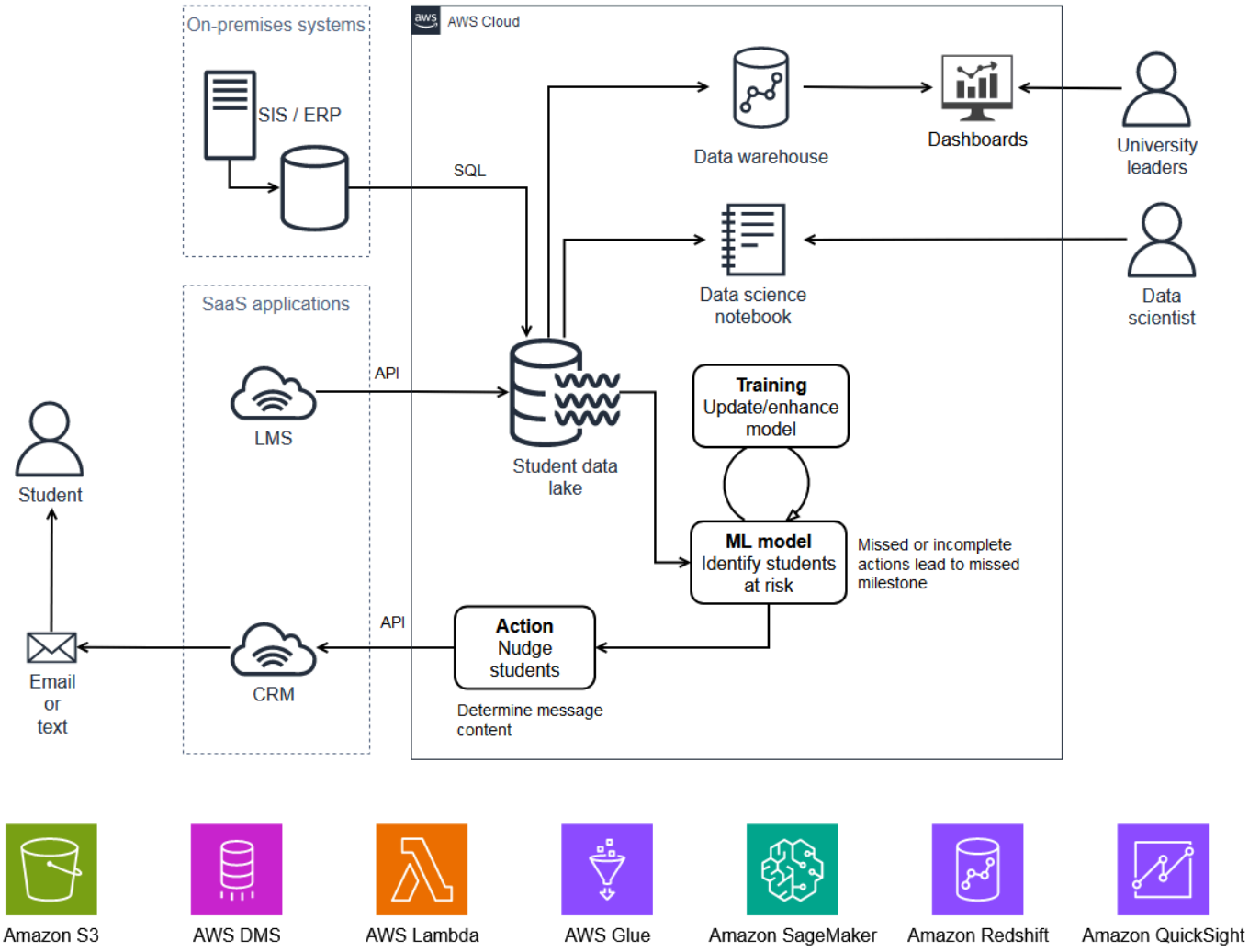
- Setzen Sie Cloud-native, verwaltete Lösungen ein, wo immer dies möglich und praktikabel ist. AppStream 2.0 ist ein verwalteter Dienst für Desktop- und Anwendungsstreaming. Sie können Desktops und Anwendungen streamen, ohne sich Gedanken über die Bereitstellung, Skalierung oder Wartung von Servern machen zu müssen. Sie installieren Ihre Anwendungen, verbinden die entsprechenden Identitäts-, Netzwerk- und Speicherlösungen und verwalten diese Anwendungen dann zentral und streamen sie an Ihre Benutzer. Dadurch entfällt ein Großteil der undifferenzierten Arbeit, die für die Verwaltung Ihrer eigenen virtuellen Desktop-Streaming-Lösung erforderlich wäre.

Den Erfolg von Studierenden vorhersagen

Eine Universität im Mittleren Westen der USA stellte fest, dass eine Handvoll wichtiger Aktivitäten für Studienanfänger den Erfolg sowohl im ersten Vorlesungssemester als auch beim Abschluss des Studiums stark vorhersagen konnten. Die Universität wollte ein System einführen, das darauf achtet, dass diese Aktivitäten abgeschlossen werden, und wenn wichtige Termine näher rückten oder verstrichen waren, wollte sie die Studierenden dazu ermutigen, diese Schritte abzuschließen.

Die Daten des SaaS-Lernmanagementsystems (LMS) waren ein wichtiger Input für diese Lösung, aber es erwies sich als schwierig, auf ihre Daten zuzugreifen und sie mit den Data Warehousing-Tools des IT-Teams der Universität zu verarbeiten. Darüber hinaus mussten die Nachrichten an die Schüler über das cloudbasierte CRM-System (Customer Relationship Management) der Schule gesendet werden. Um eine funktionierende Lösung zu entwickeln und die Wirksamkeit der Eingabeaufforderungen an die Studierenden zu beurteilen, musste die Universität Nachrichten über das CRM initiieren und daraus Daten sammeln.

Die Universität entwickelte eine Lösung und implementierte sie in einer einzigen Cloud-Umgebung. Die Lösung ist eine Mischung aus Cloud-nativen Managed Services, bereitgestellten Cloud-Servern und Integrationen mit lokalen Systemen und Cloud-basierten SaaS-Anwendungen. Wie das folgende Diagramm zeigt, nimmt die Lösung Daten aus dem Studenteninformationssystem (SIS), dem LMS und dem CRM in einen Data Lake auf. Sie verwendet diese Daten, um Studierende zu identifizieren, bei denen die Gefahr besteht, dass sie wichtige Aktivitäten verpassen, leitet Nachrichten über das CRM an sie weiter und stellt der Hochschulleitung ein Dashboard zur Verfügung.



Diese Architektur folgt den folgenden Empfehlungen:

- Wählen Sie einen primären, strategischen Cloud-Anbieter aus.Der strategische Cloud-Anbieter der Universität beherbergt die gesamte bereitgestellte Lösung. Auf diese Weise können sich die IT- und Geschäftsmitarbeiter auf die Entwicklung ihrer Fähigkeiten in einem einzigen, integrierten Satz von Cloud-Funktionen konzentrieren.
- Unterscheiden Sie zwischen SaaS-Anwendungen und grundlegenden Cloud-Diensten.Die Universität unterscheidet zwischen SaaS-Anwendungen und zentralen Cloud-Analysediensten und nutzt Integrationen mit den SaaS-Anwendungen, um Daten zu sammeln und die entsprechende Kommunikation zu initiieren.
- Legen Sie Sicherheits- und Governance-Anforderungen für jeden Cloud-Dienstanbieter fest.Die Universität stellt sicher, dass alle Komponenten der Architektur sicher sind, indem sie Leitplanken

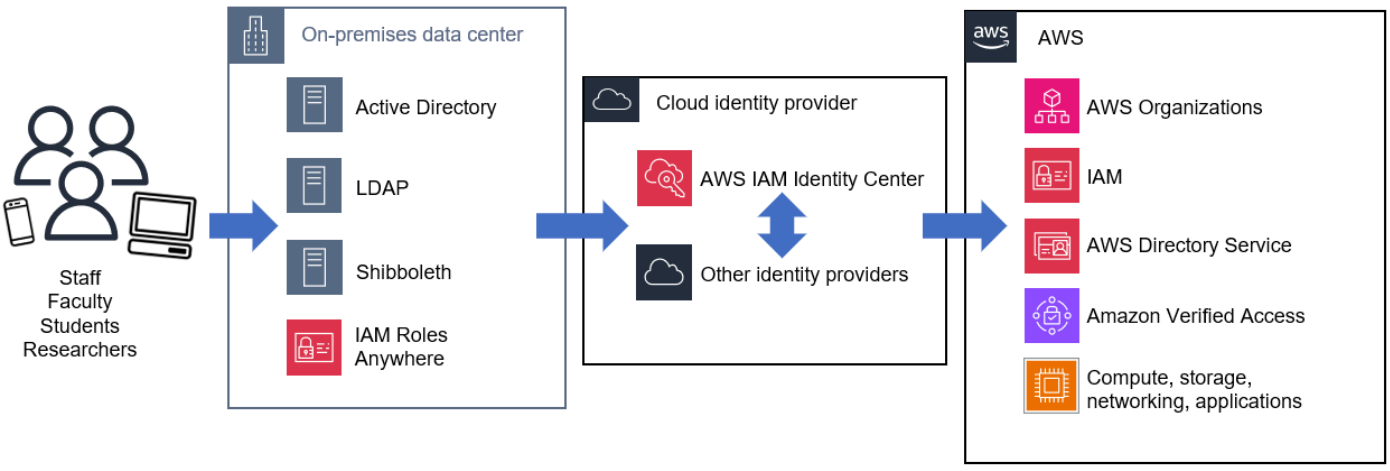
und Kontrollen durchsetzt, einschließlich Verschlüsselung bei der Übertragung und Speicherung, um die Daten der Studierenden angemessen zu handhaben.

- Setzen Sie Cloud-native, verwaltete Lösungen ein, wo immer dies möglich und praktikabel ist.Cloud-native Managed Services werden für die Datenaufnahme, Speicherung, Datenbank und ETL-Funktionalität (Extrahieren, Transformieren und Laden) verwendet, wodurch der Zeitaufwand für die Entwicklung des end-to-end Datenverarbeitungs-Workflows reduziert wird.

Identitätsverbund und Single Sign-On

Die Sicherstellung eines konsistenten Identitätsmanagements in allen Kernsystemen ist der Schlüssel zur erfolgreichen und sicheren Einführung jeder Technologie. Bildungseinrichtungen setzen zunehmend cloudbasierte Identitäts- und Single-Sign-On-Lösungen wie AWS IAM Identity CenterMicrosoft Entra ID (ehemals Azure Active Directory), Okta,,, Ping Identity ein JumpCloud OneLogin, um das Identitätsmanagement CyberArk zu vereinfachen, den Betriebsaufwand zu verringern und bewährte Verfahren wie Multi-Faktor-Authentifizierung und Least-Privilege-Zugriff zentral durchzusetzen.

Viele dieser Einrichtungen nutzen immer noch Identitätsmanagement und Verzeichnisdienste wie Active Directory und Shibboleth für ihre lokalen Umgebungen. Diese können in cloudbasierte Lösungen integriert werden, um ein zentrales Identitätsmanagement und Single Sign-On für Ihre Studierenden, Dozenten und Mitarbeiter zu ermöglichen. Anbieter von Cloud-Lösungen sollten über robuste Plattformen für das easy-to-integrate Identitätsmanagement verfügen, mit denen Sie Identitäten über Cloud-Identitätsanbieter mit Ihren vorhandenen Anwendungen, Ihren SaaS-Lösungen und Cloud-Diensten verbinden können. Das folgende Diagramm zeigt eine Beispielarchitektur.



Diese Architektur folgt den folgenden Empfehlungen:

- Wählen Sie einen primären, strategischen Cloud-Anbieter aus.Diese Architektur wird AWS als primärer Cloud-Anbieter verwendet. Durch die Integration mit einem Cloud-Identitätsanbieter und vorhandenen Identitätsverwaltungs- und Verzeichnisdiensten vor Ort unterstützt diese Architektur die automatisierte Bereitstellung und Verwaltung des Zugriffs sowohl auf die Dienste des primären Cloud-Anbieters als auch auf andere Anwendungen und SaaS-Lösungen. Dadurch wird sichergestellt, dass Sicherheits- und Governance-Anforderungen auf konsistente und einfach zu verwaltende Weise erfüllt werden, da das Technologieportfolio der Institution um weitere Anwendungen und Dienste erweitert wird.
- Unterscheiden Sie zwischen SaaS-Anwendungen und grundlegenden Cloud-Diensten.Diese Architektur integriert mehrere Arten von Cloud-basierten, SaaS- und lokalen Identitätssystemen, um den Zugriff auf AWS Cloud Dienste und andere Anwendungen zu ermöglichen. Viele cloudbasierte Identitätsanbieter- und Single Sign-On-Lösungen sind auch SaaS-Anwendungen und können native Integrationen und Standardprotokolle wie SAML verwenden, um umgebungsübergreifend zu arbeiten.
- Legen Sie Sicherheits- und Governance-Anforderungen für jeden Cloud-Dienstanbieter fest.Diese Architektur entspricht den Richtlinien für Identitäts- und Zugriffsmanagement, die von zahlreichen Sicherheits-Frameworks herausgegeben wurden, darunter das Cybersecurity Framework (CSF) des National Institute of Standards and Technology (NIST), NIST 800-171 und NIST 800-53. Integrationen mit AWS Identity and Access Management (IAM) und anderen AWS Sicherheits- AWS Organizations, Identitäts- und Compliance-Diensten tragen dazu bei, sichere, detaillierte Zugriffskontrollen auf der Grundlage von Gruppenberechtigungen bereitzustellen.
- Setzen Sie Cloud-native, verwaltete Dienste ein, wo immer dies möglich und praktikabel ist.Diese Architektur verwendet cloudbasierte, verwaltete Dienste für Identitätsmanagement und Single Sign-On. Dies reduziert den Zeit- und Energieaufwand für das Infrastrukturmanagement und erleichtert die Wartung dieser kritischen Systeme.
- Implementieren Sie Hybridarchitekturen, wenn bestehende Investitionen vor Ort Anreize für eine weitere Nutzung bieten.Diese Architektur integriert bestehende, lokale Investitionen in die Infrastruktur für das Hosten von Active Directory, Lightweight Directory Access Control (LDAP) und Shibboleth-Workloads und bietet einen Weg, zentrale Identitätsdienste letztendlich in eine cloudbasierte Infrastruktur zu verlagern. Wenn Ihre lokalen Workloads zudem zertifikatsbasierten Zugriff auf Ressourcen benötigen, können Sie Roles Anywhere verwenden. AWSAWS Identity and Access Management

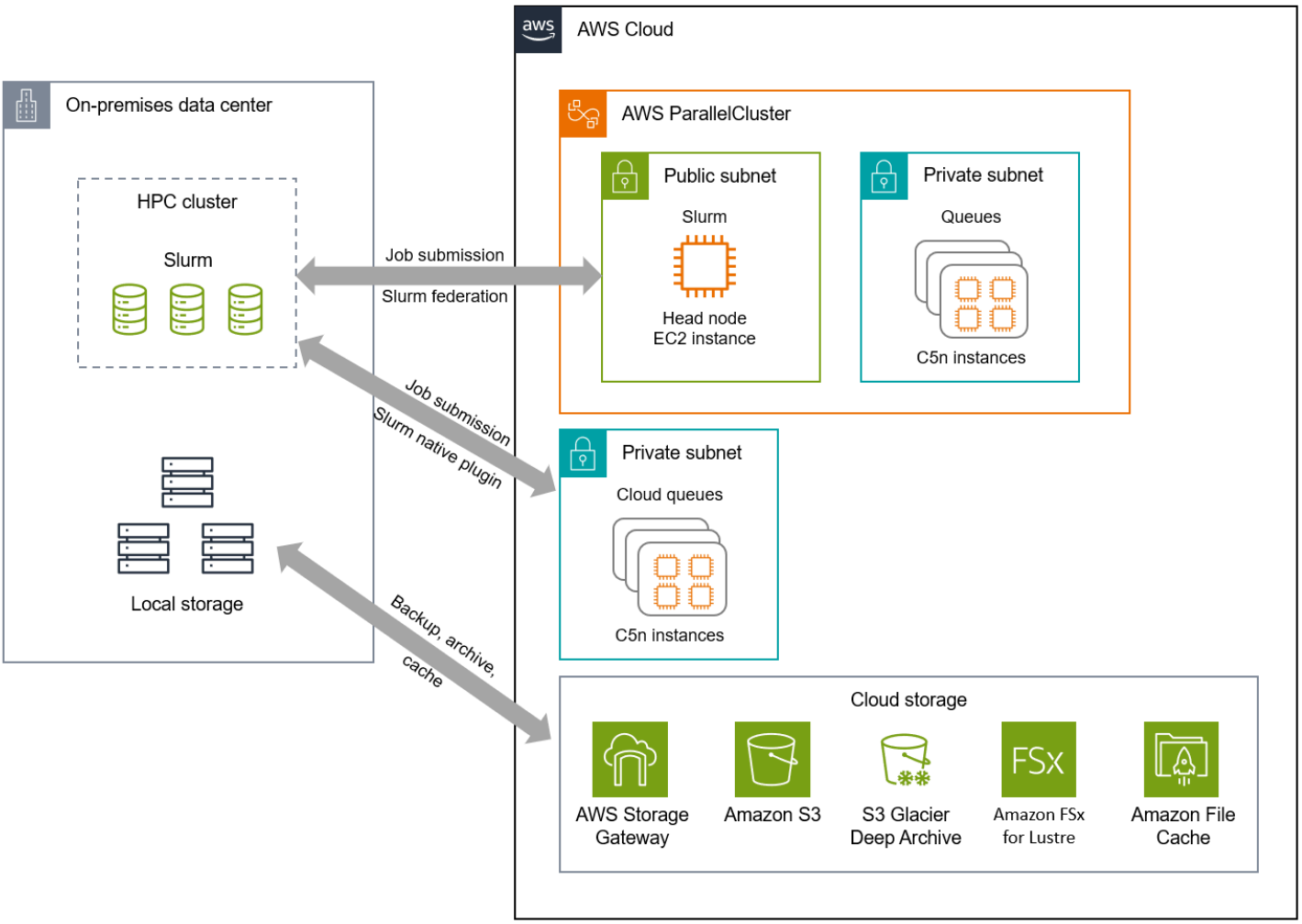
Cloud-Bursting für Forschungscomputer

Die Forschungsrechengruppe einer R1-Forschungseinrichtung (Doctoral Universities — Very High Research Activity) in den USA betrieb seit vielen Jahren lokale HPC-Cluster (High Performance Computing) mit dem Slurm-Scheduler. Abgesehen von einigen Wochen planmäßiger Wartung liefen die Cluster mit einer Auslastung von 80 bis 95 Prozent und die meisten Warteschlangen waren voll.

Die zunehmende Anzahl von Forschungsaktivitäten an der Institution führte zu Kapazitäts- und Fähigkeitsproblemen. Einige hochkarätige Forscher führten ständig Simulationen mit langer Laufzeit an bestimmten Warteschlangen durch, was die Wartezeit für andere Benutzer erhöhte. Neu eingestellte Dozenten mussten eine große Anzahl von Wettersimulationen durchführen, um ein neuartiges Modell für Wettervorhersagen mit künstlicher Intelligenz und maschinellem Lernen (KI/ML) zu entwickeln, aber sie benötigten mehr Kapazität als verfügbar war. Die Forschungsgruppe erhielt auch mehr Anfragen nach den neuesten Grafikprozessoren (GPUs) zum Trainieren von Modellen für maschinelles Lernen. Selbst mit der Finanzierung neuer Geräte müsste das Team monatelang warten GPUs, um die Genehmigung für die Erweiterung der Rackfläche im Rechenzentrum zu erhalten.

Viele Forscher waren nicht bereit, alte Daten zu löschen, sodass auch die lokale Speicherkapazität eine Herausforderung darstellte. Eine skalierbarere, langfristige Speicheroption war erforderlich, um wertvollen Hochleistungsspeicher vor Ort freizugeben.

Die Cloud begegnet diesen Herausforderungen mit hybriden Rechen- und Speicherlösungen, mit denen Sie Forschungscomputer in die Cloud verlagern können, wenn die Kapazität vor Ort nicht ausreicht. Das folgende Architekturdiagramm veranschaulicht einige Methoden zur Nutzung von Rechenleistung und Speicherplatz, bei denen Tools wie AWS ParallelClusterund zum Einsatz kommen. AWS Storage Gateway



Diese Architektur folgt den folgenden Empfehlungen:

- Wählen Sie einen primären, strategischen Cloud-Anbieter aus.Diese Architektur verwendet einen primären Cloud-Anbieter, um zu vermeiden, dass sie durch den Ansatz mit dem kleinsten gemeinsamen Nenner eingeschränkt wird. Auf diese Weise kann die Institution die Innovation und die systemeigenen Rechen- und Speicherdienste nutzen, die der primäre Cloud-Anbieter anbietet. Das Forschungsteam kann sich auf die Optimierung der Workloads in der Umgebung konzentrieren, die vom primären Cloud-Anbieter bereitgestellt wird, und nicht darauf, wie man in verschiedenen Cloud-Umgebungen arbeitet.
- Legen Sie Sicherheits- und Governance-Anforderungen für jeden Cloud-Dienstanbieter fest.Jeder Dienst und jedes Tool, das in dieser Architektur verwendet wird, kann so konfiguriert werden, dass sie die Sicherheits- und Governance-Anforderungen des Forschungsteams erfüllen, einschließlich privater Konnektivität, Datenverschlüsselung bei der Übertragung und im Ruhezustand, Aktivitätsprotokollierung und mehr.

- Setzen Sie Cloud-native, verwaltete Dienste ein, wo immer dies möglich und praktikabel ist.Diese Architektur bietet die Möglichkeit, verwaltete Speicher- und Rechendienste sowie Tools zur Vereinfachung der Clusterverwaltung zu verwenden. Auf diese Weise muss sich das Forschungsteam nicht selbst um die Verwaltung von Clustern oder der zugrunde liegenden Infrastruktur kümmern, was komplex und zeitaufwändig sein kann.
- Implementieren Sie Hybridarchitekturen, wenn bestehende Investitionen vor Ort Anreize für eine weitere Nutzung bieten.Diese Architektur ermöglicht es der Institution, ihre lokalen Ressourcen weiterhin zu nutzen und die Vorteile der Cloud zu nutzen, um die Kapazität zu erhöhen und die Rechenleistung bei Bedarf zu erweitern. Mit der Cloud kann die Institution den Rechnertyp anpassen, um das Preis-Leistungs-Verhältnis zu maximieren, und sie kann auf die neueste Technologie zugreifen, um Innovationen zu fördern, ohne im Voraus große Investitionen in zusätzliche Hardware vor Ort tätigen zu müssen.

Nächste Schritte

Die Auswahl des richtigen Bereitstellungsmodells für Cloud-Workloads erfordert sorgfältige Überlegungen. Nutzen Sie die in diesem paper dargelegten Empfehlungen als Leitfaden für Ihre Entscheidungsfindung und vermeiden Sie häufige Fallstricke wie unnötige Komplexität, steigende Personalanforderungen, inkonsistente Unternehmensführung und Ansätze mit dem kleinsten gemeinsamen Nenner. Wenn Sie diese Best Practices befolgen, können Sie Ihre Cloud-Einführung beschleunigen, um Ihre institutionellen Ziele effektiver zu erreichen und zu übertreffen.

Denken Sie daran, einen primären, strategischen Cloud-Anbieter auszuwählen und ein Cloud Center of Excellence (CCoE) einzurichten, um die organisatorische Reife zu fördern und Ihren langfristigen Erfolg sicherzustellen. Unterscheiden Sie zwischen SaaS-Anwendungen und grundlegenden Cloud-Diensten und identifizieren Sie jeweils die wichtigsten Sicherheits- und Governance-Anforderungen. Setzen Sie wann immer möglich cloudnative, verwaltete Services ein und implementieren Sie Hybridarchitekturen, wenn Ihre bestehenden Investitionen in Rechenzentren Anreize zur weiteren Nutzung bieten. Und schließlich sollten Sie Multicloud nur für die Workloads reservieren, die sie wirklich benötigen.

AWS ist gut positioniert, um Sie bei der Verwaltung von Single-, Hybrid- und Multi-Cloud-Umgebungen zu unterstützen. Ihre Institution kann AWS Management- und Observability-Lösungen wie AWS Systems ManagerAWS Config, und Amazon verwenden, CloudWatch um die Verwaltung und Überwachung Ihrer Infrastruktur und Anwendungen unabhängig von Ihrer Umgebung zu vereinfachen und zu zentralisieren. Mit Daten- und Analysediensten wie Amazon Athena und können Sie Erkenntnisse aus all Ihren Daten gewinnen AWS DataSync, unabhängig davon, wo sie gespeichert sind. AWS Glue Mit Hybridlösungen wie AWS OutpostsAWS Wavelength, und können AWS Snow FamilySie AWS Infrastruktur und Dienste dorthin bringen, wo sie benötigt werden. Tools wie Amazon EKS Distro helfen Ihnen beim Aufbau selbstverwalteter Kubernetes-Cluster in AWS, vor Ort oder in anderen Clouds.

Beachten Sie bei der Definition Ihrer Cloud-Strategie die folgenden nächsten Schritte:

1. Sehen Sie sich das AWS Cloud Adoption Framework (AWS CAF) an, um Transformationsmöglichkeiten zu identifizieren und zu priorisieren, Ihre Cloud-Bereitschaft zu bewerten und zu verbessern und Ihre Roadmap für die Transformation iterativ weiterzuentwickeln.
2. Identifizieren Sie zunächst ein System für die Cloud-Implementierung als Machbarkeitsnachweis. Dies hilft Ihnen dabei, die Cloud-Grundlage oder das Cloud-Framework zu definieren, um alle Annahmen zu validieren, und ermöglicht auch future Cloud-Implementierungen.

3. Beziehen Sie Ihr AWS Kundenbetreuungsteam ein, um Ihre Ziele für die Cloud-Implementierung zu besprechen. Das AWS Account-Team kann Ihnen bei der Klärung helfen, Lösungsansätze vorschlagen, Abhängigkeiten identifizieren und auch mit Ihren Teams zusammenarbeiten, um Ihren Weg vom ersten Konzept bis zur Implementierung zu planen.

Mitwirkende

Zu den Mitwirkenden an diesem Leitfaden gehören:

- Kevin Arand, Senior Manager, Lösungsarchitektur, Bildung, AWS
- Kevin McCandless, leitender Lösungsarchitekt, K-12 Education, AWS
- Craig Jordanien, Principal Solutions Architect, Bildung, AWS
- Jesse Roberts, leitender Lösungsarchitekt, SLG & K-12 Education, AWS
- Jianjun Xu, leitender Lösungsarchitekt, Bildung, AWS
- Josh Badal, leitender Lösungsarchitekt, Bildung, AWS
- Raj Chary, leitender Lösungsarchitekt, Bildung, AWS

Weitere Informationen

Zusätzliche Informationen finden Sie unter:

- AWS Zentrum für Architektur
- Cloud-Transformation im öffentlichen Sektor
- AWS Framework für die Cloud-Einführung (AWS CAF)
- AWS Lösungen für Hybrid- und Multicloud

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	—	15. September 2023

AWS Glossar zu präskriptiven Leitlinien

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

Zahlen

7 Rs

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

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

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

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

A

ABAC

Siehe attributbasierte Zugriffskontrolle.

abstrahierte Dienste

Weitere Informationen finden Sie unter Managed Services.

ACID

Siehe Atomarität, Konsistenz, Isolierung und Haltbarkeit.

Aktiv-Aktiv-Migration

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

Aktiv-Passiv-Migration

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

Aggregatfunktion

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

AI

Siehe künstliche Intelligenz.

AIOps

Siehe Operationen im Bereich künstliche Intelligenz.

Anonymisierung

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

Anti-Muster

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

Anwendungssteuerung

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

Anwendungsportfolio

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

künstliche Intelligenz (KI)

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

Operationen mit künstlicher Intelligenz (AIOps)

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

Asymmetrische Verschlüsselung

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

Atomizität, Konsistenz, Isolierung, Haltbarkeit (ACID)

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

Attributbasierte Zugriffskontrolle (ABAC)

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

autoritative Datenquelle

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

Availability Zone

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

AWS Framework für die Cloud-Einführung (AWS CAF)

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

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

AWS Workload-Qualifizierungsrahmen (AWS WQF)

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

B

schlechter Bot

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

BCP

Siehe Planung der Geschäftskontinuität.

Verhaltensdiagramm

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

Big-Endian-System

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

Binäre Klassifikation

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

Bloom-Filter

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

Blau/Grün-Bereitstellung

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

Bot

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

Botnetz

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

branch

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

Zugang durch Glasbruch

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

Brownfield-Strategie

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

Puffer-Cache

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

Geschäftsfähigkeit

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

Planung der Geschäftskontinuität (BCP)

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

C

CAF

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

Bereitstellung auf Kanaren

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

CCoE

Weitere Informationen finden Sie im Cloud Center of Excellence.

CDC

Siehe Erfassung von Änderungsdaten.

Erfassung von Datenänderungen (CDC)

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

Chaos-Technik

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

CI/CD

Siehe Continuous Integration und Continuous Delivery.

Klassifizierung

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

clientseitige Verschlüsselung

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

Cloud-Exzellenzzentrum (CCoE)

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

Cloud Computing

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

Cloud-Betriebsmodell

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

Phasen der Einführung der Cloud

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

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

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

CMDB

Siehe Datenbank für das Konfigurationsmanagement.

Code-Repository

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

Kalter Cache

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

Kalte Daten

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

Computer Vision (CV)

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

Drift in der Konfiguration

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

Verwaltung der Datenbankkonfiguration (CMDB)

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

Konformitätspaket

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

Kontinuierliche Bereitstellung und kontinuierliche Integration (CI/CD)

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

CV

Siehe Computer Vision.

D

Daten im Ruhezustand

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

Datenklassifizierung

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

Datendrift

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

Daten während der Übertragung

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

Datennetz

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

Datenminimierung

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

Datenperimeter

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

Vorverarbeitung der Daten

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

Herkunft der Daten

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

betroffene Person

Eine Person, deren Daten gesammelt und verarbeitet werden.

Data Warehouse

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

Datenbankdefinitionssprache (DDL)

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

Datenbankmanipulationssprache (DML)

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

DDL

Siehe Datenbankdefinitionssprache.

Deep-Ensemble

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

Deep Learning

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

defense-in-depth

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

delegierter Administrator

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

Bereitstellung

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

Entwicklungsumgebung

Siehe Umgebung.

Detektivische Kontrolle

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

Abbildung des Wertstroms in der Entwicklung (DVSM)

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

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

digitaler Zwilling

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

Maßtabelle

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

Katastrophe

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

Disaster Recovery (DR)

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

DML

Siehe Sprache zur Datenbankmanipulation.

Domainorientiertes Design

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

DR

Siehe Disaster Recovery.

Erkennung von Driften

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

DVSM

Siehe Abbildung des Wertstroms in der Entwicklung.

E

EDA

Siehe explorative Datenanalyse.

EDI

Siehe elektronischer Datenaustausch.

Edge-Computing

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

elektronischer Datenaustausch (EDI)

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

Verschlüsselung

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

Verschlüsselungsschlüssel

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

Endianismus

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

Endpunkt

Siehe Service-Endpunkt.

Endpunkt-Services

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

Unternehmensressourcenplanung (ERP)

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

Envelope-Verschlüsselung

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

Umgebung

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

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

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

Epics

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

ERP

Siehe Enterprise Resource Planning.

Explorative Datenanalyse (EDA)

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

F

Faktentabelle

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

schnell scheitern

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

Grenze zur Fehlerisolierung

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

Feature-Zweig

Siehe Zweig.

Features

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

Bedeutung der Feature

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

Featuretransformation

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

Eingabeaufforderung mit wenigen Klicks

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

FGAC

Siehe detaillierte Zugriffskontrolle.

Feinkörnige Zugriffskontrolle (FGAC)

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

Flash-Cut-Migration

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

FM

Siehe Fundamentmodell.

Fundamentmodell (FM)

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

G

generative KI

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

Geoblocking

Siehe geografische Einschränkungen.

Geografische Einschränkungen (Geoblocking)

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

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

Gitflow-Workflow

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

goldenes Bild

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

Greenfield-Strategie

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

Integritätsschutz

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

H

HEKTAR

Siehe Hochverfügbarkeit.

Heterogene Datenbankmigration

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

hohe Verfügbarkeit (HA)

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

historische Modernisierung

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

Holdout-Daten

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

Homogene Datenbankmigration

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

heiße Daten

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

Hotfix

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

Hypercare-Phase

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

I

IaC

Sehen Sie sich Infrastruktur als Code an.

Identitätsbasierte Richtlinie

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

Leerlaufanwendung

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

IIoT

Siehe Industrielles Internet der Dinge.

unveränderliche Infrastruktur

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

Eingehende (ingress) VPC

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

Inkrementelle Migration

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

Industrie 4.0

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

Infrastruktur

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

Infrastructure as Code (IaC)

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

industrielles Internet der Dinge (T) IIo

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

Inspektions-VPC

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

Internet of Things (IoT)

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

Interpretierbarkeit

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

IoT

Siehe Internet der Dinge.

IT information library (ITIL, IT-Informationsbibliothek)

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

T service management (ITSM, IT-Servicemanagement)

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

BIS

Weitere Informationen finden Sie in der IT-Informationsbibliothek.

ITSM

Siehe IT-Servicemanagement.

L

Labelbasierte Zugangskontrolle (LBAC)

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

Landing Zone

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

großes Sprachmodell (LLM)

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

Große Migration

Eine Migration von 300 oder mehr Servern.

SCHWARZ

Weitere Informationen finden Sie unter Label-basierte Zugriffskontrolle.

Geringste Berechtigung

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

Lift and Shift

Siehe 7 Rs.

Little-Endian-System

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

LLM

Siehe großes Sprachmodell.

Niedrigere Umgebungen

Siehe Umgebung.

M

Machine Learning (ML)

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

Hauptzweig

Siehe Filiale.

Malware

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

verwaltete Dienste

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

Manufacturing Execution System (MES)

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

MAP

Siehe Migration Acceleration Program.

Mechanismus

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

Mitgliedskonto

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

DURCHEINANDER

Siehe Manufacturing Execution System.

Message Queuing-Telemetrietransport (MQTT)

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

Microservice

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

Microservices-Architekturen

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

Migration Acceleration Program (MAP)

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

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

Migration in großem Maßstab

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

Migrationsfabrik

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

Migrationsmetadaten

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

Migrationsmuster

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

Migration Portfolio Assessment (MPA)

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

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

Migration Readiness Assessment (MRA)

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

Migrationsstrategie

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

ML

Siehe maschinelles Lernen.

Modernisierung

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

Bewertung der Modernisierungsfähigkeit

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

Monolithische Anwendungen (Monolithen)

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

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

MPA

Siehe Bewertung des Migrationsportfolios.

MQTT

Siehe Message Queuing-Telemetrietransport.

Mehrklassen-Klassifizierung

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

veränderbare Infrastruktur

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

O

OAC

Siehe Origin Access Control.

OAI

Siehe Zugriffsidentität von Origin.

COM

Siehe organisatorisches Change-Management.

Offline-Migration

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

OI

Siehe Betriebsintegration.

OLA

Siehe Vereinbarung auf operativer Ebene.

Online-Migration

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

OPC-UA

Siehe Open Process Communications — Unified Architecture.

Offene Prozesskommunikation — Einheitliche Architektur (OPC-UA)

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

Vereinbarung auf Betriebsebene (OLA)

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

Überprüfung der Betriebsbereitschaft (ORR)

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

Betriebstechnologie (OT)

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

Betriebsintegration (OI)

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

Organisationspfad

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

Organisatorisches Veränderungsmanagement (OCM)

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

Ursprungszugriffskontrolle (OAC)

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

Ursprungszugriffsidentität (OAI)

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

ORR

Weitere Informationen finden Sie unter Überprüfung der Betriebsbereitschaft.

NICHT

Siehe Betriebstechnologie.

Ausgehende (egress) VPC

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

P

Berechtigungsgrenze

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

persönlich identifizierbare Informationen (PII)

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

Personenbezogene Daten

Siehe persönlich identifizierbare Informationen.

Playbook

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

PLC

Siehe programmierbare Logiksteuerung.

PLM

Siehe Produktlebenszyklusmanagement.

policy

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

Polyglotte Beharrlichkeit

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

Portfoliobewertung

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

predicate

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

Prädikat Pushdown

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

Präventive Kontrolle

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

Prinzipal

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

Datenschutz von Natur aus

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

Privat gehostete Zonen

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

proaktive Steuerung

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

Produktlebenszyklusmanagement (PLM)

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

Produktionsumgebung

Siehe Umgebung.

Speicherprogrammierbare Steuerung (SPS)

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

schnelle Verkettung

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

Pseudonymisierung

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

publish/subscribe (pub/sub)

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

Q

Abfrageplan

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

Abfrageplanregression

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

R

RACI-Matrix

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

LAPPEN

Siehe Erweiterte Generierung beim Abrufen.

Ransomware

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

RASCI-Matrix

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

RCAC

Siehe Zugriffskontrolle für Zeilen und Spalten.

Read Replica

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

neu strukturieren

Siehe 7 Rs.

Recovery Point Objective (RPO)

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

Wiederherstellungszeitziel (RTO)

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

Refaktorierung

Siehe 7 Rs.

Region

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

Regression

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

rehosten

Siehe 7 Rs.

Veröffentlichung

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

umziehen

Siehe 7 Rs.

neue Plattform

Siehe 7 Rs.

Rückkauf

Siehe 7 Rs.

Ausfallsicherheit

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

Ressourcenbasierte Richtlinie

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

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

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

Reaktive Kontrolle

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

Beibehaltung

Siehe 7 Rs.

zurückziehen

Siehe 7 Rs.

Retrieval Augmented Generation (RAG)

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

Drehung

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

Zugriffskontrolle für Zeilen und Spalten (RCAC)

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

RPO

Siehe Recovery Point Objective.

RTO

Siehe Ziel der Wiederherstellungszeit.

Runbook

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

S

SAML 2.0

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

SCADA

Siehe Aufsichtskontrolle und Datenerfassung.

SCP

Siehe Richtlinie zur Dienstkontrolle.

Secret

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

Sicherheit durch Design

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

Sicherheitskontrolle

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

Härtung der Sicherheit

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

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

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

Automatisierung von Sicherheitsreaktionen

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

Serverseitige Verschlüsselung

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

Service-Kontrollrichtlinie (SCP)

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

Service-Endpunkt

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

Service Level Agreement (SLA)

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

Service-Level-Indikator (SLI)

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

Service-Level-Ziel (SLO)

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

Modell der geteilten Verantwortung

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

SIEM

Siehe Sicherheitsinformations- und Event-Management-System.

Single Point of Failure (SPOF)

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

SLA

Siehe Service Level Agreement.

SLI

Siehe Service-Level-Indikator.

ALSO

Siehe Service-Level-Ziel.

split-and-seed Modell

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

SPOTTEN

Siehe Single Point of Failure.

Sternschema

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

Strangler-Fig-Muster

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

Subnetz

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

Aufsichtskontrolle und Datenerfassung (SCADA)

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

Symmetrische Verschlüsselung

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

synthetisches Testen

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

Systemaufforderung

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

T

tags

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

Zielvariable

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

Aufgabenliste

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

Testumgebungen

Siehe Umgebung.

Training

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

Transit-Gateway

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

Stammbasierter Workflow

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

Vertrauenswürdiger Zugriff

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

Optimieren

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

Zwei-Pizzen-Team

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

U

Unsicherheit

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

undifferenzierte Aufgaben

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

höhere Umgebungen

Siehe Umgebung.

V

Vacuuming

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

Versionskontrolle

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

VPC-Peering

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

Schwachstelle

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

W

Warmer Cache

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

warme Daten

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

Fensterfunktion

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

Workload

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

Workstream

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

WURM

Sehen Sie einmal schreiben, viele lesen.

WQF

Siehe AWS Workload-Qualifizierungsrahmen.

einmal schreiben, viele lesen (WORM)

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

Z

Zero-Day-Exploit

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

Zero-Day-Sicherheitslücke

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

Zero-Shot-Aufforderung

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

Zombie-Anwendung

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

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