Netzwerkverbindungsoptionen AWS für SaaS-Angebote aktiviert

AWS Präskriptive Leitlinien

AWS Präskriptive Leitlinien: Netzwerkverbindungsoptionen AWS für SaaS-Angebote aktiviert

Table of Contents

Netzwerkverbindungsoptionen AWS für SaaS-Angebote aktiviert

Tomas Sykora und Luca Schumann, Amazon Web Services

September 2025 (Geschichte der Dokumente)

In diesem Leitfaden werden gängige Szenarien für die Verbindung von Verbraucheranwendungen mit Anbietern von Software as a Service (SaaS) untersucht. Es wird erläutert, wie Sie eine Verbindung zu Ressourcen herstellen können, die sich vor Ort, in den AWS Cloud Clouds anderer Clouddienstanbieter (CSP) oder in Hybridarchitekturen befinden. Zu diesen Szenarien gehören die folgenden:

- Bereitstellung von Webdiensten über HTTPS
- Bereitstellung von TCP-basierten Diensten
- Verwendung AWS AppSynczur Implementierung von Publish-Subscribe (Pub/Sub) und GraphQL APIs
- Nutzung von AWS Ressourcen zur Bereitstellung für Echtzeitanwendungen WebSockets
- Aktivierung des bidirektionalen Zugriffs für interaktive Servicekommunikation

Durch die Ausrichtung auf die in diesem Leitfaden beschriebenen Best Practices können SaaS-Anbieter das Vertrauen ihrer Kunden stärken und einen skalierbaren, sicheren und belastbaren Zugriff auf SaaS-Angebote unterstützen.

Dieser Leitfaden enthält auch Kriterien zur Selbsteinschätzung, anhand derer Sie beurteilen können, wie erfolgreich Sie die Netzwerkanforderungen für Verbraucher für Ihr SaaS-Angebot erfüllen. Neben Verbindungsmustern finden Sie auch umfassende Vergleiche von AWS Netzwerkdiensten, allgemeine Architekturdiagramme für verschiedene Bereitstellungsszenarien und praktische Anleitungen zur Auswahl des richtigen Ansatzes für Ihren spezifischen Geschäftskontext. In diesem Leitfaden werden Sicherheitsaspekte für jede Netzwerkoption untersucht, häufig zu vermeidende Fallstricke erörtert und Implementierungsempfehlungen gegeben, die ein Gleichgewicht zwischen technischen Anforderungen und betrieblicher Effizienz herstellen. Darüber hinaus finden Sie strategische Rahmenbedingungen, mit denen Sie Ihre Netzwerkentscheidungen auf Ihr Geschäftsmodell, Ihre Wachstumsziele und die Einhaltung gesetzlicher Vorschriften abstimmen können.

Zielgruppe

Dieser Leitfaden richtet sich an SaaS-Anbieter. Es hilft Cloud-Architekten, Produktmanagern und Netzwerktechnikern, die Netzwerkkonnektivität für SaaS-Angebote in der entwerfen, implementieren und optimieren AWS Cloud. Um die Konzepte und Empfehlungen in diesem Leitfaden zu verstehen, sollten Sie mit den AWS Grundlagen, den wichtigsten SaaS-Konzepten und Netzwerkprinzipien auf hoher Ebene vertraut sein.

Ziele

In diesem Leitfaden werden Netzwerkarchitekturoptionen und praxiserprobte Best Practices erörtert, mit denen Verbraucher den Zugriff auf SaaS-Angebote optimieren können. Die Umsetzung der Empfehlungen in diesem Leitfaden unterstützt Folgendes:

- Einfache Integration — Sorgen Sie für eine unkomplizierte Kundenreise vom Onboarding bis zur Produktion, sodass Sie die Amortisierungszeit Ihrer Kunden beschleunigen und ihren Umsatzerlösezyklus verkürzen können.
- Anpassungsfähigkeit — Integrieren Sie sich nahtlos in die bestehenden Netzwerkinfrastrukturen Ihrer Kunden, indem Sie sich an deren sich ändernde Bedürfnisse anpassen. Dies verbessert das Wertversprechen Ihres Produkts.
- Gesamtbetriebskosten — Standardisieren Sie den Netzwerkzugriff, um die Änderungskosten und die Kosten pro Mieter zu reduzieren. Durch die Verbesserung der Bereitstellungskonsistenz können Sie auch den Zeitaufwand für die Ursachenanalyse oder Reparatur reduzieren.
- Abhängigkeitsmanagement — Machen Sie sich mit den Abhängigkeiten, langfristigen Auswirkungen und Kompromissen der verschiedenen Netzwerkzugriffsoptionen vertraut. Dies hilft Produktführern, fundierte Produktentscheidungen zu treffen.
- Kombinierbarkeit und Erweiterbarkeit — Entkoppeln Sie die Entwicklung der Kernfunktionen von der Betriebsinfrastruktur. Dies hilft Entwicklungsteams, schneller voranzukommen und sich darauf zu konzentrieren, Mehrwert für Ihre Kunden zu schaffen.
- Vertrauen fördern — Durch die Bereitstellung eines stabilen, fehlertoleranten, sicheren und skalierbaren Zugriffs auf SaaS-Angebote können Sie regulatorische Risiken reduzieren und Vertrauen in Ihre Fähigkeit gewinnen, das Wachstum Ihrer Kunden zu unterstützen.

Bewertung von Netzwerkzugriffsentscheidungen für SaaS-Angebote

Verstehen Sie Ihren Markt

Die Entscheidungen, die Sie jetzt in Bezug auf Netzwerke treffen, bestimmen, ob das Wertversprechen Ihres SaaS-Produkts Ihren Kunden gerecht werden kann. Trotz der strategischen Bedeutung dieser Entscheidungen wird die Bereitstellung des Zugangs zu Ihrem SaaS-Angebot oft als rein technologisches Thema wahrgenommen. Zu den Risiken, die diese Wahrnehmung mit sich bringt, gehören längere Umsatzerfassungszyklen, betriebliche Ineffizienzen und eine Fehlausrichtung mit der Geschäftsstrategie. Wenn beispielsweise eine schnelle Expansion ein strategisches Unternehmensziel ist, sollte Ihr Entscheidungsprozess darauf ausgerichtet sein, ob die Lösungen, die Sie in Betracht ziehen, skalierbar und flexibel genug sind, um die Expansion zu unterstützen. Selbst wenn Sie Ihr Unternehmen erfolgreich ausbauen, dürfen die Betriebskosten nicht zu einem Hindernis für future Wachstum werden, und eine falsch ausgerichtete Kostenstruktur könnte all Ihre Gewinne zunichte machen.

Überlegen Sie sich beispielsweise, wie sich die folgenden Markterwägungen auf technische Aspekte des Produkts auswirken, z. B. Netzwerktechnik:

- Wenn Ihr Geschäftsmodell auf Abonnementbasis basiert, bevorzugen Ihre Kunden wahrscheinlich Lösungen mit vorhersehbaren, wiederkehrenden Kosten gegenüber großen Vorabinvestitionen.
- Wenn Ihre Geschäftsstrategie auf hochwertige Unternehmenskunden abzielt, bestimmen Kriterien in Bezug auf Sicherheit, Unternehmensführung und Einhaltung gesetzlicher Vorschriften, ob Ihr SaaS-Angebot überhaupt in Betracht gezogen wird.
- Wenn es sich bei Ihrem Zielmarkt hauptsächlich um Startups handelt, sind einfache Integration, Amortisierungszeit und Anpassungsfähigkeit wahrscheinlich wichtige Faktoren. Startups legen in der Regel Wert auf Geschwindigkeit und Agilität. Da sie eine Marke aufbauen und schnell Gewinne erzielen müssen, bevorzugen sie wahrscheinlich Lösungen, die schnell und einfach zu integrieren sind, kostengünstig skalierbar sind, die Abhängigkeit von Experten verringern und keine wertvollen Zyklen in Anspruch nehmen.
- Einige Unternehmen benötigen einen stabilen Zugriff mit hohem Durchsatz und niedriger Latenz. Dazu gehören die Unterhaltungs- und Medienbranche, das verarbeitende Gewerbe und die Verarbeitung von Finanztransaktionen. Wenn dies Ihre Zielkunden sind, ist Zuverlässigkeit ihr Hauptanliegen.

In all diesen Fällen könnten Kunden ein ansonsten gesundes SaaS-Angebot wahrnehmen, wenn der Netzwerkzugriff nicht reibungslos funktioniert. Wenn Netzwerke zu einem Hindernis werden, unterstützt dies Ihr Geschäftsszenario nicht. Wenn Ihre Kunden nicht zuverlässig auf die von Ihnen angebotenen Dienste zugreifen können, ist das Wertversprechen Ihrer SaaS-Angebote gleich Null.

Deine Rolle verstehen

Ihre Rolle bei der Unterstützung von Geschäftszielen hängt davon ab, wer Sie sind, was Ihre spezifischen Einzel- und Teamziele sind, wer Ihre Kunden sind und was für sie wichtig ist. Auch wenn Sie nicht Teil eines Teams sind, das normalerweise mit Kunden interagiert, müssen Sie sich Gedanken darüber machen, wer diese sind und was sie benötigen. Ingenieur- und Entwicklungsteams müssen sich auch mit ihren internen Kunden befassen, insbesondere mit denen, mit denen sie regelmäßig interagieren. In der Regel sind dies die Betriebs- und Kundenerfolgsteams.

Wenn Sie Teil einer Vertriebsorganisation sind, ist es wichtig, dass Sie mit den Produkt- und Entwicklungsteams über Netzwerke kommunizieren, auch wenn es sich dabei um ein scheinbar reines Technologiethema handelt. Teilen Sie Einblicke in die Struktur des Zielmarktes. Kommunizieren Sie Schwachstellen und die Bedürfnisse Ihrer bestehenden und potenziellen Kunden und Partner. Teilen Sie Daten und Anekdoten über verpasste Chancen, das prognostizierte Wachstum pro Segment und Ereignisse. Stellen Sie Fragen, die die Fähigkeit Ihres Unternehmens, das Geschäftswachstum zu unterstützen, in Frage stellen. Dies erhöht die Anzahl der Geschäftschancen und verbessert die langfristige Rentabilität Ihres Unternehmens. Letztlich hilft dies Ihrer Organisation, future Expansion und Entwicklung zu finanzieren.

Wenn Sie Teil der technischen Abteilung sind, sollten Sie sich mit der Geschäftsstrategie Ihres Unternehmens vertraut machen, bevor Sie versuchen, eine Lösung zu entwerfen. Die Ausrichtung auf die Geschäftsstrategie hilft Ihnen dabei, die richtigen Kennzahlen für die Bewertung der verschiedenen Netzwerkzugriffsoptionen auszuwählen. Sie kann auch verhindern, dass Ihr Netzwerk im Zuge des Wachstums Ihres Unternehmens teuer und umfangreich umgestaltet werden muss. Business Alignment hilft Ihrem Team, die Ressourcen zu sichern und zu behalten, die für future Herausforderungen benötigt werden. Die Mitarbeiterzahl Ihres Teams, das Budget für die berufliche Weiterentwicklung oder der Zugang zu Spitzentechnologie hängen von Ihrer Fähigkeit ab, die Ausrichtung Ihres Unternehmens nachzuweisen. Im Idealfall können Sie nachweisen, wie Ihre Entscheidungen zum Geschäftserfolg des Unternehmens beigetragen haben. Daher empfehlen wir Ihnen, den Entscheidungsprozess einschließlich der Auswahlkriterien für Kennzahlen zu erfassen. Überprüfen Sie Ihre Kennzahlen regelmäßig, um sicherzustellen, dass sie mit den Geschäftszielen übereinstimmen. Dies kann Ihrem Team helfen, die Anerkennung zu erhalten, die

es verdient. Regelmäßige Überprüfungen helfen auch dabei, sicherzustellen, dass Ihr Team keine Entscheidungen auf der Grundlage von Annahmen oder veralteten, historischen Gründen trifft.

Die Liste der Kennzahlen in den folgenden Abschnitten ist für den Netzwerkzugriff relevant:

- Produkt- und Geschäftskennzahlen
- Technische Kennzahlen, die Netzwerkentscheidungen beeinflussen

Dieser Leitfaden verwendet durchweg eine Teilmenge dieser Kennzahlen, um Ihnen zu helfen, die optimalen Netzwerkzugriffsansätze für Ihre SaaS-Angebote zu identifizieren. Wählen Sie die Kennzahlen aus, die für Ihr Unternehmen am wichtigsten und relevantesten sind, und bewerten Sie dann die Ansätze auf der Grundlage dieser Kennzahlen.

Produkt- und Geschäftskennzahlen, die Netzwerkentscheidungen beeinflussen

Produkt- und Vertriebsteams bewerten anhand von Erfolgskriterien, ob sie die Geschäftsziele erreichen. In diesem Abschnitt werden die Produkt- oder Geschäftskennzahlen beschrieben, die durch die Entscheidungen, die Ihr Unternehmen über den Netzwerkzugang trifft, positiv oder negativ beeinflusst werden können.

Verwenden Sie diese Kennzahlen und Fragen zur Selbsteinschätzung, um zu beurteilen, wie Ihr Netzwerkzugriffsansatz mit Ihrer Geschäftspositionierung und Marktstrategie übereinstimmt. Anhand dieser Bewertung können Sie feststellen, ob Ihre aktuellen Netzwerkentscheidungen die Marktdifferenzierung, die Wettbewerbsvorteile und die Bedürfnisse der Zielgruppe Ihres Unternehmens unterstützen.

Dieser Abschnitt enthält Kennzahlen und Fragen zur Selbsteinschätzung zu den folgenden Themen:

- Geschäftsmodell und Marktpositionierung
- Gesamter adressierbarer Markt, Akquisitionsrate neuer Kunden, Wachstum und Skalierbarkeit
- Kundenerlebnis und Kundenbindung
- Effizienz und finanzielle Leistungsfähigkeit
- Einhaltung gesetzlicher Vorschriften und Risikomanagement
- Strategie der Partner

Geschäftsmodell und Marktpositionierung

Diese Kennzahlen beziehen sich auf die Position Ihres Unternehmens auf dem Markt, einschließlich Wettbewerbsdifferenzierung, Marktreichweite und Markenwahrnehmung. Es ist wichtig, dass Sie die Abstimmung zwischen dem Netzwerkzugriffsansatz und dem Geschäftsmodell beurteilen. Führen Sie eine Bewertung durch, unabhängig davon, ob es sich um eine abonnementbasierte, nutzungsbasierte, kostenlose, gestaffelte, Marketplace-Version, API-First oder White-Label-Lösung handelt. Stellen Sie sicher, dass das Modell die Ziele des Unternehmens und die Ziele der Kunden unterstützt.

Highscore-Kriterien

Der Netzwerkzugriffsansatz passt sich nahtlos dem Geschäftsmodell an. Es erleichtert die Einführung und Bereitstellung des Dienstes. Es unterstützt die langfristige finanzielle Tragfähigkeit des Geschäftsmodells, und die Kostenstruktur ist mit dem erwarteten Wachstum vereinbar. Es minimiert jegliche Probleme für Kunden oder Partner bei der Annahme des Angebots. Dies verbessert die Benutzererfahrung und fördert eine breitere Akzeptanz des Dienstes.

Indikatoren mit niedrigem Punktestand

Der gewählte Ansatz für den Netzwerkzugang entspricht nicht dem Geschäftsmodell, das er unterstützen sollte. Die Kostenstruktur und die Vorlaufzeit bis zur Einführung behindern die Akzeptanz auf dem Zielmarkt. Die laufenden Infrastruktur- und Betriebskosten stehen potenziellen Gewinnen im Wege. Dies verhindert das Geschäftswachstum und macht es schwierig, in der vorgesehenen Größenordnung zu arbeiten. Alternativ könnten die Eigenschaften des Netzwerkzugangsansatzes Kunden aus regulatorischen Gründen daran hindern, den Service in Betracht zu ziehen.

Fragen zur Selbsteinschätzung

- Was sind die Kostenauswirkungen des ausgewählten Netzwerkzugriffskonzepts für die anfängliche Bereitstellung und die laufende Bereitstellung? Was sind die festen und variablen Kosten des Ansatzes?
- Kann der Netzwerkzugriffsansatz effektiv und effizient skaliert werden, um den Wachstumsanforderungen des Geschäftsmodells gerecht zu werden? Berücksichtigen Sie die Größe der einzelnen Mieter und die Anzahl der neu hinzugekommenen Mieter.
- Führt der Netzwerkzugriffsansatz zu technischen oder betrieblichen Einschränkungen, die die Flexibilität oder Anpassungsfähigkeit des Geschäftsmodells einschränken könnten?

- Wie passt die Vorlaufzeit für den Netzwerkzugang zur schnellen Markteinführung, die das Geschäftsmodell erfordert?

Gesamter adressierbarer Markt, Akquisitionsrate neuer Kunden, Wachstum und Skalierbarkeit

Es ist wichtig, dass Sie die Auswirkungen von Netzwerkentscheidungen auf die Fähigkeit des Unternehmens abschätzen, in neue Märkte zu expandieren, Kunden effektiv zu gewinnen und die betriebliche Skalierbarkeit aufrechtzuerhalten. Diese Faktoren wirken sich auf die Konversionsraten aus. Sie beeinflussen auch, ob der Netzwerkzugriffsansatz die Expansion in wichtige Marktsegmente unterstützt oder Sie darauf beschränkt, nur bestimmte Kundentypen zu bedienen.

Kriterien mit hoher Punktzahl

Der Netzwerkzugriffsansatz hilft dem Unternehmen, einen erheblichen Teil des Zielmarktes zu erreichen, oder er kann effektiv mit anderen Netzwerkansätzen kombiniert werden, um die Marktreichweite zu vergrößern. Dieser Ansatz sollte nur minimalen zusätzlichen Integrationsaufwand erfordern. Dieser Ansatz unterstützt kurze Vorlaufzeiten für die Einführung, einen schnellen Markteintritt und eine schnelle Expansion. Es ermöglicht eine hohe Anzahl parallel Bereitstellungen. Die Integration ist für Kunden unkompliziert, wodurch die Hindernisse für die Einführung gesenkt und das Kundenerlebnis verbessert werden. Dieser Ansatz minimiert die Betriebskosten, schont die Betriebskapazität und unterstützt Wachstumsprognosen.

Indikatoren mit niedrigem Punktestand

Der Netzwerkzugriffsansatz unterstützt nur einen kleinen Teil des Zielmarktes oder eignet sich hauptsächlich für Nischensegmente, denen in der Geschäftsstrategie keine Priorität eingeräumt wird. Er ergänzt andere, bereits unterstützte Netzwerkzugangsansätze nicht effektiv. Die Bereitstellungszeiten hinken den Marktanforderungen hinterher, was die Marktexpansion und die Gewinnung neuer Kunden einschränkt. Das Bereitstellungsmodell ist sequentiell, was das Risiko von Serviceengpässen bei steigender Nachfrage erhöht. Komplexe Integrationsprozesse schrecken potenzielle Kunden ab, was sich negativ auf die Akquisitionsrate und die Konversionsraten auswirkt. Ein erheblicher betrieblicher Aufwand verringert die Betriebskapazität der Organisation. Dies wird zu einem Hindernis für das prognostizierte Wachstum.

Beurteilen Sie anhand dieser Indikatoren, ob die Einführung eines neuen Netzwerkzugangsansatzes dem Unternehmen helfen kann, seine strategischen Geschäftsziele zu erreichen. Überlegen Sie, ob

der neue Netzwerkzugriffsansatz zu neuen Produktabhängigkeiten führen oder Betriebsressourcen verbrauchen könnte, ohne die gewünschten Ergebnisse zu erzielen.

Fragen zur Selbsteinschätzung

- Gibt es Lücken im aktuellen Ansatz, die Sie daran hindern, größere Segmente des Zielmarktes zu erreichen?
- Was ist die Mindestanzahl an sich nicht überschneidenden, standardisierten Netzwerkzugangsansätzen, die Sie unterstützen sollten, um 70-90% des Zielmarktes abzudecken?
- Welche Reichweite ermöglichen die einzelnen Netzwerkzugriffsansätze, und wie hoch sind die damit verbundenen Steigerungen wichtiger Kennzahlen wie Infrastrukturkosten, Betriebszyklen und Abhängigkeit von Experten?
- Wie passen die Bereitstellungsmöglichkeiten und Leistungsgrenzen der Netzwerkinfrastruktur zu den Wachstumserwartungen in Ihren Zielmärkten?
- Schafft die Netzwerkintegration Markteintrittsbarrieren für neue Kunden? Wie können diese behoben werden, um die Konversionsraten zu verbessern?
- Wie wirkt sich der betriebliche Aufwand für die Netzwerkverwaltung auf Ihre Wachstumskapazität und Skalierbarkeit aus?
- Welche Strategien können Sie umsetzen, um die Vorlaufzeiten für die Netzwerkbereitstellung zu verkürzen und die Marktexpansion und Kundengewinnung zu verbessern?
- Gibt es Abhängigkeiten von Expertenressourcen, die die Implementierung oder Integration in Kundenökosysteme verzögern würden?

Kundenerlebnis und Kundenbindung

Die Kennzahlen in diesem Abschnitt helfen Ihnen dabei, die Fähigkeit Ihres Unternehmens zu verstehen, Kunden zu gewinnen und vor allem zu binden. Das Verständnis des Zusammenhangs zwischen Netzwerkzugangsansätzen und Kundenzufriedenheit kann Produkt- und Entwicklungsteams dabei helfen, datengestützte Entscheidungen zu treffen.

Kriterien mit hoher Punktzahl

Der Netzwerkzugriffsansatz ist zuverlässig und einfach zu verwalten. Er trägt zu einer hohen Kundenzufriedenheit (CSAT) und einem hohen Net Promoter Score (NPS) bei. Diese Werte deuten auf einen guten Ruf und eine starke Kundenbindung hin. Dank der nahtlosen Integration in die

bestehenden Ökosysteme Ihrer Kunden ist die Akzeptanz gering und die Abhängigkeit von Experten ist gering. Ihr Unternehmen erfüllt durchgängig die Service Level Agreements (SLAs), wodurch das Vertrauen der Kunden und die vertraglichen Verpflichtungen gestärkt werden. Da Kunden von stabilen und zuverlässigen Services profitieren, haben Sie eine hohe Kundenbindung.

Indikatoren mit niedriger Punktzahl

Eine schwierige Integration und ein inkonsistenter Zugang zu Diensten führen häufig zu Frustration und negativem Feedback bei den Kunden. Dies schadet dem Ruf der Marke. Neukunden scheitern daran, von kostenlosen Tarifen oder Testabonnements auf kostenpflichtige Dienste umzusteigen, weil sie von Experten abhängig sind oder weil die Onboarding- und Integrationszeiten zu lang sind. Häufige Nichterfüllung SLAs führt zu finanziellen Strafen und einem Verlust an Glaubwürdigkeit, wodurch die Kundenbindungsrate möglicherweise verringert wird.

Fragen zur Selbsteinschätzung

- Wie wirkt sich die Netzwerkleistung (wie Geschwindigkeit, Verfügbarkeit und Latenz) direkt auf die CSAT- und NPS-Ergebnisse aus? Welche spezifischen Netzwerkverbesserungen könnten diese Werte erhöhen?
- Wie wirken sich aktuelle Metriken zur Netzwerklatenz und Verfügbarkeit auf die anfängliche Benutzererfahrung und die Akzeptanzraten aus? Welche spezifischen Verbesserungen der Netzwerkleistung sind erforderlich, um diese Kennzahlen zu optimieren?
- Gibt es wiederkehrende Probleme mit Netzwerkkonfigurationen oder Sicherheitseinstellungen, die die Integration für Neukunden erschweren? Wie können Sie diese Prozesse rationalisieren?
- Wie wirkt sich die einfache Konfiguration des Netzwerkzugriffs auf das Onboarding-Erlebnis neuer Benutzer aus? Gibt es spezielle Netzwerkzugangspunkte oder Vorlaufzeiten, die optimiert werden können, um die ersten Benutzereindrücke zu verbessern?
- Was sind die Herausforderungen bei der Automatisierung der Bereitstellung von Netzwerkdiensten für neue Kunden? Wie können Sie diesen Prozess anpassen, um die Skalierbarkeit und Zuverlässigkeit zu verbessern?
- Analysieren Sie die Hauptursachen der jüngsten SLA-Verstöße. Hatten sie mit Netzwerkkonfiguration, Kapazitätsplanung oder Problemen mit externen Anbietern zu tun?
- Wie oft führen Netzwerkprobleme dazu, dass Sie SLA-Verpflichtungen nicht einhalten? Was sind die häufigsten Netzwerkausfälle?
- Welche Verbesserungen der Netzwerkleistung haben sich in der Vergangenheit am stärksten positiv auf die Kundenzufriedenheit ausgewirkt?

Effizienz und finanzielle Leistungsfähigkeit

In dieser Kategorie werden die Aspekte der finanziellen Gesundheit und Rentabilität Ihres Unternehmens bewertet, z. B. Kosteneffizienz, langfristige Rentabilität, Rentabilität, Kapitalrendite (ROI) und Gesamtbetriebskosten (TCO). Durch die Rationalisierung des Netzwerkbetriebs durch Standardisierung können Sie die Betriebskosten und die Wartungskosten senken. Dies unterstützt die Wachstumsziele Ihres Unternehmens.

Highscore-Kriterien

Die Kostenstruktur des Netzwerkzugangsansatzes ist gut auf das Geschäftsmodell abgestimmt. Es unterstützt nachhaltiges Wachstum, und die erheblichen Kosteneinsparungen, die Sie erzielen, erhöhen die Rentabilität. Ein effizienter Netzwerkzugang ermöglicht ein schnelles Kunden-Onboarding, was die Zeit bis zur Wertschöpfung verkürzt und die Marktdurchdringung beschleunigt. Dadurch wird der Umsatzerfassungszyklus unmittelbar verkürzt.

Indikatoren mit niedrigem Punktestand

Kunden wenden sich an Ihre Konkurrenz, um die Bereitstellung ihrer Anwendungen und Dienste zu beschleunigen. In Ihrem Unternehmen sind die Betriebskosten aufgrund komplexer und vielfältiger Netzwerkkonfigurationen und verlängerter Vorlaufzeiten gestiegen. Die Kostenstruktur und das Geschäftsmodell sind falsch aufeinander abgestimmt, was zu hohen Vorabkosten für Dienste auf Abonnementbasis führen kann. Umständliche Onboarding-Prozesse verringern die Marktdurchdringung und verzögern die Umsatzrealisierung.

Fragen zur Selbsteinschätzung

- Was sind die aktuellen Vorlaufzeiten für die Einführung neuer Services und wie wirken sie sich auf die Markteinführungszeit und die Umsatzrealisierung aus?
- Wie effektiv reduzieren standardisierte Netzwerkoperationen die Gemeinkosten und Wartungskosten?
- Sind Expertenressourcen erforderlich, um die erste Integration erfolgreich abzuschließen, täglich zu arbeiten, Probleme zu beheben oder Änderungen zu implementieren?
- Wie nachhaltig sind aktuelle Netzwerkinvestitionen in Bezug auf technologische Fortschritte? Investieren Sie in zukunftssichere Technologien, die den prognostizierten Marktentwicklungen entsprechen?
- Wie effektiv verteilen und verfolgen Sie die Kosten im Zusammenhang mit dem Netzwerkverkehr und der Nutzung durch einzelne Mieter?

Einhaltung gesetzlicher Vorschriften und Risikomanagement

Es ist von grundlegender Bedeutung, die Einhaltung netzwerkbezogener Vorschriften zu überprüfen. Dies bestätigt, dass Sie legal arbeiten und das Vertrauen Ihrer Kunden aufrechterhalten können. Die Standardisierung des gesamten Netzwerkbetriebs vereinfacht den Compliance-Prozess und fördert die Konsistenz in verschiedenen Jurisdiktionen und Regionen. Diese Maßnahmen helfen Ihnen, Ihre Dienste zu erweitern.

Highscore-Kriterien

Der Netzwerkbetrieb hält sich konsequent und unkompliziert an gesetzliche Standards, was zur Marktexpansion beiträgt, Reibungsverluste bei der Einführung verringert und das Vertrauen der Kunden stärkt. Die nachgewiesene Einhaltung wichtiger regulatorischer Rahmenbedingungen wie dem Digital Operational Resilience Act (DORA) und dem National Institute of Standards and Technology (NIST) hilft Ihnen dabei, Kunden zu gewinnen, die auf die Einhaltung gesetzlicher Vorschriften achten. Ein kontinuierlicher Einblick in Ihren Compliance-Status reduziert den Zeitaufwand für die Durchführung eines Audits.

Indikatoren mit niedriger Punktzahl

Lücken in der Netzwerk-Compliance führen zu Problemen bei der Einführung von Diensten, Verzögerungen bei der Einführung von Diensten, rechtlichen Problemen und potenziellen Bußgeldern. Diese Herausforderungen führen zu verzögerten oder stornierten Expansionsplänen in neue Märkte. Es ist schwierig, in verschiedenen Jurisdiktionen einheitliche Compliance-Praktiken aufrechtzuerhalten, was sich auf die betriebliche Effizienz und den Ruf am Markt auswirkt.

Fragen zur Selbsteinschätzung

- Wie gut entspricht Ihr Netzwerkbetrieb den geltenden behördlichen oder branchenspezifischen Richtlinien? Was hat Ihr jüngstes Compliance-Audit ergeben?
- Wie gewährleisten Sie die Einhaltung neuer Vorschriften in den Bereichen digitale Sicherheit und Netzwerksicherheit?
- Wie effektiv ist Ihr Dokumentations- und Berichtsprozess, um die Anforderungen der verschiedenen Aufsichtsbehörden zu erfüllen?
- Über welche Risikomanagementstrategien verfügen Sie, um potenzielle Compliance-Risiken zu identifizieren und zu beheben, bevor sie zu rechtlichen Herausforderungen führen?
- Welches Maß an Compliance-Schulung und Sensibilisierung benötigen Ihre Netzwerkmanagement-Teams, um Ihre Konzepte für den Netzwerkzugriff zu unterstützen?

Strategie der Partner

Beurteilen Sie, wie gut der Netzwerkzugriffsansatz zu einem Ökosystem anerkannter Partner, Plattformen und Marktplätze passt. Dies ist besonders wichtig, wenn Ihre Wachstumsstrategie von der Skalierung durch Partner abhängt.

Kriterien mit hoher Punktzahl

Der Netzwerkzugriffsansatz ist in Ihr Partner-Ökosystem integriert. Die Kostenstruktur passt gut zu den Geschäftsmodellen Ihrer wichtigsten Partner. Partner verfügen über die erforderlichen Netzwerkkenntnisse für eine nahtlose Integration Ihrer SaaS-Angebote und können dauerhaften Zugriff und Funktionalität bereitstellen.

Indikatoren mit niedrigem Punktestand

Der gewählte Netzwerkzugriffsansatz erfordert spezielle Fähigkeiten, Ressourcen oder Geräte, die knapp oder schwer zu beschaffen sind. Es unterscheidet sich von den standardmäßigen Netzwerkzugriffsprotokollen, die üblicherweise von Plattformen und Marktplätzen verwendet werden. Dies führt zu einer unvorhersehbaren Kostenstruktur, die schwer zu vereinbaren ist. Der Netzwerkzugriffsansatz ist nicht auf die Geschäftsmodelle Ihrer wichtigsten Partner abgestimmt.

Fragen zur Selbsteinschätzung

- Was sind die Kostenauswirkungen des Netzwerkzugangsansatzes für Partner? Wie passen diese Kosten zu ihren Geschäftsmodellen? Welche Seite der Integration trägt den Großteil der Kosten und wie viele Betriebszyklen müssen investiert werden?
- Gibt es beim Netzwerkzugriffsansatz Hindernisse für die Integration oder Wartung, die sich auf die Partnerbeziehungen oder die Skalierbarkeit des Ökosystems auswirken könnten?
- Wie kann der Netzwerkzugriffsansatz optimiert werden, um die Kompatibilität und die einfache Integration im gesamten Ökosystem zu verbessern?

Technische Kennzahlen, die Netzwerkentscheidungen beeinflussen

Wie Produkt- und Vertriebsteams verwenden auch Entwicklungsteams Erfolgskriterien, um zu beurteilen, ob sie die Geschäftsziele erreichen. Diese Kennzahlen unterscheiden sich jedoch und konzentrieren sich auf die Fähigkeit des Teams, Sicherheits- und Compliance-Anforderungen zu entwickeln, zu betreiben und zu erfüllen. In diesem Abschnitt werden technische Kennzahlen

beschrieben, die durch die Entscheidungen, die Ihr Unternehmen über den Netzwerkzugriff trifft, positiv oder negativ beeinflusst werden können.

Verwenden Sie diese Kennzahlen und Fragen zur Selbsteinschätzung, um Ihren aktuellen Netzwerkzugriffsansatz anhand Ihrer Geschäftsanforderungen und technischen Möglichkeiten zu bewerten. Diese Bewertung hilft Ihnen dabei, Lücken in Ihrer Architektur zu identifizieren und Verbesserungen zu priorisieren, die Ihren strategischen Zielen entsprechen. Durch die regelmäßige Überprüfung dieser Kriterien können Sie sicherstellen, dass Ihre Netzwerkzugriffsstrategie weiterhin sowohl den Bedürfnissen Ihrer Kunden als auch den Wachstumsplänen Ihres Unternehmens entspricht.

Dieser Abschnitt enthält Kennzahlen und Fragen zur Selbsteinschätzung für die folgenden Kategorien und Themen:

Entwicklungsmetriken im Zusammenhang mit dem Netzwerkzugriff für SaaS-Angebote

Dieser Abschnitt enthält die folgenden Kennzahlen:

- Codequalität und Leistung des Entwicklungsteams
- Technischer Schuldenabbau
- Skalierbarkeit, Kapazität und Leistung

Bereitstellungshäufigkeit, Bereitstellungszeit und Sprint-Geschwindigkeit

Um die Effizienz des Entwicklungszyklus zu optimieren, ist es wichtig, dass Sie den Einfluss der Netzwerk-Stack-Bereitstellung auf die Sprint-Geschwindigkeit verstehen.

Kriterien mit hoher Punktzahl

Die Bereitstellung von Netzwerk-Stacks ist optimiert und automatisiert und erfordert nur minimale manuelle Eingriffe. Dies hat keinen wesentlichen Einfluss auf die Sprint-Geschwindigkeit. Die Bereitstellung und erneute Bereitstellung von Netzwerk-Stacks kann von jedem Teammitglied durchgeführt werden. Dadurch werden Engpässe und Abhängigkeiten von spezialisierten Ressourcen reduziert.

Indikatoren mit niedrigem Punktestand

Für die Bereitstellung des Netzwerk-Stacks ist eine große Anzahl von Storypoints erforderlich. Dies deutet auf einen komplexen und zeitaufwändigen Prozess hin, der die Entwicklung neuer Funktionen beeinträchtigt. Eine häufige Neubereitstellung des Netzwerk-Stacks ist mit einem erheblichen Zeit- und Kostenaufwand verbunden. Aufgaben zur Netzwerkbereitstellung erfordern spezialisiertes technisches Fachwissen, was zu Engpässen führt und den Entwicklungszyklus verlangsamt.

Fragen zur Selbsteinschätzung

- Welche manuellen Schritte, falls vorhanden, sind im Bereitstellungsprozess erforderlich. Wie wirken sie sich auf die Häufigkeit und Dauer der Bereitstellung aus?
- Wie werden Rollbacks im Falle von Bereitstellungsfehlern behandelt? Wie wirken sie sich auf die Bereitstellungshäufigkeit und die Wiederherstellungszeit aus?
- Wie viele Storypoints sind für die Bereitstellung des Netzwerk-Stacks erforderlich, wenn Sie neue Umgebungen einrichten?
- Wie viel zusätzliche Kosten und Zeitaufwand sind mit der häufigen Neubereitstellung des Netzwerk-Stacks während des Entwicklungsprozesses verbunden?
- Hängt die Bereitstellung des Netzwerk-Stacks von spezialisiertem Fachwissen ab oder handelt es sich um eine Aufgabe, die von jedem Teammitglied bewältigt werden kann?

Flexibilität und Bereitstellung von Funktionen

Der Netzwerkzugriffsansatz kann die Fähigkeit des Entwicklungsteams beeinflussen, Innovationen zu entwickeln und neue Funktionen effizient einzusetzen.

Kriterien mit hoher Punktzahl

Der Netzwerkzugriffsansatz bietet die Flexibilität, die für eine schnelle und reibungslose Bereitstellung von Funktionen erforderlich ist. Er unterstützt eine Vielzahl von Kommunikationsprotokollen, unidirektionaler und bidirektionaler Kommunikation sowie Nachrichtengrößen. Es schränkt Entwicklungsprozesse oder Innovationen nicht wesentlich ein.

Indikatoren mit niedrigem Punktestand

Der Netzwerkzugriffsansatz schränkt die Fähigkeit des Teams ein, neue Funktionen einzuführen, da es an unterstützten Kommunikationsprotokollen mangelt, die Nachrichtengröße nicht flexibel ist oder von bestimmten Technologien und entsprechenden Expertenressourcen abhängig ist. Dies kann zu langsameren Entwicklungszyklen führen und die Weiterentwicklung des Dienstes behindern.

Fragen zur Selbsteinschätzung

- Wie wirkt sich der Netzwerkzugriffsansatz auf die Agilität des Teams bei der Entwicklung und Bereitstellung neuer Funktionen aus?
- Gibt es Einschränkungen beim Netzwerkzugriffsansatz, die die Unterstützung bestimmter Kommunikationsprotokolle oder -technologien einschränken?
- Wie erleichtert oder begrenzt der Ansatz die Integration neuer Technologien und Innovationen in den Dienst?
- Wie wirkt sich der Netzwerkzugriffsansatz auf die Entwicklungszeitpläne und die Produkt-Roadmap aus?

Ausfallrate ändern

Der von Ihnen gewählte Netzwerkzugriffsansatz kann sich auf die Änderungsfehlerrate bei der Bereitstellung neuer Dienste oder Funktionen auswirken. Eine bessere Kontrolle bedeutet oft mehr Flexibilität, erhöht aber auch das Risiko von Fehlkonfigurationen, z. B. bei der Verwaltung einer komplexen Routing-Konfiguration.

Kriterien mit hoher Punktzahl

Sie können Änderungen am Netzwerk-Stack mit minimalem Ausfallrisiko implementieren. Es gibt ausreichend Testmechanismen, effiziente Rollback-Mechanismen und eine effektive Überwachung hilft Ihnen, Probleme schnell zu identifizieren und zu lösen.

Indikatoren mit niedrigem Punktestand

Der Netzwerkzugriffsansatz ist anfällig für Fehler bei Änderungen. Es gibt begrenzte Testmöglichkeiten, komplizierte Bereitstellungsstrategien oder unzureichende Überwachungs- und Fehlerbehebungsmöglichkeiten. Für die Teilnahme an den Sitzungen zur Problembehandlung sind mehrere Parteien erforderlich. Dies kann zu erhöhten Ausfallzeiten führen und die Verfügbarkeit des SaaS-Angebots verringern.

Fragen zur Selbsteinschätzung

- Welche Maßnahmen wurden getroffen, um das Risiko eines Änderungsfehlers bei der Aktualisierung des Netzwerkstapels zu verringern?
- Gibt es gründliche Test- und Validierungsprozesse?
- Wie schnell kann das System nach einer fehlgeschlagenen Änderung wiederhergestellt werden? Gibt es einen effizienten Rollback-Prozess?
- Gibt es proaktive Überwachungs- und Warnsysteme, um Probleme während und nach Änderungen am Netzwerk-Stack schnell zu erkennen und zu beheben?
- Wie hoch ist die Ausfallrate bei historischen Änderungen bei Netzwerk-Stack-Implementierungen? Welche Lehren wurden aus früheren Vorfällen gezogen?
- Wie erleichtert oder begrenzt der Netzwerkzugriffsansatz die Umsetzung von Änderungen? Minimiert der Ansatz Betriebsunterbrechungen?
- Wie hoch ist das Risiko, dass die Verfügbarkeit des SaaS-Angebots in der Produktionsumgebung beeinträchtigt wird, wenn Sie Änderungen vornehmen, die den Netzwerkzugriffsansatz beinhalten?

Codequalität und Leistung des Entwicklungsteams

Netzwerkzugriffsansätze können sich indirekt auf die Codequalität für SaaS-Angebote auswirken. Mangelnde Standardisierung beim Netzwerkzugriff kann das Entwicklungsteam dazu zwingen, mehrere Integrationsansätze zu unterstützen, was zu einer aufgeblähten Codebasis führen kann. Dies wiederum kann die Fähigkeit des Teams beeinträchtigen, die Tiefe und Kontrolle über die

Codequalität zu entwickeln, die für die Aufrechterhaltung leistungsfähiger Entwicklungsteams erforderlich sind.

Kriterien mit hoher Punktzahl

Dank der Modularität des Codes und der Wiederverwendbarkeit aller unterstützten Netzwerkzugriffsansätze bleibt das Entwicklungsteam konzentriert. Die Netzwerkzugriffsansätze sind mit bestehenden Bereitstellungspipelines und automatisierten Teststrategien kompatibel.

Indikatoren mit niedrigen Punktzahlen

Die Leistung des Entwicklungsteams wird aufgrund des Mehraufwands, der mit der Integration und Wartung zu vieler Netzwerkzugriffsmethoden verbunden ist, beeinträchtigt. Einige Ansätze erhöhen die Komplexität erheblich, führen zu technischen Schulden oder erfordern die Entwicklung von Behelfslösungen, um fehlende oder unzureichende Kapazitäten zu beheben.

Fragen zur Selbsteinschätzung

- Wie verwaltet der Netzwerkzugriffsansatz die Netzwerkvariabilität?
- Müssen Sie zusätzlichen Code für den Umgang mit Verbindungsunterbrechungen entwickeln?
- Lässt sich ein neuer Netzwerkzugriffsansatz nahtlos in bestehende Ansätze integrieren oder erfordert er eine umfangreiche kundenspezifische Entwicklung?
- In welchem Umfang sind Änderungen erforderlich, um ein neues Konzept für den Netzwerkzugang einzuführen? Können die bestehende Codebasis und die automatisierten Tests effektiv genutzt werden?
- Wie einfach oder schwierig ist es, den Dienst mit dem ausgewählten Netzwerkzugriffsansatz bereitzustellen oder erneut bereitzustellen? Kann dies häufig durchgeführt werden? Gibt es Abhängigkeiten von Expertenressourcen?
- Erleichtert oder erschwert der Netzwerkzugriffsansatz die Einhaltung von Kodierungsstandards und bewährten Verfahren?
- Wie wirkt sich der Ansatz auf neue Funktionen oder time-to-market Problembehebungen aus?

Technischer Schuldenabbau

Bei der Bewertung der Auswirkungen eines Netzwerkzugangsansatzes auf die technische Verschuldung sollten dessen Skalierbarkeit, Beobachtbarkeit und Sicherheitsfunktionen berücksichtigt werden.

Kriterien mit hohem Punktestand

Dieser Ansatz rationalisiert effektiv das Infrastrukturmanagement, wenn der Kundenstamm wächst. Er bietet robuste Funktionen zur Beobachtbarkeit. out-of-the-box Dies fördert eine effiziente Überwachung und Wartung.

Indikatoren mit niedrigem Punktestand

Das Konzept des Netzwerkzugangs schützt die Kommunikationskanäle nur unzureichend und es mangelt an ausreichenden Instrumenten für die qualitative metrische Beobachtung. Es könnte auch zusätzliche Entwicklungen im Bereich des Infrastrukturmanagements erfordern, wenn der Kundenstamm zunimmt, oder es könnten Behelfslösungen für Zuverlässigkeitsprobleme erforderlich sein.

Fragen zur Selbsteinschätzung

- Wie beeinflusst der Netzwerkzugriffsansatz die langfristige Skalierbarkeit der Infrastruktur? Ermöglicht er ein nahtloses Wachstum mit minimalen zusätzlichen Investitionen?
- Wie umfassend sind die mitgelieferten Observability-Tools? Ermöglichen sie eine proaktive Überwachung und Problemlösung?
- Was sind die voraussichtlichen Auswirkungen des Netzwerkzugriffsansatzes auf die Wartung und Weiterentwicklung der Codebasis im Laufe der Zeit?
- Lässt sich der Ansatz gut in die bestehende und geplante Infrastruktur integrieren? Sind wesentliche Änderungen oder Ergänzungen erforderlich?

Skalierbarkeit, Kapazität und Leistung

Um festzustellen, ob ein Netzwerkzugriffsansatz für ein SaaS-Angebot geeignet ist, muss unbedingt analysiert werden, wie er bei steigender Nachfrage die optimale Leistung beibehält.

Kriterien mit hoher Punktzahl

Der Netzwerkzugriffsansatz ermöglicht eine nahtlose Erweiterung. Es sorgt für eine geringe Latenz bei der Anforderungsverarbeitung und bewältigt effizient Verkehrsspitzen. Es bietet eine gleichbleibende Leistung unabhängig vom erhöhten Verkehrsaufkommen und setzt dem Wachstum keine betrieblichen Grenzen.

Indikatoren mit niedriger Punktzahl

Der Netzwerkzugriffsansatz lässt sich nicht effektiv skalieren, was möglicherweise auf inhärente Bandbreitenbeschränkungen oder unzureichende Infrastrukturkapazität zurückzuführen ist. Die Bereitstellung und Verwaltung von Ressourcen erhöhen die Komplexität oder schaffen Abhängigkeiten. Die Serviceleistung wird aufgrund der erhöhten Latenz, des Jitters und der Variabilität des Durchsatzes beeinträchtigt, insbesondere bei überlasteten Netzwerkbedingungen.

Fragen zur Selbsteinschätzung

- Wie trägt der Netzwerkzugriffsansatz einer steigenden Anzahl von Mandanten und deren Datenvolumen Rechnung?
- Ist es von Natur aus skalierbar, um future Anforderungen gerecht zu werden?
- Welche Maßnahmen wurden getroffen, um sicherzustellen, dass die Leistung auch in Zeiten mit hohem Verkehrsaufkommen oder bei schnellen Skalierungsereignissen konsistent ist?
- Wie geht der Ansatz mit Netzwerklatenz und Jitter um? Gibt es Mechanismen zur Optimierung des Datendurchsatzes und zur Minimierung von Verzögerungen?
- Kann der Netzwerkzugriffsansatz an unterschiedliche Netzwerkbedingungen angepasst werden? Kann es jedem Kunden ein Single-Tenant-Erlebnis bieten?
- Wie wirkt sich der Netzwerkzugriffsansatz auf die zugrunde liegende Infrastruktur aus? Sind umfangreiche Upgrades oder Änderungen an bestehenden Systemen erforderlich?

Kennzahlen zur betrieblichen Exzellenz im Zusammenhang mit dem Netzwerkzugriff für SaaS-Angebote

Dieser Abschnitt enthält die folgenden Kennzahlen:

- Betriebliche Belastbarkeit und Notfallwiederherstellung
- Überwachung der Service- und Anwendungsleistung

Betriebliche Belastbarkeit und Notfallwiederherstellung

Der Netzwerkzugriffsansatz sollte dem SaaS-Angebot helfen, verschiedenen Arten von Störungen standzuhalten und sich nach Katastrophen schnell zu erholen.

Kriterien mit hoher Punktzahl

Etablierte und getestete Notfallwiederherstellungspläne zeigen durchweg, dass der Netzwerkzugriffsansatz die Anforderungen für die Notfallwiederherstellung erfüllt. Der Netzwerkzugriffsansatz unterstützt Konfigurationen mit hoher Verfügbarkeit und unterstützt automatische, schnelle und zuverlässige Failover-Mechanismen.

Indikatoren mit niedriger Punktzahl

Der Netzwerkzugriffsansatz macht es schwierig, eine kohärente Notfallwiederherstellungsstrategie zu entwickeln. Sie beobachten längere Wiederherstellungszeiten nach Störungen. Häufige Betriebsausfälle der Netzwerkinfrastruktur beeinträchtigen die Servicebereitstellung.

Fragen zur Selbsteinschätzung

- Wann fand die letzte Notfallwiederherstellungsübung statt und was waren die Ergebnisse?
- Wie lange dauert es, kritische Dienste nach einer Unterbrechung wiederherzustellen? Welcher Teil der Netzwerkinfrastruktur muss neu bereitgestellt werden?
- Welche Verbesserungen können an der Netzwerkinfrastruktur vorgenommen werden, um Ihre Notfallwiederherstellungspläne zu optimieren?
- Sind Redundanzen für die kritischsten Netzwerkkomponenten vorhanden?
- Haben Sie die mögliche Neubereitstellung der Netzwerkinfrastruktur nach einem kritischen Ausfall automatisiert?
- Wie unterstützt der Netzwerkzugriffsansatz Fehlertoleranz und Zuverlässigkeit? Gibt es integrierte Mechanismen zur Behandlung von Netzwerkunterbrechungen und zur Aufrechterhaltung der Datenintegrität?

Überwachung der Service- und Anwendungsleistung

Der Netzwerkzugriffsansatz kann sich auf die Tools zur Leistungsüberwachung auswirken, mit denen der optimale Betrieb und die optimale Betriebszeit überprüft werden. Je nach Dienst haben Sie möglicherweise Zugriff auf Messwerte auf niedriger Ebene (z. B. Paketabwurfraten) oder auf übergeordneter Ebene (z. B. Sitzungsdauer). Low-Level-Metriken bieten detaillierte technische Einblicke in das Netzwerkverhalten, können jedoch komplex zu interpretieren sein. Im Gegensatz dazu bieten Metriken auf höherer Ebene oft eine direktere und einfachere Möglichkeit, die allgemeine Benutzererfahrung zu messen. Dies liegt daran, dass sie die Auswirkungen der zugrunde liegenden Netzwerkbedingungen zu klaren Indikatoren für die Servicequalität zusammenfassen.

Kriterien mit hoher Punktzahl

Umfassende Überwachungstools, die Einblicke nahezu in Echtzeit bieten, sind sofort verfügbar. Sie verfügen über automatisierte Warn- und Reaktionssysteme, die Leistungsprobleme beheben. Sie können potenzielle Serviceengpässe oder -ausfälle vorhersagen, bevor sie sich auf Benutzer auswirken.

Indikatoren mit niedrigem Punktestand

Häufige Betriebsunterbrechungen oder Leistungsprobleme treten auf, ohne dass etwas beobachtet oder darauf reagiert wird. Der mangelnde Einblick in die Serviceleistung führt zu einer langsamen Reaktion auf Leistungsengpässe. Zur Behebung von Problemen mit der Netzwerkinfrastruktur sind Teams mit mehreren Parteien erforderlich.

Fragen zur Selbsteinschätzung

- Welche Überwachungstools und Kennzahlen zur Netzwerkinfrastruktur sind derzeit verfügbar? Wie effektiv sind sie bei der Erkennung von Serviceanomalien?
- Wie schnell können Sie Leistungsprobleme erkennen und lösen?
- Verfügen Sie über Mechanismen, mit denen potenzielle Leistungsprobleme vorhergesagt werden können?
- Welche Verbesserungen können Sie vornehmen, um die Beobachtungsmöglichkeiten zu verbessern?

Sicherheits- und Governance-Kennzahlen im Zusammenhang mit dem Netzwerkzugriff für SaaS-Angebote

Dieser Abschnitt enthält die folgenden Kennzahlen:

- Sicherheit, Compliance und Schwachstellenmanagement

Sicherheit, Compliance und Schwachstellenmanagement

Es ist wichtig, dass Sie die Sicherheitsaspekte des Netzwerkzugriffsansatzes bewerten, einschließlich der Einhaltung von Sicherheitsstandards und des Managements von Sicherheitslücken.

Kriterien mit hoher Punktzahl

Der Netzwerkzugriffsansatz hilft Ihrem Team dabei, Sicherheitsrahmen wie die International Organization for Standardization (ISO) 27001, System and Organization Controls 2 (SOC 2) oder NIST einzuhalten. Es macht es einfach, regelmäßige Sicherheitsaudits durchzuführen. Starke Verschlüsselungs- und Authentifizierungsmechanismen sind vorhanden. Die Netzwerke sind isoliert und nur die erforderlichen Ressourcen werden der Infrastruktur des Kunden zur Verfügung gestellt. Sie können Netzwerkanomalien nahezu in Echtzeit und ohne übermäßigen Aufwand erkennen.

Indikatoren mit niedrigem Punktestand

Der Netzwerkzugriffsansatz ist anfällig für wiederkehrende Sicherheitsverletzungen oder Sicherheitslücken und entspricht nicht den wichtigsten Sicherheitsstandards. Sie beobachten häufig Verzögerungen bei der Erkennung und Reaktion auf Sicherheitsvorfälle.

Fragen zur Selbsteinschätzung

- Gibt es in letzter Zeit Sicherheitslücken im Zusammenhang mit ausgewählten Netzwerkzugriffsansätzen, und was haben wir daraus gelernt?
- Inwiefern entspricht Ihr Netzwerkzugriffsansatz den globalen Sicherheitsstandards?
- Wie lange dauert es, Sicherheitsbedrohungen zu erkennen und darauf zu reagieren? Wie unterstützt oder schränkt der Netzwerkzugriff diese Fähigkeit ein?
- Wie häufig werden Sicherheitsbewertungen der Netzwerkzugangsansätze durchgeführt? Können Sie gängige Tools verwenden, um die Sicherheit des Netzwerkzugriffsansatzes zu bewerten, oder ist spezielle Software erforderlich?
- Welches Sicherheitsniveau ist dem Netzwerkzugriffsansatz inhärent und wie entspricht er den bewährten Verfahren der Branche und den gesetzlichen Anforderungen?

Überblick über AWS Netzwerkdienste für SaaS-Angebote

In diesem Abschnitt werden die AWS Netzwerkdienste beschrieben, auf die in diesem Handbuch verwiesen wird. Außerdem werden ihre Funktionen verglichen und Sicherheitsaspekte für jeden Dienst beschrieben.

In diesem Abschnitt werden folgende Themen behandelt:

- AWS Netzwerkdienste
- Vergleich der Servicekapazitäten
- Sicherheitsmerkmale und Überlegungen

AWS Netzwerkdienste

Die folgenden werden in diesem Handbuch regelmäßig behandelt. AWS-Services

AWS PrivateLink

AWS PrivateLinkist ein Cloud-nativer Dienst, der den Zugriff auf Ihr SaaS-Angebot ermöglicht, wenn Ihre Kunden bereits in der AWS Cloud. Ihr Kunde stellt über eine VPC-Schnittstelle eine Verbindung zum SaaS-Angebot her. Dies ist eine Endpunkt-Netzwerkschnittstelle, die in einem oder mehreren Subnetzen des Kunden bereitgestellt wird. AWS-Konto In den Szenarien in diesem Handbuch wird der Datenverkehr über den VPC-Endpunkt der Schnittstelle geleitet und erreicht einen Network Load Balancer in Ihrem Konto. Der Network Load Balancer leitet den Datenverkehr an die SaaS-Anwendung weiter, die Sie als Endpunktdienst registriert haben. Über Ressourcen-VPC-Endpunkte AWS PrivateLink können Sie auch auf andere Ressourcen wie Datenbanken zugreifen.

Amazon VPC Lattice

Amazon VPC Lattice ist ein Anwendungsnetzwerk-Service, der SaaS-Anbietern hilft, ihre Dienste Kunden, die in mehreren VPCs Ländern tätig sind, sicher und effizient anzubieten. AWS-Konten Kunden greifen über VPC Lattice auf Ihr SaaS-Angebot zu, das konsistente Netzwerkkonnektivität, robuste Zugriffskontrollen und erweitertes Verkehrsmanagement bietet. In diesen Szenarien fließt der Datenverkehr über VPC Lattice zu Ihren registrierten Anwendungsdiensten. Es bietet skalierbare und sichere Kommunikation, unabhängig davon, welchen Rechendienst Sie verwenden.

VPC-Peering

VPC-Peering ist eine Netzwerkverbindung zwischen zwei virtuellen privaten Clouds (VPCs), die den Verkehr zwischen ihnen mithilfe von privaten IPv4 Adressen oder IPv6 Adressen weiterleitet. VPC-Peering wird in der Regel zwischen vertrauenswürdigen Entitäten verwendet, z. B. zwischen Entitäten innerhalb derselben Organisation. Ihr Kunde erstellt eine Peering-Anfrage an einen von Ihnen. VPCs Wenn Sie sie akzeptieren, kann der Verkehr zwischen beiden Seiten VPCs in beide Richtungen fließen. Dieser Verbindungsansatz zeichnet sich durch seine Einzigartigkeit aus, da er eine direkte Kommunikation zwischen zwei Personen beinhaltet, VPCs ohne dass ein zwischengeschalteter Dienst oder eine Infrastruktur verwaltet werden muss.

AWS Transit Gateway

AWS Transit Gatewayist ein zentraler Netzwerk-Transit-Hub VPCs, der Verbindungen zu virtuellen privaten Netzwerken (VPN), AWS Direct Connect Gateways, virtuelle Appliances von Drittanbietern in einer VPC und andere Transit-Gateways herstellen kann. Ein Transit-Gateway kann für jeden Anhang eine andere Routentabelle haben. Dies bietet maximale Flexibilität beim Routing und hilft Ihnen, die Netzwerke zu isolieren. Es wird häufig verwendet, um mehrere Geräte VPCs miteinander zu verbinden oder für zentrale Inspektionen.

AWS Site-to-Site VPN

AWS Site-to-Site VPNkann die Internet Protocol Security (IPsec) -Technologie verwenden, um Verbindungen zwischen lokalen Netzwerken, Außenstellen, Fabriken, anderen Cloud-Anbietern und dem AWS globalen Netzwerk herzustellen. Die Verbindung wird von einem virtuellen privaten Gateway oder Transit-Gateway in einer VPC in der AWS Cloud zu einem physischen oder softwarebasierten Kunden-Gateway hergestellt, das sich in der Cloud AWS Cloud, vor Ort oder in der Cloud eines anderen CSP befinden kann. Die Verbindung kann über das Internet oder über eine physische Verbindung erfolgen. AWS Direct Connect Es ist auch möglich, eine beschleunigte Site-to-Site VPN-Verbindung herzustellen, indem Sie AWS Global Accelerator. Eine beschleunigte Verbindung leitet den Datenverkehr an einen AWS Edge-Standort weiter und bietet eine geringere Latenz und eine verbesserte Leistung.

AWS Direct Connect

AWS Direct Connectstellt eine private Hochgeschwindigkeitsverbindung zwischen einem lokalen Rechenzentrum und dem AWS Cloud her. Durch die Umgehung des öffentlichen Internets wird eine zuverlässigere, sicherere und konsistentere Verbindung mit niedriger Latenz zum Direct Connect

ermöglicht. AWS Cloud Kunden stellen eine Verbindung zu einem der Direct Connect Standorte her und wählen dann entweder eine gehostete oder eine dedizierte Verbindung zu AWS. Obwohl dies eine ungewöhnliche Architekturwahl für SaaS-Angebote ist, kann sie sich gut für SaaS-Anbieter eignen, die nur wenige, aber große Unternehmenskunden haben.

Vergleich der Servicekapazitäten

In der folgenden Tabelle sind die unterstützten Funktionen von aufgeführt AWS-Services , die in diesem Handbuch beschrieben werden. Im Folgenden werden die in dieser Tabelle enthaltenen Funktionen beschrieben:

- Überlappende CIDR-Bereiche — Kann zwei oder mehr Netzwerke mit denselben oder sich überschneidenden CIDR-Bereichen verbinden
- Bidirektionale Kommunikation — Kann einen bidirektionalen Kommunikationskanal unterstützen, sodass der SaaS-Nutzer dem SaaS-Anbieter interne Ressourcen wie eine Datenbank zur Verfügung stellen kann
- IPv6— Kann entweder Single IPv6 - oder Dual-Stack unterstützen
- Jumbo-Frame — Kann Jumbo-Frames mit einer Framegröße von bis zu 8.500 Byte unterstützen
- Hybrid-Cloud — Kann eine Verbindung mit einem lokalen Netzwerk unterstützen
- Multi-Cloud — Kann eine Verbindung zwischen Netzwerken verschiedener Cloud-Dienstanbieter unterstützen

Service oder Ansatz	Überlappende CIDR-Bereiche	Bidirektionale Kommunikation	IPv6	Jumbo-Rahmen	Hybride Wolke	Multi-Cloud
VPC-Peering	Nein	Ja	Ja	Ja [5]	Nein	Nein
AWS PrivateLink	Ja	Ja [1]	Ja	Ja	Nein [6]	Nein
Amazon VPC Lattice	Ja	Ja [1]	Ja	Ja	Nein [6]	Nein

AWS Transit Gateway	Nein	Ja	Ja	Ja	Ja [3]	Ja [3]	Ja
AWS Site-to-Site VPN	Nein	Ja	Ja	Nein	Ja	Ja	
AWS Direct Connect	Nein	Ja	Ja	Ja [2]	Ja	Ja	
Öffentlicher Internetzugang [4]	Nicht zutreffend	Nein	Ja	Ja	Ja	Ja	

1. Mit VPC-Ressourcen in Amazon VPC Lattice
2. Nur für private und virtuelle Transitschnittstellen
3. Mit Site-to-Site VPN oder AWS Direct Connect Anhängen
4. Als allgemeiner Begriff für AWS Ressourcen, die eine Anwendung öffentlich zugänglich machen, wie z. B. ein Application Load Balancer
5. Nur für Peering-Verbindungen innerhalb einer AWS-Region
6. Möglich durch eine bereits bestehende Layer-3-Verbindung zwischen den Umgebungen

Sicherheitsmerkmale und Überlegungen

In der folgenden Tabelle werden die Sicherheitsfunktionen von beschrieben AWS-Services , die in diesem Handbuch behandelt werden.

- Authentifizierungsmethoden — So können Sie sicherstellen, dass nur Ihre Kunden eine Verbindung zu Ihrem Service herstellen können. Eine weitere Authentifizierungsebene für eingehende Anfragen ist in der Regel immer noch erforderlich, insbesondere in Umgebungen mit gemeinsam genutzten Mandanten.
- Verschlüsselung bei der Übertragung — Beschreibt, ob die Verschlüsselung bei der Übertragung standardmäßig bereitgestellt wird. Systemeigene Verschlüsselung beschreibt

eine Verschlüsselung, die für den gesamten Datenverkehr innerhalb VPCs VPCs, zwischen oder zwischen Rechenzentren AWS sorgt. Zusätzliche Verschlüsselung beschreibt eine Verschlüsselung, die Sie kontrollieren und die durch den jeweiligen Dienst gestoppt werden kann.

Dienst oder Ansatz	Mittel der Authentifizierung	Verschlüsselung während der Übertragung
VPC-Peering	Sie initiieren eine Peering-Anfrage an die AWS-Konto VPC Ihres Kunden oder akzeptieren eine Anfrage, die dieser initiiert. Siehe Annehmen oder Ablehnen einer VPC-Peering-Verbindung.	Nur native Verschlüsselung
AWS PrivateLink	Sie wählen aus, AWS-Konten welche Endpunkte für Ihren Service erstellen dürfen. Diese Konten werden als zulässige Hauptbenutzer bezeichnet. Siehe Verbindungsanfragen annehmen oder ablehnen.	Nur native Verschlüsselung
Amazon VPC Lattice	Sie teilen sich einen VPC-Lattice-Dienst oder ein Servicenetzwerk mit Ihren Kunden. AWS-Konten Siehe Teilen Sie Ihre VPC Lattice-Entitäten.	Native Verschlüsselung und ergänzende TLS-Verschlüsselung
AWS Transit Gateway	Ihr Kunde erstellt anhand seiner Anfrage eine Anfrage für einen Peering-Anhang AWS-Konto, oder Sie initiieren die Anfrage. Siehe Transit-Gateway-Peering-Anlagen in Amazon VPC Transit Gateways.	Systemeigene Verschlüsselung und zusätzliche IPsec Verschlüsselung mit einem VPN-Anhang

AWS Site-to-Site VPN	Sie verwenden IPsec Pre-Shared Keys oder ein privates Zertifikat auf dem Gerät des Kunden. Siehe Optionen für die AWS Site-to-Site VPN Tunnelauthentifizierung.	Zusätzliche IPsec Verschlüs selung
AWS Direct Connect	Ihr Kunde erstellt eine virtuelle Schnittstellenanfrage von seinem AWS-Konto. Siehe Direct Connect virtuelle Schnittstellen und gehostete virtuelle Schnittstellen.	Zusätzliche Layer-2-V erschlüsselung an ausgewähl ten Standorten möglich. Siehe Direct Connect Standorte.
Öffentlicher Internetzugang [1]	Eine benutzerdefinierte Authentifizierung ist erforderl ich.	Zusätzliche TLS-Versc hlüsselung möglich

1. Als allgemeiner Begriff für AWS Ressourcen, die eine Anwendung öffentlich zugänglich machen, wie z. B. ein Application Load Balancer

Bewertung von Netzwerkzugriffsoptionen für SaaS-Angebote

Welche Kennzahlen für Ihr Unternehmen wichtig sind, hängen davon ab, wer Ihre Kunden sind, welche Geschäftsstrategie Sie verfolgen und welche Unternehmensziele Sie verfolgen. In diesem Leitfaden werden Kennzahlen vorgestellt, anhand derer Sie sich für einen Netzwerkzugriffsansatz entscheiden können. Sie sollten jedoch denjenigen Kennzahlen Priorität einräumen, die den individuellen Anforderungen Ihres Anwendungsfalls entsprechen.

In diesem Abschnitt werden folgende Themen behandelt:

Bewertungsmetriken

Einige Kennzahlen sind für alle Organisationen und Anwendungsfälle einheitlich, und wir können Ihnen bei der Bewertung dieser Kennzahlen helfen. Im Folgenden sind diese Metriken aufgeführt:

- Einfache Integration — Wie schnell und einfach können Sie neue Kunden gewinnen?
- Gesamtbetriebskosten (TCO) — Wie sieht die Kostenstruktur aus? Neben den festen und variablen Infrastrukturkosten gibt es auch erhebliche zusätzliche Kostenaspekte im Zusammenhang mit den Betriebskosten, der Abhängigkeit von Experten, den Kosten für die Implementierung von Änderungen und der Einhaltung von Vorschriften. Weitere Informationen finden Sie im Abschnitt Gesamtbetriebskosten.
- Skalierbarkeit — Ist Ihr Netzwerkzugriffsansatz skalierbar, um das Wachstum Ihres Unternehmens zu unterstützen? Die Skalierung Ihres Kundenstamms ist mit wichtigen architektonischen und organisatorischen Überlegungen verbunden. Überlegen Sie, wie Sie skalieren könnten, um 5- bis 100-mal so viele Kunden zu bedienen, wie Sie es heute unterstützen.
- Anpassungsfähigkeit — Können Sie Änderungen einfach implementieren? Zu den Änderungen können eine neue Anwendung, eine neue Funktion, eine andere Plattform oder ein anderes Netzwerk gehören.
- Netzwerkisolierung — Welchen Teil der Netzwerkinfrastruktur stellen Sie Ihren Kunden zur Verfügung? Bieten Sie genau das richtige Maß an Zugriff oder setzen Sie ganze Netzwerke offen? Wenn Sie Netzwerkressourcen frühzeitig isolieren, ist es später einfacher, Sicherheit, Datenschutz und Konformität zu gewährleisten.

- Beobachtbarkeit — Was ist Ihre Fähigkeit, Serviceausfälle oder -beeinträchtigungen zu erkennen? Wie einfach und schnell ist es, das Problem zu identifizieren? Wie schnell (und mit welchem Aufwand) können Sie Ihren Kunden helfen, ihre Fehlerquellen zu verstehen und sie zu lösen?
- Zeit bis zur Reparatur — Was ist die Vorlaufzeit zwischen der Erkennung eines Ausfalls oder einer Verschlechterung des Betriebs und der Wiederaufnahme des Betriebs? Welche Faktoren beeinflussen diese Fähigkeit?

Andere Kennzahlen sind für Ihre Organisation oder Ihr Angebot einzigartig, da sie sich auf Ihre Geschäftsabläufe, Strategie oder Ziele beziehen. Nur Sie können diese Kennzahlen bewerten. Im Folgenden sind diese Metriken aufgeführt:

- Ausrichtung des Geschäftsmodells — Was ist Ihr Geschäftsmodell und wie gut passen individuelle Zugangsansätze dazu?
- Total Addressable Market (TAM) — Was ist Ihr aktueller und future Markt und wie gut wird er durch den Netzwerkzugriffsansatz abgedeckt?
- Kapitalrendite (ROI) — Welche Verbesserungen erwarten Sie in Bezug auf Rentabilität und Margen? Reichen die erwarteten finanziellen Vorteile aus, um Ihren Bedarf an anpassungsfähigen und flexiblen Servicezugängen zu decken?
- Einhaltung gesetzlicher Vorschriften — Welche regulatorischen Anforderungen gelten und in welchem Markt?
- Service Level Agreements (SLAs) — Benötigen Kunden, dass Ihr SaaS-Angebot hochverfügbar ist? Zu welchen Verpflichtungen sind Sie vertraglich verpflichtet?

Gesamtbetriebskosten

In diesem Abschnitt werden die Gesamtbetriebskosten (TCO) untersucht. Dabei handelt es sich um eine der Bewertungsmetriken, anhand derer die Konzepte für den Netzwerkzugriff verglichen werden. Die Gesamtbetriebskosten sind eine zusammengesetzte Kennzahl, die sich aus festen und variablen Infrastrukturkosten, Betriebskosten, Abhängigkeit von Spezialisten, Änderungskosten und Compliance-Kosten zusammensetzt.

Die Gesamtbetriebskosten für jeden Netzwerkzugriffsansatz können je nach Anwendungsfall variieren. Beispielsweise unterscheiden sich die Änderungskosten für einen SaaS-Anbieter mit einem einfachen Web-Service und fünf Mandanten von denen eines SaaS-Anbieters mit einem komplexen, vernetzten Produktportfolio und Hunderten oder Tausenden von Mandanten. Außerdem haben nicht

alle Komponenten das gleiche Gewicht. Beispielsweise ist die Einstellung eines Netzwerkspezialisten oft teurer als die Infrastrukturkosten, die für eine individuelle Bereitstellung Ihres Dienstes anfallen. Verwenden Sie die Werte in der folgenden Tabelle als erste Orientierung und als Bezugspunkt für weitere Diskussionen.

Zugriffsansatz	Feste Infrastrukturkosten	Variable Infrastrukturkosten	Operativer Overhead	Abhängigkeit von Spezialisten	Kosten der Änderung	Kosten der Einhaltung der Vorschriften
VPC-Peering	Keine	Keine	Hoch	Niedrig	Hoch	Mittelschwer
AWS PrivateLink	Niedrig	Niedrig	Niedrig	Keine	Niedrig	Niedrig
Amazon VPC Lattice	Mittelschwer	Mittelschwer	Niedrig	Niedrig	Niedrig	Niedrig
AWS Transit Gateway	Mittelschwer	Mittelschwer	Niedrig	Niedrig	Niedrig	Mittelschwer
AWS Site-to-Site VPN	Medium	Hoch	Hoch	Mittelschwer	Mittelschwer	Niedrig
AWS Direct Connect	Hoch	Mittelschwer	Medium	Hoch	Hoch	Niedrig
Öffentlicher Internetzugang	Niedrig	Hoch	Mittelschwer	Niedrig	Niedrig	Hoch

Kosten VPC VPC-Peering

Mit einer VPC-Peering-Verbindung sind keine direkten Infrastrukturkosten verbunden. Bleibt der Verkehr innerhalb derselben Availability Zone, fallen keine Datenübertragungsgebühren an. Der betriebliche Aufwand kann jedoch erheblich sein, da Verwaltung und Komplexität mit jeder zusätzlichen Peering-Verbindung exponentiell zunehmen. Für die Einrichtung einer Peering-Verbindung sind einige grundlegende Netzwerkkenntnisse ausreichend. Änderungen im Netzwerk lassen sich jedoch nur schwer umsetzen, wenn mehr als eine Handvoll Peering-Verbindungen vorhanden sind. Die Kosten für die Einhaltung der Vorschriften sind etwas höher, da beide Parteien sich gegenseitig eine gesamte VPC und nicht einzelne Dienste anbieten.

AWS PrivateLink Kosten

AWS PrivateLink ist oft eine kostengünstige Lösung mit geringem Betriebskosten. Dies liegt daran, dass der SaaS-Anbieter nur einen Network Load Balancer verwalten muss und der Verbraucher nur VPC-Endpunkte verwalten muss. Sie können Änderungen auf beiden Seiten transparent vornehmen, wodurch die teure und ressourcenintensive organisationsübergreifende Zusammenarbeit reduziert wird. Die Compliance-Kosten sind in der Regel gering, da der SaaS-Anbieter nur die gewünschten Dienste und nicht das gesamte Netzwerk bereitstellt.

Kosten für Amazon VPC Lattice

Amazon VPC Lattice bietet eine ausgewogene Kostenstruktur mit moderaten festen und variablen Infrastrukturkosten. Als vollständig verwaltetes Servicenetzwerk reduziert es den Betriebsaufwand erheblich, indem es die Serviceerkennung, das Verkehrsmanagement und die Zugriffskontrollen für mehrere automatisiert. VPCs Dies vereinfacht im Vergleich zu manuellen Netzwerkkonfigurationen sowohl die anfängliche Bereitstellung als auch die laufende Verwaltung. Sie können Änderungen durch richtlinienbasierte Kontrollen ohne komplexe Routing-Updates implementieren, wodurch die Abhängigkeit von Netzwerkspezialisten verringert wird. Die Compliance-Kosten sind in der Regel niedriger als bei herkömmlichen Netzwerkansätzen, da VPC Lattice durch integrierte Überwachungs- und Protokollierungsfunktionen detaillierte Zugriffskontrollen und umfassende Transparenz bietet. Dies kann es einfacher machen, die Einhaltung gesetzlicher Vorschriften nachzuweisen.

AWS Transit Gateway Kosten

AWS Transit Gateway hat höhere Stunden- und Datenverarbeitungsgebühren als AWS PrivateLink, hat aber einen ähnlichen Betriebsaufwand. Um alle Routing-Tabellen korrekt einrichten zu können, müssen Sie AWS sich mit dem AWS Transit Gateway Service und dem Routing besser auskennen.

Änderungen an der Infrastruktur erfordern möglicherweise Routing- oder DNS-Updates. Die Compliance-Kosten ähneln denen von VPC-Peering, da beide Parteien möglicherweise Teilnetze oder ganze VPCs Netzwerke gegenseitig aussetzen. AWS Transit Gateway Routing-Tabellen müssen ebenfalls mit Vorsicht behandelt werden, da sie von mehreren Benutzern gemeinsam genutzt werden und Sie keinen Datenverkehr zwischen ihnen zulassen dürfen.

AWS Site-to-Site VPN kostet

Da Site-to-Site VPN im Wesentlichen Datenverkehr ins Internet sendet, sind die variablen Kosten aufgrund der Datenübertragungsgebühren im Vergleich am höchsten. Obwohl es sich um einen verwalteten VPN-Dienst (Virtual Private Network) handelt, ist er mit erheblichem Betriebsaufwand verbunden, insbesondere am Kunden-Gateway. Bereitstellung und Betrieb erfordern fortgeschrittene Netzwerkkenntnisse, und Änderungen erfordern häufig Maßnahmen von beiden Seiten. Die Kosten für die Einhaltung der Vorschriften sind in der Regel gering, da Sicherheitsteams IPsec Tunnel häufig ohne zusätzliche Prüfung vorab genehmigen.

AWS Direct Connect Kosten

AWS Direct Connect ist mit den größten festen Infrastrukturkosten verbunden, da es sich um eine private physische Verbindung direkt in die handelt AWS Cloud. Spezialkenntnisse sind erforderlich, um eine Border Gateway Protocol (BGP) -Sitzung (falls erforderlich) einzurichten und zu betreiben, eine VPN-Verbindung zu betreiben und Verkehrstechnik durchzuführen. Dieser Service reduziert den Aufwand für Sicherheitsteams, da er private Konnektivität mit der Option verbindet, zusätzlich über Media Access Control Security (MACsec) und IPsec Verschlüsselung zu verfügen.

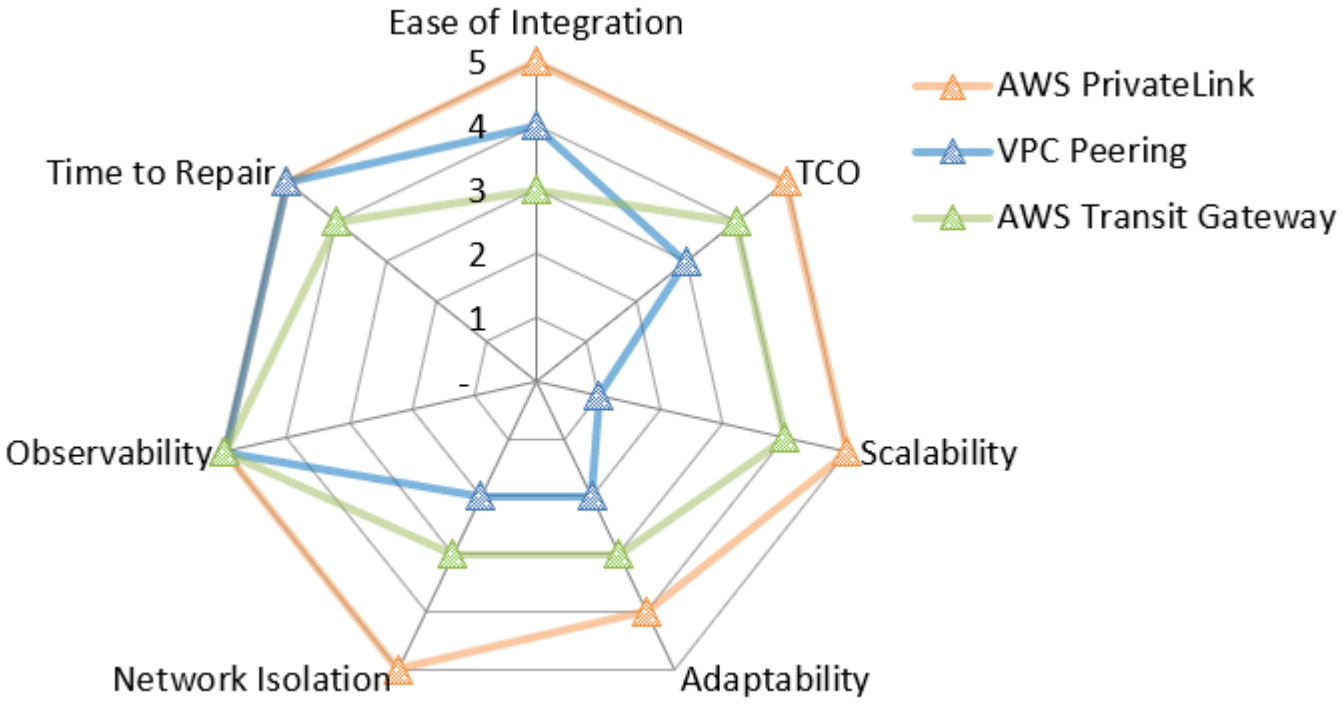
Der öffentliche Internetzugang kostet

Öffentlicher Internetzugang bezieht sich auf die AWS Ressourcen, die Sie verwenden können, um eine Anwendung öffentlich zugänglich zu machen, z. B. einen Application Load Balancer. Bei diesem Ansatz fallen variable Kosten im Zusammenhang mit der Bereitstellung des Zugriffs auf Ihre Dienste an, einschließlich Gebühren für die Datenübertragung ins Internet. Betriebs- und Compliance-Kosten können erheblich sein, da Sie den Dienst dem Internet aussetzen und zusätzliche Sicherheits- und Authentifizierungsmechanismen benötigen. Es ist jedoch kein komplexes Routing erforderlich, und keine der Parteien muss Einzelheiten über die Infrastruktur der jeweils anderen Partei kennen.

Wertübersicht der Netzwerke

Damit Sie einen Überblick über das Gesamtbild haben und fundierte Entscheidungen treffen können, enthält dieser Leitfaden für jedes Szenario eine Wertübersicht im Netzwerk. Da sich die Bewertungen von Szenario zu Szenario unterscheiden, kann derselbe Service in zwei Szenarien unterschiedlich abschneiden. Bei den Value Maps handelt es sich um Radardiagramme, bei denen ein hypothetisches perfektes Ergebnis eine Fünf in allen Kategorien wäre.

Die folgende Abbildung zeigt beispielsweise ein Beispiel für ein Radardiagramm. Es enthält nur die Metriken, bei deren Auswertung wir helfen können. Wir empfehlen Ihnen, Ihre eigene Wertübersicht zu erstellen, die die zusätzlichen Kennzahlen enthält, die nur Sie auswerten können.



Netzwerkzugriffsszenarien für SaaS-Angebote in der AWS Cloud

Dieser Abschnitt behandelt verschiedene Netzwerkzugriffsoptionen für Ihre SaaS-Angebote in der AWS Cloud. Darin werden die Ansätze aus der Sicht Ihrer Kunden erörtert, die möglicherweise Konnektivitätsanforderungen innerhalb der AWS Cloud, von lokalen Rechenzentren oder von anderen Cloud-Dienstanbietern haben (CSPs). Darüber hinaus müssen Sie möglicherweise den Zugriff von verschiedenen Arten von Benutzerumgebungen aus unterstützen.

Für die Entwicklung einer umfassenden Zugriffsstrategie ist es wichtig, die Anforderungen an die Netzwerkkonnektivität in diesen unterschiedlichen Umgebungen zu verstehen. Ihre architektonischen Entscheidungen müssen unterschiedliche Sicherheitsmodelle, Leistungserwartungen und technische Einschränkungen berücksichtigen und gleichzeitig die betriebliche Effizienz gewährleisten. Der richtige Ansatz bietet sichere, zuverlässige Konnektivität, die mit Ihrem Unternehmenswachstum skaliert und sowohl die Implementierungskomplexität als auch den laufenden Verwaltungsaufwand minimiert.

Berücksichtigen Sie bei der Bewertung der Netzwerkzugriffsoptionen, wie sich die einzelnen Ansätze auf Ihre Gesamtbetriebskosten auswirken, einschließlich nicht nur der Infrastrukturkosten, sondern auch der Betriebskosten und der Compliance-Anforderungen. Einige Ansätze zeichnen sich durch Skalierbarkeit aus, können jedoch zu Komplexität führen, während bei anderen die einfache Integration auf Kosten der Netzwerkisolierung in den Vordergrund gestellt wird. Die technischen Fähigkeiten und Ressourcen Ihrer Kunden spielen ebenfalls eine wichtige Rolle bei der Auswahl der am besten geeigneten Lösung.

Für Verbraucher auf dem Markt AWS Cloud AWS PrivateLink bieten Dienste wie z. B. erhebliche Vorteile in Bezug auf Sicherheit und Skalierbarkeit. Verbraucher vor Ort könnten von AWS Direct Connect einer gleichbleibenden Leistung oder von einem Site-to-Site VPN für kostengünstige Konnektivität profitieren. Multi-Cloud-Szenarien erfordern oft eine sorgfältige Abwägung der Interoperabilitätsprobleme, und Sie können Transit-VPC-Architekturen verwenden, um Zugriffsmuster zu standardisieren. In allen Fällen sollte Ihr Design das future Verbraucher- und Verkehrswachstum antizipieren, damit Ihre Netzwerkarchitektur robust und anpassungsfähig bleibt, wenn sich Ihr SaaS-Angebot weiterentwickelt.

Dieser Abschnitt enthält die folgenden Szenarien:

- SaaS-Verbraucher, die auf AWS

- Servicekunden, die vor Ort tätig sind
- SaaS-Verbraucher, die bei anderen Cloud-Dienstanbietern tätig sind
- Unterstützung hybrider Umgebungen

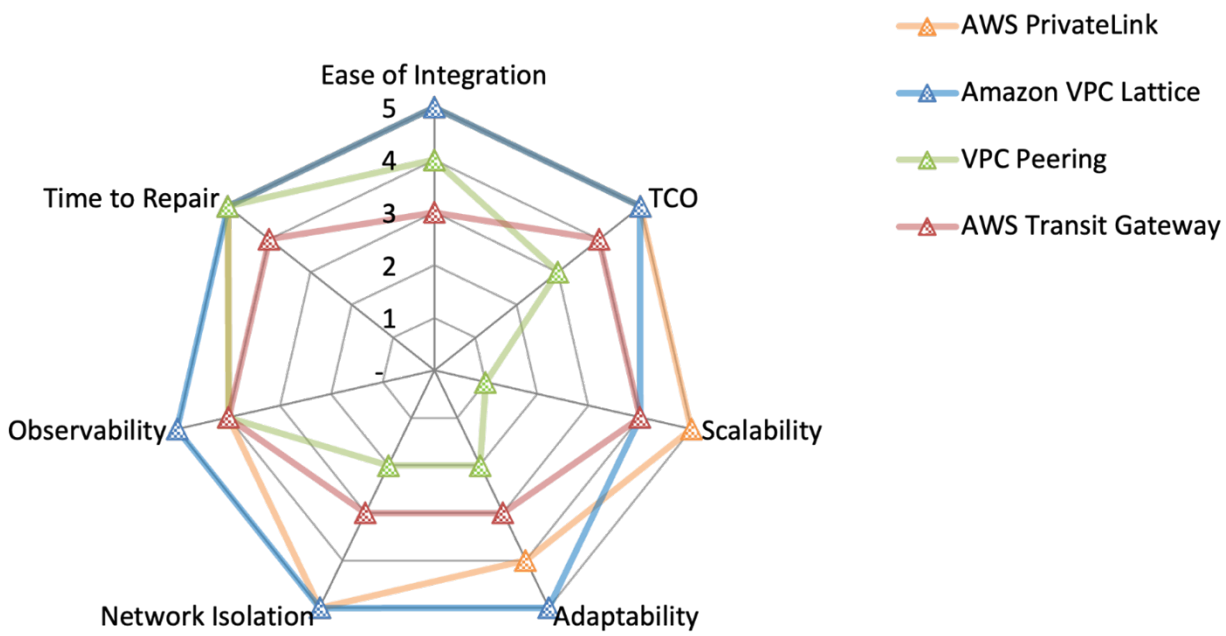
SaaS-Verbraucher, die auf AWS

In diesem Abschnitt werden die Konnektivitätsoptionen für den Fall beschrieben, dass sowohl Sie als auch Ihre Kunden in der AWS Cloud Dieses Szenario bietet die größte Flexibilität, da viele AWS-Services Systeme systemintern integriert sind und beide Parteien Zugriff auf das gesamte AWS-Service Portfolio haben.

In diesem Abschnitt werden die folgenden Ansätze für den Netzwerkzugriff erörtert:

- Integration mit AWS PrivateLink
- Einen Amazon VPC Lattice-Service teilen
- VPC-Peering-Verbindungen erstellen
- Verbindung herstellen VPCs mit AWS Transit Gateway

In der folgenden Netzwerkwerteübersicht wird zusammengefasst, wie jede dieser Optionen bei jeder Bewertungsmetrik abschneidet. Weitere Informationen zu den Bewertungsmetriken finden Sie unter Bewertungskennzahlen in diesem Leitfaden. In der Übersicht steht eine Fünf für das beste Ergebnis, z. B. für die niedrigsten Gesamtbetriebskosten, die beste Netzwerkisolierung oder die kürzeste Reparaturzeit. Weitere Informationen zum Lesen dieses Radardiagramms finden Sie Wertübersicht der Netzwerke in diesem Handbuch.



Das Radardiagramm zeigt die folgenden Werte.

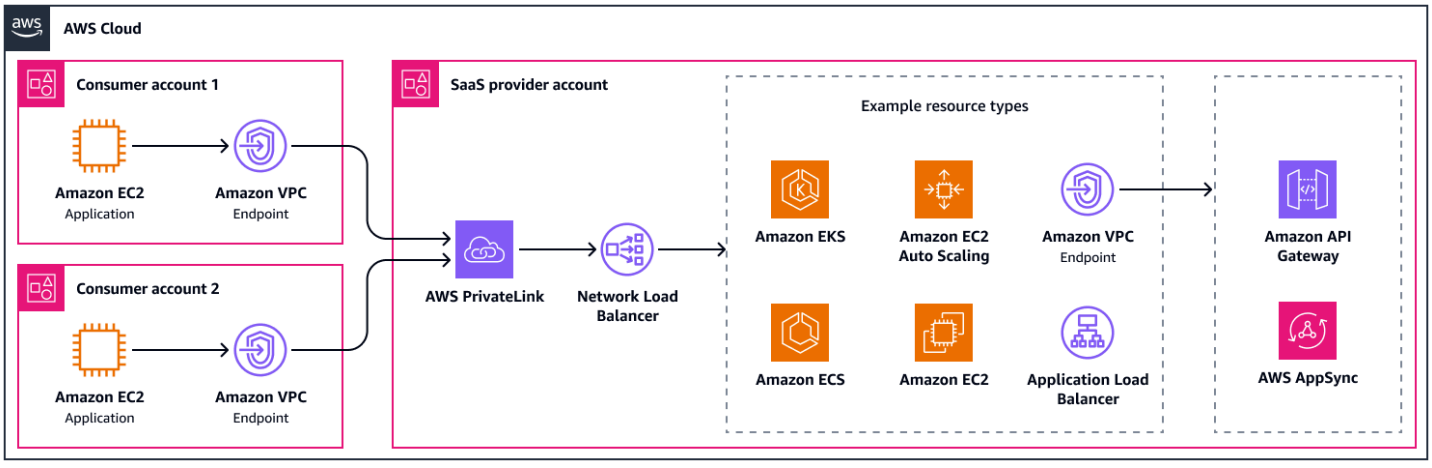
Bewertungsmetrik	AWS PrivateLink	Amazon VPC Lattice	VPC-Peering	AWS Transit Gateway
Einfache Integration	5	5	4	3
Gesamtbetriebskosten	5	5	3	4
Skalierbarkeit	5	4	1	4
Anpassungsfähigkeit	4	5	2	3
Netzwerkisolierung	5	5	2	3
Beobachtbarkeit	4	5	4	4

Bewertung smetrik	AWS PrivateLink	Amazon VPC Lattice	VPC-Peering	AWS Transit Gateway
Zeit zum Reparieren	5	5	5	4

Integration mit AWS PrivateLink

AWS PrivateLinkist die Cloud-nativste Methode zur Integration eines SaaS-Angebots. SaaS-Anbieter können ihre Anwendung entweder hinter einem Network Load Balancer hosten. Der Network Load Balancer lässt sich direkt in einen Application Load Balancer, Amazon Elastic Container Service (Amazon ECS), AmazonElastic Kubernetes Service (Amazon EKS) und Auto Scaling Scaling-Gruppen integrieren. Es ist auch möglich, den Datenverkehr vom Network Load Balancer zu VPC-Endpunkten im SaaS-Anbieterkonto weiterzuleiten. Auf diese Weise können Sie eine API verwenden, um Anwendungen zu erreichen, z. B. über Amazon API Gateway oder AWS AppSync. Wenn Ihre Anwendung Zugriff auf Ressourcen in der Kundenumgebung benötigt, die keinen Lastenausgleich aufweisen, z. B. eine Datenbank, können Sie Ressourcen-VPC-Endpunkte verwenden.

AWS PrivateLink unterstützt eine Bandbreite von bis zu 100 Gbit/s pro Availability Zone. Das folgende Diagramm zeigt eine Grundkonfiguration mit einigen möglichen Integrationen. Es verbindet zwei Verbraucherkonten über das SaaS-Anbieterkonto AWS PrivateLink. Es gibt Dienstendpunkte in den Verbraucherkonten und einen Network Load Balancer im SaaS-Anbieterkonto.



Diese Herangehensweise bietet folgende Vorteile:

- Einfache Integration: Keine Änderungen an der Routentabelle erforderlich
- Einfache Integration: Sie können Endpunktdienste anbieten über AWS Marketplace

- Einfache Integration: VPC-Endpunkte unterstützen benutzerfreundliche DNS-Namen
- Skalierbarkeit: Es kann auf Tausende von SaaS-Verbrauchern skaliert werden
- Anpassungsfähigkeit: Support für überlappende CIDR-Bereiche
- Anpassungsfähigkeit: Support für IPv6
- Anpassungsfähigkeit: Regionalübergreifende Unterstützung
- TCO: AWS PrivateLink ist ein vollständig verwalteter Service, der weniger Betriebsaufwand erfordert
- Netzwerkisolierung: Sicherheitsvorteil für den SaaS, da der Datenverkehr nicht vom SaaS-Anbieter initiiert werden kann
- Netzwerkisolierung: Sicherheitsvorteil für den SaaS-Anbieter, da er nicht ein ganzes Subnetz oder eine VPC offenlegt

Im Folgenden sind die Nachteile dieses Ansatzes aufgeführt:

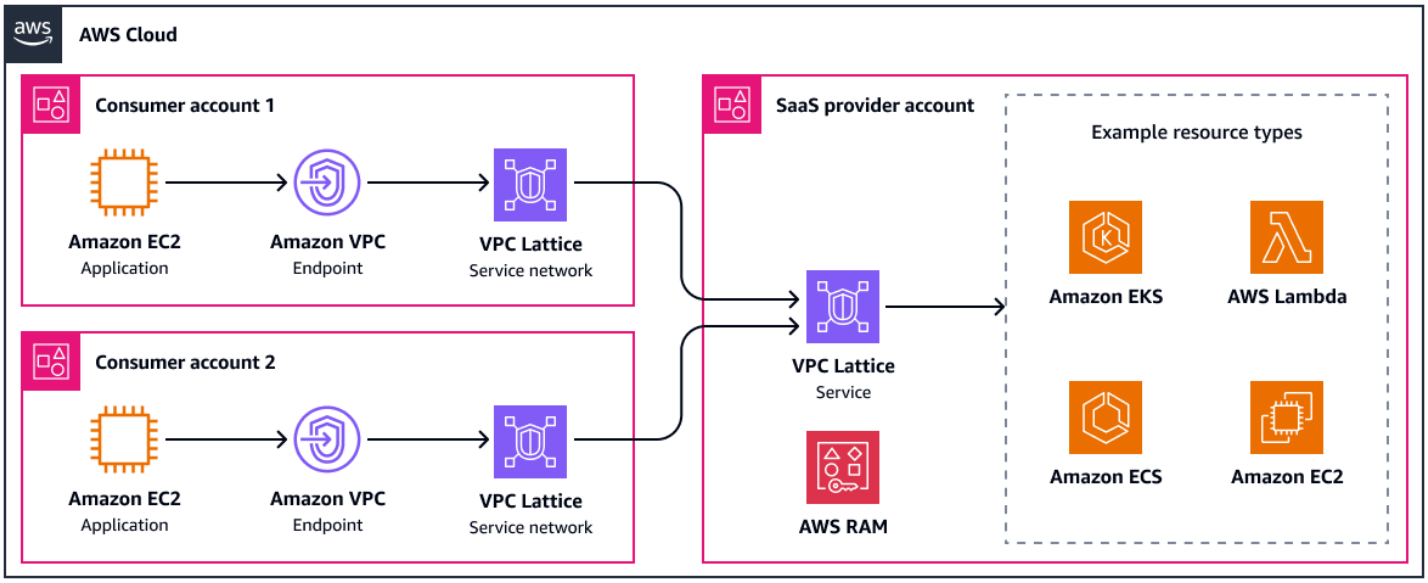
- Anpassungsfähigkeit: SaaS-Anbieter muss dieselben Availability Zones verwenden wie der Verbraucher
- Anpassungsfähigkeit: Support nur für vom Client initiierte Verbindungen, und für die dienstinitiierte Kommunikation sind Ressourcen-VPC-Endpunkte erforderlich
- Anpassungsfähigkeit: Network Load Balancer ist die einzige direkte Integration für AWS PrivateLink

Einen Amazon VPC Lattice-Service teilen

Um Amazon VPC Lattice als Konnektivitätsoption für Ihre SaaS-Anwendung zu verwenden, erstellen Sie zunächst einen oder mehrere VPC Lattice-Dienste, die Ihre SaaS-Anwendungskomponenten darstellen. Sie konfigurieren Listener und Routing-Regeln, um den Datenverkehr an Ihre Back-End-Ziele wie Amazon EC2 EC2-Instances, Container oder Funktionen weiterzuleiten. AWS Lambda Weitere Informationen finden Sie unter Verbinden von Saas-Diensten innerhalb eines VPC-Lattice-Dienstnetzwerks (AWS Blogbeitrag). Vom Konzept her entspricht dies fast der Konfiguration eines Application Load Balancer. Anschließend teilen Sie Ihren SaaS-Dienst sicher mit Kunden AWS-Konten oder Organisationen, indem Sie AWS Resource Access Manager (AWS RAM) verwenden und angeben, über welche Berechtigungen sie verfügen. Nachdem Kunden die gemeinsame Nutzung der Ressourcen akzeptiert haben, können sie Ihren SaaS-Service ihren bestehenden oder neu erstellten VPC-Lattice-Dienstnetzwerken zuordnen, um die Kommunikation zu ermöglichen service-to-service.

Jeder VPC Lattice-Dienst kann bis zu 10 Gbit/s und 10.000 Anfragen pro Sekunde pro Availability Zone unterstützen. Durch die Implementierung von Authentifizierungsrichtlinien können Ihre Kunden genau steuern, welche Dienste und Ressourcen auf die SaaS-Anwendung zugreifen können. Sie können Ressourcen-Gateways verwenden, um auf Ressourcen zuzugreifen, für die eine TCP-Verbindung erforderlich ist. Dies kann beispielsweise ein Amazon EKS-Cluster sein, den Sie verwalten, oder es könnte sich um eine vom Kunden verwaltete Ressource handeln, auf die Ihre Anwendung zugreifen muss. Weitere Informationen zur Verwendung von Ressourcen-Gateways für SaaS-Angebote finden Sie unter Erweitern der SaaS-Funktionen über die AWS-Konten Nutzung der AWS PrivateLink Unterstützung für VPC-Ressourcen (AWS Blogbeitrag).

Das folgende Diagramm zeigt eine VPC-Lattice-Konfiguration auf hoher Ebene mit einigen Beispielintegrationen. Es verwendet vom Kunden verwaltete Servicenetzwerke, um auf die SaaS-Anwendung zuzugreifen.



Diese Herangehensweise bietet folgende Vorteile:

- Einfache Integration: Keine Änderungen an der Routentabelle erforderlich
- Einfache Integration: Serviceerkennung sofort einsatzbereit
- Skalierbarkeit: Es kann auf Tausende von SaaS-Verbrauchern skaliert werden
- Anpassungsfähigkeit: Support für überlappende CIDR-Bereiche
- Anpassungsfähigkeit: Support für IPv6
- Anpassungsfähigkeit: Lässt sich als AWS VPC-Lattice-Dienst in jeden Rechendienst integrieren
- Gesamtbetriebskosten: VPC Lattice ist ein vollständig verwalteter Service, der weniger Betriebsaufwand erfordert

- TCO: Integrierter Lastenausgleich mit erweitertem Datenverkehrs-Routing
- Netzwerkisolierung: Präzise Autorisierung mit Authentifizierungsrichtlinien
- Netzwerkisolierung: Sicherheitsvorteil für den SaaS, da der Datenverkehr nicht vom SaaS-Anbieter initiiert werden kann
- Netzwerkisolierung: Sicherheitsvorteil für den SaaS-Anbieter, da Sie nicht ein ganzes Subnetz oder eine VPC offenlegen

Im Folgenden sind die Nachteile dieses Ansatzes aufgeführt:

- Anpassungsfähigkeit: Support nur für vom Client initiierte Verbindungen, und für dienstinitiierte Kommunikation sind Ressourcen-Gateways erforderlich
- Anpassungsfähigkeit: Keine regionsübergreifende Unterstützung

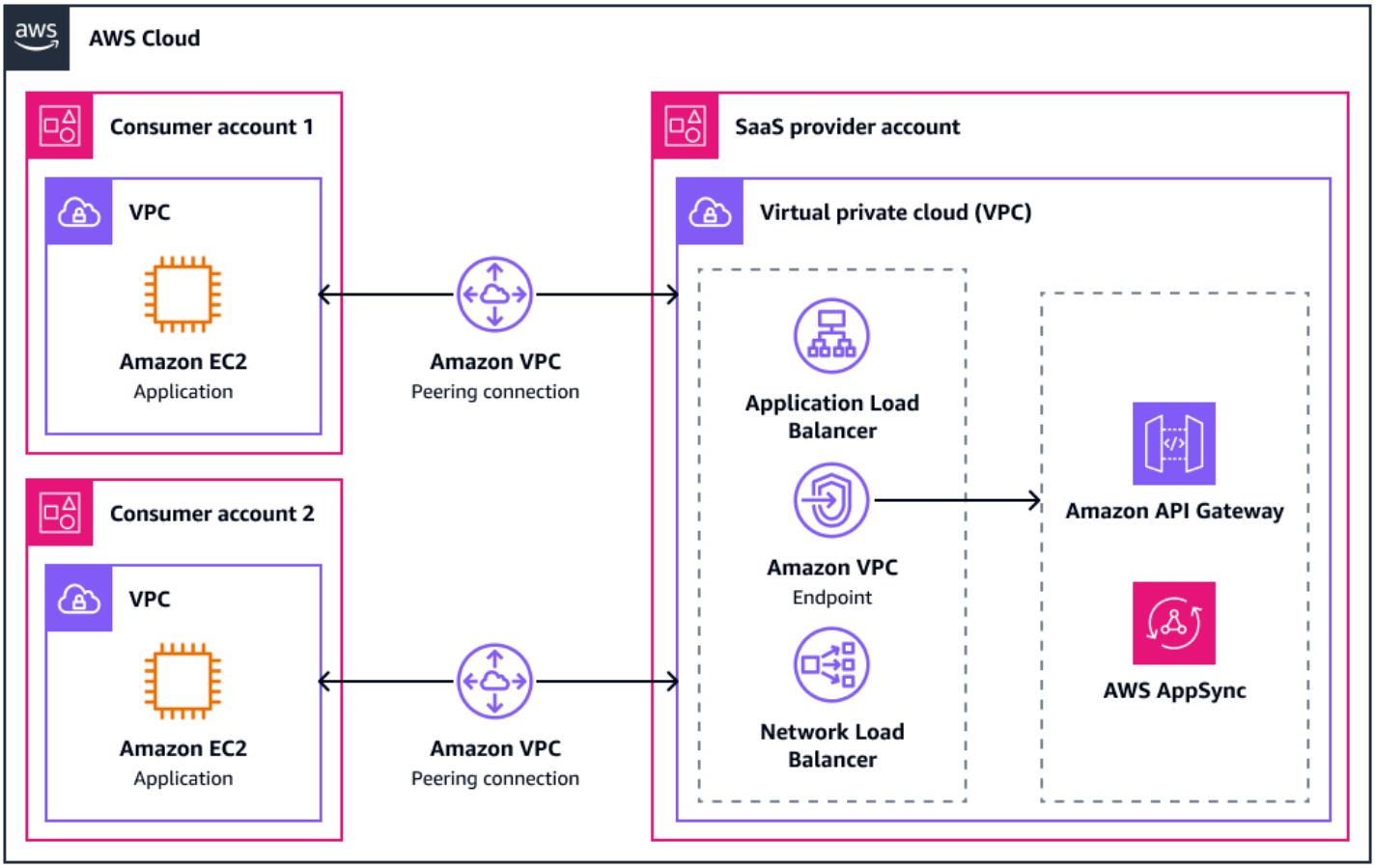
VPC-Peering-Verbindungen erstellen

Wenn Sie VPC-Peering verwenden, um die VPC des SaaS-Anbieters mit der VPC des Verbrauchers zu verbinden, können beide Parteien Verbindungen initiieren. Dies erfordert die korrekte Konfiguration von Sicherheitsgruppen, Firewalls und Netzwerkzugriffskontrolllisten () in beiden Konten. NACLs Andernfalls könnte unerwünschter Datenverkehr über die Peering-Verbindung in das Netzwerk gelangen. Sie können Sicherheitsgruppen verwenden, um auf Sicherheitsgruppen von VPCs Peered zu verweisen. Dies kann Ihnen helfen, den Zugriff auf Ihre Anwendung zu kontrollieren, da Sicherheitsgruppen, die eine Zulassungsliste enthalten, eine explizitere und detailliertere Zugriffskontrolle bieten als IP-Adressen, die auf der Zulassungsliste stehen.

Mit VPC-Peering kann das SaaS-Angebot über einen Dienst oder eine Ressource erreicht werden, die in der VPC bereitgestellt werden. Die meisten SaaS-Anwendungen befinden sich hinter einem Application Load Balancer oder Network Load Balancer. AWS AppSync Private APIs oder Amazon API Gateway Private APIs sind weitere gängige Einstiegspunkte für SaaS-Anwendungen, da sie über eine Peering-Verbindung über Schnittstellen-VPC-Endpunkte als Ziel dienen können.

Nachdem Sie eine Peering-Verbindung hergestellt haben, müssen Sie die Routing-Tabellen für beide Konten aktualisieren, um die VPCs Peering-Verbindung als nächsten Hop für den jeweiligen CIDR-Bereich zu definieren. Diese Lösung wird nur für SaaS-Anbieter mit wenigen Verbrauchern empfohlen, da die Verwaltung mehrerer Peering-Verbindungen schnell zu komplex wird.

Das folgende Diagramm zeigt eine Grundkonfiguration mit einigen möglichen Integrationen. VPCs in zwei Verbraucherkonten besteht eine Peering-Verbindung mit einer VPC im SaaS-Anbieterkonto.



Diese Herangehensweise bietet folgende Vorteile:

- Zeit bis zur Reparatur: Es gibt keine einzige Fehlerquelle für die Kommunikation
- Skalierbarkeit: Keine Bandbreitenbeschränkungen gegenüber VPC-Peering
- Gesamtbetriebskosten: Keine Kosten für die Peering-Verbindung oder den Verkehr über die Peering-Verbindung innerhalb derselben Availability Zone
- Gesamtbetriebskosten: Keine zu verwaltende Infrastruktur
- Anpassungsfähigkeit: Support für IPv6
- Anpassungsfähigkeit: Interregionales Peering wird unterstützt

Im Folgenden sind die Nachteile dieses Ansatzes aufgeführt:

- Anpassungsfähigkeit: Keine Unterstützung für transitives Routing
- Anpassungsfähigkeit: Keine Unterstützung für überlappende CIDR-Bereiche
- Skalierbarkeit: Eingeschränkte Skalierbarkeit (maximal 125 Peering-Verbindungen pro VPC)

- Gesamtbetriebskosten: Die Komplexität nimmt mit jeder weiteren Peering-Verbindung exponentiell zu
- Gesamtbetriebskosten: Mehraufwand aufgrund der Verwaltung von Routing-Tabellen, der Peering-Verbindungen selbst, der Sicherheitsgruppenregeln und der Verkehrsinspektion
- Netzwerkisolierung: Strenge Sicherheitskontrollen sind erforderlich, da VPCs beide Parteien vollständig gefährdet sind

Verbindung herstellen VPCs mit AWS Transit Gateway

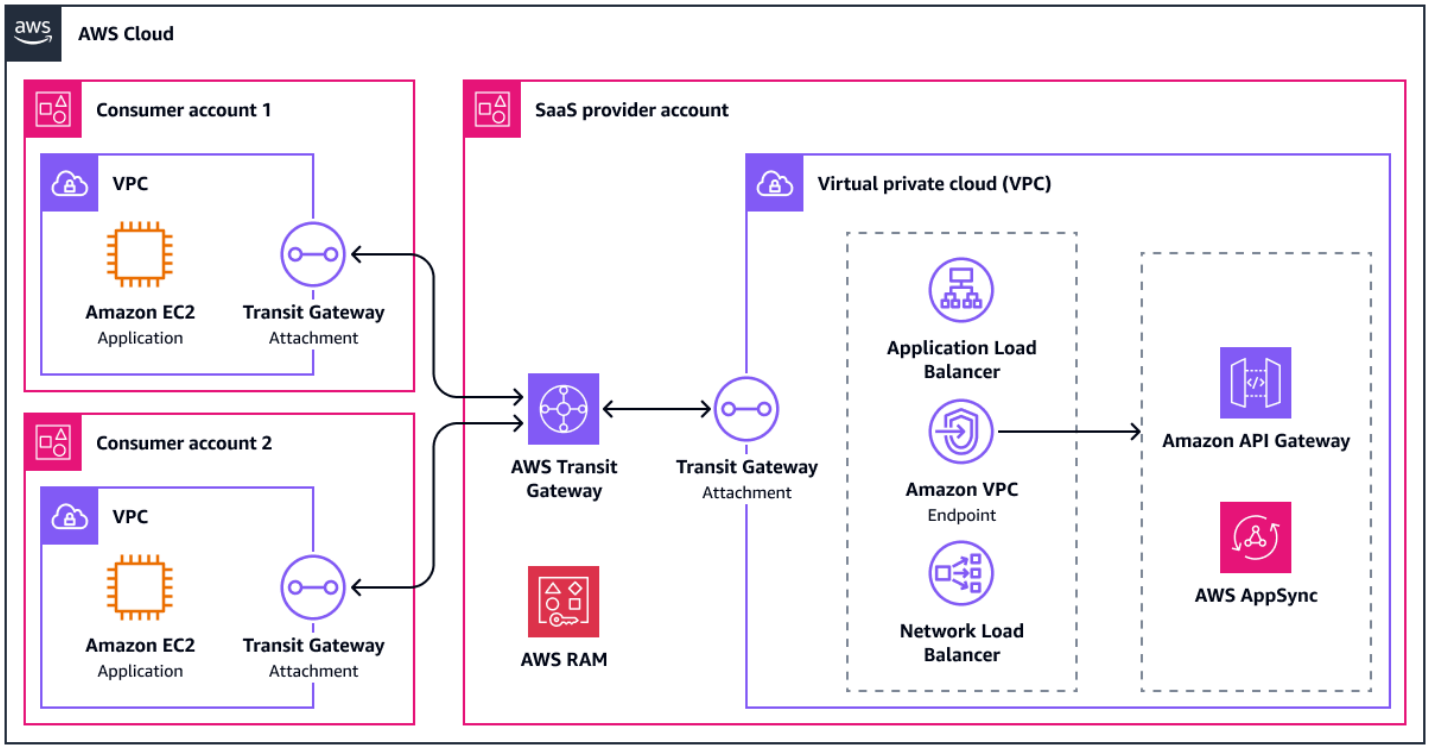
Wenn Sie eine Verbindung VPCs herstellen AWS Transit Gateway, erstellt es VPC-Anlagen und stellt Netzwerkschnittstellen in den Subnetzen jeder Availability Zone bereit, die den Verkehr zur und von der VPC weiterleiten sollen. Es wird empfohlen, in jeder Availability Zone ein eigenes /28 Subnetz für den VPC-Anhang einzurichten. Weitere Informationen finden Sie unter Bewährte Entwurfsmethoden für Amazon VPC Transit Gateways. VPCs Sie benötigen eine aktualisierte Routentabelle, um Verkehr über die bereitgestellte Netzwerkschnittstelle zu senden, und die Transit Gateway Gateway-Routentabellen müssen entsprechend aktualisiert werden. In einer Konfiguration mit mehreren Mandanten möchten Sie, dass die VPC des SaaS-Anbieters eine Route zu allen Verbrauchern hat. VPCs Der Verbraucher VPCs sollte nur eine Route zur VPC des SaaS-Anbieters haben.

Transit Gateway ist von Haus aus hochverfügbar. Es unterstützt die Überwachung mit VPC Flow Logs, und die maximale Bandbreite für einen Transit Gateway Gateway-Anhang beträgt 100 Gbit/s pro Availability Zone. Wie beim VPC-Peering ermöglicht dieser Ansatz die VPC-Sicherheitsgruppenreferenzierung, wodurch die Zugriffskontrolle zwischen den Umgebungen vereinfacht wird.

Es gibt zwei Hauptoptionen, um Verbraucher mit Ihrem SaaS-Angebot mit Transit Gateway zu verbinden.

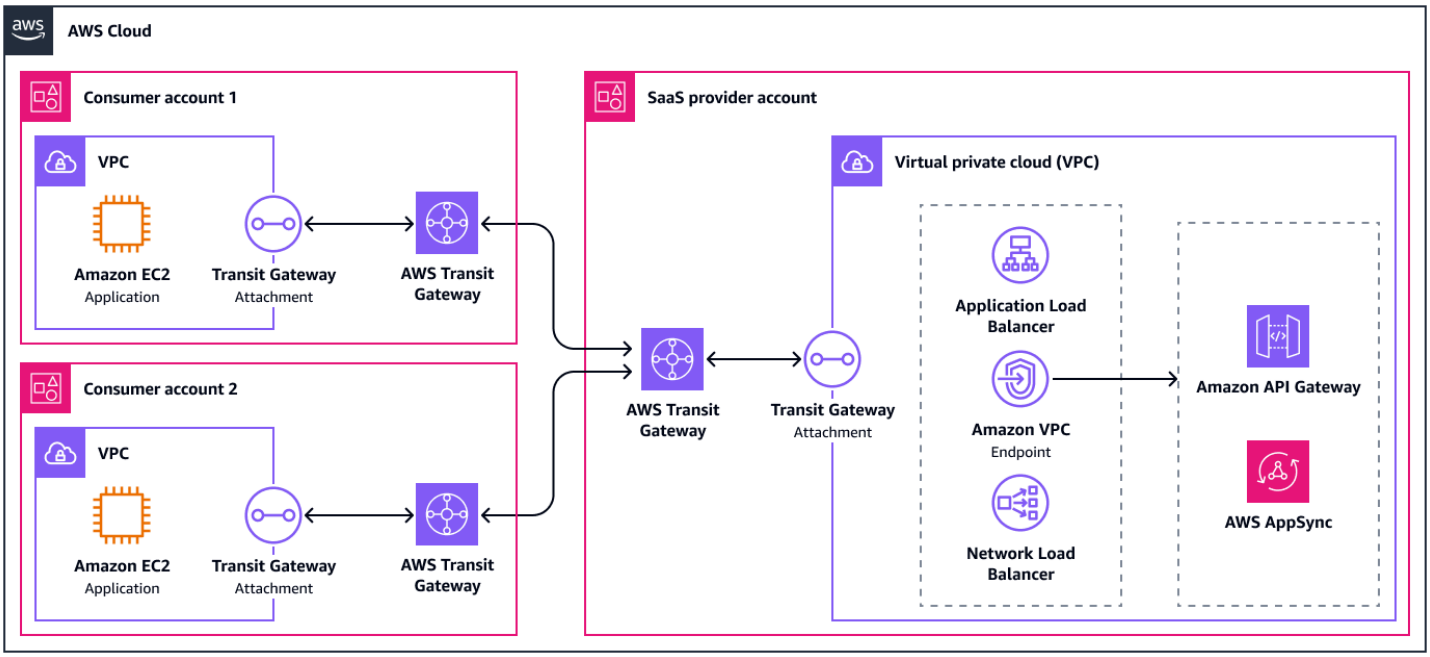
Option 1: RAM verwenden

Bei der ersten Option teilt der Dienstanbieter das Transit Gateway mithilfe von AWS Resource Access Manager (AWS RAM) mit den Verbrauchern. Auf diese Weise können die Verbraucher die VPC-Anhänge in ihren eigenen Konten bereitstellen. Das folgende Diagramm zeigt diese Option auf hoher Ebene.



Option 2: Peering-Transit-Gateways

Die zweite Option besteht darin, Ihr Transit-Gateway mit einem Transit-Gateway in den Konten der Verbraucher zu verbinden. Dies bietet Verbrauchern mehr Flexibilität, da sie jetzt die vollständige Kontrolle über die Routentabellen in ihrem Transit-Gateway haben. Sie könnten beispielsweise eine zentrale Inspektion zwischen dem Service und ihren Workloads einrichten. Ein Nachteil dieser Option besteht darin, dass nur statisches Routing zwischen Transit-Gateways unterstützt wird. Das folgende Diagramm zeigt diese Option auf hoher Ebene.



Diese Herangehensweise bietet folgende Vorteile:

- Skalierbarkeit: Support für bis zu 5.000 Anhänge
- Skalierbarkeit: Ein Ort für die Verwaltung und Überwachung aller verbundenen Geräte VPCs
- Anpassungsfähigkeit: Transit Gateway kann auch an Direct Connect Gateways und VPNs SD-WAN-Appliances von Drittanbietern angeschlossen werden
- Anpassungsfähigkeit: Flexible Architektur, z. B. Hinzufügen einer Inspektions-VPC
- Anpassungsfähigkeit: Support für transitives Routing
- Anpassungsfähigkeit: Kann interregionale und interregionale Transit-Gateways miteinander verbinden
- Anpassungsfähigkeit: Support für IPv6
- TCO: AWS Transit Gateway ist ein vollständig verwalteter Service, der weniger Betriebsaufwand erfordert
- Gesamtbetriebskosten: Die Gesamtbetriebskosten steigen linear mit jedem weiteren Transit-Gateway-Anschluss

Im Folgenden sind die Nachteile dieses Ansatzes aufgeführt:

- Einfache Integration: Die Routing-Konfiguration erfordert fortgeschrittene Netzwerkkenntnisse
- Anpassungsfähigkeit: Keine Unterstützung für überlappende CIDR-Bereiche

- Gesamtbetriebskosten: Mehraufwand aufgrund der Verwaltung von Routentabelleneinträgen, Sicherheitsgruppenregeln und der Verkehrsinspektion
- Sicherheit: Strenge Sicherheitskontrollen sind erforderlich, VPCs da beide Parteien vollständig gefährdet sind

Servicekunden, die vor Ort tätig sind

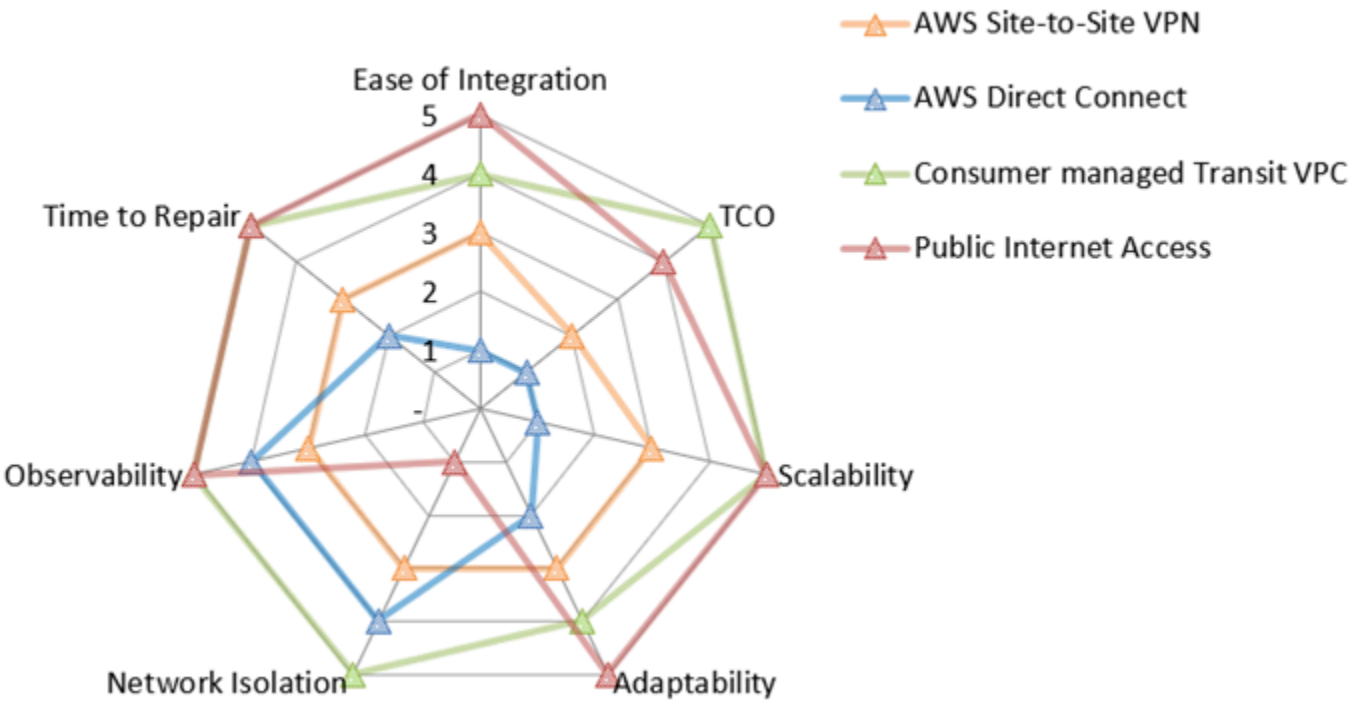
In diesem Abschnitt werden die Konnektivitätsoptionen zwischen SaaS-Workloads in den AWS Cloud und den lokalen Rechenzentren beschrieben. Viele Verbraucher mit lokalen Anforderungen, insbesondere auf Unternehmensebene, betrachten die Cloud als Erweiterung ihres physischen Netzwerks, und sie möchten dies in ihrer Architektur widerspiegeln. Das bedeutet private Konnektivität zum SaaS-Angebot in der Cloud, entweder über logische Tunnel oder sogar über eine private physische Verbindung. Andere Verbraucher werden Konnektivität über das öffentliche Internet akzeptieren, was ebenfalls in diesem Abschnitt erörtert wird.

In diesem Abschnitt werden die folgenden Ansätze für den Netzwerkzugriff erörtert:

- Verbindung herstellen mit AWS Site-to-Site VPN
- Verbindung herstellen mit AWS Direct Connect
- Verbindung mit einer Transit-VPC-Architektur herstellen
- Verbindung über das öffentliche Internet herstellen

In der folgenden Netzwerkwerteübersicht wird zusammengefasst, wie jede dieser Optionen bei jeder Bewertungsmetrik abschneidet. Weitere Informationen zu den Bewertungsmetriken finden Sie unter Bewertungskennzahlen in diesem Leitfaden. In der Übersicht steht eine Fünf für das beste Ergebnis, z. B. für die niedrigsten Gesamtbetriebskosten, die beste Netzwerkisolierung oder die kürzeste Reparaturzeit. Weitere Informationen zum Lesen dieses Radardiagramms finden Sie Wertübersicht der Netzwerke in diesem Handbuch.

> **Note**
>
> Die vom Anbieter verwaltete Transit-VPC-Option ist ausgeschlossen, da die Punktzahlen stark davon abhängen, welche Dienste betrieben werden.



Das Radardiagramm zeigt die folgenden Werte.

Bewertungsmetrik	AWS Site-to-Site VPN	AWS Direct Connect	Von Verbrauchern verwaltete Transit-VPC	Öffentlicher Internetzugang
Einfache Integration	3	1	4	5
Gesamtbetriebskosten	2	1	5	4
Skalierbarkeit	3	1	5	5
Anpassungsfähigkeit	3	2	4	5
Netzwerkisolierung	3	4	5	1
Beobachtbarkeit	3	4	5	5

Zeit zum Reparieren	3	2	5	5

Verbindung herstellen mit AWS Site-to-Site VPN

AWS Site-to-Site VPNVerbindungen können entweder auf einem Virtual Private Gateway oder einem Transit-Gateway enden. Ein virtuelles privates Gateway ist der VPN-Endpunkt auf der AWS Seite Ihrer Site-to-Site VPN-Verbindung, der an eine einzelne VPC angeschlossen werden kann. Ein Transit-Gateway ist ein Transit-Hub, über den mehrere VPCs und lokale Netzwerke miteinander verbunden werden können. Es kann auch als VPN-Endpunkt für die AWS Seite der Site-to-Site VPN-Verbindung verwendet werden. In diesem Abschnitt werden beide Optionen beschrieben.

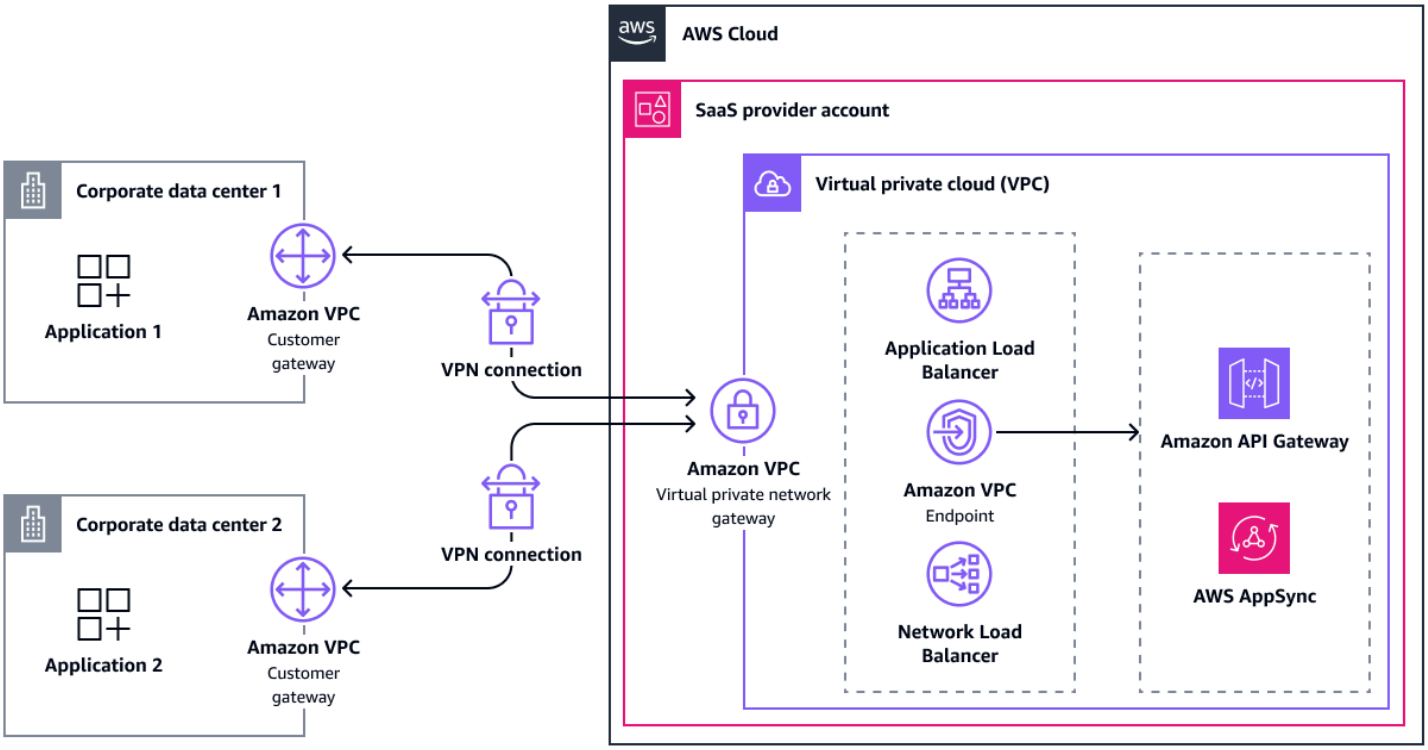
Verbindung über ein virtuelles privates Gateway

Nachdem Sie ein virtuelles privates Gateway erstellt haben, fügen Sie es der VPC hinzu, die Ihr SaaS-Angebot enthält. Anschließend aktivieren Sie die Route-Propagierung, um die VPN-Routen an die VPC-Routentabelle weiterzugeben. Bei diesen Routen kann es sich entweder um statische Routen oder um vom BGP angekündigte dynamische Routen handeln.

Um eine hohe Verfügbarkeit zu gewährleisten, verfügt eine Site-to-Site VPN-Verbindung über zwei VPN-Tunnel, die in zwei Availability Zones an der Seite enden. AWS Wenn einer nicht verfügbar ist, kann der zweite Tunnel die Kontrolle übernehmen. Ein einzelner Tunnel ermöglicht eine maximale Bandbreite von 1,25 Gbit/s. Da Virtual Private Gateways ECMP (Equal-Cost Multi-Path Routing) nicht unterstützen, können Sie jeweils nur einen Tunnel verwenden.

Um die Fehlertoleranz zu erhöhen, können Sie eine zweite VPN-Verbindung zu einem zweiten physischen Kunden-Gateway einrichten. Nachdem die Verbindung hergestellt wurde, kann der Verbraucher auf Ressourcen in der VPC des SaaS-Anbieters zugreifen.

Das folgende Diagramm zeigt diese Architektur.



Diese Herangehensweise bietet folgende Vorteile:

- Reparaturzeit: Verwaltetes Failover zum sekundären VPN-Tunnel
- Beobachtbarkeit: Integration für verwaltete aktive Überwachung mithilfe von Network Synthetic Monitor
- Einfache Integration: Unterstützung für dynamisches Routing über BGP
- Anpassungsfähigkeit: Kompatibilität mit den meisten Netzwerkgeräten vor Ort
- Anpassungsfähigkeit: Unterstützung IPv6
- TCO: AWS Site-to-Site VPN ist ein vollständig verwalteter Service, der weniger Betriebsaufwand erfordert
- Gesamtbetriebskosten: Keine Kosten für virtuelle Gateways, obwohl Gebühren für die beiden öffentlichen IPv4 Adressen auf jedem Gateway anfallen
- Netzwerkisolierung: Ermöglicht sichere private Kommunikation über das Internet

Im Folgenden sind die Nachteile dieses Ansatzes aufgeführt:

- Einfache Integration: Der Verbraucher muss sein Kunden-Gateway konfigurieren

- Skalierbarkeit: Mangelnde ECMP-Unterstützung begrenzt die Bandbreite auf 1,25 Gbit/s pro virtuellem Gateway
- Skalierbarkeit: Eingeschränkte Skalierung aufgrund der erhöhten Netzwerkkomplexität und des erhöhten Betriebsaufwands
- Anpassungsfähigkeit: IPv6 Unterstützung nur für die internen IP-Adressen der VPN-Tunnel
- Anpassungsfähigkeit: Kein transitives Routing
- Gesamtbetriebskosten: Betriebsaufwand für die Wartung, Verwaltung und Konfiguration zahlreicher VPN-Verbindungen für den SaaS-Anbieter

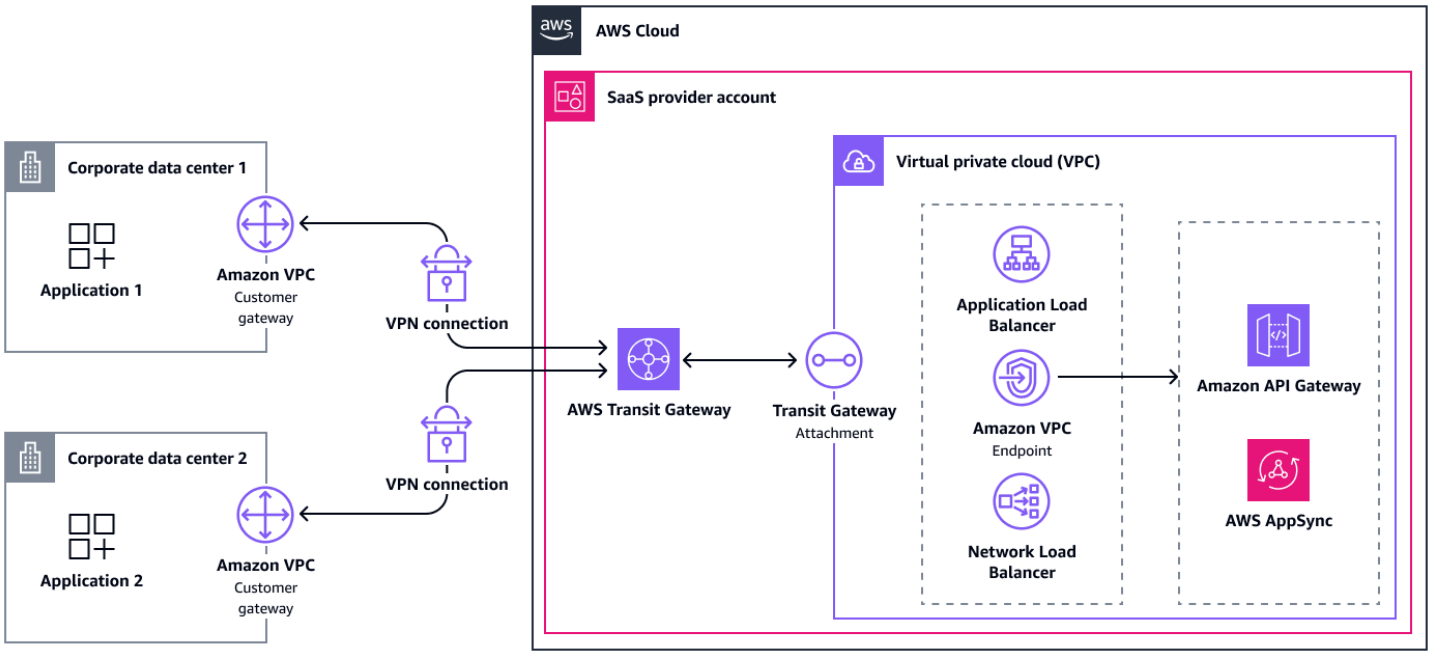
Verbindung über ein Transit-Gateway

Verbindungen über Transit-Gateways ähneln virtuellen Gateways. Es sind jedoch einige Unterschiede zu beachten.

Erstens können Routen für den VPN-Anhang automatisch innerhalb der Routentabelle des Transit-Gateways weitergegeben werden, aber Sie müssen die Routen manuell zu den angehängten VPCs Routen hinzufügen.

Im Vergleich zu einem virtuellen Gateway unterstützt Transit Gateway ECMP. Wenn das Kunden-Gateway ECMP unterstützt, kann es beide Tunnel verwenden, um einen maximalen Gesamtdurchsatz von 2,5 Gbit/s zu erreichen. Sie können mehrere Verbindungen zwischen demselben lokalen Netzwerk und dem Transit-Gateway herstellen. Mit diesem Ansatz können Sie die maximale Bandbreite um bis zu 2,5 Gbit/s pro Verbindung erhöhen.

Das folgende Diagramm zeigt diese Architektur.



Diese Herangehensweise bietet folgende Vorteile:

- Reparaturzeit: Verwaltetes Failover zum sekundären VPN-Tunnel
- Beobachtbarkeit: Integration für verwaltete aktive Überwachung mithilfe von Network Synthetic Monitor
- Einfache Integration: Unterstützung für dynamisches Routing über BGP
- Skalierbarkeit: Die ECMP-Unterstützung ermöglicht die Skalierung des VPN-Durchsatzes, um große Bandbreitenanforderungen zu erfüllen
- Skalierbarkeit: Große Anzahl von VPN-Verbindungen, die von einem einzigen Transit-Gateway unterstützt werden (bis zu fast 5.000)
- Skalierbarkeit: Ein Ort für die Verwaltung und Überwachung aller VPN-Verbindungen
- Anpassungsfähigkeit: Kompatibilität mit den meisten Netzwerkgeräten vor Ort
- Anpassungsfähigkeit: Unterstützung IPv6
- Anpassungsfähigkeit: Erben Sie die Flexibilität von AWS Transit Gateway
- TCO: AWS Transit Gateway ist ein vollständig verwalteter Service, der weniger Betriebsaufwand erfordert
- Gesamtbetriebskosten: Keine Kosten für virtuelle Gateways, obwohl Gebühren für die beiden öffentlichen IPv4 Adressen auf jedem Gateway anfallen
- Netzwerkisolierung: Ermöglicht sichere private Kommunikation über das Internet

Im Folgenden sind die Nachteile dieses Ansatzes aufgeführt:

- Einfache Integration: Der Verbraucher muss sein Kunden-Gateway konfigurieren
- Skalierbarkeit: Eingeschränkte Skalierung aufgrund der erhöhten Netzwerkkomplexität und des erhöhten betrieblichen Mehraufwands
- Anpassungsfähigkeit: IPv6 Unterstützung nur für die internen IP-Adressen der VPN-Tunnel
- Gesamtbetriebskosten: Betriebsaufwand für die Wartung, Verwaltung und Konfiguration zahlreicher VPN-Verbindungen für den SaaS-Anbieter
- Gesamtbetriebskosten: Zusätzliche Gebühren für die Nutzung von AWS Transit Gateway
- TCO: Zusätzliche Komplexität bei der Verwaltung der Routentabellen des Transit-Gateways

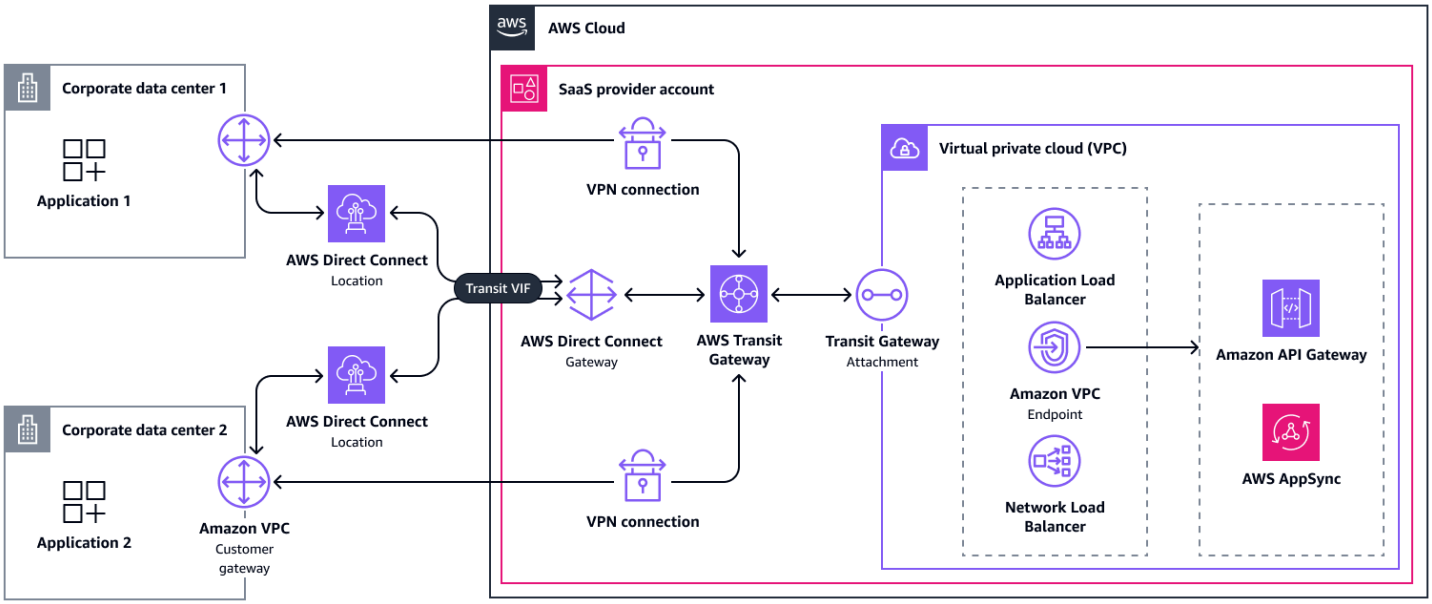
Verbindung herstellen mit AWS Direct Connect

AWS Direct Connectverbindet Ihr internes Netzwerk über ein Standard-Ethernet-Glasfaserkabel mit einem Direct Connect Standort. Im Gegensatz zu den anderen Architekturoptionen kann eine dedizierte Verbindung nicht in wenigen Minuten hergestellt werden. Stattdessen kann dieser Vorgang bis zu mehreren Tagen dauern, wenn alle Anforderungen erfüllt sind. Wenn nicht, kann es länger dauern. Wir empfehlen Ihnen daher, sich an Ihr AWS Account-Team zu wenden oder Hilfe AWS Support bei diesem Ansatz zu erhalten. Optional können Sie eine gehostete Verbindung wählen, die von einem AWS Partner bereitgestellt und mit anderen Kunden geteilt wird. Die Architektur ist trotzdem dieselbe. Sie könnten sich dafür entscheiden, Direct Connect weil sie die Latenz reduziert, die Bandbreite verbessert oder gesetzliche Anforderungen erfüllt.

Um die Direct Connect Verbindung nutzen zu können, müssen Verbraucher entweder eine öffentliche, eine private oder eine virtuelle Transitschnittstelle einrichten. Es stehen verschiedene Architekturoptionen zur Verfügung. Die flexibelste Methode, um mehrere lokale Standorte miteinander zu verbinden, AWS Cloud ist eine virtuelle Transitschnittstelle, die mit einem Direct Connect Gateway verbunden ist. Ein Direct Connect Gateway ist eine globale, logische Komponente, die es dem Dienstanbieter ermöglicht, bis zu sechs Transit-Gateways mit ihm zu verbinden. Darüber hinaus können Sie bis zu 30 virtuelle Schnittstellen mit dem Gateway verbinden. Zur Skalierung können Sie zusätzliche Direct Connect Gateways erstellen. Im SaaS-Anbieterkonto verbinden sich die Transit-Gateways dann VPCs, wie zuvor beschrieben, mit dem.

Verbraucher können je nach gewünschter Ausfallsicherheit über ein bis vier Direct Connect Verbindungen von insgesamt einem oder zwei Direct Connect Standorten aus eine Verbindung herstellen. Weitere Informationen finden Sie unter Konfiguration Direct Connect für maximale

Ausfallsicherheit. Eine AWS Site-to-Site VPN Verbindung über das Internet kann auch als kostengünstigerer Backup-Pfad für eine Verbindung dienen. Direct Connect Unterstützte Direct Connect dedizierte Verbindungen können verwendet werden MACsec, um die Verbindung auf Layer 2 zwischen dem Direct Connect Standort und dem Rechenzentrum zu verschlüsseln. Es ist üblich, eine Site-to-Site VPN-Verbindung zu haben, um die Vertraulichkeit der Daten zu erhöhen. Die Site-to-Site VPN-Verbindung kann auf dem Transit-Gateway mithilfe eines normalen VPN-Anhangs beendet werden. Das folgende Diagramm zeigt diese Architektur.



Diese Herangehensweise bietet folgende Vorteile:

- Beobachtbarkeit: Integration für verwaltete aktive Überwachung mithilfe von Network Synthetic Monitor
- Skalierbarkeit: Support für erhöhten Bandbreitendurchsatz
- Anpassungsfähigkeit: Unterstützung IPv6
- Gesamtbetriebskosten: Potenzial zur Reduzierung der Datenübertragung
- TCO: Konsistentes Netzwerkerlebnis
- Netzwerkisolierung: Private Konnektivität, die regulatorische Anforderungen erfüllen kann

Im Folgenden sind die Nachteile dieses Ansatzes aufgeführt:

- Einfache Integration: Zeit und manueller Aufwand bei der Einrichtung
- Skalierbarkeit: Eingeschränkte Skalierbarkeit bei mehr als zehn Direct Connect Verbindungen, da mehrere Kontingente nachverfolgt werden müssen

- Anpassungsfähigkeit: Die Konfigurationsoptionen hängen von den verfügbaren Direct Connect Standorten ab
- Gesamtbetriebskosten: Geplante Direct Connect Wartungsarbeiten können zu Ausfallzeiten führen, die Maßnahmen erfordern

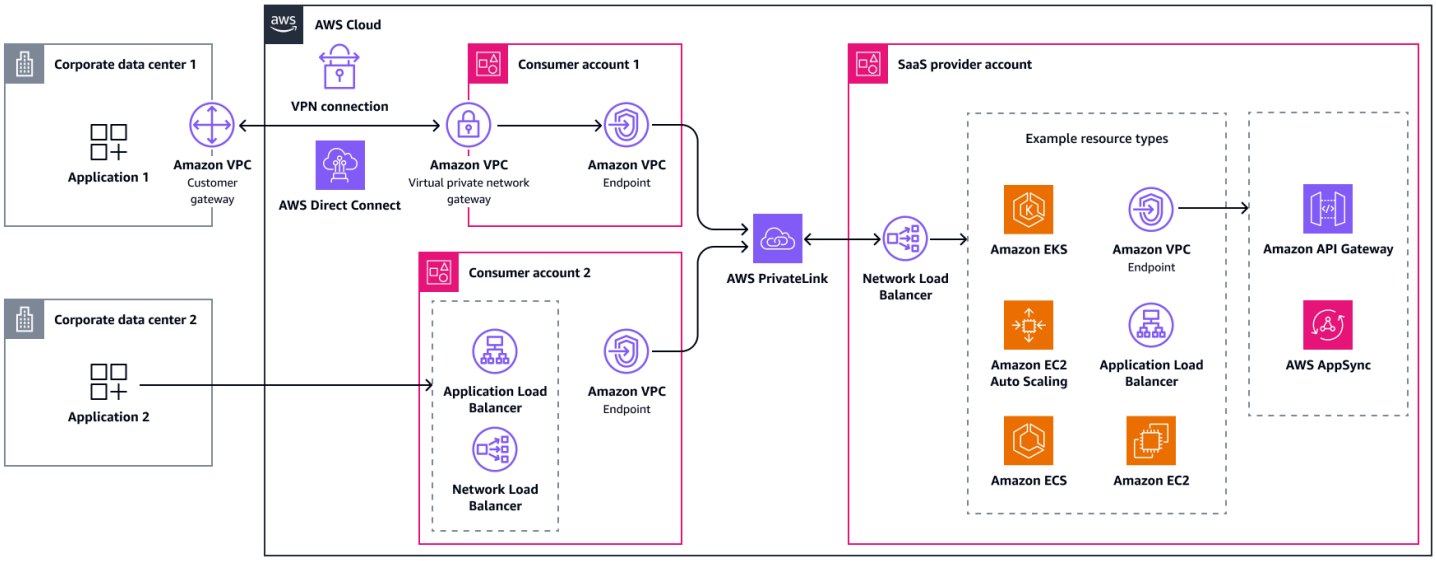
Verbindung mit einer Transit-VPC-Architektur herstellen

Transit VPC ist eine Architekturoption, die den Verbrauchern Flexibilität bei der Art der Verbindung bietet und es SaaS-Anbietern ermöglicht AWS, von einem einheitlichen Zugriff auf ihren Service zu profitieren. AWS PrivateLink Der Verbraucher stellt von einem lokalen Standort aus eine Verbindung zu einer Transit-VPC her, die nur einen Einstiegspunkt (z. B. ein virtuelles privates Gateway) und einen VPC-Schnittstellen-Endpunkt enthält, bei dem es sich um eine AWS PrivateLink Ressource handelt. Der Transit VPCs sollte entweder dem SaaS-Anbieter oder den Verbrauchern gehören. In diesem Abschnitt werden beide Optionen beschrieben.

Sie können die Transit-VPC und Subnetze mit CIDR-Bereichen erstellen, die mit dem lokalen Rechenzentrum kompatibel sind. Wenn sie private Konnektivität benötigen, können Verbraucher über AWS Direct Connect oder AWS Site-to-Site VPN eine Verbindung zu dieser VPC herstellen. Sie können den Zugriff auf das Transitkonto auch vom öffentlichen Internet aus konfigurieren, indem Sie einen Application Load Balancer oder Network Load Balancer verwenden, der auf den VPC-Endpunkt verweist.

Von Verbrauchern verwaltete Transit-VPC

Bei diesem Ansatz überlässt der SaaS-Anbieter die Verwaltung des Transports VPCs den Verbrauchern. Aus technischer Sicht ist die Architektur des SaaS-Anbieters dieselbe wie bei der AWS Cloud durchgehenden Verbindung zu Verbrauchern AWS PrivateLink. Aus Vertriebs- und Produktsicht ist dies ein zusätzlicher Aufwand, da einige Verbraucher dies AWS-Konten noch nicht getan haben. Sie zögern möglicherweise, ein Konto zu eröffnen und zu führen. Der SaaS-Anbieter sollte seinen Verbrauchern Anleitungen zum Aufbau AWS-Konten und zur Verbindung ihres lokalen Rechenzentrums geben. Das folgende Diagramm zeigt eine Mischung aus öffentlichem und privatem Zugang, wobei die Verbraucher den Transit VPCs selbst bestimmen.



Diese Herangehensweise bietet folgende Vorteile:

- Zeit bis zur Reparatur: Der betriebliche Aufwand wird größtenteils auf SaaS-Nutzer abgewälzt
- Anpassungsfähigkeit: SaaS-Verbraucher können aus verschiedenen Zugriffsoptionen wählen
- Anpassungsfähigkeit: Keine CIDR-Reichweitenkonflikte, auch bei Verwendung von VPN oder Site-to-Site Direct Connect
- Alle Kennzahlen: Der Dienstanbieter erbt Vorteile AWS PrivateLink

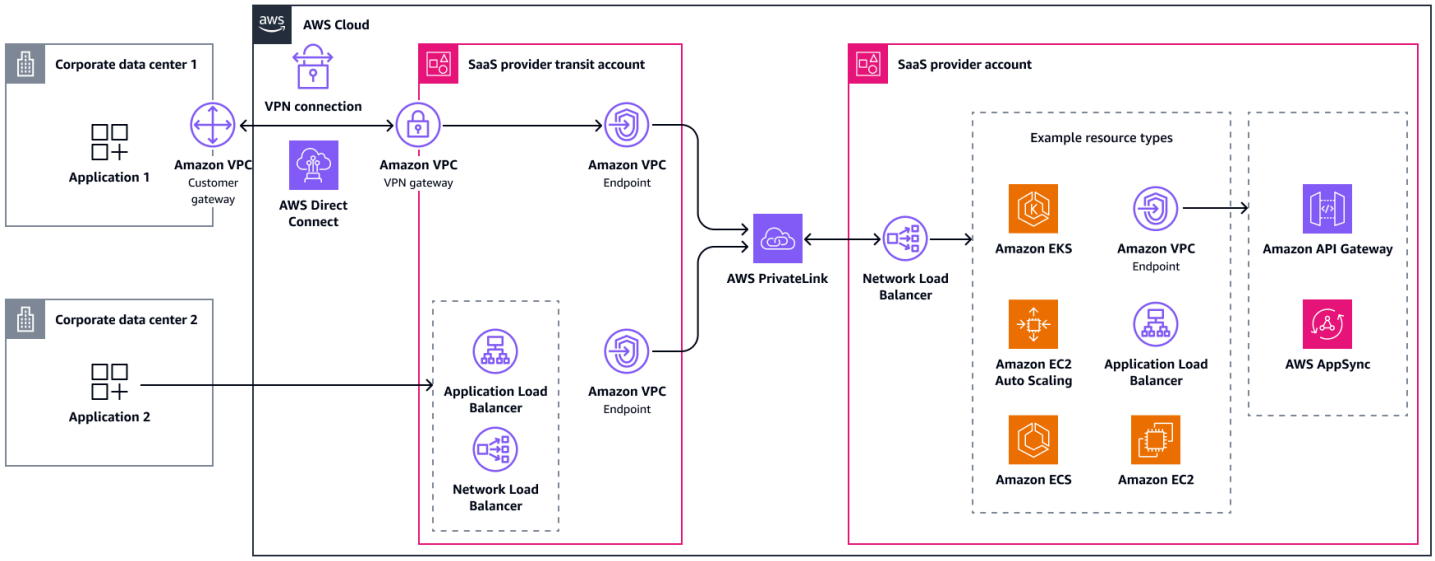
Im Folgenden sind die Nachteile dieses Ansatzes aufgeführt:

- Einfache Integration: SaaS-Verbraucher benötigen mindestens einen AWS-Konto
- Gesamtbetriebskosten: Eine Transit-VPC ist eine Architektur, kein vollständig verwalteter Service, weshalb sie einen höheren betrieblichen Aufwand erfordert

Anbieterverwaltete Transit-VPC

Bei diesem Ansatz werden dieselben Technologien verwendet, aber die Kontogrenzen und Verantwortlichkeiten ändern sich. Hier ist der SaaS-Anbieter Eigentümer des Transports VPCs, vorzugsweise in einem vom SaaS-Angebot getrennten Konto. Diese Entkopplung reduziert die Kosten, reduziert Risiken und ermöglicht es dem Transitkonto, unabhängig zu skalieren. In Umgebungen, die ein hohes Maß an Isolation erfordern, können Sie eine zusätzliche Trennung zwischen Mandanten herstellen, indem Sie ein Subnetz verwenden oder für jeden Verbraucher eine separate Transit-VPC erstellen. Die Verbraucher können dann wählen, wie sie eine Verbindung

zur Transit-VPC herstellen möchten. Dieser Ansatz bietet mehr Optionen zur Erweiterung des gesamten adressierbaren Marktes, hat jedoch höhere Gesamtbetriebskosten für den SaaS-Anbieter, da zusätzliche Architekturkomponenten betrieben und überwacht werden müssen.



Diese Herangehensweise bietet folgende Vorteile:

- Anpassungsfähigkeit: SaaS-Verbraucher können aus verschiedenen Zugriffsoptionen wählen
- Anpassungsfähigkeit: SaaS-Verbraucher müssen kein AWS-Konto
- Anpassungsfähigkeit: Keine CIDR-Reichweitenkonflikte, auch bei Verwendung von VPN oder Site-to-Site Direct Connect

Im Folgenden sind die Nachteile dieses Ansatzes aufgeführt:

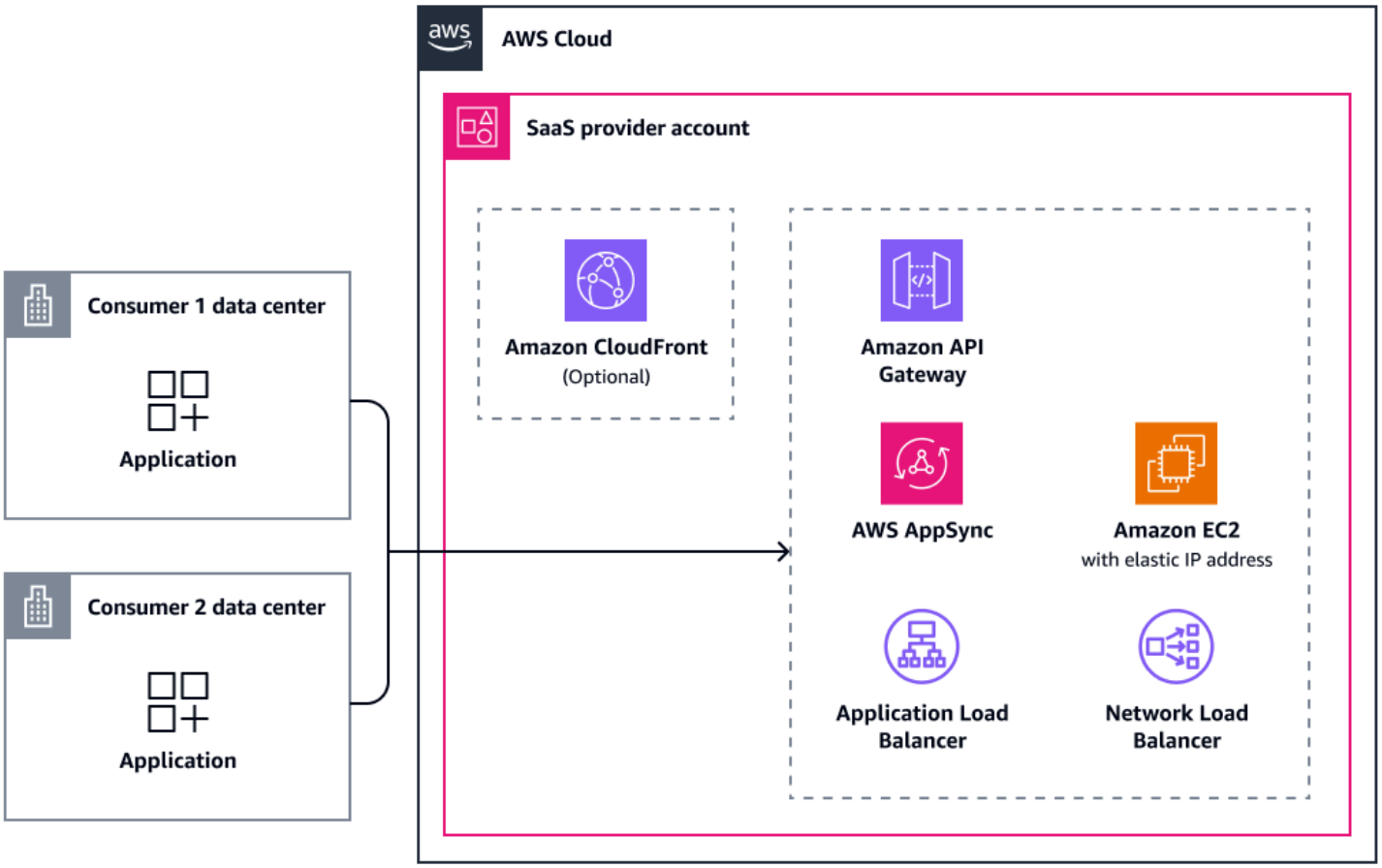
- Gesamtbetriebskosten: Eine Transit-VPC ist eine Architektur, kein vollständig verwalteter Service, weshalb sie einen höheren betrieblichen Aufwand erfordert
- Gesamtbetriebskosten: SaaS-Anbieter muss zusätzliche Architekturkomponenten betreiben und überwachen

Verbindung über das öffentliche Internet herstellen

Der öffentliche Internetzugang ist auch eine gültige Option für den Zugang zu einem SaaS-Angebot, obwohl er keine private Konnektivität im herkömmlichen Sinne bietet. Einige Verbraucher bevorzugen möglicherweise immer noch einen Ansatz mit öffentlichem Zugriff, da dafür keine zusätzliche Netzwerkinfrastruktur zwischen ihnen und dem SaaS-Anbieter erforderlich ist. Es reduziert die

Komplexität, die Kosten und die Integrationszeit und bietet im Gegenzug eine größere Angriffsfläche. Starke Authentifizierungs- und Autorisierungsmechanismen können dazu beitragen, das erhöhte Bedrohungsniveau zu verringern, und Sie sollten den Datenverkehr immer verschlüsseln. Es wird dennoch empfohlen, in diesem Szenario über eine zusätzliche Sicherheitsebene zu verfügen, z. B. durch die Verwendung von. AWS WAF

Die Architektur in diesem Szenario ist einfach. Der Verbraucher stellt über das Internet eine Verbindung zu einem öffentlichen Host (dem SaaS-Anbieter) her. Die Anwendung kann direkt auf einer öffentlichen Amazon Elastic Compute Cloud (Amazon EC2) -Instance mit einer Elastic IP-Adresse gehostet werden. Die bevorzugte Option besteht darin, es hinter einem Application Load Balancer oder einem ähnlichen Dienst zu hosten. Für eine bessere Leistung und das Zwischenspeichern statischer Ressourcen können Sie ein Content Delivery Network wie Amazon CloudFront verwenden. Um eine Anwendung mit minimaler Latenz über zwei globale statische Anycast-IP-Adressen bereitzustellen, können Sie sie vor einer Amazon EC2 EC2-Instance, einem Network Load Balancer oder einem Application Load Balancer platzieren AWS Global Accelerator. Darüber CloudFront hinaus lassen sich Application Load Balancers und Amazon API Gateway alle in integrieren AWS WAF. AWS AppSync Das folgende Diagramm bietet einen Überblick über die Verbindungsoptionen für den öffentlichen Internetzugang.



In der folgenden Tabelle werden die unterstützten Protokolle und Integrationen für dieses Szenario beschrieben.

Dienst oder Ressource	IPv6	AWS WAF Integration	Kann ein Global Accelerator-Endpunkt sein
Amazon CloudFront	Unterstützt	Unterstützt	Nicht unterstützt
Amazon API Gateway	Unterstützt	Unterstützt	Nicht unterstützt
AWS AppSync	Teilweise unterstützt	Unterstützt	Nicht unterstützt
Amazon EC2 mit einer Elastic IP-Adresse	Unterstützt	Nicht unterstützt	Unterstützt
Application Load Balancer	Unterstützt	Unterstützt	Unterstützt
Network Load Balancer	Unterstützt	Nicht unterstützt	Unterstützt

Diese Herangehensweise bietet folgende Vorteile:

- Einfache Integration: Einfachheit und Zugänglichkeit
- Skalierbarkeit: Unbegrenzter Umfang
- Anpassungsfähigkeit: Keine CIDR-Bereichskonflikte möglich
- Anpassungsfähigkeit: Unterstützung CloudFront

Im Folgenden sind die Nachteile dieses Ansatzes aufgeführt:

- Netzwerkisolierung: Keine private Konnektivität
- Netzwerkisolierung: Starke Sicherheitsmaßnahmen erforderlich

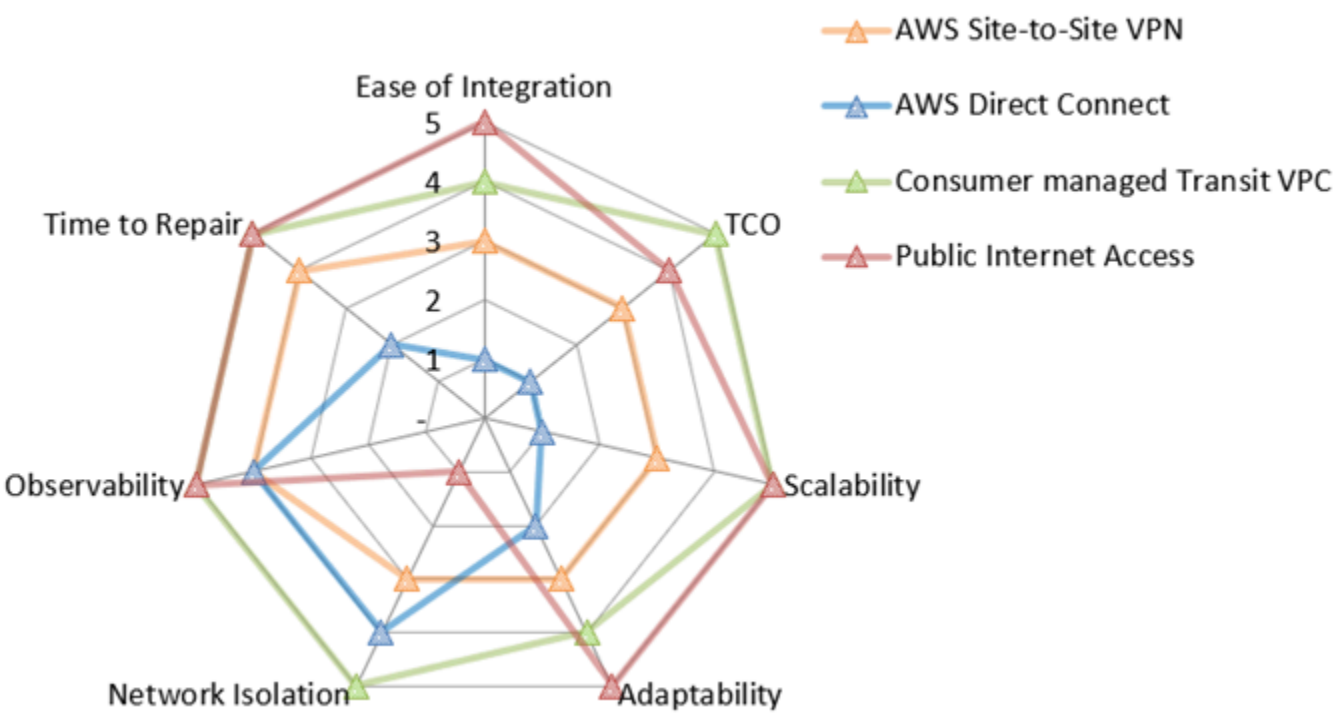
Je nachdem, für welche Dienste Sie sich entscheiden, gelten weitere Vor- und Nachteile.

SaaS-Verbraucher, die bei anderen Cloud-Dienstanbietern tätig sind

In diesem Szenario werden Lösungen für Verbraucher anderer Cloud-Dienstanbieter beschrieben (CSPs). Dieses Szenario weist einige Gemeinsamkeiten mit Verbindungen zu lokalen Rechenzentren auf. Tatsächlich sind alle Verbindungsoptionen für lokale Umgebungen auch für Verbraucher in anderen Umgebungen gültig CSPs, bei einigen AWS Direct Connect ist sogar eine private Verbindung möglich. CSPs Die meisten CSPs bieten Dokumentation und Support dazu, wie eine Verbindung AWS Cloud über AWS Site-to-Site VPN oder AWS Direct Connect hergestellt werden kann.

Bei der Wahl eines Site-to-Site VPN können Verbraucher von verwalteten Gateways oder ähnlichen Ressourcen ihres jeweiligen CSP profitieren. Verbraucher müssen sie nicht unbedingt selbst einrichten, wie im Szenario vor Ort. Dies beeinflusst einige der Kennzahlen für Site-to-Site VPN, wie z. B. die Verbesserung der Reparaturzeit und der Beobachtbarkeit. Das liegt daran, dass beide Enden der Verbindung jetzt verwaltet werden.

In der folgenden Netzwerkwerteübersicht wird zusammengefasst, wie jede dieser Optionen bei jeder Bewertungsmetrik abschneidet. Sie ist der Netzwerk-Wertemap für lokale Verbindungen sehr ähnlich, obwohl die Werte für Site-to-Site VPN unterschiedlich sind. Weitere Informationen zu den Bewertungsmetriken finden Sie Bewertungsmetriken in diesem Leitfaden. In der Übersicht steht eine Fünf für das beste Ergebnis, z. B. für die niedrigsten Gesamtbetriebskosten, die beste Netzwerkisolierung oder die kürzeste Reparaturzeit. Weitere Informationen zum Lesen dieses Radardiagramms finden Sie Wertübersicht der Netzwerke in diesem Handbuch.



Das Radardiagramm zeigt die folgenden Werte.

Bewertungsmetrik	AWS Site-to-Site VPN	AWS Direct Connect	Von Verbrauchern verwaltete Transit-VPC	Öffentlicher Internetzugang
Einfache Integration	3	1	4	5
Gesamtbetriebskosten	3	1	5	4
Skalierbarkeit	3	1	5	5
Anpassungsfähigkeit	3	2	4	5
Netzwerkisolierung	3	4	5	1
Beobachtbarkeit	4	4	5	5

Zeit zum Reparieren	4	2	5	5

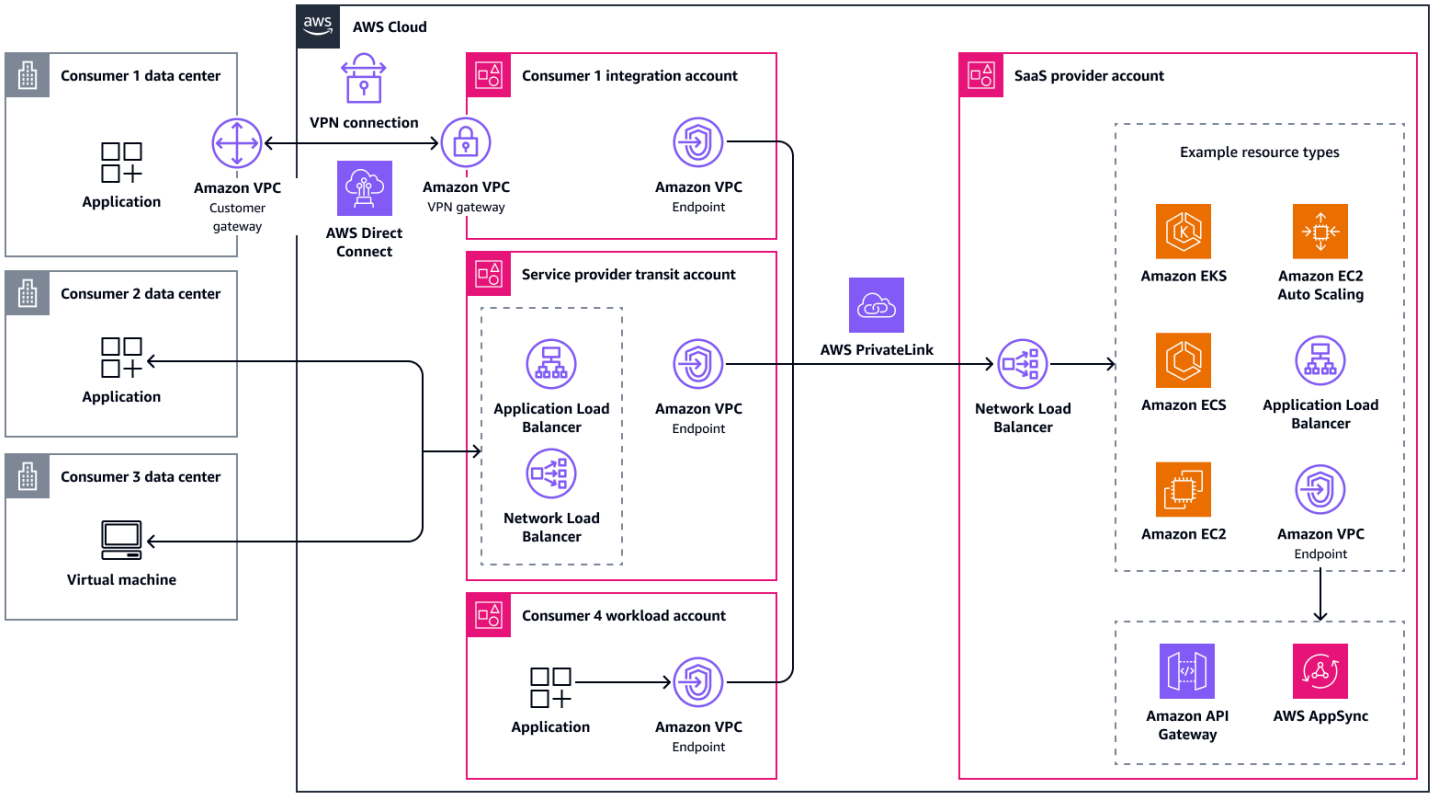
Unterstützung hybrider Umgebungen

Es ist üblich, dass Verbraucher aus unterschiedlichen Umgebungen kommen, von denen jede ihre eigenen technischen und sicherheitstechnischen Einschränkungen hat. Einige Kunden arbeiten möglicherweise ausschließlich von lokalen Rechenzentren aus, für die eine sichere Konnektivität über das Internet oder über spezielle Netzwerkverbindungen erforderlich ist. Andere führen Workloads möglicherweise bereits innerhalb von privaten Netzwerkpfaden aus AWS und erwarten dort niedrige Latenzzeiten. Eine dritte Gruppe könnte sich auf andere verlassen CSPs, bei denen die Konnektivität verschiedene Cloud-Netzwerke verbinden muss.

Unabhängig davon sollten Sie einen standardisierten Netzwerkzugriff auf Ihre SaaS-Anwendung anstreben, um Ihre Architektur zu vereinfachen und die betriebliche Komplexität zu reduzieren. Zwei der zuvor vorgestellten Ansätze — öffentlicher Internetzugang und Transit VPCs — funktionieren in diesen Szenarien gut. Der öffentliche Internetzugang bietet den schnellsten Onboarding-Pfad mit minimalem Einrichtungsaufwand für Ihre Kunden. Der öffentliche Nahverkehr VPCs bietet einen kontrollierteren und privateren Zugang, der häufig genutzt AWS PrivateLink wird.

Bei der Gestaltung Ihres SaaS-Angebots können Sie ein einziges Netzwerkzugriffsmodell verwenden oder mehrere Ansätze zu einem abgestuften Angebot kombinieren. Sie könnten beispielsweise eine Bereitstellungsstufe mit öffentlichem Zugang für Kunden anbieten, die Wert auf einfache Verbindung und schnelles Onboarding legen, und Sie könnten eine Bereitstellungsstufe mit privatem Zugriff für Kunden anbieten, die strenge Anforderungen an die Einhaltung von Vorschriften oder Sicherheitskontrollen stellen. Diese Stufen haben unterschiedliche Kosten-, Leistungs- und Risikoprofile. Es ist auch möglich, beide Ansätze in einer einzigen Architektur zu kombinieren. Stellen Sie in diesem Fall sicher, dass Sie über strenge Sicherheitsmaßnahmen verfügen, damit öffentliche und private Pfade isoliert bleiben.

Das folgende Diagramm zeigt einen hybriden Zugriffsansatz, bei dem Verbraucher die Möglichkeit haben, eine private Verbindung von ihrem Rechenzentrum oder CSP aus, öffentlich oder direkt über AWS PrivateLink (wenn sie Workloads haben) herzustellen. AWS Cloud


AWS Cloud
Consumer 1 data center
Application
Amazon VPC
Customer gateway
VPN connection
AWS Direct Connect
Amazon VPC
VPN gateway
Consumer 1 integration account
Amazon VPC
Endpoint
Consumer 2 data center
Application
Consumer 3 data center
Virtual machine
Service provider transit account
Application Load Balancer
Network Load Balancer
Amazon VPC
Endpoint
Consumer 4 workload account
Application
Amazon VPC
Endpoint
AWS PrivateLink
SaaS provider account
Network Load Balancer
Example resource types
Amazon EKS
Amazon EC2 Auto Scaling
Amazon ECS
Application Load Balancer
Amazon EC2
Amazon VPC
Endpoint
Amazon API Gateway
AWS AppSync

Erweiterte Netzwerkzugriffsszenarien für SaaS-Angebote in der AWS Cloud

Die in Netzwerkzugriffsszenarien für SaaS-Angebote in der AWS Cloud diesem Abschnitt erörterten Architekturen sollen Ihnen helfen, eine Lösung für die meisten Anwendungsfälle zu finden. Es gibt jedoch einige Szenarien mit spezifischen technischen Anforderungen. Viele gehen über den Rahmen dieses Handbuchs hinaus.

In diesem Abschnitt werden die folgenden fortgeschrittenen technischen Anforderungen und Überlegungen erörtert:

- Bidirektionale Kommunikation
- TCP, UDP und proprietäre Protokolle

Bidirektionale Kommunikation

In einigen Fällen benötigen Anwendungen bidirektionalen Verkehr, um erwartungsgemäß zu funktionieren. Häufige Anwendungsfälle sind Webhooks oder Benachrichtigungsdienste. Im Allgemeinen können Sie dies erreichen, indem Sie eine WebSocket Verbindung zwischen dem Server und dem Client herstellen. Diese Verbindung hält die TCP-Sitzung offen und ermöglicht es beiden Teilnehmern, Datenverkehr über die Verbindung zu senden. Die meisten der in diesem Handbuch beschriebenen Dienste unterstützen nativ WebSocket, einschließlich Network Load Balancers, Application Load Balancers, Amazon API Gateway und AWS AppSync (über private Echtzeit-Endpunkte). AWS PrivateLink

In anderen Fällen benötigt eine Anwendung auf der SaaS-Anbieterseite möglicherweise Zugriff auf Ressourcen auf der Verbraucherseite, z. B. eine Datenbank. Wenn Sie eine Verbindung über bidirektionale Kanäle herstellen, z. B. eine AWS Site-to-Site VPN Verbindung, ist das kein Problem.

Andererseits unterstützt Elastic Load Balancing nur unidirektionalen Datenverkehr. AWS PrivateLink Wenn Sie diese Dienste verwenden, müssen Sie einen anderen Netzwerkpfad für den Datenverkehr einrichten, der von Ihrem SaaS-Angebot ausgeht. Dies kann beispielsweise eine zusätzliche AWS PrivateLink Verbindung sein, die in umgekehrter Richtung verläuft.

TCP, UDP und proprietäre Protokolle

Viele Anwendungen werden über HTTP oder HTTPS bedient, aber nicht alle. Einige verwenden möglicherweise zusätzlich zu TCP weitere Layer-7-Protokolle, z. B. Message Queuing Telemetry Support (MQTT). Andere könnten sogar UDP verwenden, um Verbraucher zu bedienen. In seltenen Fällen verwenden Dienste proprietäre Protokolle, die innerhalb von Paketen übertragen werden müssen (Schicht 3). Für diese Szenarien ist es wichtig zu verstehen, welche Dienste Ihr SaaS-Angebot unterstützen.

Für Layer-3-Dienste können Sie Network Load Balancer verwenden AWS PrivateLink , die beide den gesamten TCP- und UDP-Verkehr unterstützen.

Für Layer-7-Services CloudFront unterstützen Application Load Balancers und Amazon HTTP WebSocket, HTTPS und Google Remote Procedure Calls (gRPC). In ähnlicher Weise unterstützen Amazon API Gateway und AWS AppSync beide HTTP, HTTPS und WebSocket. Amazon CloudFront ist der einzige Dienst, der derzeit HTTP/3 unterstützt.

Sie können Amazon VPC Lattice verwenden, um Layer-7-Anwendungen und Layer-3-Ressourcen zu verbinden. Es unterstützt HTTP-, HTTPS-, gRPC-, TCP- und TLS-Passthrough.

Wenn die Anwendung Datenverkehr nur über Layer 3 bereitstellen kann, ist es wichtig, dass Sie zentrale AWS Netzwerkdienste wie, AWS Transit Gateway AWS Direct Connect AWS Site-to-Site VPN, und VPC-Peering verwenden. Der Datenverkehr sollte dann direkt vom SaaS-Verbraucher zur Rechenschicht des SaaS-Angebots weitergeleitet werden.

Anti-Pattern für den Netzwerkzugriff in der AWS Cloud

Ein Anti-Pattern ist eine häufig verwendete Lösung für ein wiederkehrendes Problem, bei dem die Lösung kontraproduktiv, ineffektiv oder weniger wirksam als eine Alternative ist. Die in diesem Abschnitt genannten Designoptionen funktionieren in der Regel, sind jedoch mit erheblichen Nachteilen verbunden. Wenn möglich, sollten sie vermieden werden, da bessere Alternativen verfügbar sind.

In diesem Abschnitt werden die folgenden Anti-Pattern-Probleme und Herausforderungen behandelt:

- Nichtübereinstimmung der Verfügbarkeitszone mit AWS PrivateLink
- AWS Site-to-Site VPN Verbindungen zwischen AWS-Konten

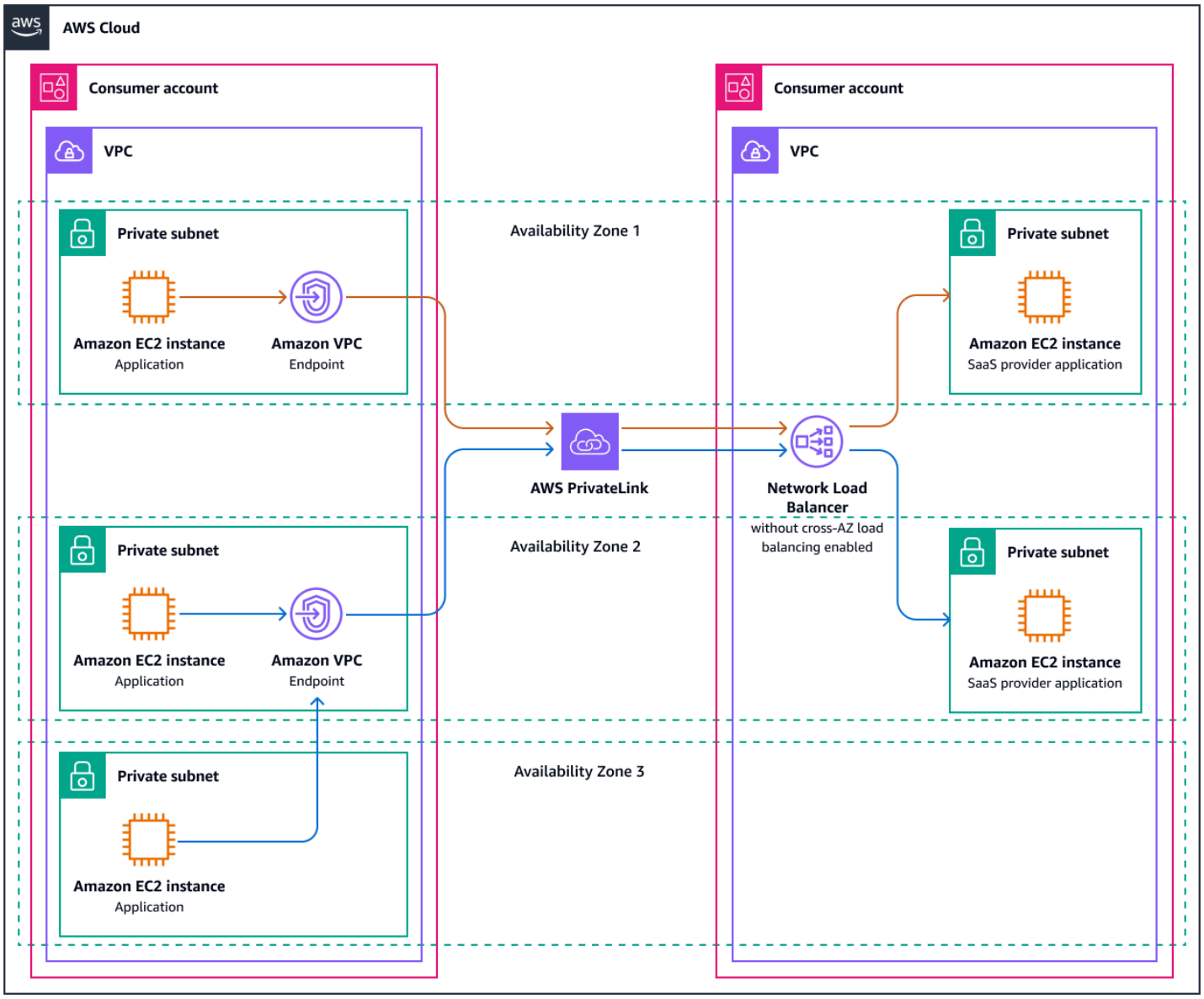
Nichtübereinstimmung der Verfügbarkeitszone mit AWS PrivateLink

Bei der Bereitstellung des Zugriffs auf eine Anwendung über AWS PrivateLink können SaaS-Verbraucher VPC-Endpunkte nur in den Availability Zones erstellen, in denen die Anwendung bereitgestellt wird. Wenn die Anwendung beispielsweise in `use1-az1` und bereitgestellt wird`use1-az2`, kann der Verbraucher keinen VPC-Endpunkt in `use1-az3` bereitstellen. Wir empfehlen, das SaaS-Angebot in jeder Availability Zone bereitzustellen. Die meisten AWS-Regionen haben drei Availability Zones, obwohl einige mehr haben. Eine umfassende Liste finden Sie unter Regionen und Availability Zones. Berücksichtigen Sie bei der Auswahl einer die Anzahl der Availability Zones AWS-Region.

> **Note**
>
> Die Namen der Verfügbarkeitszonen unterscheiden sich von denen der Availability Zone IDs. Weitere Informationen finden Sie unter Availability Zone IDs für Ihre AWS Ressourcen.

Wenn sich ein SaaS-Anbieter dafür entscheidet, nicht in allen Availability Zones zu implementieren, hat das einige Konsequenzen. Gehen Sie davon aus, dass das SaaS-Angebot in `use1-az1` und bereitgestellt wird`use1-az2`, der Verbraucher jedoch alle drei Availability Zones verwendet, einschließlich`use1-az3`. Die VPC-Endpunkte der Schnittstelle werden auf der Verbraucherseite in `use1-az1` und bereitgestellt`use1-az2`, und jetzt `use1-az3` muss die Anwendung auf einen dieser Endpunkte zugreifen. Zuallererst muss der Verkehr von den Subnetzen in den nicht

übereinstimmenden Availability Zones zu den jeweiligen VPC-Endpunkten zugelassen werden. Der Verbraucher kann sich dafür entscheiden, den regionalen AWS PrivateLink DNS-Namen zu verwenden, der in einen der beiden VPC-Endpunkte aufgelöst werden kann und der Datenverkehr gleichmäßig zwischen den beiden verteilt wird. Oder der Verbraucher kann sich dafür entscheiden, den Verkehr direkt an einen Endpunkt zu senden, z. B. `use1-az2` Dies führt dazu, dass 67% des Datenverkehrs auf der Anbieterseite ankommen `use1-az2` und 33% in`use1-az1`. Die folgende Abbildung zeigt dieses Szenario.



Bei einer großen Anzahl von Verbrauchern und einer ungleichmäßigen Verteilung des Datenverkehrs kann es vorkommen, dass ein Workload in einer Availability Zone auf Kapazitätsprobleme und in einer anderen unter Kapazität stößt. Um dieses Problem zu lösen, kann der SaaS-Anbieter beschließen, den Datenverkehr auf seiner Seite gleichmäßig zu verteilen, indem er den

zonenübergreifenden Lastenausgleich auf dem Network Load Balancer aktiviert. Dadurch fallen zusätzliche Gebühren an.

Wenn der Dienstanbieter nur einer Availability Zone entspricht, wird der gesamte Datenverkehr über einen einzigen Endpunkt geleitet. Dies führt zu einem noch größeren Ungleichgewicht. Infolgedessen ist das SaaS-Angebot für den Verbraucher nicht mehr hochverfügbar. Für den Verbraucher spielt es keine Rolle, ob die Anwendung über zusätzliche Availability Zones bereitgestellt wird, die er selbst nicht nutzt. Im schlimmsten Fall ist ein SaaS-Anbieter möglicherweise nicht in der Lage, einen Verbraucher zu bedienen, der keine der gleichen Availability Zones verwendet.

In dem seltenen Fall, dass es für den SaaS-Anbieter keine praktikable Option gibt, seine Anwendung über alle Availability Zones bereitzustellen, ist es auch möglich, ein Subnetz nur in den fehlenden Availability Zones zu erstellen und den Service dann auf diese leeren Availability Zones auszudehnen. Durch zonenübergreifendes Load Balancing kann der eingehende Verkehr dann auf die eigentlichen Anwendungsendpunkte in den anderen Availability Zones verteilt werden.

AWS Site-to-Site VPN Verbindungen zwischen AWS-Konten

Unternehmen, die von lokalen Umgebungen in die Cloud migrieren, versuchen manchmal, das gesamte Netzwerk nach oben zu verlagern. Dies kann zu Problemen führen, da es erhebliche Unterschiede zwischen lokalen und Cloud-Netzwerkpraktiken gibt. Wenn diese Änderung der Denkweise nicht stattfindet, können Dinge wie AWS Site-to-Site VPN Verbindungen von einer VPC zu einer anderen VPC passieren. Bei diesem Ansatz werden die Vorteile der speziell entwickelten Netzwerkdienste in der nicht genutzt AWS Cloud, die die Verwaltung vereinfachen und die Leistung verbessern. Die Anpassung an Cloud-native Designs trägt zur Reduzierung des Betriebsaufwands bei und führt zu einer zuverlässigeren, skalierbareren Konnektivität zwischen. VPCs

Wenn Sie darüber nachdenken, diese Konnektivitätsoption als SaaS-Anbieter anzubieten, fragen Sie sich selbst oder den Verbraucher, warum sie verwendet werden AWS Site-to-Site VPN sollte. Gehen Sie dann von diesen Anforderungen ausgehend von diesen Anforderungen zurück, um eine bessere Konnektivitätsoption zu finden. Der Abschnitt zum Vergleich der Servicefunktionen dieses Handbuchs enthält eine Matrix, anhand derer Sie Optionen identifizieren können. Anschließend können Sie die entsprechenden Abschnitte dieses Handbuchs durcharbeiten, um einen architektonischen Ansatz zu finden, der auf Ihren Anwendungsfall zugeschnitten ist.

Nächste Schritte

In diesem Leitfaden wurden verschiedene Netzwerkzugriffsansätze in verschiedenen Szenarien beschrieben und die Vor- und Nachteile der einzelnen Architekturen beschrieben. Sie sollten verstehen, warum die Wahl eines Netzwerkzugriffsansatzes keine rein technologische Diskussion sein sollte. Die Abstimmung zwischen Geschäft und Technologie ist von entscheidender Bedeutung. Die folgenden nächsten Schritte und Empfehlungen können Ihnen helfen, Ihre Netzwerkarchitekturstrategie zu bewerten und zu standardisieren, indem Sie die aktuellen Kapazitäten bewerten, Marktanforderungen analysieren und Kontrollmaßnahmen implementieren.

In diesem Abschnitt werden folgende Themen behandelt:

- Bewertung der aktuellen Architektur und Fähigkeiten
- Markt- und Kundenanalysen
- Strategische Ausrichtung
- Standardisierung
- Governance
- Wiederholung

Bewertung der aktuellen Architektur und Fähigkeiten

Überprüfen Sie die aktuelle Netzwerkarchitektur anhand relevanter Datenquellen, wie z. B. dem Selbstbewertungsrahmen in diesem Leitfaden, den aktuellen regulatorischen Anforderungen und der aktuellen Marktlage (sowohl in Bezug auf Ihre Kunden als auch in Bezug auf eine Wettbewerbsanalyse). Erwägen Sie beispielsweise die Verwendung des AWS Well-Architected Framework, das auf jahrzehntelanger Erfahrung mit dem Betrieb von Produktionssystemen in großem Maßstab in der basiert. AWS Cloud

Prüfen Sie alle möglichen Ausnahmen, Einzelfälle und historische Produktentscheidungen. Seien Sie neugierig, fordern Sie sie heraus und gehen Sie nicht automatisch davon aus, dass sie gültig sind. Kundenanforderungen von vor Jahren sind möglicherweise nicht mehr gültig. Wenn Sie Annahmen in Frage stellen, können Sie Ihre Architektur vereinfachen und ihre Komplexität reduzieren.

Einfach ausgedrückt: Dokumentieren Sie die Beobachtungen, sodass sie von verschiedenen Rollen in Ihrem Unternehmen abgerufen und verstanden werden können. Erfassen Sie, wo sich der aktuelle Status vom Zielstatus unterscheidet, was der Zielstatus ist, welche Auswirkungen es hat und wann

Beobachtungen gemacht wurden. Die Aufzeichnung dieser Informationen hilft Ihren Organisationen, Entscheidungen auf der Grundlage aktueller Daten zu treffen.

Markt- und Kundenanalysen

Sammeln Sie Einblicke in Markttrends. Was ist derzeit die bevorzugte Art von Verbrauchern, auf SaaS-Angebote wie Ihre zuzugreifen? Treffen Sie Ihre Kunden immer noch dort, wo sie sind? Haben sich die Kundenkohorten oder das Verhalten geändert? Haben Ihre Führungskräfte den Zug in Richtung eines neuen Marktes, einer Region mit spezifischen regulatorischen Anforderungen oder einer neuen Kundengruppe gesteuert? Hat sich Ihr Geschäfts- oder Betriebsmodell geändert? Denken Sie zum Beispiel darüber nach, Ihre Dienstleistungen mit einem White-Labeling zu versehen? Beinhaltet Ihr Wachstumsplan die Zusammenarbeit mit Partnern, sodass Ihr Service für Kunden verfügbar ist, wenn sie sich mit diesen Partnern verbinden?

Strategische Ausrichtung

Wenn Sie Ihre aktuellen Fähigkeiten, Ihre aktuelle Architektur, Ihren Markt und Ihre Kunden verstanden haben, sollten Sie ein Treffen zur strategischen Ausrichtung einberufen. Stellen Sie sich gemeinsam mit den relevanten Produkt-, Geschäfts- und Technologieakteuren die Frage, welche Anforderungen noch gültig sind und welche neuen Anforderungen berücksichtigt werden müssen. Finden Sie Möglichkeiten, die Komplexität zu reduzieren, indem Sie Anforderungen streichen, die nicht mehr benötigt werden. Dabei handelt es sich nicht um einen Entwurf durch ein Komitee. Das Entwicklungsteam muss die eigentliche Architektur und die Implementierungsdetails vorbereiten und selbst in die Hand nehmen. Bei diesem Treffen sollte jedoch geklärt werden, warum diese Anforderungen den größtmöglichen Nutzen für Ihre Kunden und Ihr Unternehmen bieten.

Standardisierung

Um Kunden anzulocken, könnte es verlockend sein, jedem Benutzer die Wahl zu lassen, wie er eine Verbindung zu Ihrem Dienst herstellen möchte. Schließlich könnte jede Lösung technisch funktionieren, und Sie verfügen möglicherweise auch über das Know-how und die Ressourcen, um sie alle zu verwalten und zu betreiben. Das kann bis zu einem gewissen Punkt gut funktionieren, aber wenn Ihr Unternehmen wächst, wird es schwierig, es zu verwalten. Ihr Observability-Stack muss Metriken aus mehreren Lösungen unterstützen, und die Zuverlässigkeitsingenieure Ihrer Website müssen diese auch verstehen können. Sie benötigen up-to-date Dokumentation für jeden Konnektivitätsansatz. Wesentliche Änderungen an Ihrer Anwendung müssen anhand der einzelnen

von Ihnen angebotenen Zugriffsansätze bewertet werden. Sie müssen für jeden Zugriffsansatz Automatisierungen und Infrastruktur als Code (IaC) schreiben und verwalten. Der zusätzliche Aufwand, der entsteht, wenn der Zugriff auf Ihren Service nicht standardisiert wird, muss gegen die Flexibilität abgewogen werden, die Sie Ihren Kunden bieten möchten.

Wenn Sie sich bei Ihrer Entscheidungsfindung von einem Polarstern leiten lassen möchten, empfehlen wir eine Standardisierung. Die Standardisierung der Art und Weise, wie Ihre Kunden mit den von Ihnen angebotenen Dienstleistungen interagieren, ist in der Regel die wirksamste Maßnahme, die Sie ergreifen können, um viele Erfolgskennzahlen in Ihrem Unternehmen zu verbessern. Standardisierung erleichtert es Produktteams, die Kostenstruktur Ihrer Dienstleistungen zu verstehen und datengestützte Produktentscheidungen zu treffen. In einer Umgebung, die nach vordefinierten Standards entwickelt, eingeführt und betrieben wird, ist es für Betriebsteams einfacher, Probleme zu beheben und Teile des Fehlerbehebungsprozesses zu automatisieren. Es kann Ihnen helfen, Anomalien, unerwartetes Verhalten oder Aktionen eines böswilligen Akteurs zu erkennen. Durch die Standardisierung wird auch die technische Verschuldung reduziert. Die Entwicklungsteams benötigen weniger Zyklen, um Änderungen an der Produktion zu testen und umzusetzen. Es kann auch Ihre Markteinführung beschleunigen, den Erfolg beim Self-Service-Onboarding verbessern und das regulatorische Risiko verringern.

Wir empfehlen Ihnen daher, auch alle derzeit geltenden Sonderregelungen zu überprüfen. Quantifizieren Sie die Anzahl der Betriebszyklen, die Sie für die Unterstützung Ihrer Bestandskunden aufwenden. Vergleichen Sie Ihre Ergebnisse mit historischen Daten und beurteilen Sie, ob Ihr derzeitiger Ansatz für die kommenden Jahre geeignet ist. Wann immer es notwendig ist, von Standards abzuweichen, stellen Sie die Anforderungen, die diesen Anforderungen zugrunde liegen, in Frage. Beurteilen Sie die Auswirkungen und wägen Sie die unmittelbaren Vorteile mit langfristigen Verpflichtungen ab.

In Fällen, in denen Anpassungen unvermeidlich sind, aber im Widerspruch zu Ihren Standards stehen, sollten Sie ein Modell der gemeinsamen Verantwortung in Betracht ziehen. Bei diesem Modell sind Ihre Produkte weitgehend vor den gewünschten Änderungen geschützt, und die Anpassung erfolgt in einer minimalistischen, speziellen Umgebung. Ein Beispiel finden Sie im Verbindung mit einer Transit-VPC-Architektur herstellen Abschnitt.

Governance

Für die Einhaltung regulatorischer Anforderungen und Ihrer eigenen internen Standards ist Unternehmensführung unerlässlich. Wenn eine angemessene Unternehmensführung vorhanden ist, können Sie kontrollieren, wo und wie Standards durchgesetzt werden. Sie richten auch Kontrollen

ein, um Abweichungen von den Standards aufzudecken und die Ressourcenverantwortlichen über notwendige Korrekturmaßnahmen zu informieren. AWS Organizations, AWS ConfigAWS CloudTrail, und AWS Control Towersind nur einige von vielen, AWS-Services die Ihnen bei der Verwaltung und Steuerung Ihrer Workloads in der helfen können. AWS Cloud

Wiederholung

Nutzen Sie die Erkenntnisse aus Ihren ersten Bemühungen und richten Sie einen einfachen, wiederholbaren Prozess ein, um auch in future auf dem Laufenden zu bleiben. Definieren Sie, von welchen Rollen Sie Inputs benötigen, wie oft, wie genau die Daten sein müssen, wie die Daten geteilt werden und wer darauf reagiert.

Ressourcen

AWS Dokumentation

- Integration von Diensten Dritter in die AWS Cloud (AWS Prescriptive Guidance)
- SaaS-Autorisierung und API-Zugriffskontrolle für mehrere Mandanten (AWS Prescriptive Guidance)
- Verwaltung von Mandanten über mehrere SaaS-Produkte hinweg auf einer einzigen Kontrollebene (AWS Prescriptive Guidance)
- Was ist? AWS Direct Connect (Direct Connect Dokumentation)
- Was ist AWS PrivateLink? (Amazon VPC-Dokumentation)
- Was ist AWS Site-to-Site VPN? (AWS Site-to-Site VPN Dokumentation)
- Was ist AWS Transit Gateway? (Amazon VPC-Dokumentation)
- Was ist VPC-Peering? (Amazon VPC-Dokumentation)

Andere Ressourcen AWS

- Verbindungsoptionen für Amazon Virtual Private Cloud (AWS Whitepaper)
- AWS re:Invent 2021 — So wählen Sie den richtigen Load Balancer für Ihre Workloads aus () AWS YouTube
- Was ist SaaS? (AWS Webseite)
- AWS SaaS Factory-Programm (AWS Partner Programm)
- Leitfaden für Multi-Tenant-Architekturen auf AWS (AWS Lösungsbibliothek)

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	—	12. September 2025

AWS Glossar zu präskriptiven Leitlinien

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

Zahlen

7 Rs

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

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

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

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

A

ABAC

Siehe attributbasierte Zugriffskontrolle.

abstrahierte Dienste

Siehe Managed Services.

ACID

Siehe Atomarität, Konsistenz, Isolierung und Haltbarkeit.

Aktiv-Aktiv-Migration

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

Aktiv-Passiv-Migration

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

Aggregatfunktion

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

AI

Siehe künstliche Intelligenz.

AIOps

Siehe Operationen im Bereich künstliche Intelligenz.

Anonymisierung

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

Anti-Muster

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

Anwendungssteuerung

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

Anwendungsportfolio

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

künstliche Intelligenz (KI)

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

Operationen mit künstlicher Intelligenz (AIOps)

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

Asymmetrische Verschlüsselung

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

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

Atomizität, Konsistenz, Isolierung, Haltbarkeit (ACID)

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

Attributbasierte Zugriffskontrolle (ABAC)

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

autoritative Datenquelle

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

Availability Zone

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

AWS Framework für die Einführung der Cloud (AWS CAF)

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

AWS Workload-Qualifizierungsrahmen (AWS WQF)

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

B

schlechter Bot

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

BCP

Siehe Planung der Geschäftskontinuität.

Verhaltensdiagramm

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

Big-Endian-System

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

Binäre Klassifikation

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

Bloom-Filter

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

Blau/Grün-Bereitstellung

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

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

Bot

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

Botnetz

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

branch

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

Zugang durch Glasbruch

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

Brownfield-Strategie

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

Puffer-Cache

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

Geschäftsfähigkeit

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

Planung der Geschäftskontinuität (BCP)

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

C

CAF

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

Bereitstellung auf Kanaren

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

CCoE

Weitere Informationen finden Sie im Cloud Center of Excellence.

CDC

Siehe Erfassung von Änderungsdaten.

Erfassung von Datenänderungen (CDC)

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

Chaos-Technik

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

CI/CD

Siehe Continuous Integration und Continuous Delivery.

Klassifizierung

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

clientseitige Verschlüsselung

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

Cloud-Exzellenzzentrum (CCoE)

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

Cloud Computing

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

Cloud-Betriebsmodell

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

Phasen der Einführung der Cloud

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

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

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

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

CMDB

Siehe Datenbank für das Konfigurationsmanagement.

Code-Repository

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

Kalter Cache

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

Kalte Daten

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

Computer Vision (CV)

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

Drift in der Konfiguration

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

Verwaltung der Datenbankkonfiguration (CMDB)

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

Konformitätspaket

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

Kontinuierliche Bereitstellung und kontinuierliche Integration (CI/CD)

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

CV

Siehe Computer Vision.

D

Daten im Ruhezustand

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

Datenklassifizierung

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

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

Datendrift

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

Daten während der Übertragung

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

Datennetz

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

Datenminimierung

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

Datenperimeter

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

Vorverarbeitung der Daten

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

Herkunft der Daten

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

betroffene Person

Eine Person, deren Daten gesammelt und verarbeitet werden.

Data Warehouse

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

Datenbankdefinitionssprache (DDL)

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

Datenbankmanipulationssprache (DML)

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

DDL

Siehe Datenbankdefinitionssprache.

Deep-Ensemble

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

Deep Learning

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

defense-in-depth

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

delegierter Administrator

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

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

Einsatz

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

Entwicklungsumgebung

Siehe Umgebung.

Detektivische Kontrolle

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

Abbildung des Wertstroms in der Entwicklung (DVSM)

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

digitaler Zwilling

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

Maßtabelle

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

Katastrophe

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

Notfallwiederherstellung (DR)

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

DML

Siehe Sprache zur Datenbankmanipulation.

Domainorientiertes Design

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

DR

Siehe Disaster Recovery.

Erkennung von Driften

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

DVSM

Siehe Abbildung des Wertstroms in der Entwicklung.

E

EDA

Siehe explorative Datenanalyse.

EDI

Siehe elektronischer Datenaustausch.

Edge-Computing

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

elektronischer Datenaustausch (EDI)

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

Verschlüsselung

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

Verschlüsselungsschlüssel

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

Endianismus

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

Endpunkt

Siehe Service-Endpunkt.

Endpunkt-Services

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

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

Unternehmensressourcenplanung (ERP)

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

Envelope-Verschlüsselung

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

Umgebung

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

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

Epics

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

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

ERP

Siehe Enterprise Resource Planning.

Explorative Datenanalyse (EDA)

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

F

Faktentabelle

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

schnell scheitern

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

Grenze zur Fehlerisolierung

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

Feature-Zweig

Siehe Zweig.

Features

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

Bedeutung der Feature

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

Featuretransformation

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

Eingabeaufforderung mit wenigen Klicks

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

FGAC

Siehe detaillierte Zugriffskontrolle.

Feinkörnige Zugriffskontrolle (FGAC)

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

Flash-Cut-Migration

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

FM

Siehe Fundamentmodell.

Fundamentmodell (FM)

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

G

Generative KI

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

Geoblocking

Siehe geografische Einschränkungen.

Geografische Einschränkungen (Geoblocking)

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

Gitflow-Workflow

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

goldenes Bild

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

Greenfield-Strategie

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

Integritätsschutz

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

H

HEKTAR

Siehe Hochverfügbarkeit.

Heterogene Datenbankmigration

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

hohe Verfügbarkeit (HA)

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

historische Modernisierung

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

Daten zurückhalten

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

Homogene Datenbankmigration

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

heiße Daten

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

Hotfix

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

Hypercare-Phase

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

I

IaC

Sehen Sie Infrastruktur als Code.

Identitätsbasierte Richtlinie

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

Leerlaufanwendung

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

IIoT

Siehe Industrielles Internet der Dinge.

unveränderliche Infrastruktur

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

Eingehende (ingress) VPC

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

Inkrementelle Migration

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

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

Industrie 4.0

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

Infrastruktur

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

Infrastructure as Code (IaC)

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

industrielles Internet der Dinge (T) IIo

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

Inspektions-VPC

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

Internet of Things (IoT)

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

Interpretierbarkeit

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

IoT

Siehe Internet der Dinge.

IT information library (ITIL, IT-Informationsbibliothek)

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

T service management (ITSM, IT-Servicemanagement)

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

BIS

Siehe IT-Informationsbibliothek.

ITSM

Siehe IT-Servicemanagement.

L

Labelbasierte Zugangskontrolle (LBAC)

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

Landing Zone

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

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

großes Sprachmodell (LLM)

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

Große Migration

Eine Migration von 300 oder mehr Servern.

SCHWARZ

Siehe Labelbasierte Zugriffskontrolle.

Geringste Berechtigung

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

Lift and Shift

Siehe 7 Rs.

Little-Endian-System

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

LLM

Siehe großes Sprachmodell.

Niedrigere Umgebungen

Siehe Umgebung.

M

Machine Learning (ML)

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

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

Hauptzweig

Siehe Filiale.

Malware

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

verwaltete Dienste

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

Manufacturing Execution System (MES)

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

MAP

Siehe Migration Acceleration Program.

Mechanismus

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

Mitgliedskonto

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

MES

Siehe Manufacturing Execution System.

Message Queuing-Telemetrietransport (MQTT)

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

Microservice

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

Microservices-Architekturen

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

Migration Acceleration Program (MAP)

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

Migration in großem Maßstab

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

Migrationsfabrik

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

Migrationsmetadaten

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

Migrationsmuster

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

Migration Portfolio Assessment (MPA)

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

Migration Readiness Assessment (MRA)

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

Migrationsstrategie

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

ML

Siehe maschinelles Lernen.

Modernisierung

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

Bewertung der Modernisierungsfähigkeit

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

Monolithische Anwendungen (Monolithen)

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

MPA

Siehe Bewertung des Migrationsportfolios.

MQTT

Siehe Message Queuing-Telemetrietransport.

Mehrklassen-Klassifizierung

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

veränderbare Infrastruktur

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

O

OAC

Siehe Origin Access Control.

EICHE

Siehe Zugriffsidentität von Origin.

COM

Siehe organisatorisches Change-Management.

Offline-Migration

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

OI

Siehe Betriebsintegration.

OLA

Siehe Vereinbarung auf operativer Ebene.

Online-Migration

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

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

OPC-UA

Siehe Open Process Communications — Unified Architecture.

Offene Prozesskommunikation — Einheitliche Architektur (OPC-UA)

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

Vereinbarung auf Betriebsebene (OLA)

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

Überprüfung der Betriebsbereitschaft (ORR)

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

Betriebstechnologie (OT)

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

Betriebsintegration (OI)

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

Organisationspfad

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

Organisatorisches Veränderungsmanagement (OCM)

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

Ursprungszugriffskontrolle (OAC)

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

Ursprungszugriffsidentität (OAI)

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

ORR

Weitere Informationen finden Sie unter Überprüfung der Betriebsbereitschaft.

NICHT

Siehe Betriebstechnologie.

Ausgehende (egress) VPC

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

P

Berechtigungsgrenze

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

persönlich identifizierbare Informationen (PII)

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

Personenbezogene Daten

Siehe persönlich identifizierbare Informationen.

Playbook

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

PLC

Siehe programmierbare Logiksteuerung.

PLM

Siehe Produktlebenszyklusmanagement.

policy

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

Polyglotte Beharrlichkeit

Unabhängige Auswahl der Datenspeichertechnologie eines Microservices auf der Grundlage von Datenzugriffsmustern und anderen Anforderungen. Wenn Ihre Microservices über dieselbe Datenspeichertechnologie verfügen, kann dies zu Implementierungsproblemen oder zu

Leistungseinbußen führen. Microservices lassen sich leichter implementieren und erzielen eine bessere Leistung und Skalierbarkeit, wenn sie den Datenspeicher verwenden, der ihren Anforderungen am besten entspricht.

Portfoliobewertung

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

predicate

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

Prädikat Pushdown

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

Präventive Kontrolle

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

Prinzipal

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

Datenschutz von Natur aus

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

Privat gehostete Zonen

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

proaktive Steuerung

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

Produktlebenszyklusmanagement (PLM)

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

Produktionsumgebung

Siehe Umgebung.

Speicherprogrammierbare Steuerung (SPS)

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

schnelle Verkettung

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

Pseudonymisierung

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

publish/subscribe (pub/sub)

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

Q

Abfrageplan

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

Abfrageplanregression

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

R

RACI-Matrix

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

RAG

Siehe Erweiterte Generierung beim Abrufen.

Ransomware

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

RASCI-Matrix

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

RCAC

Siehe Zugriffskontrolle für Zeilen und Spalten.

Read Replica

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

neu strukturieren

Siehe 7 Rs.

Recovery Point Objective (RPO)

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

Wiederherstellungszeitziel (RTO)

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

Refaktorierung

Siehe 7 Rs.

Region

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

Regression

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

rehosten

Siehe 7 Rs.

Veröffentlichung

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

umziehen

Siehe 7 Rs.

neue Plattform

Siehe 7 Rs.

Rückkauf

Siehe 7 Rs.

Ausfallsicherheit

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

Ressourcenbasierte Richtlinie

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

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

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

Reaktive Kontrolle

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

Beibehaltung

Siehe 7 Rs.

zurückziehen

Siehe 7 Rs.

Retrieval Augmented Generation (RAG)

Eine generative KI-Technologie, bei der ein LLM auf eine maßgebliche Datenquelle verweist, die sich außerhalb seiner Trainingsdatenquellen befindet, bevor eine Antwort generiert wird. Ein RAG-Modell könnte beispielsweise eine semantische Suche in der Wissensdatenbank oder in

benutzerdefinierten Daten einer Organisation durchführen. Weitere Informationen finden Sie unter Was ist RAG.

Drehung

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

Zugriffskontrolle für Zeilen und Spalten (RCAC)

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

RPO

Siehe Recovery Point Objective.

RTO

Siehe Ziel für die Erholungszeit.

Runbook

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

S

SAML 2.0

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

SCADA

Siehe Aufsichtskontrolle und Datenerfassung.

SCP

Siehe Richtlinie zur Dienstkontrolle.

Secret

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

Sicherheit durch Design

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

Sicherheitskontrolle

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

Härtung der Sicherheit

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

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

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

Automatisierung von Sicherheitsreaktionen

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

Serverseitige Verschlüsselung

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

Service-Kontrollrichtlinie (SCP)

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

Service-Endpunkt

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

Service Level Agreement (SLA)

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

Service-Level-Indikator (SLI)

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

Service-Level-Ziel (SLO)

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

Modell der geteilten Verantwortung

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

SIEM

Siehe Sicherheitsinformations- und Event-Management-System.

Single Point of Failure (SPOF)

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

SLA

Siehe Service Level Agreement.

SLI

Siehe Service-Level-Indikator.

ALSO

Siehe Service-Level-Ziel.

split-and-seed Modell

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

SPOTTEN

Siehe Single Point of Failure.

Sternschema

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

Strangler-Fig-Muster

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

unter Schrittweises Modernisieren älterer Microsoft ASP.NET (ASMX)-Webservices mithilfe von Containern und Amazon API Gateway.

Subnetz

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

Aufsichtskontrolle und Datenerfassung (SCADA)

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

Symmetrische Verschlüsselung

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

synthetisches Testen

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

Systemaufforderung

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

T

tags

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

Zielvariable

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

Aufgabenliste

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

Testumgebungen

Siehe Umgebung.

Training

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

Transit-Gateway

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

Stammbasierter Workflow

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

Vertrauenswürdiger Zugriff

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

Optimieren

Aspekte Ihres Trainingsprozesses ändern, um die Genauigkeit des ML-Modells zu verbessern. Sie können das ML-Modell z. B. trainieren, indem Sie einen Beschriftungssatz generieren,

Beschriftungen hinzufügen und diese Schritte dann mehrmals unter verschiedenen Einstellungen wiederholen, um das Modell zu optimieren.

Zwei-Pizzen-Team

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

U

Unsicherheit

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

undifferenzierte Aufgaben

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

höhere Umgebungen

Siehe Umgebung.

V

Vacuuming

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

Versionskontrolle

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

VPC-Peering

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

Schwachstelle

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

W

Warmer Cache

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

warme Daten

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

Fensterfunktion

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

Workload

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

Workstream

Funktionsgruppen in einem Migrationsprojekt, die für eine bestimmte Reihe von Aufgaben verantwortlich sind. Jeder Workstream ist unabhängig, unterstützt aber die anderen Workstreams

im Projekt. Der Portfolio-Workstream ist beispielsweise für die Priorisierung von Anwendungen, die Wellenplanung und die Erfassung von Migrationsmetadaten verantwortlich. Der Portfolio-Workstream liefert diese Komponenten an den Migrations-Workstream, der dann die Server und Anwendungen migriert.

WURM

Sehen Sie einmal schreiben, viele lesen.

WQF

Siehe AWS Workload-Qualifizierungsrahmen.

einmal schreiben, viele lesen (WORM)

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

Z

Zero-Day-Exploit

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

Zero-Day-Sicherheitslücke

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

Eingabeaufforderung ohne Zwischenfälle

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

Zombie-Anwendung

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

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