Einführung des Matter-Standards für Hersteller von IoT-Geräten

AWS Prescriptive Guidance

AWS Prescriptive Guidance: Einführung des Matter-Standards für Hersteller von IoT-Geräten

Table of Contents

Einführung des Matter-Standards für Hersteller von IoT-Geräten

Tushar Patel, Vijay Ujjain und David Walters, Amazon Web Services

März 2026 (Geschichte der Dokumente)

Laut Statista wird die Zahl der Smart-Home-Nutzer weltweit bis 2029 voraussichtlich 1,9 Milliarden überschreiten. Dieses schnelle Wachstum bringt Herausforderungen in Bezug auf Betrieb und Management mit sich. Aus Sicht des Verbrauchers hat jeder Geräteanbieter eine andere Methode, um das Smart-Home-Gerät über eine App, die für diesen Gerätehersteller spezifisch ist, in ein Heimnetzwerk einzubinden. Dies macht es schwierig, eine wachsende Anzahl unterschiedlicher Gerätetypen verschiedener Anbieter zu verwalten. Aus Sicht der Gerätehersteller erhöht die Zertifizierung ihrer Smart-Home-Produkte in verschiedenen Ökosystemen ebenfalls die Kosten und die Komplexität ihrer Geschäftsprozesse. Dies kann beispielsweise für dasselbe Gerätemodell unterschiedliche SKUs Anforderungen erfordern. Es ist ein zusätzlicher Aufwand, eine überzeugende Benutzererlebnis-App aufrechtzuerhalten und regelmäßige Updates bereitzustellen, wodurch Ressourcen entlastet werden, die sich nicht auf die Entwicklung und Bereitstellung eines besseren Produkts konzentrieren müssen. Sowohl Verbraucher als auch Gerätehersteller würden von einem gemeinsamen Interoperabilitätsstandard für Smart-Home-Geräte profitieren. Dieser Standard ermöglicht es Geräten verschiedener Anbieter, nahtlos, sicher und zuverlässig miteinander zu interagieren. Sowohl Verbraucher als auch Gerätehersteller haben erheblich von der Einführung eines gemeinsamen Smart-Home-Interoperabilitätsstandards profitiert, der es Geräten verschiedener Anbieter ermöglicht, nahtlos, sicher und zuverlässig zusammenzuarbeiten.

Der Matter-Standard entstand aus einer aufregenden Gelegenheit für Hersteller von Internet of Things (IoT) -Geräten im Smart-Home-Bereich, das Versprechen eines einzigen Protokolls zur Verbindung von Smart-Home-Systemen tatsächlich einzulösen. Dieser Standard zielt darauf ab, die Kompatibilität und Interoperabilität zwischen Geräten verschiedener Hersteller zu verbessern. Matter ist ein offenes Smart-Home-Konnektivitätsprotokoll, das die Kommunikation zwischen IoT-Geräten, mobilen Apps und Cloud-Diensten ermöglicht.

Ziele

Bei der Integration des Matter-Standards in ihre Produkte müssen sich Hersteller von IoT-Geräten mehreren Herausforderungen stellen, bevor sie mit der Entwicklung beginnen. Matter bietet viele

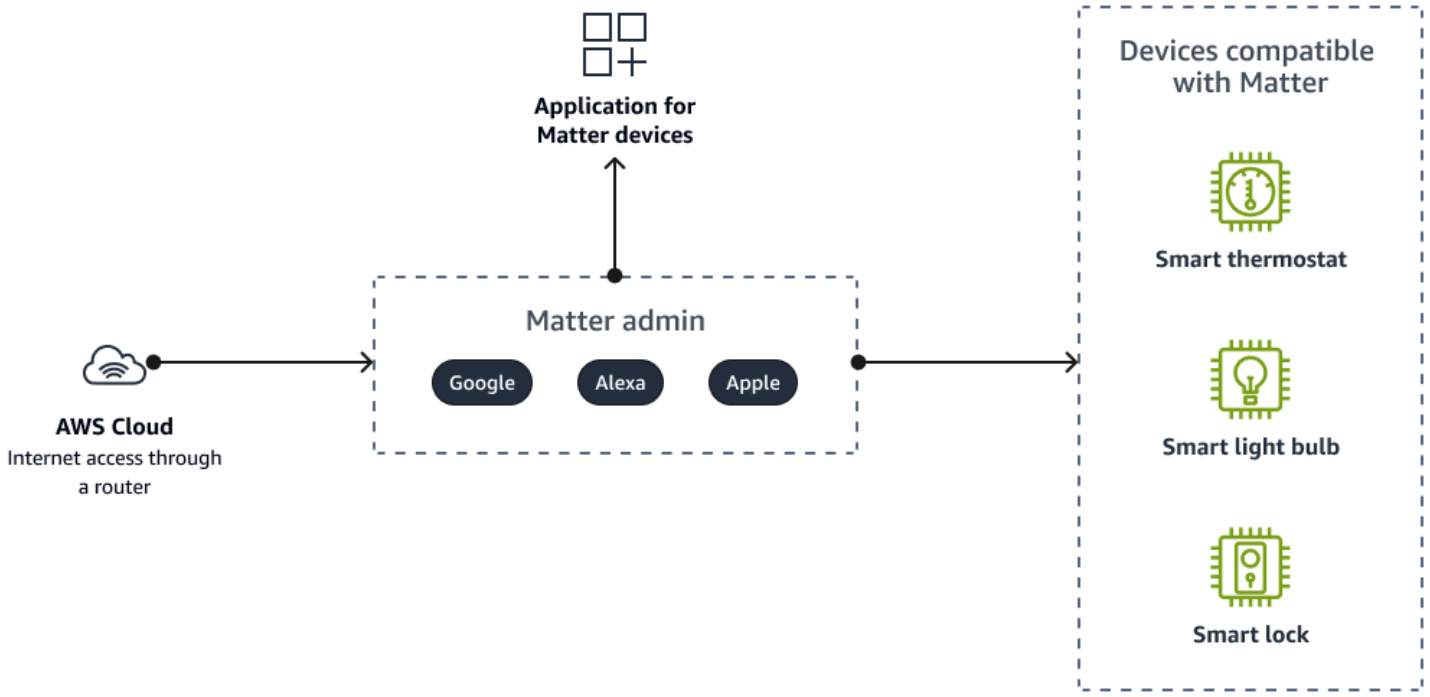
Vorteile gegenüber proprietären IoT-Protokollen, darunter Interoperabilität, Sicherheit, Einfachheit, Zuverlässigkeit und Zukunftssicherheit von Geräten. Die Integration von Matter sowohl in neue als auch in bestehende IoT-Implementierungen erfordert jedoch eine sorgfältige Planung und Strategie. Hersteller wünschen sich eine Anleitung zum Compliance-Prozess von Matter, um die Vorteile zu nutzen und gleichzeitig Fallstricke zu vermeiden. Dieser Leitfaden bietet Herstellern von IoT-Geräten umfassende Hinweise zur Einführung von Matter. Er enthält eine klare Roadmap, von der Strategie bis zur Umsetzung. Dieser Leitfaden erleichtert den Übergang zu Matter und hilft Ihnen dabei, sichere, interoperable und zukunftsfähige Produkte zu entwickeln, die im Smart-Home-Ökosystem erfolgreich sind. Mit dem richtigen strategischen Ansatz können Unternehmen die Hürden der Einführung von Matter überwinden und innovative IoT-Geräte entwickeln, die offene Standards nutzen.

Der Matter-Standard, jetzt in Version 1.5, hat sich zu einer bewährten Lösung für Hersteller von Internet of Things (IoT) -Geräten im Smart-Home-Bereich entwickelt. Dieser offene Standard hat erhebliche Verbesserungen der Kompatibilität und Interoperabilität zwischen Geräten verschiedener Hersteller gezeigt. Matter ist ein offenes Smart-Home-Konnektivitätsprotokoll, das die Kommunikation zwischen IoT-Geräten, mobilen Apps und Cloud-Diensten in wichtigen Ökosystemen wie Amazon Alexa, Google Home HomeKit, Apple und Samsung ermöglicht. SmartThings

Matter 1.5 bietet eine erweiterte Geräteunterstützung, die über die ursprüngliche Version hinausgeht und jetzt verbesserte Energiemanagementgeräte, Roboterstaubsauger, Luftqualitätssensoren, Luftreiniger und eine verbesserte Unterstützung für Kameras und Sicherheitssysteme umfasst. Der Standard bietet außerdem erweiterte Funktionen wie Multi-Admin-Funktionen, verbesserte Abläufe bei der Inbetriebnahme und erweiterte Sicherheitsprotokolle. Mit Tausenden von zertifizierten Matter-Geräten, die jetzt auf dem Markt erhältlich sind, hat das Ökosystem eine kritische Masse erreicht, sodass die Einführung von Matter für Gerätehersteller, die wettbewerbsfähig auf dem Markt sind, eher unverzichtbar als optional ist.

Dieser Leitfaden bietet Geräteherstellern einen umfassenden Überblick über Matter und die Schritte, die erforderlich sind, um Matter-konform zu werden. Es beschreibt die Vor- und Nachteile der Planung einer Strategie zur Einführung von Matter. In dem Leitfaden werden auch bewährte Verfahren zur schrittweisen Nutzung von Matter unter Beibehaltung der Unterstützung vorhandener drahtloser Protokolle vorgeschlagen. Für Hersteller von IoT-Geräten, die sich mit Smart-Home-Lösungen befassen, kann dieser Leitfaden als Grundlage für Ihre Konnektivitätsstrategie dienen.

Den Matter-Standard verstehen



Matter-Protokoll

Matter ist ein offenes Smart-Home-Konnektivitätsprotokoll, das die Kommunikation zwischen Geräten, mobilen Apps und Cloud-Diensten ermöglicht. Matter wurde von der Connectivity Standards Alliance (CSA) entwickelt und vereinfacht Konnektivität und Interoperabilität für Verbraucher und Hersteller. Matter unterstützt eine Vielzahl von Smart-Home-Kategorien. Für Verbraucher bietet Matter Onboarding, einheitliches Management und Kontrolle über alle Ökosysteme hinweg. Für Hersteller reduziert Matter die Entwicklungs- und Supportkosten durch eine einzige Zertifizierung und durch die Entwicklung von Apps. Viele große Unternehmen wie Amazon, Apple und Google fördern die Einführung von Matter. CSA bietet je nach Beteiligung der Organisation vier Mitgliedschaftsstufen an: Veranstalter, Teilnehmer, Adopter und Mitarbeiter. Mit starker Unterstützung der Branche möchte Matter Verbrauchern eine nahtlose markenübergreifende Konnektivität bieten und die Entwicklung für Hersteller rationalisieren.

Der Smart-Home-Standard von Matter ist mit der Einführung der Version 1.5 am 20. November 2025 erheblich ausgereift. Der Standard erweiterte die Unterstützung für Kamera-Streaming und Energiemanagementsysteme wie Solarenergie, Batterien und Wärmepumpen. Zu den Fortschritten

auf Protokollebene gehören Stabilitätsverbesserungen für Thread und eine bessere Integration von TV-Geräten.

Überblick darüber, wie Matter funktioniert

Matter ist ein IP-basiertes Protokoll auf Anwendungsebene für Smart-Home-Geräte in allen Anbieter-Ökosystemen. Es funktioniert auf Geräten, die verwenden. IPv6 Konzeptionell ist Materie als eine Sammlung von Netzwerkknoten organisiert, bei denen es sich um Matter-Endpunkte handelt. Im Folgenden finden Sie eine kurze Zusammenfassung der Matter-Terminologie:

- Bei Matter-Geräten handelt es sich um Smart-Home-Produkte wie Glühbirnen, Schalter, Thermostate oder Schlösser.
- Ein Matter Fabric ist das virtuelle Netzwerk, mit dem alle Geräte verbunden sind. Alle Geräte teilen sich dasselbe vertrauenswürdige Stammverzeichnis. Die Struktur bildet eine Sternnetztopologie.
- Ein Matter-Administrator erstellt, verwaltet und verwaltet die Sicherheit und die Rechte für alle Geräte auf der Fabric. Ein Administrator kann ein Hub oder eine Anwendung sein. Matter verfügt über eine Multi-Admin-Funktion, mit der ein Matter-Gerät gleichzeitig Teil mehrerer Fabrics sein kann. Beispielsweise kann ein einzelnes Matter-Gerät sowohl von einem Amazon Alexa-Gerät als auch von einem Google Home-Gerät verwaltet werden. Beide können Matter-Administratoren im selben physischen Netzwerk sein.
- Ein Matter-Beauftragter ist ein Gerät, das ein neues Matter-Gerät in Betrieb nimmt (oder einbindet). Dies kann eine App auf einem Telefon, ein Smart-Home-Gateway oder ein Matter-Administrator sein.
- Eine Matter Bridge verbindet Geräte, die kein IP-Protokoll haben, mit einer Matter Fabric.

Informationen zu den verschiedenen Rollen, die Hardware und Software in Matter übernehmen können, finden Sie unter Ein Blick hinter die Haube Ihres intelligenten Zuhauses (CSA-Blogbeitrag). Matter Version 1.4 führte Enhanced Multi-Admin mit verbesserter gemeinsamen Nutzung von Anmeldeinformationen mithilfe des Home Router Access Protocol (HRAP) ein. Matter Version 1.5 führte Kamera-Streaming ein. Matter-Versionen werden ungefähr zweimal im Jahr veröffentlicht.

Vorteile einer Zertifizierung mit Matter

Matter hat sowohl den Smart-Home-Verbrauchern als auch den Herstellern, die sie bedienen, erhebliche Vorteile gebracht. Durch die Einführung einer gemeinsamen Sprache für intelligente Geräte hat Matter den zuvor fragmentierten Markt durch vereinfachte Einrichtung, einheitliches plattformübergreifendes Management sowie erweiterte Auswahl und Flexibilität bei der Sprachsteuerung erfolgreich adressiert.

Für Verbraucher hat dieses einheitliche Erlebnis den Aufbau und die Erweiterung ihres Smart Homes deutlich weniger komplex und entmutigend gemacht. Mit Tausenden von zertifizierten Matter-Geräten, die jetzt in wichtigen Ökosystemen wie Amazon Alexa, Google Home HomeKit, Apple und Samsung erhältlich sind SmartThings, ist das Versprechen der Interoperabilität Wirklichkeit geworden. Gerätehersteller haben auch erhebliche Vorteile durch eine optimierte Zertifizierung, geringere Entwicklungskosten und einen vereinfachten Kundensupport erzielt.

Seit seiner Einführung im Jahr 2022 hat sich Matter in mehreren Versionen weiterentwickelt. Matter Version 1.5 unterstützt jetzt über 50 Gerätetypen, einschließlich der mit Spannung erwarteten Kamera-Streaming-Funktion. Der Standard hat auf dem Markt eine kritische Masse erreicht, sodass die Matter-Zertifizierung für Gerätehersteller, die wettbewerbsfähig sind, eher unverzichtbar als optional ist. Sowohl Verbraucher als auch Hersteller profitieren davon, da Matter weiterhin für mehr Interoperabilität und den Abbau von Hindernissen bei der Einführung von Smart-Home-Systemen sorgt. Insgesamt hat die Zertifizierung nach dem Matter-Standard das Wachstum des Smart-Home-Marktes beschleunigt, indem Probleme gelöst wurden, die ihn zuvor gebremst haben.

Themen

Vorteile der Matter-Zertifizierung für Smart-Home-Verbraucher

Matter bietet Verbrauchern erhebliche Vorteile. Matter bietet eine gemeinsame Sprache für Smart-Home-Geräte, sodass sie auf allen wichtigen Plattformen nahtlos zusammenarbeiten können. Durch die Zertifizierung von Geräten mit Matter profitieren Verbraucher nun von einer einfacheren Einrichtung und Verwaltung ihres Smart Homes sowie von mehr Flexibilität und Wahlmöglichkeiten bei der Steuerung ihrer Geräte.

Vereinfachte Einrichtung und einheitliches Management

Eine der größten Frustrationen, mit denen Verbraucher konfrontiert sind, sind die komplexen Einrichtungs- und Onboarding-Prozesse, die erforderlich sind, um verschiedene Smart-Home-Geräte zu bedienen und sie zum Zusammenarbeiten zu bewegen. Jedes Gerät benötigt möglicherweise eine eigene proprietäre App und ein separates Konto. Um dieses Problem zu beheben, hat Matter plug-and-play Funktionen für zertifizierte Geräte aktiviert. Das Onboarding von Matter-zertifizierten Geräten ist so einfach wie das Verbinden des Geräts mit dem lokalen Heimnetzwerk und das anschließende Verwenden des Matter-Administrators, z. B. der Alexa-App, um den QR-Code auf dem Gerät zu lesen. In Matter 1.4.1 wurde ein erweiterter Einrichtungsablauf mit QR-Codes für mehrere Geräte und NFC-Onboarding eingeführt, wodurch der Prozess noch optimierter wurde.

Diese einheitliche Einrichtung über eine einzige App bedeutet, dass Verbraucher nicht mehr mit mehreren, separaten Apps jonglieren müssen, um Geräte verschiedener Marken zu verwalten. Sie können all ihre Matter-zertifizierten Leuchten, Schlösser, Sensoren, Thermostate, Kameras, Geräte, Energiemanagementgeräte und mehr von einer einzigen Oberfläche aus anzeigen und steuern. SmartThings Nutzer von Apple HomeKit, Amazon Alexa, Google Assistant und Samsung profitieren alle davon, Matter-Geräte erkennen und steuern zu können, ohne separate Hersteller-Apps herunterladen zu müssen. Die vereinfachte Verwaltung von Smart-Home-Geräten durch ein einheitliches System reduziert die Komplexität für Verbraucher und macht den Aufbau und die Erweiterung ihrer Einrichtung viel weniger schwierig.

Verbesserte Auswahl und Flexibilität bei der Sprachsteuerung

Die Sprachsteuerung ist für Verbraucher zu einer beliebten Methode geworden, um mit ihren Smart-Home-Geräten zu interagieren. Heutzutage bestimmt die Wahl des Sprachassistenten jedoch häufig, welche Gerätemarken Sie mit Ihrer Stimme steuern können. Matter ändert dies, indem es die Sprachsteuerung in allen Ökosystemen ermöglicht.

Verbraucher erhalten die Flexibilität, zu wählen, welches Sprachassistenten-Ökosystem ihren Bedürfnissen am besten entspricht, ohne sich Gedanken über die Gerätekompatibilität machen zu müssen. Ein Nutzer, der mit dem Google-Assistenten vertraut ist, kann seine Matter-zertifizierten Geräte mit seiner Stimme steuern, auch wenn die Geräte ursprünglich für Alexa oder HomeKit andere Märkte hergestellt wurden.

Diese Kreuzkompatibilität der Sprachsteuerung schafft eine offenere Umgebung, die den Benutzern eine größere Auswahl bietet. Sie können Geräte anhand von Funktionen und Preisen auswählen, anstatt sie auf der Grundlage der Kompatibilität mit einem einzigen Ökosystem auszuwählen. Wenn

ein Benutzer in future die Sprachassistenten wechseln möchte, kann sein vorhandenes Smart-Home-Setup problemlos mitgenommen werden, da alle Geräte die gemeinsame Matter-Sprache sprechen.

Die in Matter Version 1.4 hinzugefügte erweiterte Multi-Admin-Funktion ermöglicht die gleichzeitige Steuerung eines einzelnen Geräts durch mehrere Sprachassistenten. Das bedeutet, dass Familienmitglieder ihren bevorzugten Sprachassistenten (Alexa, Google Assistant oder Siri) verwenden können, um dieselben Geräte ohne Konflikte oder zusätzliche Einstellungen zu steuern.

Vorteile der Matter-Zertifizierung für Gerätehersteller

Die Matter-Zertifizierung hilft nicht nur Verbrauchern, sondern bietet auch Herstellern intelligenter Geräte bedeutende Vorteile. Durch die Einführung des Matter-Standards können Unternehmen Vorteile erzielen, die Kosten senken und ihre Kundenreichweite erweitern. Seit der Markteinführung von Matter im Jahr 2022 und der Weiterentwicklung bis zur Version 1.5 (November 2025) wurden diese Vorteile von Herstellern aus der gesamten Smart-Home-Branche erkannt

Eine einzige Zertifizierung für alle Ökosysteme

Um die Kompatibilität zwischen Ökosystemen wie Alexa HomeKit, Google Home und Samsung sicherzustellen SmartThings, müssen Hersteller mit jeder Organisation mehrere langwierige und teure Zertifizierungsprozesse durchlaufen. Matter ändert dies, indem es eine einzige gemeinsame Zertifizierung einführt.

Gerätehersteller müssen ihre Produkte nur einmal nach dem Matter-Standard zertifizieren, um mit allen wichtigen Smart-Home-Ökosystemen und Sprachassistenten kompatibel zu sein. Dies rationalisiert die Entwicklung und reduziert die Zertifizierungskosten im Vergleich zum Status Quo erheblich. Wenn Produkte aktualisiert werden, müssen keine Ressourcen mehr für die Aufrechterhaltung separater Zertifizierungen aufgewendet werden. Eine Single Matter-Zertifizierung macht Produkte zudem zukunftssicher und gewährleistet Kompatibilität, auch wenn neue Ökosysteme entstehen.

Die CSA hat auch den Zertifizierungsprozess durch bessere Tools wie das Certification Tool, das PICS Tool und ZUTH sowie erweiterte Netzwerke von Testanbietern und eine Einrichtung für Interoperabilitätstests verbessert.

Geringere Entwicklungskosten

Matter trägt auch dazu bei, die Entwicklungskosten für Hersteller zu senken. Durch die Einführung eines gemeinsamen Konnektivitäts- und Sicherheitsstandards profitieren Unternehmen von gemeinsam genutzten Infrastrukturkomponenten, die zum gesamten Matter-Projekt beitragen.

So müssen Hersteller beispielsweise ihre eigenen Thread-Border-Router nicht mehr in ihre Produkte integrieren, wodurch diese Verantwortung den Hub-Herstellern übertragen wird. Gemeinsam genutzte Open-Source-Treiber und -Bibliotheken reduzieren überflüssigen technischen Aufwand weiter. Dank der gängigen Mechanismen zur Serviceerkennung und Geräteeinrichtung ist weniger maßgeschneiderte Anwendungsentwicklung erforderlich. Diese Senkung der Kosten für Infrastruktur und Anwendungsentwicklung kann in Form erschwinglicherer Smart-Home-Geräte an die Verbraucher weitergegeben werden.

Das Matter SDK ist seit der ersten Version erheblich ausgereift. Umfassende Entwicklungstools, Bibliotheken und Dokumentation sind jetzt verfügbar. Mit der Matter-Version 1.4.2 (Juni 2025) wurden wichtige Verbesserungen in den Bereichen Transportzuverlässigkeit, BLE-Inbetriebnahme und PSA-basierte Krypto- und Testinfrastruktur eingeführt. Diese Verbesserungen haben die Komplexität der Integration im Vergleich zu frühen Einführungsphasen reduziert und sich bei neuen Produkten beschleunigt time-to-market.

Matter unterstützt jetzt über 50 Gerätetypen in den Versionen 1.0 bis 1.5, darunter Beleuchtung, Schlösser, Thermostate, Geräte (Kühlschränke, Geschirrspüler, Backöfen, Mikrowellen), Saugroboter, Energiemanagementgeräte (Sonnenkollektoren, Batterien, Wärmepumpen), Ladegeräte für Elektrofahrzeuge, Wassermanagementgeräte, Luftqualitätssensoren und Kameras mit Streaming-Unterstützung.

Vereinfachter Kundensupport

Die derzeitige Fragmentierung auf dem Smart-Home-Markt führt zu einem hohen Kundensupport für Hersteller. Verbraucher stoßen häufig auf Probleme mit Konnektivität, Einrichtung und Kompatibilität, die behoben werden müssen. Matter zielt darauf ab, diese Probleme durch die Standardisierung der Kernfunktionen zu reduzieren.

Wenn Probleme auftreten, können Unternehmen mithilfe der gängigen Matter-Protokolle Verbindungsprobleme einfacher diagnostizieren und lösen, ohne mehrere Ökosysteme berücksichtigen zu müssen. Dies rationalisiert den Support-Prozess. Mit einer einzigen App und einheitlicher Sprachkompatibilität können Kunden außerdem leichter lernen, Geräte zu verwenden, wodurch in vielen Fällen der Bedarf an Support reduziert wird. Das vereinfachte Kundenerlebnis und

die durch Matter ermöglichte Fehlerbehebung tragen dazu bei, die langfristigen Supportkosten für Hersteller zu senken.

Überlegungen zur Zertifizierungsstrategie

Matter ermöglicht die Interoperabilität zwischen verschiedenen Smart-Home-Geräten und -Plattformen. Eine Zertifizierung mit Matter ist jedoch möglicherweise nicht immer die beste Wahl für Gerätehersteller. Die Kosten für die Implementierung und Zertifizierung sind je nach Gerätetyp und Anwendungsfällen möglicherweise nicht praktikabel oder finanziell sinnvoll. In diesem Abschnitt werden einige der wichtigsten Gründe untersucht, warum sich ein Hersteller dafür entscheiden könnte, bestimmte Geräte nicht mit Matter zu zertifizieren.

Der Matter-Standard zielt zwar darauf ab, die Entwicklung zu vereinfachen und eine universelle Kompatibilität zu ermöglichen, bei bestimmten Arten von Smart-Home-Geräten können jedoch praktische Zertifizierungshindernisse bestehen, die die Vorteile überwiegen. Für Produkte mit strengen Einschränkungen, Nicht-IP-Protokollen, begrenzten Zielgruppen oder nicht definierten Gerätetypen in Matter ist die Erlangung einer Matter-Zertifizierung zunächst möglicherweise nicht die beste Strategie. Dies könnten die Gründe sein, warum ein Hersteller die Einführung von Matter vermeiden könnte. Matter ermöglicht es jedoch, dass IP-fähige Gateway-Geräte als Proxy für Nicht-IP-Endpunkte fungieren. Für bestimmte ältere Geräte kann ein Gateway-Ansatz ein praktikabler Weg zur Matter-Kompatibilität sein und gleichzeitig eine vollständige Neugestaltung der Geräte vermeiden.

Im Jahr 2026, mit Matter in der Version 1.5 und Tausenden von zertifizierten Geräten auf dem Markt, ist das Ökosystem erheblich ausgereift. Die Hindernisse für die Zertifizierung wurden durch eine verbesserte SDKs, bessere Dokumentation und eine erweiterte Testinfrastruktur verringert. Die im Folgenden dargelegten Überlegungen bleiben jedoch für Hersteller relevant, die ihre Zertifizierungsstrategie bewerten.

Da sich der Matter-Standard weiterentwickelt und sein Anwendungsbereich auf immer mehr Anwendungsfälle ausgedehnt wird, könnten sich die Argumente für eine Zertifizierung im Laufe der Zeit verschärfen, selbst für diese Produktkategorien. Gerätehersteller müssen ihre spezifischen Situationen und Pläne bewerten, um den besten Ansatz für die Einhaltung von Matter zu finden. In vielen Situationen kann es triftige technische oder geschäftliche Gründe geben, die dafür sprechen, die Zertifizierung zumindest vorübergehend abzulehnen.

Verbindungsprotokolle, die keine IP-Verbindungen sind

Um den Matter-Standard zu übernehmen, müssen Geräte in IP-Netzwerken wie Wi-Fi, Ethernet und Thread betrieben werden. Nicht-IP-Funkprotokolle wie Zigbee, Z-Wave und Bluetooth LE werden häufig in Geräten mit geringer Bandbreite verwendet. Für diese Protokolle ist ein zusätzlicher

Protokollübersetzer erforderlich, der nicht von IP zu IP basiert, um mit Matter kompatibel zu sein. Ein Upgrade des Kommunikationsmoduls oder die Einführung eines Translation Gateways erhöhen in der Regel die Hardwarekosten des Geräts.

Das Hinzufügen von IP-Stack-Unterstützung bedeutet, dass mehr Speicher und Rechenleistung für die Netzwerkverwaltung bereitgestellt werden müssen. Dies könnte die Möglichkeiten extrem kostengünstiger Geräte mit geringem Stromverbrauch übersteigen. Das Hinzufügen von zusätzlichem Speicher oder Flash zur Unterstützung von IP würde auch die Herstellungskosten erhöhen und die Akkulaufzeit verkürzen. Für Anwendungsfälle, in denen lediglich Strom ein- und ausgeschaltet oder Sensordaten benötigt werden, können Nicht-IP-Protokolle eine effiziente Lösung sein.

Matter schließt grundsätzlich die Zertifizierung von Geräten aus, die auf proprietären, nicht IP-basierten Funkstandards basieren. Dies könnte Hersteller einschränken, die alternative Verbindungsmethoden für ihre Low-End-Produkte verwenden möchten. IP-basierte Protokolle wie Wi-Fi und Ethernet sind zwar notwendig, um verschiedene Ökosysteme miteinander zu verbinden, aber IP-fremde Standards haben in einigen Anwendungen immer noch Vorteile für die grundlegende Konnektivität von Sensoren und Schaltern.

Matter Bridges sind immer gebräuchlicher und standardisierter geworden, sodass Hersteller ihre bestehenden Nicht-IP-Gerätelinien beibehalten und gleichzeitig die Kompatibilität mit Matter durch zertifizierte Bridge-Produkte verbessern können. Dieser Ansatz hat sich für Zigbee- und Z-Wave-Geräteökosysteme als erfolgreich erwiesen, bei denen eine einzige Bridge mehrere ältere Geräte als Matter-Endpunkte einsetzen kann.

Hardwarebeschränkungen

Eine weitere Herausforderung besteht darin, dass Matter ein Mindestmaß an Rechenleistung und Speicher auf dem Gerät benötigt, um den erforderlichen Software-Stack zu unterstützen. Die grundlegendsten Smart-Home-Geräte verfügen jedoch aufgrund von Kosten- und Größenbeschränkungen häufig nur über sehr begrenzte integrierte Chipkapazitäten.

Beispielsweise kann ein einfacher Tür- oder Fenstersensor nur einen Mikrocontroller mit weniger als 100 KB Flash-Speicher und 10 KB RAM enthalten. Dies bietet nicht genügend Speicher- und Verarbeitungskapazität für eine vollständige Matter-Implementierung. Das Hinzufügen von leistungsfähigerem und teurerem Silizium würde die Materialkosten erheblich in die Höhe treiben.

In Fällen, in denen Kosten und Größe oberste Priorität haben, könnten Hersteller feststellen, dass die Anforderungen von Matter nicht mit ihren Hardware-Budgets übereinstimmen. Die Zertifizierung sehr

einfacher Sensoren, Switches oder Controller mit Matter könnte zu unnötigen Hardware-Upgrades führen, die sich negativ auf die Erschwinglichkeit auswirken.

Mit Matter 1.4.2 (Juni 2025) wurden Verbesserungen der Transportzuverlässigkeit und der Inbetriebnahme von Bluetooth Low Energy (BLE) eingeführt, wodurch die Ressourcennutzung optimiert wurde. Der Reifegrad des SDK und die Verfügbarkeit von Referenzimplementierungen haben auch den Aufwand für die Integration von Matter reduziert. Für extrem eingeschränkte Geräte (weniger als 100 KB Flash) ist der Gateway-Proxy-Ansatz jedoch nach wie vor die praktischste Lösung.

Ökosysteme der Kunden

Ein weiterer zu berücksichtigender Faktor ist, ob der Zielkundenstamm eines Herstellers Smart-Home-Plattformen verwendet, die mit Matter kompatibel sind. Wenn die meisten Verbraucher in diesem Segment keine Matter-Controller oder Matter-fähige Hubs und Apps verwenden, besteht möglicherweise kaum ein Anreiz, Produkte zu zertifizieren.

Beispielsweise könnte ein Unternehmen, das sich auf die Bedürfnisse älterer Benutzer konzentriert, feststellen, dass seine Kunden ohne Matter-Administratoren über einfache Setups verfügen. Oder do-it-yourself (Heimwerker-) Enthusiasten bevorzugen möglicherweise maßgeschneiderte Lösungen und benötigen nicht die markenübergreifende plug-and-play Erfahrung von Matter.

In Szenarien, in denen sich die Zielgruppe nicht mit der Matter-Infrastruktur auseinandersetzt, erhöht die Zertifizierung die Komplexität, ohne dass klare Vorteile bestehen. Ressourcen sollten besser für die Optimierung der Benutzererfahrung auf den entsprechenden Plattformen eingesetzt werden, anstatt sich auf die Einhaltung von Matter-Vorschriften zu konzentrieren.

Im Jahr 2026 hat die Einführung von Matter eine kritische Masse erreicht, da große Ökosysteme (Amazon Alexa, Google Home, Apple HomeKit, Samsung SmartThings) den Standard vollständig unterstützen. Das Bewusstsein der Verbraucher für Matter hat erheblich zugenommen, und das Matter-Logo wurde zu einem anerkannten Zeichen für Interoperabilität. Die demografische Zielfrage hat sich von der Frage „Nutzen Kunden Matter“ verlagert zu „Können wir es uns leisten, Matter nicht zu unterstützen?“ da dies in vielen Marktsegmenten zu einer grundlegenden Erwartung wird.

Gerätetypen sind noch nicht definiert

Der Anwendungsbereich von Matter hat sich seit der ersten Version dramatisch erweitert und deckt die gängigsten Smart-Home-Kategorien und viele Geräte ab, aber einige Nischenbranchen warten noch auf eine Standardisierung.

Wenn ein Unternehmen einzigartige Gerätetypen entwickelt, die nicht durch bestehende Matter-Profile abgedeckt werden, ist eine Zertifizierung erst möglich, wenn neue Profile erstellt wurden. Dies könnte die Markteinführung eines neuen Produkts verzögern, während darauf gewartet wird, dass Matter seinen Anwendungsbereich erweitert.

Anstatt mit der Veröffentlichung von Innovationen zu warten, könnten einige Hersteller es vorziehen, Nischenlösungen früher mit eigenen Mitteln auf den Markt zu bringen. Eine spätere Zertifizierung ist nach wie vor möglich, wenn die entsprechenden Profile ausgereift sind. Aus Gründen der Vorreiterrolle könnte es in einigen Fällen vorzuziehen sein, auf Matter zu direct-to-consumer verzichten.

Eine Alternative: Proxying an Gateways

In Situationen, in denen ein Endgerät Einschränkungen aufweist, die eine direkte Matter-Zertifizierung verhindern, besteht ein alternativer Ansatz darin, die Matter-Funktion des Geräts an einem Gateway als Proxy zu verwenden. Das Gateway dient als Brücke, die zwischen dem lokalen Funkprotokoll des Endpunkts und dem IP-basierten Matter-Protokoll übersetzt.

Beispielsweise könnte ein einfacher Temperatursensor, der über einen proprietären Funkstandard kommuniziert, dem Matter-Administrator immer noch als Matter-Gerät angezeigt werden. Das Gateway empfängt Sensordaten über eine Nicht-IP-Schnittstelle, stellt aber Controllern virtuelle Matter-Entitäten zur Verfügung, die diese Daten über IP repräsentieren. Auf diese Weise können Sie vorhandene Hardware verwenden und über das Gateway einige Interoperabilitätsvorteile erzielen.

Dies erhöht natürlich die Komplexität für Entwickler und erfordert Gateways, die die erforderliche Übersetzungsschicht unterstützen. In Fällen, in denen die direkte Zertifizierung für das Gerät selbst zu schwierig ist, könnte dies jedoch ein praktikabler Kompromiss sein. Proxys könnten dazu beitragen, dass Lösungen mit geringem Stromverbrauch oder Nischenlösungen an Matter-Ökosystemen teilhaben können, ohne dass die Hardware komplett überarbeitet werden muss.

Die Matter Bridge-Spezifikation ist ausgereift, und zahlreiche zertifizierte Bridge-Produkte sind inzwischen von großen Herstellern erhältlich. Dies hat den Gateway-Ansatz im Vergleich zu den Anfängen von Matter praktikabler und standardisierter gemacht. Hersteller können jetzt mit Bridge-Anbietern zusammenarbeiten oder ihre eigenen zertifizierten Bridges entwickeln, um Nicht-IP-Geräte in das Matter-Ökosystem aufzunehmen, ohne die Endpunkt-Hardware neu gestalten zu müssen.

Cloud-Konnektivität mit Matter

Matter ermöglicht zwar die grundlegende Interoperabilität lokaler Geräte, aber zusätzliche Cloud-Konnektivität ist erforderlich, um robuste over-the-air Updates, Telemetriedaten, Fernverwaltung und Integration mit proprietären Herstellerdiensten bereitzustellen. Geräteherstellern stehen Optionen wie der Versand eines Matter Gateway-Hubs, die Nutzung des von Matter zertifizierten Hubs eines Haushalts oder die Integration direkter Cloud-Konnektivität in Endgeräte zur Verfügung. Standards für Matter-to-cloud Konnektivität sind im Entstehen begriffen, aber die Hersteller müssen noch zusätzliche Konnektivitäts-Softwarepacks in Matter-Geräte integrieren. Um das volle Potenzial von Smart-Home-Geräten in Bereichen wie Diagnosen und Updates neuer Funktionen auszuschöpfen, müssen die Hersteller von Matter die Cloud-Integration in Betracht ziehen, die über den grundlegenden lokalen Betrieb hinausgeht.

Bereitstellung erweiterter Gerätefunktionen mit Cloud-Konnektivität für Matter-Endgeräte

Der Matter-Standard verspricht, IoT-Geräte verschiedener Anbieter über ein gemeinsames Protokoll zu vereinheitlichen. Er legt fest, wie Smart-Home-Geräte mithilfe von IP-basierten Netzwerktechnologien wie Ethernet, Wi-Fi und Thread einander im lokalen Netzwerk erkennen, kommunizieren und miteinander interagieren. Diese lokale Interoperabilität ermöglicht es Matter-zertifizierten Geräten verschiedener Anbieter, bei Aktivitäten wie automatisierten Szenen und Sprachsteuerung nahtlos zusammenzuarbeiten. Matter definiert jedoch keine Cloud-Schnittstellen und erfordert auch keine Internetverbindung für die Geräteendpunkte.

Viele intelligente Geräte verlassen sich heute auf zusätzliche Cloud-Konnektivität für wichtige Funktionen wie over-the-air (OTA-) Updates, Fernzugriff und Integrationen mit Herstellerplattformen. Gerätehersteller, die Matter-konforme Produkte entwickeln und gleichzeitig erweiterte Funktionen beibehalten möchten, stehen vor einigen Designüberlegungen, wenn es darum geht, Matter durch Cloud-Konnektivität zu ergänzen. Die grundlegende lokale Steuerung und die Integration des Sprachassistenten funktionieren zwar für einfache Matter-Geräte, jedoch ist zusätzliche Cloud-Konnektivität erforderlich, um erweiterte Funktionen zu ermöglichen.

Anwendungsfälle, die Cloud-Konnektivität erfordern

Matter kümmert sich zwar um die Interoperabilität lokaler Geräte, zusätzliche Cloud-Konnektivität ermöglicht jedoch mehrere wichtige Funktionen für Smart-Home-Geräte:

- Over-the-air (OTA) -Updates — Die Bereitstellung von Firmware- und Softwareupdates über das Internet ermöglicht es Anbietern, bereits installierte Geräte auf einfache Weise zu erweitern. Ohne OTA würden Updates manuell abgewickelt. Der Matter-Standard beschreibt zwar, wie die OTA-Updates verarbeitet und an Matter-zertifizierte Endpunkte geliefert werden, dies hängt jedoch von der Funktionalität ab, die vom Matter-Hub unterstützt wird, mit dem der Endpunkt verbunden ist. Darüber hinaus gibt es Einschränkungen in Bezug darauf, welche Updates für den Endpunkt bereitgestellt werden. Wenn der Endpunkt beispielsweise ein Update anfordert, wird nur das neueste verfügbare Update bereitgestellt. Alle Geräte desselben Typs erhalten dieses einzige Update. Es gibt keine Möglichkeit, ein sequentielles Update oder sogar ein OTA-Rollback oder Löschen eines Updates durchzuführen. Durch die Aktivierung der Cloud-Konnektivität auf dem Endpunkt kann dieser Mangel an detaillierter Verwaltung von OTA-Updates behoben werden. Matter Version 1.4.2 (Juni 2025) führte zu Verbesserungen der Transportzuverlässigkeit und der Testinfrastruktur sowie zu verbesserten OTA-Aktualisierungsmechanismen. Die grundlegenden Einschränkungen in Bezug auf sequentielle Updates und Rollback-Funktionen bleiben jedoch bestehen, sodass direkte Cloud-Konnektivität für Hersteller, die detaillierte Funktionen zur Steuerung von Updates und Flottenmanagement benötigen, wertvoll ist.
- Kamerastreaming und Medien — Matter Version 1.5 (November 2025) führte Kameraunterstützung mithilfe von Seitenkanalprotokollen wie dem Real-Time Streaming Protocol (RTSP) über WLAN oder Ethernet ein. Matter kümmert sich zwar um die Geräteerkennung und die grundlegende Steuerung, das eigentliche Videostreaming erfolgt jedoch über separate Protokolle. Dies erfordert häufig eine Cloud-Infrastruktur für Fernanzeige, Aufzeichnung und KI-basierte Funktionen wie Personenerkennung.
- Fernzugriff und Fernsteuerung — Für den Fernzugriff auf und die Fernsteuerung von Geräten von außerhalb des Heimnetzwerks ist ein Cloud-Endpunkt erforderlich. Materie unterstützt, wie derzeit definiert, nur lokalen Zugriff. Ein Matter-Endpunkt kann zwar mit einer Benutzer-App im lokalen Netzwerk gesteuert werden, die Fernsteuerung ist jedoch nur verfügbar, wenn sie vom Matter-Hub unterstützt wird. Selbst dann sind in der Regel nur grundlegende Fernbedienungen verfügbar.
- Telemetrie und Diagnose — Durch die Aggregation von Felddaten wie Fehlerprotokollen und Sensorströmen in der Cloud können Anbieter den Gerätezustand überwachen und Probleme identifizieren. Matter unterstützt zwar Funk- und protokollbezogene Diagnosen über den allgemeinen Diagnosecluster, aber für jede detaillierte, gerätespezifische Diagnose ist eine Cloud-Konnektivität erforderlich, damit der Hersteller Daten vom Gerät abrufen kann.
- Herstellerspezifische Integrationen — Alle benutzerdefinierten Funktionen und Datentypen, die nicht in der Matter-Spezifikation definiert sind, erfordern Konnektivität zu Cloud-Plattformen von Anbietern. Dies ist besonders wichtig für Geräte mit erweiterten Funktionen wie Kameras (Matter-Version 1.5), Energiemanagement-Geräte (Matter-Version 1.4) und Appliances (Matter-

Versionen 1.2-1.3), für deren volle Funktionalität möglicherweise herstellerspezifische Cloud-Dienste erforderlich sind.

- Externe Integrationen — Für die Verknüpfung mit Diensten von Drittanbietern wie Sprachassistenten, die sich nicht im Matter-Ökosystem befinden, oder Zahlungsgateways von Drittanbietern (je nach Anwendungsfall erforderlich) ist eine Internetverbindung erforderlich, die über den Matter-Administrator hinausgeht.

Da diese wichtigen Funktionen auf Cloud-Konnektivität angewiesen sind, benötigen Matter-Endgeräte häufig zusätzliche Optionen für den Internetzugang.

Architekturen zur Aktivierung von Cloud-Konnektivität

Für Matter-Geräte gibt es drei allgemeine Ansätze, um die erforderliche Cloud-Konnektivität bereitzustellen und gleichzeitig die lokalen Betriebsspezifikationen zu erfüllen.

Smart-Home-Hub mit integriertem Gateway

Einige Gerätehersteller entscheiden sich möglicherweise dafür, einen proprietären Home-Hub zu liefern, der sowohl den Matter-Administrator als auch ein Gateway zu ihren Cloud-Diensten enthält. Dieser Home-Hub würde die angeschlossenen Matter-Endpunkte standardmäßig lokal verwalten und gleichzeitig Cloud-Verbindungen für erweiterte Funktionen ermöglichen. Der Hub könnte OTA-Updates, Fernzugriff und Telemetrieerfassung für Endgeräte unterstützen.

Verlagern Sie die Cloud-Konnektivität auf einen vorhandenen Matter-Hub

Anstatt einen benutzerdefinierten Hub zu bündeln, könnten Geräte so konzipiert werden, dass sie für die Internetverbindung eine Verbindung mit Matter-Hubs wie Amazon Echo, Google Nest Hub HomePod, Apple oder Samsung SmartThings Hub herstellen. In diesem Fall wickelt der bestehende Matter Hub die lokale Gerätekommunikation gemäß dem Standard ab und bietet auch ein Gateway zur Cloud für Endgeräte, die dies benötigen. Dabei wird die Infrastruktur genutzt, über die Verbraucher möglicherweise bereits verfügen. Dieser Ansatz hängt jedoch vom Umfang der Unterstützung ab, die der Matter Hub für Funktionen bietet, die im Standard nicht als normativ für Matter Hubs spezifiziert sind.

Direkte Cloud-Konnektivität an Endpunkten

Geräte mit direkter Internetverbindung, wie z. B. WLAN, könnten separate Konnektivität für das lokale Netzwerk von Matter und für Cloud-Dienste von Anbietern integrieren. Dadurch kann das Gerät als

eigenes Gateway zur Cloud fungieren. Für non-Wi-Fi Endgeräte, die auf Protokollen wie Thread basieren, sind jedoch Lösungen erforderlich. Dadurch können Geräte unabhängig voneinander eine Verbindung zur Cloud herstellen, was jedoch für einfache, kostengünstige, batteriebetriebene Geräte möglicherweise nicht möglich ist.

Bridging Matter und Hersteller von Cloud-Plattformen

Matter vereinfacht zwar die lokale Interoperabilität, es sind jedoch zusätzliche Anstrengungen erforderlich, um die Verwaltungssysteme von Matter und die Cloud-Plattformen der Hersteller reibungslos zu verbinden. Die Connectivity Standards Alliance (CSA) entwickelt weiterhin Standards für Matter-to-cloud Konnektivität. Stand 2026, während sich die formalen Standards für Cloud-Schnittstellen noch in der Entwicklung befinden, haben sich durch den Einsatz von Tausenden von Matter-Geräten branchenweit bewährte Verfahren herauskristallisiert. Eine breite Einführung von Standards für diese Cloud-Konnektivität würde Geräteherstellern die Entwicklung erleichtern.

Der optimale Weg hängt von den Anwendungsfällen, Preisen und Geschäftsmodellen bestimmter Produkte ab. Es liegt auf der Hand, dass ein robuster Zugang zu Cloud-Diensten erforderlich ist, um die volle Funktionalität zu nutzen, die Smart-Home-Nutzer erwarten — auch für Matter-konforme Geräte, die auf lokale Interoperabilität ausgerichtet sind. Gerätehersteller haben die Möglichkeit, Matter für die Interoperabilität zu nutzen und gleichzeitig die fortschrittlichen Funktionen durch durchdachte Cloud-Konnektivität bereitzustellen.

Sicherheitsüberlegungen für den Matter-Standard

Sicherheit durch Design ist die Praxis, Sicherheitsfunktionen bereits in der Phase des Gerätedesigns zu integrieren und nicht erst im Nachhinein in späteren Entwicklungsphasen. Verschlüsselte Kommunikation und over-the-air (OTA) -Updates sind Beispiele für Sicherheit durch Design. Matter bietet eine solide Grundlage für Smart-Home-Geräte, indem es Sicherheit durch Design implementiert, angefangen bei einer vertrauenswürdigen, sicheren Produktionsstätte. Matter-Geräte können nur von Besitzern einer bekannten, vertrauenswürdigen Zertifizierungsstelle (PAA) - Zertifizierungsstelle (CA) hergestellt und bereitgestellt werden.

Ab Matter Version 1.5 wurde das Sicherheitsframework durch mehrere Versionen kontinuierlich verbessert. Matter 1.4.2 (Juni 2025) führte PSA-basierte Krypto-Verbesserungen ein und erweiterte damit die Sicherheitsgrundlage. Die Connectivity Standards Alliance (CSA), die den Matter-Standard überwacht, unterhält ein spezielles Programm zur Meldung von Sicherheitslücken, um die Sicherheitsinformationen für ihre Protokolle zu verwalten.

Geräteauthentifizierung

Matter-Geräte müssen sich gegenseitig und gegenüber einem Controller authentifizieren, bevor sie kommunizieren können. Nur autorisierte Geräte können eine Verbindung zur Matter Fabric herstellen. Während der Herstellung werden Geräte mit einer eindeutigen Identität und einem X.509-Zertifikat ausgestattet, das als Device Attestation Certificate (DAC) bezeichnet wird. Wenn das Gerät zum ersten Mal versucht, eine Verbindung zur Matter Fabric herzustellen, überprüft das Commissioner-Gerät, ob der DAC gültig ist und ob er von einer bekannten und vertrauenswürdigen PAI (Product Attestation Intermediate) CA signiert ist. Das Commissioner-Gerät überprüft auch, ob das Gerät, das versucht, eine Verbindung zum Netzwerk herzustellen, den Spezifikationen, Protokollen und Sicherheitsstandards von Matter entspricht. Dem Gerät wird nur dann Zugriff auf die Matter-Fabric gewährt, wenn alle Prüfungen erfolgreich sind.

Die CSA führt eine Liste der autorisierten Produktbescheinigungsbehörden (PAAs) und veröffentlicht diese über das Distributed Compliance Ledger (DCL). Das DCL ist ein Blockchain-basiertes System, das transparente, manipulationssichere Aufzeichnungen über zertifizierte Geräte und vertrauenswürdige Zertifizierungsstellen bereitstellt. Hersteller können beantragen, dass sie für die Bereitstellung ihrer PAAs Geräte autorisiert PAAs werden oder mit bestehenden zusammenarbeiten. Das DCL unterstützt auch Observer Nodes, über die Interessengruppen das Zertifizierungsökosystem überwachen können.

Verschlüsselte Kommunikation

Nachdem dem Gerät Zugriff auf die Matter Fabric gewährt wurde, werden alle Daten, die zwischen Geräten übertragen werden, durch eine starke Verschlüsselung gesichert. Die Datenintegrität wird durch einen mehrstufigen Ansatz gewahrt. Der Fachbeauftragte führt den Schlüsselaustausch und die Signaturüberprüfung anhand der ECC-256 secp256r1-Kurve durch. Nach dem Schlüsselaustausch verschlüsseln die Matter-Geräte Daten während der Übertragung mithilfe von AES-256. Für jede Nachricht verwenden die Geräte den SHA-256-Algorithmus, um zu überprüfen, ob die Daten während der Übertragung nicht manipuliert wurden.

Matter Version 1.4 führte erweiterte Multi-Admin-Funktionen mit dem Home Router Access Protocol (HRAP) ein. Dadurch wurde die Sicherheit in Szenarien verbessert, in denen Geräte gleichzeitig von mehreren Ökosystemen gesteuert werden. Diese Verbesserung stellt sicher, dass die gemeinsame Nutzung von Anmeldeinformationen und die Zugriffskontrolle auch dann sicher sind, wenn ein Gerät an mehreren Matter-Fabrics teilnimmt. Jede Struktur behält ihren eigenen Sicherheitskontext bei und verhindert so, dass sich Kompromisse in einem Ökosystem auf andere auswirken.

Over-the-air Aktualisierungen

Der Matter-Standard verlangt außerdem, dass Geräte ein robustes Sicherheitsniveau für over-the-air (OTA) -Updates implementieren. OTA ist ein wichtiger Bestandteil eines Smart-Home-Ökosystems, sodass Geräte Sicherheitsupdates und neue Funktionen erhalten können. Jedes Firmware-Update für Matter-Geräte muss mit dem privaten Schlüssel eines Herstellers signiert sein. Das Gerät verifiziert die Payload-Signatur mithilfe des entsprechenden asymmetrischen öffentlichen Schlüssels. Nachdem die Signatur der Payload verifiziert wurde, kann das Gerät das Image in seinen Bootloader übertragen und zurücksetzen. Während des Startvorgangs muss das Gerät das Image erneut überprüfen, um sicherzustellen, dass es nicht manipuliert wurde. Außerdem muss das Gerät überprüfen, ob auf dem Gerät die neueste bekannte Version ausgeführt wird.

Matter Version 1.4.2 (Juni 2025) führte zu erheblichen Verbesserungen der OTA-Update-Infrastruktur, darunter eine bessere Transportzuverlässigkeit und verbesserte Test-Frameworks. Diese Verbesserungen haben OTA-Updates in Produktionsbereitstellungen robuster und zuverlässiger gemacht. Hersteller sollten jedoch beachten, dass der OTA-Mechanismus von Matter Einschränkungen in Bezug auf sequentielle Updates und Rollback-Funktionen aufweist. Bei Geräten, die eine detaillierte Update-Steuerung, ein Flottenmanagement oder das A/B Testen von Firmware erfordern, müssen Hersteller den OTA von Matter möglicherweise durch direkte Cloud-Konnektivität zu ihrer eigenen Update-Infrastruktur ergänzen.

Entwicklung mit Materie

Alexa verwenden

Amazon bietet eine umfassende Suite von Tools für die Matter-Entwicklung. Diese Tools bieten einen beschleunigten Weg zur Entwicklung von Matter-Produkten, die mit allen wichtigen Ökosystemen kompatibel sind und nahtlos mit Amazon Alexa zusammenarbeiten.

Programm: Funktioniert mit Alexa

Dieses Programm stellt sicher, dass Ihre mit Alexa verbundenen Geräte ein hervorragendes Kundenerlebnis bieten. Das Works with Alexa (WWA) -Logo erhöht das Vertrauen der Kunden und trägt dazu bei, dass Ihre zertifizierten Geräte bevorzugt werden. Weitere Informationen finden Sie unter Ankündigung der Markteinführung von Matter und Einführung von Works with Alexa (WWA) für Matter-Geräte (Amazon-Blogbeitrag).

SDK: Entwickeln Sie Matter mit Alexa

Mit diesem SDK können Sie Ihrem Gerät lokale Matter-Konnektivität hinzufügen und gleichzeitig verwaltete Cloud-Konnektivität, Business Intelligence und OTA-Unterstützung nutzen. Weitere Informationen finden Sie unter Mit Alexa das Beste aus Matter herausholen.

Kit: Alexa Ambient Home Developer Kit

Dieses Kit hilft Ihnen bei der protokollübergreifenden Integration von Geräten, um mit Alexa ein intelligentes und einheitliches Zuhause zu schaffen. Weitere Informationen finden Sie unter Amazon Alexa.

Endpunkt: In Betrieb zu nehmender Endpunkt

Für Matter-Geräte, die mit Skills verbunden sind, stellt die Commissionable Endpoint API eine lokale, Matter-basierte Verbindung zu Alexa-Geräten her, ohne dass Ihr Kunde mit dessen Zustimmung Schritte ausführen muss. Weitere Informationen finden Sie unter Alexa.Commissionable Interface 1.0 (Alexa Skills Kit).

AWS Private CA Unterstützung für Matter

AWS Private Certificate Authority (AWS Private CA) bietet Anleitungen zur Verwendung des Matter-Standards.

DAC für Materie

Matter benötigt ein Device Attestation Certificate (DAC), das von einer Device Attestation CA ausgestellt werden muss, die der Matter Public Key Infrastructure (PKI) -Zertifikatsrichtlinie (CP) entspricht. Gerätehersteller können damit AWS Private CA Folgendes tun:

- Hosten Sie die Product Attestation Authority (PAA), die Zertifizierungsstelle (CA)
- Hosten Sie die PAI (Product Attestation Intermediate) CA
- Stellen Sie den DAC jedes Geräts aus, signieren Sie ihn und warten Sie ihn

Weitere Informationen finden Sie unter Verwendung AWS Private Certificate Authority zur Ausstellung von Gerätebestätigungszertifikaten für Matter im AWS Sicherheitsblog.

Betriebszertifikate für Knoten (NOC)

AWS Private CA Unterstützt zusätzlich zur Gerätebescheinigung die Ausstellung von Node Operational Certificates (NOCs), die zur Sicherung der Kommunikation innerhalb einer Matter-Fabric verwendet werden. AWS bietet Java-Beispiele für die Aktivierung einer Stammzertifizierungsstelle und einer untergeordneten Zertifizierungsstelle NOCs sowie für die Erstellung eines NOC.

Weitere Informationen finden Sie in der Dokumentation unter Verwenden der AWS Private CA API zur Implementierung von Matter-Zertifikaten. AWS Private Certificate Authority

CRL Revocation Support (Matter Version 1.2 und höher)

In Matter Version 1.2 wurde der Widerruf von Device Attestation Certificate (DAC) mithilfe von Zertifikatssperrlisten () eingeführt. CRLs Wenn Sie den CRL-Widerruf für CAs diese Ausgabe aktivieren, legen Sie bei Zertifikaten `true` im `CrlConfiguration` Objekt innerhalb der Struktur den Wert `OmitExtension` auf fest. `CrlDistributionPointExtensionConfiguration` In Matter ist der CRL Distribution Point (CDP) -URI nicht in Zertifikate eingebettet, sondern wird stattdessen aus dem Matter Distributed Compliance Ledger (DCL) abgerufen. Sie müssen den CDP-URI zur Erkennung bei der DAC-Validierung in die Matter DCL hochladen.

Infrastruktur für Materie

AWS bietet ein Beispiel, das die Verwendung von AWS Cloud Development Kit (AWS CDK)zum Einrichten der PKI-Infrastruktur für Matter demonstriert. Sie verwenden AWS Private CA , um die Anforderungen des Matter PKI CP zu erfüllen. Weitere Informationen finden Sie im Matter PKI CDK-Projekt unter. GitHub

Java-Beispiele

AWS Private CA enthält Java-Beispiele für die Erstellung von Matter-konformen PAA-Zertifikaten (Product Attestation Authority), PAI-Zertifikaten (Product Attestation Intermediate) und Device Attestation Certificates (). DACs Weitere Informationen finden Sie in der Dokumentation unter Verwenden der AWS Private CA API zur Implementierung des Matter-Standards (Java-Beispiele). AWS Private Certificate Authority

Leitfaden zur Einhaltung der Matter-PKI

In diesem Matter PKI Compliance Guide wird erklärt, wie die CSA Matter PKI CP-Anforderungen implementiert und deren Einhaltung nachgewiesen werden kann. Er enthält Informationen darüber, wie Sie Matter-konforme AWS Private CA Zertifizierungsstellen einrichten und betreiben können (). CAs

Verwaltete Integrationen mit AWS IoT Device Management

AWS IoT Device Managementbeinhaltet die Funktion für verwaltete Integrationen, die eine einheitliche Oberfläche für das Onboarding und die Verwaltung verschiedener IoT-Geräte bietet, unabhängig vom Verbindungstyp (direkt, hub-basiert oder). cloud-to-cloud

Im Folgenden sind die wichtigsten Funktionen aufgeführt, die für Matter relevant sind:

- SDKs Geräteunterstützung ZigBee, Z-Wave-, Matter- und Wi-Fi-Protokolle
- Mehr als 80 Vorlagen für Gerätedatenmodelle, die auf der AWS Implementierung des Matter-Datenmodellstandards basieren
- Von Partnern entwickelte cloud-to-cloud (C2C) Steckverbinder
- Einheitliche Gerätesteuerung für mehrere Marken und Protokolle
- Verfügbar in den Regionen Kanada (Zentral), Europa (Irland) und Naher Osten (VAE)

Weitere Informationen finden Sie unter Wozu dienen verwaltete Integrationen? AWS IoT Device Management

FAQs über den Matter-Standard

Was sind die Mitgliedschaftsstufen bei Matter?

Die Informationen zur Mitgliedschaft finden Sie auf der CSA-Website. Welche Mitgliedschaftsstufe Sie wählen, hängt davon ab, ob Sie daran interessiert sind, ein Produkt zu zertifizieren (Anwender) oder den Produkttyp innerhalb des Standards zu definieren (Teilnehmer). Weitere Informationen zu den Mitgliedschaftsstufen finden Sie unter Impact the Future of the IoT auf der CSA-Website.

Wie profitieren Smart-Home-Verbraucher von Matter?

Verbraucher profitieren auf folgende Weise von Matter:

- Vereinfachtes Onboarding von Matter-Geräten zu Hause, einschließlich verbessertem Einrichtungsablauf, QR-Codes für mehrere Geräte und NFC-Onboarding (Matter-Version 1.4.1)
- Einheitliche Verwaltung aller Smart-Home-Geräte über eine einzige App in allen wichtigen Ökosystemen (Amazon Alexa, Google Home, Apple HomeKit, Samsung) SmartThings
- Gerätesteuerung von mehreren Sprachassistenten gleichzeitig über Enhanced Multi-Admin (Matter Version 1.4)
- Zugriff auf erweiterte Gerätetypen, darunter Kameras mit Streaming, Geräte, Energiemanagementgeräte und Saugroboter

Weitere Informationen finden Sie in diesem Leitfaden unter Die Benefits of Matter-Zertifizierung für Smart-Home-Verbraucher.

Wie profitieren Gerätehersteller von Matter?

Gerätehersteller profitieren auf folgende Weise von Matter:

- Geringere Kosten für die Unterstützung von Kunden mit Infrastruktur- und Konnektivitätsproblemen
- Eine einzige Zertifizierung für ein Gerät statt mehrerer Zertifizierungen für jedes Ökosystem
- Die Entwicklung proprietärer Apps ist für die grundlegende Gerätefunktionalität nicht mehr erforderlich
- Geringere Materialkosten, da keine Infrastrukturelemente (wie Thread-Border-Router) versendet werden müssen

- Geringere Kosten für die Unterstützung von Kunden mit Infrastruktur- und Konnektivitätsproblemen
- Zugang zu ausgereiften SDKs Entwicklungstools und Testinfrastrukturen (deutlich verbessert seit der ersten Version)
- Schneller time-to-market dank etablierter Zertifizierungsprozesse und erweiterter Netzwerke von Testanbietern

Weitere Informationen finden Sie in diesem Handbuch unter Vorteile der Matter-Zertifizierung für Gerätehersteller.

Ersetzt Matter Wi-Fi, Bluetooth oder Thread?

Nein, Matter ist ein Protokoll auf Anwendungsebene, das in IP-Netzwerken ausgeführt wird. Geräte, die Wi-Fi, Ethernet oder Thread für die Konnektivität verwenden, können Matter-zertifiziert werden. In der folgenden Tabelle wird zusammengefasst, wie sich Matter von Wi-Fi, Bluetooth und Thread abhebt.

Feature	Materie	WLAN	Bluetooth	Thread
Zweck	Smart-Home-Kommunikation	Internetzugang und Datenübertragung	Drahtlose Kommunikation mit kurzer Reichweite	Drahtloses Mesh-Netzwerk mit geringem Stromverbrauch
Bereich	Variiert je nach zugrundeliegendem Protokoll	Bis zu 300 Fuß	Bis zu 30 Fuß	Bis zu 300 Fuß
Bandbreite	Variiert je nach zugrundeliegendem Protokoll	Bis zu 10 Gigabit pro Sekunde	Bis zu 2 Megabit pro Sekunde	Bis zu 250 Kilobit pro Sekunde
Stromverbrauch	Variiert je nach zugrundeliegendem Protokoll	Relativ hoch	Relativ niedrig	Sehr niedrig

Sicherheit	Variiert je nach dem zugrunde liegenden Protokoll	WPA2, WPA3	Sichere AES- und BLE-Verbindungen	AES
Cost (Kosten)	Variiert je nach Gerät	Relativ preiswert	Relativ preiswert	Relativ teuer

Was ist eine Lieferanten-ID und eine Produkt-ID?

CSA-Mitglieder können eine Lieferanten-ID beantragen, mit der sie als Lieferant identifiziert werden. Produkte des Unternehmens werden fortan dieser ID zugewiesen und können bis zu ihrer Herkunft zurückverfolgt werden. Darüber hinaus erhalten sie eine eindeutige Produkt-ID. Der 16-stellige numerische Code begleitet Produkte wie eine Passnummer und macht sie so unverwechselbar wie der Verkäufer.

Welche Geräte müssen Matter-zertifiziert sein?

Alle Geräte, die sich authentifizieren und Teil der Matter-Fabric sein müssen, müssen Matter-zertifiziert sein. Geräte, die so konzipiert sind, dass sie nur über ein nicht standardmäßiges (proprietäres) Protokoll mit dem vom Hersteller angegebenen Hub interagieren, würden jedoch nicht vom Matter-Zertifizierungsprozess profitieren. Beispielsweise muss ein Hub für ein Smart-Home-Sicherheitssystem als Matter-konform zertifiziert sein, aber ein Tür- oder Fenstersensor, der mit dem Hub kommuniziert, muss nicht als Matter-konform zertifiziert sein. Die Entscheidung, ein Produkt für Matter zertifizieren zu lassen, hängt in erster Linie von dieser Überlegung ab.

Mein Produkttyp ist derzeit nicht in Matter definiert. Für welche zusätzlichen Aufgaben sollte ich Zeit einplanen, um die Matter-Produkte zertifizieren zu lassen?

Matter hat die Abdeckung der Gerätetypen in den Versionen 1.0 bis 1.5 erheblich erweitert. Der Standard unterstützt jetzt über 50 Gerätetypen, darunter:

- Kerngeräte: Beleuchtung, Schalter, Stecker, Türschlösser, Thermostate, Fensterverkleidungen, Sensoren

- Geräte: Kühlschränke, Klimaanlagen, Geschirrspüler, Saugroboter, Mikrowellen, Backöfen
- Energiemanagement: Sonnenkollektoren, Batterien, Wärmepumpen, Warmwasserbereiter, Ladegeräte für Elektrofahrzeuge
- Umwelt: Wassermanagementgeräte, Luftqualitätssensoren, Luftreiniger
- Sicherheit: Kameras mit Streaming-Unterstützung

Wenn Ihr Gerätetyp immer noch nicht unterstützt wird, besteht der erste Schritt darin, der CSA als Teilnehmer beizutreten. Matter veröffentlicht etwa zweimal pro Jahr neue Versionen und erweitert damit kontinuierlich die Abdeckung der Gerätetypen. Als teilnehmendes Mitglied können Sie die Definition neuer Gerätetypen leiten und haben Zugriff auf Entwürfe von Spezifikationen, die eine schnellere go-to-market Strategie ermöglichen. Weitere Informationen zu den Mitgliedschaftsstufen finden Sie unter Impact the Future of the IoT auf der CSA-Website.

Einige meiner Geräte stellen eine direkte Verbindung zum Wi-Fi-Heimnetzwerk her. Müssen diese Geräte Matter-zertifiziert sein?

Die Matter-Zertifizierung kann Geräten zugute kommen, die sich direkt mit dem Smart-Home-Netzwerk verbinden, da sie eine Verbindung zur Matter-Fabric herstellen können. Auf diese Weise können Verbraucher die Geräte über ihre virtuellen Assistenten auf derselben Matter-Fabric steuern. Verbraucher müssen jedoch eine gerätespezifische App für alle Vorgänge verwenden, die anbieterspezifisch und nicht in der Matter-Spezifikation definiert sind.

Was ist die aktuelle Version von Matter und was ist neu?

Stand November 2025 ist Matter 1.5 die aktuelle Version. Zu den wichtigsten Neuerungen der letzten Versionen gehören:

- Angelegenheit 1.5 (November 2025): Unterstützung für Kamera-Streaming über RTSP, Stabilitätsverbesserungen
- Angelegenheit 1.4.2 (Juni 2025): Verbesserte BLE-Inbetriebnahme, PSA-basierte Verschlüsselung, Transportzuverlässigkeit
- Angelegenheit 1.4.1 (November 2024): Verbesserter Einrichtungsablauf, QR-Codes für mehrere Geräte, NFC-Onboarding
- Angelegenheit 1.4 (November 2024): Geräte für das Energiemanagement, erweitertes Multi-Admin, HRAP

- Angelegenheit 1.3 (Mai 2024): Geräte, Ladegeräte für Elektrofahrzeuge, verbesserte Energieberichterstattung
- Angelegenheit 1.2 (Oktober 2023): Kühlschränke, Klimaanlagen, Geschirrspüler, Saugroboter

Matter-Versionen werden ungefähr zweimal pro Jahr von der CSA-Arbeitsgruppe veröffentlicht.

Ressourcen

AWS Ressourcen

- Holen Sie mit Alexa das Beste aus Matter heraus
- Ankündigung der Markteinführung von Matter und Einführung von Works with Alexa (WWA) für Matter-Geräte (Amazon Alexa-Blog)

Connectivity Standards Alliance (CSA) für das Internet der IoT

- CSA-Webseite
- Überblick über den CSA-Zertifizierungsprozess
- Von der CSA autorisierte Testanbieter
- Spezifikationen der Materie

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
Aktualisierungen der Matter-Standardversion	Aktualisiert und enthält nun Informationen zum neuesten Matter-Standard, Version 1.5	6. März 2026
Erste Veröffentlichung	—	5. Februar 2024

AWS Glossar zu präskriptiven Leitlinien

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

Zahlen

7 Rs

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

- Refactor/re-architect — Verschieben Sie eine Anwendung und ändern Sie ihre Architektur, indem Sie alle Vorteile der Cloud-nativen Funktionen 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-Compatible Edition.
- Plattformwechsel (Lift and Reshape) – Verschieben Sie eine Anwendung in die Cloud und führen Sie ein gewisses Maß an Optimierung ein, um die Cloud-Funktionen zu nutzen. Beispiel: Migrieren Sie Ihre lokale Oracle-Datenbank zu Amazon Relational Database Service (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 Kundenbeziehungsmanagement (CRM) -System 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

A2A () Agent-to-Agent

Ein Stateful-Protokoll für die Zusammenarbeit zwischen Agenten, das die Delegierung von Aufgaben und die Zustandsübertragung unterstützt.

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.

Agent

Ein KI-System, das mithilfe von Tools selbständig Überlegungen anstellen, planen und Maßnahmen ergreifen kann, um Ziele zu erreichen.

Agent Ops

Operative Verfahren zum Erstellen, Testen, Bereitstellen und Ausführen von KI-Agenten in der Produktion im großen Maßstab.

Aggregatfunktion

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

AI

Siehe künstliche Intelligenz.

AIOps

Siehe Operationen mit künstlicher Intelligenz.

Anonymisierung

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

Anti-Muster

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

Anwendungssteuerung

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

Anwendungsportfolio

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

künstliche Intelligenz (KI)

Das Gebiet der Datenverarbeitungswissenschaft, das sich der Nutzung von Computertechnologien zur Ausführung kognitiver Funktionen widmet, die typischerweise mit

Menschen in Verbindung gebracht werden, wie Lernen, Problemlösen und Erkennen von Mustern. Weitere Informationen finden Sie unter Was ist künstliche Intelligenz?

Operationen mit künstlicher Intelligenz (AIOps)

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

Asymmetrische Verschlüsselung

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

Atomizität, Konsistenz, Isolierung, Haltbarkeit (ACID)

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

Attributbasierte Zugriffskontrolle (ABAC)

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

autoritative Datenquelle

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

Availability Zone

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

AWS Framework für die Einführung der Cloud (AWS CAF)

Ein Framework mit Richtlinien und bewährten Verfahren, das Unternehmen bei der Entwicklung eines effizienten und effektiven Plans für den erfolgreichen Umstieg auf die Cloud unterstützt.

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

AWS Workload-Qualifizierungsrahmen (AWS WQF)

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

B

schlechter Bot

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

BCP

Siehe Planung der Geschäftskontinuität.

Verhaltensdiagramm

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

Big-Endian-System

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

Binäre Klassifikation

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

Bloom-Filter

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

blue/green Einsatz

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

Bot

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

Botnetz

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

branch

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

Zugang durch Glasbruch

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

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 AWS Framework 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.

Citizen Developer

Ein Geschäftsanwender, der KI-Anwendungen mithilfe von Plattformen ohne Programmierkenntnisse erstellt. code/low

clientseitige Verschlüsselung

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

Cloud-Kompetenzzentrum (CCoE)

Ein multidisziplinäres Team, das die Cloud-Einführung in der gesamten Organisation vorantreibt, einschließlich der Entwicklung bewährter Cloud-Methoden, der Mobilisierung von Ressourcen, der Festlegung von Migrationszeitplänen und der Begleitung der Organisation durch groß angelegte

Transformationen. Weitere Informationen finden Sie in den CCoE-Beiträgen im AWS Cloud Enterprise Strategy Blog.

Cloud Computing

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

Cloud-Betriebsmodell

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

Phasen der Einführung der Cloud

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

- Projekt – Durchführung einiger Cloud-bezogener Projekte zu Machbarkeitsnachweisen und zu Lernzwecken
- Fundament – Grundlegende Investitionen tätigen, um Ihre Cloud-Einführung zu skalieren (z. B. Einrichtung einer Landing Zone, Definition eines CCoE, Einrichtung eines Betriebsmodells)
- Migration – Migrieren einzelner Anwendungen
- Re-invention — Optimierung von Produkten und Dienstleistungen sowie 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 Repositorys 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 Integration und kontinuierliche Bereitstellung () 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 des AWS Well-Architected Frameworks. Weitere Informationen finden Sie unter Datenklassifizierung.

Datendrift

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

Daten während der Übertragung

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

Datennetz

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

Datenminimierung

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

Datenperimeter

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

Vorverarbeitung der Daten

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

Herkunft der Daten

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

betroffene Person

Eine Person, deren Daten gesammelt und verarbeitet werden.

Data Warehouse

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

Datenbankdefinitionssprache (DDL)

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

Datenbankmanipulationssprache (DML)

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

DDL

Siehe Datenbankdefinitionssprache.

Deep-Ensemble

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

Deep Learning

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

Tiefgreifende Verteidigung

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 umfassender Verteidigungsansatz könnte beispielsweise Multi-Faktor-Authentifizierung, Netzwerksegmentierung und Verschlüsselung kombinieren.

delegierter Administrator

In kann ein kompatibler Dienst ein AWS Mitgliedskonto registrieren AWS Organizations, um die Konten der Organisation zu verwalten 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, z. B. unbeabsichtigte Fehlkonfigurationen oder ein Malware-Angriff.

Disaster Recovery (DR)

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

DML

Siehe Sprache zur Datenbankmanipulation.

Domainorientiertes Design

Ein Ansatz zur Entwicklung eines komplexen Softwaresystems, bei dem seine Komponenten mit sich entwickelnden Domains oder Kerngeschäftszielen verknüpft werden, denen jede

Komponente dient. Dieses Konzept wurde von Eric Evans in seinem Buch Domain-Driven Design: Tackling Complexity in the Heart of Software (Boston: Addison-Wesley Professional, 2003) vorgestellt. Informationen darüber, wie Sie domänengesteuertes Design mit dem Strangler-Fig-Muster verwenden können, finden Sie unter Schrittweise Modernisierung 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 der Wertströme 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 niedrigstwertige 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. Few-shot Eingabeaufforderungen können bei Aufgaben, die spezifische Formatierungs-, Argumentations- oder Fachkenntnisse erfordern, effektiv sein. Siehe auch Zero-Shot-Eingabeaufforderung.

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.

FM-Gateway

Ein zentraler Vermittler, der den Zugriff auf Basismodelle kontrolliert und normalisiert. Wird auch als LLM-Gateway bezeichnet.

G

Generative KI

Eine Untergruppe von KI-Modellen, die mit großen Datenmengen trainiert wurden und mithilfe 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 so 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 dabei hilft, Ressourcen, Richtlinien und die Einhaltung von Vorschriften in allen Organisationseinheiten (OUs) zu regeln. Präventiver Integritätsschutz setzt Richtlinien durch, um die Einhaltung von Standards zu gewährleisten. Sie werden mithilfe von Service-Kontrollrichtlinien und IAM-Berechtigungsgrenzen implementiert. Detektivischer Integritätsschutz erkennt Richtlinienverstöße und Compliance-Probleme und generiert Warnmeldungen zur Abhilfe. Sie werden mithilfe von AWS Config, AWS Security Hub CSPM, Amazon GuardDuty AWS Trusted Advisor, Amazon Inspector und benutzerdefinierten AWS Lambda Prüfungen implementiert.

Leitplanken (KI)

Sicherheitsmechanismen, die Eingaben und Ausgaben von Agenten filtern, validieren und einschränken, um ein verantwortungsbewusstes und sicheres Verhalten der KI zu gewährleisten.

H

HEKTAR

Siehe Hochverfügbarkeit.

Heterogene Datenbankmigration

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

hohe Verfügbarkeit (HA)

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

historische Modernisierung

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

Holdout-Daten

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

Der Mensch im Kreis (HiTL)

Ein Workflow-Muster, bei dem die Ausführung von Agenten an kritischen Entscheidungspunkten unterbrochen wird, um von einem Mitarbeiter geprüft und genehmigt zu werden.

Homogene Datenbankmigration

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

heiße Daten

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

Hotfix

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

Hypercare-Phase

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

I

IaC

Sehen Sie sich Infrastruktur als Code an.

Identitätsbasierte Richtlinie

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

Leerlaufanwendung

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

IIoT

Siehe Industrielles Internet der Dinge.

unveränderliche Infrastruktur

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

Eingehende (ingress) VPC

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

Inkrementelle Migration

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

Industrie 4.0

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

Infrastruktur

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

Infrastructure as Code (IaC)

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

Industrielles Internet der Dinge (IIoT)

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

Inspektions-VPC

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

Internet of Things (IoT)

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

Interpretierbarkeit

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

LBAC

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.

MCP

Siehe Model Context Protocol.

Model Context Protocol (MCP)

Ein zustandsloses Protokoll für die Kommunikation zwischen Agenten und Tool.

MCP-Server

Ein Dienst, der ein oder mehrere Tools über das Model Context Protocol verfügbar macht.

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 Mechanismen im AWS Well-Architected Framework erstellen.

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, auf dem publish/subscribeMuster basierendes M2M-Kommunikationsprotokoll (Machine-to-Machine) für IoT-Geräte mit beschränkten Ressourcen.

Microservice

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

Microservices-Architekturen

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

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

Migrationsmetadaten

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

Migrationsmuster

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

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. Um die Konsistenz, Zuverlässigkeit und Vorhersagbarkeit zu verbessern, 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-Kommunikationsprotokoll (M2M) 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 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 -Referenzarchitektur für die Sicherheit empfiehlt, Ihr Netzwerkkonto mit eingehenden und ausgehenden VPCs und Inspektions-VPCs einzurichten, um die bidirektionale Schnittstelle zwischen Ihrer Anwendung und dem Internet zu schützen.

P

Berechtigungsgrenze

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

persönlich identifizierbare Informationen (PII)

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

Personenbezogene Daten

Siehe persönlich identifizierbare Informationen.

Playbook

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

PLC

Siehe programmierbare Logiksteuerung.

PLM

Siehe Produktlebenszyklusmanagement.

policy

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

Polyglotte Beharrlichkeit

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

Portfoliobewertung

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

predicate

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

Prädikat Pushdown

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

Präventive Kontrolle

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

Prinzipal

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

Datenschutz von Natur aus

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

Privat gehostete Zonen

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

proaktive Steuerung

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

Produktlebenszyklusmanagement (PLM)

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

Produktionsumgebung

Siehe Umgebung.

Speicherprogrammierbare Steuerung (SPS)

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

schnelle Verkettung

Verwenden Sie die 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 für alle Parteien definiert, die an Migrationsaktivitäten und Cloud-Vorgängen beteiligt sind. 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 Benutzeranmeldedaten, die Sie in verschlüsselter Form speichern. Es besteht aus dem geheimen Wert und seinen Metadaten. Der geheime Wert kann binär, eine einzelne Zeichenfolge oder mehrere Zeichenketten sein. Weitere Informationen finden Sie unter Was ist in einem Secrets Manager Manager-Geheimnis? in der Secrets Manager Manager-Dokumentation.

Sicherheit durch Design

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

Sicherheitskontrolle

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

Härtung der Sicherheit

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

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

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

Automatisierung von Sicherheitsreaktionen

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

Serverseitige Verschlüsselung

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

Service-Kontrollrichtlinie (SCP)

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

Service-Endpunkt

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

Service Level Agreement (SLA)

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

Service-Level-Indikator (SLI)

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

Service-Level-Ziel (SLO)

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

Modell der geteilten Verantwortung

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

Schatten-KI

Nicht autorisierte KI-Anwendungen, die außerhalb der kontrollierten Kanäle innerhalb eines Unternehmens erstellt oder verwendet wurden.

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 Schrittweise Modernisierung 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

Key-value Paare, die als Metadaten für die Organisation Ihrer AWS Ressourcen dienen. 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.

tool

Eine Funktion oder API, die ein Agent aufrufen kann, um Operationen in externen Systemen auszuführen.

Transit-Gateway

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

Stammbasierter Workflow

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

Vertrauenswürdiger Zugriff

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

Optimieren

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

Zwei-Pizzen-Team

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

U

Unsicherheit

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

undifferenzierte Aufgaben

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

höhere Umgebungen

Siehe Umgebung.

V

Vacuuming

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

Versionskontrolle

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

VPC-Peering

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

Schwachstelle

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

W

Warmer Cache

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

warme Daten

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

Fensterfunktion

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

Workload

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

Workstream

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

WURM

Mal 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 wird als unveränderlich angesehen.

Z

Zero-Day-Exploit

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

Zero-Day-Sicherheitslücke

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

Eingabeaufforderung ohne Vorwarnung

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-Eingabeaufforderungen.

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.