



Anwendung des AWS Well-Architected Frameworks auf Amazon-
Anwendungen WorkSpaces

AWS Präskriptive Leitlinien



AWS Präskriptive Leitlinien: Anwendung des AWS Well-Architected Frameworks auf Amazon-Anwendungen WorkSpaces

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Die Handelsmarken und Handelsaufmachung von Amazon dürfen nicht in einer Weise in Verbindung mit nicht von Amazon stammenden Produkten oder Services verwendet werden, durch die Kunden irreführt werden könnten oder Amazon in schlechtem Licht dargestellt oder diskreditiert werden könnte. Alle anderen Handelsmarken, die nicht Eigentum von Amazon sind, gehören den jeweiligen Besitzern, die möglicherweise zu Amazon gehören oder nicht, mit Amazon verbunden sind oder von Amazon gesponsert werden.

Table of Contents

Einführung	1
Zielgruppe	1
Ziele	2
Säule „Operational Excellence“	3
Organisieren Sie Teams nach Geschäftsergebnissen	3
Implementieren Sie Beobachtbarkeit, um umsetzbare Erkenntnisse zu gewinnen	4
Automatisieren Sie sicher, wo immer möglich	5
Nehmen Sie häufige, kleine, umkehrbare Änderungen vor	7
Verfeinern Sie die Betriebsabläufe regelmäßig	9
Ausfälle antizipieren	9
Lernen Sie aus allen betrieblichen Ereignissen und Kennzahlen	11
Verwenden Sie verwaltete Dienste	11
Säule der Sicherheit	12
Implementieren Sie ein starkes Identitätsfundament	12
Sorgen Sie für Rückverfolgbarkeit	13
Wenden Sie Sicherheit auf allen Ebenen an	14
Automatisieren Sie bewährte Sicherheitsmethoden	15
Halten Sie Menschen von Daten fern	16
Bereiten Sie sich auf Sicherheitsereignisse vor	16
Säule der Zuverlässigkeit	18
Automatische Wiederherstellung nach einem Ausfall	18
Testen Sie die Wiederherstellungsverfahren	19
Horizontal skalieren, um die Verfügbarkeit der gesamten Workloads zu erhöhen	20
Hören Sie auf, die Kapazität zu erraten	20
Managen Sie Veränderungen durch Automatisierung	20
Säule der Leistungseffizienz	22
Demokratisieren Sie fortschrittliche Technologien	22
Werden Sie in wenigen Minuten global	23
Verwenden Sie serverlose Architekturen	23
Experimentieren Sie öfter	24
Denken Sie an mechanische Sympathie	24
Säule der Kostenoptimierung	26
Implementieren Sie Cloud-Finanzmanagement	26
Fügen Sie ein Nutzungsmodell hinzu	26

Messen Sie die Gesamteffizienz	27
Hören Sie auf, Geld für undifferenziertes Heben auszugeben	27
Analysieren Sie Ausgaben und ordnen Sie sie zu	28
Säule der Nachhaltigkeit	30
Verstehen Sie Ihre Wirkung	30
Legen Sie Nachhaltigkeitsziele fest	30
Maximieren der Auslastung	31
Antizipieren und implementieren Sie neue, effizientere Hardware- und Softwareangebote	31
Verwendete verwaltete Dienste	32
Reduzieren Sie die nachgelagerten Auswirkungen Ihrer Cloud-Workloads	32
Ressourcen	33
AWS Dokumentation	33
AWS Blog-Beiträge	33
Dokumentverlauf	35
Glossar	36
#	36
A	37
B	40
C	42
D	46
E	50
F	52
G	54
H	55
I	57
L	60
M	61
O	65
P	68
Q	71
R	72
S	75
T	79
U	81
V	81
W	82

Z	83
.....	lxxxiv

Anwendung des AWS Well-Architected Frameworks auf Amazon-Anwendungen WorkSpaces

Mohamed Wali, Amazon Web Services

Juli 2025 (Geschichte [der Dokumente](#))

Dieses Handbuch behandelt bewährte Methoden für die Anwendung des [AWS Well-Architected Framework](#) bei der Verwendung von [Amazon WorkSpaces](#) Applications. WorkSpaces Applications ist ein vollständig verwalteter Anwendungsstreaming-Service, mit dem Sie Desktop-Anwendungen an Benutzer streamen können, ohne sie neu schreiben zu müssen.

Das AWS Well-Architected Framework unterstützt Cloud-Architekten beim Aufbau sicherer, leistungsstarker, belastbarer und effizienter Infrastrukturen für eine Vielzahl von Anwendungen und Workloads. Es bietet Benutzern und AWS Partnern auch einen konsistenten Ansatz zur Bewertung von Architekturen und zur Implementierung skalierbarer Designs.

Das AWS Well-Architected Framework basiert auf sechs Säulen:

- Operative Exzellenz
- Sicherheit
- Zuverlässigkeit
- Leistungseffizienz
- Kostenoptimierung
- Nachhaltigkeit

In diesem Leitfaden wird erläutert, wie diese Säulen und bewährten Methoden für die Verwendung von WorkSpaces Anwendungen gelten.

Zielgruppe

Dieser Leitfaden richtet sich an:

- Cloud-Architekten und -Ingenieure, die WorkSpaces Anwendungslösungen entwerfen und implementieren und sicherstellen müssen, dass ihre Architekturen den Best Practices von AWS Well-Architected Framework entsprechen.

- IT-Betriebsteams, die WorkSpaces Anwendungsumgebungen verwalten und warten, sich um Flottenmanagement, Skalierung und Überwachung kümmern und Kosten und Leistung optimieren müssen.
- Organizations oder Unternehmen, die WorkSpaces Anwendungen erwägen oder bereits nutzen, möchten Desktop-Anwendungen an ihre Benutzer streamen und müssen sichere, leistungsstarke, belastbare und effiziente Infrastrukturen aufbauen.

Ziele

Das Befolgen der bewährten Methoden in diesem Leitfaden hilft Ihnen dabei:

- Bauen Sie eine sichere, leistungsstarke, belastbare und effiziente Infrastruktur für das Streamen von Desktop-Anwendungen in der AWS Cloud.
- Wenden Sie bei der Bewertung von WorkSpaces Anwendungsarchitekturen und der Implementierung skalierbarer Designs einen konsistenten Ansatz an.

Säule „Operational Excellence“

Operational Excellence (OE) steht für die Hingabe, hochwertige Softwarelösungen zu entwickeln, die die Erwartungen der Benutzer stets erfüllen und übertreffen. Die [Säule Operational Excellence](#) des AWS Well-Architected Framework umfasst bewährte Strategien für eine effektive Teamorganisation, ein robustes Workloaddesign, effiziente Großoperationen und eine nahtlose Anpassung an sich im Laufe der Zeit ändernde Anforderungen. Durch die Einhaltung dieser Prinzipien können Unternehmen sicherstellen, dass ihre Systeme widerstandsfähig und leistungsfähig bleiben und auf die sich ändernden Geschäftsanforderungen abgestimmt sind.

Hauptschwerpunkte für die Anwendung dieser Säule auf Ihre WorkSpaces Anwendungs-Streaming-Umgebung:

- Überwachung und Beobachtbarkeit
- Automatisierung und DevOps
- Betriebsabläufe und Dokumentation
- Support und Störungsmanagement

Organisieren Sie Teams nach Geschäftsergebnissen

Schaffen Sie ein auf die Cloud ausgerichtetes Betriebsmodell mit starkem Engagement der Führungskräfte, bei dem Geschäftsziele und wichtige Leistungsindikatoren (KPIs) die organisatorische Transformation durch optimierte Mitarbeiter, Prozesse und Technologien vorantreiben.

- Struktur des Teams. Richten Sie engagierte Teams ein, die sich an den Ergebnissen des Anwendungs-Streamings orientieren. Zum Beispiel:
 - Das Image-Management-Team ist für die Paketierung von Anwendungen und die Bildoptimierung verantwortlich.
 - Das Flottenbetriebsteam verwaltet Kapazität, Leistung und Skalierung.
 - Das User Experience Team kümmert sich um den Support und die Zufriedenheit der Endbenutzer.
- KPIs und Metriken. Definieren und verfolgen Sie geschäftsorientierte Kennzahlen wie:
 - Verfügbarkeitsraten von Anwendungen

- Zeit für die Bereitstellung neuer Anwendungen
- Kosten pro Stunde des Anwendungs-Streamings
- Betriebsmodell. Schaffen Sie klare Prozesse für:
 - Onboarding und Updates von Anwendungen
 - Kapazitätsmanagement für Flotten
 - Bereitstellung von Benutzerzugriff
 - Reaktion und Lösung von Vorfällen

Implementieren Sie Beobachtbarkeit, um umsetzbare Erkenntnisse zu gewinnen

Implementieren Sie eine umfassende Überwachung und Beobachtbarkeit, um den Zustand der Arbeitslast zu verfolgen KPIs und zu überwachen. Dieses Prinzip ermöglicht datengestützte Entscheidungen und proaktive Verbesserungen in Bezug auf Leistung, Zuverlässigkeit und Kosten.

- Implementieren Sie die Leistungsüberwachung. Konfigurieren Sie [Amazon CloudWatch](#) für:
 - Sorgen Sie für ausreichend Kapazität, um die Nachfrage zu decken. Sie können beispielsweise die folgenden Metriken verwenden:
 - `AvailableCapacity` um verfügbare Streaming-Instanzen zu überwachen
 - `InUseCapacity` um aktuell genutzte Instanzen zu verfolgen
 - `CapacityUtilization` um den Prozentsatz der Flottennutzung zu überwachen
 - Überwachen Sie die Benutzererfahrung und Leistung.
 - Identifizieren und beheben Sie Serviceprobleme umgehend.
- Verfolgen und analysieren Sie Berichte zur Nutzung von WorkSpaces Anwendungen.
- Erfassen und analysieren Sie Anwendungsprotokolle. Weitere Informationen finden Sie in den AWS Blogbeiträgen [Verwenden von Kinesis Agent for Linux zum Streamen von Anwendungsprotokollen in WorkSpaces Anwendungen](#) und [Verwenden von Kinesis Agent for Microsoft Windows zum Speichern von WorkSpaces Windows-Anwendungsprotokollen](#).
- Überwachen Sie WorkSpaces Anwendungsmetriken und Ereignisse mithilfe von Chat-Benachrichtigungen. Weitere Informationen finden Sie im AWS Blogbeitrag [Überwachung und Automatisierung der AWS Endbenutzer-Datenverarbeitung \(EUC\) mit AWS Chatbot](#).

- Ermöglichen Sie ein proaktives Sitzungsmanagement durch visuelle Hinweise. Weitere Informationen finden Sie im AWS Blogbeitrag [Sitzungsablauf und Countdown-Timer in Amazon WorkSpaces Applications anzeigen](#).
- Erstellen Sie Visualisierungen für Nutzungsmuster und Trends. Weitere Informationen finden Sie im AWS Blogbeitrag [Erfassen und Visualisieren von WorkSpaces Amazon-Anwendungsnutzungsberichten in Amazon OpenSearch Service](#).
- Verwenden Sie das EUC-Toolkit, um aktive Sitzungen zu überwachen, den Flottenbestand zu verfolgen und Sitzungsberichte zu erstellen (CSV-Export). Weitere Informationen finden Sie im AWS Blogbeitrag [Use the EUC Toolkit to manage Amazon WorkSpaces Applications and Amazon WorkSpaces](#).

Automatisieren Sie sicher, wo immer möglich

Wenden Sie die Prinzipien von Infrastructure as Code (IaC) an, um alle Aspekte Ihrer Workload-Operationen zu automatisieren. Verwenden Sie Leitplanken, um eine sichere und konsistente Ausführung zu gewährleisten und gleichzeitig manuelle Eingriffe zu reduzieren.

- Automatisieren Sie die Erstellung und Konfiguration von WorkSpaces Anwendungs-Images mithilfe der Image Assistant CLI. Weitere Informationen finden Sie unter [Programmgesteuertes Erstellen Ihres Amazon WorkSpaces Applications-Images mithilfe der Image Assistant-CLI-Operationen](#) in der WorkSpaces Anwendungsdokumentation.
 - Anwendungsinstallation: Verwenden Sie die Image Assistant CLI, um die Installation von Anwendungen während der Image-Erstellung zu automatisieren.
 - Image-Erstellung: Programmgesteuertes Erstellen von WorkSpaces Anwendungs-Images mithilfe der CLI-Befehle von Image Assistant.
 - Konfigurationsmanagement: Automatisieren Sie die Konfiguration der Standardanwendungseinstellungen und Startparameter.
- Automatisieren Sie die Anpassung von WorkSpaces Anwendungs-Images. Weitere Informationen finden Sie im AWS Blogbeitrag [Automatisches Erstellen benutzerdefinierter Windows-Images für WorkSpaces Anwendungen](#).
- Wenden Sie IaC an, um die Infrastruktur und die Anwendungskomponenten für WorkSpaces Anwendungen bereitzustellen. Weitere Informationen finden Sie im AWS Blogbeitrag [Automatisierung der Infrastruktur- und Anwendungsbereitstellung für Amazon WorkSpaces Applications with Terraform](#).

- Implementieren Sie automatisierte Prozesse für das Flottenmanagement, darunter:
 - Skalierung der Flotte auf der Grundlage der Nachfrage. Konfigurieren Sie automatische Skalierungsrichtlinien, um die Flottenkapazität automatisch auf der Grundlage von Nutzungskennzahlen anzupassen. Weitere Informationen finden Sie im AWS Blogbeitrag [Verwenden, AWS Lambda um Skalierungsschritte und Schwellenwerte für WorkSpaces Amazon-Anwendungen anzupassen](#).
 - Aktualisierungen des Basis-Images. Profitieren Sie von automatischen Updates für das Basis-Image der WorkSpaces Anwendung, das von bereitgestellt wird AWS.
 - Optimierung der Kapazität. Richten Sie automatisierte Skalierungsschwellenwerte ein, um die Ressourcennutzung auf der Grundlage von Bedarfsmustern zu optimieren.
- Konfigurieren Sie Leitplanken, um Sicherheitskontrollen zu automatisieren:
 - Maximale Flottengrößenbeschränkungen. Legen Sie Obergrenzen für die Flottenkapazität fest, um eine Überversorgung zu verhindern.
 - Skalierung der Richtlinienkonfiguration. Implementieren Sie Richtlinien zur schrittweisen Skalierung oder Zielverfolgung mit entsprechenden Schwellenwerten.
 - Dienstkontingente. Verwenden Sie AWS Servicekontingenten als integrierte Grenzwerte, um eine übermäßige Ressourcenzuweisung zu verhindern.
 - Skalierbarer Schutz. Konfigurieren Sie den Scale-In-Schutz, um zu verhindern, dass aktive Instances bei Skalierungsereignissen entfernt werden.
- Führen Sie Tests und Validierungen durch, einschließlich Image Builder-, Flotten- und Integrationstests.
 - Testen von Image Builder:
 - Testen Sie Anwendungen direkt in der Image Builder-Oberfläche.
 - Überprüfen Sie den Start und die Funktionalität der Anwendung.
 - Testen Sie Benutzereinstellungen und Konfigurationen.
 - Überprüfen Sie die Anwendungscompatibilität.
 - Flottentests:
 - Testen Sie Streaming-Sitzungen von verschiedenen Client-Geräten aus.
 - Überprüfen Sie die Benutzerberechtigungen und den Zugriff.
 - Überprüfen Sie die Anwendungsleistung.
 - Testen Sie die Benutzererfahrung für Elemente und Operationen wie Zwischenablage,

- Integrationstests:
 - Testen Sie die Active Directory- oder SAML 2.0-basierte Authentifizierung.
 - Testen Sie Basisordner und persistenten Speicher.
 - Testen Sie die Anwendungsberechtigungen.
 - Testen Sie die USB-Geräteumleitung (falls konfiguriert).
- Verwenden Sie den WorkSpaces Anwendungsmanager für Anwendungen, um das Paketieren und Bereitstellen von Anwendungen zu automatisieren. Weitere Informationen finden Sie im AWS Blogbeitrag [Optimieren Sie das Onboarding von Anwendungen mit dem Anwendungsmanager für Amazon WorkSpaces Applications](#).
- Automatisieren Sie die Bereitstellung neuer Anwendungsversionen mithilfe von CI/CD-Pipelines (Continuous Integration and Continuous Delivery). Weitere Informationen finden Sie im AWS Blogbeitrag [Screening Eagle: Optimize CI/CD and end user experience in Amazon WorkSpaces Applications](#).

Nehmen Sie häufige, kleine, umkehrbare Änderungen vor

Erstellen Sie lose gekoppelte, skalierbare Workloads, die häufige, kleine automatisierte Bereitstellungen mit minimalem Risiko und einfachen Rollback-Funktionen ermöglichen.

- Verwenden Sie für Image-Updates die Erstellung versionierter Images und inkrementelle Updates.
 - Erstellung von versionierten Images:
 - Erstellen Sie mithilfe eines Image Builders neue Images für jeden Satz von Änderungen.
 - Pflegen Sie mehrere Image-Versionen, um Rollback-Szenarien zu unterstützen.
 - Verwenden Sie [AWS Tagging-Strategien](#), um Image-Versionen und -Attribute nachzuverfolgen.
 - Inkrementelle Aktualisierungen:
 - Nehmen Sie kleine, inkrementelle Änderungen an Anwendungen oder Konfigurationen vor.
 - Testen Sie Updates im Image Builder gründlich, bevor Sie ein neues Image erstellen.
 - Dokumentieren Sie alle Änderungen, die Sie in jeder neuen Image-Version vorgenommen haben.
- Für Updates zur Kontrollflotte:
 - Erstellen Sie neue Flotten mit aktualisierten Bildern zum Testen.

- Ändern Sie bestehende Flottenattribute, ohne aktive Sitzungen zu unterbrechen.
- Richten Sie Change-Management-Verfahren für Dokumentation, Testprotokolle, Genehmigungsabläufe und Überwachungsprozesse ein.
 - Dokumentation:
 - Führen Sie detaillierte Änderungsprotokolle für alle Image- und Flottenaktualisierungen.
 - Dokumentieren Sie die Testverfahren und Ergebnisse für jede Änderung.
 - Wird verwendet [AWS CloudTrail](#), um Konfigurationsänderungen nachzuverfolgen und zu prüfen.
 - Testprotokolle:
 - Richten Sie einen umfassenden Testprozess für alle Änderungen ein.
 - Schließen Sie Tests zur Anwendungsfunktionalität, Leistung und Benutzererfahrung ein.
 - Führen Sie Tests im Image Builder durch, bevor Sie neue Images erstellen.
 - Führen Sie vor der vollständigen Bereitstellung zusätzliche Tests an Flotten durch, die nicht zur Produktion verwendet werden.
 - Workflows für Genehmigungen:
 - Implementieren Sie einen Genehmigungsprozess für Änderungen an Produktionsumgebungen.
 - Definieren Sie Kriterien für Änderungen, die genehmigt werden müssen, im Vergleich zu Standard-Updates.
 - Legen Sie Rollen und Zuständigkeiten für die Genehmigung von Änderungen fest.
 - Überwachung und Validierung:
 - Verwenden Sie [Amazon CloudWatch](#), um die Flotten- und Anwendungsleistung nach Änderungen zu überwachen.
 - Richten Sie Benachrichtigungen für wichtige Kennzahlen ein, um Probleme nach Updates schnell zu identifizieren.
 - Führen Sie Überprüfungen nach der Implementierung durch, um den Erfolg der Änderungen zu überprüfen und Erkenntnisse zu sammeln.

Verfeinern Sie die Betriebsabläufe regelmäßig

Verbessern Sie kontinuierlich die Betriebsabläufe durch regelmäßige Überprüfungen, Aktualisierungen und die Einbindung des Teams, um alle Beteiligten auf dem Laufenden zu halten und sich an bewährten Verfahren zu orientieren.

- **Verwaltung der Dokumentation.** Pflegen Sie die aktuelle, versionskontrollierte Dokumentation der WorkSpaces Anwendungsverfahren an einem zentralen Ort, um die betriebliche Konsistenz und den Wissensaustausch zwischen den Teams sicherzustellen.
 - **Erforderliche Dokumentation:** Pflegen Sie die up-to-date Dokumentation für wichtige WorkSpaces Anwendungsvorgänge zur Image-Erstellung und -Verwaltung, zum Flottenbetrieb und zur Fehlerbehebung.
 - **Betriebsüberprüfungen:** Überwachen und überprüfen Sie wichtige betriebliche Aspekte, einschließlich Leistungskennzahlen und Störfallmanagement.
- **Kontinuierliche Verbesserung.** Verbessern Sie systematisch den WorkSpaces Anwendungsbetrieb, indem AWS-Service Sie Updates, Betriebskennzahlen und bewährte Verfahren in Standardverfahren integrieren.
 - **Service-Updates:** Überwachen Sie die Versionshinweise der WorkSpaces Anwendungen auf neue Funktionen, Serviceverbesserungen, Sicherheitsupdates und regionale Verfügbarkeit.
 - **Bewährte Methoden:** Überprüfen und integrieren Sie AWS Well-Architected Framework-Updates, bewährte Methoden für WorkSpaces Anwendungen, AWS Referenzarchitekturen und AWS Sicherheitsempfehlungen.
 - **Wissensmanagement:** Pflege und Aktualisierung von Standardarbeitsanweisungen, Runbooks, Anleitungen zur Fehlerbehebung und Dokumentation zur Benutzerunterstützung.

Ausfälle antizipieren

Führen Sie regelmäßig Tests mit Ausfallszenarien durch, um Risiken zu verstehen, Reaktionsverfahren zu validieren und die Teamfähigkeit für den Umgang mit realen Vorfällen zu verbessern.

- **Tests auf Fehler.** Simulieren und testen Sie regelmäßig auf Fehler wie Erschöpfung der Flottenkapazität, Fehler beim Starten von Anwendungen und Probleme mit der Netzwerkkonnektivität.
 - **Erschöpfung der Flottenkapazität:**

- Überwachen und testen Sie das Skalierungsverhalten der Flotte bei Annäherung an Kapazitätsgrenzen.
- Konfigurieren Sie CloudWatch Alarme `CapacityUtilization` und `AvailableCapacity` Metriken.
- Implementieren Sie Verfahren für den Umgang mit Kapazitätsengpässen bei Spitzennutzung.
- Fehler beim Starten der Anwendung:
 - Testen Sie das Verhalten beim Starten von Anwendungen auf Streaming-Instances.
 - Überprüfen Sie den Anwendungszugriff und die Leistung in verschiedenen Flottenkonfigurationen.
- Probleme mit der Netzwerkkonnektivität:
 - Testen Sie die Leistung von Streaming-Sitzungen unter verschiedenen Netzwerkbedingungen.
 - Achten Sie `StreamingSessionLatency` auf Probleme mit der Verbindungsqualität.
 - Stellen Sie sicher, dass die VPC-Einstellungen und Sicherheitsgruppen ordnungsgemäß konfiguriert sind.
- Wiederherstellungsverfahren. Entwickeln und testen Sie Verfahren für:
 - Flotten-Failover zwischen AWS Availability Zones. Dokumentieren Sie außerdem Verfahren zur Skalierung der Flottenkapazität, zur Verwaltung von Flottenaktualisierungen und zur Reaktion auf Probleme mit dem Zustand von Instanzen.
 - Verwaltung von Benutzerdaten:
 - Konfigurieren und testen Sie [Persistenz- und Speicherlösungen für Anwendungseinstellungen](#) für Basisordner in Amazon Simple Storage Service (Amazon S3) für Windows-Flotten und gemeinsam genutzte Dateisysteme in Amazon Elastic File System (Amazon EFS) für Linux-Flotten.
 - Überprüfen Sie die Datensynchronisierung zwischen Sitzungen.
 - Servicekontinuität. Behalten Sie die Verfahren für die Erstellung neuer Flotteninstanzen, die Verwaltung von Image-Updates und den Umgang mit Sitzungsunterbrechungen bei.
- Risikomanagement. Identifizieren und mindern Sie:
 - Kapazitätsbeschränkungen durch die Festlegung einer angemessenen Mindestkapazität für die Flotte, die Konfiguration automatischer Skalierungsrichtlinien auf der Grundlage von Nachfragemustern und die Überwachung der Flottenauslastungstrends mithilfe von CloudWatch Kennzahlen wie `CapacityUtilizationInUseCapacity`, und `AvailableCapacity`.

- Leistungengpässe durch die Erfassung wichtiger Kennzahlen, wie `StreamingSessionLatency` z. B. die Konfiguration der entsprechenden CloudWatch Alarme.

Lernen Sie aus allen betrieblichen Ereignissen und Kennzahlen

Fördern Sie eine Kultur der kontinuierlichen Verbesserung, indem Sie die Erfahrungen aus betrieblichen Ereignissen und Misserfolgen im gesamten Unternehmen weitergeben. Betonen Sie deren Auswirkungen auf die Geschäftsergebnisse.

- Analyse von Ereignissen. Dokumentieren und analysieren Sie Serviceunterbrechungen, Leistungseinbußen, Benutzerbeschwerden und Kapazitätsprobleme.
- Überprüfung der Kennzahlen. Analysieren Sie regelmäßig Nutzungsmuster, Leistungstrends, Kostenkennzahlen und Daten zur Benutzerzufriedenheit.
- Wissensaustausch. Etablieren Sie Prozesse für Team-Lernsitzungen, die Dokumentation bewährter Verfahren, den teamübergreifenden Wissenstransfer und Rückblicke auf Vorfälle.

Verwenden Sie verwaltete Dienste

Minimiere den betrieblichen Aufwand, indem du AWS Managed Services nutzt und dafür standardisierte Verfahren aufbaust. Integrieren Sie sie in die folgenden AWS Managed Services:

- [AWS Systems Manager](#) für die Automatisierung
- [Amazon CloudWatch](#) zur Überwachung
- [AWS Identity and Access Management \(IAM\)](#) für die Zugriffskontrolle
- [Amazon S3](#) für Benutzerspeicher für Windows-Flotten
- [Amazon EFS](#) für Benutzerspeicher für Linux-Flotten
- [AWS Directory Service](#) für die Benutzerauthentifizierung

Säule der Sicherheit

Die [Sicherheitssäule](#) des AWS Well-Architected Framework konzentriert sich auf die Nutzung von Cloud-Funktionen, um robuste Schutzmechanismen für Ihre Informationen, Infrastruktur und Ressourcen einzurichten. Diese Prinzipien tragen dazu bei, Ihre allgemeine Sicherheitslage zu verbessern und gleichzeitig Innovationen zu ermöglichen.

Hauptschwerpunkte für die Anwendung dieser Säule auf Ihre WorkSpaces Anwendungs-Streaming-Umgebung:

- Datenintegrität und Vertraulichkeit
- Verwalten von Benutzerberechtigungen
- Einrichtung von Kontrollen zur Erkennung von Sicherheitsereignissen

Implementieren Sie ein starkes Identitätsfundament

Verwenden Sie die erforderlichen Mindestberechtigungen für den Zugriff auf AWS Ressourcen und zentralisieren Sie gleichzeitig das Identitätsmanagement und vermeiden Sie langfristige Anmeldeinformationen.

- Gewähren Sie Berechtigungen mit den geringsten Rechten für WorkSpaces Anwendungsressourcen:
 - Erstellen Sie spezifische IAM-Rollen für WorkSpaces Anwendungsflotten mit minimalen erforderlichen Berechtigungen.
 - Konfigurieren Sie eingeschränkte IAM-Berechtigungen für Image Builder.
 - Beschränken Sie den Administratorzugriff auf Funktionen zur WorkSpaces Anwendungsverwaltung.
 - Definieren Sie detaillierte Berechtigungen für das Stack- und Flottenmanagement.
- Implementieren Sie geeignete Mechanismen zur Benutzerauthentifizierung:
 - Konfigurieren Sie den SAML 2.0-Verbund für die Integration von Enterprise Identity Providern.
 - [AWS IAM Identity Center](#) Für die Benutzerverwaltung einrichten.
 - Verwenden Sie benutzerdefinierte Identity Broker nur, wenn dies für bestimmte Authentifizierungsszenarien erforderlich ist.
 - Implementieren Sie die Multi-Faktor-Authentifizierung (MFA), sofern sie unterstützt wird.

- Steuern Sie den Benutzerzugriff auf Anwendungen:
 - Konfigurieren Sie Anwendungsberechtigungen, um den Zugriff auf bestimmte Anwendungen einzuschränken.
 - Erstellen Sie Anwendungszuweisungsgruppen auf der Grundlage von Benutzerrollen.
 - Verwalten Sie den Anwendungszugriff mithilfe von Stack-Berechtigungen.
 - Implementieren Sie Sitzungsrichtlinien, um das Anwendungsverhalten zu steuern.
- Sichere Benutzersitzungen mit geeigneten Kontrollen:
 - Konfigurieren Sie Richtlinien für Sitzungs-Timeouts.
 - Legen Sie die Timeout-Aktionen beim Trennen fest.
 - Implementieren Sie Anforderungen an die Persistenz von Sitzungen.
 - Steuern Sie die Berechtigungen für die Dateisystemumleitung.
- Konfigurieren Sie die zertifikatsbasierte Authentifizierung für Anwendungen. WorkSpaces Weitere Informationen finden Sie im AWS Blogbeitrag [Vereinfachen Sie die zertifikatsbasierte Authentifizierung für WorkSpaces Anwendungen und WorkSpaces mit AWS Private CA Connector für Active Directory](#).
- Verwenden Sie Sitzungs-Tags, um eine differenzierte Zugriffskontrolle zu implementieren. Weitere Informationen finden Sie im AWS Blogbeitrag [Verwenden Sie Sitzungs-Tags, um WorkSpaces Anwendungsberechtigungen zu vereinfachen](#).

Sorgen Sie für Rückverfolgbarkeit

Implementieren Sie Systeme zur Echtzeitüberwachung und automatisierten Reaktion auf alle Änderungen und Aktivitäten in der Umgebung.

- Konfigurieren Sie die [CloudWatch Protokollierung](#) für Anwendungsprotokolle, um anwendungsspezifische Ereignisse wie Anwendungsstarts, Abstürze und Fehler zu überwachen. Konfigurieren Sie Sitzungsprotokolle, um Streaming-Sitzungsinformationen wie Sitzungsstarts, -stopps und Benutzerverbindungsereignisse nachzuverfolgen.
- [Aktivieren Sie diese Option CloudTrail](#) , um alle Aufrufe der WorkSpaces Anwendungs-API zu protokollieren und Verwaltungsereignisse wie Flottenerstellung und -änderungen, Image Builder-Operationen, Stack-Konfigurationen und Benutzerverwaltungsaktivitäten zu verfolgen.
- Überwachen Sie die Aktivität der WorkSpaces Anwendungsinstanz:
 - Konfigurieren Sie die Instanzprotokollierung, um Ereignisse auf Systemebene zu erfassen.

- Verfolgen Sie Anwendungsstarts und -ausfälle.
- Überwachen Sie die Nutzung und Leistung der Systemressourcen.
- Benutzeraktivitäten verfolgen:
 - Überwachen Sie Versuche und Fehlschläge bei der Benutzerauthentifizierung. Verwenden Sie CloudWatch Metriken und CloudWatch Protokolle, um Anmeldeversuche von Benutzern, Start- und Endzeiten von Sitzungen sowie Ereignisse beim Trennen von Sitzungen zu verfolgen.
 - Verfolgen Sie die Nutzungsmuster von Anwendungen. [Ermöglichen Sie WorkSpaces Anwendungsnutzungsberichte](#), um Informationen wie Sitzungsdauer, Start- und Endzeiten, verwendete Instanztypen und aufgerufene Anwendungen abzurufen.
 - Zeichnen Sie Dateisystemaktivitäten über aktivierte Basisordner auf.
 - Konfigurieren Sie die Einstellungen für die Zwischenablage und die Druckvorgänge, um Ihre Ziele zur Verhinderung von Datenverlust zu erreichen.
- Konfigurieren Sie [CloudWatchAlarmer](#) für sicherheitsrelevante Messwerte wie fehlgeschlagene Benutzerauthentifizierungen, ungewöhnliche Sitzungsmuster und Verstöße gegen den Ressourcenzugriff.
- Verwenden Sie das EUC-Toolkit, um aktive Sitzungen und Status zu verfolgen, IP-Adressen auf aktive Sitzungen zu überwachen und Sitzungsdaten für Auditzwecke zu exportieren. Weitere Informationen finden Sie im AWS Blogbeitrag [Verwenden Sie das EUC-Toolkit zur Verwaltung von Amazon WorkSpaces Applications und Amazon](#). WorkSpaces

Wenden Sie Sicherheit auf allen Ebenen an

Implementieren Sie mehrere Ebenen von Sicherheitskontrollen für alle Komponenten Ihrer Infrastruktur, vom Netzwerkrand bis zum Anwendungscode.

- Konfigurieren Sie die Sicherheit auf Netzwerkebene:
 - Implementieren Sie strenge Sicherheitsgruppenregeln.
 - Platzieren Sie Instances der WorkSpaces Anwendungsflotte in privaten Subnetzen, die keinen direkten Internetzugang haben. Steuern Sie den Internetzugang über NAT-Geräte.
 - Verwenden Sie Virtual Private Cloud (VPC) -Endpunkte, um auf unterstützte Endpunkte AWS-Services (wie Amazon S3) zuzugreifen.
 - Implementieren Sie Netzwerkzugriffskontrolllisten (ACLs) als zusätzliche Netzwerksicherheitsebene.

- Beschränken Sie den Streaming-Port-Zugriff (TCP 8443 für HTTPS und WebSocket Secure) auf bestimmte IP-Bereiche.
- Konfigurieren Sie die Sicherheit auf Zugriffsebene:
 - Implementieren Sie Richtlinien für das Sitzungs-Timeout, um die Verbindung inaktiver Benutzer automatisch zu trennen.
 - Implementieren Sie eine attributbasierte Zugriffskontrolle mithilfe von Sitzungs-Tags. Weitere Informationen finden Sie im AWS Blogbeitrag [Verwenden Sie Sitzungs-Tags, um Anwendungsberechtigungen zu vereinfachen WorkSpaces](#).
- Konfigurieren Sie die Sicherheit auf Anwendungsebene:
 - Konfigurieren Sie Anwendungsberechtigungen, um zu steuern, welche Benutzer auf bestimmte Anwendungen zugreifen können.
 - Aktivieren Sie die Steuerung der Dateisystemumleitung, um den Zugriff auf lokale Laufwerke einzuschränken.
 - Konfigurieren Sie die Berechtigungen für Zwischenablage, Dateiübertragung und Drucken entsprechend den Sicherheitsanforderungen.
 - Richten Sie die Zugriffskontrollen für USB-Geräte gemäß den Sicherheitsrichtlinien ein.
- Konfigurieren Sie die Sicherheit der Bildebene:
 - Erstellen und verwalten Sie gehärtete Basis-Images, die die Sicherheitsanforderungen erfüllen.
 - Halten Sie die Basis-Images mit den neuesten Sicherheitspatches auf dem neuesten Stand.
 - Konfigurieren Sie die Windows-Sicherheitseinstellungen in Basisimages.
 - Deaktivieren Sie nicht benötigte Windows-Dienste und -Features in Basisimages.

Automatisieren Sie bewährte Sicherheitsmethoden

Verwenden Sie automatisierte, codedefinierte Sicherheitskontrollen in versionskontrollierten Vorlagen, um eine sichere und skalierbare Infrastrukturbereitstellung zu ermöglichen.

- Verwenden Sie Infrastructure as Code (IaC), indem Sie Dienste nutzen, um beispielsweise konsistente Sicherheitskonfigurationen für alle Flottenbereitstellungen AWS CloudFormation zu implementieren. Weitere Informationen finden Sie im AWS Blogbeitrag [Automatisches Anhängen zusätzlicher Sicherheitsgruppen an Amazon WorkSpaces Applications und Amazon WorkSpaces](#).
- Automatisieren Sie Sicherheitsprozesse bei der Image-Erstellung mithilfe der Image Assistant CLI.

- Konfigurieren Sie mithilfe von CloudWatch Amazon-Alarmen, EventBridge Amazon-Regeln und AWS Lambda Funktionen für automatisierte Antworten automatische Antworten auf die Überschreitung von Kapazitätsauslastungsschwellenwerten, unbefugten Zugriffsversuchen und Änderungen der Sicherheitsgruppe.

Halten Sie Menschen von Daten fern

Automatisieren Sie Datenverarbeitungsprozesse, um den direkten menschlichen Zugriff zu minimieren und das Risiko von Fehlern oder Fehlhandhabungen zu verringern.

- Konfigurieren Sie Anwendungsberechtigungen, um zu kontrollieren, welche Benutzer auf bestimmte Anwendungen zugreifen können.
- Verwenden Sie das [Dynamic Application Framework](#), um einen dynamischen Anwendungsanbieter zu erstellen, der Anwendungen dynamisch auf der Grundlage von Benutzerattributen verfügbar macht.
- Konfigurieren Sie die Dateisystemumleitung, um zu steuern, auf welche lokalen Laufwerke Benutzer zugreifen können, um den Zugriff auf bestimmte Ordner einzuschränken und um Dateiübertragungsberechtigungen zwischen lokalen und Streaming-Sitzungen zu verwalten.
- Implementieren Sie Einschränkungen für die Zwischenablage, um die gemeinsame Nutzung der Zwischenablage zwischen lokalen Sitzungen und Streaming-Sitzungen zu deaktivieren, bei Bedarf einen unidirektionalen Zwischenablagefluss zu ermöglichen und unbefugtes Kopieren von Daten zu verhindern.
- Konfigurieren Sie die Persistenz der Anwendungseinstellungen, um Anwendungskonfigurationen automatisch zu speichern und wiederherzustellen, manuelle Konfigurationen zu vermeiden und eine konsistente Benutzererfahrung zu gewährleisten.

Bereiten Sie sich auf Sicherheitsereignisse vor

Entwickeln und praktizieren Sie Pläne zur Reaktion auf Vorfälle mithilfe automatisierter Tools, um Sicherheitsvorfälle schnell erkennen, untersuchen und beheben zu können.

- Richten Sie CloudWatch Alarme für fehlgeschlagene Authentifizierungsversuche, Änderungen an Flottensicherheitsgruppen, Änderungen an Image-Konfigurationen und ungewöhnliche Streaming-Sitzungsmuster ein.

- Dokumentieren Sie Reaktionsverfahren für gängige WorkSpaces Anwendungssicherheitsszenarien wie:
 - Unbefugte Zugriffsversuche
 - Erkennung: Überwachen Sie Authentifizierungsfehler.
 - Antwort: Widerrufen Sie Benutzerberechtigungen, überprüfen Sie Sitzungsprotokolle und aktualisieren Sie die Zugriffsrichtlinien.
 - Kompromittierte Streaming-Instanzen
 - Erkennung: Überwachen Sie das Verhalten der Instanzen.
 - Reaktion: Beenden Sie die betroffenen Sitzungen, ersetzen Sie Flotteninstanzen und überprüfen Sie die Konfigurationen der Sicherheitsgruppen.
 - Versuche, Daten zu exfiltrieren
 - Erkennung: Überwachen Sie die Dateiübertragungsaktivitäten.
 - Reaktion: Überprüfen Sie die Zwischenablage und die Dateiübertragungsprotokolle, passen Sie die Dateiübertragungsberechtigungen an und aktualisieren Sie die Datenschutzrichtlinien.
- Implementieren Sie automatisierte Wiederherstellungsprozesse für den Austausch von Flotteninstanzen, die Wiederherstellung von Sicherheitsgruppen, die Neukonfiguration des Benutzerzugriffs und die Wiederherstellung von Anwendungseinstellungen.
- Wird AWS-Services für das Sicherheitsmanagement verwendet, z. B. AWS Security Hub CSPM für Sicherheitserkenntnisse, und Amazon GuardDuty für die Erkennung von Bedrohungen.

Säule der Zuverlässigkeit

Die [Zuverlässigkeitssäule](#) des AWS Well-Architected Framework befasst sich damit, wie gut ein System seine beabsichtigte Funktionalität und Leistung während der erwarteten Betriebsperioden während seiner gesamten Lebensdauer beibehält. Es enthält umfassende Richtlinien für den Aufbau und die Wartung zuverlässiger Systeme AWS, einschließlich Strategien für Tests und Validierung in allen Phasen des Workload-Lebenszyklus.

Hauptschwerpunkte für die Anwendung dieser Säule auf Ihre WorkSpaces Anwendungs-Streaming-Umgebung:

- Flottenmanagement und Skalierung
- Zuverlässigkeit von Sitzungen
- Verfügbarkeit von Anwendungen
- Wiederherstellungsverfahren

Automatische Wiederherstellung nach einem Ausfall

Überwachen Sie KPIs den geschäftlichen Nutzen, um automatisierte Reaktionen auszulösen, mit denen Ausfälle vorhergesagt, verhindert oder behoben werden können, bevor sie sich auf den Betrieb auswirken.

- Stellen Sie sicher, dass Ihre IP-Subnetzzuweisung der Erweiterung und Verfügbarkeit Rechnung trägt.
- Überwachen Sie wichtige CloudWatch Kennzahlen, um die Verfügbarkeit und Leistung von Diensten sicherzustellen, einschließlich Kennzahlen zur Flottenkapazität wie `AvailableCapacity` und `InUseCapacity` und Kennzahlen zur Streaming-Qualität wie `StreamingSessionLatency`.
- Konfigurieren Sie Warnmeldungen für Kapazitätsgrenzwerte, Sitzungsintegritätskennzahlen, Leistungseinbußen und Änderungen des Flottenzustands.
- Verwenden Sie die integrierten Funktionen zur automatischen Skalierung von WorkSpaces Anwendungen, um:
 - Konfigurieren Sie die minimale und maximale Flottenkapazität.
 - Legen Sie Skalierungsrichtlinien auf der Grundlage der Kapazitätsauslastung fest.

- Definieren Sie Scale-Out- und Scale-In-Schwellenwerte auf der Grundlage von Kennzahlen zur Benutzererfahrung und Geschäftsanforderungen und nicht nur auf technischen Kennzahlen.
- Erstellen Sie eine Disaster-Recovery-Umgebung für Ihre Anwendungsumgebung. WorkSpaces
Weitere Informationen finden Sie im AWS Blogbeitrag [Überlegungen zur Notfallwiederherstellung mit Amazon WorkSpaces Applications](#).

Testen Sie die Wiederherstellungsverfahren

Cloud-Umgebungen ermöglichen das automatisierte Testen von Ausfallszenarien und Wiederherstellungsverfahren. Diese Funktionen helfen Ihnen dabei, Sicherheitslücken zu identifizieren und zu beheben, bevor es zu echten Ausfällen kommt.

- Tests zur Wiederherstellung von Flotten. Implementieren Sie umfassende Tests zur Wiederherstellung Ihrer Flotte in mehreren Szenarien:
 - Simulieren Sie die Instanzbeendigung, um die automatische Skalierungsreaktion zu überprüfen.
 - Überprüfen Sie die Aufrechterhaltung der Mindestkapazität der Flotte.
 - Testen Sie den Zeitplan für den Austausch der Instance und die Benutzerumleitung.
 - Überprüfen Sie die Wirksamkeit der Skalierungsrichtlinien.
 - Testen Sie die Kapazitätsgrenzen Ihrer Flotte und die Handhabung von Überläufen.
- Testen der Sitzungswiederherstellung. Implementieren Sie Verfahren zur Validierung der Sitzungswiederherstellung:
 - Testen Sie Szenarien zum Trennen und Wiederverbinden.
 - Überprüfen Sie die Beibehaltung des Anwendungsstatus.
 - Testen Sie verschiedene Szenarien für Netzwerkunterbrechungen.
 - Überprüfen Sie das Verhalten beim Sitzungs-Timeout.
 - Überprüfen Sie die Persistenz der Benutzerauthentifizierung.
 - Überprüfen Sie die Handhabung von temporärem Speicher.

Horizontal skalieren, um die Verfügbarkeit der gesamten Workloads zu erhöhen

Verteilen Sie Ihre Arbeitslast auf mehrere kleinere Ressourcen, um die Auswirkungen einzelner Ausfälle zu minimieren und einzelne Fehlerquellen zu eliminieren.

- Stellen Sie Flotteninstanzen in mehreren Availability Zones bereit.
- Konfigurieren Sie die entsprechende Mindestflottenkapazität.
- Konfigurieren Sie die automatische Skalierung für Flotten und legen Sie entsprechende Skalierungsschwellenwerte fest.
- Überwachen Sie die Kapazitätsauslastung der gesamten Flotte.
- Stellen Sie WorkSpaces Anwendungsstapel in mehreren Regionen bereit. Weitere Informationen finden Sie im AWS Blogbeitrag [Optimieren Sie die Benutzererfahrung mit latenzbasiertem Routing für Amazon-Anwendungen. WorkSpaces](#)

Hören Sie auf, die Kapazität zu erraten

Nutzen Sie die automatischen Skalierungsfunktionen der Cloud, um Ressourcen dynamisch an den Bedarf anzupassen. Dies trägt dazu bei, eine Überlastung der Ressourcen zu verhindern und gleichzeitig eine optimale Effizienz aufrechtzuerhalten.

- Überwachen Sie wichtige Kennzahlen wie `CapacityUtilization`, `AvailableCapacity`, `InUseCapacity` um den Kapazitätsbedarf zu verstehen.
- Verfolgen Sie Trends bei der Flottenauslastung über verschiedene Zeiträume hinweg. Überwachen Sie tägliche Muster, wöchentliche Schwankungen, monatliche Trends und saisonale Spitzenwerte.
- Richten Sie Skalierungsrichtlinien ein und konfigurieren Sie Skalierungsschwellenwerte.
- Stellen Sie sicher, dass zwischen den aktuellen Kontingenten und der maximalen Nutzung eine ausreichende Lücke besteht, um ein Failover zu ermöglichen.
- Berücksichtigen Sie feste Servicekontingente und Einschränkungen in Ihrer gesamten Architektur.

Managen Sie Veränderungen durch Automatisierung

Implementieren Sie Infrastrukturänderungen durch Automatisierung, einschließlich versionsgesteuerter Änderungen am Automatisierungscode selbst.

- Verwenden Sie IaC für die Flottenkonfiguration.
- Implementieren Sie konsistente Skalierungsrichtlinien.
- Verwenden Sie die [Image Assistant CLI](#) für eine konsistente Image-Erstellung.

Säule der Leistungseffizienz

Die [Säule der Leistungseffizienz](#) des AWS Well-Architected Framework konzentriert sich auf die Optimierung der Nutzung von Cloud-Ressourcen, um Leistungsziele zu erreichen oder zu übertreffen und gleichzeitig die Anpassungsfähigkeit an schwankende Anforderungen und neue Technologien sicherzustellen. Es unterstreicht die Bedeutung einer kontinuierlichen Feinabstimmung der Systeme, um in einer dynamischen Cloud-Umgebung eine maximale Effizienz aufrechtzuerhalten.

Wichtige Schwerpunktbereiche für die Anwendung dieser Säule auf Ihre WorkSpaces Anwendungs-Streaming-Umgebung:

- Auswahl und Optimierung des Instanztyps
- Optimierung der Streaming-Leistung
- Verwaltung der Flottenkapazität

Demokratisieren Sie fortschrittliche Technologien

Nutzen Sie von Cloud-Anbietern verwaltete Dienste für komplexe Technologien, sodass sich Ihr Team auf die Produktentwicklung statt auf das Infrastrukturmanagement konzentrieren kann.

- Konfigurieren Sie die entsprechenden Instanztypen auf der Grundlage der Anwendungsanforderungen:
 - Wählen Sie GPU-fähige Instanzen für grafikintensive Anwendungen aus.
 - Wählen Sie je nach [Anwendungsanforderungen geeignete GPU-Familien](#) (wie Graphics G4dn oder Graphics G5) aus.
- Wählen und konfigurieren Sie eine der folgenden Authentifizierungsmethoden:
 - Richten Sie die Integration mit einem SAML 2.0-basierten Identitätsanbieter ein.
 - Konfigurieren Sie die Einstellungen für den Benutzerpool.
 - Integrieren Sie mit [AWS Directory Service](#).
- Aktivieren und konfigurieren Sie Speicheroptionen je nach Benutzeranforderungen:
 - Richten Sie in [Amazon S3](#) Basisordner für Windows-basierte Flotten ein.
 - Richten Sie gemeinsame Dateisysteme in [Amazon EFS](#) für Linux-basierte Flotten ein.
 - Konfigurieren Sie persistente Speicherberechtigungen.
 - Aktivieren Sie die Persistenz der Anwendungseinstellungen.

Werden Sie in wenigen Minuten global

Nutzen Sie die Bereitstellung in mehreren Regionen, um die globale Benutzererfahrung durch verringerte Latenz zu verbessern.

- Konfigurieren Sie Flotten in mehreren, AWS-Regionen indem Sie Flotten in Regionen einsetzen, die Ihren Benutzern am nächsten sind, und gleichzeitig separate Stacks für jede Region erstellen.
- Implementieren Sie eine regionsübergreifende Umleitung, um WorkSpaces Anwendungsbenutzer automatisch zu den AppStream Stacks weiterzuleiten, die ihrem aktuellen Standort am nächsten sind.
- Wenn Sie eine der optionalen Funktionen von WorkSpaces Applications verwenden, z. B. Persistenz von Anwendungseinstellungen, Basisordner oder Elastic Fleets, müssen Sie die regionsübergreifende Amazon S3 S3-Replikation für Benutzerdaten für Windows-basierte Flotten und die regionsübergreifende Replikation für Linux-basierte Flotten konfigurieren.
- Replizieren Sie Bilder regionsübergreifend. Weitere Informationen finden Sie in der AWS Dokumentation unter [Kopieren eines Images, das Ihnen gehört, AWS-Region in ein anderes in Amazon WorkSpaces Applications](#).
- Stellen Sie für domänengebundene Flotten sicher, dass eine Active Directory-Infrastruktur, einschließlich Active Directory Federation Services (AD FS) (sofern Sie nicht SAML 2.0 und Amazon Cognito als Alternative verwenden), in den anderen Regionen ordnungsgemäß konfiguriert ist und dass Sie sie für Replikationsfunktionen in mehreren Regionen verwenden [AWS Directory Service for Microsoft Active Directory](#).
- Leiten Sie Benutzer zu den Anwendungsendpunkten mit der niedrigsten Latenz weiter. WorkSpaces Weitere Informationen finden Sie im AWS Blogbeitrag [Optimieren Sie die Benutzererfahrung mit latenzbasiertem Routing für Amazon-Anwendungen](#). WorkSpaces

Verwenden Sie serverlose Architekturen

Serverlose Architekturen reduzieren den Serververwaltungsaufwand und senken die Kosten, indem sie Cloud-verwaltete Dienste für Rechenfunktionen verwenden.

Verwenden Sie AWS serverlose Dienste wie die folgenden:

- [AWS Lambda](#) um Aufgaben zu automatisieren und benutzerdefinierte Logik durch ereignisgesteuerte Funktionen zu integrieren

- [Amazon S3](#) zur Bereitstellung von skalierbarem Speicher für WorkSpaces Anwendungsbenutzerdaten, Anwendungsdateien und Sitzungsartefakte
- [Amazon CloudWatch](#) bietet Überwachung, Protokollierung und Warnmeldungen für Kennzahlen zur Leistung und Nutzung von WorkSpaces Anwendungen
- [Amazon Cognito](#) zur Erleichterung der Benutzerauthentifizierung und Zugriffskontrolle für WorkSpaces Anwendungsanwendungen
- [Amazon API Gateway](#) RESTful APIs zur Erstellung einer Schnittstelle zwischen WorkSpaces Anwendungen und anderen Diensten oder benutzerdefinierten Anwendungen

Experimentieren Sie öfter

Die Cloud-Infrastruktur ermöglicht das schnelle Testen verschiedener Ressourcenkonfigurationen, um Leistung und Kosten zu optimieren.

- Testen Sie verschiedene Instanztypen, um Leistung und Kosten zu optimieren:
 - Vergleichen Sie die Stream-Leistung verschiedener Instance-Familien.
 - Bewerten Sie GPU- und Nicht-GPU-Instances für Grafikanwendungen.
 - Testen Sie speicheroptimierte Instances für speicherintensive Anwendungen.
- Testen Sie Anwendungskonfigurationen mit Image Builder:
 - Erstellen Sie Testimages mit unterschiedlichen Anwendungskonfigurationen.
 - Überprüfen Sie die Anwendungsleistung vor der Bereitstellung.
 - Testen Sie die Anwendungskompatibilität mit verschiedenen Instanztypen.
- Testen Sie die Flotteneinstellungen mithilfe von Flottenkapazitätskonfigurationen wie Mindest- und Höchstkapazität, Skalierungsrichtlinien, Sitzungseinstellungen wie maximale Sitzungsdauer und Timeout-Einstellungen beim Trennen.

Denken Sie an mechanische Sympathie

Wählen Sie Cloud-Dienste, die auf den spezifischen Anforderungen und Nutzungsmustern Ihres Workloads basieren, um optimale Leistung und Effizienz zu gewährleisten.

- Wählen Sie Graphics G5-Instances für grafikintensive Anwendungen, Anwendungen, die DirectX-, OpenGL-, OpenCL- oder 3D-Visualisierungssoftware benötigen.

- Wählen Sie `stream.standard` Instanzen für Geschäftsanwendungen, Webbrowser und leichte Grafikanwendungen aus
- Überwachen und passen Sie das Streaming-Protokoll anhand von CloudWatch Kennzahlen wie `StreamingSessionLatency`.
- Konfigurieren Sie WorkSpaces Anwendungen so VPCs , dass sie Ihren Benutzern am nächsten sind, und verwenden Sie die entsprechende Netzwerkbandbreite, die den Anforderungen Ihrer Anwendung entspricht.
- Wählen Sie auf der Grundlage des Anwendungsverhaltens den geeigneten Flottentyp aus. Wählen Sie beispielsweise Flotten mit einer Sitzung für Anwendungen, die spezielle Ressourcen benötigen, und Flotten mit mehreren Sitzungen für Anwendungen, die Ressourcen effizient gemeinsam nutzen können.
- Erwägen Sie die Anwendungskompatibilität mit Umgebungen mit mehreren Sitzungen.
- Verwenden Sie die [Funktion zur Dateisystemumleitung](#), um die Interaktionen zwischen Remote- und lokalen Anwendungen zu verwalten. Weitere Informationen finden Sie im AWS Blogbeitrag [Lokale Anwendungen aus einer Amazon WorkSpaces Applications-Streaming-Sitzung starten](#).

Säule der Kostenoptimierung

Die [Säule der Kostenoptimierung](#) des AWS Well-Architected Framework konzentriert sich auf die Maximierung des Geschäftswerts bei gleichzeitiger Minimierung der Ausgaben. Es hilft sicherzustellen, dass jeder Dollar, den Sie für Cloud-Ressourcen ausgeben, effektiv zur Erreichung Ihrer Unternehmensziele beiträgt.

Wichtige Schwerpunktbereiche für die Anwendung dieser Säule auf Ihre WorkSpaces Anwendungs-Streaming-Umgebung:

- Flottenkapazitätsmanagement und Auswahl des Instance-Typs
- Skalierung und Optimierung der Terminplanung
- Überwachung und Analyse von Nutzungsmustern
- Kostenzuweisung und -verfolgung

Implementieren Sie Cloud-Finanzmanagement

Bauen Sie mithilfe strukturierter Programme und Prozesse spezielle organisatorische Fähigkeiten für Cloud-Finanzmanagement und Kostenoptimierung auf, um den Wert und die Effizienz der Cloud zu maximieren.

- Überwachen Sie die WorkSpaces Anwendungskosten mithilfe von Nutzungs [AWS Cost Explorer](#)- und Nutzungsberichten, um die Nutzung der Streaming-Stunden nachzuverfolgen, die Kosten für Flotteninstanzen zu analysieren und die regionale Kostenverteilung zu überwachen.
- Planen und legen Sie Kostenkontrollen fest [AWS Budgets](#), indem Sie Warnmeldungen für die Gesamtkosten der WorkSpaces Anwendungsdienste einrichten, Budgetschwellenwerte für den Service festlegen und die tatsächlichen Ausgaben anhand der budgetierten Beträge überwachen. Weitere Informationen finden Sie im AWS Blogbeitrag [Wie Sie mithilfe von Automatisierung die Kosten von WorkSpaces Amazon-Anwendungen optimieren und kontrollieren können](#).

Fügen Sie ein Nutzungsmodell hinzu

Skalieren Sie die Rechenressourcen und -kosten auf der Grundlage der tatsächlichen Nutzungsmuster. Sie können beispielsweise Umgebungen außerhalb der Geschäftszeiten herunterfahren, um Ihre Ausgaben zu optimieren.

- Wählen Sie das passende Preismodell. Verwenden Sie beispielsweise ständig verfügbare Flotten für eine konsistente Nutzung und On-Demand-Flotten für variable Workloads.
- Wählen Sie die optimalen Instance-Typen aus. Verwenden Sie beispielsweise `stream.standard` Instanzen für allgemeine Anwendungen und Grafikinstanzen (G4dn) nur bei Bedarf.

Messen Sie die Gesamteffizienz

Berechnen und verfolgen Sie den Output cost-per-unit Ihres Unternehmens, um Effizienzsteigerungen zu quantifizieren und Optimierungsmaßnahmen zu steuern.

- Verfolgen Sie die Effizienz Ihrer Sitzungen.
- Überwachen Sie die Flottenauslastung anhand der folgenden CloudWatch Kennzahlen:
 - `AvailableCapacity` um ungenutzte Kapazitäten nachzuverfolgen
 - `InUseCapacity` um die tatsächliche Nutzung zu messen
- Berechnen und verfolgen Sie die Kosten pro Sitzung, z. B. die Kosten pro Streaming-Stunde, die Kosten pro Benutzer und die Kosten pro Anwendung.
- Implementieren Sie den [Cost Optimizer for WorkSpaces Applications](#), um Ihre Bauherren zu überwachen.
- Vergleichen Sie die Kosten zwischen verschiedenen Flottenarten. Vergleichen Sie zum Beispiel:
 - Lizenzkosten für Einzelsitzungen und Mehrfachsitzungen
 - Auslastungsraten der Ressourcen
 - Benutzerdichte pro Instanz
- Verwenden Sie Prozessverfolgungsdaten, um nicht ausgelastete oder unnötige Anwendungen zu identifizieren. Weitere Informationen finden Sie im AWS Blogbeitrag [Benutzerprozesse in Amazon WorkSpaces Applications-Sitzungen verfolgen](#).

Hören Sie auf, Geld für undifferenziertes Heben auszugeben

AWS verwaltet den Infrastrukturbetrieb und bietet Managed Services an, sodass sich Ihr Unternehmen auf Geschäftsziele konzentrieren kann, anstatt sich auf die IT-Wartung zu konzentrieren.

- Erstellen und verwalten Sie Anwendungsimages, indem Sie Image Builder verwenden, um Ihre Anwendungen zu verpacken, Anwendungseinstellungen zu konfigurieren und die Anwendungskompatibilität zu testen.
- Konfigurieren Sie die Flottenspezifikationen, indem Sie die entsprechenden Instance-Typen auswählen, Skalierungsschwellenwerte definieren und die gewünschten Kapazitätsgrenzen festlegen.
- Richten Sie persistente Speicheroptionen ein, indem Sie Basisordner in [Amazon S3](#) für Windows-basierte Flotten und gemeinsam genutzte Dateisysteme in [Amazon EFS](#) für Linux-basierte Flotten konfigurieren. Legen Sie Speicherberechtigungen fest und definieren Sie Aufbewahrungsrichtlinien.

Analysieren Sie Ausgaben und ordnen Sie sie zu

Die Cloud ermöglicht eine präzise Nachverfolgung des Ressourcenverbrauchs und der Kosten pro Workload, was genaue Messungen der Investitionsrendite (ROI) und gezielte Optimierungsmöglichkeiten ermöglicht.

- Implementieren Sie eine umfassende Tagging-Strategie für Flotten für die Kostenzuweisung, Bilder für die Inventarverfolgung, Image-Builder für die Zuordnung von Umgebungen und Stacks für die organisatorische Gruppierung.
- Verwenden Sie [AWS Kosten- und Nutzungsberichte \(AWS CUR\)](#), um die WorkSpaces Anwendungskosten nach markierten Ressourcen aufzuschlüsseln und die Kosten pro Flotte, Stack und Image zu analysieren.
- Wird verwendet [AWS Cost Explorer](#), um Ausgabentrends für WorkSpaces Anwendungen zu visualisieren und Kosten in verschiedenen Dimensionen wie Regionen und Instance-Typen zu vergleichen.
- Überwachen und analysieren Sie die Auslastung der Flotte, die Effizienz der Instance-Typen und die Streaming-Stunden nach Anwendung.
- Verfolgen Sie ungenutzte reservierte Kapazität, nicht ausgelastete Flotten oder Stacks sowie Leerlaufzeiten bei der Flottennutzung.
- Berechnen und verfolgen Sie die Kosten pro Benutzer für jede Anwendung, die Streaming-Stunden pro Anwendung und die Nutzerakzeptanzraten für gestreamte Anwendungen.
- Richten Sie eine detaillierte Nutzungsanalyse ein, indem Sie WorkSpaces Anwendungsnutzungsberichte konfigurieren, [Amazon Athena](#) zur Abfrage von

Nutzungsdaten verwenden und Visualisierungen in [Amazon Quick](#) erstellen, um Kosten- und Nutzungsinformationen zu erhalten.

- Bewerten Sie Überlegungen zu den Gesamtkosten wie Windows Server-Lizenzierung, Anwendungslizenzierungsmodelle und Lizenzierung pro Benutzer im Vergleich zur Lizenzierung pro Gerät.
- Verwenden Sie Amazon Athena, um die Speicherkosten und Nutzungsmuster von Basisordnern nach Benutzern abzufragen und zu analysieren. Weitere Informationen finden Sie im AWS Blogbeitrag [So melden Sie die Nutzung des Home-Ordners von Amazon WorkSpaces Applications mit Amazon Athena](#).

Säule der Nachhaltigkeit

Die [Nachhaltigkeitssäule](#) des AWS Well-Architected Framework betont die Minimierung Ihres ökologischen Fußabdrucks und die Optimierung des Energieverbrauchs und der Energieeffizienz. Es unterstützt Architekten dabei, umweltbewusste Entscheidungen in ihren Systemdesigns und Strategien zur Ressourcenzuweisung zu treffen.

Wichtige Schwerpunktbereiche für die Anwendung dieser Säule auf Ihre WorkSpaces Anwendungs-Streaming-Umgebung:

- Verständnis und Optimierung der Ressourcenzuweisung zur Deckung des tatsächlichen Bedarfs und zur Minimierung von Verschwendung in Streaming-Umgebungen
- Analyse und Anpassung an die Nutzungsmuster der Benutzer, um die Effizienz der Anwendungsbereitstellung und der Streaming-Sitzungen zu verbessern
- Auswahl und Verwendung geeigneter Hardwarekonfigurationen zur Maximierung der Energieeffizienz bei gleichzeitiger Erfüllung der Leistungsanforderungen
- Nutzung von AWS Managed-Service-Funktionen, um von den Skaleneffekten und den integrierten Effizienzfunktionen dieser Services zu profitieren

Verstehen Sie Ihre Wirkung

Überwachen und optimieren Sie die Umweltauswirkungen Ihrer Arbeitslast, indem Sie die Ressourceneffizienz und die Emissionen pro Produktionseinheit messen. Verwenden Sie diese Daten, um Nachhaltigkeitsverbesserungen zu ermitteln KPIs und zu steuern.

- Überwachen Sie die Nutzungsmuster Ihrer Flotte.
- Erfassen Sie die Streaming-Stunden pro Benutzer.
- Analysieren Sie Trends bei der Nutzung der Flottenkapazität.

Legen Sie Nachhaltigkeitsziele fest

Legen Sie für jeden Workload messbare Nachhaltigkeitsziele fest, die den Unternehmenszielen entsprechen. Konzentrieren Sie sich bei der Skalierung darauf, die Ressourcenintensität pro Transaktion zu reduzieren.

- Legen Sie Ziele für die Flottenauslastung, die Effizienz der Instance-Typen und die Optimierung der Streaming-Stunden fest.
- Planen Sie die Kapazität auf der Grundlage der tatsächlichen Nutzungsmuster.

Maximieren der Auslastung

Optimieren Sie die Workload-Effizienz, indem Sie die Ressourcen richtig dimensionieren und die Auslastung maximieren. Reduzieren Sie die ungenutzte Kapazität, um den Energieverbrauch zu minimieren und die Nachhaltigkeit zu verbessern.

- Konfigurieren Sie die automatische Skalierung entsprechend dem tatsächlichen Bedarf.
- Richtige Größe der Flottenkapazität auf der Grundlage von Nutzungsmustern.
- Implementieren Sie angemessene Mindest- und Höchstkapazitätsgrenzen.
- Wählen Sie geeignete Instance-Typen für Workloads aus.
- Überwachen und optimieren Sie die Dichte von Streaming-Sitzungen.
- Reduzieren Sie die ungenutzte Kapazität außerhalb der Spitzenzeiten.

Antizipieren und implementieren Sie neue, effizientere Hardware- und Softwareangebote

Bleiben Sie auf dem Laufenden über neue effiziente Technologien von Partnern und Lieferanten und setzen Sie diese schnell ein, um die Umweltbelastung Ihrer Workloads kontinuierlich zu verbessern.

- Verwenden Sie Instance-Typen der aktuellen Generation.
- Führen Sie ein Upgrade auf neuere Instanztypen durch, sofern verfügbar.
- Optimieren Sie die Einstellungen für das Anwendungsstreaming.
- Konfigurieren Sie die entsprechenden Streaming-Protokolle.
- Aktualisieren Sie auf die neuesten WorkSpaces Anwendungsfunktionen.

Verwendete verwaltete Dienste

Nutzen Sie gemeinsam genutzte Cloud-Dienste und verwaltete Lösungen, um die Effizienz der Ressourcennutzung zu maximieren und gleichzeitig die Umweltbelastung durch automatisierte Skalierung und Lebenszyklusmanagement zu minimieren.

- Verwenden Sie [Amazon S3](#) als Benutzerspeicher für Windows-basierte Flotten und [Amazon EFS](#) für gemeinsam genutzte Dateisysteme für Linux-basierte Flotten.
- [CloudWatch](#) Für die Überwachung implementieren.
- Konfigurieren Sie [IAM](#) für die Zugriffsverwaltung.

Reduzieren Sie die nachgelagerten Auswirkungen Ihrer Cloud-Workloads

Entwickeln Sie Services zur Minimierung der kundenseitigen Ressourcenanforderungen, zur Senkung des Energieverbrauchs und zur Verlängerung der Gerätelebensdauer für Benutzer.

- Passen Sie die maximale Sitzungsdauer an, um unnötigen Ressourcenverbrauch zu vermeiden.
- Konfigurieren Sie die entsprechenden Sitzungs-Timeouts.
- Legen Sie Richtlinien für Zeitüberschreitungen beim Trennen fest.
- Implementieren Sie bei Bedarf Richtlinien für die Persistenz von Sitzungen.

Ressourcen

AWS Dokumentation

- [AWS Well-Architected Framework](#)
- [Administratorhandbuch WorkSpaces für Amazon-Anwendungen](#)
- [CloudWatch Amazon-Benutzerhandbuch](#)
- [Amazon EFSS-Benutzerhandbuch](#)
- [Amazon S3 S3-Benutzerhandbuch](#)
- [IAM Benutzerhandbuch](#)

AWS Blog-Beiträge

- [WorkSpaces Anwendungs-Targeting auf Basis der Active Directory-Gruppenmitgliedschaft](#)
- [Erstellen Sie mit Azure AD einen einzigen Identitätsanbieter für all Ihre Amazon WorkSpaces Applications Stacks](#)
- [Konfiguration der Windows-Remoteunterstützung für Amazon WorkSpaces und WorkSpaces Amazon-Anwendungen](#)
- [Einen AS2 TrustedDomains DNS-TXT-Eintrag erstellen, um den nativen Client von Amazon WorkSpaces Applications an einen externen Identitätsanbieter umzuleiten](#)
- [Benutzerdefinierte Protokollierung und CloudWatch Amazon-Benachrichtigungen in Amazon WorkSpaces Applications erstellen](#)
- [Regionsübergreifende Umleitung mit Geo Targetly und Amazon Applications WorkSpaces](#)
- [Kontoübergreifende Ressourcen und Amazon-Anwendungen WorkSpaces](#)
- [Ermöglichen Sie den Verbund mit Bio-Key PortalGuard - und Amazon-Anwendungen WorkSpaces](#)
- [Aktivierung des Verbunds mit Simple SAMLphp - und WorkSpaces Amazon-Anwendungen](#)
- [Aktivierung des Identitätsverbunds mit Duo Single Sign-On und Amazon Applications WorkSpaces](#)
- [Aktivierung von Identity Federation mit Shibboleth- und Amazon-Anwendungen WorkSpaces](#)
- [Failover-Strategien für lokales VDI mit Amazon End User Computing](#)
- [Wie Amazon WorkSpaces Amazon-Anwendungen nutzt, um Datenwissenschaftlern und Analysten Zugriff auf sensible Daten zu gewähren](#)

- [So konfigurieren Sie die zertifikatsbasierte Authentifizierung für Amazon Applications WorkSpaces](#)
- [So verwenden Sie Okta-Claims mit Anwendungsberechtigungen für Amazon-Anwendungen WorkSpaces](#)
- [Verwaltung von Computerlabors auf WorkSpaces Amazon-Anwendungen mit Open Source Virtual Application Management](#)
- [Methoden zur Aufteilung Ihrer WorkSpaces Anwendungskosten auf Ihre Geschäftsbereiche](#)
- [Überwachung von WorkSpaces Amazon-Anwendungen mit Amazon OpenSearch Service und Amazon Kinesis Data Firehose](#)
- [Netzwerktrennung und Datenbereinigung mit Amazon WorkSpaces, Amazon WorkSpaces Applications und Amazon Macie](#)
- [OneLogin SSO mit WorkSpaces Amazon-Anwendungen](#)
- [Optimieren Sie Ihren Amazon Connect Connect-Anruf-Audiopfad mit Amazon WorkSpaces Applications](#)
- [Persistenter Speicher für Amazon WorkSpaces Applications Linux Fleets auf Amazon Elastic File System](#)
- [Eine Okta-SAML-App an den nativen Client von Amazon WorkSpaces Applications weiterleiten](#)
- [Vereinfachen Sie die Imageverwaltung von Amazon WorkSpaces Applications mit Application Masking](#)
- [Streamen Sie Anwendungen zu geringeren Kosten mit Amazon WorkSpaces Applications Elastic Fleets und Linux-Kompatibilität](#)
- [Streaming von VPC-Endpunkten mit Schnittstellen für regulierte Umgebungen mit Anwendungen WorkSpaces](#)
- [Verwenden Sie Amazon WorkSpaces Applications-Anwendungsberechtigungen mit Azure AD](#)
- [User Issue Reporter für WorkSpaces Amazon-Anwendungen](#)
- [Anwendungsberechtigungen WorkSpaces für Amazon Applications mit Google Workspace verwenden](#)
- [Auth0 mit Microsoft Active Directory auf WorkSpaces Amazon-Anwendungen verwenden](#)
- [Verwendung von Microsoft AppLocker zur Verwaltung der Anwendungserfahrung auf Amazon WorkSpaces Applications](#)
- [Verwendung von Python zur Unterstützung der Benutzeroberfläche des Linux Imaging Assistant von WorkSpaces Applications](#)
- [Optionen für die Umleitung von WorkSpaces Webanwendungen für den Applications Client](#)

Dokumentverlauf

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

Änderung	Beschreibung	Datum
Erste Veröffentlichung	—	23. Juli 2025

AWS Glossar zu präskriptiven Leitlinien

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

Zahlen

7 Rs

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

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

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

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

A

ABAC

Siehe [attributbasierte](#) Zugriffskontrolle.

abstrahierte Dienste

Siehe [Managed Services](#).

ACID

Siehe [Atomarität, Konsistenz, Isolierung und Haltbarkeit](#).

Aktiv-Aktiv-Migration

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

Aktiv-Passiv-Migration

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

Aggregatfunktion

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

AI

Siehe [künstliche Intelligenz](#).

AIOps

Siehe [Operationen im Bereich künstliche Intelligenz](#).

Anonymisierung

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

Anti-Muster

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

Anwendungssteuerung

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

Anwendungsportfolio

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

künstliche Intelligenz (KI)

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

Operationen mit künstlicher Intelligenz (AIOps)

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

Asymmetrische Verschlüsselung

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

Atomizität, Konsistenz, Isolierung, Haltbarkeit (ACID)

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

Attributbasierte Zugriffskontrolle (ABAC)

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

autoritative Datenquelle

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

Availability Zone

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

AWS Framework für die Einführung der Cloud (AWS CAF)

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

Cloud-Einführung vorzubereiten. Weitere Informationen finden Sie auf der [AWS -CAF-Webseite](#) und dem [AWS -CAF-Whitepaper](#).

AWS Workload-Qualifizierungsrahmen (AWS WQF)

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

B

schlechter Bot

Ein [Bot](#), der Einzelpersonen oder Organisationen stören oder ihnen Schaden zufügen soll.

BCP

Siehe [Planung der Geschäftskontinuität](#).

Verhaltensdiagramm

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

Big-Endian-System

Ein System, welches das höchstwertige Byte zuerst speichert. Siehe auch [Endianness](#).

Binäre Klassifikation

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

Bloom-Filter

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

Blau/Grün-Bereitstellung

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

Bot

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

Botnetz

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

branch

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

Zugang durch Glasbruch

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

Brownfield-Strategie

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

Puffer-Cache

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

Geschäftsfähigkeit

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

Planung der Geschäftskontinuität (BCP)

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

C

CAF

[Weitere Informationen finden Sie unter Framework AWS für die Cloud-Einführung.](#)

Bereitstellung auf Kanaren

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

CCoE

Weitere Informationen finden Sie [im Cloud Center of Excellence](#).

CDC

Siehe [Erfassung von Änderungsdaten](#).

Erfassung von Datenänderungen (CDC)

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

Chaos-Technik

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

CI/CD

Siehe [Continuous Integration und Continuous Delivery](#).

Klassifizierung

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

clientseitige Verschlüsselung

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

Cloud-Exzellenzzentrum (CCoE)

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

Cloud Computing

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

Cloud-Betriebsmodell

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

Phasen der Einführung der Cloud

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

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

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

CMDB

Siehe [Datenbank für das Konfigurationsmanagement](#).

Code-Repository

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

Kalter Cache

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

Kalte Daten

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

Computer Vision (CV)

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

Drift in der Konfiguration

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

Verwaltung der Datenbankkonfiguration (CMDB)

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

Konformitätspaket

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

Kontinuierliche Bereitstellung und kontinuierliche Integration (CI/CD)

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

CV

Siehe [Computer Vision](#).

D

Daten im Ruhezustand

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

Datenklassifizierung

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

Datendrift

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

Daten während der Übertragung

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

Datennetz

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

Datenminimierung

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

Datenperimeter

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

Vorverarbeitung der Daten

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

Herkunft der Daten

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

betreffene Person

Eine Person, deren Daten gesammelt und verarbeitet werden.

Data Warehouse

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

Datenbankdefinitionssprache (DDL)

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

Datenbankmanipulationssprache (DML)

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

DDL

Siehe [Datenbankdefinitionssprache](#).

Deep-Ensemble

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

Deep Learning

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

defense-in-depth

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

delegierter Administrator

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

Einsatz

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

Entwicklungsumgebung

Siehe [Umgebung](#).

Detektivische Kontrolle

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

Abbildung des Wertstroms in der Entwicklung (DVSM)

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

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

digitaler Zwilling

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

Maßtabelle

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

Katastrophe

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

Notfallwiederherstellung (DR)

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

DML

Siehe Sprache zur [Datenbankmanipulation](#).

Domainorientiertes Design

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

DR

Siehe [Disaster Recovery](#).

Erkennung von Driften

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

DVSM

Siehe [Abbildung des Wertstroms in der Entwicklung](#).

E

EDA

Siehe [explorative Datenanalyse](#).

EDI

Siehe [elektronischer Datenaustausch](#).

Edge-Computing

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

elektronischer Datenaustausch (EDI)

Der automatisierte Austausch von Geschäftsdokumenten zwischen Organisationen. Weitere Informationen finden Sie unter [Was ist elektronischer Datenaustausch](#).

Verschlüsselung

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

Verschlüsselungsschlüssel

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

Endianismus

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

Endpunkt

[Siehe](#) Service-Endpunkt.

Endpunkt-Services

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

Unternehmensressourcenplanung (ERP)

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

Envelope-Verschlüsselung

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

Umgebung

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

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

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

Epics

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

ERP

Siehe [Enterprise Resource Planning](#).

Explorative Datenanalyse (EDA)

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

F

Faktentabelle

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

schnell scheitern

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

Grenze zur Fehlerisolierung

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

Feature-Zweig

Siehe [Zweig](#).

Features

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

Bedeutung der Feature

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

Featuretransformation

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

Eingabeaufforderung mit wenigen Klicks

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

FGAC

Siehe [detaillierte Zugriffskontrolle](#).

Feinkörnige Zugriffskontrolle (FGAC)

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

Flash-Cut-Migration

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

FM

Siehe [Fundamentmodell](#).

Fundamentmodell (FM)

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

G

Generative KI

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

Geoblocking

Siehe [geografische Einschränkungen](#).

Geografische Einschränkungen (Geoblocking)

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

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

Gitflow-Workflow

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

goldenes Bild

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

Greenfield-Strategie

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

Integritätsschutz

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

H

HEKTAR

Siehe [Hochverfügbarkeit](#).

Heterogene Datenbankmigration

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

hohe Verfügbarkeit (HA)

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

historische Modernisierung

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

Daten zurückhalten

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

Homogene Datenbankmigration

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

heiße Daten

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

Hotfix

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

Hypercare-Phase

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

I

IaC

Sehen Sie [Infrastruktur als Code](#).

Identitätsbasierte Richtlinie

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

Leerlaufanwendung

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

IIoT

Siehe [Industrielles Internet der Dinge](#).

unveränderliche Infrastruktur

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

Eingehende (ingress) VPC

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

Inkrementelle Migration

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

Industrie 4.0

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

Infrastruktur

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

Infrastructure as Code (IaC)

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

industrielles Internet der Dinge (T) Ilo

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

Inspektions-VPC

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

Internet of Things (IoT)

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

Interpretierbarkeit

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

IoT

Siehe [Internet der Dinge](#).

IT information library (ITIL, IT-Informationsbibliothek)

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

T service management (ITSM, IT-Service-Management)

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-Service-Management](#).

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 Infrastrukturmgebung starten und bereitstellen können. Weitere Informationen zu Landing Zones finden Sie unter [Einrichtung einer sicheren und skalierbaren AWS -Umgebung mit mehreren Konten..](#)

großes Sprachmodell (LLM)

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

Große Migration

Eine Migration von 300 oder mehr Servern.

SCHWARZ

Siehe [Labelbasierte Zugriffskontrolle](#).

Geringste Berechtigung

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

Lift and Shift

Siehe [7 Rs](#).

Little-Endian-System

Ein System, welches das niedrigwertigste Byte zuerst speichert. Siehe auch [Endianness](#).

LLM

Siehe [großes Sprachmodell](#).

Niedrigere Umgebungen

Siehe [Umgebung](#).

M

Machine Learning (ML)

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

Hauptzweig

Siehe [Filiale](#).

Malware

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

verwaltete Dienste

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

Manufacturing Execution System (MES)

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

MAP

Siehe [Migration Acceleration Program](#).

Mechanismus

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

Mitgliedskonto

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

MES

Siehe [Manufacturing Execution System](#).

Message Queuing-Telemetrietransport (MQTT)

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

Microservice

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

Microservices-Architekturen

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

Migration Acceleration Program (MAP)

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

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

Migration in großem Maßstab

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

Migrationsfabrik

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

Migrationsmetadaten

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

Migrationsmuster

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

Migration Portfolio Assessment (MPA)

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

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

Migration Readiness Assessment (MRA)

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

Migrationsstrategie

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

ML

[Siehe maschinelles Lernen.](#)

Modernisierung

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

Bewertung der Modernisierungsfähigkeit

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

Monolithische Anwendungen (Monolithen)

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

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

MPA

Siehe [Bewertung des Migrationsportfolios](#).

MQTT

Siehe [Message Queuing-Telemetrietransport](#).

Mehrklassen-Klassifizierung

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

veränderbare Infrastruktur

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

O

OAC

Siehe [Origin Access Control](#).

EICHE

Siehe [Zugriffsidentität von Origin](#).

COM

Siehe [organisatorisches Change-Management](#).

Offline-Migration

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

OI

Siehe [Betriebsintegration](#).

OLA

Siehe Vereinbarung auf [operativer Ebene](#).

Online-Migration

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

OPC-UA

Siehe [Open Process Communications — Unified Architecture](#).

Offene Prozesskommunikation — Einheitliche Architektur (OPC-UA)

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

Vereinbarung auf Betriebsebene (OLA)

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

Überprüfung der Betriebsbereitschaft (ORR)

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

Betriebstechnologie (OT)

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

Betriebsintegration (OI)

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

Organisationspfad

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

Organisatorisches Veränderungsmanagement (OCM)

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

Ursprungszugriffskontrolle (OAC)

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

Ursprungszugriffsidentität (OAI)

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

ORR

Weitere Informationen finden Sie unter [Überprüfung der Betriebsbereitschaft](#).

NICHT

Siehe [Betriebstechnologie](#).

Ausgehende (egress) VPC

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

P

Berechtigungsgrenze

Eine IAM-Verwaltungsrichtlinie, die den IAM-Prinzipalen zugeordnet ist, um die maximalen Berechtigungen festzulegen, die der Benutzer oder die Rolle haben kann. Weitere Informationen finden Sie unter [Berechtigungsgrenzen](#) für IAM-Entitäts 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 definiert (siehe [identitätsbasierte Richtlinie](#)), Zugriffsbedingungen spezifiziert (siehe [ressourcenbasierte Richtlinie](#)) oder die maximalen Berechtigungen für alle Konten in einer Organisation definiert kann AWS Organizations (siehe [Dienststeuerungsrichtlinie](#)).

Polyglotte Beharrlichkeit

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

Portfoliobewertung

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

predicate

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

Prädikat Pushdown

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

Präventive Kontrolle

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

Prinzipal

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

Datenschutz von Natur aus

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

Privat gehostete Zonen

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

proaktive Steuerung

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

Produktlebenszyklusmanagement (PLM)

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

Produktionsumgebung

Siehe [Umgebung](#).

Speicherprogrammierbare Steuerung (SPS)

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

schnelle Verkettung

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

Pseudonymisierung

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

publish/subscribe (pub/sub)

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

Q

Abfrageplan

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

Abfrageplanregression

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

R

RACI-Matrix

Siehe [verantwortlich, rechenschaftspflichtig, konsultiert, informiert \(RACI\)](#).

RAG

Siehe Erweiterte [Generierung beim Abrufen](#).

Ransomware

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

RASCI-Matrix

Siehe [verantwortlich, rechenschaftspflichtig, konsultiert, informiert \(RACI\)](#).

RCAC

Siehe [Zugriffskontrolle für Zeilen und Spalten](#).

Read Replica

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

neu strukturieren

Siehe [7 Rs](#).

Recovery Point Objective (RPO)

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

Wiederherstellungszeitziel (RTO)

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

Refaktorisierung

Siehe [7 Rs](#).

Region

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

Regression

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

rehosten

Siehe [7 Rs.](#)

Veröffentlichung

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

umziehen

Siehe [7 Rs.](#)

neue Plattform

Siehe [7 Rs.](#)

Rückkauf

Siehe [7 Rs.](#)

Ausfallsicherheit

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

Ressourcenbasierte Richtlinie

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

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

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

Reaktive Kontrolle

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

Beibehaltung

Siehe [7 Rs](#).

zurückziehen

Siehe [7 Rs](#).

Retrieval Augmented Generation (RAG)

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

Drehung

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

Zugriffskontrolle für Zeilen und Spalten (RCAC)

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

RPO

Siehe [Recovery Point Objective](#).

RTO

Siehe [Ziel für die Erholungszeit](#).

Runbook

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

S

SAML 2.0

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

SCADA

Siehe [Aufsichtskontrolle und Datenerfassung](#).

SCP

Siehe [Richtlinie zur Dienstkontrolle](#).

Secret

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

Sicherheit durch Design

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

Sicherheitskontrolle

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

Härtung der Sicherheit

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

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

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

Automatisierung von Sicherheitsreaktionen

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

Serverseitige Verschlüsselung

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

Service-Kontrollrichtlinie (SCP)

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

Service-Endpoint

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

Service Level Agreement (SLA)

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

Service-Level-Indikator (SLI)

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

Service-Level-Ziel (SLO)

Eine Zielkennzahl, die den Zustand eines Dienstes darstellt, gemessen anhand eines [Service-Level-Indikators](#).

Modell der geteilten Verantwortung

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

SIEM

Siehe [Sicherheitsinformations- und Event-Management-System](#).

Single Point of Failure (SPOF)

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

SLA

Siehe [Service Level Agreement](#).

SLI

Siehe [Service-Level-Indikator](#).

ALSO

Siehe [Service-Level-Ziel](#).

split-and-seed Modell

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

SPOTTEN

Siehe [Single Point of Failure](#).

Sternschema

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

Strangler-Fig-Muster

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

Subnetz

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

Aufsichtskontrolle und Datenerfassung (SCADA)

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

Symmetrische Verschlüsselung

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

synthetisches Testen

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

Systemaufforderung

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

T

tags

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

Zielvariable

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

Aufgabenliste

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

Testumgebungen

[Siehe Umgebung.](#)

Training

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

Transit-Gateway

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

Stammbasierter Workflow

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

Vertrauenswürdiger Zugriff

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

Optimieren

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

Zwei-Pizzen-Team

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

U

Unsicherheit

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

undifferenzierte Aufgaben

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

höhere Umgebungen

Siehe [Umgebung](#).

V

Vacuuming

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

Versionskontrolle

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

VPC-Peering

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

Schwachstelle

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

W

Warmer Cache

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

warme Daten

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

Fensterfunktion

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

Workload

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

Workstream

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

WURM

Sehen [Sie einmal schreiben, viele lesen](#).

WQF

Siehe [AWS Workload-Qualifizierungsrahmen](#).

einmal schreiben, viele lesen (WORM)

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

Z

Zero-Day-Exploit

Ein Angriff, in der Regel Malware, der eine [Zero-Day-Sicherheitslücke](#) ausnutzt.

Zero-Day-Sicherheitslücke

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

Eingabeaufforderung ohne Zwischenfälle

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

Zombie-Anwendung

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

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