



Migration zu Amazon Service OpenSearch

# AWS Präskriptive Leitlinien



# AWS Präskriptive Leitlinien: Migration zu Amazon Service OpenSearch

Copyright © 2024 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 irregeführt 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
Übersicht .....	1
Vorteile von OpenSearch Bedienung .....	3
Einfachere Bereitstellung und Verwaltung .....	3
Kosteneffektiv .....	3
Skalierbarer und zuverlässiger .....	4
Sicher und konform .....	4
Migrationsreise .....	5
Planung .....	6
Größe .....	6
Speicher .....	7
Anzahl der Knoten und Instance-Typen .....	8
Bestimmung der Indizierungsstrategie und der Shard-Anzahl .....	9
CPU-Auslastung .....	9
Instance-Typen .....	10
Funktionalität .....	11
Aktuelle Lösungsfunktionalität .....	11
Amazon OpenSearch -Service-Funktionalität .....	11
Verpackte Plugins .....	12
Benutzerdefinierte Plugins .....	12
Versionsabhängigkeiten .....	13
Auswählen der Engine-Version .....	13
Upgrade auf die neueste OpenSearch Serviceversion .....	13
Upgrade-Strategie für Versionen .....	14
Prüfungen vor dem Upgrade .....	14
KPIs und Geschäftskontinuität .....	15
Betriebliche Leistung .....	16
Prozessleistung .....	17
Der reibungslose Übergang zu neuen Services .....	17
Finanzmetriken .....	17
Betrieb und Sicherheit .....	18
Runbooks und neue Prozesse .....	19
Support- und Ticketing-System .....	19
Sicherheit .....	19

Training .....	20
Trainingsoptionen .....	21
Datenfluss .....	22
Datenerfassung .....	22
Datenaufbewahrung .....	23
Ansätze zur Datenmigration .....	24
Bereitstellungs-Frameworks .....	26
Machbarkeitsnachweis .....	28
Definieren von Ein- und Ausstiegsriterien .....	28
Sicherung der Finanzierung .....	29
Automatisieren .....	29
Ausführliche Tests .....	29
PoC-Phasen .....	30
Simulation von Fehlern .....	31
Bereitstellung .....	32
Datenmigration .....	33
Aus einem Snapshot erstellen .....	33
Überlegungen zu Snapshots .....	34
Aus der Quelle bauen .....	35
Neuindizierung aus der Ferne .....	36
Verwenden Sie Logstash .....	37
Übernahme .....	38
Datensynchronisierung .....	38
Tauschen oder überschneiden .....	42
Operative Exzellenz .....	43
Schlussfolgerung .....	44
Ressourcen .....	45
Beitragende Faktoren .....	46
Dokumentverlauf .....	47
Glossar .....	48
# .....	48
A .....	49
B .....	52
C .....	54
D .....	57
E .....	62

---

F .....	64
G .....	65
H .....	66
I .....	67
L .....	70
M .....	71
O .....	75
P .....	78
Q .....	81
R .....	81
S .....	84
T .....	88
U .....	90
V .....	90
W .....	91
Z .....	92
.....	xciii

# Migration zu Amazon Service OpenSearch

Amazon Web Services ([Mitwirkende](#))

August 2023 ([Dokumentverlauf](#))

Für viele Kunden ist die Migration von selbstverwaltetem Elasticsearch oder OpenSearch Deployments zu [Amazon OpenSearch](#) Service eine Herausforderung. Die häufigsten Herausforderungen betreffen die Bewertung der Arbeitslast, die Kapazitätsplanung und die Architekturoptimierung. Es gibt auch Fragen dazu, wie alle Anforderungen von Betriebsanalyseanwendungen aus lokalen Rechenzentren in der Amazon Web Services (AWS) Cloud erfüllt werden können. Dieser Leitfaden behandelt den gesamten Prozess einer Migration zu Amazon OpenSearch Service und bietet bewährte Methoden, die AWS Experten im Laufe der Zeit gesammelt haben. Die step-by-step Anweisungen können Ihnen dabei helfen, Ihre Migrationen effektiv und effizient durchzuführen. Dieses Handbuch behandelt hauptsächlich von Amazon OpenSearch Service bereitgestellte Domains und nicht Amazon OpenSearch Serverless-Sammlungen.

## Übersicht

[OpenSearch](#) ist eine verteilte Open-Source-Such- und Analysesuite, die für eine Vielzahl von Anwendungsfällen im Bereich Betriebsanalysen eingesetzt wird, z. B. Anwendungsüberwachung in Echtzeit, Protokollanalysen, Datenbeobachtbarkeit und Suche nach Anwendungs- und Produktkatalogen. OpenSearch bietet eine Suchantwort mit niedriger Latenz. Mit einem integrierten Open-Source-Datenvisualisierungstool namens OpenSearch Dashboards bietet es auch schnellen Zugriff auf große Datenmengen.

Amazon OpenSearch Service unterstützt die Durchführung interaktiver Protokollanalysen, Anwendungsüberwachung in Echtzeit, Webseitensuche und mehr. Amazon OpenSearch Service bietet die neuesten Versionen von OpenSearch und Support für 19 Versionen von Elasticsearch (Versionen 1.5—7.10). Es bietet auch Visualisierungsfunktionen, die auf OpenSearch Dashboards und Kibana (Versionen 1.5—7.10) basieren. Amazon OpenSearch Service hat derzeit Zehntausende von aktiven Kunden mit Hunderttausenden von Clustern, die Hunderte von Billionen von Anfragen pro Monat verarbeiten.

Die Verwaltung von OpenSearch Elasticsearch-Clustern vor Ort oder in der Cloud-Infrastruktur ist hochkomplex, teuer und mühsam. Um diese Cluster ausführen zu können, müssen Sie die Infrastruktur bereitstellen und warten. Die Bemühungen umfassen Folgendes:

- Beschaffung und Einrichtung von Hardware
- Installation der Software
- Konfiguration, Patchen und Aktualisieren
- Überlegungen zur Zuverlässigkeit und Verfügbarkeit
- Überlegungen zu Leistung und Skalierbarkeit
- Sicherheits- und Compliance-Überlegungen, wie Netzwerkisolierung, differenzierte Zugriffskontrolle, Verschlüsselungen und Compliance-Programme wie die folgenden:
  - Föderales Risiko- und Autorisierungsmanagementprogramm (FedRAMP)
  - Datenschutz-Grundverordnung (DSGVO)
  - Health Insurance Portability and Accountability Act (HIPAA)
  - International Organization for Standardization (ISO)
  - Payment Card Industry Data Security Standard (PCI DSS)
  - System- und Organisationskontrollen (SOC).

Im Vergleich dazu erledigt Amazon OpenSearch Service diese Aufgaben für Sie. In diesem Leitfaden lernen Sie Ansätze und bewährte Methoden für die Migration von Elasticsearch vor Ort oder selbstverwaltetem Elasticsearch oder OpenSearch zum vollständig verwalteten Amazon Service kennen. OpenSearch

# Vorteile der Migration zu Amazon OpenSearch Service

Amazon OpenSearch Der Service hilft bei der Bereitstellung und bei laufenden Verwaltungsaufgaben. Er ist kostengünstig und bietet Skalierbarkeit, wodurch die Zuverlässigkeit verbessert wird. Es bietet auch Sicherheit und unterstützt Ihre Compliance-Anforderungen.

## Einfachere Bereitstellung und Verwaltung

Es ist einfacher, ein zu implementieren OpenSearch mithilfe von Amazon clustern OpenSearchService als wenn Sie selbst einen Cluster bereitstellen. Amazon OpenSearch Service hilft bei der Verwaltung von Aufgaben wie Hardwarebereitstellung, Softwareinstallation und -patching, Fehlerbehebung, Backups und Überwachung. Sie benötigen kein engagiertes Team von OpenSearch Experten für die Verwaltung Ihrer Cluster.

Ein OpenSearch Cluster bei Amazon OpenSearch Der Service wird auch als Domain bezeichnet. Amazon OpenSearch Der Service bietet die Überwachung des Domainzustands über Amazon CloudWatchService. Sie können Benachrichtigungen einrichten, um über Änderungen des Zustands Ihrer Domains informiert zu werden. Der AWS-Support bietet one-on-one technischer Support durch erfahrene Techniker. Kunden mit betrieblichen Problemen oder technischen Fragen können sich an den AWS-Support wenden und erhalten persönlichen Support mit zuverlässigen Reaktionszeiten.

## Kosteneffektiv

Amazon OpenSearch Der Service ist kostengünstig. Er bietet eine breite Palette erweiterter Funktionen, ohne dass zusätzliche Lizenzgebühren anfallen. Sie können Funktionen wie Sicherheit auf Unternehmensebene, Warnmeldungen in Echtzeit, clusterübergreifende Suche, automatisiertes Indexmanagement und Anomalieerkennung ohne zusätzliche Kosten nutzen. Für Datenübertragungen zwischen Availability Zones fallen keine Gebühren an, und stündliche Snapshots werden ohne zusätzliche Kosten bereitgestellt.

MitUltraWarm, können Sie interaktive Analysen für bis zu drei Petabyte an Protokolldaten durchführen und gleichzeitig die Kosten pro GB im Vergleich zur Hot-Storage-Stufe um bis zu 90 Prozent senken. Darüber hinaus Amazon OpenSearch Service bietet Reserved Instances an, die im Vergleich zu den Standard-On-Demand-Instances erhebliche Rabatte bieten. Weitere Informationen finden Sie unter [Kostenbewusst](#).

## Skalierbarer und zuverlässiger

Mit Amazon OpenSearch Service, Sie können Petabyte an Daten in einer einzigen Domain speichern. Sie können Daten über mehrere Domänen hinweg abfragen und all Ihre Daten in einer einzigen analysieren OpenSearch Dashboard-Oberfläche. Amazon OpenSearch Service ist auf höchste Zuverlässigkeit ausgelegt und verwendet Multi-Availability Zone (Multi-AZ) -Bereitstellungen, sodass Sie Daten zwischen bis zu drei Availability Zones in derselben AWS-Region replizieren können. Es gibt keine Ausfallzeiten, wenn Sie Software-Updates und Upgrades durchführen oder Ihre Umgebung skalieren.

Mit der Multi-AZ-Funktion mit Standby-Funktion OpenSearch Servicedomänen sind widerstandsfähig gegenüber potenziellen Infrastrukturausfällen, z. B. einem Knoten- oder Availability Zone-Ausfall. Dies ermöglicht eine Verfügbarkeit von 99,99 Prozent und eine konsistente Leistung für geschäftskritische Workloads. Mit Multi-AZ mit Standby sind Cluster widerstandsfähig gegenüber Infrastrukturausfällen wie Hardware- oder Netzwerkausfällen. Diese Option bietet eine verbesserte Zuverlässigkeit und den zusätzlichen Vorteil einer Vereinfachung der Clusterkonfiguration und -verwaltung, indem bewährte Verfahren durchgesetzt und die Komplexität reduziert werden.

## Sicher und konform

Amazon OpenSearch Der Service kümmert sich um alle Sicherheitspatches. Darüber hinaus bietet er Netzwerkisolierung durch eine Virtual Private Cloud (VPC), eine differenzierte Zugriffskontrolle und mehrere Mandanten OpenSearch Unterstützung für Dashboards. Sie können Ihre Daten im Ruhezustand und bei der Übertragung verschlüsseln. Um Sie bei der Erfüllung branchenspezifischer und regulatorischer Anforderungen zu unterstützen, hat Amazon OpenSearch Der Service ist HIPAA-fähig und entspricht den folgenden Standards:

- FedRAMP
- DSGVO
- PCI-DSS
- ISO
- SOC

Weitere Informationen finden Sie in der [Amazon OpenSearch Servicedokumentation](#).

# Migrationsreise

Abhängig von Ihrer aktuellen Bereitstellung, Migration zu einem Amazon OpenSearch Service kann ein einfaches oder komplexes Verfahren mit mehreren Schritten sein. In den folgenden Abschnitten werden Sie die Migrationsansätze und die wichtigsten Überlegungen zu jedem Schritt des Prozesses untersuchen. Dies beinhaltet die Best Practices, die auf unserer Erfahrung basieren, mit der wir vielen AWS-Kunden bei der Migration von bestehenden Tools zu Amazon OpenSearch Service geholfen haben. In diesem Abschnitt wird auch erörtert, was eine effektive Migrationsstrategie ausmacht.

Eine typische Migrationsreise umfasst fünf Phasen:

1. Planung
2. Machbarkeitsnachweis (PoC)
3. Bereitstellung
4. Datenmigration
5. Umstellung

Möglicherweise migrieren Sie von einem selbstverwalteten Elasticsearch oder OpenSearch Cluster oder Sie migrieren möglicherweise von einer anderen Technologie zu Amazon OpenSearch Service. In den meisten Fällen bleiben die Schritte gleich. Die Zeit, die Sie für jeden Schritt aufwenden, hängt von der Komplexität Ihrer Umgebung ab.

Die Migration beginnt mit einer sorgfältigen Planung, gefolgt von einer PoC-Übung, um sicherzustellen, dass die Zielumgebung Ihren Kosten-, Sicherheits-, Leistungs- und Migrationszielen entspricht. Auf die PoC-Aktivität folgt die Bereitstellung der Zielumgebung und die Migration der Daten in diese Umgebung. Wenn Sie bestätigt haben, dass Ihre Daten zwischen der aktuellen Umgebung und der neuen Umgebung synchronisiert sind, können Sie zur neuen Umgebung wechseln. Nach der Umstellung führen Sie den Betrieb der Umgebung gemäß den bewährten Betriebsmethoden durch. In den folgenden Abschnitten werden die einzelnen Phasen ausführlich behandelt.

# Phase 1 – Planung

Die Migration beginnt mit der Planung der Zielumgebung, die Sie erstellen werden, um Ihre Anforderungen zu erfüllen. Bei der Planung müssen Sie sich eine Reihe von Schwerpunktbereichen ansehen, von denen jeder eine sorgfältige Überlegung erfordert:

- [Größe](#)
- [Funktionalität](#)
- [Versionsabhängigkeiten](#)
- [Wichtige Leistungsindikatoren \(KPIs\) und Geschäftskontinuität](#)
- [Betrieb und Sicherheit](#)
- [Schulung](#)
- [Datenfluss](#)
- [Bereitstellungs-Frameworks](#)

Diese Schwerpunktbereiche helfen Ihnen dabei, Entscheidungen zu treffen, die die Migrationsstrategie bilden. Sie helfen Ihnen auch dabei, Ihre Migrationsziele zu erreichen, indem sie die Komplexität und Kosten der Migration reduzieren.

Während der Planungsphase ist es auch wichtig, Ihre aktuelle Umgebung zu bewerten und Probleme zu identifizieren, die Sie im Rahmen dieser Migration angehen möchten. Diese Problempunkte können sich auf Leistung, Sicherheit, Zuverlässigkeit, Bereitstellungsgeschwindigkeit, Kosten oder Betriebsfreundlichkeit beziehen. Überlegen Sie sich bei der Überprüfung der Schwerpunktbereiche, welche Verbesserungen Sie im Rahmen der Migration vornehmen können.

## Größe

Die Größe hilft Ihnen dabei, den richtigen Instance-Typ, die Anzahl der Datenknoten und die Speicheranforderungen für Ihre Zielumgebung zu ermitteln. Wir empfehlen Ihnen, zuerst nach dem Speicher und dann nach CPUs zu dimensionieren. Wenn Sie Elasticsearch oder bereits verwenden OpenSearch, bleibt die Größe im Allgemeinen gleich. Sie müssen jedoch den Instance-Typ identifizieren, der Ihrer aktuellen Umgebung entspricht. Um die richtige Größe zu ermitteln, empfehlen wir die folgenden Richtlinien.

## Speicher

Die Dimensionierung Ihres Clusters beginnt mit der Definition der Speicheranforderungen. Identifizieren Sie den Rohspeicher, den Sie für Ihren Cluster benötigen. Dies wird durch Bewertung der von Ihrem Quellsystem generierten Daten (z. B. Server, die Protokolle generieren, oder Rohgröße des Produktkatalogs) bestimmt. Nachdem Sie ermittelt haben, wie viele Rohdaten Sie haben, verwenden Sie die folgende Formel, um den Speicherbedarf zu berechnen. Sie können das Ergebnis dann als Ausgangspunkt für Ihr PoC verwenden.

$$\text{storage needed} = (\text{daily source data in bytes} \times 1.45) (\text{number\_of\_replicas} + 1) \times \text{number of days retained}$$

Die Formel berücksichtigt Folgendes:

- Die Größe eines Index auf der Festplatte variiert, ist aber oft 10 Prozent größer als die Quelldaten.
- Der Betriebssystem-Overhead von 5 Prozent wird von Linux für die Systemwiederherstellung und zum Schutz vor Problemen mit der Festplattendefragmentierung reserviert.
- OpenSearch reserviert 20 Prozent des Speicherplatzes jeder Instance für Segmentzusammenführungen, Protokolle und andere interne Operationen.
- Wir empfehlen, 10 Prozent zusätzlichen Speicher beizubehalten, um die Auswirkungen von Knotenausfällen und Ausfällen der Availability Zone zu minimieren.

Zusammengenommen benötigen diese Overheads und Reservierungen 45 Prozent zusätzlichen Speicherplatz basierend auf den tatsächlichen Rohdaten in der Quelle. Daher multiplizieren Sie die Quelldaten mit 1,45. Als Nächstes multiplizieren Sie dies mit der Anzahl der Datenkopien (z. B. ein primäres plus die Anzahl der Replikate, die Sie verwenden werden). Die Anzahl der Replikate hängt von Ihrer Ausfallsicherheit und Ihrem Durchsatz ab. Für einen durchschnittlichen Anwendungsfall beginnen Sie mit einem primären und einem Replikat. Zum Schluss multiplizieren Sie mit der Anzahl der Tage, für die Sie Daten in einer Hot-Storage-Stufe aufbewahren möchten.

Amazon OpenSearch Service bietet Hot-, Warm- und Cold-Speicherstufen. Die Warm-Speicherstufe verwendet UltraWarm -Speicher. UltraWarm bietet eine kostengünstige Möglichkeit, große Mengen an schreibgeschützten Daten auf Amazon OpenSearch Service zu speichern. Standarddatenknoten verwenden Hot Storage, der in Form von Instance-Speichern oder Amazon Elastic Block Store (Amazon EBS)-Volumes an jeden Knoten angefügt ist. Hot Storage bietet die schnellstmögliche Leistung für die Indizierung und die Suche nach neuen Daten. UltraWarm -Knoten verwenden Amazon Simple Storage Service (Amazon S3) als Speicher und eine ausgeklügelte Caching-Lösung

zur Verbesserung der Leistung. Für Indizes, in die Sie nicht aktiv schreiben oder die Sie weniger häufig abfragen und die nicht die gleichen Leistungsanforderungen haben, UltraWarm bietet deutlich niedrigere Kosten pro GiB Daten. Weitere Informationen zu finden Sie UltraWarm in der [AWS-Dokumentation](#).

Wenn Sie eine - OpenSearch Service-Domain erstellen und Hot Storage verwenden, müssen Sie möglicherweise die EBS-Volume-Größe definieren. Dies hängt von Ihrer Wahl des Instance-Typs für die Datenknoten ab. Sie können dieselbe Speicheranforderungsformel verwenden, um die Volume-Größe für Amazon-EBS-gestützte Instances zu bestimmen. Wir empfehlen die Verwendung von gp3-Volumes für die Instance-Familien T3, R5, R6G, M5, M5g, C5 und C6g der neuesten Generation. Mit Amazon-EBS-gp3-Volumes können Sie unabhängig von der Speicherkapazität Leistung bereitstellen. Amazon-EBS-gp3-Volumes bieten auch eine bessere Basisleistung zu 9,6 Prozent niedrigeren Kosten pro GB als vorhandene gp2-Volumes auf OpenSearch Service. Mit gp3 erhalten Sie auch dichteren Speicher für die Instance-Familien R5, R6g, M5 und M6g, was Ihnen helfen kann, Ihre Kosten weiter zu optimieren. Sie können EBS-Volumes bis zum unterstützten Kontingent erstellen. Weitere Informationen zu Kontingenten finden Sie unter [Amazon- OpenSearch Service-Kontingente](#).

Für Datenknoten mit NVM Express (NVMe)-Laufwerken wie i3- und r6gd-Instances ist die Volume-Größe festgelegt, sodass EBS-Volumes keine Option sind.

## Anzahl der Knoten und Instance-Typen

Die Anzahl der Knoten basiert auf der Anzahl der CPUs, die für den Betrieb Ihrer Workload erforderlich sind. Die Anzahl der CPUs basiert auf der Shard-Anzahl. Ein Index in OpenSearch besteht aus mehreren Shards. Wenn Sie einen Index erstellen, geben Sie die Anzahl der Shards für den Index an. Daher müssen Sie Folgendes tun:

1. Berechnen Sie die Gesamtzahl der Shards, die Sie in der Domain speichern möchten.
2. Bestimmen Sie die CPU.
3. Finden Sie den kostengünstigsten Knotentyp und die kostengünstigste Knotenanzahl, die Ihnen die erforderliche Anzahl an CPUs und Speicher bietet.

Dies ist normalerweise ein Ausgangspunkt. Führen Sie Tests durch, um festzustellen, ob die Schätzgröße Ihren funktionalen und nicht funktionalen Anforderungen entspricht.

## Bestimmung der Indizierungsstrategie und der Shard-Anzahl

Nachdem Sie die Speicheranforderungen kennen, können Sie entscheiden, wie viele Indizes Sie benötigen, und die Shard-Anzahl für jeden Index ermitteln. Im Allgemeinen verfügen Suchanwendungsfälle über einen oder einige Indizes, die jeweils eine durchsuchbare Entität oder einen Katalog darstellen. Für Anwendungsfälle für Protokollanalysen kann ein Index eine tägliche oder wöchentliche Protokolldatei darstellen. Nachdem Sie entschieden haben, wie viele Indizes Sie haben, beginnen Sie mit den folgenden Anleitungen zur Skalierung und bestimmen Sie die entsprechende Shard-Anzahl:

- Suchanwendungsfälle – 10–30 GB/Shard
- Anwendungsfälle für Protokollanalysen – 50 GB/Shard

Sie können das Gesamtdatenvolumen in einem einzigen Index durch die Shard-Größe teilen, die Sie in Ihrem Anwendungsfall anstreben. Dadurch erhalten Sie die Anzahl der Shards für den Index. Die Ermittlung der Gesamtzahl der Shards hilft Ihnen dabei, die richtigen Instance-Typen zu finden, die Ihrem Workload entsprechen. Die Shards sollten nicht zu groß oder zu zahlreich sein. Große Shards können es erschweren, sich nach einem Fehler OpenSearch zu erholen, aber da jeder Shard eine gewisse Menge an CPU und Arbeitsspeicher verwendet, kann die Verwendung zu vieler kleiner Shards zu Leistungsproblemen und out-of-memory Fehlern führen. Darüber hinaus kann ein Ungleichgewicht bei der Shard-Zuweisung zu Datenknoten zu Verzerrungen führen. Wenn Sie Indizes mit mehreren Shards haben, versuchen Sie, die Anzahl der Shards auf ein gerades Vielfaches der Anzahl der Datenknoten einzustellen. Dies sorgt dafür, dass Shards gleichmäßig über Datenknoten verteilt sind, und verhindert heiße Knoten. Wenn Sie beispielsweise 12 primäre Shards haben, sollte Ihre Datenknotenanzahl 2, 3, 4, 6 oder 12 betragen. Die Shard-Anzahl ist jedoch zweitrangig gegenüber der Shard-Größe; Wenn Sie über 5 GiB an Daten verfügen, sollten Sie dennoch einen einzelnen Shard verwenden. Das gleichmäßige Ausgleichen der Anzahl der Replikat-Shards in der gesamten Availability Zone trägt auch zur Verbesserung der Ausfallsicherheit bei.

## CPU-Auslastung

Der nächste Schritt besteht darin, zu ermitteln, wie viele CPUs Sie für Ihre Workload benötigen. Wir empfehlen, mit einer CPU-Anzahl zu beginnen, die das 1,5-fache Ihrer aktiven Shards ist. Ein aktiver Shard ist jeder Shard für einen Index, der erhebliche Schreibvorgänge erhält. Verwenden Sie die primäre Shard-Anzahl, um aktive Shards für Indizes zu ermitteln, die erhebliche Lese- oder Schreibforderungen erhalten. Für Protokollanalysen ist im Allgemeinen nur der aktuelle Index aktiv. Bei Suchanwendungsfällen werden alle primären Shards als aktive Shards betrachtet. Obwohl

wir 1,5 CPU pro aktivem Shard empfehlen, ist dies stark von der Workload abhängig. Testen und überwachen Sie unbedingt die CPU-Auslastung und skalieren Sie entsprechend.

Eine bewährte Methode für die Aufrechterhaltung Ihrer CPU-Auslastung besteht darin, sicherzustellen, dass die OpenSearch Service-Domain über genügend Ressourcen verfügt, um ihre Aufgaben auszuführen. Ein Cluster mit konstant hoher CPU-Auslastung kann die Clusterstabilität beeinträchtigen. Wenn Ihr Cluster überlastet ist, blockiert OpenSearch Service eingehende Anfragen, was zu Ablehnungen von Anfragen führt. Dies dient dazu, die Domain vor einem Ausfall zu schützen. Allgemeine Richtlinien für die CPU-Auslastung werden im Durchschnitt etwa 60 Prozent und die maximale CPU-Auslastung von 80 Prozent betragen. Gelegentliche Spitzen von 100 Prozent sind weiterhin akzeptabel und erfordern möglicherweise keine Skalierung oder Neukonfiguration.

## Instance-Typen

Amazon OpenSearch Service bietet Ihnen eine Auswahl zwischen verschiedenen Instance-Typen. Sie können die Instance-Typen auswählen, die am besten zu Ihrem Anwendungsfall passen. Amazon OpenSearch Service unterstützt die Instance-Familien R, C, M, T und I. Sie wählen eine Instance-Familie basierend auf dem Workload aus: arbeitsspeicheroptimiert, rechenoptimiert oder gemischt. Nachdem Sie eine Instance-Familie identifiziert haben, wählen Sie den Instance-Typ der neuesten Generation aus. Im Allgemeinen empfehlen wir Graviton und neuere Generationen, da sie so konzipiert sind, dass sie im Vergleich zu Instances der vorherigen Generation eine bessere Leistung mit niedrigeren Kosten bieten.

Basierend auf verschiedenen Tests, die für Anwendungsfälle für Protokollanalysen und Suchen durchgeführt wurden, empfehlen wir Folgendes:

- Für Anwendungsfälle für Protokollanalysen besteht eine allgemeine Richtlinie darin, mit der R-Familie von [Graviton](#)-Instances für Datenknoten zu beginnen. Wir empfehlen Ihnen, Tests durchzuführen, Benchmarks für Ihre Anforderungen festzulegen und die entsprechende Instance-Größe für Ihren Workload zu ermitteln.
- Für Suchanwendungsfälle empfehlen wir die Verwendung von Graviton-Instances der R- und C-Familie für Datenknoten, da Suchanwendungsfälle im Vergleich zu Anwendungsfällen für Protokollanalysen mehr CPU benötigen. Bei kleineren Workloads können Sie Graviton-Instances der M-Familie sowohl für die Suche als auch für Protokolle verwenden. Instances der I-Familie bieten NVMe-Laufwerke und werden von Kunden mit schneller Indizierung und Suchanforderungen mit niedriger Latenz verwendet.

Der Cluster besteht aus Datenknoten und Cluster-Manager-Knoten. Obwohl dedizierte Hauptknoten keine Such- und Abfrageanforderungen verarbeiten, korreliert ihre Größe stark mit der Instance-Größe und der Anzahl der Instances, Indizes und Shards, die sie verwalten können. Die [AWS-Dokumentation enthält eine Matrix](#), die den minimalen Instance-Typ des dedizierten Cluster-Managers empfiehlt.

AWS bietet Allzweck (M6g), für Datenverarbeitung (C6g) und arbeitsspeicheroptimiert (R6g und R6gd) für Amazon OpenSearch Service Version 7.9 oder höher, die von [AWS Graviton2](#)-Prozessoren betrieben wird. Diese Instances werden mit benutzerdefiniertem Silicon erstellt, das von Amazon entwickelt wurde. Es handelt sich um von Amazon entwickelte Hardware- und Softwareinnovationen, die die Bereitstellung effizienter, flexibler und sicherer Cloud-Services mit isolierter Multi-Tenancy, privatem Netzwerk und schneller lokaler Speicherung ermöglichen.

Die Graviton2-Instance-Familie reduziert die Indizierungslatenz um bis zu 50 Prozent und verbessert die Abfrageleistung im Vergleich zu Intel-basierten Instances der vorherigen Generation, die in OpenSearch Service verfügbar sind (M5, C5, R5).

## Funktionalität

Der Bereich mit dem Schwerpunkt auf Funktionen hilft Ihnen sicherzustellen, dass Sie keine Funktionalität verlieren, wenn Sie zu einer Amazon- OpenSearch Service-Zielumgebung migrieren. Wir empfehlen, genau auf die folgenden Aspekte zu achten:

- Aktuelle Lösungsfunktionalität
- Amazon OpenSearch -Service-Funktionalität
- Verpackte Plugins

## Aktuelle Lösungsfunktionalität

Wir empfehlen Ihnen, Ihre aktuelle Lösung zu analysieren und die Funktionen, Plug-Ins und APIs zu ermitteln, die Sie im aktuellen Technologie-Stack verwenden (z. B. Elasticsearch OpenSearch oder eine andere Lösung). Bestimmen Sie, welche Funktionalität für Ihr Unternehmen von entscheidender Bedeutung ist, was geändert werden kann und was während der Migration gelöscht werden kann.

## Amazon OpenSearch -Service-Funktionalität

Um sicherzustellen, dass die erforderlichen Funktionen nach der Migration verfügbar sind, empfehlen wir Ihnen, eine Analyse der neuesten von Amazon OpenSearch Service unterstützten

OpenSearch Version durchzuführen, einschließlich der Funktionen, die es bietet, und der Plugins, die in Amazon OpenSearch Service verfügbar sind. Sie möchten bestätigen, dass die Zielplattform die Funktionen unterstützt, die Sie benötigen (z. B. Indexstatusverwaltung, die das Rollover der Indizes automatisiert, oder Machine-Learning-Funktionen wie Anomalieerkennung). Ordnen Sie die vorhandene Funktionalität Ihrer aktuellen Lösung Funktionen in Amazon OpenSearch Service zu, die Ihnen gleichwertige Funktionen bieten, sodass Sie Ihre Workloads weiterhin unterstützen können.

Weitere Informationen zu den Funktionen, die in jeder unterstützten Version von Elasticsearch oder OpenSearch Software verfügbar sind, finden Sie in der [Amazon- OpenSearch Service-Dokumentation](#).

## Verpackte Plugins

Amazon OpenSearch Service unterstützt eine Reihe von Plugins, die Teil des Open-Source-OpenSearch Projekts sind. Wenn Sie ein lizenziertes Plugin aus der Elasticsearch-Suite verwenden, das Teil von X-Pack ist, oder anderweitig, sollten Sie ein entsprechendes Plugin oder eine native Funktion in den - OpenSearch Angeboten ermitteln. Möglicherweise möchten Sie dies auch als Punkt erfassen, um in der PoC-Phase nachzuweisen.

OpenSearch verfügt über mehrere Plugins, die Funktionen auf Unternehmensniveau bereitstellen, die diesen lizenzierten Plugins entsprechen. Um das richtige Plugin und die richtige Version für die Zielumgebung zu ermitteln, überprüfen Sie die Liste der Plugins in der OpenSearch Servicedokumentation nach Versionen . <https://docs.aws.amazon.com/opensearch-service/latest/developerguide/supported-plugins.html> Amazon OpenSearch Service unterstützt zwar eine Reihe von sofort OpenSearch einsatzbereiten Plug-Ins, aber Sie verwenden möglicherweise ein Open-Source- OpenSearch Plug-In, das derzeit nicht in Amazon OpenSearch Service verfügbar ist. Um das Hinzufügen des Plugins zur zukünftigen Roadmap von Amazon OpenSearch Service anzufordern, [wenden Sie sich an AWS](#) .

## Benutzerdefinierte Plugins

Zum Zeitpunkt der Erstellung dieses Handbuchs werden benutzerdefinierte Plugins nicht unterstützt. Daher müssen Sie alternative Möglichkeiten in Betracht ziehen, um die benutzerdefinierte Plugin-Funktion und -Erfahrung bereitzustellen. Wenn Ihre Lösung benutzerdefinierte Plugins verwendet, analysieren Sie die Funktionalität, um festzustellen, ob Sie die benutzerdefinierten Plugins mithilfe von Amazon- OpenSearch Service-unterstützten Plugins oder nativen Funktionen in in die Zielumgebung portieren können OpenSearch. Wir empfehlen, alle Plug-In-Optionen während der PoC-Phase zu testen und zu testen. Die Migration ist ein guter Zeitpunkt, um die aktuelle

Lösungsfunktionalität zu bewerten, um festzustellen, ob sie für Ihr Unternehmen von entscheidender Bedeutung ist.

## Versionsabhängigkeiten

Der Schwerpunktbereich für Versionsabhängigkeiten hilft Ihnen dabei, eine Roadmap Ihrer Migration durch verschiedene Versionen zu erstellen, um die neueste Version von Amazon OpenSearch Service zu erreichen. Berücksichtigen Sie die folgenden Schlüsselpunkte:

- Auswählen der Engine-Version
- Upgrade auf die neueste Version
- Upgrade-Strategie für Versionen
- Prüfungen vor dem Upgrade

## Auswählen der Engine-Version

Es ist sehr wichtig, Versionsabhängigkeiten sorgfältig zu berücksichtigen. Amazon OpenSearch Service unterstützt eine Reihe von Elasticsearch-Versionen und alle OpenSearch Engine-Hauptversionen. (Die neueste Version von OpenSearch kann jedoch einige Wochen dauern, bis sie ab dem Datum der Veröffentlichung in Amazon OpenSearch Service unterstützt wird.) Wir empfehlen Ihnen, die [von der Engine-Version unterstützten Funktionen](#) in der Amazon OpenSearch-Service-Dokumentation zu überprüfen, um die richtige Version für Ihre Anforderungen zu ermitteln. Wenn Sie dieselbe Hauptversion (und nächste Nebenversion) auswählen, können Sie den [Snapshot-Wiederherstellungsansatz](#) verwenden, um zu migrieren. Dies ist oft der direkteste Ansatz.

## Upgrade auf die neueste OpenSearch Serviceversion

Möglicherweise können Sie eine frühere Version von Amazon OpenSearch Service betreiben, wir empfehlen jedoch dringend, auf die neueste verfügbare Version zu aktualisieren. Auf diese Weise können Sie die Leistungsverbesserungen, Zuverlässigkeit, Kosteneinsparungen und viele neue Funktionen nutzen, die in den neuesten Versionen der Engine verfügbar sind. Die Migration ist eine gute Gelegenheit, die technische Belastung zu reduzieren, die durch die Ausführung früherer Softwareversionen entstehen kann.

## Upgrade-Strategie für Versionen

Wenn Sie während der Migration ein Upgrade auf die neueste Version der Software durchführen möchten, bestimmen Sie die Schritte und eine Upgrade-Strategie. Die Amazon- OpenSearch Service-Dokumentation enthält Informationen zu [Upgrade-Pfaden](#). Es ist wichtig, die grundlegenden Änderungen zwischen verschiedenen Versionen zu verstehen. In einigen Fällen erfordern die grundlegenden Änderungen möglicherweise, dass Sie Anpassungen an Ihrer Indexmodellierung und Ihrem Indexdesign planen.

### Note

Hinweis: Die Funktion Mehrere Zuordnungstypen ist nur in Elasticsearch-Versionen 5.x und früher verfügbar. Indizes, die in Versionen 6.x und höher erstellt wurden, unterstützen nur einen einzigen Zuordnungstyp für jeden Index. Wenn Sie mehrere Zuordnungstypen verwenden, empfehlen wir, diese Daten in mehrere Indizes umzuwandeln.

Im Falle einer zeitkritischen Migration sollten Sie eine grundlegende Option in Betracht ziehen, bei der Sie eine entsprechende Versionsmigration durchführen (z. B. 5.x auf 5.x) und dann die OpenSearch Serviceversion zu einem späteren Zeitpunkt aktualisieren. OpenSearch Service bietet direkte Upgrades für Domains, auf denen Elasticsearch-Versionen 5.1 (falls kompatibel) oder höher und OpenSearch 1.0 oder höher ausgeführt werden. Führen Sie einen Test durch, um festzustellen, ob Ihre Indizes für direkte Upgrades kompatibel sind, wenn Sie Elasticsearch Version 5.x ausführen. Das bedeutet, dass Sie möglicherweise zur entsprechenden Version migrieren und ein direktes Upgrade durchführen können, nachdem Sie die erforderlichen Änderungen vorgenommen haben, um Ihre Indizes und andere Funktionen mit der neuesten Version kompatibel zu machen. Lesen Sie die [Dokumentation der Upgrade-Domain](#) sorgfältig.

## Prüfungen vor dem Upgrade

Die Upgrade-Funktionalität von Amazon OpenSearch Service kann Prüfungen vor dem Upgrade durchführen, indem die Umgebung gescannt wird, um Probleme zu ermitteln, die das Upgrade blockieren können. <https://docs.aws.amazon.com/opensearch-service/latest/developerguide/version-migration.html> Das Upgrade fährt nicht mit dem nächsten Schritt fort, es sei denn, diese Prüfungen sind erfolgreich.

# KPIs und Geschäftskontinuität

Es ist wichtig, dass Sie während der Migration Ihre Geschäftsziele und Leistungsindikatoren (KPIs) festlegen, um den Erfolg zu messen. Es ist wichtig, Ihre Ziele zu Beginn des Migrationsprozesses zu bestimmen und eine Grundlage für Ihr aktuelles System zu schaffen, damit Sie messbare Verbesserungen ermitteln können. Zu den allgemeinen Zielen bei Kundenreisen gehören:

- Verbessern Sie die betriebliche Agilität.

Unter diesem Ziel können Sie Ihre vorhandene Bereitstellung mithilfe der folgenden Metriken messen und mit der Zielumgebung vergleichen:

- Durchschnittliche Zeit für die Bereitstellung des Clusters.
- Zeit für die Einführung der Bereitstellung in eine neue Geografie
- Durchschnittliche Zeit für die Konfiguration der Cluster-Sicherheit
- Durchschnittliche Zeit für die Skalierung Ihrer Umgebung (z. B. das Hinzufügen von Knoten und das Hinzufügen von Speicher)
- Durchschnittliche Zeit zum Erkennen von Abfragen mit geringer Leistung und durchschnittliche Zeit zum Reparieren
- Durchschnittliche Zeit für das Upgrade der Softwareversion
- Reduzieren Sie die Gesamtbetriebskosten (TCO).

Um Ihre aktuellen Gesamtbetriebskosten zu berechnen, können Sie die folgenden Metriken verwenden:

- Anzahl der Personalstunden für den Aufbau und Betrieb der Lösung (Entwicklung, DevOpsÜberwachung, Skalierung, Sicherung, Wiederherstellung)
- Lizenzkosten im Zusammenhang mit der vorhandenen Software
- Kosten für Rechenzentren (Betreiber und Aktualisierung von Hardware, Strom, Stromversorgung, Speicherplatz, Racks, Netzwerkgeräte)
- Personalstunden zur Konfiguration der Lösung (Softwareinstallationen, Netzwerk)
- Kosten für Compliance-Audits (HIPAA, PCI DSS, SOC, ISO, DSGVO, FedRAMP)
- Kosten für die Konfiguration der Sicherheit (Verschlüsselung im Ruhezustand und während der Übertragung, Konfiguration von Authentifizierung und Autorisierung, differenzierte Zugriffskontrolle)
- **Kosten für die Aufbewahrung einer großen Menge an warmen und kalten Daten**

- Kosten für die Konfiguration der Hochverfügbarkeit über Availability Zones hinweg
- Kosten für die Überbereitstellung, um häufige Hardware-Beanspruchungen oder den Umgang mit Spitzenlasten zu vermeiden

Diese Liste ist nicht umfassend.

- Überwachen Sie die Betriebszeit und andere Service Level Agreements (SLAs). Zu den SLAs, die Sie durch die Migration in die neue Umgebung messen und verbessern können, gehören die folgenden:
  - Gesamtbetriebszeit (Daten zur historischen Betriebszeit der vorhandenen Bereitstellung im Vergleich zu 99,9 Prozent SLA von Amazon OpenSearch Service)
  - Fehlerwiederherstellung (Ziel für Wiederherstellungspunkte und Ziel für die Wiederherstellungszeit)
  - Reaktionszeit im Zusammenhang mit verschiedenen Funktionen (z. B. Suche und Indizierung)
  - Anzahl gleichzeitiger Benutzer
  - Replikationszeit zwischen verschiedenen Regionen und Clustern.

Verwenden Sie bei der Migration zu Amazon OpenSearch Service einen iterativen Prozess, um zu überprüfen, ob Sie diese KPIs erreichen oder überschreiten und ob Sie die gewünschten Ergebnisse erzielen.

## Betriebliche Leistung

Ein wichtiger Bereich, den Sie in Ihrer aktuellen Lösung berücksichtigen sollten, sind Leistungsmetriken. Richten Sie einen Benchmark ein und ermitteln Sie Verbesserungen, die Sie in Ihrer Zielumgebung erwarten. Dazu gehören Ihre Verfügbarkeits-SLA und Latenzanforderungen. Auf diese Weise können Sie Ihre aktuellen Servicelevels einrichten und in den meisten Fällen verbessern. Normalerweise schauen sich Kunden die folgenden Servicelevel-Indikatoren an

- Lese- und Schreibvorgänge pro Sekunde
- Lese- und Schreiblatenz
- Prozentsatz der Betriebszeit

Wenn Sie Ihre eigenen SLAs entwerfen, ist es wichtig, das [Amazon OpenSearch Service – Service Level Agreement](#) vollständig zu verstehen.

## Prozessleistung

Um Ziele für die Geschäftskontinuität festzulegen, ist es wichtig, die Leistung Ihres aktuellen Prozesses zu bewerten. Identifizieren und überprüfen Sie vorhandene Runbooks oder Standardbetriebsverfahren (SOPs der aktuellen Plattform und bestimmen Sie Bereiche, in denen Ihr Team die meiste Zeit verbringt. Migration ist eine gute Gelegenheit, an der Verbesserung dieser Bereiche zu arbeiten, damit sich Ihr Team auf Innovationen, den Aufbau von Geschäftsfunktionen und die Verbesserung des Kundenerlebnisses konzentrieren kann. Sie können Probleme in Ihrer vorhandenen Umgebung identifizieren, indem Sie die historischen Support- oder Problemticketdaten überprüfen, um die Zeit zu bestimmen, die Ihr Support- und Entwicklungspersonal für die Lösung dieser Probleme aufwendet. Die Erfassung der folgenden Metriken kann Ihnen helfen, die von Ihrer Zielumgebung bereitgestellten Verbesserungen zu messen:

- Mean Time to Failure (MTTF) (Verfügbarkeit)
- Durchschnittliche Zeit zwischen Ausfällen (MTBF)
- Mittlere Zeit zum Erkennen (MTTD) eines Fehlers
- Durchschnittliche Zeit für die Reparatur (Auflösung) (M)
- Anzahl der erhaltenen Support-Tickets

## Der reibungslose Übergang zu neuen Services

Um die Geschäftskontinuität Ihrer Services sicherzustellen, ist es wichtig, einen nahtlosen Übergang sorgfältig zu planen. Die Migration ist ein guter Zeitpunkt, um Ihre Anwendung und die Services zu modernisieren, die mit Ihrer Such- oder Protokollanalyseplattform verbunden sind. Sie möchten jedoch eine sorgfältige Cutover-Strategie planen, die sich nicht auf Ihre vorhandenen Services auswirkt. Der Abschnitt [Cutover-Strategie](#) in diesem Dokument enthält Informationen zur Planung eines nahtlosen Cutovers in der Zielumgebung.

## Finanzmetriken

Es kann viele Gründe für die Migration zu Amazon OpenSearch Service geben, aber die Kosten sind im Allgemeinen ein wichtiger Faktor. Machen Sie sich mit den Gesamtbetriebskosten (TCO) der vorhandenen Umgebung vertraut, damit Sie die Kosteneinsparungen messen können, die Sie durch die Umstellung auf den verwalteten Service erzielen. Sie können mit der Liste der Metriken beginnen, die unter dem Ziel Gesamtbetriebskosten reduzieren aufgeführt sind. AWS hat eine [Benchmarking-Untersuchung zu Cloud-Werten](#) veröffentlicht, die Teams dabei helfen kann, ein Geschäftsszenario

für die Migration in die AWS Cloud zu erstellen. Die Untersuchung ist zwar nicht spezifisch für Amazon OpenSearch Service, behandelt jedoch wichtige Wertebereiche, die bei den meisten Cloud-Migrationen üblich sind, einschließlich der Migration zu Amazon OpenSearch Service.

In den meisten Fällen liefert Amazon OpenSearch Service niedrigere Gesamtbetriebskosten. Bei der Berechnung der Gesamtbetriebskosten ist es wichtig, die Personalkosten zu berücksichtigen. Es ist wichtig, die Zeit und die Kosten zu verstehen, die Ihre Techniker für die Wartung der aktuellen Umgebung aufwenden. Viele Kunden vergleichen nur die Kosten für Speicher-, Datenverarbeitungs- und Netzwerkinfrastruktur mit den Kosten des verwalteten Services. Dies bietet Ihnen jedoch möglicherweise keine genauen Gesamtbetriebskosten. Amazon OpenSearch Service bietet Ihrem Team betriebliche Effizienz, indem es Aufgaben verwaltet, die andernfalls von Ihren Technikern ausgeführt werden mussten. Dazu gehören die folgenden Aufgaben:

- Skalieren eines Clusters durch Hinzufügen oder Entfernen von Knoten
- Patchen
- Direktes Upgraden
- Erstellen von Backups
- Konfigurieren von Überwachungstools zur Erfassung von Protokollen und Metriken

Diese Aktivitäten werden vom Service automatisiert, und AWS bietet ein Support-Team auf Produktionsebene. Das bedeutet, dass sich Ihre Mitarbeiter auf Aktivitäten konzentrieren können, die Ihrem Unternehmen einen direkten Wert verleihen.

## Betrieb und Sicherheit

Wenn Sie zu Amazon OpenSearch Service migrieren, ändern sich Ihre Betriebsaktivitäten. Sie sind nicht mehr für die Bereitstellung von Knoten, das Hinzufügen von Speicher, die Installation und das Patchen des Betriebssystems, die Konfiguration und Aufrechterhaltung von Hochverfügbarkeit, Skalierung und anderen Aktivitäten auf niedriger Ebene verantwortlich. Stattdessen können Sie sich darauf konzentrieren, Ihre Anwendungsfälle und neuen Benutzererlebnisse zu entwickeln.

Amazon OpenSearch Service bietet Funktionen zur Protokollierung, Überwachung und Fehlerbehebung, mit denen Sie sich vertraut machen müssen, um Ihre Betriebsprozesse zu optimieren.

## Runbooks und neue Prozesse

Identifizieren Sie während der Planungsphase vorhandene Prozesse, die geändert oder entfernt werden müssen. Sie können dann neue Betriebsprozesse hinzufügen, für die Sie in der Vergangenheit möglicherweise keine Bandbreite hatten.

Amazon OpenSearch Service übernimmt zwar die undifferenzierte Hauptarbeit, Sie müssen jedoch dennoch sicherstellen, dass Ihre Anwendung so konzipiert und überwacht wird, dass sie die beste Leistung bietet. Sie müssen Überwachung und Warnungen für Ihre Domain konfigurieren, damit Sie sich über alle Zustandsprobleme aufgrund interner oder externer Faktoren im Klaren sind. Sie müssen Upgrades auf die neuesten Versionen planen und initiieren.

Für alle diese operativen Aktivitäten müssen Runbooks erstellt und vorhandene Runbooks geändert werden. Um die Infrastruktur zu überwachen und Betriebsmetriken in Amazon OpenSearch Service zu analysieren, ist es wichtig, Runbooks zu verwalten. Runbooks stellen sicher, dass Sie konsistent gemäß Ihren Compliance- und regulatorischen Anforderungen arbeiten. Wenn Sie keine Runbooks verwendet haben, ist es sinnvoll, dies zu erwägen. Erstellen Sie Prozesse, um regelmäßig vorab geplante Schritte auszuführen, um sicherzustellen, dass Korrekturprozesse wie die Wiederherstellung nach Anwendungsabstürzen und unerwarteten Fehlern vollständig automatisiert werden.

## Support- und Ticketing-System

Um Vorfälle im Zusammenhang mit Ihren Bereitstellungen zu erfassen, empfehlen wir Ihnen, ein Ticketsystem zu planen und zu betreiben (möglicherweise tun Sie dies bereits). Möglicherweise müssen Sie Ihre Support-Mitarbeiter darin schulen, wie sie Support-Tickets mit [AWS Support](#) erstellen. Wir empfehlen, den Prozess der Eskalation während der Ticketverifizierung zu optimieren.

Der Abschnitt [Operational Excellence](#) weiter unten in diesem Leitfaden enthält Links zu einer Reihe von bewährten Methoden und Bereichen, die Sie möglicherweise in Ihren Runbooks berücksichtigen und Prozesse aufbauen müssen.

## Sicherheit

Bei AWS hat Sicherheit höchste Priorität. Amazon OpenSearch Service bietet mehrschichtige Sicherheit. Der Service kümmert sich um alle Sicherheitspatches und bietet Netzwerkisolierung über VPC, differenzierte Zugriffskontrolle und Multi-Tenant-Unterstützung. Ihre Daten werden im Ruhezustand mit Schlüsseln verschlüsselt, die Sie über AWS Key Management Service (AWS KMS) erstellen und steuern. Die node-to-node Verschlüsselungsfunktion bietet Transport Layer Security (TLS) für die gesamte Kommunikation zwischen Instances in einer Domain. Amazon OpenSearch

Service ist auch HIPAA-fähig und entspricht PCI-DSS-, SOC-, ISO- und FedRAMP-Standards, um Sie bei der Einhaltung branchenspezifischer oder gesetzlicher Anforderungen zu unterstützen.

Identifizieren Sie in der Planungsphase die Personen und Prozesse, die mit der Domain interagieren, wählen Sie eine Netzwerktopologie aus und planen Sie die Authentifizierung und Autorisierung für jeden Prinzipal. Abhängig von Ihren organisatorischen Sicherheits- und Compliance-Anforderungen können Sie mehrere Sicherheitsfunktionen verwenden, um eine Umgebung zu erstellen, die Ihren Geschäftsanforderungen entspricht. Berücksichtigen Sie außerdem die folgenden Faktoren:

- VPC – Sie können Amazon OpenSearch Service in einer Virtual Private Cloud (VPC) in AWS konfigurieren. Dies ist die [empfohlene Konfiguration](#). Wir empfehlen nicht, eine Domain mit einem öffentlichen Endpunkt zu erstellen. Planen Sie, die erforderliche Netzwerkarchitektur zu erstellen, damit Ihre Clientanwendungen und Benutzer auf die Zielumgebung zugreifen können.
- Authentifizierung – Amazon OpenSearch Service unterstützt mehrere Möglichkeiten, einen Benutzer oder Softwareclient zu authentifizieren. Es unterstützt die [Amazon Cognito](#)- oder [SAML-Authentifizierung](#) mit Ihrem vorhandenen Identitätsanbieter, um auf [OpenSearch Dashboards](#) zuzugreifen. Es bietet auch die Integration mit IAM-Identitäten und die [grundlegende HTTP-Authentifizierung mithilfe einer internen Benutzerdatenbank](#). Sie sollten planen, eine geeignete Option für die Authentifizierung zu konfigurieren und zu testen. Weitere Informationen finden Sie in der [OpenSearch Service-Sicherheitsdokumentation](#).
- Autorisierung – Wir empfehlen Ihnen, bei der Konfiguration des Zugriffs auf den Service dem Prinzip der geringsten Berechtigung zu folgen. Amazon OpenSearch Service bietet eine differenzierte Zugriffskontrolle, mit der Sie den Zugriff auf Dokument-, Zeilen- und Spaltenebene konfigurieren können.

Machen Sie sich mit den Sicherheitsfunktionen vertraut und testen Sie sie während der PoC-Phase.

## Training

Wenn Sie mit Ihrer Migration zu AWS beginnen, müssen Ihre Softwareentwicklungs-, Betriebs-, Support- und Sicherheitsteams über Kenntnisse von Amazon OpenSearch Service verfügen. Betrachten Sie alle Teams, die mit Ihrer Lösung interagieren. Wenn Sie von einer Elasticsearch- oder einer - OpenSearch Umgebung migrieren, kann der Großteil des Wissens übertragen werden. Stellen Sie den folgenden Teams Schulungen zur Verfügung:

- Softwareentwicklungsteam – Schulen Sie Ihr Softwareentwicklungsteam über die APIs und Funktionen, wie z. B. Mechanismen zur Konfiguration der Datenaufnahme.

- **Betriebsteam** – Trainieren Sie Ihr Betriebsteam in der Interaktion mit Amazon- OpenSearch Service-Domains, überwachen Sie Betriebsmetriken und Zugriffsprotokolle mithilfe von Amazon CloudWatch. Teammitglieder sollten lernen, wie Sie automatische Alarmer einrichten, um zu warnen, wenn OpenSearch Service-Domains Aufmerksamkeit benötigen. Wenn Sie von einem vorhandenen Toolset migrieren, das Sie On-Premises verwenden, z. B. Splunk, identifizieren Sie die Überwachungsoptionen in Amazon OpenSearch Service, die einen ähnlichen Einblick in Ihre Workloads bieten können.
- **Support-Team** – Schulen Sie Ihr Support-Team bei der Implementierung von Runbooks, die OpenSearch Service-Ressourcen beinhalten. Möglicherweise möchten Sie Runbooks und Verfahren zur Ereignisverwaltung aktualisieren, um AWS Support-Services zu nutzen.
- **Sicherheitsteam** – Informieren Sie Ihr Sicherheitsteam über die Konfiguration einer differenzierten Zugriffskontrolle und die Integration in bestehende Identitätsanbieter (IDPs).

## Trainingsoptionen

AWS Training and Certification bietet sowohl digitales als auch Präsenztraining für Einsteiger bis hin zu Fachwissen in Bezug auf Cloud-Fähigkeiten, die für den Aufbau und Betrieb von Lösungen in AWS erforderlich sind. Die Inhalte werden von Experten bei AWS erstellt und regelmäßig aktualisiert. Sie haben mehrere Trainingsoptionen.

Sie können mit Ihrem AWS-Kontoteam zusammenarbeiten, um Ihnen bei der Identifizierung einer geeigneten Ressource zu helfen. Im Folgenden finden Sie einige der Ressourcen, mit denen Sie Ihre Teams auf Amazon OpenSearch Service weiterbilden können:

- **Einsteigertage** – AWS-Lösungsarchitekten können Einsteigertage durchführen, bei denen es sich um praktische Workshops handelt, die auf Anwendungsfälle, allgemeine Implementierungsmuster und Roadmap-Elemente zugeschnitten sind, die sich möglicherweise speziell auf Anwendungsfälle beziehen.
- **Praktische Workshops** – Teams können an Self-Service-Workshops teilnehmen, die von AWS-Experten erstellt wurden.
- [Whitepaper und Leitfäden](#) – AWS-Whitepaper sind eine hervorragende Möglichkeit, Ihr Wissen über die Cloud zu erweitern. Sie wurden von AWS und der AWS-Community verfasst und bieten detaillierte Inhalte, die sich häufig mit bestimmten Kundensituationen befassen.
- [Blogbeiträge](#) – Diese Blogbeiträge wurden von AWS-Experten und -Kunden verfasst und behandeln die neuesten Ankündigungen, bewährten Methoden, Lösungen, Service-Features, Kundenanwendungsfälle und andere Themen.

- Bewährte Methoden – Nutzen Sie Online- oder Konferenzvorträge oder Sitzungen von AWS-Experten, die Ihnen helfen, bewährte Methoden für Amazon OpenSearch Service zu verstehen.
- [AWS Professional Services](#) – Das AWS Professional Services-Team kann bewährte Methoden und vorgeschriebene Beratung bieten. Das Team bietet ein [Trainingsprogramm](#), das IT-Experten hilft, erfolgreiche Migrationen zu verstehen und durchzuführen.

## Datenfluss

Der Datenfluss-Fokusbereich umfasst die folgenden drei Bereiche:

- Datenerfassung
- Datenaufbewahrung
- Datenmigrationsansatz

## Datenerfassung

Die Datenaufnahme konzentriert sich darauf, wie Sie Daten in Ihre Amazon- OpenSearch Service-Domain abrufen. Ein gründliches Verständnis der Datenquellen und Formate ist bei der Auswahl des richtigen Aufnahme-Frameworks für von entscheidender Bedeutung OpenSearch.

Es gibt viele verschiedene Möglichkeiten, Ihr Aufnahmedesign zu erstellen oder zu modernisieren. Es gibt viele Open-Source-Tools zum Erstellen einer selbstverwalteten Aufnahme-Pipeline. OpenSearch Der Service unterstützt die Integration mit [Fluentd](#) , [Logstash](#) oder [OpenSearch Data Prepper](#) . Diese Tools sind bei den meisten Entwicklern von Protokollanalyselösungen beliebt. Sie können diese Tools auf einer Amazon EC2-Instance, auf Amazon Elastic Kubernetes Service (Amazon EKS) oder On-Premises bereitstellen. Sowohl Logstash als auch Fluentd unterstützen Amazon-OpenSearch Service-Domains als Ausgabeziel. Dazu müssen Sie jedoch die Fluentd- oder Logstash-Softwareversionen auf dem neuesten Stand halten, patchen, testen und halten.

Um Ihren betrieblichen Aufwand zu reduzieren, können Sie einen der AWS verwalteten Services verwenden, die die Integration mit Amazon OpenSearch Service unterstützen. Amazon [OpenSearch Ingestion](#) ist beispielsweise ein vollständig verwalteter Serverless-Datenkollektor, der Protokoll-, Metrik- und Ablaufverfolgungsdaten in Echtzeit an Amazon- OpenSearch Service-Domains liefert. Mit OpenSearch Ingestion müssen Sie keine Drittanbieterlösungen wie Logstash oder [Jaeger](#) mehr verwenden, um Daten in Ihre OpenSearch Service-Domains aufzunehmen. Sie konfigurieren Ihre Datenproduzenten so, dass Daten an OpenSearch Ingestion gesendet werden. Anschließend werden

die Daten automatisch an die von Ihnen angegebene Domain oder Sammlung übermittelt. Sie können OpenSearch Ingestion auch so konfigurieren, dass Ihre Daten vor der Bereitstellung transformiert werden.

Eine weitere Option ist [Amazon Data Firehose](#), ein vollständig verwalteter Service, der beim Aufbau einer Serverless-Erfassungspipeline hilft. Firehose bietet eine sichere Möglichkeit, [Streaming-Daten in Amazon- OpenSearch Service-Domains aufzunehmen, zu transformieren und bereitzustellen](#). Es kann automatisch an den Durchsatz Ihrer Daten angepasst werden und erfordert keine fortlaufende Administration. Firehose kann eingehende Datensätze auch transformieren AWS Lambda, indem es die Daten vor dem Laden in Ihre OpenSearch Service-Domain verwendet, komprimiert und stapelt.

Mit einem verwalteten Service können Sie Ihre vorhandene Datenaufnahme-Pipeline außer Betrieb nehmen oder Ihr aktuelles Setup erweitern, um den Betriebsaufwand zu reduzieren.

Die Migrationsplanung ist ein guter Zeitpunkt, um zu beurteilen, ob Ihre aktuelle Aufnahme-Pipeline den Anforderungen aktueller und zukünftiger Anwendungsfälle entspricht. Wenn Sie von einer selbstverwalteten Elasticsearch oder einem selbstverwalteten OpenSearch Cluster migrieren, sollte Ihre Aufnahme-Pipeline das Auslagern der Endpunkte vom aktuellen Cluster zur Amazon-OpenSearch Service-Domain mit minimalen Client-Bibliotheksaktualisierungen unterstützen.

## Datenaufbewahrung

Bei der Planung der Datenerfassung und -speicherung sollten Sie die Datenaufbewahrung planen und sich darauf einigen. Für Anwendungsfälle für Protokollanalysen ist es wichtig, dass Sie innerhalb Ihrer Domain die richtigen Richtlinien erstellt haben, um die historischen Daten außer Betrieb zu nehmen. Wenn Sie von einer vorhandenen On-Premises- und Cloud-VM-basierten Architektur wechseln, können Sie einen bestimmten Instance-Typ für alle Ihre Datenknoten verwenden. Datenknoten haben dieselbe CPU, denselben Arbeitsspeicher und dasselbe Speicherprofil. Die meisten Kunden würden Speicher mit hohem Durchsatz konfigurieren, um ihre Hochgeschwindigkeitsindizierungsanforderung zu erfüllen. Diese einzelne Speicherprofilarchitektur wird als reine Hot-Knoten-Architektur oder „nur Hot-Knoten“ bezeichnet. Die Hot-Only-Architektur koppelt Speicher mit Rechenleistung, was bedeutet, dass Sie Rechenknoten hinzufügen müssen, wenn Ihr Speicherbedarf steigt.

Um Speicher von der Datenverarbeitung zu entkoppeln, bietet Amazon OpenSearch Service die UltraWarm Speicherstufe. UltraWarm bietet eine kostengünstige Möglichkeit, schreibgeschützte Daten auf Amazon OpenSearch Service zu speichern, indem Knoten bereitgestellt werden, die ein größeres Datenvolumen aufnehmen können als herkömmliche Datenknoten.

Legen Sie bei der Planung die Datenaufbewahrungs- und Verarbeitungsanforderung fest. Um die Kosten für Ihre vorhandene Lösung zu senken, nutzen Sie die Vorteile der - UltraWarm Stufe. Identifizieren Sie die Aufbewahrungsanforderungen für Ihre Daten. Erstellen Sie dann Indexstatusverwaltungsrichtlinien, um Daten von Hot zu Warm zu verschieben oder die Daten bei Bedarf automatisch aus der Domain zu löschen. Dies trägt auch dazu bei, dass Ihrer Domain nicht der Speicherplatz ausgeht.

## Ansätze zur Datenmigration

Während der Planungsphase ist es wichtig, dass Sie sich für einen bestimmten Datenmigrationsansatz entscheiden. Ihr Datenmigrationsansatz bestimmt, wie Sie die Daten, die sich in Ihrem aktuellen Datenspeicher befinden, ohne Lücken in den Zielspeicher verschieben. Die Verfahrensdetails für diese Ansätze werden im Abschnitt [Phase 4 – Datenmigration](#) behandelt, in der Sie Ihren Ansatz implementieren.

In diesem Abschnitt werden verschiedene Möglichkeiten und Muster beschrieben, mit denen Sie einen Elasticsearch- oder OpenSearch Cluster zu Amazon OpenSearch Service migrieren können. Berücksichtigen Sie bei der Auswahl eines Musters die folgende Liste von Faktoren (nicht vollständig):

- Ob Sie Daten aus einem vorhandenen selbstverwalteten Cluster kopieren oder aus der ursprünglichen Datenquelle (Protokolldateien, Produktkatalogdatenbank) neu erstellen möchten
- Versionskompatibilität der Quell-Elasticsearch- oder OpenSearch -Cluster- und Ziel-Amazon-OpenSearch Service-Domain
- Anwendungen und Services, die vom Elasticsearch- oder OpenSearch -Cluster abhängig sind
- Das verfügbare Fenster für die Migration
- Das Volumen der indizierten Daten in Ihrer vorhandenen Umgebung

### Aus einem Snapshot erstellen

Snapshots sind die beliebteste Möglichkeit, von einem selbstverwalteten Elasticsearch-Cluster zu Amazon OpenSearch Service zu migrieren. Snapshots bieten eine Möglichkeit, Ihre - OpenSearch oder Elasticsearch-Daten mithilfe eines dauerhaften Speicherservices wie Amazon S3 zu sichern. Mit diesem Ansatz erstellen Sie einen Snapshot Ihrer aktuellen Elasticsearch- oder - OpenSearch Umgebung und stellen ihn in der Amazon- OpenSearch Service-Zielumgebung wieder her. Nach der Wiederherstellung des Snapshots können Sie Ihre Anwendung auf die neue Umgebung verweisen. Dies ist in den folgenden Situationen eine schnellere Lösung:

- Ihre Quelle und Ihr Ziel sind kompatibel.
- Der vorhandene Cluster enthält eine große Menge indizierter Daten, was für die Neuindizierung zeitaufwändig sein kann.
- Ihre Quelldaten stehen nicht für die Neuindizierung zur Verfügung.

Weitere Überlegungen finden Sie unter Snapshot-Überlegungen im Abschnitt [Phase 4 – Datenmigration](#).

### Aus der Quelle erstellen

Dieser Ansatz impliziert, dass Sie keine Daten aus Ihrem aktuellen Elasticsearch- oder OpenSearch Cluster verschieben werden. Stattdessen laden Sie die Daten direkt aus Ihrem Protokoll oder Ihrer Produktkatalogquelle in die Amazon- OpenSearch Service-Zieldomäne. Dies erfolgt in der Regel mit geringfügigen Änderungen an vorhandenen Datenerfassungspipelines. Im Anwendungsfall für die Protokollanalyse erfordert das Erstellen aus der Quelle möglicherweise auch das Neuladen der historischen Protokolle aus Ihren Quellen in die neue OpenSearch Serviceumgebung. Für Suchanwendungsfälle müssen Sie möglicherweise Ihren vollständigen Produktkatalog und Inhalt in die neue Amazon- OpenSearch Service-Domain neu laden. Dieser Ansatz funktioniert in den folgenden Szenarien gut:

- Ihre Quell- und Zielumgebungsversionen sind für die Snapshot-Wiederherstellung nicht kompatibel.
- Sie möchten Ihr Datenmodell im Rahmen der Migration in der Zielumgebung ändern.
- Sie möchten zur neuesten Version von Amazon OpenSearch Service springen, um fortlaufende Upgrades zu vermeiden, und Sie möchten die grundlegenden Änderungen in einem Schritt beheben. Dies kann eine gute Idee sein, wenn Sie eine relativ ältere Version (5.x oder früher) von Elasticsearch selbst verwalten.
- Möglicherweise möchten Sie Ihre Indizierungsstrategie ändern. Anstatt beispielsweise jeden Tag ein Rollover durchzuführen, können Sie in der neuen Umgebung jeden Monat ein Rollover durchführen.

Informationen zu den Optionen für die Erstellung aus der Quelle finden Sie unter 2. Aufbau aus der Quelle im Abschnitt [Phase 4 – Datenmigration](#).

### Remote-Neuindizierung aus einer vorhandenen Elasticsearch- oder - OpenSearch Umgebung

Dieser Ansatz verwendet die [Remote-Neuindizierungs-API](#) von Amazon OpenSearch Service. Mit der Remote-Neuindizierung können Sie Daten direkt aus Ihrer vorhandenen On-Premises- oder Cloud-

basierten Elasticsearch- oder OpenSearch Cluster-Instance in Ihre Amazon- OpenSearch Service-Domain kopieren. Sie können eine Automatisierung erstellen, mit der die Daten zwischen den beiden Umgebungsstandorten synchronisiert werden können, bis Sie zur Zielumgebung wechseln.

### Open-Source-Datenmigrationstools verwenden

Es stehen mehrere Open-Source-Tools zur Verfügung, um Daten von Ihrer vorhandenen Elasticsearch-Umgebung in Ihre Amazon- OpenSearch Zielumgebung zu migrieren. Ein solches Beispiel ist das Logstash-Dienstprogramm. Sie können das Logstash-Dienstprogramm verwenden, um Daten aus einem Elasticsearch- oder - OpenSearch Cluster zu extrahieren und in die Amazon- OpenSearch Service-Domain zu kopieren.

Wir empfehlen Ihnen, alle Ihre Optionen zu bewerten und sich für die zu entscheiden, mit der Sie am besten vertraut sind. Um sicherzustellen, dass Ihr ausgewählter Ansatz foolproof ist, testen Sie alle Ihre Tools und Automatisierungen während Ihrer PoC-Phase. Einzelheiten und step-by-step Anleitungen zur Implementierung dieser Ansätze finden Sie im Abschnitt [Phase 4 – Datenmigration](#).

## Bereitstellungs-Frameworks

Viele moderne Teams nutzen CI/CD-Methoden (Continuous Integration and Continuous Delivery) und Pipelines, um die Bereitstellung ihrer Lösungen und Infrastruktur zu automatisieren. Wenn Ihr Team bereits CI/CD-Pipelines verwendet, sollten Sie Amazon OpenSearch Service in Ihre Umgebung integrieren können. Wenn Sie manuell in Ihrem aktuellen Setup bereitstellen, sollten Sie Pipelines erstellen, um wiederholbare Arbeit zu automatisieren, den betrieblichen Aufwand zu reduzieren und menschliche Fehler zu reduzieren.

Sie können Amazon OpenSearch Service mithilfe einer Vielzahl von Open-Source-Frameworks für Infrastructure as Code (IaC) bereitstellen, darunter Terraform von HashiCorp, Chef und Puppet. Terraform bietet ein [-OpenSearch Modul](#), mit dem Sie Amazon- OpenSearch Service-Domains erstellen können. In vielen Fällen können Sie Ihre vorhandene Infrastrukturbereitstellungs-Pipeline verwenden und das Suchmaschinenmodul auf das Amazon- OpenSearch Service-Modul verweisen.

Wenn Sie darüber nachdenken, Pipelines von Grund auf neu zu erstellen, oder wenn Sie native AWS-Services verwenden möchten, bietet AWS mehrere CI/CD-Tools und Serviceoptionen. Diese umfassen u. a. folgende:

- [AWS CodePipeline](#)
- [AWS CodeBuild](#)

- [AWS Cloud Development Kit \(AWS-CDK\)](#)
- [AWS CloudFormation](#)
- [AWS CodeDeploy](#)

Sie können diese Services verwenden, um Aufbau, Test und Bereitstellung von Infrastrukturen zu automatisieren. Die Bereitstellung Ihrer Pipelines mithilfe eines dieser cloudnativen Services hat viele Vorteile, darunter die folgenden:

- Vollständig automatisierte Produktversionen end-to-end (Erstellen, Testen, Bereitstellen)
- Bereitstellung in mehreren Umgebungen (dev, test, pre-prod, prod)
- Integration mit anderen AWS-Services
- Die Möglichkeit, Ihre Bereitstellungs-Pipelines zu modernisieren, um Bereitstellungen von Amazon OpenSearch Service in mehreren Umgebungen zu automatisieren

## Phase 2 – Machbarkeitsnachweis

Bei einer Migration ist es wichtig nachzuweisen, ob die Zielstatuslösung wie erforderlich funktioniert. Wir empfehlen dringend, eine proof-of-concept (PoC)-Übung auszuführen. Dieser Abschnitt konzentriert sich auf die verschiedenen Aspekte, die bei der Ausführung eines PoC berücksichtigt werden müssen:

- Definieren von Ein- und Ausstiegskriterien
- Sicherung der Finanzierung
- Automatisieren
- Ausführliche Tests
- PoC-Phasen
- Simulation von Fehlern

### Definieren von Ein- und Ausstiegskriterien

Klare Ein- und Ausgangskriterien sind der Schlüssel für eine erfolgreiche PoC-Übung. Berücksichtigen Sie bei der Definition Ihrer Eingabekriterien Folgendes:

- Anwendungsfalldefinition
- Zugriff auf Umgebungen
- Vertrautheit mit verschiedenen -Services
- Zugeordnete Trainingsanforderungen

Definieren Sie in ähnlicher Weise Beendigungskriterien, anhand derer Sie das PoC-Ergebnis bewerten können, einschließlich der folgenden:

- Funktionalität
- Leistungsanforderungen
- PoC-Sicherheitsimplementierungen

## Sicherung der Finanzierung

Basierend auf der Definition der PoC-Kriterien, sichere Finanzierung für das PoC . Stellen Sie sicher, dass Sie die richtige Größe durchgeführt und alle damit verbundenen Kosten berücksichtigt haben. Wenn Sie von On-Premises zu AWS migrieren, schließen Sie die Kosten ein, die mit der Migration Ihrer Frameworks zu AWS Cloud von On-Premises verbunden sind. Wenn Sie bereits AWS-Kunde sind, wenden Sie sich an Ihren AWS-Kontomanager, um zu erfahren, ob Sie sich für Guthaben qualifizieren, die für die Migration zu Amazon OpenSearch Service verwendet werden können.

## Automatisieren

Identifizieren Sie, wo Automatisierung durchgeführt werden kann, und planen Sie einen dedizierten Pfad zur Automatisierung und Terminplanung der Tests. Automatisierte Bereitstellung und Tests helfen Ihnen dabei, schnell und ohne von Menschen verursachte Fehler zu reduzieren, zu wiederholen, zu testen und zu validieren.

Durch das Time-Boxing eines Tests können Sie sicherstellen, dass Sie rechtzeitig liefern und bei Herausforderungen zu anderen Aktivitäten wechseln können. Wenn Ihre Leistungstests beispielsweise länger dauern als die geschätzte Zeit, können Sie diese Aktivität anhalten. Sie können dann zu anderen Tests und Validierungsaktivitäten wechseln, während Ihre Entwickler die Probleme beheben. Sie können zu den Leistungstests zurückkehren, nachdem die Probleme behoben wurden. Führen Sie einen Benchmark für die Leistung Ihrer vorhandenen Lösung durch und erstellen Sie automatisierte Leistungstests, die die Auswirkungen Ihrer Konfigurationsänderungen während der PoC überprüfen können.

## Ausführliche Tests

Testen Sie alle Teile des Stacks, indem Sie sicherstellen, dass Sie die erforderlichen Validierungen für die verschiedenen Ebenen durchführen, z. B. Aufnahmepipelines und Abfragemechanismen, die in Ihre Amazon- OpenSearch Service-Domain integriert sind. Dies hilft Ihnen bei der Validierung der end-to-end Lösungsimplementierung.

### Darstellungsebene

Führen Sie auf der Präsentationsebene eine PoC-Übung durch, die die folgenden Aktivitäten umfasst:

- Authentifizieren – Validieren Sie die geplanten Mechanismen für die Authentifizierung Ihrer Benutzer.

- **Autorisieren** – Identifizieren Sie die Autorisierungsmechanismen, die Sie befolgen möchten, und überprüfen Sie, ob sie wie erwartet funktionieren.
- **Abfrage** – Was sind die häufigsten Anwendungsfälle, denen Sie in der Produktion begegnen werden? Welche Edge-Fall-Szenarien sind für Ihr Unternehmen von entscheidender Bedeutung? Identifizieren Sie diese Muster und validieren Sie sie während der PoC-.
- **Wiedergabe** – Werden die Daten für verschiedene Benutzer in verschiedenen Anwendungsfällen korrekt und angemessen gerendert? Für Anwendungsfälle für Protokollanalysen sollten Sie das Dashboard je nach Zielversion auf OpenSearch Dashboards oder Kibana erstellen und testen, um sicherzustellen, dass es Ihren Anforderungen entspricht.

## Aufnahmeebene

Stellen Sie sicher, dass Sie auf der Aufnahmeebene verschiedene Komponenten wie Sammlung, Pufferung, Aggregation und Speicherung auswerten:

- **Sammlung** – Überprüfen Sie für Anwendungsfälle für Protokollanalysen, ob alle Daten, die Sie protokollieren, erfasst werden. Identifizieren Sie für Suchanwendungsfälle die Quellen, die die Daten liefern, und führen Sie Validierungen der Vollständigkeit und Richtigkeit der Daten durch, um sicherzustellen, dass die Erfassungsphase erfolgreich ausgeführt wurde.
- **Puffer** – Wenn Sie einen Anstieg des Datenverkehrs haben, möchten Sie möglicherweise sicherstellen, dass Sie die aufgenommenen Daten puffern. Es gibt verschiedene Möglichkeiten, ein Pufferdesign zu erstellen. Sie können beispielsweise Daten in Amazon Data Firehose sammeln oder Amazon S3-Speicher als Puffer verwenden.
- **Aggregation** – Validieren Sie jede Aggregation von Daten, z. B. die Massen-API-Nutzung, die Sie während der Aufnahme durchführen.
- **Speicher** – Überprüfen Sie, ob der Speicher die von Ihnen durchgeführte Aufnahme optimal verarbeiten kann.

## PoC-Phasen

Wir empfehlen Ihnen, die folgenden Phasen zu verwenden, um Ihren PoC zu implementieren und das Ergebnis zu validieren. Achten Sie darauf, diese PoC-Phasen nicht zu durchlaufen und den Plan-PoC anzupassen, obwohl Sie zuvor Zeit in die Planung investieren.

- **Funktionstests und Lasttests** – Stellen Sie sicher, dass alle Ebenen gründlich getestet werden. Simulieren Sie Fehler in allen Teilen des Stacks. Wenn Sie beispielsweise einen Cluster mit

zwei großen Knoten haben und einer davon ausfällt, muss der andere Knoten den gesamten Datenverkehr auf Ihrem Cluster in Anspruch nehmen. In einem solchen Szenario kann eine höhere Anzahl kleinerer Knoten zu einer reibungsloseren Wiederherstellung nach einem Knotenausfall führen. Testen Sie Ihre Workloads bei Spitzenlasten und höher, um sicherzustellen, dass die Leistung in solchen Szenarien nicht beeinträchtigt wird. Leiten Sie während des Tests Probleme frühzeitig aus, damit potenzielle Probleme von verschiedenen Stakeholdern zur richtigen Zeit bewertet werden.

- Überprüfen der KPIs und Tuning – Stellen Sie während der PoC sicher, dass Sie die KPIs und Geschäftsergebnisse erfüllen, die Sie in Ihren PoC-Beendigungskriterien definiert haben. Passen Sie die Konfigurationen so an, dass sie die KPIs erfüllen.
- Automatisieren und Bereitstellen – Automatisierung und Überwachung sind die anderen wichtigsten Aspekte, auf die Sie sich während des PoC-Tests konzentrieren sollten. Verfeinern Sie Ihre Automatisierungsschritte und validieren Sie sie zusammen mit der detaillierten Überwachung, um allen Stakeholdern genügend Informationen zu geben, um die Ergebnisse des PoC- sicher zu bewerten. Dokumentieren Sie alle Schritte und erstellen Sie ein Runbook, das Sie für die Produktionsmigration wiederverwenden können.

## Simulation von Fehlern

Es wird dringend empfohlen, ein Fehlerszenario zu simulieren und zu überprüfen, ob Ihr Design die Ausfallsicherheit und Fehlertoleranz bietet, die erforderlich sind, um Ihre Benutzeranforderungen zu erfüllen. Möglicherweise möchten Sie einen Ausfall eines Datenknotens simulieren, um festzustellen, ob Ihr Cluster über genügend Ressourcen verfügt, um die Wiederherstellung ordnungsgemäß zu bewältigen. Um zu überprüfen, ob Ihre Domain bei der Aufnahme großer Mengen überfordert sein könnte, können Sie die Puffereinstellungen testen, indem Sie einen plötzlichen Anstieg von Protokollen aus einigen Ihrer Quellen simulieren. Stellen Sie sicher, dass Ihr Design keine Kontingente überschreitet, wenn Sie auf eine Produktionsbereitstellung skalieren. Weitere Informationen finden Sie in der Amazon- OpenSearch Service-Dokumentation zu [Service Quotas](#).

## Phase 3 — Einsatz

Bis Sie die Bereitstellungsphase erreichen, haben Sie Ihren PoC abgeschlossen und haben eine gute Vorstellung davon, wie Sie Ihre Zielumgebung in der Produktion einsetzen können. Beachten Sie folgende Überlegungen:

- Validieren Sie die Automatisierung— Führen Sie während der Bereitstellung die Automatisierung aus, die Sie während des PoC erstellt haben, und überprüfen Sie, ob sie erwartungsgemäß funktioniert. Stellen Sie außerdem sicher, dass Ihre CI/CD-Automatisierung wie erwartet funktioniert, wenn Sie Änderungen am Konfigurationscode vornehmen.
- Überprüfen Sie die Sicherheit— Es ist wichtig zu überprüfen, ob alle Ihre Sicherheitskonfigurationen wie erwartet funktionieren und dass Ihre Daten sicher sind. Vergewissern Sie sich, dass die Lösung den Sicherheitsstandards Ihres Unternehmens entspricht, z. B. der Integration von Identitätsanbietern, und dass Ihre Hauptbenutzer sich anmelden und auf Daten zugreifen können, für die sie autorisiert sind.
- Überwachung— Stellen Sie sicher, dass Sie Ihre Überwachungskonfigurationen getestet und die empfohlenen Warnmeldungen eingerichtet haben. Überwachen Sie wichtige Kennzahlen wie CPU, Arbeitsspeicher, Festplatten, JVMs und Shard-Zuweisungen. Um Ihnen Einblicke in den Zustand Ihres Amazonas zu geben OpenSearch Mit der Service-Domain und den zugehörigen Integrationen können Sie in Amazon ein Dashboard erstellen CloudWatch. Sie können überprüfen, ob Ihr Operations Support Team Zugriff auf das Dashboard hat. Das [Operative Exzellenz](#) Dieser Abschnitt enthält Links zu nützlichen Tipps für die Einrichtung eines hochleistungsfähigen, belastbaren OpenSearch Dienstdomäne.
- Trainingsalarme— Stellen Sie sicher, dass Sie alle Ihre Alarme testen. Wenn Sie Amazon verwenden CloudWatch oder ein Warn-Plugin, überprüfen Sie, ob alle Integrationen, wie Amazon Simple Notification Service (Amazon SNS), Amazon Chime oder Slack, wie erwartet funktionieren. Simulieren Sie Benachrichtigungen, um zu überprüfen, ob die Benachrichtigungen korrekt an den Zielkanal gesendet werden. Vergewissern Sie sich, dass der Warnungstext hilfreiche Informationen enthält. Die Warnung könnte beispielsweise einen Link zum zugehörigen Runbook enthalten, damit Ihr Support-Team einen entsprechenden Behebungsprozess implementieren kann.

## Stufe 4 — Datenmigration

Jetzt, da Ihre Zielumgebung bereit ist, können Sie die Datenmigrationsstrategie implementieren, die Sie in der Planungsphase gewählt haben.

In diesem Abschnitt werden die Implementierungsschritte für die vier verschiedenen Muster beschrieben:

- [Aus einer Momentaufnahme aufbauen](#)
- [Aus der Quelle heraus bauen](#)
- [Neuindizierung aus der Ferne](#)
- [Logstash verwenden](#)

### 1. Aus einer Momentaufnahme aufbauen

Wenn Sie den Snapshot-Restore-Ansatz verwenden, kopieren Sie Daten aus der Elasticsearch-Quelle oder OpenSearch Cluster zum Amazon-Ziel OpenSearch Dienstdomäne.

Im Großen und Ganzen besteht der Snapshot-Wiederherstellungsprozess aus den folgenden Schritten:

1. Erstellen Sie einen Snapshot der erforderlichen Daten (Indizes) aus dem vorhandenen Cluster und laden Sie den Snapshot in einen S3-Bucket hoch.
2. Erstelle einen Amazon OpenSearch Service-Domain.
3. Gib Amazon OpenSearch Serviceberechtigungen für den Zugriff auf den Bucket und Erteilen Sie Ihrem Benutzerkonto die Erlaubnis, mit Snapshots zu arbeiten. Erstellen Sie ein Snapshot-Repository und verweisen Sie es auf Ihren Bucket.
4. Stellen Sie den Snapshot auf Amazon wieder her OpenSearch Dienstdomäne.
5. Verweisen Sie Ihre Kundenanwendungen auf Amazon OpenSearch Service-Domain.
6. Erstellen Sie ISM-Richtlinien (Index State Management) zur Konfiguration der Aufbewahrung (optional).

Snapshots sind inkrementell. Daher kann ein Snapshot inkrementell ausgeführt und wiederhergestellt werden. Mithilfe von Snapshots können Sie Daten in großen Mengen als Dateien auf einem

Speichersystem (z. B. Amazon S3) extrahieren. Anschließend können Sie diese Dateien in die Zielumgebung laden, indem Sie `_restoreAPI`-Betrieb. Dadurch entfällt die zeitaufwändige Neuindizierung und der Netzwerkverkehr wird reduziert.

## Überlegungen zu Snapshots

Wenn Sie den Snapshot-Restore-Ansatz verwenden, sollten Sie Folgendes berücksichtigen:

- Sie können nicht suchen oder neu indizieren, während ein Index wiederhergestellt wird. Sie können jedoch einen Index durchsuchen und neu indizieren, während der Snapshot erstellt wird.
- Die Quell- und Ziel-Elasticsearch oder OpenSearch Versionen müssen kompatibel sein. Ein Snapshot eines Indexes, der erstellt wurde in:
  - 5.x kann auf 6.x wiederhergestellt werden
  - 2.x kann auf 5.x wiederhergestellt werden
  - 1.x kann auf 2.x wiederhergestellt werden
- Weil das ein point-in-time Wiederherstellung des Elasticsearch oder OpenSearch Snapshot, nachfolgende Änderungen im Quell-Cluster werden nicht auf das Ziel-Amazon repliziert OpenSearch Dienstdomäne. Sie können die Aufnahme der Daten in die Elasticsearch-Quelle beenden oder OpenSearch Clustern Sie, bis die Wiederherstellung abgeschlossen ist, oder Sie können den Snapshot-Wiederherstellungsvorgang einige Male wiederholen. Da der Snapshot inkrementell ist, werden nur die Änderungen in kürzerer Zeit als bei der ersten Wiederherstellung kopiert und in der Zielumgebung wiederhergestellt. Nachdem die Wiederherstellung erfolgreich abgeschlossen wurde, verweisen Sie die Aufnahmeanwendungen auf Amazon OpenSearch Dienstdomäne.
- Das Erstellen eines Snapshots umfasst standardmäßig einen Snapshot des Clusterstatus und aller Indizes. Bei der Migration von Elasticsearch müssen Sie möglicherweise mithilfe der ISM-Funktion in der Zielumgebung entsprechende Richtlinien für den Index-Lebenszyklus erstellen OpenSearch. Elasticsearch Index Lifecycle Management (ILM) wird in Amazon nicht unterstützt OpenSearch Dienst.
- Sie können einen Snapshot nicht auf einer früheren Version von Elasticsearch wiederherstellen oder OpenSearch. Beispielsweise können Sie einen Snapshot der Versionen 7.10 bis 7.9 nicht wiederherstellen. Ebenso können Sie Snapshots von Elasticsearch 7.11 oder höher nicht auf einem Amazon wiederherstellen OpenSearch Dienstdomäne. Wenn Sie Ihre selbstverwaltete Elasticsearch-Umgebung auf Version 7.11 oder höher migriert haben, können Sie Logstash verwenden, um Daten aus dem Elasticsearch-Cluster zu laden und sie in den OpenSearch Domäne.

- Sie exportieren einen Snapshot an einen bestimmten Speicherort, der als Repository bezeichnet wird. Elasticsearch oder OpenSearch erstellt eine Reihe von Dateien im Repository. Sie können diese Dateien nicht ändern oder löschen. Dies kann zu Inkonsistenzen führen oder dazu führen, dass der Wiederherstellungsvorgang fehlschlägt.

## 2. Aus der Quelle bauen

Wie bereits beschrieben, ist das Erstellen aus der Quelle der Ansatz, bei dem Sie keine Daten aus dem aktuellen Elasticsearch migrieren oder OpenSearch Umgebung. Stattdessen erstellen Sie Indizes in der Zieldomäne direkt aus Ihrer Protokoll- oder Produktkatalog-Datenquelle oder Inhaltsquelle.

Für die Erstellung aus der Quelle stehen zwei Optionen zur Verfügung. Welche Option Sie wählen, hängt vom Datentyp Ihrer Daten ab:

- Verwendung von AWS Database Migration Service — Wenn es sich bei der Quelle Ihrer Daten um ein relationales Datenbankmanagementsystem (RDBMS) handelt und die Quelle vom AWS Database Migration Service (AWS DMS) unterstützt wird, können Sie mit AWS DMS Daten aus Ihrer Datenquelle in Ihr Amazon-Zielsystem kopieren OpenSearch Dienstdomäne. AWS DMS unterstützt die Optionen Volllast und CDC (Change Data Capture). Bei der Vollladeoption kopiert die AWS DMS-Aufgabe alle Daten aus der Quelldatenbanktabelle in ein Ziel OpenSearch Index. Sie können die Standardzuweisung verwenden oder benutzerdefinierte Zuordnungskonfigurationen bereitstellen. Bei der CDC-Option erstellt AWS DMS zunächst eine vollständige Kopie der Datensätze der Quelltable in ein Ziel OpenSearch Index. Dann erfasst es geänderte Daten (Aktualisierungen und Einfügungen) und kopiert sie in den OpenSearchIndex. Weitere Informationen finden Sie in den Blogbeiträgen [Wir stellen vor: Amazon Elasticsearch Service als Ziel im AWS Database Migration Service](#) und [Skalieren Sie Amazon Elasticsearch Service für Migrationen mit dem AWS Database Migration Service](#).
- Aus der Dokumentenquelle erstellen — Wenn es sich bei Ihrer Datenquelle nicht um ein RDBMS handelt oder sie nicht von AWS DMS unterstützt wird, müssen Sie möglicherweise eine benutzerdefinierte Lösung mit Open-Source-Tools oder einer Kombination aus Open-Source-Tools und AWS-Services erstellen. Sie müssen Ihre Quelldaten in JSON-Dokumente konvertieren, bevor sie geladen werden können OpenSearch. Wenn Sie bereits Pipelines von Ihrer Quelle zu Ihrem aktuellen Elasticsearch eingerichtet haben oder OpenSearch Umgebung, auf die Sie diese Daten-Pipelines verweisen können OpenSearch mit entsprechenden Änderungen in den Client-Bibliotheken und (falls erforderlich) Änderungen des Datenmodells in den Indizes im Amazon

OpenSearch Dienstdomäne. Beachten Sie beim Erstellen von Indizes aus der Quelle die folgenden Überlegungen:

- Der Speicherort der Dokumente — Die Dokumente könnten bereits in der AWS-Cloud, in Objektspeichern wie Amazon S3 verfügbar sein, oder sie könnten an einem lokalen Speicherort wie einem Dateisystem gespeichert sein.
- Das Format der Dokumente — Die Dokumente könnten bereits im JSON-Format vorliegen und bereit sein, in Amazon aufgenommen zu werden OpenSearchService-Domain, oder sie müssen möglicherweise bereinigt, verarbeitet und in JSON formatiert werden, bevor sie in Amazon aufgenommen werden können OpenSearch Dienstdomäne.

Die Erstellung aus der Quelle umfasst die folgenden allgemeinen Schritte:

1. Definieren Sie die Indexzuweisung und die Einstellungen im Amazon OpenSearch Dienstdomäne.
2. Extrahieren Sie Daten aus der Dokumentenquelle und kopieren Sie sie in einen Objektspeicher wie Amazon S3. Sie können ein Open-Source-Tool (z. B. Logstash), einen AWS-Serviceclient (z. B. Amazon Kinesis Agent), ein kommerzielles Tool eines Drittanbieters oder ein benutzerdefiniertes Programm verwenden.
3. Konfigurieren Sie ein Open-Source-Tool (z. B. Logstash oder Fluent Bit) oder einen nativen AWS-Service (z. B. AWS Lambda oder AWS DMS), um Daten in JSON-Dokumente zu konvertieren und sie regelmäßig oder kontinuierlich aus dem Objektspeicher in den Amazon zu laden OpenSearch Dienstdomäne.

Weitere Informationen finden Sie unter [Streaming-Daten werden in Amazon geladen OpenSearch Dienst](#).

### 3. Neuindizierung aus der Ferne

In diesem Fall die Indizes der selbstverwalteten Quelle Elasticsearch oder OpenSearchCluster werden in den Amazon migriert OpenSearch Service-Domain unter Verwendung der [API-Vorgang für das Dokument neu indizieren](#). Sie können den API-Vorgang „Dokument neu indizieren“ verwenden, um einen Index aus einem vorhandenen Elasticsearch zu erstellen oder OpenSearch Index. Der vorhandene Index kann sich in demselben Cluster befinden, in dem Sie den Neuindizierungsvorgang ausführen, oder er kann sich in einem Remote-Cluster befinden. Amazon OpenSearch Der Service unterstützt die Verwendung des API-Vorgangs zur Neuindizierung von Dokumenten mit Remote-Clustern. Sie können von einem Index in einem selbstverwalteten Elasticsearch zu einem Index in Amazon neu indizieren OpenSearch Dienst.

Remote Reindex unterstützt Elasticsearch 1.5 und höher für den Remote-Elasticsearch-Cluster und Amazon OpenSearch Service 6.7 und höher für die lokale Domain. Weitere Informationen finden Sie im Blogbeitrag [Migrieren Sie Daten mithilfe der Remote-Neuindizierung zu Amazon ES](#). Der Blogbeitrag bezieht sich auf Amazon Elasticsearch, aber die Anleitung gilt für Amazon OpenSearch Servicedomänen gleichermaßen.

## 4. Logstash verwenden

[Log-Stash](#) ist ein Open-Source-Datenverarbeitungstool, das Daten aus der Quelle sammeln, transformieren oder filtern und Daten an ein oder mehrere Ziele senden kann. Um Daten in den Amazonas zu schreiben OpenSearch In der Service-Domain bietet Logstash die folgenden Plugins:

- logstash-input-elasticsearch
- logstash-input-opensearch
- logstash-output-opensearch

Weitere Informationen finden Sie unter [Daten werden in Amazon geladen OpenSearch Service mit Logstash](#) und der OpenSearch Blogbeitrag [Wir stellen vor logstash-input-opensearch Plugin für OpenSearch](#).

## Stufe 5 — Umstellung

In dieser Phase werden verschiedene Ansätze erörtert, die Sie verwenden können, um von Ihrem aktuellen Elasticsearch abzuweichen oder OpenSearch Umgebung zum Ziel-Amazon OpenSearch Dienstdomäne. Die Umstellung kann in zwei Schritten erfolgen:

- Richten Sie einen Datensynchronisierungsmechanismus ein, um die Zielumgebung mit der Quelle zu synchronisieren.
- Führen Sie den Wechsel von der aktuellen Umgebung zur Zielumgebung mit oder ohne Ausfallzeiten durch.

### Datensynchronisierung

Für jedes System, das kontinuierlich Daten empfängt, kann es für die Datenmigration erforderlich sein, dass Sie während der Migration keine neuen Daten mehr empfangen und die Migration in einem Wartungsfenster (mit möglichen Ausfallzeiten) ausführen. Wenn Sie sich keine Ausfallzeiten leisten können, können Sie Änderungen erfassen, nachdem Sie die Migration eingeleitet haben. Sie spielen die Änderungen auf dem Ziel erneut ab, um es auf dem neuesten Stand zu halten und mit der Quelle zu synchronisieren, bis Sie die Übernahme durchführen. In den folgenden Abschnitten werden verschiedene Möglichkeiten beschrieben, wie Sie Quelle und Ziel synchronisieren können.

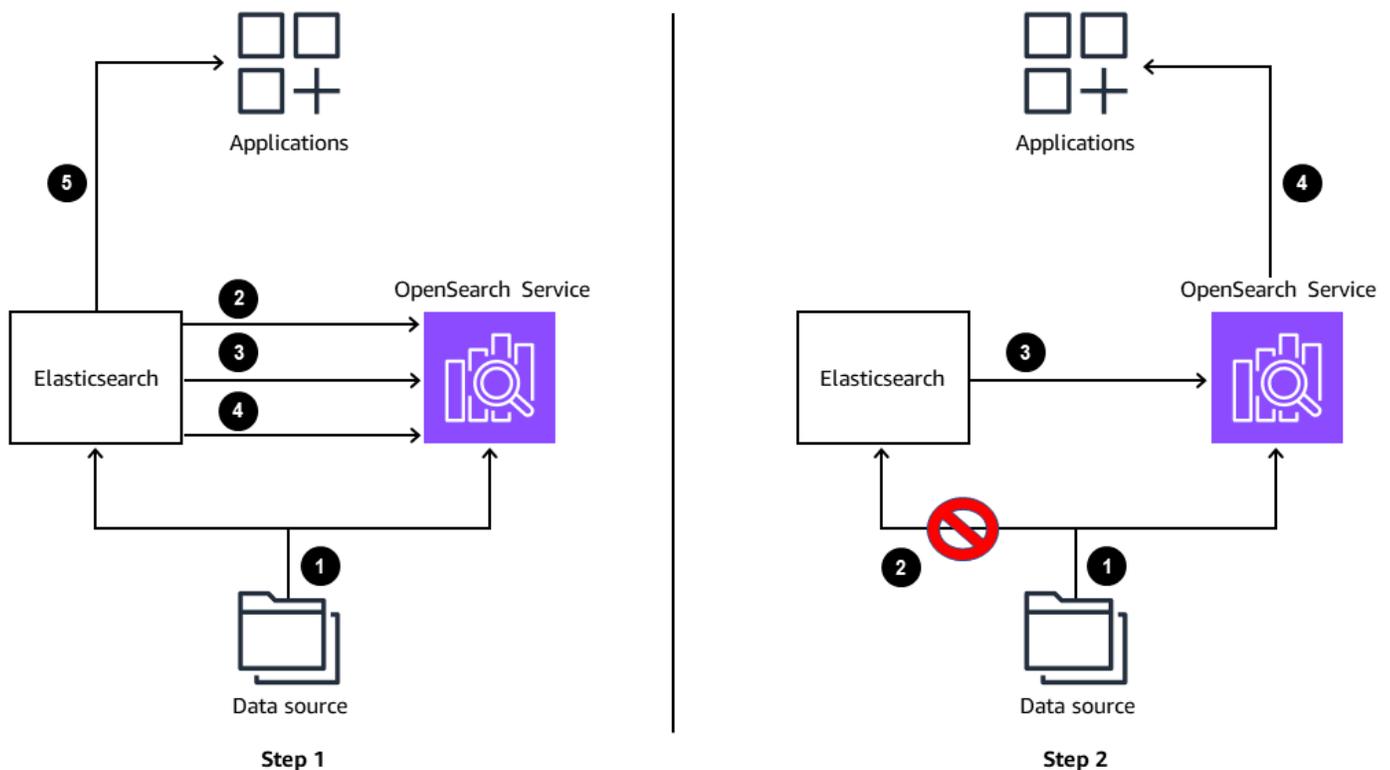
#### Analyse-Workloads protokollieren

Für Workloads zur Protokollanalyse können Sie eine Aktualisierungssynchronisierung auf folgende Weise durchführen:

- Sie können zwei Umgebungen nebeneinander ausführen, bis der Aufbewahrungszeitraum und die Datenaufnahme sowohl in der aktuellen Umgebung als auch in der Zielumgebung abgeschlossen sind. Irgendwann beschließen Sie, Ihre Anwendungen zu überschneiden und auf die neue Umgebung auszurichten. Manchmal können Sie neue Daten aus den Protokoll- oder Dokumentquellen sowohl in den vorhandenen Cluster als auch in das Ziel aufnehmen OpenSearch Serviceumgebungen. Anschließend können Sie die älteren Daten in der Zielumgebung wieder auffüllen, indem Sie sie aus der aktuellen Umgebung kopieren. In jedem Fall müssen Sie sicherstellen, dass Ihre Daten keine Lücken aufweisen, die sich auf Ihre Benutzer auswirken könnten.
- Vor der Datenmigration können Sie entscheiden, ob Sie die Datenaufnahme in die bestehende Umgebung unterbrechen möchten. Dieser Ansatz bedeutet jedoch, dass Ihre Benutzer

möglicherweise nicht in der Lage sind, die neuesten oder geänderten Daten in Ihrer vorhandenen Umgebung zu durchsuchen, bis Ihre Datenmigration abgeschlossen ist. Nach Abschluss der Datenmigration können Sie Ihre Datenaufnahme auf die Zielumgebung ausrichten und Ihre Anwendungen und Clients auf die Zielumgebung umstellen. Das bedeutet, dass keine neuen Daten verfügbar sind, bis die Migration abgeschlossen ist. Das System wird jedoch weiterhin für die Suche verfügbar sein. Sie sollten über die Möglichkeit verfügen, Quellprotokolle und -daten in Ihrer Quelle zu speichern, bis die neue Umgebung verfügbar ist.

- Sie können die aktuelle Log Analytics-Engine weiter verwenden, bis Ihr erster Datendurchlauf migriert ist. Anschließend füllen Sie die verbleibenden Daten, die seit Beginn des ersten Durchlaufs erzeugt wurden, erneut auf. Unter der Annahme, dass die verbleibenden Daten viel kleiner sind als beim ersten Durchlauf, können Sie die Aufnahme unterbrechen, während Ihre verbleibenden Daten synchronisiert sind, da die Synchronisation möglicherweise nur ein paar Minuten oder einige Stunden dauert. Sie können mit diesem Ansatz auch einige Durchläufe durchführen, bis das Synchronisierungsfenster klein genug ist, um die Aufnahme von der Quell- zur Zielumgebung zu unterbrechen und zur Zielumgebung überzugehen, ohne dass Ihre Benutzer beeinträchtigt werden. Das folgende Diagramm zeigt die Verwendung von inkrementellem Snapshot und Wiederherstellung zum Aktualisieren oder Synchronisieren von Daten.



## Schritt 1

1. Daten fließen von der Quelle über die Datenerfassungspipeline zur aktuellen Elasticsearch-Umgebung und zum Amazonasgebiet OpenSearchDienstdomäne.
2. Der erste Durchgang dauert am längsten, um von Elasticsearch zu Amazon zu wechseln OpenSearch Dienstdomäne.
3. Das erste Update oder die erste Synchronisation nimmt weniger Zeit in Anspruch.
4. Der zweite Update- oder Synchronisierungsdurchgang benötigt am wenigsten Zeit.
5. Die Daten fließen weiterhin von Elasticsearch zu den Anwendungen.

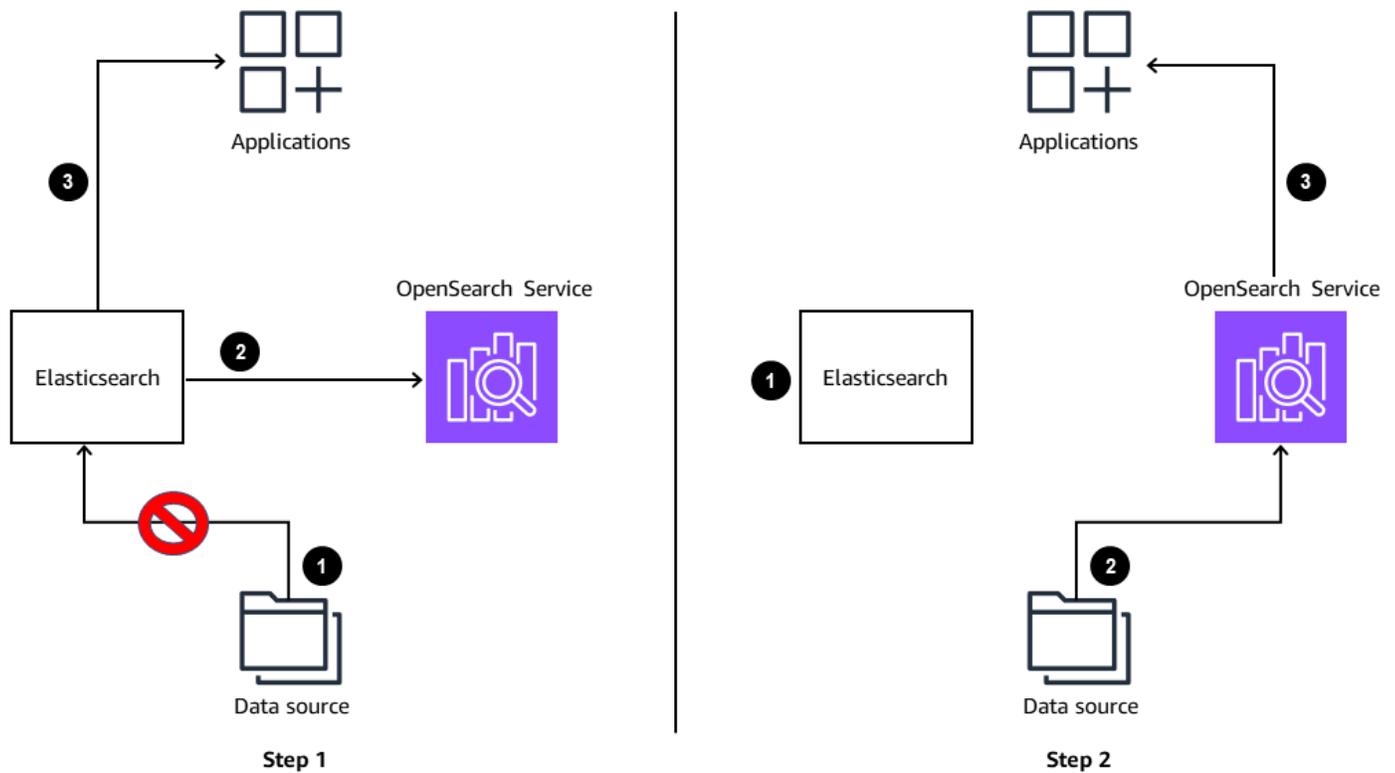
## Schritt 2

1. Die Daten fließen von der Quelle über die Datenerfassungspipeline zur OpenSearch Dienstdomäne.
2. Die Aufnahme in die aktuelle Elasticsearch-Umgebung wurde gestoppt.
3. Der letzte Update- oder Synchronisierungsdurchgang nimmt am wenigsten Zeit in Anspruch.
4. Daten fließen von OpenSearch Service für die Anwendungen.

## Suchen Sie nach Workloads

Bei den drei zuvor erläuterten Ansätzen müssen Sie sicherstellen, dass alle Daten auf Ihrem Ziel auf dem neuesten Stand sind, bevor Sie die Umstellung durchführen. Bei Such-Workloads können Sie die folgenden Vorschläge zur Aktualisierung oder Synchronisierung in Betracht ziehen:

- Bei Such-Workloads unterbrechen Sie in der Regel die Aufnahme von der Quelle bis zur aktuellen Umgebung. Sie kopieren alle Ihre Daten aus der aktuellen Umgebung in die Zielumgebung und richten einen CDC-Mechanismus (Change Data Capture) ein, mit dem festgestellt werden kann, welche Daten sich seit Beginn der Migration geändert haben. Anschließend kopieren Sie die geänderten Daten auf Amazon OpenSearchUmgebung. In den meisten Fällen ist in den Datenerfassungspipelines der Suchanwendung bereits ein CDC-Mechanismus integriert. In der Regel geht es darum, Ihre Pipeline auf die neue Umgebung zu verweisen, nachdem die Daten aus der aktuellen Umgebung migriert wurden. Das folgende Diagramm zeigt, wie ein Index für Suchanwendungsfälle vollständig aus der Quelle erstellt wird.



### Schritt 1

1. Die Aufnahme in die aktuelle Elasticsearch-Umgebung wurde angehalten.
2. Daten werden kopiert von ElasticSearch zum OpenSearch Dienstdomäne.
3. Die Daten fließen weiterhin von ElasticSearch zu den Anwendungen.

### Schritt 2

1. Die Elasticsearch-Umgebung ist nicht mehr mit der Datenquelle oder den Anwendungen verbunden.
  2. Daten zur Erfassung von Änderungsdaten (CDC) werden in die Pipeline aufgenommen und fließen in die OpenSearch Dienstdomäne.
  3. Daten fließen aus dem OpenSearch Dienstdomäne zu den Anwendungen.
- Bei einigen Such-Workloads müssen nur vollständige Daten aus der Quelldatenbank oder Datenquelle in die neue Datenbank geladen werden OpenSearch Serviceumgebung. Nach Abschluss des Ladevorgangs können die Client-Anwendungen auf die neue Umgebung umgestellt werden. Dies ist der einfachste Weg, um die Migration von Such-Workloads zu erreichen.

## Tauschen oder überschneiden

Der letzte Schritt auf dem Weg zur Migration ist die Umstellung auf die neue Umgebung. Dies ist eine der kritischen Phasen. Zu diesem Zeitpunkt sind Sie bereit, live zu gehen. Sie haben die Daten synchronisiert und auf dem neuesten Stand, Sie haben Überwachung und Benachrichtigungen konfiguriert, Ihre Runbooks sind auf dem neuesten Stand und Sie sind bereit, auf die neue Umgebung umzustellen. Sie müssen sicherstellen, dass die Datenaufnahme normal erfolgt und dass die Messwerte aus Ihrer neuen Umgebung korrekt sind. In dieser Phase planen und führen Sie die Trennung der Client-Verbindungen von Ihren bestehenden Elasticsearch- oder OpenSearch Cluster zum neuen Amazon OpenSearch Dienstdomäne. Beachten Sie alle Änderungen an der Clientbibliothek, die möglicherweise erforderlich sind. Zu diesem Zeitpunkt sollten Sie alle Ihre Client-Funktionen bei Amazon getestet haben OpenSearch Service in Ihren niedrigeren Umgebungen, um Kompatibilität und Leistung zu überprüfen.

Wenn Sie über eine Client-Anwendung verfügen, die auf die neue Umgebung verweisen muss, aktualisieren Sie den DNS-Eintrag von der alten Umgebung auf die neue Umgebung. Überwachen Sie anschließend das Anwendungsverhalten genau, um sicherzustellen, dass Ihre Benutzer die richtige Benutzererfahrung erhalten.

Generell gilt: Wenn Sie die Richtlinien in diesem Dokument befolgt haben, können Sie sicher auf den Umstieg umsteigen. Wir empfehlen Ihnen jedoch, Ihre Quellumgebung auf dem neuesten Stand zu halten, damit sie als Ausweichlösung dienen kann, falls Probleme mit der neuen Umgebung auftreten. Einige AWS-Kunden betreiben beide Umgebungen nach dem Austausch noch einige Wochen, bevor sie die ältere Umgebung außer Betrieb nehmen. Wir empfehlen Ihnen, eine Strategie zu wählen, die Ihren Anforderungen an die Geschäftskontinuität entspricht.

## Stufe 6 — Operative Exzellenz

Die Amazon OpenSearch Service-Dokumentation enthält einen eigenen Abschnitt mit [bewährten Methoden für den Betrieb](#). Zu den Themen gehören die folgenden:

- [Überwachung und Alarmierung](#)
- [Shard-Strategie](#)
- [Stabilität](#)
- [Leistung](#)
- [Sicherheit](#)
- [Kostenoptimierung](#)
- [Dimensionierung von Amazon OpenSearch Service-Domains](#)
- [Petabyte-Skala in Amazon Service OpenSearch](#)
- [Dedizierte Masterknoten in Amazon OpenSearch Service](#)
- [Empfohlene CloudWatch Alarme für Amazon OpenSearch Service](#)

Wir empfehlen Ihnen, die Anweisungen in der Dokumentation zu befolgen, um Ihre neu migrierte Umgebung zu betreiben.

# Schlussfolgerung

Amazon OpenSearch Service nimmt Ihnen die undifferenzierte Arbeit ab, die für die Entwicklung und den Betrieb von selbstverwaltetem Elasticsearch erforderlich ist, oder OpenSearch Cluster. Wenn Sie eine Migration zu Amazon in Betracht ziehen OpenSearch Service, Sie können den in diesem Leitfaden beschriebenen Prozess verwenden, um eine Migrationsstrategie zu planen und auszuwählen, die für Ihre Situation geeignet ist.

Migrationen können so einfach sein wie das Erstellen eines Snapshots aus einem selbstverwalteten Cluster und dessen Wiederherstellung in Amazon OpenSearch Service Domain, oder sie können genauso komplex sein wie das Testen aller vorhandenen Funktionen und Integrationen. Dieser Leitfaden enthält Informationen, anhand derer die Teams für Migrationsprojekte sicherstellen können, dass sie alle Aspekte einer Migration abgedeckt haben, und um eine solide Implementierungsstrategie zu entwickeln.

Amazon OpenSearch Die Servicedokumentation enthält einen eigenen Abschnitt zu [Bewährte betriebliche Verfahren](#). Wir empfehlen Ihnen, die Anweisungen in der Dokumentation zu befolgen, um Ihre neu migrierte Umgebung zu betreiben.

# Ressourcen

- [Index-Snapshots in Amazon erstellen OpenSearch Dienst](#)
- [Verwenden Sie Amazon S3, um ein einzelnes Amazon zu speichern OpenSearch Serviceindex](#)(Blogbeitrag)
- [Snapshot und Wiederherstellung mit Elasticsearch](#)(Elasticsearch-Dokumentation)
- [S3-Repository-Plugin](#)(Elasticsearch-Dokumentation)
- [Elasticsearch-Repository-Einstellungen: Empfohlene S3-Berechtigungen](#)(Elasticsearch-Dokumentation)
- [Elasticsearch-Client-Einstellungen](#)(Elasticsearch-Dokumentation)

# Beitragende Faktoren

## Mitwirkende

Zu den Mitwirkenden an diesem Dokument gehören:

- Muhammad Ali, Schulleiter OpenSearch Architekt für Lösungen
- Gene Alpert, Senior Technischer Kundenbetreuer — Analytik
- Jon Handler, Senior Principal Solutions Architect
- Prashant Agrawal senior OpenSearch Architekt für spezialisierte Lösungen
- Ina Felsheim, Leiterin Produktmarketing
- Sung-il Kim, Senior Architect für Analyselösungen
- Hajer Bouafif, OpenSearch Architekt für Lösungen
- Kevin Fallis, Schulleiter OpenSearch Architekt für spezialisierte Lösungen
- Muthu Pitchaimani senior OpenSearch Architekt für spezialisierte Lösungen
- Kunal Kusoorkar, Mgr. , OpenSearch Architekt für Lösungen
- Imtiaz Sayed, Pr. Technischer Leiter von Analytics Solutions Architect
- Soujanya Konka, Senior Solutions Architect
- Marc Clark, Mgr. , OpenSearch Spezialist
- Bob Taylor senior OpenSearch Spezialist
- Aneesh Chandra PN, leitender Architekt für Analyselösungen, Gesundheitswesen und Biowissenschaften

# 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
<a href="#">Erste Veröffentlichung</a>	—	28. August 2023

# AWS Glossar zu präskriptiven Leitlinien

Im Folgenden finden Sie häufig verwendete Begriffe in Strategien, Leitfäden und Mustern von AWS Prescriptive Guidance. Um Einträge vorzuschlagen, verwenden Sie bitte den Link Feedback geben am Ende des Glossars.

## Zahlen

### 7 Rs

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

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

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

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

## A

### ABAC

Siehe [attributbasierte](#) Zugriffskontrolle.

### abstrahierte Dienste

Weitere Informationen finden Sie unter [Managed Services](#).

### ACID

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

### Aktiv-Aktiv-Migration

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

### Aktiv-Passiv-Migration

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

### Aggregatfunktion

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

## AI

Siehe [künstliche Intelligenz](#).

## AIOps

Siehe [Operationen mit künstlicher Intelligenz](#).

## Anonymisierung

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

## Anti-Muster

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

## Anwendungssteuerung

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

## Anwendungsportfolio

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

## künstliche Intelligenz (KI)

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

## Operationen mit künstlicher Intelligenz (AIOps)

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

## Asymmetrische Verschlüsselung

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

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

### Atomizität, Konsistenz, Isolierung, Haltbarkeit (ACID)

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

### Attributbasierte Zugriffskontrolle (ABAC)

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

### autoritative Datenquelle

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

### Availability Zone

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

### AWS Framework für die Cloud-Einführung (AWS CAF)

Ein Framework mit Richtlinien und bewährten Verfahren, das Unternehmen bei der Entwicklung eines effizienten und effektiven Plans für den erfolgreichen Umstieg auf die Cloud unterstützt. AWS 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, die als bösartige Bots bezeichnet werden, 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 für die AWS Cloud-Einführung](#).

### Bereitstellung auf Kanaren

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

### CCoE

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

### CDC

Siehe [Erfassung von Änderungsdaten](#).

### Erfassung von Datenänderungen (CDC)

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

### Chaos-Technik

Absichtliches Einführen von Ausfällen oder Störungsereignissen, um die Widerstandsfähigkeit eines Systems zu testen. Sie können [AWS Fault Injection Service \(AWS FIS\)](#) verwenden, um Experimente durchzuführen, die Ihre AWS Workloads stressen, 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-Kompetenzzentrum (CCoE)

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

## Cloud Computing

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

## Cloud-Betriebsmodell

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

## Phasen der Einführung der Cloud

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

- Projekt – Durchführung einiger Cloud-bezogener Projekte zu Machbarkeitsnachweisen und zu Lernzwecken
- Fundament – Grundlegende Investitionen tätigen, um Ihre Cloud-Einführung zu skalieren (z. B. Einrichtung einer Landing Zone, Definition eines CCoE, Einrichtung eines Betriebsmodells)
- Migration – Migrieren einzelner Anwendungen

- 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 AWS CodeCommit. Jede Version des Codes wird Zweig genannt. In einer Microservice-Struktur ist jedes Repository einer einzelnen Funktionalität gewidmet. Eine einzelne CI/CD-Pipeline kann mehrere Repositorien verwenden.

## Kalter Cache

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

## Kalte Daten

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

## Computer Vision (CV)

Ein Bereich der [KI](#), der maschinelles Lernen nutzt, um Informationen aus visuellen Formaten wie digitalen Bildern und Videos zu analysieren und zu extrahieren. AWS Panorama Bietet beispielsweise Geräte an, die CV zu lokalen Kameranetzwerken hinzufügen, und Amazon SageMaker stellt Bildverarbeitungsalgorithmen für CV bereit.

## 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.

### betroffene Person

Eine Person, deren Daten gesammelt und verarbeitet werden.

## Data Warehouse

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

## Datenbankdefinitionssprache (DDL)

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

## Datenbankmanipulationssprache (DML)

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

## DDL

Siehe [Datenbankdefinitionssprache](#).

## Deep-Ensemble

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

## Deep Learning

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

## defense-in-depth

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

## delegierter Administrator

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

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

## Bereitstellung

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

## Entwicklungsumgebung

Siehe [Umgebung](#).

## Detektivische Kontrolle

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

## Abbildung des Wertstroms in der Entwicklung (DVSM)

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

## digitaler Zwilling

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

## Maßtabelle

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

## Katastrophe

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

## Notfallwiederherstellung (DR)

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

## DML

Siehe Sprache zur [Datenbankmanipulation](#).

## Domainorientiertes Design

Ein Ansatz zur Entwicklung eines komplexen Softwaresystems, bei dem seine Komponenten mit sich entwickelnden Domains oder 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](#).

## 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.

## Verschlüsselung

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

## Verschlüsselungsschlüssel

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

## Endianismus

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

## Endpunkt

[Siehe](#) Service-Endpunkt.

## Endpunkt-Services

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

## Unternehmensressourcenplanung (ERP)

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

## Envelope-Verschlüsselung

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

## Umgebung

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

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

## Epics

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

## ERP

Siehe [Enterprise Resource Planning](#).

## Explorative Datenanalyse (EDA)

Der Prozess der Analyse eines Datensatzes, um seine Hauptmerkmale zu verstehen. Sie sammeln oder aggregieren Daten und führen dann erste Untersuchungen durch, um Muster zu

finden, Anomalien zu erkennen und Annahmen zu überprüfen. EDA wird durchgeführt, indem zusammenfassende Statistiken berechnet und Datenvisualisierungen erstellt werden.

## F

### Faktentabelle

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

### schnell scheitern

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

### Grenze zur Fehlerisolierung

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

### Feature-Zweig

Siehe [Zweig](#).

### Features

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

### Bedeutung der Feature

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

## Featuretransformation

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

## FGAC

Weitere Informationen finden Sie unter [detaillierter 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.

# G

## 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.

## Greenfield-Strategie

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

## Integritätsschutz

Eine allgemeine Regel, die dabei hilft, Ressourcen, Richtlinien und die Einhaltung von Vorschriften in allen Organisationseinheiten (OUs) zu regeln. Präventiver Integritätsschutz setzt Richtlinien durch, um die Einhaltung von Standards zu gewährleisten. Sie werden mithilfe von Service-Kontrollrichtlinien und IAM-Berechtigungsgrenzen implementiert. Detektivischer Integritätsschutz erkennt Richtlinienverstöße und Compliance-Probleme und generiert Warnmeldungen zur Abhilfe. Sie werden mithilfe von AWS Config, AWS Security Hub, 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.

## Homogene Datenbankmigration

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

## heiße Daten

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

## Hotfix

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

## Hypercare-Phase

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

## I

## IaC

Sehen Sie sich [Infrastruktur als Code](#) an.

## Identitätsbasierte Richtlinie

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

## Leerlaufanwendung

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

## IIoT

Siehe [Industrielles Internet der Dinge](#).

## unveränderliche Infrastruktur

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

## Eingehende (ingress) VPC

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

## Inkrementelle Migration

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

## Industrie 4.0

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

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

## Inspektions-VPC

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

## Internet of Things (IoT)

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

## Interpretierbarkeit

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

## IoT

[Siehe Internet der Dinge.](#)

## IT information library (ITIL, IT-Informationsbibliothek)

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

## T service management (ITSM, IT-Servicemanagement)

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

### BIS

Weitere Informationen finden Sie in der [IT-Informationsbibliothek](#).

### ITSM

Siehe [IT-Servicemanagement](#).

## L

### Labelbasierte Zugangskontrolle (LBAC)

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

### Landing Zone

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

### Große Migration

Eine Migration von 300 oder mehr Servern.

### SCHWARZ

Weitere Informationen finden Sie unter [Label-basierte Zugriffskontrolle](#).

### Geringste Berechtigung

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

## Lift and Shift

Siehe [7 Rs](#).

## Little-Endian-System

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

## Niedrigere Umgebungen

[Siehe Umwelt](#).

# M

## Machine Learning (ML)

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

## Hauptzweig

Siehe [Filiale](#).

## Malware

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

## verwaltete Dienste

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

## Manufacturing Execution System (MES)

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

## MAP

Siehe [Migration Acceleration Program](#).

## Mechanismus

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

## Mitgliedskonto

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

## DURCHEINANDER

Siehe [Manufacturing Execution System](#).

## Message Queuing-Telemetrietransport (MQTT)

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

## Microservice

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

## Microservices-Architekturen

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

[Weitere Informationen finden Sie unter Origin Access Control](#).

### OAI

Siehe [Zugriffsidentität von Origin](#).

### COM

Siehe [organisatorisches Change-Management](#).

## Offline-Migration

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

OI

Siehe [Betriebsintegration](#).

OLA

Siehe Vereinbarung auf [operativer Ebene](#).

## Online-Migration

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

OPC-UA

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

## Offene Prozesskommunikation — Einheitliche Architektur (OPC-UA)

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

## Vereinbarung auf Betriebsebene (OLA)

Eine Vereinbarung, in der kargestellt 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 [Erstellen eines Pfads für eine Organisation](#).

### 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.

## ODER

Siehe [Überprüfung der Betriebsbereitschaft](#).

## NICHT

Siehe [Betriebstechnologie](#).

## Ausgehende (egress) VPC

In einer Architektur AWS mit mehreren Konten eine VPC, die Netzwerkverbindungen verarbeitet, die von einer Anwendung aus initiiert werden. Die [AWS -Referenzarchitektur für die Sicherheit](#) empfiehlt, Ihr Netzwerkkonto mit eingehenden und ausgehenden VPCs und Inspektions-VPCs einzurichten, um die bidirektionale Schnittstelle zwischen Ihrer Anwendung und dem Internet zu schützen.

## P

### Berechtigungsgrenze

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

### Polyglotte Beharrlichkeit

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

### Portfoliobewertung

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

### predicate

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

### Prädikat Pushdown

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

### Präventive Kontrolle

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

## Prinzipal

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

## Datenschutz durch Design

Ein Ansatz in der Systemtechnik, der den Datenschutz während des gesamten Engineering-Prozesses berücksichtigt.

## Privat gehostete Zonen

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

## proaktive Steuerung

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

## Produktlebenszyklusmanagement (PLM)

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

## Produktionsumgebung

Siehe [Umgebung](#).

## Speicherprogrammierbare Steuerung (SPS)

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

## 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.

## veröffentlichen/abonnieren (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 \(RACI\)](#).

### 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. Dies bestimmt, was als akzeptabler Datenverlust zwischen dem letzten Wiederherstellungspunkt und der Betriebsunterbrechung angesehen wird.

## 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](#).

## Drehung

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

## Zugriffskontrolle für Zeilen und Spalten (RCAC)

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

## RPO

Siehe [Recovery Point Objective](#).

## RTO

Siehe [Ziel der Wiederherstellungszeit](#).

## Runbook

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

# S

## SAML 2.0

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

## SCADA

Siehe [Aufsichtskontrolle und Datenerfassung](#).

## SCP

Siehe [Richtlinie zur Dienstkontrolle](#).

## Secret

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

## Sicherheitskontrolle

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

## Härtung der Sicherheit

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

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

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

## Automatisierung von Sicherheitsreaktionen

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

## Serverseitige Verschlüsselung

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

## Service-Kontrollrichtlinie (SCP)

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

## Service-Endpunkt

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

## Service Level Agreement (SLA)

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

## Service-Level-Indikator (SLI)

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

## Service-Level-Ziel (SLO)

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

## 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, wohingegen 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.

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

## Stammbasierter Workflow

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

## Vertrauenswürdiger Zugriff

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

## Optimieren

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

## Zwei-Pizzen-Team

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

# U

## Unsicherheit

Ein Konzept, das sich auf ungenaue, unvollständige oder unbekannte Informationen bezieht, die die Zuverlässigkeit von prädiktiven ML-Modellen untergraben können. Es gibt zwei Arten von Unsicherheit: Epistemische Unsicherheit wird durch begrenzte, unvollständige Daten verursacht, wohingegen aleatorische Unsicherheit durch Rauschen und Randomisierung verursacht wird, die in den Daten liegt. 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, mit der Sie den Datenverkehr mithilfe von privaten IP-Adressen weiterleiten können. Weitere Informationen finden Sie unter [Was ist VPC-Peering?](#) in der Amazon-VPC-Dokumentation.

## Schwachstelle

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

## W

### Warmer Cache

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

### warme Daten

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

### Fensterfunktion

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

### Workload

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

### Workstream

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

### WURM

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

### WQF

Weitere Informationen finden Sie unter [AWS Workload Qualification Framework](#).

## 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.

### 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.