



Backup- und Wiederherstellungsansätze auf AWS

AWS Präskriptive Leitlinien



AWS Präskriptive Leitlinien: Backup- und Wiederherstellungsansätze auf AWS

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
Warum AWS als Datenschutzplattform verwenden?	2
Gezielte Geschäftsergebnisse	4
AWS Dienste auswählen	5
Entwicklung einer Backup- und Wiederherstellungslösung	8
AWS Backup	9
Amazon S3	11
Verwenden von Amazon-S3-Speicherklassen	11
Standard-S3-Buckets erstellen	13
Verwenden der Amazon S3 S3-Versionierung	13
Sicherung und Wiederherstellung von benutzerdefinierten Konfigurationsdateien für AMIs	13
Benutzerdefiniertes Sichern und Wiederherstellen	14
Sicherung von Backup-Daten	14
Amazon EC2 mit EBS-Volumes	16
Amazon EC2-Backup und -Wiederherstellung	18
AMIs oder Snapshots	18
Server-Volumes	20
Separate Server-Volumes	21
Instance-Speicher-Volumes	21
Markieren und Durchsetzen von Standards	22
Erstellen von EBS-Volume-Backups	23
Vorbereiten eines EBS-Volumes	23
Erstellen von Snapshots über die Konsole	25
Erstellen von AMIs	25
Amazon Data Lifecycle Manager	26
AWS Backup	27
Multi-Volume-Backups	27
Schützen von Backups	29
Archivieren von Snapshots	30
Automatisieren der Snapshot- und AMI-Erstellung	30
Wiederherstellen eines Volumes oder einer Instance	31
Wiederherstellen von Dateien und Verzeichnissen aus EBS-Snapshots	32
Wiederherstellen eines EBS-Volumes aus einem Amazon-EBS-Snapshot	32
Erstellen oder Wiederherstellen einer EC2-Instance aus einem EBS-Snapshot	34

Wiederherstellen einer laufenden Instance aus einem AMI	35
Backup und Wiederherstellung vor Ort	37
File Gateway	38
Volume Gateway	38
Tape Gateway	39
Backup und Wiederherstellung von Anwendungen	41
Cloud-native AWS Dienste	42
Amazon RDS	42
Verwenden von DNS-CNAME	43
DynamoDB	45
Hybride Architekturen	47
Verlagerung zentralisierter Backup-Management-Lösungen	48
Notfallwiederherstellung	50
On-Premises-DR zu AWS	50
DR für cloudnative Workloads	52
DR in einer einzigen Availability Zone	53
DR bei einem regionalen Ausfall	54
Backups bereinigen	55
Häufig gestellte Fragen	56
Welchen Backup-Zeitplan sollte ich wählen?	56
Muss ich Backups in meinen Entwicklungskonten erstellen?	56
Kann ich Anwendungen aktualisieren und ein EBS-Volume weiterhin verwenden, während ein Snapshot erstellt wird, ohne dass dies Auswirkungen hat?	56
Nächste Schritte	57
Ressourcen	58
Dokumentverlauf	60
Glossar	64
#	64
A	65
B	68
C	70
D	73
E	78
F	80
G	81
H	82

I	83
L	86
M	87
O	91
P	94
Q	97
R	97
S	100
T	104
U	106
V	106
W	107
Z	108
.....	cix

Backup- und Wiederherstellungsansätze auf AWS

Khurram Nizami, Amazon Web Services (AWS)

Juni 2024 (Geschichte [der Dokumente](#))

In diesem Handbuch wird beschrieben, wie Sicherungs- und Wiederherstellungsansätze mithilfe von Amazon Web Services (AWS) -Diensten für lokale, cloudnative und hybride Architekturen implementiert werden. Diese Ansätze bieten niedrigere Kosten, eine höhere Skalierbarkeit und eine längere Lebensdauer, um die Recovery Time Objective (RTO), Recovery Point Objective (RPO) und Compliance-Anforderungen zu erfüllen.

Dieser Leitfaden richtet sich an technische Führungskräfte, die für den Schutz von Daten in ihren Unternehmens-IT- und Cloud-Umgebungen verantwortlich sind.

Dieser Leitfaden behandelt verschiedene Backup-Architekturen (cloudnative Anwendungen, hybride und lokale Umgebungen). Es deckt auch die zugehörigen Amazon Web Services (AWS) -Services ab, mit denen skalierbare und zuverlässige Datenschutzlösungen für die nicht unveränderlichen Komponenten Ihrer Architektur erstellt werden können.

Ein weiterer Ansatz besteht darin, Ihre Workloads zu modernisieren, um unveränderliche Architekturen zu verwenden und so den Bedarf an Backup und Wiederherstellung von Komponenten zu reduzieren. AWS bietet eine Reihe von Services zur Implementierung unveränderlicher Architekturen und zur Reduzierung des Backup- und Wiederherstellungsbedarfs, darunter:

- Serverlos mit AWS Lambda
- Container mit Amazon Elastic Container Service (Amazon ECS), Amazon Elastic Kubernetes Service (Amazon EKS) und AWS Fargate
- Amazon Machine Images (AMIs) mit Amazon Elastic Compute Cloud (Amazon EC2)

Da sich das Wachstum von Unternehmensdaten beschleunigt, wird die Aufgabe, sie zu schützen, immer schwieriger. Fragen zur Haltbarkeit und Skalierbarkeit von Backup-Ansätzen sind alltäglich, darunter diese: Wie hilft die Cloud dabei, meine Sicherungs- und Wiederherstellungsanforderungen zu erfüllen?

Dieser Leitfaden umfasst die folgenden Themen:

- [Auswahl von AWS Diensten für den Datenschutz](#)

- [Entwicklung einer Backup- und Wiederherstellungslösung](#)
- [Backup und Wiederherstellung mit AWS Backup](#)
- [Backup und Wiederherstellung mit Amazon S3](#)
- [Backup und Wiederherstellung für Amazon EC2 mit EBS-Volumes](#)
- [Backup und Wiederherstellung von der lokalen Infrastruktur auf AWS](#)
- [Backup und Wiederherstellung von Anwendungen von AWS zu Ihrem Rechenzentrum](#)
- [Backup und Wiederherstellung von Cloud-nativen AWS Diensten](#)
- [Backup und Recovery für Hybridarchitekturen](#)
- [Disaster Recovery mit AWS](#)
- [Backups bereinigen](#)

Warum AWS als Datenschutzplattform verwenden?

AWS ist eine sichere, leistungsstarke, flexible, geldsparende easy-to-use Cloud-Computing-Plattform. AWS kümmert sich um die undifferenzierte Schwerarbeit, die für die Erstellung, Implementierung und Verwaltung skalierbarer Sicherungs- und Wiederherstellungslösungen erforderlich ist.

Die Nutzung im AWS Rahmen Ihrer Datenschutzstrategie bietet viele Vorteile:

- **Haltbarkeit:** Amazon Simple Storage Service (Amazon S3) und S3 Glacier Deep Archive sind für eine Haltbarkeit von 99,999999999 Prozent (11 Neunen) ausgelegt. Beide Plattformen bieten zuverlässige Datensicherungen mit Objektreplikation über mindestens drei geografisch verteilte Availability Zones. Viele AWS Dienste verwenden Amazon S3 für Speicher- und Export-/Importvorgänge. Amazon Elastic Block Store (Amazon EBS) verwendet beispielsweise Amazon S3 für die Speicherung von Snapshots.
- **Sicherheit:** AWS bietet eine Reihe von Optionen für die Zugriffskontrolle und Datenverschlüsselung während der Übertragung und im Ruhezustand.
- **Globale Infrastruktur:** AWS Dienste sind auf der ganzen Welt verfügbar, sodass Sie Daten in der Region sichern und speichern können, die Ihren Compliance- und Workload-Anforderungen entspricht.
- **Konformität:** Die AWS Infrastruktur ist für die Einhaltung der folgenden Standards zertifiziert, sodass Sie die Backup-Lösung problemlos an Ihr bestehendes Compliance-System anpassen können:
 - Steuerung der Serviceorganisation (SOC)

- Erklärung zu den Standards für Bescheinigungen (SSAE) 16
- Internationale Organisation für Normung (ISO) 27001
- Payment Card Industry Data Security Standard (PCI DSS)
- Health Insurance Portability and Accountability Act (HIPAA)
- SEC1
- Federal Risk and Authorization Management Program (FedRAMP)
- Skalierbarkeit: Mit AWS müssen Sie sich keine Gedanken über die Kapazität machen. Wenn sich Ihre Anforderungen ändern, können Sie Ihren Verbrauch ohne Verwaltungsaufwand nach oben oder unten skalieren.
- Niedrigere Gesamtbetriebskosten (TCO): Der Umfang der AWS Betriebsabläufe senkt die Servicekosten und trägt zur Senkung der Gesamtbetriebskosten von AWS Services bei. AWS gibt diese Kosteneinsparungen durch Preissenkungen an die Kunden weiter.
- ay-as-you-go P-Preisgestaltung: Erwerben Sie AWS Dienste nach Bedarf und nur für den Zeitraum, in dem Sie sie nutzen möchten. AWS Bei der Preisgestaltung fallen keine Vorabgebühren, Kündigungsgebühren oder langfristige Verträge an.

Gezielte Geschäftsergebnisse

Ziel dieses Leitfadens ist es, einen Überblick zu geben über AWS-Dienste, die Sie zur Unterstützung von Sicherungs- und Wiederherstellungsansätzen für Folgendes verwenden können:

- Architekturen vor Ort
- Cloud-native Architekturen
- Hybride Architekturen
- Native AWS-Dienste
- Notfallwiederherstellung (DR)

Bewährte Verfahren und Überlegungen werden zusammen mit einem Überblick über die Dienste behandelt. In diesem Handbuch finden Sie auch die Kompromisse zwischen der Verwendung eines Ansatzes gegenüber einem anderen für Backup und Recovery.

Auswahl von AWS Diensten für den Datenschutz

Notice (Hinweis)

Seit dem 30. April 2024 AWS wird VMware Cloud on nicht mehr von AWS oder seinen Channel-Partnern weiterverkauft. Der Service wird weiterhin über Broadcom verfügbar sein. Wir empfehlen Ihnen, sich für weitere Informationen an Ihren AWS Vertreter zu wenden.

AWS bietet eine Reihe von Speicher- und ergänzenden Services, die als Teil Ihres Backup- und Recovery-Ansatzes genutzt werden können. Diese Dienste können sowohl cloudnative als auch hybride Architekturen unterstützen. Verschiedene Dienste sind für unterschiedliche Anwendungsfälle effektiver.

- [Amazon S3](#) eignet sich sowohl für hybride als auch für Cloud-native Anwendungsfälle. Es bietet äußerst langlebige Allzweck-Objektspeicherlösungen, die sich für die Sicherung einzelner Dateien, Server oder eines gesamten Rechenzentrums eignen.
- [AWS Storage Gateway](#) ist ideal für hybride Anwendungsfälle. Storage Gateway nutzt die Leistung von Amazon S3 für allgemeine lokale Backup- und Speicheranforderungen. Ihre Anwendungen stellen über eine virtuelle Maschine (VM) oder eine Hardware-Gateway-Appliance mithilfe der folgenden Standardspeicherprotokolle eine Verbindung zum Service her:
 - Netzwerk-Dateisystem (NFS)
 - Server-Nachrichtenblock (SMB)
 - Internet-Systemschnittstelle für kleine Computer (iSCSI)

Das Gateway verbindet diese gängigen lokalen Protokolle mit AWS Speicherdiensten wie den folgenden:

- Amazon S3
- S3 Glacier Deep Archive
- Amazon EBS

Storage Gateway erleichtert die Bereitstellung von elastischem Hochleistungsspeicher für [Dateien](#), [Volumes](#), Snapshots und [virtuelle Bänder](#). AWS

- [AWS Backup](#) ist ein vollständig verwalteter Backup-Service zur Zentralisierung und Automatisierung der datenübergreifenden Sicherung. AWS Mit ihm AWS Backup können Sie Backup-Richtlinien

zentral konfigurieren und die Backup-Aktivitäten für AWS Ressourcen überwachen, z. B. für die folgenden:

- EBS-Datenträger
- EC2-Instances (einschließlich Windows-Anwendungen)
- Amazon RDS- und Amazon Aurora Aurora-Datenbanken
- DynamoDB-Tabellen
- Amazon Neptune Neptune-Datenbanken
- Amazon-DocumentDB-Datenbanken (mit MongoDB-Kompatibilität)
- Amazon-EFS-Dateisysteme
- Amazon FSx for Lustre Lustre-Dateisysteme und Amazon FSx for Windows File Server Server-Dateisysteme
- VMware-Workloads vor Ort und in VMware Cloud auf AWS
- Storage Gateway Gateway-Volumes

Die Kosten für AWS Backup basieren auf dem Speicherplatz, den Sie in einem Monat verbrauchen, wiederherstellen und übertragen. Weitere Informationen finden Sie in den [AWS Backup Preisen](#).

- [AWS Elastic Disaster Recovery](#) repliziert Ihre Maschinen kontinuierlich in einen kostengünstigen Staging-Bereich in Ihrem AWS Zielkonto und Ihrer bevorzugten Region. Sie können Elastic Disaster Recovery für premises-to-cloud On-DR und regionsübergreifende DR verwenden.
- [AWS Config](#) bietet einen detaillierten Überblick über die Konfiguration der AWS Ressourcen in Ihrem AWS Konto. Dazu gehört auch, wie die Ressourcen miteinander in Beziehung stehen und wie sie in der Vergangenheit konfiguriert wurden. In dieser Ansicht können Sie sehen, wie sich die Ressourcenkonfiguration und die Beziehungen im Laufe der Zeit verändert haben.

Wenn Sie die [AWS Config Konfigurationsaufzeichnung](#) für Ihre AWS Ressourcen aktivieren, behalten Sie den Verlauf Ihrer Ressourcenbeziehungen im Laufe der Zeit bei. Auf diese Weise können Sie AWS Ressourcenbeziehungen (einschließlich gelöschter Ressourcen) über einen Zeitraum von bis zu sieben Jahren identifizieren und nachverfolgen. AWS Config kann beispielsweise die Beziehung zwischen einem Amazon EBS-Snapshot-Volume und der EC2-Instance verfolgen, an die das Volume angehängt wurde.

- [AWS Lambda](#) kann verwendet werden, um Ihre Sicherungs- und Wiederherstellungsverfahren für Ihre Workloads programmgesteuert zu definieren und zu automatisieren. Sie können die AWS SDKs verwenden, um mit AWS Diensten und ihren Daten zu interagieren. Sie können [Amazon CloudWatch Events](#) auch verwenden, um Ihre Lambda-Funktionen nach einem Zeitplan auszuführen.

AWS Dienste bieten spezielle Funktionen für Sicherung und Wiederherstellung. Schlagen Sie für jeden AWS Dienst, den Sie verwenden, in der AWS Dokumentation nach, welche Sicherungs-, Wiederherstellungs- und Datenschutzfunktionen der Dienst bietet. Sie können die AWS Command Line Interface (AWS CLI), AWS SDKs und API-Operationen verwenden, um die AWS dienstspezifischen Funktionen für Datensicherung und Wiederherstellung zu automatisieren.

Entwicklung einer Backup- und Wiederherstellungslösung

Bei der Entwicklung einer umfassenden Strategie für die Sicherung und Wiederherstellung von Daten müssen Sie zunächst mögliche Ausfall- oder Katastrophensituationen und deren mögliche Auswirkungen auf das Geschäft identifizieren. In einigen Branchen müssen Sie die gesetzlichen Anforderungen an Datensicherheit, Datenschutz und Aufbewahrung von Aufzeichnungen berücksichtigen.

Sicherungs- und Wiederherstellungsprozesse sollten ein angemessenes Maß an Granularität aufweisen, um das Recovery Time Objective (RTO) und das Recovery Point Objective (RPO) für den Workload und die unterstützenden Geschäftsprozesse zu erreichen, einschließlich der folgenden Punkte:

- Wiederherstellung auf Dateiebene (z. B. Konfigurationsdateien für eine Anwendung)
- Wiederherstellung auf Anwendungsdatenebene (z. B. eine bestimmte Datenbank in MySQL)
- Wiederherstellung auf Anwendungsebene (z. B. eine bestimmte Webserver-Anwendungsversion)
- Amazon EC2-Wiederherstellung auf Volume-Ebene (z. B. ein EBS-Volume)
- Wiederherstellung auf EC2-Instanzebene. (zum Beispiel eine EC2-Instance)
- Managed Service Recovery (z. B. eine DynamoDB-Tabelle)

Achten Sie darauf, alle Wiederherstellungsanforderungen für Ihre Lösung und die Datenabhängigkeiten zwischen verschiedenen Komponenten in Ihrer Architektur zu berücksichtigen. Um einen erfolgreichen Wiederherstellungsprozess zu ermöglichen, koordinieren Sie die Sicherung und Wiederherstellung zwischen verschiedenen Komponenten in Ihrer Architektur.

In den folgenden Themen werden Sicherungs- und Wiederherstellungsansätze beschrieben, die auf der Organisation Ihrer Infrastruktur basieren. Die IT-Infrastruktur kann allgemein als lokal, hybrid oder cloudnativ eingestuft werden.

Backup und Wiederherstellung mit AWS Backup

AWS Backup ist ein vollständig verwalteter Backup-Service, der die Datensicherung zentralisiert und automatisiert AWS-Services. AWS Backup bietet eine Orchestrierungsschicht, die Amazon CloudWatch integriert, AWS CloudTrail, AWS Identity and Access Management (IAM), AWS Organizations und andere AWS-Services. Dies zentralisiert, AWS Cloud-native Lösung bietet globale Backup-Funktionen, die Ihnen helfen können, Ihre Disaster Recovery- und Compliance-Anforderungen zu erfüllen. Sie können AWS Backup nutzen, um Ihre Sicherungsrichtlinien und Sicherungsaktivitäten zentral konfigurieren und überwachen. AWS Backup schätzt Ihre AWS-Ressourcen.

AWS Backup ist eine ideale Lösung für die Implementierung von Standard-Sicherungsplänen für Ihre AWS-Ressourcen in Ihrem AWS-Konto und -Regionen. Da es sich bei AWS Backup um eine zentrale Lösung handelt, erleichtert die Wartung und Implementierung einer Backup-Strategie für Workloads mit mehreren AWS-Ressourcen, die gemeinsam gesichert werden müssen. AWS Backup ermöglicht es Ihnen auch, gemeinsam einen Sicherungs- und Wiederherstellungsvorgang zu überwachen, der mehrere AWS-Ressourcen umfasst.

Wenn Sie Compliance- und Audit-Anforderungen haben, können Sie die [AWS Backup Audit Manager](#)-Funktion zum Erstellen von Audit-Frameworks und -Berichten zur Unterstützung Ihrer Compliance-Anforderungen. Die [AWS Backup Vault Lock](#) unterstützt auch Compliance-Anforderungen, indem es eine einmalige, lesbare Konfiguration (WORM) für alle Ihre Backups durchsetzt, die in einem Backup-Tresor gespeichert sind.

Ein wichtiges Unterscheidungsmerkmal für AWS Backup ist die Unterstützung für Organizations. Mit diesem Support können Sie Backup-Richtlinien auf Organisations- oder Organisationseinheitsebene definieren und verwalten und diese Richtlinien automatisch für jede zugehörige implementieren lassen. Wie bei einem neuen AWS-Konto und Region müssen Sie Backup-Pläne nicht separat definieren und verwalten.

AWS Backup kann Ihnen die Implementierung einer organisationsweiten Sicherungsrichtlinie mithilfe von Tags erleichtern. Sie können separate Sicherungspläne erstellen, die jeweils über eindeutige Frequenz- und Aufbewahrungseinstellungen verfügen, und dann eindeutige Schlüssel-Wert-Paar-Tags erstellen, die die Ressourcen auswählen, die für die Sicherung enthalten sind.

Sie könnten beispielsweise einen täglichen Backup-Plan erstellen, der täglich um 05:00 Uhr UTC ein Backup startet und über eine 35-tägige Aufbewahrungsrichtlinie verfügt. Dieser Backup-Plan kann ein [Zuweisung von Backup-Ressourcen](#) enthalten, das angibt, dass alle unterstützten AWS-Ressourcen mit dem Tag-Schlüssel Backup und -Tag-Wert täglich nach diesem Plan gesichert werden. Darüber hinaus können

Sie einen monatlichen Backup-Plan erstellen, der am ersten Tag eines jeden Monats um 05:00 UTC beginnt und über eine 366-tägige Aufbewahrungsrichtlinie verfügt. Dieser Sicherungsplan kann eine Sicherungsressourcenzuweisung enthalten, die angibt, dass alle unterstützten AWS-Ressourcen mit dem Tag-Schlüssel Backup und -Tag-Wert monatlich wird nach diesem Plan gesichert.

Sie können dann Tag-Richtlinien und die [required-tags](#) AWS Config-Regel, um sicherzustellen, dass alle Ihre AWS-unterstützten Ressourcen haben diesen Tag-Schlüssel und einen dieser Tag-Werte. Dieser Ansatz kann Ihnen helfen, einen Standard-Backup-Ansatz konsequent zu implementieren und aufrechtzuerhalten AWS für unterstützte AWS Backup-Ressourcen schützen. Sie können diesen Ansatz erweitern, um Backups für Ihre Anwendungen und Architekturschichten zu standardisieren, die unterschiedliche Anforderungen für Recovery Point Objective (RPO) haben.

Wir empfehlen, Schritte zum Sichern Ihres Backup-Tresors zu ergreifen. Sie können beispielsweise eine Dienststeuerungsrichtlinie für Organizations (SCP) implementieren, die verhindert, dass Ihr Sicherungstresor gelöscht oder für unbeabsichtigte freigegeben wird AWS-Konten. Weitere Details und andere wichtige Sicherheitsüberlegungen finden Sie in der [Top 10 bewährte Sicherheitsmethoden für die Sicherung von Sicherungen in AWS](#) Blogbeitrag

AWS Backup kann die Implementierung Ihres Disaster Recovery (DR) -Plans vereinfachen AWS weil es mehrere unterstützte AWS-Ressourcen, die gemeinsam angesprochen werden können. Sie können beispielsweise implementieren [Regionen übergreifend](#) und [Kontoübergreifend](#) Backup für die meisten der AWS-Ressourcentypen unterstützt von AWS Backup aus. Die kontoübergreifende Sicherung verbessert die Sicherungssicherheit, da eine Kopie in einem separaten Konto verfügbar ist. Regionsübergreifendes Backup verbessert die Verfügbarkeit, da die Backups in mehr als einer Region verfügbar sind. Für Details über unterstützte AWS-Ressourcentypen finden Sie im [Verfügbarkeit von Funktionen nach Ressource](#) Tabelle.

Sie können dieses Beispiel nutzen [Backup und Wiederherstellung mit AWS Backup Open-Source-Lösung](#) um eine Infrastruktur als Code (iAC) und Continuous Integration und Continuous Delivery (CI/CD) -Ansatz zur Verwaltung von Backups für Ihre AWS Organizations-Organisation. Diese Lösung enthält benutzerdefinierte Funktionen wie das automatische erneute Anwenden AWS-Stichworte bei wiederhergestellt AWS-Ressourcen sowie Einrichtung eines sekundären Backup-Tresors in einem separaten Konto und einer Region für Notfall-Zwecke.

Backup und Wiederherstellung mit Amazon S3

Sie können Amazon Simple Storage Service (Amazon S3) verwenden, um jederzeit beliebige Datenmengen zu speichern und abzurufen. Sie können Amazon S3 als dauerhaften Speicher für Ihre Anwendungsdaten und Sicherungs- und Wiederherstellungsprozesse auf Dateiebene verwenden. Beispielsweise können Sie Ihre Datenbank-Backups mit einem Backup-Skript mithilfe der AWS SDKs, AWS CLI oder von einer Datenbank-Instance nach Amazon S3 kopieren.

AWS-Services Verwenden Sie Amazon S3 für äußerst beständigen und zuverlässigen Speicher, wie in den folgenden Beispielen:

- Amazon EC2 verwendet Amazon S3 zum Speichern von Amazon EBS-Snapshots für EBS-Volumes und für EC2-Instance-Speicher.
- Storage Gateway lässt sich in Amazon S3 integrieren, um lokale Umgebungen mit Amazon S3 S3-gestützten Dateifreigaben, Volumes und Bandbibliotheken bereitzustellen.
- Amazon RDS verwendet Amazon S3 für Datenbank-Snapshots.

Viele Backup-Lösungen von Drittanbietern verwenden auch Amazon S3. Arcserve Unified Data Protection unterstützt beispielsweise Amazon S3 für dauerhafte Backups von lokalen und Cloud-nativen Servern.

Sie können die in Amazon S3 integrierten Funktionen dieser Services nutzen, um Ihren Sicherungs- und Wiederherstellungsansatz zu vereinfachen. Gleichzeitig können Sie von der hohen Haltbarkeit und Verfügbarkeit von Amazon S3 profitieren.

Amazon S3 speichert Daten als Objekte in Ressourcen, die als Buckets bezeichnet werden. Sie können beliebig viele Objekte in einem Bucket speichern. Sie können Objekte in Ihrem Bucket mit detaillierter Zugriffskontrolle schreiben, lesen und löschen. Einzelne Objekte können bis zu 5 TB groß sein.

Verwendung von Amazon S3 S3-Speicherklassen zur Senkung der Speicherkosten für Backup-Daten

Amazon S3 bietet mehrere Speicherklassen für den Einsatz in lokalen, hybriden und cloudnativen Architekturen. Alle Speicherklassen bieten skalierbare Kapazität, sodass kein Volumen- oder Medienmanagement erforderlich ist, wenn Ihre Backup-Datensätze wachsen. Durch das pay-

for-what-you Nutzungsmodell und die niedrigen Kosten pro GB/Monat eignen sich Amazon S3 S3-Speicherklassen für eine Vielzahl von Datenschutzanwendungsfällen. Amazon S3 S3-Speicherklassen sind für verschiedene Anwendungsfälle konzipiert, darunter die folgenden Kategorien:

- [Speicherklassen mit häufigem Zugriff](#) für die allgemeine Speicherung von Daten, auf die häufig zugegriffen wird (z. B. Konfigurationsdateien, ungeplante Backups, tägliche Backups). Dazu gehört die Speicherklasse S3 Standard, die Standardspeicherklasse für alle Amazon S3 S3-Objekte.
- [Speicherklassen mit seltenem Zugriff](#) für langlebige, aber selten abgerufene Daten (z. B. monatliche Backups). Dazu gehört die Speicherklasse S3 Standard-IA. IA steht für infrequent access.
- [S3 Glacier-Speicherklassen](#) für extrem langlebige Daten, auf die selten zugegriffen werden muss (z. B. jährliche Backups). Dazu gehört S3 Glacier Deep Archive, das den kostengünstigsten Speicher bietet. AWS

Für Backups mit unbekanntem oder sich ändernden Zugriffsmustern können Sie die Speicherklasse [S3 Intelligent-Tiering](#) verwenden. S3 Intelligent-Tiering überträgt Objekte automatisch auf die kostengünstigste Stufe, je nachdem, vor wie vielen Tagen auf ein Objekt zuletzt zugegriffen wurde.

Note

Für einige Speicherklassen wird eine Gebühr für die Mindestdauer erhoben. Weitere Informationen finden Sie in den [Amazon S3 S3-Preisen](#). Verwenden Sie die Websitensuche, um zu findenduration.

Amazon S3 bietet Lebenszyklusrichtlinien, die Sie konfigurieren können, um Ihre Daten während ihres gesamten Lebenszyklus zu verwalten. Nachdem eine Richtlinie festgelegt wurde, werden Ihre Daten automatisch in die entsprechende Speicherklasse migriert, ohne dass Änderungen an Ihrer Anwendung vorgenommen werden. Weitere Informationen finden Sie in der Dokumentation zum [Amazon S3 S3-Objektlebenszyklusmanagement](#).

Um Ihre Kosten für Backups zu senken, verwenden Sie einen mehrstufigen Speicherklassenansatz, der auf Ihrem Recovery Time Objective (RTO) und Recovery Point Objective (RPO) basiert, wie im folgenden Beispiel:

- Tägliche Backups der letzten 2 Wochen mit S3 Standard

- Wöchentliche Backups der letzten 3 Monate mit S3 Standard-IA
- Vierteljährliche Backups für das vergangene Jahr auf S3 Glacier Flexible Retrieval
- Jährliche Backups der letzten 5 Jahre auf S3 Glacier Deep Archive
- Backups, die nach Ablauf der 5-Jahres-Marke aus S3 Glacier Deep Archive gelöscht wurden

Erstellung von Standard-S3-Buckets für Backup und Archivierung

Sie können einen Standard-S3-Bucket für Backup und Archivierung erstellen, wobei die Sicherungs- und Aufbewahrungsrichtlinien Ihres Unternehmens in Form von S3-Lebenszyklusrichtlinien implementiert werden. Die Kennzeichnung der Kostenzuweisung und die Berichterstattung für die AWS Abrechnung basieren auf den [Tags, die auf Bucket-Ebene zugewiesen](#) wurden. Wenn die Kostenzuweisung wichtig ist, erstellen Sie separate Backup- und Archivierungs-S3-Buckets für jedes Projekt oder jede Geschäftseinheit, sodass Sie die Kosten entsprechend zuordnen können.

Ihre Backup-Skripte und -Anwendungen können den von Ihnen erstellten S3-Bucket für Backup und Archivierung verwenden, um point-in-time Snapshots für Anwendungs- und Workload-Daten zu speichern. Sie können ein standardmäßiges S3-Präfix erstellen, das Ihnen bei der Organisation Ihrer point-in-time Daten-Snapshots hilft. Wenn Sie beispielsweise stündliche Backups erstellen, sollten Sie erwägen, ein Backup-Präfix wie YYYY/MM/DD/HH/<WorkloadName>/<files...> zu verwenden. Auf diese Weise können Sie Ihre point-in-time Backups schnell manuell oder programmgesteuert abrufen.

Verwenden der Amazon S3 S3-Versionierung zur automatischen Verwaltung des Rollback-Verlaufs

Sie können die S3-Objektversionierung aktivieren, um einen Verlauf der Objektänderungen zu verwalten, einschließlich der Möglichkeit, zu einer früheren Version zurückzukehren. Dies ist nützlich für Konfigurationsdateien und andere Objekte, die sich möglicherweise häufiger ändern als Ihr point-in-time Backup-Zeitplan. Es ist auch nützlich für Dateien, die einzeln zurückgesetzt werden müssen.

Verwenden von Amazon S3 zum Sichern und Wiederherstellen von benutzerdefinierten Konfigurationsdateien für AMIs

Amazon S3 mit Objektversionierung kann Ihr Aufzeichnungssystem für Ihre Workload-Konfiguration und Optionsdateien werden. Sie können beispielsweise ein standardmäßiges AWS Marketplace

Amazon EC2 EC2-Image verwenden, das von einem ISV verwaltet wird. Dieses Image kann Software enthalten, deren Konfiguration in einer Reihe von Konfigurationsdateien verwaltet wird. Sie können Ihre benutzerdefinierten Konfigurationsdateien in Amazon S3 verwalten. Wenn Ihre Instance gestartet wird, können Sie diese Konfigurationsdateien als Teil Ihrer [Instance-Benutzerdaten in Ihrer Instance](#) kopieren. Wenn Sie diesen Ansatz anwenden, müssen Sie ein AMI nicht anpassen und neu erstellen, um eine aktualisierte Version zu verwenden.

Verwenden von Amazon S3 in Ihrem benutzerdefinierten Sicherungs- und Wiederherstellungsprozess

Amazon S3 bietet einen Allzweck-Backup-Speicher, den Sie schnell in Ihre bestehenden benutzerdefinierten Backup-Prozesse integrieren können. Sie können die AWS CLI AWS SDKs und API-Operationen verwenden, um Ihre Sicherungs- und Wiederherstellungsskripts und -prozesse zu integrieren, die Amazon S3 verwenden. Beispielsweise verfügen Sie möglicherweise über ein Datenbank-Backup-Skript, das nächtliche Datenbankexporte durchführt. Sie können dieses Skript so anpassen, dass Ihre nächtlichen Backups zur externen Speicherung nach Amazon S3 kopiert werden. Einen Überblick darüber, wie [das geht, finden Sie im Tutorial Batch-Upload von Dateien in die Cloud](#).

Sie können einen ähnlichen Ansatz für den Export und die Sicherung von Daten für verschiedene Anwendungen verwenden, basierend auf deren individuellem RPO. Darüber hinaus können Sie AWS Systems Manager damit Ihre Backup-Skripts auf Ihren verwalteten Instanzen ausführen. Systems Manager bietet Automatisierung, Zugriffskontrolle, Planung, Protokollierung und Benachrichtigung für Ihre individuellen Backup-Prozesse.

Sicherung von Backup-Daten in Amazon S3

Datensicherheit ist ein allgemeines Anliegen und AWS nimmt Sicherheit sehr ernst. Sicherheit ist die Grundlage für alle AWS-Service. Amazon S3 bietet Funktionen für Zugriffskontrolle und Verschlüsselung sowohl im Ruhezustand als auch bei der Übertragung. Alle Amazon S3 S3-Endpunkte unterstützen SSL/TLS für die Verschlüsselung von Daten während der Übertragung. Sie können die Verschlüsselung für Objekte im Ruhezustand wie folgt einrichten:

- [Serverseitige Verschlüsselung mit verwalteten Amazon S3 S3-Verschlüsselungsschlüsseln](#) verwenden (Standard)
- Verwendung der [serverseitigen Verschlüsselung mit AWS Key Management Service \(AWS KMS\) - Schlüsseln](#), die in gespeichert sind AWS KMS

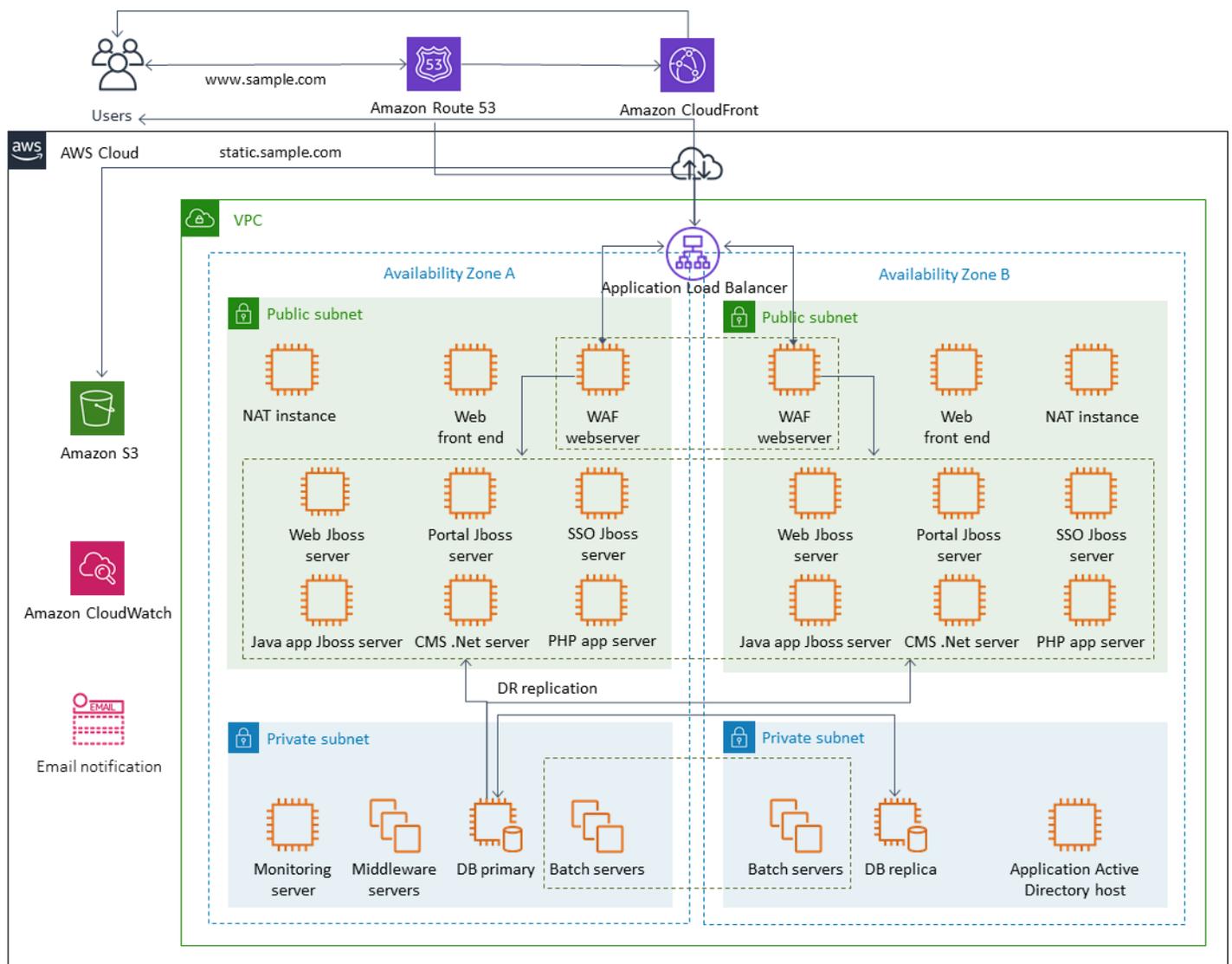
- Verwendung der [clientseitigen Verschlüsselung](#)

Sie können AWS Identity and Access Management (IAM) verwenden, um den Zugriff auf S3-Objekte zu steuern. IAM bietet die Kontrolle über die Berechtigungen für einzelne Objekte und bestimmte Präfixpfade innerhalb eines S3-Buckets. Sie können den Zugriff auf S3-Objekte überprüfen, indem Sie die Protokollierung auf [Objektebene](#) mit verwenden. AWS CloudTrail

Backup und Wiederherstellung für Amazon EC2 mit EBS-Volumes

AWS bietet mehrere Methoden zum Sichern Ihrer Amazon EC2. In diesem Abschnitt werden verschiedene Aspekte der Sicherung von Amazon Elastic Block Store (Amazon EBS)-Volumes oder Instance-Speicher-Volumes für die Speicherung behandelt. Betrachten Sie AWS Backup als erste Wahl für die Verwaltung von Backups auf AWS, wenn es Ihren Anforderungen entspricht. Denken Sie daran, dass Backups nur dann gut sind, wenn sie in der Funktion wiederhergestellt werden können, für die sie vorgesehen waren. Die Wiederherstellungs- und Wiederherstellungsfunktion sollte regelmäßig getestet werden, um dies zu bestätigen.

Die Lösungsarchitektur im folgenden Diagramm beschreibt eine Workload-Umgebung, die vollständig in besteht, AWS wobei der Großteil der Architektur auf Amazon EC2 basiert. Wie die folgende Abbildung zeigt, umfasst das Szenario Webserver, Anwendungsserver, Überwachungsserver, Datenbanken und Active Directory.



AWS bietet viele voll funktionsfähige Services für viele der Amazon EC2-Server, die in dieser Architektur dargestellt werden, um die undifferenzierte Arbeit zum Erstellen, Bereitstellen, Sichern, Wiederherstellen und Optimieren der Instances und des Speichers durchzuführen. Überlegen Sie, ob diese Services in Ihrer Architektur sinnvoll sind, um Komplexität und Verwaltung zu reduzieren. bietet AWS auch Services zur Verbesserung der Verfügbarkeit Ihrer Amazon EC2-basierten Architekturen. Berücksichtigen Sie insbesondere Amazon EC2 Auto Scaling und Elastic Load Balancing, um Ihre Workloads auf Amazon EC2 zu ergänzen. Die Verwendung dieser Services kann die Verfügbarkeit und Fehlertoleranz Ihrer Architektur verbessern und Ihnen helfen, beeinträchtigte Instances mit minimalen Auswirkungen auf die Benutzer wiederherzustellen.

EC2-Instances verwenden hauptsächlich Amazon EBS-Volumes für persistenten Speicher. Amazon EBS bietet eine Reihe von Funktionen für Backup und Wiederherstellung, die in diesem Abschnitt ausführlich behandelt werden.

Themen

- [Amazon EC2-Backup und -Wiederherstellung mit Snapshots und AMIs](#)
- [Erstellen von EBS-Volume-Backups mit AMIs und EBS-Snapshots](#)
- [Wiederherstellen eines Amazon-EBS-Volumes oder einer EC2-Instance](#)

Amazon EC2-Backup und -Wiederherstellung mit Snapshots und AMIs

Überlegen Sie, ob Sie eine vollständige Sicherung einer EC2-Instance mit einem Amazon Machine Image (AMI) erstellen oder einen Snapshot eines einzelnen Volumes erstellen müssen.

Verwenden von AMIs oder Amazon-EBS-Snapshots für Backups

Ein AMI umfasst Folgendes:

- Ein oder mehrere Snapshots. I-instance-store-backed AMIs enthalten eine Vorlage für das Stamm-Volume der Instance (z. B. ein Betriebssystem, einen Anwendungsserver und Anwendungen).
- Startberechtigungen, die steuern, welche - AWS Konten das AMI zum Starten von Instances verwenden können.
- Eine Blockgerät-Zuweisung, die die Volumes angibt, die der Instance beim Start angefügt werden sollen.

Sie können AMIs verwenden, um neue Instances mit vorkonfigurierter Software und Daten zu starten. Sie können AMIs erstellen, wenn Sie eine Baseline einrichten möchten. Dabei handelt es sich um eine wiederverwendbare Konfiguration zum Starten weiterer Instances. Wenn Sie ein AMI einer vorhandenen EC2-Instance erstellen, wird ein Snapshot für alle Volumes erstellt, die an die Instance angefügt sind. Der Snapshot enthält die Gerätezuordnungen.

Sie können keine Snapshots verwenden, um eine neue Instance zu starten, aber Sie können sie verwenden, um Volumes auf einer vorhandenen Instance zu ersetzen. Wenn Sie eine Datenbeschädigung oder einen Volume-Ausfall feststellen, können Sie ein Volume aus einem von

Ihnen erstellten Snapshot erstellen und das alte Volume ersetzen. Sie können Snapshots auch verwenden, um neue Volumes bereitzustellen und diese während eines neuen Instance-Starts anzufügen.

Wenn Sie Plattform- und Anwendungs-AMIs verwenden, die von AWS oder von verwaltet und veröffentlicht werden AWS Marketplace, sollten Sie erwägen, separate Volumes für Ihre Daten zu verwalten. Sie können Ihre Daten-Volumes als Snapshots sichern, die vom Betriebssystem und den Anwendungs-Volumes getrennt sind. Verwenden Sie dann die Daten-Volume-Snapshots mit neu aktualisierten AMIs, die von AWS oder von der veröffentlicht werden AWS Marketplace. Dieser Ansatz erfordert sorgfältige Tests und Planungen, um alle benutzerdefinierten Daten, einschließlich Konfigurationsinformationen, auf den neu veröffentlichten AMIs zu sichern und wiederherzustellen.

Der Wiederherstellungsprozess wird von Ihrer Wahl zwischen AMI-Backups oder Snapshot-Backups beeinflusst. Wenn Sie AMIs erstellen, die als Instance-Backups dienen, müssen Sie im Rahmen Ihres Wiederherstellungsprozesses eine EC2-Instance aus dem AMI starten. Möglicherweise müssen Sie auch die vorhandene Instance herunterfahren, um mögliche Kollisionen zu vermeiden. Ein Beispiel für eine mögliche Kollision sind Sicherheitskennungen (SIDs) für Windows-Instances, die mit einer Domain verbunden sind. Für den Wiederherstellungsprozess für Snapshots müssen Sie möglicherweise das vorhandene Volume trennen und das neu wiederhergestellte Volume anfügen. Oder Sie müssen möglicherweise eine Konfigurationsänderung vornehmen, um Ihre Anwendungen auf das neu angefügte Volume zu verweisen.

AWS Backup unterstützt sowohl Backups auf Instance-Ebene als AMIs als auch Backups auf Volume-Ebene als separate Snapshots:

- Erstellen Sie für eine vollständige Sicherung aller EBS-Volumes auf der Instance ein AMI der EC2-Instance, die unter [Linux](#) oder [Windows](#) ausgeführt wird. Wenn Sie ein Rollback durchführen möchten, verwenden Sie den Assistenten zum Starten von Instances, um eine Instance zu erstellen. Wählen Sie im Instance-Startassistenten Meine AMIs aus.
- Um ein einzelnes Volume zu sichern, [erstellen Sie einen Snapshot](#). Informationen zum Wiederherstellen des Snapshots finden Sie unter [Erstellen eines Volumes aus einem Snapshot](#). Sie können die AWS Management Console oder die AWS Command Line Interface (AWS CLI) verwenden.

Die Kosten eines Instance-AMI sind der Speicher aller Volumes auf der Instance, nicht jedoch der Metadaten. Die Kosten für einen EBS-Snapshot sind der Speicher des einzelnen Volumes. Weitere Informationen zu den Volume-Speicherkosten finden Sie auf der [Seite Amazon EBS – Preise](#).

Server-Volumes

EBS-Volumes sind die primäre persistente Speicheroption für Amazon EC2. Sie können diesen Blockspeicher für strukturierte Daten wie Datenbanken oder unstrukturierte Daten wie Dateien in einem Dateisystem auf einem Volume verwenden.

EBS-Volumes werden in einer bestimmten Availability Zone platziert. Die Volumes werden über mehrere Server repliziert, um den Datenverlust durch den Ausfall einer einzelnen Komponente zu verhindern. Fehler bezieht sich auf einen vollständigen oder teilweisen Verlust des Volumes, abhängig von der Größe und Leistung des Volumes.

EBS-Volumes sind für eine jährliche Ausfallrate (AFR) von 0,1–0,2 Prozent konzipiert. Dadurch werden EBS-Volumes 20-mal zuverlässiger als normale, normale Laufwerke, die mit einem AFR von etwa 4 Prozent ausfallen. Wenn Sie beispielsweise 1 000 EBS-Volumes haben, die 1 Jahr lang ausgeführt werden, sollten Sie davon ausgehen, dass ein oder zwei Volumes ausfallen.

Amazon EBS unterstützt auch eine Snapshot-Funktion für die Erstellung von point-in-time Backups Ihrer Daten. Alle EBS-Volume-Typen bieten dauerhafte Snapshot-Funktionen und sind auf eine Verfügbarkeit von 99,999 Prozent ausgelegt. Weitere Informationen finden Sie im [Amazon Compute Service Level Agreement](#).

Amazon EBS bietet die Möglichkeit, Snapshots (Backups) eines beliebigen EBS-Volumes zu erstellen. Ein Snapshot ist eine Basisfunktion zum Erstellen von Backups Ihrer EBS-Volumes. Ein Snapshot erstellt eine Kopie des EBS-Volumes und platziert es in Amazon S3, wo es redundant in mehreren Availability Zones gespeichert wird. Der erste Snapshot ist eine vollständige Kopie des Volumes. Laufende Snapshots speichern nur inkrementelle Änderungen auf Blockebene. Weitere Informationen zum Erstellen von [Amazon EC2-Dokumentation](#).

Sie können einen Wiederherstellungsvorgang durchführen, einen Snapshot löschen oder die Snapshot-Metadaten, wie z. B. Tags, aktualisieren, die dem Snapshot von [der Amazon EC2-Konsole](#) in derselben Region aus zugeordnet sind, in der Sie den Snapshot erstellt haben.

Beim Wiederherstellen eines Snapshots wird ein neues Amazon-EBS-Volume mit vollständigen Volume-Daten erstellt. Wenn Sie nur eine teilweise Wiederherstellung benötigen, können Sie das Volume unter einem anderen Gerätenamen an die ausgeführte Instance anfügen. Mounten Sie sie dann und verwenden Sie Betriebssystem-Kopierbefehle, um die Daten vom Backup-Volume auf das Produktions-Volume zu kopieren.

Amazon-EBS-Snapshots können auch zwischen - AWS Regionen kopiert werden, indem die Amazon-EBS-Snapshot-Kopierfunktion verwendet wird, wie in der [Amazon EC2Dokumentation](#)

beschrieben. Sie können diese Funktion verwenden, um Ihr Backup in einer anderen Region zu speichern, ohne die zugrunde liegende Replikationstechnologie verwalten zu müssen.

Einrichtung separater Server-Volumes

Sie können bereits einen Standardsatz separater Volumes für das Betriebssystem, Protokolle, Anwendungen und Daten verwenden. Durch die Einrichtung separater Server-Volumes können Sie den Umfang der Auswirkungen verringern, wenn Anwendungs- oder Plattformausfälle durch Ausschöpfung des Speicherplatzes verursacht werden. Dieses Risiko ist bei physischen Festplatten in der Regel größer, da Sie nicht die Flexibilität haben, Volumes schnell zu erweitern. Bei physischen Laufwerken müssen Sie die neuen Laufwerke erwerben, die Daten sichern und die Daten dann auf den neuen Laufwerken wiederherstellen. Mit wird dieses Risiko erheblich reduziert AWS, da Sie Amazon EBS verwenden können, um Ihre bereitgestellten Volumes zu erweitern. Weitere Informationen finden Sie in der [AWS -Dokumentation](#).

Verwalten Sie separate Volumes für Anwendungsdaten, Benutzerdaten, Protokolle und Auslagerungsdateien, sodass Sie separate Backup- und Wiederherstellungsrichtlinien für diese Ressourcen verwenden können. Durch die Trennung von Volumes für Ihre Daten können Sie auch verschiedene Volume-Typen verwenden, die auf den Leistungs- und Speicheranforderungen für die Daten basieren. Anschließend können Sie Ihre Kosten für verschiedene Workloads optimieren und optimieren.

Überlegungen zu Instance-Speicher-Volumes

Ein Instance-Speicher stellt für Ihre Instance temporären Speicher auf Blockebene bereit. Dieser Speicher befindet sich auf Laufwerken, die physisch mit dem Host-Computer verbunden sind. Instance-Speicher eignen sich ideal für die temporäre Speicherung von Informationen, die sich häufig ändern, wie Puffer, Caches, Scratch-Daten und andere temporäre Inhalte. Sie sind auch für Daten vorzuziehen, die über eine Flotte von Instances repliziert werden, z. B. für einen Load Balancing-Pool von Webservern.

Die Daten in einem Instance-Speicher bleiben nur während der Nutzungsdauer der jeweiligen Instance erhalten. Wenn eine Instance neu gestartet wird (absichtlich oder unabsichtlich), bleiben die Daten im Instance-Speicher erhalten. Die Daten im Instance-Speicher gehen jedoch unter den folgenden Umständen verloren.

- Das zugrunde liegende Laufwerk schlägt fehl.
- Die Instance wird gestoppt.

- Die Instance wird beendet.

Verlassen Sie sich daher nicht auf einen Instance-Speicher für wertvolle, langfristige Daten. Nutzen Sie hierfür stattdessen eine dauerhaftere Datenspeicherung, z. B. Amazon S3, Amazon EBS oder Amazon EFS.

Eine gängige Strategie bei Instance-Speicher-Volumes besteht darin, die erforderlichen Daten bei Bedarf regelmäßig in Amazon S3 zu speichern, basierend auf dem Recovery Point Objective (RPO) und dem Recovery Time Objective (RTO). Sie können die Daten dann von Amazon S3 in Ihren Instance-Speicher herunterladen, wenn eine neue Instance gestartet wird. Sie können die Daten auch in Amazon S3 hochladen, bevor eine Instance angehalten wird. Erstellen Sie aus Gründen der Persistenz ein EBS-Volume, fügen Sie es Ihrer Instance an und kopieren Sie die Daten regelmäßig vom Instance-Speicher-Volume auf das EBS-Volume. Weitere Informationen finden Sie im [AWS Knowledge Center](#).

Markieren und Durchsetzen von Standards für EBS-Snapshots und AMIs

Das Markieren all Ihrer AWS Ressourcen ist eine wichtige Methode für Kostenzuordnung, Prüfung, Fehlerbehebung und Benachrichtigung. Tagging ist für EBS-Volumes wichtig, damit die relevanten Informationen vorhanden sind, die für die Verwaltung und Wiederherstellung von Volumes erforderlich sind. Tags werden nicht automatisch von EC2-Instances in AMIs oder von Quell-Volumes in Snapshots kopiert. Stellen Sie sicher, dass Ihr Backup-Prozess die relevanten Tags aus diesen Quellen enthält. Auf diese Weise können Sie die Snapshot-Metadaten wie Zugriffsrichtlinien, Anhangsinformationen und Kostenzuordnung festlegen, um diese Backups in Zukunft zu verwenden. Weitere Informationen zum Markieren Ihrer AWS Ressourcen finden Sie im [technischen Papier zu bewährten Methoden für das Markieren von](#).

Verwenden Sie zusätzlich zu den Tags, die Sie für alle AWS Ressourcen verwenden, die folgenden Backup-spezifischen Tags:

- Quell-Instance-ID
- Quell-Volume-ID (für Snapshots)
- Beschreibung des Wiederherstellungspunkts

Sie können Tagging-Richtlinien mithilfe von AWS Config Regeln und IAM-Berechtigungen erzwingen. IAM unterstützt die erzwungene Tag-Nutzung, sodass Sie IAM-Richtlinien schreiben können, die die Verwendung bestimmter Tags bei der Ausführung von Amazon-EBS-Snapshots vorschreiben. Wenn

ein `CreateSnapshot` Vorgang ohne die Tags versucht wird, die in der IAM-Berechtigungsrichtlinie definiert sind, die Rechte gewährt, schlägt die Snapshot-Erstellung fehl, wobei der Zugriff verweigert wird. Weitere Informationen finden Sie im [Blog-Beitrag zum Markieren von Amazon-EBS-Snapshots bei der Erstellung und Implementierung strengerer Sicherheitsrichtlinien](#).

Sie können AWS Config Regeln verwenden, um die Konfigurationseinstellungen Ihrer AWS Ressourcen automatisch auszuwerten. Um Ihnen den Einstieg zu erleichtern, AWS Config stellt anpassbare, vordefinierte Regeln bereit, die als verwaltete Regeln bezeichnet werden. Zudem können Sie eigene benutzerdefinierte Regeln erstellen. Während Konfigurationsänderungen zwischen Ihren Ressourcen AWS Config kontinuierlich verfolgt, wird geprüft, ob diese Änderungen gegen eine der Bedingungen in Ihren Regeln verstoßen. Wenn eine Ressource gegen eine Regel verstößt, AWS Config markiert die Ressource und die Regel als nicht konform. Beachten Sie, dass die verwaltete Regel für [erforderliche Tags](#) derzeit keine Snapshots und AMIs unterstützt.

Erstellen von EBS-Volume-Backups mit AMIs und EBS-Snapshots

AWS bietet eine Fülle von Optionen zum Erstellen und Verwalten von AMIs und Snapshots. Sie können den Ansatz verwenden, der Ihren Anforderungen entspricht. Ein häufiges Problem, mit dem viele Kunden konfrontiert sind, besteht darin, den Snapshot-Lebenszyklus zu verwalten und Snapshots nach Zweck, Aufbewahrungsrichtlinie usw. klar auszurichten. Ohne ordnungsgemäßes Markieren besteht die Gefahr, dass Snapshots versehentlich oder im Rahmen eines automatisierten Bereinigungsprozesses gelöscht werden. Möglicherweise zahlen Sie auch für veraltete Snapshots, die aufbewahrt werden, da Sie nicht genau wissen, ob sie noch benötigt werden.

Vorbereiten eines EBS-Volumens vor dem Erstellen eines Snapshots oder AMI

Bevor Sie einen Snapshot erstellen oder ein AMI erstellen, treffen Sie die erforderlichen Vorbereitungen für Ihr EBS-Volume. Das Erstellen eines AMI führt zu einem neuen Snapshot für jedes EBS-Volume, das an die Instance angefügt ist. Diese Vorbereitungen gelten daher auch für AMIs .

Sie können einen Snapshot eines angefügten EBS-Volumens erstellen, das von einer EC2-Instance mit aktiviertem Betrieb verwendet wird. Snapshots erfassen jedoch nur Daten, die zum Zeitpunkt der Ausgabe des Snapshot-Befehls auf Ihr EBS-Volume geschrieben wurden. Dies kann alle Daten ausschließen, die von Anwendungen oder dem Betriebssystem zwischengespeichert wurden. Eine bewährte Methode besteht darin, das System in einem Zustand zu haben, in dem es keine E/A ausführt. Im Idealfall akzeptiert die Maschine keinen Datenverkehr und befindet sich in einem

angehaltenen Zustand. Dies ist jedoch selten, da IT-Operationen rund um die Uhr zur Normalität werden. Wenn Sie alle Daten aus dem Systemspeicher auf die Festplatte übertragen können, die von Ihren Anwendungen verwendet wird, und alle Dateischreibvorgänge auf das Volume lange genug unterbrechen können, um einen Snapshot zu erstellen, sollte Ihr Snapshot vollständig sein.

Um ein sauberes Backup zu erstellen, müssen Sie die Datenbank oder das Dateisystem in die Warteschlange stellen. Wie Sie dies tun, hängt von Ihrer Datenbank oder Ihrem Dateisystem ab.

Der Prozess für eine Datenbank ist wie folgt:

1. Setzen Sie die Datenbank nach Möglichkeit in den Hot-Backup-Modus.
2. Führen Sie die Amazon-EBS-Snapshot-Befehle aus.
3. Nehmen Sie die Datenbank aus dem Hot-Backup-Modus oder beenden Sie bei Verwendung eines Lesereplikats die Lesereplikat-Instance.

Der Prozess für ein Dateisystem ist ähnlich, hängt aber von den Funktionen des Betriebssystems oder Dateisystems ab. XFS ist beispielsweise ein Dateisystem, das seine Daten für ein konsistentes Backup leeren kann. Weitere Informationen finden Sie unter [xfs_freeze](#). Alternativ können Sie diesen Prozess erleichtern, indem Sie einen logischen Volume-Manager verwenden, der das Einfrieren von E/A unterstützt.

Wenn Sie jedoch nicht alle Dateischreibvorgänge auf das Volume leeren oder anhalten können, gehen Sie wie folgt vor:

1. Heben Sie das Mounting des Volumes vom Betriebssystem auf.
2. Geben Sie den Snapshot-Befehl aus.
3. Mounten Sie das Volume erneut, um einen konsistenten und vollständigen Snapshot zu erhalten. Sie können Ihr Volume erneut mounten und verwenden, während der Snapshot-Status aussteht.

Der Snapshot-Prozess wird im Hintergrund fortgesetzt und die Snapshot-Erstellung ist schnell und erfasst einen bestimmten Zeitpunkt. Die Volumes, die Sie sichern, werden nur wenige Sekunden lang nicht gemountet. Sie können ein kleines Backup-Fenster planen, in dem ein Ausfall von Clients erwartet und ordnungsgemäß behandelt wird.

Wenn Sie einen Snapshot für ein EBS-Volume erstellen, das als Root-Gerät dient, halten Sie die Instance an, bevor Sie den Snapshot erstellen. Windows stellt den Volume Shadow Copy Service (VSS) bereit, um anwendungskonsistente Snapshots zu erstellen. AWS stellt ein Systems Manager-Dokument bereit, das Sie ausführen können, um Backups von VSS-fähigen Anwendungen auf

Bildebene zu erstellen. Dazu gehören auch Daten von schwebenden Transaktionen zwischen diesen Anwendungen und dem Datenträger. Sie müssen Ihre Instances nicht herunterfahren oder trennen, wenn Sie alle angefügten Volumes sichern. Weitere Informationen finden Sie in der [AWS - Dokumentation](#).

Note

Wenn Sie ein Windows-AMI erstellen, damit Sie eine andere ähnliche Instance bereitstellen können, verwenden Sie [EC2Config](#) oder [EC2Launch](#), um Ihre Instance zu [Sysprep](#). Erstellen Sie dann ein AMI aus der angehaltenen Instance. Sysprep entfernt eindeutige Informationen aus der Amazon EC2-Windows-Instance, einschließlich der SIDs, des Computernamens und der Treiber. Doppelte SIDs können zu Problemen mit Active Directory, Windows Server Update Services (WSUS), Anmeldeproblemen, Aktivierung von Windows-Volume-Schlüsseln, Microsoft Office und Produkten von Drittanbietern führen. Verwenden Sie Sysprep nicht mit Ihrer Instance, wenn Ihr AMI für Backup-Zwecke bestimmt ist und Sie dieselbe Instance mit all ihren eindeutigen Informationen intakt wiederherstellen möchten.

Manuelles Erstellen von EBS-Volume-Snapshots über die Konsole

Erstellen Sie Snapshots der entsprechenden Volumes oder der gesamten Instance, bevor Sie wichtige Änderungen vornehmen, die nicht vollständig auf der Instance getestet wurden. Sie können beispielsweise einen Snapshot erstellen, bevor Sie die Anwendung oder Systemsoftware auf Ihrer Instance aktualisieren oder patchen.

Sie können einen Snapshot manuell über die Konsole erstellen. Wählen Sie auf der Amazon EC2-Konsole auf der Seite Elastic Block Store Volumes das Volume aus, das Sie sichern möchten. Wählen Sie dann im Menü Aktionen die Option Snapshot erstellen aus. Sie können nach Volumes suchen, die einer bestimmten Instance zugeordnet sind, indem Sie die Instance-ID in das Filterfeld eingeben.

Geben Sie eine Beschreibung ein und fügen Sie die entsprechenden Tags hinzu. Fügen Sie ein Name Tag hinzu, um das Volume später leichter zu finden. Fügen Sie basierend auf Ihrer Tagging-Strategie alle anderen geeigneten Tags hinzu.

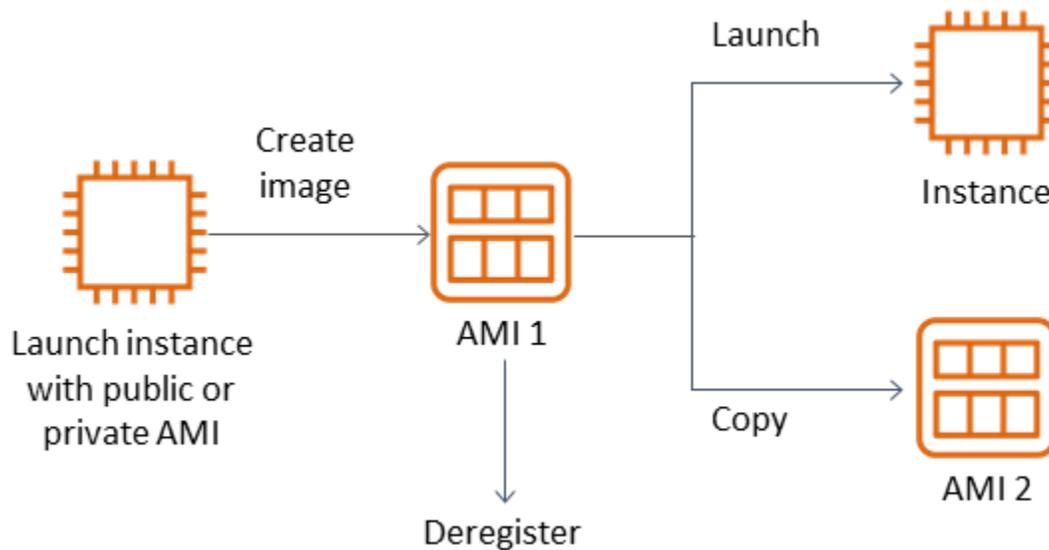
Erstellen von AMIs

Ein AMI stellt die Informationen bereit, die zum Starten einer Instance erforderlich sind. Das AMI enthält das Root-Volume und Snapshots der EBS-Volumes, die an die Instance angefügt waren, als

das Image erstellt wurde. Sie können keine neuen Instances nur aus EBS-Snapshots starten. Sie müssen neue Instances über ein AMI starten.

Wenn Sie ein AMI erstellen, wird es in dem Konto und der Region erstellt, die Sie verwenden. Der AMI-Erstellungsprozess erstellt Amazon EBS-Snapshots für jedes Volume, das an die Instance angefügt ist, und das AMI bezieht sich auf diese Amazon EBS-Snapshots. Diese Snapshots befinden sich in Amazon S3 und sind äußerst langlebig.

Nachdem Sie ein AMI Ihrer EC2-Instance erstellt haben, können Sie das AMI verwenden, um die Instance neu zu erstellen oder weitere Kopien der Instance zu starten. Sie können AMIs auch für die Anwendungsmigration oder DR von einer Region in eine andere kopieren.



Ein AMI muss von einer EC2-Instance erstellt werden, es sei denn, Sie migrieren eine virtuelle Maschine, z. B. eine virtuelle VM-Maschine, zu AWS. Um ein AMI über die Amazon EC2-Konsole zu erstellen, wählen Sie die Instance aus, wählen Sie Aktionen, wählen Sie Image und dann Image erstellen aus.

Amazon Data Lifecycle Manager

Um die Erstellung, Aufbewahrung und Löschung von Amazon-EBS-Snapshots zu automatisieren, können Sie [Amazon Data Lifecycle Manager](#) verwenden. Die Automatisierung der Snapshot-Verwaltung hilft Ihnen bei Folgendem:

- Wertvolle Daten zu schützen, indem ein regelmäßiger Backup-Plan eingehalten wird.
- Backups aufzubewahren, die für Prüfer oder interne Compliance-Vorschriften benötigt werden.

- Speicherkosten zu reduzieren, indem veraltete Backups gelöscht werden.

Mit Amazon Data Lifecycle Manager können Sie den Snapshot-Verwaltungsprozess für EC2-Instances (und die zugehörigen EBS-Volumes) oder separate EBS-Volumes automatisieren. Es unterstützt Optionen wie regionsübergreifendes Kopieren, sodass Sie Snapshots automatisch in andere AWS Regionen kopieren können. Das Kopieren von Snapshots in alternative Regionen ist ein Ansatz zur Unterstützung von DR-Bemühungen und Wiederherstellungsoptionen in einer alternativen Region. Sie können Amazon Data Lifecycle Manager auch verwenden, um eine Snapshot-Lebenszyklusrichtlinie zu erstellen, die die [schnelle Snapshot-Wiederherstellung](#) unterstützt.

Amazon Data Lifecycle Manager ist eine enthaltene Funktion von Amazon EC2 und Amazon EBS. Für Amazon Data Lifecycle Manager fallen keine Gebühren an.

AWS Backup

AWS Backup ist einzigartig in Amazon Data Lifecycle Manager, da Sie einen Backup-Plan erstellen können, der Ressourcen über mehrere AWS Services hinweg enthält. Sie können Ihr Backup so koordinieren, dass es die von Ihnen verwendeten Ressourcen abdeckt, anstatt die Backups der Ressourcen einzeln zu koordinieren.

AWS Backup beinhaltet auch das Konzept der Backup-Tresore, das den Zugriff auf die Wiederherstellungspunkte für Ihre abgeschlossenen Backups einschränken kann. Wiederherstellungsvorgänge können von initiiert werden AWS Backup , anstatt mit jeder einzelnen Ressource fortzufahren und das erstellte Backup wiederherzustellen. enthält AWS Backup auch eine Reihe zusätzlicher Funktionen wie Audit-Management und Berichterstattung. Weitere Informationen finden Sie im Abschnitt [Backup und Wiederherstellung mit AWS Backup](#) in diesem Handbuch.

Durchführen von Multi-Volume-Backups

Wenn Sie die Daten auf den EBS-Volumes in einem RAID-Array mithilfe von Snapshots sichern möchten, müssen die Snapshots konsistent sein. Dies liegt daran, dass die Snapshots dieser Volumes unabhängig voneinander erstellt werden. Das Wiederherstellen von EBS-Volumes in einem RAID-Array aus Snapshots, die nicht synchron sind, beeinträchtigt die Integrität des Arrays.

Um einen konsistenten Satz von Snapshots für Ihr RAID-Array zu erstellen, verwenden Sie die [CreateSnapshots](#)-API-Operation oder melden Sie sich bei der Amazon EC2-Konsole an und wählen Sie Elastic Block Store , Snapshots , Snapshot erstellen aus.

[Snapshots](#) > Create Snapshot

Create Snapshot

Select resource type Volume Instance

Instance ID*  

Description 

Exclude root volume

Volume ID	Volume Type	Encryption
vol-11111111	Root	Encrypted
vol-22222222	EBS	Not Encrypted
vol-33333333	EBS	Not Encrypted
vol-44444444	EBS	Not Encrypted

Copy tags from volume

Key	Value
<small>(127 characters maximum)</small>	<small>(255 characters maximum)</small>

This resource currently has no tags
Choose the [Add tag](#) button or [click to add a Name tag](#)

50 remaining (Up to 50 tags maximum)

* Required

Snapshots von Instances, denen mehrere Volumes an eine RAID-Konfiguration angefügt sind, werden zusammen als Multi-Volume-Snapshot aufgenommen. Multi-Volume-Snapshots stellen point-in-time, datenkoordinierte und absturzkonsistente Snapshots über mehrere EBS-Volumes bereit, die an eine EC2-Instance angefügt sind. Sie müssen Ihre Instance nicht anhalten, um zwischen Volumes zu koordinieren, um Konsistenz zu erreichen, da Snapshots automatisch über mehrere EBS-Volumes hinweg erstellt werden. Nachdem der Snapshot für die Volumes initiiert wurde (in der Regel ein oder zwei Sekunden), kann das Dateisystem seinen Betrieb fortsetzen.

Nach der Erstellung werden die Snapshots als individuelle Snapshots behandelt. Sie können alle Snapshot-Operationen wie Wiederherstellung, Löschen sowie regionsübergreifendes Kopieren und Konto kopieren, wie Sie es bei einem Snapshot mit einem Volume tun würden. Sie können Ihre Multi-Volume-Snapshots auch wie einen Einzel-Volume-Snapshot markieren. Wir empfehlen

Ihnen, Ihre Multi-Volume-Snapshots zu markieren, um sie während der Wiederherstellung, Kopie oder Aufbewahrung gemeinsam zu verwalten. Weitere Informationen finden Sie in der [AWS-Dokumentation](#).

Sie können diese Backups auch von einem logischen Volume-Manager oder einem Backup auf Dateisystemebene aus durchführen. In diesen Fällen ermöglicht die Verwendung eines herkömmlichen Backup-Agenten die Sicherung der Daten über das Netzwerk. Eine Reihe von agentenbasierten Backup-Lösungen sind im Internet und in der verfügbar [AWS Marketplace](#).

Ein alternativer Ansatz besteht darin, ein Replikat der primären System-Volumes zu erstellen, die auf einem einzigen großen Volume vorhanden sind. Dies vereinfacht den Backup-Prozess, da nur ein großes Volume gesichert werden muss und das Backup nicht auf dem primären System stattfindet. Stellen Sie jedoch zunächst fest, ob das einzelne Volume während des Backups ausreichend ausgeführt werden kann und ob die maximale Volume-Größe für die Anwendung geeignet ist.

Schutz Ihrer Amazon EC2-Backups

Es ist wichtig, die Sicherheit Ihrer Backups zu berücksichtigen und versehentliches oder böswilliges Löschen Ihrer Backups zu verhindern. Sie können dazu eine Reihe von Ansätzen zusammen verwenden. Um den Verlust Ihrer kritischen Backups aufgrund einer Sicherheitsverletzung zu verhindern, empfehlen wir Ihnen, Ihre Backups in ein anderes AWS Konto zu kopieren. Wenn Sie mehrere AWS-Konten haben, können Sie ein separates Konto als Archivkonto festlegen, in das alle anderen Konten Backups kopieren können. Sie können dies beispielsweise mit einem [kontoübergreifenden Backup in AWS Backup](#) erreichen.

Ihr Notfallwiederherstellungsplan erfordert möglicherweise auch, dass Sie EC2-Instances in einer anderen AWS-Region im Falle eines regionalen Ausfalls reproduzieren können. Sie können dieses Ziel unterstützen, indem Sie Ihre Backups in eine andere Region innerhalb desselben Kontos kopieren. Dies kann eine zusätzliche Ebene des Schutzes vor versehentlichem Löschen bieten und Notfallwiederherstellung (DR)-Ziele unterstützen. AWS Backup bietet Unterstützung für [regionsübergreifende Backups](#).

Erwägen Sie, IAM-Berechtigungen für die Aktionen [ec2:DeleteSnapshot](#) und [ec2:DeregisterImage](#) zu blockieren. Stattdessen können Sie Ihren Aufbewahrungsrichtlinien und -methoden den Lebenszyklus von EBS-Snapshots und Amazon EC2-AMIs verwalten lassen. Das Blockieren von Löschaktionen ist eine Möglichkeit, eine Write Once Read Many (WORM)-Strategie für Ihre EBS-Snapshots zu implementieren. Sie können auch [AWS Backup Vault Lock](#) verwenden, das Unterstützung für EBS-Snapshots und andere - AWS Ressourcen bietet.

Erwägen Sie außerdem, die Möglichkeit für Benutzer zu blockieren, AMIs und EBS-Snapshots gemeinsam zu nutzen, indem Sie die Aktionen [ec2:ModifyImageAttribute](#) und [ec2:ModifySnapshotAttribute](#) IAM blockieren. Dadurch wird verhindert, dass Ihre AMIs und Snapshots für AWS Konten außerhalb Ihrer Organisation freigegeben werden. Wenn Sie verwenden AWS Backup, sollten Sie Benutzer daran hindern, ähnliche Operationen für Backup-Tresore auszuführen. Weitere Informationen finden Sie im Abschnitt [AWS Backup](#) in diesem Handbuch.

Amazon EC2 enthält eine [Papierkorbfunktion](#), mit der Sie versehentlich gelöschte EBS-Snapshots wiederherstellen können. Wenn Sie Ihren Benutzern erlauben, Snapshots zu löschen, aktivieren Sie diese Funktion, damit benötigte Snapshots nicht dauerhaft gelöscht werden. Benutzer sollten besonders vorsichtig beim Löschen mehrerer Snapshots sein, da die Amazon EC2-Konsole Ihnen ermöglicht, mehrere Snapshots auszuwählen und sie in einer Operation zu löschen. Seien Sie außerdem vorsichtig, wenn Sie Bereinigungskripts und Automatisierung verwenden, damit Sie nicht versehentlich Snapshots löschen, die Sie benötigen. Die Papierkorb-Funktion trägt dazu bei, diese Art von Situationen zu schützen.

Archivieren von EBS-Snapshots

[Die Archivierung Ihrer EBS-Snapshots](#) kann eine kostengünstige Methode sein, um eine Kopie eines Volumes für Referenzzwecke aufzubewahren, die Sie 90 oder mehr Tage lang nicht wiederherstellen möchten. Dies kann ein guter Zwischenschritt sein, bevor alle zugehörigen Snapshots für ein EBS-Volume dauerhaft gelöscht werden. Sie können beispielsweise die Archivierung von Snapshots als end-of-lifecycle Schritt für EBS-Volumes in Betracht ziehen, die nicht mehr verwendet werden. Die Archivierung anstelle des Löschens kann auch eine kostengünstigere Methode der Löschaufbewahrung sein, anstatt den Papierkorb zu verwenden.

Automatisieren der Snapshot- und AMI-Erstellung mit Systems Manager AWS CLI, und den AWS SDKs

Ihr Backup-Ansatz erfordert möglicherweise Vorgänge vor und nach der Erstellung eines Snapshots oder AMI. Beispielsweise müssen Sie möglicherweise -Services anhalten und starten, um das Dateisystem in den Ruhezustand zu versetzen. Oder Sie müssen Ihre Instance während der AMI-Erstellung anhalten und starten. Möglicherweise müssen Sie auch Backups mehrerer Komponenten in Ihrer Architektur zusammen erstellen, jede mit eigenen Schritten vor und nach der Erstellung.

Sie können Ihre Wartungsfensterzeiten für Ihre Backups reduzieren, indem Sie Ihren Prozess automatisieren und überprüfen, ob Ihr Backup-Prozess konsistent angewendet wird. Um Ihre

benutzerdefinierten Vorgänge vor und nach der Erstellung zu automatisieren, erstellen Sie ein Skript für Ihren Backup-Prozess mithilfe der AWS CLI und des SDK.

Ihre Automatisierung kann in einem Systems Manager-Runbook definiert werden, das bei Bedarf oder während eines Systems Manager-Wartungsfensters ausgeführt werden kann. Sie können Ihren Benutzern Zugriff zum Ausführen von Systems Manager-Runbooks gewähren, ohne ihnen Berechtigungen für störende Amazon EC2-Befehle erteilen zu müssen. Auf diese Weise können Sie auch überprüfen, ob Ihr Backup-Prozess und Ihre Tags konsistent von Ihren Benutzern angewendet werden. Sie können die [AWS-CreateSnapshot](#) und [AWS-CreatelImage](#)--Runbooks zum Erstellen von Snapshots und AMIs verwenden oder anderen Benutzern Berechtigungen zur Verwendung erteilen. Systems Manager enthält auch die [AWS-UpdateLinuxAmi](#) und [AWS-UpdateWindowsAmi](#)-Runbooks zur Automatisierung des AMI-Patchings und der AMI-Erstellung.

Sie können auch die AWS CLI und verwenden [AWS Tools for Windows PowerShell](#), um Ihren Snapshot- und AMI-Erstellungsprozess zu automatisieren. Sie können den Befehl [aws ec2 create-snapshot](#) AWS CLI verwenden, um einen Snapshot eines EBS-Volumes als einen Schritt in Ihrer Automatisierung zu erstellen. Sie können den Befehl [aws ec2 create-snapshots](#) verwenden, um absturzkonsistente, synchronisierte Snapshots aller Volumes zu erstellen, die an Ihre EC2-Instance angehängt sind.

Sie können die AWS CLI verwenden, um neue AMIs zu erstellen. Sie können den Befehl [aws ec2 register-image](#) verwenden, um ein neues Image für Ihre EC2-Instance zu erstellen. Um das Herunterfahren, die Image-Erstellung und den Neustart Ihrer Instances zu automatisieren, kombinieren Sie diesen Befehl mit den Befehlen [aws ec2 stop-instances](#) und [aws ec2 start-instances](#).

Wiederherstellen eines Amazon-EBS-Volumes oder einer EC2-Instance

Wenn Sie nur ein einzelnes Volume wiederherstellen müssen, das einer EC2-Instance zugeordnet ist, können Sie dieses Volume separat wiederherstellen, das vorhandene Volume trennen und das wiederhergestellte Volume an Ihre EC2-Instance anfügen. Wenn Sie eine gesamte EC2-Instance wiederherstellen müssen, einschließlich aller zugehörigen Volumes, müssen Sie ein Amazon Machine Image (AMI)-Backup Ihrer Instance verwenden.

Um die Wiederherstellungszeit und die Auswirkungen auf abhängige Anwendungen und Prozesse zu reduzieren, muss Ihr Wiederherstellungsprozess die Ressource berücksichtigen, die er ersetzt. Um optimale Ergebnisse zu erzielen, testen Sie Ihren Wiederherstellungsprozess

regelmäßig in niedrigeren Umgebungen (z. B. Nicht-Produktion), um sicherzustellen, dass Ihr Prozess Ihr Recovery Point Objective (RPO) und Recovery Time Objective (RTO) erfüllt und dass der Wiederherstellungsprozess wie erwartet funktioniert. Überlegen Sie, wie sich der Wiederherstellungsprozess auf Anwendungen und Services auswirkt, die von der Instance abhängen, die Sie wiederherstellen, und koordinieren Sie dann die Wiederherstellung nach Bedarf. Versuchen Sie, den Wiederherstellungsprozess so weit wie möglich zu automatisieren und zu testen, um das Risiko zu verringern, dass Ihr Wiederherstellungsprozess fehlschlägt oder inkonsistent implementiert wird.

Wenn Sie Elastic Load Balancing verwenden und mehrere Instances den Datenverkehr bedienen, können Sie eine ausgefallene oder beeinträchtigte Instance außer Betrieb nehmen. Anschließend können Sie eine neue Instance wiederherstellen, um sie zu ersetzen, während die anderen Instances den Datenverkehr weiterhin ohne Unterbrechung der Benutzer bedienen.

Die folgenden beschriebenen Wiederherstellungsprozesse gelten für Instances, die Elastic Load Balancing nicht verwenden:

- Wiederherstellen einzelner Dateien und Verzeichnisse aus EBS-Snapshots
- Wiederherstellen eines EBS-Volumes aus einem Amazon-EBS-Snapshot
- Erstellen oder Wiederherstellen einer EC2-Instance aus einem EBS-Snapshot
- Wiederherstellen einer laufenden Instance aus einem AMI

Wiederherstellen von Dateien und Verzeichnissen aus EBS-Snapshots

[EBS-Snapshots](#) stellen ein point-in-time exaktes Replikat des ursprünglichen Volumes bereit, das zum Erstellen des Snapshots verwendet wurde. Gehen Sie wie folgt vor, um einzelne Dateien oder Verzeichnisse wiederherzustellen:

1. Stellen Sie [zunächst das Volume aus dem EBS-Snapshot wieder her](#), der die Dateien oder Verzeichnisse enthält.
2. Fügen Sie das Volume an die EC2-Instance an, auf der Sie die Dateien wiederherstellen möchten.
3. Kopieren Sie die Dateien vom wiederhergestellten Volume auf Ihr EC2-Instance-Volume.
4. Trennen und löschen Sie das wiederhergestellte Volume.

Wiederherstellen eines EBS-Volumes aus einem Amazon-EBS-Snapshot

Sie können ein Volume wiederherstellen, das einer vorhandenen EC2-Instance angefügt ist, indem Sie ein Volume aus seinem Snapshot erstellen und es an Ihre Instance anfügen. Sie können die Konsole, die oder die -API-Operationen verwenden AWS CLI, um ein Volume aus einem vorhandenen Snapshot zu erstellen. Anschließend können Sie das Volume mithilfe des Betriebssystems an die Instance mounten.

Beachten Sie, dass Daten aus einem Amazon-EBS-Snapshot asynchron in ein EBS-Volume geladen werden. Wenn eine Anwendung auf das Volume zugreift, auf das die Daten nicht geladen werden, ist die Latenz höher als normal, während die Daten aus Amazon S3 geladen werden. Um diese Auswirkungen für latenzempfindliche Anwendungen zu vermeiden, haben Sie zwei Möglichkeiten:

- Sie können [das EBS-Volume initialisieren](#).
- Gegen eine zusätzliche Gebühr unterstützt Amazon EBS die [schnelle Snapshot-Wiederherstellung](#), wodurch die Initialisierung Ihres Volumes überflüssig wird.

Wenn Sie ein Volume ersetzen, das denselben Mountingpunkt verwenden muss, müssen Sie dieses Volume entpacken, damit Sie das neue Volume an seiner Stelle mounten können. Um das Mounting des Volumes aufzuheben, stoppen Sie zunächst alle Prozesse, die das Volume verwenden. Wenn Sie das Stamm-Volume ersetzen, müssen Sie zuerst die Instance anhalten, bevor Sie das Stamm-Volume trennen können.

Gehen Sie beispielsweise wie folgt vor, um ein Volume mithilfe der Konsole in einer früheren point-in-time Sicherung wiederherzustellen:

1. Wählen Sie in der Amazon EC2-Konsole im Menü Elastic Block Store die Option Snapshots aus.
2. Suchen Sie nach dem Snapshot, den Sie wiederherstellen möchten, und wählen Sie ihn aus.
3. Wählen Sie Aktionen und dann Volume erstellen aus.
4. Erstellen Sie das neue Volume in derselben Availability Zone wie Ihre EC2-Instance.
5. Wählen Sie in der Amazon EC2-Konsole die Instance aus.
6. Notieren Sie sich in den Instance-Details den Gerätenamen, den Sie ersetzen möchten, im Eintrag Root-Gerät oder Blockgeräte.
7. Fügen Sie das Volume an. Der Prozess unterscheidet sich für Root-Volumes und Nicht-Root-Volumes.

Für Root-Volumes:

- a. Halten Sie die EC2-Instance an.

- b. Wählen Sie im Menü EC2 Elastic Block Store Volumes das Stamm-Volume aus, das Sie ersetzen möchten.
- c. Wählen Sie Aktionen und dann Volume trennen aus.
- d. Wählen Sie im Menü EC2 Elastic Block Store Volumes das neue Volume aus.
- e. Wählen Sie Aktionen und dann Volume anfügen aus.
- f. Wählen Sie die Instance aus, an die Sie das Volume anfügen möchten, und verwenden Sie denselben Gerätenamen, den Sie zuvor notiert haben.

Für Nicht-Root-Volumes:

- a. Wählen Sie im Menü EC2 Elastic Block Store Volumes das Nicht-Root-Volume aus, das Sie ersetzen möchten.
- b. Wählen Sie Aktionen und dann Volume trennen aus.
- c. Fügen Sie das neue Volume an, indem Sie es im Menü EC2 Elastic Block Store Volumes auswählen und dann Aktionen , Volume anfügen auswählen. Wählen Sie die Instance aus, an die Sie sie anfügen möchten, und wählen Sie dann einen verfügbaren Gerätenamen aus.
- d. Heben Sie mit dem Betriebssystem für die Instance das Mounting des vorhandenen Volumes auf und mounten Sie dann das neue Volume an seiner Stelle.

Unter Linux können Sie den `umount` Befehl verwenden. Unter Windows können Sie einen logischen Volume-Manager (LVM) wie das Dienstprogramm Datenträgerverwaltungssystem verwenden.

- e. Trennen Sie alle vorherigen Volumes, die Sie möglicherweise ersetzen, indem Sie sie im Menü EC2 Elastic Block Store Volumes auswählen und dann Aktionen , Volume trennen auswählen.

Sie können die auch AWS CLI in Kombination mit Betriebssystembefehlen verwenden, um diese Schritte zu automatisieren.

Erstellen oder Wiederherstellen einer EC2-Instance aus einem EBS-Snapshot

Um ein Backup zu erstellen, das zur Wiederherstellung einer gesamten EC2-Instance verwendet wird, empfehlen wir, ein Amazon Machine Image (AMI) zu erstellen. AMIs erfassen Maschineninformationen wie den Virtualisierungstyp. Sie erstellen auch Snapshots für jedes Volume, das an die EC2-Instance angefügt ist, einschließlich ihrer Gerätezuordnungen, sodass sie in derselben Konfiguration wiederhergestellt werden können.

Wenn Sie jedoch einen EBS-Snapshot verwenden müssen, um eine Instance wiederherzustellen, erstellen Sie zunächst ein AMI aus einem EBS-Snapshot, das zum Stamm-Volume für Ihre neue EC2-Instance wird:

1. Wählen Sie in der Amazon EC2-Konsole im Menü Elastic Block Store die Option Snapshots aus.
2. Suchen Sie nach dem Snapshot, der zum Erstellen des Stamm-Volumes für Ihre neue EC2-Instance verwendet wird, und wählen Sie ihn aus.
3. Wählen Sie Aktionen und dann Image aus Snapshot erstellen aus.
4. Geben Sie einen Namen für Ihr Image ein (z. B. YYYYMMDD-restore-for-i-012345678998765de) und wählen Sie die entsprechenden Optionen für Ihr neues Image aus.

Nachdem das Image erstellt und verfügbar wurde, können Sie eine neue EC2-Instance starten, die den EBS-Snapshot für das Stamm-Volume verwendet.

Wiederherstellen einer laufenden Instance aus einem AMI

Sie können eine neue Instance aus Ihrem AMI-Backup aufrufen, um eine vorhandene, ausgeführte Instance zu ersetzen. Ein Ansatz besteht darin, die vorhandene Instance anzuhalten, sie offline zu lassen, während Sie eine neue Instance von Ihrem AMI aus starten, und alle erforderlichen Updates durchzuführen. Dieser Ansatz reduziert das Risiko von Konflikten durch beide Instances, die gleichzeitig ausgeführt werden. Es ist ein akzeptabler Ansatz, wenn die Services, die Ihre Instance bereitstellt, ausfallen oder Sie die Wiederherstellung während eines Wartungsfensters durchführen. Nachdem Sie Ihre neue Instance getestet haben, können Sie alle Elastic IP-Adressen neu zuweisen, die der alten Instance zugewiesen wurden. Anschließend können Sie alle DNS-Datensätze (Domain Name Service) aktualisieren, um auf die neue Instance zu verweisen.

Wenn Sie jedoch während einer Wiederherstellung die Ausfallzeit Ihrer laufenden Instance minimieren müssen, sollten Sie erwägen, eine neue Instance aus Ihrem AMI-Backup zu starten und zu testen. Ersetzen Sie dann die vorhandene Instance durch die neue Instance.

Während beide Instances ausgeführt werden, müssen Sie verhindern, dass die neue Instance zu Kollisionen auf Plattform- oder Anwendungsebene führt. Beispielsweise können Probleme mit Windows-Instances auftreten, die mit der Domain verbunden sind und mit denselben SIDs und demselben Computernamen ausgeführt werden. Ähnliche Probleme können bei Netzwerkanwendungen und -services auftreten, die eindeutige Kennungen erfordern.

Um zu verhindern, dass andere Server und Services eine Verbindung zu Ihrer neuen Instance herstellen, bevor sie bereit ist, verwenden Sie Sicherheitsgruppen, um alle eingehenden

Verbindungen für Ihre neue Instance vorübergehend zu blockieren, mit Ausnahme Ihrer eigenen IP-Adresse für den Zugriff und das Testen. Sie können ausgehende Verbindungen für die neue Instance auch vorübergehend blockieren, um zu verhindern, dass Services und Anwendungen Verbindungen oder Updates zu anderen Ressourcen initiieren. Wenn die neue Instance bereit ist, stoppen Sie die vorhandene Instance, starten Sie Services und Prozesse auf der neuen Instance und entsperren Sie dann alle ein- oder ausgehenden Netzwerkverbindungen, die Sie implementiert haben.

Backup und Wiederherstellung von der lokalen Infrastruktur auf AWS

Sie können Backups AWS für die dauerhafte, externe Speicherung Ihrer lokalen Infrastruktur-Backups verwenden. Durch die Verwendung von AWS Speicherdiensten in diesem Szenario können Sie sich auf Sicherungs- und Archivierungsaufgaben konzentrieren. Sie müssen sich keine Gedanken über die Bereitstellung, Skalierung oder Infrastrukturkapazität der Speicherinfrastruktur für Ihre Backup-Aufgaben machen.

Amazon S3 bietet umfangreiche API-Operationen und SDKs zur Integration in Ihre neuen und bestehenden Backup- und Wiederherstellungsansätze. Dies bietet Anbietern von Backup-Software auch die Möglichkeit, ihre Anwendungen direkt in AWS Speicherlösungen zu integrieren.

In diesem Szenario ist die Sicherungs- und Archivierungssoftware, die Sie in Ihrer lokalen Infrastruktur verwenden, AWS über die API-Operationen direkt mit der Software verbunden. Da die Backup-Software AWS-fähig ist, werden die Daten von den lokalen Servern direkt auf Amazon S3 gesichert.

Wenn Ihre bestehende Backup-Software die AWS Cloud nicht nativ unterstützt, können Sie Storage Gateway verwenden. Storage Gateway ist ein Cloud-Speicherdienst und bietet Ihren lokalen Systemen Zugriff auf skalierbaren Cloud-Speicher. Es unterstützt offene Standardspeicherprotokolle, die mit Ihren vorhandenen Anwendungen funktionieren und gleichzeitig Ihre Daten sicher verschlüsselt in Amazon S3 speichern. Sie können Storage Gateway als Teil eines Backup- und Recovery-Ansatzes für Ihre lokalen blockbasierten Speicher-Workloads verwenden.

Storage Gateway ist in hybriden Szenarien hilfreich, in denen Sie für Ihre Backups auf Cloud-basierten Speicher umsteigen möchten. Storage Gateway hilft Ihnen auch dabei, Kapitalinvestitionen in lokalen Speicher zu reduzieren. Sie stellen Storage Gateway als VM oder als dedizierte Hardware-Appliance bereit. Dieses Handbuch konzentriert sich darauf, wie Storage Gateway auf Backup und Recovery angewendet wird.

Storage Gateway bietet drei verschiedene Optionen, um unterschiedlichen Anforderungen gerecht zu werden:

- Ein Datei-Gateway zum Speichern von Anwendungsdatendateien und Backup-Images als dauerhafte Objekte im Amazon S3 S3-Cloud-Speicher mit SMB- oder NFS-basiertem Zugriff.
- Ein Volume-Gateway zur Präsentation von cloudbasierten iSCSI-Blockspeicher-Volumes für Ihre lokalen Anwendungen. Ein Volume-Gateway bietet entweder einen lokalen Cache oder

vollständige Volumes vor Ort und speichert gleichzeitig vollständige Kopien Ihrer Volumes in der AWS Cloud.

- Ein Band-Gateway, um vertrauenswürdige Backup-Software auf ein lokales Speicher-Gateway zu verweisen, das wiederum eine Verbindung zu Amazon S3 herstellt. Diese Option bietet die Skalierbarkeit und Stabilität der Cloud für eine sichere, langfristige Aufbewahrung, ohne bestehende Investitionen oder Prozesse zu stören.

File Gateway

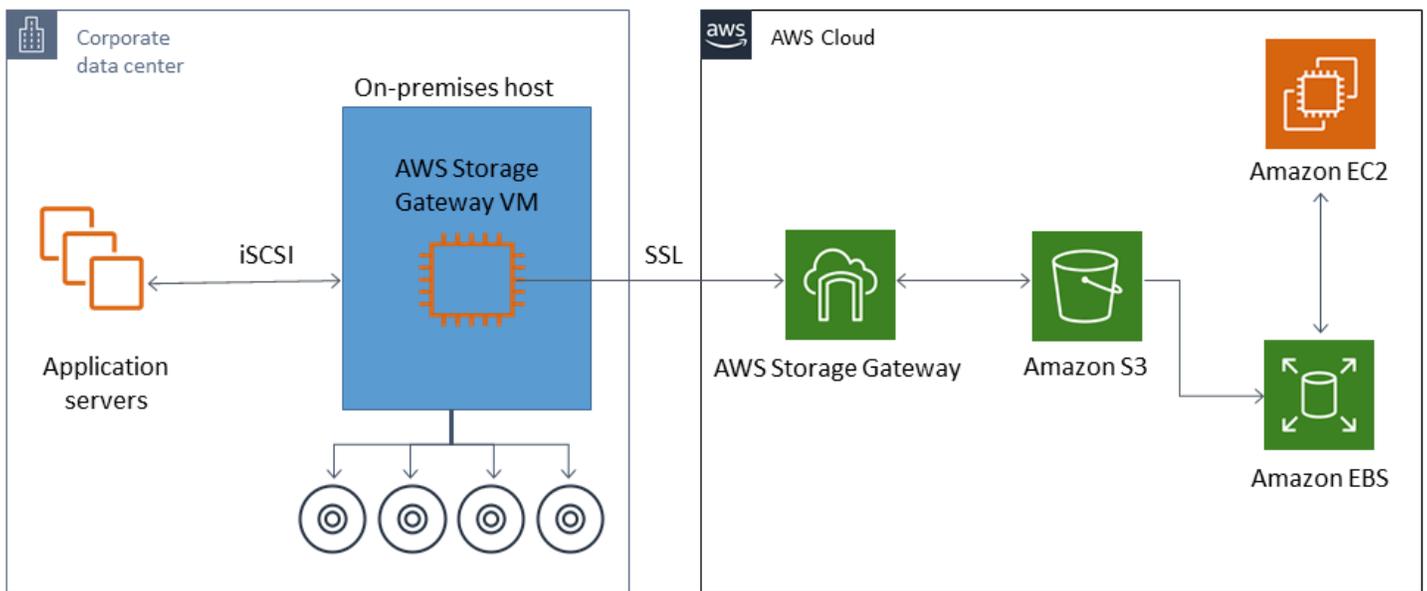
Viele Unternehmen beginnen ihre Reise in die Cloud damit, sekundäre und tertiäre Daten wie Backups in die Cloud zu verlagern. Die SMB- und NFS-Schnittstellenunterstützung eines File-Gateways bietet IT-Gruppen die Möglichkeit, Backup-Jobs von bestehenden lokalen Backup-Systemen in die Cloud zu verlagern. Backup-Anwendungen, native Datenbanktools oder Skripts, die in SMB oder NFS schreiben können, können in ein File-Gateway schreiben. Das File-Gateway speichert die Backups als Amazon S3 S3-Objekte mit einer Größe von bis zu 5 TiB. Mit einem ausreichend großen lokalen Cache können aktuelle Backups für schnelle Wiederherstellungen vor Ort verwendet werden. Langfristige Archivierungsanforderungen werden erfüllt, indem Backups den kostengünstigen Speicherklassen S3 Standard-Infrequent Access und S3 Glacier zugeordnet werden.

File Gateway bietet eine Einstiegsmöglichkeit für Ihren blockbasierten Speicher auf Amazon S3 für äußerst langlebige externe Backups. Es ist besonders nützlich für Szenarien, in denen eine kürzlich gesicherte Datei schnell wiederhergestellt werden muss. Da ein File-Gateway die SMB- und NFS-Protokolle unterstützt, können Benutzer auf Dateien genauso zugreifen wie auf eine Netzwerkdateifreigabe. Sie können auch die Funktionen zur Objektversionsverwaltung von Amazon S3 nutzen. Mithilfe der Objektversionierung können Sie frühere Objektversionen für eine Datei wiederherstellen und dann einfach mit SMB oder NFS darauf zugreifen.

Volume Gateway

Mit einem Volume-Gateway können Sie cloudbasierte iSCSI-Blockspeicher-Volumes für Ihre lokalen Server bereitstellen. Das Volume Gateway speichert Ihre Volumendaten in Amazon S3 für eine dauerhafte, skalierbare Cloud-basierte externe Speicherung. Ein Volume-Gateway erleichtert die Erstellung vollständiger point-in-time Snapshots Ihrer Volumes und deren Speicherung in der Cloud als Amazon EBS-Snapshots. Nachdem sie als Snapshots gespeichert wurden, können ganze Volumes als EBS-Volumes wiederhergestellt und an EC2-Instances angehängt werden, was eine cloudbasierte DR-Lösung beschleunigt. Die Volumes können auch auf Storage Gateway

wiederhergestellt werden, sodass Ihre lokalen Anwendungen in einen früheren Zustand zurückkehren können.



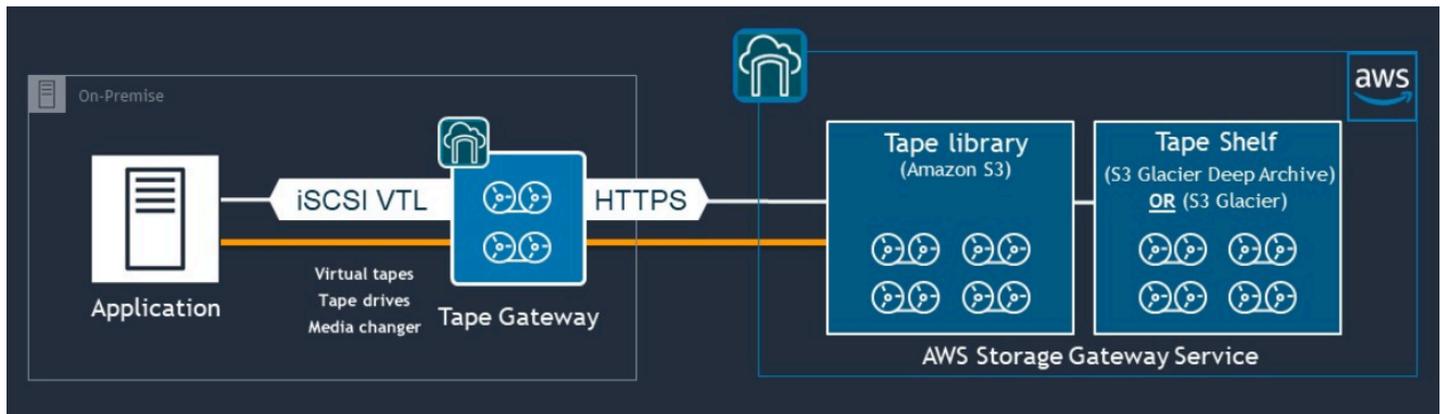
Da ein Volume-Gateway in die Amazon EBS-Volume-Funktion von Amazon EC2 integriert ist, können Sie AWS Backup damit Ihren Snapshot-Prozess automatisieren und planen. Ein Volume-Gateway bietet Ihnen die zusätzlichen Vorteile langlebiger, von Amazon S3 unterstützter Amazon EBS-Snapshots und Tagging-Funktionen. Weitere Informationen finden Sie in der [Amazon EBS-Snapshot-Dokumentation](#).

Tape Gateway

Ein Band-Gateway bietet die hohe Haltbarkeit, den kostengünstigen mehrstufigen Speicher und die umfangreichen Funktionen von Amazon S3 für Ihren externen virtuellen Bandsicherungsspeicher. Alle Ihre in Amazon S3 gespeicherten virtuellen Bänder werden repliziert und in mindestens drei geografisch verteilten Availability Zones gespeichert. Ihre virtuellen Bänder sind durch eine Haltbarkeit von 11 Stunden geschützt.

AWS führt außerdem regelmäßig Stabilitätsprüfungen durch, um sicherzustellen, dass Ihre Daten gelesen werden können und keine Fehler aufgetreten sind. Alle in Amazon S3 gespeicherten Bänder sind durch serverseitige Verschlüsselung mit Standardschlüsseln oder Ihren AWS KMS Schlüsseln geschützt. Darüber hinaus vermeiden Sie physische Sicherheitsrisiken, die mit der Portabilität von Bändern verbunden sind. Mit einem Band-Gateway erhalten Sie korrekte Daten im Vergleich zur externen Lagerung von Bändern, bei der Sie bei der Wiederherstellung möglicherweise ein falsches oder kaputtes Band erhalten.

Sie können monatliche Speicherkosten sparen, wenn Sie Ihre Daten in Amazon S3 speichern. Mit S3 Glacier Deep Archive können Sie noch mehr für Ihre langfristigen Archivierungsanforderungen sparen.



Ein Band-Gateway fungiert als virtuelle Bandbibliothek (VTL), die sich von Ihrer lokalen Umgebung bis hin zu hoch skalierbaren, redundanten und dauerhaften Speicherdiensten erstreckt: Amazon S3, S3 Glacier Flexible Retrieval und S3 Glacier Deep Archive.

Das Tape Gateway bietet Storage Gateway für Ihre bestehende Backup-Anwendung als offene Standard-iSCSI-basierte VTL mit einem Virtual Media Changer und virtuellen Bandlaufwerken. Sie können Ihre vorhandenen Backup-Anwendungen und Workflows weiterhin verwenden und gleichzeitig auf eine Sammlung virtueller Bänder schreiben, die auf dem extrem skalierbaren Amazon S3 gespeichert sind. Wenn Sie keinen sofortigen oder häufigen Zugriff mehr auf die Daten auf einem virtuellen Band benötigen, kann Ihre Backup-Anwendung sie in S3 Glacier Flexible Retrieval oder S3 Glacier Deep Archive archivieren, wodurch die Speicherkosten weiter gesenkt werden.

Sie können ein Band, das in S3 Glacier Flexible Retrieval oder S3 Glacier Deep Archive archiviert wurde, in der Regel innerhalb von 3–5 Stunden bzw. 12 Stunden abrufen. Das Tape-Gateway kann mit einer Backup-Anwendung verwendet werden, die mit der iSCSI-basierten Bandbibliotheksschnittstelle für den Zugriff auf die virtuellen Bänder kompatibel ist. Beachten Sie auch die Mindestspeichergröße von 100 GB pro Band. Weitere Informationen finden Sie in der Liste der [Backup-Anwendungen von Drittanbietern](#), die Band-Gateways unterstützen.

Backup und Wiederherstellung von Anwendungen von AWS zu Ihrem Rechenzentrum

Möglicherweise verfügen Sie über eine Richtlinie, nach der Sie ein Szenario wie DR oder Business Continuity für Ihre cloudbasierten Workloads und Ihre lokale Infrastruktur implementieren müssen. Wenn Sie bereits über ein Datensicherungs-Framework für Ihre lokalen Server verfügen, können Sie es auf Ihre AWS-Ressourcen über eine VPN-Verbindung oder durch AWS Direct Connect aus. Sie können den Backup-Agent auf den EC2-Instanzen installieren und Ihre Daten und Anwendungen gemäß Ihren Datenschutzrichtlinien sichern. Sie können Amazon S3 auch als Zwischendienst verwenden, um Ihre Backups auf Anwendungsebene zu speichern. Sie können dann die API-Operationen, SDKs oder die AWS CLI um die Daten in Ihrer lokalen Umgebung wiederherzustellen.

So sichern Sie Daten in AWS und andere Dienste als Amazon EC2, verwenden Sie die AWS CLI, SDKs und API-Operationen, um die Daten in Ihr gewünschtes Format zu extrahieren. Kopieren Sie die Daten dann in Amazon S3 und kopieren Sie sie von Amazon S3 in Ihre lokale Umgebung. Einige Dienste bieten direkten Export nach Amazon S3. Amazon RDS unterstützt beispielsweise [Native Sicherung](#) von Microsoft SQL Server-Datenbanken zu Amazon S3.

Backup und Wiederherstellung von Cloud-nativen AWS Diensten

Ihr Sicherungs- und Wiederherstellungsansatz sollte die AWS Dienste abdecken, die in Ihren Workloads verwendet werden. AWS bietet dienstspezifische Funktionen und Optionen für die Verwaltung und Interaktion mit Ihren Daten. Sie können die Konsole, die AWS CLI, SDKs und API-Operationen verwenden, um Backup und Recovery für die von Ihnen verwendeten AWS Dienste zu implementieren. In diesem Handbuch werden [Amazon RDS](#) und [Amazon DynamoDB](#) als Beispiele behandelt. AWS Backup unterstützt sowohl DynamoDB als auch Amazon RDS und sollte verwendet werden, wenn es Ihren Anforderungen entspricht.

Backup und Wiederherstellung für Amazon RDS

Amazon RDS enthält Funktionen zur Automatisierung von Datenbank-Backups. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer Datenbank-Instance, damit die gesamte DB-Instance gesichert wird und nicht nur nur nur nur nur nur nur einzelne Datenbanken. Mit Amazon RDS können Sie ein Backup-Fenster für automatische Backups einrichten, Datenbank-Instanz-Snapshots erstellen und Snapshots regionsübergreifend und kontoübergreifend teilen und kopieren.

Amazon RDS bietet zwei verschiedene Optionen für die Sicherung und Wiederherstellung Ihrer DB-Instances:

- Automatisierte Backups ermöglichen die point-in-time Wiederherstellung (PITR) Ihrer DB-Instance. Automatisierte Backups sind standardmäßig aktiviert, wenn Sie eine neue DB-Instance erstellen.

Amazon RDS führt während eines Backup-Fensters, das Sie bei der Erstellung der DB-Instance definieren, täglich eine vollständige Sicherung Ihrer Daten durch. Sie können eine Aufbewahrungsdauer von bis zu 35 Tagen für das automatische Backup konfigurieren. Amazon RDS lädt außerdem die Transaktionsprotokolle für DB-Instances alle 5 Minuten nach Amazon S3 hoch. Amazon RDS verwendet Ihre täglichen Backups zusammen mit Ihren Datenbanktransaktionsprotokollen, um Ihre DB-Instance wiederherzustellen. Sie können die Instance während Ihres Aufbewahrungszeitraums auf jede Sekunde bis zu `LatestRestorableTime` (in der Regel die letzten fünf Minuten) wiederherstellen.

Verwenden Sie den `DescribeDBInstances` API-Aufruf, um die letzte wiederherstellbare Zeit für Ihre DB-Instances zu ermitteln. Oder suchen Sie auf der Registerkarte Beschreibung nach der Datenbank in der Amazon RDS-Konsole.

Wenn Sie einen PITR initiieren, werden Transaktionsprotokolle mit dem am besten geeigneten täglichen Backup kombiniert, um Ihre DB-Instance zum angeforderten Zeitpunkt wiederherzustellen.

- -DB-Snapshots sind vom Benutzer initiierte Backups, die Sie zum Wiederherstellen Ihrer DB-Instance auf einen bekannten Zustand verwenden können, so häufig Sie möchten. Sie können diesen Zustand dann jederzeit wiederherstellen. Sie können die Amazon RDS-Konsole oder den `CreateDBSnapshot` API-Aufruf verwenden, um DB-Snapshots zu erstellen. Diese Snapshots werden so lange aufbewahrt, bis Sie sie mithilfe der Konsole oder des `DeleteDBSnapshot` API-Aufrufs explizit löschen.

Beide Backup-Optionen werden für Amazon RDS in unterstützt AWS Backup, das auch andere Funktionen bietet. Erwägen Sie AWS Backup, einen Standard-Backup-Plan für Ihre Amazon RDS-Datenbanken einzurichten, und verwenden Sie die vom Benutzer initiierten Instanz-Backup-Optionen, wenn Ihre Backup-Pläne für eine bestimmte Datenbank einzigartig sind.

Amazon RDS verhindert den direkten Zugriff auf den zugrunde liegenden Speicher, der von der DB-Instance verwendet wird. Dadurch wird auch verhindert, dass Sie die Datenbank auf einer RDS-DB-Instance direkt auf ihre lokale Festplatte exportieren. In einigen Fällen können Sie native Sicherungs- und Wiederherstellungsfunktionen mithilfe von Client-Dienstprogrammen verwenden. Sie können beispielsweise den [Befehl `mysqldump` mit einer Amazon RDS MySQL-Datenbank verwenden, um eine Datenbank](#) auf Ihren lokalen Client-Computer zu exportieren. In einigen Fällen bietet Amazon RDS auch erweiterte Optionen für die Durchführung einer systemeigenen Sicherung und Wiederherstellung einer Datenbank. Amazon RDS bietet beispielsweise gespeicherte Prozeduren zum [Exportieren und Importieren von RDS-Datenbank-Backups von SQL Server-Datenbanken](#).

Stellen Sie sicher, dass Sie Ihren Datenbankwiederherstellungsprozess und seine Auswirkungen auf die Datenbank-Clients als Teil Ihres allgemeinen Sicherungs- und Wiederherstellungsansatzes gründlich testen.

Verwendung von DNS-CNAME-Einträgen zur Reduzierung der Auswirkungen auf den Client bei einer Datenbankwiederherstellung

Wenn Sie eine Datenbank mithilfe von PITR oder einem RDS-DB-Instance-Snapshot wiederherstellen, wird eine neue DB-Instance mit einem neuen Endpunkt erstellt. Auf diese Weise können Sie mehrere DB-Instances aus einem bestimmten DB-Snapshot oder zu einem bestimmten Zeitpunkt erstellen. Bei der Wiederherstellung einer RDS-DB-Instance, um eine Live-

RDS-DB-Instance zu ersetzen, müssen besondere Überlegungen angestellt werden. Sie müssen beispielsweise festlegen, wie Sie Ihre vorhandenen Datenbank-Clients mit minimaler Unterbrechung und Änderung auf die neue Instanz umleiten. Sie müssen auch die Kontinuität und Konsistenz der Daten in der Datenbank sicherstellen, indem Sie die wiederhergestellte Datenzeit und die Wiederherstellungszeit berücksichtigen, zu der die neue Instanz beginnt, Schreibvorgänge zu empfangen.

Sie können einen separaten DNS-CNAME-Eintrag erstellen, der auf Ihren DB-Instance-Endpunkt verweist, und Ihre Kunden diesen DNS-Namen verwenden lassen. Dann können Sie den CNAME so aktualisieren, dass er auf einen neuen, wiederhergestellten Endpunkt verweist, ohne Ihre Datenbank-Clients aktualisieren zu müssen.

Stellen Sie die Gültigkeitsdauer (Time to Live) für Ihren CNAME-Eintrag auf einen entsprechenden Wert. Die von Ihnen angegebene TTL bestimmt, wie lange der Datensatz mit DNS-Resolvern zwischengespeichert wird, bevor eine weitere Anfrage gestellt wird. Es ist wichtig zu beachten, dass einige DNS-Resolver oder -Anwendungen die TTL möglicherweise nicht einhalten und den Datensatz möglicherweise länger als die TTL zwischenspeichern. Wenn Sie eine längere Dauer eingeben (beispielsweise 172 800 Sekunden oder 2 Tage), reduzieren Sie die Anzahl der Aufrufe, die rekursiven DNS-Resolver an Route 53 tätigen müssen, um die neuesten Informationen in diesem Datensatz abzurufen. Dies reduziert die Latenz und reduziert Ihre Rechnung für den Route 53-Dienst. Weitere Informationen finden Sie unter [So leitet Amazon Route 53 Datenverkehr an Ihre Domäne](#) weiter.

Anwendungen und Client-Betriebssysteme können auch DNS-Informationen zwischenspeichern, die Sie leeren oder neu starten müssen, um eine neue DNS-Auflösungsanforderung zu initiieren und den aktualisierten CNAME-Datensatz abzurufen.

Wenn Sie eine Datenbankwiederherstellung einleiten und den Traffic auf Ihre wiederhergestellte Instance verlagern, stellen Sie sicher, dass alle Ihre Clients in Ihre wiederhergestellte Instance schreiben und nicht in Ihre vorherige Instance. Ihre Datenarchitektur unterstützt möglicherweise die Wiederherstellung Ihrer Datenbank, die Aktualisierung von DNS, um den Datenverkehr auf Ihre wiederhergestellte Instance zu verlagern, und das anschließende Korrigieren aller Daten, die möglicherweise noch in Ihre vorherige Instance geschrieben wurden. Wenn dies nicht der Fall ist, können Sie Ihre bestehende Instance beenden, bevor Sie den DNS-CNAME-Eintrag aktualisieren. Dann erfolgt der gesamte Zugriff von Ihrer neu wiederhergestellten Instanz aus. Dies kann vorübergehend zu Verbindungsproblemen für einige Ihrer Datenbank-Clients führen, die Sie individuell behandeln können. Um die Auswirkungen auf den Client zu reduzieren, können Sie die Datenbankwiederherstellung während eines Wartungsfensters durchführen.

Schreiben Sie Ihre Anwendungen so, dass sie Datenbankverbindungsfehler mit Wiederholungsversuchen mithilfe des exponentiellen Backoffs ordnungsgemäß behandeln. Auf diese Weise kann Ihre Anwendung wiederhergestellt werden, wenn eine Datenbankverbindung während einer Wiederherstellung nicht verfügbar ist, ohne dass Ihre Anwendung unerwartet abstürzt.

Nachdem Sie den Wiederherstellungsvorgang abgeschlossen haben, können Sie Ihre vorherige Instance in einem gestoppten Zustand belassen. Oder Sie können Sicherheitsgruppenregeln verwenden, um den Datenverkehr auf Ihre vorherige Instance zu beschränken, bis Sie sicher sind, dass er nicht mehr benötigt wird. Beschränken Sie für eine schrittweise Außerbetriebnahme zunächst den Zugriff der Sicherheitsgruppe auf eine laufende Datenbank. Sie können die Instance irgendwann beenden, wenn sie nicht mehr benötigt wird. Erstellen Sie abschließend einen Snapshot der Datenbankinstanz und löschen Sie ihn.

Backup und Wiederherstellung für DynamoDB

DynamoDB stellt PITR bereit, damit die DynamoDB-Tabellendaten nahezu kontinuierlich Backups von DynamoDB-Tabellendaten erstellt werden. Wenn diese Option aktiviert ist, führt DynamoDB inkrementelle Backups Ihrer Tabelle für die letzten 35 Tage durch, bis Sie sie explizit deaktivieren.

Sie können auch On-Demand-Backups Ihrer DynamoDB-Tabelle erstellen, indem Sie die DynamoDB-Konsole, die AWS CLI, oder die DynamoDB-API verwenden. Weitere Informationen finden Sie unter [Sichern einer DynamoDB-Tabelle](#). Sie können periodische oder future Backups planen, indem Sie `aws backup` verwenden, oder Sie können Ihren Backupansatz mithilfe von Lambda-Funktionen anpassen und automatisieren. Weitere Informationen zur Verwendung von Lambda-Funktionen für DynamoDB finden Sie im Blog-Eintrag [A Serverless solution to schedule your Amazon DynamoDB On-Demand Backup](#). Wenn Sie keine Planungsskripts und Bereinigungsaufträge erstellen möchten, können Sie `aws backup` zum Erstellen von Backupplänen verwenden. Die Backup-Pläne enthalten Zeitpläne und Aufbewahrungsrichtlinien für Ihre DynamoDB-Tabellen. `aws backup` erstellt die Backups und löscht vorherige Backups auf der Grundlage Ihres Aufbewahrungsplans. `aws backup` enthält auch erweiterte DynamoDB-Backup-Optionen, die im DynamoDB-Service nicht verfügbar sind, darunter kostengünstigerer mehrstufiger Speicher sowie konto- und regionsübergreifendes Kopieren. Weitere Informationen finden Sie unter [Erweitertes DynamoDB-Backup](#).

In einer wiederhergestellten DynamoDB-Tabelle müssen Sie Folgendes manuell einrichten:

- Automatische Skalierungsrichtlinien
- IAM-Richtlinien

- CloudWatch Amazon-Metriken und -Alarme
- Tags (Markierungen)
- Stream-Einstellungen
- TTL-Einstellungen

Sie können nur die gesamten Tabellendaten aus einer neuen Tabelle aus einer neuen Tabelle wiederherstellen. Sie können erst Daten in die wiederhergestellte Tabelle schreiben, nachdem sie aktiv wird.

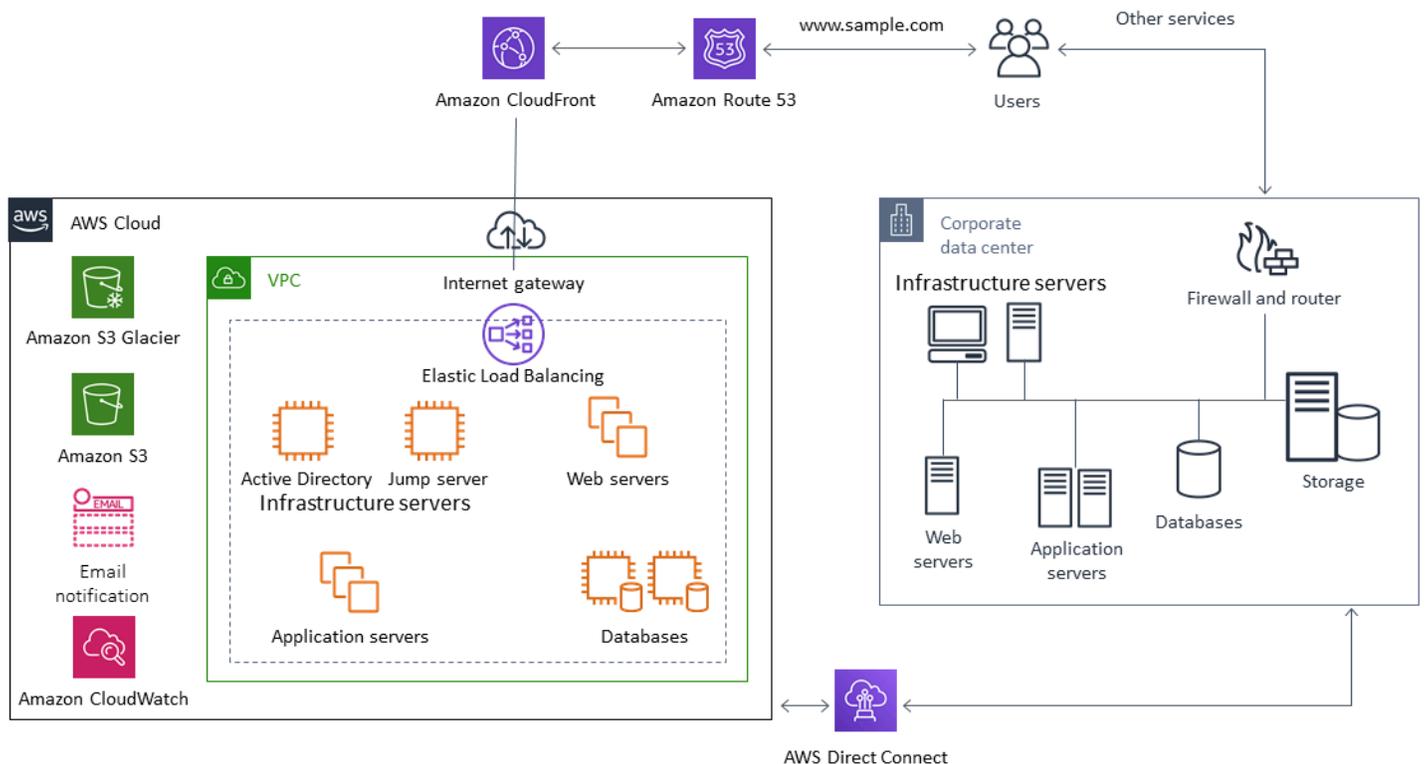
Bei Ihrem Wiederherstellungsprozess muss berücksichtigt werden, wie die Clients angewiesen werden, den Namen der neu wiederhergestellten Tabelle zu verwenden. Sie können Ihre Anwendungen und Clients so konfigurieren, dass sie den DynamoDB-Tabellennamen aus einer Konfigurationsdatei, einen AWS Systems Manager Parameterspeicherwert oder eine andere Referenz abrufen, die dynamisch aktualisiert werden kann, um den Tabellennamen wiederzugeben, den der Client verwenden soll.

Im Rahmen des Wiederherstellungsprozesses sollten Sie Ihren Umstellungsprozess sorgfältig abwägen. Sie können sich dafür entscheiden, den Zugriff auf Ihre bestehende DynamoDB-Tabelle über IAM-Berechtigungen zu verweigern und den Zugriff auf Ihre neue Tabelle zu gewähren. Anschließend können Sie die Anwendungs- und Client-Konfiguration aktualisieren, um die neue Tabelle zu verwenden. Möglicherweise müssen Sie auch die Unterschiede zwischen Ihrer vorhandenen DynamoDB-Tabelle und der neu wiederhergestellten DynamoDB-Tabelle abgleichen.

Backup und Recovery für Hybridarchitekturen

Die in diesem Leitfaden erörterten cloudnativen und lokalen Bereitstellungen können zu hybriden Szenarien kombiniert werden, in denen die Workload-Umgebung lokale Komponenten und Infrastrukturkomponenten umfasst. AWS Ressourcen, einschließlich Webserver, Anwendungsserver, Überwachungsserver, Datenbanken und Microsoft Active Directory, werden entweder im Kundenrechenzentrum oder auf dem Rechenzentrum gehostet AWS. Anwendungen, die in der AWS Cloud ausgeführt werden, sind mit Anwendungen verbunden, die vor Ort ausgeführt werden.

Dies wird zu einem häufigen Szenario für Unternehmens-Workloads. Viele Unternehmen verfügen über eigene Rechenzentren, die zur AWS Kapazitätserweiterung genutzt werden. Diese Kundenrechenzentren sind häufig über Netzwerkverbindungen mit hoher Kapazität mit dem AWS Netzwerk verbunden. Mit können Sie beispielsweise eine private [AWS Direct Connect](#), dedizierte Konnektivität von Ihrem lokalen Rechenzentrum zu einrichten. AWS Dies bietet die Bandbreite und die konsistente Latenz, um Daten aus Datenschutzgründen in die Cloud hochzuladen. Es bietet auch eine konsistente Leistung und Latenz für hybride Workloads. Das folgende Diagramm zeigt ein Beispiel für einen Ansatz in einer hybriden Umgebung.



Gut konzipierte Datenschutzlösungen verwenden in der Regel eine Kombination der Optionen, die in den cloudnativen und lokalen Lösungen in diesem Handbuch beschrieben sind. Viele ISVs bieten

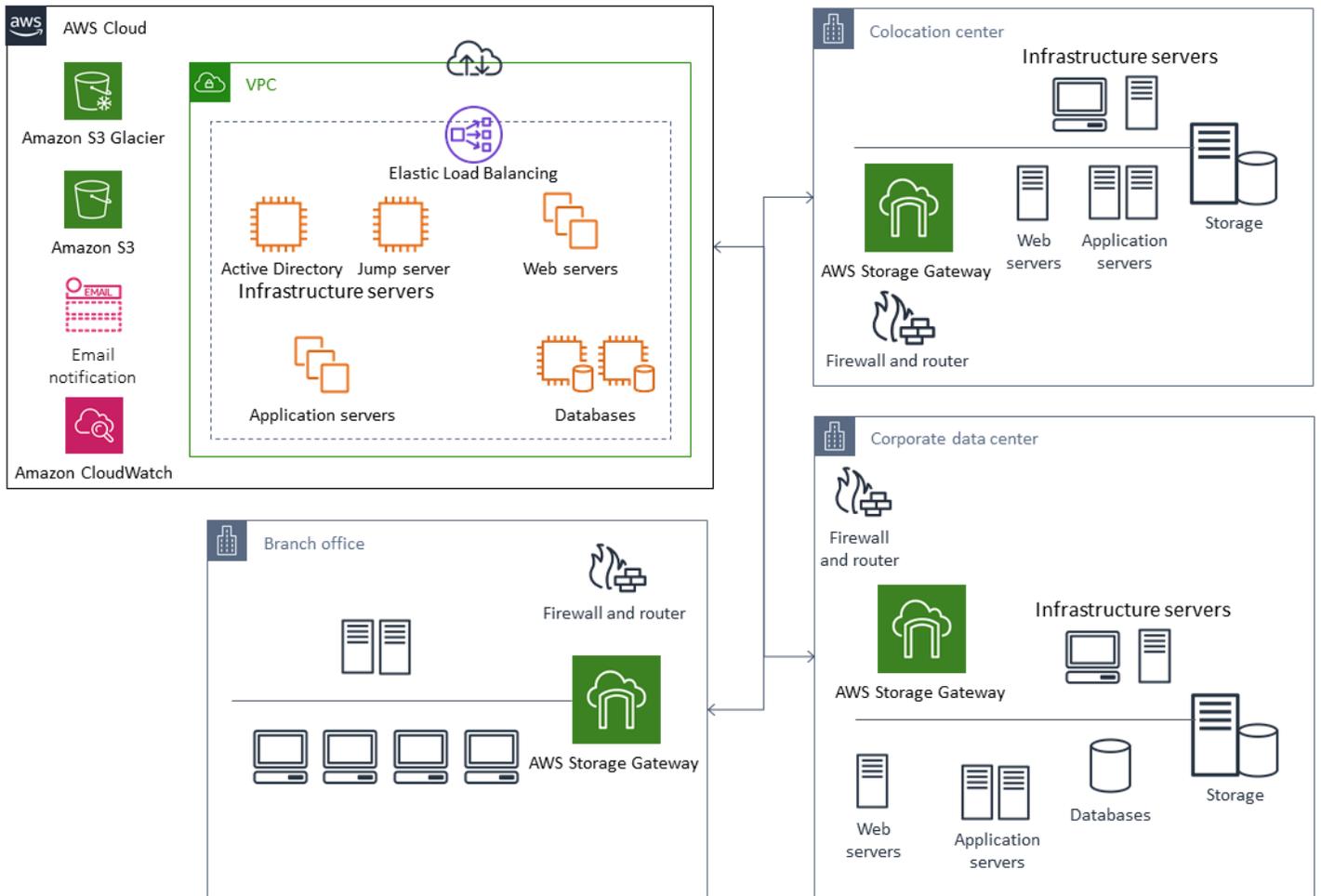
marktführende Sicherungs- und Wiederherstellungslösungen für lokale Infrastrukturen an und haben ihre Lösungen erweitert, um hybride Ansätze zu unterstützen.

Verlagerung zentralisierter Backup-Management-Lösungen in die Cloud für eine höhere Verfügbarkeit

Indem Sie Ihre vorhandenen Investitionen in die Backup-Management-Lösung nutzen AWS, können Sie die Ausfallsicherheit und Architektur Ihres Ansatzes verbessern. Möglicherweise verfügen Sie über einen primären Backup-Server und einen oder mehrere Medien- oder Speicherserver vor Ort an mehreren Standorten in der Nähe der Server und Dienste, die sie schützen. In diesem Fall sollten Sie erwägen, den primären Backup-Server auf eine EC2-Instance zu verlagern, um ihn vor lokalen Katastrophen zu schützen und eine hohe Verfügbarkeit zu gewährleisten.

Um die Backup-Datenflüsse zu verwalten, können Sie einen oder mehrere Medienserver auf EC2-Instances in derselben Region einrichten wie die Server, die sie schützen sollen. Medienserver in der Nähe der EC2-Instances sparen Ihnen Geld bei der Übertragung über das Internet. Wenn Sie auf Amazon S3 sichern, erhöhen Medienserver die allgemeine Sicherungs- und Wiederherstellungsleistung.

Sie können Storage Gateway auch verwenden, um zentralen Cloud-Zugriff auf Daten aus geografisch verteilten Rechenzentren und Büros bereitzustellen. Ein File-Gateway bietet Ihnen beispielsweise On-Demand-Zugriff mit niedriger Latenz auf Daten, die in AWS Anwendungsworkflows gespeichert sind, die sich über den ganzen Globus erstrecken können. Sie können Funktionen wie die Cache-Aktualisierung verwenden, um Daten an geografisch verteilten Standorten zu aktualisieren, sodass Inhalte problemlos in Ihren Büros gemeinsam genutzt werden können.



Disaster Recovery mit AWS

Die Backup- und Wiederherstellungsansätze sowie die unterstützenden Dienste und Technologien können zur Implementierung Ihrer Disaster Recovery-Lösung (DR) verwendet werden. Viele Unternehmen nutzen die AWS Cloud für Backup und Wiederherstellung sowie als DR-Standort. AWS bietet eine Reihe von Diensten und Funktionen, die DR und Geschäftskontinuität unterstützen.

Themen

- [On-Premises-DR zu AWS](#)
- [DR für cloudbative Workloads](#)

On-Premises-DR zu AWS

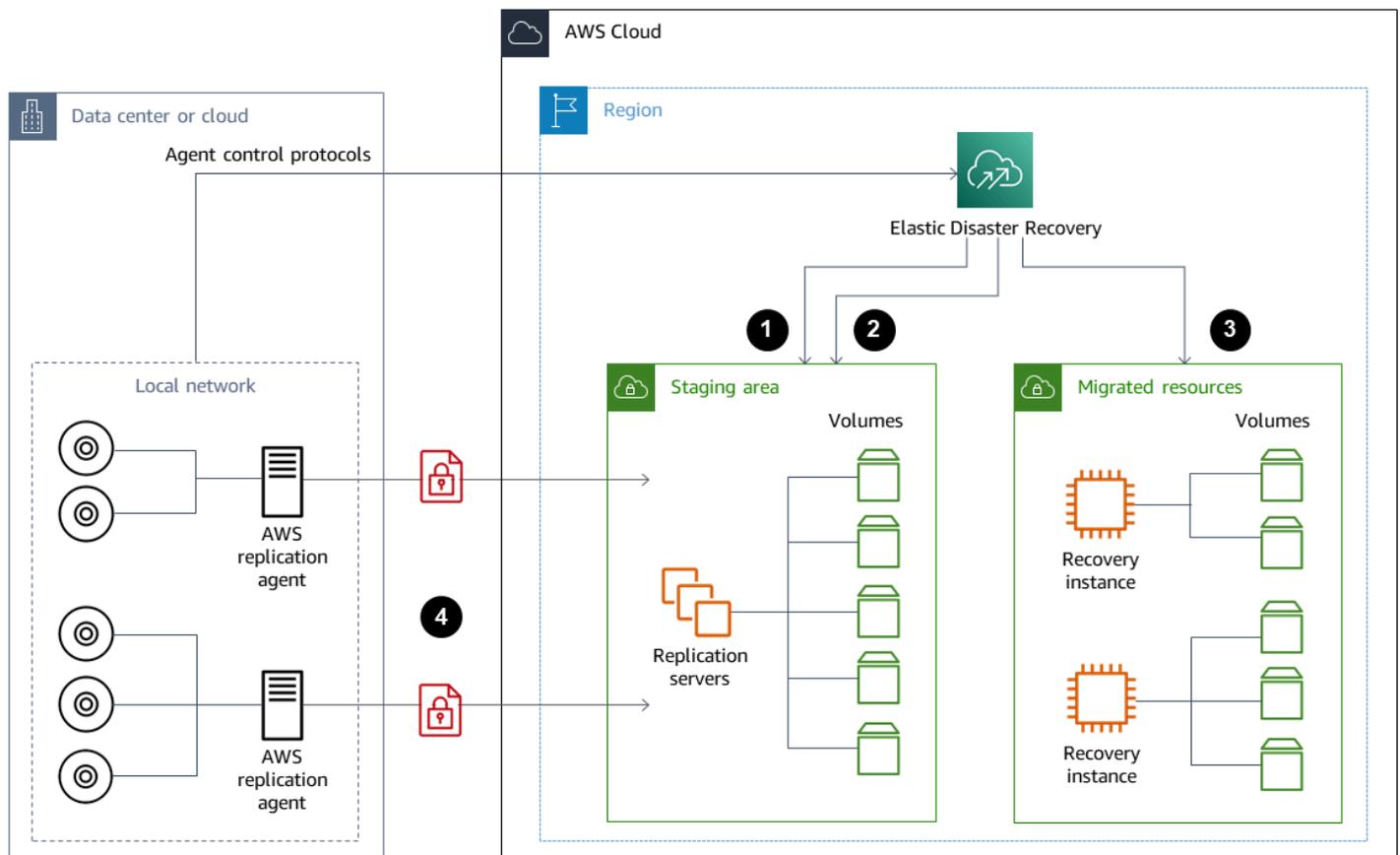
Die Verwendung AWS als externe Notfallwiederherstellungsumgebung (DR) für lokale Workloads ist ein gängiges Hybridszenario. Definieren Sie Ihre DR-Ziele, einschließlich der erforderlichen Wiederherstellungszeit und der erforderlichen Wiederherstellungspunktziele, bevor Sie die zu verwendenden Technologien auswählen. Als Hilfe bei dieser Definition können Sie die [Checkliste für den DR-Plan](#) verwenden.

Es stehen eine Reihe von Optionen zur Verfügung, mit denen Sie schnell eine DR-Umgebung einrichten und bereitstellen können. AWS Stellen Sie sicher, dass Sie all Ihre Workload-Abhängigkeiten berücksichtigen, und testen Sie Ihren DR-Plan und Ihre DR-Lösung gründlich und regelmäßig, um ihre Integrität zu überprüfen.

AWS ermöglicht [AWS Elastic Disaster Recovery](#) die Erstellung eines vollständigen Replikats Ihrer lokalen Server, einschließlich des Root-Volumens und des Betriebssystems, auf. AWS Elastic Disaster Recovery repliziert Ihre Maschinen kontinuierlich in einen kostengünstigen Staging-Bereich in Ihrem AWS-Zielkonto und Ihrem bevorzugten AWS-Konto. AWS-Region Die Replikation auf Blockebene ist eine exakte Kopie des Speichers Ihrer Server, einschließlich des Betriebssystems, der Systemstatuskonfiguration, der Datenbanken, Anwendungen und Dateien. Im Notfall können Sie Elastic Disaster Recovery anweisen, innerhalb weniger Minuten Tausende Ihrer Maschinen in ihrem vollständig bereitgestellten Zustand zu starten.

Elastic Disaster Recovery verwendet einen Agenten, der auf jedem Ihrer lokalen Server installiert ist. Die Agenten synchronisieren den Status Ihrer lokalen Server mit Amazon EC2 EC2-Äquivalenten mit geringerer Leistung, die auf laufen. AWS Mit Elastic Disaster Recovery können Sie auch Ihren DR-Failover- und Failback-Prozess automatisieren. Durch die Automatisierung Ihres Failover- und

Failback-Prozesses können Sie ein niedrigeres und einheitlicheres Recovery Time Objective (RTO) erreichen.



1. Statusberichte für den Replikationsserver
2. Ressourcen im Staging-Bereich werden automatisch erstellt und beendet
3. Wiederherstellungsinstanzen, die mit einem RTO von Minuten und einem RPO von Sekunden gestartet wurden
4. Kontinuierliche Replikation auf Blockebene (komprimiert und verschlüsselt)

Es ist wichtig, den DR-Prozess zu testen und sicherzustellen, dass die Live-Staging-Umgebung keine Konflikte mit der lokalen Umgebung verursacht. Stellen Sie beispielsweise sicher, dass die entsprechenden Lizenzen in Ihrer lokalen, Staging- und initiierten DR-Umgebung verfügbar sind und funktionieren. Stellen Sie außerdem sicher, dass alle Prozesse vom Typ Worker, die möglicherweise Arbeit aus einer zentralen Datenbank abrufen und abrufen, entsprechend konfiguriert sind, um Überschneidungen oder Konflikte zu vermeiden. Nehmen Sie in Ihren DR-Prozess alle erforderlichen Schritte auf, die ausgeführt werden müssen, bevor Ihre Wiederherstellungsserver-Instanzen online gehen. Schließen Sie auch die Schritte ein, die ausgeführt werden müssen, nachdem die

Wiederherstellungsserverinstanzen online und verfügbar sind. Sie können Lösungen wie die [AWS Elastic Disaster Recovery Plan Automation-Lösung](#) oder einen anderen Ansatz verwenden, um Ihre DR-Pläne zu automatisieren.

Sie können ein [Storage Gateway Volume Gateway](#) verwenden, um Ihre lokalen Server mit Cloud-basierten Volumes auszustatten. Diese Volumes können mithilfe von Amazon EBS-Snapshots auch schnell für die Verwendung mit Amazon EC2 bereitgestellt werden. Insbesondere Gateways für gespeicherte Volumes bieten Ihren lokalen Anwendungen Zugriff auf ihre gesamten Datensätze mit geringer Latenz. Die Volume-Gateways bieten auch dauerhafte Snapshot-basierte Backups, die für den Einsatz vor Ort oder für die Verwendung mit Amazon EC2 wiederhergestellt werden können. Sie können point-in-time Snapshots auf der Grundlage des Recovery Point Objective (RPO) für Ihren Workload planen.

 **Important**

Volume Gateway-Volumes sind für die Verwendung als Datenvolumes und nicht als Boot-Volumes vorgesehen.

Sie können ein Amazon EC2 Amazon Machine Image (AMI) mit einer Konfiguration verwenden, die Ihren lokalen Servern entspricht und Ihre Datenvolumen separat spezifiziert. Nachdem Sie das AMI konfiguriert und getestet haben, stellen Sie die EC2-Instances zusammen mit den Datenvolumes, die auf den Volume-Gateway-Snapshots basieren, über das AMI bereit. Bei diesem Ansatz müssen Sie Ihre Umgebung gründlich testen, um sicherzustellen, dass Ihre EC2-Instance ordnungsgemäß funktioniert, insbesondere bei Windows-Workloads.

DR für cloudnative Workloads

Überlegen Sie, wie Ihre cloudnativen Workloads Ihren DR-Zielen entsprechen. AWS bietet mehrere Availability Zones in Regionen auf der ganzen Welt. Viele Unternehmen, die die AWS Cloud nutzen, richten ihre Workload-Architekturen und DR-Ziele so aus, dass sie dem Verlust einer Availability Zone standhalten. Die [Zuverlässigkeitssäule](#) im AWS Well-Architected Framework unterstützt diese bewährte Methode. Sie können Ihre Workloads und deren Service- und Anwendungsabhängigkeiten so gestalten, dass mehrere Availability Zones verwendet werden. Anschließend können Sie Ihre DR automatisieren und Ihre DR-Ziele mit minimalem bis gar keinem Eingriff erreichen.

In der Praxis stellen Sie jedoch möglicherweise fest, dass Sie nicht in der Lage sind, eine redundante, aktive und automatisierte Architektur für alle Ihre Komponenten einzurichten. Untersuchen Sie

jede Ebene Ihrer Architektur, um die notwendigen DR-Prozesse zu ermitteln, um Ihre Ziele zu erreichen. Dies kann von Workload zu Workload variieren und unterschiedliche Architektur- und Serviceanforderungen haben. Dieses Handbuch behandelt Überlegungen und Optionen für Amazon EC2. Informationen zu anderen AWS Services finden Sie in der [AWS Dokumentation](#), um die Hochverfügbarkeits- und DR-Optionen zu ermitteln.

DR für Amazon EC2 in einer einzigen Availability Zone

Versuchen Sie, Ihre Workloads so zu gestalten, dass sie Kunden aus mehreren Availability Zones aktiv unterstützen und betreuen. Sie können Amazon EC2 Auto Scaling und Elastic Load Balancing verwenden, um eine Multi-AZ-Serverarchitektur für Amazon EC2 und andere Services zu erreichen.

Wenn Ihre Architektur über EC2-Instances verfügt, für die kein Lastenausgleich möglich ist und für die jeweils nur eine einzige Instance ausgeführt werden kann, können Sie eine der folgenden Optionen verwenden.

- Erstellen Sie eine Auto Scaling Scaling-Gruppe mit einer Mindest-, Höchst- und Wunschgröße von 1, die für mehrere Availability Zones konfiguriert ist. Erstellen Sie ein AMI, das verwendet werden kann, um die Instance zu ersetzen, falls sie ausfällt. Stellen Sie sicher, dass Sie die richtige Automatisierung und Konfiguration definieren, damit eine neu bereitgestellte Instanz aus dem AMI automatisch konfiguriert werden kann und den Service bereitstellen kann. Erstellen Sie einen Load Balancer, der auf die Auto Scaling Scaling-Gruppe verweist und für mehrere Availability Zones konfiguriert ist. Erstellen Sie optional einen Amazon Route 53-Alias, der auf den Load Balancer-Endpunkt verweist.
- Erstellen Sie einen Route 53-Datensatz für Ihre aktive Instance und lassen Sie Ihre Kunden über diesen Datensatz eine Verbindung herstellen. Erstellen Sie ein Skript, das ein neues AMI Ihrer aktiven Instance erstellt und das AMI verwendet, um eine neue EC2-Instance im gestoppten Zustand in einer separaten Availability Zone bereitzustellen. Konfigurieren Sie das Skript so, dass es regelmäßig ausgeführt wird und die zuvor gestoppte Instance beendet wird. Wenn ein Availability Zone-Fehler auftritt, starten Sie Ihre Backup-Instance in Ihrer alternativen Availability Zone. Aktualisieren Sie dann den Route 53-Datensatz so, dass er auf diese neue Instanz verweist.

Testen Sie Ihre Lösung gründlich, indem Sie den Fehler simulieren, vor dem die Lösung schützen sollte. Berücksichtigen Sie auch die Aktualisierungen, die Ihre DR-Lösung benötigt, wenn sich Ihre Workload-Architektur ändert.

DR für Amazon EC2 bei einem regionalen Ausfall

Kunden mit sehr hohen Verfügbarkeitsanforderungen (z. B. unternehmenskritische Anwendungen, die keine Ausfallzeiten vertragen) können diese Lösung AWS über mehrere Regionen hinweg verwenden, um die Widerstandsfähigkeit gegen Probleme auf regionaler Ebene zu erhöhen. Kunden müssen die Komplexität, die Kosten und den Aufwand, die erforderlich sind, um einen DR-Plan für mehrere Regionen einzurichten und aufrechtzuerhalten, sorgfältig gegen die Vorteile abwägen. AWS bietet Funktionen, die Architekturen mit mehreren Regionen für globale Verfügbarkeit, Failover und DR unterstützen. Dieses Handbuch behandelt einige der verfügbaren Funktionen, die spezifisch für Backup und Recovery für Amazon EC2 sind.

AWS AMIs und Amazon EBS-Snapshots sind regionale Ressourcen, die zur Bereitstellung neuer Instances innerhalb einer einzelnen Region verwendet werden können. Sie können Ihre Snapshots und AMIs jedoch in eine andere Region kopieren und sie verwenden, um neue Instances in dieser Region bereitzustellen. Um einen regionalen Notfall-DR-Plan zu unterstützen, können Sie den Vorgang des Kopierens von AMIs und Snapshots in andere Regionen automatisieren. AWS Backup und Amazon Data Lifecycle Manager unterstützen regionsübergreifendes Kopieren als Teil Ihrer Backup-Konfiguration.

[AWS Elastic Disaster Recovery](#) kann verwendet werden, um Ihre Amazon EC2-Server in einer Region zu automatisieren und kontinuierlich in eine alternative DR-Region zu replizieren. Elastic Disaster Recovery kann Ihren DR-Ansatz für mehrere Regionen vereinfachen und Ihnen helfen, Ihren regionsübergreifenden Amazon EC2 EC2-DR-Plan regelmäßig mithilfe von Übungen zu testen. Elastic Disaster Recovery kann Ihnen helfen, wenn Backup und Recovery Ihre RTO- und RPO-Ziele nicht erfüllen können. Elastic Disaster Recovery kann Ihnen helfen, Ihre RTO auf Minuten und Ihr RPO auf unter eine Sekunde zu senken.

Unabhängig davon, welche Lösung Sie verwenden, müssen Sie den Bereitstellungs-, Failover- und Failback-Prozess festlegen, der im Falle eines Ausfalls verwendet werden soll. Sie können Route 53 mit Integritätsprüfungen und Domain Name System-Failover verwenden, um Ihre Lösung zu unterstützen.

Backups bereinigen

Um die Kosten zu senken, bereinigen Sie die Backups, die nicht mehr für Wiederherstellungs- oder Aufbewahrungszwecke benötigt werden. Du kannst benutzen [AWS Backup](#) und [Amazon Data Lifecycle Manager](#), um Ihre Aufbewahrungsrichtlinien für einen Teil Ihrer Backups zu automatisieren. Selbst mit diesen Tools benötigen Sie jedoch immer noch einen Bereinigungsansatz für Backups, die separat erstellt werden.

Eine Tagging-Strategie ist eine Voraussetzung für eine Cleanup-Strategie. Verwenden Sie Tagging, um Ressourcen zu identifizieren, die gereinigt werden sollten, die Eigentümer entsprechend zu benachrichtigen und Ihren Reinigungsprozess zu automatisieren. Backups erstellt von [AWS](#) die Erstellungstermine darauf abstimmen, aber das Tagging ist wichtig, um Backups mit Ihren Workloads, Aufbewahrungsanforderungen und der Identifizierung von Wiederherstellungspunkten zu korrelieren.

Mithilfe von Automatisierung können Sie einen Bereinigungsprozess für Snapshots implementieren. Sie können Ihr Konto beispielsweise nach Snapshots durchsuchen und feststellen, ob sich die entsprechenden Volumes im Status „Angehängt“ oder im Status „Verfügbar“ befinden. Sie können die Ergebnisse weiter nach einem von Ihnen angegebenen Zeitschwellenwert filtern. Mithilfe der an das Volume angehängten Tags können Sie automatisch E-Mails an Snapshot-Besitzer senden und sie darüber informieren, dass ihre Snapshots gelöscht werden sollen. Diese automatische Problembehebung kann implementiert werden, indem [AWS Config](#) rules, ein Skript, das die [AWS CLI](#), oder eine [Lambda-Funktion](#) mit dem [AWS SDK](#).

[Systems Manager](#) bietet die [AWS — EBS löschen Volume Snapshots](#) und [ALS-Delete Snapshot](#) Dokumente, die Ihnen helfen, die Bereinigung von Amazon EBS-Snapshots zu initiieren und zu automatisieren. Sie können auch das verwenden [AWS CLI](#) und [AWS SDK](#) zur Automatisierung der Bereinigung anderer [AWS Ressourcen](#) wie Amazon RDS-Snapshots.

Häufig gestellte Fragen zu Backup und Recovery

Welchen Backup-Zeitplan sollte ich wählen?

Definieren Sie eine Häufigkeit von Backups, die Ihrem Recovery Point Objective (RPO) entspricht. Definieren Sie eine Backup-Zeit, zu der Ihr Workload am wenigsten ausgelastet ist und die Auswirkungen auf die Benutzer reduziert werden können. Erstellen Sie einen Snapshot, wann immer Sie eine wesentliche Änderung an Ihrem Workload vornehmen.

Muss ich Backups in meinen Entwicklungskonten erstellen?

Testen Sie potenziell wichtige Änderungen in Ihren Entwicklungskonten für Ihre Workloads und erstellen Sie Backups, bevor Sie wichtige Änderungen vornehmen. Vielleicht hast du noch viel mehr point-in-time Wiederherstellungs-Backups (PITR) in Ihren Entwicklungs- und Nicht-Produktionskonten aus Entwicklungs- und Testaktivitäten

Kann ich Anwendungen aktualisieren und ein EBS-Volume weiterhin verwenden, während ein Snapshot erstellt wird, ohne dass dies Auswirkungen hat?

Schnappschüsse erfolgen asynchron; Der Snapshot wird sofort erstellt, aber der Status des Snapshots ist ausstehend, bis alle geänderten Blöcke an Amazon S3 übertragen wurden. Bei großen ersten Schnappschüssen oder nachfolgenden Schnappschüssen, bei denen sich viele Blöcke geändert haben, kann die Übertragung mehrere Stunden dauern. Während der Übertragung wird ein in Bearbeitung befindlicher Snapshot nicht durch laufende Lese- und Schreibvorgänge auf dem Volume beeinträchtigt. Weitere Informationen finden Sie in der [AWS-Dokumentation](#).

Nächste Schritte

Beginne damit, deinen Backup- und Recovery-Ansatz in einer Umgebung außerhalb der Produktionsumgebung zu evaluieren, zu implementieren und zu testen. Es ist wichtig, dass Sie Ihren Wiederherstellungsprozess gründlich testen und überprüfen, ob Ihre wiederhergestellten Workloads wie erwartet funktionieren.

Testen Sie den Wiederherstellungsprozess für eine einzelne Komponente in Ihrer Architektur zusätzlich zu allen Komponenten in Ihrer Architektur. Überprüfen Sie die Wiederherstellungszeit für jeden. Überprüfen Sie außerdem die Auswirkungen Ihres Sicherungs- und Wiederherstellungsprozesses auf Upstream- und Downstream-Abhängigkeiten. Bestätigen Sie die Auswirkungen eines Serviceausfalls auf Ihre Upstream-Abhängigkeiten und die Downstream-Auswirkungen auf Ihre Backups.

Weitere Ressourcen

AWS-Ressourcen

- [AWS Präskriptive Leitlinien](#)
- [AWS-Dokumentation](#)
- [Allgemeine AWS-Referenz](#)
- [AWS-Glossar](#)

AWS-Services

- [AWS Backup](#)
- [Amazon CloudWatch](#)
- [CloudWatch Amazon-Veranstaltungen](#)
- [AWS Config](#)
- [Amazon-DynamoDB](#)
- [Amazon EBS](#)
- [Amazon EC2](#)
- [IAM](#)
- [Amazon RDS](#)
- [Amazon S3](#)
- [Storage Gateway](#)
- [AWS Systems Manager](#)

Sonstige Ressourcen

- [Backup und Recovery mit AWS Backup](#) (Lösung)
- [Disaster Recovery von Workloads auf AWS: Wiederherstellung in der Cloud](#) (Whitepaper)
- [Disaster Recovery-Serie](#) (Blogbeiträge zur AWS-Architektur)
- [Checkliste für den DR-Plan](#)
- Einsatz von [Sicherungs- und Wiederherstellungsansätzen AWS](#) (technischer paper — archiviert)
- [Erste Schritte mit AWS Backup](#)

- [AWS Marketplace — Backup und Wiederherstellung](#)

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
Aktualisierte Informationen	Die Anleitung im Bereich Amazon S3 wurde aktualisiert.	28. Juni 2024
Aktualisierte Informationen	Die Informationen im AWS Abschnitt On-Premise DR to wurden aktualisiert.	13. April 2023
Ein Abschnitt wurde hinzugefügt	Es wurden Anleitungen und Schritte zum Erstellen oder Wiederherstellen einer Instanz aus einem Snapshot hinzugefügt.	7. März 2023
Es wurden Informationen zu Elastic Disaster Recovery hinzugefügt und weitere Erläuterungen hinzugefügt	In den Abschnitten Disaster Recovery with AWS und AWS Choosing Services for Data Protection wurden Informationen über hinzugefügt AWS Elastic Disaster Recovery. In den Abschnitten Amazon EC2 EC2-Sicherung und Wiederherstellung mit Snapshots und AMIs , Vorbereiten eines EBS-Volumes vor der Erstellung eines Snapshots oder AMIs und Wiederherstellen aus einem Amazon EBS-Snapshot oder einem AMI wurden weitere Erläuteru	19. Januar 2023

ngen hinzugefügt. Zu den [häufig gestellten Fragen zu Backup und Wiederherstellung](#) hinzugefügt.

[Ein Link wurde hinzugefügt](#)

Im Abschnitt Amazon Data Lifecycle Manager wurde ein Link zur [Amazon Data Lifecycle Manager Manager-Dokumentation](#) hinzugefügt.

31. Oktober 2022

[Aktualisierte Informationen](#)

Die Informationen zur [Wiederherstellung von Volumes](#) wurden aktualisiert.

30. August 2022

Die Informationen wurden aktualisiert und ein neuer Abschnitt hinzugefügt

Im Abschnitt [Auswahl von AWS Diensten für den Datenschutz](#) wurden Dienste hinzugefügt. Der Abschnitt [Sicherung und Wiederherstellung mit AWS Backup](#) wurde hinzugefügt. Im Abschnitt [Backup und Wiederherstellung mit Amazon S3 und Amazon S3 Glacier](#) wurden Informationen zu neuen Amazon S3 Glacier-Speicherklassen hinzugefügt. Im Abschnitt [Backup und Wiederherstellung für Amazon EC2 mit EBS-Volumes](#) wurden Links zur Dokumentation und zusätzliche Informationen hinzugefügt. Im Abschnitt [Backup und Wiederherstellung von Cloud-nativen AWS Diensten](#) wurde eine Empfehlung zur Verwendung AWS Backup hinzugefügt. Im Abschnitt [Zusätzliche Ressourcen](#) wurden Ressourcen hinzugefügt.

28. Januar 2022

Aktualisierte Informationen

Dem Abschnitt [S3 Glacier Flexible Retrieval](#) wurden Informationen zum Einstellen von Speicherklassen hinzugefügt. Informationen zum Abrufen von Snapshots wurden dem Abschnitt [Amazon EC2 Backup and Recovery with Snapshots and AMIs](#) hinzugefügt.

9. September 2021

Aktualisierte Informationen

In [AWS Backup](#) diesem Abschnitt wurden Informationen zu den AWS Backup unterstützten AWS Diensten hinzugefügt.

1. Juni 2021

Erste Veröffentlichung

—

29. Juli 2020

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-Repositories 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.

IloT

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 klargelegt 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-Indikators](#).

Modell der geteilten Verantwortung

Ein Modell, das die Verantwortung beschreibt, mit der Sie gemeinsam AWS für Cloud-Sicherheit und Compliance verantwortlich sind. AWS ist für die Sicherheit der Cloud verantwortlich, 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.