Bewährte Methoden für den Aufbau einer Hybrid-Cloud-Architektur mit AWS-Services

AWS Präskriptive Leitlinien

AWS Präskriptive Leitlinien: Bewährte Methoden für den Aufbau einer Hybrid-Cloud-Architektur mit AWS-Services

Table of Contents

Bewährte Methoden für den Aufbau einer Hybrid-Cloud-Architektur mit AWS-Services

Amazon Web Services (Mitwirkende)

Juni 2025 (Verlauf der Dokumente)

Viele Unternehmen und Organisationen haben Cloud Computing als zentralen Aspekt ihrer Technologiestrategie eingeführt. In der Regel migrieren sie ihre Workloads auf die, AWS Cloud um Agilität, Kosteneinsparungen, Leistung, Verfügbarkeit, Belastbarkeit und Skalierbarkeit zu erhöhen. Die meisten Anwendungen können problemlos migriert werden, aber einige Anwendungen müssen lokal bleiben, um die Vorteile der niedrigen Latenz und der lokalen Datenverarbeitung der lokalen Umgebung zu nutzen, hohe Datenübertragungskosten zu vermeiden oder um die Einhaltung gesetzlicher Vorschriften zu gewährleisten. Darüber hinaus muss ein Teil der Anwendungen möglicherweise neu konzipiert oder modernisiert werden, bevor sie in die Cloud verlagert werden können. Dies veranlasst viele Unternehmen, nach Hybrid-Cloud-Architekturen zu suchen, um ihren lokalen Betrieb und ihren Cloud-Betrieb zu integrieren und so ein breites Spektrum von Anwendungsfällen zu unterstützen. Dieser hybride Ansatz kann die Vorteile von lokalem und cloudbasiertem Computing bieten und kann besonders für Edge-Computing-Szenarien nützlich sein.

Wenn Sie eine Hybrid Cloud mit erstellen AWS, empfehlen wir Ihnen, Ihre Hybrid-Cloud-Strategie und Ihre technische Strategie festzulegen:

- Eine Hybrid-Cloud-Strategie enthält Richtlinien, die den Verbrauch von Cloud- und lokalen Ressourcen regeln, um Ihre Geschäftsziele zu erreichen. In diesem Leitfaden werden gängige Anwendungsfälle für den Aufbau einer Hybrid Cloud beschrieben, z. B. die Unterstützung der laufenden Migration zur Cloud, die Sicherstellung der Geschäftskontinuität bei Katastrophen, die Ausweitung der Cloud-Infrastruktur auf die lokale Umgebung zur Unterstützung von Anwendungen mit niedriger Latenz oder die Erweiterung Ihrer internationalen Präsenz auf. AWS Die Definition dieser Strategie hilft Ihnen dabei, Ihre Geschäftsziele für den Aufbau einer Hybrid Cloud zu identifizieren und zu definieren, und enthält Richtlinien für die Platzierung von Workloads in der Hybrid Cloud.
- Eine technische Strategie für die Hybrid Cloud identifiziert die Leitprinzipien der Hybrid-Cloud-Architektur und definiert einen Implementierungsrahmen. In diesem Leitfaden werden allgemeine Anforderungen für eine konsistent bereitgestellte und verwaltete Hybrid-Cloud-Architektur dargelegt, um Ihnen bei der Definition von Prinzipien für eine geplante Hybrid-Cloud-

Implementierung zu helfen. Zu diesen Anforderungen gehören standardisierte Schnittstellen für die Bereitstellung und Verwaltung von Ressourcen in Ihrer gesamten Cloud-Infrastruktur.

In diesem Leitfaden wird ein Betriebs- und Management-Framework beschrieben, das Lösungsarchitekten und -betreibern dabei helfen soll, die Bausteine, bewährten Methoden sowie AWS Hybrid Cloud- und regionsinterne Dienste für die Implementierung einer Hybrid Cloud zu identifizieren. AWS

Viele Unternehmen haben die in diesem Leitfaden beschriebenen Lösungen verwendet, um erfolgreich Hybrid-Cloud-Umgebungen bereitzustellen, die die Skalierbarkeit, Agilität, Innovation und globale Präsenz von nutzen. AWS Cloud(Siehe Fallstudien.) AWS Hybrid-Cloud-Dienste bieten ein konsistentes AWS Erlebnis — von der Cloud bis hin zu lokalen Umgebungen und am Netzwerkrand. Dienste wie Compute AWS Outposts -, Speicher-, Datenbank- und andere ausgewählte Dienste AWS-Services in der Nähe von Ballungs- und Industriezentren AWS Lokale Zonen platzieren, wenn Sie eine geringe Latenz zwischen Endbenutzergeräten oder bestehenden lokalen Rechenzentren und Workload-Servern benötigen.

In diesem Leitfaden:

Übersicht

Dieser Leitfaden unterteilt die AWS Empfehlungen für die Hybrid Cloud in fünf Säulen: Netzwerk, Sicherheit, Ausfallsicherheit, Kapazitätsplanung und Infrastrukturmanagement. Es enthält Richtlinien, die Ihnen helfen sollen, Ihre Voraussetzungen zu verbessern und eine Migrationsstrategie zu entwickeln, indem Sie einen AWS Hybrid-Edge-Service wie AWS Outposts oder verwenden. AWS Lokale Zonen Wir empfehlen Ihnen dringend, mit Ihrem AWS-Konto Team zusammenzuarbeiten oder AWS Partner sicherzustellen, dass ein AWS Hybrid-Cloud-Spezialist zur Verfügung steht, der Sie bei der Befolgung dieses Leitfadens und bei der Entwicklung Ihres Prozesses unterstützt.

> **Note**
>
> Local Zones befasst sich zwar AWS Outposts mit ähnlichen Problemen, wir empfehlen Ihnen jedoch, die Anwendungsfälle sowie die verfügbaren Dienste und Funktionen zu überprüfen, um zu entscheiden, welches Angebot Ihren Anforderungen am besten entspricht. Weitere Informationen finden Sie im AWS Blogbeitrag AWS Lokale Zonen und AWS Outposts unter Auswahl der richtigen Technologie für Ihren Edge-Workload.

Workshops zur Hybrid-Cloud

Mit Unterstützung eines AWS Hybrid-Cloud-Experten (SME) können Sie einen Hybrid-Cloud-Workshop durchführen, um den Reifegrad Ihres Unternehmens in Bezug auf die fünf in diesem Leitfaden erörterten Säulen zu bewerten.

Der Workshop konzentriert sich auf interne Bereiche innerhalb Ihres Unternehmens, wie Netzwerke, Sicherheit, Compliance DevOps, Virtualisierung und Geschäftsbereiche. Er hilft Ihnen dabei, eine Hybrid-Cloud-Architektur zu entwerfen, die den Anforderungen Ihres Unternehmens entspricht, und definiert Implementierungsdetails. Folgen Sie dabei den Schritten im Abschnitt Hybrid-Cloud-Einführungsprozess dieses Leitfadens.

PoCs

Wenn Sie spezielle Anforderungen haben, können Sie Machbarkeitsnachweise (PoCs) verwenden, um die Funktionalität in Local Zones und AWS Outposts anhand dieser Anforderungen zu überprüfen.

AWS wird verwendet PoCs , um Ihnen beim Testen der Workloads zu helfen, die Sie in einen Outpost oder eine Local Zone verschieben möchten, um festzustellen, ob die Workloads unter den Testarchitekturen funktionieren. Um zu Testzwecken auf eine lokale Zone zuzugreifen, folgen Sie den Anweisungen in der Dokumentation zu Local Zones. Um Ihre Arbeitslast zu testen AWS Outposts, arbeiten Sie mit Ihrem AWS-Konto Team zusammen oder greifen Sie auf ein AWS Outposts Testlabor AWS Partner zu und lassen Sie sich von AWS Lösungsarchitekten beraten. In allen Szenarien müssen Sie für die Entwicklung eines PoC ein Testdokument erstellen, das Folgendes enthält:

- AWS-Services zu verwenden, wie Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic Block Store (Amazon EBS), Amazon Virtual Private Cloud (Amazon VPC) und Amazon Elastic Kubernetes Service (Amazon EKS)
- Größe und Anzahl der zu nutzenden Instances (z. B. oder) `m5.xlarge` `c5.2xlarge`
- Diagramm der Testarchitektur
- Erfolgskriterien für den Test
- Einzelheiten und Ziele der einzelnen durchzuführenden Tests

Säulen

Im nächsten Abschnitt werden die Voraussetzungen und Einschränkungen für die Verwendung der in diesem Handbuch erörterten Architekturen behandelt. In den darauffolgenden Abschnitten werden die Einzelheiten der einzelnen Säulen behandelt, sodass das Empfehlungsdokument, das Sie während des Hybrid-Cloud-Workshops erstellen, die für die Implementierung erforderlichen Designdetails widerspiegeln kann.

- Networking am Netzwerkrand
- Sicherheit am Netzwerkrand
- Resilienz an der Peripherie
- Kapazitätsplanung am Netzwerkrand
- Verwaltung der Edge-Infrastruktur

Voraussetzungen und Einschränkungen

Bevor Sie diesem Leitfaden folgen, sollten Sie mit Ihrem AWS-Konto Team zusammenarbeiten oder AWS Partner sich mit den Voraussetzungen und Einschränkungen für die Implementierung von Edge-Architekturen mit AWS Outposts und Local Zones vertraut machen.

Voraussetzungen

AWS Outposts

- Ihr vorhandenes Rechenzentrum muss die AWS Outposts Anforderungen an Ausstattung, Netzwerk und Stromversorgung erfüllen. AWS Outposts ist für den Betrieb in einer Rechenzentrumsumgebung konzipiert, die unter anderem über redundante Stromeingänge mit 5 bis 15 kVA, einen Luftstrom von 145,8 kVA pro Minute (CFM) und eine Umgebungstemperatur zwischen 41 °F (5 °C) und 95 °F (35 °C) verfügt.
- Vergewissern Sie sich anhand des Racks, dass der AWS Outposts Service in Ihrem Land verfügbar ist.AWS Outposts FAQs Siehe die Frage: In welchen Ländern und Gebieten ist das Outposts-Rack verfügbar?
- Wenn Ihr Unternehmen vier oder mehr AWS Outposts Racks benötigt, muss Ihr Rechenzentrum die Rack-Anforderungen für Aggregation, Core, Edge (ACE) erfüllen.
- Für die AWS Direct Connect Verbindung mit dem muss ein Internet oder eine Verbindung AWS Outposts mit mindestens 500 Mbit/s (1 Gbit/s ist besser) bereitgestellt und aufrechterhalten werden. Falls Ihr Anwendungsfall dies erfordert AWS-Region, muss eine entsprechende Backup-Konnektivität vorhanden sein. Die Latenz für die Hin- und Rückfahrt von AWS Outposts zur Region muss maximal 175 Millisekunden betragen.
- Sie müssen über einen aktiven Vertrag für AWS Enterprise Support oder AWS Enterprise On-Ramp verfügen.

AWS Lokale Zonen

- Eine AWS lokale Zone muss in der Nähe Ihrer Rechenzentren oder Benutzer verfügbar sein. AWS Lokale Zonen Standorte anzeigen.
- Vergewissern Sie sich, dass Ihre lokale Infrastruktur über eine Netzwerkverbindung mit der lokalen Zone verbunden ist:

- Option 1: Eine AWS Direct Connect Verbindung von Ihrem Rechenzentrum zum AWS Direct Connect Point of Presence (PoP), der der lokalen Zone am nächsten ist. Weitere Informationen finden Sie unter Direct Connect in der Dokumentation zu Local Zones.
- Option 2: Eine Internetverbindung zusätzlich zu einer lokalen Appliance für ein virtuelles privates Netzwerk (VPN) und die erforderlichen Lizenzen, um eine softwarebasierte VPN-Appliance bei Amazon EC2 in der lokalen Zone zu starten. Weitere Informationen finden Sie unter VPN-Verbindung in der Dokumentation Local Zones.

Weitere Verbindungsoptionen finden Sie in der Dokumentation zu Local Zones.

Einschränkungen

AWS Outposts

- Amazon Relational Database Service (Amazon RDS) in AWS Outposts Multi-AZ-Bereitstellungen erfordert kundeneigene IP-Adresspools (CoIP). Weitere Informationen finden Sie unter Kundeneigene IP-Adressen für Amazon RDS auf AWS Outposts.
- Multi-AZ on AWS Outposts ist für alle unterstützten Versionen von MySQL und PostgreSQL auf Amazon RDS on verfügbar. AWS Outposts Weitere Informationen finden Sie unter Amazon RDS auf AWS Outposts Outposts Unterstützung für Amazon RDS-Funktionen. Amazon RDS on AWS Outposts unterstützt SQL Server, Amazon RDS for MySQL und Amazon RDS for PostgreSQL PostgreSQL-Datenbanken.
- AWS Outposts ist nicht für den Betrieb konzipiert, wenn es von einem getrennt ist. AWS-Region Weitere Informationen finden Sie im Abschnitt Überlegungen zu Fehlermodi im AWS Whitepaper AWS Outposts High Availability Design and Architecture Considerations.
- Amazon Simple Storage Service (Amazon S3) AWS Outposts hat einige Einschränkungen. Diese werden im Artikel Wie unterscheidet sich Amazon S3 on Outposts von Amazon S3? behandelt. Abschnitt des Amazon S3 on Outposts-Benutzerhandbuchs.
- Bei eingeschaltetem Application Load Balancer werden Mutual TLS (mTLS) oder Sticky Sessions AWS Outposts nicht unterstützt.
- Die ACE-Racks sind nicht vollständig geschlossen und verfügen weder über Vorder- noch Hintertüren.
- Das Instanzkapazitätstool ist nur für neue Bestellungen verfügbar.

AWS Lokale Zonen

- Local Zones haben keinen AWS Site-to-Site VPN Endpunkt. Verwenden Sie stattdessen ein softwarebasiertes VPN bei Amazon EC2.
- Local Zones werden nicht unterstützt AWS Transit Gateway. Stellen Sie stattdessen mithilfe einer AWS Direct Connect privaten virtuellen Schnittstelle (VIF) eine Verbindung zur lokalen Zone her.
- Nicht alle Local Zones unterstützen Dienste wie Amazon RDS, Amazon FSx, Amazon EMR oder Amazon ElastiCache oder NAT-Gateways. Weitere Informationen finden Sie unter AWS Lokale Zonen Funktionen.
- Application Load Balancer in Local Zones unterstützen keine mTLs oder Sticky Sessions.

Prozess der Einführung von Hybrid-Clouds

In den folgenden Abschnitten werden Architekturen und Designdetails für die einzelnen Säulen der AWS Hybrid Cloud erörtert:

- Netzwerke am Netzwerkrand
- Sicherheit am Netzwerkrand
- Resilienz am Netzwerkrand
- Kapazitätsplanung am Netzwerkrand
- Verwaltung der Edge-Infrastruktur

Networking am Netzwerkrand

Wenn Sie Lösungen entwerfen, die eine AWS Edge-Infrastruktur wie AWS Outposts Local Zones verwenden, müssen Sie das Netzwerkdesign sorgfältig abwägen. Das Netzwerk bildet die Grundlage für die Konnektivität, um Workloads zu erreichen, die an diesen Edge-Standorten bereitgestellt werden, und ist entscheidend für die Sicherstellung einer niedrigen Latenz. In diesem Abschnitt werden verschiedene Aspekte der Hybrid-Edge-Konnektivität beschrieben.

VPC-Architektur

Eine virtuelle private Cloud (VPC) erstreckt sich über alle Availability Zones in ihrer. AWS-Region Sie können jede VPC in der Region nahtlos auf Outposts oder Local Zones erweitern, indem Sie die AWS Konsole oder die AWS Command Line Interface (AWS CLI) verwenden, um ein Outpost- oder Local Zone-Subnetz hinzuzufügen. Die folgenden Beispiele zeigen, wie Sie Subnetze in AWS Outposts und Local Zones mithilfe von erstellen: AWS CLI

- AWS Outposts: Um einer VPC ein Outpost-Subnetz hinzuzufügen, geben Sie den Amazon-Ressourcennamen (ARN) des Outposts an.

```
aws ec2 create-subnet --vpc-id vpc-081ec835f3EXAMPLE \
--cidr-block 10.0.0.0/24 \
--outpost-arn arn:aws:outposts:us-west-2:11111111111:outpost/op-0e32example1 \
--tag-specifications ResourceType=subnet,Tags=[{Key=Name,Value=my-ipv4-only-subnet}]
```

  Weitere Informationen finden Sie in der AWS Outposts -Dokumentation.

- Local Zones: Um einer VPC ein Subnetz der lokalen Zone hinzuzufügen, gehen Sie genauso vor wie bei Availability Zones, geben Sie jedoch die lokale Zonen-ID an (`<local-zone-name>`im folgenden Beispiel).

```
aws ec2 create-subnet --vpc-id vpc-081ec835f3EXAMPLE \
--cidr-block 10.0.1.0/24 \
--availability-zone <local-zone-name> \
--tag-specifications ResourceType=subnet,Tags=[{Key=Name,Value=my-ipv4-only-subnet}]
```

  Weitere Informationen finden Sie in der Dokumentation zu Local Zones.

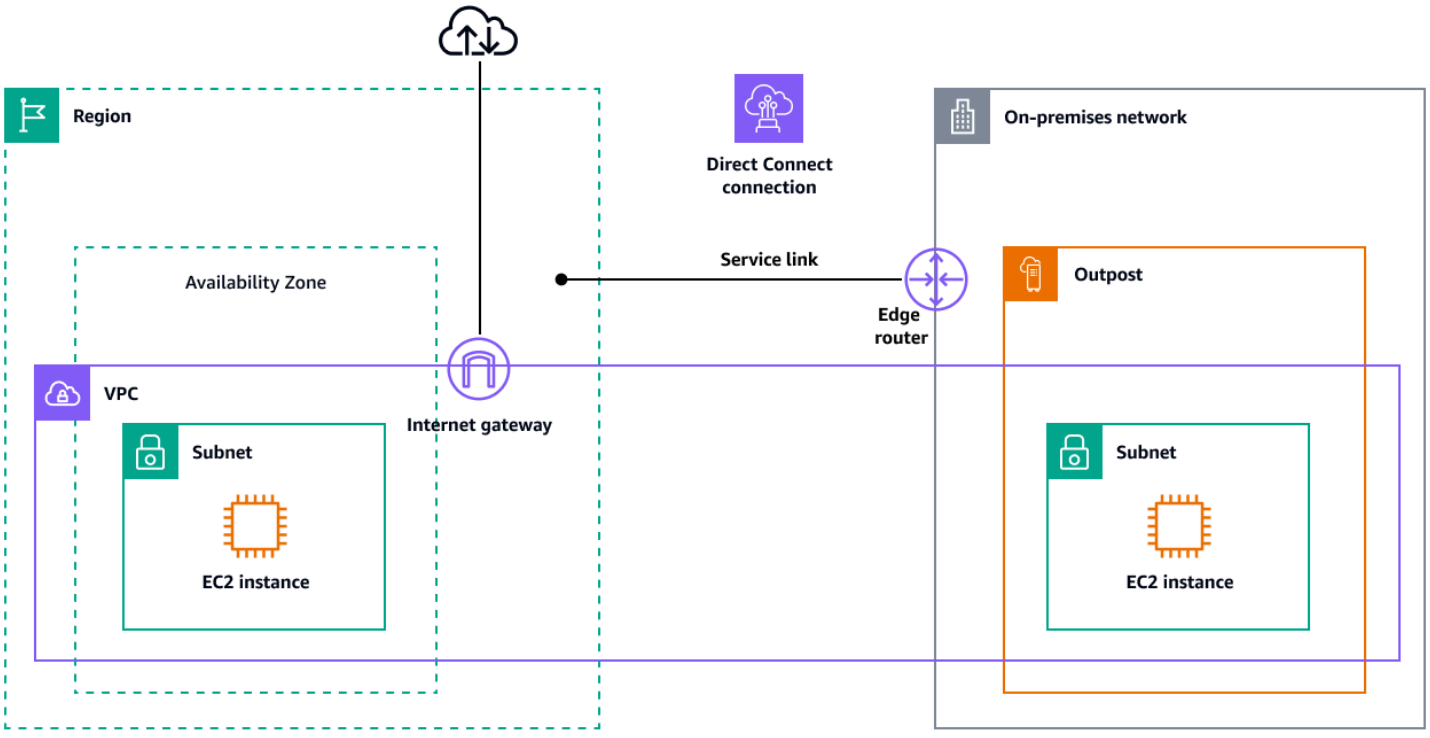
Das folgende Diagramm zeigt eine AWS Architektur, die Outpost- und Local Zone-Subnetze umfasst.

Verkehr von Rand zu Region

Wenn Sie eine Hybridarchitektur mithilfe von Diensten wie Local Zones und entwerfen AWS Outposts, sollten Sie sowohl Kontrollflüsse als auch Datenverkehrsflüsse zwischen den Edge-Infrastrukturen und berücksichtigen AWS-Regionen. Je nach Art der Edge-Infrastruktur können Ihre Zuständigkeiten variieren: Bei einigen Infrastrukturen müssen Sie die Verbindung zur übergeordneten Region verwalten, während andere dies über die AWS globale Infrastruktur abwickeln. In diesem Abschnitt werden die Auswirkungen auf die Konnektivität der Steuerungsebene und der Datenebene für Local Zones und untersucht AWS Outposts.

AWS Outposts Steuerebene

AWS Outposts stellt ein Netzwerkkonstrukt bereit, das als Service Link bezeichnet wird. Der Service Link ist eine erforderliche Verbindung zwischen AWS Outposts und der ausgewählten AWS-Region oder übergeordneten Region (auch als Heimatregion bezeichnet). Es ermöglicht die Verwaltung des Außenpostens und den Datenaustausch zwischen dem Außenposten und. AWS-Region Der Service-Link verwendet einen verschlüsselten Satz von VPN-Verbindungen, um mit der Heimatregion zu kommunizieren. Sie müssen die Konnektivität zwischen AWS Outposts und AWS-Region entweder über eine Internetverbindung oder eine AWS Direct Connect öffentliche virtuelle Schnittstelle (öffentliche VIF) oder über eine AWS Direct Connect private virtuelle Schnittstelle (private VIF) bereitstellen. Für eine optimale Benutzererfahrung und Ausfallsicherheit AWS empfiehlt die Verwendung einer redundanten Konnektivität von mindestens 500 Mbit/s (1 Gbit/s ist besser) für die Service Link-Verbindung zum. AWS-Region Die Service Link-Verbindung mit mindestens 500 Mbit/s ermöglicht es Ihnen, EC2 Amazon-Instances zu starten, Amazon EBS-Volumes anzuhängen und auf Amazon AWS-Services EKS-, Amazon EMR- und CloudWatch Amazon-Metriken zuzugreifen. Das Netzwerk muss eine maximale Übertragungseinheit (MTU) von 1.500 Byte zwischen dem Outpost und den Service Link-Endpunkten im übergeordneten System unterstützen. AWS-RegionWeitere Informationen finden Sie unter AWS Outposts Konnektivität zu AWS-Regionen in der Outposts-Dokumentation.



Informationen zur Erstellung robuster Architekturen für Service-Links, die das öffentliche Internet nutzen, finden Sie im Whitepaper High Availability Design AWS Direct Connect and Architecture Considerations im AWS Whitepaper AWS Outposts High Availability Design and Architecture Considerations.

AWS Outposts Datenebene

Die Datenebene zwischen AWS Outposts und AWS-Region wird von derselben Service Link-Architektur unterstützt, die auch von der Steuerungsebene verwendet wird. Die Bandbreite der Datenebenen-Serviceverbindung zwischen AWS Outposts und AWS-Region sollte mit der Datenmenge korrelieren, die ausgetauscht werden muss: Je größer die Datenabhängigkeit, desto größer sollte die Verbindungsbandbreite sein.

Die Bandbreitenanforderungen hängen von den folgenden Merkmalen ab:

- Die Anzahl der AWS Outposts Racks und die Kapazitätskonfigurationen
- Workload-Merkmale wie AMI-Größe, Anwendungselastizität und Anforderungen an die Burst-Geschwindigkeit
- VPC-Verkehr in die Region

Der Verkehr zwischen EC2 Instances in AWS Outposts und EC2 Instances in der AWS-Region hat eine MTU von 1.300 Byte. Wir empfehlen Ihnen, diese Anforderungen mit einem AWS Hybrid-Cloud-Spezialisten zu besprechen, bevor Sie eine Architektur vorschlagen, die wechselseitige Abhängigkeiten zwischen der Region und aufweist. AWS Outposts

Datenebene für Local Zones

Die Datenebene zwischen den Local Zones und den AWS-Region wird durch die AWS globale Infrastruktur unterstützt. Die Datenebene wird durch eine VPC von der AWS-Region zu einer lokalen Zone erweitert. Local Zones bieten außerdem eine sichere Verbindung mit hoher Bandbreite zum und ermöglichen es Ihnen AWS-Region, über dieselben Tools APIs und Tools eine nahtlose Verbindung zu allen regionalen Diensten herzustellen.

In der folgenden Tabelle sind die Verbindungsoptionen und die zugehörigen MTUs Optionen aufgeführt.

Von	Zu	MTU
Amazon EC2 in der Region	Amazon EC2 in Local Zones	1.300 Byte
AWS Direct Connect	Lokale Zonen	1.468 Byte
Internet-Gateway	Lokale Zonen	1.500 Byte
Amazon EC2 in Local Zones	Amazon EC2 in Local Zones	9.001 Byte

Local Zones nutzen die AWS globale Infrastruktur, um eine Verbindung herzustellen AWS-Regionen. Die Infrastruktur wird vollständig von verwaltet AWS, sodass Sie diese Konnektivität nicht einrichten müssen. Wir empfehlen Ihnen, Ihre Anforderungen und Überlegungen zu Local Zones mit einem AWS Hybrid-Cloud-Spezialisten zu besprechen, bevor Sie eine Architektur entwerfen, die Koabhängigkeiten zwischen der Region und den Local Zones aufweist.

Datenverkehr vom Edge zum lokalen Rechenzentrum

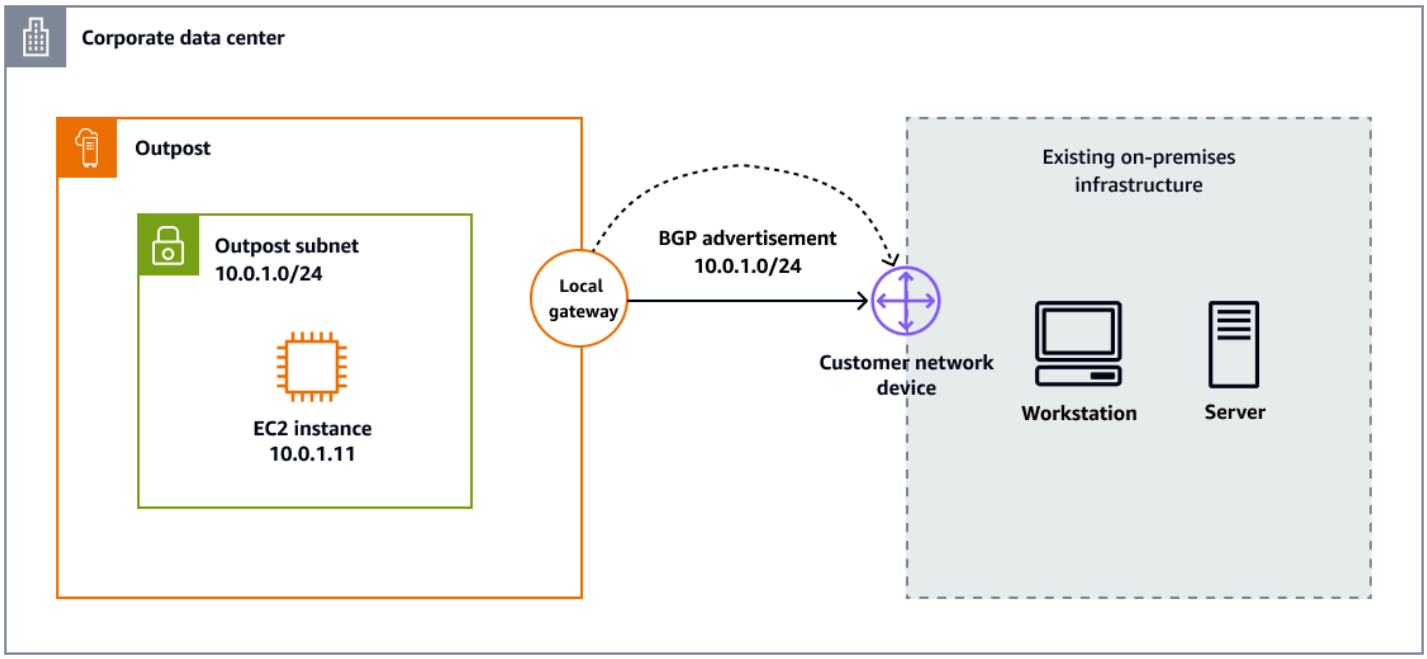
AWS Hybrid-Cloud-Dienste sind für Anwendungsfälle konzipiert, die eine geringe Latenz, lokale Datenverarbeitung oder die Einhaltung der Datenresidenz erfordern. Die Netzwerkarchitektur für den Zugriff auf diese Daten ist wichtig und hängt davon ab, ob Ihr Workload in AWS Outposts oder in Local Zones ausgeführt wird. Lokale Konnektivität erfordert auch einen klar definierten Bereich, wie in den folgenden Abschnitten beschrieben.

AWS Outposts lokales Gateway

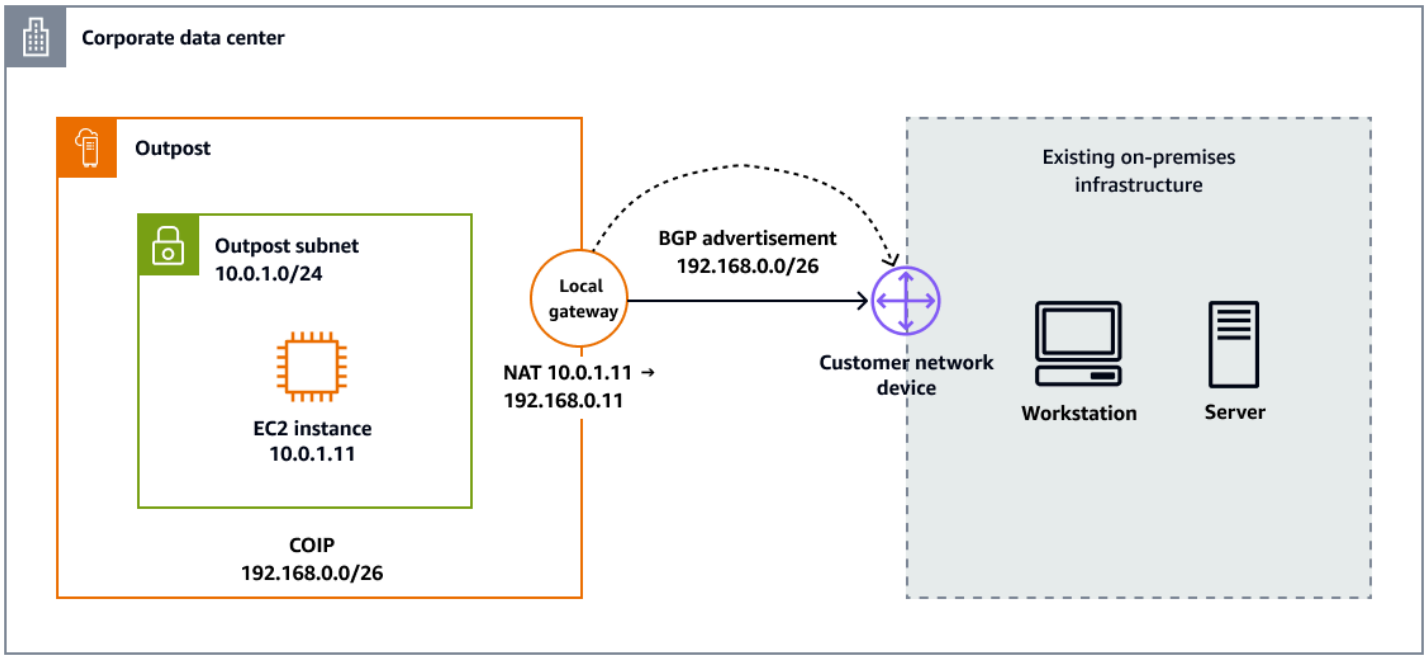
Das lokale Gateway (LGW) ist eine Kernkomponente der AWS Outposts Architektur. Das lokale Gateway ermöglicht die Konnektivität zwischen Ihren Outpost-Subnetzen und Ihrem On-Premises-Netzwerk. Die Hauptaufgabe eines LGW besteht darin, Konnektivität von einem Outpost zu Ihrem lokalen lokalen Netzwerk bereitzustellen. Es bietet auch Konnektivität zum Internet über Ihr lokales Netzwerk entweder über direktes VPC-Routing oder über kundeneigene IP-Adressen.

- Direktes VPC-Routing verwendet die private IP-Adresse der Instances in Ihrer VPC, um die Kommunikation mit Ihrem lokalen Netzwerk zu erleichtern. Diese Adressen werden in Ihrem lokalen Netzwerk mit dem Border Gateway Protocol (BGP) bekannt gegeben. Werbung bei BGP gilt nur für die privaten IP-Adressen, die zu den Subnetzen in Ihrem Outpost-Rack gehören. Diese Art von Routing ist der Standardmodus für. AWS Outposts In diesem Modus führt das lokale Gateway kein NAT für Instances durch, und Sie müssen Ihren EC2 Instances keine Elastic IP-Adressen

zuweisen. Das folgende Diagramm zeigt ein AWS Outposts lokales Gateway, das direktes VPC-Routing verwendet.



- Mit kundeneigenen IP-Adressen können Sie einen Adressbereich bereitstellen, der als kundeneigener IP-Adresspool (CoIP) bezeichnet wird und überlappende CIDR-Bereiche und andere Netzwerktopologien unterstützt. Wenn Sie sich für eine CoIP entscheiden, müssen Sie einen Adresspool erstellen, ihn der lokalen Gateway-Routentabelle zuweisen und diese Adressen Ihrem Netzwerk über BGP mitteilen. CoIP-Adressen bieten lokale oder externe Konnektivität zu Ressourcen in Ihrem lokalen Netzwerk. Sie können diese IP-Adressen Ressourcen in Ihrem Outpost, z. B. EC2 Instances, zuweisen, indem Sie eine neue Elastic IP-Adresse aus der CoIP zuweisen und diese dann Ihrer Ressource zuweisen. Das folgende Diagramm zeigt ein AWS Outposts lokales Gateway, das den CoIP-Modus verwendet.



Für die lokale Konnektivität von AWS Outposts zu einem lokalen Netzwerk sind einige Parameterkonfigurationen erforderlich, z. B. die Aktivierung des BGP-Routingprotokolls und die Bereitstellung von Präfixen zwischen den BGP-Peers. Die MTU, die zwischen Ihrem Outpost und dem lokalen Gateway unterstützt werden kann, beträgt 1.500 Byte. Weitere Informationen erhalten Sie von einem AWS Hybrid-Cloud-Spezialisten oder lesen Sie die AWS Outposts Dokumentation.

Local Zones und das Internet

Branchen, die eine geringe Latenz oder eine lokale Datenspeicherung benötigen (Beispiele hierfür sind Spiele, Live-Streaming, Finanzdienstleistungen und Behörden), können Local Zones verwenden, um ihre Anwendungen für Endbenutzer über das Internet bereitzustellen und bereitzustellen. Bei der Bereitstellung einer lokalen Zone müssen Sie öffentliche IP-Adressen für die Verwendung in einer lokalen Zone zuweisen. Wenn Sie Elastic IP-Adressen zuweisen, können Sie den Standort angeben, von dem aus die IP-Adresse angekündigt wird. Dieser Standort wird als Netzwerkgrenzgruppe bezeichnet. Eine Netzwerkgrenzgruppe ist eine Sammlung von Availability Zones, Local Zones oder AWS Wavelength Zonen, von denen aus AWS eine öffentliche IP-Adresse angekündigt wird. Dies trägt dazu bei, eine minimale Latenz oder physische Entfernung zwischen dem AWS Netzwerk und den Benutzern sicherzustellen, die auf die Ressourcen in diesen Zonen zugreifen. Eine Übersicht aller Netzwerkgrenzgruppen für Local Zones finden Sie unter Verfügbare Local Zones in der Dokumentation Local Zones.

Um einen von Amazon EC2 gehosteten Workload in einer lokalen Zone dem Internet zugänglich zu machen, können Sie beim Starten der Instance die EC2 Option Öffentliche IP automatisch zuweisen aktivieren. Wenn Sie einen Application Load Balancer verwenden, können Sie ihn als mit dem Internet verbunden definieren, sodass öffentliche IP-Adressen, die der lokalen Zone zugewiesen sind, von dem Grenznetzwerk weitergegeben werden können, das der lokalen Zone zugeordnet ist. Wenn Sie Elastic IP-Adressen verwenden, können Sie außerdem eine dieser Ressourcen einer EC2 Instance nach deren Start zuordnen. Wenn Sie Datenverkehr über ein Internet-Gateway in Local Zones senden, werden dieselben Bandbreitenspezifikationen für die Instanz angewendet, die von der Region verwendet werden. Der Netzwerkverkehr der lokalen Zone wird direkt ins Internet oder zu Points of Presence (PoPs) geleitet, ohne die übergeordnete Region der lokalen Zone zu durchqueren, um den Zugriff auf Datenverarbeitung mit niedriger Latenz zu ermöglichen.

Local Zones bieten die folgenden Verbindungsoptionen über das Internet:

- Öffentlicher Zugriff: Verbindet Workloads oder virtuelle Appliances mithilfe von Elastic IP-Adressen über ein Internet-Gateway mit dem Internet.
- Ausgehender Internetzugang: Ermöglicht es Ressourcen, öffentliche Endpunkte über NAT-Instances (Network Address Translation) oder virtuelle Appliances mit zugehörigen Elastic IP-Adressen zu erreichen, ohne dass eine direkte Internetverbindung besteht.
- VPN-Konnektivität: Stellt private Verbindungen mithilfe von Internet Protocol Security (IPsec) VPN über virtuelle Appliances mit zugehörigen Elastic IP-Adressen her.

Weitere Informationen finden Sie unter Konnektivitätsoptionen für Local Zones in der Dokumentation zu Local Zones.

Local Zones und AWS Direct Connect

Local Zones werden ebenfalls unterstützt AWS Direct Connect, sodass Sie Ihren Datenverkehr über eine private Netzwerkverbindung weiterleiten können. Weitere Informationen finden Sie unter Direct Connect in Local Zones in der Dokumentation Local Zones.

Local Zones und Transit-Gateways

AWS Transit Gateway unterstützt keine direkten VPC-Anhänge zu Subnetzen der lokalen Zone. Sie können jedoch eine Verbindung zu Workloads der lokalen Zone herstellen, indem Sie Transit Gateway Gateway-Anlagen in den übergeordneten Availability Zone-Subnetzen derselben VPC erstellen. Diese Konfiguration ermöglicht die Interkonnektivität zwischen mehreren Workloads VPCs

und Ihren lokalen Zonen-Workloads. Weitere Informationen finden Sie unter Transit-Gateway-Verbindung zwischen Local Zones in der Dokumentation zu Local Zones.

Local Zones und VPC-Peering

Sie können jede VPC von einer übergeordneten Region in eine lokale Zone erweitern, indem Sie ein neues Subnetz erstellen und es der lokalen Zone zuweisen. VPC-Peering kann zwischen VPCs diesen eingerichtet werden, die auf Local Zones ausgedehnt werden. Wenn sich die VPCs Peering-Benutzer in derselben lokalen Zone befinden, bleibt der Verkehr innerhalb der lokalen Zone und fließt nicht spiralförmig durch die übergeordnete Region.

Sicherheit am Netzwerkrand

In AWS Cloud der hat Sicherheit oberste Priorität. Wenn Unternehmen sich die Skalierbarkeit und Flexibilität der Cloud zunutze machen, AWS hilft sie ihnen, Sicherheit, Identität und Compliance als wichtige Geschäftsfaktoren zu etablieren. AWS integriert Sicherheit in seine Kerninfrastruktur und bietet Services, mit denen Sie Ihre individuellen Cloud-Sicherheitsanforderungen erfüllen können. Wenn Sie den Umfang Ihrer Architektur auf die erweitern AWS Cloud, profitieren Sie von der Integration von Infrastrukturen wie Local Zones und Outposts in AWS-Regionen. Diese Integration ermöglicht es AWS , eine ausgewählte Gruppe von zentralen Sicherheitsdiensten auf den Netzwerkrand auszudehnen.

Sicherheit ist eine gemeinsame Verantwortung zwischen Ihnen AWS und Ihnen. Das Modell der AWS gemeinsamen Verantwortung unterscheidet zwischen der Sicherheit der Cloud und der Sicherheit in der Cloud:

- Sicherheit der Cloud — AWS ist verantwortlich für den Schutz der Infrastruktur, die AWS-Services in der AWS Cloud läuft. AWS bietet Ihnen auch Dienste, die Sie sicher nutzen können. Externe Prüfer testen und verifizieren regelmäßig die Wirksamkeit der AWS Sicherheit im Rahmen von AWS Compliance-Programmen.
- Sicherheit in der Cloud — Ihre Verantwortung richtet sich nach dem AWS-Service , was Sie verwenden. Sie sind auch für andere Faktoren verantwortlich, etwa für die Vertraulichkeit Ihrer Daten, die Anforderungen Ihres Unternehmens und die geltenden Gesetze und Vorschriften.

Datenschutz

Das Modell der AWS gemeinsamen Verantwortung gilt für den Datenschutz in AWS Outposts und AWS Lokale Zonen. AWS Ist, wie in diesem Modell beschrieben, für den Schutz der globalen Infrastruktur verantwortlich, auf der die AWS Cloud (Sicherheit der Cloud) ausgeführt wird. Sie sind dafür verantwortlich, die Kontrolle über Ihre Inhalte zu behalten, die auf dieser Infrastruktur gehostet werden (Sicherheit in der Cloud). Dieser Inhalt umfasst die Sicherheitskonfiguration und die Verwaltungsaufgaben für die AWS-Services , die Sie verwenden.

Aus Datenschutzgründen empfehlen wir, dass Sie AWS-Konto Anmeldeinformationen schützen und einzelne Benutzer mit AWS Identity and Access Management (IAM) oder AWS IAM Identity Centereinrichten. Dadurch erhält jeder Benutzer nur die Berechtigungen, die er zur Erfüllung seiner Aufgaben benötigt.

Verschlüsselung im Ruhezustand

Verschlüsselung in EBS-Volumes

Mit AWS Outposts werden alle Daten im Ruhezustand verschlüsselt. Das Schlüsselmaterial ist mit einem externen Schlüssel, dem Nitro Security Key (NSK), umwickelt, der auf einem austauschbaren Gerät gespeichert ist. Der NSK ist erforderlich, um die Daten auf Ihrem Outpost-Rack zu entschlüsseln. Sie können die Amazon EBS-Verschlüsselung für Ihre EBS-Volumes und -Snapshots verwenden. Die Amazon EBS-Verschlüsselung verwendet AWS Key Management Service (AWS KMS) und KMS-Schlüssel.

Im Fall von Local Zones werden alle EBS-Volumes standardmäßig in allen Local Zones verschlüsselt, mit Ausnahme der in den AWS Lokale Zonen häufig gestellten Fragen dokumentierten Liste (siehe die Frage: Was ist das Standardverschlüsselungsverhalten von EBS-Volumes in Local Zones?), sofern die Verschlüsselung für das Konto nicht aktiviert ist.

Verschlüsselung in Amazon S3 auf Outposts

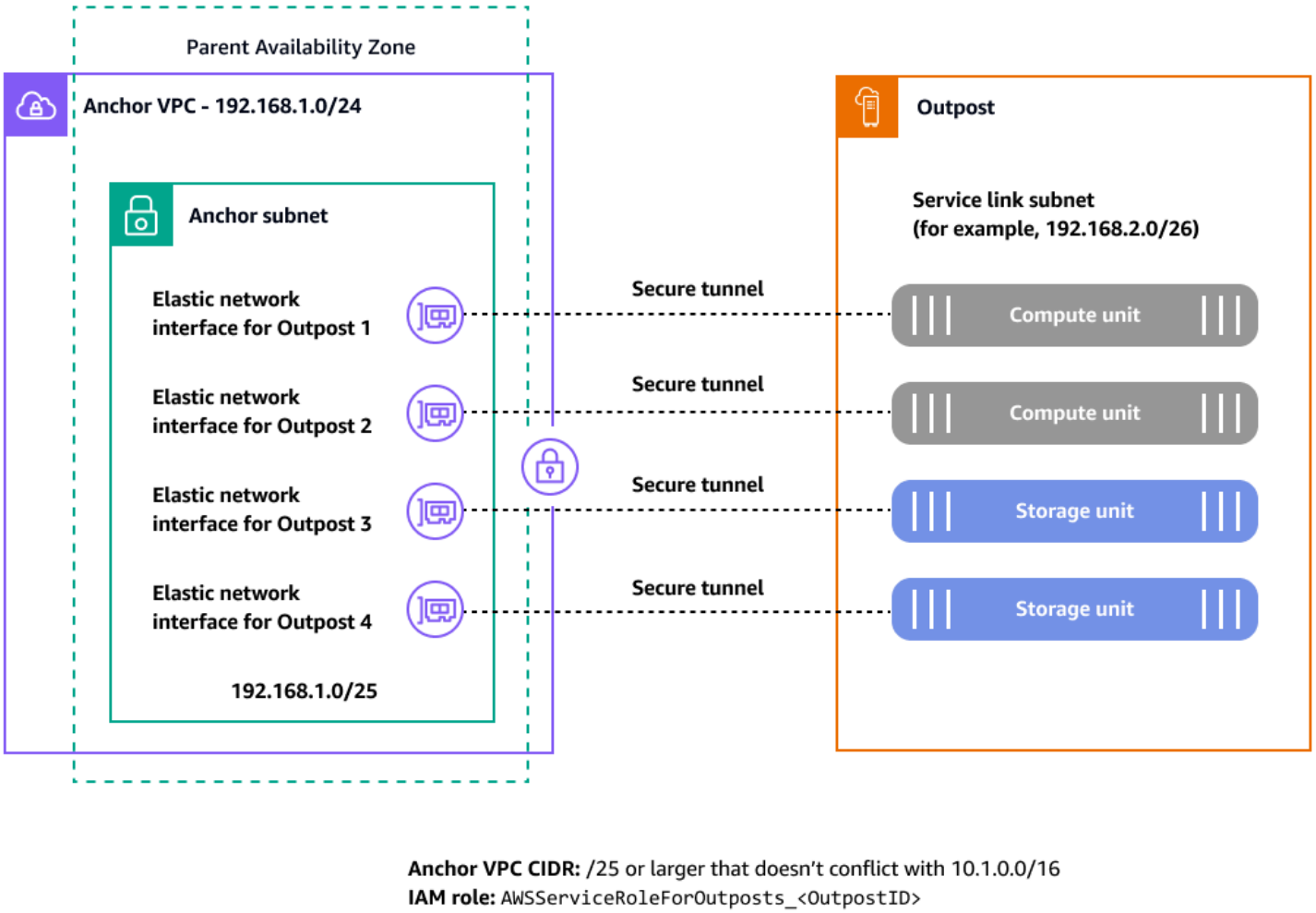
Standardmäßig werden alle in Amazon S3 on Outposts gespeicherten Daten mit serverseitiger Verschlüsselung über von Amazon S3 verwaltete Verschlüsselungsschlüssel (SSE-S3) verschlüsselt. Sie können serverseitige Verschlüsselung optional mit vom Kunden bereitgestellten Verschlüsselungsschlüsseln (SSE-C) verwenden. Wenn Sie SSE-C verwenden möchten, geben Sie einen Verschlüsselungsschlüssel als Teil Ihrer Objekt-API-Anforderungen an. Die serverseitige Verschlüsselung verschlüsselt nur die Objektdaten, nicht die Metadaten des Objekts.

> **Note**
>
> Amazon S3 on Outposts unterstützt keine serverseitige Verschlüsselung mit KMS-Schlüsseln (SSE-KMS).

Verschlüsselung während der Übertragung

Denn AWS Outposts der Service Link ist eine notwendige Verbindung zwischen Ihrem Outposts-Server und der von Ihnen ausgewählten AWS-Region (oder Heimatregion) und ermöglicht die Verwaltung des Outposts und den Austausch von Datenverkehr zu und von der. AWS-Region Der Service Link verwendet ein AWS verwaltetes VPN, um mit der Heimatregion zu kommunizieren. Jeder Host im Inneren AWS Outposts erstellt eine Reihe von VPN-Tunneln, um den Verkehr auf der Kontrollebene und den VPC-Verkehr aufzuteilen. Abhängig von der Service-Link-Konnektivität (Internet oder AWS Direct Connect) müssen für diese Tunnel Firewall-Ports geöffnet werden AWS Outposts, damit der Service-Link das Overlay darüber erstellen kann. Ausführliche technische Informationen zur Sicherheit von AWS Outposts und zum Service Link finden Sie AWS Outposts in der AWS Outposts Dokumentation unter Konnektivität über Service Link und Infrastruktursicherheit.

Der AWS Outposts Service Link erstellt verschlüsselte Tunnel, die die Konnektivität der Steuerungsebene und der Datenebene zur übergeordneten AWS-Region Komponente herstellen, wie in der folgenden Abbildung dargestellt.



Jeder AWS Outposts Host (Rechenleistung und Speicher) benötigt diese verschlüsselten Tunnel über bekannte TCP- und UDP-Ports, um mit seiner übergeordneten Region zu kommunizieren. Die folgende Tabelle zeigt die Quell- und Zielports und Adressen für die UDP- und TCP-Protokolle.

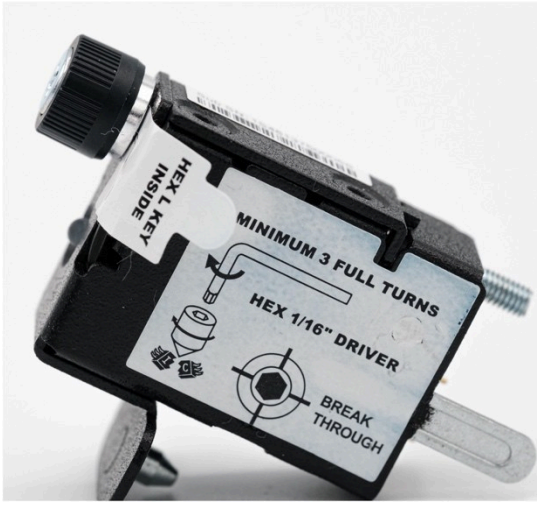
Protocol (Protokoll)	Quellport	Quelladresse	Zielport	Zieladresse
UDP	443	AWS Outposts Servicelink /26	443	AWS Outposts Öffentliche Routen oder Ankerrouten der Region — VPC CIDR

Protocol (Protokoll)	Quellport	Quelladresse	Zielport	Zieladresse
TCP	1025-65535	AWS Outposts Servicelink /26	443	AWS Outposts Öffentliche Routen oder Ankerrouten der Region — VPC CIDR

Local Zones sind auch über das redundante globale private Backbone von Amazon mit sehr hoher Bandbreite mit der übergeordneten Region verbunden. Diese Verbindung ermöglicht Anwendungen, die in Local Zones ausgeführt werden, schnellen, sicheren und nahtlosen Zugriff auf andere AWS-Services. Solange Local Zones Teil der AWS globalen Infrastruktur sind, werden alle Daten, die über das AWS globale Netzwerk fließen, automatisch auf der physischen Ebene verschlüsselt, bevor sie AWS gesicherte Einrichtungen verlassen. Wenn Sie spezielle Anforderungen für die Verschlüsselung der Daten bei der Übertragung zwischen Ihren lokalen Standorten und für den AWS Direct Connect PoPs Zugriff auf eine lokale Zone haben, können Sie MAC Security (MACsec) zwischen Ihrem lokalen Router oder Switch und dem Endpunkt aktivieren. AWS Direct Connect Weitere Informationen finden Sie im AWS Blogbeitrag Mehr MACsec Sicherheit für Verbindungen. AWS Direct Connect

Löschen von Daten

Wenn Sie eine EC2 Instance beenden oder beenden AWS Outposts, wird der ihr zugewiesene Speicher vom Hypervisor gelöscht (auf Null gesetzt), bevor er einer neuen Instance zugewiesen wird, und jeder Speicherblock wird zurückgesetzt. Das Löschen von Daten von der Outpost-Hardware erfordert die Verwendung spezieller Hardware. Das NSK ist ein kleines Gerät, das auf dem folgenden Foto abgebildet ist und an der Vorderseite jeder Computer- oder Speichereinheit in einem Outpost befestigt wird. Es wurde entwickelt, um zu verhindern, dass Ihre Daten von Ihrem Rechenzentrum oder Colocation-Standort aus offengelegt werden. Die Daten auf dem Outpost-Gerät werden geschützt, indem das zur Verschlüsselung des Geräts verwendete Schlüsselmaterial verpackt und das verpackte Material auf dem NSK gespeichert wird. Wenn Sie einen Outpost-Host zurückgeben, zerstören Sie den NSK, indem Sie eine kleine Schraube am Chip drehen, wodurch der NSK zerquetscht und der Chip physisch zerstört wird. Durch die Zerstörung des NSK werden die Daten auf deinem Outpost kryptografisch vernichtet.



Identitäts- und Zugriffsverwaltung

AWS Identity and Access Management (IAM) hilft einem Administrator AWS-Service , den Zugriff auf Ressourcen sicher zu kontrollieren. AWS IAM-Administratoren kontrollieren, wer authentifiziert (angemeldet) und autorisiert werden kann (über Berechtigungen verfügt), um Ressourcen zu verwenden. AWS Outposts Wenn Sie eine haben AWS-Konto, können Sie IAM ohne zusätzliche Kosten nutzen.

In der folgenden Tabelle sind die IAM-Funktionen aufgeführt, die Sie mit verwenden können. AWS Outposts

IAM-Funktion	AWS Outposts Unterstützung
Identitätsbasierte Richtlinien	Ja
Ressourcenbasierte Richtlinien	Ja*
Richtlinienaktionen	Ja
Richtlinienressourcen	Ja
Richtlinienbedingungsschlüssel (services pezifisch)	Ja
Zugriffskontrolllisten (ACLs)	Nein

IAM-Funktion	AWS Outposts Unterstützung
Attributbasierte Zugriffssteuerung (Attribute-Based Access Control, ABAC) (Tags in Richtlinien)	Ja
Temporäre Anmeldeinformationen	Ja
Prinzipalberechtigungen	Ja
Servicerollen	Nein
Serviceverknüpfte Rollen	Ja

* Zusätzlich zu den identitätsbasierten IAM-Richtlinien unterstützt Amazon S3 on Outposts sowohl Bucket- als auch Access-Point-Richtlinien. Dies sind ressourcenbasierte Richtlinien, die an die Ressource Amazon S3 on Outposts angehängt sind.

Weitere Informationen darüber, wie diese Funktionen unterstützt werden AWS Outposts, finden Sie im AWS Outposts Benutzerhandbuch.

Sicherheit der Infrastruktur

Der Schutz der Infrastruktur ist ein wichtiger Bestandteil eines Informationssicherheitsprogramms. Es stellt sicher, dass Workload-Systeme und -Dienste vor unbeabsichtigtem und unberechtigtem Zugriff sowie vor potenziellen Sicherheitslücken geschützt sind. Sie definieren beispielsweise Vertrauensgrenzen (z. B. Netzwerk- und Kontogrenzen), Konfiguration und Wartung der Systemsicherheit (z. B. Abhärtung, Minimierung und Patchen), Betriebssystemauthentifizierung und Autorisierungen (z. B. Benutzer, Schlüssel und Zugriffsebenen) und andere geeignete Punkte zur Durchsetzung von Richtlinien (z. B. Webanwendungs-Firewalls oder API-Gateways).

AWS bietet eine Reihe von Ansätzen für den Infrastrukturschutz, die in den folgenden Abschnitten beschrieben werden.

Schutz von Netzwerken

Ihre Benutzer können Teil Ihrer Belegschaft oder Ihrer Kunden sein und können sich überall befinden. Aus diesem Grund können Sie nicht jedem vertrauen, der Zugriff auf Ihr Netzwerk hat. Wenn Sie

dem Prinzip folgen, Sicherheit auf allen Ebenen anzuwenden, verwenden Sie einen Zero-Trust-Ansatz. Im Zero-Trust-Sicherheitsmodell werden Anwendungskomponenten oder Microservices als diskret betrachtet, und keine Komponente oder kein Microservice vertraut einer anderen Komponente oder einem anderen Microservice. Um Zero-Trust-Sicherheit zu erreichen, folgen Sie diesen Empfehlungen:

- Erstellen Sie Netzwerkschichten. Mehrschichtige Netzwerke helfen dabei, ähnliche Netzwerkkomponenten logisch zu gruppieren. Sie verringern auch das potenzielle Ausmaß der Auswirkungen eines unbefugten Netzwerkzugriffs.
- Kontrollieren Sie die Verkehrsebenen. Wenden Sie mehrere Kontrollen mit einem defense-in-depth Ansatz für eingehenden und ausgehenden Verkehr an. Dazu gehört die Verwendung von Sicherheitsgruppen (Stateful-Inspection-Firewalls), Netzwerken ACLs, Subnetzen und Routing-Tabellen.
- Implementieren Sie Inspektion und Schutz. Untersuchen und filtern Sie Ihren Datenverkehr auf jeder Ebene. Mit Network Access Analyzer können Sie Ihre VPC-Konfigurationen auf möglichen unbeabsichtigten Zugriff überprüfen. Sie können Ihre Netzwerkzugriffsanforderungen spezifizieren und potenzielle Netzwerkpfade identifizieren, die diese Anforderungen nicht erfüllen.

Schutz der Rechenressourcen

Zu den Rechenressourcen gehören EC2 Instanzen, Container, AWS Lambda Funktionen, Datenbankdienste, IoT-Geräte und mehr. Jeder Rechenressourcentyp erfordert einen anderen Sicherheitsansatz. Diese Ressourcen haben jedoch gemeinsame Strategien, die Sie berücksichtigen müssen: gründliche Abwehr, Schwachstellenmanagement, Reduzierung der Angriffsfläche, Automatisierung von Konfiguration und Betrieb sowie Durchführung von Aktionen aus der Ferne.

Hier finden Sie allgemeine Hinweise zum Schutz Ihrer Rechenressourcen für wichtige Dienste:

- Erstellen und verwalten Sie ein Vulnerability Management-Programm. Scannen und patchen Sie regelmäßig Ressourcen wie EC2 Instances, Amazon Elastic Container Service (Amazon ECS) - Container und Amazon Elastic Kubernetes Service (Amazon EKS) -Workloads.
- Automatisieren Sie den Computerschutz. Automatisieren Sie Ihre Computerschutzmechanismen, einschließlich Schwachstellenmanagement, Reduzierung der Angriffsfläche und Ressourcenverwaltung. Durch diese Automatisierung gewinnen Sie Zeit, die Sie für die Sicherung anderer Aspekte Ihres Workloads nutzen können, und trägt dazu bei, das Risiko menschlicher Fehler zu verringern.

- Reduzieren Sie die Angriffsfläche. Reduzieren Sie das Risiko unbeabsichtigter Zugriffe, indem Sie Ihre Betriebssysteme absichern und die Anzahl der verwendeten Komponenten, Bibliotheken und extern nutzbaren Dienste auf ein Minimum reduzieren.

Lesen Sie außerdem für jeden AWS-Service Dienst, den Sie verwenden, die spezifischen Sicherheitsempfehlungen in der Servicedokumentation.

Internetzugang

AWS Outposts Sowohl Local Zones als auch lokale Zonen bieten Architekturmuster, mit denen Ihre Workloads auf das und aus dem Internet zugreifen können. Wenn du diese Muster verwendest, betrachte Internetnutzung aus der Region nur dann als praktikable Option, wenn du sie für Patches, Updates, den Zugriff auf externe Git-Repositorys und ähnliche AWS Szenarien verwendest. Für dieses Architekturmuster gelten die Konzepte der zentralen Eingangsprüfung und der zentralisierten Internetausgangsprüfung. Diese Zugriffsmuster verwenden AWS Transit Gateway NAT-Gateways, Netzwerk-Firewalls und andere Komponenten, die sich in AWS Outposts oder Local Zones befinden AWS-Regionen, aber über den Datenpfad zwischen der Region und dem Edge mit diesen verbunden sind.

Local Zones verwendet ein Netzwerkkonstrukt, das als Netzwerkgrenzgruppe bezeichnet wird und in AWS-Regionen verwendet wird. AWS gibt öffentliche IP-Adressen aus diesen eindeutigen Gruppen bekannt. Eine Netzwerkgrenzgruppe besteht aus Availability Zones, Local Zones oder Wavelength Zones. Sie können explizit einen Pool öffentlicher IP-Adressen für die Verwendung in einer Netzwerkgrenzgruppe zuweisen. Sie können eine Netzwerkgrenzgruppe verwenden, um das Internet-Gateway auf Local Zones auszudehnen, indem Sie zulassen, dass Elastic IP-Adressen von der Gruppe aus bedient werden. Für diese Option müssen Sie weitere Komponenten bereitstellen, um die in Local Zones verfügbaren Kerndienste zu ergänzen. Diese Komponenten können aus Ihrer lokalen Zone stammen ISVs und Ihnen dabei helfen, Inspektionsebenen in Ihrer lokalen Zone aufzubauen, wie im AWS Blogbeitrag Hybride Inspektionsarchitekturen mit AWS Lokale Zonen beschrieben.

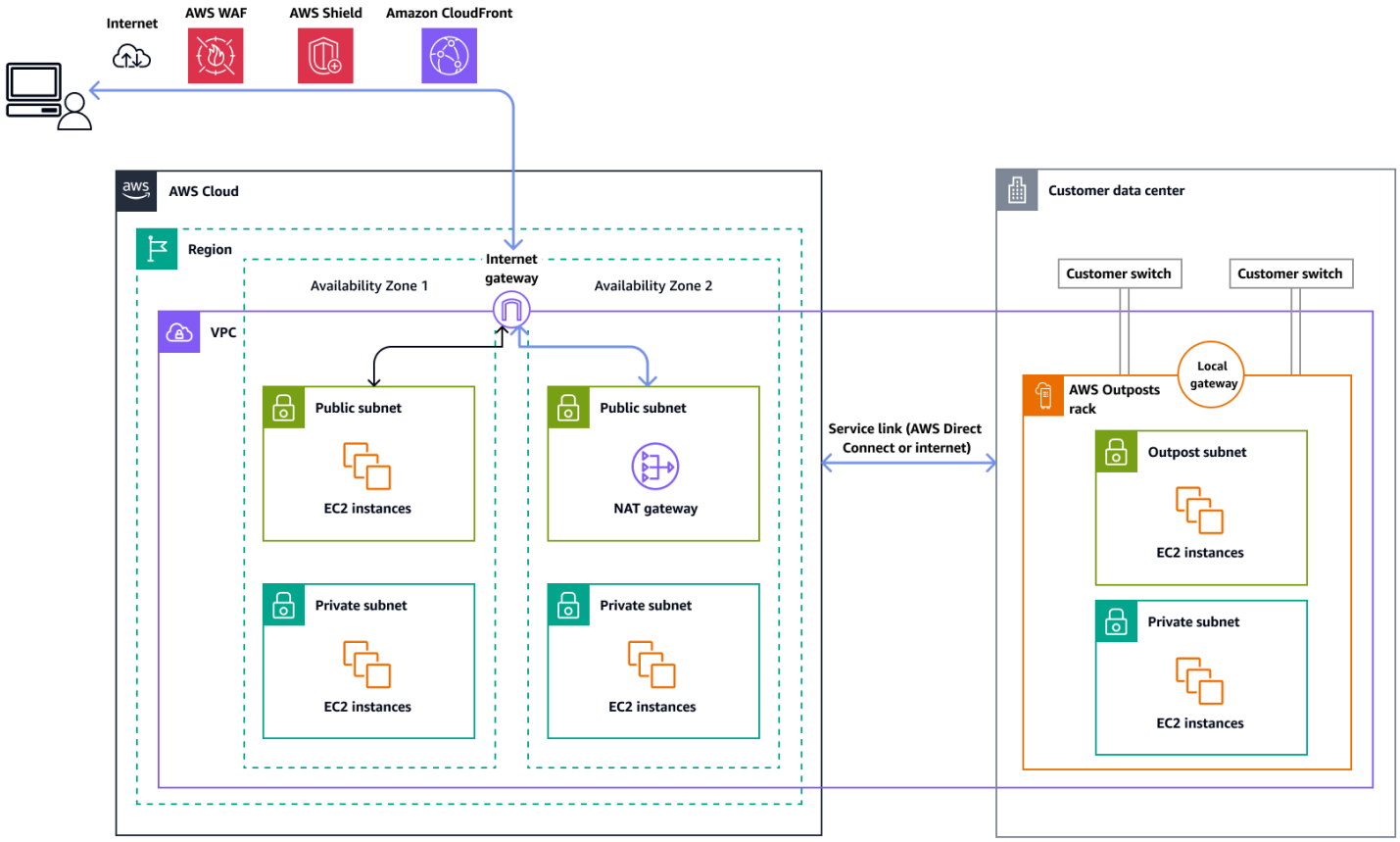
Wenn Sie das lokale Gateway (LGW) verwenden möchten AWS Outposts, um von Ihrem Netzwerk aus auf das Internet zuzugreifen, müssen Sie die benutzerdefinierte Routing-Tabelle ändern, die dem Subnetz zugeordnet ist. AWS Outposts Die Routentabelle muss über einen Standardrouteneintrag (0.0.0.0/0) verfügen, der die LGW als nächsten Hop verwendet. Sie sind dafür verantwortlich, die übrigen Sicherheitskontrollen in Ihrem lokalen Netzwerk zu implementieren, einschließlich Schutzmaßnahmen wie Firewalls und Intrusion Prevention Systems oder Intrusion Detection

Systems (IPS/IDS). Dies entspricht dem Modell der gemeinsamen Verantwortung, das die Sicherheitsaufgaben zwischen Ihnen und dem Cloud-Anbieter aufteilt.

Internetzugang durch den Elternteil AWS-Region

Bei dieser Option greifen die Workloads im Outpost über den Service Link und das Internet-Gateway im übergeordneten System auf das Internet zu. AWS-Region Ausgehender Datenverkehr ins Internet kann über das NAT-Gateway geleitet werden, das in Ihrer VPC instanziiert ist. Für zusätzliche Sicherheit für Ihren eingehenden und ausgehenden Verkehr können Sie AWS Sicherheitsdienste wie AWS WAF, AWS Shield, und Amazon CloudFront in der verwenden. AWS-Region

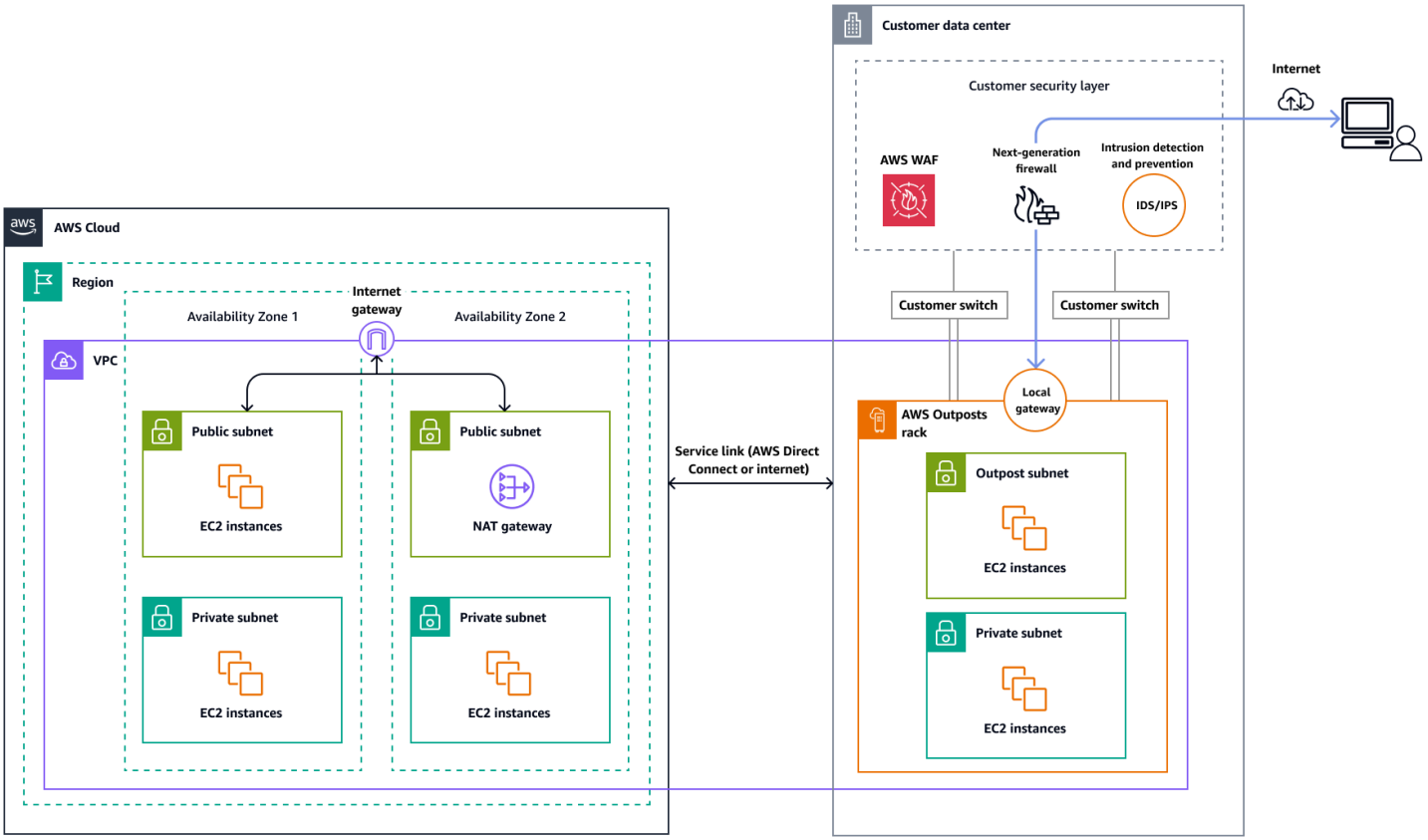
Das folgende Diagramm zeigt den Datenverkehr zwischen dem Workload in der AWS Outposts Instance und dem Internet, der über die übergeordnete Instanz fließt. AWS-Region



Internetzugang über das Netzwerk Ihres lokalen Rechenzentrums

Bei dieser Option greifen die Workloads im Outpost über Ihr lokales Rechenzentrum auf das Internet zu. Der Workload-Verkehr, der auf das Internet zugreift, durchläuft Ihren lokalen Internet-Präsenzpunkt und fließt lokal ab. In diesem Fall ist die Netzwerksicherheitsinfrastruktur Ihres lokalen Rechenzentrums für die Sicherung des Workload-Datenverkehrs verantwortlich. AWS Outposts

Die folgende Abbildung zeigt den Datenverkehr zwischen einem Workload im AWS Outposts Subnetz und dem Internet, der durch ein Rechenzentrum fließt.



Verwaltung der Infrastruktur

Unabhängig davon, ob Ihre Workloads in einer lokalen Zone oder einem AWS-Region Außenposten bereitgestellt werden, können Sie sie AWS Control Tower für die Infrastruktur-Governance verwenden. AWS Control Tower bietet eine einfache Möglichkeit, eine Umgebung mit AWS mehreren Konten einzurichten und zu verwalten und dabei die vorgeschriebenen Best Practices zu befolgen. AWS Control Tower orchestriert die Funktionen mehrerer anderer Anbieter AWS-Services, darunter AWS Organizations AWS Service Catalog, und IAM Identity Center (alle integrierten Services anzeigen), um in weniger als einer Stunde eine landing zone aufzubauen. Ressourcen werden in Ihrem Namen eingerichtet und verwaltet.

AWS Control Tower bietet eine einheitliche Steuerung für alle AWS Umgebungen, einschließlich Regionen, Local Zones (Erweiterungen mit niedriger Latenz) und Outposts (lokale Infrastruktur). Dies trägt dazu bei, konsistente Sicherheit und Compliance in Ihrer gesamten Hybrid-Cloud-Architektur zu gewährleisten. Weitere Informationen finden Sie in der AWS Control Tower -Dokumentation.

Sie können Funktionen wie Leitplanken konfigurieren AWS Control Tower , um die Anforderungen an die Datenresidenz in Regierungen und regulierten Branchen wie Finanzdienstleistungsinstituten () zu erfüllen. FSIs Im Folgenden erfahren Sie, wie Sie Leitplanken für die Datenresidenz am Netzwerkrand einrichten können:

- Bewährte Methoden für die Verwaltung der Datenresidenz AWS Lokale Zonen mithilfe von landing zone Controls (AWS Blogbeitrag)
- Architektur für die Datenresidenz mit AWS Outposts Rack- und Landezonenleitplanken (Blogbeitrag)AWS
- Datenresidenz mit Hybrid Cloud Services Lens (AWS Well-Architected Framework-Dokumentation)

Ressourcen von Outposts teilen

Da es sich bei einem Outpost um eine begrenzte Infrastruktur handelt, die sich in Ihrem Rechenzentrum oder in einem Colocation-Bereich befindet, müssen Sie für eine zentrale Verwaltung zentral kontrollieren AWS Outposts, mit welchen Konten AWS Outposts Ressourcen gemeinsam genutzt werden.

Mit Outpost Sharing können Outpost-Besitzer ihre Outposts und Outpost-Ressourcen, einschließlich Outpost-Sites und Subnetze, mit anderen teilen, AWS-Konten die sich in derselben Organisation befinden. AWS Organizations Als Outpost-Besitzer können Sie Outpost-Ressourcen von einem zentralen Ort aus erstellen und verwalten und die Ressourcen für mehrere innerhalb Ihrer Organisation gemeinsam nutzen. AWS-Konten AWS Auf diese Weise können andere Nutzer Outpost-Sites nutzen, Instanzen auf dem gemeinsam genutzten Outpost konfigurieren VPCs, starten und ausführen.

Zu den gemeinsam nutzbaren Ressourcen gehören: AWS Outposts

- Zugewiesene dedizierte Hosts
- Kapazitätsreservierungen
- Kundeneigene IP-Adresspools (CoIP)
- Routing-Tabellen für das lokale Gateway
- Outposts
- Amazon S3 on Outposts
- Standorte

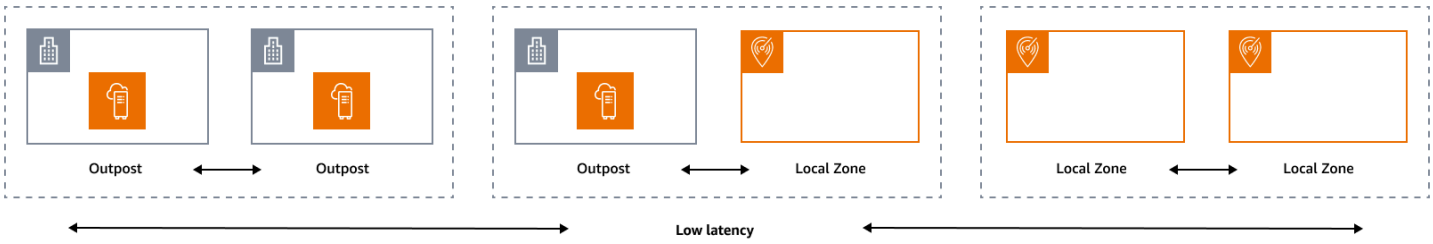
- Subnetze

Informationen zu den bewährten Methoden für die gemeinsame Nutzung Outposts Outposts-Ressourcen in einer Umgebung mit mehreren Konten finden Sie in den folgenden AWS Blogbeiträgen:

- Teilen AWS Outposts in einer AWS Umgebung mit mehreren Konten: Teil 1
- Teilen AWS Outposts in einer AWS Umgebung mit mehreren Konten: Teil 2

Resilienz an der Peripherie

Die Säule Zuverlässigkeit umfasst die Fähigkeit eines Workloads, die vorgesehene Funktion korrekt und konsistent auszuführen, wenn dies erwartet wird. Dazu gehört auch die Fähigkeit, den Workload während seines gesamten Lebenszyklus zu bedienen und zu testen. In diesem Sinne müssen Sie beim Entwurf einer ausfallsicheren Architektur am Netzwerkrand zunächst überlegen, welche Infrastrukturen Sie für die Bereitstellung dieser Architektur verwenden werden. Es gibt drei mögliche Kombinationen, die mithilfe von AWS Lokale Zonen und implementiert werden können AWS Outposts: Outpost to Outpost, Outpost to Local Zone und Local Zone to Local Zone, wie in der folgenden Abbildung dargestellt. Zwar gibt es auch andere Möglichkeiten für ausfallsichere Architekturen, wie z. B. die Kombination von AWS Edge-Services mit herkömmlicher lokaler Infrastruktur oder AWS-Regionen, doch dieser Leitfaden konzentriert sich auf diese drei Kombinationen, die für das Design von Hybrid-Cloud-Diensten gelten



Überlegungen zur Infrastruktur

Eines der Kernprinzipien des Service Designs von At AWS besteht darin, einzelne Ausfallpunkte in der zugrunde liegenden physischen Infrastruktur zu vermeiden. Aufgrund dieses Prinzips verwenden AWS Software und Systeme mehrere Availability Zones und sind widerstandsfähig gegen den Ausfall einer einzelnen Zone. At the Edge AWS bietet Infrastrukturen, die auf Local Zones und Outposts basieren. Ein entscheidender Faktor für die Gewährleistung der Ausfallsicherheit beim Infrastrukturdesign ist daher die Definition, wo die Ressourcen einer Anwendung eingesetzt werden.

Lokale Zonen

Local Zones verhalten sich ähnlich wie Availability Zones innerhalb ihrer Zonen AWS-Region, da sie als Platzierungsort für zonale AWS Ressourcen wie Subnetze und EC2 Instances ausgewählt werden können. Sie befinden sich jedoch nicht in AWS-Region, sondern in der Nähe von großen Industrie- und IT-Zentren mit großer Bevölkerung, in denen es heute keine AWS-Region gibt. Trotzdem bieten sie weiterhin sichere Verbindungen mit hoher Bandbreite zwischen lokalen Workloads in der Local Zone und Workloads, die in der Local Zone ausgeführt werden. AWS-Region Daher sollten Sie Local Zones verwenden, um Workloads näher an Ihren Benutzern bereitzustellen, um Anforderungen mit geringer Latenz zu erfüllen.

Outposts

AWS Outposts ist ein vollständig verwalteter Service, der AWS Infrastruktur AWS-Services APIs, und Tools auf Ihr Rechenzentrum ausdehnt. Dieselbe Hardware-Infrastruktur, die in verwendet wird, AWS Cloud ist in Ihrem Rechenzentrum installiert. Outposts werden dann mit den nächstgelegenen AWS-Region verbunden. Sie können Outposts verwenden, um Ihre Workloads zu unterstützen, die eine geringe Latenz oder lokale Datenverarbeitungsanforderungen haben.

Availability Zones für Eltern

Jede lokale Zone oder jeder Außenposten hat eine übergeordnete Region (auch als Heimatregion bezeichnet). In der übergeordneten Region ist die Steuerungsebene der AWS Edge-Infrastruktur (Außenposten oder Lokale Zone) verankert. Im Fall von Local Zones ist die übergeordnete Region eine grundlegende architektonische Komponente einer Local Zone und kann von Kunden nicht geändert werden. AWS Outposts erweitert das AWS Cloud auf Ihre lokale Umgebung, sodass Sie während des Bestellvorgangs eine bestimmte Region und Availability Zone auswählen müssen. Diese Auswahl verankert die Kontrollebene Ihres Outposts-Einsatzes in der ausgewählten AWS Infrastruktur.

Wenn Sie Hochverfügbarkeitsarchitekturen am Edge entwickeln, muss die übergeordnete Region dieser Infrastrukturen, wie Outposts oder Local Zones, identisch sein, damit eine VPC zwischen ihnen erweitert werden kann. Diese erweiterte VPC ist die Grundlage für die Erstellung dieser Hochverfügbarkeitsarchitekturen. Wenn Sie eine hochbelastbare Architektur definieren, müssen Sie aus diesem Grund die übergeordnete Region und die Availability Zone der Region validieren, in der der Service verankert sein wird (oder ist). Wie in der folgenden Abbildung dargestellt, müssen Sie, wenn Sie eine Hochverfügbarkeitslösung zwischen zwei Außenstellen bereitstellen möchten, zwei verschiedene Availability Zones auswählen, um die Outposts zu verankern. Dies ermöglicht

eine Multi-AZ-Architektur aus Sicht der Steuerungsebene. Wenn Sie eine hochverfügbare Lösung bereitstellen möchten, die eine oder mehrere Local Zones umfasst, müssen Sie zunächst die übergeordnete Availability Zone validieren, in der die Infrastruktur verankert ist. Verwenden Sie zu diesem Zweck den folgenden AWS CLI Befehl:

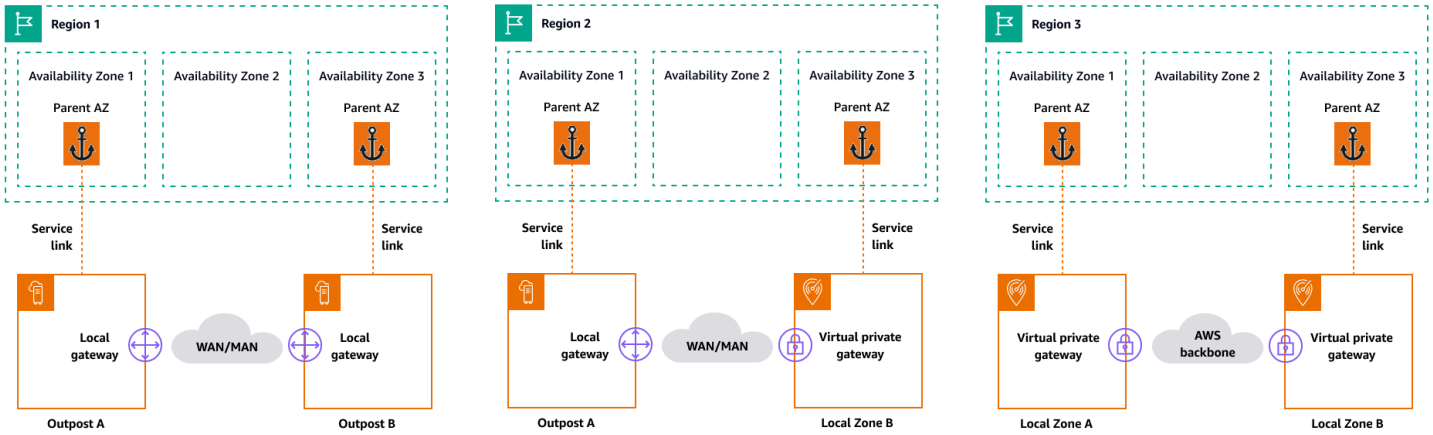
```
aws ec2 describe-availability-zones --zone-ids use1-mia1-az1
```

Ausgabe des vorherigen Befehls:

```
{     "AvailabilityZones": [
          {
             "State": "available",
             "OptInStatus": "opted-in",
             "Messages": [],
             "RegionName": "us-east-1",
             "ZoneName": "us-east-1-mia-1a",
             "ZoneId": "use1-mia1-az1",
             "GroupName": "us-east-1-mia-1",
             "NetworkBorderGroup": "us-east-1-mia-1",
             "ZoneType": "local-zone",
             "ParentZoneName": "us-east-1d",
             "ParentZoneId": "use1-az2"
          }
     ]
 }
```

In diesem Beispiel ist die Miami Local Zone (`us-east-1d-mia-1a1`) in der `us-east-1d-az2` Availability Zone verankert. Wenn Sie also eine robuste Architektur am Edge erstellen müssen, müssen Sie sicherstellen, dass die sekundäre Infrastruktur (entweder Outposts oder Local Zones) in einer anderen Availability Zone als verankert ist. **`us-east-1d-az2`** `us-east-1d-az1`Wäre zum Beispiel gültig.

Das folgende Diagramm enthält Beispiele für hochverfügbare Edge-Infrastrukturen.



Überlegungen zum Netzwerk

In diesem Abschnitt werden erste Überlegungen zu Netzwerken am Netzwerkrand erörtert, hauptsächlich im Hinblick auf Verbindungen für den Zugriff auf die Edge-Infrastruktur. Es werden gültige Architekturen untersucht, die ein stabiles Netzwerk für den Service Link bereitstellen.

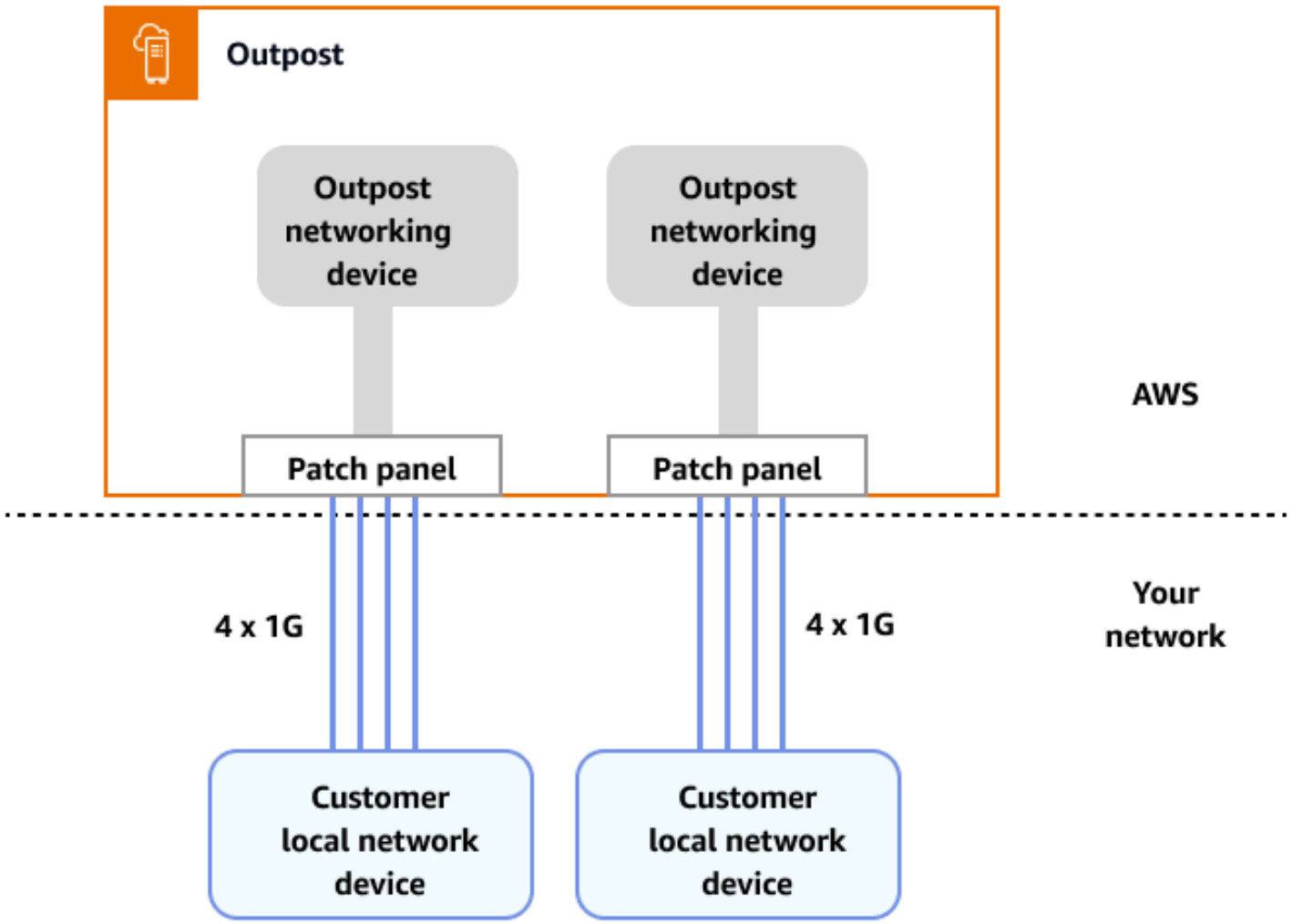
Resilienznetzwerke für Local Zones

Local Zones sind über mehrere redundante, sichere Hochgeschwindigkeitsverbindungen mit der übergeordneten Region verbunden, sodass Sie alle regionalen Dienste wie Amazon S3 und Amazon RDS problemlos nutzen können. Sie sind dafür verantwortlich, Konnektivität von Ihrer lokalen Umgebung oder Ihren Benutzern zur lokalen Zone bereitzustellen. Unabhängig von der gewählten Konnektivitätsarchitektur (z. B. VPN oder AWS Direct Connect) muss die Latenz, die über die Netzwerkverbindungen erreicht werden muss, gleichwertig sein, um jegliche Beeinträchtigung der Anwendungsleistung bei einem Ausfall einer Hauptverbindung zu vermeiden. Falls Sie diese verwenden AWS Direct Connect, entsprechen die entsprechenden Resilienzarchitekturen denen für den Zugriff auf AWS-Region, wie in den AWS Direct Connect Resilienz-Empfehlungen dokumentiert. Es gibt jedoch Szenarien, die hauptsächlich für internationale Local Zones gelten. In dem Land, in dem die Local Zone aktiviert ist, ist es mit nur einem einzigen AWS Direct Connect PoP unmöglich, die aus Gründen der AWS Direct Connect Resilienz empfohlenen Architekturen zu erstellen. Wenn Sie Zugriff auf nur einen einzigen AWS Direct Connect Standort haben oder Ausfallsicherheit benötigen, die über eine einzelne Verbindung hinausgeht, können Sie eine VPN-Appliance bei Amazon einrichten EC2 und AWS Direct Connect, wie im AWS Blogbeitrag Enabling high available connectivity from local to AWS Lokale Zonen dargestellt und besprochen.

Resilienznetzwerke für Outposts

Im Gegensatz zu Local Zones verfügen Outposts über redundante Konnektivität für den Zugriff auf Workloads, die in Outposts bereitgestellt werden, von Ihrem lokalen Netzwerk aus. Diese Redundanz wird durch zwei Outposts-Netzwerkgeräte () ONDs erreicht. Jedes OND benötigt mindestens zwei Glasfaserverbindungen mit 1 Gbit/s, 10 Gbit/s, 40 Gbit/s oder 100 Gbit/s zu Ihrem lokalen Netzwerk. Diese Verbindungen müssen als Link Aggregation Group (LAG) konfiguriert werden, um das skalierbare Hinzufügen weiterer Links zu ermöglichen.

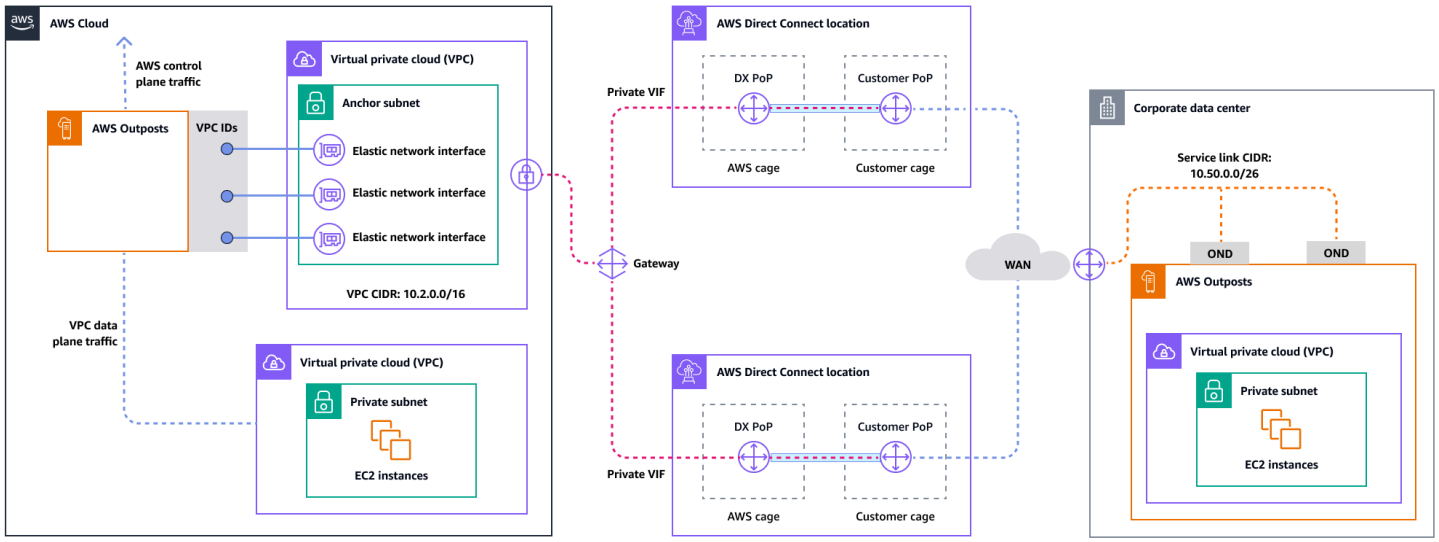
Uplink-Geschwindigkeit	Anzahl der Uplinks
1 Gbit/s	1, 2, 4, 6, oder 8
10 Gbit/s	1, 2, 4, 8, 12, oder 16
40 oder 100 Gbit/s	1, 2, oder 4



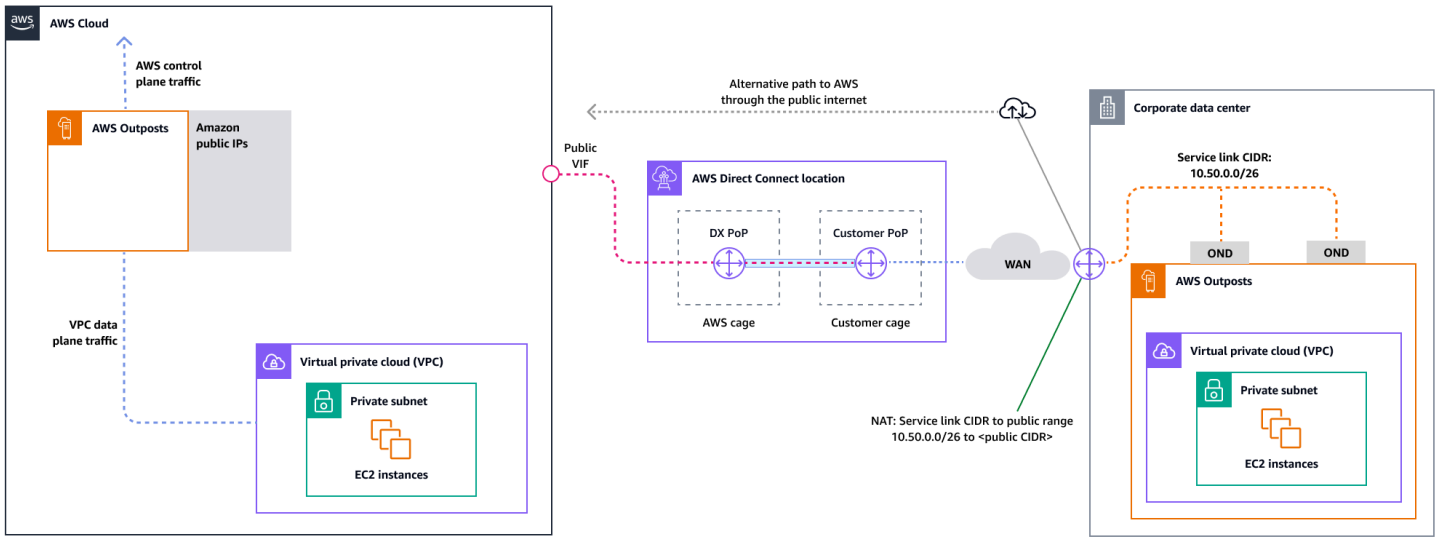
Weitere Informationen zu dieser Konnektivität finden Sie in der AWS Outposts Dokumentation unter Lokale Netzwerkkonnektivität Outposts Outposts-Racks.

Für eine optimale Benutzererfahrung und Ausfallsicherheit AWS empfiehlt es sich, redundante Konnektivität mit mindestens 500 Mbit/s (1 Gbit/s ist besser) für die Service Link-Verbindung zum zu verwenden. AWS-Region Sie können AWS Direct Connect oder eine Internetverbindung für den Service Link verwenden. Mit diesem Minimum können Sie EC2 Instances starten, EBS-Volumes anhängen und auf Amazon EKS AWS-Services, Amazon EMR und CloudWatch Metriken zugreifen.

Das folgende Diagramm veranschaulicht diese Architektur für eine hochverfügbare private Verbindung.



Das folgende Diagramm veranschaulicht diese Architektur für eine hochverfügbare öffentliche Verbindung.



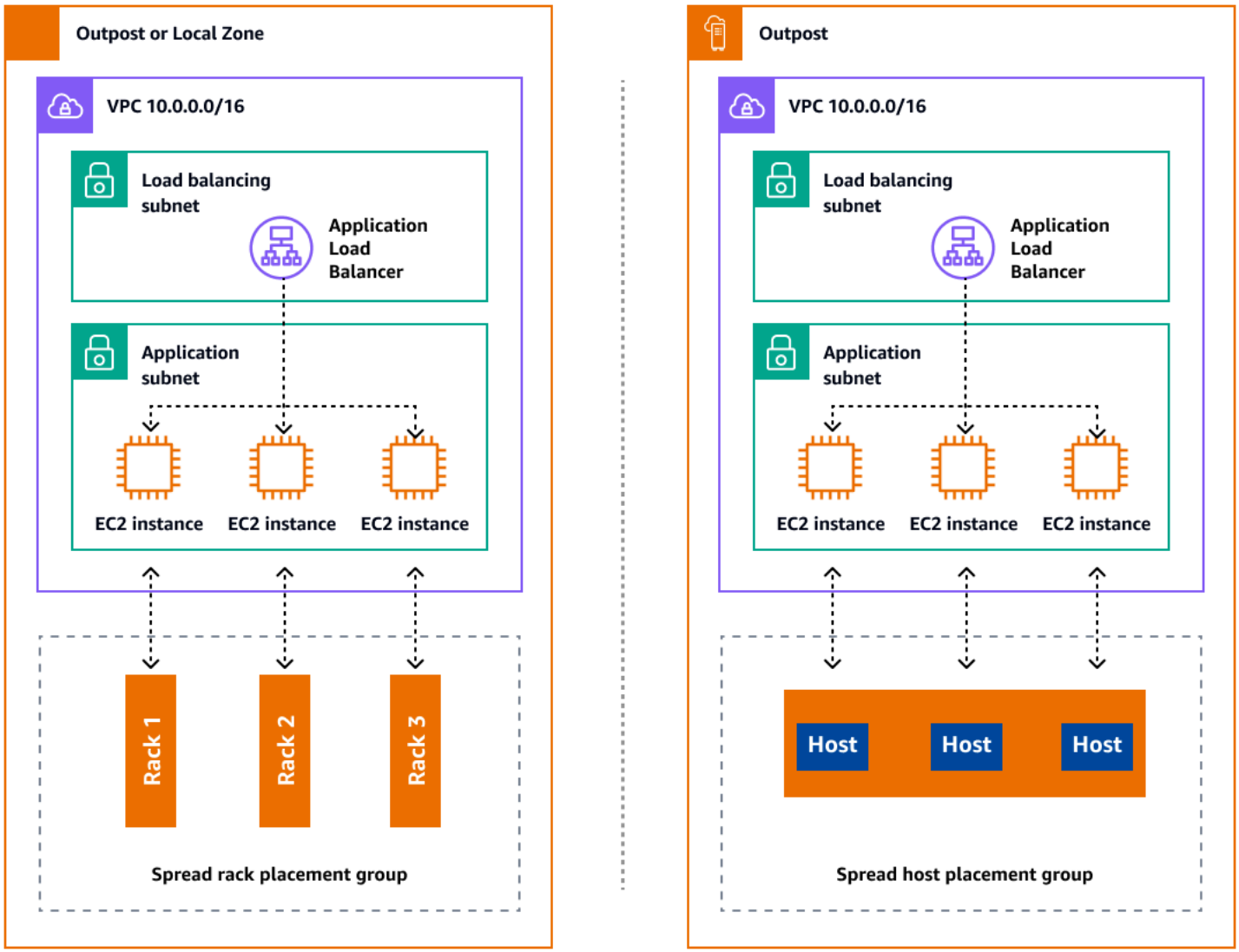
Skalierung Outposts Outposts-Rack-Bereitstellungen mit ACE-Racks

Das Aggregation, Core, Edge (ACE) -Rack dient als kritischer Aggregationspunkt für AWS Outposts Multi-Rack-Bereitstellungen und wird in erster Linie für Installationen mit mehr als drei Racks oder für die Planung future Erweiterungen empfohlen. Jedes ACE-Rack verfügt über vier Router, die Verbindungen mit 10 Gbit/s, 40 Gbit/s und 100 Gbit/s unterstützen (100 Gbit/s sind optimal). Jedes Rack kann für maximale Redundanz mit bis zu vier vorgelagerten Kundengeräten verbunden werden. ACE-Racks verbrauchen bis zu 10 kVA Strom und wiegen bis zu 705 Pfund. Zu den wichtigsten Vorteilen gehören geringere physische Netzwerkanforderungen, weniger Uplinks für Glasfaserkabel und weniger virtuelle VLAN-Schnittstellen. AWS überwacht diese Racks mithilfe von Telemetriedaten

über VPN-Tunnel und arbeitet bei der Installation eng mit den Kunden zusammen, um die richtige Stromverfügbarkeit, Netzwerkkonfiguration und optimale Platzierung sicherzustellen. Die ACE-Rack-Architektur bietet im Zuge der Skalierung der Bereitstellungen einen immer größeren Nutzen. Sie vereinfacht effektiv die Konnektivität und reduziert gleichzeitig die Komplexität und die physischen Port-Anforderungen in größeren Installationen. Weitere Informationen finden Sie im AWS Blogbeitrag Skalierung von Rack-Bereitstellungen mit ACE AWS Outposts Rack.

Verteilung von Instanzen auf Outposts und Local Zones

Outposts und Local Zones haben eine begrenzte Anzahl von Rechenservern. Wenn Ihre Anwendung mehrere verwandte Instanzen bereitstellt, werden diese Instanzen möglicherweise auf demselben Server oder auf Servern im selben Rack bereitgestellt, sofern sie nicht unterschiedlich konfiguriert sind. Zusätzlich zu den Standardoptionen können Sie Instances auf mehrere Server verteilen, um das Risiko zu minimieren, dass verwandte Instances auf derselben Infrastruktur ausgeführt werden. Sie können Instances auch mithilfe von Partitionsplatzierungsgruppen auf mehrere Racks verteilen. Dies wird als Spread-Rack-Verteilungsmodell bezeichnet. Verwenden Sie die automatische Verteilung, um Instanzen auf Partitionen in der Gruppe zu verteilen, oder stellen Sie Instanzen auf ausgewählten Zielpartitionen bereit. Durch die Bereitstellung von Instances auf Zielpartitionen können Sie ausgewählte Ressourcen im selben Rack bereitstellen und gleichzeitig andere Ressourcen auf mehrere Racks verteilen. Outposts bietet auch eine weitere Option namens Spread Host, mit der Sie Ihre Arbeitslast auf Host-Ebene verteilen können. Das folgende Diagramm zeigt die Verteilungsoptionen „Spread Rack“ und „Spread Host“.



Amazon RDS Multi-AZ im AWS Outposts

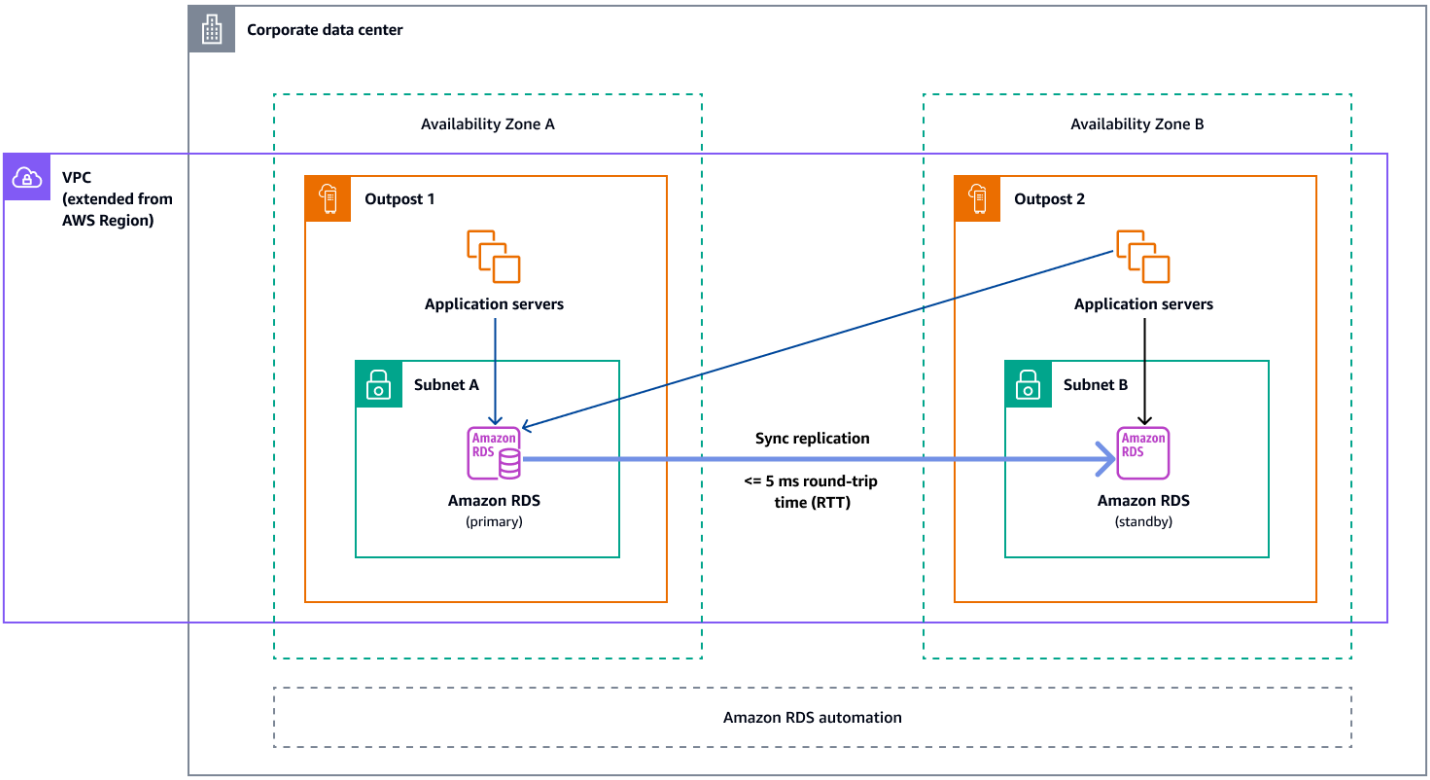
Wenn Sie Multi-AZ-Instance-Bereitstellungen auf Outposts verwenden, erstellt Amazon RDS zwei Datenbank-Instances in zwei Outposts. Jeder Outpost läuft auf seiner eigenen physischen Infrastruktur und stellt eine Verbindung zu verschiedenen Availability Zones in einer Region her, um eine hohe Verfügbarkeit zu gewährleisten. Wenn zwei Outposts über eine vom Kunden verwaltete lokale Verbindung verbunden sind, verwaltet Amazon RDS die synchrone Replikation zwischen der primären und der Standby-Datenbank-Instance. Im Falle eines Software- oder Infrastrukturausfalls stuft Amazon RDS die Standby-Instance automatisch in die primäre Rolle hoch und aktualisiert den DNS-Eintrag so, dass er auf die neue primäre Instance verweist. Für Multi-AZ-Bereitstellungen erstellt Amazon RDS eine primäre DB-Instance in einem -Outpost und repliziert die Daten synchron auf eine

Standby-DB-Instance in einem anderen Outpost. Multi-AZ-Bereitstellungen auf Outposts funktionieren wie Multi-AZ-Bereitstellungen in AWS-Regionen, mit den folgenden Unterschieden:

- Sie benötigen eine lokale Verbindung zwischen zwei oder mehr Outposts.
- Sie benötigen kundeneigene IP-Adresspools (CoIP). Weitere Informationen finden Sie unter Kundeneigene IP-Adressen für Amazon RDS AWS Outposts in der Amazon RDS-Dokumentation.
- Die Replikation läuft in Ihrem lokalen Netzwerk.

Multi-AZ-Bereitstellungen sind für alle unterstützten Versionen von MySQL und PostgreSQL auf Amazon RDS on Outposts verfügbar. Lokale Backups werden für Multi-AZ-Bereitstellungen nicht unterstützt.

Das folgende Diagramm zeigt die Architektur für Multi-AZ-Konfigurationen von Amazon RDS on Outposts.

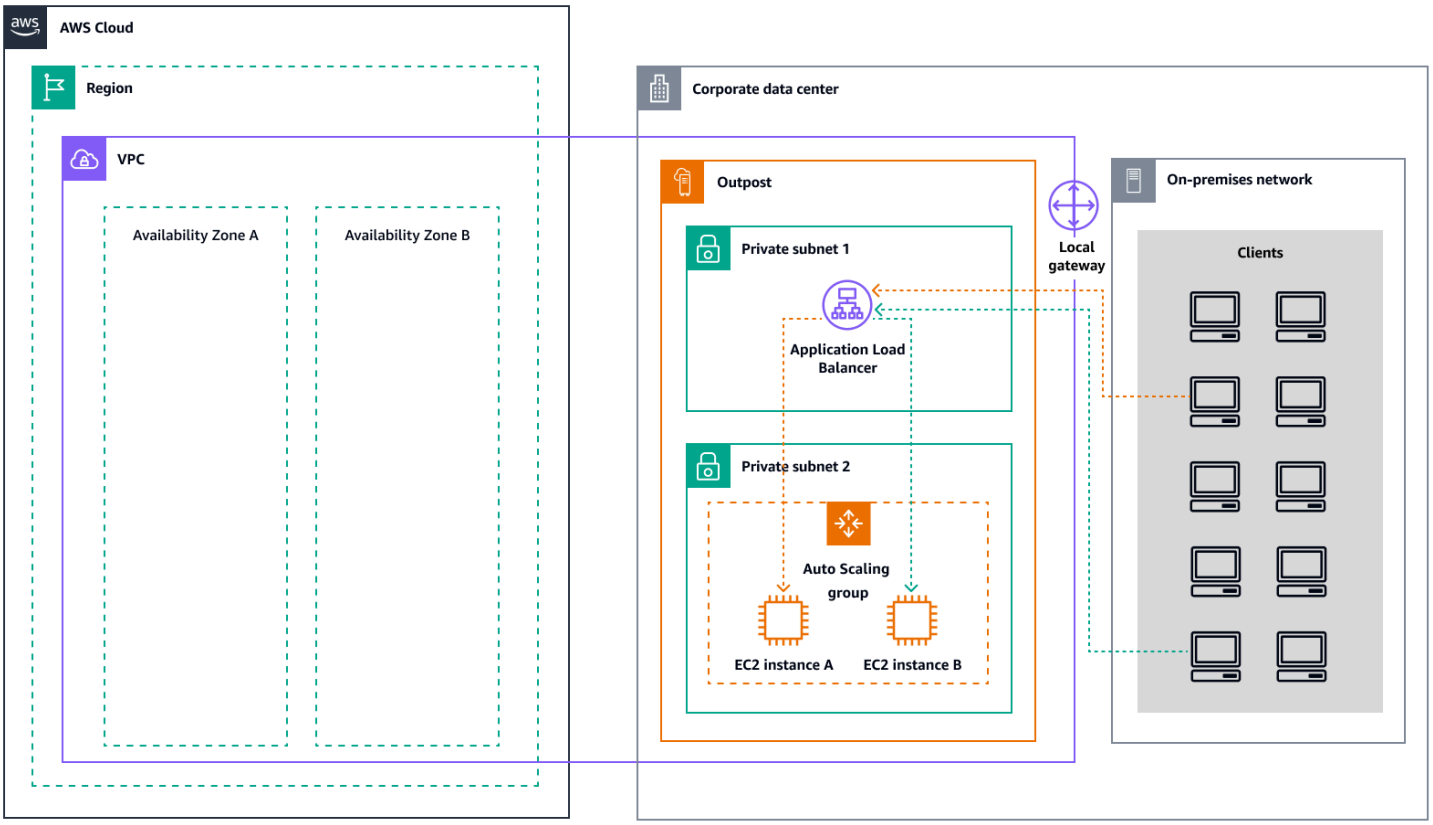


Failover-Mechanismen

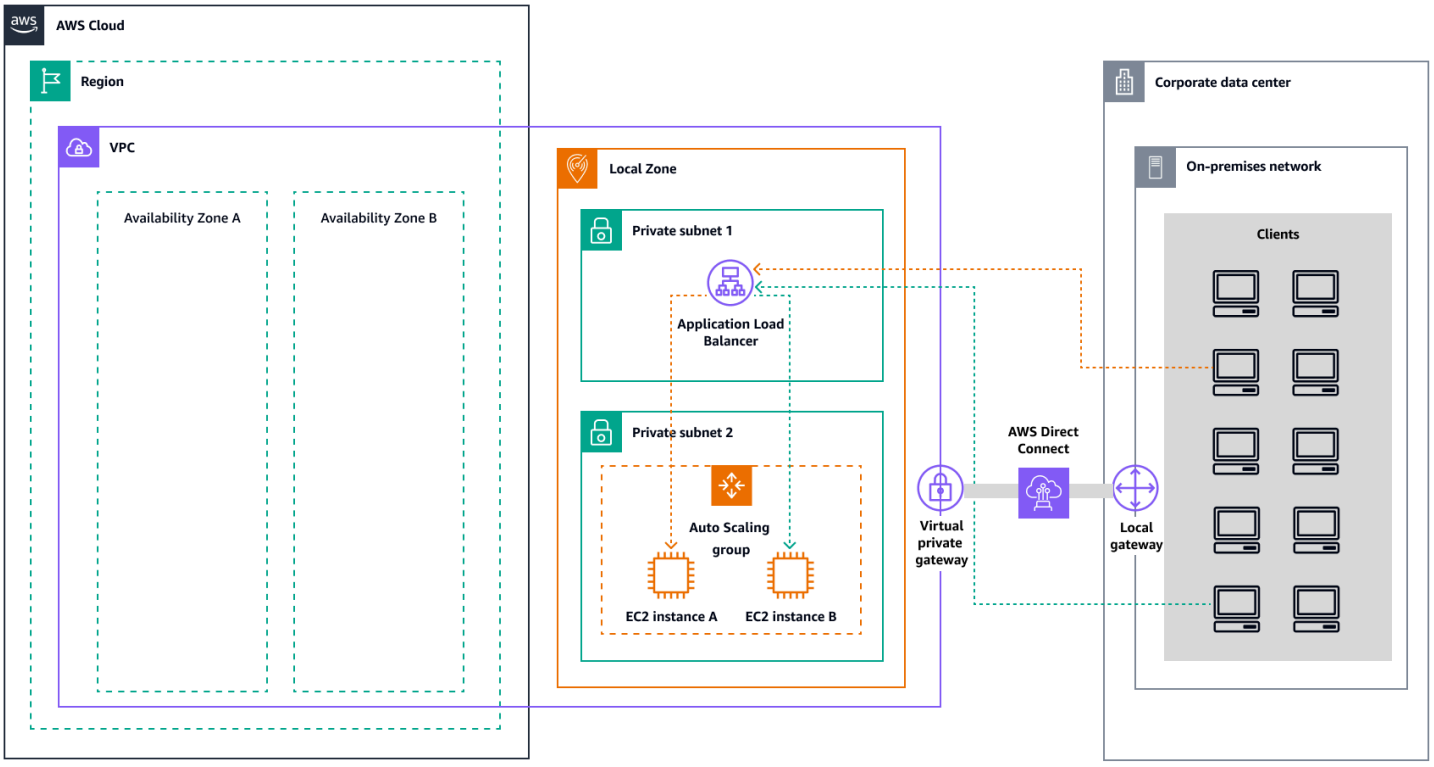
Lastenausgleich und automatische Skalierung

Elastic Load Balancing (ELB) verteilt Ihren eingehenden Anwendungsdatenverkehr automatisch auf alle EC2 Instances, die Sie ausführen. ELB hilft bei der Verwaltung eingehender Anfragen, indem es den Datenverkehr optimal weiterleitet, sodass keine einzelne Instanz überlastet wird. Um ELB mit Ihrer Amazon EC2 Auto Scaling Scaling-Gruppe zu verwenden, fügen Sie den Load Balancer Ihrer Auto Scaling Scaling-Gruppe hinzu. Dadurch wird die Gruppe beim Load Balancer registriert, der als zentrale Anlaufstelle für den gesamten eingehenden Webverkehr zu Ihrer Gruppe fungiert. Wenn Sie ELB mit Ihrer Auto Scaling Scaling-Gruppe verwenden, ist es nicht erforderlich, einzelne EC2 Instances beim Load Balancer zu registrieren. Instances, die von Ihrer Auto-Scaling-Gruppe gestartet werden, werden automatisch beim Load Balancer registriert. Ebenso werden Instances, die von Ihrer Auto Scaling Scaling-Gruppe beendet wurden, automatisch vom Load Balancer abgemeldet. Nachdem Sie Ihrer Auto Scaling Scaling-Gruppe einen Load Balancer hinzugefügt haben, können Sie Ihre Gruppe so konfigurieren, dass ELB-Metriken (wie die Anzahl der Application Load Balancer Balancer-Anfragen pro Ziel) verwendet werden, um die Anzahl der Instances in der Gruppe bei schwankendem Bedarf zu skalieren. Optional können Sie ELB-Zustandsprüfungen zu Ihrer Auto Scaling-Gruppe hinzufügen, sodass Amazon EC2 Auto Scaling fehlerhafte Instances anhand dieser Zustandsprüfungen identifizieren und ersetzen kann. Sie können auch einen CloudWatch Amazon-Alarm erstellen, der Sie benachrichtigt, wenn die Anzahl gesunder Hosts der Zielgruppe niedriger als zulässig ist.

Das folgende Diagramm zeigt, wie ein Application Load Balancer Workloads auf Amazon EC2 in verwaltet. AWS Outposts



Das folgende Diagramm zeigt eine ähnliche Architektur für Amazon EC2 in Local Zones.

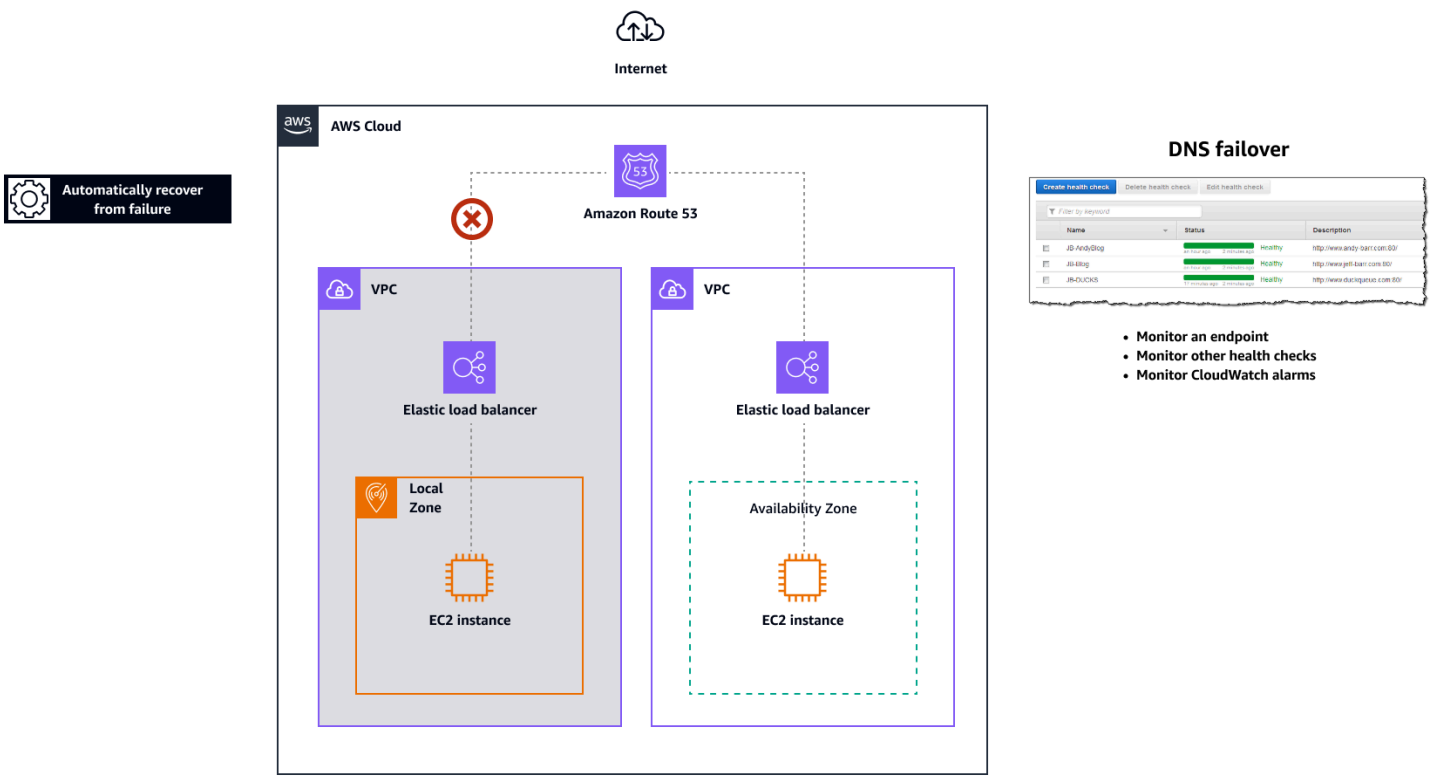


> **Note**
>
> Application Load Balancer sind sowohl in lokalen Zonen als auch AWS Outposts in Local Zones verfügbar. Um jedoch einen Application Load Balancer in zu verwenden AWS Outposts, müssen Sie die EC2 Amazon-Kapazität so dimensionieren, dass sie die Skalierbarkeit bietet, die der Load Balancer benötigt. Weitere Informationen zur Dimensionierung eines Load Balancers finden Sie im AWS Outposts AWS Blogbeitrag Configuring an Application Load Balancer on. AWS Outposts

Amazon Route 53 für DNS-Failover

Wenn mehrere Ressourcen dieselbe Funktion ausführen, z. B. mehrere HTTP- oder Mail-Server, können Sie Amazon Route 53 so konfigurieren, dass der Zustand Ihrer Ressourcen überprüft und DNS-Abfragen beantwortet werden, indem nur die fehlerfreien Ressourcen verwendet werden. Nehmen wir zum Beispiel an, dass Ihre Website,`example.com`, auf zwei Servern gehostet wird. Ein Server befindet sich in einer lokalen Zone und der andere Server in einem Outpost. Sie können Route 53 so konfigurieren, dass der Zustand dieser Server überprüft und DNS-Anfragen beantwortet werden, `example.com` indem nur die Server verwendet werden, die derzeit fehlerfrei sind. Wenn Sie Aliaseinträge verwenden, um den Verkehr an ausgewählte AWS Ressourcen weiterzuleiten, z. B. an ELB-Loadbalancer, können Sie Route 53 so konfigurieren, dass der Zustand der Ressource bewertet wird und der Verkehr nur an fehlerfreie Ressourcen weitergeleitet wird. Wenn Sie einen Aliaseintrag konfigurieren, um den Zustand einer Ressource zu bewerten, müssen Sie keine Integritätsprüfung für diese Ressource erstellen.

Das folgende Diagramm veranschaulicht die Route 53-Failover-Mechanismen.



Hinweise

- Wenn Sie Failover-Datensätze in einer privaten Hosting-Zone erstellen, können Sie eine CloudWatch Metrik erstellen, der Metrik einen Alarm zuordnen und dann eine Integritätsprüfung durchführen, die auf dem Datenstream für den Alarm basiert.
- Um eine Anwendung AWS Outposts mithilfe eines Application Application Load Balancer öffentlich zugänglich zu machen, richten Sie Netzwerkkonfigurationen ein, die Destination Network Address Translation (DNAT) von öffentlich IPs zum vollqualifizierten Domainnamen (FQDN) des Load Balancers ermöglichen, und erstellen Sie eine Route 53-Failover-Regel mit Integritätsprüfungen, die auf die exponierte öffentliche IP verweisen. Diese Kombination gewährleistet einen zuverlässigen öffentlichen Zugriff auf Ihre von OutPosts gehostete Anwendung.

Amazon Route 53 Resolver auf AWS Outposts

Amazon Route 53 Resolverist in Outposts-Racks erhältlich. Es bietet Ihren lokalen Diensten und Anwendungen eine lokale DNS-Auflösung direkt von Outposts aus. Lokale Route 53 Resolver-

Endpunkte ermöglichen auch die DNS-Auflösung zwischen Outposts und Ihrem lokalen DNS-Server. Route 53 Resolver on Outposts trägt dazu bei, die Verfügbarkeit und Leistung Ihrer lokalen Anwendungen zu verbessern.

Einer der typischen Anwendungsfälle für Outposts ist die Bereitstellung von Anwendungen, die einen Zugriff auf lokale Systeme mit geringer Latenz erfordern, wie z. B. Fabrikausrüstung, Hochfrequenz-Handelsanwendungen und medizinische Diagnosesysteme.

Wenn Sie sich für die Verwendung lokaler Route 53-Resolver auf Outposts entscheiden, profitieren Anwendungen und Dienste weiterhin von der lokalen DNS-Auflösung, um andere Dienste zu erkennen, auch wenn die Konnektivität zu einem übergeordneten Element unterbrochen AWS-Region wird. Lokale Resolver tragen auch dazu bei, die Latenz bei DNS-Auflösungen zu reduzieren, da die Abfrageergebnisse zwischengespeichert und lokal von den Outposts aus bereitgestellt werden, wodurch unnötige Roundtrips zum übergeordneten Objekt vermieden werden. AWS-Region Alle DNS-Auflösungen für Anwendungen in Outposts VPCs , die privates DNS verwenden, werden lokal bereitgestellt.

Dieser Start aktiviert nicht nur lokale Resolver, sondern auch lokale Resolver-Endpunkte. Mit ausgehenden Route 53 Resolver-Endpunkten können Route 53-Resolver DNS-Abfragen an von Ihnen verwaltete DNS-Resolver weiterleiten, z. B. in Ihrem lokalen Netzwerk. Im Gegensatz dazu leiten eingehende Route 53 Resolver-Endpunkte die DNS-Abfragen, die sie von außerhalb der VPC erhalten, an den Resolver weiter, der auf Outposts ausgeführt wird. Es ermöglicht Ihnen, DNS-Abfragen für Dienste, die auf einer privaten Outposts-VPC bereitgestellt werden, von außerhalb dieser VPC zu senden. Weitere Informationen zu eingehenden und ausgehenden Endpunkten finden Sie in der Route 53-Dokumentation unter Auflösen von DNS-Abfragen zwischen VPCs und Ihrem Netzwerk.

Kapazitätsplanung am Netzwerkrand

In der Kapazitätsplanungsphase werden die vCPU-, Arbeitsspeicher- und Speicheranforderungen für die Bereitstellung Ihrer Architektur erfasst. Im Bereich der Kostenoptimierung des AWS Well-Architected Framework ist die richtige Dimensionierung ein fortlaufender Prozess, der mit der Planung beginnt. Sie können AWS Tools verwenden, um Optimierungen auf der Grundlage des internen Ressourcenverbrauchs zu definieren. AWS

Die Edge-Kapazitätsplanung in Local Zones ist dieselbe wie in AWS-Regionen. Sie sollten sicherstellen, dass Ihre Instances in jeder lokalen Zone verfügbar sind, da sich einige Instance-Typen von den Typen in unterscheiden können AWS-Regionen. Für Outposts sollten Sie die

Kapazität auf der Grundlage Ihrer Workload-Anforderungen planen. Outposts werden mit einer festen Anzahl von Instanzen pro Host eingerichtet und können nach Bedarf neu aufgeteilt werden. Wenn für Ihre Workloads freie Kapazitäten erforderlich sind, sollten Sie dies bei der Planung Ihres Kapazitätsbedarfs berücksichtigen.

Kapazitätsplanung auf Outposts

AWS Outposts Die Kapazitätsplanung erfordert spezifische Eingaben für die Anpassung an die Region sowie bereichsspezifische Faktoren, die sich auf die Verfügbarkeit, Leistung und das Wachstum von Anwendungen auswirken. Ausführliche Hinweise finden Sie unter Kapazitätsplanung im AWS Whitepaper AWS Outposts High Availability Design and Architecture Considerations.

Kapazitätsplanung für Local Zones

Eine lokale Zone ist eine Erweiterung einer Zone AWS-Region , die sich geografisch in der Nähe Ihrer Benutzer befindet. Ressourcen, die in einer lokalen Zone erstellt werden, können lokalen Benutzern eine Kommunikation mit sehr geringer Latenz ermöglichen. Informationen zum Aktivieren einer lokalen Zone in Ihrer AWS-Konto finden Sie unter Erste Schritte mit AWS Lokale Zonen in der AWS Dokumentation. In jeder lokalen Zone stehen unterschiedliche Steckplätze für EC2 Instance-Familien zur Verfügung. Überprüfen Sie die in jeder lokalen Zone verfügbaren Instanzen, bevor Sie sie verwenden. Führen Sie den folgenden AWS CLI Befehl aus, um die verfügbaren EC2 Instances zu überprüfen:

```
aws ec2 describe-instance-type-offerings \
--location-type "availability-zone" \
--filters Name=location,Values=<local-zone-name>
```

Erwartete Ausgabe:

```
{
  "InstanceTypeOfferings": [
      {
          "InstanceType": "m5.2xlarge",
          "LocationType": "availability-zone",
          "Location": "<local-zone-name>"
      },
      {
          "InstanceType": "t3.micro",
          "LocationType": "availability-zone",
```

```
            "Location": "local.zone-name"
        },
        ...
    ]
}
```

Edge-Infrastrukturmanagement

AWS bietet vollständig verwaltete Dienste, die AWS Infrastruktur APIs, Dienste und Tools näher an Ihre Endbenutzer und Rechenzentren ausdehnen. Die Dienste, die in Outposts und Local Zones verfügbar sind, sind dieselben wie in AWS-Regionen, sodass Sie diese Dienste mit derselben AWS Konsole verwalten können, AWS CLI, oder AWS APIs. Informationen zu den unterstützten Diensten finden Sie in der Tabelle AWS Outposts mit dem Funktionsvergleich und den AWS Lokale Zonen Funktionen.

Bereitstellung von Diensten am Netzwerkrand

Sie können die verfügbaren Dienste in Local Zones und Outposts auf die gleiche Weise konfigurieren, wie Sie sie konfigurieren AWS-Regionen: mit der AWS Konsole, AWS CLI, oder AWS APIs. Der Hauptunterschied zwischen regionalen Bereitstellungen und Edge-Bereitstellungen besteht in den Subnetzen, in denen Ressourcen bereitgestellt werden. Im Abschnitt Networking at the Edge wurde beschrieben, wie Subnetze in Outposts und Local Zones bereitgestellt werden. Nachdem Sie die Edge-Subnetze identifiziert haben, verwenden Sie die Edge-Subnetz-ID als Parameter, um den Dienst in Outposts oder Local Zones bereitzustellen. Die folgenden Abschnitte enthalten Beispiele für die Bereitstellung von Edge-Diensten.

Amazon EC2 an der Peripherie

Im folgenden `run-instances` Beispiel wird eine einzelne Instance des Typs `m5.2xlarge` im Edge-Subnetz für die aktuelle Region gestartet. Das key pair ist optional, wenn Sie nicht planen, eine Verbindung zu Ihrer Instance mithilfe von SSH unter Linux oder des Remote Desktop Protocol (RDP) unter Windows herzustellen.

```
aws ec2 run-instances \
    --image-id ami-id \
    --instance-type m5.2xlarge \
    --subnet-id <subnet-edge-id> \
    --key-name MyKeyPair
```

Application Load Balancers am Edge

Im folgenden `create-load-balancer` Beispiel wird ein interner Application Load Balancer erstellt und die Local Zones oder Outposts für die angegebenen Subnetze aktiviert.

```
aws elbv2 create-load-balancer \
    --name my-internal-load-balancer \
    --scheme internal \
    --subnets <subnet-edge-id>
```

Um einen mit dem Internet verbundenen Application Load Balancer in einem Subnetz auf einem Outpost bereitzustellen, setzen Sie das `internet-facing` Flag in der `--scheme` Option und geben eine CoIP-Pool-ID an, wie in diesem Beispiel gezeigt:

```
aws elbv2 create-load-balancer \
    --name my-internal-load-balancer \
    --scheme internet-facing \
    --customer-owned-ipv4-pool <coip-pool-id>
    --subnets <subnet-edge-id>
```

Informationen zur Bereitstellung anderer Dienste am Edge finden Sie unter diesen Links:

Service	AWS Outposts	AWS Lokale Zonen
Amazon EKS	Stellen Sie Amazon EKS vor Ort bereit mit AWS Outposts	Starten Sie EKS-Cluster mit niedriger Latenz mit AWS Lokale Zonen
Amazon ECS	Amazon ECS auf AWS Outposts	Amazon ECS-Anwendungen in gemeinsam genutzten Subnetzen, Local Zones und Wellenlängenzonen
Amazon RDS	Amazon RDS auf AWS Outposts	Wählen Sie das Subnetz der lokalen Zone
Amazon S3	Erste Schritte mit Amazon S3 auf Outposts	Nicht verfügbar

Service	AWS Outposts	AWS Lokale Zonen
Amazon ElastiCache	Outposts verwenden mit ElastiCache	Verwenden von Local Zones mit ElastiCache
Amazon EMR	EMR-Cluster auf AWS Outposts	EMR-Cluster auf AWS Lokale Zonen
Amazon FSx	Nicht verfügbar	Wählen Sie das Subnetz der lokalen Zone
AWS Elastic Disaster Recovery	Arbeiten mit und AWS Elastic Disaster RecoveryAWS Outposts	Nicht verfügbar
AWS Application Migration Service	Nicht verfügbar	Wählen Sie das Subnetz der lokalen Zone als Staging-S ubnetz aus

Outposts-spezifische CLI und SDK

AWS Outposts verfügt über zwei Gruppen von Befehlen und dient APIs zum Erstellen eines Serviceauftrags oder zum Bearbeiten der Routing-Tabellen zwischen dem lokalen Gateway und Ihrem lokalen Netzwerk.

Bestellvorgang bei Outposts

Sie können die AWS CLIoder die Outposts verwenden, APIs um eine Außenposts-Website zu erstellen, einen Outposts zu erstellen und eine Outposts-Bestellung zu erstellen. Wir empfehlen Ihnen, während des AWS Outposts Bestellvorgangs mit einem Hybrid-Cloud-Spezialisten zusammenzuarbeiten, um die richtige Auswahl der Ressourcen IDs und die optimale Konfiguration für Ihre Implementierungsanforderungen sicherzustellen. Eine vollständige Liste der Ressourcen-IDs finden Sie auf der Seite mit den Preisen für AWS Outposts Racks.

Verwaltung des lokalen Gateways

Die Verwaltung und der Betrieb des lokalen Gateways (LGW) in Outposts erfordern Kenntnisse der AWS CLI für diese Aufgabe verfügbaren SDK-Befehle. Sie können das AWS CLI und unter anderem

verwenden AWS SDKs , um LGW-Routen zu erstellen und zu ändern. Weitere Informationen zur Verwaltung des LGW finden Sie in diesen Ressourcen:

- AWS CLI für Amazon EC2
- EC2.Kunde im AWS SDK for Python (Boto)
- Ec2Client im AWS SDK für Java

CloudWatch Metriken und Protokolle

AWS-Services Da sie sowohl in Outposts als auch in Local Zones verfügbar sind, werden Metriken und Protokolle auf die gleiche Weise wie in Regionen verwaltet. Amazon CloudWatch bietet Metriken, die der Überwachung von Outposts in den folgenden Dimensionen gewidmet sind:

Dimension	Beschreibung
`Account`	Das Konto oder der Dienst, der die Kapazität nutzt
`InstanceFamily`	Die Instanzfamilie
`InstanceType`	Der Instance-Typ
`OutpostId`	Die ID des Außenpostens
`VolumeType`	Der EBS-Volumetyp
`VirtualInterfaceId`	Die ID des lokalen Gateways oder der virtuellen Service Link-Schnittstelle (VIF)
`VirtualInterfaceGroupId`	Die ID der VIF-Gruppe für die lokale Gateway-VIF

Weitere Informationen finden Sie unter CloudWatch Metriken für Outposts-Racks in der Outposts-Dokumentation.

Ressourcen

AWS Verweise

- Hybrid Cloud mit AWS
- AWS Outposts Benutzerhandbuch für Outposts-Racks
- AWS Lokale Zonen -Benutzerhandbuch
- AWS Outposts Familie
- AWS Lokale Zonen
- Erweitern Sie eine VPC auf eine lokale Zone, eine Wellenlängenzone oder einen Außenposten (Amazon VPC-Dokumentation)
- Linux-Instances in Local Zones (EC2 Amazon-Dokumentation)
- Linux-Instances in Outposts (EC2 Amazon-Dokumentation)
- Beginnen Sie mit der Bereitstellung von Anwendungen mit niedriger Latenz mit AWS Lokale Zonen (Tutorial)

AWS Blog-Beiträge

- Betrieb der AWS Infrastruktur vor Ort mit Amazon EC2
- Entwicklung moderner Anwendungen mit Amazon EKS auf Amazon EC2
- So wählen Sie zwischen CoIP- und direktem VPC-Routing-Modus auf dem Amazon-Rack EC2
- Netzwerk-Switches für Ihren Amazon auswählen EC2
- Pflege einer lokalen Kopie Ihrer Daten in AWS Lokale Zonen
- Amazon ECS auf Amazon EC2
- Verwaltung von Edge-Aware-Service Mesh mit Amazon EKS für AWS Lokale Zonen
- Bereitstellung von lokalem Gateway-Ingress-Routing auf Amazon EC2
- Automatisieren Sie Ihre Workload-Bereitstellungen in AWS Lokale Zonen
- Amazon EC2 in einer AWS Umgebung mit mehreren Konten teilen: Teil 1
- Amazon EC2 in einer AWS Umgebung mit mehreren Konten teilen: Teil 2
- AWS Direct Connect und AWS Lokale Zonen Interoperabilitätsmuster

- Stellen Sie Amazon RDS auf Amazon EC2 mit Multi-AZ-Hochverfügbarkeit bereit

Mitwirkende

Die folgenden Personen haben zu diesem Leitfaden beigetragen.

Verfassen

- Leonardo Solano, Hauptarchitekt für Hybrid-Cloud-Lösungen, AWS
- Len Gomes, Architekt für Partnerlösungen, AWS
- Matt Price, Senior Enterprise Support Engineer, AWS
- Tom Gadomski, Lösungsarchitekt, AWS
- Obed Gutierrez, Lösungsarchitekt, AWS
- Dionysios Kakaletris, Technischer Kundenbetreuer, AWS
- Vamsi Krishna, Hauptspezialistin für Outposts, AWS

Überprüfend

- David Filiatrault, Lieferberater, AWS

Technisches Schreiben

- Handan Selamoglu, Senior Documentation Manager, AWS

Dokumentverlauf

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

Änderung	Beschreibung	Datum
Erste Veröffentlichung	—	10. Juni 2025

AWS Glossar zu präskriptiven Leitlinien

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

Zahlen

7 Rs

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

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

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

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

A

ABAC

Siehe attributbasierte Zugriffskontrolle.

abstrahierte Dienste

Siehe Managed Services.

ACID

Siehe Atomarität, Konsistenz, Isolierung und Haltbarkeit.

Aktiv-Aktiv-Migration

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

Aktiv-Passiv-Migration

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

Aggregatfunktion

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

AI

Siehe künstliche Intelligenz.

AIOps

Siehe Operationen im Bereich künstliche Intelligenz.

Anonymisierung

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

Anti-Muster

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

Anwendungssteuerung

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

Anwendungsportfolio

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

künstliche Intelligenz (KI)

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

Operationen mit künstlicher Intelligenz (AIOps)

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

Asymmetrische Verschlüsselung

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

Atomizität, Konsistenz, Isolierung, Haltbarkeit (ACID)

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

Attributbasierte Zugriffskontrolle (ABAC)

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

autoritative Datenquelle

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

Verfügbarkeitszone

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

Cloud-Einführung vorzubereiten. Weitere Informationen finden Sie auf der AWS -CAF-Webseite und dem AWS -CAF-Whitepaper.

AWS Workload-Qualifizierungsrahmen (AWS WQF)

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

B

schlechter Bot

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

BCP

Siehe Planung der Geschäftskontinuität.

Verhaltensdiagramm

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

Big-Endian-System

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

Binäre Klassifikation

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

Bloom-Filter

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

Blau/Grün-Bereitstellung

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

Bot

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

Botnetz

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

branch

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

Zugang durch Glasbruch

Unter außergewöhnlichen Umständen und im Rahmen eines genehmigten Verfahrens ist dies eine schnelle Methode für einen Benutzer, auf einen Bereich zuzugreifen AWS-Konto , für den er in der Regel 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 stress, und deren Reaktion zu bewerten.

CI/CD

Siehe Continuous Integration und Continuous Delivery.

Klassifizierung

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

clientseitige Verschlüsselung

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

Cloud-Exzellenzzentrum (CCoE)

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

Cloud Computing

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

Cloud-Betriebsmodell

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

Phasen der Einführung der Cloud

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

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

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

CMDB

Siehe Datenbank für das Konfigurationsmanagement.

Code-Repository

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

Kalter Cache

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

Kalte Daten

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

Computer Vision (CV)

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

Drift in der Konfiguration

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

Verwaltung der Datenbankkonfiguration (CMDB)

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

Konformitätspaket

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

Kontinuierliche Bereitstellung und kontinuierliche Integration (CI/CD)

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

CV

Siehe Computer Vision.

D

Daten im Ruhezustand

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

Datenklassifizierung

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

Datendrift

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

Daten während der Übertragung

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

Datennetz

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

Datenminimierung

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

Datenperimeter

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

Vorverarbeitung der Daten

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

Herkunft der Daten

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

betroffene Person

Eine Person, deren Daten gesammelt und verarbeitet werden.

Data Warehouse

Ein Datenverwaltungssystem, das Business Intelligence wie Analysen unterstützt. Data Warehouses enthalten in der Regel große Mengen 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 ein Malware-Angriff.

Disaster Recovery (DR)

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

DML

Siehe Sprache zur Datenbankmanipulation.

Domainorientiertes Design

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

DR

Siehe Disaster Recovery.

Erkennung von Driften

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

DVSM

Siehe Abbildung des Wertstroms in der Entwicklung.

E

EDA

Siehe explorative Datenanalyse.

EDI

Siehe elektronischer Datenaustausch.

Edge-Computing

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

elektronischer Datenaustausch (EDI)

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

Verschlüsselung

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

Verschlüsselungsschlüssel

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

Endianismus

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

Endpunkt

Siehe Service-Endpunkt.

Endpunkt-Services

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

Unternehmensressourcenplanung (ERP)

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

Envelope-Verschlüsselung

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

Umgebung

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

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

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

Epics

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

ERP

Siehe Enterprise Resource Planning.

Explorative Datenanalyse (EDA)

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

F

Faktentabelle

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

schnell scheitern

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

Grenze zur Fehlerisolierung

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

Feature-Zweig

Siehe Zweig.

Features

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

Bedeutung der Feature

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

Featuretransformation

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

Eingabeaufforderung mit wenigen Klicks

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

FGAC

Siehe detaillierte Zugriffskontrolle.

Feinkörnige Zugriffskontrolle (FGAC)

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

Flash-Cut-Migration

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

FM

Siehe Fundamentmodell.

Fundamentmodell (FM)

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

G

generative KI

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

Geoblocking

Siehe geografische Einschränkungen.

Geografische Einschränkungen (Geoblocking)

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

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

Gitflow-Workflow

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

goldenes Bild

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

Greenfield-Strategie

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

Integritätsschutz

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

H

HEKTAR

Siehe Hochverfügbarkeit.

Heterogene Datenbankmigration

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

hohe Verfügbarkeit (HA)

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

historische Modernisierung

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

Daten zurückhalten

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

Homogene Datenbankmigration

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

heiße Daten

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

Hotfix

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

Hypercare-Phase

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

I

IaC

Sehen Sie sich Infrastruktur als Code an.

Identitätsbasierte Richtlinie

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

Leerlaufanwendung

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

IIoT

Siehe Industrielles Internet der Dinge.

unveränderliche Infrastruktur

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

Eingehende (ingress) VPC

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

Inkrementelle Migration

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

Industrie 4.0

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

Infrastruktur

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

Infrastructure as Code (IaC)

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

industrielles Internet der Dinge (T) IIo

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

Inspektions-VPC

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

Internet der Dinge (IoT)

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

Interpretierbarkeit

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

IoT

Siehe Internet der Dinge.

IT information library (ITIL, IT-Informationsbibliothek)

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

T service management (ITSM, IT-Servicemanagement)

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

BIS

Siehe IT-Informationsbibliothek.

ITSM

Siehe IT-Servicemanagement.

L

Labelbasierte Zugangskontrolle (LBAC)

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

Landing Zone

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

großes Sprachmodell (LLM)

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

Große Migration

: Eine Migration von 300 oder mehr Servern.

SCHWARZ

: Siehe Labelbasierte Zugriffskontrolle.

Geringste Berechtigung

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

Lift and Shift

: Siehe 7 Rs.

Little-Endian-System

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

LLM

Siehe großes Sprachmodell.

Niedrigere Umgebungen

Siehe Umgebung.

M

Machine Learning (ML)

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

Hauptzweig

Siehe Filiale.

Malware

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

verwaltete Dienste

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

Manufacturing Execution System (MES)

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

Microservices-Architekturen

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

Migration Acceleration Program (MAP)

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

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

Migration in großem Maßstab

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

Migrationsfabrik

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

Migrationsmetadaten

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

Migrationsmuster

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

Migration Portfolio Assessment (MPA)

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

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

Migration Readiness Assessment (MRA)

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

Migrationsstrategie

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

ML

Siehe maschinelles Lernen.

Modernisierung

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

Bewertung der Modernisierungsfähigkeit

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

Monolithische Anwendungen (Monolithen)

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

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

MPA

Siehe Bewertung des Migrationsportfolios.

MQTT

Siehe Message Queuing-Telemetrietransport.

Mehrklassen-Klassifizierung

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

veränderbare Infrastruktur

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

O

OAC

Siehe Origin Access Control.

EICHE

Siehe Zugriffsidentität von Origin.

COM

Siehe organisatorisches Change-Management.

Offline-Migration

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

OI

Siehe Betriebsintegration.

OLA

Siehe Vereinbarung auf operativer Ebene.

Online-Migration

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

OPC-UA

Siehe Open Process Communications — Unified Architecture.

Offene Prozesskommunikation — Einheitliche Architektur (OPC-UA)

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

Vereinbarung auf Betriebsebene (OLA)

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

Überprüfung der Betriebsbereitschaft (ORR)

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

Betriebstechnologie (OT)

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

Betriebsintegration (OI)

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

Organisationspfad

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

Organisatorisches Veränderungsmanagement (OCM)

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

Ursprungszugriffskontrolle (OAC)

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

Ursprungszugriffsidentität (OAI)

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

ORR

Weitere Informationen finden Sie unter Überprüfung der Betriebsbereitschaft.

NICHT

Siehe Betriebstechnologie.

Ausgehende (egress) VPC

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

P

Berechtigungsgrenze

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

persönlich identifizierbare Informationen (PII)

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

Personenbezogene Daten

Siehe persönlich identifizierbare Informationen.

Playbook

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

PLC

Siehe programmierbare Logiksteuerung.

PLM

Siehe Produktlebenszyklusmanagement.

policy

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

Polyglotte Beharrlichkeit

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

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

Privat gehostete Zonen

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

proaktive Steuerung

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

Produktlebenszyklusmanagement (PLM)

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

Produktionsumgebung

Siehe Umgebung.

Speicherprogrammierbare Steuerung (SPS)

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

schnelle Verkettung

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

Pseudonymisierung

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

publish/subscribe (pub/sub)

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

Q

Abfrageplan

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

Abfrageplanregression

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

R

RACI-Matrix

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

LAPPEN

Siehe Erweiterte Generierung beim Abrufen.

Ransomware

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

RASCI-Matrix

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

RCAC

Siehe Zugriffskontrolle für Zeilen und Spalten.

Read Replica

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

neu strukturieren

Siehe 7 Rs.

Recovery Point Objective (RPO)

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

Wiederherstellungszeitziel (RTO)

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

Refaktorierung

Siehe 7 Rs.

Region

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

Regression

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

rehosten

Siehe 7 Rs.

Veröffentlichung

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

umziehen

Siehe 7 Rs.

neue Plattform

Siehe 7 Rs.

Rückkauf

Siehe 7 Rs.

Ausfallsicherheit

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

Ressourcenbasierte Richtlinie

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

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

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

Reaktive Kontrolle

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

Beibehaltung

Siehe 7 Rs.

zurückziehen

Siehe 7 Rs.

Retrieval Augmented Generation (RAG)

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

Drehung

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

Zugriffskontrolle für Zeilen und Spalten (RCAC)

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

RPO

Siehe Recovery Point Objective.

RTO

Siehe Ziel 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 Benutzeranmeldedaten, die Sie in verschlüsselter Form speichern. Es besteht aus dem geheimen Wert und seinen Metadaten. Der geheime Wert kann binär, eine einzelne Zeichenfolge oder mehrere Zeichenketten sein. Weitere Informationen finden Sie unter Was ist in einem Secrets Manager Manager-Geheimnis? in der Secrets Manager Manager-Dokumentation.

Sicherheit durch Design

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

Sicherheitskontrolle

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

Härtung der Sicherheit

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

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

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

Automatisierung von Sicherheitsreaktionen

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

Serverseitige Verschlüsselung

Verschlüsselung von Daten am Zielort durch AWS-Service den Empfänger.

Service-Kontrollrichtlinie (SCP)

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

Service-Endpunkt

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

Service Level Agreement (SLA)

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

Service-Level-Indikator (SLI)

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

Service-Level-Ziel (SLO)

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

Modell der geteilten Verantwortung

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

SIEM

Siehe Sicherheitsinformations- und Event-Management-System.

Single Point of Failure (SPOF)

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

SLA

Siehe Service Level Agreement.

SLI

Siehe Service-Level-Indikator.

ALSO

Siehe Service-Level-Ziel.

split-and-seed Modell

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

SPOTTEN

Siehe Single Point of Failure.

Sternschema

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

Strangler-Fig-Muster

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

Subnetz

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

Aufsichtskontrolle und Datenerfassung (SCADA)

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

Symmetrische Verschlüsselung

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

synthetisches Testen

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

Systemaufforderung

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

T

tags

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

Zielvariable

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

Aufgabenliste

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

Testumgebungen

Siehe Umgebung.

Training

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

Transit-Gateway

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

Stammbasierter Workflow

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

Vertrauenswürdiger Zugriff

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

Optimieren

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

Zwei-Pizzen-Team

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

U

Unsicherheit

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

undifferenzierte Aufgaben

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

höhere Umgebungen

Siehe Umgebung.

V

Vacuuming

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

Versionskontrolle

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

VPC-Peering

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

Schwachstelle

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

W

Warmer Cache

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

warme Daten

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

Fensterfunktion

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

Workload

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

Workstream

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

WURM

Mal schreiben, viele lesen.

WQF

Siehe AWS Workload-Qualifizierungsrahmen.

einmal schreiben, viele lesen (WORM)

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

Z

Zero-Day-Exploit

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

Zero-Day-Sicherheitslücke

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

Eingabeaufforderung ohne Angabe von Gründen

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

Zombie-Anwendung

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