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

AWS Prescriptive Guidance

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

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

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

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

Table of Contents

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 Local Zones 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 Local Zones 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 Local Zones 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 einen AWS Unified Operations-Plan verfügen.

AWS Local Zones

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

- Option 1: Eine Direct Connect Verbindung von Ihrem Rechenzentrum zum 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 Virtual Private Network (VPN) - Appliance und der erforderlichen Lizenzierung, um eine softwarebasierte VPN-Appliance auf 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 Tool zur Instanzkapazität ist nur für neue Bestellungen verfügbar.

AWS Local Zones

- Local Zones haben keinen AWS Site-to-Site VPN Endpunkt. Verwenden Sie stattdessen ein softwarebasiertes VPN auf Amazon EC2.
- Local Zones werden nicht unterstützt AWS Transit Gateway. Stellen Sie stattdessen mithilfe einer 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 Local Zones 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 können: 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.

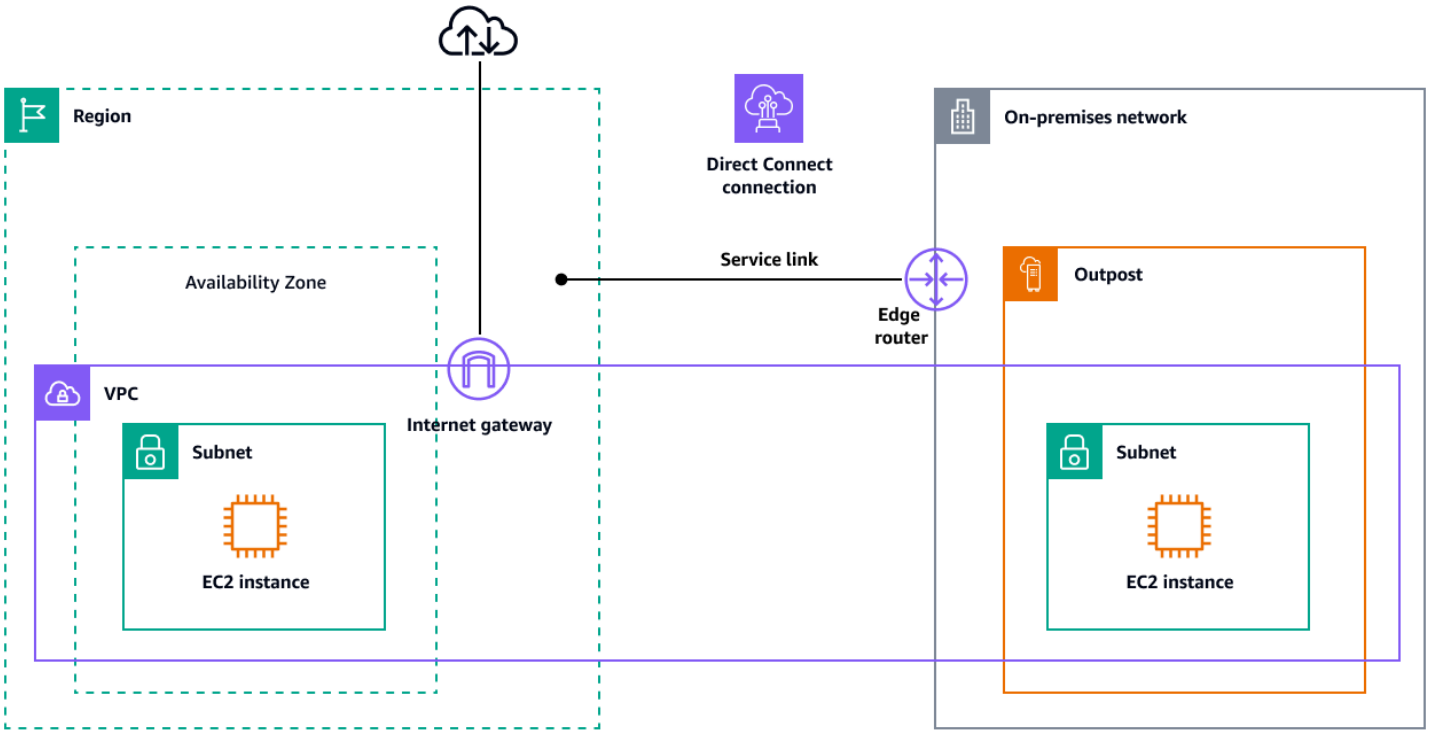
Das folgende Diagramm zeigt eine AWS Architektur, die Outpost- und Local Zone-Subnetze umfasst.

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 Direct Connect öffentliche virtuelle Schnittstelle (öffentliche VIF) oder über eine 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, Amazon EC2 EC2-Instances zu starten, Amazon EBS-Volumes anzuhängen und auf Amazon EKS-, Amazon EMR- und Amazon-Metriken zuzugreifen AWS-Services . CloudWatch 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 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 Koabhängigkeiten 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 und ermöglichen es Ihnen AWS-Region, über dieselben APIs und Toolsets eine nahtlose Verbindung zum gesamten Spektrum der regionalen Dienste herzustellen.

Die folgende Tabelle zeigt die Verbindungsoptionen und die zugehörigen MTUs.

Von	Zu	MTU
Amazon EC2 in der Region	Amazon EC2 in Local Zones	1.300 Byte
Direct Connect	Local Zones	1.468 Byte

Von	Zu	MTU
Internet-Gateway	Local Zones	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.

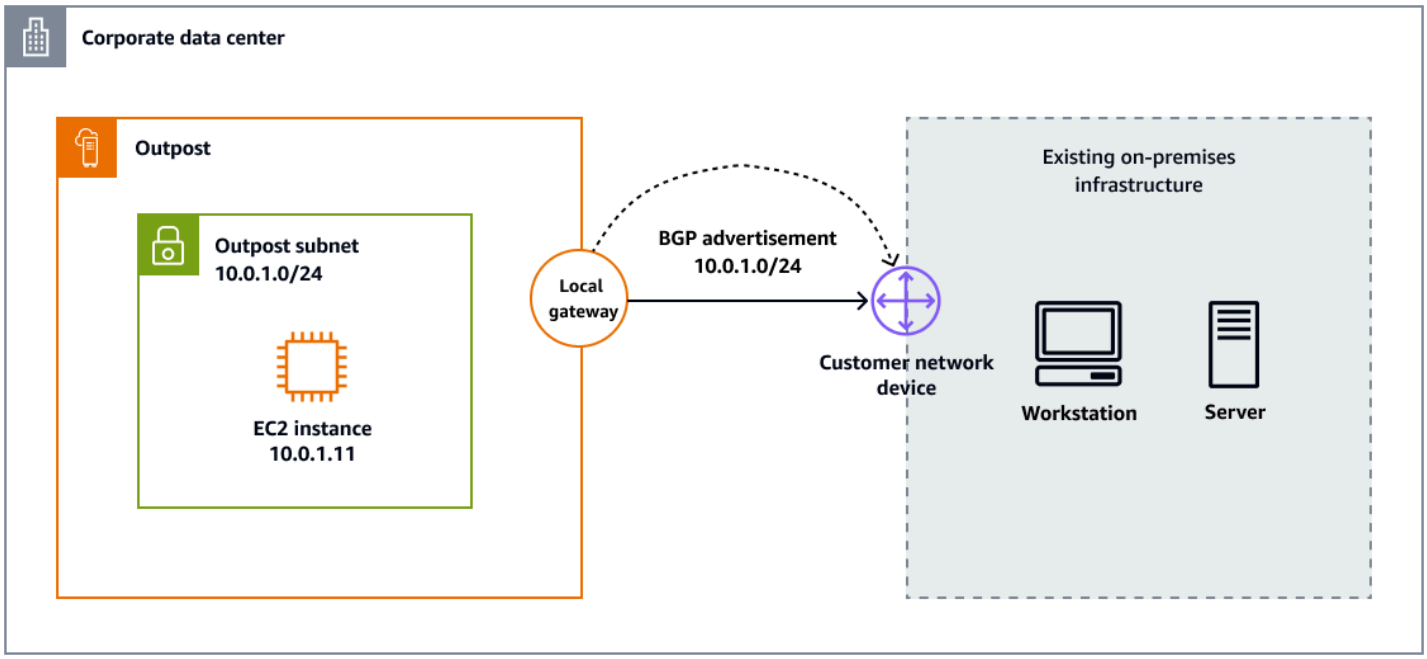
Datenverkehr vom Edge zum lokalen Rechenzentrum

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.

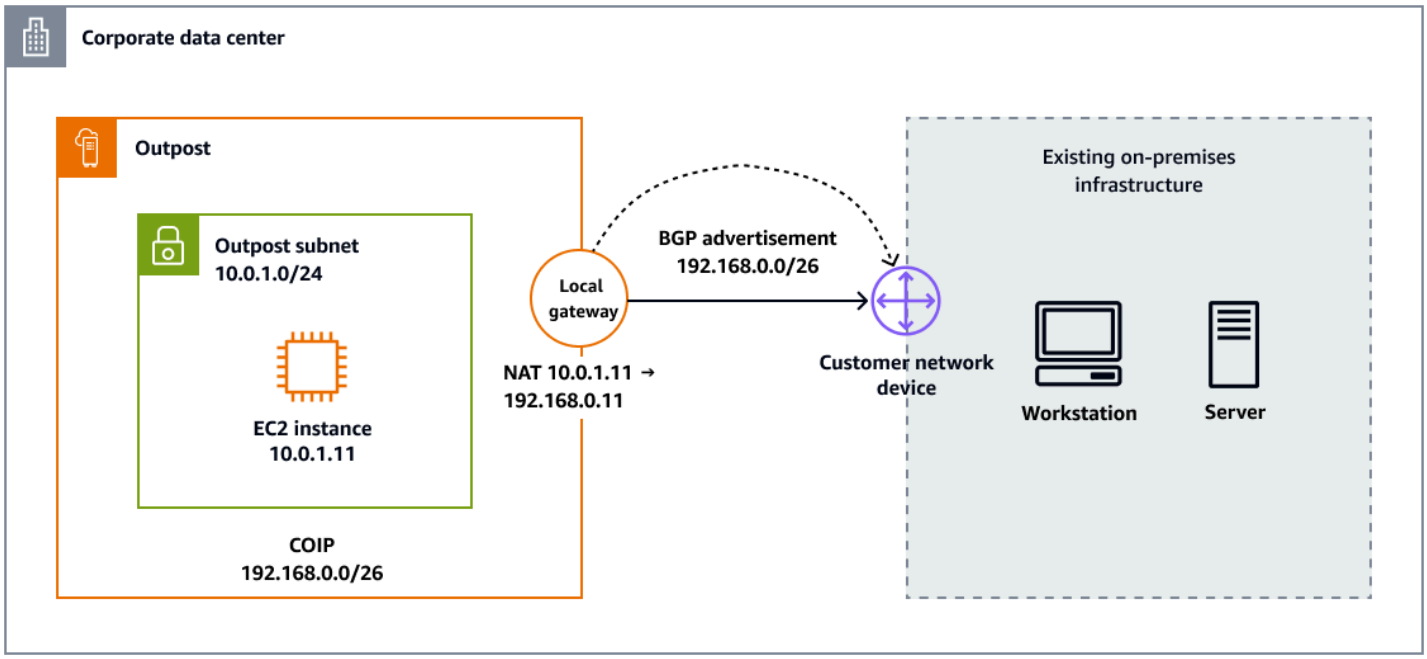
AWS Outposts lokales Gateway

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 auf Ihrem Outpost zuweisen, z. B. EC2-Instances, 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 bekannt gegeben 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 EC2-hosted Amazon-Workload in einer lokalen Zone dem Internet zugänglich zu machen, können Sie die Option Auto-assign Public IP aktivieren, wenn Sie die EC2-Instance starten. 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 Direct Connect

Local Zones werden ebenfalls unterstützt 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 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 eingerichtet werden, die auf Local Zones ausgedehnt werden. Wenn sich die per Peering verbundenen VPCs in derselben lokalen Zone befinden, verbleibt der Datenverkehr innerhalb der lokalen Zone und wird nicht durch die übergeordnete Region geleitet.

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. Third-party Auditoren 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 Local Zones. 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 Local Zones 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

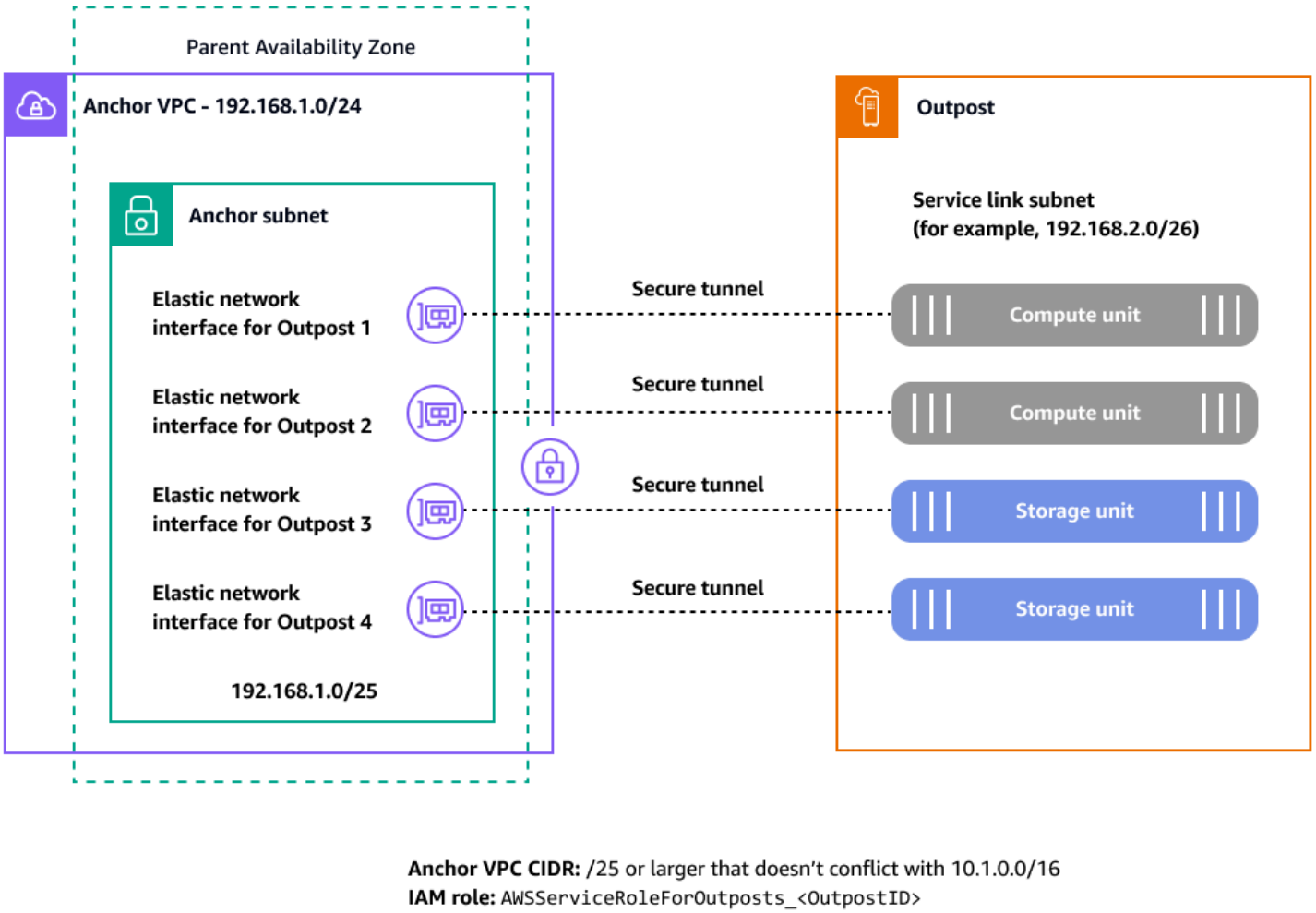
Standardmäßig werden alle in Amazon S3 auf Outposts gespeicherten Daten mithilfe einer serverseitigen Verschlüsselung mit von Amazon S3 verwalteten Verschlüsselungsschlüsseln () SSE-S3 verschlüsselt. Sie können optional serverseitige Verschlüsselung mit vom Kunden bereitgestellten Verschlüsselungsschlüsseln () verwenden. SSE-C Geben Sie zur Verwendung SSE-C einen Verschlüsselungsschlüssel als Teil Ihrer Objekt-API-Anfragen an. Server-side Durch die Verschlüsselung werden nur die Objektdaten, nicht die Objektmetadaten verschlüsselt.

> **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 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.

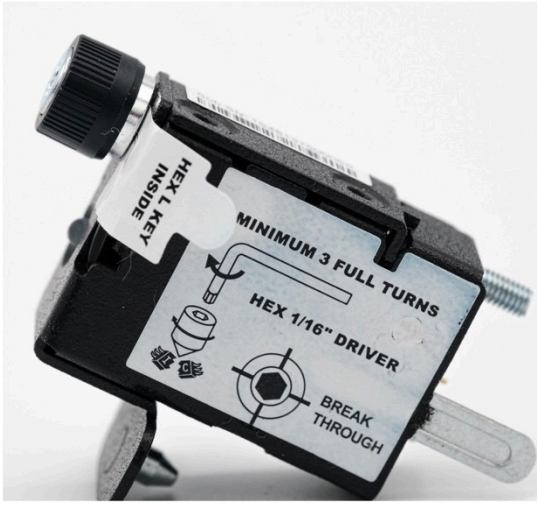
Protocol (Protokoll)	Quellport	Quelladresse	Zielport	Zieladresse
UDP	443	AWS Outposts Servicelink /26	443	AWS Outposts Öffentliche Routen oder Ankerrouten der Region — VPC CIDR

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 Direct Connect PoPs Zugriff auf eine lokale Zone haben, können Sie MAC Security (MACSec) zwischen Ihrem lokalen Router oder Switch und dem Endpunkt aktivieren. Direct Connect Weitere Informationen finden Sie im AWS Blogbeitrag MACSec-Sicherheit zu Verbindungen hinzufügen. Direct Connect

Löschen von Daten

Wenn Sie eine EC2-Instance in 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 ist so konzipiert, dass es einen Mechanismus bietet, der verhindert, dass Ihre Daten von Ihrem Rechenzentrum oder Colocation-Standort aus zugänglich gemacht 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.



Identity and Access Management

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
Identity-based Richtlinien	Ja
Resource-based Richtlinien	Ja*
Richtlinienaktionen	Ja
Richtlinienressourcen	Ja
Richtlinienbedingungsschlüssel (services pezifisch)	Ja
Zugriffssteuerungslisten (ACLs)	Nein

IAM-Funktion	AWS Outposts Unterstützung
Attribute-based Zugriffskontrolle (ABAC) (Tags in Richtlinien)	Ja
Temporäre Anmeldeinformationen	Ja
Prinzipalberechtigungen	Ja
Servicerollen	Nein
Service-linked 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 umfassenden Verteidigungsansatz sowohl für eingehenden als auch für ausgehenden Datenverkehr an. Dazu gehört die Verwendung von Sicherheitsgruppen (Stateful-Inspection-Firewalls), Netzwerk-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-Instances, 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.

Im Folgenden 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 Komponenten, Bibliotheken und extern nutzbaren Dienste, die Sie verwenden, 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 stammen möglicherweise von ISVs und helfen Ihnen beim Aufbau von Inspektionsebenen in Ihrer lokalen Zone, wie im AWS Blogbeitrag Hybride Inspektionsarchitekturen mit beschrieben. AWS Local Zones

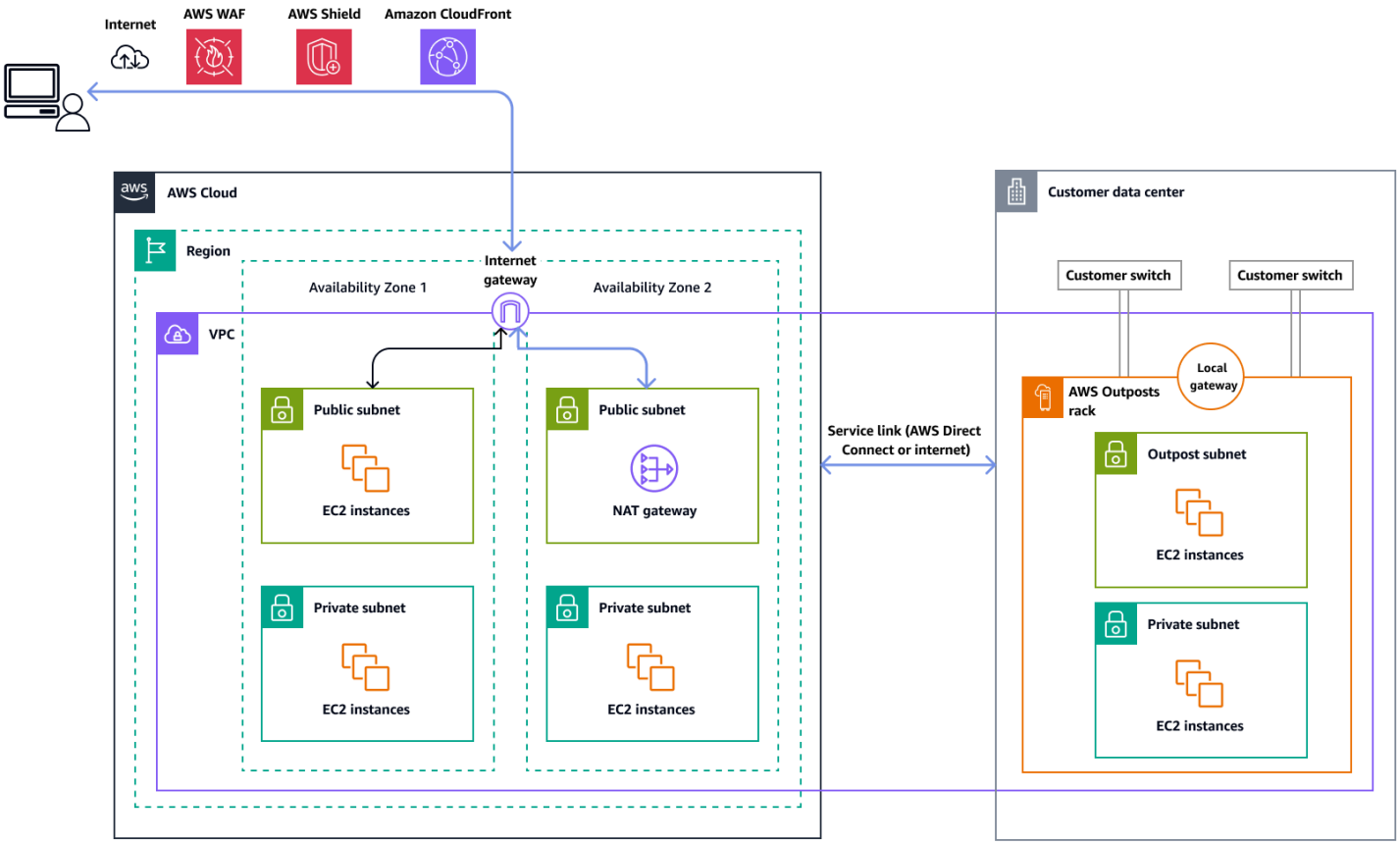
Wenn Sie das lokale Gateway (LGW) verwenden möchten AWS Outposts, um von Ihrem Netzwerk aus auf das Internet zuzugreifen, müssen Sie die benutzerdefinierte Routing-Tabelle ändern, die dem Subnetz zugeordnet ist. AWS Outposts Die Routentabelle muss einen Standardrouteneintrag (0.0.0) haben. 0/0), das den LGW als nächsten Hop verwendet. Sie sind verantwortlich für die Implementierung der verbleibenden Sicherheitskontrollen in Ihrem lokalen Netzwerk, einschließlich Schutzmaßnahmen an der Peripherie 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

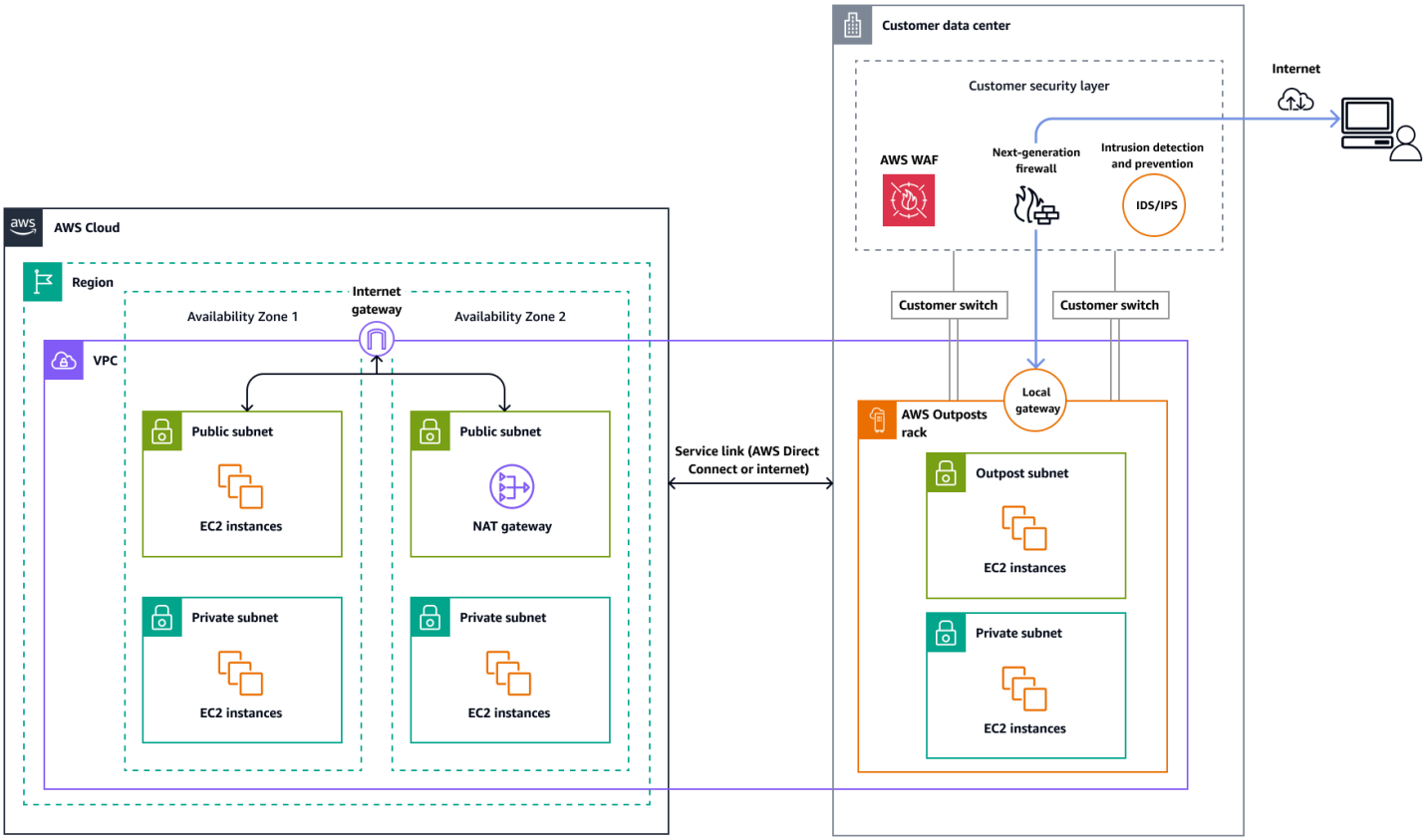


Internetzugang über das Netzwerk Ihres lokalen Rechenzentrums

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 wieder 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 (FSIs) zu erfüllen. Im Folgenden erfahren Sie, wie Sie Guardrails für die Datenresidenz am Netzwerkrand einsetzen können:

- Bewährte Methoden für die Verwaltung der Datenresidenz AWS Local Zones 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 (Framework-Dokumentation)AWS Well-Architected

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 Verbraucher Outpost-Standorte nutzen, VPCs konfigurieren und Instances auf dem freigegebenen Outpost starten und ausführen.

Zu den gemeinsam nutzbaren Ressourcen gehören: AWS Outposts

- Zugewiesene dedizierte Hosts
- Kapazitätsreservierungen
- Customer-owned IP-Adresspools (CoIP)
- Routing-Tabellen für das lokale Gateway
- Outposts

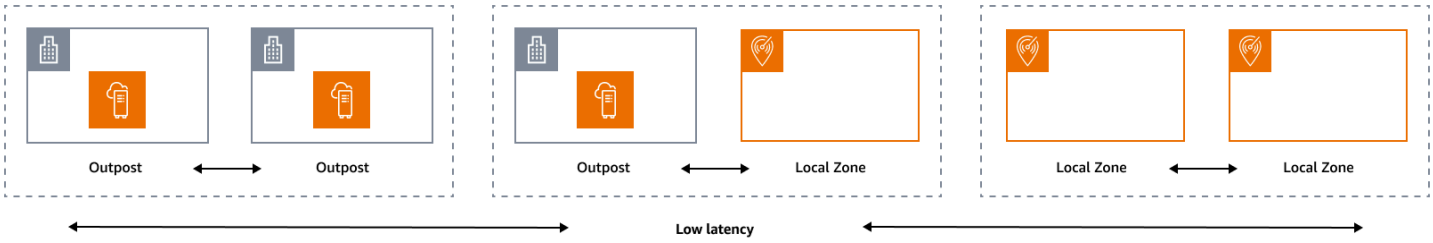
- Amazon S3 on Outposts
- Sites
- Subnets

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 Local Zones 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 robuste 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.

Local Zones

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 einem AWS-Region, sondern in der Nähe von großen Wohn-, Industrie- und IT-Zentren, in denen es heute keine gibt AWS-Region . 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 der Sicht der Kontrollebene. 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:

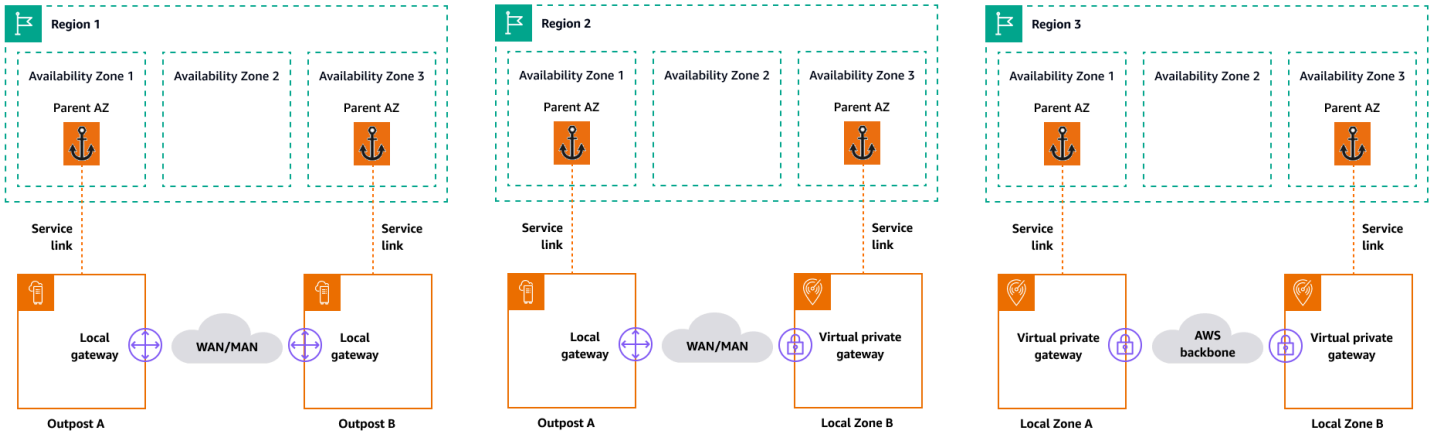
```
aws ec2 describe-availability-zones --zone-ids use1-mia1-az1
```

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.

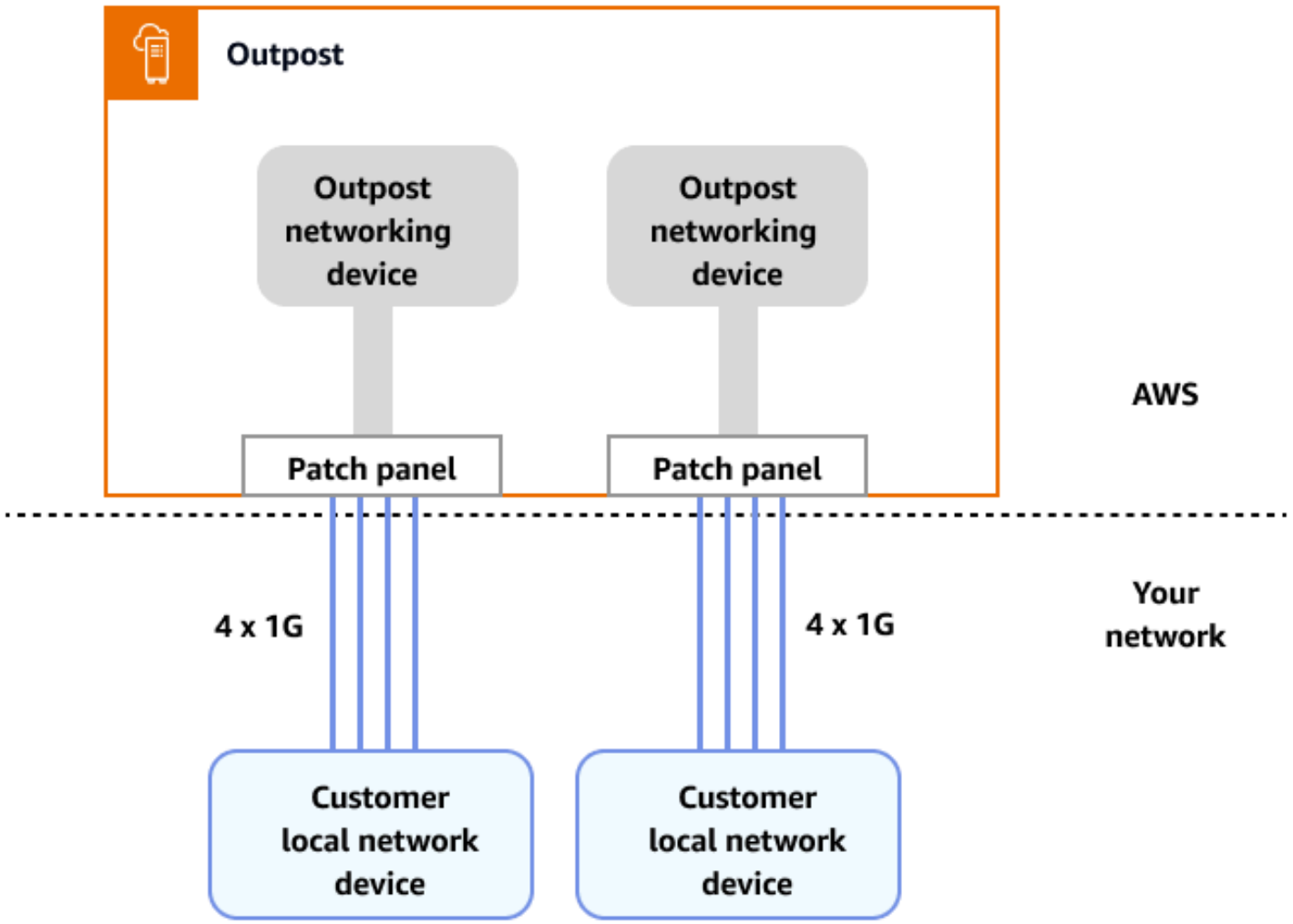
Resilienznetzwerke für Local Zones

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 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 Direct Connect, entsprechen die entsprechenden Resilienzarchitekturen denen für den Zugriff auf AWS-Region, wie in den 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 Direct Connect PoP unmöglich, die aus Gründen der Direct Connect Resilienz empfohlenen Architekturen zu erstellen. Wenn Sie Zugriff auf nur einen einzigen Direct Connect Standort haben oder Ausfallsicherheit benötigen, die über eine einzelne Verbindung hinausgeht, können Sie eine VPN-Appliance auf Amazon EC2 erstellen und Direct Connect, wie im AWS Blogbeitrag Enabling high available connectivity from local to dargestellt und besprochen. AWS Local Zones

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.

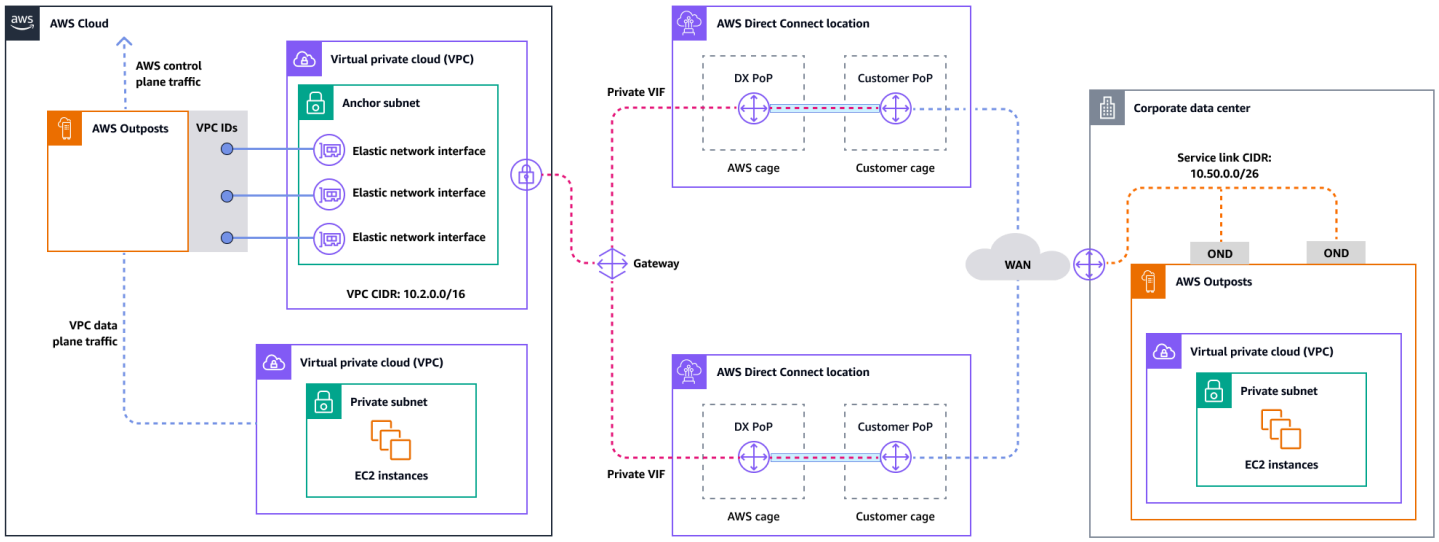
Uplink-Geschwindigkeit	Anzahl der Uplinks
1 Gbit/s	1, 2, 4, 6, oder 8
10 Gbit/s	1, 2, 4, 8, 12, oder 16
40 oder 100 Gbit/s	1, 2, oder 4



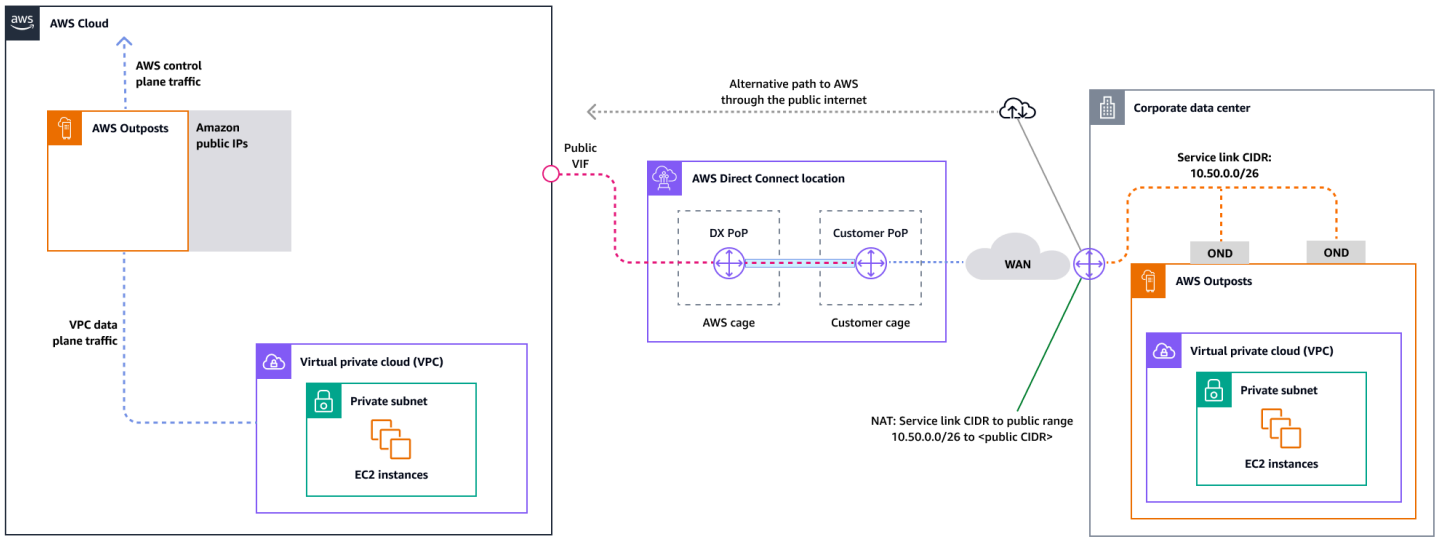
Weitere Informationen zu dieser Konnektivität finden Sie in der AWS Outposts Dokumentation unter Lokale Netzwerkkonnektivität Outposts Outposts-Racks.

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 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 Metriken zugreifen. CloudWatch

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



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



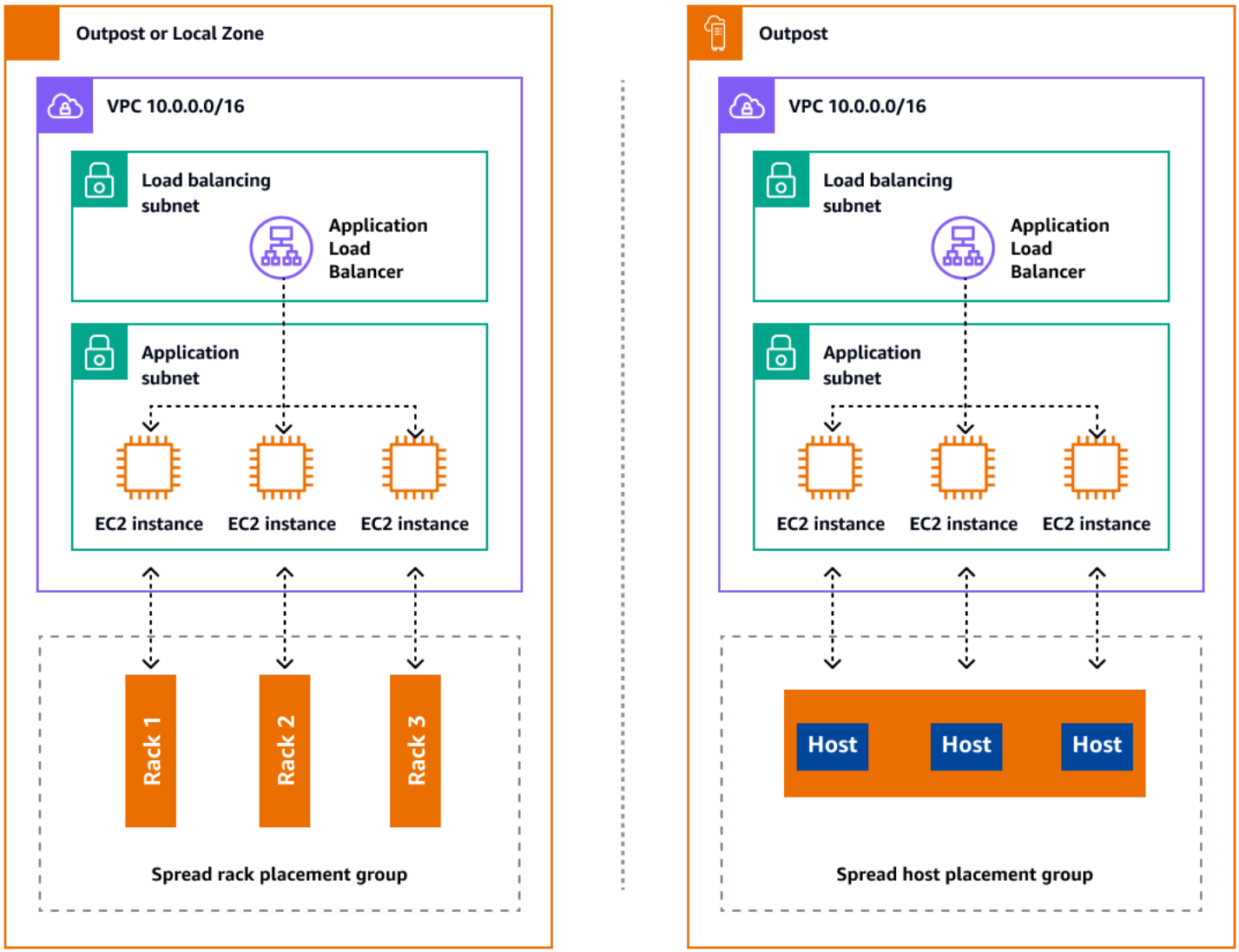
Skalierung Outposts Outposts-Rack-Bereitstellungen mit ACE-Racks

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

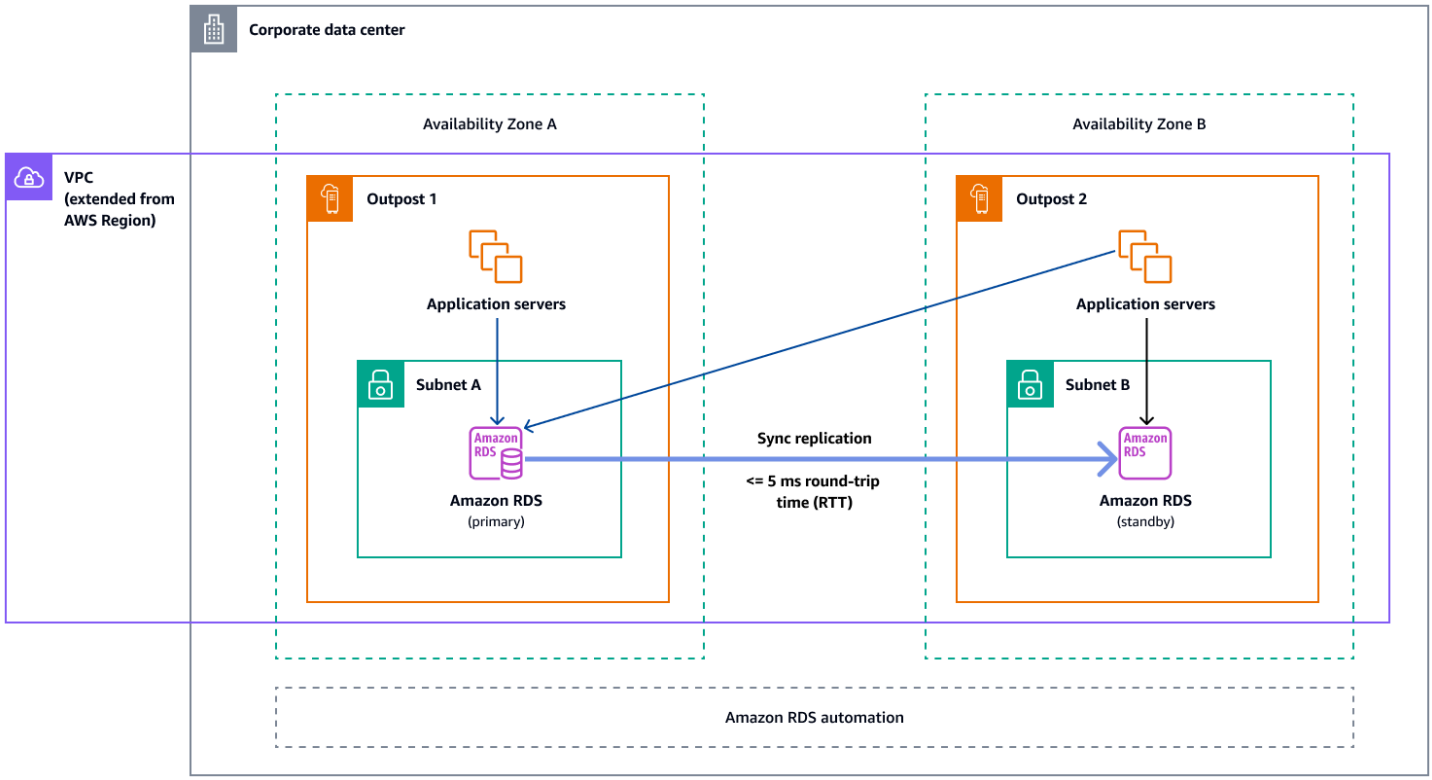
Wenn Sie Multi-AZ Instance-Bereitstellungen auf Outposts verwenden, erstellt Amazon RDS zwei Datenbank-Instances in zwei Outposts. Jeder Outpost läuft auf seiner eigenen physischen Infrastruktur und stellt eine Verbindung zu verschiedenen Availability Zones in einer Region her, um eine hohe Verfügbarkeit 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 auf einem Outpost und repliziert die Daten synchron

auf eine Standby-DB-Instance auf 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 Customer-owned 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 Bereitstellungen nicht unterstützt. Multi-AZ

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

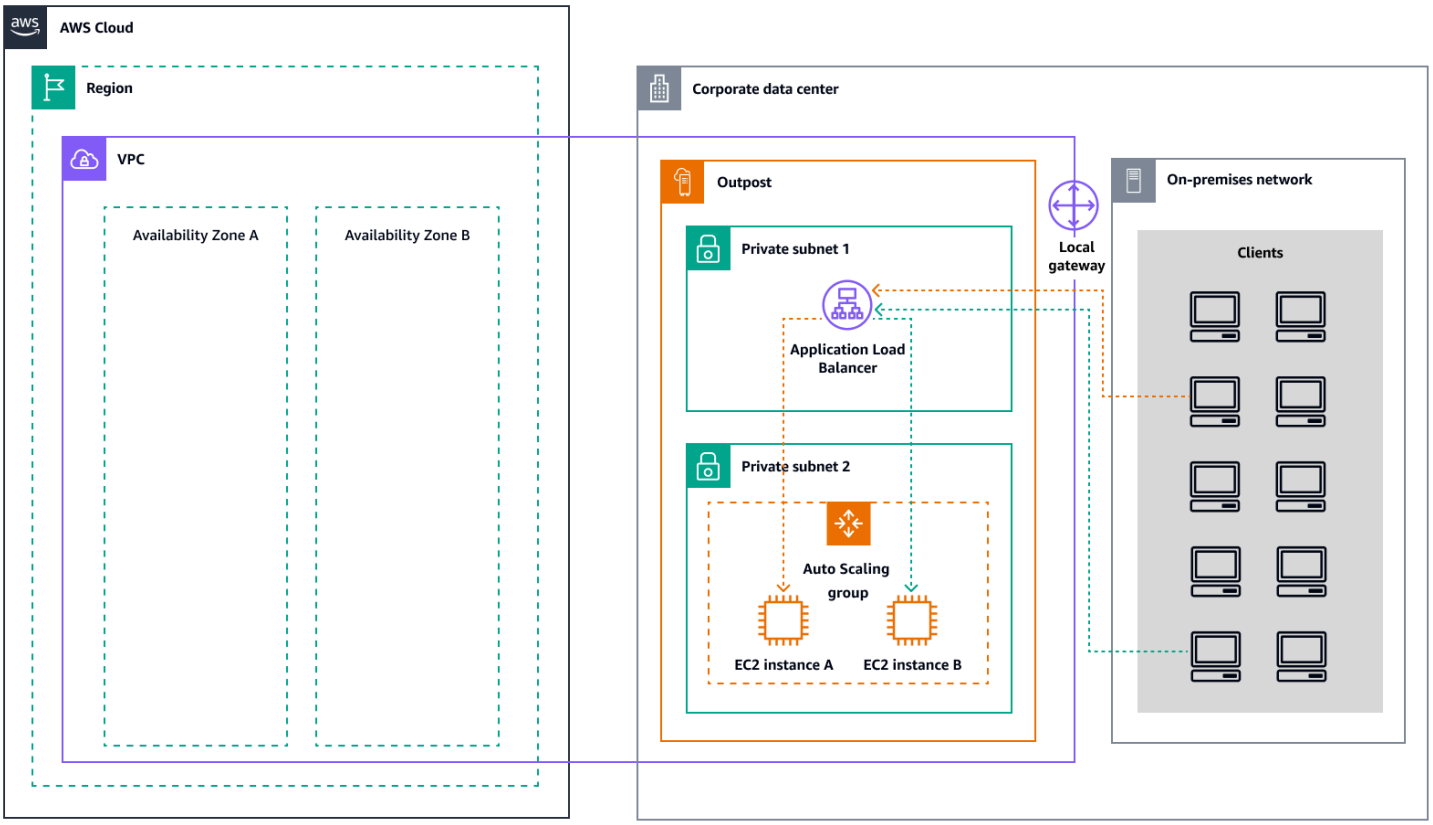


Failover-Mechanismen

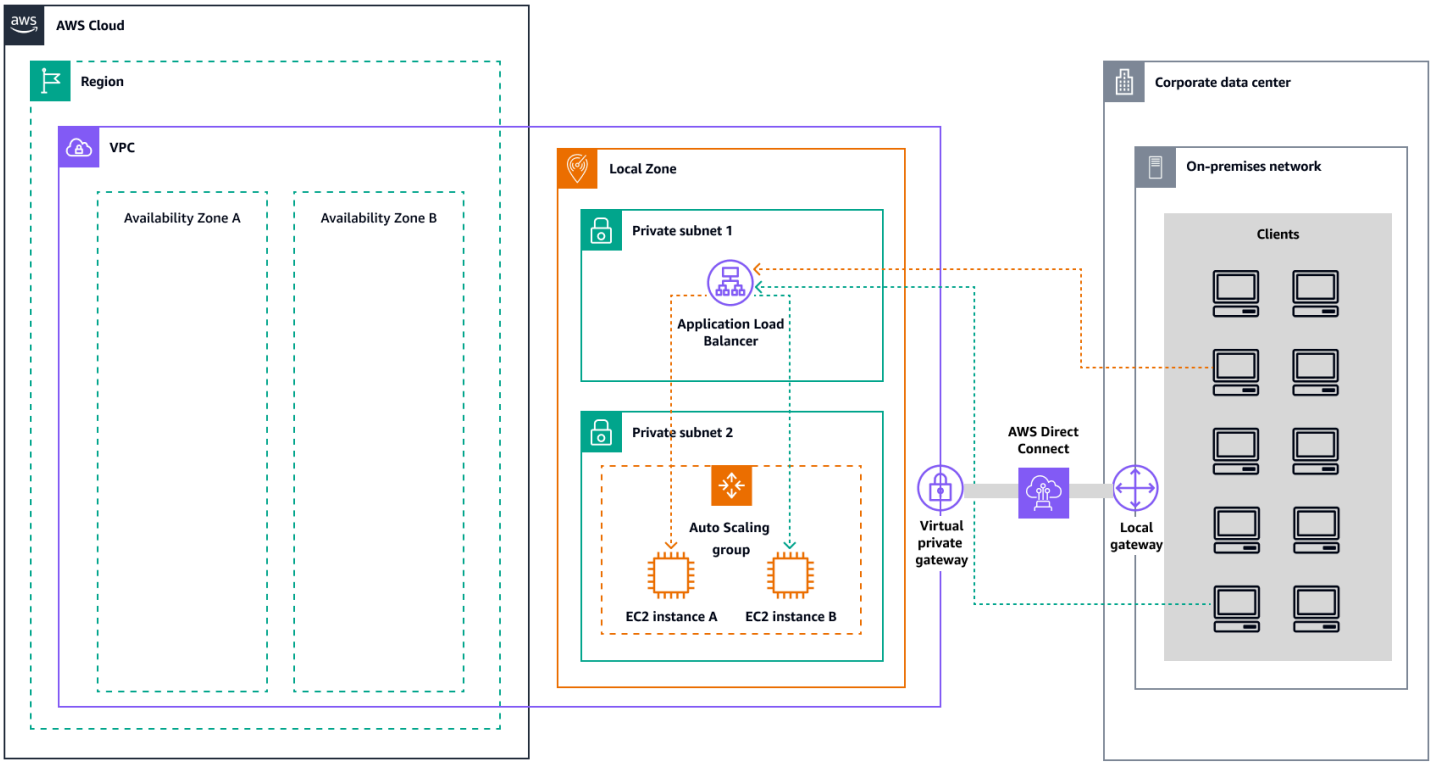
Lastenausgleich und automatische Skalierung

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 Instance überlastet wird. Um ELB mit Ihrer Amazon EC2 Auto Scaling Scaling-Gruppe zu verwenden, fügen Sie den Load Balancer Ihrer Auto Scaling-Gruppe hinzu. Dadurch wird die Gruppe beim Load Balancer registriert, der als zentrale Anlaufstelle für den gesamten eingehenden Web-Traffic 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.

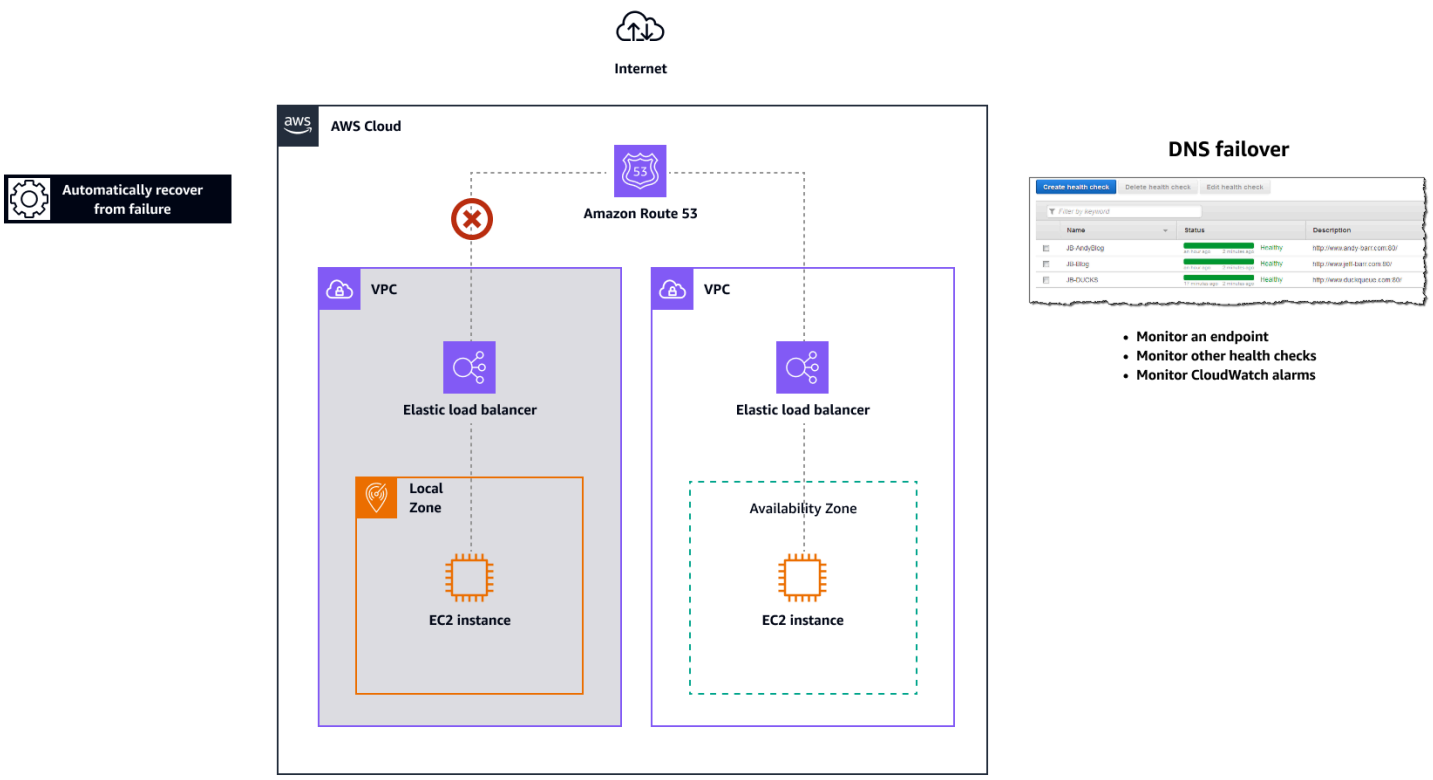


> **Note**
>
> Application Load Balancer sind sowohl in lokalen Zonen als auch AWS Outposts in Local Zones verfügbar. Um jedoch einen Application Load Balancer in zu verwenden AWS Outposts, müssen Sie die Amazon EC2 EC2-Kapazität so dimensionieren, dass sie die Skalierbarkeit bietet, die der Load Balancer 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 zur Bewertung des Zustands einer Ressource konfigurieren, 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 öffentlichen 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 Anwendung. Outposts-hosted

Amazon Route 53 Resolver on 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.

Mit diesem Start werden nicht nur lokale Resolver aktiviert, sondern auch lokale Resolver-Endpunkte aktiviert. 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 unter Auflösen von DNS-Abfragen zwischen VPCs und Ihrem Netzwerk in der Route 53-Dokumentation.

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 Local Zones 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 Local Zones 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 Local Zones
Amazon EKS	Stellen Sie Amazon EKS vor Ort bereit mit AWS Outposts	Starten Sie EKS-Cluster mit niedriger Latenz mit AWS Local Zones
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 Local Zones
Amazon ElastiCache	Outposts verwenden mit ElastiCache	Verwenden von Local Zones mit ElastiCache
Amazon EMR	EMR-Cluster auf AWS Outposts	EMR-Cluster auf AWS Local Zones
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 Transform MGN	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 für Python (Boto)
- Ec2Client im AWS SDK for 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 Local Zones -Benutzerhandbuch
- AWS Outposts Familie
- AWS Local Zones
- 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 Local Zones (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 Local Zones
- Amazon ECS auf Amazon EC2
- Verwaltung von Edge-Aware-Service Mesh mit Amazon EKS für AWS Local Zones
- Bereitstellung von lokalem Gateway-Ingress-Routing auf Amazon EC2
- Automatisieren Sie Ihre Workload-Bereitstellungen in AWS Local Zones
- 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 Local Zones 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

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