Benutzerhandbuch für Outposts-Racks

# AWS Outposts

# AWS Outposts: Benutzerhandbuch für Outposts-Racks

# Table of Contents

# Was ist AWS Outposts?

AWS Outposts ist ein vollständig verwalteter Service, der AWS Infrastruktur APIs, Dienste und Tools auf Kundenstandorte ausdehnt. Durch den lokalen Zugriff auf die AWS verwaltete Infrastruktur AWS Outposts können Kunden Anwendungen vor Ort mit denselben Programmierschnittstellen wie in AWS Regionen erstellen und ausführen und gleichzeitig lokale Rechen- und Speicherressourcen für geringere Latenz und lokale Datenverarbeitungsanforderungen nutzen.

Ein Outpost ist ein Pool von AWS Rechen- und Speicherkapazität, der an einem Kundenstandort bereitgestellt wird. AWS betreibt, überwacht und verwaltet diese Kapazität als Teil einer AWS Region. Sie können Subnetze in Ihrem Outpost erstellen und diese angeben, wenn Sie AWS Ressourcen wie EC2 Instances, EBS-Volumes, ECS-Cluster und RDS-Instances erstellen. Instances in Outpost-Subnetzen kommunizieren mit anderen Instances in der AWS Region über private IP-Adressen, alle innerhalb derselben VPC.

> **Note**
>
> Sie können einen Außenposten nicht mit einem anderen Außenposten oder einer anderen lokalen Zone verbinden, die sich innerhalb derselben VPC befindet.

Weitere Informationen finden Sie auf der AWS Outposts -Produktseite.

## Die wichtigsten Konzepte

Dies sind die wichtigsten Konzepte für. AWS Outposts

- Außenpoststandort — Die vom Kunden verwalteten physischen Gebäude, in denen Ihr Außenposten installiert AWS wird. Ein Standort muss die Anforderungen an die Einrichtung, das Netzwerk und die Stromversorgung Ihres Outposts erfüllen.
- Outpost-Kapazität – Rechen- und Speicherressourcen, die auf dem Outpost verfügbar sind. Du kannst die Kapazität deines Outposts von der Konsole aus einsehen und verwalten. AWS Outposts AWS Outposts unterstützt Self-Service-Kapazitätsmanagement, das Sie auf der Outposts-Ebene definieren können, um alle Ressourcen in Outposts oder speziell für jedes einzelne Asset neu zu konfigurieren. Ein Outpost-Asset kann ein einzelner Server in einem Outposts-Rack oder ein Outposts-Server sein.

- Outpost-Ausrüstung — Physische Hardware, die den Zugriff auf den Service ermöglicht. AWS Outposts Die Hardware umfasst Racks, Server, Switches und Kabel, die Eigentum des Unternehmens sind und von diesem verwaltet werden. AWS
- Outposts-Racks – Ein Outpost-Formfaktor, bei dem es sich um ein 42U-Rack nach Branchenstandard handelt. Zu den Racks von Outposts gehören rackmontierbare Server, Switches, ein Netzwerk-Patchpanel, ein Power-Shelf und leere Panels.
- Outposts ACE-Racks — Das Aggregation, Core, Edge (ACE) -Rack dient als Netzwerkaggregationspunkt für Outpost-Bereitstellungen mit mehreren Racks. Das ACE-Rack reduziert die Anzahl der Anforderungen an physische Netzwerkports und logische Schnittstellen, indem es Konnektivität zwischen mehreren Outpost-Compute-Racks in Ihren logischen Outposts und Ihrem lokalen Netzwerk bereitstellt.

  Sie müssen ein ACE-Rack installieren, wenn Sie über vier oder mehr Computer-Racks verfügen. Wenn Sie weniger als vier Computer-Racks haben, aber in future eine Erweiterung auf vier oder mehr Racks planen, empfehlen wir, dass Sie frühestens ein ACE-Rack installieren.

  Weitere Informationen zu ACE-Racks finden Sie unter Skalierung von AWS Outposts Rack-Bereitstellungen mit ACE-Racks.
- Outposts-Server – Ein Outpost-Formfaktor, bei dem es sich um einen 1U- oder 2U-Server nach Branchenstandard handelt, der in einem standardmäßigen EIA-310D 19-konformen 4-Post-Rack installiert werden kann. Outposts-Server bieten lokale Rechen- und Netzwerkdienste für Standorte mit begrenztem Platzbedarf oder geringeren Kapazitätsanforderungen.
- Outpost-Inhaber — Der Kontoinhaber für das Konto, das die Bestellung aufgibt. AWS Outposts Nach AWS der Kontaktaufnahme mit dem Kunden kann der Eigentümer weitere Ansprechpartner angeben. AWS wird mit den Kontakten kommunizieren, um Bestellungen, Installationstermine sowie Wartung und Austausch der Hardware zu klären. Wenden Sie sich an das AWS -Support Center, falls sich die Kontaktinformationen ändern.
- Servicelink — Netzwerkroute, die die Kommunikation zwischen Ihrem Außenposten und der zugehörigen AWS Region ermöglicht. Jeder Outpost ist eine Erweiterung einer Availability Zone und der zugehörigen Region.
- Local Gateway (LGW) — Ein virtueller Router mit logischer Verbindung, der die Kommunikation zwischen einem Outposts-Rack und Ihrem lokalen Netzwerk ermöglicht.
- Lokale Netzwerkschnittstelle — Eine Netzwerkschnittstelle, die die Kommunikation von einem Outposts-Server und Ihrem lokalen Netzwerk aus ermöglicht.

# AWS Ressourcen auf Outposts

Sie können die folgenden Ressourcen auf Ihrem Outpost erstellen, um Workloads mit geringer Latenz zu unterstützen, die in unmittelbarer Nähe zu On-Premises-Daten und Anwendungen ausgeführt werden müssen:

Datenverarbeitung

| Ressourcentyp | Racks | Server |
| --- | --- | --- |
| EC2 Amazon-Instanzen | Ja | Ja |
| Amazon-ECS-Cluster | Ja | Ja |
| Amazon-EKS-Knoten | Ja | Nein |

Datenbank und Analytik

| Ressourcentyp | Racks | Server |
| --- | --- | --- |
| ElastiCacheAmazon-Knoten (Redis-Cluster, Memcached-Cluster) | Ja | Nein |
| Amazon EMR-Cluster | Ja | Nein |
| Amazon RDS DB-Instances | Ja | Nein |

## Netzwerk

| Ressourcentyp | Racks | Server |
| --- | --- | --- |
| App Mesh Envoy-Proxy |  Ja |  Ja |
| Application Load Balancer |  Ja |  Nein |
| Amazon VPC-Subnetze |  Ja |  Ja |
| Amazon Route 53 |  Ja |  Nein |

## Speicher

| Ressourcentyp | Racks | Server |
| --- | --- | --- |
| Amazon-EBS-Volumes |  Ja |  Nein |
| Amazon-S3-Buckets |  Ja |  Nein |

Andere AWS-Services

| Service | Racks | Server |
| --- | --- | --- |
| AWS IoT Greengrass |  Ja |  Ja |

# Preisgestaltung

Die Preisgestaltung basiert auf Ihren Bestelldetails. Wenn Sie eine Bestellung aufgeben, können Sie aus einer Vielzahl von Outpost-Konfigurationen wählen, die jeweils eine Kombination aus EC2 Amazon-Instance-Typen und Speicheroptionen bieten. Sie wählen auch eine Vertragslaufzeit und eine Zahlungsoption. Die Preise beinhalten Folgendes:

- Outposts Racks — Lieferung, Installation, Wartung der Infrastruktur, Softwarepatches und Upgrades sowie Rackentfernung.
- Outpost-Server — Bereitstellung, Wartung von Infrastrukturdiensten sowie Softwarepatches und Upgrades. Sie sind für die Installation und Verpackung des Servers für die Rücksendung verantwortlich.

Ihnen werden gemeinsam genutzte Ressourcen und jegliche Datenübertragung von der AWS Region zum Outpost in Rechnung gestellt. Ihnen werden auch Datenübertragungen in Rechnung gestellt, die AWS der Aufrechterhaltung der Verfügbarkeit und Sicherheit dienen.

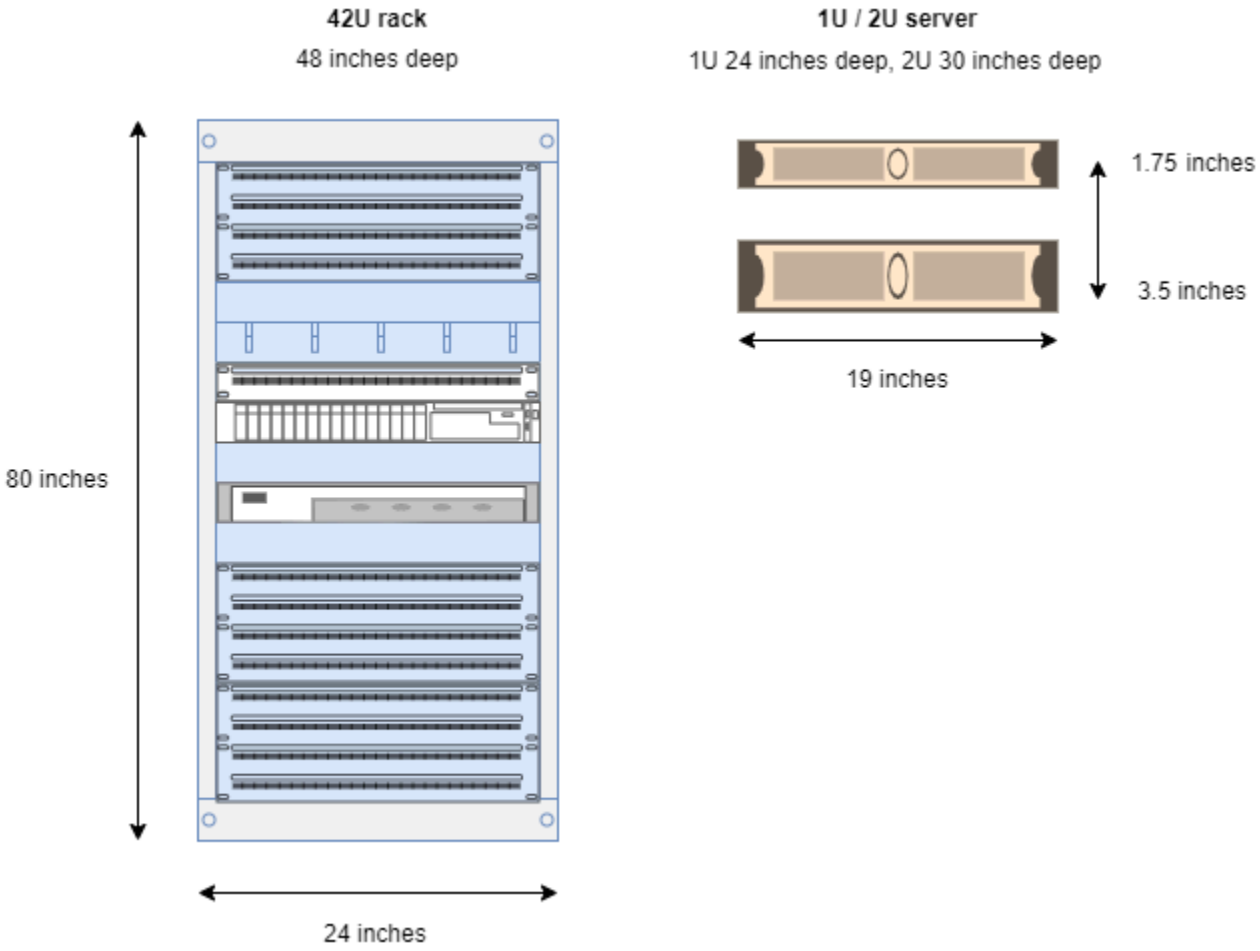
Preise, die auf Standort, Konfiguration und Zahlungsoption basieren, finden Sie unter:

- Outposts, Racks, Preise
- Preise Outposts Outposts-Server

# Wie AWS Outposts funktioniert

AWS Outposts ist für den Betrieb mit einer konstanten und konsistenten Verbindung zwischen Ihrem Außenposten und einer AWS Region konzipiert. Um diese Verbindung zur Region und zu den lokalen Workloads in Ihrer On-Premises-Umgebung herzustellen, müssen Sie Ihren Outpost mit Ihrem On-Premises-Netzwerk verbinden. Ihr lokales Netzwerk muss einen WAN-Zugriff (Wide Area Network) auf die Region ermöglichen. Es muss auch LAN- oder WAN-Zugriff auf das lokale Netzwerk bieten, in dem sich Ihre On-Premises-Workloads oder Anwendungen befinden.

Das folgende Diagramm veranschaulicht beide Outpost-Formfaktoren.




Inhalt

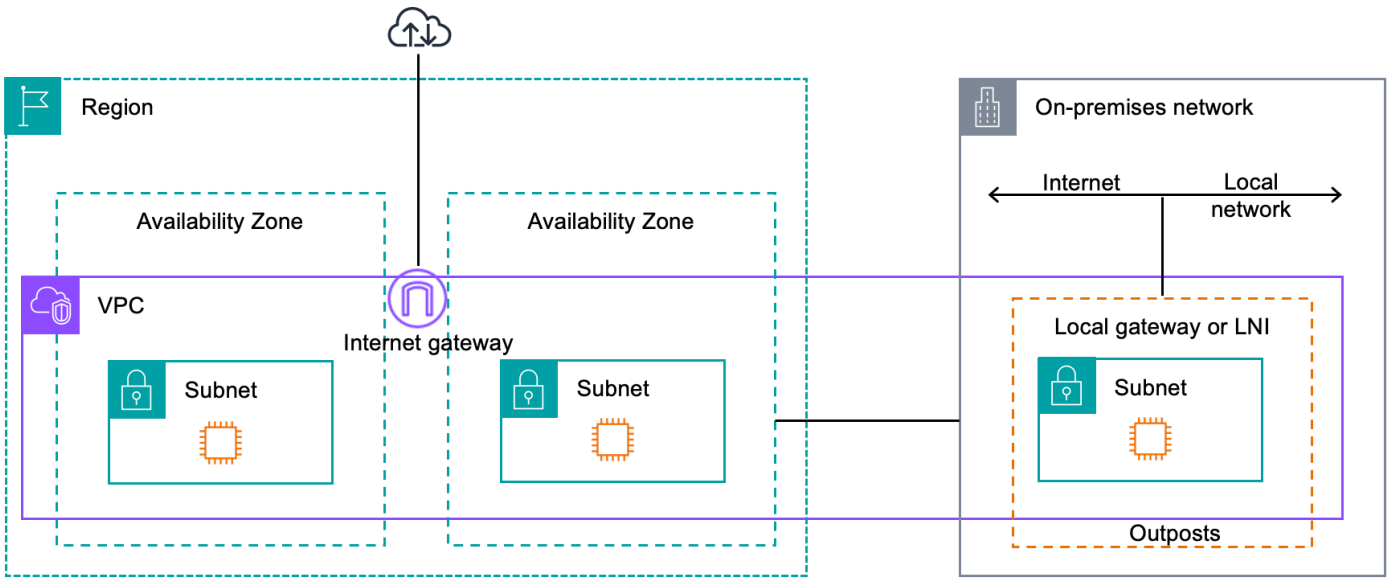
- DNS
- Service Link
- Lokale Gateways
- Lokale Netzwerkschnittstellen

# Netzwerkkomponenten

AWS Outposts erweitert eine Amazon-VPC von einer AWS Region zu einem Outpost mit den VPC-Komponenten, auf die in der Region zugegriffen werden kann, darunter Internet-Gateways, virtuelle private Gateways, Amazon VPC Transit Gateways und VPC-Endpunkte. Ein Outpost ist einer Availability Zone in der Region zugeordnet und stellt eine Erweiterung dieser Availability Zone dar, die Ihnen als Ausfallsicherheit dient.

Das folgende Diagramm zeigt die Netzwerkkomponenten für Ihren Outpost.

- Ein und ein lokales Netzwerk AWS-Region
- Eine VPC mit mehreren Subnetzen in der Region
- Ein Outpost im On-Premises-Netzwerk
- Konnektivität zwischen dem Outpost und dem lokalen Netzwerk wurde bereitgestellt:
  - Für Outposts-Racks: ein lokales Gateway
  - Für Outposts-Server: eine lokale Netzwerkschnittstelle (LNI)



# VPCs und Subnetze

Eine Virtual Private Cloud (VPC) erstreckt sich über alle Availability Zones in ihrer AWS Region. Sie können jeden VPC in der -Region auf Ihren Outpost erweitern, indem Sie ein Outpost-Subnetz hinzufügen. Um ein Outpost-Subnetz zu einer VPC hinzuzufügen, geben Sie beim Erstellen des Subnetzes den Amazon-Ressourcennamen (ARN) des Outpost an.

Outposts unterstützen mehrere Subnetze. Sie können das EC2 Instanz-Subnetz angeben, wenn Sie die EC2 Instance in Ihrem Outpost starten. Sie können die zugrunde liegende Hardware, auf der die Instance bereitgestellt wird, nicht angeben, da es sich bei Outpost um einen Pool von AWS Rechen- und Speicherkapazität handelt.

Jeder Outpost kann mehrere unterstützen VPCs , die über ein oder mehrere Outpost-Subnetze verfügen können. Weitere Informationen zu VPC-Quoten finden Sie unter Amazon VPC Quotas im Amazon VPC Benutzerhandbuch.

Sie erstellen Outpost-Subnetze aus dem VPC CIDR-Bereich der VPC, in der Sie den Outpost erstellt haben. Sie können die Outpost-Adressbereiche für Ressourcen verwenden, z. B. für EC2 Instances, die sich im Outpost-Subnetz befinden.

## Routing

Standardmäßig erbt jedes Outpost-Subnetz die Haupt-Routing-Tabelle von seiner VPC. Sie können eine benutzerdefinierte Routing-Tabelle erstellen und diese mit einem Outpost-Subnetz verknüpfen.

Die Routing-Tabellen für Outpost-Subnetze funktionieren genauso wie für Subnetze der Availability Zone. Sie können IP-Adressen, Internet-Gateways, lokale Gateways, virtuelle private Gateways und Peering-Verbindungen als Ziele angeben. Beispielsweise erbt jedes Outpost-Subnetz entweder über die geerbte Haupt-Routing-Tabelle oder eine benutzerdefinierte Tabelle die lokale VPC-Route. Das bedeutet, dass der gesamte Datenverkehr in der VPC, einschließlich des Outpost-Subnetzes mit einem Ziel im VPC-CIDR, weiterhin in der VPC geroutet wird.

Routing-Tabellen für Outpost-Subnetze können die folgenden Ziele enthalten:

- VPC CIDR-Bereich — AWS definiert dies bei der Installation. Dies ist die lokale Route und gilt für das gesamte VPC-Routing, einschließlich des Datenverkehrs zwischen Outpost-Instances in derselben VPC.

- AWS Ziele in der Region — Dazu gehören Präfixlisten für Amazon Simple Storage Service (Amazon S3), Amazon DynamoDB DynamoDB-Gateway-Endpunkte, AWS Transit Gateway virtuelle private Gateways, Internet-Gateways und VPC-Peering.

  Wenn Sie eine Peering-Verbindung mit mehreren VPCs auf demselben Outpost haben, VPCs verbleibt der Datenverkehr zwischen den Outpost und verwendet nicht den Service-Link zurück zur Region.
- VPC-interne Kommunikation über Outposts hinweg mit lokalem Gateway – Sie können die Kommunikation zwischen Subnetzen in derselben VPC über verschiedene Outposts hinweg mithilfe von lokalen Gateways mithilfe von direktem VPC-Routing herstellen. Weitere Informationen finden Sie unter:
  - Direktes VPC-Routing
  - Routing zu einem lokalen AWS Outposts -Gateway

# DNS

Für Netzwerkschnittstellen, die mit einer VPC verbunden sind, können EC2 Instances Outposts Outposts-Subnetzen den Amazon Route 53 DNS-Service verwenden, um Domainnamen in IP-Adressen aufzulösen. Route 53 unterstützt DNS-Features wie Domainregistrierung, DNS-Routing und Zustandsprüfung für Instances, die in Ihrem Outpost laufen. Sowohl öffentliche als auch privat gehostete Availability Zones werden für die Weiterleitung von Datenverkehr zu bestimmten Domains unterstützt. Route 53-Resolver werden in der Region gehostet. AWS Daher muss die Service Link-Konnektivität vom Outpost zurück zur AWS Region aktiviert sein, damit diese DNS-Funktionen funktionieren.

Abhängig von der Pfadlatenz zwischen Ihrem Outpost und der Region kann es bei Route 53 zu längeren DNS-Auflösungszeiten kommen. AWS In solchen Fällen können Sie die in Ihrer On-Premises-Umgebung installierten DNS-Server verwenden. Um Ihre eigenen DNS-Server zu verwenden, müssen Sie DHCP-Optionssätze für Ihre On-Premises-DNS-Server erstellen und sie der VPC zuordnen. Sie müssen außerdem sicherstellen, dass IP-Konnektivität zu diesen DNS-Servern besteht. Möglicherweise müssen Sie der lokalen Gateway-Routingtabelle auch Routen hinzufügen, um die Erreichbarkeit zu gewährleisten. Dies ist jedoch nur eine Option für Outposts-Racks mit lokalem Gateway. Da DHCP-Optionssätze einen VPC-Bereich haben, versuchen Instances sowohl in den Outpost-Subnetzen als auch in den Subnetzen der Availability Zone für die VPC, die angegebenen DNS-Server für die DNS-Namensauflösung zu verwenden.

Die Abfrageprotokollierung wird für DNS-Abfragen, die von einem Outpost stammen, nicht unterstützt.

## Service Link

Der Service-Link ist eine Verbindung von Ihrem Outpost zurück zu Ihrer ausgewählten AWS Region oder der Heimatregion von Outposts. Der Service Link ist ein verschlüsselter Satz von VPN-Verbindungen, die immer dann verwendet werden, wenn der Outpost mit der von Ihnen ausgewählten Heimatregion kommuniziert. Sie verwenden ein virtuelles LAN (VLAN), um den Datenverkehr auf dem Service Link zu segmentieren. Das Service Link VLAN ermöglicht die Kommunikation zwischen dem Outpost und der AWS Region sowohl für die Verwaltung des Outposts als auch für den Intra-VPC-Verkehr zwischen der Region und dem Outpost. AWS

Ihr Service Link wird erstellt, wenn Ihr Outpost bereitgestellt wird. Wenn Sie einen Serverformfaktor haben, stellen Sie die Verbindung her. Wenn Sie über ein Rack verfügen, wird der Service Link erstellt. AWS Weitere Informationen finden Sie unter:

- AWS Outposts Konnektivität zu AWS-Regionen
- Das Whitepaper „Überlegungen AWS zum Design und zur Architektur AWS Outposts hoher Verfügbarkeit“ von Anwendungen und Workloads

## Lokale Gateways

Outposts-Racks verfügen über ein lokales Gateway, das Konnektivität zu Ihrem lokalen Netzwerk bereitstellt. Wenn Sie ein Outposts-Rack haben, können Sie ein lokales Gateway als Ziel angeben, wobei das Ziel Ihr lokales Netzwerk ist. Lokale Gateways sind nur für Outposts-Racks verfügbar und können nur in VPC- und Subnetz-Routing-Tabellen verwendet werden, die einem Outposts-Rack zugeordnet sind. Weitere Informationen finden Sie unter:

- Lokale Gateways für Ihre Outposts-Racks
- Das Whitepaper „Überlegungen zum Design und zur Architektur AWS Outposts hoher Verfügbarkeit“ von Anwendungen und Workloads AWS

## Lokale Netzwerkschnittstellen

Outposts-Server verfügen über eine lokale Netzwerkschnittstelle, um Konnektivität zu Ihrem lokalen Netzwerk bereitzustellen. Eine lokale Netzwerkschnittstelle ist nur für Outposts-Server verfügbar, die in einem Outpost-Subnetz laufen. Sie können eine lokale Netzwerkschnittstelle nicht von einer EC2 Instance in einem Outposts-Rack oder in der AWS Region aus verwenden. Die lokale

Netzwerkschnittstelle ist nur für On-Premises-Standorte vorgesehen. Weitere Informationen finden Sie unter Lokale Netzwerkschnittstelle im AWS Outposts -Benutzerhandbuch für Outposts-Server.

# Standortanforderungen für Outposts-Racks

Ein Outpost-Standort ist der physische Standort, an dem Ihr Outpost läuft. Standorte sind nur in ausgewählten Ländern und Gebieten verfügbar. Weitere Informationen finden Sie unter AWS Outposts Rack FAQs. Sehen Sie sich die Frage an: In welchen Ländern und Gebieten ist Outposts-Rack verfügbar?

Diese Seite behandelt die Anforderungen für Outposts-Racks. Wenn Sie ein Aggregation, Core, Edge (ACE) -Rack installieren, muss Ihr Standort auch die unter aufgeführten Anforderungen erfüllen. Standortanforderungen für Outpost ACE-Racks

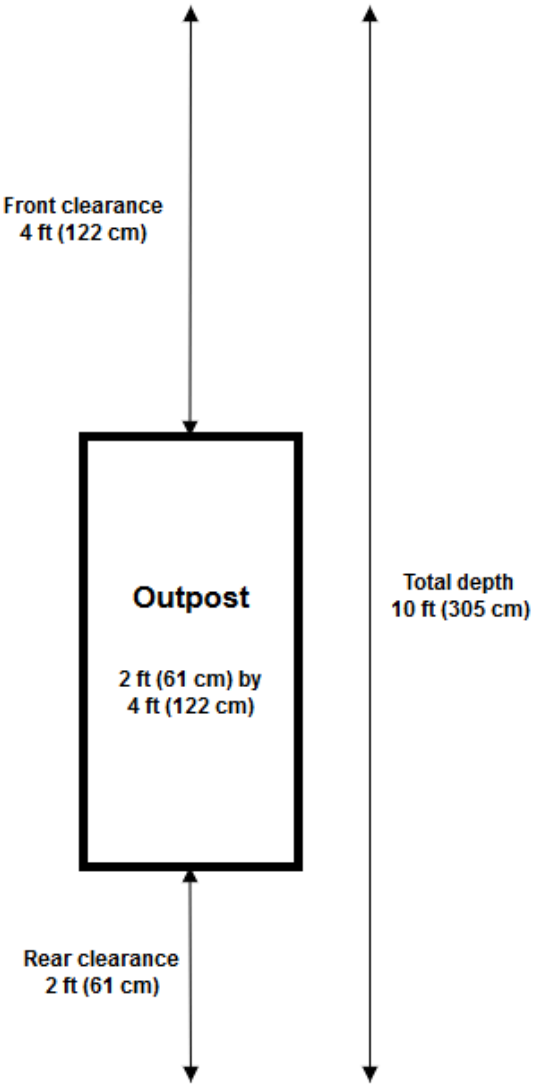
Die Anforderungen für Outposts-Server finden Sie unter Standortanforderungen für Outposts-Server im AWS Outposts -Benutzerhandbuch für Outposts-Server.

## Einrichtung

Dies sind die Anforderungen an die Einrichtung von Racks.

- Temperatur und Luftfeuchtigkeit – Die Umgebungstemperatur muss zwischen 41° F (5° C) und 95° F (35° C) liegen. Die relative Luftfeuchtigkeit muss zwischen 8 und 80 Prozent liegen und darf nicht kondensieren.
- Luftzirkulation – Die Racks saugen kalte Luft aus dem Vordergang ab und leiten warme Luft in den Hintergang ab. In der Rackposition muss ein Luftstrom von mindestens dem 145,8-fachen kVA an Kubikfuß pro Minute (CFM) bereitgestellt werden.
- Laderampe – Ihre Laderampe muss Platz für eine Regalkiste bieten, die 239 cm (94 Zoll) hoch, 138 cm (54 Zoll) breit und 130 cm (51 Zoll) tief ist.
- Gewicht – Das Gewicht variiert je nach Konfiguration. Das Gewicht für Ihre Konfiguration finden Sie in der Bestellübersicht unter den Rack-Point-Loads. Der Ort, an dem das Rack aufgestellt wird, und der Weg dorthin müssen das angegebene Gewicht tragen. Dazu gehören auch alle Güter- und Standardaufzüge entlang des Pfades.
- Bodenfreiheit – Das Rack ist 203 cm (80 Zoll) hoch, 61 cm (24 Zoll) breit und 122 cm (48 Zoll) tief. Alle Türen, Flure, Kurven, Rampen und Aufzüge müssen ausreichend Freiraum bieten. In der endgültigen Ruheposition muss ein 61 cm (24 Zoll) breiter und 122 cm (48 Zoll) tiefer Bereich für den Outpost vorhanden sein, mit zusätzlichem Abstand von 122 cm (48 Zoll) an der Vorderseite und 61 cm (24 Zoll) an der Rückseite. Die gesamte Mindestfläche, die für den Outpost erforderlich ist, ist 61 cm (24 Zoll) breit und 305 cm (10 Fuß) tief.

Das folgende Diagramm zeigt die gesamte Mindestfläche, die für den Outpost erforderlich ist, einschließlich Freiraum.




- Erdbebenabstützung — Soweit gesetzlich oder gesetzlich vorgeschrieben, müssen Sie für das Rack, solange es sich in Ihrer Anlage befindet, geeignete seismische Verankerungen und Abstützungen installieren und warten. AWS bietet bei allen Outposts-Racks Bodenhalterungen, die Schutz vor seismischen Aktivitäten von bis zu 2,0 G bieten.
- Verbindungspunkt — Wir empfehlen Ihnen, wire/point an der Rackposition eine Verklebung vorzusehen, damit Ihr Elektriker die Racks während der Installation verkleben kann. Diese wird von einem zertifizierten Techniker bestätigt. AWS

- Zugang zur Einrichtung — Sie dürfen die Einrichtung nicht in einer Weise verändern, die sich negativ auf den AWS Zugriff, die Wartung oder Entfernung des Außenpostens auswirkt.
- Höhenlage – Die Höhenlage des Raums, in dem das Rack installiert ist, muss unter 3.050 Metern (10.005 Fuß) liegen.

# Netzwerk

Dies sind die Netzwerkanforderungen für Racks.

- Stellen von Uplinks mit Geschwindigkeiten von 1 Gbit/s, 10 Gbit/s, 40 Gbit/s oder 100 Gbit/s bereit.

  Empfehlungen zur Bandbreite für die Service-Link-Verbindung finden Sie unter Bandbreitenempfehlungen.
- Stellen Sie entweder Singlemode-Glasfaser (SMF) mit Lucent Connector (LC), Multimode-Glasfaser (MMF) oder MMF mit LC bereit. OM4
- Stellen Sie ein oder zwei Upstream-Geräte bereit, bei denen es sich um Switches oder Router handeln kann. Wir empfehlen zwei Geräte, um eine hohe Verfügbarkeit zu gewährleisten.

## Checkliste zur Netzwerkbereitschaft

Verwenden Sie diese Checkliste, wenn Sie die Informationen für Ihre Outpost-Konfiguration sammeln. Dazu gehören das LAN, WAN und alle Geräte zwischen dem Outpost und lokalen Verkehrszielen sowie dem Ziel in der Region. AWS

Uplink-Geschwindigkeit, Ports und Glasfaser

Uplink-Geschwindigkeit und Ports

Ein Outpost hat zwei Outpost-Netzwerkgeräte, die an Ihr lokales Netzwerk angeschlossen sind. Die Anzahl der Uplinks, die jedes Gerät unterstützen kann, hängt von Ihren Bandbreitenanforderungen ab und davon, was Ihr Router unterstützen kann. Weitere Informationen finden Sie unter Tatsächliche Konnektivität.

Die folgende Liste zeigt, wie viele Uplink-Ports für jedes Outpost-Netzwerkgerät unterstützt werden, basierend auf der Uplink-Geschwindigkeit.

1 Gbit/s

1, 2, 4, 6 oder 8 Uplinks

10 Gbit/s

1, 2, 4, 8, 12 oder 16 Uplinks

40 Gbit/s oder 100 Gbit/s

1, 2 oder 4 Uplinks

Glasfaser

Die folgenden Glasfasertypen werden unterstützt:

- Singlemode-Glasfaser (SMF) mit Lucent-Stecker (LC)
- Multimode-Glasfaser (MMF) oder MMF mit LC OM4

Abhängig von der Uplink-Geschwindigkeit und dem ausgewählten Glasfasertyp werden die folgenden optischen Standards unterstützt.

| Uplink-Geschwindigkeit | Glasfasertyp | Optischer Standard |
|---|---|---|
| 1 Gbit/s | SMF | – 1000 Base-LX |
| 1 Gbit/s | MMF | – 1000 Base-SX |
| 10 Gbit/s | SMF | – 10 GBASE-IR<br>– 10 GBASE-LR |
| 10 Gbit/s | MMF | – 10 GBASE-SR |
| 40 GBit/s | SMF | — 40 GBASE- (L) IR4 LR4<br>— 40 G BASIS- LR4 |
| Breakout-Anwendung mit 4 x 10 Gbit/s | MMF | — 40 G BASIS- ESR4<br>— 40 G BASIS- SR4 |
| 100 Gbit/s | SMF | — 100 G MSA PSM4<br>— 100 G BASIS- CWDM4 |

| Uplink-Geschwindigkeit | Glasfasertyp | Optischer Standard |
| --- | --- | --- |
| | | — 100 GBASE- LR4 |
| Breakout-Anwendung mit 4 x 25 Gbit/s | MMF | — 100 GBASE- SR4 |

Aggregation von Outpost-Links und VLANs

Das Link Aggregation Control Protocol (LACP) ist zwischen dem Outpost und Ihrem Netzwerk erforderlich. Sie müssen dynamisches LAG mit LACP verwenden.

Folgendes VLANs ist für jedes Outpost-Netzwerkgerät erforderlich. Weitere Informationen finden Sie unter Virtuell LANs.

| Outpost-Netzwerkgerät | Service Link VLAN | Lokales Gateway VLAN |
| --- | --- | --- |
| Nr. 1 | Zulässige Werte: 1–4094 | Zulässige Werte: 1–4094 |
| Nr. 2 | Zulässige Werte: 1–4094 | Zulässige Werte: 1–4094 |

Für jedes Outpost-Netzwerkgerät können Sie wählen, ob Sie dasselbe VLANs oder ein anderes VLANs für den Service-Link und das lokale Gateway verwenden möchten. Wir empfehlen jedoch, dass jedes Outpost-Netzwerkgerät über ein anderes VLAN verfügt als das andere Outpost-Netzwerkgerät. Weitere Informationen finden Sie unter Link-Aggregation und Virtuell. LANs

Wir empfehlen außerdem redundante Layer-2-Konnektivität. LACP wird für die Link-Aggregation verwendet und nicht für Hochverfügbarkeit. LACP zwischen den Outpost-Netzwerkgeräten wird nicht unterstützt.

IP-Konnektivität von Outpost-Netzwerkgeräten

Jedes der beiden Outpost-Netzwerkgeräte benötigt eine CIDR und eine IP-Adresse für den Service-Link und das lokale Gateway. VLANs Wir empfehlen, jedem Netzwerkgerät ein eigenes Subnetz mit einem /30- oder /31-CIDR zuzuweisen. Geben Sie ein Subnetz und eine IP-Adresse aus dem Subnetz an, die der Outpost verwenden soll. Weitere Informationen finden Sie unter Netzwerk-Layer-Konnektivität.

| Outpost-Netzwerkgerät | Anforderungen für Service Link | Anforderungen für das lokale Gateway |
|---|---|---|
| Nr. 1 | – Service Link CIDR (/30 oder /31)<br>– IP-Adresse des Service Link | – Lokales Gateway CIDR (/30 oder /31)<br>– IP-Adresse des lokalen Gateways |
| Nr. 2 | – Service Link CIDR (/30 oder /31)<br>– IP-Adresse des Service Link | – Lokales Gateway CIDR (/30 oder /31)<br>– IP-Adresse des lokalen Gateways |

Maximale Übertragungseinheit (Maximum Transmission Unit, MTU) des Service Link

Das Netzwerk muss eine MTU von 1500 Byte zwischen dem Outpost und den Service Link-Endpunkten in der übergeordneten Region unterstützen. AWS Weitere Informationen über Service Link finden Sie unter AWS Outposts Konnektivität zu AWS Regionen.

Service Link für Border Gateway Protocol

Der Outpost baut eine externe BGP (eBGP)-Peering-Sitzung zwischen jedem Outpost-Netzwerkgerät und Ihrem lokalen Netzwerkgerät für die Service Link-Konnektivität über das Service Link-VLAN auf. Weitere Informationen finden Sie unter Service Link BGP-Konnektivität.

| Outpost | BGP-Anforderungen für Service Link |
|---|---|
| Ihr Outpost | – Autonome Systemnummer (ASN) von Outpost BGP. 2 Byte (16 Bit) oder 4 Byte (32 Bit). Aus Ihrem privaten ASN-Bereich (64512–65534 oder 4200000000–4294967294).<br>– Infrastruktur-CIDR (/26 erforderlich, als zwei zusammenhängende /27s angekündigt). |

| Lokales Netzwerkgerät | BGP-Anforderungen für Service Link |
| --- | --- |
| Nr. 1 | – Service-Link-BGP-Peer-IP-Adresse.<br><br>– Service Link BGP-Peer ASN. 2 Byte (16 Bit) oder 4 Byte (32 Bit). |
| Nr. 2 | – Service-Link-BGP-Peer-IP-Adresse.<br><br>– Service Link BGP-Peer ASN. 2 Byte (16 Bit) oder 4 Byte (32 Bit). |

Service Link-Firewall

UDP und TCP 443 müssen in der Firewall zustandsorientiert aufgelistet sein.

| Protokoll | Quell-Port | Quelladresse | Ziel-Port | Zieladresse |
| --- | --- | --- | --- | --- |
| UDP | 443 | Outpost-Servicelink /26 | 443 | Öffentliche Routen der Outpost-Region |
| TCP | 1025-65535 | Outpost-Servicelink /26 | 443 | Öffentliche Routen der Outpost-Region |

Sie können eine AWS Direct Connect Verbindung oder eine öffentliche Internetverbindung verwenden, um den Outpost wieder mit der Region zu verbinden. AWS Für die Outpost Service Link-Konnektivität können Sie NAT oder PAT an Ihrer Firewall oder Ihrem Edge-Router verwenden. Der Service Link-Aufbau wird immer vom Outpost aus initiiert.

Weitere Informationen zu Service-Link-Anforderungen wie MTU und 175 ms Latenz finden Sie unter Konnektivität über Service Link.

Lokales Gateway für Border Gateway Protocol

Der Outpost baut eine eBGP-Peering-Sitzung von jedem Outpost-Netzwerkgerät zu einem lokalen Netzwerkgerät auf, um eine Verbindung zwischen Ihrem lokalen Netzwerk und dem lokalen Gateway herzustellen. Weitere Informationen finden Sie unter BGP-Konnektivität für das lokale Gateway.

| Outpost | BGP-Anforderungen für das lokale Gateway |
| --- | --- |
| Ihr Outpost | – Autonome Systemnummer (ASN) von Outpost BGP. 2 Byte (16 Bit) oder 4 Byte (32 Bit). Aus Ihrem privaten ASN-Bereich (64512–65534 oder 4200000000–4294967294).<br><br>– CoIP CIDR für Werbung (öffentlich oder privat, mindestens /26). |

| Lokale Netzwerkgeräte | BGP-Anforderungen für das lokale Gateway |
| --- | --- |
| Nr. 1 | – BGP-Peer-IP-Adresse des lokalen Gateways.<br><br>– Lokales Gateway BGP-Peer-ASN. 2 Byte (16 Bit) oder 4 Byte (32 Bit). |
| Nr. 2 | – BGP-Peer-IP-Adresse des lokalen Gateways.<br><br>– Lokales Gateway BGP-Peer-ASN. 2 Byte (16 Bit) oder 4 Byte (32 Bit). |

## Stromversorgung

Das Outposts-Power-Shelf unterstützt drei Leistungskonfigurationen: 5 kVA, 10 kVA oder 15 kVA. Die Konfiguration des Power-Shelfs hängt von der Gesamtstromaufnahme der Outpost-Kapazität ab. Wenn Ihre Outpost-Ressource beispielsweise eine maximale Leistungsaufnahme von 9,7 kVA hat, müssen Sie die Energiekonfigurationen für 10 kVA angeben: 4 x L6-30P oder IEC3 09, 2 Absenkungen auf S1 und 2 Absenkungen auf S2 für redundante, einphasige Stromversorgung. Die drei Leistungskonfigurationen sind in den folgenden zweiten Tabellen beschrieben.

Um die Stromverbrauchsanforderungen für verschiedene Outpost-Ressourcen zu sehen, wählen Sie in der Konsole unter Katalog durchsuchen aus. AWS Outposts https://console.aws.amazon.com/outposts/

| Anforderung | Spezifikation |
| --- | --- |
| Netzspannung (Wechselstrom) | Einphasig 208 bis 277 VAC; 50 oder 60 Hz<br><br>Dreiphasig:<br><br>• 208 bis 250 VAC (Delta); 50 bis 60 Hz<br>• 346 bis 480 VAC (Wye); 50 bis 60 Hz |
| Stromverbrauch | 5 kVA (4 kW), 10 kVA (9 kW) oder 15 kVA (13 kW) |
| Wechselstromschutz (vorgeschaltete Leistungsschalter) | Sowohl für 1N-Eingang (nicht redundant) als auch für 2N-Eingang (redundant): 30 A, 32 A oder 50 A mit D-Kurve- oder K-Kurven-Schutzschalter.<br><br>Nur für 2N-Eingänge (redundant): C-Kurve-, D-Kurve- oder K-Kurven-Schutzschalter.<br><br>B-Kurve oder niedriger wird nicht unterstützt. |
| Typ des Wechselstromeingangs (Steckdose) | Einphasige 3XL6-30P-, P+P+E-, 30A- oder 3x 309-P+N+E-, 32A-Stecker IEC6 IP67<br><br>Dreiphasig, Wye 1x IEC6 0309, 3P+N+E, Taktposition 7, 30A-Stecker oder 1x 0309, 3P+N+E, Uhrposition 6, 32A-Stecker IP67 IEC6 IP67<br><br>Dreiphasig, Delta CS8365 1xNon-NEMA-Twistlock Hubbell C, 3P+E, mittig geerdet, 50-A-Stecker<br><br>**Note**<br>Es hat sich bewährt, einen Stecker mit einer Buchse zu verbinden. IP67 IP67 Wenn das nicht möglich ist, lässt sich der IP67 Stecker mit einer IP44 Buchse verbinden . Die Nennleistung der Kombination aus Stecker und Buchse wird zur niedrigeren Nennleistung ()IP44. |
| Kabellänge vom Stromverteiler | 3 m (10,25 Fuß) |

| Anforderung | Spezifikation |
| --- | --- |
| Kabel vom Stromverteiler bis zum Kabeleingang des Racks | Von oben oder unter dem Rack |

Das Power-Shelf verfügt über zwei Eingänge, S1 und S2, die wie folgt konfiguriert werden können.

| | Redundant, einphasig | Redundant, dreiphasig | Einphasig | Dreiphasig |
| --- | --- | --- | --- | --- |
| 5 kVA | 2 x L6-30P oder IEC3 09; 1 fällt auf S1 und 1 Abfall auf S2 | 2 x AH53 0P7W, AH532 P6W oder CS8365 C; 1 Abfall auf S1 und 1 Abfall auf S2 | Nicht angeboten | 1 x AH53 0P7W, AH532 P6W oder CS8365 C; 1 Tropfen auf S1 |
| 10 kVA | 4 x L6-30P oder IEC3 09; 2 fallen auf S1 und 2 Tropfen auf S2 | | 2 x L6-30P oder IEC3 09; 2 Tropfen fallen auf S1 | |
| 15 kVA | 6 x L6-30P oder IEC3 09; 3 Tropfen auf S1 und 3 Tropfen auf S2 | | 3 x L6-30P oder IEC3 09; 3 Tropfen auf S1 | |

Wenn die Netzkabel, die wie zuvor beschrieben AWS zur Verfügung stehen, mit einem alternativen Netzstecker ausgestattet werden müssen, ist Folgendes zu beachten:

- Nur ein zertifizierter, vom Kunden bereitgestellter Elektriker darf den Netzadapter so modifizieren, dass er zu einem neuen Steckertyp passt.
- Die Installation muss alle geltenden nationalen, Landes- und örtlichen Sicherheitsanforderungen erfüllen und wie erforderlich auf elektrische Sicherheit geprüft werden.
- Sie als Kunde sollten Ihren AWS Vertreter über Änderungen am Netzstecker informieren. Auf Anfrage stellen Sie Informationen über die Änderungen an zur AWS Verfügung. Fügen Sie bitte auch alle von der zuständigen Behörde ausgestellten Sicherheitsinspektionsberichte bei. Dies ist eine Anforderung, um die Sicherheit der Anlage zu überprüfen, bevor AWS -Mitarbeiter Arbeiten an der Ausrüstung durchführen.

# Erfüllung der Bestellung

Um die Bestellung zu erfüllen, vereinbaren AWS wir mit Ihnen einen Termin und eine Uhrzeit. Sie erhalten außerdem eine Checkliste mit Punkten, die Sie vor der Installation überprüfen oder bereitstellen müssen.

Das AWS Installationsteam wird zum geplanten Datum und zur geplanten Uhrzeit an Ihrem Standort eintreffen. Sie werden das Rack an der angegebenen Position platzieren. Sie und Ihr Elektriker sind für den elektrischen Anschluss und die Installation am Rack verantwortlich.

Sie müssen sicherstellen, dass elektrische Installationen und alle Änderungen an diesen Installationen von einem zertifizierten Elektriker in Übereinstimmung mit allen geltenden Gesetzen, Vorschriften und bewährten Praktiken durchgeführt werden. Sie müssen eine schriftliche Genehmigung von AWS uns einholen, bevor Sie Änderungen an der Outpost-Hardware oder den Elektroinstallationen vornehmen. Sie erklären sich damit einverstanden, Unterlagen zur Verfügung zu stellen AWS , die die Einhaltung und Sicherheit aller Änderungen belegen. AWS ist nicht verantwortlich für Risiken, die durch die Elektroinstallation oder die elektrische Verkabelung von Outpost oder durch Änderungen entstehen. Sie dürfen keine weiteren Änderungen an der Outposts-Hardware vornehmen.

Das Team stellt über den von Ihnen bereitgestellten Uplink die Netzwerkkonnektivität für das Outposts-Rack her und konfiguriert die Kapazität des Racks.

Die Installation ist abgeschlossen, wenn Sie bestätigen, dass die Amazon EC2 - und Amazon EBS-Kapazität für Ihr Outposts-Rack in Ihrem verfügbar ist. AWS-Konto

# Standortanforderungen für Outpost ACE-Racks

> **Note**
>
> Gilt nur, wenn Sie ein ACE-Rack benötigen.

Ein Aggregation, Core, Edge (ACE) -Rack dient als Netzwerkaggregationspunkt für Outpost-Bereitstellungen mit mehreren Racks. Sie müssen ein ACE-Rack installieren, wenn Sie über vier oder mehr Computer-Racks verfügen. Wenn Sie weniger als vier Computer-Racks haben, aber in future eine Erweiterung auf vier oder mehr Racks planen, empfehlen wir Ihnen, ein ACE-Rack zu installieren.

Um ein ACE-Rack zu installieren, müssen Sie zusätzlich zu den unter aufgeführten Anforderungen die Anforderungen in diesem Abschnitt erfüllenStandortanforderungen für Outposts-Racks.

> **Note**
>
> ACE-Racks sind nicht vollständig geschlossen und verfügen weder über eine Vordertür noch über eine Hintertür.

## Einrichtung

Dies sind die Anforderungen an die Einrichtung eines ACE-Racks.

- Stromversorgung — Alle ACE-Racks werden mit einphasigem 10-kVA-Anschluss (Typ AA+BB, IEC6 0309 oder L6-30P Whip) geliefert.
- Gewichtsunterstützung — Das ACE-Rack wiegt 705 lbs (320 kg).
- Abstand/Größenabmessung — Das ACE-Rack ist 80 Zoll (203 cm) hoch, 24 Zoll (61 cm) breit und 42 Zoll (107 cm) tief.

  Wenn das ACE-Rack über Kabelführungsarme verfügt, beträgt die Breite des Racks 36 Zoll (91,5 cm).

# Netzwerk

Dies sind die Netzwerkanforderungen für ein ACE-Rack. Informationen darüber, wie das ACE-Rack die Outposts-Netzwerkgeräte, Ihre lokalen Netzwerkgeräte und Ihre Outposts-Racks verbindet, finden Sie unter. ACE-Rack-Konnektivität

- Anforderungen an das Rack-Netzwerk — Stellen Sie sicher, dass Sie die in den Lokale Netzwerkkonnektivität für Outposts-Racks Abschnitten Checkliste zur Netzwerkbereitschaft und aufgeführten Anforderungen erfüllen, mit Ausnahme der folgenden Änderungen:
  - Das ACE-Rack hat vier Netzwerkgeräte, die mit den Upstream-Geräten verbunden sind, nicht zwei wie bei einem einzelnen Outposts-Rack.
  - ACE-Racks unterstützen keine 1-Gbit/s-Uplinks.
- Uplink-Geschwindigkeit — Stellen Sie Uplinks mit Geschwindigkeiten von 10 Gbit/s, 40 Gbit/s oder 100 Gbit/s bereit. Empfehlungen zur Bandbreite für die Service Link-Verbindung finden Sie unter Empfehlungen für die Bandbreite von Service Links

  > **Important**
  >
  > ACE-Racks unterstützen keine 1-Gbit/s-Uplinks.

- Glasfaser — Stellen Sie Singlemode-Glasfaser (SMF) mit Lucent Connector (LC) oder Multimode-Glasfaser (MMF) mit Lucent Connector (LC) bereit. Die vollständige Liste der unterstützten Glasfasertypen und optischen Standards finden Sie unter. Uplink-Geschwindigkeit, Ports und Glasfaser
- Upstream-Gerät — Stellen Sie zwei oder vier Upstream-Geräte bereit, bei denen es sich um Switches oder Router handeln kann.
- Service-VLAN und ein lokales Gateway-VLAN — Für jedes der vier ACE-Netzwerkgeräte müssen Sie ein Service-VLAN und ein anderes Local Gateway-VLAN bereitstellen. Sie können wählen, ob Sie nur zwei unterschiedliche Optionen bereitstellen möchten VLANs, eines für das Service-VLAN und eines für das lokale Gateway-VLAN, oder ob Sie VLANs in jedem ACE-Netzwerkgerät unterschiedliche Optionen für Service-VLAN und LGW-VLAN verwenden möchten, sodass insgesamt 8 verschiedene Optionen zur Verfügung stehen. VLANs Weitere Informationen zur Verwendung von Linkaggregationsgruppen (LAGs) und VLAN finden Sie unter und. Link-Aggregation Virtuell LANs
- CIDR und IP-Adresse für den Service Link und das lokale Gateway VLANs — Wir empfehlen, jedem ACE-Netzwerkgerät ein eigenes Subnetz mit einem /30- oder /31-CIDR zuzuweisen.

Alternativ ist es möglich, jedem Service- und Local Gateway-VLAN ein einzelnes /29-Subnetz zuzuweisen. In beiden Fällen müssen Sie die IP-Adressen angeben, die die ACE-Netzwerkgeräte verwenden sollen. Weitere Informationen finden Sie unter Netzwerk-Layer-Konnektivität.

- Autonome BGP Systemnummer (ASN) für Service Link VLAN und Local Gateway VLAN für Kunden und Outpost — Der Outpost richtet eine externe BGP (eBGP) -Peering-Sitzung zwischen jedem ACE-Rack-Gerät und Ihrem lokalen Netzwerkgerät ein, um die Service Link-Konnektivität über das Service Link-VLAN zu gewährleisten. Darüber hinaus richtet es eine eBGP-Peering-Sitzung von jedem ACE-Netzwerkgerät zu einem lokalen Netzwerkgerät ein, um die Konnektivität zwischen Ihrem lokalen Netzwerk und dem lokalen Gateway herzustellen. Weitere Informationen erhalten Sie unter Service Link BGP-Konnektivität und BGP-Konnektivität für das lokale Gateway.

> **Important**
>
> Service Link-Infrastruktur-Subnetze — Für jedes Compute-Rack, das in Ihrer Outposts-Installation enthalten ist, ist ein Service Link-Infrastruktur-Subnetz (muss /26 sein) erforderlich.

## Stromversorgung

Dies sind die Stromversorgungsanforderungen für ein ACE-Rack.

| Anforderung | Spezifikation |
|---|---|
| Netzspannung (Wechselstrom) | Einphasig 200 bis 240 VAC; 50 oder 60 Hz |
| Stromverbrauch | 10 kVA einphasig (AA+BB) |
| Wechselstromschutz (vorgeschaltete Leistungsschalter) | Nur für 2N-Eingänge (redundant): C-Kurve-, D-Kurve- oder K-Kurven-Schutzschalter.<br><br>B-Kurve oder niedriger wird nicht unterstützt. |
| Typ des Wechselstromeingangs (Steckdose) | IEC6Peitschensteckertypen 0309 oder L6-30P. |

Bestellen Sie einen , um loszulegen. Starten Sie nach der Installation Ihrer Outpost-Geräte eine EC2 Amazon-Instance und konfigurieren Sie die Konnektivität zu Ihrem lokalen Netzwerk.

Aufgaben

- Eine Bestellung für ein Outposts-Rack erstellen
- Starten Sie eine Instance in Ihrem Outposts-Rack
- Optimieren Sie Amazon EC2 für AWS Outposts

# Eine Bestellung für ein Outposts-Rack erstellen

Um mit der Nutzung beginnen zu können AWS Outposts, müssen Sie einen Outpost erstellen und Outpost-Kapazität bestellen.

Voraussetzungen

- Sehen Sie sich die verfügbaren Konfigurationen für Ihre Outposts-Racks an.
- Ein Outpost-Standort ist der physische Standort für Ihre Outpost-Ausrüstung. Stellen Sie vor der Bestellung von Kapazitäten sicher, dass Ihr Standort die Anforderungen erfüllt. Weitere Informationen finden Sie unter Standortanforderungen für Outposts-Racks.
- Sie müssen über einen AWS Enterprise Support Plan oder einen AWS Enterprise On-Ramp Support Plan verfügen.
- Bestimme, welche AWS-Konto du verwenden wirst, um die Outposts-Website zu erstellen, erstelle den Outpost und gib die Bestellung auf. Suchen Sie in der mit diesem Konto verknüpften E-Mail-Adresse nach Informationen von. AWS

Aufgaben

- Schritt 1: Erstellen eines Standorts
- Schritt 2: Erstellen eines Outpost
- Schritt 3: Bestellung
- Schritt 4: Ändern Sie die Instanzkapazität
- Nächste Schritte

# Schritt 1: Erstellen eines Standorts

Erstellen Sie einen Standort, um die Betriebsadresse anzugeben. Die Betriebsadresse ist der physische Standort für Ihre Outposts-Racks.

Voraussetzungen

- Bestimmen Sie die Betriebsadresse.

So erstellen Sie einen Standort:

1. Melden Sie sich an bei AWS.
2. Öffnen Sie die AWS Outposts Konsole unter https://console.aws.amazon.com/outposts/.
3. Um das übergeordnete Element auszuwählen AWS-Region, verwenden Sie die Regionsauswahl in der oberen rechten Ecke der Seite.
4. Wählen Sie im Navigationsbereich Standorte aus.
5. Wählen Sie Create site (Standort erstellen).
6. Wählen Sie unter Unterstützter Hardwaretyp die Option Racks und Server.
7. Geben Sie einen Namen, eine Beschreibung und eine Betriebsadresse für Ihren Standort ein.
8. Geben Sie unter Standortdetails die angeforderten Informationen über den Standort an.
   - Höchstgewicht – Das maximale Gewicht des Racks für diesen Standort in Pfund.
   - Leistungsaufnahme – Die Leistungsaufnahme in kVA, die an der Hardwareposition für das Rack verfügbar ist.
   - Stromoption – Die Stromoption, die Sie für die Hardware bereitstellen können.
   - Stromanschluss – Der Stromanschluss, den AWS für die Verbindungen zur Hardware vorsehen sollte.
   - Stromzufuhr – Geben Sie an, ob die Stromversorgung über oder unter dem Rack erfolgt.
   - Uplink-Geschwindigkeit – Die Uplink-Geschwindigkeit, die das Rack für die Verbindung mit der Region unterstützen soll, in Gbit/s.
   - Anzahl der Uplinks – Die Anzahl der Uplinks für jedes Outpost-Netzwerkgerät, das Sie verwenden möchten, um das Rack mit Ihrem Netzwerk zu verbinden.
   - Glasfasertyp – Der Glasfasertyp, den Sie verwenden werden, um das Rack an Ihr Netzwerk anzuschließen.

- Optischer Standard – Der Typ des optischen Standards, den Sie verwenden werden, um das Rack an Ihr Netzwerk anzuschließen.

9. (Optional) Geben Sie für Hinweise zur Website alle weiteren Informationen ein, die für AWS Sie nützlich sein könnten, um mehr über die Site zu erfahren.
10. Lesen Sie die Anforderungen an die Einrichtung und wählen Sie Ich habe die Anforderungen der Einrichtung gelesen.
11. Wählen Sie Create site (Standort erstellen).

## Schritt 2: Erstellen eines Outpost

Erstellen Sie einen Outpost für Ihre Racks. Geben Sie dann diesen Outpost an, wenn Sie Ihre Bestellung aufgeben.

Voraussetzungen

- Bestimmen Sie die AWS Availability Zone, die Sie Ihrer Site zuordnen möchten.

Erstellen eines Outpost

1. Wählen Sie im Navigationsbereich Outposts aus.
2. Wählen Sie Outposts erstellen.
3. Wählen Sie Racks.
4. Geben Sie für Ihren Outpost einen Namen und eine Beschreibung ein.
5. Wählen Sie eine Availability Zone für Ihren Outpost aus.
6. (Optional) Um private Konnektivität zu konfigurieren, wählen Sie Private Konnektivität verwenden aus. Wählen Sie eine VPC und ein Subnetz in derselben AWS-Konto Availability Zone wie Ihr Outpost. Weitere Informationen finden Sie unter the section called “Voraussetzungen”.

   > **Note**
   >
   > Wenn Sie die private Konnektivität für Ihren Outpost entfernen möchten, müssen Sie sich an das Center wenden.AWS -Support

7. Wählen Sie unter Site-ID Ihren Standort aus.
8. Wählen Sie Outposts erstellen.

# Schritt 3: Bestellung

Bestellen Sie die Outposts-Racks, die Sie benötigen.

> **Important**
>
> Sie können eine Bestellung nach dem Absenden nicht mehr bearbeiten. Prüfen Sie daher alle Details sorgfältig, bevor Sie sie absenden. Wenn Sie eine Bestellung ändern müssen, wenden Sie sich an Ihren AWS Account Manager.

## Voraussetzungen

- Bestimmen Sie, wie Sie für die Bestellung bezahlen werden. Sie haben folgende Optionen: Vollständige Vorauszahlung, Teilweise Vorauszahlung oder Keine Vorauszahlung. Wenn Sie sich nicht dafür entscheiden, alles im Voraus zu zahlen, zahlen Sie während der Vertragslaufzeit monatliche Gebühren.

  Die Preise beinhalten Lieferung, Installation, Wartung von Infrastruktur-Services sowie Softwarepatches und Upgrades.
- Bestimmen Sie, ob sich die Lieferadresse von der Betriebsadresse unterscheidet, die Sie für Standort angegeben haben.

## So bestellen Sie

1. Wählen Sie im Navigationsbereich Bestellungen aus.
2. Wählen Sie Bestellung aufgeben.
3. Wählen Sie unter Unterstützter Hardwaretyp die Option Racks aus.
4. Um Kapazität hinzuzufügen, wählen Sie eine Konfiguration aus. Wenn die verfügbaren Konfigurationen nicht Ihren Anforderungen entsprechen, wenden Sie sich an das AWS -Support Center, um eine benutzerdefinierte Kapazitätskonfiguration anzufordern.
5. Wählen Sie Weiter aus.
6. Wählen Sie Vorhandenen Outpost verwenden und wählen Sie Ihren Outpost aus.
7. Wählen Sie Weiter aus.
8. Wählen Sie eine Vertragslaufzeit und eine Zahlungsoption aus.

9. Geben Sie die Lieferadresse an. Sie können eine neue Adresse angeben oder die Betriebsadresse des Standorts auswählen. Wenn Sie die Betriebsadresse auswählen, beachten Sie bitte, dass jede künftige Änderung der Betriebsadresse des Standorts sich nicht auf bestehende Bestellungen auswirken wird. Wenn Sie den Namen und die Adresse der Versandadresse für eine bestehende Bestellung ändern müssen, wenden Sie sich an Ihren AWS Kundenbetreuer.
10. Wählen Sie Weiter aus.
11. Vergewissern Sie sich auf der Seite Überprüfen und Bestellen, dass Ihre Informationen korrekt sind, und bearbeiten Sie sie nach Bedarf. Sie können die Bestellung nicht mehr bearbeiten, nachdem Sie sie abgeschickt haben.
12. Wählen Sie Bestellung aufgeben.

## Schritt 4: Ändern Sie die Instanzkapazität

Ein Outpost stellt einen Pool an AWS Rechen- und Speicherkapazität an Ihrem Standort als private Erweiterung einer Availability Zone in einer AWS Region bereit. Da die im Outpost verfügbare Rechen- und Speicherkapazität begrenzt ist und durch die Größe und Anzahl der an Ihrem Standort installierten Racks bestimmt AWS wird, können Sie entscheiden, wie viel AWS Outposts Kapazität von Amazon EC2, Amazon EBS und Amazon S3 Sie benötigen, um Ihre anfänglichen Workloads auszuführen, future Wachstum zu bewältigen und zusätzliche Kapazität bereitzustellen, um Serverausfälle und Wartungsereignisse zu minimieren.

Die Kapazität jeder neuen Outpost-Bestellung wird mit einer Standardkapazitätskonfiguration konfiguriert. Sie können die Standardkonfiguration konvertieren, um verschiedene Instanzen zu erstellen, die Ihren Geschäftsanforderungen entsprechen. Dazu erstellen Sie eine Kapazitätsaufgabe, geben die Instanzgrößen und die Menge an und führen die Kapazitätsaufgabe aus, um die Änderungen zu implementieren.

> **Note**
>
> - Sie können die Anzahl der Instanzgrößen ändern, nachdem Sie die Bestellung für Ihre Outposts aufgegeben haben.
> - Die Größen und Mengen der Instances werden auf Outpost-Ebene definiert.
> - Instanzen werden automatisch auf der Grundlage von Best Practices platziert.

Um die Instanzkapazität zu ändern

1. Wählen Sie im linken Navigationsbereich der AWS Outposts Konsole Capacity tasks aus.
2. Wählen Sie auf der Seite Kapazitätsaufgaben die Option Kapazitätsaufgabe erstellen aus.
3. Wählen Sie auf der Seite Erste Schritte die Bestellung aus.
4. Um die Kapazität zu ändern, können Sie die Schritte in der Konsole verwenden oder eine JSON-Datei hochladen.

Console steps

1. Wählen Sie „Outpost-Kapazitätskonfiguration ändern“ aus.
2. Wählen Sie Weiter aus.
3. Auf der Seite Instance-Kapazität konfigurieren wird für jeden Instance-Typ eine Instance-Größe angezeigt, wobei die maximale Anzahl vorausgewählt ist. Um weitere Instance-Größen hinzuzufügen, wählen Sie Instance-Größe hinzufügen.
4. Geben Sie die Anzahl der Instances an und notieren Sie sich die Kapazität, die für diese Instance-Größe angezeigt wird.
5. Sehen Sie sich die Meldung am Ende jedes Abschnitts mit dem Instanztyp an, in der Sie darüber informiert werden, ob Ihre Kapazität zu hoch oder zu niedrig ist. Nehmen Sie Anpassungen auf der Ebene der Instance-Größe oder Menge vor, um Ihre verfügbare Gesamtkapazität zu optimieren.
6. Sie können auch beantragen AWS Outposts , die Instance-Menge für eine bestimmte Instance-Größe zu optimieren. Gehen Sie hierzu wie folgt vor:
   a. Wählen Sie die Instanzgröße.
   b. Wählen Sie am Ende des entsprechenden Abschnitts mit dem Instanztyp die Option Automatisches Ausgleichen aus.
7. Stellen Sie für jeden Instance-Typ sicher, dass die Instance-Menge für mindestens eine Instance-Größe angegeben ist.
8. Wählen Sie Weiter aus.
9. Überprüfen Sie auf der Seite Überprüfen und erstellen, welche Aktualisierungen Sie anfordern.
10. Wählen Sie „Erstellen“. AWS Outposts erstellt eine Kapazitätsaufgabe.
11. Überwachen Sie auf der Seite mit den Kapazitätsaufgaben den Status der Aufgabe.

> **Note**
>
> - AWS Outposts fordert Sie möglicherweise auf, eine oder mehrere laufende Instances zu beenden, um die Ausführung der Kapazitätsaufgabe zu ermöglichen. Nachdem Sie diese Instanzen beendet haben, AWS Outposts wird die Aufgabe ausgeführt.
> - Wenn Sie Ihre Kapazität nach Abschluss Ihrer Bestellung ändern müssen, wenden Sie sich an das AWS -Support Center, um die Änderungen vorzunehmen.

Upload a JSON file

1. Wählen Sie Kapazitätskonfiguration hochladen aus.
2. Wählen Sie Weiter aus.
3. Laden Sie auf der Seite Kapazitätskonfigurationsplan hochladen die JSON-Datei hoch, die den Instanztyp, die Größe und die Menge angibt.

   Example

   Beispiel für eine JSON-Datei:

   ```
   {
       "InstancePools": [
           {
               "InstanceType": "c5.24xlarge",
               "Count": 1
           },
           {
               "InstanceType": "m5.24xlarge",
               "Count": 2
           }
       ]
   }
   ```

4. Überprüfen Sie den Inhalt der JSON-Datei im Abschnitt Kapazitätskonfigurationsplan.
5. Wählen Sie Weiter aus.
6. Überprüfen Sie auf der Seite Überprüfen und erstellen, welche Aktualisierungen Sie anfordern.

7. Wählen Sie „Erstellen“. AWS Outposts erstellt eine Kapazitätsaufgabe.
8. Überwachen Sie auf der Seite mit den Kapazitätsaufgaben den Status der Aufgabe.

> **Note**
>
> - AWS Outposts fordert Sie möglicherweise auf, eine oder mehrere laufende Instances zu beenden, um die Ausführung der Kapazitätsaufgabe zu ermöglichen. Nachdem Sie diese Instanzen beendet haben, AWS Outposts wird die Aufgabe ausgeführt.
> - Wenn Sie Ihre Kapazität nach Abschluss Ihrer Bestellung ändern müssen, wenden Sie sich an das AWS -Support Center, um die Änderungen vorzunehmen.
> - Informationen zur Behebung von Problemen finden Sie unter Behebung von Problemen mit Kapazitätsaufgaben.

## Nächste Schritte

Sie können den Status Ihrer Bestellung über die AWS Outposts Konsole einsehen. Der ursprüngliche Status Ihrer Bestellung lautet Bestellung eingegangen. Wenn Sie Fragen zu Ihrer Bestellung haben, wenden Sie sich an AWS -Support das Center.

Um die Bestellung zu erfüllen, vereinbaren AWS wir mit Ihnen einen Termin und eine Uhrzeit.

Sie erhalten außerdem eine Checkliste mit Punkten, die Sie vor der Installation überprüfen oder bereitstellen müssen. Das AWS Installationsteam wird zum geplanten Datum und zur geplanten Uhrzeit an Ihrem Standort eintreffen. Das Team bringt das Rack an die angegebene Position und Ihr Elektriker kann das Rack an die Stromversorgung anschließen. Das Team stellt über den von Ihnen bereitgestellten Uplink die Netzwerkkonnektivität für das Outposts-Rack her und konfiguriert die Kapazität des Racks. Die Installation ist abgeschlossen, wenn Sie bestätigen, dass die Amazon EC2 - und Amazon EBS-Kapazität für Ihren Outpost von Ihrem AWS Konto aus verfügbar ist.

# Starten Sie eine Instance in Ihrem Outposts-Rack

Nach der Installation Ihres Outpost und der verfügbaren Datenverarbeitungs- und Speicherkapazität können Sie mit der Erstellung von Ressourcen beginnen. Starten Sie EC2 Amazon-Instances und erstellen Sie Amazon EBS-Volumes auf Ihrem Outpost mithilfe eines Outpost-Subnetzes. Sie können

auch Snapshots von Amazon EBS-Volumes auf Ihrem Outpost erstellen. Weitere Informationen finden Sie unter Lokale Amazon EBS-Snapshots AWS Outposts im Amazon EBS-Benutzerhandbuch.

Voraussetzung

Sie müssen einen Outpost an Ihrem Standort installiert haben. Weitere Informationen finden Sie unter Bestellung für ein Outposts-Rack erstellen.

Aufgaben

- Schritt 1: Erstellen einer VPC
- Schritt 2: Erstellen Sie ein Subnetz und eine benutzerdefinierte Routentabelle
- Schritt 3: Konfigurieren Sie die lokale Gateway-Konnektivität
- Schritt 4: Konfigurieren Sie das lokale Netzwerk
- Schritt 5: Starten Sie eine Instanz auf dem Outpost
- Schritt 6: Testen Sie die Konnektivität

## Schritt 1: Erstellen einer VPC

Du kannst jede VPC in der AWS Region auf deinen Außenposten ausdehnen. Überspringen Sie diesen Schritt, wenn Sie bereits über eine VPC verfügen, die Sie verwenden können.

Um eine VPC für Ihren Outpost zu erstellen

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie dieselbe Region wie das Outposts-Rack.
3. Wählen Sie im Navigationsbereich Your VPCs und dann Create VPC aus.
4. Wählen Sie nur VPC.
5. (Optional) Geben Sie für das Name-Tag einen Namen für die VPC ein.
6. Wählen Sie für IPv4 CIDR-Block die Option IPv4 CIDR Manual Input und geben Sie den IPv4 Adressbereich für die VPC in das IPv4CIDR-Textfeld ein.

> **Note**
>
> Wenn Sie direktes VPC-Routing verwenden möchten, geben Sie einen CIDR-Bereich an, der sich nicht mit dem IP-Bereich überschneidet, den Sie in Ihrem lokalen Netzwerk verwenden.

7. Wählen Sie für IPv6 CIDR-Block die Option Kein CIDR-Block aus. IPv6
8. Wählen Sie für Tenancy die Option Standard aus.
9. (Optional) Um Ihrer VPC ein Tag hinzuzufügen, wählen Sie Tag hinzufügen aus und geben Sie einen Schlüssel und einen Wert ein.
10. Wählen Sie VPC erstellen aus.

## Schritt 2: Erstellen Sie ein Subnetz und eine benutzerdefinierte Routentabelle

Sie können ein Outpost-Subnetz erstellen und zu jeder VPC in der AWS Region hinzufügen, in der der Outpost beheimatet ist. Wenn Sie dies tun, schließt die VPC den Outpost mit ein. Weitere Informationen finden Sie unter Netzwerkkomponenten.

> **Note**
>
> Wenn Sie eine Instance in einem Outpost-Subnetz starten, das von einem anderen für Sie freigegeben wurde AWS-Konto, fahren Sie mit Schritt 5: Starten einer Instance auf dem Outpost fort.

2a: Erstellen Sie ein Outpost-Subnetz

Um ein Outpost-Subnetz zu erstellen

1. Öffnen Sie die AWS Outposts Konsole unter. https://console.aws.amazon.com/outposts/
2. Wählen Sie im Navigationsbereich Outposts aus.
3. Wählen Sie den Outpost aus und klicken Sie dann auf Aktionen, Subnetz erstellen. Sie werden zum Erstellen eines Subnetzes in der Amazon-VPC-Konsole umgeleitet. Wir wählen für Sie den Outpost und die Availability Zone aus, in der sich der Outpost befindet.
4. Wählen Sie eine VPC aus.
5. Geben Sie in den Subnetzeinstellungen optional Ihrem Subnetz einen Namen und einen IP-Adressbereich für das Subnetz an.
6. Wählen Sie Subnetz erstellen.

7. (Optional) Um die Identifizierung von Outpost-Subnetzen zu vereinfachen, aktivieren Sie auf der Seite Subnetze die Spalte Outpost ID. Um die Spalte zu aktivieren, klicken Sie auf das Symbol Einstellungen, wählen Sie Outpost ID und anschließend Bestätigen aus.

### 2b: Erstellen Sie eine benutzerdefinierte Routing-Tabelle

Verwenden Sie das folgende Verfahren, um eine benutzerdefinierte Routing-Tabelle mit einer Route zum lokalen Gateway zu erstellen. Sie können nicht dieselbe Routing-Tabelle wie die Availability Zone-Subnetze verwenden.

So erstellen Sie eine benutzerdefinierte Routing-Tabelle

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Routing-Tabellen aus.
3. Klicken Sie auf Create Route Table (Routing-Tabelle erstellen).
4. (Optional) Geben Sie bei Name einen Namen für Ihre Routing-Tabelle ein.
5. Wählen Sie unter VPC Ihre VPC aus.
6. (Optional) Sie fügen ein Tag hinzu, indem Sie Add new tag (Neuen Tag hinzufügen) auswählen und den Tag-Schlüssel und -Wert eingeben.
7. Klicken Sie auf Create Route Table (Routing-Tabelle erstellen).

### 2c: Ordnen Sie das Outpost-Subnetz und die benutzerdefinierte Routentabelle zu

Damit die Routen einer Routing-Tabelle auf ein bestimmtes Subnetz angewendet werden, müssen Sie die Routing-Tabelle dem Subnetz zuordnen. Eine Routing-Tabelle kann mehreren Subnetzen zugeordnet werden. Ein Subnetz kann jedoch jeweils nur einer Routing-Tabelle zugeordnet werden. Wenn ein Subnetz nicht ausdrücklich einer Routing-Tabelle zugeordnet ist, wird es standardmäßig implizit der Haupt-Routing-Tabelle zugeordnet.

Um das Outpost-Subnetz und die benutzerdefinierte Routentabelle zu verknüpfen

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich die Option Routentabellen aus.
3. Wählen Sie auf der Registerkarte Subnet associations (Subnetzzuordnungen) die Option Edit subnet associations (Subnetzzuordnungen bearbeiten) aus.
4. Aktivieren Sie das Kontrollkästchen für das Subnetz, um es der Routing-Tabelle zuzuordnen.

5. Klicken Sie auf Save associations (Zuordnungen speichern).

## Schritt 3: Konfigurieren Sie die lokale Gateway-Konnektivität

Das lokale Gateway (LGW) ermöglicht die Konnektivität zwischen Ihren Outpost-Subnetzen und Ihrem lokalen Netzwerk.

Weitere Informationen zum LGW finden Sie unter Lokale Gateways.

Um Konnektivität zwischen einer Instance im Outposts-Subnetz und Ihrem lokalen Netzwerk bereitzustellen, müssen Sie die folgenden Aufgaben ausführen.

3a. Erstellen Sie eine benutzerdefinierte Routentabelle für das lokale Gateway

Gehen Sie wie folgt vor, um eine benutzerdefinierte Routentabelle für Ihr lokales Gateway zu erstellen.

So erstellen Sie eine benutzerdefinierte Routentabelle für das lokale Gateway

1. Öffnen Sie die AWS Outposts Konsole unter https://console.aws.amazon.com/outposts/.
2. Um das zu ändern AWS-Region, verwenden Sie die Regionsauswahl in der oberen rechten Ecke der Seite.
3. Wählen Sie im Navigationsbereich Lokale Gateway-Routing-Tabelle aus.
4. Wählen Sie Lokale Gateway-Routing-Tabelle erstellen aus.
5. (Optional) Geben Sie bei Name einen Namen für Ihre Routing-Tabelle ein.
6. Wählen Sie unter Lokales Gateway Ihr lokales Gateway aus.
7. Wählen Sie unter Modus einen Modus für die Kommunikation mit Ihrem On-Premises-Netzwerk aus.
   - Wählen Sie Direct VPC Routing, um die privaten IP-Adressen Ihrer Instances zu verwenden.
   - Wählen Sie CoIP, um Adressen aus Ihren kundeneigenen IP-Adresspools zu verwenden. Weitere Informationen finden Sie unter Einen CoIP-Pool erstellen.
8. (Optional) Um einen Tag hinzuzufügen, wählen Sie Neuen Tag hinzufügen und geben Sie einen Tag-Schlüssel und einen Tag-Wert ein.
9. Wählen Sie Lokale Gateway-Routing-Tabelle erstellen aus.

### 3b: Ordnen Sie die VPC der benutzerdefinierten Routentabelle zu

Verwenden Sie das folgende Verfahren, um Ihrer lokalen Gateway-Routentabelle eine VPC zuzuordnen. Sie sind standardmäßig nicht verknüpft.

So verknüpfen Sie eine VPC mit der benutzerdefinierten Routentabelle für das lokale Gateway

1. Öffnen Sie die AWS Outposts Konsole unter. https://console.aws.amazon.com/outposts/
2. Um das zu ändern AWS-Region, verwenden Sie die Regionsauswahl in der oberen rechten Ecke der Seite.
3. Wählen Sie im Navigationsbereich Lokale Gateway-Routing-Tabellen aus.
4. Wählen Sie die Routing-Tabelle aus und klicken Sie dann auf Aktionen, VPC zuordnen.
5. Wählen Sie für VPC-ID die VPC aus, die der lokalen Gateway-Routing-Tabelle zugeordnet werden soll.
6. (Optional) Um einen Tag hinzuzufügen, wählen Sie Neuen Tag hinzufügen und geben Sie einen Tag-Schlüssel und einen Tag-Wert ein.
7. Wählen Sie Associate VPC (VPC zuordnen) aus.

### 3c: Fügen Sie einen Routeneintrag in der Outpost-Subnetz-Routentabelle hinzu

Fügen Sie der Outpost-Subnetz-Routentabelle einen Routeneintrag hinzu, um den Verkehr zwischen den Outpost-Subnetzen und dem lokalen Gateway zu ermöglichen.

Outpost-Subnetze innerhalb einer VPC, die mit einer lokalen Gateway-Routentabelle verknüpft ist, können einen zusätzlichen Zieltyp, eine Outpost Local Gateway-ID, für ihre Routing-Tabellen haben. Stellen Sie sich den Fall vor, dass Sie den Verkehr mit der Zieladresse 172.16.100.0/24 über das lokale Gateway an das Kundennetzwerk weiterleiten möchten. Bearbeiten Sie dazu die Outpost-Subnetz-Routentabelle und fügen Sie die folgende Route mit dem Zielnetzwerk und einem Ziel des lokalen Gateways hinzu.

| Bestimmungsort | Ziel |
| --- | --- |
| 172.16.100.0/24 | `lgw-id` |

Um einen Routeneintrag mit dem lokalen Gateway als Ziel in der Subnetz-Routentabelle hinzuzufügen

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich die Option Routentabellen und dann die Routentabelle aus, in 2b: Erstellen Sie eine benutzerdefinierte Routing-Tabelle der Sie sie erstellt haben.
3. Wählen Sie Aktionen und dann Routen bearbeiten aus.
4. Um eine Route hinzuzufügen, wählen Sie Add route (Route hinzufügen).
5. Geben Sie als Ziel den CIDR-Zielblock für das Kundennetzwerk ein.
6. Wählen Sie für Target die Outpost Local Gateway ID aus.
7. Wählen Sie Änderungen speichern  aus.

3d: Erstellen Sie eine lokale Gateway-Routingdomäne, indem Sie die benutzerdefinierte Routentabelle den VIF-Gruppen zuordnen

VIF-Gruppen sind logische Gruppierungen virtueller Schnittstellen (). VIFs Ordnen Sie die lokale Gateway-Routentabelle der VIF-Gruppe zu, um eine lokale Gateway-Routingdomäne zu erstellen.

Um die benutzerdefinierte Routentabelle den VIF-Gruppen zuzuordnen

1. Öffnen Sie die AWS Outposts Konsole unter. https://console.aws.amazon.com/outposts/
2. Um das zu ändern AWS-Region, verwenden Sie die Regionsauswahl in der oberen rechten Ecke der Seite.
3. Wählen Sie im Navigationsbereich Networking und dann LGW-Routing-Domain aus.
4. Wählen Sie LGW-Routingdomäne erstellen aus.
5. Geben Sie einen Namen für die lokale Gateway-Routingdomäne ein.
6. Wählen Sie das lokale Gateway, die lokale Gateway-VIF-Gruppe und die lokale Gateway-Routentabelle aus.
7. Wählen Sie Create LGW-Routing-Domain aus.

3e: Fügen Sie einen Routeneintrag zur Routentabelle hinzu

Bearbeiten Sie die Routentabelle des lokalen Gateways, um eine statische Route hinzuzufügen, die die VIF-Gruppe als Ziel und Ihren lokalen Subnetz-CIDR-Bereich (oder 0.0.0.0/0) als Ziel hat.

| Bestimmungsort | Ziel |
| --- | --- |
| 172.16.100.0/24 | `VIF-Group-ID` |

Um einen Routeneintrag zur LGW-Routentabelle hinzuzufügen

1. Öffnen Sie die AWS Outposts Konsole unter. https://console.aws.amazon.com/outposts/
2. Wählen Sie im Navigationsbereich Lokale Gateway-Routing-Tabelle aus.
3. Wählen Sie die Routentabelle des lokalen Gateways aus und klicken Sie dann auf Aktionen, Routen bearbeiten.
4. Wählen Sie Route hinzufügen aus.
5. Geben Sie unter Zielbereich den Ziel-CIDR-Block, eine einzelne IP-Adresse oder die ID einer Präfixliste ein.
6. Wählen Sie unter Target die ID des lokalen Gateways aus.
7. Wählen Sie Save Rules (Routen speichern) aus.

3f: (Optional) Weisen Sie der Instanz eine kundeneigene IP-Adresse zu

Wenn Sie Ihre Outposts so konfiguriert haben, dass 3a. Erstellen Sie eine benutzerdefinierte Routentabelle für das lokale Gateway sie einen kundeneigenen IP-Adresspool (CoIP) verwenden, müssen Sie eine Elastic IP-Adresse aus dem CoIP-Adresspool zuweisen und die Elastic IP-Adresse der Instance zuordnen. Weitere Informationen finden Sie unter Kundeneigene IP-Adressen.

Wenn Sie Ihre Outposts für die Verwendung von Direct VPC Routing (DVR) konfiguriert haben, überspringen Sie diesen Schritt.

Freigegebene kundeneigene IP-Adresspools

Wenn Sie einen freigegebenen, kundeneigenen IP-Adresspool verwenden möchten, muss der Pool gemeinsam genutzt werden, bevor Sie mit der Konfiguration beginnen. Informationen darüber, wie Sie eine Kundenadresse teilen können, finden Sie unter. IPv4 the section called “Eine Outpost-Ressource freigeben”

# Schritt 4: Konfigurieren Sie das lokale Netzwerk

Der Outpost richtet ein externes BGP-Peering von jedem Outpost Networking Device (OND) zu einem Customer Local Network Device (CND) ein, um Traffic von Ihrem lokalen Netzwerk an die Outposts zu senden und zu empfangen.

Weitere Informationen finden Sie unter BGP-Konnektivität mit lokalem Gateway.

Um Datenverkehr von Ihrem lokalen Netzwerk an den Outpost zu senden und zu empfangen, stellen Sie sicher, dass:

- Auf den Netzwerkgeräten Ihrer Kunden befindet sich die BGP-Sitzung auf dem lokalen Gateway-VLAN von Ihren Netzwerkgeräten aus im Status AKTIV.
- Stellen Sie bei Traffic, der von lokalen Standorten zu Outposts geleitet wird, sicher, dass Sie in Ihrem CND die BGP-Werbung von Outposts erhalten. Diese BGP-Werbung enthält die Routen, die Ihr lokales Netzwerk verwenden muss, um den Verkehr vom lokalen Standort zu Outpost weiterzuleiten. Stellen Sie daher sicher, dass Ihr Netzwerk über das richtige Routing zwischen Outposts und den lokalen Ressourcen verfügt.
- Stellen Sie bei Datenverkehr, der von Outposts zum lokalen Netzwerk fließt, sicher, dass Sie CNDs die BGP-Routenankündigungen der lokalen Netzwerksubnetze an Outposts (oder 0.0.0.0/0) senden. Als Alternative können Sie eine Standardroute (z. B. 0.0.0.0/0) zu Outposts ankündigen. Die von der angekündigten lokalen Subnetze CNDs müssen einen CIDR-Bereich haben, der dem CIDR-Bereich entspricht oder in diesem enthalten ist, in dem Sie konfiguriert haben. 3e: Fügen Sie einen Routeneintrag zur Routentabelle hinzu

Beispiel: BGP-Werbung im Direct VPC-Modus

Stellen Sie sich das Szenario vor, in dem Sie einen Outpost haben, der im Direct VPC-Modus konfiguriert ist, mit zwei Outposts-Rack-Netzwerkgeräten, die über ein lokales Gateway-VLAN mit zwei lokalen Netzwerkgeräten des Kunden verbunden sind. Folgendes ist konfiguriert:

- Eine VPC mit einem CIDR-Block 10.0.0.0/16.
- Ein Outpost-Subnetz in der VPC mit einem CIDR-Block 10.0.3.0/24.
- Ein Subnetz im lokalen Netzwerk mit einem CIDR-Block 172.16.100.0/24
- Outposts verwendet die private IP-Adresse der Instances im Outpost-Subnetz, z. B. 10.0.3.0/24, um mit Ihrem lokalen Netzwerk zu kommunizieren.

In diesem Szenario wird die Route wie folgt angekündigt:

- Das lokale Gateway zu Ihren Kundengeräten ist 10.0.3.0/24.
- Ihre Kundengeräte zum lokalen Outpost-Gateway sind 172.16.100.0/24.

Infolgedessen sendet das lokale Gateway ausgehenden Datenverkehr mit dem Zielnetzwerk 172.16.100.0/24 an Ihre Kundengeräte. Stellen Sie sicher, dass Ihr Netzwerk über die richtige Routing-Konfiguration verfügt, um den Datenverkehr an den Zielhost in Ihrem Netzwerk weiterzuleiten.

Die spezifischen Befehle und die Konfiguration, die zur Überprüfung des Status der BGP-Sitzungen und der beworbenen Routen innerhalb dieser Sitzungen erforderlich sind, finden Sie in der Dokumentation Ihres Netzwerkanbieters.

Informationen zur Fehlerbehebung finden Sie in der Checkliste zur Fehlerbehebung bei AWS Outposts Rack-Netzwerken.

Beispiel: BGP-Werbung im CoIP-Modus

Stellen Sie sich das Szenario vor, in dem Sie einen Outpost mit zwei Outposts-Rack-Netzwerkgeräten haben, die über ein lokales Gateway-VLAN mit zwei lokalen Netzwerkgeräten des Kunden verbunden sind. Folgendes ist konfiguriert:

- Eine VPC mit einem CIDR-Block 10.0.0.0/16.
- Ein Subnetz in der VPC mit einem CIDR-Block 10.0.3.0/24.
- Ein kundeneigener IP-Pool (10.1.0.0/26).
- Eine Elastic IP-Adresszuweisung, die 10.0.3.112 mit 10.1.0.2 verknüpft.
- Ein Subnetz im lokalen Netzwerk mit einem CIDR-Block 172.16.100.0/24
- Bei der Kommunikation zwischen Ihrem Outpost und dem lokalen Netzwerk wird CoIP Elastic verwendet, um Instances im Outpost IPs zu adressieren. Der VPC-CIDR-Bereich wird nicht verwendet.

In diesem Szenario wird die Route angekündigt von:

- Das lokale Gateway zu Ihren Kundengeräten ist 10.1.0.0/26.
- Ihre Kundengeräte zum lokalen Outpost-Gateway sind 172.16.100.0/24.

Infolgedessen sendet das lokale Gateway ausgehenden Datenverkehr mit dem Zielnetzwerk 172.16.100.0/24 an Ihre Kundengeräte. Stellen Sie sicher, dass Ihr Netzwerk über die richtige Routing-Konfiguration verfügt, um den Datenverkehr an den Zielhost in Ihrem Netzwerk weiterzuleiten.

Die spezifischen Befehle und die Konfiguration, die zur Überprüfung des Status der BGP-Sitzungen und der beworbenen Routen innerhalb dieser Sitzungen erforderlich sind, finden Sie in der Dokumentation Ihres Netzwerkanbieters.

Informationen zur Fehlerbehebung finden Sie in der Checkliste zur Fehlerbehebung bei AWS Outposts Rack-Netzwerken.

Informationen zur Fehlerbehebung finden Sie in der Checkliste zur Fehlerbehebung bei AWS Outposts Rack-Netzwerken.

## Schritt 5: Starten Sie eine Instanz auf dem Outpost

Sie können EC2 Instances im Outpost-Subnetz, das Sie erstellt haben, oder in einem Outpost-Subnetz, das mit Ihnen geteilt wurde, starten. Sicherheitsgruppen steuern den eingehenden und ausgehenden VPC-Datenverkehr für Instances in einem Outpost-Subnetz genauso wie für Instances in einem Availability Zone-Subnetz. Um eine Verbindung zu einer EC2 Instance in einem Outpost-Subnetz herzustellen, können Sie beim Starten der Instance ein key pair angeben, genau wie bei Instances in einem Availability Zone-Subnetz.

Überlegungen

- Wenn Sie während des Instance-Startvorgangs auf Outpost Blockdatenvolumes anhängen, die von kompatiblen Blockspeichersystemen von Drittanbietern unterstützt werden, finden Sie weitere Informationen in diesem Blogbeitrag Vereinfachung der Verwendung von Blockspeicher von Drittanbietern mit. AWS Outposts
- Sie können eine Platzierungsgruppe erstellen, um zu beeinflussen, wie Amazon versuchen EC2 soll, Gruppen voneinander abhängiger Instances auf der Outposts-Hardware zu platzieren. Sie können die Platzierungsgruppenstrategie wählen, die den Anforderungen Ihres Workloads entspricht.
- Wenn Ihr Outpost für die Verwendung eines kundeneigenen IP-Adresspools (CoIP) konfiguriert wurde, müssen Sie allen Instances, die Sie starten, eine kundeneigene IP-Adresse zuweisen.

So starten Sie Instances in Ihrem Outpost-Subnetz

1. Öffnen Sie die AWS Outposts Konsole unter. https://console.aws.amazon.com/outposts/
2. Wählen Sie im Navigationsbereich Outposts aus.
3. Wählen Sie Ihren Outpost aus und klicken Sie anschließend auf Aktionen, Details anzeigen.
4. Wählen Sie auf der Outpost-Übersichtsseite die Option Instance starten aus. Sie werden zum Instance-Startassistenten in der EC2 Amazon-Konsole weitergeleitet. Wir wählen das Outpost-Subnetz für Sie aus und zeigen Ihnen nur die Instance-Typen, die von Ihrem Outposts-Rack unterstützt werden.
5. Wählen Sie einen Instance-Typ, der von Ihrem Outposts-Rack unterstützt wird. Beachten Sie, dass Instances, die ausgegraut erscheinen, nicht verfügbar sind.
6. (Optional) Um die Instances in einer Platzierungsgruppe zu starten, erweitern Sie Erweiterte Details und scrollen Sie zur Platzierungsgruppe. Sie können entweder eine bestehende Platzierungsgruppe auswählen oder eine neue Platzierungsgruppe erstellen.
7. Schließen Sie den Assistenten ab, um die Instance in Ihrem Outpost-Subnetz zu starten. Weitere Informationen finden Sie unter Launch an EC2 Instance im  EC2 Amazon-Benutzerhandbuch:

> **Note**
>
> Wenn Sie ein Amazon EBS-Volume hinzufügen, müssen Sie den Volumetyp gp2 verwenden.

## Schritt 6: Testen Sie die Konnektivität

Sie können die Konnektivität anhand der entsprechenden Anwendungsfälle testen.

Die Konnektivität von Ihrem lokalen Netzwerk zum Outpost testen

Führen Sie auf einem Computer in Ihrem lokalen Netzwerk den `ping` Befehl zur privaten IP-Adresse der Outpost-Instanz aus.

```
ping 10.0.3.128
```

Es folgt eine Beispielausgabe.

```
Pinging 10.0.3.128
```

```
Reply from 10.0.3.128:  bytes=32 time=<1ms TTL=128
Reply from 10.0.3.128:  bytes=32 time=<1ms TTL=128
Reply from 10.0.3.128:  bytes=32 time=<1ms TTL=128

Ping statistics for 10.0.3.128
Packets:  Sent = 3,  Received = 3,  Lost = 0 (0% lost)

Approximate round trip time in milliseconds
Minimum = 0ms,  Maximum = 0ms,  Average = 0ms
```

Die Konnektivität von einer Outpost-Instance zu Ihrem lokalen Netzwerk testen

Verwenden Sie je nach Betriebssystem ssh oder rdp, um eine Verbindung zur privaten IP-Adresse Ihrer Outpost-Instance herzustellen. Informationen zum Herstellen einer Verbindung mit einer Linux-Instance finden Sie unter Verbindung zu Ihrer EC2 Instance herstellen im  EC2 Amazon-Benutzerhandbuch.

Nachdem die Instance ausgeführt wurde, führen Sie den `ping`-Befehl für die IP-Adresse eines Computers in Ihrem lokalen Netzwerk aus. Im folgenden Beispiel lautet die IP-Adresse 172.16.0.130.

```
ping 172.16.0.130
```

Es folgt eine Beispielausgabe.

```
Pinging 172.16.0.130

Reply from 172.16.0.130:  bytes=32 time=<1ms TTL=128
Reply from 172.16.0.130:  bytes=32 time=<1ms TTL=128
Reply from 172.16.0.130:  bytes=32 time=<1ms TTL=128

Ping statistics for 172.16.0.130
Packets:  Sent = 3,  Received = 3,  Lost = 0 (0% lost)

Approximate round trip time in milliseconds
Minimum = 0ms,  Maximum = 0ms,  Average = 0ms
```

Testen Sie die Konnektivität zwischen der AWS Region und dem Outpost

Starten Sie eine Instance im Subnetz der AWS Region. Führen Sie zum Beispiel den Befehl run-instances aus.

```
aws ec2 run-instances \
```

```
    --image-id ami-abcdefghi1234567898 \
    --instance-type c5.large \
    --key-name MyKeyPair \
    --security-group-ids sg-1a2b3c4d123456787 \
    --subnet-id subnet-6e7f829e123445678
```

Nach dem Ausführen der Instance führen Sie die folgenden Vorgänge aus:

1. Rufen Sie die private IP-Adresse der Instance in der AWS Region ab. Diese Informationen sind in der EC2 Amazon-Konsole auf der Instance-Detailseite verfügbar.
2. Verwenden Sie je nach Betriebssystem ssh oder rdp, um eine Verbindung zur privaten IP-Adresse Ihrer Outpost-Instance herzustellen.
3. Führen Sie den ping Befehl von Ihrer Outpost-Instance aus und geben Sie die IP-Adresse der Instance in der AWS Region an.

   ```
   ping 10.0.1.5
   ```

   Es folgt eine Beispielausgabe.

   ```
   Pinging 10.0.1.5

   Reply from 10.0.1.5:  bytes=32 time=<1ms TTL=128
   Reply from 10.0.1.5:  bytes=32 time=<1ms TTL=128
   Reply from 10.0.1.5:  bytes=32 time=<1ms TTL=128

   Ping statistics for 10.0.1.5
   Packets:  Sent = 3,  Received = 3,  Lost = 0 (0% lost)

   Approximate round trip time in milliseconds
   Minimum = 0ms,  Maximum = 0ms,  Average = 0ms
   ```

Kundeneigene IP-Adressen-Konnektivitätsbeispiele

Die Konnektivität von Ihrem lokalen Netzwerk zum Outpost testen

Führen Sie auf einem Computer in Ihrem lokalen Netzwerk den `ping`-Befehl zur kundeneigenen IP-Adresse der Outpost-Instance aus.

```
ping 172.16.0.128
```

Es folgt eine Beispielausgabe.

```
Pinging 172.16.0.128

Reply from 172.16.0.128:  bytes=32 time=<1ms TTL=128
Reply from 172.16.0.128:  bytes=32 time=<1ms TTL=128
Reply from 172.16.0.128:  bytes=32 time=<1ms TTL=128

Ping statistics for 172.16.0.128
Packets:  Sent = 3,  Received = 3,  Lost = 0 (0% lost)

Approximate round trip time in milliseconds
Minimum = 0ms,  Maximum = 0ms,  Average = 0ms
```

Die Konnektivität von einer Outpost-Instance zu Ihrem lokalen Netzwerk testen

Verwenden Sie je nach Betriebssystem ssh oder rdp, um eine Verbindung zur privaten IP-Adresse Ihrer Outpost-Instance herzustellen. Weitere Informationen finden Sie unter Connect zu Ihrer EC2 Instance herstellen im  EC2 Amazon-Benutzerhandbuch.

Nachdem die Outpost-Instance ausgeführt wurde, führen Sie den `ping`-Befehl für eine IP-Adresse eines Computers in Ihrem lokalen Netzwerk aus.

```
ping 172.16.0.130
```

Es folgt eine Beispielausgabe.

```
Pinging 172.16.0.130

Reply from 172.16.0.130:  bytes=32 time=<1ms TTL=128
Reply from 172.16.0.130:  bytes=32 time=<1ms TTL=128
Reply from 172.16.0.130:  bytes=32 time=<1ms TTL=128

Ping statistics for 172.16.0.130
Packets:  Sent = 3,  Received = 3,  Lost = 0 (0% lost)

Approximate round trip time in milliseconds
Minimum = 0ms,  Maximum = 0ms,  Average = 0ms
```

Testen Sie die Konnektivität zwischen der AWS Region und dem Outpost

Starten Sie eine Instance im Subnetz der AWS Region. Führen Sie zum Beispiel den Befehl run-instances aus.

```
aws ec2 run-instances \
    --image-id ami-abcdefghi1234567898 \
    --instance-type c5.large \
    --key-name MyKeyPair \
    --security-group-ids sg-1a2b3c4d123456787 \
    --subnet-id subnet-6e7f829e123445678
```

Nach dem Ausführen der Instance führen Sie die folgenden Vorgänge aus:

1. Rufen Sie die private IP-Adresse der AWS Region-Instance ab, zum Beispiel 10.0.0.5. Diese Informationen sind in der EC2 Amazon-Konsole auf der Instance-Detailseite verfügbar.
2. Verwenden Sie je nach Betriebssystem ssh oder rdp, um eine Verbindung zur privaten IP-Adresse Ihrer Outpost-Instance herzustellen.
3. Führen Sie den `ping` Befehl von Ihrer Outpost-Instance zur IP-Adresse der AWS Region-Instance aus.

   ```
   ping 10.0.0.5
   ```

   Es folgt eine Beispielausgabe.

   ```
   Pinging 10.0.0.5

   Reply from 10.0.0.5:  bytes=32 time=<1ms TTL=128
   Reply from 10.0.0.5:  bytes=32 time=<1ms TTL=128
   Reply from 10.0.0.5:  bytes=32 time=<1ms TTL=128

   Ping statistics for 10.0.0.5
   Packets:  Sent = 3,  Received = 3,  Lost = 0 (0% lost)

   Approximate round trip time in milliseconds
   Minimum = 0ms,  Maximum = 0ms,  Average = 0ms
   ```

# Optimieren Sie Amazon EC2 für AWS Outposts

Im Gegensatz zur AWS-Region Amazon Elastic Compute Cloud (Amazon EC2) ist die Kapazität auf einem Outpost begrenzt. Sie sind durch das Gesamtvolumen der von Ihnen

bestellten Rechenkapazität eingeschränkt. Dieses Thema bietet bewährte Methoden und Optimierungsstrategien, mit denen Sie Ihre EC2 Amazon-Kapazität in optimal nutzen können AWS Outposts.

Inhalt



## Dedicated Hosts auf Outposts

Ein Amazon EC2 Dedicated Host ist ein physischer Server mit EC2 Instance-Kapazität, die vollständig für Ihre Nutzung reserviert ist. Ihr Outpost stellt Ihnen bereits dedizierte Hardware bereit, Dedicated Hosts gestatten Ihnen jedoch, vorhandene Softwarelizenzen pro Socket, Kern oder VM für einen Host zu verwenden. Weitere Informationen finden Sie unter Dedicated Hosts on AWS Outposts im  EC2 Amazon-Benutzerhandbuch.

Neben der Lizenzierung können Outpost-Besitzer Dedicated Hosts verwenden, um die Server in ihren Outpost-Bereitstellungen auf zwei Arten zu optimieren:

- Ändern des Kapazitätslayouts eines Servers
- Instance-Platzierung auf Hardwareebene steuern

### Ändern des Kapazitätslayouts eines Servers

Dedicated Hosts bietet Ihnen die Möglichkeit, das Layout der Server in Ihrer Outpost-Bereitstellung zu ändern, ohne Kontakt aufnehmen Support zu müssen. Wenn Sie Kapazität für Ihren Outpost erwerben, geben Sie ein EC2 Kapazitätslayout an, das jeder Server bereitstellt. Jeder Server unterstützt eine einzelne Familie von Instance-Typen. Ein Layout kann einen einzelnen Instance-Typ oder mehrere Instance-Typen anbieten. Mit Dedicated Hosts können Sie alles ändern, was Sie für das ursprüngliche Layout ausgewählt haben. Wenn Sie einem Host die Unterstützung eines einzelnen Instance-Typs für die gesamte Kapazität zuweisen, können Sie nur einen einzigen Instance-Typ von diesem Host aus starten. Die folgende Abbildung zeigt einen m5.24xlarge-Server mit einem homogenen Layout:

Sie können dieselbe Kapazität mehreren Instance-Typen zuweisen. Wenn Sie einem Host die Unterstützung mehrerer Instance-Typen zuweisen, erhalten Sie ein heterogenes Layout, für das kein explizites Kapazitätslayout erforderlich ist. Die folgende Abbildung zeigt einen m5.24xlarge Server mit einem heterogenen Layout bei voller Auslastung:

Weitere Informationen finden Sie unter Allocate a Dedicated Host im EC2 Amazon-Benutzerhandbuch.

Instance-Platzierung auf Hardwareebene steuern

Sie können Dedicated Hosts verwenden, um die Instance-Platzierung auf Hardwareebene zu steuern. Verwenden Sie die automatische Platzierung für Dedicated Hosts, um zu verwalten, ob Instances, die Sie starten, auf einem bestimmten Host oder auf einem beliebigen verfügbaren Host mit passender Konfiguration gestartet werden. Verwenden Sie die Host-Affinität, um eine Beziehung zwischen einer Instance und einem Dedicated Host herzustellen. Wenn Sie ein Outposts-Rack haben, können Sie diese Dedicated Hosts-Funktionen verwenden, um die Auswirkungen korrelierter Hardwarefehler zu minimieren. Weitere Informationen zur Instance-Wiederherstellung finden Sie unter Dedicated Host Auto Placement and Host Affinity im EC2 Amazon-Benutzerhandbuch.

Sie können Dedicated Hosts teilen mit. AWS Resource Access Manager Die gemeinsame Nutzung von Dedicated Hosts ermöglicht es Ihnen, Hosts in einer Outpost-Bereitstellung auf mehrere AWS-Konten-Standorte zu verteilen. Weitere Informationen finden Sie unter Gemeinsam genutzte - Ressourcen.

## Einrichten der Instance-Wiederherstellung

Instances auf Ihrem Outpost, die aufgrund eines Hardwarefehlers in einen fehlerhaften Zustand geraten, müssen auf einen fehlerfreien Host migriert werden. Sie können die automatische Wiederherstellung so einrichten, dass diese Migration auf der Grundlage von Instance-Statusprüfungen automatisch durchgeführt wird. Weitere Informationen finden Sie unter Instanzstabilität.

## Platzierungsgruppen auf Outposts

AWS Outposts unterstützt Platzierungsgruppen. Verwenden Sie Platzierungsgruppen, um zu beeinflussen, wie Amazon versuchen EC2 soll, Gruppen voneinander abhängiger Instances, die Sie starten, auf der zugrunde liegenden Hardware zu platzieren. Sie können verschiedene Strategien (Cluster, Partition oder Spread) verwenden, um den Anforderungen verschiedener Workloads

gerecht zu werden. Wenn Sie einen Outpost mit einem Rack haben, können Sie die Spread-Strategie verwenden, um Instances auf mehreren Hosts statt auf Racks zu platzieren.

## Spread Placement-Gruppen

Verwenden Sie eine Spread-Placement-Gruppe, um eine einzelne Instance auf unterschiedliche Hardware zu verteilen. Das Launchen von Instances in einer Spread-Placement-Gruppe reduziert das Risiko gleichzeitiger Ausfälle, die auftreten können, wenn Instances dieselbe Ausrüstung nutzen. Placement-Gruppen können Instances auf Racks oder Hosts verteilen. Sie können Spread Placement-Gruppen auf Host-Ebene nur mit AWS Outposts verwenden.

Placement-Gruppen auf Rack-Spread-Ebene

Ihre Rack-Spread-Level-Platzierungsgruppe kann so viele Instances aufnehmen, wie Sie Racks in Ihrer Outpost-Bereitstellung haben. Die folgende Abbildung zeigt eine Outpost-Bereitstellung mit drei Racks, bei der drei Instances in einer Rack-Spread-Level-Platzierungsgruppe ausgeführt werden.

Placement-Gruppen auf Host-Spread-Ebene

Ihre Host-Spread-Level-Platzierungsgruppe kann so viele Instances aufnehmen, wie Sie Hosts in Ihrer Outpost-Bereitstellung haben. Die folgende Abbildung zeigt eine Outpost-Bereitstellung mit einem Rack und drei Instances in einer Host-Spread-Level-Platzierungsgruppe.

## Partitions-Placement-Gruppen

Verwenden Sie eine Partition-Placement-Gruppe, um mehrere Instances auf Racks mit Partitionen zu verteilen. Jede Partition kann mehrere Instances enthalten. Sie können die automatische Verteilung verwenden, um Instances auf Partitionen zu verteilen oder Instances auf Zielpartitionen bereitzustellen. Die folgende Abbildung zeigt eine Partition-Placement-Gruppe mit automatischer Verteilung.

Sie können Instances auch auf Zielpartitionen bereitstellen. Die folgende Abbildung zeigt eine Partition-Placement-Gruppe mit gezielter Verteilung.

Weitere Informationen zur Arbeit mit Placement-Gruppen finden Sie unter Placement-Gruppen und Placement-Gruppen auf AWS Outposts im  EC2 Amazon-Benutzerhandbuch.

Weitere Informationen zur AWS Outposts Hochverfügbarkeit finden Sie unter Überlegungen zum Design und zur Architektur AWS Outposts hoher Verfügbarkeit.

# AWS Outposts Konnektivität zu AWS Regionen

AWS Outposts unterstützt WAN-Konnektivität (Wide Area Network) über die Service Link-Verbindung.

Inhalt



## Konnektivität über Service Link

Der Service-Link ist eine notwendige Verbindung zwischen Ihren Outposts und der AWS Region (oder Heimatregion). Es ermöglicht die Verwaltung der Outposts und den Verkehrsaustausch von und zur AWS Region. Der Service Link nutzt einen verschlüsselten Satz von VPN-Verbindungen, um mit der Heimatregion zu kommunizieren.

Nachdem die Service Link-Verbindung hergestellt wurde, ist Ihr Outpost betriebsbereit und wird von verwaltet. AWS Der Service Link ermöglicht den folgenden Datenverkehr:

- Kunden-VPC-Verkehr zwischen dem Outpost und allen damit verbundenen. VPCs
- Outposts Verwaltungsdatenverkehr wie Ressourcenmanagement, Ressourcenüberwachung sowie Firmware- und Softwareupdates.

### Anforderungen an die maximale Übertragungseinheit (Maximum Transmission Unit, MTU) des Service Link

Die maximale Übertragungseinheit (MTU) einer Netzwerkverbindung ist die Größe (in Byte) des größten zulässigen Datenpakets, das über die Verbindung übergeben werden kann. Das Netzwerk muss eine MTU von 1500 Byte zwischen dem Outpost und den Service Link-Endpunkten in der übergeordneten Region unterstützen. AWS

Der Datenverkehr, der von einer Instance in Outposts zu einer Instance in der Region geht, hat eine MTU von 1300.

## Empfehlungen für die Bandbreite von Service Links

Für eine optimale Benutzererfahrung und Ausfallsicherheit AWS müssen Sie redundante Konnektivität mit mindestens 500 Mbit/s für jedes Compute-Rack und eine maximale Round-Trip-Latenz von 175 ms für die Service Link-Verbindung zur AWS Region verwenden. Sie können AWS Direct Connect oder eine Internetverbindung für den Service Link verwenden. Die Mindestanforderungen von 500 Mbit/s und die maximale Roundtrip-Zeit für die Service Link-Verbindung ermöglichen es Ihnen, EC2 Amazon-Instances zu starten, Amazon EBS-Volumes anzuhängen und auf AWS Services wie Amazon EKS, Amazon EMR und CloudWatch Metriken mit optimaler Leistung zuzugreifen.

Die Bandbreitenanforderungen für Outposts variieren aufgrund der folgenden Merkmale:

- Anzahl der AWS Outposts Racks und Kapazitätskonfigurationen
- Workload-Merkmale wie AMI-Größe, Anwendungselastizität, Burst-Geschwindigkeitsanforderungen und Amazon VPC-Datenverkehr in die Region

Wenden Sie sich an Ihren AWS Vertriebsmitarbeiter oder APN-Partner, um eine individuelle Empfehlung zur für Ihre Bedürfnisse erforderlichen Service-Link-Bandbreite zu erhalten.

## Redundante Internetverbindungen

Wenn Sie die Konnektivität zwischen Ihrem Outpost und der AWS Region aufbauen, empfehlen wir Ihnen, mehrere Verbindungen einzurichten, um eine höhere Verfügbarkeit und Ausfallsicherheit zu gewährleisten. Weitere Informationen finden Sie unter AWS Direct Connect -Resiliency-Empfehlungen.

Wenn Sie Konnektivität zum öffentlichen Internet benötigen, können Sie redundante Internetverbindungen und verschiedene Internetanbieter verwenden, genau wie bei Ihren vorhandenen On-Premises-Workloads.

## Richten Sie Ihren Service-Link ein

In den folgenden Schritten wird der Einrichtungsprozess für den Service Link erläutert.

1. Wähle eine Verbindungsoption zwischen deinen Outposts und der AWS Heimatregion. Du kannst entweder eine öffentliche oder eine private Verbindung wählen.
2. Nachdem Sie Ihre Outposts-Racks bestellt haben, AWS kontaktiert er Sie, um VLAN, IP, BGP und Infrastruktursubnetz zu sammeln. IPs Weitere Informationen finden Sie unter Lokale Netzwerkkonnektivität.
3. AWS Konfiguriert während der Installation den Service Link auf dem Outpost auf der Grundlage der von Ihnen angegebenen Informationen.
4. Sie konfigurieren Ihre lokalen Netzwerkgeräte, wie Router, so, dass sie über BGP-Konnektivität eine Verbindung zu jedem Outpost-Netzwerkgerät herstellen. Informationen zur Service Link-VLAN-, IP- und BGP-Konnektivität finden Sie unter. Netzwerk
5. Sie konfigurieren Ihre Netzwerkgeräte wie Firewalls so, dass Ihre Outposts auf die AWS Region oder Heimatregion zugreifen können. AWS Outposts nutzt das Subnetz der Service Link-Infrastruktur IPs, um VPN-Verbindungen einzurichten und die Steuerung und den Datenverkehr mit der Region auszutauschen. Der Service Link-Aufbau wird immer vom Outpost aus initiiert.

> **Note**
>
> Sie können die Service Link-Konfiguration nicht mehr ändern, nachdem Sie die Bestellung abgeschlossen haben.

## Öffentliche Verbindungsoptionen für Service Link

Sie können den Service Link mit einer öffentlichen Verbindung für den Verkehr zwischen den Outposts und der AWS Heimatregion konfigurieren. Sie können wählen, ob Sie das öffentliche oder AWS Direct Connect das öffentliche Internet nutzen möchten. VIFs

Wenn Sie auf Ihren Firewalls nur die AWS Region öffentlich IPs (statt 0.0.0.0/0) zulassen möchten, müssen Sie sicherstellen, dass Ihre Firewallregeln den aktuellen IP-Adressbereichen up-to-date entsprechen. Weitere Informationen finden Sie unter AWS IP-Adressbereiche im Amazon VPC-Benutzerhandbuch.

Die folgende Abbildung zeigt beide Optionen, um eine öffentliche Service-Link-Verbindung zwischen Ihren Outposts und der AWS Region herzustellen:

### Option 1. Öffentliche Konnektivität über das Internet

Für diese Option muss das Subnetz IPs der AWS Outposts Service Link-Infrastruktur Zugriff auf die öffentlichen IP-Bereiche Ihrer AWS Region oder Heimatregion haben. Sie müssen AWS Region öffentlich IPs oder 0.0.0.0/0 auf Netzwerkgeräten wie Ihrer Firewall zulassen.

### Option 2. Öffentliche Konnektivität durch AWS Direct Connect öffentliche VIFs

Für diese Option muss das Subnetz IPs der AWS Outposts Service Link-Infrastruktur über den DX-Dienst Zugriff auf die öffentlichen IP-Bereiche Ihrer AWS Region oder Heimatregion haben. Sie müssen AWS Region public IPs oder 0.0.0.0/0 auf Netzwerkgeräten wie Ihrer Firewall zulassen.

## Private Verbindungsoptionen für Service Link

Sie können den Service Link mit einer privaten Verbindung für den Verkehr zwischen den Outposts und der AWS Heimatregion konfigurieren. Sie können wählen, ob Sie AWS Direct Connect privat oder Transit VIFs nutzen möchten.

Wählen Sie die private Verbindungsoption, wenn Sie Ihren Outpost in der AWS Outposts Konsole erstellen. Eine Anleitung dazu findest du unter Einen Außenposten erstellen.

Wenn Sie die private Konnektivitätsoption auswählen, wird nach der Installation von Outpost eine Service Link-VPN-Verbindung unter Verwendung einer von Ihnen angegebenen VPC und eines Subnetzes hergestellt. Dies ermöglicht private Konnektivität über die VPC und minimiert die Gefährdung durch das öffentliche Internet.

Die folgende Abbildung zeigt beide Optionen, um eine private Service Link-VPN-Verbindung zwischen Ihren Outposts und der AWS Region herzustellen:

### Voraussetzungen

Die folgenden Voraussetzungen sind erforderlich, bevor Sie die private Konnektivität für Ihren Outpost konfigurieren können:

- Sie müssen die Berechtigungen für eine IAM-Entität (Nutzer oder Rolle) so konfigurieren, dass der Nutzer oder die Rolle die mit dem Dienst verknüpfte Rolle für private Konnektivität erstellen kann. Die IAM-Entität benötigt die Erlaubnis, auf die folgenden Aktionen zuzugreifen:

- `iam:CreateServiceLinkedRole` auf `arn:aws:iam::*:role/aws-service-role/outposts.amazonaws.com/AWSServiceRoleForOutposts*`
- `iam:PutRolePolicy` auf `arn:aws:iam::*:role/aws-service-role/outposts.amazonaws.com/AWSServiceRoleForOutposts*`
- `ec2:DescribeVpcs`
- `ec2:DescribeSubnets`

Weitere Informationen finden Sie AWS Identity and Access Management unter AWS Outposts

- Erstellen Sie im selben AWS Konto und in derselben Availability Zone wie Ihr Outpost eine VPC für den alleinigen Zweck der privaten Outpost-Konnektivität mit einem Subnetz /25 oder höher, das nicht mit 10.1.0.0/16 in Konflikt steht. Sie könnten beispielsweise 10.3.0.0/16 verwenden.
- Konfigurieren Sie die Subnetz-Sicherheitsgruppe so, dass sie Datenverkehr für eingehende und ausgehende UDP-443-Richtungen zulässt.
- Bewerben Sie das Subnetz-CIDR in Ihrem On-Premises-Netzwerk. Sie können dies verwenden AWS Direct Connect . Weitere Informationen finden Sie unter AWS Direct Connect Virtuelle Schnittstellen und Arbeiten mit AWS Direct Connect -Gateways im AWS Direct Connect - Benutzerhandbuch.

> **Note**
>
> Um die private Verbindungsoption auszuwählen, wenn sich Ihr Outpost im Status PENDING befindet, wählen Sie in der AWS Outposts Konsole Outposts und dann Ihren Outpost aus. Wählen Sie Aktionen, Private Konnektivität hinzufügen und folgen Sie den Schritten.

Nachdem Sie die private Verbindungsoption für Ihren Outpost ausgewählt haben, AWS Outposts wird automatisch eine dienstbezogene Rolle in Ihrem Konto erstellt, die es dem Unternehmen ermöglicht, die folgenden Aufgaben in Ihrem Namen zu erledigen:

- Erstellt Netzwerkschnittstellen im Subnetz und in der VPC, die Sie angeben, und erstellt eine Sicherheitsgruppe für die Netzwerkschnittstellen.
- Erteilt dem AWS Outposts Dienst die Erlaubnis, die Netzwerkschnittstellen an eine Service Link-Endpunktinstanz im Konto anzuhängen.
- Hängt die Netzwerkschnittstellen vom Konto aus an die Service Link-Endpunkt-Instances an.

> **Important**
>
> Nachdem Ihr Outpost installiert ist, bestätigen Sie von Ihrem Outpost aus die Konnektivität mit dem privaten Bereich IPs in Ihrem Subnetz.

## Option 1. Private Konnektivität über AWS Direct Connect private VIFs

Erstellen Sie eine AWS Direct Connect Verbindung, eine private virtuelle Schnittstelle und ein virtuelles privates Gateway, damit Ihr lokaler Outpost auf die VPC zugreifen kann.

Weitere Informationen finden Sie in den folgenden Abschnitten des Benutzerhandbuchs AWS Direct Connect :

- Dedizierte und gehostete Verbindungen
- Erstellen Sie eine private virtuelle Schnittstelle
- Verknüpfungen virtueller privater Gateways

Wenn die AWS Direct Connect Verbindung über ein anderes AWS Konto als Ihre VPC erfolgt, finden Sie weitere Informationen unter Kontenübergreifendes Zuordnen eines virtuellen privaten Gateways im AWS Direct Connect Benutzerhandbuch.

## Option 2. Private Konnektivität durch AWS Direct Connect Transit VIFs

Erstellen Sie eine AWS Direct Connect Verbindung, eine virtuelle Transitschnittstelle und ein Transit-Gateway, damit Ihr lokaler Outpost auf die VPC zugreifen kann.

Weitere Informationen finden Sie in den folgenden Abschnitten des Benutzerhandbuchs AWS Direct Connect :

- Dedizierte und gehostete Verbindungen
- Erstellen Sie eine virtuelle Transitschnittstelle zum Direct Connect-Gateway
- Transit-Gateway-Verknüpfungen

# Firewalls und der Service Link

In diesem Abschnitt werden Firewallkonfigurationen und die Service-Link-Verbindung beschrieben.

In der folgenden Abbildung erweitert die Konfiguration die Amazon VPC von der AWS Region bis zum Outpost. Eine AWS Direct Connect öffentliche virtuelle Schnittstelle ist die Service Link-Verbindung. Der folgende Datenverkehr wird über den Service Link und die AWS Direct Connect -Verbindung abgewickelt:

- Verwaltung des Datenverkehrs zum Outpost über den Service Link
- Verkehr zwischen dem Außenposten und allen damit verbundenen VPCs

Wenn Sie mit Ihrer Internetverbindung eine Stateful-Firewall verwenden, um die Konnektivität vom öffentlichen Internet zum Service Link-VLAN einzuschränken, können Sie alle eingehenden Verbindungen blockieren, die über das Internet initiiert werden. Das liegt daran, dass das Service Link VPN nur vom Outpost zur Region initiiert wird, nicht von der Region zum Outpost.

Wenn Sie eine Firewall verwenden, um die Konnektivität über das Service Link-VLAN einzuschränken, können Sie alle eingehenden Verbindungen blockieren. Sie müssen ausgehende Verbindungen von der AWS Region zurück zum Außenposten gemäß der folgenden Tabelle zulassen. Wenn die Firewall zustandsorientiert ist, sollten ausgehende Verbindungen vom Outpost, die erlaubt sind, d. h. vom Outpost initiiert wurden, wieder zugelassen werden.

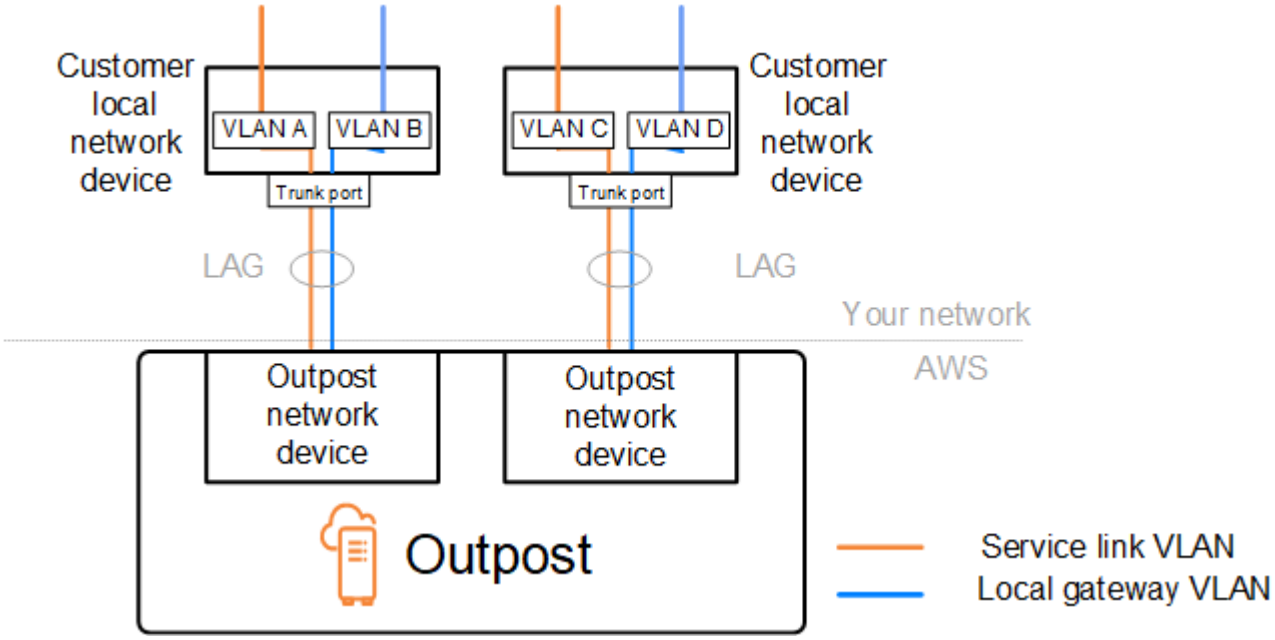
| Protokoll | Quell-Port | Quelladresse | Ziel-Port | Zieladresse |
|---|---|---|---|---|
| UDP | 443 | AWS Outposts Service-Link /26 | 443 | AWS Outposts Die Region ist öffentlich IPs |
| TCP | 1025-65535 | AWS Outposts Servicelink /26 | 443 | AWS Outposts Die Region ist öffentlich IPs |

> **Note**
>
> Instances in einem Outpost können den Service-Link nicht verwenden, um mit Instances in anderen Outposts zu kommunizieren. Nutzen Sie das Routing über das lokale Gateway oder die lokale Netzwerkschnittstelle, um zwischen Outposts zu kommunizieren.

AWS Outposts Die Racks sind außerdem mit redundanter Stromversorgung und Netzwerkausrüstung ausgestattet, einschließlich lokaler Gateway-Komponenten. Weitere Informationen finden Sie unter Resilienz in AWS Outposts.

# Checkliste zur Fehlerbehebung bei Outposts-Rack-Netzwerken

Verwenden Sie diese Checkliste, um Probleme mit einem Service-Link zu beheben, der den Status `DOWN` hat.




## Konnektivität mit Outpost-Netzwerkgeräten

Überprüfen Sie den BGP-Peering-Status auf den lokalen Netzwerkgeräten des Kunden, die mit den Outpost-Netzwerkgeräten verbunden sind. Wenn der BGP-Peering-Status `DOWN` lautet, gehen Sie wie folgt vor:

1. Pingen Sie die Remote-Peer-IP-Adresse auf den Outpost-Netzwerkgeräten von den Kundengeräten aus. Sie finden die Peer-IP-Adresse in der BGP-Konfiguration Ihres Geräts. Sie können sich auch auf die Checkliste zur Netzwerkbereitschaft beziehen, die Ihnen zum Zeitpunkt der Installation zur Verfügung gestellt wurden.
2. Wenn das Pingen nicht erfolgreich ist, überprüfen Sie die physische Verbindung und stellen Sie sicher, dass der Verbindungsstatus `UP` lautet.
   a. Bestätigen Sie den LACP-Status der lokalen Netzwerkgeräte des Kunden.

b. Überprüfen Sie den Schnittstellenstatus auf dem Gerät. Wenn der Status UP lautet, fahren Sie mit Schritt 3 fort.

c. Überprüfen Sie die lokalen Netzwerkgeräte des Kunden und vergewissern Sie sich, dass das optische Modul funktioniert.

d. Tauschen Sie defekte Glasfasern aus und stellen Sie sicher, dass sich die Lichter (Tx/Rx) innerhalb eines akzeptablen Bereichs befinden.

3. Wenn das Pingen erfolgreich ist, überprüfen Sie die lokalen Netzwerkgeräte des Kunden und stellen Sie sicher, dass die folgenden BGP-Konfigurationen korrekt sind.

   a. Vergewissern Sie sich, dass die lokale Autonome Systemnummer (Kunden-ASN) korrekt konfiguriert ist.

   b. Vergewissern Sie sich, dass die entfernte Autonome Systemnummer (Outpost ASN) korrekt konfiguriert ist.

   c. Vergewissern Sie sich, dass die Schnittstellen-IP und die Remote-Peer-IP-Adressen korrekt konfiguriert sind.

   d. Vergewissern Sie sich, dass die beworbenen und empfangenen Routen korrekt sind.

4. Wenn Ihre BGP-Sitzung zwischen dem Status Aktiv und dem Status Connect hin- und herschwankt, stellen Sie sicher, dass der TCP-Port 179 und andere relevante kurzlebige Ports auf den lokalen Netzwerkgeräten des Kunden nicht blockiert sind.

5. Wenn Sie weitere Probleme beheben müssen, überprüfen Sie Folgendes auf den lokalen Netzwerkgeräten des Kunden:

   a. BGP- und TCP-Debug-Protokolle

   b. BGP-Logs

   c. Paketerfassung

6. Wenn das Problem weiterhin besteht, führen Sie MTR/traceroute/-Paketerfassungen von Ihrem mit Outpost verbundenen Router zu den Peer-IP-Adressen der Outpost-Netzwerkgeräte durch. Teilen Sie die Testergebnisse mithilfe AWS Ihres Enterprise-Supportplans mit dem Support.

Wenn zwischen den lokalen Netzwerkgeräten des Kunden und den Outpost-Netzwerkgeräten der BGP-Peering-Status UP besteht, der Service-Link jedoch weiterhin DOWN ist, können Sie weitere Probleme beheben, indem Sie die folgenden Geräte auf den lokalen Netzwerkgeräten Ihres Kunden überprüfen. Verwenden Sie je nach Bereitstellungsart Ihrer Service Link-Konnektivität eine der folgenden Checklisten.

- Edge-Router, verbunden mit AWS Direct Connect — Öffentliche virtuelle Schnittstelle, die für Service Link-Konnektivität verwendet wird. Weitere Informationen finden Sie unter AWS Direct Connect Konnektivität über öffentliche virtuelle Schnittstellen zur Region AWS.
- Edge-Router, verbunden mit AWS Direct Connect — Private virtuelle Schnittstelle, die für die Service Link-Konnektivität verwendet wird. Weitere Informationen finden Sie unter AWS Direct Connect private virtuelle Schnittstelle, Konnektivität zur AWS Region.
- Edge-Router, die mit Internetdienstanbietern verbunden sind (ISPs) — Öffentliches Internet, das für Service Link-Konnektivität verwendet wird. Weitere Informationen finden Sie unter ISP öffentliche virtuelle Schnittstellenverbindung zur AWS -Region.

## AWS Direct Connect Konnektivität über öffentliche virtuelle Schnittstellen zur Region AWS

Verwenden Sie die folgende Checkliste, um Probleme mit Edge-Routern zu beheben, mit AWS Direct Connect denen eine Verbindung hergestellt wird, wenn eine öffentliche virtuelle Schnittstelle für Service Link-Konnektivität verwendet wird.

1. Vergewissern Sie sich, dass die Geräte, die eine direkte Verbindung zu den Outpost-Netzwerkgeräten herstellen, die IP-Adressbereiche von Service Link über BGP empfangen.
   a. Bestätigen Sie die Routen, die über BGP von Ihrem Gerät empfangen werden.
   b. Überprüfen Sie die Routing-Tabelle der Service Link Virtual Routing and Forwarding Instance (VRF). Die Anzeige sollte zeigen, dass der IP-Adressbereich verwendet wird.
2. Um die Konnektivität der Region sicherzustellen, überprüfen Sie die Routing-Tabelle für den Service Link VRF. Sie sollte die AWS öffentlichen IP-Adressbereiche oder die Standardroute enthalten.
3. Wenn Sie die AWS öffentlichen IP-Adressbereiche nicht im Service Link VRF erhalten, überprüfen Sie die folgenden Punkte.
   a. Überprüfen Sie den AWS Direct Connect Verbindungsstatus vom Edge-Router oder vom AWS Management Console.
   b. Wenn die physische Verbindung `UP` ist, überprüfen Sie den BGP-Peering-Status vom Edge-Router aus.
   c. Wenn der BGP-Peering-Status lautet`DOWN`, pingen Sie die AWS Peer-IP-Adresse an und überprüfen Sie die BGP-Konfiguration im Edge-Router. Weitere Informationen finden Sie im AWS Direct Connect Benutzerhandbuch unter Problembehandlung und AWS Direct Connect

in der Konsole ist der BGP-Status meiner virtuellen Schnittstelle ausgefallen. AWS Was soll ich tun?.

d. Wenn BGP eingerichtet ist und Sie die Standardroute oder die AWS öffentlichen IP-Adressbereiche nicht in der VRF sehen, wenden Sie sich mithilfe Ihres AWS Enterprise-Supportplans an den Support.

4. Wenn Sie eine On-Premises-Firewall haben, überprüfen Sie die folgenden Elemente.

   a. Vergewissern Sie sich, dass die für die Service Link-Konnektivität erforderlichen Ports in den Netzwerk-Firewalls zulässig sind. Verwenden Sie Traceroute auf Port 443 oder ein anderes Tool zur Netzwerkfehlerbehebung, um die Konnektivität zwischen den Firewalls und Ihren Netzwerkgeräten zu überprüfen. Die folgenden Ports müssen in den Firewall-Richtlinien für die Service Link-Konnektivität konfiguriert werden.

      - TCP-Protokoll – Quellport: TCP 1025-65535, Zielport: 443.
      - UDP-Protokoll – Quellport: TCP 1025-65535, Zielport: 443.

   b. Wenn die Firewall statusbehaftet ist, stellen Sie sicher, dass die Regeln für ausgehende Nachrichten den Service-Link-IP-Adressbereich des Outpost mit den AWS öffentlichen IP-Adressbereichen verknüpfen. Weitere Informationen finden Sie unter AWS Outposts Konnektivität zu AWS Regionen.

   c. Wenn die Firewall nicht statusbehaftet ist, stellen Sie sicher, dass auch der eingehende Datenfluss zugelassen ist (von den AWS öffentlichen IP-Adressbereichen bis zum IP-Adressbereich des Service Links).

   d. Wenn Sie in den Firewalls einen virtuellen Router konfiguriert haben, stellen Sie sicher, dass das entsprechende Routing für den Datenverkehr zwischen dem Outpost und der AWS -Region konfiguriert ist.

5. Wenn Sie NAT im On-Premises-Netzwerk so konfiguriert haben, dass die Service Link-IP-Adressbereiche des Outpost in Ihre eigenen öffentlichen IP-Adressen übersetzt werden, überprüfen Sie die folgenden Punkte.

   a. Vergewissern Sie sich, dass das NAT-Gerät nicht überlastet ist und über freie Ports für neue Sitzungen verfügt.

   b. Vergewissern Sie sich, dass das NAT-Gerät für die Adressübersetzung korrekt konfiguriert ist.

6. Wenn das Problem weiterhin besteht, führen Sie MTR/Traceroute/Paketerfassungen von Ihrem Edge-Router zu den Peer-IP-Adressen durch. AWS Direct Connect Teilen Sie die Testergebnisse mithilfe AWS Ihres Enterprise-Supportplans mit dem Support.

# AWS Direct Connect private virtuelle Schnittstelle, Konnektivität zur AWS Region

Verwenden Sie die folgende Checkliste, um Fehler bei Edge-Routern zu beheben, die verbunden sind, AWS Direct Connect wenn eine private virtuelle Schnittstelle für Service Link-Konnektivität verwendet wird.

1. Wenn die Konnektivität zwischen dem Outposts-Rack und der AWS Region die AWS Outposts private Konnektivitätsfunktion verwendet, überprüfen Sie die folgenden Punkte.
   a. Pingen Sie die AWS Remote-Peering-IP-Adresse vom Edge-Router aus an und bestätigen Sie den BGP-Peering-Status.
   b. Stellen Sie sicher, dass das BGP-Peering über die AWS Direct Connect private virtuelle Schnittstelle zwischen Ihrer Service Link-Endpunkt-VPC und dem in Ihren Räumlichkeiten installierten Outpost erfolgt. UP Weitere Informationen finden Sie unter Problembehandlung AWS Direct Connect im AWS Direct Connect Benutzerhandbuch, Der BGP-Status meiner virtuellen Schnittstelle ist in der Konsole ausgefallen. AWS Was sollte ich tun?, und Wie kann ich BGP-Verbindungsprobleme über Direct Connect beheben? .
   c. Die AWS Direct Connect private virtuelle Schnittstelle ist eine private Verbindung zu Ihrem Edge-Router an dem von Ihnen ausgewählten AWS Direct Connect Standort und verwendet BGP für den Austausch von Routen. Ihr CIDR-Bereich für Ihre private Virtual Private Cloud (VPC) wird über diese BGP-Sitzung auf Ihrem Edge-Router angekündigt. In ähnlicher Weise wird der IP-Adressbereich für den Outpost-Service Link der Region über BGP von Ihrem Edge-Router aus bekannt gegeben.
   d. Vergewissern Sie sich, dass das Netzwerk, das dem privaten Service Link-Endpunkt in Ihrer VPC ACLs zugeordnet ist, den entsprechenden Datenverkehr zulässt. Weitere Informationen finden Sie unter Checkliste zur Netzwerkbereitschaft.
   e. Wenn Sie über eine On-Premises-Firewall verfügen, stellen Sie sicher, dass die Firewall über ausgehende Regeln verfügt, die die IP-Adressbereiche für Service Links und die Outpost-Service-Endpunkte (die IP-Adressen der Netzwerkschnittstelle) zulassen, die sich in der VPC oder der VPC CIDR befinden. Stellen Sie sicher, dass die Ports TCP 1025-65535 und UDP 443 nicht blockiert sind. Weitere Informationen finden Sie unter Einführung in AWS Outposts private Konnektivität.
   f. Wenn es sich nicht um eine Stateful-Firewall handelt, stellen Sie sicher, dass die Firewall über Regeln und Richtlinien verfügt, die den von den Outpost-Service-Endpunkten in der VPC eingehenden Datenverkehr zum Outpost zulassen.

2. Wenn Sie mehr als 100 Netzwerke in Ihrem lokalen Netzwerk haben, können Sie eine Standardroute über die BGP-Sitzung zu Ihrer privaten virtuellen AWS Schnittstelle ankündigen. Wenn Sie keine Standardroute bewerben möchten, fassen Sie die Routen so zusammen, dass die Anzahl der beworbenen Routen weniger als 100 beträgt.
3. Wenn das Problem weiterhin besteht, führen Sie MTR/Traceroute/Paketerfassungen von Ihrem Edge-Router zu den Peer-IP-Adressen durch. AWS Direct Connect Teilen Sie die Testergebnisse mithilfe AWS Ihres Enterprise-Supportplans mit dem Support.

## ISP öffentliche virtuelle Schnittstellenverbindung zur AWS -Region

Verwenden Sie die folgende Checkliste für die Fehlersuche bei Edge-Routern, die über einen ISP verbunden sind, wenn Sie das öffentliche Internet für Service Link-Konnektivität nutzen.

- Vergewissern Sie sich, dass die Internetverbindung aktiv ist.
- Vergewissern Sie sich, dass die öffentlichen Server von Ihren Edge-Geräten aus zugänglich sind, die über einen ISP verbunden sind.

Wenn über die ISP-Links nicht auf das Internet oder die öffentlichen Server zugegriffen werden kann, führen Sie die folgenden Schritte aus.

1. Überprüfen Sie, ob der BGP-Peering-Status mit den ISP-Routern eingerichtet ist.
   a. Vergewissern Sie sich, dass das BGP nicht schwankt.
   b. Vergewissern Sie sich, dass das BGP die erforderlichen Routen vom ISP empfängt und bewirbt.
2. Überprüfen Sie bei einer statischen Routenkonfiguration, ob die Standardroute auf dem Edge-Gerät ordnungsgemäß konfiguriert ist.
3. Prüfen Sie, ob Sie das Internet über eine andere ISP-Verbindung erreichen können.
4. Wenn das Problem weiterhin besteht, führen Sie MTR/traceroute/-Paketerfassungen von Ihrem Edge-Router zu den -Peer-IP-Adressen durch. Teilen Sie die Ergebnisse dem technischen Support Ihres Internetdienstanbieters mit, um weitere Probleme zu beheben.

Wenn über die ISP-Links auf das Internet und die öffentlichen Server zugegriffen werden kann, führen Sie die folgenden Schritte aus.

1. Bestätigen Sie, ob auf Ihre öffentlich zugänglichen EC2 Instances oder Load Balancer in der Outpost-Heimatregion von Ihrem Edge-Gerät aus zugegriffen werden kann. Sie können Ping oder

Telnet verwenden, um die Konnektivität zu bestätigen, und dann Traceroute verwenden, um den Netzwerkpfad zu bestätigen.

2. Wenn Sie VRFs den Datenverkehr in Ihrem Netzwerk trennen, vergewissern Sie sich, dass der Service Link VRF über Routen oder Richtlinien verfügt, die den Datenverkehr zum und vom ISP (Internet) und VRF weiterleiten. Sehen Sie sich die folgenden Checkpoints an.
   a. Edge-Router, die eine Verbindung zum ISP herstellen. Überprüfen Sie in der ISP-VRF-Routing-Tabelle des Edge-Routers, ob der IP-Adressbereich für den Service Link vorhanden ist.
   b. Lokale Netzwerkgeräte des Kunden, die eine Verbindung zum Outpost herstellen. Überprüfen Sie die Konfigurationen von VRFs und stellen Sie sicher, dass das Routing und die Richtlinien, die für die Konnektivität zwischen dem Service Link VRF und dem ISP VRF erforderlich sind, ordnungsgemäß konfiguriert sind. Normalerweise wird eine Standardroute vom ISP-VRF an das Service Link-VRF für den Datenverkehr zum Internet gesendet.
   c. Wenn Sie in den Routern, die mit Ihrem Outpost verbunden sind, quellenbasiertes Routing konfiguriert haben, vergewissern Sie sich, dass die Konfiguration korrekt ist.
3. Stellen Sie sicher, dass die lokalen Firewalls so konfiguriert sind, dass sie ausgehende Konnektivität (TCP 1025-65535- und UDP 443-Ports) von den IP-Adressbereichen des Outpost Service Links zu den öffentlichen IP-Adressbereichen zulassen. AWS Wenn die Firewalls nicht zustandsorientiert sind, stellen Sie sicher, dass die eingehende Verbindung zum Outpost ebenfalls konfiguriert ist.
4. Stellen Sie sicher, dass NAT im On-Premises-Netzwerk so konfiguriert ist, dass die Service-Link-IP-Adressbereiche des Outpost in öffentliche IP-Adressen übersetzt werden. Prüfen Sie außerdem die folgenden Elemente.
   a. Das NAT-Gerät ist nicht überlastet und verfügt über freie Ports für neue Sitzungen.
   b. Das NAT-Gerät für die Adressübersetzung ist korrekt konfiguriert.

Wenn das Problem weiterhin besteht, führen Sie MTR/traceroute/-Paketerfassungen durch.

- Wenn die Ergebnisse zeigen, dass Pakete im On-Premises-Netzwerk verloren gehen oder blockiert werden, wenden Sie sich an Ihr Netzwerk- oder Technikteam, um weitere Informationen zu erhalten.
- Wenn die Ergebnisse zeigen, dass die Pakete im Netzwerk des Internetdienstanbieters verloren gehen oder blockiert werden, wenden Sie sich an den technischen Support des ISP.

- Wenn die Ergebnisse keine Probleme zeigen, sammeln Sie die Ergebnisse aller Tests (z. B. MTR, Telnet, Traceroute, Paketerfassung und BGP-Protokolle) und wenden Sie sich über Ihren Enterprise-Supportplan an den AWS Support.

## Outposts befindet sich hinter zwei Firewall-Geräten

Wenn Sie Ihren Outpost hinter einem Paar synchronisierter Firewalls mit hoher Verfügbarkeit oder zwei eigenständigen Firewalls platziert haben, kann es zu einem asymmetrischen Routing der Service-Verbindung kommen. Das bedeutet, dass eingehender Datenverkehr Firewall-1 passieren könnte, während ausgehender Datenverkehr Firewall-2 passieren könnte. Verwenden Sie die folgende Checkliste, um ein potenzielles asymmetrisches Routing des Service Links zu identifizieren, insbesondere wenn er zuvor ordnungsgemäß funktioniert hat.

- Überprüfen Sie, ob in letzter Zeit Änderungen oder laufende Wartungsarbeiten an der Routingkonfiguration Ihres Unternehmensnetzwerks vorgenommen wurden, die möglicherweise zu einem asymmetrischen Routing des Service Links durch die Firewalls geführt haben.
  - Verwenden Sie Firewall-Verkehrsdiagramme, um nach Änderungen der Verkehrsmuster zu suchen, die mit dem Beginn des Service-Link-Problems übereinstimmen.
  - Suchen Sie nach einem teilweisen Firewallausfall oder einem Szenario mit geteilten Firewall-Paaren, das möglicherweise dazu geführt hat, dass Ihre Firewalls ihre Verbindungstabellen nicht mehr miteinander synchronisieren.
  - Suchen Sie in Ihrem Unternehmensnetzwerk nach nicht funktionierenden Links oder nach kürzlichen Änderungen am Routing (OSPF/ISIS/EIGRPmetrische Änderungen, BGP-Route-Map-Änderungen), die mit dem Beginn des Service-Link-Problems übereinstimmen.
- Wenn Sie für die Serviceverbindung zur Heimatregion eine öffentliche Internetverbindung verwenden, könnte eine Wartung durch den Dienstanbieter zu einem asymmetrischen Routing der Serviceverbindung durch die Firewalls geführt haben.
  - Suchen Sie in den Datenverkehrsdiagrammen nach Links zu Ihren ISP (s) auf Änderungen der Verkehrsmuster, die mit dem Beginn des Service-Link-Problems übereinstimmen.
- Wenn Sie AWS Direct Connect Konnektivität für den Service Link verwenden, ist es möglich, dass eine AWS geplante Wartung ein asymmetrisches Routing des Service Links ausgelöst hat.
  - Suchen Sie nach Benachrichtigungen über geplante Wartungsarbeiten an Ihren AWS Direct Connect Diensten.
  - Beachten Sie, dass Sie bei redundanten AWS Direct Connect Diensten das Routing des Outposts-Servicelinks über jeden wahrscheinlichen Netzwerkpfad unter Wartungsbedingungen

proaktiv testen können. Auf diese Weise können Sie testen, ob eine Unterbrechung eines Ihrer AWS Direct Connect Dienste zu einem asymmetrischen Routing der Service-Verbindung führen könnte. Die Widerstandsfähigkeit des AWS Direct Connect Teils der end-to-end Netzwerkkonnektivität kann mit dem Resiliency with AWS Direct Connect Resiliency Toolkit getestet werden. Weitere Informationen finden Sie unter Resilienz mit dem AWS Direct Connect Resiliency Toolkit testen — Failover-Tests.

Nachdem Sie die vorherige Checkliste durchgesehen und das asymmetrische Routing der Service-Verbindung als mögliche Ursache identifiziert haben, können Sie eine Reihe weiterer Maßnahmen ergreifen:

- Stellen Sie das symmetrische Routing wieder her, indem Sie alle Änderungen am Unternehmensnetzwerk rückgängig machen oder warten, bis die vom Anbieter geplante Wartung abgeschlossen ist.
- Melden Sie sich bei einer oder beiden Firewalls an und löschen Sie alle Flussstatusinformationen für alle Datenflüsse über die Befehlszeile (sofern vom Firewall-Anbieter unterstützt).
- Filtern Sie vorübergehend BGP-Ankündigungen durch eine der Firewalls heraus oder schließen Sie die Schnittstellen an einer Firewall, um ein symmetrisches Routing durch die andere Firewall zu erzwingen.
- Starten Sie jede Firewall nacheinander neu, um mögliche Beschädigungen bei der Flow-State-Verfolgung des Service Link-Verkehrs im Speicher der Firewall zu vermeiden.
- Bitten Sie Ihren Firewall-Anbieter, die Nachverfolgung des UDP-Flow-Status für UDP-Verbindungen, die auf Port 443 basieren und für Port 443 bestimmt sind, entweder zu überprüfen oder zu lockern.

# Lokale Gateways für Ihre Outposts-Racks

Das lokale Gateway ist eine Kernkomponente der Architektur für Ihre Outposts-Racks. Ein lokales Gateway ermöglicht die Konnektivität zwischen Ihren Outpost-Subnetzen und Ihrem lokalen Netzwerk. Wenn die lokale Infrastruktur einen Internetzugang bietet, können Workloads, die auf Outposts-Racks ausgeführt werden, auch das lokale Gateway nutzen, um mit regionalen Diensten oder regionalen Workloads zu kommunizieren. Diese Konnektivität kann entweder über eine öffentliche Verbindung (Internet) oder über AWS Direct Connect Weitere Informationen finden Sie unter AWS Outposts Konnektivität zu AWS Regionen.

Inhalt



## Grundlagen zu lokalen Gateways

AWS erstellt im Rahmen des Installationsvorgangs ein lokales Gateway für jedes Outposts-Rack. Ein Outposts-Rack unterstützt ein einzelnes lokales Gateway. Das lokale Gateway gehört dem mit den Outposts AWS-Konto verbundenen Rack.

> **Note**
>
> Informationen zu den Bandbreitenbeschränkungen von Instances für den Datenverkehr, der über ein lokales Gateway fließt, finden Sie im EC2 Amazon-Benutzerhandbuch unter Netzwerkbandbreite von Amazon EC2 Instance.

Ein lokales Gateway umfasst die folgenden Komponenten:

- Routing-Tabellen — Nur der Besitzer eines lokalen Gateways kann lokale Gateway-Routentabellen erstellen. Weitere Informationen finden Sie unter the section called “Routing-Tabellen”.

- CoIP-Pools – (Optional) Sie können IP-Adressbereiche verwenden, die Sie besitzen, um die Kommunikation zwischen dem On-Premises-Netzwerk und Instances in Ihrer VPC zu erleichtern. Weitere Informationen finden Sie unter the section called “IP-Adressen im Besitz des Kunden”.
- Virtuelle Schnittstellen (VIFs) — Lokales Gateway VIFs (Virtual Interface) ist eine logische Schnittstellenkomponente von Outposts-Racks, die VLAN-, IP- und BGP-Konnektivität zwischen einem Outposts-Netzwerkgerät und einem lokalen Netzwerkgerät für lokale Gateway-Konnektivität einrichtet. AWS erstellt eine VIF für jede LAG und fügt beide zu einer VIF-Gruppe hinzu. VIFs Die Routentabelle des lokalen Gateways muss VIFs für die lokale Netzwerkkonnektivität eine Standardroute zu den beiden enthalten. Weitere Informationen finden Sie unter Lokale Netzwerkkonnektivität.
- VIF-Gruppen — AWS fügt die erstellten VIFs Gruppen zu einer VIF-Gruppe hinzu. VIF-Gruppen sind logische Gruppierungen von. VIFs
- Lokale Gateway-Routentabelle und VPC-Zuordnungen — Mit der lokalen Gateway-Routentabelle und VPC-Zuordnungen können Sie Ihre Routentabellen mit den lokalen VPCs Gateway-Routentabellen verbinden. Mit dieser Zuordnung können Sie in Ihrer Outposts-Subnetz-Routentabelle eine Route hinzufügen, die auf das lokale Gateway ausgerichtet ist. Dies ermöglicht die Kommunikation zwischen Ihren Outposts-Subnetzressourcen und Ihrem lokalen Netzwerk über das lokale Gateway.
- Lokale Gateway-Routingdomänen — Eine lokale Gateway-Routingdomäne ist die Zuordnung einer lokalen Gateway-Routingtabelle und einer lokalen Gateway-VIF-Gruppe. Mit dieser Zuordnung können Sie innerhalb Ihrer lokalen Gateway-Routentabelle eine Route hinzufügen, die auf eine lokale Gateway-VIF-Gruppe ausgerichtet ist. Dies ermöglicht die Kommunikation zwischen Ihren Outposts-Subnetzressourcen und Ihrem lokalen Netzwerk über die ausgewählte VIF-Gruppe.

Bei der AWS Bereitstellung Ihres Outposts-Racks erstellen wir einige Komponenten, und Sie sind für die Erstellung anderer verantwortlich.

AWS Verantwortlichkeiten

- Liefert die Hardware.
- Erzeugt das lokale Gateway.
- Erzeugt die virtuellen Schnittstellen (VIFs) und eine VIF-Gruppe.

Ihre Aufgaben

- Erstellen Sie die Routing-Tabelle des lokalen Gateways.

- Verknüpfen Sie eine VPC mit der Routing-Tabelle des lokalen Gateways.
- Ordnen Sie der lokalen Gateway-Routentabelle eine VIF-Gruppe zu, um eine lokale Gateway-Routingdomäne zu erstellen.

## Lokales Gateway-Routing

Die Instances in Ihrem Outpost-Subnetz können eine der folgenden Optionen für die Kommunikation mit Ihrem On-Premises-Netzwerk über das lokale Gateway verwenden:

- Private IP-Adressen – Das lokale Gateway verwendet die privaten IP-Adressen der Instances in Ihrem Outpost-Subnetz, um die Kommunikation mit Ihrem On-Premises-Netzwerk zu erleichtern. Dies ist die Standardeinstellung.
- Kundeneigene IP-Adressen – Das lokale Gateway führt die Network Address Translation (NAT) für die kundeneigenen IP-Adressen durch, die Sie den Instances im Outpost-Subnetz zuweisen. Diese Option unterstützt überlappende CIDR-Bereiche und andere Netzwerktopologien.

Weitere Informationen finden Sie unter the section called “Routing-Tabellen”.

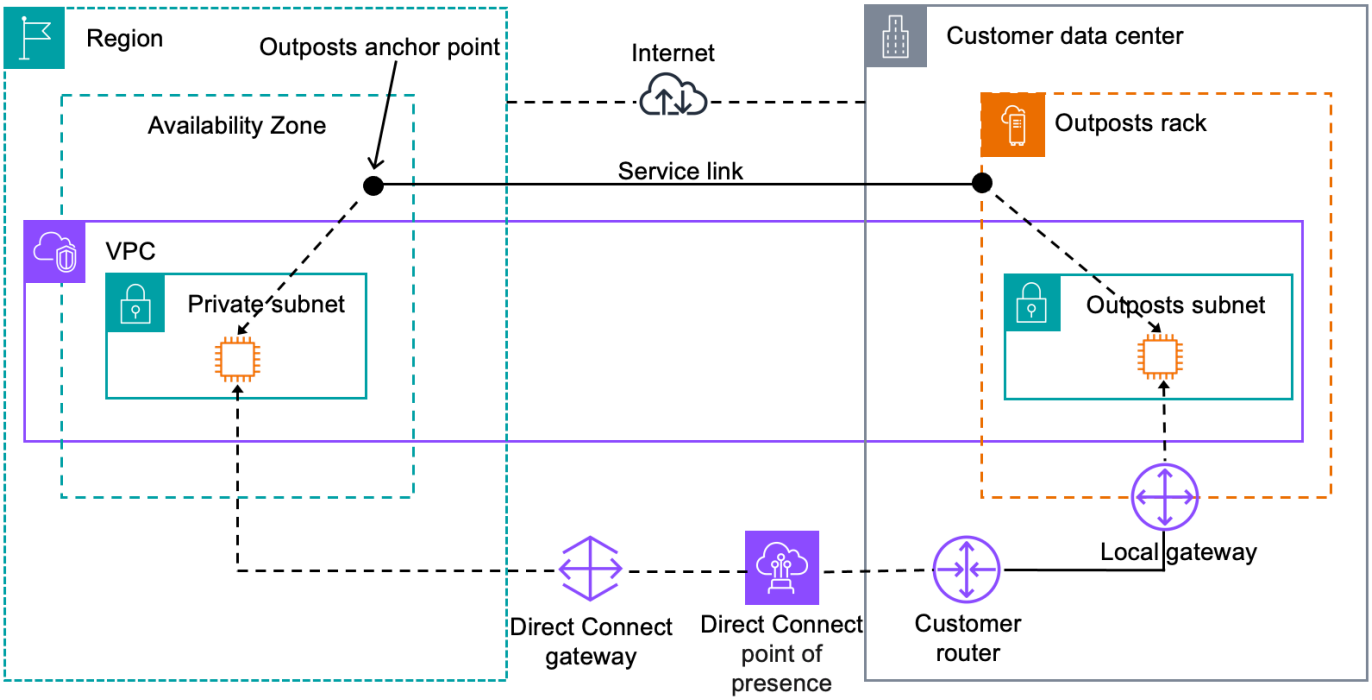
## Konnektivität über ein lokales Gateway

Die Hauptaufgabe eines On-Premises-Gateways besteht darin, Konnektivität von einem Outpost zu Ihrem On-Premises-On-Premises-Netzwerk bereitzustellen. Es bietet auch Konnektivität zum Internet über Ihr On-Premises-Netzwerk. Beispiele finden Sie unter the section called “Direktes VPC-Routing” und the section called “IP-Adressen im Besitz des Kunden”.

Das lokale Gateway kann auch einen Datenebenenpfad zurück zur AWS Region bereitstellen. Der Datenebenenpfad für das lokale Gateway verläuft vom Outpost über das lokale Gateway bis hin zu Ihrem privaten lokalen Gateway-LAN-Segment. Es würde dann einem privaten Pfad zurück zu den AWS -Service-Endpunkten in der Region folgen. Beachten Sie, dass der Pfad der Steuerebene immer die Service Link-Konnektivität verwendet, unabhängig davon, welchen Pfad Sie auf der Datenebene verwenden.

Sie können Ihre lokale Outposts-Infrastruktur privat mit der AWS-Services in der Region verbinden. AWS Direct Connect Weitere Informationen finden Sie unter AWS Outposts – private Konnektivität.

Die folgende Abbildung zeigt die Konnektivität über das lokale Gateway:




# Routing-Tabellen für das lokale Gateway

Erstellt im Rahmen der Rack-Installation das lokale Gateway, konfiguriert VIFs und AWS erstellt eine VIF-Gruppe. Das lokale Gateway gehört dem AWS Konto, das dem Outpost zugeordnet ist. Sie erstellen die Routing-Tabelle des lokalen Gateways. Eine Routing-Tabelle eines lokalen Gateways muss mit einer VIF-Gruppe und einer VPC verknüpft sein. Sie erstellen und verwalten die Zuordnung der VIF-Gruppe und der VPC. Nur der Besitzer des lokalen Gateways kann die Routentabelle des lokalen Gateways ändern.

Outpost-Subnetz-Routetabellen können eine Route zu lokalen Gateway-VIF-Gruppen enthalten, um die Konnektivität zu Ihrem lokalen Netzwerk sicherzustellen.

Routentabellen für lokale Gateways verfügen über einen Modus, der bestimmt, wie Instances Outposts Outposts-Subnetz mit Ihrem lokalen Netzwerk kommunizieren. Die Standardoption ist direktes VPC-Routing, das die privaten IP-Adressen der Instances verwendet. Die andere Option besteht darin, Adressen aus einem kundeneigenen IP-Adresspool (CoIP) zu verwenden, den Sie bereitstellen. Direktes VPC-Routing und CoIP sind sich gegenseitig ausschließende Optionen, die steuern, wie das Routing funktioniert. Informationen zur Auswahl der besten Option für Ihren Outpost finden Sie unter So wählen Sie im Outposts-Rack zwischen den Routing-Modi CoIP und Direct VPC. AWS

Sie können die lokale Gateway-Routentabelle mit anderen AWS Konten oder Organisationseinheiten gemeinsam nutzen. AWS Resource Access Manager Weitere Informationen finden Sie unter Arbeiten mit gemeinsam genutzten AWS Outposts Ressourcen.

Inhalt



## Direktes VPC-Routing

Direktes VPC-Routing verwendet die private IP-Adresse der Instances in Ihrer VPC, um die Kommunikation mit Ihrem On-Premises-Netzwerk zu erleichtern. Diese Adressen werden in Ihrem On-Premises-Netzwerk mit BGP beworben. Werbung bei BGP gilt nur für die privaten IP-Adressen, die zu den Subnetzen in Ihrem Outposts-Rack gehören. Diese Art von Routing ist der Standardmodus für Outposts. In diesem Modus führt das lokale Gateway kein NAT für Instances durch, und Sie müssen Ihren Instances keine Elastic IP-Adressen zuweisen. EC2 Sie haben die Möglichkeit, Ihren eigenen Adressraum anstelle des direkten VPC-Routing-Modus zu verwenden. Weitere Informationen finden Sie unter IP-Adressen im Besitz des Kunden.

Der direkte VPC-Routing-Modus unterstützt keine überlappenden CIDR-Bereiche.

Direktes VPC-Routing wird beispielsweise nur für Netzwerkschnittstellen unterstützt. Bei Netzwerkschnittstellen, die in Ihrem Namen AWS erstellt werden (sogenannte vom Antragsteller verwaltete Netzwerkschnittstellen), sind deren private IP-Adressen von Ihrem lokalen Netzwerk aus nicht erreichbar. VPC-Endpunkte sind beispielsweise nicht direkt von Ihrem On-Premises-Netzwerk aus erreichbar.

Die folgenden Beispiele veranschaulichen das direkte VPC-Routing.

Beispiele

## Beispiel: Internetkonnektivität über die VPC

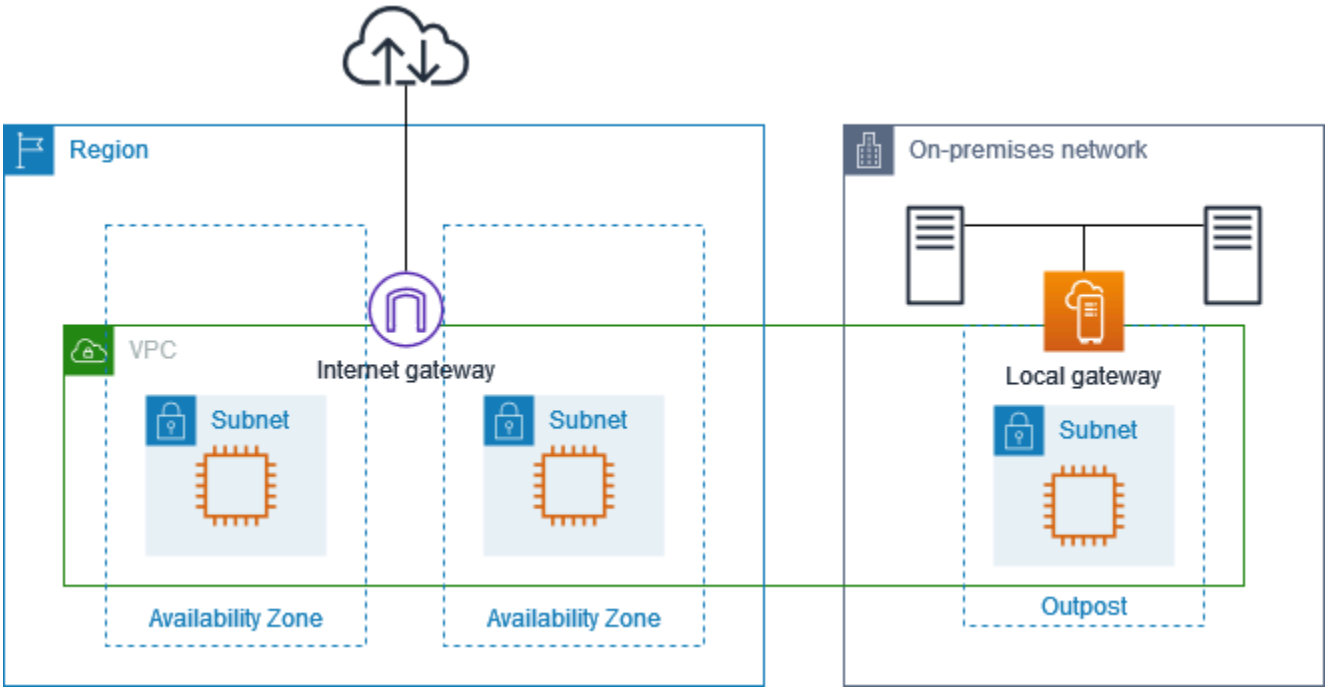
Instances in einem Outpost-Subnetz können über das an die VPC angeschlossene Internet-Gateway auf das Internet zugreifen.

Berücksichtigen Sie folgende Konfiguration:

- Die übergeordnete VPC erstreckt sich über zwei Availability Zones und hat ein Subnetz in jeder Availability Zone.
- Der Outpost hat ein Subnetz.
- Jedes Subnetz hat eine Instanz. EC2
- Das lokale Gateway verwendet BGP-Werbung, um die privaten IP-Adressen des Outpost-Subnetzes im On-Premises-Netzwerk zu bewerben.

> **Note**
>
> BGP-Werbung wird nur für Subnetze in einem Outpost unterstützt, die eine Route mit dem lokalen Gateway als Ziel haben. Alle anderen Subnetze werden nicht über BGP beworben.

Im folgenden Diagramm kann der Datenverkehr von der Instance im Outpost-Subnetz das Internet-Gateway für die VPC nutzen, um auf das Internet zuzugreifen.



Um eine Internetverbindung über die übergeordnete Region zu erreichen, muss die Routing-Tabelle für das Outpost-Subnetz die folgenden Routen haben.

| Bestimmungsort | Ziel | Kommentare |
| --- | --- | --- |
| *VPC CIDR* | Local | Stellt Konnektivität zwischen den Subnetzen in der VPC bereit. |
| 0.0.0.0 | *internet-gateway-id* | Sendet den für das Internet bestimmten Datenverkehr an das Internet-Gateway. |
| *on-premises network CIDR* | *local-gateway-id* | Sendet den für das On-Premises-Netzwerk bestimmten Datenverkehr an das lokale Gateway. |

## Beispiel: Internetkonnektivität über das On-Premises-Netzwerk

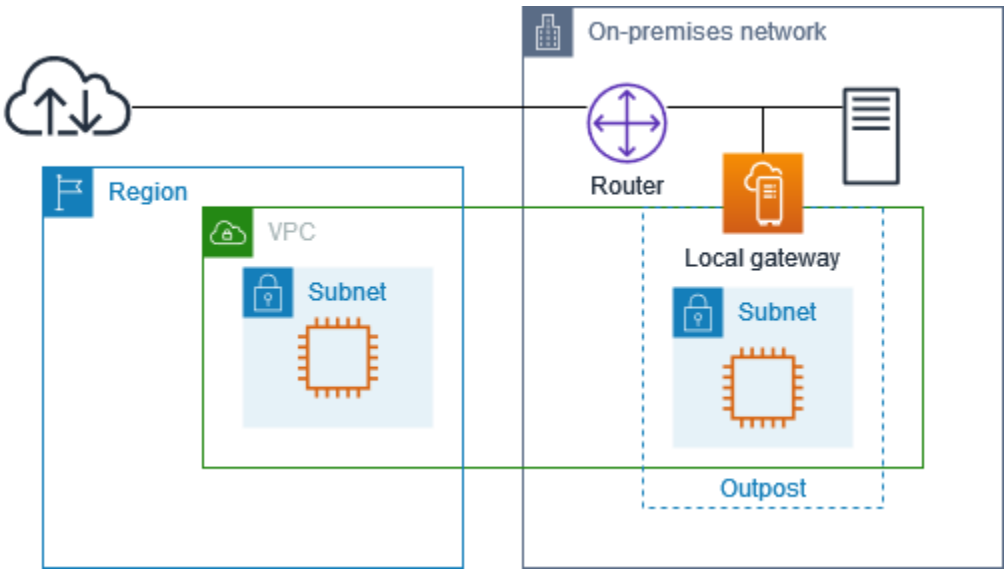
Instances in einem Outpost-Subnetz können über das On-Premises-Netzwerk auf das Internet zugreifen. Instances im Outpost-Subnetz benötigen keine öffentliche IP-Adresse oder Elastic-IP-Adresse.

Berücksichtigen Sie folgende Konfiguration:

- Das Outpost-Subnetz hat eine Instanz. EC2
- Der Router im On-Premises-Netzwerk führt Network Address Translation (NAT) aus.
- Das lokale Gateway verwendet BGP-Werbung, um die privaten IP-Adressen des Outpost-Subnetzes im On-Premises-Netzwerk zu bewerben.

> **Note**
>
> BGP-Werbung wird nur für Subnetze in einem Outpost unterstützt, die eine Route mit dem lokalen Gateway als Ziel haben. Alle anderen Subnetze werden nicht über BGP beworben.

In der folgenden Abbildung kann der Datenverkehr von der Instance im Outpost-Subnetz über das lokale Gateway auf das Internet oder das On-Premises-Netzwerk zugreifen. Der Datenverkehr aus dem On-Premises-Netzwerk verwendet das lokale Gateway, um auf die Instance im Outpost-Subnetz zuzugreifen.




Um eine Internetverbindung über das On-Premises-Netzwerk zu erreichen, muss die Routing-Tabelle für das Outpost-Subnetz die folgenden Routen haben.

| Bestimmungsort | Ziel | Kommentare |
|---|---|---|
| *VPC CIDR* | Local | Stellt Konnektivität zwischen den Subnetzen in der VPC bereit. |
| 0.0.0.0/0 | *local-gateway-id* | Sendet den für das Internet bestimmten Datenverkehr an das lokale Gateway. |

Ausgehender Zugriff auf das Internet

Datenverkehr, der von der Instance im Outpost-Subnetz mit einem Ziel im Internet initiiert wird, verwendet die Route für 0.0.0.0/0, um den Datenverkehr an das lokale Gateway weiterzuleiten. Das lokale Gateway sendet den Datenverkehr zum Router. Der Router verwendet NAT, um die private IP-Adresse in eine öffentliche IP-Adresse auf dem Router zu übersetzen, und sendet dann den Datenverkehr an das Ziel.

Ausgehender Zugriff auf das On-Premises-Netzwerk

Datenverkehr, der von der Instance im Outpost-Subnetz mit einem Ziel im On-Premises-Netzwerk initiiert wird, verwendet die Route für 0.0.0.0/0, um den Datenverkehr an das lokale Gateway weiterzuleiten. Das lokale Gateway sendet den Datenverkehr an das Ziel im On-Premises-Netzwerk.

Eingehender Zugriff aus dem On-Premises-Netzwerk

Der Datenverkehr aus dem On-Premises-Netzwerk mit einem Ziel der Instance im Outpost-Subnetz verwendet die private IP-Adresse der Instance. Wenn der Datenverkehr das lokale Gateway erreicht, sendet das lokale Gateway den Datenverkehr an das Ziel in der VPC.

## IP-Adressen im Besitz des Kunden

Standardmäßig verwendet das lokale Gateway die privaten IP-Adressen der Instances in Ihrer VPC, um die Kommunikation mit Ihrem On-Premises-Netzwerk zu erleichtern. Sie können jedoch einen Adressbereich angeben, der als kundeneigener IP-Adresspool (CoIP) bezeichnet wird und überlappende CIDR-Bereiche und andere Netzwerktopologien unterstützt.

Wenn Sie sich für CoIP entscheiden, müssen Sie einen Adresspool erstellen, ihn der lokalen Gateway-Routing-Tabelle zuweisen und diese Adressen über BGP an Ihr Kundennetzwerk weiterleiten. Alle kundeneigenen IP-Adressen, die mit Ihrer lokalen Gateway-Routing-Tabelle verknüpft sind, werden in der Routing-Tabelle als weitergegebene Routen angezeigt.

Kundeneigene IP-Adressen bieten lokale oder externe Konnektivität zu Ressourcen in Ihrem On-Premises-Netzwerk. Sie können diese IP-Adressen Ressourcen in Ihrem Outpost, z. B. EC2 Instances, zuweisen, indem Sie eine neue Elastic IP-Adresse aus dem kundeneigenen IP-Pool zuweisen und diese dann Ihrer Ressource zuweisen. Weitere Informationen finden Sie unter CoIP-Pools.

> **Note**
>
> Für einen kundeneigenen IP-Adresspool müssen Sie in der Lage sein, die Adresse in Ihrem Netzwerk weiterzuleiten.

Wenn Sie eine Elastic-IP-Adresse aus Ihrem kundeneigenen IP-Adresspool zuweisen, sind Sie weiterhin Eigentümer der IP-Adressen in Ihrem kundeneigenen IP-Adresspool. Sie sind dafür verantwortlich, sie nach Bedarf in Ihren internen Netzwerken oder Ihrem WAN zu bewerben.

Sie können Ihren kundeneigenen Pool optional mit mehreren Personen AWS-Konten in Ihrer Organisation teilen, indem Sie. AWS Resource Access Manager Nachdem Sie den Pool gemeinsam genutzt haben, können die Teilnehmer eine Elastic IP-Adresse aus dem kundeneigenen IP-Adresspool zuweisen und sie dann einer EC2 Instance im Outpost zuweisen. Weitere Informationen finden Sie unter Gemeinsam genutzte -Ressourcen.

Beispiele

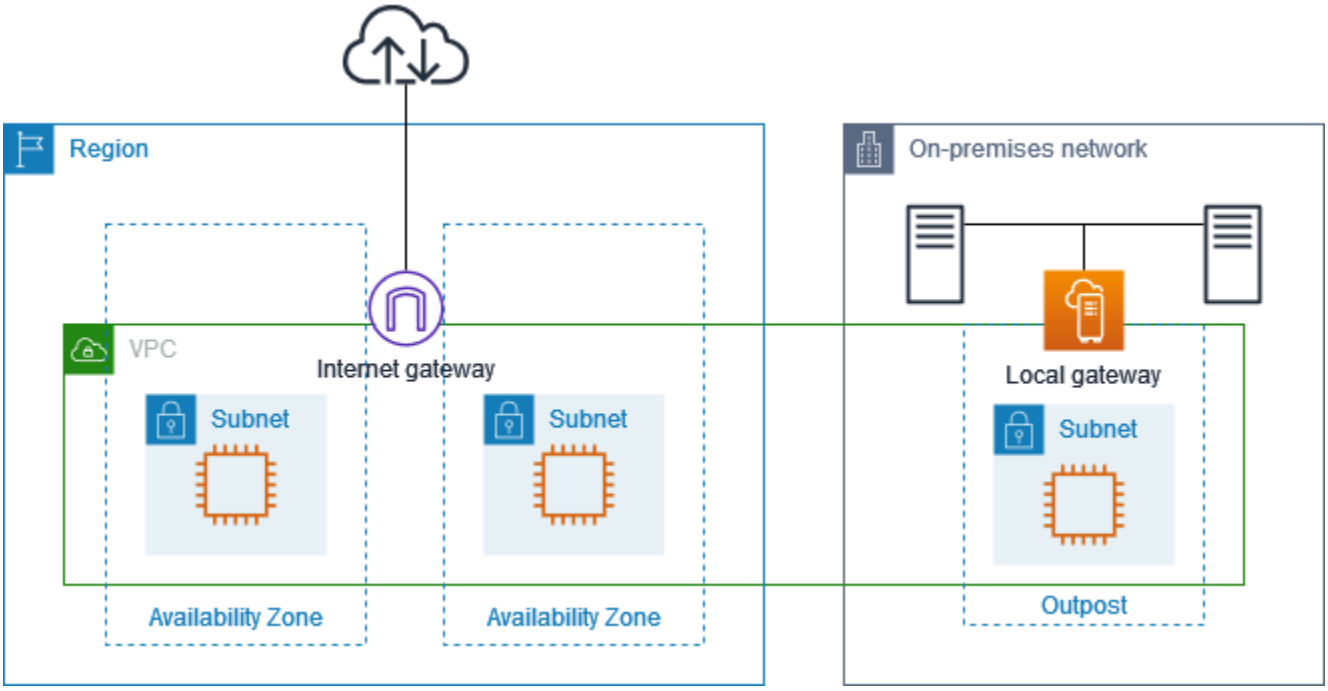
- Beispiel: Internetkonnektivität über die VPC
- Beispiel: Internetkonnektivität über das On-Premises-Netzwerk

## Beispiel: Internetkonnektivität über die VPC

Instances in einem Outpost-Subnetz können über das an die VPC angeschlossene Internet-Gateway auf das Internet zugreifen.

Berücksichtigen Sie folgende Konfiguration:

- Die übergeordnete VPC erstreckt sich über zwei Availability Zones und hat ein Subnetz in jeder Availability Zone.
- Der Outpost hat ein Subnetz.
- Jedes Subnetz hat eine Instanz. EC2
- Es gibt einen kundeneigenen IP-Adresspool.
- Die Instance im Outpost-Subnetz hat eine Elastic-IP-Adresse aus dem kundeneigenen IP-Adresspool.
- Das lokale Gateway verwendet BGP-Werbung, um den kundeneigenen IP-Adresspool im On-Premises-Netzwerk zu bewerben.



Um eine Internetverbindung über die Region zu erreichen, muss die Routing-Tabelle für das Outpost-Subnetz die folgenden Routen haben.

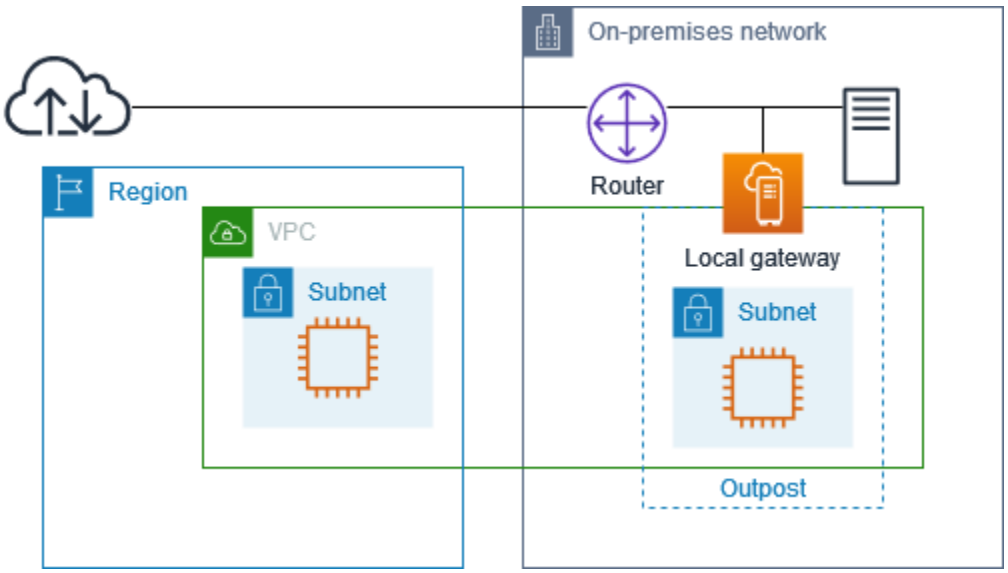
| Bestimmungsort | Ziel | Kommentare |
| --- | --- | --- |
| *VPC CIDR* | Local | Stellt Konnektivität zwischen den Subnetzen in der VPC bereit. |
| 0.0.0.0 | *internet-gateway-id* | Sendet den für das öffentliche Internet bestimmten Datenverkehr an das Internet-Gateway. |
| *On-premises network CIDR* | *local-gateway-id* | Sendet den für das On-Premises-Netzwerk bestimmten Datenverkehr an das lokale Gateway. |

## Beispiel: Internetkonnektivität über das On-Premises-Netzwerk

Instances in einem Outpost-Subnetz können über das On-Premises-Netzwerk auf das Internet zugreifen.

Berücksichtigen Sie folgende Konfiguration:

- Das Outpost-Subnetz hat eine Instanz. EC2
- Es gibt einen kundeneigenen IP-Adresspool.
- Das lokale Gateway verwendet BGP-Werbung, um den kundeneigenen IP-Adresspool im On-Premises-Netzwerk zu bewerben.
- Eine Elastic IP-Adresszuweisung, die 10.0.3.112 10.1.0.2 zuordnet.
- Der Router im On-Premises-Kundennetzwerk führt NAT durch.




Um eine Internetverbindung über lokale Gateway zu erreichen, muss die Routing-Tabelle für das Outpost-Subnetz die folgenden Routen haben.

| Bestimmungsort | Ziel | Kommentare |
|---|---|---|
| *VPC CIDR* | Local | Stellt Konnektivität zwischen den Subnetzen in der VPC bereit. |
| 0.0.0.0/0 | *local-gateway-id* | Sendet den für das Internet bestimmten Datenverkehr an das lokale Gateway. |

Ausgehender Zugriff auf das Internet

Datenverkehr, der von der EC2 Instance im Outpost-Subnetz mit einem Ziel im Internet initiiert wird, verwendet die Route für 0.0.0.0/0, um den Verkehr an das lokale Gateway weiterzuleiten. Das lokale Gateway ordnet die private IP-Adresse der Instance der kundeneigenen IP-Adresse zu und sendet dann den Datenverkehr an den Router. Der Router verwendet NAT, um die kundeneigene IP-Adresse in eine öffentliche IP-Adresse auf dem Router zu übersetzen, und sendet dann den Datenverkehr an das Ziel.

Ausgehender Zugriff auf das On-Premises-Netzwerk

Datenverkehr, der von der EC2 Instance im Outpost-Subnetz mit einem Ziel im lokalen Netzwerk initiiert wird, verwendet die Route für 0.0.0.0/0, um den Verkehr an das lokale Gateway

weiterzuleiten. Das lokale Gateway übersetzt die IP-Adresse der EC2 Instance in die kundeneigene IP-Adresse (Elastic IP-Adresse) und sendet den Datenverkehr dann an das Ziel.

Eingehender Zugriff aus dem On-Premises-Netzwerk

Der Datenverkehr aus dem On-Premises-Netzwerk mit einem Ziel der Instance im Outpost-Subnetz verwendet die kundeneigene IP-Adresse (Elastic-IP-Adresse) der Instance. Wenn der Datenverkehr das lokale Gateway erreicht, ordnet das lokale Gateway die kundeneigene IP-Adresse (Elastic-IP-Adresse) der Instance-IP-Adresse zu und sendet den Datenverkehr dann an das Ziel in der VPC. Darüber hinaus bewertet die Routing-Tabelle des lokalen Gateways alle Routen, die auf Elastic-Netzwerkschnittstellen abzielen. Wenn die Zieladresse mit dem Ziel-CIDR einer statischen Route übereinstimmt, wird der Datenverkehr an diese elastische Netzwerkschnittstelle gesendet. Wenn der Datenverkehr einer statischen Route zu einer elastischen Netzwerkschnittstelle folgt, bleibt die Zieladresse erhalten und wird nicht in die private IP-Adresse der Netzwerkschnittstelle übersetzt.

### Benutzerdefinierte Routing-Tabellen

Sie können eine benutzerdefinierte Routing-Tabelle für Ihr lokales Gateway erstellen. Die lokale Gateway-Routentabelle muss mit einer VIF-Gruppe und einer VPC verknüpft sein. step-by-stepAnweisungen finden Sie unter Lokale Gateway-Konnektivität konfigurieren.

## Routen in der Routentabelle des lokalen Gateways

Sie können lokale Gateway-Routentabellen und eingehende Routen zu Netzwerkschnittstellen auf Ihrem Outpost erstellen. Sie können auch eine bestehende lokale Gateway-Eingangsroute ändern, um die Zielnetzwerkschnittstelle zu ändern.

Eine Route hat nur dann den Status „Aktiv“, wenn ihre Zielnetzwerkschnittstelle mit einer laufenden Instance verbunden ist. Wenn die Instanz gestoppt oder die Schnittstelle getrennt ist, ändert sich der Status der Route von aktiv in Blackhole.

Inhalt

# Anforderungen und Einschränkungen

Es gelten die folgenden Anforderungen und Einschränkungen:

- Die Zielnetzwerkschnittstelle muss zu einem Subnetz in Ihrem Outpost gehören und mit einer Instance in diesem Outpost verbunden sein. Eine lokale Gateway-Route kann nicht auf eine EC2 Amazon-Instance in einem anderen Outpost oder in der übergeordneten AWS-Region Instanz abzielen.
- Das Subnetz muss zu einer VPC gehören, die der Routing-Tabelle des lokalen Gateways zugeordnet ist.
- Sie dürfen nicht mehr als 100 Netzwerkschnittstellen-Routen in derselben Routentabelle überschreiten.
- AWS priorisiert die spezifischste Route, und wenn die Routen übereinstimmen, priorisieren wir statische Routen gegenüber weitergegebenen Routen.
- Schnittstellen-VPC-Endpunkte werden nicht unterstützt.
- BGP-Werbung gilt nur für Subnetze in einem Outpost, deren Routing-Tabelle eine Route enthält, die auf das lokale Gateway abzielt. Wenn Subnetze in der Routing-Tabelle keine Route enthalten, die auf das lokale Gateway abzielt, werden diese Subnetze nicht mit BGP angekündigt.
- Nur Netzwerkschnittstellen, die mit Outpost-Instances verbunden sind, können über das lokale Gateway für diesen Outpost kommunizieren. Netzwerkschnittstellen, die zum Outpost-Subnetz gehören, aber mit einer Instance in der Region verbunden sind, können nicht über das lokale Gateway für diesen Outpost kommunizieren.
- Vom Anforderer verwaltete Schnittstellen, z. B. solche, die für VPC-Endpunkte erstellt wurden, können vom lokalen Netzwerk aus nicht über das lokale Gateway erreicht werden. Sie können nur von Instanzen aus erreicht werden, die sich im Outpost-Subnetz befinden.

Es gelten die folgenden NAT-Überlegungen:

- Das lokale Gateway führt bei Datenverkehr, der einer Netzwerkschnittstellenroute entspricht, kein NAT durch. Stattdessen wird die Ziel-IP-Adresse beibehalten.
- Schalten Sie die Quell-/Zielüberprüfung für die Zielnetzwerkschnittstelle aus. Weitere Informationen finden Sie unter Konzepte der Netzwerkschnittstelle im  EC2 Amazon-Benutzerhandbuch.
- Konfigurieren Sie das Betriebssystem so, dass der Datenverkehr vom Ziel-CIDR auf der Netzwerkschnittstelle akzeptiert wird.

# Erstellen benutzerdefinierter Routing-Tabellen für das lokale Gateway

Sie können eine benutzerdefinierte Routing-Tabelle für Ihr lokales Gateway auf der AWS Outposts - Konsole erstellen.

Erstellen einer benutzerdefinierten Routing-Tabelle des lokalen Gateways mithilfe der Konsole

1. Öffnen Sie die AWS Outposts Konsole unter https://console.aws.amazon.com/outposts/.
2. Um das zu ändern AWS-Region, verwenden Sie die Regionsauswahl in der oberen rechten Ecke der Seite.
3. Wählen Sie im Navigationsbereich Lokale Gateway-Routing-Tabelle aus.
4. Wählen Sie Lokale Gateway-Routing-Tabelle erstellen aus.
5. (Optional) Geben Sie bei Name einen Namen für Ihre Routing-Tabelle des lokalen Gateways ein.
6. Wählen Sie unter Lokales Gateway Ihr lokales Gateway aus.
7. (Optional) Wählen Sie VIF-Gruppe zuordnen und wählen Sie Ihre VIF-Gruppe.

   Bearbeiten Sie die Routentabelle des lokalen Gateways, um eine statische Route hinzuzufügen, deren Ziel die VIF-Gruppe ist.
8. Wählen Sie unter Modus einen Modus für die Kommunikation mit Ihrem On-Premises-Netzwerk aus.

   - Wählen Sie Direktes VPC-Routing, um die private IP-Adresse einer Instance zu verwenden.
   - Wählen Sie CoIP, um die kundeneigene IP-Adresse zu verwenden.
     - (Optional) Hinzufügen oder Entfernen von CoIP-Pools und zusätzlichen CIDR-Blöcken

       [CoIP-Pool hinzufügen] Wählen Sie Neuen Pool hinzufügen und führen Sie folgende Schritte aus:
       - Geben Sie unter Name einen Namen für Ihren CoIP-Pool ein.
       - Geben Sie für CIDR einen CIDR-Block mit kundeneigenen IP-Adressen ein.
     - [CIDR-Blöcke hinzufügen] Wählen Sie Neue CIDR hinzufügen und geben Sie einen Bereich von IP-Adressen im Kundenbesitz ein.
     - [Einen CoIP-Pool oder einen zusätzlichen CIDR-Block entfernen] Wählen Sie rechts neben einem CIDR-Block oder unter dem CoIP-Pool Entfernen.

       Sie können bis zu 10 CoIP-Pools und 100 CIDR-Blöcke angeben.
9. (Optional) Hinzufügen oder Entfernen eines Tags (Markierung).

[Tag (Markierung) hinzufügen] Wählen Sie Add new tag (Neuen Tag (Markierung) hinzufügen), und führen Sie die folgenden Schritte aus:

- Geben Sie bei Key (Schlüssel) den Schlüsselnamen ein.
- Geben Sie bei Value (Wert) den Wert des Schlüssels ein.

[Tag entfernen] Wählen Sie Entfernen rechts neben dem Schlüssel und dem Wert des Tags.

10. Wählen Sie Lokale Gateway-Routing-Tabelle erstellen aus.

## Wechseln Sie zwischen den Routing-Tabellen eines lokalen Gateways oder Löschen einer Routing-Tabelle eines lokalen Gateways

Sie müssen die Routing-Tabelle des lokalen Gateways löschen und neu erstellen, um zwischen den Modi zu wechseln. Das Löschen der Routing-Tabelle des lokalen Gateways führt zur Unterbrechung des Datenverkehrs im Netzwerk.

So wechseln Sie den Modus oder löschen eine Routing-Tabelle des lokalen Gateways

1. Öffnen Sie die AWS Outposts Konsole unter. https://console.aws.amazon.com/outposts/
2. Vergewissern Sie sich, dass Sie auf der richtigen Seite sind AWS-Region.

   Um die Region zu ändern, verwenden Sie die Regionsauswahl in der oberen rechten Ecke der Seite.
3. Wählen Sie im Navigationsbereich Lokale Gateway-Routing-Tabellen aus.
4. Überprüfen Sie, ob die lokale Gateway-Routentabelle einer VIF-Gruppe zugeordnet ist. Wenn sie verknüpft ist, müssen Sie die Zuordnung zwischen der lokalen Gateway-Routentabelle und der VIF-Gruppe entfernen.

   a. Wählen Sie die ID der lokalen Gateway-Routentabelle.
   b. Wählen Sie die Registerkarte VIF-Gruppenzuordnung.
   c. Wenn der lokalen Gateway-Routentabelle eine oder mehrere VIF-Gruppen zugeordnet sind, wählen Sie VIF-Gruppenzuordnung bearbeiten aus.
   d. Deaktivieren Sie das Kontrollkästchen VIF-Gruppe zuordnen.
   e. Wählen Sie Änderungen speichern aus.
5. Wählen Sie „Lokale Gateway-Routentabelle löschen“.

6. Geben Sie **`delete`** im Bestätigungsdialogfeld ein und wählen Sie dann Löschen.
7. (Optional) Erstellen Sie eine Routing-Tabelle eines lokalen Gateways mit einem neuen Modus.
   a. Wählen Sie im Navigationsbereich Lokale Gateway-Routing-Tabellen aus.
   b. Wählen Sie Lokale Gateway-Routing-Tabelle erstellen aus.
   c. Konfigurieren Sie die Routing-Tabelle des lokalen Gateways unter Verwendung des neuen Modus. Weitere Informationen finden Sie unter Erstellen benutzerdefinierter Routing-Tabellen für lokale Gateways.

## Erstellen Sie einen CoIP-Pool

Sie können IP-Adressbereiche angeben, um die Kommunikation zwischen Ihrem On-Premises-Netzwerk und Instances in Ihrer VPC zu erleichtern. Weitere Informationen finden Sie unter Kundeneigene IP-Adressen.

Kundeneigene IP-Pools sind für lokale Gateway-Routing-Tabelle im CoIP-Modus verfügbar.

Gehen Sie wie folgt vor, um einen CoIP-Pool zu erstellen.

Console

Um einen CoIP-Pool mit der Konsole zu erstellen

1. Öffnen Sie die AWS Outposts Konsole unter. https://console.aws.amazon.com/outposts/
2. Um das zu ändern AWS-Region, verwenden Sie die Regionsauswahl in der oberen rechten Ecke der Seite.
3. Wählen Sie im Navigationsbereich Lokale Gateway-Routing-Tabellen aus.
4. Wählen Sie die Routing-Tabelle.
5. Wählen Sie im Detailbereich die Registerkarte CoIP-Pools und dann CoIP-Pool erstellen aus.
6. (Optional) Geben Sie unter Name einen Namen für Ihren CoIP-Pool ein.
7. Wählen Sie Neue CIDR hinzufügen und geben Sie einen Bereich von IP-Adressen im Kundenbesitz ein.
8. (Optional) Um einen CIDR-Block hinzuzufügen, wählen Sie Neues CIDR hinzufügen und geben Sie einen Bereich von kundeneigenen IP-Adressen ein.
9. Wählen Sie CoIP-Pool erstellen.

AWS CLI

Um einen CoIP-Pool mit dem zu erstellen AWS CLI

1. Verwenden Sie den create-coip-poolBefehl, um einen Pool von CoIP-Adressen für die angegebene lokale Gateway-Routentabelle zu erstellen.

```
aws ec2 create-coip-pool --local-gateway-route-table-id lgw-rtb-
abcdefg1234567890
```

Es folgt eine Beispielausgabe.

```
{
    "CoipPool": {
        "PoolId": "ipv4pool-coip-1234567890abcdefg",
        "LocalGatewayRouteTableId": "lgw-rtb-abcdefg1234567890",
        "PoolArn": "arn:aws:ec2:us-west-2:123456789012:coip-pool/ipv4pool-
coip-1234567890abcdefg"
    }
}
```

2. Verwenden Sie den create-coip-cidrBefehl, um einen Bereich von CoIP-Adressen im angegebenen CoIP-Pool zu erstellen.

```
aws ec2 create-coip-cidr --cidr 15.0.0.0/24 --coip-pool-id ipv4pool-
coip-1234567890abcdefg
```

Es folgt eine Beispielausgabe.

```
{
    "CoipCidr": {
        "Cidr": "15.0.0.0/24",
        "CoipPoolId": "ipv4pool-coip-1234567890abcdefg",
        "LocalGatewayRouteTableId": "lgw-rtb-abcdefg1234567890"
    }
}
```

Nachdem Sie einen CoIP-Pool erstellt haben, verwenden Sie das folgende Verfahren, um Ihrer Instance eine Adresse zuzuweisen.

### Console

Um einer Instance mithilfe der Konsole eine CoIP-Adresse zuzuweisen

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Elastic IPs aus.
3. Wählen Sie Elastic-IP-Adresse zuweisen aus.
4. Wählen Sie für Network Border Group den Standort, von dem aus die IP-Adresse beworben wird.
5. Wählen Sie unter Öffentlicher IPv4 Adresspool die Option Kundeneigener IPv4 Adresspool aus.
6. Wählen Sie für Kundeneigener IPv4 Adresspool den Pool aus, den Sie konfiguriert haben.
7. Wählen Sie Allocate aus.
8. Wählen Sie die Elastic-IP-Adresse aus, und wählen Sie Aktionen, Elastic-IP-Adresse zuordnen.
9. Wählen Sie die Instance aus Instance, und klicken Sie anschließend auf Zuordnen.

### AWS CLI

Um einer Instanz eine CoIP-Adresse zuzuweisen, verwenden Sie AWS CLI

1. Verwenden Sie den describe-coip-poolsBefehl, um Informationen über Ihre kundeneigenen Adresspools abzurufen.

```
aws ec2 describe-coip-pools
```

Es folgt eine Beispielausgabe.

```
{
    "CoipPools": [
        {
            "PoolId": "ipv4pool-coip-0abcdef0123456789",
            "PoolCidrs":  [
                "192.168.0.0/16"
            ],
            "LocalGatewayRouteTableId": "lgw-rtb-0abcdef0123456789"
        }
    ]
```

```
}
```

2. Verwenden Sie den Befehl allocate-address, um eine Elastic-IP-Adresse zuzuweisen. Verwenden Sie die im vorherigen Schritt zurückgegebene Pool-ID.

```
aws ec2 allocate-address--address 192.0.2.128 --customer-owned-ipv4-
pool ipv4pool-coip-0abcdef0123456789
```

Es folgt eine Beispielausgabe.

```
{
    "CustomerOwnedIp": "192.0.2.128",
    "AllocationId": "eipalloc-02463d08ceEXAMPLE",
    "CustomerOwnedIpv4Pool": "ipv4pool-coip-0abcdef0123456789",
}
```

3. Verwenden Sie den Befehl associate-address, um die Elastic-IP-Adresse mit der Outpost -Instance zu verknüpfen. Verwenden Sie die Zuordnungs-ID aus dem vorherigen Schritt.

```
aws ec2 associate-address --allocation-id eipalloc-02463d08ceEXAMPLE --network-
interface-id eni-1a2b3c4d
```

Es folgt eine Beispielausgabe.

```
{
    "AssociationId": "eipassoc-02463d08ceEXAMPLE",
}
```

# Lokale Netzwerkkonnektivität für Outposts-Racks

Sie benötigen die folgenden Komponenten, um Ihr Outposts-Rack mit Ihrem lokalen Netzwerk zu verbinden:

- Physische Konnektivität vom Outpost-Patchpanel zu den lokalen Netzwerkgeräten Ihrer Kunden.
- Link Aggregation Control Protocol (LACP), um zwei Link Aggregation Group (LAG)-Verbindungen zu Ihren Outpost-Netzwerkgeräten und zu Ihren lokalen Netzwerkgeräten herzustellen.
- Virtuelle LAN-Konnektivität (VLAN) zwischen dem Outpost und den lokalen Netzwerkgeräten Ihrer Kunden.
- point-to-pointLayer-3-Konnektivität für jedes VLAN.
- Border Gateway Protocol (BGP) für das Bewerben der Routen zwischen dem Outpost und Ihrem On-Premises-Service-Link.
- BGP für das Bewerben der Routen zwischen dem Outpost und Ihrem On-Premises-Netzwerkgerät vor Ort für die Konnektivität zum On-Premises-Gateway.

Inhalt



## Tatsächliche Konnektivität

Ein Outposts-Rack besteht aus zwei physischen Netzwerkgeräten, die an Ihr lokales Netzwerk angeschlossen werden.

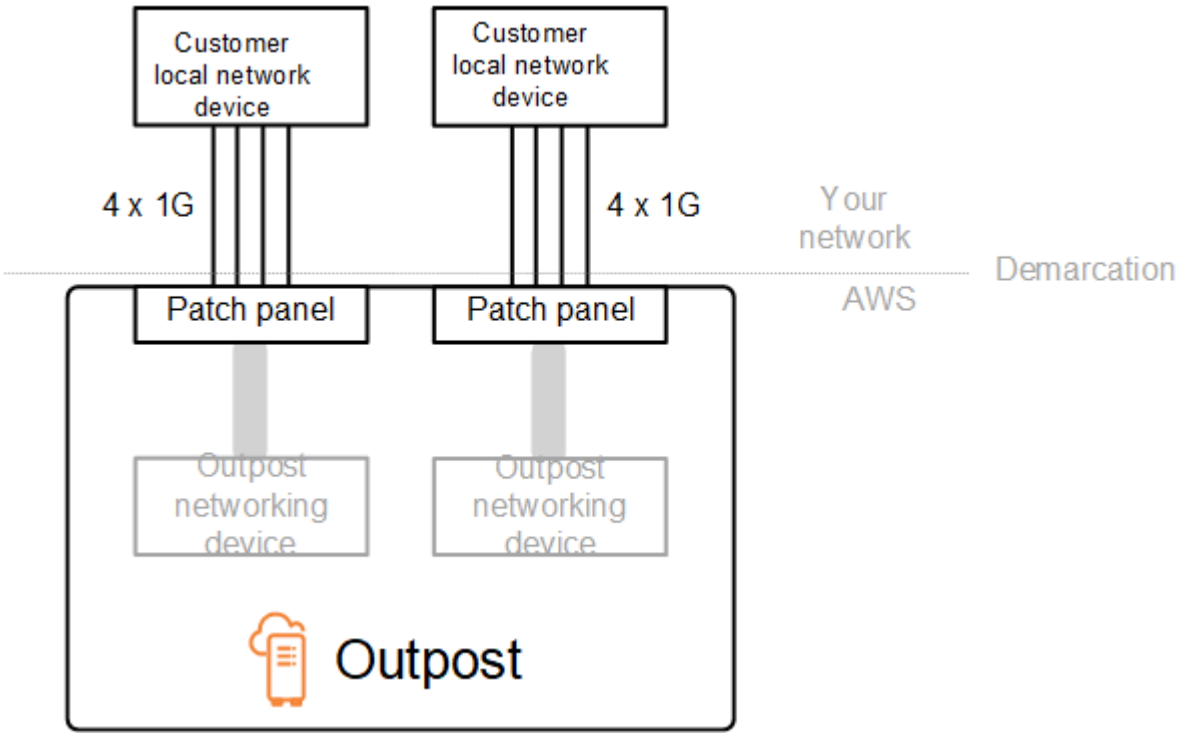
Ein Outpost benötigt mindestens zwei physische Verbindungen zwischen diesen Outpost-Netzwerkgeräten und Ihren lokalen Netzwerkgeräten. Ein Outpost unterstützt die folgenden Uplink-Geschwindigkeiten und -Mengen für jedes Outpost-Netzwerkgerät.

| 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 Gbit/s oder 100 Gbit/s | 1, 2, oder 4 |

Die Uplink-Geschwindigkeit und -Menge sind auf jedem Outpost-Netzwerkgerät symmetrisch. Wenn Sie 100 Gbit/s als Uplink-Geschwindigkeit verwenden, müssen Sie den Link mit Forward Error Correction (FEC) konfigurieren. CL91

Outposts-Racks können Singlemode-Glasfaser (SMF) mit Lucent Connector (LC), Multimode-Glasfaser (MMF) oder MMF mit LC unterstützen. OM4 AWS stellt die Optik bereit, die mit der Glasfaser kompatibel ist, die Sie an der Rack-Position bereitstellen.

In der folgenden Abbildung ist die physische Abgrenzung das Glasfaser-Patchpanel in jedem Outpost. Sie stellen die Glasfaserkabel bereit, die erforderlich sind, um den Outpost mit dem Patchpanel zu verbinden.




# Link-Aggregation

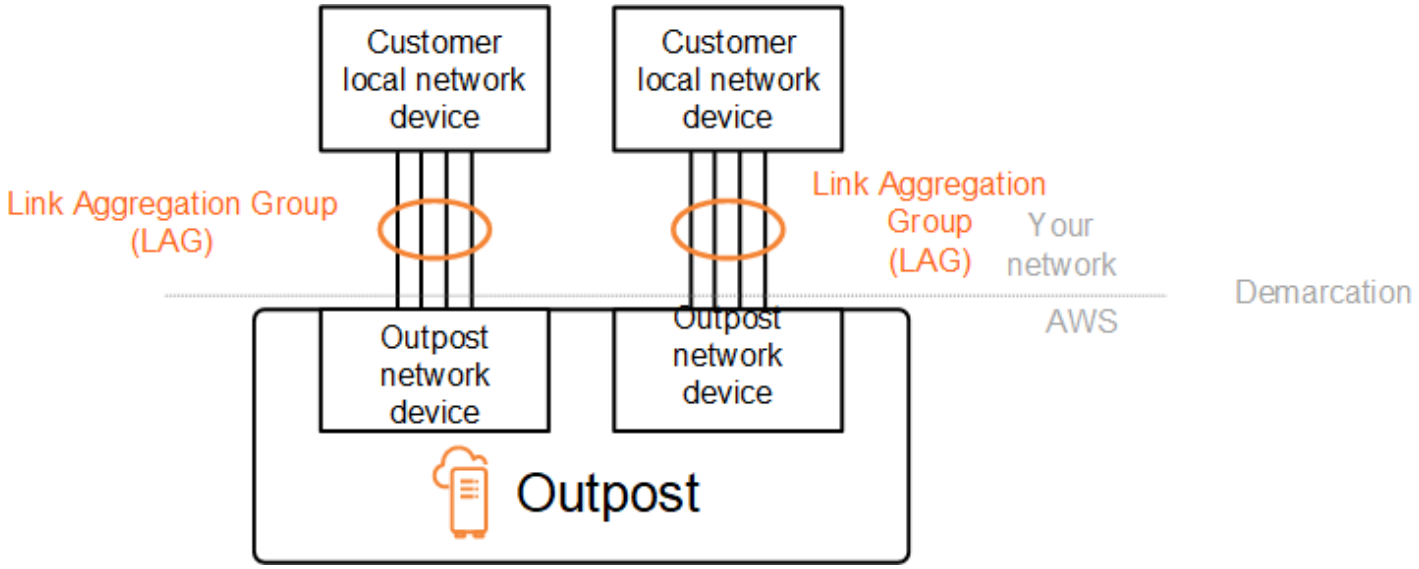
AWS Outposts verwendet das Link Aggregation Control Protocol (LACP), um LAG-Verbindungen (Link Aggregation Group) zwischen Ihren Outpost-Netzwerkgeräten und Ihren lokalen Netzwerkgeräten herzustellen. Die Links von jedem Outpost-Netzwerkgerät werden zu einer Ethernet-LAG zusammengefasst, die eine einzelne Netzwerkverbindung darstellt. Diese LAGs verwenden LACP mit Standard-Fasttimern. Sie können die Verwendung von langsamen LAGs Timern nicht konfigurieren.

Um eine Outpost-Installation an Ihrem Standort zu aktivieren, müssen Sie Ihre LAG-Verbindungen auf Ihren Netzwerkgeräten konfigurieren.

Aus logischer Sicht sollten Sie die Outpost-Patchpanels als Abgrenzungspunkt ignorieren und die Outpost-Netzwerkgeräte verwenden.

Bei Bereitstellungen mit mehreren Racks muss ein Outpost vier Racks LAGs zwischen der Aggregationsebene der Outpost-Netzwerkgeräte und Ihren lokalen Netzwerkgeräten haben.

Das folgende Diagramm zeigt vier physische Verbindungen zwischen jedem Outpost-Netzwerkgerät und dem angeschlossenen lokalen Netzwerkgerät. Wir verwenden Ethernet LAGs , um die physischen Verbindungen zwischen den Outpost-Netzwerkgeräten und den lokalen Netzwerkgeräten des Kunden zu aggregieren.




# Virtuell LANs

Jede LAG zwischen einem Outpost-Netzwerkgerät und einem lokalen Netzwerkgerät muss als IEEE 802.1q-Ethernet-Trunk konfiguriert werden. Dies ermöglicht die Verwendung mehrerer Datenpfade VLANs für die Netzwerktrennung.

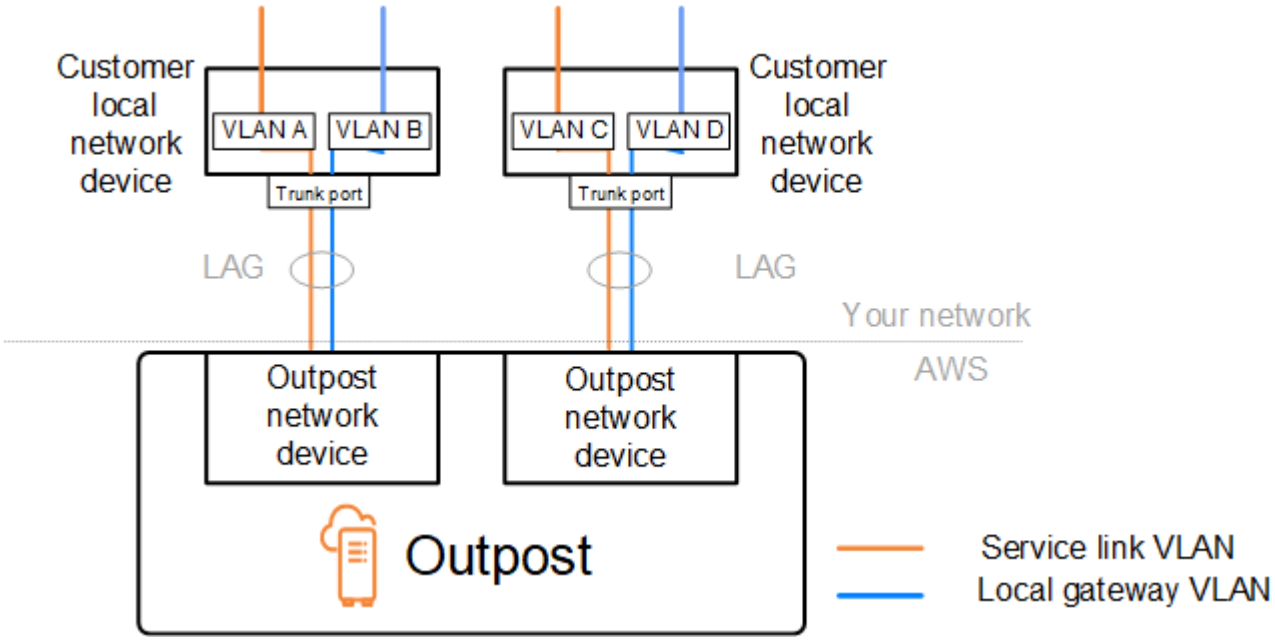
Jeder Outpost verfügt über Folgendes VLANs , um mit Ihren lokalen Netzwerkgeräten zu kommunizieren:

- Service Link VLAN – Ermöglicht die Kommunikation zwischen Ihrem Outpost und Ihren lokalen Netzwerkgeräten, um einen Service Link-Pfad für die Service Link-Konnektivität einzurichten. Weitere Informationen finden Sie unter AWS Outposts -Konnektivität zu AWS -Regionen.
- Lokales Gateway-VLAN – Ermöglicht die Kommunikation zwischen Ihrem Outpost und Ihren lokalen Netzwerkgeräten, um einen lokalen Gateway-Pfad einzurichten, um Ihre Outpost-Subnetze und Ihr lokales Netzwerk zu verbinden. Das lokale Outpost-Gateway nutzt dieses VLAN, um Ihren Instances die Verbindung zu Ihrem On-Premises-Netzwerk zu ermöglichen, was auch den Internetzugang über Ihr Netzwerk umfassen kann. Weitere Informationen finden Sie unter Lokales Gateway.

Sie können das Service Link-VLAN und das lokale Gateway-VLAN nur zwischen dem Outpost und den lokalen Netzwerkgeräten Ihres Kunden konfigurieren.

Ein Outpost ist so konzipiert, dass er die Datenpfade für Service Link und lokales Gateway in zwei isolierte Netzwerke aufteilt. Auf diese Weise können Sie auswählen, welches Ihrer Netzwerke

mit Diensten kommunizieren kann, die auf dem Outpost ausgeführt werden. Außerdem können Sie so einrichten, dass der Service ein isoliertes Netzwerk vom lokalen Gateway-Netzwerk verbindet, indem Sie mehrere Routing-Tabellen auf dem lokalen Netzwerkgerät Ihres Kunden verwenden, die allgemein als Virtual Routing and Forwarding Instances (VRF) bezeichnet werden. Die Demarkationslinie befindet sich am Port der Outpost-Netzwerkgeräte. AWS verwaltet jede Infrastruktur auf der AWS Seite der Verbindung, und Sie verwalten jede Infrastruktur auf Ihrer Seite der Leitung.




Um Ihren Outpost während der Installation und des laufenden Betriebs in Ihr lokales Netzwerk zu integrieren, müssen Sie die VLANs verbrauchten Ressourcen den Outpost-Netzwerkgeräten und den lokalen Netzwerkgeräten des Kunden zuordnen. Sie müssen diese Informationen vor der Installation angeben. AWS Weitere Informationen finden Sie unter the section called “Checkliste zur Netzwerkbereitschaft”.

## Netzwerk-Layer-Konnektivität

Um Konnektivität auf Netzwerkebene herzustellen, ist jedes Outpost-Netzwerkgerät mit virtuellen Schnittstellen (VIFs) konfiguriert, die die IP-Adresse für jedes VLAN enthalten. Über diese VIFs können AWS Outposts Netzwerkgeräte IP-Konnektivität und BGP-Sitzungen mit Ihren lokalen Netzwerkgeräten einrichten.

Wir empfehlen Folgendes:

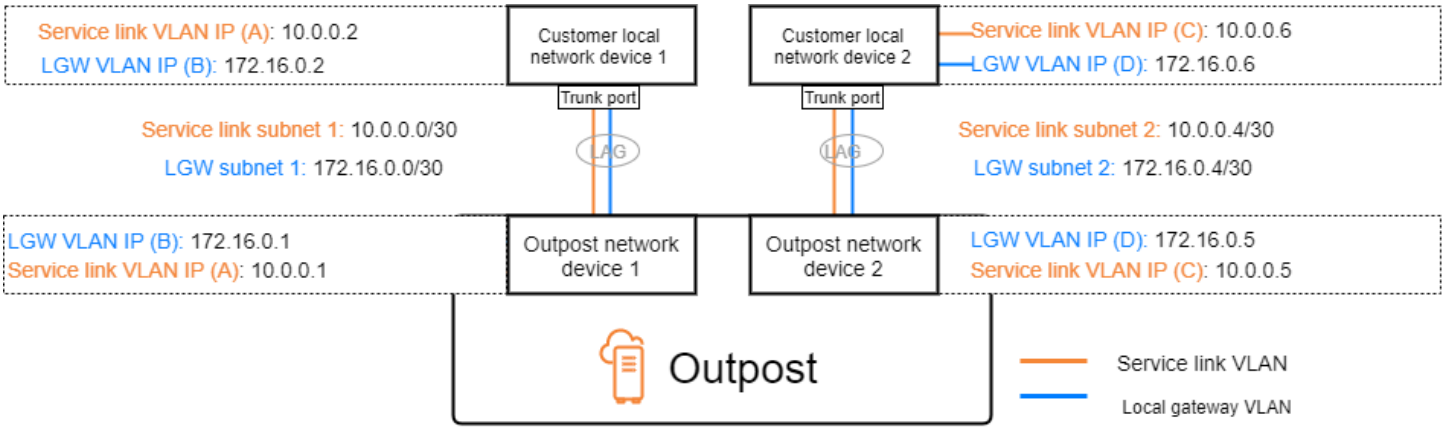
- Verwenden Sie ein dediziertes Subnetz mit einem /30- oder /31-CIDR, um diese logische Konnektivität darzustellen. point-to-point
- Stellen Sie keine Brücke VLANs zwischen Ihren lokalen Netzwerkgeräten her.

Für die Konnektivität auf Netzwerkebene müssen Sie zwei Pfade einrichten:

- Service-Link-Pfad – Um diesen Pfad einzurichten, geben Sie ein VLAN-Subnetz mit einem Bereich von /30 oder /31 und eine IP-Adresse für jedes Service Link-VLAN auf dem AWS Outposts -Netzwerkgerät an. Virtuelle Service Link-Schnittstellen (VIFs) werden für diesen Pfad verwendet, um IP-Konnektivität und BGP-Sitzungen zwischen Ihrem Outpost und Ihren lokalen Netzwerkgeräten für Service Link-Konnektivität herzustellen. Weitere Informationen finden Sie unter AWS Outposts -Konnektivität zu AWS -Regionen.
- Lokaler Gateway-Pfad – Um diesen Pfad einzurichten, geben Sie ein VLAN-Subnetz mit einem Bereich von /30 oder /31 und eine IP-Adresse für das lokale Gateway-VLAN auf dem AWS Outposts -Netzwerkgerät an. Auf diesem Pfad VIFs werden lokale Gateways verwendet, um IP-Konnektivität und BGP-Sitzungen zwischen Ihrem Outpost und Ihren lokalen Netzwerkgeräten für Ihre lokale Ressourcenkonnektivität herzustellen.

Das folgende Diagramm zeigt die Verbindungen von jedem Outpost-Netzwerkgerät zum lokalen Netzwerkgerät des Kunden für den Service-Link-Pfad und den lokalen Gateway-Pfad. Für dieses VLANs Beispiel gibt es vier:

- VLAN A steht für den Service-Link-Pfad, der das Outpost-Netzwerkgerät 1 mit dem lokalen Netzwerkgerät 1 des Kunden verbindet.
- VLAN B steht für den lokalen Gateway-Pfad, der das Outpost-Netzwerkgerät 1 mit dem lokalen Netzwerkgerät 1 des Kunden verbindet.
- VLAN C steht für den Service-Link-Pfad, der das Outpost-Netzwerkgerät 2 mit dem lokalen Netzwerkgerät 2 des Kunden verbindet.
- VLAN D steht für den lokalen Gateway-Pfad, der das Outpost-Netzwerkgerät 2 mit dem lokalen Netzwerkgerät 2 des Kunden verbindet.




Die folgende Tabelle zeigt Beispielwerte für die Subnetze, die das Outpost-Netzwerkgerät 1 mit dem lokalen Netzwerkgerät 1 des Kunden verbinden.

| VLAN | Subnetz | Kundengerät 1 (IP) | AWS EINS 1 IP |
|---|---|---|---|
| A | 10.0.0.0/30 | 10.0.0.2 | 10.0.0.1 |
| B | 172.16.0.0/30 | 172,16,0,2 | 172,16,0,1 |

Die folgende Tabelle zeigt Beispielwerte für die Subnetze, die das Outpost-Netzwerkgerät 2 mit dem lokalen Netzwerkgerät 2 des Kunden verbinden.

| VLAN | Subnetz | Kundengerät 2 (IP) | AWS EINS 2 IP |
|---|---|---|---|
| C | 10.0.0.4/30 | 10.0.0.6 | 10.0.0.5 |
| D | 172.16.0.4/30 | 172.16.0.6 | 172.16.0.5 |

# ACE-Rack-Konnektivität

> **Note**
>
> Überspringen Sie diesen Abschnitt, wenn Sie kein ACE-Rack benötigen.

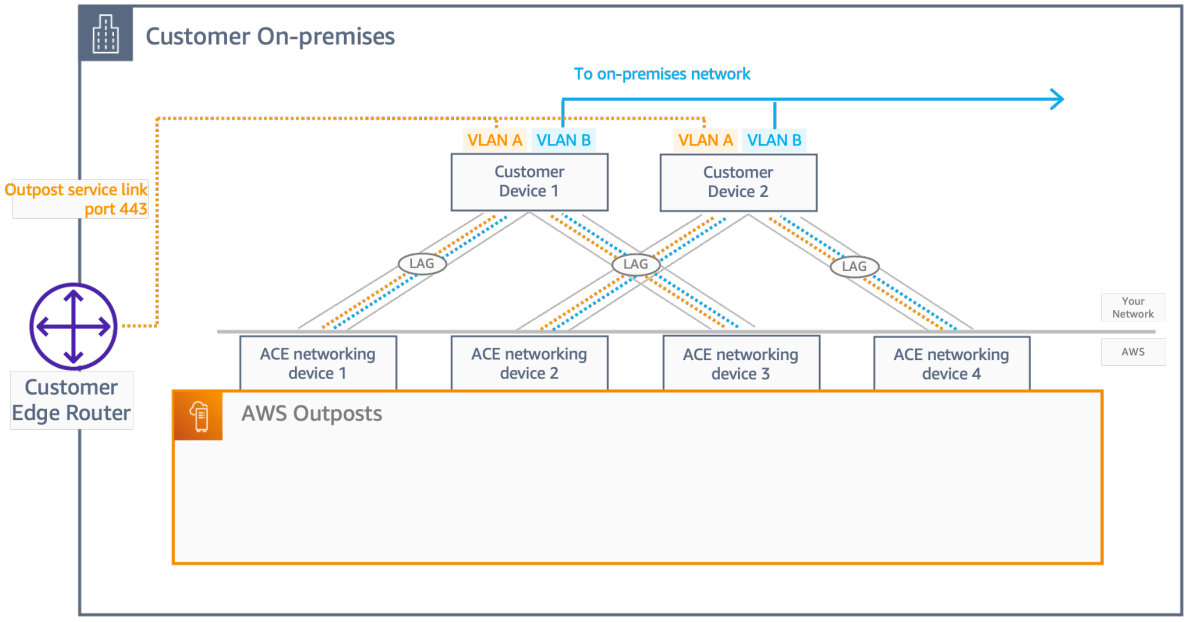
Ein Aggregation, Core, Edge (ACE) -Rack dient als Netzwerkaggregationspunkt für Outpost-Bereitstellungen mit mehreren Racks. Sie müssen ein ACE-Rack verwenden, wenn Sie über vier oder mehr Computer-Racks verfügen. Wenn Sie weniger als vier Computer-Racks haben, aber in future eine Erweiterung auf vier oder mehr Racks planen, empfehlen wir, dass Sie frühestens ein ACE-Rack installieren.

Mit einem ACE-Rack sind Outposts Outposts-Netzwerkgeräte nicht mehr direkt an Ihre lokalen Netzwerkgeräte angeschlossen. Stattdessen sind sie mit dem ACE-Rack verbunden, das die Konnektivität zu den Outposts-Racks ermöglicht. AWS Besitzt in dieser Topologie die VLAN-Schnittstellenzuweisung und -konfiguration zwischen Outposts-Netzwerkgeräten und den ACE-Netzwerkgeräten.

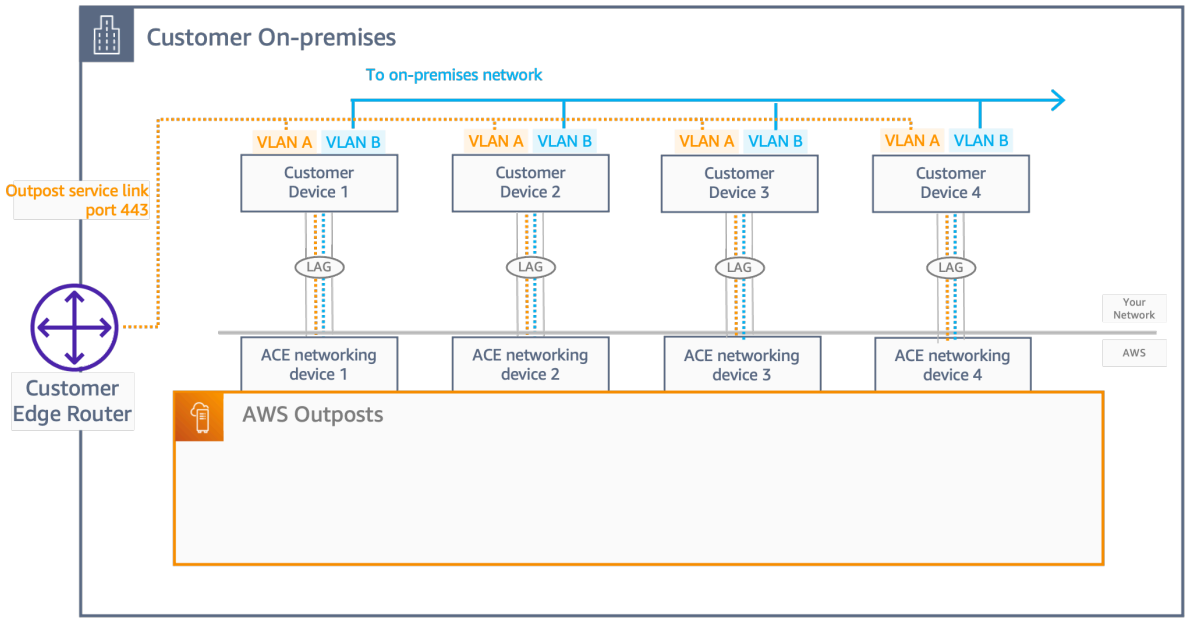
Ein ACE-Rack umfasst vier Netzwerkgeräte, die mit zwei vorgelagerten Kundengeräten in einem lokalen Kundennetzwerk oder mit vier vorgelagerten Kundengeräten verbunden werden können, um maximale Stabilität zu gewährleisten.

Die folgenden Bilder zeigen die beiden Netzwerktopologien.

Die folgende Abbildung zeigt die vier ACE-Netzwerkgeräte des ACE-Racks, die mit zwei vorgelagerten Kundengeräten verbunden sind:




Die folgende Abbildung zeigt die vier ACE-Netzwerkgeräte des ACE-Racks, die mit vier vorgelagerten Kundengeräten verbunden sind:



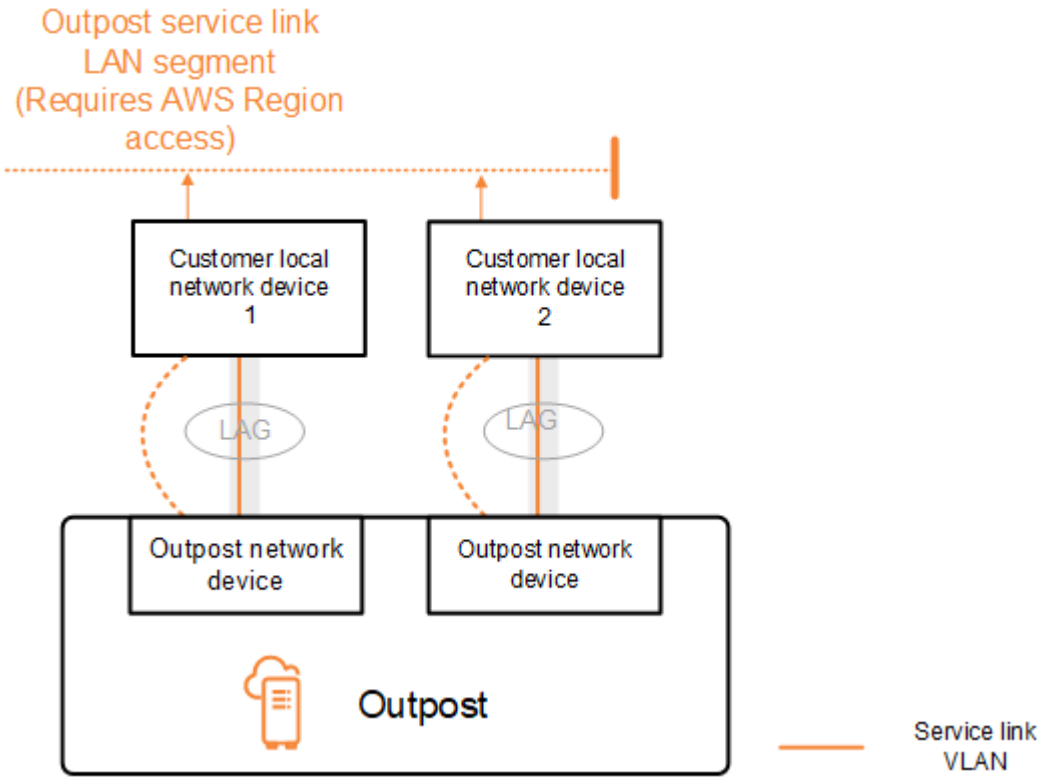

# Service Link BGP-Konnektivität

Der Outpost richtet eine externe BGP-Peering-Sitzung zwischen jedem Outpost-Netzwerkgerät und dem lokalen Netzwerkgerät des Kunden ein, um die Service Link-Konnektivität über das Service Link-VLAN herzustellen. Die BGP-Peering-Sitzung wird zwischen den für das VLAN bereitgestellten IP-Adressen /30 oder /31 eingerichtet. point-to-point Jede BGP-Peering-Sitzung verwendet eine private Autonome Systemnummer (ASN) auf dem Outpost-Netzwerkgerät und eine ASN, die Sie für die lokalen Netzwerkgeräte Ihrer Kunden auswählen. AWS Konfiguriert im Rahmen des Installationsvorgangs die von Ihnen angegebenen Attribute.

Stellen Sie sich das Szenario vor, in dem Sie einen Outpost mit zwei Outpost-Netzwerkgeräten haben, die über ein Service Link-VLAN mit zwei lokalen Netzwerkgeräten des Kunden verbunden sind. Sie konfigurieren die folgenden Infrastruktur- und BGP-ASN-Attribute für das lokale Netzwerkgerät des Kunden für jeden Service-Link:

- – Service Link BGP-Peer ASN. 2 Byte (16 Bit) oder 4 Byte (32 Bit). Die gültigen Werte sind 64512–65535 oder 4200000000–4294967294.
- Das Infrastruktur-CIDR. Dies muss ein /26 CIDR pro Rack sein.
- Die Service Link BGP-Peer-IP-Adresse für das lokale Netzwerkgerät 1 des Kunden.
- Die Service Link BGP-Peer-ASN für das lokale Netzwerkgerät 1 des Kunden. Die gültigen Werte lauten 1–4294967294.
- Die Service Link BGP-Peer-IP-Adresse für das lokale Netzwerkgerät 2 des Kunden.

- Die Service Link BGP-Peer-ASN für das lokale Netzwerkgerät 2 des Kunden. Die gültigen Werte lauten 1–4294967294. Weitere Informationen finden Sie unter RFC4893.




Der Outpost richtet mithilfe des folgenden Verfahrens eine externe BGP-Peering-Sitzung über das Service Link-VLAN ein:

1. Jedes Outpost-Netzwerkgerät verwendet die ASN, um eine BGP-Peering-Sitzung mit seinem verbundenen lokalen Netzwerkgerät einzurichten.
2. Outpost-Netzwerkgeräte geben den CIDR-Bereich /26 als zwei /27 CIDR-Bereiche an, um Verbindungs- und Geräteausfälle zu unterstützen. Jedes OND gibt sein eigenes /27-Präfix mit einer AS-Pfadlänge von 1 sowie die /27-Präfixe aller anderen ONDs mit einer AS-Pfadlänge von 4 als Backup bekannt.
3. Das Subnetz wird für die Konnektivität vom Outpost zur Region verwendet. AWS

Wir empfehlen Ihnen, die Kunden-Netzwerkgeräte so zu konfigurieren, dass sie BGP-Ankündigungen von Outposts empfangen, ohne die BGP-Attribute zu ändern. Das Kundennetzwerk sollte Routen von Outposts mit einer AS-Pfadlänge von 1 gegenüber Routen mit einer AS-Pfadlänge von 4 bevorzugen.

Das Kundennetzwerk sollte für alle gleiche BGP-Präfixe mit denselben Attributen werben. ONDs Das Outpost-Netzwerk verteilt standardmäßig ausgehenden Datenverkehr zwischen allen Uplinks. Routing-Richtlinien werden auf der Outpost-Seite verwendet, um den Datenverkehr von einem OND wegzuverlagern, falls Wartungsarbeiten erforderlich sind. Diese Verkehrsverlagerung erfordert für alle Kunden gleiche BGP-Präfixe. ONDs Wenn im Kundennetzwerk Wartungsarbeiten erforderlich sind, empfehlen wir Ihnen, AS-Path Prepending zu verwenden, um den Datenverkehr vorübergehend von bestimmten Uplinks zu verlagern.

## Service Link-Infrastruktur, Subnetz, Werbung und IP-Bereich

Während der Vorinstallation für das Subnetz der Service Link-Infrastruktur geben Sie den CIDR-Bereich /26 an. Die Outpost-Infrastruktur verwendet diesen Bereich, um über den Service Link Konnektivität mit der Region herzustellen. Das Service Link-Subnetz ist die Outpost-Quelle, die die Konnektivität initiiert.

Outpost-Netzwerkgeräte geben den CIDR-Bereich /26 als zwei /27 CIDR-Blöcke an, um Verbindungs- und Geräteausfälle zu unterstützen.

Sie müssen einen Service Link BGP ASN und ein Infrastruktursubnetz-CIDR (/26) für den Outpost bereitstellen. Geben Sie für jedes Outpost-Netzwerkgerät die BGP-Peering-IP-Adresse im VLAN des lokalen Netzwerkgeräts und die BGP-ASN des lokalen Netzwerkgeräts an.

Wenn Sie mehrere Racks bereitstellen, benötigen Sie ein /26-Subnetz pro Rack.

## BGP-Konnektivität für das lokale Gateway

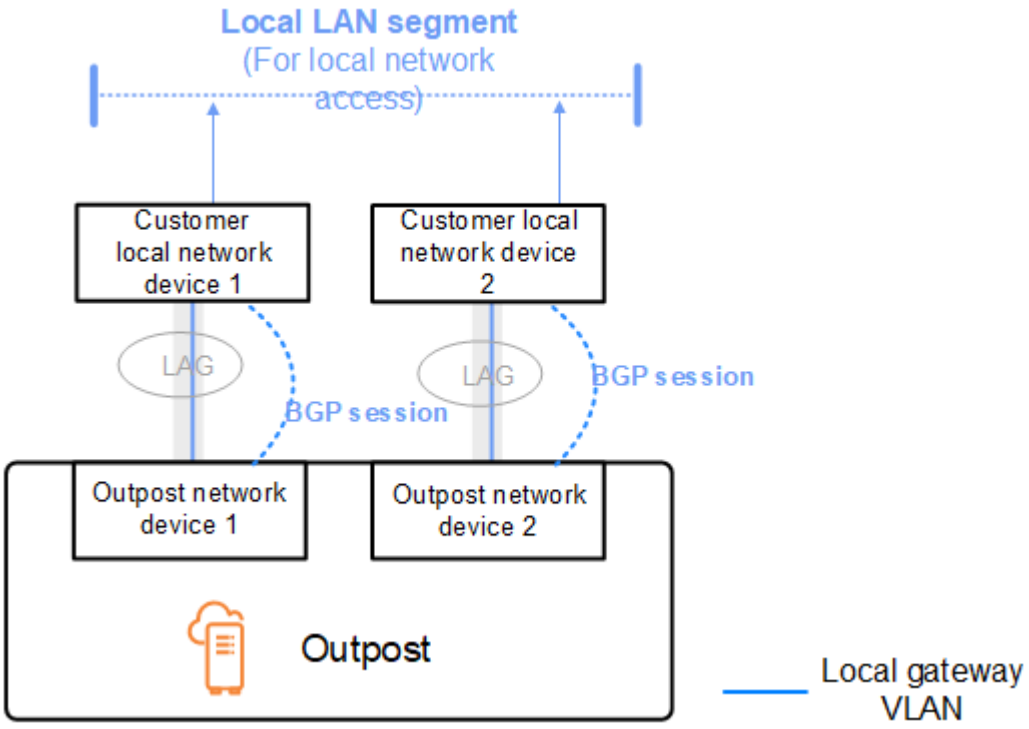
Der Outpost verwendet eine private Autonome Systemnummer (ASN), die Sie zuweisen, um die externen BGP-Sitzungen einzurichten. Jedes Outpost-Netzwerkgerät verfügt über ein einzelnes externes BGP-Peering zu einem lokalen Netzwerkgerät über sein lokales Gateway-VLAN.

Der Outpost richtet eine externe BGP-Peering-Sitzung über das lokale Gateway-VLAN zwischen jedem Outpost-Netzwerkgerät und dem angeschlossenen lokalen Netzwerkgerät des Kunden ein. Die Peering-Sitzung wird zwischen den /30 oder /31 eingerichtet IPs , die Sie bei der Einrichtung der Netzwerkkonnektivität angegeben haben, und verwendet die point-to-point Konnektivität zwischen den Outpost-Netzwerkgeräten und den lokalen Netzwerkgeräten des Kunden. Weitere Informationen finden Sie unter the section called “Netzwerk-Layer-Konnektivität”.

Jede BGP-Sitzung verwendet die private ASN auf der Seite des Outpost-Netzwerkgeräts und eine ASN, die Sie auf der Seite des lokalen Netzwerkgeräts des Kunden auswählen. AWS konfiguriert die Attribute im Rahmen des Vorinstallationsprozesses.

Stellen Sie sich das Szenario vor, in dem Sie einen Outpost mit zwei Outpost-Netzwerkgeräten haben, die über ein Service Link-VLAN mit zwei lokalen Netzwerkgeräten des Kunden verbunden sind. Sie konfigurieren die folgenden BGP ASN-Attribute für das lokale Gateway und das lokale Netzwerkgerät des Kunden für jeden Service-Link:

- Der Kunde stellt das lokale Gateway BGP ASN zur Verfügung. 2-Byte (16-Bit) oder 4-Byte (32-Bit). Die gültigen Werte sind 64512–65535 oder 4200000000–4294967294.
- (Optional) Sie stellen das kundeneigene CIDR zur Verfügung, für das geworben wird (öffentlich oder privat, mindestens /26).
- Sie stellen dem Kunden die lokale Gateway-BGP-Peer-IP-Adresse für das lokale Netzwerkgerät 1 zur Verfügung.
- Sie stellen dem Kunden das lokale Netzwerkgerät 1 (lokales Gateway, BGP-Peer-ASN) zur Verfügung. Die gültigen Werte lauten 1–4294967294. Weitere Informationen finden Sie unter RFC4893.
- Sie stellen dem Kunden die lokale Gateway-BGP-Peer-IP-Adresse für das lokale Netzwerkgerät 2 zur Verfügung.
- Sie stellen dem Kunden das lokale Netzwerkgerät 2 (lokales Gateway, BGP-Peer-ASN) zur Verfügung. Die gültigen Werte lauten 1–4294967294. Weitere Informationen finden Sie unter RFC4893.




Wir empfehlen Ihnen, die Kunden-Netzwerkgeräte so zu konfigurieren, dass sie BGP-Ankündigungen von Outposts empfangen, ohne die BGP-Attribute zu ändern, und BGP-Multipath/Load Balancing zu aktivieren, um optimale eingehende Datenströme zu erreichen. AS-Path-Präfixe werden für lokale Gateway-Präfixe verwendet, um den Datenverkehr zu verlagern, falls Wartungsarbeiten erforderlich sind. ONDs Das Kundennetzwerk sollte Routen von Outposts mit einer AS-Pfadlänge von 1 gegenüber Routen mit einer AS-Pfadlänge von 4 bevorzugen.

Das Kundennetzwerk sollte für alle gleiche BGP-Präfixe mit denselben Attributen werben. ONDs Das Outpost-Netzwerk verteilt standardmäßig ausgehenden Datenverkehr zwischen allen Uplinks. Routing-Richtlinien werden auf der Outpost-Seite verwendet, um den Datenverkehr von einem OND wegzuverlagern, falls Wartungsarbeiten erforderlich sind. Diese Verkehrsverlagerung erfordert für alle Kunden gleiche BGP-Präfixe. ONDs Wenn im Kundennetzwerk Wartungsarbeiten erforderlich sind, empfehlen wir Ihnen, AS-Path Prepending zu verwenden, um den Datenverkehr vorübergehend von bestimmten Uplinks zu verlagern.

## Kundeneigene IP-Subnetz-Werbung für das lokale Gateway

Standardmäßig verwendet das lokale Gateway die privaten IP-Adressen der Instances in Ihrer VPC (siehe Direktes VPC-Routing), um die Kommunikation mit Ihrem lokalen Netzwerk zu erleichtern.

Sie können jedoch einen kundeneigenen IP-Adresspool (Customer-owned IP Address, CoIP) bereitstellen.

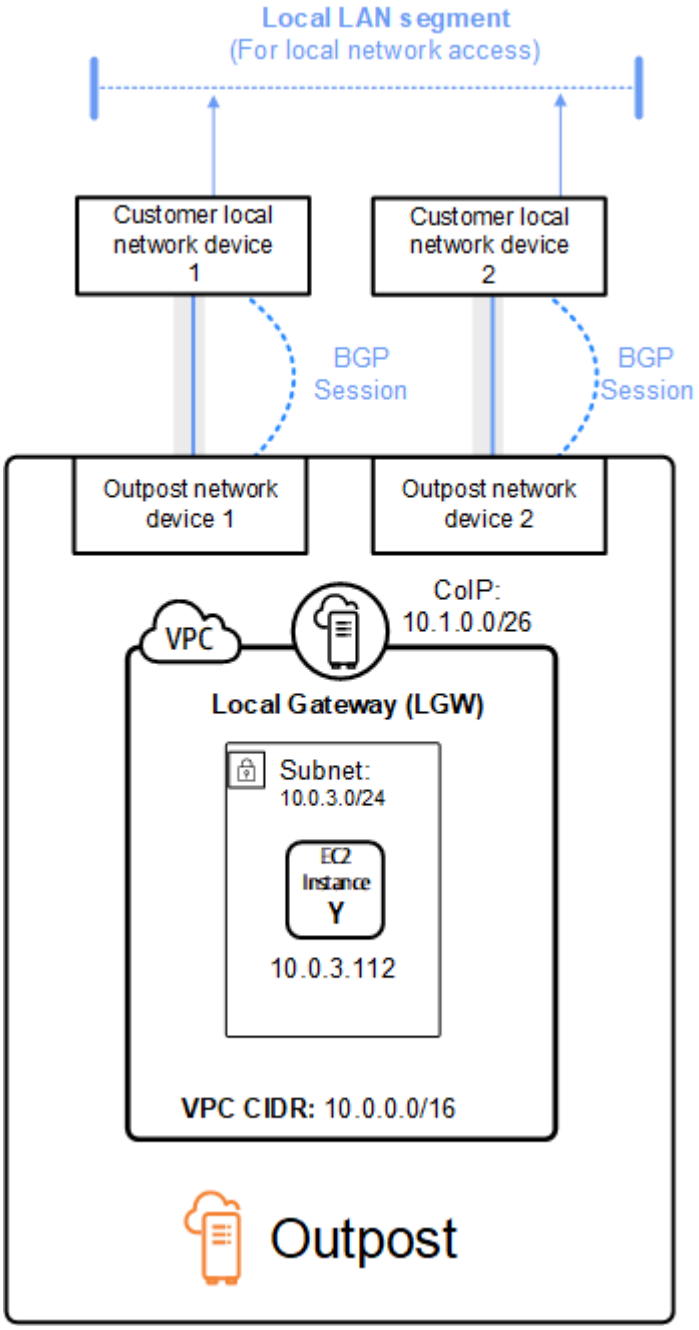
Sie können Elastic IP-Adressen aus diesem Pool erstellen und die Adressen dann Ressourcen in Ihrem Outpost zuweisen, z. B. Instances. EC2

Das lokale Gateway übersetzt die Elastic-IP-Adresse in eine Adresse aus dem kundeneigenen Pool. Das lokale Gateway gibt die übersetzte Adresse an Ihr On-Premises-Netzwerk und an jedes andere Netzwerk weiter, das mit dem Outpost kommuniziert. Die Adressen werden in beiden lokalen Gateway-BGP-Sitzungen an die lokalen Netzwerkgeräte weitergegeben.

> **Tip**
>
> Wenn Sie CoIP nicht verwenden, gibt BGP die privaten IP-Adressen aller Subnetze in Ihrem Outpost bekannt, die in der Routing-Tabelle eine Route haben, die auf das lokale Gateway abzielt.

Stellen Sie sich das Szenario vor, in dem Sie einen Outpost mit zwei Outpost-Netzwerkgeräten haben, die über ein Service Link-VLAN mit zwei lokalen Netzwerkgeräten des Kunden verbunden sind. Folgendes ist konfiguriert:

- Eine VPC mit einem CIDR-Block 10.0.0.0/16.
- Ein Subnetz in der VPC mit einem CIDR-Block 10.0.3.0/24.
- Eine EC2 Instance im Subnetz mit einer privaten IP-Adresse 10.0.3.112.
- Ein kundeneigener IP-Pool (10.1.0.0/26).
- Eine Elastic IP-Adresszuweisung, die 10.0.3.112 mit 10.1.0.2 verknüpft.
- Ein lokales Gateway, das BGP verwendet, um 10.1.0.0/26 über die On-Premises-Geräte im On-Premises-Netzwerk zu bewerben.
- Bei der Kommunikation zwischen Ihrem Outpost und dem lokalen Netzwerk wird CoIP Elastic verwendet, um Instances im Outpost IPs zu adressieren. Der VPC-CIDR-Bereich wird nicht verwendet.


Local LAN segment
(For local network access)
Customer local network device 1
Customer local network device 2
BGP Session
BGP Session
Outpost network device 1
Outpost network device 2
CoIP: 10.1.0.0/26
VPC
Local Gateway (LGW)
Subnet: 10.0.3.0/24
EC2 Instance Y
10.0.3.112
VPC CIDR: 10.0.0.0/16
Outpost

# Kapazitätsmanagement für AWS Outposts

Ein Outpost bietet einen Pool an AWS Rechen- und Speicherkapazität an Ihrem Standort als private Erweiterung einer Availability Zone in einer AWS Region. Da die in Outpost verfügbare Rechen- und Speicherkapazität begrenzt ist und von der Größe und Anzahl der Ressourcen bestimmt wird, die an Ihrem Standort AWS installiert sind, können Sie entscheiden, wie viel AWS Outposts Kapazität von Amazon EC2, Amazon EBS und Amazon S3 Sie benötigen, um Ihre anfänglichen Workloads auszuführen, future Wachstum zu bewältigen und zusätzliche Kapazität bereitzustellen, um Serverausfälle und Wartungsereignisse zu minimieren.

Themen



## Kapazität anzeigen AWS Outposts

Sie können die Kapazitätskonfiguration auf Instance- oder Outpost-Ebene einsehen.

Um die Kapazitätskonfiguration für Ihren Outpost mithilfe der Konsole anzuzeigen

1. Öffnen Sie die AWS Outposts Konsole unter. https://console.aws.amazon.com/outposts/
2. Wählen Sie im linken Navigationsbereich Outposts aus.
3. Wählen Sie den Außenposten.
4. Wählen Sie auf der Seite mit den Outpost-Details entweder die Instance-Ansicht oder die Rack-Ansicht aus.

    - Instanzansicht — Bietet Informationen zu den auf den Outposts konfigurierten Instanzen und zur Verteilung der Instanzen nach Größe und Familie.
    - Rack-Ansicht — Bietet eine Visualisierung der Instanzen auf jedem Asset innerhalb jedes Outposts und ermöglicht es Ihnen, Instance-Kapazität ändern auszuwählen, um Änderungen an der Instance-Kapazität vorzunehmen.

# AWS Outposts Instanzkapazität ändern

Die Kapazität jeder neuen Outpost-Bestellung wird mit einer Standardkapazitätskonfiguration konfiguriert. Sie können die Standardkonfiguration konvertieren, um verschiedene Instanzen zu erstellen, die Ihren Geschäftsanforderungen entsprechen. Dazu erstellen Sie eine Kapazitätsaufgabe, wählen einen Outpost oder ein einzelnes Asset aus, geben die Instanzgrößen und die Menge an und führen die Kapazitätsaufgabe aus, um die Änderungen zu implementieren.

## Überlegungen

Beachten Sie Folgendes, bevor Sie die Instance-Kapazität ändern:

- Kapazitätsaufgaben können nur von dem AWS Konto ausgeführt werden, dem die Outpost-Ressourcen gehören (Besitzer). Verbraucher können Kapazitätsaufgaben nicht ausführen. Weitere Informationen zu Eigentümern und Verbrauchern finden Sie unter AWS Outposts Ressourcen teilen.
- Größen und Mengen von Instanzen können auf Outpost-Ebene oder auf Ebene einzelner Assets definiert werden.
- Die Kapazität wird automatisch für ein Asset oder alle Assets in einem Outpost konfiguriert, basierend auf möglichen Konfigurationen und bewährten Methoden.
- Während eine Kapazitätsaufgabe ausgeführt wird, können die mit dem ausgewählten Außenposten verknüpften Ressourcen isoliert werden. Aus diesem Grund empfehlen wir, eine Kapazitätsaufgabe nur dann zu erstellen, wenn Sie nicht damit rechnen, neue Instances in Ihren Outposts zu starten.
- Sie können wählen, ob Sie die Kapazitätsaufgabe sofort ausführen möchten oder ob Sie es in den nächsten 48 Stunden regelmäßig versuchen möchten. Wenn Sie sich für die sofortige Ausführung entscheiden, ist weniger Zeit für die Isolierung der Ressourcen erforderlich. Die Aufgabe kann jedoch fehlschlagen, wenn Instances gestoppt werden müssen, um die Aufgabe auszuführen. Wenn Sie sich für die regelmäßige Ausführung entscheiden, haben Sie mehr Zeit, um Instances zu stoppen, bevor die Aufgabe fehlschlägt. Die Ressourcen können jedoch länger isoliert sein.
- Es ist möglich, dass gültige Kapazitätskonfigurationen nicht alle verfügbaren vCPUs auf einem Asset nutzen. In diesem Fall werden Sie in einer Meldung am Ende des Abschnitts Instanztyp darüber informiert, dass Ihre Kapazität nicht mehr ausreicht. Die Konfiguration kann jedoch wie gewünscht angewendet werden.
- Wenn Sie einen Outpost in der Konsole ändern, werden nicht alle unterstützten Instances angezeigt, da das Mischen von festplattengestützten Instances mit non-disk-backed Instances

in der Konsole nicht vollständig unterstützt wird. Verwenden Sie die API, um auf alle möglichen Instanzen zuzugreifen. StartCapacityTask

- Bei der Definition der Kapazität für einen Outpost werden alle Instance-Familien und -typen in die Neukonfiguration einbezogen, sofern sie nicht als zu vermeidende Instanzen aufgeführt sind.
- Sie können Ihre bestehende Outposts-Kapazitätskonfiguration nur ändern, um gültige EC2 Amazon-Instance-Größen aus Instance-Familien zu verwenden, die in Ihrem jeweiligen Asset-Modell unterstützt werden.
- Wenn auf Ihrem Outpost Instances laufen, die Sie nicht beenden möchten, um eine Kapazitätsaufgabe auszuführen, wählen Sie die entsprechende Instance-ID im Abschnitt Instances aus, die unverändert bleiben sollen — optional — und stellen Sie sicher, dass Sie die erforderliche Menge dieser Instance-Größe in Ihrer aktualisierten Kapazitätskonfiguration beibehalten. Dadurch bleiben Instances erhalten, die zur Unterstützung von Produktionsworkloads verwendet werden, während eine Kapazitätsaufgabe ausgeführt wird.
- Wenn Sie ein Asset mit mehreren Instance-Größen innerhalb einer Instance-Familie konfigurieren, stellen Sie mithilfe von Auto-Balance sicher, dass Sie nicht versuchen, Ihr Droplet zu hoch oder zu wenig bereitzustellen. Eine Überprovisionierung wird nicht unterstützt und führt zu einem Ausfall der Kapazitätsaufgabe.
- Wenn Sie eine Instance-Familie auf Ihrem Outpost komplett neu konfigurieren möchten, ohne die Instance-Größen der ursprünglichen Kapazitätskonfiguration beizubehalten, müssen Sie alle laufenden Instances dieser Familie auf Ihrem Outpost beenden, bevor Sie die Kapazitätsaufgabe ausführen. Wenn die Instanz einem anderen Konto gehört oder von einem mehrschichtigen Dienst verwendet wird, der auf dem Outpost läuft, müssen Sie das Konto des Instanzbesitzers verwenden, um die Instanz oder Dienstinstanz zu beenden.
- Mehrere Kapazitätsaufgaben können parallel ausgeführt werden, sofern sie sich auf sich gegenseitig ausschließende Asset-Sets beziehenIDs. Sie können beispielsweise mehrere Kapazitätsaufgaben auf Anlagenebene für verschiedene Anlagen IDs gleichzeitig erstellen. Wenn jedoch eine Aufgabe auf Outpost-Ebene ausgeführt wird, können Sie nicht gleichzeitig eine weitere Aufgabe auf Outpost- oder Anlagenebene erstellen. Ebenso können Sie bei einer laufenden Aufgabe auf Anlagenebene nicht gleichzeitig eine Aufgabe auf Outpost-Ebene oder eine Aufgabe auf Anlagenebene für dieselbe AssetID erstellen.

So ändern Sie die Kapazitätskonfiguration für Ihren Outpost mithilfe der Konsole

1. Öffnen Sie die AWS Outposts Konsole unter. https://console.aws.amazon.com/outposts/
2. Wählen Sie im linken Navigationsbereich Capacity-Aufgaben aus.

3. Wählen Sie auf der Seite Kapazitätsaufgaben die Option Kapazitätsaufgabe erstellen aus.
4. Wählen Sie auf der Seite Erste Schritte die Bestellung, den Outpost oder das Asset aus, die konfiguriert werden sollen.
5. Um die Kapazität zu ändern, geben Sie eine Option für Methode der Änderung: e Schritte in der Konsole an oder laden Sie eine JSON-Datei hoch.

   - Ändern Sie den Kapazitätskonfigurationsplan, um die Schritte in der Konsole zu verwenden
   - Laden Sie einen Kapazitätskonfigurationsplan hoch, um eine JSON-Datei hochzuladen

> **Note**
>
> - Um zu verhindern, dass das Kapazitätsmanagement bestimmte Instanzen zum Stoppen empfiehlt, geben Sie die Instanzen an, die nicht gestoppt werden sollen. Diese Instanzen werden aus der Liste der zu stoppenden Instanzen ausgeschlossen.

Console steps

1. Wählen Sie Instance-Ansicht oder Rack-Ansicht.
2. Wählen Sie „Outpost-Kapazitätskonfiguration ändern“ oder „Ändern“ für ein einzelnes Asset aus.
3. Wählen Sie einen Außenposten oder ein Asset aus, falls es sich von der aktuellen Auswahl unterscheidet.
4. Wählen Sie, ob Sie diese Kapazitätsaufgabe entweder sofort oder in regelmäßigen Abständen über 48 Stunden ausführen möchten.
5. Wählen Sie Weiter aus.
6. Auf der Seite Instance-Kapazität konfigurieren wird für jeden Instance-Typ eine Instance-Größe angezeigt, wobei die maximale Anzahl vorausgewählt ist. Um weitere Instance-Größen hinzuzufügen, wählen Sie Instance-Größe hinzufügen.
7. Geben Sie die Anzahl der Instances an und notieren Sie sich die Kapazität, die für diese Instance-Größe angezeigt wird.
8. Sehen Sie sich die Meldung am Ende jedes Abschnitts mit dem Instanztyp an, in der Sie darüber informiert werden, ob Ihre Kapazität zu hoch oder zu niedrig ist. Nehmen Sie

Anpassungen auf der Ebene der Instance-Größe oder Menge vor, um Ihre verfügbare Gesamtkapazität zu optimieren.

9. Sie können auch beantragen AWS Outposts , die Instance-Menge für eine bestimmte Instance-Größe zu optimieren. Gehen Sie hierzu wie folgt vor:

   a. Wählen Sie die Instanzgröße.

   b. Wählen Sie am Ende des entsprechenden Abschnitts mit dem Instanztyp die Option Automatisches Ausgleichen aus.

10. Stellen Sie für jeden Instance-Typ sicher, dass die Instance-Menge für mindestens eine Instance-Größe angegeben ist.
11. Wählen Sie optional Instances aus, die unverändert beibehalten werden sollen.
12. Wählen Sie Weiter aus.
13. Überprüfen Sie auf der Seite Überprüfen und erstellen, welche Updates Sie anfordern.
14. Wählen Sie „Erstellen“. AWS Outposts erstellt eine Kapazitätsaufgabe.
15. Überwachen Sie auf der Seite mit den Kapazitätsaufgaben den Status der Aufgabe.

Upload a JSON file

1. Wählen Sie Kapazitätskonfiguration hochladen aus.
2. Wählen Sie Weiter aus.
3. Laden Sie auf der Seite Kapazitätskonfigurationsplan hochladen die JSON-Datei hoch, die den Instanztyp, die Größe und die Menge angibt. Optional können Sie die InstancesToExcludeTaskActionOnBlockingInstancesParameter und in der JSON-Datei angeben.

   Example

   Beispiel für eine JSON-Datei:

```
{
  "InstancePools": [
    {
      "InstanceType": "c5.24xlarge",
      "Count": 1
    },
    {
      "InstanceType": "m5.24xlarge",
```

```
      "Count": 2
    }
  ],
  "InstancesToExclude": {
    "AccountIds": [
      "111122223333"
    ],
    "Instances": [
      "i-1234567890abcdef0"
    ],
    "Services": [
      "ALB"
    ]
  },
  "TaskActionOnBlockingInstances": "WAIT_FOR_EVACUATION"
}
```

4. Überprüfen Sie den Inhalt der JSON-Datei im Abschnitt Kapazitätskonfigurationsplan.
5. Wählen Sie Weiter aus.
6. Überprüfen Sie auf der Seite Überprüfen und erstellen, welche Aktualisierungen Sie anfordern.
7. Wählen Sie „Erstellen“. AWS Outposts erstellt eine Kapazitätsaufgabe.
8. Überwachen Sie auf der Seite mit den Kapazitätsaufgaben den Status der Aufgabe.

# Behebung von Problemen mit Kapazitätsaufgaben

Sehen Sie sich die folgenden bekannten Probleme an, um ein Problem im Zusammenhang mit der Kapazitätsverwaltung in einer neuen Reihenfolge zu lösen. Wenn Ihr Problem nicht aufgeführt ist, wenden Sie sich an Support.

## *oo-xxxxxx*Die Bestellung ist nicht mit der Outpost ID verknüpft *op-xxxxx*

Dieses Problem tritt auf, wenn Sie die AWS CLI oder API zum Ausführen verwenden `StartCapacityTask`und die Outpost-ID in der Anfrage nicht mit der Outpost-ID in der Bestellung übereinstimmt.

So beheben Sie dieses Problem

1. Melden Sie sich an bei. AWS

2. Öffnen Sie die AWS Outposts Konsole unter https://console.aws.amazon.com/outposts/.
3. Wählen Sie im Navigationsbereich Bestellungen aus.
4. Wählen Sie die Bestellung aus und vergewissern Sie sich, dass der Bestellstatus einer der folgenden ist: `PREPARINGIN_PROGRESS`,, oder`ACTIVE`.
5. Notieren Sie sich die Outpost-ID in der Bestellung.
6. Geben Sie die richtige Outpost-ID in die `StartCapacityTask` API-Anfrage ein.

## Der Kapazitätsplan umfasst Instance-Typen, die nicht unterstützt werden

Dieses Problem tritt auf, wenn Sie die API AWS CLI oder verwenden, um die Kapazitätsaufgabe zu erstellen oder zu ändern und die Anfrage Instance-Typen enthält, die nicht unterstützt werden.

Verwenden Sie die Konsole oder CLI, um dieses Problem zu beheben.

Verwenden der Konsole

1. Melden Sie sich an bei AWS.
2. Öffnen Sie die AWS Outposts Konsole unter https://console.aws.amazon.com/outposts/.
3. Wählen Sie im Navigationsbereich die Option Capacity Task aus.
4. Verwenden Sie die Option Kapazitätskonfiguration hochladen, um eine JSON-Datei mit derselben Liste von Instance-Typen hochzuladen.
5. Die Konsole zeigt eine Fehlermeldung mit der Liste der unterstützten Instanztypen an.
6. Korrigieren Sie die Anforderung, die nicht unterstützten Instance-Typen zu entfernen.
7. Erstellen oder ändern Sie die Kapazitätsaufgabe auf der Konsole mit dem korrigierten JSON oder verwenden Sie die CLI oder API mit dieser korrigierten Liste von Instance-Typen.

Verwendung des -CLI

1. Verwenden Sie den GetOutpostSupportedInstanceTypesBefehl, um die Liste der unterstützten Instanztypen anzuzeigen.
2. Erstellen oder ändern Sie die Kapazitätsaufgabe mit der richtigen Liste der Instance-Typen.

## Kein Außenposten mit Außenpost-ID *op-xxxxx*

Dieses Problem tritt auf, wenn Sie die AWS CLI oder -API zum Ausführen verwenden `StartCapacityTask`und die Anfrage eine Outpost-ID enthält, die aus einem der folgenden Gründe nicht gültig ist:

- Der Außenposten befindet sich in einer anderen AWS Region.
- Sie haben keine Berechtigungen für diesen Außenposten.
- Die Outpost-ID ist falsch.

So beheben Sie dieses Problem

1. Notieren Sie sich die AWS Region, die Sie in der `StartCapacityTask` API-Anfrage verwendet haben.
2. Verwenden Sie die `ListOutposts`API-Aktion, um eine Liste der Outposts abzurufen, die Sie in der AWS Region besitzen.
3. Prüfen Sie, ob die Outpost-ID aufgeführt ist.
4. Geben Sie die richtige Outpost-ID in die `StartCapacityTask` Anfrage ein.
5. Wenn Sie die Outpost-ID nicht finden, überprüfen Sie mithilfe der `ListOutposts` API-Aktion erneut, ob der Outpost in einer anderen Region existiert. AWS

## Aktiver CapacityTask Grenzwert — für Outpost op- wurde *XXXX* bereits gefunden *XXXX*

Dieses Problem tritt auf, wenn Sie die AWS Outposts Konsole oder API für die Ausführung StartCapacityTaskauf einem Outpost verwenden und es bereits eine Kapazitätsaufgabe für den Outpost gibt. Eine Kapazitätsaufgabe gilt als ausgeführt, wenn sie einen der folgenden Status hat:`REQUESTED`,`IN_PROGRESS`, `WAITING_FOR_EVACUATION` oder. `CANCELLATION_IN_PROGRESS`

Verwenden Sie die AWS Outposts Konsole oder CLI, um dieses Problem zu beheben.

Verwenden der Konsole

1. Melden Sie sich an bei AWS.
2. Öffnen Sie die AWS Outposts Konsole unter https://console.aws.amazon.com/outposts/.

3. Wählen Sie im Navigationsbereich Capacity-Aufgaben aus.
4. Stellen Sie sicher, dass es keine laufenden Kapazitätsaufgaben für die gibt OutpostId.
5. Wenn es Aufgaben mit laufender Kapazität für die gibt OutpostId, warten Sie, bis sie beendet sind, oder brechen Sie sie auf Wunsch ab.
6. Wenn es keine laufenden Kapazitätsaufgaben für die angeforderte Datei gibt OutpostId, wiederholen Sie Ihre Anfrage, um die Kapazitätsaufgabe zu erstellen.

Verwendung des -CLI

1. Verwenden Sie den ListCapacityTasksBefehl, um nach laufenden Kapazitätsaufgaben für den Outpost zu suchen.
2. Warten Sie, bis alle laufenden Kapazitätsaufgaben beendet sind, oder brechen Sie sie auf Wunsch ab.
3. Wenn für die angeforderte Datei keine Aufgaben mit laufender Kapazität verfügbar sind OutpostId, versuchen Sie erneut, die Kapazitätsaufgabe zu erstellen.

## Aktives CapacityTask Limit — wurde für das Asset *XXXX* auf Outpost OP-xxxx *XXXX* bereits gefunden

Dieses Problem tritt auf, wenn Sie die AWS Outposts Konsole oder API für die Ausführung StartCapacityTaskeines Assets verwenden und für das Asset bereits eine Kapazitätsaufgabe läuft. Eine Kapazitätsaufgabe gilt als ausgeführt, wenn sie einen der folgenden Status hat:`REQUESTED`, `IN_PROGRESSWAITING_FOR_EVACUATION`, oder`CANCELLATION_IN_PROGRESS`.

Verwenden Sie die AWS Outposts Konsole oder CLI, um dieses Problem zu beheben.

Verwenden der Konsole

1. Melden Sie sich an bei AWS.
2. Öffnen Sie die AWS Outposts Konsole unter https://console.aws.amazon.com/outposts/.
3. Wählen Sie im Navigationsbereich Capacity-Aufgaben aus.
4. Stellen Sie sicher, dass keine laufenden Kapazitätsaufgaben für die OutpostId und keine laufenden Kapazitätsaufgaben auf Anlagenebene für die vorhanden sind. AssetId
5. Wenn es laufende Kapazitätsaufgaben gibt, warten Sie, bis sie beendet sind, oder brechen Sie sie auf Wunsch ab.

6. Wenn es keine laufenden Kapazitätsaufgaben gibt, wiederholen Sie Ihre Anfrage, um die Kapazitätsaufgabe zu erstellen.

Verwendung des -CLI

1. Verwenden Sie den ListCapacityTasksBefehl, um nach laufenden Kapazitätsaufgaben für OutpostID und AssetID zu suchen.
2. Stellen Sie sicher, dass keine Kapazitätsaufgaben auf OutPost-Ebene für die und keine laufenden Kapazitätsaufgaben auf OutpostId Anlagenebene für die ausgeführt werden. AssetId
3. Wenn Kapazitätsaufgaben ausgeführt werden, warten Sie, bis sie beendet sind, oder brechen Sie sie auf Wunsch ab.
4. Versuchen Sie erneut, die Kapazitätsaufgabe zu erstellen.

## AssetId= *XXXX* ist nicht gültig für Outpost=OP- *XXXX*

Dieses Problem tritt auf, wenn Sie die AWS Outposts Konsole oder API für die Ausführung StartCapacityTaskauf einem Asset verwenden und die AssetID aus einem der folgenden Gründe nicht gültig ist:

- Das Asset ist nicht mit dem Outpost verknüpft.
- Das Asset ist isoliert.

Verwenden Sie die AWS Outposts Konsole oder CLI, um dieses Problem zu beheben.

Verwenden der Konsole

1. Melden Sie sich an bei AWS.
2. Öffnen Sie die AWS Outposts Konsole unter https://console.aws.amazon.com/outposts/.
3. Wählen Sie die Rack-Ansicht für den Outpost.
4. Stellen Sie sicher, dass der angeforderte Server dem Außenposten zugeordnet AssetId ist und dass er nicht als isolierter Host gekennzeichnet ist.

    a. Wenn das Asset isoliert ist, kann das daran liegen, dass auf ihm eine Kapazitätsaufgabe ausgeführt wird. Sie können zum Bereich „Kapazitätsaufgaben“ navigieren und überprüfen, ob Outpost- oder Asset-Aufgaben für und ausgeführt werden. OutpostId AssetId Wenn ja, warten Sie, bis die Aufgabe beendet ist und das Asset wieder verfügbar ist.

   b. Wenn es für eine isolierte Anlage keine Aufgaben zur laufenden Kapazität gibt, ist die Anlage möglicherweise beeinträchtigt.

5. Nachdem Sie sich vergewissert haben, dass das Asset vorhanden ist und sich in einem gültigen Zustand befindet, wiederholen Sie Ihre Anfrage, um die Kapazitätsaufgabe zu erstellen.

Verwendung des -CLI

1. Verwenden Sie den ListAssetsBefehl, um die mit der OutpostID verknüpften Assets zu suchen.
2. Vergewissern Sie sich, dass die angeforderte Datei dem Außenposten zugeordnet AssetId ist und ob es sich um einen Bundesstaat handelt. `ACTIVE`

   a. Wenn der Asset-Status nicht AKTIV ist, kann das daran liegen, dass für ihn ein Kapazitäts-Task ausgeführt wird. Verwenden Sie den ListCapacityTasksBefehl, um zu ermitteln, ob Outpost- oder Aufgaben auf Anlagenebene für und ausgeführt werden. OutpostId AssetId Wenn ja, warten Sie, bis die Aufgabe beendet ist und das Asset wieder AKTIV wird.

   b. Wenn es für eine isolierte Anlage keine Aufgaben zur laufenden Kapazität gibt, ist die Anlage möglicherweise beeinträchtigt.

3. Nachdem Sie sich vergewissert haben, dass das Asset vorhanden ist und sich in einem gültigen Zustand befindet, wiederholen Sie Ihre Anfrage, um die Kapazitätsaufgabe zu erstellen.

# Teilen Sie Ihre AWS Outposts Ressourcen

Mit Outpost Sharing können Outpost-Besitzer ihre Outposts und Outpost-Ressourcen, einschließlich Outpost-Sites und Subnetze, mit anderen AWS Konten derselben Organisation teilen. AWS Als Outpost-Besitzer können Sie Outpost-Ressourcen zentral erstellen und verwalten und die Ressourcen für mehrere Konten innerhalb Ihrer Organisation gemeinsam nutzen. AWS AWS Auf diese Weise können andere Verbraucher Outpost-Sites nutzen, Instanzen auf dem gemeinsam genutzten Outpost konfigurieren VPCs, starten und ausführen.

In diesem Modell teilt sich das AWS Konto, dem die Outpost-Ressourcen gehören (Eigentümer), die Ressourcen mit anderen AWS Konten (Verbrauchern) in derselben Organisation. Konsumenten können beim Erstellen von Ressourcen in Outposts so vorgehen, wie sie dies beim Erstellen von Ressourcen auf Outposts tun würden, die sie in ihrem eigenen Konto erstellen. Der Besitzer ist für die Verwaltung des Outposts und der Ressourcen, die von ihm darin erstellt werden, verantwortlich. Besitzer können die Freigabe jederzeit ändern oder widerrufen. Mit Ausnahme von Instances, die Kapazitätsreservierungen in Anspruch nehmen, können Besitzer auch Ressourcen anzeigen, ändern und löschen, die Konsumenten in freigegebenen Outposts erstellen. Besitzer können Instances, die Verbraucher in Capacity Reservations starten, nicht ändern, die sie gemeinsam genutzt haben.

Konsumenten sind verantwortlich für die Verwaltung der Ressourcen, die sie in Outposts erstellen, die für sie freigegebenen sind, einschließlich aller Ressourcen, die Kapazitätsreservierungen in Anspruch nehmen, verantwortlich. Konsumenten können Ressourcen, die anderen Konsumenten oder dem Eigentümer des Outposts gehören, nicht einsehen oder verändern. Sie können auch keine Outposts verändern, die für sie freigegeben sind.

Ein Outpost-Eigentümer kann Outpost-Ressourcen teilen mit:

- Spezifische AWS Konten innerhalb der Organisation in AWS Organizations.
- Eine Organisationseinheit innerhalb seiner Organisation in AWS Organizations.
- Seine gesamte Organisation in AWS Organizations.

Inhalt

# Freigabefähige Outpost-Ressourcen

Ein Outpost-Eigentümer kann die in diesem Abschnitt aufgeführten Outpost-Ressourcen für Konsumenten freigeben.

Dies sind die Ressourcen, die für  verfügbar sind.

- Zugewiesene Dedicated Hosts – Konsumenten mit Zugriff auf diese Ressource können:
  - Starten und führen Sie EC2 Instances auf einem Dedicated Host aus.
- Kapazitätsreservierungen – Konsumenten mit Zugriff auf diese Ressource können:
  - Identifizieren Sie Kapazitätsreservierungen, die für sie freigegeben wurden.
  - Starten und verwalten Sie Instances, die Kapazitätsreservierungen verbrauchen.
- Kundeneigene IP-Adresspools (Customer-owned, CoIP) – Konsumenten mit Zugriff auf diese Ressource können:
  - Zuweisen und Zuordnen von kundeneigenen IP-Adressen mit Instances.
- Routing-Tabellen für lokale Gateways – Konsumenten mit Zugriff auf diese Ressource können:
  - Erstellen und verwalten von VPC-Zuordnungen zu einem lokalen Gateway.
  - Sehen Sie sich die Konfigurationen der lokalen Gateway-Routing-Tabelle und virtuellen Schnittstellen an.
- Outposts – Konsumenten mit Zugang zu dieser Ressource können:
  - Erstellen und verwalten von Subnetzen auf dem Outpost.
  - EBS-Volumes auf dem Outpost erstellen und verwalten.
  - Verwenden Sie die AWS Outposts API, um Informationen über den Outpost einzusehen.
- S3 auf Outposts – Konsumenten mit Zugriff auf diese Ressource können:

  - S3-Buckets, Zugangspunkte und Endpunkte auf dem Outpost erstellen und verwalten.
- Standorte – Verbraucher mit Zugriff auf diese Ressource können:
  - Einen Outpost am Standort einrichten, verwalten und steuern.
- Subnetze – Konsumenten mit Zugriff auf diese Ressource können:
  - Anzeigen von Informationen über Subnetze.
  - Starten und führen Sie EC2 Instances in Subnetzen aus.

  Verwenden der Amazon VPC-Konsole, um ein Outpost-Subnetz freizugeben. Weitere Informationen finden Sie unter Gemeinsame Nutzung eines Subnetzes im Amazon VPC-Benutzerhandbuch.

## Voraussetzungen für die Freigabe von Outposts-Ressourcen

- Um eine Outpost-Ressource für Ihre Organisation oder eine Organisationseinheit in AWS Organizations freizugeben, müssen Sie die Freigabe für AWS Organizations aktivieren. Weitere Informationen finden Sie unter Freigabe für AWS Organizations aktivieren im AWS RAM - Benutzerhandbuch.
- Um eine Outpost-Ressource gemeinsam zu nutzen, müssen Sie sie in Ihrem AWS Konto besitzen. Sie können eine Outpost-Ressource, die mit Ihnen geteilt wurde, nicht teilen.
- Um eine Outpost-Ressource freizugeben, müssen Sie sie für ein Konto freigeben, das sich in Ihrer Organisation befindet.

## Zugehörige Services

Die gemeinsame Nutzung von Outpost-Ressourcen ist in AWS Resource Access Manager ()AWS RAM integriert. AWS RAM ist ein Dienst, mit dem Sie Ihre AWS Ressourcen mit einem beliebigen AWS Konto oder über AWS Organizations dieses teilen können. Mit AWS RAM geben Sie Ressourcen in Ihrem Besitz frei, indem Sie eine Ressourcenfreigabe erstellen. Eine Ressourcenfreigabe legt die freizugebenden Ressourcen und die Konsumenten fest, für die sie freigegeben werden sollen. Bei Verbrauchern kann es sich um einzelne AWS Konten, Organisationseinheiten oder eine gesamte Organisation handeln AWS Organizations.

Weitere Informationen zu AWS RAM finden Sie im AWS RAM Benutzerhandbuch.

# Freigeben in mehreren Availability Zones

Um sicherzustellen, dass Ressourcen auf die Availability Zones einer Region verteilt sind, ordnen wir Availability Zones einzeln Namen für jedes Konto zu. Dies könnte zu in mehreren Konten unterschiedlich benannten Availability Zones führen. Beispielsweise hat die Availability Zone `us-east-1a` für Ihr AWS Konto möglicherweise nicht denselben Standort wie `us-east-1a` für ein anderes AWS Konto.

Um den Standort Ihrer Outpost-Ressource im Verhältnis zu Ihren Konten zu identifizieren, müssen Sie die Availability Zone-ID (AZ-ID) verwenden. Die AZ-ID ist eine eindeutige und konsistente Kennung für eine Availability Zone für alle AWS Konten. Dies `use1-az1` ist beispielsweise eine AZ-ID für die `us-east-1` Region und es handelt sich in jedem AWS Konto um denselben Standort.

Um die IDs Availability Zones in Ihrem Konto einzusehen

1. Navigieren Sie in der AWS RAM Konsole zur AWS RAM Konsole.
2. Die AZ IDs für die aktuelle Region werden im Bereich „Ihre AZ-ID“ auf der rechten Seite des Bildschirms angezeigt.

> **Note**
>
> Lokale Gateway-Routing-Tabelle befinden sich in derselben AZ wie ihr Outpost, sodass Sie keine AZ-ID für Routing-Tabellen angeben müssen.

# Eine Outpost-Ressource freigeben

Wenn ein Eigentümer einen Outpost für einen Konsumenten freigibt, kann der Konsument auf dem Outpost Ressourcen auf dieselbe Weise erstellen wie auf Outposts, die er in seinem eigenen Konto erstellt. Konsument mit Zugriff auf freigegebene lokale Gateway-Routing-Tabelle können VPC-Zuordnungen erstellen und verwalten. Weitere Informationen finden Sie unter Freigabefähige Outpost-Ressourcen.

Um eine Outpost-Ressource freizugeben, müssen Sie sie zu einer Ressourcenfreigabe hinzufügen. Eine Ressourcenfreigabe ist eine AWS RAM Ressource, mit der Sie Ihre Ressourcen für mehrere AWS Konten gemeinsam nutzen können. Eine Ressourcenfreigabe gibt die freizugebenden Ressourcen und die Konsumenten an, für die sie freigegeben werden. Wenn Sie eine Outpost-Ressource über die AWS Outposts Konsole gemeinsam nutzen, fügen Sie sie einer vorhandenen

Ressourcenfreigabe hinzu. Um die Outpost-Ressource einer neuen Ressourcenfreigabe hinzufügen zu können, müssen Sie zunächst die Ressourcenfreigabe mithilfe der AWS RAM -Konsole erstellen.

Wenn Sie Teil einer Organisation sind AWS Organizations und die gemeinsame Nutzung innerhalb Ihrer Organisation aktiviert ist, können Sie Verbrauchern in Ihrer Organisation von der AWS RAM Konsole aus Zugriff auf die gemeinsam genutzte Outpost-Ressource gewähren. Andernfalls erhalten Konsumenten eine Einladung zur Teilnahme an der Ressourcenfreigabe und nach Annahme der Einladung wird ihnen Zugriff auf gemeinsam genutzte Outpost-Ressource gewährt.

Sie können eine Outpost-Ressource, die Sie besitzen, über die AWS Outposts Konsole, AWS RAM die Konsole oder die gemeinsam nutzen. AWS CLI

Um einen Outpost, den Sie besitzen, über die Konsole zu teilen AWS Outposts

1. Öffnen Sie die AWS Outposts Konsole unter. https://console.aws.amazon.com/outposts/
2. Wählen Sie im Navigationsbereich Outposts aus.
3. Wählen Sie Ihren Outpost aus und klicken Sie anschließend auf Aktionen, Details anzeigen.
4. Wählen Sie auf der Outpost-Übersichtsseite die Option Freigabe von Ressourcen.
5. Wählen Sie Create resource share (Ressourcenfreigabe erstellen) aus.

Sie werden zur AWS RAM Konsole weitergeleitet, um die gemeinsame Nutzung des Outposts abzuschließen. Gehen Sie wie folgt vor. Gehen Sie ebenfalls wie folgt vor, um eine lokale Gateway-Routing-Tabelle, die Sie besitzen, gemeinsam zu nutzen.

So geben Sie eine Routing-Tabelle des Outpost oder eines lokalen Gateways frei, die Sie über die AWS RAM -Konsole besitzen

Siehe Erstellen einer Ressourcenfreigabe im AWS RAM -Benutzerhandbuch.

Um eine Outpost- oder Local-Gateway-Routentabelle, die Sie besitzen, mit dem AWS CLI

Verwenden Sie den create-resource-share-Befehl.

## Aufheben der Freigabe einer Outpost-Ressource

Wenn Sie die gemeinsame Nutzung Ihres Outposts mit einem Verbraucher beenden, kann der Verbraucher Folgendes nicht mehr tun:

- Sehen Sie sich den Outpost in der Konsole an. AWS Outposts

- Erstellen Sie neue Subnetze im Outpost.
- Erstellen Sie neue Amazon EBS-Volumes auf dem Outpost.
- Sehen Sie sich die Outpost-Details und Instance-Typen über die AWS Outposts Konsole oder die an. AWS CLI

Subnetze, Volumes oder Instances, die der Verbraucher während des gemeinsamen Zeitraums erstellt hat, werden nicht gelöscht. Der Verbraucher kann weiterhin wie folgt vorgehen:

- Greifen Sie auf diese Ressourcen zu und ändern Sie sie.
- Starten Sie neue Instances in einem vorhandenen Subnetz, das der Verbraucher erstellt hat.

Um zu verhindern, dass der Verbraucher auf seine Ressourcen zugreift und neue Instances in Ihrem Outpost startet, fordern Sie den Verbraucher auf, seine Ressourcen zu löschen.

Wenn eine gemeinsam genutzte lokale Gateway-Routentabelle nicht mehr gemeinsam genutzt wird, kann der Verbraucher keine neuen VPC-Zuordnungen mehr zu ihr erstellen. Alle vorhandenen VPC-Zuordnungen, die der Verbraucher erstellt hat, bleiben mit der Routing-Tabelle verknüpft. Die darin enthaltenen Ressourcen VPCs können den Verkehr weiterhin an das lokale Gateway weiterleiten. Um dies zu verhindern, fordern Sie den Verbraucher auf, die VPC-Zuordnungen zu löschen.

Um die Freigabe einer freigegebenen Outpost-Ressource, deren Eigentümer Sie sind, aufzuheben, müssen Sie sie aus der Ressourcenfreigabe entfernen. Sie können dies mit der AWS RAM Konsole oder dem AWS CLI tun.

Um die gemeinsame Nutzung einer gemeinsam genutzten Outpost-Ressource, die Sie besitzen, mithilfe der Konsole rückgängig zu machen AWS RAM

Siehe Aktualisieren einer Ressourcenfreigabe im AWS RAM -Benutzerhandbuch.

Um die Freigabe einer geteilten Outpost-Ressource, deren Eigentümer Sie sind, rückgängig zu machen, verwenden Sie AWS CLI

Verwenden Sie den disassociate-resource-share-Befehl.

## Identifizieren einer freigegebenen Outpost-Ressource

Eigentümer und Verbraucher können gemeinsam genutzte Outposts über die AWS Outposts Konsole und AWS CLI identifizieren. Sie können gemeinsam genutzte lokale Gateway-Routing-Tabellen mit AWS CLI identifizieren.

Um einen gemeinsam genutzten Outpost mithilfe der Konsole zu identifizieren AWS Outposts

1. Öffnen Sie die AWS Outposts Konsole unter. https://console.aws.amazon.com/outposts/
2. Wählen Sie im Navigationsbereich Outposts aus.
3. Wählen Sie Ihren Outpost aus und klicken Sie anschließend auf Aktionen, Details anzeigen.
4. Sehen Sie sich auf der Outpost-Übersichtsseite die Besitzer-ID an, um die AWS Konto-ID des Outpost-Besitzers zu identifizieren.

Um eine gemeinsam genutzte Outpost-Ressource zu identifizieren, verwenden Sie AWS CLI

Verwenden Sie die Befehle list-outposts und -tables. describe-local-gateway-route Diese Befehle geben die Outpost-Ressourcen zurück, die Sie besitzen, und die Outpost-Ressourcen, die mit Ihnen geteilt wurden. `OwnerId`zeigt die AWS Konto-ID des Besitzers der Outpost-Ressource an.

# Berechtigungen für freigegebene Outpost-Ressourcen

## Berechtigungen für Besitzer

Die Eigentümer sind für die Verwaltung des Outposts und der Ressourcen, die sie darin anlegen, verantwortlich. Besitzer können die Freigabe jederzeit ändern oder widerrufen. Sie können AWS Organizations damit Ressourcen anzeigen, ändern und löschen, die Verbraucher in geteilten Outposts erstellen.

## Berechtigungen für Konsumenten

Konsumenten können beim Erstellen von Ressourcen in Outposts so vorgehen, wie sie dies beim Erstellen von Ressourcen auf Outposts tun würden, die sie in ihrem eigenen Konto erstellen. Konsumenten sind für die Verwaltung der Ressourcen verantwortlich, die sie auf Outposts starten, die für sie freigegeben sind. Konsumenten können sich keine Ressourcen anzeigen lassen oder ändern, die anderen Konsumenten oder dem Besitzer des Outposts gehören, und sie können keine Outposts ändern, die für sie freigegeben sind.

# Fakturierung und Messung

Eigentümern werden die Outposts und Outpost-Ressourcen in Rechnung gestellt, die sie freigeben. Ihnen werden auch alle Datenübertragungsgebühren in Rechnung gestellt, die mit dem Service Link-VPN-Verkehr ihres Outposts aus der Region verbunden sind. AWS

Für die Freigabe von lokalen Gateway-Routing-Tabellen fallen keine zusätzlichen Gebühren an. Bei gemeinsam genutzten Subnetzen werden dem VPC-Besitzer Ressourcen auf VPC-Ebene wie VPN-Verbindungen, NAT-Gateways AWS Direct Connect und Private Link-Verbindungen in Rechnung gestellt.

Konsumenten werden Anwendungsressourcen in Rechnung gestellt, die sie auf freigegebenen Outposts erstellen, wie Load Balancer und Amazon RDS-Datenbanken. Verbrauchern werden auch kostenpflichtige Datenübertragungen aus der Region in Rechnung gestellt. AWS

## Einschränkungen

Für die Arbeit mit dem AWS Outposts Teilen gelten die folgenden Einschränkungen:

- Einschränkungen für gemeinsam genutzte Subnetze gelten für die Arbeit mit der Funktion „ AWS Outposts Teilen“. Weitere Informationen über die Grenzen der VPC-Freigabe finden Sie unter Beschränkungen im Amazon Virtual Private Cloud Benutzerhandbuch.
- Servicekontingente werden auf einzelne Konten angewendet.

# Sicherheit in AWS Outposts

Sicherheit AWS hat höchste Priorität. Als AWS Kunde profitieren Sie von einer Rechenzentrums- und Netzwerkarchitektur, die darauf ausgelegt sind, die Anforderungen der sicherheitssensibelsten Unternehmen zu erfüllen.

Sicherheit ist eine gemeinsame Verantwortung von Ihnen AWS und Ihnen. Das Modell der übergreifenden Verantwortlichkeit beschreibt dies als Sicherheit der Cloud und Sicherheit in der Cloud:

- Sicherheit der Cloud — AWS ist verantwortlich für den Schutz der Infrastruktur, die AWS Dienste in der AWS Cloud ausführt. AWS bietet Ihnen auch Dienste, die Sie sicher nutzen können. Externe Prüfer testen und verifizieren regelmäßig die Wirksamkeit unserer Sicherheitsmaßnahmen im Rahmen der AWS . Weitere Informationen zu den Compliance-Programmen, die für gelten AWS Outposts, finden Sie unter AWS Services im Umfang nach Compliance-Programmen AWS .
- Sicherheit in der Cloud — Ihre Verantwortung richtet sich nach dem AWS Dienst, den Sie nutzen. Sie sind auch für andere Faktoren verantwortlich, etwa für die Vertraulichkeit Ihrer Daten, für die Anforderungen Ihres Unternehmens und für die geltenden Gesetze und Vorschriften.

Weitere Informationen zu Sicherheit und Compliance für AWS Outposts finden Sie in den häufig gestellten Fragen zu AWS Outposts.

Diese Dokumentation hilft Ihnen zu verstehen, wie Sie das Modell der gemeinsamen Verantwortung bei der Verwendung anwenden können AWS Outposts. Es zeigt Ihnen, wie Sie Ihre Sicherheits- und Compliance-Ziele zu erreichen. Sie erfahren auch, wie Sie andere AWS Dienste nutzen können, die Ihnen bei der Überwachung und Sicherung Ihrer Ressourcen helfen.

Inhalt

# Datenschutz in AWS Outposts

Das Modell der AWS gemeinsamen Verantwortung und geteilter Verantwortung gilt für den Datenschutz in AWS Outposts. Wie in diesem Modell beschrieben, AWS ist verantwortlich für den Schutz der globalen Infrastruktur, auf der alle Systeme laufen AWS Cloud. Sie sind dafür verantwortlich, die Kontrolle über Ihre in dieser Infrastruktur gehosteten Inhalte zu behalten. Dieser Inhalt umfasst die Sicherheitskonfiguration und die Verwaltungsaufgaben für AWS-Services das, was Sie verwenden.

Aus Datenschutzgründen empfehlen wir, dass Sie AWS-Konto Anmeldeinformationen schützen und einzelne Benutzer mit AWS IAM Identity Center oder AWS Identity and Access Management (IAM) einrichten. So erhält jeder Benutzer nur die Berechtigungen, die zum Durchführen seiner Aufgaben erforderlich sind.

Weitere Informationen zum Datenschutz finden Sie unter Häufig gestellte Fragen zum Datenschutz. Informationen zum Datenschutz in Europa finden Sie im Blog-Beitrag AWS -Modell der geteilten Verantwortung und in der DSGVO im AWS -Sicherheitsblog.

## Verschlüsselung im Ruhezustand

Mit AWS Outposts werden alle Daten im Ruhezustand verschlüsselt. Das Schlüsselmaterial befindet sich in einem externen Schlüssel, der auf einem austauschbaren Gerät gespeichert ist, dem Nitro Security Key (NSK).

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. Weitere Informationen finden Sie unter Amazon EBS Encryption im Amazon EBS-Benutzerhandbuch.

## Verschlüsselung während der Übertragung

AWS verschlüsselt Daten, die während der Übertragung zwischen Ihrem Outpost und seiner Region übertragen werden. AWS Weitere Informationen finden Sie unter Konnektivität über Service Link.

Sie können ein Verschlüsselungsprotokoll wie Transport Layer Security (TLS) verwenden, um sensible Daten während der Übertragung über das lokale Gateway zu Ihrem lokalen Netzwerk zu verschlüsseln.

## Löschen von Daten

Wenn Sie eine EC2 Instance stoppen oder beenden, wird der ihr zugewiesene Speicher vom Hypervisor gelöscht (auf Null gesetzt), bevor er einer neuen Instance zugewiesen wird, und jeder Speicherblock wird zurückgesetzt.

Durch die Zerstörung des Nitro-Sicherheitsschlüssels werden die Daten auf Ihrem Outpost kryptografisch vernichtet.

# Identity and access management (IAM) für AWS Outposts

AWS Identity and Access Management (IAM) ist ein AWS Dienst, der einem Administrator hilft, 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 Sie können IAM ohne zusätzliche Kosten nutzen.

Inhalt



## So funktioniert AWS Outposts mit IAM

Bevor Sie IAM verwenden, um den Zugriff auf AWS Outposts zu verwalten, sollten Sie sich darüber informieren, welche IAM-Funktionen für Outposts verfügbar sind. AWS

| IAM-Feature | AWS Unterstützung für Outposts |
| --- | --- |
| Identitätsbasierte Richtlinien | Ja |
| Ressourcenbasierte Richtlinien | Nein |
| Richtlinienaktionen | Ja |
| Richtlinienressourcen | Ja |

| IAM-Feature | AWS Unterstützung für Outposts |
| --- | --- |
| Richtlinienbedingungsschlüssel (services pezifisch) | Ja |
| ACLs | Nein |
| ABAC (Tags in Richtlinien) | Ja |
| Temporäre Anmeldeinformationen | Ja |
| Prinzipalberechtigungen | Ja |
| Servicerollen | Nein |
| Serviceverknüpfte Rollen | Ja |

## Identitätsbasierte Richtlinien für Outposts AWS

Unterstützt Richtlinien auf Identitätsbasis: Ja

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter Definieren benutzerdefinierter IAM-Berechtigungen mit vom Kunden verwalteten Richtlinien im IAM-Benutzerhandbuch.

Mit identitätsbasierten IAM-Richtlinien können Sie angeben, welche Aktionen und Ressourcen zugelassen oder abgelehnt werden. Darüber hinaus können Sie die Bedingungen festlegen, unter denen Aktionen zugelassen oder abgelehnt werden. Sie können den Prinzipal nicht in einer identitätsbasierten Richtlinie angeben, da er für den Benutzer oder die Rolle gilt, dem er zugeordnet ist. Informationen zu sämtlichen Elementen, die Sie in einer JSON-Richtlinie verwenden, finden Sie in der IAM-Referenz für JSON-Richtlinienelemente im IAM-Benutzerhandbuch.

Beispiele für identitätsbasierte Richtlinien für Outposts AWS

Beispiele für identitätsbasierte Richtlinien von AWS Outposts finden Sie unter. AWS Politische Beispiele für Outposts

## Politische Maßnahmen für AWS Outposts

Unterstützt Richtlinienaktionen: Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Das Element `Action` einer JSON-Richtlinie beschreibt die Aktionen, mit denen Sie den Zugriff in einer Richtlinie zulassen oder verweigern können. Richtlinienaktionen haben normalerweise denselben Namen wie der zugehörige AWS API-Vorgang. Es gibt einige Ausnahmen, z. B. Aktionen, die nur mit Genehmigung durchgeführt werden können und für die es keinen passenden API-Vorgang gibt. Es gibt auch einige Operationen, die mehrere Aktionen in einer Richtlinie erfordern. Diese zusätzlichen Aktionen werden als abhängige Aktionen bezeichnet.

Schließen Sie Aktionen in eine Richtlinie ein, um Berechtigungen zur Durchführung der zugeordneten Operation zu erteilen.

Eine Liste der AWS Outposts-Aktionen finden Sie unter Actions defined by AWS Outposts in der Service Authorization Reference.

Richtlinienaktionen in AWS Outposts verwenden das folgende Präfix vor der Aktion:

```
outposts
```

Um mehrere Aktionen in einer einzigen Anweisung anzugeben, trennen Sie sie mit Kommata:

```
"Action": [
    "outposts:action1",
    "outposts:action2"
]
```

Sie können auch Platzhalter verwenden, um mehrere Aktionen anzugeben. Beispielsweise können Sie alle Aktionen festlegen, die mit dem Wort `List` beginnen, einschließlich der folgenden Aktion:

```
"Action": "outposts:List*"
```

## Politische Ressourcen für AWS Outposts

Unterstützt Richtlinienressourcen: Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Das JSON-Richtlinienelement `Resource` gibt die Objekte an, auf welche die Aktion angewendet wird. Anweisungen müssen entweder ein – `Resource`oder ein `NotResource`-Element enthalten. Als bewährte Methode geben Sie eine Ressource mit dem zugehörigen Amazon-Ressourcennamen (ARN) an. Sie können dies für Aktionen tun, die einen bestimmten Ressourcentyp unterstützen, der als Berechtigungen auf Ressourcenebene bezeichnet wird.

Verwenden Sie für Aktionen, die keine Berechtigungen auf Ressourcenebene unterstützen, z. B. Auflistungsoperationen, einen Platzhalter (*), um anzugeben, dass die Anweisung für alle Ressourcen gilt.

```
"Resource": "*"
```

Einige AWS Outposts API-Aktionen unterstützen mehrere Ressourcen. Um mehrere Ressourcen in einer einzigen Anweisung anzugeben, trennen Sie sie ARNs durch Kommas.

```
"Resource": [
    "resource1",
    "resource2"
]
```

Eine Liste der AWS Outposts-Ressourcentypen und ihrer ARNs Eigenschaften finden Sie unter Ressourcentypen definiert von AWS Outposts in der Service Authorization Reference. Informationen zu den Aktionen, mit denen Sie den ARN einzelner Ressourcen angeben können, finden Sie unter Von AWS Outposts definierte Aktionen.

## Schlüssel zu den Policy-Bedingungen für AWS Outposts

Unterstützt servicespezifische Richtlinienbedingungsschlüssel: Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das Element `Condition` (oder `Condition` block) ermöglicht Ihnen die Angabe der Bedingungen, unter denen eine Anweisung wirksam ist. Das Element `Condition` ist optional. Sie können bedingte

Ausdrücke erstellen, die Bedingungsoperatoren verwenden, z. B. ist gleich oder kleiner als, damit die Bedingung in der Richtlinie mit Werten in der Anforderung übereinstimmt.

Wenn Sie mehrere `Condition`-Elemente in einer Anweisung oder mehrere Schlüssel in einem einzelnen `Condition`-Element angeben, wertet AWS diese mittels einer logischen `AND`-Operation aus. Wenn Sie mehrere Werte für einen einzelnen Bedingungsschlüssel angeben, AWS wertet die Bedingung mithilfe einer logischen `OR` Operation aus. Alle Bedingungen müssen erfüllt werden, bevor die Berechtigungen der Anweisung gewährt werden.

Sie können auch Platzhaltervariablen verwenden, wenn Sie Bedingungen angeben. Beispielsweise können Sie einem IAM-Benutzer die Berechtigung für den Zugriff auf eine Ressource nur dann gewähren, wenn sie mit dessen IAM-Benutzernamen gekennzeichnet ist. Weitere Informationen finden Sie unter IAM-Richtlinienelemente: Variablen und Tags im IAM-Benutzerhandbuch.

AWS unterstützt globale Bedingungsschlüssel und dienstspezifische Bedingungsschlüssel. Eine Übersicht aller AWS globalen Bedingungsschlüssel finden Sie unter Kontextschlüssel für AWS globale Bedingungen im IAM-Benutzerhandbuch.

Eine Liste der Bedingungsschlüssel von AWS Outposts finden Sie unter Bedingungsschlüssel für AWS Outposts in der Service Authorization Reference. Informationen zu den Aktionen und Ressourcen, mit denen Sie einen Bedingungsschlüssel verwenden können, finden Sie unter Aktionen definiert von AWS Outposts.

Beispiele für identitätsbasierte Richtlinien von AWS Outposts finden Sie unter. AWS Politische Beispiele für Outposts

## ABAC mit Outposts AWS

Unterstützt ABAC (Tags in Richtlinien): Ja

Die attributbasierte Zugriffskontrolle (ABAC) ist eine Autorisierungsstrategie, bei der Berechtigungen basierend auf Attributen definiert werden. In AWS werden diese Attribute als Tags bezeichnet. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und an viele AWS Ressourcen anhängen. Das Markieren von Entitäten und Ressourcen ist der erste Schritt von ABAC. Anschließend entwerfen Sie ABAC-Richtlinien, um Operationen zuzulassen, wenn das Tag des Prinzipals mit dem Tag der Ressource übereinstimmt, auf die sie zugreifen möchten.

ABAC ist in Umgebungen hilfreich, die schnell wachsen, und unterstützt Sie in Situationen, in denen die Richtlinienverwaltung mühsam wird.

Um den Zugriff auf der Grundlage von Tags zu steuern, geben Sie im Bedingungselement einer Richtlinie Tag-Informationen an, indem Sie die Schlüssel `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`, oder Bedingung `aws:TagKeys` verwenden.

Wenn ein Service alle drei Bedingungsschlüssel für jeden Ressourcentyp unterstützt, lautet der Wert für den Service Ja. Wenn ein Service alle drei Bedingungsschlüssel für nur einige Ressourcentypen unterstützt, lautet der Wert Teilweise.

Weitere Informationen zu ABAC finden Sie unter Definieren von Berechtigungen mit ABAC-Autorisierung im IAM-Benutzerhandbuch. Um ein Tutorial mit Schritten zur Einstellung von ABAC anzuzeigen, siehe Attributbasierte Zugriffskontrolle (ABAC) verwenden im IAM-Benutzerhandbuch.

## Temporäre Anmeldeinformationen mit AWS Outposts verwenden

Unterstützt temporäre Anmeldeinformationen: Ja

Manche funktionieren AWS-Services nicht, wenn Sie sich mit temporären Zugangsdaten anmelden. Weitere Informationen, einschließlich Informationen, die mit temporären Anmeldeinformationen AWS-Services funktionieren AWS-Services , finden Sie im IAM-Benutzerhandbuch unter Diese Option funktioniert mit IAM.

Sie verwenden temporäre Anmeldeinformationen, wenn Sie sich mit einer anderen AWS Management Console Methode als einem Benutzernamen und einem Passwort anmelden. Wenn Sie beispielsweise AWS über den Single Sign-On-Link (SSO) Ihres Unternehmens darauf zugreifen, werden bei diesem Vorgang automatisch temporäre Anmeldeinformationen erstellt. Sie erstellen auch automatisch temporäre Anmeldeinformationen, wenn Sie sich als Benutzer bei der Konsole anmelden und dann die Rollen wechseln. Weitere Informationen zum Wechseln von Rollen finden Sie unter Wechseln von einer Benutzerrolle zu einer IAM-Rolle (Konsole) im IAM-Benutzerhandbuch.

Mithilfe der AWS API AWS CLI oder können Sie temporäre Anmeldeinformationen manuell erstellen. Sie können diese temporären Anmeldeinformationen dann für den Zugriff verwenden AWS. AWS empfiehlt, temporäre Anmeldeinformationen dynamisch zu generieren, anstatt langfristige Zugriffsschlüssel zu verwenden. Weitere Informationen finden Sie unter Temporäre Sicherheitsanmeldeinformationen in IAM.

## Serviceübergreifende Prinzipalberechtigungen für Outposts AWS

Unterstützt Forward Access Sessions (FAS): Ja

Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion

in einem anderen Service initiieren. FAS verwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, kombiniert mit der Anforderung, Anfragen an nachgelagerte Dienste AWS-Service zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, für deren Abschluss Interaktionen mit anderen AWS-Services oder Ressourcen erforderlich sind. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anfragen finden Sie unter Zugriffssitzungen weiterleiten.

### Servicebezogene Rollen für Outposts AWS

Unterstützt dienstbezogene Rollen: Ja

Eine serviceverknüpfte Rolle ist eine Art von Servicerolle, die mit einer verknüpft ist. AWS-Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Dienstbezogene Rollen werden in Ihrem Dienst angezeigt AWS-Konto und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.

Einzelheiten zum Erstellen oder Verwalten von dienstbezogenen AWS Outposts-Rollen finden Sie unter. Mit Diensten verknüpfte Rollen für AWS Outposts

## AWS Politische Beispiele für Outposts

Standardmäßig sind Benutzer und Rollen nicht berechtigt, AWS Outposts-Ressourcen zu erstellen oder zu ändern. Sie können auch keine Aufgaben mithilfe der AWS Management Console, AWS Command Line Interface (AWS CLI) oder AWS API ausführen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen auszuführen, die sie benötigen. Der Administrator kann dann die IAM-Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen annehmen.

Informationen dazu, wie Sie unter Verwendung dieser beispielhaften JSON-Richtliniendokumente eine identitätsbasierte IAM-Richtlinie erstellen, finden Sie unter Erstellen von IAM-Richtlinien (Konsole) im IAM-Benutzerhandbuch.

Einzelheiten zu den von AWS Outposts definierten Aktionen und Ressourcentypen, einschließlich des Formats ARNs für die einzelnen Ressourcentypen, finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für AWS Outposts in der Service Authorization Reference.

Inhalt

- Beispiel: Nutzen von Berechtigungen auf Ressourcenebene

## Bewährte Methoden für Richtlinien

Identitätsbasierte Richtlinien legen fest, ob jemand AWS Outposts-Ressourcen in Ihrem Konto erstellen, darauf zugreifen oder sie löschen kann. Dies kann zusätzliche Kosten für Ihr verursachen AWS-Konto. Befolgen Sie beim Erstellen oder Bearbeiten identitätsbasierter Richtlinien die folgenden Anleitungen und Empfehlungen:

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten — Verwenden Sie die AWS verwalteten Richtlinien, die Berechtigungen für viele gängige Anwendungsfälle gewähren, um Ihren Benutzern und Workloads zunächst Berechtigungen zu gewähren. Sie sind in Ihrem verfügbar. AWS-Konto Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom AWS Kunden verwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind. Weitere Informationen finden Sie unter AWS -verwaltete Richtlinien oder AWS -verwaltete Richtlinien für Auftrags-Funktionen im IAM-Benutzerhandbuch.
- Anwendung von Berechtigungen mit den geringsten Rechten – Wenn Sie mit IAM-Richtlinien Berechtigungen festlegen, gewähren Sie nur die Berechtigungen, die für die Durchführung einer Aufgabe erforderlich sind. Sie tun dies, indem Sie die Aktionen definieren, die für bestimmte Ressourcen unter bestimmten Bedingungen durchgeführt werden können, auch bekannt als die geringsten Berechtigungen. Weitere Informationen zur Verwendung von IAM zum Anwenden von Berechtigungen finden Sie unter Richtlinien und Berechtigungen in IAM im IAM-Benutzerhandbuch.
- Verwenden von Bedingungen in IAM-Richtlinien zur weiteren Einschränkung des Zugriffs – Sie können Ihren Richtlinien eine Bedingung hinzufügen, um den Zugriff auf Aktionen und Ressourcen zu beschränken. Sie können beispielsweise eine Richtlinienbedingung schreiben, um festzulegen, dass alle Anforderungen mithilfe von SSL gesendet werden müssen. Sie können auch Bedingungen verwenden, um Zugriff auf Serviceaktionen zu gewähren, wenn diese für einen bestimmten Zweck verwendet werden AWS-Service, z. AWS CloudFormation B. Weitere Informationen finden Sie unter IAM-JSON-Richtlinienelemente: Bedingung im IAM-Benutzerhandbuch.
- Verwenden von IAM Access Analyzer zur Validierung Ihrer IAM-Richtlinien, um sichere und funktionale Berechtigungen zu gewährleisten – IAM Access Analyzer validiert neue und vorhandene Richtlinien, damit die Richtlinien der IAM-Richtliniensprache (JSON) und den bewährten IAM-Methoden entsprechen. IAM Access Analyzer stellt mehr als

100 Richtlinienprüfungen und umsetzbare Empfehlungen zur Verfügung, damit Sie sichere und funktionale Richtlinien erstellen können. Weitere Informationen finden Sie unter Richtlinienvalidierung mit IAM Access Analyzer im IAM-Benutzerhandbuch.

- Multi-Faktor-Authentifizierung (MFA) erforderlich — Wenn Sie ein Szenario haben, das IAM-Benutzer oder einen Root-Benutzer in Ihrem System erfordert AWS-Konto, aktivieren Sie MFA für zusätzliche Sicherheit. Um MFA beim Aufrufen von API-Vorgängen anzufordern, fügen Sie Ihren Richtlinien MFA-Bedingungen hinzu. Weitere Informationen finden Sie unter Sicherer API-Zugriff mit MFA im IAM-Benutzerhandbuch.

Weitere Informationen zu bewährten Methoden in IAM finden Sie unter Bewährte Methoden für die Sicherheit in IAM im IAM-Benutzerhandbuch.

## Beispiel: Nutzen von Berechtigungen auf Ressourcenebene

Im folgenden Beispiel werden Berechtigungen auf Ressourcenebene verwendet, um die Berechtigung zum Abrufen von Informationen über den angegebenen Outpost zu gewähren.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "outposts:GetOutpost",
      "Resource": "arn:aws:outposts:region:12345678012:outpost/op-1234567890abcdef0"
    }
  ]
}
```

Im folgenden Beispiel werden Berechtigungen auf Ressourcenebene verwendet, um die Berechtigung zum Abrufen von Informationen über den angegebenen Standort zu gewähren.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "outposts:GetSite",
      "Resource": "arn:aws:outposts:region:12345678012:site/os-0abcdef1234567890"
    }
  ]
```

```
}
```

# Mit Diensten verknüpfte Rollen für AWS Outposts

AWS Outposts verwendet AWS Identity and Access Management (IAM) serviceverknüpfte Rollen. Eine serviceverknüpfte Rolle ist eine Art von Servicerolle, mit der direkt verknüpft ist. AWS Outposts AWS Outposts definiert dienstbezogene Rollen und umfasst alle Berechtigungen, die erforderlich sind, um andere AWS Dienste in Ihrem Namen aufzurufen.

Eine dienstbezogene Rolle macht Ihre Einrichtung AWS Outposts effizienter, da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. AWS Outposts definiert die Berechtigungen ihrer dienstbezogenen Rollen und AWS Outposts kann, sofern nicht anders definiert, nur ihre Rollen übernehmen. Die definierten Berechtigungen umfassen die Vertrauens- und Berechtigungsrichtlinie. Diese Berechtigungsrichtlinie kann keinen anderen IAM-Entitäten zugewiesen werden.

Sie können eine serviceverknüpfte Rolle nur löschen, nachdem Sie zuvor die zugehörigen Ressourcen gelöscht haben. Dadurch werden Ihre AWS Outposts Ressourcen geschützt, da Sie nicht versehentlich die Zugriffsberechtigung für die Ressourcen entziehen können.

## Mit dem Dienst verknüpfte Rollenberechtigungen für AWS Outposts

AWS Outposts verwendet die mit dem Dienst verknüpfte Rolle mit dem Namen AWSServiceRoleForOutposts_ ***`OutpostID`***. Diese Rolle gewährt Outposts die Erlaubnis, Netzwerkressourcen zu verwalten, um private Konnektivität in Ihrem Namen zu ermöglichen. Diese Rolle ermöglicht es Outposts auch, Netzwerkschnittstellen zu erstellen und zu konfigurieren, Sicherheitsgruppen zu verwalten und Schnittstellen an Service Link-Endpunktinstanzen anzuhängen. Diese Berechtigungen sind erforderlich, um die sichere, private Verbindung zwischen Ihrem lokalen Outpost und den AWS Diensten herzustellen und aufrechtzuerhalten und so den zuverlässigen Betrieb Ihrer Outpost-Bereitstellung zu gewährleisten.

Die Rolle AWSService RoleForOutposts _, die *`OutpostID`* mit dem Dienst verknüpft ist, vertraut darauf, dass die folgenden Dienste die Rolle übernehmen:

- `outposts.amazonaws.com`

Richtlinien für dienstbezogene Rollen

Die *`OutpostID`* dienstbezogene Rolle AWSService RoleForOutposts _ umfasst die folgenden Richtlinien:

- AWSOutpostsServiceRolePolicy
- AWSOutpostsPrivateConnectivityPolicy_*OutpostID*

AWSOutpostsServiceRolePolicy

Die `AWSOutpostsServiceRolePolicy` Richtlinie ermöglicht den Zugriff auf AWS Ressourcen, die von verwaltet werden AWS Outposts.

Diese Richtlinie ermöglicht AWS Outposts es, die folgenden Aktionen an den angegebenen Ressourcen durchzuführen:

- Aktion: `ec2:DescribeNetworkInterfaces` für alle AWS Ressourcen
- Aktion: `ec2:DescribeSecurityGroups` für alle AWS Ressourcen
- Aktion: `ec2:DescribeSubnets` für alle AWS Ressourcen
- Aktion: `ec2:DescribeVpcEndpoints` für alle AWS Ressourcen
- Maßnahme: `ec2:CreateNetworkInterface` in Bezug auf die folgenden AWS Ressourcen:

```
"arn:*:ec2:*:*:vpc/*",
"arn:*:ec2:*:*:subnet/*",
"arn:*:ec2:*:*:security-group/*"
```

- Aktion: `ec2:CreateNetworkInterface` für die AWS Ressource`"arn:*:ec2:*:*:network-interface/*"`, die die folgende Bedingung erfüllt:

```
"ForAnyValue:StringEquals" : { "aws:TagKeys": [ "outposts:private-
connectivity-resourceId" ] }
```

- Aktion: `ec2:CreateSecurityGroup` für die folgenden AWS Ressourcen:

```
"arn:*:ec2:*:*:vpc/*"
```

- Aktion: `ec2:CreateSecurityGroup` für die AWS Ressource`"arn:*:ec2:*:*:security-group/*"`, die die folgende Bedingung erfüllt:

```
"ForAnyValue:StringEquals": { "aws:TagKeys": [ "outposts:private-
connectivity-resourceId" ] }
```

### AWSOutpostsPrivateConnectivityPolicy_OutpostID

Die `AWSOutpostsPrivateConnectivityPolicy_`*`OutpostID`* Richtlinie ermöglicht AWS Outposts es, die folgenden Aktionen für die angegebenen Ressourcen durchzuführen:

- Aktion: `ec2:AuthorizeSecurityGroupIngress` für alle AWS Ressourcen, die die folgende Bedingung erfüllen:

```
{ "StringLike" : { "ec2:ResourceTag/outposts:private-connectivity-resourceId" :
 "OutpostID" }} and { "StringEquals" : { "ec2:Vpc" : "vpcArn" }}
```

- Aktion: `ec2:AuthorizeSecurityGroupEgress` für alle AWS Ressourcen, die die folgende Bedingung erfüllen:

```
{ "StringLike" : { "ec2:ResourceTag/outposts:private-connectivity-resourceId" :
 "OutpostID" }} and { "StringEquals" : { "ec2:Vpc" : "vpcArn" }}
```

- Aktion: `ec2:CreateNetworkInterfacePermission` für alle AWS Ressourcen, die die folgende Bedingung erfüllen:

```
{ "StringLike" : { "ec2:ResourceTag/outposts:private-connectivity-resourceId" :
 "OutpostID" }} and { "StringEquals" : { "ec2:Vpc" : "vpcArn" }}
```

- Aktion: `ec2:CreateTags` für alle AWS Ressourcen, die die folgende Bedingung erfüllen:

```
{ "StringLike" : { "aws:RequestTag/outposts:private-connectivity-resourceId" :
 "{{OutpostId}}*"}},
"StringEquals": {"ec2:CreateAction" : ["CreateSecurityGroup",
 "CreateNetworkInterface"]}
```

- Aktion: `ec2:RevokeSecurityGroupIngress` für alle AWS Ressourcen, die die folgende Bedingung erfüllen:

```
{ "StringLike" : { "ec2:ResourceTag/outposts:private-connectivity-resourceId" :
 "OutpostID" }} and { "StringEquals" : { "ec2:Vpc" : "vpcArn" }}
```

- Aktion: `ec2:RevokeSecurityGroupEgress` für alle AWS Ressourcen, die die folgende Bedingung erfüllen:

```
{ "StringLike" : { "ec2:ResourceTag/outposts:private-connectivity-resourceId" :
 "OutpostID" }} and { "StringEquals" : { "ec2:Vpc" : "vpcArn" }}
```

- Aktion: `ec2:DeleteNetworkInterface` für alle AWS Ressourcen, die die folgende Bedingung erfüllen:

```
{ "StringLike" : { "ec2:ResourceTag/outposts:private-connectivity-resourceId" :
 "OutpostID" }} and { "StringEquals" : { "ec2:Vpc" : "vpcArn" }}
```

- Aktion: `ec2:DeleteSecurityGroup` für alle AWS Ressourcen, die die folgende Bedingung erfüllen:

```
{ "StringLike" : { "ec2:ResourceTag/outposts:private-connectivity-resourceId" :
 "OutpostID" }} and { "StringEquals" : { "ec2:Vpc" : "vpcArn" }}
```

Sie müssen Berechtigungen konfigurieren, damit eine juristische Stelle von IAM (z. B. Benutzer, Gruppe oder Rolle) eine serviceverknüpfte Rolle erstellen, bearbeiten oder löschen kann. Weitere Informationen finden Sie unter Serviceverknüpfte Rollenberechtigung im IAM-Benutzerhandbuch.

## Erstellen Sie eine serviceverknüpfte Rolle für AWS Outposts

Sie müssen eine serviceverknüpfte Rolle nicht manuell erstellen. Wenn Sie die private Konnektivität für Ihren Outpost in der konfigurieren AWS Management Console, AWS Outposts erstellt die serviceverknüpfte Rolle für Sie.

Weitere Informationen finden Sie unter Private Verbindungsoptionen für Service Link.

## Bearbeiten Sie eine serviceverknüpfte Rolle für AWS Outposts

AWS Outposts erlaubt es Ihnen nicht, die mit dem *OutpostID* Dienst AWSService RoleForOutposts _ verknüpfte Rolle zu bearbeiten. Da möglicherweise verschiedene Entitäten auf die Rolle verweisen, kann der Rollenname nach der Erstellung einer serviceverknüpften Rolle nicht bearbeitet werden. Sie können jedoch die Beschreibung der Rolle mit IAM bearbeiten. Weitere Informationen finden Sie unter Aktualisieren einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

## Löschen Sie eine dienstverknüpfte Rolle für AWS Outposts

Wenn Sie eine Funktion oder einen Service, die bzw. der eine serviceverknüpfte Rolle erfordert, nicht mehr benötigen, sollten Sie diese Rolle löschen. Auf diese Weise vermeiden Sie, dass eine ungenutzte Einheit nicht aktiv überwacht oder gewartet wird. Sie müssen jedoch die Ressourcen für Ihre serviceverknüpfte Rolle zunächst bereinigen, bevor Sie sie manuell löschen können.

Wenn der AWS Outposts Dienst die Rolle verwendet, wenn Sie versuchen, die Ressourcen zu löschen, schlägt das Löschen möglicherweise fehl. Wenn dies passiert, warten Sie einige Minuten und versuchen Sie es erneut.

Sie müssen Ihren Outpost löschen, bevor Sie die mit dem *OutpostID* Dienst AWSService RoleForOutposts _ verknüpfte Rolle löschen können.

Bevor Sie beginnen, stellen Sie sicher, dass Ihr Outpost nicht mit AWS Resource Access Manager () geteilt wird.AWS RAM Weitere Informationen findest du unter Aufheben der gemeinsamen Nutzung einer geteilten Outpost-Ressource.

Um AWS Outposts Ressourcen zu löschen, die von _ verwendet werden AWSService RoleForOutposts ***OutpostID***

Wenden Sie sich an den AWS Enterprise Support, um Ihren Outpost zu löschen.

So löschen Sie die -servicegebundene Rolle mit IAM

Weitere Informationen finden Sie unter Löschen einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

### Unterstützte Regionen für serviceverknüpfte Rollen AWS Outposts

AWS Outposts unterstützt die Verwendung von dienstbezogenen Rollen in allen Regionen, in denen der Dienst verfügbar ist. Weitere Informationen finden Sie in den Racks FAQs für Outposts.

## AWS verwaltete Richtlinien für AWS Outposts

Eine AWS verwaltete Richtlinie ist eine eigenständige Richtlinie, die von erstellt und verwaltet AWS wird. AWS Verwaltete Richtlinien sind so konzipiert, dass sie Berechtigungen für viele gängige Anwendungsfälle bereitstellen, sodass Sie damit beginnen können, Benutzern, Gruppen und Rollen Berechtigungen zuzuweisen.

Beachten Sie, dass AWS verwaltete Richtlinien für Ihre speziellen Anwendungsfälle möglicherweise keine Berechtigungen mit den geringsten Rechten gewähren, da sie allen AWS Kunden zur Verfügung stehen. Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom Kunden verwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind.

Sie können die in AWS verwalteten Richtlinien definierten Berechtigungen nicht ändern. Wenn die in einer AWS verwalteten Richtlinie definierten Berechtigungen AWS aktualisiert werden, wirkt sich das

Update auf alle Prinzidentitäten (Benutzer, Gruppen und Rollen) aus, denen die Richtlinie zugeordnet ist. AWS aktualisiert eine AWS verwaltete Richtlinie höchstwahrscheinlich, wenn eine neue Richtlinie eingeführt AWS-Service wird oder neue API-Operationen für bestehende Dienste verfügbar werden.

Weitere Informationen finden Sie unter Von AWS verwaltete Richtlinien im IAM-Benutzerhandbuch.

## AWS verwaltete Richtlinie: AWSOutposts ServiceRolePolicy

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es AWS Outposts ermöglicht, Aktionen in Ihrem Namen durchzuführen. Weitere Informationen finden Sie unter Service-verknüpfte Rollen.

## AWS Outposts von Updates für AWS verwaltete Richtlinien

Sehen Sie sich Details zu Aktualisierungen der AWS verwalteten Richtlinien für AWS Outposts an, seit dieser Service begonnen hat, diese Änderungen zu verfolgen.

| Änderung | Beschreibung | Datum |
| --- | --- | --- |
| Aktualisierungen der dienstbezogenen Rolle _ AWS Identity and Access Management AWSService RoleForOutposts *OutpostID* | Die Berechtigungen für die *OutpostID* dienstverknüpfte Rolle AWSServiceRoleForOutposts_ wurden aktualisiert, um die AWS Outposts Verwaltung von Netzwerkressourcen für private Konnektivität zu verfeinern. Für Service Link-Endpunktinstanzen sind genauere Kontrollen der Netzwerkschnittstellen- und Sicherheitsgruppenoperationen erforderlich. | 18. April 2025 |
| AWS Outposts haben begonnen, Änderungen zu verfolgen | AWS Outposts begann, Änderungen an seinen AWS verwalteten Richtlinien nachzuverfolgen. | 03. Dezember 2019 |

# Sicherheit der Infrastruktur in AWS Outposts

Als verwalteter Service ist AWS Outposts durch AWS globale Netzwerksicherheit geschützt. Informationen zu AWS Sicherheitsdiensten und zum AWS Schutz der Infrastruktur finden Sie unter AWS Cloud-Sicherheit. Informationen zum Entwerfen Ihrer AWS Umgebung unter Verwendung der bewährten Methoden für die Infrastruktursicherheit finden Sie unter Infrastructure Protection in Security Pillar AWS Well-Architected Framework.

Sie verwenden AWS veröffentlichte API-Aufrufe, um über das Netzwerk auf AWS Outposts zuzugreifen. Kunden müssen Folgendes unterstützen:

- Transport Layer Security (TLS). Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Verschlüsselungs-Suiten mit Perfect Forward Secrecy (PFS) wie DHE (Ephemeral Diffie-Hellman) oder ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Die meisten modernen Systeme wie Java 7 und höher unterstützen diese Modi.

Außerdem müssen Anforderungen mit einer Zugriffsschlüssel-ID und einem geheimen Zugriffsschlüssel signiert sein, der einem IAM-Prinzipal zugeordnet ist. Alternativ können Sie mit AWS Security Token Service (AWS STS) temporäre Sicherheitsanmeldeinformationen erstellen, um die Anforderungen zu signieren.

Weitere Informationen zur Infrastruktursicherheit für die EC2 Instances und EBS-Volumes, die auf Ihrem Outpost ausgeführt werden, finden Sie unter Infrastruktursicherheit in Amazon. EC2

VPC-Flow-Logs funktionieren genauso wie in einer AWS Region. Das bedeutet, dass sie zur Analyse in CloudWatch Logs, Amazon S3 oder Amazon GuardDuty veröffentlicht werden können. Daten müssen zur Veröffentlichung in diesen Diensten an die Region zurückgesendet werden, sodass sie für CloudWatch oder andere Dienste nicht sichtbar sind, wenn der Outpost nicht verbunden ist.

## Überwachung von Manipulationen an Geräten AWS Outposts

Stellen Sie sicher, dass niemand die Geräte modifiziert, verändert, zurückentwickelt oder manipuliert. AWS Outposts AWS Outposts Geräte können mit einer Manipulationsüberwachung ausgestattet werden, um die Einhaltung der AWS Servicebedingungen sicherzustellen.

# Belastbarkeit in AWS Outposts

AWS Outposts ist so konzipiert, dass es hochverfügbar ist. Outposts-Racks sind mit redundanter Strom- und Netzwerkausrüstung ausgestattet. Für zusätzliche Stabilität empfehlen wir, dass Sie zwei Stromquellen und redundante Netzwerkkonnektivität für Ihren Outpost bereitstellen.

Für eine hohe Verfügbarkeit können Sie zusätzliche integrierte und immer aktive Kapazitäten auf Outposts-Racks bereitstellen. Outpost-Kapazitätskonfigurationen sind für den Betrieb in Produktionsumgebungen konzipiert und unterstützen N+1-Instances für jede Instance-Familie, wenn Sie die entsprechende Kapazität bereitstellen. AWS empfiehlt, dass Sie Ihren unternehmenskritischen Anwendungen ausreichend zusätzliche Kapazität zuweisen, um Wiederherstellung und Failover zu ermöglichen, wenn ein zugrunde liegendes Hostproblem vorliegt. Sie können die CloudWatch Amazon-Kapazitätsverfügbarkeitsmetriken verwenden und Alarme einrichten, um den Zustand Ihrer Anwendungen zu überwachen, CloudWatch Aktionen zur Konfiguration automatischer Wiederherstellungsoptionen zu erstellen und die Kapazitätsauslastung Ihrer Outposts im Laufe der Zeit zu überwachen.

Wenn Sie einen Outpost erstellen, wählen Sie eine Availability Zone aus einer AWS Region aus. Diese Availability Zone unterstützt Operationen der Steuerebene wie die Beantwortung von API-Aufrufen, die Überwachung des Outpost und die Aktualisierung des Outpost. Um von der Ausfallsicherheit der Availability Zones zu profitieren, können Sie Anwendungen auf mehreren Outposts bereitstellen, die jeweils mit einer anderen Availability Zone verbunden sind. Auf diese Weise können Sie zusätzliche Ausfallsicherheit für Anwendungen aufbauen und die Abhängigkeit von einer einzigen Availability Zone vermeiden. Weitere Informationen über Regionen und Availability Zones finden Sie unter Globale AWS -Infrastruktur.

Sie können eine Platzierungsgruppe mit einer Spread-Strategie verwenden, um sicherzustellen, dass Instances in unterschiedlichen Outposts-Racks platziert werden. Auf diese Weise können Sie korrelierte Ausfälle reduzieren. Weitere Informationen finden Sie unter Platzierungsgruppen auf Outposts.

Sie können Instances in Outposts mithilfe von Amazon EC2 Auto Scaling starten und einen Application Load Balancer erstellen, um den Datenverkehr zwischen den Instances zu verteilen. Weitere Informationen finden Sie unter Konfigurieren eines Application Load Balancerauf AWS Outposts.

# Konformitätsprüfung für AWS Outposts

Informationen darüber, ob AWS-Service ein AWS-Services in den Geltungsbereich bestimmter Compliance-Programme fällt, finden Sie unter Umfang nach Compliance-Programm AWS-Services unter . Wählen Sie dort das Compliance-Programm aus, an dem Sie interessiert sind. Allgemeine Informationen finden Sie unter AWS Compliance-Programme AWS .

Sie können Prüfberichte von Drittanbietern unter herunterladen AWS Artifact. Weitere Informationen finden Sie unter Berichte herunterladen unter .

Ihre Verantwortung für die Einhaltung der Vorschriften bei der Nutzung AWS-Services hängt von der Vertraulichkeit Ihrer Daten, den Compliance-Zielen Ihres Unternehmens und den geltenden Gesetzen und Vorschriften ab. AWS stellt die folgenden Ressourcen zur Verfügung, die Sie bei der Einhaltung der Vorschriften unterstützen:

- Compliance und Governance im Bereich Sicherheit – In diesen Anleitungen für die Lösungsimplementierung werden Überlegungen zur Architektur behandelt. Außerdem werden Schritte für die Bereitstellung von Sicherheits- und Compliance-Features beschrieben.
- Referenz für berechtigte HIPAA-Services – Listet berechtigte HIPAA-Services auf. Nicht alle AWS-Services sind HIPAA-fähig.
- AWS Compliance-Ressourcen — Diese Sammlung von Arbeitsmappen und Leitfäden gilt möglicherweise für Ihre Branche und Ihren Standort.
- AWS Leitfäden zur Einhaltung von Vorschriften für Kunden — Verstehen Sie das Modell der gemeinsamen Verantwortung aus dem Blickwinkel der Einhaltung von Vorschriften. In den Leitfäden werden die bewährten Verfahren zur Sicherung zusammengefasst AWS-Services und die Leitlinien den Sicherheitskontrollen in verschiedenen Frameworks (einschließlich des National Institute of Standards and Technology (NIST), des Payment Card Industry Security Standards Council (PCI) und der International Organization for Standardization (ISO)) zugeordnet.
- Evaluierung von Ressourcen anhand von Regeln im AWS Config Entwicklerhandbuch — Der AWS Config Service bewertet, wie gut Ihre Ressourcenkonfigurationen den internen Praktiken, Branchenrichtlinien und Vorschriften entsprechen.
- AWS Security Hub— Auf diese AWS-Service Weise erhalten Sie einen umfassenden Überblick über Ihren internen Sicherheitsstatus. AWS Security Hub verwendet Sicherheitskontrollen, um Ihre AWS -Ressourcen zu bewerten und Ihre Einhaltung von Sicherheitsstandards und bewährten Methoden zu überprüfen. Die Liste der unterstützten Services und Kontrollen finden Sie in der Security-Hub-Steuerelementreferenz.

- Amazon GuardDuty — Dies AWS-Service erkennt potenzielle Bedrohungen für Ihre Workloads AWS-Konten, Container und Daten, indem es Ihre Umgebung auf verdächtige und böswillige Aktivitäten überwacht. GuardDuty kann Ihnen helfen, verschiedene Compliance-Anforderungen wie PCI DSS zu erfüllen, indem es die in bestimmten Compliance-Frameworks vorgeschriebenen Anforderungen zur Erkennung von Eindringlingen erfüllt.
- AWS Audit Manager— Auf diese AWS-Service Weise können Sie Ihre AWS Nutzung kontinuierlich überprüfen, um das Risikomanagement und die Einhaltung von Vorschriften und Industriestandards zu vereinfachen.

# Internetzugang für AWS Outposts Workloads

In diesem Abschnitt wird erklärt, wie AWS Outposts Workloads auf folgende Weise auf das Internet zugreifen können:

- Durch die übergeordnete Region AWS
- Über das Netzwerk Ihres lokalen Rechenzentrums

## Internetzugang über die übergeordnete AWS Region

Bei dieser Option greifen die Workloads in den Outposts über den Service Link und dann über das Internet-Gateway (IGW) in der übergeordneten Region auf das Internet zu. AWS Der ausgehende Datenverkehr zum Internet kann über das in Ihrer VPC instanziierte NAT-Gateway erfolgen. Für zusätzliche Sicherheit für Ihren eingehenden und ausgehenden Datenverkehr können Sie AWS Sicherheitsdienste wie AWS WAF AWS Shield, und Amazon CloudFront in der AWS Region verwenden.

Informationen zur Einstellung der Routentabelle im Outposts-Subnetz finden Sie unter Routentabellen für lokale Gateways.

### Überlegungen

- Verwenden Sie diese Option, wenn:
  - Sie benötigen Flexibilität bei der Sicherung des Internetverkehrs mit mehreren AWS Diensten in der AWS Region.
  - Sie verfügen in Ihrem Rechenzentrum oder Ihrer Colocation-Einrichtung nicht über einen Internet-Präsenzpunkt.

- Bei dieser Option muss der Datenverkehr die übergeordnete AWS Region durchqueren, was zu Latenz führt.
- Ähnlich wie bei Datenübertragungsgebühren in AWS Regionen fallen für die Datenübertragung von der übergeordneten Availability Zone zum Outpost Gebühren an. Weitere Informationen zur Datenübertragung finden Sie unter Amazon EC2 On-Demand-Preise.
- Die Auslastung der Service Link-Bandbreite wird zunehmen.

Die folgende Abbildung zeigt den Datenverkehr zwischen dem Workload in der Outposts-Instance und dem Internet, der durch die übergeordnete AWS Region fließt.

## Internetzugang über das Netzwerk Ihres lokalen Rechenzentrums

Bei dieser Option greifen die Workloads in den Outposts über Ihr lokales Rechenzentrum auf das Internet zu. Der Workload-Verkehr, der auf das Internet zugreift, durchläuft Ihren lokalen Internet-Präsenzpunkt und geht lokal aus. Die Sicherheitsebene des Netzwerks Ihres lokalen Rechenzentrums ist für die Sicherung des Workload-Datenverkehrs von Outposts verantwortlich.

Informationen zur Einstellung der Routentabelle im Outposts-Subnetz finden Sie unter Routentabellen für lokale Gateways.

### Überlegungen

- Verwenden Sie diese Option, wenn:
  - Ihre Workloads erfordern einen Zugriff auf Internetdienste mit geringer Latenz.
  - Sie möchten vermeiden, dass Gebühren für ausgehende Datenübertragungen (DTO) anfallen.
  - Sie möchten die Service Link-Bandbreite für den Verkehr auf der Kontrollebene beibehalten.
- Ihre Sicherheitsebene ist für die Sicherung des Workload-Verkehrs von Outposts verantwortlich.
- Wenn Sie sich für Direct VPC Routing (DVR) entscheiden, müssen Sie sicherstellen, dass die Outposts CIDRs nicht mit den lokalen in Konflikt geraten. CIDRs
- Wenn die Standardroute (0/0) über das lokale Gateway (LGW) weitergegeben wird, können Instances möglicherweise nicht zu den Service-Endpunkten gelangen. Alternativ können Sie VPC-Endpunkte auswählen, um den gewünschten Service zu erreichen.

Die folgende Abbildung zeigt den Datenverkehr zwischen dem Workload in der Outposts-Instanz und dem Internet, der über Ihr lokales Rechenzentrum fließt.

AWS Outposts lässt sich in die folgenden Dienste integrieren, die Überwachungs- und Protokollierungsfunktionen bieten:

CloudWatch Metriken

Verwenden Sie Amazon CloudWatch , um Statistiken über Datenpunkte für Ihren  als geordneten Satz von Zeitreihendaten abzurufen, die als Metriken bezeichnet werden. Mit diesen Metriken können Sie überprüfen, ob Ihr System die erwartete Leistung zeigt. Weitere Informationen finden Sie unter CloudWatch .

CloudTrail Logs

Wird verwendet AWS CloudTrail , um detaillierte Informationen über die Anrufe zu erfassen AWS APIs. Sie können diese Aufrufe als Protokolldateien in Amazon S3 speichern. Anhand dieser CloudTrail Protokolle können Sie beispielsweise ermitteln, welcher Anruf getätigt wurde, von welcher Quell-IP-Adresse der Anruf kam, wer den Anruf getätigt hat und wann der Anruf getätigt wurde.

Die CloudTrail Protokolle enthalten Informationen über die Aufrufe von API-Aktionen für AWS Outposts. Sie enthalten auch Informationen für Aufrufe von API-Aktionen von Diensten auf einem Outpost wie Amazon EC2 und Amazon EBS. Weitere Informationen finden Sie unter API-Aufrufe protokollieren mit CloudTrail.

VPC-Flow-Protokolle

Verwenden Sie VPC Flow Logs, um detaillierte Informationen über den Datenverkehr zu und von Ihrem Outpost und innerhalb Ihres Outposts zu erfassen. Weitere Informationen finden Sie unter VPC-Flow-Protokolle im Amazon-VPC-Benutzerhandbuch.

Datenverkehrsspiegelung

Verwenden Sie Traffic Mirroring, um Netzwerkverkehr von Ihrem  zu kopieren und an out-of-band Sicherheits- und Überwachungsgeräte weiterzuleiten. Sie können den gespiegelten Datenverkehr zur Inhaltsinspektion, Bedrohungsüberwachung oder Fehlerbehebung verwenden. Weitere Informationen finden Sie im Amazon VPC Traffic Mirroring Guide.

AWS Health Dashboard

AWS Health Dashboard Zeigt Informationen und Benachrichtigungen an, die durch Änderungen im Zustand der AWS Ressourcen ausgelöst werden. Diese Informationen werden auf zweierlei Weise dargestellt: in einem Dashboard, das kürzliche und kommende Ereignisse nach Kategorie

sortiert anzeigt, und in einem vollständigen Ereignisprotokoll, das alle Ereignisse der letzten 90 Tage enthält. Beispielsweise würde ein Verbindungsproblem mit dem Service-Link ein Ereignis auslösen, das im Dashboard und im Ereignisprotokoll erscheint und 90 Tage lang im Ereignisprotokoll verbleibt. Ein Teil des AWS Health Dienstes AWS Health Dashboard erfordert keine Einrichtung und kann von jedem Benutzer eingesehen werden, der in Ihrem Konto authentifiziert ist. Weitere Informationen finden Sie unter Erste Schritte mit AWS Health Dashboard.

# CloudWatch

AWS Outposts veröffentlicht Datenpunkte CloudWatch für Ihre Outposts auf Amazon. CloudWatch ermöglicht es Ihnen, Statistiken über diese Datenpunkte in Form eines geordneten Satzes von Zeitreihendaten, sogenannten Metriken, abzurufen. Sie können sich eine Metrik als eine zu überwachende Variable und die Datenpunkte als die Werte dieser Variable im Laufe der Zeit vorstellen. Sie können z. B. die Instance-Kapazität überwachen, die Ihrem Outpost für einen angegebenen Zeitraum zur Verfügung steht. Jeder Datenpunkt verfügt über einen zugewiesenen Zeitstempel und eine optionale Maßeinheit.

Mit den Metriken können Sie überprüfen, ob Ihr System die erwartete Leistung zeigt. Sie können beispielsweise einen CloudWatch Alarm erstellen, um die `ConnectedStatus` Metrik zu überwachen. Wenn die durchschnittliche Metrik niedriger als ist1, CloudWatch kann eine Aktion eingeleitet werden, z. B. das Senden einer Benachrichtigung an eine E-Mail-Adresse. Anschließend können Sie mögliche Netzwerkprobleme On-Premises oder im Uplink-Netzwerk untersuchen, die sich auf den Betrieb Ihres Outposts auswirken könnten. Zu den häufigsten Problemen gehören kürzlich vorgenommene Änderungen der On-Premises-Netzwerkkonfiguration an den Firewall- und NAT-Regeln oder Probleme mit der Internetverbindung. Bei `ConnectedStatus` Problemen empfehlen wir, die Konnektivität mit der AWS Region von Ihrem lokalen Netzwerk aus zu überprüfen und sich an den AWS Support zu wenden, falls das Problem weiterhin besteht.

Weitere Informationen zum Erstellen eines CloudWatch Alarms finden Sie unter Verwenden von Amazon CloudWatch Alarms im CloudWatch Amazon-Benutzerhandbuch. Weitere Informationen zu CloudWatch finden Sie im CloudWatch Amazon-Benutzerhandbuch.

Inhalt

# Metriken

Der `AWS/Outposts`-Namespace enthält die folgenden Metriken.

`ConnectedStatus`

Der Status der Service-Link-Verbindung eines Outposts. Liegt die durchschnittliche Statistik unter dem Wert 1, ist die Verbindung beeinträchtigt.

Einheit: Anzahl

Maximale Auflösung: 1 Minute

Statistiken: Die nützlichste Statistik ist `Average`.

Dimensionen: `OutpostId`

`CapacityExceptions`

Die Anzahl der Fehler mit unzureichender Kapazität bei Instance-Starts.

Einheit: Anzahl

Maximale Auflösung: 5 Minuten

Statistiken: Die nützlichsten Statistiken sind `Maximum` und `Minimum`.

Dimensionen: `InstanceType` und `OutpostId`

`IfTrafficIn`

Die Bitrate der Daten, die die Outposts Virtual Interfaces (VIFs) von den verbundenen lokalen Netzwerkgeräten empfangen.

Einheit: Bits pro Sekunde

Maximale Auflösung: 5 Minuten

Statistiken: Die nützlichsten Statistiken sind `Max` und `Min`.

Abmessungen für das lokale Gateway VIFs (lgw-vif):, und `OutpostsId` `VirtualInterfaceGroupId` `VirtualInterfaceId`

Abmessungen für Service Link VIFs (sl-vif): und `OutpostsId` `VirtualInterfaceId`

`IfTrafficOut`

Die Bitrate der Daten, die die Outposts Virtual Interfaces (VIFs) an die verbundenen lokalen Netzwerkgeräte übertragen.

Einheit: Bits pro Sekunde

Maximale Auflösung: 5 Minuten

Statistiken: Die nützlichsten Statistiken sind `Max` und `Min`.

Abmessungen für das lokale Gateway VIFs (lgw-vif):, und `OutpostsId` `VirtualInterfaceGroupId` `VirtualInterfaceId`

Abmessungen für Service Link VIFs (sl-vif): und `OutpostsId` `VirtualInterfaceId`

`InstanceFamilyCapacityAvailability`

Der Prozentsatz der verfügbaren Instance-Kapazität. Diese Metrik beinhaltet keine Kapazität für Dedicated Hosts, die auf dem Outpost konfiguriert sind.

Einheit: Prozent

Maximale Auflösung: 5 Minuten

Statistiken: Die nützlichsten Statistiken sind `Average` und `pNN.NN` (Perzentile).

Dimensionen: `InstanceFamily` und `OutpostId`

`InstanceFamilyCapacityUtilization`

Der Prozentsatz der verfügbaren Instance-Kapazität. Diese Metrik beinhaltet keine Kapazität für Dedicated Hosts, die auf dem Outpost konfiguriert sind.

Einheit: Prozent

Maximale Auflösung: 5 Minuten

Statistiken: Die nützlichsten Statistiken sind `Average` und `pNN.NN` (Perzentile).

Dimensionen: `Account`, `InstanceFamily` und `OutpostId`

`InstanceTypeCapacityAvailability`

Der Prozentsatz der verfügbaren Instance-Kapazität. Diese Metrik beinhaltet keine Kapazität für Dedicated Hosts, die auf dem Outpost konfiguriert sind.

Einheit: Prozent

Maximale Auflösung: 5 Minuten

Statistiken: Die nützlichsten Statistiken sind `Average` und `pNN.NN` (Perzentile).

Dimensionen: `InstanceType` und `OutpostId`

`InstanceTypeCapacityUtilization`

Der Prozentsatz der verfügbaren Instance-Kapazität. Diese Metrik beinhaltet keine Kapazität für Dedicated Hosts, die auf dem Outpost konfiguriert sind.

Einheit: Prozent

Maximale Auflösung: 5 Minuten

Statistiken: Die nützlichsten Statistiken sind `Average` und `pNN.NN` (Perzentile).

Dimensionen: `Account`, `InstanceType` und `OutpostId`

`UsedInstanceType_Count`

Die Anzahl der Instance-Typen, die derzeit verwendet werden, einschließlich aller Instance-Typen, die von Managed Services wie Amazon Relational Database Service (Amazon RDS) oder Application Load Balancer verwendet werden. Diese Metrik beinhaltet keine Kapazität für Dedicated Hosts, die auf dem Outpost konfiguriert sind.

Einheit: Anzahl

Maximale Auflösung: 5 Minuten

Dimensionen: `Account`, `InstanceType` und `OutpostId`

`AvailableInstanceType_Count`

Anzahl der verfügbaren Instance-Typen. Diese Metrik beinhaltet die Anzahl. `AvailableReservedInstances`

Um die Anzahl der Instanzen zu ermitteln, die Sie reservieren können, ziehen Sie die `AvailableReservedInstances` Anzahl von der `AvailableInstanceType_Count` Anzahl ab.

```
Number of instances that you can reserve = AvailableInstanceType_Count
 - AvailableReservedInstances
```

Diese Metrik beinhaltet keine Kapazität für Dedicated Hosts, die auf dem Outpost konfiguriert sind.

Einheit: Anzahl

Maximale Auflösung: 5 Minuten

Dimensionen: `InstanceType` und `OutpostId`

`AvailableReservedInstances`

Die Anzahl der Instances, die für den Start in die Rechenkapazität verfügbar sind, die mithilfe von Capacity Reservations reserviert wurde.

Diese Metrik beinhaltet keine Amazon EC2 Reserved Instances.

Diese Metrik beinhaltet nicht die Anzahl der Instances, die Sie reservieren können. Um zu bestimmen, wie viele Instances Sie reservieren können, subtrahieren Sie die `AvailableReservedInstances` Anzahl von der `AvailableInstanceType_Count` Anzahl.

```
Number of instances that you can reserve = AvailableInstanceType_Count
 - AvailableReservedInstances
```

Einheit: Anzahl

Maximale Auflösung: 5 Minuten

Dimensionen: `InstanceType` und `OutpostId`

`UsedReservedInstances`

Die Anzahl der Instances, die in der Rechenkapazität ausgeführt werden, die mithilfe von Kapazitätsreservierungen reserviert wurde. Diese Metrik beinhaltet keine Amazon EC2 Reserved Instances.

Einheit: Anzahl

Maximale Auflösung: 5 Minuten

Dimensionen: `InstanceType` und `OutpostId`

`TotalReservedInstances`

Die Gesamtzahl der Instances, die ausgeführt werden und für den Start verfügbar sind, ergibt sich aus der Rechenkapazität, die über Capacity Reservations reserviert wurde. Diese Metrik beinhaltet keine Amazon EC2 Reserved Instances.

Einheit: Anzahl

Maximale Auflösung: 5 Minuten

Dimensionen: `InstanceType` und `OutpostId`

`EBSVolumeTypeCapacityUtilization`

Der Prozentsatz der genutzten EBS-Volumenkapazität.

Einheit: Prozent

Maximale Auflösung: 5 Minuten

Statistiken: Die nützlichsten Statistiken sind `Average` und `pNN.NN` (Perzentile).

Dimensionen: `VolumeType` und `OutpostId`

`EBSVolumeTypeCapacityAvailability`

Der Prozentsatz der genutzten EBS-Volumenkapazität.

Einheit: Prozent

Maximale Auflösung: 5 Minuten

Statistiken: Die nützlichsten Statistiken sind `Average` und `pNN.NN` (Perzentile).

Dimensionen: `VolumeType` und `OutpostId`

`EBSVolumeTypeCapacityUtilizationGB`

Die Anzahl der für den EBS-Volumentyp verwendeten Gigabyte.

Einheit: Gigabyte

Maximale Auflösung: 5 Minuten

Statistiken: Die nützlichsten Statistiken sind `Average` und `pNN.NN` (Perzentile).

Dimensionen: `VolumeType` und `OutpostId`

`EBSVolumeTypeCapacityAvailabilityGB`

Die Anzahl der Gigabyte verfügbarer Kapazität für den EBS-Volumentyp.

Einheit: Gigabyte

Maximale Auflösung: 5 Minuten

Statistiken: Die nützlichsten Statistiken sind `Average` und `pNN.NN` (Perzentile).

Dimensionen: `VolumeType` und `OutpostId`

## Metrikdimensionen

Verwenden Sie Ihren Outpost, um die Metriken für Ihre zu filtern.

| Dimension | Beschreibung |
|---|---|
| `Account` | Das Konto oder der Dienst, der die Kapazität verwendet. |
| `InstanceFamily` | Die Instance-Familie. |
| `InstanceType` | Der Instance-Typ. |
| `OutpostId` | Die ID des Outpost. |
| `VolumeType` | Der EBS-Volume-Typ. |
| `VirtualInterfaceId` | Die ID des virtuellen Gateways oder des Service Link Virtual Interface (VIF). |
| `VirtualInterfaceGroupId` | Die ID der virtuellen Schnittstellengruppe für das virtuelle Interface (VIF) des lokalen Gateways. |

## CloudWatch

Sie können die CloudWatch Metriken für Ihren  mit der CloudWatch Konsole anzeigen.

Um Metriken mit der CloudWatch Konsole anzuzeigen

1. Öffnen Sie die CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Wählen Sie im Navigationsbereich Metriken aus.
3. Wählen Sie den Namespace des Outposts aus.

4. (Optional) Um eine Metrik in allen Dimensionen anzuzeigen, geben Sie den Namen in das Suchfeld ein.

Um Metriken mit dem anzuzeigen AWS CLI

Verwenden Sie den folgenden list-metrics-Befehl, um die verfügbaren Metriken aufzuführen.

```
aws cloudwatch list-metrics --namespace AWS/Outposts
```

Um die Statistiken für eine Metrik abzurufen, verwenden Sie AWS CLI

Verwenden Sie den folgenden get-metric-statisticsBefehl, um Statistiken für die angegebene Metrik und Dimension abzurufen. CloudWatch behandelt jede eindeutige Kombination von Dimensionen als separate Metrik. Sie können keine Statistiken abrufen, die Kombinationen von Dimensionen verwenden, die nicht speziell veröffentlicht wurden. Sie müssen die gleichen Dimensionen angeben, die bei der Erstellung der Metriken verwendet wurden.

```
aws cloudwatch get-metric-statistics \
--namespace AWS/Outposts --metric-name InstanceTypeCapacityUtilization \
--statistics Average --period 3600 \
--dimensions Name=OutpostId,Value=op-01234567890abcdef
 Name=InstanceType,Value=c5.xlarge \
--start-time 2019-12-01T00:00:00Z --end-time 2019-12-08T00:00:00Z
```

# Protokollieren Sie AWS Outposts API-Aufrufe mit AWS CloudTrail

AWS Outposts ist in einen Dienst integriert AWS CloudTrail, der eine Aufzeichnung der von einem Benutzer, einer Rolle oder einem AWS Dienst ausgeführten Aktionen bereitstellt. CloudTrail erfasst API-Aufrufe AWS Outposts als Ereignisse. Zu den erfassten Aufrufen gehören Aufrufe von der AWS Outposts Konsole und Codeaufrufen für die AWS Outposts API-Operationen. Anhand der von gesammelten Informationen können Sie die Anfrage CloudTrail, an die die Anfrage gestellt wurde AWS Outposts, die IP-Adresse, von der aus die Anfrage gestellt wurde, den Zeitpunkt der Anfrage und weitere Details ermitteln.

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Die Identitätsinformationen unterstützen Sie bei der Ermittlung der folgenden Punkte:

- Ob die Anfrage mit Anmeldeinformationen des Root-Benutzers oder des Benutzers gestellt wurde.

- Die Anforderung wurde im Namen eines IAM-Identity-Center-Benutzers erstellt.
- Gibt an, ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen Verbundbenutzer gesendet wurde.
- Ob die Anforderung aus einem anderen AWS-Service gesendet wurde.

CloudTrail ist in Ihrem AWS Konto aktiv, wenn Sie das Konto erstellen, und Sie haben automatisch Zugriff auf den CloudTrail Eventverlauf. Der CloudTrail Ereignisverlauf bietet eine einsehbare, durchsuchbare, herunterladbare und unveränderliche Aufzeichnung der aufgezeichneten Verwaltungsereignisse der letzten 90 Tage in einem. AWS-Region Weitere Informationen finden Sie im AWS CloudTrail Benutzerhandbuch unter Arbeiten mit dem CloudTrail Ereignisverlauf. Für die Anzeige des Eventverlaufs CloudTrail  fallen keine Gebühren an.

Für eine fortlaufende Aufzeichnung der Ereignisse in AWS-Konto den letzten 90 Tagen erstellen Sie einen Trail- oder CloudTrail Lake-Event-Datenspeicher.

CloudTrail Pfade

Ein Trail ermöglicht CloudTrail die Übermittlung von Protokolldateien an einen Amazon S3 S3-Bucket. Alle mit dem erstellten Pfade AWS Management Console sind regionsübergreifend. Sie können mithilfe von AWS CLI einen Einzel-Region- oder einen Multi-Region-Trail erstellen. Es wird empfohlen, einen Trail mit mehreren Regionen zu erstellen, da Sie alle Aktivitäten AWS-Regionen in Ihrem Konto erfassen. Wenn Sie einen Einzel-Region-Trail erstellen, können Sie nur die Ereignisse anzeigen, die im AWS-Region des Trails protokolliert wurden. Weitere Informationen zu Trails finden Sie unter Erstellen eines Trails für Ihr AWS-Konto und Erstellen eines Trails für eine Organisation im AWS CloudTrail -Benutzerhandbuch.

Sie können eine Kopie Ihrer laufenden Verwaltungsereignisse kostenlos an Ihren Amazon S3 S3-Bucket senden, CloudTrail indem Sie einen Trail erstellen. Es fallen jedoch Amazon S3 S3-Speichergebühren an. Weitere Informationen zur CloudTrail Preisgestaltung finden Sie unter AWS CloudTrail Preise. Informationen zu Amazon-S3-Preisen finden Sie unter Amazon S3 – Preise.

CloudTrail Datenspeicher für Ereignisse in Lake

CloudTrail Mit Lake können Sie SQL-basierte Abfragen für Ihre Ereignisse ausführen. CloudTrail Lake konvertiert bestehende Ereignisse im zeilenbasierten JSON-Format in das Apache ORC-Format. ORC ist ein spaltenförmiges Speicherformat, das für den schnellen Abruf von Daten optimiert ist. Die Ereignisse werden in Ereignisdatenspeichern zusammengefasst, bei denen es sich um unveränderliche Sammlungen von Ereignissen handelt, die auf Kriterien basieren, die Sie mit Hilfe von erweiterten Ereignisselektoren auswählen. Die Selektoren, die Sie auf einen

Ereignisdatenspeicher anwenden, steuern, welche Ereignisse bestehen bleiben und für Sie zur Abfrage verfügbar sind. Weitere Informationen zu CloudTrail Lake finden Sie unter Arbeiten mit AWS CloudTrail Lake im AWS CloudTrail Benutzerhandbuch.

CloudTrail Für das Speichern und Abfragen von Ereignisdaten in Lake fallen Kosten an. Beim Erstellen eines Ereignisdatenspeichers wählen Sie die Preisoption aus, die für den Ereignisdatenspeicher genutzt werden soll. Die Preisoption bestimmt die Kosten für die Erfassung und Speicherung von Ereignissen sowie die standardmäßige und maximale Aufbewahrungsdauer für den Ereignisdatenspeicher. Weitere Informationen zur CloudTrail Preisgestaltung finden Sie unter AWS CloudTrail Preise.

## AWS Outposts Management-Ereignisse in CloudTrail

Verwaltungsereignisse bieten Informationen über Verwaltungsvorgänge, die an Ressourcen in Ihrem ausgeführt werden AWS-Konto. Sie werden auch als Vorgänge auf Steuerebene bezeichnet. CloudTrail Protokolliert standardmäßig Verwaltungsereignisse.

AWS Outposts protokolliert alle Operationen auf der Kontrollebene AWS von Outposts als Managementereignisse. Eine Liste der Operationen auf der AWS Outposts-Kontrollebene, die AWS Outposts protokolliert CloudTrail, finden Sie in der AWS Outposts API-Referenz.

## AWS Outposts Beispiele für Ereignisse

Das folgende Beispiel zeigt ein CloudTrail Ereignis, das den `SetSiteAddress` Vorgang demonstriert.


```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AKIAIOSFODNN7EXAMPLE:jdoe",
        "arn": "arn:aws:sts::111122223333:assumed-role/example/jdoe",
        "accountId": "111122223333",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AKIAIOSFODNN7EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/example",
                "accountId": "111122223333",
```

```
                "userName": "example"
            },
            "webIdFederationData": {},
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2020-08-14T16:28:16Z"
            }
        }
    },
    "eventTime": "2020-08-14T16:32:23Z",
    "eventSource": "outposts.amazonaws.com",
    "eventName": "SetSiteAddress",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "XXX.XXX.XXX.XXX",
    "userAgent": "userAgent",
    "requestParameters": {
        "SiteId": "os-123ab4c56789de01f",
        "Address": "***"
    },
    "responseElements": {
        "Address": "***",
        "SiteId": "os-123ab4c56789de01f"
    },
    "requestID": "1abcd23e-f4gh-567j-klm8-9np01q234r56",
    "eventID": "1234a56b-c78d-9e0f-g1h2-34jk56m7n890",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
```

# Wartung von Outposts

Im Rahmen des Modells der AWS ist die für die Hardware und Software verantwortlich, mit der AWS Dienste ausgeführt werden. Das gilt für AWS Outposts, genau wie für eine AWS Region. AWS Verwaltet beispielsweise Sicherheitspatches, aktualisiert Firmware und wartet die Outpost-Geräte. AWS überwacht auch die Leistung, den Zustand und die Messwerte für Ihren  und stellt fest, ob Wartungsarbeiten erforderlich sind.

> **Warning**
>
> Daten auf Instance-Speicher-Volumes gehen verloren, wenn das zugrunde liegende Festplattenlaufwerk ausfällt oder wenn die Instance angehalten, in den Ruhezustand versetzt oder beendet wird. Um Datenverlust zu vermeiden, empfehlen wir Ihnen, Ihre langfristigen Daten auf Instance-Speicher-Volumes in einem persistenten Speicher zu sichern, z. B. in einem Amazon S3-Bucket, einem Amazon EBS-Volume oder einem Netzwerkspeichergerät in Ihrem On-Premises-Netzwerk.

Inhalt



## Kontaktdetails aktualisieren

Wenn der Outpost-Besitzer wechselt, wenden Sie sich mit dem Namen und den Kontaktinformationen des neuen Besitzers an AWS -Support Center.

## Hardware-Wartung

Wenn während der Serverbereitstellung oder beim Hosten von EC2 Amazon-Instances, die auf Ihrem laufen, ein irreparables Hardwareproblem AWS festgestellt wird, werden wir den Outpost-Eigentümer

und den Eigentümer der Instances darüber informieren, dass die betroffenen Instances stillgelegt werden sollen. Weitere Informationen finden Sie unter Instance Retirement im  EC2 Amazon-Benutzerhandbuch.

Der Outpost-Besitzer und der Instance-Besitzer können zusammenarbeiten, um das Problem zu lösen. Der Instance-Besitzer kann eine betroffene Instance stoppen und starten, um sie auf die verfügbare Kapazität zu migrieren. Instance-Besitzer können die betroffenen Instances zu einem für sie passenden Zeitpunkt beenden und starten. Andernfalls werden die betroffenen Instances am Tag der Außerbetriebnahme der Instance AWS gestoppt und gestartet. Wenn auf dem Outpost keine zusätzliche Kapazität vorhanden ist, verbleibt die Instance im Status „Gestoppt“. Der Outpost-Besitzer kann versuchen, genutzte Kapazität freizugeben oder zusätzliche Kapazität für den Outpost anfordern, damit die Migration abgeschlossen werden kann.

Falls eine Hardwarewartung erforderlich ist, AWS wird der Outpost-Besitzer kontaktiert, um Datum und Uhrzeit für den Besuch des AWS Installationsteams zu bestätigen. Besuche können bereits zwei Werktage nach dem Zeitpunkt, an dem der Outpost-Besitzer mit dem AWS Team gesprochen hat, geplant werden.

Wenn das AWS Installationsteam vor Ort eintrifft, tauscht es die fehlerhaften Hosts, Switches oder Rackelemente aus und stellt die neue Kapazität wieder in Betrieb. Installationsteam führt vor Ort keine Hardwarediagnosen oder Reparaturen durch. Wenn das Installationsteam einen Host austauscht, entfernt und vernichtet es den NIST-konformen physischen Sicherheitsschlüssel, wodurch alle Daten, die möglicherweise auf der Hardware verbleiben, vernichtet werden. Dadurch wird sichergestellt, dass keine Daten Ihren Standort verlassen. Wenn das Installationsteam ein Outpost-Netzwerkgerät ersetzt, sind möglicherweise Netzwerkkonfigurationsinformationen auf dem Gerät vorhanden, wenn es vom Standort entfernt wird. Diese Informationen können IP-Adressen beinhalten und ASNs zur Einrichtung virtueller Schnittstellen für die Konfiguration des Pfads zu Ihrem lokalen Netzwerk oder zurück zur Region verwendet werden.

## Firmware-Updates

Die Aktualisierung der Outpost-Firmware hat normalerweise keine Auswirkungen auf die Instances auf Ihrem Outpost. In dem seltenen Fall, dass wir die Outpost-Geräte neu starten müssen, um ein Update zu installieren, erhalten Sie für alle Instances, die mit dieser Kapazität laufen, eine Benachrichtigung über die Außerbetriebnahme der Instance.

# Wartung der Netzwerkausrüstung

Die Wartung der Outpost Networking Devices (OND) erfolgt ohne Beeinträchtigung des regulären Betriebs und des Datenverkehrs des Outpost. Wenn Wartungsarbeiten erforderlich sind, wird der Datenverkehr vom OND weggeleitet. Möglicherweise bemerken Sie vorübergehende Änderungen in den BGP-Ankündigungen, wie z. B. das Voranstellen von AS-Pfaden, und entsprechende Änderungen der Datenverkehrsmuster auf Outpost-Uplinks. Bei OND-Firmware-Updates bemerken Sie möglicherweise ein Flattern von BGP.

Wir empfehlen Ihnen, die Kunden-Netzwerkgeräte so zu konfigurieren, dass sie BGP-Ankündigungen von Outposts empfangen, ohne die BGP-Attribute zu ändern, und BGP-Multipath/Load Balancing zu aktivieren, um optimale eingehende Datenströme zu erreichen. AS-Path-Präfixe werden für lokale Gateway-Präfixe verwendet, um den Datenverkehr zu verlagern, ONDs falls Wartungsarbeiten erforderlich sind. Das Kundennetzwerk sollte Routen von Outposts mit einer AS-Pfadlänge von 1 gegenüber Routen mit einer AS-Pfadlänge von 4 bevorzugen.

Das Kundennetzwerk sollte für alle gleiche BGP-Präfixe mit denselben Attributen werben. ONDs Das Outpost-Netzwerk verteilt standardmäßig ausgehenden Datenverkehr zwischen allen Uplinks. Routing-Richtlinien werden auf der Outpost-Seite verwendet, um den Datenverkehr von einem OND wegzuverlagern, falls Wartungsarbeiten erforderlich sind. Diese Verkehrsverlagerung erfordert für alle Kunden gleiche BGP-Präfixe. ONDs Wenn im Kundennetzwerk Wartungsarbeiten erforderlich sind, empfehlen wir Ihnen, AS-Path Prepending zu verwenden, um den Datenverkehr vorübergehend von bestimmten Uplinks zu verlagern.

# Bewährte Methoden für -Strom- und Netzwerkereignisse

Wie in den AWS Servicebedingungen für AWS Outposts Kunden angegeben, muss die Einrichtung, in der sich die Outposts-Ausrüstung befindet, die Mindestanforderungen an Strom und Netzwerk erfüllen, um die Installation, Wartung und Nutzung der Outposts-Ausrüstung zu unterstützen. Ein  kann nur dann ordnungsgemäß funktionieren, wenn Strom und Netzwerkkonnektivität unterbrechungsfrei sind.

## Stromereignisse

Bei vollständigen Stromausfällen besteht das inhärente Risiko, dass eine AWS Outposts Ressource nicht automatisch wieder in Betrieb genommen wird. Zusätzlich zur Bereitstellung redundanter Stromversorgungs- und Notstromversorgungslösungen empfehlen wir, dass Sie im Voraus Folgendes tun, um die Auswirkungen einiger der schlimmsten Szenarien zu minimieren:

- Verschieben Sie Ihre Services und Anwendungen kontrolliert von den Outposts-Geräten, indem Sie DNS-basierte oder Off-Rack-Load-Balancing-Änderungen verwenden.
- Stoppen Sie Container, Instances und Datenbanken in einer inkrementellen Reihenfolge und verwenden Sie bei der Wiederherstellung die umgekehrte Reihenfolge.
- Testpläne für das kontrollierte Verschieben oder Stoppen von Diensten.
- Sichern Sie wichtige Daten und Konfigurationen und speichern Sie sie außerhalb der Outposts.
- Beschränken Sie Stromausfallzeiten auf ein Minimum.
- Vermeiden Sie ein wiederholtes Umschalten der Stromversorgungen (off-on-off-on) während der Wartung.
- Planen Sie innerhalb des Wartungszeitfensters zusätzliche Zeit ein, um unvorhergesehene Ereignisse zu beheben.
- Steuern Sie die Erwartungen Ihrer Benutzer und Kunden, indem Sie ein größeres Zeitfenster für die Wartung angeben, als Sie normalerweise benötigen würden.
- Erstellen Sie nach der Wiederherstellung der Stromversorgung einen Fall im AWS -Support Center, um zu überprüfen, AWS Outposts ob und die zugehörigen Dienste ausgeführt werden.

## Netzwerkkonnektivitätsereignisse

Die Service Link-Verbindung zwischen Ihrem Outpost und der AWS Region oder der Heimatregion von Outposts wird in der Regel automatisch nach Netzwerkunterbrechungen oder Problemen wiederhergestellt, die in Ihren vorgelagerten Unternehmensnetzwerkgeräten oder im Netzwerk eines Drittanbieters auftreten können, sobald die Netzwerkwartung abgeschlossen ist. Während der Zeit, in der die Service-Link-Verbindung unterbrochen ist, ist der Betrieb Ihrer Outposts auf lokale Netzwerkaktivitäten beschränkt.

EC2 Amazon-Instances, Local Gateway und Amazon EBS-Volumes auf den Outposts funktionieren weiterhin normal und können lokal über das lokale Netzwerk abgerufen werden. In ähnlicher Weise werden AWS Serviceressourcen wie Amazon ECS-Worker-Knoten weiterhin lokal ausgeführt. Die API-Verfügbarkeit wird jedoch beeinträchtigt. Beispielsweise funktionieren Ausführen, Starten, Stoppen und Beenden APIs möglicherweise nicht. Instance-Metriken und Logs werden weiterhin bis zu 7 Tage lang lokal zwischengespeichert und in die AWS Region übertragen, sobald die Konnektivität wieder hergestellt ist. Eine Verbindungsunterbrechung nach mehr als 7 Tagen kann zum Verlust von Metriken und Protokollen führen.

Weitere Informationen finden Sie in der Frage Was passiert, wenn die Netzwerkverbindung meiner Einrichtung unterbrochen wird? auf der AWS Outposts FAQsRack-Seite.

Wenn die Serviceverbindung aufgrund eines Stromausfalls vor Ort oder aufgrund eines Verlusts der Netzwerkverbindung nicht verfügbar ist, AWS Health Dashboard sendet der eine Benachrichtigung an das Konto, dem die Outposts gehören. Weder Sie noch Sie AWS können die Benachrichtigung über eine Unterbrechung der Verbindung unterdrücken, selbst wenn die Unterbrechung zu erwarten ist. Weitere Informationen finden Sie unter Erste Schritte mit dem AWS Health Dashboard im AWS Health -Benutzerhandbuch.

Ergreifen Sie im Falle einer geplanten Servicewartung, die sich auf die Netzwerkkonnektivität auswirkt, die folgenden proaktiven Maßnahmen, um die Auswirkungen potenzieller Problemszenarien zu begrenzen:

- Wenn Ihr Outposts-Rack über das Internet oder eine öffentliche Direktverbindung mit der übergeordneten AWS Region verbunden ist, sollten Sie vor einer geplanten Wartung eine Trace-Route erfassen. Ein funktionierender (pre-network-maintenance) Netzwerkpfad und ein problematischer (post-network-maintenance) Netzwerkpfad zur Identifizierung der Unterschiede wären bei der Problembehebung hilfreich. Wenn Sie nach der Wartung ein Problem an Ihren ISP AWS weiterleiten, können Sie diese Informationen angeben.

  Erfassen Sie eine Trace-Route zwischen:

  - Die öffentlichen IP-Adressen am Standort Outposts und die von `outposts.region.amazonaws.com` zurückgegebene IP-Adresse. Ersetzen Sie es *`region`* durch den Namen der übergeordneten Region. AWS
  - Jede Instance in der übergeordneten Region mit öffentlicher Internetverbindung und den öffentlichen IP-Adressen am Standort Outposts.
- Wenn Sie die Kontrolle über die Netzwerkwartung haben, begrenzen Sie die Dauer der Ausfallzeit für den Service-Link. Nehmen Sie einen Schritt in Ihren Wartungsprozess auf, mit dem überprüft wird, ob das Netzwerk wiederhergestellt wurde.
- Wenn Sie keine Kontrolle über die Netzwerkwartung haben, überwachen Sie die Ausfallzeit der Serviceverbindung in Bezug auf das angekündigte Wartungsfenster und eskalieren Sie frühzeitig an die für die geplante Netzwerkwartung verantwortliche Partei, wenn die Serviceverbindung am Ende des angekündigten Wartungsfensters nicht wieder funktioniert.

## Ressourcen

Im Folgenden finden Sie einige Ressourcen zum Thema Überwachung, mit denen Sie sicherstellen können, dass die Outposts nach einem geplanten oder ungeplanten Strom- oder Netzwerkereignis normal funktionieren:

- Der AWS Blog Bewährte Methoden zur Überwachung AWS Outposts befasst sich mit bewährten Methoden zur Beobachtbarkeit und zum Eventmanagement speziell für Outposts.
- Der AWS Blog Debugging-Tool für Netzwerkkonnektivität von Amazon VPC erklärt das AWSSupport-SetupIPMonitoringFromVPCTool. Dieses Tool ist ein AWS Systems Manager Dokument (SSM-Dokument), das eine Amazon EC2 Monitor-Instance in einem von Ihnen angegebenen Subnetz erstellt und Ziel-IP-Adressen überwacht. Das Dokument führt Ping-, MTR-, TCP-Trace-Route- und Trace-Path-Diagnosetests durch und speichert die Ergebnisse in Amazon CloudWatch Logs, die in einem CloudWatch Dashboard visualisiert werden können (z. B. Latenz, Paketverlust). Für die Überwachung von Outposts sollte sich die Monitor-Instance in einem Subnetz der übergeordneten AWS Region befinden und so konfiguriert sein, dass sie eine oder mehrere Ihrer Outpost-Instances mithilfe ihrer privaten IP (s) überwacht. Dadurch werden Diagramme zum Paketverlust und zur Latenz zwischen AWS Outposts und der übergeordneten Region angezeigt. AWS
- Der AWS Blog Deploying an automated Amazon CloudWatch dashboard for AWS OutpostsAWS CDK use beschreibt die Schritte zur Bereitstellung eines automatisierten Dashboards.
- Wenn Sie Fragen haben oder weitere Informationen benötigen, finden Sie weitere Informationen unter Erstellen eines Support-Falls im Support-Benutzerhandbuch für AWS .

# end-of-termRack-Optionen für Outposts

Am Ende Ihrer AWS Outposts Amtszeit müssen Sie zwischen den folgenden Optionen wählen:

- Erneuern Sie Ihr Abonnement und behalten Sie Ihre bestehenden Outposts-Racks.
- Beenden Sie Ihr Abonnement und bereiten Sie Ihre Outposts-Racks für die Rückgabe vor.
- Wechseln Sie zu einem month-to-month Abonnement und behalten Sie Ihre bestehenden Outposts-Racks.

## Verlängern Sie Ihr Abonnement

Sie müssen die folgenden Schritte mindestens 30 Tage vor Ablauf des aktuellen Abonnements für Ihre Outposts-Racks abschließen.

Um Ihr Abonnement zu verlängern und Ihre bestehenden Outposts-Racks zu behalten

1. Melden Sie sich bei der AWS -Support -Center-Konsole an.
2. Wählen Sie Create case (Fall erstellen) aus.
3. Wählen Sie Konto und Fakturierung aus.
4. Wählen Sie als Service Fakturierung aus.
5. Wählen Sie als Kategorie die Option Andere Fragen zur Rechnungsstellung aus.
6. Wählen Sie als Schweregrad die Option Wichtige Frage aus.
7. Wählen Sie Next step: Additional information (Nächster Schritt: Zusätzliche Informationen).
8. Geben Sie auf der Seite Zusätzliche Informationen für Betreff Ihre Verlängerungsanfrage ein, z. B. **`Renew my Outpost subscription`**.
9. Geben Sie unter Beschreibung eine der folgenden Zahlungsoptionen ein:

   - Keine Vorauszahlung
   - Teilweise Vorauszahlung
   - Komplette Vorauszahlung

   Informationen zu den Preisen finden Sie unter AWS Outposts – Rackpreise. Sie können auch ein Preisangebot anfordern.

10. Klicken Sie auf Next step: Solve now or contact us ( ()Nächster Schritt): Jetzt lösen oder Support kontaktieren).
11. Wählen Sie auf der Seite Contact us (Kontakt) Ihre bevorzugte Sprache aus.
12. Wählen Sie Ihre bevorzugte Kontaktmethode.
13. Überprüfen Sie Ihre Falldetails und wählen Sie Submit (Absenden) aus. Ihre Fall-ID-Nummer und Übersicht werden angezeigt.

AWS Der Kundensupport leitet die Verlängerung des Abonnements ein. Ihr neues Abonnement beginnt am Tag nach Ablauf Ihres aktuellen Abonnements.

Wenn Sie nicht angeben, dass Sie Ihr Abonnement verlängern oder Ihr Outposts-Rack zurückgeben möchten, werden Sie automatisch in ein month-to-month Abonnement umgewandelt. Ihr Outposts-Rack wird monatlich zum Tarif der Zahlungsoption „Keine Vorauszahlung“ erneuert, die Ihrer AWS Outposts Konfiguration entspricht. Ihr neues monatliches Abonnement beginnt am Tag nach Ablauf Ihres aktuellen Abonnements.

## Ihr Abonnement beenden und die Rückgabe vorbereiten

Sie müssen die folgenden Schritte mindestens 30 Tage vor Ablauf des aktuellen Abonnements für Ihr Outposts-Rack abschließen. AWS Sie können den Rückgabevorgang erst starten, wenn Sie dies tun.

> **Important**
>
> AWS kann den Rückgabevorgang nicht beenden, nachdem Sie eine Support-Anfrage zur Kündigung Ihres Abonnements geöffnet haben.

Um dein Abonnement zu beenden

1. Melden Sie sich bei der AWS -Support -Center-Konsole an.
2. Wählen Sie Create case (Fall erstellen) aus.
3. Wählen Sie Konto und Fakturierung aus.
4. Wählen Sie als Service Fakturierung aus.
5. Wählen Sie als Kategorie die Option Andere Fragen zur Rechnungsstellung aus.
6. Wählen Sie als Schweregrad die Option Wichtige Frage aus.

7. Wählen Sie Next step: Additional information (Nächster Schritt: Zusätzliche Informationen).
8. Geben Sie auf der Seite Zusätzliche Informationen für Betreff eine eindeutige Anfrage ein, z. B. **`End my Outpost subscription`**
9. Geben Sie unter Beschreibung das Datum ein, an dem der Outpost abgeholt werden soll.
10. Klicken Sie auf Next step: Solve now or contact us ( ()Nächster Schritt): Jetzt lösen oder Support kontaktieren).
11. Wählen Sie auf der Seite Contact us (Kontakt) Ihre bevorzugte Sprache aus.
12. Wählen Sie Ihre bevorzugte Kontaktmethode.
13. Überprüfen Sie Ihre Falldetails und wählen Sie Submit (Absenden) aus. Ihre Fall-ID-Nummer und Übersicht werden angezeigt.

AWS Der Kundensupport wird sich mit Ihnen in Verbindung setzen, um den Abruf zu koordinieren.

So bereitest du deine AWS Outposts Regale für die Rückgabe vor:

> **Important**
>
> Schalten Sie das Outposts-Rack erst aus, wenn es für den geplanten Abruf vor Ort AWS ist.

1. Wenn die Ressourcen des Outposts freigegeben sind, müssen Sie die Freigabe dieser Ressourcen aufheben.

   Sie können die Freigabe einer gemeinsam genutzten Outpost-Ressource auf eine der folgenden Arten aufheben:

   - Verwenden Sie die Konsole AWS RAM . Weitere Informationen finden Sie unter Aktualisieren einer Ressourcenfreigabe im AWS RAM -Benutzerhandbuch.
   - Verwenden Sie den AWS CLI , um den disassociate-resource-shareBefehl auszuführen.

   Eine Liste der Outpost-Ressourcen, die freigegeben werden können, finden Sie unter Freigebbare Outpost-Ressourcen.
2. Beenden Sie die aktiven Instances, die Subnetzen auf Ihrem Outpost zugeordnet sind. Um die Instances zu beenden, folgen Sie den Anweisungen unter Ihre Instance beenden im  EC2 Amazon-Benutzerhandbuch.

> **Note**
>
> Einige AWS verwaltete Dienste, die auf Ihrem Outpost ausgeführt werden, wie Application Load Balancers oder Amazon Relational Database Service (RDS), verbrauchen Kapazität. EC2 Ihre zugehörigen Instances sind jedoch im EC2 Amazon-Dashboard nicht sichtbar. Sie müssen die mit diesen Diensten verbundenen Ressourcen beenden, um Kapazitäten freizugeben. Weitere Informationen finden Sie unter Warum fehlt in meinem Outpost EC2 Instance-Kapazität? .

3. Überprüfen Sie die instance-capacity-availability Ihrer EC2 Amazon-Instances in Ihrem AWS Konto.

   a. Öffnen Sie die AWS Outposts Konsole unter https://console.aws.amazon.com/outposts/.

   b. Wählen Sie Outposts.

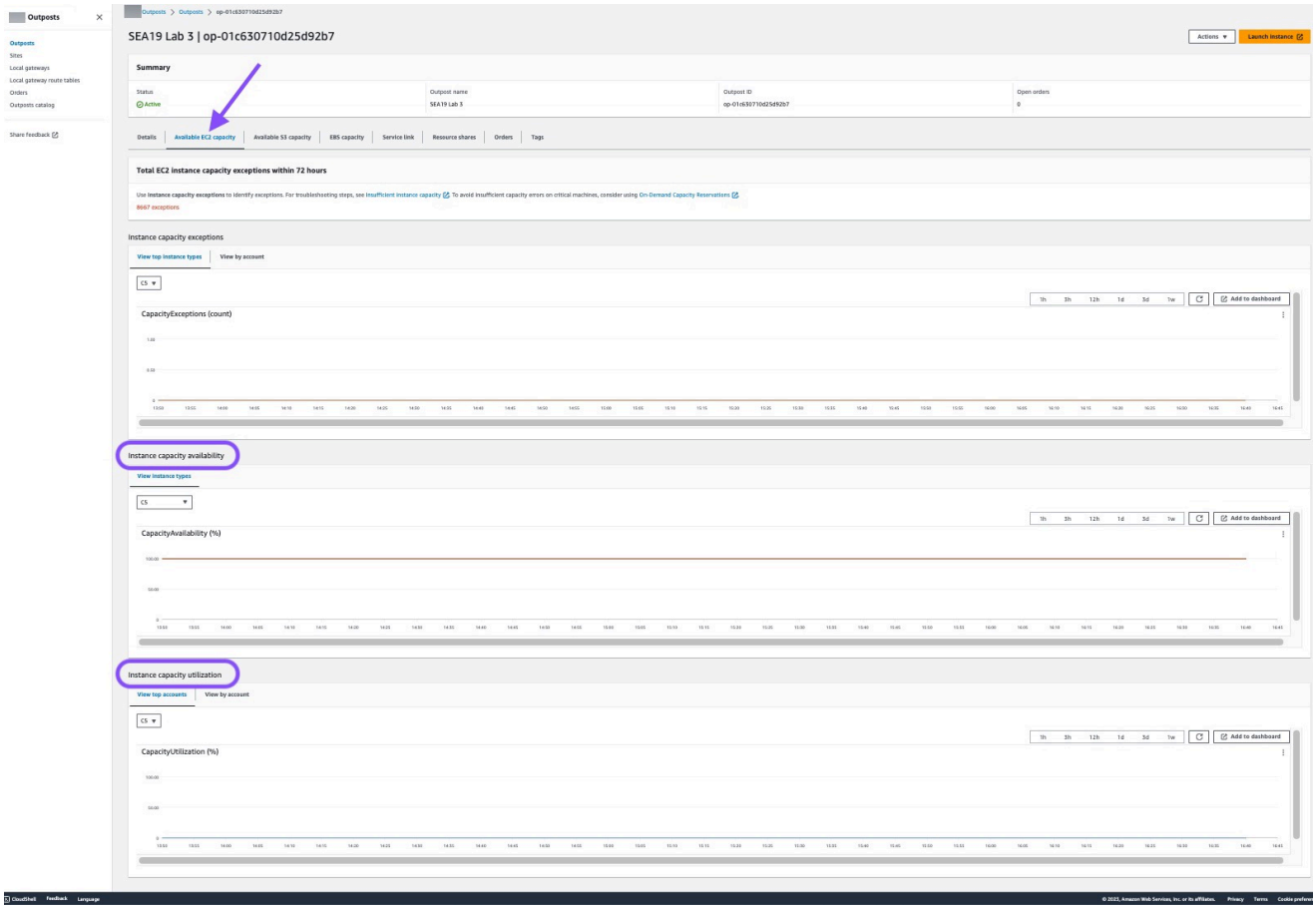
   c. Wählen Sie den spezifischen Outpost aus, zu dem Sie zurückkehren.

   d. Wählen Sie auf der Seite für den Outpost den Tab Verfügbare EC2 Kapazität aus.

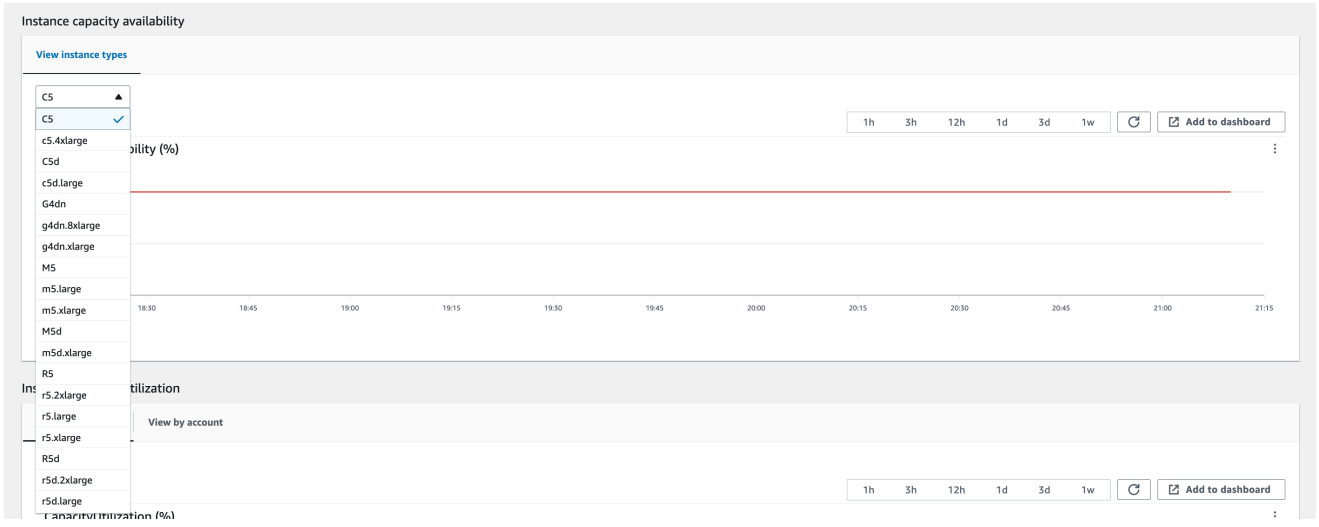
   e. Stellen Sie sicher, dass die Instance-Kapazitätsverfügbarkeit für jede Instance-Familie bei 100 % liegt.

   f. Stellen Sie sicher, dass die Instance-Kapazitätsauslastung für jede Instance-Familie bei 0 % liegt.

      Die folgende Abbildung zeigt die Diagramme zur Verfügbarkeit der Instance-Kapazität und zur Kapazitätsauslastung der Instanz auf der Registerkarte Verfügbare EC2 Kapazität.




Die folgende Abbildung zeigt die Liste der Instance-Typen.




4. Erstellen Sie Backups Ihrer EC2 Amazon-Instances und Server-Volumes. Um die Backups zu erstellen, folgen Sie den Anweisungen unter Backup und Wiederherstellung für Amazon EC2 mit EBS-Volumes im AWS Prescriptive Guidance Guide.
5. Löschen Sie die Amazon-EBS-Volumes, die Ihrem Outpost zugeordnet sind.

   a. Öffnen Sie die EC2 Amazon-Konsolenkonsole unter https://console.aws.amazon.com/ec2/.
   b. Wählen Sie im Navigationsbereich Volumes aus.
   c. Wählen Sie Aktionen und Volume löschen aus.
   d. Wählen Sie im Bestätigungs-Dialogfeld die Option Delete (Löschen).
6. Wenn Sie Amazon S3 auf Outposts haben, löschen Sie alle lokalen Snapshots in den Outposts.
   a. Öffnen Sie die EC2 Amazon-Konsolenkonsole unter https://console.aws.amazon.com/ec2/.
   b. Wählen Sie im Navigationsbereich die Option Snapshots aus.
   c. Wählen Sie die Schnappschüsse mit einem Outpost-ARN aus.
   d. Wählen Sie Aktionen und Schnappschüsse löschen.
   e. Wählen Sie im Bestätigungs-Dialogfeld die Option Delete (Löschen).
7. Löschen Sie alle Amazon S3 S3-Buckets, die mit Ihrem Outposts-Rack verknüpft sind. Um die Buckets zu löschen, folgen Sie den Anweisungen unter Löschen Ihres Amazon S3 on Outposts-Buckets im Amazon S3 on Outposts-Benutzerhandbuch.
8. Löschen Sie alle VPC-Zuordnungen und den kundeneigenen IP-Adresspool (CoIP), die Ihrem Outpost CIDRs zugeordnet sind.

Ein AWS Abrufteam schaltet das Rack aus. Nach dem Ausschalten können Sie den AWS Nitro-Sicherheitsschlüssel vernichten, oder das AWS Abrufteam kann dies in Ihrem Namen tun.

## In ein Abonnement umwandeln month-to-month

Um auf ein month-to-month Abonnement umzusteigen und Ihre bestehenden Outposts-Racks zu behalten, sind keine Maßnahmen erforderlich. Wenn Sie Fragen haben, öffnen Sie eine Support-Anfrage für die Abrechnung.

Ihre Outposts-Racks werden monatlich zum Tarif der Zahlungsoption „Keine Vorauszahlung“ erneuert, die Ihrer Outposts-Konfiguration entspricht. Ihr neues monatliches Abonnement beginnt am Tag nach dem Ende Ihres aktuellen Abonnements.

# Kontingente für AWS Outposts

Ihr AWS-Konto verfügt über Standardkontingente, die früher als Limits bezeichnet wurden, für jedes Objekt AWS-Service. Wenn nicht anders angegeben, gilt jedes Kontingent spezifisch für eine Region. Sie können Erhöhungen für einige Kontingente beantragen aber nicht für alle Kontingente.

Um die Kontingente für anzuzeigen AWS Outposts, öffnen Sie die Konsole Service Quotas. Wählen Sie im Navigationsbereich AWS-Services und anschließend AWS Outposts aus.

Informationen zur Erhöhung eines Kontingents finden Sie unter Anfordern einer Kontingenterhöhung im Service-Quotas-Benutzerhandbuch.

Ihr AWS-Konto hat die folgenden Kontingente im Zusammenhang mit AWS Outposts.

| Ressource | Standard | Anpassbar | Kommentare |
|---|---|---|---|
| Outpost-Standorte | 100 | Ja | Ein Outpost-Standort ist das vom Kunden verwaltete physische Gebäude, in dem Sie Ihre Outpost-Geräte mit Strom versorgen und an das Netzwerk anschließen.<br><br>Sie können in jeder Region Ihres AWS Kontos 100 Outposts-Websites haben. |
| Outposts pro Standort | 10 | Ja | AWS Outposts umfasst Hardware und virtuelle Ressourcen, die als Outposts bezeichnet werden. Dieses Kontingen t schränkt Ihre virtuellen Outpost-R essourcen ein.<br><br>Sie können 10 Outposts in jedem Outpost-Standort haben. |

# AWS Outposts und die Kontingente für andere Dienste

AWS Outposts stützt sich auf die Ressourcen anderer Dienste, und diese Dienste haben möglicherweise ihre eigenen Standardkontingente. Ihr Kontingent für lokale Netzwerkschnittstellen stammt beispielsweise aus dem Amazon VPC-Kontingent für Netzwerkschnittstellen.

In der folgenden Tabelle werden die Dokumentationsaktualisierungen für  beschrieben.

| Änderung | Beschreibung | Datum |
| --- | --- | --- |
| Aktualisierungen der statischen Stabilität | Für den Fall, dass Ihr Netzwerk unterbrochen wird, werden Instanz-Metriken und Logs für bis zu 7 Tage lokal zwischengespeichert. Bisher konnten Outposts Logs nur für ein paar Stunden zwischenspeichern. | 1. Mai 2025 |
| Aktualisierungen der AWS Identity and Access Management serviceverknüpften Rolle _ AWSServiceRoleForOutposts *OutpostID* | Die Berechtigungen für die *OutpostID* dienstverknüpfte Rolle AWSServiceRoleForOutposts_ wurden aktualisiert, um die AWS Outposts Verwaltung von Netzwerkressourcen für private Konnektivität zu verfeinern. Für Service Link-Endpunktinstanzen sind genauere Kontrollen der Netzwerkschnittstellen- und Sicherheitsgruppenoperationen erforderlich. | 17. April 2025 |
| Kapazitätsmanagement auf Anlagenebene | Sie können die Kapazitätskonfiguration auf Anlagenebene ändern. | 31. März 2025 |
| Private Konnektivität mit AWS Direct Connect Transit-VIF | Sie können den Service-Link jetzt so konfigurieren, dass er eine AWS Direct Connect Transit-VIF verwendet, um private Konnektivität zwischen | 11. Dezember 2024 |

| | | |
|---|---|---|
| | den Outposts und der AWS Heimatregion zu ermöglichen. | |
| Externe Blockvolumes, die durch Speicher von Drittanbietern unterstützt werden | Sie können jetzt während des Instanzstartvorgangs auf Outpost Blockdatenvolumes anhängen, die von kompatiblen Blockspeichersystemen von Drittanbietern unterstützt werden. | 01. Dezember 2024 |
| Kapazitätsmanagement | Sie können die Kapazität skonfiguration für eine Instanz ändern. | 11. November 2024 |
| Kapazitätsmanagement | Sie können die Standardkapazitätskonfiguration für Ihre neue Outposts-Bestellung ändern. | 16. April 2024 |
| AWS Outposts Das Rack unterstützt die Durchsatzmetriken der Service Link-Schnittstelle | Sie können jetzt die Durchsatznutzung zwischen den virtuellen Rack-Servicelink-Schnittstellen (VIFs) Ihrer Outposts und Ihren lokalen Netzwerkgeräten überwachen, indem Sie Metriken nutzen`IfTraffic In` . `IfTrafficOut` Amazon CloudWatch | 17. November 2023 |
| Intra-VPC-Kommunikation über AWS Outposts das lokale Gateway | Sie können die Kommunikation zwischen Subnetzen in derselben VPC über verschiedene Outposts mit lokalen Gateways herstellen. | 30. August 2023 |

| | | |
|---|---|---|
| End-of-term Optionen für AWS Outposts Racks | Am Ende Ihrer AWS Outposts Laufzeit können Sie Ihr Abonnement verlängern, beenden oder umwandeln. | 1. August 2023 |
| Amazon Route 53 on Outposts ist auf AWS Outposts Racks verfügbar. | Amazon Route 53 auf Outposts enthält einen Resolver, der alle DNS-Abfragen zwischenspeichert, die vom AWS Outposts-ausgehen. Sie können auch Hybridkonnektivität zwischen einem Outpost und einem On-Premises-DNS-Resolver einrichten, wenn Sie ein- und ausgehende Endpunkte bereitstellen. | 20. Juli 2023 |
| Eingehende Routen am lokalen Gateway | Sie können eingehende Routen für das lokale Gateway zu Elastic-Netzwerkschnittstellen auf Ihrem Outpost erstellen und ändern. | 15. September 2022 |
| Einführung von direktem VPC-Routing für AWS Outposts | Verwendet die private IP-Adresse von Instances in Ihrer VPC, um die Kommunikation mit Ihrem On-Premises-Netzwerk zu erleichtern. | 14. September 2022 |
| AWS Outposts Benutzerleitfaden für Outposts-Racks erstellt | AWS Outposts Das Benutzerhandbuch ist in separate Anleitungen für Rack und Server aufgeteilt. | 14. September 2022 |

| | | |
|---|---|---|
| Routing-Tabellen für lokale Gateways erstellen und verwalten | Erstellen und ändern Sie Routing-Tabellen lokale Gateways und CoIP-Pool s. Verwalten Sie VIF-Grupp enzuordnungen. | 14. September 2022 |
| Platzierungsgruppen auf AWS Outposts | Platzierungsgruppen, die eine Spread-Strategie verwenden, können Instances auf mehrere Hosts verteilen. | 30. Juni 2022 |
| Dedizierte Hosts auf AWS Outposts | Sie können Dedicated Hosts jetzt auf Outposts verwenden. | 31. Mai 2022 |
| Gemeinsam genutzte Outpost-Standorte | Erstellen und verwalten Sie Outpost-Sites und teilen Sie sie mit anderen AWS Konten in Ihrer Organisation. | 18. Oktober 2021 |
| Neue Dimension CloudWatch | Eine neue CloudWatch Dimension für Metriken im AWS Outposts Namespace. | 13. Oktober 2021 |
| S3-Buckets freigeben | Geben Sie S3-Buckets auf Ihrem Outpost frei und verwalten Sie sie. | 05. August 2021 |
| Unterstützung für einige Platzierungsgruppen | Sie können Cluster-, Partitions- oder Spread-Pl atzierungsstrategien genauso verwenden, wie Sie es in einer Region tun würden. | 28. Juli 2021 |
| Zusätzliche Metriken CloudWatch | Zusätzliche CloudWatch Metriken sind für Reserved Instances verfügbar. | 24. Mai 2021 |

| | | |
|---|---|---|
| Checkliste zur Fehlersuche in Netzwerken | Eine Checkliste zur Netzwerkfehlerbehebung ist verfügbar. | 22. Februar 2021 |
| Zusätzliche CloudWatch Metriken | Zusätzliche CloudWatch Metriken für EBS-Volumes sind verfügbar. | 2. Februar 2021 |
| Updates für die Konsole bestellen | Der Bestellvorgang für die Konsole wurde aktualisiert. | 14. Januar 2021 |
| Private Konnektivität | Sie können die private Konnektivität für Ihren Outpost konfigurieren, wenn Sie ihn in der AWS Outposts -Konsole erstellen. | 21. Dezember 2020 |
| Checkliste zur Netzwerkbereitschaft | Verwenden Sie die Checkliste zur Netzwerkbereitschaft, wenn Sie die Informationen für Ihre Outpost-Konfiguration sammeln. | 28. Oktober 2020 |
| Gemeinsam genutzte Ressourcen AWS Outposts | Mit Outpost Sharing können Outpost-Besitzer ihre Outposts und Outpost-Ressourcen , einschließlich lokaler Gateway-Routentabellen, mit anderen AWS Konten derselben Organisation teilen. AWS | 15. Oktober 2020 |
| Zusätzliche Metriken CloudWatch | Zusätzliche CloudWatch Metriken für die Anzahl der Instance-Typen sind verfügbar . | 21. September 2020 |

| | | |
|---|---|---|
| Zusätzliche CloudWatch Metrik | Eine zusätzliche CloudWatch Metrik für den Status der Verbindung mit dem Service Link ist verfügbar. | 11. September 2020 |
| Support für die gemeinsame Nutzung von kundeneigenen Adressen IPv4 | Wird verwendet AWS Resource Access Manager , um kundeneigene IPv4 Adressen zu teilen. | 20. April 2020 |
| Zusätzliche Metriken CloudWatch | Zusätzliche CloudWatch Metriken für EBS-Volumes sind verfügbar. | 4. April 2020 |
| Erstversion | Dies ist die erste Version von. AWS Outposts | 3. Dezember 2019 |

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.