Benutzerhandbuch für Racks

AWS Outposts

AWS Outposts: Benutzerhandbuch für Racks

Table of Contents

Was ist AWS Outposts?

AWS Outposts ist ein vollständig verwalteter Service, der AWS Infrastruktur, Services, APIs und Tools auf Kundenstandorte ausweitet. Durch die Bereitstellung des lokalen Zugriffs auf die AWS verwaltete Infrastruktur ermöglicht es Kunden, AWS Outposts Anwendungen On-Premises mit denselben Programmierschnittstellen wie in - AWS Regionen zu erstellen und auszuführen, während lokale Rechen- und Speicherressourcen für eine geringere Latenz und lokale Datenverarbeitungsanforderungen verwendet werden.

Ein Outpost ist ein Pool von AWS Rechen- und Speicherkapazität, der an einem Kundenstandort bereitgestellt wird. AWS führt diese Kapazität als Teil einer - AWS Region aus, überwacht und verwaltet sie. Sie können Subnetze auf 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, und all das innerhalb derselben VPC.

> **Note**
>
> Sie können einen Outpost nicht mit einem anderen Outpost 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.

- Outpost-Standort – Der vom Kunden verwaltete physische Ort, an dem Ihren Outpost AWS installiert. 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. Sie können die Kapazität für Ihren Outpost von der AWS Outposts -Konsole aus einsehen und verwalten.
- Outpost-Geräte – Physische Hardware, die Zugriff auf den AWS Outposts Service bietet. Die Hardware umfasst Racks, Server, Schalter und Kabel, die im Besitz von sind und von verwaltet werden AWS.

- Outposts-Racks – Ein Outpost-Formfaktor, bei dem es sich um ein 42U-Rack nach Branchenstandard handelt. Zu den Outpost-Racks gehören Server, Switches, ein Netzwerk-Patchpanel, ein Power-Shelf und leere Panels, die im Rack montiert werden können.
- 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. Outpost-Server bieten lokale Rechen- und Netzwerkdienste für Standorte mit begrenztem Platzbedarf oder geringeren Kapazitätsanforderungen.
- Service Link – Netzwerkroute, die die Kommunikation zwischen Ihrem Outpost und der zugehörigen AWS Region ermöglicht. Jeder Outpost ist eine Erweiterung einer Availability Zone und der zugehörigen Region.
- Lokales Gateway (LGW) – Ein virtueller Router mit logischer Interconnect-Verbindung, der die Kommunikation zwischen einem Outpost-Rack und Ihrem On-Premises-Netzwerk ermöglicht.
- Lokale Netzwerkschnittstelle – Eine Netzwerkschnittstelle, die die Kommunikation zwischen einem Outpost-Server und Ihrem On-Premises-Netzwerk 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
Amazon EC2-Instances	Ja	Ja
Amazon-ECS-Cluster	Ja	Ja
Amazon-EKS-Knoten	Ja	Nein

Datenbank und Analytik

Ressourcentyp	Racks	Server
Amazon- ElastiCache 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

Sonstige AWS-Services

Service	Racks	Server
AWS IoT Greengrass	 Ja	 Ja
Amazon SageMaker Edge Manager	 Ja	 Ja

Preisgestaltung

Sie können aus einer Vielzahl von Outpost-Konfigurationen wählen, von denen jede eine Kombination aus EC2-Instance-Typen und Speicheroptionen bietet. Der Preis für Rack-Konfigurationen beinhaltet Installation, Demontage und Wartung. Bei Servern müssen Sie die Geräte installieren und warten.

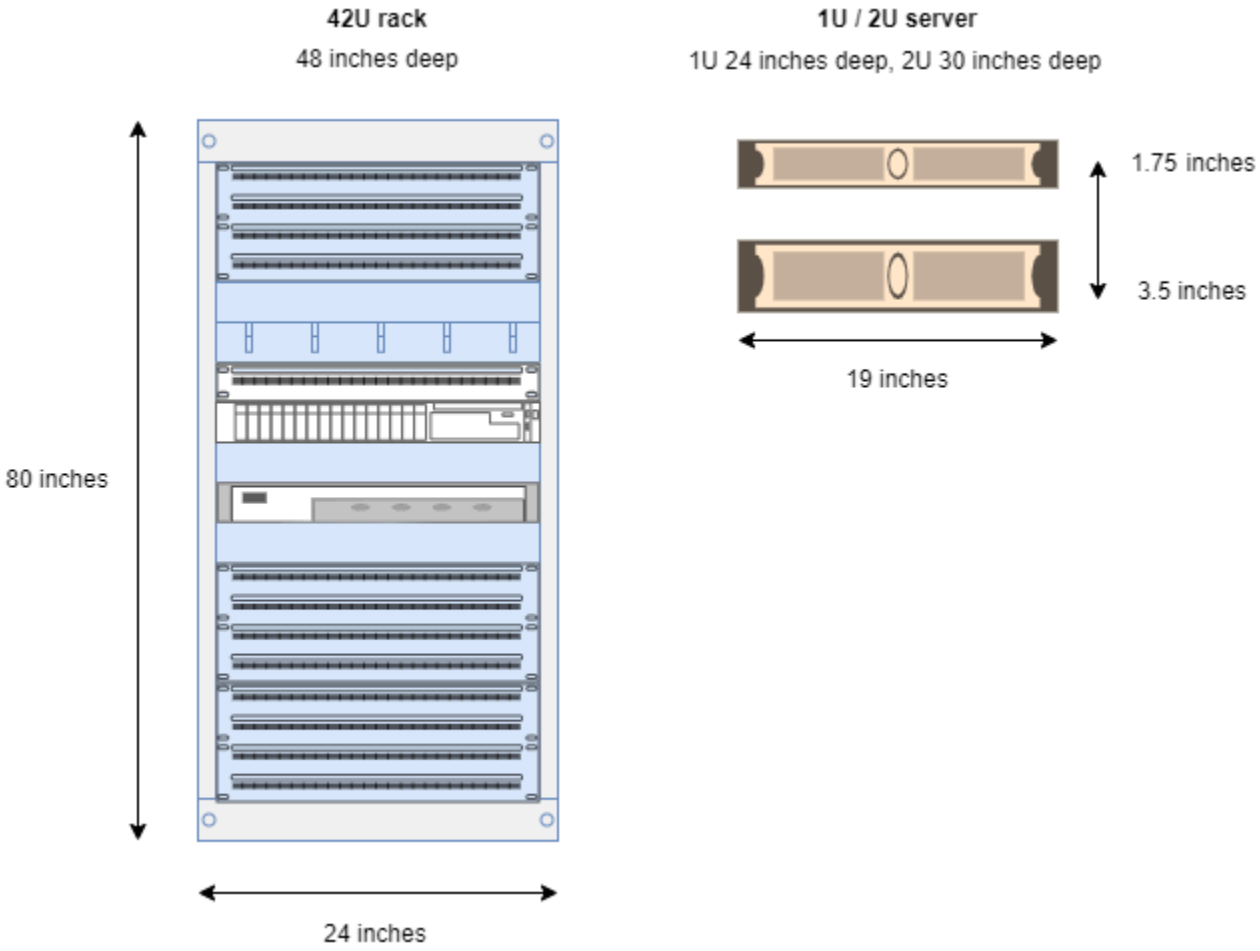
Sie erwerben eine Konfiguration mit einer Laufzeit von 3 Jahren und können zwischen drei Zahlungsoptionen wählen: Vollständige Vorauszahlung, Teilweise Vorauszahlung und Keine Vorauszahlung. Wenn Sie sich für die Zahlungsoption „Teilweise“ oder „Keine Vorauszahlung“ entscheiden, fallen monatliche Gebühren an. Alle Vorauszahlungen werden 24 Stunden, nachdem Ihr Outpost installiert wurde und die Rechen- und Speicherkapazität zur Verfügung steht, fällig. Weitere Informationen finden Sie hier:

- AWS Outposts -Rack-Preise
- AWS Outposts Preise für -Server

Funktionsweise von AWS Outposts

AWS Outpostsist 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 lokalen Umgebung herzustellen, müssen Sie Ihren Outpost mit Ihrem lokalen Netzwerk verbinden. Ihr lokales Netzwerk muss einen WAN-Zugang (Wide Area Network) zur Region und zum Internet ermöglichen. Es muss auch LAN- oder WAN-Zugriff auf das lokale Netzwerk bieten, in dem sich Ihre lokalen Workloads oder Anwendungen befinden.

Das folgende Diagramm zeigt beide Outpost-Formfaktoren.



Inhalt

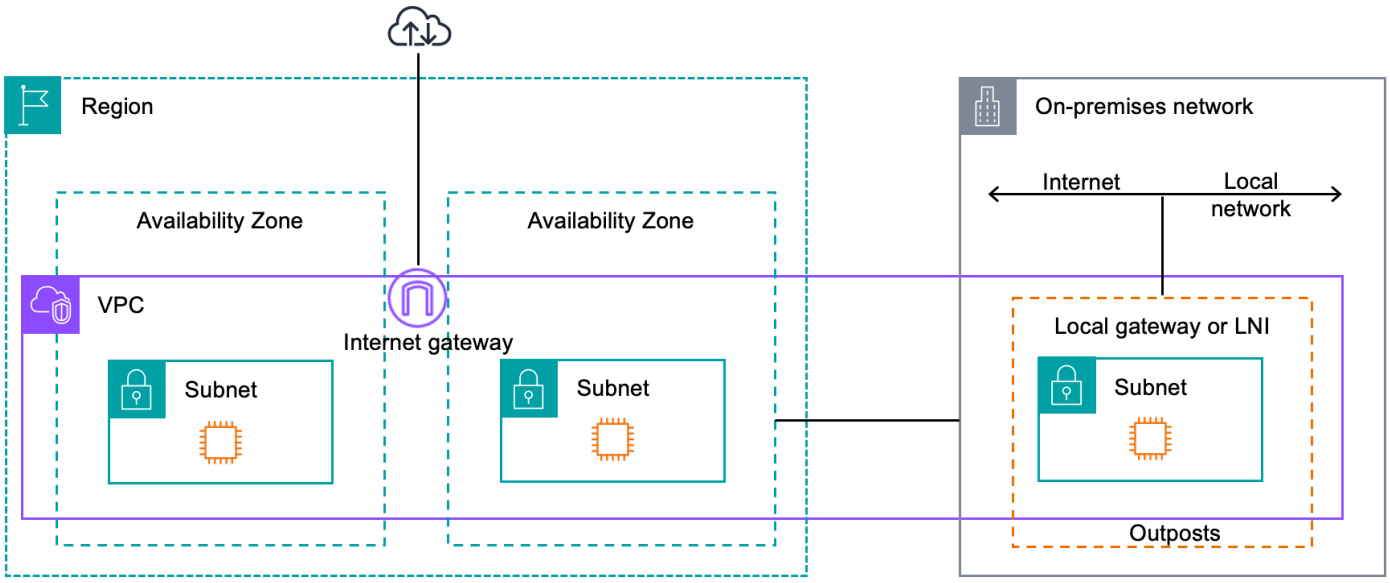
- DNS
- Link zum Dienst
- Lokale Gateways
- Lokale Netzwerkschnittstellen

Netzwerkkomponenten

AWS Outposts erweitert eine Amazon VPC von einer AWS-Region zu einem Außenposten mit den VPC-Komponenten, die in der Region zugänglich sind, einschließlich Internet-Gateways, Virtual Private Gateways, Amazon VPC Transit Gateways und VPC-Endpunkten. Ein Außenposten ist einer Availability Zone in der Region zugeordnet und ist eine Erweiterung dieser Availability Zone, die Sie für die Ausfallsicherheit verwenden können.

Das folgende Diagramm zeigt die Netzwerkkomponenten für Ihren Outpost.

- Ein AWS-Region und ein lokales Netzwerk
- Eine VPC mit mehreren Subnetzen in der Region
- Ein Außenposten im lokalen Netzwerk
- Die Konnektivität zwischen dem Outpost und dem lokalen Netzwerk wird entweder über ein lokales Gateway (Racks) oder eine lokale Netzwerkschnittstelle (Server) bereitgestellt



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-Instance-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 VPCs unterstützen, die über ein oder mehrere Outpost-Subnetze verfügen können. Informationen zu VPC-Kontingenten finden Sie unter Amazon VPC-Kontingente 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 sie einem Outpost-Subnetz zuordnen.

Die Routentabellen für Outpost-Subnetze funktionieren genauso wie für Availability Zone-Subnetze. 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 Verkehr 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.

- AWSZiele 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, verbleibt der Datenverkehr zwischen den VPCs im Outpost und verwendet nicht den Service-Link zurück zur Region.
- VPC-interne Kommunikation zwischen Outposts mit lokalem Gateway — Sie können die Kommunikation zwischen Subnetzen in derselben VPC über verschiedene Outposts mit lokalen Gateways mithilfe von direktem VPC-Routing herstellen. Weitere Informationen finden Sie unter:
  - Direktes VPC-Routing
  - Routing zu einem AWS Outposts lokalen 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-Funktionen wie Domainregistrierung, DNS-Routing und Zustandsprüfungen für Instances, die in Ihrem Outpost ausgeführt werden. Sowohl öffentliche als auch privat gehostete Availability Zones werden für die Weiterleitung von Datenverkehr zu bestimmten Domänen unterstützt. Route 53-Resolver werden in der AWS Region gehostet. 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 AWS-Region können längere DNS-Behebungszeiten mit Route 53 auftreten. In solchen Fällen können Sie die in Ihrer lokalen Umgebung installierten DNS-Server verwenden. Um Ihre eigenen DNS-Server zu verwenden, müssen Sie DHCP-Optionssätze für Ihre lokalen DNS-Server erstellen und sie der VPC zuordnen. Sie müssen außerdem sicherstellen, dass IP-Konnektivität zu diesen DNS-Servern besteht. Möglicherweise müssen Sie der Routingtabelle des lokalen Gateways auch Routen hinzufügen, um die Erreichbarkeit zu gewährleisten. Dies ist jedoch nur eine Option für Outpost-Racks mit lokalem Gateway. Da DHCP-Optionssätze einen VPC-Bereich haben, versuchen Instances sowohl in den Outpost-Subnetzen als auch in den Availability Zone-Subnetzen 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.

Link zum Dienst

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 Verkehr 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 ein Rack haben, AWS wird der Service-Link erstellt. Weitere Informationen finden Sie unter Outpost-Konnektivität zu AWS-Regionen.

Lokale Gateways

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

Lokale Netzwerkschnittstellen

Outpost-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 keine lokale Netzwerkschnittstelle von einer EC2-Instance in einem Outpost-Rack oder in der Region aus verwenden. AWS Die lokale Netzwerkschnittstelle ist nur für lokale Standorte vorgesehen. Weitere Informationen finden Sie unter Lokale Netzwerkschnittstelle im AWS OutpostsBenutzerhandbuch für Outposts-Server.

Standortanforderungen für ein Outposts-Rack.

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 – Häufig gestellte Fragen. Sehen Sie sich die Frage an: In welchen Ländern und Gebieten ist Outposts-Rack verfügbar?

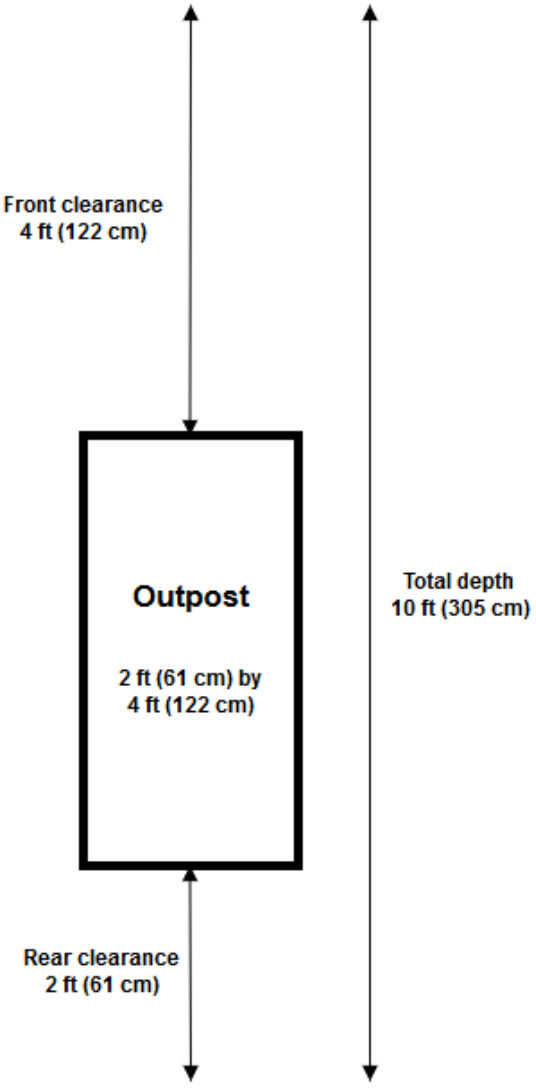
Diese Seite behandelt die Anforderungen für Outposts-Rack. Die Anforderungen für Outposts-Server finden Sie unter Standortanforderungen für Outposts-Server im AWS Outposts-Benutzerhandbuch für Outposts-Server.

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.



- Seismische Klammer – Sofern dies aufgrund von Vorschriften oder Code erforderlich ist, installieren und verwalten Sie eine angemessene seismische Verankerung und Klammer für das Rack, während es sich in Ihrer Einrichtung befindet. AWS bietet Fußklammer, die Schutz für bis zu 2,0 G an seismischen Aktivitäten mit allen Outposts-Racks bieten.
- Erdungspunkt – Wir empfehlen Ihnen, einen Erdungsdraht/Erdungspunkt an der Rack-Position vorzusehen, damit der AWS-zertifizierte Techniker die Racks während der Installation erden kann.
- Zugang zur Einrichtung – Sie dürfen die Einrichtung nicht in einer Weise verändern, die sich negativ auf die Fähigkeit von AWS auswirkt, auf den Outpost zuzugreifen, ihn zu warten oder zu entfernen.

- 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 OM4 mit LC bereit.
- 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, das WAN und alle Geräte zwischen dem Outpost und lokalen Datenverkehrszielen sowie dem Ziel in der AWS-Region.

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 OM4 mit LC

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 – 10 GBASE-LR
10 Gbit/s	MMF	– 10 GBASE-SR
40 GBit/s	SMF	– 40 GBASE-IR4 (LR4L) – 40 GBASE-LR4
Breakout-Anwendung mit 4 x 10 Gbit/s	MMF	– 40 GBASE-ESR4 – 40 GBASE-SR4
100 Gbit/s	SMF	– 100 G PSM4 MSA – 100 GBASE-CWDM4

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

Link-Aggregation und VLANs im Outpost-Bereich

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

Die folgenden VLANs sind für jedes Outpost-Netzwerkgerät erforderlich. Weitere Informationen finden Sie unter Virtuelle 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 dieselben VLANs oder unterschiedliche 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 virtuelle 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 die lokalen 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	BGP-Anforderungen für Service Link	Anforderungen für das lokale Gateway
Nr. 1	– Service Link CIDR (/30 oder /31) – IP-Adresse des Service Link	– Lokales Gateway CIDR (/30 oder /31) – IP-Adresse des lokalen Gateways
Nr. 2	– Service Link CIDR (/30 oder /31) – IP-Adresse des Service Link	– Lokales Gateway CIDR (/30 oder /31) – IP-Adresse des lokalen Gateways

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

Das Netzwerk muss eine MTU von 1 500 Byte zwischen dem Outpost und den Service Link-Endpunkten in der übergeordneten AWS Region unterstützen. Weitere Informationen über Service Link finden Sie unter AWS Outposts-Konnektivität zu AWS-Regionen.

Service Link Border Gateway-Protokoll

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). – Infrastruktur-CIDR (/26 erforderlich, als zwei zusammenhängende /27s angekündigt).

Lokales Netzwerkgerät	BGP-Anforderungen für Service Link
Nr. 1	– Service-Link-BGP-Peer-IP-Adresse. – Service Link BGP-Peer ASN. 2 Byte (16 Bit) oder 4 Byte (32 Bit).
Nr. 2	– Service-Link-BGP-Peer-IP-Adresse. – 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 AWS-Region zu verbinden. 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.

Lokales Gateway Border Gateway-Protokoll

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). – 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. – Lokales Gateway BGP-Peer-ASN. 2 Byte (16 Bit) oder 4 Byte (32 Bit).
Nr. 2	– BGP-Peer-IP-Adresse des lokalen Gateways. – 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 Stromkonfigurationen für 10 kVA angeben: 4 x L6-30P oder IEC309, 2 Absenkungen auf S1 und 2 Stromabfälle auf S2 für redundante, einphasige Stromversorgung. Die drei Leistungskonfigurationen sind in den folgenden zweiten Tabellen beschrieben.

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

Netzspannung (Wechselstrom)	Einphasig 208 bis 277 VAC (50 oder 60 Hz) Dreiphasig 346 bis 480 VAC (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 oder 32 A mit D-Kurve- oder K-Kurven-Schutzschalter. Nur für 2N-Eingänge (redundant): C-Kurve-, D-Kurve- oder K-Kurven-Schutzschalter. B-Kurve oder niedriger wird nicht unterstützt.
Typ des Wechselstromeingangs (Steckdose)	Einphasige 3xL6-30P-, P+P+E-, 30 A- oder 3xIEC60309 P+N+E-, IP67-, 32 A-Stecker Dreiphasig, Wye 1xIEC60309, 3P+N+E, IP67, Taktposition 7, 30 A-Stecker oder 1xIEC60309, 3P+N+E, IP67, Taktposition 6, 32 A-Stecker Dreiphasig, Delta 1xNon-NEMA-Twistlock Hubbell CS8365C, 3P+E, zentrale Masse, 50 A-Stecker **Note** Es hat sich bewährt, einen IP67-Stecker mit einer IP67-Steckdose zu verbinden. Wenn das nicht möglich ist, passt der IP67-Stecker zu einer IP44-Steckdose. Die Nennleistung des kombinierten Steckers und der Steckdose wird zur niedrigeren Nennleistung (IP44).
Kabellänge vom Stromverteiler	3 m (10,25 Fuß)
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.

<table>
<tr><th></th><th>Redundant, einphasig</th><th>Redundant, dreiphasig</th><th>Einphasig</th><th>Dreiphasig</th></tr>
<tr><td>5 kVA</td><td>2 x L6-30P oder IEC309, 1 Drop auf S1 und 1 Drop auf S2</td><td rowspan="3">2 x AH530P7W oder AH532P6W, 1 Drop auf S1 und 1 Drop auf S2</td><td>1 x L6-30P oder IEC309, 1 Drop auf S1</td><td rowspan="3">1 x AH530P7W oder AH532P6W, 1 Drop auf S1</td></tr>
<tr><td>10 kVA</td><td>4 x L6-30P oder IEC309, 2 Drops auf S1 und 2 Drops auf S2</td><td>2 x L6-30P oder IEC309, 2 Drops auf S1</td></tr>
<tr><td>15 kVA</td><td>6 x L6-30P oder IEC309, 3 Drops auf S1 und 3 Drops auf S2</td><td>3 x L6-30P oder IEC309, 3 Drops auf S1</td></tr>
</table>

Wenn die Wechselstromanschlusskabel, die AWS wie oben beschrieben zur Verfügung stellt, mit einem alternativen Netzstecker versehen 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 müssen Ihren AWS-Vertreter über Änderungen am Netzstecker informieren. Auf Anfrage stellen Sie AWS Informationen über die Änderungen zur 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, vereinbart AWS 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. 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 von AWS eine schriftliche Genehmigung einholen, bevor Sie Änderungen an der Outpost-Hardware oder der Elektroinstallation vornehmen. Sie erklären sich damit einverstanden, AWS Unterlagen zur Verfügung zu stellen, 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 AWS-Konto verfügbar ist.

Fangen Sie an mit AWS Outposts

Bestellen Sie einen Outpost, um loszulegen. Starten Sie nach der Installation Ihrer Outpost-Geräte Amazon EC2 EC2-Instances und greifen Sie auf Ihr On-Premises-Netzwerk zu.

Aufgaben

- Erstellen eines Outpost und Bestellung von Outpost-Kapazitäten
- Starten Sie eine Instance auf Ihrem Outpost-Rack

Erstellen eines Outpost und Bestellung von Outpost-Kapazitäten

Um mit der Nutzung zu beginnen 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 ein Outposts-Rack..
- Sie müssen über einen AWS Enterprise Support-Plan verfügen.
- Bestimme, AWS-Konto wem der Außenposten gehören wird. Verwenden Sie dieses Konto, um den Outposts-Standort zu erstellen, den Outpost zu erstellen und die Bestellung aufzugeben. Suchen Sie in der mit diesem Konto verknüpften E-Mail nach Informationen von AWS.

Aufgaben

- Schritt 1: Erstellen eines Standorts
- Schritt 2: Erstellen eines Outpost
- Schritt 3: Bestellung
- Schritt 4: Ändern Sie die Instance-Kapazität
- 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 AWS mit dem an AWS-Konto , dem der Outpost gehört.
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 Sie nützlich sein könnten, um mehr über die Website AWS 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. Sie können diesen Outpost bei der Bestellung spezifizieren.

Voraussetzungen

- Ermitteln 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”.
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. Nachdem Sie die Bestellung abgeschickt haben, wird sich ein AWS Outposts -Vertreter mit Ihnen in Verbindung setzen.

> **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 über den Zeitraum von drei Jahren 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, können Sie sich stattdessen an uns wenden, AWS 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 die Lieferadresse einer bestehenden 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 Instance-Kapazität

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 Kapazität Sie für Amazon EC2, Amazon EBS und Amazon S3 benötigen, um Ihre anfänglichen Workloads auszuführen, future Wachstum zu bewältigen und zusätzliche AWS Outposts 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 AWS Outposts 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 Neue 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.

Upload 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:

   ```
   {
       "RequestedInstancePools": [
           {
               "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.

Nächste Schritte

Sie können den Status Ihrer Bestellung über die AWS Outposts Konsole einsehen. Der ursprüngliche Status Ihrer Bestellung lautet Bestellung eingegangen. Ein AWS Vertreter wird sich innerhalb von drei Werktagen mit Ihnen in Verbindung setzen. Sie erhalten eine E-Mail-Bestätigung, wenn sich der Status Ihrer Bestellung in Bestellung in Bearbeitung ändert. Ein AWS Vertreter kann sich mit Ihnen in Verbindung setzen, um weitere erforderliche Informationen zu AWS erhalten.

Wenn Sie Fragen zu Ihrer Bestellung haben, wenden Sie sich an den AWS Support.

Um die Bestellung abzuwickeln, 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 Konto aus verfügbar ist. AWS

Starten Sie eine Instance auf Ihrem Outpost-Rack

Nach der Installation Ihres Outpost und der verfügbaren Datenverarbeitungs- und Speicherkapazität können Sie mit der Erstellung von Ressourcen beginnen. Starten Sie Amazon EC2-Instances und erstellen Sie Amazon EBS-Volumes auf Ihrem Outpost unter Verwendung eines Outpost-Subnetzes. Sie können auch Snapshots von Amazon EBS-Volumes auf Ihrem Outpost erstellen. Weitere Informationen zu Linux finden Sie unter Lokale Amazon EBS-Snapshots auf AWS Outposts im Amazon EC2-Benutzerhandbuch für Linux-Instances. Weitere Informationen zu Windows finden Sie unter Lokale Amazon EBS-Snapshots auf AWS Outposts im Amazon EC2-Benutzerhandbuch für Windows-Instances.

Voraussetzung

Sie müssen einen Outpost an Ihrem Standort installiert haben. Weitere Informationen finden Sie unter Erstellen eines Outpost und Bestellung von Outpost-Kapazitäten.

Aufgaben

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 Ihre 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 den IPv4-CIDR-Block die Option IPv4 CIDR Manual Input und geben Sie den IPv4-Adressbereich für die VPC in das IPv4 CIDR-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 IPv6-CIDR-Block aus.

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 AWS-Konto für Sie freigegeben wurde, fahren Sie mit fort. Schritt 5: Starten Sie eine Instanz auf dem Outpost

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 Lokales Gateway.

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

Sie können mit der AWS Outposts Konsole eine benutzerdefinierte Routentabelle für Ihr lokales Gateway (LGW) erstellen.

So erstellen Sie mit der Konsole eine benutzerdefinierte LGW-Routentabelle

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 Transit-Gateway-Routing-Tabelle erstellen) aus.
5. (Optional) Geben Sie unter Name einen Namen für Ihre LGW-Routentabelle 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 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.

8. (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.

9. Wählen Sie Lokale Transit-Gateway-Routing-Tabelle erstellen) aus.

3b: Ordnen Sie die VPC der benutzerdefinierten LGW-Routentabelle zu

Sie müssen die VPCs mit Ihrer LGW-Routentabelle verknüpfen. Sie sind standardmäßig nicht verknüpft.

Verwenden Sie das folgende Verfahren, um eine VPC mit einer LGW-Routentabelle zu verknüpfen.

Sie können Ihre Zuordnung optional mit Tags versehen, um sie zu identifizieren oder nach den Anforderungen Ihrer Organisation zu kategorisieren.

AWS Outposts console

So verknüpfen Sie eine VPC mit der benutzerdefinierten LGW-Routentabelle

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) Hinzufügen oder Entfernen eines Tags (Markierung).

   [Tag hinzufügen] Wählen Sie Neuen Tag 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.

Um eine Markierung zu entfernen, wählen Sie Entfernen rechts neben dem Schlüssel und dem Wert der Markierung aus.

7. Wählen Sie Associate VPC (VPC zuordnen) aus.

AWS CLI

So verknüpfen Sie eine VPC mit der benutzerdefinierten LGW-Routentabelle

Verwenden Sie den Befehl create-local-gateway-route- table-vpc-association.

Beispiel

```
aws ec2 create-local-gateway-route-table-vpc-association \
    --local-gateway-route-table-id lgw-rtb-059615ef7dEXAMPLE \
    --vpc-id vpc-07ef66ac71EXAMPLE
```

Output

```
{
    "LocalGatewayRouteTableVpcAssociation": {
        "LocalGatewayRouteTableVpcAssociationId": "lgw-vpc-assoc-0ee765bcc8EXAMPLE",
        "LocalGatewayRouteTableId": "lgw-rtb-059615ef7dEXAMPLE",
        "LocalGatewayId": "lgw-09b493aa7cEXAMPLE",
        "VpcId": "vpc-07ef66ac71EXAMPLE",
        "State": "associated"
    }
}
```

3c: Fügen Sie einen Routeneintrag zur Outpost-Subnetz-Routentabelle hinzu

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

Outpost-Subnetze innerhalb einer VPC, die mit Outpost LGW-Routing-Tabellen 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 LGW 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 LGW hinzu (). `lgw-xxxx`

Bestimmungsort	Ziel
172.16.100.0/24	`lgw-id`

Um einen Routeneintrag mit **`lgw-id`** als Ziel in der Outpost-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 der Sie sie erstellt haben. 2b: Erstellen Sie eine benutzerdefinierte Routing-Tabelle
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: Ordnen Sie die benutzerdefinierte LGW-Routentabelle den LGW-VIF-Gruppen zu

VIF-Gruppen sind logische Gruppierungen von virtuellen Schnittstellen (VIFs). Ordnen Sie die lokale Gateway-Routentabelle der VIF-Gruppe zu.

Um die benutzerdefinierte LGW-Routentabelle den LGW-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 Lokale Gateway-Routing-Tabellen aus.
4. Wählen Sie die Routing-Tabelle.
5. Wählen Sie im Detailbereich die Registerkarte VIF-Gruppenzuordnung und dann VIF-Gruppenzuordnung bearbeiten aus.
6. Wählen Sie für VIF-Gruppeneinstellungen die Option VIF-Gruppe zuordnen und wählen Sie eine VIF-Gruppe aus.

7. Wählen Sie Änderungen speichern aus.

3e: Fügen Sie einen Routeneintrag zur LGW-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 für das lokale Gateway 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 zu CoIP finden Sie unter IP-Adressen im Besitz des Kunden.

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

Amazon VPC console

Um der Instanz 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.
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 IPv4-Adresspool im Kundenbesitz.
6. Wählen Sie für den kundeneigenen 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 der Instanz eine CoIP-Adresse zuzuweisen

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 elastische 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",
}
```

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 über die Freigabe einer kundeneigenen IPv4-Adresse finden Sie unter Freigabe Ihrer AWS -Ressourcen im AWS RAM -Benutzerhandbuch.

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 Ihre 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 den CNDs beworbenen lokalen Subnetze müssen einen CIDR-Bereich haben, der dem CIDR-Bereich entspricht oder darin enthalten ist, in dem Sie konfiguriert haben. 3e: Fügen Sie einen Routeneintrag zur LGW-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.

Informationen zu den spezifischen Befehlen und der 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 elastische 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
- Die Kommunikation zwischen Ihrem Outpost und dem On-Premises-Netzwerk verwendet die CoIP Elastic IPs, um Instances im Outpost zu adressieren. Der VPC-CIDR-Bereich wird nicht verwendet.

In diesem Szenario wurde 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.

Informationen zu den spezifischen Befehlen und der 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.

Schritt 5: Starten Sie eine Instanz auf dem Outpost

Sie können EC2-Instances in dem Outpost-Subnetz starten, das Sie erstellt haben, oder in einem Outpost-Subnetz, das für Sie freigegeben wurde. 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 Schlüsselpaar angeben, genauso wie dies bei Instances in einem Availability Zone-Subnetz der Fall ist.

Überlegungen

- Sie können eine Platzierungsgruppe erstellen, um zu beeinflussen, wie Amazon EC2 versuchen soll, Gruppen von voneinander abhängigen Instances auf der Hardware des Outposts 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, Entfernen.
4. Wählen Sie auf der Outpost-Übersichtsseite die Option Instance starten aus. Sie werden zum Instance-Startassistenten in der Amazon EC2 EC2-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, für Ihren Outpost 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 den folgenden Themen im Amazon EC2 Benutzerhandbuch:

   - Linux — Starten Sie eine Instance mit dem Assistenten zum Starten neuer Instances
   - Windows — Starten Sie eine Instance mithilfe des Assistenten zum Starten neuer Instances

> **Note**
>
> Wenn Sie ein Amazon EBS-Volume erstellen, müssen Sie den Volumetyp gp2 verwenden, sonst schlägt der Assistent fehl.

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 Verbinden mit einer Linux-Instance finden Sie unter Verbinden Sie sich mit der Linux-Instance im Leitfaden Amazon EC2-Benutzerhandbuch für Linux-Instances. Informationen zum Herstellen einer Verbindung mit einer Windows-Instance finden Sie unter Herstellen einer Verbindung zu Ihrer Windows-Instance im Amazon-EC2-Benutzerhandbuch für Windows-Instances.

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 Information ist in der Amazon EC2 EC2-Konsole auf der Seite mit den Instance-Details 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-Instanz aus und geben Sie die IP-Adresse der Instanz 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. Informationen zum Verbinden mit einer Linux-Instance finden Sie unter Verbinden Sie sich mit der Linux-Instance im Leitfaden Amazon EC2-Benutzerhandbuch für Linux-Instances. Informationen zum Herstellen einer Verbindung mit einer Windows-Instance finden Sie unter Herstellen einer Verbindung zu Ihrer Windows-Instance im Amazon-EC2-Benutzerhandbuch für Windows-Instances.

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 Information ist in der Amazon EC2 EC2-Konsole auf der Seite mit den Instance-Details 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
   ```

AWS Outposts-Konnektivität zu AWS-Regionen

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

Inhalt

Konnektivität über Service Links

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

Um die Konnektivität des Service Links einzurichten, müssen Sie oder AWS während der Outpost-Bereitstellung den physischen Service-Link, das virtuelle LAN (VLAN) und die Konnektivität der Netzwerkebene mit Ihren lokalen Netzwerkgeräten konfigurieren. Weitere Informationen finden Sie unter Lokale Netzwerkkonnektivität für Racks und Standortanforderungen für das Outposts-Rack.

Für die Wide Area Network (WAN)-Konnektivität zur AWS-Region kann AWS Outposts Service Link-VPN-Verbindungen über die öffentliche Konnektivität der AWS.Region hergestellt werden. Dies setzt voraus, dass die Outposts Zugriff auf die öffentlichen IP-Bereiche der Region haben, was über das öffentliche Internet oder öffentliche virtuelle AWS Direct Connect-Schnittstellen erfolgen kann. Die aktuellen IP-Adressbereiche finden Sie unter IP-Adressbereiche für AWS im Amazon VPC-Benutzerhandbuch. Diese Konnektivität kann durch die Konfiguration spezifischer oder standardmäßiger (0.0.0.0/0) Routen im Service Link-Pfad der Netzwerkschicht aktiviert werden. Weitere Informationen finden Sie unter Service Link BGP-Konnektivität und Service Link Infrastruktur-Subnetzwerbung und IP-Bereich.

Alternativ können Sie die private Verbindungsoption für Ihren Outpost auswählen. Weitere Informationen finden Sie unter Private Service Link-Konnektivität mithilfe von VPC.

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

- Kunden-VPC-Datenverkehr zwischen dem Outpost und allen zugehörigen VPCs.
- Outposts-Verwaltungsverkehr, wie Ressourcenverwaltung, Ressourcenüberwachung und Firmware- und Software-Updates.

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 Bytes zwischen dem Outpost und den Service Link-Endpunkten in der übergeordneten AWS Region unterstützen. Informationen zur erforderlichen MTU zwischen einer Instance im Outpost und einer Instance in der AWS Region über den Service Link finden Sie unter Netzwerk-MTU (Maximum Transmission Unit) für Ihre Amazon EC2-Instance im Amazon EC2-Benutzerhandbuch für Linux-Instances.

Empfehlungen für die Bandbreite von Service Links

Für eine optimale Erfahrung und Ausfallsicherheit empfiehlt AWS, dass Sie eine redundante Konnektivität von mindestens 500 Mbps (1 Gbps ist besser) für die Service Link-Verbindung zur AWS-Region verwenden. Sie können AWS Direct Connect oder eine Internetverbindung für den Service Link verwenden. Mit der Service Link-Verbindung mit mindestens 500 Mbit/s können Sie Amazon EC2-Instances starten, Amazon-EBS-Volumes anfügen und auf -AWSServices wie Amazon EKS, Amazon EMR und CloudWatch -Metriken zugreifen.

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.

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 öffentliche virtuelle AWS Direct Connect-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
- Datenverkehr zwischen dem Outpost und allen zugehörigen 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 Outpost 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	Öffentliche Routen der AWS Outposts-Region
TCP	1025-65535	AWS Outposts-Service Link /26	443	Öffentliche Routen der AWS Outposts-Region

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.

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

Private Service Link-Konnektivität mithilfe von VPC

Sie können die Option für private Konnektivität in der Konsole auswählen, wenn Sie Ihren Outpost erstellen. Wenn Sie dies tun, wird nach der Outpost-Installation eine Service-Link-VPN-Verbindung über eine von Ihnen angegebene VPC und ein Subnetz hergestellt. Dies ermöglicht private Konnektivität über die VPC und minimiert die Gefährdung durch das öffentliche Internet.

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 unter Identity and Access Management (IAM) für AWS Outposts und Verwenden von serviceverknüpften Rollen für AWS Outposts.
- Erstellen Sie im selben AWS-Konto und in derselben Availability Zone, in denen sich Ihr Outpost befindet, eine VPC für den alleinigen Zweck der privaten Outpost-Konnektivität mit einem Subnetz /25 oder größer, das nicht mit 10.1.0.0/16 kollidiert. Beispiel: Sie könnten 10.2.0.0/16 verwenden.
- Erstellen Sie eine AWS Direct Connect-Verbindung, eine private virtuelle Schnittstelle und ein virtuelles privates Gateway, damit Ihr On-Premises-Outpost auf die VPC zugreifen kann. 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.

- Bewerben Sie das Subnetz-CIDR in Ihrem On-Premises-Netzwerk. Sie können AWS Direct Connect dazu verwenden. Weitere Informationen finden Sie unter AWS Direct ConnectVirtuelle Schnittstellen und Arbeiten mit AWS Direct Connect-Gateways im AWS Direct Connect-Benutzerhandbuch.

Sie können die Option für private Konnektivität auswählen, wenn Sie Ihren Outpost in der AWS Outposts-Konsole erstellen. Anweisungen finden Sie unter Erstellen eines Outpost und Bestellung von Outpost-Kapazitäten.

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

Nachdem Sie die Option für private Konnektivität für Ihren Outpost ausgewählt haben, wird AWS Outposts automatisch eine dienstbezogene Rolle in Ihrem Konto erstellt, mit der Outpost die folgenden Aufgaben in Ihrem Namen ausführen kann:

- Erstellt Netzwerkschnittstellen im Subnetz und in der VPC, die Sie angeben, und erstellt eine Sicherheitsgruppe für die Netzwerkschnittstellen.
- Erteilt dem AWS Outposts-Service die Berechtigung, die Netzwerkschnittstellen an eine Service Link-Endpunktinstance im Konto anzuhängen.
- Hängt die Netzwerkschnittstellen vom Konto aus an die Service Link-Endpunktinstances an.

Weitere Informationen zur serviceverknüpften Rolle finden Sie unter Verwenden von serviceverknüpften Rollen für AWS Outposts.

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

Redundante Internetverbindungen

Wenn Sie die Konnektivität zwischen Ihrem Outpost und der AWS-Region aufbauen, empfehlen wir Ihnen, mehrere Verbindungen einzurichten, um die Verfügbarkeit und Stabilität zu erhöhen. 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.

Outposts und Standorte

Verwalten Sie Outposts und Standorte für AWS Outposts.

Sie können Ihre Outposts und Standorte markieren, um sie zu identifizieren oder in Übereinstimmung mit den Anforderungen Ihrer Organisation kategorisieren zu können. Weitere Informationen zum Markieren finden Sie unter Markieren von - AWS Ressourcen im Allgemeine AWS-Referenz - Handbuch.

Themen

Outposts verwalten

AWS Outposts umfasst Hardware- und virtuelle Ressourcen, die als Outposts bezeichnet werden. Verwenden Sie diesen Abschnitt, um Outposts zu erstellen und zu verwalten, einschließlich der Änderung des Namens und dem Hinzufügen oder Anzeigen von Details oder Tags.

Erstellen eines Outpost

1. Öffnen Sie die - AWS Outposts Konsole unter https://console.aws.amazon.com/outposts/.
2. Um die zu ändern AWS-Region, verwenden Sie die Regionsauswahl in der oberen rechten Ecke der Seite.
3. Wählen Sie im Navigationsbereich Outposts aus.
4. Wählen Sie Outposts erstellen.
5. Wählen Sie einen Hardwaretyp für diesen Outpost.
6. Geben Sie für Ihren Outpost einen Namen und eine Beschreibung ein.
7. Wählen Sie eine Availability Zone für Ihren Outpost aus.
8. (Optional) Wählen Sie die Option private Konnektivität. Wählen Sie für VPC und Subnetz eine VPC und ein Subnetz im selben AWS Konto und in derselben Availability Zone wie Ihr Outpost aus.

> **Note**
>
> Wenn Sie die private Konnektivität für Ihren Outpost rückgängig machen müssen, müssen Sie sich an den Enterprise Support von AWS wenden.

9. Führen Sie von Site ID aus einen der folgenden Schritte aus:

   - Um einen vorhandenen Standort auszuwählen, wählen Sie den Standort aus.
   - Um einen neuen Standort zu erstellen, wählen Sie Standort erstellen, klicken Sie auf Weiter und geben Sie die Informationen zu Ihrem Standort in das neue Fenster ein.

     Nachdem Sie die Site erstellt haben, kehren Sie zu diesem Fenster zurück, um den Standort auszuwählen. Möglicherweise müssen Sie die Standort-Liste aktualisieren, um den neuen Standort zu sehen. Um Ihre Daten zu aktualisieren, wählen Sie das Aktualisierungssymbol ().

     Weitere Informationen finden Sie unter the section called “Standorte”.
10. Wählen Sie Outposts erstellen.

> **Tip**
>
> Um die Kapazität Ihres neuen Outposts zu erhöhen, müssen Sie eine Bestellung aufgeben.

Gehen Sie wie folgt vor, um den Namen und die Beschreibung eines Outposts zu bearbeiten.

So bearbeiten Sie Namen und Beschreibung des Outposts bearbeiten

1. Öffnen Sie die - AWS Outposts Konsole unter https://console.aws.amazon.com/outposts/.
2. Um die zu ändern AWS-Region, verwenden Sie die Regionsauswahl in der oberen rechten Ecke der Seite.
3. Wählen Sie im Navigationsbereich Outposts aus.
4. Markieren Sie den Outpost und wählen Sie dann Aktionen, Outpost bearbeiten.
5. Ändern Sie den Namen und die Beschreibung.

Geben Sie unter Name den Namen ein.

Geben Sie im Feld Beschreibung eine Beschreibung ein.

6. Wählen Sie Änderungen speichern aus.

Führen Sie die folgenden Schritte aus, um die Details zu einem Outpost anzuzeigen.

Outpost-Details anzeigen

1. Öffnen Sie die - AWS Outposts Konsole unter https://console.aws.amazon.com/outposts/.
2. Um die zu ändern AWS-Region, verwenden Sie die Regionsauswahl in der oberen rechten Ecke der Seite.
3. Wählen Sie im Navigationsbereich Outposts aus.
4. Wählen Sie Ihren Outpost aus und klicken Sie anschließend auf Aktionen, Entfernen.

Sie können auch die verwenden AWS CLI , um Outpost-Details anzuzeigen.

So zeigen Sie Outpost-Details mit der an AWS CLI

- Verwenden Sie den Befehl get-outpost AWS CLI .

Führen Sie die folgenden Schritte aus, um Tags in einem Outpost zu verwalten.

Outpost-Tags verwalten

1. Öffnen Sie die - AWS Outposts Konsole unter https://console.aws.amazon.com/outposts/.
2. Um die zu ändern AWS-Region, verwenden Sie die Regionsauswahl in der oberen rechten Ecke der Seite.
3. Wählen Sie im Navigationsbereich Outposts aus.
4. Wählen Sie den Outpost und dann Aktionen, Tags verwalten aus.
5. Hinzufügen oder Entfernen eines Tag.

   [Tag hinzufügen] Wählen Sie Neuen Tag 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.

  Um eine Markierung zu entfernen, wählen Sie Entfernen rechts neben dem Schlüssel und dem Wert der Markierung aus.

6. Wählen Sie Änderungen speichern aus.

Outpost-Standorte verwalten

Die vom Kunden verwalteten physischen Einrichtungen, in denen Ihren Outpost AWS installiert. Ein Standort muss die Anforderungen an die Einrichtung, das Netzwerk und die Stromversorgung Ihres Outposts erfüllen. Weitere Informationen finden Sie unter Voraussetzungen.

Einen Outpost-Standort erstellen

1. Öffnen Sie die - AWS Outposts Konsole unter https://console.aws.amazon.com/outposts/.
2. Um die zu ändern AWS-Region, verwenden Sie die Regionsauswahl in der oberen rechten Ecke der Seite.
3. Wählen Sie im Navigationsbereich Standorte aus.
4. Wählen Sie Create site (Standort erstellen).
5. Wählen Sie einen unterstützten Hardwaretyp für den Standort.
6. Geben Sie einen Namen, eine Beschreibung und eine Betriebsadresse für Ihren Standort ein. Wenn Sie sich für die Unterstützung von Racks am Standort entschieden haben, geben Sie die folgenden Informationen ein:

   - Höchstgewicht – Geben Sie das maximale Gewicht des Racks an, das für diesen Standort zulässig ist.
   - Leistungsaufnahme – Geben Sie die Leistungsaufnahme in kVA an, die an der Hardware-Position für das Rack verfügbar ist.
   - Stromoption – Geben Sie die Stromoption an, die Sie für Hardware bereitstellen können.
   - Power Connector – Geben Sie den Power Connector an, der für Verbindungen mit der Hardware bereitgestellt werden AWS soll.
   - Stromausfall – Legen Sie fest, ob die Stromzufuhr von oberhalb oder unterhalb des Racks erfolgt.

- Uplink-Geschwindigkeit – Geben Sie die Uplink-Geschwindigkeit an, die das Rack für die Verbindung mit der Region unterstützen soll.
- Anzahl der Uplinks – Geben Sie die Anzahl der Uplinks für jedes Outpost-Netzwerkgerät an, das Sie verwenden möchten, um das Rack mit Ihrem Netzwerk zu verbinden.
- Glasfasertyp – Geben Sie den Glasfasertyp an, den Sie verwenden werden, um den Outpost an Ihr Netzwerk anzuschließen.
- Optischer Standard – Geben Sie den Typ des optischen Standards an, den Sie verwenden werden, um den Outpost an Ihr Netzwerk anzuschließen.
- Hinweise – Geben Sie Hinweise zu einem Standort an.

7. Lesen Sie die Anforderungen an die Einrichtung und wählen Sie Ich habe die Anforderungen der Einrichtung gelesen.
8. Wählen Sie Create site (Standort erstellen).

Gehen Sie wie folgt vor, um einen Outpost-Standort zu bearbeiten.

Einen Standort bearbeiten

1. Öffnen Sie die - AWS Outposts Konsole unter https://console.aws.amazon.com/outposts/.
2. Um die zu ändern AWS-Region, verwenden Sie die Regionsauswahl in der oberen rechten Ecke der Seite.
3. Wählen Sie im Navigationsbereich Standorte aus.
4. Wählen Sie den Standort aus und klicken Sie dann auf Aktionen, Standort bearbeiten.
5. Sie können den Namen, die Beschreibung, die Betriebsadresse und die Standortdetails ändern.

   Wenn Sie die Betriebsadresse ändern, beachten Sie, dass sich die Änderungen nicht auf bestehende Bestellungen auswirken.
6. Wählen Sie Änderungen speichern aus.

Führen Sie die folgenden Schritte aus, um die Details zu einem Outpost-Standort anzuzeigen.

Standort-Details anzeigen

1. Öffnen Sie die - AWS Outposts Konsole unter https://console.aws.amazon.com/outposts/.
2. Um die zu ändern AWS-Region, verwenden Sie die Regionsauswahl in der oberen rechten Ecke der Seite.

3. Wählen Sie im Navigationsbereich Standorte aus.
4. Wählen Sie den Standort aus und klicken Sie anschließend auf Aktionen, Details anzeigen.

Gehen Sie wie folgt vor, um Tags eines Outpost-Standorts zu verwalten.

Standort-Tags verwalten

1. Öffnen Sie die - AWS Outposts Konsole unter https://console.aws.amazon.com/outposts/.
2. Um die zu ändern AWS-Region, verwenden Sie die Regionsauswahl in der oberen rechten Ecke der Seite.
3. Wählen Sie im Navigationsbereich Standorte aus.
4. Wählen Sie den Standort und dann Aktionen, Tags verwalten aus.
5. Hinzufügen oder Entfernen eines Tag.

   [Tag hinzufügen] Wählen Sie Neuen Tag 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.

   Um eine Markierung zu entfernen, wählen Sie Entfernen rechts neben dem Schlüssel und dem Wert der Markierung aus.
6. Wählen Sie Save Changes.

Lokales Gateway

Das lokale Gateway ist eine Kernkomponente der Outposts-Architektur. Das lokale Gateway ermöglicht die Konnektivität zwischen Ihren Outpost-Subnetzen und Ihrem On-Premises-Netzwerk. Wenn die lokale Infrastruktur einen Internetzugang bietet, können Workloads, die auf Outposts 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 Direct Connect erreicht werden. Weitere Informationen finden Sie unter AWS Outposts-Konnektivität zu AWS-Regionen.

Inhalt

Grundlagen zu lokalen Gateways

Jeder Outpost unterstützt ein einzelnes lokales Gateway. Ein lokales Gateway umfasst die folgenden Komponenten:

- Routing-Tabelle – verwendet, um lokale Gateway-Routing-Tabelle zu erstellen. Weitere Informationen finden Sie unter the section called “Routing-Tabellen für das lokale Gateway”.
- 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) – AWS erstellt eine VIF für jede LAG und fügt beide VIFs zu einer VIF-Gruppe hinzu. Die Routing-Tabelle des lokalen Gateways muss eine Standardroute zu den beiden VIFs für die lokale Netzwerkkonnektivität enthalten. Weitere Informationen finden Sie unter Lokale Netzwerkkonnektivität.
- VIF-Gruppenzuordnungen – AWS Fügt die erstellten VIFs einer VIF-Gruppe hinzu. VIF-Gruppen sind logische Gruppierungen von VIFs. Weitere Informationen finden Sie unter the section called “Zuordnung von VIF-Gruppen”.
- VPC-Zuordnungen – Sie verwenden sie, um VPC-Verknüpfungen mit Ihren VPCs und der lokalen Gateway-Routing-Tabelle zu erstellen. VPC-Routing-Tabelle, die Subnetzen zugeordnet sind, die

sich in einem Outpost befinden, können das lokale Gateway als Routenziel verwenden. Weitere Informationen finden Sie unter the section called “VPC-Zuordnungen”.

Wenn Ihr Outpost-Rack AWS bereitstellt, erstellen wir einige Komponenten und Sie sind für die Erstellung anderer verantwortlich.

AWS Verantwortlichkeiten

- Liefert die Hardware.
- Erzeugt das lokale Gateway.
- Erstellt 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 Routing-Tabelle des lokalen Gateways eine VIF-Gruppe zu.

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 für das lokale Gateway”.

Konnektivität über das lokale Gateway

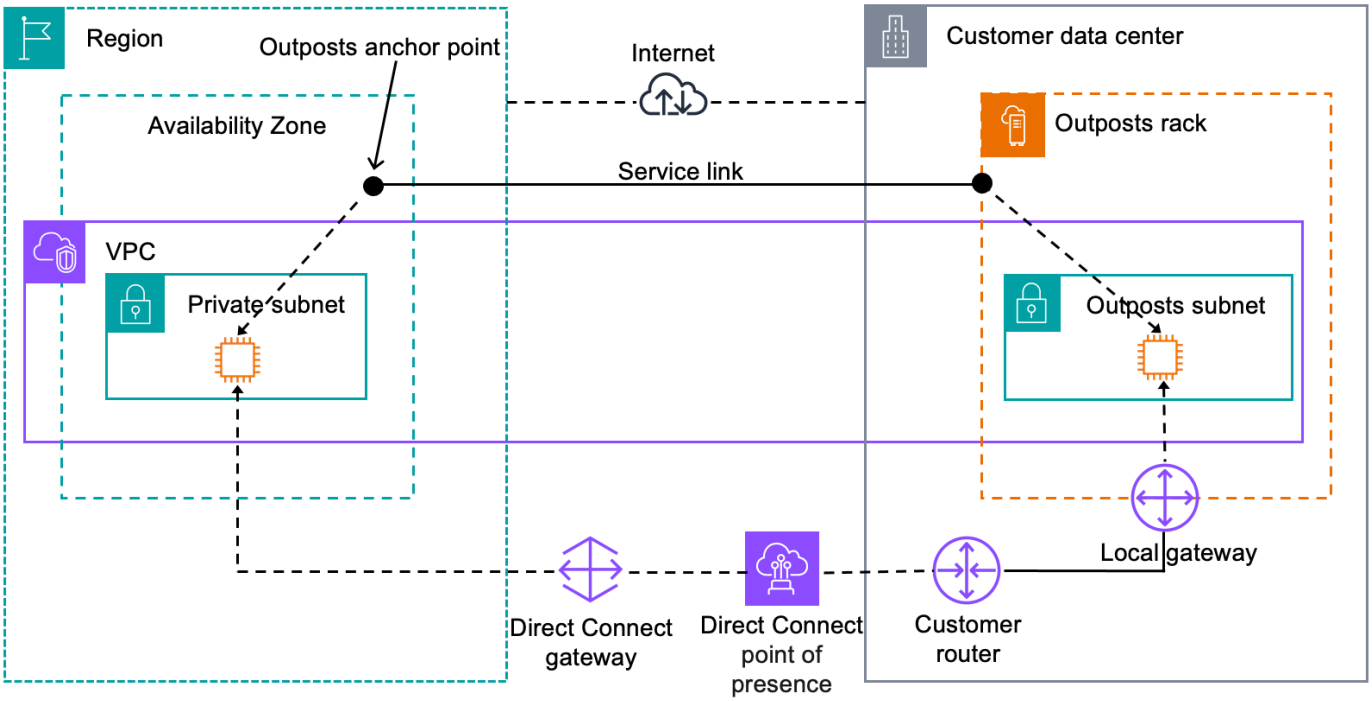
Die Hauptaufgabe eines On-Premises-Gateways besteht darin, Konnektivität von einem Outpost zu Ihrem On-Premises-On-Premises-Netzwerk bereitzustellen. Es bietet auch Konnektivität zum Internet

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 Pfad auf Datenebene 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 Steuerungsebene immer die Service Link-Konnektivität verwendet, unabhängig davon, welchen Pfad Sie auf der Datenebene verwenden.

Sie können Ihre On-Premises-Outposts-Infrastruktur mit AWS-Services in der Region privat über 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

Outpost-Subnetz-Routing-Tabellen in einem Rack können eine Route zu Ihrem On-Premises-Netzwerk enthalten. Das lokale Gateway leitet diesen Datenverkehr für Routing mit geringer Latenz an das On-Premises-Netzwerk weiter.

Standardmäßig verwendet Outposts die private IP-Adresse der Instances auf dem Outpost, um mit Ihrem On-Premises-Netzwerk zu kommunizieren. Dies wird als direktes VPC-Routing für AWS Outposts (oder direktes VPC-Routing) bezeichnet. Sie können jedoch einen Adressbereich angeben, der als kundeneigener IP-Adresspool (Customer-owned IP Address Pool, CoIP) bezeichnet wird, und Instanzen in Ihrem Netzwerk diese Adressen für die Kommunikation mit Ihrem On-Premises-Netzwerk verwenden lassen. Direktes VPC-Routing und CoIP schließen sich gegenseitig aus, und das Routing funktioniert je nach Ihrer Wahl unterschiedlich.

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 Outpost-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 EC2-Instances keine Elastic IP-Adressen zuweisen. 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.

Direktes VPC-Routing wird beispielsweise nur für Netzwerkschnittstellen unterstützt. Bei Netzwerkschnittstellen, die in Ihrem Namen AWS erstellt (als vom Anforderer verwaltete Netzwerkschnittstellen bezeichnet), sind ihre privaten IP-Adressen von Ihrem On-Premises-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

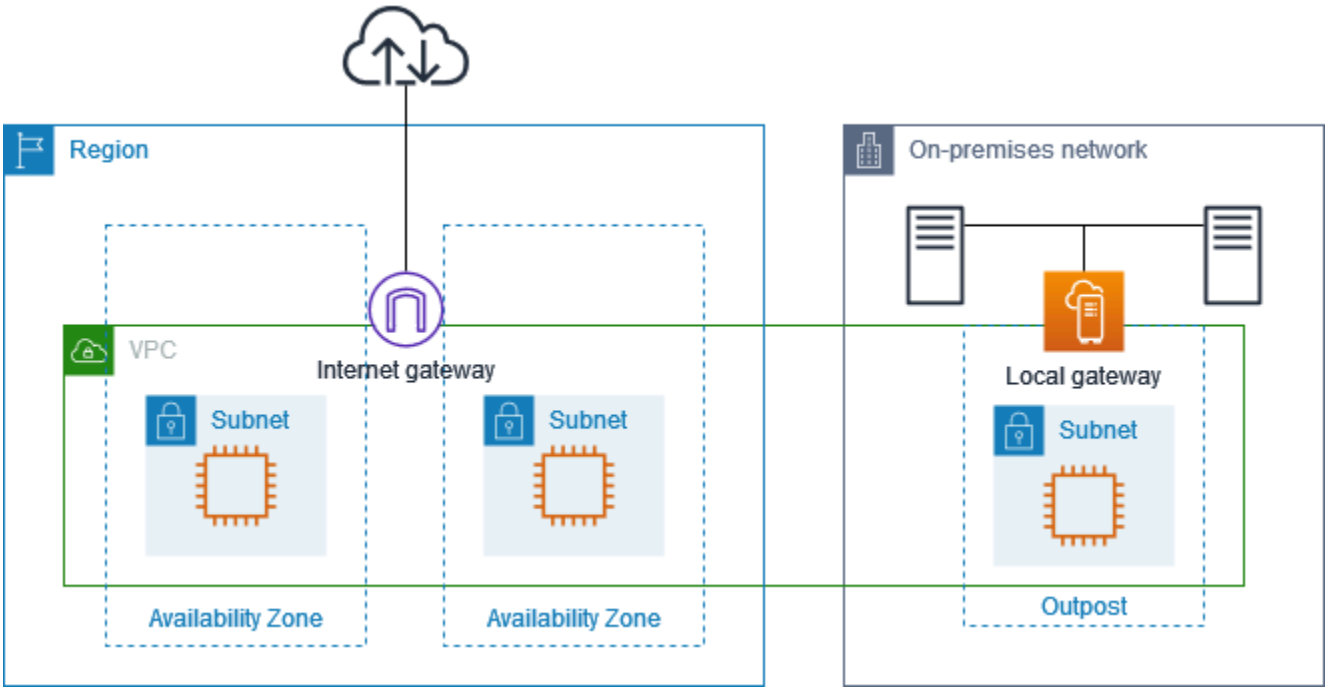
Instances in einem Outpost-Subnetz können über das an die VPC angeschlossene Internet-Gateway auf das Internet zugreifen.

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 EC2-Instance.
- 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-Netzwerk CIDR	*local-gateway-id*	Sendet den für das On-Premises-Netzwerk bestimmten Datenverkehr an das lokale Gateway.

Beispiel: Internetkonnektivität über das On-Premises-Netzwerk

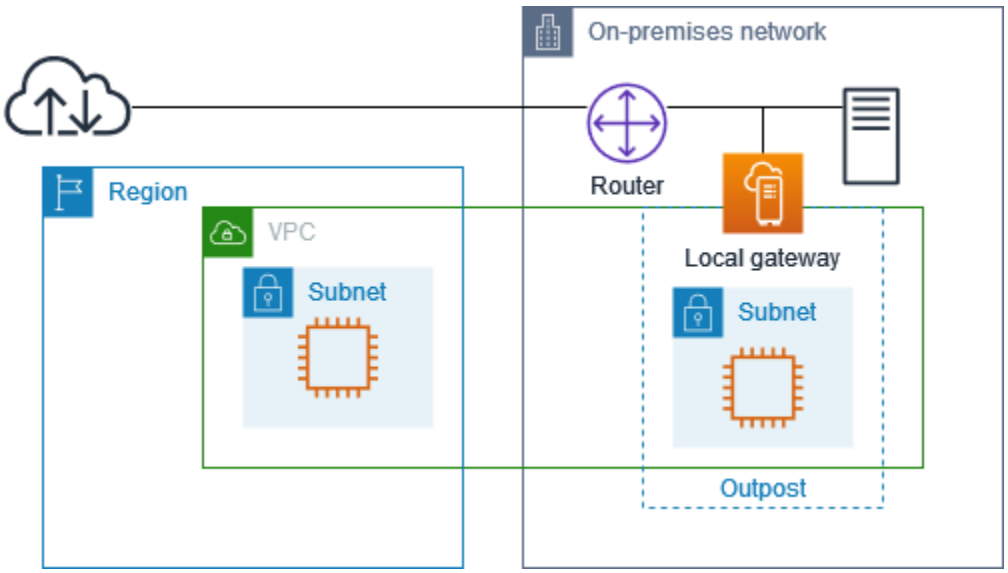
Instances in einem Outpost-Subnetz können über das On-Premises-Netzwerk auf das Internet zugreifen. Instances im Outpost-Subnetz benötigen keine öffentliche IP-Adresse oder Elastic IP-Adresse.

Berücksichtigen Sie folgende Konfiguration:

- Das Outpost-Subnetz hat eine EC2-Instance.
- 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 auf Ihrem Outpost zuweisen, z. B. EC2-Instances, indem Sie eine neue Elastic IP-Adresse aus dem kundeneigenen IP-Pool zuweisen und diese dann Ihrer Ressource zuweisen. Weitere Informationen finden Sie unter the section called “3f: (Optional) Weisen Sie der Instanz eine kundeneigene IP-Adresse zu”.

Die folgenden Anforderungen gelten für den kundeneigenen IP-Adresspool:

- Sie müssen in der Lage sein, die Adresse in Ihrem Netzwerk weiterzuleiten
- Der CIDR-Block muss mindestens /26 sein

Wenn Sie eine elastische 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 AWS-Konten in Ihrer Organisation teilen, indem Sie verwenden 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 auf dem Outpost zuweisen. Weitere Informationen finden Sie unter Freigeben Ihrer AWS -Ressourcen im AWS RAM -Benutzerhandbuch.

Beispiele

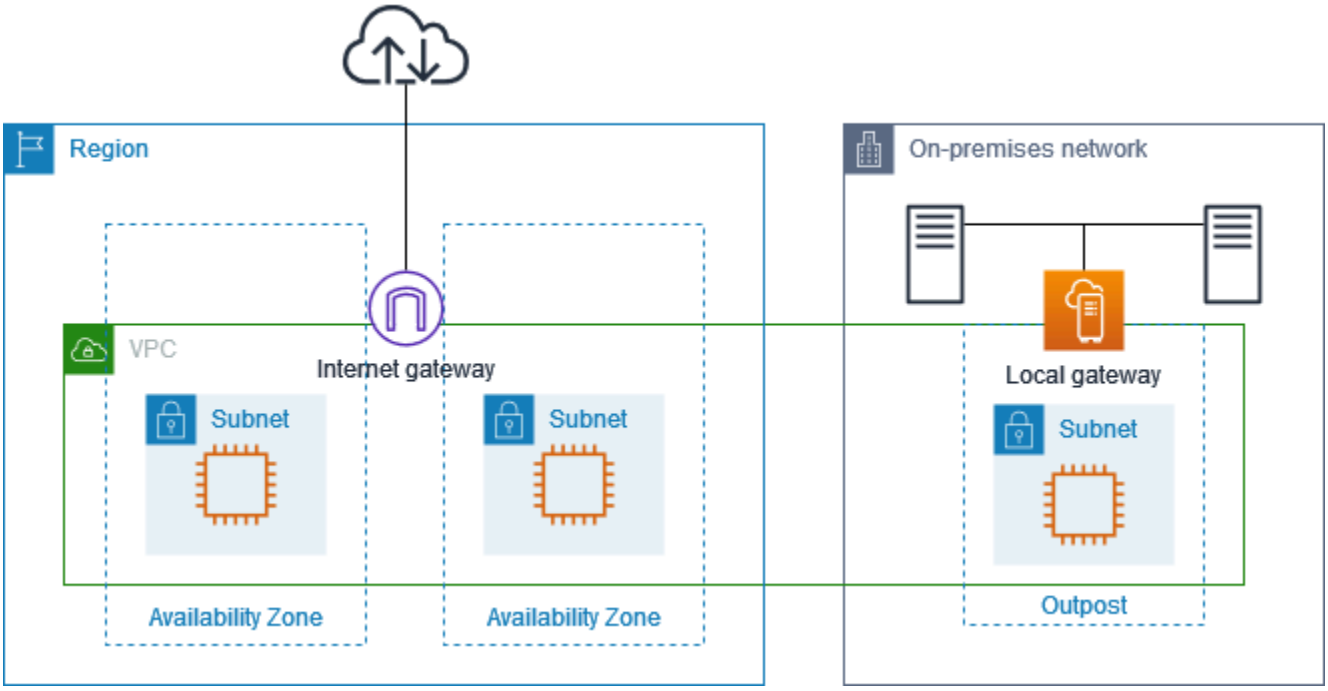
- Beispiel: Internetkonnektivität über die VPC
- Beispiel: Internetkonnektivität über das On-Premises-Netzwerk

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 EC2-Instance.
- 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.

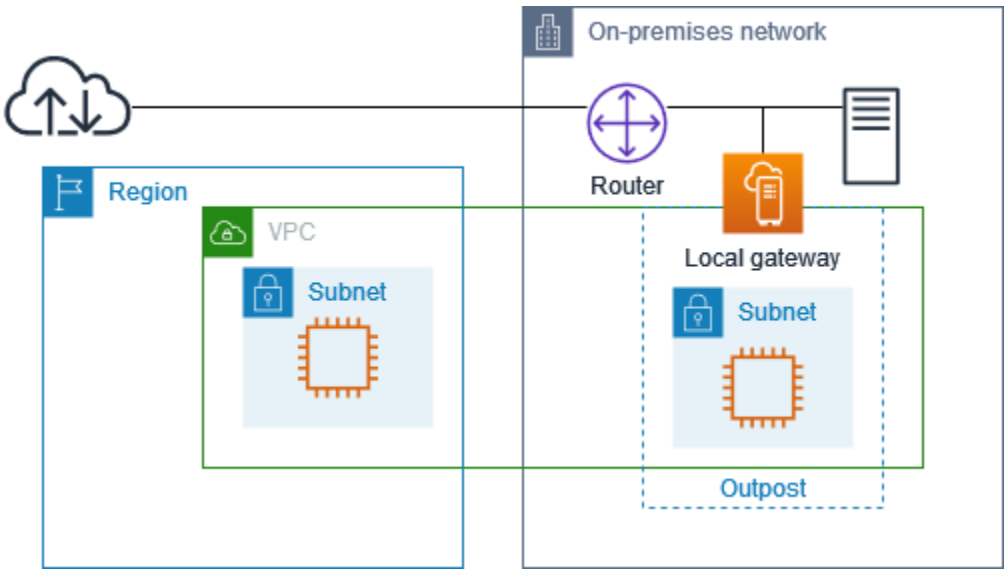
Bestimmungsort	Ziel	Kommentare
VPC-CIDR	Local	Stellt Konnektivität zwischen den Subnetzen in der VPC bereit.
0.0.0.0	*internet-gateway-id*	Sendet den für das öffentliche Internet bestimmten Datenverkehr an das Internet-Gateway.
On-Premises-Netzwerk CIDR	*local-gateway-id*	Sendet den für das On-Premises-Netzwerk 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 EC2-Instance.
- Es gibt einen kundeneigenen IP-Adresspool.
- Das lokale Gateway verwendet BGP-Werbung, um den kundeneigenen IP-Adresspool im On-Premises-Netzwerk zu bewerben.
- Eine elastische 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 Datenverkehr 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 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 übersetzt die IP-Adresse der EC2-Instance in die kundeneigene IP-Adresse (elastische IP-Adresse) und sendet dann den Datenverkehr 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 (Elastische IP-Adresse) der Instance. Das lokale Gateway übersetzt die IP-Adresse der EC2-Instance in die kundeneigene IP-Adresse (elastische IP-Adresse) und sendet dann den Datenverkehr an das Ziel. Darüber hinaus bewertet die Routing-Tabelle des lokalen Gateways alle Routen, die auf elastische 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.

Arbeiten mit lokalen Gateway-Routing-Tabellen

Im Rahmen der Rack-Installation AWS erstellt das lokale Gateway, konfiguriert VIFs und eine VIF-Gruppe. 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. Beachten Sie die folgenden Informationen zu Routing-Tabelle für lokale Gateways:

- VIF-Gruppen und lokale Gateway-Routing-Tabellen müssen eine one-to-one Beziehung haben.
- Das lokale Gateway gehört dem AWS Konto, das dem Outpost zugeordnet ist, und nur der Besitzer kann die Routing-Tabelle des lokalen Gateways ändern.
- Sie können die Routing-Tabelle des lokalen Gateways mithilfe von für andere AWS Konten oder Organisationseinheiten freigeben AWS Resource Access Manager. Weitere Informationen finden Sie unter Arbeiten mit freigegebenen AWS Outposts-Ressourcen.
- Routing-Tabellen für lokale Gateways verfügen über einen Modus, der festlegt, ob die private IP-Adresse von Instances für die Kommunikation mit Ihrem On-Premises-Netzwerk (direktes VPC-Routing) oder einem kundeneigenen IP-Adresspool (Customer-owned IP Address Pool, CoIP) verwendet werden soll. Direktes VPC-Routing und CoIP schließen sich gegenseitig aus, und das Routing funktioniert je nach Ihrer Wahl unterschiedlich. Weitere Informationen finden Sie unter ???.
- Der direkte VPC-Routing-Modus unterstützt keine überlappenden CIDR-Bereiche.

Aufgaben

- Details der Routing-Tabelle des lokalen Gateways anzeigen
- Erstellen benutzerdefinierter Routing-Tabellen für das lokale Gateway
- Routen einer Routing-Tabelle eines lokalen Gateways bearbeiten
- Verwalten von Routing-Tabellen-Tags für lokale Gateways
- Wechseln Sie zwischen den Routing-Tabellen eines lokalen Gateways oder Löschen einer Routing-Tabelle eines lokalen Gateways
- Verwalten von CoIP-Pools
- Zuordnung von VIF-Gruppen
- VPC-Zuordnungen

Details der Routing-Tabelle des lokalen Gateways anzeigen

Sie können die Details Ihrer Routing-Tabellen des lokalen Gateways mithilfe der Konsole oder der AWS CLI anzeigen.

AWS Outposts console

So zeigen Sie die Details der Routing-Tabelle des lokalen Gateways an

1. Öffnen Sie die - AWS Outposts Konsole unter https://console.aws.amazon.com/outposts/.
2. Um die 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 die Routing-Tabelle des lokalen Gateways aus, und wählen Sie dann Aktionen, Details anzeigen.

AWS CLI

So zeigen Sie die Details der Routing-Tabelle des lokalen Gateways an

Verwenden Sie den Befehl describe-local-gateway-route-tables AWS CLI .

Beispiel

```
aws ec2 describe-local-gateway-route-tables --region us-west-2
```

Output

```
{
    "LocalGatewayRouteTables": [
        {
            "LocalGatewayRouteTableId": "lgw-rtb-059615ef7deEXAMPLE",
            "LocalGatewayId": "lgw-09b493aa7cEXAMPLE",
            "OutpostArn": "arn:aws:outposts:us-west-2:111122223333:outpost/
op-0dc11b66edEXAMPLE",
            "State": "available",
            "Tags": []
        }
    ]
}
```

Note

Wenn die angezeigte Standard-Routing-Tabelle für das lokale Gateway den CoIP-Modus verwendet, ist die Routentabelle des lokalen Gateways mit einer Standardroute zu jeder der VIFs und einer weitergegebenen Route zu jeder zugehörigen kundeneigenen IP-Adresse im Pool-CoIP-Pool konfiguriert.

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 die 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 Transit-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.

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 Transit-Gateway-Routing-Tabelle erstellen) aus.

Routen einer Routing-Tabelle eines lokalen Gateways bearbeiten

Sie können lokale Gateway-Routing-Tabelle und eingehende Routen zu elastischen Netzwerkschnittstellen auf Ihrem Outpost erstellen. Sie können auch eine bestehende eingehende Route des lokalen Gateways ändern, um die Zielschnittstelle des elastischen Netzwerks zu ändern.

Eine Route ist nur dann Aktiv, wenn ihre elastische Ziel-Netzwerkschnittstelle mit einer laufenden Instance verbunden ist. Wenn die Instance gestoppt oder die Schnittstelle getrennt ist, wechselt die Route vom Status Aktiv in den Status Blackhole.

Für ein lokales Gateway gelten die folgenden Anforderungen und Einschränkungen:

- Die elastische Ziel-Netzwerkschnittstelle muss zu einem Subnetz auf Ihrem Outpost gehören und mit einer Instanz in diesem Outpost verbunden sein. Eine lokale Gateway-Route kann nicht auf eine Amazon EC2-Instance in einem anderen Outpost oder in der übergeordneten AWS-Region.
- Das Subnetz muss zu einer VPC gehören, die der Routing-Tabelle des lokalen Gateways zugeordnet ist.
- Sie dürfen nicht mehr als 100 elastic network interface Network-Interface-Routen in derselben Routing-Tabelle überschreiten.
- AWS priorisiert die spezifischste Route. Wenn die Routen übereinstimmen, priorisieren wir statische Routen gegenüber verbreiteten 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 ENIs, die an Outpost-Instances angehängt sind, können über das lokale Gateway für diesen Outpost kommunizieren. Nur ENIs, die an Outpost-Instances angehängt sind, können über das lokale Gateway für diesen Outpost kommunizieren.
- Verwaltete Schnittstellen wie VPCE-Endpunkte oder Schnittstellen können vor Ort nicht über das lokale Gateway erreicht werden. Sie können nur von Instances aus erreicht werden, die sich innerhalb des Outposts befinden.

Beachten Sie die folgenden NAT-Überlegungen:

- Das lokale Gateway führt kein NAT für Datenverkehr durch, der einer elastischen Netzwerkschnittstellenroute entspricht. Stattdessen wird die Ziel-IP-Adresse beibehalten.
- Deaktivieren Sie die Quell-/Zielprüfung für die Elastic Network-Zielschnittstelle. Weitere Informationen finden Sie unter Grundlagen der Netzwerkschnittstelle im Amazon EC2 Benutzerhandbuch für Linux-Instanzen.
- Konfigurieren Sie das Betriebssystem so, dass der Datenverkehr vom Ziel-CIDR auf der Netzwerkschnittstelle akzeptiert wird.

AWS Outposts console

So bearbeiten Sie die Route einer Routing-Tabelle eines lokalen Gateways

1. Öffnen Sie die - AWS Outposts Konsole unter https://console.aws.amazon.com/outposts/.
2. Um die 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 die Routing-Tabelle des lokalen Gateways aus, und wählen Sie dann Aktionen, Routen bearbeiten.
5. Um eine Route hinzuzufügen, wählen Sie Add route (Route hinzufügen). Geben Sie unter Zielbereich den Ziel-CIDR-Block, eine einzelne IP-Adresse oder die ID einer Präfixliste ein.
6. Um eine vorhandene Route zu ändern, ersetzen Sie unter Destination (Zielbereich) den CIDR-Block oder eine einzelne IP-Adresse. Wählen Sie unter Target (Ziel) ein Ziel aus.
7. Wählen Sie Save Rules (Routen speichern) aus.

AWS CLI

So erstellen Sie die Route einer Routing-Tabelle eines lokalen Gateways

- Verwenden Sie den create-local-gateway-route AWS CLI Befehl .

Beispiel

```
aws ec2 create-local-gateway-route \
    --local-gateway-route-table-id lgw-rtb-059615ef7dEXAMPLE \
    --network-interface-id eni-03e612f0a1EXAMPLE \
    --destination-cidr-block 192.0.2.0/24
```

Output

```
{
    "Route": {
        "DestinationCidrBlock": "192.0.2.0/24",
        "NetworkInterfaceId": "eni-03e612f0a1EXAMPLE",
        "Type": "static",
        "State": "active",
        "LocalGatewayRouteTableId": "lgw-rtb-059615ef7dEXAMPLE",
```

```
        "LocalGatewayRouteTableArn": "arn:aws:ec2:us-west-2:111122223333:local-
gateway-route-table/lgw-rtb-059615ef7dEXAMPLE",
        "OwnerId": "111122223333"
    }
}
```

So ändern Sie die Route einer Routing-Tabelle eines lokalen Gateways

Sie können die elastische Netzwerkschnittstelle ändern, auf die eine bestehende Route abzielt. Um den Änderungsvorgang verwenden zu können, muss die Routing-Tabelle bereits über eine Route mit dem angegebenen CIDR-Zielblock verfügen.

- Verwenden Sie den modify-local-gateway-route AWS CLI Befehl .

Beispiel

```
aws ec2 modify-local-gateway-route \
    --local-gateway-route-table-id lgw-rtb-059615ef7dEXAMPLE \
    --network-interface-id eni-12a345b6c7EXAMPLE \
    --destination-cidr-block 192.0.2.0/24
```

Output

```
{
    "Route": {
        "DestinationCidrBlock": "192.0.2.0/24",
        "NetworkInterfaceId": "eni-12a345b6c7EXAMPLE",
        "Type": "static",
        "State": "active",
        "LocalGatewayRouteTableId": "lgw-rtb-059615ef7dEXAMPLE",
        "LocalGatewayRouteTableArn": "arn:aws:ec2:us-west-2:111122223333:local-
gateway-route-table/lgw-rtb-059615ef7dEXAMPLE",
        "OwnerId": "111122223333"
    }
}
```

Verwalten von Routing-Tabellen-Tags für lokale Gateways

Sie können die Routing-Tabellen Ihrer lokalen Gateways mit Tags versehen, um sie zu identifizieren oder sie nach den Bedürfnissen Ihres Unternehmens zu kategorisieren.

So verwalten Sie die Tags der lokalen Gateway-Routing-Tabelle

1. Öffnen Sie die - AWS Outposts Konsole unter https://console.aws.amazon.com/outposts/.
2. Um die 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 des lokalen Gateways aus, und wählen Sie dann Aktionen, Tags verwalten.
5. Hinzufügen oder Entfernen eines Tag.

   [Tag hinzufügen] Wählen Sie Neuen Tag 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.

   Um eine Markierung zu entfernen, wählen Sie Entfernen rechts neben dem Schlüssel und dem Wert der Markierung aus.
6. Wählen Sie Änderungen speichern 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. Um die 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. Markieren Sie die Routing-Tabelle des lokalen Gateways, und wählen Sie dann Aktionen, Routing-Tabelle des lokalen Gateways löschen.
5. Geben Sie **`delete`** im Bestätigungsdialogfeld ein und wählen Sie dann Löschen.

6. (Optional) Erstellen Sie eine Routing-Tabelle eines lokalen Gateways mit einem neuen Modus.

    a. Wählen Sie Lokale Transit-Gateway-Routing-Tabelle erstellen) aus.

    b. 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.

Verwalten von CoIP-Pools

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. Informationen zum Umschalten zwischen den Routing-Tabellemodi des lokalen Gateways finden Sie unter Wechseln zwischen den Routing-Tabellemodi des lokalen Gateways.

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

So erstellen Sie einen CoIP-Pool

1. Öffnen Sie die - AWS Outposts Konsole unter https://console.aws.amazon.com/outposts/.
2. Um die 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) Hinzufügen oder Entfernen von CIDR-Blöcken

    [CIDR-Block hinzufügen] Wählen Sie Neue CIDR hinzufügen und geben Sie einen Bereich von IP-Adressen im Kundenbesitz ein.

    [CIDR-Block entfernen] Wählen Sie rechts neben einem CIDR-Block Entfernen aus.
9. Wählen Sie CoIP-Pool erstellen.

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

So bearbeiten Sie einen CoIP-Pool

1. Öffnen Sie die - AWS Outposts Konsole unter https://console.aws.amazon.com/outposts/.
2. Um die 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 wählen Sie dann einen CoIP-Pool aus.
6. Wählen Sie Aktionen, CoIP-Pool bearbeiten aus.
7. Wählen Sie Neue CIDR hinzufügen und geben Sie einen Bereich von IP-Adressen im Kundenbesitz ein.
8. (Optional) Hinzufügen oder Entfernen von CIDR-Blöcken

   [CIDR-Block hinzufügen] Wählen Sie Neue CIDR hinzufügen und geben Sie einen Bereich von IP-Adressen im Kundenbesitz ein.

   [CIDR-Block entfernen] Wählen Sie rechts neben einem CIDR-Block Entfernen aus.
9. Wählen Sie Änderungen speichern aus.

Gehen Sie wie folgt vor, um Tags zu verwalten oder einem CoIP-Pool ein Namensschild hinzuzufügen.

So verwalten Sie Tags in einem CoIP-Pool

1. Öffnen Sie die - AWS Outposts Konsole unter https://console.aws.amazon.com/outposts/.
2. Um die 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 wählen Sie dann einen CoIP-Pool aus.
6. Klicken Sie auf Aktionen, Tags verwalten.

7. Hinzufügen oder Entfernen eines Tag.

   [Tag hinzufügen] Wählen Sie Neuen Tag 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.

   Um eine Markierung zu entfernen, wählen Sie Entfernen rechts neben dem Schlüssel und dem Wert der Markierung aus.
8. Wählen Sie Änderungen speichern aus.

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

So löschen Sie einen CoIP-Pool

1. Öffnen Sie die - AWS Outposts Konsole unter https://console.aws.amazon.com/outposts/.
2. Um die 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 wählen Sie dann einen CoIP-Pool aus.
6. Wählen Sie Aktionen, CoIP-Pool löschen.
7. Geben Sie **`delete`** im Bestätigungsdialogfeld ein und wählen Sie dann Löschen.

Zuordnung von VIF-Gruppen

VIF-Gruppen sind logische Gruppierungen von virtuellen Schnittstellen (VIFs). Sie können die Routing-Tabelle des lokalen Gateways ändern, dem die VIF-Gruppe zugeordnet ist. Wenn Sie die Zuordnung einer VIF-Gruppe zu einer Routing-Tabelle eines lokalen Gateways aufheben, löschen Sie alle Routen aus der Routing-Tabelle und unterbrechen den Datenverkehr im Netzwerk.

So ändern Sie die Zuordnung einer VIF-Gruppe

1. Öffnen Sie die - AWS Outposts Konsole unter https://console.aws.amazon.com/outposts/.

2. Um die 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 VIF-Gruppenzuordnung und dann VIF-Gruppenzuordnung bearbeiten aus.
6. Führen Sie für VIF-Gruppeneinstellungen eine der folgenden Aktionen durch:

   - Um die VIF-Gruppe der lokalen Gateway-Routing-Tabelle zuzuordnen, wählen Sie VIF-Gruppe zuordnen und wählen Sie eine VIF-Gruppe aus.
   - Um die Zuordnung der VIF-Gruppe zur lokalen Gateway-Routing-Tabelle aufzuheben, deaktivieren Sie die Option VIF-Gruppe zuordnen.

   > **Important**
   >
   > Wenn Sie die Zuordnung einer VIF-Gruppe zur Routing-Tabelle des lokalen Gateways aufheben, werden automatisch alle Routen gelöscht und der Datenverkehr im Netzwerk unterbrochen.

7. Wählen Sie Änderungen speichern aus.

VPC-Zuordnungen

Sie müssen die VPCs mit Ihrer Routing-Tabelle des lokalen Gateways verknüpfen. Sie sind standardmäßig nicht verknüpft.

Erstellen Sie eine VPC-Zuordnung

Verwenden Sie das folgende Verfahren, um eine VPC der Routing-Tabelle eines lokalen Gateways zuzuordnen.

Sie können Ihre Zuordnung optional mit Tags versehen, um sie zu identifizieren oder nach den Anforderungen Ihrer Organisation zu kategorisieren.

AWS Outposts console

So ordnen Sie eine VPC zu

1. Öffnen Sie die - AWS Outposts Konsole unter https://console.aws.amazon.com/outposts/.

2. Um die 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) Hinzufügen oder Entfernen eines Tags (Markierung).

   [Tag hinzufügen] Wählen Sie Neuen Tag 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.

   Um eine Markierung zu entfernen, wählen Sie Entfernen rechts neben dem Schlüssel und dem Wert der Markierung aus.
7. Wählen Sie Associate VPC (VPC zuordnen) aus.

AWS CLI

So ordnen Sie eine VPC zu

Verwenden Sie den Befehl create-local-gateway-route-table-vpc-association.

Beispiel

```
aws ec2 create-local-gateway-route-table-vpc-association \
    --local-gateway-route-table-id lgw-rtb-059615ef7dEXAMPLE \
    --vpc-id vpc-07ef66ac71EXAMPLE
```

Output

```
{
    "LocalGatewayRouteTableVpcAssociation": {
        "LocalGatewayRouteTableVpcAssociationId": "lgw-vpc-assoc-0ee765bcc8EXAMPLE",
        "LocalGatewayRouteTableId": "lgw-rtb-059615ef7dEXAMPLE",
        "LocalGatewayId": "lgw-09b493aa7cEXAMPLE",
        "VpcId": "vpc-07ef66ac71EXAMPLE",
```

```
        "State": "associated"
    }
}
```

So löschen Sie eine VPC-Zuordnung.

Verwenden Sie das folgende Verfahren, um die Zuordnung einer VPC zur Routing-Tabelle eines lokalen Gateways aufzuheben.

AWS Outposts console

So heben Sie die Zuordnung einer VPC auf

1. Öffnen Sie die - AWS Outposts Konsole unter https://console.aws.amazon.com/outposts/.
2. Um die 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. Markieren Sie die Routing-Tabelle, und wählen Sie dann Aktionen, Details anzeigen.
5. Wählen Sie unter VPC-Zuordnungen die VPC aus, die Sie trennen möchten, und klicken Sie dann auf Trennen.
6. Wählen Sie Disassociate (Zuordnung aufheben) aus.

AWS CLI

So heben Sie die Zuordnung einer VPC auf

Verwenden Sie den Befehl delete-local-gateway-route-table-vpc-association.

Beispiel

```
aws ec2 delete-local-gateway-route-table-vpc-association \
    --local-gateway-route-table-id lgw-rtb-059615ef7dEXAMPLE \
    --vpc-id vpc-07ef66ac71EXAMPLE
```

Output

```
{
    "LocalGatewayRouteTableVpcAssociation": {
```

```
        "LocalGatewayRouteTableVpcAssociationId": "lgw-vpc-assoc-0ee765bcc8EXAMPLE",
        "LocalGatewayRouteTableId": "lgw-rtb-059615ef7dEXAMPLE",
        "LocalGatewayId": "lgw-09b493aa7cEXAMPLE",
        "VpcId": "vpc-07ef66ac71EXAMPLE",
        "State": "associated"
    }
}
```

Lokale Netzwerkkonnektivität von Racks

Sie benötigen die folgenden Komponenten, um Ihr Outpost-Rack mit Ihrem On-Premises-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.
- Layer-3- point-to-point 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 Outpost-Rack besteht aus zwei physischen Netzwerkgeräten, die an Ihr lokales Netzwerk angeschlossen werden.

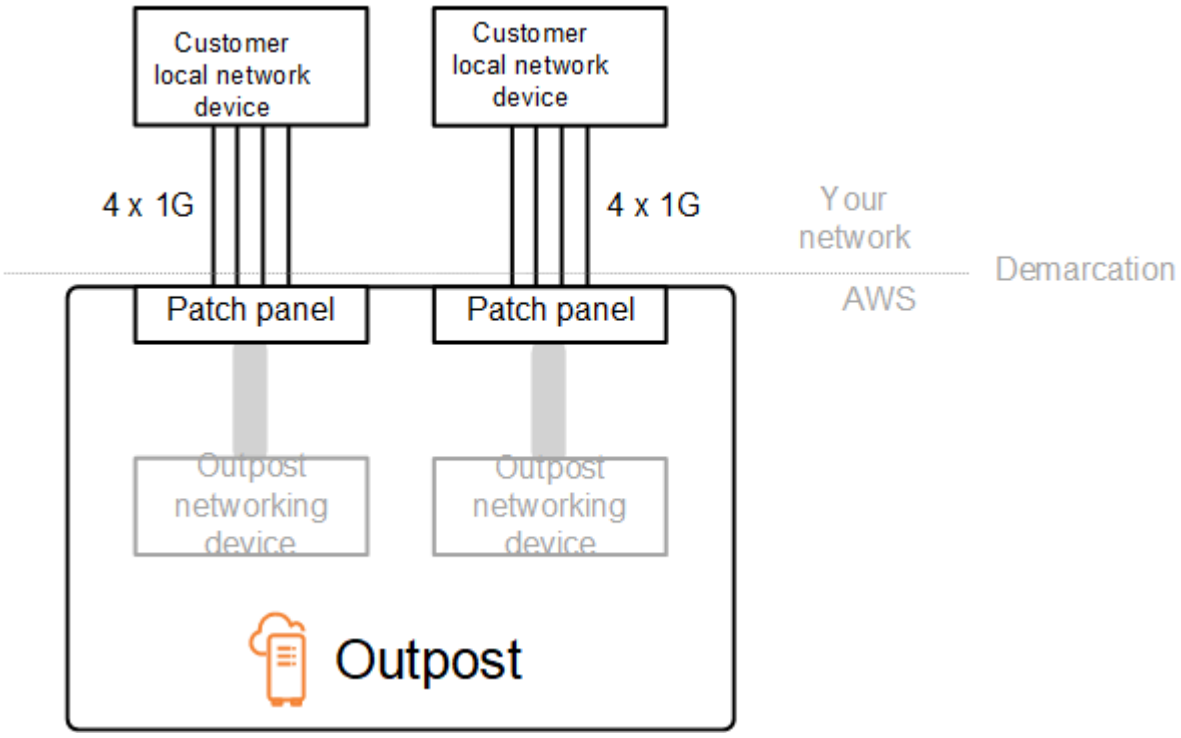
Ein Outpost benötigt mindestens zwei physische Verbindungen zwischen diesen Outpost-Netzwerkgeräten und Ihren lokalen Netzwerkgeräten. Ein Outpost unterstützt die folgenden Uplink-Geschwindigkeiten und -Mengen für jedes Outpost-Netzwerkgerät.

Uplink-Geschwindigkeit	Anzahl der Uplinks
1 Gbit/s	1, 2, 4, 6, or 8
10 Gbit/s	1, 2, 4, 8, 12, oder 16
40 Gbit/s oder 100 Gbit/s	1, 2, or 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 Vorwärtsfehlerkorrektur (FEC CL91) konfigurieren.

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

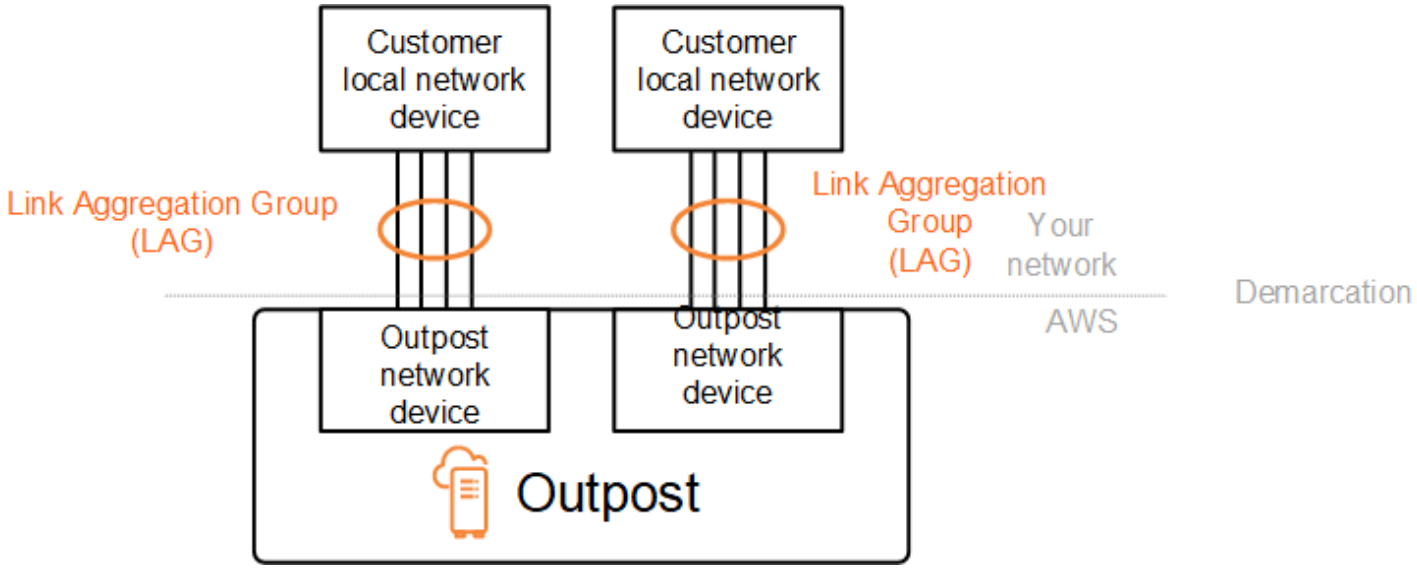
AWS Outposts verwendet das Link Aggregation Control Protocol (LACP), um zwei Link Aggregation Group (LAG)-Verbindungen herzustellen, eine von jedem Outpost-Netzwerkgerät zu jedem lokalen Netzwerkgerät. Die Links von jedem Outpost-Netzwerkgerät werden zu einer Ethernet-LAG zusammengefasst, die eine einzelne Netzwerkverbindung darstellt. Diese LAGs verwenden LACP mit Standard-Fasttimern. Sie können LAGs nicht so konfigurieren, dass sie langsame Timer verwenden.

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 über vier LAGs zwischen der Aggregationsebene der Outpost-Netzwerkgeräte und Ihren lokalen Netzwerkgeräten verfügen.

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



Virtuelle 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 VLANs für die Netzwerksegmentierung zwischen Datenpfaden.

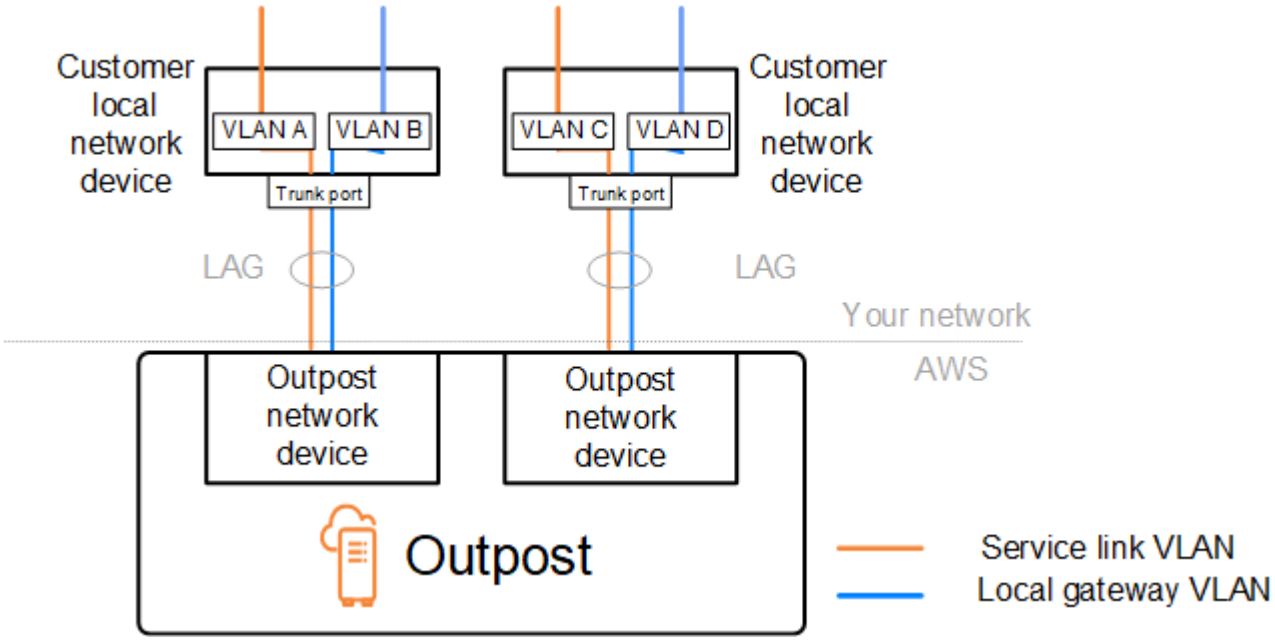
Jeder Outpost verfügt über die folgenden VLANs für die Kommunikation mit Ihren lokalen Netzwerkgeräten:

- 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 Instanzen 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 On-Premises-Netzwerk zu integrieren, müssen Sie die verwendeten VLANs den Outpost-Netzwerkgeräten und den On-Premises-Netzwerkgeräten des Kunden zuordnen. Sie müssen AWS diese Informationen vor der Installation angeben. Weitere Informationen finden Sie unter the section called “Checkliste zur Netzwerkbereitschaft”.

Netzwerk-Layer-Konnektivität

Um die Konnektivität auf der Netzwerkebene herzustellen, wird 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:

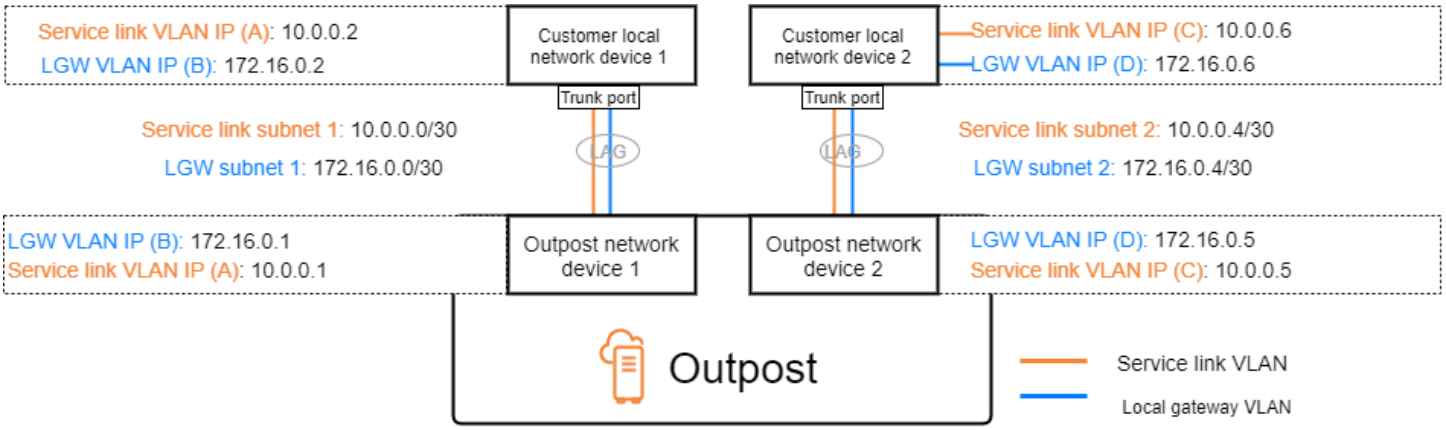
- Verwenden Sie ein dediziertes Subnetz mit einem /30- oder /31-CIDR, um diese logische point-to-point Konnektivität darzustellen.
- Stellen Sie keine Brücke zwischen den VLANs zwischen Ihren lokalen Netzwerkgeräten her.

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. Service Link Virtual Interfaces (VIFs) werden für diesen Pfad verwendet, um IP-Konnektivität und BGP-Sitzungen zwischen Ihrem Outpost und Ihren lokalen Netzwerkgeräten für die 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. Lokale Gateway-VIFs werden auf diesem Pfad 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 Beispiel gibt es vier VLANs:

- 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-OND 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-OND 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

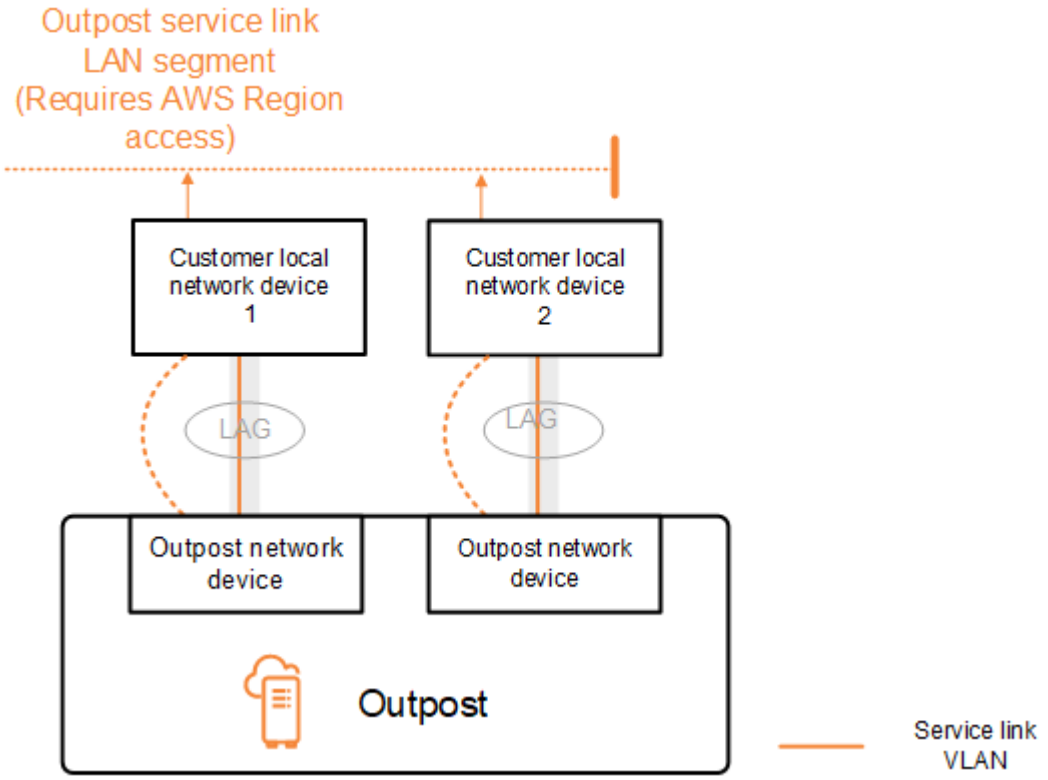
Service Link BGP-Konnektivität

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 IP-Adressen /30 oder /31 eingerichtet, die für das point-to-point VLAN bereitgestellt werden. Jede BGP-Peering-Sitzung verwendet eine private autonome Systemnnummer (ASN) auf dem Outpost-Netzwerkgerät und eine

ASN, die Sie für die lokalen Netzwerkgeräte Ihrer Kunden auswählen. AWS stellt die Attribute als Teil des Installationsprozesses bereit.

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 1 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 AWS-Region verwendet.

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 ONDs gleiche BGP-Präfixe mit denselben Attributen bewerben. 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 Datenverkehrsverlagerung erfordert gleiche BGP-Präfixe von Kundenseite für alle 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

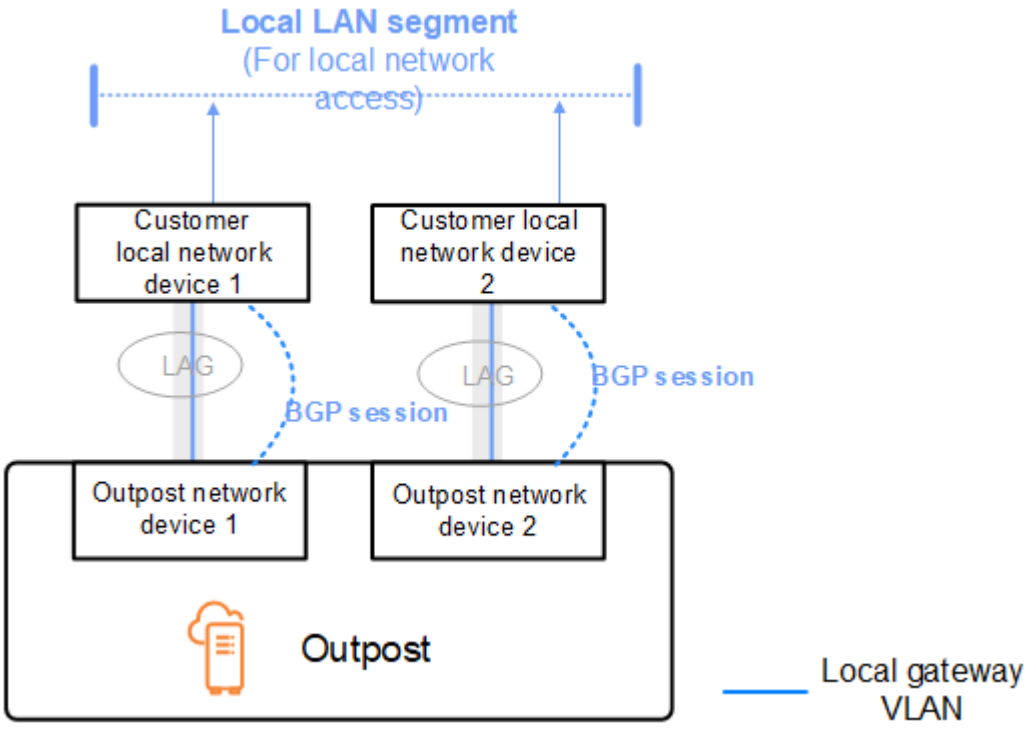
Der Outpost richtet ein externes BGP-Peering von jedem Outpost-Netzwerkgerät zu einem lokalen Netzwerkgerät ein, um die Konnektivität zum lokalen Gateway herzustellen. Es verwendet eine private autonome Systemnnummer (ASN), die Sie zuweisen, um die externen BGP-Sitzungen einzurichten. Jedes Outpost-Netzwerkgerät 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-IPs eingerichtet, die Sie beim Einrichten 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 stellt die Attribute im Rahmen des Vorinstallationsprozesses bereit.

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:

- AWS stellt das lokale Gateway BGP ASN bereit. 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.
- 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 von ONDs wegzuverlagern, 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 ONDs gleiche BGP-Präfixe mit denselben Attributen bewerben. 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 Datenverkehrsverlagerung erfordert gleiche BGP-Präfixe von Kundenseite für alle 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, um die Kommunikation mit Ihrem On-Premises-Netzwerk zu erleichtern. Sie können jedoch einen kundeneigenen IP-Adresspool (COIPs) bereitstellen.

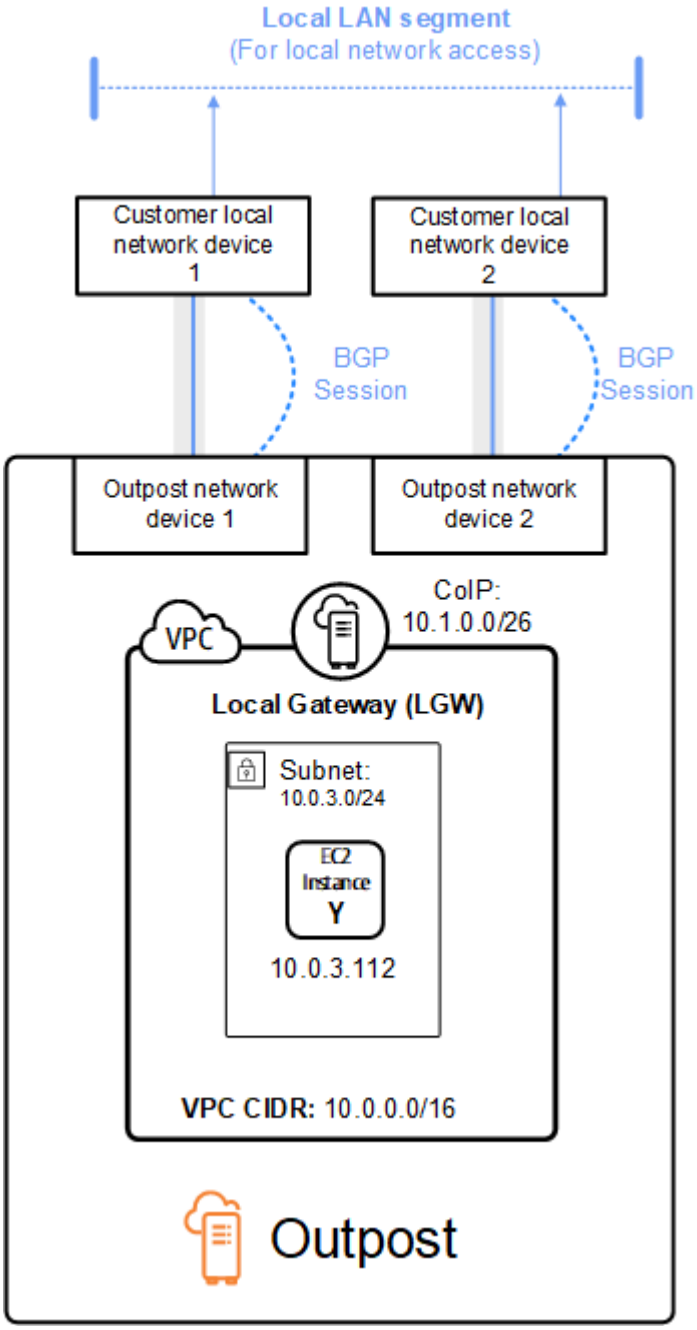
Wenn Sie sich für CoIP entscheiden, wird AWS den Pool anhand der Informationen erstellen, die Sie während des Installationsvorgangs angeben. Sie können Elastic IP-Adressen aus diesem Pool erstellen und die Adressen dann Ressourcen auf Ihrem Outpost zuweisen, wie z. B. EC2-Instanzen.

Das lokale Gateway übersetzt die elastische 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 elastische 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.
- Die Kommunikation zwischen Ihrem Outpost und dem On-Premises-Netzwerk verwendet die CoIP Elastic IPs, um Instances im Outpost 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

Mit gemeinsam genutzten AWS Outposts Ressourcen arbeiten

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, VPCs konfigurieren und Instances auf dem gemeinsam genutzten Outpost 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. Verbraucher können Ressourcen auf Outposts erstellen, die mit ihnen geteilt werden, genauso wie sie Ressourcen auf Outposts erstellen würden, die sie in ihrem eigenen Konto erstellen. Der Eigentümer ist für die Verwaltung des Outposts und der Ressourcen, die er darin erstellt, verantwortlich. Besitzer können die Freigabe jederzeit ändern oder widerrufen. Mit Ausnahme von Instances, die Kapazitätsreservierungen verbrauchen, können Besitzer auch Ressourcen einsehen, ändern und löschen, die Nutzer in geteilten Outposts erstellen. Besitzer sind nicht dazu befugt Instances, die Konsumenten in den von ihnen freigegebenen Kapazitätsreservierungen starten, zu ändern.

Verbraucher sind dafür verantwortlich, die Ressourcen zu verwalten, die sie in Outposts erstellen, die mit ihnen geteilt werden, einschließlich aller Ressourcen, die Kapazitätsreservierungen verbrauchen. Verbraucher können Ressourcen, die anderen Verbrauchern oder dem Outpost-Eigentümer gehören, nicht einsehen oder ändern. Sie können auch keine Outposts ändern, die mit ihnen geteilt wurden.

Ein Outpost-Besitzer kann Outpost-Ressourcen teilen mit:

- Spezifische AWS Konten innerhalb seiner Organisation in. AWS Organizations
- Eine Organisationseinheit innerhalb ihrer Organisation inAWS Organizations.
- Ihre gesamte Organisation inAWS Organizations.

Inhalt

- Freigeben in mehreren Availability Zones
- Eine Outpost-Ressource gemeinsam nutzen
- Aufheben der gemeinsamen Nutzung einer gemeinsam genutzten Outpost-Ressource
- Identifizieren einer gemeinsam genutzten Outpost-Ressource
- Gemeinsam genutzte Outpost-Ressourcenberechtigungen
- Fakturierung und Messung
- Einschränkungen

Gemeinsam nutzbare Outpost-Ressourcen

Ein Outpost-Besitzer kann die in diesem Abschnitt aufgeführten Outpost-Ressourcen mit Verbrauchern teilen.

Informationen zu Serverressourcen finden Sie unter Arbeiten mit gemeinsam genutzten AWS Outposts Ressourcen im AWS Outposts Benutzerhandbuch für Outposts-Server.

- Zugewiesene Dedicated Hosts — Verbraucher mit Zugriff auf diese Ressource können:
  - EC2-Instances auf einem Dedicated Host starten und ausführen.
- Kapazitätsreservierungen — Verbraucher mit Zugriff auf diese Ressource können:
  - Identifizieren Sie Kapazitätsreservierungen, die mit ihnen geteilt wurden.
  - Starten und verwalten Sie Instances, die Kapazitätsreservierungen verbrauchen.
- Kundeneigene IP-Adresspools (CoIP) — Verbraucher mit Zugriff auf diese Ressource können:
  - Kundeneigene IP-Adressen zuweisen und diesen Instanzen zuordnen.
- Routing-Tabellen für lokale Gateways — Verbraucher mit Zugriff auf diese Ressource können:
  - Erstellen und verwalten Sie VPC-Zuordnungen zu einem lokalen Gateway.
  - Sehen Sie sich die Konfigurationen der lokalen Gateway-Routentabellen und virtuellen Schnittstellen an.
- Outposts — Verbraucher mit Zugang zu dieser Ressource können:
  - Subnetze auf dem Outpost erstellen und verwalten.
  - Erstellen und verwalten Sie EBS-Volumes auf dem Outpost.
  - Verwenden Sie die AWS Outposts API, um Informationen über den Outpost einzusehen.
- S3 auf Outposts — Verbraucher mit Zugriff auf diese Ressource können:

  - S3-Buckets, Access Points und Endpoints auf dem Outpost erstellen und verwalten.
- Websites — Verbraucher mit Zugriff auf diese Ressource können:
  - Einen Außenposten am Standort einrichten, verwalten und kontrollieren.
- Subnetze — Verbraucher mit Zugriff auf diese Ressource können:
  - Informationen über Subnetze anzeigen.
  - Starten und führen Sie EC2-Instances in Subnetzen aus.

  Verwenden Sie die Amazon VPC-Konsole, um ein Outpost-Subnetz gemeinsam zu nutzen. Weitere Informationen finden Sie unter Sharing a Subnet im Amazon VPC-Benutzerhandbuch.

Voraussetzungen für die gemeinsame Nutzung von Outposts-Ressourcen

- Um eine Outpost-Ressource mit Ihrer Organisation oder einer Organisationseinheit gemeinsam zu nutzenAWS Organizations, müssen Sie das Teilen mit aktivieren. AWS Organizations Weitere Informationen finden Sie unter Freigabe für AWS Organizations aktivieren im AWS RAM-Benutzerhandbuch.
- Um eine Outpost-Ressource gemeinsam nutzen zu können, müssen Sie sie in Ihrem AWS Konto besitzen. Du kannst eine Outpost-Ressource, die mit dir geteilt wurde, nicht teilen.
- Um eine Outpost-Ressource gemeinsam zu nutzen, müssen Sie sie mit einem Konto innerhalb Ihrer Organisation teilen.

Zugehörige Services

Die gemeinsame Nutzung von Outpost-Ressourcen ist in AWS Resource Access Manager () AWS RAM integriert. AWS RAMist 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 handelnAWS 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. So befindet sich die Availability Zone `us-east-1a` für Ihr AWS-Konto möglicherweise nicht im selben Ort wie `us-east-1a` für ein anderes AWS-Konto.

Um den Standort Ihrer Outpost-Ressource im Verhältnis zu Ihren Konten zu ermitteln, müssen Sie die Availability Zone ID (AZ ID) verwenden. Die AZ-ID ist eine eindeutige, konsistente Kennung für eine Availability Zone innerhalb aller AWS-Konten. Beispielsweise ist `use1-az1` eine AZ-ID für die `us-east-1`-Region und ist derselbe Speicherort in jedem AWS-Konto.

So zeigen Sie die AZ-IDs für die Availability Zones in Ihrem Konto an

1. Öffnen Sie die AWS RAM-Konsole unter https://console.aws.amazon.com/ram.
2. Die AZ-IDs für die aktuelle Region werden im Feld Your AZ ID (Ihre AZ-ID) rechts im Bildschirm angezeigt.

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

Eine Outpost-Ressource gemeinsam nutzen

Wenn ein Besitzer einen Outposts mit einem Verbraucher teilt, kann der Verbraucher Ressourcen auf dem Außenposten erstellen, genauso wie er Ressourcen in Außenposten erstellen würde, die er in seinem eigenen Konto erstellt. Verbraucher mit Zugriff auf gemeinsam genutzte lokale Gateway-Routentabellen können VPC-Zuordnungen erstellen und verwalten. Weitere Informationen finden Sie unter Gemeinsam nutzbare Outpost-Ressourcen.

Um eine Outpost-Ressource gemeinsam zu nutzen, müssen Sie sie zu einer Ressourcenfreigabe hinzufügen. Eine Ressourcenfreigabe ist eine AWS RAM-Ressource, mit der Sie Ihre Ressourcen in mehreren 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 zu einer neuen Ressourcenfreigabe hinzuzufügen, 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 Verbraucher eine Einladung, dem Resource Share beizutreten, und erhalten nach Annahme der Einladung Zugriff auf die gemeinsam genutzte Outpost-Ressource.

Sie können eine Outpost-Ressource, die Sie besitzen, mit der AWS Outposts Konsole, AWS RAM der Konsole oder dem teilen. 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 den Außenposten aus und klicken Sie dann auf Aktionen, Details anzeigen.
4. Wählen Sie auf der Übersichtsseite von Outpost die Option Resource Shares aus.
5. Wählen Sie Create resource share (Ressourcenfreigabe erstellen) aus.

Sie werden zur AWS RAM Konsole weitergeleitet, um die gemeinsame Nutzung von Outpost abzuschließen. Gehen Sie dabei wie folgt vor. Gehen Sie ebenfalls wie folgt vor, um eine lokale Gateway-Routentabelle, die Sie besitzen, gemeinsam zu nutzen.

Um eine Outpost- oder Local-Gateway-Routentabelle, die Sie besitzen, über die AWS RAM Konsole gemeinsam zu nutzen

Siehe Erstellen einer Ressourcenfreigabe im AWS RAM-Benutzerhandbuch.

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

Verwenden Sie den create-resource-share-Befehl.

Aufheben der gemeinsamen Nutzung einer gemeinsam genutzten Outpost-Ressource

Wenn ein geteilter Outpost nicht mehr geteilt wird, können Verbraucher den Outpost nicht mehr in der Konsole sehen. AWS Outposts Sie können keine neuen Subnetze auf dem Outpost erstellen, keine neuen EBS-Volumes auf dem Outpost erstellen oder die Outpost-Details und Instance-Typen mit der Konsole oder dem anzeigen. AWS Outposts AWS CLI Bestehende Subnetze, Volumes oder Instances, die von Verbrauchern erstellt wurden, werden nicht gelöscht. Alle vorhandenen Subnetz-Verbraucher, die auf dem Outpost erstellt wurden, können weiterhin zum Starten neuer Instances verwendet werden.

Wenn eine gemeinsam genutzte lokale Gateway-Routentabelle nicht mehr gemeinsam genutzt wird, können Verbraucher keine neuen VPC-Zuordnungen mehr zu ihr erstellen. Alle vorhandenen VPC-Zuordnungen, die von Verbrauchern erstellt wurden, bleiben mit der Routentabelle verknüpft. Ressourcen in diesen VPCs können den Verkehr weiterhin an das lokale Gateway weiterleiten.

Um die gemeinsame Nutzung einer Outpost-Ressource, die Sie besitzen, rückgängig zu machen, müssen Sie sie aus der Ressourcenfreigabe entfernen. Hierfür können Sie die AWS RAM-Konsole oder die AWS CLI verwenden.

Um die gemeinsame Nutzung einer 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 gemeinsam genutzten Outpost-Ressource

Eigentümer und Verbraucher können gemeinsam genutzte Outposts über die AWS Outposts Konsole und AWS CLI identifizieren. Sie können gemeinsam genutzte lokale Gateway-Routentabellen mithilfe der AWS CLI identifizieren.

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

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 Außenposten aus und klicken Sie dann auf Aktionen, Details anzeigen.
4. Sehen Sie sich auf der Übersichtsseite des Outposts die Besitzer-ID an, um die AWS Konto-ID des Outpost-Inhabers zu identifizieren.

Um eine gemeinsam genutzte Outpost-Ressource zu identifizieren, verwenden Sie den 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.

Gemeinsam genutzte Outpost-Ressourcenberechtigungen

Berechtigungen für Besitzer

Die Eigentümer sind für die Verwaltung des Outposts und der Ressourcen, die sie darin erstellen, 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

Verbraucher können Ressourcen auf Outposts erstellen, die mit ihnen geteilt werden, genauso wie sie Ressourcen auf Outposts erstellen würden, die sie in ihrem eigenen Konto erstellen. Die Verbraucher sind dafür verantwortlich, die Ressourcen zu verwalten, die sie auf Outposts bereitstellen, die mit ihnen geteilt werden. Verbraucher können keine Ressourcen ansehen oder ändern, die anderen Verbrauchern oder dem Outpost-Besitzer gehören, und sie können Outposts, die mit ihnen geteilt wurden, nicht ändern.

Fakturierung und Messung

Den Besitzern werden Outposts und Außenpostenressourcen in Rechnung gestellt, die sie gemeinsam nutzen. Ihnen werden auch alle Datenübertragungsgebühren in Rechnung gestellt, die mit dem Service Link-VPN-Verkehr ihrer Outpost aus der Region verbunden sind. AWS

Für die gemeinsame Nutzung lokaler Gateway-Routentabellen 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.

Verbrauchern werden Anwendungsressourcen in Rechnung gestellt, die sie auf gemeinsam genutzten Outposts erstellen, z. B. 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 OutpostsTeilen“. Weitere Informationen zu VPC-Freigabelimits finden Sie unter Einschränkungen im Amazon Virtual Private Cloud Cloud-Benutzerhandbuch.
- Servicekontingente werden auf einzelne Konten angewendet.

Sicherheit in AWS Outposts

Sicherheit bei AWS hat höchste Priorität. Als - AWS Kunde profitieren Sie von einer Rechenzentrums- und Netzwerkarchitektur, die entwickelt wurde, um die Anforderungen der sicherheitskritischsten Organisationen zu erfüllen.

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

- Sicherheit der Cloud – AWS ist für den Schutz der Infrastruktur verantwortlich, die AWS Services in der AWS Cloud ausführt. stellt Ihnen AWS außerdem Services bereit, die Sie sicher nutzen können. Externe Prüfer testen und überprüfen im Rahmen der AWS Compliance-Programme regelmäßig die Wirksamkeit unserer Sicherheit. Informationen zu den Compliance-Programmen, die für gelten AWS Outposts, finden Sie unter AWS Im Rahmen des Compliance-Programms zugelassene -ServicesIm.
- Sicherheit in der Cloud – Ihre Verantwortung wird durch den - AWS Service bestimmt, den Sie verwenden. 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 finden Sie unter AWS Outposts Häufig gestellte AWS Outposts Fragen zu Rack.

Diese Dokumentation hilft Ihnen zu verstehen, wie Sie das Modell der geteilten Verantwortung bei der Verwendung von einsetzen können AWS Outposts. Es zeigt Ihnen, wie Sie Ihre Sicherheits- und Compliance-Ziele zu erreichen. Sie erfahren auch, wie Sie andere - AWS Services verwenden, die Sie bei der Überwachung und Sicherung Ihrer -Ressourcen unterstützen.

Inhalt

Datenschutz in AWS Outposts

Das AWS Modell der geteilten VerantwortungModell gilt für den Datenschutz in AWS Outposts. Wie in diesem Modell beschrieben, AWS ist für den Schutz der globalen Infrastruktur verantwortlich, die alle ausführt AWS Cloud. Sie sind dafür verantwortlich, die Kontrolle über Ihre in dieser Infrastruktur gehosteten Inhalte zu behalten. Dieser Inhalt umfasst die Sicherheitskonfigurations- und Verwaltungsaufgaben für die AWS-Services , die Sie verwenden.

Aus Datenschutzgründen empfehlen wir Ihnen, die AWS-Konto Anmeldeinformationen zu schützen und einzelne Benutzer mit AWS IAM Identity Center oder AWS Identity and Access Management (IAM) einzurichten. 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 werden AWS Outposts 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-Verschlüsselung im Amazon-EC2-Benutzerhandbuch.

Verschlüsselung während der Übertragung

AWS verschlüsselt Daten während der Übertragung zwischen Ihrem Outpost und seiner AWS Region. Weitere Informationen finden Sie unter Konnektivität über Service Links.

Sie können ein Verschlüsselungsprotokoll wie Transport Layer Security (TLS) verwenden, um sensible Daten bei 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 gesäubert (mit Null überschrieben), bevor er einer neuen Instance zugewiesen wird. 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 Service, mit dem ein Administrator den Zugriff auf - AWS Ressourcen sicher steuern kann. IAM-Administratoren steuern, wer für die Nutzung von - AWS Outposts Ressourcen authentifiziert (angemeldet) und autorisiert (im Besitz von Berechtigungen) werden kann. Sie können IAM ohne zusätzliche Kosten nutzen.

Inhalt

Funktionsweise von AWS Outposts mit IAM

Bevor Sie IAM verwenden, um den Zugriff auf AWS Outposts zu verwalten, erfahren Sie, welche IAM-Funktionen Sie mit AWS Outposts verwenden können.

IAM-Funktionen, die Sie mit AWS Outposts verwenden können

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

IAM-Feature	AWS Outposts-Unterstützung
Richtlinienbedingungsschlüssel (servicespezifisch)	Ja
ACLs	Nein
ABAC (Tags in Richtlinien)	Ja
Temporäre Anmeldeinformationen	Ja
Hauptberechtigungen	Ja
Servicerollen	Nein
Serviceverknüpfte Rollen	Ja

Identitätsbasierte Richtlinien für AWS Outposts

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 Erstellen von IAM-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 AWS Outposts

Beispiele für identitätsbasierte AWS Outposts-Richtlinien finden Sie unter AWS Beispiele für Outposts-Richtlinien.

Ressourcenbasierte Richtlinien in AWS Outposts

Unterstützt ressourcenbasierte Richtlinien	Nein

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und Amazon-S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben. Prinzipale können Konten, Benutzer, Rollen, Verbundbenutzer oder umfassen AWS-Services.

Um kontoübergreifenden Zugriff zu ermöglichen, können Sie ein gesamtes Konto oder IAM-Entitäten in einem anderen Konto als Prinzipal in einer ressourcenbasierten Richtlinie angeben. Durch das Hinzufügen eines kontoübergreifenden Auftraggebers zu einer ressourcenbasierten Richtlinie ist nur die halbe Vertrauensbeziehung eingerichtet. Wenn sich der Prinzipal und die Ressource in unterschiedlichen befinden AWS-Konten, muss ein IAM-Administrator im vertrauenswürdigen Konto auch der Prinzipal-Entität (Benutzer oder Rolle) die Berechtigung für den Zugriff auf die Ressource erteilen. Sie erteilen Berechtigungen, indem Sie der juristischen Stelle eine identitätsbasierte Richtlinie anfügen. Wenn jedoch eine ressourcenbasierte Richtlinie Zugriff auf einen Prinzipal in demselben Konto gewährt, ist keine zusätzliche identitätsbasierte Richtlinie erforderlich. Weitere Informationen finden Sie unter Wie sich IAM-Rollen von ressourcenbasierten Richtlinien unterscheiden im IAM-Benutzerhandbuch.

Richtlinienaktionen für AWS Outposts

Unterstützt Richtlinienaktionen	Ja

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

Das Element `Action` einer JSON-Richtlinie beschreibt die Aktionen, mit denen Sie den Zugriff in einer Richtlinie zulassen oder verweigern können. Richtlinienaktionen haben in der Regel denselben Namen wie die zugehörige AWS API-Operation. 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 Von definierte Aktionen AWS Outposts in der Service-Autorisierungs-Referenz.

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*"
```

Richtlinienressourcen für AWS Outposts

Unterstützt Richtlinienressourcen	Ja

Administratoren können AWS JSON-Richtlinien verwenden, um anzugeben, wer Zugriff auf was hat. Das bedeutet die Festlegung, welcher Prinzipal Aktionen für welche Ressourcen 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 die ARNs durch Kommata voneinander.

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

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

Richtlinienbedingungsschlüssel für AWS Outposts

Unterstützt servicespezifische Richtlini enbedingungsschlüssel	Ja

Administratoren können AWS JSON-Richtlinien verwenden, um anzugeben, wer Zugriff auf was 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 servicespezifische Bedingungsschlüssel. Informationen zum Anzeigen aller AWS globalen Bedingungsschlüssel finden Sie unter AWS Globale Bedingungskontextschlüssel im IAM-Benutzerhandbuch.

Eine Liste der AWS Outposts-Bedingungsschlüssel finden Sie unter Bedingungsschlüssel für AWS Outposts in der Service-Autorisierungs-Referenz. Informationen dazu, mit welchen Aktionen und Ressourcen Sie einen Bedingungsschlüssel verwenden können, finden Sie unter Von definierte Aktionen AWS Outposts.

Beispiele für identitätsbasierte AWS Outposts-Richtlinien finden Sie unter AWS Beispiele für Outposts-Richtlinien.

ACLs in AWS Outposts

Unterstützt ACLs	Nein

Zugriffssteuerungslisten (ACLs) steuern, welche Prinzipale (Kontomitglieder, Benutzer oder Rollen) auf eine Ressource zugreifen können. ACLs sind ähnlich wie ressourcenbasierte Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

ABAC mit AWS Outposts

Unterstützt ABAC (Tags in Richtlinien)	Ja

Die attributbasierte Zugriffskontrolle (ABAC) ist eine Autorisierungsstrategie, bei der Berechtigungen basierend auf Attributen definiert werden. In werden AWS diese Attribute als Tags bezeichnet. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und an viele AWS Ressourcen anfügen. 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 Was ist ABAC? im IAM-Benutzerhandbuch. Um ein Tutorial mit Schritten zur Einstellung von ABAC anzuzeigen, siehe Attributbasierte Zugriffskontrolle (ABAC) verwenden im IAM-Benutzerhandbuch.

Verwenden temporärer Anmeldeinformationen mit AWS Outposts

Unterstützt temporäre Anmeldeinformationen	Ja

Einige funktionieren AWS-Services nicht, wenn Sie sich mit temporären Anmeldeinformationen anmelden. Weitere Informationen, einschließlich der , die mit temporären Anmeldeinformationen AWS-Services funktionieren, finden Sie unter AWS-Services , die mit IAM funktionieren im IAM-Benutzerhandbuch.

Sie verwenden temporäre Anmeldeinformationen, wenn Sie sich AWS Management Console mit einer anderen Methode als einem Benutzernamen und einem Passwort bei der anmelden. Wenn Sie beispielsweise AWS über den SSO-Link (Single Sign-On) Ihres Unternehmens auf zugreifen, erstellt dieser Prozess automatisch temporäre Anmeldeinformationen. 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 zu einer Rolle (Konsole) im IAM-Benutzerhandbuch.

Sie können temporäre Anmeldeinformationen manuell mit der AWS CLI oder der AWS API erstellen. Sie können diese temporären Anmeldeinformationen dann verwenden, um auf zuzugreifen

AWS. AWS empfohlen, temporäre Anmeldeinformationen dynamisch zu generieren, anstatt langfristige Zugriffsschlüssel zu verwenden. Weitere Informationen finden Sie unter Temporäre Sicherheitsanmeldeinformationen in IAM.

Serviceübergreifende Prinzipalberechtigungen für AWS Outposts

Unterstützt Forward Access Sessions (FAS)	Ja

Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle verwenden, um Aktionen in auszuführen AWS, gelten Sie als Prinzipal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service auslösen. FAS verwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, in Kombination mit der Anforderung AWS-Service , Anforderungen an nachgelagerte Services zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Service eine Anfrage erhält, die Interaktionen mit anderen AWS-Services oder -Ressourcen erfordert. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anfragen finden Sie unter Zugriffssitzungen weiterleiten.

Servicerollen für AWS -Outposts

Unterstützt Servicerollen	Nein

Eine Servicerolle ist eine IAM-Rolle, die ein Service annimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern und löschen. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service im IAM-Benutzerhandbuch.

Serviceverknüpfte Rollen für AWS Outposts

Unterstützt serviceverknüpfte Rollen	Ja

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

Weitere Informationen zum Erstellen oder Verwalten von serviceverknüpften AWS Outposts-Rollen finden Sie unter Verwenden von serviceverknüpften Rollen für AWS Outposts.

AWS Beispiele für Outposts-Richtlinien

Benutzer und Rollen besitzen standardmäßig keine Berechtigungen zum Erstellen oder Ändern von AWS Outposts-Ressourcen. 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 im IAM-Benutzerhandbuch.

Einzelheiten zu Aktionen und Ressourcentypen, die von AWS Outposts definiert werden, einschließlich des Formats der ARNs für die einzelnen Ressourcentypen, finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für AWS Outposts in der Service-Autorisierungs-Referenz.

Inhalt

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:

- Erste Schritte mit von AWS verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen – Um Ihren Benutzern und Workloads Berechtigungen zu erteilen, verwenden Sie die von AWS verwalteten Richtlinien, die Berechtigungen für viele häufige Anwendungsfälle 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 für Ihre Anwendungsfälle spezifisch 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 Service-Aktionen zu gewähren, wenn sie über eine bestimmte verwendet werden AWS-Service, z. B. AWS CloudFormation. 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 zum 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 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 Konfigurieren eines MFA-geschützten API-Zugriffs 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"
    }
  ]
}
```

Verwenden von serviceverknüpften Rollen für AWS Outposts

AWS Outposts verwendet AWS Identity and Access Management (IAM) serviceverknüpfte Rollen . Eine serviceverknüpfte Rolle ist ein spezieller Typ einer IAM-Rolle, die direkt mit verknüpft ist AWS Outposts. Serviceverknüpfte Rollen werden von vordefiniert AWS Outposts und schließen alle Berechtigungen ein, die der Service zum Aufrufen anderer - AWS Services in Ihrem Namen erfordert.

Eine serviceverknüpfte Rolle macht die Einrichtung Ihres AWS Outposts effizienter, da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. AWS Outposts definiert die Berechtigungen seiner serviceverknüpften Rollen. Sofern keine andere Konfiguration festgelegt wurde, AWS Outposts kann nur die Rollen übernehmen. Die definierten Berechtigungen umfassen die Vertrauens- und Berechtigungsrichtlinie. Diese Berechtigungsrichtlinie kann keinen anderen IAM-Entitäten zugewiesen werden.

Sie können eine serviceverknüpfte Rolle erst löschen, nachdem die zugehörigen Ressourcen gelöscht wurden. Dies schützt Ihre AWS Outposts Ressourcen, da Sie nicht versehentlich die Berechtigung für den Zugriff auf die Ressourcen entfernen können.

Informationen zu anderen Services, die serviceverknüpften Rollen unterstützen, finden Sie unter AWS -Services, die mit IAM funktionieren. Suchen Sie nach den Services, für die Ja in der Spalte Serviceverknüpfte Rolle angegeben ist. Wählen Sie über einen Link Ja aus, um die Dokumentation zu einer serviceverknüpften Rolle für diesen Service anzuzeigen.

Berechtigungen von serviceverknüpften Rollen für AWS Outposts

AWS Outposts verwendet die serviceverknüpfte Rolle namens AWSServiceRoleForOutposts_***OutpostID*** – Ermöglicht Outposts den Zugriff auf AWS Ressourcen für private Konnektivität in Ihrem Namen. Diese dienstbezogene Rolle ermöglicht die Konfiguration privater Konnektivität, erstellt Netzwerkschnittstellen und fügt sie Service Link-Endpunkt-Instances hinzu.

Die serviceverknüpfte Rolle AWSServiceRoleForOutposts_*OutpostID* vertraut darauf, dass die folgenden Services die Rolle übernehmen:

- `outposts.amazonaws.com`

Die serviceverknüpfte Rolle AWSServiceRoleForOutposts_***OutpostID*** enthält die folgenden Richtlinien:

- AWSOutpostsServiceRolePolicy
- AWSOutpostsPrivateConnectivityPolicy_***OutpostID***

Die AWSOutpostsServiceRolePolicy Richtlinie ist eine serviceverknüpfte Rollenrichtlinie, die den Zugriff auf von verwaltete AWS Ressourcen ermöglicht AWS Outposts.

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

- Aktion: `ec2:DescribeNetworkInterfaces` für `all AWS resources`
- Aktion: `ec2:DescribeSecurityGroups` für `all AWS resources`
- Aktion: `ec2:CreateSecurityGroup` für `all AWS resources`
- Aktion: `ec2:CreateNetworkInterface` für `all AWS resources`

Die AWSOutpostsPrivateConnectivityPolicy_*OutpostID*-Richtlinie erlaubt AWS Outposts , die folgenden Aktionen für die angegebenen Ressourcen durchzuführen:

- Aktion: `ec2:AuthorizeSecurityGroupIngress` für `all AWS resources that match the following Condition:`

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

- Aktion: `ec2:AuthorizeSecurityGroupEgress` für `all AWS resources that match the following Condition:`

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

- Aktion: `ec2:CreateNetworkInterfacePermission` für `all AWS resources that match the following Condition:`

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

- Aktion: `ec2:CreateTags` für `all AWS resources that match the following Condition:`

```
{ "StringLike" : { "aws:RequestTag/outposts:private-connectivity-resourceId" :
 "{{OutpostId}}*"}}
```

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 Rollenberechtigungen im IAM-Benutzerhandbuch.

Erstellen einer serviceverknüpften Rolle für AWS Outposts

Sie müssen eine serviceverknüpfte Rolle nicht manuell erstellen. Wenn Sie 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 Service Link-Konnektivität mithilfe von VPC.

Bearbeiten einer serviceverknüpften Rolle für AWS Outposts

AWS Outposts erlaubt Ihnen nicht, die serviceverknüpfte Rolle AWSServiceRoleForOutposts_*OutpostID* zu bearbeiten. Da möglicherweise verschiedene Entitäten auf die Rolle verweisen, kann der Rollenname nach dem Erstellen einer serviceverknüpften Rolle nicht mehr geändert werden. Sie können jedoch die Beschreibung der Rolle mit IAM bearbeiten. Weitere Informationen finden Sie unter Bearbeiten einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Löschen einer serviceverknüpften 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.

> **Note**
>
> Wenn der AWS Outposts Service 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.

> **Warning**
>
> Sie müssen Ihren Outpost löschen, bevor Sie die serviceverknüpfte Rolle AWSServiceRoleForOutposts_*OutpostID* löschen können. Mit dem folgenden Verfahren wird Ihr Outpost gelöscht.

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

So löschen Sie AWS Outposts Ressourcen, die von der AWSServiceRoleForOutposts_***OutpostID*** verwendet werden

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

So löschen Sie die serviceverknüpfte Rolle mit IAM

Verwenden Sie die IAM-Konsole, die oder die - AWS API AWS CLI, um die serviceverknüpfte Rolle AWSServiceRoleForOutposts_*OutpostID* zu löschen. Weitere Informationen finden Sie unter Löschen einer serviceverknüpften Rolle im IAM-Leitfaden.

Unterstützte Regionen für serviceverknüpfte AWS Outposts -Rollen

AWS Outposts unterstützt die Verwendung von serviceverknüpften Rollen in allen Regionen, in denen der Service verfügbar ist. Weitere Informationen finden Sie unter AWS Outposts Endpunkte und -Kontingente.

AWS Von verwaltete Richtlinien für AWS Outposts

Eine AWS von verwaltete Richtlinie ist eine eigenständige Richtlinie, die von erstellt und verwaltet wird AWS. Von AWS verwaltete Richtlinien sind so konzipiert, dass sie Berechtigungen für viele häufige Anwendungsfälle bereitstellen, sodass Sie mit der Zuweisung von Berechtigungen für Benutzer, Gruppen und Rollen beginnen können.

Beachten Sie, dass von AWS verwaltete Richtlinien möglicherweise keine Berechtigungen mit den geringsten Berechtigungen für Ihre spezifischen Anwendungsfälle gewähren, da sie für alle - AWS Kunden verfügbar sind. Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie kundenverwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind.

Sie können die in verwalteten AWS Richtlinien definierten Berechtigungen nicht ändern. Wenn die in einer AWS von verwalteten Richtlinie definierten Berechtigungen AWS aktualisiert, wirkt sich die Aktualisierung auf alle Prinzipalidentitäten (Benutzer, Gruppen und Rollen) aus, denen die Richtlinie angefügt ist. aktualisiert am AWS wahrscheinlichsten eine von AWS verwaltete Richtlinie, wenn ein neuer gestartet AWS-Service wird oder neue API-Operationen für vorhandene Services verfügbar werden.

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

AWS Von verwaltete Richtlinie: AWSOutpostsServiceRolePolicy

Diese Richtlinie ist an eine serviceverknüpfte Rolle angehängt, die es ermöglicht AWS Outposts , Aktionen in Ihrem Namen durchzuführen. Weitere Informationen finden Sie unter Verwenden von serviceverknüpften Rollen.

AWS Von verwaltete Richtlinie: AWSOutpostsPrivateConnectivityPolicy

Diese Richtlinie ist an eine serviceverknüpfte Rolle angehängt, die es ermöglicht AWS Outposts , Aktionen in Ihrem Namen durchzuführen. Weitere Informationen finden Sie unter Verwenden von serviceverknüpften Rollen.

AWS Outposts -Aktualisierungen für - AWS verwaltete Richtlinien

Anzeigen von Details zu Aktualisierungen für - AWS verwaltete Richtlinien für , AWS Outposts seit dieser Service mit der Verfolgung dieser Änderungen begonnen hat.

Änderung	Beschreibung	Datum
AWS Outposts hat mit der Verfolgung von Änderungen begonnen	AWS Outposts hat mit der Verfolgung von Änderungen für seine AWS -verwalteten Richtlinien begonnen.	03. Dezember 2019

Infrastruktursicherheit in AWS Outposts

Als verwalteter Service ist AWS Outposts durch die AWS globale Netzwerksicherheit von geschützt. Informationen zu AWS Sicherheitsservices und wie die Infrastruktur AWS schützt, finden Sie unter AWS Cloud-Sicherheit. Informationen zum Entwerfen Ihrer AWS Umgebung mit den bewährten Methoden für die Infrastruktursicherheit finden Sie unter Infrastrukturschutz in Security Pillar AWS Well-Architected Framework.

Sie verwenden durch 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 GuardDuty zur Analyse in CloudWatch Logs, Amazon S3 oder in Amazon veröffentlicht werden können. Daten müssen zur Veröffentlichung an diese Services an die Region zurückgesendet werden, sodass sie von CloudWatch oder anderen Services nicht sichtbar sind, wenn sich der Outpost in einem getrennten Zustand befindet.

Überwachung von AWS Outposts Geräten durch die Vorherrschende

Stellen Sie sicher, dass niemand die AWS Outposts Ausrüstung ändert, ändert, Techniker umkehrt oder manipuliert. AWS Outposts Es kann mit einer Manipulationsüberwachung ausgestattet sein, um die Einhaltung der AWS Servicebedingungen sicherzustellen.

Ausfallsicherheit in AWS Outposts

AWS Outposts ist so konzipiert, dass es hochverfügbar ist. Outpost-Racks sind mit redundanter Stromversorgung 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 Metriken zur CloudWatch Kapazitätsverfügbarkeit von Amazon verwenden und Alarme festlegen, 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.

Compliance-Validierung für AWS Outposts

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

Sie können Auditberichte von Drittanbietern mit herunterladen AWS Artifact. Weitere Informationen finden Sie unter Herunterladen von Berichten unter AWS Artifact .

Ihre Compliance-Verantwortung bei der Verwendung von 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 Unterstützung der Compliance bereit:

- Schnellstartanleitungen für Sicherheit und Compliance – In diesen Bereitstellungsleitfäden werden Überlegungen zur Architektur erörtert und Schritte für die Bereitstellung von Basisumgebungen in bereitgestellt AWS , die sich auf Sicherheit und Compliance konzentrieren.
- Architekturerstellung für HIPAA-Sicherheit und -Compliance in Amazon Web Services – In diesem Whitepaper wird beschrieben, wie Unternehmen mithilfe AWS von HIPAA-berechtigte Anwendungen erstellen können.

> **Note**
>
> Nicht alle AWS-Services sind HIPAA-berechtigt. Weitere Informationen finden Sie in der Referenz für HIPAA-berechtigte Services.

- AWS Compliance-Ressourcen – Diese Sammlung von Arbeitsmappen und Leitfäden könnte für Ihre Branche und Ihren Standort gelten.
- AWS Kunden-Compliance-Leitfäden – Verstehen Sie das Modell der geteilten Verantwortung anhand der Compliance. Die Leitfäden fassen die bewährten Methoden zur Sicherung zusammen AWS-Services und ordnen die Leitlinien den Sicherheitskontrollen in mehreren Frameworks zu (einschließlich National Institute of Standards and Technology (NIST), Payment Card Industry Security Standards Officer (PCI) und International Organization for Standardization (ISO)).
- Bewertung von Ressourcen mit Regeln im -AWS Config Entwicklerhandbuch – Der AWS Config Service bewertet, wie gut Ihre Ressourcenkonfigurationen internen Praktiken, Branchenrichtlinien und Vorschriften entsprechen.
- AWS Security Hub – Dies AWS-Service bietet einen umfassenden Überblick über Ihren Sicherheitsstatus innerhalb von AWS. Security Hub verwendet Sicherheitskontrollen, um Ihre AWS -Ressourcen zu bewerten und Ihre Einhaltung von Sicherheitsstandards und bewährten Methoden zu überprüfen. Eine Liste der unterstützten Services und Kontrollen finden Sie in der Security-Hub-Steuerungsreferenz.
- AWS Audit Manager – Auf diese AWS-Service Weise können Sie Ihre AWS Nutzung kontinuierlich überprüfen, um den Umgang mit Risiken und die Einhaltung von Branchenstandards zu vereinfachen.

Internetzugang für AWS Outposts Workloads

In diesem Abschnitt wird erläutert, wie AWS Outposts Workloads wie folgt auf das Internet zugreifen können:

- Über die übergeordnete AWS Region
- 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 AWS Region auf das Internet zu. Der ausgehende Datenverkehr zum Internet kann über das NAT-Gateway erfolgen, das in Ihrer VPC instanziiert ist. Für zusätzliche Sicherheit für Ihren ein- und ausgehenden Datenverkehr können Sie AWS Sicherheitsservices wie AWS WAF AWS Shield und Amazon CloudFront in der AWS Region verwenden.

Informationen zur Routing-Tabelleneinstellung im Outposts-Subnetz finden Sie unter Routing-Tabellen des lokalen Gateways.

Überlegungen

- Verwenden Sie diese Option, wenn:
  - Sie benötigen Flexibilität, um den Internetdatenverkehr mit mehreren AWS Services in der AWS Region zu sichern.
  - Sie haben keinen Internet-Präsenzpunkt in Ihrem Rechenzentrum oder Ihrer Co-Location-Einrichtung.
- Bei dieser Option muss der Datenverkehr durch die übergeordnete AWS Region geleitet werden, 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 On-Demand-Preise für Amazon EC2.
- 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 führt.

Internetzugang über das Netzwerk Ihres lokalen Rechenzentrums

Bei dieser Option greifen die Workloads, die sich in den Outposts befinden, über Ihr lokales Rechenzentrum auf das Internet zu. Der Workload-Datenverkehr, 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 Outposts-Workload-Datenverkehrs verantwortlich.

Informationen zur Routing-Tabelleneinstellung im Outposts-Subnetz finden Sie unter Routing-Tabellen des lokalen Gateways.

Überlegungen

- Verwenden Sie diese Option, wenn:
  - Ihre Workloads erfordern Zugriff mit geringer Latenz auf Internetservices.
  - Sie möchten vermeiden, dass Datenübertragungsgebühren (DTO) anfallen.
  - Sie möchten die Service Link-Bandbreite für den Datenverkehr auf Steuerebene beibehalten.
- Ihre Sicherheitsebene ist dafür verantwortlich, den Workload-Datenverkehr von Outposts zu sichern.
- Wenn Sie sich für Direct VPC Routing (DVR) entscheiden, müssen Sie sicherstellen, dass die Outposts-CIDRs nicht mit den On-Premises-CIDRs in Konflikt stehen.
- Wenn die Standardroute (0/0) über das lokale Gateway (LGW) propagiert 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-Instance und dem Internet, der über Ihr lokales Rechenzentrum geleitet wird.

Überwachen eines Outpost

AWS Outposts wird in die folgenden Services integriert, die Überwachungs- und Protokollierungsfunktionen bieten:

CloudWatch -Metriken

Verwenden Sie Amazon CloudWatch , um Statistiken über Datenpunkte für Ihre Outposts 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 -Metriken für AWS Outposts.

CloudTrail -Protokolle

Verwenden Sie AWS CloudTrail, um detaillierte Informationen über die Aufrufe von AWS-APIs zu erfassen. Sie können diese Aufrufe als Protokolldateien in Amazon S3 speichern. Sie können diese CloudTrail Protokolle verwenden, um Informationen wie den getätigten Aufruf, die Quell-IP-Adresse, von der der Aufruf stammte, den Initiator des Aufrufs und den Zeitpunkt des Aufrufs zu ermitteln.

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 AWS Outposts -Informationen in 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 den Netzwerkverkehr von Outpost zu kopieren und an out-of-band Sicherheits- und Überwachungsgeräte in Outpost weiterzuleiten. Sie können den gespiegelten Datenverkehr zur Inhaltsinspektion, Bedrohungsüberwachung oder Fehlerbehebung verwenden. Weitere Informationen finden Sie im Traffic Mirroring Guide für Amazon Virtual Private Cloud.

AWS Health Dashboard

AWS Health Dashboard zeigt Informationen und Benachrichtigungen an, die durch Veränderungen 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. AWS Health Dashboard ist Teil des AWS Health-Dienstes, erfordert keine Einrichtung und kann von jedem Nutzer eingesehen werden, der in Ihrem Konto authentifiziert ist. Weitere Informationen finden Sie unter Erste Schritte mit AWS Health Dashboard.

CloudWatch -Metriken für AWS Outposts

AWS Outposts veröffentlicht Datenpunkte CloudWatch für Ihre Outposts in Amazon. CloudWatch ermöglicht es Ihnen, Statistiken zu diesen Datenpunkten als geordneten Satz von Zeitreihendaten abzurufen, die als Metriken bezeichnet werden. 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 kleiner als ist1, CloudWatch kann eine Aktion auslösen, z. B. das Senden einer Benachrichtigung an eine E-Mail-Adresse. Anschließend können Sie mögliche Netzwerkprobleme vor Ort 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 On-Premises-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-Alarmen im Amazon- CloudWatch Benutzerhandbuch. Weitere Informationen zu CloudWatchfinden Sie im Amazon CloudWatch -Benutzerhandbuch.

Inhalt

Outpost-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`.

Dimensionen für lokale Gateway-VIFs (lgw-vif): `OutpostsId`, `VirtualInterfaceGroupId` und `VirtualInterfaceId`

Dimensionen für Service Link-VIFs (sl-vif): `OutpostsId` Dimensionen `VirtualInterfaceId`

`IfTrafficOut`

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

Einheit: Bits pro Sekunde

Maximale Auflösung: 5 Minuten

Statistiken: Die nützlichsten Statistiken sind `Max` und `Min`.

Dimensionen für lokale Gateway-VIFs (lgw-vif): `OutpostsId`, `VirtualInterfaceGroupId` und `VirtualInterfaceId`

Dimensionen für Service Link-VIFs (sl-vif): `OutpostsId` Dimensionen `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 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 im Outpost für On-Demand-Kapazitätsreservierungen (ODCR) verfügbar sind. Diese Metrik misst Amazon EC2 Reserved Instances nicht.

Einheit: Anzahl

Maximale Auflösung: 5 Minuten

Dimensionen: `InstanceType` und `OutpostId`

`UsedReservedInstances`

Die Anzahl der Instances, die im Outpost für On-Demand-Kapazitätsreservierungen (ODCR) verfügbar sind. Diese Metrik misst Amazon EC2 Reserved Instances nicht.

Einheit: Anzahl

Maximale Auflösung: 5 Minuten

Dimensionen: `InstanceType` und `OutpostId`

`TotalReservedInstances`

Die Anzahl der Instances, die im Outpost für On-Demand-Kapazitätsreservierungen (ODCR) verfügbar sind. Diese Metrik misst Amazon EC2 Reserved Instances nicht.

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-Volumetyp 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-Volumetyp.

Einheit: Gigabyte

Maximale Auflösung: 5 Minuten

Statistiken: Die nützlichsten Statistiken sind `Average` und `pNN.NN` (Perzentile).

Dimensionen: `VolumeType` und `OutpostId`

Outpost-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.

Anzeigen von CloudWatch Metriken für Ihren Outpost

Sie können die CloudWatch Metriken für Ihre Load Balancer mithilfe der CloudWatch Konsole anzeigen.

So zeigen Sie Metriken mit der CloudWatch Konsole an

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.

So zeigen Sie Metriken mit der AWS CLI

Verwenden Sie den folgenden list-metrics-Befehl, um die verfügbaren Metriken aufzuführen.

```
aws cloudwatch list-metrics --namespace AWS/Outposts
```

So rufen Sie die Statistiken für eine Metrik mithilfe der AWS CLI ab

Verwenden Sie den folgenden get-metric-statistics Befehl, um Statistiken für die angegebene Metrik und Dimension abzurufen. CloudWatch erzeugt 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 von AWS Outposts-API-Aufrufen mit AWS CloudTrail

AWS Outposts ist in integriert, einem ServiceAWS CloudTrail, der die Aktionen eines Benutzers, einer Rolle oder eines -AWSServices in aufzeichnetAWS Outposts. CloudTrail erfasst alle API-Aufrufe für AWS Outposts als Ereignisse. Zu den erfassten Aufrufen gehören Aufrufe von der AWS Outposts-Konsole und Code-Aufrufe der AWS Outposts-API-Operationen. Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Bereitstellung von CloudTrail Ereignissen an einen S3-Bucket aktivieren, einschließlich Ereignissen für AWS Outposts. Wenn Sie keinen Trail konfigurieren, können Sie trotzdem die neuesten Ereignisse in der CloudTrail Konsole unter Ereignisverlauf anzeigen. Anhand der von CloudTrailgesammelten Informationen können Sie die an gestellte AnfrageAWS Outposts, die IP-Adresse, von der die Anfrage gestellt wurde, den Initiator der Anfrage, den Zeitpunkt der Anfrage und zusätzliche Details bestimmen.

Weitere Informationen zu CloudTrailfinden Sie im AWS CloudTrail -Benutzerhandbuch.

AWS Outposts -Informationen in CloudTrail

CloudTrail wird beim Erstellen des AWS Kontos in Ihrem Konto aktiviert. Wenn eine Aktivität in auftrittAWS Outposts, wird diese Aktivität in einem - CloudTrail Ereignis zusammen mit anderen -AWSServiceereignissen im Ereignisverlauf aufgezeichnet. Sie können die neusten Ereignisse in Ihr AWS-Konto herunterladen und dort suchen und anzeigen. Weitere Informationen finden Sie unter Anzeigen von Ereignissen mit dem CloudTrail Ereignisverlauf .

Zur kontinuierlichen Aufzeichnung von Ereignissen in Ihrem AWS-Konto, einschließlich Ereignissen für AWS Outposts, erstellen Sie einen Trail. Ein Trail ermöglicht CloudTrail die Bereitstellung von Protokolldateien an einen S3-Bucket in der übergeordneten AWS-Region. Wenn Sie ein Trail in der Konsole anlegen, gilt dieser für alle AWS-Regionen. Der Trail protokolliert Ereignisse aus allen

Regionen in der AWS-Partition und stellt die Protokolldateien für den von Ihnen angegebenen S3 Bucket bereit. Darüber hinaus können Sie andere -AWSServices konfigurieren, um die in den CloudTrail Protokollen erfassten Ereignisdaten weiter zu analysieren und entsprechend zu agieren. Weitere Informationen finden Sie hier:

- Übersicht zum Erstellen eines Trails
- CloudTrail Unterstützte Services und Integrationen
- Konfigurieren von Amazon SNS-Benachrichtigungen für CloudTrail
- Empfangen von CloudTrail Protokolldateien aus mehreren Regionen und Empfangen CloudTrail von Protokolldateien aus mehreren Konten

Alle -AWS OutpostsAktionen werden von protokolliert CloudTrail. Sie werden in der AWS Outposts-API-Referenz dokumentiert. Aufrufe der `ListSites` Aktionen `CreateOutpost`, `GetOutpostInstanceTypes`und erzeugen beispielsweise Einträge in den CloudTrail Protokolldateien.

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Anhand der Identitätsinformationen können Sie feststellen, ob eine Anforderung gestellt wurde:

- Mit Stammbenutzer- oder Benutzeranmeldeinformationen.
- Mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen verbundenen Benutzer.
- Von einem anderen AWS-Service.

Weitere Informationen finden Sie unter CloudTrail -Element userIdentity.

Grundlagen zu AWS Outposts-Protokolldateieinträgen

Ein Trail ist eine Konfiguration, die die Bereitstellung von Ereignissen als Protokolldateien an einen von Ihnen angegebenen S3-Bucket ermöglicht. CloudTrail Protokolldateien enthalten einen oder mehrere Protokolleinträge. Ein Ereignis stellt eine einzelne Anforderung aus einer beliebigen Quelle dar. Sie enthält Informationen über die angeforderte Aktion, das Datum und die Uhrzeit der Aktion, Anforderungsparameter usw. CloudTrail Protokolldateien sind kein geordnetes Stacktrace der öffentlichen API-Aufrufe und erscheinen daher nicht in einer bestimmten Reihenfolge.

Das folgende Beispiel zeigt einen - CloudTrail Protokolleintrag, der die `CreateOutpost` Aktion 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"
}
```

Outpost-Wartung

Im Rahmen des Modells der geteilten Verantwortung ist AWS für die Hardware und Software verantwortlich, die die AWS-Services ausführen. Das gilt für AWS Outposts, genau wie für eine AWS-Region. Beispielsweise verwaltet AWS Sicherheitspatches, aktualisiert Firmware und wartet die Outpost-Geräte. AWS überwacht außerdem die Leistung, den Zustand und die Kennzahlen Ihres Outposts 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 S3-Bucket, einem Amazon EBS-Volume oder einem Netzwerkspeichergerät in Ihrem On-Premises-Netzwerk.

Inhalt

Hardware-Wartung

Wenn AWS ein irreparables Problem mit der Hardware feststellt, auf der auf Ihrem Outpost ausgeführte Amazon EC2 EC2-Instances gehostet werden, informieren wir den Eigentümer des Outposts und den Eigentümer der Instances darüber, dass die betroffenen Instances außer Betrieb genommen werden sollen. Weitere Informationen finden Sie unter Instance-Typen im Amazon EC2-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 stoppt und startet AWS die betroffenen Instanzen am Datum der Ausmusterung der Instanz. 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.

Wenn eine Hardware-Wartung erforderlich ist, setzt sich AWS mit dem Verwalter des Outpost-Standorts in Verbindung, um ein Datum und eine Uhrzeit für den Besuch des AWS-Installationsteams zu bestätigen. Besuche können bereits zwei Arbeitstage nach dem Gespräch zwischen dem Verwalter des Standorts und dem AWS-Team geplant werden.

Wenn das AWS-Installationsteam vor Ort eintrifft, tauscht es die fehlerhaften Hosts, Switches oder Rackelemente aus und stellt die neue Kapazität bereit. 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. Zu diesen Informationen können IP-Adressen und ASNs gehören, die 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 von ONDs wegzuverlagern, 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 ONDs gleiche BGP-Präfixe mit denselben Attributen bewerben. 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 Datenverkehrsverlagerung erfordert gleiche BGP-Präfixe von Kundenseite für alle 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 AWS Outposts-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 Outposts-Rack 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 off-on-off-onwährend der Wartung ein wiederholtes Umschalten der Stromversorgungen ().
- 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.

Netzwerkkonnektivitätsereignisse

Die Service Link-Verbindung zwischen Ihrem Outpost und der AWS-Region oder der Outposts-Heimatregion 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. Weitere Informationen finden Sie in der Frage Was passiert, wenn die Netzwerkverbindung meiner Einrichtung unterbrochen wird? auf der Seite mit häufig gestellten Fragen zum AWS Outposts-Rack.

Wenn die Serviceverbindung aufgrund eines Stromausfalls vor Ort oder aufgrund eines Verlusts der Netzwerkverbindung nicht verfügbar ist, sendet AWS Health Dashboard eine Benachrichtigung an das Konto, dem die Outposts gehören. Weder Sie noch 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

würden bei der Fehlerbehebung hilfreich sein. Wenn Sie ein Problem nach der Wartung an AWS oder Ihren ISP 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 *Region* durch den Namen der AWS-Region.
- 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 AWS Outposts-Überwachung befasst sich mit bewährten Methoden zur Beobachtbarkeit und zum Eventmanagement speziell für Outposts.
- Der AWS Blog Debugging Tool for Network Connectivity from Amazon VPC erklärt das AWSSupport-SetupIPMonitoringFrom VPC Tool. 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 AWS-Region angezeigt.

- Der AWS Blog Bereitstellen eines automatisierten Amazon- CloudWatch Dashboards für die AWS Outposts Verwendung AWS CDK von 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.

Amazon EC2 für AWS Outposts optimieren

Im Gegensatz zur AWS-Region ist die Kapazität der Amazon Elastic Compute Cloud (Amazon EC2) auf einem Outpost endlich. Sie sind durch das Gesamtvolumen der von Ihnen bestellten Rechenkapazität eingeschränkt. Dieses Thema bietet bewährte Methoden und Optimierungsstrategien, mit denen Sie Ihre Amazon EC2 EC2-Kapazität in AWS Outposts optimal nutzen können.

Inhalt

Dedicated Hosts auf Outposts

Ein Amazon EC2 Dedicated Host ist ein physischer Server mit EC2-Instance-Kapazität, der ausschließlich von Ihnen genutzt wird. 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 auf AWS Outposts im Amazon EC2 Benutzerhandbuch für Linux-Instances. Für Windows finden Sie weitere Informationen unter Dedicated Host auf AWS Outposts im Amazon EC2-Benutzerhandbuch für Windows-Instances.

Neben der Lizenzierung können Outpost-Besitzer Dedicated Hosts verwenden, um die Server in ihren Outpost-Installationen 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 zu AWS Support aufnehmen 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 Dedicated Hosts zuweisen im Amazon EC2-Benutzerhandbuch für Linux-Instances oder Dedicated Hosts zuweisen im Amazon EC2-Benutzerhandbuch für Windows-Instances.

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 Instanzen, 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 über ein Outpost-Rack verfügen, können Sie diese Dedicated Hosts-Funktionen nutzen, um die Auswirkungen korrelierter Hardwarefehler zu minimieren. Weitere Informationen zur Instance-Wiederherstellung finden Sie unter Grundlegendes zur automatischen Platzierung und Affinität im Amazon EC2 EC2-Benutzerhandbuch für Linux-Instances oder unter Grundlegendes zur automatischen Platzierung und Affinität im Amazon EC2 EC2-Benutzerhandbuch für Windows-Instances.

Sie können Dedicated Hosts mithilfe von AWS Resource Access Manager freigeben. 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 Mit gemeinsam genutzten Ressourcen arbeiten.

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 Wiederherstellen Ihrer Linux-Instance oder Wiederherstellen Ihrer Windows-Instance.

Platzierungsgruppen auf Outposts

AWS Outposts unterstützt Platzierungsgruppen. Verwenden Sie Platzierungsgruppen, um zu beeinflussen, wie Amazon EC2 versuchen soll, Gruppen voneinander abhängiger Instances zu platzieren, die Sie auf der zugrunde liegenden Hardware starten. 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 Instanzen 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.

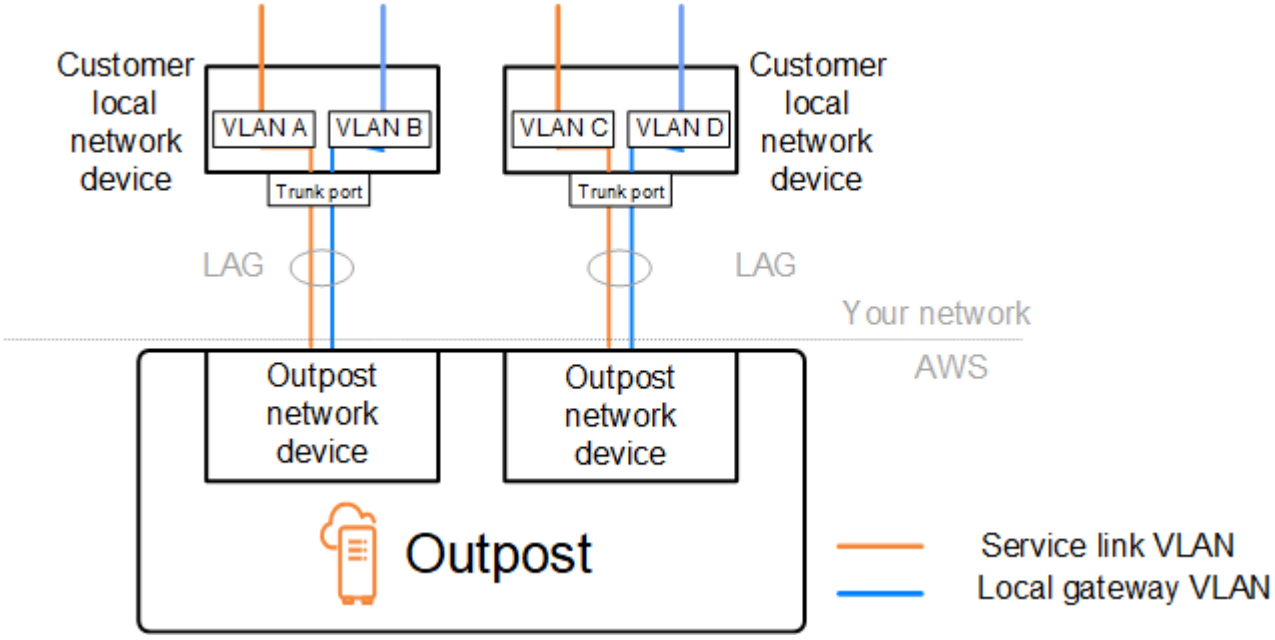
Sie können Instances auch auf Zielpartitionen bereitstellen. Die folgende Abbildung zeigt eine Partition-Placement-Gruppe mit gezielter Verteilung.

Weitere Informationen zur Arbeit mit Platzierungsgruppen finden Sie unter Platzierungsgruppen und Platzierungsgruppen auf AWS Outposts im Amazon EC2-Benutzerhandbuch für Linux-Instances. Für Windows finden Sie weitere Informationen unter Placement-Gruppen und Placement-Gruppen auf AWS Outposts im Amazon EC2 EC2-Benutzerhandbuch für Windows-Instances.

Weitere Informationen zur AWS Outposts-Hochverfügbarkeit finden Sie unter Überlegungen zum AWS Outposts-Hochverfügbarkeitsdesign und zur Architektur.

AWS Outposts-Checkliste zur Fehlersuche in Racknetzwerken

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 Ihres Enterprise-Supportplans mit dem AWS-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 öffentliche virtuelle Schnittstellenverbindung zur AWS-Region.
- 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 Schnittstellenverbindung zur AWS-Region.
- Edge-Router, die mit Internetdienstanbietern (ISPs) verbunden sind – Öffentliches Internet, das für die Service Link-Konnektivität verwendet wird. Weitere Informationen finden Sie unter ISP öffentliche virtuelle Schnittstellenverbindung zur AWS-Region.

AWS Direct Connect öffentliche virtuelle Schnittstellenverbindung zur AWS-Region

Verwenden Sie die folgende Checkliste für die Fehlersuche bei Edge-Routern, die mit AWS Direct Connect verbunden sind, 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 Routentabelle 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 öffentlichen AWS-IP-Adressbereiche oder die Standardroute enthalten.
3. Wenn Sie die öffentlichen AWS-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 der 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 `DOWN` lautet, pingen Sie die AWS-Peer-IP-Adresse an und überprüfen Sie die BGP-Konfiguration im Edge-Router. Weitere Informationen finden Sie unter AWS Direct Connect-Fehlerbehebung im AWS Direct Connect-Benutzerhandbuch und Meine virtuelle Schnittstelle BGP-Status ist down in der AWS-Konsole. Was soll ich tun?.
   d. Wenn BGP eingerichtet ist und Sie die Standardroute oder die öffentlichen AWS-IP-Adressbereiche nicht in der VRF sehen, wenden Sie sich mithilfe Ihres Enterprise-Supportplans an den AWS-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 den öffentlichen AWS-IP-Adressbereichen zuordnen. 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 öffentlichen AWS-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 AWS Direct Connect-Peer-IP-Adressen durch. Teilen Sie die Testergebnisse mithilfe Ihres Enterprise-Supportplans mit dem AWS-Support.

AWS Direct Connect private virtuelle Schnittstellenverbindung zur AWS-Region

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

1. Wenn für die Konnektivität zwischen dem Outpost-Rack und der AWS-Region die private Konnektivitätsfunktion AWS Outposts verwendet wird, überprüfen Sie die folgenden Punkte.
   a. Pingen Sie die Remote-Peering-IP-Adresse von AWS vom Edge-Router aus an und bestätigen Sie den BGP-Peering-Status.
   b. Stellen Sie sicher, dass BGP-Peering über die private virtuelle AWS Direct Connect-Schnittstelle zwischen Ihrem Service-Link-Endpunkt VPC und dem in Ihren Räumlichkeiten installierten Outpost UP ist. Weitere Informationen finden Sie unter AWS Direct Connect-Fehlerbehebung im AWS Direct Connect-Benutzerhandbuch und Meine virtuelle Schnittstelle BGP-Status ist down in der AWS-Konsole. Was sollte ich tun?, und Wie kann ich BGP-Verbindungsprobleme über Direct Connect beheben? .
   c. Die private virtuelle AWS Direct Connect-Schnittstelle ist eine private Verbindung zu Ihrem Edge-Router an Ihrem ausgewählten AWS Direct Connect-Standort und verwendet BGP, um Routen auszutauschen. 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 die Netzwerk-ACLs, die dem privaten Service Link-Endpunkt in Ihrer VPC zugeordnet sind, den entsprechenden Datenverkehr zulassen. 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-Servicendpunkte (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 von AWS Outposts-Privatkonnektivität.

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 On-Premises-Netzwerk haben, können Sie eine Standardroute über die BGP-Sitzung zu AWS auf Ihrer privaten virtuellen Schnittstelle bewerben. 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 AWS Direct Connect-Peer-IP-Adressen durch. Teilen Sie die Testergebnisse mithilfe Ihres Enterprise-Supportplans mit dem AWS-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. Vergewissern Sie sich, 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 verwenden, um den Datenverkehr in Ihrem Netzwerk zu trennen, stellen Sie sicher, dass das 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 der 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 On-Premises-Firewalls so konfiguriert sind, dass sie ausgehende Verbindungen (Ports TCP 1025-65535 und UDP 443) von den IP-Adressbereichen des Outpost-Service Links zu den öffentlichen IP-Adressbereichen von AWS erlauben. 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 asymmetrischem Routing des Service-Links kommen. Das bedeutet, dass eingehender Datenverkehr durch Firewall-1 und ausgehender Datenverkehr durch Firewall-2 geleitet werden kann. Verwenden Sie die folgende Checkliste, um potenzielles asymmetrisches Routing des Service-Links zu identifizieren, insbesondere wenn er zuvor ordnungsgemäß funktioniert hat.

- Überprüfen Sie, ob es in letzter Zeit Änderungen oder laufende Wartungsarbeiten an der Routing-Einrichtung Ihres Unternehmensnetzwerks gegeben hat, die möglicherweise zu einem asymmetrischen Routing der Serviceverbindung über die Firewalls geführt haben.
  - Verwenden Sie Firewall-Datenverkehrsdiagramme, um nach Änderungen an Datenverkehrsmustern zu suchen, die mit dem Anfang des Service Link-Problems übereinstimmen.
  - Überprüfen Sie, ob eine teilweise Firewall ausfällt oder ob Ihre Firewalls ihre Verbindungstabellen nicht mehr miteinander synchronisieren.
  - Suchen Sie in Ihrem Unternehmensnetzwerk nach Links zu den letzten Änderungen am Routing (OSPF/ISIS/EIGRP-Metrikänderungen, BGP-Routing-Map-Änderungen), die mit dem Start des Service Link-Problems übereinstimmen.

- Wenn Sie öffentliche Internetverbindung für den Service Link zur Heimatregion verwenden, könnte eine Serviceanbieterwartung zu asymmetrischem Routing des Service Links über die Firewalls geführt haben.
  - Überprüfen Sie Datenverkehrsdiagramme auf Links zu Ihren ISP(s) auf Änderungen an Datenverkehrsmustern, die mit dem Anfang 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 Link ausgelöst hat.
  - Überprüfen Sie, ob Sie Benachrichtigungen über geplante Wartungsarbeiten an Ihrem/Ihren AWS Direct Connect Service(s) erhalten.
  - Beachten Sie, dass Sie bei redundanten AWS Direct Connect Services das Routing des Outposts-Service-Links über jeden wahrscheinlichen Netzwerkpfad unter Wartungsbedingungen proaktiv testen können. Auf diese Weise können Sie testen, ob eine Unterbrechung eines Ihrer AWS Direct Connect Services zu asymmetrischem Routing des Service-Links führen könnte. Die Ausfallsicherheit des -AWS Direct ConnectTeils der end-to-end Netzwerkkonnektivität kann vom AWS Direct Connect Resiliency with Resiliency Toolkit getestet werden. Weitere Informationen finden Sie unter Testen AWS Direct Connect der Ausfallsicherheit mit dem Resiliency Toolkit – Failover-Tests.

Nachdem Sie die vorangehende Checkliste durchlaufen und das asymmetrische Routing des Service-Links als mögliche Ursache festgelegt haben, können Sie eine Reihe weiterer Maßnahmen ergreifen:

- Stellen Sie symmetrisches Routing wieder her, indem Sie Änderungen am Unternehmensnetzwerk rückgängig machen oder darauf warten, dass die geplante Wartung eines Anbieters abgeschlossen ist.
- Melden Sie sich bei einer oder beiden Firewalls an und löschen Sie alle Flow-Statusinformationen für alle Flows aus der Befehlszeile (sofern vom Firewall-Anbieter unterstützt).
- Filtern Sie BGP-Ankündigungen vorübergehend durch eine der Firewalls oder schließen Sie die Schnittstellen auf einer Firewall, um ein symmetrisches Routing über die andere Firewall zu erzwingen.
- Starten Sie jede Firewall neu, um potenzielle Beschädigungen bei der Flow-Zustandsverfolgung des Service Link-Datenverkehrs im Arbeitsspeicher der Firewall zu vermeiden.
- Bitten Sie Ihren Firewall-Anbieter, die Nachverfolgung des UDP-Flow-Zustands für UDP-Verbindungen, die auf Port 443 stammen und für Port 443 bestimmt sind, entweder zu überprüfen oder zu vereinfachen.

AWS Outposts end-of-term -Optionen

Am Ende Ihrer AWS Outposts-Laufzeit haben Sie drei Möglichkeiten:

- Verlängern Sie Ihr Abonnement und behalten Sie Ihren vorhandenen Outpost.
- Beenden Sie Ihr Abonnement und bereiten Sie Ihre Outpost-Racks für die Rückgabe vor.
- Konvertieren Sie in ein month-to-month Abonnement und behalten Sie Ihren vorhandenen Outpost bei.

Wenn Sie nicht angeben, dass Sie Ihr Abonnement verlängern oder Ihren Outpost zurückgeben möchten, werden Sie in ein month-to-month Abonnement umgewandelt.

Themen

Verlängern Sie Ihr Abonnement

So verlängern Sie Ihr Abonnement und behalten Ihren vorhandenen Outpost:

Führen Sie die folgenden Schritte mindestens 30 Tage vor Ablauf der Laufzeit Ihres Outposts durch:

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.

Der AWS-Kundensupport leitet den Verlängerungsprozess für das Abonnement ein. Ihr neues Abonnement beginnt am Tag nach Ablauf Ihres aktuellen Abonnements.

Ihr Abonnement beenden und die Rückgabe vorbereiten

> **Important**
>
> AWS kann den Rückgabeprozess erst beginnen, wenn Sie die folgenden Verfahren abgeschlossen haben. Nachdem Sie einen Support-Fall eröffnet haben, um Ihr Abonnement zu beenden, können wir den Rückgabeprozess nicht mehr stoppen.

So beenden Sie Ihr Abonnement:

Führen Sie die folgenden Schritte mindestens 30 Tage vor Ablauf der Laufzeit Ihres Outposts durch:

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.

Der AWS-Kundensupport wird sich mit Ihnen in Verbindung setzen, um den Abruf zu koordinieren.

So bereitest Sie Ihre AWS Outposts-Racks für die Rückgabe vor:

> **Important**
>
> Schalten Sie das Outpost-Rack nicht aus, bevor AWS für die geplante Abholung vor Ort 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:

   - Verwendung der AWS RAM-Konsole. Weitere Informationen finden Sie unter Aktualisieren einer Ressourcenfreigabe im AWS RAM-Benutzerhandbuch.
   - Verwenden Sie die AWS CLI zum Ausführen des disassociate-resource-share-Befehls.

   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 Beenden Ihrer Instance im Amazon EC2 Benutzerhandbuch für Linux Instances.

3. Überprüfen Sie die Ihrer Amazon EC2- instance-capacity-availability Instances in Ihrem AWS Konto.

   a. Öffnen Sie die AWS Outposts-Konsole unter https://console.aws.amazon.com/outposts/.

   b. Wählen Sie Outposts.

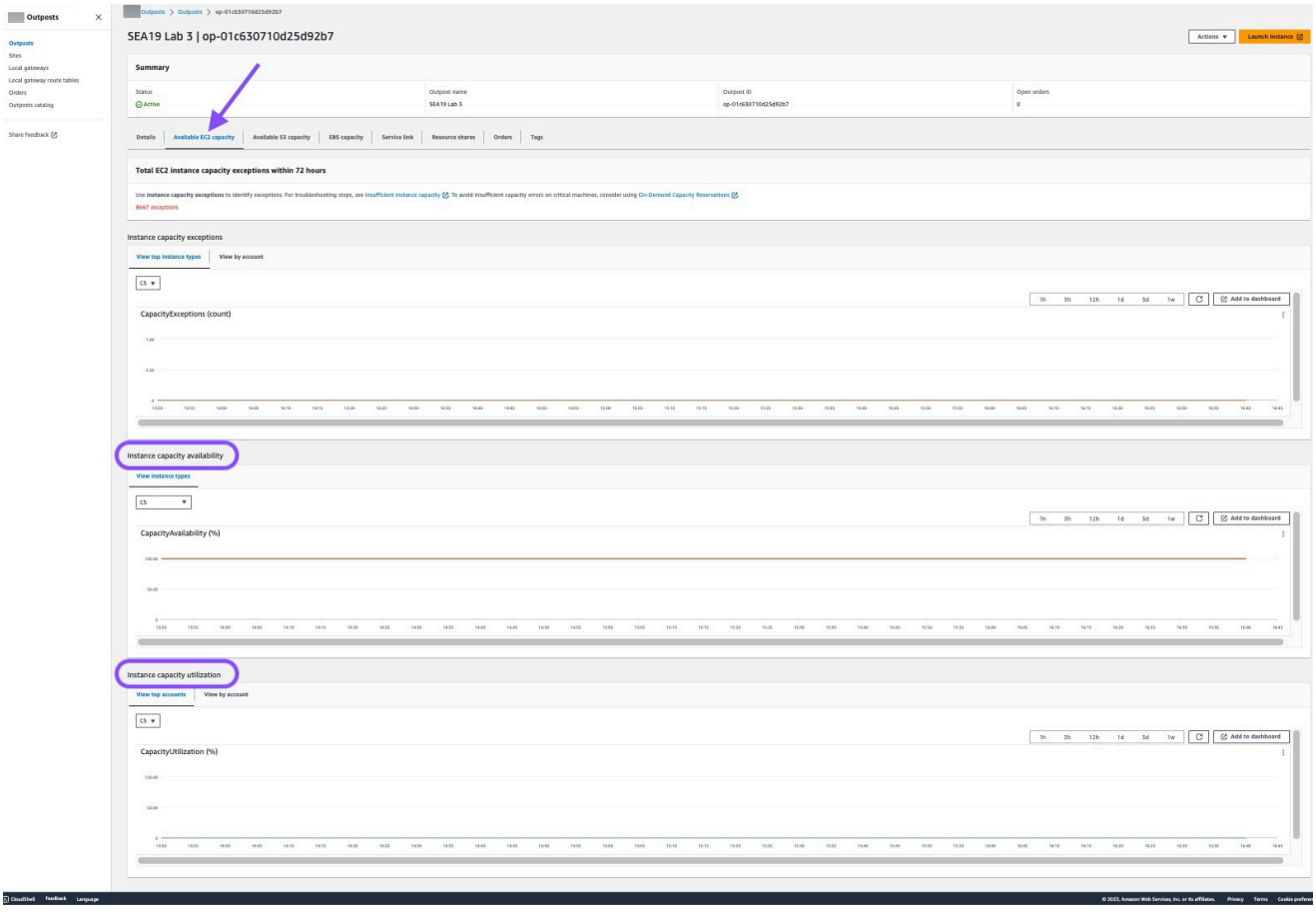
   c. Wählen Sie den spezifischen Outpost aus, zu dem Sie zurückkehren.

   d. Wählen Sie auf der Seite für den Outpost die Registerkarte Verfügbare EC2-Kapazität aus.

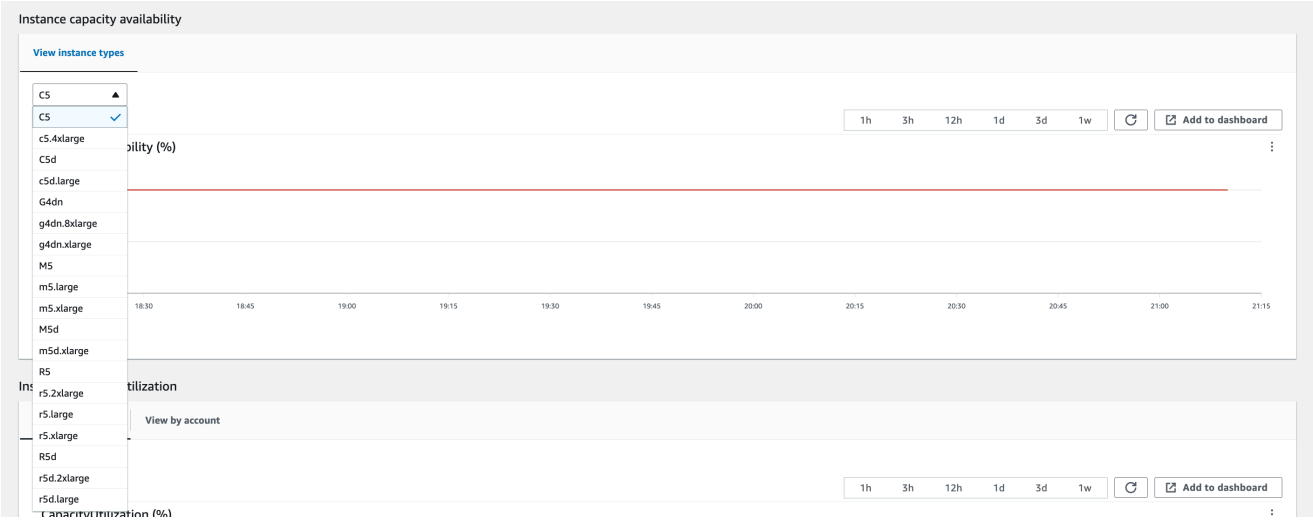
   e. Stellen Sie sicher, dass die Instance-Kapazitätsverfügbarkeit für jede Instance-Familie bei 100 % liegt.

   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 Instance auf der Registerkarte Verfügbare EC2-Kapazität.



   Die folgende Abbildung zeigt die Liste der Instance-Typen.



4. Erstellen Sie Backups Ihrer Amazon EC2 EC2-Instances und Server-Volumes. Um die Backups zu erstellen, folgen Sie den Anweisungen unter Backup und Wiederherstellung für Amazon EC2 mit EBS-Volumes im AWSPrescriptive Guidance-Handbuch.
5. Löschen Sie die Amazon EBS-Volumes, die Ihrem Outpost zugeordnet sind.
   a. Öffnen Sie die Amazon EC2-Konsole 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 Amazon EC2-Konsole 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 Outpost verknüpft sind. Um die Buckets zu löschen, folgen Sie den Anweisungen unter Löschen Ihres Amazon S3 in Outposts Buckets im Amazon Simple Storage Service Benutzerhandbuch.
8. Löschen Sie alle VPC-Verknüpfungen und kundeneigenen IP-Adresspool(CoIP)-CIDRs, die Ihrem Outpost zugeordnet sind.

Ein AWS-Abholteam schaltet das Rack aus. Nach dem Ausschalten können Sie den AWS-Nitro-Sicherheitsschlüssel vernichten, oder das AWS-Abholteam kann dies in Ihrem Namen tun.

In ein month-to-month Abonnement umwandeln

Um zu einem month-to-month Abonnement zu konvertieren und Ihren vorhandenen Outpost beizubehalten, ist keine Aktion erforderlich. Wenn Sie Fragen haben, öffnen Sie eine Support-Anfrage für die Abrechnung.

Ihr Outpost 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.

Kontingente für AWS Outposts

DasAWS-Konto verfügt über Standardkontingente (früher als Limits bezeichnet) für jeden - ServiceAWS-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 AWS Outposts anzuzeigen, öffnen Sie die Service-Quotas-Konsole. Wählen Sie im Navigationsbereich aus und wählen AWS-ServicesSie aus AWS Outposts.

Informationen zur Erhöhung eines Kontingents finden Sie unter Anfordern einer Kontingenterhöhung im Service-Quotas-Benutzerhandbuch.

Ihr AWS-Konto umfasst die folgenden Kontingente für 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. Du kannst in jeder Region deinesAWS Accounts 100 Outposts-Standorte haben.
Outposts pro Standort	10	Ja	AWS Outpostsumfassen Hardware und virtuelle Ressourcen, die als Outposts bekannt sind. Dieses Kontingent schränkt Ihre virtuellen Outpost-Ressourcen ein. Du kannst auf jeder Außenposten-Websit e 10 Outposts haben.

AWS Outpostsund die Kontingente für andere Dienstleistungen

AWS Outpostsist auf die Ressourcen anderer Dienste angewiesen, und diese Dienste haben möglicherweise ihre eigenen Standardkontingente. Ihr Kontingent für lokale Netzwerkschnittstellen stammt beispielsweise aus dem Amazon VPC-Kontingent für Netzwerkschnittstellen.

Dokumentverlauf

In der folgenden Tabelle werden wichtige Änderungen am AWS Outposts Benutzerhandbuch beschrieben.

Änderung	Beschreibung	Datum
Kapazitätsmanagement	Sie können die Standardk apazitätskonfiguration für Ihre neue Outposts-Bestellung ändern.	16. April 2024
AWS Outposts Das Rack unterstützt Durchsatzmetriken für die Service Link-Schn ittstelle	Sie können jetzt die Durchsatz nutzung zwischen Ihren virtuellen Outpost-Rack-Servi celink-Schnittstellen (VIFs) und Ihren lokalen Netzwerkg eräten überwachen, indem Sie Messwerte nutzen`IfTraffic In` . `IfTrafficOut` Amazon CloudWatch	17. November 2023
Intra-VPC-Kommunikation über AWS Outposts das lokale Gateway	Sie können die Kommunika tion zwischen Subnetzen in derselben VPC über verschied ene Outposts mit lokalen Gateways herstellen.	30. August 2023
nd-of-term E-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-Anfra gen zwischenspeichert, die	20. Juli 2023

	vom AWS Outposts-ausgehen. Sie können auch Hybridkon nektivität zwischen einem Outpost und einem On-Premis es-DNS-Resolver einrichten, wenn Sie ein- und ausgehend e Endpunkte bereitstellen.	
Eingehende Routen am lokalen Gateway	Sie können eingehende Routen für das lokale Gateway zu elastischen Netzwerks chnittstellen 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 Kommunika tion mit Ihrem On-Premises-Netzwerk zu erleichtern.	14. September 2022
AWS Outposts Benutzerl eitfaden für Outposts Rack erstellt	AWS Outposts Das Benutzerh andbuch 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 Netzwerkf ehlerbehebung 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 Freigabe von kundeneigenen IPv4-Adressen	Wird verwendet AWS Resource Access Manager , um kundeneigene IPv4-Adressen gemeinsam zu nutzen.	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.