Benutzerhandbuch für Outposts-Racks

AWS Outposts

AWS Outposts: Benutzerhandbuch für Outposts-Racks

Table of Contents

Was ist AWS Outposts?

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

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

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

Weitere Informationen finden Sie auf der AWS Outposts -Produktseite.

Die wichtigsten Konzepte

Dies sind die wichtigsten Konzepte für. AWS Outposts

- Außenpoststandort — Die vom Kunden verwalteten physischen Gebäude, in denen Ihr Außenposten installiert AWS wird. Ein Standort muss die Anforderungen an die Einrichtung, das Netzwerk und die Stromversorgung Ihres Outposts erfüllen.
- Outpost-Kapazität – Rechen- und Speicherressourcen, die auf dem Outpost verfügbar sind. Sie können die Kapazität für Ihren Outpost von der AWS Outposts -Konsole aus einsehen und verwalten.
- Outpost-Ausrüstung — Physische Hardware, die den Zugriff auf den Service ermöglicht. AWS Outposts Die Hardware umfasst Racks, Server, Switches und Kabel, die Eigentum des Unternehmens sind und von diesem verwaltet werden. AWS

- Outposts-Racks – Ein Outpost-Formfaktor, bei dem es sich um ein 42U-Rack nach Branchenstandard handelt. Zu den Racks von Outposts gehören rackmontierbare Server, Switches, ein Netzwerk-Patchpanel, ein Power-Shelf und leere Panels.
- ACEOutposts-Racks — Das Aggregation-, Core-, Edge (ACE) -Rack dient als Netzwerkaggregationspunkt für Outpost-Bereitstellungen mit mehreren Racks. Das ACE Rack reduziert die Anzahl der Anforderungen an physische Netzwerkports und logische Schnittstellen, indem es Konnektivität zwischen mehreren Outpost-Compute-Racks in Ihren logischen Outposts und Ihrem lokalen Netzwerk bereitstellt.

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

  Weitere Informationen zu ACE Racks finden Sie unter Skalierung von AWS Outposts Rack-Bereitstellungen mit ACE Racks.
- Outposts-Server — Ein Outpost-Formfaktor, bei dem es sich um einen 1U- oder 2U-Server nach Industriestandard handelt, der in einem standardmäßigen EIA -310D 19-konformen 4-Post-Rack installiert werden kann. Outposts-Server bieten lokale Rechen- und Netzwerkdienste für Standorte mit begrenztem Platzbedarf oder geringeren Kapazitätsanforderungen.
- Serviceverbindung — 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 Verbindung, der die Kommunikation zwischen einem Outposts-Rack und Ihrem lokalen Netzwerk ermöglicht.
- Lokale Netzwerkschnittstelle — Eine Netzwerkschnittstelle, die die Kommunikation von einem Outposts-Server und Ihrem lokalen Netzwerk aus ermöglicht.

AWS Ressourcen auf Outposts

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

Datenverarbeitung

Ressourcentyp	Racks	Server
EC2Amazon-Instanzen	 Ja	 Ja
ECSAmazon-Cluster	 Ja	 Ja
EKSAmazon-Knoten	 Ja	 Nein

Datenbank und Analytik

Ressourcentyp	Racks	Server
ElastiCache Amazon-Knoten (Redis-Cluster, Memcached-Cluster)	 Ja	 Nein
EMRAmazon-Cluster	 Ja	 Nein
RDSAmazon-DB-Instances	 Ja	 Nein

Netzwerk

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

Speicher

Ressourcentyp	Racks	Server
EBSAmazon-Volumen	 Ja	 Nein
Amazon-S3-Buckets	 Ja	 Nein

Andere 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.

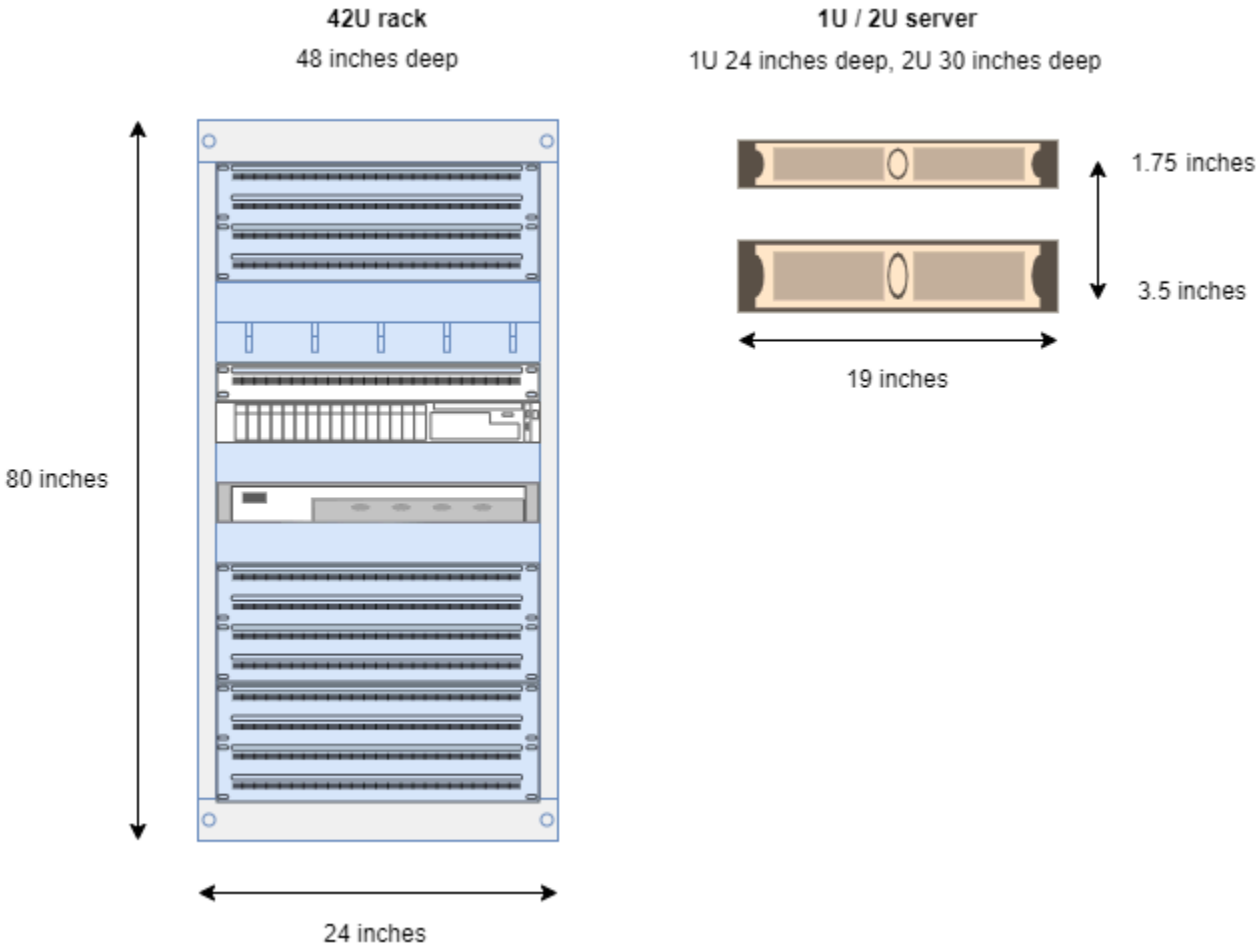
Sie erwerben eine Konfiguration mit einer Laufzeit von einem oder drei Jahren und können zwischen drei Zahlungsoptionen wählen: Vollständig im Voraus, Teilweise im Voraus und Keine Vorauszahlung. Wenn Sie die Option Teilweise Vorauszahlung oder Keine Vorauszahlung wählen, fallen monatliche Gebühren an. Jede Vorauszahlung fällt 24 Stunden nach der Aktivierung Ihres Outposts-Racks an, d. h. wenn Ihre Outposts-Rack-Kapazität für den Start von Instances verfügbar ist. Weitere Informationen finden Sie unter:

- AWS Outposts Preise für Racks
- AWS Outposts Preisgestaltung für Server

Wie AWS Outposts funktioniert

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

Das folgende Diagramm veranschaulicht beide Outpost-Formfaktoren.



Inhalt

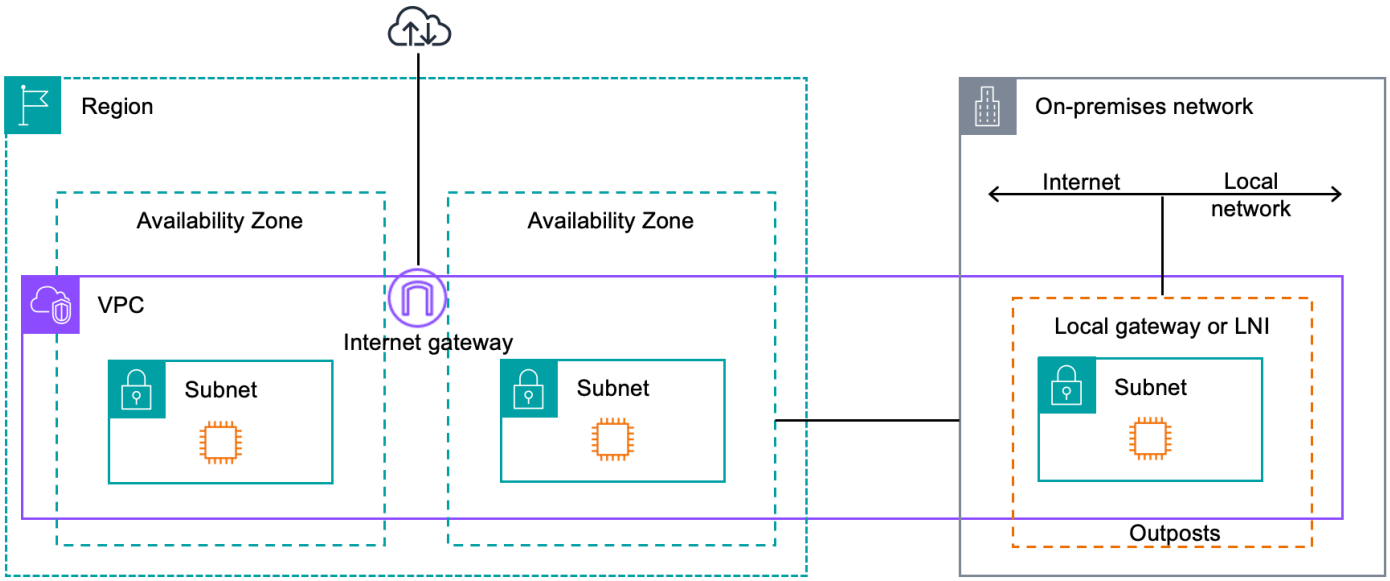
- DNS
- Service Link
- Lokale Gateways
- Lokale Netzwerkschnittstellen

Netzwerkkomponenten

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

Das folgende Diagramm zeigt die Netzwerkkomponenten für Ihren Outpost.

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



VPCsund Subnetze

Eine virtuelle private Cloud (VPC) erstreckt sich über alle Availability Zones in ihrer AWS Region. Sie können jede VPC in der Region auf Ihren Outpost ausdehnen, indem Sie ein Outpost-Subnetz hinzufügen. Um ein Outpost-Subnetz zu einem hinzuzufügenVPC, geben Sie bei der Erstellung des Subnetzes den Amazon-Ressourcennamen (ARN) des Outposts an.

Outposts unterstützen mehrere Subnetze. Sie können das EC2 Instance-Subnetz angeben, wenn Sie die Instance in Ihrem Outpost starten. EC2 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 unterstützenVPCs, die über ein oder mehrere Outpost-Subnetze verfügen können. Informationen zu VPC Kontingenten finden Sie unter VPCAmazon-Kontingente im VPCAmazon-Benutzerhandbuch.

Sie erstellen Outpost-Subnetze aus dem VPC CIDR Bereich, VPC in dem 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 seinem. VPC Sie können eine benutzerdefinierte Routing-Tabelle erstellen und diese mit einem Outpost-Subnetz verknüpfen.

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

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

- VPCCIDRBereich — AWS definiert dies bei der Installation. Dies ist die lokale Route und gilt für das gesamte VPC Routing, einschließlich des Datenverkehrs zwischen Outpost-Instanzen innerhalb derselbenVPC.

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

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

DNS

Für Netzwerkschnittstellen, die mit a verbunden sindVPC, können EC2 Instances in Outposts-Subnetzen den Amazon Route DNS 53-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 Domains 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 Region kann es bei Route 53 zu längeren DNS Lösungszeiten kommen. AWS In solchen Fällen können Sie die lokal 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 diese den zuordnen. VPC Sie müssen außerdem sicherstellen, dass IP-Konnektivität zu diesen DNS Servern besteht. Möglicherweise müssen Sie der lokalen Gateway-Routingtabelle auch Routen hinzufügen, um die Erreichbarkeit zu gewährleisten. Dies ist jedoch nur eine Option für Outposts-Racks mit lokalem Gateway. Da DHCP Optionssätze einen bestimmten VPC Bereich haben, versuchen Instanzen sowohl in den Outpost-Subnetzen als auch in den Availability Zone-Subnetzen für die, die angegebenen Server für VPC die Namensauflösung zu verwenden. DNS DNS

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

Service Link

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

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
- Das Whitepaper zum Routing von Anwendungen und Workloads im Zusammenhang mit Design und Architektur für AWS Outposts hohe Verfügbarkeit AWS

Lokale Gateways

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

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

Lokale Netzwerkschnittstellen

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

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

Standortanforderungen für Outposts-Racks

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

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

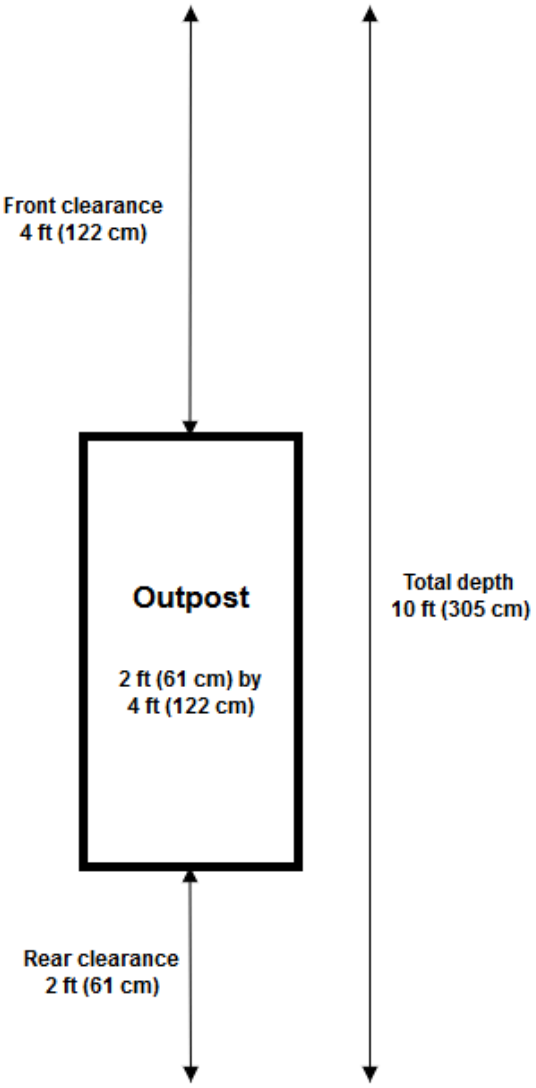
Die Anforderungen für Outposts-Server finden Sie unter Standortanforderungen für Outposts-Server im AWS Outposts -Benutzerhandbuch für Outposts-Server.

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 gewährleistet sein.
- 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 Abstützung — Soweit gesetzlich oder gesetzlich vorgeschrieben, müssen Sie geeignete seismische Verankerungen und Abstützungen für das Rack installieren und warten, solange es sich in Ihrer Einrichtung befindet. AWS bietet bei allen Outposts-Racks Bodenhalterungen, die Schutz vor seismischen Aktivitäten von bis zu 2,0 G bieten.
- Verbindungspunkt — Wir empfehlen Ihnen, an der Rackposition einen Verbindungsdraht bzw. eine Verbindungsstelle anzubringen, damit der AWS zertifizierte Techniker die Racks während der Installation verbinden kann.

- Zugang zur Einrichtung — Sie dürfen die Einrichtung nicht in einer Weise verändern, die sich negativ auf die Fähigkeit auswirkt, auf den Außenposten zuzugreifen, ihn AWS 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 LANWAN, und alle Geräte zwischen dem Außenposten und lokalen Verkehrszielen sowie dem Ziel in der Region. AWS

Uplink-Geschwindigkeit, Ports und Glasfaser

Uplink-Geschwindigkeit und Ports

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

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

1 Gbit/s

- 1, 2, 4, 6 oder 8 Uplinks

10 Gbit/s

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

40 Gbit/s oder 100 Gbit/s

- 1, 2 oder 4 Uplinks

Glasfaser

Die folgenden Glasfasertypen werden unterstützt:

- Singlemode-Glasfaser (SMF) mit Lucent Connector (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 -LR GBASE
10 Gbit/s	MMF	— 10 -SR GBASE
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

Uplink-Geschwindigkeit	Glasfasertyp	Optischer Standard
100 Gbit/s	SMF	— 100 G PSM4 MSA — 100 GBASE - CWDM4 — 100 GBASE - LR4
Breakout-Anwendung mit 4 x 25 Gbit/s	MMF	— 100 GBASE - SR4

Aggregation von Outpost-Links und VLANs

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

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

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

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

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

IP-Konnektivität von Outpost-Netzwerkgeräten

Jedes der beiden Outpost-Netzwerkgeräte benötigt eine CIDR IP-Adresse für den Service Link und das lokale Gateway. VLANs Wir empfehlen, jedem Netzwerkgerät mit einem /30 oder /31 ein eigenes

Subnetz zuzuweisen. CIDR Geben Sie ein Subnetz und eine IP-Adresse aus dem Subnetz an, die der Outpost verwenden soll. Weitere Informationen finden Sie unter Netzwerk-Layer-Konnektivität.

Outpost-Netzwerkgerät	Anforderungen für Service Link	Anforderungen für das lokale Gateway
Nr. 1	— Service-Link CIDR (/30 oder /31) – 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 der Serviceverbindung () MTU

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

Service Link für Border Gateway Protocol

Der Outpost richtet eine externe BGP (EBGP) Peering-Sitzung zwischen jedem Outpost-Netzwerkgerät und Ihrem lokalen Netzwerkgerät ein, um die Service Link-Konnektivität über den Service Link zu gewährleisten. VLAN Weitere Informationen finden Sie unter Service BGP Link-Konnektivität.

Outpost	Anforderungen an den Service Link BGP
Ihr Outpost	— BGP Autonome Systemnummer des Außenpostens (ASN). 2 Byte (16 Bit) oder 4 Byte (32 Bit). Aus Ihrem privaten ASN Bereich (64512-65534 oder 4200000000-4294967294).

Outpost	Anforderungen an den Service Link BGP
	— Infrastruktur (/26 erforderlich, beworben als zwei zusammenhängende /27s). CIDR

Lokales Netzwerkgerät	BGPAnforderungen an den Service Link
Nr. 1	— BGP Peer-IP-Adresse für Service Link. — Service BGP Link-PeerASN. 2 Byte (16 Bit) oder 4 Byte (32 Bit).
Nr. 2	— BGP Peer-IP-Adresse für den Service Link. — Service BGP Link-PeerASN. 2 Byte (16 Bit) oder 4 Byte (32 Bit).

Service Link-Firewall

UDPund TCP 443 muss statusmäßig in der Firewall aufgeführt sein.

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

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

Lokales Gateway für Border Gateway Protocol

Der Outpost richtet eine BGP E-Peering-Sitzung von jedem Outpost-Netzwerkgerät zu einem lokalen Netzwerkgerät ein, um die Konnektivität zwischen Ihrem lokalen Netzwerk und dem lokalen Gateway herzustellen. Weitere Informationen finden Sie unter Lokale Gateway-Konnektivität BGP.

Outpost	Anforderungen an das lokale Gateway BGP
Ihr Outpost	— BGP Autonome Systemnummer des Außenpostens (ASN). 2 Byte (16 Bit) oder 4 Byte (32 Bit). Aus Ihrem privaten ASN Bereich (64512-65534 oder 4200000000-4294967294). — CoIP für Werbung (öffentlich oder privat, mindestens /26). CIDR

Lokale Netzwerkgeräte	Anforderungen an das lokale Gateway BGP
Nr. 1	— BGP Peer-IP-Adresse des lokalen Gateways. — Lokaler BGP Gateway-PeerASN. 2 Byte (16 Bit) oder 4 Byte (32 Bit).
Nr. 2	— BGP Peer-IP-Adresse des lokalen Gateways. — Lokaler BGP Gateway-PeerASN. 2 Byte (16 Bit) oder 4 Byte (32 Bit).

Stromversorgung

Das Outposts-Power-Shelf unterstützt drei Leistungskonfigurationen: 5 kVA, 10 kVA oder 15 kVA. Die Konfiguration des Power-Shelfs hängt von der Gesamtstromaufnahme der Outpost-Kapazität ab. Wenn Ihre Outpost-Ressource beispielsweise eine maximale Leistungsaufnahme von 9,7 kVA hat, müssen Sie die Energiekonfigurationen für 10 kVA angeben: 4 x L6-30P oder IEC3 09, 2

Stromabfälle 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 zu sehen, wählen Sie in der Konsole unter Katalog durchsuchen aus. AWS Outposts https://console.aws.amazon.com/outposts/

Anforderung	Spezifikation
Netzspannung (Wechselstrom)	Einphasig 208 bis 277VAC; 50 oder 60 Hz Dreiphasig: • 208 bis 250 VAC (Delta); 50 bis 60 Hz • 346 bis 480 VAC (Wye); 50 bis 60 Hz
Stromverbrauch	5 kVA (4 kW), 10 kVA (9 kW) oder 15 kVA (13 kW)
Wechselstromschutz (vorgeschaltete Leistungsschalter)	Sowohl für 1N-Eingang (nicht redundant) als auch für 2N-Eingang (redundant): 30 A, 32 A oder 50 A mit D-Kurve- oder K-Kurven-Schutzschalter. 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-, 30A- oder 3x 309-P+N+E-, 32A-Stecker IEC6 IP67 Dreiphasig, Wye 1x IEC6 0309, 3P+N+E, Taktposition 7, 30A-Stecker oder 1x 0309, 3P+N+E, Uhrposition 6, 32A-Stecker IP67 IEC6 IP67 DreiphasigNEMA, xNon Delta 1 - Twistlock-Hubbell, 3P+E, Mittelerdung, 50-A-Stecker CS8365C

Anforderung	Spezifikation
	Note Es hat sich bewährt, einen Stecker mit einer Buchse zu verbinden. IP67 IP67 Wenn das nicht möglich ist, lässt sich der IP67 Stecker mit einer IP44 Buchse verbinden . Die Nennleistung der Kombination aus Stecker und Buchse wird zur niedrigeren Nennleistung ()IP44.
Kabellänge vom Stromverteiler	3 m (10,25 Fuß)
Kabel vom Stromverteiler bis zum Kabeleingang des Racks	Von oben oder unter dem Rack

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

	Redundant, einphasig	Redundant, dreiphasig	Einphasig	Dreiphasig
5 kVA	2 x L6-30P oder IEC3 09; 1 fällt auf S1 und 1 Abfall auf S2	2 x AH53 0P7W,AH53 2P6W, oderCS8365C; 1 Abfall auf S1 und 1 Abfall auf S2	Nicht angeboten	1 x AH53 0P7W AH532P6W oderCS8365C; 1 fallend auf S1
10 kVA	4 x L6-30P oder IEC3 09; 2 fallen auf S1 und 2 Tropfen auf S2		2 x L6-30P oder IEC3 09; 2 Tropfen fallen auf S1	
15 kVA	6 x L6-30P oder IEC3 09; 3 Tropfen auf S1 und 3 Tropfen auf S2		3 x L6-30P oder IEC3 09; 3 Tropfen auf S1	

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

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

Erfüllung der Bestellung

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

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

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

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

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

Standortanforderungen für Outpost-Racks ACE

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

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

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

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

Einrichtung

Dies sind die Anforderungen an die Einrichtung eines ACE Racks.

- Stromversorgung — Alle Racks werden mit einphasigem 10-kVA-Anschluss (Typ AA+BB, IEC6 0309 oder L6-30P Whip) geliefert.
- Gewichtsstütze — Das Gewicht des Racks beträgt 705 lbs bzw. 320 kg.
- Abstand/Größe — Die Größe des Regals beträgt 80 Zoll (203 cm) hoch, 24 Zoll (61 cm) breit und 42 Zoll (107 cm) tief.

Netzwerk

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

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

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

- Glasfaser — Stellen Sie Singlemode-Glasfaser (SMF) mit Lucent Connector (LC) oder Multimode-Glasfaser () mit Lucent Connector (LCMMF) bereit. Die vollständige Liste der unterstützten Glasfasertypen und optischen Standards finden Sie unter. Uplink-Geschwindigkeit, Ports und Glasfaser
- Upstream-Gerät — Stellen Sie zwei oder vier Upstream-Geräte bereit, bei denen es sich um Switches oder Router handeln kann.
- Dienst VLAN und ein lokales Gateway VLAN — Für jedes der vier ACE Netzwerkgeräte müssen Sie einen Dienst VLAN und ein anderes lokales Gateway VLAN bereitstellen. Sie können wählen, ob Sie nur zwei unterschiedliche Geräte bereitstellen möchtenVLANs, einen für den Dienst VLAN und einen für das lokale GatewayVLAN, oder Sie können VLANs in jedem ACE Netzwerkgerät unterschiedliche Dienste VLAN und LGW VLAN insgesamt 8 verschiedene Geräte verwendenVLANs. Weitere Informationen zur Verwendung der Link-Aggregationsgruppen (LAGs) und VLAN finden Sie unter Link-Aggregation undVirtuell LANs.
- CIDRund IP-Adresse für den Service Link und das lokale Gateway VLANs — Wir empfehlen, jedem ACE Netzwerkgerät ein eigenes Subnetz mit einem /30 oder /31 zuzuweisen. CIDR Alternativ ist es möglich, jedem Dienst und jedem lokalen Gateway ein einzelnes /29-Subnetz zuzuweisen. VLAN In beiden Fällen müssen Sie die IP-Adressen angeben, die die ACE Netzwerkgeräte verwenden sollen. Weitere Informationen finden Sie unter Netzwerk-Layer-Konnektivität.
- BGPAutonome Systemnummer für Kunden und Außenposten (ASN) für die Service-Verbindung VLAN und ein lokales Gateway VLAN — Der Outpost richtet eine externe BGP (EBGP) Peering-Sitzung zwischen jedem ACE Rack-Gerät und Ihrem lokalen Netzwerkgerät ein, um die Service

Link-Konnektivität über den Service Link zu gewährleisten. VLAN Darüber hinaus wird eine BGP E-Peering-Sitzung von jedem ACE Netzwerkgerät zu einem lokalen Netzwerkgerät eingerichtet, um die Konnektivität zwischen Ihrem lokalen Netzwerk und dem lokalen Gateway zu gewährleisten. Weitere Informationen erhalten Sie unter Service BGP Link-Konnektivität und Lokale Gateway-Konnektivität BGP.

Important

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

Stromversorgung

Dies sind die Stromversorgungsanforderungen für ein Rack. ACE

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

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

Aufgaben

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

Eine Bestellung für ein Outposts-Rack erstellen

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

Voraussetzungen

- Sehen Sie sich die verfügbaren Konfigurationen für Ihre Outposts-Racks an.
- Ein Outpost-Standort ist der physische Standort für Ihre Outpost-Ausrüstung. Stellen Sie vor der Bestellung von Kapazitäten sicher, dass Ihr Standort die Anforderungen erfüllt. Weitere Informationen finden Sie unter Standortanforderungen für Outposts-Racks.
- Sie müssen über einen AWS Enterprise Support Plan oder einen AWS Enterprise On-Ramp Support Plan verfügen.
- Bestimme, AWS-Konto wem der Outpost gehören soll. 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. Geben Sie dann diesen Outpost an, wenn Sie Ihre Bestellung aufgeben.

Voraussetzungen

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

Erstellen eines Outpost

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

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

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

Schritt 3: Bestellung

Bestellen Sie die Outposts-Racks, die Sie benötigen.

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

Voraussetzungen

- Bestimmen Sie, wie Sie für die Bestellung bezahlen werden. Sie haben folgende Optionen: Vollständige Vorauszahlung, Teilweise Vorauszahlung oder Keine Vorauszahlung. Wenn Sie sich nicht dafür entscheiden, alles im Voraus zu zahlen, zahlen Sie 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.
6. Wählen Sie Vorhandenen Outpost verwenden und wählen Sie Ihren Outpost aus.
7. Wählen Sie Weiter.
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.
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 bietet einen Pool an AWS Rechen- und Speicherkapazität an Ihrem Standort als private Erweiterung einer Availability Zone in einer AWS Region. 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 Amazon-EC2, Amazon- und Amazon S3 AWS Outposts S3-Kapazität Sie benötigenEBS, um Ihre anfänglichen Workloads auszuführen, future Wachstum zu bewältigen und zusätzliche Kapazität bereitzustellen, um Serverausfälle und Wartungsereignisse zu minimieren.

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

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

Um die Instanzkapazität zu ändern

1. Wählen Sie im 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.
2. Wählen Sie Weiter.
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.
9. Überprüfen Sie auf der Seite Überprüfen und erstellen, welche Aktualisierungen Sie anfordern.
10. Wählen Sie „Erstellen“. AWS Outposts erstellt eine Kapazitätsaufgabe.

11. Überwachen Sie auf der Seite mit den Kapazitätsaufgaben den Status der Aufgabe.

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

Upload JSON file

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

   Example

   JSONBeispieldatei:

```
{
    "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.
6. Überprüfen Sie auf der Seite Überprüfen und erstellen, welche Updates Sie anfordern.

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

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

Nächste Schritte

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

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

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

Starten Sie eine Instance in Ihrem Outposts-Rack

Nach der Installation Ihres Outpost und der verfügbaren Datenverarbeitungs- und Speicherkapazität können Sie mit der Erstellung von Ressourcen beginnen. Starten Sie EC2 Amazon-Instances und erstellen Sie EBS Amazon-Volumes in Ihrem Outpost mithilfe eines Outpost-Subnetzes. Sie können auch Snapshots von EBS Amazon-Volumes in Ihrem Outpost erstellen. Weitere Informationen finden Sie unter EBSLokale Amazon-Schnappschüsse AWS Outposts im EBSAmazon-Benutzerhandbuch.

Voraussetzung

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

Aufgaben

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

Schritt 1: Erstellen Sie ein VPC

Du kannst jeden VPC in der AWS Region auf deinen Außenposten ausdehnen. Überspringe diesen Schritt, wenn du bereits einen hastVPC, den du verwenden kannst.

Um eine VPC für deinen Außenposten zu erstellen

1. Öffnen Sie die VPC Amazon-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie dieselbe Region wie das Outposts-Rack.
3. Wählen Sie im Navigationsbereich Ihr VPCs und anschließend Erstellen VPC aus.
4. Wählen Sie VPCnur.
5. (Optional) Geben Sie für das Namensschild einen Namen für das einVPC.
6. Wählen Sie für IPv4CIDRBlock die Option IPv4CIDRManuelle Eingabe und geben Sie den IPv4 Adressbereich für VPC in das IPv4CIDRTextfeld ein.

   > **Note**
   >
   > Wenn Sie Direct 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 IPv6CIDRBlock die Option Kein IPv6 CIDR Block aus.
8. Wählen Sie für Tenancy die Option Standard.

9. (Optional) Um Ihrem ein Tag hinzuzufügenVPC, wählen Sie Tag hinzufügen aus und geben Sie einen Schlüssel und einen Wert ein.
10. Wählen Sie „Erstellen VPC“.

Schritt 2: Erstellen Sie ein Subnetz und eine benutzerdefinierte Routentabelle

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

> **Note**
>
> Wenn Sie eine Instance in einem Outpost-Subnetz starten, das von einem anderen für Sie freigegeben wurde AWS-Konto, fahren Sie mit 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 umgeleitet, um ein Subnetz in der VPC Amazon-Konsole zu erstellen. Wir wählen für Sie den Outpost und die Availability Zone aus, in der sich der Outpost befindet.
4. Wählen Sie einVPC.
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 VPC Amazon-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. Für VPC, wählen Sie IhreVPC.
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 VPC Amazon-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 zu finden Sie unter LGW 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

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

So erstellen Sie eine benutzerdefinierte Routentabelle für das lokale Gateway

1. Öffnen Sie die AWS Outposts Konsole unter https://console.aws.amazon.com/outposts/.
2. Um das zu ändern AWS-Region, verwenden Sie die Regionsauswahl in der oberen rechten Ecke der Seite.
3. Wählen Sie im Navigationsbereich Lokale Gateway-Routing-Tabelle aus.
4. Wählen Sie Lokale Gateway-Routing-Tabelle erstellen aus.
5. (Optional) Geben Sie bei Name einen Namen für Ihre Routing-Tabelle ein.
6. Wählen Sie unter Lokales Gateway Ihr lokales Gateway aus.
7. Wählen Sie unter Modus einen Modus für die Kommunikation mit Ihrem On-Premises-Netzwerk aus.
   - Wählen Sie Direktes VPC Routing, um die privaten IP-Adressen Ihrer Instances zu verwenden.
   - Wählen Sie CoIP, um Adressen aus Ihren kundeneigenen IP-Adresspools zu verwenden. Sie können bis zu 10 CoIP-Pools und 100 Blöcke angeben. CIDR Weitere Informationen finden Sie unter CoIP-Pools.
8. (Optional) Um ein Tag hinzuzufügen, wählen Sie Neues Tag hinzufügen und geben Sie einen Tag-Schlüssel und einen Tag-Wert ein.
9. Wählen Sie Lokale Gateway-Routing-Tabelle erstellen aus.

3b: Ordnen Sie das VPC der benutzerdefinierten Routentabelle zu

Gehen Sie wie folgt vor, um Ihrem lokalen Gateway eine VPC Routentabelle zuzuordnen. Sie sind standardmäßig nicht verknüpft.

Um eine Routentabelle VPC mit dem benutzerdefinierten lokalen Gateway zu verknüpfen

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, Zuordnen. VPC
5. Wählen Sie VPCunter ID die Routentabelle aus, die mit dem lokalen Gateway verknüpft werden VPC soll.
6. (Optional) Um ein Tag hinzuzufügen, wählen Sie Neues Tag hinzufügen und geben Sie einen Tag-Schlüssel und einen Tag-Wert ein.
7. Wählen Sie AssociateVPC aus.

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

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

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

Bestimmungsort	Ziel
172.16.100.0/24	`lgw-id`

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

1. Öffnen Sie die VPC Amazon-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Route-Tabellen und anschließend die Routing-Tabelle aus, in der Sie sie erstellt haben2b: 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 zum Kundennetzwerk ein.
6. Wählen Sie für Target die Outpost Local Gateway ID aus.
7. Wählen Sie Änderungen speichern.

3d: Ordnen Sie die benutzerdefinierte Routentabelle den Gruppen zu VIF

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

Um die benutzerdefinierte Routentabelle den VIF Gruppen zuzuordnen

1. Öffnen Sie die AWS Outposts Konsole unter https://console.aws.amazon.com/outposts/.
2. Um das zu ändern AWS-Region, verwenden Sie die Regionsauswahl in der oberen rechten Ecke der Seite.
3. Wählen Sie im Navigationsbereich Lokale Gateway-Routing-Tabellen aus.
4. Wählen Sie die Routing-Tabelle.
5. Wählen Sie im Detailbereich die Registerkarte VIFGruppenzuordnung und dann Gruppenzuordnung bearbeiten VIF aus.
6. Wählen Sie für VIFGruppeneinstellungen die Option VIFGruppe zuordnen und wählen Sie eine VIF Gruppe aus.
7. Wählen Sie Änderungen speichern.

3e: Fügen Sie der Routentabelle einen Routeneintrag hinzu

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

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

Um einen Routeneintrag zur Routentabelle hinzuzufügen LGW

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

2. Wählen Sie im Navigationsbereich Lokale Gateway-Routing-Tabelle aus.
3. Wählen Sie die Routentabelle des lokalen Gateways aus und klicken Sie dann auf Aktionen, Routen bearbeiten.
4. Wählen Sie Route hinzufügen aus.
5. Geben Sie als Ziel den CIDR Zielblock, eine einzelne IP-Adresse oder die ID einer Präfixliste ein.
6. Wählen Sie unter Target die ID des lokalen Gateways aus.
7. Wählen Sie Save Rules (Routen speichern) aus.

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

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

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

Freigegebene kundeneigene IP-Adresspools

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

Schritt 4: Konfigurieren Sie das lokale Netzwerk

Der Outpost richtet ein externes BGP Peering von jedem Outpost-Netzwerkgerät (OND) zu einem lokalen Netzwerkgerät des Kunden (CND) ein, um Datenverkehr von Ihrem lokalen Netzwerk an die Outposts zu senden und zu empfangen. Weitere Informationen finden Sie unter Lokale Gateway-Konnektivität. BGP

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

- Auf den Netzwerkgeräten Ihrer Kunden VLAN befindet sich die BGP Sitzung auf dem lokalen Gateway im ACTIVE Status Ihrer Netzwerkgeräte.

- Stellen Sie bei Traffic, der von lokalen Standorten zu Außenstellen geleitet wird, sicher, dass Sie in Ihren Nachrichten CND die BGP Werbung von Outposts erhalten. Diese BGP Werbung enthält die Routen, die Ihr lokales Netzwerk verwenden muss, um den Verkehr von den lokalen Standorten 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 Außenstellen zum lokalen Netzwerk geleitet wird, sicher, dass Sie CNDs die BGP Routenankündigungen der lokalen Netzwerksubnetze an Outposts (oder 0.0.0.0/0) senden. Als Alternative können Sie eine Standardroute (z. B. 0.0.0.0/0) zu Outposts ankündigen. Die von der beworbenen lokalen Subnetze CNDs müssen einen CIDR Bereich haben, der dem Bereich entspricht oder in dem Bereich enthalten ist, in dem Sie konfiguriert haben. CIDR 3e: Fügen Sie der Routentabelle einen Routeneintrag hinzu

Beispiel: BGP Werbung im Direktmodus VPC

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

- A VPC mit einem CIDR Block 10.0.0.0/16.
- Ein Outpost-Subnetz im mit einem Block 10.0.3.0/24VPC. CIDR
- Ein Subnetz im lokalen Netzwerk mit einem Block 172.16.100.0/24 CIDR
- 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 angekündigt von:

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

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

Die spezifischen Befehle und die Konfiguration, die zur Überprüfung des Status der BGP Sitzungen und der angekündigten 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 Outpost-Rack-Netzwerkgeräten haben, die über ein lokales Gateway VLAN mit zwei lokalen Netzwerkgeräten des Kunden verbunden sind. Folgendes ist konfiguriert:

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

In diesem Szenario wird die Route angekündigt von:

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

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

Die spezifischen Befehle und die Konfiguration, die zur Überprüfung des Status der BGP Sitzungen und der angekündigten 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 im Outpost-Subnetz, das Sie erstellt haben, oder in einem Outpost-Subnetz, das mit Ihnen geteilt wurde, starten. Sicherheitsgruppen kontrollieren den eingehenden

und ausgehenden VPC Verkehr für Instances in einem Outpost-Subnetz genauso wie für Instances in einem Availability Zone-Subnetz. Um eine Verbindung zu einer EC2 Instance in einem Outpost-Subnetz herzustellen, können Sie beim Starten der Instance ein key pair angeben, genau wie bei Instances in einem Availability Zone-Subnetz.

Überlegungen

- Sie können eine Platzierungsgruppe erstellen, um zu beeinflussen, wie Amazon versuchen EC2 soll, Gruppen voneinander abhängiger Instances auf der Outposts-Hardware zu platzieren. Sie können die Platzierungsgruppenstrategie wählen, die den Anforderungen Ihres Workloads entspricht.
- Wenn Ihr Outpost für die Verwendung eines kundeneigenen IP-Adresspools (CoIP) konfiguriert wurde, müssen Sie allen Instances, die Sie starten, eine kundeneigene IP-Adresse zuweisen.

So starten Sie Instances in Ihrem Outpost-Subnetz

1. Öffnen Sie die AWS Outposts Konsole unter. https://console.aws.amazon.com/outposts/
2. Wählen Sie im Navigationsbereich Outposts aus.
3. Wählen Sie Ihren Outpost aus und klicken Sie anschließend auf Aktionen, Details anzeigen.
4. Wählen Sie auf der Outpost-Übersichtsseite die Option Instance starten aus. Sie werden zum Instance-Startassistenten in der EC2 Amazon-Konsole weitergeleitet. Wir wählen das Outpost-Subnetz für Sie aus und zeigen Ihnen nur die Instance-Typen, die von Ihrem Outposts-Rack unterstützt werden.
5. Wählen Sie einen Instance-Typ, der von Ihrem Outposts-Rack unterstützt wird. Beachten Sie, dass Instances, die ausgegraut erscheinen, nicht verfügbar sind.
6. (Optional) Um die Instances in einer Platzierungsgruppe zu starten, erweitern Sie Erweiterte Details und scrollen Sie zur Platzierungsgruppe. Sie können entweder eine bestehende Platzierungsgruppe auswählen oder eine neue Platzierungsgruppe erstellen.
7. Schließen Sie den Assistenten ab, um die Instance in Ihrem Outpost-Subnetz zu starten. Weitere Informationen finden Sie unter Launch an EC2 Instance im EC2Amazon-Benutzerhandbuch:

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

Schritt 6: Testen Sie die Konnektivität

Sie können die Konnektivität anhand der entsprechenden Anwendungsfälle testen.

Die Konnektivität von Ihrem lokalen Netzwerk zum Outpost testen

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

```
ping 10.0.3.128
```

Es folgt eine Beispielausgabe.

```
Pinging 10.0.3.128

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

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

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

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

Verwenden Sie je nach Betriebssystem ssh oder rdp, um eine Verbindung zur privaten IP-Adresse Ihrer Outpost-Instance herzustellen. Informationen zum Herstellen einer Verbindung mit einer Linux-Instance finden Sie unter Verbindung zu Ihrer EC2 Instance herstellen im EC2Amazon-Benutzerhandbuch.

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

```
ping 172.16.0.130
```

Es folgt eine Beispielausgabe.

```
Pinging 172.16.0.130
```

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

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

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

Testen Sie die Konnektivität zwischen der AWS Region und dem Outpost

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

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

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

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

   ```
   ping 10.0.1.5
   ```

   Es folgt eine Beispielausgabe.

   ```
   Pinging 10.0.1.5

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

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

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

Kundeneigene IP-Adressen-Konnektivitätsbeispiele

Die Konnektivität von Ihrem lokalen Netzwerk zum Outpost testen

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

```
ping 172.16.0.128
```

Es folgt eine Beispielausgabe.

```
Pinging 172.16.0.128

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

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

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

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

Verwenden Sie je nach Betriebssystem ssh oder rdp, um eine Verbindung zur privaten IP-Adresse Ihrer Outpost-Instance herzustellen. Weitere Informationen finden Sie unter Connect zu Ihrer EC2 Instance herstellen im EC2Amazon-Benutzerhandbuch.

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

```
ping 172.16.0.130
```

Es folgt eine Beispielausgabe.

```
Pinging 172.16.0.130

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

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

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

Testen Sie die Konnektivität zwischen der AWS Region und dem Outpost

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

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

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

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

   ```
   ping 10.0.0.5
   ```

   Es folgt eine Beispielausgabe.

   ```
   Pinging 10.0.0.5
   ```

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

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

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

Optimieren Sie Amazon EC2 für AWS Outposts

Im Gegensatz zur AWS-Region Amazon Elastic Compute Cloud (AmazonEC2) ist die Kapazität auf einem Outpost begrenzt. Sie sind durch das Gesamtvolumen der von Ihnen bestellten Rechenkapazität eingeschränkt. Dieses Thema bietet bewährte Methoden und Optimierungsstrategien, mit denen Sie Ihre EC2 Amazon-Kapazität in optimal nutzen können AWS Outposts.

Inhalt

Dedicated Hosts auf Outposts

Ein Amazon EC2 Dedicated Host ist ein physischer Server mit EC2 Instance-Kapazität, die vollständig für Ihre Nutzung reserviert ist. Ihr Outpost stellt Ihnen bereits dedizierte Hardware bereit, Dedicated Hosts gestatten Ihnen jedoch, vorhandene Softwarelizenzen pro Socket, Kern oder VM für einen Host zu verwenden. Weitere Informationen finden Sie unter Dedicated Hosts on AWS Outposts im EC2Amazon-Benutzerhandbuch.

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

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

Ändern des Kapazitätslayouts eines Servers

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

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

Weitere Informationen finden Sie unter Allocate a Dedicated Host im EC2Amazon-Benutzerhandbuch.

Instance-Platzierung auf Hardwareebene steuern

Sie können Dedicated Hosts verwenden, um die Instance-Platzierung auf Hardwareebene zu steuern. Verwenden Sie die automatische Platzierung für Dedicated Hosts, um zu verwalten, ob Instances, die Sie starten, auf einem bestimmten Host oder auf einem beliebigen verfügbaren Host mit passender Konfiguration gestartet werden. Verwenden Sie die Host-Affinität, um eine Beziehung zwischen einer Instance und einem Dedicated Host herzustellen. Wenn Sie ein Outposts-Rack haben, können Sie diese Dedicated Hosts-Funktionen verwenden, um die Auswirkungen korrelierter Hardwarefehler zu minimieren. Weitere Informationen zur Instance-Wiederherstellung finden Sie unter Dedicated Host Auto Placement and Host Affinity im EC2Amazon-Benutzerhandbuch.

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

Einrichten der Instance-Wiederherstellung

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

Platzierungsgruppen auf Outposts

AWS Outposts unterstützt Platzierungsgruppen. Verwenden Sie Platzierungsgruppen, um zu beeinflussen, wie Amazon versuchen EC2 soll, Gruppen voneinander abhängiger Instances, die Sie starten, auf der zugrunde liegenden Hardware zu platzieren. Sie können verschiedene Strategien (Cluster, Partition oder Spread) verwenden, um den Anforderungen verschiedener Workloads gerecht zu werden. Wenn Sie einen Outpost mit einem Rack haben, können Sie die Spread-Strategie verwenden, um Instances auf mehreren Hosts statt auf Racks zu platzieren.

Spread Placement-Gruppen

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

Placement-Gruppen auf Rack-Spread-Ebene

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

Placement-Gruppen auf Host-Spread-Ebene

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

Partitions-Placement-Gruppen

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

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

Weitere Informationen zur Arbeit mit Placement-Gruppen finden Sie unter Placement-Gruppen und Placement-Gruppen auf AWS Outposts im EC2Amazon-Benutzerhandbuch.

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

AWS Outposts Konnektivität zu AWS Regionen

AWS Outposts unterstützt Wide Area Network-Konnektivität (WAN) 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 Verkehr zu und von der AWS Region. Der Service Link nutzt einen verschlüsselten Satz von VPN Verbindungen, um mit der Heimatregion zu kommunizieren.

Um die Service Link-Konnektivität einzurichten, müssen Sie oder AWS müssen während der Outpost-Bereitstellung die physische, virtuelle LAN (VLAN) und Netzwerkebenenkonnektivität des Service Links 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 AWS Outposts können Service VPN Link-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 AWS Direct Connect öffentliche virtuelle Schnittstellen erfolgen kann. Die aktuellen IP-Adressbereiche finden Sie unter AWSIP-Adressbereiche im VPCAmazon-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 BGP Link-Konnektivität und Service Link-Infrastruktur, Subnetzankündigung 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:

- VPCKundenverkehr zwischen dem Outpost und allen verbundenen Unternehmen. VPCs
- Outposts-Verwaltungsverkehr, wie Ressourcenverwaltung, Ressourcenüberwachung und Firmware- und Software-Updates.

Maximale Anforderungen an die Übertragungseinheit (MTU) für die Service-Verbindung

Die maximale Übertragungseinheit (MTU) einer Netzwerkverbindung entspricht der Größe des größten zulässigen Pakets, das über die Verbindung übertragen werden kann, in Byte. Das Netzwerk muss 1500 Byte MTU zwischen dem Outpost und den Service Link-Endpunkten in der übergeordneten Region unterstützen. AWS Informationen zu den Anforderungen MTU zwischen einer Instance im Outpost und einer Instance in der AWS Region über den Service-Link finden Sie unter Network maximum transmission unit (MTU) für Ihre EC2 Amazon-Instance im EC2Amazon-Benutzerhandbuch.

Empfehlungen für die Bandbreite von Service Links

Für eine optimale Benutzererfahrung und Ausfallsicherheit AWS müssen Sie redundante Konnektivität mit mindestens 500 Mbit/s (1 Gbit/s ist besser) und eine maximale Roundtrip-Latenz von 175 ms für die Service Link-Verbindung zur Region verwenden. AWS Sie können für den Service Link eine Internetverbindung verwenden AWS Direct Connect . Die Mindestanforderungen von 500 Mbit/s und die maximale Roundtrip-Zeit für die Service Link-Verbindung ermöglichen es Ihnen, EC2 Amazon-Instances zu starten, EBS Amazon-Volumes anzuhängen und auf AWS Services wie Amazon EKSEMR, Amazon und CloudWatch Metriken mit optimaler Leistung zuzugreifen.

Die Bandbreitenanforderungen für Outposts variieren aufgrund der folgenden Merkmale:

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

Wenden Sie sich an Ihren AWS Vertriebsmitarbeiter oder APN Partner, um eine individuelle Empfehlung zur für Ihre Anforderungen 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 den Amazon VPC von der AWS Region bis zum Außenposten. Eine AWS Direct Connect öffentliche virtuelle Schnittstelle ist die Service Link-Verbindung. Der folgende Datenverkehr wird über den Service Link und die AWS Direct Connect -Verbindung abgewickelt:

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

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

Wenn Sie eine Firewall verwenden, um die Konnektivität über den Service Link einzuschränkenVLAN, 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	AWS Outposts Öffentliche Routen der Region
TCP	1025-65535	AWS Outposts Servicelink /26	443	AWS Outposts Öffentliche Routen der 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.
> AWS Outposts Die Racks sind außerdem mit redundanter Stromversorgung und Netzwerkausrüstung ausgestattet, einschließlich lokaler Gateway-Komponenten. Weitere Informationen finden Sie unter Resilienz in AWS Outposts.

Private Service Link-Konnektivität mit VPC

Sie können die Option für private Konnektivität in der Konsole auswählen, wenn Sie Ihren Outpost erstellen. Wenn Sie dies tun, wird nach der Installation von Outpost eine Service VPN Link-Verbindung unter Verwendung eines VPC von Ihnen angegebenen UND-Subnetzes hergestellt. Dies ermöglicht private Konnektivität über das 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 Berechtigungen für eine IAM Entität (Benutzer oder Rolle) konfigurieren, damit der Benutzer oder die Rolle die dienstbezogene 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 erhalten Sie unter Identitäts- und Zugriffsmanagement () für IAM AWS Outposts und Mit Diensten verknüpfte Rollen für AWS Outposts.

- Erstellen Sie im selben AWS Konto und in derselben Availability Zone wie Ihr Outpost eine VPC private Konnektivität mit einem Subnetz /25 oder höher, das nicht mit 10.1.0.0/16 in Konflikt steht. 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 lokaler Outpost auf die zugreifen kann. VPC Wenn die AWS Direct Connect Verbindung über ein anderes AWS Konto als Ihr Konto erfolgtVPC, finden Sie weitere Informationen unter Kontenübergreifendes Zuordnen eines virtuellen privaten Gateways im AWS Direct Connect Benutzerhandbuch.
- Machen Sie das Subnetz CIDR in Ihrem lokalen Netzwerk bekannt. Sie können es verwenden AWS Direct Connect , um dies zu tun. Weitere Informationen finden Sie unter AWS Direct Connect Virtuelle 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. Detaillierte Anweisungen finden Sie unter Eine Bestellung für ein Outposts-Rack erstellen.

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

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

- Erstellt Netzwerkschnittstellen in dem von Ihnen angegebenen Subnetz und VPC erstellt eine Sicherheitsgruppe für die Netzwerkschnittstellen.
- Erteilt dem AWS Outposts Dienst die Berechtigung, die Netzwerkschnittstellen an eine Service Link-Endpunktinstanz im Konto anzuhängen.
- Hängt die Netzwerkschnittstellen vom Konto aus an die Service Link-Endpunkt-Instances an.

Weitere Informationen zur serviceverknüpften Rolle finden Sie unter Mit Diensten verknüpfte Rollen für AWS Outposts.

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

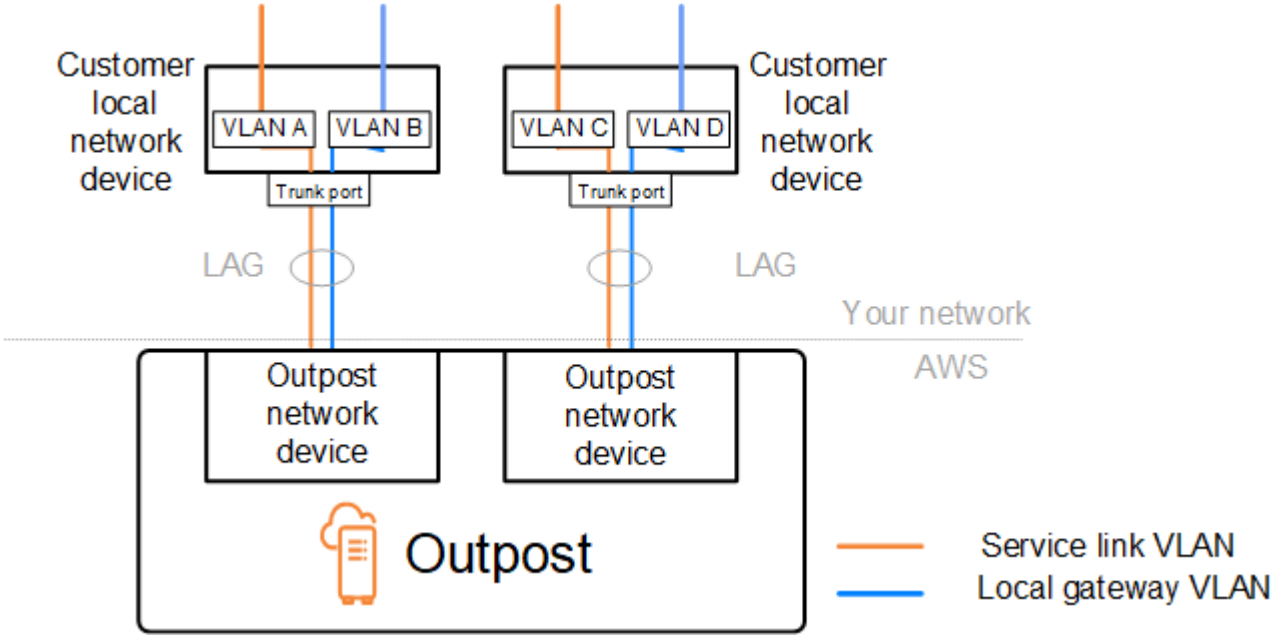
Redundante Internetverbindungen

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

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

Checkliste zur Fehlerbehebung bei Outposts-Rack-Netzwerken

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



Konnektivität mit Outpost-Netzwerkgeräten

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

1. Pingen Sie die Remote-Peer-IP-Adresse auf den Outpost-Netzwerkgeräten von den Kundengeräten aus. Die Peer-IP-Adresse finden Sie 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 Nummer des autonomen Systems (KundeASN) korrekt konfiguriert ist.
   b. Vergewissern Sie sich, dass die Nummer des autonomen Fernsystems (OutpostASN) 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 Aktiv- und Verbindungsstatus hin- und herschwankt, stellen Sie sicher, dass 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. BGPund Debug-Protokolle TCP

   b. BGPLogs

   c. Paketerfassung

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

Wenn der BGP Peering-Status `UP` zwischen den lokalen Netzwerkgeräten des Kunden und den Outpost-Netzwerkgeräten besteht, der Service-Link jedoch weiterhin besteht`DOWN`, 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 die Service Link-Konnektivität verwendet wird. Weitere Informationen finden Sie unter AWS Direct Connect Konnektivität über öffentliche virtuelle Schnittstellen zur Region AWS.
- Edge-Router, verbunden mit AWS Direct Connect — Private virtuelle Schnittstelle, die für die Service Link-Konnektivität verwendet wird. Weitere Informationen finden Sie unter AWS Direct Connect private virtuelle Schnittstelle, Konnektivität zur AWS Region.
- Edge-Router, die mit Internetdienstanbietern verbunden sind (ISPs) — Öffentliches Internet, das für Service Link-Konnektivität verwendet wird. Weitere Informationen finden Sie unter ISPöffentliche Internetverbindung zur AWS Region.

AWS Direct Connect Konnektivität über öffentliche virtuelle Schnittstellen zur Region AWS

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

1. Vergewissern Sie sich, dass die Geräte, die eine direkte Verbindung zu den Outpost-Netzwerkgeräten herstellen, die IP-Adressbereiche für den Service Link über empfangen. BGP

   a. Bestätigen Sie die Routen, über die Sie BGP von Ihrem Gerät empfangen werden.

   b. Überprüfen Sie die Routing-Tabelle der Service-Link-Instanz für virtuelles Routing and Forwarding (VRF). Die Anzeige sollte zeigen, dass der IP-Adressbereich verwendet wird.

2. Um die Konnektivität der Region sicherzustellen, überprüfen Sie die Routentabelle für den Service-LinkVRF. Sie sollte die AWS öffentlichen IP-Adressbereiche oder die Standardroute enthalten.
3. Wenn Sie die AWS öffentlichen IP-Adressbereiche nicht über den Service-Link erhaltenVRF, überprüfen Sie die folgenden Punkte.
   a. Überprüfen Sie den AWS Direct Connect Verbindungsstatus vom Edge-Router oder vom AWS Management Console.
   b. Wenn die physische Verbindung aktiviert istUP, überprüfen Sie den BGP Peering-Status vom Edge-Router aus.
   c. Wenn der BGP Peering-Status lautetDOWN, pingen Sie die AWS Peer-IP-Adresse an und überprüfen Sie die BGP Konfiguration im Edge-Router. Weitere Informationen finden Sie unter Problembehandlung AWS Direct Connect im AWS Direct Connect Benutzerhandbuch und Mein virtueller BGP Schnittstellenstatus ist ausgefallen in der AWS Konsole. Was soll ich tun?.
   d. Wenn BGP es eingerichtet ist und Sie die Standardroute oder die AWS öffentlichen IP-Adressbereiche im nicht sehenVRF, wenden Sie sich AWS mithilfe Ihres Enterprise-Supportplans an den Support.
4. Wenn Sie eine On-Premises-Firewall haben, überprüfen Sie die folgenden Elemente.
   a. Vergewissern Sie sich, dass die für die Service Link-Konnektivität erforderlichen Ports in den Netzwerk-Firewalls zulässig sind. Verwenden Sie Traceroute auf Port 443 oder ein anderes Tool zur Netzwerkfehlerbehebung, um die Konnektivität zwischen den Firewalls und Ihren Netzwerkgeräten zu überprüfen. Die folgenden Ports müssen in den Firewall-Richtlinien für die Service Link-Konnektivität konfiguriert werden.
      - TCPProtokoll — Quellport: TCP 1025-65535, Zielport: 443.
      - UDPProtokoll — 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 IP-Adressbereichen zuordnen. AWS Weitere Informationen finden Sie unter AWS Outposts Konnektivität zu AWS Regionen.
   c. Wenn die Firewall nicht statusbehaftet ist, stellen Sie sicher, dass auch der eingehende Datenfluss zugelassen ist (von den AWS öffentlichen IP-Adressbereichen bis zum IP-Adressbereich des Service Links).
   d. Wenn Sie in den Firewalls einen virtuellen Router konfiguriert haben, stellen Sie sicher, dass das entsprechende Routing für den Datenverkehr zwischen dem Outpost und der AWS -Region konfiguriert ist.

5. Wenn Sie NAT im lokalen Netzwerk so konfiguriert haben, dass die Service-Link-IP-Adressbereiche von 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 Anschlüsse 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 AWS Ihres Enterprise-Supportplans mit dem Support.

AWS Direct Connect private virtuelle Schnittstelle, Konnektivität zur AWS Region

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

1. Wenn die Konnektivität zwischen dem Outposts-Rack und der AWS Region die AWS Outposts private Konnektivitätsfunktion verwendet, überprüfen Sie die folgenden Punkte.
   a. Pingen Sie die AWS Remote-Peering-IP-Adresse vom Edge-Router aus an und bestätigen Sie den BGP Peering-Status.
   b. Stellen Sie sicher, dass das BGP Peering über die AWS Direct Connect private virtuelle Schnittstelle zwischen Ihrem Service Link-Endpunkt VPC und dem in Ihren Räumlichkeiten installierten Outpost erfolgt. UP Weitere Informationen finden Sie unter Problembehandlung AWS Direct Connect im AWS Direct Connect Benutzerhandbuch, Mein virtueller BGP Schnittstellenstatus ist ausgefallen in der AWS Konsole. Was sollte ich tun? , und Wie kann ich BGP Verbindungsprobleme über Direct Connect beheben? .
   c. Die AWS Direct Connect private virtuelle Schnittstelle ist eine private Verbindung zu Ihrem Edge-Router an Ihrem ausgewählten AWS Direct Connect Standort und dient BGP zum Austausch von Routen. Ihr privater virtueller privater CIDR Cloud-Bereich (VPC) wird während dieser BGP Sitzung Ihrem Edge-Router mitgeteilt. In ähnlicher Weise wird der IP-Adressbereich für den Outpost-Servicelink der Region BGP von Ihrem Edge-Router aus bekannt gegeben.
   d. Vergewissern Sie sich, dass das Netzwerk, das mit dem privaten Service-Link-Endpunkt in Ihrem System ACLs verknüpft ist, den entsprechenden Datenverkehr VPC zulässt. Weitere Informationen finden Sie unter Checkliste zur Netzwerkbereitschaft.

e. Wenn Sie über eine lokale Firewall verfügen, stellen Sie sicher, dass die Firewall über Regeln für ausgehenden Datenverkehr verfügt, die die IP-Adressbereiche für den Service Link und die Outpost-Servicendpunkte (die IP-Adressen der Netzwerkschnittstelle) zulassen, die sich im oder im befinden. VPC VPC CIDR Stellen Sie sicher, dass die Ports TCP 1025-65535 und 443 nicht blockiert sind. UDP Weitere Informationen finden Sie unter Einführung in private Konnektivität. AWS Outposts

f. Wenn die Firewall nicht statusbehaftet ist, stellen Sie sicher, dass die Firewall über Regeln und Richtlinien verfügt, die eingehenden Datenverkehr zum Outpost von den Outpost-Dienstendpunkten in der zulassen. VPC

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

ISPöffentliche Internetverbindung zur AWS Region

Verwenden Sie die folgende Checkliste, um Fehler bei Edge-Routern zu beheben, die über und ISP bei Verwendung des öffentlichen Internets für Service Link-Konnektivität verbunden sind.

- Vergewissern Sie sich, dass die Internetverbindung aktiv ist.
- Vergewissern Sie sich, dass auf die öffentlichen Server von Ihren Edge-Geräten aus zugegriffen werden kann, die über eine verbunden sind. ISP

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 hergestellt ist.
   a. Vergewissern Sie sich, dass der nicht BGP flattert.
   b. Vergewissern Sie BGP sich, dass der die erforderlichen Routen von empfängt und ankündigt. ISP
2. Überprüfen Sie bei einer statischen Routenkonfiguration, ob die Standardroute auf dem Edge-Gerät ordnungsgemäß konfiguriert ist.

3. Bestätigen Sie, ob Sie über eine andere ISP Verbindung auf das Internet zugreifen können.
4. Wenn das Problem weiterhin besteht, führen Sie MTR /traceroute/-Paketerfassungen auf Ihrem Edge-Router durch. Teilen Sie die Ergebnisse Ihrem technischen Support-Team mitISP, um weitere Probleme zu beheben.

Wenn über die ISP Links auf das Internet und öffentliche 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 den Datenverkehr in Ihrem Netzwerk trennen, vergewissern Sie sich, dass der Service-Link VRF über Routen oder Richtlinien verfügt, die den Datenverkehr zum und vom ISP (Internet) und weiterleiten. VRF Sehen Sie sich die folgenden Checkpoints an.
   a. Edge-Router, die eine Verbindung mit dem ISP herstellen. Überprüfen Sie in der ISP VRF Routing-Tabelle des Edge-Routers, ob der IP-Adressbereich für den Service Link vorhanden ist.
   b. Lokale Netzwerkgeräte des Kunden, die eine Verbindung zum Outpost herstellen. Überprüfen Sie die Konfigurationen von VRFs und stellen Sie sicher, dass das Routing und die Richtlinien, die für die Konnektivität zwischen dem Service Link VRF und dem erforderlich ISP VRF sind, ordnungsgemäß konfiguriert sind. Normalerweise wird für den Datenverkehr VRF zum Internet eine Standardroute vom ISP VRF in den Service-Link gesendet.
   c. Wenn Sie in den Routern, die mit Ihrem Outpost verbunden sind, quellenbasiertes Routing konfiguriert haben, vergewissern Sie sich, dass die Konfiguration korrekt ist.
3. Stellen Sie sicher, dass die lokalen Firewalls so konfiguriert sind, dass sie ausgehende Konnektivität (Ports TCP 1025-65535 und UDP 443) von den IP-Adressbereichen des Outpost Service Links zu den öffentlichen IP-Adressbereichen zulassen. AWS Wenn die Firewalls nicht zustandsorientiert sind, stellen Sie sicher, dass die eingehende Verbindung zum Outpost ebenfalls konfiguriert ist.
4. Stellen Sie sicher, dass dies im lokalen Netzwerk so konfiguriert NAT ist, dass die Service-Link-IP-Adressbereiche von 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, die für neue Sitzungen reserviert werden können.
   b. Das NAT Gerät ist für die Adressübersetzung 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 Netzwerks verloren gehen oder blockiert werden, wenden Sie sich an den technischen Support ISP des Netzwerks. ISP
- Wenn die Ergebnisse keine Probleme zeigen, sammeln Sie die Ergebnisse aller Tests (z. B. TelnetMTR, Traceroute, Paketerfassung und BGP Protokolle) und wenden Sie sich über Ihren AWS Enterprise-Supportplan an den Support.

Outposts steckt hinter zwei Firewall-Geräten

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

- Überprüfen Sie, ob in letzter Zeit Änderungen oder laufende Wartungsarbeiten an der Routingkonfiguration Ihres Unternehmensnetzwerks vorgenommen wurden, die möglicherweise zu einem asymmetrischen Routing des Service Links durch die Firewalls geführt haben.
  - Verwenden Sie Firewall-Verkehrsdiagramme, um nach Änderungen der Verkehrsmuster zu suchen, die mit dem Beginn des Service-Link-Problems übereinstimmen.
  - Suchen Sie nach einem teilweisen Firewallausfall oder einem Szenario mit geteilten Firewall-Paaren, das möglicherweise dazu geführt hat, dass Ihre Firewalls ihre Verbindungstabellen nicht mehr miteinander synchronisieren.
  - Suchen Sie in Ihrem Unternehmensnetzwerk nach nicht funktionierenden Links oder nach kürzlichen Änderungen am BGP Routing (OSPFISIS//EIGRPMetrikänderungen, Änderungen der Routenzuweisung), die mit dem Beginn des Service-Link-Problems übereinstimmen.
- Wenn Sie eine öffentliche Internetverbindung für die Verbindung zur Heimatregion verwenden, könnte eine Wartung durch den Dienstanbieter zu einem asymmetrischen Routing der Serviceverbindung durch die Firewalls geführt haben.
  - Suchen Sie in den Verkehrsdiagrammen nach Links zu Ihren ISP (n), ob sich die Verkehrsmuster geändert haben, die mit dem Beginn des Dienstverbindungsproblems übereinstimmen.

- Wenn Sie AWS Direct Connect Konnektivität für den Service Link verwenden, ist es möglich, dass eine AWS geplante Wartung ein asymmetrisches Routing des Service Links ausgelöst hat.
  - Suchen Sie nach Benachrichtigungen über geplante Wartungsarbeiten an Ihren AWS Direct Connect Diensten.
  - Beachten Sie, dass Sie bei redundanten AWS Direct Connect Diensten das Routing des Outposts-Servicelinks über jeden wahrscheinlichen Netzwerkpfad unter Wartungsbedingungen proaktiv testen können. Auf diese Weise können Sie testen, ob eine Unterbrechung eines Ihrer AWS Direct Connect Dienste zu einem asymmetrischen Routing der Service-Verbindung führen könnte. Die Widerstandsfähigkeit des AWS Direct Connect Teils der end-to-end Netzwerkkonnektivität kann mit dem Resiliency with AWS Direct Connect Resiliency Toolkit getestet werden. Weitere Informationen finden Sie unter Resilienz mit dem AWS Direct Connect Resiliency Toolkit testen — Failover-Tests.

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

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

Lokale Gateways für Ihre Outposts-Racks

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

Inhalt

Grundlagen zu lokalen Gateways

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

Ein lokales Gateway umfasst die folgenden Komponenten:

- Routing-Tabellen — Nur der Besitzer eines lokalen Gateways kann lokale Gateway-Routentabellen erstellen. Weitere Informationen finden Sie unter the section called “Routing-Tabellen”.
- CoIP-Pools — (Optional) Sie können IP-Adressbereiche verwenden, deren Eigentümer Sie sind, um die Kommunikation zwischen dem lokalen Netzwerk und den Instanzen in Ihrem Netzwerk zu erleichtern. VPC Weitere Informationen finden Sie unter the section called “IP-Adressen im Besitz des Kunden”.
- Virtuelle Schnittstellen (VIFs) — AWS erstellt eine VIF für jede Schnittstelle LAG und fügt beide VIFs zu einer VIF Gruppe hinzu. Die Routentabelle des lokalen Gateways muss VIFs für die lokale

Netzwerkkonnektivität eine Standardroute zu den beiden enthalten. Weitere Informationen finden Sie unter Lokale Netzwerkkonnektivität.

- VIFGruppenzuordnungen — AWS VIFs fügt die erstellten Verbindungen zu einer VIF Gruppe hinzu. VIFGruppen sind logische Gruppierungen von. VIFs
- VPCVerknüpfungen — Sie verwenden diese Option, um VPC Verknüpfungen mit Ihrer VPCs und der lokalen Gateway-Routentabelle zu erstellen. VPCRoutentabellen, die Subnetzen zugeordnet sind, die sich in einem Outpost befinden, können das lokale Gateway als Routenziel verwenden.

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

AWS Verantwortlichkeiten

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

Ihre Aufgaben

- Erstellen Sie die Routing-Tabelle des lokalen Gateways.
- Ordnet der VPC lokalen Gateway-Routentabelle eine zu.
- Ordnen Sie der lokalen Gateway-Routentabelle eine VIF Gruppe zu.

Lokales Gateway-Routing

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

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

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

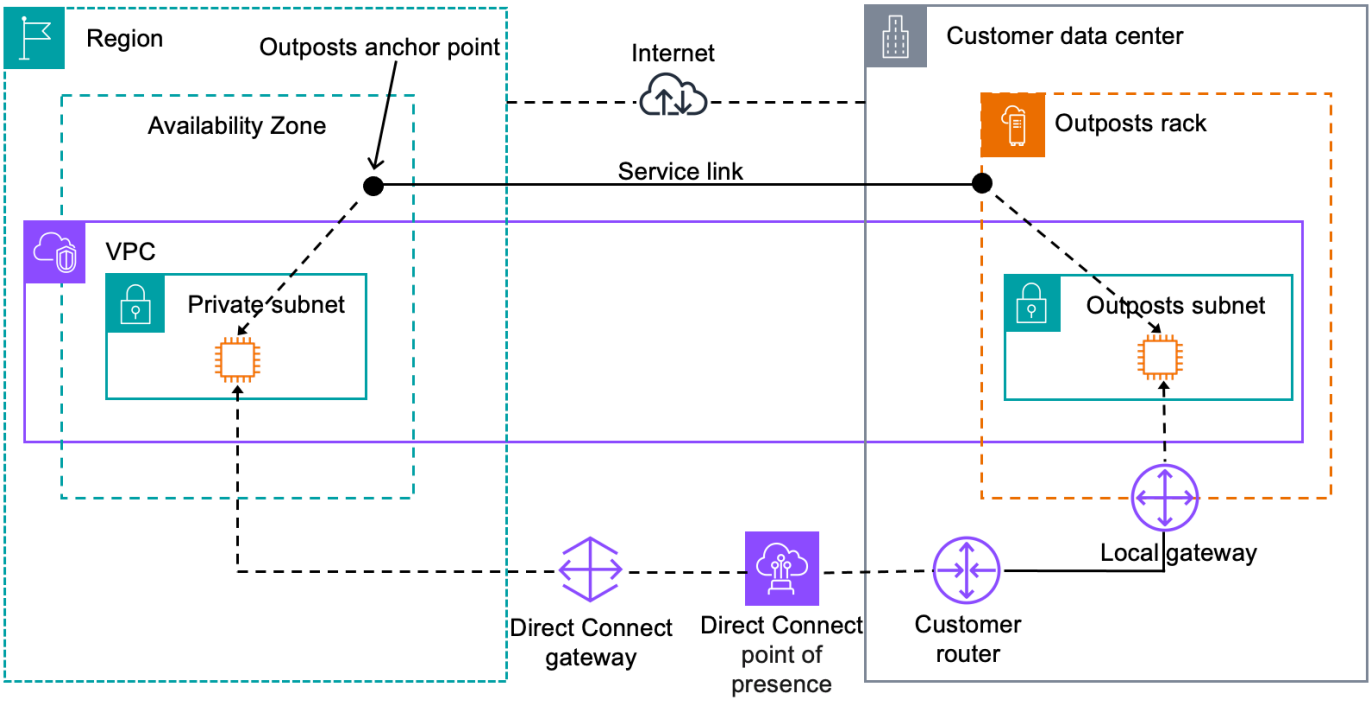
Konnektivität über ein lokales Gateway

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

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

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

Die folgende Abbildung zeigt die Konnektivität über das lokale Gateway:



Routing-Tabellen für das lokale Gateway

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

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.

Routentabellen für lokale Gateways verfügen über einen Modus, der bestimmt, wie Instances Outposts Outposts-Subnetz mit Ihrem lokalen Netzwerk kommunizieren. Die Standardoption ist direktes VPC Routing, bei dem die privaten IP-Adressen der Instances verwendet werden. Die andere Option besteht darin, Adressen aus einem kundeneigenen IP-Adresspool (CoIP) zu verwenden, den Sie bereitstellen. Direktes VPC Routing und CoIP schließen sich gegenseitig aus und steuern, wie das Routing funktioniert.

Sie können die Routingtabelle des lokalen Gateways mit anderen AWS Konten oder Organisationseinheiten gemeinsam nutzen AWS Resource Access Manager, indem Sie. Weitere Informationen finden Sie unter Arbeiten mit gemeinsam genutzten AWS Outposts Ressourcen.

Inhalt

Direktes VPC Routing

Direktes VPC Routing verwendet die private IP-Adresse der Instances in IhremVPC, um die Kommunikation mit Ihrem lokalen Netzwerk zu erleichtern. Diese Adressen werden in Ihrem lokalen Netzwerk mit beworben. BGP Werbung für BGP gilt nur für die privaten IP-Adressen, die zu den Subnetzen in Ihrem Outposts-Rack gehören. Diese Art von Routing ist der Standardmodus für Outposts. In diesem Modus funktioniert das lokale Gateway nicht NAT für Instances, und Sie müssen Ihren EC2 Instances keine Elastic IP-Adressen zuweisen. Sie haben die Möglichkeit, anstelle des

direkten VPC Routing-Modus Ihren eigenen Adressraum zu verwenden. Weitere Informationen finden Sie unter IP-Adressen im Besitz des Kunden.

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

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

Die folgenden Beispiele veranschaulichen das direkte VPC Routing.

Beispiele

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

Beispiel: Internetkonnektivität über VPC

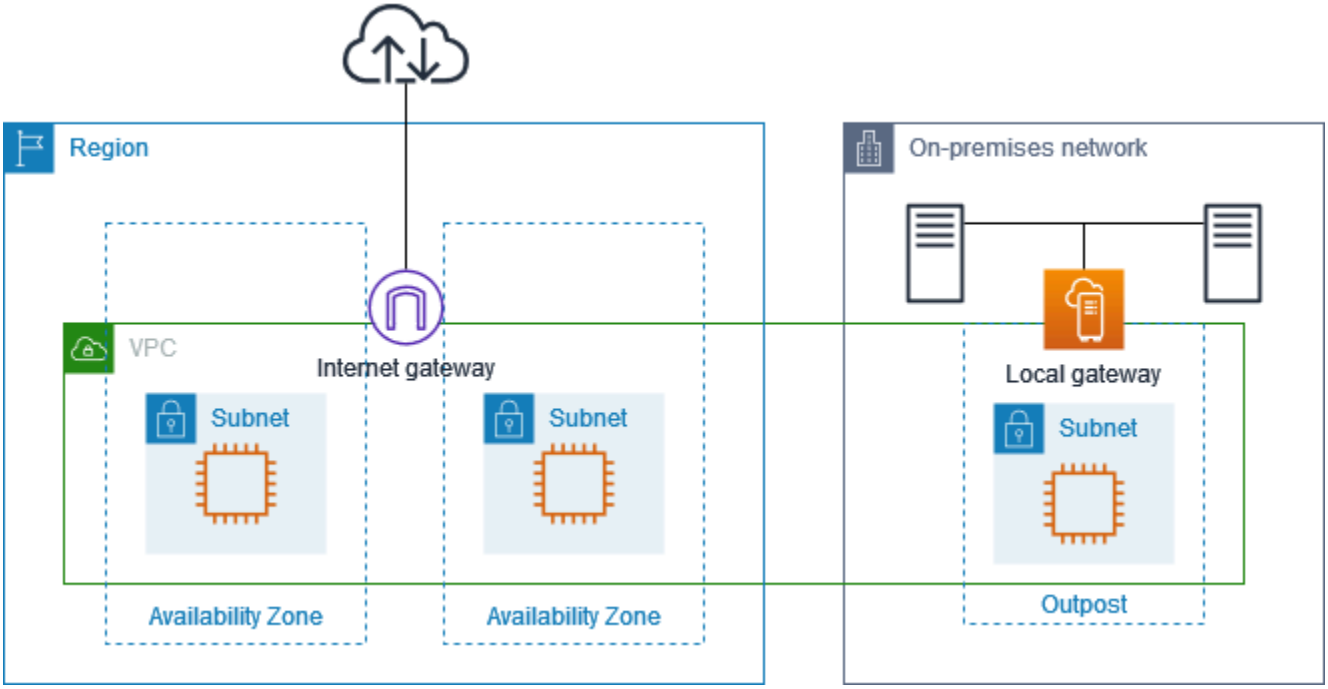
Instances in einem Outpost-Subnetz können über das Internet-Gateway, das an das angeschlossen ist, auf das Internet zugreifen. VPC

Berücksichtigen Sie folgende Konfiguration:

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

> **Note**
>
> BGPWerbung wird nur für Subnetze in einem Outpost unterstützt, die eine Route mit dem lokalen Gateway als Ziel haben. Andere Subnetze werden nicht über angekündigt. BGP

In der folgenden Abbildung kann der Datenverkehr von der Instance im Outpost-Subnetz über das Internet-Gateway VPC auf das Internet zugreifen.



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 bereit. VPC
0.0.0.0	*internet-gateway-id*	Sendet den für das Internet bestimmten Datenverkehr an das Internet-Gateway.
on-premises network CIDR	*local-gateway-id*	Sendet den für das On-Premises-Netzwerk bestimmten Datenverkehr an das lokale Gateway.

Beispiel: Internetkonnektivität über das On-Premises-Netzwerk

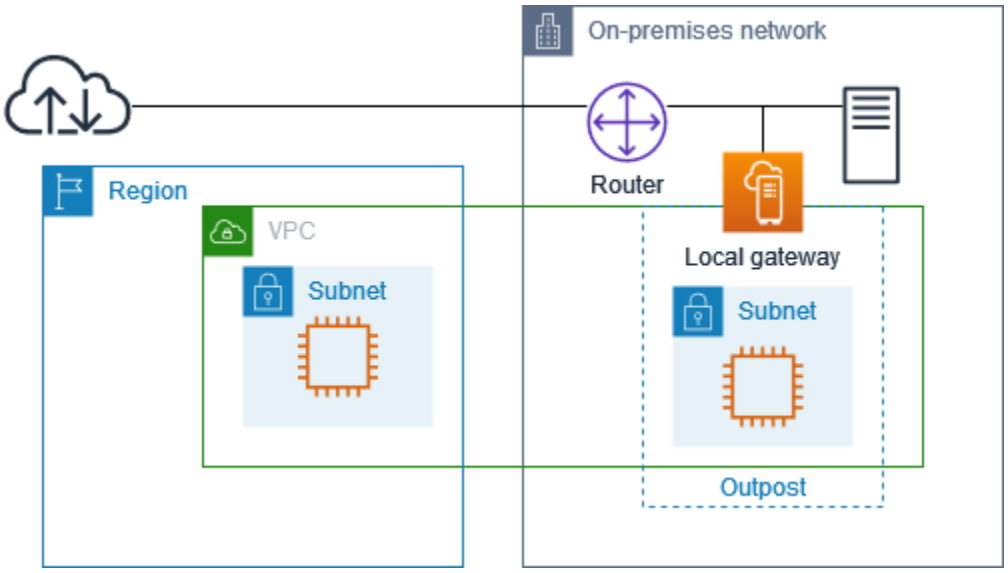
Instances in einem Outpost-Subnetz können über das On-Premises-Netzwerk auf das Internet zugreifen. Instances im Outpost-Subnetz benötigen keine öffentliche IP-Adresse oder Elastic-IP-Adresse.

Berücksichtigen Sie folgende Konfiguration:

- Das Outpost-Subnetz hat eine Instanz. EC2
- Der Router im lokalen Netzwerk führt die Netzwerkadressübersetzung durch (). NAT
- Das lokale Gateway verwendet BGP Werbung, um die privaten IP-Adressen des Outpost-Subnetzes im lokalen Netzwerk bekannt zu geben.

> **Note**
>
> BGPWerbung wird nur für Subnetze in einem Outpost unterstützt, die eine Route mit dem lokalen Gateway als Ziel haben. Andere Subnetze werden nicht über angekündigt. BGP

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 bereit. VPC	

Bestimmungsort	Ziel	Kommentare	
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 übersetzt NAT die private IP-Adresse in eine öffentliche IP-Adresse auf dem Router 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 Verkehr das lokale Gateway erreicht, sendet das lokale Gateway den Verkehr an das Ziel in derVPC.

IP-Adressen im Besitz des Kunden

Standardmäßig verwendet das lokale Gateway die privaten IP-Adressen der Instances in Ihrem, VPC um die Kommunikation mit Ihrem lokalen 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 Routingtabelle des lokalen Gateways zuweisen und diese Adressen dann an Ihr Kundennetzwerk weiterleiten. BGP Alle kundeneigenen IP-Adressen, die mit Ihrer lokalen Gateway-Routing-Tabelle verknüpft sind, werden in der Routing-Tabelle als weitergegebene Routen angezeigt.

Kundeneigene IP-Adressen bieten lokale oder externe Konnektivität zu Ressourcen in Ihrem On-Premises-Netzwerk. Sie können diese IP-Adressen Ressourcen in Ihrem Outpost, z. B. EC2

Instances, zuweisen, indem Sie eine neue Elastic IP-Adresse aus dem kundeneigenen IP-Pool zuweisen und diese dann Ihrer Ressource zuweisen. Weitere Informationen finden Sie unter CoIP-Pools.

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

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

Beispiele

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

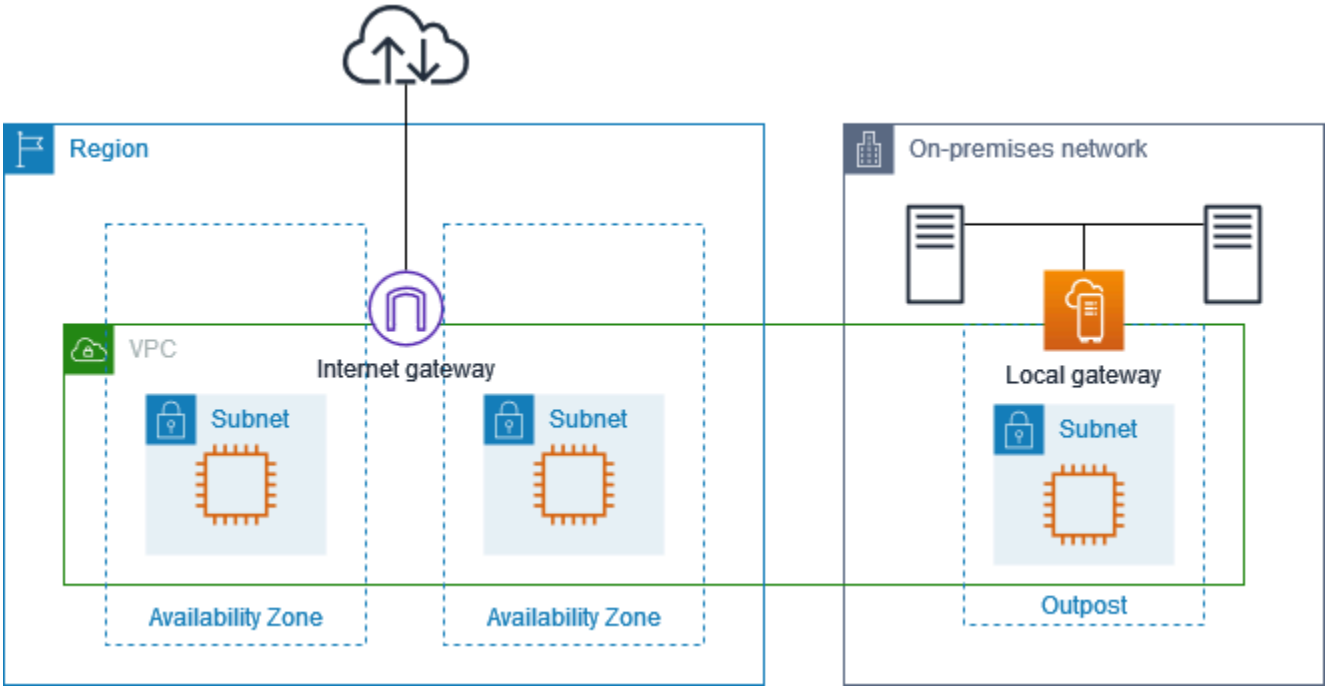
Beispiel: Internetkonnektivität über VPC

Instances in einem Outpost-Subnetz können über das Internet-Gateway, das an das angeschlossen ist, auf das Internet zugreifen. VPC

Berücksichtigen Sie folgende Konfiguration:

- Das übergeordnete System VPC erstreckt sich über zwei Availability Zones und hat in jeder Availability Zone ein Subnetz.
- Der Outpost hat ein Subnetz.
- Jedes Subnetz hat eine Instanz. EC2
- Es gibt einen kundeneigenen IP-Adresspool.
- Die Instance im Outpost-Subnetz hat eine Elastic-IP-Adresse aus dem kundeneigenen IP-Adresspool.

- Das lokale Gateway verwendet BGP Werbung, um den kundeneigenen IP-Adresspool im lokalen Netzwerk bekannt zu geben.



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

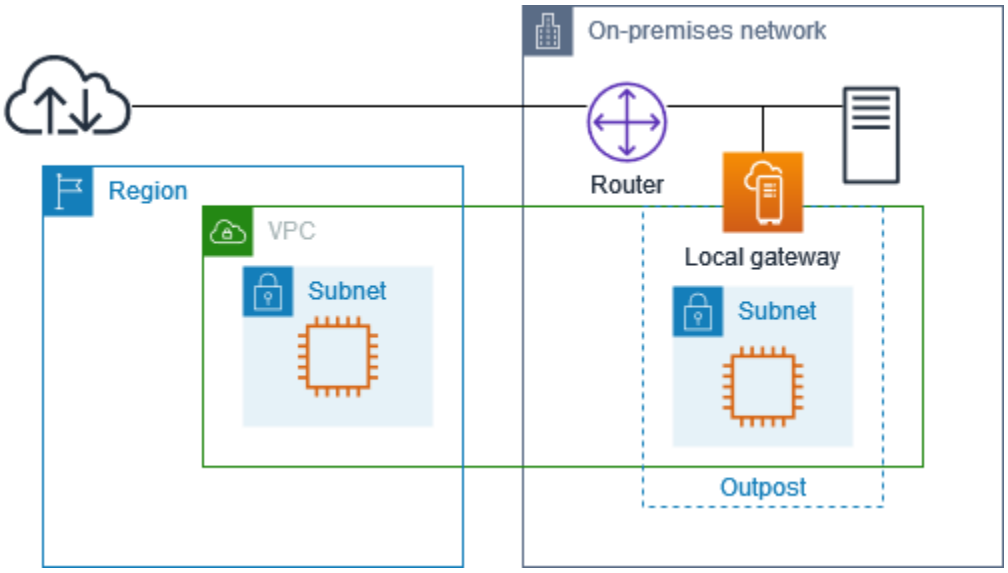
Bestimmungsort	Ziel	Kommentare
VPC CIDR	Local	Stellt Konnektivität zwischen den Subnetzen in der bereit. VPC
0.0.0.0	*internet-gateway-id*	Sendet den für das öffentliche Internet bestimmten Datenverkehr an das Internet-Gateway.
On-premises network CIDR	*local-gateway-id*	Sendet den für das On-Premises-Netzwerk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

Beispiel: Internetkonnektivität über das On-Premises-Netzwerk

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

Berücksichtigen Sie folgende Konfiguration:

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



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 bereit. VPC
0.0.0.0/0	*local-gateway-id*	Sendet den für das Internet bestimmten Datenverkehr an das lokale Gateway.

Ausgehender Zugriff auf das Internet

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

Ausgehender Zugriff auf das On-Premises-Netzwerk

Der Datenverkehr, der von der EC2 Instance im Outpost-Subnetz mit einem Ziel im lokalen Netzwerk initiiert wird, verwendet die Route für 0.0.0.0/0, um den Verkehr an das lokale Gateway weiterzuleiten. Das lokale Gateway übersetzt die IP-Adresse der EC2 Instance in die kundeneigene IP-Adresse (Elastic IP-Adresse) und sendet den Datenverkehr dann an das Ziel.

Eingehender Zugriff aus dem On-Premises-Netzwerk

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

Benutzerdefinierte Routing-Tabellen

Sie können eine benutzerdefinierte Routentabelle für Ihr lokales Gateway erstellen. Die Routentabelle des lokalen Gateways muss eine Zuordnung zu einer VIF Gruppe und einer habenVPC. step-by-step Anweisungen finden Sie unter Lokale Gateway-Konnektivität konfigurieren.

Routen in der Routentabelle des lokalen Gateways

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

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

Es gelten die folgenden Anforderungen und Einschränkungen:

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

Es gelten die folgenden NAT Überlegungen:

- Das lokale Gateway verarbeitet keinen Datenverkehr, NAT der einer Netzwerkschnittstellenroute entspricht. Stattdessen wird die Ziel-IP-Adresse beibehalten.
- Schalten Sie die Quell-/Zielüberprüfung für die Zielnetzwerkschnittstelle aus. Weitere Informationen finden Sie unter Konzepte der Netzwerkschnittstelle im EC2Amazon-Benutzerhandbuch.

- Konfigurieren Sie das Betriebssystem so, dass der Datenverkehr vom Ziel CIDR auf der Netzwerkschnittstelle akzeptiert wird.

Erstellen Sie einen CoIP-Pool

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

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

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

Console

Um einen CoIP-Pool mit der Konsole zu erstellen

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

AWS CLI

Um einen CoIP-Pool mit dem zu erstellen AWS CLI

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

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

Es folgt eine Beispielausgabe.

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

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

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

Es folgt eine Beispielausgabe.

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

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

Console

Um einer Instance mithilfe der Konsole eine CoIP-Adresse zuzuweisen

1. Öffnen Sie die VPC Amazon-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Elastic ausIPs.

3. Wählen Sie Elastic-IP-Adresse zuweisen aus.
4. Wählen Sie für Network Border Group den Standort, von dem aus die IP-Adresse beworben wird.
5. Wählen Sie unter Öffentlicher IPv4 Adresspool die Option Kundeneigener IPv4 Adresspool aus.
6. Wählen Sie für Kundeneigener IPv4 Adresspool den Pool aus, den Sie konfiguriert haben.
7. Wählen Sie Allocate aus.
8. Wählen Sie die Elastic-IP-Adresse aus, und wählen Sie Aktionen, Elastic-IP-Adresse zuordnen.
9. Wählen Sie die Instance aus Instance, und klicken Sie anschließend auf Zuordnen.

AWS CLI

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

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

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

Es folgt eine Beispielausgabe.

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

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

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

Es folgt eine Beispielausgabe.

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

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

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

Es folgt eine Beispielausgabe.

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

Lokale Netzwerkkonnektivität für Outposts-Racks

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

- Physische Konnektivität vom Outpost-Patchpanel zu den lokalen Netzwerkgeräten Ihrer Kunden.
- Link Aggregation Control Protocol (LACP), um zwei Link Aggregation Group (LAG) -Verbindungen zu Ihren Outpost-Netzwerkgeräten und zu Ihren lokalen Netzwerkgeräten herzustellen.
- Virtuelle LAN (VLAN) Konnektivität zwischen dem Outpost und den lokalen Netzwerkgeräten Ihrer Kunden.
- point-to-point Layer-3-Konnektivität für jedenVLAN.
- Border Gateway Protocol (BGP) für die Routenankündigung zwischen dem Outpost und Ihrem lokalen Service-Link.
- BGPfür die Routenankündigung zwischen dem Outpost und Ihrem lokalen Netzwerkgerät für die Konnektivität zum lokalen Gateway.

Inhalt

Tatsächliche Konnektivität

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

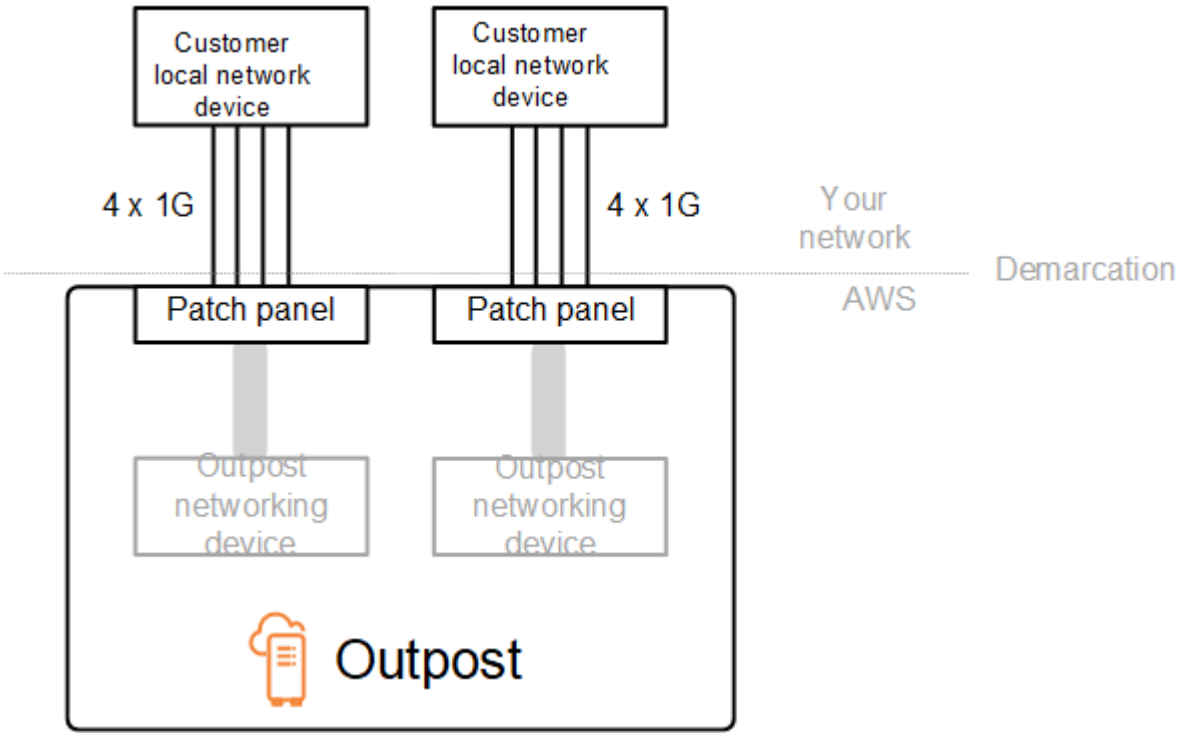
Ein Outpost benötigt mindestens zwei physische Verbindungen zwischen diesen Outpost-Netzwerkgeräten und Ihren lokalen Netzwerkgeräten. Ein Outpost unterstützt die folgenden Uplink-Geschwindigkeiten und -Mengen für jedes Outpost-Netzwerkgerät.

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

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

Outposts-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 Rack-Position bereitstellen.

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



Link-Aggregation

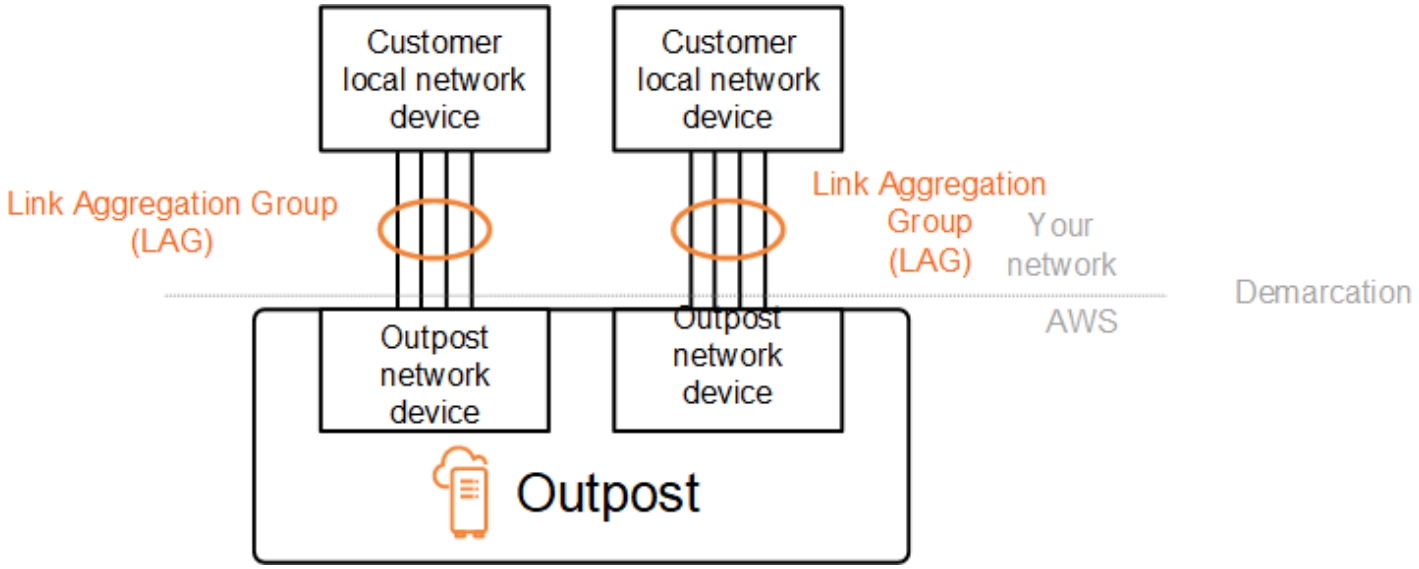
AWS Outposts verwendet das Link Aggregation Control Protocol (LACP), um zwei Link Aggregation Group (LAG) -Verbindungen herzustellen, eine von jedem Outpost-Netzwerkgerät zu jedem lokalen Netzwerkgerät. Die Links von jedem Outpost-Netzwerkgerät werden zu einem Ethernet LAG zusammengefasst, das eine einzelne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

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

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

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

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



Virtuell LANs

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

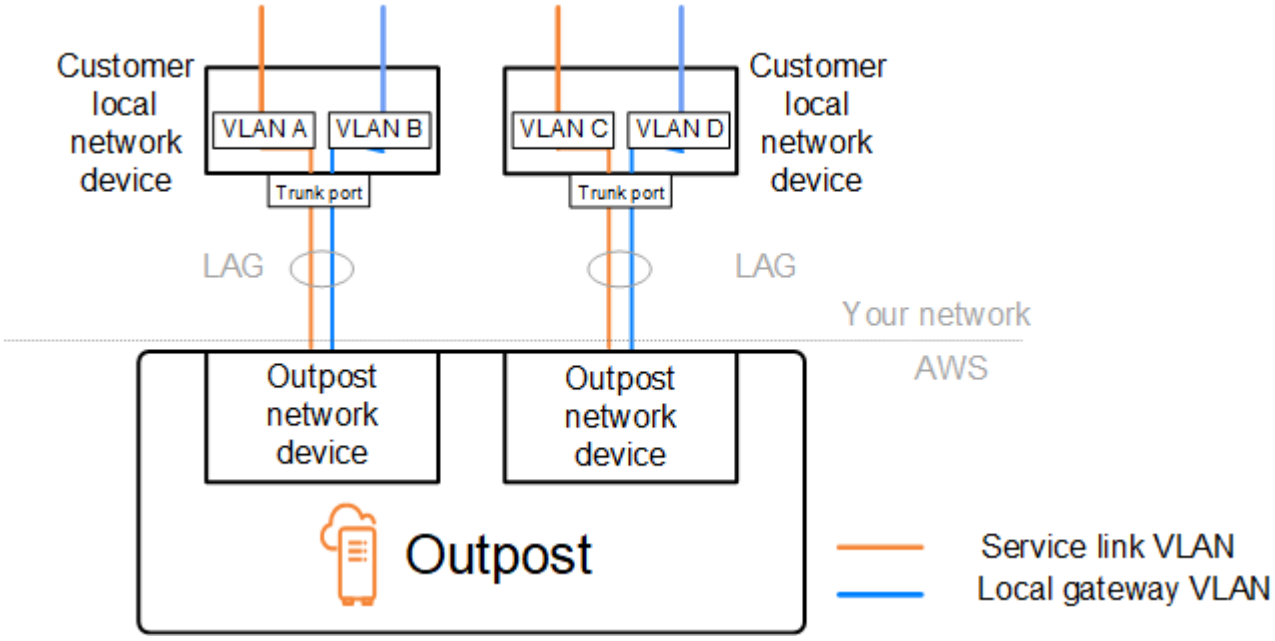
Jeder Outpost verfügt über FolgendesVLANs, um mit Ihren lokalen Netzwerkgeräten zu kommunizieren:

- Service Link VLAN — Ermöglicht die Kommunikation zwischen Ihrem Outpost und Ihren lokalen Netzwerkgeräten, um einen Service-Link-Pfad für die Service Link-Konnektivität einzurichten. Weitere Informationen finden Sie unter AWS Outposts -Konnektivität zu AWS -Regionen.
- Lokales Gateway VLAN — Ermöglicht die Kommunikation zwischen Ihrem Outpost und Ihren lokalen Netzwerkgeräten, um einen lokalen Gateway-Pfad einzurichten, um Ihre Outpost-Subnetze und Ihr lokales Netzwerk zu verbinden. Outpost Local Gateway nutzt diesVLAN, um Ihren Instanzen die Konnektivität zu Ihrem lokalen Netzwerk zu bieten, was auch den Internetzugang über Ihr Netzwerk beinhalten kann. Weitere Informationen finden Sie unter Lokales Gateway.

Sie können den 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. Es ermöglicht Ihnen auch,

den Service Link zu einem vom lokalen Gateway-Netzwerk isolierten Netzwerk zu machen, indem Sie mehrere Routing-Tabellen auf dem lokalen Netzwerkgerät Ihres Kunden verwenden, die allgemein als virtuelle Routing- und Forwarding-Instances (VRF) bezeichnet werden. Die Demarkationslinie befindet sich am Port der Outpost-Netzwerkgeräte. AWS verwaltet jede Infrastruktur auf der AWS Seite der Verbindung, und Sie verwalten jede Infrastruktur auf Ihrer Seite der Leitung.



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

Netzwerk-Layer-Konnektivität

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

Wir empfehlen Folgendes:

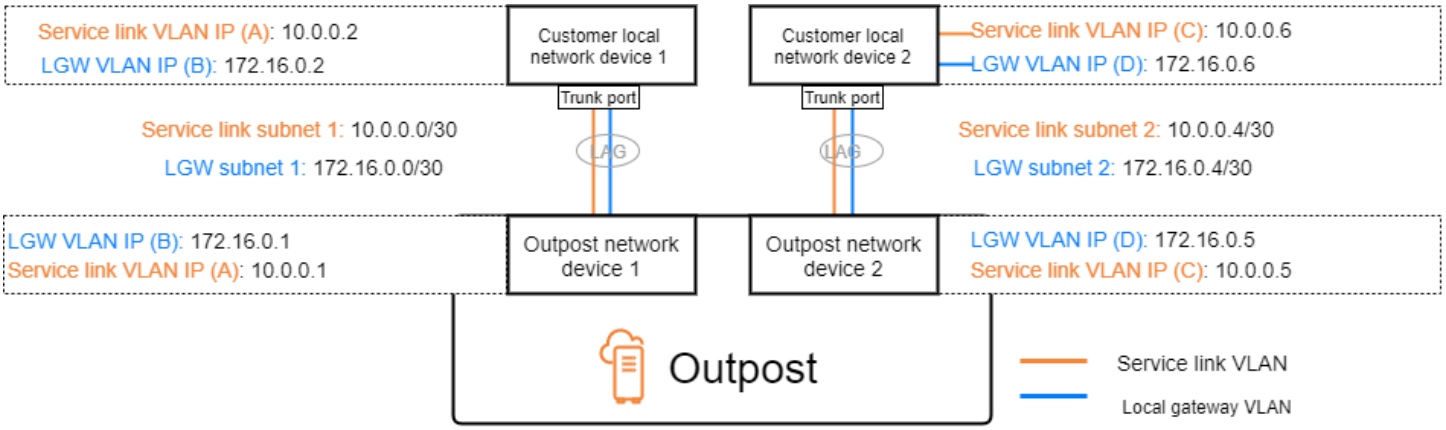
- Verwenden Sie ein dediziertes Subnetz mit einem /30 oder /31CIDR, um diese logische Konnektivität darzustellen. point-to-point
- Stellen Sie keine Brücke VLANs zwischen Ihren lokalen Netzwerkgeräten her.

Für die Konnektivität auf Netzwerkebene müssen Sie zwei Pfade einrichten:

- Service-Link-Pfad — Um diesen Pfad einzurichten, geben Sie ein VLAN Subnetz mit einem Bereich von /30 oder /31 und eine IP-Adresse für jeden Service-Link VLAN auf dem AWS Outposts Netzwerkgerät an. Virtuelle Service-Link-Schnittstellen (VIFs) werden für diesen Pfad verwendet, um IP-Konnektivität und BGP Sitzungen zwischen Ihrem Outpost und Ihren lokalen Netzwerkgeräten für 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 Netzwerkgerät an. AWS Outposts Lokale Gateways 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 VLANs Beispiel gibt es vier:

- VLANA steht für den Service-Link-Pfad, der das Outpost-Netzwerkgerät 1 mit dem lokalen Netzwerkgerät 1 des Kunden verbindet.
- VLANB steht für den lokalen Gateway-Pfad, der das Outpost-Netzwerkgerät 1 mit dem lokalen Netzwerkgerät 1 des Kunden verbindet.
- VLANC steht für den Service-Link-Pfad, der das Outpost-Netzwerkgerät 2 mit dem lokalen Netzwerkgerät 2 des Kunden verbindet.
- VLAND 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 OND1 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 OND2 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

ACERack-Konnektivität

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

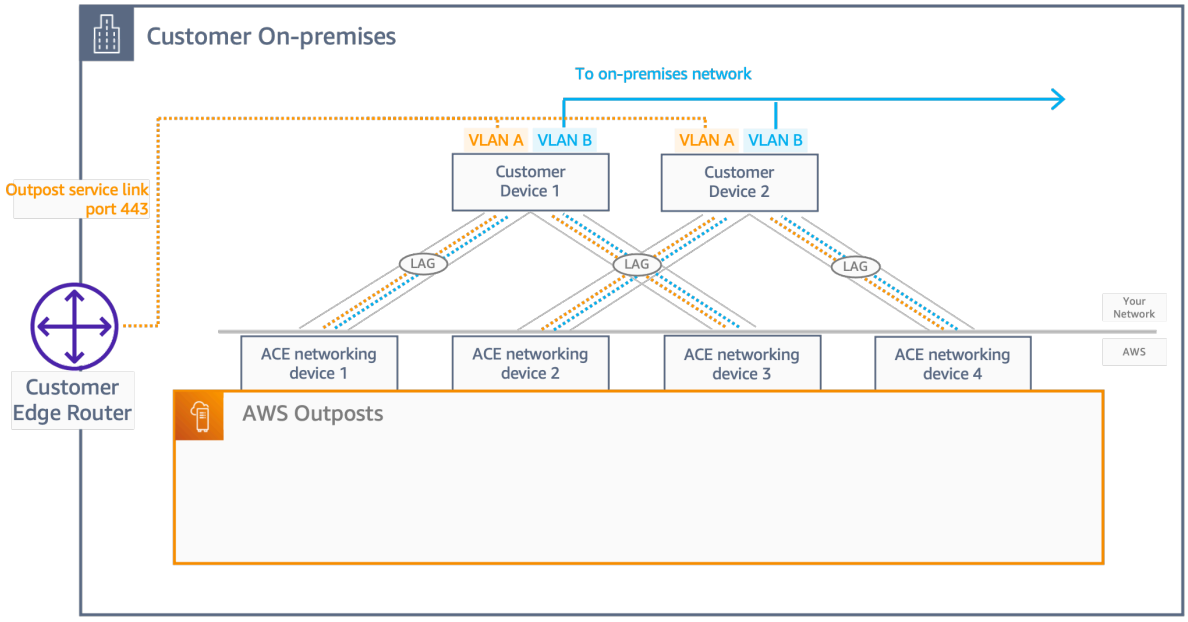
Ein Aggregations-, Core-, Edge- (ACE) -Rack dient als Netzwerkaggregationspunkt für Outpost-Bereitstellungen mit mehreren Racks. Sie müssen ein ACE Rack verwenden, wenn Sie fünf oder mehr Computer-Racks haben. Wenn Sie weniger als fünf Computer-Racks haben, aber in future eine Erweiterung auf fünf oder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

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

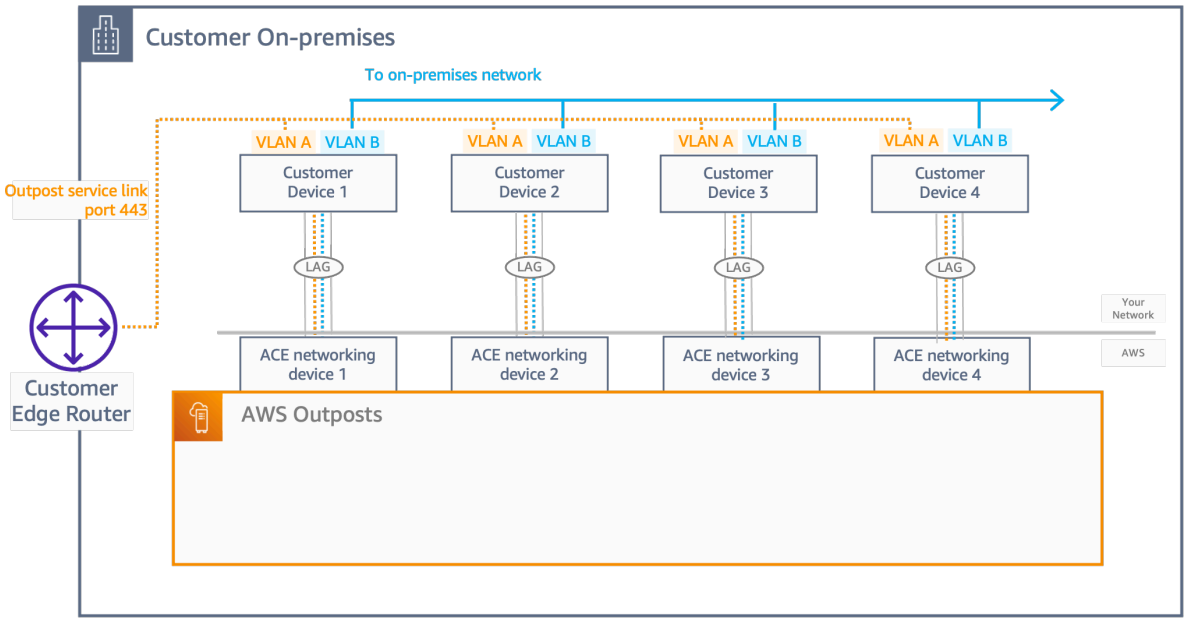
Ein ACE Rack umfasst vier Netzwerkgeräte, die für maximale Stabilität mit zwei vorgelagerten Kundengeräten in einem lokalen Kundennetzwerk oder mit vier vorgelagerten Kundengeräten verbunden werden können.

Die folgenden Bilder zeigen die beiden Netzwerktopologien.

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



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



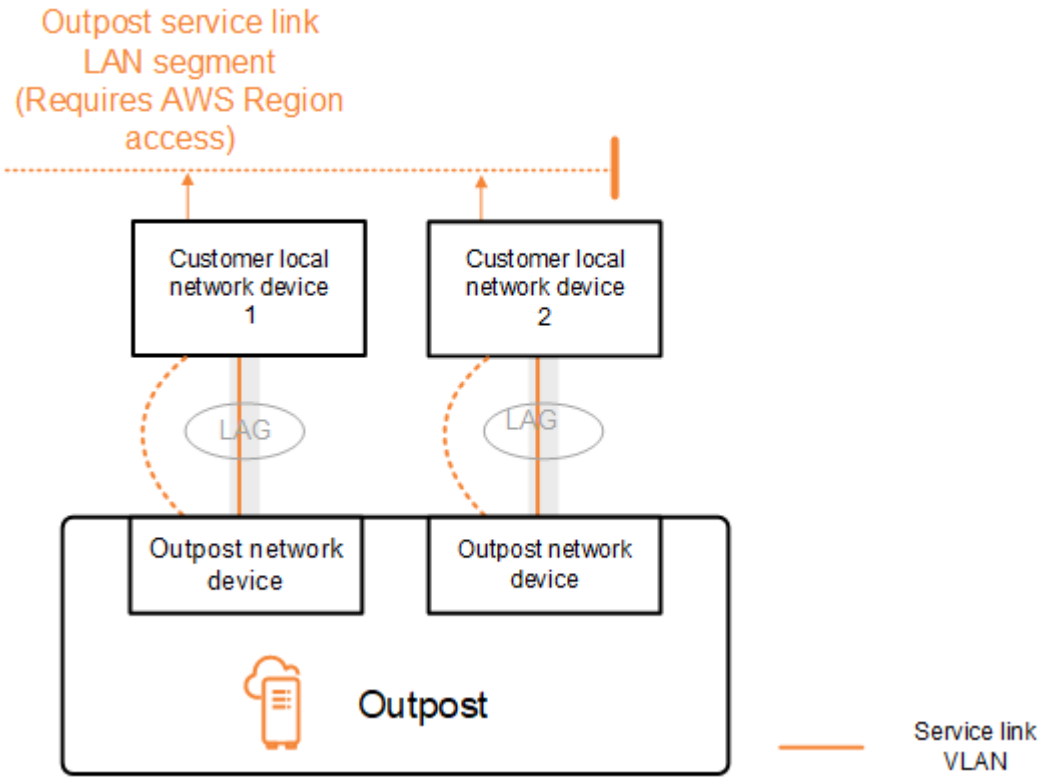
Service BGP Link-Konnektivität

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 den Service Link herzustellen. VLAN Die BGP Peering-Sitzung wird zwischen den IP-Adressen /30 oder /31 eingerichtet, die für die bereitgestellt wurden. point-to-point VLAN Jede BGP Peering-Sitzung verwendet eine private autonome Systemnummer (ASN) auf dem Outpost-Netzwerkgerät und eineASN, die Sie für die lokalen Netzwerkgeräte Ihrer Kunden auswählen. AWS stellt die Attribute im Rahmen des Installationsvorgangs bereit.

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

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

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



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

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

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

Das Kundennetzwerk sollte für alle gleiche BGP Präfixe mit denselben Attributen werben. ONDs Das Outpost-Netzwerk verteilt standardmäßig ausgehenden Datenverkehr zwischen allen Uplinks. Routing-Richtlinien werden auf der Outpost-Seite verwendet, um den Verkehr von einem Ort wegzuleiten, OND falls Wartungsarbeiten erforderlich sind. Diese Verkehrsverlagerung erfordert auf allen Seiten gleiche BGP Präfixe von Seiten des Kunden. 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

Sie geben während der Vorinstallation für das CIDR Subnetz der Service Link-Infrastruktur den 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 CIDR /27-Blöcke an, um Verbindungs- und Geräteausfälle zu unterstützen.

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

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

Lokale Gateway-Konnektivität BGP

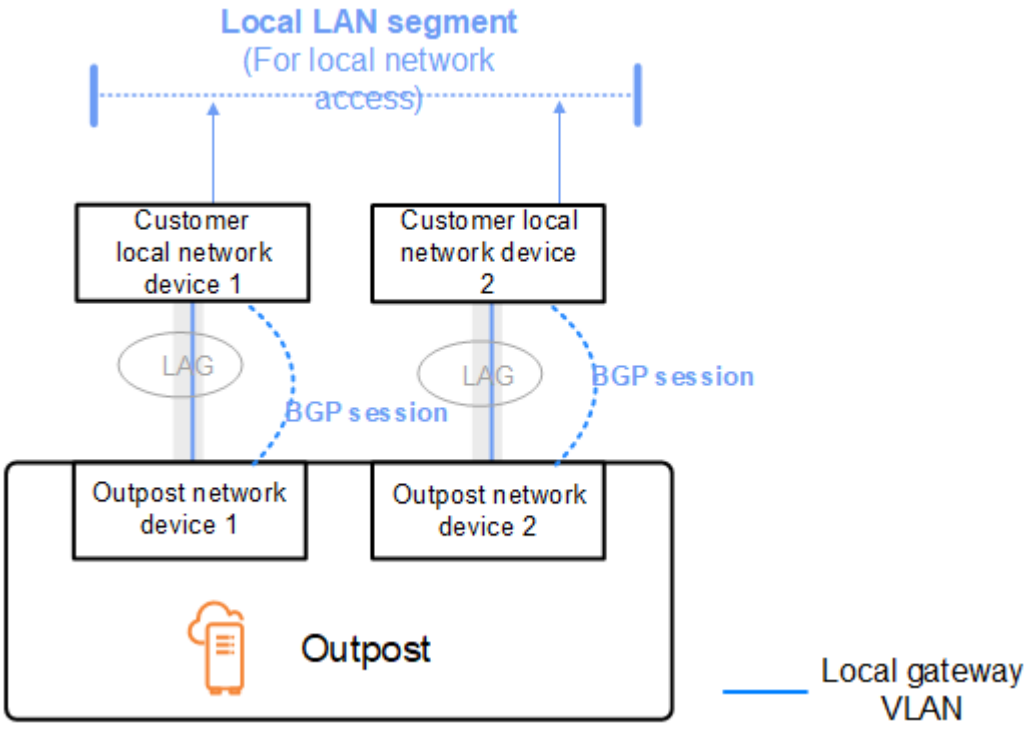
Der Outpost richtet ein externes BGP Peering von jedem Outpost-Netzwerkgerät zu einem lokalen Netzwerkgerät ein, um die Konnektivität zum lokalen Gateway herzustellen. Er verwendet eine private autonome Systemnummer (ASN), die Sie zuweisen, um die externen Sitzungen einzurichten. BGP Jedes Outpost-Netzwerkgerät verfügt über ein einziges externes BGP Peering zu einem lokalen Netzwerkgerät über sein lokales Gateway. VLAN

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

Jede BGP Sitzung verwendet die private Verbindung 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 als Teil des Vorinstallationsprozesses bereit.

Stellen Sie sich das Szenario vor, in dem Sie einen Outpost mit zwei Outpost-Netzwerkgeräten haben, die über eine Service-Verbindung 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 bereit BGPASN. 2 Byte (16 Bit) oder 4 Byte (32 Bit). Die gültigen Werte sind 64512–65535 oder 4200000000–4294967294.
- (Optional) Sie stellen dem Kunden das Eigentum zur VerfügungCIDR, das beworben wird (öffentlich oder privat, mindestens /26).
- Sie geben dem Kunden eine BGP Peer-IP-Adresse für das lokale Netzwerkgerät mit einem lokalen Gateway.
- Sie stellen dem Kunden das lokale Netzwerkgerät 1 lokalen BGP Gateway-Peer zur VerfügungASN. Die gültigen Werte lauten 1–4294967294. Weitere Informationen finden Sie unter RFC4893.
- Sie geben dem Kunden die BGP Peer-IP-Adresse des lokalen Netzwerkgeräts 2 für das lokale Gateway.
- Sie stellen dem Kunden den lokalen BGP Gateway-Peer für das lokale Netzwerkgerät 2 zur VerfügungASN. Die gültigen Werte lauten 1–4294967294. Weitere Informationen finden Sie unter RFC4893.



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

Das Kundennetzwerk sollte allen gleiche BGP Präfixe mit denselben Attributen bekannt geben. ONDs Das Outpost-Netzwerk verteilt standardmäßig ausgehenden Datenverkehr zwischen allen Uplinks. Routing-Richtlinien werden auf der Outpost-Seite verwendet, um den Verkehr von einem Ort wegzuleiten, OND falls Wartungsarbeiten erforderlich sind. Diese Verkehrsverlagerung erfordert auf allen Seiten gleiche BGP Präfixe von Seiten des Kunden. 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 Ihrem System, VPC um die Kommunikation mit Ihrem lokalen Netzwerk zu erleichtern. Sie können jedoch einen kundeneigenen IP-Adresspool (Customer-owned IP Address, CoIP) bereitstellen.

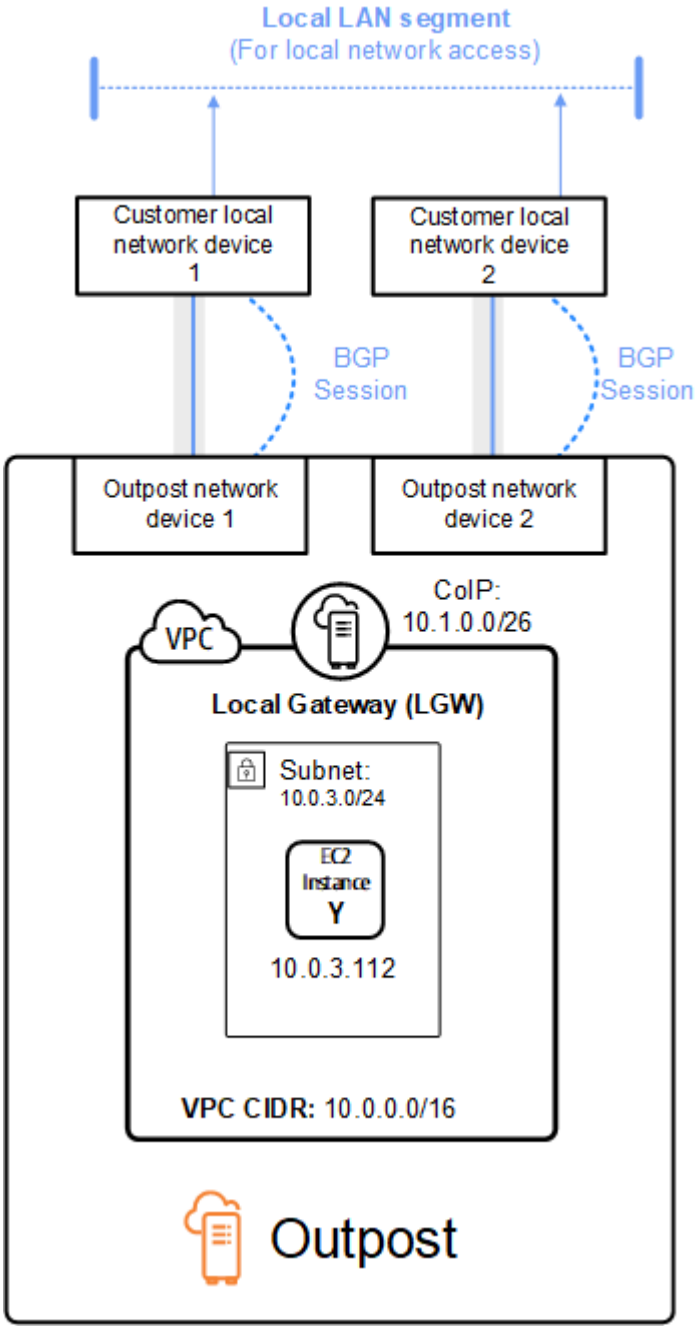
Wenn Sie sich für CoIP entscheiden, AWS wird der Pool anhand der Informationen erstellt, die Sie während des Installationsvorgangs angeben. Sie können Elastic IP-Adressen aus diesem Pool erstellen und die Adressen dann Ressourcen in Ihrem Outpost zuweisen, z. B. EC2 Instances.

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

> **Tip**
>
> Wenn Sie CoIP nicht verwenden, werden die privaten IP-Adressen aller Subnetze in Ihrem Outpost bekannt gegeben, für die in der Routentabelle eine Route BGP angegeben ist, die auf das lokale Gateway abzielt.

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

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


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

Teilen Sie Ihre AWS Outposts Ressourcen

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

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

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

Ein Outpost-Eigentümer kann Outpost-Ressourcen teilen mit:

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

Inhalt

- Freigeben in mehreren Availability Zones
- Eine Outpost-Ressource freigeben
- Aufheben der Freigabe einer Outpost-Ressource
- Identifizieren einer freigegebenen Outpost-Ressource
- Berechtigungen für freigegebene Outpost-Ressourcen
- Fakturierung und Messung
- Einschränkungen

Freigabefähige Outpost-Ressourcen

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

Dies sind die Ressourcen, die für verfügbar sind. Informationen zu Outposts-Serverressourcen finden Sie unter Arbeiten mit gemeinsam genutzten AWS Outposts Ressourcen im AWS Outposts Benutzerhandbuch für Outposts-Server.

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

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

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

Voraussetzungen für die Freigabe von Outposts-Ressourcen

- Um eine Outpost-Ressource mit Ihrer Organisation oder einer Organisationseinheit gemeinsam zu nutzen AWS 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. Sie können eine Outpost-Ressource, die mit Ihnen geteilt wurde, nicht teilen.
- Um eine Outpost-Ressource freizugeben, müssen Sie sie für ein Konto freigeben, das sich in Ihrer Organisation befindet.

Zugehörige Services

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

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

Freigeben in mehreren Availability Zones

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

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

Um die AZ IDs für die Availability Zones in Ihrem Konto anzuzeigen

1. Öffnen Sie die AWS RAM Konsole unter https://console.aws.amazon.com/ram.
2. Die AZ IDs für die aktuelle Region werden im Bereich „Ihre AZ-ID“ auf der rechten Seite des Bildschirms angezeigt.

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

Eine Outpost-Ressource freigeben

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

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

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

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

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

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

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

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

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

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-shareBefehl.

Aufheben der Freigabe einer 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 über die Konsole oder die anzeigen. AWS Outposts AWS CLI Bestehende Subnetze, Volumes oder Instances, die von Konsumenten erstellt wurden, werden nicht gelöscht. Alle vorhandenen Subnetz-Konsument, 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 Verknüpfungen mehr zu ihr erstellen. VPC Alle vorhandenen VPC Assoziationen, die von Verbrauchern erstellt wurden, bleiben mit der Routing-Tabelle verknüpft. Die darin enthaltenen Ressourcen VPCs können den Verkehr weiterhin an das lokale Gateway weiterleiten.

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

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

Siehe Aktualisieren einer Ressourcenfreigabe im AWS RAM -Benutzerhandbuch.

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

Verwenden Sie den Befehl disassociate-resource-share.

Identifizieren einer freigegebenen Outpost-Ressource

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

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

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

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

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

Berechtigungen für freigegebene Outpost-Ressourcen

Berechtigungen für Besitzer

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

Berechtigungen für Konsumenten

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

Fakturierung und Messung

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

Für die Freigabe von lokalen Gateway-Routing-Tabellen fallen keine zusätzlichen Gebühren an. Bei gemeinsam genutzten Subnetzen werden dem VPC Eigentümer Ressourcen VPC auf der Ebene A, wie z. B. VPN AND-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, wie Load Balancers und Amazon-Datenbanken. RDS Verbrauchern werden auch kostenpflichtige Datenübertragungen aus der Region in Rechnung gestellt. AWS

Einschränkungen

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

- Einschränkungen für gemeinsam genutzte Subnetze gelten für die Arbeit mit der Funktion „ AWS Outposts Teilen“. Weitere Informationen 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 AWS hat höchste Priorität. Als AWS Kunde profitieren Sie von einer Rechenzentrums- und Netzwerkarchitektur, die darauf ausgelegt sind, die Anforderungen der sicherheitssensibelsten Unternehmen zu erfüllen.

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

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

Weitere Informationen zu Sicherheit und Compliance finden AWS Outposts Sie unter AWS Outposts FAQ.

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

Inhalt

Datenschutz in AWS Outposts

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

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

Weitere Informationen zum Datenschutz finden Sie im Abschnitt Datenschutz FAQ. Informationen zum Datenschutz in Europa finden Sie im AWS Shared Responsibility Model und im GDPR Blogbeitrag auf dem AWS Security Blog.

Verschlüsselung im Ruhezustand

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

Sie können die EBS Amazon-Verschlüsselung für Ihre EBS Volumes und Snapshots verwenden. Die EBS Amazon-Verschlüsselung verwendet AWS Key Management Service (AWS KMS) und KMS Schlüssel. Weitere Informationen finden Sie unter Amazon EBS Encryption im EC2Amazon-Benutzerhandbuch.

Verschlüsselung während der Übertragung

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

Sie können ein Verschlüsselungsprotokoll wie Transport Layer Security (TLS) verwenden, um sensible Daten zu verschlüsseln, die über das lokale Gateway in Ihr lokales Netzwerk übertragen werden.

Löschen von Daten

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

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

Identitäts- und Zugriffsmanagement () für IAM AWS Outposts

AWS Identity and Access Management (IAM) ist ein AWS Dienst, der einem Administrator hilft, den Zugriff auf AWS Ressourcen sicher zu kontrollieren. IAMAdministratoren kontrollieren, wer authentifiziert (angemeldet) und autorisiert werden kann (über Berechtigungen verfügt), um AWS Outposts Ressourcen zu verwenden. Sie können es ohne IAM zusätzliche Kosten nutzen.

Inhalt

So funktioniert AWS Outposts mit IAM

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

IAMFunktionen, die du mit AWS Outposts verwenden kannst

IAMFunktion	AWS Unterstützung für Outposts
Identitätsbasierte Richtlinien	Ja
Ressourcenbasierte Richtlinien	Nein
Richtlinienaktionen	Ja
Richtlinienressourcen	Ja

IAMFunktion	AWS Unterstützung für Outposts
Richtlinienbedingungsschlüssel (services pezifisch)	Ja
ACLs	Nein
ABAC(Markierungen in Richtlinien)	Ja
Temporäre Anmeldeinformationen	Ja
Hauptberechtigungen	Ja
Servicerollen	Nein
Serviceverknüpfte Rollen	Ja

Identitätsbasierte Richtlinien für Outposts AWS

Unterstützt Richtlinien auf Identitätsbasis: Ja

Identitätsbasierte Richtlinien sind Dokumente mit JSON Berechtigungsrichtlinien, die Sie an eine Identität anhängen können, z. B. an einen Benutzer, eine IAM Benutzergruppe oder eine Rolle. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen einer identitätsbasierten Richtlinie finden Sie unter IAMRichtlinien erstellen im Benutzerhandbuch. IAM

Mit IAM identitätsbasierten Richtlinien können Sie zulässige oder verweigerte Aktionen und Ressourcen sowie die Bedingungen angeben, unter denen Aktionen zulässig oder verweigert werden. Sie können den Prinzipal nicht in einer identitätsbasierten Richtlinie angeben, da er für den Benutzer oder die Rolle gilt, dem er zugeordnet ist. Weitere Informationen zu allen Elementen, die Sie in einer JSON Richtlinie verwenden können, finden Sie in der Referenz zu den IAM JSON Richtlinienelementen im IAMBenutzerhandbuch.

Beispiele für identitätsbasierte Richtlinien für Outposts AWS

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

Ressourcenbasierte Richtlinien innerhalb von Outposts AWS

Unterstützt ressourcenbasierte Richtlinien: Nein

Ressourcenbasierte Richtlinien sind JSON Richtliniendokumente, die Sie an eine Ressource anhängen. Beispiele für ressourcenbasierte Richtlinien sind IAM Rollenvertrauensrichtlinien und Amazon S3 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. Zu den Prinzipalen können Konten, Benutzer, Rollen, Verbundbenutzer oder gehören. AWS-Services

Um den kontoübergreifenden Zugriff zu ermöglichen, können Sie in einer ressourcenbasierten Richtlinie ein ganzes Konto oder IAM Entitäten in einem anderen Konto als Prinzipal angeben. Durch das Hinzufügen eines kontoübergreifenden Auftraggebers zu einer ressourcenbasierten Richtlinie ist nur die halbe Vertrauensbeziehung eingerichtet. Wenn sich der Prinzipal und die Ressource unterscheiden AWS-Konten, muss ein IAM Administrator des vertrauenswürdigen Kontos auch der Prinzipalentität (Benutzer oder Rolle) die Berechtigung zum Zugriff auf die Ressource gewähren. 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 IAMim IAMBenutzerhandbuch unter Kontenübergreifender Ressourcenzugriff.

Politische Maßnahmen für AWS Outposts

Unterstützt Richtlinienaktionen: Ja

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

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

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

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

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

```
outposts
```

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

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

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

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

Politische Ressourcen für AWS Outposts

Unterstützt Richtlinienressourcen: Ja

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

Das `Resource` JSON Richtlinienelement gibt das Objekt oder die Objekte an, für die die Aktion gilt. Anweisungen müssen entweder ein – `Resource`oder ein `NotResource`-Element enthalten. Es hat sich bewährt, eine Ressource mit ihrem Amazon-Ressourcennamen (ARN) anzugeben. 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 API Outposts-Aktionen unterstützen mehrere Ressourcen. Um mehrere Ressourcen in einer einzigen Anweisung anzugeben, trennen Sie sie ARNs durch Kommas.

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

Eine Liste der AWS Outposts-Ressourcentypen und ihrer ARNs Eigenschaften finden Sie unter Ressourcentypen definiert von AWS Outposts in der Service Authorization Reference. Informationen darüber, mit welchen Aktionen Sie die ARN einzelnen Ressourcen spezifizieren können, finden Sie unter Aktionen definiert von AWS Outposts.

Schlüssel zu den Policy-Bedingungen für AWS Outposts

Unterstützt servicespezifische Richtlinienbedingungsschlüssel: Ja

Administratoren können mithilfe von AWS JSON Richtlinien festlegen, 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. Sie können einem IAM Benutzer beispielsweise nur dann Zugriff auf eine Ressource gewähren, wenn sie mit seinem IAM Benutzernamen gekennzeichnet ist. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter IAMRichtlinienelemente: Variablen und Tags.

AWS unterstützt globale Bedingungsschlüssel und dienstspezifische Bedingungsschlüssel. Eine Übersicht aller AWS globalen Bedingungsschlüssel finden Sie unter Kontext-Schlüssel für AWS globale Bedingungen im IAMBenutzerhandbuch.

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

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

ACLsin AWS Outposts

UnterstütztACLs: Nein

Zugriffskontrolllisten (ACLs) steuern, welche Principals (Kontomitglieder, Benutzer oder Rollen) über Zugriffsberechtigungen für eine Ressource verfügen. ACLsähneln ressourcenbasierten Richtlinien, verwenden jedoch nicht das JSON Richtliniendokumentformat.

ABACmit AWS Outposts

Unterstützt ABAC (Tags in Richtlinien): Ja

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

ABACist hilfreich in Umgebungen, die schnell wachsen, und hilft in Situationen, in denen die Richtlinienverwaltung umständlich 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 finden Sie ABAC unter Was ist? ABAC im IAMBenutzerhandbuch. Ein Tutorial mit Schritten zur Einrichtung finden Sie im ABAC Benutzerhandbuch unter Verwenden der attributebasierten Zugriffskontrolle (ABAC). IAM

Temporäre Anmeldeinformationen mit AWS Outposts verwenden

Unterstützt temporäre Anmeldeinformationen: Ja

Manche funktionieren AWS-Services nicht, wenn Sie sich mit temporären Zugangsdaten anmelden. Weitere Informationen, einschließlich Informationen darüber, AWS-Services wie Sie mit temporären Anmeldeinformationen arbeiten können AWS-Services , finden Sie IAM im IAMBenutzerhandbuch unter Informationen zum Arbeiten mit.

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

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

Serviceübergreifende Prinzipalberechtigungen für Outposts AWS

Unterstützt Forward-Access-Sitzungen (FAS): Ja

Wenn Sie einen IAM Benutzer oder eine Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. FASverwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, kombiniert mit der Anforderung, Anfragen AWS-Service an nachgelagerte Dienste zu stellen. FASAnfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, für deren Abschluss Interaktionen mit anderen AWS-Services oder Ressourcen erforderlich sind. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien beim Stellen von FAS Anfragen finden Sie unter Zugriffssitzungen weiterleiten.

Servicerollen für AWS -Outposts

Unterstützt Servicerollen: Nein

Eine Servicerolle ist eine IAMRolle, die ein Dienst übernimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM Administrator kann eine Servicerolle von innen heraus erstellen, ändern und löschenIAM. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter Erstellen einer Rolle zum Delegieren von Berechtigungen AWS-Service an eine.

Servicebezogene Rollen für Outposts AWS

Unterstützt dienstbezogene Rollen: Ja

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

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

AWS Politische Beispiele für Outposts

Standardmäßig sind Benutzer und Rollen nicht berechtigt, AWS Outposts-Ressourcen zu erstellen oder zu ändern. Sie können auch keine Aufgaben mithilfe von AWS Management Console, AWS Command Line Interface (AWS CLI) oder AWS API ausführen. Um Benutzern die Berechtigung zu erteilen, Aktionen mit den Ressourcen durchzuführen, die sie benötigen, kann ein IAM Administrator IAM Richtlinien erstellen. Der Administrator kann dann die IAM Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen übernehmen.

Informationen zum Erstellen einer IAM identitätsbasierten Richtlinie anhand dieser JSON Beispieldokumente finden Sie unter IAMRichtlinien erstellen im IAMBenutzerhandbuch.

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

Inhalt

- Bewährte Methoden für Richtlinien
- Beispiel: Nutzen von Berechtigungen auf Ressourcenebene

Bewährte Methoden für Richtlinien

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

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten — Verwenden Sie die AWS verwalteten Richtlinien, die Berechtigungen für viele gängige Anwendungsfälle gewähren, um Ihren Benutzern und Workloads zunächst Berechtigungen zu gewähren. Sie sind in Ihrem verfügbar. AWS-Konto Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom AWS Kunden verwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind. Weitere Informationen finden Sie AWS im IAMBenutzerhandbuch unter AWS Verwaltete Richtlinien oder Verwaltete Richtlinien für Jobfunktionen.
- Berechtigungen mit den geringsten Rechten anwenden — Wenn Sie Berechtigungen mit IAM Richtlinien festlegen, gewähren Sie nur die Berechtigungen, die für die Ausführung 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 IAM zum Anwenden von Berechtigungen finden Sie IAMim Benutzerhandbuch unter Richtlinien und Berechtigungen. IAM
- Verwenden Sie Bedingungen in IAM Richtlinien, um den Zugriff weiter einzuschränken — Sie können Ihren Richtlinien eine Bedingung hinzufügen, um den Zugriff auf Aktionen und Ressourcen einzuschränken. Sie können beispielsweise eine Richtlinienbedingung schreiben, um anzugeben, dass alle Anfragen mit gesendet werden müssenSSL. Sie können auch Bedingungen verwenden, um Zugriff auf Serviceaktionen zu gewähren, wenn diese über einen bestimmten Zweck verwendet werden AWS-Service, z. AWS CloudFormation B. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter IAMJSONRichtlinienelemente: Bedingung.
- Verwenden Sie IAM Access Analyzer, um Ihre IAM Richtlinien zu validieren, um sichere und funktionale Berechtigungen zu gewährleisten. IAM Access Analyzer validiert neue und bestehende Richtlinien, sodass die Richtlinien der IAM Richtliniensprache (JSON) und den IAM bewährten Methoden entsprechen. IAMAccess Analyzer bietet mehr als 100 Richtlinienprüfungen und umsetzbare Empfehlungen, um Sie bei der Erstellung sicherer und funktionaler Richtlinien zu

unterstützen. Weitere Informationen finden Sie unter IAMAccess Analyzer-Richtlinienvalidierung im IAMBenutzerhandbuch.

- Multi-Faktor-Authentifizierung erforderlich (MFA) — Wenn Sie ein Szenario haben, in dem IAM Benutzer oder ein Root-Benutzer erforderlich sind AWS-Konto, aktivieren Sie die Option MFA für zusätzliche Sicherheit. Wenn Sie festlegen möchten, MFA wann API Operationen aufgerufen werden, fügen Sie MFA Bedingungen zu Ihren Richtlinien hinzu. Weitere Informationen finden Sie unter Konfiguration des MFA -geschützten API Zugriffs im IAMBenutzerhandbuch.

Weitere Informationen zu bewährten Methoden finden Sie unter Bewährte Sicherheitsmethoden IAM im IAM Benutzerhandbuch. IAM

Beispiel: Nutzen von Berechtigungen auf Ressourcenebene

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

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

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

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

Mit Diensten verknüpfte Rollen für AWS Outposts

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

Eine dienstbezogene Rolle macht Ihre Einrichtung AWS Outposts effizienter, da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. AWS Outposts definiert die Berechtigungen ihrer dienstbezogenen Rollen und AWS Outposts kann, sofern nicht anders definiert, nur ihre Rollen übernehmen. Zu den definierten Berechtigungen gehören die Vertrauensrichtlinie und die Berechtigungsrichtlinie, und diese Berechtigungsrichtlinie kann keiner anderen IAM Entität zugeordnet werden.

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

Mit dem Dienst verknüpfte Rollenberechtigungen für AWS Outposts

AWS Outposts verwendet die mit dem Dienst verknüpfte Rolle mit dem Namen _ 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.

Das AWSServiceRoleForOutposts _*`OutpostID`* Die dienstbezogene Rolle vertraut darauf, dass die folgenden Dienste die Rolle übernehmen:

- `outposts.amazonaws.com`

Das _ AWSServiceRoleForOutposts***OutpostID***Die dienstbezogene Rolle umfasst die folgenden Richtlinien:

- AWSOutpostsServiceRolePolicy
- AWSOutpostsPrivateConnectivityPolicy_***OutpostID***

Bei der AWSOutpostsServiceRolePolicyRichtlinie handelt es sich um eine dienstbezogene Rollenrichtlinie, die den Zugriff auf AWS Ressourcen ermöglicht, die von verwaltet werden. 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`

Das AWSOutpostsPrivateConnectivityPolicy _***OutpostID***Die Richtlinie AWS Outposts ermöglicht es, 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 IAM Entität (z. B. ein Benutzer, eine Gruppe oder eine Rolle) eine dienstbezogene Rolle erstellen, bearbeiten oder löschen kann. Weitere Informationen finden Sie unter Berechtigungen für dienstbezogene Rollen im IAMBenutzerhandbuch.

Erstellen Sie eine dienstverknüpfte Rolle für AWS Outposts

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

Weitere Informationen finden Sie unter Private Service Link-Konnektivität mit VPC.

Bearbeiten Sie eine serviceverknüpfte Rolle für AWS Outposts

AWS Outposts erlaubt Ihnen nicht, das _ zu bearbeiten AWSServiceRoleForOutposts*OutpostID* Rolle, die mit einem Dienst verknüpft ist. Nachdem Sie eine serviceverknüpfte Rolle erstellt haben, können Sie den Namen der Rolle nicht mehr ändern, da verschiedene Entitäten auf die Rolle verweisen könnten. Sie können die Beschreibung der Rolle jedoch mit IAM bearbeiten. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter Aktualisieren einer dienstbezogenen Rolle.

Löschen Sie eine dienstverknüpfte Rolle für AWS Outposts

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

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

Du musst deinen Outpost löschen, bevor du _ löschen kannst AWSServiceRoleForOutposts*OutpostID* Rolle, die mit einem Dienst verknüpft ist.

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

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

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

Um die mit dem Service verknüpfte Rolle manuell zu löschen, verwenden Sie IAM

Weitere Informationen finden Sie im IAMBenutzerhandbuch unter Löschen einer dienstverknüpften Rolle.

Unterstützte Regionen für AWS Outposts dienstverknüpfte Rollen

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

AWS verwaltete Richtlinien für AWS Outposts

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

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

Sie können die in AWS verwalteten Richtlinien definierten Berechtigungen nicht ändern. Wenn die in einer AWS verwalteten Richtlinie definierten Berechtigungen AWS aktualisiert werden, wirkt sich das Update auf alle Prinzidentitäten (Benutzer, Gruppen und Rollen) aus, denen die Richtlinie zugeordnet ist. AWS aktualisiert eine AWS verwaltete Richtlinie höchstwahrscheinlich, wenn eine neue Richtlinie eingeführt AWS-Service wird oder neue API Operationen für bestehende Dienste verfügbar werden.

Weitere Informationen finden Sie im IAMBenutzerhandbuch unter AWS Verwaltete Richtlinien.

AWS verwaltete Richtlinie: AWSOutpostsServiceRolePolicy

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

AWS verwaltete Richtlinie: AWSOutpostsPrivateConnectivityPolicy

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

AWS Outposts Aktualisierungen AWS verwalteter Richtlinien

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

Änderung	Beschreibung	Datum
AWS Outposts haben begonnen, Änderungen zu verfolgen	AWS Outposts begann, Änderungen an seinen AWS verwalteten Richtlinien nachzuverfolgen.	03. Dezember 2019

Sicherheit der Infrastruktur in AWS Outposts

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

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

- Sicherheit auf Transportschicht (TLS). Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Cipher-Suites mit Perfect Forward Secrecy (PFS) wie (Ephemeral Diffie-Hellman) oder DHE (Elliptic Curve Ephemeral Diffie-Hellman). ECDHE Die meisten modernen Systeme wie Java 7 und höher unterstützen diese Modi.

Darüber hinaus müssen Anfragen mithilfe einer Zugriffsschlüssel-ID und eines geheimen Zugriffsschlüssels, der einem Prinzipal zugeordnet ist, signiert werden. IAM 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.

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

Überwachung von Manipulationen an Geräten AWS Outposts

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

Belastbarkeit in AWS Outposts

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

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

Wenn Sie einen Outpost erstellen, wählen Sie eine Availability Zone aus einer AWS Region aus. Diese Availability Zone unterstützt Operationen auf Kontrollebene wie das Beantworten von API Anrufen, das Überwachen des Außenpostens und das Aktualisieren des Außenpostens. 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.

Überprüfung der Einhaltung der Vorschriften für AWS Outposts

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

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

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

- Schnellstartanleitungen zu Sicherheit und Compliance — In diesen Bereitstellungsleitfäden werden architektonische Überlegungen erörtert und Schritte für die Implementierung von Basisumgebungen beschrieben AWS , bei denen Sicherheit und Compliance im Mittelpunkt stehen.
- Architecting for HIPAA Security and Compliance on Amazon Web Services — In diesem Whitepaper wird beschrieben, wie Unternehmen Anwendungen erstellen HIPAA können, die AWS für sie in Frage kommen.

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

- AWS Ressourcen zur AWS von Vorschriften — Diese Sammlung von Arbeitsmappen und Leitfäden kann auf Ihre Branche und Ihren Standort zutreffen.
- AWS Leitfäden zur Einhaltung von Vorschriften für Kunden — Verstehen Sie das Modell der gemeinsamen Verantwortung aus dem Blickwinkel der Einhaltung von Vorschriften. In den Leitfäden werden die bewährten Verfahren zur Sicherung zusammengefasst AWS-Services und die Leitlinien für Sicherheitskontrollen in verschiedenen Frameworks (einschließlich des National Institute of Standards and Technology (NIST), des Payment Card Industry Security Standards Council (PCI) und der International Organization for Standardization (ISO)) zusammengefasst.
- Evaluierung von Ressourcen anhand von Regeln im AWS Config Entwicklerhandbuch — Der AWS Config Service bewertet, wie gut Ihre Ressourcenkonfigurationen den internen Praktiken, Branchenrichtlinien und Vorschriften entsprechen.
- AWS Security Hub— Auf diese AWS-Service Weise erhalten Sie einen umfassenden Überblick über Ihren internen Sicherheitsstatus. AWS Security Hub verwendet Sicherheitskontrollen, um Ihre AWS -Ressourcen zu bewerten und Ihre Einhaltung von Sicherheitsstandards und bewährten Methoden zu überprüfen. Eine Liste der unterstützten Services und Kontrollen finden Sie in der Security-Hub-Steuerungsreferenz.
- Amazon GuardDuty — Dies AWS-Service erkennt potenzielle Bedrohungen für Ihre Workloads AWS-Konten, Container und Daten, indem es Ihre Umgebung auf verdächtige und böswillige Aktivitäten überwacht. GuardDuty kann Ihnen helfen, verschiedene Compliance-Anforderungen zu erfüllen PCIDSS, z. B. durch die Erfüllung der Anforderungen zur Erkennung von Eindringlingen, die in bestimmten Compliance-Frameworks vorgeschrieben sind.
- AWS Audit Manager— Auf diese AWS-Service Weise können Sie Ihre AWS Nutzung kontinuierlich überprüfen, um das Risikomanagement und die Einhaltung von Vorschriften und Industriestandards zu vereinfachen.

Internetzugang für AWS Outposts Workloads

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

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

Internetzugang über die übergeordnete AWS Region

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

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

Überlegungen

- Verwenden Sie diese Option, wenn:
  - Sie benötigen Flexibilität bei der Sicherung des Internetverkehrs mit mehreren AWS Diensten in der AWS Region.
  - Sie verfügen in Ihrem Rechenzentrum oder Ihrer Colocation-Einrichtung nicht über einen Internet-Präsenzpunkt.
- Bei dieser Option muss der Datenverkehr die übergeordnete AWS Region durchqueren, was zu Latenz führt.
- Ähnlich wie bei Datenübertragungsgebühren in AWS Regionen fallen für die Datenübertragung von der übergeordneten Availability Zone zum Outpost Gebühren an. Weitere Informationen zur Datenübertragung finden Sie unter Amazon EC2 On-Demand-Preise.
- Die Auslastung der Service Link-Bandbreite wird zunehmen.

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

Internetzugang über das Netzwerk Ihres lokalen Rechenzentrums

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

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

Überlegungen

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

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

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

CloudWatch Metriken

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

CloudTrail Logs

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

Die CloudTrail Protokolle enthalten Informationen über die Aufrufe zu API Aktionen für AWS Outposts. Sie enthalten auch Informationen für API Aktionsaufforderungen von Diensten in einem Outpost wie Amazon EC2 und AmazonEBS. Weitere Informationen finden Sie unter APIAnrufe protokollieren mit CloudTrail.

VPC-Flow-Protokolle

Verwenden Sie VPC Flow Logs, um detaillierte Informationen über den Verkehr zu und von Ihrem Außenposten und innerhalb Ihres Außenpostens zu erfassen. Weitere Informationen finden Sie unter VPCFlow Logs im VPCAmazon-Benutzerhandbuch.

Datenverkehrsspiegelung

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

AWS Health Dashboard

AWS Health Dashboard Zeigt Informationen und Benachrichtigungen an, die durch Änderungen im Zustand der AWS Ressourcen ausgelöst werden. Diese Informationen werden auf zweierlei

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

CloudWatch

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

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

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

Inhalt

- CloudWatch

Metriken

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

`ConnectedStatus`

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

Einheit: Anzahl

Maximale Auflösung: 1 Minute

Statistiken: Die nützlichste Statistik ist `Average`.

Dimensionen: `OutpostId`

`CapacityExceptions`

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

Einheit: Anzahl

Maximale Auflösung: 5 Minuten

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

Dimensionen: `InstanceType` und `OutpostId`

`IfTrafficIn`

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

Einheit: Bits pro Sekunde

Maximale Auflösung: 5 Minuten

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

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

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

`IfTrafficOut`

Die Bitrate der Daten, die die Outposts Virtual Interfaces (VIFs) an die verbundenen lokalen Netzwerkgeräte übertragen.

Einheit: Bits pro Sekunde

Maximale Auflösung: 5 Minuten

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

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

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

`InstanceFamilyCapacityAvailability`

Der Prozentsatz der verfügbaren Instance-Kapazität. Diese Metrik beinhaltet keine Kapazität für Dedicated Hosts, die auf dem Outpost konfiguriert sind.

Einheit: Prozent

Maximale Auflösung: 5 Minuten

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

Dimensionen: `InstanceFamily` und `OutpostId`

`InstanceFamilyCapacityUtilization`

Der Prozentsatz der verfügbaren Instance-Kapazität. Diese Metrik beinhaltet keine Kapazität für Dedicated Hosts, die auf dem Outpost konfiguriert sind.

Einheit: Prozent

Maximale Auflösung: 5 Minuten

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

Dimensionen: `Account`, `InstanceFamily` und `OutpostId`

`InstanceTypeCapacityAvailability`

Der Prozentsatz der verfügbaren Instance-Kapazität. Diese Metrik beinhaltet keine Kapazität für Dedicated Hosts, die auf dem Outpost konfiguriert sind.

Einheit: Prozent

Maximale Auflösung: 5 Minuten

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

Dimensionen: `InstanceType` und `OutpostId`

`InstanceTypeCapacityUtilization`

Der Prozentsatz der verfügbaren Instance-Kapazität. Diese Metrik beinhaltet keine Kapazität für Dedicated Hosts, die auf dem Outpost konfiguriert sind.

Einheit: Prozent

Maximale Auflösung: 5 Minuten

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

Dimensionen: `Account`, `InstanceType` und `OutpostId`

`UsedInstanceType_Count`

Die Anzahl der Instance-Typen, die derzeit verwendet werden, einschließlich aller Instance-Typen, die von Managed Services wie Amazon Relational Database Service (AmazonRDS) 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 für den Start in die Rechenkapazität verfügbar sind, die mithilfe von Capacity Reservations reserviert wurde. Diese Metrik beinhaltet keine Amazon EC2 Reserved Instances.

Einheit: Anzahl

Maximale Auflösung: 5 Minuten

Dimensionen: `InstanceType` und `OutpostId`

`UsedReservedInstances`

Die Anzahl der Instances, die in der Rechenkapazität ausgeführt werden, die mithilfe von Capacity Reservations reserviert wurde. Diese Metrik beinhaltet keine Amazon EC2 Reserved Instances.

Einheit: Anzahl

Maximale Auflösung: 5 Minuten

Dimensionen: `InstanceType` und `OutpostId`

`TotalReservedInstances`

Die Gesamtzahl der Instances, die ausgeführt werden und für den Start verfügbar sind, ergibt sich aus der Rechenkapazität, die über Capacity Reservations reserviert wurde. Diese Metrik beinhaltet keine Amazon EC2 Reserved Instances.

Einheit: Anzahl

Maximale Auflösung: 5 Minuten

Dimensionen: `InstanceType` und `OutpostId`

`EBSVolumeTypeCapacityUtilization`

Der Prozentsatz der EBS genutzten Kapazität vom Typ Volume.

Einheit: Prozent

Maximale Auflösung: 5 Minuten

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

Dimensionen: `VolumeType` und `OutpostId`

`EBSVolumeTypeCapacityAvailability`

Der Prozentsatz der verfügbaren 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 an verfügbarer Kapazität für den Volumetyp. EBS

Einheit: Gigabyte

Maximale Auflösung: 5 Minuten

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

Dimensionen: `VolumeType` und `OutpostId`

Metrische Abmessungen

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 Volumentyp.
`VirtualInterfaceId`	Die ID der virtuellen Schnittstelle (VIF) des lokalen Gateways oder Service Links.
`VirtualInterfaceGroupId`	Die ID der virtuellen Schnittstellengruppe für das virtuelle Interface (VIF) des lokalen Gateways.

CloudWatch

Sie können die CloudWatch Metriken für Ihren mit der CloudWatch Konsole anzeigen.

Um Metriken mit der CloudWatch Konsole anzuzeigen

1. Öffnen Sie die CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Wählen Sie im Navigationsbereich Metriken aus.
3. Wählen Sie den Namespace des Outposts aus.
4. (Optional) Um eine Metrik in allen Dimensionen anzuzeigen, geben Sie den Namen in das Suchfeld ein.

Um Metriken mit dem anzuzeigen AWS CLI

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

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

Um die Statistiken für eine Metrik abzurufen, verwenden Sie AWS CLI

Verwenden Sie den folgenden get-metric-statisticsBefehl, um Statistiken für die angegebene Metrik und Dimension abzurufen. CloudWatch behandelt jede eindeutige Kombination von Dimensionen als separate Metrik. Sie können keine Statistiken abrufen, die Kombinationen von Dimensionen verwenden, die nicht speziell veröffentlicht wurden. Sie müssen die gleichen Dimensionen angeben, die bei der Erstellung der Metriken verwendet wurden.

```
aws cloudwatch get-metric-statistics \
--namespace AWS/Outposts --metric-name InstanceTypeCapacityUtilization \
--statistics Average --period 3600 \
--dimensions Name=OutpostId,Value=op-01234567890abcdef
 Name=InstanceType,Value=c5.xlarge \
--start-time 2019-12-01T00:00:00Z --end-time 2019-12-08T00:00:00Z
```

AWS Outposts APIAnrufe protokollieren mit AWS CloudTrail

AWS Outposts ist in einen Dienst integriert AWS CloudTrail, der eine Aufzeichnung der von einem Benutzer, einer Rolle oder einem AWS Dienst ausgeführten Aktionen bereitstellt. CloudTrail erfasst API Aufrufe AWS Outposts als Ereignisse. Zu den erfassten Aufrufen gehören Aufrufe von der AWS Outposts Konsole und Code-Aufrufe der AWS Outposts API Operationen. Anhand der von gesammelten Informationen können Sie die Anfrage CloudTrail, an die die Anfrage gestellt wurde AWS Outposts, die IP-Adresse, von der aus die Anfrage gestellt wurde, den Zeitpunkt der Anfrage und weitere Details ermitteln.

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Die Identitätsinformationen unterstützen Sie bei der Ermittlung der folgenden Punkte:

- Ob die Anfrage mit Anmeldeinformationen des Root-Benutzers oder des Benutzers gestellt wurde.
- Ob die Anfrage im Namen eines IAM Identity Center-Benutzers gestellt wurde.
- Gibt an, ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen Verbundbenutzer gesendet wurde.
- Ob die Anforderung aus einem anderen AWS-Service gesendet wurde.

CloudTrail ist in Ihrem AWS Konto aktiv, wenn Sie das Konto erstellen, und Sie haben automatisch Zugriff auf den CloudTrail Eventverlauf. Der CloudTrail Ereignisverlauf bietet eine einsehbare, durchsuchbare, herunterladbare und unveränderliche Aufzeichnung der aufgezeichneten Verwaltungsereignisse der letzten 90 Tage in einem. AWS-Region Weitere Informationen finden Sie im AWS CloudTrail Benutzerhandbuch unter Arbeiten mit dem CloudTrail Ereignisverlauf. Für die Anzeige des Eventverlaufs CloudTrail fallen keine Gebühren an.

Für eine fortlaufende Aufzeichnung der Ereignisse in AWS-Konto den letzten 90 Tagen erstellen Sie einen Trail- oder CloudTrailLake-Event-Datenspeicher.

CloudTrail Pfade

Ein Trail ermöglicht CloudTrail die Übermittlung von Protokolldateien an einen Amazon S3 S3-Bucket. Alle mit dem erstellten Pfade AWS Management Console sind regionsübergreifend. Sie können einen Pfad mit einer oder mehreren Regionen erstellen, indem Sie den verwenden. AWS CLI Es wird empfohlen, einen Trail mit mehreren Regionen zu erstellen, da Sie alle Aktivitäten in Ihrem Konto AWS-Regionen erfassen. Wenn du einen Trail mit nur einer Region erstellst, kannst du dir nur die Ereignisse ansehen, die in den Trails protokolliert wurden. AWS-Region Weitere Informationen zu Trails finden Sie unter Einen Trail für Sie erstellen AWS-Konto und Einen Trail für eine Organisation erstellen im AWS CloudTrail Benutzerhandbuch.

Sie können eine Kopie Ihrer laufenden Verwaltungsereignisse kostenlos an Ihren Amazon S3 S3-Bucket senden, CloudTrail indem Sie einen Trail erstellen. Es fallen jedoch Amazon S3 S3-Speichergebühren an. Weitere Informationen zur CloudTrail Preisgestaltung finden Sie unter AWS CloudTrail Preise. Informationen zu Amazon-S3-Preisen finden Sie unter Amazon S3-Preise.

CloudTrail Datenspeicher für Ereignisse in Lake

CloudTrail Mit Lake können Sie SQL basierte Abfragen zu Ihren Ereignissen ausführen. CloudTrail Lake konvertiert bestehende Ereignisse im zeilenbasierten JSON Format in das ORCApache-Format. ORCist ein spaltenförmiges Speicherformat, das für den schnellen Abruf von Daten optimiert ist. Die Ereignisse werden in Ereignisdatenspeichern zusammengefasst, bei denen es sich um unveränderliche Sammlungen von Ereignissen handelt, die auf Kriterien basieren, die Sie mit Hilfe von erweiterten Ereignisselektoren auswählen. Die Selektoren, die Sie auf einen Ereignisdatenspeicher anwenden, steuern, welche Ereignisse bestehen bleiben und für Sie zur Abfrage verfügbar sind. Weitere Informationen zu CloudTrail Lake finden Sie im AWS CloudTrail Benutzerhandbuch unter Arbeiten mit AWS CloudTrail Lake.

CloudTrail Für das Speichern und Abfragen von Ereignisdaten in Lake fallen Kosten an. Beim Erstellen eines Ereignisdatenspeichers wählen Sie die Preisoption aus, die für den

Ereignisdatenspeicher genutzt werden soll. Die Preisoption bestimmt die Kosten für die Erfassung und Speicherung von Ereignissen sowie die standardmäßige und maximale Aufbewahrungsdauer für den Ereignisdatenspeicher. Weitere Informationen zur CloudTrail Preisgestaltung finden Sie unter AWS CloudTrail Preise.

AWS Outposts Management-Ereignisse in CloudTrail

Verwaltungsereignisse bieten Informationen über Verwaltungsvorgänge, die an Ressourcen in Ihrem ausgeführt werden AWS-Konto. Sie werden auch als Vorgänge auf Steuerebene bezeichnet. CloudTrail Protokolliert standardmäßig Verwaltungsereignisse.

AWS Outposts protokolliert alle Operationen auf der Kontrollebene AWS von Outposts als Managementereignisse. Eine Liste der Operationen auf der Kontrollebene von AWS Outposts, die AWS Outposts protokolliert CloudTrail, finden Sie in der AWS APIOutposts-Referenz.

AWS Outposts Beispiele für Ereignisse

Das folgende Beispiel zeigt ein CloudTrail Ereignis, das den `SetSiteAddress` Vorgang demonstriert.


```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AKIAIOSFODNN7EXAMPLE:jdoe",
        "arn": "arn:aws:sts::111122223333:assumed-role/example/jdoe",
        "accountId": "111122223333",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AKIAIOSFODNN7EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/example",
                "accountId": "111122223333",
                "userName": "example"
            },
            "webIdFederationData": {},
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2020-08-14T16:28:16Z"
            }
```

```
        }
    },
    "eventTime": "2020-08-14T16:32:23Z",
    "eventSource": "outposts.amazonaws.com",
    "eventName": "SetSiteAddress",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "XXX.XXX.XXX.XXX",
    "userAgent": "userAgent",
    "requestParameters": {
        "SiteId": "os-123ab4c56789de01f",
        "Address": "***"
    },
    "responseElements": {
        "Address": "***",
        "SiteId": "os-123ab4c56789de01f"
    },
    "requestID": "1abcd23e-f4gh-567j-klm8-9np01q234r56",
    "eventID": "1234a56b-c78d-9e0f-g1h2-34jk56m7n890",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
```

Wartung von Outposts

Im Rahmen des Modells der AWS ist die für die Hardware und Software verantwortlich, mit der AWS Dienste ausgeführt werden. Das gilt für AWS Outposts, genau wie für eine AWS Region. AWS Verwaltet beispielsweise Sicherheitspatches, aktualisiert Firmware und wartet die Outpost-Geräte. AWS überwacht auch die Leistung, den Zustand und die Messwerte für Ihren und stellt fest, ob Wartungsarbeiten erforderlich sind.

> **Warning**
>
> Daten auf Instance-Speicher-Volumes gehen verloren, wenn das zugrunde liegende Festplattenlaufwerk ausfällt oder wenn die Instance angehalten, in den Ruhezustand versetzt oder beendet wird. Um Datenverlust zu vermeiden, empfehlen wir Ihnen, Ihre langfristigen Daten auf Instance-Speicher-Volumes in einem persistenten Speicher zu sichern, z. B. in einem Amazon S3 S3-Bucket, einem EBS Amazon-Volume oder einem Netzwerkspeichergerät in Ihrem lokalen Netzwerk.

Inhalt

Hardware-Wartung

Wenn während der Serverbereitstellung oder beim Hosten von EC2 Amazon-Instances, die auf Ihrem laufen, ein irreparables Hardwareproblem AWS festgestellt wird, werden wir sowohl den Outpost-Eigentümer als auch den Eigentümer der Instances darüber informieren, dass die betroffenen Instances stillgelegt werden sollen. Weitere Informationen finden Sie unter Instance Retirement im EC2Amazon-Benutzerhandbuch.

Der Outpost-Besitzer und der Instance-Besitzer können zusammenarbeiten, um das Problem zu lösen. Der Instance-Besitzer kann eine betroffene Instance stoppen und starten, um sie auf die verfügbare Kapazität zu migrieren. Instance-Besitzer können die betroffenen Instances zu einem für sie passenden Zeitpunkt beenden und starten. Andernfalls werden die betroffenen Instances am

Tag der Außerbetriebnahme der Instance AWS gestoppt und neu gestartet. Wenn auf dem Outpost keine zusätzliche Kapazität vorhanden ist, verbleibt die Instance im Status „Gestoppt“. Der Outpost-Besitzer kann versuchen, genutzte Kapazität freizugeben oder zusätzliche Kapazität für den Outpost anfordern, damit die Migration abgeschlossen werden kann.

Falls eine Hardwarewartung erforderlich ist, AWS kontaktiert er den Manager der Outpost-Site, um Datum und 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 wieder in Betrieb. Installationsteam führt vor Ort keine Hardwarediagnosen oder Reparaturen durch. Wenn sie einen Host austauschen, entfernen und vernichten sie den NIST -konformen physischen Sicherheitsschlüssel, wodurch alle Daten, die möglicherweise auf der Hardware verbleiben, vernichtet werden. Dadurch wird sichergestellt, dass keine Daten Ihren Standort verlassen. Wenn das Installationsteam ein Outpost-Netzwerkgerät ersetzt, sind möglicherweise Netzwerkkonfigurationsinformationen auf dem Gerät vorhanden, wenn es vom Standort entfernt wird. Diese Informationen können IP-Adressen beinhalten und ASNs zur Einrichtung virtueller Schnittstellen für die Konfiguration des Pfads zu Ihrem lokalen Netzwerk oder zurück zur Region verwendet werden.

Firmware-Updates

Die Aktualisierung der Outpost-Firmware hat normalerweise keine Auswirkungen auf die Instances auf Ihrem Outpost. In dem seltenen Fall, dass wir die Outpost-Geräte neu starten müssen, um ein Update zu installieren, erhalten Sie für alle Instances, die mit dieser Kapazität laufen, eine Benachrichtigung über die Außerbetriebnahme der Instance.

Wartung der Netzwerkausrüstung

Die Wartung der Outpost-Netzwerkgeräte (OND) erfolgt ohne Beeinträchtigung des regulären Outpost-Betriebs und des Datenverkehrs. Wenn Wartungsarbeiten erforderlich sind, wird der Verkehr vom OND Möglicherweise stellen Sie vorübergehende Änderungen in den BGP Werbeanzeigen fest, wie z. B. das Voranstellen von AS-Path, und entsprechende Änderungen der Verkehrsmuster auf Outpost-Uplinks. Bei OND Firmware-Updates stellen Sie möglicherweise ein Flattern fest. BGP

Wir empfehlen Ihnen, die Netzwerkausrüstung Ihrer Kunden so zu konfigurieren, dass sie BGP Werbung von Outposts empfangen, ohne die BGP Attribute zu ändern, und BGP Multipath-/Load-

Balancing zu aktivieren, um optimale eingehende Datenflüsse zu erzielen. AS-Path-Präfixe werden für lokale Gateway-Präfixe verwendet, um den Datenverkehr zu verlagern, falls Wartungsarbeiten erforderlich sind. ONDs Das Kundennetzwerk sollte Routen von Outposts mit einer AS-Pfadlänge von 1 gegenüber Routen mit einer AS-Pfadlänge von 4 bevorzugen.

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

Bewährte Methoden für -Strom- und Netzwerkereignisse

Wie in den AWS Servicebedingungen für AWS Outposts Kunden angegeben, muss die Einrichtung, in der sich die Outposts-Ausrüstung befindet, die Mindestanforderungen an Strom und Netzwerk erfüllen, um die Installation, Wartung und Nutzung der Outposts-Ausrüstung zu unterstützen. Ein kann nur dann ordnungsgemäß funktionieren, wenn Strom und Netzwerkkonnektivität unterbrechungsfrei sind.

Stromereignisse

Bei vollständigen Stromausfällen besteht das inhärente Risiko, dass eine AWS Outposts Ressource nicht automatisch wieder in Betrieb genommen wird. Zusätzlich zur Bereitstellung redundanter Stromversorgungs- und Notstromversorgungslösungen empfehlen wir, dass Sie im Voraus Folgendes tun, um die Auswirkungen einiger der schlimmsten Szenarien zu minimieren:

- Verlagern Sie Ihre Dienste und Anwendungen auf kontrollierte Weise von den Outposts-Geräten, indem Sie Änderungen beim Lastenausgleich DNS auf Basis oder außerhalb des Racks verwenden.
- Stoppen Sie Container, Instances und Datenbanken in einer inkrementellen Reihenfolge und verwenden Sie bei der Wiederherstellung die umgekehrte Reihenfolge.
- Testpläne für das kontrollierte Verschieben oder Stoppen von Diensten.
- Sichern Sie wichtige Daten und Konfigurationen und speichern Sie sie außerhalb der Outposts.
- Beschränken Sie Stromausfallzeiten auf ein Minimum.

- Vermeiden Sie ein wiederholtes Umschalten der Stromversorgungen (off-on-off-on) während der Wartung.
- Planen Sie innerhalb des Wartungszeitfensters zusätzliche Zeit ein, um unvorhergesehene Ereignisse zu beheben.
- Steuern Sie die Erwartungen Ihrer Benutzer und Kunden, indem Sie ein größeres Zeitfenster für die Wartung angeben, als Sie normalerweise benötigen würden.

Netzwerkkonnektivitätsereignisse

Die Service Link-Verbindung zwischen Ihrem Outpost und der AWS Region oder der Heimatregion von Outposts wird in der Regel automatisch nach Netzwerkunterbrechungen oder Problemen wiederhergestellt, die in Ihren vorgelagerten Unternehmensnetzwerkgeräten oder im Netzwerk eines Drittanbieters auftreten können, sobald die Netzwerkwartung abgeschlossen ist. Während der Zeit, in der die Service-Link-Verbindung unterbrochen ist, ist der Betrieb Ihrer Outposts auf lokale Netzwerkaktivitäten beschränkt.

Weitere Informationen finden Sie in der Frage Was passiert, wenn die Netzwerkverbindung meiner Einrichtung unterbrochen wird? auf der AWS Outposts FAQsRack-Seite.

Wenn die Serviceverbindung aufgrund eines Stromausfalls vor Ort oder aufgrund eines Verlusts der Netzwerkverbindung nicht verfügbar ist, AWS Health Dashboard sendet der eine Benachrichtigung an das Konto, dem die Outposts gehören. Weder Sie noch Sie AWS können die Benachrichtigung über eine Unterbrechung der Verbindung unterdrücken, selbst wenn die Unterbrechung zu erwarten ist. Weitere Informationen finden Sie unter Erste Schritte mit dem AWS Health Dashboard im AWS Health -Benutzerhandbuch.

Ergreifen Sie im Falle einer geplanten Servicewartung, die sich auf die Netzwerkkonnektivität auswirkt, die folgenden proaktiven Maßnahmen, um die Auswirkungen potenzieller Problemszenarien zu begrenzen:

- Wenn Ihr Outposts-Rack über das Internet oder eine öffentliche Direktverbindung mit der übergeordneten AWS Region verbunden ist, sollten Sie vor einer geplanten Wartung eine Trace-Route erfassen. Ein funktionierender (pre-network-maintenance) Netzwerkpfad und ein problematischer (post-network-maintenance) Netzwerkpfad zur Identifizierung der Unterschiede wären bei der Problembehebung hilfreich. Falls Sie ein Problem nach der Wartung an AWS oder Ihren weiterleitenISP, 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 *region* mit dem Namen der übergeordneten 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 Überwachung AWS Outposts befasst sich mit bewährten Methoden zur Beobachtbarkeit und zum Eventmanagement speziell für Outposts.
- Der AWS Blog Debugging-Tool für Netzwerkkonnektivität von Amazon VPC erklärt das Tool AWSSupport-S etupIPMonitoring From VPC. Dieses Tool ist ein AWS Systems Manager Dokument (SSMDokument), das eine Amazon EC2 Monitor-Instance in einem von Ihnen angegebenen Subnetz erstellt und Ziel-IP-Adressen überwacht. Das Dokument führt Ping-MTR, TCP Trace-Route- und Trace-Path-Diagnosetests durch und speichert die Ergebnisse in Amazon CloudWatch Logs, die in einem CloudWatch Dashboard visualisiert werden können (z. B. Latenz, Paketverlust). Für die Überwachung von Outposts sollte sich die Monitor-Instance in einem Subnetz der übergeordneten AWS Region befinden und so konfiguriert sein, dass sie eine oder mehrere Ihrer Outpost-Instances mithilfe ihrer privaten IP (s) überwacht. Dadurch werden Diagramme zum Paketverlust und zur Latenz zwischen AWS Outposts und der übergeordneten Region angezeigt. AWS
- Der AWS Blog Deploying an automated Amazon CloudWatch dashboard for AWS OutpostsAWS CDK use beschreibt die Schritte zur Bereitstellung eines automatisierten Dashboards.

- Wenn Sie Fragen haben oder weitere Informationen benötigen, finden Sie weitere Informationen unter Erstellen eines Support-Falls im Support-Benutzerhandbuch für AWS .

end-of-term Rack-Optionen für Outposts

Am Ende Ihrer AWS Outposts Amtszeit müssen Sie zwischen den folgenden Optionen wählen:

- Erneuern Sie Ihr Abonnement und behalten Sie Ihre bestehenden Outposts-Racks.
- Beenden Sie Ihr Abonnement und bereiten Sie Ihre Outposts-Racks für die Rückgabe vor.
- Wechseln Sie zu einem month-to-month Abonnement und behalten Sie Ihre bestehenden Outposts-Racks.

Verlängern Sie Ihr Abonnement

Sie müssen die folgenden Schritte mindestens 30 Tage vor Ablauf des aktuellen Abonnements für Ihre Outposts-Racks abschließen.

Um Ihr Abonnement zu verlängern und Ihre bestehenden Outposts-Racks zu behalten

1. Melden Sie sich bei der AWS Support -Center-Konsole an.
2. Wählen Sie Create case (Fall erstellen) aus.
3. Wählen Sie Konto und Fakturierung aus.
4. Wählen Sie als Service Fakturierung aus.
5. Wählen Sie als Kategorie die Option Andere Fragen zur Rechnungsstellung aus.
6. Wählen Sie als Schweregrad die Option Wichtige Frage aus.
7. Wählen Sie Next step: Additional information (Nächster Schritt: Zusätzliche Informationen).
8. Geben Sie auf der Seite Zusätzliche Informationen für Betreff Ihre Verlängerungsanfrage ein, z. B. **`Renew my Outpost subscription`**.
9. Geben Sie unter Beschreibung eine der folgenden Zahlungsoptionen ein:

   - Keine Vorauszahlung
   - Teilweise Vorauszahlung
   - Komplette Vorauszahlung

   Informationen zu den Preisen finden Sie unter AWS Outposts – Rackpreise. Sie können auch ein Preisangebot anfordern.

10. Klicken Sie auf Next step: Solve now or contact us (()Nächster Schritt): Jetzt lösen oder Support kontaktieren).
11. Wählen Sie auf der Seite Contact us (Kontakt) Ihre bevorzugte Sprache aus.
12. Wählen Sie Ihre bevorzugte Kontaktmethode.
13. Überprüfen Sie Ihre Falldetails und wählen Sie Submit (Absenden) aus. Ihre Fall-ID-Nummer und Übersicht werden angezeigt.

AWS Der Kundensupport leitet die Verlängerung des Abonnements ein. Ihr neues Abonnement beginnt am Tag nach Ablauf Ihres aktuellen Abonnements.

Wenn Sie nicht angeben, dass Sie Ihr Abonnement verlängern oder Ihr Outposts-Rack zurückgeben möchten, werden Sie automatisch in ein month-to-month Abonnement umgewandelt. Ihr Outposts-Rack wird monatlich zum Tarif der Zahlungsoption „Keine Vorauszahlung“ erneuert, die Ihrer AWS Outposts Konfiguration entspricht. Ihr neues monatliches Abonnement beginnt am Tag nach Ablauf Ihres aktuellen Abonnements.

Ihr Abonnement beenden und die Rückgabe vorbereiten

Sie müssen die folgenden Schritte mindestens 30 Tage vor Ablauf des aktuellen Abonnements für Ihr Outposts-Rack abschließen. AWS Sie können den Rückgabevorgang erst starten, wenn Sie dies tun.

> **Important**
>
> AWS kann den Rückgabevorgang nicht beenden, nachdem Sie eine Support-Anfrage zur Kündigung Ihres Abonnements geöffnet haben.

Um dein Abonnement zu beenden

1. Melden Sie sich bei der AWS Support -Center-Konsole an.
2. Wählen Sie Create case (Fall erstellen) aus.
3. Wählen Sie Konto und Fakturierung aus.
4. Wählen Sie als Service Fakturierung aus.
5. Wählen Sie als Kategorie die Option Andere Fragen zur Rechnungsstellung aus.
6. Wählen Sie als Schweregrad die Option Wichtige Frage aus.

7. Wählen Sie Next step: Additional information (Nächster Schritt: Zusätzliche Informationen).
8. Geben Sie auf der Seite Zusätzliche Informationen für Betreff eine eindeutige Anfrage ein, z. B. **`End my Outpost subscription`**
9. Geben Sie unter Beschreibung das Datum ein, an dem der Outpost abgeholt werden soll.
10. Klicken Sie auf Next step: Solve now or contact us (()Nächster Schritt): Jetzt lösen oder Support kontaktieren).
11. Wählen Sie auf der Seite Contact us (Kontakt) Ihre bevorzugte Sprache aus.
12. Wählen Sie Ihre bevorzugte Kontaktmethode.
13. Überprüfen Sie Ihre Falldetails und wählen Sie Submit (Absenden) aus. Ihre Fall-ID-Nummer und Übersicht werden angezeigt.

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

So bereitest du deine AWS Outposts Regale für die Rückgabe vor:

> **Important**
>
> Schalten Sie das Outposts-Rack erst aus, wenn es für den geplanten Abruf vor Ort AWS ist.

1. Wenn die Ressourcen des Outposts freigegeben sind, müssen Sie die Freigabe dieser Ressourcen aufheben.

   Sie können die Freigabe einer gemeinsam genutzten Outpost-Ressource auf eine der folgenden Arten aufheben:

   - Verwenden Sie die Konsole AWS RAM . Weitere Informationen finden Sie unter Aktualisieren einer Ressourcenfreigabe im AWS RAM -Benutzerhandbuch.
   - Verwenden Sie den AWS CLI , um den disassociate-resource-shareBefehl auszuführen.

   Eine Liste der Outpost-Ressourcen, die freigegeben werden können, finden Sie unter Freigebbare Outpost-Ressourcen.
2. Beenden Sie die aktiven Instances, die Subnetzen auf Ihrem Outpost zugeordnet sind. Um die Instances zu beenden, folgen Sie den Anweisungen unter Ihre Instance beenden im EC2Amazon-Benutzerhandbuch.

> **Note**
>
> Einige AWS verwaltete Dienste, die auf Ihrem Outpost ausgeführt werden, wie Application Load Balancers oder Amazon Relational Database Service (RDS), verbrauchen Kapazität. EC2 Ihre zugehörigen Instances sind jedoch im EC2 Amazon-Dashboard nicht sichtbar. Sie müssen die mit diesen Diensten verbundenen Ressourcen beenden, um Kapazitäten freizugeben. Weitere Informationen finden Sie unter Warum fehlt in meinem Outpost EC2 Instance-Kapazität? .

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

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

   b. Wählen Sie Outposts.

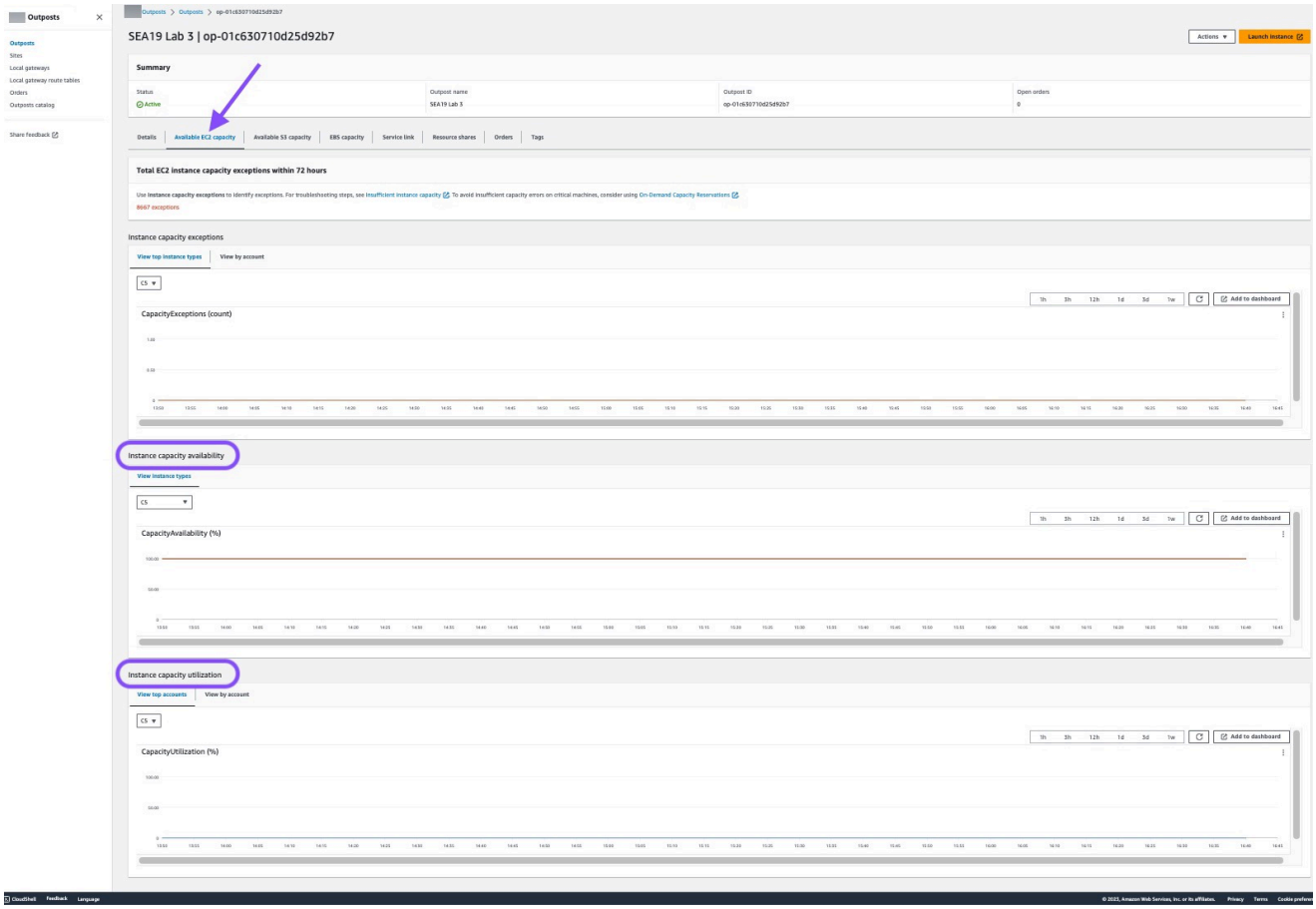
   c. Wählen Sie den spezifischen Outpost aus, zu dem Sie zurückkehren.

   d. Wählen Sie auf der Seite für den Outpost den Tab Verfügbare EC2 Kapazität aus.

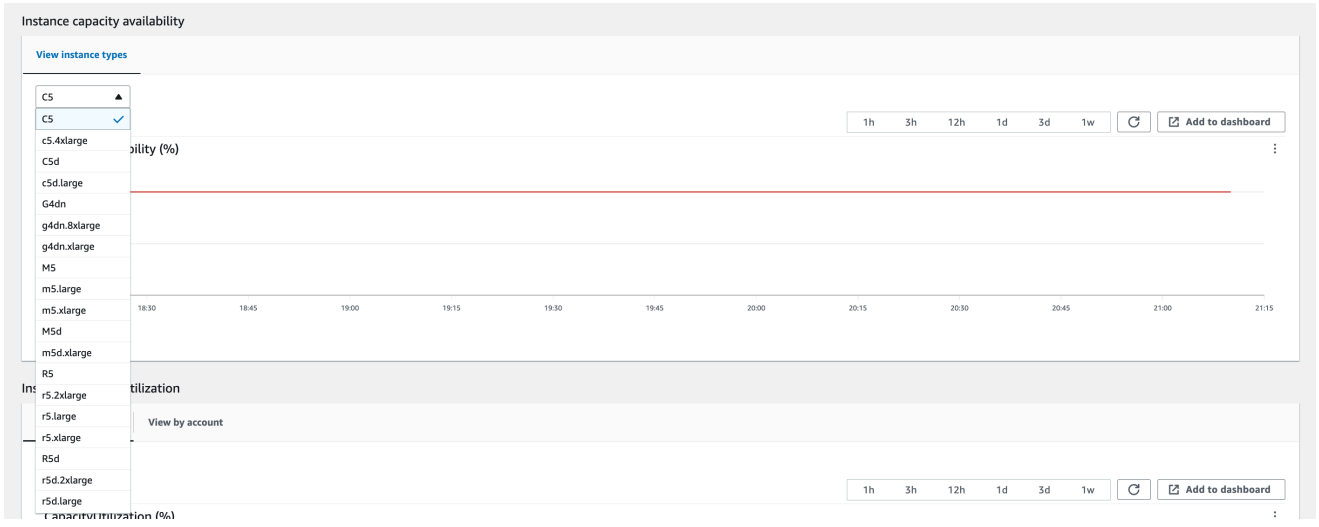
   e. Stellen Sie sicher, dass die Instance-Kapazitätsverfügbarkeit für jede Instance-Familie bei 100 % liegt.

   f. Stellen Sie sicher, dass die Instance-Kapazitätsauslastung für jede Instance-Familie bei 0 % liegt.

      Die folgende Abbildung zeigt die Diagramme zur Verfügbarkeit der Instance-Kapazität und zur Kapazitätsauslastung der Instanz auf der Registerkarte Verfügbare EC2 Kapazität.



Die folgende Abbildung zeigt die Liste der Instance-Typen.



4. Erstellen Sie Backups Ihrer EC2 Amazon-Instances und Server-Volumes. Um die Backups zu erstellen, folgen Sie den Anweisungen unter Backup and Recovery for Amazon EC2 with EBS Volumes im AWS Prescriptive Guidance Guide.
5. Löschen Sie die EBS Amazon-Volumes, die mit Ihrem Outpost verknüpft sind.

   a. Öffnen Sie die EC2 Amazon-Konsolenkonsole unter https://console.aws.amazon.com/ec2/.
   b. Wählen Sie im Navigationsbereich Volumes aus.
   c. Wählen Sie Aktionen und Volume löschen aus.
   d. Wählen Sie im Bestätigungs-Dialogfeld die Option Delete (Löschen).
6. Wenn Sie Amazon S3 auf Outposts haben, löschen Sie alle lokalen Snapshots in den Outposts.
   a. Öffnen Sie die EC2 Amazon-Konsolenkonsole unter https://console.aws.amazon.com/ec2/.
   b. Wählen Sie im Navigationsbereich die Option Snapshots aus.
   c. Wählen Sie die Schnappschüsse mit einem Outpost ausARN.
   d. Wählen Sie Aktionen und Schnappschüsse löschen.
   e. Wählen Sie im Bestätigungs-Dialogfeld die Option Delete (Löschen).
7. Löschen Sie alle Amazon S3 S3-Buckets, die mit Ihrem Outposts-Rack verknüpft sind. Um die Buckets zu löschen, folgen Sie den Anweisungen unter Löschen Ihres Amazon S3 in Outposts Buckets im Amazon Simple Storage Service Benutzerhandbuch.
8. Löschen Sie alle VPC Verknüpfungen und den kundeneigenen IP-Adresspool (CoIP), die mit Ihrem Outpost CIDRs verknüpft sind.

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

In ein Abonnement umwandeln month-to-month

Um auf ein month-to-month Abonnement umzusteigen und Ihre bestehenden Outposts-Racks zu behalten, sind keine Maßnahmen erforderlich. Wenn Sie Fragen haben, öffnen Sie eine Support-Anfrage für die Abrechnung.

Ihre Outposts-Racks werden monatlich zum Tarif der Zahlungsoption „Keine Vorauszahlung“ erneuert, die Ihrer Outposts-Konfiguration entspricht. Ihr neues monatliches Abonnement beginnt am Tag nach dem Ende Ihres aktuellen Abonnements.

Kontingente für AWS Outposts

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.

In der folgenden Tabelle werden die Dokumentationsaktualisierungen für 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 den virtuelle n Rack-Servicelink-Schnittste llen (VIFs) Ihrer Outposts und Ihren lokalen Netzwerkg eräten überwachen, indem Sie Metriken nutzen`IfTraffic In` . `IfTrafficOut` Amazon CloudWatch	17. November 2023
VPCIntrakommunikation über AWS Outposts das lokale Gateway	Sie können die Kommunika tion zwischen Subnetzen desselben 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 on Outposts enthält einen Resolver, der alle DNS Anfragen zwischens peichert, die von der stammen. AWS Outposts Sie können auch eine Hybridverbindung zwischen einem Outpost	20. Juli 2023

	und einem lokalen DNS Resolver einrichten, wenn Sie eingehende und ausgehende Endpunkte bereitstellen.	
Eingehende Routen am lokalen Gateway	Sie können eingehende Routen für das lokale Gateway zu Elastic-Netzwerkschnittstellen auf Ihrem Outpost erstellen und ändern.	15. September 2022
VPCWir führen direktes Routing ein für AWS Outposts	Verwendet die private IP-Adresse der Instances in IhremVPC, um die Kommunikation mit Ihrem lokalen Netzwerk zu erleichtern.	14. September 2022
AWS Outposts Benutzerleitfaden für Outposts-Racks erstellt	AWS Outposts Das Benutzerhandbuch ist in separate Anleitungen für Rack und Server aufgeteilt.	14. September 2022
Routing-Tabellen für lokale Gateways erstellen und verwalten	Erstellen und ändern Sie Routing-Tabellen lokale Gateways und CoIP-Pools. VIFGruppenzuordnungen verwalten.	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 Volumen 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 AWS Outposts Ressourcen	Mit Outpost Sharing können Outpost-Besitzer ihre Outposts und Outpost-Ressourcen , einschließlich lokaler Gateway-Routentabellen, mit anderen AWS Konten derselben Organisation teilen. AWS	15. Oktober 2020
Zusätzliche Metriken CloudWatch	Zusätzliche CloudWatch Metriken für die Anzahl der Instance-Typen sind verfügbar .	21. September 2020
Zusätzliche CloudWatch Metrik	Eine zusätzliche CloudWatch Metrik für den Status der Verbindung mit dem Service Link ist verfügbar.	11. September 2020
Support für die gemeinsame Nutzung von kundeneigenen Adressen IPv4	Wird verwendet AWS Resource Access Manager , um kundeneigene IPv4 Adressen zu teilen.	20. April 2020
Zusätzliche Metriken CloudWatch	Zusätzliche CloudWatch Metriken für EBS Volumen 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.