Benutzerhandbuch für Server

AWS Outposts

AWS Outposts: Benutzerhandbuch für Server

Table of Contents

Was ist AWS Outposts?

AWS Outposts ist ein vollständig verwalteter Service, der AWS Infrastruktur, Dienste, APIs 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 am Standort eines Kunden 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 und Subnetze erstellen. Instances in Outpost-Subnetzen kommunizieren mit anderen Instances in der AWS -Region mithilfe privater IP-Adressen, sämtlich innerhalb derselben VPC.

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

Weitere Informationen finden Sie auf der AWS Outposts -Produktseite.

Die wichtigsten Konzepte

Dies sind die wichtigsten Konzepte für. AWS Outposts

- 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 Outpost-Racks gehören Server, Switches, ein Netzwerk-Patchpanel, ein Power-Shelf und leere Panels, die im Rack montiert werden können.
- Sie müssen ein ACE-Rack installieren, wenn Sie über fünf oder mehr Computer-Racks verfügen. 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 Branchenstandard handelt, der in einem standardmäßigen EIA-310D 19-konformen 4-Post-Rack installiert werden kann. Outpost-Server bieten lokale Rechen- und Netzwerkdienste für Standorte mit begrenztem Platzbedarf oder geringeren Kapazitätsanforderungen.
- Serviceverbindung — Netzwerkroute, die die Kommunikation zwischen Ihrem Außenposten und der zugehörigen AWS Region ermöglicht. Jeder Outpost ist eine Erweiterung einer Availability Zone und der zugehörigen Region.
- Lokales Gateway (LGW) — Ein virtueller Router mit logischer Verbindung, der die Kommunikation zwischen einem Outpost-Rack und Ihrem lokalen Netzwerk ermöglicht.
- Lokale Netzwerkschnittstelle – Eine Netzwerkschnittstelle, die die Kommunikation zwischen einem Outpost-Server und Ihrem On-Premises-Netzwerk ermöglicht.

AWS Ressourcen auf Outposts

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

Datenverarbeitung

Ressourcentyp	Racks	Server
Amazon EC2-Instances	Ja	Ja

Ressourcentyp	Racks	Server
Amazon-ECS-Cluster	 Ja	 Ja
Amazon-EKS-Knoten	 Ja	 Nein

Datenbank und Analytik

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

Netzwerk

Ressourcentyp	Racks	Server
App Mesh Envoy-Proxy	 Ja	 Ja

Ressourcentyp	Racks	Server
Application Load Balancer	Ja	Nein
Amazon VPC-Subnetze	Ja	Ja
Amazon Route 53	Ja	Nein

Speicher

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

Andere AWS-Services

Service	Racks	Server
AWS IoT Greengrass	Ja	Ja

Service	Racks	Server
Amazon SageMaker Edge-Manager	 Ja	 Ja

Preisgestaltung

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

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

- AWS Outposts Preisgestaltung
- 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 On-Premises-Netzwerk muss einen Wide Area Network (WAN)-Zugriff zur Region und zum Internet ermöglichen. Es muss auch LAN- oder WAN-Zugriff auf das lokale Netzwerk bieten, in dem sich Ihre On-Premises-Workloads oder Anwendungen befinden.

Das folgende Diagramm veranschaulicht beide Outpost-Formfaktoren.

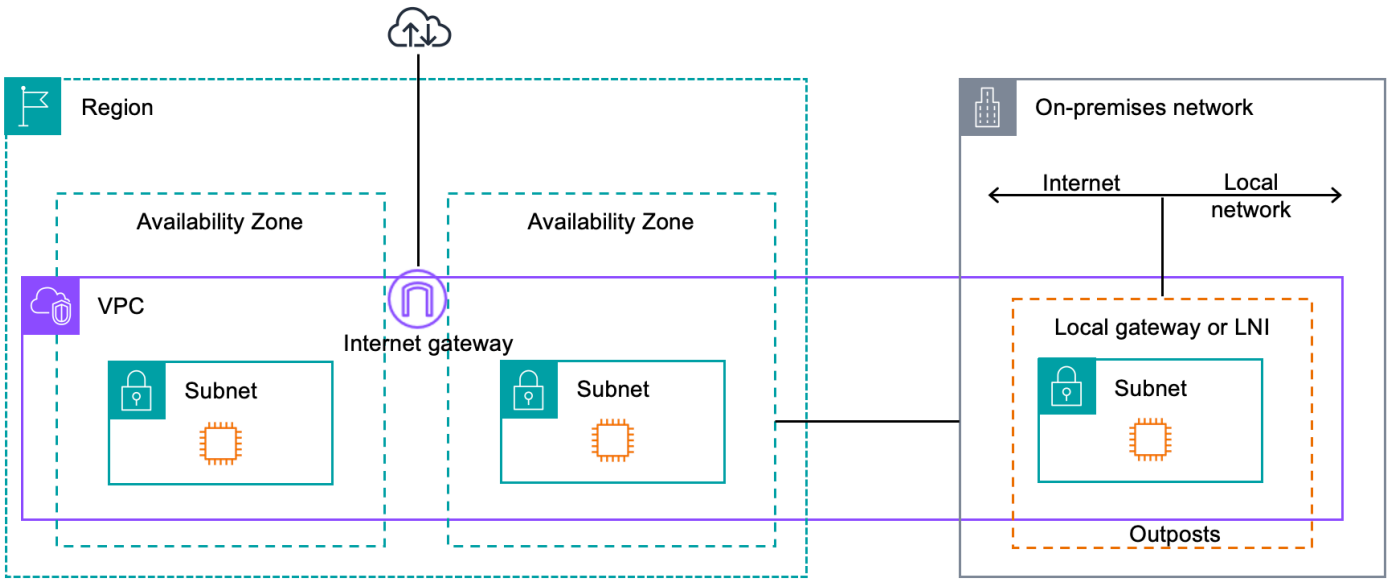
Inhalt

Netzwerkkomponenten

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

Das folgende Diagramm zeigt die Netzwerkkomponenten für Ihren Outpost.

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



VPCs und Subnetze

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

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

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

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

Routing

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

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

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

- VPC CIDR-Bereich — AWS definiert dies bei der Installation. Dies ist die lokale Route und gilt für das gesamte VPC-Routing, einschließlich des Datenverkehrs zwischen Outpost-Instances in derselben VPC.
- AWS Ziele in der Region — Dazu gehören Präfixlisten für Amazon Simple Storage Service (Amazon S3), Amazon DynamoDB DynamoDB-Gateway-Endpunkte, AWS Transit Gateway virtuelle private Gateways, Internet-Gateways und VPC-Peering.

  Wenn Sie eine Peering-Verbindung mit mehreren VPCs auf demselben Outpost haben, verbleibt der Datenverkehr zwischen den VPCs im Outpost und verwendet nicht den Service Link zurück zur Region.

DNS

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

Abhängig von der Pfadlatenz zwischen Ihrem Outpost und der Region kann es bei Route 53 zu längeren DNS-Auflösungszeiten kommen. AWS In solchen Fällen können Sie die in Ihrer On-Premises-Umgebung installierten DNS-Server verwenden. Um Ihre eigenen DNS-Server zu verwenden, müssen Sie DHCP-Optionssätze für Ihre On-Premises-DNS-Server erstellen und sie der VPC zuordnen. Sie müssen außerdem sicherstellen, dass IP-Konnektivität zu diesen DNS-Servern besteht. Möglicherweise müssen Sie der Routing-Tabelle des lokalen Gateways auch Routen hinzufügen, um die Erreichbarkeit zu gewährleisten. Dies ist jedoch nur eine Option für Outpost-

Racks mit lokalem Gateway. Da DHCP-Optionssätze einen VPC-Bereich haben, versuchen Instances sowohl in den Outpost-Subnetzen als auch in den Subnetzen der Availability Zone für die VPC, die angegebenen DNS-Server für die DNS-Namensauflösung zu verwenden.

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

Service Link

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

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

- Outpost-Konnektivität zu AWS-Regionen
- Das Whitepaper zum Routing von Anwendungen und Workloads im Hinblick auf Design und Architektur zur AWS Outposts Hochverfügbarkeit AWS

Lokale Netzwerkschnittstellen

Outpost-Server verfügen über eine lokale Netzwerkschnittstelle, um die Konnektivität zu Ihrem On-Premises-Netzwerk herzustellen. Eine lokale Netzwerkschnittstelle ist nur für Outposts-Server verfügbar, die in einem Outpost-Subnetz laufen. Sie können keine lokale Netzwerkschnittstelle von einer EC2-Instance in einem Outpost-Rack oder in der Region aus verwenden. AWS Die lokale Netzwerkschnittstelle ist nur für On-Premises-Standorte vorgesehen. Weitere Informationen finden Sie unter Lokale Netzwerkschnittstellen.

Standortanforderungen für

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 -Servers – FAQs. Sehen Sie sich die Frage an: In welchen Ländern und Territorien sind Outposts Server verfügbar?

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

Einrichtung

Dies sind die Anforderungen an die Einrichtung von Servern.

> **Note**
>
> Die Spezifikationen gelten für Server unter normalen Betriebsbedingungen. Beispielsweise kann es sein, dass die Akustik bei der Erstinstallation lauter klingt und nach Abschluss der Installation mit der Nennschallleistung betrieben wird.

- Temperatur – Die Umgebungstemperatur muss zwischen 5–35° C (41–95° F) liegen.

  Der Server wird heruntergefahren, wenn die Temperatur außerhalb dieses Bereichs liegt, und wird neu gestartet, wenn die Temperatur wieder innerhalb dieses Bereichs liegt.
- Luftfeuchtigkeit – Die relative Luftfeuchtigkeit muss zwischen 8 und 80 Prozent liegen und darf nicht kondensieren.
- Luftqualität – Die Luft muss mit einem MERV8-Filter (oder höher) gefiltert werden.
- Luftstrom – Die Position des Servers muss einen Mindestabstand von 6 Zoll (15 cm) zwischen dem Server und den Wänden vor und hinter dem Server gewährleisten, um einen ausreichenden Luftstrom zu gewährleisten.
- Gewicht – Der 1U-Server wiegt 26 Pfund und der 2U-Server wiegt 36 Pfund. Vergewissern Sie sich, dass der Standort, an dem Sie den Server aufstellen möchten, das Gewicht des Servers tragen kann.

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

- Kompatibilität mit Schienensets – Das im Lieferumfang enthaltene Schienenset ist mit einer L-förmigen Standardhalterung eines EIA-310-D-konformen 19-Zoll-Racks kompatibel.

  > **Important**
  >
  > Das Schienenset ist nicht mit einer U-förmigen Montagehalterung kompatibel, wie in der folgenden Abbildung gezeigt.

- Platzierung des Racks – Wir empfehlen die Verwendung von standardmäßigen 19-Zoll-EIA-310D-Racks mit einer Tiefe von mindestens 36 Zoll (914 mm).
  - Outposts 2U-Server benötigen Speicherplatz mit den folgenden Abmessungen: 3,5 Zoll Höhe (88,9 mm), 17,5 Zoll Breite (447 mm), 30 Zoll Tiefe (762 mm)
  - Outposts 1U-Server benötigen Speicherplatz mit den folgenden Abmessungen: 1,75 Zoll Höhe (44,45 mm), 17,5 Zoll Breite (447 mm), 24 Zoll Tiefe (610 mm)

  > **Note**
  >
  > - Die vertikale Montage AWS Outposts von Servern wird nicht unterstützt.
  > - Outposts 1U Server haben dieselbe Breite wie Outposts 2U Server, aber halb so hoch und weniger tief

  AWS bietet ein Schienenset für die Rackmontage des Servers. Weitere Informationen finden Sie unter Schritt 3: Rack-Montage.

  Wenn Sie den Server nicht in einem Rack platzieren, müssen Sie dennoch die anderen in diesem Abschnitt aufgeführten Anforderungen erfüllen.

- Wartungsfreundlichkeit – Outposts-Server können beim Kunden gewartet werden.
- Akustik – Die Schallleistung ist für weniger als 78 dBA bei Temperaturen von 80 °F (27 °C) ausgelegt und entspricht der GR-63 CORE NEBS-Konformität.

- Erdbebensichere Verankerung – Soweit dies durch Vorschriften oder Gesetze vorgeschrieben ist, werden Sie eine angemessene erdbebensichere Verankerung und Verstrebung für den Server installieren und aufrechterhalten, solange er sich in Ihrer Einrichtung befindet.
- Höhenlage – Die Höhenlage des Raums, in dem das Rack installiert ist, muss unter 3.050 Metern (10.005 Fuß) liegen.
- Reinigung – Wischen Sie die Oberflächen mit feuchten Tüchern ab, die zugelassene antistatische Reinigungschemikalien enthalten.

Netzwerk

Jeder Outposts-Server umfasst nicht redundante physische Uplink-Ports. Ports haben ihre eigenen Geschwindigkeits- und Konnektoranforderungen, wie unten beschrieben.

Portkennzeichnungen	Geschwindigkeit	Anschluss am Upstream-Netzwerkgerät	Datenverkehr
Port: 3	10 GbE	SFP+	Sowohl Service- als auch LNI-Link-Datenverkehr – Das QSFP+-Breakout-Kabel (10 Fuß / 3 m) segmentiert den Datenverkehr. Weitere Informationen finden Sie unter Konfigurieren des QSFP-Netzwerks.

Service Link-Firewall

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

Protokoll	Quell-Port	Quelladresse	Ziel-Port	Zieladresse
UDP	1024 - 65535	Service-Link-IP	53	DNS-Server, der über DHCP bereitgestellt wird
UDP	443, 1024-65535	Service-Link-IP	443	Outposts Service Link-Endpunkte
TCP	1024 - 65535	Service-Link-IP	443	Endpunkte für die Registrierung von Outposts

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

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

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

Empfehlungen für die Bandbreite von Service Links

Für eine optimale Benutzererfahrung und Ausfallsicherheit AWS empfiehlt es sich, für die Service Link-Verbindung zur Region redundante Konnektivität mit mindestens 500 Mbit/s zu verwenden. AWS Die maximale Auslastung für jeden Outpost-Server beträgt 500 Mbit/s. Verwenden Sie mehrere Outpost-Server, um die Verbindungsgeschwindigkeit zu erhöhen. Wenn Sie beispielsweise drei AWS Outposts -Server haben, erhöht sich die maximale Verbindungsgeschwindigkeit auf 1,5 Gbit/s (1.500 Mbit/s). Weitere Informationen finden Sie unter Service Link-Datenverkehr für Server.

Ihre AWS Outposts Service Link-Bandbreitenanforderungen variieren je nach Workload-Merkmalen wie AMI-Größe, Anwendungselastizität, Burst-Geschwindigkeitsanforderungen und Amazon VPC-

Verkehr in die Region. Beachten Sie, dass AWS Outposts Server keine AMIs zwischenspeichern. AMIs werden bei jedem Instance-Start aus der Region heruntergeladen.

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

Service Link erfordert eine DHCP-Antwort

Der Service Link erfordert eine IPv4-DHCP-Antwort, um die Netzwerkeinstellungen zu konfigurieren.

Maximale Latenz von Service Link

Service Links können bis zu einer maximalen Netzwerklatenz von 250 ms vom Server und seiner Availability Zone unterstützten.

Stromversorgung

Dies sind die Stromversorgungsanforderungen für Outposts-Server.

Voraussetzungen

- Strom-Unterstützung
- Leistungsaufnahme
- Stromkabel
- Redundanz der Stromversorgung

Strom-Unterstützung

Server sind für Wechselstrom von bis zu 1600 W, 90–264 VAC, 47/63 Hz ausgelegt.

Leistungsaufnahme

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

Stromkabel

Der Server wird mit einem IEC C14-C13-Stromkabel geliefert.

Stromverkabelung vom Server zum Rack

Verwenden Sie das mitgelieferte IEC C14-C13-Stromkabel, um den Server mit dem Rack zu verbinden.

Stromverkabelung vom Server zur Wandsteckdose

Um den Server an eine Standardsteckdose anzuschließen, müssen Sie entweder einen Adapter für den C14-Eingang oder ein landesspezifisches Netzkabel verwenden.

Stellen Sie sicher, dass Sie den richtigen Adapter oder das richtige Netzkabel für Ihre Region haben, um Zeit bei der Serverinstallation zu sparen.

- In den Vereinigten Staaten benötigen Sie ein IEC C13-NEMA-5-15P-Netzkabel.
- In Teilen Europas benötigen Sie möglicherweise ein IEC C13-CEE-7/7-Netzkabel.
- In Indien benötigen Sie ein IEC C13-IS1293-Netzkabel.

Redundanz der Stromversorgung

Server verfügen über mehrere Stromanschlüsse und werden mit Kabeln geliefert, um einen redundanten Betrieb zu ermöglichen. Wir empfehlen Stromredundanz, Redundanz ist jedoch nicht erforderlich.

Server verfügen nicht über eine unterbrechungsfreie Stromversorgung (USV).

Erfüllung der Bestellung

Um die Bestellung zu erfüllen, AWS wird die Outposts-Serverausrüstung, einschließlich Schienenhalterungen und der erforderlichen Strom- und Netzwerkkabel, an die von Ihnen angegebene Adresse versendet. Der Karton, in dem der Server geliefert wird, hat die folgenden Abmessungen:

- Karton mit einem 2U-Server:
  - Länge: 44 Zoll/111,8 cm
  - Höhe: 26,5 Zoll / 67,3 cm
  - Breite: 17 Zoll / 43,2 cm
- Karton mit einem 1U-Server:

- Länge: 34,5 Zoll / 87,6 cm
- Höhe: 24 Zoll / 61 cm
- Breite: 9 Zoll / 22,9 cm

Ihr Team oder ein Drittanbieter muss das Gerät installieren. Weitere Informationen finden Sie unter Installation des Outpost-Servers.

Die Installation ist abgeschlossen, wenn Sie bestätigen, dass die Amazon EC2 EC2-Kapazität für Ihren Outposts-Server von Ihrem AWS Konto aus verfügbar ist.

Fangen Sie an mit AWS Outposts

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

Aufgaben

- Erstellen eines Outpost und Bestellung von Outpost-Kapazitäten
- Installation des Outpost-Servers
- Starten Sie eine Instanz auf Ihrem Outpost-Server

Erstellen eines Outpost und Bestellung von Outpost-Kapazitäten

Um mit der Nutzung zu beginnen AWS Outposts, melden Sie sich mit dem AWS Konto an, dem der Outpost gehören wird. Erstellen Sie einen Standort und einen Outpost. Geben Sie dann eine Bestellung für die Outposts-Server auf, die Sie benötigen.

Voraussetzungen

- Sehen Sie sich die verfügbaren Konfigurationen für Ihre Outposts-Server 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 .
- 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 Standort, an dem Sie Ihre Outposts-Server installieren und ausführen werden. Nachdem Sie die Site erstellt haben, AWS Outposts weist Sie Ihrer Site eine ID zu. Sie müssen diesen Standort angeben, wenn Sie einen Outpost erstellen.

Voraussetzungen

- Bestimmen Sie die Betriebsadresse.

So erstellen Sie einen Standort:

1. Melde dich 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 Nur Server aus.
7. Geben Sie den Namen, die Beschreibung und die Betriebsadresse für Ihren Standort ein.
8. (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.
9. Wählen Sie Create site (Standort erstellen).

Schritt 2: Erstellen eines Outpost

Erstellen Sie für jeden Server einen Outpost. Ein Outpost kann nur mit einem einzigen Server verknüpft werden. Sie spezifizieren diesen Outpost bei der Bestellung.

Voraussetzungen

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

Erstellen eines Outpost

1. Wählen Sie im Navigationsbereich Outposts aus.
2. Wählen Sie Outposts erstellen.
3. Wählen Sie Servers (Server) aus.
4. Geben Sie den Namen und eine Beschreibung für Ihren Outpost ein.
5. Wählen Sie eine Availability Zone für Ihren Outpost aus.
6. Wählen Sie unter Site-ID Ihren Standort aus.
7. Wählen Sie Outposts erstellen.

Schritt 3: Bestellung

Geben Sie eine Bestellung für die Outposts-Server auf, die Sie benötigen. Nachdem Sie die Bestellung abgeschickt haben, wird sich ein AWS Outposts -Vertreter mit Ihnen in Verbindung setzen.

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

Voraussetzungen

- Bestimmen Sie, wie Sie für die Bestellung bezahlen werden. Sie haben folgende Optionen: Vollständige Vorauszahlung, Teilweise Vorauszahlung oder Keine Vorauszahlung. Wenn Sie die Zahlungsoption teilweise oder ohne Vorauszahlung wählen, zahlen Sie über die Laufzeit 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 Server aus.
4. Um Kapazität hinzuzufügen, wählen Sie eine Konfiguration aus.
5. Wählen Sie Weiter aus.
6. Wählen Sie Vorhandenen Outpost verwenden und wählen Sie Ihren Outpost aus.
7. Wählen Sie Weiter aus.
8. Wählen Sie eine Vertragslaufzeit und eine Zahlungsoption aus.
9. Geben Sie die Lieferadresse an. Sie können eine neue Adresse angeben oder die Betriebsadresse des Standorts auswählen. Wenn Sie die Betriebsadresse auswählen, beachten Sie bitte, dass jede künftige Änderung der Betriebsadresse des Standorts sich nicht auf bestehende Bestellungen auswirken wird. Wenn Sie die Lieferadresse einer bestehenden Bestellung ändern müssen, wenden Sie sich an Ihren AWS Kundenbetreuer.
10. Wählen Sie Weiter aus.
11. Vergewissern Sie sich auf der Seite Überprüfen und Bestellen, dass Ihre Informationen korrekt sind, und bearbeiten Sie sie nach Bedarf. Sie können die Bestellung nicht mehr bearbeiten, nachdem Sie sie abgeschickt haben.
12. Wählen Sie Bestellung aufgeben.

Schritt 4: Ändern Sie die Instance-Kapazität

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 aus.
3. Auf der Seite Instance-Kapazität konfigurieren wird für jeden Instance-Typ eine Instance-Größe angezeigt, wobei die maximale Anzahl vorausgewählt ist. Um weitere Instance-Größen hinzuzufügen, wählen Sie Instance-Größe hinzufügen.
4. Geben Sie die Anzahl der Instances an und notieren Sie sich die Kapazität, die für diese Instance-Größe angezeigt wird.
5. Sehen Sie sich die Meldung am Ende jedes Abschnitts mit dem Instanztyp an, in der Sie darüber informiert werden, ob Ihre Kapazität zu hoch oder zu niedrig ist. Nehmen Sie Anpassungen auf der Ebene der Instance-Größe oder Menge vor, um Ihre verfügbare Gesamtkapazität zu optimieren.
6. Sie können auch beantragen AWS Outposts , die Instance-Menge für eine bestimmte Instance-Größe zu optimieren. Gehen Sie hierzu wie folgt vor:
   a. Wählen Sie die Instanzgröße.
   b. Wählen Sie am Ende des entsprechenden Abschnitts mit dem Instanztyp die Option Automatisches Ausgleichen aus.
7. Stellen Sie für jeden Instance-Typ sicher, dass die Instance-Menge für mindestens eine Instance-Größe angegeben ist.

8. Wählen Sie Weiter aus.
9. Überprüfen Sie auf der Seite Überprüfen und erstellen, welche Aktualisierungen Sie anfordern.
10. Wählen Sie Erstellen. AWS Outposts erstellt eine Kapazitätsaufgabe.
11. Überwachen Sie auf der Seite mit den Kapazitätsaufgaben den Status der Aufgabe.

> **Note**
>
> AWS Outposts fordert Sie möglicherweise auf, eine oder mehrere laufende Instances zu beenden, um die Ausführung der Kapazitätsaufgabe zu ermöglichen. Nachdem Sie diese Instanzen beendet haben, AWS Outposts wird die Aufgabe ausgeführt.

Upload JSON file

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

   Example

   Beispiel für eine JSON-Datei:

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

4. Überprüfen Sie den Inhalt der JSON-Datei im Abschnitt Kapazitätskonfigurationsplan.
5. Wählen Sie Weiter aus.

6. Überprüfen Sie auf der Seite Überprüfen und erstellen, welche Aktualisierungen Sie anfordern.
7. Wählen Sie Erstellen. AWS Outposts erstellt eine Kapazitätsaufgabe.
8. Überwachen Sie auf der Seite mit den Kapazitätsaufgaben den Status der Aufgabe.

> **Note**
>
> AWS Outposts fordert Sie möglicherweise auf, eine oder mehrere laufende Instances zu beenden, um die Ausführung der Kapazitätsaufgabe zu ermöglichen. Nachdem Sie diese Instanzen beendet haben, AWS Outposts wird die Aufgabe ausgeführt.

Nächste Schritte

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

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

Um die Bestellung zu erfüllen, vereinbaren AWS wir einen Liefertermin.

Sie sind für alle Installationsaufgaben verantwortlich, einschließlich der physischen Installation und der Netzwerkkonfiguration. Sie können einen Drittanbieter mit der Ausführung dieser Aufgaben für Sie beauftragen. Unabhängig davon, ob Sie die Installation selbst durchführen oder einen Dritten damit beauftragen, erfordert die Installation IAM-Anmeldeinformationen in dem AWS-Konto , das den Outpost enthält, um die Identität des neuen Geräts zu überprüfen. Sie sind für die Bereitstellung und Verwaltung dieses Zugriffs verantwortlich. Weitere Informationen finden Sie unter the section called “Installation des Outpost-Servers”.

Die Installation ist abgeschlossen, wenn Amazon EC2-Kapazität für Ihren Outpost in Ihrem AWS-Konto verfügbar ist. Nach der Verfügbarkeit der Kapazität können Sie Amazon EC2-Instances auf Ihrem Outpost-Server starten. Weitere Informationen finden Sie unter the section called “Starten einer -Instance”.

Installation des Outpost-Servers

Wenn Sie einen Outpost-Server bestellen, sind Sie für die Installation verantwortlich, unabhängig davon, ob Sie sie selbst durchführen oder einen Drittanbieter beauftragen. Die Partei, die die Installation durchführt, benötigt spezielle Berechtigungen, um die Identität des neuen Geräts zu überprüfen. Weitere Informationen finden Sie unter Berechtigungen erteilen.

Voraussetzung

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

> **Note**
>
> Wir empfehlen Ihnen, sich vor und während des Installationsvorgangs das Schulungsvideo zur Installation von AWS Outposts Servern anzusehen. Um an der Schulung teilnehmen zu können, müssen Sie sich bei AWS -Skill Builder anmelden oder ein Konto erstellen.

Aufgaben

- Schritt 1: Erteilen von Berechtigungen
- Schritt 2: Überprüfen
- Schritt 3: Rack-Montage
- Schritt 4: Einschalten
- Schritt 5: Netzwerk verbinden
- Schritt 6: Autorisieren des Servers
- Befehlsreferenz für das Outpost Configuration Tool

Schritt 1: Erteilen von Berechtigungen

Um die Identität des neuen Geräts zu überprüfen, müssen Sie über IAM-Anmeldeinformationen in dem AWS-Konto verfügen, das den Outpost enthält. Die AWSOutpostsAuthorizeServerPolicy-Richtlinie gewährt die für die Installation eines Outpost-Servers erforderlichen Berechtigungen. Weitere Informationen finden Sie unter the section called “Identity and Access Management”.

Überlegungen

- Wenn Sie einen Drittanbieter verwenden, der keinen Zugriff auf Ihre Daten hat AWS-Konto, müssen Sie temporären Zugriff gewähren.
- AWS Outposts unterstützt die Verwendung temporärer Anmeldeinformationen. Sie können temporäre Anmeldeinformationen konfigurieren, die bis zu 36 Stunden gültig sind. Stellen Sie sicher, dass Sie dem Installationsdienstleister genügend Zeit geben, um alle Schritte der Serverinstallation durchzuführen. Weitere Informationen finden Sie unter the section called “Temporäre Anmeldeinformationen”.

Schritt 2: Überprüfen

Um die Ausrüstung des Outposts zu überprüfen, sollten Sie den Versandkarton auf Schäden untersuchen, den Karton auspacken und den Nitro Security Key (NSK) suchen. Beachten Sie die folgenden Informationen zur Inspektion des Servers:

- Die Versandverpackung verfügt über Stoßsensoren, die sich an den beiden größten Seiten des Kartons befinden.
- Die Innenklappe der Versandverpackung enthält Anweisungen zum Auspacken des Servers und zum Auffinden des NSK.
- Der NSK ist ein Verschlüsselungsmodul. Um die Inspektion abzuschließen, suchen Sie den NSK. Sie bringen den NSK in einem späteren Schritt am Server an.

Versandverpackung überprüfen

So überprüfen Sie die Versandverpackung

- Überprüfen Sie vor dem Öffnen der Versandverpackung beide Stoßsensoren und stellen Sie fest, ob sie aktiviert wurden. Wenn die Stoßsensoren aktiviert wurden, wurde das Gerät möglicherweise beschädigt. Fahren Sie mit der Installation fort und nehmen Sie sich Zeit, um weitere Schäden am Server oder am Zubehör festzustellen. Wenn ein Teil des Systems offensichtlich beschädigt ist oder die Installation nicht wie erwartet abläuft, wenden Sie sich an den AWS Support, um Informationen zum Austausch Ihres Outposts-Servers zu erhalten.

Wenn der Balken in der Mitte des Sensors rot ist, wurde der Sensor aktiviert.

Versandverpackung auspacken

So packen Sie die Versandverpackung aus

- Öffnen Sie den Karton und stellen Sie sicher, dass er Folgendes enthält:
  - Server
  - Nitro Security Key (Verschlüsselungsmodul) – Verpackung, die rot mit „NSK“ gekennzeichnet ist. Weitere Informationen finden Sie im folgenden Verfahren zum Auffinden des NSK in der Versandverpackung.
  - Rack-Montagesatz (2 innere Schienen, 2 äußere Schienen und Schrauben)
  - Installationsbroschüre
  - Zubehörsatz
    - Paar C13/14-Stromkabel – 3 m (10 Fuß)
    - QSFP-Breakout-Kabel – 3 m (10 Fuß)

- USB-Kabel, Micro-USB auf USB-C – 3 m (10 Fuß)
- Bürstenschutz

Den NSK finden

Der NSK befindet sich in dem Karton mit der Aufschrift A, der das Zubehör für den Server enthält.

> **Important**
>
> Verwenden Sie den NSK nicht, um während der Installation Daten auf dem Server zu zerstören.

Der NSK ist erforderlich, um den Server zu aktivieren. Der NSK wird ferner verwendet, um Daten auf dem Server zu vernichten, wenn Sie den Server zurückschicken. Ignorieren Sie in diesem Installationsschritt die Anweisungen auf dem Gehäuse des NSK, da diese Anweisungen dazu dienen, Daten zu vernichten.

Schritt 3: Rack-Montage

Um diesen Schritt abzuschließen, müssen Sie die inneren Schienen am Server und die äußeren Schienen am Rack befestigen und dann den Server im Rack montieren. Für diese Schritte benötigen Sie einen Kreuzschlitzschraubendreher.

Alternativen zur Rack-Montage

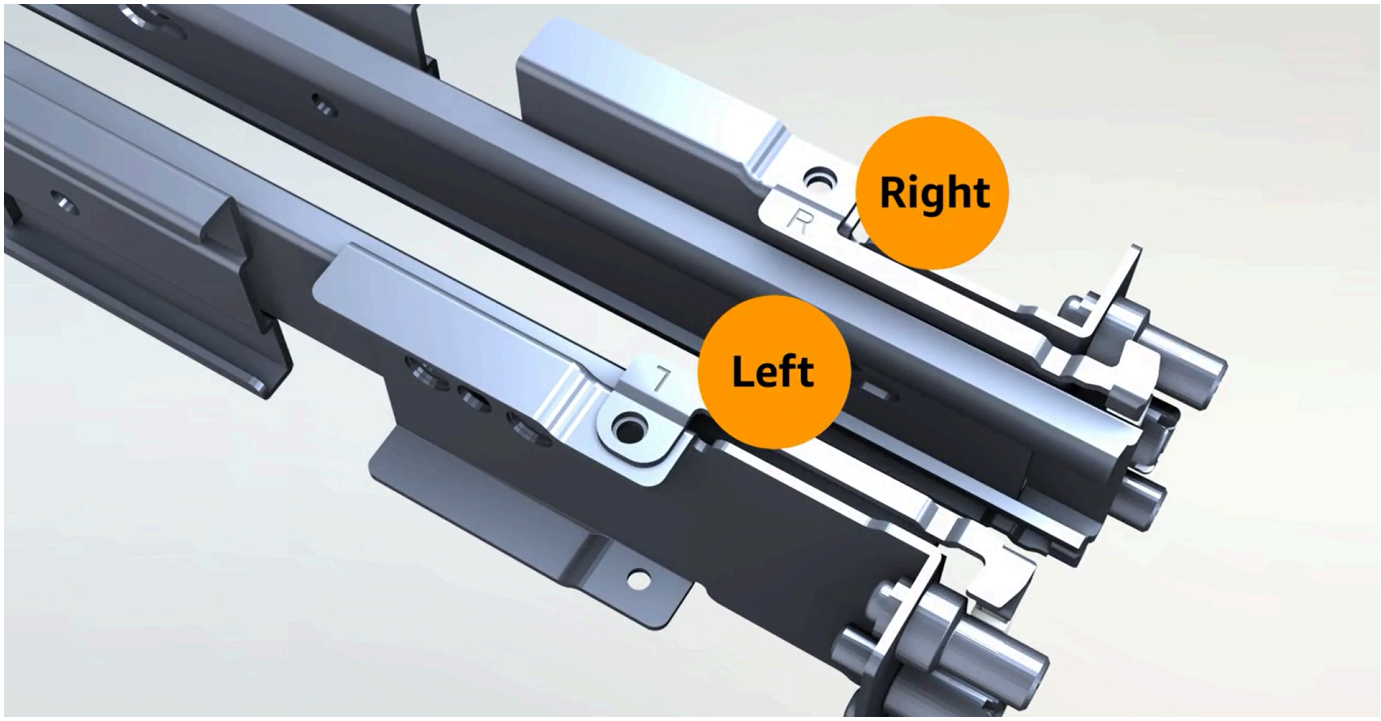
Sie müssen den Server nicht in einem Rack montieren. Wenn Sie den Server nicht in einem Rack montieren, beachten Sie die folgenden Informationen:

- Achten Sie auf einen Mindestabstand von 15 cm (6 Zoll) zwischen dem Server und den Wänden vor und hinter dem Server, damit die heiße Luft zirkulieren kann.
- Stellen Sie den Server auf eine stabile Oberfläche, die frei von mechanischen Gefahren wie Feuchtigkeit oder herabfallenden Gegenständen ist.
- Um die im Lieferumfang des Servers enthaltenen Netzwerkkabel verwenden zu können, müssen Sie den Server in einem Umkreis von 3 m von Ihrem Upstream-Netzwerkgerät platzieren.
- Befolgen Sie die lokalen Richtlinien für erdbebensichere Aussteifung und Verankerung.

Identifizieren Sie Seiten und Enden

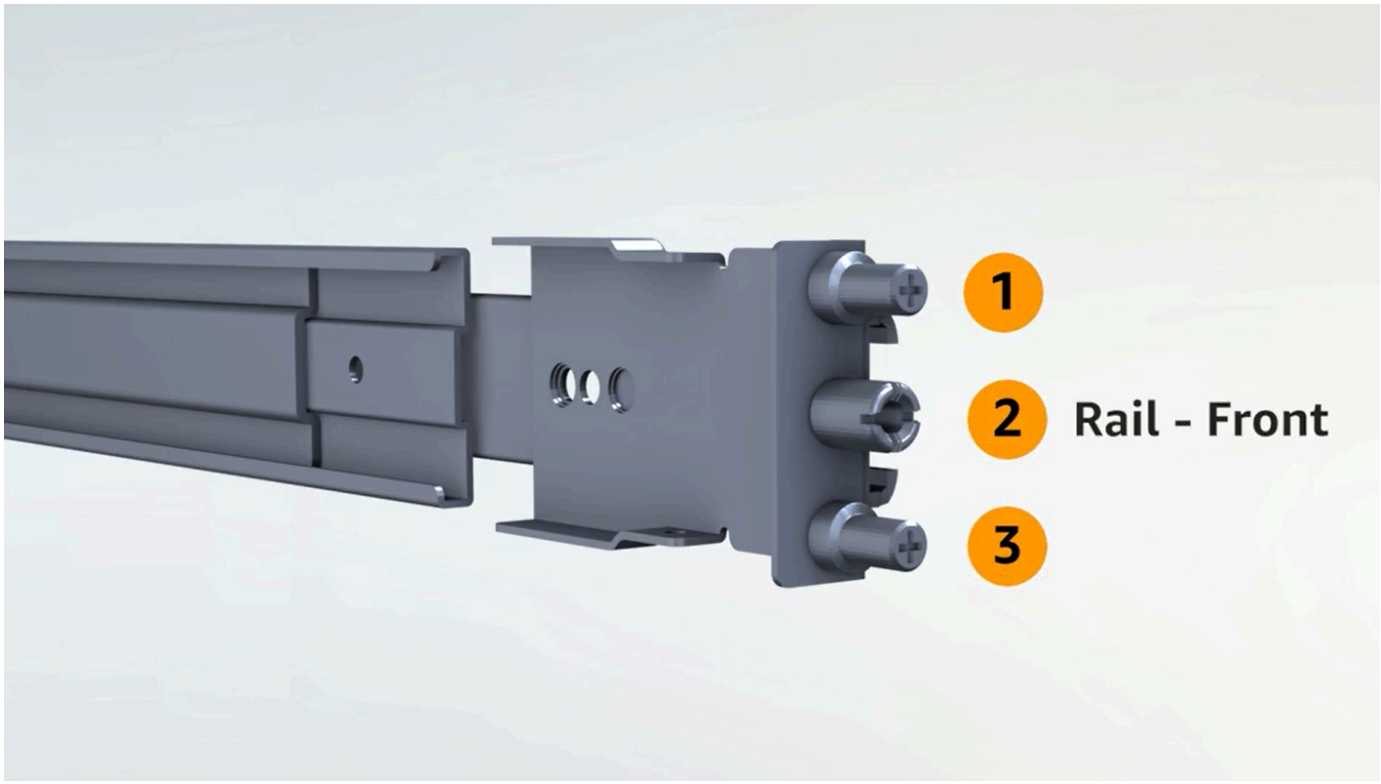
So unterscheiden Sie links von rechts, vorne von hinten

1. Suchen Sie den Karton mit den Rack-Schienen, die im Lieferumfang des Servers enthalten war, und öffnen Sie ihn.
2. Sehen Sie sich die Markierungen auf den Schienen an, um festzustellen, welche links und welche rechts ist. Diese Markierungen bestimmen, an welcher Seite des Servers die einzelnen Schienen befestigt werden.

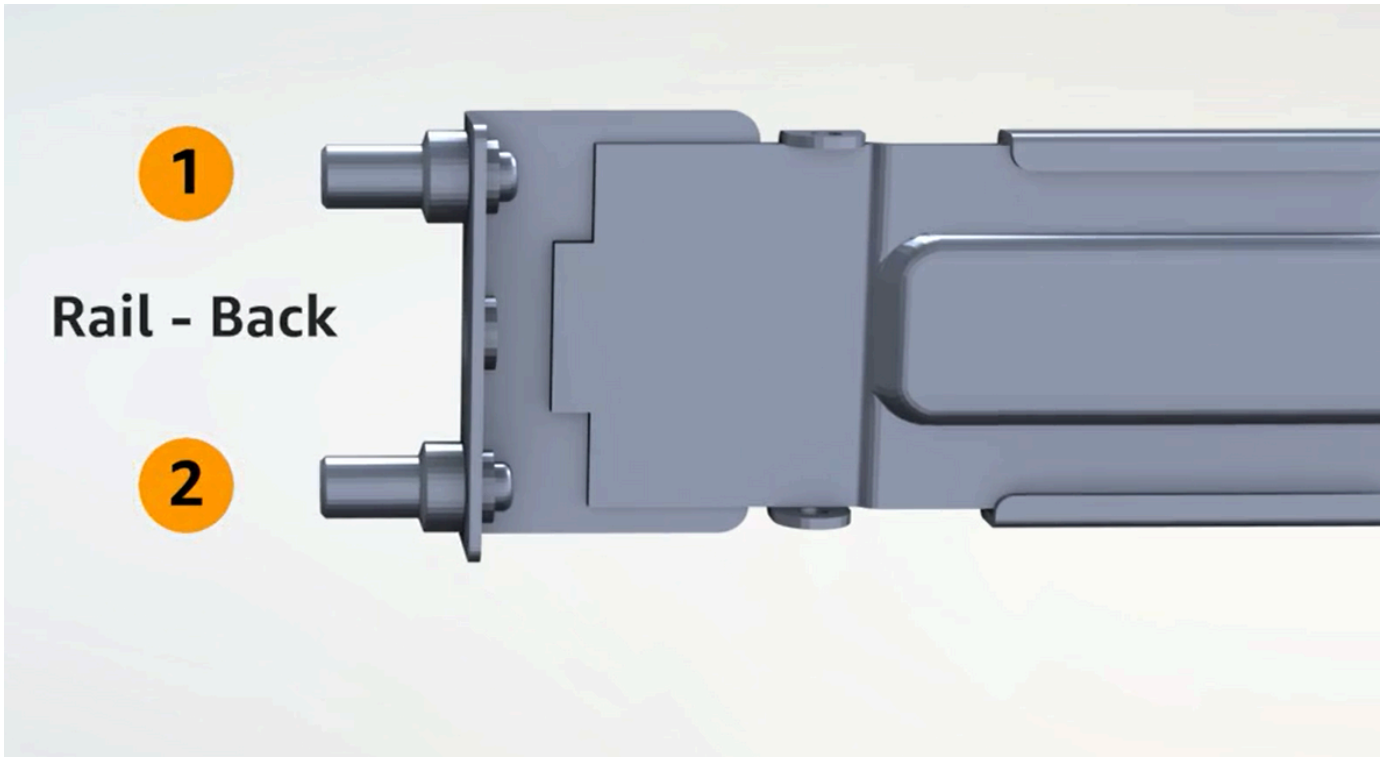


3. Schauen Sie sich die Streben an beiden Enden der Schienen an, um festzustellen, welche vorne und welche hinten ist.

   Das vordere Ende hat drei Streben.



Das hintere Ende hat zwei Streben.



Anbringen der inneren Schienen

So bringen Sie die inneren Schienen am Server an

1. Lösen Sie bei beiden Schienen die innere Schiene von der äußeren Schiene. Sie sollten nun vier Schienen haben.
2. Befestigen Sie die rechte Innenschiene an der rechten Seite des Servers und sichern Sie die Schiene mit einer Schraube. Achten Sie darauf, dass Sie die Schiene korrekt am Server ausrichten. Richten Sie den vorderen Teil der Schiene zur Vorderseite des Servers aus.
3. Befestigen Sie die linke Innenschiene an der linken Seite des Servers und sichern Sie die Schiene mit einer Schraube.

Anbringen der äußeren Schienen

So bringen Sie die äußeren Schienen am Rack an

1. Schauen Sie auf das Rack und verwenden Sie die mit R markierte Schiene auf der rechten Seite des Racks. Befestigen Sie zuerst die Rückseite der Schiene am Rack und fahren Sie dann die Schiene aus, um sie mit der Vorderseite des Racks zu verbinden.

   > **Tip**
   >
   > Achten Sie auf die Ausrichtung der Schienen. Verwenden Sie bei Bedarf die mitgelieferten Pinadapter.

2. Wiederholen Sie dies mit der linken Schiene auf der linken Seite.

Montieren des Servers

So montieren Sie den Server im Rack

- Schieben Sie den Server in die äußeren Schienen, die Sie im vorherigen Schritt am Rack angebracht haben, und sichern Sie den Server an der Vorderseite mit zwei mitgelieferten Schrauben.

  > **Tip**
  >
  > Schieben Sie den Server mit zwei Personen in das Rack.

Schritt 4: Einschalten

Zum Abschluss der Inbetriebnahme bringen Sie den NSK an, schließen den Server an eine Stromquelle an und überprüfen, ob der Server eingeschaltet ist. Beachten Sie die folgenden Informationen zur Stromversorgung des Servers:

- Der Server funktioniert mit einer Stromquelle, AWS empfiehlt jedoch aus Redundanzgründen die Verwendung von zwei Stromquellen.
- Schließen Sie die Stromkabel vor dem Anschluss der Netzwerkkabel an.
- Verwenden Sie die beiden Stromkabel mit C13-Ausgang und C14-Eingang, um den Server mit einem Netzteil im Rack zu verbinden. Wenn Sie das Stromkabel des C14-Eingangs nicht verwenden, um den Server an eine Stromversorgung im Rack anzuschließen, müssen Sie Adapter für die C14-Eingänge bereitstellen, die an eine Stromquelle angeschlossen werden.

NSK anbringen

Sie müssen den NSK am Server anbringen, damit er die Daten auf dem Server während des Betriebs entschlüsseln kann.

Important

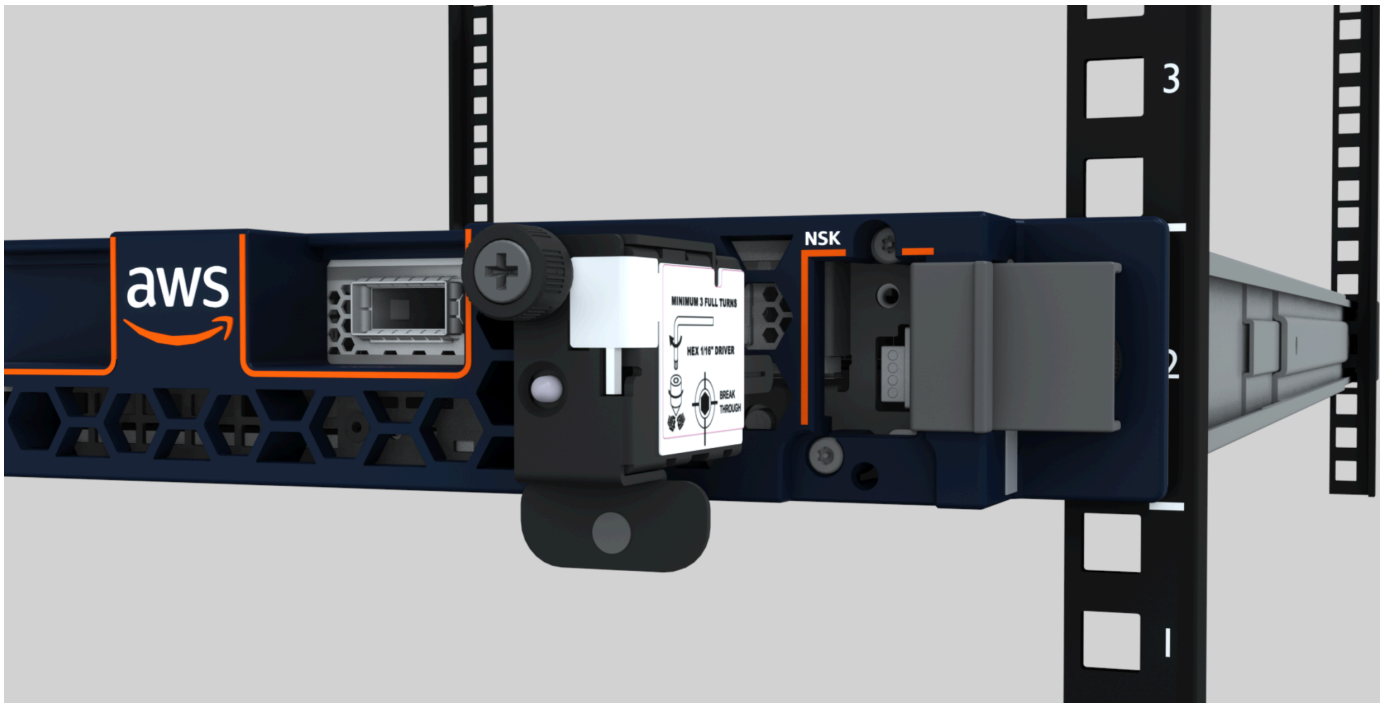
- An der Seite des NSK finden Sie Anweisungen zur Zerstörung des NSK. Folgen Sie diesen Anweisungen jetzt nicht. Folgen Sie diesen Anweisungen nur, wenn Sie zum Server an AWS zurückgeben, um die Daten auf dem Server kryptografisch zu vernichten.
- Wenn Sie mehrere Server gleichzeitig installieren, stellen Sie sicher, dass Sie die NSKs nicht verwechseln. Sie müssen den NSK an dem Server anbringen, mit dem er geliefert wurde. Wenn Sie einen anderen NSK verwenden, kann der Server nicht gestartet werden.

So bringen Sie den NSK an

1. Öffnen Sie auf der rechten Vorderseite des Servers das NSK-Fach.

   Das folgende Bild zeigt den NSK, der an einem 2U-Server angebracht ist.

Die folgende Abbildung zeigt den NSK, der an einem 1U-Server angebracht ist.

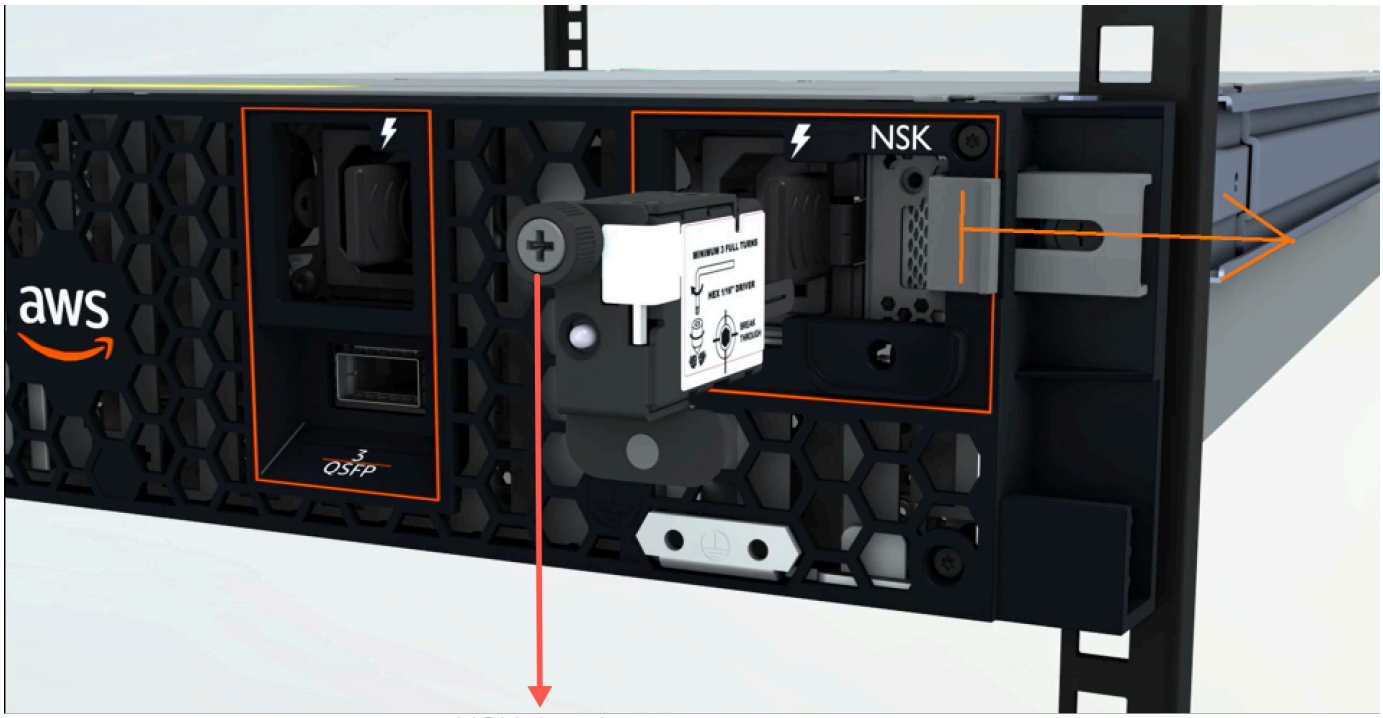


2. Stellen Sie sicher, dass die Seriennummer (SN) auf dem NSK mit der Seriennummer auf der ausziehbaren Lasche am Rahmen des NSK-Fachs auf dem Server übereinstimmt.

Die folgende Abbildung zeigt die SN-Nummer auf dem NSK und der herausziehbaren Lasche am Rahmen:

3. Setzen Sie den NSK in den Steckplatz ein.
4. Mit der Rändelschraube von Hand oder mit einem Schraubenzieher (0,7 Nm / 0,52 lb-ft) festziehen, bis es fest sitzt. Verwenden Sie kein Elektrowerkzeug, da dies zu einem zu starken Drehmoment führen und den NSK beschädigen könnte.

Die folgende Abbildung zeigt die Position der Rändelschraube.



NSK thumbscrew

Die folgende Abbildung zeigt den Schraubenziehertyp, mit dem Sie den NSK am Server befestigen können.

Einschalten

So schließen Sie den Server an die Stromversorgung an

1. Suchen Sie das Paar C13/C14-Stromkabel, das im Lieferumfang des Servers enthalten ist.
2. Schließen Sie das C14-Ende der beiden Kabel an Ihre Stromquelle an.
3. Verbinden Sie das C13-Ende der beiden Kabel mit den Anschlüssen an der Vorderseite des Servers.

Überprüfen Sie die Serverleistung

Um zu überprüfen, ob der Server mit Strom versorgt wird

1. Vergewissern Sie sich, dass Sie den Server laufen hören können.

   > **Tip**
   >
   > Der Geräuschpegel sinkt, nachdem sich der Server selbst eingerichtet hat.

2. Vergewissern Sie sich, dass die LED-Leuchten über den Netzanschlüssen leuchten.

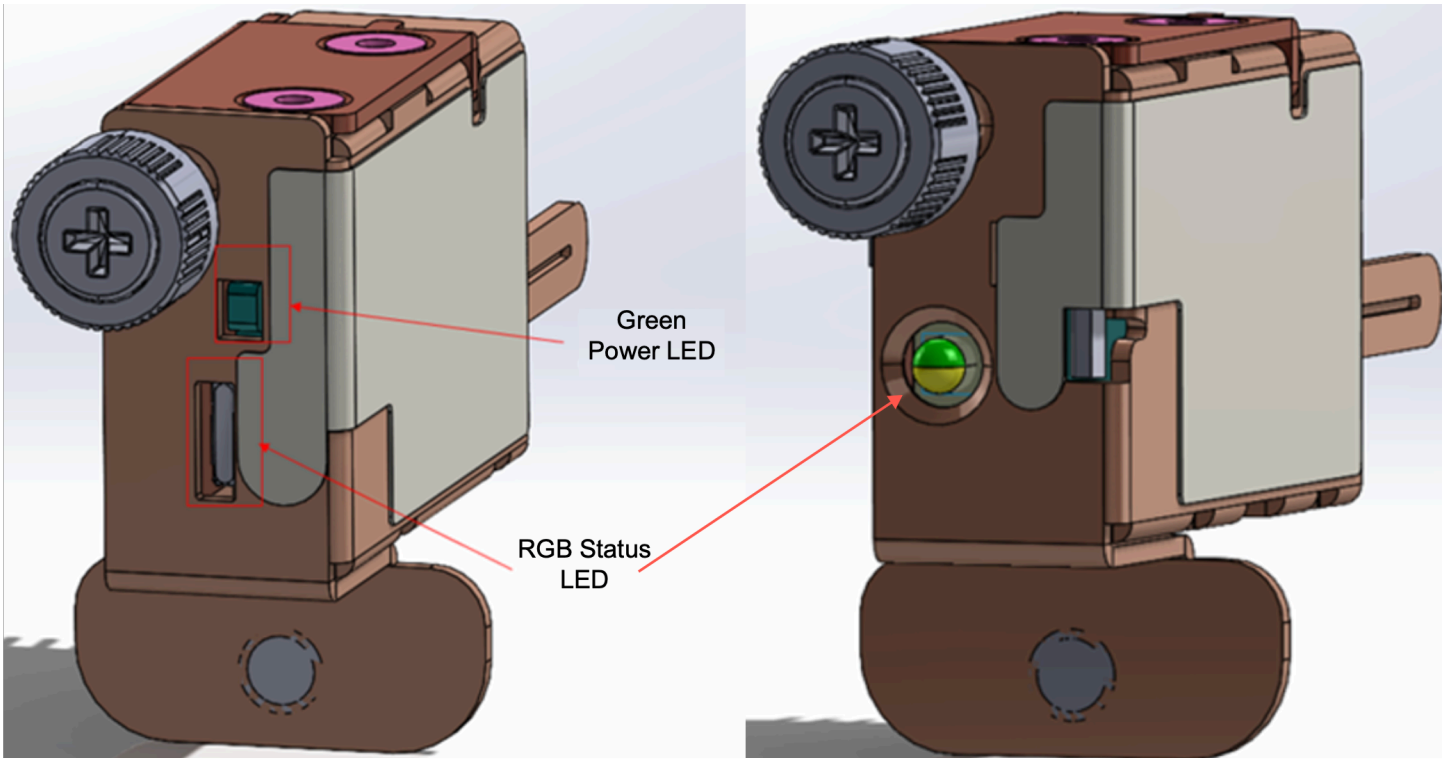
   Das folgende Bild zeigt die LED-Betriebsleuchten eines 2U-Servers

Das folgende Image zeigt die LED-Betriebsleuchten eines 1U-Servers

Überprüfen Sie die Power-LED am Atlas 3.0. NSK

AWS Outposts unterstützt zwei Versionen von NSK: Atlas 2.0 und Atlas 3.0. Beide NSK-Versionen haben eine RGB-Status-LED. Darüber hinaus verfügt der Atlas 3.0 über eine grüne Power-LED. Dieser Schritt gilt nur für den Atlas 3.0 NSK.

Das folgende Bild zeigt die Position der LEDs an den Atlas 2.0- und Atlas 3.0-NSKs:



Atlas 3.0 Atlas 2.0

Wenn Sie den Atlas 2.0 NSK haben, fahren Sie mit dem nächsten Schritt fort, Schritt 5: Netzwerk verbinden da diese Version des NSK nur über die RGB-Status-LED verfügt, die Sie überprüfen müssen, nachdem der Outpost-Server bereitgestellt und aktiviert wurde.

Wenn Sie den Atlas 3.0 NSK haben, überprüfen Sie die grüne Betriebs-LED:

- Wenn das grüne Licht leuchtet, ist der NSK korrekt mit dem Host verbunden und mit Strom versorgt. Sie können mit dem nächsten Schritt fortfahren.
- Wenn das grüne Licht aus ist, ist der NSK nicht richtig mit dem Host verbunden oder/und hat keinen Strom. Kontakt. AWS Support

Schritt 5: Netzwerk verbinden

Um die Netzwerkeinrichtung abzuschließen, verbinden Sie den Server über ein Netzwerkkabel mit Ihrem Upstream-Netzwerkgerät.

Beachten Sie die folgenden Informationen zur Verbindung mit dem Netzwerk:

- Der Server benötigt Verbindungen für zwei Arten von Datenverkehr: Datenverkehr über Service Links und Datenverkehr über lokale Netzwerkschnittstellen (LNI). In den Anweisungen im

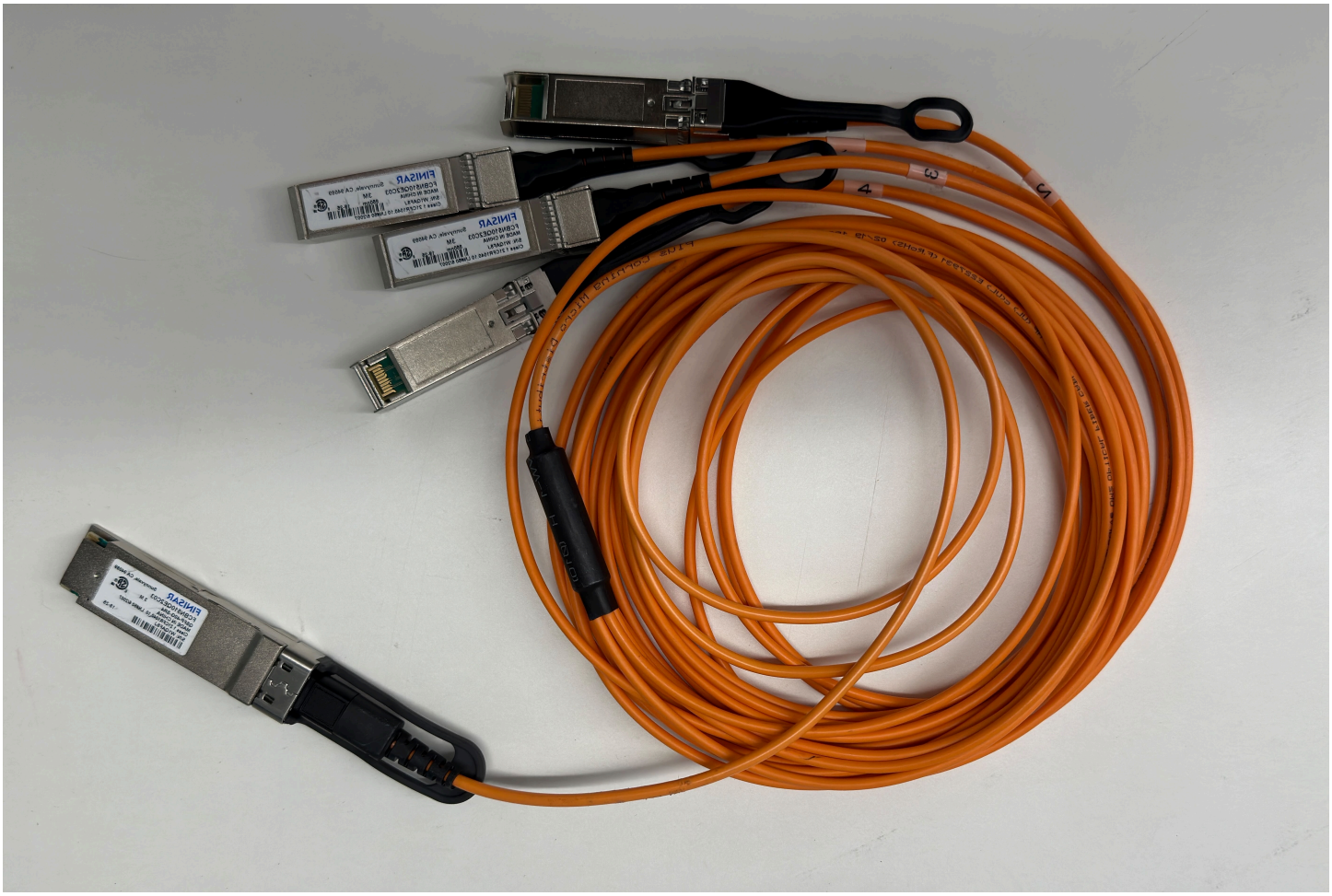
folgenden Abschnitt wird beschrieben, welche Ports auf dem Server zur Segmentierung des Datenverkehrs verwendet werden müssen. Erkundigen Sie sich bei Ihrer IT-Abteilung, welcher Port auf Ihrem Upstream-Netzwerkgerät die einzelnen Datenverkehrstypen übertragen soll.

- Stellen Sie sicher, dass der Server eine Verbindung zu Ihrem Upstream-Netzwerkgerät hergestellt hat und ihm eine IP-Adresse zugewiesen wurde. Weitere Informationen finden Sie unter Zuweisung von Server-IP-Adressen.
- Die optische Verbindung auf einem AWS Outposts Server unterstützt nur 10 Gbit/s und unterstützt keine automatische Aushandlung der Portgeschwindigkeit. Wenn der Host-Port versucht, eine Portgeschwindigkeit auszuhandeln, z. B. zwischen 10 und 25 Gbit/s, können Probleme auftreten. In solchen Fällen empfehlen wir Ihnen Folgendes:
  - Stellen Sie die Portgeschwindigkeit am Switch-Port auf 10 Gbit/s ein.
  - Arbeiten Sie mit Ihrem Switch-Anbieter zusammen, um eine statische Konfiguration zu unterstützen.

Konfigurieren des QSFP-Netzwerks

Mit dem QSFP-Breakout-Kabel verwenden Sie Breakouts, um den Datenverkehr zu segmentieren.

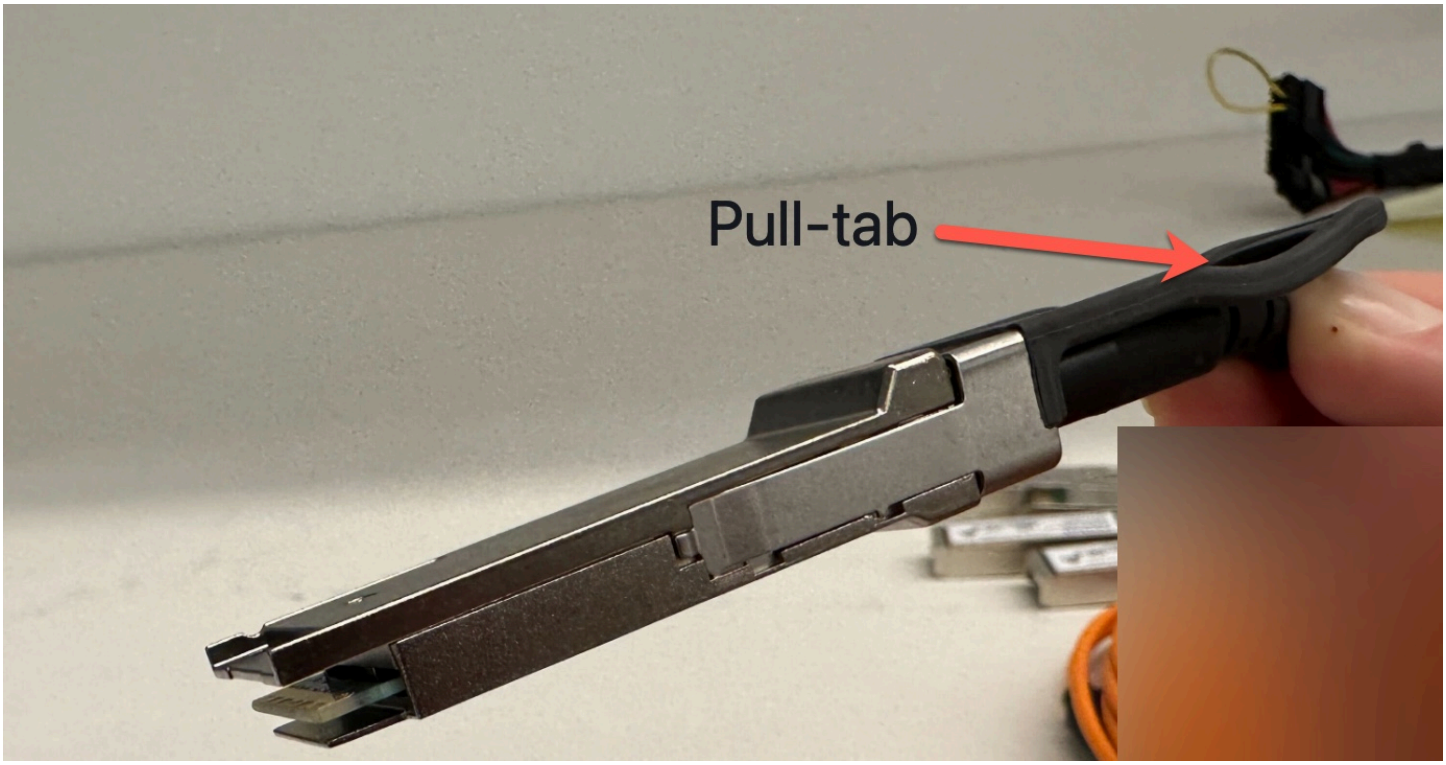
Die folgende Abbildung zeigt das QSFP-Breakout-Kabel:



> **Note**
>
> AWS Outposts Server haben neben dem QSFP-Anschluss einen physischen RJ45-Port. Dieser RJ45-Anschluss ist jedoch nicht für die Verwendung durch Kunden aktiviert. Wenn Sie eine RJ45-1GbE-Konnektivität benötigen, verwenden Sie das mitgelieferte QSFP-Kabel, um ein 10GBASE-X SFP+ mit einem 1-GbE-RJ45-Medienkonverter zu verbinden.

Ein Ende des QSFP-Kabels hat einen einzelnen Anschluss. Verbinden Sie dieses Ende mit dem Server.

Die folgende Abbildung zeigt das Ende des Kabels mit dem einzelnen Anschluss:



Am anderen Ende des QSFP-Kabels befinden sich 4 Breakout-Kabel, die mit 1 bis 4 gekennzeichnet sind. Verwenden Sie das Kabel mit der Bezeichnung 1 für den LNI-Link-Datenverkehr und das mit 2 beschriftete Kabel für den Service Link-Datenverkehr.

Die folgende Abbildung zeigt das Ende des Kabels mit den 4 Breakout-Kabeln:

So verbinden Sie den Server über das QSFP-Breakout-Kabel mit dem Netzwerk

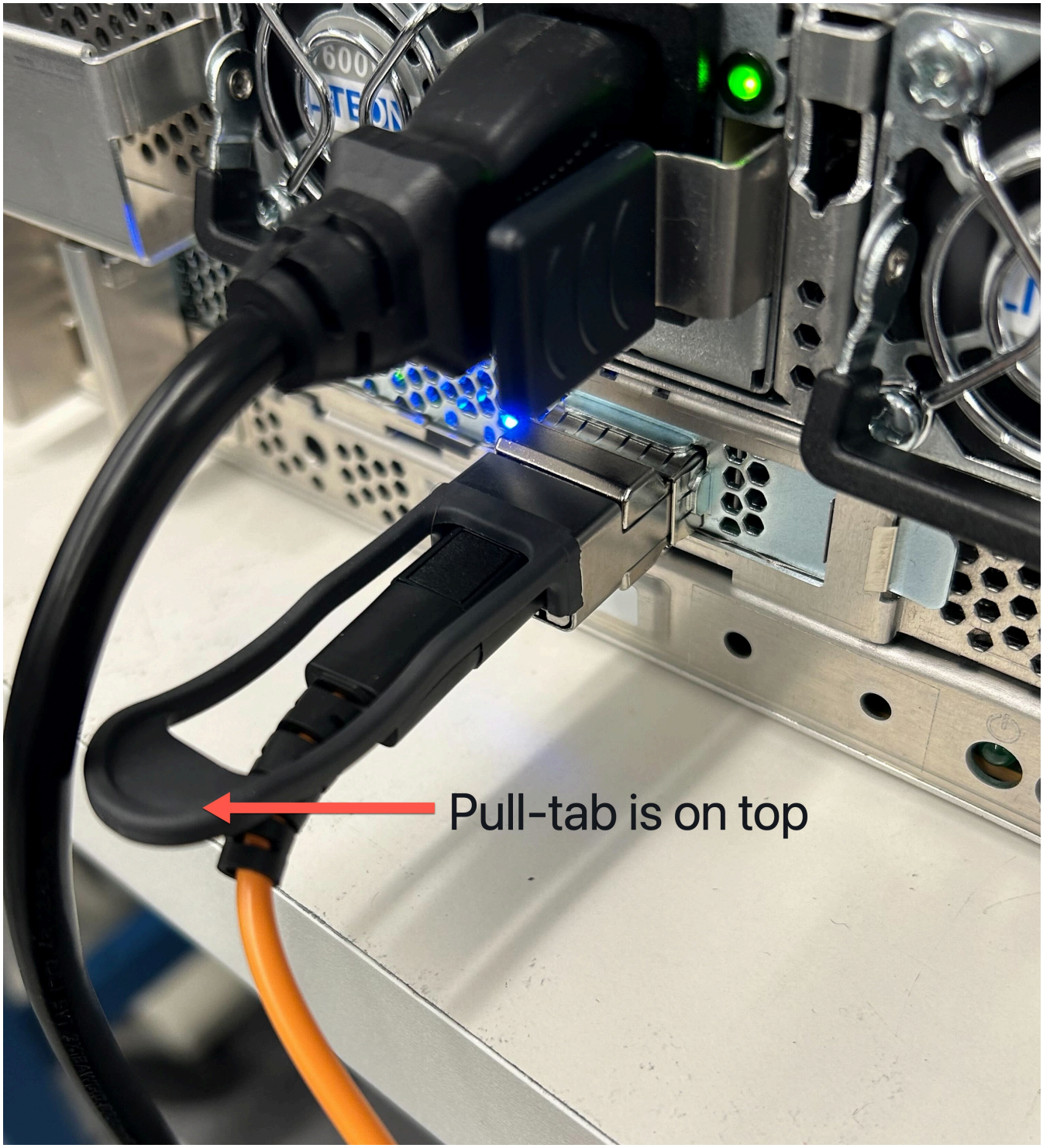
1. Suchen Sie das QSFP-Breakout-Kabel, das im Lieferumfang des Servers enthalten ist
2. Schließen Sie das eine Ende des QSFP-Breakout-Kabels an den QSFP-Port des Servers an.
    1. Suchen Sie den QSFP-Port.

        Die folgende Abbildung zeigt die Position des QSFP-Ports auf dem 2U-Server.

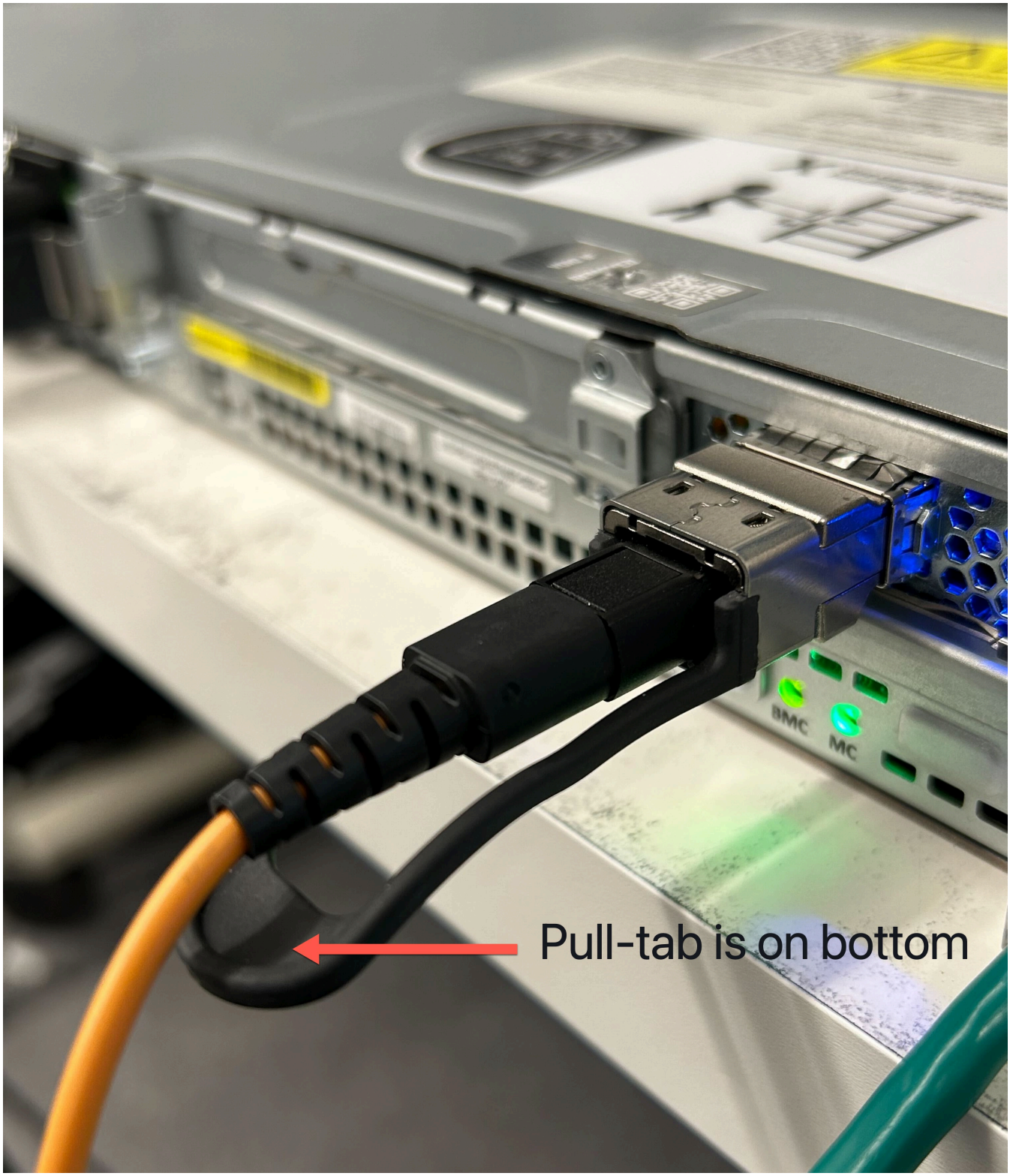
Die folgende Abbildung zeigt die Position des QSFP-Ports auf dem 1U-Server.

2. Stecken Sie den QSFP mit der Zuglasche in der richtigen Ausrichtung ein.

   Bei einem 2U-Server stecken Sie den QSFP mit der Zuglasche nach oben ein, wie in der folgenden Abbildung gezeigt.



Bei einem 1U-Server stecken Sie den QSFP mit der Zuglasche nach unten ein, wie die folgende Abbildung zeigt.



3. Vergewissern Sie sich, dass Sie ein Klicken spüren oder hören, wenn Sie die Kabel einstecken. Dies zeigt an, dass Sie die Kabel richtig eingesteckt haben.

3. Verbinden Sie die Breakouts 1 und 2 des QSFP-Kabels mit dem Upstream-Netzwerkgerät.

> **Important**
>
> Damit ein Outpost Server funktioniert, sind beide der folgenden Kabel erforderlich.
>
> - Verwenden Sie das mit 1 beschriftete Kabel für LNI-Link-Datenverkehr.
> - Verwenden Sie das mit 2 beschriftete Kabel für Service Link-Datenverkehr.

Schritt 6: Autorisieren des Servers

Um den Server zu autorisieren, müssen Sie Ihren Laptop über ein USB-Kabel mit dem Server verbinden und dann ein befehlsbasiertes serielles Protokoll verwenden, um die Verbindung zu testen und den Server zu autorisieren. Zusätzlich zu den IAM-Anmeldeinformationen benötigen Sie ein USB-Kabel, einen Laptop und serielle Terminalsoftware wie PuTTY oder screen, um diese Schritte auszuführen.

Wenn Sie ein Android-Telefon oder -Tablet mit einem USB-C- oder Micro-USB-Anschluss mit USB On The Go-Unterstützung (OTG) haben, können Sie alternativ die Outposts Server Activator-App verwenden, um Sie durch den Serverautorisierungsprozess zu führen. Sie können die App von Google Play herunterladen

Beachten Sie die folgenden Informationen zur Stromversorgung des Servers:

- Um den Server zu autorisieren, benötigen Sie oder die Partei, die den Server installiert, IAM-Anmeldeinformationen in dem Ordner AWS-Konto , der den Outpost enthält. Weitere Informationen finden Sie unter the section called “Schritt 1: Erteilen von Berechtigungen”.
- Sie müssen sich nicht mit den IAM-Anmeldeinformationen authentifizieren, um Ihre Verbindung zu testen.
- Erwägen Sie, die Verbindung zu testen, bevor Sie den Exportbefehl verwenden, um IAM-Anmeldeinformationen als Umgebungsvariablen festzulegen.
- Zum Schutz Ihres Kontos speichert das Outpost Configuration Tool niemals Ihre IAM Anmeldeinformationen.
- Wenn Sie Ihren Laptop mit dem Server verbinden möchten, stecken Sie das USB-Kabel immer zuerst in Ihren Laptop und dann in den Server.

Aufgaben

Verbinden Sie Ihren Laptop mit dem Server

Schließen Sie das USB-Kabel zuerst an Ihren Laptop und dann an den Server an. Der Server enthält einen USB-Chip, der eine virtuelle serielle Schnittstelle auf dem Laptop zur Verfügung stellt. Sie können diese virtuelle serielle Schnittstelle verwenden, um mit der Emulationssoftware für serielle Terminals eine Verbindung zum Server herzustellen. Diese virtuelle serielle Schnittstelle können Sie nur dazu verwenden, um Befehle des Outpost Configuration Tools auszuführen.

So verbinden Sie den Laptop mit dem Server

Stecken Sie das USB-Kabel zuerst in Ihren Laptop und dann in den Server.

> **Note**
>
> Der USB-Chip benötigt Treiber, um die virtuelle serielle Schnittstelle zu erstellen. Ihr Betriebssystem sollte die erforderlichen Treiber automatisch installieren, sofern sie nicht bereits vorhanden sind. Informationen zum Herunterladen und Installieren der Treiber finden Sie in den Installationsanleitungen von FTDI.

Eine serielle Verbindung zum Server herstellen

Dieser Abschnitt enthält Anweisungen zur Verwendung gängiger serieller Terminalprogramme. Sie müssen diese Programme jedoch nicht verwenden. Verwenden Sie das von Ihnen bevorzugte serielle Terminalprogramm mit einer Verbindungsgeschwindigkeit von `115200` Baud.

Beispiele

Serielle Verbindung unter Windows

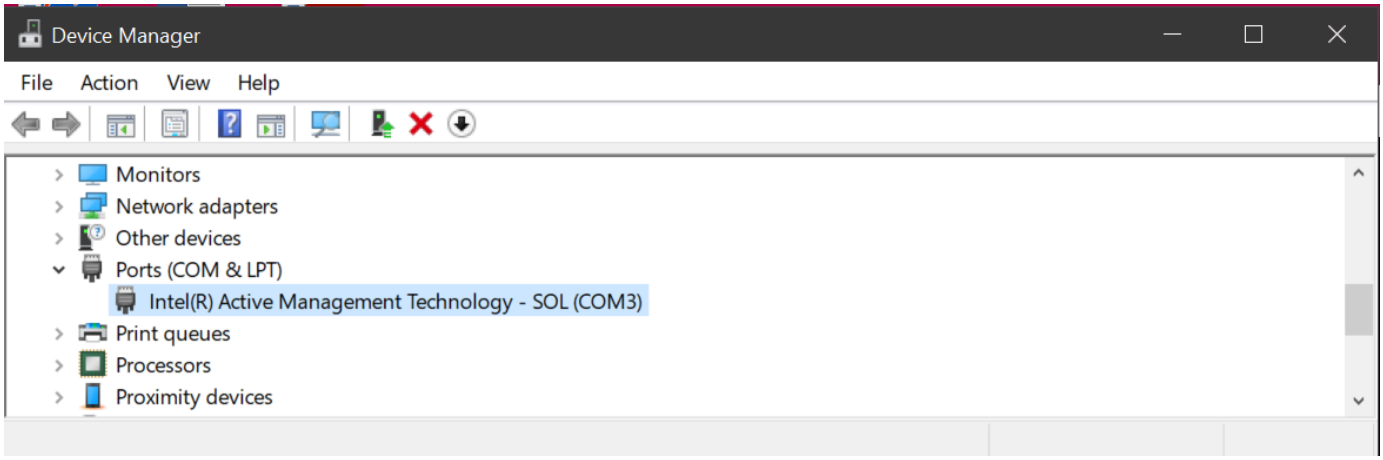
Die folgenden Anweisungen beziehen sich auf PuTTY unter Windows. PuTTY ist kostenlos, aber Sie müssen es möglicherweise herunterladen.

PuTTY herunterladen

Laden Sie PuTTY über die Downloadseite für PuTTY herunter und führen Sie die Installation durch.

So erstellen Sie ein serielles Terminal unter Windows mit PuTTY

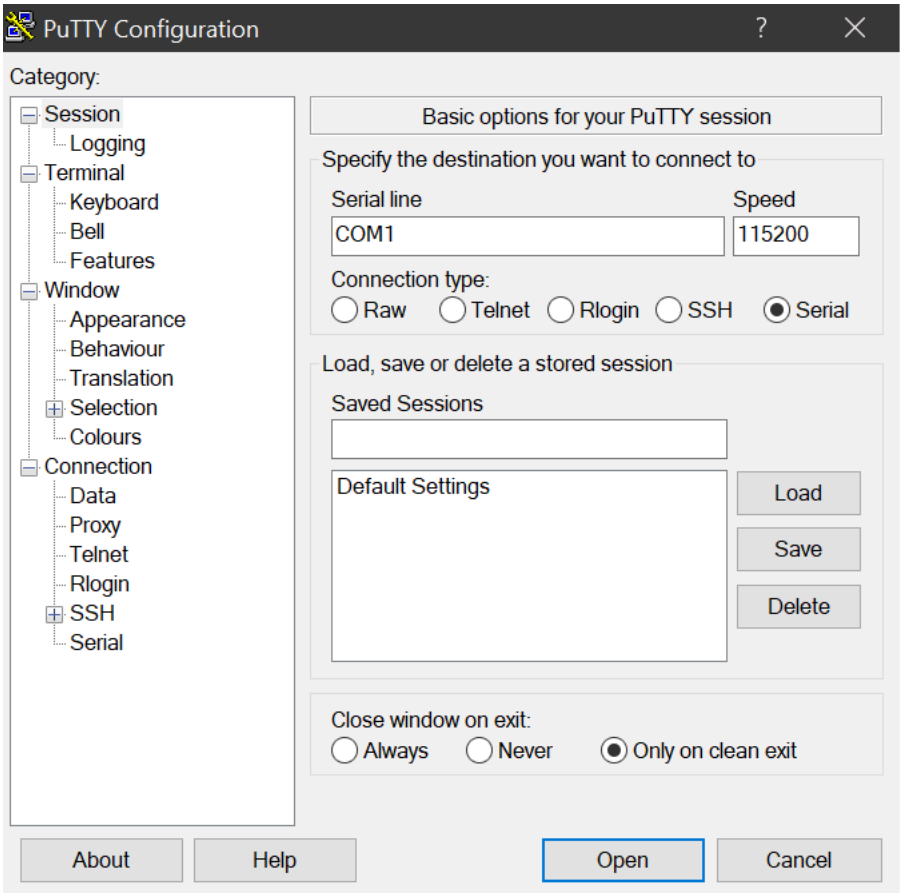
1. Stecken Sie das USB-Kabel zuerst in Ihren Windows-Laptop und dann in den Server.
2. Klicken Sie auf dem Desktop mit der rechten Maustaste auf Start und wählen Sie Geräte-Manager.
3. Erweitern Sie im Geräte-Manager die Option Anschlüsse (COM und LPT), um den COM-Port für die serielle USB-Verbindung zu ermitteln. Sie werden einen Knoten mit dem Namen USB Serial Port (COM *#*) sehen. Der Wert für den COM-Port hängt von Ihrer Hardware ab.



4. Wählen Sie in PuTTY unter Sitzung die Option Seriell als Verbindungstyp aus, und geben Sie dann die folgenden Informationen ein:

   - Geben Sie unter Serielle Leitung den COM *#-Port* aus dem Geräte-Manager ein.
   - Geben Sie unter Geschwindigkeit Folgendes ein: `115200`

   Die folgende Abbildung zeigt ein Beispiel auf der Seite PuTTY-Konfiguration:



5. Klicken Sie auf Open.

   Ein leeres Konsolenfenster wird angezeigt. Es kann zwischen 1 und 2 Minuten dauern, bis eine der folgenden Optionen angezeigt wird:

   - `Please wait for the system to stabilize. This can take up to 900 seconds, so far x seconds have elapsed on this boot.`
   - Die `Outpost>`-Eingabeaufforderung.

Serielle Verbindung unter macOS

Die folgenden Anweisungen gelten für screen unter macOS. screen ist im Betriebssystem enthalten.

So erstellen Sie ein serielles Terminal unter macOS mit screen

1. Stecken Sie das USB-Kabel zuerst in Ihren Mac-Laptop und dann in den Server.
2. Listen Sie in Terminal `/dev` mit einem `*usb*`-Filter für die Ausgabe auf, um die virtuelle serielle Schnittstelle zu finden.

```
ls -ltr /dev/*usb*
```

Das serielle Gerät wird angezeigt als `tty`. Betrachten Sie dazu die folgende Beispielausgabe des vorherigen list-Befehls:

```
ls -ltr /dev/*usb*
crw-rw-rw-  1 root  wheel   21,   3 Feb  8 15:48 /dev/cu.usbserial-EXAMPLE1
crw-rw-rw-  1 root  wheel   21,   2 Feb  9 08:56 /dev/tty.usbserial-EXAMPLE1
```

3. Verwenden Sie in Terminal screen zusammen mit dem seriellen Gerät und einer Baudrate der seriellen Verbindung die serielle Verbindung, um die serielle Verbindung einzurichten. Ersetzen Sie im folgenden Befehl *EXAMPLE1* durch den Wert auf Ihrem Laptop.

```
screen /dev/tty.usbserial-EXAMPLE1 115200
```

Ein leeres Konsolenfenster wird angezeigt. Es kann zwischen 1 und 2 Minuten dauern, bis eine der folgenden Optionen angezeigt wird:

- `Please wait for the system to stabilize. This can take up to 900 seconds, so far x seconds have elapsed on this boot.`
- Die `Outpost>`-Eingabeaufforderung.

Verbindung testen

In diesem Abschnitt wird beschrieben, wie Sie mit dem Outpost Configuration Tool die Verbindung testen. Sie benötigen keine IAM-Anmeldeinformationen, um die Verbindung zu testen. Ihre Verbindung muss in der Lage sein, DNS aufzulösen, um auf die AWS-Region zugreifen zu können.

1. Testen Sie die Links und sammeln Sie Informationen über die Verbindung
2. Testen Sie den DNS-Resolver
3. Testen Sie den Zugriff auf AWS-Region

So testen Sie die Links

1. Stecken Sie das USB-Kabel zuerst in Ihren Laptop und dann in den Server.

2. Verwenden Sie ein serielles Terminalprogramm wie PuTTY oder screen, um eine Verbindung zum Server herzustellen. Weitere Informationen finden Sie unter the section called “Eine serielle Verbindung zum Server herstellen”.
3. Drücken Sie Enter, um die Eingabeaufforderung des Outpost Configuration Tools aufzurufen.

```
Outpost>
```

> **Note**
>
> Wenn Sie nach dem Einschalten ein rotes Licht im Gehäuse des Servers auf der linken Seite dauerhaft leuchten sehen und keine Verbindung zum Outpost Configuration Tool herstellen können, müssen Sie den Server möglicherweise ausschalten und das System entladen, um fortzufahren. Um den Server zu entladen, trennen Sie alle Netzwerk- und Stromkabel, warten Sie fünf Minuten, schalten Sie das Gerät wieder ein und stellen Sie die Netzwerkverbindung wieder her.

4. Verwenden Sie describe-links, um Informationen über die Netzwerkverbindungen auf dem Server zu erhalten. Outpost-Server müssen über einen Service Link und einen LNI-Link (Local Network Interface) verfügen.

```
Outpost>describe-links
---
service_link_connected: True
local_link_connected: False
links:
-
  name: local_link
  connected: False
  mac: 00:00:00:00:00:00
-
  name: service_link
  connected: True
  mac: 0A:DC:FE:D7:8E:1F
checksum: 0x46FDC542
```

Wenn Sie für eine der beiden Verbindungen `connected: False` erhalten, sollten Sie die Netzwerkverbindung auf der Hardware überprüfen.

5. Verwenden Sie describe-ip, um den IP-Zuweisungsstatus und die Konfiguration des Service-Links zurückzugeben.

```
Outpost>describe-ip
---
links:
-
  name: service_link
  configured: True
  ip: 192.168.0.0
  netmask: 255.255.0.0
  gateway: 192.168.1.1
  dns: [ "192.168.1.1" ]
  ntp: [ ]
checksum: 0x8411B47C
```

Der NTP-Wert fehlt möglicherweise, da NTP in einem DHCP-Optionssatz optional ist. Es sollten keine weiteren Werte fehlen.

So testen Sie DNS

1. Stecken Sie das USB-Kabel zuerst in Ihren Laptop und dann in den Server.
2. Verwenden Sie ein serielles Terminalprogramm wie PuTTY oder screen, um eine Verbindung zum Server herzustellen. Weitere Informationen finden Sie unter the section called “Eine serielle Verbindung zum Server herstellen”.
3. Drücken Sie Enter, um die Eingabeaufforderung des Outpost Configuration Tools aufzurufen.

```
Outpost>
```

> **Note**
>
> Wenn Sie nach dem Einschalten ein rotes Licht im Gehäuse des Servers auf der linken Seite dauerhaft leuchten sehen und keine Verbindung zum Outpost Configuration Tool herstellen können, müssen Sie den Server möglicherweise ausschalten und das System entladen, um fortzufahren. Um den Server zu entladen, trennen Sie alle Netzwerk- und Stromkabel, warten Sie fünf Minuten, schalten Sie das Gerät wieder ein und stellen Sie die Netzwerkverbindung wieder her.

4. Verwenden Sie export, um die übergeordnete Region des Outpost-Servers als Wert für AWS_DEFAULT_REGION einzugeben.

   AWS_DEFAULT_REGION=*Region*

   ```
   Outpost>export AWS_DEFAULT_REGION=us-west-2

   result: OK
   checksum: 0xB2A945RE
   ```

   - Fügen Sie vor oder nach dem Gleichheitszeichen (=) kein Leerzeichen ein.
   - Es werden keine Umgebungswerte gespeichert. Sie müssen AWS-Region jedes Mal exportieren, wenn Sie das Outpost Configuration Tool ausführen.
   - Wenn Sie einen Drittanbieter für die Installation des Servers verwenden, müssen Sie dem Drittanbieter die übergeordnete Region angeben.

5. Verwenden Sie describe-resolve, um festzustellen, ob der Outpost-Server einen DNS-Resolver erreichen und die IP-Adresse des Outpost-Konfigurationsendpunkts in der Region auflösen kann. Erfordert mindestens einen Link mit einer IP-Konfiguration.

   ```
   Outpost>describe-resolve
   ---
   dns_responding: True
   dns_resolving: True
   dns: [ "198.xx.xxx.xx", "198.xx.xxx.xx" ]
   query: outposts.us-west-2.amazonaws.com
   records: [ "18.xxx.xx.xxx", "44.xxx.xxx.xxx", "44.xxx.xxx.xxx" ]
   checksum: 0xB6A961CE
   ```

Um den Zugriff auf zu testen AWS-Regionen

1. Stecken Sie das USB-Kabel zuerst in Ihren Laptop und dann in den Server.
2. Verwenden Sie ein serielles Terminalprogramm wie PuTTY oder screen, um eine Verbindung zum Server herzustellen. Weitere Informationen finden Sie unter the section called “Eine serielle Verbindung zum Server herstellen”.
3. Drücken Sie Enter, um die Eingabeaufforderung des Outpost Configuration Tools aufzurufen.

   ```
   Outpost>
   ```

> **Note**
>
> Wenn Sie nach dem Einschalten ein rotes Licht im Gehäuse des Servers auf der linken Seite dauerhaft leuchten sehen und keine Verbindung zum Outpost Configuration Tool herstellen können, müssen Sie den Server möglicherweise ausschalten und das System entladen, um fortzufahren. Um den Server zu entladen, trennen Sie alle Netzwerk- und Stromkabel, warten Sie fünf Minuten, schalten Sie das Gerät wieder ein und stellen Sie die Netzwerkverbindung wieder her.

4. Verwenden Sie export, um die übergeordnete Region des Outpost-Servers als Wert für `AWS_DEFAULT_REGION` einzugeben.

   `AWS_DEFAULT_REGION=`*`Region`*

   ```
   Outpost>export AWS_DEFAULT_REGION=us-west-2

   result: OK
   checksum: 0xB2A945RE
   ```

   - Fügen Sie vor oder nach dem Gleichheitszeichen (=) kein Leerzeichen ein.
   - Es werden keine Umgebungswerte gespeichert. Sie müssen AWS-Region jedes Mal exportieren, wenn Sie das Outpost Configuration Tool ausführen.
   - Wenn Sie einen Drittanbieter für die Installation des Servers verwenden, müssen Sie dem Drittanbieter die übergeordnete Region angeben.

5. Verwenden Sie describe-reachability, um festzustellen, ob der Outpost-Server den Outpost-Konfigurationsendpunkt in der Region erreichen kann. Erfordert eine funktionierende DNS-Konfiguration, die Sie mithilfe von describe-resolve ermitteln können.

   ```
   Outpost>describe-reachability
   ---
   is_reachable: True
   src_ip: 10.0.0.0
   dst_ip: 54.xx.x.xx
   dst_port: xxx
   checksum: 0xCB506615
   ```

   - `is_reachable` gibt das Ergebnis des Tests an

- `src_ip` ist die IP-Adresse des Servers
- `dst_ip` ist die IP-Adresse des Outpost-Konfigurationsendpunkts in der Region
- `dst_port` ist der Port, über den sich der Server mit `dst_ip` verbindet

Den Server autorisieren

In diesem Abschnitt wird beschrieben, wie Sie das Outpost Configuration Tool und die IAM-Anmeldeinformationen des AWS -Kontos verwenden, das den Outpost enthält, um den Server zu autorisieren.

So autorisieren Sie den Server

1. Stecken Sie das USB-Kabel zuerst in Ihren Laptop und dann in den Server.
2. Verwenden Sie ein serielles Terminalprogramm wie PuTTY oder screen, um eine Verbindung zum Server herzustellen. Weitere Informationen finden Sie unter the section called “Eine serielle Verbindung zum Server herstellen”.
3. Drücken Sie Enter, um die Eingabeaufforderung des Outpost Configuration Tools aufzurufen.

   ```
   Outpost>
   ```

   > **Note**
   >
   > Wenn Sie nach dem Einschalten ein rotes Licht im Gehäuse des Servers auf der linken Seite dauerhaft leuchten sehen und keine Verbindung zum Outpost Configuration Tool herstellen können, müssen Sie den Server möglicherweise ausschalten und das System entladen, um fortzufahren. Um den Server zu entladen, trennen Sie alle Netzwerk- und Stromkabel, warten Sie fünf Minuten, schalten Sie das Gerät wieder ein und stellen Sie die Netzwerkverbindung wieder her.

4. Verwenden Sie export, um Ihre IAM Anmeldeinformationen in das Outpost Configuration Tool einzugeben. Wenn Sie einen Drittanbieter für die Installation des Servers verwenden, müssen Sie dem Drittanbieter die IAM-Anmeldeinformationen angeben.

   Zur Authentifizierung müssen Sie die folgenden vier Variablen exportieren. Exportieren Sie jeweils eine Variable. Fügen Sie vor oder nach dem Gleichheitszeichen (=) kein Leerzeichen ein.

   - `AWS_ACCESS_KEY_ID=`*`Zugriffsschlüssel-ID`*

- `AWS_SECRET_ACCESS_KEY=`*`Geheimer Zugriffsschlüssel`*
- `AWS_SESSION_TOKEN=`*`Sitzungstoken`*
  - Verwenden Sie den AWS CLI `GetSessionToken` Befehl, um das abzurufen. `AWS_SESSION_TOKEN` Weitere Informationen finden Sie unter get-session-token in der AWS CLI -Befehlsreferenz.

    > **Note**
    >
    > Sie müssen die AWSOutpostsAuthorizeServerPolicyan Ihre IAM-Rolle angehängt haben, um die `AWS_SESSION_TOKEN` zu erhalten.

  - Informationen zur AWS CLI Installation von finden Sie unter Installation oder Aktualisierung der neuesten Version der AWS-CLI im AWS CLI Benutzerhandbuch für Version 2.
- `AWS_DEFAULT_REGION=`*`Region`*

  Verwenden Sie die übergeordnete Region des Outpost-Servers als Wert für `AWS_DEFAULT_REGION`. Wenn Sie einen Drittanbieter für die Installation des Servers verwenden, müssen Sie dem Drittanbieter die übergeordnete Region angeben.

Die Ausgabe in den folgenden Beispielen zeigt erfolgreiche Exporte.

```
Outpost>export AWS_ACCESS_KEY_ID=AKIAIOSFODNN7EXAMPLE

result: OK
checksum: example-checksum
```

```
Outpost>export AWS_SECRET_ACCESS_KEY=wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY

result: OK
checksum: example-checksum
```

```
Outpost>export AWS_SESSION_TOKEN=MIICiTCCAfICCQD6m7oRw0uXOjANBgk
VVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6
b24xFDASBgNVBAsTC0lBTSBDb25zb2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAd
BgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5jb20wHhcNMTEwNDI1MjA0NTIxWhcN
MTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYD
VQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAsTC0lBTSBDb25z
b2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEWEG5vb25lQGFt
```

```
YXpvbi5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ
21uUSfwfEvySWtC2XADZ4nB+BLYgVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T
rDHudUZg3qX4waLG5M43q7Wgc/MbQITxOUSQv7c7ugFFDzQGBzZswY6786m86gpE
Ibb3OhjZnzcvQAaRHhdlQWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4
nUhVVxYUntneD9+h8Mg9q6q+auNKyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0Fkb
FFBjvSfpJIlJ00zbhNYS5f6GuoEDmFJl0ZxBHjJnyp378OD8uTs7fLvjx79LjSTb
NYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE=

result: OK
checksum: example-checksum
```

```
Outpost>export AWS_DEFAULT_REGION=us-west-2

result: OK
checksum: example-checksum
```

5. Verwenden Sie start-connection, um eine sichere Verbindung zur Region herzustellen.

   Die Ausgabe im folgenden Beispiel zeigt, dass eine Verbindung erfolgreich gestartet wurde.

```
Outpost>start-connection

is_started: True
asset_id: example-asset-id
connection_id: example-connection-id
timestamp: 2021-10-01T23:30:26Z
checksum: example-checksum
```

6. Warten Sie etwa 5 Minuten.
7. Verwenden Sie get-connection, um zu prüfen, ob die Verbindung zur Region hergestellt wurde.

   Die Ausgabe im folgenden Beispiel zeigt eine erfolgreiche Verbindung.

```
Outpost>get-connection


---
keys_exchanged: True
connection_established: True
exchange_active: False
primary_peer: xx.xx.xx.xx:xxx
primary_status: success
```

```
primary_connection_id: a1b2c3d4567890abcdefEXAMPLE11111
primary_handshake_age: 1111111111
primary_server_public_key: AKIAIOSFODNN7EXAMPLE
primary_client_public_key: AKIAI44QH8DHBEXAMPLE
primary_server_endpoint: xx.xx.xx.xx:xxx
secondary_peer: xx.xxx.xx.xxx:xxx
secondary_status: success
secondary_connection_id: a1b2c3d4567890abcdefEXAMPLE22222
secondary_handshake_age: 1111111111
secondary_server_public_key: wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY
secondary_client_public_key: je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY
secondary_server_endpoint: xx.xxx.xx.xxx:xxx
timestamp: 2023-02-22T22:19:28Z
checksum: 0x83FA0123
```

Nachdem `keys_exchanged` und `connection_established` sich auf `True` geändert haben, wird der Outpost-Server automatisch bereitgestellt und auf die neueste Software und Konfiguration aktualisiert.

> **Note**
>
> Beachten Sie die folgenden Hinweise zum Bereitstellungsprozess:
>
> - Nach Abschluss der Aktivierung kann es bis zu 10 Stunden dauern, bis Ihr Outpost-Server einsatzbereit ist.
> - Während dieses Vorgangs müssen die Stromversorgung und das Netzwerk des Outpost-Servers angeschlossen und stabil bleiben.
> - Es ist normal, dass der Service Link während dieses Vorgangs schwankt.
> - Wenn `exchange_active` `True` ist, wird die Verbindung immer noch hergestellt. Versuchen Sie es in 5 Minuten erneut.
> - Wenn `keys_exchanged` oder `connection_established` `False` ist, und wenn `exchange_active` `True` ist, wird die Verbindung immer noch hergestellt. Versuchen Sie es in 5 Minuten erneut.
> - Wenn `keys_exchanged` oder `connection_established` auch nach 1 Stunde noch `False` ist, wenden Sie sich an AWS Support -Center.
> - Wenn die Meldung `primary_status: No such asset id found.` angezeigt wird, bestätigen Sie Folgendes:
>   - Sie haben die richtige Region angegeben.

- Sie verwenden dasselbe Konto wie das Konto, mit dem Sie den Outpost-Server bestellt haben.

  Wenn die Region korrekt ist und Sie dasselbe Konto verwenden, mit dem Sie den Outpost-Server bestellt haben, wenden Sie sich an AWS Support Center.

- Das `LifeCycleStatus`-Attribut des Outposts wechselt von `Provisioning` zu `Active`. Sie erhalten dann eine E-Mail, in der Sie darüber informiert werden, dass Ihr Outpost-Server bereitgestellt und aktiviert ist.
- Sie müssen den Outposts-Server nicht erneut autorisieren, nachdem der Outposts-Server aktiviert wurde.

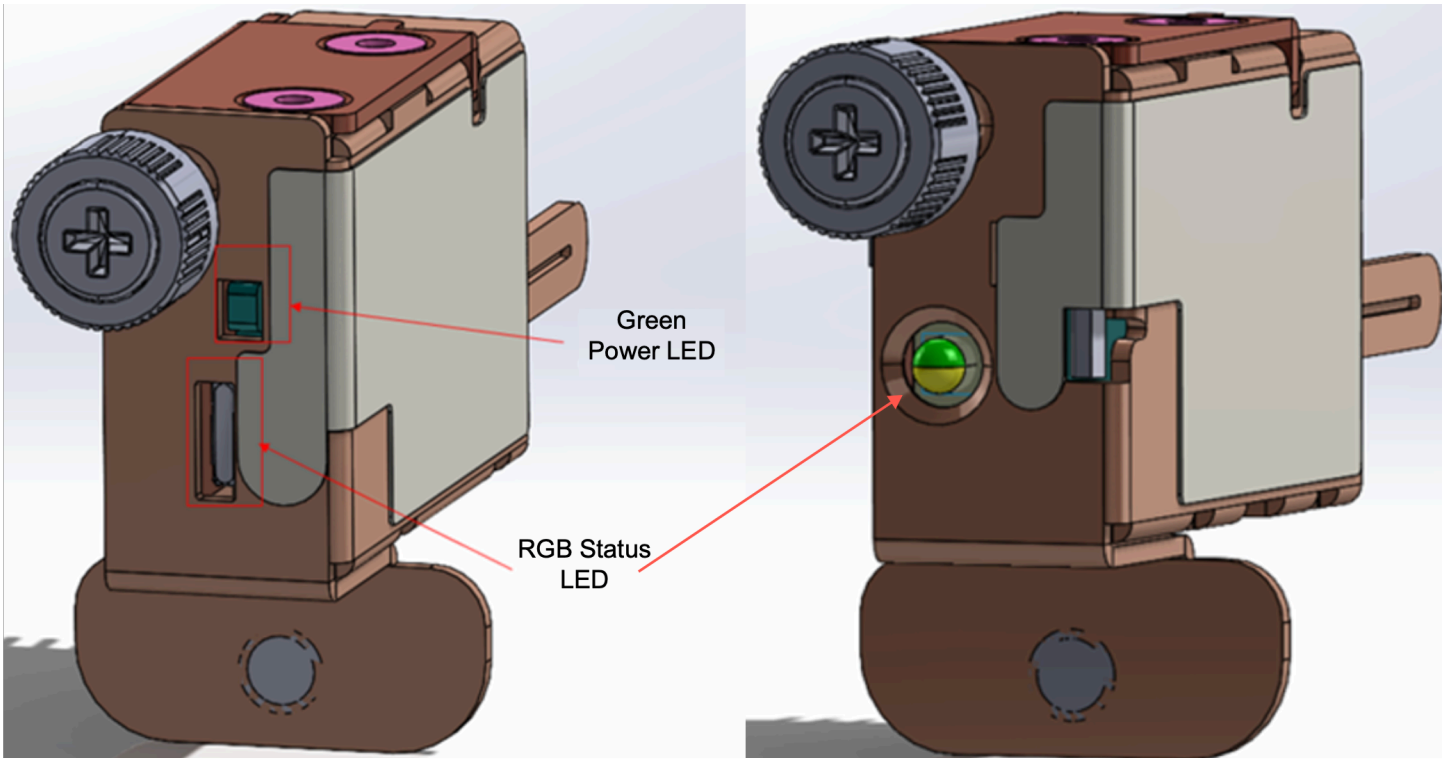
8. Nachdem Sie eine erfolgreiche Verbindung hergestellt haben, können Sie Ihren Laptop vom Server trennen.

Überprüfen Sie die NSK-LEDs

Überprüfen Sie nach Abschluss des Bereitstellungsvorgangs die NSK-LEDs.

AWS Outposts unterstützt zwei Versionen von NSK: Atlas 2.0 und Atlas 3.0. Beide NSK-Versionen haben eine RGB-Status-LED. Darüber hinaus verfügt der Atlas 3.0 über eine grüne Power-LED.

Das folgende Bild zeigt die Position der LEDs auf dem Atlas 2.0 und dem Atlas 3.0:



Atlas 3.0 Atlas 2.0

Um die Status- und Power-LEDs am NSK zu überprüfen

1. Überprüfen Sie die Farbe der RGB-Status-LED. Wenn die Farbe grün ist, ist der NSK fehlerfrei. Wenn die Farbe nicht grün ist, wenden Sie sich an AWS Support.
2. Wenn Sie einen Atlas 3.0 NSK haben, überprüfen Sie die grüne Power-LED. Wenn das grüne Licht leuchtet, ist der NSK korrekt mit dem Host verbunden und mit Strom versorgt. Wenn das grüne Licht nicht leuchtet, wenden Sie sich an AWS Support.

Befehlsreferenz für das Outpost Configuration Tool

Das Outpost Configuration Tool bietet die folgenden Befehle.

Befehle

- Export
- Echo
- Links beschreiben
- IP beschreiben
- Auflösung beschreiben

- Erreichbarkeit beschreiben
- Verbindung starten
- Verbindung herstellen

Export

Export

Verwenden Sie export, um IAM-Anmeldeinformationen als Umgebungsvariablen festzulegen.

Syntax

```
Outpost>export variable=value
```

export verwendet die Anweisung zur Variablenzuweisung.

Sie müssen das folgende Format verwenden: *variable*=*value*.

Zur Authentifizierung müssen Sie die folgenden vier Variablen exportieren. Exportieren Sie jeweils eine Variable. Fügen Sie vor oder nach dem Gleichheitszeichen (=) kein Leerzeichen ein.

- AWS_ACCESS_KEY_ID=*Zugriffsschlüssel-ID*
- AWS_SECRET_ACCESS_KEY=*Geheimer Zugriffsschlüssel*
- AWS_SESSION_TOKEN=*Sitzungstoken*
- AWS_DEFAULT_REGION=*Region*

  Verwenden Sie die übergeordnete Region des Outpost-Servers als Wert für AWS_DEFAULT_REGION.

Example : erfolgreiche Importe von Anmeldeinformationen

```
Outpost>export AWS_ACCESS_KEY_ID=AKIAIOSFODNN7EXAMPLE

result: OK
checksum: example-checksum
```

```
Outpost>export AWS_SECRET_ACCESS_KEY=wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY

result: OK
```

```
checksum: example-checksum
```

```
Outpost>export AWS_SESSION_TOKEN=MIICiTCCAfICCQD6m7oRw0uXOjANBgk
VVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6
b24xFDASBgNVBAsTC0lBTSBDb25zb2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAd
BgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5jb20wHhcNMTEwNDI1MjA0NTIxWhcN
MTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYD
VQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAsTC0lBTSBDb25z
b2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEWEG5vb25lQGFt
YXpvbi5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ
21uUSfwfEvySWtC2XADZ4nB+BLYgVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T
rDHudUZg3qX4waLG5M43q7Wgc/MbQITxOUSQv7c7ugFFDzQGBzZswY6786m86gpE
Ibb3OhjZnzcvQAaRHhdlQWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4
nUhVVxYUntneD9+h8Mg9q6q+auNKyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0Fkb
FFBjvSfpJIlJ00zbhNYS5f6GuoEDmFJl0ZxBHjJnyp378OD8uTs7fLvjx79LjSTb
NYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE=

result: OK
checksum: example-checksum
```

```
Outpost>export AWS_DEFAULT_REGION=us-west-2

result: OK
checksum: example-checksum
```

Echo

echo

Verwenden Sie echo, um den Wert anzuzeigen, den Sie mit dem export-Befehl für eine Variable festgelegt haben.

Syntax

```
Outpost>echo $variable-name
```

Der *Variable-Name* kann einer der folgenden sein:

- AWS_ACCESS_KEY_ID
- AWS_SECRET_ACCESS_KEY
- AWS_SESSION_TOKEN

- AWS_DEFAULT_REGION

Example : Erfolg

```
Outpost>export AWS_DEFAULT_REGION=us-west-2

result: OK
checksum: example-checksum

---

Outpost>echo $AWS_DEFAULT_REGION

variable name: AWS_DEFAULT_REGION
variable value: us-west-2
checksum: example-checksum
```

Example : Fehler, weil der Variablenwert nicht mit dem export-Befehl festgelegt wurde

```
Outpost> echo $AWS_ACCESS_KEY_ID

error_type: execution_error
error_attributes:
  AWS_ACCESS_KEY_ID: no value set
error_message: No value set for AWS_ACCESS_KEY_ID using export.
checksum: example-checksum
```

Example : Fehler, weil der Variablenname nicht gültig ist

```
Oupost>echo $foo

error_type: invalid_argument
error_attributes:
  foo: invalid variable name
error_message: Variables can only be AWS credentials.
checksum: example-checksum
```

Example : Fehler aufgrund eines Syntaxproblems

```
Outpost>echo AWS_SECRET_ACCESS_KEY
```

```
error_type: invalid_argument
error_attributes:
  AWS_SECRET_ACCESS_KEY: not a variable
error_message: Expecting $ before variable name.
checksum: example-checksum
```

Links beschreiben

describe-links

Verwenden Sie describe-links, um Informationen über die Netzwerkverbindungen auf dem Server zu erhalten. Outpost-Server müssen über einen Service Link und einen LNI-Link (Local Network Interface) verfügen.

Syntax

```
Outpost>describe-links
```

describe-links verwendet keine Argumente.

IP beschreiben

describe-ip

Verwenden Sie describe-ip, um den IP-Zuweisungsstatus und die Konfiguration jedes angeschlossenen Links zurückzugeben.

Syntax

```
Outpost>describe-ip
```

describe-ip verwendet keine Argumente.

Auflösung beschreiben

describe-resolve

Verwenden Sie describe-resolve, um festzustellen, ob der Outpost-Server einen DNS-Resolver erreichen und die IP-Adresse des Outpost-Konfigurationsendpunkts in der Region auflösen kann. Erfordert mindestens einen Link mit einer IP-Konfiguration.

Syntax

```
Outpost>describe-resolve
```

describe-resolve verwendet keine Argumente.

Erreichbarkeit beschreiben

describe-reachability

Verwenden Sie describe-reachability, um festzustellen, ob der Outpost-Server den Outpost-Konfigurationsendpunkt in der Region erreichen kann. Erfordert eine funktionierende DNS-Konfiguration, die Sie mithilfe von describe-resolve ermitteln können.

Syntax

```
Outpost>describe-reachability
```

describe-reachability verwendet keine Argumente.

Verbindung starten

start-connection

Verwenden Sie start-connection, um eine Verbindung mit dem Outpost-Dienst in der Region herzustellen. Dieser Befehl bezieht die Anmeldeinformationen für Signature Version 4 (SigV4) aus den Umgebungsvariablen, die Sie mit export geladen haben. Die Verbindung läuft asynchron und gibt sofort etwas zurück. Um den Status der Verbindung zu überprüfen, verwenden Sie get-connection.

Syntax

```
Outpost>start-connection [0|1]
```

start-connection verwendet einen optionalen Verbindungsindex, um eine weitere Verbindung zu initiieren. Nur Werte von `0` und 1 sind gültig.

Example : Verbindung gestartet

```
Outpost>start-connection

is_started: True
asset_id: example-asset-id
connection_id: example-connecdtion-id
timestamp: 2021-10-01T23:30:26Z
checksum: example-checksum
```

Verbindung herstellen

get-connection

Verwenden Sie get-connection, um den Status der Verbindung zurückzugeben.

Syntax

```
Outpost>get-connection [0|1]
```

get-connection verwendet einen optionalen Verbindungsindex, um den Status einer anderen Verbindung zurückzugeben. Nur Werte von `0` und `1` sind gültig.

Example : Verbindung erfolgreich

```
Outpost>get-connection


---
keys_exchanged: True
connection_established: True
exchange_active: False
primary_peer: xx.xx.xx.xx:xxx
primary_status: success
primary_connection_id: a1b2c3d4567890abcdefEXAMPLE11111
primary_handshake_age: 1111111111
primary_server_public_key: AKIAIOSFODNN7EXAMPLE
primary_client_public_key: AKIAI44QH8DHBEXAMPLE
primary_server_endpoint: xx.xx.xx.xx:xxx
secondary_peer: xx.xxx.xx.xxx:xxx
secondary_status: success
```

```
secondary_connection_id: a1b2c3d4567890abcdefEXAMPLE22222
secondary_handshake_age: 1111111111
secondary_server_public_key: wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY
secondary_client_public_key: je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY
secondary_server_endpoint: xx.xxx.xx.xxx:xxx
timestamp: 2023-02-22T22:19:28Z
checksum: 0x83FA0123
```

Hinweis:

- Wenn `exchange_active` `True` ist, wird die Verbindung immer noch hergestellt. Versuchen Sie es in 5 Minuten erneut.
- Wenn `keys_exchanged` oder `connection_established` `False` ist, und wenn `exchange_active` `True` ist, wird die Verbindung immer noch hergestellt. Versuchen Sie es in 5 Minuten erneut.

Wenn das Problem nach 1 Stunde weiterhin besteht, wenden Sie sich an das AWS Support - Center.

Starten Sie eine Instanz auf Ihrem Outpost-Server

Nach der Installation Ihres Outpost und der verfügbaren Datenverarbeitungs- und Speicherkapazität können Sie mit der Erstellung von Ressourcen beginnen. Sie können zum Beispiel Amazon EC2-Instances starten.

Voraussetzung

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

Aufgaben

- Schritt 1: Erstellen eines Subnetzes
- Schritt 2: Starten einer Instance im Outpost
- Schritt 3: Konnektivität konfigurieren
- Schritt 4: Testen der Verbindung

Schritt 1: Erstellen eines Subnetzes

Sie können Outpost-Subnetze zu jeder VPC in der AWS Region für den Outpost hinzufügen. Wenn Sie dies tun, bezieht die VPC auch den Outpost mit ein. Weitere Informationen finden Sie unter Netzwerkkomponenten.

> **Note**
>
> Wenn Sie eine Instance in einem Outpost-Subnetz starten, das von einem anderen für Sie freigegeben wurde, fahren Sie mit fort. AWS-KontoSchritt 2: Starten einer Instance im Outpost

So erstellen Sie ein 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 den Outpost aus und klicken Sie dann auf Aktionen, Subnetz erstellen. Sie werden zum Erstellen eines Subnetzes in der Amazon-VPC-Konsole umgeleitet. Wir wählen für Sie den Outpost und die Availability Zone aus, in der sich der Outpost befindet.
4. Wählen Sie eine VPC aus und geben Sie einen IP-Adressbereich für das Subnetz an.
5. Wählen Sie Erstellen.
6. Nachdem das Subnetz erstellt wurde, aktivieren Sie das Subnetz für lokale Netzwerkschnittstellen.

Schritt 2: Starten einer Instance im Outpost

Sie können EC2-Instances in dem Outpost-Subnetz starten, das Sie erstellt haben, oder in einem Outpost-Subnetz, das für Sie freigegeben wurde. Sicherheitsgruppen steuern den eingehenden und ausgehenden VPC-Datenverkehr für Instances in einem Outpost-Subnetz genauso wie für Instances in einem Availability Zone-Subnetz. Um eine Verbindung zu einer EC2-Instance in einem Outpost-Subnetz herzustellen, können Sie beim Starten der Instance ein Schlüsselpaar angeben, genauso wie dies bei Instances in einem Availability Zone-Subnetz der Fall ist.

Überlegungen

- Instances auf Outposts-Servern umfassen Instance-Speicher-Volumes, aber keine EBS-Volumes. Wählen Sie eine Instance-Größe mit ausreichend Instance-Speicher, um die Anforderungen Ihrer Anwendung zu erfüllen. Weitere Informationen finden Sie unter Instance-Speicher-Volumes im Amazon EC2-Benutzerhandbuch.
- Sie müssen ein AMI mit nur einem Snapshot angeben. AMIs mit mehr als einem Snapshot werden nicht unterstützt.
- Die Daten auf den Instance-Speicher-Volumes bleiben nach einem Neustart der Instance erhalten, nicht aber nach dem Beenden der Instance. Um die langfristigen Daten auf Ihren Instance-Speicher-Volumes über die Lebensdauer der Instance hinaus beizubehalten, sollten Sie sicherstellen, dass Sie die Daten in einem persistenten Speicher sichern, z. B. einem Amazon-S3-Bucket oder einem Netzwerkspeichergerät in Ihrem On-Premises-Netzwerk.
- Um eine Instance in einem Outpost-Subnetz mit Ihrem On-Premises-Netzwerk zu verbinden, müssen Sie eine lokale Netzwerkschnittstelle hinzufügen, wie im folgenden Verfahren beschrieben.

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 Amazon EC2-Konsole weitergeleitet. Wir wählen das Outpost-Subnetz für Sie aus und zeigen Ihnen nur die Instance-Typen, die von Ihren Outposts-Servern unterstützt werden.
5. Wählen Sie einen Instance-Typ, der von Ihren Outposts-Servern unterstützt wird.
6. (Optional) Sie können jetzt oder nach der Erstellung der Instance eine lokale Netzwerkschnittstelle hinzufügen. Um sie jetzt hinzuzufügen, erweitern Sie Erweiterte Netzwerkkonfiguration und wählen Sie Netzwerkschnittstelle hinzufügen aus. Wählen Sie das Outpost-Subnetz aus. Dadurch wird eine Netzwerkschnittstelle für die Instance erstellt, die den Geräteindex 1 verwendet. Wenn Sie 1 als LNI-Geräteindex für das Outpost-Subnetz angegeben haben, ist diese Netzwerkschnittstelle die lokale Netzwerkschnittstelle für die Instance.
7. Schließen Sie den Assistenten ab, um die Instance in Ihrem Outpost-Subnetz zu starten. Weitere Informationen finden Sie unter den folgenden Themen im Amazon EC2 Benutzerhandbuch:

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

Schritt 3: Konnektivität konfigurieren

Wenn Sie Ihrer Instance beim Start der Instance keine lokale Netzwerkschnittstelle hinzugefügt haben, müssen Sie dies jetzt tun. Weitere Informationen finden Sie unter Hinzufügen eines LNI nach dem Start.

Sie müssen die lokale Netzwerkschnittstelle für die Instance mit einer IP-Adresse aus Ihrem lokalen Netzwerk konfigurieren. In der Regel verwenden Sie dazu DHCP. Informationen hierzu finden Sie in der Dokumentation des Betriebssystems, das auf der Instance läuft. Suchen Sie nach Informationen zum Konfigurieren zusätzlicher Netzwerkschnittstellen und sekundärer IP-Adressen.

Schritt 4: Testen der Verbindung

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 IP-Adresse der lokalen Netzwerkschnittstelle 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 Connect to your Linux Instance im Amazon EC2 EC2-Benutzerhandbuch. Informationen zum Herstellen einer Verbindung mit einer Windows-Instance finden Sie unter Connect to your Windows Instance im Amazon EC2 EC2-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 Information ist in der Amazon EC2-Konsole auf der Seite mit den Instance-Details verfügbar.
2. Verwenden Sie je nach Betriebssystem ssh oder rdp, um eine Verbindung zur privaten IP-Adresse Ihrer Outpost-Instance herzustellen.
3. Führen Sie den ping Befehl von Ihrer Outpost-Instanz aus und geben Sie die IP-Adresse der Instanz in der AWS Region an.

   ```
   ping 10.0.1.5
   ```

   Es folgt eine Beispielausgabe.

   ```
   Pinging 10.0.1.5

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

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

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

AWS Outposts Konnektivität zu AWS Regionen

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

> **Note**
>
> Sie können keine private Konnektivität für Ihre Service Link-Verbindung verwenden, die Ihren Outpost-Server mit Ihrer AWS Region oder AWS Outposts Heimatregion verbindet.

Inhalt

Konnektivität über Service Links

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

Der Outpost ist in der Lage, den Service Link VPN zurück zur AWS -Region über die öffentliche Region-Konnektivität zu erstellen. Dazu benötigt der Outpost Konnektivität zu den öffentlichen IP-Bereichen der AWS Region, entweder über das öffentliche Internet oder über eine öffentliche virtuelle Schnittstelle. AWS Direct Connect Diese Konnektivität kann über bestimmte Routen im Service-Link-VLAN oder über eine Standardroute von 0.0.0.0/0 erfolgen. Weitere Informationen über die öffentlichen Bereiche für AWS finden Sie unter IP-Adressbereiche für AWS.

Nachdem die Serviceverbindung hergestellt wurde, ist der Outpost in Betrieb und wird von verwaltet. AWS Der Service-Link wird für den folgenden Datenverkehr verwendet:

- Verwaltung des Datenverkehrs zum Outpost über den Service Link, einschließlich des Datenverkehrs auf interner Steuerebene, Überwachung interner Ressourcen und Updates für Firmware und Software.
- Datenverkehr zwischen dem Outpost und allen zugehörigen VPCs, einschließlich des Datenverkehrs auf Kundendatenebene.

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

Die maximale Übertragungseinheit (MTU) einer Netzwerkverbindung ist die Größe (in Byte) des größten zulässigen Datenpakets, das über die Verbindung übergeben werden kann. Das Netzwerk muss eine MTU von 1500 Byte zwischen dem Outpost und den Service Link-Endpunkten in der übergeordneten Region unterstützen. AWS Informationen zur erforderlichen 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 Amazon EC2 EC2-Instance im Amazon EC2 EC2-Benutzerhandbuch.

Empfehlungen für die Bandbreite von Service Links

Für eine optimale Benutzererfahrung und Ausfallsicherheit AWS empfiehlt es sich, für die Service Link-Verbindung mit der Region eine redundante Konnektivität von mindestens 500 Mbit/s zu verwenden. AWS Die maximale Auslastung für jeden Outpost-Server beträgt 500 Mbit/s. Verwenden Sie mehrere Outpost-Server, um die Verbindungsgeschwindigkeit zu erhöhen. Wenn Sie beispielsweise drei AWS Outposts -Server haben, erhöht sich die maximale Verbindungsgeschwindigkeit auf 1,5 Gbit/s (1.500 Mbit/s). Weitere Informationen finden Sie unter Service Link-Datenverkehr für Server.

Ihre AWS Outposts Service Link-Bandbreitenanforderungen variieren je nach Workload-Merkmalen wie AMI-Größe, Anwendungselastizität, Burst-Geschwindigkeitsanforderungen und Amazon VPC-Verkehr in die Region. Beachten Sie, dass AWS Outposts Server keine AMIs zwischenspeichern. AMIs werden bei jedem Instance-Start aus der Region heruntergeladen.

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

Firewalls und der Service Link

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

In der folgenden Abbildung erweitert die Konfiguration die Amazon VPC von der AWS Region bis zum Outpost. Eine 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
- Datenverkehr zwischen dem Outpost und allen zugehörigen VPCs

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

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

Protokoll	Quell-Port	Quelladresse	Ziel-Port	Zieladresse
UDP	1024 - 65535	Service-Link-IP	53	DNS-Server, der über DHCP bereitgestellt wird
UDP	443, 1024-65535	Service-Link-IP	443	AWS Outposts Service Link-Endpunkte
TCP	1024 - 65535	Service-Link-IP	443	AWS Outposts Endpunkte für die Registrierung

> **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.

Updates und der Service Link

AWS unterhält eine sichere Netzwerkverbindung zwischen Ihrem Outpost-Server und seiner übergeordneten AWS Region. Diese Netzwerkverbindung, die als Service Link bezeichnet wird, ist für die Verwaltung des Outposts unerlässlich, da sie den Intra-VPC-Verkehr zwischen dem Outpost und der Region bereitstellt. AWS AWS Bewährte Well-Architected Practices empfehlen die Bereitstellung von Anwendungen in zwei Outposts, die verschiedenen Availability Zones zugeordnet sind, mit einem Active-Active-Design. Weitere Informationen finden Sie unter Überlegungen zum AWS Outposts Hochverfügbarkeitsdesign und zur Architektur.

Der Service-Link wird regelmäßig aktualisiert, um die Betriebsqualität und Leistung aufrechtzuerhalten. Während der Wartung kann es zu kurzen Latenzzeiten und Paketverlusten in diesem Netzwerk kommen, was sich auf Workloads auswirkt, die von der VPC-Konnektivität zu Ressourcen abhängen, die in der Region gehostet werden. Der Datenverkehr, der die lokalen Netzwerkschnittstellen (LNI) passiert, wird jedoch nicht beeinträchtigt. Sie können Auswirkungen auf Ihre Anwendung vermeiden, indem Sie die Best Practices von AWS Well-Architected befolgen und sicherstellen, dass Ihre Anwendungen gegen Ausfälle oder Wartungsaktivitäten, die einen einzelnen Outpost-Server betreffen, resistent sind.

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.

Outposts und Standorte

Verwalten Sie Outposts und Standorte für AWS Outposts.

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

Themen

Outposts verwalten

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

Erstellen eines Outpost

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

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

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

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

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

     Weitere Informationen finden Sie unter the section called “Standorte”.

10. Wählen Sie Outposts erstellen.

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

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

So bearbeiten Sie Namen und Beschreibung des Outposts bearbeiten

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

Geben Sie unter Name den Namen ein.

Geben Sie im Feld Beschreibung eine Beschreibung ein.

6. Wählen Sie Änderungen speichern aus.

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

Outpost-Details anzeigen

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

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

So zeigen Sie Outpost-Details mit der an AWS CLI

- Verwenden Sie den Befehl get-outpost AWS CLI .

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

Outpost-Tags verwalten

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

   [Tag hinzufügen] Wählen Sie Neuen Tag hinzufügen, und führen Sie die folgenden Schritte aus:

   - Geben Sie bei Key (Schlüssel) den Schlüsselnamen ein.

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

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

6. Wählen Sie Änderungen speichern aus.

Outpost-Standorte verwalten

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

Einen Outpost-Standort erstellen

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

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

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

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

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

Einen Standort bearbeiten

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

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

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

Standort-Details anzeigen

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

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

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

Standort-Tags verwalten

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

   [Tag hinzufügen] Wählen Sie Neuen Tag hinzufügen, und führen Sie die folgenden Schritte aus:

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

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

Einen AWS Outposts Server zurückgeben

Wenn AWS Outposts ein Serverdefekt festgestellt wird, informieren wir Sie, starten den Austauschvorgang, um Ihnen einen neuen Server zuzusenden, und stellen Ihnen das Versandetikett über die AWS Outposts Konsole zur Verfügung.

Wenn Sie den Server zurückgeben möchten, weil der Server das Ende der Vertragslaufzeit erreicht hat oder aus einem anderen Grund, wenden Sie sich an das AWS Support -Center.

Themen

In den folgenden Schritten wird erläutert, wie Sie einen Server an AWS zurückgeben.

1. Den Server für die Rückgabe vorbereiten

Um den Server auf die Rückgabe vorzubereiten, heben Sie die gemeinsame Nutzung von Ressourcen auf, sichern Sie Daten, löschen Sie lokale Netzwerkschnittstellen und beenden Sie aktive Instances.

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

   Eine Liste der Outpost-Ressourcen, die freigegeben werden können, finden Sie unter Freigebbare Outpost-Ressourcen.

2. Erstellen Sie Backups der Daten, die im Instance-Speicher der Amazon EC2 EC2-Instances gespeichert sind, die auf dem AWS Outposts Server ausgeführt werden.
3. Löschen Sie die lokalen Netzwerkschnittstellen, die den Instances zugeordnet sind, die auf dem Server ausgeführt wurden.
4. Beenden Sie die aktiven Instances, die Subnetzen auf Ihrem Outpost zugeordnet sind. Um die Instances zu beenden, folgen Sie den Anweisungen unter Terminate your Instance im Amazon EC2 EC2-Benutzerhandbuch.

2. Besorgen Sie sich das Versandetikett

> **Important**
>
> Sie dürfen nur das mitgelieferte Versandetikett verwenden AWS . Erstellen Sie kein eigenes Versandetikett.

Besorgen Sie sich Ihr Versandetikett auf der Grundlage des Grundes für Ihre Rücksendung.

Shipping label for a server that is being replaced

1. Öffnen Sie die AWS Outposts Konsole unter https://console.aws.amazon.com/outposts/.
2. Wählen Sie im Navigationsbereich Bestellungen aus.
3. Wählen Sie unter Übersicht der Ersatzbestellung die Option Versandetikett drucken und wählen Sie die Konfigurations-ID des Servers aus, den Sie zurücksenden möchten.

Shipping label for a server that is not being replaced

1. Kontaktieren Sie das AWS Support -Center.
2. Fordern Sie ein Versandetikett für den Server an, den Sie zurücksenden möchten.

3. Verpacken Sie den Server

Verwenden Sie zum Verpacken Ihres Servers den Karton, in dem der Server ursprünglich geliefert wurde, und das Verpackungsmaterial. Sie können auch den Karton verwenden, in der der Ersatzserver geliefert wird. Sie können sich auch an das AWS Support -Center wenden, um

einen Karton anzufordern. Bringen Sie nach dem Verpacken des Servers das AWS mitgelieferte Versandetikett an.

4. Senden Sie den Server über den Kurierdienst zurück

Sie müssen den Server über den für Ihr Land zuständigen Kurierdienst zurücksenden. Sie können den Server an den Kurierdienst übergeben oder den Tag und die Uhrzeit festlegen, an dem der Kurier den Server abholt. Das mitgelieferte Versandetikett AWS enthält die richtige Adresse für die Rücksendung an den Server.

Die folgende Tabelle zeigt, wer für das Land, aus dem Sie versenden, zu kontaktieren ist:

Land	Kontakt
Argentinien	Kontaktieren Sie das AWS Support -Center. Geben Sie in Ihrer Anfrage die folgenden Informationen an: • Die Sendungsverfolgungsnummer, die sich auf dem AWS mitgelieferten Versandetikett befindet • Das Datum und die Uhrzeit, zu der der Kurierdienst den Server abholen soll • Ein Ansprechpartner • Eine Telefonnummer • Eine E-Mail-Adresse
Bahrain	
Brasilien	
Brunei	
Kanada	
Chile	
Kolumbien	
Hong Kong	
Indien	
Indonesien	
Japan	
Malaysia	
Nigeria	
Oman	

Land	Kontakt
Panama	
Peru	
Philippinen	
Serbien	
Singapur	
Südafrika	
Südkorea	
Taiwan	
Thailand	
Vereinigte Arabische Emirate	
Vietnam	
United States of America	Wenden Sie sich an UPS. Sie können den Server auf folgende Weise zurückgeben: • Senden Sie den Server im Rahmen einer routinemäßigen UPS-Abholung an Ihrem Standort zurück. • Geben Sie den Server an einem UPS-Standort ab. • Vereinbaren Sie eine Abholung für ein Datum und eine Uhrzeit, die Sie bevorzugen. Geben Sie für den kostenlosen Versand die Sendungsverfolgungsnummer auf dem AWS mitgelieferten Versandetikett ein.

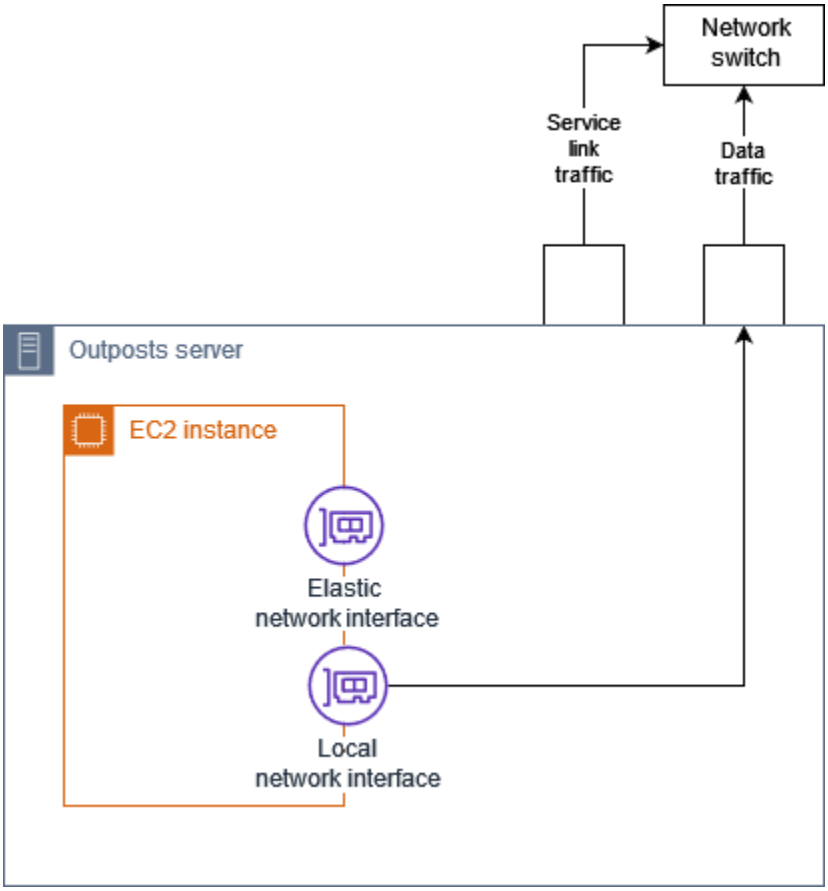
Land	Kontakt
Alle anderen Länder	Wenden Sie sich an DHL. Sie können den Server auf folgende Weise zurückgeben: • Geben Sie den Server an einem DHL-Standort ab. • Vereinbaren Sie eine Abholung für ein Datum und eine Uhrzeit, die Sie bevorzugen. Geben Sie für den kostenlosen Versand die AWS DHL-Frachtbriefnummer auf dem mitgelieferten Versandetikett ein. Wenn Sie die folgende Fehlermeldung erhalten: `Courier pickup cannot be scheduled for an import shipment`, bedeutet dies in der Regel, dass das von Ihnen gewählte Abholland nicht mit dem Abholland auf dem Versandetikett der Rücksendung übereinstimmt. Wählen Sie das Land aus, aus dem die Sendung stammt, und versuchen Sie es erneut.

Lokale Netzwerkschnittstellen

Bei AWS Outposts Servern ist eine lokale Netzwerkschnittstelle (LNI) eine logische Netzwerkkomponente, die die Amazon EC2 EC2-Instances in Ihrem Outposts-Subnetz mit Ihrem lokalen Netzwerk verbindet.

Eine lokale Netzwerkschnittstelle läuft direkt in Ihrem lokalen Netzwerk. Bei dieser Art von lokaler Konnektivität benötigen Sie keine Router oder Gateways, um mit Ihren On-Premises-Geräten zu kommunizieren. Lokale Netzwerkschnittstellen werden ähnlich wie Netzwerkschnittstellen oder Elastic-Netzwerkschnittstellen benannt. Wir unterscheiden zwischen den beiden Schnittstellen, indem wir immer lokal verwenden, wenn wir von lokalen Netzwerkschnittstellen sprechen.

Nachdem Sie lokale Netzwerkschnittstellen in einem Outpost-Subnetz aktiviert haben, können Sie die EC2-Instances im Outpost-Subnetz so konfigurieren, dass sie zusätzlich zur Elastic Network-Schnittstelle eine lokale Netzwerkschnittstelle enthalten. Die lokale Netzwerkschnittstelle stellt eine Verbindung zum On-Premises-Netzwerk her, während die Netzwerkschnittstelle eine Verbindung zur VPC herstellt. Das folgende Diagramm zeigt eine EC2-Instance auf einem Outposts-Server mit sowohl einer elastic network interface als auch einer lokalen Netzwerkschnittstelle.



Sie müssen das Betriebssystem so konfigurieren, dass die lokale Netzwerkschnittstelle in Ihrem On-Premises-Netzwerk kommunizieren kann, genau wie bei allen anderen On-Premises-Geräten. Sie können in einer VPC keine DHCP-Optionssätze verwenden, um eine lokale Netzwerkschnittstelle zu konfigurieren, da eine lokale Netzwerkschnittstelle in Ihrem lokalen Netzwerk ausgeführt wird.

Die elastische Netzwerkschnittstelle funktioniert genau wie bei Instances in einem Availability Zone-Subnetz. Sie können beispielsweise die VPC-Netzwerkverbindung verwenden, um auf die öffentlichen regionalen Endpunkte zuzugreifen AWS-Services, oder Sie können Schnittstellen-VPC-Endpunkte für den Zugriff verwenden. AWS-Services AWS PrivateLink Weitere Informationen finden Sie unter AWS Outposts Konnektivität zu AWS Regionen.

Inhalt

Lokale Netzwerkschnittstellen – Grundlagen

Lokale Netzwerkschnittstellen ermöglichen den Zugriff auf ein physisches Layer-2-Netzwerk. Eine VPC ist ein virtualisiertes Layer-Three-Netzwerk. Lokale Netzwerkschnittstellen unterstützen keine VPC-Netzwerkkomponenten. Zu diesen Komponenten gehören Sicherheitsgruppen, Netzwerkzugriffssteuerungslisten, virtualisierte Router oder Routing-Tabellen sowie Flussprotokolle. Die lokale Netzwerkschnittstelle bietet dem Outpost-Server keinen Einblick in die VPC-Layer-3-Flüsse. Das Host-Betriebssystem der Instance hat vollen Einblick in Frames aus dem physischen Netzwerk. Sie können die Standard-Firewalllogik auf Informationen innerhalb dieser Frames anwenden. Diese Kommunikation findet jedoch innerhalb der Instance statt, jedoch außerhalb des Zuständigkeitsbereichs der virtualisierten Konstrukte.

Überlegungen

- Lokale Netzwerkschnittstellen unterstützen ARP- und DHCP-Protokolle. Sie unterstützen keine allgemeinen L2-Broadcast-Nachrichten.
- Die Kontingente für lokale Netzwerkschnittstellen entsprechen Ihrem Kontingent für Netzwerkschnittstellen. Weitere Informationen finden Sie unter Netzwerk-Schnittstellen im Amazon VPC Benutzerhandbuch.
- Jede EC2-Instance kann über eine lokale Netzwerkschnittstelle verfügen.

- Eine lokale Netzwerkschnittstelle kann die primäre Netzwerkschnittstelle (eth0) der Instance nicht verwenden.
- Outposts-Server können mehrere EC2-Instances hosten, jede mit einer lokalen Netzwerkschnittstelle.

> **Note**
>
> EC2-Instances innerhalb desselben Servers können direkt kommunizieren, ohne Daten außerhalb des Outposts-Servers zu senden. Diese Kommunikation umfasst Datenverkehr über eine lokale Netzwerkschnittstelle oder Elastic-Netzwerkschnittstellen.

- Lokale Netzwerkschnittstellen sind nur für Instances verfügbar, die in einem Outposts-Subnetz auf einem Outpost-Server laufen.
- Lokale Netzwerkschnittstellen unterstützen weder den Promiscuous-Modus noch das Spoofing von MAC-Adressen.

Leistung

Das LNI jeder Instance-Größe stellt einen Teil der verfügbaren physischen 10-GbE-LNI-Bandbreite bereit. In der folgenden Tabelle ist die LNI-Netzwerkleistung für jeden Instance-Typ aufgeführt:

Instance-Typ	Baseline-Bandbreite (Gbit/s)	Maximale Bandbreite (Gbit/s)
c6id.large	0.15625	2.5
c6id.large	0,15625	2.5
c6id.xlarge	0,3125	2.5
c6id.2xlarge	0,625	2.5
c6id.4xlarge	1,25	2.5
c6id.8xlarge	2.5	2.5
c6id.12xlarge	3,75	3,75
c6id.16xlarge	5	5

Instance-Typ	Baseline-Bandbreite (Gbit/s)	Maximale Bandbreite (Gbit/s)
c6id.24xlarge	7,5	7,5
c6id.32xlarge	10	10
c6gd.medium	0,15625	4
c6gd.large	0,3125	4
c6gd.xlarge	0,625	4
c6gd.2xlarge	1,25	4
c6gd.4xlarge	2.5	4
c6gd.8xlarge	4,8	4,8
c6gd.12xlarge	7,5	7,5
c6gd.16xlarge	10	10

Sicherheitsgruppen

Die lokale Netzwerkschnittstelle verwendet standardmäßig keine Sicherheitsgruppen in Ihrer VPC. Eine Sicherheitsgruppe kontrolliert den eingehenden und ausgehenden VPC-Datenverkehr. Die lokale Netzwerkschnittstelle ist nicht mit der VPC verbunden. Die lokale Netzwerkschnittstelle ist mit Ihrem lokalen Netzwerk verbunden. Verwenden Sie eine Firewall oder eine ähnliche Strategie, um den eingehenden und ausgehenden Datenverkehr auf der On-Premises-Netzwerkschnittstelle zu kontrollieren, genau wie Sie es mit den übrigen Geräten vor Ort tun würden.

Überwachen

CloudWatch Metriken werden für jede lokale Netzwerkschnittstelle erstellt, genau wie für elastische Netzwerkschnittstellen. Weitere Informationen zu Linux-Instances finden Sie unter Überwachen der Netzwerkleistung für Ihre EC2-Instance im Amazon EC2 EC2-Benutzerhandbuch. Informationen zu Windows-Instances finden Sie unter Überwachen der Netzwerkleistung für Ihre EC2-Instance im Amazon EC2 EC2-Benutzerhandbuch.

MAC-Adressen

AWS stellt MAC-Adressen für lokale Netzwerkschnittstellen bereit. Lokale Netzwerkschnittstellen verwenden lokal verwaltete Adressen (LAA) für ihre MAC-Adressen. Eine lokale Netzwerkschnittstelle verwendet dieselbe MAC-Adresse, bis Sie die Schnittstelle löschen. Nachdem Sie eine lokale Netzwerkschnittstelle gelöscht haben, entfernen Sie die MAC-Adresse aus Ihren lokalen Konfigurationen. AWS kann MAC-Adressen wiederverwenden, die nicht mehr verwendet werden.

Subnetze auf Outposts-Servern für lokale Netzwerkschnittstellen aktivieren

Verwenden Sie den Befehl modify-subnet-attribute von, um ein Outpost-Subnetz für lokale Netzwerkschnittstellen AWS CLI zu aktivieren. Sie müssen die Position der Netzwerkschnittstelle auf dem Geräteindex angeben. Alle Instances, die in einem aktivierten Outpost-Subnetz gestartet werden, verwenden diese Gerätepositionen für lokale Netzwerkschnittstellen. Ein Wert von 1 gibt beispielsweise an, dass die sekundäre Netzwerkschnittstelle (eth1) für eine Instance im Outpost-Subnetz die lokale Netzwerkschnittstelle ist.

Subnetze auf Outposts-Servern für lokale Netzwerkschnittstellen aktivieren

Führen Sie in der Eingabeaufforderung den folgenden Befehl aus, um die Gerätepositionen für die lokale Netzwerkschnittstelle anzugeben.

```
aws ec2 modify-subnet-attribute \
    --subnet-id subnet-1a2b3c4d \
    --enable-lni-at-device-index 1
```

Arbeiten mit lokalen Netzwerkschnittstellen

In diesem Abschnitt erfahren Sie, wie mit lokalen Netzwerkschnittstellen gearbeitet wird.

Aufgaben

- Lokale Netzwerkschnittstelle hinzufügen
- Sehen Sie sich die lokale Netzwerkschnittstelle an
- Konfiguration des Betriebssystems

Lokale Netzwerkschnittstelle hinzufügen

Sie können einer Amazon EC2-Instance in einem Outposts-Subnetz während oder nach dem Start eine lokale Netzwerkschnittstelle (LNI) hinzufügen. Dazu fügen Sie der Instance eine sekundäre Netzwerkschnittstelle hinzu und verwenden dabei den Geräteindex, den Sie bei der Aktivierung des Outpost-Subnetzes für lokale Netzwerkschnittstellen angegeben haben.

Überlegungen

Wenn Sie die sekundäre Netzwerkschnittstelle mithilfe der Konsole angeben, wird die Netzwerkschnittstelle anhand des Geräteindex 1 erstellt. Wenn dies nicht der Geräteindex ist, den Sie bei der Aktivierung des Outpost-Subnetzes für lokale Netzwerkschnittstellen angegeben haben, können Sie stattdessen den richtigen Geräteindex angeben, indem Sie das oder ein SDK verwenden. AWS CLI AWS Verwenden Sie beispielsweise die folgenden Befehle von AWS CLI: create-network-interface und attach-network-interface.

So fügen Sie beim Start der Instance ein LNI hinzu

1. Wählen Sie im Launch Instance Wizard neben Netzwerkeinstellungen die Option Bearbeiten aus.
2. Erweiterte Netzwerkkonfiguration erweitert
3. Wählen Sie Add network interface aus. Dadurch wird eine Netzwerkschnittstelle mit dem Geräteindex 1 erstellt. Wenn Sie 1 als LNI-Geräteindex für das Outpost-Subnetz angegeben haben, ist diese Netzwerkschnittstelle die lokale Netzwerkschnittstelle für die Instance.
4. Wählen Sie das Outpost-Subnetz aus und aktualisieren Sie die Konfiguration für die Netzwerkschnittstelle nach Bedarf.
5. Folgen Sie den Anweisungen des Assistenten, um die Instance zu starten.

So fügen Sie der Instance nach dem Start ein LNI hinzu

1. Klicken Sie im Navigationsbereich unter Netzwerk und Sicherheit auf Netzwerkschnittstellen.
2. Erstellen der Netzwerkschnittstelle
    a. Klicken Sie auf Create network interface (Netzwerkschnittstellen erstellen).
    b. Wählen Sie dasselbe Outpost-Subnetz wie die Instance aus.
    c. Vergewissern Sie sich, dass Private IPv4-Adresse auf Automatisch zuweisen eingestellt ist.

d. Auswählen aller Sicherheitsgruppen Sicherheitsgruppen gelten nicht für LNIs, sodass die von Ihnen ausgewählte Sicherheitsgruppe nicht relevant ist.

e. Klicken Sie auf Create network interface (Netzwerkschnittstellen erstellen).

3. Zuordnen einer Netzwerkschnittstelle zur Instance

a. Aktivieren Sie das Kontrollkästchen für die neu erstellte Netzwerkschnittstelle.

b. Wählen Sie Actions (Aktionen) und Attach (Anfügen).

c. Wählen Sie die Instance aus.

d. Wählen Sie Anfügen aus. Die Netzwerkschnittstelle ist an Geräteindex 1 gebunden. Wenn Sie 1 als LNI-Geräteindex für das Outpost-Subnetz angegeben haben, ist diese Netzwerkschnittstelle die lokale Netzwerkschnittstelle für die Instance.

Sehen Sie sich die lokale Netzwerkschnittstelle an

Während die Instance in Betrieb ist, können Sie die Amazon EC2-Konsole verwenden, um sowohl die elastische Netzwerkschnittstelle als auch die lokale Netzwerkschnittstelle für die Instances in Ihrem Outpost-Subnetz anzuzeigen. Markieren Sie die Instance und wählen Sie die Registerkarte Netzwerk.

Die Konsole zeigt eine private IPv4-Adresse für das LNI aus dem Subnetz-CIDR an. Diese Adresse ist nicht die IP-Adresse des LNI und kann nicht verwendet werden. Diese Adresse wird jedoch über das Subnetz-CIDR zugewiesen, sodass Sie sie bei der Subnetzdimensionierung berücksichtigen müssen. Sie müssen die IP-Adresse für das LNI im Gastbetriebssystem entweder statisch oder über Ihren DHCP-Server festlegen.

Konfiguration des Betriebssystems

Nachdem Sie lokale Netzwerkschnittstellen aktiviert haben, verfügen Amazon EC2-Instances über zwei Netzwerkschnittstellen. Eine davon ist eine lokale Netzwerkschnittstelle. Stellen Sie sicher, dass Sie das Betriebssystem der Amazon EC2-Instances, die Sie starten, so konfigurieren, dass es eine mehrfach vernetzte Netzwerkkonfiguration unterstützt.

Lokale Netzwerkkonnektivität für Server.

Verwenden Sie dieses Thema, um sich mit den Netzwerkverkabelungs- und Topologieanforderungen für das Hosten eines Outpost-Servers vertraut zu machen. Weitere Informationen finden Sie unter Lokale Netzwerkschnittstellen.

Inhalt

Servertopologie in Ihrem Netzwerk

Ein Outpost-Server benötigt zwei unterschiedliche Verbindungen zu Ihren Netzwerkgeräten. Jede Verbindung verwendet ein anderes Kabel und überträgt eine andere Art von Datenverkehr. Die mehreren Kabel dienen nur der Isolierung des Datenverkehrs und nicht der Redundanz. Die beiden Kabel müssen nicht mit einem gemeinsamen Netzwerk verbunden werden.

Die folgende Tabelle beschreibt die Arten des Datenverkehrs auf dem Outpost-Server und die Kennzeichnung.

Datenverkehrskennzeichnung	Beschreibung
2	Service Link-Verkehr — Dieser Verkehr ermöglicht die Kommunikation zwischen dem Outpost und der AWS Region sowohl für die Verwaltung des Outposts als auch für den Intra-VPC-Verkehr zwischen der AWS Region und dem Outpost. Der Service-Link-Daten verkehr umfasst die Service-Link-Verbindung vom Outpost zur Region. Der Service Link ist ein benutzerdefiniertes VPN oder VPNs vom Outpost zur Region. Der Outpost stellt eine Verbindung zur Availability Zone in der Region her, die Sie beim Kauf ausgewählt haben.
1	Datenverkehr über die lokale Netzwerks chnittstelle (LNI) – Dieser Datenverkehr ermöglicht die Kommunikation von Ihrem

Datenverkehrskennzeichnung	Beschreibung
	VPC zu Ihrem lokalen LAN über die lokale Netzwerkschnittstelle. Der lokale Link-Date nverkehr umfasst Instances, die auf dem Outpost laufen und mit Ihrem On-Premises-Netzwerk kommunizieren. Der lokale Link-Datenverkehr kann auch Instances umfassen, die über Ihr On-Premises-Netzwerk mit dem Internet kommunizieren.

Physische Serverkonnektivität

Jeder Outpost-Server umfasst nicht redundante physische Uplink-Ports. Ports haben ihre eigenen Geschwindigkeits- und Konnektoranforderungen wie folgt:

- 10 GbE – Steckertyp QSFP+

QSFP+-Kabel

Das QSFP+-Kabel hat einen Anschluss, den Sie an Port 3 des Outpost-Servers anschließen. Das andere Ende des QSFP+-Kabels hat vier SFP+-Schnittstellen, die Sie an Ihren Switch anschließen. Zwei der Switch-Seiten-Schnittstellen sind mit 1 und 2 gekennzeichnet. Damit ein Outpost-Server überhaupt funktioniert, sind beide Schnittstellen erforderlich. Verwenden Sie die 2-Schnittstelle für den Service Link-Datenverkehr und die 1-Schnittstelle für den LNI-Link-Datenverkehr. Die übrigen Schnittstellen werden nicht verwendet.

Service Link-Datenverkehr für Server

Konfigurieren Sie den Service Link-Port auf Ihrem Switch als Zugangsport ohne Tags zu einem VLAN mit einem Gateway und einer Route zu den folgenden regionalen Endpunkten:

- Service Link-Endpunkte
- Outpost-Registrierungsendpunkt

Für die Service Link-Verbindung muss öffentliches DNS verfügbar sein, damit der Outpost seinen Registrierungsendpunkt in der Region ermitteln kann. AWS Die Verbindung kann über ein NAT-

Gerät zwischen dem Outpost-Server und dem Registrierungsendpunkt hergestellt werden. Weitere Informationen zu den öffentlichen Adressbereichen für AWS finden Sie unter AWS IP-Adressbereiche im Amazon VPC-Benutzerhandbuch und AWS Outposts Endpunkte und Kontingente im. Allgemeine AWS-Referenz

Um den Server zu registrieren, öffnen Sie die folgenden Netzwerkports:

- TCP 443
- UDP 443
- UDP 53

Uplink-Geschwindigkeit

Jeder Outposts-Server benötigt eine Mindest-Uplink-Geschwindigkeit von 20 Mbit/s zur AWS -Region.

Abhängig von Ihrer LNI-Verbindung und der Auslastung des Service-Links benötigen Sie möglicherweise einen schnelleren Uplink. Weitere Informationen finden Sie unter Bandbreitenempfehlungen für Service-Links.

Link-Datenverkehr über die lokale Netzwerkschnittstelle (LNI)

Konfigurieren Sie den LNI-Link-Port auf Ihrem Upstream-Netzwerkgerät als Standardzugriffsport zu einem VLAN in Ihrem lokalen Netzwerk. Wenn Sie mehr als ein VLAN haben, konfigurieren Sie alle Ports auf dem Upstream-Netzwerkgerät als Trunk-Ports. Konfigurieren Sie den Port auf Ihrem Upstream-Netzwerkgerät so, dass mehrere MAC-Adressen erwartet werden. Jede auf dem Server gestartete Instance verwendet eine MAC-Adresse. Einige Netzwerkgeräte bieten Port-Sicherheitsfunktionen, mit denen ein Port, der mehrere MAC-Adressen meldet, heruntergefahren wird.

> **Note**
>
> AWS Outposts Server kennzeichnen keinen VLAN-Verkehr. Wenn Sie Ihr LNI als Trunk konfigurieren, müssen Sie sicherstellen, dass Ihr Betriebssystem den VLAN-Datenverkehr kennzeichnet.

Im folgenden Beispiel wird veranschaulicht, wie Sie VLAN-Tagging für Ihr LNI unter Amazon Linux 2023 konfigurieren. Wenn Sie eine andere Linux-Distribution verwenden, informieren Sie sich in der Dokumentation Ihrer Linux-Distribution über die Konfiguration von VLAN-Tagging.

Beispiel: Um VLAN-Tagging für Ihr LNI unter Amazon Linux 2023 und Amazon Linux 2 zu konfigurieren

1. Stellen Sie sicher, dass das 8021q-Modul in den Kernel geladen ist. Wenn nicht, laden Sie es mit dem `modprobe`-Befehl.

```
modinfo 8021q
modprobe --first-time 8021q
```

2. Erstellen Sie das VLAN-Gerät. In diesem Beispiel:

   - Der Name der Schnittstelle des LNI lautet `ens6`
   - Die VLAN-ID lautet 59
   - Der dem VLAN-Gerät zugewiesene Name lautet `ens6.59`

```
ip link add link ens6 name ens6.59 type vlan id 59
```

3. Optional. Schließen Sie diesen Schritt ab, wenn Sie die IP manuell zuweisen möchten. In diesem Beispiel weisen wir die IP 192.168.59.205 zu, wobei das Subnetz CIDR 192.168.59.0/24 ist.

```
ip addr add 192.168.59.205/24 brd 192.168.59.255 dev ens6.59
```

4. Aktivieren Sie den Link.

```
ip link set dev ens6.59 up
```

Um Ihre Netzwerkschnittstellen auf Betriebssystemebene zu konfigurieren und die Änderungen am VLAN-Tagging dauerhaft zu machen, finden Sie in den folgenden Ressourcen:

- Wenn Sie Amazon Linux 2 verwenden, finden Sie weitere Informationen unter Konfigurieren Ihrer Netzwerkschnittstelle mithilfe von ec2-net-utils für Amazon Linux im Amazon EC2 EC2-Benutzerhandbuch.

- Wenn Sie Amazon Linux 2023 verwenden, finden Sie weitere Informationen unter Netzwerkservice im Amazon Linux 2023-Benutzerhandbuch.

Zuweisung von Server-IP-Adressen

Sie benötigen keine öffentlichen IP-Adresszuweisungen für Outpost-Server.

Das Dynamic Host Control Protocol (DHCP) ist ein Netzwerkverwaltungsprotokoll, das zur Automatisierung der Konfiguration von Geräten in IP-Netzwerken verwendet wird. Im Kontext von Outpost-Servern können Sie DHCP auf zwei Arten verwenden:

- Netzwerkkarten auf dem Server
- Lokale Netzwerkschnittstellen auf Instances

Für Service Link verwenden Outpost-Server DHCP, um eine Verbindung zum lokalen Netzwerk herzustellen. DHCP muss DNS-Nameserver und ein Standard-Gateway zurückgeben. Outpost-Server unterstützen keine statische IP-Zuweisung von Service-Links.

Verwenden Sie für LNI Link DHCP, um Instances so zu konfigurieren, dass sie an Ihr lokales Netzwerk angeschlossen werden. Weitere Informationen finden Sie unter the section called “Konfiguration des Betriebssystems”.

> **Note**
>
> Stellen Sie sicher, dass Sie eine stabile IP-Adresse für den Outpost-Server verwenden. Änderungen der IP-Adresse können zu vorübergehenden Dienstunterbrechungen im Outpost-Subnetz führen.

Serverregistrierung

Wenn Outpost-Server eine Verbindung im lokalen Netzwerk herstellen, verwenden sie die Service-Link-Verbindung, um eine Verbindung zu den Outpost-Registrierungsendpunkten herzustellen und sich selbst zu registrieren. Für die Registrierung ist öffentliches DNS erforderlich. Wenn sich Server registrieren, erstellen sie einen sicheren Tunnel zu ihrem Service Link-Endpunkt in der Region. Outpost-Server verwenden den TCP-Port 443, um die Kommunikation mit der Region über das öffentliche Internet zu erleichtern. Derzeit unterstützen AWS Outposts Server keine

private Konnektivität über VPC. Weitere Informationen finden Sie unter the section called “Schritt 6: Autorisieren des Servers”.

Mit gemeinsam genutzten AWS Outposts Ressourcen arbeiten

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

In diesem Modell teilt sich das AWS Konto, dem die Outpost-Ressourcen gehören (Eigentümer), die Ressourcen mit anderen AWS Konten (Verbrauchern) in derselben Organisation. Verbraucher können Ressourcen auf Outposts erstellen, die mit ihnen geteilt werden, genauso wie sie Ressourcen auf Outposts erstellen würden, die sie in ihrem eigenen Konto erstellen. Der Eigentümer ist für die Verwaltung des Outposts und der Ressourcen, die er darin erstellt, verantwortlich. Besitzer können die Freigabe jederzeit ändern oder widerrufen. Mit Ausnahme von Instances, die Kapazitätsreservierungen verbrauchen, können Besitzer auch Ressourcen einsehen, ändern und löschen, die Nutzer in geteilten Outposts erstellen. Besitzer sind nicht dazu befugt Instances, die Konsumenten in den von ihnen freigegebenen Kapazitätsreservierungen starten, zu ändern.

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

Ein Outpost-Besitzer kann Outpost-Ressourcen teilen mit:

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

Inhalt

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

Gemeinsam nutzbare Outpost-Ressourcen

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

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

- Zugewiesene Dedicated Hosts — Verbraucher mit Zugriff auf diese Ressource können:
  - EC2-Instances auf einem Dedicated Host starten und ausführen.
- Outposts — Verbraucher mit Zugang zu dieser Ressource können:
  - Subnetze auf dem Outpost erstellen und verwalten.
  - Verwenden Sie die AWS Outposts API, um Informationen über den Outpost einzusehen.
- Websites — Verbraucher mit Zugriff auf diese Ressource können:
  - Einen Außenposten am Standort einrichten, verwalten und kontrollieren.
- Subnetze — Verbraucher mit Zugriff auf diese Ressource können:
  - Informationen über Subnetze anzeigen.
  - Starten und führen Sie EC2-Instances in Subnetzen aus.

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

Voraussetzungen für die gemeinsame Nutzung von Outposts-Ressourcen

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

Zugehörige Services

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

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

Freigeben in mehreren Availability Zones

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

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

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

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

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

Eine Outpost-Ressource gemeinsam nutzen

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

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

Wenn Sie Teil einer Organisation sind AWS Organizations und die gemeinsame Nutzung innerhalb Ihrer Organisation aktiviert ist, können Sie Verbrauchern in Ihrer Organisation von der AWS RAM Konsole aus Zugriff auf die gemeinsam genutzte Outpost-Ressource gewähren. Andernfalls erhalten Verbraucher eine Einladung, dem Resource Share beizutreten, und erhalten nach Annahme der Einladung Zugriff auf die gemeinsam genutzte Outpost-Ressource.

Sie können eine Outpost-Ressource, die Sie besitzen, mit der AWS Outposts Konsole, AWS RAM der Konsole oder dem teilen. AWS CLI

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

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

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

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

Siehe Erstellen einer Ressourcenfreigabe im AWS RAM-Benutzerhandbuch.

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

Verwenden Sie den create-resource-share-Befehl.

Aufheben der gemeinsamen Nutzung einer gemeinsam genutzten Outpost-Ressource

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

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

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

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

Siehe Aktualisieren einer Ressourcenfreigabe im AWS RAM-Benutzerhandbuch.

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

Verwenden Sie den disassociate-resource-share-Befehl.

Identifizieren einer gemeinsam genutzten Outpost-Ressource

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

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

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

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

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

Gemeinsam genutzte Outpost-Ressourcenberechtigungen

Berechtigungen für Besitzer

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

Berechtigungen für Konsumenten

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

Fakturierung und Messung

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

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

Verbrauchern werden Anwendungsressourcen in Rechnung gestellt, die sie auf gemeinsam genutzten Outposts erstellen, z. B. Load Balancer und Amazon RDS-Datenbanken. Verbrauchern werden auch kostenpflichtige Datenübertragungen aus der Region in Rechnung gestellt. AWS

Einschränkungen

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

- Einschränkungen für gemeinsam genutzte Subnetze gelten für die Arbeit mit der Funktion „AWS OutpostsTeilen“. Weitere Informationen zu VPC-Freigabelimits finden Sie unter Einschränkungen im Amazon Virtual Private Cloud Cloud-Benutzerhandbuch.
- Servicekontingente werden auf einzelne Konten angewendet.

Sicherheit in AWS Outposts

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

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

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

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

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

Inhalt

Datenschutz in AWS Outposts

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

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

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

Verschlüsselung im Ruhezustand

Mit AWS Outposts werden alle Daten im Ruhezustand verschlüsselt. Das Schlüsselmaterial befindet sich in einem externen Schlüssel, der auf einem austauschbaren Gerät gespeichert ist, dem Nitro Security Key (NSK). Der NSK ist erforderlich, um die Daten auf Ihren Outpost-Servern zu entschlüsseln.

Verschlüsselung während der Übertragung

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

Löschen von Daten

Wenn Sie eine EC2-Instance beenden, wird der ihr zugewiesene Speicher vom Hypervisor gesäubert (mit Null überschrieben), bevor er einer neuen Instance zugewiesen wird. Jeder Speicherblock wird zurückgesetzt.

Durch die Zerstörung des Nitro-Sicherheitsschlüssels werden die Daten auf Ihrem Outpost kryptografisch vernichtet. Weitere Informationen finden Sie unter Kryptografisch geschredderte Serverdaten.

Identitäts- und Zugriffsmanagement (IAM) für AWS Outposts

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

Inhalt

So funktioniert AWS Outposts mit IAM

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

IAM-Funktionen, die Sie mit AWS Outposts verwenden können

IAM-Feature	AWS Unterstützung für Outposts
Identitätsbasierte Richtlinien	Ja
Ressourcenbasierte Richtlinien	Nein
Richtlinienaktionen	Ja
Richtlinienressourcen	Ja
Richtlinienbedingungsschlüssel (services pezifisch)	Ja
ACLs	Nein
ABAC (Tags in Richtlinien)	Ja
Temporäre Anmeldeinformationen	Ja

IAM-Feature	AWS Unterstützung für Outposts
Hauptberechtigungen	Ja
Servicerollen	Nein
Serviceverknüpfte Rollen	Ja

Identitätsbasierte Richtlinien für Outposts AWS

Unterstützt Richtlinien auf Identitätsbasis.	Ja

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

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

Beispiele für identitätsbasierte Richtlinien für 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 anfügen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und

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

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

Politische Maßnahmen für AWS Outposts

Unterstützt Richtlinienaktionen	Ja

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

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

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

Eine Liste der AWS Outposts-Aktionen finden Sie unter Aktionen definiert von AWS Outposts in der Service Authorization Reference.

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

```
outposts
```

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

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

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

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

Politische Ressourcen für AWS Outposts

Unterstützt Richtlinienressourcen	Ja

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

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

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

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

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

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

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

Schlüssel zu den Policy-Bedingungen für AWS Outposts

Unterstützt servicespezifische Richtlinienbedingungsschlüssel	Ja

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

Das Element `Condition` (oder `Condition` block) ermöglicht Ihnen die Angabe der Bedingungen, unter denen eine Anweisung wirksam ist. Das Element `Condition` ist optional. Sie können bedingte Ausdrücke erstellen, die Bedingungsoperatoren verwenden, z. B. ist gleich oder kleiner als, damit die Bedingung in der Richtlinie mit Werten in der Anforderung übereinstimmt.

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

Sie können auch Platzhaltervariablen verwenden, wenn Sie Bedingungen angeben. Beispielsweise können Sie einem IAM-Benutzer die Berechtigung für den Zugriff auf eine Ressource nur dann

gewähren, wenn sie mit dessen IAM-Benutzernamen gekennzeichnet ist. Weitere Informationen finden Sie unter IAM-Richtlinienelemente: Variablen und Tags im IAM-Benutzerhandbuch.

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

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

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

ACLs in Outposts AWS

Unterstützt ACLs	Nein

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

ABAC mit Outposts AWS

Unterstützt ABAC (Tags in Richtlinien)	Ja

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

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

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

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

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

Temporäre Anmeldeinformationen mit AWS Outposts verwenden

Unterstützt temporäre Anmeldeinformationen	Ja

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

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

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

Serviceübergreifende Prinzipalberechtigungen für Outposts AWS

Unterstützt Forward Access Sessions (FAS)	Ja

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

Servicerollen für AWS -Outposts

Unterstützt Servicerollen	Nein

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

Servicebezogene Rollen für Outposts AWS

Unterstützt serviceverknüpfte Rollen	Ja

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

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

AWS Politische Beispiele für Outposts

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

auszuführen, die sie benötigen. Der Administrator kann dann die IAM-Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen annehmen.

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

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

Inhalt

Bewährte Methoden für Richtlinien

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

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten — Verwenden Sie die AWS verwalteten Richtlinien, die Berechtigungen für viele gängige Anwendungsfälle gewähren, um Ihren Benutzern und Workloads zunächst Berechtigungen zu gewähren. Sie sind in Ihrem verfügbar. AWS-Konto Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom AWS Kunden verwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind. Weitere Informationen finden Sie unter AWS -verwaltete Richtlinien oder AWS -verwaltete Richtlinien für Auftrags-Funktionen im IAM-Benutzerhandbuch.
- Anwendung von Berechtigungen mit den geringsten Rechten – Wenn Sie mit IAM-Richtlinien Berechtigungen festlegen, gewähren Sie nur die Berechtigungen, die für die Durchführung einer Aufgabe erforderlich sind. Sie tun dies, indem Sie die Aktionen definieren, die für bestimmte Ressourcen unter bestimmten Bedingungen durchgeführt werden können, auch bekannt als die geringsten Berechtigungen. Weitere Informationen zur Verwendung von IAM zum Anwenden von Berechtigungen finden Sie unter Richtlinien und Berechtigungen in IAM im IAM-Benutzerhandbuch.

- Verwenden von Bedingungen in IAM-Richtlinien zur weiteren Einschränkung des Zugriffs – Sie können Ihren Richtlinien eine Bedingung hinzufügen, um den Zugriff auf Aktionen und Ressourcen zu beschränken. Sie können beispielsweise eine Richtlinienbedingung schreiben, um festzulegen, dass alle Anforderungen mithilfe von SSL gesendet werden müssen. Sie können auch Bedingungen verwenden, um Zugriff auf Serviceaktionen zu gewähren, wenn diese für einen bestimmten Zweck verwendet werden AWS-Service, z. AWS CloudFormation B. Weitere Informationen finden Sie unter IAM-JSON-Richtlinienelemente: Bedingung im IAM-Benutzerhandbuch.
- Verwenden von IAM Access Analyzer zur Validierung Ihrer IAM-Richtlinien, um sichere und funktionale Berechtigungen zu gewährleisten – IAM Access Analyzer validiert neue und vorhandene Richtlinien, damit die Richtlinien der IAM-Richtliniensprache (JSON) und den bewährten IAM-Methoden entsprechen. IAM Access Analyzer stellt mehr als 100 Richtlinienprüfungen und umsetzbare Empfehlungen zur Verfügung, damit Sie sichere und funktionale Richtlinien erstellen können. Weitere Informationen finden Sie unter Richtlinienvalidierung zum IAM Access Analyzer im IAM-Benutzerhandbuch.
- Multi-Faktor-Authentifizierung (MFA) erforderlich — Wenn Sie ein Szenario haben, das IAM-Benutzer oder einen Root-Benutzer in Ihrem System erfordert AWS-Konto, aktivieren Sie MFA für zusätzliche Sicherheit. Um MFA beim Aufrufen von API-Vorgängen anzufordern, fügen Sie Ihren Richtlinien MFA-Bedingungen hinzu. Weitere Informationen finden Sie unter Konfigurieren eines MFA-geschützten API-Zugriffs im IAM-Benutzerhandbuch.

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

Beispiel: Nutzen von Berechtigungen auf Ressourcenebene

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

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

```
}
```

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

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

Verwenden von serviceverknüpften Rollen für AWS Outposts

AWS Outposts verwendet AWS Identity and Access Management (IAM) serviceverknüpfte Rollen. Eine serviceverknüpfte Rolle ist ein einzigartiger Typ von IAM-Rolle, mit der direkt verknüpft ist. AWS Outposts Mit Diensten verknüpfte Rollen sind vordefiniert AWS Outposts und enthalten alle Berechtigungen, die der Dienst benötigt, um andere AWS Dienste in Ihrem Namen aufzurufen.

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

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

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

Berechtigungen von serviceverknüpften Rollen für AWS Outposts

AWS Outposts verwendet die serviceverknüpfte Rolle 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.

Die serviceverknüpfte Rolle AWSServiceRoleForOutposts _ *outpostID* vertraut darauf, dass die folgenden Dienste die Rolle übernehmen:

- `outposts.amazonaws.com`

Die AWSServiceRoleForOutpostsserviceverknüpfte Rolle _ ***outpostID umfasst*** die folgenden Richtlinien:

- AWSOutpostsServiceRolePolicy
- AWSOutpostsPrivateConnectivityPolicy_ outpostID

Die AWSOutpostsServiceRolePolicyRichtlinie ist 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`

Die AWSOutpostsPrivateConnectivityPolicy_ ***OutpostID-Richtlinie*** ermöglicht es AWS Outposts , die folgenden Aktionen auf den angegebenen Ressourcen durchzuführen:

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

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

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

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

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

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

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

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

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

Erstellen einer serviceverknüpften Rolle für AWS Outposts

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

Bearbeiten einer serviceverknüpften Rolle für AWS Outposts

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

Löschen einer serviceverknüpften Rolle für AWS Outposts

Wenn Sie eine Funktion oder einen Service, die bzw. der eine serviceverknüpfte Rolle erfordert, nicht mehr benötigen, sollten Sie diese Rolle löschen. Auf diese Weise vermeiden Sie, dass eine

ungenutzte Einheit nicht aktiv überwacht oder gewartet wird. Sie müssen jedoch die Ressourcen für Ihre serviceverknüpfte Rolle zunächst bereinigen, bevor Sie sie manuell löschen können.

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

> **Warning**
>
> Sie müssen Ihren Outpost löschen, bevor Sie die mit dem Dienst verknüpfte Rolle AWSServiceRoleForOutposts _ *`OutpostID`* löschen können. Mit dem folgenden Verfahren wird Ihr Outpost gelöscht.

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

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

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

So löschen Sie die serviceverknüpfte Rolle mit IAM

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

Unterstützte Regionen für serviceverknüpfte AWS Outposts -Rollen

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

AWS verwaltete Richtlinien für AWS Outposts

Eine AWS verwaltete Richtlinie ist eine eigenständige Richtlinie, die von erstellt und verwaltet wird AWS. 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 unter Von AWS verwaltete Richtlinien im IAM-Benutzerhandbuch.

AWS verwaltete Richtlinie: AWSOutpostsServiceRolePolicy

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, mit der AWS Outposts Sie Aktionen in Ihrem Namen ausführen können. Weitere Informationen finden Sie unter Verwenden von serviceverknüpften Rollen.

AWS verwaltete Richtlinie: AWSOutpostsPrivateConnectivityPolicy

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, mit der AWS Outposts Sie Aktionen in Ihrem Namen ausführen können. Weitere Informationen finden Sie unter Verwenden von serviceverknüpften Rollen.

AWS verwaltete Richtlinie: AWSOutpostsAuthorizeServerPolicy

Verwenden Sie diese Richtlinie, um die für die Autorisierung der Outpost-Serverhardware in Ihrem On-Premises-Netzwerk erforderlichen Berechtigungen zu gewähren. Weitere Informationen finden Sie unter Berechtigungen erteilen.

Diese Richtlinie umfasst die folgenden Berechtigungen.

```
{
```

```
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "outposts:StartConnection",
        "outposts:GetConnection"
      ],
      "Resource": "*"
    }
  ]
}
```

AWS Outposts Aktualisierungen der AWS verwalteten Richtlinien

Hier finden Sie Informationen zu Aktualisierungen AWS verwalteter Richtlinien AWS Outposts seit Beginn der Nachverfolgung dieser Änderungen durch diesen Dienst.

Änderung	Beschreibung	Datum
AWSOutpostsAuthorizeServerPolicy – Neue Richtlinie.	AWS Outposts hat eine Richtlinie hinzugefügt, die Berechtigungen zur Autorisierung von Outpost-Serverhardware in Ihrem lokalen Netzwerk gewährt.	4. Januar 2023
AWS Outposts hat begonnen, Änderungen zu verfolgen	AWS Outposts hat begonnen, Änderungen für die AWS verwalteten Richtlinien zu verfolgen.	03. Dezember 2019

Sicherheit der Infrastruktur in AWS Outposts

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

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

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

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

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

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

Belastbarkeit in AWS Outposts

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

Wenn Sie einen Outpost erstellen, wählen Sie eine Availability Zone aus einer AWS Region aus. Diese Availability Zone unterstützt Operationen der Steuerebene wie die Beantwortung von API-Aufrufen, die Überwachung des Outpost und die Aktualisierung des Outpost. Um von der Ausfallsicherheit der Availability Zones zu profitieren, können Sie Anwendungen auf mehreren

Outposts bereitstellen, die jeweils mit einer anderen Availability Zone verbunden sind. Auf diese Weise können Sie zusätzliche Ausfallsicherheit für Anwendungen aufbauen und die Abhängigkeit von einer einzigen Availability Zone vermeiden. Weitere Informationen über Regionen und Availability Zones finden Sie unter Globale AWS -Infrastruktur.

Outposts-Server enthalten Instance-Speicher-Volumes, unterstützen jedoch keine Amazon EBS-Volumes. Die Daten auf den Instance-Speicher-Volumes bleiben nach einem Neustart der Instance erhalten, nicht aber nach dem Beenden der Instance. Um die langfristigen Daten auf Ihren Instance-Speicher-Volumes über die Lebensdauer der Instance hinaus beizubehalten, sollten Sie sicherstellen, dass Sie die Daten in einem persistenten Speicher sichern, z. B. einem Amazon-S3-Bucket oder einem Netzwerkspeichergerät in Ihrem On-Premises-Netzwerk.

Konformitätsprüfung für AWS Outposts

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

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

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

- 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 HIPAA-fähige Anwendungen erstellen AWS können.

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

- AWS Compliance-Ressourcen — Diese Sammlung von Arbeitsmappen und Leitfäden gilt möglicherweise für Ihre Branche und Ihren Standort.
- AWS Leitfäden zur Einhaltung von Vorschriften für Kunden — Verstehen Sie das Modell der gemeinsamen Verantwortung aus dem Blickwinkel der Einhaltung von Vorschriften. In den Leitfäden werden die bewährten Verfahren zur Sicherung zusammengefasst AWS-Services und die Leitlinien den Sicherheitskontrollen in verschiedenen Frameworks (einschließlich des National Institute of Standards and Technology (NIST), des Payment Card Industry Security Standards Council (PCI) und der International Organization for Standardization (ISO)) zugeordnet.
- Evaluierung von Ressourcen anhand von Regeln im AWS Config Entwicklerhandbuch — Der AWS Config Service bewertet, wie gut Ihre Ressourcenkonfigurationen den internen Praktiken, Branchenrichtlinien und Vorschriften entsprechen.
- AWS Security Hub— Auf diese AWS-Service Weise erhalten Sie einen umfassenden Überblick über Ihren internen Sicherheitsstatus. AWS Security Hub verwendet Sicherheitskontrollen, um Ihre AWS -Ressourcen zu bewerten und Ihre Einhaltung von Sicherheitsstandards und bewährten Methoden zu überprüfen. 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 wie PCI DSS zu erfüllen, indem es die in bestimmten Compliance-Frameworks vorgeschriebenen Anforderungen zur Erkennung von Eindringlingen erfüllt.
- AWS Audit Manager— Auf diese AWS-Service Weise können Sie Ihre AWS Nutzung kontinuierlich überprüfen, um das Risikomanagement und die Einhaltung von Vorschriften und Industriestandards zu vereinfachen.

Überwachen eines Outpost

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

CloudWatch -Metriken

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

CloudTrail -Protokolle

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

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

VPC-Flow-Protokolle

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

Datenverkehrsspiegelung

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

AWS Health Dashboard

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

CloudWatch -Metriken für AWS Outposts

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

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

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

Inhalt

Outpost-Metriken

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

`ConnectedStatus`

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

Einheit: Anzahl

Maximale Auflösung: 1 Minute

Statistiken: Die nützlichste Statistik ist `Average`.

Dimensionen: `OutpostId`

`CapacityExceptions`

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

Einheit: Anzahl

Maximale Auflösung: 5 Minuten

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

Dimensionen: `InstanceType` und `OutpostId`

`InstanceFamilyCapacityAvailability`

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

Einheit: Prozent

Maximale Auflösung: 5 Minuten

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

Dimensionen: `InstanceFamily` und `OutpostId`

`InstanceFamilyCapacityUtilization`

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

Einheit: Prozent

Maximale Auflösung: 5 Minuten

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

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

`InstanceTypeCapacityAvailability`

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

Einheit: Prozent

Maximale Auflösung: 5 Minuten

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

Dimensionen: `InstanceType` und `OutpostId`

`InstanceTypeCapacityUtilization`

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

Einheit: Prozent

Maximale Auflösung: 5 Minuten

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

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

`UsedInstanceType_Count`

Die Anzahl der Instance-Typen, die derzeit verwendet werden, einschließlich aller Instance-Typen, die von Managed Services wie Amazon Relational Database Service (Amazon RDS) oder Application Load Balancer verwendet werden. Diese Metrik beinhaltet keine Kapazität für Dedicated Hosts, die auf dem Outpost konfiguriert sind.

Einheit: Anzahl

Maximale Auflösung: 5 Minuten

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

`AvailableInstanceType_Count`

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

Einheit: Anzahl

Maximale Auflösung: 5 Minuten

Dimensionen: `InstanceType` und `OutpostId`

`AvailableReservedInstances`

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

Einheit: Anzahl

Maximale Auflösung: 5 Minuten

Dimensionen: `InstanceType` und `OutpostId`

`UsedReservedInstances`

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

Einheit: Anzahl

Maximale Auflösung: 5 Minuten

Dimensionen: `InstanceType` und `OutpostId`

`TotalReservedInstances`

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

Einheit: Anzahl

Maximale Auflösung: 5 Minuten

Dimensionen: `InstanceType` und `OutpostId`

Outpost-Metrikdimensionen

Verwenden Sie Ihren Outpost, um die Metriken für Ihre zu filtern.

Dimension	Beschreibung
`Account`	Das Konto oder der Dienst, der die Kapazität verwendet.
`InstanceFamily`	Die Instance-Familie.
`InstanceType`	Der Instance-Typ.
`OutpostId`	Die ID des Outpost.
`VolumeType`	Der EBS-Volume-Typ.
`VirtualInterfaceId`	Die ID des virtuellen Gateways oder des Service Link Virtual Interface (VIF).
`VirtualInterfaceGroupId`	Die ID der virtuellen Schnittstellengruppe für das virtuelle Interface (VIF) des lokalen Gateways.

Anzeigen von CloudWatch Metriken für Ihren Outpost

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

So zeigen Sie Metriken mit der CloudWatch Konsole an

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

So zeigen Sie Metriken mit der AWS CLI

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

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

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

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

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

Protokollieren von AWS Outposts-API-Aufrufen mit AWS CloudTrail

AWS Outposts ist in integriert, einem ServiceAWS CloudTrail, der die Aktionen eines Benutzers, einer Rolle oder eines -AWSServices in aufzeichnetAWS Outposts. CloudTrail erfasst alle API-Aufrufe für AWS Outposts als Ereignisse. Zu den erfassten Aufrufen gehören Aufrufe von der AWS Outposts-Konsole und Code-Aufrufe der AWS Outposts-API-Operationen. Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Bereitstellung von CloudTrail Ereignissen an einen S3-Bucket aktivieren, einschließlich Ereignissen für AWS Outposts. Wenn Sie keinen Trail konfigurieren, können Sie trotzdem die neuesten Ereignisse in der CloudTrail Konsole unter Ereignisverlauf

anzeigen. Anhand der von CloudTrailgesammelten Informationen können Sie die an gestellte AnfrageAWS Outposts, die IP-Adresse, von der die Anfrage gestellt wurde, den Initiator der Anfrage, den Zeitpunkt der Anfrage und zusätzliche Details bestimmen.

Weitere Informationen zu CloudTrailfinden Sie im AWS CloudTrail -Benutzerhandbuch.

AWS Outposts -Informationen in CloudTrail

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

Zur kontinuierlichen Aufzeichnung von Ereignissen in Ihrem AWS-Konto, einschließlich Ereignissen für AWS Outposts, erstellen Sie einen Trail. Ein Trail ermöglicht CloudTrail die Bereitstellung von Protokolldateien an einen S3-Bucket in der übergeordneten AWS-Region. Wenn Sie ein Trail in der Konsole anlegen, gilt dieser für alle AWS-Regionen. Der Trail protokolliert Ereignisse aus allen Regionen in der AWS-Partition und stellt die Protokolldateien für den von Ihnen angegebenen S3 Bucket bereit. Darüber hinaus können Sie andere -AWSServices konfigurieren, um die in den CloudTrail Protokollen erfassten Ereignisdaten weiter zu analysieren und entsprechend zu agieren. Weitere Informationen finden Sie hier:

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

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

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

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

Weitere Informationen finden Sie unter CloudTrail -Element userIdentity.

Grundlagen zu AWS Outposts-Protokolldateieinträgen

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

Das folgende Beispiel zeigt einen - CloudTrail Protokolleintrag, der die `CreateOutpost` Aktion demonstriert.

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

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

Outpost-Wartung

Im Rahmen des Modells der der 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 außerdem die Leistung, den Zustand und die Kennzahlen Ihres Outposts und stellt fest, ob Wartungsarbeiten erforderlich sind.

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

Inhalt

Hardware-Wartung

Wenn ein AWS irreparables Problem mit der Hardware festgestellt wird, auf der Amazon EC2 EC2-Instances gehostet werden, die auf Ihrem Outpost ausgeführt werden, werden wir den Eigentümer des Outposts und den Eigentümer der Instances darüber informieren, dass die betroffenen Instances stillgelegt werden sollen. Weitere Informationen finden Sie unter Instance-Typen im Amazon EC2-Benutzerhandbuch.

AWS beendet die betroffenen Instances am Auslaufdatum der Instance. Die Daten auf Instance-Speicher-Volumes bleiben nach Beendigung der Instance nicht erhalten. Daher ist es wichtig, dass Sie vor dem Datum für die Außerbetriebnahme Ihrer Instance Maßnahmen ergreifen. Übertragen Sie zunächst Ihre langfristigen Daten von den Instance-Speicher-Volumes für jede betroffene Instance in

einen persistenten Speicher, z. B. einen Amazon S3-Bucket oder ein Netzwerkspeichergerät in Ihrem Netzwerk.

Ein Ersatzserver wird an den Outpost-Standort geliefert. Führen Sie dann die folgenden Schritte aus:

- Entfernen Sie die Netzwerk- und Stromkabel vom irreparablen Server und entfernen Sie ihn gegebenenfalls aus Ihrem Rack.
- Installieren Sie den Ersatzserver am selben Standort. Folgen Sie den Installationsanweisungen unter Outpost-Serverinstallation.
- Verpacken Sie den irreparablen Server AWS in derselben Verpackung, in der der Ersatzserver geliefert wurde.
- Verwenden Sie das frankierte Rücksendeetikett, das in der Konsole verfügbar ist und den Konfigurationsdetails der Bestellung oder der Ersatzserverbestellung beigefügt ist.
- Bringen Sie den Server zurück zu. AWS Weitere Informationen finden Sie unter Rückgabe eines AWS Outposts -Servers.

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.

Bewährte Methoden für AWS Outposts Strom- und Netzwerkereignisse

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

Stromereignisse

Bei vollständigen Stromausfällen besteht das inhärente Risiko, dass eine AWS Outposts Ressource nicht automatisch wieder in Betrieb genommen wird. Zusätzlich zur Bereitstellung redundanter

Stromversorgungs- und Notstromversorgungslösungen empfehlen wir, dass Sie im Voraus Folgendes tun, um die Auswirkungen einiger der schlimmsten Szenarien zu minimieren:

- Verschieben Sie Ihre Services und Anwendungen kontrolliert von den Outposts-Geräten, indem Sie DNS-basierte oder Off-Rack-Load-Balancing-Änderungen verwenden.
- Stoppen Sie Container, Instances und Datenbanken in einer inkrementellen Reihenfolge und verwenden Sie bei der Wiederherstellung die umgekehrte Reihenfolge.
- Testpläne für das kontrollierte Verschieben oder Stoppen von Diensten.
- Sichern Sie wichtige Daten und Konfigurationen und speichern Sie sie außerhalb der Outposts.
- Beschränken Sie Stromausfallzeiten auf ein Minimum.
- Vermeiden Sie während der Wartung ein wiederholtes Ausschalten der Stromversorgungen (Aus-Ein-Aus-Ein).
- 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.

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 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:

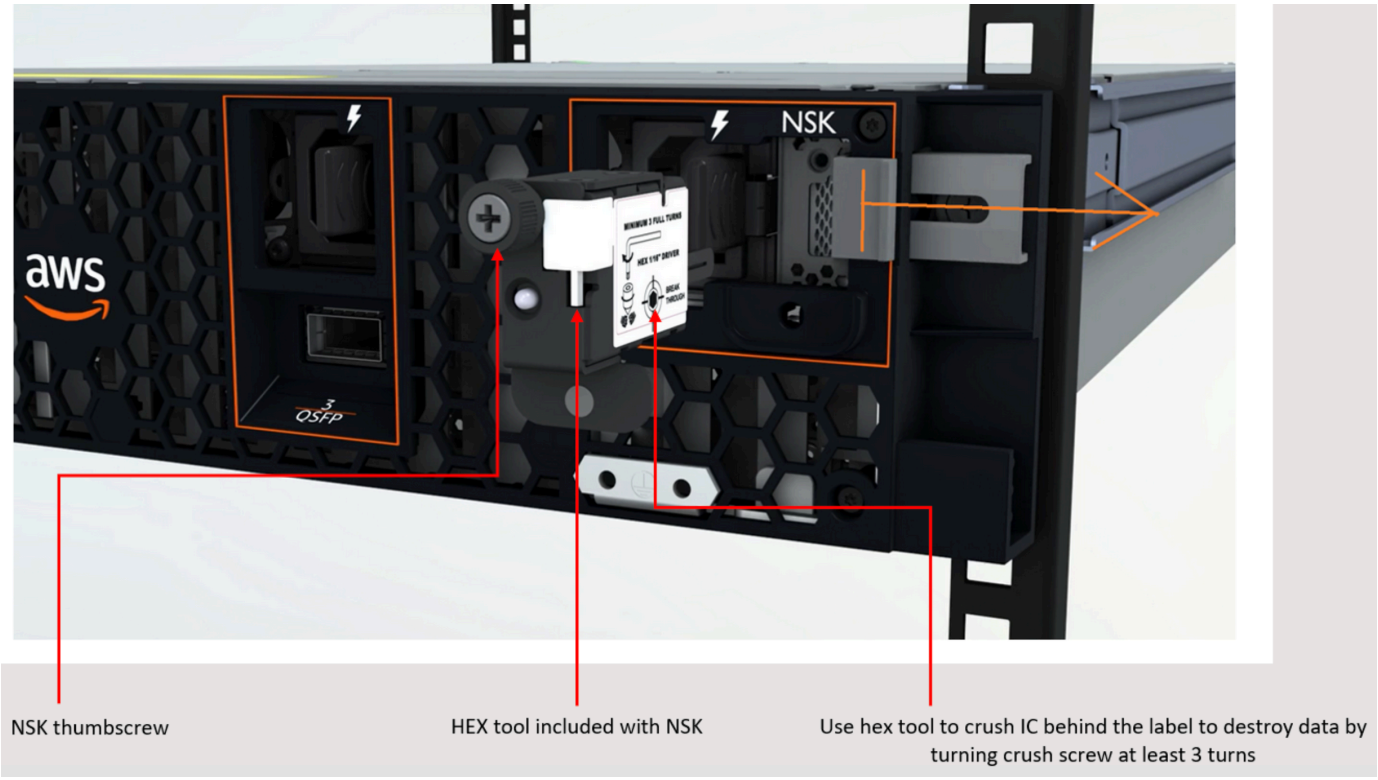
- Der AWS Blog Bewährte Methoden zur Überwachung AWS Outposts befasst sich mit bewährten Methoden zur Beobachtbarkeit und zum Eventmanagement speziell für Outposts.
- Der AWS Blog Debugging-Tool für Netzwerkkonnektivität von Amazon VPC erklärt das VPC-Tool AWSSupport -SetupIP. MonitoringFrom Dieses Tool ist ein AWS Systems Manager -Dokument (SSM-Dokument), das eine Amazon EC2 Monitor-Instance in einem von Ihnen angegebenen Subnetz erstellt und Ziel-IP-Adressen überwacht. Das Dokument führt Ping-, MTR-, TCP-Trace-Route- und Trace-Path-Diagnosetests durch und speichert die Ergebnisse in Amazon CloudWatch Logs, die in einem CloudWatch Dashboard visualisiert werden können (z. B. Latenz, Paketverlust). Für die Überwachung von Outposts sollte sich die Monitor-Instance in einem Subnetz der übergeordneten AWS Region befinden und so konfiguriert sein, dass sie eine oder mehrere Ihrer Outpost-Instances mithilfe ihrer privaten IP (s) überwacht. Dadurch werden Diagramme zum Paketverlust und zur Latenz zwischen AWS Outposts und der übergeordneten Region angezeigt. AWS
- Der AWS Blog Deploying an automated Amazon CloudWatch dashboard for AWS OutpostsAWS CDK use beschreibt die Schritte zur Bereitstellung eines automatisierten Dashboards.
- Wenn Sie Fragen haben oder weitere Informationen benötigen, finden Sie weitere Informationen unter Erstellen eines Support-Falls im Support-Benutzerhandbuch für AWS .

Kryptografisch geschredderte Serverdaten

Der Nitro Security Key (NSK) ist erforderlich, um Daten auf dem Server zu entschlüsseln. Wenn Sie den Server an zurückgeben AWS, entweder weil Sie den Server austauschen oder den Service einstellen, können Sie den NSK zerstören, um die Daten auf dem Server kryptografisch zu vernichten.

Um Daten auf dem Server kryptografisch zu vernichten

1. Entfernen Sie den NSK vom Server, bevor Sie den Server wieder an ihn zurückschicken. AWS
2. Stellen Sie sicher, dass Sie über das richtige NSK verfügen, das mit dem Server geliefert wurde.
3. Entfernen Sie das kleine Sechskantwerkzeug / den Inbusschlüssel unter dem Aufkleber.
4. Verwenden Sie das Sechskantwerkzeug, um die kleine Schraube unter dem Aufkleber drei volle Umdrehungen zu drehen. Diese Aktion zerstört den NSK und vernichtet kryptografisch alle Daten auf dem Server.



AWS Outposts end-of-term Optionen

Am Ende Ihrer AWS Outposts Amtszeit haben Sie drei Möglichkeiten:

- Verlängern Sie Ihr Abonnement und behalten Sie Ihren vorhandenen Outpost.
- Beenden Sie Ihr Abonnement und geben Sie Ihren Outpost-Server zurück.
- Wechseln Sie zu einem month-to-month Abonnement und behalten Sie Ihren bestehenden Outpost-Server.

Themen

Verlängern Sie Ihr Abonnement

So verlängern Sie Ihr Abonnement und behalten Ihren vorhandenen Outpost-Server:

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

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

- Komplette Vorauszahlung

Die Preise finden Sie unter AWS Outposts -Serverpreise. 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 Ihren Outpost-Server zurückgeben möchten, wird Ihr month-to-month Abonnement automatisch in ein Abonnement umgewandelt. Ihr Outpost wird monatlich zum Tarif der Zahlungsoption „Keine Vorauszahlung“ verlängert, die Ihrer Konfiguration entspricht. AWS Outposts Ihr neues monatliches Abonnement beginnt am Tag nach Ablauf Ihres aktuellen Abonnements.

Beenden Sie Ihr Abonnement und geben Sie den Server zurück

> **Important**
>
> AWS Sie können den Rückgabevorgang erst starten, wenn Sie das folgende Verfahren abgeschlossen haben. Nachdem Sie einen Support-Fall eröffnet haben, um Ihr Abonnement zu beenden, können wir den Rückgabeprozess nicht mehr stoppen.

So beenden Sie Ihr Abonnement:

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

1. Melden Sie sich bei der AWS Support -Center-Konsole an.
2. Wählen Sie Create case (Fall erstellen) aus.
3. Wählen Sie Konto und Fakturierung aus.

4. Wählen Sie als Service Fakturierung aus.
5. Wählen Sie als Kategorie die Option Andere Fragen zur Rechnungsstellung aus.
6. Wählen Sie als Schweregrad die Option Wichtige Frage aus.
7. Wählen Sie Next step: Additional information (Nächster Schritt: Zusätzliche Informationen).
8. Geben Sie auf der Seite Zusätzliche Informationen für Betreff eine eindeutige Anfrage ein, z. B. **`End my Outpost subscription`**
9. Geben Sie unter Beschreibung das Datum ein, an dem Sie Ihr Abonnement beenden möchten.
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. Falls erforderlich, sichern Sie alle auf Ihrem Server vorhandenen Instanzen und Instanzdaten.
14. Beenden Sie die auf Ihrem Server gestarteten Instances.
15. Überprüfen Sie Ihre Falldetails und wählen Sie Submit (Absenden) aus. Ihre Fall-ID-Nummer und Übersicht werden angezeigt.
16. Fahren Sie den Server NICHT herunter und trennen Sie ihn NICHT vom Netzwerk, bis Sie im Support-Fall dazu aufgefordert werden.

Um Ihren AWS Outposts Server zurückzugeben, folgen Sie den Anweisungen unter AWS Outposts Server zurückgeben.

In ein month-to-month Abonnement umwandeln

Um zu einem month-to-month Abonnement zu wechseln und Ihren bestehenden Outpost-Server beizubehalten, sind keine weiteren Schritte erforderlich. Wenn Sie Fragen haben, öffnen Sie eine Support-Anfrage für die Abrechnung.

Ihr Outpost wird monatlich zum Tarif der Zahlungsoption „Keine Vorauszahlung“ erneuert, die Ihrer Konfiguration entspricht. AWS Outposts Ihr neues monatliches Abonnement beginnt am Tag nach Ablauf Ihres aktuellen Abonnements.

Kontingente für AWS Outposts

DasAWS-Konto verfügt über Standardkontingente (früher als Limits bezeichnet) für jedenAWS-Service. Wenn nicht anders angegeben, gilt jedes Kontingent spezifisch für eine Region. Sie können Erhöhungen für einige Kontingente beantragen, aber nicht für alle Kontingente.

Um die Kontingente für AWS Outposts anzuzeigen, öffnen Sie die Service-Quotas-Konsole. Wählen Sie im Navigationsbereich aus und wählen AWS-ServicesSie aus AWS Outposts.

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

Ihr AWS-Konto umfasst die folgenden Kontingente für AWS Outposts.

Ressource	Standard	Anpassbar	Kommentare
Outpost-Standorte	100	Ja	Ein Outpost-Standort ist das vom Kunden verwaltete physische Gebäude, in dem Sie Ihre Outpost-Geräte mit Strom versorgen und an das Netzwerk anschließen. Du kannst in jeder Region deinesAWS Accounts 100 Outposts-Standorte haben.
Outposts pro Standort	10	Ja	AWS Outpostsumfassen Hardware und virtuelle Ressourcen, die als Outposts bekannt sind. Dieses Kontingent schränkt Ihre virtuellen Outpost-Ressourcen ein. Du kannst auf jeder Außenposten-Websit e 10 Outposts haben.

AWS Outpostsund die Kontingente für andere Dienstleistungen

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

Dokumentverlauf

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

Änderung	Beschreibung	Datum
Kapazitätsmanagement	Sie können die Standardk apazitätskonfiguration für Ihre neue Outposts-Bestellung ändern.	16. April 2024
nd-of-term E-Optionen für Server AWS Outposts	Am Ende Ihrer AWS Outposts Laufzeit können Sie Ihr Abonnement verlängern, beenden oder umwandeln.	1. August 2023
AWS Outposts Benutzerl eitfaden für Outposts erstellt	AWS Outposts Das Benutzerh andbuch ist in separate Anleitungen für Rack und Server aufgeteilt.	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
Einführung von Outpost-S ervern	Outposts-Server hinzugefü gt, ein neuer AWS Outposts Formfaktor.	30. November 2021

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.