Benutzerhandbuch für Outposts-Server

AWS Outposts

AWS Outposts: Benutzerhandbuch für Outposts-Server

Table of Contents

Was ist AWS Outposts?

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

Ein Outpost ist ein Pool von AWS Rechen- und Speicherkapazitäten, 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 über private IP-Adressen, die sich alle innerhalb derselben befinden. VPC

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

Weitere Informationen finden Sie auf der AWS Outposts -Produktseite.

Die wichtigsten Konzepte

Dies sind die wichtigsten Konzepte für. AWS Outposts

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

- Outposts-Racks – Ein Outpost-Formfaktor, bei dem es sich um ein 42U-Rack nach Branchenstandard handelt. Zu den Racks von Outposts gehören rackmontierbare Server, Switches, ein Netzwerk-Patchpanel, ein Power-Shelf und leere Panels.
- Outposts-Server — Ein Outpost-Formfaktor, bei dem es sich um einen 1U- oder 2U-Server nach Industriestandard handelt, der in einem standardmäßigen EIA -310D 19-konformen 4-Post-Rack installiert werden kann. Outposts-Server bieten lokale Rechen- und Netzwerkdienste für Standorte mit begrenztem Platzbedarf oder geringeren Kapazitätsanforderungen.
- Outpost-Inhaber — Der Kontoinhaber für das Konto, das die Bestellung aufgibt. AWS Outposts Nach AWS der Kontaktaufnahme mit dem Kunden kann der Eigentümer weitere Ansprechpartner angeben. AWS wird mit den Kontakten kommunizieren, um Bestellungen, Installationstermine sowie Wartung und Austausch der Hardware zu klären. Wenden Sie sich an das AWS Support Center, falls sich die Kontaktinformationen ändern.
- Servicelink — Netzwerkroute, die die Kommunikation zwischen Ihrem Außenposten und der zugehörigen AWS Region ermöglicht. Jeder Outpost ist eine Erweiterung einer Availability Zone und der zugehörigen Region.
- Lokales Gateway (LGW) — Ein virtueller Router mit logischer Verbindung, der die Kommunikation zwischen einem Outposts-Rack und Ihrem lokalen Netzwerk ermöglicht.
- Lokale Netzwerkschnittstelle — Eine Netzwerkschnittstelle, die die Kommunikation von einem Outposts-Server und Ihrem lokalen Netzwerk aus ermöglicht.

AWS Ressourcen auf Outposts

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

Datenverarbeitung

Ressourcentyp	Racks	Server
EC2Amazon-Instanzen	 Ja	 Ja

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

Datenbank und Analytik

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

Netzwerk

Ressourcentyp	Racks	Server
App Mesh Envoy-Proxy	 Ja	 Ja

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

Speicher

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

Andere AWS-Services

Service	Racks	Server
AWS IoT Greengrass	 Ja	 Ja

Service	Racks	Server
Amazon SageMaker Edge-Manager	 Ja	 Ja

Preisgestaltung

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

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

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

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

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

Wie AWS Outposts funktioniert

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

Das folgende Diagramm veranschaulicht beide Outpost-Formfaktoren.

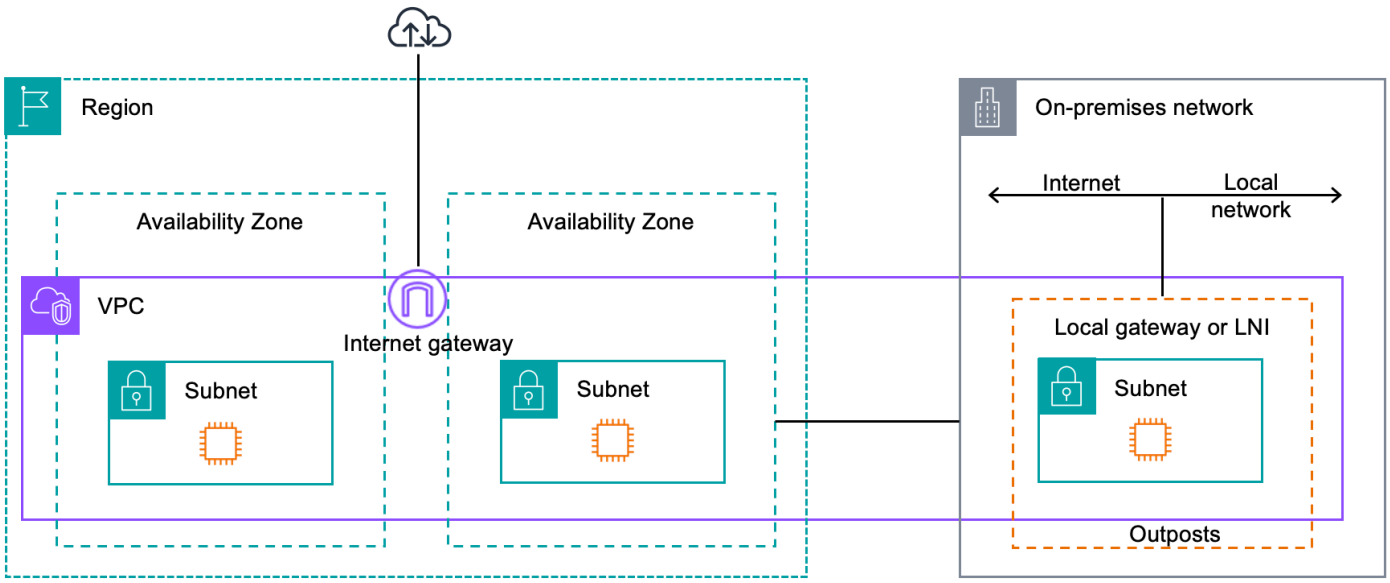
Inhalt

Netzwerkkomponenten

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

Das folgende Diagramm zeigt die Netzwerkkomponenten für Ihren Outpost.

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



VPCsund Subnetze

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

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

Jeder Outpost kann mehrere unterstützenVPCs, die über ein oder mehrere Outpost-Subnetze verfügen können. Informationen zu VPC Kontingenten finden Sie unter VPCAmazon-Kontingente im VPCAmazon-Benutzerhandbuch.

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

Routing

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

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

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

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

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

DNS

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

Abhängig von der Pfadlatenz zwischen Ihrem Outpost und der Region kann es bei Route 53 zu längeren DNS Lösungszeiten kommen. AWS In solchen Fällen können Sie die lokal in Ihrer lokalen Umgebung installierten DNS Server verwenden. Um Ihre eigenen DNS Server zu verwenden, müssen Sie DHCP Optionssätze für Ihre lokalen DNS Server erstellen und diese den zuordnen. VPC Sie müssen außerdem sicherstellen, dass IP-Konnektivität zu diesen DNS Servern besteht. Möglicherweise müssen Sie der lokalen Gateway-Routingtabelle auch Routen hinzufügen, um die Erreichbarkeit zu gewährleisten. Dies ist jedoch nur eine Option für Outposts-Racks mit

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

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

Service Link

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

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

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

Lokale Netzwerkschnittstellen

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

Standortanforderungen für Outposts-Server

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

Inhalt

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 (oder einem höheren) Filter 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 zu sehen, wählen Sie in der AWS Outposts Konsole unter https://console.aws.amazon.com/outposts/Katalog durchsuchen aus.
- Kompatibilität mit Rail-Kits — Das in Ihrem Versandpaket enthaltene Schienen-Kit ist mit einer L-förmigen Standard-Montagehalterung eines EIA -310-D-konformen 19-Zoll-Racks kompatibel. Das Schienenkit ist nicht mit einer U-förmigen Montagehalterung kompatibel, wie in der folgenden Abbildung gezeigt.

- Rack-Platzierung — Wir empfehlen die Verwendung von 19-Zoll-Standardracks des EIA Typs -310D mit einer Tiefe von mindestens 36 Zoll (914 mm). AWS bietet ein Schienenkit für die Rackmontage des Servers.
  - Outposts 2U-Server benötigen Platz 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)
  - 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

  Wenn Sie den Server nicht in einem Rack platzieren, müssen Sie trotzdem die anderen Standortanforderungen erfüllen.
- Wartungsfreundlichkeit – Outposts-Server können beim Kunden gewartet werden.
- Akustik — Nennleistung von weniger als 78 dBA bei Temperaturen von 80 °F (27 °C) und erfüllt die CORE NEBS GR-63-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-Verkehr — QSFP + Breakout-Kabel (10 Fuß/3 m) segmentiert den Verkehr.

Service Link-Firewall

UDPund TCP 443 muss statusmäßig in der Firewall aufgeführt sein.

Protokoll	Quell-Port	Quelladresse	Ziel-Port	Zieladresse
UDP	1024 - 65535	Service-Link-IP	53	DHCPbereitgestellter Server DNS
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 für Service Link () MTU

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

Empfehlungen für die Bandbreite von Service Links

Für eine optimale Benutzererfahrung und Ausfallsicherheit AWS müssen Sie für die Service Link-Verbindung mit der AWS Region eine redundante Konnektivität von mindestens 500 Mbit/s und eine maximale Roundtrip-Latenz von 175 ms verwenden. Die maximale Auslastung für jeden Outposts-Server beträgt 500 Mbit/s. Verwenden Sie mehrere Outposts-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-Verkehr für Server im AWS Outposts Benutzerhandbuch für Server.

Ihre AWS Outposts Service Link-Bandbreitenanforderungen variieren je nach Workload-Merkmalen wie AMI Größe, Anwendungselastizität, Burst-Geschwindigkeitsanforderungen und VPC Amazon-Traffic in die Region. Beachten Sie, dass AWS Outposts Server nicht zwischenspeichernAMIs. AMIswerden 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.

Für den Service Link ist eine DHCP Antwort erforderlich

Für den Service Link ist eine IPv4 DHCP Antwort erforderlich, um die Netzwerkeinstellungen zu konfigurieren.

Maximale Latenz von Service Link

Service Links können eine maximale Netzwerklatenz von bis zu 175 ms vom Server und seiner Availability Zone aus unterstützen.

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/Katalog durchsuchen aus.

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 USA benötigen Sie ein IEC C13-5-15P-Netzkabel. NEMA

- In Teilen Europas benötigen Sie möglicherweise ein Netzkabel vom Typ IEC C13 bis CEE 7/7.
- In Indien benötigen Sie ein IEC C13-Netzkabel. IS1293

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 (). UPS

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 Service Link-Verkehr für Server im AWS Outposts Benutzerhandbuch für Server.

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

Erste Schritte mit

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

Aufgaben

- Erstellen eines Outpost und Bestellung von Outpost-Kapazitäten
- Starten Sie eine Instanz auf Ihrem Outposts-Server

Erstellen eines Outpost und Bestellung von Outpost-Kapazitäten

Um mit der Nutzung zu beginnen AWS Outposts, melden Sie sich mit Ihrem AWS Konto an. 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 Outposts-Server.
- Sie müssen über einen AWS Enterprise Support Plan oder einen AWS Enterprise On-Ramp Support Plan verfügen.
- Bestimme, welche AWS-Konto du verwenden wirst, um die Outposts-Website zu erstellen, erstelle den Outpost und gib die Bestellung auf. Suchen Sie in der mit diesem Konto verknüpften E-Mail-Adresse nach Informationen von. AWS

Aufgaben

- Schritt 1: Erstellen eines Standorts
- Schritt 2: Erstellen eines Outpost
- Schritt 3: Bestellung
- Schritt 4: Ändern Sie die 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. Melden Sie sich an bei. AWS
2. Öffnen Sie die AWS Outposts Konsole unter https://console.aws.amazon.com/outposts/.
3. Um das übergeordnete Element auszuwählen AWS-Region, verwenden Sie die Regionsauswahl in der oberen rechten Ecke der Seite.
4. Wählen Sie im Navigationsbereich Standorte aus.
5. Wählen Sie Create site (Standort erstellen).
6. Wählen Sie unter Unterstützter Hardwaretyp die Option 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 anderen 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.

> **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 das AWS Support Center.

Voraussetzungen

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

Schritt 4: Ändern Sie die Instance-Kapazität

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

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

Um die Instanzkapazität zu ändern

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

Console steps

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

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

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

Upload JSON file

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

   Example

   JSONBeispieldatei:

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

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

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

Nächste Schritte

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

Um die Bestellung zu erfüllen, vereinbaren AWS wir 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 durchführen oder einen Vertrag mit einem Drittanbieter abschließen, erfordert die Installation IAM Anmeldeinformationen in der AWS-Konto Datei, die 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 in der Serverinstallationsanleitung.

Die Installation ist abgeschlossen, wenn EC2 Amazon-Kapazität für Ihren Outpost bei Ihrem AWS-Konto verfügbar ist. Sobald die Kapazität verfügbar ist, können Sie EC2 Amazon-Instances auf Ihrem Outposts starten. Weitere Informationen finden Sie unter the section called “Starten einer -Instance”.

Starten Sie eine Instanz auf Ihrem Outposts-Server

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

Sie können Outpost-Subnetze zu allen Subnetzen VPC in der AWS Region für den Outpost hinzufügen. Wenn du das tust, erstreckt sich das VPC auch über den Außenposten. Weitere Informationen finden Sie unter Netzwerkkomponenten.

> **Note**
>
> Wenn Sie eine Instance in einem Outpost-Subnetz starten, das von einem anderen AWS-Konto für Sie freigegeben wurde, fahren Sie mit fort. Schritt 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 umgeleitet, um ein Subnetz in der VPC Amazon-Konsole zu erstellen. Wir wählen für Sie den Outpost und die Availability Zone aus, in der sich der Outpost befindet.
4. Wählen Sie einen VPC und geben Sie einen IP-Adressbereich für das Subnetz an.
5. Wählen Sie Create (Erstellen) aus.
6. Nachdem das Subnetz erstellt wurde, müssen Sie das Subnetz für lokale Netzwerkschnittstellen aktivieren. Sie verwenden den Befehl modify-subnet-attribute in der AWS CLI. 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. Im folgenden Beispiel wird der Wert 1 verwendet, um eine sekundäre Netzwerkschnittstelle anzugeben.

```
aws ec2 modify-subnet-attribute \
    --subnet-id subnet-1a2b3c4d \
```

```
    --enable-lni-at-device-index 1
```

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

Überlegungen

- Instanzen auf Outposts-Servern beinhalten 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 Store Volumes und Create an Instance Store-Backed AMI im EC2Amazon-Benutzerhandbuch.
- Sie müssen ein EBS Amazon-gestütztes Gerät AMI mit nur einem einzigen EBS Snapshot verwenden. AMIsmit mehr als einem EBS 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 EC2 Amazon-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 Geräteindex der lokalen Netzwerkschnittstelle für das Outpost-Subnetz angegeben haben, ist diese Netzwerkschnittstelle die lokale Netzwerkschnittstelle für die Instance. Informationen zum späteren Hinzufügen finden Sie auch unter. Lokale Netzwerkschnittstelle hinzufügen
7. Schließen Sie den Assistenten ab, um die Instance in Ihrem Outpost-Subnetz zu starten. Weitere Informationen finden Sie unter Launch an EC2 Instance im EC2Amazon-Benutzerhandbuch:

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 Lokale Netzwerkschnittstelle hinzufügen.

Sie müssen die lokale Netzwerkschnittstelle für die Instance mit einer IP-Adresse aus Ihrem lokalen Netzwerk konfigurieren. In der Regel verwenden Sie dazuDHCP. 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 von einem Computer in Ihrem lokalen Netzwerk aus 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 EC2 Instance finden Sie unter Verbindung zu Ihrer EC2 Instance herstellen im EC2Amazon-Benutzerhandbuch.

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

```
ping 172.16.0.130
```

Es folgt eine Beispielausgabe.

```
Pinging 172.16.0.130

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

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

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

Testen Sie die Konnektivität zwischen der AWS Region und dem Outpost

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

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

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

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

   ```
   ping 10.0.1.5
   ```

   Es folgt eine Beispielausgabe.

   ```
   Pinging 10.0.1.5

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

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

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

AWS Outposts Konnektivität zu AWS Regionen

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

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

Inhalt

Konnektivität über Service Link

Während der AWS Outposts Bereitstellung erstellen Sie oder erstellen eine AWS Service Link-Verbindung, die Ihren Outposts-Server mit der von Ihnen ausgewählten AWS Region oder 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 Verkehr auf dem Service-Link zu segmentieren. Die Serviceverbindung VLAN ermöglicht die Kommunikation zwischen dem Außenposten und der AWS Region sowohl für die Verwaltung des Außenpostens als auch für den internen VPC Verkehr zwischen der AWS Region und dem Außenposten.

Der Außenposten ist in der Lage, die Serviceverbindung VPN zurück zur Region über öffentliche Konnektivität der AWS Region herzustellen. Dazu benötigt der Outpost Konnektivität zu den öffentlichen IP-Bereichen der AWS Region, entweder über das öffentliche Internet oder über eine AWS Direct Connect öffentliche virtuelle Schnittstelle. Diese Konnektivität kann über bestimmte Routen in der Service-Verbindung VLAN oder über eine Standardroute 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.
- Verkehr zwischen dem Outpost und allen damit verbundenen DatenVPCs, einschließlich Datenverkehr auf Kundendatenebene.

Anforderungen an die maximale Übertragungseinheit (MTU) für den Service Link

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

Empfehlungen für die Bandbreite von Service Links

Für ein optimales Erlebnis und eine optimale Ausfallsicherheit AWS müssen Sie für die Service Link-Verbindung zur Region eine redundante Konnektivität von mindestens 500 Mbit/s und eine maximale Roundtrip-Latenz von 175 ms verwenden. AWS Die maximale Auslastung für jeden Outposts-Server beträgt 500 Mbit/s. Verwenden Sie mehrere Outposts-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-Verkehr für Server.

Ihre AWS Outposts Service Link-Bandbreitenanforderungen variieren je nach Workload-Merkmalen wie AMI Größe, Anwendungselastizität, Burst-Geschwindigkeitsanforderungen und VPC Amazon-Traffic in die Region. Beachten Sie, dass AWS Outposts Server nicht zwischenspeichernAMIs. AMIswerden 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 Anforderungen erforderlichen Service-Link-Bandbreite zu erhalten.

Firewalls und der Service Link

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

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

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

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

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

Protokoll	Quell-Port	Quelladresse	Ziel-Port	Zieladresse
UDP	1024 - 65535	Service-Link-IP	53	DHCPbereitgestellter DNS Server
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 Outposts-Server und seiner übergeordneten AWS Region. Diese Netzwerkverbindung, die als Service Link bezeichnet wird, ist für die Verwaltung des Outposts unerlässlich, da sie den internen VPC Verkehr zwischen dem Outpost und der Region sicherstellt. 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 Outposts-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.

Einen Outposts-Server zurückgeben

Wenn AWS Outposts ein Defekt am Server festgestellt wird, informieren wir Sie, starten den Austauschprozess, um Ihnen einen neuen Server zu schicken, und stellen Ihnen das Versandetikett über die AWS Outposts Konsole zur Verfügung. Führen Sie zunächst die folgenden Schritte aus.

Aufgaben

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.

Schritt 1: Bereiten Sie den Server für die Rückgabe vor

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 disassociate-resource-shareBefehl 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 EC2 Amazon-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 Ihre Instance beenden im EC2Amazon-Benutzerhandbuch.

Schritt 2: Besorgen Sie sich das Rücksendeetikett

> **Important**
>
> Sie dürfen nur das mitgelieferte Versandetikett verwenden, da es spezifische Informationen, wie z. B. die Asset-ID, über den Server enthält, den Sie zurücksenden. 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.

Schritt 3: Packen Sie den Server

Verwenden Sie zum Verpacken Ihres Servers die von bereitgestellte Box und das Verpackungsmaterial AWS.

1. Verpacken Sie den Server in eines der folgenden Kartons:

- Die Box und das Verpackungsmaterial, in denen der Server ursprünglich geliefert wurde.
- Der Karton und das Verpackungsmaterial, in dem der Ersatzserver geliefert wurde.

Sie können sich auch an das AWS Support -Center wenden, um einen Karton anzufordern.

2. Bringen Sie das AWS mitgelieferte Versandetikett an der Außenseite des Kartons an.

> **Important**
>
> Stellen Sie sicher, dass die Asset-ID auf dem Versandetikett mit der Asset-ID auf dem Server übereinstimmt, den Sie zurücksenden.
> Die Asset-ID befindet sich auf der ausziehbaren Registerkarte an der Vorderseite des Servers. Beispiel: oder `1203779889 9305589922`

3. Verschließen Sie die Schachtel sicher.

Schritt 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
Bahrain	
Brasilien	
Brunei	
Kanada	
Chile	

Land	Kontakt
Kolumbien	• Eine Telefonnummer • Eine E-Mail-Adresse
Hong Kong	
Indien	
Indonesien	
Japan	
Malaysia	
Nigeria	
Oman	
Panama	
Peru	
Philippinen	
Serbien	
Singapur	
Südafrika	
Südkorea	
Taiwan	
Thailand	
Vereinigte Arabische Emirate	
Vietnam	

Land	Kontakt
United States of America	Kontakt UPS. Sie können den Server auf folgende Weise zurückgeben: • Geben Sie den Server während einer routinemäßigen UPS Abholung an Ihrem Standort zurück. • Geben Sie den Server an einem UPSStandort ab. • Vereinbaren Sie eine Abholung für ein Datum und eine Uhrzeit, die Sie bevorzugen. Geben Sie für den kostenlosen Versand die Sendungsverfolgungsnummer auf dem von AWS bereitgestellten Versandetikett ein.

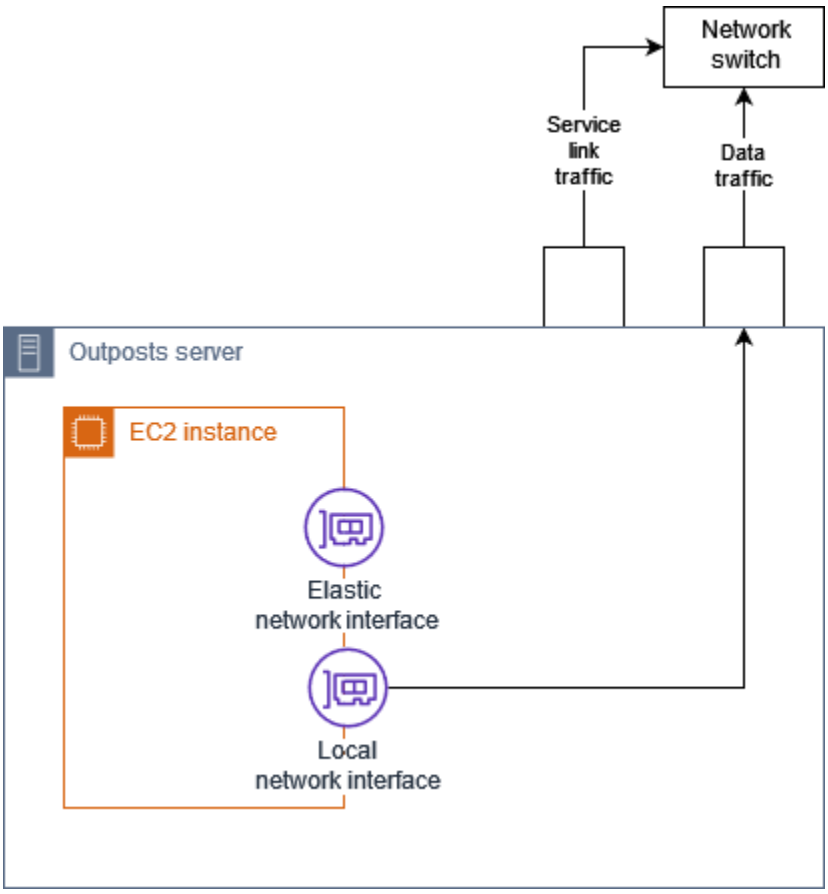
Land	Kontakt
Alle anderen Länder	Kontakt DHL. Sie können den Server auf folgende Weise zurückgeben: • Geben Sie den Server an einem DHLStandort ab. • Vereinbaren Sie eine Abholung für ein Datum und eine Uhrzeit, die Sie bevorzugen. Geben Sie für den DHL kostenlosen Versand die Frachtbriefnummer auf dem AWS mitgelief erten Versandetikett ein. Wenn Sie die folgende Fehlermeldung erhalten: `Courier pickup can't 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 für Ihre Outposts-Server

Bei Outposts-Servern ist eine lokale Netzwerkschnittstelle eine logische Netzwerkkomponente, die die EC2 Amazon-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 lokalen Netzwerk her, während die Netzwerkschnittstelle eine Verbindung zum herstellt. VPC Das folgende Diagramm zeigt eine EC2 Instanz 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 DHCP Optionssätze in a nicht verwendenVPC, 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 VPC Schnittstellen-Endpunkte für den Zugriff AWS-Services verwenden. 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. A VPC ist ein virtualisiertes Layer-3-Netzwerk. Lokale Netzwerkschnittstellen unterstützen VPC keine Netzwerkkomponenten. Zu diesen Komponenten gehören Sicherheitsgruppen, Netzwerkzugriffssteuerungslisten, virtualisierte Router oder Routing-Tabellen sowie Flussprotokolle. Die lokale Netzwerkschnittstelle bietet dem Outposts-Server keinen Einblick in VPC Layer-3-Datenflüsse. 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

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

- Eine lokale Netzwerkschnittstelle kann die primäre Netzwerkschnittstelle der Instanz nicht verwenden.
- Outposts-Server können mehrere EC2 Instanzen hosten, jede mit einer lokalen Netzwerkschnittstelle.

> **Note**
>
> EC2Instanzen 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 Outposts-Server ausgeführt werden.
- Lokale Netzwerkschnittstellen unterstützen weder den Promiscuous-Modus noch Adress-Spoofing. MAC

Leistung

Die lokale Netzwerkschnittstelle jeder Instanzgröße stellt einen Teil der verfügbaren physischen Bandbreite von 10 GbE bereit. In der folgenden Tabelle ist die Netzwerkleistung für jeden Instance-Typ aufgeführt:

Instance-Typ	Baseline-Bandbreite (Gbit/s)	Maximale Bandbreite (Gbit/s)
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 IhremVPC. Eine Sicherheitsgruppe kontrolliert den eingehenden und ausgehenden DatenverkehrVPC. Die lokale Netzwerkschnittstelle ist nicht an die angeschlossen. VPC 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 finden Sie unter Überwachen der Netzwerkleistung für ENA Einstellungen auf Ihrer EC2 Instance im EC2Amazon-Benutzerhandbuch.

MACAdressen

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.

Fügen Sie einer EC2 Instanz in einem Outposts-Subnetz eine lokale Netzwerkschnittstelle hinzu

Sie können einer EC2 Amazon-Instance in einem Outposts-Subnetz während oder nach dem Start eine lokale Netzwerkschnittstelle 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 den richtigen Geräteindex angeben, indem Sie stattdessen das AWS CLI oder ein verwenden. AWS SDK Verwenden Sie beispielsweise die folgenden Befehle aus AWS CLI: create-network-interfaceund. attach-network-interface

Gehen Sie wie folgt vor, um die lokale Netzwerkschnittstelle hinzuzufügen, nachdem Sie die Instance gestartet haben. Informationen zum Hinzufügen während des Instance-Starts finden Sie unter Starten einer Instance auf dem Outpost.

So fügen Sie einer Instance eine lokale Netzwerkschnittstelle hinzu EC2

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Klicken Sie im Navigationsbereich unter Netzwerk und Sicherheit auf Netzwerkschnittstellen.
3. 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 die IPv4Privatadresse auf Automatisch zuweisen eingestellt ist.

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

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

4. 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 Geräteindex für die lokale Netzwerkschnittstelle für das Outpost-Subnetz angegeben haben, ist diese Netzwerkschnittstelle die lokale Netzwerkschnittstelle für die Instance.

Sehen Sie sich die lokale Netzwerkschnittstelle an

Während sich die Instance im laufenden Zustand befindet, können Sie die EC2 Amazon-Konsole verwenden, um sowohl die elastic network interface 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 die lokale Netzwerkschnittstelle aus dem Subnetz an. CIDR Diese Adresse ist nicht die IP-Adresse der lokalen Netzwerkschnittstelle und kann nicht verwendet werden. Diese Adresse wird jedoch vom Subnetz aus zugewiesenCIDR, sodass Sie sie bei der Subnetzdimensionierung berücksichtigen müssen. Sie müssen die IP-Adresse für die lokale Netzwerkschnittstelle innerhalb des Gastbetriebssystems entweder statisch oder über Ihren Server festlegen. DHCP

Konfiguration des Betriebssystems

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

Lokale Netzwerkkonnektivität für Outposts-Server

Verwenden Sie dieses Thema, um die Netzwerkverkabelungs- und Topologieanforderungen für das Hosten eines Outposts-Servers zu verstehen. Weitere Informationen finden Sie unter Lokale Netzwerkschnittstellen für Ihre Outposts-Server.

Inhalt

Servertopologie in Ihrem Netzwerk

Ein Outposts-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.

In der folgenden Tabelle werden die Typen und Labels des Outposts-Serververkehrs beschrieben.

Datenverkehrskennzeichnung	Beschreibung
2	Service Link-Verkehr — Dieser Verkehr ermöglicht die Kommunikation zwischen dem Außenposten und der AWS Region sowohl für die Verwaltung des Außenpostens als auch für den internen VPC Verkehr zwischen der AWS Region und dem Außenposten. Der Service-Link-Datenverkehr umfasst die Service-Link-Verbindung vom Outpost zur Region. Der Service-Link ist benutzerdefiniert VPN oder führt VPNs vom Außenposten zur Region. Der Outpost stellt eine Verbindung zur Availabil

Datenverkehrskennzeichnung	Beschreibung
	ity Zone in der Region her, die Sie beim Kauf ausgewählt haben.
1	Link-Traffic über die lokale Netzwerks chnittstelle — Dieser Verkehr ermöglicht die Kommunikation von Ihrem VPC Gerät zu Ihrem lokalen Netzwerk 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 Outposts-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 Outposts-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. Beide Schnittstellen sind erforderlich, damit ein Outposts-Server funktioniert. Verwenden Sie die 2 Schnittstelle für den Service-Link-Verkehr und die 1 Schnittstelle für den Link-Verkehr über die lokale Netzwerkschnittstelle. 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

Die Service Link-Verbindung muss öffentlich DNS verfügbar sein, damit der Outpost seinen Registrierungsendpunkt in der Region ermitteln kann. AWS Die Verbindung kann über ein NAT Gerät zwischen dem Outposts-Server und dem Registrierungsendpunkt hergestellt werden. Weitere Informationen zu den öffentlichen Adressbereichen für AWS finden Sie unter AWS IP-Adressbereiche im VPCAmazon-Benutzerhandbuch und unter AWS Outposts Endpunkte und Kontingente im Allgemeine AWS-Referenz.

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

- TCP443
- UDP443
- UDP53

Uplink-Geschwindigkeit

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

Abhängig von Ihrer lokalen Netzwerkschnittstelle und der Auslastung der Servicelinks benötigen Sie möglicherweise einen schnelleren Uplink. Weitere Informationen finden Sie unter Bandbreitenempfehlungen für Service-Links.

Link-Verkehr über die lokale Netzwerkschnittstelle

Konfigurieren Sie den Link-Port der lokalen Netzwerkschnittstelle auf Ihrem Upstream-Netzwerkgerät als Standardzugriffsport zu einem in VLAN Ihrem lokalen Netzwerk. Wenn Sie mehr als einen habenVLAN, konfigurieren Sie alle Anschlüsse 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 Instanz 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 Datenverkehr. Wenn Sie Ihre lokale Netzwerkschnittstelle als Trunk konfigurieren, müssen Sie sicherstellen, dass Ihr Betriebssystem den VLAN Datenverkehr kennzeichnet.

Das folgende Beispiel zeigt, wie Sie VLAN Tagging für Ihre lokale Netzwerkschnittstelle auf Amazon Linux 2023 konfigurieren. Wenn Sie eine andere Linux-Distribution verwenden, finden Sie in der Dokumentation Ihrer Linux-Distribution Informationen zur Konfiguration von VLAN Tagging.

Beispiel: So konfigurieren Sie VLAN Tagging für Ihre lokale Netzwerkschnittstelle auf Amazon Linux 2023 und Amazon Linux 2

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 Schnittstellenname der lokalen Netzwerkschnittstelle lautet `ens6`
   - Die VLAN ID ist `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 192.168.59.0/24 ist. CIDR

   ```
   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
   ```

Informationen zur Konfiguration Ihrer Netzwerkschnittstellen auf Betriebssystemebene und zur dauerhaften Speicherung der VLAN Tagging-Änderungen 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-Benutzerhandbuch. EC2
- 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 Outposts-Server.

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

- Netzwerkkarten auf dem Server
- Lokale Netzwerkschnittstellen auf Instances

Für Service Link Outposts DHCP Outposts-Server eine Verbindung zum lokalen Netzwerk . DHCPmuss DNS Nameserver und ein Standard-Gateway zurückgeben. Outposts-Server unterstützen keine statische IP-Zuweisung von Service-Links.

Verwenden Sie diese Option für die lokale Netzwerkschnittstelle, DHCP um Instanzen 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 Outposts-Server verwenden. Änderungen der IP-Adresse können zu vorübergehenden Dienstunterbrechungen im Outpost-Subnetz führen.

Serverregistrierung

Wenn Outposts-Server eine Verbindung im lokalen Netzwerk herstellen, verwenden sie die Service Link-Verbindung, um eine Verbindung zu Outpost-Registrierungsendpunkten herzustellen und sich selbst zu registrieren. Die Registrierung muss öffentlich sein. DNS Wenn sich Server registrieren, erstellen sie einen sicheren Tunnel zu ihrem Service Link-Endpunkt in der Region. Die Server von Outposts verwenden TCP Port 443, um die Kommunikation mit der Region über das öffentliche Internet zu erleichtern. Outposts-Server unterstützen keine private Konnektivität überVPC.

Teilen Sie Ihre AWS Outposts Ressourcen

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

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

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

Ein Outpost-Eigentümer kann Outpost-Ressourcen teilen mit:

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

Inhalt

- Eine Outpost-Ressource freigeben
- Aufheben der Freigabe einer Outpost-Ressource
- Identifizieren einer freigegebenen Outpost-Ressource
- Berechtigungen für freigegebene Outpost-Ressourcen
- Fakturierung und Messung
- Einschränkungen

Freigabefähige Outpost-Ressourcen

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

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

- Zugewiesene Dedicated Hosts – Konsumenten mit Zugriff auf diese Ressource können:
  - Starten und führen Sie EC2 Instances auf einem Dedicated Host aus.
- Outposts – Konsumenten mit Zugang zu dieser Ressource können:
  - Erstellen und verwalten von Subnetzen auf dem Outpost.
  - Verwenden Sie den AWS Outposts API, um Informationen über den Außenposten einzusehen.
- Standorte – Verbraucher mit Zugriff auf diese Ressource können:
  - Einen Outpost am Standort einrichten, verwalten und steuern.
- Subnetze – Konsumenten mit Zugriff auf diese Ressource können:
  - Anzeigen von Informationen über Subnetze.
  - EC2Instances in Subnetzen starten und ausführen.

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

Voraussetzungen für die Freigabe von Outposts-Ressourcen

- Um eine Outpost-Ressource mit Ihrer Organisation oder einer Organisationseinheit gemeinsam zu nutzen AWS Organizations, müssen Sie das Teilen mit aktivieren. AWS Organizations Weitere

Informationen finden Sie unter Freigabe für AWS Organizations aktivieren im AWS RAM - Benutzerhandbuch.

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

Zugehörige Services

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

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

Freigeben in mehreren Availability Zones

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

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

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

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

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

Eine Outpost-Ressource freigeben

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

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

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

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

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

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

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

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

Siehe Erstellen einer Ressourcenfreigabe im AWS RAM -Benutzerhandbuch.

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

Verwenden Sie den create-resource-shareBefehl.

Aufheben der Freigabe einer Outpost-Ressource

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

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

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

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

Siehe Aktualisieren einer Ressourcenfreigabe im AWS RAM -Benutzerhandbuch.

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

Verwenden Sie den Befehl disassociate-resource-share.

Identifizieren einer freigegebenen Outpost-Ressource

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

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

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

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

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

Berechtigungen für freigegebene Outpost-Ressourcen

Berechtigungen für Besitzer

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

Berechtigungen für Konsumenten

Konsumenten können beim Erstellen von Ressourcen in Outposts so vorgehen, wie sie dies beim Erstellen von Ressourcen auf Outposts tun würden, die sie in ihrem eigenen Konto erstellen. Konsumenten sind für die Verwaltung der Ressourcen verantwortlich, die sie auf Outposts starten, die

für sie freigegeben sind. Konsumenten können sich keine Ressourcen anzeigen lassen oder ändern, die anderen Konsumenten oder dem Besitzer des Outposts gehören, und sie können keine Outposts ändern, die für sie freigegeben sind.

Fakturierung und Messung

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

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

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

Einschränkungen

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

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

Sicherheit in AWS Outposts

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

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

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

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

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

Inhalt

Datenschutz in AWS Outposts

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

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

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

Verschlüsselung im Ruhezustand

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

Verschlüsselung während der Übertragung

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

Löschen von Daten

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

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

Identitäts- und Zugriffsmanagement () für IAM AWS Outposts

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

Inhalt

So funktioniert AWS Outposts mit IAM

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

IAMFunktionen, die du mit AWS Outposts verwenden kannst

IAMFunktion	AWS Unterstützung für Outposts
Identitätsbasierte Richtlinien	Ja
Ressourcenbasierte Richtlinien	Nein
Richtlinienaktionen	Ja
Richtlinienressourcen	Ja
Richtlinienbedingungsschlüssel (services pezifisch)	Ja
ACLs	Nein
ABAC(Markierungen in Richtlinien)	Ja
Temporäre Anmeldeinformationen	Ja

IAMFunktion	AWS Unterstützung für Outposts
Hauptberechtigungen	Ja
Servicerollen	Nein
Serviceverknüpfte Rollen	Ja

Identitätsbasierte Richtlinien für Outposts AWS

Unterstützt Richtlinien auf Identitätsbasis: Ja

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

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

Beispiele für identitätsbasierte Richtlinien für Outposts AWS

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

Ressourcenbasierte Richtlinien innerhalb von Outposts AWS

Unterstützt ressourcenbasierte Richtlinien: Nein

Ressourcenbasierte Richtlinien sind JSON Richtliniendokumente, die Sie an eine Ressource anhängen. Beispiele für ressourcenbasierte Richtlinien sind IAM Rollenvertrauensrichtlinien und Amazon S3 S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche

Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben. Zu den Prinzipalen können Konten, Benutzer, Rollen, Verbundbenutzer oder gehören. AWS-Services

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

Politische Maßnahmen für AWS Outposts

Unterstützt Richtlinienaktionen: Ja

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

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

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

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

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

```
outposts
```

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

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

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

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

Politische Ressourcen für AWS Outposts

Unterstützt Richtlinienressourcen: Ja

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

Das `Resource` JSON Richtlinienelement gibt das Objekt oder die Objekte an, für die die Aktion gilt. Anweisungen müssen entweder ein – `Resource`oder ein `NotResource`-Element enthalten. Es hat sich bewährt, eine Ressource mit ihrem Amazon-Ressourcennamen (ARN) anzugeben. Sie können dies für Aktionen tun, die einen bestimmten Ressourcentyp unterstützen, der als Berechtigungen auf Ressourcenebene bezeichnet wird.

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

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

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

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

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

Schlüssel zu den Policy-Bedingungen für AWS Outposts

Unterstützt servicespezifische Richtlinienbedingungsschlüssel: Ja

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

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

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

Sie können auch Platzhaltervariablen verwenden, wenn Sie Bedingungen angeben. Sie können einem IAM Benutzer beispielsweise nur dann Zugriff auf eine Ressource gewähren, wenn sie mit seinem IAM Benutzernamen gekennzeichnet ist. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter IAMRichtlinienelemente: Variablen und Tags.

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

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

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

ACLsin AWS Outposts

UnterstütztACLs: Nein

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

ABACmit AWS Outposts

Unterstützt ABAC (Tags in Richtlinien): Ja

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

ABACist hilfreich in Umgebungen, die schnell wachsen, und hilft in Situationen, in denen die Richtlinienverwaltung umständlich wird.

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

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

Weitere Informationen zu finden Sie ABAC unter Was ist? ABAC im IAMBenutzerhandbuch. Ein Tutorial mit Schritten zur Einrichtung finden Sie im ABAC Benutzerhandbuch unter Verwenden der attributebasierten Zugriffskontrolle (ABAC). IAM

Temporäre Anmeldeinformationen mit AWS Outposts verwenden

Unterstützt temporäre Anmeldeinformationen: Ja

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

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

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

Serviceübergreifende Prinzipalberechtigungen für Outposts AWS

Unterstützt Forward-Access-Sitzungen (FAS): Ja

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

Servicerollen für AWS -Outposts

Unterstützt Servicerollen: Nein

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

Servicebezogene Rollen für Outposts AWS

Unterstützt dienstbezogene Rollen: Ja

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

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

AWS Politische Beispiele für Outposts

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

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

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

Inhalt

Bewährte Methoden für Richtlinien

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

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten — Verwenden Sie die AWS verwalteten Richtlinien, die Berechtigungen

für viele gängige Anwendungsfälle gewähren, um Ihren Benutzern und Workloads zunächst Berechtigungen zu gewähren. Sie sind in Ihrem verfügbar. AWS-Konto Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom AWS Kunden verwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind. Weitere Informationen finden Sie AWS im IAMBenutzerhandbuch unter AWS Verwaltete Richtlinien oder Verwaltete Richtlinien für Jobfunktionen.

- Berechtigungen mit den geringsten Rechten anwenden — Wenn Sie Berechtigungen mit IAM Richtlinien festlegen, gewähren Sie nur die Berechtigungen, die für die Ausführung einer Aufgabe erforderlich sind. Sie tun dies, indem Sie die Aktionen definieren, die für bestimmte Ressourcen unter bestimmten Bedingungen durchgeführt werden können, auch bekannt als die geringsten Berechtigungen. Weitere Informationen zur Verwendung IAM zum Anwenden von Berechtigungen finden Sie IAMim Benutzerhandbuch unter Richtlinien und Berechtigungen. IAM
- Verwenden Sie Bedingungen in IAM Richtlinien, um den Zugriff weiter einzuschränken — Sie können Ihren Richtlinien eine Bedingung hinzufügen, um den Zugriff auf Aktionen und Ressourcen einzuschränken. Sie können beispielsweise eine Richtlinienbedingung schreiben, um anzugeben, dass alle Anfragen mit gesendet werden müssenSSL. Sie können auch Bedingungen verwenden, um Zugriff auf Serviceaktionen zu gewähren, wenn diese über einen bestimmten Zweck verwendet werden AWS-Service, z. AWS CloudFormation B. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter IAMJSONRichtlinienelemente: Bedingung.
- Verwenden Sie IAM Access Analyzer, um Ihre IAM Richtlinien zu validieren, um sichere und funktionale Berechtigungen zu gewährleisten. IAM Access Analyzer validiert neue und bestehende Richtlinien, sodass die Richtlinien der IAM Richtliniensprache (JSON) und den IAM bewährten Methoden entsprechen. IAMAccess Analyzer bietet mehr als 100 Richtlinienprüfungen und umsetzbare Empfehlungen, um Sie bei der Erstellung sicherer und funktionaler Richtlinien zu unterstützen. Weitere Informationen finden Sie unter IAMAccess Analyzer-Richtlinienvalidierung im IAMBenutzerhandbuch.
- Multi-Faktor-Authentifizierung erforderlich (MFA) — Wenn Sie ein Szenario haben, in dem IAM Benutzer oder ein Root-Benutzer erforderlich sind AWS-Konto, aktivieren Sie die Option MFA für zusätzliche Sicherheit. Wenn Sie festlegen möchten, MFA wann API Operationen aufgerufen werden, fügen Sie MFA Bedingungen zu Ihren Richtlinien hinzu. Weitere Informationen finden Sie unter Konfiguration des MFA -geschützten API Zugriffs im IAMBenutzerhandbuch.

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

Beispiel: Nutzen von Berechtigungen auf Ressourcenebene

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

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

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

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

Mit Diensten verknüpfte Rollen für AWS Outposts

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

Eine dienstbezogene Rolle macht Ihre Einrichtung AWS Outposts effizienter, da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. AWS Outposts definiert die Berechtigungen ihrer dienstbezogenen Rollen und AWS Outposts kann, sofern nicht anders definiert, nur ihre

Rollen übernehmen. Zu den definierten Berechtigungen gehören die Vertrauensrichtlinie und die Berechtigungsrichtlinie, und diese Berechtigungsrichtlinie kann keiner anderen IAM Entität zugeordnet werden.

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

Mit dem Dienst verknüpfte Rollenberechtigungen für AWS Outposts

AWS Outposts verwendet die mit dem Dienst verknüpfte Rolle mit dem Namen _ AWSServiceRoleForOutposts***OutpostID***— Ermöglicht Outposts den Zugriff auf AWS Ressourcen für private Konnektivität in Ihrem Namen. Diese dienstbezogene Rolle ermöglicht die Konfiguration privater Konnektivität, erstellt Netzwerkschnittstellen und fügt sie Service Link-Endpunkt-Instances hinzu.

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

- `outposts.amazonaws.com`

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

- AWSOutpostsServiceRolePolicy
- AWSOutpostsPrivateConnectivityPolicy_***OutpostID***

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

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

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

Das AWSOutpostsPrivateConnectivityPolicy _*OutpostID*Die Richtlinie AWS Outposts ermöglicht es, die folgenden Aktionen für die angegebenen Ressourcen durchzuführen:

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

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

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

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

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

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

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

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

Sie müssen Berechtigungen konfigurieren, damit eine IAM Entität (z. B. ein Benutzer, eine Gruppe oder eine Rolle) eine dienstbezogene Rolle erstellen, bearbeiten oder löschen kann. Weitere Informationen finden Sie unter Berechtigungen für dienstbezogene Rollen im IAMBenutzerhandbuch.

Erstellen Sie eine dienstverknüpfte Rolle für AWS Outposts

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

Bearbeiten Sie eine serviceverknüpfte Rolle für AWS Outposts

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

Löschen Sie eine dienstverknüpfte Rolle für AWS Outposts

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

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

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

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

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

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

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

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

Unterstützte Regionen für AWS Outposts dienstverknüpfte Rollen

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

AWS verwaltete Richtlinien für AWS Outposts

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

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

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

Weitere Informationen finden Sie im IAMBenutzerhandbuch unter AWS Verwaltete Richtlinien.

AWS verwaltete Richtlinie: AWSOutpostsServiceRolePolicy

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

AWS verwaltete Richtlinie: AWSOutpostsPrivateConnectivityPolicy

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

AWS verwaltete Richtlinie: AWSOutpostsAuthorizeServerPolicy

Verwenden Sie diese Richtlinie, um die Berechtigungen zu gewähren, die für die Autorisierung der Outposts-Serverhardware in Ihrem lokalen Netzwerk erforderlich sind.

Diese Richtlinie umfasst die folgenden Berechtigungen.

```
{
  "Version": "2012-10-17",
```

```
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "outposts:StartConnection",
        "outposts:GetConnection"
      ],
      "Resource": "*"
    }
  ]
}
```

AWS Outposts Aktualisierungen AWS verwalteter Richtlinien

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

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

Sicherheit der Infrastruktur in AWS Outposts

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

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

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

Darüber hinaus müssen Anfragen mithilfe einer Zugriffsschlüssel-ID und eines geheimen Zugriffsschlüssels, der einem Prinzipal zugeordnet ist, signiert werden. IAM Alternativ können Sie mit AWS Security Token Service (AWS STS) temporäre Sicherheitsanmeldeinformationen erstellen, um die Anforderungen zu signieren.

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

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

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 auf Kontrollebene wie das Beantworten von API Anrufen, das Überwachen des Außenpostens und das Aktualisieren des Außenpostens. Um von der Ausfallsicherheit der Availability Zones zu profitieren, können Sie Anwendungen auf mehreren

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

Outposts-Server enthalten Instance-Speicher-Volumes, unterstützen jedoch keine EBS Amazon-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.

Überprüfung der Einhaltung der Vorschriften für AWS Outposts

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

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

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

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

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

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

Überwachen Sie Ihren

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

CloudWatch Metriken

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

CloudTrail Logs

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

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

VPC-Flow-Protokolle

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

Datenverkehrsspiegelung

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

AWS Health Dashboard

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

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

CloudWatch Metriken für

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

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

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

Inhalt

- CloudWatch Metriken für Ihren anzeigen

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 (AmazonRDS) oder Application Load Balancer verwendet werden. Diese Metrik beinhaltet keine Kapazität für Dedicated Hosts, die auf dem Outpost konfiguriert sind.

Einheit: Anzahl

Maximale Auflösung: 5 Minuten

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

`AvailableInstanceType_Count`

Anzahl der verfügbaren Instance-Typen. Diese Metrik beinhaltet die `AvailableReservedInstances` Anzahl.

Um die Anzahl der Instanzen zu ermitteln, die Sie reservieren können, ziehen Sie die `AvailableReservedInstances` Anzahl von der `AvailableInstanceType_Count` Anzahl ab.

```
Number of instances that you can reserve = AvailableInstanceType_Count
 - AvailableReservedInstances
```

Diese Metrik beinhaltet keine Kapazität für Dedicated Hosts, die auf dem Outpost konfiguriert sind.

Einheit: Anzahl

Maximale Auflösung: 5 Minuten

Dimensionen: `InstanceType` und `OutpostId`

`AvailableReservedInstances`

Die Anzahl der Instances, die für den Start in die Rechenkapazität verfügbar sind, die mithilfe von Capacity Reservations reserviert wurde.

Diese Metrik beinhaltet keine Amazon EC2 Reserved Instances.

Diese Metrik beinhaltet nicht die Anzahl der Instances, die Sie reservieren können.
Um zu bestimmen, wie viele Instances Sie reservieren können, subtrahieren Sie die `AvailableReservedInstances` Anzahl von der `AvailableInstanceType_Count` Anzahl.

```
Number of instances that you can reserve = AvailableInstanceType_Count
 - AvailableReservedInstances
```

Einheit: Anzahl

Maximale Auflösung: 5 Minuten

Dimensionen: `InstanceType` und `OutpostId`

`UsedReservedInstances`

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

Einheit: Anzahl

Maximale Auflösung: 5 Minuten

Dimensionen: `InstanceType` und `OutpostId`

`TotalReservedInstances`

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

Einheit: Anzahl

Maximale Auflösung: 5 Minuten

Dimensionen: `InstanceType` und `OutpostId`

Metrische Abmessungen

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

Dimension	Beschreibung
`Account`	Das Konto oder der Dienst, der die Kapazität verwendet.
`InstanceFamily`	Die Instance-Familie.
`InstanceType`	Der Instance-Typ.
`OutpostId`	Die ID des Outpost.
`VolumeType`	Der EBS Volumentyp.

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

CloudWatch Metriken für Ihren anzeigen

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

Um Metriken mit der CloudWatch Konsole anzuzeigen

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

Um Metriken mit dem anzuzeigen AWS CLI

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

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

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

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

```
aws cloudwatch get-metric-statistics \
--namespace AWS/Outposts --metric-name InstanceTypeCapacityUtilization \
--statistics Average --period 3600 \
```

```
--dimensions Name=OutpostId,Value=op-01234567890abcdef
 Name=InstanceType,Value=c5.xlarge \
--start-time 2019-12-01T00:00:00Z --end-time 2019-12-08T00:00:00Z
```

AWS Outposts APIAnrufe protokollieren mit AWS CloudTrail

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

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

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

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

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

CloudTrail Pfade

Ein Trail ermöglicht CloudTrail die Übermittlung von Protokolldateien an einen Amazon S3 S3-Bucket. Alle mit dem erstellten Pfade AWS Management Console sind regionsübergreifend. Sie können einen Pfad mit einer oder mehreren Regionen erstellen, indem Sie den verwenden. AWS

CLI Es wird empfohlen, einen Trail mit mehreren Regionen zu erstellen, da Sie alle Aktivitäten in Ihrem Konto AWS-Regionen erfassen. Wenn du einen Trail mit nur einer Region erstellst, kannst du dir nur die Ereignisse ansehen, die in den Trails protokolliert wurden. AWS-Region Weitere Informationen zu Trails finden Sie unter Einen Trail für Sie erstellen AWS-Konto und Einen Trail für eine Organisation erstellen im AWS CloudTrail Benutzerhandbuch.

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

CloudTrail Datenspeicher für Ereignisse in Lake

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

CloudTrail Für das Speichern und Abfragen von Ereignisdaten in Lake fallen Kosten an. Beim Erstellen eines Ereignisdatenspeichers wählen Sie die Preisoption aus, die für den Ereignisdatenspeicher genutzt werden soll. Die Preisoption bestimmt die Kosten für die Erfassung und Speicherung von Ereignissen sowie die standardmäßige und maximale Aufbewahrungsdauer für den Ereignisdatenspeicher. Weitere Informationen zur CloudTrail Preisgestaltung finden Sie unter AWS CloudTrail Preise.

AWS Outposts Management-Ereignisse in CloudTrail

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

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

AWS Outposts Beispiele für Ereignisse

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


```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AKIAIOSFODNN7EXAMPLE:jdoe",
        "arn": "arn:aws:sts::111122223333:assumed-role/example/jdoe",
        "accountId": "111122223333",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AKIAIOSFODNN7EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/example",
                "accountId": "111122223333",
                "userName": "example"
            },
            "webIdFederationData": {},
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2020-08-14T16:28:16Z"
            }
        }
    },
    "eventTime": "2020-08-14T16:32:23Z",
    "eventSource": "outposts.amazonaws.com",
    "eventName": "SetSiteAddress",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "XXX.XXX.XXX.XXX",
    "userAgent": "userAgent",
    "requestParameters": {
        "SiteId": "os-123ab4c56789de01f",
        "Address": "***"
    },
    "responseElements": {
        "Address": "***",
        "SiteId": "os-123ab4c56789de01f"
    },
    "requestID": "1abcd23e-f4gh-567j-klm8-9np01q234r56",
```

```
    "eventID": "1234a56b-c78d-9e0f-g1h2-34jk56m7n890",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
```

Wartung von Outposts

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

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

Inhalt

Kontaktinformationen aktualisieren

Wenn der Outpost-Besitzer wechselt, wenden Sie sich mit dem Namen und den Kontaktinformationen des neuen Besitzers an AWS Support Center.

Hardware-Wartung

Wenn während der Serverbereitstellung oder beim Hosten von EC2 Amazon-Instances, die auf Ihrem laufen, ein irreparables Hardwareproblem AWS festgestellt wird, werden wir den Outpost-Eigentümer und den Eigentümer der Instances darüber informieren, dass die betroffenen Instances stillgelegt

werden sollen. Weitere Informationen finden Sie unter Instance Retirement im EC2Amazon-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 Outposts-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 -Strom- und Netzwerkereignisse

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

Stromereignisse

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

- Verlagern Sie Ihre Dienste und Anwendungen auf kontrollierte Weise von den Outposts-Geräten, indem Sie Änderungen beim Lastenausgleich DNS auf Basis oder außerhalb des Racks verwenden.
- Stoppen Sie Container, Instances und Datenbanken in einer inkrementellen Reihenfolge und verwenden Sie bei der Wiederherstellung die umgekehrte Reihenfolge.
- Testpläne für das kontrollierte Verschieben oder Stoppen von Diensten.
- Sichern Sie wichtige Daten und Konfigurationen und speichern Sie sie außerhalb der Outposts.
- Beschränken Sie Stromausfallzeiten auf ein Minimum.
- Vermeiden Sie ein wiederholtes Umschalten der Stromversorgungen (off-on-off-on) während der Wartung.
- Planen Sie innerhalb des Wartungszeitfensters zusätzliche Zeit ein, um unvorhergesehene Ereignisse zu beheben.
- Steuern Sie die Erwartungen Ihrer Benutzer und Kunden, indem Sie ein größeres Zeitfenster für die Wartung angeben, als Sie normalerweise benötigen würden.
- Erstellen Sie nach der Wiederherstellung der Stromversorgung einen Fall im AWS Support Center, um zu überprüfen, AWS Outposts ob und die zugehörigen Dienste ausgeführt werden.

Netzwerkkonnektivitätsereignisse

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

EC2Amazon-Instances, LNI Netzwerke und Instance-Speichervolumes auf Outposts Outposts-Server funktionieren weiterhin normal und können lokal über das lokale Netzwerk und LNI abgerufen werden. In ähnlicher Weise werden AWS Serviceressourcen wie Amazon ECS Worker Nodes

weiterhin lokal ausgeführt. Die API Verfügbarkeit wird jedoch beeinträchtigt. Beispielsweise funktionieren Ausführen, Starten, Stoppen und Beenden APIs möglicherweise nicht. Instance-Metriken und Logs werden weiterhin für einige Stunden lokal zwischengespeichert und in die AWS Region übertragen, sobald die Konnektivität wieder hergestellt ist. Wenn die Verbindung nach einigen Stunden unterbrochen wird, kann dies jedoch zum Verlust von Metriken und Protokollen führen.

Wenn die Serviceverbindung aufgrund eines Stromausfalls vor Ort oder eines Verlusts der Netzwerkverbindung unterbrochen 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 Tool AWSSupport-S etupIPMonitoring From VPC. Dieses Tool ist ein AWS Systems Manager Dokument (SSMDokument), das eine Amazon EC2 Monitor-Instance in einem von Ihnen angegebenen Subnetz erstellt und Ziel-IP-Adressen überwacht. Das Dokument führt Ping-MTR, TCP Trace-

Route- und Trace-Path-Diagnosetests durch und speichert die Ergebnisse in Amazon CloudWatch Logs, die in einem CloudWatch Dashboard visualisiert werden können (z. B. Latenz, Paketverlust). Für die Überwachung von Outposts sollte sich die Monitor-Instance in einem Subnetz der übergeordneten AWS Region befinden und so konfiguriert sein, dass sie eine oder mehrere Ihrer Outpost-Instances mithilfe ihrer privaten IP (s) überwacht. Dadurch werden Diagramme zum Paketverlust und zur Latenz zwischen AWS Outposts und der übergeordneten Region angezeigt. AWS

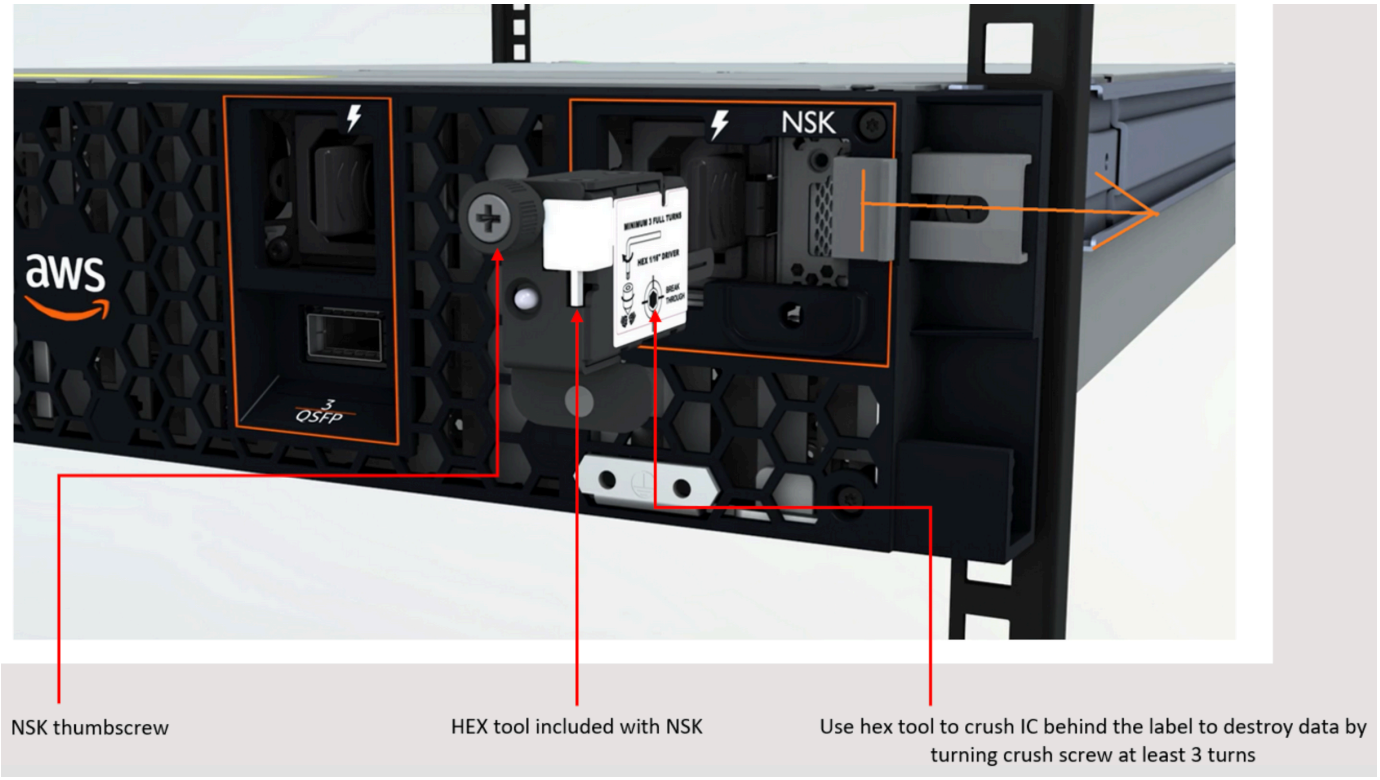
- Der AWS Blog Deploying an automated Amazon CloudWatch dashboard for AWS OutpostsAWS CDK use beschreibt die Schritte zur Bereitstellung eines automatisierten Dashboards.
- Wenn Sie Fragen haben oder weitere Informationen benötigen, finden Sie weitere Informationen unter Erstellen eines Support-Falls im Support-Benutzerhandbuch für AWS .

Kryptografisch geschredderte Serverdaten

Der Nitro-Sicherheitsschlüssel (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 Dienst einstellen, können Sie den vernichten, um die Daten NSK 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 zurücksenden. AWS
2. Stellen Sie sicher, dass Sie das richtige Produkt habenNSK, 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. Durch diese Aktion werden alle Daten auf dem Server zerstört NSK und kryptografisch vernichtet.


NSK
aws
QSFP
NSK thumbscrew
HEX tool included with NSK
Use hex tool to crush IC behind the label to destroy data by turning crush screw at least 3 turns

Outposts-Serveroptionen end-of-term

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

- Erneuern Sie Ihr Abonnement und behalten Sie Ihre bestehenden Outposts-Server.
- Beenden Sie Ihr Abonnement und geben Sie Ihre Outposts-Server zurück.
- Wechseln Sie zu einem month-to-month Abonnement und behalten Sie Ihre bestehenden Outposts-Server.

Verlängern Sie Ihr Abonnement

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

Um Ihr Abonnement zu verlängern und Ihre bestehenden Outposts-Server beizubehalten

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 den Verlängerungsprozess für das Abonnement ein. Ihr neues Abonnement beginnt am Tag nach Ablauf Ihres aktuellen Abonnements.

Wenn Sie nicht angeben, dass Sie Ihr Abonnement verlängern oder Ihren Outposts-Server zurückgeben möchten, werden Sie automatisch in ein month-to-month 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

Sie müssen die folgenden Schritte mindestens 30 Tage vor Ablauf des aktuellen Abonnements für Ihre Outposts-Server abschließen. AWS Sie können den Rückgabevorgang erst starten, wenn Sie dies getan haben.

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

Um dein Abonnement zu beenden

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

7. Wählen Sie Next step: Additional information (Nächster Schritt: Zusätzliche Informationen).
8. Geben Sie auf der Seite Zusätzliche Informationen für Betreff eine eindeutige Anfrage ein, z. B. **`End my Outpost subscription`**
9. Geben Sie unter Beschreibung das Datum ein, an dem 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 NOT Sie den Server herunter oder trennen Sie ihn 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 auf ein month-to-month Abonnement umzusteigen und Ihre bestehenden Outposts-Server beizubehalten, sind keine Maßnahmen 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 Monatsabonnement beginnt am Tag nach dem Ende 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.

Dokumentenverlauf für

In der folgenden Tabelle werden die Dokumentationsaktualisierungen für beschrieben.

Änderung	Beschreibung	Datum
Kapazitätsmanagement	Sie können die Standardk apazitätskonfiguration für Ihre neue Outposts-Bestellung ändern.	16. April 2024
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
Wir stellen vor: Outposts-Server	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.