Guía del usuario para bastidores de Outposts

AWS Outposts

AWS Outposts: Guía del usuario para bastidores de Outposts

Table of Contents

¿Qué es AWS Outposts?

AWS Outposts es un servicio totalmente gestionado que extiende la AWS infraestructura APIs, los servicios y las herramientas a las instalaciones del cliente. Al proporcionar acceso local a la infraestructura AWS gestionada, los AWS Outposts clientes pueden crear y ejecutar aplicaciones en las instalaciones mediante las mismas interfaces de programación que en AWS Regions y, al mismo tiempo, utilizar los recursos informáticos y de almacenamiento locales para reducir la latencia y las necesidades de procesamiento de datos locales.

Un Outpost es un conjunto de capacidades AWS informáticas y de almacenamiento desplegadas en las instalaciones de un cliente. AWS opera, supervisa y administra esta capacidad como parte de una AWS región. Puede crear subredes en su Outpost y especificarlas al crear AWS recursos, como EC2 instancias, volúmenes de EBS, clústeres de ECS e instancias de RDS. Las instancias de las subredes de Outpost se comunican con otras instancias de la AWS región mediante direcciones IP privadas, todas dentro de la misma VPC.

> **Note**
>
> No puede conectar un Outpost a otro Outpost o zona local que esté dentro de la misma VPC.

Para obtener más información, consulte la página del producto de AWS Outposts.

Conceptos clave

Estos son los conceptos clave de. AWS Outposts

- Sitio de Outpost: los edificios físicos gestionados por el cliente donde se AWS instalará tu Outpost. Un sitio debe cumplir con los requisitos de instalaciones, redes y alimentación de su Outpost.
- Capacidad del Outpost: recursos informáticos y de almacenamiento disponibles en el Outpost. Puedes ver y administrar la capacidad de tu Outpost desde la consola. AWS Outposts AWS Outposts admite la gestión de capacidad de autoservicio que puedes definir a nivel de Outposts para reconfigurar todos los activos de un Outposts o específicamente para cada activo individual. Un activo de Outpost puede ser un único servidor dentro de un rack de Outposts o un servidor de Outposts.
- Equipo de Outpost: hardware físico que proporciona acceso al servicio. AWS Outposts El hardware incluye racks, servidores, conmutadores y cableado propiedad de y gestionados por. AWS

- Bastidores de Outposts: un factor de forma de Outpost que constituye un bastidor de 42U estándar del sector. Los bastidores del Outposts incluyen servidores que se pueden montar en bastidores, conmutadores, un panel de conexiones de red, un estante de suministro eléctrico y paneles vacíos.
- Bastidores ACE de Outposts: el bastidor Aggregation, Core, Edge (ACE) actúa como un punto de agregación de red para implementaciones de Outpost con varios bastidores. El bastidor ACE reduce la cantidad de puertos de red físicos y los requisitos de interfaz lógica al proporcionar conectividad entre varios bastidores de computación de Outpost en sus Outposts lógicos y en su red en las instalaciones.

  Debe instalar un bastidor ACE si tiene cuatro o más bastidores de computación. Si tiene menos de cuatro bastidores de computación, pero planea ampliarlos a cuatro o más en el futuro, le recomendamos que instale un bastidor ACE lo antes posible.

  Para obtener información adicional sobre los racks ACE, consulte Escalar las implementaciones de AWS Outposts racks con racks ACE.
- Servidores para Outposts: un factor de forma del Outpost que constituye un servidor de 1U o 2U con protocolo estándar del sector, y se puede instalar en un bastidor de 4 postes estándar conforme con la norma EIA-310D 19. Los servidores de Outposts proporcionan servicios de computación y red locales a sitios que tienen requisitos de espacio limitado o capacidad más reducida.
- Propietario de Outpost: el propietario de la cuenta que realiza el pedido. AWS Outposts Tras AWS contactar con el cliente, el propietario puede incluir puntos de contacto adicionales. AWS se comunicará con los contactos para aclarar los pedidos, las citas de instalación y el mantenimiento y reemplazo del hardware. Comuníquese con AWS Support Center si la información de contacto cambia.
- Enlace de servicio: ruta de red que permite la comunicación entre su puesto de avanzada y AWS la región asociada. Cada Outpost es una extensión de una zona de disponibilidad y su región asociada.
- Puerta de enlace local (LGW): un enrutador virtual de interconexión lógica que permite la comunicación entre un bastidor de Outposts y la red en las instalaciones.
- Interfaz de red local: una interfaz de red que permite la comunicación entre un servidor de Outposts y la red en las instalaciones.

AWS recursos en Outposts

Puede crear los siguientes recursos en Outpost para soportar cargas de trabajo de baja latencia que deben ejecutarse cerca de los datos y las aplicaciones en las instalaciones:

Computación

Tipo de recurso	Bastidores	Servidores
EC2 Instancias de Amazon	 S	 Sí
Clústeres de Amazon ECS	 S	 Sí
Nodos de Amazon EKS	 S	 No

Base de datos y análisis

Tipo de recurso	Bastidores	Servidores
ElastiCacheNodos de Amazon (clúster de Redis, clúster de Memcached)	 S	 No
Clústeres de Amazon EMR	 S	 No
Instancias de base de datos de Amazon RDS	 S	 No

Red

Tipo de recurso	Bastidores	Servidores
Proxy App Mesh Envoy	 S	 Sí
Equilibrador de carga de aplicación	 S	 No
Subredes de Amazon VPC	 S	 Sí
Amazon Route 53	 S	 No

Almacenamiento

Tipo de recurso	Bastidores	Servidores
Volúmenes de Amazon EBS	 S	 No
Buckets de Amazon S3	 S	 No

Otros Servicios de AWS

Servicio	Bastidores	Servidores
AWS IoT Greengrass	 S	 Sí

Precios

El precio se basa en los detalles de su pedido. Cuando realizas un pedido, puedes elegir entre una variedad de configuraciones de Outpost, cada una de las cuales ofrece una combinación de tipos de EC2 instancias de Amazon y opciones de almacenamiento. También puede elegir un plazo del contrato y una opción de pago. El precio incluye lo siguiente:

- Bastidores de Outposts: entrega, instalación, mantenimiento de servicios de infraestructura, parches y actualizaciones de software y retirada de bastidores.
- Servidores de Outposts: entrega, mantenimiento de servicios de infraestructura y parches y actualizaciones de software. Usted es responsable de la instalación y el embalaje del servidor para su devolución.

Se te facturarán los recursos compartidos y cualquier transferencia de datos de la AWS región a Outpost. También se le facturarán las transferencias de datos que se realicen para mantener AWS la disponibilidad y la seguridad.

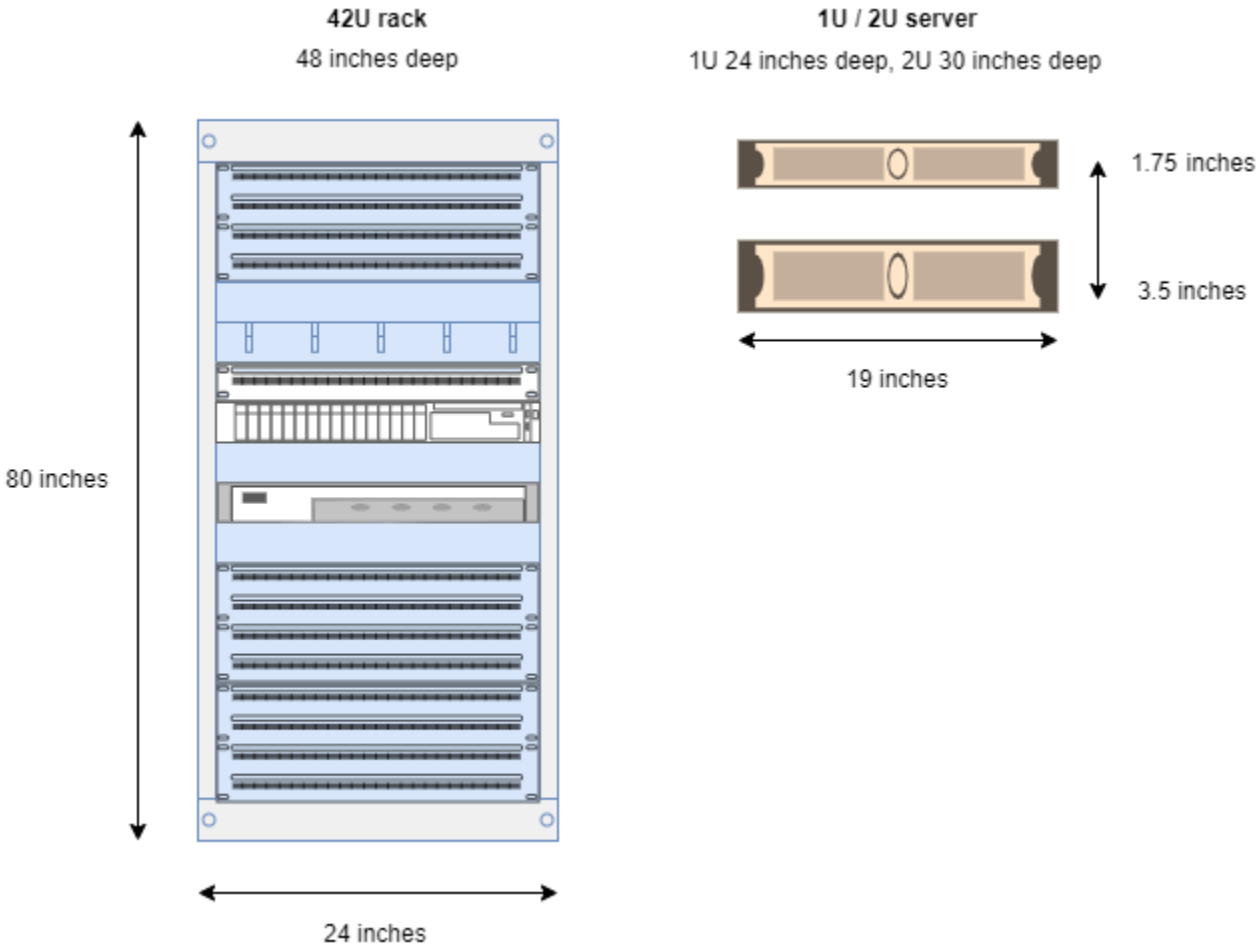
Para ver los precios según la ubicación, la configuración y la opción de pago, consulte:

- Precios de bastidores de Outposts
- Precios de servidores de Outposts

Cómo AWS Outposts funciona

AWS Outposts está diseñado para funcionar con una conexión constante y uniforme entre tu puesto de avanzada y una AWS región. Para lograr esta conexión con la región y con las cargas de trabajo locales del entorno local en las instalaciones, debe conectar el Outpost a la red local. La red local debe proporcionar acceso a la red de área amplia (WAN) a la región. También debe proporcionar acceso LAN o WAN a la red en las instalaciones en la que residen las cargas de trabajo o aplicaciones en las instalaciones.

El siguiente diagrama ilustra ambos factores de forma de Outpost.



Contenido

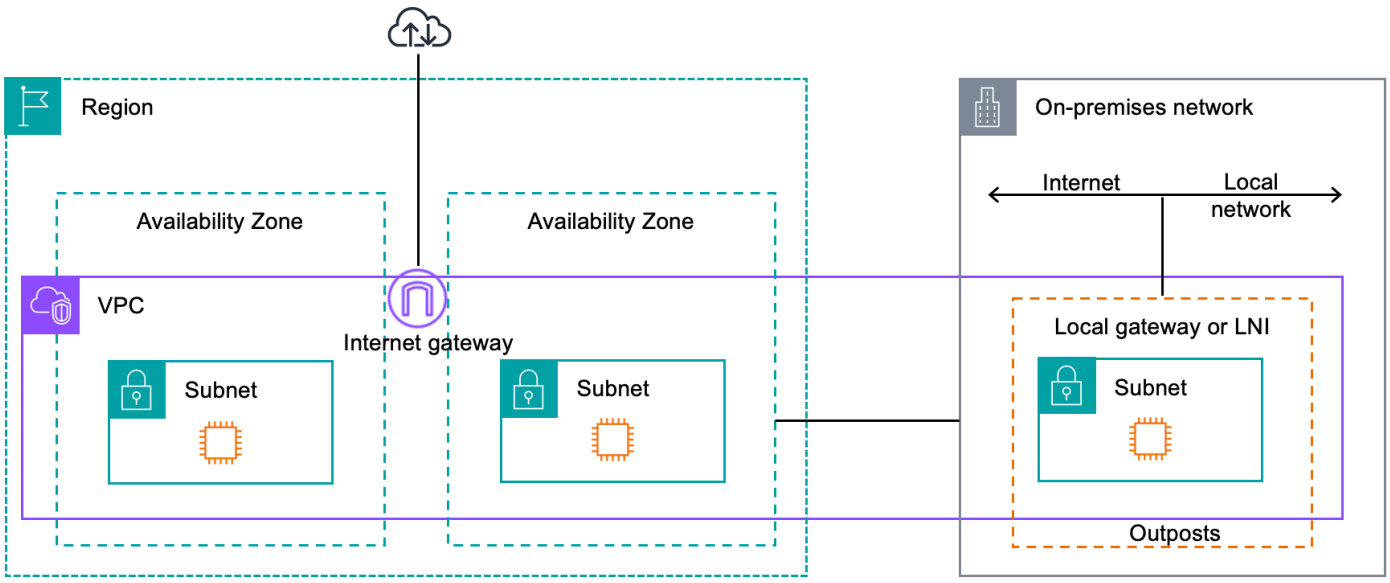
- DNS
- Enlace de servicio
- Puertas de enlace locales
- Interfaces de red local

Componentes de la red

AWS Outposts extiende una VPC de Amazon de una AWS región a un puesto avanzado con los componentes de VPC a los que se puede acceder en la región, incluidas las puertas de enlace de Internet, las puertas de enlace privadas virtuales, las pasarelas de tránsito de Amazon VPC y los puntos de enlace de VPC. Un Outpost está destinado a una zona de disponibilidad de la región y es una extensión de esa zona de disponibilidad que puede utilizar para obtener resiliencia.

El siguiente diagrama ilustra los componentes de la red de su Outpost.

- Una red local y una red local Región de AWS
- Una VPC con múltiples subredes en la región
- Un Outpost en la red en las instalaciones
- La conectividad entre el Outpost y la red local proporcionó:
  - Para los racks de Outposts: una puerta de enlace local
  - Para los servidores Outposts: una interfaz de red local (LNI)



VPCs y subredes

Una nube privada virtual (VPC) abarca todas las zonas de disponibilidad de su región. AWS Puede ampliar cualquier VPC de la región del Outpost al agregar una subred de Outpost. Para agregar una subred de Outpost a una VPC, especifique el nombre de recurso de Amazon (ARN) del Outpost al crear la subred.

Los Outposts admiten múltiples subredes. Puedes especificar la subred de la EC2 instancia al lanzar la EC2 instancia en tu Outpost. No puedes especificar el hardware subyacente en el que se implementa la instancia, porque el Outpost es un conjunto de capacidades de AWS cómputo y almacenamiento.

Cada Outpost puede admitir varias subredes VPCs que pueden tener una o más subredes de Outpost. Para obtener más información acerca de las cuotas de VPC, consulte Cuotas de Amazon VPC en la Guía del usuario de Amazon VPC.

Puede crear subredes de Outpost a partir del rango CIDR de VPC de la VPC en la que se creó el Outpost. Puedes usar los rangos de direcciones de Outpost para los recursos, como las EC2 instancias que residen en la subred de Outpost.

Enrutamiento

De forma predeterminada, cada subred de Outpost hereda la tabla de enrutamiento principal de la VPC. Puede crear una tabla de enrutamiento personalizada y asociarla a una subred de Outpost.

Las tablas de enrutamiento de las subredes de Outpost funcionan tal como lo hacen con las subredes de las zonas de disponibilidad. Puede especificar direcciones IP, puertas de enlace de Internet, puertas de enlace locales, puertas de enlace privadas virtuales y conexiones de emparejamiento como destinos. Por ejemplo, cada subred de Outpost, ya sea a través de la tabla de enrutamiento principal heredada o de una tabla personalizada, hereda la ruta local de la VPC. Esto significa que todo el tráfico de la VPC, incluida la subred de Outpost con el CIDR de la VPC como destino, permanece enrutado en la VPC.

Las tablas de enrutamiento de subredes de Outpost pueden incluir los siguientes destinos:

- Rango CIDR de VPC: lo AWS define en la instalación. Esta es la ruta local y se aplica a todos los enrutamientos de VPC, incluido el tráfico entre instancias de Outpost en la misma VPC.
- AWS Destinos regionales: incluye listas de prefijos para Amazon Simple Storage Service (Amazon S3), los puntos de enlace de puerta de enlace de Amazon DynamoDB, las puertas de enlace

privadas virtuales AWS Transit Gateway, las puertas de enlace de Internet y el emparejamiento de VPC.

Si tiene una conexión de emparejamiento con varias VPCs en el mismo Outpost, el tráfico entre ellas VPCs permanece en el Outpost y no utiliza el enlace de servicio para volver a la región.

- Comunicación dentro de la VPC entre Outposts con puerta de enlace local: para establecer la comunicación entre las subredes de la misma VPC en diferentes Outposts con puertas de enlace locales, utilice el enrutamiento directo de la VPC. Para obtener más información, consulte:
  - Enrutamiento de VPC directo
  - Enrutamiento a una puerta de enlace local de AWS Outposts

DNS

Para las interfaces de red conectadas a una VPC, EC2 las instancias de las subredes de Outposts pueden usar el servicio DNS de Amazon Route 53 para convertir nombres de dominio en direcciones IP. Route 53 es compatible con las características de DNS, como el registro de dominio, el enrutamiento de DNS y las comprobaciones de estado de las instancias que se ejecutan en Outpost. Para enrutar el tráfico a dominios específicos, se admiten zonas de disponibilidad alojadas tanto a nivel público como privado. Los resolutores de Route 53 están alojados en la región. AWS Por lo tanto, la conectividad del enlace de servicio desde el puesto de avanzada a la AWS región debe estar activa y en funcionamiento para que estas funciones de DNS funcionen.

Es posible que encuentres tiempos de resolución de DNS más prolongados con Route 53, según la latencia de la ruta entre tu Outpost y la AWS región. En tales casos, puede utilizar los servidores DNS instalados localmente en su entorno en las instalaciones. Para usar sus propios servidores DNS, debe crear conjuntos de opciones de DHCP para los servidores DNS en las instalaciones y asociarlos a la VPC. También debe asegurarse de que haya conectividad IP con estos servidores DNS. Es posible que también necesite agregar rutas a la tabla de enrutamiento de la puerta de enlace local para garantizar su accesibilidad, pero esta opción solo es válida para los bastidores de Outposts con puerta de enlace local. Como los conjuntos de opciones de DHCP tienen un ámbito de VPC, las instancias de las subredes de Outpost y de las subredes de la zona de disponibilidad de la VPC intentarán usar los servidores DNS especificados para la resolución de nombres DNS.

El registro de consultas no es compatible con las consultas de DNS que se originan en un Outpost.

Enlace de servicio

El enlace de servicio es una conexión desde tu Outpost a la AWS región elegida o a la región de origen de Outposts. El enlace de servicio es un conjunto cifrado de conexiones VPN que se utilizan siempre que el Outpost se comunica con la región de origen elegida. Debe utilizar una LAN virtual (VLAN) para segmentar el tráfico en el enlace de servicio. La VLAN de enlace de servicio permite la comunicación entre el puesto de avanzada y la AWS región tanto para la administración del tráfico del puesto de avanzada como dentro de la VPC entre la región y el puesto de avanzada. AWS

El enlace de servicio se crea cuando se aprovisiona el Outpost. Si tiene un factor de forma de servidor, usted debe crear la conexión. Si tiene un rack, crea el enlace de servicio. AWS Para obtener más información, consulte:

- AWS Outposts conectividad a Regiones de AWS
- El enrutamiento de aplicaciones y cargas de trabajo en el documento AWS Outposts técnico sobre consideraciones de arquitectura y diseño de alta disponibilidad AWS

Puertas de enlace locales

Los bastidores de Outposts incluyen una puerta de enlace local para proporcionar conectividad a la red en las instalaciones. Si tiene un bastidor de Outposts, puede incluir una puerta de enlace local como destino donde el destino sea su red en las instalaciones. Las puertas de enlace locales solo están disponibles para los bastidores de Outposts y solo se pueden usar en tablas de enrutamiento de subredes y VPC asociadas a un bastidor de Outposts. Para obtener más información, consulte:

- Puertas de enlace locales para tus racks de Outposts
- El enrutamiento de aplicaciones y cargas de trabajo en el documento técnico sobre consideraciones de arquitectura y AWS Outposts diseño de alta disponibilidad AWS

Interfaces de red local

Los servidores de Outposts incluyen una interfaz de red en las instalaciones para proporcionar conectividad a la red en las instalaciones. La interfaz de red local solo está disponible para los servidores de Outposts que se ejecutan en una subred de Outpost. No puedes usar una interfaz de red local desde una EC2 instancia de un rack de Outposts o de la AWS Región. La interfaz de red

local está destinada únicamente a ubicaciones en las instalaciones. Para obtener más información, consulte Interfaz de red local en la Guía del usuario de AWS Outposts para servidores de Outposts.

Requisitos del sitio para los bastidores de Outposts

Un sitio de Outpost es la ubicación física donde opera el Outpost. Los sitios solo están disponibles en países y territorios seleccionados. Para obtener más información, consulte AWS Outposts rack FAQs. Consulte la pregunta: ¿En qué países y territorios está disponible el bastidor de Outposts?

En esta página se describen los requisitos de los bastidores de Outposts. Si va a instalar un bastidor Aggregation, Core, Edge (ACE), su sitio también debe cumplir los requisitos que se indican en Requisitos del sitio para los bastidores ACE de Outpost.

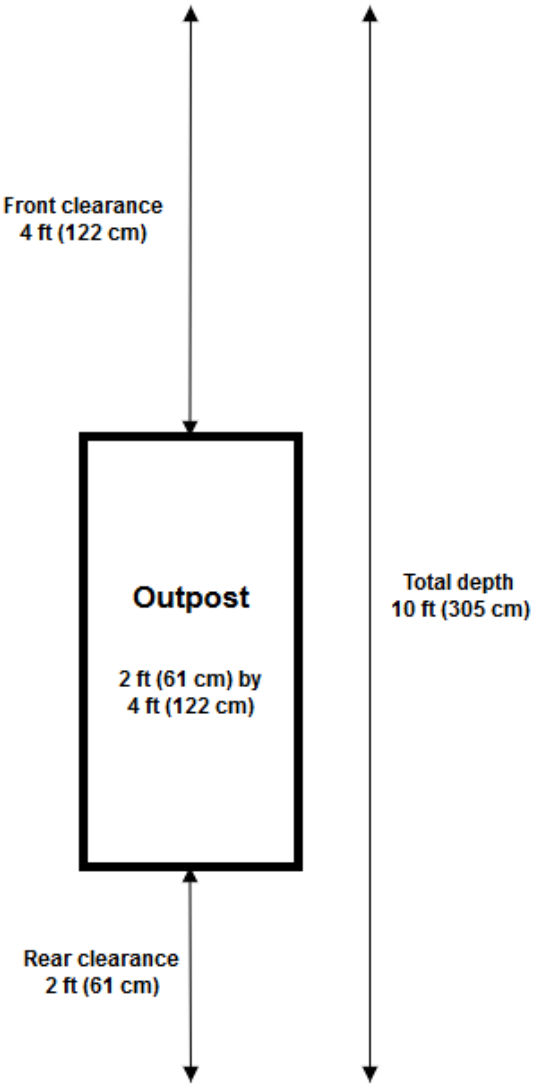
Para conocer los requisitos de los servidores de Outposts, consulte Requisitos del sitio para los servidores de Outposts en la Guía del usuario de AWS Outposts para los servidores de Outposts.

Instalación

A continuación, se describen los requisitos de la instalación de los bastidores.

- Temperatura y humedad: la temperatura ambiente debe oscilar entre 41 °F (5 °C) y 95 °F (35 °C). La humedad relativa debe oscilar entre el 8 % y el 80 % sin condensación.
- Flujo de aire: los bastidores extraen aire frío del pasillo delantero y expulsan el aire caliente hacia el pasillo trasero. La posición del bastidor debe proporcionar un flujo de aire de, al menos, 145,8 veces el kVA de pies cúbicos por minuto (CFM).
- Muelle de carga: el muelle de carga debe admitir un contenedor de bastidores cuyas medidas sean 94 pulgadas (239 cm) de alto por 54 pulgadas (138 cm) de ancho por 51 pulgadas (130 cm) de profundidad.
- Soporte del peso: el peso varía según la configuración. El peso de su configuración se encuentra especificado en el resumen del pedido del punto de carga del bastidor. La ubicación en la que está instalado el bastidor y la ruta hasta esa ubicación deben soportar el peso especificado. Esto incluye todos los elevadores de carga y estándares que se encuentren en las instalaciones.
- Espacio libre: el bastidor mide 80 pulgadas (203 cm) de alto por 24 pulgadas (61 cm) de ancho por 48 pulgadas (122 cm) de profundidad. Todas las puertas, pasillos, curvas, rampas y elevadores deben tener suficiente espacio libre. En la posición de descanso final, debe haber un área de 24 pulgadas (61 cm) de ancho por 48 pulgadas (122 cm) de profundidad para el Outpost, con 48 pulgadas (122 cm) adicionales de espacio libre en la parte delantera y 24 pulgadas (61 cm) de espacio libre en la parte trasera. El área mínima total requerida para el Outpost es de 24 pulgadas (61 cm) de ancho por 10 pies (305 cm) de profundidad.

El siguiente diagrama muestra el área mínima total requerida para el Outpost, incluida la distancia libre.



- Refuerzo sísmico: en la medida en que lo exija la normativa o el código, instalará y mantendrá los anclajes antisísmicos y los refuerzos adecuados para la estantería mientras esté en sus instalaciones. AWS proporciona soportes de suelo que protegen hasta 2 g de actividad sísmica con todos los estantes Outposts.
- Punto de unión: le recomendamos que coloque una unión wire/point en la posición de las estanterías para que el electricista pueda fijar las estanterías durante la instalación, lo que será validado por un técnico certificado. AWS

- Acceso a las instalaciones: no cambiará las instalaciones de forma que afecte negativamente a la capacidad de AWS acceso, mantenimiento o desmontaje del puesto de avanzada.
- Elevación: la altura de la sala donde está instalado el bastidor debe ser inferior a 10 005 ft (3,05 m).

Red

A continuación, se describen los requisitos de las redes para los bastidores.

- Proporcione enlaces ascendentes con velocidades de 1 Gbps, 10 Gbps, 40 Gbps o 100 Gbps.

  Para obtener recomendaciones de ancho de banda para la conexión de enlace de servicio, consulte Recomendaciones de ancho de banda.
- Proporcione fibra monomodo (SMF) con Lucent Connector (LC), fibra multimodo (MMF) o MMF con LC. OM4
- Proporcione uno o dos dispositivos ascendentes, que pueden ser conmutadores o enrutadores. Recomendamos dos dispositivos para ofrecer una alta disponibilidad.

Lista de verificación de disponibilidad de red

Use esta lista de verificación cuando recopile la información para su configuración de Outpost. Esto incluye la LAN, la WAN y cualquier dispositivo entre el Outpost y los destinos de tráfico local y el destino de la región. AWS

Velocidad de enlace ascendente, puertos y fibra

Velocidad de enlace ascendente y puertos

Un Outpost tiene dos dispositivos de red del Outpost que se conectan a la red local. La cantidad de enlaces ascendentes que admite cada dispositivo depende de sus necesidades de ancho de banda y de lo que pueda admitir el enrutador. Para obtener más información, consulte Conectividad física.

La siguiente lista muestra cuántos puertos de enlace ascendente son compatibles con cada dispositivo de red del Outpost, en función de la velocidad del enlace ascendente.

1 Gbps

1, 2, 4, 6 u 8 enlaces ascendentes

10 Gbps

- 1, 2, 4, 8, 12 o 16 enlaces ascendentes

40 Gbps o 100 Gbps

- 1, 2 o 4 enlaces ascendentes

Fibra

Se admiten los siguientes tipos de fibra:

- Fibra monomodo (SMF) con conector Lucent (LC)
- Fibra multimodo (MMF) o MMF con LC OM4

Según la velocidad del enlace ascendente y el tipo de fibra que elija, se admiten los siguientes estándares ópticos.

Velocidad de enlace ascendente	Tipo de fibra	Estándares ópticos
1 Gbps	SMF	: 1000Base-LX
1 Gbps	MMF	: 1000Base-SX
10 Gbps	SMF	: 10GBASE-IR : 10GBASE-LR
10 Gbps	MMF	: 10 GBASE-SR
40 Gbps	SMF	— BASE DE 40 G (L) IR4 LR4 — BASE DE 40 G - LR4
Aplicación breakout de 4 x 10 Gbps	MMF	— BASE DE 40 G- ESR4 — BASE DE 40 G- SR4
100 Gbps	SMF	— 100 G DE MASA PSM4

Velocidad de enlace ascendente	Tipo de fibra	Estándares ópticos
		— 100 G DE BASE- CWDM4 — 100 G BASE- LR4
Aplicación breakout de 4 x 25 Gbps	MMF	— 100 G BASE- SR4

Agregación de enlaces de Outpost y VLANs

Se requiere el protocolo de control de agregación de enlaces (LACP) entre el Outpost y su red. Debe utilizar un LAG dinámico con el LACP.

VLANs Se requiere lo siguiente para cada dispositivo de red Outpost. Para obtener más información, consulte Virtual LANs.

Dispositivo de red del Outpost	VLAN de enlace de servicio	VLAN de puerta de enlace local
N.º 1	Valores válidos: 1-4094	Valores válidos: 1-4094
N.º 2	Valores válidos: 1-4094	Valores válidos: 1-4094

Para cada dispositivo de red Outpost, puede elegir si desea utilizar el mismo VLANs o uno diferente VLANs para el enlace de servicio y la puerta de enlace local. Sin embargo, recomendamos que cada dispositivo de red del Outpost tenga una VLAN diferente a la del otro dispositivo de red de Outpost. Para obtener más información, consulte Agregación de enlaces y virtual LANs.

También recomendamos una conectividad redundante de capa 2. El LACP se utiliza para la agregación de enlaces y no para la alta disponibilidad. No se admite el LACP entre los dispositivos de la red del Outpost.

Conectividad IP del dispositivo de red del Outpost

Cada uno de los dos dispositivos de red Outpost requiere un CIDR y una dirección IP para el enlace de servicio y la puerta de enlace local. VLANs Recomendamos asignar una subred dedicada para

cada dispositivo de red con un CIDR /30 o /31. Especifique una subred y una dirección IP de la subred para que las utilice el Outpost. Para obtener más información, consulte Conectividad de capa de red.

Dispositivo de red del Outpost	Requisitos de enlace de servicio	Requisitos de la puerta de enlace local
N.º 1	: enlace de servicio con CIDR (/30 o /31) : dirección IP del enlace de servicio	: puerta de enlace local con CIDR (/30 o /31) : dirección IP de la puerta de enlace local
N.º 2	: enlace de servicio con CIDR (/30 o /31) : dirección IP del enlace de servicio	: puerta de enlace local con CIDR (/30 o /31) : dirección IP de la puerta de enlace local

Unidad de transmisión máxima (MTU) del enlace de servicio

La red debe admitir una MTU de 1500 bytes entre los puntos finales de Outpost y de enlace de servicio en la región principal. AWS Para obtener más información sobre el enlace de servicio, consulte AWS Outposts conectividad con las AWS regiones.

Protocolo de puerta de enlace fronteriza

El Outpost establece una sesión de interconexión BGP (eBGP) externa entre cada dispositivo de red del Outpost y su dispositivo de red local para la conectividad del enlace de servicio a través de la VLAN del enlace de servicio. Para obtener más información, consulte Conectividad BGP de Service Link.

Outpost	Requisitos de BGP del enlace de servicio
Su Outpost	: número de sistema autónomo (ASN) BGP de Outpost. 2 bytes (16 bits) o 4 bytes (32 bits). Desde su rango de ASN privado (64512-65534 o 4200000000-4294967294).

Outpost	Requisitos de BGP del enlace de servicio
	: CIDR de la infraestructura (se requiere /26, anunciado como dos /27 contiguos).

Dispositivo de red local	Requisitos de BGP del enlace de servicio
N.º 1	: dirección IP homóloga BGP del enlace de servicio. : enlace de servicio BGP por ASN. 2 bytes (16 bits) o 4 bytes (32 bits).
N.º 2	: dirección IP homóloga BGP del enlace de servicio. : enlace de servicio BGP por ASN. 2 bytes (16 bits) o 4 bytes (32 bits).

Firewall del enlace de servicio

Los protocolos UDP y TCP 443 deben estar listados por estado en el firewall.

Protocolo	Puerto de origen	Dirección de origen	Puerto de destino	Dirección de destino
UDP	443	Enlace al servicio del Outpost /26	443	Rutas públicas de la región del Outpost
TCP	1025-65535	Enlace al servicio del Outpost /26	443	Rutas públicas de la región del Outpost

Puedes usar una AWS Direct Connect conexión o una conexión pública a Internet para volver a conectar el Outpost a la región. AWS Para la conectividad por enlace de servicio del Outpost, puede usar NAT o PAT en su firewall o enrutador de periferia. El establecimiento del enlace de servicio siempre se inicia desde el Outpost.

Para obtener más información sobre los requisitos de enlace de servicio, como la MTU y la latencia de 175 ms, consulta Conectividad a través del enlace de servicio.

Protocolo de puerta de enlace fronteriza

El Outpost establece una sesión de emparejamiento eBGP desde cada dispositivo de red del Outpost a un dispositivo de red local para la conectividad de la red local a la puerta de enlace local. Para obtener más información, consulte Conectividad del BGP de la puerta de enlace local.

Outpost	Requisitos del BGP para la puerta de enlace local
Su Outpost	: número de sistema autónomo (ASN) BGP de Outpost. 2 bytes (16 bits) o 4 bytes (32 bits). Desde su rango de ASN privado (64512-65534 o 4200000000-4294967294). : CoIP de CIDR para anunciar (pública o privada, /26 como mínimo).

Dispositivos de red local	Requisitos del BGP para la puerta de enlace local
N.º 1	: dirección IP peer del BGP para la puerta de enlace local. : puerta de enlace local del peer BGP de ASN. 2 bytes (16 bits) o 4 bytes (32 bits).
N.º 2	: dirección IP peer del BGP para la puerta de enlace local. : puerta de enlace local del peer BGP de ASN. 2 bytes (16 bits) o 4 bytes (32 bits).

Alimentación

La bandeja de alimentación de los Outposts admite tres configuraciones de alimentación: 5 kVA, 10 kVA o 15 kVA. La configuración de la bandeja de alimentación depende del consumo total de energía de la capacidad del Outpost. Por ejemplo, si su recurso Outpost tiene un consumo de energía máximo de 9,7 kVA, debe proporcionar las configuraciones de alimentación para 10 kVA: 4 x L6-30P o IEC3 09, 2 caídas a S1 y 2 caídas a S2 para alimentación monofásica redundante. Las tres configuraciones de alimentación se describen en la siguiente segunda tabla.

Para ver los requisitos de consumo de energía de los distintos recursos de Outpost, selecciona Explorar el catálogo en la consola en. AWS Outposts https://console.aws.amazon.com/outposts/

Requisito	Especificación
Tensión de línea AC	Monofásica de 208 a 277 V CA; 50 o 60 Hz Trifásica: • 208 a 250 V CA (Delta); 50 a 60 Hz • 346 a 480 V CA (Delta); 50 a 60 Hz
Consumo de energía	5 kVA (4 kW), 10 kVA (9 kW) o 15 kVA (13 kW)
Protección de corriente alterna (disyuntores ascendentes)	Tanto para la entrada de 1 N (no redundante) como para la entrada de 2 N (redundante): 30 A o 32 A o 50 A con disyuntor con curva D o curva K. Solo para entradas de 2N (redundante): disyuntor de curva C, curva D o curva K. No se admite una curva B o inferior.
Tipo de entrada AC (receptáculo)	Conectores monofásicos 3xL6-30P, P+P+E, 30 A o 3 conectores P+N+E 0309, 32 A IEC6 IP67 Trifásicos, Wye 1x IEC6 0309, 3P+N+E, posición de reloj 7, conector 30A o 1x 0309, 3P+N+E, posición de reloj 6, conector 32A IP67 IEC6 IP67

Requisito	Especificación
	Hubbell C trifásico, CS8365 Delta, 1 x no NEMA, 3P+E, conexión a tierra central, conector de 50 A **Note** La mejor práctica es conectar un enchufe a un receptáculo. IP67 IP67 Si eso no es posible, el IP67 enchufe se acoplará a un IP44 receptáculo. La clasificación del enchufe y la toma combinados pasará a ser la clasificación más baja ()IP44.
Longitud del látigo	10,25 pies (3 m)
Látigo - Entrada de cableado del bastidor	Desde arriba o desde abajo del bastidor

La bandeja de alimentación tiene dos entradas, S1 y S2, que se pueden configurar de la siguiente manera.

	Redundante, monofásico	Redundante, trifásico	Monofásico	Trifásico
5 kVA	2 x L6-30P o IEC3 09; 1 caída a S1 y 1 caída a S2	2 x AH530P7W, AH532P6W o CS8365C; 1 caída a S1 y 1 caída a S2	No ofrecido	1 x AH530P7W, P6W o C; 1 caída a AH532 S1 CS8365
10 kVA	4 x L6-30P o IEC3 09; 2 caídas a S1 y 2 caídas a S2		2 x L6-30P o IEC3 09; 2 caen a S1	
15 kVA	6 x L6-30P o IEC3 09; 3 caídas a S1 y 3 caídas a S2		3 x L6-30P o IEC3 09; 3 caen a S1	

Si los látigos de corriente alterna que se AWS suministran tal y como se ha descrito anteriormente deben estar equipados con un enchufe de alimentación alternativo, tenga en cuenta lo siguiente:

- Solo un electricista certificado proporcionado por el cliente debe modificar la toma de corriente alterna para adaptarla a un nuevo tipo de enchufe.
- A fin de garantizar su seguridad eléctrica, la instalación debe cumplir con todos los requisitos de seguridad nacionales, estatales y locales vigentes, y debe inspeccionarse según sea necesario.
- Usted, el cliente, debe notificar a su AWS representante las modificaciones introducidas en la bujía de alimentación de corriente alterna. Si lo solicita, proporcionará información sobre las modificaciones a AWS. También incluirá cualquier registro de inspección de seguridad emitido por la autoridad competente. Este es un requisito para validar la seguridad de la instalación antes de que los empleados de AWS trabajen en el equipo.

Procesamiento de pedido

Para cumplir con el pedido, AWS programaremos una fecha y hora con usted. También recibirá una lista de verificación con los elementos que debe comprobar o proporcionar antes de la instalación.

El equipo de AWS instalación llegará a sus instalaciones en la fecha y hora programadas. Colocarán el bastidor en la posición identificada. Usted y su electricista son responsables de realizar la conexión eléctrica y la instalación del bastidor.

Debe asegurarse de que las instalaciones eléctricas y cualquier cambio en esas instalaciones sean realizadas por un electricista certificado conforme a todas las leyes, códigos y prácticas recomendadas vigentes. Debe obtener la aprobación por escrito antes de realizar cualquier cambio AWS en el hardware o las instalaciones eléctricas de Outpost. Usted acepta proporcionar AWS documentación que verifique el cumplimiento y la seguridad de cualquier cambio. AWS no se hace responsable de los riesgos que puedan generar la instalación eléctrica o el cableado eléctrico de la instalación de Outpost ni de ningún cambio. No debe realizar ninguna otra modificación en el hardware de los Outposts.

El equipo establecerá la conectividad de red para el bastidor de Outposts a través del enlace ascendente que usted proporcione; asimismo, el equipo configurará la capacidad del bastidor.

La instalación se completará cuando confirmes que la capacidad de Amazon EC2 y Amazon EBS para tu rack de Outposts está disponible en tu. Cuenta de AWS

Requisitos del sitio para los bastidores ACE de Outpost

> **Note**
>
> Solo se aplica si necesita un bastidor ACE.

Un bastidor Aggregation, Core, Edge (ACE) actúa como punto de agregación de red para implementaciones de Outpost con varios bastidores. Debe instalar un bastidor ACE si tiene cuatro o más bastidores de computación. Si tiene menos de cuatro bastidores de computación pero planea ampliarlos a cuatro o más en el futuro, le recomendamos que instale un bastidor ACE.

Para instalar un bastidor ACE, debe cumplir los requisitos de esta sección además de los requisitos enumerados en Requisitos del sitio para los bastidores de Outposts.

> **Note**
>
> Los bastidores ACE no están completamente encerrados y no incluyen una puerta delantera ni una puerta trasera.

Instalación

A continuación, se describen los requisitos de la instalación para un bastidor ACE.

- Alimentación: todos los racks ACE se envían monofásicos de 10 kVA (tipos de conector AA+BB; IEC6 0309 o L6-30P Whip).
- Soporte de peso: el bastidor ACE pesa 705 libras (320 kg).
- Dimensión de espacio libre/tamaño: el bastidor ACE mide 80 in (203 cm) de alto, 24 in (61 cm) de ancho y 42 in (107 cm) de profundidad.

  Si el bastidor ACE tiene brazos para la organización de cables, el ancho del bastidor es de 36 in (91,5 cm).

Red

A continuación, se describen los requisitos de red para un bastidor ACE. Para entender cómo el bastidor de Outposts conecta los dispositivos de red de Outposts, sus dispositivos de red en las instalaciones y sus bastidores de Outposts, consulte Conectividad de bastidor ACE.

- Requisitos de red del bastidor: asegúrese de cumplir los requisitos que se indican en las secciones Conectividad de red local para bastidores de Outposts y Lista de verificación de disponibilidad de red, excepto en lo que respecta a los siguientes cambios:
  - El bastidor ACE tiene cuatro dispositivos de red que se conectan a los dispositivos ascendentes, no dos como en el caso de un solo bastidor de Outposts.
  - Los bastidores ACE no admiten enlaces ascendentes de 1 Gbps.
- Velocidad de enlace ascendente: proporcione enlaces ascendentes con velocidades de 10 Gbps, 40 Gbps o 100 Gbps. Para obtener recomendaciones de ancho de banda para la conexión de enlace de servicio, consulte Recomendaciones de ancho de banda para el enlace de servicio.

  > **Important**
  >
  > Los bastidores ACE no admiten enlaces ascendentes de 1 Gbps.

- Fibra: proporcione fibra monomodo (SMF) con Lucent Connector (LC) o fibra multimodo (MMF) con Lucent Connector (LC). Para ver una lista completa de los tipos de fibra y estándares ópticos admitidos, consulte Velocidad de enlace ascendente, puertos y fibra.
- Dispositivo ascendente: proporcione dos o cuatro dispositivos ascendentes, que pueden ser conmutadores o enrutadores.
- Una VLAN de servicio y una VLAN de puerta de enlace local: para cada uno de los cuatro dispositivos de red de ACE, debe proporcionar una VLAN de servicio y una VLAN de puerta de enlace local diferente. Puede elegir entre proporcionar solo dos opciones distintas VLANs, una para la VLAN de servicio y otra para la VLAN de puerta de enlace local, o tener diferentes dispositivos de red ACE para la VLAN de servicio y la VLAN LGW, con un total de 8 diferentes VLANs . VLANs Para obtener más información sobre cómo se utilizan los grupos de agregación de enlaces (LAGs) y la VLAN, consulte y. Agregación de enlaces Virtual LANs
- CIDR y dirección IP para el enlace de servicio y la puerta de enlace local VLANs: recomendamos asignar una subred dedicada para cada dispositivo de red ACE con un CIDR /30 o /31. Como alternativa, es posible asignar una única subred /29 en cada VLAN de servicio y de puerta de

enlace local. En ambos casos, debe especificar las direcciones IP que van a utilizar los dispositivos de red de ACE. Para obtener más información, consulte Conectividad de capa de red.

- Número de sistema autónomo (ASN) de BGP de cliente y de Outpost para la VLAN de enlace de servicio y una VLAN de puerta de enlace local: el Outpost establece una sesión de emparejamiento de BGP externo (eBGP) entre cada dispositivo de bastidor ACE y su dispositivo de red local para la conectividad de enlace de servicio a través de la VLAN de enlace de servicio. Adicionalmente, establece una sesión de emparejamiento de eBGP desde cada dispositivo de red de ACE a un dispositivo de red local para la conectividad de la red local a la puerta de enlace local. Para obtener más información, consulte Conectividad BGP de Service Link y Conectividad del BGP de la puerta de enlace local.

> **Important**
>
> Subredes de infraestructura de enlace de servicio: se requiere una subred de infraestructura de enlace de servicio (debe ser /26) para cada bastidor de computación incluido en la instalación de Outposts.

Alimentación

A continuación se describen los requisitos de alimentación para un bastidor ACE.

Requisito	Especificación
Tensión de línea AC	Monofásica de 200 a 240 V CA; 50 o 60 Hz
Consumo de energía	Monofásico de 10 kVA (AA+BB)
Protección de corriente alterna (disyuntores ascendentes)	Solo para entradas de 2N (redundante): disyuntor de curva C, curva D o curva K. No se admite una curva B o inferior.
Tipo de entrada AC (receptáculo)	IEC6Tipos de conectores tipo Whip 0309 o L6-30P.

Introducción a los servidores de Outposts

Pida un bastidor de Outposts para empezar. Tras instalar tu equipo Outpost, lanza una EC2 instancia de Amazon y configura la conectividad con tu red local.

Tareas

- Crear un pedido de un bastidor de Outposts
- Lance una instancia en su bastidor de Outposts.
- Optimiza Amazon EC2 para AWS Outposts

Crear un pedido de un bastidor de Outposts

Para empezar a usarlo AWS Outposts, debes crear un Outpost y solicitar la capacidad de Outpost.

Requisitos previos

- Revise las configuraciones disponibles para sus bastidores de Outposts.
- Un sitio de Outpost es la ubicación física del equipo de Outpost. Antes de solicitar capacidad, compruebe que el sitio cumple con los requisitos. Para obtener más información, consulte Requisitos del sitio para los bastidores de Outposts.
- Debe tener un plan AWS Enterprise Support o un plan AWS Enterprise On-Ramp Support.
- Determina cuál Cuenta de AWS usarás para crear el sitio de Outposts, crea el Outpost y realiza el pedido. Supervisa el correo electrónico asociado a esta cuenta para obtener información de. AWS

Tareas

- Paso 1: crear un sitio
- Paso 2: crear un Outpost
- Paso 3: realizar el pedido
- Paso 4: Modificar la capacidad de la instancia
- Pasos a seguir a continuación

Paso 1: crear un sitio

Cree un sitio para especificar la dirección operativa. La dirección operativa es la ubicación física de sus bastidores de Outposts.

Requisitos previos

- Determine la dirección operativa.

Cómo crear un sitio

1. Inicie sesión en AWS.
2. Abre la AWS Outposts consola en https://console.aws.amazon.com/outposts/.
3. Para seleccionar la principal Región de AWS, utilice el selector de regiones situado en la esquina superior derecha de la página.
4. En el panel de navegación, seleccione Sitios.
5. Seleccione Crear sitio.
6. En Tipo de hardware compatible, seleccione Racks y servidores.
7. Introduzca un nombre, una descripción y una dirección operativa para el sitio.
8. Para obtener los detalles del sitio, proporcione la información solicitada del sitio.
    - Peso máximo: el peso máximo del bastidor que puede soportar este sitio; se expresa en libras.
    - Consumo de energía: el consumo de energía disponible en la posición de colocación del hardware para el bastidor, en kVA.
    - Opción de alimentación: la opción de alimentación que puede proporcionar para el hardware.
    - Conector de alimentación: el conector de alimentación que AWS debe utilizar para las conexiones al hardware.
    - Caída de alimentación: indique si la alimentación se produce por encima o por debajo del bastidor.
    - Velocidad de enlace ascendente: la velocidad de enlace ascendente que debe soportar el bastidor para la conexión a la región, en Gbps.
    - Número de enlaces ascendentes: el número de enlaces ascendentes de cada dispositivo de red de Outpost que planifica utilizar para conectar el bastidor a la red.
    - Tipo de fibra: el tipo de fibra que utilizará para conectar el bastidor a la red.

- Estándar óptico: el tipo de estándar óptico que utilizará para conectar el bastidor a la red.

9. (Opcional) En las notas del sitio, introduce cualquier otra información que pueda ser útil AWS para conocer el sitio.
10. Lee los requisitos de las instalaciones y, a continuación, seleccione He leído los requisitos de las instalaciones.
11. Seleccione Crear sitio.

Paso 2: crear un Outpost

Crea un Outpost para sus bastidores. A continuación, especifique este Outpost cuando realice el pedido.

Requisitos previos

- Determine la zona de AWS disponibilidad que desea asociar a su sitio.

Para crear un Outpost

1. En el panel de navegación, elija Outposts.
2. Seleccione Crear Outpost.
3. Elija Bastidores.
4. Escriba un nombre y la descripción de su Outpost.
5. Elija una zona de disponibilidad para su Outpost.
6. (Opcional) Para configurar la conectividad privada, seleccione Usar conectividad privada. Elija una VPC y una subred en la misma Cuenta de AWS zona de disponibilidad que su Outpost. Para obtener más información, consulte the section called “Requisitos previos”.

   > **Note**
   >
   > Si necesita deshacer la conectividad privada de su Outpost, debe ponerse en contacto con AWS Support Center.

7. En ID del sitio, elija el sitio.
8. Seleccione Crear Outpost.

Paso 3: realizar el pedido

Realice un pedido de los bastidores de Outposts que necesite.

> **Important**
>
> No puede editar un pedido después de enviarlo, así que revisa todos los detalles detenidamente antes de enviarlo. Si necesitas cambiar un pedido, ponte en contacto con tu administrador de AWS cuentas.

Requisitos previos

- Determine cómo pagará el pedido. Puede pagar en efectivo, con un pago inicial parcial y sin pagar nada de forma inicial. Si opta por no pagar todo por adelantado, pagará los cargos mensuales durante la vigencia del contrato.

  Los precios incluyen entrega, instalación y mantenimiento de servicios de infraestructura y parches, así como actualizaciones de software.
- Determine si la dirección de entrega es diferente de la dirección operativa que especificó para el sitio.

Hacer un pedido

1. En el panel de navegación, elija Pedidos.
2. Seleccione Realizar pedido.
3. En Tipo de hardware compatible, seleccione Bastidores.
4. Para agregar capacidad, elija una configuración. Si las configuraciones disponibles no satisfacen sus necesidades, puede ponerse en contacto con AWS Support Center para solicitar una configuración de capacidad personalizada.
5. Elija Siguiente.
6. Elija Utilizar un Outpost existente y seleccione el Outpost.
7. Elija Siguiente.
8. Seleccione un plazo del contrato y una opción de pago.
9. Especifique la dirección de envío. Puede especificar una nueva dirección o seleccionar la dirección operativa del sitio. Si selecciona la dirección operativa, tenga en cuenta que cualquier

cambio futuro en la dirección operativa del sitio no se propagará a los pedidos existentes. Si necesita cambiar la dirección de envío de un pedido existente, póngase en contacto con su administrador de cuenta de AWS .

10. Elija Siguiente.
11. En la página Revisar y pedir, compruebe que la información es correcta y edítela según sea necesario. No podrá editar el pedido después de enviarlo.
12. Seleccione Realizar pedido.

Paso 4: Modificar la capacidad de la instancia

Un Outpost proporciona un conjunto de capacidad AWS informática y de almacenamiento en su sitio como una extensión privada de una zona de disponibilidad en una AWS región. Como la capacidad de procesamiento y almacenamiento disponible en Outpost es limitada y está determinada por el tamaño y la cantidad de racks que se AWS instalen en su sitio, usted decide cuánta AWS Outposts capacidad de Amazon, EC2 Amazon EBS y Amazon S3 necesita para ejecutar sus cargas de trabajo iniciales, adaptarse al crecimiento futuro y proporcionar capacidad adicional para mitigar los fallos del servidor y los eventos de mantenimiento.

La capacidad de cada nuevo pedido de Outpost se configura con una configuración de capacidad predeterminada. Puede convertir la configuración predeterminada para crear varias instancias para satisfacer las necesidades de su empresa. Para ello, debe crear una tarea de capacidad, especificar los tamaños y la cantidad de instancias y ejecutar la tarea de capacidad para implementar los cambios.

> **Note**
>
> - Puede cambiar la cantidad de tamaños de instancia después de realizar el pedido de sus Outposts.
> - Los tamaños y las cantidades de las instancias se definen a nivel de Outpost.
> - Las instancias se colocan automáticamente en función de las prácticas recomendadas.

Para modificar la capacidad de las instancias:

1. En el panel de navegación izquierdo de de la consola de AWS Outposts, seleccione Tareas de capacidad.

2. En la página Tareas de capacidad, seleccione Crear tarea de capacidad.
3. En la página Introducción, elija el pedido.
4. Para modificar la capacidad, puede seguir los pasos de la consola o cargar un archivo JSON.

Console steps

1. Elija Modificar la configuración de capacidad de un Outpost.
2. Elija Siguiente.
3. En la página Configurar la capacidad de la instancia, cada tipo de instancia muestra un tamaño de instancia con la cantidad máxima preseleccionada. Para añadir más tamaños de instancia, seleccione Agregar tamaño de instancia.
4. Especifique la cantidad de instancias y anote la capacidad que se muestra para ese tamaño de instancia.
5. Consulte el mensaje al final de cada sección de tipos de instancia que le informa si está por encima o por debajo de su capacidad. Realice ajustes en el nivel de tamaño o cantidad de instancias para optimizar su capacidad total disponible.
6. También puede solicitar la optimización AWS Outposts de la cantidad de instancias para un tamaño de instancia específico. Para ello:
   a. Elija el tamaño de instancia.
   b. Seleccione Equilibrio automático al final de la sección relacionada con el tipo de instancia.
7. Para cada tipo de instancia, asegúrese de que la cantidad de instancias esté especificada para al menos un tamaño de instancia.
8. Elija Siguiente.
9. En la página Revisar y crear, compruebe las actualizaciones que solicita.
10. Selecciona Crear. AWS Outposts crea una tarea de capacidad.
11. En la página de tareas de capacidad, supervise el estado de la tarea.

> **Note**
>
> - AWS Outposts podría solicitarle que detenga una o más instancias en ejecución para permitir la ejecución de la tarea de capacidad. Tras detener estas instancias, AWS Outposts ejecutará la tarea.

- Si necesita cambiar su capacidad después de completar su pedido, póngase en contacto con AWS Support Center para realizar los cambios.

Upload a JSON file

1. Seleccione Cargar la configuración de capacidad.
2. Elija Siguiente.
3. En la página Cargar el plan de configuración de la capacidad de carga, suba el archivo JSON que especifica el tipo, el tamaño y la cantidad de instancias.

   Example

   Ejemplo de archivo JSON:

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

4. Revise el contenido del archivo JSON en la sección Plan de configuración de capacidad.
5. Elija Siguiente.
6. En la página Revisar y crear, compruebe las actualizaciones que solicita.
7. Elija Crear. AWS Outposts crea una tarea de capacidad.
8. En la página de tareas de capacidad, supervise el estado de la tarea.

> **Note**
>
> - AWS Outposts podría solicitarle que detenga una o más instancias en ejecución para permitir la ejecución de la tarea de capacidad. Tras detener estas instancias, AWS Outposts ejecutará la tarea.
> - Si necesita cambiar su capacidad después de completar su pedido, póngase en contacto con AWS Support Center para realizar los cambios.
> - Para solucionar problemas, consulta Solución de problemas de tareas de capacidad.

Pasos a seguir a continuación

Puedes ver el estado de tu pedido desde la AWS Outposts consola. El estado inicial de su pedido es Pedido recibido. Si tiene alguna consulta acerca del pedido, póngase en contacto con AWS Support Center.

Para tramitar el pedido, AWS programaremos una fecha y hora contigo.

También recibirá una lista de verificación con los elementos que debe comprobar o proporcionar antes de la instalación. El equipo de AWS instalación llegará a sus instalaciones en la fecha y hora programadas. El equipo hará rodar el bastidor hasta la posición identificada y el electricista podrá alimentarlo. El equipo establecerá la conectividad de red para el bastidor a través del enlace ascendente que usted proporcione y configurará la capacidad del bastidor. La instalación finaliza cuando confirmas que la capacidad de Amazon EC2 y Amazon EBS para tu Outpost está disponible en tu AWS cuenta.

Lance una instancia en su bastidor de Outposts.

Una vez que esté instalado el Outpost y la capacidad de computación y de almacenamiento estén disponibles para su uso, puede comenzar con la creación de recursos. Lance EC2 instancias de Amazon y cree volúmenes de Amazon EBS en su Outpost mediante una subred de Outpost. También puede crear snapshots de volúmenes de Amazon EBS en su Outpost. Para obtener más información, consulte Amazon EBS local snapshots en AWS Outposts en la Guía del usuario de Amazon EBS.

Requisito previo

Debe tener un Outpost instalado en su sitio. Para obtener más información, consulta Cómo crear un pedido para un rack de Outposts.

Tareas

- Paso 1: Crear una VPC
- Paso 2: Crear una subred y una tabla de enrutamiento personalizada
- Paso 3: Configurar la conectividad de la puerta de enlace local
- Paso 4: Configurar la red en las instalaciones
- Paso 5: Lanzar una instancia en el Outpost
- Paso 6: Comprobar la conectividad

Paso 1: Crear una VPC

Puedes extender cualquier VPC de la AWS región a tu puesto de avanzada. Omita este paso si ya dispone de una VPC que pueda utilizar.

Para crear una VPC para el Outpost:

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. Elija la misma región que la del bastidor de Outposts.
3. En el panel de navegación, elija Su VPCs y, a continuación, elija Crear VPC.
4. Elija Solo VPC.
5. (Opcional) En Etiqueta de nombre, introduzca un nombre para la VPC.
6. Para el bloque IPv4 CIDR, elija la entrada manual IPv4 CIDR e introduzca el rango de IPv4 direcciones de la VPC en el IPv4 cuadro de texto CIDR.

   > **Note**
   >
   > Si quieres usar el enrutamiento directo de VPC, especifique un rango de CIDR que no se superponga con el rango de IP que usa en su red en las instalaciones.

7. Para el bloque IPv6 CIDR, elija Sin bloque CIDR. IPv6
8. En Tenencia, elija Predeterminada.
9. (Opcional) Para agregar una etiqueta a su VPC, elija Agregar etiqueta e ingrese una clave y un valor de etiqueta.

10. Seleccione Creación de VPC.

Paso 2: Crear una subred y una tabla de enrutamiento personalizada

Puedes crear y añadir una subred de Outpost a cualquier VPC de la AWS región a la que se aloja el Outpost. Al hacerlo, la VPC incluirá el Outpost. Para obtener más información, consulta Componentes de red.

> **Note**
>
> Si vas a lanzar una instancia en una subred de Outpost que otra persona ha compartido contigo Cuenta de AWS, ve al paso 5: lanza una instancia en Outpost.

2a: Crear una subred de Outpost

Para crear una subred de Outpost:

1. Abre la consola en AWS Outposts . https://console.aws.amazon.com/outposts/
2. En el panel de navegación, elija Outposts.
3. Seleccione el Outpost y, a continuación, elija Acciones, Crear subred. Se le redirigirá para crear una subred en la consola de Amazon VPC. Seleccionamos el Outpost y la zona de disponibilidad a la que está destinado el Outpost.
4. Seleccione una VPC.
5. En Configuración de la subred, si lo desea, asigne un nombre a la subred y especifique un rango de direcciones IP para ella.
6. Elija Create subnet (Crear subred).
7. (Opcional) Para facilitar la identificación de las subredes de Outpost, habilite la columna ID de Outpost en la página Subredes. Para habilitar la columna, seleccione el icono Preferencias, seleccione ID de Outpost y elija Confirm.

2b: Crear una tabla de enrutamiento personalizada

Utilice el siguiente procedimiento para crear una tabla de enrutamiento personalizada con una ruta a la puerta de enlace local. No puede usar la misma tabla de enrutamiento que las subredes de la zona de disponibilidad.

Para crear una tabla de enrutamiento personalizada

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Tablas de enrutamiento.
3. Elija Create Route Table (Crear tabla de enrutamiento).
4. (Opcional) En Name (Etiqueta), escriba el nombre de la tabla de enrutamiento.
5. En VPC, elija su VPC.
6. (Opcional) Para agregar una etiqueta, elija Add new tag (Agregar etiqueta nueva) e ingrese la clave y el valor de la etiqueta.
7. Elija Create Route Table (Crear tabla de enrutamiento).

2c: Asociar la subred de Outpost y la tabla de enrutamiento personalizada

Para aplicar rutas de tablas de ruteo a una subred determinada, debe asociar la tabla de enrutamiento a la subred. Una tabla de enrutamiento se puede asociar con varias subredes. Sin embargo, una subred sólo puede asociarse a una tabla de enrutamiento a la vez. Las subredes que no estén asociadas de manera explícita a ninguna tabla se asociarán implícitamente a la tabla de enrutamiento principal de forma predeterminada.

Para asociar la subred de Outpost y la tabla de enrutamiento personalizada:

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Tablas de enrutamiento.
3. En la pestaña Subnet associations (Asociaciones de subred), elija Edit subnet associations (Editar asociaciones de subred).
4. Seleccione la casilla de verificación para la subred que desee asociar a la tabla de enrutamiento.
5. Seleccione Save associations (Guardar asociaciones).

Paso 3: Configurar la conectividad de la puerta de enlace local

La puerta de enlace local (LGW) permite la conectividad entre las subredes de Outpost y la red en las instalaciones.

Para obtener más información sobre la LGW, consulte Puertas de enlace locales.

Para proporcionar conectividad entre una instancia de la subred de Outposts y su red local, debe completar las siguientes tareas.

3a. Crear una tabla de enrutamiento de la puerta de enlace local personalizada

Utilice el siguiente procedimiento para crear una tabla de enrutamiento personalizada para su puerta de enlace local.

Para crear una tabla de enrutamiento de la puerta de enlace local personalizada:

1. Abra la AWS Outposts consola en. https://console.aws.amazon.com/outposts/
2. Para cambiarla Región de AWS, usa el selector de regiones en la esquina superior derecha de la página.
3. En el panel de navegación, elija Tabla de enrutamiento de puerta de enlace local.
4. Elija Crear tabla de enrutamiento de puerta de enlace local.
5. (Opcional) En Name (Etiqueta), escriba el nombre de la tabla de enrutamiento.
6. En Puerta de enlace local, elija la puerta de enlace local.
7. En Modo, elija un modo de comunicación con la red en las instalaciones.
   - Elija Enrutamiento directo de VPC para usar las direcciones IP privadas de su instancia.
   - Elija CoIP para usar direcciones de los grupos de direcciones IP propiedad de sus clientes. Para obtener más información, consulte Crear un grupo de CoIP.
8. (Opcional) Para agregar una etiqueta, elija Agregar nueva etiqueta e introduzca una clave y un valor de etiqueta.
9. Elija Crear tabla de enrutamiento de puerta de enlace local.

3b: Asociar la VPC a la tabla de enrutamiento personalizada

Utilice el siguiente procedimiento para asociar la VPC a la tabla de enrutamiento de la puerta de enlace local. No están asociadas de forma predeterminada.

Para Asociar una VPC a una tabla de enrutamiento de puerta de enlace local:

1. Abra la AWS Outposts consola en. https://console.aws.amazon.com/outposts/
2. Para cambiarla Región de AWS, usa el selector de regiones en la esquina superior derecha de la página.
3. En el panel de navegación, elija Tablas de enrutamiento de puerta de enlace de tránsito.

4. Seleccione la tabla de enrutamiento y, a continuación, elija Acciones, VPC asociada.
5. Para el ID de VPC, seleccione la VPC que desee asociar a la tabla de enrutamiento de la puerta de enlace local.
6. (Opcional) Para agregar una etiqueta, elija Agregar nueva etiqueta e introduzca una clave y un valor de etiqueta.
7. Elija Asociar VPC.

3c: Agregar una entrada de ruta en la tabla de enrutamiento de subred de Outpost

Agregue una entrada de ruta en la tabla de enrutamiento de subred de Outpost para habilitar el tráfico entre las subredes de Outpost y la puerta de enlace local.

Las subredes de Outpost dentro de una VPC, que está asociada a una tabla de enrutamiento de puerta de enlace local, pueden tener un tipo de destino adicional de un ID de puerta de enlace local de Outpost para sus tablas de enrutamiento. Considere el caso en el que desea enrutar el tráfico con una dirección de destino de 172.16.100.0/24 a la red del cliente a través de la puerta de enlace local. Para ello, edite la tabla de enrutamiento de la subred de Outpost y añada la siguiente ruta con la red de destino y una puerta de enlace local como destino.

Destino	Objetivo
172.16.100.0/24	`lgw-id`

Para agregar una entrada de enrutamiento con la puerta de enlace local como destino en la tabla de enrutamiento de subred:

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, seleccione Tablas de enrutamiento y elija la tabla de enrutamiento que ha creado en 2b: Crear una tabla de enrutamiento personalizada.
3. Elija Acciones y, a continuación, Editar rutas.
4. Para agregar una ruta, elija Añadir ruta.
5. En Destino, introduzca el bloque de CIDR de destino en la red del cliente.
6. En Destino, elija el ID de puerta de enlace local de Outpost.
7. Seleccione Save changes (Guardar cambios).

3d: Cree un dominio de enrutamiento de puerta de enlace local asociando la tabla de rutas personalizada a los grupos de VIF

Los grupos VIF son agrupaciones lógicas de interfaces virtuales (). VIFs Asocie la tabla de rutas de la puerta de enlace local al grupo VIF para crear un dominio de enrutamiento de la puerta de enlace local.

Para asociar la tabla de enrutamiento personalizada a los grupos de VIF:

1. Abra la AWS Outposts consola en. https://console.aws.amazon.com/outposts/
2. Para cambiarla Región de AWS, usa el selector de regiones en la esquina superior derecha de la página.
3. En el panel de navegación, elija Redes y, a continuación, Dominio de enrutamiento LGW.
4. Elija Crear dominio de enrutamiento LGW.
5. Introduzca un nombre para el dominio de enrutamiento de la puerta de enlace local.
6. Elija la puerta de enlace local, el grupo VIF de la puerta de enlace local y la tabla de enrutamiento de la puerta de enlace local.
7. Elija Crear dominio de enrutamiento LGW.

3e: Agregar una entrada de ruta en la tabla de enrutamiento

Edite la tabla de enrutamiento de la puerta de enlace local para agregar una ruta estática que tenga el grupo de VIF como destino y el rango de CIDR de la subred en las instalaciones (o 0.0.0.0/0) como destino.

Destino	Objetivo
172.16.100.0/24	`VIF-Group-ID`

Para agregar una entrada de ruta en la tabla de enrutamiento de la LGW:

1. Abra la AWS Outposts consola en. https://console.aws.amazon.com/outposts/
2. En el panel de navegación, elija Tabla de enrutamiento de puerta de enlace local.
3. Seleccione la tabla de enrutamiento de la puerta de enlace local y, a continuación, elija Acciones, Editar rutas.
4. Seleccione Añadir ruta.

5. En Destino introduzca el bloque de CIDR de destino, una única dirección IP o el ID de una lista de prefijos.
6. En Objetivo, seleccione el ID de la puerta de enlace local.
7. Elija Guardar rutas.

3f: (Opcional) Asignar una dirección IP propiedad del cliente a la instancia

Si ha configurado sus Outposts en la 3a. Crear una tabla de enrutamiento de la puerta de enlace local personalizada para usar un grupo de direcciones IP (CoIP) propiedad del cliente, debe asignar una dirección IP elástica del grupo de direcciones CoIP y asociar la dirección IP elástica a la instancia. Para obtener más información, consulte Direcciones IP propiedad del cliente.

Si ha configurado sus Outposts para usar el enrutamiento directo de VPC (DVR), omita este paso.

Grupos de direcciones IP compartidos propiedad del cliente

Si desea utilizar un grupo de direcciones IP compartido propiedad del cliente, debe compartirlo antes de iniciar la configuración. Para obtener información sobre cómo compartir una dirección propiedad del cliente IPv4 , consulte. the section called “Uso compartido de un recurso de Outpost”

Paso 4: Configurar la red en las instalaciones

El Outpost establece un emparejamiento de BGP externo desde cada dispositivo de red de Outpost (OND) a un dispositivo de red local (CND) del cliente para enviar y recibir tráfico desde su red en las instalaciones a los Outposts.

Para obtener más información, consulte Conectividad del BGP de la puerta de enlace local.

Para enviar y recibir tráfico desde la red en las instalaciones al Outpost, asegúrese de lo siguiente:

- En los dispositivos de red de sus clientes, la sesión de BGP en la VLAN de la puerta de enlace local está en un estado ACTIVO desde sus dispositivos de red.
- Para el tráfico que va desde las instalaciones a los Outposts, asegúrese de recibir en su CND los anuncios de BGP de Outposts. Estos anuncios de BGP contienen las rutas que la red en las instalaciones debe utilizar para enrutar el tráfico desde las instalaciones al Outpost. Por lo tanto, asegúrese de que su red tenga la ruta correcta entre los Outposts y los recursos en las instalaciones.
- Para el tráfico que va de Outposts a la red local, asegúrese de enviar los anuncios de ruta BGP de CNDs las subredes de la red local a Outposts (o 0.0.0.0/0). Como alternativa, puede anunciar

una ruta predeterminada (p. ej. 0.0.0.0/0) a los Outposts. Las subredes locales que anuncie CNDs deben tener un rango de CIDR igual o estar incluido en el rango de CIDR en el que configuró. 3e: Agregar una entrada de ruta en la tabla de enrutamiento

Ejemplo: Anuncios de BGP en modo de VPC directa

Considere el escenario en el que tiene un Outpost, configurado en modo de VPC directa, con dos dispositivos de red de bastidor de Outposts conectados por una VLAN de puerta de enlace local a dos dispositivos de red local de cliente. Se configura lo siguiente:

- Una VPC con un bloque CIDR 10.0.0.0/16.
- Una subred de Outpost en la VPC con un bloque de CIDR 10.0.3.0/24.
- Una subred en la red en las instalaciones con un bloque de CIDR 172.16.100.0/24
- Outposts utiliza la dirección IP privada de las instancias de la subred de Outpost, por ejemplo 10.0.3.0/24, para comunicarse con su red en las instalaciones.

En este escenario, la ruta anunciada por:

- La puerta de enlace local a los dispositivos de cliente es 10.0.3.0/24.
- Los dispositivos de cliente a la puerta de enlace local de Outpost es 172.16.100.0/24.

Como resultado, la puerta de enlace local enviará tráfico saliente con destino a la red 172.16.100.0/24 a los dispositivos de cliente. Asegúrese de que la red tenga la configuración de enrutamiento correcta para entregar el tráfico al host de destino de la red.

Para obtener información sobre los comandos y la configuración específicos necesarios para comprobar el estado de las sesiones de BGP y las rutas anunciadas dentro de esas sesiones, consulte la documentación de su proveedor de redes.

Para solucionar problemas, consulte Lista de comprobación de solución de problemas de redes en bastidor de AWS Outposts.

Ejemplo: Anuncios de BGP en modo de CoIP

Considere el escenario en el que tiene un Outpost con dos dispositivos de red de bastidor de Outposts conectados por una VLAN de puerta de enlace local a dos dispositivos de red local de cliente. Se configura lo siguiente:

- Una VPC con un bloque CIDR 10.0.0.0/16.
- Una subred en la VPC con un bloque CIDR 10.0.3.0/24.
- Un grupo de IP propiedad del cliente (10.1.0.0/26).
- Una asociación de direcciones IP elásticas que asigna de 10.0.3.112 a 10.1.0.2.
- Una subred en la red en las instalaciones con un bloque de CIDR 172.16.100.0/24
- La comunicación entre el Outpost y la red local utilizará el CoIP Elastic IPs para abordar las instancias del Outpost, no se utilizará el rango CIDR de VPC.

En este escenario, la ruta anunciada por:

- La puerta de enlace local a los dispositivos de cliente es is 10.1.0.0/26.
- Los dispositivos de cliente a la puerta de enlace local de Outpost es 172.16.100.0/24.

Como resultado, la puerta de enlace local enviará tráfico saliente con destino a la red 172.16.100.0/24 a los dispositivos de cliente. Asegúrese de que la red tenga la configuración de enrutamiento correcta para entregar el tráfico al host de destino de la red.

Para obtener información sobre los comandos y la configuración específicos necesarios para comprobar el estado de las sesiones de BGP y las rutas anunciadas dentro de esas sesiones, consulte la documentación de su proveedor de redes.

Para solucionar problemas, consulte Lista de comprobación de solución de problemas de redes en bastidor de AWS Outposts.

Para solucionar problemas, consulte Lista de comprobación de solución de problemas de redes en bastidor de AWS Outposts.

Paso 5: Lanzar una instancia en el Outpost

Puedes lanzar EC2 instancias en la subred de Outpost que has creado o en una subred de Outpost que se haya compartido contigo. Los grupos de seguridad controlan el tráfico entrante y saliente de la VPC para las instancias de una subred de Outpost, al igual que lo hacen para las instancias de una subred de una zona de disponibilidad. Para conectarse a una EC2 instancia de una subred de Outpost, puede especificar un key par al lanzar la instancia, del mismo modo que lo hace con las instancias de una subred de una zona de disponibilidad.

Consideraciones

- Si vas a adjuntar volúmenes de datos en bloque respaldados por sistemas de almacenamiento en bloques de terceros compatibles durante el proceso de lanzamiento de la instancia en Outpost, consulta esta entrada del blog Cómo simplificar el uso del almacenamiento en bloque de terceros con. AWS Outposts
- Puedes crear un grupo de ubicación para influir en la forma en que Amazon EC2 debe intentar colocar grupos de instancias interdependientes en el hardware de Outposts. Puede elegir la estrategia de grupos de ubicación que mejor se adapte a las necesidades de la carga de trabajo.
- Si el Outpost se ha configurado para usar un grupo de direcciones IP (CoIP) propiedad del cliente, debe asignar una dirección IP propiedad del cliente a todas las instancias que lance.

Para iniciar instancias en una subred de Outpost

1. Abre la AWS Outposts consola en. https://console.aws.amazon.com/outposts/
2. En el panel de navegación, elija Outposts.
3. Seleccione el Outpost y, a continuación, elija Acciones, Ver detalles.
4. En la página de Resumen de Outpost, seleccione Lanzar instancia. Se le redirigirá al asistente de lanzamiento de instancias en la EC2 consola de Amazon. Seleccionamos la subred de Outpost por usted y le mostramos solo los tipos de instancia compatibles con su bastidor de Outposts.
5. Elija un tipo de instancia que sea admitida por su bastidor de Outposts. Tenga en cuenta que las instancias que aparecen atenuadas no están disponibles.
6. (Opcional) Para lanzar las instancias a un grupo de ubicación, expanda Detalles avanzados y desplácese hasta Grupo de ubicación. Puede seleccionar un grupo de ubicación existente o crear uno nuevo.
7. Complete el asistente para lanzar la instancia en la subred del Outpost. Para obtener más información, consulta Cómo lanzar una EC2 instancia en la Guía del EC2 usuario de Amazon:

> **Note**
>
> Si agrega un volumen de Amazon EBS, debe utilizar el tipo de volumen gp2.

Paso 6: Comprobar la conectividad

Puede probar la conectividad mediante los casos de uso adecuados.

Pruebe la conectividad desde la red local al Outpost

Desde un ordenador de la red local, ejecute el comando `ping` en la dirección IP privada de la instancia de Outpost.

```
ping 10.0.3.128
```

A continuación, se muestra un ejemplo del resultado.

```
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
```

Pruebe la conectividad desde una instancia de Outpost a su red local

En función de su sistema operativo, utilice ssh o rdp para conectarse a la dirección IP privada de su instancia del Outpost. Para obtener información sobre la conexión a una instancia de Linux, consulta Conéctate a tu EC2 instancia en la Guía del EC2 usuario de Amazon.

Una vez ejecutada la instancia, ejecute el comando de `ping` en una dirección IP de una computadora de la red local. En el siguiente ejemplo, la dirección IP es 172.16.0.130.

```
ping 172.16.0.130
```

A continuación, se muestra un ejemplo del resultado.

```
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
```

Pruebe la conectividad entre la AWS región y el puesto avanzado

Lance una instancia en la subred de la AWS región. Por ejemplo, utilice el comando run-instances.

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

Una vez que se esté ejecutando la instancia, realice las siguientes operaciones:

1. Obtenga la dirección IP privada de la instancia en la AWS región. Esta información está disponible en la EC2 consola de Amazon, en la página de detalles de la instancia.
2. En función de su sistema operativo, utilice ssh o rdp para conectarse a la dirección IP privada de su instancia del Outpost.
3. Ejecuta el ping comando desde tu instancia de Outpost y especifica la dirección IP de la instancia en la AWS región.

   ```
   ping 10.0.1.5
   ```

   A continuación, se muestra un ejemplo del resultado.

   ```
   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
```

Ejemplos de conectividad de direcciones IP propiedad del cliente

Pruebe la conectividad de la red local al Outpost

Desde un ordenador de la red local, ejecute el comando `ping` en la dirección IP propiedad del cliente de la instancia de Outpost.

```
ping 172.16.0.128
```

A continuación, se muestra un ejemplo del resultado.

```
Pinging 172.16.0.128

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

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

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

Pruebe la conectividad desde una instancia de Outpost a su red local

En función de su sistema operativo, utilice ssh o rdp para conectarse a la dirección IP privada de su instancia del Outpost. Para obtener más información, consulta Connect to your EC2 instance en la Guía del EC2 usuario de Amazon.

Una vez ejecutada la instancia de Outpost, ejecute el comando `ping` en una dirección IP de un ordenador de la red local.

```
ping 172.16.0.130
```

A continuación, se muestra un ejemplo del resultado.

```
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
```

Pruebe la conectividad entre la AWS región y el puesto de avanzada

Lance una instancia en la subred de la AWS región. Por ejemplo, utilice el comando run-instances.

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

Una vez que se esté ejecutando la instancia, realice las siguientes operaciones:

1. Obtenga la dirección IP privada de la instancia de la AWS región, por ejemplo, 10.0.0.5. Esta información está disponible en la EC2 consola de Amazon, en la página de detalles de la instancia.
2. En función de su sistema operativo, utilice ssh o rdp para conectarse a la dirección IP privada de su instancia del Outpost.
3. Ejecuta el `ping` comando desde tu instancia de Outpost a la dirección IP de la instancia AWS regional.

   ```
   ping 10.0.0.5
   ```

   A continuación, se muestra un ejemplo del resultado.

   ```
   Pinging 10.0.0.5
   ```

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

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

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

Optimiza Amazon EC2 para AWS Outposts

A diferencia de Amazon Elastic Compute Cloud (Amazon EC2) Región de AWS, la capacidad de un Outpost es finita. Se encuentra limitado por el volumen total de capacidad de cómputo que solicitó. En este tema se ofrecen las prácticas recomendadas y las estrategias de optimización que le ayudarán a aprovechar al máximo la EC2 capacidad de Amazon en AWS Outposts.

Contenido

Hosts dedicados en Outposts

Un host EC2 dedicado de Amazon es un servidor físico con capacidad de EC2 instancia totalmente dedicada a su uso. Su Outpost ya le proporciona hardware dedicado, pero el host dedicado le permite usar las licencias de software existentes con restricciones de licencia por conector, por núcleo o por VM frente un solo host. Para obtener más información, consulta Hosts dedicados AWS Outposts en la Guía del EC2 usuario de Amazon.

Además de conceder licencias, los propietarios de Outpost pueden utilizar hosts dedicados para optimizar los servidores en sus implementaciones de Outpost de dos maneras:

- Alterar el diseño de la capacidad de un servidor
- Controlar la ubicación de las instancias a nivel de hardware

Alteración del diseño de la capacidad de un servidor

Dedicated Hosts le ofrece la posibilidad de modificar el diseño de los servidores de su implementación de Outpost sin necesidad de contactar con Soporte ellos. Cuando adquieres capacidad para tu Outpost, especificas el diseño de EC2 capacidad que proporciona cada servidor. Cada servidor admite una única familia de tipos de instancias. Un diseño puede ofrecer un solo tipo de instancia o varios tipos de instancia. Los hosts dedicados le permiten modificar lo que haya elegido para ese diseño inicial. Si asigna un host para que admita un único tipo de instancia para toda la capacidad, solo podrá lanzar un único tipo de instancia desde ese host. La siguiente ilustración presenta un servidor m5.24xlarge con un diseño homogéneo:

Puede asignar la misma capacidad para varios tipos de instancias. Cuando asigna un host para que admita varios tipos de instancias, obtiene un diseño heterogéneo que no requiere un diseño de capacidad explícito. La siguiente ilustración presenta un servidor m5.24xlarge con un diseño heterogéneo a plena capacidad:

Para obtener más información, consulte Asignar un host dedicado en la Guía del EC2 usuario de Amazon.

Controlar la ubicación de las instancias a nivel de hardware

Puede usar hosts dedicados para controlar la ubicación de las instancias a nivel de hardware. Utilice la autoubicación para los hosts dedicados para determinar si las instancias que lanza se lanzan en un host específico o en cualquier host disponible que tenga configuraciones coincidentes. Utilice la afinidad del host para establecer una relación entre una instancia y un host dedicado. Si tiene un bastidor de Outposts, puede usar estas características de hosts dedicados para minimizar el impacto de los fallos de hardware relacionados. Para obtener más información sobre la recuperación de instancias, consulte Ubicación automática de hosts dedicados y afinidad de hosts en la Guía del EC2 usuario de Amazon.

Puede compartir hosts dedicados utilizando AWS Resource Access Manager. Compartir hosts dedicados le permite distribuir los hosts en una implementación de Outpost entre Cuentas de AWS. Para obtener más información, consulte Recursos de compartidos.

Configuración de recuperación de instancias

Las instancias de su Outpost que estén en mal estado debido a un fallo de hardware se deben migrar a un host en buen estado. Puede configurar la recuperación automática para que esta migración se

realice automáticamente en función de las comprobaciones del estado de la instancia. Para obtener más información, consulte Resiliencia de las instancias.

Grupos de ubicación en Outposts

AWS Outposts admite grupos de colocación. Usa los grupos de ubicación para influir en la forma en que Amazon EC2 debe intentar colocar los grupos de instancias interdependientes que lances en el hardware subyacente. Puede utilizar diferentes estrategias (ubicación de clústeres, particiones o lotes) para satisfacer las necesidades de las distintas cargas de trabajo. Si tiene un Outpost de un solo bastidor, puede usar la estrategia de dispersión para colocar las instancias en los hosts en lugar de en los bastidores.

Grupos de ubicación distribuida

Utilice un grupo con ubicación distribuida para distribuir una sola instancia en distintos tipos de hardware. El lanzamiento de instancias en un grupo con ubicación distribuida reduce el riesgo de fallos simultáneos que podrían producirse cuando las instancias utilizan el mismo equipo. Los grupos de ubicación pueden distribuir instancias entre bastidores o hosts. Solo puede utilizar grupos de ubicación dispersos a nivel de anfitrión con AWS Outposts.

Grupos de ubicación a nivel de distribución de bastidor

Su grupo de ubicación a nivel de distribución de bastidores puede contener tantas instancias como bastidores tenga en su implementación del Outpost. En la siguiente ilustración, se muestra una implementación de Outpost de tres bastidores que ejecuta tres instancias en un grupo de ubicación a nivel de dispersión de bastidores.

Grupos de ubicación a nivel de distribución de hosts

Su grupo de ubicación de niveles dispersos de hosts puede contener tantas instancias como hosts tenga en su implementación de Outpost. En la siguiente ilustración, se muestra una implementación de Outpost de un solo bastidor que ejecuta tres instancias en un grupo de ubicación a nivel de dispersión de hosts.

Grupos de ubicación de particiones

Utilice un grupo con ubicación en particiones para distribuir varias instancias en bastidores con particiones. Cada partición puede contener múltiples instancias. Puede usar la distribución

automática para distribuir las instancias entre las particiones o implementar instancias en las particiones de destino. La siguiente ilustración muestra un grupo con ubicación en particiones con distribución automática.

También puede implementar instancias en las particiones de destino. La siguiente ilustración muestra un grupo con ubicación en particiones con una distribución segmentada.

Para obtener más información sobre cómo trabajar con grupos de ubicación, consulte Grupos de ubicación y Grupos de ubicación AWS Outposts en la Guía del EC2 usuario de Amazon.

Para obtener más información sobre la AWS Outposts alta disponibilidad, consulte Consideraciones de arquitectura y diseño de AWS Outposts alta disponibilidad.

AWS Outposts conectividad con las AWS regiones

AWS Outposts admite la conectividad de red de área amplia (WAN) a través de la conexión de enlace de servicio.

Contenido

Conectividad a través de enlace de servicio

El enlace de servicio es una conexión necesaria entre sus Outposts y la región de AWS (o la región de origen). Permite la gestión de los Outposts y el intercambio de tráfico hacia y desde la AWS Región. El enlace de servicio utiliza un conjunto cifrado de conexiones VPN para comunicarse con la región de origen.

Una vez establecida la conexión de enlace de servicio, su puesto de avanzada pasa a estar operativo y es gestionado por. AWS El enlace de servicio se utiliza para el siguiente tráfico:

- Tráfico de VPC del cliente entre el Outpost y cualquier servidor asociado. VPCs
- El tráfico de administración de Outposts, como la administración de recursos, la supervisión de recursos y las actualizaciones de firmware y software.

Requisitos de unidad de transmisión máxima (MTU) del enlace de servicio

La unidad de transmisión máxima (MTU) de una conexión de red es el tamaño, en bytes, del mayor paquete permitido que se puede transferir a través de la conexión. La red debe admitir una MTU de 1500 bytes entre el Outpost y los puntos de conexión del enlace de servicio en la región de AWS principal.

El tráfico que va de una instancia en Outposts a una instancia en la región tiene una MTU de 1300.

Recomendaciones de ancho de banda para el enlace de servicio

Para una experiencia y una resiliencia óptimas, AWS requiere que utilice una conectividad redundante de al menos 500 Mbps para cada rack de cómputo y una latencia máxima de ida y vuelta de 175 ms para la conexión del enlace de servicio a la AWS región. Puede utilizar AWS Direct Connect o una conexión de Internet para el enlace del servicio. Los requisitos de tiempo mínimo de 500 Mbps y máximo de ida y vuelta para la conexión de enlace de servicio le permiten lanzar EC2 instancias de Amazon, adjuntar volúmenes de Amazon EBS y acceder a AWS servicios, como Amazon EKS, Amazon EMR CloudWatch y métricas con un rendimiento óptimo.

Los requisitos de ancho de banda para el enlace de un servicio de Outposts varían en función de las siguientes características:

- Número de AWS Outposts racks y configuraciones de capacidad
- Características de la carga de trabajo, como el tamaño de la AMI, la elasticidad de las aplicaciones, las necesidades de velocidad de ráfaga y el tráfico de Amazon VPC a la región

Para recibir una recomendación personalizada sobre el ancho de banda de Service Link necesario para sus necesidades, póngase en contacto con su representante de AWS ventas o socio de APN.

Conexiones de Internet redundantes

Cuando cree conectividad desde su puesto de avanzada con la AWS región, le recomendamos que cree varias conexiones para aumentar la disponibilidad y la resiliencia. Para obtener más información, consulte Recomendaciones de resiliencia de AWS Direct Connect.

Si necesita conectividad a la Internet pública, puede usar conexiones a Internet redundantes y diversos proveedores de Internet, tal como lo haría con sus cargas de trabajo en las instalaciones existentes.

Configura tu enlace de servicio

En los siguientes pasos se explica el proceso de configuración del enlace de servicio.

1. Elige una opción de conexión entre tus Outposts y la región de origen AWS . Puedes elegir una conexión pública o privada.
2. Una vez que hayas pedido tus racks de Outposts, se pondrá en AWS contacto contigo para recopilar la VLAN, la IP, el BGP y la subred de infraestructura. IPs Para obtener más información, consulte Conectividad de red local.

3. Durante la instalación, AWS configura el enlace de servicio en el Outpost en función de la información que ha proporcionado.
4. Los dispositivos de red locales, como los enrutadores, se configuran para que se conecten a cada dispositivo de red de Outpost a través de la conectividad BGP. Para obtener información sobre la conectividad VLAN, IP y BGP de enlace de servicio, consulte Red.
5. Configura sus dispositivos de red, como los firewalls, para permitir que sus Outposts accedan a AWS la región o región de origen. AWS Outposts utiliza la subred de la infraestructura de enlace de servicios IPs para configurar las conexiones VPN e intercambiar el control y el tráfico de datos con la región. El establecimiento del enlace de servicio siempre se inicia desde el Outpost.

> **Note**
>
> No podrá modificar la configuración del enlace de servicio después de completar el pedido.

Opciones de conectividad pública de Service Link

Puedes configurar el enlace de servicio con una conexión pública para el tráfico entre los Outposts y la región de origen AWS . Puede elegir entre utilizar la Internet pública o la AWS Direct Connect pública VIFs.

Si planea incluir solo la AWS región pública IPs (en lugar de la 0.0.0.0/0) en sus firewalls, debe asegurarse de que las reglas de su firewall se up-to-date ajusten a los rangos de direcciones IP actuales. Para obtener más información, consulte Rangos de dirección IP de AWS en la Guía del usuario de Amazon VPC.

La siguiente imagen muestra ambas opciones para establecer una conexión pública de enlace de servicio entre tus Outposts y la AWS región:

Opción 1. Conectividad pública a través de internet

Esta opción requiere que la subred IPs de infraestructura de enlace de AWS Outposts servicios tenga acceso a los rangos de IP públicas de su AWS región o región de origen. Debe permitir incluir la AWS región pública IPs o 0.0.0.0/0 en los dispositivos de red, como su firewall.

Opción 2. AWS Direct Connect Conectividad pública a través de redes públicas VIFs

Esta opción requiere que la subred IPs de la infraestructura de enlace de AWS Outposts servicios tenga acceso a los rangos de IP públicas de su AWS región o región de origen a través del servicio DX. Debe permitir incluir la AWS región pública IPs o 0.0.0.0/0 en los dispositivos de red, como su firewall.

Opciones de conectividad privada de Service Link

Puedes configurar el enlace del servicio con una conexión privada para el tráfico entre los Outposts y la región de origen AWS . Puede optar por utilizar el transporte AWS Direct Connect privado o el de tránsito VIFs.

Selecciona la opción de conectividad privada al crear tu Outpost en la AWS Outposts consola. Para obtener instrucciones, consulta Cómo crear un puesto de avanzada.

Al seleccionar la opción de conectividad privada, se establece una conexión VPN de enlace de servicio después de instalar el Outpost, mediante una VPC y una subred que especifique. Esto permite la conectividad privada a través de la VPC y minimiza la exposición pública a Internet.

La siguiente imagen muestra ambas opciones para establecer una conexión privada VPN de enlace de servicio entre tus Outposts y la AWS región:

Requisitos previos

Para poder configurar la conectividad privada de su Outpost, debe cumplir con los siguientes requisitos previos:

- Debe configurar permisos para que una entidad de IAM (usuario o rol) permita al usuario o al rol crear o editar el rol vinculado al servicio para una conectividad privada. La entidad de IAM necesita permiso para acceder a las siguientes acciones:
  - `iam:CreateServiceLinkedRole` del `arn:aws:iam::*:role/aws-service-role/outposts.amazonaws.com/AWSServiceRoleForOutposts*`
  - `iam:PutRolePolicy` del `arn:aws:iam::*:role/aws-service-role/outposts.amazonaws.com/AWSServiceRoleForOutposts*`

  - `ec2:DescribeVpcs`
  - `ec2:DescribeSubnets`

  Para obtener más información, AWS Identity and Access Management consulte AWS Outposts
- En la misma AWS cuenta y zona de disponibilidad que su Outpost, cree una VPC con el único propósito de la conectividad privada de Outpost con una subred /25 o superior que no entre en conflicto con la versión 10.1.0.0/16. Por ejemplo, puedes usar 10.3.0.0/16.
- Configure el grupo de seguridad de subred para permitir el tráfico en las direcciones de entrada y salida del UDP 443.
- Anuncie el CIDR de la subred en las instalaciones. Puede usarlo AWS Direct Connect para hacerlo. Para obtener más información, consulte Interfaces virtuales de AWS Direct Connect y Uso de puertas de enlace de AWS Direct Connect en la Guía del usuario de AWS Direct Connect .

> **Note**
>
> Para seleccionar la opción de conectividad privada cuando tu Outpost esté en estado PENDIENTE, selecciona Outposts en AWS Outposts la consola y selecciona tu Outpost. Seleccione Acciones, Agregar conectividad privada y siga los pasos.

Tras seleccionar la opción de conectividad privada para tu Outpost, crea AWS Outposts automáticamente un rol vinculado al servicio en tu cuenta que le permite completar las siguientes tareas en tu nombre:

- Crea interfaces de red en la subred y la VPC que especifique, y crea un grupo de seguridad para las interfaces de red.
- Concede permiso al AWS Outposts servicio para conectar las interfaces de red a una instancia de punto final de enlace de servicio de la cuenta.
- Adjunta las interfaces de red a las instancias del punto de conexión del enlace de servicio desde la cuenta.

> **Important**
>
> Una vez instalado tu Outpost, confirma la conectividad a la red privada IPs de tu subred desde tu Outpost.

Opción 1. Conectividad privada a través de privada AWS Direct Connect VIFs

Cree una AWS Direct Connect conexión, una interfaz virtual privada y una puerta de enlace privada virtual para permitir que su Outpost local acceda a la VPC.

Para obtener más información, consulte las siguientes secciones de la Guía del AWS Direct Connect usuario:

- Conexiones dedicadas y alojadas
- Cree una interfaz virtual privada
- Asociaciones de pasarelas privadas virtuales

Si la AWS Direct Connect conexión se realiza en una AWS cuenta diferente a la de su VPC, consulte Asociación de una puerta de enlace privada virtual entre cuentas en la Guía del AWS Direct Connect usuario.

Opción 2. Conectividad privada a través del tránsito AWS Direct Connect VIFs

Cree una AWS Direct Connect conexión, una interfaz virtual de tránsito y una puerta de enlace de tránsito para permitir que su Outpost local acceda a la VPC.

Para obtener más información, consulte las siguientes secciones de la Guía del AWS Direct Connect usuario:

- Conexiones dedicadas y alojadas
- Cree una interfaz virtual de tránsito para la puerta de enlace Direct Connect
- Asociaciones de la puerta de enlace de tránsito

Firewalls y enlace de servicio

En esta sección, se describen las configuraciones del firewall y la conexión del enlace de servicio.

En el siguiente diagrama, la configuración extiende la Amazon VPC desde la AWS región hasta el Outpost. Una interfaz virtual AWS Direct Connect pública es la conexión de enlace de servicio. El siguiente tráfico pasa por el enlace de servicio y la conexión de AWS Direct Connect :

- Tráfico de administración al Outpost a través del enlace de servicio
- Tráfico entre el puesto de avanzada y cualquier dispositivo asociado VPCs

Si utiliza un firewall activo en su conexión a Internet para limitar la conectividad de la Internet pública a la VLAN del enlace de servicio, puede bloquear todas las conexiones entrantes que se inicien desde Internet. Esto se debe a que la VPN del enlace de servicio se inicia solo desde el Outpost a la región, y no desde la región al Outpost.

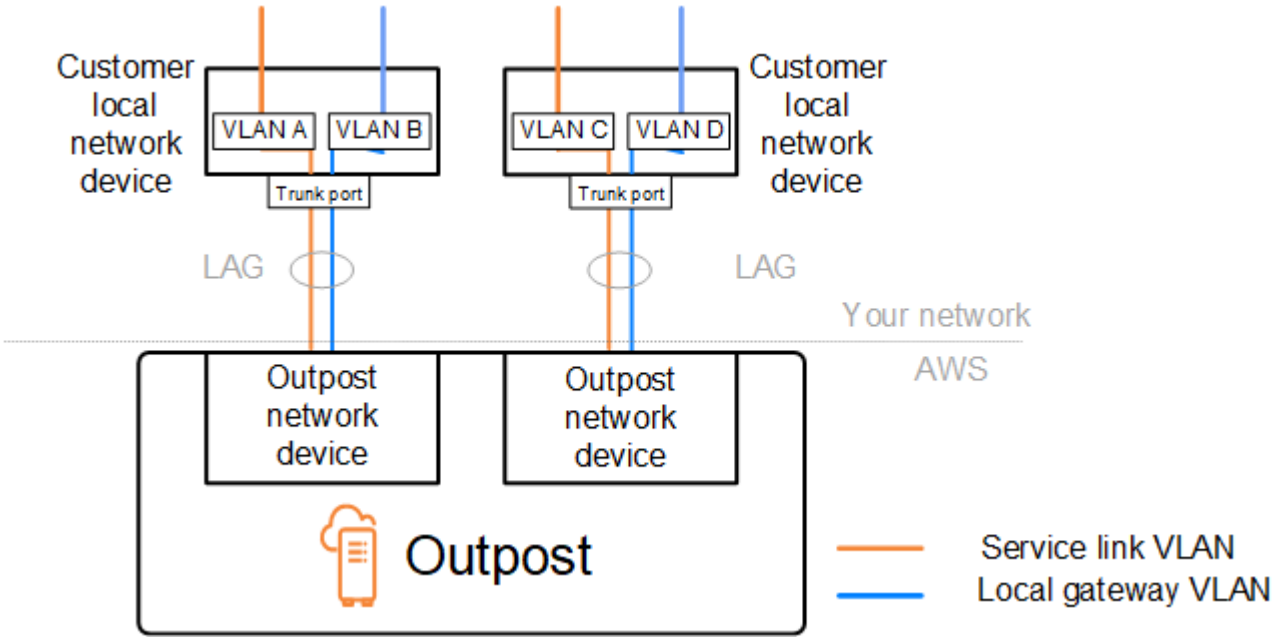
Si utiliza un firewall para limitar la conectividad desde la VLAN de enlace de servicio, puede bloquear todas las conexiones entrantes. Debe permitir que las conexiones salientes regresen al puesto de avanzada desde la AWS región, según se indica en la siguiente tabla. Si el firewall está activo, las conexiones salientes del Outpost que estén permitidas, es decir, las que se iniciaron desde el Outpost, deberían poder volver a entrar.

Protocolo	Puerto de origen	Dirección de origen	Puerto de destino	Dirección de destino
UDP	443	AWS Outposts enlace de servicio /26	443	AWS Outposts Público de la región IPs
TCP	1025-65535	AWS Outposts enlace de servicio /26	443	AWS Outposts Público de la región IPs

> **Note**
>
> Las instancias de un Outpost no pueden usar el enlace de servicio para comunicarse con instancias de otro Outpost. Aproveche el enrutamiento a través de la puerta de enlace local o la interfaz de red local para comunicarse entre Outposts.
> AWS Outposts Los racks también están diseñados con equipos de red y alimentación redundantes, incluidos los componentes de las puertas de enlace locales. Para obtener más información, consulte Resiliencia en. AWS Outposts

Lista de comprobación de solución de problemas de redes en bastidor de Outposts

Utilice esta lista de verificación para solucionar problemas de un enlace de servicio cuyo estado es `DOWN`.



Conectividad con dispositivos de red de Outpost

Compruebe el estado de la interconexión BGP en los dispositivos de la red local del cliente que están conectados a los dispositivos de la red de Outpost. Si el estado del emparejamiento BGP es `DOWN`, siga estos pasos:

1. Haga ping a la dirección IP de emparejamiento remoto en los dispositivos de la red de Outpost desde los dispositivos del cliente. Puede encontrar la dirección IP de intercambio de tráfico en la configuración de BGP de su dispositivo. También puede consultar la Lista de verificación de disponibilidad de red que se le proporcionó en el momento de la instalación.
2. Si el ping no se realiza correctamente, compruebe la conexión física y asegúrese de que el estado de la conectividad sea `UP`.
   a. Confirme el estado LACP de los dispositivos de la red local del cliente.
   b. Compruebe el estado de la interfaz del dispositivo. Si el estado es `UP`, vaya al paso 3.
   c. Compruebe los dispositivos de la red local del cliente y confirme que el módulo óptico funciona.

   d. Sustituya las fibras defectuosas y asegúrese de que las luces (Tx/Rx) estén dentro de un rango aceptable.

3. Si el ping se realiza correctamente, compruebe los dispositivos de la red local del cliente y asegúrese de que las siguientes configuraciones de BGP sean correctas.
   a. Confirme que el número de sistema autónomo local (ASN del cliente) esté configurado correctamente.
   b. Confirme que el número de sistema autónomo remoto (ASN de Outpost) esté configurado correctamente.
   c. Confirme que la IP de la interfaz y las direcciones IP de emparejamiento remoto están configuradas correctamente.
   d. Confirme que las rutas anunciadas y recibidas son correctas.
4. Si su sesión de BGP oscila entre los estados activo y de conexión, verifique que el puerto TCP 179 y otros puertos efímeros relevantes no estén bloqueados en los dispositivos de la red local del cliente.
5. Si necesita seguir solucionando problemas, compruebe los siguientes elementos en los dispositivos de la red local del cliente:
   a. Registros de depuración de BGP y TCP
   b. Registros de BGP
   c. Captura de paquetes
6. Si el problema persiste, realice capturas de MTR, traceroute o paquetes desde el enrutador conectado a Outpost a las direcciones IP homólogas del dispositivo de red de Outpost. Comparta los resultados de las pruebas con AWS Support, mediante su plan de soporte empresarial.

Si el estado de interconexión BGP se encuentra `UP` entre los dispositivos de la red local del cliente y los dispositivos de la red de Outpost, pero el enlace de servicio sigue `DOWN`, puede seguir solucionando el problema comprobando los siguientes dispositivos en los dispositivos de la red local del cliente. Utilice una de las siguientes listas de comprobación en función de cómo se aprovisione la conectividad del enlace de servicio.

- Enrutadores perimetrales conectados a AWS Direct Connect : interfaz virtual pública que se utiliza para la conectividad por enlace de servicio. Para obtener más información, consulte AWS Direct Connect interfaz virtual pública: conectividad con la AWS región.

- Enrutadores perimetrales conectados con AWS Direct Connect : interfaz virtual privada que se utiliza para la conectividad de enlace de servicio. Para obtener más información, consulte AWS Direct Connect interfaz virtual privada: conectividad con la AWS región.
- Enrutadores perimetrales conectados a proveedores de servicios de Internet (ISPs): se utiliza Internet pública para la conectividad por enlace de servicio. Para obtener más información, consulte Conectividad de Internet pública del ISP a la región de AWS.

AWS Direct Connect interfaz virtual pública: conectividad con la AWS región

Utilice la siguiente lista de verificación para solucionar los problemas de los enrutadores periféricos a los que se conecta AWS Direct Connect cuando se utiliza una interfaz virtual pública para la conectividad de enlace de servicio.

1. Confirme que los dispositivos que se conectan directamente a la red de Outpost reciben los rangos de direcciones IP del enlace de servicio mediante BGP.
   a. Confirme las rutas que se reciben a través de BGP desde su dispositivo.
   b. Consulte la tabla de enrutamiento de la instancia de enrutamiento y reenvío virtual (VRF) del enlace de servicio. Debería mostrar que está utilizando el rango de direcciones IP.
2. Para garantizar la conectividad regional, consulte la tabla de enrutamiento para ver la VRF del enlace de servicio. Debe incluir los rangos de direcciones IP AWS públicas o la ruta predeterminada.
3. Si no recibe los rangos de direcciones IP AWS públicas en el enlace de servicio VRF, compruebe lo siguiente.
   a. Compruebe el estado del AWS Direct Connect enlace desde el router perimetral o el AWS Management Console.
   b. Si el enlace físico es `UP`, compruebe el estado del emparejamiento de BGP desde el enrutador de periferia.
   c. Si el estado de emparejamiento BGP es`DOWN`, haga ping a la dirección AWS IP del mismo nivel y compruebe la configuración del BGP en el router perimetral. Para obtener más información, consulte Solución de problemas AWS Direct Connect en la Guía del AWS Direct Connect usuario y El estado del BGP de mi interfaz virtual es inactivo en la consola. AWS ¿Qué debo hacer?

d. Si se ha establecido el BGP y no ve la ruta predeterminada o los rangos de direcciones IP AWS públicas en el VRF, póngase en contacto con Support AWS mediante su plan de soporte empresarial.

4. Si tiene un firewall en las instalaciones, compruebe los siguientes elementos.

   a. Confirme que los puertos necesarios para la conectividad del enlace de servicio estén permitidos en los firewalls de la red. Utilice traceroute en el puerto 443 o cualquier otra herramienta de solución de problemas de red para confirmar la conectividad a través de los firewalls y los dispositivos de red. Es necesario configurar los siguientes puertos en las políticas de firewall para la conectividad del enlace de servicio.

      - Protocolo TCP: puerto de origen: TCP 1025-65535, puerto de destino: 443.
      - Protocolo UDP: puerto de origen: TCP 1025-65535, puerto de destino: 443.

   b. Si el firewall tiene estado activo, asegúrese de que las reglas de salida permitan el intervalo de direcciones IP del enlace de servicio del Outpost con los AWS rangos de direcciones IP públicas. Para obtener más información, consulte AWS Outposts conectividad con las AWS regiones.

   c. Si el firewall no está en estado activo, asegúrese de permitir también el flujo entrante (desde los rangos de direcciones IP AWS públicas hasta el rango de direcciones IP del enlace de servicio).

   d. Si ha configurado un enrutador virtual en los firewalls, asegúrese de que el enrutamiento adecuado esté configurado para el tráfico entre el Outpost y la región de AWS .

5. Si ha configurado la NAT en la red en las instalaciones para traducir los rangos de direcciones IP del enlace de servicio de Outpost a sus propias direcciones IP públicas, compruebe los siguientes elementos.

   a. Confirme que el dispositivo NAT no esté sobrecargado y que tenga puertos libres para asignarlos a nuevas sesiones.

   b. Confirme que el dispositivo NAT esté configurado correctamente para realizar la traducción de direcciones.

6. Si el problema persiste, realice capturas MTR, traceroute o paquetes desde el router perimetral a las direcciones IP homólogas. AWS Direct Connect Comparta los resultados de las pruebas con AWS Support, mediante su plan de soporte empresarial.

AWS Direct Connect interfaz virtual privada: conectividad con la AWS región

Utilice la siguiente lista de verificación para solucionar los problemas de los enrutadores periféricos a los que se conecta AWS Direct Connect cuando se utiliza una interfaz virtual privada para la conectividad de enlace de servicio.

1. Si la conectividad entre el rack de Outposts y la AWS región utiliza la función de conectividad AWS Outposts privada, compruebe lo siguiente.
   a. Haga ping a la dirección AWS IP de emparejamiento remoto desde el router perimetral y confirme el estado del emparejamiento BGP.
   b. Asegúrese de que la interconexión de BGP a través de la interfaz virtual AWS Direct Connect privada entre la VPC del punto final de enlace de servicio y el Outpost instalado en sus instalaciones lo sea. UP Para obtener más información, consulte Solución de problemas AWS Direct Connect en la guía del AWS Direct Connect usuario. El estado del BGP de mi interfaz virtual es inactivo en la consola. AWS ¿Qué debo hacer? y ¿Cómo puedo solucionar problemas de conexión del BGP a través de Direct Connect?.
   c. La interfaz virtual AWS Direct Connect privada es una conexión privada al router perimetral en la AWS Direct Connect ubicación elegida y utiliza BGP para intercambiar rutas. El rango de CIDR de su nube privada virtual (VPC) se anuncia a través de esta sesión de BGP en su enrutador de periferia. Del mismo modo, el rango de direcciones IP del enlace de servicio del Outpost se anuncia en la región mediante el BGP desde su enrutador de periferia.
   d. Confirme que la red ACLs asociada al punto final privado del enlace de servicio en su VPC permita el tráfico correspondiente. Para obtener más información, consulte Lista de verificación de disponibilidad de red.
   e. Si tiene un firewall en las instalaciones, asegúrese de que el firewall tenga reglas de salida que permitan los rangos de direcciones IP del enlace de servicio y los puntos de conexión del servicio de Outpost (las direcciones IP de la interfaz de red) ubicados en la VPC o en el CIDR de la VPC. Asegúrese de que los puertos TCP 1025-65535 y UDP 443 no estén bloqueados. Para obtener más información, consulte Introducción a la conectividad AWS Outposts privada.
   f. Si el firewall no está activo, asegúrese de que tenga reglas y políticas que permitan el tráfico entrante al Outpost desde los puntos de conexión del servicio de Outpost en la VPC.
2. Si tiene más de 100 redes en su red local, puede anunciar una ruta predeterminada a través de la sesión de BGP hasta su AWS interfaz virtual privada. Si no quiere anunciar una ruta predeterminada, resuma las rutas de forma que el número de rutas anunciadas sea inferior a 100.

3. Si el problema persiste, realice capturas MTR, traceroute o paquetes desde el router perimetral a las direcciones IP homólogas. AWS Direct Connect Comparta los resultados de las pruebas con AWS Support, mediante su plan de soporte empresarial.

Conectividad de Internet pública del ISP a la región de AWS

Utilice la siguiente lista de verificación para solucionar problemas con los enrutadores de periferia conectados a través de un ISP cuando se utiliza la Internet pública para la conectividad del enlace de servicio.

- Confirme que la conexión a Internet esté activa.
- Confirme que se puede acceder a los servidores públicos desde sus dispositivos periféricos conectados a través de un ISP.

Si no se puede acceder a Internet o a los servidores públicos a través de los enlaces del ISP, complete los siguientes pasos.

1. Compruebe si el estado de emparejamiento de BGP con los enrutadores del ISP está establecido.
   a. Confirme que el BGP no esté fallando.
   b. Confirme que el BGP recibe y anuncia las rutas requeridas por parte del ISP.
2. En el caso de una configuración de ruta estática, compruebe que la ruta predeterminada esté configurada correctamente en el dispositivo perimetral.
3. Confirme si puede conectarse a Internet mediante otra conexión de ISP.
4. Si el problema persiste, realice capturas MTR, traceroute o paquetes en su enrutador de periferia. Comparta los resultados con el equipo de soporte técnico de su ISP para seguir solucionando problemas.

Si se puede acceder a Internet y a los servidores públicos a través de los enlaces del ISP, complete los siguientes pasos.

1. Confirme si alguna de sus EC2 instancias o balanceadores de carga accesibles públicamente en la región de origen de Outpost está accesible desde su dispositivo perimetral. Puede utilizar ping o telnet para confirmar la conectividad y, a continuación, utilizar traceroute para confirmar la ruta de la red.

2. Si lo utilizas VRFs para separar el tráfico de tu red, confirma que el enlace de servicio VRF tenga rutas o políticas que dirijan el tráfico hacia y desde el ISP (Internet) y el VRF. Consulte los siguientes puntos de control.
   a. Enrutadores de periferia que se conectan con el ISP. Compruebe la tabla de enrutamiento de la VRF del ISP del enrutador de periferia para confirmar que existe el rango de direcciones IP del enlace de servicio.
   b. Dispositivos de red local del cliente que se conectan al Outpost. Compruebe las configuraciones VRFs y asegúrese de que el enrutamiento y las políticas necesarias para la conectividad entre el VRF del enlace de servicio y el VRF del ISP estén configurados correctamente. Por lo general, el VRF del ISP envía una ruta predeterminada al VRF del enlace de servicio para el tráfico a Internet.
   c. Si configuró el enrutamiento basado en el origen en los enrutadores conectados a su Outpost, confirme que la configuración sea correcta.
3. Asegúrese de que los firewalls locales estén configurados para permitir la conectividad saliente (puertos TCP 1025-65535 y UDP 443) desde los rangos de direcciones IP del enlace del servicio Outpost hasta los rangos de direcciones IP públicas. AWS Si los firewalls no son del tipo con estado, asegúrese de que la conectividad entrante al Outpost también esté configurada.
4. Asegúrese de que la NAT esté configurada en la red en las instalaciones para convertir los rangos de direcciones IP del enlace de servicio del Outpost en direcciones IP públicas. Además, confirme los siguientes elementos.
   a. El dispositivo NAT no está sobrecargado y tiene puertos libres para asignarlos a nuevas sesiones.
   b. El dispositivo NAT está configurado correctamente para realizar la traducción de direcciones.

Si el problema persiste, realice capturas MTR, traceroute o paquetes.

- Si los resultados muestran que los paquetes se están descartando o están bloqueados en la red en las instalaciones, consulte a su equipo técnico o de red para obtener más información.
- Si los resultados muestran que los paquetes se están descargando o están bloqueados en la red del ISP, póngase en contacto con el equipo de soporte técnico del ISP.
- Si los resultados no muestran ningún problema, recopile los resultados de todas las pruebas (como MTR, telnet, traceroute, capturas de paquetes y registros de BGP) y póngase en contacto con Support mediante su plan de AWS soporte empresarial.

Outposts detrás de dos dispositivos de firewall

Si ha colocado su Outpost detrás de dos firewalls sincronizados de alta disponibilidad o de dos firewalls independientes, es posible que se produzca un enrutamiento asimétrico del enlace de servicio. Esto significa que el tráfico entrante puede pasar por el firewall-1, mientras que el tráfico saliente puede pasar por el firewall-2. Utilice la siguiente lista de verificación para identificar el posible enrutamiento asimétrico del enlace de servicio, especialmente si antes funcionaba correctamente.

- Compruebe si se ha producido algún cambio reciente o un mantenimiento continuo en la configuración de enrutamiento de la red corporativa que pueda haber provocado un enrutamiento asimétrico del enlace de servicio a través de los firewalls.
  - Utilice los gráficos de tráfico de los firewalls para comprobar si se han producido cambios en los patrones de tráfico que coincidan con el inicio del problema del enlace de servicio.
  - Compruebe si se ha producido un fallo parcial en los firewalls o una desconexión entre los dos firewalls que pueda haber provocado que estos dejaran de sincronizar sus tablas de conexiones entre sí.
  - Compruebe si hay enlaces inactivos o cambios recientes en el enrutamiento (cambios en las OSPF/ISIS/EIGRP métricas, cambios en el mapa de rutas de BGP) en su red corporativa que estén relacionados con el inicio del problema de enlace de servicio.
- Si utiliza una conexión pública a Internet para el enlace de servicio a la región de origen, el mantenimiento por parte del proveedor de servicios podría haber provocado un enrutamiento asimétrico del enlace de servicio a través de los firewalls.
  - Compruebe los gráficos de tráfico de los enlaces con su(s) ISP en busca de cambios en los patrones de tráfico que coincidan con el inicio del problema del enlace de servicio.
- Si utiliza la AWS Direct Connect conectividad para el enlace de servicio, es posible que un mantenimiento AWS planificado haya provocado un enrutamiento asimétrico del enlace de servicio.
  - Compruebe si hay notificaciones de mantenimiento planificado en sus AWS Direct Connect servicios.
  - Ten en cuenta que si tienes AWS Direct Connect servicios redundantes, puedes probar de forma proactiva el enrutamiento del enlace del servicio Outposts a través de cada ruta de red probable en condiciones de mantenimiento. Esto le permite probar si una interrupción en uno de sus servicios de AWS Direct Connect podría provocar un enrutamiento asimétrico del enlace de servicio. La resiliencia de la AWS Direct Connect parte de la conectividad de la end-to-end red se puede probar con el kit de herramientas Resiliency with AWS Direct Connect Resiliency. Para

obtener más información, consulte Probar la resiliencia con el kit de herramientas de AWS Direct Connect resiliencia: pruebas de conmutación por error.

Una vez que haya revisado la lista de verificación anterior y haya identificado el enrutamiento asimétrico del enlace de servicio como una posible causa raíz, puede tomar varias medidas adicionales:

- Restaure el enrutamiento simétrico revirtiendo cualquier cambio en la red corporativa o esperando a que finalice el mantenimiento planificado por un proveedor.
- Inicie sesión en uno o ambos firewalls y borre toda la información de estado de todos los flujos desde la línea de comandos (si lo admite el proveedor del firewall).
- Filtre temporalmente los anuncios de BGP a través de uno de los firewalls o cierre las interfaces de un firewall para forzar el enrutamiento simétrico a través del otro firewall.
- Reinicie cada firewall uno por uno para evitar posibles daños en el seguimiento del estado de flujo del tráfico del enlace de servicio en la memoria del firewall.
- Pídale al proveedor del firewall que verifique o relaje el seguimiento del estado de flujo de UDP de las conexiones UDP originadas en el puerto 443 y destinadas al puerto 443.

Puertas de enlace locales para los bastidores de Outposts

La puerta de enlace local es un componente central de la arquitectura de sus bastidores de Outposts. Una puerta de enlace local permite la conectividad entre las subredes de Outpost y la red en las instalaciones. Si la infraestructura en las instalaciones proporciona acceso a Internet, las cargas de trabajo que se ejecutan en los bastidores de Outposts también pueden aprovechar la puerta de enlace local para comunicarse con los servicios regionales o las cargas de trabajo regionales. Esta conectividad se puede lograr mediante una conexión pública (Internet) o mediante AWS Direct Connect. Para obtener más información, consulte AWS Outposts conectividad con las AWS regiones.

Contenido

Conceptos básicos de la puerta de enlace local

AWS crea una puerta de enlace local para cada rack de Outposts como parte del proceso de instalación. Un bastidor de Outposts admite una única puerta de enlace local. La puerta de enlace local es propiedad de la Cuenta de AWS asociada al bastidor de Outposts.

> **Note**
>
> Para entender las limitaciones de ancho de banda de las instancias para el tráfico que pasa por una puerta de enlace local, consulta el ancho de banda de la red de EC2 instancias de Amazon en la Guía del EC2 usuario de Amazon.

Una puerta de enlace local tiene los siguientes componentes:

- Tablas de enrutamiento: solo el propietario de una puerta de enlace local puede crear tablas de enrutamiento de puerta de enlace local. Para obtener más información, consulte the section called “Tablas de enrutamiento”.

- Grupos de CoIP: (opcional) puede usar los rangos de direcciones IP de su propiedad para facilitar la comunicación entre la red en las instalaciones y las instancias de su VPC. Para obtener más información, consulte the section called “Direcciones IP propiedad del cliente”.
- Interfaces virtuales (VIFs): la puerta de enlace local VIFs (interfaz virtual) es un componente de interfaz lógica de los racks de Outposts que configura la conectividad VLAN, IP y BGP entre un dispositivo de red de Outposts y un dispositivo de red local para la conectividad de la puerta de enlace local. AWS crea un VIF para cada LAG y los agrega a un grupo de VIF. VIFs La tabla de rutas de la puerta de enlace local debe tener una ruta predeterminada hacia las dos VIFs para la conectividad de la red local. Para obtener más información, consulte Conectividad de red local.
- Grupos VIF: AWS agrega VIFs lo que crea a un grupo VIF. Los grupos VIF son agrupaciones lógicas de. VIFs
- Tabla de enrutamiento de la puerta de enlace local y asociaciones de VPC: la tabla de enrutamiento de la puerta de enlace local y las asociaciones de VPC le permiten conectarse a las tablas de enrutamiento de la puerta de enlace local. VPCs Con esta asociación, puedes agregar una ruta dirigida a la puerta de enlace local dentro de tu tabla de rutas de subred de Outposts. Esto permite la comunicación entre los recursos de la subred de Outposts y la red local a través de la puerta de enlace local.
- Dominios de enrutamiento de puerta de enlace local: un dominio de enrutamiento de puerta de enlace local es la asociación de una tabla de enrutamiento de puerta de enlace local y un grupo VIF de puerta de enlace local. Con esta asociación, puede agregar una ruta dirigida a un grupo VIF de puerta de enlace local dentro de la tabla de rutas de la puerta de enlace local. Esto permite la comunicación entre los recursos de la subred de Outposts y la red local a través del grupo VIF seleccionado.

Cuando AWS aprovisiona tu estante de Outposts, creamos algunos componentes y tú eres responsable de crear otros.

AWS responsabilidades

- Entrega el hardware.
- Crea la puerta de enlace local.
- Crea las interfaces virtuales (VIFs) y un grupo VIF.

Sus responsabilidades

- Crear la tabla de enrutamiento de la puerta de enlace local.

- Asociar un VPC a una tabla de enrutamiento de puerta de enlace local.
- Asocie un grupo VIF a la tabla de enrutamiento de la puerta de enlace local para crear un dominio de enrutamiento de la puerta de enlace local.

Enrutamiento de puerta de enlace local

Las instancias de la subred de Outpost pueden usar una de las siguientes opciones para comunicarse con la red en las instalaciones a través de la puerta de enlace local:

- Direcciones IP privadas: la puerta de enlace local usa las direcciones IP privadas de las instancias de la subred de Outpost para facilitar la comunicación con la red en las instalaciones. Esta es la opción predeterminada.
- Direcciones IP propiedad del cliente: la puerta de enlace local realiza la traducción de direcciones de red (NAT) para las direcciones IP propiedad del cliente que usted asigna a las instancias de la subred de Outpost. Esta opción admite rangos de CIDR superpuestos y otras topologías de red.

Para obtener más información, consulte the section called “Tablas de enrutamiento”.

Conectividad a través de una puerta de enlace local

El rol principal de una puerta de enlace local es proporcionar conectividad desde un Outpost a la red local en las instalaciones. También proporciona conectividad a Internet a través de la red en las instalaciones. Para ver ejemplos, consulte the section called “Enrutamiento de VPC directo” y the section called “Direcciones IP propiedad del cliente”.

La puerta de enlace local también puede proporcionar una ruta en el plano de datos de regreso a la AWS región. La ruta del plano de datos de la puerta de enlace local va desde el Outpost, pasa por la puerta de enlace local y llega hasta el segmento de LAN de la puerta de enlace local privada. A continuación, seguiría una ruta privada de regreso a los puntos de conexión del servicio AWS en la región. Tenga en cuenta que la ruta del plano de control siempre utiliza la conectividad del enlace de servicio, independientemente de la ruta del plano de datos que utilice.

Puedes conectar tu infraestructura de Outposts local a la región de forma Servicios de AWS privada a través de. AWS Direct Connect Para obtener más información, consulte Conectividad privada de AWS Outposts.

En la imagen siguiente, se muestra la conectividad a través de la puerta de enlace local:

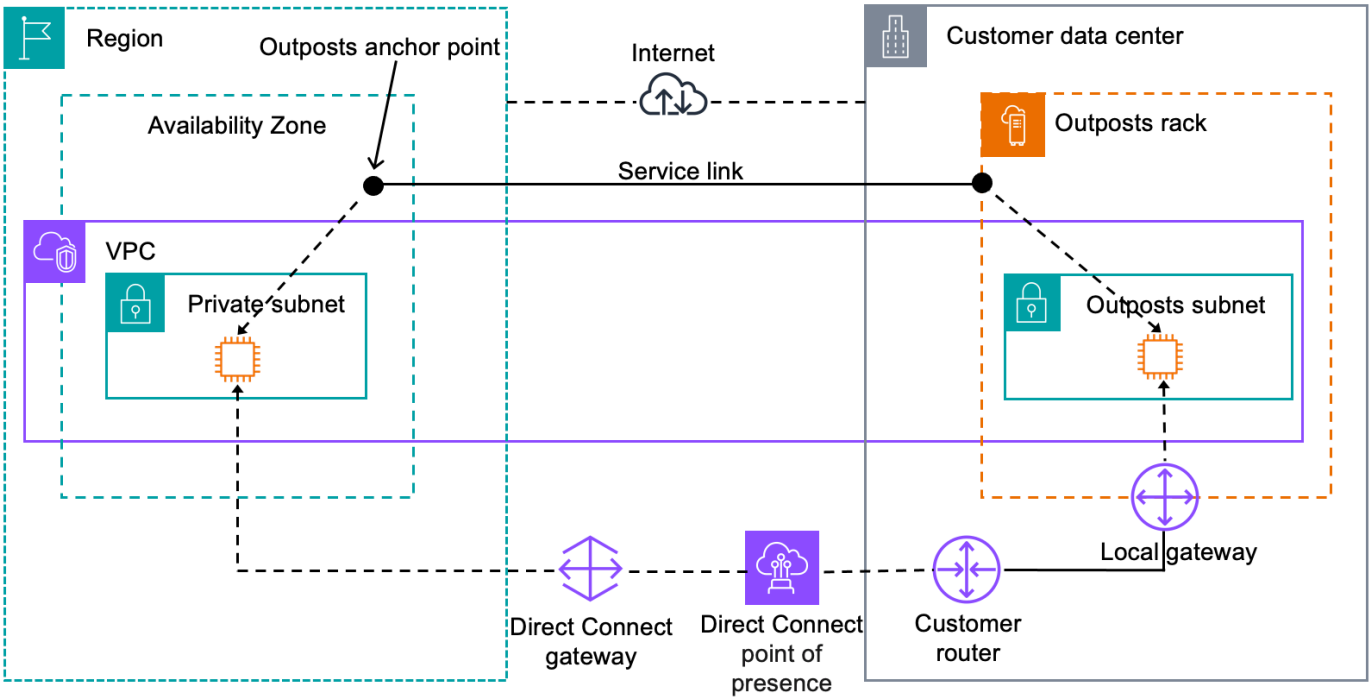


Tabla de enrutamiento de la puerta de enlace local

Como parte de la instalación en rack, AWS crea la puerta de enlace local, configura un grupo VIFs VIF. La puerta de enlace local es propiedad de la AWS cuenta asociada al Outpost. Cree la tabla de enrutamiento de la puerta de enlace local. La tabla de enrutamiento de una puerta de enlace local debe tener una asociación con un grupo VIF y una VPC. Cree y administre la asociación del grupo VIF y la VPC. Solo el propietario de la puerta de enlace local puede modificar la tabla de enrutamiento de la puerta de enlace local.

Las tablas de enrutamiento de subred de Outpost pueden incluir una ruta a los grupos VIF de las puertas de enlace locales para proporcionar conectividad a la red local.

Las tablas de enrutamiento de puerta de enlace local tienen un modo que determina cómo se comunican las instancias de la subred Outposts con la red en las instalaciones. La opción predeterminada es el enrutamiento directo de VPC, que utiliza las direcciones IP privadas de las instancias. La otra opción es usar direcciones de un grupo de direcciones IP (CoIP) que usted proporcione. El enrutamiento directo de VPC y CoIP son opciones que se excluyen mutuamente y que controlan el funcionamiento del enrutamiento. Para determinar cuál es la mejor opción para tu Outpost, consulta Cómo elegir entre los modos de enrutamiento CoIP y VPC directo en el rack de Outposts. AWS

Puedes compartir la tabla de rutas de la puerta de enlace local con otras AWS cuentas o unidades organizativas mediante. AWS Resource Access Manager Para obtener más información, consulte Trabajar con AWS Outposts recursos compartidos.

Contenido

Enrutamiento de VPC directo

El enrutamiento directo de la VPC utiliza la dirección IP privada de las instancias de la VPC para facilitar la comunicación con la red en las instalaciones. Estas direcciones se anuncian en la red en las instalaciones con BGP. La publicidad en BGP es solo para las direcciones IP privadas que pertenecen a las subredes de su bastidor de Outposts. Este tipo de enrutamiento es el modo predeterminado para Outposts. En este modo, la puerta de enlace local no realiza la NAT en las instancias y no es necesario asignar direcciones IP elásticas a las EC2 instancias. Tiene la opción de usar su propio espacio de direcciones en lugar del modo de enrutamiento de VPC directo. Para obtener más información, consulte Direcciones IP propiedad del cliente.

El modo de enrutamiento directo de VPC no admite rangos de CIDR superpuestos.

El enrutamiento directo de VPC solo se admite en las interfaces de red de la instancia. Con las interfaces de red que se AWS crean en su nombre (conocidas como interfaces de red administradas por el solicitante), no se puede acceder a sus direcciones IP privadas desde la red local. Por ejemplo, no se puede acceder directamente a los puntos de enlace de VPC desde la red en las instalaciones.

Los siguientes ejemplos ilustran el enrutamiento de VPC directo.

Ejemplos

Ejemplo: conectividad a Internet a través de la VPC

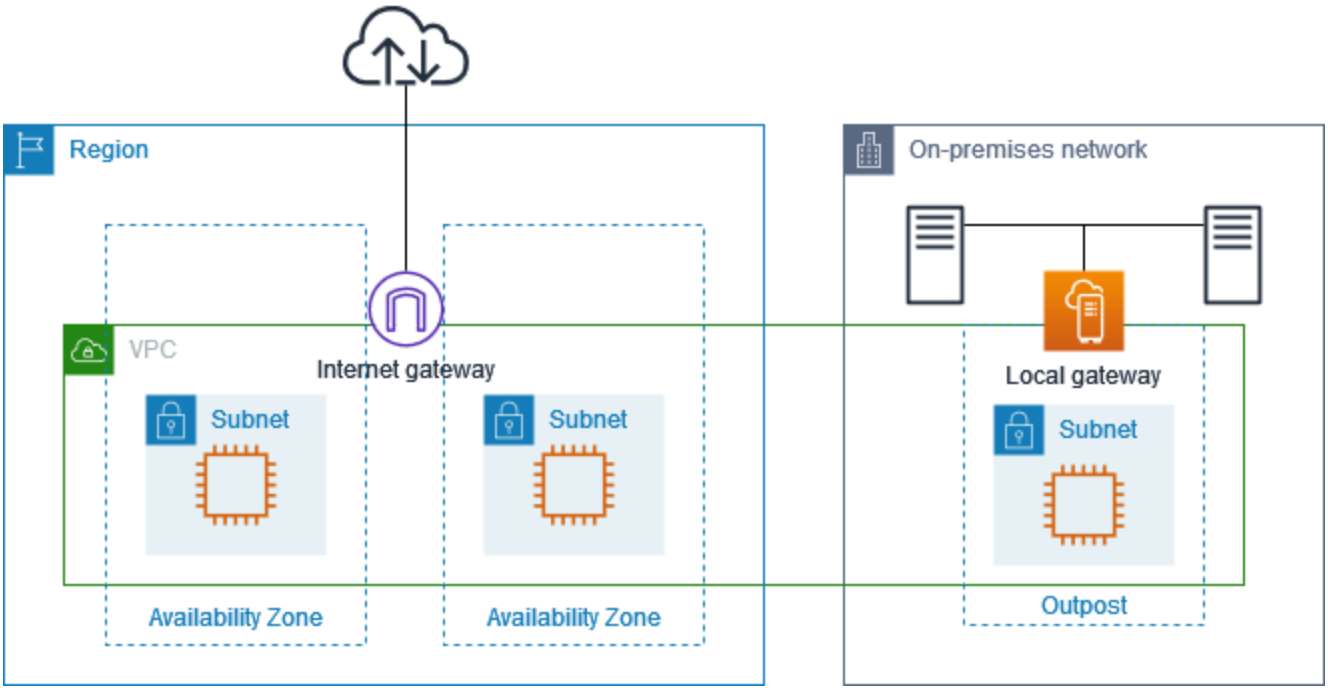
Las instancias de una subred de Outpost pueden acceder a Internet a través de la puerta de enlace de Internet conectada a la VPC.

Considere la siguiente configuración:

- La VPC principal abarca dos zonas de disponibilidad y tiene una subred en cada zona de disponibilidad.
- El Outpost tiene una subred.
- Cada subred tiene una instancia. EC2
- La puerta de enlace local utiliza anuncios de BGP para anunciar las direcciones IP privadas de la subred Outpost en la red en las instalaciones.

> **Note**
>
> La publicidad de BGP solo se admite en las subredes de un Outpost que tengan una ruta con la puerta de enlace local como destino. Las demás subredes no se anuncian a través de BGP.

En el siguiente diagrama, el tráfico de la instancia de la subred Outpost puede usar la puerta de enlace de Internet para que la VPC acceda a Internet.



Para lograr la conectividad a Internet a través de la región principal, la tabla de enrutamiento de la subred Outpost debe tener las siguientes rutas.

Destino	Objetivo	Comentarios
VPC CIDR	Local	Proporciona conectividad entre las subredes de la VPC.
0.0.0.0	*internet-gateway-id*	Envía el tráfico que tenga como destino la puerta de enlace de Internet.
on-premises network CIDR	*local-gateway-id*	Envía el tráfico destinado a la red en las instalaciones a la puerta de enlace local privada.

Ejemplo: conectividad a Internet a través de la red en las instalaciones

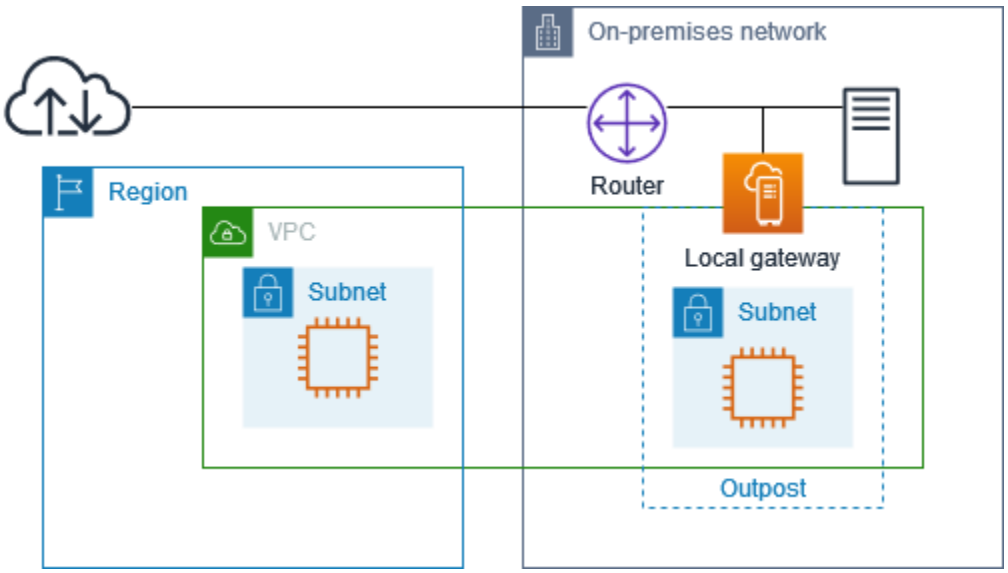
Las instancias de una subred de Outpost pueden acceder a Internet a través de la red en las instalaciones. Las instancias de la subred Outpost no necesitan una dirección IP pública o una dirección IP elástica.

Considere la siguiente configuración:

- La subred Outpost tiene una instancia. EC2
- El router de la red en las instalaciones realiza la traducción de direcciones de red (NAT).
- La puerta de enlace local utiliza anuncios de BGP para anunciar las direcciones IP privadas de la subred Outpost en la red en las instalaciones.

> **Note**
>
> La publicidad de BGP solo se admite en las subredes de un Outpost que tengan una ruta con la puerta de enlace local como destino. Las demás subredes no se anuncian a través de BGP.

En el siguiente diagrama, el tráfico de la instancia de la subred Outpost puede utilizar la puerta de enlace local para acceder a Internet o a la red en las instalaciones. El tráfico de la red en las instalaciones utiliza la puerta de enlace local para acceder a la instancia en la subred Outpost.



Para lograr la conectividad a Internet a través de la red en las instalaciones, la tabla de enrutamiento para la subred Outpost debe tener las siguientes rutas.

Destino	Objetivo	Comentarios
VPC CIDR	Local	Proporciona conectividad entre las subredes de la VPC.
0.0.0.0/0	*local-gateway-id*	Envía el tráfico que tenga como destino la puerta de enlace local.

Acceso de salida a Internet

El tráfico iniciado desde la instancia de la subred Outpost con un destino de internet utiliza la ruta 0.0.0.0/0 para enrutar el tráfico a la puerta de enlace local. La puerta de enlace local envía el tráfico al router. El router utiliza NAT para traducir la dirección IP privada a una dirección IP pública del enrutador y, a continuación, envía el tráfico al destino.

Acceso saliente a la red en las instalaciones

El tráfico iniciado desde la instancia de la subred Outpost con un destino de la red en las instalaciones utiliza la ruta 0.0.0.0/0 para enrutar el tráfico a la puerta de enlace local. La puerta de enlace local envía el tráfico al destino en la red en las instalaciones.

Acceso entrante desde la red en las instalaciones

El tráfico de la red en las instalaciones con un destino de la instancia en la subred Outpost utiliza la dirección IP privada de la instancia. Cuando el tráfico llega a la puerta de enlace local, la puerta de enlace local envía el tráfico al destino de la VPC.

Direcciones IP propiedad del cliente

Por defecto, la puerta de enlace local utiliza las direcciones IP privadas de las instancias de su VPC para facilitar la comunicación con su red en las instalaciones. Sin embargo, puede proporcionar un rango de direcciones, conocido como grupo de direcciones IP propiedad del cliente (CoIP), que admita rangos de CIDR superpuestos y otras topologías de red.

Si elige CoIP, debe crear un conjunto de direcciones, asignarlo a la tabla de enrutamiento de la puerta de enlace local y volver a anunciar estas direcciones a su red de clientes mediante BGP. Todas las direcciones IP propiedad del cliente asociadas a la tabla de enrutamiento de la puerta de enlace local se muestran en la tabla de enrutamiento como rutas propagadas.

Las direcciones IP propiedad del cliente proporcionan conectividad local o externa a los recursos de su red en las instalaciones. Puedes asignar estas direcciones IP a los recursos de tu Outpost, como las EC2 instancias, asignando una nueva dirección IP elástica del grupo de IP propiedad del cliente y, a continuación, asignándola a tu recurso. Para obtener más información, consulte Grupos de CoIP.

> **Note**
>
> En el caso de un conjunto de direcciones IP propiedad del cliente, debe poder enrutar la dirección en su red.

Al asignar una dirección IP elástica del conjunto de direcciones IP propiedad del cliente, usted sigue siendo el propietario de las direcciones IP del grupo de direcciones IP propiedad del cliente. Usted es responsable de anunciarlas según sea necesario en sus redes internas o WAN.

Si lo desea, puede compartir su grupo propiedad del cliente con varios Cuentas de AWS miembros de su organización mediante. AWS Resource Access Manager Después de compartir el grupo, los participantes pueden asignar una dirección IP elástica del grupo de direcciones IP propiedad del cliente y, a continuación, asignarla a una EC2 instancia en Outpost. Para obtener más información, consulte Recursos de compartidos.

Ejemplos

- Ejemplo: conectividad a Internet a través de la VPC

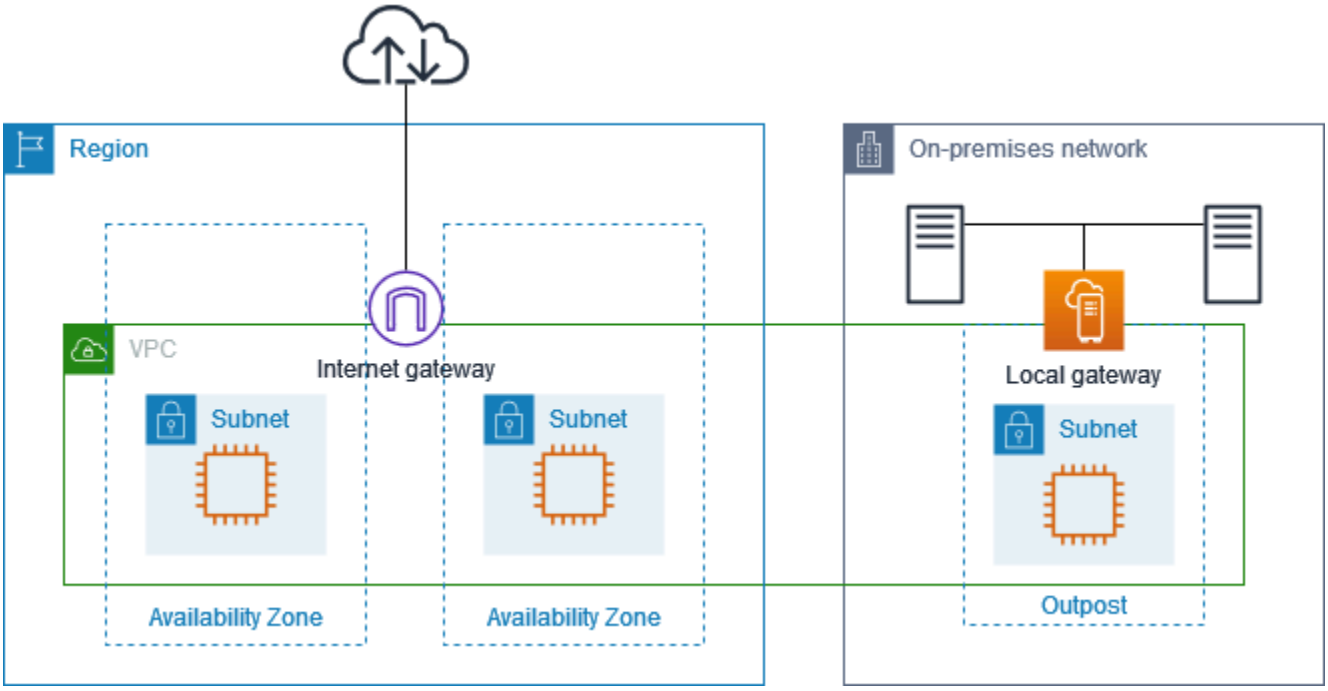
- Ejemplo: conectividad a Internet a través de la red en las instalaciones

Ejemplo: conectividad a Internet a través de la VPC

Las instancias de una subred de Outpost pueden acceder a Internet a través de la puerta de enlace de Internet conectada a la VPC.

Considere la siguiente configuración:

- La VPC principal abarca dos zonas de disponibilidad y tiene una subred en cada zona de disponibilidad.
- El Outpost tiene una subred.
- Cada subred tiene una EC2 instancia.
- Hay un conjunto de direcciones IP propiedad del cliente.
- La instancia de la subred Outpost tiene una dirección IP elástica del conjunto de direcciones IP propiedad del cliente.
- La puerta de enlace local utiliza anuncios de BGP para anunciar el conjunto de direcciones IP propiedad del cliente en la red en las instalaciones.



Para lograr la conectividad a Internet a través de la región, la tabla de enrutamiento de la subred Outpost debe tener las siguientes rutas.

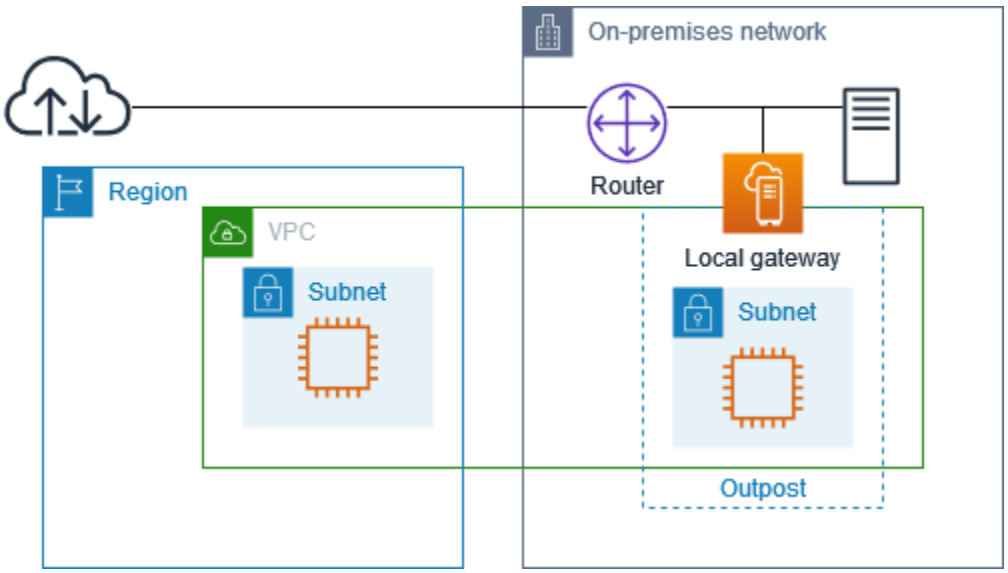
Destino	Objetivo	Comentarios
VPC CIDR	Local	Proporciona conectividad entre las subredes de la VPC.
0.0.0.0	*internet-gateway-id*	Envía el tráfico que tenga como destino la puerta de enlace de Internet pública.
On-premises network CIDR	*local-gateway-id*	Envía el tráfico destinado a la red en las instalaciones a la puerta de enlace local privada.

Ejemplo: conectividad a Internet a través de la red en las instalaciones

Las instancias de una subred de Outpost pueden acceder a Internet a través de la red en las instalaciones.

Considere la siguiente configuración:

- La subred Outpost tiene una instancia. EC2
- Hay un conjunto de direcciones IP propiedad del cliente.
- La puerta de enlace local utiliza anuncios de BGP para anunciar el conjunto de direcciones IP propiedad del cliente en la red en las instalaciones.
- Una asociación de direcciones IP elásticas que asigna de 10.0.3.112 a 10.1.0.2.
- El router de la red en las instalaciones del cliente realiza la NAT.



Para lograr la conectividad a Internet a través de la puerta de enlace local, la tabla de enrutamiento de la subred Outpost debe tener las siguientes rutas.

Destino	Objetivo	Comentarios
VPC CIDR	Local	Proporciona conectividad entre las subredes de la VPC.
0.0.0.0/0	*local-gateway-id*	Envía el tráfico que tenga como destino la puerta de enlace local.

Acceso de salida a Internet

El tráfico iniciado desde la EC2 instancia de la subred Outpost con un destino de Internet utiliza la ruta 0.0.0.0/0 para enrutar el tráfico a la puerta de enlace local. La puerta de enlace local asigna la dirección IP privada de la instancia a la dirección IP propiedad del cliente y, a continuación, envía el tráfico al router. El router utiliza NAT para traducir la dirección IP de un cliente a una dirección IP pública del enrutador y, a continuación, envía el tráfico al destino.

Acceso saliente a la red en las instalaciones

El tráfico iniciado desde la EC2 instancia de la subred Outpost con un destino de la red local utiliza la ruta 0.0.0.0/0 para enrutar el tráfico a la puerta de enlace local. La puerta de enlace local traduce la dirección IP de la EC2 instancia a la dirección IP propiedad del cliente (dirección IP elástica) y, a continuación, envía el tráfico al destino.

Acceso entrante desde la red en las instalaciones

El tráfico de la red en las instalaciones con un destino de la instancia en la subred Outpost utiliza la dirección IP privada (dirección IP elástica) de la instancia. Cuando el tráfico llega a la puerta de enlace local, esta asigna la dirección IP propiedad del cliente (dirección IP elástica) a la dirección IP de la instancia y, a continuación, envía el tráfico al destino en la VPC. Además, la tabla de enrutamiento de la puerta de enlace local evalúa cualquier ruta que se dirija a las interfaces de red elásticas. Si la dirección de destino coincide con el CIDR de destino de alguna ruta estática, el tráfico se envía a esa interfaz de red elástica. Cuando el tráfico sigue una ruta estática hacia una interfaz de red elástica, la dirección de destino se conserva y no se traduce a la dirección IP privada de la interfaz de red.

Tablas de enrutamiento personalizadas

Puede crear una tabla de enrutamiento personalizada para su puerta de enlace local. La tabla de enrutamiento de una puerta de enlace local debe tener una asociación con un grupo VIF y una VPC. Para obtener step-by-step instrucciones, consulte Configurar la conectividad de la puerta de enlace local.

Rutas de tabla de enrutamiento de puerta de enlace local

Puede crear tablas de enrutamiento de puertas de enlace locales y rutas entrantes a las interfaces de red de su Outpost. También puede modificar la ruta de entrada de una puerta de enlace local existente para cambiar la interfaz de red de destino.

Una ruta está en estado activo solo cuando su interfaz de red de destino está conectada a una instancia en ejecución. Si la instancia está detenida o la interfaz está desconectada, la ruta pasa del estado activo al estado de agujero negro.

Contenido

Requisitos y limitaciones

Tenga en cuenta los siguientes requisitos y limitaciones:

- La interfaz de red de destino debe pertenecer a una subred de su Outpost y debe estar conectada a una instancia de ese Outpost. Una ruta de puerta de enlace local no puede dirigirse a una EC2 instancia de Amazon en un Outpost diferente o en la instancia principal Región de AWS.
- La subred debe pertenecer a una VPC asociada a la tabla de enrutamiento de la puerta de enlace local.
- No debe superar más de 100 rutas de interfaz de red en la misma tabla de enrutamiento.
- AWS prioriza la ruta más específica y, si las rutas coinciden, priorizamos las rutas estáticas sobre las rutas propagadas.
- No se admiten los puntos de conexión de VPC.
- La publicidad de BGP solo se admite en las subredes de un Outpost que tengan una ruta con la tabla de enrutamiento que tiene como objetico la puerta de enlace local. Si las subredes no tienen una ruta en la tabla de enrutamiento que se dirija a la puerta de enlace local, esas subredes no se anuncian con BGP.
- Solo las interfaces de red que están conectadas a las instancias de Outpost pueden comunicarse a través de la puerta de enlace local de ese Outpost. Las interfaces de red que pertenecen a la subred del Outpost pero están conectadas a una instancia en la región no pueden comunicarse a través de la puerta de enlace local para ese Outpost.
- No se puede acceder a las interfaces administradas por el solicitante, como las creadas para los puntos de conexión de VPC, desde la red en las instalaciones a través de la puerta de enlace local. Solo se puede acceder a ellas desde instancias que se encuentren en la subred del Outpost.

Se aplican las siguientes consideraciones de NAT.

- La puerta de enlace local no realiza la NAT en el tráfico que coincide con una ruta de interfaz de red. En cambio, se conserva la dirección IP de destino.
- Deshabilite la comprobación de origen/destino de la interfaz de red de destino. Para obtener más información, consulte Conceptos de interfaz de red en la Guía del EC2 usuario de Amazon.
- Configure el sistema operativo para permitir que el tráfico del CIDR de destino se acepte en la interfaz de red.

Cree la tabla de enrutamiento de la puerta de enlace local personalizada

Puede crear una tabla de enrutamiento personalizada para su puerta de enlace local mediante la consola de AWS Outposts .

Para crear una tabla de enrutamiento de puerta de enlace local personalizada mediante la consola

1. Abra la AWS Outposts consola en https://console.aws.amazon.com/outposts/.
2. Para cambiarla Región de AWS, usa el selector de regiones en la esquina superior derecha de la página.
3. En el panel de navegación, elija Tabla de enrutamiento de puerta de enlace local.
4. Elija Crear tabla de enrutamiento de puerta de enlace local.
5. (Opcional) En Nombre, escriba el nombre de la tabla de enrutamiento de la puerta de enlace.
6. En Puerta de enlace local, elija la puerta de enlace local.
7. (Opcional) Elija el Grupo VIF asociado y elija su Grupo VIF.

   Edite la tabla de rutas de la puerta de enlace local para agregar una ruta estática que tenga al grupo VIF como destino.
8. En Modo, elija un modo de comunicación con la red en las instalaciones.

   - Elija el Enrutamiento directo de VPC para usar la dirección IP privada de una instancia.
   - Elija CoIP para usar la dirección IP propiedad del cliente.
     - (Opcional) Agregue o elimine grupos de CoIP y bloques de CIDR adicionales

       [Agregar un grupo CoIP] Elija Agregar nuevo grupo y haga lo siguiente:

       - En Nombre, escriba un nombre para la política de CoIP.
       - En CIDR, introduzca un bloque CIDR de direcciones IP propiedad del cliente.
     - [Agregar bloques CIDR] Seleccione Agregar nuevo CIDR e introduzca un rango de direcciones IP propiedad del cliente.
     - [Eliminar un grupo de CoIP o un bloque de CIDR adicional] Seleccione Eliminar a la derecha de un bloque de CIDR o debajo del grupo de CoIP.

       Puede especificar hasta 10 grupos de CoIP y 100 bloques de CIDR.
9. (Opcional) Añada o elimine una etiqueta.

   [Agregar una etiqueta] Elija Agregar nueva etiqueta y haga lo siguiente:

   - En Clave, escriba el nombre de la clave.
   - En Valor, escriba el valor de la clave.

[Eliminar una etiqueta] Elija Eliminar a la derecha de la clave y el valor de la etiqueta.

10. Elija Crear tabla de enrutamiento de puerta de enlace local.

Cambiar los modos de la tabla de enrutamiento de puerta de enlace local o eliminar una tabla de enrutamiento de puerta de enlace local

Debe eliminar y volver a crear la tabla de enrutamiento de puerta de enlace local para cambiar de modo. Eliminar la tabla de enrutamiento de puerta de enlace local provoca la interrupción del tráfico de red.

Para cambiar de modo o eliminar una tabla de enrutamiento de puerta de enlace local

1. Abra la AWS Outposts consola en. https://console.aws.amazon.com/outposts/
2. Compruebe que se encuentra en la región de Región de AWS correcta.

   Para cambiar la región, utilice el selector de regiones en la esquina superior derecha de la página.
3. En el panel de navegación, elija Tablas de enrutamiento de puerta de enlace de tránsito.
4. Compruebe si la tabla de enrutamiento de la puerta de enlace local está asociada a un grupo de VIF. Si está asociada, debe eliminar la asociación entre la tabla de enrutamiento de la puerta de enlace local y el grupo de VIF.

   a. Elija el ID de la tabla de enrutamiento de la puerta de enlace local.
   b. Elija la pestaña Asociación de grupo de VIF.
   c. Si uno o más grupos de VIF están asociados a la tabla de enrutamiento de la puerta de enlace local, elija Editar asociación de grupo de VIF.
   d. Desactive la casilla de verificación Asociar grupo de VIF.
   e. Seleccione Save changes (Guardar cambios).
5. Elija Crear tabla de enrutamiento de puerta de enlace local.
6. En el cuadro de diálogo de confirmación, escriba **`delete`** y elija Eliminar.
7. (Opcional) Cree una tabla de enrutamiento de puerta de enlace local con un modo nuevo.

   a. En el panel de navegación, elija Tablas de enrutamiento de puerta de enlace de tránsito.
   b. Elija Crear tabla de enrutamiento de puerta de enlace local.

c. Configure la tabla de enrutamiento de puerta de enlace local mediante el nuevo modo. Para obtener más información, consulte Crear una tabla de enrutamiento de puerta de elace local personalizada.

Crear un grupo de CoIP

Puede proveer los rangos de direcciones IP para facilitar la comunicación entre la red en las instalaciones y las instancias de su VPC. Para obtener más información, consulte Direcciones IP propiedad del cliente.

Los grupos de IP propiedad del cliente están disponibles para las tablas de enrutamiento de las puertas de enlace locales en modo CoIP.

Utilice el siguiente procedimiento para crear un grupo de CoIP.

Console

Para crear un grupo de CoIP dedicado utilizando la consola:

1. Abra la AWS Outposts consola en https://console.aws.amazon.com/outposts/.
2. Para cambiarla Región de AWS, usa el selector de regiones en la esquina superior derecha de la página.
3. En el panel de navegación, elija Tablas de enrutamiento de puerta de enlace de tránsito.
4. Elija la tabla de enrutamiento.
5. Seleccione la pestaña Grupos de CoIP en el panel de detalles y, a continuación, elija Crear grupo de CoIP.
6. (Opcional) En Nombre, escriba un nombre para la política de CoIP.
7. Seleccione Agregar nuevo CIDR e introduzca un rango de direcciones IP propiedad del cliente.
8. (Opcional) Para agregar un bloque de CIDR, elija Agregar CIDR nuevo e introduzca un rango de direcciones IP propiedad del cliente.
9. Elija Crear grupo CoIP.

AWS CLI

Para crear un grupo de CoIP mediante el AWS CLI

1. Utilice el create-coip-poolcomando para crear un conjunto de direcciones CoIP para la tabla de rutas de la puerta de enlace local especificada.

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

A continuación, se muestra un ejemplo del resultado.

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

2. Utilice el create-coip-cidrcomando para crear un rango de direcciones CoIP en el grupo de CoIP especificado.

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

A continuación, se muestra un ejemplo del resultado.

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

Tras crear un grupo de CoIP, utilice el siguiente procedimiento para asignar una dirección a la instancia.

Console

Para asignar una dirección CoIP a una instancia utilizando la consola:

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Elastic. IPs
3. Elija Asignar dirección IP elástica.
4. En Grupo de borde de red, seleccione la ubicación desde la que se anuncia la dirección IP.
5. En Grupo de IPv4 direcciones público, elija Grupo de IPv4 direcciones propiedad del cliente.
6. En Grupo de IPv4 direcciones propiedad del cliente, seleccione el grupo que configuró.
7. Elija Asignar.
8. Seleccione la dirección IP elástica que desea asociar y elija Acciones, Asociar dirección IP elástica.
9. Seleccione la instancia en Instancia y, a continuación, elija Asociar.

AWS CLI

Para asignar una dirección CoIP a una instancia mediante el AWS CLI

1. Use el describe-coip-poolscomando para recuperar información sobre los grupos de direcciones propiedad de sus clientes.

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

A continuación, se muestra un ejemplo del resultado.

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

2. Utilice el comando allocate-address para asignar una dirección IP elástica. Utilice el ID de grupo obtenido en el paso anterior.

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

A continuación, se muestra un ejemplo del resultado.

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

3. Utilice el comando associate-address para asociar la dirección IP elástica con la instancia del Outpost. Utilice el ID de asignación que obtuvo en el paso anterior.

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

A continuación, se muestra un ejemplo del resultado.

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

Conectividad de red local para bastidores de Outposts

Necesita los siguientes componentes para conectar su bastidor de Outposts a su red en las instalaciones:

- Conectividad física desde el panel de conexiones de Outpost a los dispositivos de la red local del cliente.
- Protocolo de control de agregación de enlaces (LACP) para establecer dos conexiones de grupos de agregación de enlaces (LAG) a sus dispositivos de red Outpost y a sus dispositivos de red local.
- Conectividad LAN virtual (VLAN) entre el Outpost y los dispositivos de la red local del cliente.
- point-to-pointConectividad de capa 3 para cada VLAN.
- Protocolo de puerta de enlace fronteriza (BGP) para el anuncio de ruta entre el Outpost y el enlace de servicio en las instalaciones.
- BGP para el anuncio de ruta entre el Outpost y su dispositivo de red local en las instalaciones para la conectividad con la puerta de enlace local.

Contenido

Conectividad física

Un bastidor de Outposts tiene dos dispositivos de red físicos que se conectan a la red local.

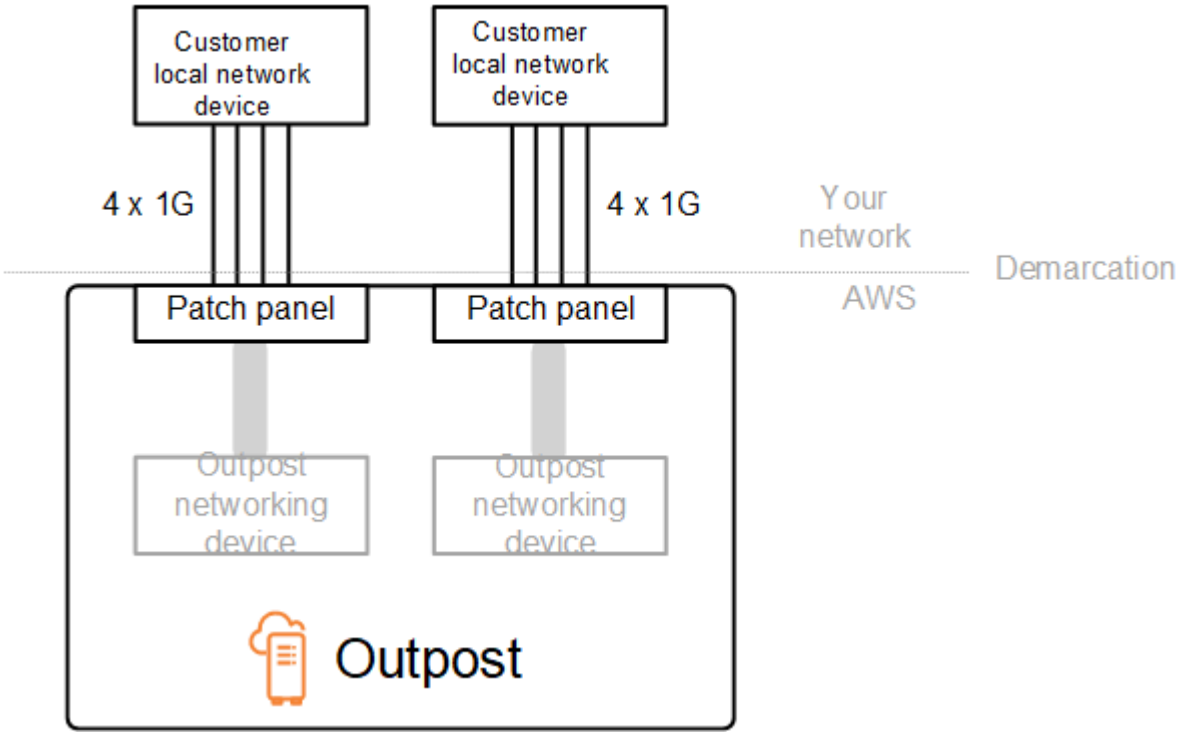
Un Outpost requiere un mínimo de dos enlaces físicos entre estos dispositivos de red Outpost y sus dispositivos de red local. Un Outpost admite las siguientes velocidades y cantidades de enlace ascendente para cada dispositivo de red Outpost.

Velocidad de enlace ascendente	Número de enlaces ascendentes
1 Gbps	1, 2, 4, 6 o 8
10 Gbps	1, 2, 4, 8, 12 o 16
40 Gbps o 100 Gbps	1, 2 o 4

La velocidad y la cantidad del enlace ascendente son simétricas en cada dispositivo de red Outpost. Si utiliza 100 Gbps como velocidad de enlace ascendente, debe configurar el enlace con la corrección de errores de reenvío (FEC). CL91

Los racks Outposts admiten fibra monomodo (SMF) con Lucent Connector (LC), fibra multimodo (MMF) o MMF con LC. OM4 AWS proporciona la óptica compatible con la fibra que se proporciona en la posición del bastidor.

En el siguiente diagrama, la demarcación física es el panel de conexiones de fibra de cada Outpost. Usted proporciona los cables de fibra necesarios para conectar el Outpost al panel de conexiones.



Agregación de enlaces

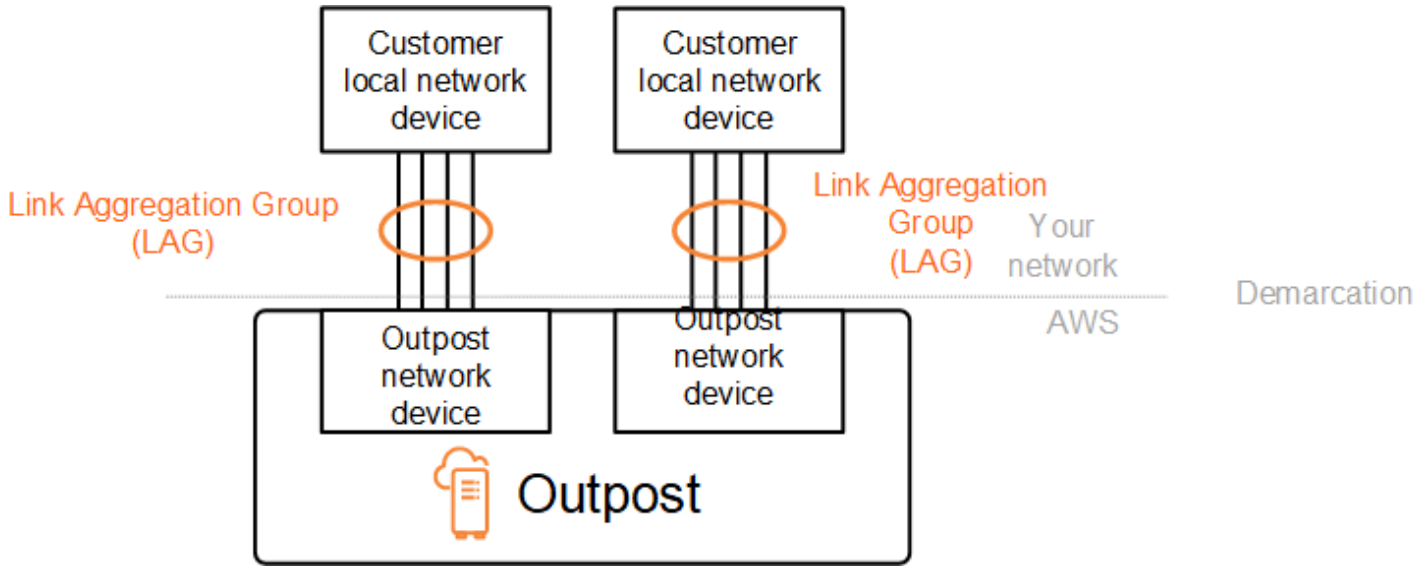
AWS Outposts utiliza el Protocolo de control de agregación de enlaces (LACP) para establecer las conexiones de los grupos de agregación de enlaces (LAG) entre los dispositivos de la red Outpost y los dispositivos de la red local. Los enlaces de cada dispositivo de red Outpost se agregan en un LAG Ethernet para representar una única conexión de red. LAGs Utilizan el LACP con temporizadores rápidos estándar. No se puede configurar LAGs para usar temporizadores lentos.

Para habilitar la instalación de Outpost en su sitio, debe configurar su lado de las conexiones LAG en sus dispositivos de red.

Desde una perspectiva lógica, ignore los paneles de conexiones de Outpost como punto de demarcación y utilice los dispositivos de red de Outpost.

Para las implementaciones que tienen varios racks, un Outpost debe tener cuatro LAGs entre la capa de agregación de los dispositivos de la red Outpost y los dispositivos de la red local.

El siguiente diagrama muestra cuatro conexiones físicas entre cada dispositivo de red Outpost y su dispositivo de red local conectado. Usamos Ethernet LAGs para agregar los enlaces físicos que conectan los dispositivos de la red Outpost y los dispositivos de la red local del cliente.



Virtual LANs

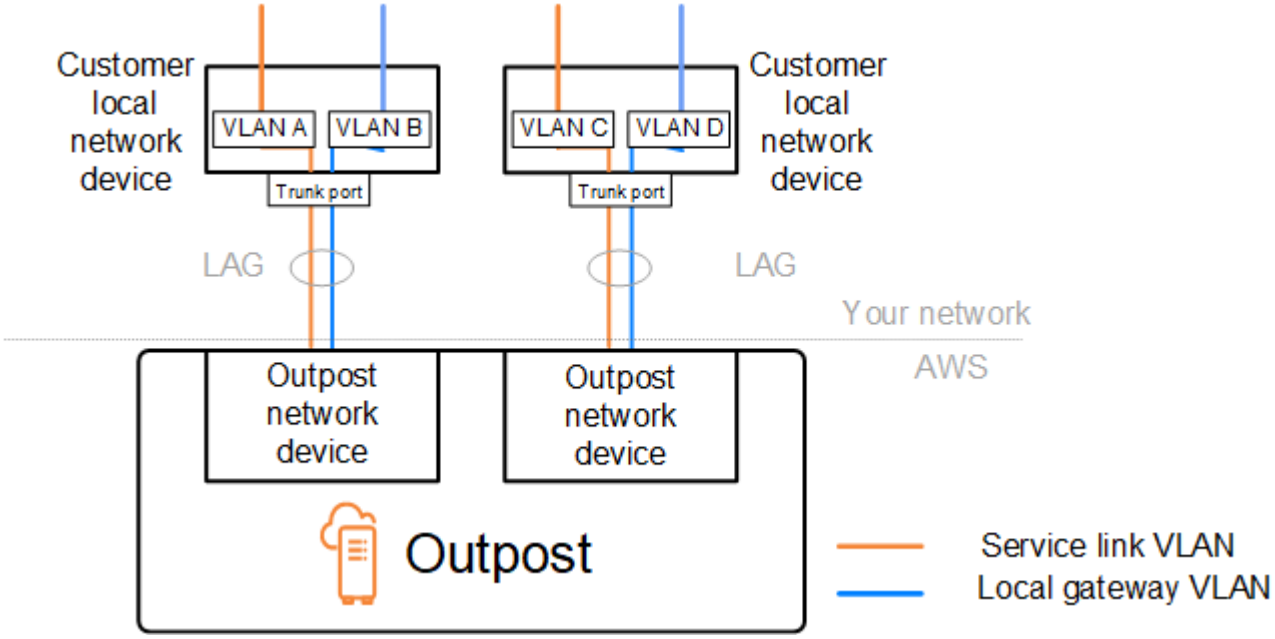
Cada LAG entre un dispositivo de red Outpost y un dispositivo de red local debe configurarse como un enlace troncal Ethernet IEEE 802.1q. Esto permite el uso de varios VLANs para la segregación de la red entre las rutas de datos.

Cada Outpost tiene lo siguiente VLANs para comunicarse con los dispositivos de su red local:

- VLAN de enlace de servicio: permite la comunicación entre su Outpost y los dispositivos de la red local para establecer una ruta de enlace de servicio para la conectividad del enlace de servicio. Para obtener más información, consulte Conectividad de AWS Outposts a las regiones de AWS.
- VLAN de puerta de enlace local: permite la comunicación entre su Outpost y los dispositivos de la red local para establecer una ruta de puerta de enlace local que conecte sus subredes de Outpost y su red de área local. La puerta de enlace local de Outpost usa esta VLAN para proporcionar a sus instancias la conectividad con la red en las instalaciones, lo que puede incluir el acceso a Internet a través de la red. Para obtener más información, consulte Puerta de enlace local.

Puede configurar la VLAN de enlace de servicio y la VLAN de puerta de enlace local solo entre el Outpost y los dispositivos de la red local del cliente.

Un Outpost está diseñado para separar las rutas de datos del enlace de servicio y de la puerta de enlace local en dos redes aisladas. Esto le permite elegir cuáles de sus redes se pueden comunicar con los servicios que se ejecutan en el Outpost. También le permite vincular el servicio a una red aislada de la red de puerta de enlace local mediante una tabla de enrutamiento múltiple en el dispositivo de la red local del cliente, lo que se conoce comúnmente como instancias de enrutamiento y reenvío virtuales (VRF). La línea de demarcación existe en el puerto de los dispositivos de red de Outpost. AWS administra cualquier infraestructura del AWS lado de la conexión y usted administra cualquier infraestructura del lado de la línea.



Para integrar su Outpost con su red local durante la instalación y el funcionamiento continuo, debe asignar lo VLANs utilizado entre los dispositivos de la red Outpost y los dispositivos de la red local del cliente. Debe proporcionar esta información antes de la instalación. AWS Para obtener más información, consulte the section called “Lista de verificación de disponibilidad de red”.

Conectividad de capa de red

Para establecer la conectividad a nivel de red, cada dispositivo de red Outpost se configura con interfaces virtuales (VIFs) que incluyen la dirección IP de cada VLAN. A través de ellas VIFs, los dispositivos de AWS Outposts red pueden configurar la conectividad IP y las sesiones de BGP con su equipo de red local.

Le recomendamos lo siguiente:

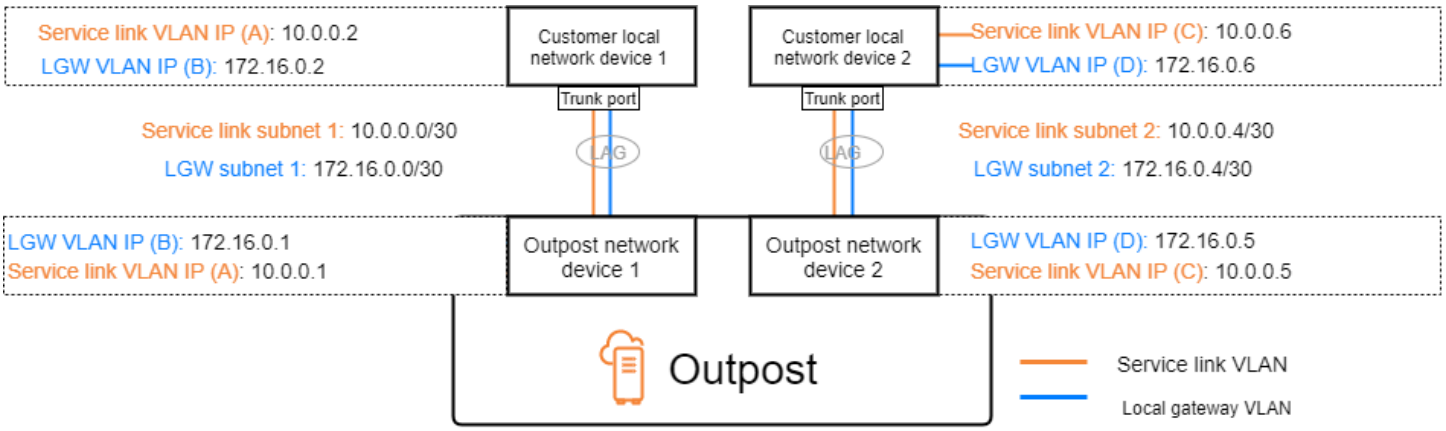
- Utilice una subred dedicada, con un CIDR /30 o /31, para representar esta conectividad lógica. point-to-point
- No cree puentes VLANs entre los dispositivos de la red local.

Para la conectividad de la capa de red, debe establecer dos rutas:

- Ruta de enlace de servicio: para establecer esta ruta, especifique una subred de VLAN con un rango de /30 o /31 y una dirección IP para la VLAN de enlace de servicio en el dispositivo de red de AWS Outposts . Las interfaces virtuales de enlace de servicio (VIFs) se utilizan en esta ruta para establecer la conectividad IP y las sesiones de BGP entre su Outpost y los dispositivos de la red local para la conectividad de enlace de servicio. Para obtener más información, consulte Conectividad de AWS Outposts a las regiones de AWS.
- Ruta de puerta de enlace local: para establecer esta ruta, especifique una subred de VLAN con un rango de /30 o /31 y una dirección IP para la VLAN de puerta de enlace local en el dispositivo de red de AWS Outposts . La puerta de enlace local VIFs se utiliza en esta ruta para establecer la conectividad IP y las sesiones de BGP entre su Outpost y los dispositivos de la red local para la conectividad de los recursos locales.

El siguiente diagrama muestra las conexiones desde cada dispositivo de red Outpost al dispositivo de red local del cliente para la ruta del enlace de servicio y la ruta de la puerta de enlace local. VLANsPara este ejemplo, hay cuatro:

- La VLAN A es la ruta de enlace de servicio que conecta el dispositivo de red Outpost 1 con el dispositivo de red local 1 del cliente.
- La VLAN B para la puerta de enlace local que conecta el dispositivo de red Outpost 1 con el dispositivo de red local 1 del cliente.
- La VLAN C es la ruta de enlace de servicio que conecta el dispositivo de red Outpost 2 con el dispositivo de red local 2 del cliente.
- La VLAN D para la puerta de enlace local que conecta el dispositivo de red Outpost 2 con el dispositivo de red local 2 del cliente.



La siguiente tabla muestra valores de ejemplo para las subredes que conectan el dispositivo de red Outpost 1 con el dispositivo de red local 1 del cliente.

VLAN	Subred	Dispositivo 1 del cliente IP	AWS UNO (1 IP)
A	10.0.0.0/30	10.0.0.2	10.0.0.1
B	172.16.0.0/30	17216.0.2	172216,01

La siguiente tabla muestra valores de ejemplo para las subredes que conectan el dispositivo de red Outpost 2 con el dispositivo de red local 2 del cliente.

VLAN	Subred	Dispositivo 2 del cliente IP	AWS UNA IP DE 2
C	10.0.0.4/30	10.0.0.6	10.0.0.5
D	172.16.0.4/30	172.16.0.6	172.16.0.5

Conectividad de bastidor ACE

> **Note**
>
> Omita esta sección si no necesita un bastidor ACE.

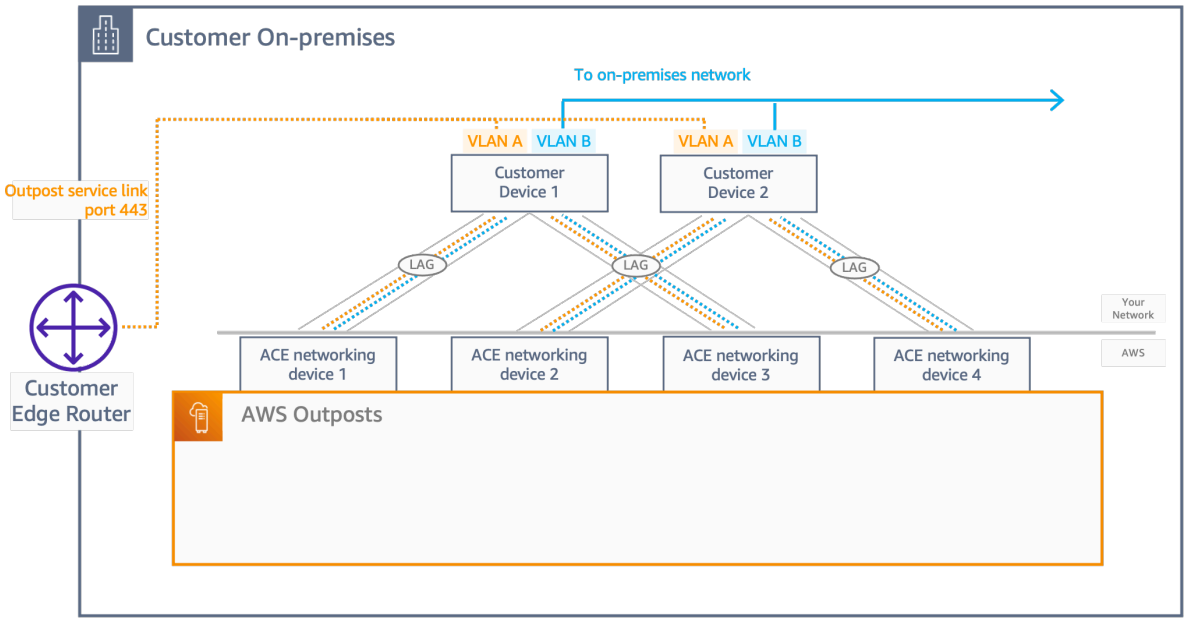
Un bastidor Aggregation, Core, Edge (ACE) actúa como punto de agregación de red para implementaciones de Outpost con varios bastidores. Debe usar un bastidor ACE si tiene cuatro o más bastidores de computación. Si tiene menos de cuatro bastidores de computación pero planea ampliarlos a cuatro o más en el futuro, le recomendamos que instale un bastidor ACE lo antes posible.

Con un bastidor ACE, los dispositivos de red de Outposts ya no se conectan directamente a los dispositivos de red en las instalaciones. En su lugar, se conectan al bastidor ACE, que proporciona conectividad a los bastidores de Outposts. En esta topología, AWS es propietario de la asignación y configuración de la interfaz VLAN entre los dispositivos de red Outposts y los dispositivos de red ACE.

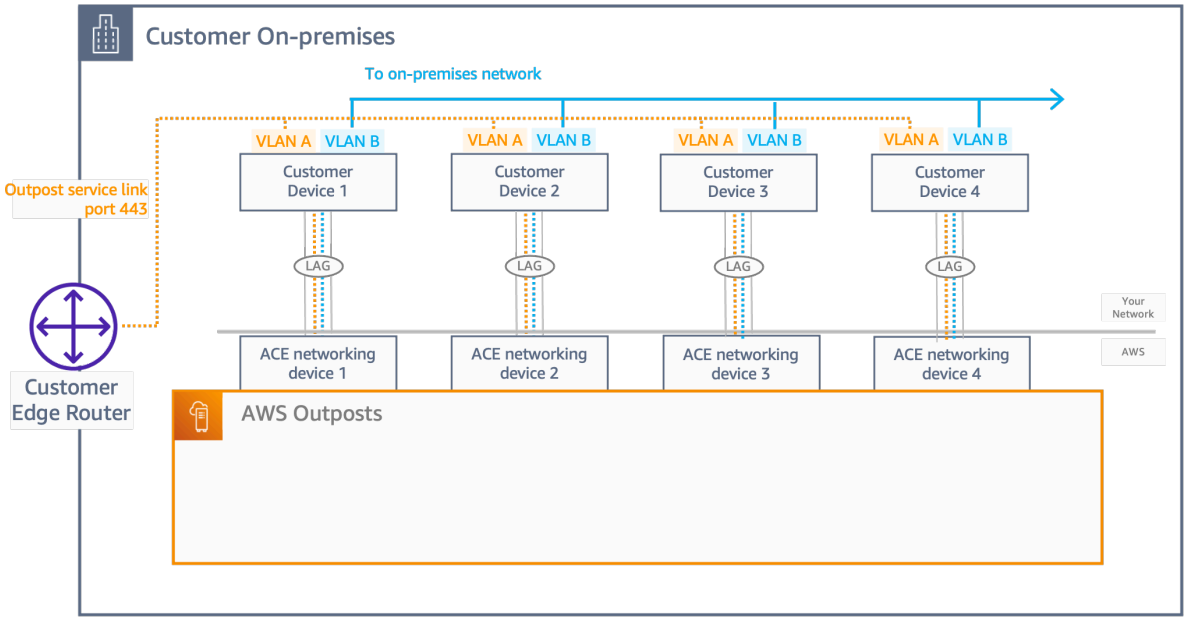
Un bastidor ACE incluye cuatro dispositivos de red que se pueden conectar a dos dispositivos de cliente ascendentes en la red en las instalaciones del cliente o a cuatro dispositivos de cliente ascendentes para obtener la máxima resiliencia.

En las siguientes imágenes se muestran las dos topologías de red.

La siguiente imagen muestra los cuatro dispositivos de red de ACE del bastidor ACE conectados a dos dispositivos de cliente ascendentes:



La siguiente imagen muestra los cuatro dispositivos de red de ACE del bastidor ACE conectados a cuatro dispositivos de cliente ascendentes:



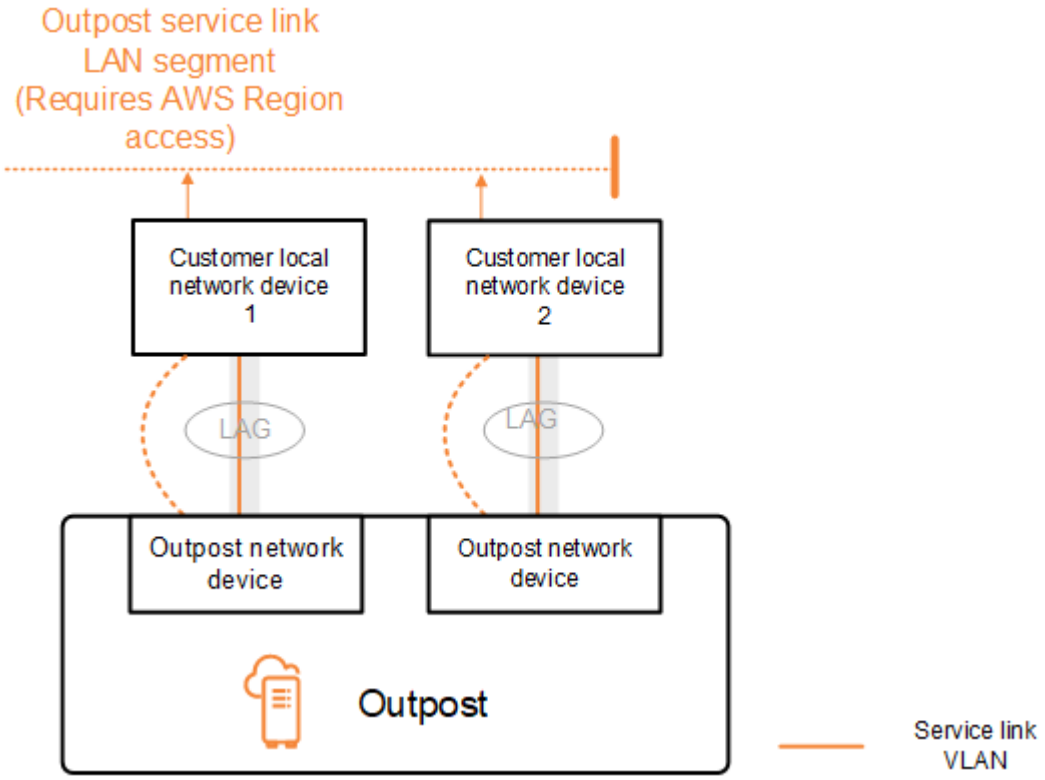
Conectividad BGP de Service Link

El Outpost establece una sesión de interconexión BGP externa entre cada dispositivo de red Outpost y el dispositivo de red local del cliente para la conectividad del enlace de servicio a través de la VLAN del enlace de servicio. La sesión de emparejamiento BGP se establece entre las direcciones IP /30 o /31 proporcionadas para la VLAN. point-to-point Cada sesión de interconexión BGP utiliza un número de sistema autónomo (ASN) privado en el dispositivo de red Outpost y un ASN que usted

elija para los dispositivos de la red local del cliente. Como parte del proceso de instalación, AWS configura los atributos que ha proporcionado.

Considere el escenario en el que tiene un Outpost con dos dispositivos de red Outpost conectados mediante una VLAN de enlace de servicio a dos dispositivos de la red local del cliente. Debe configurar la siguiente infraestructura y los atributos ASN BGP del dispositivo de red local del cliente para cada enlace de servicio:

- El enlace de servicio BGP ASN. 2 bytes (16 bits) o 4 bytes (32 bits). Los valores válidos son 64512-65535 o 4200000000-4294967294.
- La infraestructura CIDR. Debe ser un CIDR de /26 por bastidor.
- El dispositivo de red local del cliente 1 enlaza la dirección IP del servicio de par BGP.
- El dispositivo de red local del cliente 1 enlaza el ASN del servicio de par BGP. Los valores válidos son 1-4294967294.
- El dispositivo de red local del cliente 2 enlaza la dirección IP del servicio de par BGP.
- El dispositivo de red local del cliente 2 enlaza el ASN del servicio de par BGP. Los valores válidos son 1-4294967294. Para obtener más información, consulte RFC4893.



El Outpost establece una sesión de emparejamiento BGP externa a través de la VLAN del enlace de servicio mediante el siguiente proceso:

1. Cada dispositivo de red Outpost utiliza la ASN para establecer una sesión de emparejamiento BGP con su dispositivo de red local conectado.
2. Los dispositivos de red Outpost anuncian el rango CIDR de /26 como dos rangos de CIDR de /27 para detectar fallos de enlace y dispositivo. Como respaldo, cada OND publica su propio prefijo /27 con una longitud AS-Path de 1, además de los prefijos /27 de todos los demás ONDs con una longitud AS-Path de 4.
3. La subred se utiliza para la conectividad entre el puesto de avanzada y la región. AWS

Le recomendamos que configure el equipo de red del cliente para recibir anuncios de BGP de Outposts sin cambiar los atributos de BGP. La red de clientes debería preferir las rutas de Outposts con una longitud de AS-Path de 1 a las rutas con una longitud de AS-Path de 4.

La red del cliente debe anunciar prefijos BGP iguales con los mismos atributos para todas las redes. ONDs El equilibrador de carga de red de Outpost equilibra el tráfico saliente entre todos los enlaces ascendentes de forma predeterminada. Las políticas de enrutamiento se utilizan en el Outpost para desviar el tráfico de un OND si es necesario realizar tareas de mantenimiento. Este cambio de tráfico requiere que todos los clientes tengan los mismos prefijos de BGP. ONDs Si es necesario realizar tareas de mantenimiento en la red del cliente, le recomendamos que utilice AS-Path para desplazar temporalmente la matriz de tráfico desde enlaces ascendentes específicos.

Infraestructura de enlace de servicio, publicidad de subredes y rango de IP

Debe proporcionar un rango de CIDR de /26 durante el proceso de preinstalación de la subred de infraestructura de Service Link. La infraestructura de Outpost utiliza este rango para establecer la conectividad con la región a través del enlace de servicio. La subred del enlace de servicio es la fuente de Outpost, que inicia la conectividad.

Los dispositivos de red Outpost anuncian el rango CIDR de /26 como dos bloques de CIDR de /27 para detectar fallos de enlace y dispositivo.

Debe proporcionar un enlace de servicio BGP ASN y una subred de infraestructura CIDR (/26) para el Outpost. Para cada dispositivo de red Outpost, proporcione la dirección IP de emparejamiento BGP en la VLAN del dispositivo de red local y el ASN BGP del dispositivo de red local.

Si tiene una implementación de varios bastidores, debe tener una subred /26 por bastidor.

Conectividad del BGP de la puerta de enlace local

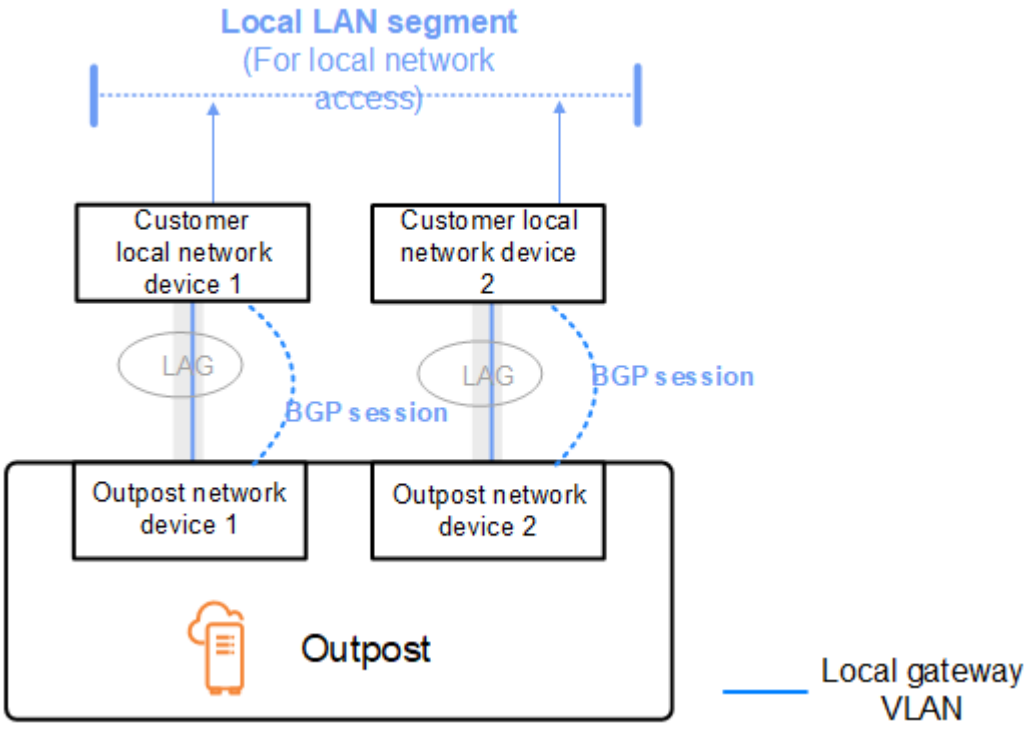
El Outpost utiliza un número de sistema autónomo (ASN) privado que usted asigna para establecer las sesiones de BGP externas. Cada dispositivo de red Outpost tiene un único BGP externo que se conecta a un dispositivo de red local mediante la VLAN de su puerta de enlace local.

El Outpost establece una sesión de interconexión BGP externa a través de la VLAN de la puerta de enlace local entre cada dispositivo de red Outpost y el dispositivo de red local del cliente conectado. La sesión de emparejamiento se establece entre el /30 o el /31 IPs que proporcionó al configurar la conectividad de red y utiliza la point-to-point conectividad entre los dispositivos de red de Outpost y los dispositivos de la red local del cliente. Para obtener más información, consulte the section called “Conectividad de capa de red”.

Cada sesión de BGP utiliza el ASN privado en el dispositivo de red de Outpost y un ASN que usted elija en el dispositivo de red local del cliente. AWS configura los atributos como parte del proceso previo a la instalación.

Considere el escenario en el que tiene un Outpost con dos dispositivos de red Outpost conectados mediante una VLAN de enlace de servicio a dos dispositivos de la red local del cliente. Debe configurar los siguientes atributos BGP ASN de la puerta de enlace local y del dispositivo de red local del cliente para cada enlace de servicio:

- El cliente proporciona la puerta de enlace local BGP ASN. 2 bytes (16 bits) o 4 bytes (32 bits). Los valores válidos son 64512-65535 o 4200000000-4294967294.
- (Opcional) Debe proporcionar el CIDR propiedad del cliente que se anuncia (público o privado, /26 como mínimo).
- Usted proporciona al dispositivo de red local del cliente 1 puertas de enlace locales BGP par de dirección IP.
- Usted proporciona al dispositivo de red local del cliente 1 puertas de enlace locales BGP par ASN. Los valores válidos son 1-4294967294. Para obtener más información, consulte RFC4893.
- Usted proporciona al dispositivo de red local del cliente 2 puertas de enlace locales BGP par de dirección IP.
- Usted proporciona al dispositivo de red local del cliente 2 puertas de enlace locales BGP par ASN. Los valores válidos son 1-4294967294. Para obtener más información, consulte RFC4893.



Le recomendamos que configure el equipo de red del cliente para recibir anuncios de BGP de Outposts sin cambiar los atributos de BGP y que habilite el equilibrador de multiruta y de carga del BGP para lograr flujos de tráfico entrante óptimos. El prefijo AS-Path se utiliza para desviar el tráfico de los prefijos de las puertas de enlace locales si es necesario realizar tareas de mantenimiento. ONDs La red de clientes debería preferir las rutas de Outposts con una longitud de AS-Path de 1 a las rutas con una longitud de AS-Path de 4.

La red del cliente debe anunciar a todas ellas prefijos BGP iguales con los mismos atributos. ONDs El equilibrador de carga de red de Outpost equilibra el tráfico saliente entre todos los enlaces ascendentes de forma predeterminada. Las políticas de enrutamiento se utilizan en el Outpost para desviar el tráfico de un OND si es necesario realizar tareas de mantenimiento. Este cambio de tráfico requiere que todos los clientes tengan los mismos prefijos de BGP. ONDs Si es necesario realizar tareas de mantenimiento en la red del cliente, le recomendamos que utilice AS-Path para desplazar temporalmente la matriz de tráfico desde enlaces ascendentes específicos.

Anuncio de subred IP propiedad del cliente de la puerta de enlace local

De forma predeterminada, la puerta de enlace local usa las direcciones IP privadas de las instancias de la VPC (consulte Enrutamiento directo de la VPC) para facilitar la comunicación con la red local.

Sin embargo, puede proporcionar un grupo de direcciones IP (CoIP) que son propiedad del cliente (CoIP).

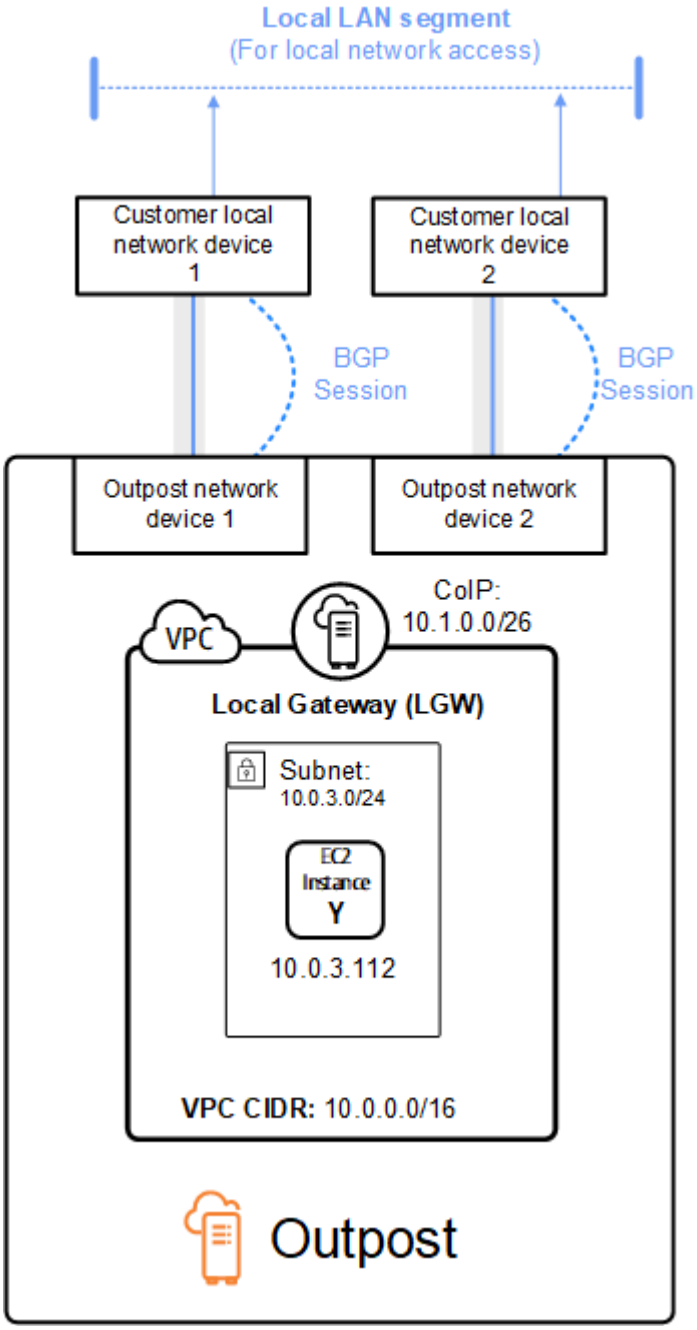
Puedes crear direcciones IP elásticas a partir de este grupo y, a continuación, asignarlas a los recursos de tu Outpost, como las instancias. EC2

La puerta de enlace local traduce la dirección IP elástica a una dirección del grupo propiedad del cliente. La puerta de enlace local anuncia la dirección traducida en la red en las instalaciones y en cualquier otra red que se comunique con el Outpost. Las direcciones se anuncian en las dos sesiones BGP de la puerta de enlace local y se envían a los dispositivos de la red local.

> **Tip**
>
> Si no utiliza CoIP, BGP anuncia las direcciones IP privadas de cualquier subred de su Outpost que tenga una ruta en la tabla de enrutamiento que se dirija a la puerta de enlace local.

Considere el escenario en el que tiene un Outpost con dos dispositivos de red Outpost conectados mediante una VLAN de enlace de servicio a dos dispositivos de la red local del cliente. Se configura lo siguiente:

- Una VPC con un bloque CIDR 10.0.0.0/16.
- Una subred en la VPC con un bloque CIDR 10.0.3.0/24.
- Una EC2 instancia en la subred con una dirección IP privada 10.0.3.112.
- Un grupo de IP propiedad del cliente (10.1.0.0/26).
- Una asociación de direcciones IP elásticas que asigna de 10.0.3.112 a 10.1.0.2.
- Una puerta de enlace local que utiliza BGP para anunciar la versión 10.1.0.0/26 en la red en las instalaciones a través de los dispositivos locales.
- La comunicación entre el Outpost y la red local utilizará el CoIP Elastic IPs para abordar las instancias del Outpost, no se utilizará el rango CIDR de VPC.


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

Administración de capacidad para AWS Outposts

Un puesto de avanzada proporciona un conjunto de capacidad AWS informática y de almacenamiento en su sitio como una extensión privada de una zona de disponibilidad en una AWS región. Como la capacidad de procesamiento y almacenamiento disponible en Outpost es limitada y está determinada por el tamaño y la cantidad de activos que se AWS instalen en su sitio, usted decide cuánta AWS Outposts capacidad de Amazon, EC2 Amazon EBS y Amazon S3 necesita para ejecutar sus cargas de trabajo iniciales, adaptarse al crecimiento futuro y proporcionar capacidad adicional para mitigar los fallos del servidor y los eventos de mantenimiento.

Temas

Vea AWS Outposts la capacidad

Puede ver la configuración de capacidad a nivel de instancia o Outpost.

Para ver la configuración de capacidad de tu Outpost mediante la consola

1. Abre la AWS Outposts consola en. https://console.aws.amazon.com/outposts/
2. En el panel de navegación izquierdo, selecciona Outposts.
3. Elige el Outpost.
4. En la página de detalles de Outpost, selecciona la vista de instancia o la vista de rack.
    - Vista de instancias: proporciona información sobre las instancias configuradas en los Outposts y la distribución de las instancias por tamaño y familia.
    - Vista en rack: proporciona una visualización de las instancias de cada activo de cada Outpost y le permite seleccionar Modificar la capacidad de la instancia para realizar cambios en la capacidad de la instancia.

Modifique la capacidad de las AWS Outposts instancias

La capacidad de cada nuevo pedido de Outpost se configura con una configuración de capacidad predeterminada. Puede convertir la configuración predeterminada para crear varias instancias para satisfacer las necesidades de su empresa. Para ello, debes crear una tarea de capacidad, elegir un Outposts o un solo activo, especificar el tamaño y la cantidad de las instancias y ejecutar la tarea de capacidad para implementar los cambios.

Consideraciones

Ten en cuenta lo siguiente antes de modificar la capacidad de la instancia:

- Las tareas de capacidad solo las puede ejecutar la AWS cuenta propietaria de los recursos de Outpost (propietaria). Los consumidores no pueden ejecutar tareas de capacidad. Para obtener más información sobre propietarios y consumidores, consulte Comparta sus AWS Outposts recursos.
- Los tamaños y cantidades de las instancias se pueden definir a nivel de Outpost o a nivel de activo individual.
- La capacidad se configura automáticamente en un activo o en todos los activos de un Outpost en función de las posibles configuraciones y las mejores prácticas.
- Mientras se ejecuta una tarea de capacidad, es posible que los activos asociados al puesto de avanzada seleccionado estén aislados. Por este motivo, te recomendamos crear una tarea de capacidad solo cuando no esperes lanzar nuevas instancias en tus Outposts.
- Puedes elegir ejecutar la tarea de capacidad al instante o seguir intentándola periódicamente durante las próximas 48 horas. Si opta por ejecutarla de forma instantánea, se requiere menos tiempo de aislamiento de los activos, pero la tarea podría fallar si es necesario detener las instancias para ejecutarla. Si opta por ejecutarla periódicamente, dispondrá de más tiempo para detener las instancias antes de que la tarea falle, pero los activos pueden permanecer aislados durante más tiempo.
- Es posible que las configuraciones de capacidad válidas no utilicen toda la vCPU disponible en un activo. En ese caso, aparecerá un mensaje al final de la sección de tipos de instancia en el que se le informará de que su capacidad es insuficiente, pero permitirá que la configuración se aplique según lo solicitado.
- Al modificar un Outpost en la consola, no se muestran todas las instancias compatibles, ya que la consola no admite totalmente la combinación de instancias respaldadas en disco con non-disk-backed instancias. Para acceder a todas las instancias posibles, utiliza la API. StartCapacityTask

- Al definir la capacidad de un Outpost, todas las familias y tipos de instancias se incluirán en la reconfiguración, a menos que se incluyan como instancias que se deben evitar.
- Solo puedes modificar la configuración de capacidad de Outposts existente para usar tamaños de EC2 instancia de Amazon válidos de familias de instancias compatibles con tu modelo de activos respectivo.
- Si tienes instancias ejecutándose en tu Outpost y no quieres detenerlas para ejecutar una tarea de capacidad, selecciona el ID de instancia correspondiente en la sección Instancias para mantenerlas como están (opcional) y asegúrate de conservar la cantidad necesaria de este tamaño de instancia en tu configuración de capacidad actualizada. Esto mantendrá las instancias que se utilizan para soportar las cargas de trabajo de producción mientras se ejecuta una tarea de capacidad.
- Cuando configures un activo con varios tamaños de instancias dentro de una familia de instancias, usa el equilibrio automático para asegurarte de que no estás intentando aprovisionar demasiado o insuficientemente tu contenido. El aprovisionamiento excesivo no es compatible y provocará un fallo en la tarea de capacidad.
- Si quieres reconfigurar por completo una familia de instancias en tu Outpost sin conservar ninguno de los tamaños de instancia de la configuración de capacidad original, debes detener todas las instancias de esa familia en ejecución en tu Outpost antes de ejecutar la tarea de capacidad. Si la instancia es propiedad de otra cuenta o la usa un servicio por capas que se ejecuta en Outpost, debes usar la cuenta del propietario de la instancia para detener la instancia o la instancia de servicio.
- Se pueden ejecutar varias tareas de capacidad en paralelo siempre que se apliquen a conjuntos de activos que se excluyen mutuamenteIDs. Por ejemplo, puede crear varias tareas de capacidad a nivel de activo para diferentes activos IDs al mismo tiempo. Sin embargo, si hay una tarea de Outpost en ejecución, no puedes crear otra tarea de Outpost o de nivel de activo al mismo tiempo. Del mismo modo, si hay una tarea de nivel de activo en ejecución, no puedes crear una tarea de nivel de Outpost o una tarea de nivel de activo en el mismo AssetID al mismo tiempo.

Para modificar la configuración de capacidad de tu Outpost mediante la consola

1. Abre la AWS Outposts consola en. https://console.aws.amazon.com/outposts/
2. En el panel de navegación izquierdo, selecciona Tareas de capacidad.
3. En la página Tareas de capacidad, seleccione Crear tarea de capacidad.
4. En la página de introducción, elige el pedido, el puesto de avanzada o el activo que deseas configurar.

5. Para modificar la capacidad, especifique una opción en Método de modificación: pasos electrónicos en la consola o cargue un archivo JSON.

   - Modifique el plan de configuración de la capacidad para seguir los pasos de la consola
   - Cargue un plan de configuración de capacidad para cargar un archivo JSON

> **Note**
>
> - Para evitar que la administración de capacidad recomiende detener instancias específicas, especifique las instancias que no se deben detener. Estas instancias se excluirán de la lista de instancias que se deben detener.

Console steps

1. Elija la vista de instancias o la vista de rack.
2. Elija Modificar la configuración de capacidad de un puesto avanzado o Modificar en un solo activo.
3. Elija un puesto de avanzada o un activo si es diferente de la selección actual.
4. Elija ejecutar esta tarea de capacidad de forma inmediata o periódica durante 48 horas.
5. Elija Siguiente.
6. En la página Configurar la capacidad de la instancia, cada tipo de instancia muestra un tamaño de instancia con la cantidad máxima preseleccionada. Para añadir más tamaños de instancia, seleccione Agregar tamaño de instancia.
7. Especifique la cantidad de instancias y anote la capacidad que se muestra para ese tamaño de instancia.
8. Consulte el mensaje al final de cada sección de tipos de instancia que le informa si está por encima o por debajo de su capacidad. Realice ajustes en el nivel de tamaño o cantidad de instancias para optimizar su capacidad total disponible.
9. También puede solicitar la optimización AWS Outposts de la cantidad de instancias para un tamaño de instancia específico. Para ello:

   a. Elija el tamaño de instancia.
   b. Seleccione Equilibrio automático al final de la sección relacionada con el tipo de instancia.

10. Para cada tipo de instancia, asegúrese de que la cantidad de instancias esté especificada para al menos un tamaño de instancia.
11. Si lo desea, elija instancias para mantenerlas tal como están.
12. Elija Siguiente.
13. En la página Revisar y crear, compruebe las actualizaciones que solicita.
14. Elija Crear. AWS Outposts crea una tarea de capacidad.
15. En la página de tareas de capacidad, supervise el estado de la tarea.

Upload a JSON file

1. Seleccione Cargar la configuración de capacidad.
2. Elija Siguiente.
3. En la página Cargar el plan de configuración de la capacidad de carga, suba el archivo JSON que especifica el tipo, el tamaño y la cantidad de instancias. Si lo desea, puede especificar los InstancesToExcludeTaskActionOnBlockingInstancesparámetros y en el archivo JSON.

   Example

   Ejemplo de archivo JSON:

```
{
  "InstancePools": [
    {
      "InstanceType": "c5.24xlarge",
      "Count": 1
    },
    {
      "InstanceType": "m5.24xlarge",
      "Count": 2
    }
  ],
  "InstancesToExclude": {
    "AccountIds": [
      "111122223333"
    ],
    "Instances": [
      "i-1234567890abcdef0"
    ],
    "Services": [
```

```
      "ALB"
    ]
  },
  "TaskActionOnBlockingInstances": "WAIT_FOR_EVACUATION"
}
```

4. Revise el contenido del archivo JSON en la sección Plan de configuración de capacidad.
5. Elija Siguiente.
6. En la página Revisar y crear, compruebe las actualizaciones que solicita.
7. Seleccione Crear. AWS Outposts crea una tarea de capacidad.
8. En la página de tareas de capacidad, supervise el estado de la tarea.

Solución de problemas de tareas de capacidad

Revise los siguientes problemas conocidos para resolver un problema relacionado con la administración de la capacidad en un nuevo pedido. Si su problema no aparece en la lista, póngase en contacto con Soporte.

oo-xxxxxxEl pedido no está asociado a Outpost ID ***op-xxxxx***

Este problema se produce cuando utilizas la API AWS CLI o para ejecutar la solicitud `StartCapacityTask`y el ID de Outpost de la solicitud no coincide con el ID de Outpost del pedido.

Para resolver este problema, siga estos pasos:

1. Inicia sesión en. AWS
2. Abre la AWS Outposts consola en https://console.aws.amazon.com/outposts/.
3. En el panel de navegación, selecciona Pedidos.
4. Seleccione el pedido y compruebe que el estado del pedido es uno de los siguientes:`PREPARING`,`IN_PROGRESS`, o`ACTIVE`.
5. Anote el ID de Outpost en el pedido.
6. Introduce el ID de Outpost correcto en la solicitud de `StartCapacityTask` API.

El plan de capacidad incluye tipos de instancias que no son compatibles

Este problema se produce cuando utilizas la API AWS CLI o para crear o modificar la tarea de capacidad y la solicitud contiene tipos de instancias no compatibles.

Para resolver este problema, utilice la consola o la CLI.

Uso de la consola

1. Inicie sesión en AWS.
2. Abre la AWS Outposts consola en https://console.aws.amazon.com/outposts/.
3. En el panel de navegación, elija la tarea de capacidad.
4. Usa la opción de configuración Cargar una capacidad para cargar un JSON con la misma lista de tipos de instancias.
5. La consola muestra un mensaje de error con la lista de tipos de instancias compatibles.
6. Corrija la solicitud para eliminar los tipos de instancias no compatibles.
7. Cree o modifique la tarea de capacidad en la consola mediante el JSON corregido o utilice la CLI o la API con esta lista corregida de tipos de instancias.

Utilizar la CLI de

1. Usa el GetOutpostSupportedInstanceTypescomando para ver la lista de tipos de instancias compatibles.
2. Cree o modifique la tarea de capacidad con la lista correcta de tipos de instancias.

No hay Outpost con un ID de Outpost *op-xxxxx*

Este problema se produce cuando utilizas la API AWS CLI o para ejecutar la solicitud `StartCapacityTask`y la solicitud contiene un ID de Outpost que no es válido por uno de los siguientes motivos:

- El puesto de avanzada se encuentra en una región diferente. AWS
- No tienes permisos para acceder a este puesto de avanzada.
- El ID del puesto de avanzada es incorrecto.

Para resolver este problema, siga estos pasos:

1. Anota la AWS región que utilizaste en la solicitud de `StartCapacityTask` API.
2. Usa la acción de la `ListOutposts`API para obtener una lista de los Outposts de tu propiedad en la AWS región.

3. Comprueba si el ID de Outpost aparece en la lista.
4. Introduce el ID de Outpost correcto en la `StartCapacityTask` solicitud.
5. Si no encuentras el ID de Outpost, vuelve a utilizar la acción de la `ListOutposts` API para comprobar si el Outpost existe en una región diferente. AWS

CapacityTaskLímite activo: *XXXX* ya se ha encontrado para Outpost op- *XXXX*

Este problema se produce cuando utilizas la AWS Outposts consola o la API para ejecutar StartCapacityTaskun Outpost y ya hay una tarea de capacidad de ejecución para el Outpost. Se considera que una tarea de capacidad está en ejecución si tiene alguno de los siguientes estados:`REQUESTED`,`IN_PROGRESS`, `WAITING_FOR_EVACUATION` o. `CANCELLATION_IN_PROGRESS`

Para resolver este problema, utilice la AWS Outposts consola o la CLI.

Uso de la consola

1. Inicie sesión en AWS.
2. Abre la AWS Outposts consola en https://console.aws.amazon.com/outposts/.
3. En el panel de navegación, seleccione Tareas de capacidad.
4. Asegúrese de que no haya tareas de capacidad en ejecución para OutpostId.
5. Si hay tareas de capacidad en ejecución para ellas OutpostId, espere a que finalicen o cancélelas si lo desea.
6. Cuando no haya tareas de capacidad de ejecución para la solicitada OutpostId, vuelva a intentar la solicitud para crear la tarea de capacidad.

Utilizar la CLI de

1. Usa el ListCapacityTaskscomando para buscar tareas de capacidad de ejecución para el Outpost.
2. Espere a que finalicen todas las tareas de capacidad en ejecución o cancélelas si lo desea.
3. Cuando no haya tareas de capacidad de ejecución para la solicitada OutpostId, vuelva a intentar la solicitud para crear la tarea de capacidad.

CapacityTaskLímite activo: *XXXX* ya se ha encontrado para Asset *XXXX* on Outpost OP-xxxx

Este problema se produce cuando utilizas la AWS Outposts consola o la API para ejecutar StartCapacityTaskun activo y ya existe una tarea de capacidad de ejecución para el activo. Se considera que una tarea de capacidad está en ejecución si tiene alguno de los siguientes estados:`REQUESTED`, `IN_PROGRESSWAITING_FOR_EVACUATION`, o`CANCELLATION_IN_PROGRESS`.

Para resolver este problema, utilice la AWS Outposts consola o la CLI.

Uso de la consola

1. Inicie sesión en AWS.
2. Abre la AWS Outposts consola en https://console.aws.amazon.com/outposts/.
3. En el panel de navegación, seleccione Tareas de capacidad.
4. Asegúrese de que no haya tareas de capacidad en ejecución ni tareas de OutpostId capacidad a nivel de activo en ejecución para el. AssetId
5. Si hay tareas de capacidad en ejecución, espere a que finalicen o cancélelas si lo desea.
6. Cuando no haya tareas de capacidad en ejecución, vuelva a intentar la solicitud para crear la tarea de capacidad.

Utilizar la CLI de

1. Use el ListCapacityTaskscomando para buscar tareas de capacidad de ejecución para OutPostID y AssetID.
2. Asegúrese de que no se estén ejecutando tareas de capacidad a nivel de Outpost ni tareas de capacidad a nivel de OutpostId activo en ejecución para el. AssetId
3. Si hay tareas de capacidad en ejecución, espere a que finalicen o cancélelas si lo desea.
4. Vuelva a intentar la solicitud para crear la tarea de capacidad.

AssetId= no *XXXX* es válido para Outpost=OP- *XXXX*

Este problema se produce cuando se utiliza la AWS Outposts consola o la API para ejecutar StartCapacityTaskun activo y el AssetID no es válido por uno de los siguientes motivos:

- El activo no está asociado al Outpost.
- El activo está aislado.

Para resolver este problema, utilice la AWS Outposts consola o la CLI.

Uso de la consola

1. Inicie sesión en AWS.
2. Abre la AWS Outposts consola en https://console.aws.amazon.com/outposts/.
3. Elija la vista de estantería para el puesto de avanzada.
4. Compruebe que la solicitud AssetId esté asociada al puesto de avanzada y que no esté marcada como host aislado.

    a. Si el activo está aislado, puede deberse a que se esté ejecutando una tarea de capacidad en él. Puedes ir al panel de tareas de capacidad y comprobar si hay alguna tarea de Outpost o de nivel de activo en ejecución para y. OutpostId AssetId Si las hay, espera a que la tarea finalice y a que el activo vuelva a estar disponible.

    b. Si no hay tareas de capacidad de ejecución para un activo aislado, es posible que el activo esté degradado.
5. Tras comprobar que el activo existe y se encuentra en un estado válido, vuelva a intentar realizar la solicitud para crear la tarea de capacidad.

Utilizar la CLI de

1. Utilice el ListAssetscomando para buscar los activos asociados al OutpostID.
2. Compruebe que la solicitud AssetId esté asociada al Outpost y que su estado lo esté. `ACTIVE`

    a. Si el estado del activo no es ACTIVO, puede deberse a que se esté ejecutando una tarea de capacidad en él. Usa el ListCapacityTaskscomando para determinar si se están ejecutando tareas de Outpost o de nivel de activo para y. OutpostId AssetId Si las hay, espere a que la tarea finalice y a que el activo vuelva a estar ACTIVO.

    b. Si no hay tareas de capacidad de ejecución para un activo aislado, es posible que el activo esté degradado.
3. Tras comprobar que el activo existe y se encuentra en un estado válido, vuelva a intentar realizar la solicitud para crear la tarea de capacidad.

Comparta sus AWS Outposts recursos

Al compartir Outpost, los propietarios de Outpost pueden compartir sus recursos de Outposts y Outpost, incluidos los sitios y subredes de Outpost, con otras cuentas de la misma organización. AWS AWS Como propietario de Outpost, puedes crear y administrar los recursos de Outpost de forma centralizada y compartir los recursos entre varias cuentas de tu organización. AWS AWS Esto permite a otros consumidores usar los sitios de Outpost, configurar VPCs, lanzar y ejecutar instancias en el Outpost compartido.

En este modelo, la AWS cuenta propietaria de los recursos de Outpost (propietaria) comparte los recursos con otras AWS cuentas (consumidores) de la misma organización. Los consumidores pueden crear recursos en los Outposts que se comparten con ellos del mismo modo que crearían recursos en los Outposts que crean en su propia cuenta. El propietario es responsable de administrar el Outpost y los recursos que crean en él. Los propietarios pueden cambiar o revocar el acceso compartido en cualquier momento. Con la excepción de los casos que consumen reservas de capacidad, los propietarios también pueden ver, modificar y eliminar recursos que crean los consumidores en los Outposts compartidos. Los propietarios no pueden modificar instancias que los consumidores inician en reservas de capacidad que han compartido.

Los consumidores son responsables de administrar los recursos que crean en los Outposts que comparten con ellos, incluidos los recursos que consumen reservas de capacidad. Los consumidores no pueden ver o modificar recursos que sean propiedad de otros consumidores o del propietario del Outpost. Tampoco pueden modificar los Outposts que compartan con ellos.

Un propietario de Outpost puede compartir recursos de Outpost con:

- AWS Cuentas específicas de su organización en AWS Organizations.
- Una unidad organizativa dentro de la organización en AWS Organizations.
- Toda la organización en AWS Organizations.

Contenido

- Dejar de compartir un recurso de Outpost compartido
- Identificación de un recurso de Outpost compartido
- Permisos de recursos de Outpost compartidos
- Facturación y medición
- Limitaciones

Recursos de Outpost compartibles

El propietario de Outpost puede compartir con los consumidores los recursos de Outpost que se enumeran en esta sección.

A continuación, se describen los recursos disponibles para los servidores de Outposts.

- Hosts dedicados asignados: los consumidores con acceso a este recurso pueden:
  - Lanza y ejecuta EC2 instancias en un host dedicado.
- Reservas de capacidad: los consumidores con acceso a este recurso pueden:
  - Identifique las reservas de capacidad compartidas con ellos.
  - Lance y gestione instancias que consumen reservas de capacidad.
- Grupos de direcciones IP propiedad del cliente (CoIP): los consumidores con acceso a este recurso pueden:
  - Asigne y asocie direcciones IP propiedad del cliente con las instancias.
- Tablas de enrutamiento de las puertas de enlace locales: los consumidores con acceso a este recurso pueden:
  - Cree y administre asociaciones de VPC a una puerta de enlace local.
  - Vea las configuraciones de las tablas de enrutamiento y las interfaces virtuales de las puertas de enlace locales.
- Outposts: los consumidores con acceso a este recurso pueden:
  - Crear y administrar una subred en el Outpost.
  - Cree y administre volúmenes de EBS en el Outpost.
  - Usa la AWS Outposts API para ver información sobre el Outpost.
- S3 en Outposts: los consumidores con acceso a este recurso pueden:
  - Cree y administre buckets de S3, puntos de acceso y puntos de conexión en el Outpost.
- Sitios: los consumidores con acceso a este recurso pueden:

  - Crear, administrar y controlar un Outpost en el sitio.
- Subredes: los consumidores con acceso a este recurso pueden:
  - Ver información sobre subredes.
  - Lanza y ejecuta EC2 instancias en subredes.

  Utilice la consola de Amazon VPC para compartir una subred de Outpost. Para obtener más información, consulte Compartir una subred en la Guía del usuario de Amazon VPC.

Requisitos previos para compartir recursos de Outposts

- Para compartir un recurso de Outpost con la organización o con una unidad organizativa en AWS Organizations, debe habilitar el uso compartido con AWS Organizations. Para obtener más información, consulte Habilitar el uso compartido con AWS Organizations en la Guía del usuario de AWS RAM .
- Para compartir un recurso de Outpost, debes tenerlo en tu AWS cuenta. No puede compartir un recurso de Outpost que se haya compartido con usted.
- Para compartir un recurso de Outpost, debe compartirlo con una cuenta que se encuentre dentro de la organización.

Servicios relacionados

El intercambio de recursos de Outpost se integra con AWS Resource Access Manager ()AWS RAM. AWS RAM es un servicio que le permite compartir sus AWS recursos con cualquier AWS cuenta o a través AWS Organizations de. Con AWS RAM, puede compartir recursos de su propiedad creando un uso compartido de recursos. Un uso compartido de recursos especifica los recursos que compartir y los consumidores con quienes compartirlos. Los consumidores pueden ser AWS cuentas individuales, unidades organizativas o toda una organización AWS Organizations.

Para obtener más información al respecto AWS RAM, consulte la Guía AWS RAM del usuario.

Uso compartido entre zonas de disponibilidad

Para garantizar que los recursos se distribuyen por todas las zonas de disponibilidad de una región, asignamos zonas de disponibilidad de manera independiente a nombres de cada cuenta. Esto podría dar lugar a diferencias de nomenclatura de zona de disponibilidad entre cuentas. Por ejemplo, es

posible que la zona `us-east-1a` de disponibilidad de su AWS cuenta no tenga la misma ubicación que la `us-east-1a` de otra AWS cuenta.

Para identificar la ubicación del recurso de Outpost relativo a sus cuentas, debe utilizar el ID de zona de disponibilidad (ID de AZ). El ID de zona de disponibilidad es un identificador único y coherente de una zona de disponibilidad en todas AWS las cuentas. Por ejemplo, `use1-az1` es un ID de zona geográfica para la `us-east-1` región y se encuentra en la misma ubicación en todas las AWS cuentas.

Para ver las IDs zonas de disponibilidad de su cuenta

1. Navegue hasta la AWS RAM consola en la AWS RAM consola.
2. Las AZ IDs de la región actual se muestran en el panel Tu ID de AZ, en la parte derecha de la pantalla.

> **Note**
>
> Las tablas de enrutamiento de las puertas de enlace locales están en la misma AZ que sus Outpost, por lo que no es necesario especificar un ID de AZ para las tablas de enrutamiento.

Uso compartido de un recurso de Outpost

Cuando un propietario comparte un Outpost con un consumidor, el consumidor puede crear recursos en el Outpost del mismo modo que lo haría en los recursos en Outposts que crea en su propia cuenta. Los consumidores con acceso a tablas de enrutamiento de puertas de enlace locales compartidas pueden crear y administrar asociaciones de VPC. Para obtener más información, consulte Recursos de Outpost compartibles.

Para compartir un recurso de Outpost, debe agregarlo al recurso compartido. Un recurso compartido es un AWS RAM recurso que te permite compartir tus recursos entre AWS cuentas. Un uso compartido de recursos especifica los recursos que compartir y los consumidores con quienes se comparten. Cuando compartes un recurso de Outpost mediante la AWS Outposts consola, lo agregas a un recurso compartido existente. Para agregar el recurso de Outpost a un nuevo uso compartido de recurso, debe crear el uso compartido del recurso utilizando la consola de AWS RAM.

Si formas parte de una organización AWS Organizations y el uso compartido dentro de tu organización está activado, puedes conceder a los consumidores de tu organización acceso desde

la AWS RAM consola al recurso de Outpost compartido. De lo contrario, los consumidores reciben una invitación para unirse al recurso compartido y se les concede acceso al recurso de Outpost compartido al aceptar la invitación.

Puedes compartir un recurso de Outpost que te pertenezca mediante la AWS Outposts consola, la AWS RAM consola o el. AWS CLI

Para compartir un Outpost de tu propiedad mediante la consola AWS Outposts

1. Abre la AWS Outposts consola en. https://console.aws.amazon.com/outposts/
2. En el panel de navegación, elija Outposts.
3. Seleccione el Outpost y, a continuación, elija Acciones, Ver detalles.
4. En la página de Resumen de Outpost, seleccione Recursos compartidos.
5. Elija Crear recurso compartido.

Se le redirigirá a la AWS RAM consola para terminar de compartir el Outpost mediante el siguiente procedimiento. Para compartir una tabla de enrutamiento de la puerta de enlace local de su propiedad, utilice también el siguiente procedimiento.

Cómo compartir una tabla de enrutamiento de Outpost o puerta de enlace local de su propiedad mediante la consola de AWS RAM

Consulte Crear un recurso compartido en la Guía del usuario de AWS RAM .

Para compartir una tabla de rutas de Outpost o una puerta de enlace local que sea de su propiedad mediante el AWS CLI

Utilice el comando create-resource-share.

Dejar de compartir un recurso de Outpost compartido

Cuando deja de compartir su Outpost con un consumidor, el consumidor ya no puede hacer lo siguiente:

- Ve el Outpost en la AWS Outposts consola.
- Crear nuevas subredes en el Outpost.
- Crear y administrar volúmenes de EBS en el Outpost.

- Vea los detalles de Outpost y los tipos de instancias mediante la AWS Outposts consola o el. AWS CLI

Las subredes, los volúmenes o las instancias que el consumidor creó durante el período compartido no se eliminan y el consumidor puede seguir haciendo lo siguiente:

- Acceder a estos recursos y modificarlos.
- Lanzar nuevas instancias en una subred existente que haya creado el consumidor.

Para evitar que el consumidor acceda a sus recursos y lance nuevas instancias en su Outpost, pídale al consumidor que elimine sus recursos.

Cuando una tabla de enrutamiento de una puerta de enlace local deja de compartirse, los consumidores ya no pueden crear nuevas asociaciones de VPC con ella. Todas las asociaciones de VPC existentes que haya creado el consumidor permanecen asociadas a la tabla de enrutamiento. Los recursos que contienen VPCs pueden seguir dirigiendo el tráfico a la puerta de enlace local. Para evitarlo, solicite al consumidor que elimine las asociaciones de VPC.

Para dejar de compartir un recurso de Outpost de su propiedad, debe quitarlo del recurso compartido. Puede hacerlo mediante la AWS RAM consola o el AWS CLI.

Para dejar de compartir un recurso de Outpost compartido que te pertenezca mediante la consola AWS RAM

Consulte Actualizar un recurso compartido en la Guía del usuario de AWS RAM .

Para dejar de compartir un recurso de Outpost compartido del que seas propietario mediante el AWS CLI

Utilice el comando disassociate-resource-share.

Identificación de un recurso de Outpost compartido

Los propietarios y los consumidores pueden identificar los Outposts compartidos mediante la AWS Outposts consola y. AWS CLI Pueden identificar tablas de enrutamiento de la puerta de enlace local compartidas mediante el uso de AWS CLI.

Para identificar un Outpost compartido mediante la consola AWS Outposts

1. Abre la AWS Outposts consola en. https://console.aws.amazon.com/outposts/

2. En el panel de navegación, elija Outposts.
3. Seleccione el Outpost y, a continuación, elija Acciones, Ver detalles.
4. En la página de resumen de Outpost, consulta el ID de propietario para identificar el ID de AWS cuenta del propietario de Outpost.

Para identificar un recurso de Outpost compartido mediante el AWS CLI

Utilice los comandos list-outposts y -tables. describe-local-gateway-route Estos comandos devuelven los recursos de Outpost que posees y los recursos de Outpost que se comparten contigo. `OwnerId`muestra el ID de AWS cuenta del propietario del recurso de Outpost.

Permisos de recursos de Outpost compartidos

Permisos de los propietarios

Los propietarios son responsables de administrar el Outpost y los recursos que crean en él. Los propietarios pueden cambiar o revocar el acceso compartido en cualquier momento. Se pueden usar AWS Organizations para ver, modificar y eliminar los recursos que los consumidores crean en los Outposts compartidos.

Permisos de los consumidores

Los consumidores pueden crear recursos en los Outposts que se comparten con ellos del mismo modo que crearían recursos en los Outposts que crean en su propia cuenta. Los consumidores son responsables de administrar los recursos que lanzan en los Outposts que se comparten con ellos. Los consumidores no pueden ver ni modificar recursos que son propiedad de otros consumidores o del propietario de Outpost, y no pueden modificar los Outposts que se comparten con ellos.

Facturación y medición

A los propietarios se les cobran los Outposts y los recursos de Outpost que comparten. También se les facturará cualquier cargo de transferencia de datos asociado al tráfico de VPN de enlace de servicio de Outpost desde la región. AWS

No se aplican cargos adicionales por compartir tablas de enrutamiento de la puerta de enlace local. En el caso de las subredes compartidas, se facturan al propietario de la VPC los recursos de nivel de

VPC, AWS Direct Connect como las conexiones VPN, las puertas de enlace NAT y las conexiones de enlace privado.

A los consumidores se les facturan los recursos de las aplicaciones que crean en Outposts compartidos, como los equilibradores de carga y las bases de datos de Amazon RDS. A los consumidores también se les facturan las transferencias de datos cobrables desde la región. AWS

Limitaciones

Al trabajar con el AWS Outposts uso compartido se aplican las siguientes limitaciones:

- Las limitaciones de las subredes compartidas se aplican al AWS Outposts uso compartido. Para obtener más información acerca de los límites de uso compartido de la VPC, consulte Limitaciones en la Guía del usuario de Amazon Virtual Private Cloud.
- Las cuotas de servicio se aplican a cada cuenta.

Seguridad en AWS Outposts

La seguridad AWS es la máxima prioridad. Como AWS cliente, usted se beneficia de una arquitectura de centro de datos y red diseñada para cumplir con los requisitos de las organizaciones más sensibles a la seguridad.

La seguridad es una responsabilidad compartida entre usted AWS y usted. El modelo de responsabilidad compartida la describe como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta AWS los servicios en la AWS nube. AWS también le proporciona servicios que puede utilizar de forma segura. Los auditores externos prueban y verifican periódicamente la eficacia de nuestra seguridad como parte de los AWS programas de de . Para obtener más información sobre los programas de cumplimiento aplicables AWS Outposts, consulte AWS Servicios incluidos en el ámbito de aplicación por programa de conformidad y AWS servicios incluidos .
- Seguridad en la nube: su responsabilidad viene determinada por el AWS servicio que utilice. También eres responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y la normativa aplicables.

Para obtener más información sobre la seguridad y el cumplimiento AWS Outposts, consulte las Preguntas frecuentes sobre de AWS Outposts rack.

Esta documentación le ayuda a comprender cómo aplicar el modelo de responsabilidad compartida cuando se utiliza AWS Outposts. Muestra cómo cumplir sus objetivos de seguridad y conformidad. También aprenderá a utilizar otros AWS servicios que le ayudan a supervisar y proteger sus recursos.

Contenido

Protección de datos en AWS Outposts

El modelo de responsabilidad AWS compartida modelo se aplica a la protección de datos en AWS Outposts. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global que ejecuta todos los Nube de AWS. Eres responsable de mantener el control sobre el contenido alojado en esta infraestructura. Este contenido incluye las tareas de configuración y administración de la seguridad Servicios de AWS que utilice.

Con fines de protección de datos, le recomendamos que proteja Cuenta de AWS las credenciales y configure los usuarios individuales con AWS IAM Identity Center o AWS Identity and Access Management (IAM). De esta manera, solo se otorgan a cada usuario los permisos necesarios para cumplir sus obligaciones laborales.

Para obtener más información sobre la privacidad de los datos, consulta las Preguntas frecuentes sobre la privacidad de datos. Para obtener información sobre la protección de datos en Europa, consulta la publicación de blog sobre el Modelo de responsabilidad compartida de AWS y GDPR en el Blog de seguridad de AWS .

Cifrado en reposo

Con AWS Outposts, todos los datos se cifran en reposo. El material clave está encapsulado en una clave externa almacenada en un dispositivo extraíble: la clave de seguridad Nitro (NSK). La NSK es necesaria para descifrar los datos de sus bastidores de Outposts.

Puede utilizar el cifrado de Amazon EBS para volúmenes e instantáneas de EBS. El cifrado de Amazon EBS utiliza AWS Key Management Service (AWS KMS) y claves KMS. Para obtener más información, consulte Amazon EBS Encryption en la Guía del usuario de Amazon EBS.

Cifrado en tránsito

AWS cifra los datos en tránsito entre su Outpost y su región. AWS Para obtener más información, consulte Conectividad a través de enlace de servicio.

Puede utilizar un protocolo de cifrado, como la Seguridad de la capa de transporte (TLS) para cifrar datos en tránsito confidenciales a través de la puerta de enlace local a la red local.

Eliminación de datos

Al detener o cerrar una EC2 instancia, el hipervisor limpia la memoria que se le ha asignado (se establece en cero) antes de asignarla a una nueva instancia y se restablecen todos los bloques de almacenamiento.

Al destruir la clave de seguridad Nitro, los datos de su Outpost se destruyen criptográficamente.

Identity and Access Management (IAM) para AWS Outposts

AWS Identity and Access Management (IAM) es un AWS servicio que ayuda al administrador a controlar de forma segura el acceso a los recursos. AWS Los administradores de IAM controlan quién puede autenticarse (iniciar sesión) y quién puede autorizarse (tener permisos) para usar los recursos. AWS Outposts El uso de IAM no está sujeto a ningún cargo adicional.

Contenido

Cómo funciona AWS Outposts con IAM

Antes de usar IAM para administrar el acceso a AWS Outposts, descubre qué funciones de IAM están disponibles para usar con Outposts. AWS

Característica de IAM	AWS Soporte para Outposts
Políticas basadas en identidades	Sí
Políticas basadas en recursos	No
Acciones de políticas	Sí
Recursos de políticas	Sí
Claves de condición de política (específicas del servicio)	Sí

Característica de IAM	AWS Soporte para Outposts
ACLs	No
ABAC (etiquetas en políticas)	Sí
Credenciales temporales	Sí
Permisos de entidades principales	Sí
Roles de servicio	No
Roles vinculados al servicio	Sí

Políticas basadas en la identidad para Outposts AWS

Compatibilidad con las políticas basadas en identidad: sí

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede asociar a una identidad, como un usuario de IAM, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en identidad, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Con las políticas basadas en identidades de IAM, puede especificar las acciones y los recursos permitidos o denegados, así como las condiciones en las que se permiten o deniegan las acciones. No es posible especificar la entidad principal en una política basada en identidad porque se aplica al usuario o rol al que está asociada. Para obtener más información sobre los elementos que puede utilizar en una política de JSON, consulte Referencia de los elementos de las políticas de JSON de IAM en la Guía del usuario de IAM.

Ejemplos de políticas basadas en la identidad para Outposts AWS

Para ver ejemplos de políticas basadas en la identidad de AWS Outposts, consulte. AWS Ejemplos de políticas de Outposts

Acciones políticas para AWS Outposts

Compatibilidad con las acciones de políticas: sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Action` de una política JSON describe las acciones que puede utilizar para conceder o denegar el acceso en una política. Las acciones políticas suelen tener el mismo nombre que la operación de AWS API asociada. Hay algunas excepciones, como acciones de solo permiso que no tienen una operación de API coincidente. También hay algunas operaciones que requieren varias acciones en una política. Estas acciones adicionales se denominan acciones dependientes.

Incluya acciones en una política para conceder permisos y así llevar a cabo la operación asociada.

Para ver una lista de las acciones de AWS Outposts, consulta las acciones definidas AWS Outposts en la Referencia de autorización del servicio.

Las acciones políticas en AWS Outposts usan el siguiente prefijo antes de la acción:

```
outposts
```

Para especificar varias acciones en una única instrucción, sepárelas con comas.

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

Puede utilizar caracteres comodín (*) para especificar varias acciones . Por ejemplo, para especificar todas las acciones que comiencen con la palabra `List`, incluya la siguiente acción:

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

Recursos de políticas para AWS Outposts

Compatibilidad con los recursos de políticas: sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puedes realizar acciones en qué recursos y en qué condiciones.

El elemento `Resource` de la política JSON especifica el objeto u objetos a los que se aplica la acción. Las instrucciones deben contener un elemento `Resource` o `NotResource`. Como práctica recomendada, especifique un recurso utilizando el Nombre de recurso de Amazon (ARN). Puedes

hacerlo para acciones que admitan un tipo de recurso específico, conocido como permisos de nivel de recurso.

Para las acciones que no admiten permisos de nivel de recurso, como las operaciones de descripción, utiliza un carácter comodín (*) para indicar que la instrucción se aplica a todos los recursos.

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

Algunas acciones de la API de AWS Outposts admiten varios recursos. Para especificar varios recursos en una sola sentencia, sepárelos ARNs con comas.

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

Para ver una lista de los tipos de recursos de AWS Outposts y sus tipos ARNs, consulta los tipos de recursos definidos AWS Outposts en la Referencia de autorización de servicio. Para obtener información sobre las acciones con las que puede especificar el ARN de cada recurso, consulte Acciones definidas por AWS Outposts.

Claves condicionales de la política para AWS Outposts

Compatibilidad con claves de condición de políticas específicas del servicio: sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puedes realizar acciones en qué recursos y en qué condiciones.

El elemento `Condition` (o bloque de `Condition`) permite especificar condiciones en las que entra en vigor una instrucción. El elemento `Condition` es opcional. Puedes crear expresiones condicionales que utilizan operadores de condición, tales como igual o menor que, para que la condición de la política coincida con los valores de la solicitud.

Si especifica varios elementos de `Condition` en una instrucción o varias claves en un único elemento de `Condition`, AWS las evalúa mediante una operación `AND` lógica. Si especifica varios valores para una única clave de condición, AWS evalúa la condición mediante una `OR` operación lógica. Se deben cumplir todas las condiciones antes de que se concedan los permisos de la instrucción.

También puedes utilizar variables de marcador de posición al especificar condiciones. Por ejemplo, puedes conceder un permiso de usuario de IAM para acceder a un recurso solo si está etiquetado con su nombre de usuario de IAM. Para más información, consulta Elementos de la política de IAM: variables y etiquetas en la Guía del usuario de IAM.

AWS admite claves de condición globales y claves de condición específicas del servicio. Para ver todas las claves de condición AWS globales, consulte las claves de contexto de condición AWS globales en la Guía del usuario de IAM.

Para ver una lista de las claves de condición de AWS Outposts, consulta las claves de condición AWS Outposts en la Referencia de autorización de servicio. Para saber con qué acciones y recursos puede utilizar una clave de condición, consulte Acciones definidas por AWS Outposts.

Para ver ejemplos de políticas basadas en la identidad de AWS Outposts, consulte. AWS Ejemplos de políticas de Outposts

ABAC con Outposts AWS

Admite ABAC (etiquetas en las políticas): sí

El control de acceso basado en atributos (ABAC) es una estrategia de autorización que define permisos en función de atributos. En AWS, estos atributos se denominan etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a muchos AWS recursos. El etiquetado de entidades y recursos es el primer paso de ABAC. A continuación, designa las políticas de ABAC para permitir operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso al que se intenta acceder.

ABAC es útil en entornos que crecen con rapidez y ayuda en situaciones en las que la administración de las políticas resulta engorrosa.

Para controlar el acceso en función de etiquetas, debe proporcionar información de las etiquetas en el elemento de condición de una política utilizando las claves de condición `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Si un servicio admite las tres claves de condición para cada tipo de recurso, el valor es Sí para el servicio. Si un servicio admite las tres claves de condición solo para algunos tipos de recursos, el valor es Parcial.

Para obtener más información sobre ABAC, consulte Definición de permisos con la autorización de ABAC en la Guía del usuario de IAM. Para ver un tutorial con los pasos para configurar ABAC, consulte Uso del control de acceso basado en atributos (ABAC) en la Guía del usuario de IAM.

Uso de credenciales temporales con AWS Outposts

Compatibilidad con credenciales temporales: sí

Algunas Servicios de AWS no funcionan cuando inicias sesión con credenciales temporales. Para obtener información adicional, incluida la información sobre cuáles Servicios de AWS funcionan con credenciales temporales, consulta Cómo Servicios de AWS funcionan con IAM en la Guía del usuario de IAM.

Utiliza credenciales temporales si inicia sesión en ellas AWS Management Console mediante cualquier método excepto un nombre de usuario y una contraseña. Por ejemplo, cuando accedes AWS mediante el enlace de inicio de sesión único (SSO) de tu empresa, ese proceso crea automáticamente credenciales temporales. También crea credenciales temporales de forma automática cuando inicia sesión en la consola como usuario y luego cambia de rol. Para obtener más información sobre el cambio de roles, consulte Cambio de un usuario a un rol de IAM (consola) en la Guía del usuario de IAM.

Puedes crear credenciales temporales manualmente mediante la AWS CLI API o. AWS A continuación, puede utilizar esas credenciales temporales para acceder AWS. AWS recomienda generar credenciales temporales de forma dinámica en lugar de utilizar claves de acceso a largo plazo. Para obtener más información, consulte Credenciales de seguridad temporales en IAM.

Permisos principales entre servicios para Outposts AWS

Admite sesiones de acceso directo (FAS): sí

Cuando utilizas un usuario o un rol de IAM para realizar acciones en él AWS, se te considera principal. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. FAS utiliza los permisos del principal que llama y los que solicita Servicio de AWS para realizar solicitudes a los servicios descendentes. Servicio de AWS Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte Reenviar sesiones de acceso.

Funciones vinculadas al servicio para Outposts AWS

Admite roles vinculados a servicios: sí

Un rol vinculado a un servicio es un tipo de rol de servicio que está vinculado a un. Servicio de AWS El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio

aparecen en usted Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

Para obtener más información sobre la creación o administración de AWS roles vinculados al servicio Outposts, consulte. Funciones vinculadas al servicio para AWS Outposts

AWS Ejemplos de políticas de Outposts

De forma predeterminada, los usuarios y los roles no tienen permiso para crear o modificar los recursos de AWS Outposts. Tampoco pueden realizar tareas mediante la AWS Management Console, AWS Command Line Interface (AWS CLI) o la AWS API. Un administrador de IAM puede crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan. A continuación, el administrador puedes añadir las políticas de IAM a roles y los usuarios puedes asumirlos.

Para obtener información acerca de cómo crear una política basada en identidades de IAM mediante el uso de estos documentos de políticas JSON de ejemplo, consulte Creación de políticas de IAM (consola) en la Guía del usuario de IAM.

Para obtener más información sobre las acciones y los tipos de recursos definidos por AWS Outposts, incluido el formato de cada uno de los tipos de recursos, consulta las claves de condición, recursos y acciones de la Referencia AWS Outposts de autorización de servicio. ARNs

Contenido

Prácticas recomendadas sobre las políticas

Las políticas basadas en la identidad determinan si alguien puede crear, acceder o eliminar los recursos de AWS Outposts de tu cuenta. Estas acciones pueden generar costos adicionales para su Cuenta de AWS. Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidades:

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos: para empezar a conceder permisos a sus usuarios y cargas de trabajo, utilice las políticas AWS administradas que otorgan permisos para muchos casos de uso comunes. Están disponibles en su. Cuenta de AWS Le recomendamos que reduzca aún más los permisos

definiendo políticas administradas por el AWS cliente que sean específicas para sus casos de uso. Con el fin de obtener más información, consulta las políticas administradas por AWS o las políticas administradas por AWS para funciones de tarea en la Guía de usuario de IAM.

- Aplique permisos de privilegio mínimo: cuando establezca permisos con políticas de IAM, conceda solo los permisos necesarios para realizar una tarea. Para ello, debe definir las acciones que se pueden llevar a cabo en determinados recursos en condiciones específicas, también conocidos como permisos de privilegios mínimos. Con el fin de obtener más información sobre el uso de IAM para aplicar permisos, consulta Políticas y permisos en IAM en la Guía del usuario de IAM.
- Utilice condiciones en las políticas de IAM para restringir aún más el acceso: puede agregar una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puede escribir una condición de políticas para especificar que todas las solicitudes deben enviarse utilizando SSL. También puedes usar condiciones para conceder el acceso a las acciones del servicio si se utilizan a través de una acción específica Servicio de AWS, por ejemplo AWS CloudFormation. Para obtener más información, consulta Elementos de la política de JSON de IAM: Condición en la Guía del usuario de IAM.
- Utiliza el analizador de acceso de IAM para validar las políticas de IAM con el fin de garantizar la seguridad y funcionalidad de los permisos: el analizador de acceso de IAM valida políticas nuevas y existentes para que respeten el lenguaje (JSON) de las políticas de IAM y las prácticas recomendadas de IAM. El analizador de acceso de IAM proporciona más de 100 verificaciones de políticas y recomendaciones procesables para ayudar a crear políticas seguras y funcionales. Para más información, consulte Validación de políticas con el Analizador de acceso de IAM en la Guía del usuario de IAM.
- Requerir autenticación multifactor (MFA): si tiene un escenario que requiere usuarios de IAM o un usuario raíz en Cuenta de AWS su cuenta, active la MFA para mayor seguridad. Para exigir la MFA cuando se invoquen las operaciones de la API, añada condiciones de MFA a sus políticas. Para más información, consulte Acceso seguro a la API con MFA en la Guía del usuario de IAM.

Para obtener más información sobre las prácticas recomendadas de IAM, consulte Prácticas recomendadas de seguridad en IAM en la Guía del usuario de IAM.

Ejemplo: uso de permisos de nivel de recursos

El siguiente ejemplo utiliza permisos a nivel de recursos para conceder permisos, con el fin de obtener información acerca del Outpost especificado.

```
{
```

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

El siguiente ejemplo utiliza permisos de nivel de recurso para conceder permiso para obtener información acerca del sitio especificado.

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

Funciones vinculadas al servicio para AWS Outposts

AWS Outposts usa roles vinculados al AWS Identity and Access Management servicio (IAM). Un rol vinculado a un servicio es un tipo de rol de servicio al que se vincula directamente. AWS Outposts AWS Outposts define los roles vinculados al servicio e incluye todos los permisos necesarios para llamar a otros AWS servicios en su nombre.

Un rol vinculado a un servicio hace que la configuración sea AWS Outposts más eficiente, ya que no es necesario añadir manualmente los permisos necesarios. AWS Outposts define los permisos de sus funciones vinculadas al servicio y, a menos que se defina lo contrario, solo AWS Outposts puede asumir sus funciones. Los permisos definidos incluyen las políticas de confianza y de permisos, y que la política de permisos no se puede asociar a ninguna otra entidad de IAM.

Solo puede eliminar un rol vinculado a servicios después de eliminar los recursos relacionados. Esto protege sus AWS Outposts recursos porque no puede eliminar inadvertidamente el permiso de acceso a los recursos.

Permisos de rol vinculados al servicio para AWS Outposts

AWS Outposts usa el rol vinculado al servicio denominado AWSService RoleForOutposts _. ***OutpostID*** Esta función otorga a Outposts permisos para gestionar los recursos de red a fin de habilitar la conectividad privada en tu nombre. Esta función también permite a Outposts crear y configurar interfaces de red, gestionar grupos de seguridad y adjuntar interfaces a instancias de punto final de enlace de servicio. Estos permisos son necesarios para establecer y mantener una conexión privada y segura entre tu Outpost local y los AWS servicios, lo que garantiza un funcionamiento fiable de tu implementación de Outpost.

El rol AWSService RoleForOutposts _ *OutpostID* vinculado al servicio confía en los siguientes servicios para asumir el rol:

- `outposts.amazonaws.com`

Políticas de funciones vinculadas al servicio

El rol AWSService RoleForOutposts _ *OutpostID* vinculado al servicio incluye las siguientes políticas:

- AWSOutpostsServiceRolePolicy
- AWSOutpostsPrivateConnectivityPolicy_*OutpostID*

AWSOutpostsServiceRolePolicy

La `AWSOutpostsServiceRolePolicy` política permite el acceso a AWS los recursos gestionados por. AWS Outposts

Esta política permite AWS Outposts realizar las siguientes acciones en los recursos especificados:

- Acción: `ec2:DescribeNetworkInterfaces` en todos los AWS recursos
- Acción: `ec2:DescribeSecurityGroups` sobre todos los AWS recursos
- Acción: `ec2:DescribeSubnets` sobre todos los AWS recursos
- Acción: `ec2:DescribeVpcEndpoints` sobre todos los AWS recursos
- Acción: `ec2:CreateNetworkInterface` sobre los siguientes AWS recursos:

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

```
"arn:*:ec2:*:*:security-group/*"
```

- Acción: `ec2:CreateNetworkInterface` en el AWS recurso `"arn:*:ec2:*:*:network-interface/*"` que cumpla la siguiente condición:

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

- Acción: `ec2:CreateSecurityGroup` en los siguientes AWS recursos:

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

- Acción: `ec2:CreateSecurityGroup` en el AWS recurso `"arn:*:ec2:*:*:security-group/*"` que cumpla la siguiente condición:

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

AWSOutpostsPrivateConnectivityPolicy_OutpostID

La `AWSOutpostsPrivateConnectivityPolicy_OutpostID` política permite AWS Outposts realizar las siguientes acciones en los recursos especificados:

- Acción: `ec2:AuthorizeSecurityGroupIngress` en todos los AWS recursos que cumplan la siguiente condición:

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

- Acción: `ec2:AuthorizeSecurityGroupEgress` en todos los AWS recursos que cumplan la siguiente condición:

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

- Acción: `ec2:CreateNetworkInterfacePermission` en todos los AWS recursos que cumplan la siguiente condición:

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

- Acción: `ec2:CreateTags` en todos los AWS recursos que cumplan la siguiente condición:

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

- Acción: `ec2:RevokeSecurityGroupIngress` en todos los AWS recursos que cumplan la siguiente condición:

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

- Acción: `ec2:RevokeSecurityGroupEgress` en todos los AWS recursos que cumplan la siguiente condición:

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

- Acción: `ec2:DeleteNetworkInterface` en todos los AWS recursos que cumplan la siguiente condición:

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

- Acción: `ec2:DeleteSecurityGroup` en todos los AWS recursos que cumplan la siguiente condición:

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

Debe configurar permisos para permitir a una entidad de IAM (como un usuario, grupo o rol) crear, editar o eliminar un rol vinculado a servicios. Para obtener más información, consulte Permisos de roles vinculados a servicios en la Guía del usuario de IAM.

Cree un rol vinculado a un servicio para AWS Outposts

No necesita crear manualmente un rol vinculado a servicios. Cuando configuras la conectividad privada para tu Outpost en AWS Management Console, AWS Outposts crea automáticamente el rol vinculado al servicio.

Para obtener más información, consulte Opciones de conectividad privada de Service Link.

Edita un rol vinculado a un servicio para AWS Outposts

AWS Outposts no permite editar el rol AWSService RoleForOutposts _ vinculado al *OutpostID* servicio. Después de crear un rol vinculado a un servicio, no puede cambiarle el nombre, ya que varias entidades pueden hacer referencia a él. Sin embargo, puede editar la descripción del rol mediante IAM. Para obtener más información, consulte Actualizar un rol vinculado a servicios en la Guía del usuario de IAM.

Elimine un rol vinculado a un servicio para AWS Outposts

Si ya no necesita utilizar una característica o servicio que requiere un rol vinculado a un servicio, le recomendamos que elimine dicho rol. De esta forma, evitará tener una entidad no utilizada que no se monitorice ni mantenga de forma activa. Sin embargo, debe limpiar los recursos de su rol vinculado al servicio antes de eliminarlo manualmente.

Si el AWS Outposts servicio utiliza el rol al intentar eliminar los recursos, es posible que la eliminación no se realice correctamente. En tal caso, espere unos minutos e intente de nuevo la operación.

Debes eliminar tu Outpost antes de poder eliminar el rol AWSService RoleForOutposts _ vinculado al *OutpostID* servicio.

Antes de empezar, asegúrate de que tu Outpost no se comparta mediante (). AWS Resource Access Manager AWS RAM Para obtener más información, consulta Dejar de compartir un recurso de Outpost compartido.

Para eliminar AWS Outposts los recursos utilizados por _ AWSService RoleForOutposts ***OutpostID***

Ponte en contacto con AWS Enterprise Support para eliminar tu Outpost.

Para eliminar manualmente el rol vinculado a servicios mediante IAM

Para obtener más información, consulte Eliminación de un rol vinculado a servicios en la Guía del usuario de IAM.

Regiones compatibles para los roles vinculados AWS Outposts al servicio

AWS Outposts admite el uso de funciones vinculadas al servicio en todas las regiones en las que el servicio está disponible. Para obtener más información, consulta los FAQs racks de Outposts.

AWS políticas gestionadas para AWS Outposts

Una política AWS administrada es una política independiente creada y administrada por. AWS AWS Las políticas administradas están diseñadas para proporcionar permisos para muchos casos de uso comunes, de modo que pueda empezar a asignar permisos a usuarios, grupos y funciones.

Ten en cuenta que es posible que las políticas AWS administradas no otorguen permisos con privilegios mínimos para tus casos de uso específicos, ya que están disponibles para que los usen todos los AWS clientes. Se recomienda definir políticas administradas por el cliente específicas para sus casos de uso a fin de reducir aún más los permisos.

No puedes cambiar los permisos definidos en AWS las políticas administradas. Si AWS actualiza los permisos definidos en una política AWS administrada, la actualización afecta a todas las identidades principales (usuarios, grupos y roles) a las que está asociada la política. AWS es más probable que actualice una política AWS administrada cuando Servicio de AWS se lance una nueva o cuando estén disponibles nuevas operaciones de API para los servicios existentes.

Para obtener más información, consulte Políticas administradas de AWS en la Guía del usuario de IAM.

AWS política gestionada: AWSOutposts ServiceRolePolicy

Esta política está asociada a un rol vinculado a un servicio que permite a AWS Outposts realizar acciones en tu nombre. Para obtener más información, consulte Roles vinculados a servicios.

AWS Outposts actualiza las políticas gestionadas AWS

Consulta los detalles sobre las actualizaciones de las políticas AWS gestionadas de AWS Outposts desde que este servicio comenzó a rastrear estos cambios.

Cambio	Descripción	Fecha
Actualizaciones del rol vinculado al servicio _ AWS Identity and Access Management AWSService RoleForOutposts *OutpostID*	Los permisos del rol AWSServiceRoleForOutposts_ ***OutpostID*** vinculado al servicio se actualizan para refinar la forma en que se AWS Outposts administr	18 de abril de 2025

Cambio	Descripción	Fecha
	an los recursos de red para la conectividad privada, y se necesitan controles más precisos sobre las operacion es de la interfaz de red y los grupos de seguridad para las instancias de punto final del enlace de servicio.	
AWS Outposts comenzó a rastrear los cambios	AWS Outposts comenzó a realizar un seguimiento de los cambios en sus políticas AWS gestionadas.	03 de diciembre de 2019

Seguridad de la infraestructura en AWS Outposts

Como servicio gestionado, AWS Outposts está protegido por la seguridad de la red AWS global. Para obtener información sobre los servicios AWS de seguridad y cómo se AWS protege la infraestructura, consulte Seguridad AWS en la nube. Para diseñar su AWS entorno utilizando las mejores prácticas de seguridad de la infraestructura, consulte Protección de infraestructuras en un marco de buena AWS arquitectura basado en el pilar de la seguridad.

Utilizas las llamadas a la API AWS publicadas para acceder a AWS Outposts a través de la red. Los clientes deben admitir lo siguiente:

- Seguridad de la capa de transporte (TLS). Exigimos TLS 1.2 y recomendamos TLS 1.3.
- Conjuntos de cifrado con confidencialidad directa total (PFS) como DHE (Ephemeral Diffie-Hellman) o ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos.

Además, las solicitudes deben estar firmadas mediante un ID de clave de acceso y una clave de acceso secreta que esté asociada a una entidad principal de IAM. También puedes utilizar AWS Security Token Service (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.

Para obtener más información sobre la seguridad de la infraestructura proporcionada para las EC2 instancias y los volúmenes de EBS que se ejecutan en su Outpost, consulte Infrastructure Security in Amazon. EC2

Los registros de flujo de VPC funcionan de la misma manera que en una AWS región. Esto significa que se pueden publicar en CloudWatch Logs, Amazon S3 o Amazon GuardDuty para su análisis. Los datos deben enviarse a la región para su publicación en estos servicios, de modo que no sean visibles desde CloudWatch otros servicios cuando el Outpost esté desconectado.

Supervisión de manipulaciones en los equipos AWS Outposts

Asegúrese de que nadie modifique, altere, realice ingeniería inversa ni manipule el equipo. AWS Outposts AWS Outposts el equipo puede estar equipado con un sistema de control de manipulaciones para garantizar el cumplimiento de las condiciones del servicio.AWS

Resiliencia en AWS Outposts

AWS Outposts está diseñado para ofrecer una alta disponibilidad. Los bastidores de Outposts están diseñados con equipos de red y alimentación redundantes. Para obtener una mayor resiliencia, le recomendamos que proporcione fuentes de alimentación duales y conectividad de red redundante para su Outpost.

Para una alta disponibilidad, puede aprovisionar capacidad adicional integrada y siempre activa en los bastidores de Outpost, . Las configuraciones de capacidad de Outpost están diseñadas para funcionar en entornos de producción y admiten instancias N+1 para cada familia de instancias cuando se aprovisiona la capacidad necesaria para ello. AWS recomienda asignar suficiente capacidad adicional para sus aplicaciones de misión crítica, a fin de permitir la recuperación y la conmutación por error si se produce un problema con el host subyacente. Puedes usar las métricas de disponibilidad de CloudWatch capacidad de Amazon y configurar alarmas para monitorear el estado de tus aplicaciones, crear CloudWatch acciones para configurar las opciones de recuperación automática y monitorear la utilización de la capacidad de tus Outposts a lo largo del tiempo.

Al crear un puesto de avanzada, se selecciona una zona de disponibilidad de una AWS región. Esta zona de disponibilidad admite operaciones del plano de control, como responder a las llamadas a la API, supervisar el Outpost y actualizar el Outpost. Para aprovechar la resiliencia que ofrecen las zonas de disponibilidad, puede implementar aplicaciones en varios Outposts, cada uno de ellos conectado a una zona de disponibilidad diferente. Esto le permite aumentar la resiliencia de las aplicaciones y evitar la dependencia de una única zona de disponibilidad. Para obtener

más información sobre las zonas de disponibilidad y las regiones de disponibilidad, consulte Infraestructura global de AWS.

Puede usar un grupo de ubicación con una estrategia de dispersión, a fin de asegurarse de que las instancias se coloquen en distintos bastidores de Outposts. De este modo, puede ayudar a reducir las fallas correlacionadas. Para obtener más información, consulte Grupos de ubicación en Outposts.

Puede lanzar instancias en Outposts con Amazon EC2 Auto Scaling y crear un Application Load Balancer para distribuir el tráfico entre las instancias. Para obtener más información, consulte Configurar un Equilibrador de carga de aplicación en AWS Outposts.

Validación de conformidad para AWS Outposts

Para saber si uno Servicio de AWS está dentro del ámbito de aplicación de programas de cumplimiento específicos, consulte Servicios de AWS Alcance por programa de cumplimiento Servicios de AWS de cumplimiento y elija el programa de cumplimiento que le interese. Para obtener información general, consulte Programas de AWS cumplimiento > Programas AWS .

Puede descargar informes de auditoría de terceros utilizando AWS Artifact. Para obtener más información, consulte Descarga de informes en AWS Artifact .

Su responsabilidad de cumplimiento al Servicios de AWS utilizarlos viene determinada por la confidencialidad de sus datos, los objetivos de cumplimiento de su empresa y las leyes y reglamentos aplicables. AWS proporciona los siguientes recursos para ayudar con el cumplimiento:

- Cumplimiento de seguridad y gobernanza: en estas guías se explican las consideraciones de arquitectura y se proporcionan pasos para implementar las características de seguridad y cumplimiento.
- Referencia de servicios válidos de HIPAA: muestra una lista con los servicios válidos de HIPAA. No todos Servicios de AWS cumplen con los requisitos de la HIPAA.
- AWS Recursos de de cumplimiento: esta colección de libros de trabajo y guías puede aplicarse a su industria y ubicación.
- AWS Guías de cumplimiento para clientes: comprenda el modelo de responsabilidad compartida desde el punto de vista del cumplimiento. Las guías resumen las mejores prácticas para garantizar la seguridad Servicios de AWS y orientan los controles de seguridad en varios marcos (incluidos el Instituto Nacional de Estándares y Tecnología (NIST), el Consejo de Normas de Seguridad del Sector de Tarjetas de Pago (PCI) y la Organización Internacional de Normalización (ISO)).

- Evaluación de los recursos con reglas en la guía para AWS Config desarrolladores: el AWS Config servicio evalúa en qué medida las configuraciones de los recursos cumplen con las prácticas internas, las directrices del sector y las normas.
- AWS Security Hub— Esto Servicio de AWS proporciona una visión completa del estado de su seguridad interior AWS. Security Hub utiliza controles de seguridad para evaluar sus recursos de AWS y comprobar su cumplimiento con los estándares y las prácticas recomendadas del sector de la seguridad. Para obtener una lista de los servicios y controles compatibles, consulte la Referencia de controles de Security Hub.
- Amazon GuardDuty: Servicio de AWS detecta posibles amenazas para sus cargas de trabajo Cuentas de AWS, contenedores y datos mediante la supervisión de su entorno para detectar actividades sospechosas y maliciosas. GuardDuty puede ayudarlo a cumplir con varios requisitos de conformidad, como el PCI DSS, al cumplir con los requisitos de detección de intrusiones exigidos por ciertos marcos de cumplimiento.
- AWS Audit Manager— Esto le Servicio de AWS ayuda a auditar continuamente su AWS uso para simplificar la gestión del riesgo y el cumplimiento de las normativas y los estándares del sector.

Acceso a Internet para cargas AWS Outposts de trabajo

En esta sección se explica cómo AWS Outposts las cargas de trabajo pueden acceder a Internet de las siguientes maneras:

- A través de la región principal AWS
- A través de la red de su centro de datos local

Acceso a Internet a través de la región de AWS principal

En esta opción, las cargas de trabajo de los Outposts acceden a Internet a través del enlace de servicio y, después, a través de la pasarela de Internet (IGW) de la región principal. AWS El tráfico saliente a Internet puede enrutarse a través de la instancia de puerta de enlace de NAT creada en su VPC. Para aumentar la seguridad del tráfico de entrada y salida, puede utilizar servicios de AWS seguridad como AWS WAF AWS Shield, y Amazon CloudFront in the AWS Region.

Para ver la configuración de la tabla de enrutamiento en la subred de Outposts, consulte Local gateway route tables.

Consideraciones

- Use esta opción cuando:
  - Necesita flexibilidad para proteger el tráfico de Internet con varios AWS servicios en la AWS región.
  - No tenga un punto de presencia de Internet en su centro de datos o centro de coubicación.
- En esta opción, el tráfico debe atravesar la AWS región principal, lo que introduce latencia.
- Al igual que ocurre con los cargos por transferencia de datos en AWS las regiones, la transferencia de datos desde la zona de disponibilidad principal al puesto avanzado conlleva gastos. Para obtener más información sobre la transferencia de datos, consulta los precios de Amazon EC2 On-Demand.
- La utilización del ancho de banda del enlace de servicio aumentará.

La siguiente imagen muestra el tráfico entre la carga de trabajo de la instancia de Outposts e Internet que pasa por la región principal AWS .

Acceso a Internet a través de la red de su centro de datos local

En esta opción, las cargas de trabajo que residen en los Outposts acceden a Internet a través de su centro de datos local. El tráfico de carga de trabajo que accede a Internet pasa por el punto de presencia local de Internet y sale localmente. La capa de seguridad de la red de su centro de datos local es responsable de proteger el tráfico de carga de trabajo de Outposts.

Para ver la configuración de la tabla de enrutamiento en la subred de Outposts, consulte Local gateway route tables.

Consideraciones

- Use esta opción cuando:
  - Sus cargas de trabajo requieren un acceso de baja latencia a los servicios de Internet.
  - Prefiere evitar incurrir en cargos por transferencia de datos saliente (DTO).
  - Desea conservar el ancho de banda del enlace de servicio para el tráfico del plano de control.
- Su capa de seguridad es responsable de proteger el tráfico de carga de trabajo de Outposts.
- Si optas por el enrutamiento directo de VPC (DVR), debes asegurarte de que los Outposts CIDRs no entren en conflicto con los locales. CIDRs

- Si la ruta predeterminada (0/0) se propaga a través de la puerta de enlace local (LGW), es posible que las instancias no puedan llegar a los puntos de conexión del servicio. Como alternativa, puede elegir puntos de conexión de VPC para acceder al servicio deseado.

La siguiente imagen muestra el tráfico entre la carga de trabajo de la instancia de Outposts e Internet que pasa por su centro de datos local.

Supervisión de bastidores de Outposts

AWS Outposts se integra con los siguientes servicios que ofrecen capacidades de monitoreo y registro:

CloudWatch métricas

Usa Amazon CloudWatch para recuperar estadísticas sobre puntos de datos para tu rack de Outposts como un conjunto ordenado de datos de series temporales, conocidos como métricas. Utilice estas métricas para comprobar que el sistema funciona de acuerdo con lo esperado. Para obtener más información, consulte CloudWatch .

CloudTrail registros

Se utiliza AWS CloudTrail para capturar información detallada sobre las llamadas realizadas a AWS APIs. Puede almacenar estas llamadas como archivos de registro en Amazon S3. Puede usar estos CloudTrail registros para determinar información como qué llamada se realizó, la dirección IP de origen de la llamada, quién hizo la llamada y cuándo se realizó la llamada.

Los CloudTrail registros contienen información sobre las llamadas a las acciones de la API AWS Outposts. También contienen información sobre las llamadas a las acciones de la API desde los servicios de un Outpost, como Amazon EC2 y Amazon EBS. Para obtener más información, consulte Registra las llamadas a la API mediante CloudTrail.

Logs de flujo de VPC

Utilice registros de flujo de VPC para capturar información detallada sobre el tráfico entrante y saliente del Outpost y dentro de su Outpost. Para obtener más información, consulte Logs de flujo de VPC en la Guía del usuario de Amazon VPC.

Replicación de tráfico

Usa Traffic Mirroring para copiar y reenviar el tráfico de red desde tu rack de Outposts a dispositivos de out-of-band seguridad y monitoreo. Puede utilizar el tráfico reflejado para inspeccionar el contenido, supervisar las amenazas o solucionar problemas. Para obtener más información, consulte la Guía de creación de reflejo de tráfico de Amazon VPC.

AWS Health Dashboard

AWS Health Dashboard Muestra información y notificaciones iniciadas por cambios en el estado de los recursos. AWS La información se presenta de dos formas: en un panel donde se muestran

los eventos recientes y próximos organizados por categorías, y en un registro de eventos que contiene todos los eventos de los últimos 90 días. Por ejemplo, un problema de conectividad en el enlace del servicio iniciaría un evento que aparecería en el panel y en el registro de eventos, y permanecería en el registro de eventos durante 90 días. Como parte del AWS Health servicio, no AWS Health Dashboard requiere configuración y puede verlo cualquier usuario que esté autenticado en su cuenta. Para obtener más información, consulte Introducción a AWS Health Dashboard.

CloudWatch

AWS Outposts publica puntos de datos en Amazon CloudWatch para tus Outposts. CloudWatch le permite recuperar estadísticas sobre esos puntos de datos como un conjunto ordenado de datos de series temporales, conocidos como métricas. Una métrica es una variable que hay que monitorizar y los puntos de datos son los valores de esa variable a lo largo del tiempo. Por ejemplo, puede supervisar la capacidad de instancias disponible para su Outpost durante un período de tiempo específico. Cada punto de datos tiene una marca temporal asociada y una unidad de medida opcional.

Puede utilizar estas métricas para comprobar si el sistema funciona de acuerdo con lo esperado. Por ejemplo, puede crear una CloudWatch alarma para supervisar la `ConnectedStatus` métrica. Si la métrica media es inferior a1, CloudWatch puede iniciar una acción, como enviar una notificación a una dirección de correo electrónico. A continuación, puede investigar los posibles problemas de red en las instalaciones o de enlace ascendente que podrían estar afectando a las operaciones de su Outpost. Entre los problemas más comunes se incluyen los cambios recientes en la configuración de la red en las instalaciones en las reglas de firewall y NAT, o los problemas de conexión a Internet. En caso de `ConnectedStatus` problemas, te recomendamos comprobar la conectividad con la AWS región desde tu red local y ponerte en contacto con AWS Support si el problema persiste.

Para obtener más información sobre cómo crear una CloudWatch alarma, consulta Uso de Amazon CloudWatch Alarms en la Guía del CloudWatch usuario de Amazon. Para obtener más información CloudWatch, consulta la Guía del CloudWatch usuario de Amazon.

Contenido

Métricas

El espacio de nombres de `AWS/Outposts` incluye las siguientes métricas.

`ConnectedStatus`

El estado de la conexión de enlace de servicio de un Outpost. Si la estadística media es inferior a `1`, la conexión está dañada.

Unidad: recuento

Resolución máxima: 1 minuto

Estadísticas: la estadística más útil es `Average`.

Dimensiones: `OutpostId`

`CapacityExceptions`

El número de errores de capacidad insuficiente para los lanzamientos de instancias.

Unidad: recuento

Resolución máxima: 5 minutos

Estadísticas: las estadísticas más útiles son `Maximum` y `Minimum`.

Dimensiones: `InstanceType` y `OutpostId`

`IfTrafficIn`

La tasa de bits de los datos que las interfaces virtuales de Outposts VIFs () reciben de los dispositivos de la red local conectados.

Unidad: bits por segundo

Resolución máxima: 5 minutos

Estadísticas: las estadísticas más útiles son `Max` y `Min`.

Dimensiones de la puerta de enlace local VIFs (lgw-vif):, y `OutpostsId` `VirtualInterfaceGroupId` `VirtualInterfaceId`

Dimensiones del enlace de servicio VIFs (sl-vif): y `OutpostsId` `VirtualInterfaceId`

`IfTrafficOut`

La velocidad de bits de los datos que las interfaces virtuales de Outposts VIFs () transfieren a los dispositivos de la red local conectados.

Unidad: bits por segundo

Resolución máxima: 5 minutos

Estadísticas: las estadísticas más útiles son `Max` y `Min`.

Dimensiones de la puerta de enlace local VIFs (lgw-vif):, y `OutpostsId` `VirtualInterfaceGroupId` `VirtualInterfaceId`

Dimensiones del enlace de servicio VIFs (sl-vif): y `OutpostsId` `VirtualInterfaceId`

`InstanceFamilyCapacityAvailability`

El porcentaje de capacidad de instancia disponible. Esta métrica no incluye la capacidad de ningún host dedicado configurado en el Outpost.

Unidad: porcentaje

Resolución máxima: 5 minutos

Estadísticas: las estadísticas más útiles son `Average` y `pNN.NN` (percentiles).

Dimensiones: `InstanceFamily` y `OutpostId`

`InstanceFamilyCapacityUtilization`

El porcentaje de capacidad de instancia en uso. Esta métrica no incluye la capacidad de ningún host dedicado configurado en el Outpost.

Unidad: porcentaje

Resolución máxima: 5 minutos

Estadísticas: las estadísticas más útiles son `Average` y `pNN.NN` (percentiles).

Dimensiones: `Account`, `InstanceFamily` y `OutpostId`

`InstanceTypeCapacityAvailability`

El porcentaje de capacidad de instancia disponible. Esta métrica no incluye la capacidad de ningún host dedicado configurado en el Outpost.

Unidad: porcentaje

Resolución máxima: 5 minutos

Estadísticas: las estadísticas más útiles son `Average` y `pNN.NN` (percentiles).

Dimensiones: `InstanceType` y `OutpostId`

`InstanceTypeCapacityUtilization`

El porcentaje de capacidad de instancia en uso. Esta métrica no incluye la capacidad de ningún host dedicado configurado en el Outpost.

Unidad: porcentaje

Resolución máxima: 5 minutos

Estadísticas: las estadísticas más útiles son `Average` y `pNN.NN` (percentiles).

Dimensiones: `Account`, `InstanceType` y `OutpostId`

`UsedInstanceType_Count`

El número de tipos de instancias que se utilizan actualmente, incluido cualquier tipo de instancia que utilicen los servicios gestionados, como Amazon Relational Database Service (Amazon RDS) o Equilibrador de carga de aplicación. Esta métrica no incluye la capacidad de ningún host dedicado configurado en el Outpost.

Unidad: recuento

Resolución máxima: 5 minutos

Dimensiones: `Account`, `InstanceType` y `OutpostId`

`AvailableInstanceType_Count`

El número de tipos de instancias disponibles. Esta métrica incluye el recuento de `AvailableReservedInstances`.

Para determinar el número de instancias que puede reservar, reste el recuento de `AvailableReservedInstances` del recuento de `AvailableInstanceType_Count`.

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

Esta métrica no incluye la capacidad de ningún host dedicado configurado en el Outpost.

Unidad: recuento

Resolución máxima: 5 minutos

Dimensiones: `InstanceType` y `OutpostId`

`AvailableReservedInstances`

El número de instancias que están disponibles para su lanzamiento en la capacidad de computación reservada mediante reservas de capacidad.

Esta métrica no incluye las instancias EC2 reservadas de Amazon.

Esta métrica no incluye el número de instancias que puede reservar. Para determinar el número de instancias que puede reservar, reste el recuento de `AvailableReservedInstances` del recuento de `AvailableInstanceType_Count`.

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

Unidad: recuento

Resolución máxima: 5 minutos

Dimensiones: `InstanceType` y `OutpostId`

`UsedReservedInstances`

El número de instancias que se están ejecutando en la capacidad de computación reservada mediante reservas de capacidad. Esta métrica no incluye las instancias EC2 reservadas de Amazon.

Unidad: recuento

Resolución máxima: 5 minutos

Dimensiones: `InstanceType` y `OutpostId`

`TotalReservedInstances`

El número total de instancias, en ejecución y disponibles para su lanzamiento, proporcionado por la capacidad de computación reservada mediante reservas de capacidad. Esta métrica no incluye las instancias EC2 reservadas de Amazon.

Unidad: recuento

Resolución máxima: 5 minutos

Dimensiones: `InstanceType` y `OutpostId`

`EBSVolumeTypeCapacityUtilization`

El porcentaje de capacidad del tipo de volumen de EBS en uso.

Unidad: porcentaje

Resolución máxima: 5 minutos

Estadísticas: las estadísticas más útiles son `Average` y `pNN.NN` (percentiles).

Dimensiones: `VolumeType` y `OutpostId`

`EBSVolumeTypeCapacityAvailability`

El porcentaje de capacidad del tipo de volumen de EBS disponible.

Unidad: porcentaje

Resolución máxima: 5 minutos

Estadísticas: las estadísticas más útiles son `Average` y `pNN.NN` (percentiles).

Dimensiones: `VolumeType` y `OutpostId`

`EBSVolumeTypeCapacityUtilizationGB`

El número de gigabytes que se utilizan para el tipo de volumen de EBS.

Unidad: Gigabyte

Resolución máxima: 5 minutos

Estadísticas: las estadísticas más útiles son `Average` y `pNN.NN` (percentiles).

Dimensiones: `VolumeType` y `OutpostId`

`EBSVolumeTypeCapacityAvailabilityGB`

El número de gigabytes de capacidad disponible para el tipo de volumen de EBS.

Unidad: Gigabyte

Resolución máxima: 5 minutos

Estadísticas: las estadísticas más útiles son `Average` y `pNN.NN` (percentiles).

Dimensiones: `VolumeType` y `OutpostId`

Dimensiones de la métrica

Para filtrar las métricas de su Outpost, utilice las siguientes dimensiones.

Dimensión	Descripción
`Account`	La cuenta o el servicio que utiliza la capacidad.
`InstanceFamily`	La familia de instancias.
`InstanceType`	El tipo de instancia.
`OutpostId`	El ID del Outpost.
`VolumeType`	El tipo de volumen EBS.
`VirtualInterfaceId`	El ID de la puerta de enlace local o de la interfaz virtual (VIF) del enlace de servicio.
`VirtualInterfaceGroupId`	El ID del grupo de interfaces virtuales de la interfaz virtual (VIF) de la puerta de enlace local.

Puedes ver las CloudWatch métricas de tu rack de Outposts mediante la CloudWatch consola.

Para ver las métricas mediante la consola CloudWatch

1. Abra la CloudWatch consola en https://console.aws.amazon.com/cloudwatch/.
2. En el panel de navegación, seleccione Métricas.
3. Selecciona el espacio de nombres de Outposts.
4. (Opcional) Para ver una métrica en todas las dimensiones, ingrese su nombre en el campo de búsqueda.

Para ver las métricas mediante el AWS CLI

Utilice el siguiente comando list-metrics para obtener una lista de las métricas disponibles.

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

Para obtener las estadísticas de una métrica mediante el AWS CLI

Utilice el siguiente get-metric-statisticscomando para obtener las estadísticas de la métrica y la dimensión especificadas. CloudWatch trata cada combinación única de dimensiones como una métrica independiente. No se pueden recuperar estadísticas utilizando combinaciones de dimensiones que no se han publicado expresamente. Debe especificar las mismas dimensiones que se utilizaron al crear las métricas.

```
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
```

Registre las llamadas a la AWS Outposts API mediante AWS CloudTrail

AWS Outposts está integrado con AWS CloudTrail un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o un AWS servicio. CloudTrail captura las llamadas a la API AWS Outposts como eventos. Las llamadas capturadas incluyen llamadas desde la AWS Outposts consola y llamadas en código a las operaciones de la AWS Outposts API. Con la información recopilada por CloudTrail, puede determinar a qué solicitud se realizó AWS Outposts, la dirección IP desde la que se realizó la solicitud, cuándo se realizó y detalles adicionales.

Cada entrada de registro o evento contiene información sobre quién generó la solicitud. La información de identidad del usuario le ayuda a determinar lo siguiente:

- Si la solicitud se realizó con las credenciales del usuario raíz o del usuario.
- Si la solicitud se realizó en nombre de un usuario de IAM Identity Center.
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado.

- Si la solicitud la realizó otro Servicio de AWS.

CloudTrail está activa en tu AWS cuenta cuando la creas y tienes acceso automáticamente al historial de CloudTrail eventos. El historial de CloudTrail eventos proporciona un registro visible, consultable, descargable e inmutable de los últimos 90 días de eventos de gestión registrados en un. Región de AWSPara obtener más información, consulte Uso del historial de CloudTrail eventos en la Guía del usuario.AWS CloudTrail La visualización del historial de eventos no conlleva ningún CloudTrail cargo.

Para tener un registro continuo de los eventos de Cuenta de AWS los últimos 90 días, crea un almacén de datos de eventos de senderos o CloudTrail lagos.

CloudTrail senderos

Un rastro permite CloudTrail entregar archivos de registro a un bucket de Amazon S3. Todos los senderos creados con él AWS Management Console son multirregionales. Puede crear un registro de seguimiento de una sola región o multirregionales mediante la AWS CLI. Se recomienda crear un sendero multirregional, ya que puedes capturar toda la actividad de tu Regiones de AWS cuenta. Si crea un registro de seguimiento de una sola región, solo podrá ver los eventos registrados en la Región de AWS del registro de seguimiento. Para obtener más información acerca de los registros de seguimiento, consulte Creación de un registro de seguimiento para su Cuenta de AWS y Creación de un registro de seguimiento para una organización en la Guía del usuario de AWS CloudTrail .

Puede enviar una copia de sus eventos de administración en curso a su bucket de Amazon S3 sin coste alguno CloudTrail mediante la creación de una ruta; sin embargo, hay cargos por almacenamiento en Amazon S3. Para obtener más información sobre CloudTrail los precios, consulte AWS CloudTrail Precios. Para obtener información acerca de los precios de Amazon S3, consulte Precios de Amazon S3.

CloudTrail Almacenes de datos de eventos en Lake

CloudTrail Lake le permite ejecutar consultas basadas en SQL en sus eventos. CloudTrail Lake convierte los eventos existentes en formato JSON basado en filas al formato Apache ORC. ORC es un formato de almacenamiento en columnas optimizado para una recuperación rápida de datos. Los eventos se agregan en almacenes de datos de eventos, que son recopilaciones inmutables de eventos en función de criterios que se seleccionan aplicando selectores de eventos avanzados. Los selectores que se aplican a un almacén de datos de eventos controlan los eventos que perduran y están disponibles para la consulta. Para obtener más información sobre

CloudTrail Lake, consulte Cómo trabajar con AWS CloudTrail Lake en la Guía del AWS CloudTrail usuario.

CloudTrail Los almacenes de datos y las consultas sobre eventos de Lake conllevan costes. Cuando crea un almacén de datos de eventos, debe elegir la opción de precios que desee utilizar para él. La opción de precios determina el costo de la incorporación y el almacenamiento de los eventos, así como el período de retención predeterminado y máximo del almacén de datos de eventos. Para obtener más información sobre CloudTrail los precios, consulte AWS CloudTrail Precios.

AWS Outposts eventos de gestión en CloudTrail

Los eventos de administración proporcionan información sobre las operaciones de administración que se llevan a cabo en los recursos de su empresa Cuenta de AWS. Se denominan también operaciones del plano de control. De forma predeterminada, CloudTrail registra los eventos de administración.

AWS Outposts registra todas las operaciones del plano de control de AWS Outposts como eventos de gestión. Para obtener una lista de las operaciones del plano de control de AWS Outposts en las que AWS Outposts inicia sesión, CloudTrail consulta la Referencia de la API de AWS Outposts.

AWS Outposts ejemplos de eventos

El siguiente ejemplo muestra un CloudTrail evento que demuestra la `SetSiteAddress` operación.


```
{
    "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"
}
```

Mantenimiento de bastidores de Outposts

Según el modelo de responsabilidad compartida de AWS es responsable del hardware y el software que ejecutan AWS los servicios. Esto se aplica a una AWS región AWS Outposts, igual que a ella. Por ejemplo, AWS administra los parches de seguridad, actualiza el firmware y mantiene el equipo de Outpost. AWS también supervisa el rendimiento, el estado y las métricas de su rack Outposts y determina si es necesario realizar algún tipo de mantenimiento.

> **Warning**
>
> Los datos de los volúmenes del almacén de instancias se pierden si la unidad de disco subyacente falla o si la instancia se detiene, hiberna o finaliza. Para evitar la pérdida de datos, le recomendamos que guarde copias de seguridad de los datos a largo plazo de los volúmenes del almacén de instancias en un almacenamiento persistente, como un bucket de Amazon S3, un volumen de Amazon EBS o un dispositivo de almacenamiento en red de su red en las instalaciones.

Contenido

Actualización de los datos de contacto

Si el propietario de Outpost cambia, comuníquese con AWS Support Center para facilitarles el nombre y la información de contacto del nuevo propietario.

Mantenimiento del hardware

Si AWS detecta un problema irreparable con el hardware durante el proceso de aprovisionamiento del servidor o al alojar EC2 instancias de Amazon que se ejecutan en su rack de Outposts,

notificaremos al propietario de Outpost y al propietario de las instancias que las instancias afectadas están programadas para su retirada. Para obtener más información, consulte Retirada de instancias en la Guía del EC2 usuario de Amazon.

El propietario de Outpost y el propietario de la instancia pueden trabajar juntos para resolver el problema. El propietario de la instancia puede detener e iniciar una instancia afectada para migrarla a la capacidad disponible. Los propietarios de las instancias pueden detener e iniciar las instancias afectadas en el momento que les resulte más conveniente. De lo contrario, AWS detiene e inicia las instancias afectadas en la fecha de retirada de la instancia. Si no hay capacidad adicional en el Outpost, la instancia permanece detenida. A fin de poder completar la migración, el propietario del Outpost puede intentar liberar la capacidad utilizada o solicitar capacidad adicional para el Outpost.

Si se requiere mantenimiento del hardware, se AWS pondrá en contacto con el propietario de Outpost para confirmar la fecha y la hora de la visita del equipo de AWS instalación. Las visitas se pueden programar en un plazo máximo de dos días laborables a partir del momento en que el propietario del Outpost hable con el equipo de AWS .

Cuando el equipo de AWS instalación llegue a las instalaciones, sustituirá los hosts, conmutadores o elementos del rack que no estén funcionando correctamente y pondrá en funcionamiento la nueva capacidad. El equipo no realizará ningún diagnóstico ni reparación del hardware in situ. Si sustituye un host, quitará y destruirá la clave de seguridad física conforme con la norma NIST, y destruirá cualquier dato que pudiera permanecer en el hardware. Esto garantiza que ningún dato salga de su sitio. Si el equipo sustituye un dispositivo de red de Outpost, es posible que la información de configuración de la red esté presente en el dispositivo cuando se elimine del sitio. Esta información puede incluir direcciones IP y ASNs usarse para establecer interfaces virtuales para configurar la ruta a la red local o de regreso a la región.

Actualizaciones de firmware

La actualización del firmware de Outpost no suele afectar a las instancias de su Outpost. En el raro caso de que necesitemos reiniciar el equipo de Outpost para instalar una actualización, recibirá un aviso de retirada de todas las instancias que se ejecuten en esa capacidad.

Mantenimiento del equipo de red

El mantenimiento de los dispositivos de red de Outpost (OND) se realiza sin afectar las operaciones y el tráfico habituales del Outpost. Si es necesario realizar tareas de mantenimiento, el tráfico se aleja del OND. Es posible que observe cambios temporales en los anuncios de BGP, como el

AS-Path Prepending y los correspondientes cambios en los patrones de tráfico en los enlaces ascendentes del Outpost. Con las actualizaciones de firmware de OND, es posible que note que el BGP sufre interrupciones.

Le recomendamos que configure el equipo de red del cliente para recibir anuncios de BGP de Outposts sin cambiar los atributos de BGP y que habilite el equilibrador de multiruta y de carga del BGP para lograr flujos de tráfico entrante óptimos. El prefijo AS-Path se utiliza en los prefijos de las puertas de enlace locales para desviar el tráfico ONDs si es necesario realizar tareas de mantenimiento. La red de clientes debería preferir las rutas de Outposts con una longitud de AS-Path de 1 a las rutas con una longitud de AS-Path de 4.

La red del cliente debe anunciar a todas ellas prefijos BGP iguales con los mismos atributos. ONDs El equilibrador de carga de red de Outpost equilibra el tráfico saliente entre todos los enlaces ascendentes de forma predeterminada. Las políticas de enrutamiento se utilizan en el Outpost para desviar el tráfico de un OND si es necesario realizar tareas de mantenimiento. Este cambio de tráfico requiere que todos los clientes tengan los mismos prefijos de BGP. ONDs Si es necesario realizar tareas de mantenimiento en la red del cliente, le recomendamos que utilice AS-Path para desplazar temporalmente la matriz de tráfico desde enlaces ascendentes específicos.

Mejores prácticas para eventos de alimentación y red de

Como se indica en los Términos de AWS servicio para AWS Outposts los clientes, la instalación donde se encuentra el equipo de Outposts debe cumplir con los requisitos mínimos de energía y red para respaldar la instalación, el mantenimiento y el uso del equipo de Outposts. Un servidor en de Outposts solo puede funcionar correctamente cuando la alimentación y la conectividad de red no sufren interrupciones.

Eventos de alimentación

En caso de cortes de energía totales, existe el riesgo inherente de que un AWS Outposts recurso no vuelva a funcionar automáticamente. Además de desplegar soluciones de alimentación redundante y de respaldo, le recomendamos que haga lo siguiente con antelación para mitigar el impacto de algunos de los peores escenarios posibles:

- Retire sus servicios y aplicaciones de los equipos de Outposts de forma controlada mediante cambios en el equilibrador de carga basados en DNS o fuera del bastidor.
- Detenga los contenedores, las instancias y las bases de datos de forma ordenada e incremental, y utilice el orden inverso al restaurarlos.

- Pruebe los planes para el traslado o la detención controlados de los servicios.
- Realice copias de seguridad de los datos y configuraciones de relevancia y guárdelos fuera de los Outposts.
- Mantenga los tiempos de inactividad del suministro de alimentación al mínimo.
- Evite cambiar repetidamente las fuentes de alimentación (off-on-off-on) durante el mantenimiento.
- Prevea tiempo adicional dentro del período de mantenimiento para hacer frente a cualquier imprevisto.
- Gestione las expectativas de sus usuarios y clientes comunicando un plazo de mantenimiento más amplio del que normalmente necesitaría.
- Cuando se restablezca la alimentación, cree una caja en el AWS Support Centro para solicitar la verificación de que los servicios relacionados AWS Outposts y los servicios relacionados están funcionando.

Eventos de conectividad de red

La conexión de enlace de servicio entre tu Outpost y la AWS región o región de origen de Outposts normalmente se recuperará automáticamente de las interrupciones o problemas de red que puedan producirse en los dispositivos de la red corporativa principal o en la red de cualquier proveedor de conectividad externo una vez que se complete el mantenimiento de la red. Durante el tiempo en que la conexión del enlace de servicio esté inactiva, sus operaciones de Outposts se limitarán a las actividades de la red local.

EC2 Las instancias de Amazon, la puerta de enlace local y los volúmenes de Amazon EBS de los Outposts seguirán funcionando con normalidad y se podrá acceder a ellos de forma local a través de la red local. Del mismo modo, los recursos de AWS servicio, como los nodos de trabajo de Amazon ECS, siguen ejecutándose localmente. Sin embargo, la disponibilidad de la API disminuirá. Por ejemplo, es posible que las funciones ejecutar, iniciar, detener y terminar no APIs funcionen. Las métricas y los registros de las instancias seguirán almacenándose en caché local durante un máximo de 7 días y se transferirán a la AWS región cuando se restablezca la conectividad. Si se desconecta durante más de 7 días, es posible que se pierdan métricas y registros.

Para obtener más información, consulta la pregunta ¿Qué ocurre cuando se interrumpe la conexión de red de mi centro? en la AWS Outposts FAQspágina principal.

Si el enlace de servicio no funciona debido a un problema de energía in situ o a una pérdida de conectividad de red, AWS Health Dashboard envía una notificación a la cuenta propietaria de los

Outposts. Ni tú ni tú AWS podéis suprimir la notificación de una interrupción del enlace de servicio, incluso si la interrupción es esperada. Para obtener más información, consulte Introducción a su AWS Health Dashboard en la Guía del usuario de AWS Health .

En el caso de un mantenimiento planificado del servicio que afecte a la conectividad de la red, tome las siguientes medidas proactivas para limitar el impacto de posibles escenarios problemáticos:

- Si tu rack de Outposts se conecta a la AWS región principal a través de Internet o Direct Connect público, captura una ruta de rastreo antes del mantenimiento planificado. Disponer de una ruta de red que funcione (pre-network-maintenance) y una ruta de red problemática (post-network-maintenance) para identificar las diferencias ayudaría a solucionar el problema. Si planteas un problema posterior al mantenimiento AWS o a tu ISP, puedes incluir esta información.

  Capture una ruta de rastreo entre:

  - Las direcciones IP públicas de la ubicación de Outposts y la dirección IP devuelta por los `outposts.region.amazonaws.com`. *region*Sustitúyala por el nombre de la región principal. AWS
  - Cualquier instancia en la región principal con conectividad pública a Internet y las direcciones IP públicas en la ubicación de Outposts.
- Si tiene el control del mantenimiento de la red, limite la duración del tiempo de inactividad del enlace de servicio. Incluya un paso en el proceso de mantenimiento que verifique que la red se haya recuperado.
- Si no tiene el control del mantenimiento de la red, supervise el tiempo de inactividad del enlace de servicio con respecto al período de mantenimiento anunciado e infórmele cuanto antes a la parte encargada del mantenimiento planificado de la red si el enlace de servicio no vuelve a funcionar al final del período de mantenimiento anunciado.

Recursos

A continuación, se detallan algunos recursos relacionados con la supervisión que pueden garantizar que los Outposts estén funcionando normalmente después de un evento de alimentación o red planificado o no planificado:

- El AWS blog Monitoring best practices for AWS Outposts cubre las mejores prácticas de observabilidad y gestión de eventos específicas de Outposts.
- En el AWS blog Herramienta de depuración para conectividad de red de Amazon VPC se explica AWSSupport-SetupIPMonitoringFromVPCla herramienta. Esta herramienta es un AWS Systems

Manager documento (documento SSM) que crea una instancia de Amazon EC2 Monitor en una subred especificada por usted y monitorea las direcciones IP de destino. El documento ejecuta pruebas de diagnóstico de ruta de rastreo de ping, MTR, TCP y ruta de rastreo y almacena los resultados en Amazon CloudWatch Logs, que se pueden visualizar en un CloudWatch panel de control (por ejemplo, latencia o pérdida de paquetes). Para el monitoreo de Outposts, la instancia de monitoreo debe estar en una subred de la AWS región principal y estar configurada para monitorear una o más de tus instancias de Outpost utilizando sus IP privadas; esto proporcionará gráficos de pérdida de paquetes y latencia entre AWS Outposts la región principal y la región principal. AWS

- El AWS blog Cómo implementar un CloudWatch panel automatizado de Amazon para su AWS Outposts uso AWS CDK describe los pasos necesarios para implementar un panel automatizado.
- Si tiene preguntas o necesita más información, consulte Creating a support case en la Guía del usuario de AWS Support.

Opciones de estantes Outposts end-of-term

Al final de su AWS Outposts mandato, debe elegir entre las siguientes opciones:

- Renovar su suscripción y conservar sus bastidores Outposts actuales.
- Finalizar su suscripción y preparar sus bastidores de Outposts para su devolución.
- Conviértelo en una month-to-month suscripción y conserva tus racks de Outposts existentes.

Renovar la suscripción

Debe completar los siguientes pasos al menos 30 días antes de que finalice la suscripción actual de sus bastidores de Outposts.

Para renovar su suscripción y conservar sus bastidores de Outposts actuales:

1. Inicie sesión en la consola del AWS Support Center.
2. Elija Crear caso.
3. Elija Cuenta y facturación.
4. Para Servicio, elija Facturación.
5. Para Categoría, elija Otras preguntas sobre facturación.
6. Para Severidad, elija Pregunta importante.
7. Elija Siguiente paso: información adicional.
8. En la página Información adicional, para Asunto, introduzca su solicitud de renovación, por ejemplo **`Renew my Outpost subscription`**.
9. En Descripción, introduzca una de las siguientes opciones de pago:

   - Sin pago inicial
   - Pago inicial parcial
   - Pago inicial total

   Para obtener información acerca de los precios, consulte Precios de bastidores de AWS Outposts. También puede solicitar una cotización.
10. Elija Siguiente paso: Resuelva ahora o póngase en contacto con nosotros.
11. En la página Contacte con nosotros, elija su idioma preferido.

12. Cambie el método de contacto preferido.
13. Revise los detalles de su caso y elija Enviar. Aparecerán el número de ID del caso y el resumen.

AWS Customer Support iniciará el proceso de renovación de la suscripción. La nueva suscripción comenzará el día siguiente a la finalización de la suscripción actual.

Si no indicas que quieres renovar tu suscripción o devolver tu rack de Outposts, pasarás a ser una month-to-month suscripción automáticamente. Tu rack de Outposts se renovará mensualmente según la tarifa de la opción de pago sin anticipado que corresponda a tu configuración. AWS Outposts Su nueva suscripción mensual comenzará el día siguiente a la finalización de la suscripción actual.

Finalice su suscripción y prepare los bastidores para su devolución

Debes completar los siguientes pasos al menos 30 días antes de que finalice la suscripción actual de tu rack de Outposts. AWS no puedes iniciar el proceso de devolución hasta que lo hagas.

> **Important**
>
> AWS no puedes detener el proceso de devolución después de abrir un caso de soporte para finalizar tu suscripción.

Para finalizar su suscripción:

1. Inicie sesión en la consola del AWS Support Center.
2. Elija Crear caso.
3. Elija Cuenta y facturación.
4. Para Servicio, elija Facturación.
5. Para Categoría, elija Otras preguntas sobre facturación.
6. Para Severidad, elija Pregunta importante.
7. Elija Siguiente paso: información adicional.
8. En la página Información adicional, para Asunto, introduzca su solicitud de renovación, por ejemplo **`End my Outpost subscription`**.
9. Para Descripción, introduzca la fecha en la que prefiere que se recupere el Outpost.
10. Elija Siguiente paso: Resuelva ahora o póngase en contacto con nosotros.

11. En la página Contacte con nosotros, elija su idioma preferido.
12. Cambie el método de contacto preferido.
13. Revise los detalles de su caso y elija Enviar. Aparecerán el número de ID del caso y el resumen.

AWS Customer Support se pondrá en contacto con usted para coordinar la recuperación.

Para preparar sus AWS Outposts estanterías para la devolución:

> **Important**
>
> No apagues el rack de Outposts hasta que AWS esté in situ para la recuperación programada.

1. Si los recursos del Outpost se comparten, debe dejar de compartirlos.

   Puede dejar de compartir un recurso de Outpost compartido de una de las siguientes formas:

   - Usa la consola. AWS RAM Para obtener más información, consulte Actualizar un recurso compartido en la Guía del usuario de AWS RAM .
   - Utilice el AWS CLI para ejecutar el disassociate-resource-sharecomando.

   Para ver la lista de recursos de Outpost que se pueden compartir, consulte Recursos de Outpost que se pueden compartir.
2. Finalice las instancias activas asociadas a las subredes de su Outpost. Para finalizar las instancias, sigue las instrucciones de Termina tu instancia en la Guía del EC2 usuario de Amazon.

   > **Note**
   >
   > Algunos servicios AWS gestionados que se ejecutan en su Outpost, como los balanceadores de carga de aplicaciones o Amazon Relational Database Service (RDS), consumen capacidad. EC2 Sin embargo, sus instancias asociadas no están visibles en el EC2 panel de control de Amazon. Debe eliminar los recursos vinculados a estos servicios para liberar capacidad. Para obtener más información, consulta ¿Por qué falta capacidad de EC2 instancias en mi Outpost? .

3. Verifica instance-capacity-availability las EC2 instancias de Amazon de tu AWS cuenta.

   a. Abre la AWS Outposts consola en https://console.aws.amazon.com/outposts/.

   b. Elija Outposts.

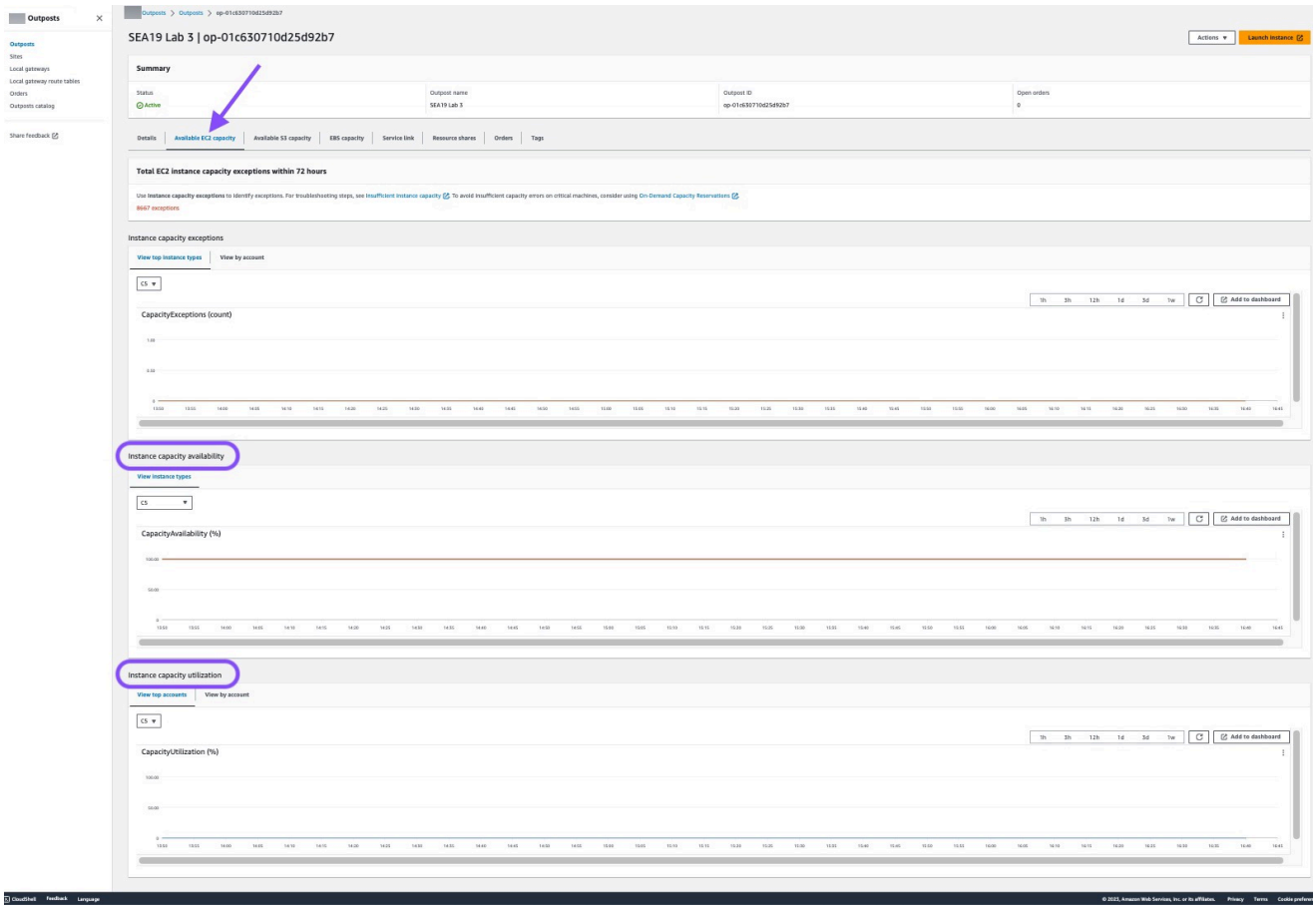
   c. Elija el Outpost específico que va a devolver.

   d. En la página del Outpost, selecciona la pestaña EC2 Capacidad disponible.

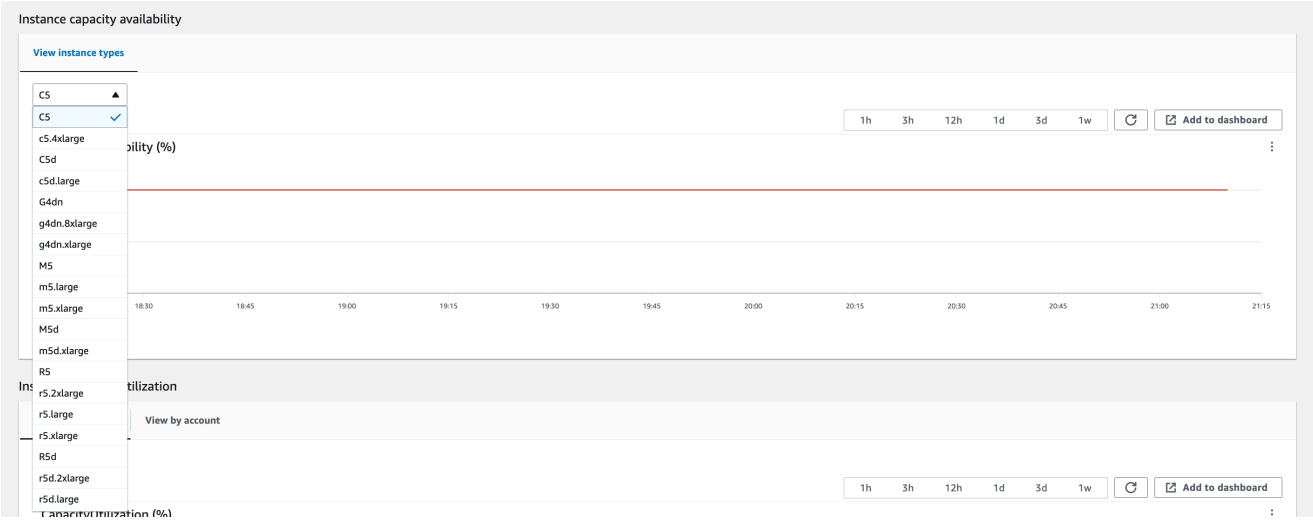
   e. Asegúrese de que la disponibilidad de la capacidad de las instancias sea del 100% para cada familia de instancias.

   f. Asegúrese de que la utilización de la capacidad de las instancias sea del 0% para cada familia de instancias.

   La siguiente imagen muestra los gráficos de disponibilidad de la capacidad de la instancia y utilización de la capacidad de la instancia en la pestaña EC2Capacidad disponible.



   En la imagen siguiente, se muestra la lista de tipos de instancias.



4. Cree copias de seguridad de sus EC2 instancias y volúmenes de servidores de Amazon. Para crear las copias de seguridad, siga las instrucciones de Backup and recovery for Amazon EC2 with EBS volumes de la guía AWS prescriptiva.
5. Elimine los volúmenes de Amazon EBS asociados a su Outpost.
   a. Abre la EC2 consola Amazon en https://console.aws.amazon.com/ec2/.
   b. En el panel de navegación, elija Volúmenes.
   c. Elija Acciones y Eliminar volúmenes.
   d. En el cuadro de diálogo de confirmación, elija Eliminar.
6. Si tiene Amazon S3 en los Outposts, elimine las instantáneas locales del Outposts.
   a. Abre la EC2 consola Amazon en https://console.aws.amazon.com/ec2/.
   b. En el panel de navegación, elija Instantáneas.
   c. Seleccione las instantáneas con un ARN de Outpost.
   d. Elija Acciones y Eliminar instantáneas.
   e. En el cuadro de diálogo de confirmación, elija Eliminar.
7. Elimine todos los buckets de Amazon S3 asociados a su bastidor de Outposts. Para eliminar los buckets, sigue las instrucciones de Eliminar tu bucket de Amazon S3 on Outposts en la guía del usuario de Amazon S3 on Outposts.
8. Elimine cualquier asociación de VPC y el conjunto de direcciones IP (CoIP) CIDRs propiedad del cliente asociado a su Outpost.

Un equipo de AWS recuperación apagará el rack. Cuando se apague, puedes destruir la llave de seguridad AWS Nitro o el equipo de AWS recuperación puede hacerlo en tu nombre.

Conviértelo en una suscripción month-to-month

Para convertirlos en una month-to-month suscripción y conservar tus racks de Outposts existentes, no es necesario realizar ninguna acción. Si tiene alguna pregunta, abra un caso de soporte de facturación.

Sus bastidores de Outposts se renovarán mensualmente según la tarifa de la opción de pago sin pago inicial que corresponda a su configuración de Outposts. Su nueva suscripción mensual comenzará el día siguiente a la finalización de la suscripción actual.

Cuotas para AWS Outposts

Cuenta de AWS Tiene cuotas predeterminadas, anteriormente denominadas límites, para cada uno de ellos Servicio de AWS. A menos que se indique lo contrario, cada cuota es específica de la región. Puede solicitar el aumento de algunas cuotas, pero no de todas.

Para ver las cuotas AWS Outposts, abra la consola Service Quotas. En el panel de navegación, elija Servicios de AWS y seleccione AWS Outposts.

Para solicitar un aumento de cuota, consulte Solicitud de un aumento de cuota en la Guía de usuario de Service Quotas.

Cuenta de AWS Tiene las siguientes cuotas relacionadas con AWS Outposts.

Recurso	Predeterminado	Ajustable	Comentarios
Sitios de Outpost	100	Sí	Un sitio de Outpost es el edificio físico administrado por el cliente donde se alimenta y se conecta el equipo de Outpost a la red. Puedes tener 100 sitios de Outposts en cada región de tu AWS cuenta.
Outposts por sitio	10	Sí	AWS Outposts incluye recursos virtuales y de hardware, conocidos como Outposts. Esta cuota limita los recursos virtuales de Outpost. Puede tener 10 Outposts en cada sitio de Outpost.

AWS Outposts y las cuotas de otros servicios

AWS Outposts depende de los recursos de otros servicios y esos servicios pueden tener sus propias cuotas predeterminadas. Por ejemplo, su cuota para las interfaces de red locales proviene de la cuota de Amazon VPC para las interfaces de red.

Historial de documentos de servidores de Outposts

En la tabla siguiente se describen las actualizaciones realizadas en la documentación de los servidores de Outposts.

Cambio	Descripción	Fecha
Actualizaciones de la estabilidad estática	En caso de que se interrumpa la red, las métricas y los registros de las instancias se almacenarán en caché local durante un máximo de 7 días. Anteriormente, Outposts podía almacenar en caché los registros solo durante unas horas.	1 de mayo de 2025
Actualizaciones del rol vinculado al AWS Identity and Access Management servicio _ AWSService RoleForOutposts *OutpostID*	Los permisos del rol AWSServiceRoleForOutposts_ ***OutpostID*** vinculado al servicio se actualizan para refinar la forma en que se AWS Outposts administran los recursos de red para la conectividad privada, y se necesitan controles más precisos sobre las operaciones de la interfaz de red y los grupos de seguridad para las instancias de punto final del enlace de servicio.	17 de abril de 2025
Administración de la capacidad a nivel de activos	Puede modificar la configuración de la capacidad a nivel de activo.	31 de marzo de 2025

Conectividad privada mediante AWS Direct Connect Transit VIF	Ahora puedes configurar el enlace de servicio para usar un VIF de AWS Direct Connect tránsito para habilitar la conectividad privada entre los Outposts y la AWS región de origen.	11 de diciembre de 2024
Volúmenes de bloques externos respaldados por almacenamiento de terceros	Ahora puede adjuntar volúmenes de datos en bloque respaldados por sistemas de almacenamiento en bloque de terceros compatibles durante el proceso de lanzamiento de la instancia en Outpost.	1 de diciembre de 2024
Administración de la capacidad	Puedes modificar la configura ción de capacidad de una instancia.	11 de noviembre de 2024
Administración de la capacidad	Puede modificar la configura ción de capacidad predeterm inada para su nuevo pedido de Outposts.	16 de abril de 2024
AWS Outposts rack admite las métricas de rendimiento de la interfaz de enlace de servicio	Ahora puedes monitorear el uso del rendimiento entre tus interfaces virtuales de enlace de servicio rack de Outposts VIFs () y tus dispositi vos de red local, mediante el `IfTrafficIn` aprovecha miento `IfTrafficOut` Amazon CloudWatch de las métricas.	17 de noviembre de 2023

Comunicación dentro de la VPC a través de la puerta de AWS Outposts enlace local	Puede establecer comunicación entre subredes de la misma VPC a través de diferentes Outposts con puerta de enlace locales.	30 de agosto de 2023
End-of-term opciones para AWS Outposts estantes	Al final del AWS Outposts periodo, puedes renovar, finalizar o convertir tu suscripción.	1 de agosto de 2023
Amazon Route 53 en Outposts está disponible en AWS Outposts estantes.	Amazon Route 53 en Outposts incluye un solucionador que almacena en caché todas las consultas de DNS que se originan en AWS Outposts. También puede configurar la conectividad híbrida entre un Outpost y un solucionador de DNS en las instalaciones mediante la implementación de puntos de conexión entrantes y salientes.	20 de julio de 2023
Rutas de entrada de puerta de enlace local	Puede crear y modificar las rutas de entrada de las puertas de enlace locales para convertirlas en interfaces de red elásticas en el Outpost.	15 de septiembre de 2022
Presentamos el enrutamiento directo de VPC para AWS Outposts	Usa la dirección IP privada de las instancias de la VPC para facilitar la comunicación con la red en las instalaciones.	14 de septiembre de 2022

Creé una guía AWS Outposts de usuario para los racks de Outposts	AWS Outposts La guía del usuario se dividió en guías separadas para racks y servidores.	14 de septiembre de 2022
Creación y administración de tablas de enrutamiento de puertas de enlace locales	Cree y modifique las tablas de enrutamiento de las puertas de enlace locales y los grupos de CoIP. Administre las asociaciones de grupos VIF.	14 de septiembre de 2022
Coloque los grupos en AWS Outposts	Los grupos de ubicación que utilizan una estrategia de distribución pueden distribuir las instancias entre los hosts.	30 de junio de 2022
Hosts dedicados activados AWS Outposts	Ahora, puede usar hosts dedicados en Outposts.	31 de mayo de 2022
Sitios de Outpost compartidos	Crea y administra sitios de Outpost y compártelos con otras AWS cuentas de tu organización.	18 de octubre de 2021
Nueva dimensión CloudWatch	Una nueva CloudWatch dimensión para las métricas del espacio de AWS Outposts nombres.	13 de octubre de 2021
Comparta buckets de S3	Comparta y administre los buckets de S3 en el Outpost.	5 de agosto de 2021
Soporte para algunos grupos de ubicación	Puede utilizar estrategias de ubicación de clústeres, particiones o lotes tal como lo haría en una región.	28 de julio de 2021

Métricas adicionales CloudWatch	Hay CloudWatch métricas adicionales disponibles para las instancias reservadas.	24 de mayo de 2021
Lista de comprobación de solución de problemas de red	Se encuentra disponible una lista de comprobación para la solución de problemas de red.	22 de febrero de 2021
CloudWatch Métricas adicionales	Están disponibles CloudWatch métricas adicionales para los volúmenes de EBS.	2 de febrero de 2021
Actualizaciones de pedidos de consolas	Se ha actualizado el proceso de pedido de la consola.	14 de enero de 2021
Conectividad privada	Puede configurar la conectividad privada para su Outpost al crearlo en la consola AWS Outposts .	21 de diciembre de 2020
Lista de verificación de disponibilidad de red	Utilice la lista de verificación de disponibilidad de la red cuando recopile la información para la configuración de Outpost.	28 de octubre de 2020
Recursos compartidos AWS Outposts	Al compartir Outpost, los propietarios de Outpost pueden compartir sus recursos de Outposts y Outpost, incluidas las tablas de rutas de las puertas de enlace locales, con otras AWS cuentas de la misma organización. AWS	15 de octubre de 2020

Métricas adicionales CloudWatch	Hay CloudWatch métricas adicionales disponibles para el recuento de tipos de instancia s.	21 de septiembre de 2020
CloudWatch Métrica adicional	Hay disponible una CloudWatc h métrica adicional para el estado de conexión del enlace de servicio.	11 de septiembre de 2020
Support para compartir direcciones propiedad de los clientes IPv4	Se usa AWS Resource Access Manager para compartir direcciones propiedad de los clientes IPv4 .	20 de abril de 2020
Métricas adicionales CloudWatch	Están disponibles CloudWatc h métricas adicionales para los volúmenes de EBS.	4 de abril de 2020
Versión inicial	Esta es la versión inicial de AWS Outposts.	3 de diciembre de 2019

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.