Guía del usuario de bastidores

AWS Outposts

AWS Outposts: Guía del usuario de bastidores

Table of Contents

¿Qué es AWS Outposts?

AWS Outposts es un servicio totalmente gestionado que extiende la AWS infraestructura, los servicios, las API 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 de forma local con 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 instancias de EC2, 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. Puede ver y administrar la capacidad de su Outpost desde la consola de AWS 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 Outpost incluyen servidores que se pueden montar en bastidores, conmutadores, un panel de conexiones de red, un estante de suministro eléctrico y paneles vacíos.

- 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 Outpost proporcionan servicios de cómputo y red locales a sitios que tienen requisitos de espacio limitado o capacidad más reducida.
- Enlace de servicio: ruta de red que permite la comunicación entre su puesto de avanzada y la región asociada. AWS Cada Outpost es una extensión de una zona de disponibilidad y su región asociada.
- Puerta de enlace local (LGW): enrutador virtual de interconexión lógica que permite la comunicación entre un rack de Outpost y la red local.
- Interfaz de red local: interfaz de red que permite la comunicación entre un servidor del Outpost 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:

Cálculo

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

Base de datos y análisis

Tipo de recurso	Bastidores	Servidores
ElastiCache Nodos 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
Amazon SageMaker Edge Manager	 S	 Sí

Precios

Puede elegir entre una variedad de configuraciones de Outpost, cada una de las cuales ofrece una combinación de tipos de instancias EC2 y opciones de almacenamiento. El precio de las configuraciones en bastidor incluye la instalación, el desmontaje y el mantenimiento. En el caso de los servidores, es usted quien debe instalar y mantener el equipo.

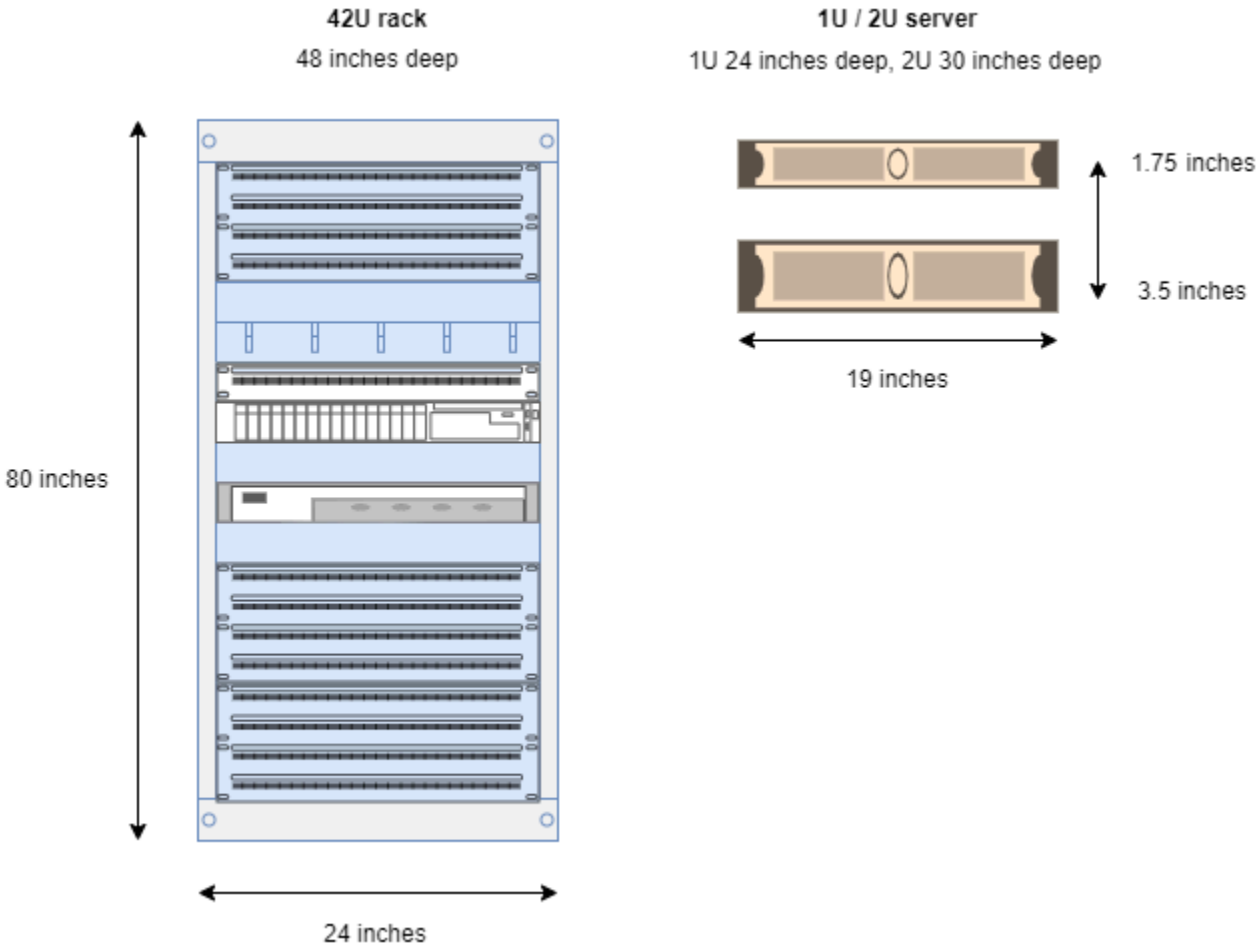
Debe adquirir una configuración por un período de 3 años y puede elegir entre tres opciones de pago: pago inicial total, pago inicial parcial y sin pago inicial. Si elige la opción de pago inicial parcial o sin pago inicial, se aplicarán cargos mensuales. Todos los cargos correspondientes a los pagos iniciales se aplican 24 horas después de que esté instalado el Outpost y la capacidad de cómputo y de almacenamiento estén disponibles para el uso. Para obtener más información, consulte:

- AWS Outposts precios de seguimiento
- AWS Outposts precios de servidores

Cómo funciona AWS Outposts

AWS Outposts está diseñado para funcionar con una conexión constante y uniforme entre el Outpost y una región de AWS. 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 en las instalaciones debe proporcionar acceso a la red de área extendida (WAN) de vuelta a la región y a Internet. 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

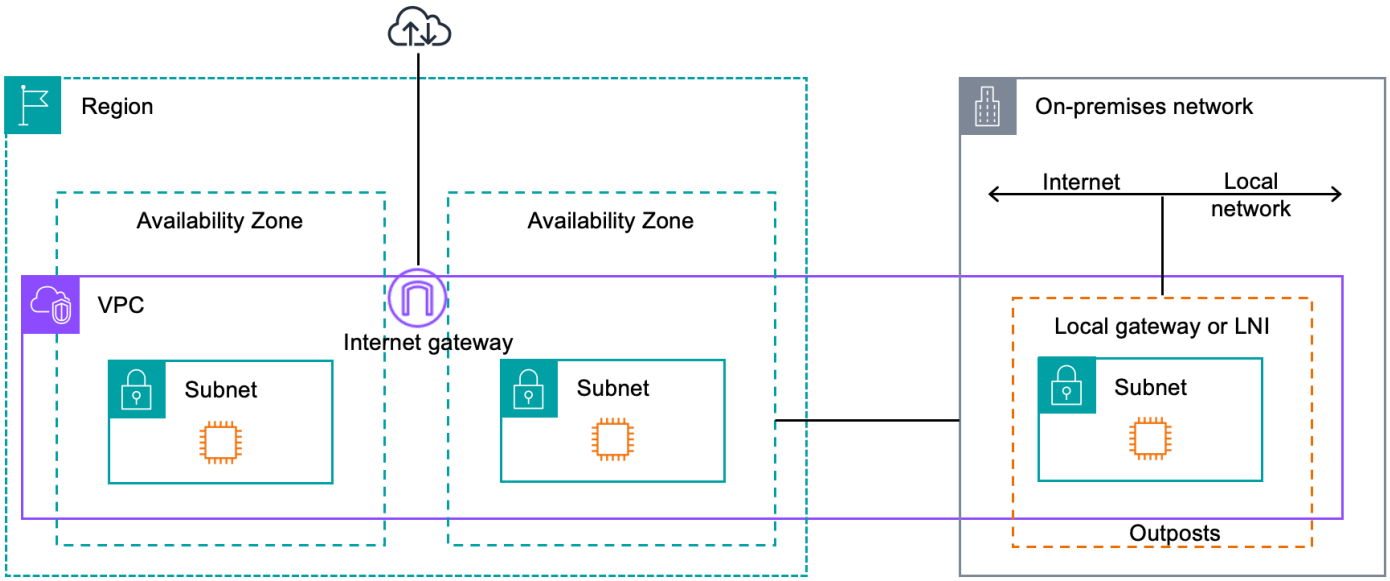
- DNS
- Enlace de servicio
- Puertas de enlace locales
- Interfaces de red local

Componentes de la red

AWS Outposts amplía una Amazon VPC desde una región de AWS a un Outpost con los componentes de VPC a los que se puede acceder en la región, incluidas puertas de enlace de Internet, puertas de enlace privadas virtuales, puertas de enlace de tránsito de Amazon VPC y puntos de conexión 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 Región de AWS y una red en las instalaciones
- 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 se proporciona mediante una puerta de enlace local (bastidores) o una interfaz de red local (servidores)



VPC y subredes

Una nube privada virtual (VPC) se extiende por todas las zonas de disponibilidad de la región de 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. Puede especificar la subred de la instancia EC2 al lanzar la instancia EC2 en el Outpost. No puede especificar el hardware subyacente en el que se despliega la instancia, ya que el Outpost es un grupo de capacidades informáticas y de almacenamiento de AWS.

Cada Outpost puede admitir múltiples VPC 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. Puede usar los rangos de direcciones de Outpost para los recursos, como las instancias EC2 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: AWS lo 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.
- Destinos regionales de AWS: incluye listas de prefijos para Amazon Simple Storage Service (Amazon S3), el punto de conexión de la puerta de enlace de Amazon DynamoDB, AWS

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

Si tiene una conexión de emparejamiento con varias VPC en el mismo Outpost, el tráfico entre las VPC 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

En el caso de las interfaces de red conectadas a una VPC, las instancias EC2 de las subredes de Outposts pueden utilizar el servicio Amazon Route 53 DNS para resolver nombres de dominio en direcciones IP. Route 53 es compatible con las funciones 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 solucionadores de Route 53 están alojados en la región de AWS. Por lo tanto, la conectividad del enlace de servicio desde el Outpost hasta la región de AWS debe estar activa y en funcionamiento para que estas características de DNS funcionen.

Es posible que encuentre tiempos de resolución DNS más largos con Route 53, según la latencia de ruta entre Outpost y la región de AWS. 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 Outpost 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 su Outpost a la región de AWS 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 Outpost y la región de AWS, tanto para la administración del tráfico del Outpost como dentro de la VPC entre la región AWS y el Outpost.

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 bastidor, AWS crea el enlace de servicio. Para obtener más información, consulte Conectividad de Outpost a Regiones de AWS.

Puertas de enlace locales

Los bastidores de Outpost incluyen una puerta de enlace local para proporcionar conectividad a la red en las instalaciones. Si tiene un bastidor de Outpost, 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 Outpost y solo se pueden usar en tablas de enrutamiento de subredes y VPC asociadas a un bastidor de Outpost. Para obtener más información, consulte Puerta de enlace local.

Interfaces de red local

Los servidores de Outpost 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 puede utilizar una interfaz de red local desde una instancia EC2 en un bastidor de Outpost o en la región de AWS. 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 el bastidor 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 Preguntas frecuentes sobre bastidores de AWS Outposts. Consulte la pregunta: ¿En qué países y territorios está disponible el bastidor de Outposts?

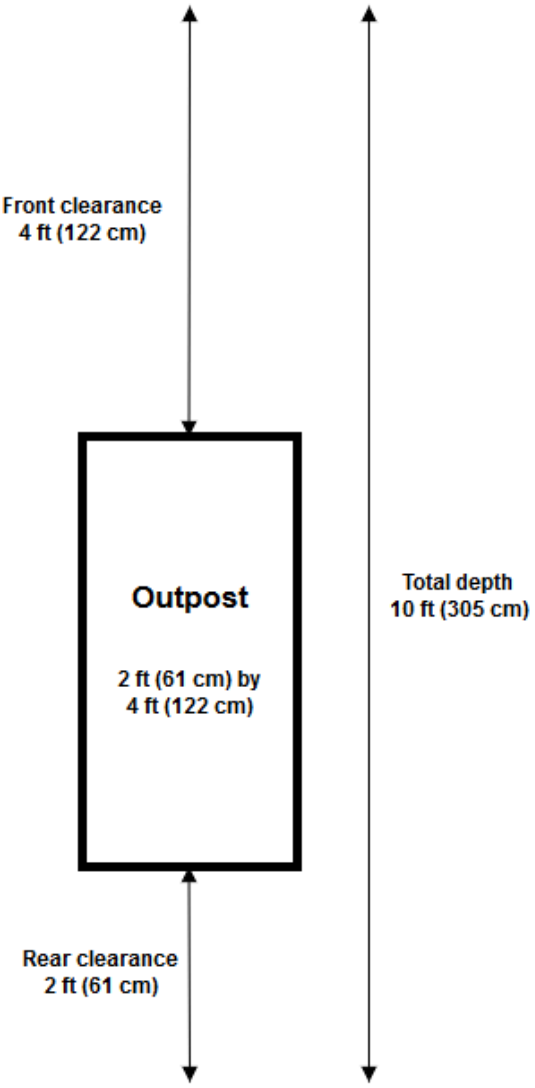
En esta página se describen los requisitos del bastidor de Outposts. Para conocer los requisitos de los servidores de Outposts, consulte Requisitos del sitio para los servidores de Outposts en la Guía del usuario de AWS Outposts para los servidores de Outposts.

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 el anclaje sísmico y el refuerzo adecuados para el estante mientras esté en sus instalaciones. AWSproporciona soportes de suelo que protegen hasta 2 g de actividad sísmica con todos los estantes Outposts.
- Punto de unión: le recomendamos que coloque un hilo / punto de unión en la posición del bastidor para que un técnico certificado de AWS pueda unir los bastidores durante la instalación.
- Acceso a las instalaciones: no modificará las instalaciones de forma que afecte negativamente la capacidad de AWS acceder, mantener o desmontar el Outpost.

- 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 conector Lucent (LC), fibra multimodo (MMF) o MMF OM4 con LC.
- 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. 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 OM4 con LC

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	: 40 GBASE-IR4 (LR4L) : 40 GBASE-LR4
Aplicación breakout de 4 x 10 Gbps	MMF	: 40 GBASE-ESR4 : 40 GBASE-SR4
100 Gbps	SMF	: 100 G PSM4 MSA : 100 GBASE-CWDM4 : 100 GBASE-LR4

Velocidad de enlace ascendente	Tipo de fibra	Estándares ópticos
Aplicación breakout de 4 x 25 Gbps	MMF	: 100 GBASE-SR4

Agregación de enlaces de Outpost y VLAN

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.

Se requieren las siguientes VLAN para cada dispositivo de red del Outpost. Para obtener más información, consulte LAN virtuales.

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 del Outpost, puede elegir si desea utilizar las mismas VLAN o diferentes VLAN 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 LAN virtuales.

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 del Outpost requiere un CIDR y una dirección IP para las VLAN del enlace de servicio y de la puerta de enlace local. 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 Service Link en la región principal. AWS Para obtener más información sobre el enlace de servicio, consulte Conectividad de AWS Outposts con las regiones de AWS.

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). : 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

Puede usar una conexión de AWS Direct Connect 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 perimetral. El establecimiento del enlace de servicio siempre se inicia desde el Outpost.

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 el recurso de Outpost tiene un consumo de energía máximo de 9,7 kVA, debe proporcionar las configuraciones de alimentación para 10 kVA: 4 L6-30P o IEC309, 2 caídas a S1 y 2 caídas a S2, a fin de obtener energía 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, seleccione Examinar catálogo en la consola de AWS Outposts en https://console.aws.amazon.com/outposts/.

Tensión de línea AC	Monofásica de 208 a 277 VCA (50 o 60 Hz) Trifásica de 346 a 480 VCA (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 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)	Enchufes monofásicos 3xL6-30P, P+P+E, 30A o 3xIEC60309 P+N+E, IP67, 32A Wye trifásicos 1xIEC60309, 3P+N+E, IP67, posición de reloj 7, conector 30A o 1xIEC60309, 3P+N+E, IP67, posición de reloj 6, enchufe de 32A Delta trifásicos cierre giratorio 1xNon-NEMA Hubbell CS8365C, 3P+E, conexión a tierra central, enchufe de 50A **Note** La mejor práctica es acoplar un enchufe de IP67 a un receptáculo IP67. Si eso no es posible, el enchufe de IP67 se acoplará a un receptáculo IP44. 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 L6-30P o IEC309, 1 caída a S1 y 1 caída a S2	2 AH530P7W o AH532P6W, 1 caída a S1 y 1 caída a S2	1 L6-30P o IEC309, 1 caída a S1	1 AH530P7W o AH532P6W, 1 caída a S1
10 kVA	4 unidades L6-30P o IEC309, 2 caídas a S1 y 2 caídas a S2		2 L6-30P o IEC309, 2 caídas a S1	
15 kVA	6 unidades L6-30P o IEC309, 3 caídas a S1 y 3 caídas a S2		3 L6-30P o IEC309, 3 caídas a S1	

En el caso que los látigos de AC que AWS suministra, 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 representante de AWS las modificaciones realizadas al enchufe látigo de AC. 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 tramitar el pedido, AWS programará 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 instalación de AWS llegará a sus instalaciones en la fecha y hora programadas. El equipo hará rodar el bastidor hasta 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 de AWS por escrito antes de realizar cualquier cambio en el hardware o las instalaciones eléctricas del Outpost. Usted acepta proporcionar la AWS documentación que verifique el cumplimiento y la seguridad de cualquier modificación realizada. AWS no se hace responsable de los riesgos que pudieran generar la instalación eléctrica o el cableado eléctrico de la instalación del Outpost, ni de ninguna modificación que se realice. 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 finaliza cuando confirma que la capacidad de Amazon EC2 y Amazon EBS para el bastidor de Outposts se encuentra disponible en su Cuenta de AWS.

Comience con AWS Outposts

Solicite un Outpost para comenzar. Tras instalar su equipo de Outpost, lance las instancias de Amazon EC2 y acceda a la red en las instalaciones.

Tareas

- Crear un Outpost y solicitar capacidad de Outpost
- Lanza una instancia en tu rack de Outpost

Crear un Outpost y solicitar capacidad de Outpost

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 el bastidor de Outposts.
- Debe tener un plan AWS Enterprise Support.
- Determine quién Cuenta de AWS será el propietario del Outpost. Utilice esta cuenta para crear el sitio de Outposts, crear el Outpost y realizar 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
- Siguientes pasos

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. Inicia sesión para AWS usar Cuenta de AWS el propietario del Outpost.
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 el caso de 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. Podrá especificar este Outpost al realizar 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”.
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. Después de enviar el pedido, un representante de AWS Outposts se pondrá en contacto con usted.

> **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 AWS administrador de 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 elige no pagar todo por adelantado, pagará los cargos mensuales durante un período de tres años.

  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 se ajustan a sus necesidades, puede ponerse en contacto con nosotros AWS 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 necesitas cambiar la dirección de envío de un pedido existente, ponte en contacto con tu administrador de AWS cuentas.

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 capacidad de Amazon EC2, Amazon EBS y Amazon S3 AWS Outposts 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 que se adapten a las necesidades de su empresa. Para ello, debe crear una tarea de capacidad, especificar los tamaños y la cantidad de las instancias y ejecutar la tarea de capacidad para implementar los cambios.

> **Note**
>
> - Puedes cambiar la cantidad de tamaños de instancia después de realizar el pedido de tus Outposts.
> - Los tamaños y las cantidades de las instancias se definen a nivel de Outpost.
> - Las instancias se colocan automáticamente según las mejores prácticas.

Para modificar la capacidad de las instancias

1. En el panel de navegación AWS Outposts izquierdo de la AWS Outposts consola, selecciona Tareas de capacidad.
2. En la página Tareas de capacidad, selecciona Crear tarea de capacidad.
3. En la página de introducción, selecciona el orden.
4. Para modificar la capacidad, puede seguir los pasos de la consola o cargar un archivo JSON.

Console steps

1. Selecciona Modificar una nueva configuración de capacidad de 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, selecciona Añadir 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 su capacidad está por encima o por debajo de la capacidad. Realice ajustes en el tamaño o la cantidad de la instancia para optimizar la 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. Elige el tamaño de la instancia.
   b. Selecciona 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.

Upload JSON file

1. Seleccione Cargar una configuración de capacidad.

2. Elija Siguiente.
3. En la página del plan de configuración de la capacidad de carga, carga el archivo JSON que especifica el tipo, el tamaño y la cantidad de la instancia.

   Example

   Ejemplo de archivo JSON:

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

4. Revisa 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. Selecciona 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.

Siguientes pasos

Puede ver el estado de su pedido mediante la AWS Outposts consola. El estado inicial de su pedido es Pedido recibido. Un AWS representante se pondrá en contacto contigo en un plazo de tres días laborables. Recibirá una confirmación por correo electrónico cuando el estado del pedido cambie al

de Pedido en proceso. Un AWS representante puede ponerse en contacto con usted para obtener cualquier información adicional que AWS necesite.

Si tiene alguna pregunta sobre su pedido, póngase en contacto con AWS Support.

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 confirma que la capacidad de Amazon EC2 y Amazon EBS para su Outpost está disponible en su cuenta. AWS

Lanza una instancia en tu rack de Outpost

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 instancias de Amazon EC2 y cree volúmenes de Amazon EBS en el Outpost utilizando una subred de Outpost. También puede crear snapshots de volúmenes de Amazon EBS en su Outpost. Para obtener más información aplicable a Linux, consulte Instantáneas locales de Amazon EBS en AWS Outposts en la Guía del usuario de Amazon EC2 para instancias de Linux. Para obtener más información aplicable a Windows, consulte Instantáneas locales de Amazon EBS en AWS Outposts en la Guía del usuario de Amazon EC2 para instancias de Windows.

Requisito previo

Debe tener un Outpost instalado en su sitio. Para obtener más información, consulte Crear un Outpost y solicitar capacidad de Outpost.

Tareas

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

Paso 1: Crear una VPC

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

Para crear una VPC para tu Outpost

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. Elige la misma región que el estante Outposts.
3. En el panel de navegación, elija Sus VPC 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 CIDR de IPv4, elija la entrada manual de CIDR de IPv4 e introduzca el rango de direcciones IPv4 de la VPC en el cuadro de texto CIDR de IPv4.

   > **Note**
   >
   > Si quieres usar el enrutamiento directo de VPC, especifica un rango de CIDR que no se superponga con el rango de IP que usas en tu red local.

7. Para el bloque CIDR de IPv6, elija Sin bloque CIDR de IPv6.
8. En Arrendamiento, elija Predeterminado.
9. (Opcional) Para añadir una etiqueta a la VPC, elija Añadir etiqueta e introduzca una clave y un valor.
10. Seleccione Crear VPC.

Paso 2: Cree una tabla de 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 incluye el Outpost. Para obtener más información, consulte Componentes de la red.

> **Note**
>
> Si vas a lanzar una instancia en una subred de Outpost que otra Cuenta de AWS persona ha compartido contigo, salta a. Paso 5: Lanza una instancia en el Outpost

2a: Crea una subred de Outpost

Para crear 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, 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 subred, si lo desea, asigne un nombre a la subred y especifique un rango de direcciones IP para la subred.
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 de subredes. Para activar la columna, selecciona el icono de Preferencias, selecciona el ID de Outpost y selecciona Confirmar.

2b: Crea una tabla de rutas 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: Asocie la subred de Outpost y la tabla de rutas 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 local. Para obtener más información sobre la LGW, consulte Puerta de enlace local.

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

3a. Crea una tabla de rutas de puerta de enlace local personalizada

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

Para crear una tabla de rutas LGW 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, ingresa un nombre para la tabla de rutas de LGW.
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 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.
8. (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.
9. Elija Crear tabla de enrutamiento de puerta de enlace local.

3b: Asocie la VPC a la tabla de enrutamiento LGW personalizada

Debe asociar las VPC a su tabla de enrutamiento de LGW. No están asociadas de forma predeterminada.

Utilice el siguiente procedimiento para asociar una VPC a una tabla de enrutamiento LGW.

Puede etiquetar de forma opcional su asociación para ayudarlo a identificarlo o clasificarlo en función de las necesidades de su organización.

AWS Outposts console

Para asociar una VPC a la tabla de enrutamiento LGW 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 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) Añada o elimine una etiqueta.

   Para 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.

   Para eliminar una etiqueta, elija Eliminar a la derecha de la clave y valor de la etiqueta.
7. Elija Asociar VPC.

AWS CLI

Para asociar una VPC a la tabla de enrutamiento LGW personalizada

Utilice el comando create-local-gateway-route- table-vpc-association.

Ejemplo

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

Salida

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

3c: Agregue una entrada de ruta en la tabla de rutas de la subred de Outpost

Agregue una entrada de ruta en la tabla de rutas de subred de Outpost para habilitar el tráfico entre las subredes de Outpost y LGW.

Las subredes de Outpost dentro de una VPC, que está asociada a las tablas de enrutamiento LGW de Outpost, pueden tener un tipo de destino adicional, 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 LGW. Para ello, edite la tabla de rutas de subred de Outpost y añada la siguiente ruta con la red de destino y un destino de la LGW (). `lgw-xxxx`

Destino	Objetivo
172.16.100.0/24	`lgw-id`

Para agregar una entrada de ruta **`lgw-id`** como destino en la tabla de enrutamiento de subred de Outpost:

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Tablas de rutas y seleccione la tabla de rutas en la que creó. 2b: Crea una tabla de rutas personalizada
3. Elija Acciones y, a continuación, Editar rutas.
4. Para agregar una ruta, elija Añadir ruta.
5. En Destino, introduzca el bloque CIDR de destino en la red del cliente.
6. En Target, elija el ID de puerta de enlace local de Outpost.

7. Elija Guardar cambios.

3d: asocie la tabla de rutas LGW personalizada a los grupos VIF de LGW

Los grupos VIF son agrupaciones lógicas de interfaces virtuales (VIF). Asocie la tabla de rutas de la puerta de enlace local al grupo VIF.

Para asociar la tabla de rutas de LGW personalizada a los grupos de VIF de LGW

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 de asociación de grupos de VIF en el panel de detalles y, a continuación, elija Editar asociación de grupos de VIF.
6. Para la configuración del grupo VIF, seleccione Asociar grupo VIF y elija un grupo VIF.
7. Elija Guardar cambios.

3e: Agregue una entrada de ruta en la tabla de rutas de LGW

Edite la tabla de rutas de la puerta de enlace local para agregar una ruta estática que tenga el grupo VIF como destino y el rango CIDR de la subred local (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 rutas de 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 rutas 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) Asigne una dirección IP propiedad del cliente a la instancia

Si configuraste tus Outposts 3a. Crea una tabla de rutas de puerta de enlace local personalizada para usar un grupo de direcciones IP (CoIP) propiedad del cliente, debes asignar una dirección IP elástica del grupo de direcciones CoIP y asociar la dirección IP elástica a la instancia. Para obtener más información acerca de CoIP, consulte Direcciones IP propiedad del cliente.

Si configuraste tus Outposts para usar el enrutamiento directo de VPC (DVR), omite este paso.

Amazon VPC console

Para asignar una dirección CoIP a la instancia

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 direcciones IPV4 públicas, elija Grupo de direcciones IPv4 propiedad del cliente.
6. Para Grupo de direcciones IPv4 propiedad del cliente, seleccione el grupo que haya configurado.
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 la instancia

1. Usa el describe-coip-poolscomando para recuperar información sobre los grupos de direcciones propiedad de tus 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",
}
```

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 IPv4 propiedad del cliente, consulte Compartir sus recursos de AWS en la Guía del usuario de AWS RAM .

Paso 4: Configurar la red local

El Outpost establece un emparejamiento BGP externo desde cada dispositivo de red Outpost (OND) a un dispositivo de red local (CND) del cliente para enviar y recibir tráfico de su red local a los Outposts. Para obtener más información, consulte Conectividad BGP de una puerta de enlace local.

Para enviar y recibir tráfico de su red local 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 del local a Outposts, asegúrate de recibir en tu CND los anuncios de BGP de Outposts. Estos anuncios de BGP contienen las rutas que su red local debe utilizar para enrutar el tráfico desde la red local a Outpost. Por lo tanto, asegúrate de que tu red tenga la ruta correcta entre Outposts y los recursos locales.
- Para el tráfico que va de Outposts a la red local, asegúrese de que sus CND envíen los anuncios de la ruta BGP de las subredes de la red local a Outposts (o 0.0.0.0/0). Como alternativa, puedes anunciar una ruta predeterminada (por ejemplo, 0.0.0.0/0) a Outposts. Las subredes locales anunciadas por los CND deben tener un rango de CIDR igual o estar incluido en el rango de CIDR en el que se configuró. 3e: Agregue una entrada de ruta en la tabla de rutas de LGW

Ejemplo: anuncios de BGP en modo VPC directo

Considere el escenario en el que tiene un Outpost, configurado en modo VPC directo, con dos dispositivos de red en rack de Outposts conectados mediante una VLAN de puerta de enlace local a dos dispositivos de red local del 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 CIDR 10.0.3.0/24.
- Una subred en la red local con un bloque CIDR 172.16.100.0/24
- Outposts usa la dirección IP privada de las instancias de la subred Outpost, por ejemplo, 10.0.3.0/24, para comunicarse con la red local.

En este escenario, la ruta anunciada por:

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

Como resultado, la puerta de enlace local enviará el tráfico saliente con la red de destino 172.16.100.0/24 a los dispositivos de sus clientes. 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 la lista de verificación para la solución de problemas de redes en AWS Outposts rack.

Ejemplo: anuncios de BGP en modo CoIP

Considere el escenario en el que tiene un Outpost con dos dispositivos de red en rack de Outposts conectados mediante una VLAN de puerta de enlace local a dos dispositivos de 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.
- 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 local con un bloque CIDR 172.16.100.0/24

- La comunicación entre el Outpost y la red en las instalaciones utilizará las IP elásticas de CoIP 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 sus clientes es 10.1.0.0/26.
- Los dispositivos de sus clientes a la puerta de enlace local de Outpost son 172.16.100.0/24.

Como resultado, la puerta de enlace local enviará el tráfico saliente con la red de destino 172.16.100.0/24 a los dispositivos de sus clientes. Asegúrese de que su red tenga la configuración de enrutamiento correcta para entregar el tráfico al host de destino de su 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 la lista de verificación para la solución de problemas de redes en AWS Outposts rack.

Paso 5: Lanza una instancia en el Outpost

Puede lanzar instancias EC2 en la subred de Outpost que ha creado o en una subred de Outpost que se haya compartido con usted. 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 instancia EC2 en una subred de Outpost, puede especificar un par de claves al lanzar la instancia, tal como lo hace para las instancias de una subred de una zona de disponibilidad.

Consideraciones

- Puede crear grupos de ubicación para influir en la forma en que Amazon EC2 debe intentar colocar grupos de instancias interdependientes en el hardware de los 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 consola de Amazon EC2. Seleccionamos la subred de Outpost por ti y te mostramos solo los tipos de instancias compatibles con tu rack de Outposts.
5. Elige un tipo de instancia que sea compatible con tu rack de Outposts. Ten en cuenta que las instancias que aparecen en gris no están disponibles para tu Outpost.
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, consulte los siguientes temas en la Guía del usuario de Amazon EC2:

   - Linux: lanza una instancia mediante el nuevo asistente de lanzamiento de instancias
   - Windows: lanza una instancia mediante el asistente de lanzamiento de nuevas instancias

> **Note**
>
> Si está creando un volumen de Amazon EBS, debe usar el tipo de volumen gp2 o el asistente fallará.

Paso 6: Pruebe 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, ejecuta el `ping` comando 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, consulte Conexión con la instancia de Linux en Guía del usuario de Amazon EC2 para instancias de Linux. Para obtener más información sobre cómo conectarse a una instancia de Windows, consulte Conectarse a su instancia de Windows en la Guía del usuario de Amazon EC2 para instancias de Windows.

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
```

Prueba 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 en la AWS región. Esta información está disponible en la consola de Amazon EC2 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 información sobre la conexión a una instancia de Linux, consulte Conexión con la instancia de Linux en Guía del usuario de Amazon EC2 para instancias de Linux. Para obtener más información sobre cómo conectarse a una instancia de Windows, consulte Conectarse a su instancia de Windows en la Guía del usuario de Amazon EC2 para instancias de Windows.

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
```

Prueba 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 consola de Amazon EC2 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 de AWS Region.

   ```
   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
   ```

Conectividad de AWS Outposts con las regiones de AWS

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

Contenido

Conectividad a través de enlaces de servicio

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

Para configurar la conectividad del enlace de servicio, AWS debe configurar la conectividad física, la LAN virtual (VLAN) y la conectividad de capa de red del enlace de servicio con los dispositivos de la red local durante el aprovisionamiento de Outpost. Para obtener más información, consulta Conectividad de red local para los racks y Requisitos del sitio para el rack Outposts.

Para la conectividad de la red de área amplia (WAN) con la AWS región, AWS Outposts puede establecer conexiones VPN de enlace de servicio a través de la conectividad pública de la AWS región. Esto requiere que los Outposts tengan acceso a los rangos de IP públicas de la Región, que pueden ser a través de Internet pública o interfaces virtuales AWS Direct Connect públicas. Para conocer los rangos de direcciones IP actuales, consulte los rangos de direcciones IP de AWS en la guía del usuario de Amazon VPC. Esta conectividad se puede habilitar configurando rutas específicas o predeterminadas (0.0.0.0/0) en la ruta de la capa de red del enlace de servicio. Para obtener más información, consulte Conectividad BGP de Service Link y Anuncio de subredes y rango de IP de la infraestructura de Service Link.

Como alternativa, puede seleccionar la opción de conectividad privada para su Outpost. Para obtener más información, consulte Conectividad privada de Service Link mediante VPC.

Una vez establecida la conexión de enlace de servicio, su Outpost comienza a funcionar y es administrado por. AWS El enlace de servicio se utiliza para el siguiente tráfico:

- Tráfico de VPC del cliente entre Outpost y cualquier VPC asociada.
- El tráfico de administración de Outposts, como la administración de recursos, el monitoreo 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 los puntos finales de Outpost y Service Link en la región principal. AWS Para obtener información sobre la MTU requerida entre una instancia de Outpost y una instancia de la AWS región a través del enlace de servicio, consulte la unidad máxima de transmisión (MTU) de la red para su instancia de Amazon EC2 en la Guía del usuario de Amazon EC2 para instancias de Linux.

Recomendaciones de ancho de banda para el enlace de servicio

Para disfrutar de una experiencia y una resiliencia óptimas, AWS recomienda utilizar una conectividad redundante de al menos 500 Mbps (1 Gbps es mejor) para la conexión del enlace de servicio a la región de AWS. Puede utilizar AWS Direct Connect o una conexión de Internet para el enlace del servicio. La conexión de enlace de servicio mínima de 500 Mbps le permite lanzar instancias de Amazon EC2, adjuntar volúmenes de Amazon EBS y acceder a AWS servicios, como Amazon EKS, Amazon EMR y métricas. CloudWatch

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

- Número de bastidores de AWS Outposts 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 para el enlace de servicio requerido para sus necesidades, póngase en contacto con su representante de ventas de AWS o un socio de APN.

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 región de AWS hasta el Outpost. Una interfaz virtual pública de AWS Direct Connect es la conexión del 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 Outpost y cualquier VPC asociada

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 Outpost desde la región de AWS, como 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	Enlace de servicio de AWS Outposts /26	443	Rutas públicas de la región de AWS Outposts
TCP	1025-65535	Enlace de servicio de AWS Outposts /26	443	Rutas públicas de la región de AWS Outposts

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.

Los bastidores de AWS Outposts también están diseñados con equipos de red y alimentación redundantes, incluidos los componentes de la puerta de enlace local. Para obtener más información, consulte Resiliencia en AWS Outposts.

Conectividad privada del enlace de servicio mediante el uso de VPC

Puede seleccionar la opción de conectividad privada en la consola al crear su Outpost. Al hacerlo, 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.

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, consulte Gestión de identidad y acceso (IAM) para AWS Outposts y Uso de roles vinculados a servicios de AWS Outposts.
- En la misma cuenta y zona de disponibilidad de AWS que su Outpost, cree una VPC con el fin de que la conectividad privada de Outpost con una subred /25 o superior no entre en conflicto con la versión 10.1.0.0/16. Por ejemplo, puede usar 10.2.0.0/16.
- Cree una conexión de AWS Direct Connect, una interfaz virtual privada y una puerta de enlace privada virtual para permitir que su Outpost en las instalaciones acceda a la VPC. Si la conexión de AWS Direct Connect se realiza en una cuenta de AWS diferente a la de su VPC, consulte

Asociación de una puerta de enlace privada virtual entre cuentas en la Guía del usuario de AWS Direct Connect.

- Anuncie el CIDR de la subred en las instalaciones. Puede usar 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.

Puede seleccionar la opción de conectividad privada al crear su Outpost en la consola de AWS Outposts. Para obtener instrucciones, consulte Crear un Outpost y solicitar capacidad de Outpost.

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

Tras seleccionar la opción de conectividad privada para su Outpost, AWS Outposts crea de forma automática un rol vinculado al servicio en su cuenta que le permite completar las siguientes tareas en su 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 servicio de AWS Outposts para conectar las interfaces de red a una instancia de punto de conexión del 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.

Para obtener más información sobre el rol vinculado a servicios, consulte Uso de roles vinculados a servicios de AWS Outposts.

> **Important**
>
> Una vez instalado su Outpost, confirme la conectividad con las IP privadas de su subred desde su Outpost.

Conexiones de Internet redundantes

Al desarrollar la conectividad entre su Outpost y la región de AWS, 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.

Outposts y sitios

Administra Outposts y sitios para. AWS Outposts

Puede etiquetar sus recursos y sitios de Outposts para ayudarle a identificarlos o clasificarlos según las necesidades de su organización. Para obtener más información sobre el etiquetado, consulte Etiquetado de AWS recursos en la guía.Referencia general de AWS

Temas

- Administre Outposts
- Administre los sitios de Outposts

Administre Outposts

AWS Outposts incluye recursos virtuales y de hardware conocidos como Outposts. Utilice esta sección para crear y administrar Outposts, como cambiar el nombre y agregar o ver detalles o etiquetas.

Para crear un Outpost

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 Outposts.
4. Seleccione Crear Outpost.
5. Elija un tipo de hardware para este Outpost.
6. Escriba un nombre y la descripción de su Outpost.
7. Seleccione una zona de disponibilidad para su Outpost.
8. (Opcional) Elija Opción de conectividad privada. Para la VPC y la subred, selecciona una VPC y una subred en la misma AWS cuenta y zona de disponibilidad que tu Outpost.

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

9. Desde ID del sitio, realice una de las siguientes operaciones:

   - Para seleccionar un sitio existente, selecciónelo.
   - Para crear un sitio nuevo, elija Crear sitio, haga clic en Siguiente e introduzca la información sobre el sitio en la nueva ventana.

     Tras crear el sitio, vuelva a esta ventana para seleccionarlo. Puede que tenga que actualizar la lista de sitios para ver el nuevo sitio. Para actualizar los datos, elija el icono de actualización ( ).

     Para obtener más información, consulte the section called “Sitios”.
10. Seleccione Crear Outpost.

> **Tip**
>
> Para agregar capacidad a su nuevo Outpost, debe realizar un pedido.

Siga los siguientes pasos para editar el nombre y la descripción de un Outpost.

Para editar el nombre y la descripción del Outpost

1. Abre la consola en https://console.aws.amazon.com/outposts/. AWS 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 Outposts.
4. Seleccione el Outpost y, a continuación, elija Acciones, Editar Outpost.
5. Modifique el nombre y la descripción.

   Para Nombre, escriba el nombre.

   En Descripción, escriba la descripción.
6. Elija Guardar cambios.

Utilice los siguientes pasos para ver los detalles de un Outpost.

Para ver los detalles de Outpost

1. Abre 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 Outposts.
4. Seleccione el Outpost y, a continuación, elija Acciones, Ver detalles.

También puedes usarlo para ver los detalles AWS CLI de Outpost.

Para ver los detalles de Outpost con el AWS CLI

- Utilice el comando get-outpost AWS CLI .

Siga los siguientes pasos para administrar las etiquetas de un Outpost.

Para administrar las etiquetas de Outpost

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 Outposts.
4. Seleccione el Outpost y, a continuación, elija Acciones, Administrar etiquetas.
5. Añada o elimine una etiqueta.

   Para 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.

   Para eliminar una etiqueta, elija Eliminar a la derecha de la clave y valor de la etiqueta.
6. Elija Guardar cambios.

Administre los sitios de Outposts

Los edificios físicos gestionados por el cliente donde AWS instalarás tu Outpost. Un sitio debe cumplir con los requisitos de instalaciones, redes y alimentación de su Outpost. Para obtener más información, consulte Requisitos.

Para crear un sitio de Outpost

1. Abre 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, seleccione Sitios.
4. Seleccione Crear sitio.
5. Elija un tipo de hardware compatible para el sitio.
6. Introduzca un nombre, una descripción y una dirección operativa para el sitio. Si elige admitir bastidores en el sitio, introduzca la siguiente información:
   - Peso máximo: especifique el peso máximo del bastidor que este sitio puede admitir.
   - Consumo de energía: especifique en kVA el consumo de energía disponible en la posición de colocación del hardware para el bastidor.
   - Opción de alimentación: especifique la opción de alimentación que puede proporcionar para el hardware.
   - Conector de alimentación: especifique el conector de alimentación que AWS debe utilizarse para las conexiones al hardware.
   - Caída de alimentación: especifique si la alimentación se produce por encima o por debajo del bastidor.
   - Velocidad de enlace ascendente: especifique la velocidad de enlace ascendente que debe admitir el bastidor para la conexión con la región.
   - Número de enlaces ascendentes: especifique el número de enlaces superiores de cada dispositivo de red del Outpost que vaya a utilizar para conectar el bastidor a la red.
   - Tipo de fibra: especifique el tipo de fibra que utilizará para conectar el Outpost a su red.
   - Estándar óptico: especifique el tipo de estándar óptico que utilizará para conectar el Outpost a su red.
   - Notas: especifique las notas sobre un sitio.

7. Lea los requisitos de la instalación y elija He leído los requisitos de la instalación.
8. Seleccione Crear sitio.

Siga los siguientes pasos para editar un sitio para el Outpost.

Para editar un sitio

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, seleccione Sitios.
4. Seleccione el sitio y, a continuación, seleccione Acciones, Editar sitio.
5. Puede modificar el nombre, la descripción, la dirección operativa y los detalles del sitio.

   Si cambia la dirección operativa, tenga en cuenta que los cambios no se propagarán a los pedidos existentes.
6. Elija Guardar cambios.

Utilice los siguientes pasos para ver los detalles de un sitio de Outpost.

Para consultar los detalles del servicio

1. Abre 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, seleccione Sitios.
4. Seleccione el sitio y, a continuación, elija Acciones, Ver detalles.

Utilice los siguientes pasos para administrar las etiquetas de un sitio de Outpost.

Para administrar las etiquetas del sitio

1. Abre 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, seleccione Sitios.

4. Seleccione el sitio y, a continuación, elija Acciones, Administrar etiquetas.
5. Añada o elimine una etiqueta.

   Para 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.

   Para eliminar una etiqueta, elija Eliminar a la derecha de la clave y valor de la etiqueta.
6. Elija Guardar cambios.

Puerta de enlace local

La puerta de enlace local es un componente central de la arquitectura de Outposts. La puerta de enlace local permite la conectividad entre las subredes 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 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 Direct Connect. Para obtener más información, consulte Conectividad de AWS Outposts con las regiones de AWS.

Contenido

Conceptos básicos de la puerta de enlace local

Cada Outpost admite una única puerta de enlace local. Una puerta de enlace local tiene los siguientes componentes:

- Tablas de enrutamiento: se utilizan para crear tablas de enrutamiento de puertas de enlace locales. Para obtener más información, consulte the section called “Tabla de enrutamiento de la puerta de enlace local”.
- 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 (VIF): AWS crea un VIF para cada LAG y agrega ambos VIF a un grupo de VIF. La tabla de enrutamiento de la puerta de enlace local debe tener una ruta predeterminada a las dos VIF para la conectividad de la red local. Para obtener más información, consulte Conectividad de red local.
- Asociaciones de grupos de VIF: AWS agrega los VIF que crea a un grupo de VIF. Los grupos de VIF son agrupaciones lógicas de VIF. Para obtener más información, consulte the section called “Asociación de grupos VIF ”.

- Asociaciones de VPC: se utilizan para crear asociaciones de VPC con las VPC y la tabla de enrutamiento de la puerta de enlace local. Las tablas de enrutamiento de VPC asociadas a las subredes que residen en un Outpost pueden usar la puerta de enlace local como destino de ruta. Para obtener más información, consulte the section called “Asociaciones de VPC”.

Cuando AWS aprovisiona su rack de Outpost, creamos algunos componentes y usted es responsable de crear otros.

AWS responsabilidades

- Entrega el hardware.
- Crea la puerta de enlace local.
- Crea las interfaces virtuales (VIF) y un grupo de 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.
- Asociar un grupo VIF a una tabla de enrutamiento de puerta de enlace local.

Enrutamiento

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 “Tabla de enrutamiento de la puerta de enlace local”.

Conectividad a través de la 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 de 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:

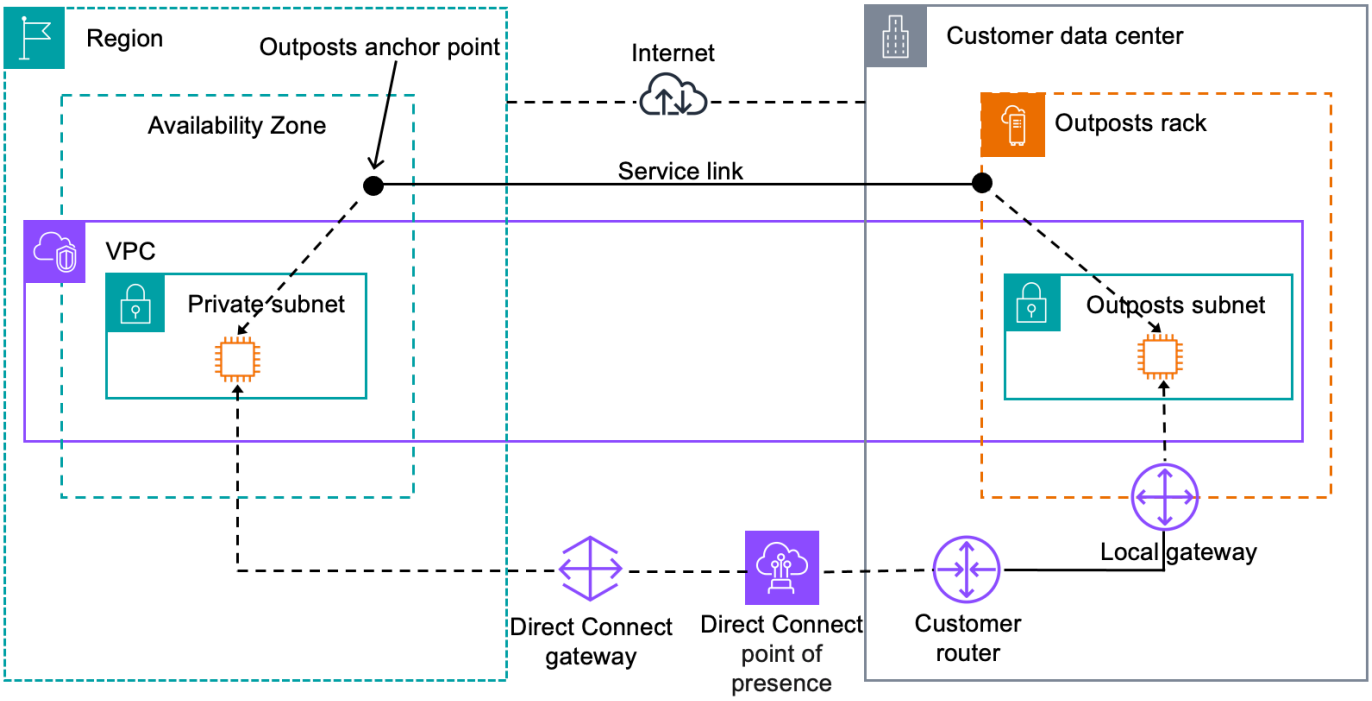


Tabla de enrutamiento de la puerta de enlace local

Las tablas de enrutamiento de subred de Outpost en un bastidor pueden incluir una ruta a la red en las instalaciones. La puerta de enlace local enruta este tráfico para enrutarlo de baja latencia a la red en las instalaciones.

De forma predeterminada, Outposts usa la dirección IP privada de las instancias de Outpost para comunicarse con su red en las instalaciones. Esto se conoce como enrutamiento directo de VPC para AWS Outposts (o enrutamiento directo de VPC). Sin embargo, puede proporcionar un rango de direcciones, conocido como grupo de direcciones IP (CoIP) propiedad del cliente, y hacer que las instancias de su red usen esas direcciones para comunicarse con la red en las instalaciones. El enrutamiento directo de VPC y el CoIP son opciones que se excluyen mutuamente y el enrutamiento funciona de manera diferente según su elección.

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 Outpost. Este tipo de enrutamiento es el modo predeterminado para Outposts. En este modo, la puerta de enlace local no realiza la NAT para las instancias y no es necesario asignar direcciones IP elásticas a las instancias de EC2. 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 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

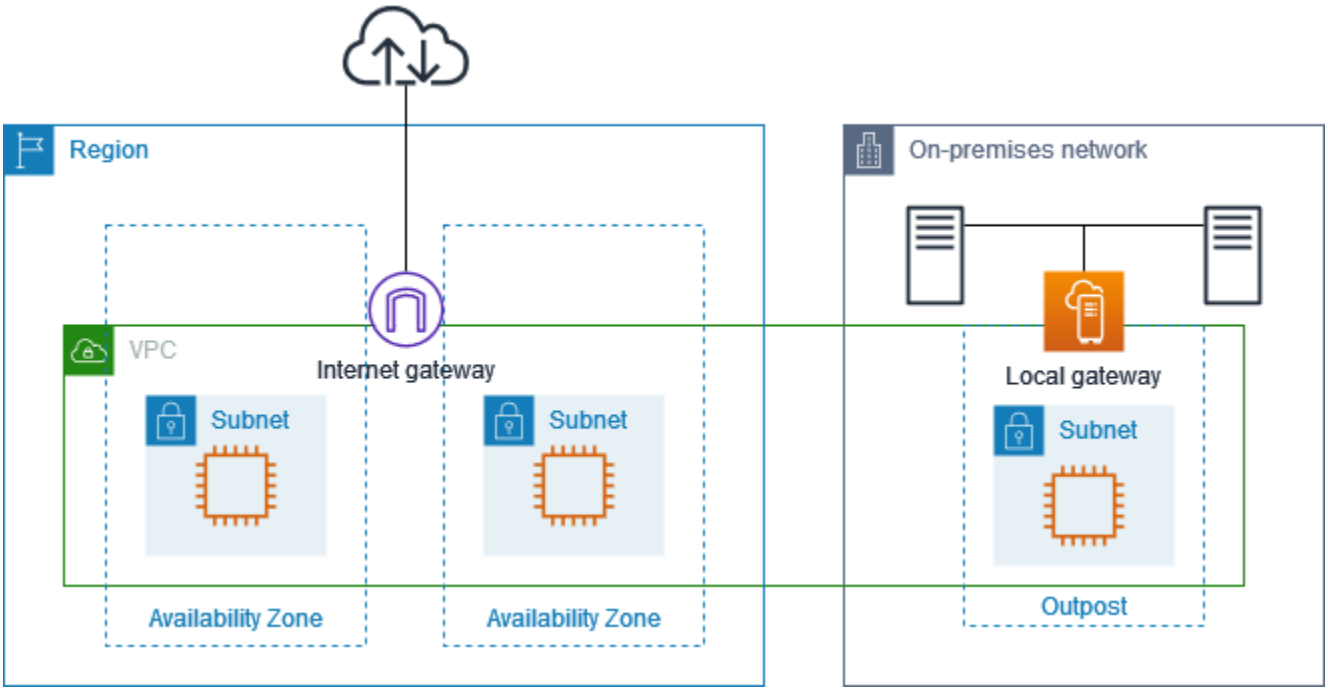
Las instancias de una subred de Outpost pueden acceder a Internet a través de la puerta de enlace de Internet conectada a la VPC.

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
CIDR DE VPC	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.
Red CIDR en las instalaciones	*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

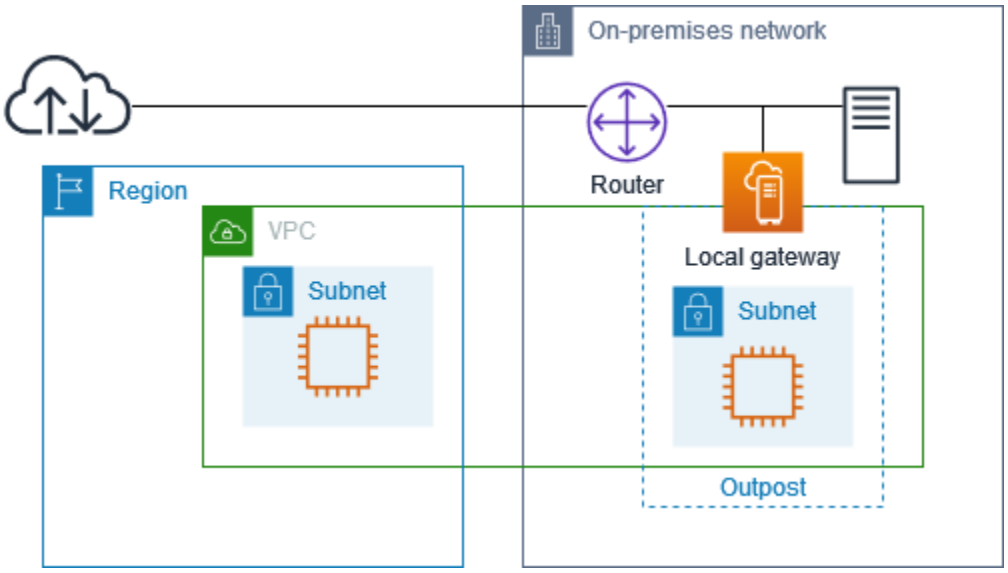
Las instancias de una subred de Outpost pueden acceder a Internet a través de la red en las instalaciones. Las instancias de la subred Outpost no necesitan una dirección IP pública o una dirección IP elástica.

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	
CIDR DE VPC	Local	Proporciona conectividad entre las subredes de la VPC.	

Destino	Objetivo	Comentarios	
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. Puede asignar estas direcciones IP a los recursos de su Outpost, como las instancias de EC2, asignando una nueva dirección IP elástica del grupo de IP propiedad

del cliente y, a continuación, asignándola a su recurso. Para obtener más información, consulte the section called “3f: (opcional) Asigne una dirección IP propiedad del cliente a la instancia”.

Los siguientes requisitos se aplican al conjunto de direcciones IP propiedad del cliente:

- Debe poder enrutar la dirección en su red
- El bloque CIDR debe tener un mínimo de /26

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 miembros de su organización mediante. Cuentas de AWS 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 instancia EC2 en Outpost. Para obtener más información, consulte Cómo compartir los recursos de AWS en la Guía del usuario de AWS RAM .

Ejemplos

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

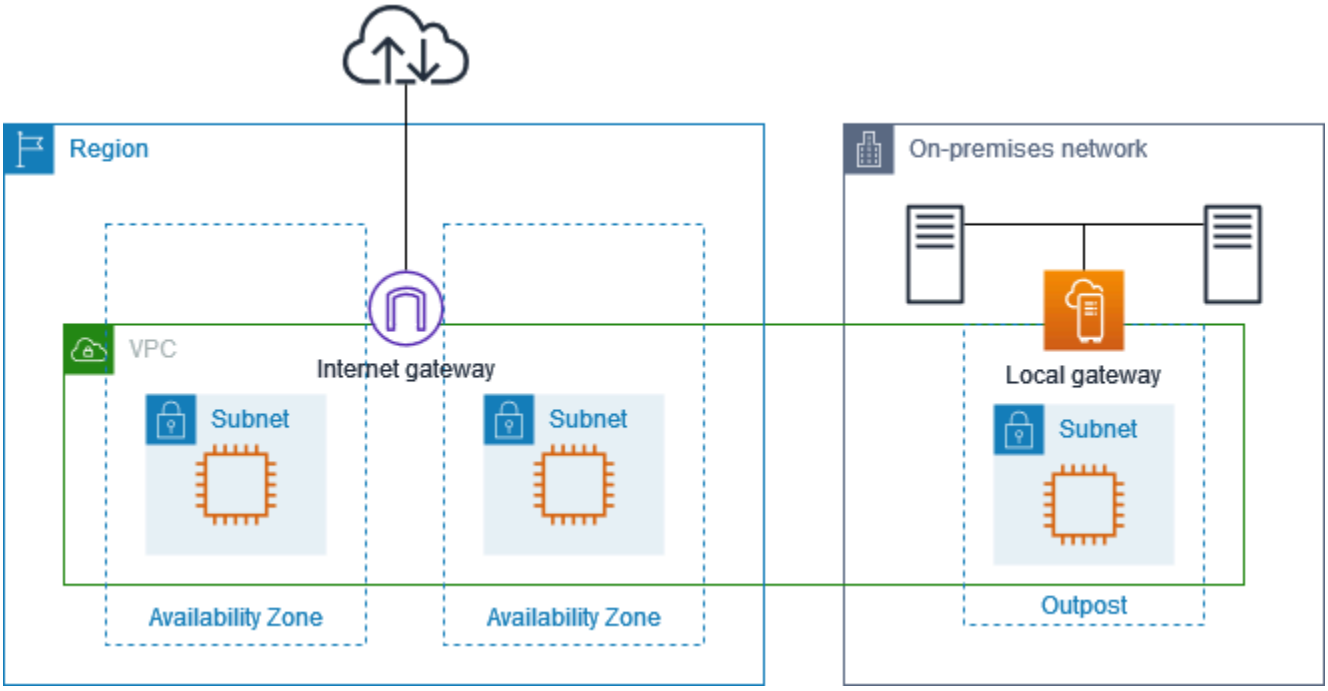
Ejemplo: conectividad a Internet a través de la VPC

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 instancia EC2.
- 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.

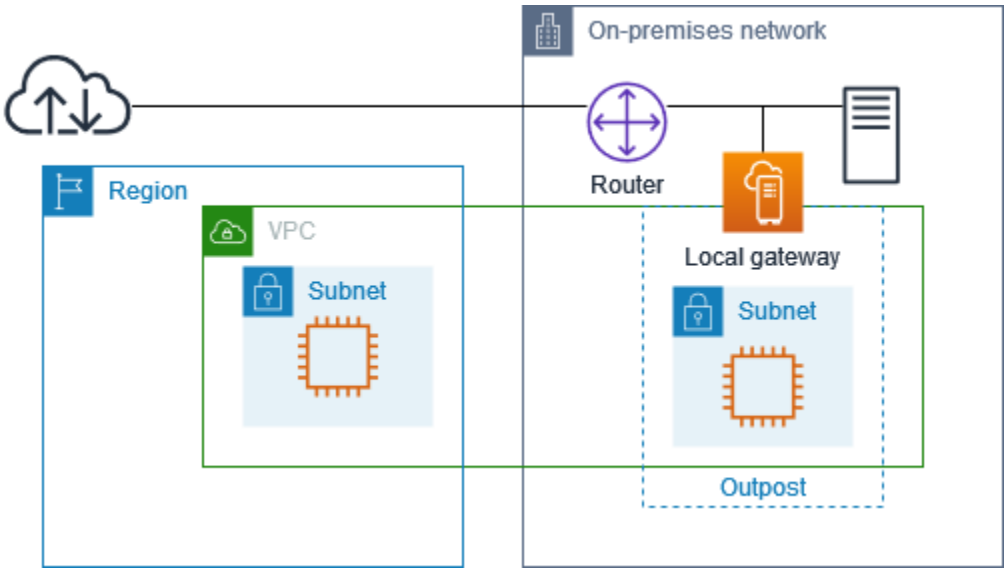
Destino	Objetivo	Comentarios
CIDR DE VPC	Local	Proporciona conectividad entre las subredes de la VPC.
0.0.0.0	*internet-gateway-id*	Envía el tráfico que tenga como destino la puerta de enlace de Internet pública.
Red CIDR en las instalaciones	*local-gateway-id*	Envía el tráfico destinado a la red en 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
CIDR DE VPC	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 EC2 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 instancia EC2 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 traduce la dirección IP de la instancia EC2 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.

Trabajo con tablas de enrutamiento de puerta de enlace local

Como parte de la instalación en rack, AWS crea la puerta de enlace local, configura los VIF y un grupo de VIF. 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. Tenga en cuenta la siguiente información sobre las tablas de enrutamiento de las puertas de enlace locales:

- Los grupos de VIF y las tablas de enrutamiento de las puertas de enlace locales deben tener una relación. one-to-one
- La puerta de enlace local es propiedad de la AWS cuenta asociada al Outpost y solo el propietario puede modificar la tabla de rutas de la puerta de enlace local.

- 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 Trabajo con recursos compartidos de AWS Outposts.
- Las tablas de enrutamiento de las puertas de enlace locales tienen un modo que determina si se debe usar la dirección IP privada de las instancias para comunicarse con la red en las instalaciones (enrutamiento directo de VPC) o con un grupo de direcciones IP propiedad del cliente (CoIP). El enrutamiento directo de VPC y el CoIP son opciones que se excluyen mutuamente y el enrutamiento funciona de manera diferente según su elección. Para obtener más información, consulte ???.
- El modo de enrutamiento directo de VPC no admite rangos de CIDR superpuestos.

Tareas

- Visualización de detalles de la tabla de enrutamiento de la puerta de enlace local
- Cree la tabla de enrutamiento de la puerta de enlace local personalizada
- Administrar las tablas de enrutamiento de puerta de enlace local
- Administrar las etiquetas de las tablas 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
- Administrar grupos de CoIP
- Asociación de grupos VIF
- Asociaciones de VPC

Visualización de detalles de la tabla de enrutamiento de la puerta de enlace local

Puede ver los detalles de las tablas de enrutamiento de puerta de enlace local mediante la consola o la AWS CLI.

AWS Outposts console

Para ver detalles de la tabla de enrutamiento de la puerta de enlace local

1. Abre 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. Seleccione la tabla de enrutamiento de la puerta de enlace local y, a continuación, elija Acciones, Ver detalles.

AWS CLI

Visualización de detalles de la tabla de enrutamiento de la puerta de enlace local

Utilice el comando describe-local-gateway-route-tables AWS CLI .

Ejemplo

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

Salida

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

> **Note**
>
> Si la tabla de enrutamiento de la puerta de enlace local predeterminada que está viendo utiliza el modo CoIP, la tabla de enrutamiento de la puerta de enlace local se configura con una ruta predeterminada a cada uno de los VIF y una ruta propagada a cada dirección IP asociada propiedad del cliente en el conjunto de CoIP del grupo.

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.
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 Key (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.

Administrar las tablas 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 elásticas de su Outpost. También puede modificar la ruta de entrada de una puerta de enlace local existente para cambiar la interface de red elástica de destino.

Una ruta está en estado activo solo cuando su interfaz de red elástica 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.

Los siguientes requisitos y limitaciones se aplican a una puerta de enlace local:

- La interfaz elastic network 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 instancia de Amazon EC2 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 interface de red elástica 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 los ENI que están conectados a las instancias de Outpost pueden comunicarse a través de la puerta de enlace local de ese Outpost. Los ENI que pertenecen a la subred del Outpost pero están conectados 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, como los puntos de conexión o las interfaces de VPCE, en las instalaciones a través de la puerta de enlace local. Solo se puede acceder a ellos desde instancias que se encuentren dentro del Outpost.

Tenga en cuenta las siguientes consideraciones NAT.

- La puerta de enlace local no realiza la NAT en el tráfico que coincide con una ruta de interface de red elástica. En cambio, se conserva la dirección IP de destino.

- Deshabilite la comprobación de origen/destino de la interfaz de red elástica de destino. Para más información, consulte Conceptos básicos de la interfaz de red en la Guía del usuario de Amazon EC2 para instancias Linux.
- Configure el sistema operativo para permitir que el tráfico del CIDR de destino se acepte en la interfaz de red.

AWS Outposts console

Para editar una las tabla de enrutamiento de puerta de enlace local

1. Abre 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. Seleccione la tabla de enrutamiento de la puerta de enlace local y, a continuación, elija Acciones, Editar rutas.
5. Para agregar una ruta, elija Añadir ruta. En Destino introduzca el bloque de CIDR de destino, una única dirección IP o el ID de una lista de prefijos.
6. Para modificar una ruta existente, para Destino, sustituya el bloque de CIDR de destino o la dirección IP única. En Objetivo, elija un objetivo.
7. Elija Guardar rutas.

AWS CLI

Para crear una ruta de la tabla de enrutamiento de puerta de enlace local

- Usa el comando. create-local-gateway-route AWS CLI

Ejemplo

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

Salida

```
{
    "Route": {
        "DestinationCidrBlock": "192.0.2.0/24",
        "NetworkInterfaceId": "eni-03e612f0a1EXAMPLE",
        "Type": "static",
        "State": "active",
        "LocalGatewayRouteTableId": "lgw-rtb-059615ef7dEXAMPLE",
        "LocalGatewayRouteTableArn": "arn:aws:ec2:us-west-2:111122223333:local-
gateway-route-table/lgw-rtb-059615ef7dEXAMPLE",
        "OwnerId": "111122223333"
    }
}
```

Para modificar una las tabla de enrutamiento de puerta de enlace local

Puede modificar la interfaz de red elástica a la que apunta una ruta existente. Para utilizar la operación de modificación, la tabla de enrutamiento ya debe tener una ruta con el bloque CIDR de destino especificado.

- Usa el modify-local-gateway-route AWS CLI comando.

Ejemplo

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

Salida

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

```
}
```

Administrar las etiquetas de las tablas de enrutamiento de puerta de enlace local

Puede etiquetar sus tablas de enrutamiento de la puerta de enlace local como ayudarlo a identificarlas o clasificarlas según las necesidades de su organización.

Para administrar las etiquetas de las tablas 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 de la puerta de enlace local y, a continuación, elija Acciones, Gestionar rutas.
5. Añada o elimine una etiqueta.

   Para 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.

   Para eliminar una etiqueta, elija Eliminar a la derecha de la clave y valor de la etiqueta.
6. Elija Guardar cambios.

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. Abre 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 de la puerta de enlace local y, a continuación, elija Acciones, Eliminar tabla de enrutamiento de la puerta de enlace local.
5. En el cuadro de diálogo de confirmación, escriba **`delete`** y elija Eliminar.
6. (Opcional) Cree una tabla de enrutamiento de puerta de enlace local con un modo nuevo.

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

    b. 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.

Administrar grupos 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. Para cambiar entre los modos de la tabla de enrutamiento de la puerta de enlace local, consulte Cambiar los modos de la tabla de enrutamiento de la puerta de enlace local.

Utilice el siguiente procedimiento para crear un grupo de CoIP.

Para crear un grupo CoIP

1. Abre 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) Añada o elimine bloques de CIDR

   [Agregar bloque CIDR] Seleccione Agregar nuevo CIDR e introduzca un rango de direcciones IP propiedad del cliente.

   [Eliminar bloque CIDR] Seleccione Eliminar a la derecha de un bloque CIDR.
9. Elija Crear grupo CoIP.

Utilice el siguiente procedimiento para editar un grupo de CoIP.

Para editar un grupo de CoIP

1. Abre 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 Grupo de CoIP.
6. Elija Acciones, edite el grupo de CoIP.
7. Seleccione Agregar nuevo CIDR e introduzca un rango de direcciones IP propiedad del cliente.
8. (Opcional) Añada o elimine bloques de CIDR

   [Agregar bloque CIDR] Seleccione Agregar nuevo CIDR e introduzca un rango de direcciones IP propiedad del cliente.

   [Eliminar bloque CIDR] Seleccione Eliminar a la derecha de un bloque CIDR.
9. Seleccione Guardar cambios.

Utilice el siguiente procedimiento para administrar las etiquetas o añadir una etiqueta de nombre a un grupo de CoIP.

Para administrar las etiquetas de un grupo de CoIP

1. Abre 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 Grupo de CoIP.
6. Elija Acciones, Administrar etiquetas.
7. Añada o elimine una etiqueta.

   Para 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.

   Para eliminar una etiqueta, elija Eliminar a la derecha de la clave y valor de la etiqueta.
8. Elija Guardar cambios.

Utilice el siguiente procedimiento para eliminar un grupo de CoIP.

Para eliminar un grupo CoIP

1. Abre 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 Grupo de CoIP.
6. Elija Acciones, Eliminar grupo CoIP.
7. En el cuadro de diálogo de confirmación, escriba **`delete`** y elija Eliminar.

Asociación de grupos VIF

Los grupos VIF son agrupaciones lógicas de interfaces virtuales (VIF). Puede cambiar la tabla de enrutamiento de la puerta de enlace local a la que está asociado el grupo VIF. Al desasociar un grupo VIF de una tabla de enrutamiento de una puerta de enlace local, se eliminan todas las rutas de la tabla de enrutamiento e se interrumpe el tráfico de la red.

Para cambiar la asociación de un grupo de VIF

1. Abre 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 de asociación de grupos de VIF en el panel de detalles y, a continuación, elija Editar asociación de grupos de VIF.
6. Para la configuración de grupo VIF, realice una de las siguientes acciones:
   - Para asociar el grupo VIF a la tabla de enrutamiento de la puerta de enlace local, seleccione Asociar grupo de VIF y elija un grupo de VIF.
   - Para desasociar el grupo VIF de la tabla de enrutamiento de la puerta de enlace local, desactive Asociar grupo VIF.

   > **Important**
   >
   > Al desasociar un grupo VIF de la tabla de enrutamiento de la puerta de enlace local, se eliminan automáticamente todas las rutas e interrumpe el tráfico de la red.
7. Seleccione Guardar cambios.

Asociaciones de VPC

Asociar un VPC con su tabla de enrutamiento de puerta de enlace local. No están asociadas de forma predeterminada.

Crear una asociación de VPC

Utilice el siguiente procedimiento para asociar una VPC a una tabla de enrutamiento de puerta de enlace local.

Puede etiquetar de forma opcional su asociación para ayudarlo a identificarlo o clasificarlo en función de las necesidades de su organización.

AWS Outposts console

Para asociar una VPC

1. Abre 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) Añada o elimine una etiqueta.

   Para 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.

   Para eliminar una etiqueta, elija Eliminar a la derecha de la clave y valor de la etiqueta.
7. Elija Asociar VPC.

AWS CLI

Para asociar una VPC

Usa el comando create-local-gateway-route- table-vpc-association.

Ejemplo

```
aws ec2 create-local-gateway-route-table-vpc-association \
```

```
    --local-gateway-route-table-id lgw-rtb-059615ef7dEXAMPLE \
    --vpc-id vpc-07ef66ac71EXAMPLE
```

Salida

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

Para eliminar una asociación de VPC

Utilice el siguiente procedimiento para desasociar una VPC de una tabla de enrutamiento de puerta de enlace local.

AWS Outposts console

Para desasociar una VPC

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, Ver detalles.
5. En las Asociaciones de VPC, seleccione la VPC que desee disociar y, a continuación, elija Desasociar.
6. Elija Desasociar.

AWS CLI

Para desasociar una VPC

Usa el comando delete-local-gateway-route- table-vpc-association.

Ejemplo

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

Salida

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

Conectividad de red local para bastidores

Necesita los siguientes componentes para conectar su bastidor Outpost a la 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-point Conectividad 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 Outpost tiene dos dispositivos de red físicos que se conectan a la red local.

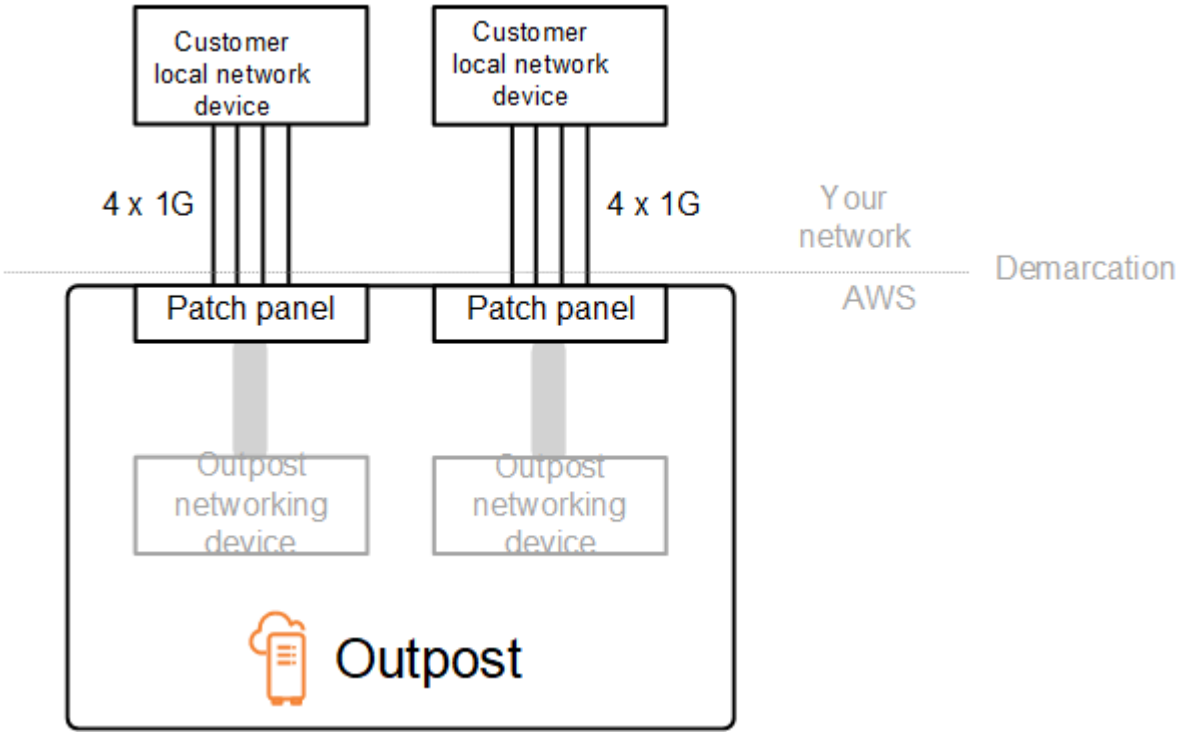
Un Outpost requiere un mínimo de dos enlaces físicos entre estos dispositivos de red Outpost y sus dispositivos de red local. Un Outpost admite las siguientes velocidades y cantidades de enlace ascendente para cada dispositivo de red Outpost.

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 bastidores de Outpost admiten fibra monomodo (SMF) con Lucent Connector (LC), fibra multimodo (MMF) o MMF OM4 con LC. AWS proporciona la óptica compatible con la fibra que se proporciona en la posición de los bastidores.

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

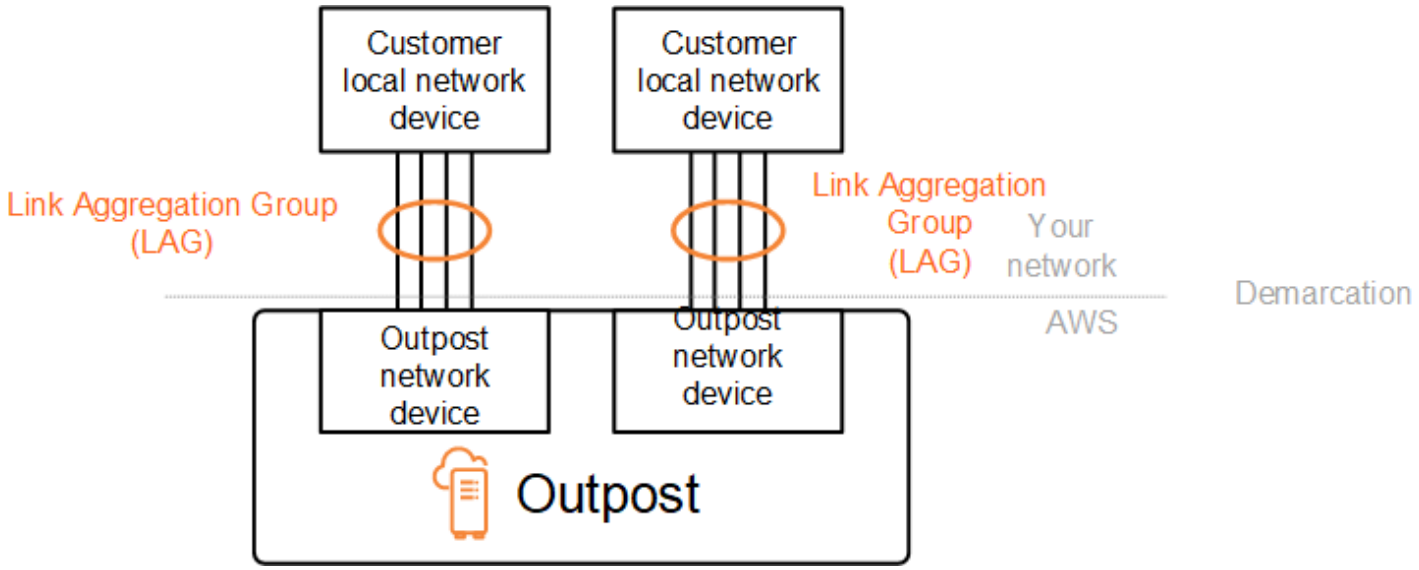
AWS Outposts usa el Protocolo de control de agregación de enlaces (LACP) para establecer dos conexiones de grupos de agregación de enlaces (LAG), uno por cada res Outpost y a cada dispositivo de red local. Los enlaces de cada dispositivo de red Outpost se agregan en un LAG Ethernet para representar una única conexión de red. Estos LAG utilizan el LACP con temporizadores rápidos estándar. No puede configurar los LAG para que usen 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 bastidores, un Outpost debe tener cuatro LAG entre la capa de agregación de los dispositivos de red de 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 los LAG de Ethernet para agregar los enlaces físicos que conectan los dispositivos de red Outpost y los dispositivos de la red local del cliente.



LAN virtuales

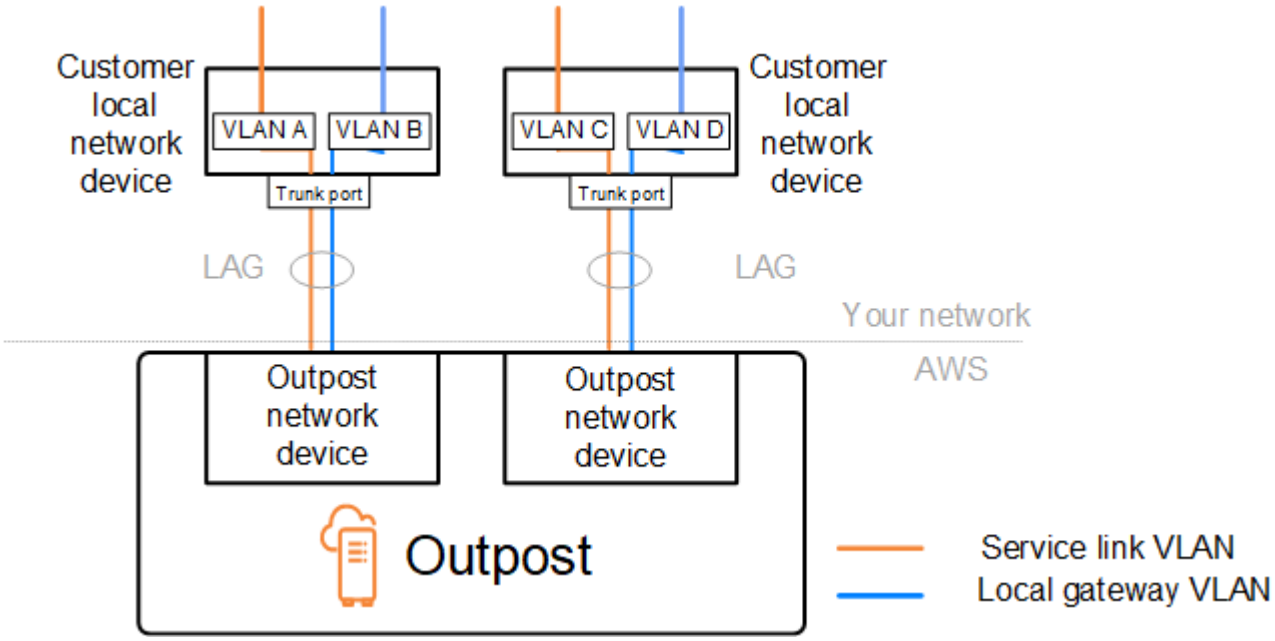
Cada LAG entre un dispositivo de red Outpost y un dispositivo de red local debe configurarse como un enlace troncal Ethernet IEEE 802.1q. Esto permite el uso de varias VLAN para la división de la red entre las rutas de datos.

Cada Outpost tiene las siguientes VLAN para comunicarse con los dispositivos de la red local:

- VLAN de enlace de servicio: permite la comunicación entre su Outpost y los dispositivos de su red local para establecer una ruta de enlace de servicio para la conectividad del enlace de servicio. Para obtener más información, consulte AWS OutpostsConectividad con las AWS regiones.
- VLAN de puerta de enlace local: permite la comunicación entre su Outpost y los dispositivos de su 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 aprovecha esta VLAN para proporcionar a las instancias la conectividad con la red local, lo que puede incluir el acceso a Internet a través de la red. Para obtener más información, consulta 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 la red Outpost. AWS administra cualquier infraestructura del lado AWS de la conexión y usted administra cualquier infraestructura del lado de la línea.



Para integrar su Outpost con su red en las instalaciones durante la instalación y el funcionamiento continuo, debe asignar las VLAN utilizadas entre los dispositivos de red Outpost y los dispositivos de red local del cliente. Debe proporcionar esta información a AWS antes de la instalación. 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 (VIF) que incluyen la dirección IP de cada VLAN. A través de estas VIF, los dispositivos AWS Outposts de 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 conecte las VLAN entre los dispositivos de la red local.

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

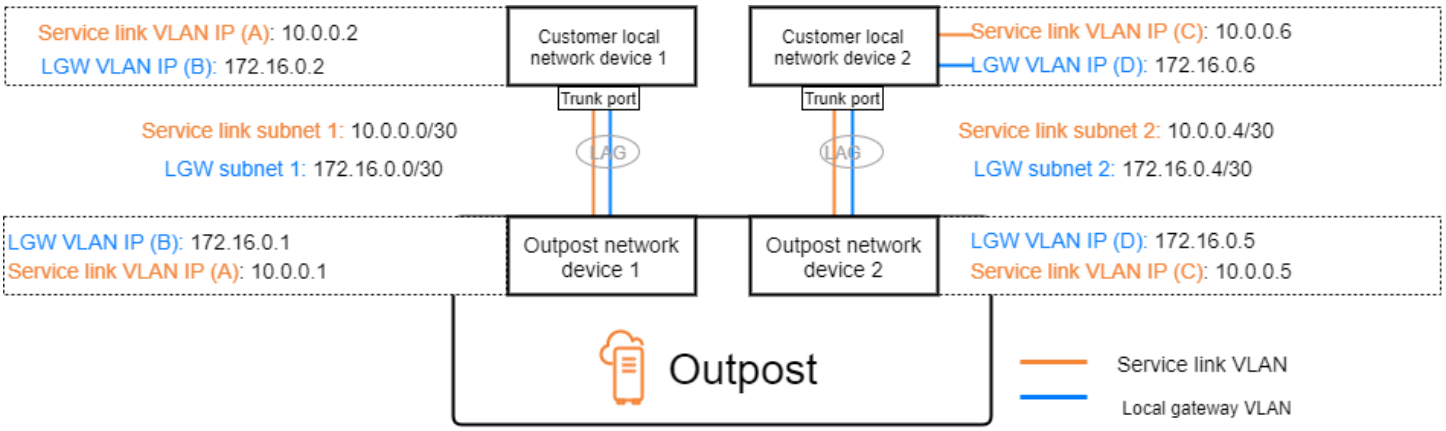
- Ruta de enlace de servicio: para establecer esta ruta, especifique una subred de VLAN con un rango de /30 o /31 y una dirección IP para cada VLAN de enlace de servicio del dispositivo de red. AWS Outposts Las interfaces virtuales (VIF) de enlace de servicio se utilizan en esta ruta para

establecer la conectividad IP y las sesiones de BGP entre su Outpost y los dispositivos de la red local para la conectividad del enlace de servicio. Para obtener más información, consulte AWS OutpostsConectividad con las regiones. AWS

- Ruta de la 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 la puerta de enlace local en el dispositivo de red. AWS Outposts Los VIF de la puerta de enlace local se utilizan en esta ruta para establecer la conectividad IP y las sesiones de BGP entre el 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. Para este ejemplo, hay cuatro VLAN:

- 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 OND 1 IP
A	10.0.0.0/30	10,00.2	10.0.0.1
B	17216,0,0/30	172216,02	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 OND 2 IP
C	10,0,4/30	10.0.0.6	10.0.0.5
D	17216,0,4/30	1722160,6	172.16.0.5

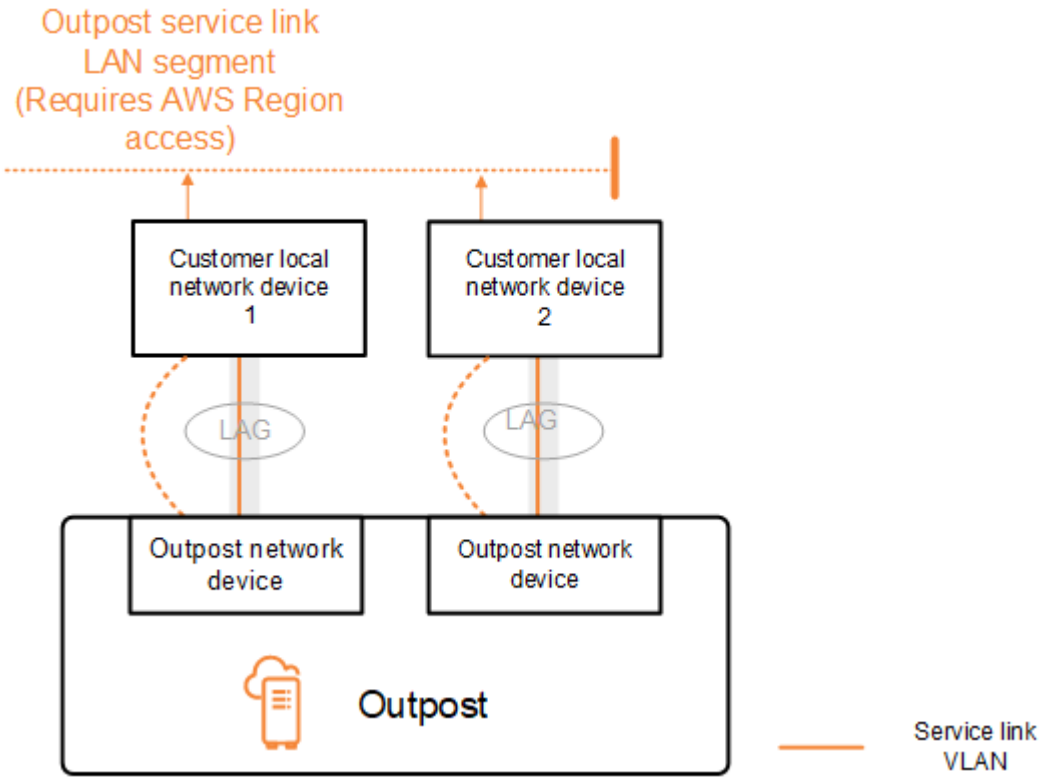
Conectividad BGP de Service Link

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. AWS proporciona los atributos como parte del proceso de 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 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 de AS-Path de 1, además de los prefijos /27 de todos los demás OND con una longitud de AS-Path de 4.
3. La subred se utiliza para la conectividad entre el Outpost 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 de clientes debe anunciar prefijos BGP iguales con los mismos atributos en todos los OND. El equilibrador de carga de red de Outpost equilibra el tráfico saliente entre todos los enlaces superiores de forma predeterminada. Las políticas de enrutamiento se utilizan en el lado del Outpost para desviar el tráfico de un OND si es necesario realizar tareas de mantenimiento. Este cambio de tráfico requiere la misma cantidad de prefijos de BGP por parte del cliente en todos los OND. 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 establece un emparejamiento BGP externo desde cada dispositivo de red Outpost a un dispositivo de red local para la conectividad con la puerta de enlace local. Utiliza un número de sistema autónomo (ASN) privado que usted asigna para establecer las sesiones 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.

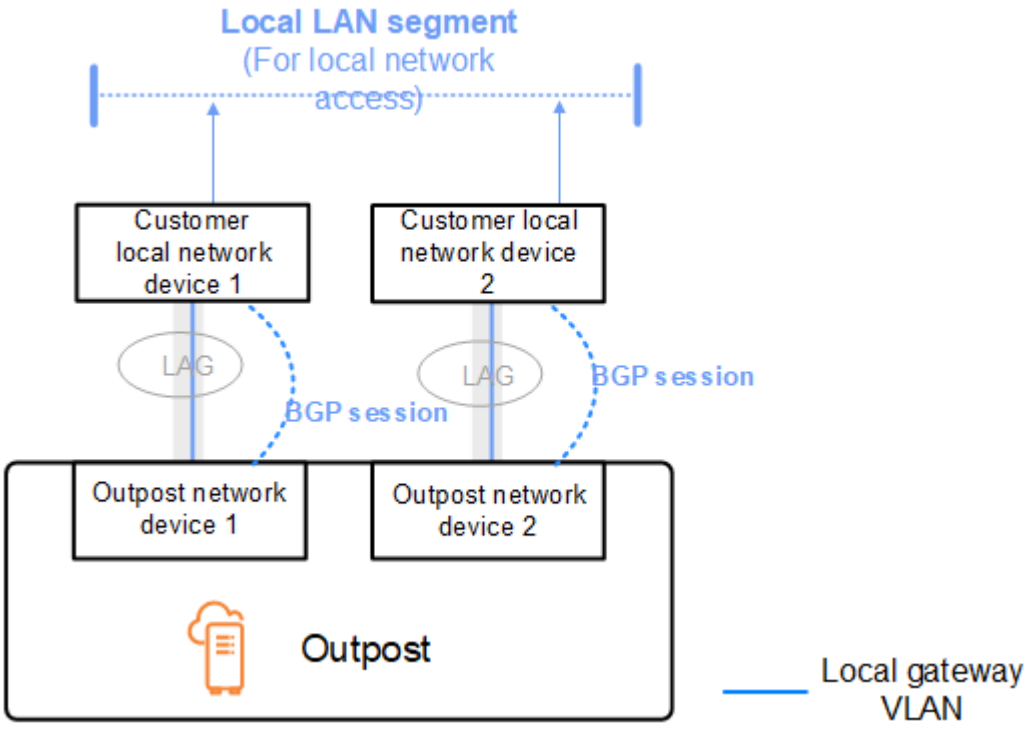
El Outpost establece una sesión de interconexión BGP externa a través de la VLAN de la puerta de enlace local entre cada dispositivo de red Outpost y el dispositivo de red local del cliente conectado.

La sesión de emparejamiento se establece entre las IP /30 o /31 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 la red local del cliente. AWS proporciona 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:

- AWS 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. La técnica AS-Path Prepending se utiliza para los prefijos de las puertas de enlace locales a fin de desviar el tráfico de los OND en caso de que sea 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 de clientes debe anunciar prefijos BGP iguales con los mismos atributos en todos los OND. El equilibrador de carga de red de Outpost equilibra el tráfico saliente entre todos los enlaces superiores de forma predeterminada. Las políticas de enrutamiento se utilizan en el lado del Outpost para desviar el tráfico de un OND si es necesario realizar tareas de mantenimiento. Este cambio de tráfico requiere la misma cantidad de prefijos de BGP por parte del cliente en todos los OND. 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

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 grupo de direcciones IP (CoIP) que son propiedad del cliente (CoIP).

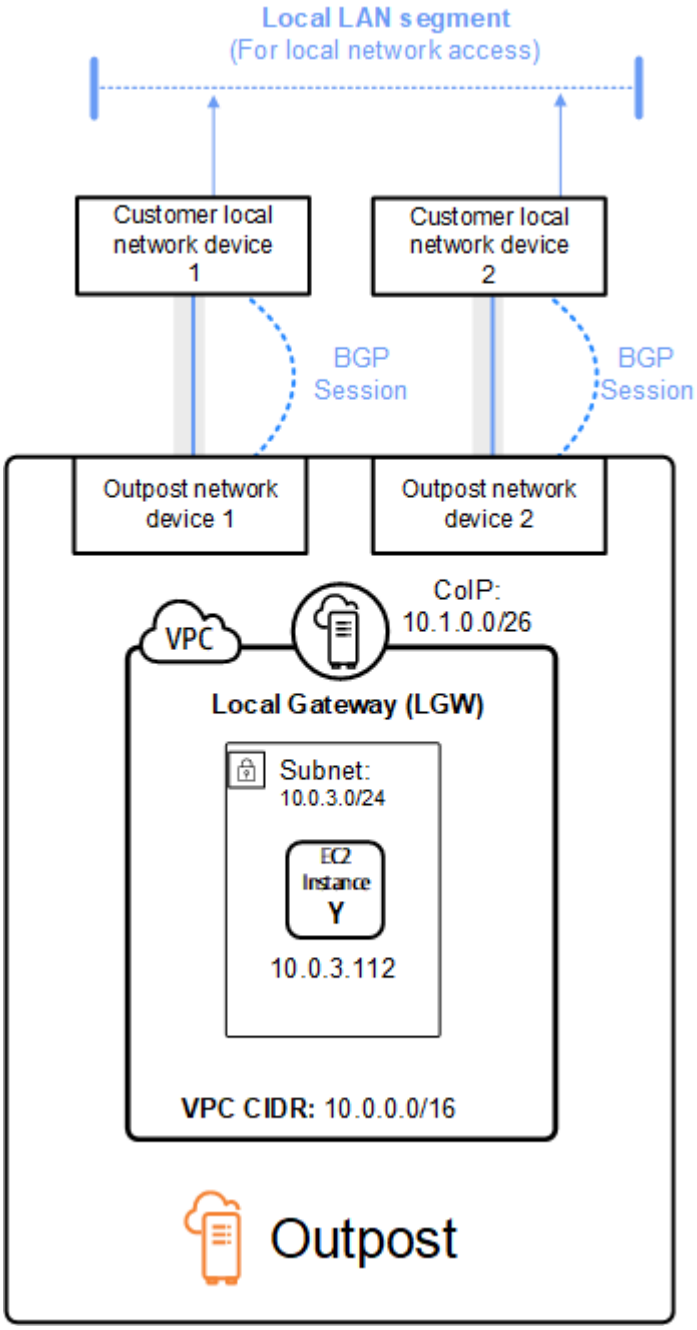
Si elige CoIP, AWS crea el conjunto a partir de la información que proporcione durante el proceso de instalación. Puede crear direcciones IP elásticas a partir de este grupo y, a continuación, asignarlas a los recursos de su Outpost, como las instancias EC2.

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 instancia de EC2 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 en las instalaciones utilizará las IP elásticas de CoIP 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

Trabajar con recursos de AWS Outposts compartidos

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

Para este modelo, la cuenta de AWS propietaria de los recursos de Outpost (propietario) comparte los recursos con otras cuentas de AWS (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 lanzan 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:

- Cuentas de AWS específicas dentro de la 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.

Estos son los recursos disponibles para los servidores en de Outpost. Para obtener información sobre los recursos del servidor, consulte Cómo trabajar con recursos de AWS Outposts compartidos en la Guía del usuario de AWS Outposts para los servidores de Outposts.

- Hosts dedicados asignados: los consumidores con acceso a este recurso pueden:
  - Lance y ejecute instancias EC2 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.
  - Utilice la API de AWS Outposts 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.
  - Lance y ejecute instancias EC2 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, debe ser propietario de ese recurso en su cuenta de AWS. 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 uso compartido de recursos de Outpost se integra con AWS Resource Access Manager (AWS RAM). AWS RAM es un servicio que le permite compartir sus recursos de AWS con cualquier cuenta de AWS o a través de AWS Organizations. 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 cuentas de AWS individuales, unidades organizativas o toda una organización de AWS Organizations.

Para obtener más información sobre AWS RAM, consulte la Guía del usuario de AWS RAM.

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 de disponibilidad `us-east-1a` de su cuenta de AWS no se encuentre en la misma ubicación de `us-east-1a` que otra cuenta de AWS.

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 AZ es un identificador único y coherente para una zona de disponibilidad en todas las cuentas de AWS. Por ejemplo, `use1-az1` es un ID de AZ para la región `us-east-1` y está en la misma ubicación en todas las cuentas de AWS.

Para ver los ID de AZ para las zonas de disponibilidad de su cuenta

1. Abra la consola de AWS RAM en https://console.aws.amazon.com/ram.
2. Los ID de AZ de la región actual se muestran en el panel Su ID de zona de disponibilidad en el lado derecho 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 uso compartido de recursos es un recurso de AWS RAM que le permite compartir los recursos a través de cuentas de AWS. Un uso compartido de recursos especifica los recursos que compartir y los consumidores con quienes se comparten. Cuando se comparte un recurso de Outpost mediante el uso de la consola

de AWS Outposts, la agrega a un uso compartido de recurso 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 forma parte de una organización de AWS Organizations y esta permite el uso compartido, puede conceder a los consumidores de la organización acceso desde la consola de AWS RAM 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.

Puede compartir un recurso de Outpost del cual es propietario mediante el uso de la consola de AWS Outposts, de la consola de AWS RAM o AWS CLI.

Cómo compartir un Outpost del cual es propietario mediante el uso de la consola de AWS Outposts

1. Abra la consola de AWS Outposts 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 consola de AWS RAM 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.

Cómo compartir una tabla de enrutamiento de Outpost o una puerta de enlace local que sea de su propiedad mediante AWS CLI

Utilice el comando create-resource-share.

Dejar de compartir un recurso de Outpost compartido

Cuando se deja de compartir un Outpost compartido, los consumidores ya no pueden verlo en la consola de AWS Outposts. No pueden crear nuevas subredes en Outpost, nuevos volúmenes de

EBS en Outpost ni ver los detalles y los tipos de instancias de Outpost mediante la consola de AWS Outposts o la de AWS CLI. Las subredes, los volúmenes o las instancias existentes creados por los consumidores no se eliminan. Todas las subredes existentes que los consumidores hayan creado en Outpost se pueden seguir utilizando para lanzar nuevas instancias.

Cuando una tabla de enrutamiento de una puerta de enlace local compartida no se comparte, los consumidores ya no pueden crear nuevas asociaciones de VPC con ella. Todas las asociaciones de VPC existentes que hayan creado los consumidores permanecen asociadas a la tabla de enrutamiento. Los recursos de estas VPC pueden seguir enrutando el tráfico a la puerta de enlace local.

Para dejar de compartir un recurso de Outpost de su propiedad, debe quitarlo del recurso compartido. Para ello, puede utilizar la consola de AWS RAM o la AWS CLI.

Cómo dejar de compartir un recurso de Outpost compartido de su propiedad mediante el uso de la consola de AWS RAM

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

Cómo dejar de compartir un Outpost compartido del cual es propietario mediante el uso de AWS CLI

Utilice el comando disassociate-resource-share.

Identificación de un recurso de Outpost compartido

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

Cómo identificar un Outpost compartido mediante el uso de la consola de AWS Outposts

1. Abra la consola de AWS Outposts 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, consulte el ID de propietario para identificar el ID de cuenta de AWS del propietario de Outpost.

Cómo identificar un recurso de Outpost compartido mediante el uso de la AWS CLI

Utilice los comandos list-outposts y describe-local-gateway-route-tables. El comando devuelve los recursos de Outpost que son de su propiedad y los que se comparten con usted. `OwnerId` muestra el ID de cuenta de AWS 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. Pueden utilizar AWS Organizations para ver, modificar y eliminar recursos que crean los consumidores 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 facturarán los gastos de transferencia de datos relacionados con el tráfico de la 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, como AWS Direct Connect y 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 facturables desde la región AWS.

Limitaciones

Se aplican las siguientes limitaciones al uso compartido de AWS Outposts:

- Las limitaciones de las subredes compartidas se aplican al uso compartido de AWS Outposts. 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. Usted también es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y los reglamentos 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. Usted es 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 datos, consulte Preguntas frecuentes sobre la privacidad de datos. Para obtener información sobre la protección de datos en Europa, consulte 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 y bastidores del Outpost.

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 Cifrado de Amazon EBS en la Guía del usuario de Amazon EC2.

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 enlaces 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 finalizar una instancia EC2, el hipervisor limpia la memoria que tiene asignada (la establece en cero) antes de asignarla a una instancia nueva. Además, se restablece cada bloque de almacenamiento.

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

Gestión de identidad y acceso (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 AWS recursos. 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

Funciones de IAM que puedes 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

Característica de IAM	AWS Soporte para Outposts
Claves de condición de política (específicas del servicio)	Sí
ACL	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 identidades	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 adjunto. Para 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

Políticas basadas en recursos dentro de Outposts AWS

Compatibilidad con las políticas basadas en recursos	No

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política en función de recursos. Los directores pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Para habilitar el acceso entre cuentas, puede especificar toda una cuenta o entidades de IAM de otra cuenta como la entidad principal de una política en función de recursos. Añadir a una política en función de recursos una entidad principal entre cuentas es solo una parte del establecimiento de una relación de confianza. Cuando el principal y el recurso son diferentes Cuentas de AWS, el administrador de IAM de la cuenta de confianza también debe conceder a la entidad principal (usuario o rol) permiso para acceder al recurso. Para conceder el permiso, adjunte la entidad a una política basada en identidad. Sin embargo, si la política en función de recursos concede el acceso a una entidad principal de la misma cuenta, no es necesaria una política basada en identidad adicional. Para más información, consulte Cómo los roles de IAM difieren de las políticas basadas en recursos en la Guía del usuario de IAM.

Acciones políticas para AWS Outposts

Admite 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

Admite 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 puede 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). Puede 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, utilice 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 única instrucción, separe los ARN con comas.

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

Para ver una lista de los tipos de recursos de AWS Outposts y sus ARN, 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

Admite 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 puede 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. Puede crear expresiones condicionales que utilicen 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 lógica `AND`. 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 puede utilizar variables de marcador de posición al especificar condiciones. Por ejemplo, puede 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, consulte 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

ACL en Outposts AWS

Admite las ACL	No

Las listas de control de acceso (ACL) controlan qué entidades principales (miembros de cuentas, usuarios o roles) tienen permisos para acceder a un recurso. Las ACL son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

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 ¿Qué es 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

Compatible con el uso de credenciales temporales	Sí

Algunas Servicios de AWS no funcionan cuando inicias sesión con credenciales temporales. Para obtener información adicional, incluidas las que 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 más información sobre el cambio de roles, consulte Cambio a un rol (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 más información, consulte Credenciales de seguridad temporales en IAM.

Permisos principales entre servicios para Outposts AWS

Admite Forward access sessions (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.

Roles de servicio para AWS Outposts

Compatible con funciones de servicio	No

Un rol de servicio es un rol de IAM que asume un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte Creación de un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.

Funciones vinculadas al servicio para Outposts AWS

Compatible con roles vinculados al servicio	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. Uso de roles vinculados a servicios de 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 puede agregar las políticas de IAM a roles, y los usuarios pueden 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 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 los ARN de cada uno de los tipos de recursos, consulte Acciones, recursos y claves de condición de la Referencia de AWS Outposts autorización de servicio.

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 costes 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, consulte las políticas administradas por AWS o las políticas administradas por AWS para funciones de trabajo en la Guía del 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, consulte 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, consulte Elementos de la política de JSON de IAM: Condición en la Guía del usuario de IAM.

- Utilice 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 Política de validación de Analizador de acceso de IAM en la Guía de 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 solicitar la MFA cuando se invocan las operaciones de la API, agregue las condiciones de la MFA a sus políticas. Para más información, consulte Configuración del acceso a una API protegido por MFA en la Guía de usuario de IAM.

Para obtener más información sobre las prácticas recomendadas de IAM, consulte las 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"
    }
  ]
}
```

Uso de roles vinculados a servicios de AWS Outposts

AWS Outposts usa roles vinculados al AWS Identity and Access Management servicio (IAM). Un rol vinculado a un servicio es un tipo único de rol de IAM al que se vincula directamente. AWS Outposts Los roles vinculados al servicio están predefinidos AWS Outposts e incluyen todos los permisos que el servicio requiere 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 pueda adjuntar 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.

Para obtener información acerca de otros servicios que admiten roles vinculados a servicios, consulte Servicios de AWS que funcionan con IAM y busque los servicios que muestran Sí en la columna Rol vinculado a un servicio. Seleccione una opción Sí con un enlace para ver la documentación relativa al rol vinculado al servicio en cuestión.

Permisos de roles vinculados a servicios de AWS Outposts

AWS Outposts usa el rol vinculado al servicio denominado AWSServiceRoleForOutposts_ ***OutPostID: permite a Outposts*** acceder a los AWS recursos para la conectividad privada en tu nombre. Este rol vinculado a un servicio permite la configuración de la conectividad privada, crea interfaces de red y las conecta a las instancias de punto de conexión del enlace de servicio.

El rol vinculado al servicio AWSServiceRoleForOutposts _ *OutpostID confía en* que los siguientes servicios asuman el rol:

- `outposts.amazonaws.com`

La función vinculada al servicio AWSServiceRoleForOutposts_ ***OutpostID incluye*** las siguientes políticas:

- AWSOutpostsServiceRolePolicy
- AWSOutpostsPrivateConnectivityPolicy_ OutpostID

La AWSOutpostsServiceRolePolicypolítica es una política de funciones vinculadas al servicio que 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 `all AWS resources`
- Acción: `ec2:DescribeSecurityGroups` en `all AWS resources`
- Acción: `ec2:CreateSecurityGroup` en `all AWS resources`
- Acción: `ec2:CreateNetworkInterface` en `all AWS resources`

La política AWSOutpostsPrivateConnectivityPolicy_ ***OutpostID*** permite AWS Outposts realizar las siguientes acciones en los recursos especificados:

- Acción: `ec2:AuthorizeSecurityGroupIngress` en `all AWS resources that match the following Condition:`

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

- Acción: `ec2:AuthorizeSecurityGroupEgress` en `all AWS resources that match the following Condition:`

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

- Acción: `ec2:CreateNetworkInterfacePermission` en `all AWS resources that match the following Condition:`

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

- Acción: `ec2:CreateTags` en `all AWS resources that match the following Condition:`

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

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.

Creación de un rol vinculado a un servicio de 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 Conectividad privada del enlace de servicio mediante el uso de VPC.

Modificación de un rol vinculado a servicios de AWS Outposts

AWS Outposts no le permite editar la función vinculada al *servicio AWSServiceRoleForOutposts _ OutpostID*. Después de crear un rol vinculado al servicio, no podrá cambiar el nombre del rol, ya que varias entidades podrían hacer referencia al rol. Sin embargo, sí puede editar la descripción del rol con IAM. Para obtener más información, consulte Modificación de un rol vinculado a servicios en la Guía del usuario de IAM..

Eliminación de un rol vinculado a un servicio de 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.

> **Note**
>
> 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.

> **Warning**
>
> Debes eliminar tu Outpost para poder eliminar el rol AWSServiceRoleForOutposts _ *`OutpostID`* vinculado al servicio. El siguiente procedimiento elimina su Outpost.

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

Para eliminar AWS Outposts los recursos utilizados por AWSServiceRoleForOutposts _ OutpostID

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

Cómo eliminar manualmente el rol vinculado a servicios mediante IAM

Utilice la consola de IAM AWS CLI, la o la AWS API para eliminar la función vinculada al *`servicio AWSServiceRoleForOutposts _ OutpostID.`* Para obtener más información, consulte Eliminar un rol vinculado a un servicio en la Guía del usuario de IAM.

Regiones admitidas para los roles vinculados a un servicio de AWS Outposts

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, consulte Puntos de conexión y cuotas de AWS 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 por AWS en la Guía del usuario de IAM.

AWS política gestionada: AWSOutpostsServiceRolePolicy

Esta política está asociada a un rol vinculado al servicio que permite AWS Outposts realizar acciones en su nombre. Para obtener más información, consulte Uso de roles vinculados a servicios.

AWS política gestionada: AWSOutpostsPrivateConnectivityPolicy

Esta política está asociada a un rol vinculado al servicio que permite AWS Outposts realizar acciones en su nombre. Para obtener más información, consulte Uso de roles vinculados a servicios.

AWS Outposts actualizaciones de las políticas AWS gestionadas

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

Cambio	Descripción	Fecha
AWS Outposts comenzó a rastrear los cambios	AWS Outposts comenzó a realizar un seguimiento de los cambios de 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 puede 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 instancias de EC2 y los volúmenes de EBS que se ejecutan en su Outpost, consulte Seguridad de infraestructura en 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 Outpost 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 equilibrador de carga de aplicación 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:

- Guías de inicio rápido sobre seguridad y cumplimiento: estas guías de implementación analizan las consideraciones arquitectónicas y proporcionan los pasos para implementar entornos básicos centrados en AWS la seguridad y el cumplimiento.
- Diseño de arquitectura para garantizar la seguridad y el cumplimiento de la HIPAA en Amazon Web Services: en este documento técnico se describe cómo pueden utilizar AWS las empresas para crear aplicaciones aptas para la HIPAA.

  > **Note**
  >
  > No Servicios de AWS todas cumplen con los requisitos de la HIPAA. Para más información, consulte la Referencia de servicios compatibles con 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.

- AWS Audit Manager— Esto le Servicio de AWS ayuda a auditar continuamente su AWS consumo 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 AWS región matriz

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 realizarse a través de la puerta de enlace NAT instanciada en la 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 Outposts, consulte Tablas de enrutamiento de la puerta de enlace local.

Consideraciones

- Use esta opción cuando:
  - Necesita flexibilidad para proteger el tráfico de Internet con varios AWS servicios en la AWS región.
  - No tiene un punto de presencia de Internet en su centro de datos o instalación de ubicación conjunta.
- 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 hasta el puesto avanzado conlleva gastos. Para obtener más información sobre la transferencia de datos, consulte los precios bajo demanda de Amazon EC2.
- Aumentará la utilización del ancho de banda del enlace de servicio.

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 tu 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 Outposts, consulte Tablas de enrutamiento de la puerta de enlace local.

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.
- Tu 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 CIDR de Outposts no entren en conflicto con los CIDR locales.
- 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 finales 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 tu centro de datos local.

Monitorice su Outpost

AWS Outposts se integra con los siguientes servicios que ofrecen funciones de monitorización y registro:

CloudWatch métricas

Usa Amazon CloudWatch para recuperar estadísticas sobre los puntos de datos de tus 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 métricas para AWS Outposts.

CloudTrail registros

Utilice AWS CloudTrail para recopilar información detallada sobre las llamadas realizadas a la API de AWS. 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 APIAWS 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 AWS Outpostsinformación en 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

Utilice la duplicación de tráfico para copiar y reenviar el tráfico de red de Outpost a los dispositivos de out-of-band seguridad y supervisión de Outpost. Puede utilizar el tráfico reflejado para inspeccionar el contenido, supervisar las amenazas o solucionar problemas. Para obtener más información, consulte Guía de duplicación de tráfico para Amazon Virtual Private Cloud.

AWS Health Dashboard

El AWS Health Dashboard muestra información y notificaciones que se inician por cambios en la salud de los recursos de 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 servicio de AWS Health, AWS Health Dashboard no requiere ninguna configuración y cualquier usuario autenticado en su cuenta puede consultarlo. Para obtener más información, consulte Introducción a AWS Health Dashboard.

CloudWatch métricas para AWS Outposts

AWS Outpostspublica 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 problemas del tipo `ConnectedStatus`, le recomendamos que compruebe la conectividad con la región de AWS desde su red en las instalaciones y que se ponga 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 al respecto CloudWatch, consulta la Guía del CloudWatch usuario de Amazon.

Contenido

Métricas de Outpost

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 (VIF) de Outposts 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 las VIF de las puertas de enlace locales (lgw-vif):, y `OutpostsId` `VirtualInterfaceGroupId` `VirtualInterfaceId`

Dimensiones de los VIF de enlace de servicio (sl-vif): y `OutpostsId` `VirtualInterfaceId`

`IfTrafficOut`

La velocidad de bits de los datos que las interfaces virtuales (VIF) de Outposts 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 las VIF de las puertas de enlace locales (lgw-vif):, y `OutpostsId` `VirtualInterfaceGroupId` `VirtualInterfaceId`

Dimensiones de los VIF de enlace de servicio (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: y `InstanceFamily` `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 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 disponibles en el Outpost para reservas de capacidad bajo demanda (ODCR). Esta métrica no mide instancias reservadas de Amazon EC2.

Unidad: recuento

Resolución máxima: 5 minutos

Dimensiones: `InstanceType` y `OutpostId`

`UsedReservedInstances`

El número de instancias disponibles en el Outpost para reservas de capacidad bajo demanda (ODCR). Esta métrica no mide instancias reservadas de Amazon EC2.

Unidad: recuento

Resolución máxima: 5 minutos

Dimensiones: `InstanceType` y `OutpostId`

`TotalReservedInstances`

El número de instancias disponibles en el Outpost para reservas de capacidad bajo demanda (ODCR). Esta métrica no mide instancias reservadas de Amazon EC2.

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 métricas de Outpost

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.

Dimensión	Descripción
`InstanceType`	El tipo de instancia.
`OutpostId`	El ID del Outpost.
`VolumeType`	El tipo de volumen EBS.
`VirtualInterfaceId`	El ID de la pasarela 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.

Vea CloudWatch las métricas de su puesto de avanzada

Puedes ver las CloudWatch métricas de tus balanceadores de carga 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 métricas mediante la 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 desde la 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 API de AWS Outposts con AWS CloudTrail.

AWS Outpostsestá integrado con AWS CloudTrail un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o un AWS servicio enAWS Outposts. CloudTrail captura todas las llamadas a la API AWS Outposts como eventos. Las llamadas capturadas incluyen las llamadas desde la consola de AWS Outposts y las llamadas desde el código a las operaciones de la API de AWS Outposts. Si crea un registro, puede habilitar la entrega continua de CloudTrail eventos a un bucket de S3, incluidos los eventos deAWS Outposts. Si no configuras una ruta, podrás ver los eventos más recientes en la CloudTrail consola, en el historial de eventos. Con la información recopilada por usted CloudTrail, puede determinar a AWS Outposts qué dirección IP se realizó la solicitud, quién la realizó, cuándo se realizó y detalles adicionales.

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

AWS Outpostsinformación en CloudTrail

CloudTrail está habilitada en su AWS cuenta al crear la cuenta. Cuando se produce una actividad enAWS Outposts, esa actividad se registra en un CloudTrail evento junto con otros eventos de AWS servicio en el historial de eventos. Puede ver, buscar y descargar los últimos eventos de la cuenta de AWS. Para obtener más información, consulte Visualización de eventos con el historial de CloudTrail eventos.

Para mantener un registro continuo de eventos en la cuenta de AWS, incluidos los eventos de AWS Outposts, cree un registro de seguimiento. Un registro permite CloudTrail entregar los archivos de registro a un bucket de S3 en el contenedor principalRegión de AWS. De manera predeterminada, cuando se crea un registro de seguimiento en la consola, el registro de seguimiento se aplica a todas las regiones de AWS. El registro de seguimiento registra los eventos de todas las regiones de la partición de AWS y envía los archivos de registro al bucket de S3 especificado. Además, puede

configurar otros AWS servicios para analizar más a fondo los datos de eventos recopilados en los CloudTrail registros y actuar en función de ellos. Para más información, consulte los siguientes temas:

- Introducción a la creación de registros de seguimiento
- CloudTrail Servicios e integraciones compatibles
- Configuración de las notificaciones de Amazon SNS para CloudTrail
- Recibir archivos de CloudTrail registro de varias regiones y recibir archivos de CloudTrail registro de varias cuentas

Todas AWS Outposts las acciones son registradas por CloudTrail. Estas acciones se documentan en la Referencia de la API de AWS Outposts. Por ejemplo, las llamadas a las `CreateOutpost` `ListSites` acciones y las llamadas generan entradas en los archivos de CloudTrail registro. `GetOutpostInstanceTypes`

Cada entrada de registro o evento contiene información sobre quién generó la solicitud. La información de identidad le ayudará a determinar si la solicitud se realizó:

- Con credenciales de usuario o raíz.
- Con credenciales de seguridad temporales de un rol o de un usuario federado.
- Por otro Servicio de AWS.

Para obtener más información, consulte el elemento userIdentity de CloudTrail .

Descripción de las entradas de los archivos de registro de AWS Outposts

Un registro es una configuración que permite la entrega de eventos como archivos de registro a un bucket de S3 que usted especifique. CloudTrail Los archivos de registro contienen una o más entradas de registro. Un evento representa una única solicitud desde cualquier origen. Incluye información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud, etc. CloudTrail Los archivos de registro no son un registro ordenado de las llamadas a las API públicas, por lo que no aparecen en ningún orden específico.

En el siguiente ejemplo, se muestra una entrada de CloudTrail registro que demuestra la `CreateOutpost` acción.

```
{
```

```
    "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 un Outpost

Según el modelo de responsabilidad compartida, AWS es responsable del hardware y el software que ejecutan los servicios de AWS. Esto se aplica a AWS Outposts, tal como lo hace en una región de AWS. 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 Outpost, 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

Mantenimiento del hardware

Si AWS detecta un problema irreparable con el hardware que aloja las instancias de Amazon EC2 y que se ejecutan en su Outpost, notificaremos al propietario del Outpost y al propietario de las instancias que se prevé retirar las instancias afectadas. Para obtener más información, consulte Retirada de instancia en la Guía del usuario de Amazon EC2.

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 es necesario realizar tareas de mantenimiento en el hardware, AWS se pondrá en contacto con el administrador del sitio del Outpost para confirmar la fecha y la hora de la visita del equipo de instalación de AWS. Las visitas se pueden programar en un plazo máximo de dos días laborables a partir del momento en que el administrador del sitio hable con el equipo de AWS.

Cuando el equipo de instalación de AWS llegue a las instalaciones, sustituirá los hosts, los conmutadores o los elementos del bastidor 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 las direcciones IP y las ASN que se utilizan para establecer interfaces virtuales, a fin de 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. La técnica AS-Path Prepending se utiliza para los prefijos de las puertas de enlace locales a fin de desviar el tráfico de los OND en caso de que sea 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 de clientes debe anunciar prefijos BGP iguales con los mismos atributos en todos los OND. El equilibrador de carga de red de Outpost equilibra el tráfico saliente entre todos los enlaces superiores de forma predeterminada. Las políticas de enrutamiento se utilizan en el lado del Outpost para desviar el tráfico de un OND si es necesario realizar tareas de mantenimiento. Este cambio de tráfico requiere la misma cantidad de prefijos de BGP por parte del cliente en todos los OND. 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 AWS Outposts

Como se indica en los Términos de servicio de AWS para los clientes de AWS Outposts, la instalación donde se encuentra el equipo de Outposts debe cumplir con los requisitos mínimos de alimentación y red para respaldar la instalación, el mantenimiento y el uso del equipo de Outposts. Un bastidor de Outposts solo puede funcionar correctamente cuando la alimentación y la conectividad de red no sufren interrupciones.

Eventos de alimentación

En caso de cortes totales de suministro de energía, existe el riesgo inherente de que un recurso de AWS Outposts 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.

Eventos de conectividad de red

Una vez que se complete el mantenimiento de la red, la conexión del enlace de servicio entre su Outpost y la región de AWS o la región de origen de Outposts se debería recuperar 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. 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. Para obtener más información, consulte la pregunta: ¿qué ocurre cuando se interrumpe la conexión de red de mis instalaciones? en la página de Preguntas frecuentes sobre bastidores de AWS Outposts.

Si el enlace de servicio no funciona debido a un problema de alimentación in situ o a una pérdida de conectividad de red, AWS Health Dashboard envía una notificación a la cuenta propietaria de los Outposts. Ni usted ni AWS puede suprimir la notificación de una interrupción del enlace de servicio, incluso si se espera la interrupción. 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 su bastidor de Outposts se conecta a la región de AWS 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 escala un inconveniente posmantenimiento a AWS o a su ISP, puede 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`. Reemplace *`región`* por el nombre de la región principal de 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 blog de AWS Prácticas recomendadas de supervisión de AWS Outposts aborda las mejores prácticas de observabilidad y administración de eventos específicas de Outposts.
- En el AWS blog Herramienta de depuración para conectividad de red de Amazon VPC se explica la herramienta de VPC AWSSupport -SetupIP. MonitoringFrom Esta herramienta es un documento de AWS Systems Manager (documento SSM) que crea una instancia de supervisión de Amazon EC2 en una subred especificada por usted, y supervisa 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 la supervisión de Outposts, la instancia de supervisión debe estar en una subred de la región de AWS principal y debe estar configurada para supervisar una o más de sus instancias de Outpost mediante el uso de sus IP privadas; esto proporcionará gráficos de pérdida de paquetes y latencia entre AWS Outposts y la región de AWS principal.
- 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 Creación de un caso de soporte en la Guía del usuario de Soporte de AWS.

Optimice Amazon EC2 para AWS Outposts

A diferencia de la Región de AWS, la capacidad de Amazon Elastic Compute Cloud (Amazon EC2) la capacidad en un Outpost es limitada. 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 capacidad de Amazon EC2 en AWS Outposts.

Contenido

Hosts dedicados en Outposts

Un host dedicado de Amazon EC2 es un servidor físico con capacidad de instancias EC2 totalmente dedicado 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, consulte Host dedicado en AWS Outposts en la Guía del usuario de instancias de Linux de Amazon EC2. Para Windows, consulte Host dedicado en AWS Outposts en la Guía del usuario de Amazon EC2 para instancias de Windows.

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

Alterar el diseño de la capacidad de un servidor

Los hosts dedicados le ofrecen la posibilidad de alterar el diseño de los servidores durante la implementación del Outpost sin necesidad de ponerse en contacto con AWS Support. Cuando adquiere capacidad para su Outpost, especifica el diseño de la capacidad de EC2 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 Asignación de hosts dedicados en la Guía del usuario de Amazon EC2 para instancias de Linux o Asignación de hosts dedicados en la Guía del usuario de Amazon EC2 para instancias de Windows.

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 Outpost, 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 Comprender la ubicación automática y la afinidad en la Guía del usuario de Amazon EC2 para instancias de Linux o Comprender la ubicación automática y la afinidad en la Guía del usuario de Amazon EC2 para instancias de Windows.

Puede compartir hosts dedicados mediante el uso de 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 Trabajar con recursos 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 Recuperación de su instancia de Linux o Recuperación de su instancia de Windows.

Grupos de ubicación en Outposts

AWS Outposts admite grupos de ubicación. Utilice los grupos de ubicación para influir en la forma en que Amazon EC2 debe intentar ubicar los grupos de instancias interdependientes que lance 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. Puede usar grupos de ubicación de distribución a nivel de host solo 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.

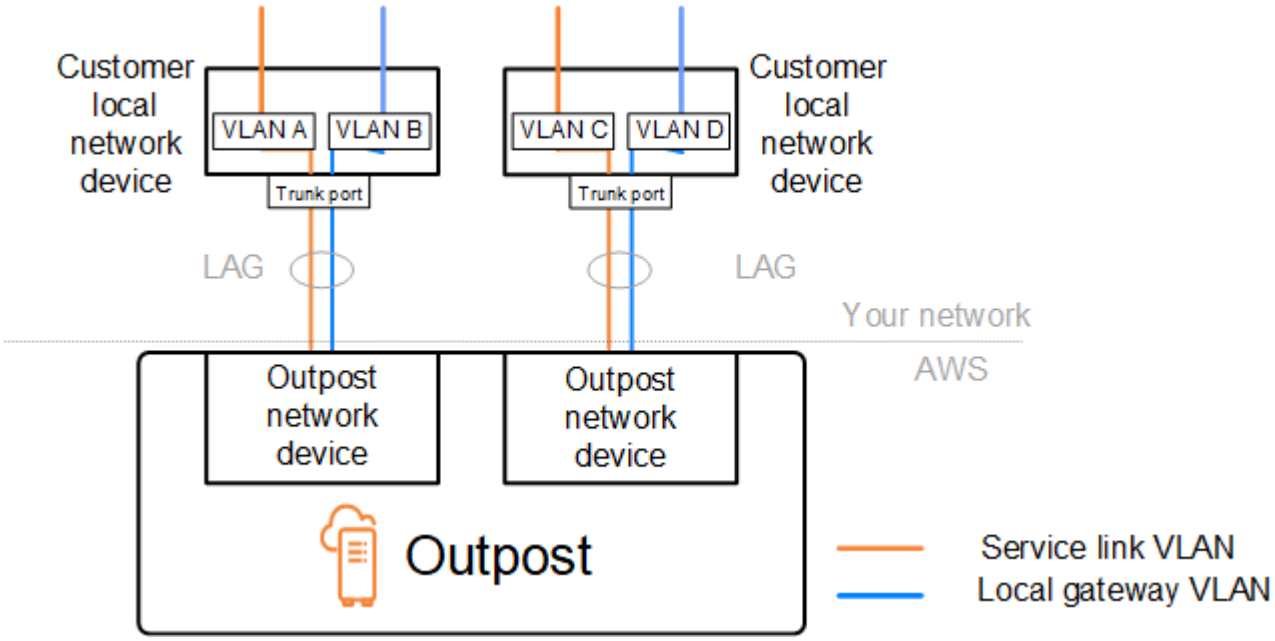
También puede implementar instancias en las particiones de destino. La siguiente ilustración muestra un grupo con ubicación en particiones con una distribución segmentada.

Para más información sobre el uso de grupos de ubicación, consulte Grupos de ubicación y Grupos de ubicación en AWS Outposts en la Guía del usuario de Amazon EC2 para instancias Linux. Para Windows, consulte Grupos de ubicación y Grupos de ubicación en AWS Outposts en la Guía del usuario de Amazon EC2 para instancias de Windows.

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

Lista de comprobación de solución de problemas de redes en bastidor de AWS 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 el uso de su plan de Enterprise Support.

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

Conectividad de la interfaz virtual pública de AWS Direct Connect con la región AWS

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. La tabla de enrutamiento debe incluir los rangos de direcciones IP de AWS públicas o la ruta predeterminada.
3. Si no recibe los rangos de direcciones IP de AWS públicas en el VRF del enlace de servicio, compruebe los siguientes elementos.
   a. Compruebe el estado del enlace de AWS Direct Connect desde el enrutador perimetral o el AWS Management Console.
   b. Si el enlace físico es `UP`, compruebe el estado del emparejamiento de BGP desde el enrutador perimetral.
   c. Si el estado de emparejamiento de BGP es `DOWN`, haga ping a la dirección IP de intercambio de tráfico de AWS y compruebe la configuración del BGP en el enrutador perimetral. Para obtener más información, consulte Solución de problemas de AWS Direct Connect en la Guía del usuario de AWS Direct Connect y El estado del BGP de mi interfaz virtual está inactivo en la consola de AWS. ¿Qué debo hacer?
   d. Si se ha establecido el BGP y no ve la ruta predeterminada o los rangos de direcciones IP de AWS públicas en el VRF, póngase en contacto con AWSSupport mediante el uso de su plan de Enterprise Support.
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 rango de direcciones IP del enlace de servicio del Outpost con los rangos de direcciones IP públicas de AWS. Para obtener más información, consulte Conectividad de AWS Outposts con las regiones de AWS.
   c. Si el firewall no está en estado activo, asegúrese de permitir también el flujo entrante (desde los rangos de direcciones IP públicas de AWS 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 enrutador perimetral a las direcciones IP de emparejamiento de AWS Direct Connect. Comparta los resultados de las pruebas con AWS Support, mediante el uso de su plan de Enterprise Support.

Conectividad de la interfaz virtual privada de AWS Direct Connect con la región AWS

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 del enlace de servicio.

1. Si la conectividad entre el bastidor de Outpost y la región de AWS utiliza la característica de conectividad de AWS Outposts privada, compruebe los siguientes elementos.
   a. Haga ping a la dirección IP de emparejamiento remoto en AWS desde el enrutador perimetral y confirme el estado del emparejamiento de BGP.
   b. Asegúrese de que el emparejamiento de BGP a través de la interfaz virtual de AWS Direct Connect privada entre la VPC del punto de conexión del enlace de servicio y el Outpost instalado en sus instalaciones sea UP. Para obtener más información, consulte Solución de problemas de AWS Direct Connect en la Guía del usuario de AWS Direct Connect y El estado del BGP de mi interfaz virtual está inactivo en la consola de AWS. ¿Qué debo hacer? y ¿Cómo puedo solucionar problemas de conexión del BGP a través de Direct Connect?.
   c. La interfaz virtual privada de AWS Direct Connect es una conexión privada al enrutador perimetral de la ubicación AWS Direct Connect 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 perimetral. 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 perimetral.

d. Confirme que las ACL de red asociadas al punto de conexión privado del enlace de servicio en su VPC permiten 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 de 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 en las instalaciones, puede anunciar una ruta predeterminada a través de la sesión del BGP hasta su interfaz virtual privada de AWS. 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 enrutador perimetral a las direcciones IP de emparejamiento de AWS Direct Connect. Comparta los resultados de las pruebas con AWS Support, mediante el uso de su plan de Enterprise Support.

Conectividad de Internet pública del ISP a la región de AWS

Utilice la siguiente lista de verificación para solucionar problemas con los enrutadores periféricos 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 perimetral. 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 se puede acceder a alguna de sus instancias EC2 o a los equilibradores de carga de acceso público en la región de origen del Outpost 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 usa los VRF para separar el tráfico de la red, confirme que el VRF del enlace de servicio 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 perimetrales que se conectan con el ISP. Compruebe la tabla de enrutamiento de la VRF del ISP del enrutador perimetral 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 de los VRF 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 en las instalaciones estén configurados para permitir la conectividad saliente (puertos TCP 1025-65535 y UDP 443) desde los rangos de direcciones IP del enlace del servicio de Outpost hasta los rangos de direcciones IP de AWS públicas. 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 AWS Support mediante el uso de su plan de Enterprise Support.

Outposts está detrás de dos dispositivos de firewall

Si has colocado tu Outpost detrás de un par de 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 pasa por el firewall-2. Utilice la siguiente lista de verificación para identificar el posible enrutamiento asimétrico del enlace de servicio, especialmente si anteriormente 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 del firewall para comprobar si hay cambios en los patrones de tráfico que estén relacionados con el inicio del problema de enlace de servicio.
  - Compruebe si se ha producido un fallo parcial del firewall o si se ha producido una confusión entre dos cortafuegos que podría haber provocado que los firewalls dejaran de sincronizar sus tablas de conexiones entre sí.
  - Compruebe si los enlaces están inactivos o si se han producido cambios recientes en el enrutamiento (cambios en las métricas de OSPF/ISIS/EIGRP, 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 del proveedor de servicios podría haber provocado un enrutamiento asimétrico del enlace de servicio a través de los firewalls.
  - Consulte los gráficos de tráfico de los enlaces a sus ISP para ver si hay cambios en los patrones de tráfico que estén relacionados con el inicio del problema de enlace del servicio.
- Si utiliza la AWS Direct Connect conectividad para el enlace de servicio, es posible que un mantenimiento AWS planificado haya activado el 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 comprobar si una interrupción en uno de sus AWS Direct Connect servicios 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 otras medidas:

- Restaure el enrutamiento simétrico revertiendo 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 en estado de flujo del tráfico del enlace de servicio en la memoria del firewall.
- Pídele al proveedor del firewall que verifique o relaje el seguimiento del estado de flujo UDP de las conexiones UDP originadas en el puerto 443 y destinadas al puerto 443.

AWS Outposts end-of-term opciones

Al finalizar su plazo de AWS Outposts, tiene tres opciones:

- Renovar su suscripción y conservar su Outpost actual.
- Finalizar su suscripción y devolver su servidor de Outpost.
- Conviértelo en una month-to-month suscripción y conserva tu Outpost actual.

Si no indicas que deseas renovar tu suscripción o devolver tu Outpost, pasarás a ser una month-to-month suscripción.

Temas

Renovar la suscripción

Para renovar su suscripción y conservar su servidor de Outpost actual:

Complete los siguientes pasos al menos 30 días antes de que finalice el plazo de su Outpost:

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.

El servicio de atención al cliente de AWS iniciará el proceso de renovación de la suscripción. La nueva suscripción comenzará el día siguiente a la finalización de la suscripción actual.

Finalice su suscripción y prepare los bastidores para su devolución

> **Important**
>
> AWS no puede iniciar el proceso de devolución hasta que haya completado los siguientes procedimientos. No podemos detener el proceso de devolución después de que haya abierto un caso de soporte para finalizar su suscripción.

Para finalizar su suscripción:

Complete los siguientes pasos al menos 30 días antes de que finalice el plazo de su Outpost:

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.

El servicio de atención al cliente de AWS se pondrá en contacto con usted para coordinar la recuperación.

Para preparar sus bastidores de AWS Outposts para la devolución:

> **Important**
>
> No apague el bastidor de Outpost 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:

   - Use la consola de AWS RAM. Para obtener más información, consulte Actualizar un recurso compartido en la Guía del usuario de AWS RAM.
   - Utilice la AWS CLI para ejecutar el comando disassociate-resource-share.

   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, siga los pasos indicados en Finalizar una instancia en la Guía del usuario de Amazon EC2 para instancias de Linux.
3. Verifique las instancias instance-capacity-availability de Amazon EC2 de su AWS cuenta.

   a. Abra la consola de AWS Outposts en https://console.aws.amazon.com/outposts/.

   b. Elija Outposts.

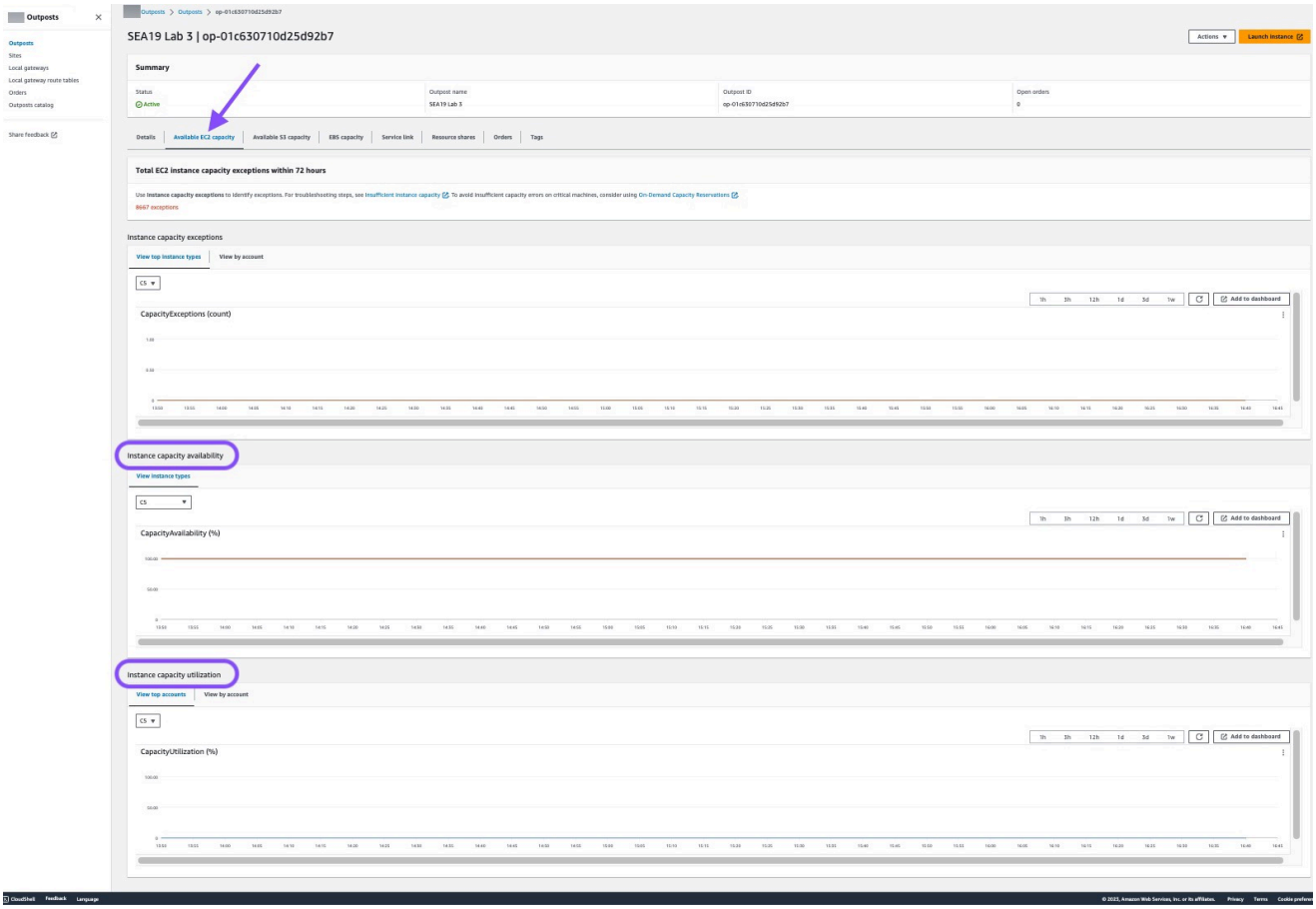
c. Elija el Outpost específico que va a devolver.

d. En la página del Outpost, elija la pestaña de Capacidad de EC2 disponible.

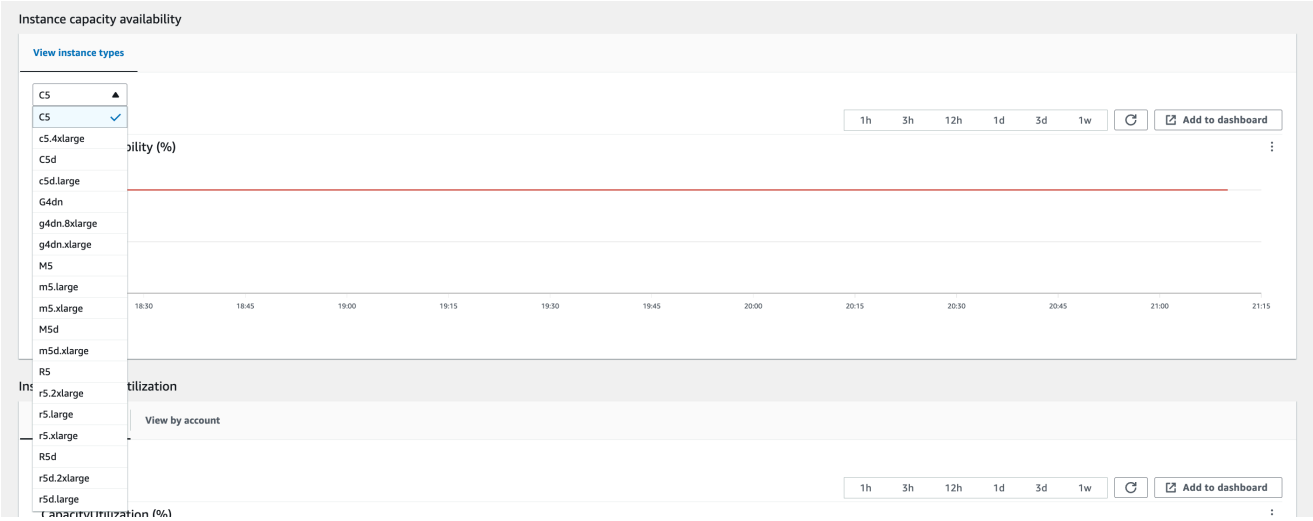
e. Asegúrese de que la disponibilidad de la capacidad de las instancias sea del 100% para cada familia de instancias.

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 Disponibilidad de la capacidad de la instancia y Utilización de la capacidad de la instancia en la pestaña Capacidad de EC2 disponible.



En la imagen siguiente, se muestra la lista de tipos de instancias.



4. Cree copias de seguridad de sus instancias y volúmenes de servidores de Amazon EC2. Para crear las copias de seguridad, siga las instrucciones de Copias de seguridad y recuperación para Amazon EC2 con volúmenes de EBS de la guía Recomendaciones de AWS.
5. Elimine los volúmenes de Amazon EBS asociados a su Outpost.
   a. Abra la consola de Amazon EC2 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. Abra la consola de Amazon EC2 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 Outpost. Para ello, siga las instrucciones de Eliminar un bucket de Outpost de Amazon S3 en la Guía del usuario de Amazon Simple Storage Service.
8. Elimine todas las asociaciones de VPC y los CIDR del grupo de direcciones IP (CoIP) asociados a su Outpost.

Un equipo de recuperación de AWS apagará el bastidor. Cuando se apague, puede destruir la clave de seguridad Nitro de AWS o el equipo de recuperación de AWS puede hacerlo por usted.

Conviértala en una suscripción month-to-month

Para convertirla en una month-to-month suscripción y conservar tu Outpost actual, no es necesario realizar ninguna acción. Si tiene alguna pregunta, abra un caso de soporte de facturación.

Su Outpost se renovará mensualmente según la tarifa de la opción de pago sin pago inicial que corresponda a su configuración de AWS Outposts. Su nueva suscripción mensual comenzará el día siguiente a la finalización de la suscripción actual.

Cuotas para AWS Outposts

Su Cuenta de AWS tiene cuotas predeterminadas —anteriormente conocidas como «límites»— para cada servicio de Servicio de AWS. A menos que se indique otra cosa, cada cuota es específica de la región. Puede solicitar el aumento de algunas cuotas, pero no de todas.

Para ver todas las cuotas de AWS Outposts, abra la consola de 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.

La Cuenta de AWS incluye las siguientes cuotas en relación con AWS Outposts:

Recurso	Valor 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. Puede tener 100 sitios de Outposts en cada región de la cuenta de AWS.
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 para 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

En la siguiente tabla se describen cambios importantes en la Guía del usuario de AWS Outposts .

Cambio	Descripción	Fecha
Administración de la capacidad	Puedes modificar la configura ción de capacidad predeterm inada para tu 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 puede monitorear el uso del rendimiento entre sus interfaces virtuales (VIF) de enlace de servicio rack de Outpost y sus dispositivos de red local, aprovechando las métricas. `IfTrafficIn` `IfTrafficOut` Amazon CloudWatch	17 de noviembre de 2023
Comunicación dentro de la VPC a través de la puerta de AWS Outposts enlace local	Puede establecer comunicac ión entre subredes de la misma VPC a través de diferentes Outposts con puerta de enlace locales.	30 de agosto de 2023
nd-of-term Opciones de E para AWS Outposts pistas	Al final de su AWS Outposts período, puede renovar, finalizar o convertir su 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.	20 de julio de 2023

	También puede configurar la conectividad híbrida entre un Outpost y un soluciona dor de DNS en las instalaci ones mediante la implement ación de puntos de conexión entrantes y salientes.	
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 enrutamie nto 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 de AWS Outposts usuario para Outposts rack	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 informaci ón 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
Soporte para compartir direcciones IPv4 que sean propiedad de los clientes	Se usa AWS Resource Access Manager para compartir las direcciones IPv4 propiedad del cliente.	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.