Guía de usuario de servidores de Outposts

AWS Outposts

AWS Outposts: Guía de usuario de servidores de Outposts

Table of Contents

¿Qué es AWS Outposts?

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

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

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

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

Conceptos clave

Estos son los conceptos clave de. AWS Outposts

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

- Bastidores de Outposts: un factor de forma de Outpost que constituye un bastidor de 42U estándar del sector. Los bastidores del Outposts incluyen servidores que se pueden montar en bastidores, conmutadores, un panel de conexiones de red, un estante de suministro eléctrico y paneles vacíos.
- Servidores para Outposts: un factor de forma del Outpost que constituye un servidor de 1U o 2U con protocolo estándar del sector, y se puede instalar en un bastidor de 4 postes estándar conforme con la norma EIA-310D 19. Los servidores de Outposts proporcionan servicios de computación y red locales a sitios que tienen requisitos de espacio limitado o capacidad más reducida.
- Propietario de Outpost: el propietario de la cuenta que realiza el pedido. AWS Outposts Tras AWS contactar con el cliente, el propietario puede incluir puntos de contacto adicionales. AWS se comunicará con los contactos para aclarar los pedidos, las citas de instalación y el mantenimiento y reemplazo del hardware. Comuníquese con AWS Support Center si la información de contacto cambia.
- Enlace de servicio: ruta de red que permite la comunicación entre su puesto de avanzada y AWS la región asociada. Cada Outpost es una extensión de una zona de disponibilidad y su región asociada.
- Puerta de enlace local (LGW): un enrutador virtual de interconexión lógica que permite la comunicación entre un bastidor de Outposts y la red en las instalaciones.
- Interfaz de red local: una interfaz de red que permite la comunicación entre un servidor de Outposts y la red en las instalaciones.

AWS recursos en Outposts

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

Computación

Tipo de recurso	Bastidores	Servidores
Instancias de Amazon EC2	S	Sí

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

Base de datos y análisis

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

Red

Tipo de recurso	Bastidores	Servidores
Proxy App Mesh Envoy	 S	 Sí

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

Almacenamiento

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

Otros Servicios de AWS

Servicio	Bastidores	Servidores
AWS IoT Greengrass	 S	 Sí

Precios

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

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

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

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

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

Cómo AWS Outposts funciona

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

El siguiente diagrama ilustra ambos factores de forma de Outpost.

Contenido

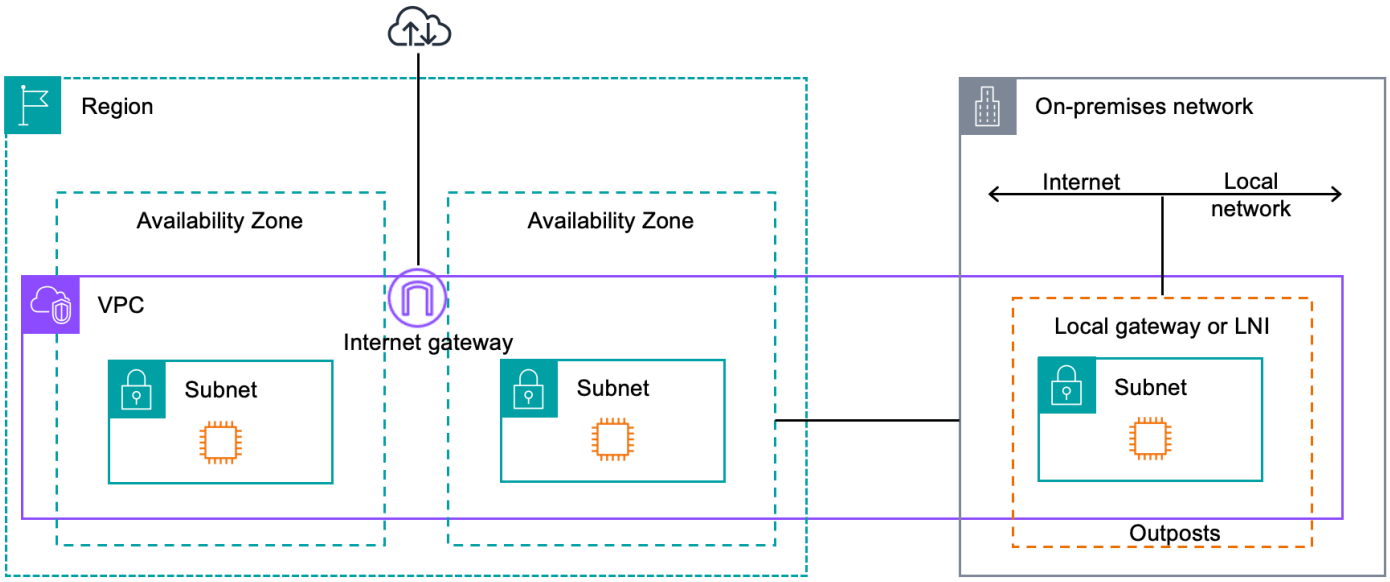
Componentes de la red

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

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

- Una red local y una red local Región de AWS
- Una VPC con múltiples subredes en la región
- Un Outpost en la red en las instalaciones
- La conectividad entre el Outpost y la red local proporcionó:

- Para los racks de Outposts: una puerta de enlace local
- Para los servidores Outposts: una interfaz de red local (LNI)



VPCs y subredes

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

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

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

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

Enrutamiento

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

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

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

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

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

DNS

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

Es posible que encuentres tiempos de resolución de DNS más prolongados con Route 53, según la latencia de la ruta entre tu Outpost y la AWS región. En tales casos, puede utilizar los servidores

DNS instalados localmente en su entorno en las instalaciones. Para usar sus propios servidores DNS, debe crear conjuntos de opciones de DHCP para los servidores DNS en las instalaciones y asociarlos a la VPC. También debe asegurarse de que haya conectividad IP con estos servidores DNS. Es posible que también necesite agregar rutas a la tabla de enrutamiento de la puerta de enlace local para garantizar su accesibilidad, pero esta opción solo es válida para los bastidores de Outposts con puerta de enlace local. Como los conjuntos de opciones de DHCP tienen un ámbito de VPC, las instancias de las subredes de Outpost y de las subredes de la zona de disponibilidad de la VPC intentarán usar los servidores DNS especificados para la resolución de nombres DNS.

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

Enlace de servicio

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

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

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

Interfaces de red local

Los servidores de Outposts incluyen una interfaz de red en las instalaciones para proporcionar conectividad a la red en las instalaciones. La interfaz de red local solo está disponible para los servidores de Outposts que se ejecutan en una subred de Outpost. No puedes usar una interfaz de red local desde una EC2 instancia de un rack de Outposts o de la AWS Región. La interfaz de red local está destinada únicamente a ubicaciones en las instalaciones. Para obtener más información, consulte Interfaces de red local para sus servidores de Outposts.

Requisitos del sitio para los servidores de Outposts

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

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

Contenido

Instalación

Estos son los requisitos para la instalación de los servidores.

> **Note**
>
> Las especificaciones son para servidores en condiciones de funcionamiento normales. Por ejemplo, la acústica puede sonar más fuerte durante la instalación inicial y, después, funcionar con la potencia acústica nominal una vez finalizada la instalación.

- Temperatura: la temperatura ambiente debe oscilar entre 41 y 95 °F (5 y 35 °C).

  El servidor se apagará cuando la temperatura esté fuera de este rango y se reiniciará cuando la temperatura vuelva a estar dentro del rango.
- Humedad: la humedad relativa debe estar entre el 8 % y el 80 % sin condensación.
- Calidad del aire: el aire debe filtrarse con un filtro MERV8 (o uno superior).

- Flujo de aire: la posición del servidor debe garantizar un espacio mínimo de 6 pulgadas (15 cm) entre el servidor y las paredes situadas delante y detrás del servidor para dejar suficiente espacio libre para el flujo de aire.
- Peso: el servidor de 1U pesa 26 lb (11,79 kg) y el servidor de 2U pesa 36 lb (16,36 kg). Confirme que la ubicación en la que piensa colocar el servidor puede soportar el peso del servidor.

  Para ver los requisitos de peso de los distintos recursos de Outposts, selecciona Explorar el catálogo en la AWS Outposts consola en. https://console.aws.amazon.com/outposts/
- Compatibilidad del kit de rieles: el kit de rieles que se incluye en el paquete de envío es compatible con un soporte de montaje estándar en forma de L de un bastidor de 19 in (482,6 mm) conforme a la norma EIA-310-D. El kit de rieles no es compatible con un soporte de montaje en forma de U, como se muestra en la siguiente imagen.

- Ubicación del bastidor: recomendamos el uso de bastidores EIA-310D estándar de 19 in (482,6 mm), con una profundidad de al menos 36 in (914 mm). AWS proporciona un kit de raíles para el montaje en bastidor del servidor.
  - Los servidores de Outposts 2U requieren espacio con las siguientes dimensiones: 3,5 in de alto (88,9 mm), 17,5 in de ancho (447 mm) y 30 in de profundidad (762 mm).
  - Los servidores de Outposts 1U requieren espacio con las siguientes dimensiones: 1,75 in de alto (44,45 mm), 17,5 in de ancho (447 mm) y 24 in de profundidad (610 mm).
  - No se admite el montaje vertical de los AWS Outposts servidores.
  - Los servidores de Outposts 1U tienen el mismo ancho que los servidores de Outposts 2U, pero tienen la mitad de altura y menos profundidad.

  Si no coloca el servidor en un bastidor, deberá seguir cumpliendo los demás requisitos del sitio.
- Facilidad de mantenimiento: los servidores de Outposts se pueden reparar en el pasillo delantero.
- Acústica: tiene una potencia acústica inferior a 78 dBA a temperaturas de 80 °F (27 °C), y cumple con la norma GR-63 CORE NEBS.
- Refuerzo sísmico: en la medida en que lo exija la normativa o el código, debe instalar y mantener los anclajes y refuerzos sísmicos adecuados para el servidor mientras esté en sus instalaciones.
- Elevación: la altura de la sala donde está instalado el bastidor debe ser inferior a 10 005 ft (3,05 m).
- Limpieza: limpie las superficies con paños húmedos que contengan productos químicos de limpieza antiestáticos debidamente homologados.

Red

Cada servidor de Outposts incluye puertos de enlace ascendente físicos no redundantes. Los puertos tienen sus propios requisitos de velocidad y conector, como se detalla a continuación.

Etiqueta de puerto	Velocidad	Conector en el dispositivo de red ascendente	Tráfico
Puerto 3	10 GbE	SFP+	Tanto el tráfico de servicio como el de enlace LNI: el cable de conexión QSFP+ (10 ft / 3 m) segmenta el tráfico.

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	1024-65535	IP del enlace de servicio	53	servidor del DNS
UDP	443, 1024-65535	IP del enlace de servicio	443	Puntos de conexión del enlace de servicio de Outposts
TCP	1024-65535	IP del enlace de servicio	443	Punto de conexión del registro de Outposts

Puedes usar una Direct Connect conexión o una conexión pública a Internet para volver a conectar el puesto de avanzada a la AWS región. Para la conectividad del enlace de servicio del Outposts,

puede usar NAT o PAT en su firewall o enrutador de periferia. El establecimiento del enlace de servicio siempre se inicia desde el Outpost.

Unidad de transmisión máxima (MTU) del enlace de servicio

La red debe admitir una MTU de 1500 bytes entre el Outpost y los puntos de enlace de servicio de la región principal. AWS Para obtener más información sobre el enlace de servicio, consulte Conectividad de AWS Outposts a regiones de AWS en la Guía del usuario de AWS Outposts .

Recomendaciones de ancho de banda para el enlace de servicio

Para una experiencia y una resiliencia óptimas, AWS requiere que utilice una conectividad redundante de al menos 500 Mbps y una latencia máxima de ida y vuelta de 175 ms para la conexión del enlace de servicio a la región. AWS La utilización máxima de cada servidor de Outposts es de 500 Mbps. Para aumentar la velocidad de conexión, utilice varios servidores de Outposts. Por ejemplo, si tiene tres servidores de AWS Outposts , la velocidad máxima de conexión aumentará a 1,5 Gbps (1500 Mbps). Para obtener más información, consulte Tráfico de enlace de servicio para servidores en la Guía del usuario de AWS Outposts para servidores.

Los requisitos de ancho de banda de AWS Outposts Service Link varían en función de las 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. Tenga en cuenta que AWS Outposts los servidores no almacenan en caché AMIs. AMIs se descargan de la región con cada lanzamiento de una instancia.

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

Alimentación

A continuación, se describen los requisitos de alimentación para los servidores de Outposts.

Requisitos

- Soporte de alimentación
- Consumo de energía
- Cable de alimentación

Soporte de alimentación

Los servidores tienen una potencia de hasta 1600 W, 90-264 VAC y 47/63 Hz AC.

Consumo de energía

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

Cable de alimentación

El servidor se suministra con un cable de alimentación IEC C14-C13.

Cableado de alimentación del servidor al bastidor

Utilice el cable de alimentación IEC C14-C13 suministrado para conectar el servidor al bastidor.

Cableado de alimentación del servidor a la toma de pared

Para conectar el servidor a una toma de pared estándar, debe utilizar un adaptador para la entrada C14 o un cable de alimentación específico para cada país.

Asegúrese de tener el adaptador o el cable de alimentación correctos para su región, a fin de ahorrar tiempo durante la instalación del servidor.

- En Estados Unidos, necesita un cable de alimentación NEMA 5-15P a IEC C13.
- En algunas partes de Europa, es posible que necesite un cable de alimentación CEE 7/7 a IEC C13.
- En India, se necesita un cable de IS1293 alimentación IEC C13.

Redundancia de alimentación

Los servidores incluyen varias conexiones de alimentación y se suministran con cables para permitir un funcionamiento con redundancia de alimentación. Recomendamos la redundancia de alimentación, aunque no es obligatoria.

Los servidores no incluyen un sistema de alimentación ininterrumpida (SAI).

Procesamiento de pedido

Para cumplir con el pedido, AWS enviaremos el equipo del servidor de Outposts, incluidos los soportes de raíles y los cables de alimentación y red necesarios, a la dirección que nos haya proporcionado. La caja en la que se envía el servidor tiene las siguientes dimensiones:

- Caja con un servidor de 2U:
  - Longitud: 44 in / 111,8 cm
  - Altura: 26,5 ft / 67,3 cm
  - Ancho: 17 ft / 43,2 cm
- Caja con un servidor de 1U:
  - Longitud: 34,5 ft / 87,6 cm
  - Altura: 24 ft / 61 cm
  - Ancho: 9 ft / 22,9 cm

Su equipo o un proveedor externo debe instalar el equipo. Para obtener más información, consulte Tráfico de enlace de servicio para servidores en la Guía del usuario de AWS Outposts para servidores.

La instalación finaliza al confirmar que la capacidad de Amazon EC2 para su servidor de Outposts está disponible en su Cuenta de AWS.

Introducción a los bastidores de Outposts

Pida un servidor de Outposts para empezar. Tras instalar su equipo de Outpost, lance una instancia de Amazon EC2 y configure la conectividad con su red en las instalaciones.

Tareas

- Crear un Outpost y solicitar capacidad de Outpost
- Lance una instancia en su servidor de Outposts.

Crear un Outpost y solicitar capacidad de Outpost

Para empezar a usarlo AWS Outposts, inicia sesión con tu AWS cuenta. Cree un sitio y un Outpost. Luego, realice un pedido para los servidores de Outposts que necesite.

Requisitos previos

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

Tareas

- Paso 1: crear un sitio
- Paso 2: crear un Outpost
- Paso 3: realizar el pedido
- Paso 4: Modificar la capacidad de la instancia
- Siguientes pasos

Paso 1: crear un sitio

Cree un sitio para especificar la dirección operativa. La dirección de operación es la ubicación en la que instalará y ejecutará sus servidores de Outposts. Después de crear el sitio, AWS Outposts asigna un ID a tu sitio. Debe especificar este sitio al crear un Outpost.

Requisitos previos

- Determine la dirección operativa.

Cómo crear un sitio

1. Inicia sesión en. AWS
2. Abre la AWS Outposts consola en https://console.aws.amazon.com/outposts/.
3. Para seleccionar la principal Región de AWS, utilice el selector de regiones situado en la esquina superior derecha de la página.
4. En el panel de navegación, seleccione Sitios.
5. Seleccione Crear sitio.
6. En Tipo de hardware compatible, seleccione Solo servidores.
7. Introduzca el nombre, la descripción y la dirección operativa del sitio.
8. (Opcional) En las notas del sitio, introduce cualquier otra información que pueda ser útil AWS para conocer el sitio.
9. Seleccione Crear sitio.

Paso 2: crear un Outpost

Cree un Outpost para cada servidor. Un Outpost solo se puede asociar a un servidor de Outpost. Debe especificar este Outpost cuando realice el pedido.

Requisitos previos

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

Para crear un Outpost

1. En el panel de navegación, elija Outposts.

2. Seleccione Crear Outpost.
3. Elija Servidores.
4. Escriba un nombre y una descripción para el Outpost.
5. Elija una zona de disponibilidad para su Outpost.
6. En ID del sitio, elija el sitio.
7. Seleccione Crear Outpost.

> **Note**
>
> No podrás modificar la ubicación física ni el punto de anclaje en la zona de disponibilidad de tu Outpost después de completar el pedido.

Paso 3: realizar el pedido

Realice un pedido de los servidores de Outposts que necesite.

> **Important**
>
> No puede editar un pedido después de enviarlo, así que revisa todos los detalles detenidamente antes de enviarlo. Si necesita cambiar un pedido, póngase en contacto con AWS Support Center.

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 la opción de pago parcial por adelantado o sin pago por adelantado, pagará cargos mensuales durante el periodo.

  Los precios incluyen entrega, mantenimiento de servicios de infraestructura y parches y actualizaciones de software.
- Determine si la dirección de envío 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 Servidores.
4. Para agregar capacidad, elija una configuración.
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

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

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

- Las instancias se colocan automáticamente en función de las prácticas recomendadas.

Para modificar la capacidad de las instancias:

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

Console steps

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

11. En la página de tareas de capacidad, supervise el estado de la tarea.

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

Upload JSON file

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

   Example

   Ejemplo de archivo JSON:

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

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

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

Siguientes pasos

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

Para tramitar el pedido, AWS programaremos una fecha de entrega.

Usted es responsable de todas las tareas de instalación, incluidas la instalación física y la configuración de la red. Puede contratar a un tercero para que se encargue de realizar estas tareas. Tanto si realiza la instalación como si contrata a un tercero, la instalación requiere las credenciales de IAM de Cuenta de AWS que contienen el Outpost para comprobar la identidad del nuevo dispositivo. Usted es responsable de proporcionar y administrar este acceso. Para obtener más información, consulte la Guía de instalación del servidor.

La instalación se completará cuando la capacidad de Amazon EC2 para su Outpost esté disponible en su Cuenta de AWS. Una vez que la capacidad esté disponible, puede lanzar instancias de Amazon EC2 en el servidor de Outposts. Para obtener más información, consulte the section called “Iniciar una instancia”.

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

Lance una instancia en su servidor de Outposts.

Una vez que esté instalado el Outpost y la capacidad de computación y de almacenamiento estén disponibles para su uso, puede comenzar con la creación de recursos. Por ejemplo, puede lanzar instancias de Amazon EC2.

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 subred

Puede añadir subredes de Outpost a cualquier VPC de la AWS región de Outpost. Al hacerlo, la VPC también se extiende por 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 persona ha compartido contigo, salta a. Cuenta de AWSPaso 2: lanzar una instancia en el 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 y especifique un rango de direcciones IP para la subred.
5. Seleccione Crear.
6. Una vez creada la subred, debe habilitar la subred para las interfaces de red locales. Utilice el comando modify-subnet-attribute desde la AWS CLI. Debe especificar la posición de la interfaz de red en el índice de dispositivos. Todas las instancias lanzadas en una subred de Outpost habilitada utilizan esta posición del dispositivo para las interfaces de red local. En el siguiente ejemplo, se utiliza el valor 1 para especificar una interfaz de red secundaria.

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

Paso 2: lanzar 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

- Las instancias en servidores Outposts incluyen volúmenes de almacén de instancias pero no volúmenes de EBS. Elija un tamaño de instancia con suficiente almacenamiento de instancias para cumplir con las necesidades de la aplicación. Para obtener más información, consulte Volúmenes de almacén de instancias y Creación de una AMI basada en el almacén de instancias en la Guía del usuario de Amazon EC2.
- Debe utilizar una AMI respaldada por Amazon EBS-Based con una sola instantánea de EBS. AMIs no se admiten con más de una instantánea de EBS.
- Los datos de los volúmenes del almacén de instancias persisten tras el reinicio de la instancia, pero no persisten tras la finalización de la instancia. Para retener los datos a largo plazo de los volúmenes de almacén de instancias más allá de la vida útil de la instancia, asegúrese de realizar una copia de seguridad de los datos en un almacenamiento persistente, como un bucket de Amazon S3 o un dispositivo de almacenamiento de red en su red en las instalaciones.
- Para usar volúmenes de arranque o datos en bloque respaldados por un almacenamiento de terceros compatible, debe aprovisionar y configurar estos volúmenes para usarlos con instancias EC2 en Outposts. Para obtener más información, consulte Almacenamiento en bloque de terceros.
- Para conectar una instancia de una subred de Outpost en las instalaciones de la red local, debe agregar una interfaz de red local, tal y como se describe en el siguiente procedimiento.

Para iniciar instancias en una subred de Outpost

1. Abra 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 usted y le mostramos solo los tipos de instancias compatibles con sus servidores de Outposts.
5. Elija un tipo de instancia que sea admitida por sus servidores de Outposts. Tenga en cuenta que las instancias que aparecen atenuadas no están disponibles.
6. (Opcional) Puede agregar una interfaz de red local ahora o después de crear la instancia. Para agregarla ahora, expanda Configuración de red avanzada y elija Agregar interfaz de red. Elija la subred del Outpost. Esto crea una interfaz de red para la instancia mediante el índice de dispositivo 1. Si especificó 1 como índice de dispositivos en la interfaz de red local para la subred de Outpost, entonces esta interfaz de red es la interfaz de red local de la instancia. Si desea agregarla más adelante como alternativa, consulte Agregue una interfaz de red local.
7. (Opcional) Puede añadir un volumen de datos de terceros.
   a. Amplíe Configurar almacenamiento. Junto a Volumen de almacenamiento externo, selecciona Editar.
   b. Para Storage Network Protocol, elija iSCSI.
   c. Introduzca el IQN del iniciador y, a continuación, añada la dirección IP de destino, el puerto y el IQN de la matriz de almacenamiento externo.
8. Complete el asistente para lanzar la instancia en la subred del Outpost. Para obtener más información, consulte Lanzamiento de una instancia de EC2 en la Guía del usuario de Amazon EC2.

Paso 3: configurar la conectividad

Si no agregó una interfaz de red local a la instancia durante el lanzamiento de la instancia, debe hacerlo ahora. Para obtener más información, consulte Agregue una interfaz de red local.

Debe configurar la interfaz de red local de la instancia con una dirección IP de la red local. Para obtener más información, consulte la documentación del sistema operativo que se ejecuta en la

instancia. Busque información sobre cómo configurar interfaces de red adicionales y direcciones IP secundarias.

Paso 4: comprobar la conexión

Puede probar la conectividad mediante los casos de uso adecuados.

Pruebe la conectividad desde la red local al Outpost

Desde un ordenador de la red local, ejecute el comando `ping` en la dirección IP de la interfaz de red local 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 cómo conectarse a su instancia de EC2, consulte Conexión con instancias EC2 en la Guía del usuario de Amazon EC2.

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

```
ping 172.16.0.130
```

A continuación, se muestra un ejemplo del resultado.

```
Pinging 172.16.0.130

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

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

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

Pruebe la conectividad entre la AWS región y el puesto avanzado

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

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

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

1. Obtenga la dirección IP privada de la instancia en la AWS región. Esta información está disponible en la 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
```

AWS Outposts conectividad con las AWS regiones

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

> **Note**
>
> No puedes usar la conectividad privada para tu conexión de enlace de servicio que conecta tu servidor de Outposts con tu AWS región o región de AWS Outposts origen.

Contenido

Conectividad a través de enlace de servicio

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

El Outpost puede crear la VPN del enlace de servicio a la región mediante la conectividad pública de la región de AWS . Para ello, el Outpost necesita conectividad con los rangos de IP públicas de la AWS región, ya sea a través de Internet pública o de una interfaz virtual pública. AWS Direct Connect Esta conectividad puede realizarse a través de rutas específicas en la VLAN del enlace de servicio o a través de una ruta predeterminada de 0.0.0.0/0. Para obtener más información sobre los rangos públicos AWS, consulte los rangos de direcciones AWS IP en la Guía del usuario de Amazon VPC.

Una vez establecido el enlace de servicio, el Outpost estará en servicio y será gestionado por. AWS El enlace de servicio se utiliza para el siguiente tráfico:

- Tráfico de administración que llega al Outpost a través del enlace de servicio, incluido el tráfico del plano de control interno, la supervisión de los recursos internos y las actualizaciones del firmware y el software.
- El tráfico entre el Outpost y cualquier dispositivo asociado VPCs, incluido el tráfico del plano de datos de los clientes.

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.

Tenga en cuenta lo siguiente:

- La red debe admitir una MTU de 1500 bytes entre el Outpost y los puntos finales del enlace de servicio en la región principal. AWS
- El tráfico que va desde una instancia de Outposts a una instancia de la región tiene una MTU de 1300 bytes, que es inferior a la MTU requerida de 1500 bytes debido a la sobrecarga de paquetes.

Recomendaciones de ancho de banda para el enlace de servicio

Para una experiencia y una resiliencia óptimas, AWS requiere que utilice una conectividad redundante de al menos 500 Mbps y una latencia máxima de ida y vuelta de 175 ms para la conexión del enlace de servicio a la AWS región. La utilización máxima de cada servidor de Outposts es de 500 Mbps. Para aumentar la velocidad de conexión, utilice varios servidores de Outposts. Por ejemplo, si tiene tres AWS Outposts servidores, la velocidad máxima de conexión aumenta a 1,5 Gbps (1500 Mbps). Para obtener más información, consulte Tráfico de enlace de servicio para servidores.

Los requisitos de ancho de banda de AWS Outposts Service Link varían en función de las 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. Tenga en cuenta que AWS Outposts los servidores no almacenan en caché AMIs. AMIs se descargan de la región con cada lanzamiento de una instancia.

Le recomendamos encarecidamente que consulte a su representante de AWS ventas o socio de APN para evaluar las opciones de región de origen disponibles en su zona geográfica y solicitar

una recomendación personalizada sobre los requisitos de ancho de banda y latencia del enlace de servicio para sus cargas de trabajo.

Conexiones de Internet redundantes

Al desarrollar la conectividad entre tu puesto de avanzada y la AWS región, te recomendamos que crees varias conexiones para aumentar la disponibilidad y la resiliencia. Para obtener más información, consulte Recomendaciones de resiliencia de 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.

Actualizaciones y enlace de servicio

AWS mantiene una conexión de red segura entre tu servidor de Outposts y su región principal AWS . Esta conexión de red, denominada enlace de servicio, es esencial para administrar el Outpost, ya que proporciona tráfico dentro de la VPC entre el Outpost y la región. AWS Según las prácticas recomendadas de AWS AWS Well-Architected, se deben implementar aplicaciones en dos Outposts vinculados a diferentes zonas de disponibilidad principales con un diseño activo-activo. Para obtener más información, consulte Consideraciones sobre el diseño y la arquitectura de alta disponibilidad de AWS Outposts.

El enlace de servicio se actualiza periódicamente para mantener la calidad y el rendimiento operativos. Durante el mantenimiento, es posible que observe breves períodos de latencia y pérdida de paquetes en esta red, lo que repercute en las cargas de trabajo que dependen de la conectividad de la VPC con los recursos alojados en la región. Sin embargo, el tráfico que atraviesa las interfaces de red local (LNI) no se verá afectado. Puede evitar el impacto en su aplicación si sigue las prácticas recomendadas de AWS Well-Architected y se asegura de que sus aplicaciones sean resistentes a los fallos o a las actividades de mantenimiento que afecten a un único servidor de Outposts.

Firewalls y enlace de servicio

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

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

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

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

Si utiliza un firewall activo que sea compatible con UDP y TCP para limitar la conectividad con respecto a la VLAN de enlace de servicio, puede denegar todas las conexiones entrantes. Si el firewall actúa de forma activa, las conexiones salientes permitidas desde el enlace del servicio Outposts deberían permitir automáticamente que el tráfico de respuesta vuelva a entrar sin una configuración de reglas explícita. Solo las conexiones salientes iniciadas desde el enlace del servicio Outpost deben configurarse como permitidas.

Protocolo	Puerto de origen	Dirección de origen	Puerto de destino	Dirección de destino
UDP	1024-65535	IP del enlace de servicio	53	servidor del DNS
UDP	443, 1024-65535	IP del enlace de servicio	443	AWS Outposts Puntos finales de Service Link
TCP	1024-65535	IP del enlace de servicio	443	AWS Outposts Puntos finales de registro

Si utilizas un firewall sin estado para limitar la conectividad con respecto a la VLAN de enlace de servicio, debes permitir las conexiones salientes iniciadas desde el enlace del servicio Outposts a las redes públicas de la región. AWS Outposts También debes permitir de forma explícita la entrada de tráfico de respuesta desde las redes públicas de la Región de Outposts a la VLAN de enlace de servicio. La conectividad siempre se inicia de forma saliente desde el enlace del servicio Outposts, pero se debe permitir que el tráfico de respuesta regrese a la VLAN del enlace de servicio.

Protocolo	Puerto de origen	Dirección de origen	Puerto de destino	Dirección de destino
UDP	1024-65535	IP del enlace de servicio	53	Servidor del DNS
UDP	443, 1024-65535	IP del enlace de servicio	443	AWS Outposts puntos finales de Service Link
TCP	1025-65535	IP del enlace de servicio	443	AWS Outposts Puntos finales de Service Link
UDP	53	Servidor del DNS	1025-65535	IP del enlace de servicio
UDP	443	AWS Outposts Puntos finales de Service Link	443, 1024-65535	IP del enlace de servicio
TCP	443	AWS Outposts Puntos finales de Service Link	1025-65535	IP del enlace de servicio

> **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.

Solución de problemas de red del servidor Outposts

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

Evaluación inicial

Verifica el estado del enlace del servicio a través de CloudWatch las métricas de Amazon:

1. Supervisa la ConnectedStatusmétrica en el espacio de AWS Outposts nombres.
2. Si el valor promedio es inferior a 1, esto confirma que el enlace del servicio está dañado.
3. Si el enlace de servicio está dañado, complete los pasos de las siguientes secciones para resolver y restablecer la conexión.

Paso 1. Compruebe la conectividad física

1. Compruebe que está utilizando el cable de conexión QSFP suministrado. Si los problemas persisten, pruébelo con un cable de conexión QSFP diferente, si está disponible.
2. Compruebe que el cable de conexión QSFP del servidor de Outposts esté bien colocado.
3. Compruebe que el cable 1 (LNI) esté firmemente colocado en el conmutador.
4. Compruebe que el cable 2 (enlace de servicio) esté firmemente colocado en el conmutador.
5. Realice una comprobación general del funcionamiento del conmutador, por ejemplo, compruebe las luces del enlace.

Paso 2. Pruebe la conexión del servidor de Outposts a AWS

Cree una conexión en serie con el servidor de Outposts y realice las siguientes pruebas:

1. Pruebe los enlaces.
   a. Si tiene éxito, continúe con la siguiente prueba.
   b. Si no funciona,Compruebe la configuración de la red.
2. Pruebe la resolución de DNS.
   a. Si tiene éxito, continúe con la siguiente prueba.
   b. Si no funciona,Consulte las reglas del firewall.
3. Prueba de acceso a la AWS región.
   a. Si tiene éxito, proceda a restablecer la conexión.
   b. Si se produce un error,Verifique la MTU.

Compruebe la configuración de la red

Asegúrese de que el conmutador cumpla las siguientes especificaciones:

- Configuración básica: el puerto de enlace de servicio debe ser un puerto de acceso sin etiquetas a una VLAN con una puerta de enlace y una ruta a los puntos de enlace de AWS.
- Velocidad de enlace: el puerto del conmutador debe tener una velocidad de enlace establecida en 10 Gb y la negociación automática debe estar desactivada.

Verifique la MTU

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

Consulte las reglas del firewall

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

Protocolo	Puerto de origen	Dirección de origen	Puerto de destino	Dirección de destino
UDP	1024-65535	IP del enlace de servicio	53	servidor del DNS
UDP	443, 1024-65535	IP del enlace de servicio	443	AWS Outposts Puntos finales de Service Link
TCP	1024-65535	IP del enlace de servicio	443	AWS Outposts Puntos finales de registro

Paso 3. Restablecer la conectividad

Si se aprueban las comprobaciones anteriores pero el enlace de servicio permanece `DOWN` (ConnectedStatusmide menos de 1 CloudWatch pulgada), siga los pasos de Autorizar el servidor de Outposts mediante la herramienta de configuración de Outpost para restablecer la conexión.

> **Note**
>
> Si el enlace del servicio permanece inactivo, cree un caso en el Centro.AWS Support

Devolver un servidor de Outposts

> **Note**
>
> Si recibiste un servidor dañado durante el envío, consulta el paso 2: Inspeccionar el equipo del servidor de Outposts en la guía de instalación del AWS Outposts servidor.
> Para devolver un servidor que esté en uso y desee sustituirlo o un servidor cuya suscripción haya finalizado, consulte esta sección.

Si AWS Outposts detecta un defecto en un servidor, le informaremos, iniciaremos el proceso de reemplazo para enviarle un servidor nuevo y le proporcionaremos la etiqueta de devolución en la AWS Outposts consola. No se te cobrará una tarifa de envío cuando devuelvas un servidor de Outposts. Sin embargo, si devuelves un servidor dañado, podrías incurrir en un coste.

Para comenzar, complete los siguientes pasos.

Tareas

- Paso 1: Prepare el servidor para la devolución
- Paso 2: Imprima la etiqueta de devolución
- Paso 3: Empaquete el servidor
- Paso 4: Devuelva el servidor a través del servicio de mensajería

Paso 1: Prepare el servidor para la devolución

Para preparar el servidor para la devolución, deje de compartir los recursos, haga copias de seguridad de los datos, elimine las interfaces de red locales y finalice las instancias activas.

1. Si los recursos del Outpost se comparten, debe dejar de compartirlos.

   Puede dejar de compartir un recurso de Outpost compartido de una de las siguientes formas:

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

Para ver la lista de recursos de Outpost que se pueden compartir, consulte Recursos de Outpost que se pueden compartir.

2. Cree copias de seguridad de los datos almacenados en el almacenamiento de instancias de las EC2 instancias de Amazon que se ejecutan en el AWS Outposts servidor.
3. Elimine las interfaces de red locales asociadas a las instancias que se estaban ejecutando en el servidor.
4. Finalice las instancias activas asociadas a las subredes de su Outpost. Para finalizar las instancias, sigue las instrucciones de Termina tu instancia en la Guía del EC2 usuario de Amazon.
5. Destruye la clave de seguridad Nitro (NSK) para destruir criptográficamente los datos del servidor. Para destruir la NSK, siga las instrucciones de Triture criptográficamente los datos del servidor.

Paso 2: Imprima la etiqueta de devolución

> **Important**
>
> Solo debes usar la etiqueta de devolución que se AWS proporciona porque contiene información específica, como el identificador del activo, sobre el servidor al que vas a devolver. No cree su propia etiqueta de devolución.

Para obtener tu etiqueta de devolución:

1. Abra la AWS Outposts consola en https://console.aws.amazon.com/outposts/.
2. En el panel de navegación, elija Pedidos.
3. Elige el orden del servidor que quieres devolver.
4. En la página de detalles del pedido, en la sección Estado del pedido, selecciona Imprimir etiqueta de devolución.

> **Note**
>
> La devolución de tus servidores de Outpost antes de que finalice la suscripción actual no cancelará ningún cargo pendiente asociado a este Outpost.

Paso 3: Empaquete el servidor

Para empacar su servidor, utilice la caja y el material de embalaje proporcionados por. AWS

1. Empaquete el servidor en una de las siguientes cajas:

   - La caja y el material de empaquetado en la que el servidor se entregó originalmente.
   - La caja y el material de empaquetado en la que el servidor de sustitución se entregó originalmente.

   También puede ponerse en contacto con el AWS Support Center para solicitar una caja.
2. Pegue la etiqueta de devolución AWS incluida en el exterior de la caja.

   > **Important**
   >
   > Comprueba que el identificador del activo de la etiqueta de devolución coincide con el identificador del activo del servidor que vas a devolver.
   > El ID de artículo se encuentra en la pestaña extraíble de la parte frontal del servidor.
   > Ejemplo: `1203779889` o `9305589922`
3. Selle bien la caja.

Paso 4: Devuelva el servidor a través del servicio de mensajería

Debe devolver el servidor a través del servicio de mensajería designado para su país. Puede entregar el servidor al mensajero o programar el día y la hora que prefiera para que el mensajero recoja el servidor. La etiqueta de devolución que se AWS proporciona contiene la dirección correcta para devolver el servidor.

La siguiente tabla muestra con quién debe ponerse en contacto en el país desde el que realiza el envío:

País	Contacto
Argentina	Ponerse en contacto con el AWS Support Center. En la solicitud, incluya la siguiente información: • El número de seguimiento que figura en la etiqueta AWS de devolución proporcionada • La fecha y la hora en las que prefiere que el mensajero recoja el servidor • Un nombre de contacto • Un número de teléfono • Una dirección de correo electrónico
Bahréin	
Brasil	
Brunéi	
Canadá	
Chile	
Colombia	
Hong Kong	
India	
Indonesia	
Japón	
Malasia	
Nigeria	
Omán	
Panamá	
Perú	
Filipinas	
Serbia	
Singapur	
Sudáfrica	

País	Contacto
Corea del Sur	
Taiwán	
Tailandia	
Emiratos Árabes Unidos	
Vietnam	
México	AWS contacta con DB Schenker y solicita que lo recojan en su ubicación. A continuación, DB Schenker se pondrá en contacto con usted para programar la fecha y la hora de la recogida.
Estados Unidos de América	Ponerse en contacto con UPS. Puede devolver el servidor mediante alguna de las siguientes formas: • Devolver el servidor durante una recogida rutinaria de UPS en sus instalaciones. • Dejar el servidor en una sucursal de UPS. • Programar una recogida para la fecha y hora que prefiera. Introduzca el número de seguimiento de la etiqueta de devolución AWS proporcionada para obtener el envío gratuito.

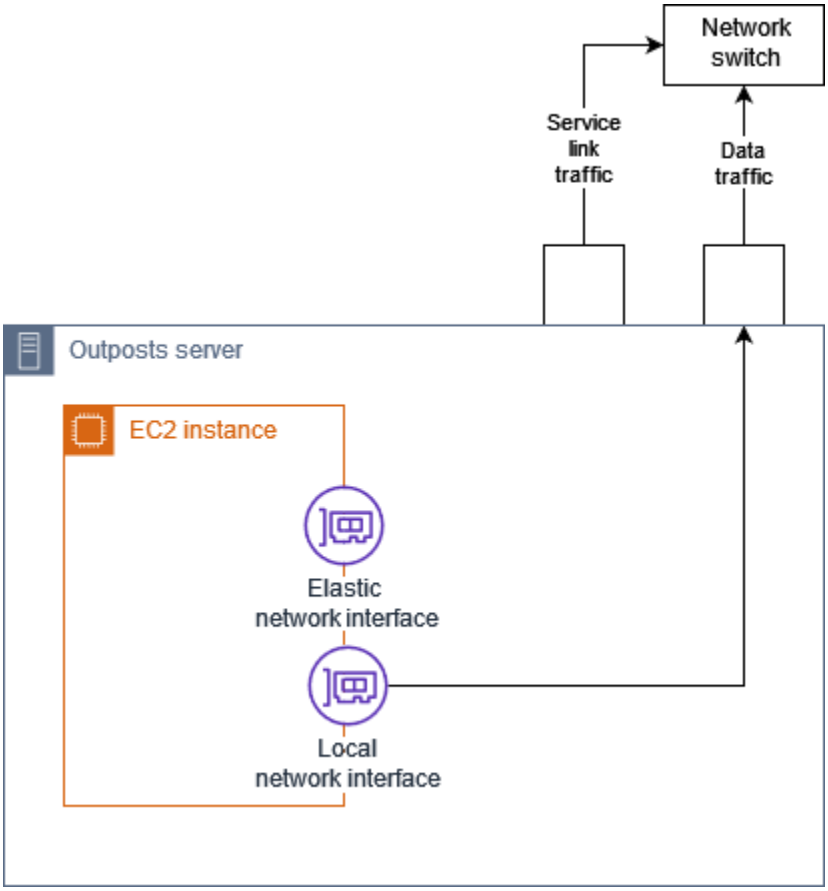
País	Contacto
Todos los otros países	Ponerse en contacto con DHL. Puede devolver el servidor mediante alguna de las siguientes formas: • Dejar el servidor en una sucursal de DHL. • Programar una recogida para la fecha y hora que prefiera. Introduce el número de guía de DHL que aparece en la etiqueta de devolución AWS proporcionada para el envío gratuito. Si aparece el siguiente `Courier pickup can't be scheduled for an import shipment` error, suele significar que el país de recuperación que ha seleccionado no coincide con el país de recuperación que aparece en la etiqueta de devolución. Seleccione el país desde el que se origina el envío e inténtelo de nuevo.

Interfaces de red local para sus servidores de Outposts

Con los servidores de Outposts, una interfaz de red local es un componente de red lógico que conecta las instancias de Amazon EC2 de la subred de Outposts a la red en las instalaciones.

Una interfaz de red local se ejecuta directamente en su red de área local. Con este tipo de conectividad local, no necesita enrutadores ni puertas de enlace para comunicarse con su equipo en las instalaciones. Las interfaces de red local reciben el mismo nombre que las interfaces de red o las interfaces de red elástica. Para distinguir entre las dos interfaces, utilizamos siempre local cuando nos referimos a las interfaces de red local.

Tras habilitar las interfaces de red local en una subred de Outpost, puede configurar las instancias EC2 de la subred de Outpost para que incluyan, además de la interfaz de red elástica, una interfaz de red local. La interfaz de red local se conecta a la red en las instalaciones, mientras que la interfaz de red se conecta a la VPC. El siguiente diagrama muestra una instancia EC2 en un servidor de Outposts con una interfaz de red elástica y una interfaz de red local.



Debe configurar el sistema operativo para permitir que la interfaz de red local se comunique con su red de área local, tal como lo haría con cualquier otro equipo en las instalaciones. No puede usar los conjuntos de opciones de DHCP en una VPC para configurar una interfaz de red local porque una interfaz de red local se ejecuta en la red de área local.

La interfaz de red elástica funciona exactamente igual que para las instancias de una subred de una zona de disponibilidad. Por ejemplo, puede usar la conexión de red de la VPC para acceder a los puntos de conexión regionales públicos Servicios de AWS, o puede usar los puntos de enlace de la VPC de la interfaz para acceder mediante. Servicios de AWS AWS PrivateLink Para obtener más información, consulte AWS Outposts conectividad con las AWS regiones.

Contenido

Conceptos básicos de la interfaz de red local

Las interfaces de red local proporcionan acceso a una red física de capa 2. Una VPC es una red de capa 3 virtualizada. Las interfaces de red local no admiten los componentes de red de VPC. Estos componentes incluyen grupos de seguridad, listas de control de acceso a la red, enrutadores virtualizados o tablas de enrutamiento y registros de flujo. La interfaz de red local no proporciona al servidor de Outposts visibilidad de los flujos de capa 3 de la VPC. El sistema operativo del host de la instancia tiene visibilidad total de las tramas de la red física. Puede aplicar una lógica de firewall estándar a la información que se encuentre dentro de estos marcos. Sin embargo, esta comunicación se produce dentro de la instancia, pero fuera del ámbito de las estructuras virtualizadas.

Consideraciones

- Las interfaces de red local admiten los protocolos ARP y DHCP. No admiten mensajes de difusión L2 generales.
- Las cuotas para las interfaces de red local provienen de su cuota para las interfaces de red. Para obtener información, consulte las cuotas de interfaz de red en la Guía del usuario de Amazon VPC.
- Cada instancia EC2 puede tener una interfaz de red local.
- Una interfaz de red local no puede usar la interfaz de red principal de la instancia.

- Los servidores de Outposts pueden alojar múltiples instancias de EC2, cada una con una interfaz de red local.

> **Note**
>
> Las instancias EC2 del mismo servidor pueden comunicarse directamente sin enviar datos fuera del servidor de Outposts. Esta comunicación incluye el tráfico a través de una interfaz de red local o de interfaces de red elásticas.

- Las interfaces de red local solo están disponibles para las instancias que se ejecutan en una subred de Outposts de un servidor de Outposts.
- Las interfaces de red local no admiten el modo promiscuo ni la suplantación de direcciones MAC.

Desempeño

La interfaz de red local de cada tamaño de instancia proporciona una parte del ancho de banda físico disponible de 10 GbE. En la siguiente tabla se enumeran los resultados de red para cada tipo de instancia:

Tipo de instancia	Banda ancha de base (Gbps)	Banda ancha con ráfagas (Gbps)
c6id.large	0,15625	2,5
c6id.xlarge	0,3125	2,5
c6id.2xlarge	0,625	2,5
c6id.4xlarge	1,25	2,5
c6id.8xlarge	2,5	2,5
c6id.12xlarge	3.75	3.75
c6id.16xlarge	5	5
c6id.24xlarge	7.5	7.5
c6id.32xlarge	10	10

Tipo de instancia	Banda ancha de base (Gbps)	Banda ancha con ráfagas (Gbps)
c6gd.medium	0,15625	4
c6gd.large	0,3125	4
c6gd.xlarge	0,625	4
c6gd.2xlarge	1,25	4
c6gd.4xlarge	2,5	4
c6gd.8xlarge	4.8	4.8
c6gd.12xlarge	7.5	7.5
c6gd.16xlarge	10	10

Grupos de seguridad

Debido a su diseño, la interfaz de red local no utiliza grupos de seguridad en la VPC. Un grupo de seguridad controla el tráfico de la VPC entrante y saliente. La interfaz de red local no está asociada a la VPC. La interfaz de red local está asociada a la red local. Para controlar el tráfico entrante y saliente en la interfaz de red local, utilice un firewall o una estrategia similar, tal como lo haría con el resto de su equipo en las instalaciones.

Supervisión

CloudWatch las métricas se generan para cada interfaz de red local, al igual que para las interfaces de red elásticas. Para obtener más información, consulte Supervisar el rendimiento de la red para ajustes ENA en la instancia de EC2 en la Guía del usuario de Amazon EC2.

Direcciones MAC

AWS proporciona direcciones MAC para las interfaces de red locales. Las interfaces de red local utilizan direcciones administradas localmente (LAA) para sus direcciones MAC. Una interfaz de red local utiliza la misma dirección MAC hasta que se elimine la interfaz. Tras eliminar una interfaz de red

local, elimine la dirección MAC de las configuraciones locales. AWS puede reutilizar las direcciones MAC que ya no se utilizan.

Agregar una interfaz de red local a una instancia de EC2 en una subred de Outposts

Puede agregar una interfaz de red local a una instancia de Amazon EC2 en una subred de Outposts durante o después del lanzamiento. Para ello, agregue una interfaz de red secundaria a la instancia mediante el uso del índice de dispositivos que especificó al habilitar la subred de Outpost para las interfaces de red local.

Consideración

Al especificar la interfaz de red secundaria mediante la consola, la interfaz de red se crea mediante el uso del índice de dispositivos 1. Si este no es el índice de dispositivos que especificó al habilitar la subred Outpost para las interfaces de red locales, puede especificar el índice de dispositivos correcto utilizando el AWS CLI o un AWS SDK en su lugar. Por ejemplo, usa los siguientes comandos de AWS CLI: create-network-interfacey. attach-network-interface

Use el siguiente procedimiento para agregar la interfaz de red local después de lanzar la instancia. Para obtener información sobre cómo agregarla durante el lanzamiento de la instancia, consulte Lanzar una instancia en Outpost.

Para agregar una interfaz de red local en una instancia de EC2:

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Red y seguridad y, a continuación, Interfaces de red.
3. Crear la interfaz de red
    a. Elija Crear interfaz de red.
    b. Seleccione la misma subred de Outpost que la instancia.
    c. Compruebe que la IPv4 dirección privada esté configurada para asignarse automáticamente.
    d. Seleccione cualquier grupo de seguridad. Los grupos de seguridad no se aplican a la interfaz de red local, por lo que el grupo de seguridad que seleccione no es relevante.
    e. Elija Crear interfaz de red.
4. Asociar una interfaz de red a una instancia

a. Seleccione la casilla de verificación de la interfaz de red recién creada.

b. Elija Acciones, Asociar.

c. Seleccione la instancia.

d. Elija Asociar. El índice de dispositivo está asociado al índice de dispositivos 1. Si especificó 1 como índice de dispositivos en la interfaz de red local para la subred de Outpost, entonces esta interfaz de red es la interfaz de red local de la instancia.

Visualice la interfaz de red local

Mientras la instancia esté en ejecución, puede utilizar la consola Amazon EC2 para visualizar la interfaz de red elástica y la interfaz de red local de las instancias de la subred de Outpost. Seleccione la instancia y haga clic en la pestaña Red.

La consola muestra una IPv4 dirección privada para la interfaz de red local desde el CIDR de la subred. Esta dirección no es la dirección IP de la interfaz de red local y no se puede utilizar. Sin embargo, esta dirección se asigna desde el CIDR de la subred, por lo que debe tenerla en cuenta al dimensionar la subred. Debe configurar la dirección IP de la interfaz de red local en el sistema operativo invitado, ya sea de forma estática o mediante el servidor DHCP.

Configuración del sistema operativo

Tras habilitar las interfaces de red local, las instancias de Amazon EC2 tendrán dos interfaces de red, y una de las cuales será una interfaz de red local. Asegúrese de configurar el sistema operativo de las instancias de Amazon EC2 que lance para que admitan una configuración de red con varios hosts.

Conectividad de red local para servidores de Outposts

Utilice este tema para comprender los requisitos de cableado y topología de la red para alojar un servidor de Outposts. Para obtener más información, consulte Interfaces de red local para sus servidores de Outposts.

Contenido

- Tráfico de enlace de servicio para servidores
- Tráfico de enlace de la interfaz de red local
- Asignación de direcciones IP del servidor
- Registro del servidor

Topología del servidor de su red

Un servidor de Outposts requiere dos conexiones distintas a su equipo de red. Cada conexión utiliza un cable diferente y transporta un tipo de tráfico diferente. Los cables múltiples sirven únicamente para aislar las clases de tráfico y no para crear redundancia. No es necesario conectar los dos cables a una red común.

En la siguiente tabla se describen los tipos y las etiquetas de tráfico del servidor de Outposts.

Etiqueta de tráfico	Description (Descripción)
2	Tráfico de enlace de servicio: este tráfico permite la comunicación entre el puesto de avanzada y la AWS región para la gestión del puesto de avanzada y el tráfico dentro de la VPC entre la AWS región y el puesto de avanzada. El tráfico del enlace de servicio incluye la conexión del enlace de servicio desde el Outpost a la región. El enlace de servicio es una VPN personalizada o va VPNs desde el Outpost a la región. El Outpost se conecta a la zona de disponibilidad de la región que haya elegido en el momento de la compra.
1	Tráfico de enlace de la interfaz de red local: este tráfico permite la comunicación desde la VPC a la LAN local a través de la interfaz de red local. El tráfico de enlaces locales incluye las instancias que se ejecutan en el Outpost y que se comunican con la red en las instalaciones. El tráfico de enlace local también

Etiqueta de tráfico	Description (Descripción)
	puede incluir instancias que se comunican con Internet a través de la red en las instalaciones.

Conectividad física del servidor

Cada servidor de Outposts incluye puertos de enlace ascendente físicos no redundantes. Los puertos tienen sus propios requisitos de velocidad y conector, tal como se indica a continuación:

- 10 GbE: conector tipo QSFP+

Cable QSFP+

El cable QSFP+ tiene un conector que debe conectar al puerto 3 del servidor de Outposts. El otro extremo del cable QSFP+ tiene cuatro interfaces SFP+ que se conectan al conmutador. Dos de las interfaces del conmutador están etiquetadas como 1 y 2. Ambas interfaces son necesarias para que un servidor de Outposts funcione. Utilice la interfaz de 2 para el tráfico de enlace de servicio y la interfaz de 1 para el tráfico de enlace de la interfaz de red local. Las interfaces restantes no se utilizan.

Tráfico de enlace de servicio para servidores

Configure el puerto de enlace de servicio del conmutador como un puerto de acceso sin etiquetas a una VLAN con una puerta de enlace y una ruta a los siguientes puntos de conexión de la región:

- Puntos de conexión del enlace de servicio
- Punto de conexión del registro de Outposts

La conexión de enlace de servicio debe tener un DNS público disponible para que el Outpost detecte su punto final de registro en la AWS región. La conexión puede tener un dispositivo NAT entre el servidor de Outposts y el punto de conexión del registro. Para obtener más información sobre los rangos de direcciones públicas AWS, consulte los rangos de direcciones AWS IP en la Guía del usuario de Amazon VPC y los AWS Outposts puntos finales y las cuotas en. Referencia general de AWS

Para registrar el servidor, abra los siguientes puertos de red:

- TCP 443
- UDP 443
- UDP 53

Tráfico de enlace de la interfaz de red local

Configure el puerto de enlace de la interfaz de red local de su dispositivo de red ascendente como un puerto de acceso estándar a una VLAN de su red local. Si tiene más de una VLAN, configure todos los puertos del dispositivo de red ascendente como puertos troncales. Configure el puerto de su dispositivo de red ascendente para poder recibir múltiples direcciones MAC. Cada instancia que se lance al servidor utilizará una dirección MAC. Algunos dispositivos de red ofrecen características de seguridad de puertos que desactivan un puerto que informa sobre múltiples direcciones MAC.

> **Note**
>
> AWS Outposts los servidores no etiquetan el tráfico de VLAN. Si configura su interfaz de red local como enlace troncal, debe asegurarse de que su sistema operativo etiquete el tráfico de la VLAN.

En el siguiente ejemplo, se muestra cómo configurar el etiquetado de la VLAN para la interfaz de red local en Amazon Linux 2023. Si utiliza otra distribución de Linux, consulte la documentación sobre la configuración del etiquetado VLAN correspondiente a su distribución de Linux.

Ejemplo: Cómo configurar el etiquetado de la VLAN para la interfaz de red local en Amazon Linux 2023 y Amazon Linux 2

1. Asegúrese de que el módulo 8021q esté cargado en el kernel. Si no es así, cárguelo con el comando `modprobe`.

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

2. Cree el dispositivo de la VLAN. En este ejemplo:

   - El nombre de la interfaz de red local es `ens6`
   - El ID de la VLAN es 59
   - El nombre asignado al dispositivo de la VLAN es `ens6.59`

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

3. Opcional. Complete este paso si desea asignar la IP de forma manual. En este ejemplo, asignamos la IP 192.168.59.205, donde el CIDR de la subred es 192.168.59.0/24.

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

4. Active el enlace.

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

Para configurar las interfaces de red a nivel del sistema operativo y hacer que los cambios en el etiquetado de la VLAN sean persistentes, consulte los siguientes recursos:

- Si utiliza Amazon Linux 2, consulte Configurar la interfaz de red mediante ec2-net-utils en AL2 la Guía del usuario de Amazon Linux 2.
- Si utiliza Amazon Linux 2023, consulte Servicio de red en la Guía del usuario de Amazon Linux 2023.

Asignación de direcciones IP del servidor

No necesita asignar direcciones IP públicas para el enlace de servicio AWS Outposts del servidor ni para las interfaces de red local en las instancias. Para el enlace de servicio, puede asignar direcciones IP manualmente o usar el protocolo de control dinámico de host (DHCP). Para configurar la conexión del enlace de servicio, consulte Configurar y probar la conexión en la guía de instalación AWS Outposts del servidor.

Para configurar el enlace de la interfaz de red local, consultethe section called “Configuración del sistema operativo”.

> **Note**
>
> Asegúrese de utilizar una dirección IP estable para el servidor de Outposts. Los cambios en la dirección IP pueden provocar interrupciones temporales del servicio en la subred de Outpost.

Registro del servidor

Cuando los servidores de Outposts establecen una conexión en la red local, utilizan la conexión de enlace de servicio para conectarse a los puntos de conexión de registro de Outpost y registrarse ellos mismos. El registro requiere un DNS público. Cuando los servidores se registran, crean un túnel seguro hasta su punto de conexión del enlace de servicio en la región. Los servidores de Outposts utilizan el puerto TCP 443 para facilitar la comunicación con la región a través de Internet pública. Los servidores de Outposts no admiten la conectividad privada a través de VPC.

Administración de capacidad para AWS Outposts

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

Temas

Consulte AWS Outposts la capacidad

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

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

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

Modifique la capacidad de las AWS Outposts instancias

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

Consideraciones

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

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

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

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

1. Abre la AWS Outposts consola en. https://console.aws.amazon.com/outposts/
2. En el panel de navegación izquierdo, selecciona Tareas de capacidad.
3. En la página Tareas de capacidad, seleccione Crear tarea de capacidad.
4. En la página de introducción, elige el pedido, el puesto de avanzada o el activo que deseas configurar.
5. Para modificar la capacidad, especifique una opción en Método de modificación: pasos electrónicos en la consola o cargue un archivo JSON.
   - Modifique el plan de configuración de la capacidad para seguir los pasos de la consola
   - Cargue un plan de configuración de capacidad para cargar un archivo JSON

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

Console steps

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

   a. Elija el tamaño de instancia.

   b. Seleccione Equilibrio automático al final de la sección relacionada con el tipo de instancia.
10. Para cada tipo de instancia, asegúrese de que la cantidad de instancias esté especificada para al menos un tamaño de instancia.
11. Si lo desea, elija instancias para mantenerlas tal como están.
12. Elija Siguiente.
13. En la página Revisar y crear, compruebe las actualizaciones que solicita.

14. Elija Crear. AWS Outposts crea una tarea de capacidad.
15. En la página de tareas de capacidad, supervise el estado de la tarea.

Upload a JSON file

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

   Example

   Ejemplo de archivo JSON:

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

4. Revise el contenido del archivo JSON en la sección Plan de configuración de capacidad.

5. Elija Siguiente.
6. En la página Revisar y crear, compruebe las actualizaciones que solicita.
7. Seleccione Crear. AWS Outposts crea una tarea de capacidad.
8. En la página de tareas de capacidad, supervise el estado de la tarea.

Solución de problemas de tareas de capacidad

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

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

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

Para resolver este problema, siga estos pasos:

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

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

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

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

Uso de la consola

1. Inicie sesión en AWS.

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

Utilizar la CLI de

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

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

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

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

Para resolver este problema, siga estos pasos:

1. Anota la AWS región que utilizaste en la solicitud de `StartCapacityTask` API.
2. Usa la acción de la `ListOutposts`API para obtener una lista de los Outposts de tu propiedad en la AWS región.
3. Comprueba si el ID de Outpost aparece en la lista.
4. Introduce el ID de Outpost correcto en la `StartCapacityTask` solicitud.
5. Si no encuentras el ID de Outpost, vuelve a utilizar la acción de la `ListOutposts` API para comprobar si el Outpost existe en una región diferente. AWS

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

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

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

Uso de la consola

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

Utilizar la CLI de

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

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

Este problema se produce cuando utilizas la AWS Outposts consola o la API para ejecutar StartCapacityTaskun activo y ya existe una tarea de capacidad de ejecución

para el activo. Se considera que una tarea de capacidad está en ejecución si tiene alguno de los siguientes estados:`REQUESTED`, `IN_PROGRESSWAITING_FOR_EVACUATION`, o`CANCELLATION_IN_PROGRESS`.

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

Uso de la consola

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

Utilizar la CLI de

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

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

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

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

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

Uso de la consola

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

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

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

Utilizar la CLI de

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

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

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

Comparta sus AWS Outposts recursos

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

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

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

Un propietario de Outpost puede compartir recursos de Outpost con:

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

Contenido

- Uso compartido de un recurso de Outpost
- 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.

Para ver los recursos del servidor de Outposts, consulta Cómo trabajar con recursos compartidos AWS Outposts.

A continuación, se describen los recursos disponibles para los bastidores de Outposts. Para ver los recursos del rack de Outposts, consulta Cómo trabajar con AWS Outposts recursos compartidos en la Guía del AWS Outposts usuario de los racks de Outposts.

- Hosts dedicados asignados: los consumidores con acceso a este recurso pueden:
  - Lance y ejecute instancias EC2 en un host dedicado.
- Outposts: los consumidores con acceso a este recurso pueden:
  - Crear y administrar una subred en el Outpost.
  - Usa la AWS Outposts API para ver información sobre 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, debes tenerlo en tu AWS cuenta. No puede compartir un recurso de Outpost que se haya compartido con usted.
- Para compartir un recurso de Outpost, debe compartirlo con una cuenta que se encuentre dentro de la organización.

Servicios relacionados

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

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

Uso compartido entre zonas de disponibilidad

Para garantizar que los recursos se distribuyen por todas las zonas de disponibilidad de una región, asignamos zonas de disponibilidad de manera independiente a nombres de cada cuenta. Esto podría dar lugar a diferencias de nomenclatura de zona de disponibilidad entre cuentas. Por ejemplo, es posible que la zona `us-east-1a` de disponibilidad de su AWS cuenta no tenga la misma ubicación que la `us-east-1a` de otra AWS cuenta.

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

Para ver las IDs zonas de disponibilidad de su cuenta

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

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

Uso compartido de un recurso de Outpost

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

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

Si formas parte de una organización AWS Organizations y el uso compartido dentro de tu organización está activado, puedes conceder a los consumidores de tu organización acceso desde la AWS RAM consola al recurso de Outpost compartido. De lo contrario, los consumidores reciben una invitación para unirse al recurso compartido y se les concede acceso al recurso de Outpost compartido al aceptar la invitación.

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

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

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

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

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

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

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

Utilice el comando create-resource-share.

Dejar de compartir un recurso de Outpost compartido

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

- Ve el Outpost en la AWS Outposts consola.
- Crear nuevas subredes en el Outpost.
- Crear y administrar volúmenes de EBS en el Outpost.
- Vea los detalles de Outpost y los tipos de instancias mediante la AWS Outposts consola o el. AWS CLI

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

- Acceder a estos recursos y modificarlos.

- Lanzar nuevas instancias en una subred existente que haya creado el consumidor.

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

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

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

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

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

Para dejar de compartir un recurso de Outpost compartido que te pertenezca mediante el AWS CLI

Utilice el comando disassociate-resource-share.

Identificación de un recurso de Outpost compartido

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

Para identificar un Outpost compartido mediante la consola AWS Outposts

1. Abre la AWS Outposts consola en. https://console.aws.amazon.com/outposts/
2. En el panel de navegación, elija Outposts.
3. Seleccione el Outpost y, a continuación, elija Acciones, Ver detalles.
4. En la página de resumen de Outpost, consulta el ID de propietario para identificar el ID de AWS cuenta del propietario de Outpost.

Para identificar un recurso de Outpost compartido mediante el AWS CLI

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

Permisos de recursos de Outpost compartidos

Permisos de los propietarios

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

Permisos de los consumidores

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

Facturación y medición

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

No se aplican cargos adicionales por compartir tablas de enrutamiento de la puerta de enlace local. En el caso de las subredes compartidas, se facturan al propietario de la VPC los recursos de nivel de VPC, Direct Connect como las conexiones VPN, las puertas de enlace NAT y las conexiones de enlace privado.

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

Limitaciones

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

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

Con los servidores Outposts, puedes aprovechar los datos existentes que están almacenados en matrices de almacenamiento de terceros. Puede especificar volúmenes de datos de bloques externos y volúmenes de arranque de bloques externos para sus instancias EC2 en Outposts. Con esta integración, puede utilizar volúmenes de arranque y datos en bloque externos respaldados por proveedores externos, como Dell, HPE Alletra Storage MP B10000 PowerStore, cabinas de almacenamiento empresarial NetApp locales y sistemas de almacenamiento Pure Storage. FlashArray

Consideraciones

- Disponible en los racks Outposts y en los servidores Outposts 2U. No disponible en los servidores Outposts 1U.
- Disponible en todas AWS las regiones donde se admiten los servidores Outposts 2U.
- Disponible sin coste adicional.
- Usted es responsable de la configuración y la day-to-day administración del arreglo de almacenamiento. También crea y administra los volúmenes de bloques externos en la matriz de almacenamiento. Si tiene problemas con el hardware, el software o la conectividad del arreglo de almacenamiento, póngase en contacto con el proveedor de almacenamiento externo.

> **Note**
>
> El volumen de bloques almacenado en su arreglo de almacenamiento externo contiene el sistema operativo que se iniciará en una instancia EC2 en Outposts. No se admite el lanzamiento de una AMI respaldada por matrices de almacenamiento externas. Para lanzar una AMI, se utiliza el almacenamiento de instancias en el servidor de Outposts.

Volúmenes de datos en bloques externos

Tras aprovisionar y configurar los volúmenes de datos en bloque respaldados por un sistema de almacenamiento de terceros compatible, puede adjuntar los volúmenes a las instancias de EC2 al lanzarlas. Si configura los volúmenes para la conexión múltiple en el arreglo de almacenamiento, puede adjuntar un volumen a varias instancias de EC2.

Pasos clave

- Usted es responsable de establecer la conectividad entre las subredes de Outpost y la red local a través de la interfaz de red local.
- Utilice la interfaz de administración de la matriz de almacenamiento externo para crear el volumen. A continuación, configurará la asignación de iniciadores creando un nuevo grupo de iniciadores y añadiendo el nombre cualificado iSCSI (IQN) de la instancia EC2 de destino a este grupo. Esto asocia el volumen de datos de bloques externo a la instancia EC2.
- El volumen de datos externo se añade al lanzar la instancia. Necesitarás el IQN del iniciador, la dirección IP de destino, el puerto y el IQN de la matriz de almacenamiento externo. Para obtener más información, consulte Lanzar una instancia en el Outpost.

Para obtener más información, consulte Simplificar el uso del almacenamiento en bloque de terceros con. AWS Outposts

Volúmenes de arranque en bloque externos

El arranque de una instancia EC2 en Outposts desde matrices de almacenamiento externas proporciona una solución centralizada, rentable y eficiente para las cargas de trabajo locales que dependen del almacenamiento de terceros. Puede elegir entre las opciones siguientes:

Arranque de SAN iSCSI

Proporciona un arranque directo desde el arreglo de almacenamiento externo. Utiliza una AMI auxiliar AWS de iPXE proporcionada para que las instancias puedan arrancar desde una ubicación de red. Cuando iPXE se combina con iSCSI, la instancia EC2 trata el destino iSCSI remoto (el arreglo de almacenamiento) como un disco local. Todas las operaciones de lectura y escritura del sistema operativo se realizan en el arreglo de almacenamiento externo.

iSCSI o NVMe-over-TCP LocalBoot

Lanza las instancias EC2 mediante una copia del volumen de arranque recuperado del arreglo de almacenamiento, sin modificar la imagen de origen original. Lanzamos una instancia auxiliar mediante una LocalBoot AMI. Esta instancia auxiliar copia el volumen de arranque del arreglo de almacenamiento al almacén de instancias de la instancia EC2 y actúa como iniciador o host iSCSI. NVMe-over-TCP Por último, la instancia EC2 se reinicia utilizando el volumen de almacenamiento de instancias local.

Como el almacén de instancias es un almacenamiento temporal, el volumen de arranque se elimina cuando se termina la instancia EC2. Por lo tanto, esta opción es adecuada para los volúmenes de arranque de solo lectura, como los que se utilizan en la infraestructura de escritorios virtuales (VDI).

No puede arrancar instancias EC2 de Windows con. NVMe-over-TCP LocalBoot Esto solo se admite con instancias EC2 de Linux.

Para obtener más información, consulte Implementación de volúmenes de arranque externos para usarlos con AWS Outposts.

Seguridad en AWS Outposts

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

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

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

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

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

Contenido

Protección de datos en AWS Outposts

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

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

Para obtener más información sobre la privacidad de los datos, consulte las 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 servidores de Outposts.

Cifrado en tránsito

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

Eliminación de datos

Al 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. Para obtener más información, consulte Destrucción criptográfica de los datos del servidor.

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

Característica de IAM	AWS Soporte para Outposts
Políticas basadas en identidades	Sí
Políticas basadas en recursos	No
Acciones de políticas	Sí
Recursos de políticas	Sí
Claves de condición de política (específicas del servicio)	Sí
ACLs	No
ABAC (etiquetas en políticas)	Sí
Credenciales temporales	Sí
Permisos de entidades principales	Sí

Característica de IAM	AWS Soporte para Outposts
Roles de servicio	No
Roles vinculados al servicio	Sí

Políticas basadas en la identidad para Outposts AWS

Compatibilidad con las políticas basadas en identidad: sí

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

Ejemplos de políticas basadas en identidad para Outposts AWS

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

Acciones políticas para AWS Outposts

Compatibilidad con las acciones de políticas: sí

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

El elemento `Action` de una política JSON describe las acciones que puede utilizar para conceder o denegar el acceso en una política. Incluya acciones en una política para conceder permisos y así llevar a cabo la operación asociada.

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

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

```
outposts
```

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

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

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

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

Recursos de políticas para AWS Outposts

Compatibilidad con los recursos de políticas: sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal 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. Como práctica recomendada, especifique un recurso utilizando el Nombre de recurso de Amazon (ARN). En el caso de las acciones que no admiten permisos por recurso, 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 sola sentencia, sepárelos ARNs con comas.

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

Para ver una lista de los tipos de recursos de AWS Outposts y sus tipos ARNs, consulta los tipos de recursos definidos AWS Outposts en la Referencia de autorización de servicio. Para obtener

información sobre las acciones con las que puede especificar el ARN de cada recurso, consulte Acciones definidas por AWS Outposts.

Claves condicionales de la política para AWS Outposts

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

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

El elemento `Condition` especifica cuándo se ejecutan las instrucciones en función de criterios definidos. Puede crear expresiones condicionales que utilizan operadores de condición, tales como igual o menor que, para que la condición de la política coincida con los valores de la solicitud. Para ver todas las claves de condición AWS globales, consulte las claves de contexto de condición AWS globales en la Guía del usuario de IAM.

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

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

ABAC con Outposts AWS

Admite ABAC (etiquetas en las políticas): sí

El control de acceso basado en atributos (ABAC) es una estrategia de autorización que define permisos en función de atributos denominados etiquetas. Puede adjuntar etiquetas a las entidades y AWS los recursos de IAM y, a continuación, diseñar políticas de ABAC para permitir las operaciones cuando la etiqueta del principal coincida con la etiqueta del recurso.

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

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

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

Uso de credenciales temporales con AWS Outposts

Compatibilidad con credenciales temporales: sí

Las credenciales temporales proporcionan acceso a AWS los recursos a corto plazo y se crean automáticamente cuando utilizas la federación o cambias de rol. AWS recomienda generar credenciales temporales de forma dinámica en lugar de utilizar claves de acceso a largo plazo. Para obtener más información, consulte Credenciales de seguridad temporales en IAM y Servicios de AWS que funcionan con IAM en la Guía del usuario de IAM.

Permisos principales entre servicios para Outposts AWS

Admite sesiones de acceso directo (FAS): sí

Las sesiones de acceso directo (FAS) utilizan los permisos del operador principal que realiza la llamada Servicio de AWS, junto con los que solicitan, Servicio de AWS para realizar solicitudes a los servicios descendentes. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte Sesiones de acceso directo.

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. Funciones vinculadas al servicio para AWS Outposts

AWS Ejemplos de políticas de Outposts

De forma predeterminada, los usuarios y los roles no tienen permiso para crear o modificar los recursos de AWS Outposts. Un administrador de IAM puede crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan.

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

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

Contenido

Prácticas recomendadas sobre las políticas

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

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos: para empezar a conceder permisos a sus usuarios y cargas de trabajo, utilice las políticas AWS administradas que otorgan permisos para muchos casos de uso comunes. Están disponibles en su. Cuenta de AWS Le recomendamos que reduzca aún más los permisos definiendo políticas administradas por el AWS cliente que sean específicas para sus casos de uso. Con el fin de obtener más información, consulte las políticas administradas por AWS o las políticas administradas por AWS para funciones de tarea en la Guía de usuario de IAM.
- Aplique permisos de privilegio mínimo: cuando establezca permisos con políticas de IAM, conceda solo los permisos necesarios para realizar una tarea. Para ello, debe definir las acciones que se pueden llevar a cabo en determinados recursos en condiciones específicas, también conocidos como permisos de privilegios mínimos. Con el fin de obtener más información sobre el uso de IAM para aplicar permisos, 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

CloudFormation. Para obtener más información, consulte Elementos de la política de JSON de IAM: Condición en la Guía del usuario de IAM.

- Utiliza el analizador de acceso de IAM para validar las políticas de IAM con el fin de garantizar la seguridad y funcionalidad de los permisos: el analizador de acceso de IAM valida políticas nuevas y existentes para que respeten el lenguaje (JSON) de las políticas de IAM y las prácticas recomendadas de IAM. El analizador de acceso de IAM proporciona más de 100 verificaciones de políticas y recomendaciones procesables para ayudar a crear políticas seguras y funcionales. Para más información, consulte Validación de políticas con el Analizador de acceso de IAM en la Guía del usuario de IAM.
- Requerir autenticación multifactor (MFA): si tiene un escenario que requiere usuarios de IAM o un usuario raíz en Cuenta de AWS su cuenta, active la MFA para mayor seguridad. Para exigir la MFA cuando se invoquen las operaciones de la API, añada condiciones de MFA a sus políticas. Para más información, consulte Acceso seguro a la API con MFA en la Guía del usuario de IAM.

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

Ejemplo: uso de permisos de nivel de recursos

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

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "outposts:GetOutpost",
            "Resource": "arn:aws:outposts:us-east-1:111122223333:outpost/
op-1234567890abcdef0"
        }
    ]
}
```

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

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "outposts:GetSite",
            "Resource": "arn:aws:outposts:us-east-1:111122223333:site/
os-0abcdef1234567890"
        }
    ]
}
```

Funciones vinculadas al servicio para AWS Outposts

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

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

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

Permisos de rol vinculados al servicio para AWS Outposts

AWS Outposts usa el rol vinculado al servicio denominado AWSService RoleForOutposts _. ***OutpostID*** Este rol otorga a Outposts permisos para administrar los recursos de red y habilitar la conectividad privada en tu nombre. Esta función también permite a Outposts crear y configurar

interfaces de red, gestionar grupos de seguridad y adjuntar interfaces a instancias de punto final de enlace de servicio. Estos permisos son necesarios para establecer y mantener una conexión privada y segura entre tu Outpost local y los AWS servicios, lo que garantiza un funcionamiento fiable de tu implementación de Outpost.

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

- `outposts.amazonaws.com`

Políticas de funciones vinculadas al servicio

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

- AWSOutpostsServiceRolePolicy
- AWSOutpostsPrivateConnectivityPolicy_*`OutpostID`*

AWSOutpostsServiceRolePolicy

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

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

- Acción: `ec2:DescribeNetworkInterfaces` en todos los AWS recursos
- Acción: `ec2:DescribeSecurityGroups` sobre todos los AWS recursos
- Acción: `ec2:CreateSecurityGroup` sobre todos los AWS recursos
- Acción: `ec2:CreateNetworkInterface` sobre todos los AWS recursos

AWSOutpostsPrivateConnectivityPolicy_OutpostID

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

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

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

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

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

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

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

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

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

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

Cree un rol vinculado a un servicio para AWS Outposts

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

Edita un rol vinculado a un servicio para AWS Outposts

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

Elimine un rol vinculado a un servicio para AWS Outposts

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

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

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

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

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

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

Para eliminar manualmente el rol vinculado a servicios mediante IAM

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

Regiones compatibles para los roles vinculados AWS Outposts al servicio

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

AWS políticas gestionadas para AWS Outposts

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

Ten en cuenta que es posible que las políticas AWS administradas no otorguen permisos con privilegios mínimos para tus casos de uso específicos, ya que están disponibles para que los usen

todos los AWS clientes. Se recomienda definir políticas administradas por el cliente específicas para sus casos de uso a fin de reducir aún más los permisos.

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

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

AWS política gestionada: AWSOutposts ServiceRolePolicy

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

AWS política gestionada: AWSOutposts AuthorizeServerPolicy

Utilice esta política para conceder los permisos necesarios para autorizar el hardware del servidor de Outposts en su red en las instalaciones.

Esta política incluye los siguientes permisos.

JSON

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

AWS Outposts actualiza las políticas gestionadas AWS

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

Cambio	Descripción	Fecha
AWSOutpostsAuthorizeServerPolicy: política nueva	AWS Outposts agregó una política que otorga permisos para autorizar el hardware del servidor de Outposts en tu red local.	4 de enero de 2023
AWS Outposts comenzó a rastrear los cambios	AWS Outposts comenzó a rastrear los cambios en sus políticas AWS gestionadas.	03 de diciembre de 2019

Seguridad de la infraestructura en AWS Outposts

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

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

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

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.

Resiliencia en AWS Outposts

Para una alta disponibilidad, puede , solicitar servidores de Outpost adicionales. 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, 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.

Los servidores de Outposts incluyen volúmenes de almacenes de instancias, pero no admiten los volúmenes de Amazon EBS. Los datos de los volúmenes del almacén de instancias persisten tras el reinicio de la instancia, pero no persisten tras la finalización de la instancia. Para retener los datos a largo plazo de los volúmenes de almacén de instancias más allá de la vida útil de la instancia, asegúrese de realizar una copia de seguridad de los datos en un almacenamiento persistente, como un bucket de Amazon S3 o un dispositivo de almacenamiento de red en su red en las instalaciones.

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. Para obtener más información sobre su responsabilidad de conformidad al utilizarlos Servicios de AWS, consulte AWS la documentación de seguridad.

Supervisión de servidores de Outposts

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

CloudWatch métricas

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

CloudTrail registros

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

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

Logs de flujo de VPC

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

Replicación de tráfico

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

Panel de AWS Health

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

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

CloudWatch

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

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

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

Contenido

Métricas de la instancia

Las siguientes métricas están disponibles para las instancias de Amazon EC2.

Métrica	Dimensión	Description (Descripción)
`InstanceFamilyCapacityAvailability`	`InstanceFamily` y `OutpostId`	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).
`InstanceFamilyCapacityUtilization`	`Account`, `InstanceFamily` , y `OutpostId`	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

Métrica	Dimensión	Description (Descripción)
		Estadísticas: las estadísticas más útiles son `Average` y `pNN.NN` (percentiles).
`InstanceTypeCapacityAvailability`	`InstanceType` y `OutpostId`	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).
`InstanceTypeCapacityUtilization`	`Account`, `InstanceType` , y `OutpostId`	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).

Métrica	Dimensión	Description (Descripción)
`UsedInstanceType_Count`	`Account`, `InstanceType` , y `OutpostId`	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

Métrica	Dimensión	Description (Descripción)
`AvailableInstanceType_Count`	`InstanceType` y `OutpostId`	El número de tipos de instancias disponibles. Esta métrica incluye el recuento de `AvailableReservedInstances`. Para determinar el número de instancias que puede reservar, reste el recuento de `AvailableReservedInstances` del recuento de `AvailableInstanceType_Count`. `Number of instances that you can reserve = AvailableInstanceType_Count - AvailableReservedInstances` Esta métrica no incluye la capacidad de ningún host dedicado configurado en el Outpost. Unidad: recuento Resolución máxima: 5 minutos

Métrica	Dimensión	Description (Descripción)
`AvailableReservedInstances`	`InstanceType` y `OutpostId`	El número de instancias que están disponibles para su lanzamiento en la capacidad de computación reservada mediante reservas de capacidad. Esta métrica no incluye instancias reservadas de Amazon EC2. Esta métrica no incluye el número de instancias que puede reservar. Para determinar el número de instancias que puede reservar, reste el recuento de `AvailableReservedInstances` del recuento de `AvailableInstanceType_Count` . `Number of instances that you can reserve = AvailableInstanceType_Count - AvailableReservedInstances` Unidad: recuento Resolución máxima: 5 minutos

Métrica	Dimensión	Description (Descripción)
`UsedReservedInstances`	`InstanceType` y `OutpostId`	El número de instancias que se están ejecutando en la capacidad de computación reservada mediante reservas de capacidad. Esta métrica no incluye instancias reservadas de Amazon EC2. Unidad: recuento Resolución máxima: 5 minutos
`TotalReservedInstances`	`InstanceType` y `OutpostId`	El número total de instancias, en ejecución y disponibles para su lanzamiento, proporcionado por la capacidad de computación reservada mediante reservas de capacidad. Esta métrica no incluye instancias reservadas de Amazon EC2. Unidad: recuento Resolución máxima: 5 minutos

Métricas de Outposts

Las siguientes métricas están disponibles para tus Outposts.

Métrica	Dimensión	Description (Descripción)
`ConnectedStatus`	`OutpostId`	El estado de la conexión de enlace de servicio de un Outpost. Si la estadísti

Métrica	Dimensión	Description (Descripción)
		ca media es inferior a 1, la conexión está dañada. Unidad: recuento Resolución máxima: 1 minuto Estadísticas: la estadística más útil es `Average`.
`CapacityExceptions`	`InstanceType` y `OutpostId`	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 de la métrica

Para filtrar las métricas de su Outpost, utilice las siguientes dimensiones.

Dimensión	Description (Descripción)
`Account`	La cuenta o el servicio que utiliza la capacidad.
`InstanceFamily`	La familia de instancias.
`InstanceType`	El tipo de instancia.
`OutpostId`	El ID del Outpost.

Puedes ver las CloudWatch métricas de tu servidor de Outposts mediante la CloudWatch consola.

Para ver las métricas mediante la consola CloudWatch

1. Abra la CloudWatch consola en https://console.aws.amazon.com/cloudwatch/.
2. En el panel de navegación, seleccione Métricas.
3. Selecciona el espacio de nombres de Outposts.
4. (Opcional) Para ver una métrica en todas las dimensiones, ingrese su nombre en el campo de búsqueda.

Para ver las métricas mediante el AWS CLI

Utilice el siguiente comando list-metrics para obtener una lista de las métricas disponibles.

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

Para obtener las estadísticas de una métrica mediante el AWS CLI

Utilice el siguiente get-metric-statisticscomando para obtener las estadísticas de la métrica y la dimensión especificadas. CloudWatch trata cada combinación única de dimensiones como una métrica independiente. No se pueden recuperar estadísticas utilizando combinaciones de dimensiones que no se han publicado expresamente. Debe especificar las mismas dimensiones que se utilizaron al crear las métricas.

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

Registre las llamadas a la AWS Outposts API mediante AWS CloudTrail

AWS Outposts está integrado con AWS CloudTrail un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o un AWS servicio. CloudTrail captura las llamadas a la API AWS Outposts como eventos. Las llamadas capturadas incluyen llamadas desde la

AWS Outposts consola y llamadas en código a las operaciones de la AWS Outposts API. Con la información recopilada por CloudTrail, puede determinar a qué solicitud se realizó AWS Outposts, la dirección IP desde la que se realizó la solicitud, cuándo se realizó y detalles adicionales.

Cada entrada de registro o evento contiene información sobre quién generó la solicitud. La información de identidad del usuario le ayuda a determinar lo siguiente:

- Si la solicitud se realizó con las credenciales del usuario raíz o del usuario.
- Si la solicitud se realizó en nombre de un usuario de IAM Identity Center.
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado.
- Si la solicitud la realizó otro Servicio de AWS.

CloudTrail está activa en tu AWS cuenta cuando la creas y tienes acceso automáticamente al historial de CloudTrail eventos. El historial de CloudTrail eventos proporciona un registro visible, consultable, descargable e inmutable de los últimos 90 días de eventos de gestión registrados en un. Región de AWSPara obtener más información, consulte Uso del historial de CloudTrail eventos en la Guía del usuario.AWS CloudTrail La visualización del historial de eventos no conlleva ningún CloudTrail cargo.

Para tener un registro continuo de los eventos de Cuenta de AWS los últimos 90 días, crea un almacén de datos de eventos de senderos o CloudTrail lagos.

CloudTrail senderos

Un rastro permite CloudTrail entregar archivos de registro a un bucket de Amazon S3. Todos los senderos creados con él Consola de administración de AWS son multirregionales. Puede crear un registro de seguimiento de una sola región o multirregionales mediante la AWS CLI. Se recomienda crear un sendero multirregional, ya que puedes capturar toda la actividad de tu Regiones de AWS cuenta. Si crea un registro de seguimiento de una sola región, solo podrá ver los eventos registrados en la Región de AWS del registro de seguimiento. Para obtener más información acerca de los registros de seguimiento, consulte Creación de un registro de seguimiento para su Cuenta de AWS y Creación de un registro de seguimiento para una organización en la Guía del usuario de AWS CloudTrail .

Puede enviar una copia de sus eventos de administración en curso a su bucket de Amazon S3 sin coste alguno CloudTrail mediante la creación de una ruta; sin embargo, hay cargos por almacenamiento en Amazon S3. Para obtener más información sobre CloudTrail los precios,

consulte AWS CloudTrail Precios. Para obtener información acerca de los precios de Amazon S3, consulte Precios de Amazon S3.

CloudTrail Almacenes de datos de eventos en Lake

CloudTrail Lake le permite ejecutar consultas basadas en SQL en sus eventos. CloudTrail Lake convierte los eventos existentes en formato JSON basado en filas al formato Apache ORC. ORC es un formato de almacenamiento en columnas optimizado para una recuperación rápida de datos. Los eventos se agregan en almacenes de datos de eventos, que son recopilaciones inmutables de eventos en función de criterios que se seleccionan aplicando selectores de eventos avanzados. Los selectores que se aplican a un almacén de datos de eventos controlan los eventos que perduran y están disponibles para la consulta. Para obtener más información sobre CloudTrail Lake, consulte Cómo trabajar con AWS CloudTrail Lake en la Guía del AWS CloudTrail usuario.

CloudTrail Los almacenes de datos y las consultas sobre eventos de Lake conllevan costes. Cuando crea un almacén de datos de eventos, debe elegir la opción de precios que desee utilizar para él. La opción de precios determina el costo de la incorporación y el almacenamiento de los eventos, así como el período de retención predeterminado y máximo del almacén de datos de eventos. Para obtener más información sobre CloudTrail los precios, consulte AWS CloudTrail Precios.

AWS Outposts eventos de gestión en CloudTrail

Los eventos de administración proporcionan información sobre las operaciones de administración que se llevan a cabo en los recursos de su empresa Cuenta de AWS. Se denominan también operaciones del plano de control. De forma predeterminada, CloudTrail registra los eventos de administración.

AWS Outposts registra todas las operaciones del plano de control de AWS Outposts como eventos de gestión. Para obtener una lista de las operaciones del plano de control de AWS Outposts en las que AWS Outposts inicia sesión, CloudTrail consulta la Referencia de la API de AWS Outposts.

AWS Outposts ejemplos de eventos

El siguiente ejemplo muestra un CloudTrail evento que demuestra la `SetSiteAddress` operación.

```
{
    "eventVersion": "1.05",
```

```
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AKIAIOSFODNN7EXAMPLE:jdoe",
        "arn": "arn:aws:sts::111122223333:assumed-role/example/jdoe",
        "accountId": "111122223333",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AKIAIOSFODNN7EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/example",
                "accountId": "111122223333",
                "userName": "example"
            },
            "webIdFederationData": {},
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2020-08-14T16:28:16Z"
            }
        }
    },
    "eventTime": "2020-08-14T16:32:23Z",
    "eventSource": "outposts.amazonaws.com",
    "eventName": "SetSiteAddress",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "XXX.XXX.XXX.XXX",
    "userAgent": "userAgent",
    "requestParameters": {
        "SiteId": "os-123ab4c56789de01f",
        "Address": "***"
    },
    "responseElements": {
        "Address": "***",
        "SiteId": "os-123ab4c56789de01f"
    },
    "requestID": "1abcd23e-f4gh-567j-klm8-9np01q234r56",
    "eventID": "1234a56b-c78d-9e0f-g1h2-34jk56m7n890",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
```

Mantenimiento de servidores de Outposts

Según el modelo de responsabilidad compartida de AWS es responsable del hardware y el software que ejecutan AWS los servicios. Esto se aplica a una AWS región AWS Outposts, igual que a ella. Por ejemplo, AWS administra los parches de seguridad, actualiza el firmware y mantiene el equipo de Outpost. AWS también supervisa el rendimiento, el estado y las métricas de su servidor Outposts y determina si es necesario realizar algún tipo de mantenimiento.

> **Warning**
>
> Los datos de los volúmenes del almacén de instancias se pierden si se produce un error en la unidad de disco subyacente o si la instancia finaliza. Para evitar la pérdida de datos, te recomendamos que guardes 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 o un dispositivo de almacenamiento en red de tu red local.

Contenido

Actualización de los datos de contacto

Si el propietario de Outpost cambia, comuníquese con AWS Support Center para facilitarles el nombre y la información de contacto del nuevo propietario.

Mantenimiento del hardware

Si AWS detecta un problema irreparable con el hardware durante el proceso de aprovisionamiento del servidor o mientras aloja las instancias de Amazon EC2 que se ejecutan en su servidor rack de , notificaremos al propietario de las instancias de que está previsto retirar las instancias afectadas.

Para obtener más información, consulte Retirada de instancia en la Guía del usuario de Amazon EC2.

AWS finaliza las instancias afectadas en la fecha de retirada de la instancia. Los datos de los volúmenes del almacén de instancias no persisten después de la finalización de la instancia. Por tanto, es importante que lo haga antes de la fecha de retirada de la instancia. En primer lugar, transfiera los datos a largo plazo de los volúmenes del almacén de instancias de cada instancia afectada a un almacenamiento persistente, como un bucket de Amazon S3 o un dispositivo de almacenamiento en red de su red.

Se suministrará un servidor de reemplazo al sitio del Outpost. A continuación, proceda del modo siguiente:

- Extraiga los cables de red y alimentación del servidor irreparable y, si es necesario, extráigalo del bastidor.
- Instale el servidor de reemplazo en la misma ubicación. Siga las instrucciones de instalación que se indican en Instalación del servidor de Outposts.
- Empaque el servidor irreparable AWS en el mismo paquete en el que llegó el servidor de reemplazo.
- Utilice la etiqueta de devolución prepagada que está disponible en la consola anexa a los detalles de configuración del pedido o al pedido del servidor de reemplazo.
- Devuelva el servidor a. AWS Para obtener más información, consulte Return an AWS Outposts server.

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.

Mejores prácticas para eventos de alimentación y red de

Como se indica en los Términos de AWS servicio para AWS Outposts los clientes, la instalación donde se encuentra el equipo de Outposts debe cumplir con los requisitos mínimos de energía y red para respaldar la instalación, el mantenimiento y el uso del equipo de Outposts. Un en 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 de energía totales, existe el riesgo inherente de que un AWS Outposts recurso no vuelva a funcionar automáticamente. Además de desplegar soluciones de alimentación redundante y de respaldo, le recomendamos que haga lo siguiente con antelación para mitigar el impacto de algunos de los peores escenarios posibles:

- Retire sus servicios y aplicaciones de los equipos de Outposts de forma controlada mediante cambios en el equilibrador de carga basados en DNS o fuera del bastidor.
- Detenga los contenedores, las instancias y las bases de datos de forma ordenada e incremental, y utilice el orden inverso al restaurarlos.
- Pruebe los planes para el traslado o la detención controlados de los servicios.
- Realice copias de seguridad de los datos y configuraciones de relevancia y guárdelos fuera de los Outposts.
- Mantenga los tiempos de inactividad del suministro de alimentación al mínimo.
- Evite cambiar repetidamente las fuentes de alimentación (off-on-off-on) durante el mantenimiento.
- Prevea tiempo adicional dentro del período de mantenimiento para hacer frente a cualquier imprevisto.
- Gestione las expectativas de sus usuarios y clientes comunicando un plazo de mantenimiento más amplio del que normalmente necesitaría.
- Cuando se restablezca la alimentación, cree una caja en el AWS Support Centro para solicitar la verificación de que los servicios relacionados AWS Outposts y los servicios relacionados están funcionando.

Eventos de conectividad de red

La conexión de enlace de servicio entre tu Outpost y la AWS región o región de origen de Outposts normalmente se recuperará automáticamente de las interrupciones o problemas de la red que puedan producirse en los dispositivos de la red corporativa principal o en la red de cualquier proveedor de conectividad externo una vez que se complete el mantenimiento de la red. Durante el tiempo en que la conexión del enlace de servicio esté inactiva, sus operaciones de Outposts se limitarán a las actividades de la red local.

Las instancias de Amazon EC2, las redes de LNI y los volúmenes de almacenamiento de instancias en el servidor de Outposts seguirán funcionando con normalidad y se podrá acceder a ellos de forma local a través de la red local y la LNI. Del mismo modo, los recursos de AWS servicio, como los

nodos de trabajo de Amazon ECS, siguen ejecutándose localmente. Sin embargo, la disponibilidad de la API disminuirá. Por ejemplo, es posible que las funciones ejecutar, iniciar, detener y terminar no APIs funcionen. Las métricas y los registros de las instancias seguirán almacenándose en caché local durante un máximo de 7 días y se transferirán a la AWS región cuando se restablezca la conectividad. Si se desconecta durante más de 7 días, es posible que se pierdan las métricas y los registros.

Si el enlace de servicio no funciona debido a un problema de energía in situ o a una pérdida de conectividad de red, Panel de estado envía una notificación a la cuenta propietaria de los Outposts. Ni tú ni tú AWS podéis suprimir la notificación de una interrupción del enlace de servicio, incluso si la interrupción es esperada. Para obtener más información, consulte Introducción a su Panel de estado 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 tiene el control del mantenimiento de la red, limite la duración del tiempo de inactividad del enlace de servicio. Incluya un paso en el proceso de mantenimiento que verifique que la red se haya recuperado.
- Si no tiene el control del mantenimiento de la red, supervise el tiempo de inactividad del enlace de servicio con respecto al período de mantenimiento anunciado e infórmele cuanto antes a la parte encargada del mantenimiento planificado de la red si el enlace de servicio no vuelve a funcionar al final del período de mantenimiento anunciado.

Recursos

A continuación, se detallan algunos recursos relacionados con la supervisión que pueden garantizar que los Outposts estén funcionando normalmente después de un evento de alimentación o red planificado o no planificado:

- El AWS blog Monitoring best practices for AWS Outposts cubre las mejores prácticas de observabilidad y gestión de eventos específicas de Outposts.
- En el AWS blog Herramienta de depuración para conectividad de red de Amazon VPC se explica AWSSupport-SetupIPMonitoringFromVPCla herramienta. Esta herramienta es un 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 el monitoreo de Outposts, la instancia de monitoreo debe estar en una subred de la AWS región principal y estar configurada para monitorear una o más de tus instancias de Outpost utilizando sus IP privadas; esto proporcionará gráficos de pérdida de paquetes y latencia entre AWS Outposts la región principal y la región principal. AWS

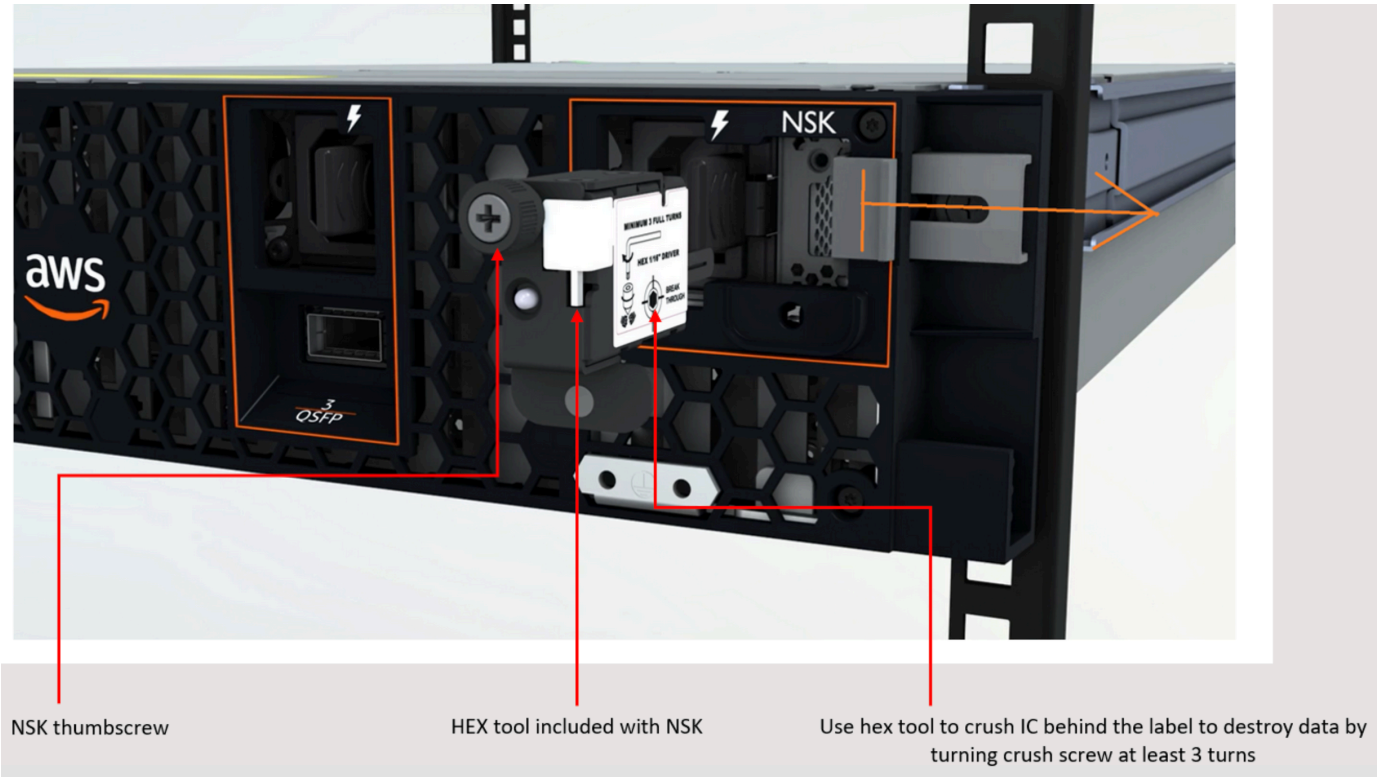
- El AWS blog Cómo implementar un CloudWatch panel automatizado de Amazon para su AWS Outposts uso AWS CDK describe los pasos necesarios para implementar un panel automatizado.
- Si tiene preguntas o necesita más información, consulte Creating a support case en la Guía del usuario de AWS Support.

Destrucción criptográfica de los datos del servidor

La clave de seguridad Nitro (NSK) es necesaria para descifrar los datos del servidor. Cuando devuelvas el servidor a AWS, ya sea porque estás sustituyendo el servidor o interrumpiendo el servicio, puedes destruir el NSK para destruir criptográficamente los datos del servidor.

Cómo destruir criptográficamente los datos del servidor

1. Extraiga el NSK del servidor antes de volver a enviarlo. AWS
2. Asegúrese de que tiene el NSK que fue suministrado con el servidor.
3. Quite la pequeña herramienta hexagonal o llave Allen de debajo de la pegatina.
4. Use la herramienta hexagonal para girar tres veces el tornillo de mariposa que está debajo de la pegatina. Esta acción destruye el NSK y destruye criptográficamente todos los datos del servidor.


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

Opciones del servidor Outposts end-of-term

Al final de su AWS Outposts mandato, debe elegir entre las siguientes opciones:

- Renovar la suscripción y conservar sus servidores de Outposts actuales.
- Devuelve tus servidores de Outposts.
- Conviértelo en una month-to-month suscripción y conserva tus servidores Outposts existentes.

Renovar la suscripción

Debes completar los siguientes pasos al menos 5 días hábiles antes de que finalice la suscripción actual de tus servidores de Outposts. Si no completa estos pasos al menos 5 días hábiles antes de que finalice la suscripción actual, es posible que se le cobren cargos imprevistos.

Para renovar su suscripción y conservar sus servidores de Outposts actuales:

1. Abre la AWS Outposts consola en. https://console.aws.amazon.com/outposts/
2. En el panel de navegación, elija Outposts.
3. Elija Acciones.
4. Elige Renovar Outpost.
5. Elija la duración del plazo de suscripción y la opción de pago.

   Para ver los precios, consulte los precios de servidores de AWS Outposts. También puede solicitar una cotización.
6. Selecciona Enviar solicitud de soporte.

> **Note**
>
> Si la renuevas antes de que finalice la suscripción actual para tus servidores de Outposts, se te cobrará inmediatamente cualquier tarifa por adelantado.

La nueva suscripción comenzará el día siguiente a la finalización de la suscripción actual.

Si no indicas que deseas renovar tu suscripción o devolver tu servidor de Outposts, pasarás a ser una month-to-month suscripción automáticamente. Tu Outpost se renovará mensualmente al precio

de la opción de pago sin pago por adelantado que corresponda a tu configuración. AWS Outposts Su nueva suscripción mensual comenzará el día siguiente a la finalización de la suscripción actual.

Devuelva los servidores Outposts

Para devolver un servidor porque el servidor ha llegado al final del plazo del contrato, primero debes completar el proceso de desmantelamiento al menos 5 días hábiles antes de que finalice la suscripción actual de tus servidores de Outposts. AWS no puedes iniciar el proceso de devolución hasta que lo hagas. Si no se completa el proceso de desmantelamiento al menos 5 días hábiles antes de que finalice la suscripción actual, es posible que se produzcan retrasos en el desmantelamiento y cargos imprevistos.

Tras completar el proceso de desmantelamiento, debe preparar el servidor para la devolución, obtener la etiqueta de envío y embalar y devolver el servidor a dónde. AWS

No se te cobrará una tarifa de envío cuando devuelvas un servidor de Outposts. Sin embargo, si devuelves un servidor dañado, podrías incurrir en un coste.

Tareas

- Paso 1: Prepare el servidor para la devolución
- Paso 2: Retirar el servidor
- Paso 3: Obtenga la etiqueta de envío de devolución
- Paso 4: Empaca el servidor
- Paso 5: Devuelva el servidor a través del servicio de mensajería

Paso 1: Prepare el servidor para la devolución

Para preparar el servidor para la devolución, deje de compartir los recursos, haga copias de seguridad de los datos, elimine las interfaces de red locales y finalice las instancias activas.

1. Si los recursos del Outpost se comparten, debe dejar de compartirlos.

   Puede dejar de compartir un recurso de Outpost compartido de una de las siguientes formas:

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

Para ver la lista de recursos de Outpost que se pueden compartir, consulte Recursos de Outpost que se pueden compartir.

2. Cree copias de seguridad de los datos almacenados en el almacenamiento de instancias de las EC2 instancias de Amazon que se ejecutan en el AWS Outposts servidor.
3. Elimine las interfaces de red locales asociadas a las instancias que se estaban ejecutando en el servidor.
4. Finalice las instancias activas asociadas a las subredes de su Outpost. Para finalizar las instancias, sigue las instrucciones de Termina tu instancia en la Guía del EC2 usuario de Amazon.
5. Destruye la clave de seguridad Nitro (NSK) para destruir criptográficamente los datos del servidor. Para destruir la NSK, siga las instrucciones de la sección Destruya criptográficamente los datos del servidor.

Paso 2: Retirar el servidor

Completa los siguientes pasos al menos 5 días hábiles antes de que finalice la suscripción actual para tus servidores de Outposts.

> **Important**
>
> AWS no puedes detener el proceso de devolución después de haber presentado tu solicitud de retirada del servicio.

1. Abre la AWS Outposts consola en. https://console.aws.amazon.com/outposts/
2. En el panel de navegación, elija Outposts.
3. Elija Acciones.
4. Selecciona Decomisionar Outpost y sigue el flujo de trabajo para eliminar los recursos.
5. Elija Submit request (Enviar solicitud).

> **Note**
>
> La devolución de tus servidores de Outpost antes de que finalice la suscripción actual no cancelará ningún cargo pendiente asociado a este Outpost.

Paso 3: Obtenga la etiqueta de envío de devolución

> **Important**
>
> Solo debes usar la etiqueta de envío que se AWS proporciona, ya que contiene información específica, como el identificador del producto, sobre el servidor al que vas a devolver. No cree su propia etiqueta de envío.

Para obtener tu etiqueta de envío:

1. Abre la AWS Outposts consola en https://console.aws.amazon.com/outposts/.
2. En el panel de navegación, elija Pedidos.
3. Elige el orden del servidor que quieres devolver.
4. En la página de detalles del pedido, en la sección Estado del pedido, selecciona Imprimir etiqueta de devolución.

> **Note**
>
> La devolución de tus servidores de Outpost antes de que finalice la suscripción actual no cancelará ningún cargo pendiente asociado a este Outpost.

Paso 4: Empaca el servidor

Para embalar el servidor, utilice la caja y el material de embalaje proporcionados por AWS.

1. Empaquete el servidor en una de las siguientes cajas:
   - La caja y el material de empaquetado en la que el servidor se entregó originalmente.

- La caja y el material de empaquetado en la que el servidor de sustitución se entregó originalmente.

También puede ponerse en contacto con el AWS Support Center para solicitar una caja.

2. Coloca la etiqueta de envío AWS incluida en la parte exterior de la caja.

> **Important**
>
> Compruebe que el ID de artículo de la etiqueta de envío coincide con el ID de artículo del servidor que va a devolver.
> El ID de artículo se encuentra en la pestaña extraíble de la parte frontal del servidor.
> Ejemplo: `1203779889` o `9305589922`

3. Selle bien la caja.

Paso 5: Devuelva el servidor a través del servicio de mensajería

Debe devolver el servidor a través del servicio de mensajería designado para su país. Puede entregar el servidor al mensajero o programar el día y la hora que prefiera para que el mensajero recoja el servidor. La etiqueta de envío que se AWS proporciona contiene la dirección correcta para devolver el servidor.

La siguiente tabla muestra con quién debe ponerse en contacto en el país desde el que realiza el envío:

País	Contacto
Argentina	Ponerse en contacto con el AWS Support Center. En la solicitud, incluya la siguiente información: • El número de seguimiento que figura en la etiqueta AWS de envío proporcionada • La fecha y la hora en las que prefiere que el mensajero recoja el servidor • Un nombre de contacto
Bahréin	
Brasil	
Brunéi	
Canadá	
Chile	

País	Contacto
Colombia	• Un número de teléfono • Una dirección de correo electrónico
Hong Kong	
India	
Indonesia	
Japón	
Malasia	
Nigeria	
Omán	
Panamá	
Perú	
Filipinas	
Serbia	
Singapur	
Sudáfrica	
Corea del Sur	
Taiwán	
Tailandia	
Emiratos Árabes Unidos	
Vietnam	

País	Contacto
Estados Unidos de América	Ponerse en contacto con UPS. Puede devolver el servidor mediante alguna de las siguientes formas: • Devolver el servidor durante una recogida rutinaria de UPS en sus instalaciones. • Dejar el servidor en una sucursal de UPS. • Programar una recogida para la fecha y hora que prefiera. Introduzca el número de seguimiento de la etiqueta de envío proporcionada por AWS para obtener un envío gratuito.
Todos los otros países	Ponerse en contacto con DHL. Puede devolver el servidor mediante alguna de las siguientes formas: • Dejar el servidor en una sucursal de DHL. • Programar una recogida para la fecha y hora que prefiera. Introduce el número de guía de DHL que figura en la etiqueta de envío AWS proporcionada para obtener un envío gratuito. Si aparece el siguiente `Courier pickup can't be scheduled for an import shipment` error, suele significar que el país de recuperación que ha seleccionado no coincide con el país de recuperación que aparece en la etiqueta de devolución. Seleccione el país desde el que se origina el envío e inténtelo de nuevo.

Conviértelo en una suscripción month-to-month

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

Tu Outpost se renovará mensualmente al precio de la opción de pago sin pago por adelantado que corresponda a tu configuración. AWS Outposts Su nueva suscripción mensual comenzará el día siguiente a la finalización de la suscripción actual.

Cuotas para AWS Outposts

Cuenta de AWS Tiene cuotas predeterminadas, anteriormente denominadas límites, para cada uno de ellos Servicio de AWS. A menos que se indique lo contrario, cada cuota es específica de la región. Puede solicitar el aumento de algunas cuotas, pero no de todas.

Para ver las cuotas AWS Outposts, abra la consola Service Quotas. En el panel de navegación, elija Servicios de AWS y seleccione AWS Outposts.

Para solicitar un aumento de cuota, consulte Solicitud de un aumento de cuota en la Guía de usuario de Service Quotas.

Cuenta de AWS Tiene las siguientes cuotas relacionadas con AWS Outposts.

Recurso	Predeterminado	Ajustable	Comentarios
Sitios de Outpost	100	Sí	Un sitio de Outpost es el edificio físico administrado por el cliente donde se alimenta y se conecta el equipo de Outpost a la red. Puedes tener 100 sitios de Outposts en cada región de tu AWS cuenta.
Outposts por sitio	10	Sí	AWS Outposts incluye recursos virtuales y de hardware, conocidos como Outposts. Esta cuota limita los recursos virtuales de Outpost. Puede tener 10 Outposts en cada sitio de Outpost.

AWS Outposts y las cuotas de otros servicios

AWS Outposts depende de los recursos de otros servicios y esos servicios pueden tener sus propias cuotas predeterminadas. Por ejemplo, su cuota para las interfaces de red locales proviene de la cuota de Amazon VPC para las interfaces de red.

Historial de documentos de bastidores de Outposts

En la tabla siguiente se describen las actualizaciones realizadas en la documentación de los bastidores de Outposts.

Cambio	Descripción	Fecha
AWS Outposts admite volúmenes de bloques externos de cabinas de almacenamiento Dell y HPE	Puede utilizar volúmenes de arranque y datos en bloque externos respaldados por proveedores externos, como Dell PowerStore y HPE Alletra Storage MP B10000.	30 de septiembre de 2025
Renovar la suscripción y preparar los servidores para la devolución	Para renovar una suscripción o devolver un servidor, debe completar el proceso al menos 10 días hábiles antes de que finalice la suscripción actual.	16 de julio de 2025
Solución de problemas de la conexión del enlace de servicio	Si la conexión entre tu servidor de Outposts y tu AWS región no funciona, sigue estos pasos para solucionar el problema.	5 de mayo de 2025
Actualizaciones de la estabilidad estática	En caso de que se interrumpa la red, las métricas y los registros de las instancias se almacenarán en caché local durante un máximo de 7 días. Anteriormente, Outposts podía almacenar en caché los registros solo durante unas horas.	1 de mayo de 2025

Administración de la capacidad a nivel de activos	Puede modificar la configuración de la capacidad a nivel de activo.	31 de marzo de 2025
Volúmenes de bloques externos respaldados por almacenamiento de terceros	Ahora puede adjuntar volúmenes de datos en bloque respaldados por sistemas de almacenamiento en bloque de terceros compatibles durante el proceso de lanzamiento de la instancia en Outpost.	1 de diciembre de 2024
Administración de la capacidad	Puede modificar la configuración de capacidad predeterminada para su nuevo pedido de Outposts.	16 de abril de 2024
End-of-term opciones para servidores AWS Outposts	Al final del AWS Outposts periodo, puedes renovar, finalizar o convertir tu suscripción.	1 de agosto de 2023
Creé una guía AWS Outposts de usuario para los servidores de Outposts	AWS Outposts La guía del usuario se dividió en guías separadas para racks y servidores.	14 de septiembre de 2022
Grupos de colocación 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
Presentación de los servidores de Outposts	Se agregaron los servidores Outposts, un nuevo AWS Outposts formato.	30 de noviembre de 2021

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.