Guía del usuario para servidores

AWS Outposts

AWS Outposts: Guía del usuario para servidores

Table of Contents

¿Qué es AWS Outposts?

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

Un Outpost es un conjunto de capacidades AWS informáticas y de almacenamiento desplegadas en las instalaciones de un cliente. AWS opera, supervisa y administra esta capacidad como parte de una AWS región. Puede crear subredes en su Outpost y especificarlas al crear AWS recursos, como instancias 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 en los que se AWS instalará tu Outpost. Un sitio debe cumplir con los requisitos de instalaciones, redes y alimentación de su Outpost.
- Capacidad del Outpost: recursos informáticos y de almacenamiento disponibles en el Outpost. Puede ver y administrar la capacidad de su Outpost desde la consola de AWS Outposts .
- Equipo de Outpost: hardware físico que proporciona acceso al servicio. AWS Outposts El hardware incluye racks, servidores, conmutadores y cableado propiedad de y gestionados por. AWS
- Bastidores de Outposts: un factor de forma de Outpost que constituye un bastidor de 42U estándar del sector. Los bastidores del Outpost incluyen servidores que se pueden montar en bastidores, conmutadores, un panel de conexiones de red, un estante de suministro eléctrico y paneles vacíos.

- Debe instalar un rack ACE si tiene cinco o más racks de cómputo. Si tiene menos de cinco racks de cómputo pero planea ampliarlos a cinco o más en el futuro, le recomendamos que instale un rack ACE lo antes posible.

  Para obtener información adicional sobre los racks ACE, consulte Escalar las implementaciones de AWS Outposts racks con racks ACE.
- Servidores para Outposts: un factor de forma del Outpost que constituye un servidor de 1U o 2U con protocolo estándar del sector, y se puede instalar en un bastidor de 4 postes estándar conforme con la norma EIA-310D 19. Los servidores de Outpost proporcionan servicios de cómputo y red locales a sitios que tienen requisitos de espacio limitado o capacidad más reducida.
- Enlace de servicio: ruta de red que permite la comunicación entre su puesto de avanzada y la región asociada. AWS Cada Outpost es una extensión de una zona de disponibilidad y su región asociada.
- Puerta de enlace local (LGW): enrutador virtual de interconexión lógica que permite la comunicación entre un rack de Outpost y la red local.
- Interfaz de red local: interfaz de red que permite la comunicación entre un servidor del Outpost y la red en las instalaciones.

AWS recursos en Outposts

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

Cálculo

Tipo de recurso	Bastidores	Servidores
Instancias de Amazon EC2	S	Sí
Clústeres de Amazon ECS	S	Sí

Tipo de recurso	Bastidores	Servidores
Nodos de Amazon EKS	S	No

Base de datos y análisis

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

Red

Tipo de recurso	Bastidores	Servidores
Proxy App Mesh Envoy	S	Sí
Equilibrador de carga de aplicación	S	No

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

Almacenamiento

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

Otros Servicios de AWS

Servicio	Bastidores	Servidores
AWS IoT Greengrass	 S	 Sí
Amazon SageMaker Edge Manager	 S	 Sí

Precios

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

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

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

Cómo 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 en las instalaciones debe proporcionar acceso a la red de área extendida (WAN) de vuelta a la región y a Internet. También debe proporcionar acceso LAN o WAN a la red en las instalaciones en la que residen las cargas de trabajo o aplicaciones en las instalaciones.

El siguiente diagrama ilustra ambos factores de forma de Outpost.

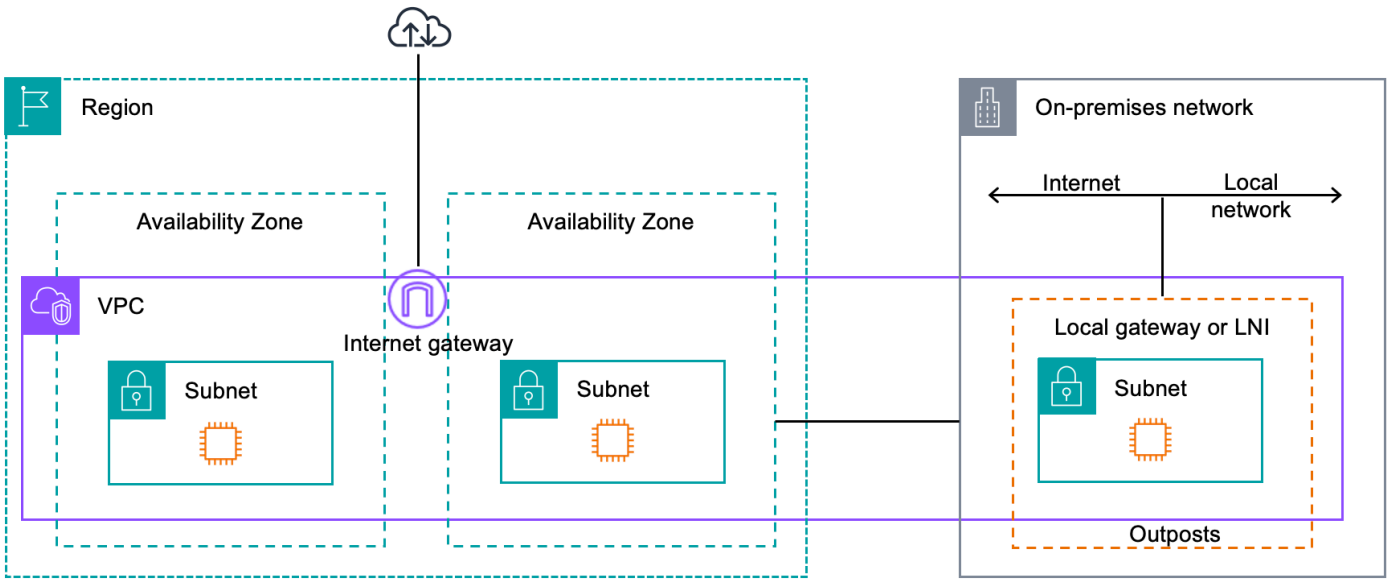
Contenido

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 se proporciona mediante una puerta de enlace local (bastidores) o una interfaz de red local (servidores)



VPC 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. Puede especificar la subred de la instancia EC2 al lanzar la instancia EC2 en el Outpost. No puede especificar el hardware subyacente en el que se implementa la instancia, ya que el Outpost es un conjunto de capacidades AWS informáticas y de almacenamiento.

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

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

Enrutamiento

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

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

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

- Rango CIDR de VPC: 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 VPC en el mismo Outpost, el tráfico entre las VPC permanece en el Outpost y no utiliza el enlace de servicio para volver a la región.

DNS

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

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

Outpost con puerta de enlace local. Como los conjuntos de opciones de DHCP tienen un ámbito de VPC, las instancias de las subredes de Outpost y de las subredes de la zona de disponibilidad de la VPC intentarán usar los servidores DNS especificados para la resolución de nombres DNS.

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

Enlace de servicio

El enlace de servicio es una conexión desde 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:

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

Interfaces de red local

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

Un sitio de Outpost es la ubicación física donde opera el Outpost. Los sitios solo están disponibles en países y territorios seleccionados. Para obtener más información, consulte Preguntas frecuentes sobre servidores de AWS Outposts. 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 del bastidor de Outposts, consulte los requisitos del sitio para el bastidor de Outposts en la Guía del usuario de AWS Outposts para bastidores de Outposts.

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 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.

  > **Important**
  >
  > 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).
  - Los servidores Outposts 2U requieren espacio con las siguientes dimensiones: 3,5 pulgadas de alto (88,9 mm), 17,5 pulgadas de ancho (447 mm), 30 pulgadas de profundidad (762 mm)
  - Los servidores Outposts 1U requieren espacio con las siguientes dimensiones: 1,75 pulgadas de alto (44,45 mm), 17,5 pulgadas de ancho (447 mm), 24 pulgadas de profundidad (610 mm)

  > **Note**
  >
  > - No se admite el montaje vertical de AWS Outposts los servidores.
  > - Los servidores Outposts 1U tienen el mismo ancho que los servidores Outposts 2U, pero tienen la mitad de altura y menos profundidad.

  AWS proporciona un kit de rieles para montar el servidor en rack. Para obtener más información, consulte Paso 3: montar un bastidor.

  Si no coloca el servidor en un bastidor, deberá seguir cumpliendo los demás requisitos enumerados en esta sección.
- 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 Outposts incluye 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. Para obtener más información, consulte Configurar la red QSFP.

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 DNS proporcionado por DHCP
UDP	443, 1024-65535	IP del enlace de servicio	443	Puntos finales de Outposts Service Link

Protocolo	Puerto de origen	Dirección de origen	Puerto de destino	Dirección de destino
TCP	1024 - 65535	IP del enlace de servicio	443	Puntos finales de registro de Outposts

Puedes usar una AWS Direct Connect conexión o una conexión pública a Internet para volver a conectar el puesto de avanzada a la región. AWS Para la conectividad del enlace del servicio Outposts, puedes usar NAT o PAT en tu firewall o router perimetral. 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 finales del enlace de servicio en la región principal. AWS Para obtener más información sobre el enlace de servicio, consulte AWS Outposts conectividad con las AWS regiones.

Recomendaciones de ancho de banda para el enlace de servicio

Para una experiencia y una resiliencia óptimas, se AWS recomienda utilizar una conectividad redundante de al menos 500 Mbps para la conexión del enlace de servicio a la región. AWS La utilización máxima de cada servidor de Outpost es de 500 Mbps. Para aumentar la velocidad de conexión, utilice múltiples servidores de Outpost. 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.

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 las AMI en caché. Las AMI se descargan de la región cada vez que se lanza 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.

El enlace de servicio requiere una respuesta de DHCP

El enlace de servicio requiere una respuesta DHCP IPv4 para configurar los ajustes de red.

Latencia máxima del enlace de servicio

Los enlaces de servicio pueden admitir una latencia de red máxima de 250 ms desde el servidor y su zona de disponibilidad.

Alimentación

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

Requisitos

- Soporte de alimentación
- Consumo de energía
- Cable de alimentación
- Redundancia 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 la India, necesita un cable de alimentación IS1293 a 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 pulgadas/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 Instalación del servidor del Outpost.

La instalación finaliza cuando confirmas que la capacidad de Amazon EC2 para tu servidor de Outposts está disponible en tu cuenta. AWS

Comience con AWS Outposts

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

Tareas

- Crear un Outpost y solicitar capacidad de Outpost
- Instalación del servidor del Outpost
- Lanza una instancia en tu servidor Outpost

Crear un Outpost y solicitar capacidad de Outpost

Para empezar a usarlo AWS Outposts, inicia sesión con la AWS cuenta que será propietaria del Outpost. 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 .
- Debe tener un plan AWS Enterprise Support o un plan AWS Enterprise On-Ramp Support.
- Determine quién Cuenta de AWS será el propietario del Outpost. Utilice esta cuenta para crear el sitio de Outposts, crear el Outpost y realizar el pedido. Supervisa el correo electrónico asociado a esta cuenta para obtener información de AWS.

Tareas

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

Paso 1: crear un sitio

Cree un sitio para especificar la dirección operativa. La dirección 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 para AWS usar el Cuenta de AWS propietario del Outpost.
2. Abre la AWS Outposts consola en https://console.aws.amazon.com/outposts/.
3. Para seleccionar la principal Región de AWS, utilice el selector de regiones situado en la esquina superior derecha de la página.
4. En el panel de navegación, seleccione Sitios.
5. Seleccione Crear sitio.
6. En Tipo de hardware compatible, seleccione Solo servidores.
7. Introduzca el nombre, la descripción y la dirección operativa del sitio.
8. (Opcional) En el caso de 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.

Paso 3: realizar el pedido

Haz un pedido de los servidores de Outposts que necesites. Después de enviar el pedido, un representante de AWS Outposts se pondrá en contacto con usted.

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

Requisitos previos

- Determine cómo pagará el pedido. Puede pagar en efectivo, con un pago inicial parcial y sin pagar nada de forma inicial. Si elige la opción de pago parcial por adelantado o sin pago por adelantado, pagarás cargos mensuales durante un período de tres años.

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

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

Para modificar la capacidad de las instancias

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

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

Console steps

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

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

Upload JSON file

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

   Example

   Ejemplo de archivo JSON:

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

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

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

Siguientes pasos

Puede ver el estado de su pedido mediante la AWS Outposts consola. El estado inicial de su pedido es Pedido recibido. Un AWS representante se pondrá en contacto contigo en un plazo de tres días laborables. Recibirá una confirmación por correo electrónico cuando el estado del pedido cambie al de Pedido en proceso. Un AWS representante puede ponerse en contacto con usted para obtener cualquier información adicional que sea AWS necesaria.

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

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 the section called “Instalación del servidor del Outpost”.

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 del Outpost. Para obtener más información, consulte the section called “Iniciar una instancia”.

Instalación del servidor del Outpost

Cuando solicita un servidor Outpost, usted es responsable de la instalación, ya sea que lo haga usted mismo o contrate a un tercero. La parte que realiza la instalación requiere permisos específicos para verificar la identidad del nuevo dispositivo. Para obtener más información, consulte Conceder permisos.

Requisito previo

Debe tener un factor de forma para el servidor del Outpost en el sitio. Para obtener más información, consulte Crear un Outpost y solicitar capacidad de Outpost.

> **Note**
>
> Le recomendamos que vea el vídeo de formación sobre la instalación de AWS Outposts servidores antes y durante el proceso de instalación. Para acceder a la formación, debe iniciar sesión o crear una cuenta en Skill Builder de AWS.

Tareas

- Paso 1: conceder permisos
- Paso 2: inspeccionar
- Paso 3: montar un bastidor
- Paso 4: encender
- Paso 5: conectar la red
- Paso 6: autorizar el servidor
- Referencia de comandos de la herramienta de configuración del Outpost

Paso 1: conceder permisos

Para verificar la identidad del nuevo dispositivo, debe tener las credenciales de IAM de Cuenta de AWS que contienen el Outpost. La política de AWSOutpostsAuthorizeServerPolicy concede los permisos necesarios para instalar un servidor del Outpost. Para obtener más información, consulte the section called “Administración de identidades y accesos”.

Consideraciones

- Si utiliza un tercero que no tiene acceso al suyo Cuenta de AWS, debe proporcionar un acceso temporal.
- AWS Outposts admite el uso de credenciales temporales. Puede configurar credenciales temporales que duren hasta 36 horas. Asegúrese de dar al instalador el tiempo suficiente para realizar todos los pasos de la instalación del servidor. Para obtener más información, consulte the section called “Credenciales temporales”.

Paso 2: inspeccionar

Para completar una inspección del equipo de Outposts, debe comprobar si el paquete de envío está dañado, desembalarlo y ubicar la clave de seguridad Nitro (NSK). Tenga en cuenta la siguiente información sobre la inspección del servidor:

- El paquete de envío tiene sensores de choque ubicados sobre los dos lados más grandes de la caja.
- La solapa interior del paquete de envío contiene instrucciones sobre cómo desembalar el servidor y ubicar el NSK.
- El NSK es un módulo de cifrado. Para completar la inspección, localice el NSK. En un paso posterior, debe conectar el NSK al servidor.

Compruebe el paquete de envío

Para inspeccionar el paquete de envío

- Antes de abrir el paquete de envío, observe si ambos sensores de choque y están activados. Si los sensores de choque se han activado, es posible que la unidad se haya dañado. Continúe con la instalación y tome nota de cualquier daño adicional en el servidor o en los accesorios. Si alguna parte del sistema está obviamente dañada o la instalación no se realiza según lo esperado, ponte en contacto con AWS Support para recibir orientación sobre cómo reemplazar tu servidor de Outposts.

Si la barra situada en el centro del sensor está roja, significa que el sensor se ha activado.

Desembalaje del paquete de envío

Desembalaje del paquete de envío

- Abra el paquete y asegúrese de que contiene los siguientes elementos:
  - Server
  - Clave de seguridad Nitro (módulo de cifrado): embalaje marcado con “NSK” en rojo. Consulte el siguiente procedimiento para localizar el NSK en el paquete de envío y obtener más información.
  - Kit de instalación de bastidores (2 rieles interiores, 2 rieles exteriores y tornillos)
  - Folleto de instalación
  - Kit de accesorios
    - Par de cables de alimentación C13/14 - 10 ft (3 m)
    - Cable de conexión QSFP - 10 ft (3 m)

- Cable USB, micro-USB a USB-C - 10 ft (3 m)
- Protector de cepillo

Encuentre el NSK

El NSK está dentro de la caja con la etiqueta A que incluye los accesorios para el servidor.

> **Important**
>
> No utilice el NSK para destruir los datos del servidor durante la instalación.

Se requiere el NSK para activar el servidor. El NSK también se utiliza para destruir los datos del servidor cuando se devuelve el servidor. En este paso de instalación, ignore las instrucciones sobre cuerpo del NSK, ya que esas instrucciones tienen por objeto destruir los datos.

Paso 3: montar un bastidor

Para completar este paso, debe fijar los rieles interiores al servidor y los rieles exteriores al bastidor y, a continuación, montar el servidor en el bastidor. Necesitará un destornillador Phillips para realizar estos pasos.

Alternativas de montaje de bastidores

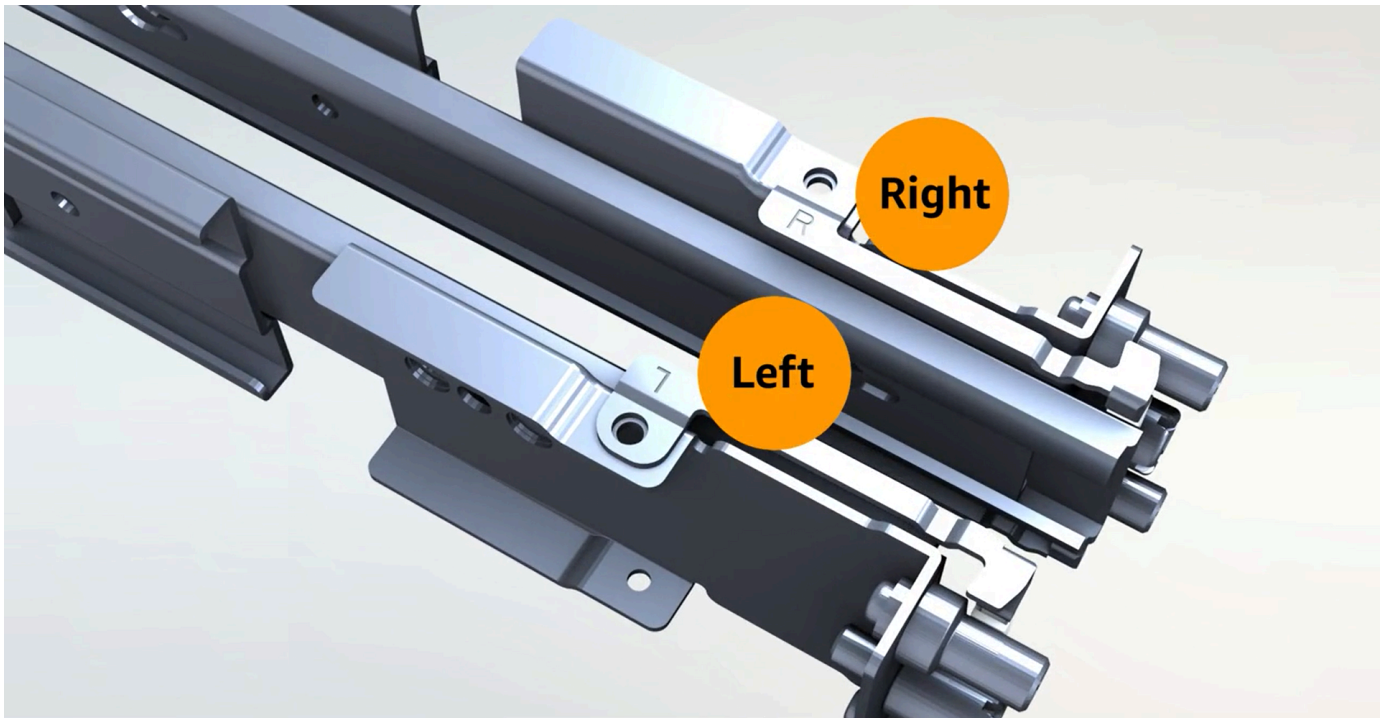
No es necesario montar el servidor en un bastidor. Si no va a montar el servidor en un bastidor, tenga en cuenta la siguiente información:

- Asegúrese de que haya una separación mínima de 6 ft (15 cm) entre el servidor y las paredes situadas delante y detrás del servidor, a fin de permitir que el aire caliente circule.
- Coloque el servidor sobre una superficie estable y libre de riesgos mecánicos, como la humedad o la caída de objetos.
- Para usar los cables de red incluidos con el servidor, debe colocar el servidor a una distancia de 10 pies (3 m) del dispositivo de red ascendente.
- Siga las instrucciones locales para las juntas y los refuerzos sísmicos.

Identificación de los lados y los extremos

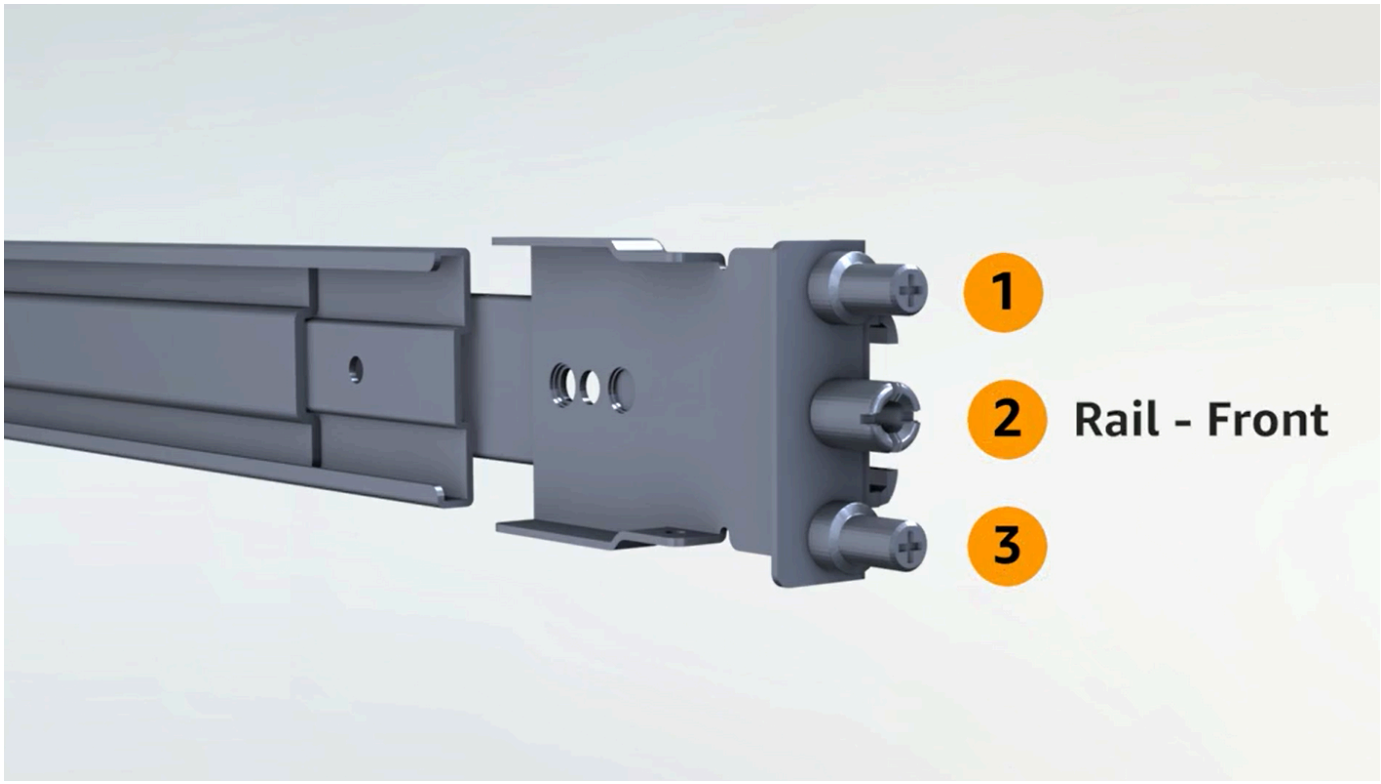
Para identificar la izquierda de la derecha y la parte delantera de la trasera

1. Ubique y abra la caja de rieles para bastidores suministrado junto al servidor.
2. Observe las marcas sobre los rieles para determinar cuál es el lado izquierdo y el derecho. Estas marcas determinan de qué lado del servidor se conecta cada riel.

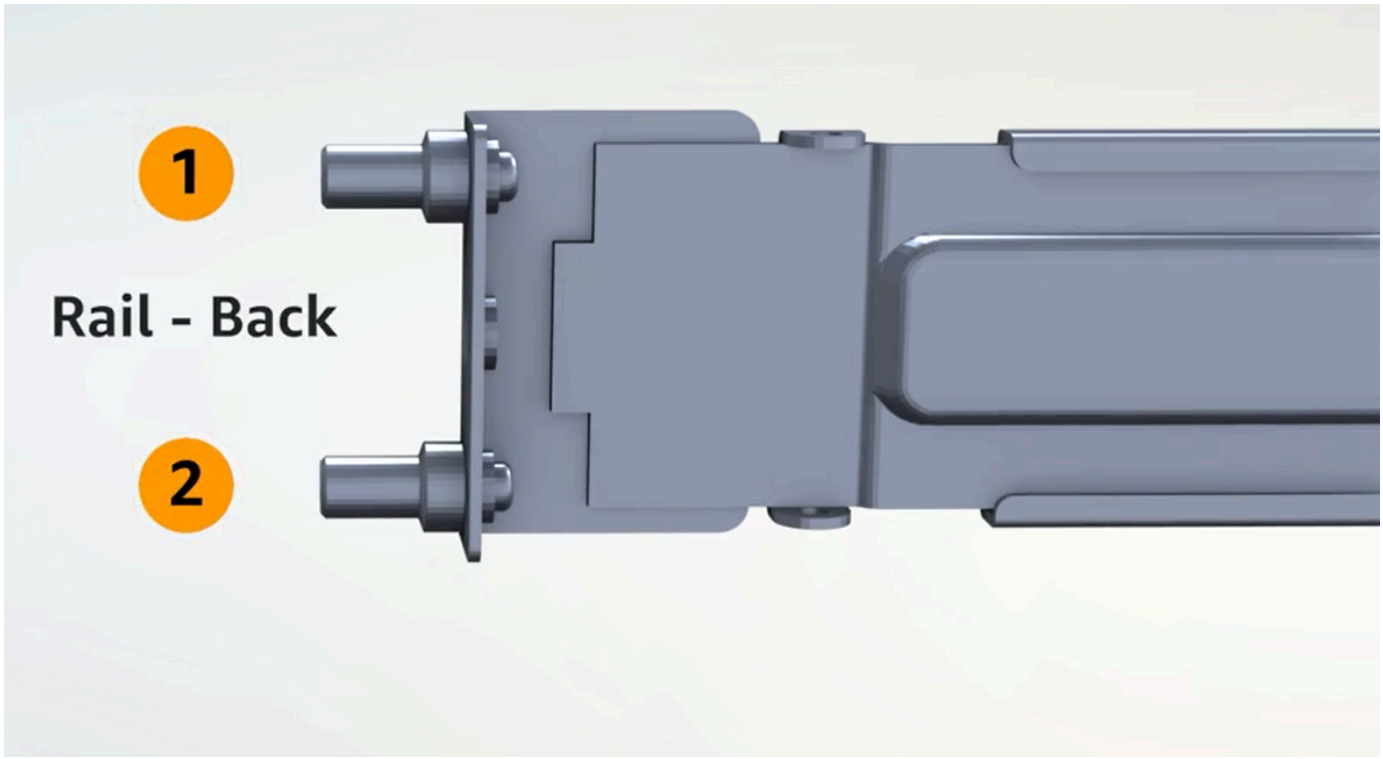


3. Observe los postes de cada extremo de los rieles para determinar cuál está en la parte delantera y cuál en la trasera.

   La parte delantera tiene tres postes.



La parte trasera tiene dos postes.



Fijar los rieles interiores

Para fijar los rieles interiores al servidor

1. Separe el riel interior del riel exterior de ambos rieles. Debe tener cuatro rieles.
2. Fije el riel interior derecho del lado derecho del servidor y asegúrelo con un tornillo. Asegúrese de orientar el riel correctamente con el servidor. Coloque la parte delantera del riel hacia la parte delantera del servidor.
3. Fije el riel interior izquierdo del lado izquierdo del servidor y asegúrelo con un tornillo.

Fijar los rieles exteriores

Para fijar los rieles exteriores al bastidor

1. Coloque el bastidor de frente y utilice el riel marcado con una R en el lado derecho del bastidor. Primero, junte la parte trasera del riel al bastidor y, a continuación, extienda el riel para conectarlo a la parte delantera del bastidor.

   > **Tip**
   >
   > Preste atención a la orientación de los rieles. De ser necesario, utilice los adaptadores de clavijas suministrados.

2. Repita el procedimiento con el riel izquierdo en el lado izquierdo.

Montar el servidor

Para montar el servidor en el bastidor

- Coloque el servidor en los rieles exteriores que instaló en el bastidor en el paso anterior y fíjelo en la parte delantera con los dos tornillos incluidos.

  > **Tip**
  >
  > Dos personas deben colocar el servidor en el bastidor.

Paso 4: encender

Para completar el encendido, conecte el NSK, conecte el servidor a una fuente de alimentación y compruebe que el servidor esté encendido. Tenga en cuenta la siguiente información sobre la alimentación del servidor:

- El servidor funciona con una sola fuente de alimentación, pero se AWS recomienda utilizar dos fuentes de alimentación para garantizar la redundancia.
- Conecte los cables de alimentación antes de conectar los cables de red.
- Utilice el par de cables de alimentación con salida C13 y entrada C14 para conectar el servidor a una fuente de alimentación del bastidor. Si no utiliza el cable de alimentación con entrada C14 para conectar el servidor a una fuente de alimentación del bastidor, debe proporcionar adaptadores para las entradas C14 que se puedan conectar a una fuente de alimentación.

Conexión del NSK

Debe conectar el NSK al servidor para que pueda descifrar los datos del servidor durante su funcionamiento.

Important

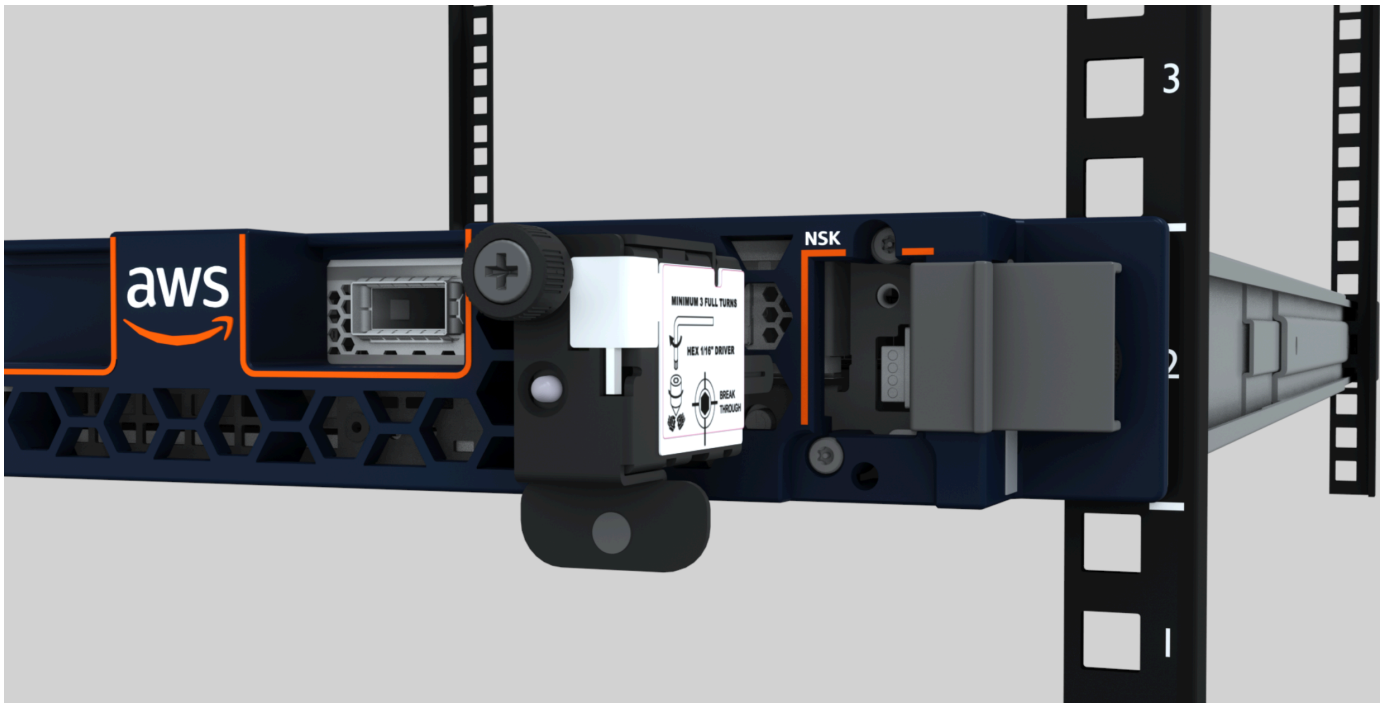
- La sección de NSK contiene instrucciones sobre cómo destruir el NSK. No siga esas instrucciones ahora. Siga esas instrucciones solo cuando devuelva el servidor a AWS, para destruir criptográficamente los datos en el servidor.
- Si va a instalar varios servidores al mismo tiempo, asegúrese de no mezclar los NSK. Debe conectar el NSK al servidor con el que se suministra. Si utiliza un NSK diferente, el servidor no se iniciará.

Para conectar el NSK

1. En la parte frontal derecha del servidor, abra el compartimento NSK.

   En la imagen siguiente, se muestra el NSK conectado a un servidor de 2U.

En la imagen siguiente, se muestra el NSK conectado a un servidor de 1U.

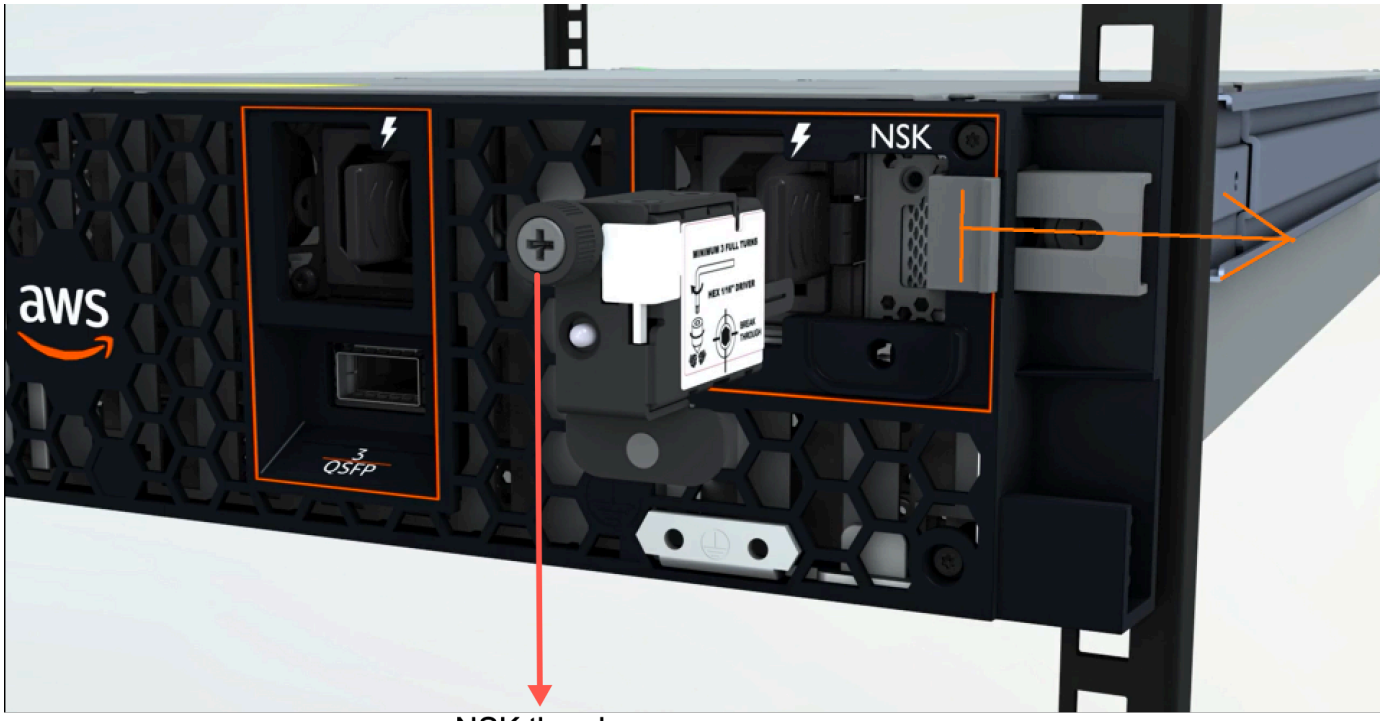


2. Asegúrese de que el número de serie (SN) que figura en el NSK coincida con el SN de la lengüeta extraíble del bisel del compartimento NSK del servidor.

   La siguiente imagen muestra el número SN sobre el NSK y en la lengüeta extraíble del bisel:

3. Inserte el NSK en la ranura.
4. Apriete a mano con el tornillo de mariposa o apriételo con un destornillador (0,7 Nm/0,52 lb-pie) hasta que quede ajustado. No utilice la herramienta eléctrica, ya que podría apretar en exceso y dañar el NSK.

   En la imagen siguiente, se muestra la ubicación del tornillo de mariposa.



NSK thumbscrew

La siguiente imagen muestra el tipo de destornillador que puede utilizar para conectar el NSK al servidor.

Encender

Para conectar el servidor a la fuente de alimentación

1. Localice el par de cables de alimentación C13/C14 que se suministran con el servidor.
2. Conecte el extremo C14 de ambos cables a su fuente de alimentación.
3. Conecte el extremo C13 de ambos cables a los puertos de la parte frontal del servidor.

Compruebe la alimentación del servidor

Para comprobar que el servidor tiene alimentación

1. Compruebe que puede oír el funcionamiento del servidor.

   > **Tip**
   >
   > El nivel de ruido disminuye una vez que el servidor se aprovisiona por sí mismo.

2. Compruebe que las luces LED de alimentación situadas sobre los puertos de alimentación estén encendidas.

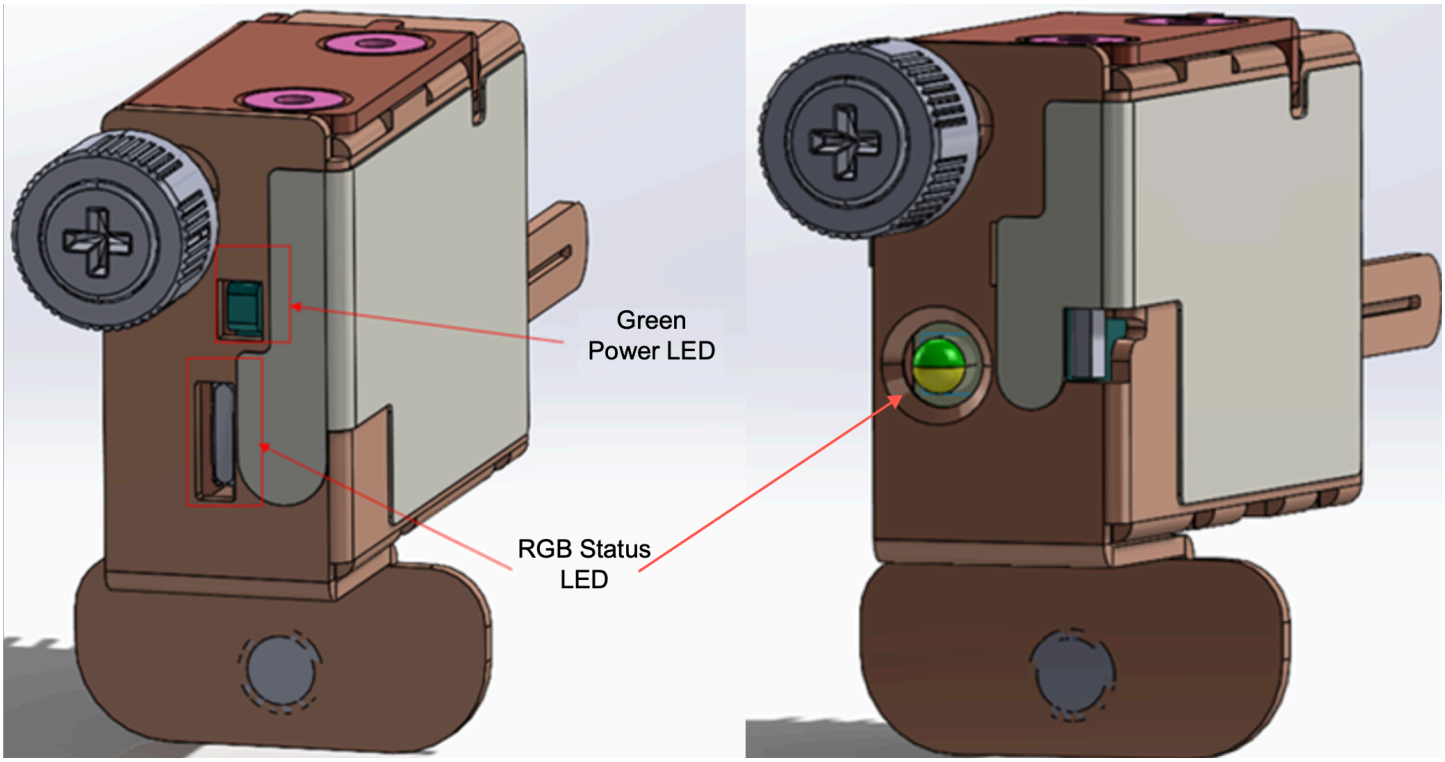
   En la imagen siguiente, se muestran las luces LED de la fuente de alimentación de un servidor de 2U

En la imagen siguiente, se muestran las luces LED de la fuente de alimentación de un servidor de 1U

Compruebe el LED de alimentación del Atlas 3.0. ENSK

AWS Outposts admite dos versiones de NSK: Atlas 2.0 y Atlas 3.0. Ambas versiones de NSK tienen un LED de estado RGB. Además, el Atlas 3.0 tiene un LED de alimentación verde. Este paso es solo para el Atlas 3.0 NSK.

La siguiente imagen muestra la ubicación de los LED en los NSK Atlas 2.0 y Atlas 3.0:



Atlas 3.0 Atlas 2.0

Si tiene el Atlas 2.0 NSK, pase al siguiente paso, Paso 5: conectar la red ya que esta versión del NSK solo tiene el LED de estado RGB, que debe comprobar una vez que se haya aprovisionado y activado el servidor Outpost.

Si tiene el Atlas 3.0 NSK, compruebe el LED de alimentación verde:

- Si la luz verde está encendida, el NSK está correctamente conectado al host y tiene alimentación. Puede continuar con el siguiente paso.
- Si la luz verde está apagada, el NSK no está correctamente conectado al host o no tiene alimentación. Contacto. AWS Support

Paso 5: conectar la red

Para completar la configuración de la red, conecte el servidor al dispositivo de red ascendente con un cable de red.

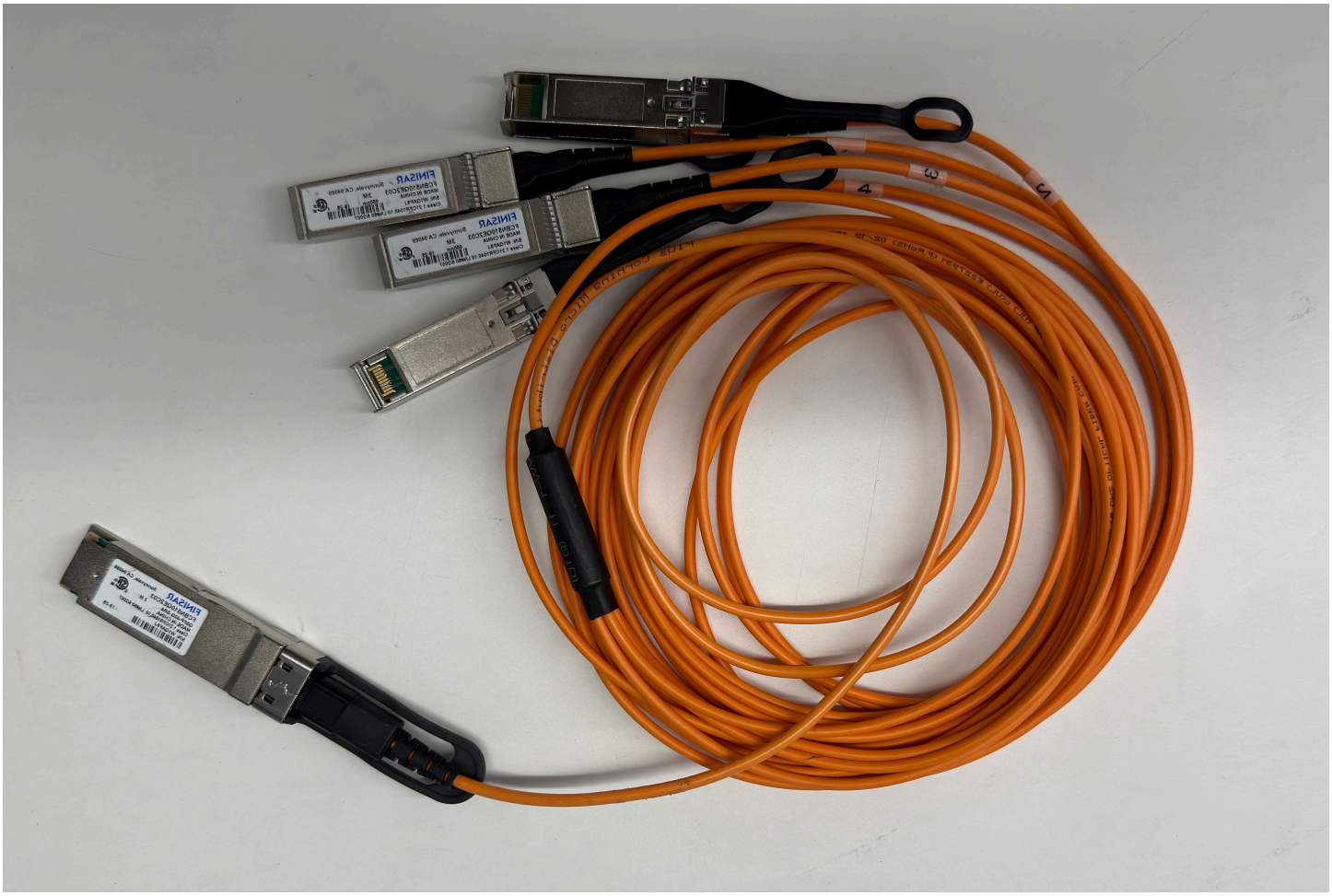
Tenga en cuenta la siguiente información acerca de la conexión a la red:

- El servidor requiere conexiones para dos tipos de tráfico: tráfico de enlace de servicio y tráfico de enlace de interfaz de red local (LNI). En las instrucciones de la siguiente sección se describen los puertos que se deben usar en el servidor para segmentar el tráfico. Consulte a su grupo de TI para determinar qué puerto del dispositivo de red ascendente debe transportar cada tipo de tráfico.
- Asegúrese de que el servidor se haya conectado al dispositivo de red ascendente y de que se le haya asignado una dirección IP. Para obtener más información, consulte Asignación de direcciones IP del servidor.
- La conexión óptica de un AWS Outposts servidor solo admite 10 Gbits y no admite la negociación automática de la velocidad del puerto. Si el puerto del host intenta negociar la velocidad del puerto, por ejemplo, entre 10 Gbits y 25 Gbits, es posible que surjan problemas. En estos casos, recomendamos que haga lo siguiente:
  - Establezca la velocidad del puerto del conmutador en 10 Gbits.
  - Trabaje con su proveedor de conmutadores para admitir una configuración estática.

Configurar la red QSFP

Con el cable de conexión QSFP, puede utilizar las conexiones para segmentar el tráfico.

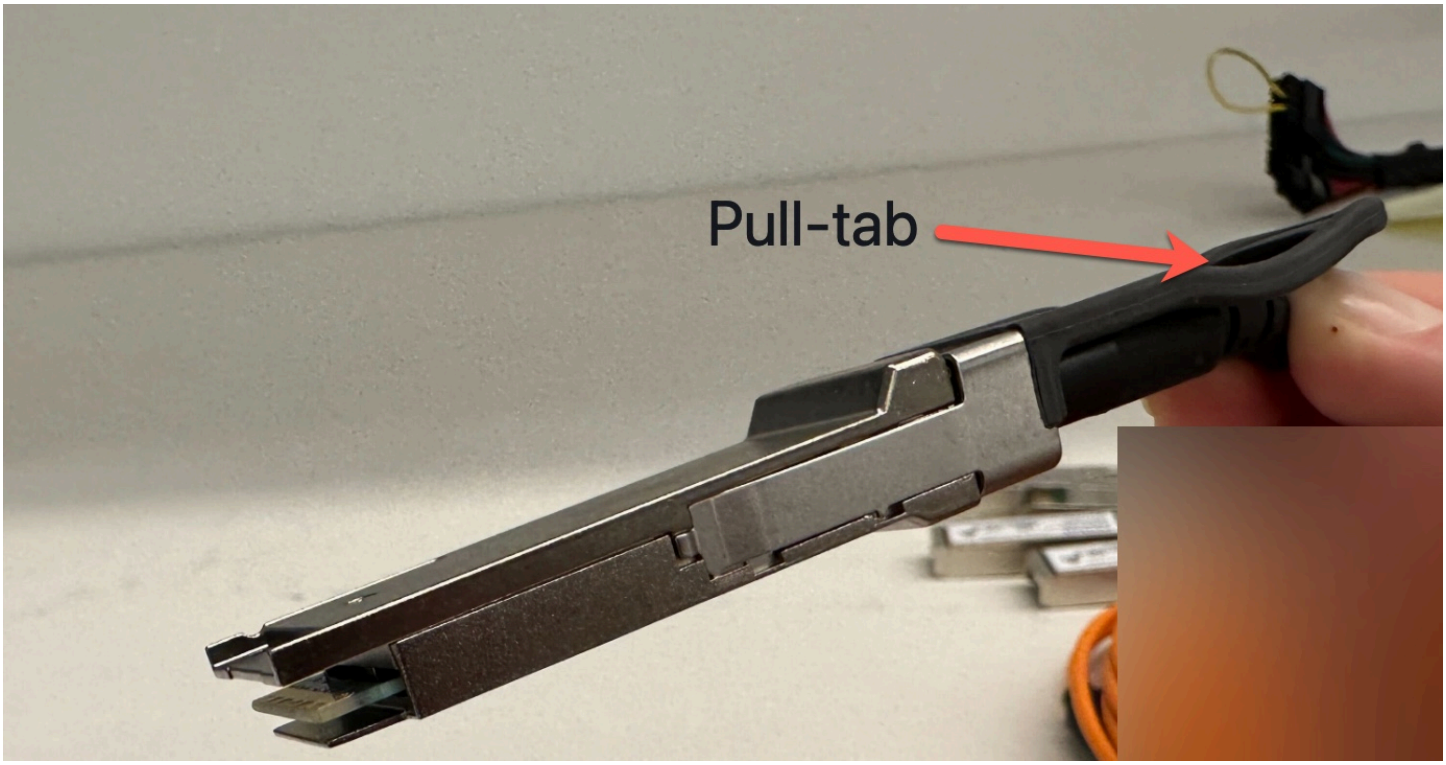
En la imagen siguiente, se muestra el cable de conexión QSFP:



> **Note**
>
> AWS Outposts los servidores tienen un puerto RJ45 físico junto al puerto QSFP. Sin embargo, este puerto RJ45 no está habilitado para el uso de ningún cliente. Si necesita conectividad RJ45 de 1 GbE, utilice el cable QSFP incluido para conectar un conversor multimedia 10GBASE-X SFP+ a un convertidor multimedia RJ45 de 1 GbE.

Un extremo del cable QSFP tiene un único conector. Conecte este extremo al servidor.

En la imagen siguiente, se muestra el extremo del cable con un conector:



El otro extremo del cable QSFP tiene 4 cables de conexión etiquetados del 1 al 4. Utilice el cable con la etiqueta 1 para el tráfico de enlace de LNI y el cable con la etiqueta 2 para el tráfico de enlace de servicio.

La siguiente imagen muestra el extremo del cable con los 4 cables de conexión:

Para conectar el servidor a la red con el cable multiconector QSFP

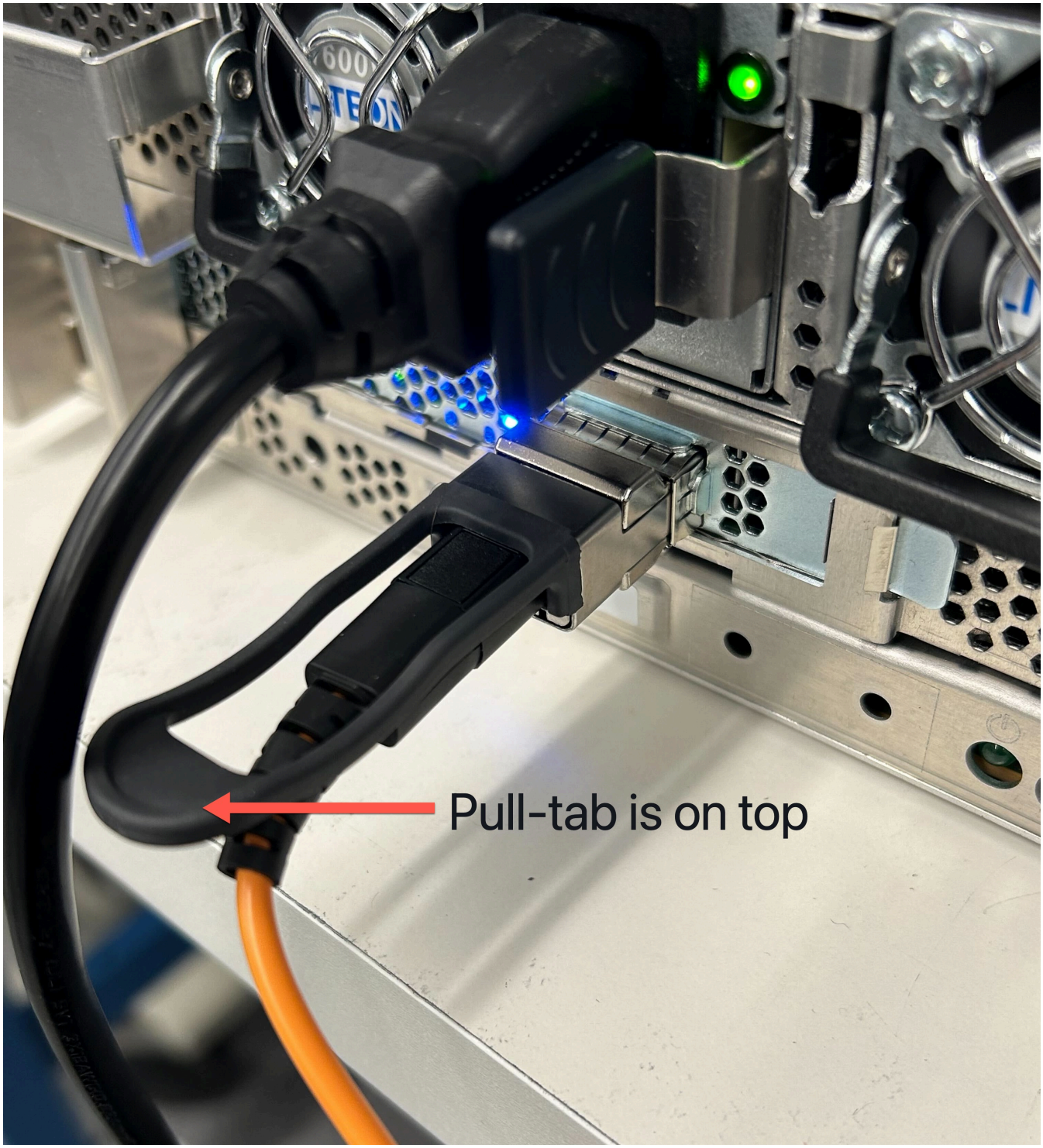
1. Localice el cable breakout QSFP que se suministra con el servidor.
2. Conecte el extremo único del cable breakout QSFP al puerto QSFP del servidor.
    1. Localice el puerto QSFP.

        La siguiente imagen muestra la ubicación del puerto QSFP en el servidor 2U.

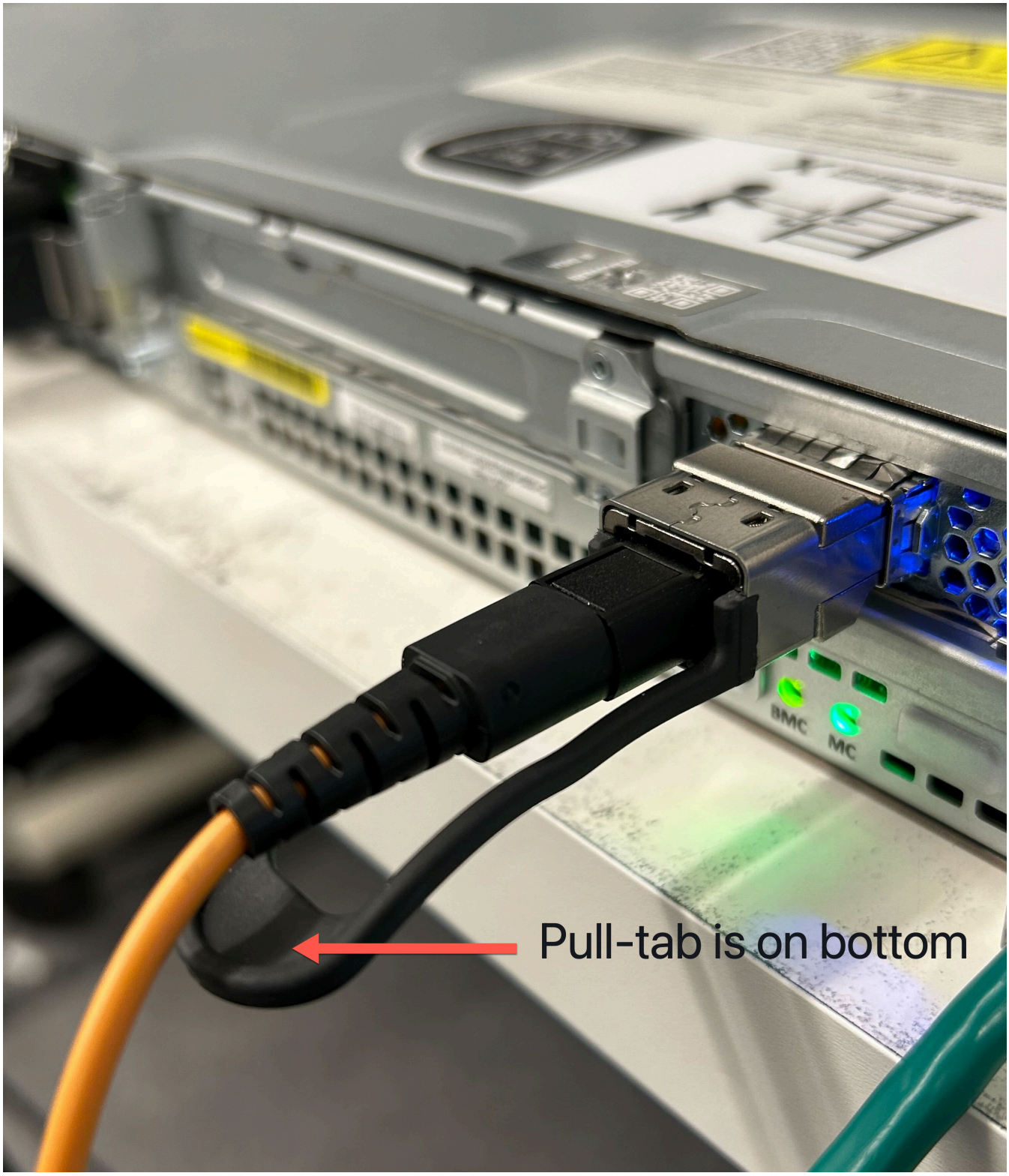
La siguiente imagen muestra la ubicación del puerto QSFP en el servidor 1U.

2. Enchufe el QSFP con la lengüeta extraíble en la orientación correcta.

   Para el servidor de 2U, conecte el QSFP con la lengüeta extraíble en la parte superior, como se muestra en la siguiente imagen.



Para el servidor de 1U, conecte el QSFP con la lengüeta extraíble en la parte inferior, como se muestra en la siguiente imagen.



3. Asegúrese de sentir u oír un clic al conectar los cables. Esto indica que ha enchufado los cables correctamente.

3. Conecte los breakout 1 y 2 del cable QSFP al dispositivo de red ascendente.

> **Important**
>
> Para que un servidor Outpost funcione, es necesario contar con los siguientes cables.
>
> - Utilice el cable con la etiqueta 1 para el tráfico de enlace LNI.
> - Utilice el cable con la etiqueta 2 para el tráfico de enlace de servicio.

Paso 6: autorizar el servidor

Para autorizar el servidor, debe conectar su portátil al servidor con un cable USB y, a continuación, utilizar un protocolo en serie basado en comandos para probar la conexión y autorizar el servidor. Además de las credenciales de IAM, necesita un cable USB, un portátil y un software de terminal serie, como PuTTY o screen, para completar estos pasos.

Como alternativa, si tiene un teléfono o tablet Android con un conector USB-C o micro-USB compatible con USB On The Go (OTG), puede usar la aplicación Activador del servidor de Outposts para guiarle por el proceso de autorización del servidor. Puede descargar la aplicación desde Google Play

Tenga en cuenta la siguiente información que autoriza el servidor:

- Para autorizar el servidor, tú o la parte que lo instale necesitáis las credenciales de IAM Cuenta de AWS que contengan el Outpost. Para obtener más información, consulte the section called “Paso 1: conceder permisos”.
- No necesita autenticarse con las credenciales de IAM para probar la conexión.
- Considere la posibilidad de probar la conexión antes de utilizar el comando de exportación para establecer las credenciales de IAM como variables de entorno.
- Para proteger su cuenta, la herramienta de configuración del Outpost nunca guarda sus credenciales de IAM.
- Para conectar su portátil al servidor, conecte siempre el cable USB al portátil en primer lugar, y luego al servidor.

Tareas

- Conecte su portátil al servidor
- Cree una conexión en serie con el servidor

- Pruebe la conexión
- Autorice el servidor
- Compruebe los LED NSK

Conecte su portátil al servidor

Conecte primero el cable USB al portátil y, después, al servidor. El servidor incluye un chip USB que crea un puerto de serie virtual disponible en el portátil. Puede utilizar este puerto de serie virtual para conectarse al servidor con un software de emulación de terminal serie. Solo puede usar este puerto de serie virtual para ejecutar los comandos de la herramienta de configuración del Outpost.

Para conectar su portátil al servidor

Conecte primero el cable USB al portátil y, después, al servidor.

> **Note**
>
> El chip USB requiere controladores para crear el puerto de serie virtual. Su sistema operativo debería instalar de forma automática los controladores necesarios si aún no están presentes. Para descargar e instalar los controladores, consulte las Guías de instalación de FTDI.

Cree una conexión en serie con el servidor

Esta sección contiene instrucciones para utilizar los programas de terminal serie más populares, pero no es obligatorio que los utilice. Utilice el programa de terminal serie que prefiera con una velocidad de conexión de `115200` baudios.

Ejemplos

- Conexión en serie de Windows
- Conexión de serie Mac

Conexión en serie de Windows

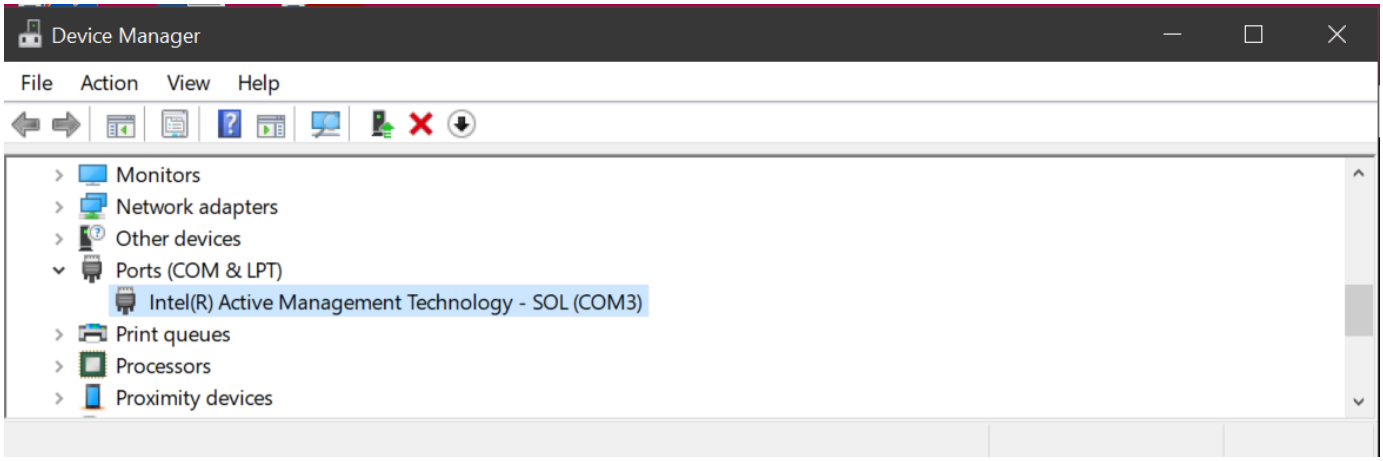
Las siguientes instrucciones son para PuTTY en Windows. PuTTY es gratuito, pero puede que deba descargarlo.

Descargar PuTTY

Descargue e instale PuTTY desde la página de descarga de PuTTY.

Para crear un terminal serie en Windows con PuTTY

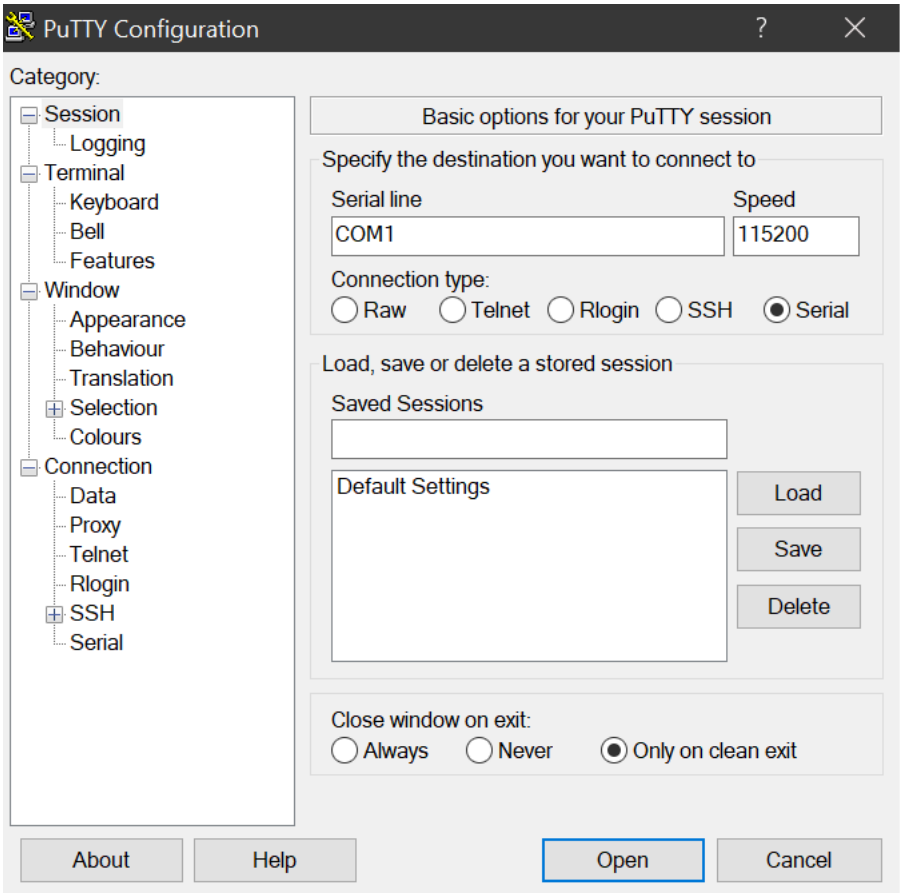
1. Conecte primero el cable USB a su portátil con Windows y después al servidor.
2. Desde el escritorio, haga clic con el botón derecho en Inicio y seleccione Administrador de dispositivos.
3. En Administrador de dispositivos, expanda Puertos (COM y LPT) para determinar el puerto COM de la conexión de serie USB. Verá un nodo denominado Puerto de serie USB (COM **#**). El valor del puerto COM depende del hardware.



4. En PuTTY, en Sesión, seleccione Serie como Tipo de conexión y, a continuación, introduzca la siguiente información:

   - En Línea de serie, ingrese el puerto COM # del administrador de dispositivos.
   - En Velocidad, introduzca: `115200`

   La imagen siguiente muestra un ejemplo de la página de Configuración de PuTTY:



5. Elija Open.

   Aparece una ventana de consola vacía. Puede tardar entre 1 y 2 minutos en aparecer una de las siguientes opciones:

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

Conexión de serie Mac

Las siguientes instrucciones son para screen en macOS. Puede encontrar screen en el sistema operativo.

Para crear un terminal serie en macOS mediante screen

1. Conecte primero el cable USB a su portátil Mac y después al servidor.

2. En Terminal, haga una lista `/dev` con un filtro `*usb*` de salida para encontrar el puerto serie virtual.

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

   El dispositivo en serie aparece como `tty`. Por ejemplo, considere la siguiente salida de muestra del comando list anterior:

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

3. En Terminal, use screen con el dispositivo en serie y una velocidad en baudios de la conexión en serie para configurar la conexión en serie. En el siguiente comando, sustituya *EJEMPLO1* por el valor de su portátil.

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

   Aparece una ventana de consola vacía. Puede tardar entre 1 y 2 minutos en aparecer una de las siguientes opciones:

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

Pruebe la conexión

En esta sección se describe cómo utilizar la herramienta de configuración de Outpost para probar la conexión. No necesita credenciales de IAM para probar la conexión. Su conexión debe poder resolver el DNS para acceder al Región de AWS.

1. Pruebe los enlaces y recopile información sobre la conexión
2. Pruebe el solucionador de DNS
3. Compruebe el acceso al Región de AWS

Para probar los enlaces

1. Primero, conecte el cable USB al portátil y, después, al servidor.
2. Utilice un programa de terminal serie, como PuTTY o screen, para conectarse al servidor. Para obtener más información, consulte the section called “Cree una conexión en serie con el servidor”.
3. Pulse Enter para acceder a la línea de comandos de la herramienta de configuración de Outpost.

```
Outpost>
```

> **Note**
>
> Si tras encender el servidor, ve una luz roja persistente en el interior del chasis del servidor, en el lado izquierdo, y no logra conectarse a la herramienta de configuración del Outpost, es posible que tenga que apagar y drenar el servidor para continuar. Para drenar el servidor, desconecte todos los cables de la red y de la fuente de alimentación, espere cinco minutos y, a continuación, encienda y vuelva a conectar la red.

4. Utilice describe-links para obtener información sobre los enlaces de red del servidor. Los servidores del Outpost deben tener un enlace de servicio y un enlace de interfaz de red local (LNI).

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

Si obtiene `connected: False` por alguno de los enlaces, solucione los problemas de conexión de red del hardware.

5. Utilice describe-ip para obtener el estado de la asignación de IP y la configuración del enlace de servicio.

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

Es posible que falte el valor NTP, ya que el NTP es opcional en un conjunto de opciones de DHCP. No debería faltar ningún otro valor.

Para probar el DNS

1. Primero, conecte el cable USB al portátil y, después, al servidor.
2. Utilice un programa de terminal serie, como PuTTY o screen, para conectarse al servidor. Para obtener más información, consulte the section called “Cree una conexión en serie con el servidor”.
3. Pulse Enter para acceder a la línea de comandos de la herramienta de configuración de Outpost.

```
Outpost>
```

> **Note**
>
> Si tras encender el servidor, ve una luz roja persistente en el interior del chasis del servidor, en el lado izquierdo, y no logra conectarse a la herramienta de configuración del Outpost, es posible que tenga que apagar y drenar el servidor para continuar. Para drenar el servidor, desconecte todos los cables de la red y de la fuente de alimentación, espere cinco minutos y, a continuación, encienda y vuelva a conectar la red.

4. Utilice export para introducir la región principal del servidor del Outpost como valor para AWS_DEFAULT_REGION.

   AWS_DEFAULT_REGION=*Region*

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

   result: OK
   checksum: 0xB2A945RE
   ```

   - No incluya ningún espacio antes o después del signo igual (=).
   - No se guarda ningún valor del entorno. Debe exportar Región de AWS cada vez que ejecute la herramienta de configuración de Outpost.
   - En el caso que decida que un tercero instale el servidor, debe proporcionarle la región principal.

5. Use describe-resolve para determinar si el servidor Outpost puede acceder a un solucionador de DNS y resolver la dirección IP del punto de conexión de configuración de Outpost en la región. Requiere al menos un enlace con una configuración IP.

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

Para probar el acceso a Regiones de AWS

1. Primero, conecte el cable USB al portátil y, después, al servidor.
2. Utilice un programa de terminal serie, como PuTTY o screen, para conectarse al servidor. Para obtener más información, consulte the section called “Cree una conexión en serie con el servidor”.
3. Pulse Enter para acceder a la línea de comandos de la herramienta de configuración de Outpost.

   ```
   Outpost>
   ```

> **Note**
>
> Si tras encender el servidor, ve una luz roja persistente en el interior del chasis del servidor, en el lado izquierdo, y no logra conectarse a la herramienta de configuración del Outpost, es posible que tenga que apagar y drenar el servidor para continuar. Para drenar el servidor, desconecte todos los cables de la red y de la fuente de alimentación, espere cinco minutos y, a continuación, encienda y vuelva a conectar la red.

4. Utilice export para introducir la región principal del servidor del Outpost como valor para `AWS_DEFAULT_REGION`.

   `AWS_DEFAULT_REGION=`*`Region`*

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

   result: OK
   checksum: 0xB2A945RE
   ```

   - No incluya ningún espacio antes o después del signo igual (=).
   - No se guarda ningún valor del entorno. Debe exportar Región de AWS cada vez que ejecute la herramienta de configuración de Outpost.
   - En el caso que decida que un tercero instale el servidor, debe proporcionarle la región principal.

5. Utilice describe-reachability para determinar si el servidor del Outpost puede acceder al punto de conexión de la configuración del Outpost de la región. Es necesario contar con una configuración de DNS que funcione; usted la puede determinar mediante el uso de describe-resolve.

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

   - `is_reachable` indica el resultado de la prueba
   - `src_ip` es la dirección IP del servidor

- `dst_ip` es la dirección IP del punto de conexión de la configuración del Outpost en la región
- `dst_port` es el puerto al que se conecta el servidor de `dst_ip`

Autorice el servidor

En esta sección se describe cómo utilizar la herramienta de configuración de Outpost y las credenciales de IAM de la cuenta de AWS que contiene el Outpost para autorizar el servidor.

Para autorizar el servidor

1. Primero, conecte el cable USB al portátil y, después, al servidor.
2. Utilice un programa de terminal serie, como PuTTY o screen, para conectarse al servidor. Para obtener más información, consulte the section called “Cree una conexión en serie con el servidor”.
3. Pulse Enter para acceder a la línea de comandos de la herramienta de configuración de Outpost.

   ```
   Outpost>
   ```

   > **Note**
   >
   > Si tras encender el servidor, ve una luz roja persistente en el interior del chasis del servidor, en el lado izquierdo, y no logra conectarse a la herramienta de configuración del Outpost, es posible que tenga que apagar y drenar el servidor para continuar. Para drenar el servidor, desconecte todos los cables de la red y de la fuente de alimentación, espere cinco minutos y, a continuación, encienda y vuelva a conectar la red.

4. Use export para introducir sus credenciales de IAM en la herramienta de configuración de Outpost. Si utiliza un tercero para instalar el servidor, debe proporcionarle a dicho tercero las credenciales IAM.

   Para realizar la autenticación, debe exportar las cuatro variables siguientes. Exporte una variable a la vez. No incluya ningún espacio antes o después del signo igual (=).

   - `AWS_ACCESS_KEY_ID=`*`access-key-id`*
   - `AWS_SECRET_ACCESS_KEY=`*`secret-access-key`*
   - `AWS_SESSION_TOKEN=`*`session-token`*

- Utilice el AWS CLI `GetSessionToken` comando para obtener el`AWS_SESSION_TOKEN`. Para obtener más información, consulte get-session-token en la Referencia de comandos de AWS CLI .

  > **Note**
  >
  > Debe tener el archivo AWSOutpostsAuthorizeServerPolicyadjunto a su función de IAM para obtener el`AWS_SESSION_TOKEN`.

- Para instalarlo AWS CLI, consulte Instalación o actualización de la última versión de la AWS CLI en la Guía del AWS CLI usuario de la versión 2.

- `AWS_DEFAULT_REGION=`*`Region`*

  Utilice la región principal del servidor Outpost como valor para `AWS_DEFAULT_REGION`. Si utiliza un tercero para instalar el servidor, debe proporcionarle a dicho tercero la región principal.

El resultado de los siguientes ejemplos muestra que las exportaciones se han realizado correctamente.

```
Outpost>export AWS_ACCESS_KEY_ID=AKIAIOSFODNN7EXAMPLE

result: OK
checksum: example-checksum
```

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

result: OK
checksum: example-checksum
```

```
Outpost>export AWS_SESSION_TOKEN=MIICiTCCAfICCQD6m7oRw0uXOjANBgk
VVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6
b24xFDASBgNVBAsTC0lBTSBDb25zb2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAd
BgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5jb20wHhcNMTEwNDI1MjA0NTIxWhcN
MTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYD
VQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAsTC0lBTSBDb25z
b2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEWEG5vb25lQGFt
YXpvbi5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ
```

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

result: OK
checksum: example-checksum
```

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

result: OK
checksum: example-checksum
```

5. Utilice start-connection para crear una conexión segura con la región.

   El resultado del siguiente ejemplo muestra que la conexión se ha iniciado correctamente.

```
Outpost>start-connection

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

6. Espere unos 5 minutos.
7. Utilice get-connection para verificar si se ha establecido la conexión con la región.

   El resultado del siguiente ejemplo muestra una conexión correcta.

```
Outpost>get-connection


---
keys_exchanged: True
connection_established: True
exchange_active: False
primary_peer: xx.xx.xx.xx:xxx
primary_status: success
primary_connection_id: a1b2c3d4567890abcdefEXAMPLE11111
```

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

Después de que `keys_exchanged` y `connection_established` cambian a `True`, el servidor Outpost se aprovisiona automáticamente y se actualiza con el software y la configuración más recientes.

> **Note**
>
> Tenga en cuenta lo siguiente acerca del proceso de aprovisionamiento:
>
> - Una vez completada la activación, pueden pasar hasta 10 horas hasta que el servidor Outpost se ponga en funcionamiento.
> - Debe mantener la alimentación y la red del servidor del Outpost conectadas y estables durante este proceso.
> - Es normal que el enlace de servicio fluctúe durante este proceso.
> - Si `exchange_active` es `True`, la conexión aún se está estableciendo. Vuelva a intentarlo en 5 minutos.
> - Si `keys_exchanged` o `connection_established` es `False`, y si `exchange_active` es `True`, la conexión aún se está estableciendo. Vuelva a intentarlo en 5 minutos.
> - Si `keys_exchanged` o `connection_established` es `False` incluso después de 1 hora, póngase en contacto con el AWS Support Center.
> - Si `primary_status: No such asset id found.` aparece el mensaje, confirme lo siguiente:
>   - Ha especificado la región correcta.
>   - Estás utilizando la misma cuenta que utilizaste para solicitar el servidor Outpost.

Si la región es correcta y está utilizando la misma cuenta que utilizó para solicitar el servidor Outpost, póngase en contacto con AWS Support Center.

- El atributo de `LifeCycleStatus` del Outpost pasará de `Provisioning` a `Active`. A continuación, recibirá un correo electrónico informándole que el servidor del Outpost está aprovisionado y activado.
- No necesita volver a autorizar el servidor de Outposts una vez activado el servidor de Outposts.

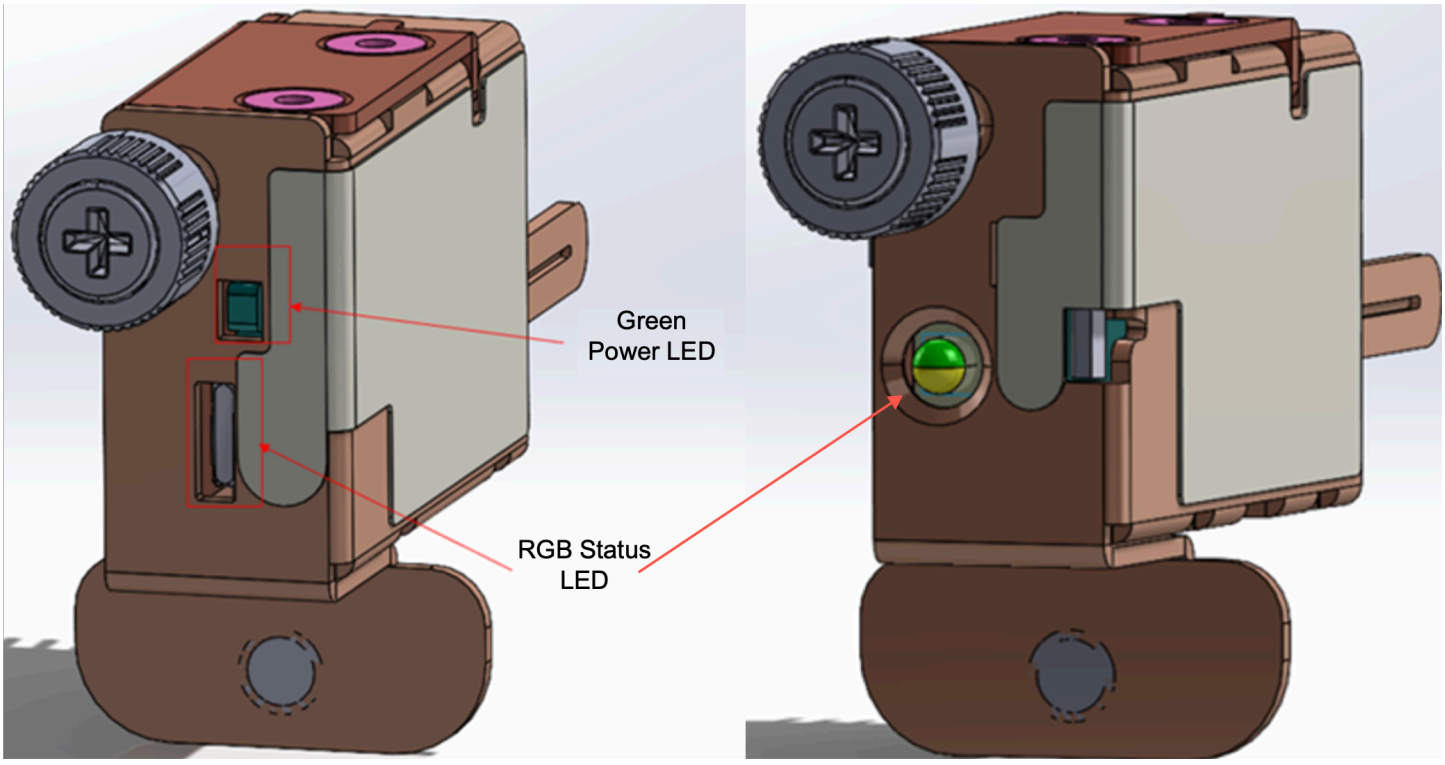
8. Después de realizar una conexión exitosa, puede desconectar su portátil del servidor.

Compruebe los LED NSK

Una vez finalizado el proceso de aprovisionamiento, compruebe los LED de NSK.

AWS Outposts admite dos versiones de NSK: Atlas 2.0 y Atlas 3.0. Ambas versiones de NSK tienen un LED de estado RGB. Además, el Atlas 3.0 tiene un LED de alimentación verde.

La siguiente imagen muestra la ubicación de los LED en el Atlas 2.0 y el Atlas 3.0:



Atlas 3.0 Atlas 2.0

Para verificar los LED de estado y alimentación del NSK

1. Compruebe el color del LED de estado RGB. Si el color es verde, el NSK está en buen estado. Si el color no es verde, póngase en contacto AWS Support.
2. Si tiene un Atlas 3.0 NSK, compruebe el LED de alimentación verde. Si la luz verde está encendida, el NSK está correctamente conectado al host y tiene alimentación. Si la luz verde no está encendida, póngase en contacto con AWS Support.

Referencia de comandos de la herramienta de configuración del Outpost

La herramienta de configuración del Outpost proporciona los siguientes comandos.

Comandos

- Exportar
- Echo
- Describir enlaces
- Describir la IP
- Describir la resolución
- Describir la accesibilidad
- Iniciar conexión
- Conseguir la conexión

Exportar

export

Utilice export para establecer las credenciales de IAM como variables de entorno.

Sintaxis

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

export adopta la sentencia de asignación de variables.

Debe utilizar el siguiente formato: *variable*=*value*

Para realizar la autenticación, debe exportar las cuatro variables siguientes. Exporte una variable a la vez. No incluya ningún espacio antes o después del signo igual (=).

- AWS_ACCESS_KEY_ID=*access-key-id*
- AWS_SECRET_ACCESS_KEY=*secret-access-key*
- AWS_SESSION_TOKEN=*session-token*
- AWS_DEFAULT_REGION=*Region*

  Utilice la región principal del servidor Outpost como valor para AWS_DEFAULT_REGION.

Example : importaciones de credenciales con éxito

```
Outpost>export AWS_ACCESS_KEY_ID=AKIAIOSFODNN7EXAMPLE

result: OK
checksum: example-checksum
```

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

result: OK
checksum: example-checksum
```

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

result: OK
checksum: example-checksum
```

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

result: OK
checksum: example-checksum
```

Echo

echo

Utilice echo para mostrar el valor que se ha establecido para una variable mediante el uso del comando export.

Sintaxis

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

El *variable-name* puede ser uno de los siguientes:

- AWS_ACCESS_KEY_ID
- AWS_SECRET_ACCESS_KEY
- AWS_SESSION_TOKEN
- AWS_DEFAULT_REGION

Example : correcto

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

result: OK
checksum: example-checksum

---

Outpost>echo $AWS_DEFAULT_REGION

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

Example : error, porque el valor de la variable no se estableció con el comando export

```
Outpost> echo $AWS_ACCESS_KEY_ID
```

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

Example : error, porque el nombre de la variable no es válido

```
Oupost>echo $foo

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

Example : error, porque hay un problema de sintaxis

```
Outpost>echo AWS_SECRET_ACCESS_KEY

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

Describir enlaces

describe-links

Utilice describe-links para obtener información sobre los enlaces de red del servidor. Los servidores del Outpost deben tener un enlace de servicio y un enlace de interfaz de red local (LNI).

Sintaxis

```
Outpost>describe-links
```

describe-links no adopta argumentos.

Describir la IP

describe-ip

Utilice describe-ip para devolver el estado de la asignación de IP y la configuración para cada enlace conectado.

Sintaxis

```
Outpost>describe-ip
```

describe-ip no adopta argumentos.

Describir la resolución

describe-resolve

Use describe-resolve para determinar si el servidor Outpost puede acceder a un solucionador de DNS y resolver la dirección IP del punto de conexión de configuración de Outpost en la región. Requiere al menos un enlace con una configuración IP.

Sintaxis

```
Outpost>describe-resolve
```

describe-resolve no adopta argumentos.

Describir la accesibilidad

describe-reachability

Utilice describe-reachability para determinar si el servidor del Outpost puede acceder al punto de conexión de la configuración del Outpost de la región. Es necesario contar con una configuración de DNS que funcione; usted la puede determinar mediante el uso de describe-resolve.

Sintaxis

```
Outpost>describe-reachability
```

describe-reachability no adopta argumentos.

Iniciar conexión

start-connection

Utilice start-connection para iniciar una conexión con el servicio Outpost de la región. Este comando obtiene las credenciales de Signature Version 4 (SigV4) de las variables de entorno que haya cargado con export. La conexión se ejecuta de forma asíncrona y se devuelve inmediatamente. Para verificar el estado de la conexión, utilice get-connection.

Sintaxis

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

start-connection utiliza un índice de conexión opcional para iniciar otra conexión. Los únicos valores válidos son `0` y `1`.

Example : conexión iniciada

```
Outpost>start-connection

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

Conseguir la conexión

get-connection

Utilice get-connection para obtener el estado de la conexión.

Sintaxis

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

get-connection toma un índice de conexión opcional para devolver el estado de otra conexión. Los únicos valores válidos son `0` y `1`.

Example : conexión realizada correctamente

```
Outpost>get-connection


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

Nota:

- Si `exchange_active` es `True`, la conexión aún se está estableciendo. Vuelva a intentarlo en 5 minutos.
- Si `keys_exchanged` o `connection_established` es `False`, y si `exchange_active` es `True`, la conexión aún se está estableciendo. Vuelva a intentarlo en 5 minutos.

Si el problema persiste después de 1 hora, póngase en contacto con el AWS Support Center.

Lanza una instancia en tu servidor Outpost

Una vez que esté instalado el Outpost y la capacidad de computación y de almacenamiento estén disponibles para su uso, puede comenzar con la creación de recursos. 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
- Paso 2: lanzar una instancia en el Outpost
- Paso 3: configurar la conectividad
- Paso 4: comprobar la conexión

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, habilite la subred para las interfaces de red locales.

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 espacio de almacenamiento para satisfacer las necesidades de la aplicación. Para obtener más información, consulte Volúmenes de almacén de instancias en la Guía del usuario de Amazon EC2.
- Debe especificar una AMI con una sola instantánea. No se admiten las AMI con más de una instantánea.
- 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 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. Abre la AWS Outposts consola en https://console.aws.amazon.com/outposts/.
2. En el panel de navegación, elija Outposts.
3. Seleccione el Outpost y, a continuación, elija Acciones, Ver detalles.
4. En la página de Resumen de Outpost, seleccione Lanzar instancia. Se le redirigirá al asistente de lanzamiento de instancias en la consola de Amazon EC2. Seleccionamos la subred de Outpost por ti y te mostramos solo los tipos de instancias compatibles con tus servidores de Outposts.
5. Elige un tipo de instancia que sea compatible con tus servidores de Outposts.

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 LNI para la subred de Outpost, esta interfaz de red será la interfaz de red local de la instancia.
7. Complete el asistente para lanzar la instancia en la subred del Outpost. Para obtener más información, consulte los siguientes temas en la Guía del usuario de Amazon EC2:

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

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 Agregar un LNI después del lanzamiento.

Debe configurar la interfaz de red local de la instancia con una dirección IP de la red local. Normalmente, esto se hace mediante DHCP. 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, ejecuta el `ping` comando 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 la conexión a una instancia de Linux, consulte Conectarse a una instancia de Linux en la Guía del usuario de Amazon EC2. Para obtener información sobre la conexión a una instancia de Windows, consulte Conectarse a una instancia de Windows 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 de avanzada

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

```
aws ec2 run-instances \
    --image-id ami-abcdefghi1234567898 \
    --instance-type c5.large \
```

```
    --key-name MyKeyPair \
    --security-group-ids sg-1a2b3c4d123456787 \
    --subnet-id subnet-6e7f829e123445678
```

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

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

   ```
   ping 10.0.1.5
   ```

   A continuación, se muestra un ejemplo del resultado.

   ```
   Pinging 10.0.1.5

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

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

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

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 puede utilizar la conectividad privada para la conexión de enlace de servicio que conecta el servidor Outpost con su AWS región o región de AWS Outposts origen.

Contenido

Conectividad a través de enlaces de servicio

Durante el AWS Outposts aprovisionamiento, creas o AWS creas una conexión de enlace de servicio que conecta tu Outpost con la AWS región o AWS Outposts región de origen que 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 para AWS, consulte Rangos de direcciones IP de AWS.

Una vez establecido el enlace de servicio, el Outpost entra en servicio y es 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.
- Tráfico entre el Outpost y cualquier VPC asociada, 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. La red debe admitir una MTU de 1500 bytes entre los puntos finales de Outpost y Service Link en la región principal. AWS Para obtener información sobre la MTU requerida entre una instancia de Outpost y una instancia de la AWS región a través del enlace de servicio, consulte la unidad máxima de transmisión (MTU) de la red para su instancia de Amazon EC2 en la Guía del usuario de Amazon EC2.

Recomendaciones de ancho de banda para el enlace de servicio

Para disfrutar de una experiencia y una resiliencia óptimas, se AWS recomienda utilizar una conectividad redundante de al menos 500 Mbps para la conexión del enlace de servicio a la región. AWS La utilización máxima de cada servidor de Outpost es de 500 Mbps. Para aumentar la velocidad de conexión, utilice múltiples servidores de Outpost. 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.

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 las AMI en caché. Las AMI se descargan de la región cada vez que se lanza una instancia.

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

Firewalls y enlace de servicio

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

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

- Tráfico de administración al Outpost a través del enlace de servicio
- Tráfico entre el Outpost y cualquier VPC asociada

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

Si utiliza un firewall para limitar la conectividad desde la VLAN de enlace de servicio, puede bloquear todas las conexiones entrantes. Debe permitir que las conexiones salientes regresen al 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 DNS proporcionado por DHCP
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

> **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.

Actualizaciones y enlace de servicio

AWS mantiene una conexión de red segura entre su servidor Outpost y su AWS región principal. 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 AWS Las mejores prácticas de WellArchitected recomiendan implementar aplicaciones en dos Outposts patentados en diferentes zonas de disponibilidad con un diseño activo-activo. Para obtener más información, consulte Consideraciones sobre el diseño y la arquitectura de AWS Outposts alta disponibilidad.

El enlace de servicio se actualiza periódicamente para mantener la calidad y el rendimiento operativos. Durante el mantenimiento, es posible que se observen 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 siguiendo las mejores prácticas de AWS Well-Architected y asegurándose de que sus aplicaciones sean resistentes a los fallos o a las actividades de mantenimiento que afecten a un único servidor Outpost.

Conexiones de Internet redundantes

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

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

Outposts y sitios

Administra Outposts y sitios para. AWS Outposts

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

Temas

- Administre Outposts
- Administre los sitios de Outposts

Administre Outposts

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

Para crear un Outpost

1. Abra la AWS Outposts consola en https://console.aws.amazon.com/outposts/.
2. Para cambiarla Región de AWS, usa el selector de regiones en la esquina superior derecha de la página.
3. En el panel de navegación, elija Outposts.
4. Seleccione Crear Outpost.
5. Elija un tipo de hardware para este Outpost.
6. Escriba un nombre y la descripción de su Outpost.
7. Seleccione una zona de disponibilidad para su Outpost.
8. (Opcional) Elija Opción de conectividad privada. Para la VPC y la subred, selecciona una VPC y una subred en la misma AWS cuenta y zona de disponibilidad que tu Outpost.

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

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

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

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

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

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

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

Para editar el nombre y la descripción del Outpost

1. Abre la consola en https://console.aws.amazon.com/outposts/. AWS Outposts
2. Para cambiarla Región de AWS, usa el selector de regiones en la esquina superior derecha de la página.
3. En el panel de navegación, elija Outposts.
4. Seleccione el Outpost y, a continuación, elija Acciones, Editar Outpost.
5. Modifique el nombre y la descripción.

   Para Nombre, escriba el nombre.

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

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

Para ver los detalles de Outpost

1. Abre la AWS Outposts consola en https://console.aws.amazon.com/outposts/.
2. Para cambiarla Región de AWS, usa el selector de regiones en la esquina superior derecha de la página.
3. En el panel de navegación, elija Outposts.
4. Seleccione el Outpost y, a continuación, elija Acciones, Ver detalles.

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

Para ver los detalles de Outpost con el AWS CLI

- Utilice el comando get-outpost AWS CLI .

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

Para administrar las etiquetas de Outpost

1. Abra la AWS Outposts consola en https://console.aws.amazon.com/outposts/.
2. Para cambiarla Región de AWS, usa el selector de regiones en la esquina superior derecha de la página.
3. En el panel de navegación, elija Outposts.
4. Seleccione el Outpost y, a continuación, elija Acciones, Administrar etiquetas.
5. Añada o elimine una etiqueta.

   Para agregar una etiqueta, elija Agregar nueva etiqueta y haga lo siguiente:

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

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

Administre los sitios de Outposts

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

Para crear un sitio de Outpost

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

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

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

Para editar un sitio

1. Abra la AWS Outposts consola en https://console.aws.amazon.com/outposts/.
2. Para cambiarla Región de AWS, usa el selector de regiones en la esquina superior derecha de la página.
3. En el panel de navegación, seleccione Sitios.
4. Seleccione el sitio y, a continuación, seleccione Acciones, Editar sitio.
5. Puede modificar el nombre, la descripción, la dirección operativa y los detalles del sitio.

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

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

Para consultar los detalles del servicio

1. Abre la AWS Outposts consola en https://console.aws.amazon.com/outposts/.
2. Para cambiarla Región de AWS, usa el selector de regiones en la esquina superior derecha de la página.
3. En el panel de navegación, seleccione Sitios.
4. Seleccione el sitio y, a continuación, elija Acciones, Ver detalles.

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

Para administrar las etiquetas del sitio

1. Abre la AWS Outposts consola en https://console.aws.amazon.com/outposts/.
2. Para cambiarla Región de AWS, usa el selector de regiones en la esquina superior derecha de la página.
3. En el panel de navegación, seleccione Sitios.

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

   Para agregar una etiqueta, elija Agregar nueva etiqueta y haga lo siguiente:

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

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

Devolver un AWS Outposts servidor

Si AWS Outposts detecta un defecto en el servidor, le informaremos, iniciaremos el proceso de sustitución para enviarle un nuevo servidor y le proporcionaremos la etiqueta de envío a través de la AWS Outposts consola.

Si quiere devolver el servidor porque este ha llegado al final de la vigencia del contrato o por cualquier otro motivo, póngase en contacto con el AWS Support Center.

Temas

Los siguientes pasos explican cómo devolver un servidor a AWS.

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 comando disassociate-resource-share.

   Para ver la lista de recursos de Outpost que se pueden compartir, consulte Recursos de Outpost que se pueden compartir.
2. Cree copias de seguridad de los datos almacenados en el almacenamiento de instancias de las instancias Amazon EC2 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, siga las instrucciones de Termine su instancia en la Guía del usuario de Amazon EC2.

2. Obtenga la etiqueta de envío para la devolución

> **Important**
>
> Solo debes usar la etiqueta de envío que se AWS proporciona. No cree su propia etiqueta de envío.

Obtenga su etiqueta de envío según el motivo de la devolución.

Shipping label for a server that is being replaced

1. Abra la AWS Outposts consola en https://console.aws.amazon.com/outposts/.
2. En el panel de navegación, elija Pedidos.
3. En Resumen del pedido de sustitución, seleccione Imprimir etiqueta de devolución y elija el identificador de configuración del servidor que planifica devolver.

Shipping label for a server that is not being replaced

1. Ponerse en contacto con el AWS Support Center.
2. Solicite una etiqueta de envío para el servidor que desea devolver.

3. Empaquete el servidor

Para empaquetar el servidor, utilice la caja en el que vino originalmente, así como el material de embalaje suministrado. También puede utilizar la caja en la que viene el servidor de reemplazo. También puede ponerse en contacto con el AWS Support Center para solicitar una caja. Después de embalar el servidor, pegue la etiqueta de envío AWS proporcionada.

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 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 • Un número de teléfono • Una dirección de correo electrónico
Bahréin	
Brasil	
Brunéi	
Canadá	
Chile	
Colombia	
Hong Kong	
India	
Indonesia	
Japón	
Malasia	
Nigeria	
Omán	
Panamá	

País	Contacto
Perú	
Filipinas	
Serbia	
Singapur	
Sudáfrica	
Corea del Sur	
Taiwán	
Tailandia	
Emiratos Árabes Unidos	
Vietnam	
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. Introduce el número de seguimiento de la etiqueta AWS de envío proporcionada para obtener un envío gratuito.

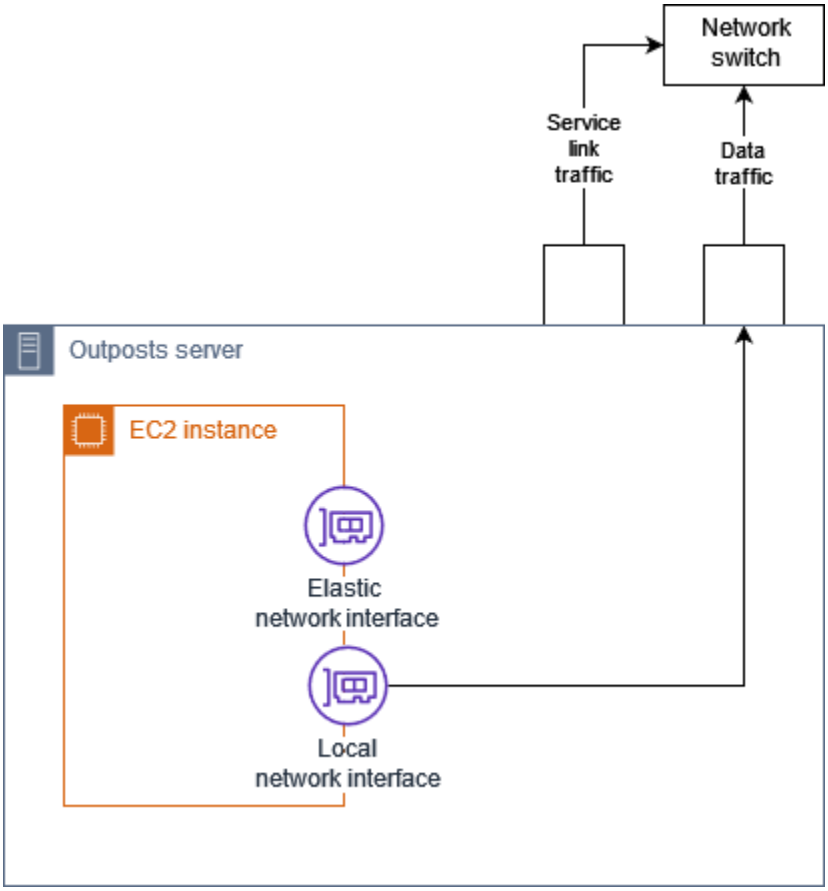
País	Contacto
Todos los otros países	Ponerse en contacto con DHL. Puede devolver el servidor mediante alguna de las siguientes formas: • Dejar el servidor en una sucursal de DHL. • Programar una recogida para la fecha y hora que prefiera. Introduce el número de guía de DHL que aparece en la etiqueta de envío AWS proporcionada para obtener un envío gratuito. Si aparece el siguiente `Courier pickup cannot 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

En el caso de AWS Outposts los servidores, una interfaz de red local (LNI) es un componente de red lógico que conecta las instancias de Amazon EC2 de la subred de Outposts a la red local.

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 Outpost 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 Interfaces 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 (eth0) 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 Outpost.
- Las interfaces de red local no admiten el modo promiscuo ni la suplantación de direcciones MAC.

Rendimiento

El LNI de cada tamaño de instancia proporciona una parte del ancho de banda físico disponible del LNI de 10 GbE. En la siguiente tabla, se muestra el rendimiento de la red LNI 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.large	0,1625	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

Tipo de instancia	Banda ancha de base (Gbps)	Banda ancha con ráfagas (Gbps)
c6id.32xlarge	10	10
c6gd.medium	0,15625	4
c6gd.large	0,3125	4
c6gd.xlarge	0,625	4
c6gd.2xlarge	1,25	4
c6gd.4xlarge	2,5	4
c6gd.8xlarge	4.8	4.8
c6gd.12xlarge	7.5	7.5
c6gd.16xlarge	10	10

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 sobre las instancias de Linux, consulte Supervisar el rendimiento de la red de su instancia EC2 en la Guía del usuario de Amazon EC2. Para las instancias de Windows, consulte Supervisar el rendimiento de la red de su instancia 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.

Habilitar las subredes en los servidores de Outposts para las interfaces de redes locales

Utilice el comando modify-subnet-attribute de AWS CLI para habilitar una subred Outpost para las interfaces de red locales. 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. Por ejemplo, un valor de 1 indica que la interfaz de red secundaria (eth1) de una instancia de la subred de Outpost es la interfaz de red local.

Habilitación de una subred de Outpost para las interfaces de red local

En el símbolo del sistema, use el comando siguiente para especificar la posición del dispositivo para la interfaz de red locales.

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

Uso de interfaces de red local

Utilice esta sección para entender cómo trabajar con interfaces de red local.

Tareas

- Agregue una interfaz de red local
- Visualice la interfaz de red local
- Configuración del sistema operativo

Agregue una interfaz de red local

Puede agregar una interfaz de red local (LNI) 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 o un SDK en su lugar. AWS CLI AWS Por ejemplo, usa los siguientes comandos de AWS CLI: create-network-interface y attach-network-interface.

Cómo agregar un LNI durante el lanzamiento de la instancia

1. En el asistente de inicialización de instancias, seleccione Editar que se encuentra junto a Configuración de red.
2. Expanda Configuración de red avanzada.
3. Elija Agregue interfaz de red. Se crea una interfaz de red al usar el índice de dispositivos 1. Si especificó 1 como índice de dispositivos LNI para la subred de Outpost, esta interfaz de red será la interfaz de red local de la instancia.
4. Elija la subred de Outpost y actualice la configuración de la interfaz de red según sea necesario.
5. Complete el asistente para lanzar la instancia.

Cómo agregar un LNI después del lanzamiento de la instancia

1. En el panel de navegación, elija Red y seguridad y, a continuación, Interfaces de red.
2. Crear la interfaz de red
    a. Elija Crear interfaz de red.
    b. Seleccione la misma subred de Outpost que la instancia.
    c. Verifique que la dirección IPv4 privada esté configurada para laasignación automática.
    d. Seleccione cualquier grupo de seguridad. Los grupos de seguridad no se aplican a las LNI, por lo que el grupo de seguridad que seleccione no es relevante.

e. Elija Crear interfaz de red.

3. 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 LNI 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 dirección IPv4 privada para el LNI de la subred CIDR. Esta dirección no es la dirección IP del LNI 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 del LNI en el sistema operativo del host, 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

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

Contenido

- Conectividad física del servidor
- Tráfico de enlace de servicio para servidores
- Tráfico de enlaces de la interfaz de red local (LNI)
- Asignación de direcciones IP del servidor
- Registro del servidor

Topología del servidor de su red

Un servidor de Outpost 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 Outpost.

Etiqueta de tráfico	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 o varias VPN personalizadas 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 (LNI): 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

Etiqueta de tráfico	Descripción
	red en las instalaciones. El tráfico de enlace local también puede incluir instancias que se comunican con Internet a través de la red en las instalaciones.

Conectividad física del servidor

Cada servidor de Outpost 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 Outpost. 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 Outpost funcione. Utilice la interfaz de 2 para el tráfico de enlace de servicio y la interfaz de 1 para el tráfico de enlace LNI. 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 del enlace de servicio debe tener un DNS público disponible para que Outpost detecte su punto final de registro en la región. AWS La conexión puede tener un dispositivo NAT entre el servidor de Outpost 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

Velocidad de enlace ascendente

Cada servidor de Outposts requiere una velocidad mínima de enlace ascendente de 20 Mbps a la región de AWS .

En función del uso del enlace LNI y del enlace de servicio, es posible que necesite un enlace ascendente más rápido. Para obtener más información, consulte Recomendaciones de ancho de banda para enlaces de servicios.

Tráfico de enlaces de la interfaz de red local (LNI)

Configure el puerto de enlace LNI 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 LNI 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 el LNI 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 el LNI 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 del LNI 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 para Amazon Linux en la Guía del usuario de Amazon EC2.
- 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 asignaciones de direcciones IP públicas para los servidores de Outpost.

El protocolo de configuración dinámica de hosts (DHCP) es un protocolo de administración de redes que se utiliza para automatizar el proceso de configuración de dispositivos en redes IP. En el contexto de los servidores de Outpost, puede utilizar DHCP de dos maneras:

- Tarjetas de red en el servidor
- Interfaces de red local en las instancias

Para el enlace de servicio, los servidores de Outpost utilizan DHCP para asociarse a la red local. El DHCP debe devolver los servidores de nombres DNS y una puerta de enlace predeterminada. Los servidores de Outpost no admiten la asignación de IP estática del enlace de servicio.

En el caso del enlace LNI, utilice DHCP para configurar las instancias que se asociarán a la red local. Para obtener más información, consulte the section called “Configuración del sistema operativo”.

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

Registro del servidor

Cuando los servidores de Outpost 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 Outpost utilizan el puerto TCP 443 para facilitar la comunicación con la región a través de Internet pública. Actualmente, AWS Outposts los servidores no admiten la conectividad privada a través de VPC. Para obtener más información, consulte the section called “Paso 6: autorizar el servidor”.

Trabajar con recursos de AWS Outposts compartidos

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

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

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

Un propietario de Outpost puede compartir recursos de Outpost con:

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

Contenido

- 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.

Estos son los recursos disponibles para los en bastidor de Outpost. Para obtener información sobre los recursos del bastidor, consulte Cómo trabajar con recursos de AWS Outposts compartidos en la Guía del usuario de AWS Outposts para bastidores de los 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.
  - Utilice la API de AWS Outposts 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, debe ser propietario de ese recurso en su cuenta de AWS. No puede compartir un recurso de Outpost que se haya compartido con usted.
- Para compartir un recurso de Outpost, debe compartirlo con una cuenta que se encuentre dentro de la organización.

Servicios relacionados

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

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

Uso compartido entre zonas de disponibilidad

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

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

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

1. Abra la consola de AWS RAM en https://console.aws.amazon.com/ram.
2. Los ID de AZ de la región actual se muestran en el panel Su ID de zona de disponibilidad en el lado derecho de la pantalla.

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

Uso compartido de un recurso de Outpost

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

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

Si forma parte de una organización de AWS Organizations y esta permite el uso compartido, puede conceder a los consumidores de la organización acceso desde la consola de AWS RAM al recurso de Outpost compartido. De lo contrario, los consumidores reciben una invitación para unirse al recurso compartido y se les concede acceso al recurso de Outpost compartido al aceptar la invitación.

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

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

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

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

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

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

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

Utilice el comando create-resource-share.

Dejar de compartir un recurso de Outpost compartido

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

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

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

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

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

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

Utilice el comando disassociate-resource-share.

Identificación de un recurso de Outpost compartido

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

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

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

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

Utilice los comandos list-outposts y describe-local-gateway-route-tables. El comando devuelve los recursos de Outpost que son de su propiedad y los que se comparten con usted. `OwnerId` muestra el ID de cuenta de AWS del propietario del recurso de Outpost.

Permisos de recursos de Outpost compartidos

Permisos de los propietarios

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

Permisos de los consumidores

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

Facturación y medición

A los propietarios se les cobran los Outposts y los recursos de Outpost que comparten. También se les facturarán los gastos de transferencia de datos relacionados con el tráfico de la VPN de enlace de servicio de Outpost desde la región AWS.

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

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

Limitaciones

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

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

Seguridad en AWS Outposts

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

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

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

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

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

Contenido

Protección de datos en AWS Outposts

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

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

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

Cifrado en reposo

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

Cifrado en tránsito

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

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

Funciones de IAM que puedes usar con Outposts AWS

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

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

Políticas basadas en la identidad para Outposts AWS

Compatibilidad con las políticas basadas en identidad	Sí

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

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

Ejemplos de políticas basadas en la identidad para Outposts AWS

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

Políticas basadas en recursos dentro de Outposts AWS

Compatibilidad con las políticas basadas en recursos	No

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

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

Acciones políticas para AWS Outposts

Admite acciones de política	Sí

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

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

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

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

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

```
outposts
```

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

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

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

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

Recursos de políticas para AWS Outposts

Admite recursos de políticas	Sí

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

El elemento `Resource` de la política JSON especifica el objeto u objetos a los que se aplica la acción. Las instrucciones deben contener un elemento `Resource` o `NotResource`. Como práctica recomendada, especifique un recurso utilizando el Nombre de recurso de Amazon (ARN). Puede hacerlo para acciones que admitan un tipo de recurso específico, conocido como permisos de nivel de recurso.

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

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

Algunas acciones de la API de AWS Outposts admiten varios recursos. Para especificar varios recursos en una única instrucción, separe los ARN con comas.

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

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

Claves condicionales de la política para AWS Outposts

Admite claves de condición de políticas específicas del servicio	Sí

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

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

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

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

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

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

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

ACL en Outposts AWS

Admite las ACL	No

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

ABAC con Outposts AWS

Admite ABAC (etiquetas en las políticas)	Sí

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

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

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

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

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

Uso de credenciales temporales con AWS Outposts

Compatible con el uso de credenciales temporales	Sí

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

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

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

Permisos principales entre servicios para Outposts AWS

Admite Forward access sessions (FAS)	Sí

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

realizar ambas acciones. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte Reenviar sesiones de acceso.

Roles de servicio para AWS Outposts

Compatible con roles de servicio	No

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

Funciones vinculadas al servicio para Outposts AWS

Compatible con roles vinculados al servicio	Sí

Un rol vinculado a un servicio es un tipo de rol de servicio que está vinculado a un. Servicio de AWS El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio aparecen en usted Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

Para obtener más información sobre la creación o administración de AWS roles vinculados al servicio Outposts, consulte. Uso de roles vinculados a servicios de AWS Outposts

AWS Ejemplos de políticas de Outposts

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

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

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

Contenido

Prácticas recomendadas sobre las políticas

Las políticas basadas en la identidad determinan si alguien puede crear, acceder o eliminar los recursos de AWS Outposts de tu cuenta. Estas acciones pueden generar 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 trabajo 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 AWS CloudFormation. Para obtener más información, consulte Elementos de la política de JSON de IAM: Condición en la Guía del usuario de IAM.
- Utilice el analizador de acceso de IAM para validar las políticas de IAM con el fin de garantizar la seguridad y funcionalidad de los permisos: el analizador de acceso de IAM valida políticas

nuevas y existentes para que respeten el lenguaje (JSON) de las políticas de IAM y las prácticas recomendadas de IAM. El analizador de acceso de IAM proporciona más de 100 verificaciones de políticas y recomendaciones procesables para ayudar a crear políticas seguras y funcionales. Para más información, consulte Política de validación de Analizador de acceso de IAM en la Guía de usuario de IAM.

- Requerir autenticación multifactor (MFA): si tiene un escenario que requiere usuarios de IAM o un usuario raíz en Cuenta de AWS su cuenta, active la MFA para mayor seguridad. Para solicitar la MFA cuando se invocan las operaciones de la API, agregue las condiciones de la MFA a sus políticas. Para más información, consulte Configuración del acceso a una API protegido por MFA en la Guía de usuario de IAM.

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

Ejemplo: uso de permisos de nivel de recursos

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

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

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

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

```
    }
  ]
}
```

Uso de roles vinculados a servicios de AWS Outposts

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

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

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

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

Permisos de roles vinculados a servicios de AWS Outposts

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

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

- `outposts.amazonaws.com`

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

- AWSOutpostsServiceRolePolicy
- AWSOutpostsPrivateConnectivityPolicy_ OutpostID

La AWSOutpostsServiceRolePolicypolítica es una política de funciones vinculadas al servicio que permite el acceso a AWS los recursos gestionados por. AWS Outposts

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

- Acción: `ec2:DescribeNetworkInterfaces` en `all AWS resources`
- Acción: `ec2:DescribeSecurityGroups` en `all AWS resources`
- Acción: `ec2:CreateSecurityGroup` en `all AWS resources`
- Acción: `ec2:CreateNetworkInterface` en `all AWS resources`

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

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

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

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

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

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

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

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

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

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

Creación de un rol vinculado a un servicio de AWS Outposts

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

Modificación de un rol vinculado a servicios de AWS Outposts

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

Eliminación de un rol vinculado a un servicio de AWS Outposts

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

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

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

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

Para eliminar AWS Outposts los recursos utilizados por AWSServiceRoleForOutposts _ OutpostID

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

Eliminación manual del rol vinculado a servicios mediante IAM

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

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

AWS Outposts admite el uso de funciones vinculadas al servicio en todas las regiones en las que el servicio está disponible. Para obtener más información, consulte Puntos de conexión y cuotas de AWS Outposts.

AWS políticas gestionadas para AWS Outposts

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

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

No puedes cambiar los permisos definidos en AWS las políticas administradas. Si AWS actualiza los permisos definidos en una política AWS administrada, la actualización afecta a todas las identidades

principales (usuarios, grupos y roles) a las que está asociada la política. AWS es más probable que actualice una política AWS administrada cuando Servicio de AWS se lance una nueva o cuando estén disponibles nuevas operaciones de API para los servicios existentes.

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

AWS política gestionada: AWSOutpostsServiceRolePolicy

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

AWS política gestionada: AWSOutpostsPrivateConnectivityPolicy

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

AWS política gestionada: AWSOutpostsAuthorizeServerPolicy

Utilice esta política para conceder los permisos necesarios para autorizar el hardware del servidor del Outpost en su red en las instalaciones. Para obtener más información, consulte Conceder permiso.

Esta política incluye los siguientes permisos.

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

AWS Outposts actualizaciones de las políticas AWS gestionadas

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

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

Seguridad de la infraestructura en AWS Outposts

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

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

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

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

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

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

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

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. AWS proporciona los siguientes recursos para ayudar con el cumplimiento:

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

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

- AWS Recursos de de cumplimiento: esta colección de libros de trabajo y guías puede aplicarse a su industria y ubicación.
- AWS Guías de cumplimiento para clientes: comprenda el modelo de responsabilidad compartida desde el punto de vista del cumplimiento. Las guías resumen las mejores prácticas para garantizar la seguridad Servicios de AWS y orientan los controles de seguridad en varios marcos (incluidos el Instituto Nacional de Estándares y Tecnología (NIST), el Consejo de Normas de Seguridad del Sector de Tarjetas de Pago (PCI) y la Organización Internacional de Normalización (ISO)).
- Evaluación de los recursos con reglas en la guía para AWS Config desarrolladores: el AWS Config servicio evalúa en qué medida las configuraciones de los recursos cumplen con las prácticas internas, las directrices del sector y las normas.

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

Monitorice su Outpost

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

CloudWatch métricas

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

CloudTrail registros

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

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

Logs de flujo de VPC

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

Replicación de tráfico

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

AWS Health Dashboard

El AWS Health Dashboard muestra información y notificaciones que se inician por cambios en la salud de los recursos de AWS. La información se presenta de dos formas: en un panel donde

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

CloudWatch métricas para AWS Outposts

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

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

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

Contenido

Métricas de Outpost

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

`ConnectedStatus`

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

Unidad: recuento

Resolución máxima: 1 minuto

Estadísticas: la estadística más útil es `Average`.

Dimensiones: `OutpostId`

`CapacityExceptions`

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

Unidad: recuento

Resolución máxima: 5 minutos

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

Dimensiones: `InstanceType` y `OutpostId`

`InstanceFamilyCapacityAvailability`

El porcentaje de capacidad de instancia disponible. Esta métrica no incluye la capacidad de ningún host dedicado configurado en el Outpost.

Unidad: porcentaje

Resolución máxima: 5 minutos

Estadísticas: las estadísticas más útiles son `Average` y `pNN.NN` (percentiles).

Dimensiones: y `InstanceFamily` `OutpostId`

`InstanceFamilyCapacityUtilization`

El porcentaje de capacidad de instancia en uso. Esta métrica no incluye la capacidad de ningún host dedicado configurado en el Outpost.

Unidad: porcentaje

Resolución máxima: 5 minutos

Estadísticas: las estadísticas más útiles son `Average` y `pNN.NN` (percentiles).

Dimensiones: `Account`, `InstanceFamily` y `OutpostId`

`InstanceTypeCapacityAvailability`

El porcentaje de capacidad de instancia disponible. Esta métrica no incluye la capacidad de ningún host dedicado configurado en el Outpost.

Unidad: porcentaje

Resolución máxima: 5 minutos

Estadísticas: las estadísticas más útiles son `Average` y `pNN.NN` (percentiles).

Dimensiones: `InstanceType` y `OutpostId`

`InstanceTypeCapacityUtilization`

El porcentaje de capacidad de instancia en uso. Esta métrica no incluye la capacidad de ningún host dedicado configurado en el Outpost.

Unidad: porcentaje

Resolución máxima: 5 minutos

Estadísticas: las estadísticas más útiles son `Average` y `pNN.NN` (percentiles).

Dimensiones: `Account`, `InstanceType` y `OutpostId`

`UsedInstanceType_Count`

El número de tipos de instancias que se utilizan actualmente, incluido cualquier tipo de instancia que utilicen los servicios gestionados, como Amazon Relational Database Service (Amazon RDS) o Equilibrador de carga de aplicación. Esta métrica no incluye la capacidad de ningún host dedicado configurado en el Outpost.

Unidad: recuento

Resolución máxima: 5 minutos

Dimensiones: `Account`, `InstanceType` y `OutpostId`

`AvailableInstanceType_Count`

El número de tipos de instancias disponibles. Esta métrica no incluye la capacidad de ningún host dedicado configurado en el Outpost.

Unidad: recuento

Resolución máxima: 5 minutos

Dimensiones: `InstanceType` y `OutpostId`

`AvailableReservedInstances`

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

Unidad: recuento

Resolución máxima: 5 minutos

Dimensiones: `InstanceType` y `OutpostId`

`UsedReservedInstances`

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

Unidad: recuento

Resolución máxima: 5 minutos

Dimensiones: `InstanceType` y `OutpostId`

`TotalReservedInstances`

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

Unidad: recuento

Resolución máxima: 5 minutos

Dimensiones: `InstanceType` y `OutpostId`

Dimensiones de métricas de Outpost

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

Dimensión	Descripción
`Account`	La cuenta o el servicio que utiliza la capacidad.
`InstanceFamily`	La familia de instancias.
`InstanceType`	El tipo de instancia.
`OutpostId`	El ID del Outpost.
`VolumeType`	El tipo de volumen EBS.
`VirtualInterfaceId`	El ID de la pasarela local o de la interfaz virtual (VIF) del enlace de servicio.
`VirtualInterfaceGroupId`	El ID del grupo de interfaces virtuales de la interfaz virtual (VIF) de la puerta de enlace local.

Vea CloudWatch las métricas de su puesto de avanzada

Puedes ver las CloudWatch métricas de tus balanceadores de carga mediante la CloudWatch consola.

Para ver las métricas mediante la consola CloudWatch

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

Para ver métricas mediante la AWS CLI

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

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

Para obtener las estadísticas de una métrica desde la AWS CLI

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

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

Registre las llamadas a la API de AWS Outposts con AWS CloudTrail.

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

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

AWS Outpostsinformación en CloudTrail

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

Para mantener un registro continuo de eventos en la cuenta de AWS, incluidos los eventos de AWS Outposts, cree un registro de seguimiento. Un registro permite CloudTrail entregar los archivos de registro a un bucket de S3 en el contenedor principalRegión de AWS. De manera predeterminada, cuando se crea un registro de seguimiento en la consola, el registro de seguimiento se aplica a todas las regiones de AWS. El registro de seguimiento registra los eventos de todas las regiones de la partición de AWS y envía los archivos de registro al bucket de S3 especificado. Además, puede configurar otros AWS servicios para analizar más a fondo los datos de eventos recopilados en los CloudTrail registros y actuar en función de ellos. Para más información, consulte los siguientes temas:

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

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

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

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

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

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

Un registro es una configuración que permite la entrega de eventos como archivos de registro a un bucket de S3 que usted especifique. CloudTrail Los archivos de registro contienen una o más entradas de registro. Un evento representa una única solicitud desde cualquier origen. Incluye información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud,

etc. CloudTrail Los archivos de registro no son un registro ordenado de las llamadas a las API públicas, por lo que no aparecen en ningún orden específico.

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


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

```
    "requestID": "1abcd23e-f4gh-567j-klm8-9np01q234r56",
    "eventID": "1234a56b-c78d-9e0f-g1h2-34jk56m7n890",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
```

Mantenimiento de un Outpost

Según el modelo de responsabilidad compartida 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 tu Outpost y determina si es necesario realizar algún tipo de mantenimiento.

> **Warning**
>
> Los datos de los volúmenes del almacén de instancias se pierden si la unidad de disco subyacente falla o si la instancia finaliza. Para evitar la pérdida de datos, le recomendamos que guarde copias de seguridad de los datos a largo plazo de los volúmenes del almacén de instancias en un almacenamiento persistente, como un bucket de Amazon S3, un o un dispositivo de almacenamiento en red de su red en las instalaciones.

Contenido

Mantenimiento del hardware

Si AWS detecta un problema irreparable con el hardware que aloja las instancias de Amazon EC2 que se ejecutan en su Outpost, notificaremos al propietario del Outpost y al propietario de las instancias 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 Outpost server installation.
- 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 AWS Outposts de energía y red

Como se indica en los Términos de AWS servicio para AWS Outposts los clientes, la instalación donde se encuentra el equipo de Outposts debe cumplir con los requisitos mínimos de energía y red para respaldar la instalación, el mantenimiento y el uso del equipo de Outposts. Un servidor de Outposts solo puede funcionar correctamente cuando la conectividad eléctrica y de red es ininterrumpida.

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 conmutar repetidamente las fuentes de alimentación (apagado - encendido - apagado-encendido) durante el mantenimiento.
- Prevea tiempo adicional dentro del período de mantenimiento para hacer frente a cualquier imprevisto.
- Gestione las expectativas de sus usuarios y clientes comunicando un plazo de mantenimiento más amplio del que normalmente necesitaría.

Eventos de conectividad de red

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

Si el enlace de servicio no funciona debido a un problema de energía in situ o a una pérdida de conectividad de red, AWS Health Dashboard envía una notificación a la cuenta propietaria de los Outposts. Ni tú ni tú AWS podéis suprimir la notificación de una interrupción del enlace de servicio, incluso si la interrupción es esperada. Para obtener más información, consulte Introducción a su AWS Health Dashboard en la Guía del usuario de AWS Health .

En el caso de un mantenimiento planificado del servicio que afecte a la conectividad de la red, tome las siguientes medidas proactivas para limitar el impacto de posibles escenarios problemáticos:

- Si 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 la herramienta de VPC AWSSupport -SetupIP. MonitoringFrom Esta herramienta es un documento de AWS Systems Manager (documento SSM) que crea una instancia de supervisión de Amazon EC2 en una subred especificada por usted, y supervisa las direcciones IP de destino. El documento ejecuta pruebas de diagnóstico de ruta de rastreo de ping, MTR, TCP y ruta de rastreo y almacena los resultados en Amazon CloudWatch Logs, que se pueden visualizar en un CloudWatch panel de control (por ejemplo, latencia o pérdida de paquetes). Para 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.

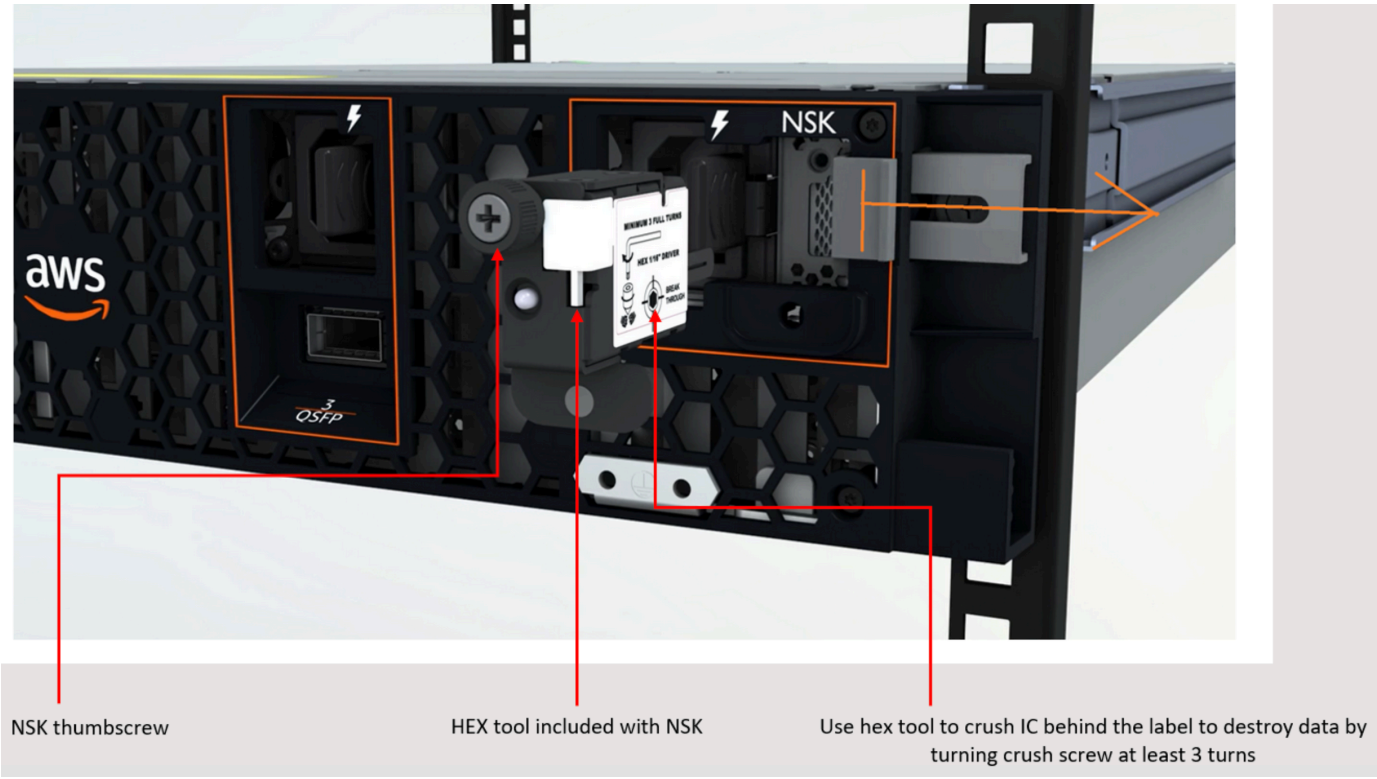
Destrucción criptográfica de los datos del servidor

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.



AWS Outposts end-of-term opciones

Al final de su AWS Outposts mandato, tiene tres opciones:

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

Temas

Renovar la suscripción

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

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

1. Inicie sesión en la consola del AWS Support Center.
2. Elija Crear caso.
3. Elija Cuenta y facturación.
4. Para Servicio, elija Facturación.
5. Para Categoría, elija Otras preguntas sobre facturación.
6. Para Severidad, elija Pregunta importante.
7. Elija Siguiente paso: información adicional.
8. En la página Información adicional, para Asunto, introduzca su solicitud de renovación, por ejemplo **`Renew my Outpost subscription`**.
9. En Descripción, introduzca una de las siguientes opciones de pago:
    - Sin pago inicial
    - Pago inicial parcial
    - Pago inicial total

Para ver los precios, consulte los precios de servidores de AWS Outposts. También puede solicitar una cotización.

10. Elija Siguiente paso: Resuelva ahora o póngase en contacto con nosotros.
11. En la página Contacte con nosotros, elija su idioma preferido.
12. Cambie el método de contacto preferido.
13. Revise los detalles de su caso y elija Enviar. Aparecerán el número de ID del caso y el resumen.

AWS Customer Support iniciará el proceso de renovación de la suscripción. La nueva suscripción comenzará el día siguiente a la finalización de la suscripción actual.

Si no indica que desea renovar su suscripción o devolver su servidor Outpost, pasará 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.

Finalice su suscripción y devuelva el servidor

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

Finalización de su suscripción:

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

1. Inicie sesión en la consola del AWS Support Center.
2. Elija Crear caso.
3. Elija Cuenta y facturación.
4. Para Servicio, elija Facturación.
5. Para Categoría, elija Otras preguntas sobre facturación.
6. Para Severidad, elija Pregunta importante.

7. Elija Siguiente paso: información adicional.
8. En la página Información adicional, para Asunto, introduzca su solicitud de renovación, por ejemplo **`End my Outpost subscription`**.
9. En Descripción, introduzca la fecha en la que desea finalizar la suscripción.
10. Elija Siguiente paso: Resuelva ahora o póngase en contacto con nosotros.
11. En la página Contacte con nosotros, elija su idioma preferido.
12. Cambie el método de contacto preferido.
13. Si es necesario, haz una copia de seguridad de las instancias y los datos de las instancias presentes en tu servidor.
14. Termine las instancias lanzadas en su servidor.
15. Revise los detalles de su caso y elija Enviar. Aparecerán el número de ID del caso y el resumen.
16. NO apague ni desconecte el servidor de la red hasta que se le indique lo contrario en el caso de soporte.

Para devolver el AWS Outposts servidor, siga los procedimientos de Devolución de un AWS Outposts servidor.

Conviértalo en una month-to-month suscripción

Para convertirlo en una month-to-month suscripción y conservar tu servidor Outpost actual, 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

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

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

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

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

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

AWS Outposts y las cuotas para otros servicios

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

Historial de documentos

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

Cambio	Descripción	Fecha
Administración de la capacidad	Puedes modificar la configuración de capacidad predeterminada para tu nuevo pedido de Outposts.	16 de abril de 2024
nd-of-term Opciones E para servidores AWS Outposts	Al final de su AWS Outposts período, puede renovar, finalizar o convertir su 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
Hosts dedicados activados AWS Outposts	Ahora, puede usar hosts dedicados en Outposts.	31 de mayo de 2022
Presentación de los servidores de Outpost	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.