Guía de usuario para servidores Outposts

AWS Outposts

AWS Outposts: Guía de usuario para servidores Outposts

Table of Contents

¿Qué es AWS Outposts?

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

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

> **Note**
>
> No puedes conectar un Outpost a otro Outpost o zona local que se encuentre dentro de la misma. VPC

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

Conceptos clave

Estos son los conceptos clave de. AWS Outposts

- Sitio de Outpost: los edificios físicos gestionados por el cliente donde se AWS instalará tu Outpost. Un sitio debe cumplir con los requisitos de instalaciones, redes y alimentación de su Outpost.
- Capacidad del Outpost: recursos informáticos y de almacenamiento disponibles en el Outpost. Puede ver y administrar la capacidad de su Outpost desde la consola de AWS Outposts .
- Equipo de Outpost: hardware físico que proporciona acceso al servicio. AWS Outposts El hardware incluye racks, servidores, conmutadores y cableado propiedad de y gestionados por. AWS
- Bastidores de Outposts: un factor de forma de Outpost que constituye un bastidor de 42U estándar del sector. Los racks Outposts incluyen servidores montables en bastidor, conmutadores, un panel de conexiones de red, un estante de alimentación y paneles vacíos.

- Servidores Outposts: un formato Outpost que es un servidor de 1U o 2U estándar del sector, que se puede instalar en un rack de 4 postes que cumple con la norma EIA -310D 19. Los servidores Outposts proporcionan servicios de computación y redes locales a sitios que tienen requisitos de espacio limitado o capacidad más pequeños.
- Propietario de Outpost: el propietario de la cuenta que realiza el AWS Outposts pedido. Tras AWS contactar con el cliente, el propietario puede incluir puntos de contacto adicionales. AWS se comunicará con los contactos para aclarar los pedidos, las citas de instalación y el mantenimiento y reemplazo del hardware. Póngase en contacto con el AWS Support Centro de contacto si la información de contacto cambia.
- Enlace de servicio: ruta de red que permite la comunicación entre su puesto de avanzada y AWS la región asociada. Cada Outpost es una extensión de una zona de disponibilidad y su región asociada.
- Puerta de enlace local (LGW): un enrutador virtual de interconexión lógica que permite la comunicación entre un rack de Outposts y la red local.
- Interfaz de red local: una interfaz de red que permite la comunicación entre un servidor de Outposts y tu red local.

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
EC2Instancias de Amazon	S	Sí
ECSClústeres de Amazon	S	Sí

Tipo de recurso	Bastidores	Servidores
EKSNodos de Amazon	S	No

Base de datos y análisis

Tipo de recurso	Bastidores	Servidores
ElastiCache Nodos de Amazon (clúster de Redis, clúster de Memcached)	S	No
EMRClústeres de Amazon	S	No
Instancias RDS de Amazon DB	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
VPCSubredes de Amazon	S	Sí
Amazon Route 53	S	No

Almacenamiento

Tipo de recurso	Bastidores	Servidores
EBSVolúmenes de Amazon	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

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

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

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

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

- Outposts publica precios
- Precios de los servidores Outposts

Cómo AWS Outposts funciona

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

El siguiente diagrama ilustra ambos factores de forma de Outpost.

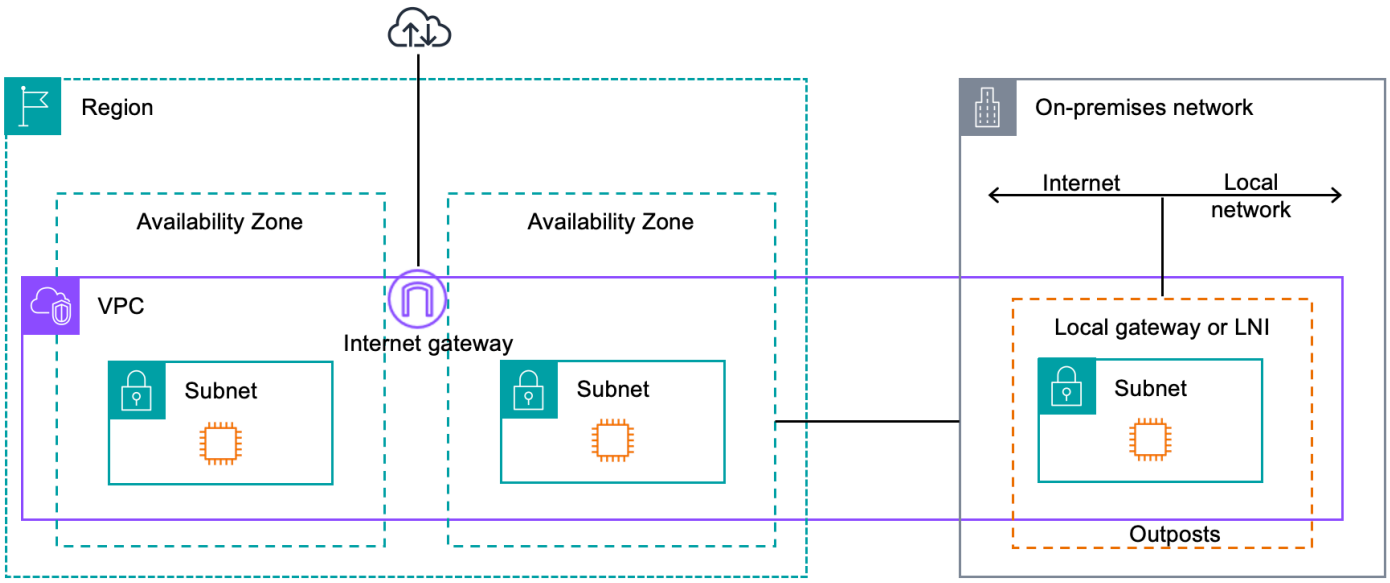
Contenido

Componentes de la red

AWS Outposts extiende un Amazon VPC de una AWS región a un puesto avanzado con VPC los componentes a los que se puede acceder en la región, incluidas las pasarelas de Internet, las pasarelas privadas virtuales, las pasarelas de Amazon VPC Transit y los puntos de conexión. 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 y una red local Región de AWS
- A VPC con varias 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)



VPCsy subredes

Una nube privada virtual (VPC) abarca todas las zonas de disponibilidad de su AWS región. Puedes extender cualquier parte de VPC la región a tu Outpost añadiendo una subred de Outpost. Para añadir una subred de Outpost aVPC, especifique el nombre de recurso de Amazon (ARN) del Outpost al crear la subred.

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

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

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

Enrutamiento

De forma predeterminada, cada subred de Outpost hereda la tabla de rutas principal de la suya. 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 rutas principal heredada o de una tabla personalizada, hereda la ruta local. VPC Esto significa que todo el tráfico de laVPC, incluida la subred de Outpost con un destino en la VPCCIDR, permanece enrutado en. VPC

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

- VPCCIDRrango: lo AWS define en la instalación. Esta es la ruta local y se aplica a todos los VPC enrutamientos, incluido el tráfico entre las instancias de Outpost de la mismaVPC.
- 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 peering. VPC

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

DNS

Para las interfaces de red conectadas a aVPC, EC2 las instancias de las subredes de Outposts pueden usar el DNS servicio Amazon Route 53 para convertir los nombres de dominio en direcciones IP. Route 53 admite DNS funciones como el registro de dominios, el DNS enrutamiento y las comprobaciones de estado para las instancias que se ejecutan en tu 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 AWS región. Por lo tanto, la conectividad de enlace de servicio desde el puesto de avanzada hasta la AWS región debe estar activa y en funcionamiento para que estas DNS funciones funcionen.

Es posible que encuentres tiempos de DNS resolución más largos con Route 53, según la latencia de la ruta entre tu puesto de avanzada y la AWS región. En esos casos, puede usar los DNS servidores instalados localmente en su entorno local. Para usar sus propios DNS servidores, debe crear conjuntos de DHCP opciones para DNS los servidores locales y asociarlos al. VPC También debe asegurarse de que haya conectividad IP con estos DNS servidores. Es posible que también necesites añadir rutas a la tabla de enrutamiento de la puerta de enlace local para que sean accesibles, pero esta solo es una opción para los racks de Outposts con puerta de enlace

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

El registro de consultas no es compatible con DNS las consultas 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 VPN conexiones que se utilizan siempre que el Outpost se comunica con la región de origen elegida. Usas un virtual LAN (VLAN) para segmentar el tráfico en el enlace de servicio. El enlace de servicio VLAN permite la comunicación entre el puesto de avanzada y la AWS región, tanto para la gestión del puesto de avanzada como para el VPC tráfico interno entre la AWS región y el puesto de avanzada.

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

Requisitos del sitio para los servidores de Outposts

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

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

Contenido

Instalación

Estos son los requisitos para la instalación de los servidores.

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

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

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

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

  Para ver los requisitos de peso de los distintos recursos de Outposts, selecciona Explorar el catálogo en la AWS Outposts consola en. https://console.aws.amazon.com/outposts/
- Compatibilidad con el kit de raíles: el kit de raíles 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 pulgadas compatible con la EIA -310-D. El kit de raíles no es compatible con un soporte de montaje en forma de U, como se muestra en la siguiente imagen.

- Colocación del estante: recomendamos el uso de bastidores EIA -310D estándar de 19 pulgadas, con una profundidad de al menos 36 pulgadas (914 mm). AWS incluye un kit de rieles para montar el servidor en rack.
  - 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)
  - 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

  Si no coloca el servidor en un rack, aún debe cumplir con los demás requisitos del sitio.
- Facilidad de mantenimiento: los servidores de Outposts se pueden reparar en el pasillo delantero.
- Acústica: tiene una potencia acústica nominal inferior a 78 dBA a temperaturas de 80 °F (27 °C) y cumple con la normativa CORE NEBS GR-63.
- 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+	Tráfico tanto de servicio como de LNI enlace: QSFP + un cable de conexión (10 pies/3 m) segmenta el tráfico.

Firewall del enlace de servicio

UDPy TCP 443 deben figurar correctamente 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	DHCPservidor proporcionado DNS
UDP	443, 1024-65535	IP del enlace de servicio	443	Puntos finales de Outposts Service Link
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 de Service Link () MTU

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

Recomendaciones de ancho de banda para el enlace de servicio

Para una experiencia y una resiliencia óptimas, AWS requiere que utilice una conectividad redundante de al menos 500 Mbps y una latencia máxima de ida y vuelta de 175 ms para la conexión del enlace de servicio a la AWS región. La utilización máxima de cada servidor de Outposts es de 500 Mbps. Para aumentar la velocidad de conexión, usa varios servidores Outposts. Por ejemplo, si tiene tres servidores de AWS Outposts , la velocidad máxima de conexión aumentará a 1,5 Gbps (1500 Mbps). Para obtener más información, consulte Tráfico de enlaces de servicio para servidores en la guía del AWS Outposts usuario de 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 AMI tamaño, la elasticidad de las aplicaciones, las necesidades de velocidad de ráfaga y el VPC tráfico de Amazon a la región. Tenga en cuenta que AWS Outposts los servidores no se almacenan en cachéAMIs. AMIsse descargan de la región con cada lanzamiento de una instancia.

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

El enlace de servicio requiere una DHCP respuesta

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

Latencia máxima del enlace de servicio

Los enlaces de servicio pueden admitir una latencia de red máxima de 175 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 rack.

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

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 una fuente de alimentación ininterrumpida (). UPS

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 Tráfico de enlaces de servicio para servidores en la guía del AWS Outposts usuario de servidores.

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

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

Tareas

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

Crear un Outpost y solicitar capacidad de Outpost

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

Requisitos previos

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

Tareas

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

Paso 1: crear un sitio

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

Requisitos previos

- Determine la dirección operativa.

Cómo crear un sitio

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

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

Requisitos previos

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

  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 Next (Siguiente).
6. Elija Utilizar un Outpost existente y seleccione el Outpost.
7. Elija Next (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 cuentas. AWS

10. Elija Next (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 JSON archivo.

Console steps

1. Seleccione Modificar una nueva configuración de capacidad de Outpost.

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

Example

JSONArchivo de ejemplo:

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

4. Revise el contenido del JSON archivo en la sección del plan de configuración de la capacidad.
5. Elija Next (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. Si tiene alguna pregunta sobre su pedido, póngase en contacto con AWS Support el Centro.

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. Ya sea que realices la instalación o contrates a un tercero, la instalación requiere IAM las credenciales Cuenta de AWS que contienen el Outpost para verificar la identidad del nuevo dispositivo. Usted es responsable de proporcionar y administrar este acceso. Para obtener más información, consulte la guía de instalación del servidor.

La instalación se completará cuando la EC2 capacidad de Amazon para tu Outpost esté disponible en tu Cuenta de AWS. Cuando la capacidad esté disponible, podrás lanzar EC2 instancias de Amazon en tu servidor de Outposts. Para obtener más información, consulte the section called "Iniciar una instancia".

Lanza una instancia en tu servidor de Outposts

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

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

Puedes añadir subredes de Outpost a cualquier parte de la VPC AWS región para el Outpost. Al hacerlo, 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 Cuenta de AWS persona ha compartido contigo, salta a. Paso 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 te redirigirá para crear una subred en la VPC consola de Amazon. Seleccionamos el Outpost y la zona de disponibilidad a la que está destinado el Outpost.
4. Seleccione VPC y especifique un rango de direcciones IP para la subred.
5. Seleccione Crear.
6. Una vez creada la subred, debe habilitarla para las interfaces de red locales. Utilice el comando modify-subnet-attribute desde la AWS CLI. Debe especificar la posición de la interfaz de red en el índice de dispositivos. Todas las instancias lanzadas en una subred de Outpost habilitada utilizan esta posición del dispositivo para las interfaces de red local. En el siguiente ejemplo, se utiliza el valor 1 para especificar una interfaz de red secundaria.

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

Paso 2: lanzar una instancia en el Outpost

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

Consideraciones

- Las instancias en los servidores de Outposts incluyen volúmenes de almacenes de instancias, pero no EBS volúmenes. Elija un tamaño de instancia con suficiente almacenamiento de instancias para cumplir con las necesidades de la aplicación. Para obtener más información, consulta Volúmenes de almacenes de instancias y Crear un almacén de instancias respaldado AMI en la Guía EC2del usuario de Amazon.
- Debes usar una EBS copia respaldada por Amazon AMI con una sola EBS instantánea. AMIscon más de una EBS instantánea no son compatibles.
- 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. Abra la AWS Outposts consola en https://console.aws.amazon.com/outposts/.
2. En el panel de navegación, elija Outposts.
3. Seleccione el Outpost y, a continuación, elija Acciones, Ver detalles.
4. En la página de Resumen de Outpost, seleccione Lanzar instancia. Se le redirigirá al asistente de lanzamiento de instancias en la EC2 consola de Amazon. 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 especificaste 1 como índice de dispositivos de interfaz de red local para la subred de Outpost, esta interfaz de red es la interfaz de red local de la instancia. Como alternativa, para añadirla más adelante, consulte. Agregue una interfaz de red local
7. Complete el asistente para lanzar la instancia en la subred del Outpost. Para obtener más información, consulta Cómo lanzar una EC2 instancia en la Guía del EC2 usuario de Amazon:

Paso 3: configurar la conectividad

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

Debe configurar la interfaz de red local de la instancia con una dirección IP de la red local. Normalmente, esto se hace medianteDHCP. 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 cómo conectarse a una EC2 instancia, consulta Conéctate a tu EC2 instancia en la Guía del EC2 usuario de Amazon.

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

```
ping 172.16.0.130
```

A continuación, se muestra un ejemplo del resultado.

```
Pinging 172.16.0.130

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

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

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

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

   ```
   ping 10.0.1.5
   ```

A continuación, se muestra un ejemplo del resultado.

```
Pinging 10.0.1.5

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

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

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

AWS Outposts conectividad con las AWS regiones

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

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

Contenido

Conectividad a través del enlace de servicio

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

El Outpost puede crear el enlace de servicio con la Región a través de la VPN conectividad pública de la AWS Región. 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 AWS Direct Connect pública. Esta conectividad puede realizarse a través de rutas específicas en el enlace VLAN 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.
- El tráfico entre el Outpost y cualquier dispositivo asociadoVPCs, incluido el tráfico del plano de datos de los clientes.

Requisitos de unidad máxima de transmisión del enlace de servicio MTU

La unidad de transmisión máxima (MTU) de una conexión de red es el tamaño, en bytes, del paquete más grande permitido que se puede pasar a través de la conexión. La red debe admitir 1500 bytes MTU entre los puntos finales de Outpost y de enlace de servicio en la región principal. AWS Para obtener información sobre los requisitos MTU entre una instancia de Outpost y una instancia de la AWS región a través del enlace de servicio, consulta la unidad máxima de transmisión de red (MTU) para tu EC2 instancia de Amazon en la Guía del EC2 usuario de Amazon.

Recomendaciones de ancho de banda para el enlace de servicio

Para una experiencia y una resiliencia óptimas, AWS requiere que utilices una conectividad redundante de al menos 500 Mbps y una latencia máxima de ida y vuelta de 175 ms para la conexión del enlace de servicio a la región. AWS La utilización máxima de cada servidor de Outposts es de 500 Mbps. Para aumentar la velocidad de conexión, usa varios servidores Outposts. Por ejemplo, si tiene tres AWS Outposts servidores, la velocidad máxima de conexión aumentará a 1,5 Gbps (1500 Mbps). Para obtener más información, consulte Tráfico de enlaces 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 AMI tamaño, la elasticidad de las aplicaciones, las necesidades de velocidad de ráfaga y el VPC tráfico de Amazon a la región. Tenga en cuenta que AWS Outposts los servidores no se almacenan en cachéAMIs. AMIsse descargan de la región con cada lanzamiento de una instancia.

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

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 Amazonía VPC desde la AWS región hasta el puesto avanzado. Una interfaz virtual AWS Direct Connect pública es la conexión de enlace de servicio. El siguiente tráfico pasa por el enlace de servicio y la conexión de AWS Direct Connect :

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

Si utiliza un firewall activo con su conexión a Internet para limitar la conectividad de la Internet pública al enlace de servicioVLAN, puede bloquear todas las conexiones entrantes que se inicien desde Internet. Esto se debe a que el enlace de servicio VPN se inicia únicamente desde el puesto de avanzada a la región, no desde la región al puesto de avanzada.

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

Protocolo	Puerto de origen	Dirección de origen	Puerto de destino	Dirección de destino
UDP	1024 - 65535	IP del enlace de servicio	53	DHCPDNSservidor proporcionado
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 Outposts. 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 tu servidor de Outposts y su región principal AWS . Esta conexión de red, denominada enlace de servicio, es esencial para gestionar el puesto de avanzada, ya que proporciona VPC tráfico interno entre el puesto de avanzada 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 produzcan breves períodos de latencia y pérdida de paquetes en esta red, lo que repercute en las cargas de trabajo que dependen de la VPC conectividad con los recursos alojados en la región. Sin embargo, el tráfico que atraviesa las interfaces de la red local (LNI) no se verá afectado. Puedes evitar el impacto en tu aplicación si sigues las mejores prácticas de AWS Well-Architected y te aseguras de que tus aplicaciones sean resistentes a los fallos o a las actividades de mantenimiento que afecten a un único servidor de Outposts.

Conexiones de Internet redundantes

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

Devolver un servidor de Outposts

Si AWS Outposts detectas un defecto en el servidor, te avisaremos, iniciaremos el proceso de sustitución para enviarte un nuevo servidor y te proporcionaremos la etiqueta de envío a través de la AWS Outposts consola. Para empezar, sigue estos pasos.

Tareas

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

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

Paso 1: Prepare el servidor para la devolución

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

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

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

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

   Para ver la lista de recursos de Outpost que se pueden compartir, consulte Recursos de Outpost que se pueden compartir.
2. Cree copias de seguridad de los datos almacenados en el almacenamiento de instancias de las EC2 instancias de Amazon que se ejecutan en el AWS Outposts servidor.
3. Elimine las interfaces de red locales asociadas a las instancias que se estaban ejecutando en el servidor.

4. Finalice las instancias activas asociadas a las subredes de su Outpost. Para finalizar las instancias, sigue las instrucciones de Termina tu instancia en la Guía del EC2 usuario de Amazon.

Paso 2: Obtenga la etiqueta de envío de devolución

> **Important**
>
> Solo debes usar la etiqueta de envío que se AWS proporciona porque contiene información específica, como el identificador del producto, sobre el servidor al que vas a devolver. 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.

Paso 3: Empaque el servidor

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

1. Empaque el servidor en una de las siguientes cajas:
   - La caja y el material de embalaje en los que venía originalmente el servidor.
   - La caja y el material de embalaje en los que venía el servidor de reemplazo.

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

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

> **Important**
>
> Comprueba que el identificador del artículo de la etiqueta de envío coincide con el identificador del artículo del servidor al que vas a devolver.
> El identificador del activo se encuentra en la pestaña desplegable situada en la parte frontal del servidor. Ejemplo: `1203779889` o `9305589922`

3. Sella bien la caja.

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

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

País	Contacto
Hong Kong	
India	
Indonesia	
Japón	
Malasia	
Nigeria	
Omán	
Panamá	
Perú	
Filipinas	
Serbia	
Singapur	
Sudáfrica	
Corea del Sur	
Taiwán	
Tailandia	
Emiratos Árabes Unidos	
Vietnam	

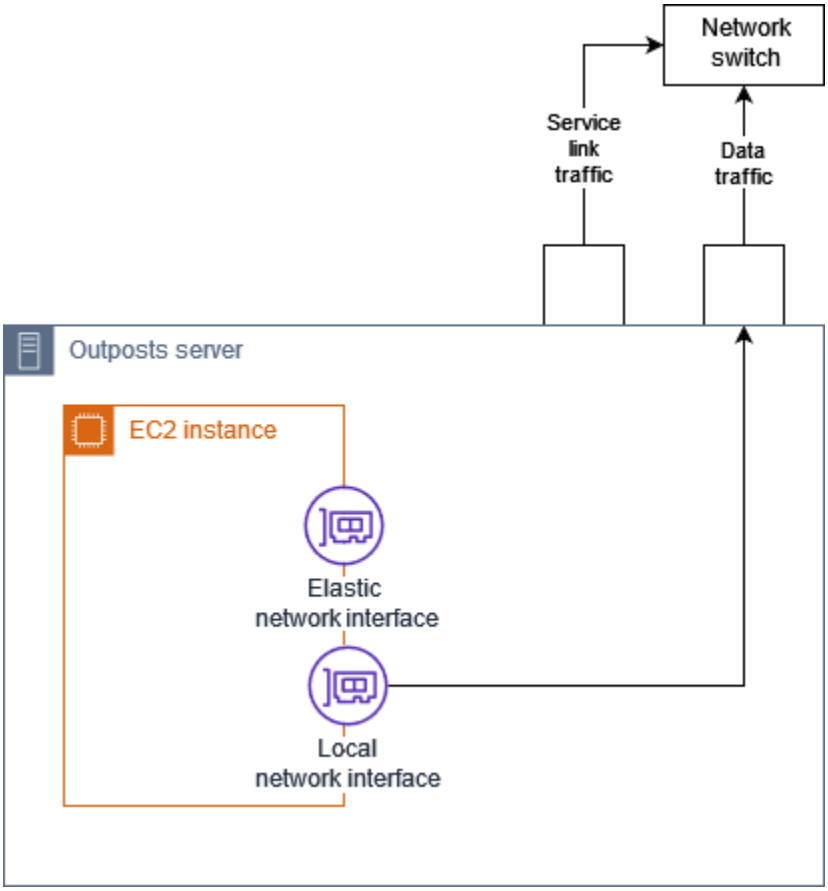
País	Contacto
Estados Unidos de América	Contacto UPS. Puede devolver el servidor mediante alguna de las siguientes formas: • Devuelva el servidor durante una UPS recogida rutinaria en su sitio. • Deja el servidor en una UPSubicación. • Programar una recogida para la fecha y hora que prefiera. Introduzca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

Interfaces de red local para tus servidores Outposts

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

Después de habilitar las interfaces de red local en una subred de Outpost, puede configurar las EC2 instancias de la subred de Outpost para que incluyan una interfaz de red local además de la interfaz de red elástica. La interfaz de red local se conecta a la red local, mientras que la interfaz de red se conecta a. VPC El siguiente diagrama muestra una EC2 instancia 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 puedes usar los conjuntos de DHCP opciones de VPC a para configurar una interfaz de red local porque una interfaz de red local se ejecuta en tu 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 VPC red para acceder a los puntos finales regionales públicos Servicios de AWS, o puede usar los VPC puntos finales de la interfaz para acceder Servicios de AWS mediante. 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. A VPC es una red virtualizada de capa tres. Las interfaces de red local no admiten VPC componentes de red. Estos componentes incluyen grupos de seguridad, listas de control de acceso a la red, enrutadores virtualizados o tablas de enrutamiento y registros de flujo. La interfaz de red local no proporciona al servidor de Outposts visibilidad de los flujos de VPC capa tres. 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

- Soporte ARP y protocolos de interfaces de red locales. 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 más información, consulte Cuotas de interfaz de red en la Guía del VPC usuario de Amazon.
- Cada EC2 instancia puede tener una interfaz de red local.
- Una interfaz de red local no puede usar la interfaz de red principal de la instancia.

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

> **Note**
>
> EC2las instancias dentro del mismo servidor pueden comunicarse directamente sin enviar datos fuera del servidor de Outposts. Esta comunicación incluye el tráfico a través de una interfaz de red local o de interfaces de red elásticas.

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

Rendimiento

La interfaz de red local de cada tamaño de instancia proporciona una parte del ancho de banda físico disponible de 10 GbE. En la siguiente tabla, se muestra el rendimiento de la red para cada tipo de instancia:

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

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

Grupos de seguridad

Por diseño, la interfaz de red local no utiliza grupos de seguridad en suVPC. Un grupo de seguridad controla el tráfico entrante y salienteVPC. La interfaz de red local no está conectada al. 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, consulta Supervisar el rendimiento de la red para ver la ENA configuración de tu EC2 instancia en la Guía del EC2 usuario de Amazon.

MACdirecciones

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

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

Añadir una interfaz de red local a una EC2 instancia de una subred de Outposts

Puedes añadir una interfaz de red local a una EC2 instancia de Amazon 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 especificaste al habilitar la subred Outpost para las interfaces de red locales, puedes especificar el índice de dispositivos correcto utilizando o an en su lugar. AWS CLI AWS SDK Por ejemplo, utilice los siguientes comandos de AWS CLI: create-network-interfacey. attach-network-interface

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

Para añadir una interfaz de red local a una instancia EC2

1. Abre la EC2 consola de Amazon en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Red y seguridad y, a continuación, Interfaces de red.
3. Crear la interfaz de red
    a. Elija Crear interfaz de red.
    b. Seleccione la misma subred de Outpost que la instancia.
    c. Comprueba que la IPv4dirección privada esté configurada para asignarse automáticamente.
    d. Seleccione cualquier grupo de seguridad. Los grupos de seguridad no se aplican a la interfaz de red local, por lo que el grupo de seguridad que seleccione no es relevante.
    e. Elija Crear interfaz de red.
4. Asociar una interfaz de red a una instancia

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

b. Elija Acciones, Asociar.

c. Seleccione la instancia.

d. Elija Asociar. El índice de dispositivo está asociado al índice de dispositivos 1. Si especificó 1 como índice de dispositivos para la interfaz de red local de la subred Outpost, 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, puedes usar la EC2 consola de Amazon para ver tanto la interfaz de red elástica como la interfaz de red local de las instancias de tu subred de Outpost. Seleccione la instancia y haga clic en la pestaña Red.

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

Configuración del sistema operativo

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

Conectividad de red local para servidores Outposts

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

Contenido

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

Topología del servidor de su red

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

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

Etiqueta de tráfico	Descripción
2	Tráfico de enlace de servicio: este tráfico permite la comunicación entre el puesto de avanzada y la AWS región, tanto para la gestión del puesto de avanzada como para el VPC tráfico interno 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 personalizado VPN o va VPNs desde el puesto de avanzada 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 interfaz de red local: este tráfico permite la comunicación entre el usuario y el local VPC a LAN través de la interfaz de red local. El tráfico de enlaces locales incluye las instancias que se ejecutan en el Outpost y que se comunican con la red en las

Etiqueta de tráfico	Descripción
	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 Outposts incluye no redundantes. Los puertos tienen sus propios requisitos de velocidad y conector, tal como se indica a continuación:

- 10 GbE: tipo de conector + QSFP

QSFP+ cable

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

Tráfico de enlace de servicio para servidores

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

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

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

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

- TCP443

- UDP443
- UDP53

Velocidad de enlace ascendente

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

Es posible que necesite un enlace ascendente más rápido en función del enlace de interfaz de red local y del uso del enlace de servicio. Para obtener más información, consulte Recomendaciones de ancho de banda para enlaces de servicios.

Tráfico de enlace de interfaz de red local

Configure el puerto de enlace de la interfaz de red local de su dispositivo de red ascendente como un puerto de acceso estándar a un puerto VLAN de su red local. Si tiene más de unoVLAN, configure todos los puertos del dispositivo de red ascendente como puertos troncales. Configure el puerto de su dispositivo de red ascendente para que espere varias MAC direcciones. Cada instancia lanzada en el servidor utilizará una MAC dirección. Algunos dispositivos de red ofrecen funciones de seguridad de puertos que desactivan un puerto que informa de varias MAC direcciones.

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

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

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

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

```
modinfo 8021q
```

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

2. Cree el VLAN dispositivo. En este ejemplo:

   - El nombre de la interfaz de red local es `ens6`
   - El VLAN identificador es `59`
   - El nombre asignado al VLAN dispositivo 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 la subred es 192.168.59.0/24. CIDR

```
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 de VLAN etiquetado 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 necesitas asignaciones de direcciones IP públicas para los servidores de Outposts.

El protocolo de control dinámico de host (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 Outposts, puedes usar DHCP dos formas:

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

Para el enlace de servicio, los servidores de Outposts DHCP suelen conectarse a la red local. DHCPdebe devolver los servidores de DNS nombres y una puerta de enlace predeterminada. Los servidores Outposts no admiten la asignación de IP estática del enlace de servicio.

Para el enlace de la interfaz de red local, DHCP utilícelo para configurar las instancias que se conectarán a la red local. Para obtener más información, consulte the section called “Configuración del sistema operativo”.

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

Registro del servidor

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

Comparta sus AWS Outposts recursos

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

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

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

Un propietario de Outpost puede compartir recursos de Outpost con:

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

Contenido

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

Recursos de Outpost compartibles

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

Estos son los recursos disponibles para los servidores de Outposts . Para ver los recursos del rack de Outposts, consulta Cómo trabajar con AWS Outposts recursos compartidos en la Guía del AWS Outposts usuario de los racks de Outposts.

- Hosts dedicados asignados: los consumidores con acceso a este recurso pueden:
  - Lance y ejecute EC2 instancias en un host dedicado.
- Outposts: los consumidores con acceso a este recurso pueden:
  - Crear y administrar una subred en el Outpost.
  - AWS Outposts APIUtilícela para ver información sobre el puesto de avanzada.
- 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 EC2 instancias en subredes.

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

Requisitos previos para compartir recursos de Outposts

- Para compartir un recurso de Outpost con tu organización o unidad organizativa AWS Organizations, debes habilitar el uso compartido con. AWS Organizations Para obtener más

información, consulte Habilitar el uso compartido con AWS Organizations en la Guía del usuario de AWS RAM .

- Para compartir un recurso de Outpost, debes tenerlo en tu AWS cuenta. No puedes compartir un recurso de Outpost que se haya compartido contigo.
- Para compartir un recurso de Outpost, debe compartirlo con una cuenta que se encuentre dentro de la organización.

Servicios relacionados

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

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

Uso compartido entre zonas de disponibilidad

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

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

Para ver la zona de disponibilidad IDs de las zonas de disponibilidad de su cuenta

1. Abra la AWS RAM consola en https://console.aws.amazon.com/ram.
2. Las AZ IDs de la región actual se muestran en el panel Tu ID de AZ, en la parte derecha de la pantalla.

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

Uso compartido de un recurso de Outpost

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

Para compartir un recurso de Outpost, debe agregarlo al recurso compartido. Un recurso compartido es un AWS RAM recurso que te permite compartir tus recursos entre AWS cuentas. Un uso compartido de recursos especifica los recursos que compartir y los consumidores con quienes se comparten. Cuando 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 formas parte de una organización AWS Organizations y el uso compartido dentro de tu organización está activado, puedes conceder a los consumidores de tu organización acceso desde la AWS RAM consola al recurso de Outpost compartido. De lo contrario, los consumidores reciben una invitación para unirse al recurso compartido y se les concede acceso al recurso de Outpost compartido al aceptar la invitación.

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

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

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

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

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

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

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

Usa el create-resource-sharecomando.

Dejar de compartir un recurso de Outpost compartido

Cuando un Outpost compartido deja de estar compartido, los consumidores ya no pueden verlo en la consola. AWS Outposts No pueden crear nuevas subredes en Outpost, crear nuevos EBS volúmenes en Outpost ni ver los detalles y los tipos de instancias de Outpost mediante la consola o el. AWS Outposts 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 rutas de una puerta de enlace local compartida deja de compartirse, los consumidores ya no pueden crear nuevas asociaciones con ella. VPC Todas las VPC asociaciones existentes que hayan creado los consumidores permanecen asociadas a la tabla de rutas. Los recursos incluidos en ellas VPCs 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. Puede hacerlo mediante la AWS RAM consola o el AWS CLI.

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

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

Para dejar de compartir un recurso de Outpost compartido de tu propiedad mediante el AWS CLI

Usa el comando. disassociate-resource-share

Identificación de un recurso de Outpost compartido

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

Para identificar un Outpost compartido mediante la consola AWS Outposts

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

Para identificar un recurso de Outpost compartido mediante el AWS CLI

Utilice los comandos list-outposts y -tables. describe-local-gateway-route 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. Se pueden usar AWS Organizations para ver, modificar y eliminar los recursos que los consumidores crean en los Outposts compartidos.

Permisos de los consumidores

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

Facturación y medición

A los propietarios se les cobran los Outposts y los recursos de Outpost que comparten. También se les facturará cualquier cargo de transferencia de datos asociado con el VPN tráfico de enlaces de servicio de su 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 VPC propietario los recursos de VPC nivel básico, como VPN las conexiones, las NAT pasarelas AWS Direct Connect y las conexiones de enlace privado.

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

Limitaciones

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

- Las limitaciones de las subredes compartidas se aplican al AWS Outposts uso compartido. Para obtener más información sobre los límites de VPC uso compartido, 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 los FAQ AWS Outposts servidores en FAQ.

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 los datos, consulte la sección Privacidad de datos FAQ. Para obtener información sobre la protección de datos en Europa, consulte el modelo de responsabilidad AWS compartida y la entrada del GDPR blog sobre AWS seguridad.

Cifrado en reposo

Con AWS Outposts, todos los datos en reposo se cifran. El material clave está empaquetado en una clave externa almacenada en un dispositivo extraíble, la clave de seguridad Nitro (NSK). NSKEs necesario para descifrar los datos de tu servidor rack de .

Cifrado en tránsito

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

Eliminación de datos

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

Al destruir la clave de seguridad Nitro, los datos de su Outpost se destruyen criptográficamente. Para obtener más información, consulte Destrucción criptográfica de los datos del servidor.

Administración 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 AWS los recursos. IAMlos administradores controlan quién puede autenticarse (iniciar sesión) y quién está autorizado (tiene permisos) para usar AWS Outposts los recursos. Puede utilizarlos IAM sin coste adicional.

Contenido

Cómo AWS funciona Outposts con IAM

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

IAMfunciones que puedes usar con AWS Outposts

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

IAMcaracterística	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 la identidad son documentos de política de JSON permisos que puede adjuntar a una identidad, como un IAM usuario, 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 información sobre cómo crear una política basada en la identidad, consulte Creación de IAM políticas en la Guía del usuario. IAM

Con las políticas IAM basadas en la identidad, 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 obtener más información sobre todos los elementos que puede utilizar en una JSON política, consulte la referencia sobre los elementos de la IAM JSON política en la Guía del IAMusuario.

Ejemplos de políticas basadas en identidad para Outposts AWS

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

Políticas basadas en recursos dentro de Outposts AWS

Admite políticas basadas en recursos: no

Las políticas basadas en recursos son documentos de JSON política que se adjuntan a un recurso. Algunos ejemplos de políticas basadas en recursos son las políticas de confianza de IAM roles 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 principales pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Para habilitar el acceso entre cuentas, puede especificar una cuenta completa o IAM entidades de otra cuenta como principales en una política basada en 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 IAM administrador de la cuenta de confianza también debe conceder permiso a la entidad principal (usuario o rol) 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 obtener más información, consulte Acceso a recursos entre cuentas IAM en la Guía del IAM usuario.

Acciones políticas para AWS Outposts

Compatibilidad con las acciones de política: sí

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

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

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

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

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

```
outposts
```

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

```
"Action": [
```

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

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

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

Recursos de políticas para AWS Outposts

Compatibilidad con los recursos de políticas: sí

Los administradores pueden usar AWS JSON políticas 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` JSON de política especifica el objeto o los objetos a los que se aplica la acción. Las instrucciones deben contener un elemento `Resource` o `NotResource`. Como práctica recomendada, especifique un recurso mediante su 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 API acciones AWS de Outposts admiten varios recursos. Para especificar varios recursos en una sola sentencia, sepárelos ARNs con comas.

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

Para ver una lista de los tipos de recursos de AWS Outposts y sus tiposARNs, consulta los tipos de recursos definidos AWS Outposts en la Referencia de autorización de servicio. Para saber con qué acciones puede especificar cada recurso, consulte Acciones definidas por AWS Outposts. ARN

Claves condicionales de la política para AWS Outposts

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

Los administradores pueden usar AWS JSON políticas 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 a un IAM usuario permiso para acceder a un recurso solo si está etiquetado con su nombre de IAM usuario. Para obtener más información, consulte los elementos de IAM política: variables y etiquetas en la Guía del IAM usuario.

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 IAMusuario.

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

ACLsen AWS Outposts

SoportesACLs: No

Las listas de control de acceso (ACLs) controlan qué directores (miembros de la cuenta, usuarios o roles) tienen permisos para acceder a un recurso. ACLsson similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de JSON políticas.

ABACcon AWS Outposts

Soportes ABAC (etiquetas en las políticas): Sí

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

ABACes útil en entornos de rápido crecimiento y ayuda en situaciones en las que la administración de políticas se vuelve 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 al respectoABAC, consulte ¿Qué es? ABAC en la Guía IAM del usuario. Para ver un tutorial con los pasos de configuraciónABAC, consulte Usar el control de acceso basado en atributos (ABAC) en la Guía del IAMusuario.

Uso de credenciales temporales con AWS Outposts

Compatibilidad con credenciales temporales: sí

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

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

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

Permisos principales entre servicios para Outposts AWS

Admite sesiones de acceso directo (FAS): Sí

Cuando utilizas un IAM usuario o un rol para realizar acciones en AWSél, se te considera director. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. FASutiliza los permisos del principal que llama a una Servicio de AWS y los solicita Servicio de AWS para realizar solicitudes a los servicios descendentes. FASlas solicitudes 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 detalles sobre la política a la hora de realizar FAS solicitudes, consulte Reenviar sesiones de acceso.

Roles de servicio para AWS Outposts

Compatible con roles de servicio: No

Una función de servicio es una IAMfunción que un servicio asume para realizar acciones en su nombre. Un IAM administrador puede crear, modificar y eliminar un rol de servicio desde dentroIAM. Para obtener más información, consulte Crear un rol para delegar permisos Servicio de AWS en un rol en el IAMManual del usuario.

Funciones vinculadas al servicio para Outposts AWS

Admite 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 IAM administrador puede ver los permisos de los roles vinculados al servicio, pero no editarlos.

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

AWS Ejemplos de políticas de Outposts

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

Para obtener información sobre cómo crear una política IAM basada en la identidad mediante estos documentos de JSON política de ejemplo, consulte Creación de IAM políticas en la Guía del IAMusuario.

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

Contenido

Prácticas recomendadas sobre las políticas

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

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos: para empezar a conceder permisos a sus usuarios y cargas de trabajo, utilice las políticas AWS administradas que otorgan permisos para muchos casos de uso comunes. Están disponibles en su. Cuenta de AWS Le recomendamos que reduzca aún más los permisos definiendo políticas administradas por el AWS cliente que sean específicas para sus casos de uso. Para obtener más información, consulte las políticas AWS gestionadas o las políticas AWS gestionadas para las funciones laborales en la Guía del IAM usuario.
- Aplique permisos con privilegios mínimos: cuando establezca permisos con IAM políticas, 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. Para obtener más información sobre cómo IAM aplicar permisos, consulte Políticas y permisos IAM en la IAM Guía del usuario.

- Utilice las condiciones en IAM las políticas para restringir aún más el acceso: puede añadir una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puede escribir una condición de política para especificar que todas las solicitudes deben enviarse medianteSSL. 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 los elementos IAM JSON de la política: Condición en la Guía del IAM usuario.
- Utilice IAM Access Analyzer para validar sus IAM políticas y garantizar permisos seguros y funcionales: IAM Access Analyzer valida las políticas nuevas y existentes para que se ajusten al lenguaje de las políticas (JSON) y IAM a las IAM mejores prácticas. IAMAccess Analyzer proporciona más de 100 comprobaciones de políticas y recomendaciones prácticas para ayudarle a crear políticas seguras y funcionales. Para obtener más información, consulte la validación de políticas de IAM Access Analyzer en la Guía del IAM usuario.
- Requerir autenticación multifactorial (MFA): si se encuentra en una situación en la que se requieren IAM usuarios o un usuario raíz Cuenta de AWS, actívela MFA para aumentar la seguridad. Para solicitarlo MFA cuando se convoque a API las operaciones, añada MFA condiciones a sus políticas. Para obtener más información, consulte Configuración del API acceso MFA protegido en la Guía del IAM usuario.

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

Ejemplo: uso de permisos de nivel de recursos

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

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

```
}
```

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

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

Funciones vinculadas al servicio para AWS Outposts

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

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

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

Permisos de rol vinculados al servicio para AWS Outposts

AWS Outposts utiliza el rol vinculado al servicio denominado _ AWSServiceRoleForOutposts***OutpostID***— Permite a Outposts acceder a AWS los 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 AWSServiceRoleForOutposts _*OutpostID* el rol vinculado al servicio confía en los siguientes servicios para asumir el rol:

- `outposts.amazonaws.com`

El _ AWSServiceRoleForOutposts***OutpostID***la función vinculada al servicio 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`

El AWSOutpostsPrivateConnectivityPolicy _***OutpostID***la política AWS Outposts permite 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 los permisos para permitir que una IAM entidad (como un usuario, un grupo o un rol) cree, edite o elimine un rol vinculado a un servicio. Para obtener más información, consulte los permisos de los roles vinculados a un servicio en la Guía del usuario. IAM

Cree un rol vinculado a un servicio para AWS Outposts

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

Edita un rol vinculado a un servicio para AWS Outposts

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

Elimine un rol vinculado a un servicio para AWS Outposts

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

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

Debes eliminar tu Outpost antes de poder eliminar el _ AWSServiceRoleForOutposts*OutpostID* rol vinculado a un servicio.

Antes de empezar, asegúrate de que tu Outpost no se comparta mediante 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.

Para eliminar manualmente el rol vinculado al servicio mediante IAM

Para obtener más información, consulte Eliminar un rol vinculado a un servicio en la Guía del usuario. IAM

Regiones compatibles para AWS Outposts los roles vinculados al servicio

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

AWS políticas gestionadas para AWS Outposts

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

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

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

Para obtener más información, consulte las políticas AWS administradas en la Guía del IAM usuario.

AWS política gestionada: AWSOutpostsServiceRolePolicy

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

AWS política gestionada: AWSOutpostsPrivateConnectivityPolicy

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

AWS política gestionada: AWSOutpostsAuthorizeServerPolicy

Usa esta política para conceder los permisos necesarios para autorizar el hardware del servidor de Outposts en tu red local.

Esta política incluye los siguientes permisos.

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

AWS Outposts actualiza las políticas gestionadas AWS

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

Cambio	Descripción	Fecha
AWSOutpostsAuthorizeServerPolicy—Nueva política	AWS Outposts agregó una política que otorga permisos para autorizar el hardware del	4 de enero de 2023

Cambio	Descripción	Fecha
	servidor de Outposts en tu red local.	
AWS Outposts comenzó a rastrear los cambios	AWS Outposts comenzó a rastrear los cambios en sus políticas AWS gestionadas.	03 de diciembre de 2019

Seguridad de la infraestructura en AWS Outposts

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

Usas API las llamadas 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). Necesitamos TLS 1.2 y recomendamos TLS 1.3.
- Cifre suites con perfecto secreto (PFS), como (Ephemeral Diffie-Hellman) o DHE 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 firmarse con un identificador de clave de acceso y una clave de acceso secreta asociada a un director. IAM También puede utilizar AWS Security Token Service (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.

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

VPCLos registros de flujo 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 está 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 API llamadas, supervisar el puesto de avanzada y actualizar el puesto de avanzada. 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 AmazonEBS. 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.
- Diseñando una arquitectura basada en la HIPAA seguridad y el cumplimiento en Amazon Web Services: en este documento técnico se describe cómo pueden utilizar las empresas AWS para crear HIPAA aplicaciones aptas.

  > **Note**
  >
  > No todos son aptos. Servicios de AWS HIPAA Para obtener más información, consulta la Referencia de servicios HIPAA aptos.

- 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. En las guías se resumen las mejores prácticas para garantizar la seguridad Servicios de AWS y se orientan a 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, por ejemplo PCIDSS, cumpliendo 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 consumo para simplificar la gestión del riesgo y el cumplimiento de las normativas y los estándares del sector.

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

CloudWatch métricas

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

CloudTrail registros

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

Los CloudTrail registros contienen información sobre las llamadas a la API acción de AWS Outposts. También contienen información sobre las llamadas a la API acción de los servicios de un Outpost, como Amazon EC2 y AmazonEBS. Para obtener más información, consulte APIRegistra llamadas usando CloudTrail.

Registros de flujo de VPC

Usa los registros de VPC flujo para recopilar información detallada sobre el tráfico que entra y sale de tu puesto de avanzada y dentro de tu puesto de avanzada. Para obtener más información, consulta VPCFlow Logs en la Guía del VPC usuario de Amazon.

Replicación de tráfico

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

AWS Health Dashboard

AWS Health Dashboard Muestra información y notificaciones iniciadas por cambios en el estado de AWS los recursos. La información se presenta de dos formas: en un panel donde se muestran los eventos recientes y próximos organizados por categorías, y en un registro de eventos que contiene todos los eventos de los últimos 90 días. Por ejemplo, un problema de conectividad en el enlace del servicio iniciaría un evento que aparecería en el panel y en el registro de eventos,

y permanecería en el registro de eventos durante 90 días. Como parte del AWS Health servicio, no AWS Health Dashboard requiere configuración y puede verlo cualquier usuario que esté autenticado en su cuenta. Para obtener más información, consulte Introducción a AWS Health Dashboard.

CloudWatch

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

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

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

Contenido

Métricas

El espacio de 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 (RDSAmazon) o Application Load Balancer. Esta métrica no incluye la capacidad de ningún host dedicado configurado en el Outpost.

Unidad: recuento

Resolución máxima: 5 minutos

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

`AvailableInstanceType_Count`

El número de tipos de instancias disponibles. Esta métrica incluye el `AvailableReservedInstances` recuento.

Para determinar el número de instancias que puede reservar, reste el `AvailableReservedInstances` recuento del `AvailableInstanceType_Count` recuento.

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

Esta métrica no incluye la capacidad de ningún host dedicado configurado en el Outpost.

Unidad: recuento

Resolución máxima: 5 minutos

Dimensiones: `InstanceType` y `OutpostId`

`AvailableReservedInstances`

El número de instancias que están disponibles para su lanzamiento en la capacidad de cómputo reservada mediante las reservas de capacidad.

Esta métrica no incluye las instancias EC2 reservadas de Amazon.

Esta métrica no incluye el número de instancias que puede reservar. Para determinar cuántas instancias puede reservar, reste el `AvailableReservedInstances` recuento del `AvailableInstanceType_Count` recuento.

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

Unidad: recuento

Resolución máxima: 5 minutos

Dimensiones: `InstanceType` y `OutpostId`

`UsedReservedInstances`

El número de instancias que se ejecutan en la capacidad de procesamiento reservada mediante las reservas de capacidad. Esta métrica no incluye las instancias EC2 reservadas de Amazon.

Unidad: recuento

Resolución máxima: 5 minutos

Dimensiones: `InstanceType` y `OutpostId`

`TotalReservedInstances`

El número total de instancias, en ejecución y disponibles para su lanzamiento, proporcionado por la capacidad de procesamiento reservada mediante las reservas de capacidad. Esta métrica no incluye las instancias EC2 reservadas de Amazon.

Unidad: recuento

Resolución máxima: 5 minutos

Dimensiones: `InstanceType` y `OutpostId`

Dimensiones de la métrica

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

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

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

Para ver las métricas mediante la consola CloudWatch

1. Abra la CloudWatch consola en https://console.aws.amazon.com/cloudwatch/.

2. En el panel de navegación, seleccione Métricas.
3. Selecciona el espacio de nombres de Outposts.
4. (Opcional) Para ver una métrica en todas las dimensiones, ingrese su nombre en el campo de búsqueda.

Para ver las métricas mediante el AWS CLI

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

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

Para obtener las estadísticas de una métrica mediante el AWS CLI

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

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

Registre AWS Outposts API las llamadas mediante AWS CloudTrail

AWS Outposts está integrado con AWS CloudTrail un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o un AWS servicio. CloudTrail captura API las llamadas AWS Outposts como eventos. Las llamadas capturadas incluyen las llamadas desde la AWS Outposts consola y las llamadas en código a las AWS Outposts API operaciones. Con la información recopilada por CloudTrail, puede determinar el destinatario de la solicitud AWS Outposts, la dirección IP desde la que se realizó la solicitud, el momento en que se realizó y otros detalles.

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

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

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

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

CloudTrail senderos

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

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

CloudTrail Almacenes de datos de eventos en Lake

CloudTrail Lake le permite ejecutar consultas SQL basadas en sus eventos. CloudTrail Lake convierte los eventos existentes en JSON formato basado en filas al ORC formato Apache.

ORCes un formato de almacenamiento en columnas que está optimizado para una rápida recuperación de datos. Los eventos se agregan en almacenes de datos de eventos, que son recopilaciones inmutables de eventos en función de criterios que se seleccionan aplicando selectores de eventos avanzados. Los selectores que se aplican a un almacén de datos de eventos controlan los eventos que perduran y están disponibles para la consulta. Para obtener más información acerca de CloudTrail Lake, consulte Cómo trabajar con AWS CloudTrail Lake en la Guía del AWS CloudTrail usuario.

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

AWS Outposts eventos de gestión en CloudTrail

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

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

AWS Outposts ejemplos de eventos

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


```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AKIAIOSFODNN7EXAMPLE:jdoe",
        "arn": "arn:aws:sts::111122223333:assumed-role/example/jdoe",
        "accountId": "111122223333",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
```

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

Mantenimiento del servidor Outposts

Esto se aplica al AWS Outposts igual que a una AWS región. Por ejemplo, AWS administra los parches de seguridad, actualiza el firmware y mantiene el equipo de Outpost. AWS también supervisa el rendimiento, el estado y las métricas de su servidor Outposts y determina si es necesario realizar algún tipo de mantenimiento.

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

Contenido

Actualiza los datos de contacto

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

Mantenimiento del hardware

Si AWS detecta un problema irreparable con el hardware durante el proceso de aprovisionamiento del servidor o al alojar EC2 instancias de Amazon que se ejecutan en su servidor de Outposts, notificaremos al propietario de Outpost y al propietario de las instancias que las instancias afectadas están programadas para su retirada. Para obtener más información, consulte Retirada de instancias en la Guía del EC2 usuario de Amazon.

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. Sigue las instrucciones de instalación en la instalación del servidor Outposts.
- Empaque el servidor irreparable AWS en el mismo paquete en el que llegó el servidor de reemplazo.
- Utilice la etiqueta de devolución prepagada que está disponible en la consola anexa a los detalles de configuración del pedido o al pedido del servidor de reemplazo.
- Devuelva el servidor a. AWS Para obtener más información, consulte Return an AWS Outposts server.

Actualizaciones de firmware

La actualización del firmware de Outpost no suele afectar a las instancias de su Outpost. En el raro caso de que necesitemos reiniciar el equipo de Outpost para instalar una actualización, recibirá un aviso de retirada de todas las instancias que se ejecuten en esa capacidad.

Mejores prácticas para eventos de alimentación y red de

Como se indica en los Términos de AWS servicio para AWS Outposts los clientes, la instalación donde se encuentra el equipo de Outposts debe cumplir con los requisitos mínimos de energía y red para respaldar la instalación, el mantenimiento y el uso del equipo de Outposts. Un 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:

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

Eventos de conectividad de red

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

EC2Las instancias, las LNI redes y los volúmenes de almacenamiento de instancias de Amazon en el servidor de Outposts seguirán funcionando con normalidad y se podrá acceder a ellos de forma local a través de la red local y. LNI Del mismo modo, los recursos de AWS servicio, como los ECS

nodos de trabajo de Amazon, siguen ejecutándose localmente. Sin embargo, la API disponibilidad disminuirá. Por ejemplo, es posible que las funciones ejecutar, iniciar, detener y terminar no APIs funcionen. Las métricas y los registros de las instancias seguirán almacenándose en caché local durante unas horas y se transferirán a la AWS región cuando se restablezca la conectividad. Sin embargo, la desconexión después de unas horas podría provocar la pérdida de métricas y registros.

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.
- El AWS blog Debugging tool for network connectivity de Amazon VPC explica la herramienta AWSSupport-S etupIPMonitoring FromVPC. Esta herramienta es un AWS Systems Manager documento (SSMdocumento) que crea una instancia de Amazon EC2 Monitor en una subred especificada por usted y monitorea las direcciones IP de destino. El documento ejecuta pruebas de diagnóstico de pingMTR, TCP trace-route y trace-path 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

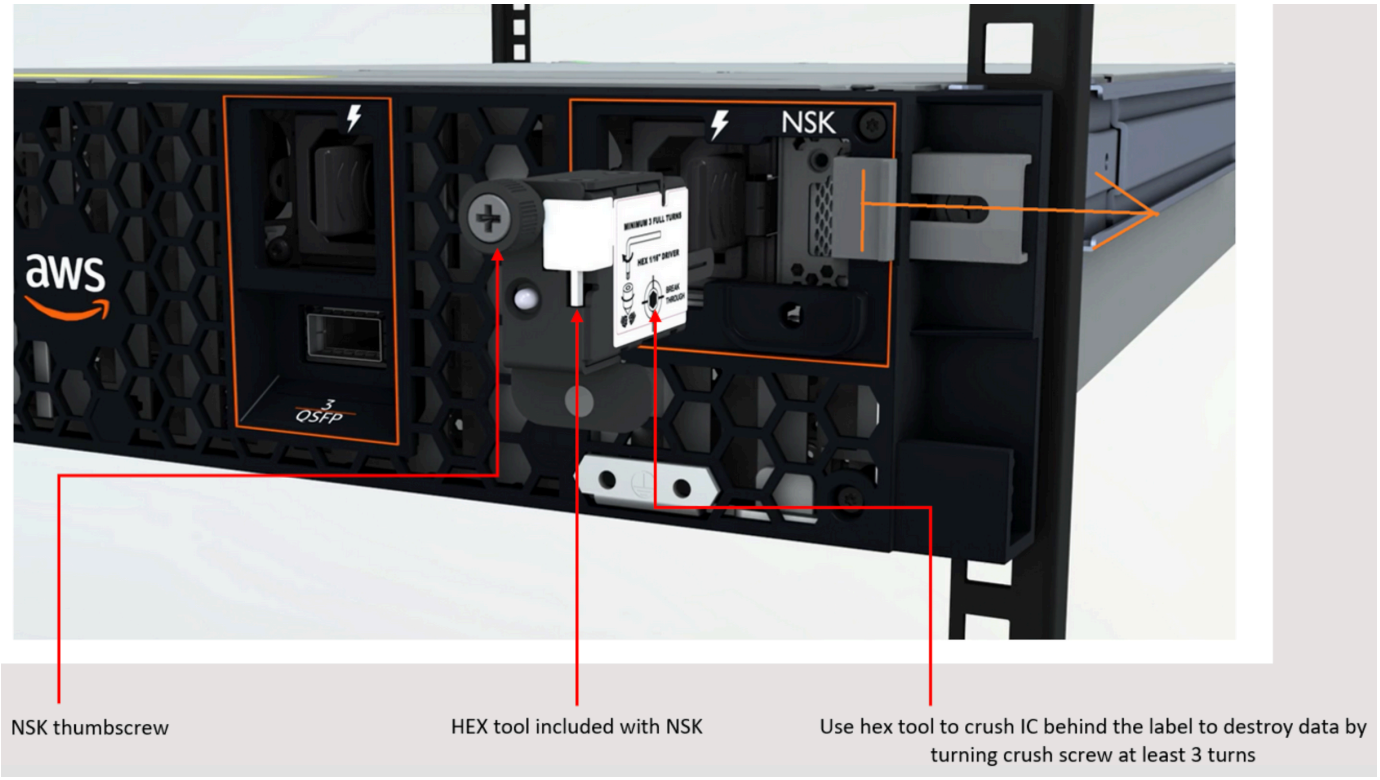
- El AWS blog Cómo implementar un CloudWatch panel automatizado de Amazon para su AWS Outposts uso AWS CDK describe los pasos necesarios para implementar un panel automatizado.
- Si tiene preguntas o necesita más información, consulte Creating a support case en la Guía del usuario de AWS Support.

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 destruirlo NSK para destruir criptográficamente los datos del servidor.

Cómo destruir criptográficamente los datos del servidor

1. Quítelo NSK del servidor antes de volver a enviarlo. AWS
2. Asegúrese de tener el correcto NSK que se envió 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 NSK y tritura criptográficamente todos los datos del servidor.


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

Opciones del servidor Outposts end-of-term

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

- Renueva tu suscripción y conserva tus servidores Outposts existentes.
- Finaliza tu suscripción y devuelve tus servidores de Outposts.
- Conviértelo en una month-to-month suscripción y conserva tus servidores Outposts existentes.

Renovar la suscripción

Debes completar los siguientes pasos al menos 30 días antes de que finalice la suscripción actual de tus servidores de Outposts.

Para renovar tu suscripción y conservar tus servidores Outposts existentes

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 indicas que deseas renovar tu suscripción o devolver tu servidor de Outposts, pasarás a ser una month-to-month suscripción automáticamente. Tu Outpost se renovará mensualmente al precio de la opción de pago sin pago por adelantado que corresponda a tu configuración. AWS Outposts Su nueva suscripción mensual comenzará el día siguiente a la finalización de la suscripción actual.

Finalice su suscripción y devuelva el servidor

Debes completar los siguientes pasos al menos 30 días antes de que finalice la suscripción actual de tus servidores de Outposts. AWS no puedes iniciar el proceso de devolución hasta que lo hagas.

> **Important**
>
> AWS no puedes detener el proceso de devolución después de haber abierto un caso de soporte para finalizar tu suscripción.

Para finalizar tu suscripción

1. Inicie sesión en la consola del AWS Support Center.
2. Elija Crear caso.
3. Elija Cuenta y facturación.
4. Para Servicio, elija Facturación.
5. Para Categoría, elija Otras preguntas sobre facturación.
6. Para Severidad, elija Pregunta importante.
7. Elija Siguiente paso: información adicional.
8. En la página Información adicional, para Asunto, introduzca su solicitud de renovación, por ejemplo **`End my Outpost subscription`**.
9. En Descripción, introduce la fecha en la que deseas 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. NOTApague o 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 convertirla en una month-to-month suscripción y conservar tus servidores Outposts existentes, no es necesario realizar ninguna acción. Si tiene alguna pregunta, abra un caso de soporte de facturación.

Tu Outpost se renovará mensualmente al precio de la opción de pago sin pago por adelantado que corresponda a tu configuración. AWS Outposts Tu nueva suscripción mensual comienza 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.

En la siguiente tabla se describen las actualizaciones de la documentación de los servidores 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
Opciones E para servidores nd-of-term 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
Presentamos los servidores Outposts	Se agregaron los servidores Outposts, un nuevo AWS Outposts formato.	30 de noviembre de 2021

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.