Mejores prácticas para crear una arquitectura de nube híbrida con Servicios de AWS

AWS Orientación prescriptiva

AWS Orientación prescriptiva: Mejores prácticas para crear una arquitectura de nube híbrida con Servicios de AWS

Table of Contents

Mejores prácticas para crear una arquitectura de nube híbrida con Servicios de AWS

Amazon Web Services (colaboradores)

Junio de 2025 (historial del documento)

Muchas empresas y organizaciones han adoptado la computación en nube como un aspecto clave de su estrategia tecnológica. Por lo general, migran sus cargas de trabajo a una Nube de AWS para aumentar la agilidad, el ahorro de costes, el rendimiento, la disponibilidad, la resiliencia y la escalabilidad. La mayoría de las aplicaciones se pueden migrar fácilmente, pero algunas aplicaciones deben permanecer en las instalaciones para aprovechar la baja latencia y el procesamiento de datos local del entorno local, evitar los altos costos de transferencia de datos o para cumplir con la normativa. Además, es posible que sea necesario rediseñar o modernizar un subconjunto de aplicaciones antes de poder trasladarlas a la nube. Esto lleva a muchas organizaciones a buscar arquitecturas de nube híbrida para integrar sus operaciones locales y en la nube para dar soporte a una amplia gama de casos de uso. Este enfoque híbrido puede proporcionar los beneficios de la computación local y basada en la nube, y puede resultar particularmente útil en escenarios de computación perimetral.

Cuando cree una nube híbrida con AWS, le recomendamos que determine su estrategia de nube híbrida y su estrategia técnica:

- Una estrategia de nube híbrida proporciona pautas que rigen el consumo de recursos locales y de la nube para respaldar sus objetivos empresariales. Esta guía describe los casos de uso más habituales para crear una nube híbrida, como respaldar la migración continua a la nube, garantizar la continuidad empresarial en caso de desastre, extender la infraestructura de la nube al entorno local para admitir aplicaciones de baja latencia o ampliar su presencia internacional en AWS Definir esta estrategia le ayuda a identificar y definir sus objetivos empresariales para crear una nube híbrida y proporciona directrices para la ubicación de las cargas de trabajo en la nube híbrida.
- Una estrategia técnica para la nube híbrida identifica los principios rectores de la arquitectura de la nube híbrida y define un marco de implementación. Esta guía describe los requisitos comunes para una arquitectura de nube híbrida implementada y administrada de manera coherente para ayudarlo a definir los principios para una implementación planificada de la nube híbrida. Estos requisitos

incluyen interfaces estandarizadas para el aprovisionamiento y la administración de recursos en toda su infraestructura de nube.

Esta guía describe un marco de operaciones y administración para ayudar a los arquitectos y operadores de soluciones a identificar los componentes básicos, las mejores prácticas y los servicios regionales y de nube AWS híbrida con los que implementar una nube híbrida. AWS

Muchas organizaciones han utilizado las soluciones descritas en esta guía para implementar con éxito entornos de nube híbrida que aprovechen la escala, la agilidad, la innovación y la presencia global que ofrece la Nube de AWS nube. (Consulte los casos prácticos). AWS Los servicios de nube híbrida ofrecen una AWS experiencia uniforme desde la nube hasta las instalaciones y en la periferia. Servicios como AWS Outposts el procesamiento, el almacenamiento, las bases de datos y otros servicios selectos Servicios de AWS cerca de grandes centros industriales y de población cuando se necesita una baja latencia entre los dispositivos de los usuarios finales o entre los centros de datos locales y los servidores de carga de trabajo existentes. Zonas locales de AWS

En esta guía:

Información general

Esta guía clasifica AWS las recomendaciones para la nube híbrida en cinco pilares: redes, seguridad, resiliencia, planificación de la capacidad y administración de la infraestructura. Proporciona pautas para ayudarlo a mejorar su preparación y desarrollar una estrategia de migración mediante el uso de un servicio perimetral AWS híbrido, como AWS Outposts o. Zonas locales de AWS Le recomendamos encarecidamente que trabaje con su Cuenta de AWS equipo o AWS Partner que se asegure de que haya un especialista en nube AWS híbrida disponible para ayudarlo a seguir esta guía y desarrollar su proceso.

> **Note**
>
> Si bien AWS Outposts las Zonas Locales abordan problemas similares, le recomendamos que revise los casos de uso, así como los servicios y funciones disponibles, para decidir qué oferta se adapta mejor a sus necesidades. Para obtener más información, consulte la entrada del AWS blog Zonas locales de AWS y AWS Outposts elija la tecnología adecuada para su carga de trabajo perimetral.

Talleres sobre la nube híbrida

Con la ayuda de un experto en la materia (PYME) sobre la nube AWS híbrida, puede organizar un taller sobre la nube híbrida para evaluar el nivel de madurez de su empresa en relación con los cinco pilares que se describen en esta guía.

El taller se centra en las áreas internas de su organización, como las redes, la seguridad, el cumplimiento DevOps, la virtualización y las unidades de negocio. Le ayuda a diseñar una arquitectura de nube híbrida que cumpla con los requisitos de su organización y a definir los detalles de la implementación, siguiendo los pasos de la sección sobre el proceso de adopción de la nube híbrida de esta guía.

PoCs

Si tiene requisitos específicos, puede utilizar pruebas de concepto (PoCs) para validar la funcionalidad en las Zonas Locales y AWS Outposts compararla con esos requisitos.

AWS se utiliza PoCs para ayudarle a probar las cargas de trabajo que desea trasladar a un puesto avanzado o a una zona local, a fin de determinar si las cargas de trabajo funcionarán en las arquitecturas de prueba. Para acceder a una zona local para realizar pruebas, siga las instrucciones de la documentación de las zonas locales. Para evaluar su carga de trabajo AWS Outposts, trabaje con su Cuenta de AWS equipo o acceda AWS Partner a un laboratorio de AWS Outposts pruebas y reciba orientación de los arquitectos de AWS soluciones. En todos los escenarios, el desarrollo de un PoC requiere que se genere un documento de prueba que contenga:

- Servicios de AWS para usar, como Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic Block Store (Amazon EBS), Amazon Virtual Private Cloud (Amazon VPC) y Amazon Elastic Kubernetes Service (Amazon EKS)
- Tamaño y cantidad de instancias que se van a consumir (por ejemplo, o) `m5.xlarge` `c5.2xlarge`
- Diagrama de arquitectura de prueba
- Criterios de éxito del ensayo
- Detalles y objetivos de cada prueba a realizar

Pilares

En la siguiente sección, se describen los requisitos previos y las limitaciones para usar las arquitecturas que se describen en esta guía. En las secciones siguientes se tratan los detalles de cada pilar, de modo que el documento de recomendaciones que se cree durante el taller sobre la nube híbrida pueda reflejar los detalles de diseño necesarios para la implementación.

- Redes en la periferia
- Seguridad en la periferia
- Resiliencia en la periferia
- La planificación de la capacidad en la periferia
- Administración de la infraestructura perimetral

Requisitos previos y limitaciones

Antes de seguir esta guía, trabaje con su Cuenta de AWS equipo o AWS Partner revise los requisitos previos y las limitaciones para implementar arquitecturas perimetrales con Zonas AWS Outposts Locales.

Requisitos previos

AWS Outposts

- Su centro de datos actual debe cumplir los AWS Outposts requisitos de instalaciones, redes y alimentación. AWS Outposts está diseñado para funcionar en un entorno de centro de datos con entradas de alimentación redundantes de entre 5 y 15 kVA, un flujo de aire de 145,8 veces el kVA de pies cúbicos por minuto (CFM) y una temperatura ambiente de entre 41 °F (5 °C) y 95 °F (35 °C), entre otros requisitos.
- Confirme que el servicio está disponible en su país consultando el rack AWS Outposts .AWS Outposts FAQs Consulta la pregunta: ¿En qué países y territorios está disponible el estante Outposts?
- Si su organización necesita cuatro o más AWS Outposts racks, su centro de datos debe cumplir con los requisitos de rack Aggregation, Core y Edge (ACE).
- Se debe disponer de una conexión a Internet o un AWS Direct Connect enlace de al menos 500 Mbps (1 Gbps es mejor) para poder conectarse AWS Outposts al mismo Región de AWS, con la conectividad de respaldo adecuada si su caso de uso lo requiere. La latencia de ida y vuelta desde AWS Outposts la región debe ser de 175 milisegundos como máximo.
- Debe tener un contrato activo para AWS Enterprise Support o un plan de operaciones AWS unificadas.

Zonas locales de AWS

- Debe haber una zona AWS local disponible cerca de sus centros de datos o usuarios. Consulte Zonas locales de AWS las ubicaciones.
- Confirme que tiene conectividad de red desde su infraestructura local a la zona local:

- Opción 1: un Direct Connect enlace desde el centro de datos al Direct Connect punto de presencia (PoP) más cercano a la zona local. Para obtener más información, consulte Direct Connect en la documentación de las Zonas Locales.
- Opción 2: un enlace a Internet además de un dispositivo de red privada virtual (VPN) local y las licencias necesarias para lanzar un dispositivo VPN basado en software en Amazon EC2 en la zona local. Para obtener más información, consulte Conexión VPN en la documentación de las Zonas Locales.

Para ver opciones de conectividad adicionales, consulte la documentación de las Zonas Locales.

Limitaciones

AWS Outposts

- Amazon Relational Database Service (Amazon RDS) AWS Outposts en las implementaciones Multi-AZ requiere conjuntos de direcciones IP (CoIP) propiedad del cliente. Para obtener más información, consulte Direcciones IP propiedad del cliente para Amazon RDS en. AWS Outposts
- Multi-AZ on AWS Outposts está disponible para todas las versiones compatibles de MySQL y PostgreSQL en Amazon RDS on. AWS Outposts Para obtener más información, consulte Compatibilidad de Amazon RDS on AWS Outposts con las características de Amazon RDS. Amazon RDS on AWS Outposts es compatible con las bases de datos de SQL Server, Amazon RDS for MySQL y Amazon RDS for PostgreSQL.
- AWS Outposts no está diseñado para funcionar cuando está desconectado de un. Región de AWS Para obtener más información, consulte la sección Pensar en términos de modos de falla en el AWS documento técnico Consideraciones sobre arquitectura y diseño de AWS Outposts alta disponibilidad.
- Amazon Simple Storage Service (Amazon S3) tiene algunas AWS Outposts limitaciones. Se analizan en la sección ¿En qué se diferencia Amazon S3 en Outposts de Amazon S3? sección de la Guía del usuario de Amazon S3 on Outposts.
- Los balanceadores de carga de aplicaciones activados AWS Outposts no admiten TLS mutuos (mTLS) ni sesiones fijas.
- Los estantes ACE no están completamente cerrados y no incluyen puertas delanteras ni traseras.
- La herramienta de capacidad de instancias solo se aplica a los nuevos pedidos.

Zonas locales de AWS

- Las Zonas Locales no tienen un AWS Site-to-Site VPN punto final. En su lugar, utilice una VPN basada en software en Amazon EC2.
- Las Zonas Locales no son compatibles AWS Transit Gateway. En su lugar, conéctese a la zona local mediante una interfaz virtual Direct Connect privada (VIF).
- No todas las Zonas Locales admiten servicios como Amazon RDS, Amazon FSx, Amazon EMR o ElastiCache Amazon o las puertas de enlace NAT. Para más información, consulte Características de Zonas locales de AWS.
- Los balanceadores de carga de aplicaciones en las Zonas Locales no admiten MTL ni sesiones fijas.

Proceso de adopción de la nube híbrida

En las siguientes secciones se analizan las arquitecturas y los detalles de diseño de cada pilar de la AWS nube híbrida:

- Redes en la periferia
- Seguridad en la periferia
- Resiliencia en la periferia
- La planificación de la capacidad en la periferia
- Administración de la infraestructura perimetral

Redes en la periferia

Al diseñar soluciones que utilizan una infraestructura AWS perimetral, como AWS Outposts las Zonas Locales, debe considerar detenidamente el diseño de la red. La red constituye la base de la conectividad para llegar a las cargas de trabajo que se despliegan en estas ubicaciones periféricas y es fundamental para garantizar una baja latencia. En esta sección se describen varios aspectos de la conectividad perimetral híbrida.

Arquitectura de la VPC

Una nube privada virtual (VPC) abarca todas las zonas de disponibilidad de su. Región de AWS Puedes extender sin problemas cualquier VPC de la región a Outposts o Local Zones mediante la AWS consola o el AWS Command Line Interface (AWS CLI) para añadir una subred de Outpost o Zona Local. Los siguientes ejemplos muestran cómo crear subredes en AWS Outposts las Zonas Locales mediante: AWS CLI

- AWS Outposts: Para añadir una subred de Outpost a una VPC, especifique el nombre de recurso de Amazon (ARN) del Outpost.

```
aws ec2 create-subnet --vpc-id vpc-081ec835f3EXAMPLE \
--cidr-block 10.0.0.0/24 \
--outpost-arn arn:aws:outposts:us-west-2:11111111111:outpost/op-0e32example1 \
--tag-specifications ResourceType=subnet,Tags=[{Key=Name,Value=my-ipv4-only-subnet}]
```

  Para obtener más información, consulte la Documentación de AWS Outposts.

- Zonas locales: para añadir una subred de zona local a una VPC, siga el mismo procedimiento que utiliza con las zonas de disponibilidad, pero especifique el ID de zona local `<local-zone-name>` (en el siguiente ejemplo).

```
aws ec2 create-subnet --vpc-id vpc-081ec835f3EXAMPLE \
--cidr-block 10.0.1.0/24 \
--availability-zone <local-zone-name> \
--tag-specifications ResourceType=subnet,Tags=[{Key=Name,Value=my-ipv4-only-subnet}]
```

  Para obtener más información, consulte la documentación de las Zonas Locales.

El siguiente diagrama muestra una AWS arquitectura que incluye subredes de Outpost y de zona local.

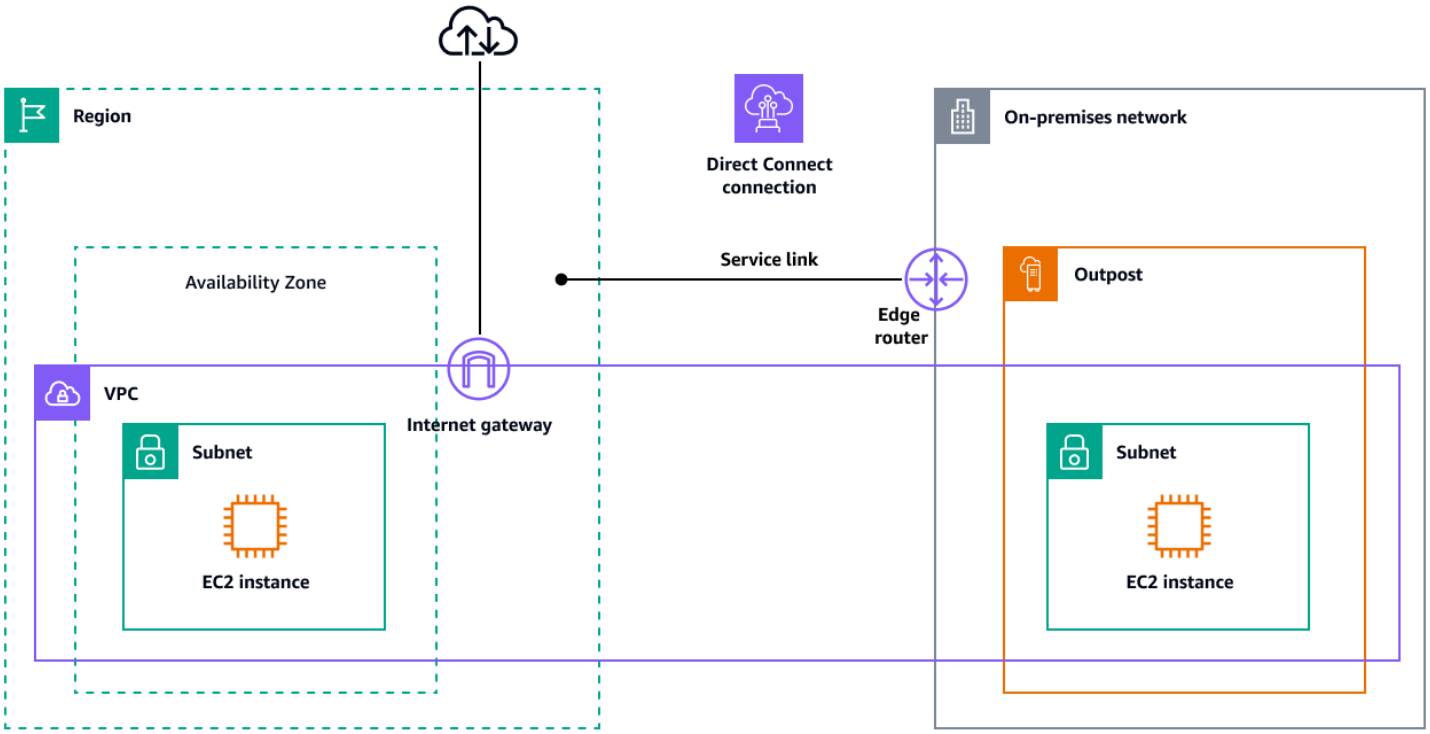
Tráfico de extremo a región

Cuando diseñe una arquitectura híbrida mediante servicios como las Zonas Locales y AWS Outposts tenga en cuenta tanto los flujos de control como los flujos de tráfico de datos entre las infraestructuras perimetrales y Regiones de AWS. Según el tipo de infraestructura perimetral, su responsabilidad puede variar: algunas infraestructuras requieren que gestione la conexión con la región principal, mientras que otras lo hacen a través de la infraestructura AWS global. Esta sección

explora las implicaciones de conectividad del plano de control y el plano de datos para las Zonas Locales y AWS Outposts.

AWS Outposts plano de control

AWS Outposts proporciona una estructura de red denominada enlace de servicio. El enlace de servicio es una conexión obligatoria entre AWS Outposts y la región seleccionada Región de AWS o principal (también denominada región de origen). Permite la gestión del puesto de avanzada y el intercambio de tráfico entre el puesto de avanzada y. Región de AWS El enlace de servicio utiliza un conjunto cifrado de conexiones VPN para comunicarse con la región de origen. Debe proporcionar conectividad entre AWS Outposts y la, Región de AWS ya sea a través de un enlace a Internet o una interfaz virtual Direct Connect pública (VIF pública), o a través de una interfaz virtual Direct Connect privada (VIF privada). Para una experiencia y una resiliencia óptimas, se AWS recomienda utilizar una conectividad redundante de al menos 500 Mbps (1 Gbps es mejor) para la conexión del enlace de servicio al. Región de AWS La conexión de enlace de servicio mínima de 500 Mbps le permite lanzar instancias de Amazon EC2, adjuntar volúmenes de Amazon EBS y acceder a métricas Servicios de AWS como Amazon EKS, Amazon EMR y Amazon. CloudWatch La red debe admitir una unidad de transmisión (MTU) máxima de 1500 bytes entre el Outpost y los puntos de enlace de servicio del servidor principal. Región de AWSPara obtener más información, consulta la AWS Outposts conectividad a Regiones de AWS en la documentación de Outposts.



Para obtener información sobre cómo crear arquitecturas resilientes para los enlaces de servicios que utilizan Internet pública, consulte la sección sobre conectividad de Anchor en el AWS documento técnico Consideraciones sobre arquitectura Direct Connect y diseño de AWS Outposts alta disponibilidad.

AWS Outposts plano de datos

El plano de datos entre AWS Outposts y el Región de AWS es compatible con la misma arquitectura de enlace de servicio que utiliza el plano de control. El ancho de banda del enlace de servicio del plano de datos entre AWS Outposts y Región de AWS debe correlacionarse con la cantidad de datos que se deben intercambiar: cuanto mayor sea la dependencia de los datos, mayor debe ser el ancho de banda del enlace.

Los requisitos de ancho de banda varían según las siguientes características:

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

El tráfico entre las instancias EC2 de dentro AWS Outposts y las instancias de EC2 de la misma Región de AWS tiene una MTU de 1300 bytes. Le recomendamos que analice estos requisitos con un especialista en nube AWS híbrida antes de proponer una arquitectura que tenga codependencias entre la región y. AWS Outposts

Plano de datos de Zonas Locales

El plano de datos entre las Zonas Locales y las Región de AWS es compatible con la infraestructura AWS global. El plano de datos se extiende a través de una VPC desde una zona local. Región de AWS Las Zonas Locales también proporcionan una conexión segura y de gran ancho de Región de AWS banda y le permiten conectarse sin problemas a toda la gama de servicios regionales a través de las mismas API y conjuntos de herramientas.

La siguiente tabla muestra las opciones de conexión y las MTU asociadas.

De	Para	MTU
Amazon EC2 en la región	Amazon EC2 en Zonas Locales	1.300 bytes
Direct Connect	Zonas locales	1.468 bytes
Puerta de enlace de Internet	Zonas locales	1.500 bytes
Amazon EC2 en Zonas Locales	Amazon EC2 en Zonas Locales	9.001 bytes

Las Zonas Locales utilizan la infraestructura AWS global para conectarse con Regiones de AWS. La infraestructura está totalmente gestionada por AWS, por lo que no es necesario configurar esta conectividad. Le recomendamos que analice los requisitos y consideraciones de sus Zonas Locales con un especialista en nube AWS híbrida antes de diseñar cualquier arquitectura que tenga codependencias entre la Región y las Zonas Locales.

El tráfico de la periferia al local

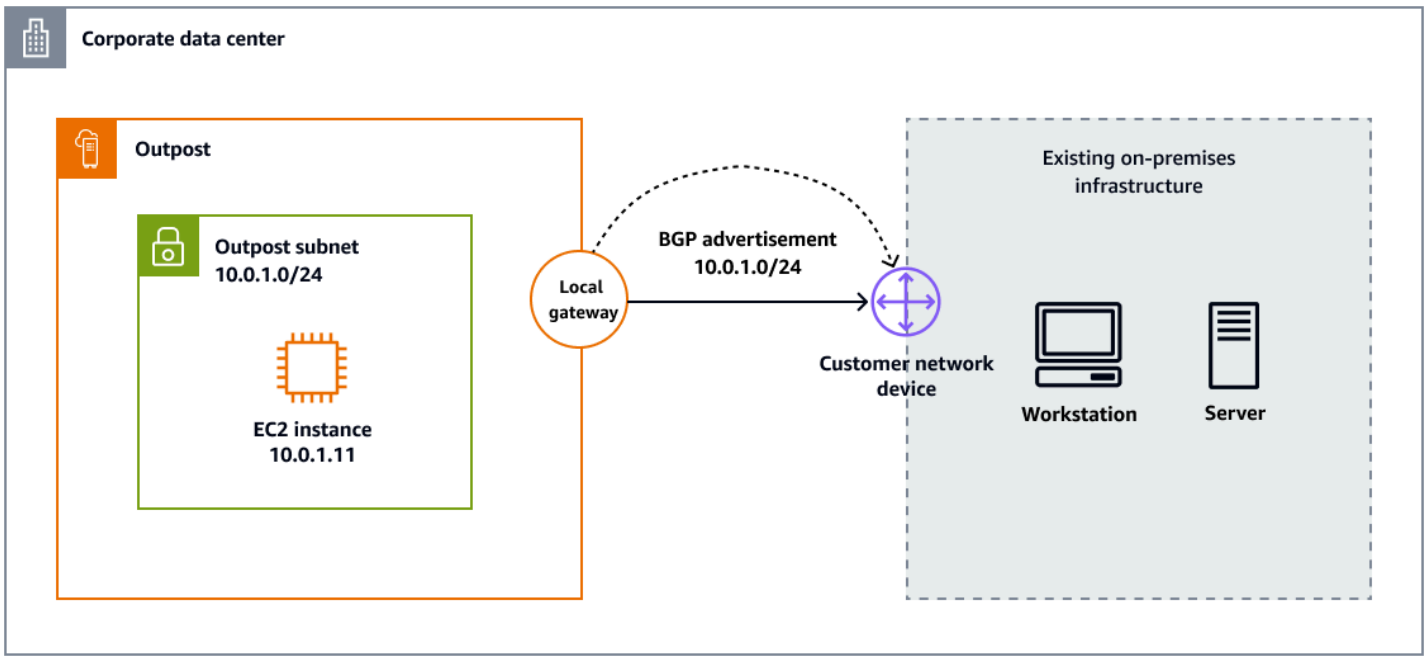
AWS Los servicios de nube híbrida están diseñados para abordar casos de uso que requieren baja latencia, procesamiento de datos local o cumplimiento de la residencia de datos. La arquitectura de red para acceder a estos datos es importante y depende de si la carga de trabajo se ejecuta en Zonas Locales AWS Outposts o en ellas. La conectividad local también requiere un ámbito bien definido, como se explica en las siguientes secciones.

AWS Outposts puerta de enlace local

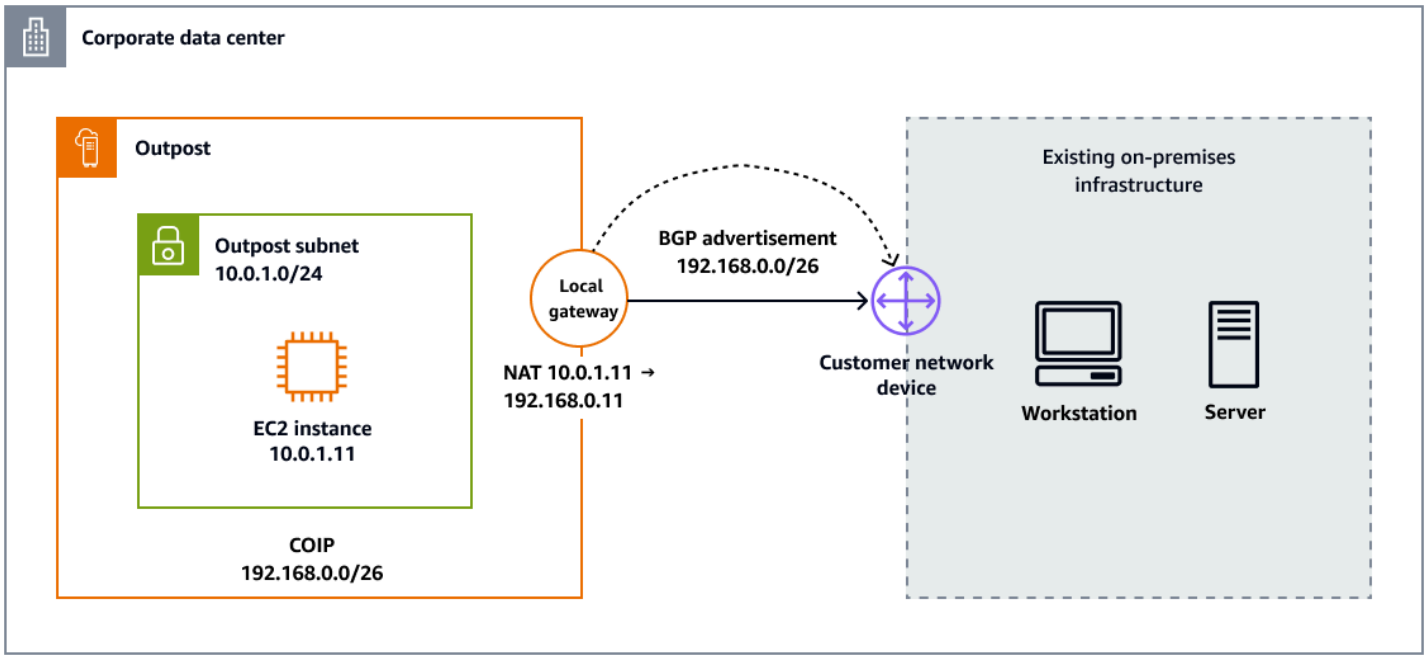
La puerta de enlace local (LGW) es un componente central de la AWS Outposts arquitectura. La puerta de enlace local permite la conectividad entre las subredes Outpost y la red en las instalaciones. La función principal de una LGW es proporcionar conectividad desde un puesto de avanzada a la red local local. También proporciona conectividad a Internet a través de la red local mediante el enrutamiento directo de la VPC o las direcciones IP propiedad del cliente.

- El enrutamiento directo de la VPC utiliza la dirección IP privada de las instancias de la VPC para facilitar la comunicación con la red local. Estas direcciones se anuncian en su red local mediante el protocolo Border Gateway (BGP). La publicidad en BGP es solo para las direcciones IP privadas que pertenecen a las subredes de su bastidor de Outpost. Este tipo de enrutamiento

es el modo predeterminado. AWS Outposts En este modo, la puerta de enlace local no realiza la NAT para las instancias y no es necesario asignar direcciones IP elásticas a las instancias de EC2. En el siguiente diagrama, se muestra una puerta de enlace AWS Outposts local que utiliza el enrutamiento directo de VPC.



- Con las direcciones IP propiedad del cliente, puedes proporcionar un rango de direcciones, conocido como conjunto de direcciones IP propiedad del cliente (CoIP), que admite rangos de CIDR superpuestos y otras topologías de red. Al elegir un CoIP, debe crear un conjunto de direcciones, asignarlo a la tabla de rutas de la puerta de enlace local y volver a anunciar estas direcciones a su red mediante BGP. Las direcciones CoIP proporcionan conectividad local o externa a los recursos de la red local. Puede asignar estas direcciones IP a los recursos de su Outpost, como las instancias EC2, asignando una nueva dirección IP elástica desde el CoIP y, a continuación, asignándola a su recurso. El siguiente diagrama muestra una puerta de enlace AWS Outposts local que utiliza el modo CoIP.



La conectividad local desde AWS Outposts una red local requiere algunas configuraciones de parámetros, como habilitar el protocolo de enrutamiento BGP y anunciar los prefijos entre los pares BGP. La MTU que se puede admitir entre tu Outpost y la puerta de enlace local es de 1500 bytes. Para obtener más información, póngase en contacto con un especialista en nube AWS híbrida o consulte la AWS Outposts documentación.

Zonas Locales e Internet

Las industrias que requieren baja latencia o residencia de datos local (por ejemplo, los juegos, la transmisión en vivo, los servicios financieros y el gobierno) pueden usar las Zonas Locales para implementar y proporcionar sus aplicaciones a los usuarios finales a través de Internet. Durante el despliegue de una zona local, debe asignar direcciones IP públicas para usarlas en una zona local. Al asignar direcciones IP elásticas, puede especificar la ubicación desde la que se anuncia la dirección IP. Esta ubicación se denomina grupo fronterizo de red. Un grupo fronterizo de red es un conjunto de Zonas de disponibilidad, Zonas Locales o AWS Wavelength Zonas desde las que se AWS anuncia una dirección IP pública. Esto ayuda a garantizar una latencia o distancia física mínima entre la AWS red y los usuarios que acceden a los recursos de estas zonas. Para ver todos los grupos fronterizos de la red para las zonas locales, consulte Zonas locales disponibles en la documentación de Zonas locales.

Para exponer a Internet una EC2-hosted carga de trabajo de Amazon en una zona local, puede habilitar la opción IP Auto-assign pública al lanzar la instancia EC2. Si usa un Application Load

Balancer, puede definirlo como orientado a Internet para que las direcciones IP públicas asignadas a la zona local puedan propagarse por la red fronteriza asociada a la zona local. Además, cuando utiliza direcciones IP elásticas, puede asociar uno de estos recursos a una instancia EC2 después de su lanzamiento. Cuando envía tráfico a través de una puerta de enlace de Internet en las Zonas Locales, se aplican las mismas especificaciones de ancho de banda de instancia que utiliza la región. El tráfico de la red de la zona local va directamente a Internet o a los puntos de presencia (PoPs) sin atravesar la región principal de la zona local, lo que permite el acceso a la informática de baja latencia.

Las Zonas Locales ofrecen las siguientes opciones de conectividad a través de Internet:

- Acceso público: conecta cargas de trabajo o dispositivos virtuales a Internet mediante direcciones IP elásticas a través de una puerta de enlace de Internet.
- Acceso saliente a Internet: permite que los recursos lleguen a puntos finales públicos a través de instancias de traducción de direcciones de red (NAT) o dispositivos virtuales con direcciones IP elásticas asociadas, sin exposición directa a Internet.
- Conectividad VPN: establece conexiones privadas mediante una VPN de seguridad de protocolo de Internet (IPsec) a través de dispositivos virtuales con direcciones IP elásticas asociadas.

Para obtener más información, consulte Opciones de conectividad para zonas locales en la documentación de Zonas locales.

Zonas Locales y Direct Connect

También son compatibles con las Zonas Locales Direct Connect, lo que te permite enrutar el tráfico a través de una conexión de red privada. Para obtener más información, consulte Conexión directa en zonas locales en la documentación de Zonas locales.

Zonas Locales y pasarelas de tránsito

AWS Transit Gateway no admite los adjuntos de VPC directos a las subredes de la zona local. Sin embargo, puede conectarse a las cargas de trabajo de la zona local creando adjuntos de Transit Gateway en las subredes principales de la zona de disponibilidad de la misma VPC. Esta configuración permite la interconectividad entre varias VPC y las cargas de trabajo de la zona local. Para obtener más información, consulte Conexión de pasarela de tránsito entre zonas locales en la documentación de Zonas locales.

Zonas Locales y emparejamiento de VPC

Puede extender cualquier VPC de una región principal a una zona local creando una nueva subred y asignándola a la zona local. El emparejamiento de VPC se puede establecer entre las VPC que se extienden a las Zonas Locales. Cuando las VPC interconectadas se encuentran en la misma zona local, el tráfico permanece dentro de la zona local y no pasa por la región principal.

Seguridad en el límite

En el Nube de AWS, la seguridad es la máxima prioridad. A medida que las organizaciones adoptan la escalabilidad y la flexibilidad de la nube, las AWS ayuda a adoptar la seguridad, la identidad y el cumplimiento como factores empresariales clave. AWS integra la seguridad en su infraestructura principal y ofrece servicios que le ayudan a cumplir sus requisitos exclusivos de seguridad en la nube. Al ampliar el alcance de su arquitectura Nube de AWS, se beneficiará de la integración de infraestructuras como Zonas Locales y Outposts en ellas. Regiones de AWS Esta integración permite AWS extender un grupo selecto de servicios de seguridad básicos a la periferia.

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

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que se ejecuta Servicios de AWS en la Nube de AWS. AWS también le proporciona servicios que puede utilizar de forma segura. Third-party los auditores prueban y verifican periódicamente la eficacia de la AWS seguridad como parte de los programas de AWS cumplimiento.
- Seguridad en la nube: su responsabilidad viene determinada por lo Servicio de AWS que utilice. También es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y los reglamentos aplicables.

Protección de datos

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

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

Cifrado en reposo

Cifrado en volúmenes de EBS

Con AWS Outposts, todos los datos se cifran en reposo. El material de la clave viene empaquetado con una clave externa, la clave de seguridad Nitro (NSK), que se guarda en un dispositivo extraíble. La NSK es necesaria para descifrar los datos de su rack de Outpost. Puede utilizar el cifrado de Amazon EBS para volúmenes e instantáneas de EBS. El cifrado de Amazon EBS utiliza AWS Key Management Service (AWS KMS) y claves KMS.

En el caso de las zonas locales, todos los volúmenes de EBS se cifran de forma predeterminada en todas las zonas locales, excepto en la lista documentada en las Zonas locales de AWS preguntas frecuentes (consulte la pregunta: ¿Cuál es el comportamiento de cifrado predeterminado de los volúmenes de EBS en las zonas locales?), a menos que el cifrado esté habilitado para la cuenta.

Cifrado en Amazon S3 en Outposts

De forma predeterminada, todos los datos almacenados en Amazon S3 en Outposts se cifran mediante el cifrado del lado del servidor con claves de cifrado gestionadas por Amazon S3 (). SSE-S3 Si lo desea, puede utilizar el cifrado del lado del servidor con claves de cifrado proporcionadas por el cliente (). SSE-C Para utilizarla SSE-C, especifique una clave de cifrado como parte de las solicitudes de la API de sus objetos. Server-side el cifrado cifra solo los datos del objeto, no los metadatos del objeto.

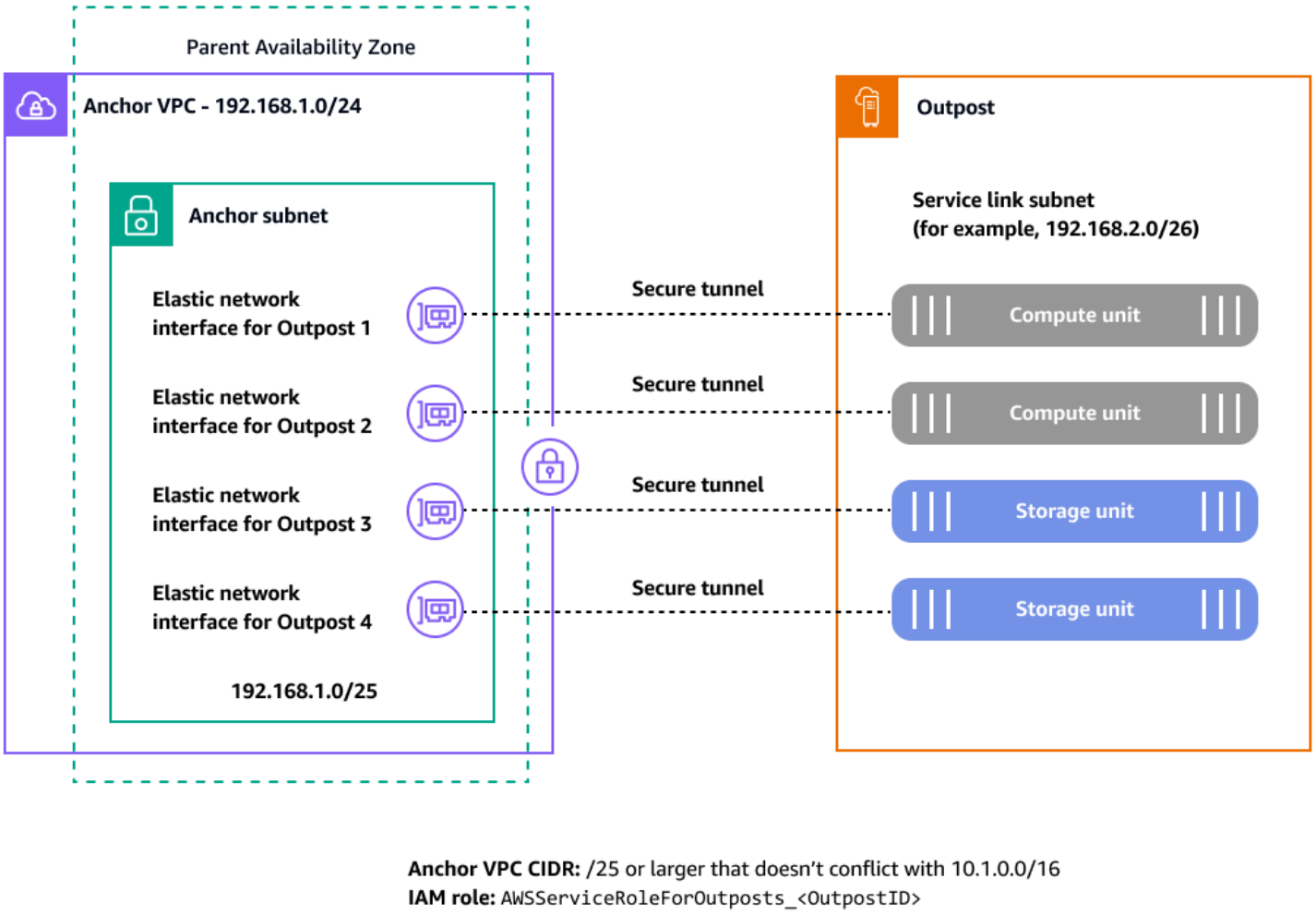
> **Note**
>
> Amazon S3 en Outposts no admite el cifrado del lado del servidor con claves KMS (). SSE-KMS

Cifrado en tránsito

En AWS Outposts efecto, el enlace de servicio es una conexión necesaria entre el servidor de Outposts y la región elegida Región de AWS (o región de origen) y permite la gestión del Outpost y el intercambio de tráfico desde y hacia. Región de AWS El enlace de servicio utiliza una VPN

AWS gestionada para comunicarse con la región de origen. Cada host interno AWS Outposts crea un conjunto de túneles VPN para dividir el tráfico del plano de control y el tráfico de VPC. Dependiendo de la conectividad del enlace de servicio (Internet o Direct Connect) AWS Outposts, esos túneles requieren que se abran los puertos del firewall para que el enlace de servicio cree una capa superpuesta sobre ellos. Para obtener información técnica detallada sobre la seguridad AWS Outposts y el enlace de servicio, consulte Conectividad a través del enlace de servicio y Seguridad de la infraestructura AWS Outposts en la AWS Outposts documentación.

El enlace AWS Outposts de servicio crea túneles cifrados que establecen la conectividad del plano de control y del plano de datos con el plano principal Región de AWS, como se muestra en el siguiente diagrama.



Cada AWS Outposts host (procesamiento y almacenamiento) necesita estos túneles cifrados a través de puertos TCP y UDP conocidos para comunicarse con su región principal. En la siguiente tabla, se muestran los puertos y las direcciones de origen y destino de los protocolos UDP y TCP.

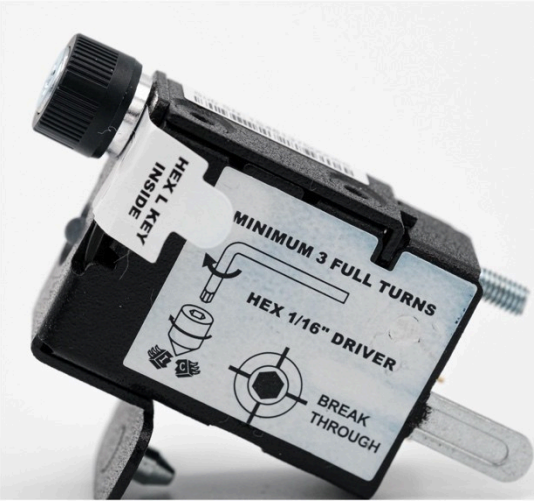
Protocolo	Puerto de origen	Dirección de origen	Puerto de destino	Dirección de destino
UDP	443	AWS Outposts enlace de servicio /26	443	AWS Outposts Rutas públicas de la región o anclaje VPC CIDR
TCP	1025-65535	AWS Outposts enlace de servicio /26	443	AWS Outposts Rutas públicas de la región o anclaje VPC CIDR

Las Zonas Locales también están conectadas a la región principal a través de la red troncal privada global redundante y de gran ancho de banda de Amazon. Esta conexión proporciona a las aplicaciones que se ejecutan en las Zonas Locales un acceso rápido, seguro y sin problemas a otras Servicios de AWS. Mientras las Zonas Locales formen parte de la infraestructura AWS global, todos los datos que fluyen por la red AWS global se cifran automáticamente en la capa física antes de salir de las instalaciones AWS seguras. Si tiene requisitos específicos para cifrar los datos en tránsito entre sus ubicaciones locales y acceder Direct Connect PoPs a una zona local, puede habilitar la seguridad MAC (MACsec) entre el router o conmutador local y el terminal. Direct Connect Para obtener más información, consulte la AWS entrada del blog Cómo añadir la seguridad MACsec a las conexiones. Direct Connect

Eliminación de datos

Al detener o cerrar una instancia EC2 en AWS Outposts, 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. La eliminación de datos del hardware de Outpost implica el uso de hardware especializado. El NSK es un dispositivo pequeño, ilustrado en la siguiente fotografía, que se conecta a la parte frontal de cada unidad de cómputo o almacenamiento de un Outpost. Está diseñado para proporcionar un mecanismo que evite que sus datos queden expuestos desde su centro de datos o sitio de colocación. Los datos del dispositivo Outpost se protegen envolviendo el material de codificación utilizado para cifrar el dispositivo y almacenándolo en el NSK. Cuando

devuelves un anfitrión de Outpost, destruyes el NSK girando un pequeño tornillo en el chip que aplasta al NSK y lo destruye físicamente. Al destruir el NSK, se destruyen criptográficamente los datos de tu Outpost.



Identity and Access Management

AWS Identity and Access Management (IAM) es un dispositivo Servicio de AWS que ayuda al administrador a controlar de forma segura el acceso a los recursos. AWS Los administradores de IAM controlan quién puede autenticarse (iniciar sesión) y quién puede autorizarse (tener permisos) para usar los recursos. AWS Outposts Si tiene uno Cuenta de AWS, puede utilizar IAM sin coste adicional.

En la siguiente tabla se enumeran las funciones de IAM con las que puede utilizar. AWS Outposts

Característica de IAM	AWS Outposts soporte
Identity-based políticas	Sí
Resource-based políticas	Sí*
Acciones de políticas	Sí
Recursos de políticas	Sí
Claves de condición de política (específicas del servicio)	Sí
Listas de control de acceso (ACL)	No

Característica de IAM	AWS Outposts soporte
Attribute-based control de acceso (ABAC) (etiquetas en las políticas)	Sí
Credenciales temporales	Sí
Permisos de entidades principales	Sí
Roles de servicio	No
Service-linked roles	Sí

* Además de las políticas de IAM basadas en la identidad, Amazon S3 on Outposts admite políticas de bucket y de puntos de acceso. Se trata de políticas basadas en recursos que se adjuntan al recurso Amazon S3 on Outposts.

Para obtener más información sobre cómo se admiten estas funciones AWS Outposts, consulte la guía del AWS Outposts usuario.

Seguridad de la infraestructura

La protección de la infraestructura representa una parte clave de un programa de seguridad de la información. Garantiza que los sistemas y servicios de carga de trabajo estén protegidos contra el acceso no deseado y no autorizado y contra posibles vulnerabilidades. Por ejemplo, se definen los límites de confianza (por ejemplo, los límites de la red y la cuenta), la configuración y el mantenimiento de la seguridad del sistema (por ejemplo, el refuerzo, la minimización y la aplicación de parches), la autenticación y las autorizaciones del sistema operativo (por ejemplo, los usuarios, las claves y los niveles de acceso) y otros puntos de aplicación de políticas adecuados (por ejemplo, firewalls de aplicaciones web o puertas de enlace de API).

AWS proporciona varios enfoques para la protección de la infraestructura, tal como se explica en las siguientes secciones.

Protección de redes

Sus usuarios pueden ser parte de su fuerza laboral o de sus clientes, y pueden estar ubicados en cualquier lugar. Por este motivo, no puede confiar en todos los que tienen acceso a su red. Si sigue

el principio de aplicar la seguridad en todos los niveles, emplea un enfoque de confianza cero. En el modelo de seguridad de confianza cero, los componentes de las aplicaciones o los microservicios se consideran discretos y ningún componente o microservicio confía en ningún otro componente o microservicio. Para lograr una seguridad de confianza cero, siga estas recomendaciones:

- Cree capas de red. Las redes en capas ayudan a agrupar de forma lógica componentes de red similares. También reducen el alcance potencial del impacto del acceso no autorizado a la red.
- Controle las capas de tráfico. Aplica varios controles con un enfoque de defensa exhaustivo tanto para el tráfico entrante como para el saliente. Esto incluye el uso de grupos de seguridad (firewalls de inspección de estado), ACL de red, subredes y tablas de enrutamiento.
- Implemente la inspección y la protección. Inspeccione y filtre su tráfico en cada capa. Puede inspeccionar las configuraciones de su VPC para detectar posibles accesos no deseados mediante Network Access Analyzer. Puede especificar sus requisitos de acceso a la red e identificar las posibles rutas de red que no los cumplan.

Proteger los recursos informáticos

Los recursos informáticos incluyen instancias EC2, contenedores, AWS Lambda funciones, servicios de bases de datos, dispositivos de IoT y más. Cada tipo de recurso informático requiere un enfoque de seguridad diferente. Sin embargo, estos recursos comparten estrategias comunes que debe tener en cuenta: una defensa exhaustiva, la gestión de vulnerabilidades, la reducción de la superficie de ataque, la automatización de la configuración y el funcionamiento y la realización de acciones a distancia.

Esta es una guía general para proteger los recursos informáticos de los servicios clave:

- Cree y mantenga un programa de gestión de vulnerabilidades. Escanee y aplique parches con regularidad a recursos como instancias EC2, contenedores de Amazon Elastic Container Service (Amazon ECS) y cargas de trabajo de Amazon Elastic Kubernetes Service (Amazon EKS).
- Automatice la protección informática. Automatice sus mecanismos informáticos de protección, incluida la gestión de vulnerabilidades, la reducción de la superficie de ataque y la gestión de los recursos. Esta automatización libera tiempo que puede utilizar para proteger otros aspectos de su carga de trabajo y ayuda a reducir el riesgo de errores humanos.
- Reduzca la superficie de ataque. Reduzca su exposición al acceso no deseado reforzando sus sistemas operativos y minimizando los componentes, las bibliotecas y los servicios consumibles externos que utiliza.

Además, para cada uno de los Servicio de AWS que utilice, consulte las recomendaciones de seguridad específicas de la documentación del servicio.

Acceso a Internet

AWS Outposts Tanto las Zonas Locales como las Zonas Locales proporcionan patrones arquitectónicos que permiten a sus cargas de trabajo acceder desde y hacia Internet. Cuando utilices estos patrones, considera que el consumo de Internet desde la región es una opción viable solo si lo utilizas para aplicar parches, actualizar, acceder a repositorios de Git externos y AWS situaciones similares. Para este patrón arquitectónico, se aplican los conceptos de inspección centralizada de entradas y salida centralizada de Internet. Estos patrones de acceso utilizan puertas de enlace NAT AWS Transit Gateway, firewalls de red y otros componentes que residen en las Zonas Locales Regiones de AWS, pero que están conectados a AWS Outposts ellas a través de la ruta de datos entre la Región y el perímetro.

Las Zonas Locales adoptan una construcción de red denominada grupo fronterizo de red, que se utiliza en Regiones de AWS. AWS anuncia las direcciones IP públicas de estos grupos únicos. Un grupo fronterizo de red se compone de Availability Zones, Local Zones o Wavelength Zones. Puede asignar explícitamente un conjunto de direcciones IP públicas para su uso en un grupo fronterizo de red. Puede usar un grupo fronterizo de red para extender la puerta de enlace de Internet a las Zonas Locales al permitir que el grupo sirva direcciones IP elásticas. Esta opción requiere que implemente otros componentes para complementar los servicios principales disponibles en las Zonas Locales. Estos componentes pueden provenir de los ISV y ayudarle a crear capas de inspección en su zona local, tal y como se describe en la entrada del AWS blog Arquitecturas de inspección híbridas con. Zonas locales de AWS

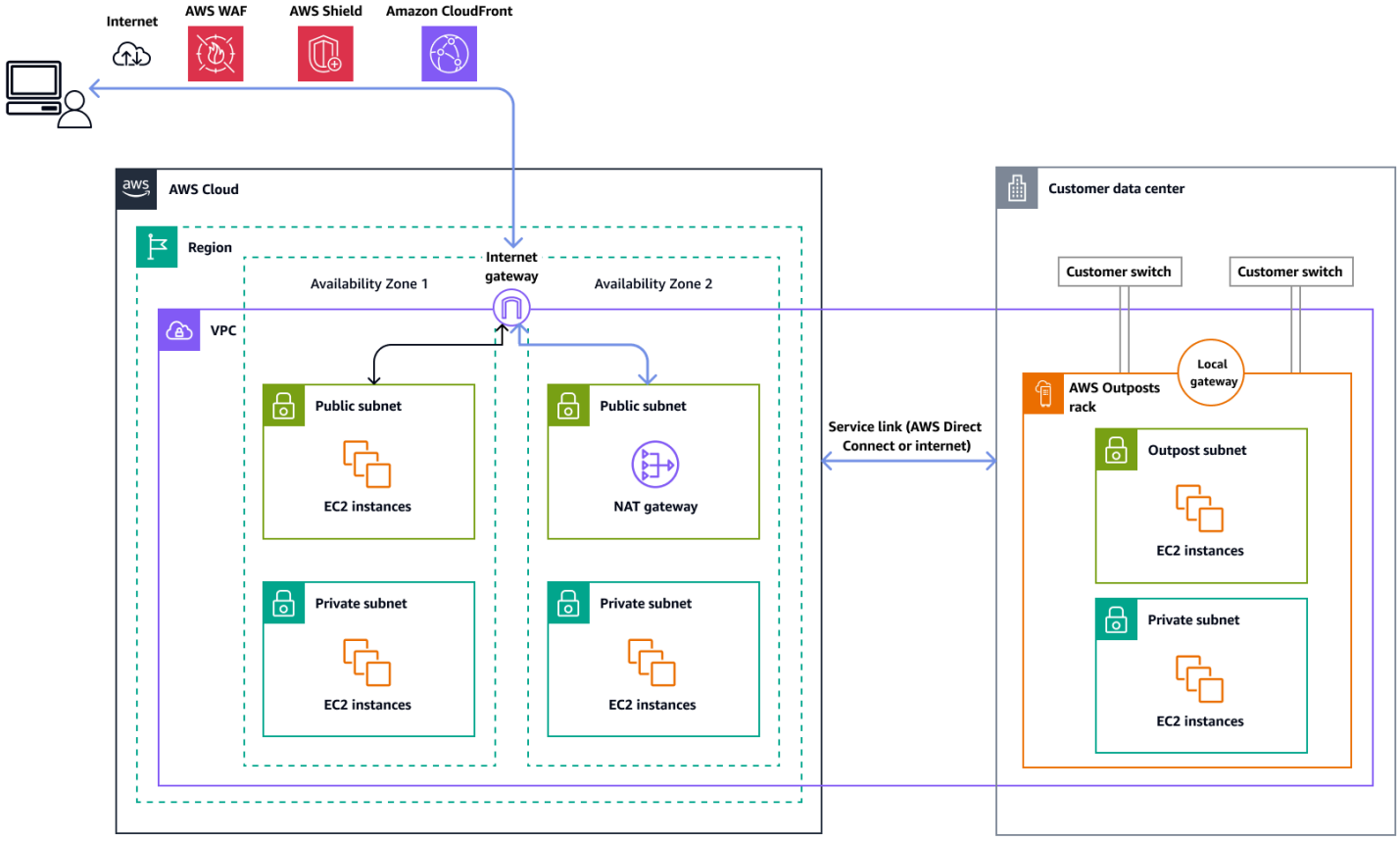
En AWS Outposts, si desea utilizar la puerta de enlace local (LGW) para conectarse a Internet desde su red, debe modificar la tabla de enrutamiento personalizada asociada a la subred. AWS Outposts La tabla de rutas debe tener una entrada de ruta predeterminada (0.0.0). 0/0) que usa la LGW como siguiente salto. Usted es responsable de implementar el resto de los controles de seguridad en su red local, incluidas las defensas perimetrales, como los firewalls y los sistemas de prevención o detección de intrusos (). IPS/IDS Esto se alinea con el modelo de responsabilidad compartida, que divide las tareas de seguridad entre usted y el proveedor de la nube.

Acceso a Internet a través del progenitor Región de AWS

En esta opción, las cargas de trabajo del Outpost acceden a Internet a través del enlace de servicio y la pasarela de Internet del servidor principal. Región de AWS El tráfico saliente a Internet se puede

enrutar a través de la puerta de enlace NAT que está instanciada en la VPC. Para mayor seguridad para su tráfico de entrada y salida, puede utilizar servicios de AWS seguridad como AWS WAF AWS Shield, y Amazon CloudFront en el. Región de AWS

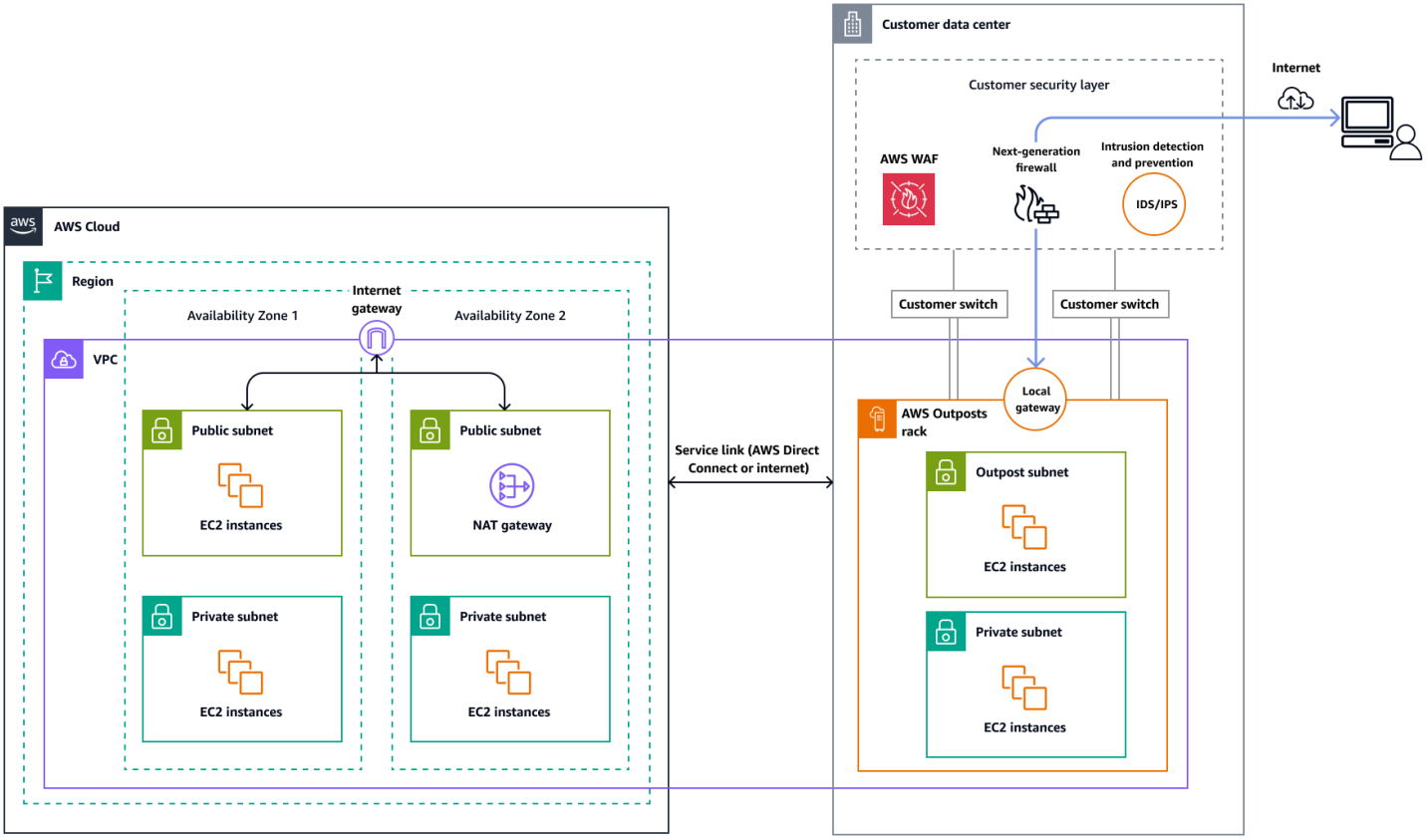
En el siguiente diagrama se muestra el tráfico entre la carga de trabajo de la AWS Outposts instancia e Internet que pasa por la instancia principal. Región de AWS



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

En esta opción, las cargas de trabajo del Outpost acceden a Internet a través del centro de datos local. El tráfico de carga de trabajo que accede a Internet pasa por el punto de presencia local de Internet y sale de forma local. En este caso, la infraestructura de seguridad de la red del centro de datos local es responsable de proteger el AWS Outposts tráfico de carga de trabajo.

La siguiente imagen muestra el tráfico entre una carga de trabajo de la AWS Outposts subred e Internet que pasa por un centro de datos.



Gobernanza de la infraestructura

Independientemente de si sus cargas de trabajo se despliegan en una Región de AWS zona local o en un puesto avanzado, puede utilizarlas AWS Control Tower para la gobernanza de la infraestructura. AWS Control Tower ofrece una forma sencilla de configurar y gobernar un entorno de AWS múltiples cuentas, siguiendo las mejores prácticas prescriptivas. AWS Control Tower organiza las capacidades de varios otros Servicios de AWS AWS Organizations AWS Service Catalog, incluido el IAM Identity Center (consulte todos los servicios integrados) para crear una landing zone en menos de una hora. Los recursos se configuran y administran en su nombre.

AWS Control Tower proporciona una gobernanza unificada en todos los AWS entornos, incluidas las Regiones, las Zonas Locales (extensiones de baja latencia) y los Outposts (infraestructura local). Esto ayuda a garantizar una seguridad y un cumplimiento uniformes en toda la arquitectura de nube híbrida. Para obtener más información, consulte la Documentación de AWS Control Tower.

Puede configurar AWS Control Tower funciones como barreras de protección para cumplir con los requisitos de residencia de datos de los gobiernos y los sectores regulados, como las instituciones de

servicios financieros (FSI). Para saber cómo implementar barandas para la residencia de datos en la periferia, consulte lo siguiente:

- Mejores prácticas para gestionar la residencia de datos Zonas locales de AWS mediante el uso de controles de landing zone (AWS entrada del blog)
- Diseño de arquitectura para la residencia de datos con barandas de AWS Outposts estanterías y zonas de landing zone (AWS entrada del blog)
- Residencia de datos desde el punto de vista de los servicios de nube híbrida (documentación de Framework)AWS Well-Architected

Compartir los recursos de Outposts

Dado que un Outpost es una infraestructura finita que se encuentra en su centro de datos o en un espacio compartido, para una gobernanza centralizada AWS Outposts, es necesario controlar de forma centralizada con qué cuentas se comparten AWS Outposts los recursos.

Al compartir Outpost, los propietarios de Outpost pueden compartir sus Outposts y recursos de Outpost, incluidos los sitios y subredes de Outpost, con otros Cuentas de AWS que estén en la misma organización. AWS Organizations Como propietario de Outpost, puedes crear y administrar los recursos de Outpost desde una ubicación central y compartir los recursos entre varios miembros de tu organización. Cuentas de AWS AWS Esto permite a otros consumidores utilizar los sitios de Outpost, configurar las VPC y lanzar y ejecutar instancias en el Outpost compartido.

Los recursos que se pueden compartir son: AWS Outposts

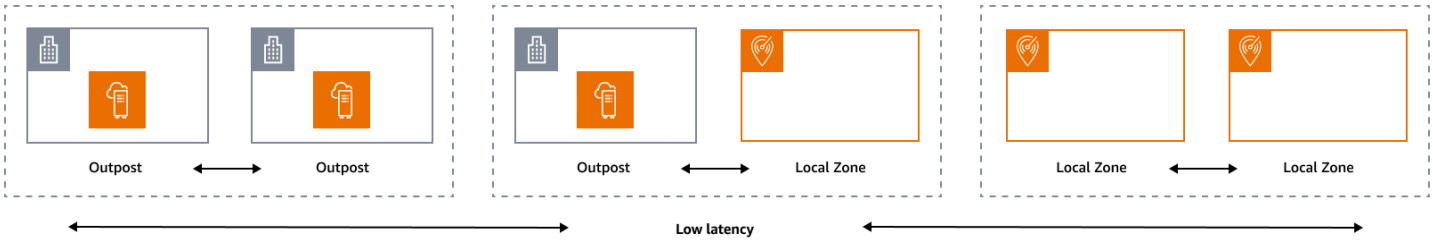
- Anfitriones dedicados asignados
- Reservas de capacidad
- Customer-owned Grupos de direcciones IP (CoIP)
- Tabla de enrutamiento de la puerta de enlace local
- Outposts
- Amazon S3 en Outposts
- Sitios
- Subredes

Para seguir las prácticas recomendadas para compartir los recursos de Outposts en un entorno de varias cuentas, consulta las siguientes AWS entradas de blog:

- Compartir AWS Outposts en un AWS entorno de varias cuentas: primera parte
- Compartir AWS Outposts en un AWS entorno de múltiples cuentas: parte 2

Resiliencia en la periferia

El pilar de la fiabilidad abarca la capacidad de una carga de trabajo para realizar la función prevista de forma correcta y coherente cuando se espera que lo haga. Esto incluye la capacidad de operar y probar la carga de trabajo durante todo su ciclo de vida. En este sentido, cuando diseñe una arquitectura resiliente en la periferia, primero debe considerar qué infraestructuras utilizará para implementar esa arquitectura. Existen tres combinaciones posibles que se pueden implementar utilizando Zonas locales de AWS y AWS Outposts: de Outpost a Outpost, de Outpost a zona local y de zona local a zona local, como se muestra en el siguiente diagrama. Si bien existen otras posibilidades de arquitecturas resilientes, como la combinación de servicios AWS perimetrales con la infraestructura local tradicional Regiones de AWS, esta guía se centra en estas tres combinaciones que se aplican al diseño de servicios de nube híbrida



Consideraciones sobre infraestructura

En AWS resumen, uno de los principios fundamentales del diseño de servicios es evitar puntos únicos de falla en la infraestructura física subyacente. Debido a este principio, el AWS software y los sistemas utilizan varias zonas de disponibilidad y son resistentes a los fallos de una sola zona. At the Edge, AWS ofrece infraestructuras basadas en Zonas Locales y Outposts. Por lo tanto, un factor fundamental para garantizar la resiliencia en el diseño de la infraestructura es definir dónde se despliegan los recursos de una aplicación.

Zonas locales

Las zonas locales actúan de manera similar a las zonas de disponibilidad dentro de ellas Región de AWS, ya que se pueden seleccionar como ubicación de ubicación para AWS los recursos zonales, como las subredes y las instancias de EC2. Sin embargo, no están ubicadas en un centro poblacional Región de AWS, industrial y de TI, sino cerca de ellos, donde no Región de AWS existen

en la actualidad. A pesar de ello, siguen manteniendo conexiones seguras y con un gran ancho de banda entre las cargas de trabajo locales de la zona local y las cargas de trabajo que se ejecutan en la misma. Región de AWS Por lo tanto, debe usar las Zonas Locales para implementar cargas de trabajo más cerca de sus usuarios para requisitos de baja latencia.

Outposts

AWS Outposts es un servicio totalmente gestionado que extiende la AWS infraestructura Servicios de AWS, las API y las herramientas a su centro de datos. La misma infraestructura de hardware que se utiliza en el Nube de AWS está instalada en su centro de datos. Los Outposts se conectan entonces a los más cercanos. Región de AWS Puedes usar Outposts para respaldar tus cargas de trabajo que tienen baja latencia o requisitos de procesamiento de datos local.

Zonas de disponibilidad principales

Cada zona local o puesto avanzado tiene una región principal (también denominada región de origen). La región principal es donde está anclado el plano de control de la infraestructura AWS perimetral (puesto avanzado o zona local). En el caso de las Zonas Locales, la región principal es un componente arquitectónico fundamental de una Zona Local y los clientes no pueden modificarla. AWS Outposts se extiende Nube de AWS a su entorno local, por lo que debe seleccionar una región y una zona de disponibilidad específicas durante el proceso de pedido. Esta selección ancla el plano de control de tu despliegue de Outposts a la AWS infraestructura elegida.

Al desarrollar arquitecturas de alta disponibilidad en la periferia, la región principal de estas infraestructuras, como Outposts o Local Zones, debe ser la misma, de modo que se pueda extender una VPC entre ellas. Esta VPC extendida es la base para crear estas arquitecturas de alta disponibilidad. Al definir una arquitectura altamente resiliente, es por eso que debe validar la región principal y la zona de disponibilidad de la región en la que estará (o estará) anclado el servicio. Como se ilustra en el siguiente diagrama, si deseas implementar una solución de alta disponibilidad entre dos Outposts, debes elegir dos zonas de disponibilidad diferentes para anclar los Outposts. Esto permite crear una Multi-AZ arquitectura desde la perspectiva del plano de control. Si desea implementar una solución de alta disponibilidad que incluya una o más Zonas Locales, primero debe validar la Zona de disponibilidad principal en la que está anclada la infraestructura. Para ello, utilice el siguiente AWS CLI comando:

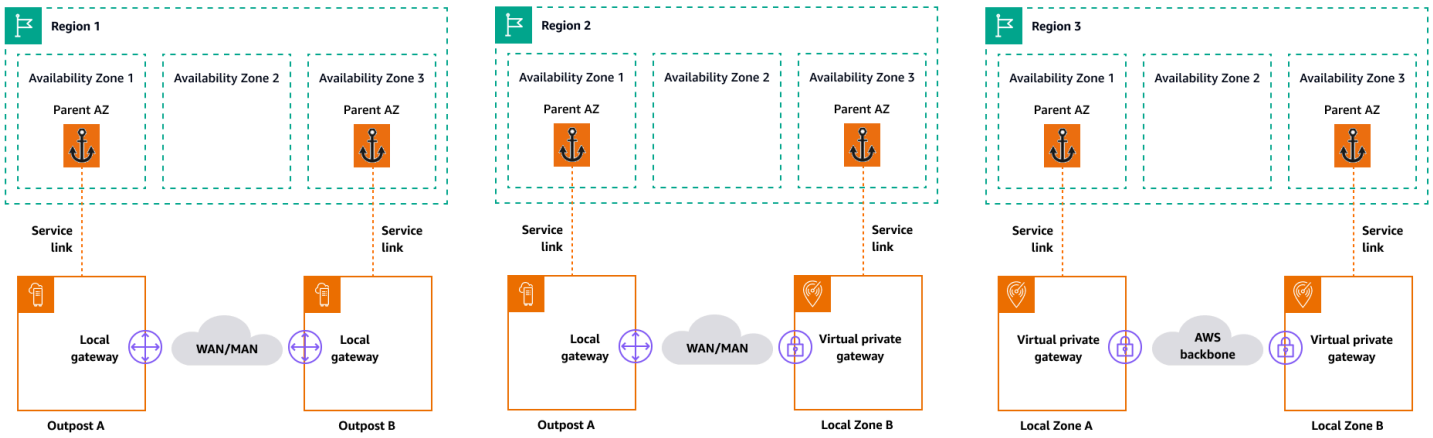
```
aws ec2 describe-availability-zones --zone-ids use1-mia1-az1
```

Resultado del comando anterior:

```
{     "AvailabilityZones": [
          {
              "State": "available",
              "OptInStatus": "opted-in",
              "Messages": [],
              "RegionName": "us-east-1",
              "ZoneName": "us-east-1-mia-1a",
              "ZoneId": "use1-mia1-az1",
              "GroupName": "us-east-1-mia-1",
              "NetworkBorderGroup": "us-east-1-mia-1",
              "ZoneType": "local-zone",
              "ParentZoneName": "us-east-1d",
              "ParentZoneId": "use1-az2"
          }
      ]
 }
```


En este ejemplo, la zona local de Miami (`us-east-1d-mia-1a1`) está anclada en la zona de `us-east-1d-az2` disponibilidad. Por lo tanto, si necesita crear una arquitectura resiliente en la periferia, debe asegurarse de que la infraestructura secundaria (Outposts o Zonas Locales) esté anclada a una zona de disponibilidad distinta de. **`us-east-1d-az2`** Por ejemplo, `us-east-1d-az1` sería válido.

El siguiente diagrama proporciona ejemplos de infraestructuras perimetrales de alta disponibilidad.



Consideraciones sobre redes

En esta sección se analizan las consideraciones iniciales sobre las redes periféricas, principalmente en lo que respecta a las conexiones de acceso a la infraestructura perimetral. Repasa las arquitecturas válidas que proporcionan una red resiliente para el enlace de servicio.

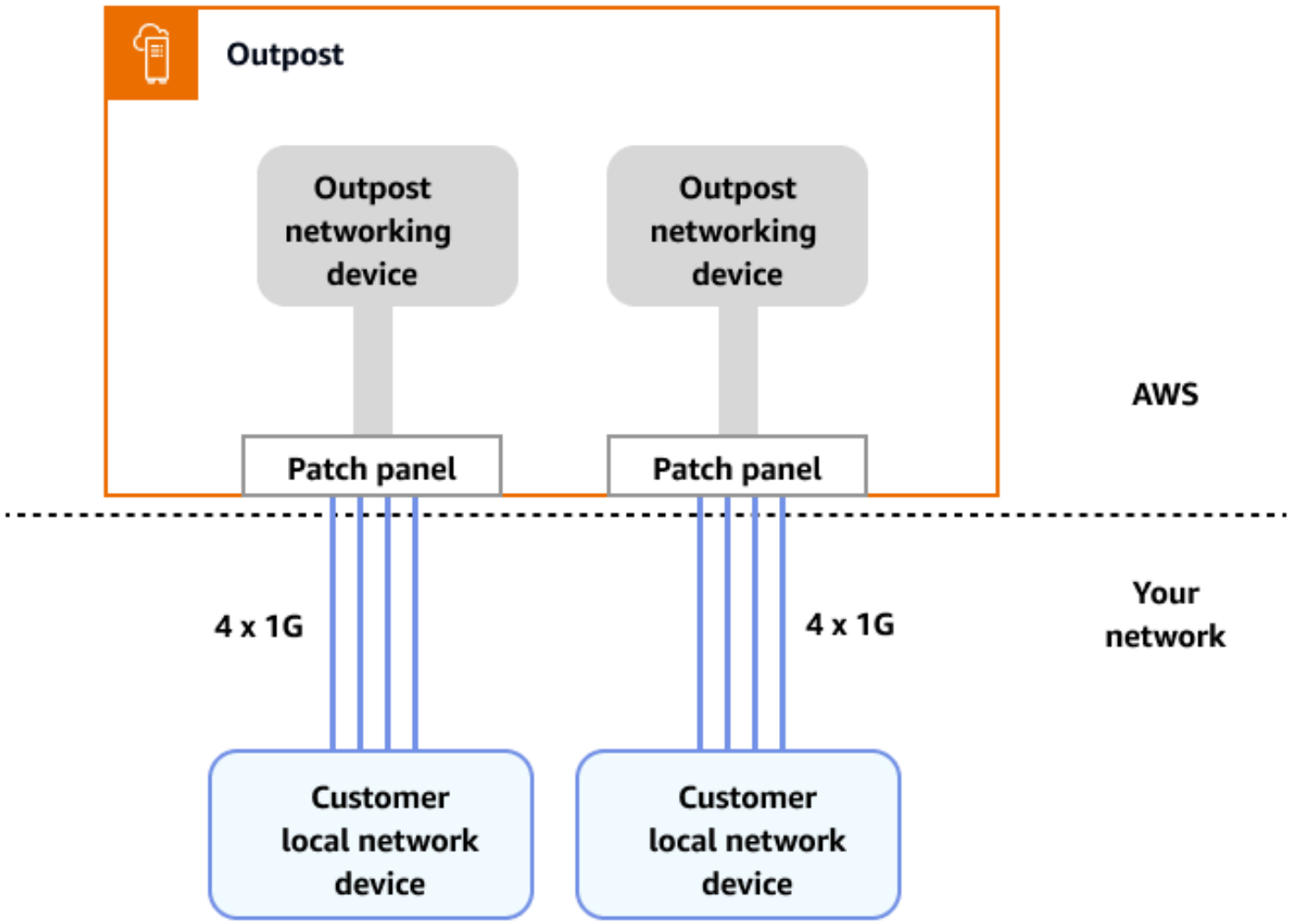
Redes de resiliencia para Zonas Locales

Las Zonas Locales están conectadas a la región principal mediante enlaces múltiples, redundantes, seguros y de alta velocidad que le permiten utilizar cualquier servicio regional, como Amazon S3 y Amazon RDS, sin problemas. Usted es responsable de proporcionar conectividad desde su entorno local o sus usuarios a la zona local. Independientemente de la arquitectura de conectividad que elija (por ejemplo, VPN o VPN Direct Connect), la latencia que debe lograrse a través de los enlaces de red debe ser equivalente para evitar cualquier impacto en el rendimiento de la aplicación en caso de que se produzca un fallo en un enlace principal. Si la utiliza Direct Connect, las arquitecturas de resiliencia aplicables son las mismas que las utilizadas para acceder a una Región de AWS, tal y como se documenta en las recomendaciones de Direct Connect resiliencia. Sin embargo, hay escenarios que se aplican principalmente a las Zonas Locales internacionales. En el país donde la zona local está habilitada, tener un solo Direct Connect PoP hace que sea imposible crear las arquitecturas recomendadas para la Direct Connect resiliencia. Si tiene acceso a una sola Direct Connect ubicación o necesita resiliencia más allá de una sola conexión, puede crear un dispositivo VPN en Amazon EC2 Direct Connect y, como se ilustra y analiza en AWS la entrada del blog, habilitar la conectividad de alta disponibilidad desde las instalaciones hasta. Zonas locales de AWS

Redes de resiliencia para Outposts

A diferencia de las Zonas Locales, los Outposts tienen conectividad redundante para acceder a las cargas de trabajo desplegadas en Outposts desde tu red local. Esta redundancia se logra a través de dos dispositivos de red Outposts (OND). Cada OND requiere al menos dos conexiones de fibra a 1 Gbps, 10 Gbps, 40 Gbps o 100 Gbps a su red local. Estas conexiones deben configurarse como un grupo de agregación de enlaces (LAG) para permitir la adición escalable de más enlaces.

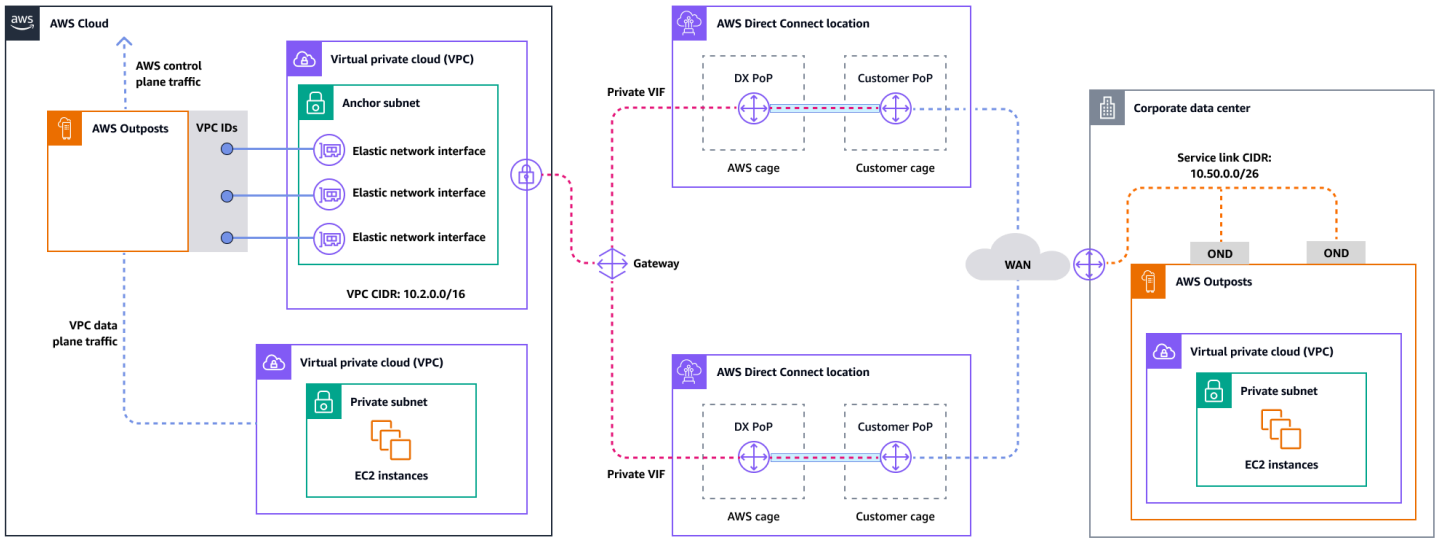
Velocidad de enlace ascendente	Número de enlaces ascendentes
1 Gbps	1, 2, 4, 6 o 8
10 Gbps	1, 2, 4, 8, 12 o 16
40 o 100 Gbps	1, 2 o 4



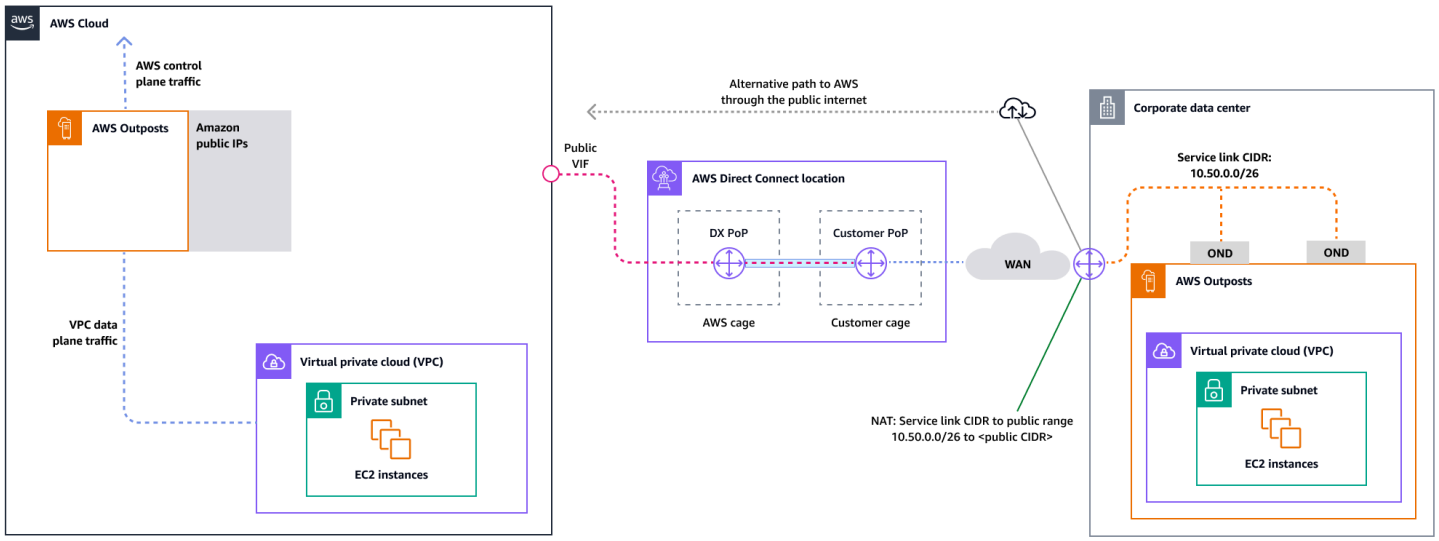
Para obtener más información sobre esta conectividad, consulta Conectividad de red local para Outposts Racks en la documentación. AWS Outposts

Para una experiencia y una resiliencia óptimas, se AWS recomienda utilizar una conectividad redundante de al menos 500 Mbps (1 Gbps es mejor) para la conexión de enlace de servicio al. Región de AWS Puede utilizar Direct Connect una conexión a Internet para el enlace de servicio. Este mínimo le permite lanzar instancias EC2, adjuntar volúmenes de EBS y acceder a ellas Servicios de AWS, como Amazon EKS, Amazon EMR y métricas. CloudWatch

El siguiente diagrama ilustra esta arquitectura para una conexión privada de alta disponibilidad.



El siguiente diagrama ilustra esta arquitectura para una conexión pública de alta disponibilidad.



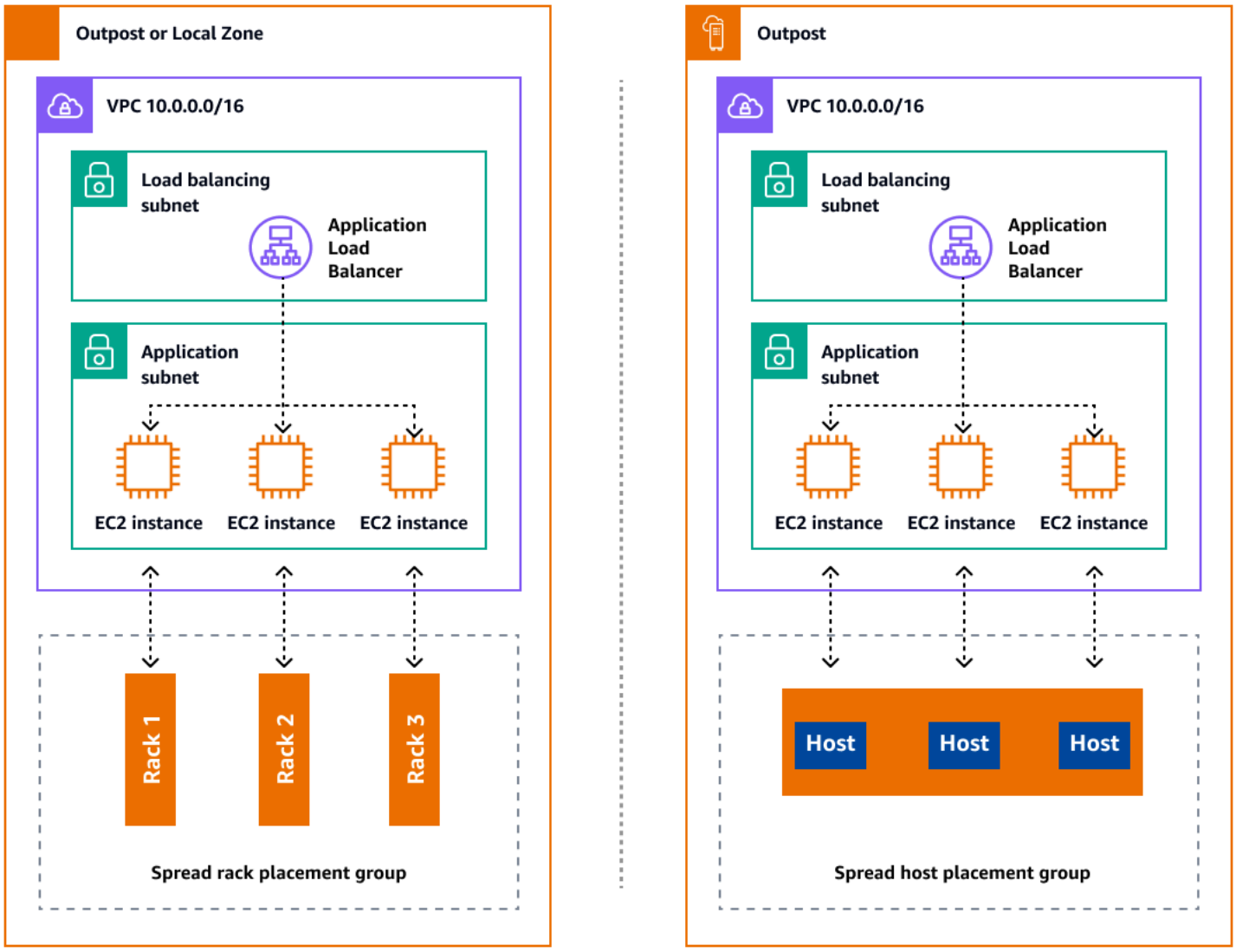
Escalar las implementaciones de racks de Outposts con racks ACE

El rack Aggregation, Core, Edge (ACE) sirve como punto de agregación crítico para las implementaciones de AWS Outposts varios racks y se recomienda principalmente para instalaciones que superen los tres racks o para planificar una futura expansión. Cada rack ACE cuenta con cuatro enrutadores que admiten conexiones de 10 Gbps, 40 Gbps y 100 Gbps (100 Gbps es lo óptimo). Cada rack se puede conectar a hasta cuatro dispositivos de cliente ascendentes para obtener la máxima redundancia. Los racks ACE consumen hasta 10 kVA de energía y pesan hasta 705 libras. Los beneficios clave incluyen una reducción de los requisitos de redes físicas, menos enlaces ascendentes de cableado de fibra y una disminución de las interfaces virtuales de VLAN. AWS supervisa estos racks mediante datos de telemetría a través de túneles VPN y trabaja en

estrecha colaboración con los clientes durante la instalación para garantizar una disponibilidad de energía adecuada, una configuración de red y una ubicación óptima. La arquitectura de rack ACE proporciona un valor cada vez mayor a medida que las implementaciones se amplían y simplifica de forma eficaz la conectividad, a la vez que reduce la complejidad y los requisitos de puertos físicos en instalaciones de mayor tamaño. Para obtener más información, consulte la AWS entrada del blog Cómo escalar las implementaciones en AWS Outposts rack con ACE Rack.

Distribución de instancias en Outposts y Zonas Locales

Los Outposts y las Zonas Locales tienen un número finito de servidores de cómputo. Si la aplicación implementa varias instancias relacionadas, estas instancias podrían implementarse en el mismo servidor o en servidores del mismo rack, a menos que estén configuradas de forma diferente. Además de las opciones predeterminadas, puede distribuir las instancias entre los servidores para mitigar el riesgo de ejecutar instancias relacionadas en la misma infraestructura. También puede distribuir las instancias en varios racks mediante grupos de ubicación de particiones. Esto se denomina modelo de distribución de racks dispersos. Utilice la distribución automática para distribuir las instancias entre las particiones del grupo o despliegue las instancias en las particiones de destino seleccionadas. Al implementar instancias en las particiones de destino, puede implementar los recursos seleccionados en el mismo rack y, al mismo tiempo, distribuir otros recursos entre los racks. Outposts también ofrece otra opción llamada spread host que te permite distribuir tu carga de trabajo a nivel de anfitrión. En el siguiente diagrama se muestran las opciones de distribución por rack y por servidor de dispersión.



Amazon RDS en Multi-AZ AWS Outposts

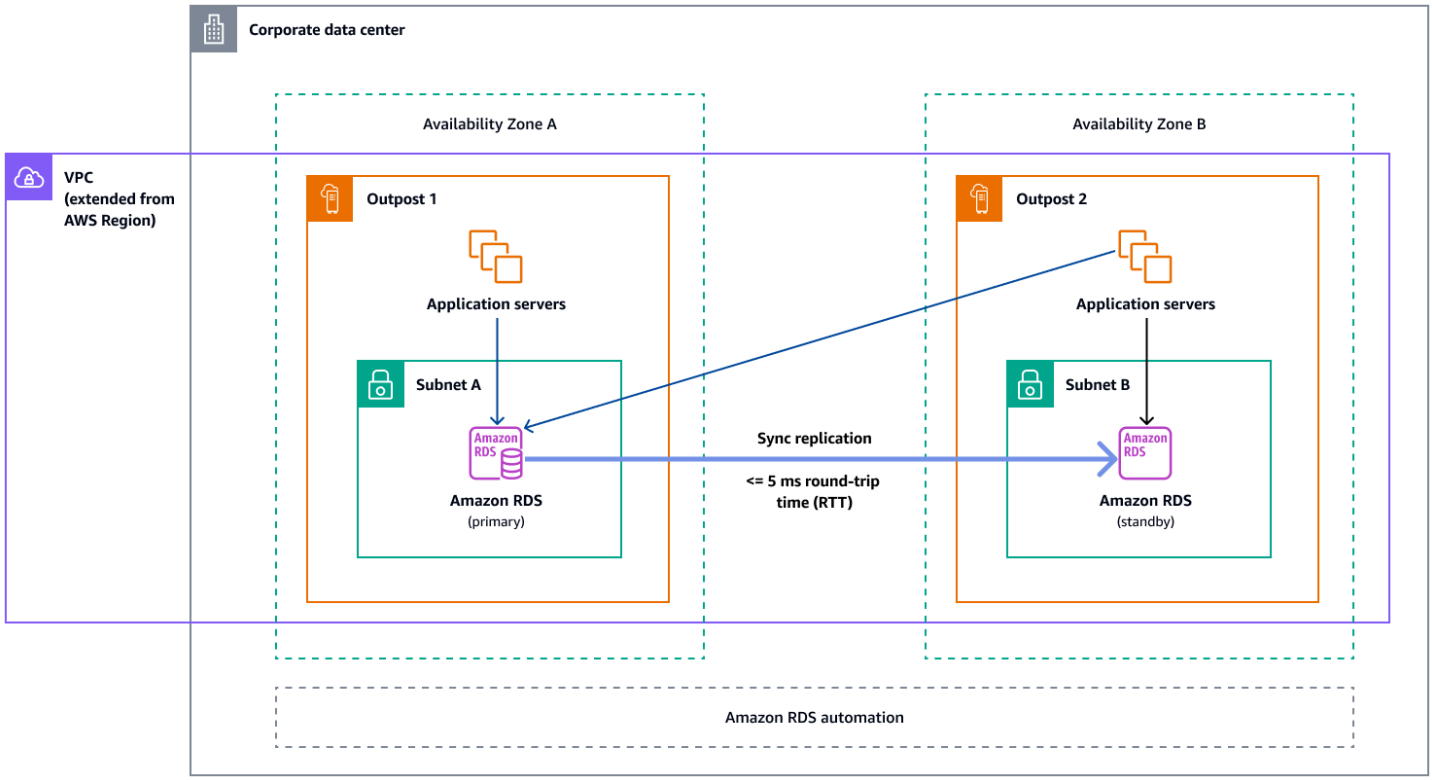
Cuando utiliza despliegues de Multi-AZ instancias en Outposts, Amazon RDS crea dos instancias de base de datos en dos Outposts. Cada Outpost se ejecuta en su propia infraestructura física y se conecta a diferentes zonas de disponibilidad de una región para ofrecer una alta disponibilidad. Cuando dos Outposts se conectan a través de una conexión local gestionada por el cliente, Amazon RDS gestiona la replicación sincrónica entre las instancias de base de datos principal y en espera. En caso de que se produzca un error en el software o la infraestructura, Amazon RDS promoverá automáticamente la instancia en espera a la función principal y actualizará el registro DNS para que apunte a la nueva instancia principal. Para Multi-AZ las implementaciones, Amazon RDS crea una instancia de base de datos principal en un Outpost y replica los datos de forma sincrónica en una

instancia de base de datos en espera en un Outpost diferente. Multi-AZ los despliegues en Outposts funcionan Multi-AZ como los despliegues Regiones de AWS en, con las siguientes diferencias:

- Requieren una conexión local entre dos o más Outposts.
- Requieren grupos de direcciones IP (CoIP) propiedad del cliente. Para obtener más información, consulte las direcciones Customer-owned IP de Amazon RDS AWS Outposts en la documentación de Amazon RDS.
- La replicación se ejecuta en la red local.

Multi-AZ las implementaciones están disponibles para todas las versiones compatibles de MySQL y PostgreSQL en Amazon RDS en Outposts. Las copias de seguridad locales no son compatibles con las implementaciones. Multi-AZ

El siguiente diagrama muestra la arquitectura de Amazon RDS en las configuraciones de Multi-AZ Outposts.

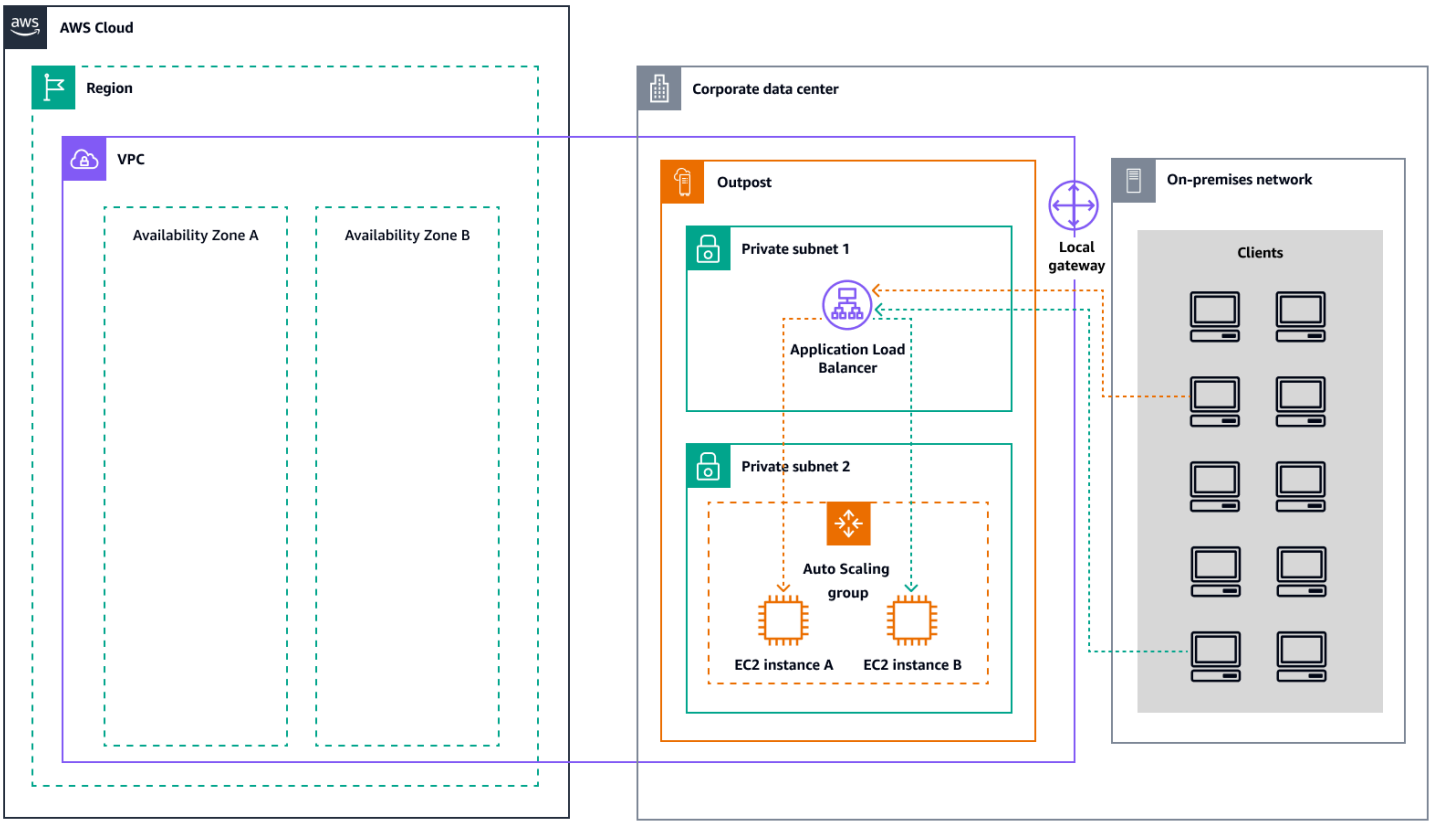


Mecanismos de conmutación por error

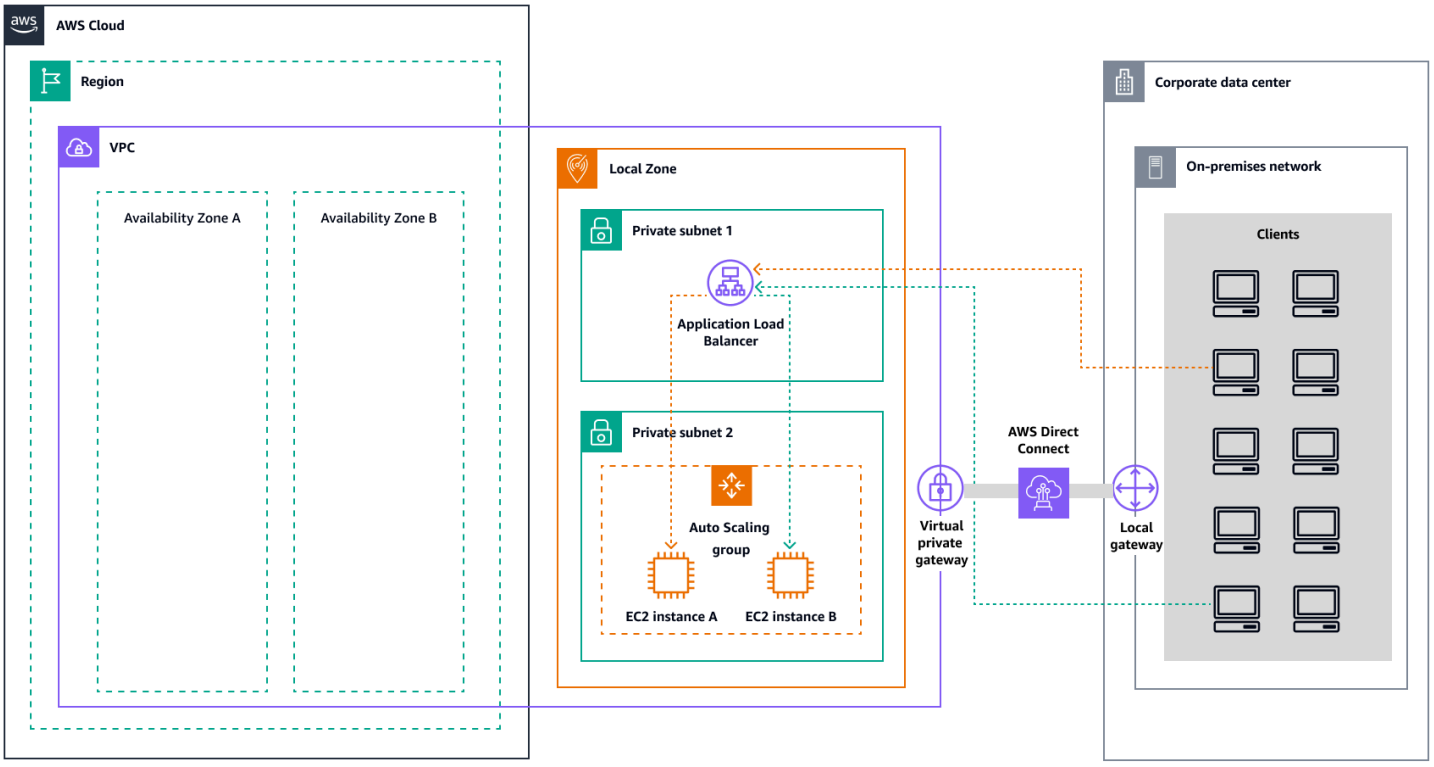
Equilibrio de carga y escalado automático

Elastic Load Balancing (ELB) distribuye automáticamente el tráfico entrante de las aplicaciones entre todas las instancias de EC2 que esté ejecutando. ELB ayuda a administrar las solicitudes entrantes al enrutar el tráfico de manera óptima para que ninguna instancia se vea sobrecargada. Para usar ELB con su grupo de Auto Scaling de Amazon EC2, adjunte el balanceador de carga a su grupo de Auto Scaling. Esto registra el grupo en el balanceador de carga, que actúa como punto de contacto único para todo el tráfico web entrante a su grupo. Cuando usa ELB con su grupo de Auto Scaling, no es necesario registrar instancias EC2 individuales en el balanceador de carga. Las instancias lanzadas por el grupo de Auto Scaling se registran automáticamente en el balanceador de carga. Del mismo modo, las instancias canceladas por su grupo de Auto Scaling se cancelan automáticamente del balanceador de cargas. Después de adjuntar un balanceador de cargas a su grupo de Auto Scaling, puede configurar su grupo para que use métricas de ELB (como el recuento de solicitudes del Application Load Balancer por destino) para escalar el número de instancias del grupo a medida que fluctúa la demanda. Si lo desea, puede añadir comprobaciones de estado de ELB a su grupo de Auto Scaling para que Amazon EC2 Auto Scaling pueda identificar y sustituir las instancias en mal estado en función de estas comprobaciones de estado. También puedes crear una CloudWatch alarma de Amazon que te notifique si el número de anfitriones en buen estado del grupo objetivo es inferior al permitido.

El siguiente diagrama ilustra cómo un Application Load Balancer gestiona las cargas de trabajo en Amazon EC2 en. AWS Outposts



El siguiente diagrama ilustra una arquitectura similar para Amazon EC2 en las Zonas Locales.

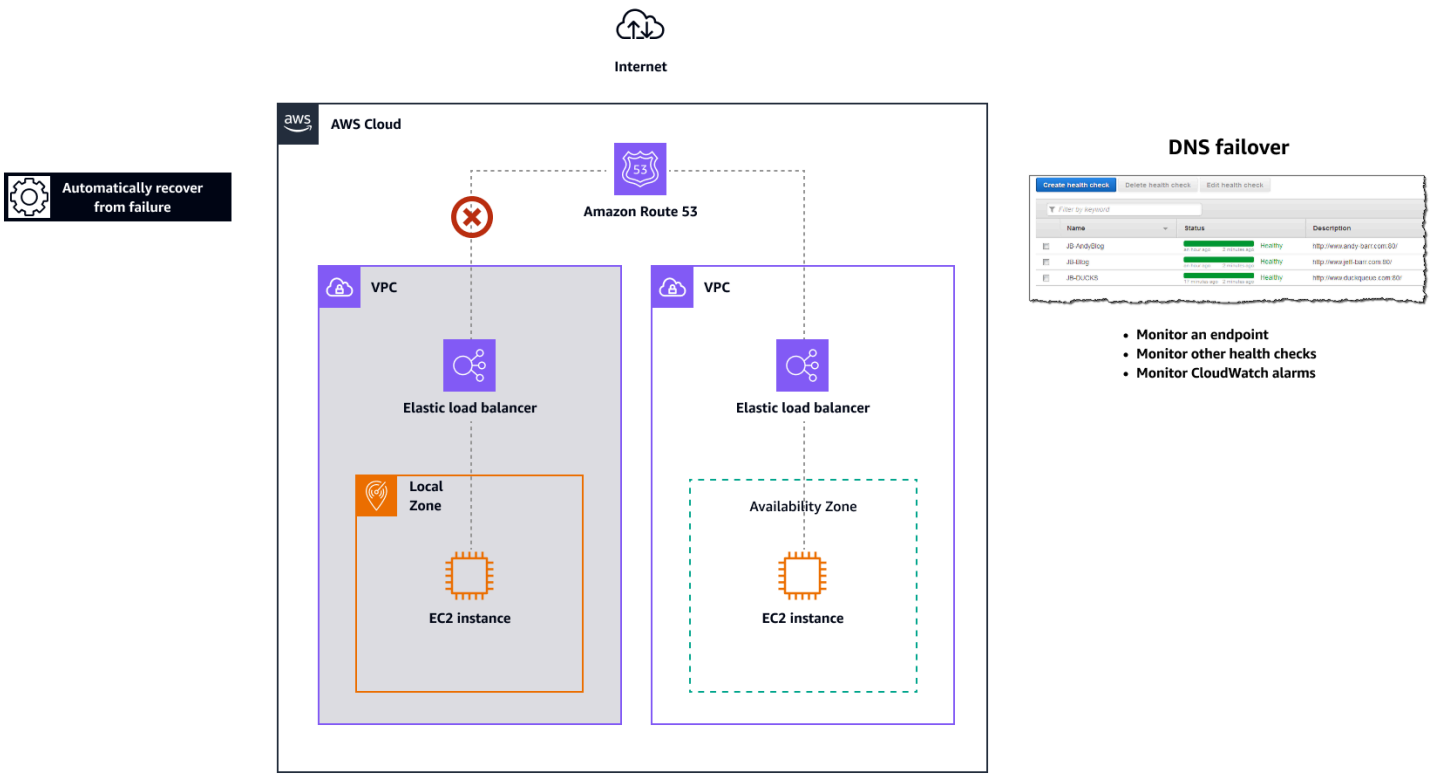


> **Note**
>
> Los balanceadores de carga de aplicaciones están disponibles tanto AWS Outposts en las Zonas Locales como en las Zonas Locales. Sin embargo, para utilizar un Application Load Balancer AWS Outposts, debe dimensionar la capacidad de Amazon EC2 para proporcionar la escalabilidad que requiere el balanceador de carga. Para obtener más información sobre el tamaño de un balanceador de carga AWS Outposts, consulta la entrada del AWS blog Configuring an Application Load Balancer en. AWS Outposts

Amazon Route 53 para conmutación por error de DNS

Si tiene más de un recurso que realiza la misma función (por ejemplo, varios servidores HTTP o de correo), puede configurar Amazon Route 53 para comprobar el estado de sus recursos y responder a las consultas de DNS utilizando únicamente los recursos en buen estado. Por ejemplo, supongamos que su sitio web está alojado en dos `example.com` servidores. Un servidor está en una zona local y el otro en un Outpost. Puede configurar Route 53 para comprobar el estado de esos servidores y responder a las consultas de DNS `example.com` utilizando solo los servidores que están en buen estado actualmente. Si usa registros de alias para enrutar el tráfico a AWS recursos seleccionados, como los balanceadores de carga ELB, puede configurar Route 53 para evaluar el estado del recurso y enrutar el tráfico solo a los recursos que estén en buen estado. Al configurar un registro de alias para evaluar el estado de un recurso, no es necesario crear una comprobación del estado de ese recurso.

El siguiente diagrama ilustra los mecanismos de conmutación por error de Route 53.



Notas

- Si va a crear registros de conmutación por error en una zona alojada privada, puede crear una CloudWatch métrica, asociar una alarma a la métrica y, a continuación, crear una comprobación de estado basada en el flujo de datos de la alarma.
- Para hacer que una aplicación sea accesible públicamente AWS Outposts mediante un Application Load Balancer, configure las configuraciones de red que permitan la traducción de direcciones de red de destino (DNAT) de las IP públicas al nombre de dominio completo (FQDN) del balanceador de cargas y cree una regla de conmutación por error de Route 53 con comprobaciones de estado que apunten a la IP pública expuesta. Esta combinación garantiza un acceso público fiable a la aplicación. Outposts-hosted

Amazon Route 53 Resolver on AWS Outposts

Amazon Route 53 Resolverestá disponible en los estantes de Outposts. Proporciona a tus servicios y aplicaciones locales una resolución de DNS local directamente desde Outposts. Los puntos finales locales de Route 53 Resolver también permiten la resolución de DNS entre Outposts y su servidor

DNS local. Route 53 Resolver on Outposts ayuda a mejorar la disponibilidad y el rendimiento de las aplicaciones locales.

Uno de los casos de uso típicos de Outposts es implementar aplicaciones que requieren acceso de baja latencia a sistemas locales, como equipos de fábrica, aplicaciones comerciales de alta frecuencia y sistemas de diagnóstico médico.

Si opta por utilizar los Resolvers de Route 53 locales en Outposts, las aplicaciones y los servicios seguirán beneficiándose de la resolución de DNS local para detectar otros servicios, incluso si se pierde la conectividad con uno de los Región de AWS padres. Los solucionadores locales también ayudan a reducir la latencia de las resoluciones de DNS, ya que los resultados de las consultas se almacenan en caché y se sirven localmente desde los Outposts, lo que elimina los viajes de ida y vuelta innecesarios al servidor principal. Región de AWS Todas las resoluciones de DNS para las aplicaciones de las VPC de Outposts que utilizan DNS privado se proporcionan de forma local.

Además de habilitar los Resolvers locales, este lanzamiento también habilita los puntos finales de Resolver locales. Los puntos de conexión salientes de Route 53 Resolver permiten a los Route 53 Resolver reenviar las consultas de DNS a los solucionadores de DNS que usted administra, por ejemplo, en la red local. Por el contrario, los puntos finales entrantes de Route 53 Resolver reenvían las consultas de DNS que reciben desde fuera de la VPC al Resolver que se ejecuta en Outposts. Te permite enviar consultas de DNS para servicios desplegados en una VPC privada de Outposts desde fuera de esa VPC. Para obtener más información sobre los puntos de enlace entrantes y salientes, consulte Resolución de consultas de DNS entre las VPC y su red en la documentación de Route 53.

Planificación de la capacidad en la periferia

La fase de planificación de la capacidad implica recopilar los requisitos de vCPU, memoria y almacenamiento para implementar la arquitectura. En el pilar de optimización de costos del AWS Well-Architected Framework, el dimensionamiento correcto es un proceso continuo que comienza con la planificación. Puede utilizar AWS las herramientas para definir las optimizaciones en función del consumo interno de recursos. AWS

La planificación de la capacidad perimetral en las Zonas Locales es la misma que en Regiones de AWS. Asegúrese de que sus instancias estén disponibles en cada zona local, ya que algunos tipos de instancias pueden diferir de los que hay en ellas Regiones de AWS. En el caso de Outposts, debes planificar la capacidad en función de tus requisitos de carga de trabajo. Los Outposts se distribuyen con un número fijo de instancias por host y se pueden redistribuir según sea necesario.

Si sus cargas de trabajo requieren capacidad adicional, téngalo en cuenta a la hora de planificar sus necesidades de capacidad.

Planificación de la capacidad en Outposts

AWS Outposts La planificación de la capacidad requiere insumos específicos para ajustar el tamaño a nivel regional, además de factores específicos de cada sector que afectan a la disponibilidad, el rendimiento y el crecimiento de las aplicaciones. Para obtener una guía detallada, consulte la planificación de la capacidad en el AWS documento técnico Consideraciones sobre arquitectura y diseño de AWS Outposts alta disponibilidad.

Planificación de la capacidad para las Zonas Locales

Una zona local es una extensión de una Región de AWS que se encuentra geográficamente cerca de sus usuarios. Los recursos que se crean en una zona local pueden servir a los usuarios locales con comunicaciones de muy baja latencia. Para habilitar una zona local en tu zona Cuenta de AWS, consulta la AWS documentación sobre cómo empezar Zonas locales de AWS. Cada zona local tiene una distribución diferente disponible para las familias de EC2 instancias. Valide las instancias disponibles en cada zona local antes de usarlas. Para confirmar las EC2 instancias disponibles, ejecuta el siguiente AWS CLI comando:

```
aws ec2 describe-instance-type-offerings \
--location-type "availability-zone" \
--filters Name=location,Values=<local-zone-name>
```

Resultado previsto:

```
{
  "InstanceTypeOfferings": [
      {
          "InstanceType": "m5.2xlarge",
          "LocationType": "availability-zone",
          "Location": "<local-zone-name>"
      },
      {
          "InstanceType": "t3.micro",
          "LocationType": "availability-zone",
          "Location": "local.zone-name"
      },
      ...
```

```
  ]
}
```

Administración de infraestructura perimetral

AWS proporciona servicios totalmente gestionados que extienden la AWS infraestructura APIs, los servicios y las herramientas más cerca de los usuarios finales y los centros de datos. Los servicios que están disponibles en Outposts y Zonas Locales son los mismos que los disponibles en Regiones de AWS, por lo que puedes gestionarlos con la misma AWS consola AWS CLI, o. AWS APIs Para ver los servicios compatibles, consulta la AWS Outposts tabla comparativa de Zonas locales de AWS funciones y las características.

Implementación de servicios en la periferia

Puede configurar los servicios disponibles en las Zonas Locales y en los Outposts de la misma forma en que los Regiones de AWS configuró: mediante la AWS consola AWS CLI, o. AWS APIs La principal diferencia entre las implementaciones regionales y periféricas son las subredes en las que se aprovisionarán los recursos. La sección Redes en el borde describe cómo se despliegan las subredes en Outposts y Zonas Locales. Tras identificar las subredes perimetrales, utiliza el ID de subred perimetral como parámetro para implementar el servicio en Outposts o Local Zones. En las siguientes secciones se proporcionan ejemplos de implementación de servicios perimetrales.

Amazon EC2 al límite

En el siguiente `run-instances` ejemplo, se lanza una única instancia de este tipo `m5.2xlarge` en la subred perimetral de la región actual. El par de claves es opcional si no tienes pensado conectarte a la instancia mediante SSH en Linux o el protocolo de escritorio remoto (RDP) en Windows.

```
aws ec2 run-instances \
    --image-id ami-id \
    --instance-type m5.2xlarge \
    --subnet-id <subnet-edge-id> \
    --key-name MyKeyPair
```

Equilibradores de carga de aplicaciones en la periferia

El siguiente `create-load-balancer` ejemplo crea un Application Load Balancer interno y habilita las Zonas Locales o Outposts para las subredes especificadas.

```
aws elbv2 create-load-balancer \
    --name my-internal-load-balancer \
    --scheme internal \
    --subnets <subnet-edge-id>
```

Para implementar un Application Load Balancer con acceso a Internet en una subred de un Outpost, debe establecer `internet-facing` el indicador en `--scheme` la opción y proporcionar un ID de grupo de CoIP, como se muestra en este ejemplo:

```
aws elbv2 create-load-balancer \
    --name my-internal-load-balancer \
    --scheme internet-facing \
    --customer-owned-ipv4-pool <coip-pool-id>
    --subnets <subnet-edge-id>
```

Para obtener información sobre la implementación de otros servicios en la periferia, siga estos enlaces:

Servicio	AWS Outposts	Zonas locales de AWS
Amazon EKS	Implemente Amazon EKS de forma local con AWS Outposts	Lance clústeres EKS de baja latencia con Zonas locales de AWS
Amazon ECS	Amazon ECS en AWS Outposts	Aplicaciones de Amazon ECS en subredes compartidas, Zonas Locales y Zonas de Longitud de onda
Amazon RDS	Amazon RDS en AWS Outposts	Seleccione la subred de la zona local
Amazon S3	Cómo empezar a usar Amazon S3 en Outposts	No disponible
Amazon ElastiCache	Uso de Outposts con ElastiCache	Uso de Zonas Locales con ElastiCache

Servicio	AWS Outposts	Zonas locales de AWS
Amazon EMR	EMR se agrupa en AWS Outposts	EMR se agrupa en Zonas locales de AWS
Amazon FSx	No disponible	Seleccione la subred de la zona local
AWS Elastic Disaster Recovery	Trabajando con y AWS Elastic Disaster RecoveryAWS Outposts	No disponible
AWS Transform MGN	No disponible	Seleccione la subred de zona local como subred provisional

CLI y SDK específicos para Outposts

AWS Outposts tiene dos grupos de comandos y sirve APIs para crear una orden de servicio o manipular las tablas de enrutamiento entre la puerta de enlace local y la red local.

Proceso de pedido de Outposts

Puedes usar Outposts AWS CLIo Outposts APIs para crear un sitio de Outposts, crear un Outpost y crear un pedido de Outposts. Le recomendamos que trabaje con un especialista en la nube híbrida durante el proceso de AWS Outposts pedido para garantizar una selección adecuada del recurso IDs y una configuración óptima para sus necesidades de implementación. Para obtener una lista completa de identificadores de recursos, consulte la página de precios de AWS Outposts Racks.

Administración de puertas de enlace locales

La administración y el funcionamiento de la puerta de enlace local (LGW) en Outposts requieren conocer los comandos AWS CLI del SDK disponibles para esta tarea. Puedes usar AWS CLI y AWS SDKs para crear y modificar las rutas de la LGW, entre otras tareas. Para obtener más información sobre la administración de la LGW, consulte estos recursos:

- AWS CLI para Amazon EC2
- EC2.Cliente en el AWS SDK para Python (Boto)
- Ec2Client en el AWS SDK para Java

CloudWatch métricas y registros

Dado Servicios de AWS que están disponibles tanto en Outposts como en las Zonas Locales, las métricas y los registros se administran de la misma manera que en las Regiones. Amazon CloudWatch proporciona métricas dedicadas a monitorear Outposts en 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 puesto de avanzada
`VolumeType`	El tipo de volumen de EBS
`VirtualInterfaceId`	El ID de la pasarela local o de la interfaz virtual de enlace de servicio (VIF)
`VirtualInterfaceGroupId`	El ID del grupo de VIF para la puerta de enlace local VIF

Para obtener más información, consulta CloudWatch las métricas de los racks de Outposts en la documentación de Outposts.

Recursos

AWS referencias

- Nube híbrida con AWS
- AWS Outposts Guía del usuario de los racks Outposts
- Guía del usuario de Zonas locales de AWS
- AWS Outposts Familia
- Zonas locales de AWS
- Amplíe una VPC a una zona local, Wavelength Zone o Outpost (documentación de Amazon VPC)
- Instancias de Linux en Zonas Locales (EC2 documentación de Amazon)
- Instancias de Linux en Outposts (documentación de Amazon EC2)
- Comience a implementar aplicaciones de baja latencia con Zonas locales de AWS (tutorial)

AWS publicaciones de blog

- Ejecución de AWS la infraestructura en las instalaciones con Amazon EC2
- Creación de aplicaciones modernas con Amazon EKS en Amazon EC2
- Cómo elegir entre los modos de enrutamiento CoIP y VPC directo en Amazon rack EC2
- Selección de conmutadores de red para su Amazon EC2
- Mantener una copia local de sus datos en Zonas locales de AWS
- Amazon ECS en Amazon EC2
- Administración de una red de servicios con reconocimiento perimetral con Amazon EKS para Zonas locales de AWS
- Implementación del enrutamiento de entrada de una puerta de enlace local en Amazon EC2
- Automatizar sus despliegues de carga de trabajo en Zonas locales de AWS
- Compartir Amazon EC2 en un AWS entorno de múltiples cuentas: Parte 1
- Compartir Amazon EC2 en un AWS entorno de múltiples cuentas: parte 2
- AWS Direct Connect y patrones de Zonas locales de AWS interoperabilidad

- Implemente Amazon RDS en Amazon EC2 con alta disponibilidad en zonas de disponibilidad múltiples

Colaboradores

Las siguientes personas y organizaciones han colaborado en esta guía.

Creación

- Leonardo Solano, arquitecto principal de soluciones de nube híbrida, AWS
- Len Gomes, arquitecto de soluciones asociado, AWS
- Matt Price, ingeniero sénior de Enterprise Support, AWS
- Tom Gadomski, arquitecto de soluciones, AWS
- Obed Gutierrez, arquitecto de soluciones, AWS
- Dionysios Kakaletris, gerente técnico de cuentas, AWS
- Vamsi Krishna, especialista principal en Outposts, AWS

Revisión

- David Filiatrault, consultor de entregas, AWS

Redacción técnica

- Handan Selamoglu, gerente sénior de documentación, AWS

Historial de documentos

En la siguiente tabla, se describen cambios significativos de esta guía. Si quiere recibir notificaciones de futuras actualizaciones, puede suscribirse a las notificaciones RSS.

Cambio	Descripción	Fecha
Publicación inicial	—	10 de junio de 2025

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.