AWS Documento técnico

AWS Outposts Consideraciones de arquitectura y diseño de alta disponibilidad

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Outposts Consideraciones de arquitectura y diseño de alta disponibilidad: AWS Documento técnico

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Las marcas comerciales y la imagen comercial de Amazon no se pueden utilizar en relación con ningún producto o servicio que no sea de Amazon, de ninguna manera que pueda causar confusión entre los clientes y que menosprecie o desacredite a Amazon. Todas las demás marcas registradas que no son propiedad de Amazon son propiedad de sus respectivos propietarios, que pueden o no estar afiliados, conectados o patrocinados por Amazon.

Table of Contents

Resumen e introducción i
¿Tiene Well-Architected? 1
Introducción 1
Extender AWS la infraestructura y los servicios a las ubicaciones locales 2
Comprensión del modelo de responsabilidad AWS Outposts compartida 5
Planteamiento en torno a los modos de falla 7
Modo de error 1: red 7
Modo de error 2: instancias 8
Modo de error 3: computación 8
Modo de error 4: racks o centros de datos 9
Modo de error 5: zona o AWS región de disponibilidad 9
Creación de aplicaciones de alta disponibilidad y soluciones de infraestructura con un bastidor de AWS Outposts 11
Red 12
Conexión de redes 13
Conectividad de anclaje 19
Enrutamiento de aplicaciones y cargas de trabajo 23
Computación 27
Planificación de la capacidad 27
Administración de la capacidad 31
Ubicación de instancias 34
Almacenamiento 37
Protección de los datos 38
Bases de datos 41
Amazon RDS en Outposts con Multi-AZ 41
Amazon RDS en réplicas de AWS Outposts lectura 43
El escalado automático del almacenamiento de Amazon RDS está activado AWS Outposts 44
Amazon RDS en el backup AWS Outposts local 44
Modos de error más extensos 45
Enrutamiento dentro de la VPC de Outposts Rack 46
Enrutamiento entre VPC de Outposts Rack 47
Route 53 Local Resolver en Outposts 48
Clúster local de EKS en Outposts 50

Conclusión 52
Colaboradores 53
Historial del documento 54
Avisos 55
AWS Glosario 56
..... lvii

AWS Outposts Consideraciones de arquitectura y diseño de alta disponibilidad

Fecha de publicación: 12 de agosto de 2021 (Historial del documento)

Este documento técnico analiza las consideraciones de arquitectura y las prácticas recomendadas que los administradores de TI y los arquitectos de sistemas pueden aplicar para crear entornos de aplicaciones locales de alta disponibilidad. AWS Outposts

¿Usa Well-Architected?

El marco de AWS Well-Architected le ayuda a entender las ventajas y desventajas de las decisiones que toma al crear sistemas en la nube. Los seis pilares del marco le permitirán aprender las prácticas recomendadas de arquitectura para diseñar y utilizar sistemas fiables, seguros, eficientes, rentables y sostenibles. Mediante AWS Well-Architected Tool, disponible sin costo alguno en la Consola de administración de AWS, puede comparar las cargas de trabajo con estas prácticas recomendadas respondiendo a una serie de preguntas para cada pilar.

Para obtener más orientación experta y prácticas recomendadas para la arquitectura de la nube (implementaciones de arquitectura de referencia, diagramas y documentos técnicos), consulte el Centro de arquitectura de AWS.

Introducción

Este paper está dirigido a los administradores de TI y arquitectos de sistemas que desean implementar, migrar y operar aplicaciones mediante la plataforma en la AWS nube y ejecutar esas aplicaciones en las instalaciones con un AWS Outposts rack, el formato de rack de 42U de AWS Outposts.

Presenta los patrones de arquitectura, los antipatrones y las prácticas recomendadas para crear sistemas de alta disponibilidad que incluyan AWS Outposts racks. Aprenderá a administrar la capacidad de sus AWS Outposts racks y a utilizar los servicios de redes y centros de datos para configurar soluciones de infraestructura de AWS Outposts racks de alta disponibilidad.

AWS Outposts rack es un servicio totalmente gestionado que proporciona un conjunto lógico de capacidades de computación, almacenamiento y redes en la nube. Con los racks de Outposts, los

clientes pueden utilizar los servicios AWS gestionados compatibles en sus entornos locales, como Amazon Elastic Compute Cloud (Amazon) EC2, Amazon Elastic Block Store (Amazon EBS), Amazon S3 on Outposts, Amazon ElasticKubernetes Service (Amazon EKS), Amazon Elastic Container Service (Amazon ECS) y Amazon Relational Database Service (Amazon RDS) y otros servicios en Outposts.AWS Los servicios de Outposts se prestan en el mismo AWS Nitro System que se utiliza en las Regiones de AWS.

Al aprovechar el AWS Outposts rack, puede crear, administrar y escalar aplicaciones locales de alta disponibilidad mediante herramientas y servicios AWS en la nube conocidos. AWS Outposts rack es ideal para cargas de trabajo que requieren acceso de baja latencia a sistemas locales, procesamiento de datos local, residencia de datos y migración de aplicaciones con interdependencias entre sistemas locales.

Extender la AWS infraestructura y los servicios a ubicaciones locales

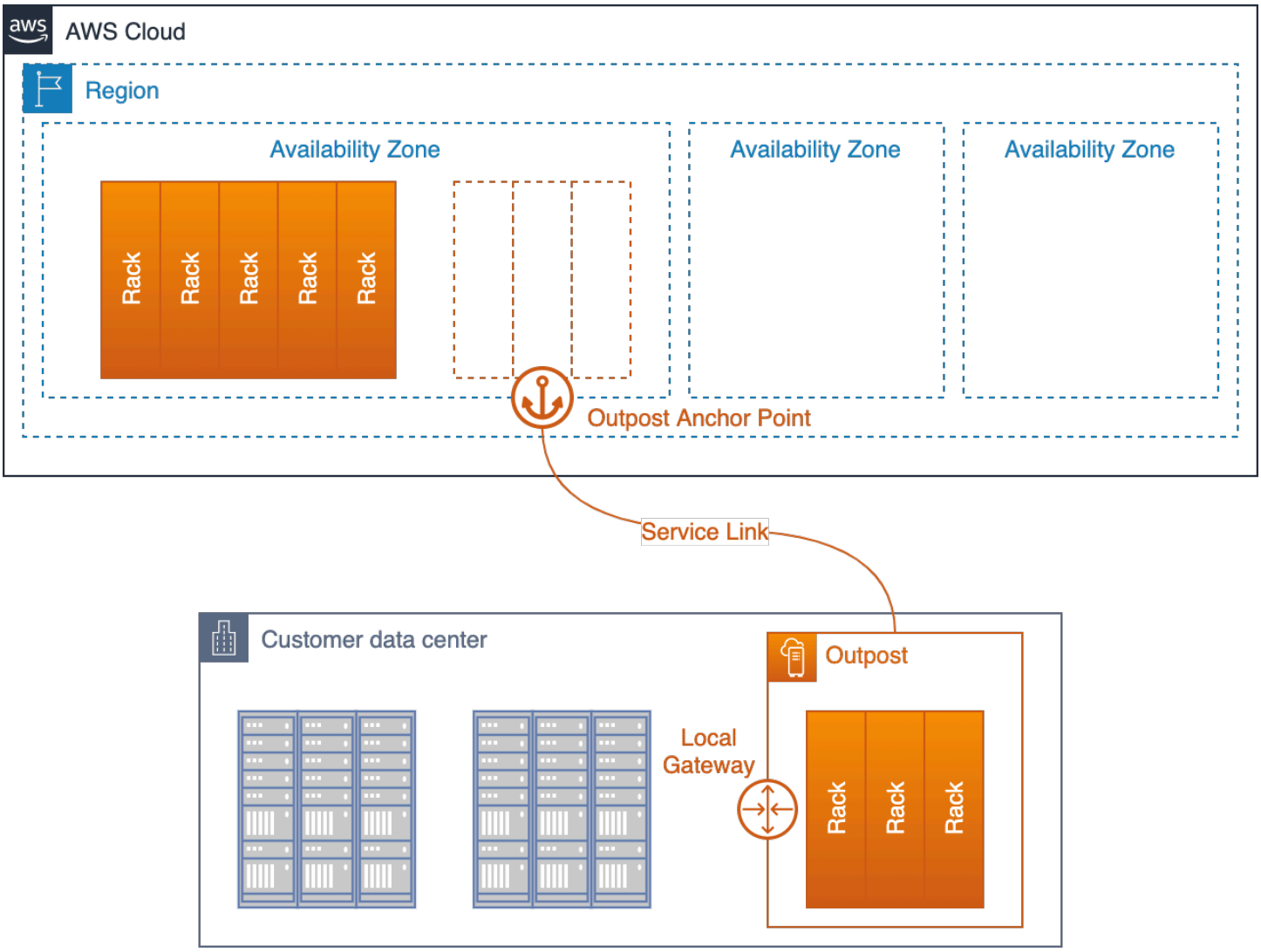
El AWS Outposts servicio ofrece AWS infraestructura y servicios a ubicaciones locales en más de 50 países y territorios, lo que brinda a los clientes la posibilidad de implementar la misma AWS infraestructura APIs, AWS servicios y herramientas en prácticamente cualquier centro de datos, espacio de ubicación conjunta o instalación local para lograr una experiencia híbrida verdaderamente coherente. Para entender cómo diseñar con Outposts, debes entender los diferentes niveles que componen la AWS nube.

Una Región de AWS es un área geográfica del mundo. Cada uno Región de AWS es un conjunto de centros de datos que se agrupan de forma lógica en zonas de disponibilidad ()AZs. Regiones de AWS proporcionan varias (al menos dos) zonas de disponibilidad aisladas y separadas físicamente que estén conectadas con una conectividad de red redundante, de baja latencia y de alto rendimiento. Cada AZ consta de uno o varios centros de datos físicos.

Un Outpost lógico (en adelante denominado Outpost) es un despliegue de uno o más AWS Outposts racks conectados físicamente y gestionados como una sola entidad. Un Outpost proporciona un conjunto de capacidad AWS informática y de almacenamiento en uno de sus sitios como una extensión privada de una zona de disponibilidad en un. Región de AWS

Quizás el mejor modelo conceptual AWS Outposts sea pensar en desconectar uno o más racks de un centro de datos en una zona de disponibilidad e instalarlos en su propio centro de datos o instalación de colocación. Región de AWS Los bastidores se implementan desde el centro de datos de la AZ hasta su propio centro de datos. Luego, conecte los racks a los puntos de anclaje del centro de datos AZ con un cable (muy) largo para que los racks sigan funcionando como parte

del. Región de AWS También se conectan a la red local para proporcionar una conectividad de baja latencia entre las redes en las instalaciones y las cargas de trabajo que se ejecutan en dichos bastidores. Esto le proporciona la coherencia operativa y de API del sistema Nube de AWS, a la vez que mantiene su carga de trabajo local.



Instancia de Outposts implementada en el centro de datos del cliente y que se conecta de nuevo a la AZ de anclaje y la región principal

El Outpost funciona como una extensión de la AZ donde está anclado. AWS opera, monitorea y administra la AWS Outposts infraestructura como parte de. Región de AWS En lugar de un cable físico muy largo, una instancia de Outposts se conecta a su región principal a través de un conjunto de túneles VPN cifrados denominados enlace de servicio.

El enlace de servicio termina en un conjunto de puntos de anclaje de una zona de disponibilidad (AZ) de la región principal de la instancia de Outposts.

La ubicación donde se almacena su contenido es solo suya. Puede replicar y hacer copias de seguridad de su contenido en esa ubicación Región de AWS o en otras ubicaciones. El contenido no se trasladará ni copiará a otras ubicaciones sin su consentimiento, excepto cuando sea necesario para cumplir la ley o una orden vinculante de un organismo público. Para obtener más información, consulte Preguntas frecuentes sobre privacidad de datos de AWS.

Las cargas de trabajo que implementa en esos bastidores se ejecutan de forma local. Además, si bien la capacidad de procesamiento y almacenamiento disponible en esos racks es limitada y no permite ejecutar los servicios a escala de nube propios de un rack Región de AWS, los recursos desplegados en el rack (sus instancias y su almacenamiento local) se benefician de la ejecución local mientras el plano de administración sigue funcionando en el mismo. Región de AWS

Para implementar cargas de trabajo en una instancia de Outposts, añada subredes a sus entornos de nube privada virtual (VPC) y especifique una instancia de Outposts como ubicación para las subredes. A continuación, selecciona la subred deseada al implementar AWS los recursos compatibles a través de las Consola de administración de AWS herramientas CLI APIs, CDK o infraestructura como código (IaC). Las instancias en las subredes de Outposts se comunican con otras instancias en Outposts o en la región a través de redes VPC.

El enlace de servicio de la instancia de Outposts transporta tanto el tráfico de administración de la instancia en sí como el tráfico de la VPC del cliente (tráfico de la VPC entre las subredes de la instancia de Outposts y las subredes de la región).

Términos importantes:

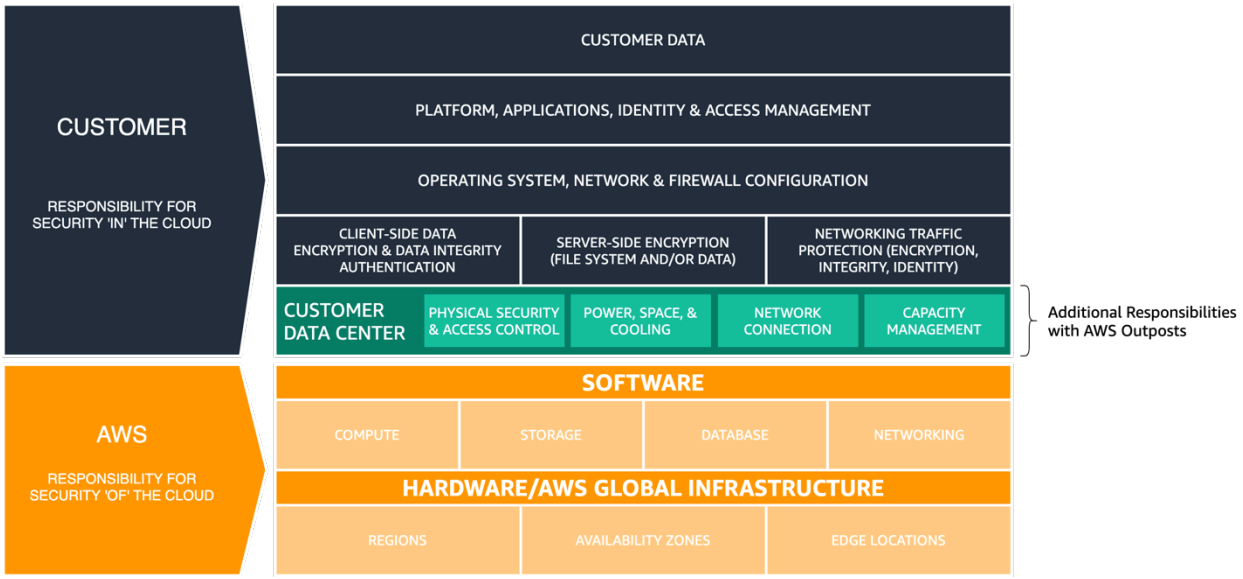
- AWS Outposts— es un servicio totalmente gestionado que ofrece la misma AWS infraestructura APIs, AWS servicios y herramientas para prácticamente cualquier centro de datos, espacio compartido o instalación local para ofrecer una experiencia híbrida verdaderamente coherente.
- Outpost: es una implementación de uno o más AWS Outposts racks conectados físicamente que se administra como una entidad lógica única y un conjunto de AWS recursos informáticos, almacenamiento y redes desplegados en las instalaciones de un cliente.
- Región principal: la Región de AWS que proporciona la administración, los servicios de plano de control y los AWS servicios regionales necesarios para un despliegue de Outpost.
- Zona de disponibilidad de anclaje (AZ de anclaje): la zona de disponibilidad de la región principal que aloja los puntos de anclaje de una implementación de Outposts. Un puesto avanzado funciona como una extensión de su base AZ. El cliente elige el ancla AZ al realizar el pedido de Outposts. Una vez elegida una AZ ancla, no se puede cambiar durante el periodo de AWS Outposts suscripción.

- Puntos de anclaje: puntos de conexión de la AZ de anclaje que reciben las conexiones de las instancias de Outposts implementadas de forma remota.
- Enlace de servicio: conjunto de túneles VPN cifrados que conectan una instancia de Outposts con su zona de disponibilidad principal de anclaje en su región principal.
- Puerta de enlace local (LGW): un enrutador virtual de interconexión lógica que permite la comunicación entre la instancia de Outposts y la red en las instalaciones del usuario.

Entendiendo el modelo de responsabilidad AWS Outposts compartida

Al implementar la AWS Outposts infraestructura en sus centros de datos o instalaciones de ubicación compartida, asume responsabilidades adicionales en el modelo de responsabilidad AWS compartida. Por ejemplo, en la región, AWS ofrece diversas fuentes de alimentación, redes centrales redundantes y una conectividad de red de área amplia (WAN) flexible para garantizar la disponibilidad de los servicios en caso de que se produzcan fallos en uno o más componentes.

Con Outposts, usted es responsable de garantizar un suministro eléctrico y conectividad de red resilientes a los bastidores de Outposts a fin de satisfacer sus propios requisitos de disponibilidad para las cargas de trabajo que se ejecutan en Outposts.



AWS Modelo de responsabilidad compartida actualizado para AWS Outposts

Con AWS Outposts, usted es responsable de la seguridad física y los controles de acceso del entorno del centro de datos. Debe proporcionar energía, espacio y refrigeración suficientes para mantener la instancia de Outposts y las conexiones de red operativas para volver a conectar la instancia con la región.

Dado que la capacidad de Outpost es finita y está determinada por el tamaño y la cantidad de racks AWS instalados en su sitio, debe decidir qué cantidad EC2, EBS y S3 de la capacidad de Outpost, necesita para ejecutar sus cargas de trabajo iniciales, adaptarse al crecimiento futuro y proporcionar capacidad adicional para mitigar las fallas del servidor y los eventos de mantenimiento.

AWS es responsable de la disponibilidad de la infraestructura de Outposts, incluidas las fuentes de alimentación, los servidores y los equipos de red de los AWS Outposts racks. AWS también administra el hipervisor de virtualización, los sistemas de almacenamiento y los AWS servicios que se ejecutan en Outposts.

En cada bastidor de Outposts se instala un sistema eléctrico central que convierte la corriente alterna en corriente continua y suministra energía a los servidores del bastidor a través de una arquitectura de barras de distribución. Con este tipo de arquitectura, la mitad de las fuentes de alimentación del bastidor pueden fallar sin que ninguno de los servidores interrumpa su funcionamiento.

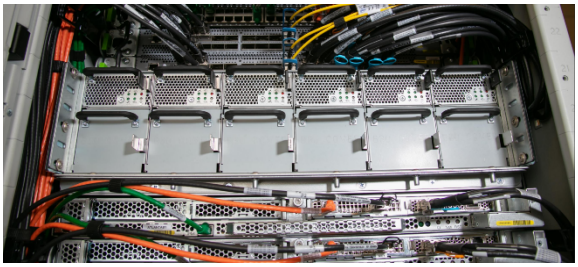


Figura 3: fuentes AWS Outposts AC-to-DC de alimentación y distribución de energía mediante barra colectora

Los conmutadores de red y el cableado dentro y entre los bastidores de Outposts también son totalmente redundantes. Un panel de conexiones de fibra proporciona conectividad entre un rack Outpost y la red local y sirve como punto de demarcación entre el entorno del centro de datos gestionado por el cliente y el entorno gestionado. AWS Outposts

Al igual que en la región, AWS es responsable de los servicios en la nube que se ofrecen en Outposts y asume responsabilidades adicionales a medida que selecciona e implementa servicios gestionados de nivel superior, como Amazon RDS en Outposts. Lea el Modelo de responsabilidad compartida de AWS y las páginas de preguntas frecuentes de cada servicio antes de elegir los servicios que quiera implementar en Outposts. Estos recursos proporcionan detalles adicionales sobre la división de responsabilidades entre usted y. AWS

Planteamiento en torno a los modos de falla

Al diseñar una aplicación o un sistema de alta disponibilidad, debe tener en cuenta qué componentes podrían fallar, qué impacto tendrán las fallas de los componentes en el sistema, así como los objetivos de RPO/RTO de su aplicación, y qué mecanismos puede implementar para mitigar o eliminar el impacto de las fallas de los componentes. ¿La aplicación en cuestión se ejecuta en un único servidor, en un único rack o en un único centro de datos? ¿Qué ocurrirá cuando un servidor, rack o centro de datos experimente un error temporal o permanente? ¿Qué ocurre cuando se produce un error en un subsistema esencial como la red o en la propia aplicación? Hablamos de modos de error.

El usuario debe tener en cuenta los modos de error especificados en esta sección cuando planifique las implementaciones de Outposts y otras aplicaciones. En las secciones siguientes, se analizará cómo mitigar estos modos de error para proporcionar un mayor nivel de alta disponibilidad para el entorno de aplicaciones.

Modo de error 1: red

Una implementación de Outposts depende de una conexión resiliente con su región principal para su propia administración y supervisión. Las interrupciones de la red pueden deberse a diversos problemas, como errores del operador, errores del equipo e interrupciones del proveedor de servicios. Una implementación de Outposts, que puede estar compuesta por uno o más racks conectados entre sí en el sitio, se considera desconectada cuando no puede comunicarse con la región a través del enlace de servicio.

Las rutas de red redundantes pueden ayudar a mitigar el riesgo de que se produzcan eventos de desconexión. Se deben asignar el tráfico de red y las dependencias de la aplicación para conocer el impacto que los eventos de desconexión tendrían en las operaciones de las cargas de trabajo. El usuario debe planificar una redundancia de red suficiente para satisfacer los requisitos de disponibilidad de las aplicaciones.

Durante un evento de desconexión, las instancias que se ejecutan en una implementación de Outposts siguen ejecutándose y se puede acceder a ellas desde las redes en las instalaciones a través de la puerta de enlace local de Outposts (LGW). Las cargas de trabajo y los servicios locales pueden verse dañados o fallar si dependen de los servicios de la región. Las solicitudes de mutación (como iniciar o detener instancias en el Outpost), las operaciones del plano de control y la telemetría de los servicios (por ejemplo, CloudWatch las métricas) fallarán mientras el Outpost

esté desconectado de la región. CloudWatch Las métricas se almacenarán localmente en tu Outpost durante breves períodos de desconexión de la red y se enviarán a la región para que las revise cuando se restablezca la conexión del enlace de servicio.

Modo de error 2: instancias

EC2 Las instancias de Amazon pueden estropearse o fallar si el servidor en el que se ejecutan tiene un problema o si la instancia experimenta un error en el sistema operativo o en la aplicación. La forma en que las aplicaciones gestionan estos tipos de errores depende de la arquitectura de la aplicación. Las aplicaciones monolíticas suelen utilizar funciones de aplicaciones o sistemas para la recuperación, mientras que las arquitecturas modulares orientadas a los servicios o de microservicios suelen sustituir los componentes defectuosos para mantener la disponibilidad del servicio.

Puede reemplazar las instancias fallidas por instancias nuevas mediante mecanismos automatizados, como los grupos de Amazon EC2 Auto Scaling. La recuperación automática de instancias puede reiniciar las instancias que fallan debido a fallas en el servidor, siempre que haya suficiente capacidad libre disponible en los servidores restantes y el enlace de servicio siga conectado.

Modo de error 3: computación

Los servidores pueden fallar o verse dañados. Es posible que sea necesario ponerlos fuera de servicio (temporal o permanentemente) por diversos motivos, como errores de los componentes y operaciones de mantenimiento programadas. La forma en que los servicios del rack de Outposts gestionan los errores y los problemas de los servidores varía y puede depender de la forma en que los clientes configuren las opciones de alta disponibilidad.

El usuario debe solicitar una capacidad informática suficiente para admitir un modelo de disponibilidad `N+M`, en el que `N` es la capacidad requerida y `M` es la capacidad de reserva que se aprovisiona para adaptarse a los errores de los servidores.

Los reemplazos de hardware para los servidores averiados se proporcionan como parte del servicio de AWS Outposts rack totalmente gestionado. AWS supervisa activamente el estado de todos los servidores y dispositivos de red en una implementación de Outpost. Si es necesario realizar un mantenimiento físico, AWS programará una visita al sitio del usuario para sustituir los componentes con errores. El aprovisionamiento de la capacidad sobrante le permite mantener sus cargas de trabajo resistentes a los fallos del host mientras los servidores en mal estado quedan fuera de servicio y se sustituyen.

Modo de error 4: racks o centros de datos

Los errores de los racks pueden producirse debido a una pérdida total de la alimentación de estos o a problemas con el entorno, como una pérdida de la refrigeración o daños físicos en el centro de datos a causa de una inundación o un terremoto. Las deficiencias en las arquitecturas de distribución eléctrica del centro de datos o los errores que se producen durante el mantenimiento de la alimentación estándar del centro de datos pueden provocar la pérdida de energía en uno o más racks, o incluso en todo el centro de datos.

Estos escenarios se pueden mitigar mediante la implementación de la infraestructura en varios pisos o ubicaciones del centro de datos que sean independientes entre sí dentro del mismo campus o área metropolitana.

Adoptar este enfoque con AWS Outposts rack requerirá una cuidadosa consideración de cómo se diseñan y distribuyen las aplicaciones para que se ejecuten en varios Outposts lógicos independientes a fin de mantener la disponibilidad de las aplicaciones.

Modo de error 5: región o zona de disponibilidad de AWS

Cada implementación de Outposts está anclada a una zona de disponibilidad (AZ) específica dentro de una Región de AWS. Los errores de la región principal o la zona de disponibilidad de anclaje pueden provocar la pérdida de la gestión y la mutabilidad de Outposts, así como interrumpir la comunicación de red entre Outposts y la región.

Al igual que los errores de la red, los de la zona de disponibilidad o la región pueden provocar que Outposts se desconecte de la región. Las instancias que se ejecutan en una implementación de Outposts siguen ejecutándose y se puede acceder a ellas desde las redes en las instalaciones a través de la puerta de enlace local (LGW) de Outposts. Además, si dependen de los servicios de la región, pueden verse dañadas o fallar, tal y como se ha descrito anteriormente.

Para mitigar el impacto de los fallos AWS en las zonas de disponibilidad y las regiones, puedes desplegar varios Outposts, cada uno anclado a una zona o región diferente. Después, se puede diseñar la carga de trabajo para que funcione en un modelo de implementación distribuido de varias instancias de Outposts utilizando muchos de los mecanismos y patrones arquitectónicos similares a los que ya se utilizan para el diseño y la implementación en AWS .

El plano de control de los servicios que se ejecutan AWS Outposts reside en la región a la que está anclado, lo que genera una dependencia tanto de los servicios zonales, como Amazon y EC2

Amazon EBS, como de los servicios regionales, como Amazon RDS, Elastic Load Balancing y Amazon EKS. En Outposts, las aplicaciones se pueden implementar bajo el concepto de estabilidad estática para ayudar a mejorar la resiliencia para controlar las deficiencias del avión.

Creación de aplicaciones de alta disponibilidad y soluciones de infraestructura con AWS Outposts rack

Con AWS Outposts rack, puede crear, administrar y escalar aplicaciones locales de alta disponibilidad utilizando herramientas y servicios en AWS la nube que ya conoce. Es importante entender que, por lo general, las arquitecturas y los enfoques de alta disponibilidad en la nube difieren de las arquitecturas de alta disponibilidad tradicionales en las instalaciones que podrían estar actualmente en uso en su centro de datos.

Con las implementaciones tradicionales de aplicaciones de alta disponibilidad locales, las aplicaciones se implementan en máquinas virtuales (). VMs Para garantizar el buen funcionamiento y estado de estas máquinas virtuales, se implementan y mantienen sistemas e infraestructuras de TI complejos. VMs Suelen tener identidades específicas y cada máquina virtual puede desempeñar un papel fundamental en la arquitectura total de la aplicación.

Estos roles de la arquitectura se encuentran estrechamente acoplados a las identidades de las VM. Los arquitectos de sistemas aprovechan las características de la infraestructura de TI para brindar entornos de tiempo de ejecución de VM de alta disponibilidad que, a su vez, proporcionan a cada una de ellas un acceso fiable a la capacidad informática, los volúmenes de almacenamiento y los servicios de red. Si una VM falla, se ejecutan procesos de recuperación automatizados o manuales para restaurar la VM con errores a un buen estado, a menudo en otra infraestructura o en un centro de datos completamente diferente.

Las arquitecturas de alta disponibilidad en la nube adoptan un enfoque diferente. AWS los servicios en la nube proporcionan capacidades confiables de cómputo, almacenamiento y redes. Los componentes de la aplicación se implementan en EC2 instancias, contenedores, funciones sin servidor u otros servicios gestionados.

Una instancia es una instanciación de un componente de una aplicación (quizás uno de los muchos que desempeñan ese rol). Los componentes de la aplicación se acoplan de forma flexible entre sí y al rol que desempeñan en la arquitectura total de la aplicación. La identidad individual de una instancia no suele tener importancia. Se pueden crear o destruir instancias adicionales para escalarlas o reducirlas verticalmente según la demanda. Las instancias fallidas o en mal estado se sustituyen por instancias nuevas en buen estado.

AWS Outposts rack es un servicio totalmente gestionado que extiende la AWS computación, el almacenamiento, las redes, las bases de datos y otros servicios en la nube a las ubicaciones

locales para ofrecer una experiencia híbrida verdaderamente coherente. No considere el servicio de bastidores de Outposts un sustituto directo de los sistemas de infraestructura de TI con mecanismos de alta disponibilidad tradicionales en las instalaciones. Intentar utilizar AWS los servicios y Outposts para dar soporte a una arquitectura de alta disponibilidad local tradicional va en contra de los patrones.

Las cargas de trabajo que se ejecutan en AWS Outposts rack utilizan mecanismos de alta disponibilidad en la nube, como Amazon EC2 Auto Scaling (para escalar horizontalmente y satisfacer las demandas de las cargas de trabajo), las comprobaciones de EC2 estado (para detectar y eliminar las instancias en mal estado) y los balanceadores de carga de aplicaciones (para redirigir el tráfico de carga de trabajo entrante a instancias escaladas o reemplazadas). Al migrar aplicaciones a la nube, ya sea a un AWS Outposts rack Región de AWS o a un rack, debe actualizar la arquitectura de las aplicaciones de alta disponibilidad para empezar a aprovechar los servicios gestionados en la nube y los mecanismos de alta disponibilidad en la nube.

En las siguientes secciones, se presentan los patrones de arquitectura, los antipatrones y las prácticas recomendadas para implementar el AWS Outposts rack en sus entornos locales a fin de ejecutar cargas de trabajo con requisitos de alta disponibilidad. Estas secciones ofrecen una introducción sobre los patrones y prácticas; sin embargo, no proporcionan detalles en torno a la configuración y la implementación. Debe leer y familiarizarse con el AWS Outposts rack y la Guía del usuario FAQs FAQs y la documentación de servicio de los servicios que se ejecutan en el rack de Outposts mientras prepara su entorno para el rack de Outposts y sus aplicaciones para la migración a los servicios. AWS

Temas

- Red
- Computación
- Almacenamiento
- Bases de datos
- Modos de error más extensos

Red

Para que las operaciones de administración, supervisión y servicio funcionen correctamente, la implementación de una instancia de Outposts depende de una conexión resiliente a su zona de disponibilidad (AZ) de anclaje. Debe aprovisionar su red local para proporcionar conexiones de red

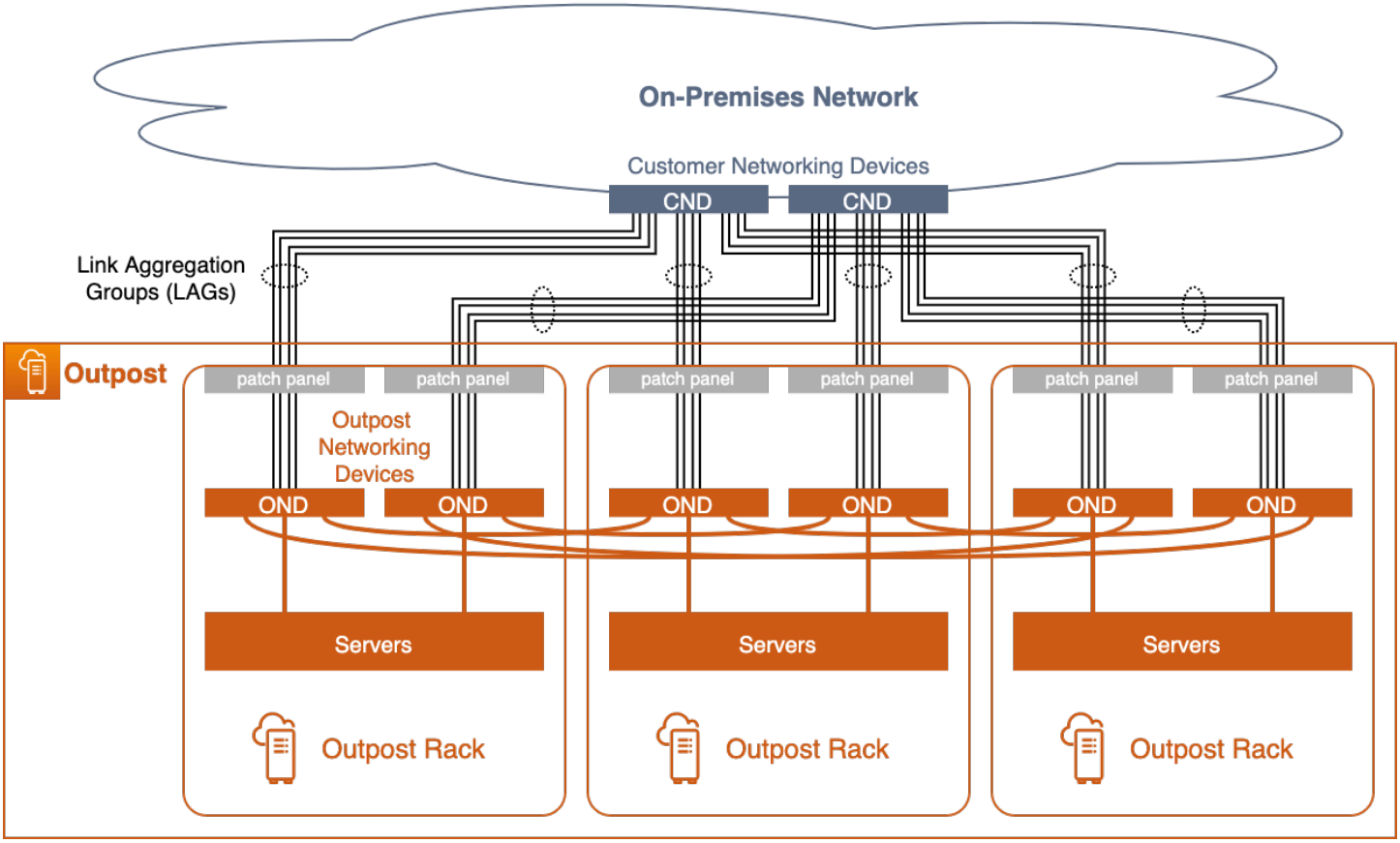
redundantes para cada rack de Outpost y una conectividad fiable hasta los puntos de anclaje de la nube. AWS También deben tenerse en cuenta las rutas de red entre las cargas de trabajo de las aplicaciones que se ejecutan en Outposts y el resto de sistemas en las instalaciones y la nube con los que se comunican. ¿Cómo se va a enrutar este tráfico en la red?

Temas

- Conexión de redes
- Conectividad de anclaje
- Enrutamiento de aplicaciones y cargas de trabajo

Conexión de redes

Cada AWS Outposts rack está configurado con top-of-rack conmutadores redundantes denominados Outpost Networking Devices (). ONDs Los servidores de cómputo y almacenamiento de cada rack se conectan a ambos. ONDs Debe conectar cada OND a un conmutador independiente denominado dispositivo de red del cliente (CND) del centro de datos para proporcionar diversas rutas físicas y lógicas para cada rack de Outpost. ONDs conéctese al suyo CNDs mediante una o más conexiones físicas mediante cables de fibra óptica y transceptores ópticos. Las conexiones físicas se configuran en enlaces lógicos de grupos de agregación de enlaces (LAG).



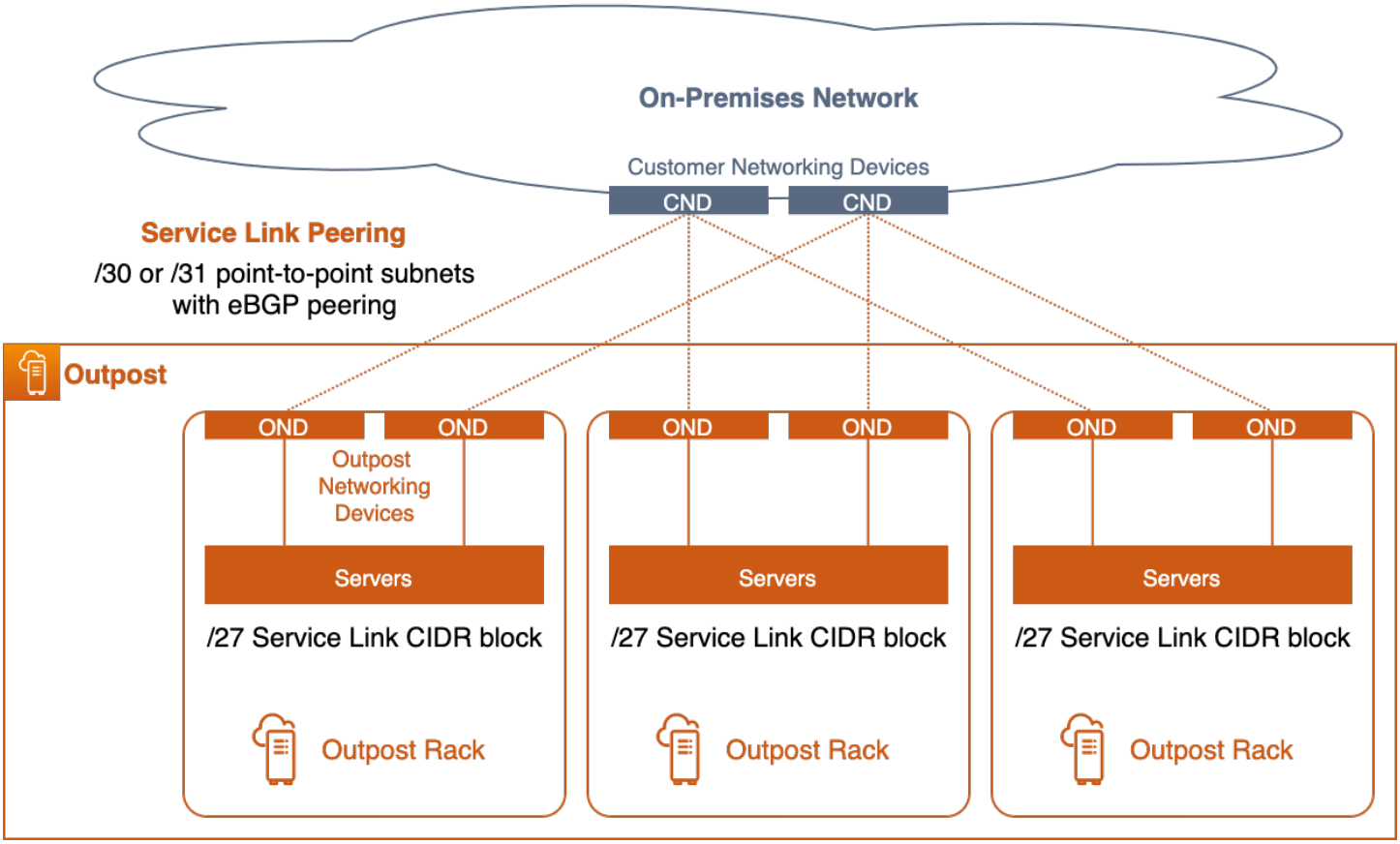
Instancia de múltiples bastidores de Outposts con conexiones redundantes de red

Los enlaces OND a CND siempre se configuran en un LAG, aunque la conexión física sea un solo cable de fibra óptica. La configuración de los enlaces como grupos LAG permite aumentar el ancho de banda de los enlaces mediante la incorporación de conexiones físicas adicionales al grupo lógico. Los enlaces LAG se configuran como redes troncales Ethernet de estándar IEEE 802.1q para permitir la creación de redes segregadas entre Outposts y la red en las instalaciones.

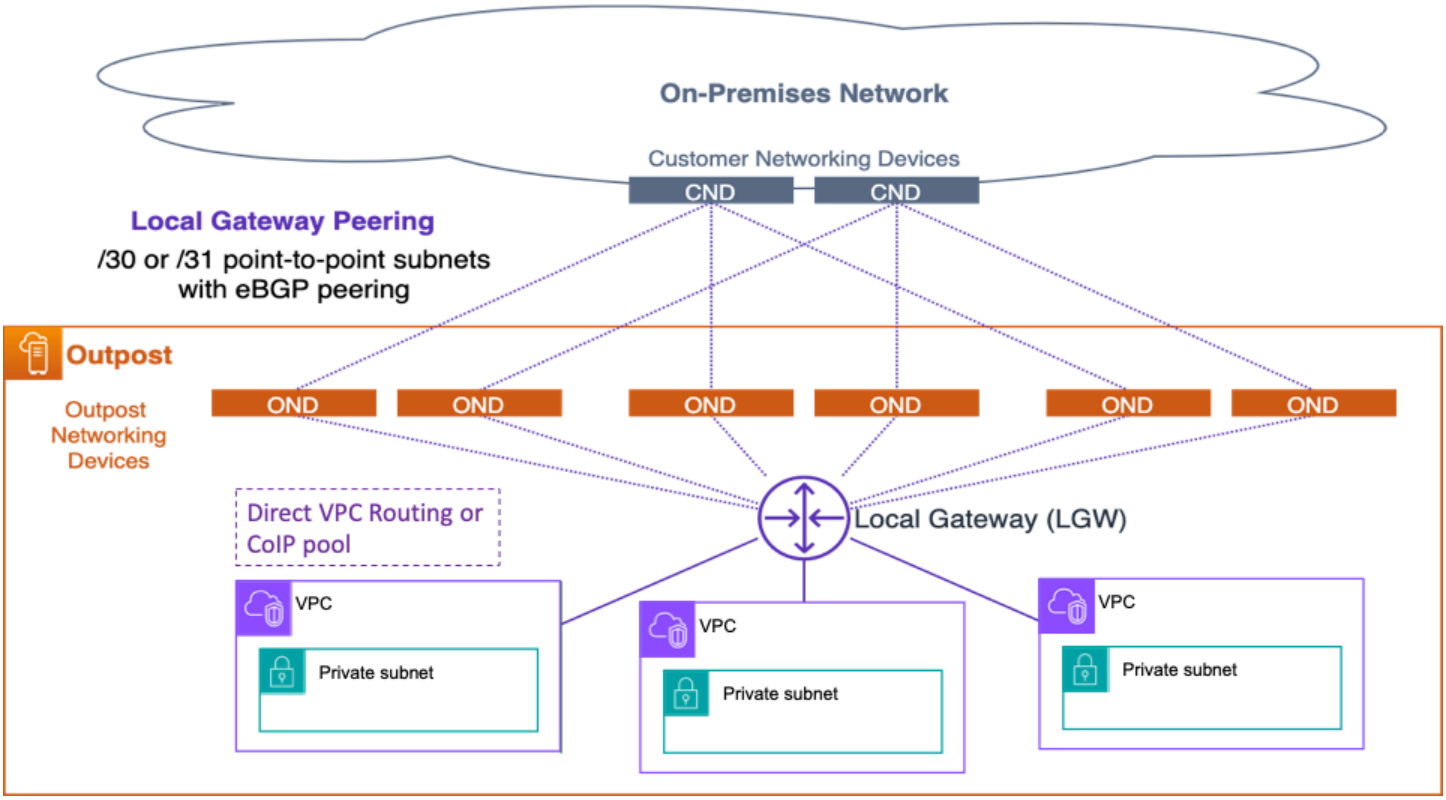
Cada instancia de Outposts tiene al menos dos redes segregadas de forma lógica que deben comunicarse con la red del cliente o a través de ella:

- Red de enlace de servicio: asigna las direcciones IP del enlace de servicio a los servidores de Outpost y facilita la comunicación con la red local para permitir que los servidores se conecten de nuevo a los puntos de anclaje de Outpost en la región. Si tienes múltiples implementaciones de rack en un único Outposts lógico, necesitas asignar un CIDR de Service Link /26 para cada rack.
- Red de puerta de enlace local: permite la comunicación entre las subredes de VPC de Outposts y la red en las instalaciones a través de la puerta de enlace local (LGW) de Outposts.

Estas redes segregadas se conectan a la red local mediante un conjunto de conexiones IP a través de point-to-point los enlaces LAG. Cada enlace LAG de OND a CND se configura con VLAN IDs, subredes IP point-to-point (/30 o /31) y emparejamiento eBGP para cada red segregada (enlace de servicio y LGW). Debe considerar los enlaces LAG, con sus subredes y subredes, como conexiones de capa 3 enrutadas point-to-point VLANs y segmentadas de capa 2. Las conexiones IP enrutadas proporcionan rutas lógicas redundantes que facilitan la comunicación entre las redes segregadas de Outposts y la red en las instalaciones.



Emparejamiento de enlaces de servicio



Interconexión de una puerta de enlace local

Debe terminar los enlaces LAG de capa 2 (y sus enlaces VLANs) en los conmutadores CND conectados directamente y configurar las interfaces IP y la interconexión BGP en los conmutadores CND. No debe conectar el LAG entre los conmutadores de su centro de datos VLANs . Para obtener más información, consulte Conectividad de la capa de red en la Guía del usuario de AWS Outposts .

Dentro de un Outpost lógico con varios racks, ONDs están interconectados de forma redundante para ofrecer una conectividad de red de alta disponibilidad entre los racks y las cargas de trabajo que se ejecutan en los servidores. AWS es responsable de la disponibilidad de la red en el Outpost.

Prácticas recomendadas para una conexión de red de alta disponibilidad sin ACE

- Cada dispositivo de red de Outposts (OND) de un bastidor de Outposts debe conectarse a un dispositivo de red del cliente (CND) independiente del centro de datos.
- Termine los enlaces de capa 2 VLANs, las subredes IP de capa 3 y la interconexión BGP en los conmutadores de dispositivos de red del cliente (CND) conectados directamente. No conecte el OND con el CND entre la red local o a través de ella VLANs . CNDs

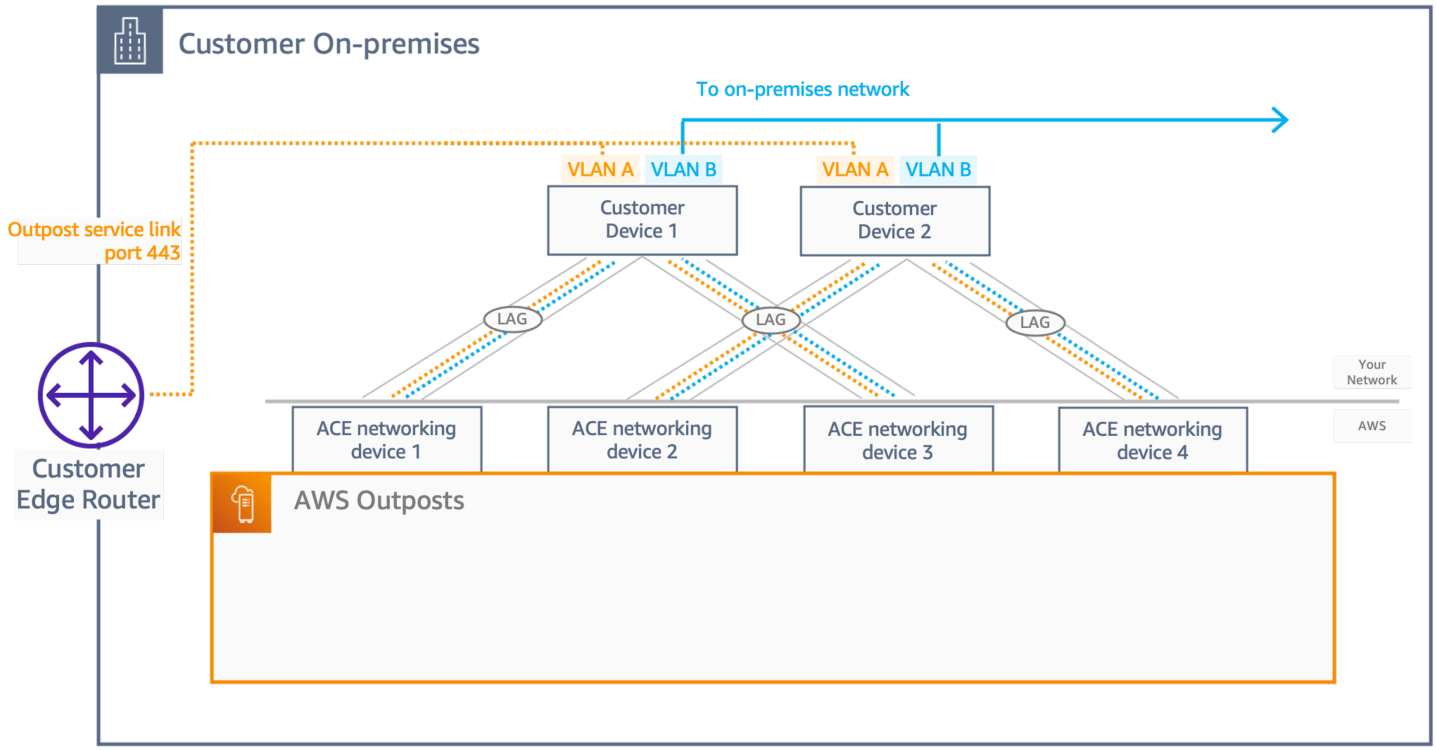
- Agregue enlaces a los grupos de agregación de enlaces (LAGs) para aumentar el ancho de banda disponible entre el puesto de avanzada y el centro de datos. No confíe en el ancho de banda agregado de las diversas rutas que atraviesan ambos ONDs.
- Utilice las diversas rutas a través de la redundante ONDs para proporcionar una conectividad flexible entre las redes de Outpost y la red local.
- Para lograr una redundancia óptima y permitir un mantenimiento de los OND sin interrupciones, recomendamos que los clientes configuren los anuncios y las políticas de BGP de la siguiente manera:
  - El equipo de red del cliente debe recibir anuncios de BGP de Outpost sin cambiar los atributos de BGP y habilitar el BGP en caso de que sea necesario realizar tareas de mantenimiento. multipath/load-balancing to achieve optimal inbound traffic flows (from customer towards Outpost). AS-Path prepending is used for Outpost BGP prefixes to shift traffic away from a particular OND/uplink La red del cliente debería preferir las rutas de Outposts con una longitud del atributo AS-Path de 1 a las rutas con una longitud del atributo AS-Path de 4; es decir, debe reaccionar al atributo AS-Path.
  - La red de clientes debe anunciar en Outpost prefijos BGP iguales con los mismos atributos. ONDs De forma predeterminada, la carga de red de Outposts equilibra el tráfico saliente (hacia el cliente) de todos los enlaces ascendentes. Las políticas de enrutamiento se utilizan en Outposts para desviar el tráfico de un OND en particular en caso de que sea necesario realizar tareas de mantenimiento. Para realizar este cambio de tráfico y realizar el mantenimiento de forma no disruptiva, ONDs se requieren prefijos BGP iguales por parte del cliente. Cuando sea necesario realizar tareas de mantenimiento en la red del cliente, recomendamos utilizar prefijos con el atributo AS-Path a fin de desviar temporalmente el tráfico procedente de un enlace ascendente o dispositivo concreto.

Prácticas recomendadas para una conexión de red de alta disponibilidad con ACE

Para una implementación de varios racks con cuatro o más racks de cómputo, debe usar el rack Aggregation, Core y Edge (ACE), que actuará como punto de agregación de la red para reducir la cantidad de enlaces de fibra a los dispositivos de red locales. El rack ACE proporciona la conectividad a cada rack de Outposts, por lo que AWS será propietario de la asignación y configuración de la interfaz VLAN entre ONDs los dispositivos de red ACE. ONDs

Se siguen necesitando capas de red aisladas para las redes Service Link y Local Gateway, independientemente de si se utiliza o no un rack ACE, cuyo objetivo es tener una VLAN point-to-point

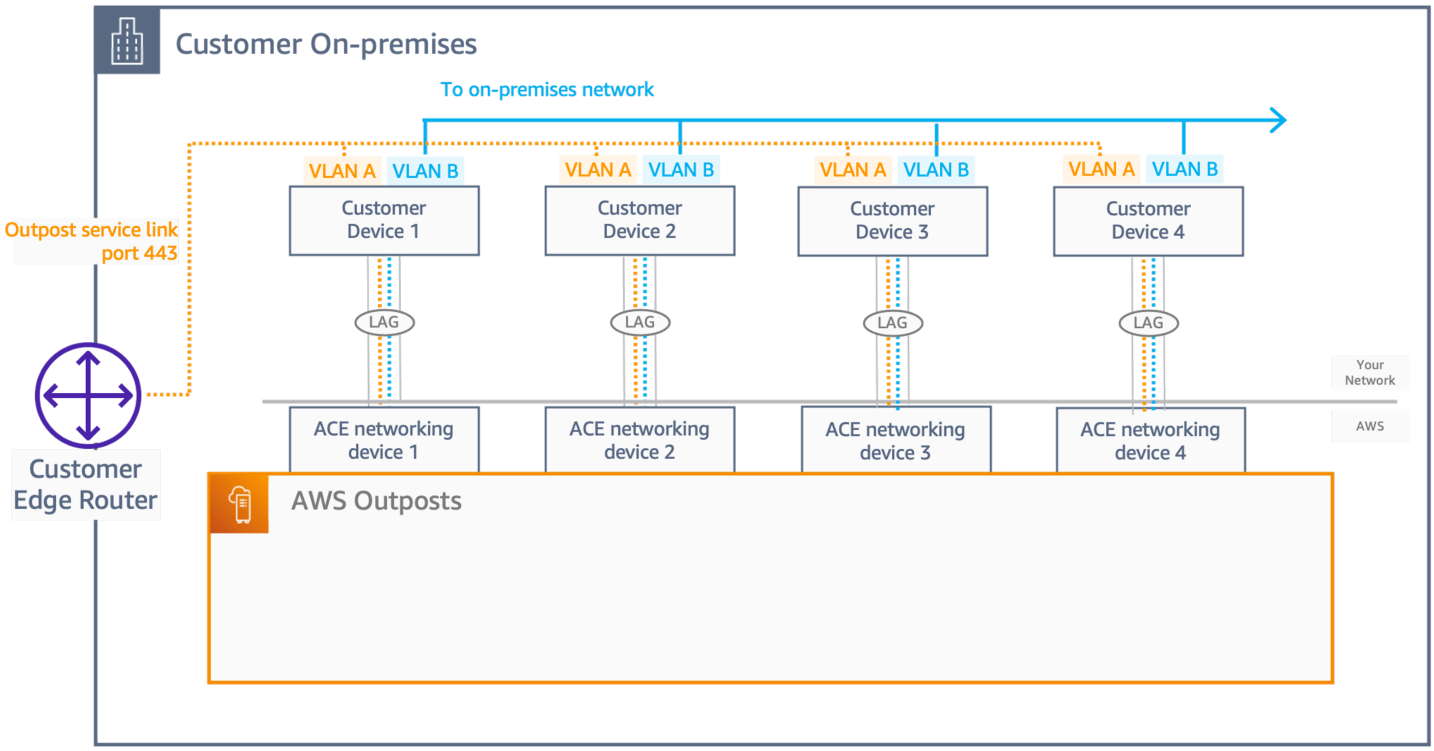
(/30 o /31), subredes IP y una configuración de interconexión eBGP para cada red segregada. Las arquitecturas propuestas deben seguir cualquiera de las dos arquitecturas siguientes:



Dispositivos de red para dos clientes

- Con esta arquitectura, el cliente debe tener dos dispositivos de red (CND) para interconectar los dispositivos de red ACE, lo que proporciona redundancia.
- Para cada conexión física, debe habilitar un LAG (para aumentar el ancho de banda disponible entre el Outpost y el centro de datos), incluso si se trata de un único puerto físico, y transportará dos segmentos de red, con configuraciones de 2 point-to-point VLANs (/30 o /31) y eBGP entre y. ACEs CNDs
- En un estado estable, la carga del tráfico se equilibra siguiendo el to/from the customer network from the ACE layer, 25% traffic distribution across the ACE to customer. In order to allow this behavior, the eBGP peering's between ACEs and CNDs must have BGP multipath/load equilibrio de patrones de rutas múltiples de igual costo (ECMP) habilitado y se anuncian los prefijos del cliente con la misma métrica de BGP en las 4 conexiones de emparejamiento eBGP.
- Para lograr una redundancia óptima y permitir un mantenimiento del OND sin interrupciones, recomendamos a los clientes que sigan estas recomendaciones:
  - El dispositivo de red del cliente debe anunciar prefijos BGP iguales con los mismos atributos en todos los anuncios de Outpost. ONDs

- El dispositivo de red del cliente debe recibir anuncios de BGP de Outpost sin cambiar los atributos de BGP y habilitar el equilibrio de carga y rutas múltiples de BGP.



Dispositivos de red para cuatro clientes

Con esta arquitectura, el cliente dispondrá de cuatro dispositivos de red (CND) para interconectar los dispositivos de red ACE, lo que proporcionará redundancia y la misma lógica de red VLANs, incluidos eBGP y ECMP aplicables a una arquitectura de 2 CND.

Conectividad de anclaje

Un enlace de servicio de Outpost se conecta a puntos de anclaje públicos o privados (no a ambos) en una zona de disponibilidad (AZ) específica de la región principal del Outpost. Los servidores de Outpost inician las conexiones VPN de enlace de servicio saliente desde sus direcciones IP de enlace de servicio hasta los puntos de anclaje de la AZ de anclaje. Estas conexiones utilizan los puertos UDP y TCP 443. AWS es responsable de la disponibilidad de los puntos de anclaje en la Región.

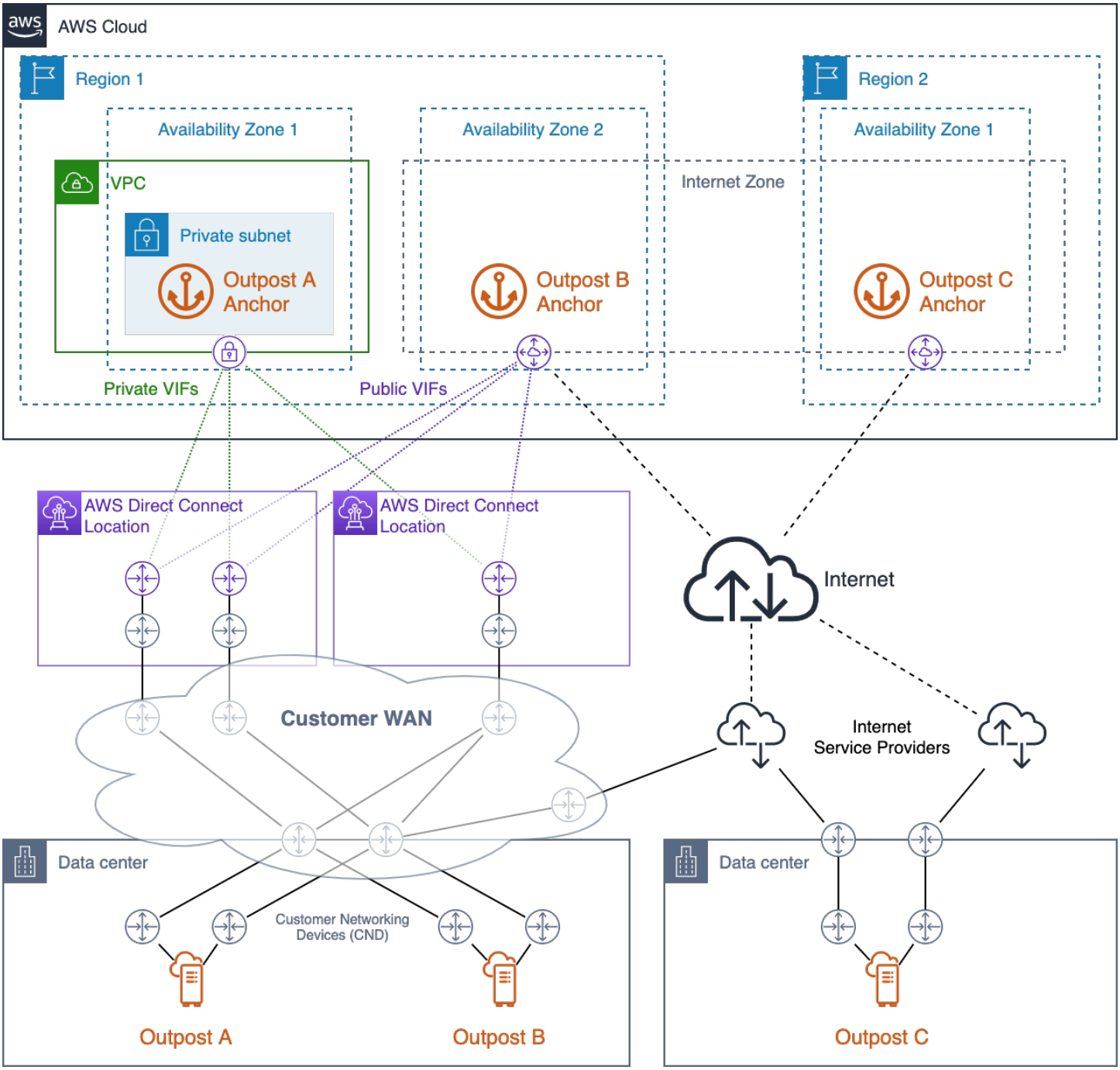
Debe asegurarse de que las direcciones IP del enlace del servicio Outpost puedan conectarse a través de su red a los puntos de anclaje de la zona de anclaje. Las direcciones IP del enlace de servicio no necesitan comunicarse con otros hosts de la red local.

Los puntos de anclaje públicos residen en los rangos de IP públicas de la región (en los bloques CIDR del EC2 servicio) y se puede acceder a ellos a través de Internet o de las interfaces virtuales públicas AWS Direct Connect(DX) (VIFs). El uso de puntos de anclaje públicos permite una selección de rutas más flexible, ya que el tráfico del enlace de servicio se puede enrutar por cualquier ruta disponible que pueda llegar correctamente a los puntos de anclaje de la Internet pública.

Los puntos de anclaje privados permiten usar al usuario sus propios rangos de direcciones IP para establecer la conectividad de anclaje. Los puntos de anclaje privados se crean en una subred privada dentro de una VPC dedicada mediante direcciones IP asignadas por el cliente. La VPC se crea en la VPC propietaria del recurso Outpost y usted es responsable de garantizar Cuenta de AWS que la VPC esté disponible y configurada correctamente. Utilice una política de control de seguridad (SCP) en AWSOrigamiServiceGateway Organizations para evitar que los usuarios eliminen esa Virtual Private Cloud (VPC). Se debe acceder a los puntos de anclaje privados mediante Direct Connect private. VIFs

Se deben aprovisionar rutas de red redundantes entre Outposts y los puntos de anclaje de la región, con conexiones que terminen en dispositivos independientes de más de una ubicación. Se debe configurar el direccionamiento dinámico para redirigir automáticamente el tráfico a rutas alternativas cuando las conexiones o los dispositivos de red fallen. Se debe aprovisionar una capacidad de red suficiente para garantizar que un error en una ruta WAN no sobrecargue las rutas restantes.

El siguiente diagrama muestra tres Outposts con rutas de red redundantes hasta su punto de anclaje AZs , AWS Direct Connect además de conectividad pública a Internet. Las instancias de Outposts A y B están ancladas a diferentes zonas de disponibilidad de la misma región. La instancia de Outposts A se conecta a puntos de anclaje privados en la AZ 1 de la región 1. La instancia de Outposts B se conecta a puntos de anclaje públicos en la AZ 2 de la región 1. La instancia de Outposts B se conecta a puntos de anclaje públicos en la AZ 2 de la región 1.



Conectividad de anclaje de alta disponibilidad con AWS Direct Connect acceso público a Internet

La instancia de Outposts A tiene tres rutas de red redundantes para llegar al punto de anclaje privado. Hay dos rutas disponibles a través de circuitos de Direct Connect redundantes en una única ubicación de Direct Connect. La tercera ruta está disponible a través de un circuito de Direct Connect en una segunda ubicación de Direct Connect. Este diseño mantiene el tráfico del enlace de servicio

del Outpost A en las redes privadas y proporciona una redundancia de rutas que permite el fallo de cualquiera de los circuitos de Direct Connect o el fallo de toda una ubicación de Direct Connect.

La instancia de Outposts B tiene cuatro rutas de red redundantes para llegar al punto de anclaje privado. Hay tres rutas disponibles a través de VIFs aprovisionamiento público en los circuitos y ubicaciones de Direct Connect utilizados por Outpost A. La cuarta ruta está disponible a través de la WAN del cliente y la Internet pública. El tráfico del enlace de servicio de Outpost B puede enrutarse a través de cualquier ruta disponible que pueda llegar correctamente a los puntos de anclaje de la Internet pública. El uso de las rutas Direct Connect puede proporcionar una latencia más coherente y una mayor disponibilidad de ancho de banda, mientras que la ruta de Internet pública se puede usar para la recuperación de desastres o aumentar el ancho de banda.

La instancia de Outposts C tiene dos rutas de red redundantes para llegar al punto de anclaje privado. La instancia de Outposts C se encuentra implementada en un centro de datos diferente al de las instancias de Outposts A y B. El centro de datos de la instancia de Outposts C no tiene circuitos dedicados que se conecten a la WAN del cliente. En cambio, el centro de datos tiene conexiones a Internet redundantes proporcionadas por dos proveedores de servicios de Internet diferentes (). ISPs El tráfico del enlace de servicio de Outpost C puede enrutarse a través de cualquiera de las redes del ISP para llegar a los puntos de anclaje de la Internet pública. Este diseño ofrece flexibilidad para enrutar el tráfico de los enlaces de servicio a través de cualquier conexión pública a Internet disponible. Sin embargo, la end-to-end ruta depende de las redes públicas de terceros, donde la disponibilidad del ancho de banda y la latencia de la red fluctúan.

La ruta de red entre un Outpost y sus puntos de anclaje de enlace de servicio debe cumplir con la siguiente especificación de ancho de banda:

- 500 Mbps: 1 Gbps de ancho de banda disponible por bastidor de Outposts (por ejemplo, para 3 bastidores, el ancho de banda disponible debe ser de entre 1,5 y 3 Gbps)

Prácticas recomendadas para una conectividad de anclaje de alta disponibilidad

- Proporcione rutas de red redundantes entre cada implementación de Outposts y sus puntos de anclaje en la región.
- Utilice las rutas de Direct Connect (DX) para controlar la latencia y la disponibilidad del ancho de banda.
- Asegúrese de que los puertos TCP y UDP 443 estén abiertos (salientes) desde los bloques CIDR de Outpost Service Link hasta los rangos de direcciones EC2 IP de la región principal. Confirme que los puertos estén abiertos en todas las rutas de red.

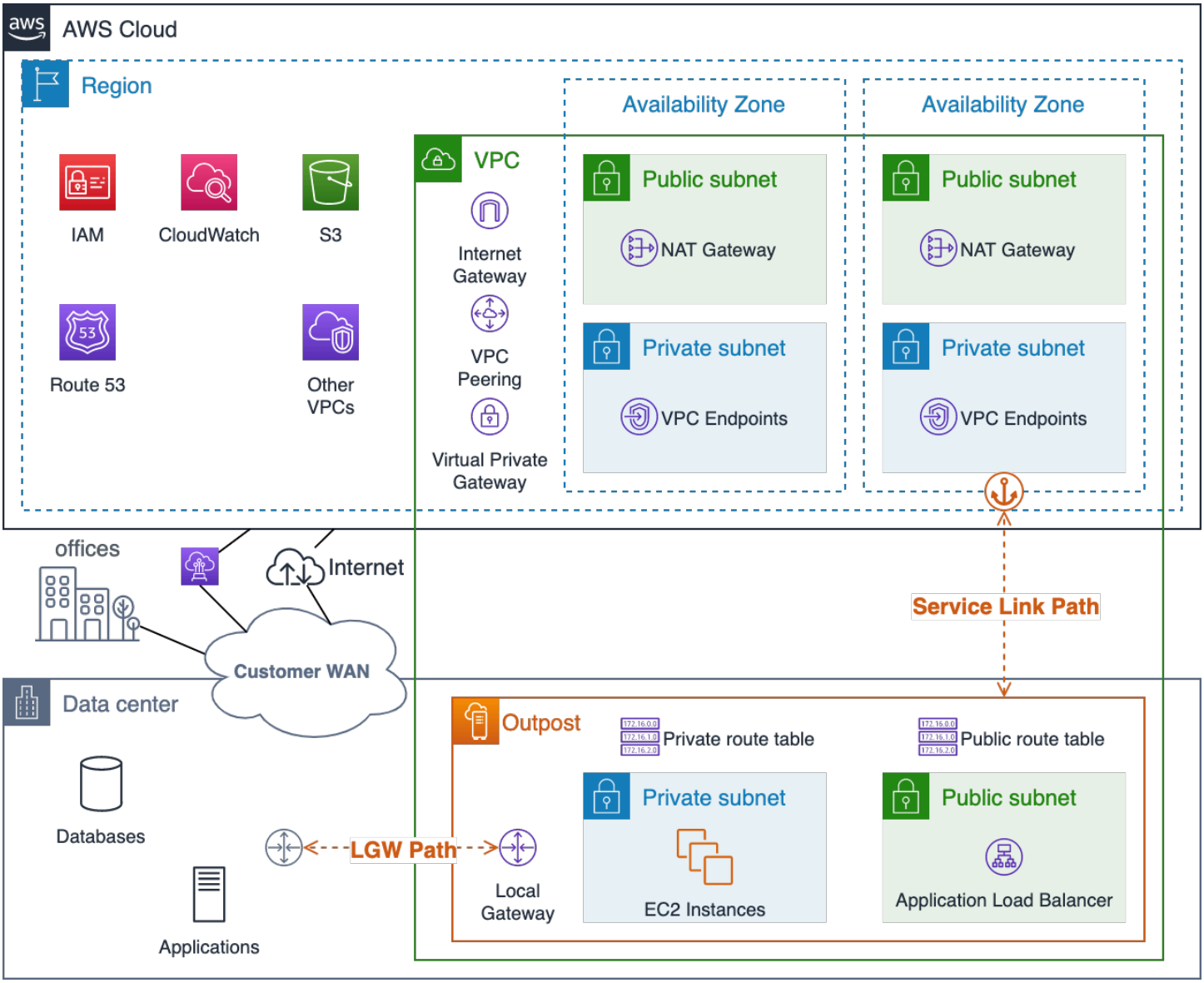
- Realice un seguimiento de los rangos de direcciones EC2 IP de Amazon en su firewall si utiliza un subconjunto de rangos de CIDR para la región.
- Compruebe que cada ruta cumple con los requisitos de latencia y disponibilidad de ancho de banda específicos.
- Utilice el direccionamiento dinámico para automatizar el redireccionamiento del tráfico en caso de producirse errores en la red.
- Pruebe a enrutar el tráfico del enlace de servicio a través de cada ruta de red planificada para asegurarse de que la ruta funcione según lo esperado.

Enrutamiento de aplicaciones y cargas de trabajo

Hay dos rutas de salida de Outposts para las cargas de trabajo de las aplicaciones:

- La ruta del enlace del servicio: tenga en cuenta que el tráfico de las aplicaciones competirá con el tráfico del plano de control de Outposts, además de limitar la MTU a 1300 bytes.
- La ruta de la puerta de enlace local (LGW): tenga en cuenta que la red local del cliente permite el acceso tanto a las aplicaciones locales como a las que se encuentran en la misma. Región de AWS

Las tablas de enrutamiento de la subred de Outposts se configuran para controlar la ruta que se debe seguir para llegar a las redes de destino. Las rutas que apuntan a la LGW dirigirán el tráfico desde la puerta de enlace local hacia la red en las instalaciones. Las rutas que apuntan a los servicios y recursos de la región, como Internet Gateway, NAT Gateway, Virtual Private Gateway y TGW, utilizarán Service Link para alcanzar estos objetivos. Si tienes una conexión de emparejamiento de VPC con varias 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. Para obtener información sobre la interconexión de VPC, consulte Conectarse mediante la interconexión de VPCs VPC en la Guía del usuario de Amazon VPC.



Visualización del enlace del servicio Outpost y de las rutas de red LGW

A la hora de planificar el enrutamiento de las aplicaciones, se debe tener en cuenta tanto el funcionamiento normal como la disponibilidad limitada del servicio y el enrutamiento cuando se producen errores en la red. La ruta de enlace de servicio no está disponible si Outposts está desconectado de la región.

Se deben aprovisionar diversas rutas y configurar el direccionamiento dinámico entre la LGW de Outposts y las aplicaciones, sistemas y usuarios esenciales en las instalaciones. Las rutas de red redundantes permiten a la red redirigir el tráfico en caso de error y garantizar que los recursos en las instalaciones puedan comunicarse con las cargas de trabajo que se ejecutan en Outposts en caso de que la red falle parcialmente.

Las configuraciones de enrutamiento de las VPC de Outposts son estáticas. Las tablas de enrutamiento de subred se configuran mediante la Consola de administración de AWS CLI y otras herramientas de infraestructura como código (IaC); sin embargo, no podrá modificar las tablas de enrutamiento de subred durante un evento de desconexión. APIs Deberá restablecerse la conectividad entre Outposts y la región para que las tablas de enrutamiento puedan actualizarse. Deben usarse las mismas rutas para las operaciones normales que las previstas para los eventos de desconexión.

Los recursos del Outpost pueden acceder a Internet a través del enlace de servicio y una puerta de enlace de Internet (IGW) en la región o a través de la ruta de puerta de enlace local (LGW). Enrutar el tráfico de Internet a través de la ruta LGW y la red local permite utilizar los puntos de entrada y salida de Internet locales existentes y puede ofrecer una latencia más baja y unos costes de salida de AWS datos más altos MTUs y reducidos en comparación con el uso de la ruta de enlace de servicio a una IGW de la región.

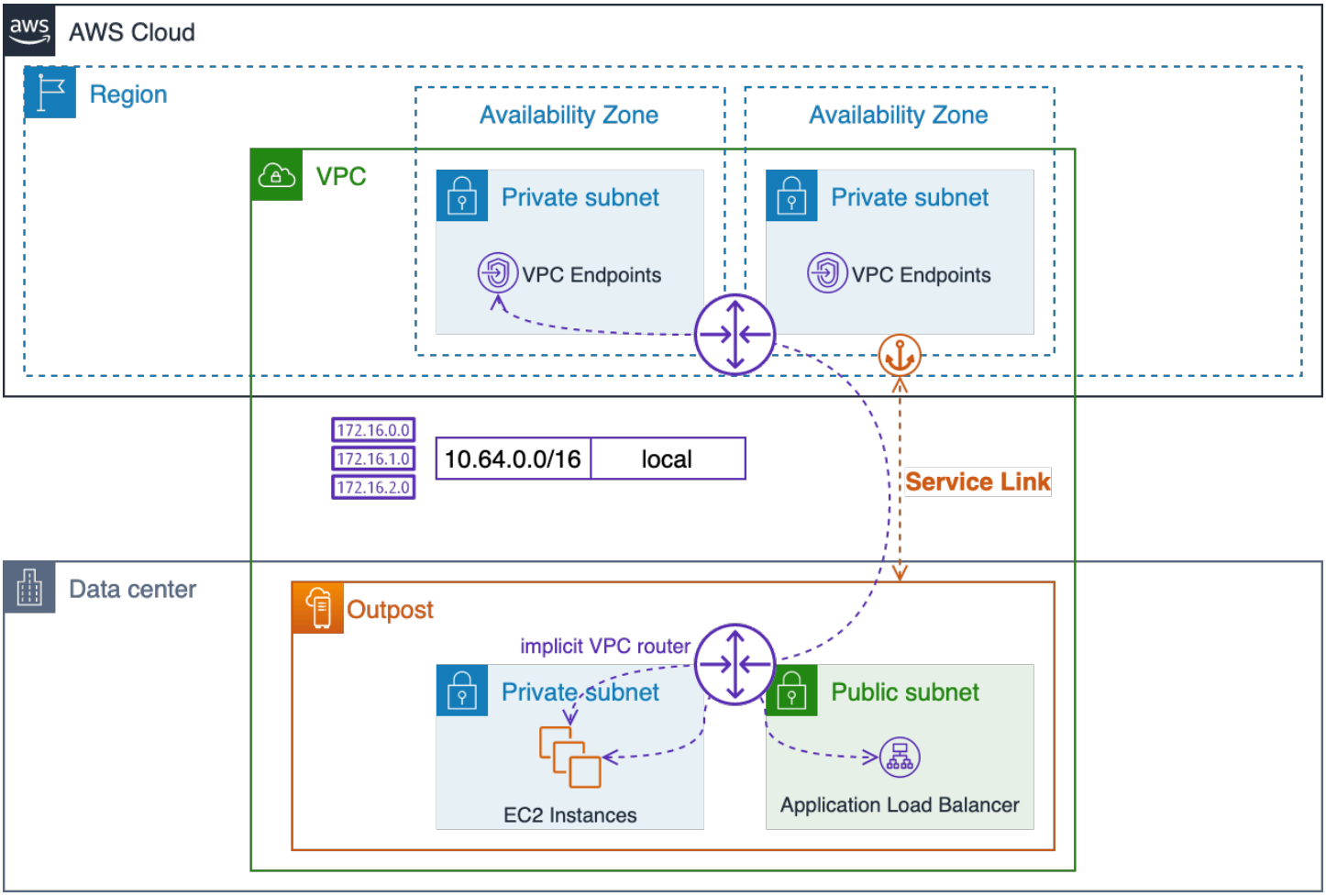
Si la aplicación debe ejecutarse en las instalaciones y es necesario que se pueda acceder a ella desde la Internet pública, el tráfico de la aplicación se debe enrutar a través de las conexiones a Internet en las instalaciones hasta la LGW con el objetivo de llegar a los recursos de Outposts.

Si bien se pueden configurar las subredes en Outposts como subredes públicas de la región, no representa la práctica más deseable para la mayoría de los casos de uso. El tráfico de Internet entrante entrará por el enlace de servicio Región de AWS y se enrutará a través del enlace de servicio hasta los recursos que se encuentran en el Outpost.

El tráfico de respuesta, a su vez, se enrutará a través del enlace del servicio y regresará a través de las conexiones a Internet del Región de AWS servicio. Este patrón de tráfico puede aumentar la latencia e incurrir en gastos de salida de datos cuando el tráfico salga de la región en dirección a Outposts y el tráfico de retorno vuelva a través de la región hacia Internet. Si la aplicación se puede ejecutar en la región, será el mejor lugar para ejecutarla.

El tráfico entre los recursos de la VPC (en la misma VPC) siempre seguirá la ruta CIDR de la VPC local y los enrutadores de VPC implícitos lo redirigirán entre las subredes.

Por ejemplo, el tráfico entre una EC2 instancia que se ejecuta en Outpost y un punto final de VPC en la región siempre se enrutará a través del enlace de servicio.



Enrutamiento de la VPC local a través de enrutadores implícitos

Prácticas recomendadas para el enrutamiento de aplicaciones y cargas de trabajo

- Siempre que sea posible, utilice la ruta de la puerta de enlace local (LGW) en lugar de la ruta del enlace de servicio.
- Enrute el tráfico de Internet a través de la ruta LGW.
- Configure las tablas de enrutamiento de la subred de Outposts con un conjunto estándar de rutas; se usarán tanto para las operaciones normales como durante los eventos de desconexión.
- Aprovisione rutas de red redundantes entre la LGW de Outposts y los recursos esenciales de las aplicaciones en las instalaciones. Utilice el direccionamiento dinámico para automatizar el redireccionamiento del tráfico en caso de producirse errores en la red en las instalaciones.

Computación

Si bien EC2 la capacidad de Amazon Regiones de AWS es aparentemente infinita, la capacidad de Outposts es finita. El usuario es responsable de planificar y administrar la capacidad informática de las implementaciones de Outposts.

Temas

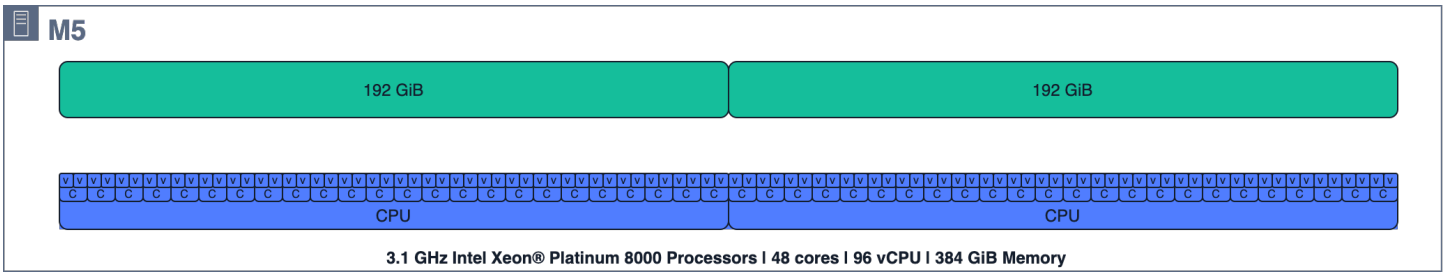
- Planificación de la capacidad
- Administración de la capacidad
- Ubicación de instancias

Planificación de la capacidad

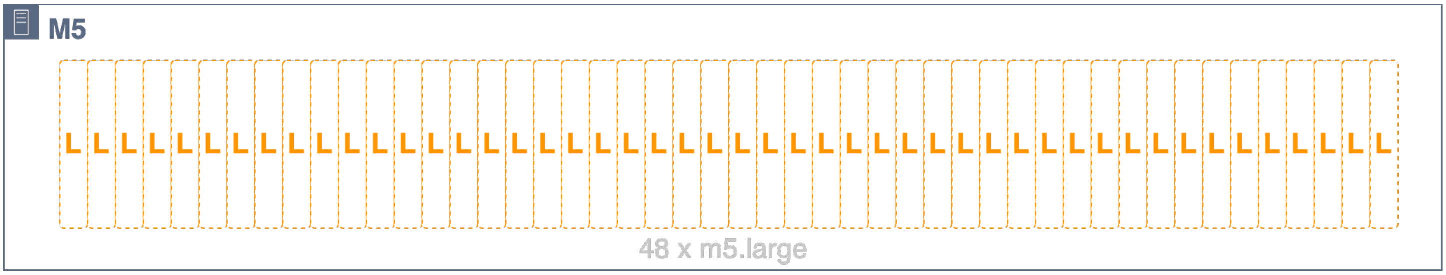
Si bien la EC2 capacidad de Amazon Regiones de AWS es aparentemente infinita, la capacidad de Outposts es finita, limitada por el volumen total de capacidad de cómputo solicitada. El usuario es responsable de planificar y administrar la capacidad informática de las implementaciones de Outposts. El usuario debe solicitar una capacidad informática suficiente para admitir un modelo de disponibilidad N+M, en el que N es la capacidad requerida y M es el número de servidores de reserva aprovisionados para adaptarse a los errores de los servidores. N+1 y N+2 son los niveles de disponibilidad más comunes.

Cada host (`C5`,`M5`,`R5`, etc.) admite una sola familia de EC2 instancias. Antes de lanzar instancias en servidores de EC2 procesamiento, debe proporcionar diseños de ranuras que especifiquen los tamaños de EC2 instancia que desea que proporcione cada servidor. AWS configura cada servidor con el diseño de ranuras solicitado.

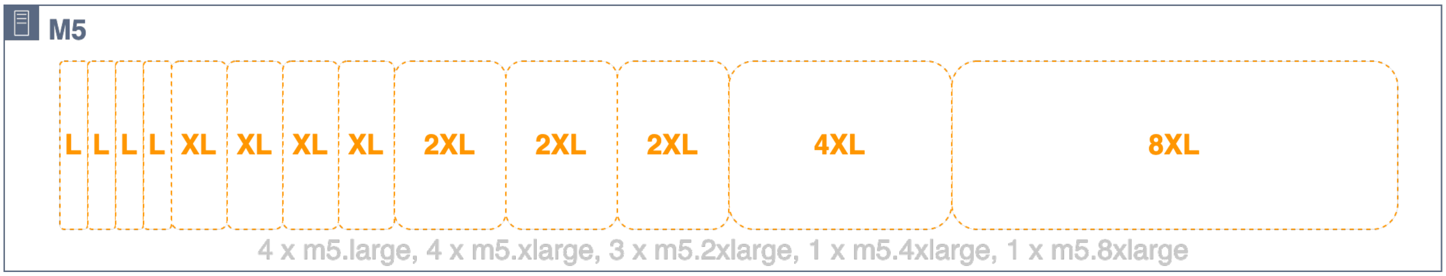
Los hosts pueden tener ranuras homogéneas cuando todas las ranuras tienen el mismo tamaño de instancia (por ejemplo, 48 `m5.large` ranuras) o heterogéneamente con una mezcla de tipos de instancias (por ejemplo, 4, 4`m5.large`, 3 `m5.xlarge` `m5.2xlargem5.4xlarge`, 1 y 1`m5.8xlarge`). Consulte las tres figuras siguientes para ver una visualización de estas configuraciones de asignación de ranuras.



`m5.24xlarge`alojar los recursos de cómputo



`m5.24xlarge`host distribuido homogéneamente en 48 ranuras `m5.large`



`m5.24xlarge`host distribuido de forma heterogénea en 4`m5.large`, 4, 3 `m5.xlargem5.2xlarge`, 1 y 1 ranuras `m5.4xlarge` `m5.8xlarge`

No es necesario asignar toda la capacidad del host. Se pueden agregar ranuras a un host que tenga capacidad disponible sin asignar. Puede modificar un diseño de ranuras mediante la administración de capacidad APIs o UIs creando una nueva tarea de capacidad. AWS Outposts Para obtener más información, consulte [Gestión de la capacidad AWS Outposts] en la guía del AWS Outposts usuario de racks. Es posible que deba cerrar o reiniciar determinadas instancias para completar una nueva tarea de capacidad si el nuevo diseño de ranuras no se puede aplicar mientras determinadas ranuras estén ocupadas por instancias en ejecución. La `CreateCapacityTask` API te permite expresar el número del tamaño de cada instancia que debe estar presente en el ID de Outpost indicado y, en el caso de que una tarea no se pueda completar debido a la ejecución de instancias, devuelve las instancias que deben detenerse para satisfacer la solicitud. En este punto, si lo desea, puede indicar si desea ver «N» opciones adicionales en caso de que prefiera no detener una de las instancias devueltas, y también puede indicar un ID de EC2 instancia, una etiqueta de EC2 instancia, una cuenta o un servicio que no deba sugerirse como instancia para cerrar para satisfacer la solicitud de tarea de capacidad. Tras seleccionar la opción que prefiera, le recomendamos que utilice el parámetro Dry Run para validar los cambios propuestos y comprender el impacto potencial antes de implementarlos.

Todos los hosts aportan las ranuras aprovisionadas a los grupos de EC2 capacidad del Outpost, y todas las ranuras de un tipo y tamaño de instancia determinados se administran como un único

grupo de EC2 capacidad. Por ejemplo, el host anterior distribuido de forma heterogénea con ranuras`m5.large`,, `m5.xlarge` `m5.2xlarge`m`5.4xlarge`, y distribuiría estas `m5.8xlarge` ranuras para formar cinco grupos de EC2 capacidad, uno para cada tipo y tamaño de instancia. Estos grupos pueden estar repartidos en varios hosts, por lo que se debe tener en cuenta la ubicación de las instancias para lograr una alta disponibilidad de la carga de trabajo.

Es importante tener en cuenta la distribución de los hosts y los grupos de EC2 capacidad al planificar la capacidad sobrante para la disponibilidad de los hosts de N+M. AWS detecta cuando un host falla o se degrada y programa una visita al sitio para reemplazar el host defectuoso. Debe diseñar sus grupos de EC2 capacidades de manera que toleren el fallo de al menos un servidor de cada familia de instancias (N+1) en un Outpost. Con este nivel mínimo de disponibilidad de hosts, cuando un host falla o es necesario dejarlo fuera de servicio, puede reiniciar las instancias defectuosas o degradadas en las ranuras libres de los hosts restantes de la misma familia.

Planificar la disponibilidad de N+M es sencillo cuando se dispone de hosts con ranuras homogéneas o grupos de hosts con ranuras heterogéneas con diseños de ranuras idénticos. Solo tiene que calcular la cantidad de hosts (N) que necesita para ejecutar todas sus cargas de trabajo y, a continuación, añadir (M) hosts adicionales para cumplir con los requisitos de disponibilidad del servidor en caso de averías o de mantenimiento.

Las siguientes configuraciones de asignación de ranuras no se pueden utilizar debido a los límites de NUMA:

- 3 `m5.8xlarge`
- 1 `m5.16xlarge` y 1 `m5.8xlarge`

Consulte a su Cuenta de AWS equipo para validar la configuración de ranuras de AWS Outposts estanterías planificada.

En la siguiente figura, cuatro `m5.24xlarge` hosts tienen ranuras heterogéneas con un diseño de ranuras idéntico. Los cuatro hosts crean cinco grupos de capacidad. EC2 Cada grupo se ejecuta con un uso máximo (75%) para mantener una disponibilidad de N+1 para las instancias que se ejecutan en estos cuatro hosts. Si algún host falla, hay espacio suficiente para reiniciar las instancias fallidas en los hosts restantes.

Visualización de las ranuras de EC2 host, las instancias en ejecución y los grupos de ranuras

Para diseños de ranuras más complejos, en los que los hosts no tienen la misma distribución, tendrá que calcular la disponibilidad de N+M para cada grupo de capacidad. EC2 Puede usar la siguiente fórmula para calcular cuántos hosts (que aportan espacios a un grupo de EC2 capacidad determinado) pueden fallar y, aun así, permitir que los hosts restantes alojen las instancias en ejecución:

$$M = \left\lceil \frac{poolSlots_{available}}{serverSlots_{max}} \right\rceil$$

Donde:

- PoolSlots $_{available}$ es la cantidad de ranuras disponibles en un grupo de EC2 capacidad determinado (el número total de ranuras del grupo menos el número de instancias en ejecución)
- ServerSlots $_{max}$ es la cantidad máxima de ranuras que cualquier host aporta a la reserva de capacidad determinada EC2
- M es la cantidad de hosts que pueden fallar y, aun así, permitir que los hosts restantes alojen las instancias en ejecución

Ejemplo: un Outpost tiene tres hosts que aportan espacios a un grupo `m5.2xlarge` de capacidad. El primero aporta 4 plazas, el segundo aporta 3 plazas y el tercer anfitrión aporta 2 plazas. El grupo

de `m5.2xlarge` instancias del Outpost tiene una capacidad total de 9 ranuras (4 + 3 + 2). El Outpost tiene 4 instancias en ejecución`m5.2xlarge`. ¿Cuántos hosts pueden fallar y seguir permitiendo que los hosts restantes alojen las instancias en ejecución?

$$poolSlots_{available} = total\ capacity - running\ instances = 9 - 4 = 5$$

$$serverSlots_{max} = \max([4, 3, 2]) = 4$$

$$M = \left\lceil \frac{poolSlots_{available}}{serverSlots_{max}} \right\rceil = \left\lceil \frac{5}{4} \right\rceil = [1.25] = 1$$

Respuesta: Puede perder cualquiera de los hosts y seguir manteniendo las instancias en ejecución en los hosts restantes.

Prácticas recomendadas para la planificación de la capacidad de cómputo

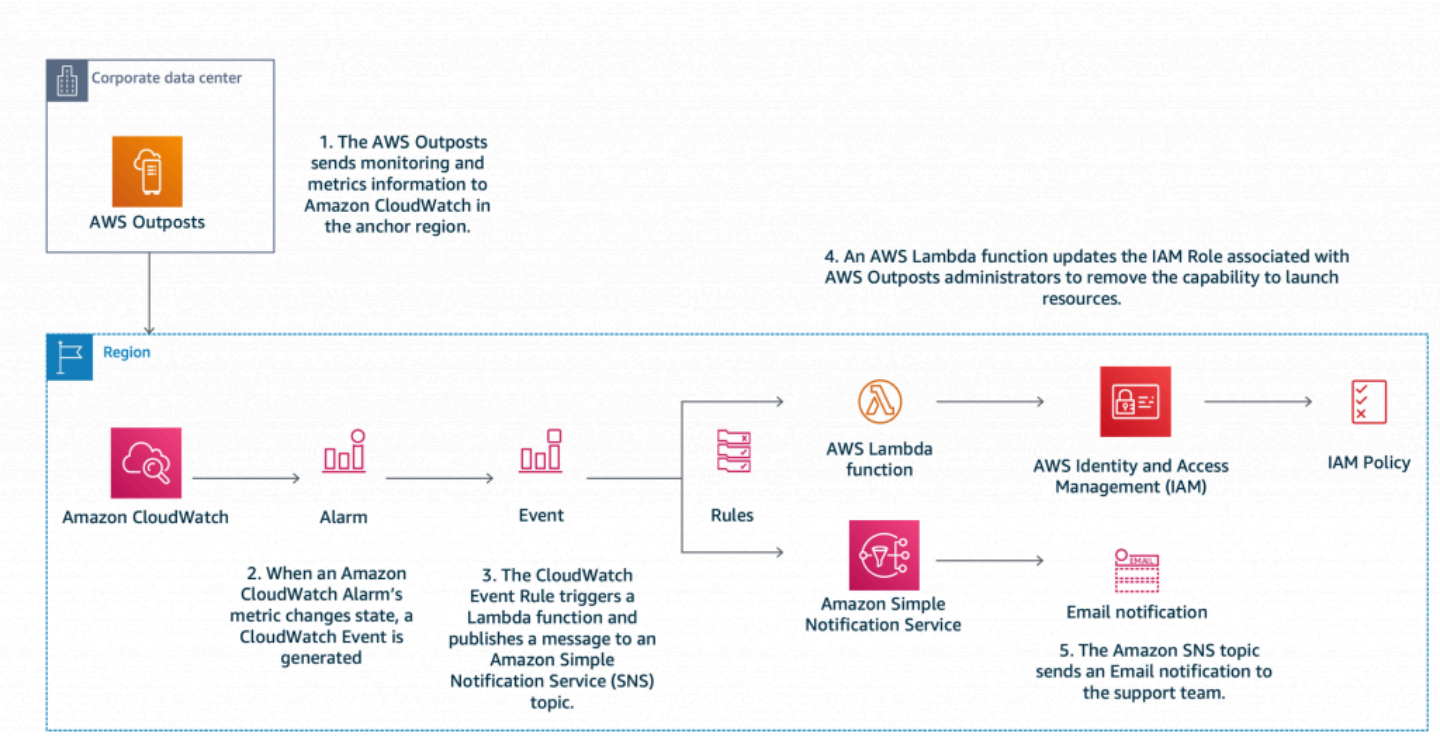
- Dimensione su capacidad de cómputo para proporcionar una redundancia N+M para cada grupo de EC2 capacidad de un Outpost.
  - Implemente servidores N+M para servidores con configuraciones homogéneas de slots, o bien heterogéneas e idénticas.
  - Calcule la disponibilidad de N+M para cada grupo de EC2 capacidad y asegúrese de que cada grupo cumpla con sus requisitos de disponibilidad.

Administración de la capacidad

Puede supervisar el uso del grupo de EC2 instancias de Outpost en las CloudWatch métricas de Amazon Consola de administración de AWS y a través de ellas. Póngase en contacto con Enterprise Support para recuperar o cambiar los diseños de slots de las implementaciones de Outposts.

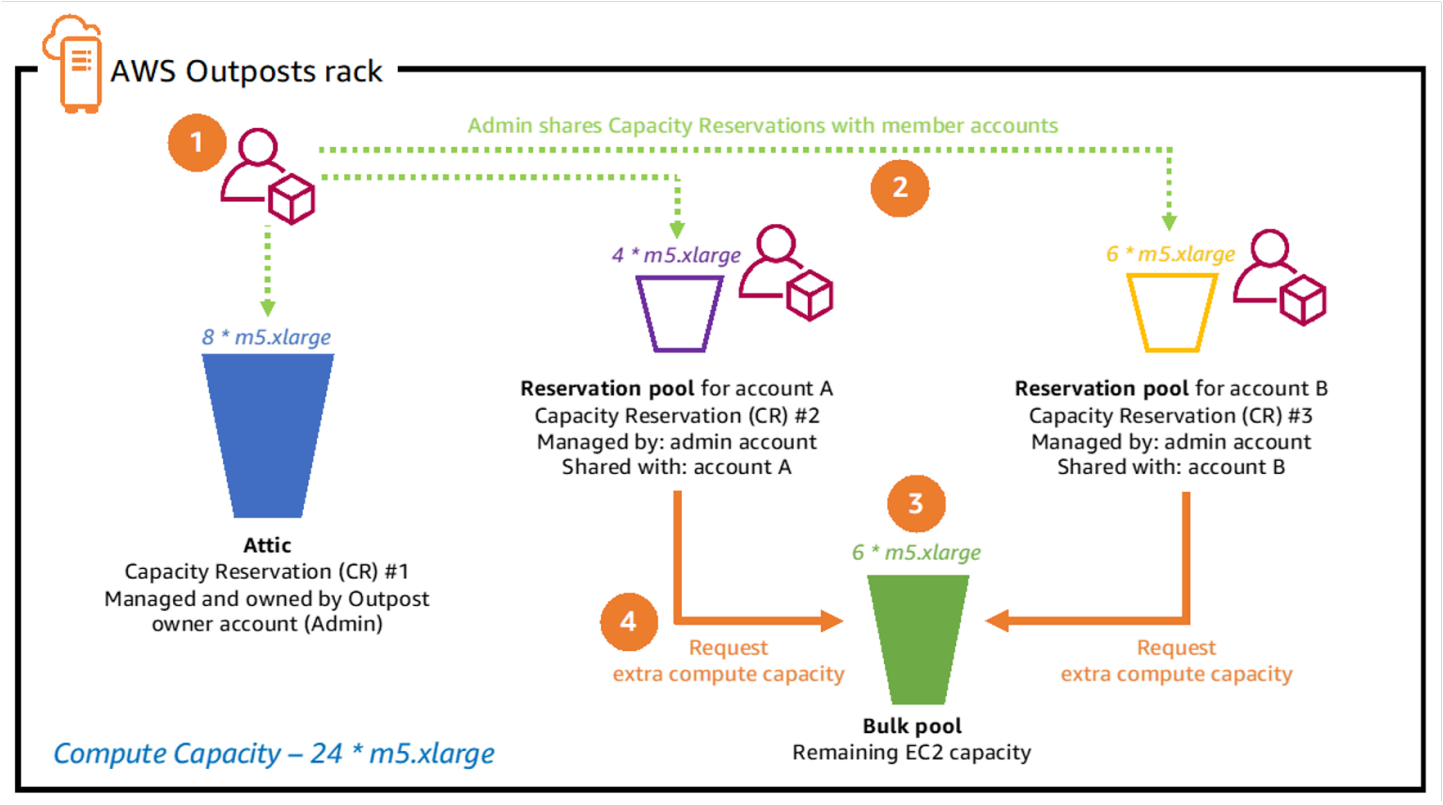
Utiliza los mismos mecanismos de recuperación automática de instancias y EC2 Auto Scaling para recuperar o reemplazar las instancias afectadas por fallas del servidor y eventos de mantenimiento. Se debe supervisar y administrar la capacidad de Outposts para garantizar que siempre haya suficiente capacidad de reserva disponible para adaptarse a los errores del servidor. La publicación Managing AWS Outposts your capacity using Amazon CloudWatch and AWS Lambda blog contiene

un tutorial práctico en el que se muestra cómo combinar AWS CloudWatch y gestionar la capacidad de Outpost AWS Lambda para mantener la disponibilidad de las instancias.

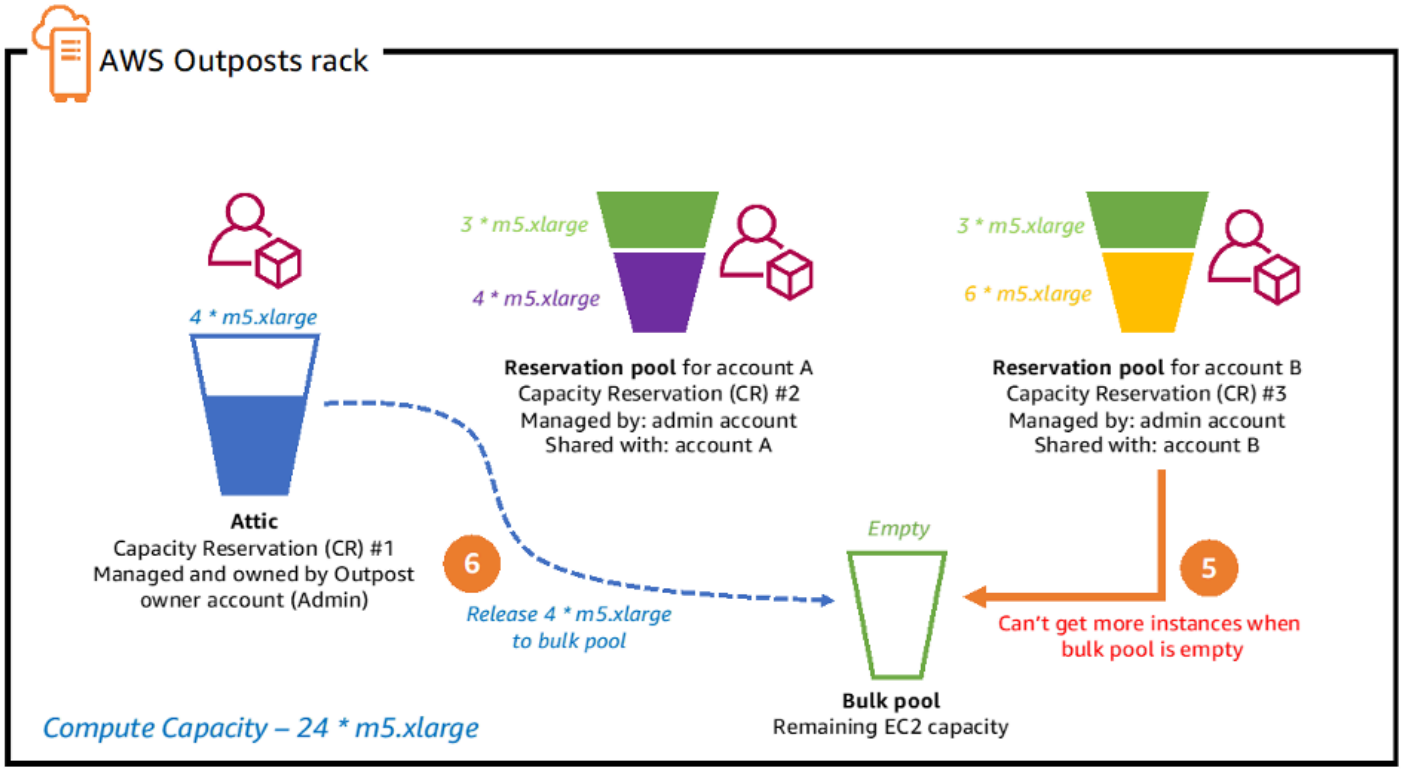


Administrar AWS Outposts la capacidad con Amazon CloudWatch y AWS Lambda

Las reservas de capacidad se pueden utilizar en un entorno de varias cuentas para controlar la cantidad de la capacidad informática de Outpost que utiliza una sola cuenta o una unidad AWS organizativa (OU) que contiene varias cuentas. Puedes crear una reserva de capacidad para Amazon EC2 en Outposts, así como para Outposts compatibles, como Amazon Elastic Kubernetes Service (EKS), Amazon Elastic Container Service (ECS) y Amazon Elastic Map Reduce (EMR). Servicios de AWS Las reservas de capacidad se crean y comparten en las cuentas a través de AWS Resource Access Manager (AWS RAM) en la cuenta del propietario de Outpost. La sección Cómo crear cuotas informáticas en AWS Outposts rack con el uso compartido de reservas de EC2 capacidad ofrece un tutorial práctico y orientación adicional para implementar las reservas de capacidad con su Outpost con el fin de gestionar la capacidad.



Capacity Reservation sharing process steps 1-4



Capacity Reservation sharing process steps 5-6

Prácticas recomendadas para la administración de la capacidad de cómputo

- Configura tus EC2 instancias en grupos de Auto Scaling o usa la recuperación automática de instancias para reiniciar las instancias fallidas.
- Automatice la supervisión de la capacidad de las implementaciones de Outposts y configure las notificaciones y (opcionalmente) las respuestas automatizadas para las alarmas de capacidad.
- Utilice las reservas de capacidad para tener un control pormenorizado sobre la cantidad de capacidad informática que se comparte con otras cuentas de su AWS organización.

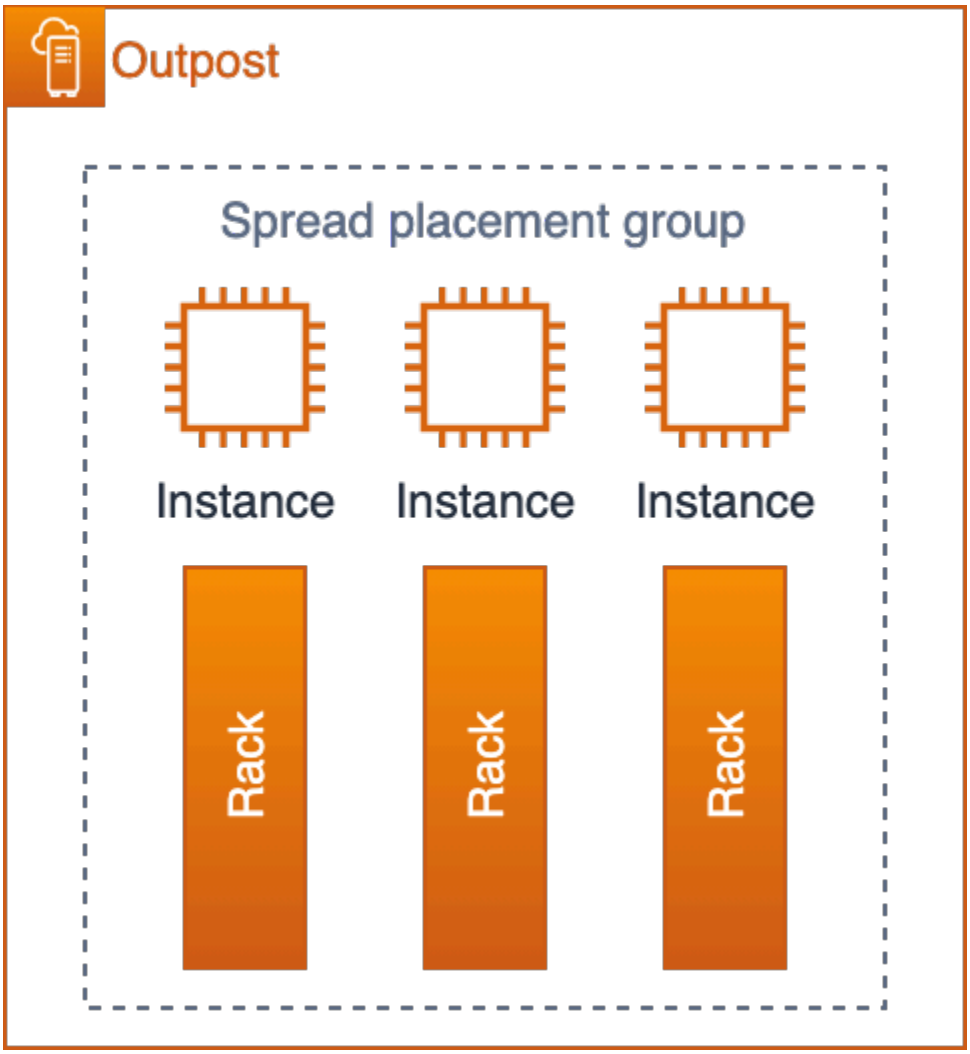
Ubicación de instancias

Los Outposts tienen un número finito de hosts de cómputo. Si tu aplicación despliega varias instancias relacionadas en Outposts, sin configuración adicional, las instancias se pueden implementar en los mismos hosts o en hosts del mismo rack. En la actualidad, existen tres mecanismos para distribuir las instancias a fin de mitigar el riesgo de ejecutar instancias relacionadas en la misma infraestructura:

Implementación de varias instancias de Outposts: de forma similar a una estrategia con múltiples zonas de disponibilidad en la región, se pueden implementar varias instancias de Outposts en centros de datos independientes, así como recursos de aplicaciones para instancias específicas de Outposts. Esto permite ejecutar instancias en la implementación de Outposts deseada (un conjunto lógico de bastidores). La comunicación dentro de la VPC entre varios Outposts con enrutamiento directo de VPC es otra estrategia que se puede utilizar para distribuir las cargas de trabajo entre varios Outposts dentro de la misma VPC mediante las puertas de enlace locales (LGW) de Outpost para crear rutas entre las subredes de los Outposts. Se puede emplear una estrategia de Outpost múltiple para protegerse contra los modos de falla del rack y del centro de datos y, si los Outposts están anclados a regiones AZs o regiones separadas, también pueden brindar protección contra los modos de falla AZ o regional. Para obtener más información acerca de las arquitecturas con múltiples implementaciones de Outposts, consulte la publicación Modos de error más extensos.

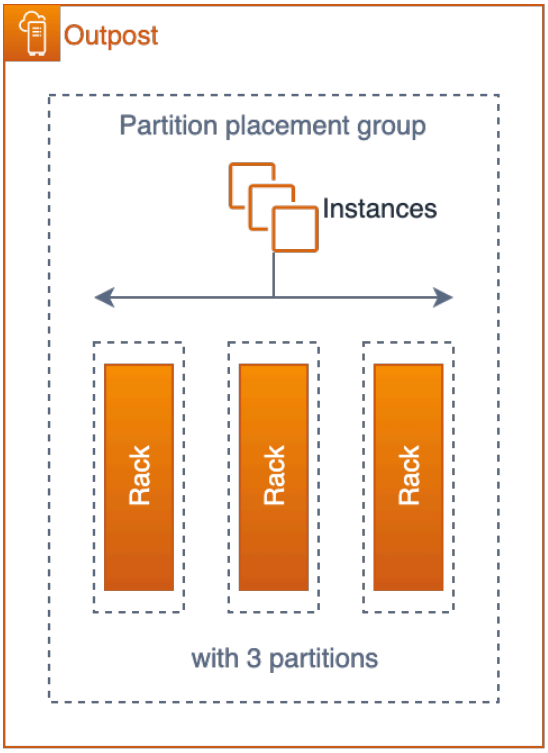
Grupos de EC2 ubicación de Amazon en Outposts (ubicación de una sola instancia de Outpost con varios estantes): puedes crear grupos de ubicación en Outposts que hayas creado en tu cuenta. Esto le permite distribuir instancias en el equipo subyacente en un Outpost en su sitio. Cuando crea un grupo de ubicación con una estrategia de distribución en Outpost, puede elegir que el grupo de ubicación distribuya instancias entre hosts o bastidores.

Un grupo de ubicación distribuida proporciona una forma sencilla de distribuir las instancias individuales entre racks o hosts para reducir la posibilidad de que se produzcan errores correlacionados. Solo puede implementar en el grupo tantas instancias como hosts tenga en su Outpost.

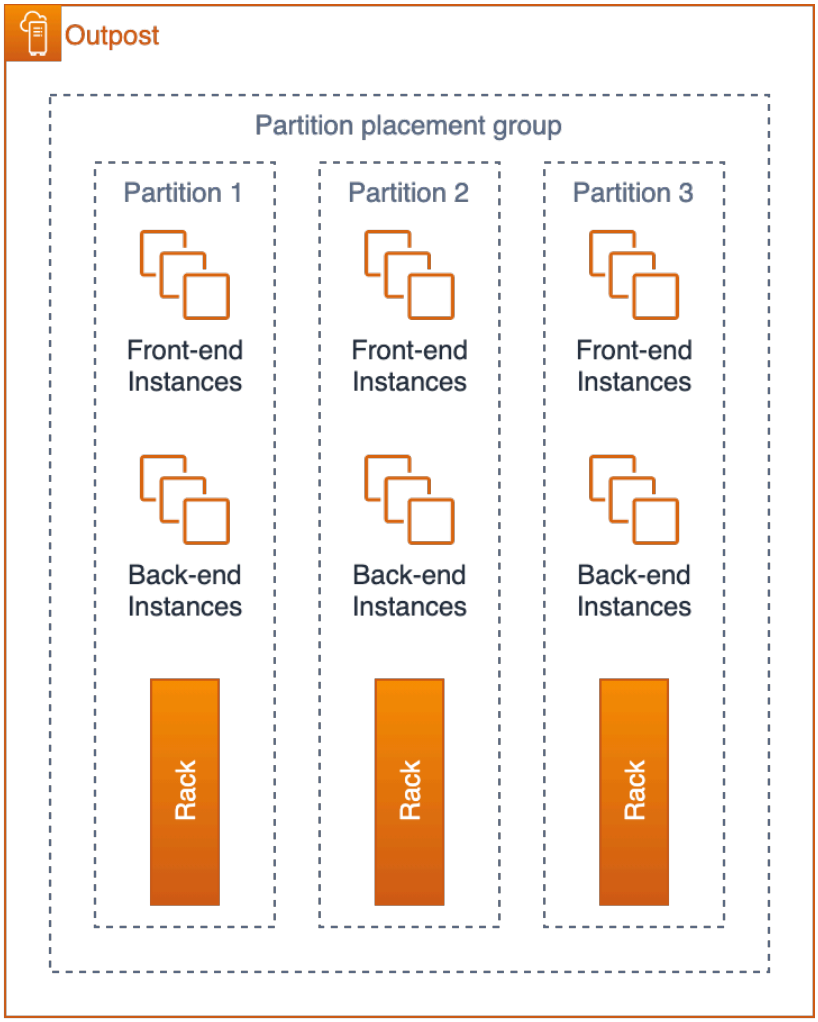


EC2 distribuya el grupo de ubicación en un puesto avanzado con tres estantes

También se pueden distribuir las instancias en varios bastidores con grupos con ubicación en particiones. La distribución automática se utiliza para distribuir las instancias entre las particiones del grupo o implementar las instancias en las particiones de destino seleccionadas. La implementación de instancias en las particiones de destino permite implementar los recursos seleccionados en el mismo bastidor y, al mismo tiempo, distribuir otros recursos entre todos los bastidores. Por ejemplo, si el usuario dispone de una instancia lógica de Outposts con tres bastidores, crear un grupo con ubicación en particiones con tres particiones le va a permitir distribuir los recursos entre los bastidores.



automatic distribution



targeted placement

EC2 grupos de ubicación de particiones en un puesto avanzado con tres estantes

Configuración creativa de slots para servidores: si el usuario cuenta con una implementación de Outposts de un solo bastidor o si el servicio que utiliza en Outposts no admite grupos de ubicación, es posible que pueda utilizar una configuración de slots creativa para que las instancias no se implementen en el mismo servidor físico. Si las instancias relacionadas tienen el mismo tamaño de EC2 instancia, es posible que pueda colocar ranuras en sus servidores para limitar la cantidad de ranuras de ese tamaño configuradas en cada servidor, distribuyendo las ranuras entre los servidores. La configuración de slots de los servidores limitará el número de instancias (de ese tamaño) que se pueden ejecutar en un único servidor.

Un ejemplo es el diseño de configuración de slots que se ha mostrado anteriormente en la figura 13. Si su aplicación necesitara implementar tres `m5.4xlarge` instancias en el Outpost configurado con este diseño de ranuras, EC2 colocaría cada instancia en un servidor independiente y no habría

posibilidad de que estas instancias se ejecutaran en el mismo servidor, siempre que la configuración de asignación de ranuras no cambie para abrir `m5.4xlarge` ranuras adicionales en los servidores.

Prácticas recomendadas para la colocación de instancias de cómputo

- Usa los grupos de EC2 ubicación de Amazon en Outposts para controlar la ubicación de las instancias en los racks dentro de un único Outpost lógico.
- En lugar de pedir un Outpost con un único rack de Outpost de tamaño mediano o grande, considere dividir la capacidad en dos racks pequeños o medianos para aprovechar la capacidad de los grupos de EC2 ubicación para distribuir las instancias entre los racks.
- El grupo Amazon EC2 Placement en Outposts se puede utilizar para influir en la ubicación de los grupos de nodos de EKS, los nodos del plano de control para el clúster local de EKS y la tarea de ECS.
- Usa la comunicación dentro de la VPC para distribuir las cargas de trabajo entre varios Outposts dentro de la misma VPC.

Almacenamiento

El servicio de almacenamiento en AWS Outposts rack ofrece tres tipos de almacenamiento:

- Almacenamiento de instancias en los tipos de EC2 instancias compatibles
- Volúmenes gp2 de Amazon Elastic Block Store (EBS) para el almacenamiento de bloques persistentes
- Amazon Simple Storage Service en Outposts (S3 en Outposts) para el almacenamiento de objetos locales

El almacenamiento de instancias se proporciona en servidores compatibles (`C5d`, `M5d`, `R5d`, `G4dn` y `I3en`). Al igual que en la región, los datos de un almacén de instancias solo se conservan durante la vida útil (ejecución) de la instancia.

Los volúmenes EBS de Outposts y el almacenamiento de objetos S3 en Outposts se proporcionan como parte de los servicios administrados de bastidores de AWS Outposts . Los clientes son responsables de la administración de la capacidad de los grupos de almacenamiento de Outposts. Los clientes especifican sus requisitos de almacenamiento para EBS y S3 al solicitar un Outpost. AWS configura el Outpost con la cantidad de servidores de almacenamiento necesarios para proporcionar la capacidad de almacenamiento solicitada. AWS es responsable de la disponibilidad

de los servicios de almacenamiento de EBS y S3 en Outposts. Se han aprovisionado suficientes servidores de almacenamiento para proporcionar servicios de almacenamiento de alta disponibilidad a Outposts. La pérdida de un único servidor de almacenamiento no debería interrumpir los servicios ni ocasionar la pérdida de datos.

Puedes usar las CloudWatch métricas Consola de administración de AWS y para monitorear la utilización de la capacidad de Outpost, EBS y S3 sobre la utilización de la capacidad de Outposts.

Protección de los datos

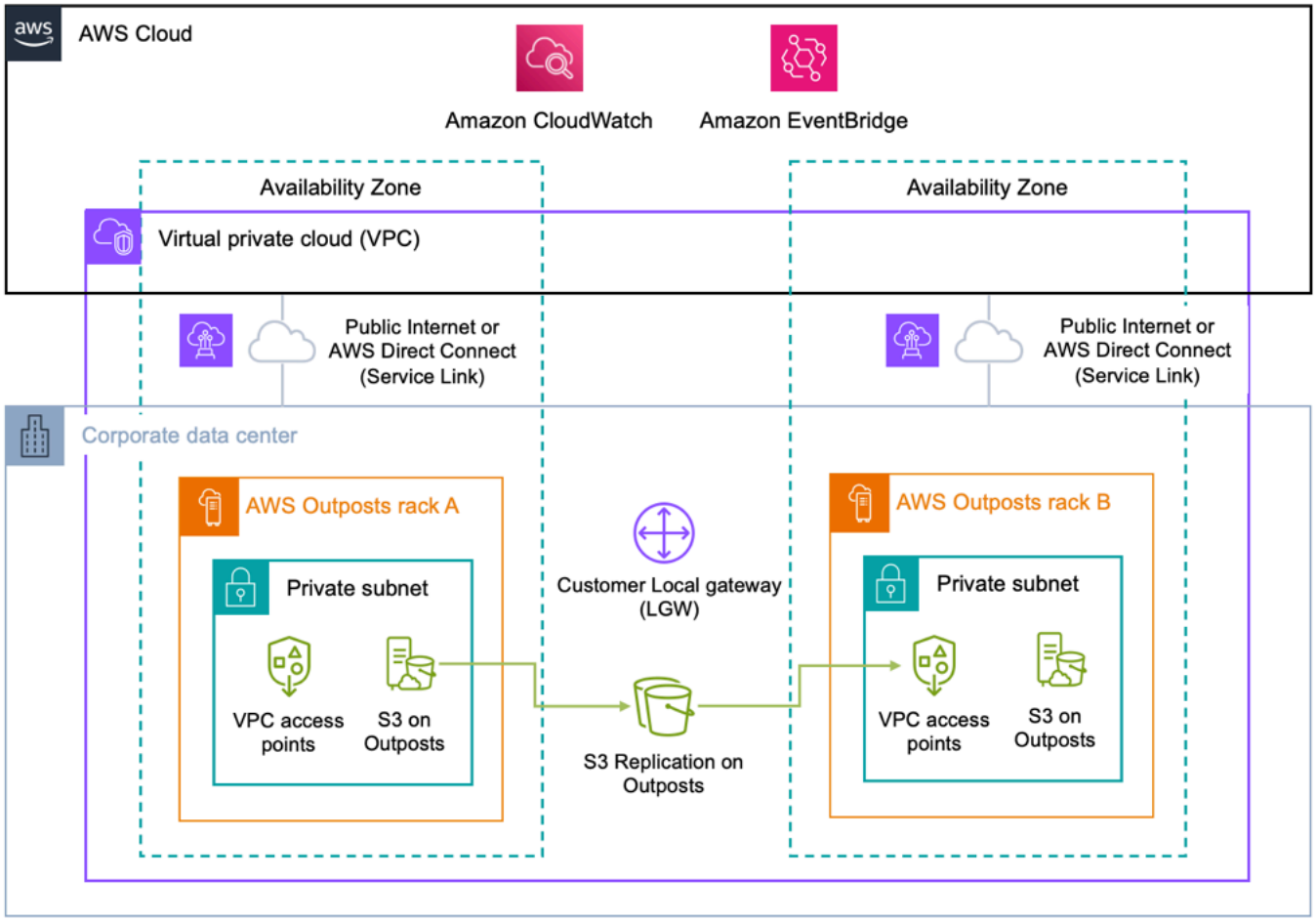
Para los volúmenes de EBS: AWS Outposts rack admite instantáneas de volúmenes de EBS para proporcionar un mecanismo de protección de datos simple y seguro que proteja los datos de almacenamiento en bloque. Las instantáneas son copias de seguridad point-in-time incrementales de sus volúmenes de EBS. De forma predeterminada, las instantáneas de los volúmenes de Amazon EBS de Outposts se almacenan en Amazon S3, en la región correspondiente. Si la capacidad de Outposts se ha configurado con S3, se pueden usar instantáneas locales de EBS en Outposts para almacenar las instantáneas localmente en la implementación de Outposts utilizando el almacenamiento de S3 en Outposts.

Para los buckets de S3 en Outposts (casos de uso de residencia de datos):

- El control de versiones de S3 en Outposts se puede utilizar para guardar todos los cambios y el historial de los objetos. Cuando está habilitado, el control de versiones de S3 guarda diversas copias de un objeto en el mismo bucket. Puede utilizar el control de versiones de S3 para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Outposts. EL control de versiones de S3 ayuda a recuperarse de acciones no deseadas del usuario y de errores de la aplicación.
- La replicación de S3 en Outposts se puede utilizar para crear y configurar reglas de replicación que repliquen automáticamente los objetos de S3 en otra instancia de Outposts o en otro bucket de la misma instancia de Outposts. Durante la replicación, los objetos de S3 en Outposts se envían a través de la puerta de enlace local (LGW) del cliente y los objetos no regresan a Región de AWS. S3 Replication on Outposts proporciona una forma fácil y flexible de replicar automáticamente los datos dentro de un perímetro de datos específico para abordar los requisitos de redundancia y cumplimiento de los datos.

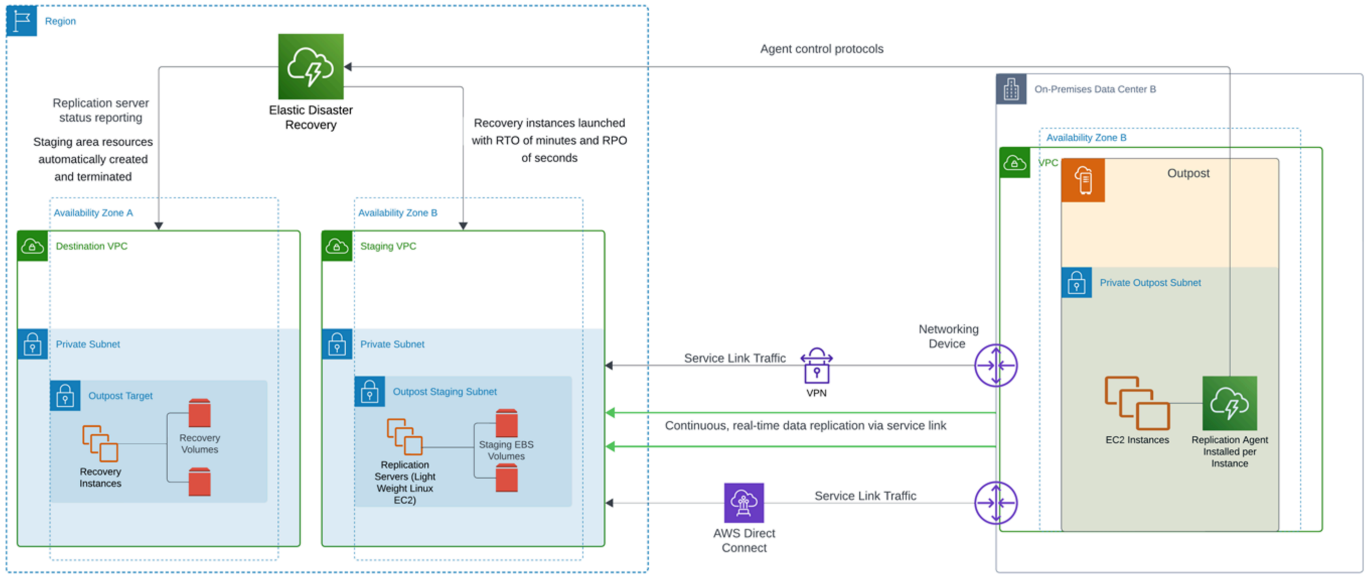
  La replicación de S3 en Outposts también proporciona métricas detalladas y notificaciones para supervisar el estado de la replicación de los objetos. Puedes monitorizar el progreso de la replicación mediante el seguimiento de los bytes pendientes, las operaciones pendientes y la

latencia de replicación entre los depósitos de Outposts de origen y destino mediante Amazon. CloudWatch También puede configurar EventBridge las reglas de Amazon para recibir eventos de error de replicación a fin de diagnosticar y corregir rápidamente los problemas de configuración. Consulte el YouTube vídeo Replicación de Amazon S3 en Outposts para obtener información adicional sobre cómo configurar.



Para grupos de S3 on Outposts (casos de uso no relacionados con la residencia de datos) a Regiones de AWS: puede utilizarlos para automatizar las transferencias de datos de AWS DataSync Amazon S3 on Outposts entre su Outpost y la región. DataSync le permite elegir qué transferir, cuándo transferir y cuánto ancho de banda utilizar. Hacer copias de seguridad en las instalaciones de los buckets de S3 en Outposts a buckets de S3 en Región de AWS permite aprovechar el 99,999999999 % (11 nueves) de durabilidad de los datos y los niveles de almacenamiento adicionales (Standard, Infrequent Access y Glacier) para optimizar los costos disponibles con el servicio S3 regional.

Replicación de instancias: puede usar AWS Elastic Disaster Recovery (AWS DRS) para replicar instancias individuales y almacenamiento en bloque adjunto desde sistemas locales a un Outpost, desde un Outpost a la región, desde la región a un Outpost o desde un Outpost a otro Outpost. La entrada del blog Architecting for Disaster Recovery on AWS Outposts Racks with AWS Elastic Disaster Recovery describe cada uno de estos escenarios y cómo diseñar una solución con DRS. AWS



Recuperación de desastres desde una implementación de Outposts a la región

El uso de AWS Outposts rack como destino de AWS DRS (objetivo de replicación) requiere el almacenamiento S3 on Outposts, que se utiliza con el fin de almacenar las instantáneas replicadas de Amazon EBS. El almacenamiento de S3 on Outposts también es necesario en los Outposts de origen para la recuperación por recuperación. El rack de Outposts debe usar el enrutamiento directo de VPC (DVR) para usar DRS. AWS AWS El DRS no se puede usar para proteger las instancias de servicios gestionados en Outposts, solo se admite para la recuperación ante desastres de las EC2 instancias y sus volúmenes de EBS adjuntos.

Prácticas recomendadas para la protección de datos

- Utilice las instantáneas de EBS para crear point-in-time copias de seguridad de los volúmenes de almacenamiento en bloque en Amazon S3 en la región o en S3 en Outposts.
- Use el control de versiones de objetos de S3 en Outposts para mantener múltiples versiones y el historial de objetos.

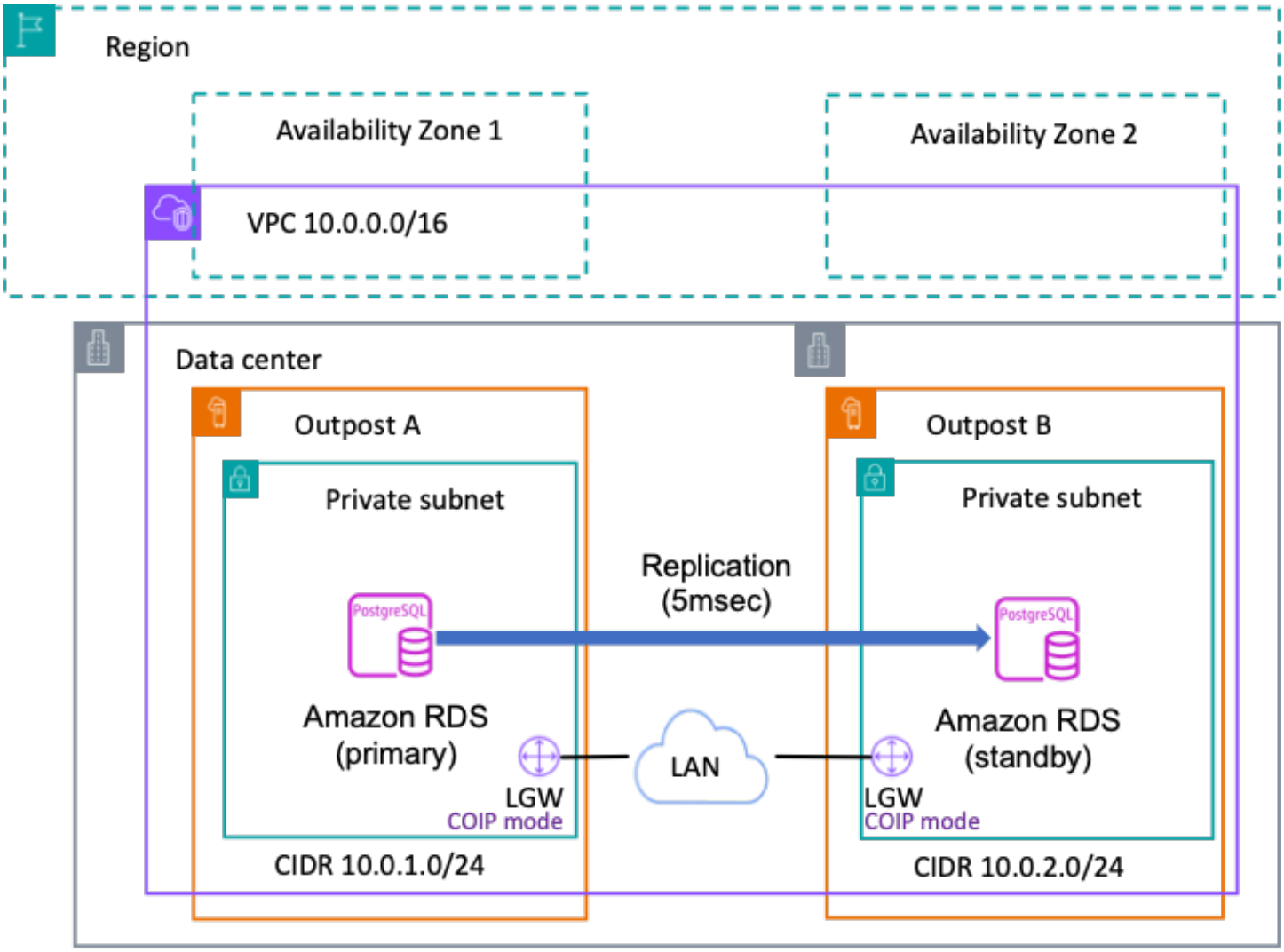
- Emplee la replicación de S3 en Outposts para replicar automáticamente los datos de los objetos en otra implementación de Outposts.
- Para los casos de uso no relacionados con la residencia de datos, AWS DataSync úselo para hacer copias de seguridad de los objetos almacenados en S3 en Outpost en Amazon S3 de la región.
- Use AWS DRS para replicar instancias entre sistemas locales, Outposts lógicos y la región.

Bases de datos

Amazon Relational Database Service (RDS) amplía las bases de datos RDS AWS Outposts para SQL Server, RDS para MySQL y RDS para PostgreSQL a las implementaciones. AWS Outposts Para aquellas implementaciones en las que se debe proporcionar una arquitectura de alta disponibilidad, Amazon RDS admite el despliegue de instancias Multi-AZ para PostgreSQL y MySQL on. AWS Outposts

Amazon RDS en Outposts con Multi-AZ

En las implementaciones Multi-AZ, Amazon RDS crea una instancia de base de datos principal en una AWS Outposts y RDS replica los datos de forma sincrónica en una instancia de base de datos en espera en un Outposts diferente. Para proporcionar una arquitectura resiliente, las dos AWS Outposts deben estar ancladas a distintas zonas de disponibilidad de una región determinada y deben funcionar según un modelo de IP propiedad del cliente (CoIP). Para permitir la replicación entre la instancia principal y la instancia en espera, debe haber un enlace de red entre los dos Outposts con una latencia de tiempo de ida y vuelta (RTT) de milisegundos de un solo dígito. Recomendamos 5 milisegundos o menos. Considere también dimensionar el enlace de replicación entre Outposts con un ancho de banda suficiente para evitar poner en cola los trabajos de replicación.



Amazon RDS en Outpost con múltiples zonas de disponibilidad

Consideraciones para Amazon RDS en Outposts con Multi-AZ

Revise las siguientes consideraciones para las implementaciones de Amazon RDS on Outposts en zonas de disponibilidad múltiples (Multi-AZ):

- Ten al menos dos despliegues de Outposts anclados en diferentes zonas de disponibilidad en la misma zona. Región de AWS
- Tanto la instancia principal como la instancia en espera requieren una sola VPC y una subred por implementación de Outposts.
- Asocie la VPC de la instancia de base de datos a todas las tablas de enrutamiento de la puerta de enlace local.
- Asegúrate de que tus Outposts usen el enrutamiento IP propiedad del cliente.

- Tu red local debe permitir el tráfico saliente y el tráfico entrante relacionado entre Outposts for Internet Security Association y Key Management Protocol (ISAKAMP), que utilizan el puerto UPD 500, y IPsec Network Address Translation Traversal (NAT-T), que utiliza el puerto UDP 4500.
- Las copias de seguridad de RDS locales no son compatibles con las implementaciones Multi-AZ.
- Si su carga de trabajo debe cumplir con las normas de residencia de datos de su sector o región geográfica, consulte a las autoridades reguladoras para determinar si el RDS Multi-AZ cumplirá sus requisitos.

Para obtener más información, consulte Cómo trabajar con despliegues Multi-AZ para Amazon RDS en AWS Outposts.

Amazon RDS en réplicas de AWS Outposts lectura

Las réplicas de lectura de Amazon RDS proporcionan un rendimiento y una durabilidad mejorados para las instancias de bases de datos (DB) de Amazon RDS. Facilitan la escalabilidad elástica más allá de las limitaciones de capacidad de una sola instancia de base de datos para cargas de trabajo de bases de datos con un uso intensivo de lecturas. Amazon RDS on AWS Outposts utiliza la funcionalidad de replicación integrada en los motores de base de datos MySQL y PostgreSQL para crear una réplica de lectura a partir de una instancia de base de datos de origen. La instancia de base de datos de origen se convierte en la instancia de base de datos principal. Las actualizaciones realizadas en la instancia de base de datos principal se copian de forma asíncrona en la réplica de lectura. La réplica de lectura utiliza un modelo de IP propiedad del cliente (CoIP) y las replicaciones se ejecutan en su red local.

Consideraciones para Amazon RDS sobre las réplicas de lectura de Outposts

Revise las siguientes consideraciones para las implementaciones de Amazon RDS on Outposts para réplicas de lectura:

- No puede crear réplicas de lectura en RDS para SQL Server en instancias de bases de datos de RDS en Outposts.
- Las réplicas de lectura entre regiones no se admiten en RDS en Outposts.
- Las réplicas de lectura en cascada no se admiten en RDS en Outposts.
- La instancia de base de datos de origen de RDS en Outposts no puede tener copias de seguridad locales. El destino de la copia de seguridad para la instancia de base de datos de origen debe ser su Región de AWS. Asegúrese de tener una conexión de enlace de servicio redundante de al

menos 500 Mbps para enviar sus copias de seguridad de RDS a Región de AWS bases de datos con datos que cambian con frecuencia o con un tráfico de escritura intenso.

- Las réplicas de lectura requieren grupos de IP propiedad del cliente (CoIP).
- Las réplicas de lectura en RDS en Outposts solo se pueden crear en la misma nube privada virtual (VPC) que la instancia de base de datos de origen.
- Las réplicas de lectura de RDS en Outposts pueden estar ubicadas en el mismo Outpost o en otro de la misma VPC que la instancia de base de datos de origen.
- No puede crear réplicas de lectura para instancias de base de datos cifradas con un almacén de claves AWS KMS externo (XKS).
- La creación de su réplica de lectura como instancia de base de datos Multi-AZ es independiente de si la base de datos de origen es una instancia de base de datos Multi-AZ.

El escalado automático del almacenamiento de Amazon RDS está activado AWS Outposts

Si su carga de trabajo es impredecible, puede habilitar el escalado automático de almacenamiento para una instancia de base de datos de Amazon RDS. Amazon Relational Database Service (Amazon RDS) admite AWS Outposts el escalado de almacenamiento manual y automático. Con el escalado automático del almacenamiento activado, cuando Amazon RDS detecta que su instancia de base de datos se está quedando sin espacio libre en la base de datos, amplía automáticamente el almacenamiento en función de la capacidad de EBS dimensionada para su implementación de Outposts. La función proporciona las mismas capacidades que en las regiones en las que hay algunos factores específicos que se aplican al escalado automático, como se puede encontrar en la guía de escalado automático de Amazon RDS. Es importante administrar cuidadosamente el almacenamiento máximo asignado a las instancias de RDS en Outposts, ya que los recursos de EBS están restringidos a la capacidad aprovisionada en Outpost. El escalado automático del almacenamiento de Amazon RDS le permite establecer un límite máximo de almacenamiento, lo que garantiza que su implementación se mantenga dentro de la capacidad de EBS disponible. Para obtener más información sobre la gestión de la capacidad de Outposts, consulta la sección Gestión de la capacidad de este documento técnico.

Amazon RDS en el backup AWS Outposts local

Las copias de seguridad locales de Amazon RDS le AWS Outposts permiten recuperar una instancia de base de datos de RDS directamente desde S3 almacenada localmente en sus Outposts. Esto le permite cumplir con los requisitos de residencia de los datos y reduce la latencia en comparación con

la recuperación de una. Región de AWS Con Amazon RDS activado AWS Outposts, dispone de las siguientes opciones de restauración:

- A partir de una instantánea de base de datos manual almacenada en la región principal o localmente en tus Outposts.
- una copia de seguridad automática (point-in-time recuperación):
  - Si lo restauras desde el dispositivo principal Región de AWS, puedes almacenar las copias de seguridad en tus Outposts Región de AWS o en ellos.
  - Si restauras desde Outposts, las copias de seguridad deben almacenarse localmente en Outposts compatibles con S3.

Consideraciones sobre el backup local de Amazon RDS en AWS Outposts

Consulte las siguientes consideraciones para aprovechar las copias de seguridad locales de Amazon RDS en AWS Outposts:

- Necesitas la capacidad de S3 en Outposts para almacenar las copias de seguridad localmente.
- Las instancias de base de datos MySQL y PostgreSQL admiten copias de seguridad locales.
- Las copias de seguridad locales no se admiten en las implementaciones de instancias Multi-AZ ni en las réplicas de lectura.

Exportación y restauración de instantáneas para RDS en AWS Outposts

Exportación de instantáneas a S3 y restauración de una instancia de base de datos desde Amazon S3: si bien las instantáneas de RDS se pueden exportar o restaurar directamente desde Amazon S3 en el Región de AWS, esto no es compatible con los entornos. AWS Outposts

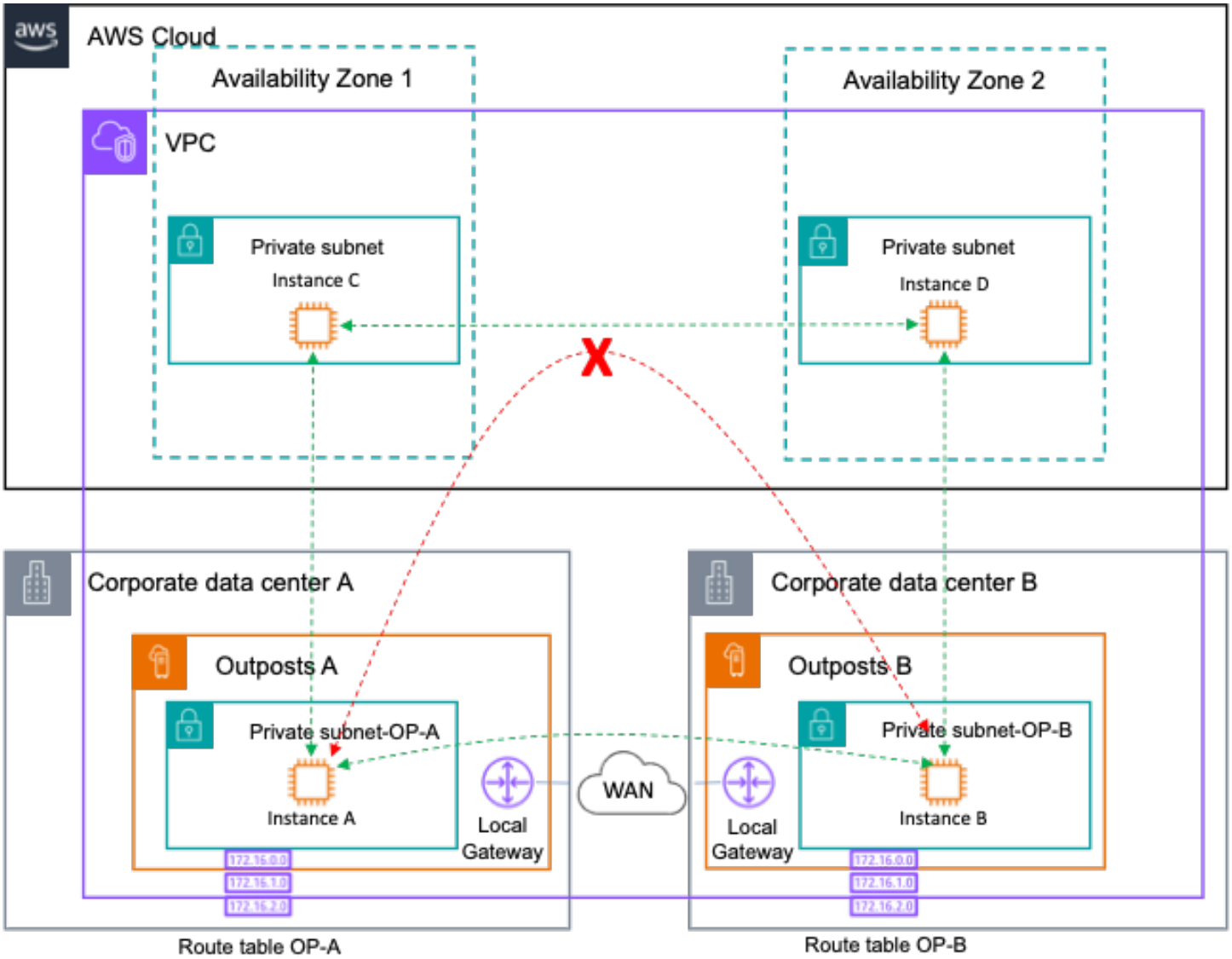
Modos de error más extensos

Para diseñar arquitecturas de alta disponibilidad que mitiguen los modos de error más extensos, como errores de bastidor, de centro de datos, de zonas de disponibilidad (AZ) o de regiones, es necesario implementar varias instancias de Outposts con suficiente capacidad de infraestructura en centros de datos separados con conectividad WAN y alimentación independientes. Anclas los Outposts a diferentes zonas de disponibilidad (AZs) dentro de una Región de AWS o entre varias regiones. También debe proporcionar una site-to-site conectividad flexible y suficiente entre las ubicaciones para admitir la replicación de datos sincrónica o asincrónica y la redirección del tráfico

de la carga de trabajo. Según la arquitectura de tu aplicación, puedes usar Amazon Route 53 DNS y Amazon Route 53 en Outposts, disponibles en todo el mundo, para dirigir el tráfico a la ubicación deseada y automatizar el redireccionamiento del tráfico a las ubicaciones supervivientes en caso de que se produzcan errores a gran escala.

Enrutamiento dentro de la VPC de Outposts Rack

AWS Outposts rack admite la comunicación dentro de la VPC a través de varios Outposts. Los recursos de dos Outposts lógicos separados pueden comunicarse entre sí mediante el enrutamiento del tráfico entre subredes dentro de la misma VPC que las atraviesa mediante las puertas de enlace locales (LGW) de Outpost. Con la comunicación dentro de la VPC entre varios Outposts, puedes anular la ruta local en la tabla de rutas asociada a la subred de Outposts añadiendo una ruta más específica a la otra subred de Outposts utilizando la LGW local como siguiente salto. Puede ofrecer ventajas a la hora de diseñar aplicaciones que requieren extender una VPC entre dos Outposts lógicos, como Amazon ECS en dos racks de Outposts o un clúster de Amazon EKS entre sí. AWS Outposts

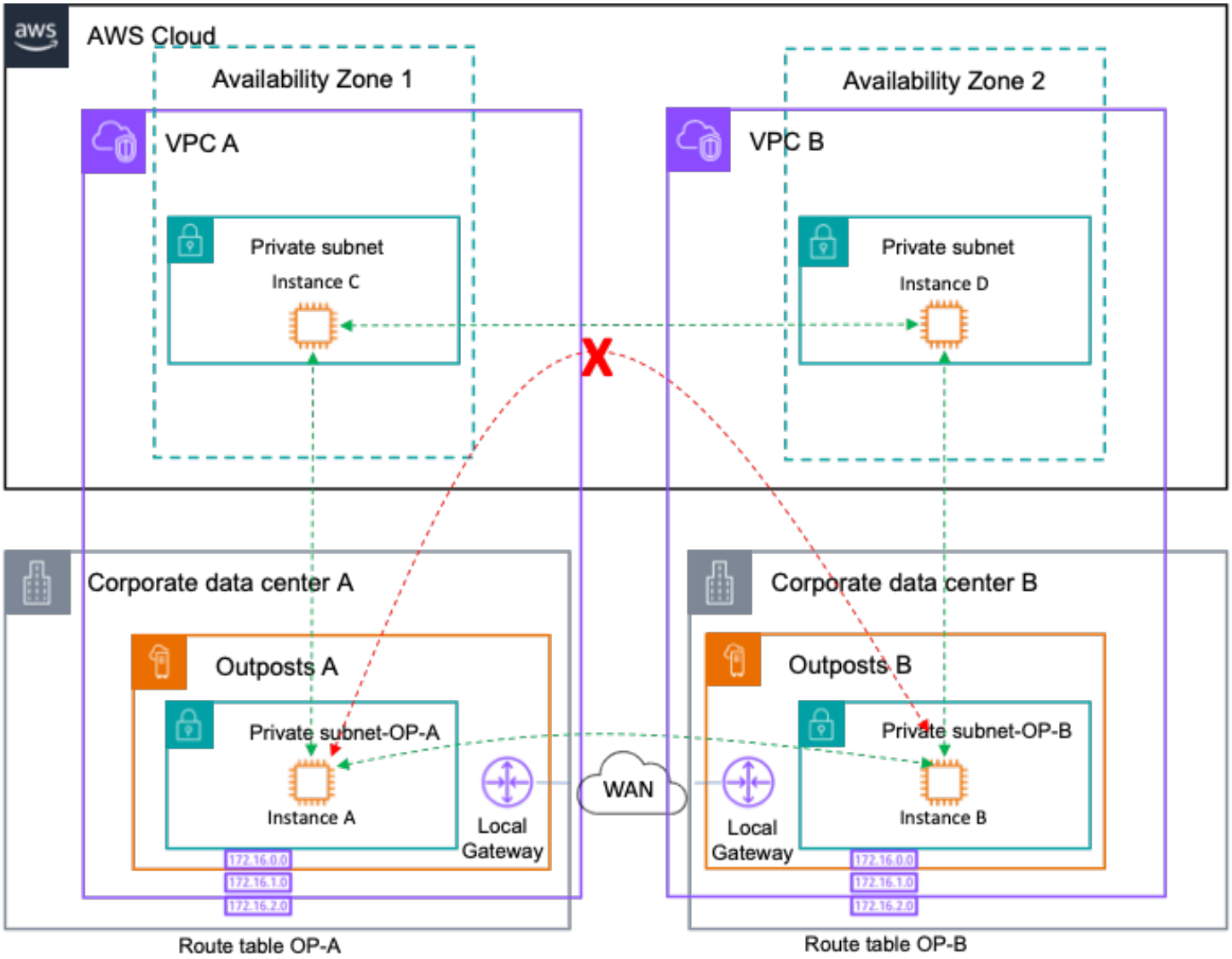


Rutas de red para una sola VPC con múltiples Outposts lógicos

Outposts-to-Outposts El enrutamiento del tráfico a través de la región está bloqueado, ya que no es un patrón. Este tráfico generaría gastos de salida en ambas direcciones y una latencia significativamente mayor que si se enrutara el tráfico a través de la WAN del cliente.

Enrutamiento entre VPC de Outposts Rack

Los recursos de dos Outposts separados desplegados en lugares diferentes VPCs pueden comunicarse entre sí a través de la red del cliente. La implementación de esta arquitectura le permite enrutar el tráfico a Outposts-to-Outposts través de sus redes locales locales y WAN, agregando rutas hacia las subredes de VPC o Outpost homólogas.



Rutas de red para múltiples VPC con múltiples Outposts lógicos

Prácticas recomendadas para protegerse frente a modos de error más extensos

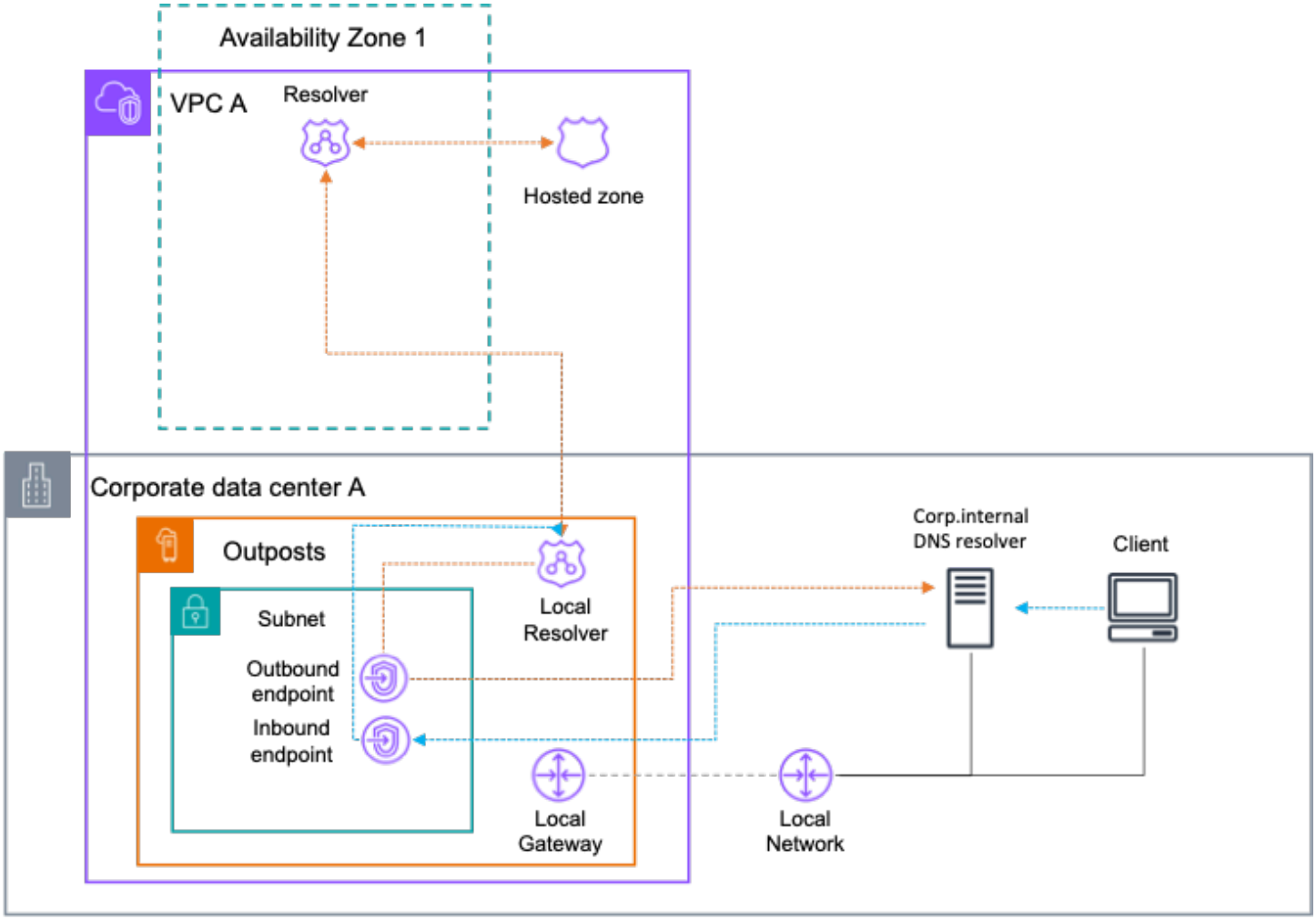
- Despliega varios Outposts anclados en múltiples AZs regiones.
- Utilízalo VPCs por separado para cada puesto de avanzada en un despliegue de varios puestos de avanzada.

Route 53 Local Resolver en Outposts

Cuando el enlace del AWS Outposts servicio se ve afectado por una desconexión temporal, la resolución del DNS local falla, lo que dificulta que las aplicaciones y los servicios descubran otros

servicios, incluso cuando se ejecutan en el mismo rack de Outposts. Sin embargo, con Route 53 Resolver activado AWS Outposts, las aplicaciones y los servicios seguirán beneficiándose de la resolución de DNS local para detectar otros servicios, incluso en el caso de que el principal pierda la conectividad Región de AWS. Al mismo tiempo, para la resolución de DNS para nombres de host locales, el Route 53 Resolver de Outposts ayuda a reducir la latencia, ya que los resultados de las consultas se almacenan en caché y se sirven localmente, a la vez que se integra completamente con los puntos finales de Route 53 Resolver.

Los puntos finales entrantes del solucionador de Route 53 reenvían las consultas de DNS que reciben desde fuera de la VPC al solucionador que se ejecuta en Outposts. Por el contrario, Route 53 Resolver Outbound permite a los Resolvers de Route 53 reenviar consultas de DNS a los solucionadores de DNS que usted administra en la red local, como se ilustra en el siguiente diagrama.



Resolver Route 53 en Outposts

Consideraciones sobre Route 53 Resolver on Outposts

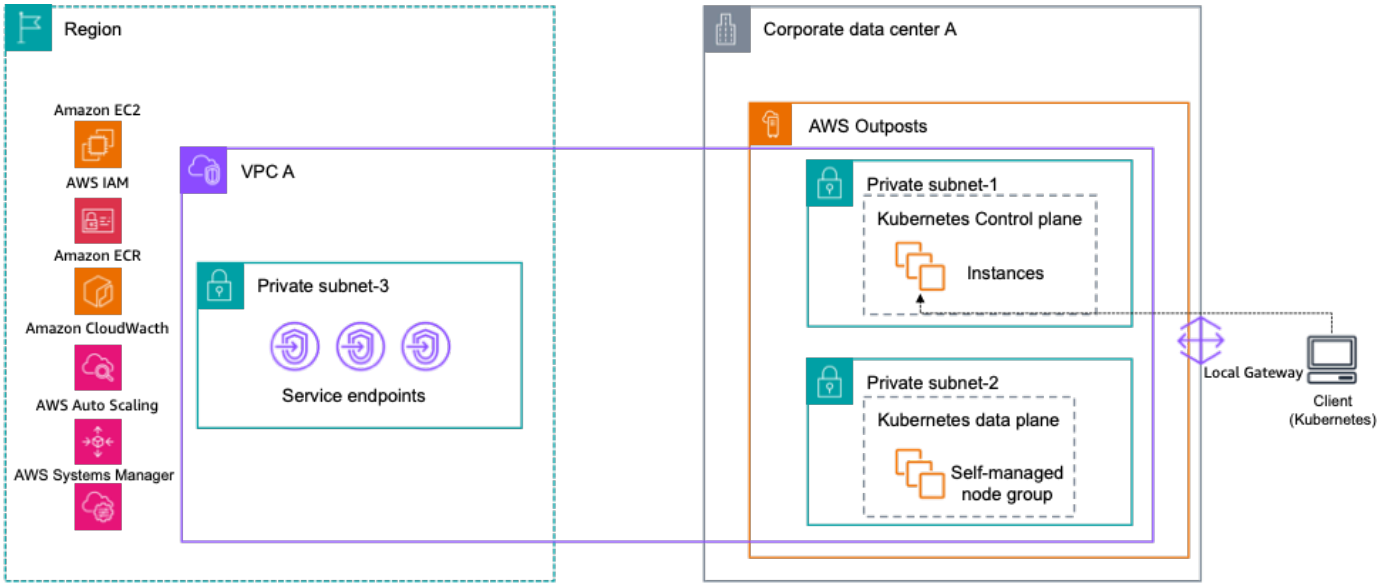
Considere lo siguiente:

- Debes habilitar el Solucionador de Route 53 en Outposts y se aplica a todo el despliegue de Outposts, incluso si se trata de varios racks de cómputo con un único ID de Outposts.
- Para habilitar esta función, tus Outposts deben tener suficiente capacidad de cómputo para implementar el solucionador local en forma de al menos 4 EC2 instancias de cualquier c5.xlarge, m5.large o m5.xlarge.
- Si utiliza un DNS privado, debe compartir la zona alojada privada con los Outposts VPCs necesarios para almacenar en caché los registros de forma local en el Route 53 Resolver de Outposts.
- Para permitir la integración con el DNS local con los puntos de conexión entrantes y salientes, sus Outposts deben tener suficiente capacidad de procesamiento para implementar dos instancias por cada punto de conexión de Route53. EC2

Clúster local de EKS en Outposts

Cuando se produce una desconexión del enlace del servicio de Outposts desde la región matriz, es posible que surjan problemas con servicios como el EKS Extended Cluster, donde el plano de control se encuentra en la región. Entre los desafíos está la pérdida de comunicación entre el plano de control del EKS y los nodos trabajadores y. PODs Aunque ambos nodos de trabajo PODs pueden seguir funcionando y dando servicio a las aplicaciones que residen en Outposts de forma local, el plano de control de Kubernetes puede considerarlas insalubres y programar su reemplazo cuando se recupere la conexión con el plano de control. Esto puede provocar tiempos de inactividad de las aplicaciones cuando se restablezca la conectividad.

Para simplificar esto, existe la opción de alojar todo tu clúster de EKS en Outposts. En esta configuración, tanto el plano de control de Kubernetes como los nodos de trabajo se ejecutan localmente en las instalaciones de la capacidad de cómputo de Outposts. De esta forma, el clúster seguirá funcionando incluso en caso de que se interrumpa temporalmente la conexión del enlace de servicio y después de que se restablezca.



Clúster local de Amazon EKS en Outposts

Consideraciones sobre el Clúster Local de EKS en Outposts

Hay algunas consideraciones a tener en cuenta a la hora de implementar un clúster local de EKS en Outposts:

- Durante una desconexión, no hay opciones para ejecutar ningún cambio en el propio clúster que requiera agregar nuevos nodos de trabajo o escalar automáticamente un grupo de nodos, siempre que EC2 dependa de las llamadas de la API de ASG a la AWS región principal.
- • Hay un conjunto de funciones no compatibles en los clústeres locales que figuran en la lista de compatibilidad con eksctl. AWS Outposts .

Conclusión

Con AWS Outposts rack, puede crear, gestionar y escalar aplicaciones locales de alta disponibilidad mediante AWS herramientas y servicios conocidos, como Amazon EC2, Amazon EBS, Amazon S3 on Outposts, Amazon ECS, Amazon EKS y Amazon RDS. Las cargas de trabajo pueden ejecutarse de forma local, servir a clientes, acceder a las aplicaciones y los sistemas de las redes en las instalaciones y acceder al conjunto completo de servicios de Región de AWS. Los bastidores de Outposts son ideales para cargas de trabajo que requieren acceso de baja latencia a sistemas en las instalaciones, procesamiento de datos local, residencia de datos y migración de aplicaciones con interdependencias de sistemas locales.

Si proporciona una implementación de Outpost con la energía, el espacio y la refrigeración adecuados y conexiones flexibles Región de AWS, puede crear servicios de centro de datos únicos de alta disponibilidad. Para obtener niveles más altos de disponibilidad y resiliencia, se pueden implementar varias instancias de Outposts y distribuir las aplicaciones más allá de límites lógicos y geográficos.

El rack Outposts elimina el pesado trabajo indiferenciado de crear grupos de redes de aplicaciones, almacenamiento y cómputo locales y le permite extender el alcance de la infraestructura AWS global a sus centros de datos e instalaciones de ubicación conjunta. Los usuarios ya pueden dedicar su tiempo y energía a modernizar sus aplicaciones, agilizar las implementaciones y hacer que los servicios de TI repercutan más y mejor en la empresa.

Colaboradores

Los colaboradores de este documento son:

- Jesus Federico, arquitecto principal de soluciones, Telco, Amazon Web Services
- Mallory Gershenfeld, S3 en Outposts, Amazon Web Services
- Rob Goodwin, arquitecto sénior de soluciones, nube híbrida, Amazon Web Services
- Chris Lunsford, arquitecto sénior especializado en soluciones AWS Outposts, Amazon Web Services
- Rohan Mathews, arquitecto principal de Amazon AWS Outposts Web Services
- Brianna Rosentrater, arquitecta especializada en soluciones Hybrid Edge, Amazon Web Services
- Leonardo Solano, arquitecto principal de soluciones especializadas en Hybrid Edge, Amazon Web Services
-

Historial del documento

Para recibir notificaciones sobre las actualizaciones de este documento técnico, suscríbase a la fuente RSS.

Cambio	Descripción	Fecha
Actualización importante	Se agregaron actualizaciones sobre redes, compatibilidad con DRS, Amazon EKS Local Cluster, Placement Groups y Amazon RDS en AWS Outposts	24 de noviembre de 2024
Actualización menor	Se agregó una guía adicional de asignación de fechas en la planificación de la capacidad.	9 de febrero de 2024
Actualización menor	Se ha actualizado para reflejar el lanzamiento de nuevas características desde su publicación inicial.	19 de julio de 2023
Actualización menor	Se han actualizado las prácticas recomendadas para conexiones de redes de alta disponibilidad.	29 de junio de 2023
Publicación inicial	Documento técnico publicado por primera vez.	12 de agosto de 2021

> **Note**
>
> Para suscribirse a las actualizaciones de RSS, debe tener un complemento de RSS habilitado para el navegador que esté utilizando.

Avisos

Es responsabilidad de los clientes realizar su propia evaluación independiente de la información que contiene este documento. Este documento: (a) tiene únicamente fines informativos, (b) representa las ofertas y prácticas de AWS productos actuales, que están sujetas a cambios sin previo aviso, y (c) no crea ningún compromiso ni garantía por parte de AWS sus filiales, proveedores o licenciantes. AWS los productos o servicios se proporcionan «tal cual» sin garantías, representaciones o condiciones de ningún tipo, ya sean expresas o implícitas. Las responsabilidades y obligaciones de AWS sus clientes están reguladas por AWS acuerdos, y este documento no forma parte de ningún acuerdo entre sus clientes AWS y sus clientes ni lo modifica.

© 2023 Amazon Web Services, Inc. o sus filiales. Todos los derechos reservados.

AWS Glosario

Para obtener la AWS terminología más reciente, consulte el AWS glosario de la Glosario de AWS Referencia.

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.