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

AWS Guía prescriptiva

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

Table of Contents

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

Amazon Web Services (colaboradores)

Junio de 2025 (historial del documento)

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

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

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

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

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

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

En esta guía:

Información general

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

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

Talleres sobre la nube híbrida

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

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

PoCs

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

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

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

Pilares

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

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

Requisitos previos y limitaciones

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

Requisitos previos

AWS Outposts

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

Zonas locales de AWS

- Debe haber una zona AWS local disponible cerca de sus centros de datos o usuarios. Consulte Zonas locales de AWS las ubicaciones.
- Confirme que tiene conectividad de red desde su infraestructura local a la zona local:
  - Opción 1: un AWS Direct Connect enlace desde el centro de datos al AWS Direct Connect punto de presencia (PoP) más cercano a la zona local. Para obtener más información, consulte Direct Connect en la documentación de las Zonas Locales.

- Opción 2: un enlace a Internet además de un dispositivo de red privada virtual (VPN) local y las licencias necesarias para lanzar un dispositivo VPN basado en software EC2 en Amazon en la zona local. Para obtener más información, consulte Conexión VPN en la documentación de las Zonas Locales.

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

Limitaciones

AWS Outposts

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

Zonas locales de AWS

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

Proceso de adopción de la nube híbrida

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

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

Redes en la periferia

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

Arquitectura de VPC

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

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

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

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

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

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

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

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

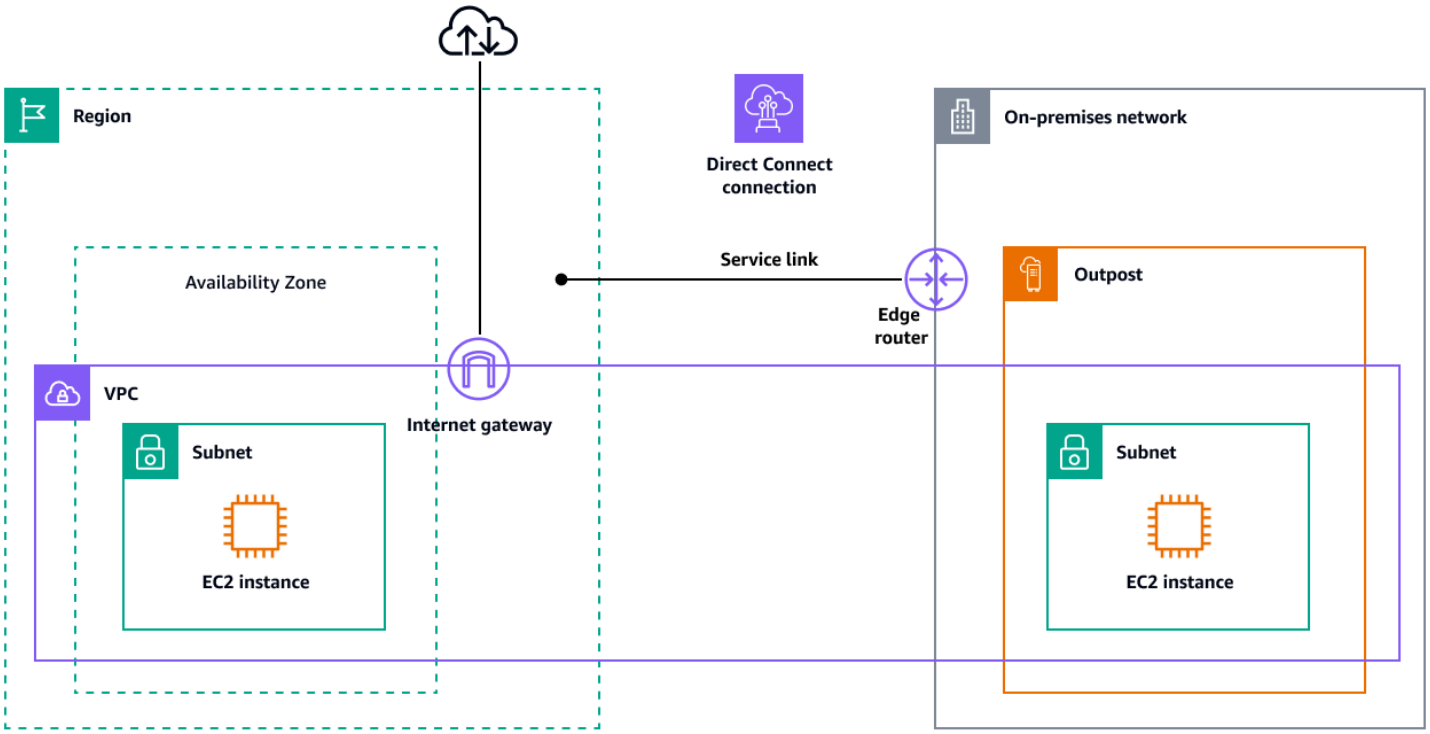
Tráfico de extremo a región

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

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

AWS Outposts plano de control

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



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

AWS Outposts plano de datos

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

Los requisitos de ancho de banda varían en función de las siguientes características:

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

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

Plano de datos de Zonas Locales

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

En la siguiente tabla se muestran las opciones de conexión y las asociadas MTUs.

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

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

El tráfico se extiende desde el límite hasta el tráfico local

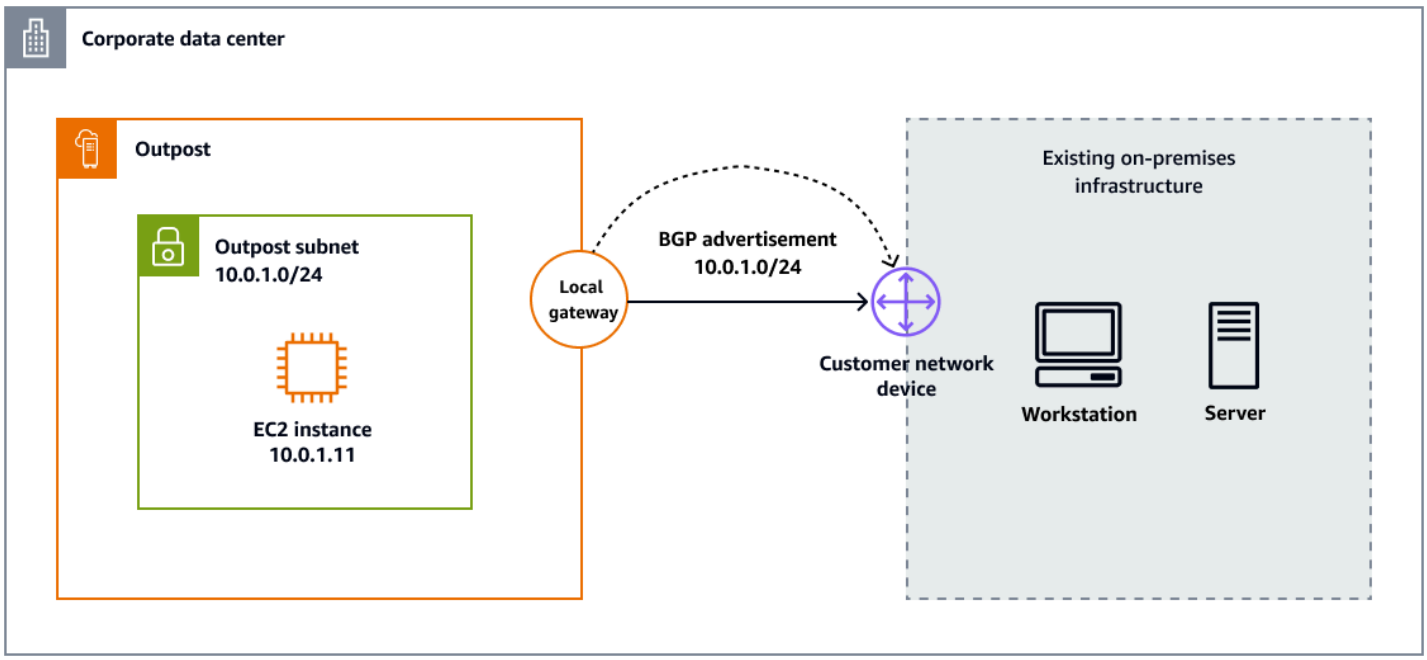
AWS Los servicios de nube híbrida están diseñados para abordar casos de uso que requieren baja latencia, procesamiento de datos local o cumplimiento de la residencia de datos. La arquitectura de red para acceder a estos datos es importante y depende de si la carga de trabajo se ejecuta en Zonas Locales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

AWS Outposts puerta de enlace local

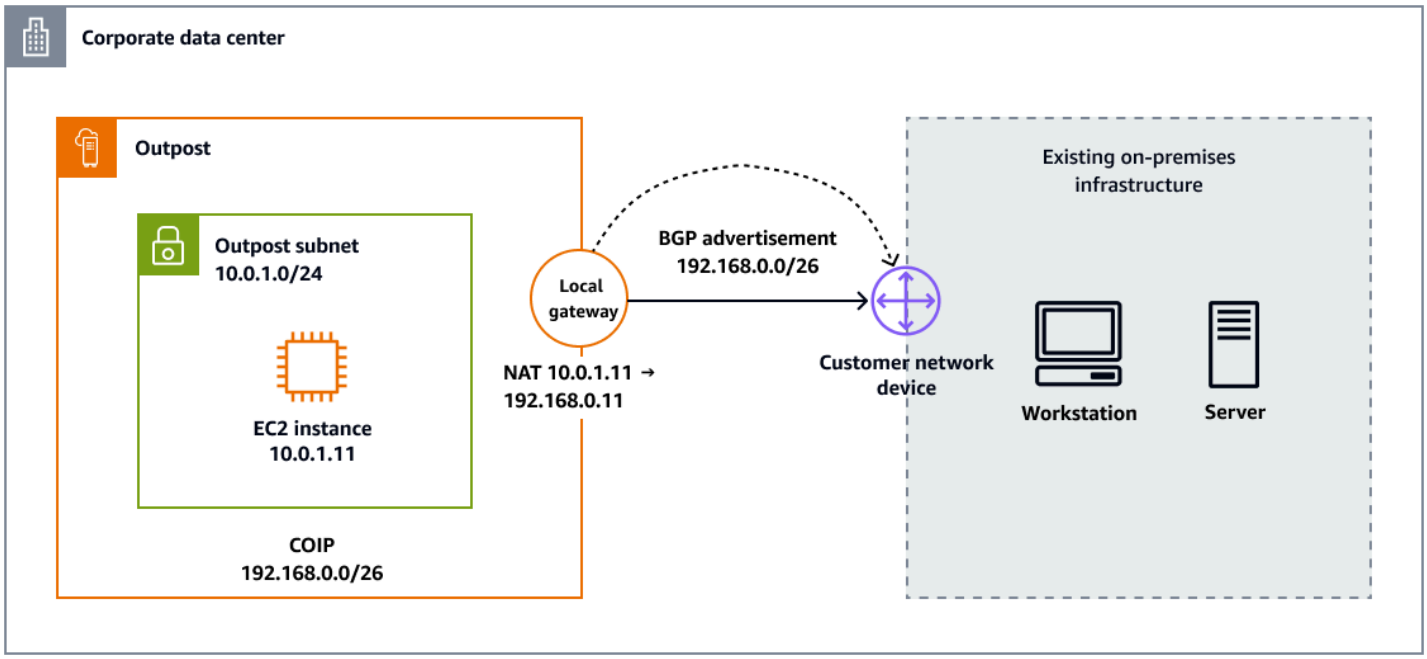
La puerta de enlace local (LGW) es un componente central de la AWS Outposts arquitectura. La puerta de enlace local permite la conectividad entre las subredes Outpost y la red en las instalaciones. La función principal de una LGW es proporcionar conectividad desde un puesto de avanzada a la red local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

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

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



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



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

Zonas Locales e Internet

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

Para exponer a Internet una carga EC2 de trabajo alojada en Amazon en una zona local, puedes habilitar la opción Asignar automáticamente una IP pública al lanzar la EC2 instancia. Si usa un

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

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

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

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

Zonas Locales y AWS Direct Connect

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

Zonas Locales y pasarelas de tránsito

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

Zonas Locales y emparejamiento de VPC

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

Seguridad en la periferia

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

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

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

Protección de los datos

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

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

Cifrado en reposo

Cifrado en volúmenes de EBS

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

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

Cifrado en Amazon S3 en Outposts

De forma predeterminada, todos los datos almacenados en Amazon S3 en Outposts se cifran mediante cifrado del lado del servidor con claves de cifrado administradas de Amazon S3 (SSE-S3). Opcionalmente, puede usar el cifrado del lado del servidor con claves proporcionadas por el cliente (SSE-C). Para utilizar SSE-C, especifique una clave de cifrado como parte de las solicitudes de API de objeto. El cifrado en el servidor solo cifra los datos de objetos, no los metadatos de objetos.

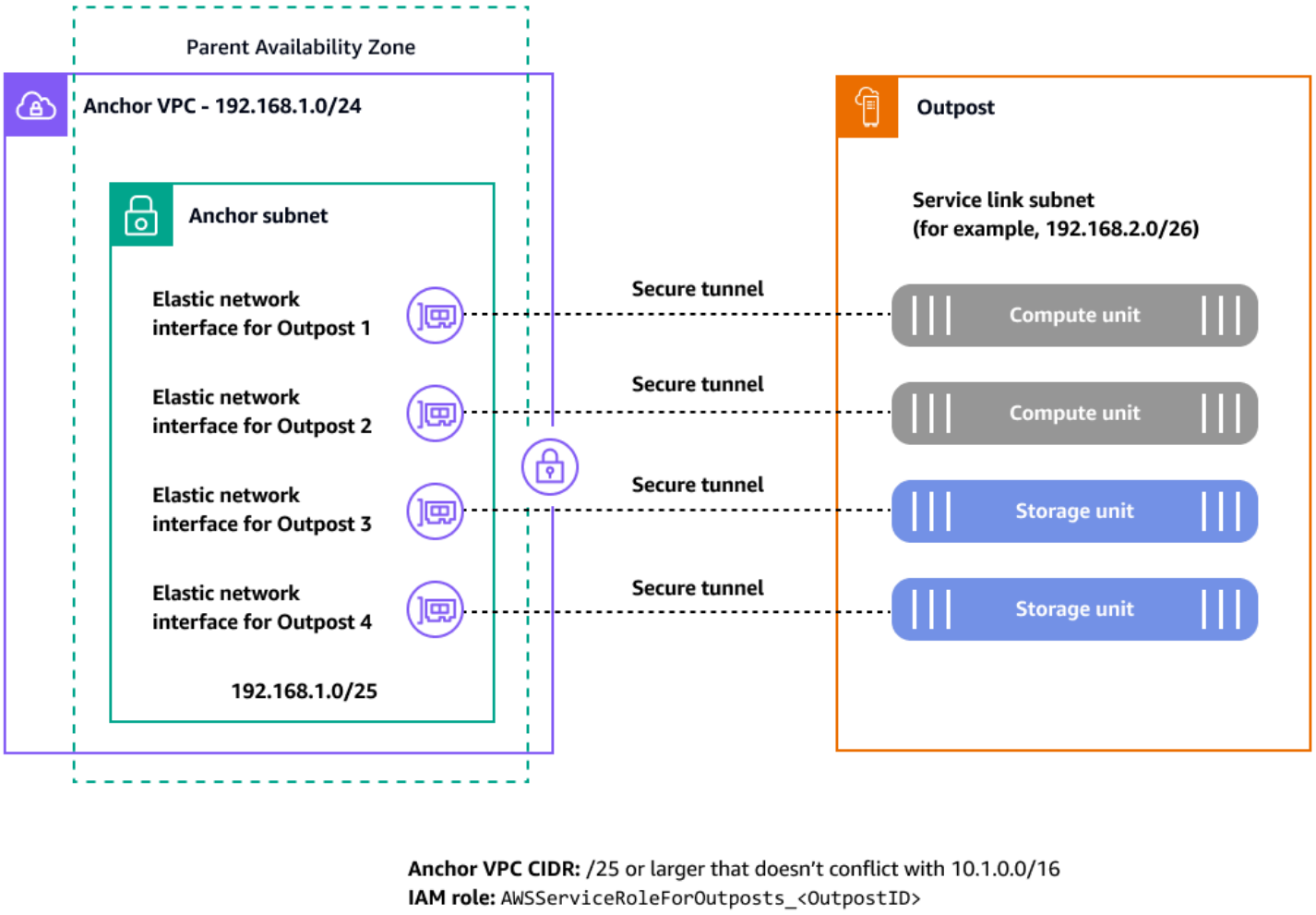
> **Note**
>
> Amazon S3 en Outposts no admite el cifrado del lado del servidor con claves KMS (SSE-KMS).

Cifrado en tránsito

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

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

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



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

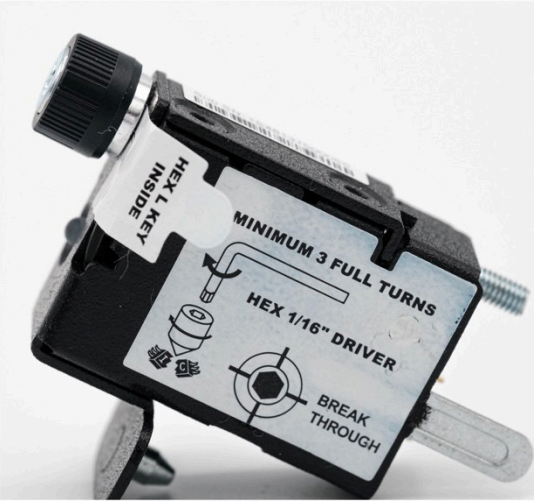
Protocolo	Puerto de origen	Dirección de origen	Puerto de destino	Dirección de destino
UDP	443	AWS Outposts enlace de servicio /26	443	AWS Outposts Rutas públicas de la región o anclaje VPC CIDR
TCP	1025-65535	AWS Outposts enlace de servicio /26	443	AWS Outposts Rutas públicas de la región o anclaje VPC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

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

Eliminación de datos

Al detener o terminar una EC2 instancia en AWS Outposts, el hipervisor limpia la memoria que se le ha asignado (se establece en cero) antes de asignarla a una nueva instancia y se restablecen todos los bloques de almacenamiento. La eliminación de datos del hardware de Outpost implica el uso de hardware especializado. El NSK es un dispositivo pequeño, ilustrado en la siguiente fotografía, que se conecta a la parte frontal de cada unidad de cómputo o almacenamiento de un Outpost. Está diseñado para proporcionar un mecanismo que evite que sus datos queden expuestos desde su centro de datos o sitio de colocación. Los datos del dispositivo Outpost se protegen envolviendo el material de codificación utilizado para cifrar el dispositivo y almacenándolo en el NSK. Cuando

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



Identity and Access Management

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

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

Característica de IAM	AWS Outposts soporte
Políticas basadas en identidades	Sí
Políticas basadas en recursos	Sí*
Acciones de políticas	Sí
Recursos de políticas	Sí
Claves de condición de política (específicas del servicio)	Sí
Listas de control de acceso (ACLs)	No

Característica de IAM	AWS Outposts soporte
Control de acceso basado en atributos (ABAC) (etiquetas en políticas)	Sí
Credenciales temporales	Sí
Permisos de entidades principales	Sí
Roles de servicio	No
Roles vinculados al servicio	Sí

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

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

Seguridad de la infraestructura

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

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

Protección de redes

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

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

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

Proteger los recursos informáticos

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

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

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

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

Acceso a Internet

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

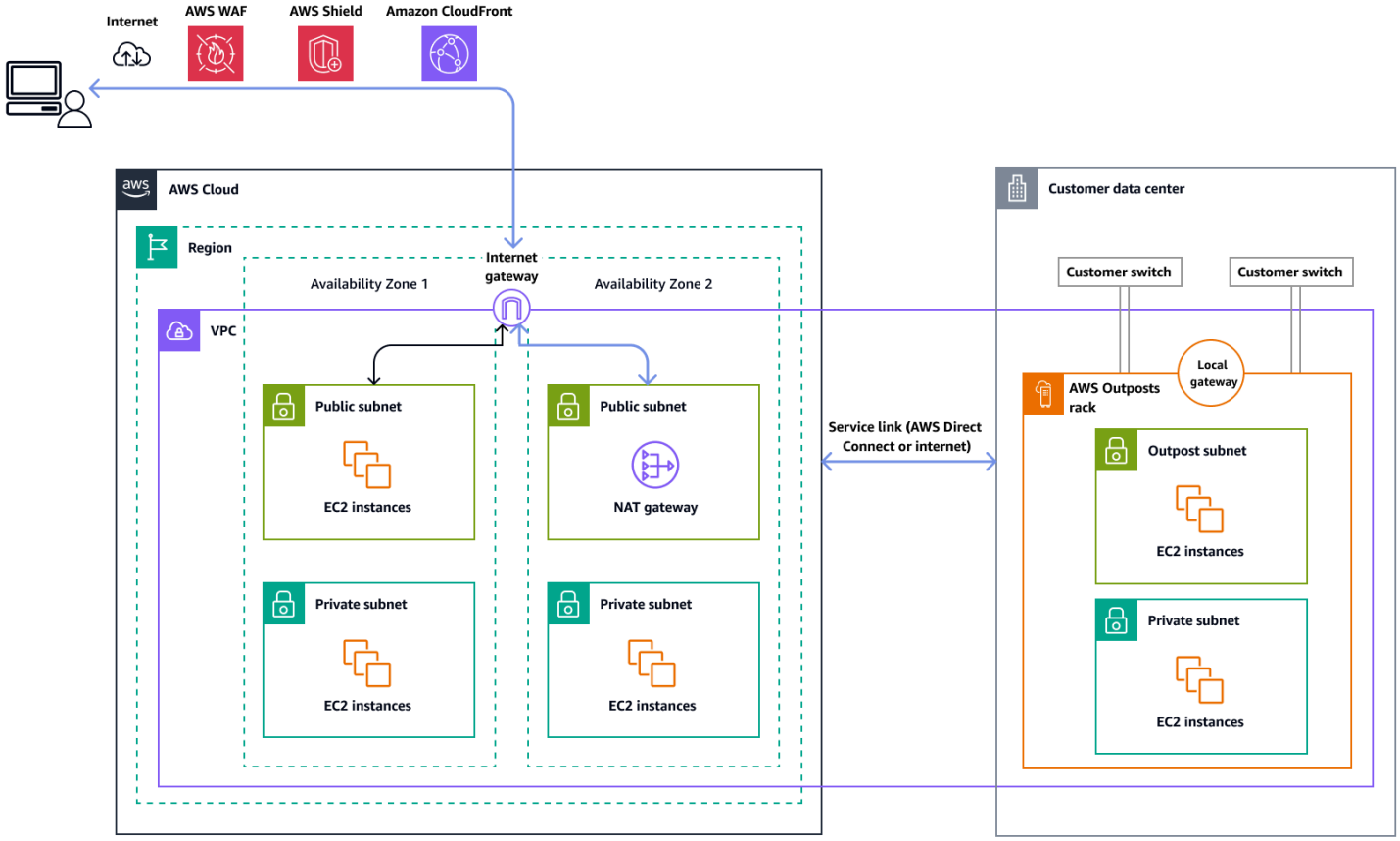
Las Zonas Locales adoptan una construcción de red denominada grupo fronterizo de red, que se utiliza en Regiones de AWS. AWS anuncia las direcciones IP públicas de estos grupos únicos. Un grupo fronterizo de red se compone de Availability Zones, Local Zones o Wavelength Zones. Puede asignar explícitamente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

En AWS Outposts, si desea utilizar la puerta de enlace local (LGW) para conectarse a Internet desde su red, debe modificar la tabla de enrutamiento personalizada asociada a la AWS Outposts subred. La tabla de rutas debe tener una entrada de ruta predeterminada (0.0.0.0/0) que utilice la LGW como siguiente salto. Usted es responsable de implementar el resto de los controles de seguridad en su red local, incluidas las defensas perimetrales, como los firewalls y los sistemas de prevención de intrusiones o los sistemas de detección de intrusiones (IPS/IDS). Esto se alinea con el modelo de responsabilidad compartida, que divide las tareas de seguridad entre usted y el proveedor de la nube.

Acceso a Internet a través del progenitor Región de AWS

En esta opción, las cargas de trabajo del Outpost acceden a Internet a través del enlace de servicio y la pasarela de Internet del servidor principal. Región de AWS El tráfico saliente a Internet se puede enrutar a través de la puerta de enlace NAT que está instanciada en la VPC. Para mayor seguridad para su tráfico de entrada y salida, puede utilizar servicios de AWS seguridad como AWS WAF AWS Shield, y Amazon CloudFront en el. Región de AWS

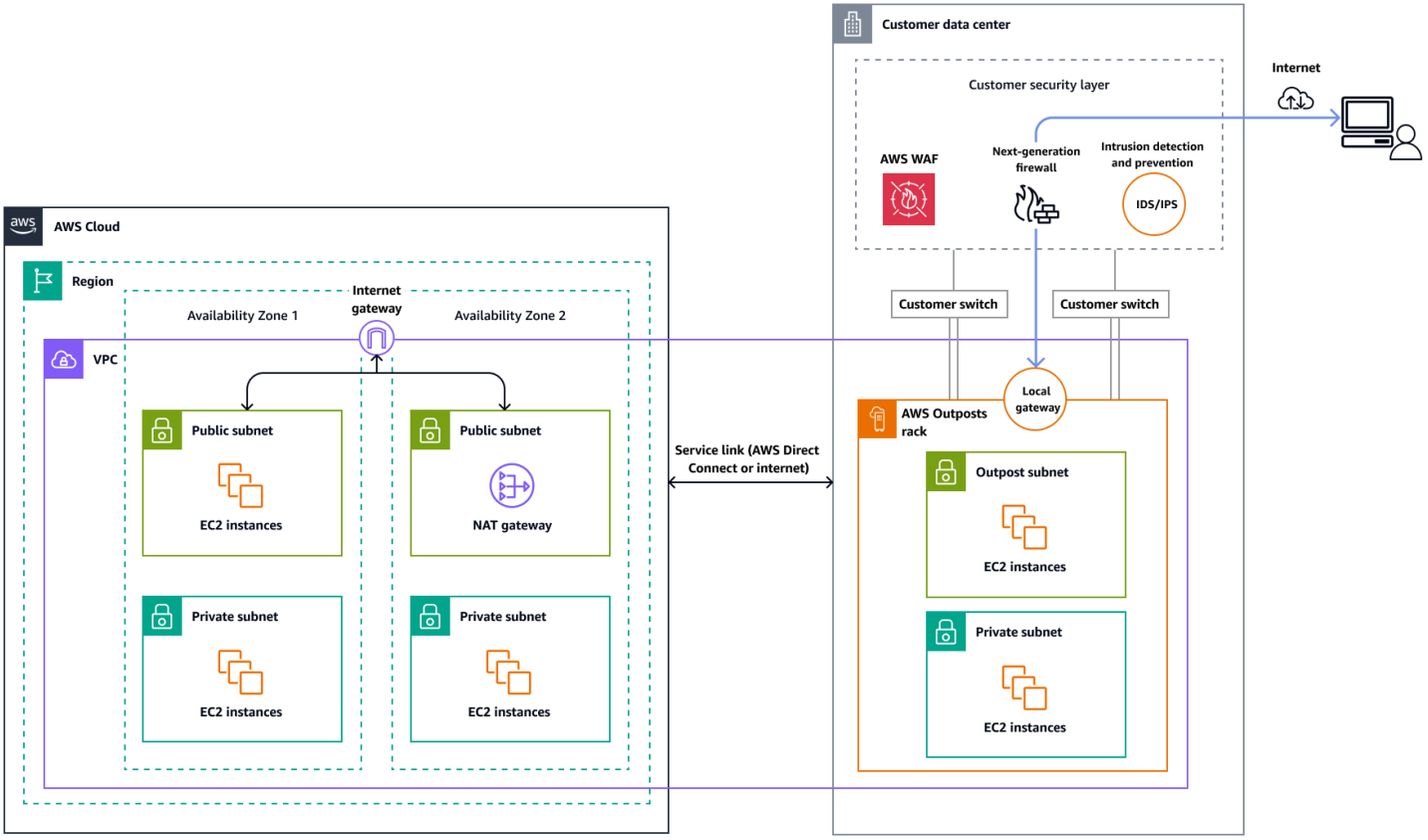
En el siguiente diagrama se muestra el tráfico entre la carga de trabajo de la AWS Outposts instancia e Internet que pasa por la instancia principal. Región de AWS



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

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

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



Gobernanza de la infraestructura

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

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

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

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

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

Compartir los recursos de Outposts

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

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

Los recursos que se pueden compartir son: AWS Outposts

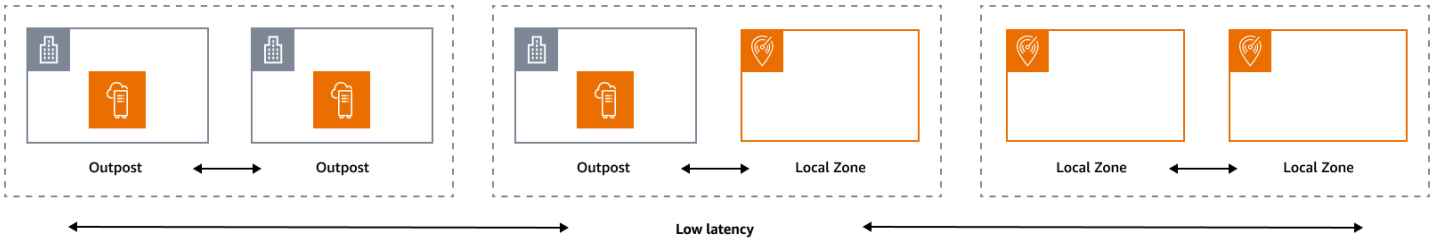
- Anfitriones dedicados asignados
- Reservas de capacidad
- Grupos de direcciones IP (CoIP) propiedad del cliente
- Tabla de enrutamiento de la puerta de enlace local
- Outposts
- Amazon S3 en Outposts
- Sitios
- Subredes

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

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

Resiliencia en la periferia

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



Consideraciones sobre infraestructura

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

Zonas locales

Las zonas locales actúan de manera similar a las zonas de disponibilidad dentro de ellas Región de AWS, ya que se pueden seleccionar como ubicación de ubicación para AWS los recursos zonales, como subredes e EC2 instancias. Sin embargo, no se encuentran en un centro de TI Región de AWS, sino cerca de grandes centros de población, industriales y de TI que actualmente no Región

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

Outposts

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

Zonas de disponibilidad principales

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

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

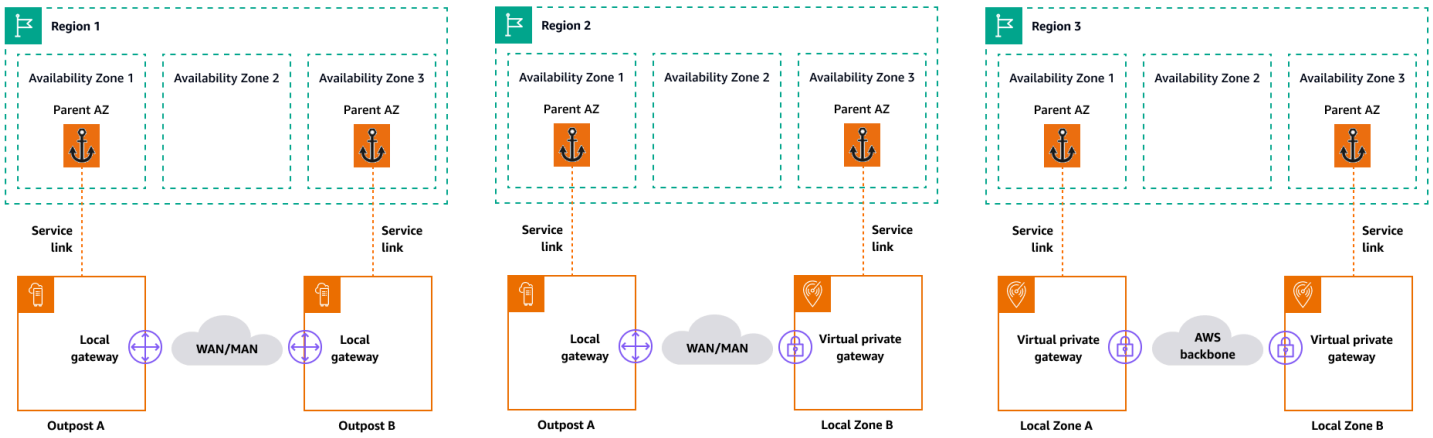
```
aws ec2 describe-availability-zones --zone-ids use1-mia1-az1
```

Resultado del comando anterior:

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


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

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



Consideraciones sobre redes

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

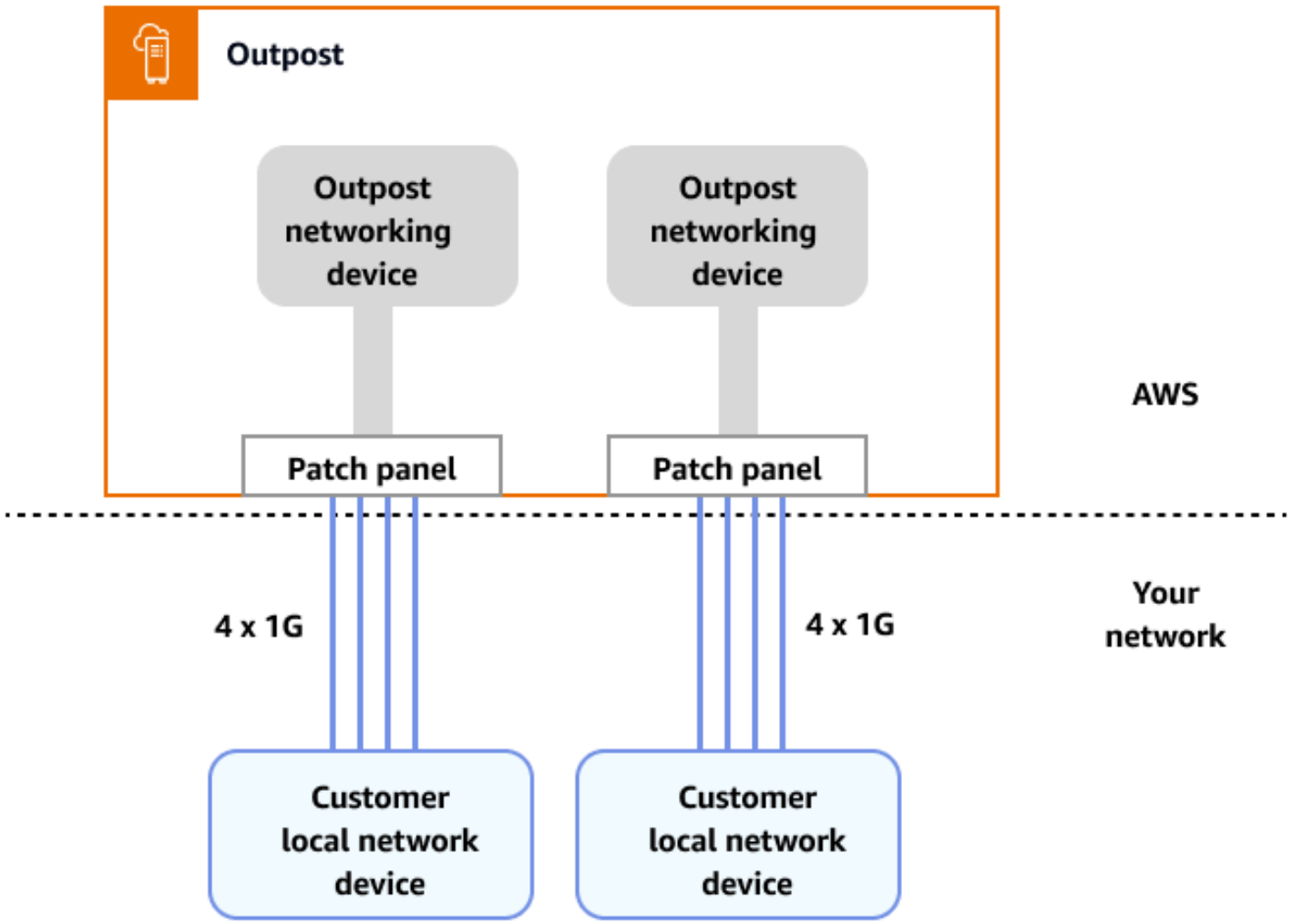
Redes de resiliencia para Zonas Locales

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

Redes de resiliencia para Outposts

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

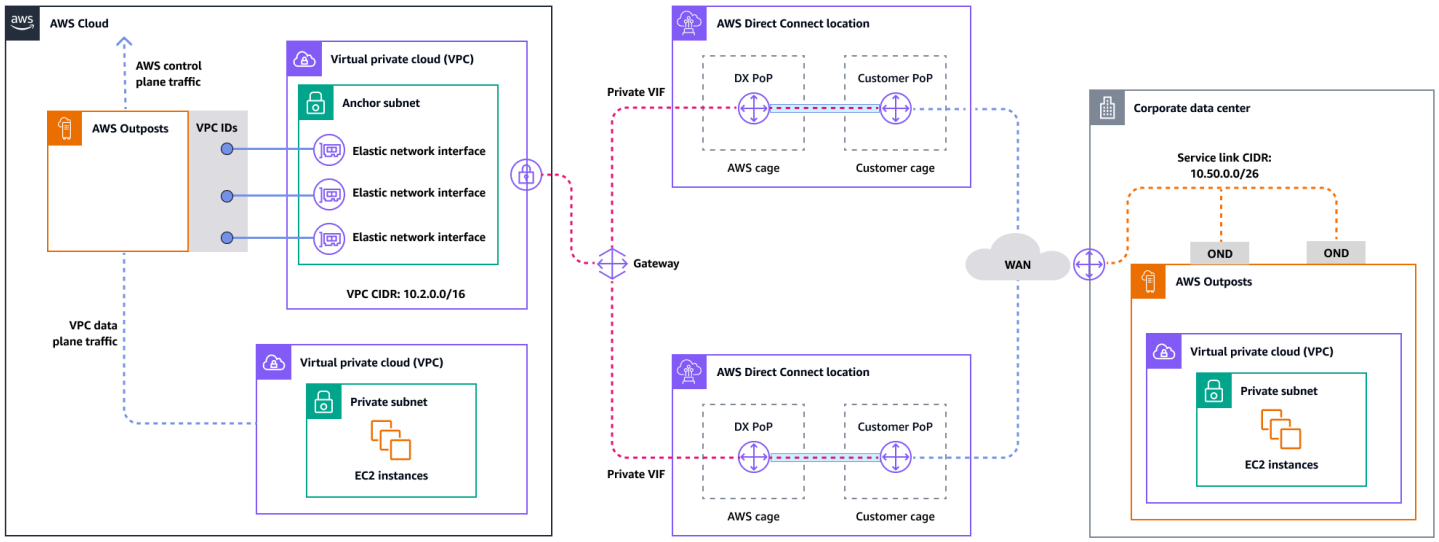
Velocidad de enlace ascendente	Número de enlaces ascendentes
1 Gbps	1, 2, 4, 6 o 8
10 Gbps	1, 2, 4, 8, 12 o 16
40 o 100 Gbps	1, 2 o 4



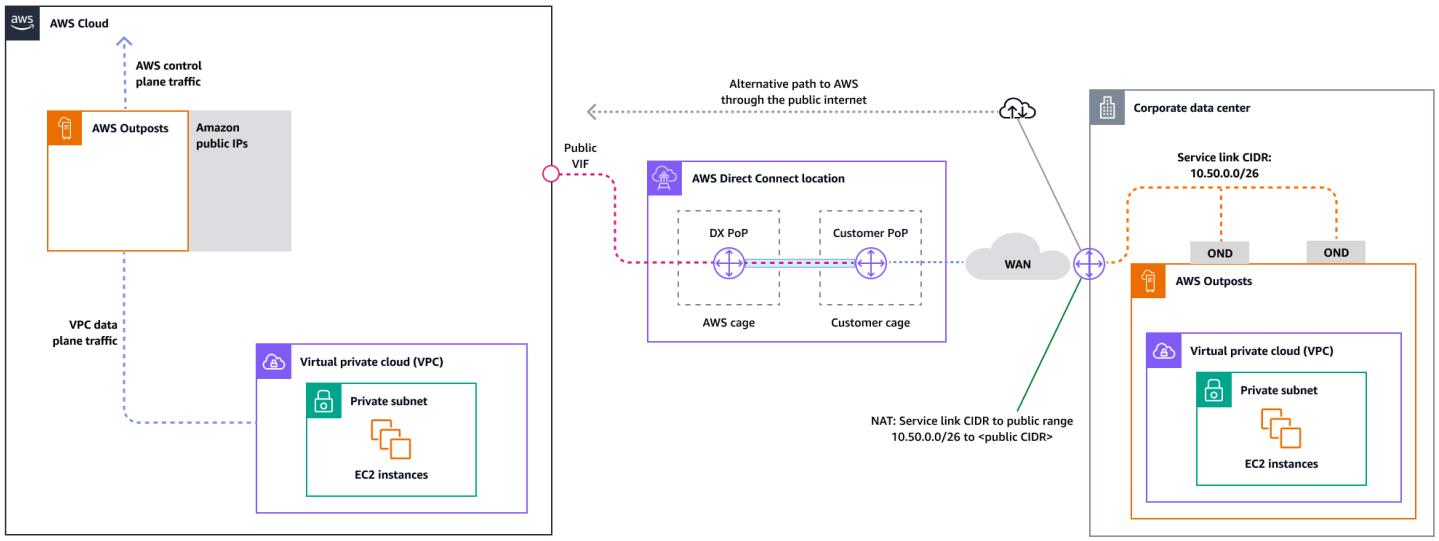
Para obtener más información sobre esta conectividad, consulta Conectividad de red local para Outposts Racks en la documentación. AWS Outposts

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

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



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



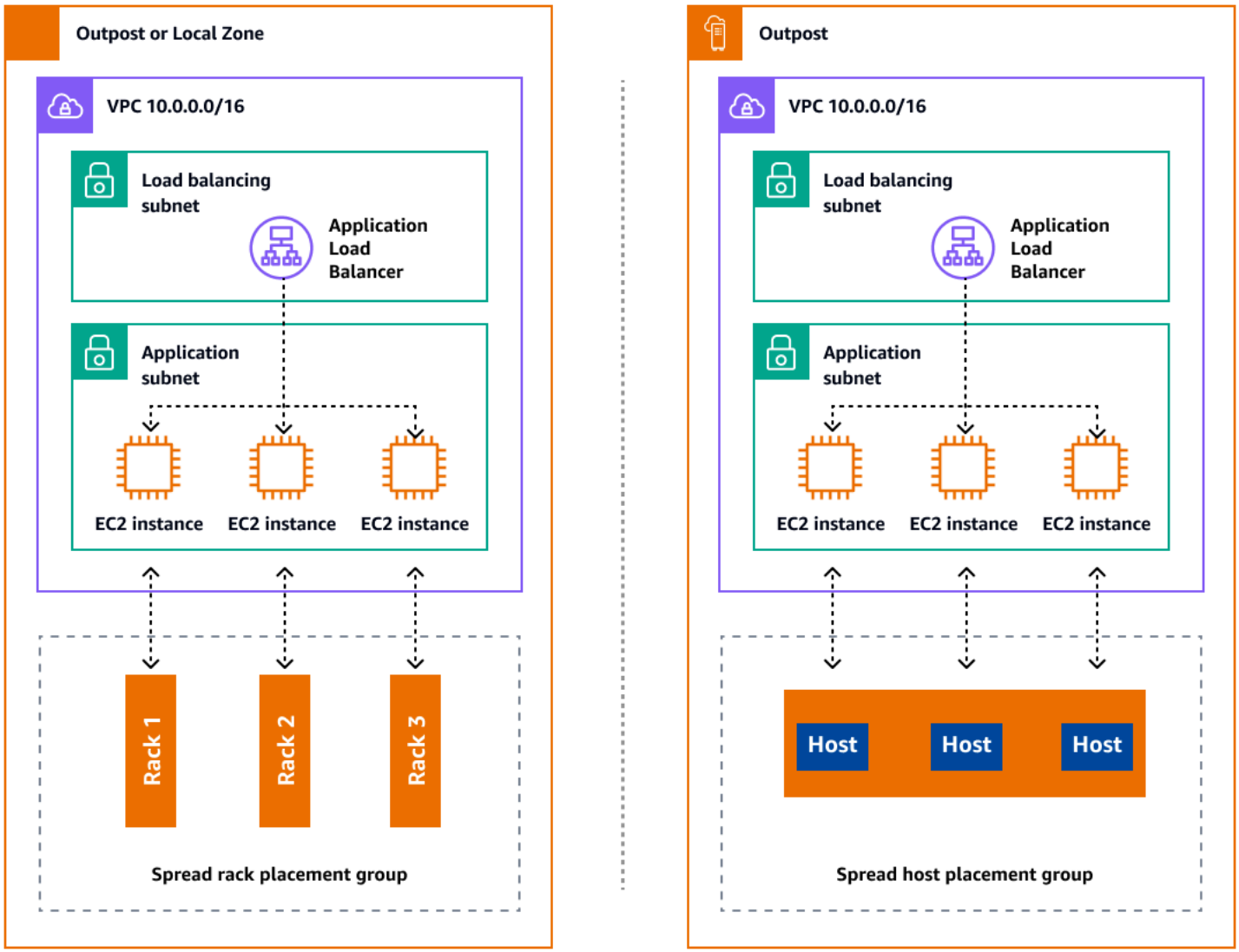
Escalar las implementaciones de racks de Outposts con racks ACE

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

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

Distribución de instancias en Outposts y Zonas Locales

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



Amazon RDS Multi-AZ en AWS Outposts

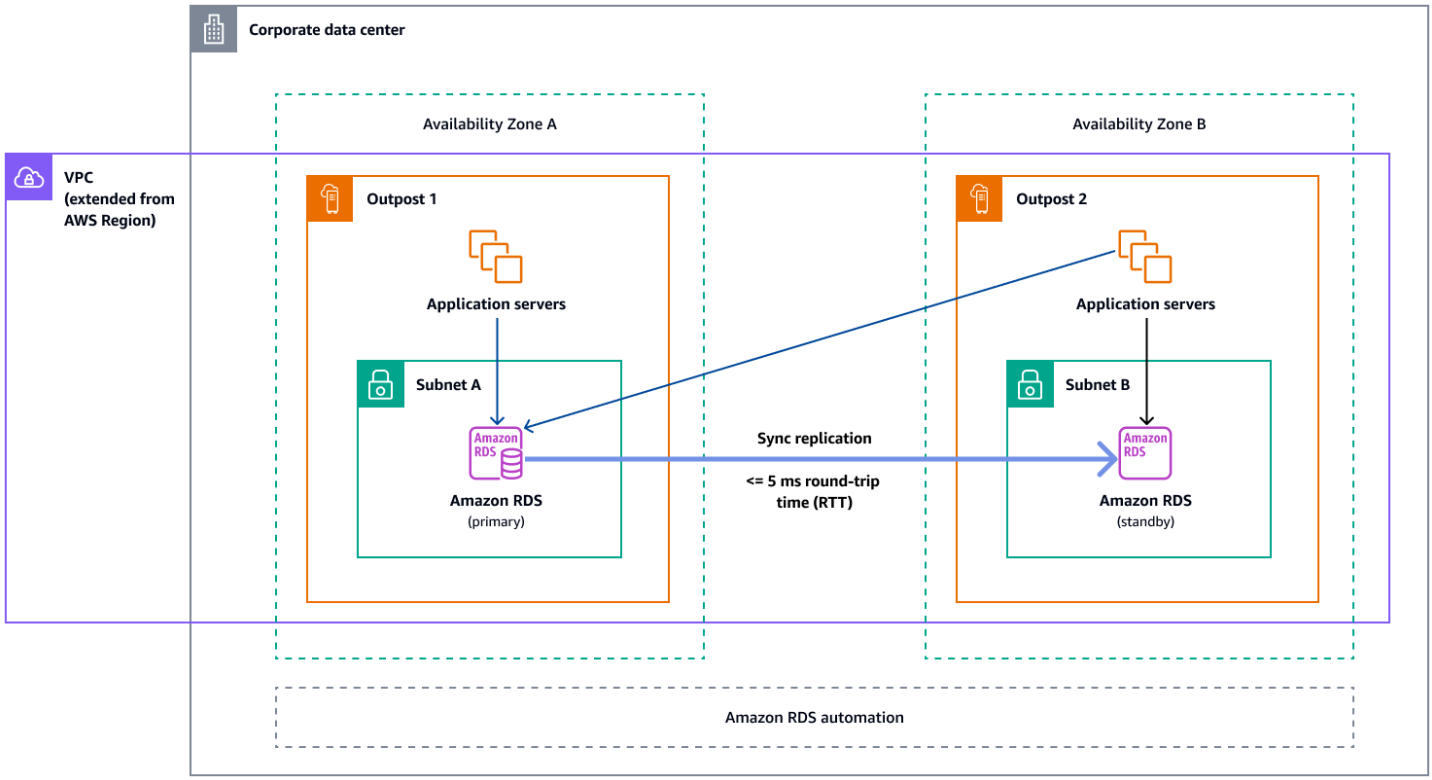
Cuando utiliza despliegues de instancias Multi-AZ en Outposts, Amazon RDS crea dos instancias de base de datos en dos Outposts. Cada Outpost se ejecuta en su propia infraestructura física y se conecta a diferentes zonas de disponibilidad de una región para ofrecer una alta disponibilidad. Cuando dos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

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

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

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

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

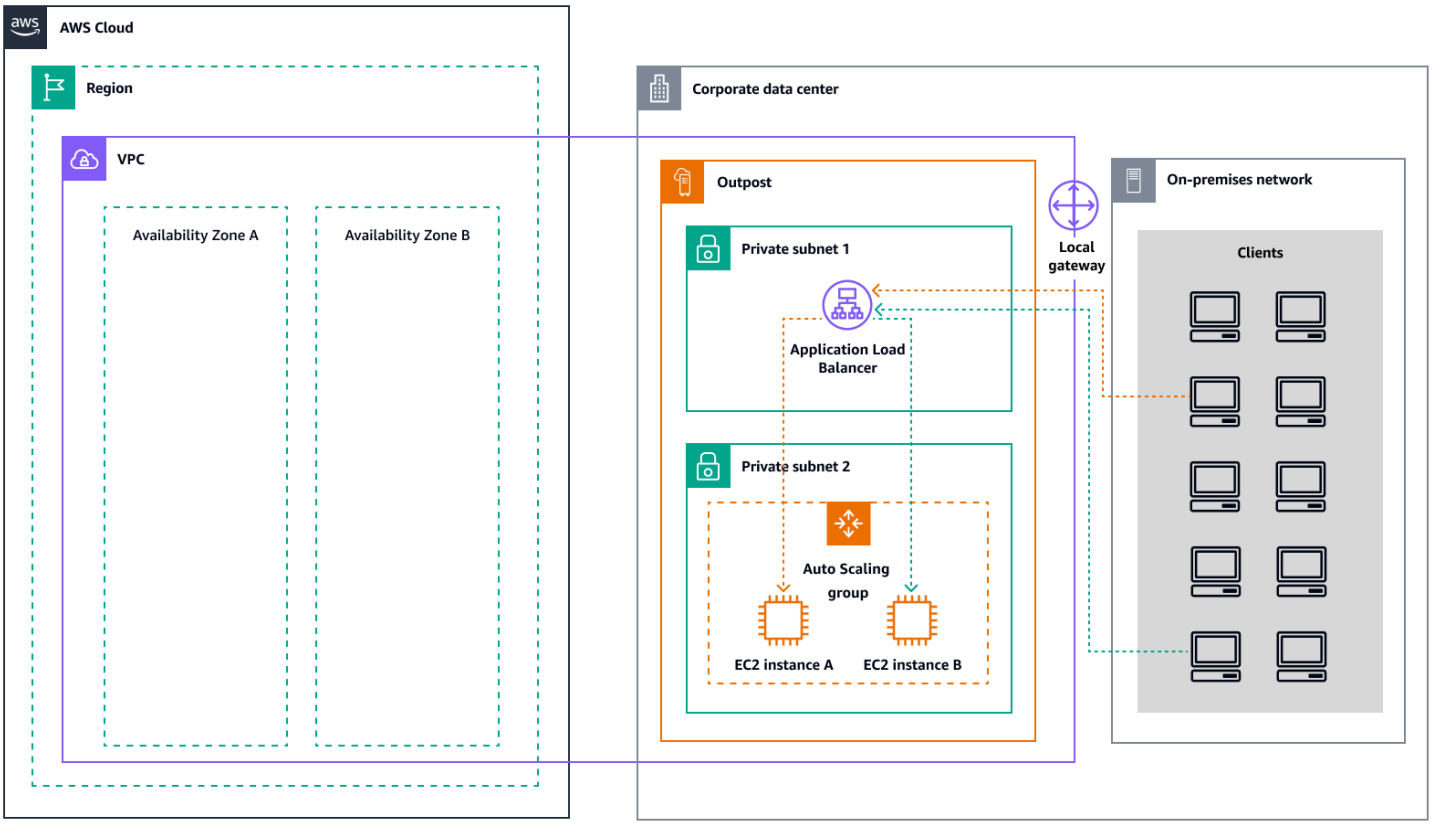


Mecanismos de conmutación por error

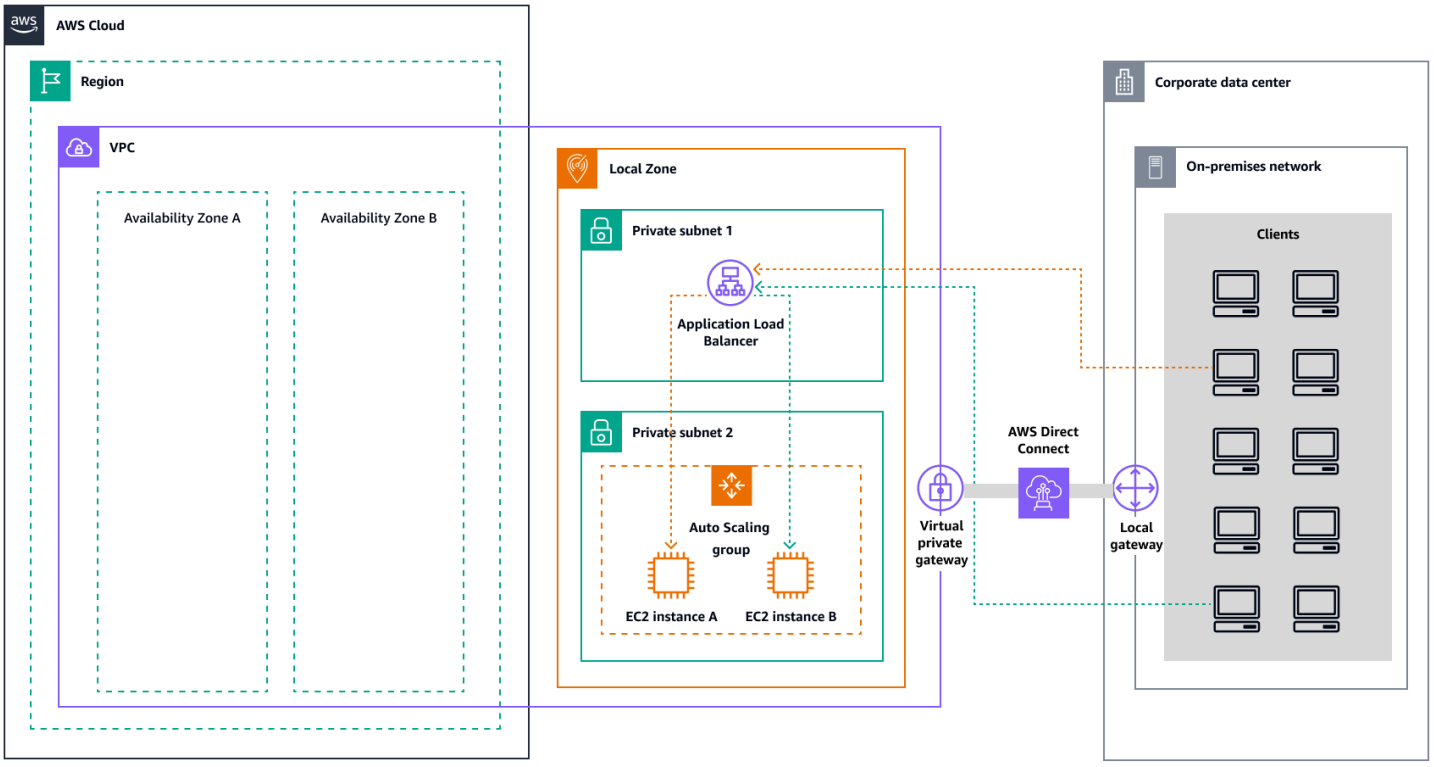
Equilibrio de carga y escalado automático

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

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



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

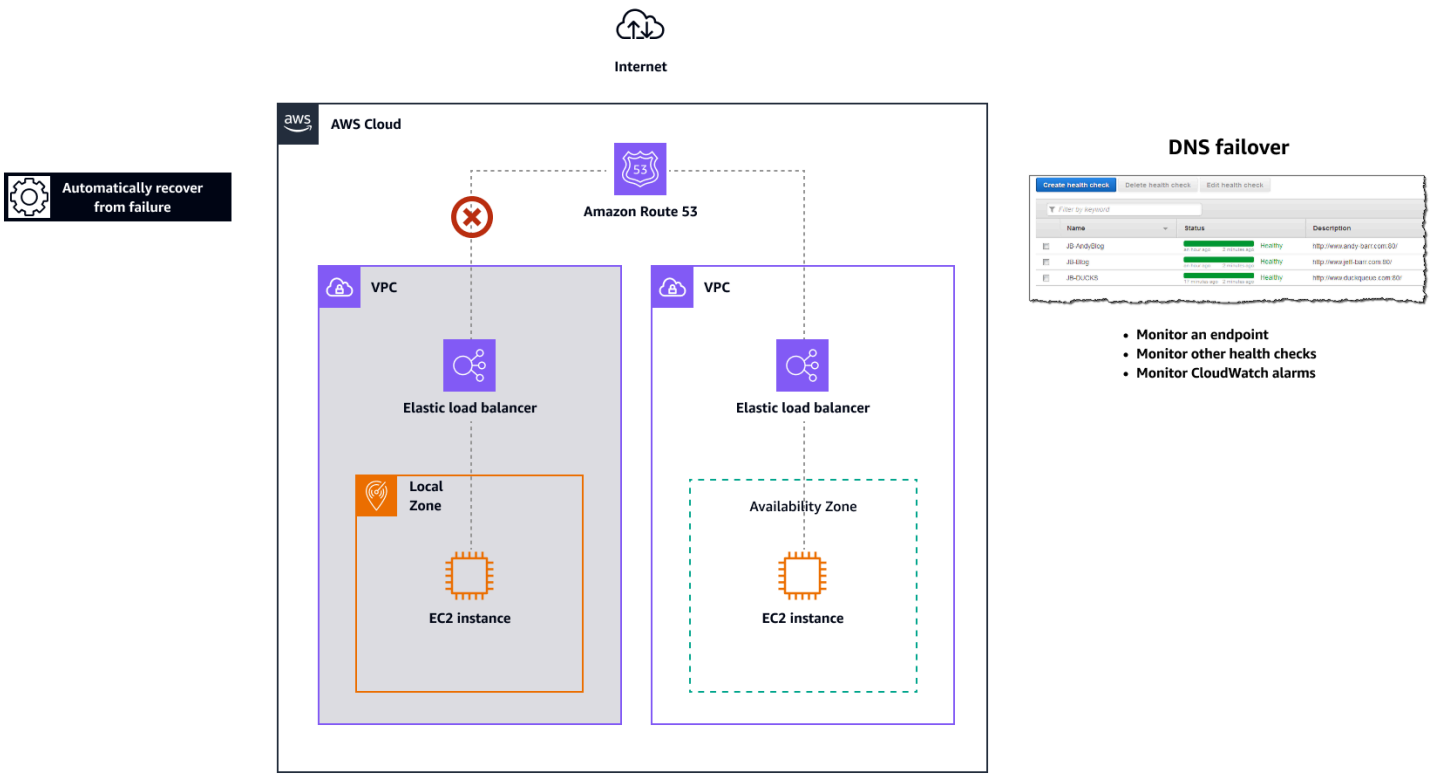


> **Note**
>
> Los balanceadores de carga de aplicaciones están disponibles tanto AWS Outposts en las Zonas Locales como en las Zonas Locales. Sin embargo, para usar un Application Load Balancer AWS Outposts, debes dimensionar la EC2 capacidad de Amazon para proporcionar la escalabilidad que requiere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

Amazon Route 53 para conmutación por error de DNS

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

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



Notas

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

Amazon Route 53 Resolver activado AWS Outposts

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

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

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

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

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

Planificación de la capacidad en la periferia

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

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

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

Planificación de la capacidad en Outposts

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

Planificación de la capacidad para las Zonas Locales

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

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

Resultado previsto:

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

```
  ]
}
```

Administración de infraestructura perimetral

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

Implementación de servicios en la periferia

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

Amazon EC2 al límite

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

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

Equilibradores de carga de aplicaciones en la periferia

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

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

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

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

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

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

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

CLI y SDK específicos para Outposts

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

Proceso de pedido de Outposts

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

Administración de puertas de enlace locales

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

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

CloudWatch métricas y registros

Dado Servicios de AWS que están disponibles tanto en Outposts como en las Zonas Locales, las métricas y los registros se administran de la misma manera que en las Regiones. Amazon CloudWatch proporciona métricas dedicadas a monitorear Outposts en las siguientes dimensiones:

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

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

Recursos

AWS referencias

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

AWS publicaciones de blog

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

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

Colaboradores

Las siguientes personas colaboraron en la elaboración de esta guía.

Creación

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

Revisando

- David Filiatrault, consultor de entregas, AWS

Redacción técnica

- Handan Selamoglu, gerente sénior de documentación, AWS

Historial de documentos

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

Cambio	Descripción	Fecha
Publicación inicial	—	10 de junio de 2025

AWS Glosario de orientación prescriptiva

Los siguientes son términos de uso común en las estrategias, guías y patrones proporcionados por la Guía AWS prescriptiva. Para sugerir entradas, utilice el enlace Enviar comentarios al final del glosario.

Números

Las 7 R

Siete estrategias de migración comunes para trasladar aplicaciones a la nube. Estas estrategias se basan en las 5 R que Gartner identificó en 2011 y consisten en lo siguiente:

- Refactorizar/rediseñar: traslade una aplicación y modifique su arquitectura mediante el máximo aprovechamiento de las características nativas en la nube para mejorar la agilidad, el rendimiento y la escalabilidad. Por lo general, esto implica trasladar el sistema operativo y la base de datos. Ejemplo: migre su base de datos Oracle local a la edición compatible con PostgreSQL de Amazon Aurora.
- Redefinir la plataforma (transportar y redefinir): traslade una aplicación a la nube e introduzca algún nivel de optimización para aprovechar las capacidades de la nube. Ejemplo: migre su base de datos Oracle local a Amazon Relational Database Service (Amazon RDS) para Oracle en el. Nube de AWS
- Recomprar (readquirir): cambie a un producto diferente, lo cual se suele llevar a cabo al pasar de una licencia tradicional a un modelo SaaS. Ejemplo: migre su sistema de gestión de relaciones con los clientes (CRM) a Salesforce.com.
- Volver a alojar (migrar mediante lift-and-shift): traslade una aplicación a la nube sin realizar cambios para aprovechar las capacidades de la nube. Ejemplo: migre su base de datos Oracle local a Oracle en una EC2 instancia del. Nube de AWS
- Reubicar: (migrar el hipervisor mediante lift and shift): traslade la infraestructura a la nube sin comprar equipo nuevo, reescribir aplicaciones o modificar las operaciones actuales. Los servidores se migran de una plataforma local a un servicio en la nube para la misma plataforma. Ejemplo: migrar una Microsoft Hyper-V aplicación a AWS.
- Retener (revisitar): conserve las aplicaciones en el entorno de origen. Estas pueden incluir las aplicaciones que requieren una refactorización importante, que desee posponer para más adelante, y las aplicaciones heredadas que desee retener, ya que no hay ninguna justificación empresarial para migrarlas.

- Retirar: retire o elimine las aplicaciones que ya no sean necesarias en un entorno de origen.

A

ABAC

Consulte control de acceso basado en atributos.

servicios abstractos

Consulte servicios gestionados.

ACID

Consulte atomicidad, consistencia, aislamiento y durabilidad.

migración activa-activa

Método de migración de bases de datos en el que las bases de datos de origen y destino se mantienen sincronizadas (mediante una herramienta de replicación bidireccional o mediante operaciones de escritura doble) y ambas bases de datos gestionan las transacciones de las aplicaciones conectadas durante la migración. Este método permite la migración en lotes pequeños y controlados, en lugar de requerir una transición única. Es más flexible, pero requiere más trabajo que la migración activa-pasiva.

migración activa-pasiva

Método de migración de bases de datos en el que las bases de datos de origen y destino se mantienen sincronizadas, pero solo la base de datos de origen gestiona las transacciones de las aplicaciones conectadas mientras los datos se replican en la base de datos de destino. La base de datos de destino no acepta ninguna transacción durante la migración.

función de agregación

Función SQL que opera en un grupo de filas y calcula un único valor de retorno para el grupo. Entre los ejemplos de funciones agregadas se incluyen `SUM` y `MAX`.

IA

Véase inteligencia artificial.

AIOps

Consulte las operaciones de inteligencia artificial.

anonimización

El proceso de eliminar permanentemente la información personal de un conjunto de datos. La anonimización puede ayudar a proteger la privacidad personal. Los datos anonimizados ya no se consideran datos personales.

antipatrones

Una solución que se utiliza con frecuencia para un problema recurrente en el que la solución es contraproducente, ineficaz o menos eficaz que una alternativa.

control de aplicaciones

Un enfoque de seguridad que permite el uso únicamente de aplicaciones aprobadas para ayudar a proteger un sistema contra el malware.

cartera de aplicaciones

Recopilación de información detallada sobre cada aplicación que utiliza una organización, incluido el costo de creación y mantenimiento de la aplicación y su valor empresarial. Esta información es clave para el proceso de detección y análisis de la cartera y ayuda a identificar y priorizar las aplicaciones que se van a migrar, modernizar y optimizar.

inteligencia artificial (IA)

El campo de la informática que se dedica al uso de tecnologías informáticas para realizar funciones cognitivas que suelen estar asociadas a los seres humanos, como el aprendizaje, la resolución de problemas y el reconocimiento de patrones. Para más información, consulte ¿Qué es la inteligencia artificial?

operaciones de inteligencia artificial (AIOps)

El proceso de utilizar técnicas de machine learning para resolver problemas operativos, reducir los incidentes operativos y la intervención humana, y mejorar la calidad del servicio. Para obtener más información sobre cómo AIOps se utiliza en la estrategia de AWS migración, consulte la guía de integración de operaciones.

cifrado asimétrico

Algoritmo de cifrado que utiliza un par de claves, una clave pública para el cifrado y una clave privada para el descifrado. Puede compartir la clave pública porque no se utiliza para el descifrado, pero el acceso a la clave privada debe estar sumamente restringido.

atomicidad, consistencia, aislamiento, durabilidad (ACID)

Conjunto de propiedades de software que garantizan la validez de los datos y la fiabilidad operativa de una base de datos, incluso en caso de errores, cortes de energía u otros problemas.

control de acceso basado en atributos (ABAC)

La práctica de crear permisos detallados basados en los atributos del usuario, como el departamento, el puesto de trabajo y el nombre del equipo. Para obtener más información, consulte ABAC AWS en la documentación AWS Identity and Access Management (IAM).

origen de datos fidedigno

Ubicación en la que se almacena la versión principal de los datos, que se considera la fuente de información más fiable. Puede copiar los datos del origen de datos autorizado a otras ubicaciones con el fin de procesarlos o modificarlos, por ejemplo, anonimizarlos, redactarlos o seudonimizarlos.

Zona de disponibilidad

Una ubicación distinta dentro de una Región de AWS que está aislada de los fallos en otras zonas de disponibilidad y que proporciona una conectividad de red económica y de baja latencia a otras zonas de disponibilidad de la misma región.

AWS Marco de adopción de la nube (AWS CAF)

Un marco de directrices y mejores prácticas AWS para ayudar a las organizaciones a desarrollar un plan eficiente y eficaz para migrar con éxito a la nube. AWS CAF organiza la orientación en seis áreas de enfoque denominadas perspectivas: negocios, personas, gobierno, plataforma, seguridad y operaciones. Las perspectivas empresariales, humanas y de gobernanza se centran en las habilidades y los procesos empresariales; las perspectivas de plataforma, seguridad y operaciones se centran en las habilidades y los procesos técnicos. Por ejemplo, la perspectiva humana se dirige a las partes interesadas que se ocupan de los Recursos Humanos (RR. HH.), las funciones del personal y la administración de las personas. Desde esta perspectiva, AWS CAF proporciona orientación para el desarrollo, la formación y la comunicación de las personas a fin de preparar a la organización para una adopción exitosa de la nube. Para obtener más información, consulte la Página web de AWS CAF y el Documento técnico de AWS CAF.

AWS Marco de calificación de la carga de trabajo (AWS WQF)

Herramienta que evalúa las cargas de trabajo de migración de bases de datos, recomienda estrategias de migración y proporciona estimaciones de trabajo. AWS WQF se incluye con AWS

Schema Conversion Tool ().AWS SCT Analiza los esquemas de bases de datos y los objetos de código, el código de las aplicaciones, las dependencias y las características de rendimiento y proporciona informes de evaluación.

B

Un bot malo

Un bot destinado a interrumpir o causar daño a personas u organizaciones.

BCP

Consulte la planificación de la continuidad del negocio.

gráfico de comportamiento

Una vista unificada e interactiva del comportamiento de los recursos y de las interacciones a lo largo del tiempo. Puede utilizar un gráfico de comportamiento con Amazon Detective para examinar los intentos de inicio de sesión fallidos, las llamadas sospechosas a la API y acciones similares. Para obtener más información, consulte Datos en un gráfico de comportamiento en la documentación de Detective.

sistema big-endian

Un sistema que almacena primero el byte más significativo. Véase también endianness.

clasificación binaria

Un proceso que predice un resultado binario (una de las dos clases posibles). Por ejemplo, es posible que su modelo de ML necesite predecir problemas como “¿Este correo electrónico es spam o no es spam?” o “¿Este producto es un libro o un automóvil?”.

filtro de floración

Estructura de datos probabilística y eficiente en términos de memoria que se utiliza para comprobar si un elemento es miembro de un conjunto.

implementación azul/verde

Una estrategia de despliegue en la que se crean dos entornos separados pero idénticos. La versión actual de la aplicación se ejecuta en un entorno (azul) y la nueva versión de la aplicación en el otro entorno (verde). Esta estrategia le ayuda a revertirla rápidamente con un impacto mínimo.

bot

Una aplicación de software que ejecuta tareas automatizadas a través de Internet y simula la actividad o interacción humana. Algunos bots son útiles o beneficiosos, como los rastreadores web que indexan información en Internet. Algunos otros bots, conocidos como bots malos, tienen como objetivo interrumpir o causar daños a personas u organizaciones.

botnet

Redes de bots que están infectadas por malware y que están bajo el control de una sola parte, conocida como pastor u operador de bots. Las botnets son el mecanismo más conocido para escalar los bots y su impacto.

branch

Área contenida de un repositorio de código. La primera rama que se crea en un repositorio es la rama principal. Puede crear una rama nueva a partir de una rama existente y, a continuación, desarrollar características o corregir errores en la rama nueva. Una rama que se genera para crear una característica se denomina comúnmente rama de característica. Cuando la característica se encuentra lista para su lanzamiento, se vuelve a combinar la rama de característica con la rama principal. Para obtener más información, consulte Acerca de las sucursales (GitHub documentación).

acceso con cristales rotos

En circunstancias excepcionales y mediante un proceso aprobado, un usuario puede acceder rápidamente a un sitio para el Cuenta de AWS que normalmente no tiene permisos de acceso. Para obtener más información, consulte el indicador Implemente procedimientos de rotura de cristales en la guía Well-Architected AWS .

estrategia de implementación sobre infraestructura existente

La infraestructura existente en su entorno. Al adoptar una estrategia de implementación sobre infraestructura existente para una arquitectura de sistemas, se diseña la arquitectura en función de las limitaciones de los sistemas y la infraestructura actuales. Si está ampliando la infraestructura existente, puede combinar las estrategias de implementación sobre infraestructuras existentes y de implementación desde cero.

caché de búfer

El área de memoria donde se almacenan los datos a los que se accede con más frecuencia.

capacidad empresarial

Lo que hace una empresa para generar valor (por ejemplo, ventas, servicio al cliente o marketing). Las arquitecturas de microservicios y las decisiones de desarrollo pueden estar impulsadas por las capacidades empresariales. Para obtener más información, consulte la sección Organizado en torno a las capacidades empresariales del documento técnico Ejecutar microservicios en contenedores en AWS.

planificación de la continuidad del negocio (BCP)

Plan que aborda el posible impacto de un evento disruptivo, como una migración a gran escala en las operaciones y permite a la empresa reanudar las operaciones rápidamente.

C

CAF

Consulte el marco AWS de adopción de la nube.

despliegue canario

El lanzamiento lento e incremental de una versión para los usuarios finales. Cuando se tiene confianza, se despliega la nueva versión y se reemplaza la versión actual en su totalidad.

CCoE

Consulte Cloud Center of Excellence.

CDC

Consulte la captura de datos de cambios.

captura de datos de cambio (CDC)

Proceso de seguimiento de los cambios en un origen de datos, como una tabla de base de datos, y registro de los metadatos relacionados con el cambio. Puede utilizar los CDC para diversos fines, como auditar o replicar los cambios en un sistema de destino para mantener la sincronización.

ingeniería del caos

Introducir intencionalmente fallos o eventos disruptivos para poner a prueba la resiliencia de un sistema. Puedes usar AWS Fault Injection Service (AWS FIS) para realizar experimentos que estresen tus AWS cargas de trabajo y evalúen su respuesta.

CI/CD

Consulte la integración continua y la entrega continua.

clasificación

Un proceso de categorización que permite generar predicciones. Los modelos de ML para problemas de clasificación predicen un valor discreto. Los valores discretos siempre son distintos entre sí. Por ejemplo, es posible que un modelo necesite evaluar si hay o no un automóvil en una imagen.

cifrado del cliente

Cifrado de datos localmente, antes de que el objetivo los Servicio de AWS reciba.

Centro de excelencia en la nube (CCoE)

Equipo multidisciplinario que impulsa los esfuerzos de adopción de la nube en toda la organización, incluido el desarrollo de las prácticas recomendadas en la nube, la movilización de recursos, el establecimiento de plazos de migración y la dirección de la organización durante las transformaciones a gran escala. Para obtener más información, consulte las publicaciones de CCo E en el blog de estrategia Nube de AWS empresarial.

computación en la nube

La tecnología en la nube que se utiliza normalmente para la administración de dispositivos de IoT y el almacenamiento de datos de forma remota. La computación en la nube suele estar conectada a la tecnología de computación perimetral.

modelo operativo en la nube

En una organización de TI, el modelo operativo que se utiliza para crear, madurar y optimizar uno o más entornos de nube. Para obtener más información, consulte Creación de su modelo operativo de nube.

etapas de adopción de la nube

Las cuatro fases por las que suelen pasar las organizaciones cuando migran a Nube de AWS:

- Proyecto: ejecución de algunos proyectos relacionados con la nube con fines de prueba de concepto y aprendizaje
- Fundamento: realizar inversiones fundamentales para escalar su adopción de la nube (p. ej., crear una landing zone, definir una CCo E, establecer un modelo de operaciones)

- Migración: migración de aplicaciones individuales
- Reinvención: optimización de productos y servicios e innovación en la nube

Stephen Orban definió estas etapas en la entrada del blog The Journey Toward Cloud-First & the Stages of Adoption en el blog Nube de AWS Enterprise Strategy. Para obtener información sobre su relación con la estrategia de AWS migración, consulte la guía de preparación para la migración.

CMDB

Consulte la base de datos de administración de la configuración.

repositorio de código

Una ubicación donde el código fuente y otros activos, como documentación, muestras y scripts, se almacenan y actualizan mediante procesos de control de versiones. Los repositorios en la nube más comunes incluyen GitHub oBitbucket Cloud. Cada versión del código se denomina rama. En una estructura de microservicios, cada repositorio se encuentra dedicado a una única funcionalidad. Una sola canalización de CI/CD puede utilizar varios repositorios.

caché en frío

Una caché de búfer que está vacía no está bien poblada o contiene datos obsoletos o irrelevantes. Esto afecta al rendimiento, ya que la instancia de la base de datos debe leer desde la memoria principal o el disco, lo que es más lento que leer desde la memoria caché del búfer.

datos fríos

Datos a los que se accede con poca frecuencia y que suelen ser históricos. Al consultar este tipo de datos, normalmente se aceptan consultas lentas. Trasladar estos datos a niveles o clases de almacenamiento de menor rendimiento y menos costosos puede reducir los costos.

visión artificial (CV)

Campo de la IA que utiliza el aprendizaje automático para analizar y extraer información de formatos visuales, como imágenes y vídeos digitales. Por ejemplo, Amazon SageMaker AI proporciona algoritmos de procesamiento de imágenes para CV.

desviación de configuración

En el caso de una carga de trabajo, un cambio de configuración con respecto al estado esperado. Puede provocar que la carga de trabajo deje de cumplir las normas y, por lo general, es gradual e involuntario.

base de datos de administración de configuración (CMDB)

Repositorio que almacena y administra información sobre una base de datos y su entorno de TI, incluidos los componentes de hardware y software y sus configuraciones. Por lo general, los datos de una CMDB se utilizan en la etapa de detección y análisis de la cartera de productos durante la migración.

paquete de conformidad

Conjunto de AWS Config reglas y medidas correctivas que puede reunir para personalizar sus comprobaciones de conformidad y seguridad. Puede implementar un paquete de conformidad como una entidad única en una región Cuenta de AWS y, o en una organización, mediante una plantilla YAML. Para obtener más información, consulta los paquetes de conformidad en la documentación. AWS Config

integración y entrega continuas (CI/CD)

El proceso de automatización de las etapas de origen, compilación, prueba, puesta en escena y producción del proceso de publicación del software. CI/CD se describe comúnmente como una canalización. CI/CD puede ayudarlo a automatizar los procesos, mejorar la productividad, mejorar la calidad del código y entregar más rápido. Para obtener más información, consulte Beneficios de la entrega continua. CD también puede significar implementación continua. Para obtener más información, consulte Entrega continua frente a implementación continua.

CV

Vea la visión artificial.

D

datos en reposo

Datos que están estacionarios en la red, como los datos que se encuentran almacenados.

clasificación de datos

Un proceso para identificar y clasificar los datos de su red en función de su importancia y sensibilidad. Es un componente fundamental de cualquier estrategia de administración de riesgos de ciberseguridad porque lo ayuda a determinar los controles de protección y retención adecuados para los datos. La clasificación de datos es un componente del pilar de seguridad

del AWS Well-Architected Framework. Para obtener más información, consulte Clasificación de datos.

desviación de datos

Una variación significativa entre los datos de producción y los datos que se utilizaron para entrenar un modelo de machine learning, o un cambio significativo en los datos de entrada a lo largo del tiempo. La desviación de los datos puede reducir la calidad, la precisión y la imparcialidad generales de las predicciones de los modelos de machine learning.

datos en tránsito

Datos que se mueven de forma activa por la red, por ejemplo, entre los recursos de la red.

malla de datos

Un marco arquitectónico que proporciona una propiedad de datos distribuida y descentralizada con una administración y un gobierno centralizados.

minimización de datos

El principio de recopilar y procesar solo los datos estrictamente necesarios. Practicar la minimización de los datos Nube de AWS puede reducir los riesgos de privacidad, los costos y la huella de carbono de la analítica.

perímetro de datos

Un conjunto de barreras preventivas en su AWS entorno que ayudan a garantizar que solo las identidades confiables accedan a los recursos confiables desde las redes esperadas. Para obtener más información, consulte Crear un perímetro de datos sobre. AWS

preprocesamiento de datos

Transformar los datos sin procesar en un formato que su modelo de ML pueda analizar fácilmente. El preprocesamiento de datos puede implicar eliminar determinadas columnas o filas y corregir los valores faltantes, incoherentes o duplicados.

procedencia de los datos

El proceso de rastrear el origen y el historial de los datos a lo largo de su ciclo de vida, por ejemplo, la forma en que se generaron, transmitieron y almacenaron los datos.

titular de los datos

Persona cuyos datos se recopilan y procesan.

almacenamiento de datos

Un sistema de administración de datos que respalde la inteligencia empresarial, como el análisis. Los almacenes de datos suelen contener grandes cantidades de datos históricos y, por lo general, se utilizan para consultas y análisis.

lenguaje de definición de datos (DDL)

Instrucciones o comandos para crear o modificar la estructura de tablas y objetos de una base de datos.

lenguaje de manipulación de datos (DML)

Instrucciones o comandos para modificar (insertar, actualizar y eliminar) la información de una base de datos.

DDL

Consulte el lenguaje de definición de bases de datos.

conjunto profundo

Combinar varios modelos de aprendizaje profundo para la predicción. Puede utilizar conjuntos profundos para obtener una predicción más precisa o para estimar la incertidumbre de las predicciones.

aprendizaje profundo

Un subcampo del ML que utiliza múltiples capas de redes neuronales artificiales para identificar el mapeo entre los datos de entrada y las variables objetivo de interés.

defense-in-depth

Un enfoque de seguridad de la información en el que se distribuyen cuidadosamente una serie de mecanismos y controles de seguridad en una red informática para proteger la confidencialidad, la integridad y la disponibilidad de la red y de los datos que contiene. Al adoptar esta estrategia AWS, se añaden varios controles en diferentes capas de la AWS Organizations estructura para ayudar a proteger los recursos. Por ejemplo, un defense-in-depth enfoque podría combinar la autenticación multifactorial, la segmentación de la red y el cifrado.

administrador delegado

En AWS Organizations, un servicio compatible puede registrar una cuenta de AWS miembro para administrar las cuentas de la organización y gestionar los permisos de ese servicio. Esta

cuenta se denomina administrador delegado para ese servicio. Para obtener más información y una lista de servicios compatibles, consulte Servicios que funcionan con AWS Organizations en la documentación de AWS Organizations .

Implementación

El proceso de hacer que una aplicación, características nuevas o correcciones de código se encuentren disponibles en el entorno de destino. La implementación abarca implementar cambios en una base de código y, a continuación, crear y ejecutar esa base en los entornos de la aplicación.

entorno de desarrollo

Consulte entorno.

control de detección

Un control de seguridad que se ha diseñado para detectar, registrar y alertar después de que se produzca un evento. Estos controles son una segunda línea de defensa, ya que lo advierten sobre los eventos de seguridad que han eludido los controles preventivos establecidos. Para obtener más información, consulte Controles de detección en Implementación de controles de seguridad en AWS.

asignación de flujos de valor para el desarrollo (DVSM)

Proceso que se utiliza para identificar y priorizar las restricciones que afectan negativamente a la velocidad y la calidad en el ciclo de vida del desarrollo de software. DVSM amplía el proceso de asignación del flujo de valor diseñado originalmente para las prácticas de fabricación ajustada. Se centra en los pasos y los equipos necesarios para crear y transferir valor a través del proceso de desarrollo de software.

gemelo digital

Representación virtual de un sistema del mundo real, como un edificio, una fábrica, un equipo industrial o una línea de producción. Los gemelos digitales son compatibles con el mantenimiento predictivo, la supervisión remota y la optimización de la producción.

tabla de dimensiones

En un esquema en estrella, tabla más pequeña que contiene los atributos de datos sobre los datos cuantitativos de una tabla de hechos. Los atributos de la tabla de dimensiones suelen ser campos de texto o números discretos que se comportan como texto. Estos atributos se utilizan habitualmente para restringir consultas, filtrar y etiquetar conjuntos de resultados.

desastre

Un evento que impide que una carga de trabajo o un sistema cumplan sus objetivos empresariales en su ubicación principal de implementación. Estos eventos pueden ser desastres naturales, fallos técnicos o el resultado de acciones humanas, como una configuración incorrecta involuntaria o un ataque de malware.

recuperación de desastres (DR)

La estrategia y el proceso que se utilizan para minimizar el tiempo de inactividad y la pérdida de datos ocasionados por un desastre. Para obtener más información, consulte Recuperación ante desastres de cargas de trabajo en AWS: Recovery in the Cloud in the AWS Well-Architected Framework.

DML

Consulte el lenguaje de manipulación de bases de datos.

diseño basado en el dominio

Un enfoque para desarrollar un sistema de software complejo mediante la conexión de sus componentes a dominios en evolución, o a los objetivos empresariales principales, a los que sirve cada componente. Este concepto lo introdujo Eric Evans en su libro, Diseño impulsado por el dominio: abordando la complejidad en el corazón del software (Boston: Addison-Wesley Professional, 2003). Para obtener información sobre cómo utilizar el diseño basado en dominios con el patrón de higos estranguladores, consulte Modernización gradual de los servicios web antiguos de Microsoft ASP.NET (ASMX) mediante contenedores y Amazon API Gateway.

DR

Consulte recuperación ante desastres.

detección de desviaciones

Seguimiento de las desviaciones con respecto a una configuración de referencia. Por ejemplo, puedes usarlo AWS CloudFormation para detectar desviaciones en los recursos del sistema o puedes usarlo AWS Control Tower para detectar cambios en tu landing zone que puedan afectar al cumplimiento de los requisitos de gobierno.

DVSM

Consulte el mapeo del flujo de valor del desarrollo.

E

EDA

Consulte el análisis exploratorio de datos.

EDI

Véase intercambio electrónico de datos.

computación en la periferia

La tecnología que aumenta la potencia de cálculo de los dispositivos inteligentes en la periferia de una red de IoT. En comparación con la computación en nube, la computación perimetral puede reducir la latencia de la comunicación y mejorar el tiempo de respuesta.

intercambio electrónico de datos (EDI)

El intercambio automatizado de documentos comerciales entre organizaciones. Para obtener más información, consulte Qué es el intercambio electrónico de datos.

cifrado

Proceso informático que transforma datos de texto plano, legibles por humanos, en texto cifrado.

clave de cifrado

Cadena criptográfica de bits aleatorios que se genera mediante un algoritmo de cifrado. Las claves pueden variar en longitud y cada una se ha diseñado para ser impredecible y única.

endianidad

El orden en el que se almacenan los bytes en la memoria del ordenador. Los sistemas big-endianos almacenan primero el byte más significativo. Los sistemas Little-Endian almacenan primero el byte menos significativo.

punto de conexión

Consulte el punto final del servicio.

servicio de punto de conexión

Servicio que puede alojar en una nube privada virtual (VPC) para compartir con otros usuarios. Puede crear un servicio de punto final AWS PrivateLink y conceder permisos a otros directores

Cuentas de AWS o a AWS Identity and Access Management (IAM). Estas cuentas o entidades principales pueden conectarse a su servicio de punto de conexión de forma privada mediante la creación de puntos de conexión de VPC de interfaz. Para obtener más información, consulte Creación de un servicio de punto de conexión en la documentación de Amazon Virtual Private Cloud (Amazon VPC).

planificación de recursos empresariales (ERP)

Un sistema que automatiza y gestiona los procesos empresariales clave (como la contabilidad, el MES y la gestión de proyectos) de una empresa.

cifrado de sobre

El proceso de cifrar una clave de cifrado con otra clave de cifrado. Para obtener más información, consulte el cifrado de sobres en la documentación de AWS Key Management Service (AWS KMS).

entorno

Una instancia de una aplicación en ejecución. Los siguientes son los tipos de entornos más comunes en la computación en la nube:

- entorno de desarrollo: instancia de una aplicación en ejecución que solo se encuentra disponible para el equipo principal responsable del mantenimiento de la aplicación. Los entornos de desarrollo se utilizan para probar los cambios antes de promocionarlos a los entornos superiores. Este tipo de entorno a veces se denomina entorno de prueba.
- entornos inferiores: todos los entornos de desarrollo de una aplicación, como los que se utilizan para las compilaciones y pruebas iniciales.
- entorno de producción: instancia de una aplicación en ejecución a la que pueden acceder los usuarios finales. En un CI/CD proceso, el entorno de producción es el último entorno de implementación.
- entornos superiores: todos los entornos a los que pueden acceder usuarios que no sean del equipo de desarrollo principal. Esto puede incluir un entorno de producción, entornos de preproducción y entornos para las pruebas de aceptación por parte de los usuarios.

epopeya

En las metodologías ágiles, son categorías funcionales que ayudan a organizar y priorizar el trabajo. Las epopeyas brindan una descripción detallada de los requisitos y las tareas de implementación. Por ejemplo, las epopeyas AWS de seguridad de CAF incluyen la gestión de identidades y accesos, los controles de detección, la seguridad de la infraestructura, la protección

de datos y la respuesta a incidentes. Para obtener más información sobre las epopeyas en la estrategia de migración de AWS , consulte la Guía de implementación del programa.

PERP

Consulte planificación de recursos empresariales.

análisis de datos de tipo exploratorio (EDA)

El proceso de analizar un conjunto de datos para comprender sus características principales. Se recopilan o agregan datos y, a continuación, se realizan las investigaciones iniciales para encontrar patrones, detectar anomalías y comprobar las suposiciones. El EDA se realiza mediante el cálculo de estadísticas resumidas y la creación de visualizaciones de datos.

F

tabla de datos

La tabla central de un esquema en forma de estrella. Almacena datos cuantitativos sobre las operaciones comerciales. Normalmente, una tabla de hechos contiene dos tipos de columnas: las que contienen medidas y las que contienen una clave externa para una tabla de dimensiones.

fallan rápidamente

Una filosofía que utiliza pruebas frecuentes e incrementales para reducir el ciclo de vida del desarrollo. Es una parte fundamental de un enfoque ágil.

límite de aislamiento de fallas

En el Nube de AWS, un límite, como una zona de disponibilidad Región de AWS, un plano de control o un plano de datos, que limita el efecto de una falla y ayuda a mejorar la resiliencia de las cargas de trabajo. Para obtener más información, consulte Límites de AWS aislamiento de errores.

rama de característica

Consulte la sucursal.

características

Los datos de entrada que se utilizan para hacer una predicción. Por ejemplo, en un contexto de fabricación, las características pueden ser imágenes que se capturan periódicamente desde la línea de fabricación.

importancia de las características

La importancia que tiene una característica para las predicciones de un modelo. Por lo general, esto se expresa como una puntuación numérica que se puede calcular mediante diversas técnicas, como las explicaciones aditivas de Shapley (SHAP) y los gradientes integrados. Para obtener más información, consulte Interpretabilidad del modelo de aprendizaje automático con AWS.

transformación de funciones

Optimizar los datos para el proceso de ML, lo que incluye enriquecer los datos con fuentes adicionales, escalar los valores o extraer varios conjuntos de información de un solo campo de datos. Esto permite que el modelo de ML se beneficie de los datos. Por ejemplo, si divide la fecha del “27 de mayo de 2021 00:15:37” en “jueves”, “mayo”, “2021” y “15”, puede ayudar al algoritmo de aprendizaje a aprender patrones matizados asociados a los diferentes componentes de los datos.

indicaciones de unos pocos pasos

Proporcionar a un LLM un pequeño número de ejemplos que demuestren la tarea y el resultado deseado antes de pedirle que realice una tarea similar. Esta técnica es una aplicación del aprendizaje contextual, en el que los modelos aprenden a partir de ejemplos (planos) integrados en las instrucciones. Las indicaciones con pocas tomas pueden ser eficaces para tareas que requieren un formato, un razonamiento o un conocimiento del dominio específicos. Consulte también el apartado de mensajes sin intervención.

FGAC

Consulte el control de acceso detallado.

control de acceso preciso (FGAC)

El uso de varias condiciones que tienen por objetivo permitir o denegar una solicitud de acceso.

migración relámpago

Método de migración de bases de datos que utiliza la replicación continua de datos mediante la captura de datos modificados para migrar los datos en el menor tiempo posible, en lugar de utilizar un enfoque gradual. El objetivo es reducir al mínimo el tiempo de inactividad.

FM

Consulte el modelo básico.

modelo de base (FM)

Una gran red neuronal de aprendizaje profundo que se ha estado entrenando con conjuntos de datos masivos de datos generalizados y sin etiquetar. FMs son capaces de realizar una amplia variedad de tareas generales, como comprender el lenguaje, generar texto e imágenes y conversar en lenguaje natural. Para obtener más información, consulte Qué son los modelos básicos.

G

IA generativa

Un subconjunto de modelos de IA que se han entrenado con grandes cantidades de datos y que pueden utilizar un simple mensaje de texto para crear contenido y artefactos nuevos, como imágenes, vídeos, texto y audio. Para obtener más información, consulte Qué es la IA generativa.

bloqueo geográfico

Consulta las restricciones geográficas.

restricciones geográficas (bloqueo geográfico)

En Amazon CloudFront, una opción para impedir que los usuarios de países específicos accedan a las distribuciones de contenido. Puede utilizar una lista de permitidos o bloqueados para especificar los países aprobados y prohibidos. Para obtener más información, consulta la sección Restringir la distribución geográfica del contenido en la CloudFront documentación.

Flujo de trabajo de Gitflow

Un enfoque en el que los entornos inferiores y superiores utilizan diferentes ramas en un repositorio de código fuente. El flujo de trabajo de Gitflow se considera heredado, y el flujo de trabajo basado en enlaces troncales es el enfoque moderno preferido.

imagen dorada

Instantánea de un sistema o software que se utiliza como plantilla para implementar nuevas instancias de ese sistema o software. Por ejemplo, en la fabricación, una imagen dorada se puede utilizar para aprovisionar software en varios dispositivos y ayuda a mejorar la velocidad, la escalabilidad y la productividad de las operaciones de fabricación de dispositivos.

estrategia de implementación desde cero

La ausencia de infraestructura existente en un entorno nuevo. Al adoptar una estrategia de implementación desde cero para una arquitectura de sistemas, puede seleccionar todas las tecnologías nuevas sin que estas deban ser compatibles con una infraestructura existente, lo que también se conoce como implementación sobre infraestructura existente. Si está ampliando la infraestructura existente, puede combinar las estrategias de implementación sobre infraestructuras existentes y de implementación desde cero.

barrera de protección

Una regla de alto nivel que ayuda a regular los recursos, las políticas y el cumplimiento en todas las unidades organizativas (OUs). Las barreras de protección preventivas aplican políticas para garantizar la alineación con los estándares de conformidad. Se implementan mediante políticas de control de servicios y límites de permisos de IAM. Las barreras de protección de detección detectan las vulneraciones de las políticas y los problemas de conformidad, y generan alertas para su corrección. Se implementan mediante Amazon AWS Config AWS Security Hub GuardDuty AWS Trusted Advisor, Amazon Inspector y AWS Lambda cheques personalizados.

H

HA

Consulte la alta disponibilidad.

migración heterogénea de bases de datos

Migración de la base de datos de origen a una base de datos de destino que utilice un motor de base de datos diferente (por ejemplo, de Oracle a Amazon Aurora). La migración heterogénea suele ser parte de un esfuerzo de rediseño de la arquitectura y convertir el esquema puede ser una tarea compleja. AWS ofrece AWS SCT, lo cual ayuda con las conversiones de esquemas.

alta disponibilidad (HA)

La capacidad de una carga de trabajo para funcionar de forma continua, sin intervención, en caso de desafíos o desastres. Los sistemas de alta disponibilidad están diseñados para realizar una conmutación por error automática, ofrecer un rendimiento de alta calidad de forma constante y gestionar diferentes cargas y fallos con un impacto mínimo en el rendimiento.

modernización histórica

Un enfoque utilizado para modernizar y actualizar los sistemas de tecnología operativa (TO) a fin de satisfacer mejor las necesidades de la industria manufacturera. Un histórico es un tipo de base de datos que se utiliza para recopilar y almacenar datos de diversas fuentes en una fábrica.

datos retenidos

Parte de los datos históricos etiquetados que se ocultan de un conjunto de datos que se utiliza para entrenar un modelo de aprendizaje automático. Puede utilizar los datos de reserva para evaluar el rendimiento del modelo comparando las predicciones del modelo con los datos de reserva.

migración homogénea de bases de datos

Migración de la base de datos de origen a una base de datos de destino que comparte el mismo motor de base de datos (por ejemplo, Microsoft SQL Server a Amazon RDS para SQL Server). La migración homogénea suele formar parte de un esfuerzo para volver a alojar o redefinir la plataforma. Puede utilizar las utilidades de bases de datos nativas para migrar el esquema.

datos recientes

Datos a los que se accede con frecuencia, como datos en tiempo real o datos traslacionales recientes. Por lo general, estos datos requieren un nivel o una clase de almacenamiento de alto rendimiento para proporcionar respuestas rápidas a las consultas.

hotfix

Una solución urgente para un problema crítico en un entorno de producción. Debido a su urgencia, las revisiones suelen realizarse fuera del flujo de trabajo habitual de las versiones. DevOps

periodo de hiperatención

Periodo, inmediatamente después de la transición, durante el cual un equipo de migración administra y monitorea las aplicaciones migradas en la nube para solucionar cualquier problema. Por lo general, este periodo dura de 1 a 4 días. Al final del periodo de hiperatención, el equipo de migración suele transferir la responsabilidad de las aplicaciones al equipo de operaciones en la nube.

I

IaC

Vea la infraestructura como código.

políticas basadas en identidades

Política asociada a uno o más directores de IAM que define sus permisos en el Nube de AWS entorno.

aplicación inactiva

Aplicación que utiliza un promedio de CPU y memoria de entre 5 y 20 por ciento durante un periodo de 90 días. En un proyecto de migración, es habitual retirar estas aplicaciones o mantenerlas en las instalaciones.

IIoT

Consulte Internet de las cosas industrial.

infraestructura inmutable

Un modelo que implementa una nueva infraestructura para las cargas de trabajo de producción en lugar de actualizar, parchear o modificar la infraestructura existente. Las infraestructuras inmutables son intrínsecamente más consistentes, fiables y predecibles que las infraestructuras mutables. Para obtener más información, consulte las prácticas recomendadas para implementar con una infraestructura inmutable en Well-Architected Framework AWS .

VPC entrante (de entrada)

En una arquitectura de AWS cuentas múltiples, una VPC que acepta, inspecciona y enruta las conexiones de red desde fuera de una aplicación. La arquitectura AWS de referencia de seguridad recomienda configurar la cuenta de red con entradas, salidas e inspección VPCs para proteger la interfaz bidireccional entre la aplicación y el resto de Internet.

migración gradual

Estrategia de transición en la que se migra la aplicación en partes pequeñas en lugar de realizar una transición única y completa. Por ejemplo, puede trasladar inicialmente solo unos pocos microservicios o usuarios al nuevo sistema. Tras comprobar que todo funciona correctamente, puede trasladar microservicios o usuarios adicionales de forma gradual hasta que pueda retirar su sistema heredado. Esta estrategia reduce los riesgos asociados a las grandes migraciones.

Industria 4.0

Un término que Klaus Schwab introdujo en 2016 para referirse a la modernización de los procesos de fabricación mediante avances en la conectividad, los datos en tiempo real, la automatización, el análisis y la inteligencia artificial/aprendizaje automático.

infraestructura

Todos los recursos y activos que se encuentran en el entorno de una aplicación.

infraestructura como código (IaC)

Proceso de aprovisionamiento y administración de la infraestructura de una aplicación mediante un conjunto de archivos de configuración. La IaC se ha diseñado para ayudarlo a centralizar la administración de la infraestructura, estandarizar los recursos y escalar con rapidez a fin de que los entornos nuevos sean repetibles, fiables y consistentes.

Internet de las cosas industrial (T) IIo

El uso de sensores y dispositivos conectados a Internet en los sectores industriales, como el productivo, el eléctrico, el automotriz, el sanitario, el de las ciencias de la vida y el de la agricultura. Para obtener más información, consulte Creación de una estrategia de transformación digital de la Internet de las cosas (IIoT) industrial.

VPC de inspección

En una arquitectura de AWS cuentas múltiples, una VPC centralizada que gestiona las inspecciones del tráfico de red VPCs entre Internet y las redes locales (en una misma o Regiones de AWS diferente). La arquitectura AWS de referencia de seguridad recomienda configurar su cuenta de red con entrada, salida e inspección VPCs para proteger la interfaz bidireccional entre la aplicación e Internet en general.

Internet de las cosas (IoT)

Red de objetos físicos conectados con sensores o procesadores integrados que se comunican con otros dispositivos y sistemas a través de Internet o de una red de comunicación local. Para obtener más información, consulte ¿Qué es IoT?.

interpretabilidad

Característica de un modelo de machine learning que describe el grado en que un ser humano puede entender cómo las predicciones del modelo dependen de sus entradas. Para obtener más información, consulte Interpretabilidad del modelo de aprendizaje automático con. AWS

IoT

Consulte Internet de las cosas.

biblioteca de información de TI (ITIL)

Conjunto de prácticas recomendadas para ofrecer servicios de TI y alinearlos con los requisitos empresariales. La ITIL proporciona la base para la ITSM.

administración de servicios de TI (ITSM)

Actividades asociadas con el diseño, la implementación, la administración y el soporte de los servicios de TI para una organización. Para obtener información sobre la integración de las operaciones en la nube con las herramientas de ITSM, consulte la Guía de integración de operaciones.

ITIL

Consulte la biblioteca de información de TI.

ITSM

Consulte Administración de servicios de TI.

L

control de acceso basado en etiquetas (LBAC)

Una implementación del control de acceso obligatorio (MAC) en la que a los usuarios y a los propios datos se les asigna explícitamente un valor de etiqueta de seguridad. La intersección entre la etiqueta de seguridad del usuario y la etiqueta de seguridad de los datos determina qué filas y columnas puede ver el usuario.

zona de aterrizaje

Una landing zone es un AWS entorno multicuenta bien diseñado, escalable y seguro. Este es un punto de partida desde el cual las empresas pueden lanzar e implementar rápidamente cargas de trabajo y aplicaciones con confianza en su entorno de seguridad e infraestructura. Para obtener más información sobre las zonas de aterrizaje, consulte Configuración de un entorno de AWS seguro y escalable con varias cuentas.

modelo de lenguaje grande (LLM)

Un modelo de IA de aprendizaje profundo que se entrena previamente con una gran cantidad de datos. Un LLM puede realizar múltiples tareas, como responder preguntas, resumir documentos, traducir textos a otros idiomas y completar oraciones. Para obtener más información, consulte Qué son. LLMs

migración grande

Migración de 300 servidores o más.

LBAC

Consulte el control de acceso basado en etiquetas.

privilegio mínimo

La práctica recomendada de seguridad que consiste en conceder los permisos mínimos necesarios para realizar una tarea. Para obtener más información, consulte Aplicar permisos de privilegio mínimo en la documentación de IAM.

migrar mediante lift-and-shift

Ver 7 Rs.

sistema little-endian

Un sistema que almacena primero el byte menos significativo. Véase también endianness.

LLM

Véase un modelo de lenguaje amplio.

entornos inferiores

Véase entorno.

M

machine learning (ML)

Un tipo de inteligencia artificial que utiliza algoritmos y técnicas para el reconocimiento y el aprendizaje de patrones. El ML analiza y aprende de los datos registrados, como los datos del

Internet de las cosas (IoT), para generar un modelo estadístico basado en patrones. Para más información, consulte Machine learning.

rama principal

Ver sucursal.

malware

Software diseñado para comprometer la seguridad o la privacidad de la computadora. El malware puede interrumpir los sistemas informáticos, filtrar información confidencial u obtener acceso no autorizado. Algunos ejemplos de malware son los virus, los gusanos, el ransomware, los troyanos, el spyware y los registradores de pulsaciones de teclas.

servicios gestionados

Servicios de AWS para los que AWS opera la capa de infraestructura, el sistema operativo y las plataformas, y usted accede a los puntos finales para almacenar y recuperar datos. Amazon Simple Storage Service (Amazon S3) y Amazon DynamoDB son ejemplos de servicios gestionados. También se conocen como servicios abstractos.

sistema de ejecución de fabricación (MES)

Un sistema de software para rastrear, monitorear, documentar y controlar los procesos de producción que convierten las materias primas en productos terminados en el taller.

MAP

Consulte Migration Acceleration Program.

mecanismo

Un proceso completo en el que se crea una herramienta, se impulsa su adopción y, a continuación, se inspeccionan los resultados para realizar los ajustes necesarios. Un mecanismo es un ciclo que se refuerza y mejora a sí mismo a medida que funciona. Para obtener más información, consulte Creación de mecanismos en el AWS Well-Architected Framework.

cuenta de miembro

Todas las Cuentas de AWS demás cuentas, excepto la de administración, que forman parte de una organización. AWS Organizations Una cuenta no puede pertenecer a más de una organización a la vez.

MES

Consulte el sistema de ejecución de la fabricación.

Transporte telemétrico de Message Queue Queue (MQTT)

Un protocolo de comunicación ligero machine-to-machine (M2M), basado en el patrón de publicación/suscripción, para dispositivos de IoT con recursos limitados.

microservicio

Un servicio pequeño e independiente que se comunica a través de una red bien definida APIs y que, por lo general, es propiedad de equipos pequeños e independientes. Por ejemplo, un sistema de seguros puede incluir microservicios que se adapten a las capacidades empresariales, como las de ventas o marketing, o a subdominios, como las de compras, reclamaciones o análisis. Los beneficios de los microservicios incluyen la agilidad, la escalabilidad flexible, la facilidad de implementación, el código reutilizable y la resiliencia. Para obtener más información, consulte Integrar microservicios mediante AWS servicios sin servidor.

arquitectura de microservicios

Un enfoque para crear una aplicación con componentes independientes que ejecutan cada proceso de la aplicación como un microservicio. Estos microservicios se comunican a través de una interfaz bien definida mediante un uso ligero. APIs Cada microservicio de esta arquitectura se puede actualizar, implementar y escalar para satisfacer la demanda de funciones específicas de una aplicación. Para obtener más información, consulte Implementación de microservicios en. AWS

Programa de aceleración de la migración (MAP)

Un AWS programa que proporciona soporte de consultoría, formación y servicios para ayudar a las organizaciones a crear una base operativa sólida para migrar a la nube y para ayudar a compensar el costo inicial de las migraciones. El MAP incluye una metodología de migración para ejecutar las migraciones antiguas de forma metódica y un conjunto de herramientas para automatizar y acelerar los escenarios de migración más comunes.

migración a escala

Proceso de transferencia de la mayoría de la cartera de aplicaciones a la nube en oleadas, con más aplicaciones desplazadas a un ritmo más rápido en cada oleada. En esta fase, se utilizan las prácticas recomendadas y las lecciones aprendidas en las fases anteriores para implementar una fábrica de migración de equipos, herramientas y procesos con el fin de agilizar la migración de las cargas de trabajo mediante la automatización y la entrega ágil. Esta es la tercera fase de la estrategia de migración de AWS.

fábrica de migración

Equipos multifuncionales que agilizan la migración de las cargas de trabajo mediante enfoques automatizados y ágiles. Los equipos de las fábricas de migración suelen incluir a analistas y propietarios de operaciones, empresas, ingenieros de migración, desarrolladores y DevOps profesionales que trabajan a pasos agigantados. Entre el 20 y el 50 por ciento de la cartera de aplicaciones empresariales se compone de patrones repetidos que pueden optimizarse mediante un enfoque de fábrica. Para obtener más información, consulte la discusión sobre las fábricas de migración y la Guía de fábricas de migración a la nube en este contenido.

metadatos de migración

Información sobre la aplicación y el servidor que se necesita para completar la migración. Cada patrón de migración requiere un conjunto diferente de metadatos de migración. Algunos ejemplos de metadatos de migración son la subred de destino, el grupo de seguridad y AWS la cuenta.

patrón de migración

Tarea de migración repetible que detalla la estrategia de migración, el destino de la migración y la aplicación o el servicio de migración utilizados. Ejemplo: realoje la migración a Amazon EC2 con AWS Application Migration Service.

Migration Portfolio Assessment (MPA)

Una herramienta en línea que proporciona información para validar el modelo de negocio para migrar a. Nube de AWS La MPA ofrece una evaluación detallada de la cartera (adecuación del tamaño de los servidores, precios, comparaciones del costo total de propiedad, análisis de los costos de migración), así como una planificación de la migración (análisis y recopilación de datos de aplicaciones, agrupación de aplicaciones, priorización de la migración y planificación de oleadas). La herramienta MPA (requiere iniciar sesión) está disponible de forma gratuita para todos los AWS consultores y consultores asociados de APN.

Evaluación de la preparación para la migración (MRA)

Proceso que consiste en obtener información sobre el estado de preparación de una organización para la nube, identificar sus puntos fuertes y débiles y elaborar un plan de acción para cerrar las brechas identificadas mediante el AWS CAF. Para obtener más información, consulte la Guía de preparación para la migración. La MRA es la primera fase de la estrategia de migración de AWS.

estrategia de migración

El enfoque utilizado para migrar una carga de trabajo a. Nube de AWS Para obtener más información, consulte la entrada de las 7 R de este glosario y consulte Movilice a su organización para acelerar las migraciones a gran escala.

ML

Consulte el aprendizaje automático.

modernización

Transformar una aplicación obsoleta (antigua o monolítica) y su infraestructura en un sistema ágil, elástico y de alta disponibilidad en la nube para reducir los gastos, aumentar la eficiencia y aprovechar las innovaciones. Para obtener más información, consulte Estrategia para modernizar las aplicaciones en el Nube de AWS.

evaluación de la preparación para la modernización

Evaluación que ayuda a determinar la preparación para la modernización de las aplicaciones de una organización; identifica los beneficios, los riesgos y las dependencias; y determina qué tan bien la organización puede soportar el estado futuro de esas aplicaciones. El resultado de la evaluación es un esquema de la arquitectura objetivo, una hoja de ruta que detalla las fases de desarrollo y los hitos del proceso de modernización y un plan de acción para abordar las brechas identificadas. Para obtener más información, consulte Evaluación de la preparación para la modernización de las aplicaciones en el Nube de AWS.

aplicaciones monolíticas (monolitos)

Aplicaciones que se ejecutan como un único servicio con procesos estrechamente acoplados. Las aplicaciones monolíticas presentan varios inconvenientes. Si una característica de la aplicación experimenta un aumento en la demanda, se debe escalar toda la arquitectura. Agregar o mejorar las características de una aplicación monolítica también se vuelve más complejo a medida que crece la base de código. Para solucionar problemas con la aplicación, puede utilizar una arquitectura de microservicios. Para obtener más información, consulte Descomposición de monolitos en microservicios.

MAPA

Consulte la evaluación de la cartera de migración.

MQTT

Consulte Message Queue Queue Telemetría y Transporte.

clasificación multiclase

Un proceso que ayuda a generar predicciones para varias clases (predice uno de más de dos resultados). Por ejemplo, un modelo de ML podría preguntar "¿Este producto es un libro, un automóvil o un teléfono?" o "¿Qué categoría de productos es más interesante para este cliente?".

infraestructura mutable

Un modelo que actualiza y modifica la infraestructura existente para las cargas de trabajo de producción. Para mejorar la coherencia, la fiabilidad y la previsibilidad, el AWS Well-Architected Framework recomienda el uso de una infraestructura inmutable como práctica recomendada.

O

OAC

Consulte el control de acceso de origen.

OAI

Consulte la identidad de acceso de origen.

OCM

Consulte gestión del cambio organizacional.

migración fuera de línea

Método de migración en el que la carga de trabajo de origen se elimina durante el proceso de migración. Este método implica un tiempo de inactividad prolongado y, por lo general, se utiliza para cargas de trabajo pequeñas y no críticas.

OI

Consulte integración de operaciones.

OLA

Véase el acuerdo a nivel operativo.

migración en línea

Método de migración en el que la carga de trabajo de origen se copia al sistema de destino sin que se desconecte. Las aplicaciones que están conectadas a la carga de trabajo pueden seguir

funcionando durante la migración. Este método implica un tiempo de inactividad nulo o mínimo y, por lo general, se utiliza para cargas de trabajo de producción críticas.

OPC-UA

Consulte Open Process Communications: arquitectura unificada.

Comunicaciones de proceso abierto: arquitectura unificada (OPC-UA)

Un protocolo de comunicación machine-to-machine (M2M) para la automatización industrial. El OPC-UA proporciona un estándar de interoperabilidad con esquemas de cifrado, autenticación y autorización de datos.

acuerdo de nivel operativo (OLA)

Acuerdo que aclara lo que los grupos de TI operativos se comprometen a ofrecerse entre sí, para respaldar un acuerdo de nivel de servicio (SLA).

revisión de la preparación operativa (ORR)

Una lista de preguntas y las mejores prácticas asociadas que le ayudan a comprender, evaluar, prevenir o reducir el alcance de los incidentes y posibles fallos. Para obtener más información, consulte Operational Readiness Reviews (ORR) en AWS Well-Architected Framework.

tecnología operativa (OT)

Sistemas de hardware y software que funcionan con el entorno físico para controlar las operaciones, los equipos y la infraestructura industriales. En la industria manufacturera, la integración de los sistemas de TO y tecnología de la información (TI) es un enfoque clave para las transformaciones de la industria 4.0.

integración de operaciones (OI)

Proceso de modernización de las operaciones en la nube, que implica la planificación de la preparación, la automatización y la integración. Para obtener más información, consulte la Guía de integración de las operaciones.

registro de seguimiento organizativo

Un registro creado por el AWS CloudTrail que se registran todos los eventos para todos Cuentas de AWS los miembros de una organización AWS Organizations. Este registro de seguimiento se crea en cada Cuenta de AWS que forma parte de la organización y realiza un seguimiento de la actividad en cada cuenta. Para obtener más información, consulte Crear un registro para una organización en la CloudTrail documentación.

administración del cambio organizacional (OCM)

Marco para administrar las transformaciones empresariales importantes y disruptivas desde la perspectiva de las personas, la cultura y el liderazgo. La OCM ayuda a las empresas a prepararse para nuevos sistemas y estrategias y a realizar la transición a ellos, al acelerar la adopción de cambios, abordar los problemas de transición e impulsar cambios culturales y organizacionales. En la estrategia de AWS migración, este marco se denomina aceleración del personal, debido a la velocidad de cambio que requieren los proyectos de adopción de la nube. Para obtener más información, consulte la Guía de OCM.

control de acceso de origen (OAC)

En CloudFront, una opción mejorada para restringir el acceso y proteger el contenido del Amazon Simple Storage Service (Amazon S3). El OAC admite todos los buckets de S3 Regiones de AWS, el cifrado del lado del servidor AWS KMS (SSE-KMS) y las solicitudes dinámicas `PUT` y `DELETE` dirigidas al bucket de S3.

identidad de acceso de origen (OAI)

En CloudFront, una opción para restringir el acceso y proteger el contenido de Amazon S3. Cuando utiliza OAI, CloudFront crea un principal con el que Amazon S3 puede autenticarse. Los directores autenticados solo pueden acceder al contenido de un bucket de S3 a través de una distribución específica. CloudFront Consulte también el OAC, que proporciona un control de acceso más detallado y mejorado.

ORR

Consulte la revisión de la preparación operativa.

OT

Consulte la tecnología operativa.

VPC saliente (de salida)

En una arquitectura de AWS cuentas múltiples, una VPC que gestiona las conexiones de red que se inician desde una aplicación. La arquitectura AWS de referencia de seguridad recomienda configurar la cuenta de red con entradas, salidas e inspección VPCs para proteger la interfaz bidireccional entre la aplicación e Internet en general.

P

límite de permisos

Una política de administración de IAM que se adjunta a las entidades principales de IAM para establecer los permisos máximos que puede tener el usuario o el rol. Para obtener más información, consulte Límites de permisos en la documentación de IAM.

información de identificación personal (PII)

Información que, vista directamente o combinada con otros datos relacionados, puede utilizarse para deducir de manera razonable la identidad de una persona. Algunos ejemplos de información de identificación personal son los nombres, las direcciones y la información de contacto.

PII

Consulte la información de identificación personal.

manual de estrategias

Conjunto de pasos predefinidos que capturan el trabajo asociado a las migraciones, como la entrega de las funciones de operaciones principales en la nube. Un manual puede adoptar la forma de scripts, manuales de procedimientos automatizados o resúmenes de los procesos o pasos necesarios para operar un entorno modernizado.

PLC

Consulte controlador lógico programable.

PLM

Consulte la gestión del ciclo de vida del producto.

policy

Un objeto que puede definir los permisos (consulte la política basada en la identidad), especifique las condiciones de acceso (consulte la política basada en los recursos) o defina los permisos máximos para todas las cuentas de una organización AWS Organizations (consulte la política de control de servicios).

persistencia políglota

Elegir de forma independiente la tecnología de almacenamiento de datos de un microservicio en función de los patrones de acceso a los datos y otros requisitos. Si sus microservicios tienen la misma tecnología de almacenamiento de datos, pueden enfrentarse a desafíos de

implementación o experimentar un rendimiento deficiente. Los microservicios se implementan más fácilmente y logran un mejor rendimiento y escalabilidad si utilizan el almacén de datos que mejor se adapte a sus necesidades. Para obtener más información, consulte Habilitación de la persistencia de datos en los microservicios.

evaluación de cartera

Proceso de detección, análisis y priorización de la cartera de aplicaciones para planificar la migración. Para obtener más información, consulte la Evaluación de la preparación para la migración.

predicate

Una condición de consulta que devuelve `true` o`false`, por lo general, se encuentra en una cláusula. `WHERE`

pulsar un predicado

Técnica de optimización de consultas de bases de datos que filtra los datos de la consulta antes de transferirlos. Esto reduce la cantidad de datos que se deben recuperar y procesar de la base de datos relacional y mejora el rendimiento de las consultas.

control preventivo

Un control de seguridad diseñado para evitar que ocurra un evento. Estos controles son la primera línea de defensa para evitar el acceso no autorizado o los cambios no deseados en la red. Para obtener más información, consulte Controles preventivos en Implementación de controles de seguridad en AWS.

entidad principal

Una entidad AWS que puede realizar acciones y acceder a los recursos. Esta entidad suele ser un usuario raíz para un Cuenta de AWS rol de IAM o un usuario. Para obtener más información, consulte Entidad principal en Términos y conceptos de roles en la documentación de IAM.

privacidad desde el diseño

Un enfoque de ingeniería de sistemas que tiene en cuenta la privacidad durante todo el proceso de desarrollo.

zonas alojadas privadas

Un contenedor que contiene información sobre cómo desea que Amazon Route 53 responda a las consultas de DNS de un dominio y sus subdominios dentro de uno o más VPCs. Para obtener más información, consulte Uso de zonas alojadas privadas en la documentación de Route 53.

control proactivo

Un control de seguridad diseñado para evitar el despliegue de recursos que no cumplan con las normas. Estos controles escanean los recursos antes de aprovisionarlos. Si el recurso no cumple con el control, significa que no está aprovisionado. Para obtener más información, consulte la guía de referencia de controles en la AWS Control Tower documentación y consulte Controles proactivos en Implementación de controles de seguridad en AWS.

gestión del ciclo de vida del producto (PLM)

La gestión de los datos y los procesos de un producto a lo largo de todo su ciclo de vida, desde el diseño, el desarrollo y el lanzamiento, pasando por el crecimiento y la madurez, hasta el rechazo y la retirada.

entorno de producción

Consulte el entorno.

controlador lógico programable (PLC)

En la fabricación, una computadora adaptable y altamente confiable que monitorea las máquinas y automatiza los procesos de fabricación.

encadenamiento rápido

Utilizar la salida de un mensaje de LLM como entrada para el siguiente mensaje para generar mejores respuestas. Esta técnica se utiliza para dividir una tarea compleja en subtareas o para refinar o ampliar de forma iterativa una respuesta preliminar. Ayuda a mejorar la precisión y la relevancia de las respuestas de un modelo y permite obtener resultados más detallados y personalizados.

seudonimización

El proceso de reemplazar los identificadores personales de un conjunto de datos por valores de marcadores de posición. La seudonimización puede ayudar a proteger la privacidad personal. Los datos seudonimizados siguen considerándose datos personales.

publish/subscribe (pub/sub)

Un patrón que permite las comunicaciones asíncronas entre microservicios para mejorar la escalabilidad y la capacidad de respuesta. Por ejemplo, en un MES basado en microservicios, un microservicio puede publicar mensajes de eventos en un canal al que se puedan suscribir otros microservicios. El sistema puede añadir nuevos microservicios sin cambiar el servicio de publicación.

Q

plan de consulta

Serie de pasos, como instrucciones, que se utilizan para acceder a los datos de un sistema de base de datos relacional SQL.

regresión del plan de consulta

El optimizador de servicios de la base de datos elige un plan menos óptimo que antes de un cambio determinado en el entorno de la base de datos. Los cambios en estadísticas, restricciones, configuración del entorno, enlaces de parámetros de consultas y actualizaciones del motor de base de datos PostgreSQL pueden provocar una regresión del plan.

R

Matriz RACI

Véase responsable, responsable, consultado, informado (RACI).

RAG

Consulte Retrieval Augmented Generation.

ransomware

Software malicioso que se ha diseñado para bloquear el acceso a un sistema informático o a los datos hasta que se efectúe un pago.

Matriz RASCI

Véase responsable, responsable, consultado, informado (RACI).

RCAC

Consulte control de acceso por filas y columnas.

réplica de lectura

Una copia de una base de datos que se utiliza con fines de solo lectura. Puede enrutar las consultas a la réplica de lectura para reducir la carga en la base de datos principal.

rediseñar

Ver 7 Rs.

objetivo de punto de recuperación (RPO)

La cantidad de tiempo máximo aceptable desde el último punto de recuperación de datos. Esto determina qué se considera una pérdida de datos aceptable entre el último punto de recuperación y la interrupción del servicio.

objetivo de tiempo de recuperación (RTO)

La demora máxima aceptable entre la interrupción del servicio y el restablecimiento del servicio.

refactorizar

Ver 7 Rs.

Región

Una colección de AWS recursos en un área geográfica. Cada uno Región de AWS está aislado y es independiente de los demás para proporcionar tolerancia a las fallas, estabilidad y resiliencia. Para obtener más información, consulte Regiones de AWS Especificar qué cuenta puede usar.

regresión

Una técnica de ML que predice un valor numérico. Por ejemplo, para resolver el problema de "¿A qué precio se venderá esta casa?", un modelo de ML podría utilizar un modelo de regresión lineal para predecir el precio de venta de una vivienda en función de datos conocidos sobre ella (por ejemplo, los metros cuadrados).

volver a alojar

Consulte 7 Rs.

versión

En un proceso de implementación, el acto de promover cambios en un entorno de producción.

trasladarse

Ver 7 Rs.

redefinir la plataforma

Ver 7 Rs.

recompra

Ver 7 Rs.

resiliencia

La capacidad de una aplicación para resistir las interrupciones o recuperarse de ellas. La alta disponibilidad y la recuperación ante desastres son consideraciones comunes a la hora de planificar la resiliencia en el. Nube de AWS Para obtener más información, consulte Nube de AWS Resiliencia.

política basada en recursos

Una política asociada a un recurso, como un bucket de Amazon S3, un punto de conexión o una clave de cifrado. Este tipo de política especifica a qué entidades principales se les permite el acceso, las acciones compatibles y cualquier otra condición que deba cumplirse.

matriz responsable, confiable, consultada e informada (RACI)

Una matriz que define las funciones y responsabilidades de todas las partes involucradas en las actividades de migración y las operaciones de la nube. El nombre de la matriz se deriva de los tipos de responsabilidad definidos en la matriz: responsable (R), contable (A), consultado (C) e informado (I). El tipo de soporte (S) es opcional. Si incluye el soporte, la matriz se denomina matriz RASCI y, si la excluye, se denomina matriz RACI.

control receptivo

Un control de seguridad que se ha diseñado para corregir los eventos adversos o las desviaciones con respecto a su base de seguridad. Para obtener más información, consulte Controles receptivos en Implementación de controles de seguridad en AWS.

retain

Consulte 7 Rs.

jubilarse

Ver 7 Rs.

Generación aumentada de recuperación (RAG)

Tecnología de inteligencia artificial generativa en la que un máster hace referencia a una fuente de datos autorizada que se encuentra fuera de sus fuentes de datos de formación antes de generar una respuesta. Por ejemplo, un modelo RAG podría realizar una búsqueda semántica en la base de conocimientos o en los datos personalizados de una organización. Para obtener más información, consulte Qué es el RAG.

rotación

Proceso de actualizar periódicamente un secreto para dificultar el acceso de un atacante a las credenciales.

control de acceso por filas y columnas (RCAC)

El uso de expresiones SQL básicas y flexibles que tienen reglas de acceso definidas. El RCAC consta de permisos de fila y máscaras de columnas.

RPO

Consulte el objetivo del punto de recuperación.

RTO

Consulte el objetivo de tiempo de recuperación.

manual de procedimientos

Conjunto de procedimientos manuales o automatizados necesarios para realizar una tarea específica. Por lo general, se diseñan para agilizar las operaciones o los procedimientos repetitivos con altas tasas de error.

S

SAML 2.0

Un estándar abierto que utilizan muchos proveedores de identidad (IdPs). Esta función permite el inicio de sesión único (SSO) federado, de modo que los usuarios pueden iniciar sesión AWS Management Console o llamar a las operaciones de la AWS API sin tener que crear un usuario en IAM para todos los miembros de la organización. Para obtener más información sobre la federación basada en SAML 2.0, consulte Acerca de la federación basada en SAML 2.0 en la documentación de IAM.

SCADA

Consulte el control de supervisión y la adquisición de datos.

SCP

Consulte la política de control de servicios.

secreta

Información confidencial o restringida, como una contraseña o credenciales de usuario, que almacene de forma cifrada. AWS Secrets Manager Se compone del valor secreto y sus metadatos. El valor secreto puede ser binario, una sola cadena o varias cadenas. Para obtener más información, consulta ¿Qué hay en un secreto de Secrets Manager? en la documentación de Secrets Manager.

seguridad desde el diseño

Un enfoque de ingeniería de sistemas que tiene en cuenta la seguridad durante todo el proceso de desarrollo.

control de seguridad

Barrera de protección técnica o administrativa que impide, detecta o reduce la capacidad de un agente de amenazas para aprovechar una vulnerabilidad de seguridad. Existen cuatro tipos principales de controles de seguridad: preventivos, de detección, con capacidad de respuesta y proactivos.

refuerzo de la seguridad

Proceso de reducir la superficie expuesta a ataques para hacerla más resistente a los ataques. Esto puede incluir acciones, como la eliminación de los recursos que ya no se necesitan, la implementación de prácticas recomendadas de seguridad consistente en conceder privilegios mínimos o la desactivación de características innecesarias en los archivos de configuración.

sistema de información sobre seguridad y administración de eventos (SIEM)

Herramientas y servicios que combinan sistemas de administración de información sobre seguridad (SIM) y de administración de eventos de seguridad (SEM). Un sistema de SIEM recopila, monitorea y analiza los datos de servidores, redes, dispositivos y otras fuentes para detectar amenazas y brechas de seguridad y generar alertas.

automatización de la respuesta de seguridad

Una acción predefinida y programada que está diseñada para responder automáticamente a un evento de seguridad o remediarlo. Estas automatizaciones sirven como controles de seguridad detectables o adaptables que le ayudan a implementar las mejores prácticas AWS de seguridad. Algunos ejemplos de acciones de respuesta automatizadas incluyen la modificación de un grupo de seguridad de VPC, la aplicación de parches a una EC2 instancia de Amazon o la rotación de credenciales.

cifrado del servidor

Cifrado de los datos en su destino, por parte de quien Servicio de AWS los recibe.

política de control de servicio (SCP)

Política que proporciona un control centralizado de los permisos de todas las cuentas de una organización en AWS Organizations. SCPs defina barreras o establezca límites a las acciones que un administrador puede delegar en usuarios o roles. Puede utilizarlas SCPs como listas de permitidos o rechazados para especificar qué servicios o acciones están permitidos o prohibidos. Para obtener más información, consulte las políticas de control de servicios en la AWS Organizations documentación.

punto de enlace de servicio

La URL del punto de entrada de un Servicio de AWS. Para conectarse mediante programación a un servicio de destino, puede utilizar un punto de conexión. Para obtener más información, consulte Puntos de conexión de Servicio de AWS en Referencia general de AWS.

acuerdo de nivel de servicio (SLA)

Acuerdo que aclara lo que un equipo de TI se compromete a ofrecer a los clientes, como el tiempo de actividad y el rendimiento del servicio.

indicador de nivel de servicio (SLI)

Medición de un aspecto del rendimiento de un servicio, como la tasa de errores, la disponibilidad o el rendimiento.

objetivo de nivel de servicio (SLO)

Una métrica objetivo que representa el estado de un servicio, medido mediante un indicador de nivel de servicio.

modelo de responsabilidad compartida

Un modelo que describe la responsabilidad que compartes con respecto a la seguridad y AWS el cumplimiento de la nube. AWS es responsable de la seguridad de la nube, mientras que usted es responsable de la seguridad en la nube. Para obtener más información, consulte el Modelo de responsabilidad compartida.

SIEM

Consulte la información de seguridad y el sistema de gestión de eventos.

punto único de fallo (SPOF)

Una falla en un único componente crítico de una aplicación que puede interrumpir el sistema.

SLA

Consulte el acuerdo de nivel de servicio.

SLI

Consulte el indicador de nivel de servicio.

SLO

Consulte el objetivo de nivel de servicio.

split-and-seed modelo

Un patrón para escalar y acelerar los proyectos de modernización. A medida que se definen las nuevas funciones y los lanzamientos de los productos, el equipo principal se divide para crear nuevos equipos de productos. Esto ayuda a ampliar las capacidades y los servicios de su organización, mejora la productividad de los desarrolladores y apoya la innovación rápida. Para obtener más información, consulte Enfoque gradual para modernizar las aplicaciones en el Nube de AWS.

SPOF

Consulte el punto único de falla.

esquema en forma de estrella

Estructura organizativa de una base de datos que utiliza una tabla de datos grande para almacenar datos transaccionales o medidos y una o más tablas dimensionales más pequeñas para almacenar los atributos de los datos. Esta estructura está diseñada para usarse en un almacén de datos o con fines de inteligencia empresarial.

patrón de higo estrangulador

Un enfoque para modernizar los sistemas monolíticos mediante la reescritura y el reemplazo gradual de las funciones del sistema hasta que se pueda desmantelar el sistema heredado. Este patrón utiliza la analogía de una higuera que crece hasta convertirse en un árbol estable y, finalmente, se apodera y reemplaza a su host. El patrón fue presentado por Martin Fowler como una forma de gestionar el riesgo al reescribir sistemas monolíticos. Para ver un ejemplo con la aplicación de este patrón, consulte Modernización gradual de los servicios web antiguos de Microsoft ASP.NET (ASMX) mediante contenedores y Amazon API Gateway.

subred

Un intervalo de direcciones IP en la VPC. Una subred debe residir en una sola zona de disponibilidad.

supervisión, control y adquisición de datos (SCADA)

En la industria manufacturera, un sistema que utiliza hardware y software para monitorear los activos físicos y las operaciones de producción.

cifrado simétrico

Un algoritmo de cifrado que utiliza la misma clave para cifrar y descifrar los datos.

pruebas sintéticas

Probar un sistema de manera que simule las interacciones de los usuarios para detectar posibles problemas o monitorear el rendimiento. Puede usar Amazon CloudWatch Synthetics para crear estas pruebas.

indicador del sistema

Una técnica para proporcionar contexto, instrucciones o pautas a un LLM para dirigir su comportamiento. Las indicaciones del sistema ayudan a establecer el contexto y las reglas para las interacciones con los usuarios.

T

etiquetas

Pares clave-valor que actúan como metadatos para organizar los recursos. AWS Las etiquetas pueden ayudarle a administrar, identificar, organizar, buscar y filtrar recursos. Para obtener más información, consulte Etiquetado de los recursos de AWS.

variable de destino

El valor que intenta predecir en el ML supervisado. Esto también se conoce como variable de resultado. Por ejemplo, en un entorno de fabricación, la variable objetivo podría ser un defecto del producto.

lista de tareas

Herramienta que se utiliza para hacer un seguimiento del progreso mediante un manual de procedimientos. La lista de tareas contiene una descripción general del manual de

procedimientos y una lista de las tareas generales que deben completarse. Para cada tarea general, se incluye la cantidad estimada de tiempo necesario, el propietario y el progreso.

entorno de prueba

Consulte entorno.

entrenamiento

Proporcionar datos de los que pueda aprender su modelo de ML. Los datos de entrenamiento deben contener la respuesta correcta. El algoritmo de aprendizaje encuentra patrones en los datos de entrenamiento que asignan los atributos de los datos de entrada al destino (la respuesta que desea predecir). Genera un modelo de ML que captura estos patrones. Luego, el modelo de ML se puede utilizar para obtener predicciones sobre datos nuevos para los que no se conoce el destino.

puerta de enlace de tránsito

Un centro de tránsito de red que puede usar para interconectar sus VPCs redes con las locales. Para obtener más información, consulte Qué es una pasarela de tránsito en la AWS Transit Gateway documentación.

flujo de trabajo basado en enlaces troncales

Un enfoque en el que los desarrolladores crean y prueban características de forma local en una rama de característica y, a continuación, combinan esos cambios en la rama principal. Luego, la rama principal se adapta a los entornos de desarrollo, preproducción y producción, de forma secuencial.

acceso de confianza

Otorgar permisos a un servicio que especifique para realizar tareas en su organización AWS Organizations y en sus cuentas en su nombre. El servicio de confianza crea un rol vinculado al servicio en cada cuenta, cuando ese rol es necesario, para realizar las tareas de administración por usted. Para obtener más información, consulte AWS Organizations Utilización con otros AWS servicios en la AWS Organizations documentación.

ajuste

Cambiar aspectos de su proceso de formación a fin de mejorar la precisión del modelo de ML. Por ejemplo, puede entrenar el modelo de ML al generar un conjunto de etiquetas, incorporar etiquetas y, luego, repetir estos pasos varias veces con diferentes ajustes para optimizar el modelo.

equipo de dos pizzas

Un DevOps equipo pequeño al que puedes alimentar con dos pizzas. Un equipo formado por dos integrantes garantiza la mejor oportunidad posible de colaboración en el desarrollo de software.

U

incertidumbre

Un concepto que hace referencia a información imprecisa, incompleta o desconocida que puede socavar la fiabilidad de los modelos predictivos de ML. Hay dos tipos de incertidumbre: la incertidumbre epistémica se debe a datos limitados e incompletos, mientras que la incertidumbre aleatoria se debe al ruido y la aleatoriedad inherentes a los datos. Para más información, consulte la guía Cuantificación de la incertidumbre en los sistemas de aprendizaje profundo.

tareas indiferenciadas

También conocido como tareas arduas, es el trabajo que es necesario para crear y operar una aplicación, pero que no proporciona un valor directo al usuario final ni proporciona una ventaja competitiva. Algunos ejemplos de tareas indiferenciadas son la adquisición, el mantenimiento y la planificación de la capacidad.

entornos superiores

Ver entorno.

V

succión

Una operación de mantenimiento de bases de datos que implica limpiar después de las actualizaciones incrementales para recuperar espacio de almacenamiento y mejorar el rendimiento.

control de versión

Procesos y herramientas que realizan un seguimiento de los cambios, como los cambios en el código fuente de un repositorio.

Interconexión con VPC

Una conexión entre dos VPCs que le permite enrutar el tráfico mediante direcciones IP privadas. Para obtener más información, consulte ¿Qué es una interconexión de VPC? en la documentación de Amazon VPC.

vulnerabilidad

Defecto de software o hardware que pone en peligro la seguridad del sistema.

W

caché caliente

Un búfer caché que contiene datos actuales y relevantes a los que se accede con frecuencia. La instancia de base de datos puede leer desde la caché del búfer, lo que es más rápido que leer desde la memoria principal o el disco.

datos templados

Datos a los que el acceso es infrecuente. Al consultar este tipo de datos, normalmente se aceptan consultas moderadamente lentas.

función de ventana

Función SQL que realiza un cálculo en un grupo de filas que se relacionan de alguna manera con el registro actual. Las funciones de ventana son útiles para procesar tareas, como calcular una media móvil o acceder al valor de las filas en función de la posición relativa de la fila actual.

carga de trabajo

Conjunto de recursos y código que ofrece valor comercial, como una aplicación orientada al cliente o un proceso de backend.

flujo de trabajo

Grupos funcionales de un proyecto de migración que son responsables de un conjunto específico de tareas. Cada flujo de trabajo es independiente, pero respalda a los demás flujos de trabajo del proyecto. Por ejemplo, el flujo de trabajo de la cartera es responsable de priorizar las aplicaciones, planificar las oleadas y recopilar los metadatos de migración. El flujo de trabajo de la cartera entrega estos recursos al flujo de trabajo de migración, que luego migra los servidores y las aplicaciones.

GUSANO

Mira, escribe una vez, lee muchas.

WQF

Consulte el marco AWS de calificación de la carga de trabajo.

escribe una vez, lee muchas (WORM)

Un modelo de almacenamiento que escribe los datos una sola vez y evita que los datos se eliminen o modifiquen. Los usuarios autorizados pueden leer los datos tantas veces como sea necesario, pero no pueden cambiarlos. Esta infraestructura de almacenamiento de datos se considera inmutable.

Z

ataque de día cero

Un ataque, normalmente de malware, que aprovecha una vulnerabilidad de día cero.

vulnerabilidad de día cero

Un defecto o una vulnerabilidad sin mitigación en un sistema de producción. Los agentes de amenazas pueden usar este tipo de vulnerabilidad para atacar el sistema. Los desarrolladores suelen darse cuenta de la vulnerabilidad a raíz del ataque.

aviso de tiro cero

Proporcionar a un LLM instrucciones para realizar una tarea, pero sin ejemplos (imágenes) que puedan ayudar a guiarla. El LLM debe utilizar sus conocimientos previamente entrenados para realizar la tarea. La eficacia de las indicaciones cero depende de la complejidad de la tarea y de la calidad de las indicaciones. Consulte también las indicaciones de pocos pasos.

aplicación zombi

Aplicación que utiliza un promedio de CPU y memoria menor al 5 por ciento. En un proyecto de migración, es habitual retirar estas aplicaciones.

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.