



Migración de servidores locales a redes AWS privadas mediante AWS
Application Migration Service

AWS Guía prescriptiva



AWS Guía prescriptiva: Migración de servidores locales a redes AWS privadas mediante AWS Application Migration Service

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

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

Table of Contents

Introducción	1
Escenarios	2
Replicación únicamente a través de redes privadas	2
Salida HTTPS pública en el origen y recursos del área de pruebas privados	4
Salida HTTPS pública en el origen y recursos del área de pruebas públicos	5
Componentes y requisitos de la arquitectura para la replicación restringida	7
Subred de pruebas	7
Subred de origen	8
Subred de destino	8
Prácticas recomendadas de configuración	10
Configuraciones de subredes y enrutamiento	10
Configuración de puntos de conexión de VPC	11
Puntos de enlace de interfaz de VPC	12
Puntos de conexión de puertas de enlace de VPC	13
Puntos de conexión de entrada del solucionador de DNS	14
Grupos de seguridad para la interfaz de red elástica	15
Instalación del agente de Application Migration Service en los servidores de origen	15
Implementación del entorno de PoC	17
Implementación manual	17
Automatización de las implementaciones del agente	19
Supervisión y solución de problemas	21
Pruebas de conectividad y resolución de nombres desde el servidor de origen	21
Pruebas de conectividad y resolución de nombres desde la red del área de pruebas	22
Conclusión	24
Recursos	25
Historial de documentos	26
Glosario	27
#	27
A	28
B	31
C	33
D	36
E	41
F	43

G	45
H	46
I	47
L	50
M	51
O	56
P	58
Q	61
R	62
S	65
T	69
U	70
V	71
W	71
Z	73
.....	lxxiv

Migración de servidores locales a AWS través de redes privadas mediante AWS Application Migration Service

Mike Kuznetsov y Dipin Jain, Amazon Web Services (AWS)

Marzo de 2023 ([historial de documentos](#))

Muchas empresas migran a entornos AWS de red aislados o semiaislados, como centros de datos locales u otras infraestructuras en la nube o híbridas. Por lo general, estas redes aisladas no permiten ningún tráfico de salida hacia puntos de conexión externos, lo cual es necesario para la migración a través de la red. [Otras empresas permiten el tráfico de salida HTTPS de sus redes internas, pero no permiten las comunicaciones específicas en los puertos de red necesarios AWS Application Migration Service, lo que es lo principal Servicio de AWS en las migraciones de gran envergadura. lift-and-shift](#) En un tercer escenario, se permite el tráfico HTTPS desde las áreas de origen y de pruebas, pero el tráfico de replicación de datos debe pasar por el canal privado por motivos de cumplimiento.

El Servicio de migración de aplicaciones [admite estos casos de uso](#) y le permite migrar desde entornos aislados y seguros utilizando únicamente una conectividad de private/public red privada o híbrida. Esta guía describe estos tres escenarios, que van desde los dos public/private modelos híbridos hasta el modelo totalmente aislado, y se centra en los pasos detallados y los requisitos de infraestructura para la opción más restrictiva y exclusiva para el sector privado. Se basa en el patrón de orientación AWS prescriptiva [Connect to Application Migration Service, datos y planos de control a través de una red privada](#), proporcionando:

- Detalles adicionales sobre la conectividad necesaria en cada escenario
- Explicaciones de AWS los recursos que se deben crear
- Opciones de automatización para construir la infraestructura de pruebas AWS e implementarla durante la fase de migración
- Opciones para supervisar y solucionar problemas de conectividad para cada caso de uso

Para obtener más información sobre el funcionamiento de Application Migration Service, consulte estas entradas en el blog:

- [Acelere su migración con AWS Application Migration Service](#)
- [Cómo utilizar lo nuevo AWS Application Migration Service para las Lift-and-Shift migraciones](#)

Escenarios

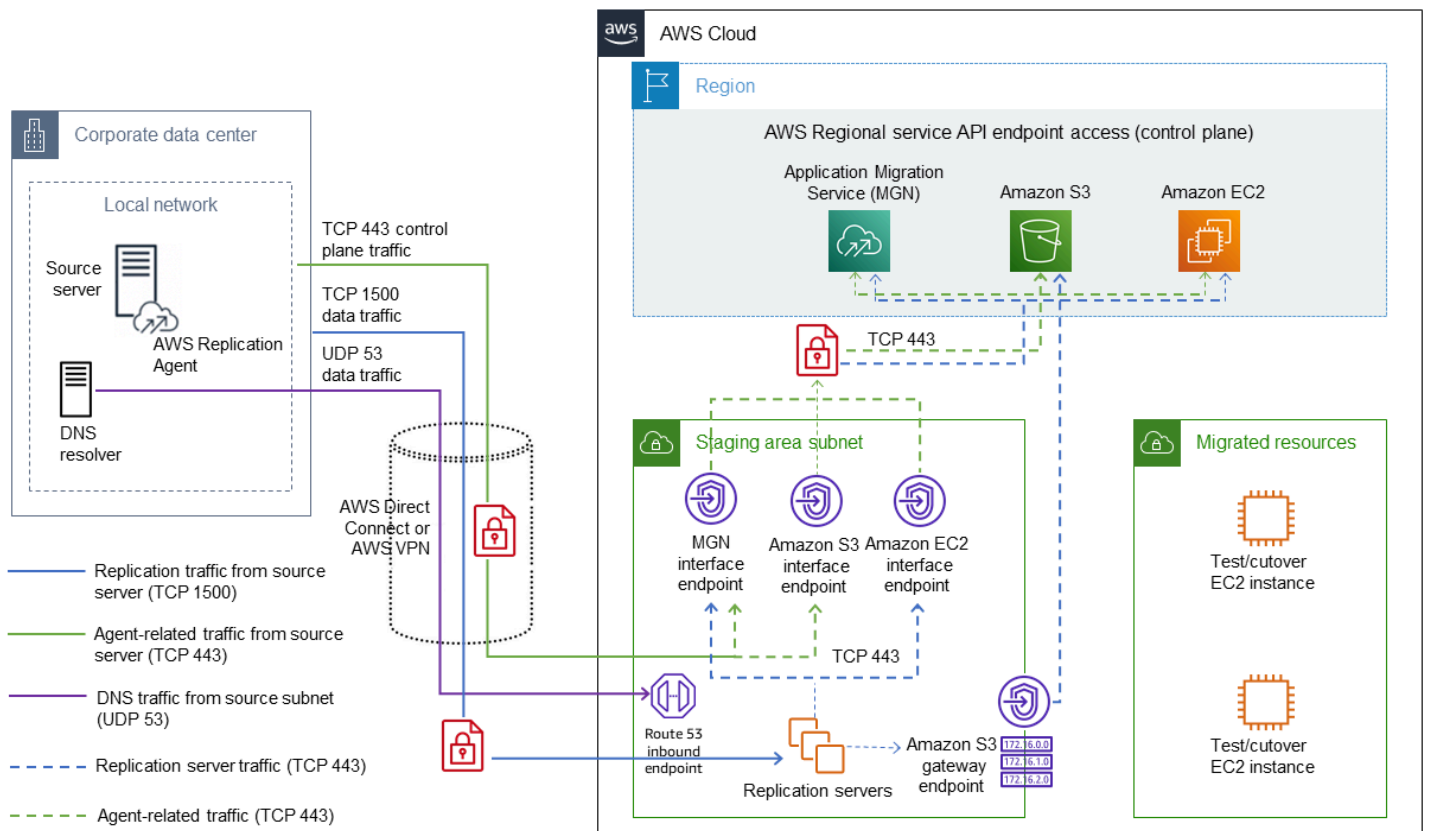
En esta guía se describen los componentes de infraestructura necesarios que debe crear para completar la migración en los siguientes escenarios:

- [Replicación únicamente a través de redes privadas](#), que es el escenario más habitual y restrictivo.
- Escenario híbrido en el que se permite la comunicación de salida HTTPS pero el resto del tráfico está restringido. Este escenario consta de dos opciones:
 - [Salida HTTPS pública en el origen y recursos del área de pruebas privados](#)
 - [Salida HTTPS pública en el origen y recursos del área de pruebas públicos](#)

Para cada escenario, la guía proporciona un ejemplo de configuración y la lista completa de los componentes de AWS requeridos.

Replicación únicamente a través de redes privadas

El siguiente diagrama muestra la arquitectura del escenario más restrictivo, en el que todo el tráfico pasa por el canal privado (Site-to-Site VPN o Direct Connect) entre el entorno de origen y AWS



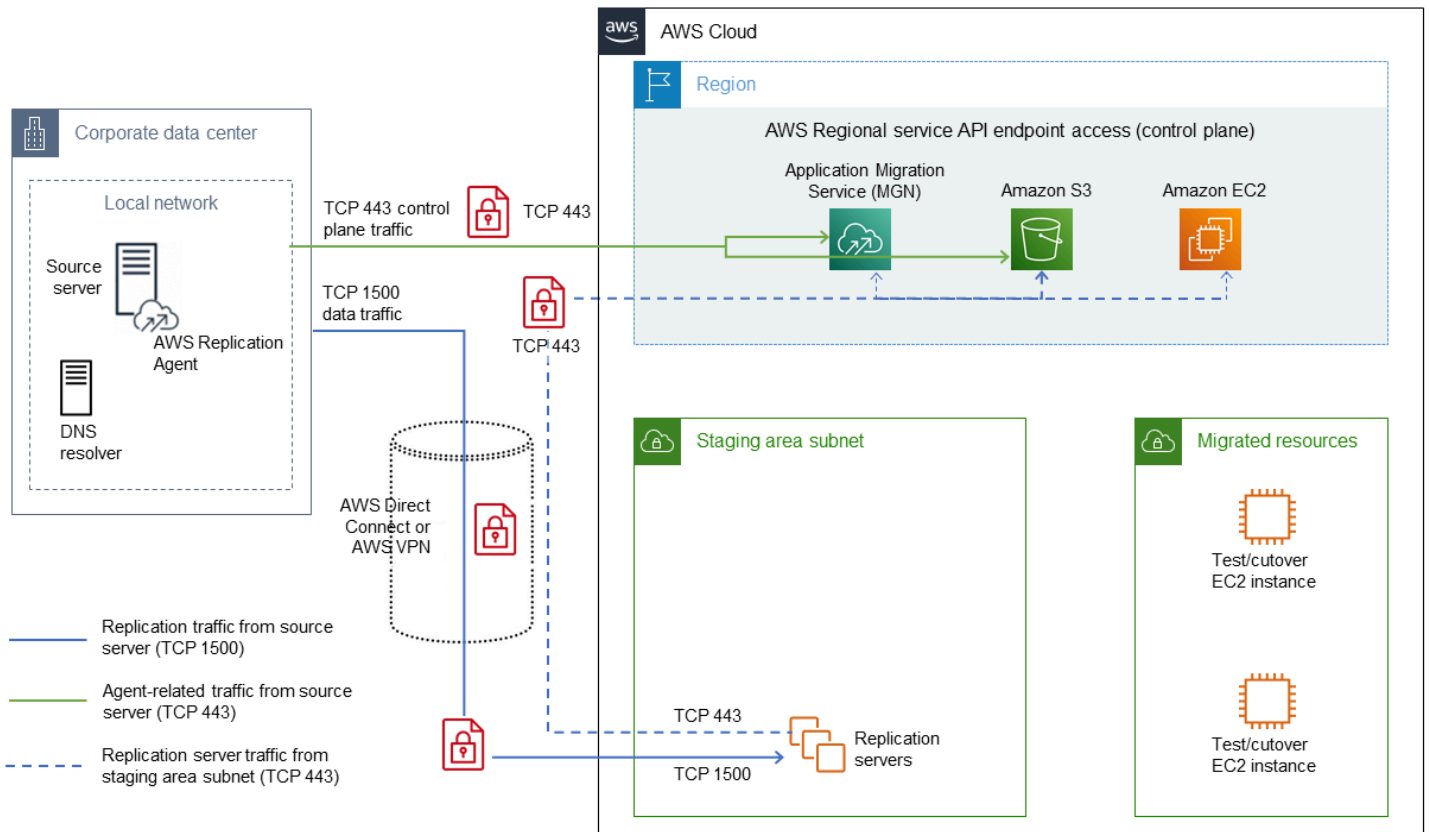
Los principales componentes de esta arquitectura son los siguientes:

- Entorno de origen en el centro de datos corporativo (a la izquierda). Este es el entorno desde el que se va a migrar.
- Entorno de puesta en escena AWS con una nube privada virtual privada (VPC) y una subred (en el medio). Este es el entorno que utilizará Application Migration Service para crear recursos relacionados con la replicación. Estos recursos pueden incluir servidores de replicación, servidores de conversión y volúmenes relacionados con Amazon Elastic Block Store (Amazon EBS) y sus instantáneas de Amazon Simple Storage Service (Amazon S3).
- Conexión VPN desde el entorno de origen a la VPC de pruebas y a las subredes para gestionar tres tipos de tráfico:
 - Puerto HTTPS/TCP 443 para la comunicación con la API
 - Puerto TCP 1500 para la transferencia de datos
 - Tráfico del sistema de nombres de dominio (DNS) a través del puerto UDP 53

- El entorno de destino se encuentra en AWS (a la derecha). Puede ser una VPC completamente aislada o una subred en el entorno de pruebas. (Nota: No hay ningún requisito de conectividad de red desde la subred del entorno de pruebas hasta las subredes de destino).
- Puntos de conexión de interfaz de Amazon VPC para Application Migration Service, Amazon Elastic Compute Cloud (Amazon EC2) y Amazon S3 creados en el entorno de ensayo y un punto de conexión de puerta de enlace de VPC de Amazon S3 al que se puede acceder desde la subred de ensayo.
- Y, por último, el [punto de conexión de entrada del solucionador de DNS](#) en la subred de pruebas. Esto es necesario para que los sistemas de origen conviertan en privados los nombres de dominio completos (FQDNs) de los puntos finales de la VPC. IPs

Salida HTTPS pública en el origen y recursos del área de pruebas privados

El siguiente diagrama ilustra la arquitectura en el escenario híbrido, en el que se permite el tráfico de salida HTTPS desde cualquier servidor de origen y se utiliza para comunicarse con los puntos de enlace de Application Migration Service y Amazon S3, mientras que los datos de replicación en el puerto TCP 1500 pasan por el canal privado (Site-to-Site VPN o Direct Connect) entre el entorno de origen y. AWS



En este escenario, solo el tráfico de replicación de datos en el puerto TCP 1500 pasa por el canal privado. El resto de la comunicación, tanto desde la subred de origen como desde la subred de pruebas, se produce a través de la red pública con los puntos de conexión HTTPS públicos estándar.

Componentes y requisitos de la arquitectura para la replicación restringida

En esta sección se proporciona una descripción detallada del escenario más restrictivo, en el que toda la comunicación se produce únicamente a través del canal privado, e incluye una explicación detallada de los requisitos y los componentes correspondientes que se van a crear para cada área.

Subred de pruebas

La [subred de pruebas](#) es la parte más importante de la infraestructura de replicación. Aquí es donde se lanzarán todos los [servidores de replicación](#) de Application Migration Service y contiene las direcciones IP a las que se dirigirá el tráfico de replicación. Para la replicación de datos privados entrantes, configure los [ajustes del servidor de replicación](#) para Application Migration Service con la opción [Usar IP privada](#).

Para [los requisitos de salida](#), puede utilizar la opción [Crear IP pública](#) para elegir si los servidores de replicación se comunicarán con los AWS servicios necesarios (Amazon S3, Application Migration Service, Amazon EC2) a través de una IP privada o pública. Las opciones estándar para proporcionar conectividad a Internet de salida se enumeran en la [documentación de Application Migration Service](#): una dirección IP pública con una puerta de enlace de Internet o una dirección IP privada con una puerta de enlace de NAT. Ambas opciones le permiten implementar un escenario híbrido simplificado en el que el tráfico de replicación de datos pasa por una conexión privada (Site-to-Site VPN o AWS Direct Connect) mientras los servidores de replicación se comunican con los AWS servicios a través de la red pública.

Sin embargo, la conectividad de salida pública suele estar prohibida en entornos corporativos cerrados, y este es el escenario más restrictivo que se analiza en la siguiente sección. En este caso, debe usar AWS PrivateLink y configurar los siguientes puntos finales de VPC en las subredes de almacenamiento provisional de los servidores de replicación:

- Punto de conexión de la puerta de enlace de VPC para comunicarse con Amazon S3
- Puntos de conexión de la interfaz de VPC para comunicarse con Application Migration Service y Amazon EC2

Para obtener más información sobre los puntos de conexión de VPC, consulte la documentación de [AWS PrivateLink](#).

Subred de origen

La subred de origen es cualquier subred desde la que realiza la replicación. Aquí es donde se encuentran [los servidores de origen](#) y donde instalará el agente de AWS replicación en estos servidores. Los [requisitos de red](#) de un agente son los siguientes:

- Comunicación a través HTTPS/TCP del puerto 443 Servicios de AWS con Amazon S3 y Application Migration Service
- Comunicación con la dirección IP del servidor de replicación (privada o pública, según la configuración)

El agente también admite escenarios híbridos en los que la comunicación Servicios de AWS puede realizarse a través de la red pública (mediante el tráfico HTTPS estándar), mientras que los datos de replicación se envían a través de redes privadas a la IP privada del servidor de replicación.

Esta guía se centra en un escenario más restrictivo, en el que ni siquiera se permite el tráfico HTTPS a Servicios de AWS desde los sistemas de origen, por lo que los siguientes puntos de conexión están configurados en la subred de pruebas:

- Puntos de conexión de interfaz de VPC para Application Migration Service y Amazon S3 (punto de conexión de interfaz regional, no el punto de conexión de puerta de enlace que se necesita para los servidores de replicación)
- Un [punto de conexión de resolución de DNS entrante](#), para permitir que los orígenes en las instalaciones y los servidores DNS resuelvan las direcciones IP privadas de los puntos de conexión de VPC, ubicados en la subred de pruebas

Subred de destino

La subred de destino es cualquier subred en la que planea lanzar los servidores, incluidas las instancias de prueba y de transición. Estas subredes no requieren conectividad de red en absoluto y podrían estar ubicadas en cualquier otra VPC de la Cuenta de AWS misma región. Esto se debe a que Application Migration Service utiliza las API de Amazon EC2 para crear nuevas instancias de prueba o transición (por lo que los servidores de replicación de la subred de pruebas requieren conectividad HTTPS de salida con Amazon EC2) y accede a las instantáneas regionales de S3 creadas a partir de volúmenes de EBS replicados. Ninguna de estas operaciones necesita acceso

directo a la red desde o hacia la subred de destino, por lo que incluso podría tratarse de una subred privada completamente aislada.

Sin embargo, Application Migration Service también [instala automáticamente](#) varias herramientas, como EC2 Config o AWS Systems Manager Agents (SSM Agents), en las instancias de destino, y estas actividades requieren la conectividad del HTTPS/TCP puerto 443 de salida desde las instancias y subredes de destino.

Prácticas recomendadas de configuración

En esta sección se proporciona una descripción detallada del escenario más restrictivo, en el que toda la comunicación se produce únicamente a través del canal privado, e incluye una explicación detallada de los requisitos y los componentes correspondientes que se van a crear para cada área.

En esta sección se describe la configuración para el escenario más restrictivo (la replicación únicamente a través de redes privadas), tal como se muestra en el [primer diagrama](#), según las consideraciones expuestas anteriormente. Puede configurar ambos escenarios híbridos omitiendo partes de la configuración más restrictiva:

- Para el escenario híbrido que admite la salida HTTPS pública en el origen y los recursos del área de pruebas privada, no se necesita el punto de conexión de VPC de la interfaz de Amazon S3.
- Para el escenario híbrido que admite la salida HTTPS pública en el origen y los recursos del área de pruebas privada, no se necesita ningún punto de conexión de VPC en la subred del área de pruebas.

En las siguientes secciones se presupone que ya ha completado la configuración inicial de Application Migration Service, tal como se describe en las entradas en el blog [Accelerate your Migration with AWS Application Migration Service](#) y [How to Use the New AWS Application Migration Service for Lift-and-Shift Migrations](#)). Este análisis se centra en los componentes que son específicos del escenario restrictivo y se presupone que hay una subred de pruebas privada que no tiene conectividad a Internet.

Configuraciones de subredes y enrutamiento

Para el escenario restrictivo, debe configurar los recursos de AWS necesarios en la subred privada de una VPC de pruebas. Esta subred no tiene conectividad a Internet (no hay ninguna puerta de enlace de Internet conectada a la tabla de enrutamiento como ruta predeterminada). En su lugar, utiliza una puerta de enlace virtual asociada a una puerta de enlace de [AWS Site-to-Site VPN](#) (conectada a través de un túnel IPsec a una puerta de enlace en las instalaciones) o está conectada a una puerta de enlace de transferencia o a servicios de Direct Connect para proporcionar interconectividad privada a los centros de datos en las instalaciones.

Utilizará esa subred privada como subred de pruebas para los recursos relacionados con la replicación administrados por Application Migration Service y configurará todo el acceso a la red

necesario a través de esta subred mediante puntos de conexión de VPC, como se explica en la siguiente sección.

Configuración de puntos de conexión de VPC

Ahora tiene que crear puntos de conexión de VPC en la subred de pruebas para proporcionar conectividad a los servidores de replicación y a los agentes de Application Migration Service desde las subredes en las instalaciones.

Esta es una lista completa de los puntos de conexión de VPC que necesita:

- Los puntos de conexión de interfaz de Application Migration Service y Amazon EC2, que proporcionan sus propias interfaces de red elásticas con direcciones IP privadas y nombres de DNS privados para que los utilicen tanto los servidores de replicación como los agentes. (Los agentes utilizarán únicamente el punto de conexión de Application Migration Service).
- Punto de conexión de puerta de enlace de Amazon S3 que proporciona una ruta específica en la tabla de enrutamiento de la subred (mediante una lista de prefijos). Lo utilizarán los servidores de replicación.
- Punto de conexión de interfaz de Amazon S3 que proporciona una interfaz de red elástica específica con una dirección IP privada dedicada en la subred privada. Los agentes de Application Migration Service utilizarán esta dirección a través de un nombre de DNS específico.

En las siguientes secciones se explica con más detalle el funcionamiento de los puntos de conexión de VPC. En la siguiente tabla se enumeran todos los puntos de conexión creados para la subred privada de pruebas. (Tenga en cuenta que el punto de conexión de la puerta de enlace de Amazon S3 no tiene ninguna interfaz de red aprovisionada, pero tiene listas de prefijos específicas aprovisionadas en la tabla de enrutamiento de la subred, como se describirá más adelante en esta guía).

Servicio de AWS	VPC endpoint type	Private DNS	Related subnet
Amazon EC2	Interfaz	Habilitado	Subred privada de pruebas
Application Migration Service	Interfaz	Habilitado	Subred privada de pruebas

Servicio de AWS	VPC endpoint type	Private DNS	Related subnet
Amazon S3	Interfaz	No disponible	Subred privada de pruebas
Amazon S3	Puerta de enlace	No disponible	Conexión a la tabla de enrutamiento de la subred privada de pruebas

Puede crear puntos de conexión de VPC opcionales para permitir el acceso a las instancias de EC2 en subredes privadas aisladas a través de AWS Systems Manager, tal como se explica en [Creación de puntos de conexión de VPC](#) en la documentación de Systems Manager.

Servicio de AWS	VPC endpoint type	Private DNS	Related subnet
Systems Manager	Interfaz	Habilitado	Subred privada de pruebas
ssmmessages	Interfaz	Habilitado	Subred privada de pruebas
ec2messages	Interfaz	Habilitado	Subred privada de pruebas
AWS Key Management Service (AWS KMS)	Interfaz	Habilitado	Subred privada de pruebas
Registros	Interfaz	Habilitado	Subred privada de pruebas

Puntos de enlace de interfaz de VPC

Al crear un punto de conexión de interfaz, también se crea una interfaz de red elástica específica para cada subred para la que se aprovisiona el punto de conexión de interfaz en cuestión. Por ejemplo, el punto de conexión de interfaz de Application Migration Service se aprovisiona en una

subred privada de la VPC de pruebas con una interfaz de red elástica que está asociada a la dirección IP de esa subred y también tiene tres nombres de DNS que se pueden resolver desde la subred a esta dirección IP:

- Un nombre de DNS privado, `mgn.<region>.amazonaws.com`
- Dos nombres de DNS basados en el ID del punto de conexión (`vpce-xxx`), con y sin la región incluida en el nombre: `vpce-xxx-<region>.<service-name>` y `vpce-xxx.<service-name>`

Esto permite que todas las instancias que se ejecuten en la subred y que utilicen la configuración predeterminada del [conjunto de opciones del protocolo de configuración dinámica de host \(DHCP\)](#) en la VPC y que tenga los [atributos de DNS](#) `enableDnsHostnames` y `enableDnsSupport` habilitados pueda hacer lo siguiente:

- Resolver el nombre de DNS de Application Migration Service (`mgn.<region>.amazonaws.com`) en una dirección IP privada asignada a la interfaz de red elástica.
- Conectarse a Application Migration Service únicamente a través de la red local.

Esto corrige la conectividad de cualquier instancia que se ejecute en la subred de pruebas (como el servidor de replicación o el servidor de conversión de Application Migration Service) de cualquier Servicio de AWS que tenga puntos de conexión de interfaz aprovisionados en la subred (como Amazon EC2, Application Migration Service, Systems Manager, AWS KMS, etc.).

Puntos de conexión de puertas de enlace de VPC

En el caso de los servicios como Amazon S3, no se puede aprovisionar ningún nombre de DNS fijo porque cada bucket tiene su propio nombre de DNS. Para este escenario, utilizará puntos de conexión de puerta de enlace de VPC.

Al crear un punto de conexión de puerta de enlace de Amazon S3, también se crea un objeto de lista de prefijos específico con una lista de destinos de subred (en notación CIDR), que se puede agregar a la tabla de enrutamiento de subred. Por lo tanto, se podría acceder a los nombres de DNS de los buckets de S3 resueltos en las direcciones IP incluidas en esta lista a través de la conectividad interna.

Al aprovisionar un punto de conexión de puerta de enlace de Amazon S3, puede especificar las subredes en las tablas de enrutamiento que deben incluir ese ID de lista de prefijos (`PL-<id>`). La

tabla de enrutamiento resultante para la subred privada de pruebas debe incluir ese ID de la lista de prefijos, como en esta tabla de enrutamiento de ejemplo:

Destination	Target
<code>pl-<id></code>	<code>vpce-<id-of-S3-Gateway-VPC-endpoint></code>
Cualquier otra ruta (por ejemplo, los CIDR de la subred de origen)	Cualquier destino, como los ID de las puertas de enlace virtuales
CIDR local	<code>"local"</code>

Puntos de conexión de entrada del solucionador de DNS

La configuración que se describe en la sección anterior es suficiente para las instancias que se ejecutan dentro de las subredes de AWS, porque ya están configuradas para usar servidores DNS internos de Amazon Route 53. Sin embargo, los servidores de origen en las instalaciones requieren pasos adicionales para poder comunicarse con Servicios de AWS de forma privada. En concreto, el agente de Application Migration Service debe descargar el instalador de Amazon S3 y, a continuación, comunicarse con Application Migration Service mediante los nombres de DNS que se proporcionan en la [documentación](#). Los servidores en las instalaciones utilizan sus servidores DNS predeterminados para resolver estos nombres de DNS, lo que da como resultado direcciones IP públicas. Los firewalls corporativos bloquean finalmente las comunicaciones con estas direcciones a través del puerto HTTPS/TCP 443.

Para evitarlo, debe configurar los servidores de origen o sus servidores DNS predeterminados para utilizar [Amazon Route 53 Resolver](#) en la resolución de estos nombres de DNS específicos o de una zona de subdominio (es decir, toda la zona `*.<region>.amazonaws.com`). Esto se puede configurar mediante la creación de un [punto de conexión de entrada de Route 53 Resolver](#) que, como un punto de conexión de interfaz de VPC, tiene una interfaz de red elástica dedicada creada en la subred privada dedicada de AWS y, por lo tanto, puede reenviar las solicitudes de DNS a Amazon Route 53 Resolver.

Grupos de seguridad para la interfaz de red elástica

Cada interfaz de red elástica tiene un grupo de seguridad dedicado asociado, que debe permitir el tráfico esperado para esta interfaz de red elástica y el punto de conexión correspondiente. Por lo tanto, el grupo de seguridad del punto de conexión del solucionador de DNS debe permitir el puerto UDP 53 entrante (y, a veces, el puerto TCP 53) para las solicitudes de DNS, y los grupos de seguridad del punto de conexión para la mayoría de los demás servicios (Application Migration Service, Amazon EC2, Systems Manager, etc.) necesitan que esté habilitado el puerto HTTPS/TCP 443 de entrada.

Instalación del agente de Application Migration Service en los servidores de origen

Para instalar el agente de Application Migration Service en los servidores de origen, debe proporcionar los nombres de DNS de Application Migration Service y los puntos de conexión de la interfaz de Amazon S3 a los parámetros de la línea de comandos del agente (consulte [Installing the Agent on a secured network](#) en la documentación de Application Migration Service).

Para el punto de conexión de Application Migration Service, puede usar cualquiera de los nombres DNS asociados (un campo DNS privado [mgn.<region>.amazonaws.com] o un nombre DNS específico de VPC [vpce-<VPC-id>-<suffix>.mgn.<region>.vpce.amazonaws.com]) y proporcionar un argumento: `--endpoint <FQDN>`. De hecho, si omite este argumento, el agente utilizará la Región de AWS especificada para volver a crear el FQDN de DNS predeterminado (mgn.<region>.amazonaws.com) y lo utilizará para acceder al plano de control de Application Migration Service. En la mayoría de los casos, ese comportamiento predeterminado debería ser suficiente, siempre que el FQDN se resuelva correctamente desde el servidor de origen en la dirección IP privada de la interfaz de red elástica del punto de conexión de VPC de Application Migration Service creado en la subred de pruebas.

El punto de conexión de interfaz de Amazon S3 no tendrá un único nombre de DNS privado (ya que cada bucket de S3 tendrá el suyo propio), por lo que esa opción no se admite. Sin embargo, un punto de conexión de interfaz de Amazon S3 todavía tiene asociada una interfaz de red elástica. También tiene una IP privada específica y nombres de DNS comodín (en el formato .vpce-<VPC-ID>-<suffix>.s3.<region>.vpce.amazonaws.com o vpce-<VPC-ID>-<suffix>-<region>.s3.<region>.vpce.amazonaws.com específico de la región) que se pueden resolver en esta IP privada.

Ese nombre de DNS comodín se puede utilizar para el argumento `--s3-endpoint`, como se muestra a continuación:

```
aws-replication-installer-init.py --region <region> --aws-access-key-id  
<MGN_IAM_ACCESS_KEY> --aws-secret-access-key <MGN_IAM_SECRET> --no-prompt \  
  --endpoint vpce-<VPC-id>-<suffix>.mgn.<region>.vpce.amazonaws.com --s3-endpoint  
  vpce-<VPC-ID>-<suffix>-<region>.s3.<region>.vpce.amazonaws.com
```

En la siguiente sección se proporciona un ejemplo de cómo configurar Application Migration Service, incluidos todos los puntos de conexión de VPC necesarios, y cómo implementar los agentes mediante puntos de conexión de VPC en servidores de origen de Windows y Linux. En la sección se tratan tanto la implementación manual como la automatizada.

Implementación del entorno de PoC

Muchos usuarios prefieren probar con antelación todos los canales de comunicación y los pasos de migración de forma exhaustiva. Probar la migración desde redes aisladas puede suponer un reto.

Para abordar esa necesidad, AWS ofrece dos opciones:

- Una [plantilla de CloudFormation](#) que prepara todos los recursos necesarios en AWS. La plantilla crea un entorno de prueba de concepto (PoC) que emula los componentes del entorno del centro de datos y configura la infraestructura de AWS. Incluye VPC de origen y destino aisladas, subredes y puntos de conexión de VPC.
- Un taller dedicado ([Migrate the Well-Architected Way](#)) con instrucciones detalladas paso a paso para crear su entorno de pruebas (consulte el paso [Create VPC Endpoints](#)).

Como alternativa, puede implementar el entorno de PoC siguiendo los pasos que se indican en las secciones siguientes.

Implementación manual

En la siguiente lista se indican los pasos principales para las implementaciones manuales en su entorno. Para obtener más información, consulte el patrón de Recomendaciones de AWS [Connect to Application Migration Service data and control planes over a private network](#).

1. Cree la VPC de origen y la VPC del área de pruebas con una subred privada.
2. Cree los siguientes puntos de conexión de VPC en la subred del área de pruebas:
 - Application Migration Service, y habilite el nombre de DNS privado (compartido por el servidor de replicación y el servidor de origen).
 - Amazon EC2, y habilite el nombre de DNS privado (compartido por el servidor de replicación y el servidor de origen).
 - Amazon S3 (no es compatible con el nombre de DNS privado). Los puntos de conexión de interfaz son compatibles con Direct Connect, Site-to-Site VPN y el emparejamiento de VPC. Por lo tanto, esto únicamente es necesario para que los servidores de origen (que podrían estar en las instalaciones) se conecten al plano de control de Application Migration Service a través de una red privada.

Note

Los puntos de conexión ssm y ssmmessages son opcionales y se han creado actualmente para conectar el servidor de origen a través del Administrador de sesiones de SSM.

- Punto de conexión de la puerta de enlace de Amazon S3 en la subred del área de pruebas. El servidor de replicación lo necesita para conectarse a Amazon S3. Debe actualizar las rutas de la subred del área de pruebas.
3. Cree un punto de conexión del solucionador de entrada en la VPC del área de pruebas para permitir la resolución del registro DNS privado (para los puntos de conexión de interfaz de VPC) desde la VPC de origen.
 4. Actualice las opciones de DHCP de la VPC de origen con el punto de conexión del solucionador de entrada de la VPC del área de pruebas como IP del servidor DNS.
 5. Habilite el emparejamiento entre las VPC de origen y de pruebas y actualice ambas tablas de enrutamiento de VPC.
 6. Cree un grupo de seguridad en las VPC de origen y de pruebas para permitir los siguientes puertos.

Source	Destination	Port	Description
Su centro de datos de origen	La URL del servicio Amazon S3	443 (TCP)	Comunicación a través del puerto TCP 443
Su centro de datos de origen	Dirección de consola específica de la Región de AWS de Application Migration Service	443 (TCP)	Comunicación entre los servidores de origen y el Servicio de migración de aplicaciones a través del puerto TCP 443
Su centro de datos de origen	Subred de área de almacenamiento	1500 (TCP)	Comunicación entre los servidores de origen y la subred del

Source	Destination	Port	Description
			área de almacenamiento a través del puerto TCP 1500
Subred de área de almacenamiento	Dirección de consola específica de la Región de AWS de Application Migration Service	443 (TCP)	Comunicación entre la subred del área de ensayo y el Servicio de migración de aplicaciones a través del puerto TCP 443
Subred de área de almacenamiento	La URL del servicio Amazon S3	443 (TCP)	Comunicación a través del puerto TCP 443
Subred de área de almacenamiento	Punto de conexión de Amazon EC2 de su Región de AWS	443 (TCP)	Comunicación a través del puerto TCP 443

7. Inicie Application Migration Service en la Región de AWS del área de pruebas. Para ello, actualice los detalles de la subred del área de pruebas y habilite la comunicación a través de una IP privada.
8. Cree un rol de AWS Identity and Access Management (IAM) para instalar el agente de Application Migration Service. Asocie políticas administradas y genere claves de acceso y una clave de secretos.
9. Cree un perfil de IAM para conectar Amazon EC2 a través del Administrador de sesiones de SSM.
10. Instale un agente en las máquinas de origen.

Automatización de las implementaciones del agente con Cloud Migration Factory

[Cloud Migration Factory en AWS](#) automatiza la implementación del agente de Application Migration Service en el escenario de las redes privadas, con parámetros adicionales de la línea de comandos.

Al implementar esta solución (consulte las opciones de [implementación automatizada](#)), puede usar estos scripts y una de las siguientes opciones:

- Ejecute estos [scripts](#) manualmente desde la línea de comandos, tal y como se describe en la sección [Run automations from command prompt](#) de la [Guía de implementación de Cloud Migration Factory](#).
- Agregue los [scripts](#) a Migration Factory según las instrucciones de la sección [Scripts management](#) para lograr una integración completa con Cloud Migration Factory.

Estos scripts automatizan lo siguiente:

- Instalación del agente de Application Migration Service en un servidor Windows mediante puntos de conexión privados
- Instalación del agente de Application Migration Service en servidores Linux mediante puntos de conexión privados

Supervisión y solución de problemas

Puede supervisar el Servicio de migración de aplicaciones mediante [Amazon CloudWatch](#), [Amazon EventBridge](#) [AWS CloudTrail](#), que recopilan datos sin procesar y los procesan en near-real-time métricas legibles. Para obtener más información, consulte [Supervisión del servicio de migración de aplicaciones](#) en la AWS documentación.

Si tiene algún problema y desea inicializar nuevas instancias de prueba o transición, puede revertir la acción de prueba o transición. Esto revertirá el estado del ciclo de vida de los servidores de origen a la etapa anterior, lo que indicará que estos servidores no se han sometido a ninguna transición. Durante una reversión, también tendrá la opción de eliminar las instancias de prueba o de transición para ahorrar costos. Para obtener más información, consulte [Troubleshooting](#) en la documentación de Application Migration Service.

Cuando se haya instalado el agente, el servidor de origen aparecerá en la consola de Application Migration Service y podrá consultar los detalles del servidor para comprobar el progreso de la replicación.

Pruebas de conectividad y resolución de nombres desde el servidor de origen

Inicie sesión en el servidor de origen mediante el protocolo de escritorio remoto (RDP) de Windows, Secure Shell (SSH) o el Administrador de AWS sesiones y pruebe lo siguiente:

- Conectividad a través de HTTPS en el puerto TCP 443 con el punto de conexión de Application Migration Service.
 - En Windows (en PowerShell):

```
Test-NetConnection -ComputerName mgn.<aws_region>.amazonaws.com -Port 443
```

- En Linux o Windows (cmd):

```
Telnet mgn.<aws_region>.amazonaws.com 443
```

- Conectividad a través de HTTPS en el puerto TCP 443 con el punto de conexión de Amazon S3.
 - En Windows (en PowerShell):

```
Test-NetConnection -ComputerName <s3_endpoint_name> -Port 443
```

- En Linux o Windows (cmd):

```
Telnet <s3_endpoint_name> 443
```

- Conectividad del puerto TCP 1500 con la IP del servidor de replicación:
 - En Windows (en PowerShell):

```
Test-NetConnection -ComputerName <Replication_Server_Private_IP> -Port 1500
```

- En Linux o Windows (cmd):

```
Telnet <Replication_Server_Private_IP> 1500
```

Además, asegúrese de que los puntos de enlace de la API de Amazon EC2 y Application Migration Service se conviertan en privados IPs mediante los siguientes comandos. (Puede usar los mismos comandos en Windows y en Linux.)

- nslookup ec2.<aws_region>.amazonaws.com
- nslookup mgn.<aws_region>.amazonaws.com

Pruebas de conectividad y resolución de nombres desde la red del área de pruebas

Para probar la conectividad desde el área de pruebas, inicialice una instancia de EC2 temporal en la subred de pruebas y pruebe lo siguiente:

- Conectividad a través de HTTPS en el puerto TCP 443 con el punto de conexión de Application Migration Service.
 - En Windows (en PowerShell):

```
Test-NetConnection -ComputerName mgn.<aws_region>.amazonaws.com -Port 443
```

- En Linux o Windows (cmd):

```
Telnet mgn.<aws_region>.amazonaws.com 443
```

- Conectividad a través de HTTPS en el puerto TCP 443 con el punto de conexión de Amazon EC2.
- En Windows (en PowerShell):

```
Test-NetConnection -ComputerName ec2.<aws_region>.amazonaws.com -Port 443
```

- En Linux o Windows (cmd):

```
Telnet ec2.<aws_region>.amazonaws.com 443
```

Si la inicialización de la replicación se detiene en el paso “Descarga del software de replicación” después de instalar el agente en el servidor de origen, compruebe lo siguiente.

- Resolución de nombres:

```
nslookup s3.<aws_region>.amazonaws.com
```

Note

El punto de conexión de Amazon S3 se resolverá en una IP pública, pero se conectará de forma privada a través del punto de conexión de la puerta de enlace de Amazon S3.

- Conectividad a través del protocolo HTTPS en el puerto TCP/443.
- En Windows:

```
Test-NetConnection -ComputerName s3.<aws_region>.amazonaws.com -Port 443
```

- En Linux:

```
Telnet s3.<aws_region>.amazonaws.com 443
```

Conclusión

En esta guía se describen los requisitos y se proporciona un ejemplo de configuración para utilizar Application Migration Service a fin de migrar mediante lift-and-shift servidores desde redes en las instalaciones seguras a AWS a través de una conectividad privada (Site-to-Site VPN o Direct Connect). Este es un escenario típico de muchas migraciones corporativas. En la guía también se proporciona orientación sobre formas de realizar pruebas mediante la implementación automática o manual, y sobre la supervisión y la solución de problemas de conectividad en caso de que surjan.

Recursos

Publicaciones de blog

- [Accelerate your Migration with AWS Application Migration Service](#)
- [How to Use the New AWS Application Migration Service for Lift-and-Shift Migrations](#)

Guías y patrones

- [Connect to AWS MGN data and control planes over a private network](#)
- [AWS large-migration strategy and best practices](#)
- [Automatizar las migraciones de servidores a gran escala con Cloud Migration Factory](#)

Soluciones

- [Coordinate and automate large scale migrations to the Nube de AWS using the Cloud Migration Factory on AWS solution](#)

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 marzo de 2023

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: Migrar la base de datos de Oracle en las instalaciones a Amazon Aurora PostgreSQL-Compatible Edition.
- **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: Migrar la base de datos Oracle en las instalaciones a Amazon Relational Database Service (Amazon RDS) para Oracle en la nube de 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: Migrar el sistema de administración de las 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: Migrar la base de datos de Oracle en las instalaciones a Oracle en una instancia de EC2 en la 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 en las instalaciones 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 administrados](#).

ACID

Consulte [atomicidad, consistencia, aislamiento, 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 una [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 de origen gestiona las transacciones de las aplicaciones conectadas, mientras los datos se replican en la de destino. La base de datos de destino no acepta ninguna transacción durante la migración.

función de agregación

Función SQL que actúa en un grupo de filas y calcula un único valor de devolución para el grupo. Entre los ejemplos de funciones de agregación se incluyen SUM y MAX.

IA

Consulte [inteligencia artificial](#).

AIOps

Consulte [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.

antipatronos

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

Enfoque de seguridad que permite usar de manera exclusiva 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

bot malicioso

[Bot](#) destinado a causar interrupciones o daños a personas u organizaciones.

BCP

Consulte [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. Consulte también [endianidad](#).

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

Estrategia de implementación 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 se ejecuta en el otro entorno (verde). Esta estrategia lo ayuda a hacer reversiones rápidas con un impacto mínimo.

bot

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 la información de Internet. Otros bots, conocidos como bots maliciosos, tienen como objetivo causar interrupciones o daños a personas u organizaciones.

botnet

Redes de [bots](#) infectadas por [malware](#) y que están bajo el control de una sola parte, conocida como pastor de bots 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 de emergencia

En circunstancias excepcionales y mediante un proceso aprobado, es una forma rápida de que un usuario pueda acceder a un Cuenta de AWS sitio al que normalmente no tiene permisos de acceso. Para más información, consulte el indicador [Implement break-glass procedures](#) en la guía de AWS Well-Architected.

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 [AWS Cloud Adoption Framework](#).

implementación canario

Lanzamiento lento e incremental de una versión para los usuarios finales. Cuando tenga mayor confianza en la nueva versión, la implementa y reemplaza la versión actual en su totalidad.

CCoE

Consulte [Centro de excelencia en la nube](#).

CDC

Consulte [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

Introducción intencionada de 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 [integración continua y 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 CCoE](#) 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 relacionada con la tecnología de [computación de periferia](#).

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 siguientes son las cuatro fases por las que suelen pasar las empresas cuando migran a la 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 CCoE, establecer un modelo de operaciones)

- Migración: migración de aplicaciones individuales
- Reinención: 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 [base de datos de administración de 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. Algunos repositorios en la nube comunes son GitHub o Bitbucket 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 machine learning para analizar y extraer información de formatos visuales, como imágenes y videos digitales. Por ejemplo, Amazon SageMaker AI proporciona algoritmos de procesamiento de imágenes para CV.

deriva de configuración

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

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

Un conjunto de AWS Config reglas y medidas correctivas que puede reunir para personalizar sus controles 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

Consulte [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](#).

deriva 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 deriva de 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

Marco de arquitectura que proporciona una propiedad de datos distribuida y descentralizada con una administración y una gobernanza centralizadas.

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

Sistema de administración de datos que respalda la inteligencia empresarial, como los análisis. Los almacenes de datos suelen contener grandes cantidades de datos históricos y, por lo general, se utilizan para las consultas y los 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 [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 en 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 suelen utilizar para restringir consultas, filtrarlas y etiquetar los 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)

Estrategia y proceso que utiliza para minimizar el tiempo de inactividad y la pérdida de datos a causa de 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 [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 con línea de base. 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 [asignación de flujos de valor para el desarrollo](#).

E

EDA

Consulte [análisis de datos de tipo exploratorio](#).

EDI

Consulte [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 la nube](#), la computación de periferia puede reducir la latencia de la comunicación y mejorar el tiempo de respuesta.

intercambio electrónico de datos (EDI)

Intercambio automatizado de documentos comerciales entre organizaciones. Para más información, consulte [¿Qué es el intercambio electrónico de datos?](#)

cifrado

Proceso de computación que transforma datos de texto plano, que son 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 [punto de conexión de 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 otras Cuentas de AWS o a responsables AWS Identity and Access Management (de 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)

Sistema que automatiza y administra los procesos empresariales clave (como la contabilidad, [MES](#) y la administración 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](#).

ERP

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 hechos

Tabla central de un [esquema en estrella](#). Almacena datos cuantitativos sobre operaciones empresariales. Por lo general, 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.

Fail Fast

Filosofía que utiliza pruebas frecuentes e incrementales para reducir el ciclo de vida del desarrollo. Es una parte fundamental de los enfoques ágiles.

límite de aislamiento de errores

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 más información, consulte [AWS Fault Isolation Boundaries](#).

rama de característica

Consulte [rama](#).

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.

peticiones con pocos pasos

Proporcionar a un [LLM](#) una pequeña cantidad de ejemplos que demuestren la tarea y el resultado deseado antes de pedirle que lleve a cabo una tarea similar. Esta técnica es una aplicación del aprendizaje contextual, mediante el que los modelos aprenden a partir de ejemplos (pasos) incrustados en las peticiones. La técnica de peticiones con pocos pasos puede ser eficaz para las tareas que requieren un formato, un razonamiento o un conocimiento del dominio específicos. Consulte también [peticiones desde cero](#).

FGAC

Consulte [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 de cambio](#) 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 [modelo fundacional](#).

Modelo fundacional (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 más información, consulte [¿Qué son los modelos fundacionales?](#)

G

IA generativa

Subconjunto de modelos de [IA](#) que se entrenaron con grandes cantidades de datos y que pueden utilizar una simple petición de texto para crear contenido y artefactos nuevos, como imágenes, videos, texto y audio. Para más información, consulte [¿Qué es la IA generativa?](#)

bloqueo geográfico

Consulte [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, mientras que el [flujo de trabajo basado en enlaces troncales](#) es el enfoque moderno preferido.

imagen dorada

Instantánea de un sistema o software que se usa 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 CSPM GuardDuty AWS Trusted Advisor, Amazon Inspector y AWS Lambda cheques personalizados.

H

HA

Consulte [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 de reserva

Parte de los datos históricos etiquetados que se ocultan de un conjunto de datos que se utiliza para entrenar un modelo de [machine learning](#). Puede utilizar los datos de reserva para evaluar el rendimiento del modelo mediante la comparación de 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, una revisión suele realizarse fuera del flujo de trabajo de DevOps publicación típico.

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

Consulte [infraestructura como código](#).

políticas basadas en identidades

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

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

Modelo que implementa una nueva infraestructura para las cargas de trabajo de producción en lugar de actualizar o modificar la infraestructura existente o aplicarle revisiones. Las infraestructuras inmutables son de manera intrínseca más coherentes, fiables y predecibles que las [infraestructuras mutables](#). Para más información, consulte la práctica recomendada [Implementación mediante una infraestructura inmutable](#) en el Marco de AWS Well-Architected.

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

Término que introdujo [Klaus Schwab](#) en 2016 para referirse a la modernización de los procesos de fabricación mediante los avances en la conectividad, los datos en tiempo real, la automatización, el análisis, la IA y el ML.

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 (IIoT)

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 [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 de gran tamaño (LLM)

Modelo de [IA](#) de aprendizaje profundo que se entrenó previamente con una gran cantidad de datos. Un LLM puede llevar a cabo varias 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 [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

Consulte [Las 7 R](#).

sistema little-endian

Un sistema que almacena primero el byte menos significativo. Consulte también [endianidad](#).

LLM

Consulte [modelo de lenguaje de gran tamaño](#).

entornos inferiores

Consulte [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

Consulte [rama](#).

malware

Software diseñado para comprometer la seguridad o la privacidad de la computadora. El malware podría 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 administrados

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

sistema de ejecución de fabricación (MES)

Sistema de software para seguir, supervisar, documentar y controlar los procesos de producción que convierten las materias primas en productos acabados en la zona de producción.

MAP

Consulte [Programa de aceleración de la migración](#).

mecanismo

Proceso completo mediante el que se crea una herramienta, se impulsa su adopción y, a continuación, se inspeccionan los resultados para hacer ajustes. Un mecanismo es un ciclo que se refuerza y mejora por 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 [sistema de ejecución de fabricación](#).

Message Queuing Telemetry Transport (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: rehospede la migración a Amazon EC2 AWS con Application Migration Service.

Migration Portfolio Assessment (MPA)

Herramienta en línea que proporciona información a fin de validar los argumentos comerciales necesarios para migrar a la 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 de los socios 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

Enfoque utilizado para migrar una carga de trabajo a la Nube de AWS. Para más información, consulte la entrada [Las 7 R](#) de este glosario y también [Mobilize your organization to accelerate large-scale migrations](#).

ML

Consulte [machine learning](#).

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 más información, consulte [Strategy for modernizing applications in the 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 más información, consulte [Evaluating modernization readiness for applications in the 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](#).

MPA

Consulte [Migration Portfolio Assessment](#).

MQTT

Consulte [Message Queuing Telemetry Transport](#).

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

Modelo que actualiza y modifica la infraestructura actual 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 [control de acceso de origen](#).

OAI

Consulte [identidad de acceso de origen](#).

OCM

Consulte [administración 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

Consulte [acuerdo de 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](#).

Open Process Communications: arquitectura unificada (OPC-UA)

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

Lista de comprobación de preguntas y prácticas recomendadas asociadas que son útiles para comprender, evaluar, prevenir o reducir el alcance de los incidentes y posibles errores. Para más información, consulte [Operational Readiness Reviews \(ORR\)](#) en el Marco de AWS Well-Architected.

tecnología operativa (TO)

Sistemas de hardware y software que funcionan con el entorno físico para controlar las operaciones, los equipos y la infraestructura industriales. En el sector de la fabricación, 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 y AWS CloudTrail que registra todos los eventos para todos los miembros Cuentas de AWS 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 de 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 [revisión de la preparación operativa](#).

OT

Consulte [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 [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 [administración del ciclo de vida del producto](#).

policy

Objeto que puede definir permisos (consulte [política basada en identidad](#)), especificar las condiciones de acceso (consulte [política basada en recursos](#)) o definir los permisos máximos para todas las cuentas de una organización de AWS Organizations (consulte [política de control de servicio](#)).

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.

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

Condición de consulta que devuelve true o false. En general, se encuentra en una cláusula WHERE.

inserción de predicados

Técnica de optimización de consultas en bases de datos que filtra los datos de la consulta antes de transferirlos. Esta técnica reduce la cantidad de datos de la base de datos relacional que se tienen que recuperar y procesar. Además, 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

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

[Control de seguridad](#) que se diseñó para evitar la implementación de recursos que no cumplan con la normativa. Estos controles analizan los recursos antes de aprovisionarlos. Si el recurso no cumple con los requisitos del control, no se aprovisiona. Para obtener más información, consulte la [guía de referencia de controles](#) en la AWS Control Tower documentación y consulte [Controles proactivos](#) en la sección Implementación de controles de seguridad en AWS.

administración del ciclo de vida del producto (PLM)

Administración 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 la reducción de su uso y su retirada.

entorno de producción

Consulte [entorno](#).

controlador lógico programable (PLC)

En el sector de la fabricación, computadora adaptable y altamente fiable que supervisa las máquinas y automatiza los procesos de fabricación.

encadenamiento de peticiones

Uso de la salida de una petición de [LLM](#) como entrada para la siguiente petición a fin de generar mejores respuestas. Esta técnica se utiliza para dividir una tarea compleja en tareas secundarias 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)

Patrón que permite establecer 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 pueden suscribir otros microservicios. El sistema puede agregar 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

Consulte [responsable, fiable, consultada e informada \(RACI\)](#).

RAG

Consulte [generación aumentada por recuperación](#).

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

Consulte [responsable, fiable, consultada e informada \(RACI\)](#).

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

Consulte [Las 7 R](#).

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

Consulte [Las 7 R](#).

Region

Conjunto de AWS recursos en un área geográfica. Cada uno Región de AWS está aislado e independiente de los demás para proporcionar tolerancia a las fallas, estabilidad y resiliencia. Para más información, consulte [Specify which Regions de AWS your account can use](#).

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 [Las 7 R](#).

versión

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

reubicar

Consulte [Las 7 R](#).

redefinir la plataforma

Consulte [Las 7 R](#).

recomprar

Consulte [Las 7 R](#).

resiliencia

Capacidad de una aplicación para resistir interrupciones o recuperarse de ellas. Al planificar la resiliencia en la Nube de AWS, la [alta disponibilidad](#) y la [recuperación ante desastres](#) son consideraciones comunes. Para más información, consulte [Resiliencia en la Nube de AWS](#).

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 [Las 7 R](#).

retirar

Consulte [Las 7 R](#).

Generación aumentada de recuperación (RAG)

Tecnología de [IA generativa](#) mediante la que un [LLM](#) hace referencia a un origen de datos autorizado que se encuentra fuera de sus orígenes de datos de entrenamiento antes de generar una respuesta. Por ejemplo, un modelo de RAG podría hacer una búsqueda semántica en la base de conocimientos o en los datos personalizados de una organización. Para más información, consulte [¿Qué es RAG \(generación aumentada por recuperación\)?](#)

rotación

Proceso mediante el que periódicamente se actualiza un [secreto](#) para que resulte más difícil que un atacante pueda acceder 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 [objetivo de punto de recuperación](#).

RTO

Consulte [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 en la Consola de administración de AWS 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 [control de supervisión y adquisición de datos](#).

SCP

Consulte [política de control de servicio](#).

secreta

En AWS Secrets Manager, información confidencial o restringida, como una contraseña o credenciales de usuario, que se almacena de forma cifrada. Se compone del valor del secreto y de sus metadatos. El valor del secreto puede ser binario, una sola cadena o varias cadenas. Para más información, consulte [What's in a Secrets Manager secret?](#) en la documentación de Secrets Manager.

seguridad desde el diseño

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 de controles de seguridad principales: [preventivos](#), [de detección](#), [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

Acción predefinida y programada que está diseñada para responder automáticamente a un evento de seguridad o corregirlo. Estas automatizaciones sirven como controles de seguridad [preventivos o adaptables](#) que le ayudan a implementar las mejores prácticas AWS de seguridad. La modificación de un grupo de seguridad de VPC, la aplicación de revisiones a una instancia de Amazon EC2 o la rotación de credenciales son algunos ejemplos de acciones de respuesta automatizadas.

cifrado del servidor

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

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 con AWS la que compartes la seguridad y 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 [sistema de administración de eventos e información de seguridad](#).

único punto de error (SPOF)

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

SLA

Consulte [acuerdo de nivel de servicio](#).

SLI

Consulte [indicador de nivel de servicio](#).

SLO

Consulte [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 más información, consulte [Phased approach to modernizing applications in the Nube de AWS](#).

SPOF

Consulte [único punto de error](#).

esquema en estrella

Estructura organizativa de una base de datos que utiliza una tabla de hechos de gran tamaño para almacenar datos transaccionales o medidos y una o varias tablas dimensionales más pequeñas para almacenar los atributos de los datos. Esta estructura está diseñada para utilizarse 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 dismantelar 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.

control de supervisión y adquisición de datos (SCADA)

En el sector de la fabricación, sistema que utiliza hardware y software para supervisar 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

Prueba de un sistema de manera que simule las interacciones de los usuarios para detectar posibles problemas o supervisar el rendimiento. Puede usar [Amazon CloudWatch Synthetics](#) para crear estas pruebas.

petición del sistema

Técnica para proporcionar contexto, instrucciones o pautas a un [LLM](#) para dirigir su comportamiento. Las peticiones 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 ayudar a administrar, identificar, organizar, buscar y filtrar recursos de . 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 redes con VPCs 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.

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

Consulte [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.

Emparejamiento de 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 hace un cálculo en un grupo de filas que se relacionan de alguna manera con el registro actual. Las funciones de ventana son útiles para las tareas de procesamiento, 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.

WORM

Consulte [escritura única y lectura múltiple](#).

WQF

Consulte [AWS Workload Qualification Framework](#).

escritura única y lectura múltiple (WORM)

Modelo de almacenamiento que escribe los datos una sola vez y evita que se eliminen o modifiquen. Los usuarios autorizados pueden leer los datos tantas veces como sea necesario, pero no los pueden cambiar. Esta infraestructura de almacenamiento de datos se considera [inmutable](#).

Z

ataque de día cero

Ataque, normalmente de malware, que se aprovecha de 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.

peticiones desde cero

Proporcionar a un [LLM](#) instrucciones para llevar a cabo una tarea, pero sin ejemplos (pasos) que puedan ayudar a guiarlo. El LLM debe usar los conocimientos del entrenamiento previo para llevar a cabo la tarea. La eficacia de la petición desde cero depende de la complejidad de la tarea y de la calidad de la petición. Consulte también [peticiones con 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 versión original de inglés, prevalecerá la versión en inglés.