



Migración de F5 BIG-IP a F5 BIG-IP VE en la nube AWS

AWS Guía prescriptiva



AWS Guía prescriptiva: Migración de F5 BIG-IP a F5 BIG-IP VE en la nube AWS

Copyright © 2024 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
Resultados empresariales específicos	2
Evaluación de los costos y las habilidades de migración	3
Evaluación de los costos de licencias e instancias	3
Evaluación de una base de conocimientos de AWS y F5	4
Mapeo de las aplicaciones y diseño de la arquitectura	6
Mapeo de las aplicaciones	6
Planificación de la arquitectura	11
Planificación de la migración	14
Decisión sobre qué migrar	14
Desescalada de las configuraciones	15
Elección de un tipo de instancia	17
Puntos clave de decisión	18
Descripción general de la migración	19
Migración de datos	22
Migración de una configuración completa	22
Migración de una configuración parcial	24
Implementaciones de alta densidad sin IP elásticas	25
Interconexión de las VPC	26
Conexión a la infraestructura de AWS	30
Recursos	34
Historial de documentos	35
Glosario	36
#	36
A	37
B	40
C	41
D	44
E	49
F	51
G	52
H	53
I	54
L	56

M	57
O	61
P	63
Q	66
R	66
S	69
T	72
U	74
V	75
W	75
Z	76
.....	lxxvii

Migración de F5 BIG-IP a F5 BIG-IP VE en la nube AWS

Amazon Web Services, Suresh Veeragoni (AWS)

Noviembre de 2020 ([historial de documentos](#))

Esta guía proporciona una descripción general de los pasos, la arquitectura, las herramientas y las consideraciones para migrar las soluciones de seguridad y administración del tráfico de F5 BIG-IP a la nube de Amazon Web Services (AWS). [F5 BIG-IP](#) es un conjunto de productos diseñados en torno a soluciones de disponibilidad, control de acceso y seguridad. Se ejecutan en el [sistema operativo de administración del tráfico \(TMOS\) de F5](#).

Sus soluciones de seguridad y administración del tráfico F5 BIG-IP se migran a AWS Cloud mediante las [estrategias de migración de realojamiento y redefinición de la plataforma](#) que forman parte de las siete estrategias de migración habituales (7 R). La carga de trabajo de F5 se migrará volviendo a alojar un entorno existente y utilizando aspectos de redefinición de la plataforma, como la detección de servicios y las integraciones de la API.

En esta guía se explican los cuatro pasos principales de la migración.

- [Evaluación de los costos y las habilidades de migración](#): comprender los costos de la migración y los conocimientos necesarios sobre AWS y sobre los productos y servicios de F5.
- [Mapeo de las aplicaciones y diseño de la arquitectura](#): evaluar cómo se integran sus aplicaciones y diseñar la arquitectura para el futuro entorno.
- [Planificación de la migración](#) : utilizar un plan general para su migración y tomar decisiones clave sobre qué cosas migrar.
- [Migración de datos](#): implementar las configuraciones disponibles para migrar las cargas de trabajo de F5 BIG-IP a AWS Cloud y migrar sus datos.

Para obtener una descripción completa de los pasos de migración, consulte el patrón [Migración de una carga de trabajo de F5 BIG-IP a F5 BIG-IP VE en AWS Cloud](#) en el sitio web de Recomendaciones de AWS.

Esta guía está destinada a los equipos de ingeniería técnica y arquitectura que están migrando las soluciones de seguridad y administración del tráfico de F5 a AWS Cloud.

Resultados empresariales específicos

Las organizaciones optan por migrar a AWS Cloud para aumentar su agilidad y resiliencia. Esta migración ofrece beneficios significativos, pero también conlleva riesgos que deben minimizarse. En concreto, el riesgo y la complejidad de la adopción de la nube aumentan cuando se dividen servicios de aplicaciones importantes, como la administración del tráfico o la seguridad.

Si migra las cargas de trabajo BIG-IP de F5 a AWS Cloud, podrá centrarse en la agilidad y adoptar modelos operativos de alto valor en toda la arquitectura empresarial. También generará un beneficio neto para su adopción de la nube, ya que sus entornos tecnológicos pueden federarse.

También puede crear una ventaja empresarial al limitar la proliferación de proveedores o herramientas. Esto reduce el riesgo al migrar una aplicación, ya que limita o elimina los cambios en la ruta de datos, las funciones, las herramientas y el modelo operativo del entorno de origen.

Evaluación de los costos y las habilidades de migración

Antes de decidir migrar sus soluciones de seguridad y administración del tráfico de F5 BIG-IP a la nube de AWS, debe evaluar los costos de la migración y las habilidades necesarias.

En las siguientes secciones se ofrece un resumen de los posibles costos de migración, así como una visión general de los conocimientos sobre AWS y sobre los productos y servicios de F5 que necesitará su equipo.

Temas

- [Evaluación de los costos de licencias e instancias](#)
- [Evaluación de una base de conocimientos de AWS y F5](#)

Evaluación de los costos de licencias e instancias

El costo de ejecutar las cargas de trabajo de F5 BIG-IP en la nube de AWS variará en función de los costos combinados de licencias e instancias. Cuando migre a la nube de AWS, tendrá que combinar sus licencias actuales y activar las funciones del sistema de origen en el sistema de destino.

Los productos de F5 tienen varios modelos de licencia, pero sus requisitos técnicos y empresariales suelen coincidir con los siguientes modelos: Traiga su propia licencia (BYOL), mercado, oferta privada, suscripción y acuerdos de licencia empresarial (ELA).

El costo de la migración también variará en función de si utiliza instancias de pago por uso, con un precio anual o si tiene un acuerdo individual con AWS. Es importante destacar que el costo de una licencia de F5 también puede cambiar en función del modelo y de sus requisitos individuales.

Puede utilizar la [calculadora de precios de AWS](#) para calcular sus posibles costos de ejecución. Los tres ejemplos siguientes proporcionan información sobre los costos de las instancias y la infraestructura de AWS.

- [F5 BIG-IP pequeño: 100 Mbps](#)
- [F5 BIG-IP medio: 200 Mbps](#)
- [F5 BIG-IP grande: 800 Mbps](#)

Evaluación de una base de conocimientos de AWS y F5

Antes de empezar a migrar su carga de trabajo de F5 BIG-IP, debe asegurarse de que su equipo conoce los siguientes productos y servicios de AWS y de F5.

Búsqueda de productos y servicios de AWS

- [AWS CloudFormation](#) le permite crear y aprovisionar implementaciones de infraestructura de AWS de forma predecible y uniforme.
- [Amazon CloudWatch](#) proporciona una solución de monitorización de confianza, escalable y flexible que podrá iniciar en cuestión de minutos.
- [Amazon Elastic Compute Cloud \(Amazon EC2\)](#) es un servicio web que proporciona una capacidad de computación redimensionable para que pueda crear y alojar sus sistemas de software.
- [\(IAM\) AWS Identity and Access Management](#) es un servicio web para controlar el acceso de forma segura a los servicios de AWS.
- [AWS Landing Zone](#) es una solución que ayuda a los clientes a configurar rápidamente un entorno de AWS seguro y con varias cuentas según las prácticas recomendadas de AWS.
- [Amazon Simple Storage Service \(Amazon S3\)](#) es un servicio de almacenamiento de objetos basado en la nube que lo ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.
- [\(AWS STS\) AWS Security Token Service](#) permite solicitar credenciales temporales con privilegios limitados para los usuarios.
- [AWS Transit Gateway](#) es un servicio escalable y de alta disponibilidad que permite consolidar la configuración de enrutamiento de Región de AWS Amazon VPC para una región con una arquitectura radial.
- [Amazon Virtual Private Cloud \(Amazon VPC\)](#) lo ayuda a lanzar recursos de AWS en una red virtual que haya definido.

Important

Su equipo debe comprender las diferentes formas de conectar una o varias nubes privadas virtuales (VPC) a los centros de datos existentes, así como la forma de crear recursos en su infraestructura de AWS. Para obtener más información sobre esto, consulte [Opciones de conectividad de red a Amazon VPC](#) en la documentación de Amazon VPC.

Productos y servicios de F5

- El [sistema operativo de administración del tráfico \(F5 TMOS\)](#) es la base de software de todos los productos de red o tráfico de F5.
- [Local Traffic Manager \(F5 LTM\)](#) le ayuda a controlar el tráfico de la red, seleccionando el destino correcto en función del rendimiento, la seguridad y la disponibilidad del servidor.
- [Global Traffic Manager \(F5 GTM\)](#) distribuye las solicitudes de DNS y de aplicaciones de usuario en función de las políticas empresariales, las condiciones del centro de datos y los servicios en la nube, la ubicación del usuario y el rendimiento de las aplicaciones.
- [Access Policy Manager \(F5 APM\)](#) protege, simplifica y centraliza el acceso a las aplicaciones, las API y los datos, sin importar dónde se encuentren los usuarios y sus aplicaciones.
- [Application Security Manager \(F5 ASM\)](#) es un firewall de aplicaciones web flexible que protege las aplicaciones web en entornos de nube tradicionales, virtuales y privados.
- [Advanced Firewall Manager \(F5 AFM\)](#) mitiga las amenazas de red antes de que interrumpan los recursos críticos del centro de datos.
- [F5 BIG-IQ](#) proporciona un punto de control central para los dispositivos físicos y virtuales de F5 y para las soluciones que se ejecutan en ellos.

Mapeo de las aplicaciones y diseño de la arquitectura

Las siguientes secciones le ayudan a entender cómo se integran sus aplicaciones en su entorno actual y cómo diseñar su nueva arquitectura.

Temas

- [Mapeo de las aplicaciones](#)
- [Planificación de la arquitectura](#)

Mapeo de las aplicaciones

No existe un enfoque estándar a la hora de migrar las aplicaciones y sus dependencias asociadas a la AWS nube. La siguiente tabla proporciona una descripción general de las principales consideraciones para las diferentes aplicaciones que se suelen migrar con cargas de trabajo de F5 BIG-IP a la nube. AWS

Tipo de aplicación	Caso de uso	Acción sugerida
Aplicaciones personalizadas o comerciales off-the-shelf (COT)	<p>Planea cerrar un centro de datos o una instancia de coubicación después de migrar las aplicaciones a la nube AWS, o ejecutar una combinación de productos o servicios de AWS en las instalaciones. No tiene previsto modernizar estas aplicaciones.</p> <p>Es posible que haya integrado el controlador de entrega de aplicaciones (ADC) de F5 como parte de la lógica de la aplicación y haya necesitado que transfiera la misma lógica a la nube AWS.</p>	<p>Revise las configuraciones actuales de F5 y divídalas en los componentes de la aplicación que deben migrarse.</p> <p>Asegúrese de que se ajusta al modelo de licencia utilizado , ya sea a través de los módulos o del programa F5 Good, Better, Best (GBB).</p>

Tipo de aplicación	Caso de uso	Acción sugerida
	Es posible o no que los componentes de la aplicación se migren al mismo tiempo.	
Aplicaciones con requisitos de alta conformidad o relacionados con la seguridad	<p>Si bien estas aplicaciones se pueden volver a alojar, redefinir la plataforma o rediseñar su arquitectura, requerirán protecciones avanzadas.</p> <p>Estas protecciones avanzadas pueden incluir la protección conductual, la seguridad de las aplicaciones móviles, la detección avanzada de bots, la inteligencia IP profunda y el filtrado de salida de los datos de respuesta.</p>	<p>Si ya utiliza F5 ASM, asegúrese de migrar la política de seguridad o conformidad.</p> <p>Si se trata de una aplicación nueva, debería evaluar la mejor forma de aprovechar F5 ASM o F5 Web Application Firewall (F5 WAF).</p>
Aplicaciones de próxima generación o nativas de la nube alojadas en Amazon Elastic Container Service (Amazon ECS), Amazon Elastic Kubernetes Service (Amazon EKS) o Amazon EC2 que alojen K8S	Estas aplicaciones requieren ajustes de protocolo, como redes móviles u otros tipos de redes con pérdidas, optimizaciones HTTP, un plano de datos programable (iRules) o servicios avanzados que alineen los algoritmos de equilibrio de carga.	Para obtener información sobre la entrada de contenidos, consulte los Servicios de entrada de contenedores de F5 en la documentación de F5 .

Tipo de aplicación	Caso de uso	Acción sugerida
Aplicaciones híbridas o de espacio de nombres federado	<p>Se trata de aplicaciones en las que la entrega del nivel de presentación está federada en una implementación híbrida o en las que los servicios consumidos se encuentran en una implementación híbrida.</p> <p>Por ejemplo, puede utilizar F5 GTM junto con F5 LTM de forma local y haber aprovechado las funciones avanzadas de F5 GTM para trazar las dependencias complejas y establecer una lógica avanzada sobre la ubicación a la que enviar a los clientes.</p>	<p><u>Esta implementación debe tener un mínimo de dos sistemas DNS de F5 o DNS de F5 Cloud Services.</u></p> <p>La implementación requerirá la creación de una o más VPC en la nube. AWS</p> <p>Será necesario asignar una VPC al sistema como centro de datos. Podrían ser varias VPC si utilizas un diseño de VPC de tránsito.</p>

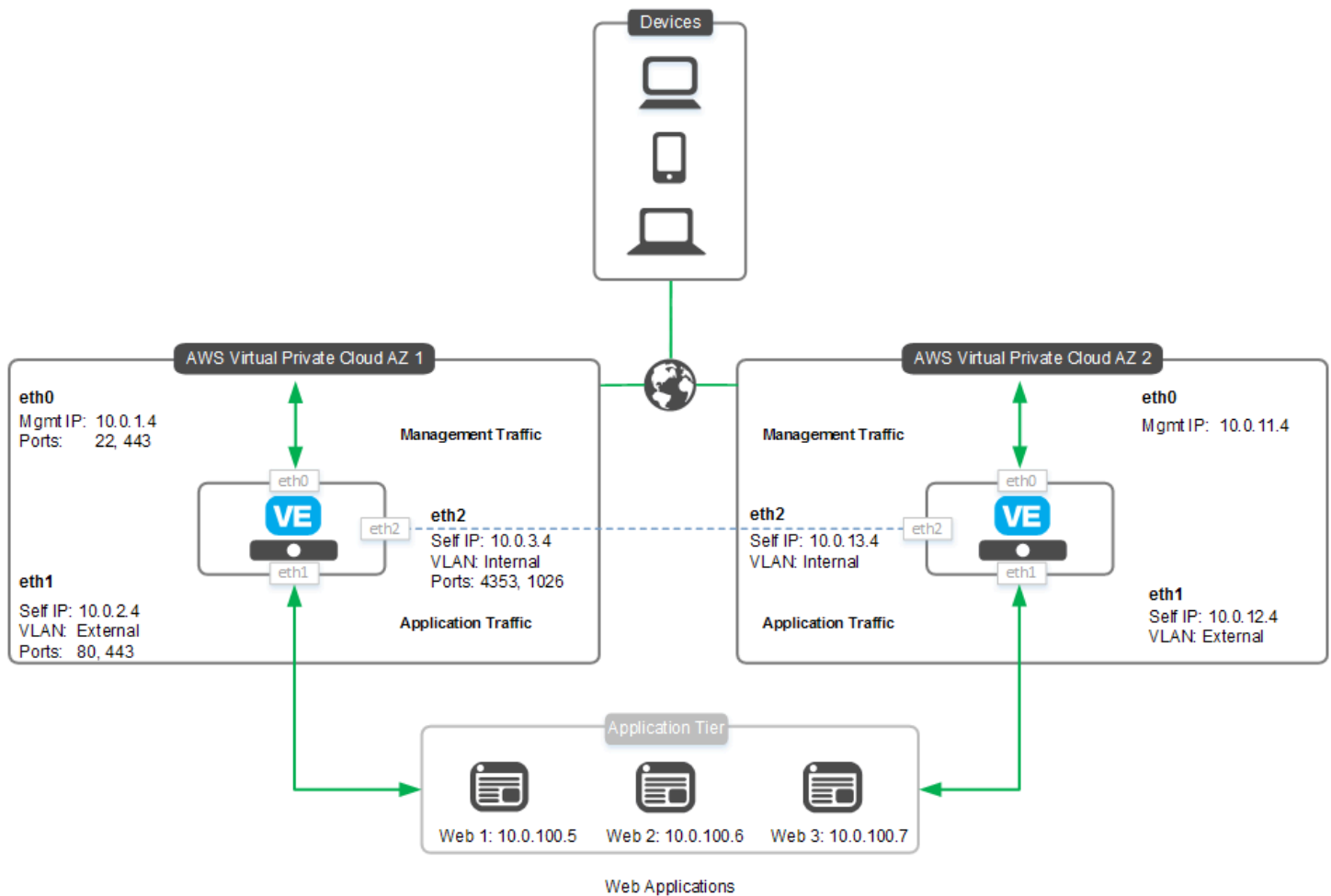
Tipo de aplicación	Caso de uso	Acción sugerida
Aplicaciones de rendimiento optimizado	Aplicaciones que pueden tener perfiles muy ajustados en las capas de sesión (L4) y de aplicaciones (L7), aplicaciones móviles o en las que le preocupa el aumento de latencia, las optimizaciones HTTP (SPDY) y la compresión debido a la migración hacia y desde la nube. AWS	<p>Esto requiere el despliegue del sistema LTM de F5 que ejecute servidores virtuales de tipo estándar (proxy TTCP completo) o superior (proxy de aplicaciones como HTTP), con un tráfico simétrico bajo entre los servidores de aplicaciones y los clientes.</p> <p>El tráfico se puede procesar mediante una traducción de direcciones de red de origen (SNAT) o las instancias BIG-IP de F5 pueden ser la puerta de enlace predeterminada para la instancia y la tabla de enrutamiento.</p>
Aplicación interna en varias zonas de disponibilidad, alta disponibilidad (HA) pero sin DNS	Necesita implementar una aplicación y desea admitir la compatibilidad entre zonas para aumentar la disponibilidad, pero no desea utilizar el DNS y no puede cambiar la dirección IP.	Deberá utilizar puertas de enlace de cliente en la VPC que estén vinculadas a una puerta de enlace privada virtual para anunciar el espacio de direcciones ajenas, además de utilizar la plantilla iApp HA de F5 Advanced para manipular la tabla de enrutamiento. Los sistemas F5 pueden ser las puertas de enlace de cliente en la VPC o una solución de terceros puede ser la pasarela del cliente.

Tipo de aplicación	Caso de uso	Acción sugerida
Aplicaciones WAF o IDS/IPS	<p>Estas aplicaciones requieren funciones de seguridad avanzadas, como las firmas SNORT, la protección contra los bots, los conjuntos de reglas WAF profundos y complejos (más de 2900 firmas) y la integración de escáneres de seguridad.</p>	<p>Elija una topología de AWS CloudFormation plantilla que satisfaga las necesidades de la aplicación (alta disponibilidad AWS Auto Scaling, independiente) y, a continuación, cree y valide la política de seguridad adecuada.</p>
Aplicaciones de VPC de tránsito de seguridad y servicios	<p>Se trata de una variante de una VPC de tránsito en la que se centralizan la seguridad y los servicios de Internet o la intranet y se sincronizan con otras VPC.</p> <p>Esta topología se puede utilizar junto con otros tipos de aplicaciones y listas de casos de uso. Se utiliza para reducir la superficie expuesta a ataques a Internet de la estructura de VPC de una organización, centralizar los controles y separar las tareas. También se utiliza para insertar aplicaciones avanzadas y servicios de seguridad entre una VPC específica, otras VPC e Internet.</p>	<p>Implemente una VPC de tránsito junto con los requisitos de visibilidad de la dirección IP de la VPC homóloga (aplicación).</p>

Tipo de aplicación	Caso de uso	Acción sugerida
Aplicaciones de seguridad de DNS, rápidas e híbridas	Replique tablas de búsqueda de DNS seguras y coherentes en la AWS nube y el centro de datos con la capacidad de gestionar grandes volúmenes de consultas de DNS; sobrevivir a una interrupción de la conexión directa mediante AWS Direct Connect un DNS gestionado centralmente y basado en políticas en todo el entorno; el almacenamiento en caché del DNS y la validación y seguridad del protocolo DNS (DNSSEC).	Utilice las prácticas recomendadas para implementar DNS y tratar cada VPC como un centro de datos virtual.

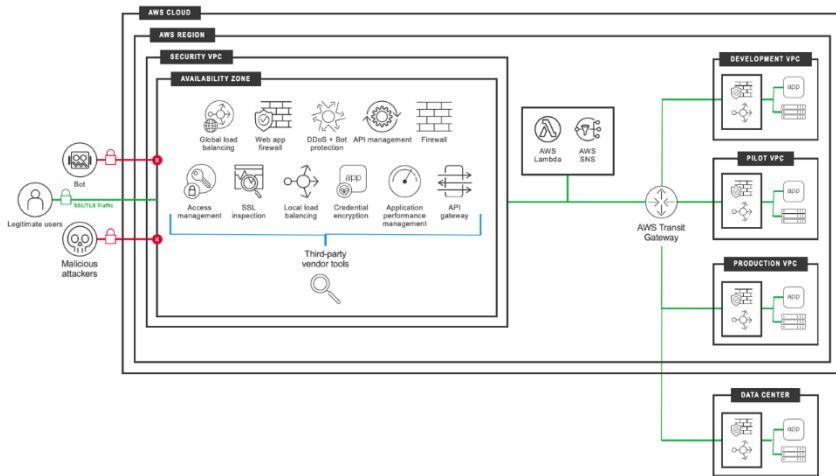
Planificación de la arquitectura

El siguiente diagrama muestra la arquitectura básica de las VPC perimetrales y las VPC de aplicaciones que están conectadas mediante Transit GatewayAWS. Las VPC pueden formar parte de la misma cuenta o de cuentas diferentes.



Por ejemplo, una zona de aterrizaje normalmente despliega una cuenta de red que controlará las VPC periféricas. F5 denomina a este patrón una [arquitectura de nube segura](#), que ayuda a los usuarios a aprovechar las políticas, los procesos y las plataformas comunes en todo el conjunto de aplicaciones.

El siguiente diagrama muestra dos instancias de interfaz de red (NIC) de una carga de trabajo BIG-IP de F5 implementadas en un clúster en espera activo. Puede añadir interfaces de red más elásticas a estos sistemas, hasta el límite de instancias. F5 recomienda utilizar un patrón Multi-AZ para la implementación a fin de evitar errores en la zona de disponibilidad.



Planificación de la migración

Planificar el proceso de migración es clave para garantizar una migración fluida y exitosa. En las siguientes secciones se explica cómo planificar la migración, así como las principales consideraciones al respecto.

Temas

- [Decisión sobre qué migrar](#)
- [Desescalada de las configuraciones](#)
- [Elección de un tipo de instancia](#)
- [Puntos clave de decisión](#)
- [Descripción general de la migración](#)

Decisión sobre qué migrar

Al migrar, debe decidir qué cargas de trabajo son esenciales; qué cargas de trabajo son «deseables» pero no esenciales; y qué cargas de trabajo no son necesarias y se pueden [retirar una vez que se complete la migración](#).

Una parte importante del proceso de toma de decisiones incluirá los requisitos individuales que tenga en materia de automatización, API, herramientas y otros procesos. También tendrá que tener en cuenta los requisitos funcionales y de rendimiento de su organización.

Por ejemplo, es posible que haya utilizado plataformas de hardware compartidas en un centro de datos existente con particiones de usuario. Sin embargo, la migración puede requerir que los servicios se ejecuten en sistemas que no estén tan ampliamente compartidos debido a las limitaciones de rendimiento que supone pasar de soluciones aceleradas por hardware. Por ejemplo, las transacciones por segundo (TPS) de la capa de conexión segura (SSL) podrían requerir que un determinado servicio no se ejecute en un sistema compartido.

Tras identificar y documentar las aplicaciones que se van a migrar y sus requisitos, debe preparar los sistemas de origen siguiendo las prácticas recomendadas que se enumeran a continuación.

- Ejecutar la misma versión de F5 TMOS que ejecutará en AWS Cloud. Se recomienda la [versión 14.1](#) o posterior, pero también se puede utilizar la [versión 13.1](#) o posterior. Si bien puede migrar la versión [12.1.x](#), es posible que tenga problemas de seguridad, automatización y mantenimiento.

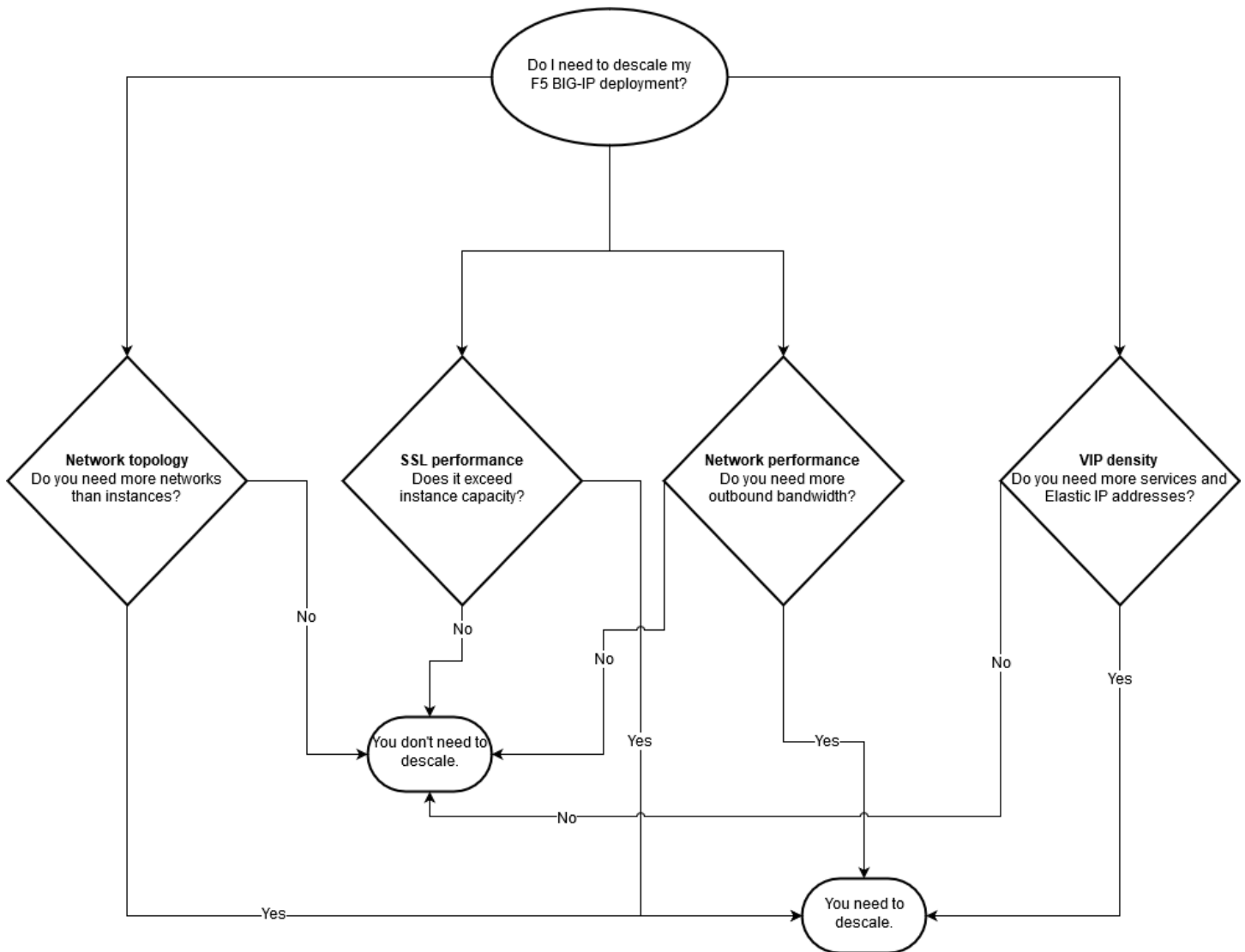
- Tener copias de seguridad válidas de todas las configuraciones de cada dispositivo. Dado que la copia de seguridad de Univention Corporate Server (UCS) contiene atributos y objetos específicos del centro de datos (como direcciones IP, nodos o miembros del grupo), F5 recomienda crear un archivo de comandos shell (SCF) para editar y combinar las configuraciones.
- Tener copias de seguridad de todos los certificados de seguridad pertinentes y considerar la posibilidad de pasar del cifrado RSA al cifrado ECC para mejorar el rendimiento.
- Contar con métricas de rendimiento detalladas a nivel del servidor virtual para planificar el escalamiento y la capacidad.
- Disponer de una solución [de equilibrador de carga global del servidor \(GSLB\) de F5](#) para la transición del centro de datos a AWS Cloud.
- Comprender el impacto de la migración de un modelo de dispositivo de hardware a un modelo virtualizado y de software en términos de rendimiento, escalabilidad y alta disponibilidad.
- Tener definidos los requisitos de lo que se migrará a la nube de AWS y tener en cuenta las siguientes consideraciones.
 - Tener en cuenta que cualquier migración a la nube de AWS requiere decidir si se migrarán las configuraciones completas o parciales. Por lo general, un movimiento parcial a la vez es más eficiente.
 - Comprender qué rutas y direcciones IP se modificarán.
 - Identificar qué grupos de SNAT deben reemplazarse por el [F5 SNAT Automap](#).

También debería considerar la posibilidad de consultar a [socios de AWS](#) o al equipo de servicios profesionales de F5. Esto ayudará a garantizar una alta probabilidad de que la migración se lleve a cabo correctamente.

Desescalada de las configuraciones

«Desescalar» significa pasar de una configuración de F5 BIG-IP a una configuración más baja o más rentable, en función de las características o métricas requeridas tras la detección inicial. Debe evaluar detenidamente todas estas opciones, ya que afectarán a la arquitectura y a la cantidad de instancias necesarias.

El siguiente diagrama le ayuda a evaluar si la desescalada es adecuada para sus necesidades y requisitos.



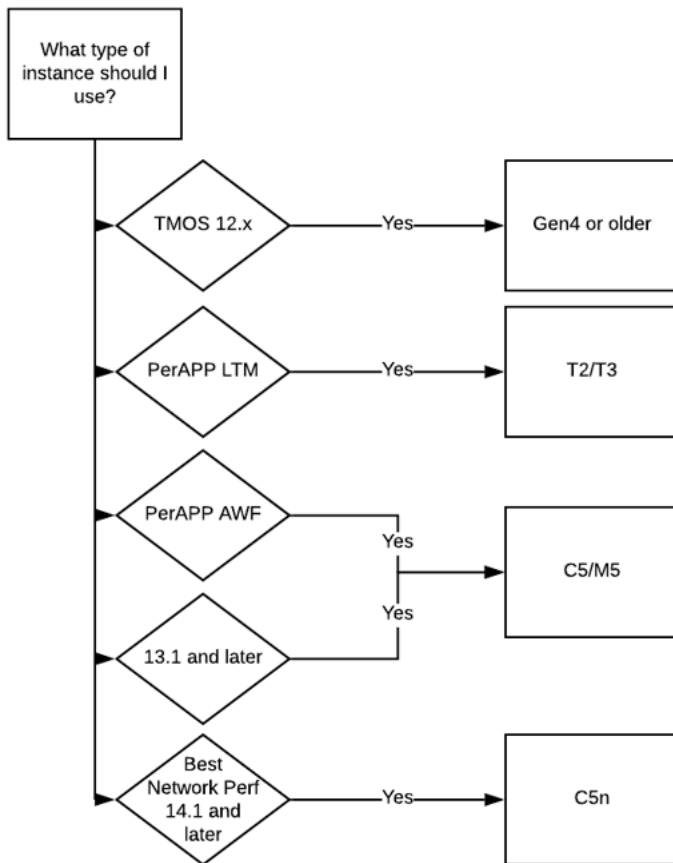
La migración también generará nuevas consideraciones en las siguientes áreas.

- Topología de red: actualmente, AWS no admite VLAN con etiquetado 802.1q, por lo que la cantidad de interfaces de la instancia (menos una para la administración) limita la cantidad de redes que puede admitir una instancia. Si necesita una topología específica, debe evaluarla comparándola con las distintas instancias que F5 admite en AWS Cloud.
- Rendimiento de SSL: los dispositivos y el chasis de F5 tienen un rendimiento de SSL que supera lo que se puede lograr con x86. Debe evaluar los requisitos de SSL agregados y por servidor virtual.
- Rendimiento de la red: debe evaluar las características de la red agregada, saliente e interna. Los tipos de instancias de AWS tienen diferentes características de red (baja, media, alta, hasta X o dedicada) que deben tenerse en cuenta. También hay límites en cuanto al tráfico que una sola instancia puede enviar de forma saliente o a través de una conexión directa.

- Densidad de las VIP: si tiene una cantidad mayor de direcciones IP virtuales (VIP), debe tener en cuenta el límite máximo de instancias según la cantidad de VIP que se pueden asignar a las interfaces de red.
- Conexión simultánea: hay límites de flujo en cuanto al número máximo de conexiones que pueden admitir las instancias.
- Estado de la sesión: las distintas aplicaciones utilizan distintos tipos de persistencia. Las aplicaciones con y sin estado cambiarán los métodos utilizados a un estado compartido, y esto puede afectar a la escala de las operaciones de entrada y salida.

Elección de un tipo de instancia

F5 admite varios tipos de instancias y elegir cuál usar puede ser una decisión compleja. Para la mayoría de las migraciones, c5n.2x1 y c5n.4x1 serán las opciones de instancias más comunes porque ofrecen una combinación de rendimiento de red, densidad de la CPU, densidad de la interfaz y cantidad de IP compatibles con la instancia. En el siguiente diagrama se brindan ejemplos de las instancias que debe elegir, en función de los productos de F5 que utilice.



Puntos clave de decisión

Hay muchos aspectos de la migración que deben tenerse en cuenta, pero antes de comenzar la migración de la carga de trabajo de F5 BIG-IP, hágase las siguientes preguntas para aclarar el proceso de migración.

¿Quiénes son los usuarios de las aplicaciones?

Evalúe si se trata de usuarios internos (que no recorren una dirección IP elástica) o usuarios externos (que recorren una dirección IP elástica). Si los usuarios son internos, evalúe si la aplicación puede usar el DNS para adaptarse al fallo de una zona de disponibilidad o de una implementación activa. También debe comprobar si necesita utilizar un patrón de diseño alternativo que permita que una subred abarque varias zonas de disponibilidad.

¿Qué partes de sus aplicaciones migrarán a AWS Cloud?

Evalúe si se está trasladando toda la aplicación o solo el nivel de presentación. También debería tener en cuenta las dependencias adicionales en torno a la seguridad y al espacio de nombres de DNS. La evaluación debe determinar lo que se necesitaría de la topología de la red. Además, determine qué se requiere de un acuerdo de nivel de servicio (SLA) en caso de que se produzca un evento a nivel de zona de disponibilidad, VPC o región de AWS.

¿Por qué se migra la aplicación?

Es posible que esté migrando su aplicación porque está cerrando centros de datos o porque desea más elasticidad. Evalúe si la aplicación está migrando para tener una arquitectura por aplicación, en comparación con los patrones monolíticos compartidos comunes en muchos centros de datos. También vale la pena considerar qué esfuerzos de modernización deberían realizarse junto con la migración.

¿Adónde se migra la aplicación?


Evalúe si la aplicación debe trasladarse a una sola VPC con una o dos zonas de disponibilidad. Determine si la topología de la VPC es de interconexión o de tránsito, junto con la necesidad de implementaciones en varias regiones. Esto afectará al diseño del patrón de migración.

Descripción general de la migración

Antes de comenzar la migración, es útil diseñar todo el proceso de manera general. El siguiente es un ejemplo de los pasos que puede seguir para migrar una carga de trabajo de F5 BIG-IP a AWS Cloud. Puede encontrar pasos y procesos más detallados para una migración de F5 BIG-IP en el patrón [Migración de una carga de trabajo de F5 BIG-IP a F5 BIG-IP VE en AWS Cloud](#).

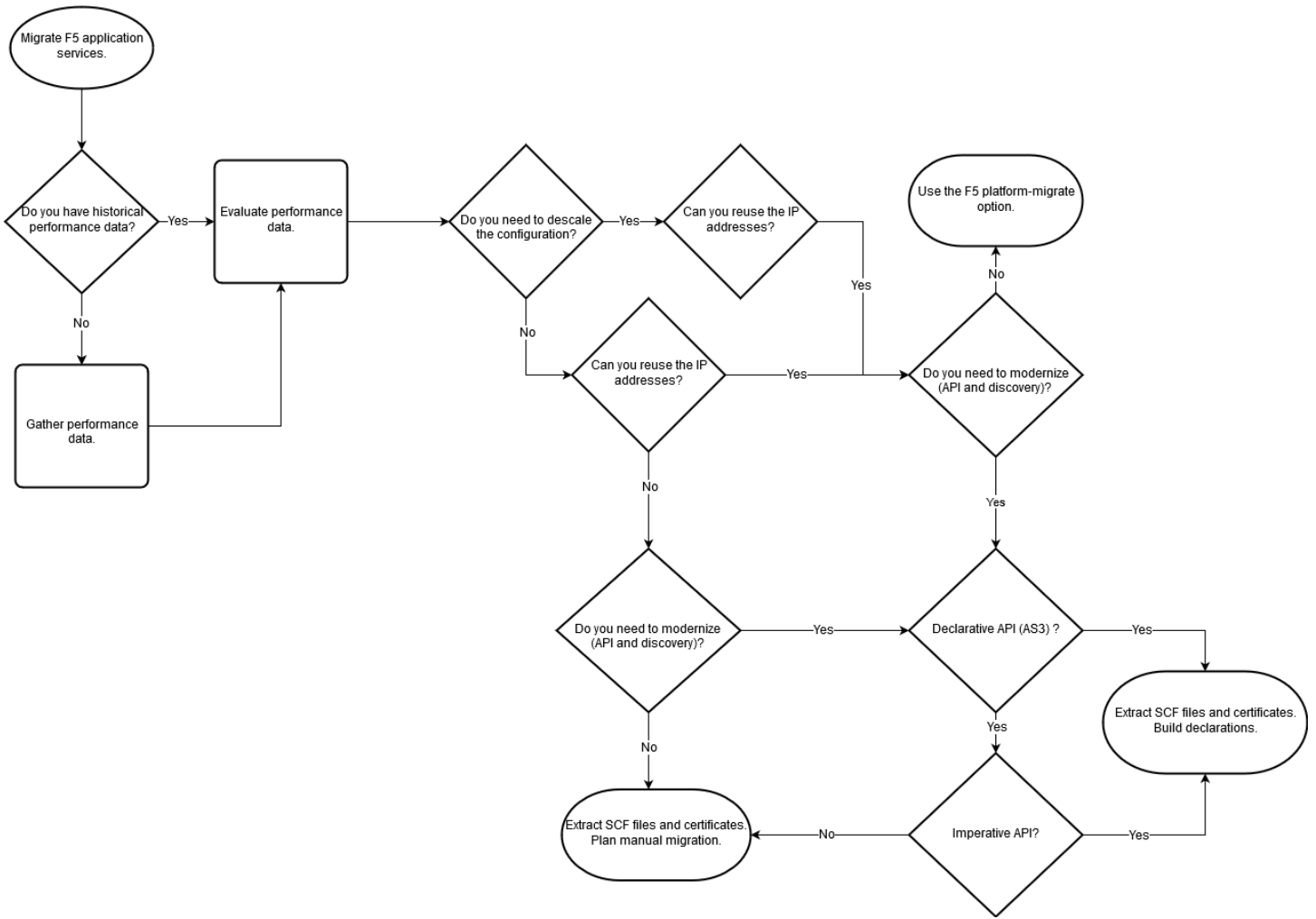
1. Implemente la cantidad necesaria de VPC en función de los requisitos individuales. Esta implementación puede ser manual o automatizada mediante una herramienta como la [zona de aterrizaje de AWS](#).
2. Evalúe las licencias, los usos y las configuraciones actuales de F5.
3. Evalúe las aplicaciones públicas e internas.
4. Evalúe las configuraciones actuales de F5.
5. Evalúe los requisitos de tamaño y de dirección IP y elija la cantidad y el tipo de instancias de F5 y AWS necesarios.
6. Identifique qué estrategia de migración implementar. Por ejemplo, migrar mediante lift-and-shift; mediante shift-and-modernize; o utilizando una estrategia híbrida.

7. Evalúe e identifique el diseño del DNS.
8. Evalúe cómo se dirigirá el tráfico a la aplicación si esta existe tanto en las instalaciones como en AWS Cloud.
9. Realice las implementaciones iniciales de las instancias de F5 mediante AWS CloudFormation plantillas.
10. Modifique las implementaciones para cumplir con los requisitos de topología con tablas de enrutamiento e interfaces de red elásticas adicionales.
11. Alinee las direcciones IP elásticas con las IP propias o de administración y planifique el mapeo de IP elásticas a IP virtuales (VIP).
12. Cree direcciones secundarias en las interfaces de red elásticas para las VIP.
13. Aplique direcciones secundarias en AWS Cloud.
14. Asigne las direcciones IP elásticas a la dirección secundaria para las VIP.
15. Extraiga las configuraciones y compile una lista de objetos para moverlos.
16. Implemente las configuraciones en F5 BIG-IP.
17. Asigne las direcciones secundarias a las VIP.
18. Realice una prueba de tráfico.
19. Realice una prueba de conmutación por error.
20. Si está creando una estrategia híbrida, asegúrese de incorporar el sistema al DNS de F5.

 Important

Se requiere el acceso a los puntos de conexión de la API de AWS. Las direcciones NAT o IP elásticas también son necesarias para una alta disponibilidad dentro de las zonas de disponibilidad o entre ellas.

En el siguiente diagrama se muestra el flujo del proceso de alto nivel para una migración a F5 BIG-IP.



Migración de datos

Todas las migraciones deben iterar sobre una configuración y desarrollar el árbol de dependencias. Cuando se utiliza un único archivo de configuración, todo se hace automáticamente. Si utiliza la [API TMSH](#), tendrá que iterar y desarrollar el árbol de dependencias. En las siguientes secciones se describen las diferentes opciones y configuraciones disponibles al migrar una carga de trabajo de F5 BIG-IP.

Temas

- [Migración de una configuración completa](#)
- [Migración de una configuración parcial](#)
- [Implementaciones de alta densidad sin IP elásticas](#)
- [Interconexión de las VPC](#)
- [Conexión a la infraestructura de AWS](#)

Migración de una configuración completa

En este enfoque, se toma una configuración de un sistema existente y se migra a un sistema nuevo. Este proceso copiará la configuración existente, las direcciones IP, los certificados, las claves, las frases de contraseña y las credenciales de inicio de sesión.

El motivo principal para migrar una configuración completa es sustituir el sistema por otro igual, como una actualización de hardware o una RMA. Por lo general, estos conceptos no se aplican a AWS Cloud.

Puede usar archivos UCS o SCF para migrar una configuración completa, y en las tablas a continuación se ofrece una descripción general de las ventajas y desventajas de usarlos.

Utilizar un archivo UCS o qkview

Ventajas	Desventajas
Todos los archivos se trasladan como un archivo único.	El caso de uso principal para usar un archivo UCS sería reemplazar un dispositivo averiado. El archivo contiene información específica del

Ventajas	Desventajas
<p>Se conservan las cuentas de usuario locales. Si están integradas en su Active Directory, se conserva la configuración.</p>	<p>dispositivo que podría hacer que la carga de trabajo de F5 BIG-IP fuera inaccesible.</p> <p>Si ha configurado una integración de directorios, es posible que tenga problemas de acceso. Si no tiene acceso a las contraseñas de los usuarios, es posible que también tenga problemas de acceso.</p>
<p>Se conservan todas las configuraciones del servidor virtual.</p>	<p>Puede que tenga que editar las direcciones IP del dispositivo, los servidores virtuales y los miembros del grupo.</p>
<p>Se conserva la estructura de archivos.</p>	<p>Debe saber qué archivos editar.</p> <p>Este proceso es más complejo que un SCF o un movimiento objeto por objeto.</p> <p>Mayor riesgo de error, que incluye una reimplementación o la posibilidad de que la configuración no se cargue.</p> <p>Diseñado para flujos de trabajo de reemplazo de sistemas completos.</p>

Uso de un archivo SCF

Ventajas	Desventajas
<p>Crea un archivo de texto de la configuración.</p>	<p>Será necesario realizar modificaciones porque habrá propiedades específicas del dispositivo en el archivo que pueden afectar al acceso si el archivo simplemente se carga.</p>

Ventajas	Desventajas
Se puede editar fácilmente en cualquier editor de texto de Unix o Linux.	Debe comprender la configuración y la estructura de los archivos para realizar las modificaciones.
El archivo de configuración tiene el orden correcto de las operaciones de carga.	Debe saber qué partes del archivo debe eliminar para evitar que se sobrescriban las configuraciones específicas del dispositivo.
Puede encontrar fácilmente los objetos que se van a migrar.	

Migración de una configuración parcial

Cuando decida migrar una configuración parcial, utilizará un archivo TMSH o SCF como punto de partida. También tendrá que buscar los objetos que desee mover y compilarlos en el orden correcto. En la tabla a continuación se explican las ventajas y desventajas de migrar una configuración parcial.

Ventajas	Desventajas
Se pueden analizar las configuraciones y realizar correcciones a medida que avanza el trabajo.	Es necesario conocer los objetos y las estructuras de archivos de F5. También debe poder leer iRules.
Los cambios de configuración se pueden agrupar en lotes.	La migración lleva tiempo.
Es más fácil solucionar problemas de carga de configuración.	Editar los archivos o extraer la información puede llevar mucho tiempo.
Se reduce el riesgo de que se bloquee el acceso al dispositivo.	
Es más fácil mover la configuración a una topología adecuada.	

Ventajas	Desventajas
<p>Es más fácil abordar las particiones del administrador y enrutar los dominios porque se trata de un archivo plano.</p>	
<p>La estructura plana de archivos permite el uso de herramientas de texto de Linux si desea buscar y reemplazar direcciones IP mediante programación.</p>	

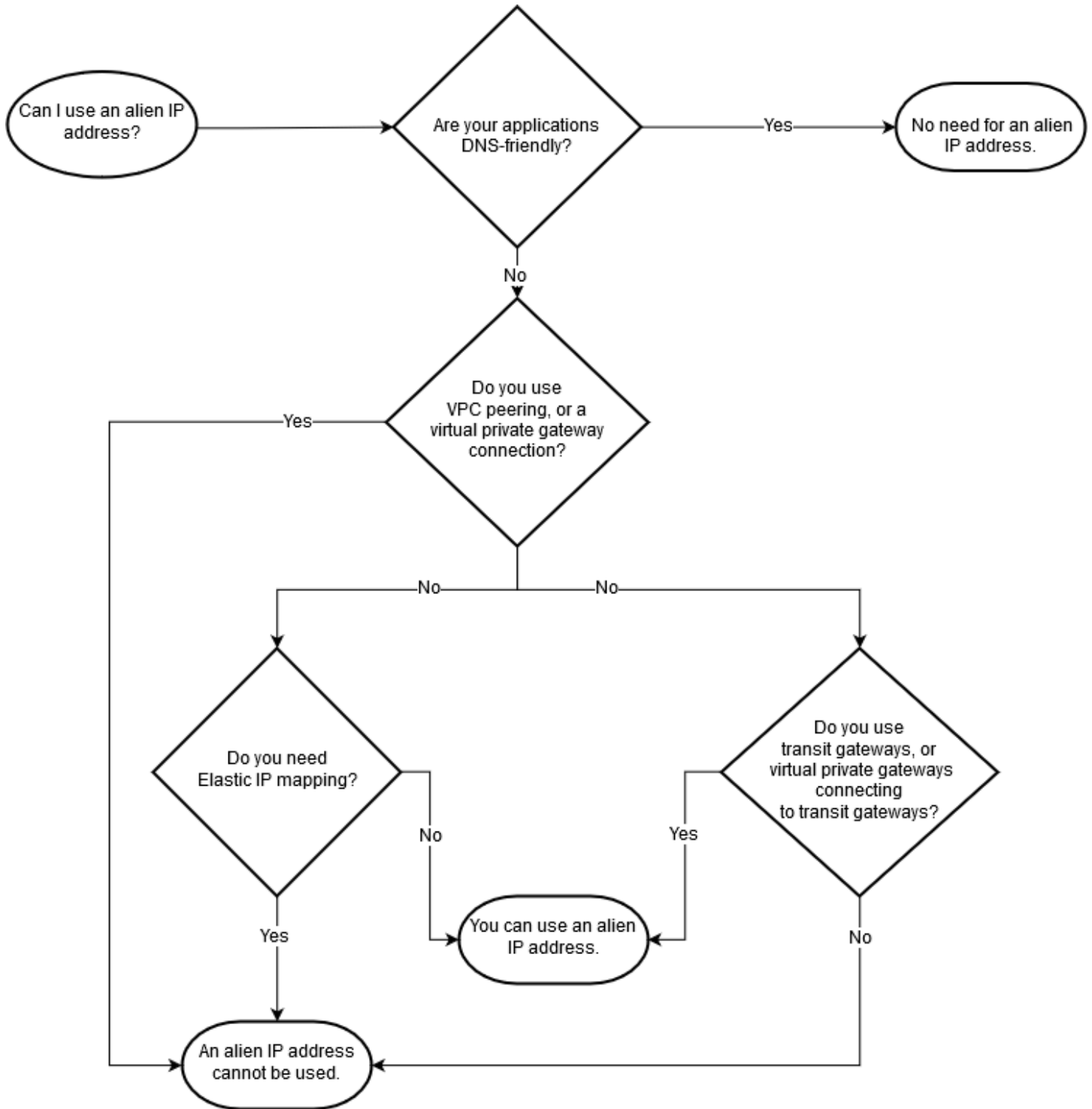
Implementaciones de alta densidad sin IP elásticas

Si necesita implementaciones muy densas, puede utilizar las métricas de desempeño, y estas aplicaciones no requieren el uso de IP elásticas. Esto se conoce como «IP ajenas».

Una IP ajena es un rango de redes o subredes externo al bloque CIDR de la VPC y al que F5 asigna servicios virtuales. Las direcciones IP ajenas no funcionan en todas las situaciones, pero se pueden usar para una alta densidad de servidores virtuales. Antes de poder utilizar una IP ajena, se requieren los siguientes recursos.

- Una subred para alojar las aplicaciones
- Una implementación de F5 BIG-IP con una extensión de conmutación por error en Cloud para administrar las rutas
- Una ruta en las tablas de enrutamiento de AWS que apunta a las interfaces de red elásticas

El uso de direcciones IP ajenas tiene implicaciones en la forma en que se interconectan las VPC con otras VPC, así como en la forma en que se pueden interconectar las VPC con sus centros de datos. El siguiente diagrama ayuda a determinar si se necesita una dirección IP ajena.



Interconexión de las VPC

En las tablas a continuación se muestran las consideraciones clave a la hora de interconectar las VPC.

VPC de seguridad con emparejamiento de VPC		VPC de seguridad con AWS Transit Gateway		VPC de seguridad con interconexión VPN	
Ventajas	Desventajas	Ventajas	Desventajas	Ventajas	Desventajas
<ul style="list-style-type: none"> • Configura ción rápida y sencilla • Direccio namiento simple • Alta redundancia • Ancho de banda alto 	<ul style="list-style-type: none"> • Solo admite el tráfico de rangos de CIDR asignados por VPC • No se puede insertar una inspección de seguridad entre las VPC • Es complejo de administrar a escala (todas son de punto a punto) 	<ul style="list-style-type: none"> • Configura ción sencilla • Enrutamie nto flexible sin SNAT • Alta redundancia • Ancho de banda alto • Administr ación sencilla a escala 	<ul style="list-style-type: none"> • El enrutamie nto es más complejo (tablas de enrutamie nto de VPC y tablas de enrutamie nto de AWS Transit Gateway) • Topología compleja para insertar la inspección de seguridad entre las VPC 	<ul style="list-style-type: none"> • Enrutamie nto flexible sin SNAT • Fácil inserción de una inspección de seguridad entre las VPC 	<ul style="list-style-type: none"> • Ancho de banda bajo • Conmutaci ón por error compleja y dependien te de un proveedor • Es complejo de administr ar a escala (todas son de punto a punto)

Cliente (envía SYN)	AWS Transit Gateway	Emparejamiento de VPC	VPN entre las VPC	Descripción general de la solución y posibles problemas
Se utiliza Internet o AWS Direct Connect para prestar servicio en una sola VPC con una subred pública o privada.	N/A	N/A	N/A	El tráfico atraviesa la puerta de enlace de Internet, o la puerta de enlace virtual, así que no necesita cruzar más allá del límite de la VPC. La VPC actúa como redes stub diseñadas. El tráfico ingresa desde las instalaciones a AWS Cloud (AWS Direct Connect, VPN).
Internet o AWS Direct Connect en una VPC con clientes en otras VPC (por ejemplo, miembros de un grupo en otra VPC), sin SNAT.	Sí	No	Sí	<p>AWS Transit Gateway o las VPN hacen que el tráfico eluda el filtro de emparejamiento de la VPC que solo los CIDR asignados por VPC pueden pasar.</p> <p>Las soluciones de VPN estarán restringidas. No hay enrutamiento de múltiples rutas de igual costo (ECMP) (solo una ruta) ni ancho de banda (alrededor de 1,2 GB por segundo por túnel, en general solo un túnel).</p>
Internet o AWS Direct Connect para un servicio en una VPC con clientes en otras VPC (por ejemplo, miembros de un grupo en otra VPC), sin SNAT.	Sí (pero no obligatorio)	Sí	Sí (pero no obligatorio)	<p>Como la interconexión entre las VPC detecta el tráfico de los CIDR asignados por las VPC, cualquiera de ellas funcionará.</p> <p>Las soluciones de VPN estarán restringidas. No hay ECMP (solo una ruta) ni ancho de banda (alrededor de 1,2 GB por segundo por túnel, en general solo un túnel).</p>

Cliente (envía SYN)	AWS Transit Gateway	Emparejamiento de VPC	VPN entre las VPC	Descripción general de la solución y posibles problemas
Dentro de la VPC para prestar servicio en la misma VPC.	N/A	N/A	N/A	Todo el tráfico está restringido a una única VPC. No es obligatoria la interconexión.
Dentro de una VPC para prestar servicio en la misma VPC. El servicio está en el CIDR de la VPC de destino.	Sí (pero no obligatorio)	Sí	Sí (pero no obligatorio)	Como la interconexión entre las VPC detecta el tráfico de los CIDR asignados por las VPC, cualquiera de ellas funcionará.
Dentro de una VPC para prestar servicio en la misma VPC. El servicio está fuera del rango de CIDR de la VPC.	Sí	No	Sí	<p>Como la interconexión entre las VPC detecta el tráfico de los CIDR asignados por las VPC, cualquiera de ellas funcionará.</p> <p>Las soluciones de VPN estarán restringidas. No hay ECMP (solo una ruta) ni ancho de banda (alrededor de 1,2 GB por segundo por túnel, en general solo un túnel).</p>
Dentro de una sola VPC a un servicio de Internet.	N/A	N/A	N/A	El tráfico proviene de un CIDR asignado por VPC. Si los constructos de la IP elástica, NAT o de la tabla de enrutamiento están en línea, el tráfico fluirá.

Cliente (envía SYN)	AWS Transit Gateway	Emparejamiento de VPC	VPN entre las VPC	Descripción general de la solución y posibles problemas
Dentro de una VPC a un servicio de Internet, enrutamiento a través de una VPC de seguridad o inspección.	Sí	No	Sí	<p>Dado que la interconexión entre las VPC detecta el tráfico desde fuera de un rango de CIDR asignado por la VPC, no se puede utilizar el emparejamiento de VPC.</p> <p>Las soluciones de VPN estarán restringidas. No hay ECMP (solo una ruta) ni ancho de banda (alrededor de 1,2 GB por segundo por túnel, en general solo un túnel).</p>

Conexión a la infraestructura de AWS

En la tabla a continuación se muestran las principales consideraciones a tener en cuenta a la hora de conectarse a la nueva infraestructura de AWS durante una migración de F5 BIG-IP.

Método de conexión	Compatibilidad con el protocolo de enrutamiento	Límite de ancho de banda	Dirección IP de punto de conexión (pública, privada o ambas)	Admite espacio de dirección ajena	Admite varias VPC en una conexión	Admite múltiples regiones
Internet	N/A	Se conecta a AWS 5 GB por segundo por instancia de salida	Public	No	Sí	Sí

Método de conexión	Compatibilidad con el protocolo de enrutamiento	Límite de ancho de banda	Dirección IP de punto de conexión (pública, privada o ambas)	Admite espacio de dirección ajena	Admite varias VPC en una conexión	Admite múltiples regiones
VPN: VPC	Estático, BGP	Límites de IPsec (alrededor de 1,2 GB por segundo por túnel)	Private	Sí (debe configurarse un túnel IPsec adicional desde F5 BIG-IP de la VPC hasta la puerta de enlace virtual conectada a la VPC).	No	No
VPN y AWS Transit Gateway	Estático, BGP	Límites de IPsec (alrededor de 1,2 GB por segundo por túnel)	Private	Sí	Sí	No (si se amplía la puerta de enlace de tránsito, se verá afectada)

Método de conexión	Compatibilidad con el protocolo de enrutamiento	Límite de ancho de banda	Dirección IP de punto de conexión (pública, privada o ambas)	Admite espacio de dirección ajena	Admite varias VPC en una conexión	Admite múltiples regiones
AWS Direct Connect: VPC	Estático, BGP	Límites de AWS Direct Connect (admite la conexión), las instancias individuales se limitan a 5 GB por segundo	Ambos	No	No	No
AWS Direct Connect: puerta de enlace	Estático, BGP	Límites de AWS Direct Connect (admite la conexión), las instancias individuales se limitan a 5 GB por segundo	Ambos	No	Sí	Sí

Método de conexión	Compatibilidad con el protocolo de enrutamiento	Límite de ancho de banda	Dirección IP de punto de conexión (pública, privada o ambas)	Admite espacio de dirección ajena	Admite varias VPC en una conexión	Admite múltiples regiones
Puerta de enlace de AWS Direct Connect: AWS Transit Gateway (limitado a varias regiones de AWS)	Estático, BGP	Límites de AWS Direct Connect (admite la conexión), las instancias individuales se limitan a 5 GB por segundo	Confirmación verbal del equipo de arquitectos de AWS	Sí	Sí	Limitado a varias regiones

Recursos

Documentación de F5

- [Extensión de conmutación por error en la nube de F5](#)
- [Streaming de telemetría de F5](#)
- [Laboratorio de topología de F5](#)
- [Servicios de aplicaciones de F5 en AWS: información general \(video\)](#)
- [Guía del usuario de la Extensión Application Services 3 de F5](#)
- [F5 devcentral GitHub](#)
- [iControl REST de F5 wiki](#)
- [Descripción general de los archivos de configuración individuales \(11.x - 15.x\) de F5](#)
- [Documentos técnicos de F5](#)
- [Descripción general de la opción de «migración de plataforma» del archivo UCS](#)
- [Centro de conocimiento de F5 BIG-IP Cloud Edition](#)

Recursos de AWS

- [F5 en AWS Marketplace](#)
- [F5 BIG-IP VE en AWS: Inicio rápido](#)

Socios de AWS

- [F5 en AWS](#)

Guías y patrones relacionados

- [Migración de una carga de trabajo de F5 BIG-IP a F5 BIG-IP VE en AWS Cloud](#)

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	—	16 de noviembre de 2020

Glosario de las Recomendaciones de AWS

Los siguientes son términos de uso común en las estrategias, guías y patrones que se ofrecen en las Recomendaciones de AWS. Para sugerir entradas, utilice el enlace [Enviar comentarios](#) al final del glosario.

Números

Las 7 R

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

- **Refactorizar/rediseñar:** traslade una aplicación y modifique su arquitectura mediante el máximo aprovechamiento de las características nativas en la nube para mejorar la agilidad, el rendimiento y la escalabilidad. Por lo general, esto implica trasladar el sistema operativo y la base de datos. Ejemplo: Migre 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: Migre la base de datos Oracle en las instalaciones a Amazon Relational Database Service (Amazon RDS) para Oracle en la nube de AWS.
- **Recomprar (readquirir):** cambie a un producto diferente, lo cual se suele llevar a cabo al pasar de una licencia tradicional a un modelo SaaS. Ejemplo: Migre 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: Migre su 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. Este escenario de migración es específico de VMware Cloud en AWS, que permite la compatibilidad de máquinas virtuales (VM) y la portabilidad de cargas de trabajo entre el entorno en las instalaciones y de AWS. Puede utilizar las tecnologías de VMware Cloud Foundation desde los centros de datos en las instalaciones al migrar una infraestructura a VMware Cloud en AWS. Ejemplo: Reubicar el hipervisor que aloja la base de datos de Oracle a VMware Cloud en AWS.

- **Retener (revisitar):** conserve las aplicaciones en el entorno de origen. Estas pueden incluir las aplicaciones que requieren una refactorización importante, que desee posponer para más adelante, y las aplicaciones heredadas que desee retener, ya que no hay ninguna justificación empresarial para migrarlas.
- **Retirar:** retire o elimine las aplicaciones que ya no sean necesarias en un entorno de origen.

A

ABAC

Consulte control de [acceso basado en atributos](#).

servicios abstractos

Consulte [servicios gestionados](#).

ACID

Consulte [atomicidad, consistencia, aislamiento y durabilidad](#).

migración activa-activa

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

migración activa-pasiva

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

función agregada

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

IA

Véase [inteligencia artificial](#).

AIOps

Consulte las [operaciones de inteligencia artificial](#).

anonimización

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

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

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

cartera de aplicaciones

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

inteligencia artificial (IA)

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

operaciones de inteligencia artificial (AIOps)

El proceso de utilizar técnicas de machine learning para resolver problemas operativos, reducir los incidentes operativos y la intervención humana, y mejorar la calidad del servicio. Para obtener más información sobre cómo se utiliza AIOps en la estrategia de migración de AWS, 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. A fin de obtener más información, consulte [ABAC para AWS](#) en la documentación de 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

Ubicación diferenciada de una Región de AWS que está aislada de los errores que se producen en otras zonas de disponibilidad y que brinda conectividad de red económica y de baja latencia a otras zonas de disponibilidad de la misma región.

AWS Cloud Adoption Framework (AWS CAF)

Marco de directrices y prácticas recomendadas de AWS para ayudar a las empresas a desarrollar un plan eficiente y eficaz a fin de migrar con éxito a la nube. AWS CAF organiza la orientación en seis áreas de enfoque llamadas perspectivas: empresarial, humana, gobernanza, 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 brinda orientación para el desarrollo, la capacitación y la comunicación de las personas, con el fin de ayudar a preparar 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 Workload Qualification Framework (AWS WQF)

Herramienta que evalúa las cargas de trabajo de migración de bases de datos, recomienda estrategias de migración y brinda 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

BCP

Consulte la [planificación de la continuidad del negocio](#).

gráfico de comportamiento

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

sistema big-endian

Un sistema que almacena primero el byte más significativo. Véase también [endianness](#).

clasificación binaria

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

filtro de floración

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

rama

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 \(documentación\)](#) GitHub .

acceso con cristales rotos

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

estrategia de implementación sobre infraestructura existente

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

caché de búfer

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

capacidad empresarial

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

planificación de la continuidad del negocio (BCP)

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

C

CAF

[Consulte el marco AWS de adopción de la nube.](#)

CCoE

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

CDC

Consulte la [captura de datos de cambios](#).

captura de datos de cambio (CDC)

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

ingeniería del caos

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

CI/CD

Consulte la [integración continua y la entrega continua](#).

clasificación

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

cifrado del cliente

Cifrado de datos de forma local, antes de que el Servicio de AWS de destino los 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 del CCoE](#) en el Blog de estrategia empresarial en la nube de AWS.

computación en la nube

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

modelo operativo en la nube

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

etapas de adopción de la nube

Las 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: realización de inversiones fundamentales para escalar la adopción de la nube (p. ej., crear una zona de aterrizaje, definir un 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 publicación del blog [The Journey Toward Cloud-First & the Stages of Adoption](#) (El camino hacia la nube como prioridad y las etapas de adopción) en el Blog de estrategia empresarial en la nube de AWS. Para obtener información sobre cómo se relacionan con la estrategia de migración de AWS, consulte la [Guía de preparación para la migración](#).

CMDB

Consulte la [base de datos de gestión de la configuración](#).

repositorio de código

Una ubicación donde el código fuente y otros activos, como documentación, muestras y scripts, se almacenan y actualizan mediante procesos de control de versiones. Los repositorios en la nube más comunes incluyen GitHub o AWS CodeCommit. 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

Campo de IA utilizado por las máquinas para identificar personas, lugares y cosas en imágenes con una precisión igual o superior a la humana. Construido a menudo con modelos de aprendizaje profundo, automatiza la extracción, el análisis, la clasificación y la comprensión de información útil a partir de una sola imagen o una secuencia de imágenes.

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

Una colección de acciones correctivas y reglas de AWS Config que puede reunir para personalizar sus controles de seguridad y conformidad. Puede implementar un paquete de conformidad como una sola entidad en una región y Cuenta de AWS, o en toda una organización, mediante una plantilla YAML. Para obtener más información, consulte [Paquetes de conformidad](#) en la documentación de AWS Config.

integración y entrega continuas (CI/CD)

El proceso de automatización de las etapas de origen, compilación, prueba, presentación y producción del proceso de lanzamiento del software. La CI/CD se describe comúnmente como una canalización. La CI/CD puede ayudarlo a automatizar los procesos, mejorar la productividad, mejorar la calidad del código y entregar con mayor rapidez. 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](#).

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 Marco de AWS Well-Architected. Para obtener más información, consulte [Clasificación de datos](#).

desviación de datos

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

datos en tránsito

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

minimización de datos

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

perímetro de datos

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

preprocesamiento de datos

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

procedencia de los datos

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

titular de los datos

Persona cuyos datos se recopilan y procesan.

almacenamiento de datos

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

lenguaje de definición de datos (DDL)

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

lenguaje de manipulación de datos (DML)

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

DDL

Consulte el [lenguaje de definición de bases de datos](#) 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. Cuando se adopta esta estrategia en AWS, se suman varios controles en diferentes capas de la estructura de AWS Organizations 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 miembro de AWS a fin de administrar las cuentas de la organización y los permisos para ese servicio. Esta cuenta

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

Implementación

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

entorno de desarrollo

[Consulte entorno.](#)

control de detección

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

asignación de flujos de valor para el desarrollo (DVSM)

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

gemelo digital

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

tabla de dimensiones

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

desastre

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

recuperación de desastres (DR)

La estrategia y el proceso que se utilizan para minimizar el tiempo de inactividad y la pérdida de datos ocasionados por un [desastre](#). Para obtener más información, consulte [Recuperación de desastres de cargas de trabajo en AWS: Recuperación en la nube](#) en un marco Well-Architected AWS.

DML

Consulte el [lenguaje de manipulación de bases](#) de datos.

diseño basado en el dominio

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

DR

Consulte [recuperación ante desastres](#).

detección de deriva

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

DVSM

Consulte [el mapeo del flujo de valor del desarrollo](#).

E

EDA

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

computación en la periferia

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

cifrado

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

clave de cifrado

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

endianidad

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

punto de conexión

[Consulte el punto final del servicio](#).

servicio de punto de conexión

Servicio que puede alojar en una nube privada virtual (VPC) para compartir con otros usuarios. Puede crear un servicio de punto de conexión con AWS PrivateLink y conceder permisos a otras Cuentas de AWS o para entidades principales de AWS Identity and Access Management (IAM). Estas cuentas o entidades principales pueden conectarse a su servicio de punto de conexión de forma privada mediante la creación de puntos de conexión de VPC de interfaz. Para obtener más información, consulte [Creación de un servicio de punto de conexión](#) en la documentación de Amazon Virtual Private Cloud (Amazon VPC).

cifrado de sobre

El proceso de cifrar una clave de cifrado con otra clave de cifrado. Para obtener más información, consulte [Cifrado de sobre](#) en la documentación de AWS Key Management Service (AWS KMS).

environment

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 una canalización de CI/CD, 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 de seguridad de AWS CAF incluyen la administración 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](#).

análisis de datos de tipo exploratorio (EDA)

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

F

tabla de datos

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

fallan rápidamente

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

límite de aislamiento de fallas

En elNube de AWS, un límite, como una zona de disponibilidadRegión de AWS, un plano de control o un plano de datos, que limita el efecto de una falla y ayuda a mejorar la resiliencia de las cargas de trabajo. Para obtener más información, consulte [Límites de AWS aislamiento](#) de errores.

rama de característica

Consulte la [sucursal](#).

características

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

importancia de las características

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

transformación de funciones

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

de aprendizaje a aprender patrones matizados asociados a los diferentes componentes de los datos.

FGAC

Consulte el control [de acceso detallado](#).

control de acceso preciso (FGAC)

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

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

G

bloqueo geográfico

Consulta [las restricciones geográficas](#).

restricciones geográficas (bloqueo geográfico)

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

Flujo de trabajo de Gitflow

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

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

H

JA

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.

migración homogénea de bases de datos

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

datos recientes

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

hotfix

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

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

laC

Vea [la infraestructura como código](#).

políticas basadas en identidad

Una política asociada a una o más entidades principales de IAM que define sus permisos en el entorno de la 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

Véase el [Internet industrial de las cosas](#).

infraestructura inmutable

Un modelo que implementa una nueva infraestructura para las cargas de trabajo de producción en lugar de actualizar, parchear o modificar la infraestructura existente. [Las infraestructuras](#)

[inmutables son intrínsecamente más consistentes, fiables y predecibles que las infraestructuras mutables](#). Para obtener más información, consulte las prácticas recomendadas para [implementar con una infraestructura inmutable](#) en Well-Architected FrameworkAWS.

VPC entrante (de entrada)

En una arquitectura de varias cuentas de AWS, una VPC que acepta, inspecciona y enruta las conexiones de red desde fuera de una aplicación. La [Arquitectura de referencia de seguridad de AWS](#) recomienda configurar su cuenta de red con VPC entrantes, salientes y de inspección para proteger la interfaz bidireccional entre su aplicación e Internet en general.

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.

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 del Internet de las cosas industrial \(IIoT\)](#).

VPC de inspección

En una arquitectura de varias cuentas de AWS, una VPC centralizada que administra las inspecciones del tráfico de red entre VPC (en la misma o en diferentes Regiones de AWS), Internet y las redes en las instalaciones. La [Arquitectura de referencia de seguridad de AWS](#) recomienda configurar su cuenta de red con VPC entrantes, salientes y de inspección para proteger la interfaz bidireccional entre su 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 más información, consulte [Interpretabilidad del modelo de machine learning con AWS](#).

IoT

[Consulte Internet de las cosas.](#)

biblioteca de información de TI (ITIL)

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

administración de servicios de TI (ITSM)

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

ITIL

Consulte la [biblioteca de información de TI](#).

ITSM

Consulte [Administración de servicios de TI](#).

L

control de acceso basado en etiquetas (LBAC)

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

zona de aterrizaje

Una zona de aterrizaje es un entorno de AWS correctamente diseñado, con varias cuentas, que es 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](#).

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

Ver [7 Rs](#).

sistema little-endian

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

entornos inferiores

[Véase entorno](#).

M

machine learning (ML)

Un tipo de inteligencia artificial que utiliza algoritmos y técnicas para el reconocimiento y el aprendizaje de patrones. El ML analiza y aprende de los datos registrados, como los datos del Internet de las cosas (IoT), para generar un modelo estadístico basado en patrones. Para más información, consulte [Machine learning](#).

rama principal

Ver [sucursal](#).

servicios gestionados

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

MAP

Consulte [Migration Acceleration Program](#).

mecanismo

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

cuenta de miembro

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

microservicio

Un servicio pequeño e independiente que se comunica a través de API bien definidas 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 [Integración de microservicios mediante servicios sin servidor de AWS](#).

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 API ligeras. 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)

Programa de AWS que brinda soporte de consultoría, capacitación y servicios para ayudar a las empresas a construir una base operativa sólida para migrar a la nube y 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 Migration Factory suelen incluir operadores, analistas de negocio y propietarios, 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 las subredes de destino, los grupos de seguridad y las cuentas de AWS.

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: Volver a alojar la migración en Amazon EC2 con AWS Application Migration Service.

Migration Portfolio Assessment (MPA)

Herramienta en línea que brinda 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 inicio de sesión) está disponible de forma gratuita para todos los consultores de AWS y los consultores asociados de APN.

Evaluación de la preparación para la migración (MRA)

Proceso que consiste en obtener información sobre el estado de preparación de la nube de una organización, identificar los puntos fuertes y débiles, y elaborar un plan de acción para cerrar las brechas identificadas, mediante 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 obtener más información, consulte la entrada de las [7 R](#) de este glosario y consulte [Movilice a su organización para acelerar las migraciones a gran escala](#).

ML

[Consulte el aprendizaje automático.](#)

MAPA

Consulte [la evaluación de la cartera de migración](#).

modernización

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

evaluación de la preparación para la modernización

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

brechas identificadas. Para obtener más información, consulte [Evaluación de la preparación para la modernización de las aplicaciones en la 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](#).

clasificación multiclase

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

infraestructura mutable

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

O

OAC

[Consulte el control de acceso de origen.](#)

OAI

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

OCM

Consulte [gestión del cambio organizacional](#).

migración fuera de línea

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

OI

Consulte [integración de operaciones](#).

OLA

Véase el [acuerdo a nivel operativo](#).

migración en línea

Método de migración en el que la carga de trabajo de origen se copia al sistema de destino sin que se desconecte. Las aplicaciones que están conectadas a la carga de trabajo pueden seguir funcionando durante la migración. Este método implica un tiempo de inactividad nulo o mínimo y, por lo general, se utiliza para cargas de trabajo de producción críticas.

acuerdo de nivel operativo (OLA)

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

revisión de la preparación operativa (ORR)

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

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

Registro de seguimiento creado por AWS CloudTrail que registra todos los eventos para todas las Cuentas de AWS en una organización en 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 migración de AWS, este marco se denomina aceleración de personas, debido a la velocidad de cambio requerida en 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 es compatible con todos los buckets de S3 en todas las Regiones de AWS, cifrado del servidor con AWS KMS (SSE-KMS), y solicitudes PUT y DELETE dinámicas 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.

O

Consulte la [revisión de la preparación operativa](#).

VPC saliente (de salida)

En una arquitectura de varias cuentas de AWS, una VPC que gestiona las conexiones de red que se inician desde una aplicación. La [Arquitectura de referencia de seguridad de AWS](#) recomienda configurar su cuenta de red con VPC entrantes, salientes y de inspección para proteger la interfaz bidireccional entre su aplicación e Internet en general.

P

límite de permisos

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

información de identificación personal (PII)

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

PII

Consulte la [información de identificación personal](#).

manual de estrategias

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

política

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

persistencia políglota

Elegir de forma independiente la tecnología de almacenamiento de datos de un microservicio en función de los patrones de acceso a los datos y otros requisitos. Si sus microservicios tienen la misma tecnología de almacenamiento de datos, pueden enfrentarse a desafíos de implementación o experimentar un rendimiento deficiente. Los microservicios se implementan más fácilmente y logran un mejor rendimiento y escalabilidad si utilizan el almacén de datos que mejor se adapte a sus necesidades. Para obtener más información, consulte [Habilitación de la persistencia de datos en los microservicios](#).

evaluación de cartera

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

predicate

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

pulsar un predicado

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

control preventivo

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

entidad principal

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

Privacidad desde el diseño

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

zonas alojadas privadas

Contenedor que aloja información acerca de cómo desea que responda Amazon Route 53 a las consultas de DNS de un dominio y sus subdominios en una o varias VPC. Para obtener más información, consulte [Uso de zonas alojadas privadas](#) en la documentación de Route 53.

control proactivo

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

entorno de producción

Consulte [entorno](#).

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.

Q

plan de consulta

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

regresión del plan de consulta

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

R

Matriz RACI

Véase [responsable, responsable, consultado, informado \(RACI\)](#).

ransomware

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

Matriz RASCI

Véase [responsable, responsable, consultado, informado \(RACI\)](#).

RCAC

Consulte control de [acceso por filas y columnas](#).

read replica

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

rediseñar

Ver [7 Rs](#).

objetivo de punto de recuperación (RPO)

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

objetivo de tiempo de recuperación (RTO)

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

refactorizar

Ver [7 Rs.](#)

Región

Conjunto de recursos de AWS que se encuentran en un área geográfica. Cada Región de AWS está aislada y es independiente de las demás para ofrecer tolerancia a errores, estabilidad y resistencia. Para obtener más información, consulte [Administración de Regiones de AWS](#) en Referencia general de AWS.

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

Ver [7 Rs.](#)

versión

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

trasladarse

Ver [7 Rs.](#)

redefinir la plataforma

Ver [7 Rs.](#)

recompra

Ver [7 Rs.](#)

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

Ver [7 Rs](#).

jubilarse

Ver [7 Rs](#).

rotación

Proceso de actualizar periódicamente un [secreto](#) para dificultar el acceso de un atacante a las credenciales.

control de acceso por filas y columnas (RCAC)

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

RPO

Consulte el [objetivo del punto de recuperación](#).

RTO

Consulte el [objetivo de tiempo de recuperación](#).

manual de procedimientos

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

S

SAML 2.0

Un estándar abierto que utilizan muchos proveedores de identidad (IdPs). Esta característica permite el inicio de sesión único (SSO) federado a fin de que los usuarios puedan iniciar sesión en la AWS Management Console o llamar a la API de AWS sin necesidad de crear un usuario de IAM para cada persona 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.

SCP

Consulte la [política de control de servicios](#).

secreta

Información confidencial o restringida, como una contraseña o credenciales de usuario, que almacene de forma cifrada. AWS Secrets Manager Se compone del valor secreto y sus metadatos. El valor secreto puede ser binario, una sola cadena o varias cadenas. Para obtener más información, consulte la documentación de [Secret](#) in the Secrets Manager.

control de seguridad

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

refuerzo de la seguridad

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

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

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

automatización de la respuesta de seguridad

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

cifrado del servidor

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

política de control de servicio (SCP)

Una política que proporciona un control centralizado de los permisos de todas las cuentas de una organización en AWS Organizations. Las SCP definen barreras de protección o establecen límites a las acciones que un administrador puede delegar en los usuarios o roles. Puede utilizar las SCP como listas de permitidos o rechazados, para especificar qué servicios o acciones se encuentra permitidos o prohibidos. Para obtener más información, consulte [Políticas de control de servicio](#) en la documentación de AWS Organizations.

punto de enlace de servicio

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

acuerdo de nivel de servicio (SLA)

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

indicador de nivel de servicio (SLI)

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

objetivo de nivel de servicio (SLO)

[Una métrica objetivo que representa el estado de un servicio, medido mediante un indicador de nivel de servicio.](#)

modelo de responsabilidad compartida

Modelo que describe la responsabilidad que comparte con AWS en cuanto a la conformidad y la seguridad en la nube. AWS es responsable de la seguridad de la nube, mientras que usted es responsable de la seguridad en la nube. Para obtener más información, consulte el [Modelo de responsabilidad compartida.](#)

SIEM

Consulte [la información de seguridad y el sistema de gestión de eventos.](#)

punto único de fallo (SPOF)

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

SLA

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

SLI

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

ASÍ QUE

Consulte el objetivo de [nivel de servicio.](#)

split-and-seed modelo

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

SPOF

Consulte el [punto único de falla.](#)

esquema en forma de estrella

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

patrón de higo estrangulador

Un enfoque para modernizar los sistemas monolíticos mediante la reescritura y el reemplazo gradual de las funciones del sistema hasta que se pueda 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.

cifrado simétrico

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

pruebas sintéticas

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

T

etiquetas

Pares de clave y valor que funcionan como metadatos para organizar los recursos de AWS. Las etiquetas pueden ayudarle a administrar, identificar, organizar, buscar y filtrar recursos. Para obtener más información, consulte [Etiquetado de los recursos de AWS](#).

variable de destino

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

lista de tareas

Herramienta que se utiliza para hacer un seguimiento del progreso mediante un manual de procedimientos. La lista de tareas contiene una descripción general del manual de procedimientos y una lista de las tareas generales que deben completarse. Para cada tarea general, se incluye la cantidad estimada de tiempo necesario, el propietario y el progreso.

entorno de prueba

Consulte [entorno](#).

entrenamiento

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

puerta de enlace de tránsito

Centro de tránsito de red que puede utilizar para interconectar las VPC y las redes en las instalaciones. Para obtener más información, consulte [¿Qué es una puerta de enlace de tránsito?](#) en la documentación de AWS Transit Gateway.

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

Concesión de permisos a un servicio que especifique para realizar tareas en su empresa en 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 [Uso de AWS Organizations con otros servicios de AWS](#) en la documentación de AWS Organizations.

ajuste

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

equipo de dos pizzas

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

U

incertidumbre

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

tareas indiferenciadas

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

entornos superiores

Ver [entorno](#).

V

succión

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

control de versión

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

Emparejamiento de VPC

Conexión entre dos VPC que 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 tibios

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

función de ventana

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

carga de trabajo

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

flujo de trabajo

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

GUSANO

Mira, [escribe una vez, lee muchas](#).

WQF

Consulte el [marco de calificación de cargas de trabajo de AWS](#).

escribe una vez, lee muchas (WORM)

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

Z

ataque de día cero

Un ataque, normalmente de malware, que aprovecha una vulnerabilidad de [día cero](#).

vulnerabilidad de día cero

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

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.