Aplicación automática de parches para instancias mutables en la nube híbrida mediante AWS Systems Manager

AWS Guía prescriptiva

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Guía prescriptiva: Aplicación automática de parches para instancias mutables en la nube híbrida mediante AWS Systems Manager

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

Aplicación automática de revisiones para instancias mutables en la nube híbrida mediante AWS Systems Manager

Chandra Allaka, Amazon Web Services (AWS)

Junio de 2020 (historial de documentos)

Esta guía prescriptiva describe una solución de aplicación automática de parches que utiliza Amazon Web Services (AWS) Systems Manager. Puede utilizar esta solución para aplicar revisiones a instancias mutables (de ejecución prolongada) de Amazon Elastic Compute Cloud (Amazon EC2) de Amazon Elastic Compute Cloud (Amazon EC2), que abarcan varias cuentas AWS y regionesAWS, así como a instancias en las instalaciones.

Esta guía está dirigida a los usuarios que participan en el diseño y la creación de capacidades operativas en un entorno de nube híbrida para que los equipos de aplicaciones puedan cumplir con las políticas de parches de sus empresas. Le proporciona un mecanismo de autoservicio para implementar parches previamente aprobados en sus servidores de aplicaciones.

En esta guía, se presupone una buena comprensión de los siguientes servicios AWS y conceptos:

- Systems Manager: proporciona una interfaz de usuario unificada para que pueda ver los datos operativos de varios servicios AWS y automatizar tareas operativas en todos sus recursos AWS.
- Systems Manager Inventory: proporciona visibilidad de su entorno informático en las instalaciones y de Amazon EC2. Puede utilizar Inventory para recopilar metadatos de las instancias administradas.
- Systems Manager Patch Manager: automatiza el proceso de aplicación de parches a instancias administradas con actualizaciones relacionadas con la seguridad y otros tipos de actualizaciones.
- Systems Manager Maintenance Windows: le permite definir una programación de periodos de mantenimiento para el momento en que realizar acciones potencialmente problemáticas en sus instancias, como por ejemplo, la aplicación de revisiones a un sistema operativo (SO), la actualización de los controladores o la instalación de software.
- AWS Lambda: con este, puede ejecutar código sin aprovisionar ni administrar servidores.

- Amazon QuickSight: le permite crear y publicar fácilmente paneles interactivos, que incluyen información sobre machine learning (ML). Puede acceder a los paneles desde cualquier dispositivo e integrarlos en sus aplicaciones, portales y sitios web.
- Tagging: puede asignar metadatos a los recursos AWS en forma de etiquetas. Cada etiqueta es una marca que consta de una clave y un valor definidos por el usuario. Las etiquetas pueden ayudarle a administrar, identificar, organizar, buscar y filtrar recursos.

Información general acerca de la administración de parches

Si se dedica a operaciones de aplicaciones o infraestructuras, entiende la importancia de una solución de revisión del sistema operativo (SO) que sea lo suficientemente flexible y escalable como para cumplir con los diversos requisitos de sus equipos de aplicaciones. En una organización típica, algunos equipos de aplicaciones utilizan una arquitectura que incluye instancias inmutables, mientras que otros implementan sus aplicaciones en instancias mutables.

La aplicación de revisiones de instancias inmutables implica la aplicación de las revisiones a las Imágenes de máquina de Amazon (AMI) que se utilizan para aprovisionar las instancias de aplicaciones EC2 inmutables. La aplicación de revisiones de instancias mutables implica la implementación de revisiones in situ en las instancias en ejecución durante un período de mantenimiento programado.

Esta guía prescriptiva describe cómo usar Patch Manager AWS Systems Manager para revisar instancias mutables que abarcan varias cuentas AWS y regiones AWS de forma automatizada, en función de los períodos de mantenimiento y los grupos de revisiones definidos por los equipos de aplicaciones en sus servidores mediante etiquetas.

La guía describe una solución de revisiones automatizada que utiliza AWS Lambda para automatizar las configuraciones y la programación de las revisiones mediante el administrador de revisiones y las ventanas de mantenimiento. Amazon QuickSight proporciona las funciones de informes y panel de control necesarias para informar sobre el cumplimiento de las revisiones.

Además, en esta guía se describe una arquitectura de referencia para entornos de nube híbrida. Los usuarios que ejecutan sus aplicaciones en una configuración de nube híbrida buscan oportunidades para consolidar, simplificar, estandarizar y optimizar sus operaciones de administración de revisiones en toda la AWS y en las la infraestructura en las instalaciones. La guía explica cómo se puede ampliar la solución de revisiones automatizada para instancias mutables para que sea compatible con escenarios de nube híbrida.

En esta guía se describe:

- Historias de usuarios clave sobre la administración de revisiones
- El proceso de aplicación de revisiones
- Administración de revisiones para instancias mutables en una sola cuenta y una sola región AWS; consideraciones y limitaciones de la arquitectura

- Administración de revisiones para instancias mutables en un entorno con varias cuentas y regiones; consideraciones y limitaciones de la arquitectura
- Administración de revisiones para instancias en las instalaciones en un entorno de nube híbrida; consideraciones y limitaciones arquitectónicas
- Principales partes interesadas, funciones y responsabilidades

> **Note**
>
> En esta guía, se describe la arquitectura de una solución automatizada (denominada solución de aplicación automática de revisiones) que puede implementar para cumplir con los requisitos de administración de revisiones en instancias mutables. No proporciona el código para crear la solución.

Términos y conceptos

Plazo	Definición
Instancias inmutables	Las instancias inmutables son instancias de servidor EC2 que no sufren ningún cambio mientras están en ejecución. Si es necesario realizar cambios, debe crear una nueva instancia con la imagen de servidor actualiza da, volver a implementar la instancia y destruir la imagen de servidor existente.
Línea de base de revisiones	La línea de base de revisiones es específica de un tipo de sistema operativo y define la lista de revisiones aprobadas para su instalación en las instancias. Para obtener más informaci ón, consulte Acerca de las líneas de base de revisiones predefinidas y personalizadas en la documentación de Systems Manager.
Grupo de revisiones	Un grupo de revisiones representa los servidores de un entorno de aplicaciones

Plazo	Definición
	que son objetivos de una línea de base de revisiones específica. Los grupos de revisione s ayudan a garantizar que las líneas de base de revisiones adecuadas se implementarán en el conjunto correcto de instancias. También pueden ayudarle a evitar la implementación de revisiones antes de que se hayan probado adecuadamente. Los grupos de revisiones se representan mediante la etiqueta Grupo de revisiones. Para obtener más información, consulte Acerca de los grupos de revisiones en la documentación de Systems Manager.
Maintenance window (Periodo de mantenimi ento)	El mantenimiento de windows le permite definir una programación para establecer el momento en que se realizarán acciones que pueden provocar interrupciones en las instancias, como la aplicación de parches en un sistema operativo, la actualización de controladores o la instalación de software o parches. Cada periodo de mantenimiento tiene una programac ión, una duración máxima, un conjunto de instancias de destinos registrados y un conjunto de tareas registradas. Las ventanas de mantenimiento se representan mediante la etiqueta Ventana de mantenimiento. Para obtener más información, consulte Acerca de los programas de aplicación de revisione s mediante ventanas de mantenimiento en la documentación de Systems Manager.

Historias de usuarios clave

El proceso típico de aplicación de revisiones al sistema operativo implica tres tareas:

1. Escanear las instancias EC2 y los servidores en las instalaciones en busca de las revisiones de sistema operativo aplicables.
2. Agrupar y aplicar revisiones a las instancias en el momento adecuado.
3. Informar sobre el cumplimiento de las revisiones en todo el entorno del servidor.

En la tabla siguiente se indican las principales historias de usuarios sobre gestión de revisiones.

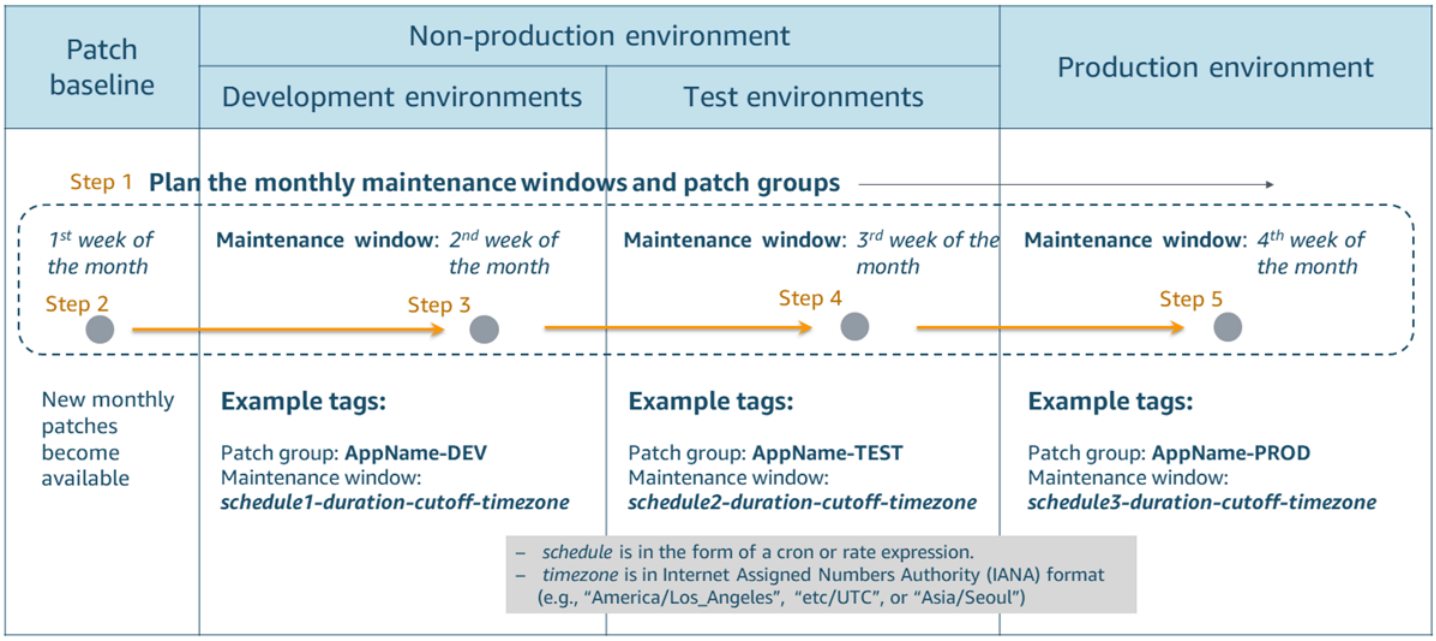
Escenario	Roles de usuario	Descripción
Mecanismo de aplicación de revisiones	Equipos de desarrollo y soporte de aplicaciones	Como miembro del equipo de aplicaciones responsable de aplicar revisiones al sistema operativo, necesito un mecanismo para revisar mis instancias mutables o de larga ejecución, de modo que pueda mitigar cualquier vulnerabilidad de seguridad del sistema operativo y también garantizar que las instancias cumplan con la línea de base de revisiones definida por el equipo de seguridad.
Solución de revisión	Propietario del servicio en la nube	Como propietario de un servicio en la nube y responsable de proporcionar servicios en la nube a los equipos de aplicaciones, necesito crear una solución de revisión del sistema operativo que sea compatible con varias cuentas AWS y regiones AWS, así como con servidores en las instalaciones, de modo que los equipos de aplicacio

Escenario	Roles de usuario	Descripción
		nes puedan mitigar cualquier vulnerabilidad de seguridad del sistema operativo y, además, cumplir con la línea de base de revisiones definida por el equipo de seguridad.
Informes de conformidad con la aplicación de revisiones	Director de operaciones de seguridad	Como gerente de operacion es de seguridad responsab le de garantizar el cumplimie nto de las revisiones, necesito informes e información detallados sobre el cumplimie nto de las revisiones en todo el entorno de la nube para poder identificar los servidore s que no cumplen con la línea de base de revisiones y alertar a los equipos para que implementen las medidas de mitigación necesarias.
Definición de funciones y responsabilidades	Propietario del servicio en la nube	Como propietario de un servicio en la nube, necesito crear una matriz de funciones y responsabilidades bien definida que explique quién se encarga de cada tarea a la hora de gestionar la solución de revisiones en la nube híbrida que he creado, de modo que se publiquen y cumplan las obligaciones relativas a las operaciones de aplicación de revisiones.

Proceso de revisión

Los principales usuarios de la solución de revisiones son los equipos de operaciones y desarrollo de aplicaciones. Por lo general, cada aplicación se implementa en varios entornos, como los de desarrollo, prueba (integración, aceptación del usuario, etc.) y producción. Los equipos de aplicaciones deben planificar los programas de aplicación de revisiones para cada entorno, de modo que cuando se aplique una revisión al entorno de producción, ya se haya probado y se haya determinado que no tiene efectos adversos en la aplicación.

El siguiente flujo de trabajo proporciona un ejemplo de cómo planificar las ventanas de aplicación de revisiones para una aplicación que se implementa en varios entornos y cómo configurar las etiquetas.



- Paso 1. Cada equipo de aplicaciones planifica las ventanas de mantenimiento de sus servidores en distintos entornos y configura las etiquetas que representan los grupos de revisiones y las ventanas de mantenimiento de los servidores en consecuencia:
  - La etiqueta Patch Group representa los servidores de un entorno de aplicaciones que son los objetivos de una línea de base de revisiones específica. Los grupos de revisiones ayudan a garantizar que las líneas de base de revisiones adecuadas se implementarán en el conjunto correcto de instancias. Los grupos de revisiones también le ayudan a evitar la implementación de revisiones en el entorno de producción antes de que estos se hayan probado suficientemente.

- Si los servidores de aplicaciones incluyen varios sistemas operativos, el equipo de aplicaciones crea grupos de revisiones en función de la combinación del entorno y del sistema operativo. Un grupo de revisiones puede registrarse con solo una línea de base de revisiones y una instancia puede formar parte de solo un grupo de revisiones.

  Por ejemplo: *appname*`-DEV-WIN` y *appname*`-DEV-RHEL`

- La etiqueta Ventana de mantenimiento representa el calendario de aplicación de revisiones a los servidores. Todos los servidores de un grupo de revisiones deben estar en el mismo período de mantenimiento. La etiqueta de la ventana de mantenimiento debe seguir un formato coherente para las expresiones de frecuencia y cronológicas, de modo que la función de Lambda que defina pueda analizar las expresiones fácilmente. (En esta guía, nos referiremos a esta función de Lambda como `automate-patch`).

  Por ejemplo: *schedule-duration-cutoff-timezone*

  `cron(0 2 ? * SAT#3 *)` representa a las 02:00 a.m. del tercer sábado de cada mes. Para obtener información detallada acerca de las expresiones de frecuencia y cronológicas, consulte la documentación de Systems Manager.

- Paso 2. Systems Manager Patch Manager hace que las nuevos revisiones estén disponibles periódicamente a través de líneas de base de revisiones específicas del sistema operativo en función de las configuraciones definidas.
  - Para cada sistema operativo, puede definir una línea de base de revisiones personalizada que incluya las reglas de aprobación y las revisiones que deben aplicarse a las instancias del entorno de la nube.
- Paso 3. Su código de automatización personalizado configura Patch Manager para configurar las revisiones en función de las etiquetas del grupo de revisiones y de la ventana de mantenimiento, y aplica las revisiones al entorno de desarrollo.
  - Una vez finalizada la aplicación de revisiones, los equipos de desarrollo y soporte de la aplicación prueban la aplicación y comprueban que todo funciona correctamente.
  - Si la aplicación encuentra algún problema con la nueva revisión, los equipos de aplicaciones piden al equipo de servicios en la nube que deje de aplicar revisiones a otros grupos de revisiones y a otros entornos, desactivando los períodos de mantenimiento o anulando el registro de la ejecución de la tarea de la revisión.
- Paso 4. Una vez que el entorno de desarrollo se ha revisado correctamente, las revisiones se implementan en cualquier otro entorno que no sea de producción. Al igual que en el entorno de

desarrollo, se prueba y se verifica que la aplicación funcione correctamente en todos los entornos que no son de producción. Si hay algún problema, los equipos de aplicaciones piden al equipo de servicios en la nube que deje de aplicar revisiones al entorno de producción.

- Paso 5. Una vez que todos los entornos que no son de producción se hayan revisado correctamente, las revisiones se aplican al entorno de producción.

Diseño de solución de revisiones para instancias EC2 mutables

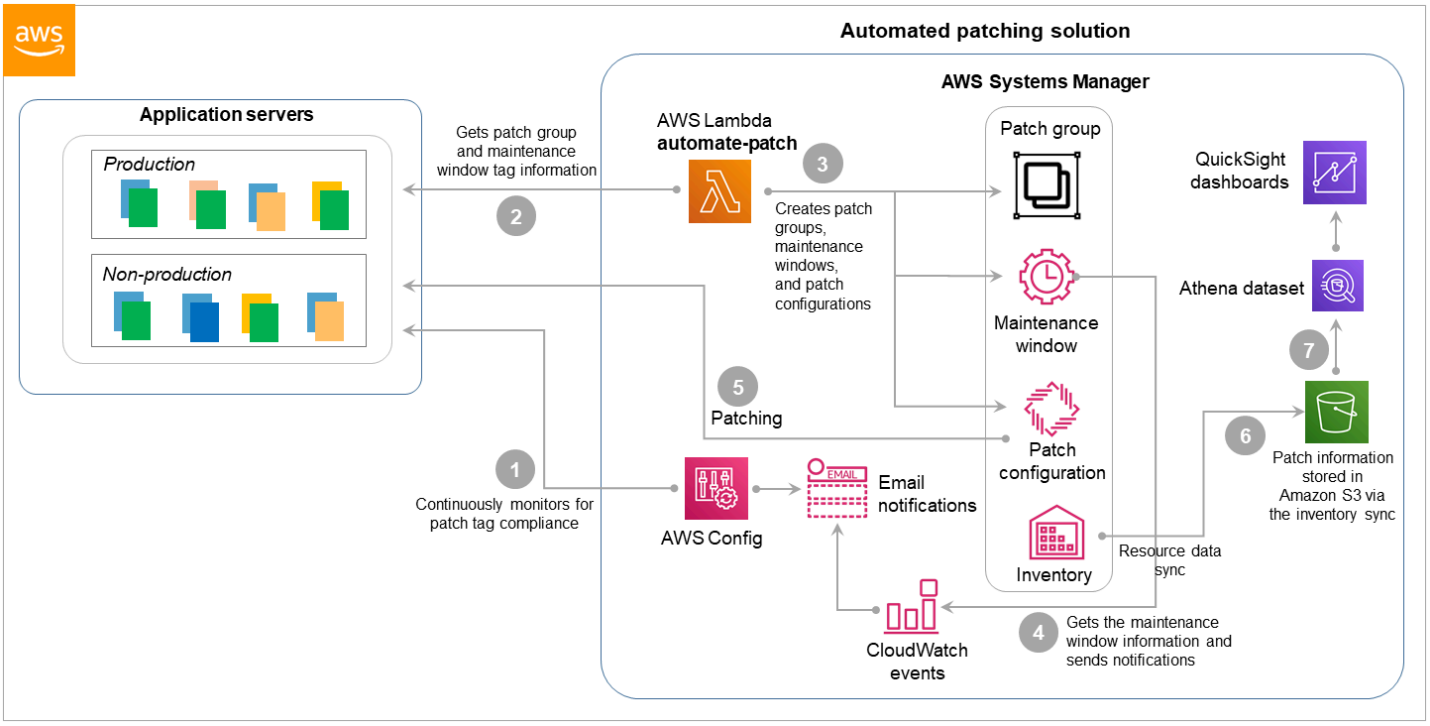
El proceso de aplicación de revisiones para las instancias mutables implica los siguientes equipos y acciones:

- Los equipos de aplicaciones (DevOps) definen los grupos de revisiones para sus servidores en función del entorno de la aplicación, el tipo de sistema operativo u otros criterios. También definen los períodos de mantenimiento específicos de cada grupo de revisiones. Esta información se almacena en las etiquetas del grupo de revisiones y de la ventana de mantenimiento de las instancias de la aplicación EC2. Durante cada ciclo de revisiones, los equipos de aplicaciones se preparan para aplicar las revisiones, prueban la aplicación después de aplicarlos y solucionan cualquier problema con sus aplicaciones y su sistema operativo durante la aplicación de las revisiones.
- El equipo de operaciones de seguridad define la línea de base de revisiones para los distintos tipos de sistemas operativos que utilizan los equipos de aplicaciones, aprueba las revisiones y los pone a disposición a través de Systems Manager Patch Manager.
- La solución de revisiones automatizada se ejecuta de forma regular e implementa las revisiones definidas en la línea de base de revisiones en función de los grupos de revisiones definidas por el usuario y los períodos de mantenimiento. La información sobre la conformidad de las revisiones se obtiene mediante una sincronización de datos de recursos en el inventario de Systems Manager y se utiliza para la elaboración de informes sobre la conformidad de las revisiones a través de los paneles de Amazon QuickSight.
- Los equipos de gobierno y conformidad definen las directrices de aplicación de revisiones, definen los procesos y mecanismos de excepción y obtienen los informes de conformidad de Amazon QuickSight.

Para obtener información detallada sobre las principales partes interesadas que intervienen en una solución exitosa de administración de revisiones del sistema operativo y sus responsabilidades, consulte la sección sobre las principales partes interesadas, funciones y responsabilidades más adelante en esta guía.

Proceso automatizado

La solución de revisiones automatizada utiliza varios servicios AWS que funcionan en conjunto para implementar las revisiones en las instancias de EC2. En este proceso se incluyen AWS Config, AWS Lambda, Systems Manager, Amazon Simple Storage Service (Amazon S3), y Amazon QuickSight. En el siguiente diagrama se muestra la arquitectura de referencia y el flujo de trabajo.



El flujo de trabajo incluye estos pasos, donde los números de los pasos coinciden con los rótulos del diagrama:

1. AWS Config supervisa continuamente lo siguiente y envía notificaciones con los detalles de las instancias no conformes y las configuraciones necesarias:
   - Cumplimiento del etiquetado de revisiones en las instancias EC2. AWS Configcomprueba las instancias que no tienen etiquetas de grupo de revisiones ni de ventana de mantenimiento.
   - El perfil de instancia AWS Identity and Access Management (IAM) con la función Systems Manager, que permite a Systems Manager gestionar las instancias.
2. La función de Lambda (la llamaremos `automate-patch`) se ejecuta según un programa predefinido y recopila la información del grupo de revisiones y la ventana de mantenimiento de todos los servidores.

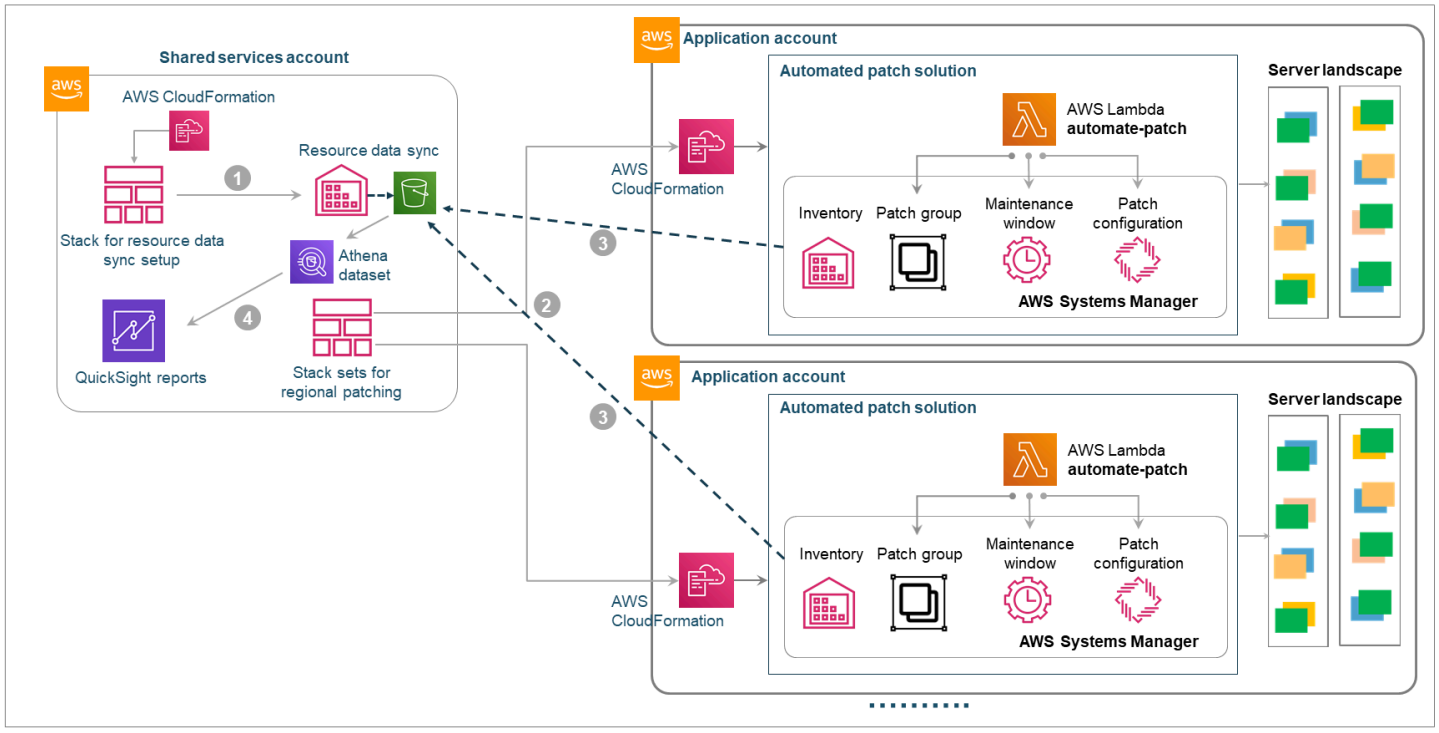
3. A continuación, la función `automate-patch` crea o actualiza los grupos de revisiones y las ventanas de mantenimiento correspondientes, asocia los grupos de revisiones a las líneas base de revisiones, configura el análisis de revisiones y despliega la tarea de aplicación de revisiones. De forma opcional, la función `automate-patch` también crea Eventos de Amazon CloudWatch para notificar a los usuarios de las revisiones inminentes.
4. En función de los períodos de mantenimiento, los eventos envían notificaciones de revisiones a los equipos de aplicaciones con los detalles de la inminente operación de aplicación de revisiones.
5. Patch Manager realiza las revisiones del sistema en función del cronograma definido y de los grupos de revisiones.
6. Una sincronización de datos de recursos en Systems Manager Inventory recopila los detalles de las revisiones y los publica en un bucket de S3.
7. Los informes y los paneles de conformidad de las revisiones están integrados en Amazon QuickSight a partir de la información del bucket S3.

Diseño de solución de revisiones para múltiples cuentas AWS y regiones

Puede ampliar la solución de revisiones automatizados para que sea compatible con servidores que abarquen varias cuentas AWS y varias regiones AWS. La solución ampliada implica configurar la solución de automatización de revisiones en cada cuenta AWS mediante StackSets AWS CloudFormation en una cuenta de servicios compartidos y configurar una sincronización de datos de recursos entre las cuentas con la cuenta de servicios compartidos.

Proceso automatizado

En el siguiente diagrama se ilustra la arquitectura de este escenario. Esta arquitectura incluye StackSets AWS CloudFormation y una cuenta de servicio compartida AWS.



El flujo de trabajo es similar al proceso descrito en la sección anterior, pero incluye los siguientes pasos adicionales, en los que los números de los pasos coinciden con los rótulos del diagrama:

1. En la cuenta de servicios compartidos, se utiliza un conjunto de pilas AWS CloudFormation para configurar el bucket de S3 para la sincronización de los datos de los recursos a través de Systems Manager Inventory.
2. El conjunto de pilas de CloudFormation crea la pila con la función de Lambda `automate-patch`, configura las líneas de base de revisiones y configura la sincronización de los datos de los recursos de inventario de Systems Manager en las cuentas de la aplicación para sincronizar los recursos de la cuenta de servicios compartidos.
3. La información de recursos de las cuentas de la aplicación se sincroniza con la información de recursos de la cuenta de servicios compartidos.
4. Amazon QuickSight genera informes de conformidad con las revisiones utilizando el conjunto de datos de Amazon Athena para la información de recursos sincronizada.

Condiciones y limitaciones de la arquitectura

Tiempos de mantenimiento por cuenta

La arquitectura ilustrada y descrita en la sección anterior crea una ventana de mantenimiento para cada grupo de revisiones. Sin embargo, la cuota de períodos de mantenimiento por cuenta AWS es de 50 (suponiendo que no haya solicitado un aumento de la cuota de servicio). Si espera que el número de grupos de revisiones supere los 50 grupos en una sola cuenta AWS, esta arquitectura no se escalará a sus necesidades.

Si un aumento de la cuota de servicio no es suficiente para sus necesidades, hay dos opciones para gestionar este desafío: usar ventanas de mantenimiento predefinidas y usar CloudWatch Events. Aquí están las ventajas y desventajas de cada enfoque.

Opción 1. Utilice ventanas de mantenimiento predefinidas

- Defina una lista de períodos de mantenimiento con varios intervalos de tiempo (por ejemplo, de 15 a 20 períodos de mantenimiento por cuenta).
- Los equipos de aplicaciones eligen los períodos de mantenimiento que más les convengan de la lista predefinida y etiquetan las instancias en consecuencia.
- Actualice la solución de revisiones automatizada para asignar los grupos de revisiones a las ventanas de mantenimiento seleccionadas, en lugar de crear nuevas ventanas de mantenimiento.

Ventajas:

- Administración simplificada.

Desventajas:

- Menor flexibilidad para definir ventanas de mantenimiento personalizadas.
- Cuando varios grupos de revisiones comparten períodos de mantenimiento y tareas de revisiones, cancelar una tarea de revisión específica para un grupo de revisiones específico requiere un esfuerzo manual adicional.

Opción 2. Utilice CloudWatch Events para activar tareas de revisiones en lugar de utilizar ventanas de mantenimiento

- En lugar de crear ventanas de mantenimiento, utilice CloudWatch Events para activar las tareas de revisiones en función de la programación y los grupos de revisiones.
- En este escenario, cada grupo de revisiones está asociado a un evento de CloudWatch Events en lugar de a un período de mantenimiento.
- Actualice la solución de revisiones automatizada para crear eventos en lugar de ventanas de mantenimiento.

Ventajas:

- Diseño escalable.
- Proporciona flexibilidad para definir ventanas de mantenimiento personalizadas.

Desventajas:

- Los períodos de mantenimiento proporcionan funciones adicionales (como la duración y las horas límite) que no están disponibles en CloudWatch Events.

Otras consideraciones

- La solución de revisiones automatizados que se describe en esta sección no es compatible con las instancias EC2 que están cerradas.

- Este proceso admite instancias EC2 en subredes públicas. Para aplicar revisiones a las instancias en subredes privadas, debe implementar un repositorio de revisiones local, como Windows Server Update Services (WSUS).
- Debe ajustar la frecuencia de ejecución de la función de Lambda para que los grupos de revisiones y las ventanas de mantenimiento se actualicen según la programación requerida.

Diseño de solución de revisiones para instancias en las instalaciones en un entorno de nube híbrida

También puede ampliar la solución descrita en esta guía para aplicar revisiones a las instancias de servidor en las instalaciones en un entorno de nube híbrida.

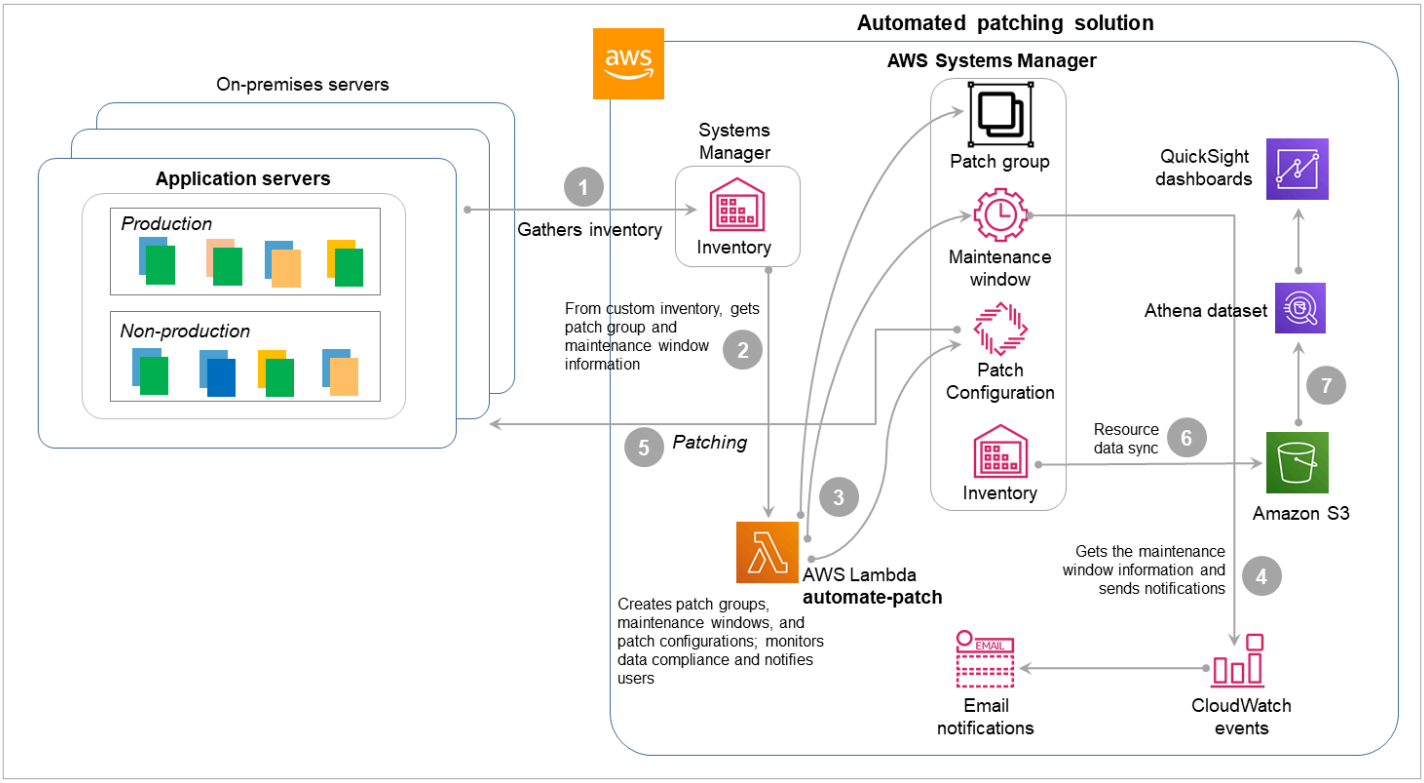
El proceso de aplicación de revisiones estándar para las instancias en las instalaciones consta de dos pasos:

- Los servidores en las instalaciones se configuran para que sean administrados por Systems Manager. Para obtener información detallada sobre este proceso, consulte Configuración de Systems Manager para entornos híbridos en la documentación de Systems Manager.
- Para configurar el grupo de revisiones y las etiquetas de ventana de mantenimiento adecuadas para estas instancias gestionadas en las instalaciones, utilice el comando AWS Command Line Interface (AWS CLI) add-tags-to-resource.

Sin embargo, este enfoque requiere que el equipo de aplicaciones o el equipo de la nube ejecuten manualmente los comandos AWS CLI siempre que quieran realizar cambios en los grupos de revisiones o en las ventanas de mantenimiento.

Proceso automatizado

En la siguiente ilustración, se describe un enfoque alternativo para aplicar revisiones a las instancias en las instalaciones que utiliza la opción de inventario personalizado de Systems Manager. Este proceso es una extensión de la solución de revisiones automatizadas que describimos anteriormente para las instancias EC2 mutables.



1. En lugar de usar etiquetas, Systems Manager captura la información de revisiones (grupos de revisiones y ventanas de mantenimiento) de las instancias administradas en las instalaciones mediante una colección de inventario personalizada.

```
Sample custom inventory JSON file
{
    "SchemaVersion": "1.0",
    "TypeName": "Custom:PatchInformation",
    "Content": {
        "Patch Group": "<APP-PROD>",
        "Maintenance Window": "XXX"
    }
}
```

2. La función de Lambda `automate-patch` se ejecuta todos los días, recopila la información del grupo de revisiones y la ventana de mantenimiento del inventario personalizado del servidor en las instalaciones y crea las etiquetas del grupo de revisiones y la ventana de mantenimiento en las instancias administradas.
3. A continuación, la función de Lambda `automate-patch` crea o actualiza los grupos de revisiones y las ventanas de mantenimiento adecuados, asocia los grupos de revisiones a las líneas de

base de revisiones, configura los escaneos de revisiones e implementa la tarea de revisiones en función del inventario personalizado que se recopiló. De forma opcional, la función `automate-patch` también crea eventos en CloudWatch Events para notificar a los usuarios de las revisiones inminentes.

4. En función de los períodos de mantenimiento, los eventos envían notificaciones de revisiones a los equipos de aplicaciones con los detalles de la inminente operación de aplicación de revisiones.
5. Patch Manager realiza las revisiones del sistema en función del cronograma definido y de los grupos de revisiones.
6. Una sincronización de datos de recursos en Systems Manager Inventory recopila los detalles de las revisiones y los publica en un bucket de S3.
7. Los informes y los paneles de conformidad de las revisiones están integrados en Amazon QuickSight a partir de la información del bucket S3.

Condiciones y limitaciones de la arquitectura

Como se ha explicado en las secciones anteriores, existen dos enfoques para aplicar revisiones a las instancias en las instalaciones: mediante un inventario personalizado o mediante etiquetas. Aquí están las ventajas y desventajas de cada enfoque.

Opción 1. Usa un inventario personalizado para obtener información sobre las revisiones

- Los equipos de aplicaciones que trabajan con servidores en las instalaciones configuran la información de las revisiones en el archivo de inventario personalizado y Systems Manager selecciona esa información.
- A continuación, la información de las revisiones del inventario personalizado se utiliza para crear las tareas de las revisiones.

Ventajas:

- Es mucho más fácil de configurar porque solo implica una actualización de archivos.

Desventajas:

- Los cambios en la configuración de las revisiones se limitan al calendario de recogida de inventario.

Opción 2. Usa etiquetas para las instancias administradas en las instalaciones

- Los equipos de aplicaciones que trabajan con servidores en las instalaciones crean etiquetas de grupo de revisiones y ventanas de mantenimiento utilizando la información de revisiones adecuada AWS CLI.
- La información de las etiquetas se utiliza para crear las tareas de revisiones.

Ventajas:

- Un enfoque coherente en todas las instalaciones AWS y en las instalaciones para impulsar la estandarización y la automatización de las revisiones.

Desventajas:

- Los equipos de aplicaciones que trabajan con instancias en las instalaciones tienen que aprender a crear o actualizar AWS CLI para crear o actualizar las etiquetas.

Principales partes interesadas, funciones y responsabilidades en la administración de parches

Para que la gestión de parches del sistema operativo tenga éxito, es necesario tener bien definidas las funciones y responsabilidades para dar soporte a su solución automatizada de parches y optimizarla continuamente. En esta sección, se describen las funciones y responsabilidades sugeridas que puede modificar según sus necesidades y su estructura organizativa.

Personas usuarias

En la siguiente tabla se describen las personas usuarias que intervienen en la solución de aplicación automática de parches.

Persona de usuario	Descripción
Consumidores (C)	La solución de administración de parches para instancias de ejecución prolongada la utilizan diferentes equipos que participan en la administración del sistema operativo, entre los que se incluyen: • Equipos de desarrollo que gestionan entornos de aplicaciones completos. • Equipos de operaciones que administran el sistema operativo del servidor de aplicacio nes.
Ingeniería en la nube (CE)	El equipo responsable de: • Optimizar continuamente la solución de administración de parches. • Construir la automatización de los servicios en la nube. • Apoyando la automatización.
Oficina empresarial en la nube (CBO)	El equipo que participa en:

Persona de usuario	Descripción
	• Administrar la experiencia del consumidor para la solución. • Habilitación y participación de los usuarios. • Asegurarse de que la solución de parches satisfaga las necesidades de los consumido res.
Propietario del servicio/producto (CPO) en la nube	La persona responsable de: • Proporcionar servicios en la nube a los consumidores • Trabajar en estrecha colaboración con el equipo directivo para alinear la prestación de servicios con las expectativas y las directric es • Gestionar todas las expectativas y escalamie ntos de los clientes relacionados con la plataforma • Ser propietario de la hoja de ruta de la plataforma
Operaciones de seguridad (SO)	Equipo que gestiona las bases de referencia y las aprobaciones de los parches
Director de operaciones de seguridad (SOM)	Administrador responsable del cumplimiento de los parches

Matriz RACI

La matriz “responsables, encargados, consultados e informados” (RACI, por sus siglas en inglés) especifica las actividades que implica la solución de administración de parches. Para cada paso del proceso, enumera las partes interesadas y su participación:

- R: responsable de completar el paso

- A: encargado de aprobar y terminar el trabajo
- C: se le consulta para proporcionar información para una tarea
- I: informado del progreso, pero sin estar directamente involucrado en la tarea

Solución de gestión de parches	CPO	CBO	CE	SO	SOM	C
Ejecución de la hoja de ruta del producto de gestión de parches	A	C	R	C	C	I
Arquitectura y diseño de administración de parches	A	I	R	C	I	
Gestión del desarrollo y la configuración de parches	A		R	C		
Validación y pruebas de la administración de parches	A	I	R	I	I	

Solución de gestión de parches	CPO	CBO	CE	SO	SOM	C
Incorporación de nuevas cuentas AWS, aplicaciones y servidores para la aplicación de parches	A	C	R	I		
Participación y habilitación de usuarios	A	R	I	I	I	
Gestión de la escalación y los comentarios de los usuarios	A	R		I	I	
Gestión de cambios de productos	A	R	C	I		

Solución de gestión de parches	CPO	CBO	CE	SO	SOM	C
Gestión y resolución de problemas	A		R	C		
Aplicación de parches y cumplimiento de los parches en los servidores			C	C		AR
Configuración de línea de base de parches			C	R	A	C
Informes y cumplimiento de los parches			C	R	AR	I

Pasos siguientes

En esta guía, se describe una solución de aplicación automática de parches para instancias mutables en AWS y en las instalaciones en un entorno de nube híbrida. Para crear la solución, le recomendamos que consulte la documentación de los servicios AWS descritos en esta guía. Si tiene alguna pregunta, póngase en contacto con su equipo de cuentas AWS para obtener ayuda.

Para obtener más información, consulte la sección Recursos adicionales.

Recursos adicionales

Recursos de AWS

- Recomendaciones de AWS
- Documentación de AWS
- referencia general de AWS
- glosario de AWS

Servicios de AWS

- AWS CloudFormation
- Amazon CloudWatch
- Amazon EC2
- IAM
- AWS Lambda
- Amazon QuickSight
- AWS Systems Manager

Otros recursos

- Cómo aplicar revisiones a las instancias de Amazon EC2 en subredes privadas mediante AWS Systems Manager (blog de administración y gobierno AWS)
- Cómo Moody utiliza AWS Systems Manager para revisiones los servidores de varios proveedores de nube (blog sobre administración y gobierno AWS)
- Configuración de AWS Systems Manager para entornos híbridos (Systems Manager Documentation)
- Aplicación de revisiones centralizada en varias cuentas y regiones con automatizaciónAWS Systems Manager (blog de administración y gobernanza de AWS)
- Cómo aplicar revisiones a las instancias de Amazon EC2 mediante AWS Systems ManagerPatch Manager (blog sobre administración y gobernanza AWS)
- Cómo aplicar revisiones, inspeccionar y proteger las cargas de trabajo de Microsoft Windows en AWS–Parte 1 (blog de seguridad AWS)

Historial de documentos

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

Cambio	Descripción	Fecha
Publicación inicial	—	12 de junio 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.

antipatrones

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

control de aplicaciones

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

cartera de aplicaciones

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

inteligencia artificial (IA)

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

operaciones de inteligencia artificial (AIOps)

El proceso de utilizar técnicas de machine learning para resolver problemas operativos, reducir los incidentes operativos y la intervención humana, y mejorar la calidad del servicio. Para obtener más información sobre cómo 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
- Reinvención: 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 oAWS 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.

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 GuardDutyAWS 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

IaC

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

subred

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

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 version original de inglés, prevalecerá la version en inglés.