Guía de registro y monitoreo para propietarios de aplicaciones

AWS Guía prescriptiva

AWS Guía prescriptiva: Guía de registro y monitoreo para propietarios de aplicaciones

Table of Contents

Guía de registro y monitoreo para propietarios de aplicaciones

John Buckley, Amazon Web Services (AWS)

Enero de 2023 (historial de documentos)

Una carga de trabajo es un conjunto de recursos y código que ofrece valor comercial, como una aplicación orientada al cliente o un proceso de backend. Una carga de trabajo puede consistir en un subconjunto de recursos en una sola Cuenta de AWS o puede abarcar varias Cuentas de AWS. En la nube, una aplicación es un tipo de carga de trabajo. Puede implementarse exclusivamente en el entorno de nube o también puede ser compatible con el equipo local y en las instalaciones. Muchas publicaciones se centran en el registro y el monitoreo de la infraestructura de la nube y están destinadas a los equipos de seguridad. Esta guía está destinada a los propietarios de aplicaciones y se centra en los enfoques eficaces y eficientes para registrar y monitorear las aplicaciones en la Nube de AWS.

Esta guía ayuda a configurar el registro y el monitoreo en un nivel adecuado para que pueda identificar las anomalías y responder a ellas rápidamente. También ayuda a asegurarse de que los registros de las aplicaciones permitan un análisis detallado y la resolución de cualquier problema.

Aunque esta guía está escrita teniendo en cuenta las implementaciones de Nube de AWS, puede aplicar estos principios a las aplicaciones que se ejecutan en las instalaciones o en la infraestructura de otro proveedor de servicios en la nube.

Resultados empresariales específicos

Después de leer esta guía debería poder comprender:

- Los tipos de eventos que suelen registrarse en las aplicaciones
- Los atributos del evento (como quién, qué y cuándo) que debería considerar registrar
- Los tipos de datos que debería considerar excluir de los registros, como los datos que puedan comprometer su postura de seguridad o la información de identificación personal
- Cómo configurar el registro y el monitoreo en un nivel adecuado para su aplicación
- Quién debería poder administrar los registros de su aplicación y acceder a ellos

- Los Servicios de AWS y las características que puede configurar para monitorear y registrar sus aplicaciones en la Nube de AWS
- Cómo utilizar los datos de registro de su aplicación y los Servicios de AWS y las características para clasificar y diagnosticar problemas

Acerca del registro y el monitoreo de aplicaciones

El registro, el monitoreo, las alertas y los informes son procesos de seguridad diferentes que funcionan juntos para aportar visibilidad del estado y el rendimiento de su aplicación. Es fundamental que cree y mantenga un registro detallado de las acciones y los eventos de su aplicación, de modo que pueda monitorear, alertar e informar en función de la actividad registrada.

El registro de aplicaciones es el proceso de recopilar los eventos generados por la aplicación y registrarlos en uno o más archivos de registro. Este historial de eventos puede ayudarlo a realizar análisis de seguridad y rendimiento, realizar un seguimiento de los cambios en los recursos y solucionar problemas de las aplicaciones.

Monitoreo de aplicaciones es el proceso de evaluar el rendimiento y el estado generales de su aplicación. Debería poder monitorear el frontend y el backend de la aplicación constantemente. Como las aplicaciones alojadas en la nube están muy distribuidas, las herramientas de registro y monitoreo pueden ayudarlo a solucionar rápidamente los problemas de rendimiento o a identificar y corregir las amenazas de seguridad en tiempo real. Los datos de registro son una entrada fundamental para el monitoreo.

La observabilidad es similar al monitoreo, pero presenta formas de medir el comportamiento de las aplicaciones mediante distintos parámetros y permite establecer correlaciones complejas. Un ejemplo es medir la tasa de éxito de HTTP en un día determinado, para un conjunto de usuarios de una región geográfica específica. Para obtener más información, consulte Monitoreo y observabilidad (marketing de AWS).

En última instancia, el objetivo de los propietarios de las aplicaciones es mantener las aplicaciones seguras y en buen estado, y brindar una experiencia de usuario positiva con esas aplicaciones. Al implementar el registro y el monitoreo, sus desarrolladores y equipos de operaciones pueden planificar y solucionar los problemas de las aplicaciones con mayor rapidez.

El nivel de registro y monitoreo necesarios varía para cada aplicación. Entre los factores que pueden afectar a los niveles de monitoreo y registro, se incluyen las políticas y los procedimientos de la organización, el nivel de riesgo de seguridad que supone la aplicación, su importancia para las operaciones empresariales y la confidencialidad de los datos que maneja la aplicación. En general, las aplicaciones públicas o orientadas al cliente requieren un mayor nivel de monitoreo y registro que las aplicaciones que se utilizan internamente en la organización. En esta guía, se incluye información general y recomendaciones, y debe personalizar su enfoque en función de los requisitos de su aplicación.

> **Note**
>
> Los estándares o procedimientos de su organización pueden exigir atributos específicos de registro y monitoreo. Un ejemplo es transferir los permisos de los usuarios a un sistema empresarial de revisión de derechos. Asegúrese de que su plan de registro y monitoreo aborde los requisitos de su organización.

Registro de aplicaciones en la Nube de AWS

Para registrar aplicaciones en la Nube de AWS, revise los tipos de eventos más comunes, los atributos de los eventos y las prácticas recomendadas.

Esta sección se incluyen los siguientes temas:

- Event types (Tipos de eventos)
- Atributos del evento
- Prácticas recomendadas de registro

Event types (Tipos de eventos)

Una de las consideraciones más importantes a la hora de establecer una estrategia de registro de aplicaciones es decidir qué eventos y acciones se van a registrar. Si bien los requisitos de su organización y aplicación pueden afectar a esta decisión, le recomendamos que registre siempre lo siguiente si se aplica a su aplicación:

- Errores de validación de entradas: algunos ejemplos son las infracciones del protocolo, las codificaciones inaceptables y los nombres y valores de los parámetros no válidos.
- Errores de validación de salida: algunos ejemplos son las discordancias de los conjuntos de registros de la base de datos y la codificación de datos no válida.
- Éxitos y fracasos en la autenticación de identidad: registre las actividades de autenticación, pero no registre los nombres de usuario y las contraseñas. Como los usuarios pueden escribir accidentalmente sus contraseñas en un campo de nombre de usuario, le recomendamos que no registre los nombres de usuario. Esto podría exponer las credenciales de forma no intencionada y provocar el acceso autorizado. Implemente controles de seguridad para todos los registros que contengan datos de autenticación.
- Errores de autorización (control de acceso): en el caso de los sistemas de autorización relacionados, registre los intentos de acceso fallidos. Puede monitorear estos datos de registro para detectar patrones que puedan indicar un ataque o problemas con el sistema de autorización de la aplicación.
- Errores de administración de sesiones: algunos ejemplos incluyen la modificación de las cookies o los tokens de sesión. Las aplicaciones suelen utilizar cookies o tokens para administrar los estados de los usuarios. Los usuarios malintencionados pueden intentar modificar los valores de

las cookies para obtener acceso no autorizado. El registro de los tokens de sesión manipulados brinda una forma de detectar este comportamiento.

- Errores de aplicación y eventos del sistema: algunos ejemplos son los errores de sintaxis y tiempo de ejecución, los problemas de conectividad, los problemas de rendimiento, los mensajes de error de servicios de terceros, los errores del sistema de archivos, la detección de virus al cargar archivos y los cambios de configuración.
- Estado de la aplicación: iniciar o detener la aplicación y sus recursos relacionados.
- Estado del registro: iniciar, detener o pausar el registro.
- Uso de características de mayor riesgo: algunos ejemplos son los cambios en la conexión de red, la adición o eliminación de usuarios, el cambio de privilegios, la asignación de usuarios a tokens, la adición o eliminación de tokens, el uso de privilegios administrativos del sistema, el acceso por parte de los administradores de aplicaciones, todas las acciones realizadas por los usuarios con privilegios administrativos, el acceso a los datos de los titulares de tarjetas de pago, el uso de claves de cifrado de datos, el cambio de las claves de cifrado, la creación y eliminación de objetos a nivel del sistema, el envío de contenido generado por los usuarios (especialmente la carga de archivos) y la importación y exportación de datos (incluidos los informes).
- Opciones legales y de otro tipo: los ejemplos incluyen permisos para capacidades de teléfonos móviles, términos de uso, términos y condiciones, consentimiento de uso de datos personales y permisos para recibir comunicaciones de marketing.

Además de los atributos recomendados para su aplicación, considere qué atributos adicionales podrían aportar datos útiles para monitoreo, las alertas y los informes. Entre los ejemplos se incluyen:

- Errores de secuenciación
- Atributos que lo ayudan a evaluar el comportamiento de los usuarios que infringe la política de uso aceptable de su organización
- Cambios de datos
- Atributos necesarios para cumplir con las normas o reglamentos, como prevenir los delitos financieros, limitar la negociación de acciones o recopilar información de salud u otro tipo de información personal.
- Atributos que ayudan a identificar comportamientos sospechosos o inesperados, como los intentos de realizar acciones no autorizadas
- Cambios de configuración

- Cambios en la memoria o en el archivo de código de la aplicación

Atributos del evento

Cada entrada de registro debe incluir información suficientemente detallada para el monitoreo y el análisis. Puede registrar todos los datos del contenido, pero es más eficiente registrar un extracto o resumir las propiedades. Los registros de la aplicación deben registrar los cuándo, dónde, quién, qué y cuál de cada evento. Las propiedades de estos dispositivos variarán según la arquitectura, la clase de aplicación y el sistema o dispositivo de host.

Al registrar las marcas de fecha y hora, utilice la hora universal coordinada (UTC) y los formatos de fecha y hora reconocidos internacionalmente en ISO 8601 (sitio web de la ISO).

> **Note**
>
> Considere utilizar un servicio de sincronización horaria de red para garantizar la precisión de las marcas horarias. Amazon brinda el servicio de sincronización temporal de Amazon, que utilizan muchos Servicios de AWS, incluido Amazon Elastic Compute Cloud (Amazon EC2). El Servicio de sincronización temporal de Amazon utiliza una flota de relojes atómicos de referencia conectados vía satélite en cada Región de AWS para entregar lecturas horarias precisas del estándar global de UTC a través del protocolo de tiempo de red (NTP). Para obtener más información, consulte Mantener el tiempo con el Servicio de sincronización temporal de Amazon (publicación de blog de AWS).

Los siguientes atributos de eventos suelen incluirse en los registros.

Categoría de atributo	Atributo del evento	Descripción
Cuando	Fecha y hora de registro	Registre la fecha y la hora en que se agregó el evento al registro.
	Fecha y hora del evento	Registre la fecha y la hora a la que se produjo el evento. Puede ser diferente al registro del registro, por ejemplo,

		cuando el registro se retrasa porque la aplicación cliente está alojada en un dispositivo remoto que está conectado de forma periódica o intermitente.
	Identificador de eventos	Registre un nombre de usuario, un número de cuenta u otro atributo exclusivo que garantice que el evento siempre se pueda identificar.
Donde	Identificador de la aplicación	Registre el nombre y la versión de la aplicación.
	Dirección de la aplicación	Registre el clúster o el nombre de host, la dirección IPv4 o IPv6 del servidor, el número de puerto, la identidad de la estación de trabajo y el identificador del dispositivo local.
	Servicio	Registre el nombre y el protocolo del servicio.
	Geolocalización	Registre las ubicaciones geográficas del usuario.
	Ventana, formulario o página	Registre la URL del punto de entrada, el método HTTP de una aplicación web o el nombre del cuadro de diálogo en el que se realizó la acción.
	Ubicación del código	Registre el nombre del script o módulo.

Quién (usuario humano o máquina)	Dirección de origen	Registre el identificador del dispositivo del usuario, la dirección IP, el identificador de la torre de telefonía móvil o radiofrecuencia (RF) o el número de teléfono móvil.
	Identidad de usuario	Si el usuario está autentica do o es conocido por alguna otra razón, registre el valor de la clave principal, el nombre de usuario o el número de licencia de la tabla de la base de datos de usuarios.
	Clasificación de tipos de usuarios	Registre el tipo de usuario, como el público, el autentica do, el CMS, el motor de búsqueda, el probador de penetración autorizado o el monitor de tiempo de actividad . Para obtener más informaci ón sobre los monitores de tiempo de actividad, consulte Precauciones y exclusiones en esta guía.
	Solicite encabezados HTTP o un agente de usuario HTTP	(Solo aplicaciones web) Registre la información del encabezado de la solicitud HTTP, incluida la cadena HTTP usuario-agente, ya que estos valores afectan a la información que el cliente envía al servidor.

Qué	Tipo de evento	Registre si el evento es informativo, una advertencia o un error.
	Gravedad del evento	Clasifique la gravedad del evento, como alta, media y baja.
	Indicador de eventos de seguridad	Si el registro contiene datos no relacionados con eventos de seguridad, cree una marca para los eventos relacionados con la seguridad que lo ayude a identificarlos.
	Descripción del evento	(Opcional) Incluye una descripción breve del evento.
	Acción o intención	Registre el propósito original previsto de la solicitud, como iniciar sesión, actualizar el ID de sesión, cerrar sesión o actualizar un perfil.
	Respuesta del usuario o de la aplicación	Registre la respuesta del usuario o la aplicación al evento, como un código de estado, mensajes de texto personalizados, la interrupción de la sesión o las alertas del administrador.
	Estado del resultado	Registre si la acción se ha realizado correctamente, si fue un éxito, si ha fallado o se ha aplazado.

	Motivo del resultado	Registre el motivo por el que se produjo el estado. Por ejemplo, una solicitud de inicio de sesión puede fallar porque el usuario no está autenticado en la base de datos.
	Detalles ampliados	Registre cualquier información adicional asociada al evento, como el seguimiento de la pila, los mensajes de error del sistema, la información de depuración y el cuerpo de la solicitud HTTP.
	Código de estado de respuesta de HTTP	(Solo aplicaciones web) Registre el código de estado de la respuesta HTTP devuelto al usuario, como `200` o `301`. Para obtener más información, consulte la sección Niveles de registro de esta guía.
Cuál	Recursos afectados	Registre sobre qué recursos se ha actuado
	Objeto	Registre los componentes u otros objetos afectados, como una cuenta de usuario, un recurso de datos, un archivo, una URL o un identificador de sesión.
	Nombre del recurso	Registre los nombres de los recursos afectados.

	Etiquetas de recursos	Registre las etiquetas asignadas a los recursos afectados. Para obtener más información sobre las etiquetas, consulte Etiquetado de los recursos de AWS (Referencia general de AWS).
Otros	Confianza analítica	Registre la confianza del servicio de registro en la detección de eventos, por ejemplo, asignando una calificación baja, media o alta o un valor numérico.
	Clasificaciones internas	Registre cualquier clasificación interna para estándares o conformidad.
	Clasificaciones externas	Registre cualquier clasificación externa para estándares o conformidad, como el Protocolo de automatización de contenido de seguridad (SCAP) de NIST.

Prácticas recomendadas de registro

Niveles de registro

Tenga cuidado de no registrar una cantidad excesiva de datos. Los registros deben capturar datos útiles y procesables. El registro excesivo puede afectar negativamente al rendimiento y también puede aumentar los costos de almacenamiento y procesamiento de los registros. El registro excesivo también puede provocar que los problemas y los eventos de seguridad pasen desapercibidos.

El registro de los códigos de estado de respuesta HTTP puede generar una cantidad significativa de datos de registro, especialmente códigos de estado de nivel 200 (éxito) y nivel 300 (redirección). Le

recomendamos que considere registrar únicamente los códigos de estado de nivel 400 (errores del lado del cliente) y de nivel 500 (errores del lado del servidor).

Los marcos de registro de aplicaciones brinden diferentes niveles de registro, como información, depuración o error. Para los entornos de desarrollo, es posible que desee utilizar un registro detallado, como información y depuración para ayudar a sus desarrolladores. Sin embargo, le recomendamos que deshabilite los niveles información y depuración para entornos de producción, ya que pueden generar un exceso de datos de registro.

Precauciones y exclusiones

- Asegúrese de que los datos que está registrando estén legalmente permitidos, en especial en las jurisdicciones en las que opera su organización.
- No excluya ningún evento relacionado con usuarios conocidos (como otros sistemas internos), terceros de confianza, robots de motores de búsqueda, monitores del tiempo de actividad o de procesos y otros sistemas de monitoreo remoto. Sin embargo, puede incluir un indicador de clasificación para cada uno de ellos en los datos registrados. Tenga en cuenta que los archivos de registro generados por su aplicación pueden ser utilizados por terceros, como soluciones de monitoreo de registros de terceros o proveedores de servicios externos, que no están autorizados a ver ningún dato confidencial que procese la aplicación.
- Los siguientes atributos no se deben registrar directamente en los registros. Elimine, oculte, desinfecte, codifique o cifre lo siguiente:
  - Código fuente de la aplicación
  - Valores de identificación de la sesión (considere sustituirlos por un valor hash si necesita realizar un seguimiento de los eventos específicos de la sesión)
  - Tokens de acceso
  - Datos personales confidenciales y algunos tipos de información de identificación personal (PII), como información de salud o identificadores emitidos por el Gobierno
  - Contraseñas de autenticación
  - Cadenas de conexión a la base de datos
  - Claves de cifrado y otros secretos principales
  - Datos del titular de la cuenta bancaria o de la tarjeta de pago
  - Se permite almacenar datos con una clasificación de seguridad superior a la del sistema de registro
  - Información confidencial para el comercio

- Información cuya recopilación es ilegal en las jurisdicciones pertinentes
- Información que un usuario ha optado por no recibir o no ha dado su consentimiento explícito a la recopilación
- Información que el consentimiento para recopilar ha caducado

Tipos de datos especiales

A veces, los siguientes datos también se pueden registrar en registros. Si bien puede ser útil para fines de investigación y solución de problemas, puede revelar información confidencial sobre el sistema. Es posible que necesite anonimizar, codificar o cifrar estos tipos de datos antes de que se registre el evento:

- Rutas de archivo
- Nombres y direcciones de redes internas
- Datos personales no confidenciales, como nombres personales, números de teléfono y direcciones de correo electrónico

Utilice la anonimización de los datos si no se requiere la identidad real de la persona en el registro o si el riesgo se considera demasiado grande.

Administración de cambios y accesos

- Los usuarios no administrativos no deberían poder deshabilitar el registro de eventos, en especial aquellos que sean necesarios para cumplir con los requisitos de conformidad.
- Solo los usuarios administrativos deberían poder pausar o detener los servicios de registro o modificar las configuraciones.
- Si su servicio de registro tiene una característica de validación de la integridad de los archivos de registro, habilítela. Esto lo ayuda a detectar la modificación, la eliminación o la falsificación de los archivos de registro. Para obtener más información sobre esta característica en los Servicios de AWS, consulte Utilización de CloudTrail en esta guía.
- El registro de los cambios debe ser intrínseco a la aplicación, por ejemplo, la aplicación debe realizarlos de forma automática en función de un algoritmo aprobado. O bien, debe seguir un proceso de administración de cambios aprobado, como cuando se cambian los datos de configuración o se modifica el código fuente.

Servicios de AWS para el registro y el monitoreo

Esta guía se centra en el registro y el monitoreo de las aplicaciones implementadas en la Nube de AWS. Puede usar los Servicios de AWS para implementar su plan de registro y monitoreo, o puede usarlos para mejorar sus soluciones actuales. Por ejemplo, si está solucionando un problema con su aplicación, podría:

- Clasifique los registros de la aplicación con la característica de registros de flujos de VPC de Amazon Virtual Private Cloud (Amazon VPC) y visualice el tráfico de red correspondiente al problema.
- Utilice AWS CloudTrail para ver las llamadas a la API que corresponden a los tiempos del evento del problema.
- Revise los registros de Amazon CloudWatch para comprobar si hay picos de CPU que correspondan con los tiempos del evento del problema.

Puede implementar los siguientes Servicios de AWS y características para registrar y monitorear su aplicación:

- AWS CloudTrail ayuda a auditar la gobernanza, la conformidad y el riesgo operativo de su Cuenta de AWS mediante el registro de las acciones realizadas por un usuario, un rol o un Servicio de AWS. Para obtener más información sobre el uso de este servicio para registrar o monitorear eventos de la aplicación, consulte Información en esta guía.
- Amazon CloudWatch ayuda a analizar los registros y a monitorear las métricas de los recursos y aplicaciones alojadas de AWS en tiempo real. También puede usar la característica ServiceLens para monitorear el estado de su aplicación o usar la característica Synthetics para crear valores controlados que monitoreen sus puntos de conexión y las API. Para obtener más información sobre el uso de este servicio para monitorear la aplicación, consulte CloudWatch en esta guía.
- Los Registros de Amazon CloudWatch ayudan a centralizar los registros de todos sus sistemas, aplicaciones y Servicios de AWS para que pueda monitorearlos y archivarlos de forma segura. Para obtener más información sobre el uso de este servicio para registrar eventos para la aplicación, consulte Registros de CloudWatch en esta guía.
- La característica de registros de flujo de VPC de Amazon Virtual Private Cloud (Amazon VPC) captura información acerca del tráfico IP entrante y saliente por las interfaces de red de su VPC. Para obtener más información sobre el uso de este servicio para registrar eventos para la aplicación, consulte Logs de flujo de VPC en esta guía.

- AWS X-Ray recopila datos sobre las solicitudes que atiende su aplicación y lo ayuda a ver, filtrar y obtener información sobre esos datos para identificar problemas y oportunidades de optimización. Para obtener más información sobre el uso de este servicio para monitorear la aplicación, consulte X-Ray en esta guía.

Registro y monitoreo de aplicaciones mediante AWS CloudTrail

AWS CloudTrail es un Servicio de AWS que ayuda a habilitar la auditoría operativa y de riesgos, la gobernanza y la conformidad de su Cuenta de AWS. Las acciones que realiza un usuario, el rol o un Servicio de AWS se registran como eventos en CloudTrail. Los eventos pueden incluir las acciones llevadas a cabo en la AWS Management Console, la AWS Command Line Interface (AWS CLI) y los SDK y API de AWS.

Utilización de CloudTrail

CloudTrail se habilita en su Cuenta de AWS cuando la crea. Cuando se produce actividad en su Cuenta de AWS, esta se registra en un evento de CloudTrail. Puede ver fácilmente los eventos recientes en la consola de CloudTrail yendo a Historial de eventos.

Para mantener un registro continuo de la actividad y de los eventos en su Cuenta de AWS, cree un registro de seguimiento. Puede crear registros de seguimiento para una sola Región de AWS o para todas las regiones. Los registros de seguimiento graban los archivos de registro de cada región y CloudTrail distribuye los archivos de registro a un bucket de Amazon Simple Storage Service (Amazon S3) consolidado.

Puede configurar varios registros de seguimiento de forma distinta, de modo que procesen y registren únicamente los eventos que especifique. Esto puede resultar útil cuando desee clasificar los eventos que se producen en su Cuenta de AWS con los eventos que se producen en su aplicación.

> **Note**
>
> CloudTrail tiene una característica de validación que puede utilizar para determinar si un archivo de registro se modificó, eliminó o no se modificó después de que CloudTrail lo entregó. Esta característica se compila mediante los algoritmos estándar de la industria: SHA-256 para el hash y SHA-256 con RSA para la firma digital. De ese modo, resulta imposible desde el punto de vista informático modificar, eliminar o falsificar archivos de registros de CloudTrail sin que se sepa. Puede utilizar la AWS CLI para validar los archivos en la ubicación donde los envió CloudTrail. Para obtener más información sobre esta

característica y cómo habilitarla, consulte Validar la integridad de los archivos de registros de CloudTrail (documentación de CloudTrail).

Casos de uso de CloudTrail

- Ayuda a la conformidad: el uso de CloudTrail puede ayudar a cumplir con las políticas internas y los estándares normativos al brindar un historial de eventos en su Cuenta de AWS.
- Análisis de seguridad: puede realizar un análisis de seguridad y detectar patrones de comportamiento de los usuarios al incorporar los archivos de registro de CloudTrail en soluciones de análisis y administración de registros, como CloudWatch Logs, Amazon EventBridge, Amazon Athena, Amazon OpenSearch Service u otra solución de terceros.
- Exfiltración de datos: puede detectar la exfiltración de datos al recopilar datos de actividad en los objetos de Amazon S3 mediante los eventos de la API a nivel de objeto registrados en CloudTrail. Una vez recopilados los datos de actividad, puede utilizar otros Servicios de AWS, como EventBridge y AWS Lambda, para activar una respuesta automática.
- Solución de problemas operativos: puede solucionar problemas operativos mediante los archivos de registro de CloudTrail. Por ejemplo, puede identificar rápidamente los cambios más recientes realizados en los recursos de su entorno, incluida la creación, modificación y eliminación de recursos de AWS.

Prácticas recomendadas para CloudTrail

- Habilite CloudTrail en todas las Regiones de AWS.
- Habilite la validación de la integridad de los archivos de registro.
- Cifre los registros.
- Incorpore los archivos de registro de CloudTrail en registros de CloudWatch.
- Centralice los registros de todas las Cuentas de AWS y regiones.
- Aplique políticas de ciclo de vida a los buckets de S3 que contienen archivos de registro.
- Impida que los usuarios puedan desactivar el registro en CloudTrail. Aplique la siguiente política de control de servicio (SCP) en AWS Organizations. Esta SCP establece una regla de denegación explícita para las acciones `StopLogging` y `DeleteTrail` en toda la organización.

```
{
"Version": "2012-10-17",
```

```
"Statement":
       [
                 { "Action":
                     [
                     "cloudtrail:StopLogging",
                     "cloudtrail:DeleteTrail"
                      ],
                      "Resource": "*",
                      "Effect": "Deny"
                  }
        ]
}
```

Registro y monitoreo de aplicaciones mediante Amazon CloudWatch

Amazon CloudWatch monitorea los recursos de AWS y las aplicaciones que ejecuta en AWS en tiempo real. Puede utilizar CloudWatch para recopilar y hacer un seguimiento de métricas, que son las variables que puede medir en los recursos y aplicaciones.

Uso de CloudWatch

CloudWatch es esencialmente un repositorio de métricas. Un Servicio de AWS, como Amazon EC2, coloca las métricas en el repositorio y usted obtiene las estadísticas en función de dichas métricas. Si coloca sus propias métricas personalizadas en el repositorio, también puede recuperar estadísticas sobre estas métricas. Para obtener más información, consulte Uso de las métricas de CloudWatch (documentación de CloudWatch).

También puede configurar alarmas, que inician acciones en su nombre de forma automática. Una alarma observa una única métrica durante un periodo específico y realiza una o más acciones específicas, según el valor de la métrica en relación con un umbral a lo largo del tiempo. Por ejemplo, la alarma podría enviar una notificación a un tema de Amazon Simple Notification Service (Amazon SNS). También puede agregar alarmas a paneles. Para obtener más información consulte Uso de alarmas de CloudWatch (documentación de CloudWatch).

La consola de CloudWatch muestra automáticamente las métricas sobre todos los Servicio de AWS que utilice. Puede crear paneles personalizados adicionales para mostrar las métricas y las alarmas de sus aplicaciones. Para obtener más información, consulte Uso de los paneles de CloudWatch (documentación de CloudWatch).

CloudWatch admite automáticamente la funcionalidad entre regiones. No es necesario realizar ningún paso adicional para mostrar métricas de distintas Regiones de AWS de una sola cuenta en el mismo gráfico o panel. Puede lograr la funcionalidad entre cuentas al implementar observabilidad entre cuentas (documentación de CloudWatch).

Para obtener más información y orientación detallada sobre el uso de CloudWatch para registrar y monitorear las cargas de trabajo en la Nube de AWS, consulte Diseño e implementación del registro y el monitoreo con Amazon CloudWatch (Recomendaciones de AWS).

Casos de uso de CloudWatch

- Monitoreo del estado de las aplicaciones: CloudWatch ServiceLens mejora la observabilidad de sus servicios y aplicaciones al permitirle integrar seguimientos, métricas, registros, alarmas y otra información sobre el estado de los recursos en un solo lugar. ServiceLens integra CloudWatch a AWS X-Ray para proporcionar una vista integral de la aplicación a fin de ayudarlo a identificar de manera más eficiente los cuellos de botella del rendimiento y los usuarios afectados. Para obtener más información, consulte Uso de ServiceLens para monitorear el estado de sus aplicaciones (documentación de CloudWatch).
- Monitoreo sintético: puede utilizar Amazon CloudWatch Synthetics para crear valores controlados, scripts configurables que se ejecutan según una programación, para monitorear los puntos de conexión y las API. Los Canaries siguen las mismas rutas y realizan las mismas acciones que un cliente, lo que le permite verificar continuamente su experiencia de cliente incluso cuando no tiene tráfico de clientes en sus aplicaciones. Los Canaries comprueban la disponibilidad y latencia de sus puntos de enlace, y pueden almacenar datos de tiempo de carga y capturas de pantalla de la interfaz de usuario. Monitorean las API de REST, las URL y el contenido del sitio web, y pueden comprobar si hay cambios no autorizados de suplantación de identidad, inyección de código y scripting entre sitios. Para obtener más información, consulte Uso del monitoreo sintético (documentación de CloudWatch).
- Monitoreo de usuarios: con CloudWatch RUM, puede realizar un monitoreo real de usuarios para recopilar y ver datos del lado del cliente sobre el rendimiento de su aplicación web. Los datos incluyen tiempos de carga de páginas, errores del lado del cliente y comportamiento del usuario. Puede utilizar los datos recopilados para identificar y depurar rápidamente los problemas de rendimiento del lado del cliente. Para obtener más información, consulte Uso de CloudWatch RUM (documentación de CloudWatch).
- Detección de comportamiento anómalo: cuando habilita la detección de anomalías para una métrica, CloudWatch aplica algoritmos estadísticos y machine learning. Estos algoritmos analizan continuamente las métricas de sistemas y las aplicaciones, determinan los valores de referencia

normales y detectan anomalías en la superficie. Para obtener más información, consulte Uso de la detección de anomalías de CloudWatch (documentación de CloudWatch).

- Validación de características y experimentos A/B: puede utilizar Amazon CloudWatch Evidently para validar nuevas características de forma segura si se las proporciona a un porcentaje específico de sus usuarios mientras implementa la característica. También puede llevar a cabo experimentos A/B para tomar decisiones de diseño de características basadas en pruebas y datos. Para obtener más información, consulte Realización de lanzamientos y experimentos A/B con CloudWatch Evidently (documentación de CloudWatch).

Registro y monitoreo de aplicaciones mediante Registros de Amazon CloudWatch

Registros de Amazon CloudWatch le permiten centralizar los registros de todos los sistemas, aplicaciones y los Servicios de AWS que utilice, en un único servicio de gran escalabilidad. De este modo, los puede consultar fácilmente, buscar códigos de error o patrones específicos, filtrarlos en función de campos específicos o archivarlos de forma segura para análisis futuros. Puede ver todos los eventos de registro, independientemente de su origen, como un flujo único y constante de eventos ordenados de manera temporal. Puede consultarlos y ordenarlos, agruparlos por campos específicos, crear cálculos personalizados y visualizar los datos de registro en paneles.

Uso de registros de CloudWatch

En los registros de CloudWatch, los eventos de registro se organizan en flujos de registro y grupos de registro. Un flujo de registro es una secuencia de eventos de registro que comparten la misma fuente. En concreto, un flujo de registro en general, está pensado para representar la secuencia de eventos procedente de la instancia de aplicación o recurso que se monitoriza. Los grupos de registros definen uno o más flujos de registro que comparten la misma configuración de retención, monitoreo y control de acceso. Cada flujo de registro debe pertenecer a un grupo de registro. Para obtener más información, consulte Trabajo con grupos de registros y flujos de registros (documentación de Registros de CloudWatch).

Puede utilizar la Información de registros de CloudWatch para buscar y analizar los datos de registro en Registros de Amazon CloudWatch. Puede realizar consultas que le ayuden a responder de forma más eficaz a los problemas de funcionamiento. Si se produce un problema, puede utilizar Información de registros de CloudWatch para identificar posibles causas y validar soluciones

implementadas. Para obtener más información, consulte Análisis de los datos de registros con Información de registros de Amazon CloudWatch (documentación de registros de CloudWatch).

Puede buscar y filtrar los datos de registro que entran en Registros de CloudWatch al crear uno o varios filtros de métricas. Los filtros de métricas definen los términos y los patrones que hay que buscar en los datos de registro a medida que se envían a Registros de CloudWatch. Registros de CloudWatch utiliza estos filtros de métricas para convertir los datos de registro en métricas numéricas de CloudWatch que puede representar gráficamente o en las que puede configurar una alarma. Para obtener más información, consulte Creación de métricas a partir de eventos de registro mediante filtros (documentación de Registros de CloudWatch).

Casos de uso de Registros de CloudWatch

- Monitoreo de registros de CloudTrail: puede crear alarmas en CloudWatch y recibir notificaciones de la actividad de la API particular capturada por CloudTrail y utilizar la notificación para llevar a cabo la resolución de problemas. Para obtener más información, consulte Envío de eventos de CloudTrail a Registros de CloudWatch (documentación de CloudTrail).
- Registrar llamadas a la API de AWS: si dispone de una solución de monitoreo de terceros implementada, puede utilizar los registros de CloudWatch para registrar las llamadas de la API de AWS. Debe configurar el servicio de monitoreo de terceros para evaluar este registro y las API a nivel de aplicación.
- Configuración de la retención de registro: de forma predeterminada, los registros de los Registros de CloudWatch se conservan de forma indefinida y no caducan nunca. Puede ajustar la política de retención para cada grupo de registro, al mantener la retención indefinida o seleccionar un periodo de retención de un día a 10 años.
- Archivar y almacenar registros: puede utilizar Registros de CloudWatch para almacenar datos de registro en un almacenamiento de alta durabilidad. El agente de Registros de CloudWatch envía datos de registro rotados y no rotados al servicio de registro. Posteriormente, cuando lo necesite, podrá obtener acceso a los datos de log en su estado original.

Registro y monitoreo de aplicaciones mediante registros de flujo de VPC

Los registros de flujo de VPC son una característica de Amazon Virtual Private Cloud (Amazon VPC) que ayuda a capturar información acerca del tráfico IP que entra y sale de las interfaces de red en la VPC.

Uso de registros de flujo de VPC

Puede crear un registro de flujo para una nube privada virtual (VPC), una subred o una interfaz de red. Si crea un log de flujo para una subred o VPC, se supervisará cada interfaz de red de la VPC o la subred. Para obtener más información, consulte Trabajo con registros de flujo (documentación de Amazon VPC).

Los datos del registro de flujo para una interfaz de red monitoreada se graban como registros de flujo. Un registro de registros de flujo representa un flujo de red en su VPC. De forma predeterminada, cada registro captura un flujo de tráfico IP de red que ocurre dentro de un intervalo de agregación. Cada registro es una cadena con campos separados por espacios. Un registro incluye valores para los distintos componentes del flujo de IP, por ejemplo, el origen, el destino y el protocolo. Al crear un registro de flujo, puede utilizar el formato predeterminado para el registro del registro de flujo o puede especificar un formato personalizado. Para obtener más información, consulte Ejemplos de registro de registros de flujo (documentación de Amazon VPC).

Los registros de flujo no capturan la siguiente información:

- Tráfico generado por instancias al contactar con el servidor del Sistema de nombres de dominio (DNS) de Amazon. Si utiliza su propio servidor DNS, sí se registrará el tráfico a ese servidor DNS.
- Tráfico generado por una instancia de Windows para la activación de licencia de Windows para Amazon.
- Tráfico entrante y saliente de `254.169.254` para metadatos de instancias.
- Tráfico entrante y saliente de `254.169.123` para el Servicio de sincronización temporal de Amazon.
- Tráfico del Protocolo de configuración dinámica de host (DHCP).
- Tráfico a la dirección IP reservada para el router VPC predeterminado.
- El tráfico entre una interfaz de red de punto de enlace y una interfaz de red de Network Load Balancer.

Los datos del registro de flujo se pueden publicar en varios Servicios de AWS, incluidos los registros de Amazon CloudWatch. Después de crear un registro de flujo, puede recuperar y ver los registros de flujo en Registros de CloudWatch en el grupo de registro que configure. Para obtener más información, consulte Publicación de registros de flujo para Registros de CloudWatch (documentación de Amazon VPC).

Los datos de registro de flujo se recopilan fuera de la ruta del tráfico de red y, por lo tanto, no afectan al rendimiento ni a la latencia de la red. Puede crear o eliminar registros de flujo sin ningún riesgo de impacto en el rendimiento de la red.

Casos de uso de los registros de flujo de VPC

- Diagnosticar reglas de grupo de seguridad muy restrictivas
- Monitorear el tráfico que llega a la instancia de su aplicación
- Determinar la dirección del tráfico

Registro y monitoreo de aplicaciones mediante AWS X-Ray

AWS X-Ray recopila datos sobre las solicitudes que atiende su aplicación y lo ayuda a ver, filtrar y obtener información sobre esos datos para identificar problemas y oportunidades de optimización.

Uso de X-Ray

AWS X-Ray recibe registros de seguimiento de su aplicación y, si están integradas con X-Ray, de los Servicios de AWS que utiliza su aplicación. X-Ray toma muestras y visualiza las solicitudes en un gráfico de servicio cuando fluyen por los componentes de la aplicación. X-Ray genera identificadores de seguimiento para que pueda correlacionar una solicitud cuando pasa por varios componentes, lo que lo ayuda a ver la solicitud de principio a fin. Puede mejorarlo aún más al incluir anotaciones y metadatos para ayudar a buscar e identificar de forma exclusiva las características de una solicitud.

Le recomendamos que configure cada servidor o punto de conexión de su aplicación con X-Ray. X-Ray se implementa en el código de su aplicación al hacer llamadas al servicio de X-Ray. X-Ray también brinda SDK de AWS para varios idiomas, incluidos clientes instrumentados que envían datos automáticamente a X-Ray. Los SDK de X-Ray ofrecen revisiones para bibliotecas comunes que se utilizan para realizar llamadas a otros servicios (por ejemplo, HTTP, MySQL, PostgreSQL o MongoDB).

Para obtener más información, consulte Seguimiento de aplicaciones con AWS X-Ray (Recomendaciones de AWS).

Casos de uso para X-Ray

- Análisis y depuración de aplicaciones: los datos de registros de seguimiento pueden ayudarlo a depurar la aplicación al ofrecer una vista integral de la solicitud para que pueda identificar los

cuellos de botella y solucionar los problemas. El mapa de servicio de X-Ray es una herramienta visual que lo ayuda a identificar dónde se producen los errores, las conexiones con alta latencia o los registros de seguimiento de las solicitudes fallidas.

- Análisis de rendimiento: la consola de análisis es una herramienta interactiva para interpretar datos de los registros de seguimiento para comprender rápidamente cómo se están desempeñando su aplicación y sus servicios subyacentes. La consola lo ayuda a explorar, analizar y visualizar los registros de seguimiento. También puede comparar conjuntos de registros de seguimiento con diferentes condiciones para analizar la causa raíz.

Preguntas frecuentes

¿Puedo usar mi servicio de monitoreo actual?

Amazon CloudWatch es un servicio de monitoreo y observabilidad creado para ingenieros de DevOps, desarrolladores, ingenieros de confiabilidad del sitio (SRE), administradores de TI y propietarios de aplicaciones. Ofrece datos e información procesable para ayudarlo a monitorear sus aplicaciones, responder a los cambios de rendimiento que afectan a todo el sistema y optimizar el uso de recursos. Sin embargo, si cuenta con un servicio de monitoreo establecido, no es necesario que lo sustituya.

¿Cómo puedo evitar que se manipulen los archivos de registro?

Puede habilitar la validación de la integridad de los archivos de registro. Es una práctica recomendada administrar y almacenar sus registros en una Cuenta de AWS dedicada y restringir el acceso a esa cuenta. Para obtener más información, consulte la sección Utilización de CloudTrail de esta guía.

¿Tengo que mantener archivos de registro separados para cada aplicación?

No, puede consolidar los datos de registro de varias aplicaciones en el mismo archivo de registro. Sin embargo, asegúrese de que se registre un identificador único para cada aplicación en el flujo de registro.

Recursos

Documentación de AWS

- Documentación de AWS CloudTrail
- Vea la documentación de Nube de AWSWatch
- Vea la documentación de registros de Nube de AWSWatch
- Documentación de registros de flujo de Amazon VPC
- Documentación de AWS X-Ray
- Diseño e implementación del registro y monitoreo con Amazon CloudWatch (Recomendaciones de AWS)

Marketing de AWS

- AWS CloudTrail
- Amazon CloudWatch
- Registros centralizados en AWS (Soluciones de AWS)
- Monitoreo y observabilidad (Operaciones de Nube de AWS)
- Cómo monitorear sus aplicaciones de forma eficaz (Startups de 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	—	6 de enero de 2023

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.