Creación de un programa de gestión de vulnerabilidades escalable sobre AWS

AWS Guía prescriptiva

AWS Guía prescriptiva: Creación de un programa de gestión de vulnerabilidades escalable sobre AWS

Table of Contents

Creación de un programa de gestión de vulnerabilidades escalable en AWS

Anna McAbee y Megan O'Neil, Amazon Web Services ()AWS

Octubre de 2023 (historial del documento)

Según la tecnología subyacente que utilice, una variedad de herramientas y escaneos pueden generar hallazgos de seguridad en un entorno de nube. Si no se implementan procesos para gestionar estos hallazgos, pueden empezar a acumularse y, a menudo, dar lugar a miles o decenas de miles de hallazgos en un corto período de tiempo. Sin embargo, con un programa estructurado de gestión de vulnerabilidades y una operacionalización adecuada de sus herramientas, su organización puede gestionar y clasificar una gran cantidad de hallazgos de diversas fuentes.

La gestión de vulnerabilidades se centra en descubrir, priorizar, evaluar, corregir e informar sobre las vulnerabilidades. La administración de parches, por otro lado, se centra en parchear o actualizar el software para eliminar o corregir las vulnerabilidades de seguridad. La administración de parches es solo un aspecto de la administración de vulnerabilidades. Por lo general, se recomienda establecer un patch-in-place proceso (también conocido como mitigate-in-placeproceso) para abordar situaciones críticas en las que es necesario aplicar parches ahora, y un proceso estándar que ejecute de forma regular para lanzar paquetes de software, contenedores o imágenes de Amazon Machine Images (AMI) parcheados. Estos procesos ayudan a preparar a su organización para responder rápidamente a una vulnerabilidad de día cero. Para los sistemas críticos de un entorno de producción, utilizar un patch-in-place proceso puede ser más rápido y fiable que implementar una nueva AMI en toda la flota. En el caso de los parches programados con regularidad, como los parches del sistema operativo (SO) y de software, le recomendamos que los cree y pruebe mediante procesos de desarrollo estándar, como haría con cualquier cambio a nivel de software. Esto proporciona una mayor estabilidad para los modos de funcionamiento estándar. Puede utilizar Patch Manager, una funcionalidad u otros productos de terceros como patch-in-place soluciones. AWS Systems Manager Para obtener más información sobre el uso del administrador de parches, consulte Administración de parches en AWS Cloud Adoption Framework: Operations Perspective. Además, puede utilizar EC2 Image Builder para automatizar la creación, la administración y el despliegue de imágenes personalizadas up-to-date y de servidor.

La creación de un programa de gestión de vulnerabilidades escalable AWS implica gestionar las vulnerabilidades tradicionales de software y red, además de los riesgos de configuración de la

nube. Un riesgo de configuración en la nube, como un depósito de Amazon Simple Storage Service (Amazon S3) sin cifrar, debería seguir un proceso de clasificación y corrección similar al de una vulnerabilidad de software. En ambos casos, el equipo de aplicaciones debe ser el propietario y responsable de la seguridad de la aplicación, incluida la infraestructura subyacente. Esta distribución de la propiedad es clave para un programa de gestión de vulnerabilidades eficaz y escalable.

Esta guía explica cómo agilizar la identificación y la corrección de las vulnerabilidades para reducir el riesgo general. Utilice las siguientes secciones para crear e iterar su programa de gestión de vulnerabilidades:

1. Prepárese: prepare a su personal, sus procesos y su tecnología para identificar, evaluar y corregir las vulnerabilidades de su entorno.
2. Clasifique y corrija: envíe los hallazgos de seguridad a las partes interesadas pertinentes, identifique la acción correctiva adecuada y, a continuación, tome las medidas correctivas.
3. Informe y mejore: utilice los mecanismos de presentación de informes para identificar las oportunidades de mejora y, a continuación, modifique su programa de gestión de vulnerabilidades.

La creación de un programa de gestión de vulnerabilidades en la nube suele implicar iteraciones. Dé prioridad a las recomendaciones de esta guía y revise periódicamente su cartera pendiente para mantenerse al día con los cambios tecnológicos y los requisitos de su empresa.

Destinatarios previstos

Esta guía está destinada a grandes empresas que tienen tres equipos principales responsables de los hallazgos relacionados con la seguridad: un equipo de seguridad, un Cloud Center of Excellence (CCoE) o equipo de nube y equipos de aplicaciones (o desarrolladores). Esta guía utiliza los modelos operativos empresariales más comunes y se basa en esos modelos operativos para permitir una respuesta más eficiente a los hallazgos de seguridad y mejorar los resultados de seguridad. Las organizaciones que lo utilizan AWS pueden tener estructuras y modelos operativos diferentes; sin embargo, puede modificar muchos de los conceptos de esta guía para adaptarlos a diferentes modelos operativos y organizaciones más pequeñas.

Objetivos

Esta guía puede ayudarle a usted y a su organización a:

- Desarrolle políticas para agilizar la gestión de vulnerabilidades y garantizar la rendición de cuentas

- Establezca mecanismos para distribuir la responsabilidad de la seguridad entre los equipos de aplicaciones
- Configure Servicios de AWS según las mejores prácticas para una gestión escalable de las vulnerabilidades
- Distribuya la propiedad de los hallazgos de seguridad
- Establezca mecanismos para informar sobre su programa de gestión de vulnerabilidades e iterarlo
- Mejore la visibilidad de la búsqueda de seguridad y mejore la postura general de seguridad

Prepare su programa escalable de gestión de vulnerabilidades

Prepararse para crear un programa de gestión de vulnerabilidades escalable implica formar a las personas, desarrollar procesos e implementar la tecnología adecuada de acuerdo con las mejores prácticas. Las personas, los procesos y la tecnología son igual de importantes para que un programa de gestión de vulnerabilidades sea eficaz, y es necesario integrarlos estrechamente para gestionar las vulnerabilidades a escala.

En esta sección de la guía, se analizan las medidas fundamentales que puede tomar para preparar su programa escalable de gestión de vulnerabilidades. AWS

Temas

Defina un plan de gestión de vulnerabilidades

El primer paso a la hora de preparar su programa de gestión de vulnerabilidades en la nube es definir su plan de gestión de vulnerabilidades. Este plan incluye las políticas y los procesos que sigue su organización. Este plan debe estar documentado y ser accesible para todas las partes interesadas. Un plan de gestión de vulnerabilidades es un documento de alto nivel que normalmente incluye las siguientes secciones:

- Objetivos y alcance: describa los objetivos, las funciones y el alcance de la gestión de vulnerabilidades.
- Funciones y responsabilidades: enumere las partes interesadas en la gestión de vulnerabilidades y detalle sus responsabilidades.

- Definiciones de gravedad y priorización de la vulnerabilidad: determine cómo clasificar la gravedad de una vulnerabilidad y cómo priorizarla.
- Acuerdos de nivel de servicio (SLA) para la remediación: para cada nivel de gravedad, defina el tiempo máximo del que dispone el propietario de la remediación para resolver un problema de seguridad. Dado que el cumplimiento de los SLA es una parte integral de contar con un programa de gestión de vulnerabilidades eficaz y escalable, considere cómo hacer un seguimiento de si está cumpliendo con estos SLA.
- Proceso de excepciones: detalle el proceso de presentación, aprobación y actualización de las excepciones. Este proceso debe garantizar que las excepciones sean legítimas, tengan un límite de tiempo y se rastreen.
- Fuentes de información sobre vulnerabilidades: enumere las fuentes o herramientas que generan hallazgos de seguridad. Para obtener más información sobre qué Servicios de AWS podrían ser las fuentes de los hallazgos de seguridad, consulta Configure los servicios de seguridad AWS esta guía.

Si bien estas secciones son comunes en empresas de diferentes tamaños e industrias, el plan de gestión de vulnerabilidades de cada organización es único. Debe crear un plan de gestión de vulnerabilidades que funcione mejor para su organización. Espere repetir su plan con el tiempo para incorporar las lecciones aprendidas y las tecnologías en evolución.

Distribuya la propiedad de la seguridad

El modelo de responsabilidad AWS compartida define cómo AWS y sus clientes comparten la responsabilidad por la seguridad y el cumplimiento de la nube. En este modelo, AWS protege la infraestructura en la que se ejecutan todos los servicios que se ofrecen en él Nube de AWS, y AWS los clientes son responsables de proteger sus datos y aplicaciones.

Puede reflejar este modelo en su organización y distribuir las responsabilidades entre sus equipos de nube y de aplicaciones. Esto le ayuda a escalar sus programas de seguridad en la nube de manera más eficaz, ya que los equipos de aplicaciones se hacen cargo de determinados aspectos de seguridad de sus aplicaciones. La interpretación más sencilla del modelo de responsabilidad compartida es que si tiene acceso para configurar el recurso, es responsable de la seguridad de ese recurso.

Una parte clave de la distribución de las responsabilidades de seguridad entre los equipos de aplicaciones consiste en crear herramientas de seguridad de autoservicio que ayuden a los equipos

de aplicaciones a automatizar. Inicialmente, esto puede ser un esfuerzo conjunto. El equipo de seguridad puede traducir los requisitos de seguridad en herramientas de escaneo de código y, a continuación, los equipos de aplicaciones pueden usar esas herramientas para crear y compartir soluciones con su comunidad interna de desarrolladores. Esto contribuye a aumentar la eficiencia de otros equipos que deben cumplir requisitos de seguridad similares.

En la siguiente tabla se describen los pasos para distribuir la propiedad entre los equipos de aplicaciones y se proporcionan ejemplos.

Paso	Acción	Ejemplo
1	Defina sus requisitos de seguridad: ¿qué está intentando conseguir? Esto puede provenir de un estándar de seguridad o de un requisito de cumplimiento.	Un ejemplo de requisito de seguridad es el acceso con privilegios mínimos para las identidades de las aplicacio nes.
2	Enumere los controles de un requisito de seguridad: ¿qué significa realmente este requisito desde el punto de vista del control? ¿Qué debo hacer para lograrlo?	Para lograr el mínimo privilegi o para las identidades de las aplicaciones, a continuación se muestran dos ejemplos de controles: • Utilice funciones AWS Identity and Access Management (IAM) • No utilice caracteres comodín en las políticas de IAM
3	Guía documental para los controles: con estos controles , ¿qué orientación puede proporcionar a un desarroll ador para ayudarlo a cumplir con el control?	En primer lugar, puede empezar por documentar políticas de ejemplo sencillas , incluidas las políticas de IAM seguras y no seguras y las políticas de bucket de

Paso	Acción	Ejemplo
		Amazon Simple Storage Service (Amazon S3). A continuación, puede integrar soluciones de análisis de políticas en los procesos de integración continua y entrega continua (CI/CD), por ejemplo, mediante el uso de reglas para una evaluación proactiva .AWS Config
4	Desarrolle artefactos reutilizables: con esta guía, ¿podrá hacerlo aún más fácil y desarrollar artefactos reutilizables para los desarrolladores?	Puede crear una infraestructura como código (IaC) para implementar políticas de IAM que sigan el principio de privilegios mínimos. Puede almacenar estos artefactos reutilizables en un repositorio de código.

Es posible que el autoservicio no funcione para todos los requisitos de seguridad, pero puede funcionar en escenarios estándar. Al seguir estos pasos, las organizaciones pueden capacitar a sus equipos de aplicaciones para que se ocupen de una mayor parte de sus propias responsabilidades de seguridad de forma escalable. En general, el modelo de responsabilidad distribuida conduce a prácticas de seguridad más colaborativas en muchas organizaciones.

Desarrolle un programa de divulgación de vulnerabilidades

Para defense-in-depthadoptar un enfoque de gestión de vulnerabilidades, cree un programa de divulgación de vulnerabilidades para que las personas de su organización o ajenas a ella puedan denunciar las vulnerabilidades o los riesgos de seguridad.

Para las personas de su organización, establezca un proceso para presentar los riesgos o las vulnerabilidades. Esto se puede hacer a través de un sistema de venta de entradas o por correo

electrónico. Independientemente del proceso que elija, es fundamental que sus empleados estén al tanto del proceso y puedan denunciar fácilmente cualquier vulnerabilidad o riesgo que encuentren.

Para las personas ajenas a su organización, cree una página web externa para enviar información sobre posibles vulnerabilidades de seguridad. A modo de ejemplo, consulte la página web de informes de AWS vulnerabilidades. Esta página web también debe contener directrices de divulgación para ayudar a proteger los datos y los activos de su organización. Un programa de divulgación de vulnerabilidades no debe fomentar actividades potencialmente dañinas, por lo que es esencial contar con una política clara con directrices. Crear un programa de divulgación responsable y maduro es un objetivo por el que hay que esforzarse a medida que vaya madurando el programa. La mayoría no comienza con un programa de divulgación externo, y hacerlo bien lleva tiempo.

Prepare su AWS entorno

Antes de implementar cualquier herramienta de administración de vulnerabilidades, asegúrese de que su AWS entorno esté diseñado para soportar un programa de administración de vulnerabilidades escalable. La estructura de sus políticas de etiquetado Cuentas de AWS y las de su organización puede simplificar el proceso de creación de un programa de gestión de vulnerabilidades escalable.

Desarrolle una estructura Cuenta de AWS

AWS Organizationsayuda a gestionar y gobernar un AWS entorno de forma centralizada a medida que su empresa crece y amplía sus AWS recursos. Una organización los AWS Organizations consolida Cuentas de AWS en grupos lógicos, o unidades organizativas, para que pueda administrarlos como una sola unidad. La administración se AWS Organizations realiza desde una cuenta dedicada, denominada cuenta de administración. Para obtener más información, consulte Terminología y conceptos de AWS Organizations.

Le recomendamos que administre su entorno de AWS múltiples cuentas en AWS Organizations. Esto ayuda a crear un inventario completo de las cuentas y los recursos de su empresa. Este inventario completo de activos es un aspecto fundamental de la gestión de vulnerabilidades. Los equipos de aplicaciones no deben usar cuentas ajenas a la organización.

AWS Control Towerle ayuda a configurar y administrar un entorno de AWS múltiples cuentas, siguiendo las mejores prácticas prescriptivas. Si aún no ha establecido un entorno de múltiples cuentas, AWS Control Tower es un buen punto de partida.

Recomendamos utilizar la estructura de cuentas dedicada y las prácticas recomendadas que se describen en la Arquitectura AWS de referencia de seguridad (AWS SRA). La cuenta Security

Tooling debe servir como administradora delegada de sus servicios de seguridad. Más adelante en esta guía encontrará más información sobre la configuración de las herramientas de gestión de vulnerabilidades en esta cuenta. Aloje las aplicaciones en cuentas dedicadas en la unidad organizativa (OU) de cargas de trabajo. Esto establece un fuerte aislamiento a nivel de carga de trabajo y límites de seguridad explícitos para cada aplicación. Para obtener información sobre los principios de diseño y las ventajas de utilizar un enfoque de cuentas múltiples, consulte Cómo organizar su AWS entorno con varias cuentas (documento técnico).AWS

Disponer de una estructura contable intencionada y gestionar de forma centralizada los servicios de seguridad desde una cuenta dedicada son aspectos fundamentales de un programa de gestión de vulnerabilidades escalable.

Defina, implemente y aplique etiquetas

Las etiquetas son pares clave-valor que actúan como metadatos para organizar AWS los recursos. Para obtener más información, consulte Etiquetado de los recursos de AWS. Puede utilizar etiquetas para proporcionar un contexto empresarial, como la unidad de negocio, el propietario de la aplicación, el entorno y el centro de costes. En la siguiente tabla se muestra un conjunto de etiquetas de ejemplo.

Clave	Valor
BusinessUnit	HumanResources
CostCenter	CC101
ApplicationTeam	HumanResourcesTechnology
Entorno	Producción

Las etiquetas pueden ayudarle a priorizar los hallazgos. Por ejemplo, pueden ayudarle a:

- Identifique al propietario de un recurso responsable de reparar una vulnerabilidad
- Realice un seguimiento de qué aplicaciones o unidades de negocio tienen un gran número de hallazgos
- Aumente la gravedad de los hallazgos relacionados con determinadas clasificaciones de datos, como la información de identificación personal (PII) o los datos del sector de tarjetas de pago (PCI)

- Identifique el tipo de datos del entorno, como los datos de prueba en un entorno de desarrollo de nivel inferior o los datos de producción

Para ayudarle a lograr un etiquetado eficaz a gran escala, siga las instrucciones que se indican en Cómo crear su estrategia de etiquetado, que se encuentra en Best Practices for Tagging AWS Resources (documento técnico).AWS

AWS Supervise los boletines de seguridad

Recomendamos encarecidamente supervisar los boletines de AWS seguridad de forma regular y frecuente. Los boletines de seguridad pueden notificarle cualquier nueva vulnerabilidad relacionada con la seguridad, los servicios afectados y las actualizaciones aplicables. También puede suscribirse a una fuente RSS para recibir los boletines de seguridad y crear un proceso para asimilar y abordar estos boletines como parte de su programa de gestión de vulnerabilidades.

Configure los servicios de seguridad AWS

AWS ofrece una variedad de servicios de seguridad diseñados para ayudar a proteger su AWS entorno. Para su programa de gestión de vulnerabilidades, le recomendamos que habilite lo siguiente Servicios de AWS en cada cuenta:

- Amazon GuardDuty ayuda a detectar las amenazas activas en su entorno. Un GuardDuty hallazgo podría ayudarle a identificar una vulnerabilidad desconocida que se ha explotado en su entorno. También podría ayudarle a comprender los efectos de una vulnerabilidad no parcheada.
- AWS Healthproporciona una visibilidad continua del rendimiento de sus recursos y de la disponibilidad de sus cuentas Servicios de AWS .
- AWS Identity and Access Management Access Analyzeranaliza las políticas basadas en recursos de su AWS entorno para identificar los recursos que se comparten con una entidad externa. Esto puede ayudarlo a identificar las vulnerabilidades asociadas con el acceso no deseado a sus recursos y datos. Para cada instancia de un recurso compartido fuera de su cuenta, el Analizador de acceso de IAM genera un resultado.
- Amazon Inspector es un servicio de gestión de vulnerabilidades que analiza continuamente sus AWS cargas de trabajo en busca de vulnerabilidades de software y exposición no intencionada a la red.
- AWS Security Huble ayuda a comprobar su AWS entorno con respecto a los estándares del sector de la seguridad y puede identificar los riesgos de configuración de la nube. También proporciona

una visión completa del estado de su AWS seguridad mediante la agregación de los resultados de otros servicios de AWS seguridad y herramientas de seguridad de terceros.

En esta sección se explica cómo activar y configurar Amazon Inspector y Security Hub para ayudarle a establecer un programa de gestión de vulnerabilidades escalable.

Uso de Amazon Inspector en su programa de gestión de vulnerabilidades

Amazon Inspector es un servicio de gestión de vulnerabilidades que escanea continuamente las instancias de Amazon Elastic Compute Cloud (Amazon EC2), las imágenes AWS Lambda de los contenedores de Amazon Elastic Container Registry (Amazon ECR) y funciona para detectar vulnerabilidades de software y exposiciones no intencionadas de la red. Puede utilizar Amazon Inspector para obtener visibilidad y priorizar la resolución de las vulnerabilidades de software en sus AWS entornos.

Amazon Inspector evalúa continuamente su entorno durante todo el ciclo de vida de sus recursos. Vuelve a analizar automáticamente los recursos en respuesta a los cambios que podrían introducir una nueva vulnerabilidad. Por ejemplo, se vuelve a escanear cuando se instala un paquete nuevo en una instancia de EC2, cuando se instala un parche o cuando se publica un nuevo documento sobre vulnerabilidades y exposiciones comunes (CVE) que afecta al recurso. Cuando Amazon Inspector identifica una vulnerabilidad o una ruta de red abierta, produce un hallazgo que usted puede investigar. El hallazgo proporciona información completa sobre la vulnerabilidad, que incluye lo siguiente:

- Puntuación de riesgo de Amazon Inspector
- Puntuación del Common Vulnerability Scoring System (CVSS)
- Recurso afectado
- Datos de inteligencia de vulnerabilidades sobre el CVE de Amazon Recorded Future, y Cybersecurity and Infrastructure Security Agency (CISA)
- Recomendaciones de remediación

Para obtener instrucciones sobre la configuración de Amazon Inspector, consulte Introducción a Amazon Inspector. El paso Activar Amazon Inspector de este tutorial proporciona dos opciones de configuración: un entorno de cuentas independientes y un entorno de cuentas múltiples. Le recomendamos que utilice la opción de entorno de varias cuentas si desea monitorizar varias cuentas Cuentas de AWS que sean miembros de una organización. AWS Organizations

Al configurar Amazon Inspector para un entorno de varias cuentas, designas una cuenta de la organización como administradora delegada de Amazon Inspector. El administrador delegado puede gestionar las conclusiones y algunos ajustes para los miembros de la organización. Por ejemplo, el administrador delegado puede ver los detalles de las conclusiones agregadas de todas las cuentas de los miembros, activar o desactivar los escaneos de las cuentas de los miembros y revisar los recursos escaneados. La AWS SRA recomienda crear una cuenta de Security Tooling y utilizarla como administrador delegado de Amazon Inspector.

Utilícela AWS Security Hub en su programa de gestión de vulnerabilidades

La creación de un programa de gestión de vulnerabilidades escalable AWS implica gestionar las vulnerabilidades tradicionales de software y red, además de los riesgos de configuración de la nube. AWS Security Hub le ayuda a comparar su AWS entorno con los estándares del sector de la seguridad y puede identificar los riesgos de configuración de la nube. Security Hub también proporciona una visión completa del estado de su seguridad AWS al agregar los hallazgos de seguridad de otros servicios de AWS seguridad y herramientas de seguridad de terceros.

En las siguientes secciones, ofrecemos prácticas recomendadas y recomendaciones para configurar Security Hub para respaldar su programa de gestión de vulnerabilidades:

- Configuración de Security Hub
- Habilitación de los estándares de Security Hub
- Gestión de los hallazgos de Security Hub
- Agregar los resultados de otros servicios y herramientas de seguridad

Configuración de Security Hub

Para obtener instrucciones de configuración, consulte Configuración AWS Security Hub. Para usar Security Hub, debe habilitarlo AWS Config. Para obtener más información, consulte Habilitación y configuración AWS Config en la documentación de Security Hub.

Si está integrado con AWS Organizations, desde la cuenta de administración de la organización, designa una cuenta como administrador delegado de Security Hub. Para obtener instrucciones, consulte Designación del administrador delegado de Security Hub. La AWS SRA recomienda crear una cuenta de Security Tooling y utilizarla como administrador delegado de Security Hub.

El administrador delegado tiene acceso automáticamente para configurar Security Hub para todas las cuentas de los miembros de la organización y para ver los resultados asociados a esas cuentas. Le

recomendamos que habilite AWS Config Security Hub en todos Regiones de AWS y cada uno de sus Cuentas de AWS. Puede configurar Security Hub para tratar automáticamente las nuevas cuentas de la organización como cuentas de miembros de Security Hub. Para obtener instrucciones, consulte Administrar las cuentas de los miembros que pertenecen a una organización.

Habilitación de los estándares de Security Hub

Security Hub genera hallazgos mediante la ejecución de comprobaciones de seguridad automatizadas y continuas contra los controles de seguridad. Los controles están asociados a uno o más estándares de seguridad. Los controles ayudan a determinar si se cumplen los requisitos de un estándar.

Al habilitar un estándar en Security Hub, Security Hub habilita automáticamente los controles que se aplican al estándar. Security Hub utiliza AWS Config reglas para realizar la mayoría de las comprobaciones de seguridad de los controles. Puede activar o desactivar los estándares de Security Hub en cualquier momento. Para obtener más información, consulte Controles y estándares de seguridad en AWS Security Hub. Para obtener una lista completa de estándares, consulte la referencia de estándares de Security Hub.

Si su organización aún no tiene un estándar de seguridad preferido, le recomendamos que utilice el estándar AWS Foundational Security Best Practices (FSBP). Este estándar está diseñado para detectar cuándo Cuentas de AWS y cuándo los recursos se desvían de las mejores prácticas de seguridad. AWS selecciona este estándar y lo actualiza periódicamente para incluir nuevas funciones y servicios. Tras evaluar los resultados del FSBP, considere la posibilidad de habilitar otros estándares.

Gestión de los hallazgos de Security Hub

Security Hub ofrece varias funciones que lo ayudan a abordar grandes volúmenes de hallazgos de toda la organización y a comprender el estado de seguridad de su AWS entorno. Para ayudarle a gestionar los hallazgos, le recomendamos que habilite las dos funciones siguientes de Security Hub:

- Utilice la agregación entre regiones para agregar los hallazgos, encontrar actualizaciones, información, controlar los estados de cumplimiento y las puntuaciones de seguridad de varias regiones de agregación Regiones de AWS a una sola región de agregación.
- Utilice los resultados de control consolidados para reducir el problema de las búsquedas mediante la eliminación de los resultados duplicados. Cuando los resultados de control consolidados están activados en su cuenta, Security Hub genera un único resultado nuevo o una actualización de

resultados para cada control de seguridad de un control, incluso si un control se aplica a varios estándares habilitados.

Agregar los resultados de otros servicios y herramientas de seguridad

Además de generar hallazgos de seguridad, puede usar Security Hub para agregar datos de búsqueda de varias Servicios de AWS soluciones de seguridad de terceros compatibles. Esta sección se centra en enviar las conclusiones de seguridad a Security Hub. En la siguiente secciónPrepárese para asignar las conclusiones de seguridad,, se explica cómo puede integrar Security Hub con productos que puedan recibir las conclusiones de Security Hub.

Hay muchos Servicios de AWS productos de terceros y soluciones de código abierto disponibles que puede integrar con Security Hub. Si acaba de empezar, le recomendamos que haga lo siguiente:

1. Habilitar la integración Servicios de AWS: la mayoría de Servicio de AWS las integraciones que envían los resultados a Security Hub se activan automáticamente después de habilitar tanto el Security Hub como el servicio integrado. Para su programa de gestión de vulnerabilidades, le recomendamos que habilite Amazon Inspector GuardDuty AWS Health, Amazon e IAM Access Analyzer en cada cuenta. Estos servicios envían automáticamente sus resultados a Security Hub. Para obtener una lista completa de Servicio de AWS las integraciones compatibles, consulta la Servicios de AWS sección Enviar los resultados a Security Hub.

   > **Note**
   >
   > AWS Health envía los resultados a Security Hub si se cumple una de las siguientes condiciones:
   >
   > - El hallazgo está asociado a un servicio AWS de seguridad
   > - El código de tipo de búsqueda contiene las palabras `securityabuse`, o `certificate`
   > - El AWS Health servicio de búsqueda es `risk` o `abuse`

2. Configurar integraciones de terceros: para obtener una lista de las integraciones compatibles actualmente, consulta las integraciones de productos de socios de terceros disponibles. Seleccione cualquier herramienta adicional que pueda enviar o recibir las conclusiones de Security Hub. Es posible que ya tengas algunas de estas herramientas de terceros. Siga las instrucciones del producto para configurar la integración con Security Hub.

Prepárese para asignar las conclusiones de seguridad

En esta sección, configurará las herramientas que sus equipos utilizan para gestionar y asignar los hallazgos de seguridad. En esta sección se incluyen las siguientes opciones:

- Gestione los hallazgos de las herramientas y los flujos de trabajo existentes— Esta opción se integra AWS Security Hub con los sistemas existentes que sus equipos utilizan para gestionar sus tareas diarias, como la cartera de productos pendientes. Esta opción se recomienda para los equipos que han establecido herramientas para gestionar sus flujos de trabajo.
- Gestione los hallazgos en Security Hub— Esta opción configura las notificaciones de los eventos del Security Hub para que el equipo correspondiente reciba una alerta y pueda abordar el hallazgo en Security Hub.

Decida qué flujo de trabajo funcionaría mejor para sus equipos y asegúrese de que los responsables de las cuestiones de seguridad lleguen rápidamente a sus respectivos propietarios.

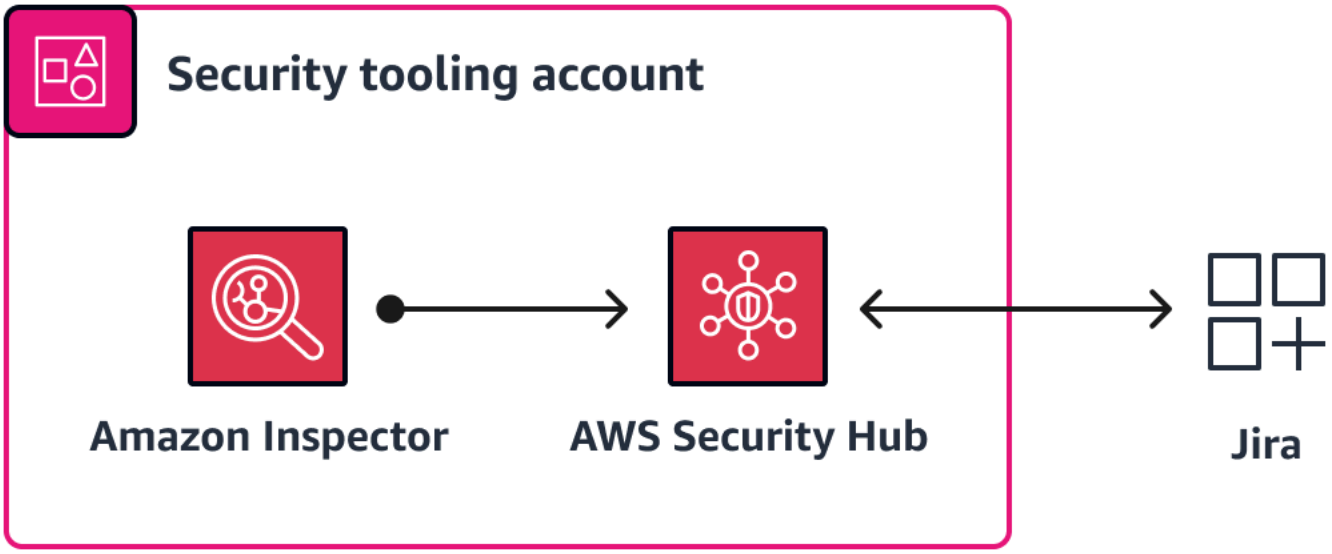
Gestione los hallazgos de las herramientas y los flujos de trabajo existentes

Recomendamos integraciones adicionales de Security Hub para las organizaciones empresariales que cuentan con herramientas establecidas que los equipos utilizan para gestionar o realizar sus tareas diarias. Puede importar los datos de búsqueda de Security Hub a varias plataformas tecnológicas. Entre los ejemplos se incluyen:

- Los sistemas de información de seguridad y gestión de eventos (SIEM) ayudan a los equipos de seguridad a clasificar los eventos de seguridad operativa. Los sistemas SIEM proporcionan un análisis en tiempo real de las alertas de seguridad generadas por las aplicaciones y el hardware de la red.
- Los sistemas de gobierno, riesgo y cumplimiento (GRC) ayudan a los equipos de cumplimiento y gobierno a monitorear los datos de gestión de riesgos e informar sobre ellos. Las herramientas de GRC son aplicaciones de software que las empresas pueden utilizar para gestionar las políticas, evaluar los riesgos, controlar el acceso de los usuarios y agilizar el cumplimiento. Puede utilizar las herramientas de GRC para integrar los procesos empresariales, reducir los costes y mejorar la eficiencia.
- Los sistemas de registro de productos y venta de entradas ayudan a los equipos de aplicaciones y de nube a gestionar las funciones y priorizar las tareas de desarrollo. Atlassian Jiray Microsoft Azure DevOpsson ejemplos de estos sistemas.

La integración de los hallazgos de Security Hub directamente con estos sistemas empresariales existentes puede mejorar el tiempo medio de recuperación (MTTR) y los resultados de seguridad, ya que el flujo de trabajo operativo diario no tiene por qué cambiar. Los equipos pueden responder y aprender de las conclusiones de seguridad mucho más rápido, ya que no tienen que utilizar flujos de trabajo y herramientas independientes. La integración hace que abordar los hallazgos de seguridad sea parte del flujo de trabajo normal y estándar.

Security Hub se integra con varios productos de socios de terceros. Para obtener una lista completa y las instrucciones, consulte las integraciones de productos de socios externos disponibles en la documentación de Security Hub. Las integraciones más comunes incluyen Atlassian - Jira Service Managementla integración bidireccional AWS Security Hub con Jira el software y. ServiceNow – ITSM En el siguiente diagrama se muestra cómo puede configurar Amazon Inspector para que envíe las conclusiones a Security Hub y, a continuación, configurar Security Hub para que envíe todas las conclusiones aJira.



Gestione los hallazgos en Security Hub

Puede crear un sistema de notificaciones basado en la nube para los hallazgos de Security Hub mediante EventBridge las reglas de Amazon y los temas del Amazon Simple Notification Service (Amazon SNS). Este sistema notifica al equipo correspondiente acerca de un hallazgo cuando se crea. Para este enfoque, la estrategia de cuentas múltiples descrita en la sección Desarrolle una estructura Cuenta de AWS es fundamental porque las aplicaciones se dividen en cuentas dedicadas. Esto le ayuda a notificar cada hallazgo a los equipos correctos.

Los equipos de seguridad o de nube pueden optar por recibir los eventos de todos Cuentas de AWS. En este caso, cree una EventBridge regla en la cuenta de administrador delegado de Security Hub y suscríbase a un tema de Amazon SNS que notifique a estos equipos. Para los equipos de aplicaciones, configure una EventBridge regla y un tema de SNS en sus respectivas cuentas de aplicaciones. Cuando se produce un hallazgo de Security Hub en una cuenta de aplicación, se notifica al equipo responsable sobre el hallazgo.

Security Hub ya envía automáticamente todos los nuevos hallazgos y todas las actualizaciones de los hallazgos existentes EventBridge como Security Hub Findings - Imported events. Cada evento de Security Hub Findings: Imported contiene un único hallazgo. Puede aplicar filtros a las EventBridge reglas para que un hallazgo inicie la regla solo si el hallazgo coincide con los filtros. Para obtener instrucciones, consulte Configurar una EventBridge regla para el envío automático de los resultados. Para obtener más información sobre la creación y suscripción a los temas de Amazon SNS, consulte Configuración de Amazon SNS.

Tenga en cuenta lo siguiente cuando utilice este enfoque:

- Para los equipos de aplicaciones, cree EventBridge reglas dentro de cada uno de ellos Cuenta de AWS y en el Región de AWS lugar donde se aloja la aplicación.
- Para los equipos de seguridad y de nube, cree EventBridge reglas en la cuenta de administrador delegado de Security Hub. Esto notifica a los equipos todos los hallazgos en las cuentas de los miembros.
- Amazon SNS envía una notificación todos los días si el estado del hallazgo de seguridad es el mismo. `NEW` Si quieres desactivar las notificaciones diarias, puedes crear una AWS Lambda función personalizada que cambie el estado del hallazgo de `NEW` a `NOTIFIED` después de que el suscriptor de Amazon SNS reciba la notificación.

Clasifique y corrija los hallazgos de seguridad en su entorno AWS

La clasificación de un hallazgo de seguridad implica remitirlo a la parte interesada correspondiente, evaluarlo y priorizarlo y, luego, subsanarlo. En esta sección se analiza cada uno de estos pasos en detalle y se proporcionan recomendaciones de escalabilidad y eficiencia. También incluye ejemplos para ayudar a ilustrar el proceso de clasificación y remediación.

Temas

Defina la propiedad de los hallazgos de seguridad

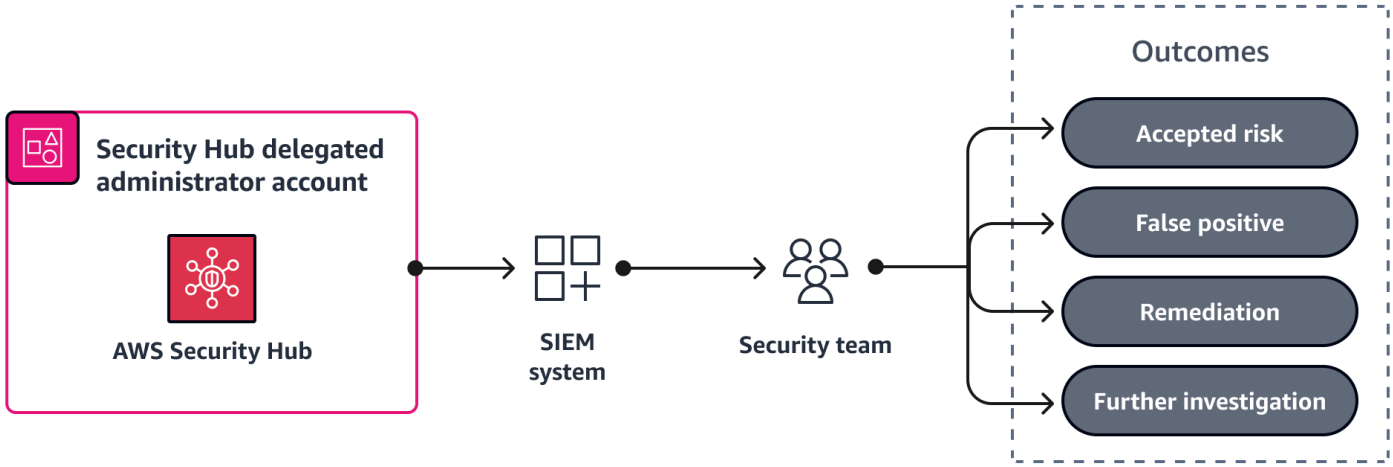
Definir un modelo de propiedad para clasificar los hallazgos de seguridad puede ser difícil, pero no tiene por qué serlo. El panorama de la seguridad cambia constantemente y los profesionales deben ser flexibles para adaptarse a estos cambios. Adopte un enfoque flexible para desarrollar su modelo de propiedad para los hallazgos de seguridad. Su modelo inicial debería permitir a sus equipos actuar de inmediato. Recomendamos empezar con una lógica de propiedad básica y afinar esa lógica con el tiempo. Si se demora en definir los criterios de propiedad perfectos, el número de hallazgos de seguridad seguirá aumentando.

Para facilitar la asignación de los hallazgos a los equipos y recursos adecuados, recomendamos AWS Security Hub integrarlos con cualquier sistema existente que sus equipos utilicen para gestionar sus tareas diarias. Por ejemplo, puede integrar Security Hub con sistemas de gestión de eventos e información de seguridad (SIEM) o con sistemas de registro de productos y venta de entradas. Para obtener más información, consulte la sección Prepárese para asignar las conclusiones de seguridad de esta guía.

El siguiente es un ejemplo de un modelo de propiedad que puede utilizar como punto de partida:

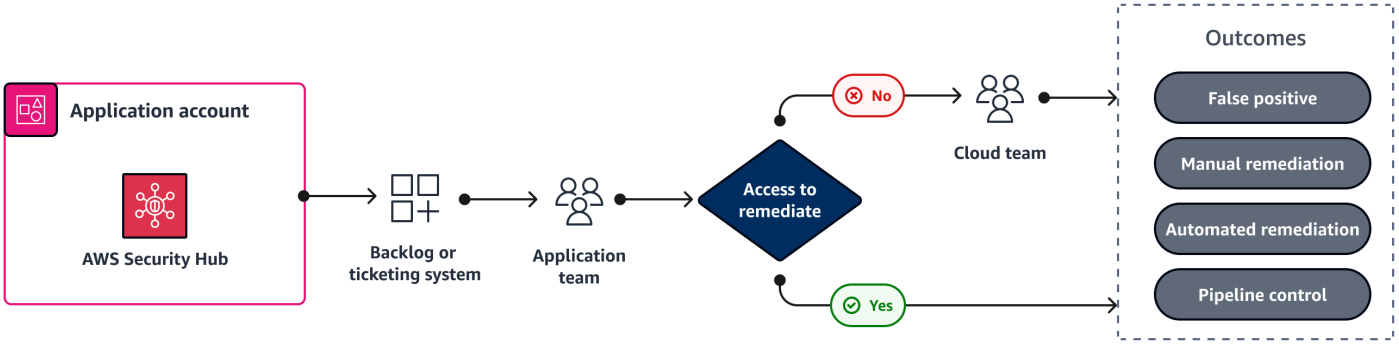
- El equipo de seguridad analiza las posibles amenazas activas y ayuda a evaluar y priorizar los hallazgos de seguridad. El equipo de seguridad tiene la experiencia y las herramientas para

evaluar adecuadamente el contexto. Comprenden los datos adicionales relacionados con la seguridad que les ayudan a evaluar y priorizar las vulnerabilidades e investigar los eventos de detección de amenazas. Si es necesario determinar la gravedad o realizar ajustes adicionales, consulte la Evalúe y priorice los hallazgos de seguridad sección de esta guía. Para ver un ejemplo, consulte Ejemplo de un equipo de seguridad esta guía.



- Distribuya las conclusiones de seguridad entre los equipos de nube y de aplicaciones: como se explica en la Distribuya la propiedad de la seguridad sección, el equipo que tiene acceso para configurar el recurso es responsable de su configuración segura. Los equipos de aplicaciones son responsables de las conclusiones de seguridad relacionadas con los recursos que crean y configuran, y el equipo de la nube es responsable de las conclusiones de seguridad relacionadas con las configuraciones de amplio alcance. En la mayoría de los casos, los equipos de aplicaciones no tienen acceso a cambiar configuraciones de gran alcance Servicios de AWS, como las políticas de control de servicios (SCP) AWS Control Tower, las configuraciones de VPC relacionadas con la red y el Centro de identidad de IAM. AWS OrganizationsAWS

  En el caso de entornos con varias cuentas que separan las aplicaciones en cuentas dedicadas, normalmente se pueden integrar las conclusiones relacionadas con la seguridad de la cuenta en el sistema de gestión de solicitudes pendientes o de registro de la aplicación. Desde ese sistema, el equipo de la nube o el equipo de aplicaciones pueden abordar el hallazgo. Para ver ejemplos, consulte Ejemplo de equipo en la nube o Ejemplo de equipo de aplicaciones consulte esta guía.



- Asigna al equipo de la nube las conclusiones restantes que no se hayan resuelto. Las conclusiones residuales pueden estar relacionadas con la configuración predeterminada o con configuraciones de gran alcance que el equipo de la nube pueda abordar. Es probable que este equipo sea el que tenga más conocimientos históricos y acceso para resolver el hallazgo. En general, este suele ser un subconjunto significativamente menor del total de los hallazgos.

Evalúe y priorice los hallazgos de seguridad

Un componente fundamental de un programa eficaz de gestión de vulnerabilidades es la capacidad de evaluar y priorizar los hallazgos de seguridad. Aquí es donde entra en juego el contexto, el historial de la organización y el ajuste de los sistemas de detección. La priorización de los hallazgos de seguridad ayuda a establecer la velocidad adecuada para el nivel de respuesta.

En el caso de Amazon Inspector y Amazon GuardDuty, los resultados contienen una etiqueta o puntuación de gravedad. AWS Security Hub Recomendamos priorizar la investigación de todos los hallazgos críticos y de alta gravedad en Security Hub, incluidos los relacionados con el estándar Foundational Security Best Practices (FSBP), Amazon Inspector y. GuardDuty Para encontrar las etiquetas de gravedad y las puntuaciones, se determina de la siguiente manera:

- La puntuación de Amazon Inspector es una puntuación altamente contextualizada para cada hallazgo. Se calcula correlacionando la información de la puntuación básica del Common Vulnerability Scoring System (CVSS) con los resultados de accesibilidad de la red y los datos de explotabilidad. Con esta puntuación, puede priorizar los hallazgos para centrarse en los hallazgos más importantes y en los recursos vulnerables. Además de la puntuación, Amazon Inspector también proporciona información de vulnerabilidad mejorada sobre vulnerabilidades y exposiciones comunes (CVE). Este es un resumen de la información disponible sobre el CVE de Amazon, así como de las fuentes de inteligencia de seguridad estándar del sector, como Recorded Future y Cybersecurity and Infrastructure Security Agency (CISA). Por ejemplo, Amazon Inspector puede

proporcionar los nombres de los kits de malware conocidos que se utilizan para aprovechar una vulnerabilidad. Para obtener más información, consulte Inteligencia sobre vulnerabilidades.

- Cada GuardDuty hallazgo tiene un nivel de gravedad y un valor asignados que reflejan el riesgo potencial del hallazgo para su entorno. Este nivel y valor los determinan los ingenieros AWS de seguridad. Por ejemplo, un nivel de `High` gravedad indica que un recurso está comprometido y se está utilizando activamente con fines no autorizados. Le recomendamos que dé prioridad a `High` la GuardDuty determinación de la gravedad y que la corrija de inmediato para evitar un uso no autorizado posterior.
- La gravedad de un hallazgo de control del Security Hub viene determinada por la dificultad de explotación y la probabilidad de que se ponga en peligro. La dificultad viene determinada por el grado de sofisticación o complejidad que se requiere para utilizar la debilidad para llevar a cabo un escenario de amenaza. La probabilidad de que se ponga en peligro indica la probabilidad de que el escenario de amenaza provoque una interrupción o una violación de sus recursos Servicios de AWS o de sus recursos.

Para ajustar las conclusiones, puede suprimir o archivar las conclusiones específicas directamente en la consola de servicio correspondiente o mediante la API del servicio. Además, puede realizar cambios en las conclusiones de Security Hub mediante reglas de automatización. GuardDuty y las conclusiones de Amazon Inspector se envían automáticamente a Security Hub. Puede utilizar las reglas de automatización para actualizar automáticamente (por ejemplo, cambiar la gravedad) o suprimir los resultados prácticamente en tiempo real, en función de los criterios que defina. Al crear reglas de automatización, te recomendamos añadir contexto a la descripción de la regla, como la fecha de creación o modificación, quién la creó y por qué es necesaria la regla. Esta información suele ser útil para consultarla en el futuro.

Corrija los hallazgos de seguridad

Después de evaluar y priorizar un hallazgo, la siguiente acción es corregir el hallazgo. Hay muchas medidas diferentes que puede tomar para corregir un hallazgo. En el caso de las vulnerabilidades de software, puede actualizar el sistema operativo o aplicar un parche. Para encontrar información sobre la configuración de la nube, puede actualizar la configuración de los recursos. En general, las acciones que se toman para corregir se pueden agrupar en uno de los siguientes resultados:

- Solución manual: se proporciona manualmente una solución a la vulnerabilidad, por ejemplo, se modifican las propiedades de un AWS recurso para habilitar el cifrado. Si el hallazgo proviene de

una comprobación gestionada en Security Hub, el hallazgo incluye un enlace a instrucciones para corregir manualmente el hallazgo.

- Artefacto reutilizable: se actualiza la infraestructura como código (IaC) para corregir la vulnerabilidad y saber que otras personas podrían beneficiarse de una solución similar. Considere la posibilidad de cargar el IaC actualizado y un breve resumen de la resolución en un repositorio de código interno compartido.
- Reparación automática: la vulnerabilidad se corrige automáticamente mediante los mecanismos que usted creó.
- Control de canalización: se aplica un control dentro de la canalización de integración y entrega continuas (CI/CD) que impide el despliegue si la vulnerabilidad está presente.
- Riesgo aceptado: no realiza ninguna acción ni implementa un control compensatorio, y acepta el riesgo que presenta la vulnerabilidad. Realice un seguimiento del riesgo aceptado en una ubicación específica, como un registro de riesgos.
- Falso positivo: no realiza ninguna acción porque ha determinado que el hallazgo no identificó correctamente una vulnerabilidad.

En esta guía no se incluye una lista completa de las diversas medidas y herramientas que puede utilizar para corregir una vulnerabilidad. Sin embargo, vale la pena mencionar algunos servicios y herramientas que pueden ayudarle a corregir las vulnerabilidades a gran escala, entre los que se incluyen:

- El administrador de parches, una capacidad de AWS Systems Manager, automatiza el proceso de parchear los nodos gestionados tanto con actualizaciones relacionadas con la seguridad como con otros tipos de actualizaciones. Puede utilizar Patch Manager para aplicar parches a los sistemas operativos y a las aplicaciones.
- AWS Firewall Managerle ayuda a configurar y administrar de forma centralizada las reglas de firewall en todas sus cuentas y aplicaciones en. AWS Organizations A medida que se crean nuevas aplicaciones, Firewall Manager facilita el cumplimiento de las nuevas aplicaciones y recursos mediante la aplicación de un conjunto común de reglas de seguridad.
- Automated Security AWS Response on es una AWS solución que funciona con Security Hub y proporciona acciones de respuesta y remediación predefinidas basadas en los estándares de cumplimiento de la industria y las mejores prácticas para las amenazas de seguridad.

Ejemplos de clasificación y corrección de los hallazgos de seguridad

En esta sección se proporcionan ejemplos del proceso de clasificación para los equipos de seguridad, nube y aplicaciones. En él se analizan los tipos de conclusiones que suele abordar cada equipo y se proporciona un ejemplo de cómo responder a ellas. También se incluye una guía de remediación de alto nivel.

En esta sección se incluyen los siguientes ejemplos:

- Ejemplo de equipo de seguridad: creación de una regla de automatización de Security Hub
- Ejemplo de equipo de nube: cambio de configuraciones de VPC
- Ejemplo de equipo de aplicaciones: creación de una regla AWS Config

Ejemplo de equipo de seguridad: creación de una regla de automatización de Security Hub

El equipo de seguridad recibe las conclusiones relacionadas con la detección de amenazas, incluidas las de Amazon GuardDuty . Para obtener una lista completa de los tipos de GuardDuty búsqueda clasificados por tipo de AWS recurso, consulte Búsqueda de tipos en la GuardDuty documentación. Los equipos de seguridad deben estar familiarizados con todos estos tipos de hallazgos.

Para este ejemplo, el equipo de seguridad acepta el nivel de riesgo asociado a los hallazgos de seguridad en un Cuenta de AWS documento que se utiliza estrictamente con fines de aprendizaje y no incluye datos importantes o confidenciales. El nombre de esta cuenta es `sandbox` y el ID de la cuenta es`123456789012`. El equipo de seguridad puede crear una regla de AWS Security Hub automatización que suprima todos los GuardDuty hallazgos de esta cuenta. Pueden crear una regla a partir de una plantilla, que cubre muchos casos de uso comunes, o pueden crear una regla personalizada. En Security Hub, recomendamos obtener una vista previa de los resultados de los criterios para confirmar que la regla arroja los resultados esperados.

> **Note**
>
> En este ejemplo, se destaca la funcionalidad de las reglas de automatización. No recomendamos suprimir todos los GuardDuty resultados de una cuenta. El contexto es

importante, y cada organización debe elegir qué hallazgos suprimir en función del tipo de datos, la clasificación y los controles de mitigación.

Los siguientes son los parámetros que se utilizan para crear esta regla de automatización:

- Regla:
  - El nombre de la regla es `Suppress findings from Sandbox account`
  - La descripción de la regla es `Date: 06/25/23 Authored by: John Doe Reason: Suppress GuardDuty findings from the sandbox account`
- Criterios:
  - `AwsAccountId` = `123456789012`
  - `ProductName` = `GuardDuty`
  - `WorkflowStatus` = `NEW`
  - `RecordState` = `ACTIVE`
- Acción automatizada:
  - `Workflow.status` es `SUPPRESSED`

Para obtener más información, consulte Reglas de automatización en la documentación de Security Hub. Los equipos de seguridad tienen muchas opciones para investigar y corregir los hallazgos relacionados con las amenazas detectadas. Para obtener más información, consulte la Guía de respuesta a incidentes de AWS seguridad. Le recomendamos que consulte esta guía para confirmar que ha establecido procesos sólidos de respuesta a incidentes.

Ejemplo de equipo de nube: cambio de configuraciones de VPC

El equipo de la nube es responsable de clasificar y corregir los hallazgos de seguridad que tienen tendencias comunes, como los cambios en la configuración AWS predeterminada que podrían no adaptarse a su caso de uso. Estos hallazgos suelen afectar a muchos Cuentas de AWS recursos, como las configuraciones de VPC, o incluyen una restricción que debería aplicarse a todo el entorno. En su mayor parte, el equipo de la nube realiza cambios manuales y puntuales, como agregar o actualizar una política.

Después de que su organización haya utilizado un AWS entorno durante algún tiempo, es posible que se esté desarrollando un conjunto de antipatrones. Un antipatrón es 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. Como alternativa a estos antipatrones, su organización puede utilizar restricciones más eficaces en todo el entorno, como las políticas de control de AWS Organizations servicios (SCP) o los conjuntos de permisos del IAM Identity Center. Los SCP y los conjuntos de permisos pueden proporcionar restricciones adicionales para los tipos de recursos, como impedir que los usuarios configuren un bucket público de Amazon Simple Storage Service (Amazon S3). Si bien puede resultar tentador restringir todas las configuraciones de seguridad posibles, existen límites de tamaño en las políticas para los SCP y los conjuntos de permisos. Recomendamos un enfoque equilibrado de los controles preventivos y de detección.

Los siguientes son algunos controles del estándar de mejores prácticas de seguridad AWS Security Hub fundamentales (FSBP) de los que podría ser responsable el equipo de la nube:

- [EC2.2] El grupo de seguridad predeterminado de la VPC no debe permitir el tráfico entrante ni saliente
- [EC2.6] El registro de flujo de VPC debe estar habilitado en todas las VPC
- [EC2.23] Amazon EC2 Transit Gateways no debe aceptar automáticamente las solicitudes de adjuntos de VPC
- [CloudTrail.1] CloudTrail debe habilitarse y configurarse con al menos un registro multirregional que incluya eventos de administración de lectura y escritura
- [Config.1] AWS Config debe estar activado

Para este ejemplo, el equipo de la nube está abordando un hallazgo relacionado con el control EC2.2 del FSBP. En la documentación de este control se recomienda no utilizar el grupo de seguridad predeterminado, ya que permite un amplio acceso mediante las reglas de entrada y salida predeterminadas. Como el grupo de seguridad predeterminado no se puede eliminar, se recomienda cambiar la configuración de las reglas para restringir el tráfico entrante y saliente. Para abordar este problema de manera eficiente, el equipo de la nube debe usar los mecanismos establecidos para modificar las reglas de los grupos de seguridad para todas las VPC, ya que cada VPC tiene este grupo de seguridad predeterminado. En la mayoría de los casos, los equipos de nube administran las configuraciones de VPC mediante AWS Control Towerpersonalizaciones o una herramienta de infraestructura como código (IaC), como o. HashiCorp TerraformAWS CloudFormation

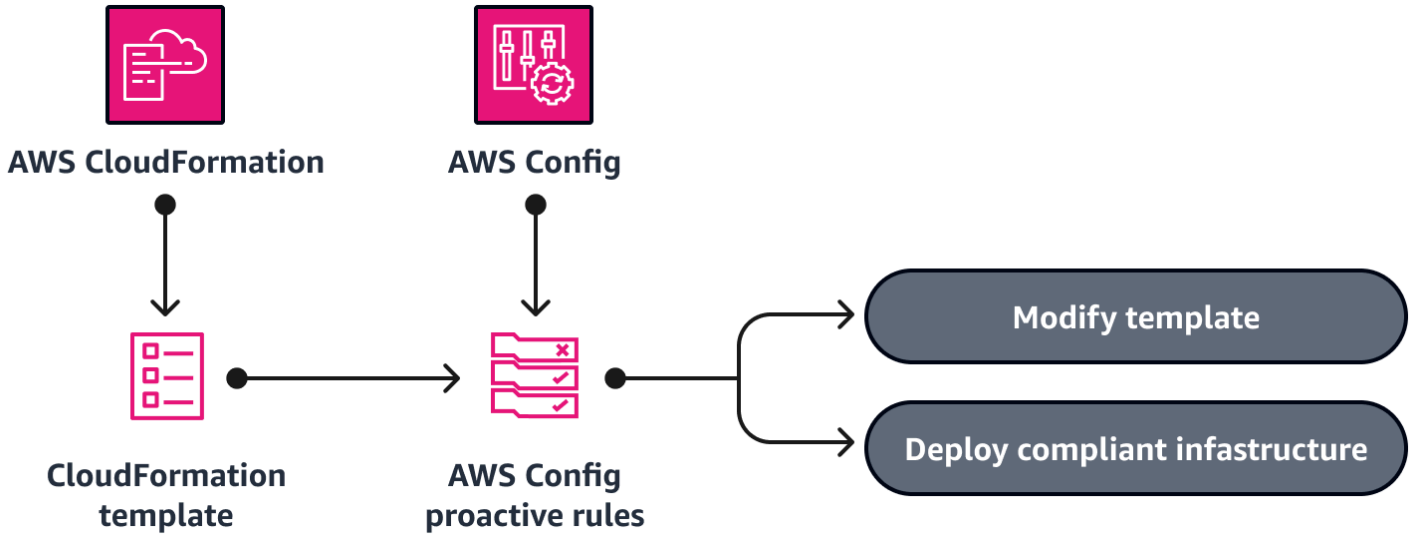
Ejemplo de equipo de aplicaciones: creación de una regla AWS Config

Los siguientes son algunos controles del estándar de seguridad de Security Hub Foundational Security Practices (FSBP) de los que podría ser responsable la aplicación o el equipo de desarrollo:

- [CloudFront.1] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado
- [EC2.19] Los grupos de seguridad no deben permitir el acceso ilimitado a los puertos de alto riesgo
- [CodeBuild.1] CodeBuild GitHub o las URL del repositorio fuente de Bitbucket deben usar OAuth
- [ECS.4] Los contenedores de ECS deben ejecutarse sin privilegios
- [ELB.1] Application Load Balancer debe configurarse para redirigir todas las solicitudes HTTP a HTTPS

Para este ejemplo, el equipo de aplicaciones está abordando el hallazgo del control EC2.19 del FSBP. Este control comprueba si el tráfico entrante ilimitado de los grupos de seguridad es accesible para los puertos especificados que tienen el mayor riesgo. Este control falla si alguna de las reglas de un grupo de seguridad permite la entrada de tráfico desde `0.0.0.0/0` o hacia esos puertos. `::/0` La documentación de este control recomienda eliminar las reglas que permiten este tráfico.

Además de abordar la regla del grupo de seguridad individual, este es un excelente ejemplo de un hallazgo que debería dar como resultado una nueva AWS Config regla. Al utilizar el modo de evaluación proactiva, puede ayudar a evitar el despliegue de reglas de grupos de seguridad riesgosas en el futuro. El modo proactivo evalúa los recursos antes de que se desplieguen para evitar que los recursos estén mal configurados y los resultados de seguridad asociados a ellos. Al implementar un nuevo servicio o una nueva funcionalidad, los equipos de aplicaciones pueden ejecutar reglas de forma proactiva como parte de su proceso de integración y entrega continuas (CI/CD) para identificar los recursos que no cumplen con las normas. La siguiente imagen muestra cómo puede utilizar una AWS Config regla proactiva para confirmar que la infraestructura definida en una AWS CloudFormation plantilla es compatible.



En este ejemplo se puede obtener otra eficiencia importante. Cuando un equipo de aplicaciones crea una AWS Config regla proactiva, puede compartirla en un repositorio de código común para que otros equipos de aplicaciones puedan usarla.

Cada hallazgo asociado a un control de Security Hub contiene detalles sobre el hallazgo y un enlace a las instrucciones para solucionar el problema. Si bien los equipos de la nube pueden encontrar hallazgos que requieran una solución manual y puntual, cuando proceda, recomendamos crear comprobaciones proactivas que identifiquen los problemas lo antes posible en el proceso de desarrollo.

Informe y mejore su programa de gestión de vulnerabilidades

La presentación de informes eficaz para la gestión de la vulnerabilidad implica revisar los datos, monitorear las tendencias y compartir conocimientos. Esto proporciona visibilidad y ayuda a los equipos a mejorar la postura de seguridad de sus organizaciones en el Nube de AWS

Realice reuniones mensuales sobre operaciones de seguridad

Las reuniones mensuales sobre las operaciones de seguridad son un mecanismo eficaz para promover la titularidad, la responsabilidad y la alineación continuas entre los equipos. En la reunión, las partes interesadas de los equipos de seguridad, nube y aplicaciones revisan los datos para detectar las principales conclusiones en materia de seguridad, las que no están contempladas en los acuerdos de nivel de servicio (SLA) y los equipos que tienen más conclusiones.

Estas reuniones ayudan a sus equipos a identificar patrones contradictorios, como las oportunidades de añadir más restricciones. Los controles preventivos y las oportunidades de automatización también se pueden descubrir y compartir. Las reuniones también ayudan a identificar lo que funciona y lo que no funciona bien en el programa de gestión de vulnerabilidades, a fin de poder realizar mejoras.

Al revisar los datos, identificar los antipatrones y los problemas y compartir información sobre los controles y las automatizaciones, los equipos pueden obtener información valiosa y realizar mejoras continuas que pueden reforzar su postura de seguridad y reducir sus acuerdos de nivel de servicio relacionados con la seguridad.

Utilice los conocimientos de Security Hub para identificar antipatrones

AWS Security Hub Los conocimientos también pueden ayudarlo a identificar los antipatrones y a hacer un seguimiento de su progreso en la corrección de los hallazgos. Una visión de Security Hub es una colección de hallazgos relacionados. Identifica un área de seguridad que requiere atención e intervención. Los conocimientos de Security Hub pueden ayudarlo a identificar requisitos específicos y desarrollar informes. Security Hub ofrece varios datos gestionados integrados. Para realizar un

seguimiento de los problemas de seguridad que son exclusivos de su AWS entorno y uso, puede crear información personalizada.

Conclusión y siguientes pasos

En resumen, un programa de gestión de vulnerabilidades eficaz requiere una preparación minuciosa y requiere disponer de las herramientas e integraciones adecuadas, ajustarlas con precisión, clasificar los problemas de forma eficiente e informar y mejorar continuamente. Si siguen las prácticas recomendadas de esta guía, las organizaciones pueden crear un programa de gestión de vulnerabilidades escalable que ayude AWS a proteger sus entornos de nube.

Puede ampliar este programa para incluir vulnerabilidades y hallazgos adicionales relacionados con la seguridad, como las vulnerabilidades de seguridad de las aplicaciones. AWS Security Hub admite integraciones de productos personalizadas. Considere usar Security Hub como punto de integración para herramientas y productos de seguridad adicionales. Esta integración le permite aprovechar los procesos y flujos de trabajo que ya ha establecido en su programa de gestión de vulnerabilidades, como la integración directa con la cartera de productos y las reuniones mensuales de revisión de seguridad.

En la siguiente tabla se resumen las fases y las medidas que se describen en esta guía.

Fase	Elementos de acción
Preparación	• Defina un plan de gestión de vulnerabilidades. • Distribuya la propiedad de los hallazgos. • Desarrolle un programa de divulgación de vulnerabilidades. • Desarrolle una Cuenta de AWS estructura. • Defina, implemente y aplique las etiquetas. • Supervise los boletines de AWS seguridad. • Habilite Amazon Inspector con un administrador delegado. • Habilite Security Hub con un administrador delegado. • Habilite los estándares de Security Hub. • Configure la agregación entre regiones de Security Hub.

Fase	Elementos de acción
	• Habilite los hallazgos de control consolidados en Security Hub. • Configure y gestione las integraciones de Security Hub, incluidas las integraciones descendentes aplicables con SIEM, GRC o sistemas de gestión de pedidos o venta de entradas de productos
Clasifique y corrija	• Distribuya los hallazgos en función de una estrategia de cuentas múltiples. • Dirija los resultados a los equipos de seguridad, nube y aplicaciones o desarroll adores. • Ajuste los resultados de seguridad para asegurarse de que sean procesables para su entorno específico. • Desarrolle mecanismos de remediación automatizados, siempre que sea posible. • Siempre que sea posible, implemente controles de tuberías de CI/CD u otras barreras que ayuden a evitar problemas de seguridad. • Utilice las reglas de automatización de Security Hub para aumentar o suprimir los hallazgos.
Informe y mejore	• Organice reuniones mensuales sobre operaciones de seguridad. • Utilice los conocimientos de Security Hub para identificar los antipatrones.

Recursos

AWS documentación de servicio

- Integraciones de productos ()AWS Security Hub
- Integrándose AWS Security Hub en Jira Service Management Cloud ()AWS Security Hub
- Reglas de automatización (AWS Security Hub)
- Reglas de evaluación proactiva (AWS Config)
- Gestor de parches (AWS Systems Manager)

Otros AWS recursos

- Prácticas recomendadas para etiquetar AWS recursos (documentoAWS técnico)
- Respuesta de seguridad automatizada en (biblioteca de soluciones AWS)AWS
- AWS Guía de respuesta a incidentes de seguridad (guíaAWS técnica)
- AWS boletines de seguridad

Historial de documentos

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

Cambio	Descripción	Fecha
Publicación inicial	—	12 de octubre de 2023

AWS Glosario de orientación prescriptiva

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

Números

Las 7 R

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

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

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

A

ABAC

Consulte control de acceso basado en atributos.

servicios abstractos

Consulte servicios gestionados.

ACID

Consulte atomicidad, consistencia, aislamiento y durabilidad.

migración activa-activa

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

migración activa-pasiva

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

función agregada

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

IA

Véase inteligencia artificial.

AIOps

Consulte las operaciones de inteligencia artificial.

anonimización

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

antipatrones

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

control de aplicaciones

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

cartera de aplicaciones

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

inteligencia artificial (IA)

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

operaciones de inteligencia artificial (AIOps)

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

cifrado asimétrico

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

atomicidad, consistencia, aislamiento, durabilidad () ACID

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

control de acceso basado en atributos () ABAC

La práctica de crear permisos detallados basados en los atributos del usuario, como el departamento, el puesto de trabajo y el nombre del equipo. Para obtener más información, consulte ABACla AWS 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

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

AWS Marco de adopción de la nube ()AWS CAF

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

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

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

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

B

un bot malo

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

BCP

Consulte la planificación de la continuidad del negocio.

gráfico de comportamiento

Una vista unificada e interactiva del comportamiento de los recursos y de las interacciones a lo largo del tiempo. Puede utilizar un gráfico de comportamiento con Amazon Detective para examinar los intentos de inicio de sesión fallidos, las API llamadas sospechosas 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 endianismo.

clasificación binaria

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

filtro de floración

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

implementación azul/verde

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

bot

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

botnet

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

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 (GitHub documentación).

acceso con cristales rotos

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

estrategia de implementación sobre infraestructura existente

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

caché de búfer

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

capacidad empresarial

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

planificación de la continuidad del negocio () BCP

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

C

CAF

Consulte el marco AWS de adopción de la nube.

despliegue canario

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

CCoE

Consulte Cloud Center of Excellence.

CDC

Consulte la captura de datos de cambios.

cambiar la captura de datos (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. Se puede utilizar CDC para varios fines, como auditar o replicar los cambios en un sistema de destino para mantener la sincronización.

ingeniería del caos

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

CI/CD

Consulte la integración continua y la entrega continua.

clasificación

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

cifrado del cliente

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

Centro de excelencia en la nube (CCoE)

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

computación en la nube

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

modelo operativo en la nube

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

etapas de adopción de la nube

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

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

- Reinvención: optimización de productos y servicios e innovación en la nube

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

CMDB

Consulte la base de datos de administración de la configuración.

repositorio de código

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

caché en frío

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

datos fríos

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

visión artificial (CV)

Campo de la IA que utiliza el aprendizaje automático para analizar y extraer información de formatos visuales, como imágenes y vídeos digitales. Por ejemplo, AWS Panorama ofrece dispositivos que añaden CV a las redes de cámaras locales, y Amazon SageMaker proporciona algoritmos de procesamiento de imágenes para CV.

desviación de configuración

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

base de datos de gestión de la 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, se utilizan datos CMDB de una etapa de migración de descubrimiento y análisis de la cartera.

paquete de conformidad

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

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. CI/CD is commonly described as a pipeline. CI/CDpueden 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.

CV

Vea la visión artificial.

D

datos en reposo

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

clasificación de datos

Un proceso para identificar y clasificar los datos de su red en función de su importancia y sensibilidad. Es un componente fundamental de cualquier estrategia de administración de riesgos de ciberseguridad porque lo ayuda a determinar los controles de protección y retención adecuados para los datos. La clasificación de datos es un componente del pilar de seguridad del AWS Well-Architected Framework. Para obtener más información, consulte Clasificación de datos.

desviación de datos

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

datos en tránsito

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

malla de datos

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

minimización de datos

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

perímetro de datos

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

preprocesamiento de datos

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

procedencia de los datos

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

titular de los datos

Persona cuyos datos se recopilan y procesan.

almacenamiento de datos

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

lenguaje de definición de bases 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 bases de datos (DML)

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

DDL

Consulte el lenguaje de definición de bases de datos.

conjunto profundo

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

aprendizaje profundo

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

defense-in-depth

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

administrador delegado

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

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

Implementación

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

entorno de desarrollo

Consulte entorno.

control de detección

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

mapeo del flujo de valor de 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. DVSMamplía el proceso de mapeo del flujo de valor diseñado originalmente para las prácticas de fabricación ajustada. Se centra en los pasos y los equipos necesarios para crear y transferir valor a través del proceso de desarrollo de software.

gemelo digital

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

tabla de dimensiones

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

desastre

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

recuperación de desastres (DR)

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

DML

Consulte el lenguaje de manipulación de bases de datos.

diseño basado en el dominio

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

DR

Consulte recuperación ante desastres.

detección de desviaciones

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

DVSM

Consulte el mapeo del flujo de valor del desarrollo.

E

EDA

Consulte el análisis exploratorio de datos.

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

Un servicio que puede alojar en una nube privada virtual (VPC) para compartirlo con otros usuarios. Puede crear un servicio de punto final con otros Cuentas de AWS o AWS Identity and Access Management (IAM) principales AWS PrivateLink y conceder permisos a ellos. Estas cuentas o entidades principales pueden conectarse a su servicio de puntos finales de forma privada mediante la creación de puntos finales de interfazVPC. Para obtener más información, consulte Crear un servicio de punto final en la documentación de Amazon Virtual Private Cloud (AmazonVPC).

planificación de recursos empresariales (ERP)

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

cifrado de sobre

El proceso de cifrar una clave de cifrado con otra clave de cifrado. Para obtener más información, consulte Cifrado de sobres 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 cuestiones AWS CAF de seguridad incluyen la gestión de identidades y accesos, los controles de detección, la seguridad de la infraestructura, la protección de datos y la respuesta a incidentes. Para obtener más información sobre las epopeyas en la estrategia de migración de AWS , consulte la Guía de implementación del programa.

ERP

Consulte la planificación de recursos empresariales.

análisis exploratorio de datos () 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. EDAse realiza mediante el cálculo de estadísticas resumidas y la creación de visualizaciones de datos.

F

tabla de datos

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

fallan rápidamente

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

límite de aislamiento de fallas

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

rama de característica

Consulte la sucursal.

características

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

importancia de las características

La importancia que tiene una característica para las predicciones de un modelo. Por lo general, 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 detallado () 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 el cumplimiento en todas las unidades organizativas (). OUs Las barreras de protección preventivas aplican políticas para garantizar la alineación con los estándares de conformidad. Se implementan mediante políticas de control de servicios y límites de IAM permisos. Las barreras de protección de detección detectan las vulneraciones de las políticas y los problemas de conformidad, y generan alertas para su corrección. Se implementan mediante Amazon AWS Config AWS Security Hub GuardDuty AWS Trusted Advisor, Amazon Inspector y AWS Lambda cheques personalizados.

H

JA

Consulte alta disponibilidad.

migración heterogénea de bases de datos

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

alta disponibilidad (HA)

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

modernización histórica

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

migración homogénea de bases de datos

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

datos recientes

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

hotfix

Una solución urgente para un problema crítico en un entorno de producción. Debido a su urgencia, una revisión se suele realizar fuera del flujo de trabajo de DevOps publicación habitual.

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

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

aplicación inactiva

Aplicación que tiene un uso medio CPU de memoria entre el 5 y el 20 por ciento durante un período de 90 días. En un proyecto de migración, es habitual retirar estas aplicaciones o mantenerlas en las instalaciones.

IIoT

Consulte Internet de las cosas industrial.

infraestructura inmutable

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

entrante (ingreso) VPC

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

Industria 4.0

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

infraestructura

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

infraestructura como código (IaC)

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

Internet de las cosas industrial () 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 (IIoT) industrial.

inspección VPC

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

Internet de las cosas (IoT)

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

interpretabilidad

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

IoT

Consulte Internet de las cosas.

Biblioteca de información de TI (ITIL)

Conjunto de prácticas recomendadas para ofrecer servicios de TI y alinearlos con los requisitos empresariales. ITILproporciona la base paraITSM.

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 ITSM las herramientas, consulte la guía de integración de operaciones.

ITIL

Consulte la biblioteca de información de TI.

ITSM

Consulte Administración de servicios de TI.

L

control de acceso basado en etiquetas () LBAC

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

zona de aterrizaje

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

migración grande

Migración de 300 servidores o más.

LBAC

Consulte el control de acceso basado en etiquetas.

privilegio mínimo

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

migrar mediante lift-and-shift

Consulte 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.

malware

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

servicios gestionados

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

sistema de ejecución de fabricación () MES

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

MAP

Consulte Migration Acceleration Program.

mecanismo

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

cuenta de miembro

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

MES

Consulte el sistema de ejecución de la fabricación.

Transporte de telemetría y cola de mensajes () MQTT

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

microservicio

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

arquitectura de microservicios

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

Migration Acceleration Program (MAP)

Un AWS programa que brinda soporte de consultoría, capacitación y servicios para ayudar a las organizaciones a construir una base operativa sólida para migrar a la nube y para ayudar a compensar el costo inicial de las migraciones. MAPincluye 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 habituales.

migración a escala

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

fábrica de migración

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

metadatos de migración

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

patrón de migración

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

Evaluación de la cartera de migración () MPA

Una herramienta en línea que proporciona información para validar el argumento empresarial para migrar a. Nube de AWS MPAproporciona una evaluación detallada de la cartera (tamaño

correcto de los servidores, precios, TCO comparaciones y 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 la oleada). La MPAherramienta (requiere iniciar sesión) está disponible de forma gratuita para todos los consultores y AWS consultores de los socios. APN

Evaluación de la preparación para la migración (MRA)

El proceso que consiste en obtener información sobre el estado de preparación de una organización para la nube, identificar los puntos fuertes y débiles y elaborar un plan de acción para cerrar las brechas identificadas, utilizando la AWS CAF. Para obtener más información, consulte la Guía de preparación para la migración. MRAes la primera fase de la estrategia de AWS migración.

estrategia de migración

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

ML

Consulte el aprendizaje automático.

modernización

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

evaluación de la preparación para la modernización

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

aplicaciones monolíticas (monolitos)

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

MPA

Consulte la evaluación de la cartera de migración.

MQTT

Consulte Message Queue Queue Telemetría y Transporte.

clasificación multiclase

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

infraestructura mutable

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

O

OAC

Consulte el control de acceso de origen.

OAI

Consulte la identidad de acceso de origen.

OCM

Consulte gestión del cambio organizacional.

migración fuera de línea

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

OI

Consulte integración de operaciones.

OLA

Consulte el acuerdo a nivel operativo.

migración en línea

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

OPC-UA

Consulte Open Process Communications: arquitectura unificada.

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

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

acuerdo a nivel operativo () OLA

Un acuerdo que aclara lo que los grupos de TI funcionales se prometen ofrecer entre sí, para respaldar un acuerdo de nivel de servicio (). SLA

revisión de la preparación operativa () ORR

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

tecnología operativa (OT)

Sistemas de hardware y software que funcionan con el entorno físico para controlar las operaciones, los equipos y la infraestructura industriales. En la industria manufacturera, la

integración de los sistemas de TO y tecnología de la información (TI) es un enfoque clave para las transformaciones de la industria 4.0.

integración de operaciones (OI)

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

registro de seguimiento organizativo

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

gestión del cambio organizacional (OCM)

Marco para administrar las transformaciones empresariales importantes y disruptivas desde la perspectiva de las personas, la cultura y el liderazgo. OCMayuda a las organizaciones a prepararse para los nuevos sistemas y estrategias y a realizar la transición a ellos acelerando la adopción del cambio, abordando los problemas de la transición e impulsando los cambios culturales y organizacionales. En la estrategia de AWS migración, este marco se denomina aceleración de las personas, debido a la velocidad de cambio que requieren los proyectos de adopción de la nube. Para obtener más información, consulte la OCMguía.

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). OACadmite todos los depósitos de S3 Regiones de AWS, el cifrado del lado del servidor con AWS KMS (SSE-KMS) y el cifrado dinámico `PUT` y `DELETE` las solicitudes al depósito de S3.

identidad de acceso de origen () OAI

En CloudFront, una opción para restringir el acceso y proteger el contenido de Amazon S3. Cuando lo usaOAI, 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 OAC, que proporciona un control de acceso mejorado y más detallado.

ORR

Consulte la revisión de la preparación operativa.

NO

Consulte tecnología operativa.

saliente (salida) VPC

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

P

límite de permisos

Una política IAM de administración asociada a IAM los directores para establecer los permisos máximos que puede tener el usuario o el rol. Para obtener más información, consulte los límites de los permisos en la IAM documentación.

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 PII incluyen nombres, direcciones e información de contacto.

PII

Consulte la información de identificación personal.

manual de estrategias

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

PLC

Consulte controlador lógico programable.

PLM

Consulte la gestión del ciclo de vida del producto.

política

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

persistencia políglota

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

evaluación de cartera

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

predicate

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

pulsar un predicado

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

control preventivo

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

entidad principal

Una entidad AWS que puede realizar acciones y acceder a los recursos. Esta entidad suele ser un usuario raíz de un Cuenta de AWS, un IAM rol o un usuario. Para obtener más información, consulte los términos y conceptos de Principal in Roles en la IAM documentación.

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

Un contenedor que contiene información sobre cómo desea que Amazon Route 53 responda a DNS las consultas de un dominio y sus subdominios dentro de uno o másVPCs. 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 no conformes. Estos controles escanean los recursos antes de aprovisionarlos. Si el recurso no cumple con el control, significa que no está aprovisionado. Para obtener más información, consulte la guía de referencia de controles en la AWS Control Tower documentación y consulte Controles proactivos en Implementación de controles de seguridad en AWS.

gestión del ciclo de vida del producto (PLM)

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

entorno de producción

Consulte el entorno.

controlador lógico programable () PLC

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

seudonimización

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

publish/subscribe (pub/sub)

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

Q

plan de consulta

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

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

RACImatriz

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.

RASCImatriz

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

RCAC

Consulte el 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

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

regresión

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

volver a alojar

Consulte 7 Rs.

versión

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

trasladarse

Ver 7 Rs.

redefinir la plataforma

Ver 7 Rs.

recompra

Ver 7 Rs.

resilencia

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

política basada en recursos

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

matriz responsable, responsable, consultada, 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 RASCImatriz y, si la excluye, se denomina RACImatriz.

control receptivo

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

retain

Consulte 7 Rs.

jubilarse

Ver 7 Rs.

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 SQL expresiones básicas y flexibles que tienen reglas de acceso definidas. RCACconsta 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

SAML2.0

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

SCADA

Consulte el control de supervisión y la adquisición de datos.

SCP

Consulte la política de control de servicios.

secreta

Información confidencial o restringida, como una contraseña o credenciales de usuario, que almacene de forma cifrada. AWS Secrets Manager Se compone del valor secreto y sus

metadatos. El valor secreto puede ser binario, una sola cadena o varias cadenas. Para obtener más información, consulta ¿Qué hay en un secreto de Secrets Manager? en la documentación de Secrets Manager.

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. Hay cuatro tipos principales de controles de seguridad: preventivos, de detección, de respuesta y proactivos.

refuerzo de la seguridad

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

sistema de información de seguridad y gestión de eventos (SIEM)

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

automatización de las respuestas 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 automática incluyen la modificación de un grupo VPC de seguridad, la aplicación de parches a una EC2 instancia de Amazon o la rotación de credenciales.

cifrado del servidor

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

política de control de servicios (SCP)

Una política que proporciona un control centralizado de los permisos de todas las cuentas de una organización en AWS Organizations. SCPsdefina barreras o establezca límites a las acciones que un administrador puede delegar en usuarios o roles. Puede utilizarlas SCPs como listas de permitidos o rechazados para especificar qué servicios o acciones están permitidos o

prohibidos. Para obtener más información, consulte las políticas de control de servicios en la AWS Organizations documentación.

punto de enlace de servicio

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

acuerdo de nivel de servicio () SLA

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

indicador de nivel de servicio () SLI

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

objetivo de nivel de servicio () SLO

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

modelo de responsabilidad compartida

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

SIEM

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

punto único de fallo (SPOF)

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

SLA

Consulte el acuerdo de nivel de servicio.

SLI

Consulte el indicador de nivel de servicio.

SLO

Consulte el objetivo de nivel de servicio.

split-and-seed modelo

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

SPOF

Consulte el punto único de fallo.

esquema en forma de estrella

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

patrón de higo estrangulador

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

subred

Un rango de direcciones IP en su. VPC Una subred debe residir en una sola zona de disponibilidad.

control de supervisión y adquisición de datos (SCADA)

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

cifrado simétrico

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

pruebas sintéticas

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

T

etiquetas

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

variable de destino

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

lista de tareas

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

entorno de prueba

Consulte entorno.

entrenamiento

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

puerta de enlace de tránsito

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

flujo de trabajo basado en enlaces troncales

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

acceso de confianza

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

ajuste

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

equipo de dos pizzas

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

U

incertidumbre

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

tareas indiferenciadas

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

entornos superiores

Ver entorno.

V

succión

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

control de versión

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

VPCmirando

Una conexión entre dos VPCs que permite enrutar el tráfico mediante direcciones IP privadas. Para obtener más información, consulta Qué es el VPC peering en la VPC documentación de Amazon.

vulnerabilidad

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

W

caché caliente

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

datos templados

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

función de ventana

SQLFunción 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.

WORM

Mira, escribe una vez, lee muchas.

WQF

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

escribe una vez, lee muchas (WORM)

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

Z

ataque de día cero

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

vulnerabilidad de día cero

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

aplicación zombi

Una aplicación que tiene un uso medio CPU de memoria inferior 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.