Implementación de una estrategia de control de bots en AWS

AWS Guía prescriptiva

AWS Guía prescriptiva: Implementación de una estrategia de control de bots en AWS

Table of Contents

Implementación de una estrategia de control de bots en AWS

Amazon Web Services (colaboradores)

Febrero de 2024 (historial del documento)

Internet tal como lo conocemos no sería posible sin los bots. Los bots ejecutan tareas automatizadas a través de Internet y simulan la actividad o interacción humana. Permiten a las empresas incorporar eficiencia a sus procesos y tareas. Los bots útiles, como los rastreadores web, indexan información en Internet y nos ayudan a encontrar rápidamente la información más relevante para nuestras consultas de búsqueda. Los bots son un buen mecanismo para mejorar los negocios y aportar valor a las empresas. Sin embargo, con el tiempo, los delincuentes empezaron a utilizar los bots como medio para abusar de los sistemas y aplicaciones existentes de formas nuevas y creativas.

Las botnets son el mecanismo más conocido para escalar los bots y su impacto. Las botnets son redes de bots que están infectadas por malware y que están bajo el control de una sola parte, conocida como el pastor o el operador de los bots. Desde un punto central, el operador puede ordenar a todos los ordenadores de su botnet que lleven a cabo simultáneamente una acción coordinada, por lo que las botnets también se denominan sistemas command-and-control (C2).

La escala de una botnet puede ser de varios millones de bots. Una botnet ayuda al operador a realizar acciones a gran escala. Como las botnets permanecen bajo el control de un operador remoto, las máquinas infectadas pueden recibir actualizaciones y cambiar su comportamiento sobre la marcha. Como resultado, para obtener importantes beneficios económicos, los sistemas C2 pueden alquilar el acceso a segmentos de su red de bots en el mercado negro.

La prevalencia de las botnets ha seguido creciendo. Los expertos lo consideran la herramienta favorita de los malos actores. Mirai es una de las mayores botnets. Surgió en 2016, sigue en funcionamiento y se estima que ha infectado hasta 350.000 dispositivos de Internet de las cosas (IoT). Esta botnet se ha adaptado y utilizado para muchos tipos de actividades, incluidos los ataques distribuidos de denegación de servicio (DDoS). Más recientemente, los delincuentes intentaron ocultar aún más su actividad y obtener su tráfico mediante la obtención de direcciones IP mediante el uso de servicios de proxy residenciales. Esto crea un peer-to-peer sistema legítimo e interconectado que añade sofisticación a la actividad y dificulta su detección y mitigación.

Este documento se centra en el panorama de los bots, su efecto en las aplicaciones y las estrategias y opciones de mitigación disponibles. Esta guía prescriptiva y sus prácticas recomendadas le ayudan

a comprender y mitigar los distintos tipos de ataques de bots. Además, en esta guía se describen las estrategias de mitigación de los bots Servicios de AWS y sus características, y cómo cada una de ellas puede ayudarle a proteger sus aplicaciones. También incluye una descripción general de la supervisión de los bots y las mejores prácticas para optimizar los costes de las soluciones.

Comprensión de las amenazas y las operaciones de los bots

Según Security Today, más del 47% de todo el tráfico de Internet se debe a los bots. Esto incluye la parte útil de los bots, aquellos que se autoidentifican y aportan valor. Alrededor del 30% del tráfico de bots está compuesto por bots no identificados que realizan actividades maliciosas, como ataques tipo DDo S, reventa de entradas, robo de inventario o acaparamiento. La revista Security Magazine informa de un aumento del 300% en los eventos DDo S volumétricos durante la primera mitad de 2023. Esto hace que este tema sea más relevante y hace que el conocimiento sobre las herramientas y tecnologías de prevención y protección disponibles sea aún más importante.

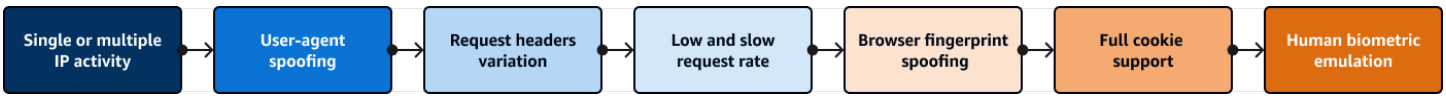
La siguiente tabla clasifica los distintos tipos de actividad de los bots y el impacto empresarial que cada uno de ellos puede tener. No se trata de una lista exhaustiva, sino de un resumen de las actividades de bots más comunes. Destaca la importancia de los controles de monitoreo y mitigación. Para obtener una lista exhaustiva de las amenazas provocadas por los bots, consulte el manual de amenazas automatizadas a las aplicaciones de OWASP (sitio web de OWASP).

Tipo de actividad del bot	Description (Descripción)	Impacto potencial
Extracción de contenido	Copia de contenido patentado para su uso en sitios de terceros	El impacto en tu SEO se debe a la duplicación del contenido , al impacto en la marca y a los problemas de rendimiento causados por la agresividad de los rastreadores
Relleno de credenciales	Pruebas de las bases de datos de credenciales robadas en su sitio web para obtener acceso a la información o validarla	Problemas para los usuarios, como el fraude y el bloqueo de cuentas, que aumentan las consultas de soporte y disminuyen la confianza en la marca
Desciframiento de tarjetas	Probar bases de datos de datos de tarjetas de crédito robadas para validar o complementar la información faltante	Problemas para los usuarios, como el robo de identidad y el fraude, y daños en la puntuación de fraude

Tipo de actividad del bot	Description (Descripción)	Impacto potencial
Denegación del servicio	Aumentar el tráfico a un sitio web específico para ralentizar la respuesta o hacer que no esté disponible para el tráfico legítimo	Pérdida de ingresos y daños a la reputación
Creación de una cuenta	Creación de varias cuentas con el propósito de utilizarlas indebidamente o con fines lucrativos	Obstaculizó el crecimiento y sesgó los análisis de marketing
Scalping	Adquirir productos de disponibilidad limitada, entradas frecuentes, en lugar de consumidores genuinos	Pérdida de ingresos y problemas para los usuarios, como la falta de acceso a los productos que se venden

¿Cómo funcionan las botnets

Las tácticas, técnicas y procedimientos (TTP) de los operadores de botnets han evolucionado sustancialmente con el tiempo. Han tenido que mantenerse al día con las tecnologías de detección y mitigación desarrolladas por las empresas. La siguiente figura muestra esta evolución. Las botnets comenzaron simplemente con el uso de direcciones IP como medio de operación y, finalmente, evolucionaron para utilizar una sofisticada emulación biométrica humana. Esta sofisticación es cara y no todas las botnets utilizan las herramientas más avanzadas. Hay una mezcla de operadores en Internet y es probable que evalúen cuál es la mejor herramienta para el trabajo a fin de ofrecer un buen retorno de la inversión. Uno de los objetivos de la defensa contra los bots es encarecer la actividad de las redes de bots para que el objetivo deje de ser viable.



Por lo general, los bots se clasifican en comunes o segmentados:

- Bots comunes: estos bots se identifican a sí mismos y no intentarán emular a los navegadores. Muchos de estos bots realizan tareas útiles, como el rastreo de contenido, la optimización de

motores de búsqueda (SEO) o la agregación. Es importante identificar y entender cuáles de estos bots habituales llegan a tu sitio y el efecto que tienen en el tráfico y el rendimiento.

- Bots segmentados: estos bots intentan evadir la detección emulando los navegadores. Utilizan la tecnología de los navegadores, como los navegadores headless, o falsifican las huellas digitales del navegador. Tienen la capacidad de ejecutar JavaScript y admitir cookies. Su intención no siempre está clara y el tráfico que generan puede parecerse al tráfico normal de los usuarios.

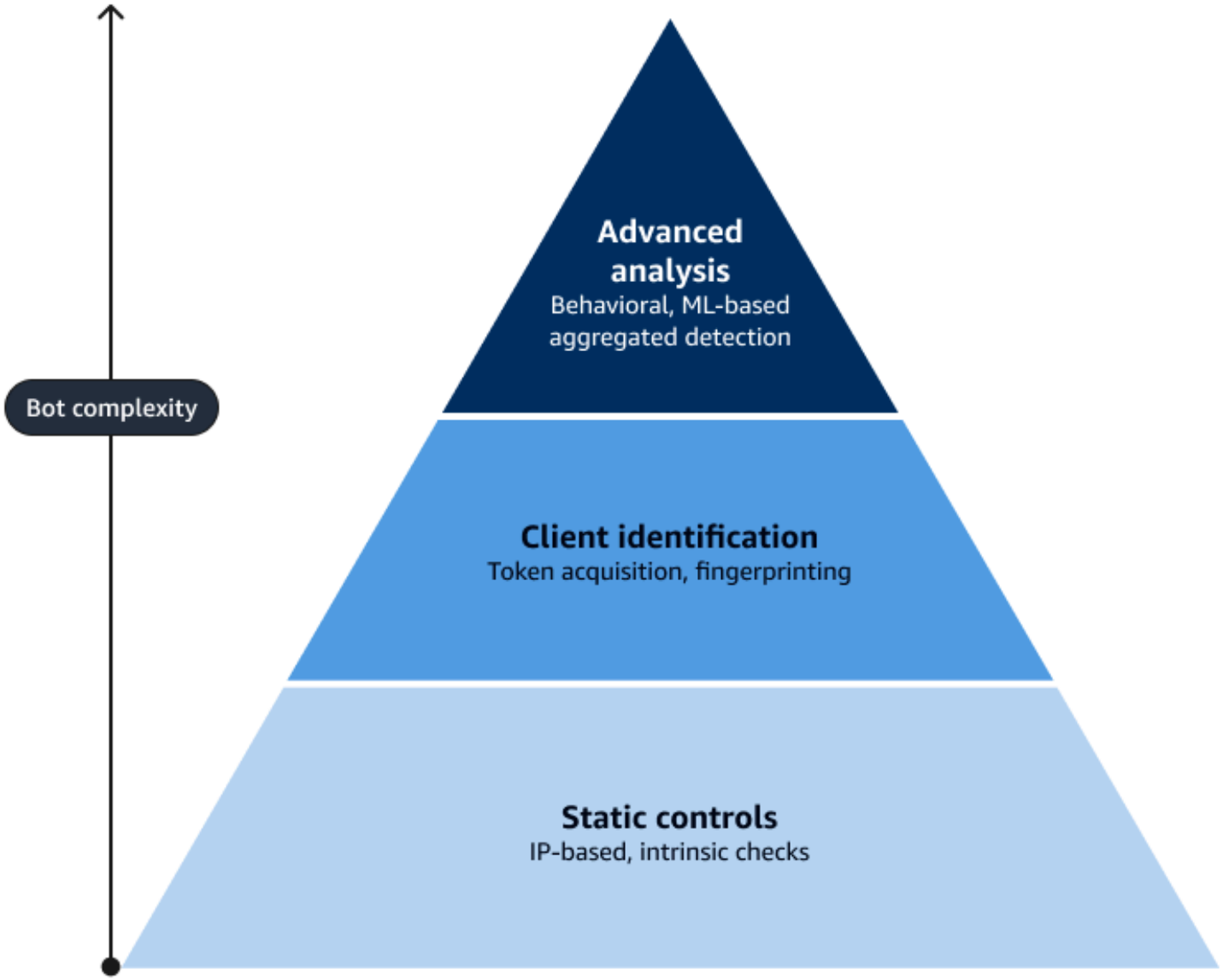
Los bots segmentados más avanzados y persistentes emulan el comportamiento humano al generar movimientos de ratón y clics similares a los de los humanos en un sitio web. Son los más sofisticados y difíciles de detectar, pero también los más caros de operar.

A menudo, un operador combina estas técnicas. Esto crea un juego de persecución constante, en el que hay que cambiar con frecuencia el enfoque de protección y mitigación para adaptarlo a las técnicas más recientes del operador. Estos bots se consideran una amenaza persistente avanzada (APT). Para obtener más información, consulte Amenaza persistente avanzada en el centro de recursos del NIST.

Técnicas para el control de bots

El objetivo principal de la mitigación de los bots es limitar el impacto negativo de la actividad automatizada de los bots en los sitios web, los servicios y las aplicaciones de una organización. La tecnología y las técnicas utilizadas dependen del tipo de tráfico o actividad contra el que quieras defenderte. Para lograrlo, es fundamental comprender la aplicación y su tráfico. Para obtener más información sobre por dónde empezar, consulte la Directrices para monitorizar tu estrategia de control de bots sección de esta guía.

En general, los controles que proporcionan las soluciones de mitigación de bots se pueden agrupar en las siguientes categorías de alto nivel: estáticos, de identificación de clientes y análisis avanzado. En la siguiente figura se muestran las diferentes técnicas disponibles y cómo se pueden utilizar en función de la complejidad de la actividad del bot. Esto pone de relieve cómo se puede obtener la base, o la mitigación más amplia, mediante el uso de controles estáticos, como las comprobaciones intrínsecas y de registro de permisos. La parte más pequeña de los bots es siempre la más avanzada, y mitigarlos requiere una tecnología más avanzada y una combinación de controles.



A continuación, esta guía explora cada categoría y sus técnicas. También describe las opciones disponibles AWS WAFpara implementar estos controles:

- Controles estáticos para gestionar los bots
- Controles de identificación de clientes para gestionar los bots
- Controles de análisis avanzados para gestionar los bots

Controles estáticos para gestionar los bots

Para realizar una acción, los controles estáticos evalúan la información estática de la solicitud HTTP (S), como su dirección IP o sus encabezados. Estos controles pueden resultar útiles para las

actividades de bots incorrectas poco sofisticadas o para el tráfico de bots potencialmente beneficioso que se espera que deba verificarse y gestionarse. Entre las técnicas de control estático se incluyen las listas de permisos, los controles basados en IP y las comprobaciones intrínsecas.

¿Permitir la inclusión

Permitir la publicación es un control que permite identificar el tráfico amigable mediante los controles de mitigación de bots existentes. Existen diversas formas de lograrlo. La más sencilla consiste en utilizar una regla que coincida con un conjunto de direcciones IP o con una condición de coincidencia similar. Cuando una solicitud coincide con una regla que está configurada para una `Allow` acción, las reglas posteriores no la evalúan. En algunos casos, es necesario evitar que solo se apliquen determinadas reglas; en otras palabras, es necesario permitir la lista de una regla, pero no de todas. Este es un escenario habitual para gestionar los falsos positivos en las reglas. Permitir la inclusión en la lista se considera una regla de amplio alcance. Para reducir la posibilidad de que aparezcan falsos negativos, te recomendamos que la asocies con otra opción que sea más detallada, como una coincidencia de ruta o encabezado.

Controles basados en IP

Bloques de direcciones IP únicas

Una herramienta que se utiliza habitualmente para mitigar el impacto de los bots consiste en limitar las solicitudes de un único solicitante. El ejemplo más simple es bloquear la dirección IP de origen del tráfico si sus solicitudes son maliciosas o tienen un volumen elevado. Esto utiliza reglas de coincidencia de conjuntos de AWS WAF IP para implementar bloqueos basados en IP. Estas reglas coinciden con las direcciones IP y aplican una acción de `BlockChallenge`, o`CAPTCHA`. Para determinar cuándo llegan demasiadas solicitudes desde una dirección IP, consulte la red de entrega de contenido (CDN), un firewall de aplicaciones web o los registros de aplicaciones y servicios. Sin embargo, en la mayoría de los casos, este control no es práctico sin la automatización.

La automatización de las listas de direcciones IP bloqueadas AWS WAF se suele realizar con reglas basadas en tasas. Para obtener más información, consulte la sección Reglas basadas en frecuencia de esta guía. También puede implementar las automatizaciones de seguridad para la solución. AWS WAF Esta solución actualiza automáticamente una lista de direcciones IP para bloquearlas y una AWS WAF regla deniega las solicitudes que coinciden con esas direcciones IP.

Una forma de reconocer un ataque de bot es si una multitud de solicitudes de la misma dirección IP se centran en un número reducido de páginas web. Esto indica que el bot está descartando

precios o intentando iniciar sesión repetidamente, lo que supone un alto porcentaje de errores. Puedes crear automatizaciones que reconozcan inmediatamente este patrón. Las automatizaciones bloquean la dirección IP, lo que reduce la eficacia del ataque al identificarlo y mitigarlo rápidamente. El bloqueo de direcciones IP específicas es menos eficaz cuando un atacante tiene un gran conjunto de direcciones IP desde las que lanzar ataques o cuando el comportamiento de ataque es difícil de reconocer y separar del tráfico normal.

Reputación de la dirección IP

Un servicio de reputación IP proporciona información que ayuda a evaluar la confiabilidad de una dirección IP. Por lo general, esta inteligencia se obtiene mediante la agregación de información relacionada con la IP de la actividad pasada de esa dirección IP. La actividad previa ayuda a indicar la probabilidad de que una dirección IP genere solicitudes maliciosas. Los datos se agregan a las listas administradas que rastrean el comportamiento de las direcciones IP.

Las direcciones IP anónimas son un caso especializado de reputación de direcciones IP. La dirección IP de origen proviene de fuentes conocidas de direcciones IP fáciles de adquirir, como máquinas virtuales basadas en la nube, o de proxies, como proveedores de VPN conocidos o nodos Tor. Los grupos de reglas gestionados por la lista de reputación IP de AWS WAF Amazon y la lista de IP anónimas utilizan la inteligencia de amenazas interna de Amazon para ayudar a identificar estas direcciones IP.

La información proporcionada por estas listas gestionadas puede ayudarle a actuar en función de las actividades identificadas a partir de estas fuentes. Basándose en esta información, puede crear reglas que bloqueen directamente el tráfico o reglas que limiten el número de solicitudes (como las reglas basadas en tarifas). También puedes usar esta información para evaluar el origen del tráfico mediante las reglas del `COUNT` modo. De este modo, se examinan los criterios de coincidencia y se aplican etiquetas que puede utilizar para crear reglas personalizadas.

Reglas basadas en frecuencia

Las reglas basadas en tasas pueden ser una herramienta valiosa en determinados escenarios. Por ejemplo, las reglas basadas en tarifas son eficaces cuando el tráfico de bots alcanza volúmenes elevados en comparación con los usuarios que utilizan identificadores uniformes de recursos confidenciales (URIs) o cuando el volumen de tráfico comienza a afectar a las operaciones normales. La limitación de velocidad puede mantener las solicitudes en niveles manejables y limitar y controlar el acceso. AWS WAF puede implementar una regla de limitación de velocidad en una lista de control de acceso web (ACL web) mediante una declaración de reglas basada en la velocidad. Cuando se utilizan reglas basadas en la tasa, se recomienda incluir una regla general que abarque todo el sitio,

reglas específicas de la URI y reglas basadas en la tasa de reputación de la IP. Las reglas basadas en la tasa de reputación de IP combinan la inteligencia de la reputación de la dirección IP con la funcionalidad de limitar la velocidad.

Para todo el sitio, una regla general basada en la tasa de reputación de IP crea un límite que impide que bots poco sofisticados inunden un sitio a partir de un número reducido de ellos. IPs La limitación de velocidad se recomienda especialmente para proteger las páginas URIs que tienen un alto coste o impacto, como las páginas de inicio de sesión o de creación de cuentas.

Las reglas que limitan la velocidad pueden proporcionar una primera capa de defensa rentable. Puede utilizar reglas más avanzadas para proteger los datos confidenciales. URIs Las reglas basadas en tarifas específicas de la URI pueden limitar el impacto en las páginas críticas o en las APIs que afectan al backend, como el acceso a la base de datos. Las mitigaciones avanzadas para proteger determinadas variables URIs, que se analizan más adelante en esta guía, suelen implicar costes adicionales, y estas reglas basadas en las tarifas específicas de los URI pueden ayudarle a controlar los costes. Para obtener más información sobre las reglas basadas en tarifas que se recomiendan habitualmente, consulte las tres reglas basadas en tarifas más importantes AWS WAF en el blog de seguridad. AWS En algunas situaciones, resulta útil limitar el tipo de solicitud que se evalúa mediante una regla basada en tasas. Puede usar instrucciones de alcance reducido para, por ejemplo, limitar las reglas basadas en la tasa por el área geográfica de la dirección IP de origen.

AWS WAF ofrece una capacidad avanzada para establecer reglas basadas en tasas mediante el uso de claves de agregación. Con esta funcionalidad, puede configurar una regla basada en tasas para utilizar otras claves de agregación y combinaciones de teclas, además de la dirección IP de origen. Por ejemplo, como una combinación única, puede agregar las solicitudes en función de una dirección IP reenviada, el método HTTP y un argumento de consulta. Esto le ayuda a configurar reglas más detalladas para una mitigación sofisticada del tráfico volumétrico.

Controles intrínsecos

Los controles intrínsecos son varios tipos de validaciones o verificaciones internas o inherentes dentro de un sistema o proceso. Para el control de los bots, AWS WAF realiza una comprobación intrínseca al validar que la información enviada en la solicitud coincide con las señales del sistema. Por ejemplo, realiza búsquedas inversas de DNS y otras verificaciones del sistema. Algunas solicitudes automatizadas son necesarias, como las relacionadas con el SEO. Permitir la inclusión en la lista es una forma de permitir el paso de los bots buenos y esperados. Sin embargo, a veces, los bots malintencionados emulan a los buenos y puede resultar difícil separarlos. AWS WAF proporciona métodos para lograrlo mediante el grupo de reglas de control de AWS WAF bots

gestionado. Las reglas de este grupo permiten comprobar que los bots autoidentificados son quienes dicen ser. AWS WAF compara los detalles de la solicitud con el patrón conocido de ese bot y también realiza búsquedas inversas en el DNS y otras verificaciones objetivas.

Controles de identificación de clientes para gestionar los bots

Si el tráfico relacionado con los ataques no se puede reconocer fácilmente mediante atributos estáticos, la detección debe poder identificar con precisión al cliente que realiza la solicitud. Por ejemplo, las reglas basadas en la tasa suelen ser más eficaces y más difíciles de evadir cuando el atributo al que se limita la velocidad es específico de la aplicación, como una cookie o un token. El uso de una cookie vinculada a una sesión evita que los operadores de botnets puedan duplicar flujos de solicitudes similares en muchos bots.

La adquisición de fichas se suele utilizar para identificar a los clientes. Para la adquisición de fichas, un JavaScript código recopila información para generar una ficha que se evalúa en el servidor. La evaluación puede abarcar desde la verificación de que JavaScript se está ejecutando en el cliente hasta la recopilación de información del dispositivo para la toma de huellas digitales. La adquisición de un token requiere la integración de un JavaScript SDK en el sitio o la aplicación, o bien requiere que un proveedor de servicios realice la inyección de forma dinámica.

La necesidad de JavaScript asistencia supone un obstáculo adicional para los bots que intentan emular los navegadores. Cuando se trata de un SDK, como en una aplicación móvil, la adquisición de un token verifica la implementación del SDK y evita que los bots imiten las solicitudes de la aplicación.

La adquisición de los tokens requiere el uso de una SDKs conexión implementada en el lado del cliente. Las siguientes AWS WAF funciones proporcionan un SDK JavaScript basado en navegadores y un SDK basado en aplicaciones para dispositivos móviles: Bot Control, Fraud Control, prevención de apropiación de cuentas (ATP) y Fraud Control, prevención del fraude en la creación de cuentas (ACFP).

Las técnicas de identificación de los clientes incluyen el CAPTCHA, la creación de perfiles del navegador, la toma de huellas digitales de los dispositivos y la toma de huellas digitales mediante TLS.

CAPTCHA

La prueba de Turing pública y completamente automatizada para diferenciar ordenadores y humanos (CAPTCHA) se utiliza para distinguir entre visitantes robóticos y humanos y para evitar el rastreo de

páginas web, el uso de credenciales y el spam. Existen diversas implementaciones, pero a menudo implican un rompecabezas que un humano puede resolver. CAPTCHAsofrecen una capa adicional de defensa contra los bots más comunes y pueden reducir los falsos positivos en la detección de bots.

AWS WAF permite a las reglas ejecutar una acción de CAPTCHA contra las solicitudes web que coincidan con los criterios de inspección de una regla. Esta acción es el resultado de la evaluación de la información de identificación del cliente recopilada por el servicio. AWS WAF las reglas pueden requerir que se resuelvan problemas relacionados con el CAPTCHA en el caso de recursos específicos a los que suelen dirigirse los bots, como el inicio de sesión, las búsquedas y el envío de formularios. AWS WAF puede enviar CAPTCHA directamente a través de medios intersticiales o utilizando un SDK para gestionarlo desde el lado del cliente. Para obtener más información, consulte CAPTCHA y Challenge en. AWS WAF

Elaboración de perfiles del navegador

La creación de perfiles del navegador es un método de recopilación y evaluación de las características del navegador, como parte de la adquisición de un token, para distinguir a las personas reales que utilizan un navegador interactivo de la actividad distribuida de los bots. Puedes crear perfiles del navegador de forma pasiva mediante los encabezados, el orden de los encabezados y otras características de las solicitudes que son inherentes al funcionamiento de los navegadores.

También puedes crear perfiles del navegador en código mediante la adquisición de tokens. Si se utiliza JavaScript para la creación de perfiles del navegador, puede determinar rápidamente si un cliente es compatible. JavaScript Esto le ayuda a detectar bots simples que no lo admiten. La creación de perfiles del navegador comprueba algo más que los encabezados y la JavaScript compatibilidad con HTTP; la creación de perfiles del navegador dificulta que los bots emulen completamente un navegador web. Ambas opciones de creación de perfiles del navegador tienen el mismo objetivo: encontrar patrones en el perfil del navegador que indiquen una incoherencia con el comportamiento de un navegador real.

AWS WAF El control de bots para los bots objetivo proporciona una indicación, como parte de una evaluación simbólica, de si un navegador muestra indicios de automatización o señales incoherentes. AWS WAF marca la solicitud para realizar la acción especificada en la regla. Para obtener más información, consulte Detectar y bloquear el tráfico avanzado de bots en el blog AWS de seguridad.

Toma de huellas dactilares del dispositivo

La toma de huellas dactilares de los dispositivos es similar a la creación de perfiles del navegador, pero no se limita a los navegadores. El código que se ejecuta en un dispositivo (que puede ser un dispositivo móvil o un navegador web) recopila los detalles del dispositivo y los envía a un servidor back-end. Los detalles pueden incluir los atributos del sistema, como la memoria, el tipo de CPU, el tipo de núcleo del sistema operativo (SO), la versión del sistema operativo y la virtualización.

Puedes utilizar las huellas digitales del dispositivo para reconocer si un bot está emulando un entorno o si hay indicios directos de que se está utilizando la automatización. Además, las huellas dactilares del dispositivo también se pueden utilizar para reconocer las solicitudes repetidas del mismo dispositivo.

Reconocer las solicitudes repetidas del mismo dispositivo, incluso si el dispositivo intenta cambiar algunas características de la solicitud, permite que un sistema interno imponga reglas de limitación de velocidad. Las reglas de limitación de velocidad que se basan en la huella digital del dispositivo suelen ser más eficaces que las reglas de limitación de velocidad basadas en las direcciones IP. Esto le ayuda a mitigar el tráfico de bots que se mueve entre VPNs o desde proxies, pero que proviene de un número reducido de dispositivos.

Cuando se usa con la integración de aplicaciones SDKs, el control de AWS WAF bots para los bots específicos puede agregar el comportamiento de las solicitudes de sesión del cliente. Esto le ayuda a detectar y separar las sesiones de clientes legítimas de las sesiones de clientes malintencionadas, incluso cuando ambas se originan en la misma dirección IP. Para obtener más información sobre el control de AWS WAF bots para los bots objetivo, consulte Detectar y bloquear el tráfico avanzado de bots en el blog AWS de seguridad.

Toma de huellas digitales mediante TLS

Las huellas digitales TLS, también conocidas como reglas basadas en firmas, se utilizan habitualmente cuando los bots se originan en muchas direcciones IP pero presentan características similares. Cuando se utiliza HTTPS, el cliente y el servidor intercambian mensajes para reconocerse y verificarse mutuamente. Establecen algoritmos criptográficos y claves de sesión. Esto se denomina apretón de manos TLS. La forma en que se implementa un protocolo de enlace TLS es una firma que suele ser valiosa para reconocer los grandes ataques repartidos en muchas direcciones IP.

La huella digital TLS permite a los servidores web determinar la identidad de un cliente web con un alto grado de precisión. Solo requiere los parámetros de la primera conexión de paquetes, antes de que se produzca cualquier intercambio de datos entre aplicaciones. En este caso, el cliente web se

refiere a la aplicación que inicia una solicitud, que puede ser un navegador, una herramienta CLI, un script (bot), una aplicación nativa u otro cliente.

Un enfoque de toma de huellas digitales de SSL y TLS es la huella digital. JA3 JA3toma las huellas digitales de una conexión de cliente en función de los campos del mensaje de saludo del cliente del protocolo de enlace SSL o TLS. Le ayuda a crear perfiles de clientes SSL y TLS específicos en diferentes direcciones IP de origen, puertos y certificados X.509.

Amazon CloudFront admite añadir JA3 encabezados a las solicitudes. Un `CloudFront-Viewer-JA3-Fingerprint` encabezado contiene una huella digital hash de 32 caracteres del paquete TLS Client Hello de una solicitud entrante de un espectador. La huella digital encapsula la información sobre cómo se comunica el cliente. Esta información se puede utilizar para perfilar los clientes que comparten el mismo patrón. Puede añadir el `CloudFront-Viewer-JA3-Fingerprint` encabezado a una política de solicitudes de origen y adjuntar la política a una CloudFront distribución. A continuación, puede inspeccionar el valor del encabezado en las aplicaciones de origen o en Lambda @Edge y CloudFront Functions. Puede comparar el valor del encabezado con una lista de huellas de malware conocidas para bloquear los clientes malintencionados. También puede comparar el valor del encabezado con una lista de huellas digitales esperadas para permitir solo las solicitudes de clientes conocidos.

Controles de análisis avanzados para gestionar los bots

Algunos bots utilizan herramientas de engaño avanzadas para evadir activamente la detección. Estos bots imitan el comportamiento humano para realizar una actividad específica, como el scalping. Estos bots tienen un propósito y, por lo general, están vinculados a una gran recompensa monetaria.

Estos bots avanzados y persistentes utilizan una combinación de tecnologías para evitar ser detectados o mezclarse con el tráfico normal. A su vez, esto también requiere una combinación de diferentes tecnologías de detección para identificar y mitigar con precisión el tráfico malicioso.

Casos de uso específicos

Los datos de casos de uso pueden ofrecer oportunidades de detección de bots. Las detecciones de fraude son casos de uso especial en los que se justifica una mitigación especial. Por ejemplo, para evitar el robo de cuentas, puedes comparar una lista de nombres de usuario y contraseñas de cuentas comprometidas con las solicitudes de inicio de sesión o creación de cuentas. Esto ayuda a los propietarios de sitios web a detectar los intentos de inicio de sesión que utilizan credenciales comprometidas. El uso de credenciales comprometidas puede indicar que los bots están intentando

apoderarse de una cuenta o puede tratarse de usuarios que no saben que sus credenciales están comprometidas. En este caso de uso, los propietarios de sitios web pueden tomar medidas adicionales para verificar al usuario y, después, ayudarlo a cambiar su contraseña. AWS WAF proporciona la regla gestionada de prevención de apropiación de cuentas (ATP) de Control de Fraude para este caso de uso.

Detección de bots agregados o a nivel de aplicación

Algunos casos de uso requieren combinar datos sobre las solicitudes de la red de entrega de contenido (CDN) y el backend de la aplicación o el servicio. AWS WAF A veces, incluso es necesario integrar inteligencia de terceros para poder tomar decisiones fiables sobre los bots.

Funcionan en Amazon CloudFront y AWS WAF pueden enviar señales a la infraestructura de backend o, posteriormente, pueden agregar reglas a través de encabezados y etiquetas. CloudFront expone los encabezados de JA3 huellas digitales, como se mencionó anteriormente. Este es un ejemplo de cómo CloudFront proporcionar dichos datos a través de un encabezado. AWS WAF puede enviar etiquetas cuando coincide con una regla. Las reglas posteriores pueden usar estas etiquetas para tomar mejores decisiones sobre los bots. Cuando se combinan varias reglas, puede implementar controles muy detallados. Un caso de uso habitual consiste en hacer coincidir partes de una regla gestionada mediante una etiqueta y, a continuación, combinarlas con otros datos de la solicitud. Para obtener más información, consulta los ejemplos de coincidencia de etiquetas en la AWS WAF documentación.

Análisis de aprendizaje automático

El aprendizaje automático (ML) es una técnica poderosa para hacer frente a los bots. El aprendizaje automático puede adaptarse a los cambios de los detalles y, cuando se combina con otras herramientas, proporciona la forma más sólida y completa de mitigar los bots con un mínimo de falsos positivos. Las dos técnicas de aprendizaje automático más comunes son el análisis del comportamiento y la detección de anomalías. Con el análisis del comportamiento, un sistema (en el cliente, el servidor o ambos) supervisa la forma en que un usuario interactúa con la aplicación o el sitio web. Supervisa los patrones de movimiento del ratón o la frecuencia de las interacciones entre el clic y el tacto. Luego, el comportamiento se analiza con un modelo de aprendizaje automático para reconocer los bots. La detección de anomalías es similar. Se centra en detectar comportamientos o patrones que son significativamente diferentes de una línea de base definida para la aplicación o el sitio web.

AWS WAF Los controles específicos para bots proporcionan una tecnología predictiva de aprendizaje automático. Esta tecnología ayuda a defenderse de los ataques distribuidos y basados

en proxies realizados por bots diseñados para evadir la detección. El grupo de reglas de control de AWS WAF bots gestionado utiliza un análisis automatizado y basado en el aprendizaje automático de las estadísticas de tráfico de sitios web para detectar un comportamiento anómalo que sea indicativo de una actividad de bots distribuida y coordinada.

Despliegue e implementación de su estrategia de control de bots

Hay varios factores que se deben tener en cuenta a la hora de planificar una estrategia de despliegue del control de bots. Además de las características únicas de las aplicaciones web, el tamaño del entorno, el proceso de desarrollo y la estructura organizativa afectan a la estrategia de despliegue. Según las características del entorno y la aplicación, se puede utilizar una estrategia de implementación centralizada o descentralizada:

- Estrategia de implementación centralizada: un enfoque centralizado permite un mayor grado de control cuando se desea aplicar estrictamente el control de los bots. Este enfoque es ideal si los equipos de aplicaciones prefieren delegarse de la administración. Un enfoque centralizado es más eficaz cuando las aplicaciones web comparten características similares. En este caso, las aplicaciones se benefician de un conjunto común de reglas de control de bots y acciones de mitigación de bots.
- Estrategia de despliegue descentralizado: un enfoque descentralizado proporciona a los equipos de aplicaciones autonomía para definir e implementar las configuraciones de control de bots de forma independiente. Este enfoque es común en entornos más pequeños o cuando los equipos de aplicaciones necesitan mantener el control sobre sus políticas de control de bots. Debido a la naturaleza de muchas aplicaciones web, a menudo es necesario mantener políticas de control de bots independientes que se adapten a las características únicas de las aplicaciones, lo que resulta en un enfoque descentralizado.
- Estrategia combinada: una combinación de estos dos enfoques es adecuada para una combinación de aplicaciones web. Por ejemplo, esto podría implicar un conjunto de reglas básicas que se apliquen a toda la web ACLs, mientras que la gestión de políticas de control de bots más específicas se delegue en los equipos de aplicaciones.

Puede utilizarlas AWS Firewall Managerpara centralizar y automatizar el despliegue de AWS WAF sitios web ACLs que definen las políticas de control de bots. Cuando utilice Firewall Manager, considere si es apropiado centralizar las políticas de control de bots, incluso si deben delegarse a los equipos de aplicaciones. Con Firewall Manager, puede usar el etiquetado para permitir que los equipos de aplicaciones opten por AWS WAF las políticas. Esto proporciona una funcionalidad AWS WAF inteligente de mitigación de amenazas. También puede habilitar el AWS WAF registro centralizado para las operaciones de aplicaciones y seguridad.

Independientemente de la estrategia de despliegue utilizada, se recomienda definir y gestionar el proceso de incorporación mediante marcos basados en la infraestructura como código (IaC), como AWS CloudFormationo el. AWS Cloud Development Kit (AWS CDK) Esto le ayuda a configurar el control de código fuente para almacenar y versionar los objetos de configuración. Para obtener más información, consulte los ejemplos de AWS WAF configuración de AWS CDK(GitHub) y CloudFormation(AWS documentación).

Estrategia de implementación

Una vez que haya seleccionado una estrategia de despliegue, podrá comenzar la implementación. La estrategia de despliegue define cómo se implementan las reglas en las distintas aplicaciones. En la estrategia de implementación, la atención se centra en el proceso iterativo de agregar controles, probarlos, monitorearlos continuamente y, luego, evaluar sus efectos.

Comprender los patrones de tráfico

Para entender realmente los patrones de tráfico, es importante que se familiarice con la función empresarial de la aplicación y los atributos esperados, como los patrones de uso, los recursos clave y los personajes de los usuarios. Incorpore el tráfico de producción y el tráfico generado durante las pruebas con respecto a la aplicación para establecer una base de referencia para la evaluación. Asegúrese de que el marco temporal incluya datos de tráfico que representen suficientemente varios picos de uso.

Con la herramienta que prefiera, revise los registros y las métricas de tráfico durante el período de uso representativo. Analice los datos de AWS WAF registro para detectar solicitudes anómalas filtrando campos de registro como `headers` (por ejemplo, `User-Agent` y`Referer`)`country`, y`clientIp`. Anote los identificadores de recursos uniformes (URIs) y su frecuencia de acceso. Clasifique el tráfico, por ejemplo, identifique los bots buenos. Por ejemplo, permite el acceso a bots beneficiosos, como los rastreadores y monitores de los motores de búsqueda.

En la AWS WAF consola, en el panel de control de bots, hay disponible una muestra de la actividad de los bots para cualquier ACL web activa. Si bien esto proporciona una perspectiva inicial de los volúmenes de solicitudes de bots más comunes, realice una configuración y un análisis adicionales para comprender mejor la actividad de los bots.

Para una implementación eficaz, debes conocer bien el tráfico de bots, sus efectos y qué solicitudes de bots son beneficiosas o maliciosas. Esto ayuda en la siguiente fase, que consiste en seleccionar los controles, y te ayuda a evaluar el tráfico de bots en paralelo.

Seleccionar y añadir controles

El análisis de tráfico inicial ayuda a determinar qué controles de bots utilizar y qué acciones seleccionar para cada uno de ellos. También puede optar por registrar y monitorear la actividad para posibles acciones futuras. El análisis inicial del tráfico le ayuda a seleccionar el mejor control para gestionar el tráfico. Para obtener más información sobre los controles disponibles, consulte Técnicas para el control de bots esta guía.

Considere la posibilidad de incluir implementaciones de SDK adicionales durante este paso. Esto le ayuda a probar y completar las implementaciones del SDK en todas las aplicaciones necesarias. AWS WAF Las reglas de control de bots y control del fraude proporcionan una ventaja total de evaluación al implementar el JavaScript SDK o el SDK móvil. Para obtener más información, consulta la sección Por qué deberías usar la integración de aplicaciones SDKs con Bot Control en la AWS WAF documentación.

Recomendamos implementar la adquisición de tokens para los diferentes tipos de aplicaciones de la siguiente manera:

- Aplicación de una sola página (SPA): JavaScript SDK (sin redireccionamiento)
- Navegador móvil: acciones de JavaScript SDK o reglas (CAPTCHA o Challenge)
- Vistas web: acciones JavaScript del SDK o de las reglas (CAPTCHA o Challenge)
- Aplicaciones nativas: SDK móvil
- iFrames — SDK JavaScript

Para obtener más información sobre cómo implementarlos SDKs, consulte la integración de aplicaciones AWS WAF cliente en la AWS WAF documentación.

Pruebas e implementación en producción

Los controles deben implementarse inicialmente en un entorno que no sea de producción en el que se puedan realizar pruebas para comprobar que se conserva la funcionalidad esperada de la aplicación web. Realice siempre una validación exhaustiva en un entorno de prueba antes de la implementación en producción.

Tras realizar las pruebas y la validación en un entorno que no sea de producción, se puede proceder a la versión de producción. Seleccione una fecha y una hora con el menor tráfico de usuarios esperado. Antes de la implementación, los equipos de aplicaciones y seguridad deben revisar la

preparación operativa, analizar cómo revertir los cambios y revisar los paneles de control para garantizar que estén configuradas todas las métricas y alarmas requeridas.

Con la implementación CloudFront continua de Amazon, puede enviar una pequeña cantidad de tráfico a una distribución provisional que tenga una ACL AWS WAF web configurada específicamente para la evaluación del control de bots. AWS WAF gestiona las versiones de cualquier regla gestionada nueva o actualizada para que puedas probar y aprobar los cambios antes de que empiecen a evaluar el tráfico de producción.

Evaluación y ajuste de los controles

Los controles implementados pueden proporcionar una mayor visión y visibilidad de la actividad y los patrones del tráfico. Supervise y analice con frecuencia el tráfico de las aplicaciones para añadir o ajustar los controles de seguridad. Normalmente hay una fase de ajuste para mitigar los posibles falsos negativos y falsos positivos. Los falsos negativos son ataques que no han sido detectados por tus controles y que requieren que endurezcas tus reglas. Los falsos positivos representan solicitudes legítimas que se identificaron incorrectamente como ataques y, en consecuencia, se bloquearon.

El análisis y el ajuste se pueden realizar manualmente o con la ayuda de herramientas. Un sistema de gestión de eventos e información de seguridad (SIEM) es una herramienta común que ayuda a proporcionar métricas y un monitoreo inteligente. Hay muchos disponibles con distintos grados de sofisticación, pero todos proporcionan un buen punto de partida para obtener información sobre el tráfico.

Definir indicadores clave de rendimiento importantes (KPIs) para sitios web y aplicaciones puede ayudarle a identificar más rápidamente cuándo las cosas no funcionan como se esperaba. Por ejemplo, puedes utilizar las devoluciones de cargos de las tarjetas de crédito, las ventas por cuenta o las tasas de conversión como indicadores de las anomalías empresariales que pueden generar los bots. Definir y comprender qué métricas y cuáles KPIs son valiosas monitorear es incluso más importante que el simple acto de monitorear.

Comprender cómo obtener las métricas y los registros correctos de una solución de control de bots es tan importante como identificar las métricas que se van a monitorear. En la siguiente secciónDirectrices para monitorizar tu estrategia de control de bots, se detallan las opciones de monitoreo y visibilidad que se deben considerar.

Directrices para monitorizar tu estrategia de control de bots

Para el tráfico de bots y el tráfico de aplicaciones web, la supervisión y la visibilidad son de gran importancia. Le ayuda a priorizar las actividades y las operaciones de seguridad. Si no es posible realizar un registro detallado o utilizar un sistema SIEM, un buen punto de partida es supervisar las métricas básicas proporcionadas por la solución o el proveedor que haya seleccionado.

Esta visibilidad es útil para obtener información sobre amenazas, reforzar las reglas, solucionar los falsos positivos y responder a un incidente. Hay varias opciones de monitoreo disponibles con. AWS WAF Para un monitoreo de alto nivel, AWS WAF proporciona información general del tráfico en el Consola de administración de AWS. Está disponible para todo el tráfico, así como para una vista detallada del tráfico de bots, cuando el grupo de reglas de control de bots está habilitado en su ACL web.

AWS WAF ofrece diferentes opciones para el registro detallado del tráfico de ACL web. También puede añadir etiquetas a las solicitudes, que puede utilizar para facilitar el análisis de los registros y configurar las reglas de evaluación de los bots. Al integrar Amazon CloudWatch Logs Insights, puede consultar los AWS WAF registros y visualizar los resultados.

Si activa el registro detallado, AWS WAF proporciona una visibilidad adicional más allá del panel de control de bots preconfigurado. El uso de AWS WAF registros para visualizar el tráfico, así como de las investigaciones ad hoc, puede proporcionar una comprensión profunda de los patrones de tráfico y las opciones de mitigación de una aplicación web.

Puede integrar los datos de AWS WAF registro con Amazon CloudWatch Logs, Amazon Simple Storage Service (Amazon S3) o Amazon Data Firehose. Para obtener más información, consulte Activar el AWS WAF registro y enviar registros a CloudWatch Amazon S3 o Amazon Data Firehose. También puedes enviar registros a varios objetivos para su análisis, incluso a Amazon OpenSearch Service o a una AWS Marketplacesolución. Para obtener más información, consulte Configuración de destino en la documentación de Firehose. Si se utilizan varias fuentes de registro, se recomienda una solución de registro centralizada para correlacionar las fuentes.

A continuación, en esta guía se ofrecen recomendaciones sobre cómo empezar a monitorizar el tráfico de bots y ganar visibilidad con Amazon CloudWatch.

Seguimiento de las principales reglas

El seguimiento de las reglas más afectadas puede poner de relieve tendencias y actividades potencialmente anómalas. El aumento de las tasas de una regla específica puede indicar un posible falso positivo o una actividad específica que deberías investigar. La regla más común para el seguimiento serían Controles basados en IP las reglas de bloqueo geográfico (un pico en este caso puede mostrar tráfico procedente de países poco comunes, que podrían no estar bloqueados automáticamente), y Reglas basadas en frecuencia Estas reglas siempre tienen variaciones inherentes, pero una anomalía en el patrón de tráfico puede ser indicativa de la actividad de los bots. Ten esto en cuenta si estableces los umbrales manualmente.

Realizar un seguimiento de las principales etiquetas y espacios de nombres

Al utilizar CloudWatch métricas para realizar un seguimiento de las etiquetas principales, puedes ver qué AWS WAF reglas se invocan con frecuencia. Esto le ayuda a detectar anomalías, como el aumento de la actividad de los rastreadores, el tráfico procedente de fuentes sospechosas o un intento de uso indebido de la página de inicio de sesión o la API de la aplicación.

Los siguientes son ejemplos de etiquetas que podrían ser de interés:

- `awswaf:managed:aws:bot-control:signal:non_browser_user_agent`
- `awswaf:managed:aws:bot-control:bot:category:http_library`
- `awswaf:managed:aws:bot-control:bot:name:curl`
- `awswaf:managed:aws:atp:signal:credential_compromised`
- `awswaf:managed:aws:core-rule-set:NoUserAgent_Header`
- `awswaf:managed:token:rejected`

A continuación se muestran ejemplos de espacios de nombres de etiquetas que podrían ser de interés:

- `awswaf:managed:aws:bot-control:`
- `awswaf:managed:aws:atp:`
- `awswaf:managed:aws:anonymous-ip-list:`

Crear expresiones matemáticas

En Amazon CloudWatch, puedes crear expresiones matemáticas para cualquiera de las reglas o para todas ellas. Si configuras alertas en las expresiones matemáticas, se te notificará si hay anomalías en las tasas, no en las cantidades, de determinadas métricas. Se trata de una herramienta importante para reducir la fatiga provocada por las alertas.

Cree una métrica personalizada basada en una expresión matemática. Observe las tasas relativas de las reglas a partir del número total de solicitudes a una aplicación. La siguiente es una expresión matemática común:

```
[ruleX count * 100]/[All allowed requests + All blocked requests]
```

Esta expresión matemática proporciona un porcentaje para que puedas realizar un seguimiento de una regla específica y visualizar su tendencia a lo largo del tiempo.

Uso de la detección de anomalías

El uso de la detección de CloudWatch anomalías en cualquier CloudWatch métrica puede generar alertas sobre tendencias anormalmente bajas o altas, sin necesidad de configurar el umbral real de forma manual. Estos algoritmos analizan continuamente las métricas de los sistemas y las aplicaciones, determinan las líneas de base normales y detectan las anomalías con una intervención mínima del usuario. CloudWatch aplica algoritmos estadísticos y de aprendizaje automático en su función de detección de anomalías.

Uso de CloudWatch las métricas de Amazon

AWS WAF procesa el tráfico y agrega etiquetas a las solicitudes que coinciden con las reglas definidas en la ACL web. Cada etiqueta crea una métrica en CloudWatch. Al mismo tiempo, cada regla de ACL web también crea métricas para cada una de sus posibles acciones. Utilice estas métricas de etiquetas y acciones para obtener una comprensión exhaustiva del tráfico de bots. Se trata de un enfoque rentable para visualizar las tendencias. Para obtener más información, consulte Ver las métricas disponibles y Graficar las métricas en la CloudWatch documentación.

CloudWatch ofrece la opción de enviar datos a un recopilador o agregador de registros, ya sea una solución Servicio de AWS o una de terceros. La ingesta de datos CloudWatch puede proporcionar una experiencia de observabilidad de la seguridad más consolidada, en la que se

pueden correlacionar los datos de varias fuentes. Esto puede ayudarle a investigar, ver o configurar sus alertas y automatizaciones de seguridad.

Crear un panel

Tras identificar las métricas importantes a las que hay que hacer un seguimiento, cree un panel que contenga las métricas más relevantes. Mostrarlas side-by-side bajo un solo panel de vidrio puede proporcionar visibilidad y control adicionales.

Siempre es preferible configurar alertas y reglas de automatización para valores métricos anómalos. No confíe en las personas para identificar las anomalías mirando un panel de control. Sin embargo, los paneles pueden ser útiles para fines de investigación después de recibir una alerta.

Optimización de los costes de su estrategia de control de bots

La naturaleza del tráfico web es dinámica. Esto significa que la tecnología y los servicios utilizados para mitigar las amenazas pueden variar y ajustarse con el tiempo. Esto es fundamental a la hora de considerar una estrategia de control de bots y los controles que incluye. La optimización a lo largo del tiempo es el principio principal a tener en cuenta, y proviene del pilar de optimización de costos del AWS Well-Architected Framework.

AWS WAF La web ACLs puede ser dinámica, especialmente cuando se lanzan nuevas funciones o se intenta mitigar una nueva amenaza. Controlar sus costes implica comprender las dimensiones de los costes del AWS WAF servicio y la forma en que cada una de ellas afecta a su gasto final. El principal coste de generación es el número de solicitudes evaluadas por el servicio. Se aplican cargos adicionales si utilizas los grupos de reglas gestionados por el control de bots y la prevención de apropiación de cuentas (ATP) o si utilizas acciones avanzadas, como el CAPTCHA o la impugnación.

Dado que los controles de bots especializados tienen un coste elevado, el objetivo principal de optimización de costes es reducir el número de solicitudes inspeccionadas por estos controles avanzados. Las técnicas aplicables incluyen separar el contenido de alto valor, aplicar primero medidas de menor costo, delimitar el área de evaluación y combinar la protección contra los bots con otros tipos de controles. Las técnicas de supervisión de costes proporcionan una visibilidad adicional en toda la organización.

Separar el contenido dinámico del estático

Una técnica de reducción de costes consiste en aislar el contenido estático de la aplicación dinámica. La mayoría de las solicitudes a aplicaciones web típicas son solicitudes a objetos estáticos. Un método habitual para reducir la carga en los servidores de aplicaciones consiste en mover el contenido estático a su propia URL, por ejemplo`static.example.com`. Esto suele lograrse mediante la creación de una distribución de contenido única con la configuración de almacenamiento en caché optimizada para el contenido estático. Esta técnica también puede ayudar a reducir los costes de control de los bots si el sitio o la aplicación no suelen segmentar contenido estático. Separar el contenido estático de la aplicación dinámica puede permitir una aplicación más precisa de los controles avanzados de los bots.

Aplicar primero las reglas de menor coste

Otra técnica consiste en aplicar reglas básicas de menor coste que filtren el tráfico no deseado antes de utilizar controles avanzados, que son más caros. En la práctica, esto suele implicar utilizar las medidas de mitigación del control mediante bots como último nivel de defensa y utilizar los controles anteriores para filtrar el tráfico no deseado. Este enfoque piramidal se analizó anteriormente Técnicas para el control de bots en esta guía. El objetivo principal es utilizar estas opciones de menor coste para detener el tráfico no deseado, lo que reduce el número de solicitudes procesadas mediante técnicas de mitigación avanzadas y de mayor coste.

Reducir el alcance del área de evaluación

AWS WAFLas declaraciones de alcance reducido proporcionan una técnica eficaz para reducir el número de solicitudes inspeccionadas mediante normas avanzadas. Si no se puede separar el contenido estático en su propia URL, las declaraciones de alcance reducido son otro método para filtrar las solicitudes que no requieren técnicas de mitigación avanzadas. Esto se puede hacer definiendo una ruta de aplicación específica, un método HTTP (como POST) o una combinación similar.

Combinar la protección contra bots con otros controles

Se deben tener en cuenta otras consideraciones de control de costes a la hora de proteger las aplicaciones contra múltiples amenazas, además del tráfico de bots no deseado. Por ejemplo, la protección contra los ataques de denegación de servicio distribuidos y contra la apropiación de cuentas requiere una configuración adicional que puede repercutir en los costes. DDo Se recomienda Shield Advanced para ayudar a proteger las aplicaciones contra los ataques DDo S. En concreto, sus mitigaciones a nivel de aplicación permiten abordar automáticamente el flujo de solicitudes, reduciendo así el número de solicitudes que puede procesar el grupo de reglas de control de AWS WAF bots si se coloca la regla por delante en el orden de evaluación. Shield Advanced tiene una ventaja adicional: AWS WAF las reglas gestionadas y personalizadas estándar no tienen coste adicional para los recursos protegidos por Shield Advanced. Tenga en cuenta que los grupos de reglas de mitigación de amenazas inteligentes, incluido Bot Control, incurren en costos adicionales, incluso para los recursos protegidos por Shield Advanced.

Las aplicaciones que requieren la prevención de la apropiación de cuentas pueden usar el grupo de reglas de prevención de apropiación de cuentas (ATP) de AWS WAF Fraud Control. El costo de inspección por solicitud del grupo de reglas de ATP es mayor que el del grupo de reglas de Control

de bots. Ese costo más alto hace que sea fundamental aplicar el grupo de reglas de la ATP con la mayor precisión posible. El uso del grupo de reglas de control de bots junto con la ATP puede ayudar a lograr este objetivo. El grupo de reglas de control de bots debe colocarse antes que el ATP en la ACL web para filtrar las solicitudes de bots y reducir la cantidad de solicitudes inspeccionadas por ATP.

Para una optimización continua, la actividad más importante es monitorear CloudWatchlas métricas asociadas al grupo de reglas de control de bots. Con el tiempo, el objetivo es reducir el número de solicitudes evaluadas por el grupo de reglas de control de bots a aquellas que se destinen a los recursos que necesita para protegerse contra la actividad no deseada de los bots. La creación de CloudWatch paneles proporciona visibilidad de las métricas más importantes de las aplicaciones, incluidos AWS WAF los costos y el uso.

Supervisión de costos

AWS Cost Explorer es una herramienta que le permite ver y analizar sus costos y uso. Cost Explorer facilita el análisis de AWS los costes, incluidos AWS WAF los costes incurridos. La herramienta proporciona información sobre los costos de los últimos 12 meses y prevé el gasto futuro para los próximos 12 meses.

AWS La detección de anomalías en los costes es otra herramienta de control de la gestión de costes que puede resultar útil para monitorizar AWS WAF los costes. Utiliza tecnologías avanzadas de aprendizaje automático para identificar los gastos anómalos y sus causas fundamentales. Esto le ayuda a tomar medidas rápidamente o a recibir alertas en caso de que se produzca un aumento inesperado de los costes. Para recibir una alerta cuando se alcance un umbral de costo específico, AWS Budgetspuede proporcionar esa funcionalidad de seguimiento y supervisión.

Recursos

AWS documentación

- AWS WAF guía para desarrolladores
- AWS Mejores prácticas para la resiliencia ante los ataques DDoS (documentos técnicos)AWS
- Directrices de implementación AWS WAF(documentos técnicos)AWS

Otros recursos AWS

- Análisis AWS WAF de registros en Amazon CloudWatch Logs (AWS entrada de blog)
- Implemente un panel de control AWS WAF con un esfuerzo mínimo (AWS entrada de blog)
- Automatizaciones de seguridad para AWS WAF (biblioteca de AWS soluciones)
- Las tres reglas AWS WAF basadas en tarifas más importantes (AWS entrada de blog)
- Visualiza AWS WAF los registros con un CloudWatch panel de Amazon (AWS entrada del blog)

Colaboradores

Creación

- Diana Alvarado, arquitecta sénior de soluciones, AWS
- Cameron Worrell, arquitecto empresarial, AWS
- Geary Scherer, arquitecto de soluciones, AWS
- Tzoori Tamam, arquitecta principal de soluciones, AWS

Revisando

- Jess Izen, ingeniera sénior de desarrollo de software, AWS
- Kaustubh Phatak, director sénior de productos, AWS
- Vikramaditya Bhatnagar, consultora sénior de seguridad, AWS

Redacción técnica

- Lilly AbouHarb, redactora técnica sénior, AWS

Historial de documentos

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

Cambio	Descripción	Fecha
Publicación inicial	—	21 de febrero de 2024

AWS Glosario de orientación prescriptiva

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

Números

Las 7 R

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

- Refactor/re-architect — Mueva una aplicación y modifique su arquitectura aprovechando al máximo las funciones nativas de 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 PostgreSQL-Compatible edición 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: Migrar la base de datos Oracle en las instalaciones a Amazon Relational Database Service (Amazon RDS) para Oracle en la nube de Nube de AWS.
- Recomprar (readquirir): cambie a un producto diferente, lo cual se suele llevar a cabo al pasar de una licencia tradicional a un modelo SaaS. Ejemplo: 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 hacer cambios para aprovechar las funcionalidades de la nube. Ejemplo: Migrar la base de datos de Oracle en las instalaciones a Oracle en una instancia de EC2 en la Nube de AWS.
- Reubicar: (migrar el hipervisor mediante lift and shift): traslade la infraestructura a la nube sin comprar equipo nuevo, reescribir aplicaciones o modificar las operaciones actuales. Los servidores se migran de una plataforma en las instalaciones a un servicio en la nube para la misma plataforma. Ejemplo: migrar una Microsoft Hyper-V aplicación a AWS.
- Retener (revisitar): conserve las aplicaciones en el entorno de origen. Estas pueden incluir las aplicaciones que requieren una refactorización importante, que desee posponer para más adelante, y las aplicaciones heredadas que desee retener, ya que no hay ninguna justificación empresarial para migrarlas.

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

A

A2A () Agent-to-Agent

Un protocolo completo para la colaboración entre agentes que facilita la delegación de tareas y la transferencia de estados.

ABAC

Consulte control de acceso basado en atributos.

servicios abstractos

Consulte servicios administrados.

ACID

Consulte atomicidad, consistencia, aislamiento, durabilidad.

migración activa-activa

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

migración activa-pasiva

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

Agente

Un sistema de IA que puede razonar, planificar y tomar medidas de forma autónoma utilizando herramientas para alcanzar los objetivos.

Agent Ops

Prácticas operativas para crear, probar, implementar y ejecutar agentes de IA en producción a escala.

función de agregación

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

IA

Consulte inteligencia artificial.

AIOps

Consulte operaciones de inteligencia artificial

anonimización

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

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

Enfoque de seguridad que permite usar de manera exclusiva aplicaciones aprobadas para ayudar a proteger un sistema contra el malware.

cartera de aplicaciones

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

inteligencia artificial (IA)

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

operaciones de inteligencia artificial (AIOps)

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

cifrado asimétrico

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

atomicidad, consistencia, aislamiento, durabilidad (ACID)

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

control de acceso basado en atributos (ABAC)

La práctica de crear permisos detallados basados en los atributos del usuario, como el departamento, el puesto de trabajo y el nombre del equipo. Para obtener más información, consulte ABAC AWS en la documentación AWS Identity and Access Management (IAM).

origen de datos fidedigno

Ubicación en la que se almacena la versión principal de los datos, que se considera la fuente de información más fiable. Puede copiar los datos del origen de datos autorizado a otras ubicaciones con el fin de procesarlos o modificarlos, por ejemplo, anonimizarlos, redactarlos o seudonimizarlos.

Zona de disponibilidad

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

AWS Marco de adopción de la nube (AWS CAF)

Un marco de directrices y mejores prácticas AWS para ayudar a las organizaciones a desarrollar un plan eficiente y eficaz para migrar con éxito a la nube. AWS CAF organiza la orientación en seis áreas de enfoque denominadas perspectivas: negocios, personas, gobierno, plataforma, seguridad y operaciones. Las perspectivas empresariales, humanas y de gobernanza se centran en las habilidades y los procesos empresariales; las perspectivas de plataforma, seguridad y

operaciones se centran en las habilidades y los procesos técnicos. Por ejemplo, la perspectiva humana se dirige a las partes interesadas que se ocupan de los Recursos Humanos (RR. HH.), las funciones del personal y la administración de las personas. Desde esta perspectiva, AWS CAF proporciona orientación para el desarrollo, la formación y la comunicación de las personas a fin de preparar a la organización para una adopción exitosa de la nube. Para obtener más información, consulte la Página web de AWS CAF y el Documento técnico de AWS CAF.

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

Herramienta que evalúa las cargas de trabajo de migración de bases de datos, recomienda estrategias de migración y proporciona estimaciones de trabajo. AWS WQF se incluye con AWS Schema Conversion Tool ().AWS SCT Analiza los esquemas de bases de datos y los objetos de código, el código de las aplicaciones, las dependencias y las características de rendimiento y proporciona informes de evaluación.

B

bot malicioso

Bot destinado a causar interrupciones o daños a personas u organizaciones.

BCP

Consulte planificación de la continuidad del negocio.

gráfico de comportamiento

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

sistema big-endian

Un sistema que almacena primero el byte más significativo. Consulte también endianidad.

clasificación binaria

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

filtro de floración

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

blue/green despliegue

Estrategia de implementación en la que se crean dos entornos separados, pero idénticos. La versión actual de la aplicación se ejecuta en un entorno (azul) y la nueva versión de la aplicación se ejecuta en el otro entorno (verde). Esta estrategia lo ayuda a hacer reversiones rápidas con un impacto mínimo.

bot

Aplicación de software que ejecuta tareas automatizadas a través de Internet y simula la actividad o interacción humana. Algunos bots son útiles o beneficiosos, como los rastreadores web que indexan la información de Internet. Otros bots, conocidos como bots maliciosos, tienen como objetivo causar interrupciones o daños a personas u organizaciones.

botnet

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

branch

Área contenida de un repositorio de código. La primera rama que se crea en un repositorio es la rama principal. Puede crear una rama nueva a partir de una rama existente y, a continuación, desarrollar características o corregir errores en la rama nueva. Una rama que se genera para crear una característica se denomina comúnmente rama de característica. Cuando la característica se encuentra lista para su lanzamiento, se vuelve a combinar la rama de característica con la rama principal. Para obtener más información, consulte Acerca de las sucursales (GitHub documentación).

acceso de emergencia

En circunstancias excepcionales y mediante un proceso aprobado, es una forma rápida de que un usuario pueda acceder a un Cuenta de AWS sitio al que normalmente no tiene permisos de acceso. Para obtener más información, consulte el indicador de implementación de procedimientos rompe-cristales en la AWS Well-Architected guía.

estrategia de implementación sobre infraestructura existente

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

caché de búfer

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

capacidad empresarial

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

planificación de la continuidad del negocio (BCP)

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

C

CAF

Consulte AWS Cloud Adoption Framework.

implementación canario

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

CCoE

Consulte Centro de excelencia en la nube.

CDC

Consulte captura de datos de cambios.

captura de datos de cambio (CDC)

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

ingeniería del caos

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

CI/CD

Consulte integración continua y entrega continua.

clasificación

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

Desarrollador ciudadano

Un usuario empresarial que crea aplicaciones de IA utilizando plataformas sin code/low código sin conocimientos técnicos especializados.

cifrado del cliente

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

Centro de excelencia en la nube (CCoE)

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

computación en la nube

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

modelo operativo en la nube

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

etapas de adopción de la nube

Las siguientes son las cuatro fases por las que suelen pasar las empresas cuando migran a la Nube de AWS:

- Proyecto: ejecución de algunos proyectos relacionados con la nube con fines de prueba de concepto y aprendizaje
- Fundamento: realización de inversiones fundamentales para escalar la adopción de la nube (p. ej., crear una zona de aterrizaje, definir un CCoE, establecer un modelo de operaciones)
- Migración: migración de aplicaciones individuales
- Re-invention — Optimizar los productos y servicios e innovar en la nube

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

CMDB

Consulte base de datos de administración de configuración.

repositorio de código

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

caché en frío

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

datos fríos

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

visión artificial (CV)

Campo de la IA que utiliza el machine learning para analizar y extraer información de formatos visuales, como imágenes y videos digitales. Por ejemplo, Amazon SageMaker AI proporciona algoritmos de procesamiento de imágenes para CV.

deriva de configuración

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

base de datos de administración de configuración (CMDB)

Repositorio que almacena y administra información sobre una base de datos y su entorno de TI, incluidos los componentes de hardware y software y sus configuraciones. Por lo general, los datos de una CMDB se utilizan en la etapa de detección y análisis de la cartera de productos durante la migración.

paquete de conformidad

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

integración y entrega continuas () CI/CD

El proceso de automatización de las etapas de origen, creación, prueba, puesta en escena y producción del proceso de publicación del software. CI/CD se describe comúnmente como una canalización. CI/CD puede ayudarlo a automatizar los procesos, mejorar la productividad, mejorar la calidad del código y entregar más rápido. Para obtener más información, consulte Beneficios de la entrega continua. CD también puede significar implementación continua. Para obtener más información, consulte Entrega continua frente a implementación continua.

CV

Consulte visión artificial.

D

datos en reposo

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

clasificación de datos

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

deriva de datos

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

datos en tránsito

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

malla de datos

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

minimización de datos

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

perímetro de datos

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

preprocesamiento de datos

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

procedencia de los datos

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

titular de los datos

Persona cuyos datos se recopilan y procesan.

almacenamiento de datos

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

lenguaje de definición de datos (DDL)

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

lenguaje de manipulación de datos (DML)

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

DDL

Consulte lenguaje de definición de bases de datos.

conjunto profundo

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

aprendizaje profundo

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

defensa en profundidad

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 enfoque de defensa en profundidad podría combinar la autenticación multifactor, la segmentación de la red y el cifrado.

administrador delegado

En AWS Organizations, un servicio compatible puede registrar una cuenta de AWS miembro para administrar las cuentas de la organización y gestionar los permisos de ese servicio. Esta cuenta se denomina administrador delegado para ese servicio. Para obtener más información y una lista de servicios compatibles, consulte Servicios que funcionan con AWS Organizations en la documentación de AWS Organizations .

Implementación

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

entorno de desarrollo

Consulte entorno.

control de detección

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

asignación de flujos de valor para el desarrollo (DVSM)

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

gemelo digital

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

tabla de dimensiones

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

desastre

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

recuperación de desastres (DR)

Estrategia y proceso que utiliza para minimizar el tiempo de inactividad y la pérdida de datos a causa de un desastre. Para obtener más información, consulte Recuperación de cargas de trabajo ante desastres en AWS: Recuperación en la nube en el AWS Well-Architected marco.

DML

Consulte lenguaje de manipulación de bases de datos.

diseño basado en el dominio

Un enfoque para desarrollar un sistema de software complejo mediante la conexión de sus componentes a dominios en evolución, o a los objetivos empresariales principales, a los que sirve cada componente. Eric Evans introdujo este concepto en su libro Domain-Driven Design: Tackling Complexity in the Heart of Software (Boston: Addison-Wesley Professional, 2003). Para obtener información sobre cómo utilizar el diseño basado en dominios con el patrón de higos estranguladores, consulte Modernización gradual de los servicios web antiguos de ASP.NET Microsoft (ASMX) mediante contenedores y Amazon API Gateway.

DR

Consulte recuperación ante desastres.

Detección de desviaciones

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

DVSM

Consulte asignación de flujos de valor para el desarrollo.

E

EDA

Consulte análisis de datos de tipo exploratorio.

EDI

Consulte intercambio electrónico de datos.

computación en la periferia

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

intercambio electrónico de datos (EDI)

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

cifrado

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

clave de cifrado

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

endianidad

El orden en el que se almacenan los bytes en la memoria del ordenador. Big-endian los sistemas almacenan primero el byte más significativo. Little-endian los sistemas almacenan primero el byte menos significativo.

punto de conexión

Consulte punto de conexión de servicio.

servicio de punto de conexión

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

planificación de recursos empresariales (ERP)

Sistema que automatiza y administra los procesos empresariales clave (como la contabilidad, MES y la administración de proyectos) de una empresa.

cifrado de sobre

El proceso de cifrar una clave de cifrado con otra clave de cifrado. Para obtener más información, consulte el cifrado de sobres en la documentación de AWS Key Management Service (AWS KMS).

entorno

Una instancia de una aplicación en ejecución. Los siguientes son los tipos de entornos más comunes en la computación en la nube:

- entorno de desarrollo: instancia de una aplicación en ejecución que solo se encuentra disponible para el equipo principal responsable del mantenimiento de la aplicación. Los entornos de desarrollo se utilizan para probar los cambios antes de promocionarlos a los entornos superiores. Este tipo de entorno a veces se denomina entorno de prueba.
- entornos inferiores: todos los entornos de desarrollo de una aplicación, como los que se utilizan para las compilaciones y pruebas iniciales.

- entorno de producción: instancia de una aplicación en ejecución a la que pueden acceder los usuarios finales. En un CI/CD proceso, el entorno de producción es el último entorno de implementación.
- entornos superiores: todos los entornos a los que pueden acceder usuarios que no sean del equipo de desarrollo principal. Esto puede incluir un entorno de producción, entornos de preproducción y entornos para las pruebas de aceptación por parte de los usuarios.

epopeya

En las metodologías ágiles, son categorías funcionales que ayudan a organizar y priorizar el trabajo. Las epopeyas brindan una descripción detallada de los requisitos y las tareas de implementación. Por ejemplo, las epopeyas AWS de seguridad de CAF incluyen la gestión de identidades y accesos, los controles de detección, la seguridad de la infraestructura, la protección de datos y la respuesta a incidentes. Para obtener más información sobre las epopeyas en la estrategia de migración de AWS , consulte la Guía de implementación del programa.

ERP

Consulte planificación de recursos empresariales.

análisis de datos de tipo exploratorio (EDA)

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

F

tabla de hechos

Tabla central de un esquema en estrella. Almacena datos cuantitativos sobre operaciones empresariales. Por lo general, una tabla de hechos contiene dos tipos de columnas: las que contienen medidas y las que contienen una clave externa para una tabla de dimensiones.

Fail Fast

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

límite de aislamiento de errores

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

rama de característica

Consulte rama.

características

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

importancia de las características

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

transformación de funciones

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

peticiones con pocos pasos

Proporcionar a un LLM una pequeña cantidad de ejemplos que demuestren la tarea y el resultado deseado antes de pedirle que lleve a cabo una tarea similar. Esta técnica es una aplicación del aprendizaje contextual, en el que los modelos aprenden a partir de ejemplos (tomas) integrados en las instrucciones. Few-shot Las indicaciones pueden ser eficaces para tareas que requieren un formato, un razonamiento o un conocimiento del dominio específicos. Consulte también peticiones desde cero.

FGAC

Consulte control de acceso detallado.

control de acceso preciso (FGAC)

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

migración relámpago

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

FM

Consulte modelo fundacional.

Modelo fundacional (FM)

Gran red neuronal de aprendizaje profundo que se entrenó con conjuntos de datos masivos de datos generalizados y no etiquetados. Los FM pueden hacer una amplia variedad de tareas generales, como comprender el lenguaje, generar texto e imágenes y conversar en lenguaje natural. Para más información, consulte ¿Qué son los modelos fundacionales?

Puerta de enlace FM

Un intermediario centralizado que controla y normaliza el acceso a los modelos básicos. También se conoce como puerta de enlace LLM.

G

IA generativa

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

bloqueo geográfico

Consulte restricciones geográficas.

restricciones geográficas (bloqueo geográfico)

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

Flujo de trabajo de Gitflow

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

imagen dorada

Instantánea de un sistema o software que se usa como plantilla para implementar nuevas instancias de ese sistema o software. Por ejemplo, en la fabricación, una imagen dorada se puede utilizar para aprovisionar software en varios dispositivos y ayuda a mejorar la velocidad, la escalabilidad y la productividad de las operaciones de fabricación de dispositivos.

estrategia de implementación desde cero

La ausencia de infraestructura existente en un entorno nuevo. Al adoptar una estrategia de implementación desde cero para una arquitectura de sistemas, puede seleccionar todas las tecnologías nuevas sin que estas deban ser compatibles con una infraestructura existente, lo que también se conoce como implementación sobre infraestructura existente. Si está ampliando la infraestructura existente, puede combinar las estrategias de implementación sobre infraestructuras existentes y de implementación desde cero.

barrera de protección

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

barandas (AI)

Mecanismos de seguridad que filtran, validan y restringen las entradas y salidas de los agentes para ayudar a garantizar un comportamiento responsable y seguro de la IA.

H

HA

Consulte alta disponibilidad.

migración heterogénea de bases de datos

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

alta disponibilidad (HA)

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

modernización histórica

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

datos de reserva

Parte de los datos históricos etiquetados que se ocultan de un conjunto de datos que se utiliza para entrenar un modelo de machine learning. Puede utilizar los datos de reserva para evaluar el rendimiento del modelo mediante la comparación de las predicciones del modelo con los datos de reserva.

human-in-the-loop (HiTL)

Un patrón de flujo de trabajo en el que la ejecución de los agentes se detiene para su revisión y aprobación por parte de una persona en los puntos de decisión críticos.

migración homogénea de bases de datos

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

datos recientes

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

hotfix

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

periodo de hiperatención

Periodo, inmediatamente después de la transición, durante el cual un equipo de migración administra y monitorea las aplicaciones migradas en la nube para solucionar cualquier problema. Por lo general, este periodo dura de 1 a 4 días. Al final del periodo de hiperatención, el equipo de migración suele transferir la responsabilidad de las aplicaciones al equipo de operaciones en la nube.

I

IaC

Consulte infraestructura como código.

políticas basadas en identidades

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

aplicación inactiva

Aplicación que utiliza un promedio de CPU y memoria de entre 5 y 20 por ciento durante un periodo de 90 días. En un proyecto de migración, es habitual retirar estas aplicaciones o mantenerlas en las instalaciones.

IIoT

Consulte Internet de las cosas industrial.

infraestructura inmutable

Modelo que implementa una nueva infraestructura para las cargas de trabajo de producción en lugar de actualizar o modificar la infraestructura existente o aplicarle revisiones. Las infraestructuras inmutables son de manera intrínseca más coherentes, fiables y predecibles que las infraestructuras mutables. Para obtener más información, consulte las mejores prácticas del Framework para implementar con una infraestructura inmutable. AWS Well-Architected

VPC entrante (de entrada)

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

migración gradual

Estrategia de transición en la que se migra la aplicación en partes pequeñas en lugar de realizar una transición única y completa. Por ejemplo, puede trasladar inicialmente solo unos pocos microservicios o usuarios al nuevo sistema. Tras comprobar que todo funciona correctamente, puede trasladar microservicios o usuarios adicionales de forma gradual hasta que pueda retirar su sistema heredado. Esta estrategia reduce los riesgos asociados a las grandes migraciones.

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. AI/ML

infraestructura

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

infraestructura como código (IaC)

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

Internet de las cosas industrial (IIoT)

El uso de sensores y dispositivos conectados a Internet en los sectores industriales, como el productivo, el eléctrico, el automotriz, el sanitario, el de las ciencias de la vida y el de la agricultura. Para obtener más información, consulte Creación de una estrategia de transformación digital del Internet de las cosas industrial (IIoT).

VPC de inspección

En una arquitectura de AWS cuentas múltiples, una VPC centralizada que gestiona las inspecciones del tráfico de red entre las VPC (iguales o Regiones de AWS diferentes), Internet y las redes locales. La Arquitectura de referencia de seguridad de AWS recomienda configurar su

cuenta de red con VPC entrantes, salientes y de inspección para proteger la interfaz bidireccional entre su aplicación e Internet en general.

Internet de las cosas (IoT)

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

interpretabilidad

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

IoT

Consulte Internet de las cosas.

biblioteca de información de TI (ITIL)

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

administración de servicios de TI (ITSM)

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

ITIL

Consulte biblioteca de información de TI.

ITSM

Consulte administración de servicios de TI.

L

control de acceso basado en etiquetas (LBAC)

Una implementación del control de acceso obligatorio (MAC) en la que a los usuarios y a los propios datos se les asigna explícitamente un valor de etiqueta de seguridad. La intersección

entre la etiqueta de seguridad del usuario y la etiqueta de seguridad de los datos determina qué filas y columnas puede ver el usuario.

zona de aterrizaje

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

modelo de lenguaje de gran tamaño (LLM)

Modelo de IA de aprendizaje profundo que se entrenó previamente con una gran cantidad de datos. Un LLM puede llevar a cabo varias tareas, como responder preguntas, resumir documentos, traducir textos a otros idiomas y completar oraciones. Para más información, consulte ¿Qué es un LLM (modelo de lenguaje de gran tamaño)?

migración grande

Migración de 300 servidores o más.

LBAC

Consulte control de acceso basado en etiquetas.

privilegio mínimo

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

migrar mediante lift-and-shift

Consulte Las 7 R.

sistema little-endian

Un sistema que almacena primero el byte menos significativo. Consulte también endianidad.

LLM

Consulte modelo de lenguaje de gran tamaño.

entornos inferiores

Consulte entorno.

M

machine learning (ML)

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

rama principal

Consulte rama.

malware

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

Servicios administrados

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

sistema de ejecución de fabricación (MES)

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

MAP

Consulte Programa de aceleración de la migración.

MCP

Consulte Model Context Protocol.

Protocolo de contexto para modelos (MCP)

Un protocolo sin estado para la comunicación entre el agente y la herramienta.

Servidor MCP

Un servicio que expone una o más herramientas a través del protocolo Model Context.

mecanismo

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

cuenta de miembro

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

MES

Consulte sistema de ejecución de fabricación.

Message Queuing Telemetry Transport (MQTT)

Un protocolo de comunicación ligero de máquina a máquina (M2M), basado en el publish/subscribepatrón, para dispositivos de IoT con recursos limitados.

microservicio

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

arquitectura de microservicios

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

Programa de aceleración de la migración (MAP)

Un AWS programa que proporciona soporte de consultoría, formación y servicios para ayudar a las organizaciones a crear una base operativa sólida para migrar a la nube y para ayudar a

compensar el costo inicial de las migraciones. El MAP incluye una metodología de migración para ejecutar las migraciones antiguas de forma metódica y un conjunto de herramientas para automatizar y acelerar los escenarios de migración más comunes.

migración a escala

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

fábrica de migración

Cross-functional equipos que agilizan la migración de las cargas de trabajo mediante enfoques ágiles y automatizados. 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: rehospede la migración a Amazon EC2 AWS con Application Migration Service.

Migration Portfolio Assessment (MPA)

Herramienta en línea que proporciona información a fin de validar los argumentos comerciales necesarios para migrar a la Nube de AWS. La MPA ofrece una evaluación detallada de la cartera (adecuación del tamaño de los servidores, precios, comparaciones del costo total de propiedad, análisis de los costos de migración), así como una planificación de la migración (análisis y recopilación de datos de aplicaciones, agrupación de aplicaciones, priorización de la migración y

planificación de oleadas). La herramienta MPA (requiere iniciar sesión) está disponible de forma gratuita para todos los AWS consultores y consultores de los socios de APN.

Evaluación de la preparación para la migración (MRA)

Proceso que consiste en obtener información sobre el estado de preparación de una organización para la nube, identificar sus puntos fuertes y débiles y elaborar un plan de acción para cerrar las brechas identificadas mediante el AWS CAF. Para obtener más información, consulte la Guía de preparación para la migración. La MRA es la primera fase de la estrategia de migración de AWS.

estrategia de migración

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

ML

Consulte machine learning.

modernización

Transformar una aplicación obsoleta (antigua o monolítica) y su infraestructura en un sistema ágil, elástico y de alta disponibilidad en la nube para reducir los gastos, aumentar la eficiencia y aprovechar las innovaciones. Para más información, consulte Strategy for modernizing applications in the Nube de AWS.

evaluación de la preparación para la modernización

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

aplicaciones monolíticas (monolitos)

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

una arquitectura de microservicios. Para obtener más información, consulte Descomposición de monolitos en microservicios.

MPA

Consulte Migration Portfolio Assessment.

MQTT

Consulte Message Queuing Telemetry Transport.

clasificación multiclase

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

infraestructura mutable

Modelo que actualiza y modifica la infraestructura actual para las cargas de trabajo de producción. Para mejorar la coherencia, la confiabilidad y la previsibilidad, el AWS Well-Architected Marco recomienda el uso de una infraestructura inmutable como práctica recomendada.

O

OAC

Consulte control de acceso de origen.

OAI

Consulte identidad de acceso de origen.

OCM

Consulte administración del cambio organizacional.

migración fuera de línea

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

OI

Consulte integración de operaciones.

OLA

Consulte acuerdo de nivel operativo.

migración en línea

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

OPC-UA

Consulte Open Process Communications: arquitectura unificada.

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

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

acuerdo de nivel operativo (OLA)

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

revisión de la preparación operativa (ORR)

Lista de comprobación de preguntas y prácticas recomendadas asociadas que son útiles para comprender, evaluar, prevenir o reducir el alcance de los incidentes y posibles errores. Para obtener más información, consulte las revisiones de preparación operativa (ORR) en el AWS Well-Architected marco.

tecnología operativa (TO)

Sistemas de hardware y software que funcionan con el entorno físico para controlar las operaciones, los equipos y la infraestructura industriales. En el sector de la fabricación, la integración de los sistemas de TO y tecnología de la información (TI) es un enfoque clave para las transformaciones de la industria 4.0.

integración de operaciones (OI)

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

registro de seguimiento organizativo

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

administración del cambio organizacional (OCM)

Marco para administrar las transformaciones empresariales importantes y disruptivas desde la perspectiva de las personas, la cultura y el liderazgo. La OCM ayuda a las empresas a prepararse para nuevos sistemas y estrategias y a realizar la transición a ellos, al acelerar la adopción de cambios, abordar los problemas de transición e impulsar cambios culturales y organizacionales. En la estrategia de AWS migración, este marco se denomina aceleración de personal, debido a la velocidad de cambio que requieren los proyectos de adopción de la nube. Para obtener más información, consulte la Guía de OCM.

control de acceso de origen (OAC)

En CloudFront, una opción mejorada para restringir el acceso y proteger el contenido del Amazon Simple Storage Service (Amazon S3). El OAC admite todos los buckets de S3 Regiones de AWS, el cifrado del lado del servidor con AWS KMS (SSE-KMS) y `DELETE` las solicitudes `PUT` y dinámicas al bucket de S3.

identidad de acceso de origen (OAI)

En CloudFront, una opción para restringir el acceso y proteger el contenido de Amazon S3. Cuando utiliza OAI, CloudFront crea un principal con el que Amazon S3 puede autenticarse. Los directores autenticados solo pueden acceder al contenido de un bucket de S3 a través de una distribución específica. CloudFront Consulte también el OAC, que proporciona un control de acceso más detallado y mejorado.

ORR

Consulte revisión de la preparación operativa.

OT

Consulte tecnología operativa.

VPC saliente (de salida)

En una arquitectura de AWS cuentas múltiples, una VPC que gestiona las conexiones de red que se inician desde una aplicación. La Arquitectura de referencia de seguridad de AWS recomienda

configurar su cuenta de red con VPC entrantes, salientes y de inspección para proteger la interfaz bidireccional entre su aplicación e Internet en general.

P

límite de permisos

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

información de identificación personal (PII)

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

PII

Consulte información de identificación personal.

manual de estrategias

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

PLC

Consulte controlador lógico programable.

PLM

Consulte administración del ciclo de vida del producto.

policy

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

persistencia políglota

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

evaluación de cartera

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

predicate

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

inserción de predicados

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

control preventivo

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

entidad principal

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

Privacidad desde el diseño

Enfoque de ingeniería de sistemas que tiene en cuenta la privacidad durante todo el proceso de desarrollo.

zonas alojadas privadas

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

control proactivo

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

administración del ciclo de vida del producto (PLM)

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

entorno de producción

Consulte entorno.

controlador lógico programable (PLC)

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

encadenamiento de peticiones

Uso de la salida de una petición de LLM como entrada para la siguiente petición a fin de generar mejores respuestas. Esta técnica se utiliza para dividir una tarea compleja en tareas secundarias o para refinar o ampliar de forma iterativa una respuesta preliminar. Ayuda a mejorar la precisión y la relevancia de las respuestas de un modelo y permite obtener resultados más detallados y personalizados.

seudonimización

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

publish/subscribe (pub/sub)

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

Q

plan de consulta

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

regresión del plan de consulta

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

R

Matriz RACI

Consulte responsable, fiable, consultada e informada (RACI).

RAG

Consulte generación aumentada por recuperación.

ransomware

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

Matriz RASCI

Consulte responsable, fiable, consultada e informada (RACI).

RCAC

Consulte control de acceso por filas y columnas.

réplica de lectura

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

rediseñar

Consulte Las 7 R.

objetivo de punto de recuperación (RPO)

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

objetivo de tiempo de recuperación (RTO)

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

refactorizar

Consulte Las 7 R.

Region

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

regresión

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

volver a alojar

Consulte Las 7 R.

versión

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

reubicar

Consulte Las 7 R.

redefinir la plataforma

Consulte Las 7 R.

recomprar

Consulte Las 7 R.

resiliencia

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

política basada en recursos

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

matriz responsable, confiable, consultada e informada (RACI)

Una matriz que define las funciones y responsabilidades de todas las partes involucradas en las actividades de migración y las operaciones de la nube. El nombre de la matriz se deriva de los tipos de responsabilidad definidos en la matriz: responsable (R), contable (A), consultado (C) e informado (I). El tipo de soporte (S) es opcional. Si incluye el soporte, la matriz se denomina matriz RASCI y, si la excluye, se denomina matriz RACI.

control receptivo

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

retain

Consulte Las 7 R.

retirar

Consulte Las 7 R.

Generación aumentada de recuperación (RAG)

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

rotación

Proceso mediante el que periódicamente se actualiza un secreto para que resulte más difícil que un atacante pueda acceder a las credenciales.

control de acceso por filas y columnas (RCAC)

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

RPO

Consulte objetivo de punto de recuperación.

RTO

Consulte objetivo de tiempo de recuperación.

manual de procedimientos

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

S

SAML 2.0

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

SCADA

Consulte control de supervisión y adquisición de datos.

SCP

Consulte política de control de servicio.

secreta

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

seguridad desde el diseño

Enfoque de ingeniería de sistemas que tiene en cuenta la seguridad durante todo el proceso de desarrollo.

control de seguridad

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

refuerzo de la seguridad

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

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

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

automatización de la respuesta de seguridad

Acción predefinida y programada que está diseñada para responder automáticamente a un evento de seguridad o corregirlo. Estas automatizaciones sirven como controles de seguridad

preventivos o adaptables que le ayudan a implementar las mejores prácticas AWS de seguridad. La modificación de un grupo de seguridad de VPC, la aplicación de revisiones a una instancia de Amazon EC2 o la rotación de credenciales son algunos ejemplos de acciones de respuesta automatizadas.

cifrado del servidor

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

política de control de servicio (SCP)

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

punto de enlace de servicio

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

acuerdo de nivel de servicio (SLA)

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

indicador de nivel de servicio (SLI)

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

objetivo de nivel de servicio (SLO)

Métrica objetivo que representa el estado de un servicio medido mediante un indicador de nivel de servicio.

modelo de responsabilidad compartida

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

Shadow AI

Aplicaciones de IA no autorizadas creadas o utilizadas fuera de los canales regulados dentro de una organización.

SIEM

Consulte sistema de administración de eventos e información de seguridad.

único punto de error (SPOF)

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

SLA

Consulte acuerdo de nivel de servicio.

SLI

Consulte indicador de nivel de servicio.

SLO

Consulte objetivo de nivel de servicio.

modelo de dividir y sembrar

Un patrón para escalar y acelerar los proyectos de modernización. A medida que se definen las nuevas funciones y los lanzamientos de los productos, el equipo principal se divide para crear nuevos equipos de productos. Esto ayuda a ampliar las capacidades y los servicios de su organización, mejora la productividad de los desarrolladores y apoya la innovación rápida. Para más información, consulte Phased approach to modernizing applications in the Nube de AWS.

SPOF

Consulte único punto de error.

esquema en estrella

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

patrón de higo estrangulador

Un enfoque para modernizar los sistemas monolíticos mediante la reescritura y el reemplazo gradual de las funciones del sistema hasta que se pueda 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, consulte Modernización gradual de los servicios web antiguos de Microsoft ASP.NET (ASMX) mediante contenedores y Amazon API Gateway.

subred

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

control de supervisión y adquisición de datos (SCADA)

En el sector de la fabricación, sistema que utiliza hardware y software para supervisar los activos físicos y las operaciones de producción.

cifrado simétrico

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

pruebas sintéticas

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

petición del sistema

Técnica para proporcionar contexto, instrucciones o pautas a un LLM para dirigir su comportamiento. Las peticiones del sistema ayudan a establecer el contexto y las reglas para las interacciones con los usuarios.

T

etiquetas

Key-value pares que actúan como metadatos para organizar sus AWS recursos. Las etiquetas pueden ayudar a administrar, identificar, organizar, buscar y filtrar recursos de . Para obtener más información, consulte Etiquetado de los recursos de AWS.

variable de destino

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

lista de tareas

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

entorno de prueba

Consulte entorno.

entrenamiento

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

herramienta

Una función o API que un agente puede invocar para realizar operaciones en sistemas externos.

puerta de enlace de tránsito

Centro de tránsito de red que puede utilizar para interconectar las VPC y las redes en las instalaciones. Para obtener más información, consulte Qué es una pasarela de tránsito en la AWS Transit Gateway documentación.

flujo de trabajo basado en enlaces troncales

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

acceso de confianza

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

ajuste

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

equipo de dos pizzas

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

U

incertidumbre

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

tareas indiferenciadas

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

entornos superiores

Consulte entorno.

V

succión

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

control de versión

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

Emparejamiento de VPC

Conexión entre dos VPC que permite enrutar el tráfico mediante direcciones IP privadas. Para obtener más información, consulte ¿Qué es una interconexión de VPC? en la documentación de Amazon VPC.

vulnerabilidad

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

W

caché caliente

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

datos templados

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

función de ventana

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

carga de trabajo

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

flujo de trabajo

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

WORM

Consulte escritura única y lectura múltiple.

WQF

Consulte AWS Workload Qualification Framework.

escritura única y lectura múltiple (WORM)

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

Z

ataque de día cero

Ataque, normalmente de malware, que se aprovecha de una vulnerabilidad de día cero.

vulnerabilidad de día cero

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

peticiones desde cero

Proporcionar a un LLM instrucciones para llevar a cabo una tarea, pero sin ejemplos (pasos) que puedan ayudar a guiarlo. El LLM debe usar los conocimientos del entrenamiento previo para

llevar a cabo la tarea. La eficacia de la petición desde cero depende de la complejidad de la tarea y de la calidad de la petición. Consulte también peticiones con pocos pasos.

aplicación zombi

Aplicación que utiliza un promedio de CPU y memoria menor al 5 por ciento. En un proyecto de migración, es habitual retirar estas aplicaciones.

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.