Adopción de Confianza cero: una estrategia para una transformación empresarial segura y ágil

AWS Guía prescriptiva

AWS Guía prescriptiva: Adopción de Confianza cero: una estrategia para una transformación empresarial segura y ágil

Table of Contents

Adopción de Confianza cero: una estrategia para una transformación empresarial segura y ágil

Greg Gooden, Amazon Web Services (AWS)

Diciembre de 2023 (historial de documentos)

Hoy, más que nunca, las organizaciones se centran en la seguridad como prioridad clave. Esto ofrece una amplia gama de beneficios, desde el mantenimiento de la confianza de sus clientes hasta la mejora de la movilidad del personal y la apertura de nuevas oportunidades empresariales digitales. Mientras lo hacen, siguen planteándose una vieja pregunta: ¿cuáles son los patrones óptimos para garantizar los niveles adecuados de seguridad y disponibilidad para mis sistemas y datos? Cada vez más, Confianza cero se ha convertido en el término utilizado para describir la respuesta moderna a esta pregunta.

Una arquitectura de Confianza cero (ZTA) es un modelo conceptual y un conjunto asociado de mecanismos que se centran en proporcionar controles de seguridad en torno a los activos digitales que no dependen única o fundamentalmente de los controles de red o los perímetros de red tradicionales. En cambio, los controles de red se complementan con la identidad, el dispositivo, el comportamiento y otros contextos y señales completos para tomar decisiones de acceso más detalladas, inteligentes, adaptables y continuas. Al implementar un modelo de ZTA, puede lograr una próxima iteración significativa en la maduración continua de la ciberseguridad y, en particular, los conceptos de defensa en profundidad.

Procesos de toma de decisiones

La implementación de una estrategia de ZTA requiere unos procesos cuidadosos de planificación y toma de decisiones. Implica evaluar varios factores y alinearlos con los objetivos de la organización. Entre los procesos clave de toma de decisiones para embarcarse en un proceso de ZTA se incluyen los siguientes:

1. Participación de las partes interesadas: es crucial involucrar a otros directores de experiencias, vicepresidentes y directivos sénior para comprender sus prioridades, preocupaciones y visión de la postura de seguridad de su organización. Al involucrar a las partes interesadas clave desde el principio, puede alinear la implementación de la ZTA con los objetivos estratégicos generales y obtener el respaldo y los recursos necesarios.

2. Evaluación de riesgos: realizar una evaluación de riesgos exhaustiva ayuda a identificar los problemas, el área expuesta excesiva y los activos críticos, lo que le ayuda a tomar decisiones informadas sobre los controles de seguridad y la inversión. Evalúe la postura de seguridad existente de su organización, identifique las posibles debilidades y priorice las áreas de mejora en función del panorama de riesgos específico de su sector y entorno operativo.
3. Evaluación de la tecnología: evaluar el panorama tecnológico actual de la organización e identificar las brechas ayuda a seleccionar las herramientas y soluciones adecuadas que se alinean con los principios de la ZTA. Esta evaluación debe incluir un análisis exhaustivo de lo siguiente:
    - Arquitectura de redes
    - Sistemas de administración de identidades y accesos
    - Mecanismos de autenticación y autorización
    - Administración unificada de puntos de conexión
    - Herramientas y procesos de propiedad de recursos
    - Tecnologías de cifrado
    - Capacidades de supervisión y registro
    - Elegir la pila de tecnología adecuada es crucial para crear un modelo de ZTA sólido.
4. Administración de los cambios: es esencial reconocer los impactos culturales y organizativos de la adopción de un modelo de ZTA. La implementación de prácticas de administración de cambios ayuda a garantizar una transición y una aceptación fluidas en toda la organización. Implica educar a los empleados sobre los principios y beneficios de la ZTA, impartir capacitación sobre nuevas prácticas de seguridad y fomentar una cultura consciente de la seguridad que fomente la responsabilidad y el aprendizaje continuo.

Esta guía prescriptiva tiene como objetivo proporcionar a los directores de experiencias, vicepresidentes y directivos sénior una estrategia integral para implementar la ZTA. Se profundizará en los aspectos clave de la ZTA, incluidos los siguientes:

- Preparación organizativa
- Enfoques de adopción gradual
- Colaboración de las partes interesadas
- Prácticas recomendadas para lograr una transformación empresarial segura y ágil

Si sigue estas instrucciones, su organización podrá navegar por el panorama de la ZTA y lograr resultados satisfactorios en el proceso de seguridad en la nube de Amazon Web Services (AWS). AWS ofrece una variedad de servicios que puede utilizar para implementar una ZTA, como Acceso verificado de AWS, AWS Identity and Access Management (IAM), Amazon Virtual Private Cloud (Amazon VPC), Amazon VPC Lattice, Amazon Verified Permissions, Amazon API Gateway y Amazon GuardDuty. Estos servicios pueden ayudar a proteger los recursos de AWS del acceso no autorizado.

Resultados empresariales específicos

En esta sección se abordan los resultados esperados que están asociados a la definición e implementación de una arquitectura de Confianza cero en toda su organización.

Posición de seguridad mejorada

Al adoptar los principios de Confianza cero, su organización puede reforzar su postura de seguridad, mitigar los riesgos de seguridad y proteger la infraestructura y los datos de la nube. El principio fundamental de Confianza cero que consiste en conceder acceso en función de lo que se necesite saber, junto con controles estrictos, reduce considerablemente el área expuesta y limita el posible impacto de los eventos de seguridad. Este enfoque proactivo ayuda a las organizaciones a anticiparse a los riesgos de seguridad emergentes y a garantizar la confidencialidad, la integridad y la disponibilidad de los activos.

Adopción de la nube sin problemas

Desarrollar un plan de adopción de una arquitectura de Confianza cero (ZTA) bien definido puede ayudar a garantizar una transición fluida y exitosa al entorno de nube. Los principios de la ZTA se alinean estrechamente con las prácticas recomendadas de seguridad de la nube al proporcionar una base sólida para que las organizaciones obtengan de forma segura los beneficios de la computación en la nube. La incorporación de los principios de la ZTA desde el principio ayuda a su organización a diseñar su arquitectura de nube con la seguridad como elemento central.

Conformidad y alineación normativa

La implementación de las prácticas de la ZTA puede ayudar a su organización a cumplir con los requisitos y estándares normativos del sector. La ZTA promueve intrínsecamente el principio de privilegio mínimo e impone controles de acceso estrictos. Los controles de acceso suelen ser obligatorios en virtud de normativas como las siguientes:

- Programa Federal de Administración de Riesgos y Autorizaciones (Federal Risk and Authorization Management Program, FedRAMP)
- Ley de Portabilidad y Responsabilidad de Seguros Médicos de EE. UU (Health Insurance Portability and Accountability Act, HIPAA).

- Estándar de Seguridad de Datos del Sector de las Tarjetas de Pago (PCI DSS, Payment Card Industry Data Security Standard).

Al adoptar Confianza cero, su organización puede ayudar a demostrar su compromiso con la protección de los datos, la privacidad y la conformidad de las normas, al tiempo que minimiza las posibles sanciones o daños de reputación.

Protección de datos mejorada

Las organizaciones pueden proteger los datos confidenciales durante todo el proceso de adopción de la nube mediante la implementación del cifrado de datos, los controles de acceso y las evaluaciones de seguridad periódicas. Su organización puede seguir estos pasos específicos:

- Cifrado de datos: el cifrado de datos es el proceso de cifrar datos de texto no cifrado en texto cifrado de una manera que requiere una clave para volver a descifrar los datos en su formato original de texto no cifrado. Esto hace que sea mucho más difícil para las personas no autorizadas acceder a los datos confidenciales, incluso si pueden obtener una copia de los datos.
- Controles de acceso: los controles de acceso restringen qué usuarios pueden acceder a los datos confidenciales y qué pueden hacer con ellos. Para ello, puede asignar roles y permisos a los usuarios y utilizar la autenticación multifactor u otros métodos para verificar la identidad de los usuarios.
- Evaluaciones de seguridad periódicas: las evaluaciones de seguridad periódicas pueden ayudar a las organizaciones a identificar y abordar los problemas de seguridad y a solucionarlos de forma proactiva. Estas evaluaciones pueden llevarlas a cabo equipos de seguridad internos o empresas de seguridad externas.

Las arquitecturas de Confianza cero adoptan un enfoque integral de la protección de datos mediante la implementación de una serie de medidas de seguridad. Estas medidas incluyen una autenticación sólida, el cifrado de datos y los controles de acceso detallados. Este enfoque minimiza el riesgo de eventos de seguridad relacionados con los datos y protege la información confidencial del acceso no autorizado.

Respuesta a incidentes eficiente

Las organizaciones pueden detectar los eventos de seguridad y responder a ellos de manera más rápida y eficaz si establecen marcos de supervisión y respuesta a incidentes en el entorno de nube.

Las arquitecturas de Confianza cero hacen hincapié en la supervisión continua, la integración de la inteligencia sobre amenazas y la visibilidad en tiempo real de las actividades de los usuarios, el tráfico de la red y el comportamiento del sistema. De este modo, los equipos de seguridad pueden identificar y mitigar los eventos de seguridad de forma proactiva. Este enfoque reduce el tiempo necesario para detectar posibles problemas y responder a ellos y minimiza el impacto en las operaciones comerciales. Entre los puntos clave se incluyen los siguientes:

- Pruebas: independientemente del marco o la metodología de respuesta a incidentes con el que se alinee su organización, debe probar su plan de respuesta a incidentes con regularidad. Los ejercicios de escritorio, las simulaciones y los equipos rojos ofrecen la oportunidad de practicar la respuesta a incidentes en entornos realistas, descubrir las carencias de las herramientas y capacidades y fomentar la experiencia y la confianza del personal de respuesta a incidentes.
- Supervisión: supervise continuamente sus entornos de nube para detectar signos de actividad anómala. Para ello, puede utilizar diversas herramientas y técnicas, como el análisis de registros, la supervisión de la red y el análisis de vulnerabilidades.
- Integración de la inteligencia sobre amenazas: integre la inteligencia sobre amenazas en sus marcos de supervisión y respuesta a incidentes. Esto ayudará a su organización a identificar las amenazas y responder a ellas de forma más rápida y eficaz.
- Visibilidad en tiempo real: para identificar los incidentes de seguridad y responder a ellos con rapidez, su organización necesita visibilidad en tiempo real de las actividades de los usuarios, el tráfico de la red y el comportamiento del sistema.
- Identificación y mitigación proactivas: al identificar y mitigar de forma proactiva los eventos de seguridad, su organización puede reducir el tiempo de detección de las posibles amenazas y respuesta a ellas y minimizar así el impacto en las operaciones comerciales.

Productividad del personal mejorada

El personal moderno necesita flexibilidad para realizar su trabajo desde una variedad cada vez mayor de ubicaciones, dispositivos y horarios. Al implementar una ZTA, puede cumplir con estos requisitos y mejorar la movilidad, la productividad y la satisfacción del personal, al tiempo que mantiene o mejora la postura de seguridad de la organización.

Posibilitación de la transformación digital

Las organizaciones buscan cada vez más la interconexión de dispositivos, máquinas, instalaciones, infraestructura y procesos fuera del perímetro de la red tradicional como parte de la transformación digital. Los dispositivos de Internet de las cosas (IoT) y tecnología operativa (OT, también conocida como Internet de las cosas industrial o IIoT) suelen transmitir información de telemetría y mantenimiento predictivo directamente a la nube. Para proteger las cargas de trabajo, se requiere la aplicación de controles de seguridad que vayan más allá del enfoque perimetral tradicional.

Sección de resumen

Al centrarse en estos resultados empresariales específicos, su organización puede aprovechar todo el potencial de la ZTA y reforzar su postura de seguridad en la nube. Es importante alinear estos resultados con los objetivos organizativos específicos, adaptarlos a los requisitos empresariales específicos y evaluar periódicamente su eficacia para impulsar la mejora continua.

Descripción de los principios de Confianza cero

Una arquitectura de Confianza cero (ZTA) se basa en un conjunto de principios fundamentales que constituyen la base de su modelo de seguridad. Comprender estos principios es esencial para las organizaciones que desean adoptar una estrategia de ZTA de manera eficaz. En esta sección se presentan los principios básicos de una ZTA.

Verificación y autenticación

El principio de verificación y autenticación enfatiza la importancia de una identificación y autenticación sólidas para las entidades principales de todos los tipos, incluidos los usuarios, las máquinas y los dispositivos. Una ZTA requiere la verificación continua de las identidades y el estado de la autenticación durante toda la sesión, idealmente en cada solicitud. No se basa únicamente en la ubicación o los controles de red tradicionales. Esto incluye la implementación de una autenticación multifactor (MFA) moderna y sólida y la evaluación de señales ambientales y contextuales adicionales durante los procesos de autenticación. Al adoptar este principio, las organizaciones pueden ayudar a garantizar que las decisiones de autorización de recursos tengan las mejores entradas de identidad posibles.

Acceso con privilegios mínimos

El principio del privilegio mínimo implica conceder a las entidades principales el nivel mínimo de acceso necesario para realizar sus tareas. Al adoptar el principio de acceso con privilegios mínimos, las organizaciones pueden aplicar controles de acceso detallados, de modo que las entidades principales solo tengan acceso a los recursos necesarios para cumplir sus funciones y responsabilidades. Esto incluye la implementación del aprovisionamiento del acceso cuando es necesario, los controles de acceso basados en roles (RBAC) y las revisiones periódicas del acceso para minimizar el área expuesta y el riesgo de acceso no autorizado.

Microsegmentación

La microsegmentación es una estrategia de seguridad de red que divide una red en segmentos más pequeños y aislados para autorizar flujos de tráfico específicos. Puede lograr la microsegmentación mediante la creación de límites de cargas de trabajo y la aplicación de controles de acceso estrictos entre los distintos segmentos.

La microsegmentación se puede implementar mediante la virtualización de la red, las redes definidas por el software (SDN), los firewalls basados en hosts, las listas de control de acceso a la red (NACL) y características específicas de AWS, como los grupos de seguridad de Amazon Elastic Compute Cloud (Amazon EC2) o AWS PrivateLink. Las puertas de enlace de segmentación controlan el tráfico entre los segmentos para autorizar el acceso de forma explícita. Las puertas de enlace de microsegmentación y segmentación ayudan a las organizaciones a restringir las rutas innecesarias a través de la red, especialmente las que conducen a sistemas y datos críticos.

Supervisión y análisis continuos

La supervisión y el análisis continuos implican la recopilación, el análisis y la correlación de los eventos y datos relacionados con la seguridad en todo el entorno de la organización. Al implementar herramientas sólidas de supervisión y análisis, su organización puede evaluar los datos de seguridad y la telemetría de manera convergente.

Este principio hace hincapié en la importancia de la visibilidad del comportamiento de los usuarios, el tráfico de la red y las actividades del sistema para identificar anomalías y posibles eventos de seguridad. Tecnologías avanzadas como la administración de eventos e información de seguridad (SIEM), el análisis del comportamiento de los usuarios y las entidades (UEBA) y las plataformas de inteligencia sobre amenazas desempeñan un papel fundamental a la hora de lograr una supervisión continua y una detección proactiva de las amenazas.

Automatización y orquestación

La automatización y la orquestación ayudan a las organizaciones a optimizar los procesos de seguridad, reducir la intervención manual y mejorar los tiempos de respuesta. Al automatizar las tareas de seguridad rutinarias y utilizar las capacidades de orquestación, su organización puede aplicar políticas de seguridad coherentes y responder rápidamente a los eventos de seguridad. Este principio también incluye la automatización de los procesos de aprovisionamiento y desaprovisionamiento del acceso para ayudar a garantizar una administración puntual y precisa de los permisos de los usuarios. Al adoptar la automatización y la orquestación, su organización puede mejorar la eficiencia operativa, reducir los errores humanos y centrar los recursos en iniciativas de seguridad más estratégicas.

Autorización

En una ZTA, cada solicitud de acceso a un recurso debe estar autorizada de forma explícita por un punto de aplicación de puertas. Además de la identidad autenticada, las políticas de autorización deben tener en cuenta un contexto adicional, como el estado y la postura del dispositivo, los patrones de comportamiento, la clasificación de los recursos y los factores de red. El proceso de autorización debe evaluar este contexto convergente en relación con las políticas de acceso correspondientes que sean pertinentes para el recurso al que se accede. De manera óptima, los modelos de machine learning pueden proporcionar un complemento dinámico a las políticas declarativas. Cuando se utilizan, estos modelos deberían centrarse únicamente en las restricciones adicionales y no deberían conceder un acceso que no se haya especificado explícitamente.

Sección de resumen

Al cumplir con estos principios básicos de la ZTA, las organizaciones pueden establecer un modelo de seguridad sólido que se adapte a la diversidad del entorno empresarial moderno. La implementación de estos principios requiere un enfoque integral que combine tecnología, procesos y personas para lograr una mentalidad de Confianza cero y desarrollar una postura de seguridad resiliente.

Componentes clave de una arquitectura de Confianza cero

Para implementar una estrategia de arquitectura de Confianza cero (ZTA) de manera eficaz, su organización debe comprender los componentes clave de una ZTA. Estos componentes trabajan en conjunto para mejorar de forma continua un modelo de seguridad integral que se alinee con los principios de Confianza cero. En esta sección se describen dichos componentes clave de una ZTA.

Administración de identidades y accesos

La administración de identidades y accesos constituye la base de una ZTA, ya que proporciona una autenticación de usuarios sólida y mecanismos de control de acceso generales. Incluye tecnologías como el inicio de sesión único (SSO), la autenticación multifactor (MFA) y las soluciones de administración y gobernanza de identidades. La administración de identidades y accesos proporciona un nivel elevado de garantía de autenticación y un contexto importante que son fundamentales para tomar decisiones de autorización de Confianza cero. Al mismo tiempo, una ZTA es un modelo de seguridad en el que el acceso a las aplicaciones y los recursos se otorga por usuario, dispositivo y sesión. Esto ayuda a proteger a las organizaciones del acceso no autorizado, incluso si las credenciales de un usuario están en peligro.

Periferia de servicio de acceso seguro

La periferia de servicio de acceso seguro (SASE) es un nuevo enfoque de seguridad de la red que virtualiza, combina y distribuye las funciones de red y seguridad en un único servicio basado en la nube. El SASE puede proporcionar acceso seguro a las aplicaciones y los recursos, independientemente de la ubicación del usuario.

El SASE incluye una variedad de características de seguridad, como puertas de enlace web seguras, firewall como servicio y acceso a la red de Confianza cero (ZTNA). Estas características funcionan en conjunto para proteger a las organizaciones de una amplia gama de amenazas, como el malware, la suplantación de identidad y el ransomware.

Prevención de pérdida de datos

Las tecnologías de prevención de pérdida de datos (DLP) pueden ayudar a las organizaciones a proteger los datos confidenciales de la divulgación no autorizada. Las soluciones de DLP supervisan y controlan los datos en movimiento y en reposo. Esto ayuda a las organizaciones a definir y aplicar

políticas que eviten los eventos de seguridad relacionados con los datos, lo que ayuda a garantizar que la información confidencial permanezca protegida en toda la red.

Administración de eventos e información de seguridad (SIEM)

Las soluciones de administración de eventos e información de seguridad (SIEM) recopilan, agregan y analizan los registros de eventos de seguridad de diversos orígenes en la infraestructura de una organización. Puede utilizar estos datos para detectar incidentes de seguridad, facilitar la respuesta a los incidentes y proporcionar información sobre las posibles amenazas y vulnerabilidades.

En el caso de una ZTA en concreto, la capacidad de una solución de SIEM de correlacionar y comprender la telemetría relacionada de los distintos sistemas de seguridad es fundamental para mejorar la detección y la respuesta a patrones anómalos.

Catálogo de propiedad de recursos empresariales

Para conceder acceso a los recursos empresariales de forma adecuada, una organización debe contar con un sistema fiable que catalogue estos recursos y, lo que es más importante, quién es su propietario. Esta fuente de verdad debe proporcionar flujos de trabajo que faciliten las solicitudes de acceso, las decisiones de aprobación asociadas y las atestaciones periódicas de estas. Con el tiempo, esta fuente de verdad contendrá las respuestas a “¿quién puede acceder a qué?” de la organización. Puede utilizar las respuestas tanto para la autorización como para la auditoría y la conformidad.

Administración unificada de puntos de conexión

Además de autenticar de forma sólida al usuario, una ZTA también debe tener en cuenta el estado y la postura del dispositivo del usuario para evaluar si el acceso a los datos y recursos corporativos es seguro. Una plataforma de administración unificada de puntos de conexión (UEM) ofrece las siguientes capacidades:

- Aprovisionamiento de dispositivos
- Administración continua de la configuración y las revisiones
- Definición de la línea de base de seguridad
- Creación de informes de telemetría
- Limpieza y retirada de dispositivos

Puntos de aplicación basados en políticas

En una ZTA, el acceso a cada recurso debe estar autorizado de forma explícita por un punto de aplicación basado en políticas de puertas. Inicialmente, estos puntos de aplicación pueden basarse en los puntos de aplicación existentes en los sistemas de red e identidad existentes. Los puntos de aplicación pueden ser cada vez más idóneos si se tiene en cuenta la gama más amplia de contextos y señales que proporciona la ZTA. A largo plazo, su organización debería implementar puntos de aplicación específicos de la ZTA que funcionen en un contexto convergente, integren de manera coherente a los proveedores de señales, mantengan un conjunto de políticas integral y se mejoren con la inteligencia obtenida de la telemetría combinada.

Sección de resumen

Comprender estos componentes clave es esencial para las organizaciones que planean adoptar una ZTA. Al implementar estos componentes e integrarlos en un modelo de seguridad coherente, su organización puede establecer una postura de seguridad sólida basada en los principios de Confianza cero. En las siguientes secciones se analizan la preparación organizativa, los enfoques de adopción gradual y las prácticas recomendadas para ayudarlo a implementar correctamente una ZTA en su organización.

Evaluación de la preparación organizativa para la adopción de Confianza cero

La adopción de una nueva estrategia de arquitectura es una tarea importante que requiere una planificación cuidadosa y una consideración de los factores organizativos. Esta sección se centra en las principales consideraciones de preparación organizativa para la adopción de Confianza cero en toda la empresa. Al abordar estas consideraciones, su organización puede allanar el camino para adoptar una postura de seguridad más sólida y eficaz.

Alineación y comunicación de la dirección

La alineación y la comunicación de la dirección son esenciales para la implementación exitosa de Confianza cero. La dirección debe comprender los beneficios de Confianza cero y los recursos necesarios. La dirección también debe estar dispuesta a realizar cambios en la cultura y los procesos de la organización. La comunicación con los empleados es necesaria para generar confianza y aceptación. Los empleados deben entender por qué la organización está implementando Confianza cero, qué significa para ellos y cómo pueden ayudar. La comunicación debe ser abierta, transparente y continua.

Apoyo y aceptación de la dirección

Para una implementación exitosa de la arquitectura de Confianza cero (ZTA), es crucial alinear a las partes interesadas y los ejecutivos clave con respecto a los objetivos, los beneficios y las medidas de éxito de la arquitectura. Comparta la importancia de los principios de Confianza cero para mejorar la seguridad y permitir la agilidad empresarial al pasar de la seguridad tradicional basada en el perímetro a un enfoque más detallado y centrado en el usuario. Al cambiar a este enfoque, su organización puede adaptarse a los cambios y las amenazas con mayor rapidez. La alineación de los ejecutivos establece el tono de la organización y ayuda a superar la posible resistencia al cambio.

Comunicación transparente

Mantenga una comunicación abierta y transparente con los empleados durante todo el proceso de implementación de Confianza cero. Explique los motivos, los beneficios y los resultados esperados de la adopción y aborde las inquietudes con prontitud. Proporcione actualizaciones periódicas sobre el progreso de la implementación. De esta forma se aumentará la aceptación, se reducirá la resistencia y se generará confianza.

Desarrollo de habilidades y capacitación

Una vez que la dirección esté alineada y la comunicación sea abierta, es importante desarrollar las habilidades y los conocimientos de los empleados que implementarán Confianza cero. Esto incluye comprender los principios de Confianza cero, cómo implementarlos en su trabajo y cómo responder a los eventos de seguridad. Ofrezca oportunidades de capacitación y desarrollo para ayudar a los empleados a adquirir estas habilidades.

Conocimientos y habilidades sobre la nube

Evalúe las carencias de conocimientos y habilidades de la organización en relación con las tecnologías en la nube y los principios de Confianza cero. Ofrezca programas de capacitación y desarrollo para mejorar las habilidades de los empleados y dotarlos de la experiencia necesaria para trabajar de forma eficaz en un entorno centrado en la nube y de Confianza cero. Para mantenerse al día con la evolución de las tecnologías y las prácticas de seguridad, fomente una cultura de aprendizaje continuo.

Cultura y concienciación en materia de seguridad

Evalúe la cultura de seguridad de la organización. Evalúe el nivel de concienciación en materia de seguridad entre los empleados, su comprensión de las prácticas recomendadas de seguridad y su cumplimiento de las políticas y los procedimientos. Identifique cualquier laguna en los conocimientos sobre seguridad. Considere la posibilidad de llevar a cabo programas de capacitación de concienciación en materia de seguridad para educar a los empleados sobre la importancia de Confianza cero y sus funciones a la hora de mantener un entorno seguro.

Estructura y funciones organizativas

Para implementar Confianza cero con éxito, establezca una estructura y unas funciones organizativas eficaces. Esto incluye la creación de un Centro de excelencia en la nube (CCoE), la revisión y modificación de las operaciones de seguridad y la asignación de funciones y responsabilidades para la administración de vulnerabilidades, la respuesta a incidentes y la supervisión de la seguridad.

Centro de excelencia en la nube

Establezca un CCoE para proporcionar orientación, prácticas recomendadas y supervisión de las operaciones en la nube. Un CCoE es un equipo o grupo de personas responsables de crear e implementar las prácticas recomendadas, directrices y políticas de gobernanza relacionadas con la

nube. El CCoE debe incluir representantes de diferentes unidades de negocio y equipos de TI para ayudar a garantizar la colaboración y la alineación. El CCoE desempeña un papel crucial a la hora de impulsar la adopción de los principios de Confianza cero en las cargas de trabajo alojadas en la nube. El CCoE también facilita el intercambio de conocimientos en toda la organización.

Operaciones de seguridad

Para satisfacer las necesidades de un entorno de Confianza cero, revise y modifique la organización de operaciones de seguridad actual. Para mejorar las capacidades de supervisión, respuesta a incidentes e inteligencia sobre amenazas, considere la posibilidad de implementar centros de operaciones de seguridad (SOC) o proveedores de servicios de seguridad administrados (MSSP). Establezca funciones y responsabilidades para la administración de vulnerabilidades, la respuesta a incidentes y la supervisión de la seguridad. Un proceso de respuesta a incidentes que funcione correctamente es fundamental para garantizar que los eventos de seguridad de menor importancia puedan detectarse y remediarse rápidamente para interrumpir la secuencia de eventos. De esta forma, se ayuda a evitar que un evento de menor importancia se convierta en uno de mayor impacto.

Infraestructura y arquitectura de TI

Examine la arquitectura y la infraestructura de TI de su empresa para encontrar cualquier limitación o dependencia que pueda afectar a la adopción de un enfoque de Confianza cero. Determine si las aplicaciones y los sistemas actuales son compatibles con los componentes arquitectónicos de Confianza cero necesarios. Analice si es necesario mejorar o ajustar la infraestructura para respaldar la implementación exitosa de los principios de Confianza cero. Para cada aplicación o sistema, considere si es mejor implementar Confianza cero de forma local o mediante un esfuerzo de modernización mayor.

Administración de riesgos, gobernanza y control de cambios

Para implementar con éxito Confianza cero, establezca procesos eficaces de administración de riesgos, gobernanza y control de cambios. Esto incluye alinear la administración de riesgos con los principios de Confianza cero, desarrollar un plan de respuesta a incidentes, trabajar con los departamentos de asuntos legales y de conformidad y establecer un proceso de control de cambios.

Administración de riesgos

Examine la estrategia de administración de riesgos vigente en su empresa y determine en qué medida se ajusta a los principios de Confianza cero. Analice la eficiencia de los sistemas actuales

de respuesta a incidentes, las medidas de seguridad y los procedimientos de evaluación de riesgos. Determine qué áreas deben mejorarse para cumplir con la estrategia Confianza cero. Comience a desarrollar un sistema automatizado de respuesta a incidentes o un marco de supervisión y análisis continuos para aumentar la velocidad de resolución.

Procesos de control de cambios

Para garantizar que todas las modificaciones relacionadas con la nube cumplan con los requisitos de seguridad y conformidad, establezca métodos de control de cambios eficaces. Establezca un procedimiento sistemático de administración de cambios que incluya el análisis de la configuración de seguridad, las evaluaciones de riesgos, las aprobaciones y la documentación. Revise y audite las actualizaciones con frecuencia para preservar la integridad de la arquitectura de Confianza cero.

Supervisión y evaluación

Para implementar Confianza cero con éxito, su organización debe supervisar y evaluar continuamente su postura de seguridad. Esto incluye establecer indicadores clave de rendimiento (KPI), supervisar y evaluar los KPI y fomentar una cultura de mejora continua. Al seguir estos pasos, las organizaciones pueden asegurarse de que su implementación de Confianza cero sea exitosa y de que siempre estén trabajando para mejorar su seguridad.

Indicadores clave de rendimiento

Establezca los indicadores clave de rendimiento (KPI) pertinentes para evaluar el éxito y la eficacia de la implementación de Confianza cero. Estos KPI pueden medir la satisfacción de los usuarios, el progreso del equipo y la implementación, la reducción de costos, la observabilidad de la conformidad y el número de incidentes de seguridad. Para hacer un seguimiento del desarrollo general y encontrar oportunidades de mejora, supervise y evalúe periódicamente estos KPI.

Mejora continua

Establecer sistemas para obtener opiniones y puntos de vista de las partes interesadas ayudará a fomentar una cultura de mejora continua. Anime a los miembros del personal a ofrecer ideas y propuestas para mejorar la seguridad, la eficacia y la experiencia del usuario del entorno de nube. Utilice esta información para agilizar los procedimientos, mejorar las medidas de seguridad e impulsar la innovación.

Sección de resumen

Al abordar estas consideraciones organizativas y culturales, su organización puede fomentar un entorno propicio para la adopción en la nube de un modelo de seguridad de Confianza cero. En la siguiente sección se analizan los enfoques de adopción gradual y se proporcionan instrucciones sobre cómo implementar gradualmente los principios de Confianza cero de una manera práctica y controlable.

Cultivar una mentalidad de confianza cero

La implementación de Zero Trust va más allá de las implementaciones técnicas. Requiere un cambio cultural dentro de su organización. Fomentar una mentalidad de confianza cero implica enfatizar los siguientes aspectos clave.

Educación y formación sobre Zero Trust

Eduque a los empleados sobre los valores y las ventajas de la arquitectura de confianza cero (ZTA). Proporcione explicaciones técnicas y no técnicas de los conceptos y enfoques de la ZTA a través de sesiones de capacitación, talleres y otros recursos. Aliente a los miembros del personal a que sean conscientes de sus responsabilidades a la hora de establecer y mantener un paradigma de seguridad de confianza cero.

Colaboración y comunicación

Fomente la colaboración y la transparencia en todos los equipos y departamentos involucrados en la implementación de ZTA. Para garantizar que todos comprendan a fondo el plan, promueva la comunicación interfuncional, el intercambio de conocimientos y el intercambio de información. Cree una cultura de responsabilidad compartida en la que todos reconozcan la importancia de sus contribuciones a la seguridad general de la empresa.

Aprendizaje y mejora continuos

Priorice el aprendizaje y la mejora continuos en el contexto de Zero Trust. Anime a los empleados a mantenerse al día sobre las últimas tendencias, tecnologías y mejores prácticas de seguridad. Fomente una cultura de innovación y experimentación en la que se aliente a los empleados a explorar nuevas soluciones y enfoques para reforzar la postura de seguridad de la organización.

Métricas y responsabilidad

Establezca métricas claras y mecanismos de responsabilidad para medir la eficacia de la estrategia Zero Trust. Defina los indicadores clave de rendimiento (KPI) que se alineen con los objetivos de seguridad de la organización y realice un seguimiento periódico del progreso. Haga que las personas y los equipos rindan cuentas por sus contribuciones a la implementación y el mantenimiento de los principios de Zero Trust.

Resumen de la sección

Al abordar estos aspectos y cultivar una mentalidad de confianza cero, las organizaciones pueden crear una base sólida para la adopción e implementación exitosas de Zero Trust. Este cambio cultural es esencial para ayudar a todos los miembros de la organización a comprender la importancia de Zero Trust y contribuir activamente a su éxito.

La siguiente sección explora los enfoques de adopción gradual y proporciona orientación sobre cómo implementar gradualmente los principios de Zero Trust de una manera práctica y manejable.

Enfoque gradual hacia Confianza cero

La adopción de una arquitectura de Confianza cero (ZTA) requiere una planificación e implementación cuidadosas. Recomendamos un enfoque de adopción gradual para facilitar la transición y minimizar las interrupciones en las operaciones comerciales. En esta sección se proporcionan instrucciones sobre las fases clave que implica la adopción de una ZTA.

Fase 1: evaluación y planificación

La primera fase de la implementación de Confianza cero consiste en la evaluación y la planificación. Esta fase es fundamental para el éxito de la implementación general, ya que implica identificar y abordar cualquier brecha en la postura de seguridad actual de su organización. Si dedica tiempo a evaluar su estado actual y definir sus objetivos de seguridad, puede sentar las bases para una implementación exitosa de Confianza cero.

Al mismo tiempo, una evaluación perfectamente completa y precisa puede no ser siempre realista. Para evitar una paralización de los análisis que le impida avanzar a fases posteriores, prepárese para compartimentarlos o aceptar algún grado de imperfección.

1. Evalúe el estado actual: evalúe la infraestructura, las políticas y los controles de seguridad existentes. Identifique las posibles vulnerabilidades, las brechas de seguridad y las áreas en las que la implementación de los principios de Confianza cero puede proporcionar mejoras.
2. Defina los objetivos de seguridad: en función de los resultados de la evaluación del estado actual, defina los objetivos de seguridad que se alineen con los principios de Confianza cero. Estos objetivos de seguridad también deben alinearse con la estrategia de seguridad general de su organización y abordar las vulnerabilidades y brechas identificadas.
3. Diseñe la arquitectura: desarrolle una ZTA que respalde los objetivos de seguridad de su organización. Esta arquitectura debe incluir los componentes necesarios, como las soluciones de administración de identidades y accesos, los mecanismos de segmentación de la red y los sistemas de supervisión continua. La arquitectura también debe ser escalable, adaptable y capaz de adaptarse al crecimiento futuro y a los avances tecnológicos. Lo ideal es que esta arquitectura se represente en un formato que los equipos responsables de su implementación puedan utilizar fácilmente, como una plantilla de AWS CloudFormation, y no simplemente como un documento o un diagrama.
4. Involucre a las partes interesadas: involucre a todas las partes interesadas, incluidas las unidades de negocio, los equipos de TI y los equipos de seguridad, para obtener información y alinear sus

objetivos con el plan de implementación de la ZTA. Fomente la colaboración y la comunicación para establecer una comprensión compartida de los beneficios y los requisitos del enfoque de Confianza cero.

Fase 2: pruebas piloto e implementación

La segunda fase de la implementación de Confianza cero consiste en las pruebas piloto y la implementación. Esta fase implica probar el ZTA en un entorno controlado a pequeña escala y, a continuación, implementarlo de forma iterativa en toda la organización. Es importante informar a los empleados sobre las nuevas medidas de seguridad y sus funciones a la hora de mantener un entorno de Confianza cero.

1. Haga pruebas piloto de la implementación: pruebe la ZTA en un entorno controlado a pequeña escala. Implemente los componentes y controles de seguridad necesarios que se definieron en la fase de diseño de la arquitectura. Supervise con atención la implementación piloto, recopile comentarios y realice los ajustes necesarios. Prepárese para ser flexible al principio del proceso, cuando Confianza cero pase de ser un ejercicio hipotético a uno con el que crea una experiencia real.
2. Implemente de forma iterativa: basándose en las lecciones aprendidas en la implementación piloto, comience la implementación iterativa de Confianza cero en toda la organización. Genere impulso mediante un efecto volante que no requiera una campaña exhaustiva para alcanzar una masa de implementación crítica. Reserve los mandatos de la dirección o los escalamientos para la cola más larga de la implementación, donde puede que sean necesarios.
3. Capacite y sensibilice a los usuarios: eduque a los empleados sobre las nuevas medidas de seguridad y sus funciones a la hora de mantener un entorno de Confianza cero. Haga hincapié en la importancia de las prácticas seguras, como las contraseñas seguras, la autenticación multifactor y las actualizaciones de seguridad periódicas.
4. Administre el cambio: cree un plan integral de administración de cambios para abordar los cambios organizativos y culturales asociados con la adopción de Confianza cero. Comunique a los empleados los beneficios y los motivos de la adopción y aborde cualquier inquietud o resistencia. Brinde apoyo y orientación continuos para facilitar una transición sin problemas.

Fase 3: supervisión y mejora continua

La tercera y última fase de la implementación de Confianza cero consiste en la supervisión y la mejora continua. Esta fase implica establecer un programa integral de supervisión y análisis, crear un plan integral de respuesta a incidentes y solicitar periódicamente comentarios a las partes interesadas y los usuarios.

1. Supervise continuamente: establezca un programa integral de supervisión y análisis para evaluar continuamente la postura de seguridad y detectar cualquier posible anomalía. Utilice herramientas y tecnologías de seguridad avanzadas para supervisar el comportamiento de los usuarios, el tráfico de la red y las actividades del sistema.
2. Planifique la respuesta a los incidentes y su solución: cree un plan integral de respuesta a incidentes que se alinee con los principios de Confianza cero. Establezca vías de escalamiento claras, defina las funciones y responsabilidades e implemente mecanismos automatizados de respuesta a incidentes cuando sea posible. Pruebe y actualice periódicamente el plan de respuesta a incidentes.
3. Obtenga comentarios y evaluaciones: solicite periódicamente comentarios a las partes interesadas y los usuarios para recopilar información sobre la eficacia de la arquitectura de Confianza cero (ZTA). Realice evaluaciones periódicas para medir el impacto en la postura de seguridad, la eficiencia operativa y la experiencia del usuario. Utilice los comentarios y los resultados de la evaluación para identificar las áreas de mejora. Tenga en cuenta que sus ZTA cambiarán con el tiempo y considere cómo los equipos de desarrollo implementarán estas actualizaciones con una cantidad mínima de esfuerzo o interrupciones.

Sección de resumen

Al seguir este enfoque de adopción gradual, las organizaciones pueden realizar la transición de forma eficaz a una ZTA y, al mismo tiempo, minimizar los riesgos y las interrupciones. En la siguiente sección, se analizan las prácticas recomendadas para lograr el éxito con la implementación de Confianza cero y se abordan las principales consideraciones y recomendaciones para los directores de experiencias, los vicepresidentes y los directivos sénior.

Prácticas recomendadas para lograr el éxito con Confianza cero

La adopción correcta de la arquitectura de Confianza cero (ZTA) requiere un enfoque estratégico y el cumplimiento de las prácticas recomendadas. En esta sección se presenta un conjunto de prácticas recomendadas para guiar a los directores de experiencias, vicepresidentes y directivos sénior a fin de lograr el éxito en la adopción de Confianza cero. Al seguir estas recomendaciones, su organización puede establecer una base de seguridad sólida y aprovechar los beneficios de un enfoque de Confianza cero:

- Defina objetivos claros y resultados empresariales: defina con claridad los objetivos y los resultados empresariales deseados de las operaciones en la nube. Alinee estos objetivos con los principios de Confianza cero para garantizar una base de seguridad sólida y, al mismo tiempo, permitir el crecimiento y la innovación empresarial.
- Realice una evaluación exhaustiva: realice una evaluación exhaustiva de la infraestructura de TI, las aplicaciones y los activos de datos actuales. Identifique las dependencias, la deuda técnica y los posibles problemas de compatibilidad. Esta evaluación servirá de base para el plan de adopción y ayudará a priorizar las cargas de trabajo en función de la criticidad, la complejidad y el impacto empresarial.
- Desarrolle un plan de adopción: incorpore un plan de adopción detallado en el que se describa paso a paso el enfoque para trasladar las cargas de trabajo, las aplicaciones y los datos a la nube. Defina las fases de adopción, los plazos y las dependencias. Involucre a las partes interesadas clave y asigne los recursos en consecuencia.
- Empiece a crear desde el principio: su capacidad para representar con autenticidad el aspecto que tendrá Confianza cero en su organización aumentará considerablemente una vez que comience a crearla e implementarla (en lugar de analizarla y hablar de ella).
- Obtenga el patrocinio ejecutivo: obtenga el patrocinio y el apoyo de los ejecutivos para la implementación de Confianza cero. Involucre a otros ejecutivos de alto nivel para que impulsen la iniciativa y asignen los recursos necesarios. El compromiso de los líderes es esencial para impulsar los cambios culturales y organizativos necesarios para una implementación exitosa.
- Implemente un marco de gobernanza: cree un marco de gobernanza que defina las funciones, las responsabilidades y los procesos de toma de decisiones para la implementación de Confianza cero. Defina claramente la responsabilidad y la propiedad de los controles de seguridad, la

administración de riesgos y la conformidad. Revise y actualice periódicamente el marco de gobernanza para adaptarlo a los cambiantes requisitos de seguridad.

- Apoye la colaboración multifuncional: fomente la colaboración y la comunicación entre las diferentes unidades de negocio, equipos de TI y equipos de seguridad. Cree una cultura de responsabilidad compartida para fomentar la alineación y la coordinación durante la implementación de Confianza cero. Fomente las interacciones frecuentes, el intercambio de conocimientos y la resolución conjunta de problemas.
- Proteja sus datos y aplicaciones: Confianza cero no se limita a que los usuarios finales accedan a los recursos y las aplicaciones. Los principios de Confianza cero también deben implementarse dentro de las cargas de trabajo y entre ellas. Aplique los mismos principios técnicos (identidad sólida, microsegmentación y autorización) utilizando también todo el contexto disponible en el centro de datos.
- Ofrezca una defensa exhaustiva: implemente una estrategia de defensa exhaustiva mediante el uso de varios niveles de controles de seguridad. Combine varias tecnologías de seguridad, como la autenticación multifactor (MFA), la segmentación de la red, el cifrado y la detección de anomalías, para ofrecer una protección integral. Asegúrese de que cada capa complemente a las demás para crear un sistema de defensa sólido.
- Exija una autenticación sólida: aplique mecanismos de autenticación sólida, como la MFA, para todos los usuarios que accedan a todos los recursos. Lo ideal sería considerar la MFA modernas, como las claves de seguridad respaldadas por hardware FIDO2, que proporciona un alto nivel de garantía de autenticación para Confianza cero y ofrece amplias ventajas de seguridad (por ejemplo, protección contra la suplantación de identidad).
- Centralice y mejore la autorización: autorice específicamente cada intento de acceso. Según las características específicas del protocolo, esto debe hacerse por conexión o por solicitud. Lo ideal es por solicitud. Utilice todo el contexto disponible, incluida la información sobre la identidad, el dispositivo, el comportamiento y la red, para tomar decisiones de autorización más detalladas, adaptables y sofisticadas.
- Utilice el principio del privilegio mínimo: implemente el principio del privilegio mínimo para conceder a los usuarios los derechos de acceso mínimos necesarios para realizar sus tareas laborales. Revise y actualice periódicamente los permisos de acceso en función de las funciones laborales, las responsabilidades y las necesidades empresariales. Implemente el aprovisionamiento de acceso cuando es necesario.
- Utilice la administración del acceso con privilegios: implemente una solución de administración del acceso con privilegios (PAM) para proteger las cuentas con privilegios y reducir el riesgo de acceso no autorizado a los sistemas críticos. Las soluciones de PAM pueden proporcionar

controles de acceso con privilegios, grabación de sesiones y capacidades de auditoría para ayudar a su organización a proteger sus datos y sistemas más confidenciales.

- Utilice la microsegmentación: divida su red en segmentos más pequeños y aislados. Utilice la microsegmentación para aplicar controles de acceso estrictos entre los segmentos según las funciones de los usuarios, las aplicaciones o la confidencialidad de los datos. Esfuércese por eliminar todas las vías de red innecesarias, especialmente las que conducen a los datos.
- Supervise las alertas de seguridad y responda a ellas: implemente un programa integral de supervisión de seguridad y respuesta a incidentes en el entorno de la nube. Utilice herramientas y servicios de seguridad nativos en la nube para detectar amenazas en tiempo real, analizar los registros y automatizar la respuesta a los incidentes. Establezca procedimientos claros de respuesta a incidentes, lleve a cabo evaluaciones de seguridad periódicas y supervise continuamente para detectar anomalías o actividades sospechosas.
- Utilice la supervisión continua: para detectar incidentes de seguridad de forma rápida y eficaz y responder a ellos, implemente una supervisión continua. Utilice herramientas de análisis de seguridad avanzadas para supervisar el comportamiento de los usuarios, el tráfico de la red y las actividades del sistema. Automatice las alertas y notificaciones para garantizar que se responda a los incidentes de manera oportuna.
- Promueva una cultura de seguridad y conformidad: promueva una cultura de seguridad y conformidad en toda la organización. Informe a los empleados sobre las prácticas recomendadas de seguridad, la importancia de cumplir con los principios de Confianza cero y el papel de los empleados a la hora de mantener un entorno de nube seguro. Imparta sesiones periódicas de capacitación sobre concienciación en materia de seguridad para garantizar que los empleados estén atentos a la ingeniería social y que comprendan sus responsabilidades en relación con la protección de los datos y la privacidad.
- Utilice simulaciones de ingeniería social: realice simulaciones de ingeniería social para evaluar la susceptibilidad de los usuarios a los ataques de ingeniería social. Utilice los resultados de las simulaciones para adaptar los programas de capacitación a fin de mejorar la concienciación de los usuarios y la respuesta a las posibles amenazas.
- Promueva la educación continua: establezca una cultura de educación y aprendizaje continuos con sesiones de capacitación y recursos de seguridad continuos. Mantenga a los usuarios informados sobre las prácticas recomendadas de seguridad en evolución. Anime a los usuarios a estar atentos y a denunciar cualquier actividad sospechosa con prontitud.
- Evalúe y optimice de forma continua: evalúe periódicamente el entorno de nube para detectar las áreas de mejora. Utilice herramientas nativas en la nube para supervisar el uso y el rendimiento

de los recursos y lleve a cabo evaluaciones de vulnerabilidad y pruebas de penetración para identificar y abordar cualquier punto débil.

- Establezca un marco de gobernanza y conformidad: desarrolle un marco de gobernanza y conformidad que lo ayude a garantizar que la organización esté alineada con los estándares y requisitos normativos del sector. En el marco, defina políticas, procedimientos y controles para proteger los datos y los sistemas del acceso, el uso, la divulgación, la interrupción, la modificación o la destrucción no autorizados. Implemente mecanismos para hacer un seguimiento de las métricas de cumplimiento e informar sobre ellas, realizar auditorías periódicas y abordar cualquier problema de incumplimiento con prontitud.
- Fomente la colaboración y el intercambio de conocimientos: fomente la colaboración y el intercambio de conocimientos entre los equipos que participan en la adopción de la ZTA. Para ello, fomente la comunicación y la colaboración interfuncionales entre las unidades de TI, seguridad y negocios. Su organización también puede organizar foros, talleres y sesiones de intercambio de conocimientos para promover la comprensión, abordar los desafíos y compartir las lecciones aprendidas durante el proceso de adopción.

Conclusiones clave

En esta guía se han explorado los aspectos esenciales del desarrollo de una estrategia exitosa de arquitectura de Confianza cero (ZTA). En esta sección se resumen las principales conclusiones de la guía prescriptiva presentada:

- Comprenda los principios de Confianza cero: Confianza cero es un modelo conceptual y un conjunto asociado de mecanismos que se centran en proporcionar controles de seguridad en torno a los activos digitales que no dependen única o fundamentalmente de los controles de red o los perímetros de red tradicionales. En cambio, los controles de red se complementan con la identidad, el dispositivo, el comportamiento y otros contextos y señales completos para tomar decisiones de acceso más detalladas, inteligentes, adaptables y continuas. Familiarícese con los principios básicos de Confianza cero, como el privilegio mínimo, la microsegmentación, la autenticación continua y la autorización adaptativa.
- Defina objetivos claros: defina con claridad los objetivos y los resultados empresariales deseados tras la adopción de la ZTA. Alinee estos objetivos con los principios de Confianza cero para ayudar a garantizar una base de seguridad sólida y, al mismo tiempo, permitir el crecimiento y la innovación empresarial.
- Realice evaluaciones exhaustivas: realice una evaluación exhaustiva de su infraestructura de TI, aplicaciones y activos de datos existentes. Identifique las dependencias, la deuda técnica y los problemas de compatibilidad para fundamentar su estrategia de adopción.
- Desarrolle un plan de adopción de la ZTA: cree un plan detallado en el que se describa paso a paso el enfoque para trasladar las cargas de trabajo, las aplicaciones y los datos a la nube. Tenga en cuenta factores como los requisitos de conformidad y la modernización de las aplicaciones.
- Implemente una ZTA sólida: diseñe e implemente una ZTA que aplique controles de acceso detallados, mecanismos de autenticación sólidos y supervisión continua. Para una adopción de la ZTA más eficiente, utilice los servicios de Confianza cero nativos en la nube, como Acceso verificado de AWS y Amazon VPC Lattice.
- Priorice la seguridad de los datos y las aplicaciones: aplique los principios de Confianza cero (identidad sólida, microsegmentación y autorización) para proporcionar todo el contexto disponible. Utilice este contexto para los usuarios que acceden a los sistemas y recursos y para el flujo de comunicaciones y datos dentro de los componentes del back-end y entre ellos.
- Establezca marcos de supervisión y respuesta a incidentes: implemente capacidades sólidas de supervisión de seguridad y respuesta a incidentes en el entorno de nube. Utilice herramientas de seguridad nativas en la nube para la detección de amenazas en tiempo real, el análisis de registros

y la automatización de la respuesta a incidentes, como Amazon Inspector, AWS Security Hub y Amazon GuardDuty.

- Fomente una cultura de seguridad y conformidad: promueva una cultura de concienciación sobre la seguridad y conformidad en toda la organización. Informe a los empleados sobre las prácticas recomendadas de seguridad y su función en el mantenimiento de un entorno de nube seguro.
- Evalúe y optimice de forma continua: evalúe periódicamente el entorno de nube, los controles de seguridad y los procesos operativos. Para recopilar información y optimizar la utilización de los recursos, la administración de costos y el rendimiento, utilice herramientas de análisis y supervisión nativas en la nube, como Amazon CloudWatch y AWS Security Hub.
- Establezca marcos de gobernanza y conformidad: desarrolle marcos de gobernanza y conformidad que se alineen con los estándares y requisitos normativos del sector. Defina políticas, procedimientos y controles para garantizar el cumplimiento de las normas de seguridad, privacidad y conformidad.

Siguientes pasos

Adoptar una arquitectura de Confianza cero (ZTA) es una de las formas más seguras de mejorar la postura de su organización y reducir el riesgo. En esta guía prescriptiva se ha proporcionado una hoja de ruta completa para implementar Confianza cero, que abarca desde la comprensión de los principios hasta la evaluación de su preparación y la implementación de los componentes necesarios.

Los siguientes pasos de este flujo de trabajo o dominio conllevan lo siguiente:

- La implementación del plan de adopción
- La implementación de la ZTA
- La realización de evaluaciones de seguridad periódicas
- La optimización continua del entorno de nube y los controles de seguridad

La ZTA es un proceso continuo que requiere una supervisión, evaluación y adaptación constantes para garantizar una base de seguridad sólida. Si sigue las prácticas recomendadas descritas en esta guía, su organización puede mejorar su postura de seguridad, garantizar la conformidad con las normativas y proteger los datos confidenciales.

Preguntas frecuentes

En esta sección se ofrecen respuestas a preguntas frecuentes sobre el diseño e implementación de una arquitectura de Confianza cero (ZTA).

¿Qué es Confianza cero?

Confianza cero es un modelo conceptual y un conjunto asociado de mecanismos que se centran en proporcionar controles de seguridad en torno a los activos digitales que no dependen única o fundamentalmente de los controles de red o los perímetros de red tradicionales. En cambio, los controles de red se complementan con la identidad, el dispositivo, el comportamiento y otros contextos y señales completos para tomar decisiones de acceso más detalladas, inteligentes, adaptables y continuas.

¿Qué Servicios de AWS pueden ayudarme a implementar una arquitectura de Confianza cero?

AWS brinda varios servicios que pueden ayudar a implementar Confianza cero, como Acceso verificado de AWS, AWS Identity and Access Management (IAM), Amazon Virtual Private Cloud (Amazon VPC), Amazon VPC Lattice, Amazon Verified Permissions, Amazon API Gateway y Amazon GuardDuty.

¿Cómo puedo garantizar la seguridad de los datos con AWS?

AWS ofrece servicios como AWS Key Management Service (AWS KMS) para el cifrado de datos en reposo y en tránsito, Amazon Virtual Private Cloud (Amazon VPC) para el aislamiento de la red y AWS Secrets Manager para el almacenamiento y la recuperación seguros de credenciales.

¿Puede AWS ayudar con los requisitos de conformidad en un entorno de Confianza cero?

Sí, AWS cuenta con programas y servicios de conformidad que ayudan a cumplir con diversos requisitos normativos. AWS Artifact proporciona acceso a los informes de conformidad de AWS y AWS Config respalda la supervisión y la evaluación continuas de la conformidad.

¿Existen herramientas o servicios de AWS para automatizar la seguridad en un entorno de Confianza cero?

AWS proporciona servicios como AWS Security Hub, que centraliza y automatiza los resultados de seguridad, y reglas de AWS Config para definir y aplicar las políticas de seguridad.

¿Cómo puedo garantizar la supervisión continua y la respuesta a los incidentes en un entorno de nube de Confianza cero con AWS?

AWS ofrece servicios como Amazon CloudWatch para la supervisión en tiempo real y AWS CloudTrail para el registro y el análisis. Para conocer las prácticas recomendadas de respuesta a incidentes, puede utilizar el documento AWS Security Incident Response Guide.

Recursos

Referencias

- What is a cloud center of excellence and why should your organization create one?: en esta entrada de blog se ofrece información general sobre los CCoE, las prácticas recomendadas para crear un CCoE eficaz y mucho más.
- Confianza cero en AWS: en esta página se ofrece información general sobre los principios de seguridad y las prácticas recomendadas de Confianza cero en el entorno de AWS.
- Zero Trust architecture: An AWS perspective: en esta entrada de blog se comparte una definición y los principios rectores sobre la forma en que se implementa Confianza cero en AWS.
- Guía del usuario de AWS Identity and Access Management (IAM): en esta guía se ofrece una documentación completa sobre la administración del acceso y los permisos de los usuarios en IAM, un componente crucial de la arquitectura de Confianza cero.
- AWS Security Hub: obtenga información sobre Security Hub, un servicio que brinda una vista integral de las alertas de seguridad y del estado de conformidad de sus Cuentas de AWS.
- Marco de AWS Well-Architected: explore el Marco de Well-Architected, que brinda orientación sobre cómo crear arquitecturas seguras, de alto rendimiento, resilientes y eficientes en AWS.
- AWS Security Incident Response Guide: en esta guía se presenta información general sobre los fundamentos de la respuesta a incidentes de seguridad en el entorno de la Nube de AWS de su organización. Se proporciona información general sobre los conceptos de seguridad en la nube y respuesta a incidentes y se identifican las capacidades, los servicios y los mecanismos de la nube que están disponibles para los clientes que responden a problemas de seguridad.

Herramientas

- Amazon API Gateway
- AWS Artifact
- AWS CloudTrail
- Amazon CloudWatch
- AWS Config
- Amazon GuardDuty

- AWS Identity and Access Management
- AWS Key Management Service
- AWS Secrets Manager
- AWS Security Hub
- Acceso verificado de AWS

Historial del documento

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
Se agregaron actualizaciones	Se agregó información a la sección Componentes clave de una arquitectura de Confianza cero, se realizaron cambios en la sección Evaluación de la preparación organizativa para la adopción de Confianza cero, se agregó información a la sección Prácticas recomendadas y se realizaron cambios en Preguntas frecuentes.	4 de diciembre de 2023
Publicación inicial	—	19 de junio de 2023

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:

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

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

A

ABAC

Consulte control de acceso basado en atributos.

servicios abstractos

Consulte servicios gestionados.

ACID

Consulte atomicidad, consistencia, aislamiento y durabilidad.

migración activa-activa

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

migración activa-pasiva

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

función agregada

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

IA

Véase inteligencia artificial.

AIOps

Consulte las operaciones de inteligencia artificial.

anonimización

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

antipatrones

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

control de aplicaciones

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

cartera de aplicaciones

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

inteligencia artificial (IA)

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

operaciones de inteligencia artificial (AIOps)

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

cifrado asimétrico

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

atomicidad, consistencia, aislamiento, durabilidad () ACID

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

control de acceso basado en atributos () ABAC

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

origen de datos fidedigno

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

Zona de disponibilidad

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

AWS Marco de adopción de la nube ()AWS CAF

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

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

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

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

B

un bot malo

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

BCP

Consulte la planificación de la continuidad del negocio.

gráfico de comportamiento

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

sistema big-endian

Un sistema que almacena primero el byte más significativo. Véase también endianismo.

clasificación binaria

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

filtro de floración

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

implementación azul/verde

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

bot

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

botnet

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

rama

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

acceso con cristales rotos

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

estrategia de implementación sobre infraestructura existente

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

caché de búfer

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

capacidad empresarial

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

planificación de la continuidad del negocio () BCP

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

C

CAF

Consulte el marco AWS de adopción de la nube.

despliegue canario

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

CCoE

Consulte Cloud Center of Excellence.

CDC

Consulte la captura de datos de cambios.

cambiar la captura de datos (CDC)

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

ingeniería del caos

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

CI/CD

Consulte la integración continua y la entrega continua.

clasificación

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

cifrado del cliente

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

Centro de excelencia en la nube (CCoE)

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

computación en la nube

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

modelo operativo en la nube

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

etapas de adopción de la nube

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

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

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

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

CMDB

Consulte la base de datos de administración de la configuración.

repositorio de código

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

caché en frío

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

datos fríos

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

visión artificial (CV)

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

desviación de configuración

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

base de datos de gestión de la configuración () CMDB

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

paquete de conformidad

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

integración y entrega continuas (CI/CD)

El proceso de automatización de las etapas de origen, compilación, prueba, presentación y producción del proceso de lanzamiento del software. CI/CD is commonly described as a pipeline. CI/CDpueden ayudarlo a automatizar los procesos, mejorar la productividad, mejorar la calidad del código y entregar con mayor rapidez. Para obtener más información, consulte Beneficios de la entrega continua. CD también puede significar implementación continua. Para obtener más información, consulte Entrega continua frente a implementación continua.

CV

Vea la visión artificial.

D

datos en reposo

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

clasificación de datos

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

desviación de datos

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

datos en tránsito

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

malla de datos

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

minimización de datos

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

perímetro de datos

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

preprocesamiento de datos

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

procedencia de los datos

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

titular de los datos

Persona cuyos datos se recopilan y procesan.

almacenamiento de datos

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

lenguaje de definición de bases de datos (DDL)

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

lenguaje de manipulación de bases de datos (DML)

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

DDL

Consulte el lenguaje de definición de bases de datos.

conjunto profundo

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

aprendizaje profundo

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

defense-in-depth

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

administrador delegado

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

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

Implementación

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

entorno de desarrollo

Consulte entorno.

control de detección

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

mapeo del flujo de valor de desarrollo (DVSM)

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

gemelo digital

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

tabla de dimensiones

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

desastre

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

recuperación de desastres (DR)

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

DML

Consulte el lenguaje de manipulación de bases de datos.

diseño basado en el dominio

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

DR

Consulte recuperación ante desastres.

detección de desviaciones

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

DVSM

Consulte el mapeo del flujo de valor del desarrollo.

E

EDA

Consulte el análisis exploratorio de datos.

EDI

Véase 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 nube, la computación perimetral puede reducir la latencia de la comunicación y mejorar el tiempo de respuesta.

intercambio electrónico de datos () EDI

El intercambio automatizado de documentos comerciales entre organizaciones. Para obtener más información, consulte Qué es el intercambio electrónico de datos.

cifrado

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

clave de cifrado

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

endianidad

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

punto de conexión

Consulte el punto final del servicio.

servicio de punto de conexión

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

consulte Crear un servicio de punto final en la documentación de Amazon Virtual Private Cloud (AmazonVPC).

planificación de recursos empresariales (ERP)

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

cifrado de sobre

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

environment

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

- entorno de desarrollo: instancia de una aplicación en ejecución que solo se encuentra disponible para el equipo principal responsable del mantenimiento de la aplicación. Los entornos de desarrollo se utilizan para probar los cambios antes de promocionarlos a los entornos superiores. Este tipo de entorno a veces se denomina entorno de prueba.
- entornos inferiores: todos los entornos de desarrollo de una aplicación, como los que se utilizan para las compilaciones y pruebas iniciales.
- entorno de producción: instancia de una aplicación en ejecución a la que pueden acceder los usuarios finales. En una canalización de CI/CD, el entorno de producción es el último entorno de implementación.
- entornos superiores: todos los entornos a los que pueden acceder usuarios que no sean del equipo de desarrollo principal. Esto puede incluir un entorno de producción, entornos de preproducción y entornos para las pruebas de aceptación por parte de los usuarios.

epopeya

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

ERP

Consulte la planificación de recursos empresariales.

análisis exploratorio de datos () EDA

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

F

tabla de datos

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

fallan rápidamente

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

límite de aislamiento de fallas

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

rama de característica

Consulte la sucursal.

características

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

importancia de las características

La importancia que tiene una característica para las predicciones de un modelo. Por lo general, se expresa como una puntuación numérica que se puede calcular mediante diversas técnicas,

como las explicaciones aditivas de Shapley (SHAP) y los gradientes integrados. Para obtener más información, consulte Interpretabilidad del modelo de aprendizaje automático con:.AWS

transformación de funciones

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

indicaciones de pocos pasos

LLMProporcionando un pequeño número de ejemplos que demuestren la tarea y el resultado deseado antes de pedirle que realice una tarea similar. Esta técnica es una aplicación del aprendizaje contextual, en el que los modelos aprenden a partir de ejemplos (planos) integrados en las instrucciones. Las indicaciones con pocas tomas pueden ser eficaces para tareas que requieren un formato, un razonamiento o un conocimiento del dominio específicos. Consulte también el apartado de mensajes sin intervención.

FGAC

Consulte el control de acceso detallado.

control de acceso detallado () FGAC

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

migración relámpago

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

FM

Consulte el modelo básico.

modelo de cimentación (FM)

Una gran red neuronal de aprendizaje profundo que se ha estado entrenando con conjuntos de datos masivos de datos generalizados y sin etiquetar. FMsson capaces de realizar una amplia variedad de tareas generales, como comprender el lenguaje, generar texto e imágenes

y conversar en lenguaje natural. Para obtener más información, consulte Qué son los modelos básicos.

G

IA generativa

Un subconjunto de modelos de IA que se han entrenado con grandes cantidades de datos y que pueden utilizar un simple mensaje de texto para crear contenido y artefactos nuevos, como imágenes, vídeos, texto y audio. Para obtener más información, consulte Qué es la IA generativa.

bloqueo geográfico

Consulta las restricciones geográficas.

restricciones geográficas (bloqueo geográfico)

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

Flujo de trabajo de Gitflow

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

imagen dorada

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

H

JA

Consulte alta disponibilidad.

migración heterogénea de bases de datos

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

alta disponibilidad (HA)

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

modernización histórica

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

datos retenidos

Parte de los datos históricos etiquetados que se ocultan de un conjunto de datos que se utiliza para entrenar un modelo de aprendizaje automático. Puede utilizar los datos de reserva para evaluar el rendimiento del modelo comparando las predicciones del modelo con los datos de reserva.

migración homogénea de bases de datos

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

datos recientes

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

hotfix

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

periodo de hiperatención

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

I

IaC

Vea la infraestructura como código.

políticas basadas en identidad

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

aplicación inactiva

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

IIoT

Consulte Internet de las cosas industrial.

infraestructura inmutable

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

entrante (ingreso) VPC

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

migración gradual

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

Industria 4.0

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

infraestructura

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

infraestructura como código (IaC)

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

Internet de las cosas industrial () IIoT

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

inspección VPC

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

Internet de las cosas (IoT)

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

interpretabilidad

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

IoT

Consulte Internet de las cosas.

Biblioteca de información de TI (ITIL)

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

Administración de servicios de TI (ITSM)

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

ITIL

Consulte la biblioteca de información de TI.

ITSM

Consulte Administración de servicios de TI.

L

control de acceso basado en etiquetas () LBAC

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

zona de aterrizaje

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

modelo de lenguaje grande () LLM

Un modelo de IA de aprendizaje profundo que se entrena previamente con una gran cantidad de datos. An LLM puede realizar múltiples tareas, como responder preguntas, resumir documentos, traducir textos a otros idiomas y completar oraciones. Para obtener más información, consulte Qué son. LLMs

migración grande

Migración de 300 servidores o más.

LBAC

Consulte el control de acceso basado en etiquetas.

privilegio mínimo

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

migrar mediante lift-and-shift

Consulte 7 Rs.

sistema little-endian

Un sistema que almacena primero el byte menos significativo. Véase también endianness.

LLM

Véase un modelo de lenguaje amplio.

entornos inferiores

Véase entorno.

M

machine learning (ML)

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

rama principal

Ver sucursal.

malware

Software diseñado para comprometer la seguridad o la privacidad de la computadora. El malware puede interrumpir los sistemas informáticos, filtrar información confidencial u obtener acceso

no autorizado. Algunos ejemplos de malware son los virus, los gusanos, el ransomware, los troyanos, el spyware y los registradores de pulsaciones de teclas.

servicios gestionados

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

sistema de ejecución de fabricación () MES

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

MAP

Consulte Migration Acceleration Program.

Mecanismo

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

cuenta de miembro

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

MES

Consulte el sistema de ejecución de la fabricación.

Transporte de telemetría y cola de mensajes () MQTT

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

microservicio

Un servicio pequeño e independiente que se comunica a través de una red bien definida APIs y que, por lo general, es propiedad de equipos pequeños e independientes. Por ejemplo,

un sistema de seguros puede incluir microservicios que se adapten a las capacidades empresariales, como las de ventas o marketing, o a subdominios, como las de compras, reclamaciones o análisis. Los beneficios de los microservicios incluyen la agilidad, la escalabilidad flexible, la facilidad de implementación, el código reutilizable y la resiliencia. Para obtener más información, consulte Integrar microservicios mediante AWS servicios sin servidor.

arquitectura de microservicios

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

Migration Acceleration Program (MAP)

Un AWS programa que brinda soporte de consultoría, capacitación y servicios para ayudar a las organizaciones a construir una base operativa sólida para migrar a la nube y para ayudar a compensar el costo inicial de las migraciones. MAPincluye una metodología de migración para ejecutar las migraciones antiguas de forma metódica y un conjunto de herramientas para automatizar y acelerar los escenarios de migración habituales.

migración a escala

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

fábrica de migración

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

metadatos de migración

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

patrón de migración

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

Evaluación de la cartera de migración () MPA

Una herramienta en línea que proporciona información para validar el argumento empresarial para migrar a. Nube de AWS MPAproporciona una evaluación detallada de la cartera (tamaño correcto de los servidores, precios, TCO comparaciones y análisis de los costos de migración), así como una planificación de la migración (análisis y recopilación de datos de aplicaciones, agrupación de aplicaciones, priorización de la migración y planificación de la oleada). La MPAherramienta (requiere iniciar sesión) está disponible de forma gratuita para todos los consultores y AWS consultores de los socios. APN

Evaluación de la preparación para la migración (MRA)

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

estrategia de migración

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

ML

Consulte el aprendizaje automático.

modernización

Transformar una aplicación obsoleta (antigua o monolítica) y su infraestructura en un sistema ágil, elástico y de alta disponibilidad en la nube para reducir los gastos, aumentar la eficiencia y

aprovechar las innovaciones. Para obtener más información, consulte Estrategia para modernizar las aplicaciones en el Nube de AWS.

evaluación de la preparación para la modernización

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

aplicaciones monolíticas (monolitos)

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

MPA

Consulte la evaluación de la cartera de migración.

MQTT

Consulte Message Queue Queue Telemetría y Transporte.

clasificación multiclase

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

infraestructura mutable

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

O

OAC

Consulte el control de acceso de origen.

OAI

Consulte la identidad de acceso de origen.

OCM

Consulte gestión del cambio organizacional.

migración fuera de línea

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

OI

Consulte integración de operaciones.

OLA

Consulte el acuerdo a nivel operativo.

migración en línea

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

OPC-UA

Consulte Open Process Communications: arquitectura unificada.

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

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

acuerdo a nivel operativo () OLA

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

revisión de la preparación operativa () ORR

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

tecnología operativa (OT)

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

integración de operaciones (OI)

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

registro de seguimiento organizativo

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

gestión del cambio organizacional (OCM)

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

control de acceso de origen (OAC)

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

identidad de acceso de origen () OAI

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

ORR

Consulte la revisión de la preparación operativa.

NO

Consulte tecnología operativa.

saliente (salida) VPC

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

P

límite de permisos

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

información de identificación personal (PII)

Información que, vista directamente o combinada con otros datos relacionados, puede utilizarse para deducir de manera razonable la identidad de una persona. Algunos ejemplos PII incluyen nombres, direcciones e información de contacto.

PII

Consulte la información de identificación personal.

manual de estrategias

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

PLC

Consulte controlador lógico programable.

PLM

Consulte la gestión del ciclo de vida del producto.

política

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

persistencia políglota

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

evaluación de cartera

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

predicate

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

pulsar un predicado

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

control preventivo

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

entidad principal

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

privacidad desde el diseño

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

zonas alojadas privadas

Un contenedor que contiene información sobre cómo desea que Amazon Route 53 responda a DNS las consultas de un dominio y sus subdominios dentro de uno o másVPCs. Para obtener más información, consulte Uso de zonas alojadas privadas en la documentación de Route 53.

control proactivo

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

gestión del ciclo de vida del producto (PLM)

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

entorno de producción

Consulte el entorno.

controlador lógico programable () PLC

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

encadenamiento rápido

Utilizar la salida de un LLMmensaje como entrada para el siguiente mensaje para generar mejores respuestas. Esta técnica se utiliza para dividir una tarea compleja en subtareas 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)

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

Q

plan de consulta

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

regresión del plan de consulta

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

R

RACImatriz

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

RAG

Consulte Retrieval Augmented Generation.

ransomware

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

RASCImatriz

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

RCAC

Consulte el control de acceso por filas y columnas.

read replica

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

rediseñar

Ver 7 Rs.

objetivo de punto de recuperación (RPO)

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

objetivo de tiempo de recuperación (RTO)

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

refactorizar

Ver 7 Rs.

Región

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

regresión

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

volver a alojar

Consulte 7 Rs.

versión

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

trasladarse

Ver 7 Rs.

redefinir la plataforma

Ver 7 Rs.

recompra

Ver 7 Rs.

resilencia

La capacidad de una aplicación para resistir las interrupciones o recuperarse de ellas. La alta disponibilidad y la recuperación ante desastres son consideraciones comunes a la hora de

planificar la resiliencia en el. Nube de AWS Para obtener más información, consulte Nube de AWS Resiliencia.

política basada en recursos

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

matriz responsable, responsable, consultada, informada (RACI)

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

control receptivo

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

retain

Consulte 7 Rs.

jubilarse

Ver 7 Rs.

Generación aumentada de recuperación () RAG

Una tecnología de IA generativa en la que, antes de generar una respuesta, LLMhace referencia a una fuente de datos autorizada que se encuentra fuera de sus fuentes de datos de entrenamiento. Por ejemplo, un RAG modelo puede realizar una búsqueda semántica en la base de conocimientos o en los datos personalizados de una organización. Para obtener más información, consulte Qué es RAG.

Rotation

Proceso de actualizar periódicamente un secreto para dificultar el acceso de un atacante a las credenciales.

control de acceso por filas y columnas (RCAC)

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

RPO

Consulte el objetivo del punto de recuperación.

RTO

Consulte el objetivo de tiempo de recuperación.

manual de procedimientos

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

S

SAML2.0

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

SCADA

Consulte el control de supervisión y la adquisición de datos.

SCP

Consulte la política de control de servicios.

secreta

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

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

seguridad desde el diseño

Un 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 principales de controles de seguridad: preventivos, de detección, con capacidad de respuesta y proactivos.

refuerzo de la seguridad

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

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

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

automatización de las respuestas de seguridad

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

cifrado del servidor

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

política de control de servicios (SCP)

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

punto de enlace de servicio

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

acuerdo de nivel de servicio () SLA

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

indicador de nivel de servicio () SLI

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

objetivo de nivel de servicio () SLO

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

modelo de responsabilidad compartida

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

SIEM

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

punto único de fallo (SPOF)

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

SLA

Consulte el acuerdo de nivel de servicio.

SLI

Consulte el indicador de nivel de servicio.

SLO

Consulte el objetivo de nivel de servicio.

split-and-seed modelo

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

SPOF

Consulte el punto único de fallo.

esquema en forma de estrella

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

patrón de higo estrangulador

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

subred

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

control de supervisión y adquisición de datos (SCADA)

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

cifrado simétrico

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

pruebas sintéticas

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

indicador del sistema

Técnica para proporcionar contexto, instrucciones o pautas LLMa un comportamiento y dirigirlo. Las indicaciones del sistema ayudan a establecer el contexto y las reglas para las interacciones con los usuarios.

T

etiquetas

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

variable de destino

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

lista de tareas

Herramienta que se utiliza para hacer un seguimiento del progreso mediante un manual de procedimientos. La lista de tareas contiene una descripción general del manual de

procedimientos y una lista de las tareas generales que deben completarse. Para cada tarea general, se incluye la cantidad estimada de tiempo necesario, el propietario y el progreso.

entorno de prueba

Consulte entorno.

entrenamiento

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

puerta de enlace de tránsito

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

flujo de trabajo basado en enlaces troncales

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

acceso de confianza

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

ajuste

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

equipo de dos pizzas

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

U

incertidumbre

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

tareas indiferenciadas

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

entornos superiores

Ver entorno.

V

succión

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

control de versión

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

VPCmirando

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

vulnerabilidad

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

W

caché caliente

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

datos templados

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

función de ventana

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

carga de trabajo

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

flujo de trabajo

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

WORM

Mira, escribe una vez, lee muchas.

WQF

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

escribe una vez, lee muchas (WORM)

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

Z

ataque de día cero

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

vulnerabilidad de día cero

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

aviso de tiro cero

Proporciona instrucciones para realizar una LLMtarea, pero no proporciona ejemplos (imágenes) que puedan ayudar a guiarla. LLMDebe utilizar sus conocimientos previamente entrenados para realizar la tarea. La eficacia de las indicaciones rápidas depende de la complejidad de la tarea y de la calidad de las mismas. Consulte también las indicaciones de pocos pasos.

aplicación zombi

Una aplicación que tiene un uso medio CPU de memoria inferior al 5 por ciento. En un proyecto de migración, es habitual retirar estas aplicaciones.

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