Alcanzar la madurez de Essential Eight el AWS

AWS Orientación prescriptiva

AWS Orientación prescriptiva: Alcanzar la madurez de Essential Eight el AWS

Table of Contents

Alcanzar la madurez de Essential Eight sobre AWS: seguridad y cumplimiento para las organizaciones australianas

Amazon Web Services (colaboradores)

Noviembre de 2024 (historial de documentos)

La Dirección de Señales de Australia (ASD) creó y priorizó las estrategias para ayudar a las organizaciones a mitigar los riesgos de las amenazas a la ciberseguridad. Se eligieron ocho de estas estrategias para formar el marco de Essential Eight. Muchas organizaciones de los sectores público y privado de Australia deben alcanzar la madurez en el marco de Essential Eight.

El Centro Australiano de Ciberseguridad (ACSC) creó el marco de Essential Eight para ayudar a proteger las redes conectadas a internet basadas en Microsoft. Sin embargo, muchas organizaciones deben alcanzar la madurez de Essential Eight en todos sus entornos, en las instalaciones y en la nube.

El marco de Essential Eight también incluye un modelo de madurez diseñado para ayudar a las organizaciones a implementar el marco a través de una iteración progresiva. El modelo describe los niveles de madurez de cero a tres. El nivel de madurez tres representa la resiliencia frente a las tácticas de ciberseguridad avanzadas y los ataques altamente dirigidos. Esta guía proporciona una guía específica y fundamentada que le ayudará a alcanzar el tercer nivel de madurez de Essential Eight. AWS

Seguridad y cumplimiento para las organizaciones australianas

Muchas organizaciones en Australia lo utilizan Nube de AWS para almacenar datos confidenciales, procesar transacciones confidenciales y crear servicios críticos.

Si bien en esta guía se explica cómo adaptar el marco de Essential Eight a la nube, AWS también proporciona las certificaciones y modelos siguientes que son útiles para satisfacer los requisitos de seguridad y cumplimiento de su organización:

- Programa de Evaluadores Registrados de Seguridad de la Información
- Marco de certificación de alojamiento
- AWS modelo de responsabilidad compartida
- AWS Marco Well-Architected

Programa de Evaluadores Registrados de Seguridad de la Información

Servicios de AWS han sido evaluadas en el marco del Programa de Evaluadores Registrados de Seguridad de la Información (IRAP) del Centro Australiano de Ciberseguridad (ACSC) en el nivel de PROTECCIÓN. Un evaluador IRAP independiente certificado por la Dirección de Señales de Australia (ASD) completó la evaluación IRAP de. AWS Esta evaluación garantiza que, con respecto a los AWS productos y servicios, se implementan los controles aplicables para las cargas de trabajo de nivel PROTEGIDO.

El paquete AWS IRAP PROTECTED está disponible en. AWS Artifact El informe del IRAP se desarrolló mediante la guía de seguridad en la nube del ACSC (sitio web del ACSC). Para una lista completa de los Servicios de AWS incluidos, consulte Servicios de AWS in scope: IRAP.

Marco de certificación de alojamiento

El marco de certificación de alojamiento australiano se desarrolló para facilitar la administración segura de los sistemas y datos gubernamentales. Este marco está destinado a ayudar a las organizaciones a mitigar los riesgos de propiedad de la cadena de suministro y los centros de datos. AWS recibió la certificación de nivel estratégico certificado. Esto ayuda a las agencias

gubernamentales a seguir innovando a un ritmo rápido, sabiendo que AWS cumplen con los requisitos gubernamentales.

AWS modelo de responsabilidad compartida

El modelo de responsabilidad AWS compartida define cómo se comparte la responsabilidad en materia de seguridad y cumplimiento en la nube. AWS AWS protege la infraestructura en la que se ejecutan todos los servicios que se ofrecen en ella Nube de AWS, y usted es responsable de proteger el uso de esos servicios, como sus datos y aplicaciones.

Este modelo compartido puede ayudar a liberar la carga operativa, porque AWS opera, administra y controla muchos componentes, desde el sistema operativo host y la capa de virtualización hasta la seguridad física en las instalaciones en las que opera el servicio. Asume la responsabilidad de administrar el sistema operativo invitado (que incluye las actualizaciones y las revisiones de seguridad) y cualquier otro software de aplicaciones asociadas. También asume la responsabilidad de configurar el firewall del grupo de seguridad que proporciona AWS .

Es fundamental que comprenda el modelo de responsabilidad AWS compartida cuando se acerque a la madurez de Essential Eight. AWS Sus responsabilidades variarán según los servicios que se utilicen, la integración de estos con el entorno de TI y las leyes y normativas aplicables.

AWS Marco Well-Architected

AWS WellArchitected ayuda a los arquitectos de la nube a crear una infraestructura segura, de alto rendimiento, resiliente y eficiente para una variedad de aplicaciones y cargas de trabajo. El AWS Well-Architected Framework proporciona las mejores prácticas de arquitectura que le ayudan a diseñar, construir y operar sistemas en ellos. AWS Este marco consta de seis pilares: excelencia operativa, seguridad, fiabilidad, eficacia del rendimiento, optimización de costos y sostenibilidad.

AWS también proporciona un servicio para revisar sus cargas de trabajo. Le AWS Well-Architected Toolayuda a revisar y evaluar su arquitectura mediante el AWS Well-Architected Framework. Proporciona recomendaciones para que las cargas de trabajo sean más fiables, seguras, eficientes y rentables.

Reinterpretación de las estrategias de Essential Eight para la nube

Las siguientes son las estrategias de mitigación originales de Essential Eight que se diseñaron para redes basadas en Microsoft conectadas a internet:

- Control de aplicaciones
- Revisiones para las aplicaciones
- Configuración de los valores de macros de Microsoft Office
- Endurecimiento de las aplicaciones de usuario
- Restricción de los privilegios administrativos
- Aplicación de revisiones a sistemas operativos
- Autenticación multifactor
- Copias de seguridad periódicas

Es importante reiterar que el marco de Essential Eight no está diseñado para entornos en la nube. Sin embargo, los principios subyacentes son aplicables y existe una superposición entre las ocho estrategias esenciales y las mejores prácticas del AWS Well-Architected Framework.

Varios enfoques nativos en la nube pueden mejorar la seguridad y reducir de manera drástica la carga de cumplimiento. En los entornos en las instalaciones, es responsable de todos los aspectos de la seguridad y no hay controles heredados. Al ejecutar cargas de trabajo en la nube, AWS es responsable de proteger la infraestructura en la que se ejecutan nuestros servicios. También puede reducir la carga de cumplimiento mediante el uso de servicios administrados y de automatización. Los servicios gestionados, también conocidos como servicios abstractos, son aquellos en Servicios de AWS los que se AWS opera la capa de infraestructura, el sistema operativo y las plataformas, y se accede a los puntos finales para almacenar y recuperar datos. Amazon Simple Storage Service (Amazon S3) y Amazon DynamoDB son ejemplos de servicios administrados. Para más información, consulte la sección Tema 1: uso de servicios administrados de esta guía.

Por lo tanto, es necesario hacer una reinterpretación para que las estrategias Essential Eight sean adecuadas para las cargas de trabajo en AWS. Esta guía convierte las ocho estrategias esenciales en AWS temas.

Uso de los temas

Esta guía se divide en ocho temas. Cada estrategia de Essential Eight se asigna a uno o más de los siguientes temas, y cada tema se asigna a una o más prácticas recomendadas del Well-Architected Framework AWS :

- Tema 1: uso de servicios administrados
- Tema 2: gestión de la infraestructura inmutable mediante canalizaciones seguras
- Tema 3: administración de la infraestructura mutable con automatización
- Tema 4: administración de identidades
- Tema 5: establecimiento de un perímetro de datos
- Tema 6: automatización de las copias de seguridad
- Tema 7: centralización del registro y de la supervisión
- Tema 8: implementación de mecanismos para los procesos manuales

Cada tema incluye una descripción general del tema, las mejores prácticas relacionadas con el AWS Well-Architected Framework e instrucciones sobre cómo alcanzar la madurez de Essential Eight y monitorear el cumplimiento. Las instrucciones proporcionan pasos manuales o son útiles para configurar las automatizaciones mediante reglas de AWS Config Los pasos manuales requieren mecanismos para garantizar que se aborden los resultados. Para obtener más información, consulte. Tema 8: implementación de mecanismos para los procesos manuales AWS Config las reglas requieren una supervisión o automatización similar para corregir los recursos que no cumplen con las normas. Si sigue las directrices relacionadas con estos temas, podrá alcanzar la madurez de Essential Eight con un enfoque que también maximice las ventajas de la nube.

Reinterpretación de las estrategias de Essential Eight para la nube

Como el marco de Essential Eight no está diseñado para entornos en la nube, es esencial adoptar un enfoque nativo en la nube al abordar los principios subyacentes de cada estrategia de Essential Eight. El enfoque varía según dos cuestiones clave.

¿Qué servicios utiliza?

El AWS modelo de responsabilidad compartida puede ayudar a aliviar sus cargas operativas y de cumplimiento. Los servicios gestionados transfieren una mayor AWS responsabilidad a la hora de mantener la disponibilidad, el rendimiento y la optimización de la seguridad del servicio

implementado. Los servicios administrados también eliminan la carga operativa y administrativa del mantenimiento de un servicio, lo que proporciona al equipo más tiempo para centrarse en la innovación.

Los servicios administrados incluyen servicios sin servidor, como Amazon API Gateway, AWS Lambda y DynamoDB. Una base de datos en Amazon Relational Database Service (Amazon RDS) requiere menos responsabilidad operativa que una base de datos en Amazon Elastic Compute Cloud (Amazon EC2).

Por ejemplo, si va a adaptar la estrategia Essential Eight de los sistemas operativos Patch a la nube, debe tener en cuenta qué servicios utiliza y si es responsable de aplicar parches a esos recursos. AWS es responsable de aplicar parches a los servicios totalmente gestionados, como Lambda y DynamoDB. Para otros servicios, como Amazon RDS o Amazon Redshift, es posible que deba gestionar las revisiones durante los periodos de mantenimiento.

¿Qué modelo de implementación utiliza?

¿Su organización utiliza un enfoque de infraestructura mutable o inmutable?

El modelo de infraestructura mutable actualiza y modifica la infraestructura actual para las cargas de trabajo de producción. Este era el método de implementación estándar antes de la nube, cuando reemplazar la infraestructura del servidor era tan costoso y tardaba tanto tiempo que el enfoque más práctico consistía en aplicar los cambios a los servidores que ya se encontraban en producción. Un ejemplo de enfoque mutable en la nube es la implementación de los cambios en las aplicaciones directamente en las instancias de EC2 en ejecución, ya sea de manera manual o mediante un servicio de implementación de software, como AWS Systems Manager Run Command o AWS CodeDeploy.

El modelo de infraestructura inmutable implementa una nueva infraestructura para las cargas de trabajo de producción en lugar de actualizar, aplicar revisiones o modificar la infraestructura existente. Un ejemplo de enfoque inmutable es definir una pila de aplicaciones en AWS CloudFormation o AWS Cloud Development Kit (AWS CDK). Puede utilizar estos servicios para implementar una pila de aplicaciones mediante las canalizaciones de integración continua y entrega continua (CI/CD). Este enfoque utiliza métodos de implementación como el continuo o el azul/verde. Para más información sobre este enfoque, consulte las práctica recomendada Implementación mediante una infraestructura inmutable en el Marco de AWS Well-Architected.

Por ejemplo, si va a adaptar la estrategia Essential Eight de aplicación de revisiones a sistemas operativos a la nube, debe tener en cuenta cómo se aplican las revisiones al modelo de

implementación. En el caso de una infraestructura mutable, puede aplicar revisiones a los recursos de manera manual o mejorar la eficiencia operativa mediante la automatización. Si utiliza una infraestructura inmutable, utilizaría una CI/CD canalización para implementar una nueva infraestructura con la versión más reciente del sistema operativo. De hecho, el término aplicar revisión es un término inadecuado en este modelo porque la infraestructura se reemplazaría en lugar de aplicarse una revisión.

Tema 1: uso de servicios administrados

Estrategias de Essential Eight que se abarcan

Aplique revisiones a las aplicaciones, restrinja los privilegios administrativos, aplique revisiones a los sistemas operativos

Los servicios gestionados le ayudan a reducir sus obligaciones de conformidad AWS al permitirle gestionar algunas tareas de seguridad, como la aplicación de parches y la gestión de vulnerabilidades.

Como se explica en la AWS modelo de responsabilidad compartida sección, usted comparte la responsabilidad de la seguridad y AWS el cumplimiento de la nube. Esto puede reducir la carga operativa, ya AWS que opera, gestiona y controla los componentes, desde el sistema operativo anfitrión y la capa de virtualización hasta la seguridad física de las instalaciones en las que opera el servicio.

Sus responsabilidades pueden incluir la gestión de los períodos de mantenimiento de los servicios gestionados, como Amazon Relational Database Service (Amazon RDS) o Amazon Redshift, y la búsqueda de vulnerabilidades AWS Lambda en el código o las imágenes de los contenedores. Como sucede con todos los temas de esta guía, también es responsable de la supervisión y la generación de informes de cumplimiento. Puede utilizar Amazon Inspector para informar sobre las vulnerabilidades en todas sus Cuentas de AWS. Puede utilizar las reglas AWS Config para asegurarse de que los servicios, como Amazon RDS y Amazon Redshift, tengan habilitadas las actualizaciones menores y los períodos de mantenimiento.

Por ejemplo, si ejecuta una instancia de Amazon EC2, entre sus responsabilidades se incluyen las siguientes:

- Control de aplicaciones
- Aplicación de revisiones a las aplicaciones
- Restricción de los privilegios administrativos al plano de control de Amazon EC2 y al sistema operativo (OS)
- Aplicación de revisiones al sistema operativo
- Aplicación de la autenticación multifactor (MFA) para acceder al plano de AWS control y al sistema operativo

- Copias de seguridad de los datos y de la configuración

Mientras que si ejecuta una función de Lambda, sus responsabilidades se reducen e incluyen lo siguiente:

- Control de aplicaciones
- Confirmando que las bibliotecas son up-to-date
- Restricción de los privilegios administrativos al plano de control de Lambda
- Hacer que la MFA acceda al plano de control AWS
- Copias de seguridad del código y de la configuración de la función de Lambda

Mejores prácticas relacionadas en el AWS Well-Architected Framework

- SEC01- BP05 Reducir el alcance de la gestión de la seguridad

Implementación de este tema

Habilitación de la aplicación de revisiones

- Aplique las actualizaciones de Amazon RDS
- Habilite las actualizaciones gestionadas en AWS Elastic Beanstalk
- Tenga en cuenta los periodos de mantenimiento de clústeres de Amazon Redshift

Escaneo para detectar vulnerabilidades

- Escanee imágenes de contenedores de Amazon Elastic Container Registry (Amazon ECR) con Amazon Inspector
- Escanee funciones de Lambda con Amazon Inspector

Supervisión de este tema

Implementación de controles de gobernanza

- Habilite el paquete de mejores prácticas operativas para la conformidad con el ACSC Essential 8 AWS Config

Supervisión de Amazon Inspector

- Evaluación de la cobertura a nivel de cuenta
- Administración de varias cuentas

Implemente las siguientes reglas AWS Config

- `RDS_AUTOMATIC_MINOR_VERSION_UPGRADE_ENABLED`
- `ELASTIC_BEANSTALK_MANAGED_UPDATES_ENABLED`
- `REDSHIFT_CLUSTER_MAINTENANCESETTINGS_CHECK`
- `EC2_MANAGEDINSTANCE_PATCH_COMPLIANCE_STATUS_CHECK`
- `EKS_CLUSTER_SUPPORTED_VERSION`

Tema 2: gestión de la infraestructura inmutable mediante canalizaciones seguras

> Estrategias de Essential Eight que se abarcan
>
> Control de aplicaciones, revisiones para las aplicaciones, revisiones para los sistemas operativos

Para una infraestructura inmutable, debe proteger los canales de despliegue para los cambios en el sistema. AWS El distinguido ingeniero Colm Maccárthaigh explicó este principio en la presentación (YouTubevídeo) de operaciones sin privilegios: ejecución de servicios sin acceso a los datos en la conferencia re:Invent de 2022. AWS

Al restringir el acceso directo para configurar AWS los recursos, puede exigir que todos los recursos se desplieguen o modifiquen mediante procesos aprobados, seguros y automatizados. Por lo general, se crean políticas de AWS Identity and Access Management (IAM) que permiten a los usuarios acceder solo a la cuenta que aloja la canalización de la implementación. También se configuran las políticas de IAM que permiten el acceso de emergencia a un número limitado de usuarios. Para evitar cambios manuales, puede utilizar los grupos de seguridad para bloquear el acceso a los servidores mediante SSH y el protocolo de escritorio remoto (RDP) de Windows. El administrador de sesiones, una capacidad de AWS Systems Manager, puede proporcionar acceso a las instancias sin necesidad de abrir puertos de entrada ni mantener los hosts bastiones.

Las imágenes de máquina de Amazon (AMI) y las imágenes de contenedor se deben crear de manera segura y repetible. En el caso de las instancias de Amazon EC2, puede utilizar EC2 Image Builder para AMIs compilarlas con funciones de seguridad integradas, como la detección de instancias, el control de aplicaciones y el registro. Para más información acerca del control de aplicaciones, consulte Implementing Application Control en el sitio web de ACSC. También puede utilizar el Generador de imágenes para crear imágenes de contenedores y puede utilizar Amazon Elastic Container Registry (Amazon ECR) para compartirlas entre cuentas. Un equipo de seguridad central puede aprobar el proceso automatizado para crear estas imágenes AMIs y las de contenedores, de modo que cualquier AMI o imagen de contenedor resultante esté aprobada para su uso por parte de los equipos de aplicaciones.

Las aplicaciones deben definirse en la infraestructura como código (IaC), mediante el uso de servicios como AWS CloudFormation o AWS Cloud Development Kit (AWS CDK). Las herramientas

de análisis de código AWS CloudFormation Guard, como cfn-nag o cdk-nag, pueden comparar automáticamente el código con las mejores prácticas de seguridad aprobadas.

Al igual que con Tema 1: uso de servicios administrados, Amazon Inspector puede informar sobre las vulnerabilidades en sus Cuentas de AWS. Los equipos centralizados de la nube y seguridad pueden utilizar esta información para verificar que el equipo de aplicaciones satisface los requisitos de seguridad y cumplimiento normativo.

Para supervisar el cumplimiento e informar al respecto, haga revisiones continuas de los recursos y registros de IAM. Utilice AWS Config reglas para asegurarse de que solo se AMIs utilizan los aprobados y asegúrese de que Amazon Inspector esté configurado para analizar los recursos de Amazon ECR en busca de vulnerabilidades.

Mejores prácticas relacionadas en el AWS Well-Architected Framework

- OPS05- BP04 Utilice sistemas de gestión de construcción e implementación
- REL08- BP04 Implemente utilizando una infraestructura inmutable
- SEC06- BP03 Reduzca la gestión manual y el acceso interactivo

Implementación de este tema

Implementación de canalizaciones de creación de contenedores y AMI

- Utilice EC2 Image Builder e incorpore lo siguiente a su AMIs:
  - AWS Systems Manager Agente (SSM Agent), que se utiliza para la detección y administración de instancias
  - Herramientas de seguridad para el control de aplicaciones, como Security Enhanced Linux (SELinux) (GitHub), File Access Policy Daemon (fapolicyd) (GitHub) u OpenSCAP
  - Amazon CloudWatch Agent, que se utiliza para registrar
- En el caso de todas las instancias de EC2, incluya las políticas `CloudWatchAgentServerPolicy` y `AmazonSSMManagedInstanceCore` en el perfil de instancia o en el rol de IAM que utiliza System Manager para acceder a la instancia
- Comparte AMIs con toda la organización
- Comparta los recursos de EC2 Image Builder

- Asegúrese de que los equipos de aplicaciones consulten las últimas AMIs
- Utilice la canalización de AMI para la administración de revisiones
- Implemente canalizaciones de creación de contenedores:
  - Cree una canalización de imágenes de contenedores mediante el asistente de consola EC2 Image Builder
  - Cree un canal de entrega continua para las imágenes de sus contenedores utilizando Amazon ECR como fuente (entrada del AWS blog)
- Comparta las imágenes de contenedores de ECR en su organización a través de arquitecturas con varias cuentas y varias regiones

Implementación de canalizaciones seguras para la creación de aplicaciones

- Implemente procesos de compilación para IaC, por ejemplo, mediante EC2 Image Builder y AWS CodePipeline (entrada de blog)AWS
- Utilice herramientas de análisis de código AWS CloudFormation Guard, como cfn-nag (GitHub) o cdk-nag (GitHub), en las CI/CD canalizaciones para ayudar a detectar infracciones de las mejores prácticas, como:
  - Políticas de IAM demasiado permisivas, como las que utilizan caracteres comodines
  - Reglas de grupos de seguridad que son demasiado permisivas, como las que utilizan caracteres comodines o permiten el acceso por SSH
  - Registros de acceso que no están habilitados
  - Cifrado que no está habilitado
  - Literales de contraseñas
- Implemente herramientas de escaneo en las canalizaciones (entrada del blog)AWS
- Úselo AWS Identity and Access Management Access Analyzer en canalizaciones (AWS entrada de blog) para validar las políticas de IAM definidas en las plantillas CloudFormation
- Configure las políticas de IAM y las políticas de control de servicios para que el acceso con privilegios mínimos pueda utilizar la canalización o hacer modificaciones en la misma

Implementación del escaneo de vulnerabilidades

- Habilite Amazon Inspector en todas las cuentas de su organización
- Utilice Amazon Inspector para escanear AMIs su proceso de creación de AMI:

  - Gestione el ciclo de vida de las AMI en EC2 Image Builder GitHub ()
- Configure los escaneos mejorados para los repositorios de Amazon ECR mediante Amazon Inspector
- Cree un programa de administración de vulnerabilidades para clasificar y corregir los resultados de seguridad

Supervisión de este tema

Supervisión de IAM y registros de manera continua

- Revise periódicamente las políticas de IAM para asegurarse de que:
  - Solo las canalizaciones de implementación tengan acceso directo a los recursos
  - Solo los servicios aprobados tengan acceso directo a los datos
  - Los usuarios no tengan acceso directo a los recursos o datos
- Supervise AWS CloudTrail los registros para confirmar que los usuarios modifican los recursos a través de canalizaciones y no los modifican directamente ni acceden a los datos
- Revise de manera periódica los resultados del Analizador de acceso de IAM
- Configure una alerta para que le notifique si se utilizan las credenciales del usuario raíz de una Cuenta de AWS

Implemente las siguientes reglas AWS Config

- `APPROVED_AMIS_BY_ID`
- `APPROVED_AMIS_BY_TAG`
- `ECR_PRIVATE_IMAGE_SCANNING_ENABLED`

Tema 3: administración de la infraestructura mutable con automatización

Estrategias de Essential Eight que se abarcan

Control de aplicaciones, revisiones para las aplicaciones, revisiones para los sistemas operativos

Al igual que la infraestructura inmutable, administra la infraestructura mutable como IaC y modifica o actualiza esta infraestructura a través de procesos automatizados. Muchos de los pasos de implementación de la infraestructura inmutable también se aplican a la infraestructura mutable. Sin embargo, en el caso de una infraestructura mutable, también debe implementar controles manuales para asegurarse de que las cargas de trabajo modificadas aún sigan las prácticas recomendadas.

Para una infraestructura mutable, puede automatizar la administración de parches mediante el Administrador de parches, una capacidad de AWS Systems Manager. Habilite el Administrador de parches en todas las cuentas de su organización de AWS .

Evite el acceso directo por SSH y RDP y exija a los usuarios que utilicen el Administrador de sesiones o Run Command, que también son funcionalidades de Systems Manager. A diferencia de SSH y RDP, estas funcionalidades pueden registrar los cambios y el acceso al sistema.

Para supervisar el cumplimiento e informar al respecto, debe hacer evaluaciones continuas del cumplimiento de la aplicación de las revisiones. Puede utilizar AWS Config reglas para asegurarse de que todas las instancias de Amazon EC2 estén gestionadas por Systems Manager, tengan los permisos necesarios y las aplicaciones instaladas y cumplan con los parches.

Mejores prácticas relacionadas en el AWS Well-Architected Framework

- SEC06- BP03 Reduzca la gestión manual y el acceso interactivo
- SEC06- BP05 Automatice la protección informática

Implementación de este tema

Automatización de la aplicación de revisiones

- Implemente los pasos sobre cómo habilitar el Administrador de parches en todas las cuentas de su organización de AWS
- En el caso de todas las instancias de EC2, incluya `CloudWatchAgentServerPolicy` y `AmazonSSMManagedInstanceCore` en el perfil de instancia o rol de IAM que utiliza System Manager para acceder a la instancia

Uso de la automatización en lugar de los procesos manuales

- Implemente las directrices de Implement AMI and container build pipelines en Tema 2: gestión de la infraestructura inmutable mediante canalizaciones seguras
- Utilice Administrador de sesiones o Run Command en lugar del acceso directo por SSH o RDP

Uso de la automatización para instalar lo siguiente en las instancias de EC2

- AWS Systems Manager Agente (SSM Agent), que se utiliza para la detección y la administración de instancias
- Herramientas de seguridad para el control de aplicaciones, como Security Enhanced Linux (SELinux) (GitHub), File Access Policy Daemon (fapolicyd) (GitHub) u OpenSCAP
- Amazon CloudWatch Agent, que se utiliza para el registro

Uso de la revisión entre compañeros antes de los lanzamientos para garantizar que los cambios cumplen con las prácticas recomendadas

- Políticas de IAM demasiado permisivas, como las que utilizan caracteres comodines
- Reglas de grupos de seguridad que son demasiado permisivas, como las que utilizan caracteres comodines o permiten el acceso por SSH
- Registros de acceso que no están habilitados
- Cifrado que no está habilitado
- Literales de contraseñas

- Políticas de IAM seguras

Uso de controles de identidad

- Para exigir que los usuarios modifiquen los recursos a través de procesos automatizados y evitar la configuración manual, conceda permisos de solo lectura a los roles que pueden asumir los usuarios.
- Conceda permisos para modificar los recursos solo a los roles de servicio, como el rol que utiliza Systems Manager

Implementación del escaneo de vulnerabilidades

- Implemente las directrices de Implementación del escaneo de vulnerabilidades en Tema 2: gestión de la infraestructura inmutable mediante canalizaciones seguras
- Escanee las instancias de EC2 con Amazon Inspector

Supervisión de este tema

Supervisión del cumplimiento de las revisiones de manera continua

- Informe sobre el cumplimiento de las revisiones mediante la automatización y los paneles
- Implemente un mecanismo para revisar los paneles de control para comprobar el cumplimiento de las revisiones

Supervisión de IAM y registros de manera continua

- Revise periódicamente las políticas de IAM para asegurarse de que:
  - Solo las canalizaciones de implementación tengan acceso directo a los recursos
  - Solo los servicios aprobados tengan acceso directo a los datos
  - Los usuarios no tengan acceso directo a los recursos o datos
- Supervise AWS CloudTrail los registros para asegurarse de que los usuarios modifican los recursos a través de procesos y no los modifican directamente ni acceden a los datos
- Revise AWS Identity and Access Management Access Analyzer periódicamente los hallazgos

- Configure una alerta para que le notifique si se utilizan las credenciales del usuario raíz de una Cuenta de AWS

Implemente las siguientes AWS Config reglas

- `EC2_MANAGEDINSTANCE_PATCH_COMPLIANCE_STATUS_CHECK`
- `EC2_INSTANCE_MANAGED_BY_SSM`
- `EC2_MANAGEDINSTANCE_APPLICATIONS_REQUIRED - SELinux/fapolicyd/OpenSCAP, CW Agent`
- `EC2_MANAGEDINSTANCE_APPLICATIONS_BLACKLISTED - any unsupported apps`
- `IAM_ROLE_MANAGED_POLICY_CHECK - CW Logs, SSM`
- `EC2_MANAGEDINSTANCE_ASSOCIATION_COMPLIANCE_STATUS_CHECK`
- `REQUIRED_TAGS`
- `RESTRICTED_INCOMING_TRAFFIC - 22, 3389`

Tema 4: administración de identidades

Estrategias de Essential Eight que se abarcan

Restricción de los privilegios administrativos, autenticación multifactor

Una administración sólida de la identidad y los permisos es un aspecto fundamental de la administración de la seguridad en la nube. Las prácticas de identidad sólidas equilibran el acceso necesario y el privilegio mínimo. Esto ayuda a los equipos de desarrollo a avanzar de manera rápida sin comprometer la seguridad.

Utilice la federación de identidades para centralizar la administración de las identidades. De este modo se facilita la administración del acceso en varias aplicaciones y servicios porque administra el acceso desde un único lugar. También le será útil para implementar permisos temporales y autenticación multifactor (MFA).

Conceda a los usuarios solo los permisos que necesitan para hacer sus tareas. AWS Identity and Access Management Access Analyzer puede validar las políticas y verificar el acceso público y el acceso entre cuentas. Características como las políticas de control de AWS Organizations servicios (SCPs), las condiciones de las políticas de IAM, los límites de los permisos de IAM y los conjuntos de AWS IAM Identity Center permisos pueden ayudarle a configurar un control de acceso detallado (FGAC).

Al llevar a cabo cualquier tipo de autenticación, es mejor utilizar credenciales temporales para reducir o eliminar los riesgos. Por ejemplo, que las credenciales se divulguen, compartan o roben de manera inadvertida. Utilice roles de IAM en lugar de usuarios de IAM.

Utilice mecanismos de inicio de sesión sólidos, como MFA, para mitigar el riesgo en caso de que las credenciales de inicio de sesión se hayan divulgado de manera inadvertida o sean fáciles de adivinar. Exija MFA para el usuario raíz. También puede necesitarla a nivel de federación. Si el uso de usuarios de IAM es inevitable, aplique MFA.

Para supervisar el cumplimiento y generar informes al respecto, debe dedicar esfuerzos continuos a la reducción de permisos, la supervisión de los resultados del Analizador de acceso de IAM y la eliminación de recursos de IAM que no se utilicen. Utilice AWS Config reglas para asegurarse de que se apliquen mecanismos de inicio de sesión sólidos, que las credenciales sean efímeras y que se utilicen los recursos de IAM.

Mejores prácticas relacionadas en el AWS Well-Architected Framework

- SEC02- BP01 Utilice mecanismos de inicio de sesión sólidos
- SEC02- BP02 Usa credenciales temporales
- SEC02- BP03 Almacene y use los secretos de forma segura
- SEC02- BP04 Confíe en un proveedor de identidad centralizado
- SEC02- BP05 Audite y modifique las credenciales periódicamente
- SEC02- BP06 Emplee grupos y atributos de usuarios
- SEC03- BP01 Definir los requisitos de acceso
- SEC03- BP02 Otorgue el acceso con privilegios mínimos
- SEC03- BP03 Establecer un proceso de acceso de emergencia
- SEC03- BP04 Reduzca los permisos de forma continua
- SEC03- BP05 Defina barreras de permisos para su organización
- SEC03- BP06 Gestione el acceso en función del ciclo de vida
- SEC03- BP07 Analice el acceso público y entre cuentas
- SEC03- BP08 Comparta los recursos de forma segura dentro de su organización

Implementación de este tema

Implementación de la federación de identidades

- Exija a los usuarios humanos que se federen con un proveedor de identidad para acceder a AWS mediante credenciales temporales
- Implemente un acceso elevado temporal a los entornos de AWS

Aplicación de permisos de privilegio mínimo

- Proteja sus credenciales de usuario raíz y no las utilice para las tareas diarias
- Utilice IAM Access Analyzer para generar políticas de privilegios mínimos en función de la actividad de acceso
- Verifique el acceso público y multicuenta a los recursos con IAM Access Analyzer

- Utilice IAM Access Analyzer para validar las políticas de IAM con objeto de garantizar la seguridad y funcionalidad de los permisos
- Establezca barreras de protección de permisos en varias cuentas
- Utilice los límites de permisos para establecer los permisos máximos que puede conceder una política basada en identidades
- Utilice las condiciones de las políticas de IAM para restringir aún más el acceso
- Revise y elimine periódicamente los usuarios, funciones, permisos, políticas y credenciales que no utilice
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos
- Utilice la característica de conjuntos de permisos de IAM Identity Center

Rotación de las credenciales

- Exija que las cargas de trabajo utilicen las funciones de IAM para acceder AWS
- Automatice la eliminación de los roles de IAM no utilizados
- Cambie las claves de acceso con regularidad para los casos de uso que requieran credenciales a largo plazo

Aplicación de la MFA

- Exija la MFA para el usuario raíz
- Exija la MFA a través de IAM Identity Center
- Considere la posibilidad de exigir la MFA para las acciones de API específicas del servicio

Supervisión de este tema

Supervisión del acceso con privilegio mínimo

- Envíe las conclusiones del IAM Access Analyzer a AWS Security Hub CSPM
- Considere la posibilidad de configurar las notificaciones para los resultados críticos de IAM Identity Center
- Revise periódicamente los informes de credenciales de su Cuentas de AWS

Implemente las siguientes reglas AWS Config

- ACCESS_KEYS_ROTATED
- IAM_ROOT_ACCESS_KEY_CHECK
- IAM_USER_MFA_ENABLED
- IAM_USER_UNUSED_CREDENTIALS_CHECK
- IAM_PASSWORD_POLICY
- ROOT_ACCOUNT_HARDWARE_MFA_ENABLED

Tema 5: establecimiento de un perímetro de datos

Estrategias de Essential Eight que se abarcan

Restricción de los privilegios administrativos

Un perímetro de datos es un conjunto de barreras de protección en el entorno de AWS que ayudan a garantizar que solo las identidades de confianza accedan a los recursos de confianza desde las redes previstas. Estas barreras sirven como límites permanentes que ayudan a proteger sus datos en un amplio conjunto de recursos. Cuentas de AWS Estas barreras de protección para toda la organización no sustituyen a los estrictos controles de acceso existentes. Por el contrario, ayudan a mejorar la estrategia de seguridad al garantizar que todos los usuarios, funciones y recursos AWS Identity and Access Management (de IAM) cumplan con un conjunto de normas de seguridad definidas.

Puede establecer un perímetro de datos mediante políticas que impidan el acceso desde fuera de los límites de una organización, que por lo general se crean en AWS Organizations. Las tres condiciones principales de autorización perimetral que se utilizan para establecer un perímetro de datos son las siguientes:

- Identidades confiables: personas principales (funciones o usuarios de IAM) que actúan en su Cuentas de AWS nombre o que Servicios de AWS actúan en su nombre.
- Recursos confiables: recursos que están en su poder Cuentas de AWS o que se administran Servicios de AWS actuando en su nombre.
- Redes esperadas: sus centros de datos locales y sus nubes privadas virtuales (VPCs), o las redes que Servicios de AWS actúan en su nombre.

Considere la posibilidad de implementar perímetros de datos entre entornos de distintas clasificaciones de datos, como `OFFICIAL:SENSITIVE` o `PROTECTED` con distintos niveles de riesgo, como desarrollo, pruebas o producción. Para obtener más información, consulte Creación de un perímetro de datos en AWS (AWS documento técnico) y Establecimiento de un perímetro de datos en AWS: descripción general (AWS entrada del blog).

Mejores prácticas relacionadas en el AWS Well-Architected Framework

- SEC03- BP05 Defina las barreras de permisos para su organización
- SEC07- BP02 Aplique controles de protección de datos en función de la confidencialidad de los datos

Implementación de este tema

Implementación de controles de identidad

- Permita que solo las identidades confiables accedan a sus recursos: utilice políticas basadas en recursos con las claves de condición `aws:PrincipalOrgID` y `aws:PrincipalIsAWSService`. Esto permite que solo los directores de su AWS organización y origen accedan AWS a sus recursos.
- Permita identidades confiables solo de su red: utiliza las políticas de puntos de conexión de VPC con las claves de condición `aws:PrincipalOrgID` y `aws:PrincipalIsAWSService`. Esto permite que solo los directores de su AWS organización y desde accedan AWS a los servicios a través de los puntos de enlace de la VPC.

Implementación de controles de los recursos

- Permita que sus identidades accedan solo a recursos confiables: utilice las políticas de control de servicios (SCPs) con la clave de condición. `aws:ResourceOrgID` Esto permite que sus identidades accedan solo a los recursos de su AWS organización.
- Permita el acceso a los recursos de confianza solo desde su red: utilice políticas de puntos de conexión de VPC con la clave de condición `aws:ResourceOrgID`. Esto permite que las identidades accedan a los servicios solo a través de los puntos de conexión de VPC que forman parte de su organización de AWS .

Implementación de los controles de red

- Permita que las identidades accedan a los recursos solo desde las redes esperadas: utilícelas SCPs con las claves de condición `aws:SourceIp` `aws:SourceVpcaws:SourceVpce`,,

y`aws:ViaAWSService`. Esto permite que sus identidades accedan a los recursos solo desde las direcciones IP esperadas y los puntos finales de VPC, y desde allí. VPCs Servicios de AWS

- Permita el acceso a los recursos solo desde las redes previstas: utilice las políticas basadas en recursos con las claves de condición `aws:SourceIp`, `aws:SourceVpc`, `aws:SourceVpce`, `aws:ViaAWSService` y `aws:PrincipalIsAWSService`. Esto permite el acceso a sus recursos solo desde los puntos de enlace de VPC IPs esperados VPCs, esperados o esperados Servicios de AWS, hasta o cuando la identidad de llamada sea una. Servicio de AWS

Supervisión de este tema

Supervisión de políticas

- Implemente mecanismos de revisión SCPs, políticas de IAM y políticas de puntos finales de VPC

Implemente las siguientes reglas AWS Config

- `SERVICE_VPC_ENDPOINT_ENABLED`

Tema 6: automatización de las copias de seguridad

Estrategias de Essential Eight que se abarcan

Copias de seguridad periódicas

“Los errores son un hecho y, con el tiempo, todo tendrá errores: desde los enrutadores hasta los discos duros, desde los sistemas operativos hasta las unidades de memoria que dañan los paquetes TCP, desde los errores transitorios hasta los errores permanentes. Esto es un hecho, ya sea que utilice hardware de la más alta calidad o los componentes más económicos”. —Werner Vogels, director de tecnología de Amazon, All Things Distributed

El respaldo y la recuperación de datos son una parte fundamental de la confiabilidad de un sistema. AWS está diseñado para facilitar la creación de copias de seguridad, mantener la durabilidad de los datos respaldados y garantizar que los datos respaldados sigan siendo recuperables.

AWS Backup es un servicio de copia de seguridad totalmente administrado que centraliza y automatiza las copias de seguridad de datos en Servicios de AWS. Es compatible con varios tipos de AWS recursos y le ayuda a implementar y mantener una estrategia de respaldo para las cargas de trabajo que utilizan varios AWS recursos y que deben respaldarse de forma colectiva. AWS Backup también le ayuda a supervisar de forma colectiva una operación de copia de seguridad y restauración de varios AWS recursos.

AWS Backup El bloqueo de bóveda es una función opcional de una bóveda de respaldo y puede proporcionar seguridad y control adicionales. Cuando hay un bloqueo activo en el modo de cumplimiento y finaliza el periodo de gracia, ni el usuario ni el responsable de la cuenta o los datos ni AWS pueden modificar ni eliminar la configuración del almacén. Cada almacén puede tener implementado un bloqueo de almacén. De este modo se permite configurar una escritura única y lectura múltiple (WORM) y se garantiza el cumplimiento de los periodos de retención.

Si sigue las instrucciones de configuración actuales, AWS Backup puede proporcionar una durabilidad anual del 99,19%, también conocida como 11 nueves. Utiliza la infraestructura AWS global para replicar sus copias de seguridad en varias zonas de disponibilidad. Para obtener más información, consulte Resiliencia en AWS Backup.

AWS Backup le ayuda a automatizar la recuperación y las pruebas de los datos respaldados para verificar la integridad y los procesos de respaldo.

Mejores prácticas relacionadas en el AWS Well-Architected Framework

- SEC09- BP01 Implemente una gestión segura de claves y certificados
- SEC09- BP02 Imponga el cifrado en tránsito
- SEC09- BP03 Autenticar las comunicaciones de red

Implementación de este tema

Automatización de la copia de seguridad y la recuperación de datos

- Implemente el respaldo de datos en AWS
- Automatice el respaldo de datos a escala (AWS entrada del blog)
- Automatice la validación de la recuperación de datos con AWS Backup (entrada AWS del blog)

Implemente la gobernanza en todos sus AWS Backup resultados

- Las 10 mejores prácticas de seguridad para proteger las copias de seguridad en AWS (AWS entrada del blog)
- Utilice AWS Backup Vault Lock para mejorar la seguridad de sus almacenes de respaldo
- Utilice AWS Backup Audit Manager para auditar el cumplimiento de sus políticas de AWS Backup

Supervisión de este tema

Implemente las siguientes reglas AWS Config

- `RDS_IN_BACKUP_PLAN`
- `RDS_LAST_BACKUP_RECOVERY_POINT_CREATED`
- `RDS_RESOURCES_PROTECTED_BY_BACKUP_PLAN`
- `REDSHIFT_BACKUP_ENABLED`
- `AURORA_LAST_BACKUP_RECOVERY_POINT_CREATED`
- `AURORA_RESOURCES_PROTECTED_BY_BACKUP_PLAN`

- BACKUP_PLAN_MIN_FREQUENCY_AND_MIN_RETENTION_CHECK
- BACKUP_RECOVERY_POINT_ENCRYPTED
- BACKUP_RECOVERY_POINT_MANUAL_DELETION_DISABLED
- BACKUP_RECOVERY_POINT_MINIMUM_RETENTION_CHECK
- DB_INSTANCE_BACKUP_ENABLED
- DYNAMODB_IN_BACKUP_PLAN
- DYNAMODB_LAST_BACKUP_RECOVERY_POINT_CREATED
- DYNAMODB_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- EBS_IN_BACKUP_PLAN
- EBS_LAST_BACKUP_RECOVERY_POINT_CREATED
- EBS_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- EC2_LAST_BACKUP_RECOVERY_POINT_CREATED
- S3_LAST_BACKUP_RECOVERY_POINT_CREATED
- S3_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- STORAGEGATEWAY_LAST_BACKUP_RECOVERY_POINT_CREATED
- STORAGEGATEWAY_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- VIRTUALMACHINE_LAST_BACKUP_RECOVERY_POINT_CREATED
- VIRTUALMACHINE_RESOURCES_PROTECTED_BY_BACKUP_PLAN

Tema 7: centralización del registro y de la supervisión

Estrategias de Essential Eight que se abarcan

Control de aplicaciones, revisiones de aplicaciones, restricción de privilegios administrativos, autenticación multifactor

AWS proporciona herramientas y funciones que le permiten ver lo que sucede en su AWS entorno. Entre ellos se incluyen:

- AWS CloudTraille ayuda a supervisar sus AWS despliegues mediante la creación de un registro histórico de las llamadas a las AWS API de su cuenta, incluidas las llamadas a las API realizadas a través de las Consola de administración de AWS herramientas de línea de comandos y las de línea de comandos. AWS SDKs En el caso de los servicios compatibles CloudTrail, también puedes identificar qué usuarios y cuentas llamaron a la API del servicio, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron.
- Amazon le CloudWatch ayuda a supervisar las métricas de sus AWS recursos y las aplicaciones en las que se ejecuta AWS en tiempo real.
- Amazon CloudWatch Logs le ayuda a centralizar los registros de todos sus sistemas y aplicaciones Servicios de AWS para que pueda supervisarlos y archivarlos de forma segura.
- Amazon GuardDuty es un servicio de supervisión continua de la seguridad que analiza y procesa los registros para identificar actividades inesperadas y potencialmente no autorizadas en su AWS entorno. GuardDuty se integra con Amazon EventBridge para iniciar una respuesta automática o notificar a un humano.
- AWS Security Hub CSPMproporciona una visión completa de su estado de seguridad en AWS. También le ayuda a comparar su AWS entorno con los estándares y las mejores prácticas del sector de la seguridad.

Estas herramientas y características están diseñadas para aumentar la visibilidad y ayudar a resolver los problemas antes de que afecten de manera negativa a su entorno. Esto le es útil para mejorar la posición de seguridad de su organización en la nube y reduce el perfil de riesgo de su entorno.

Mejores prácticas relacionadas en el AWS Well-Architected Framework

- SEC04- BP01 Configurar el registro de servicios y aplicaciones
- SEC04- BP02 Capture registros, hallazgos y métricas en ubicaciones estandarizadas

Implementación de este tema

Activación del registro

- Utilice el CloudWatch agente para publicar registros a nivel de sistema en Logs CloudWatch
- Configure alertas para detectar los hallazgos GuardDuty
- Cree un registro de la organización en CloudTrail

Implementación de prácticas recomendadas de seguridad de registros

- Implemente CloudTrail las mejores prácticas de seguridad
- Úselo SCPs para evitar que los usuarios deshabiliten los servicios de seguridad (AWS entrada del blog)
- Cifre los datos de registro en los CloudWatch registros mediante AWS Key Management Service

Centralización de los registros

- Reciba CloudTrail registros de varias cuentas
- Envíe los registros a una cuenta de archivo de registros
- Centralice CloudWatch los registros de una cuenta para su auditoría y análisis (AWS entrada de blog)
- Centralice la administración de Amazon Inspector
- Cree un agregador para toda la organización en AWS Config (entrada de blog)AWS
- Centralice la gestión de Security Hub (CSPM)
- Centralice la gestión de GuardDuty
- Considere utilizar Amazon Security Lake

Supervisión de este tema

Implementación de mecanismos

- Establezca un mecanismo para revisar los resultados del registro
- Establecer un mecanismo para revisar las conclusiones del CSPM de Security Hub
- Establezca un mecanismo para responder a los hallazgos GuardDuty

Implemente las siguientes AWS Config reglas

- `CLOUDTRAIL_SECURITY_TRAIL_ENABLED`
- `GUARDDUTY_ENABLED_CENTRALIZED`
- `SECURITYHUB_ENABLED`
- `ACCOUNT_PART_OF_ORGANIZATIONS`

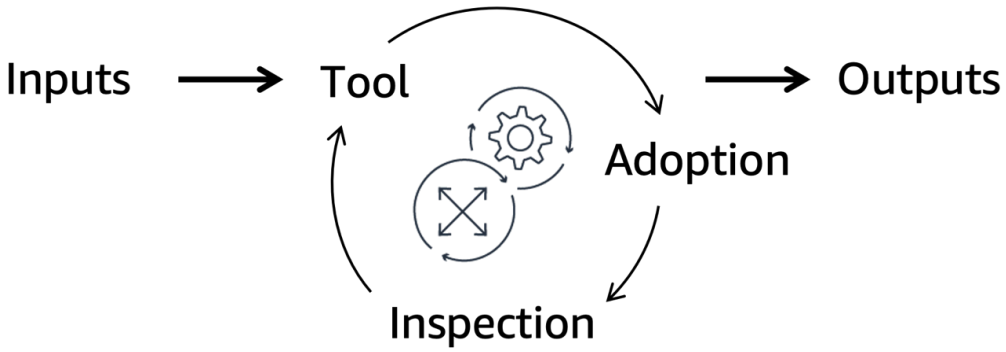
Tema 8: implementación de mecanismos para los procesos manuales

Estrategias de Essential Eight que se abarcan

Control de aplicaciones, revisiones para aplicaciones

En Amazon, tenemos un dicho: las buenas intenciones no funcionan, los mecanismos sí (entrada del AWS blog). Esto significa que hay que sustituir los mejores esfuerzos por herramientas y procesos automatizados, repetibles y escalables para lograr los resultados deseados.

Como se muestra en el diagrama siguiente, un mecanismo es un proceso completo en el que se crea una herramienta, se impulsa su adopción y, a continuación, se inspeccionan los resultados para hacer los ajustes necesarios. Se trata de un ciclo que se refuerza y mejora por sí mismo a medida que funciona. Toma entradas controlables y las transforma en salidas continuas para abordar un desafío empresarial recurrente. Para obtener más información, consulte Creación de mecanismos en el AWS Well-Architected Framework.



Mejores prácticas relacionadas en el AWS Well-Architected Framework

- OPS02- Los BP01 recursos han identificado a sus propietarios
- OPS02- BP02 Los procesos y procedimientos tienen propietarios identificados
- OPS02- BP03 Las actividades operativas han identificado a los propietarios responsables de su desempeño

- OPS02- Existen BP04 mecanismos para gestionar las responsabilidades y la propiedad
- OPS03- BP01 Proporcionar patrocinio ejecutivo
- OPS03- Se fomenta la BP03 escalada

Implementación de este tema

- Establezca mecanismos para revisar y solucionar los problemas de cumplimiento
- Establezca mecanismos para actualizar las políticas de seguridad
- Elimine las aplicaciones que no sean compatibles y, a continuación, agréguelas a la lista de negación de reglas de AWS Config
- Valide las políticas de acceso con AWS Identity and Access Management Access Analyzer
- Habilite Amazon Inspector, que guarda automáticamente los registros de vulnerabilidades up-to-date
- Por lo menos una vez al año, revise los conjuntos de reglas de control de aplicaciones.
- Considere la posibilidad de implementar la automatización, como las reglas de AWS Config, para reducir la carga de los procesos manuales
- Considere la posibilidad de utilizar Inventario de AWS Systems Manager para ver qué instancias ejecutan el software que necesita la política del software

Supervisión de este tema

- Establezca una supervisión para que los patrocinadores ejecutivos puedan hacer un seguimiento del avance hacia las metas, lo que incluye el cumplimiento, la inspección de los problemas y la evaluación de los mecanismos.

Estudio de caso indicativo para alcanzar el vencimiento de Essential Eight el AWS

En este capítulo se presenta un caso práctico indicativo para una agencia gubernamental cuyo objetivo es que Essential Eight alcance la madurez en AWS.

Secciones de este capítulo:

- Información general del escenario y de la arquitectura
- Ejemplo de carga de trabajo: lago de datos sin servidor
- Ejemplo de carga de trabajo: servicio web en contenedores
- Ejemplo de carga de trabajo: software COTS en Amazon EC2

Información general del escenario y de la arquitectura

La agencia gubernamental tiene tres cargas de trabajo en la Nube de AWS:

- Un lago de datos sin servidor que utiliza Amazon Simple Storage Service (Amazon S3) para el almacenamiento AWS Lambda y para las operaciones de extracción, transformación y carga (ETL)
- Un servicio web de contenedores que se ejecuta en Amazon Elastic Container Service (Amazon ECS) y utiliza una base de datos de Amazon Relational Database Service (Amazon RDS).
- Un software comercial off-the-shelf (COTS) que se ejecuta en Amazon EC2

Un equipo en la nube proporciona una plataforma centralizada para la organización que ejecuta los servicios principales para el AWS medio ambiente. Un equipo de nube proporciona servicios básicos para el AWS medio ambiente. Cada carga de trabajo es responsabilidad de un equipo de aplicaciones distinto, también denominado equipo de desarrolladores o equipo de entrega.

Arquitectura principal

El equipo de la nube ya estableció las funcionalidades siguientes en la Nube de AWS:

- La federación de identidades AWS IAM Identity Center se vincula a su instancia de Microsoft Entra ID (anteriormente Azure Active Directory). La federación aplica la MFA, la caducidad automática de las cuentas de usuario y el uso de credenciales de corta duración AWS Identity and Access Management a través de funciones (IAM).

- Se utiliza una canalización de AMI centralizada para aplicar revisiones a los sistemas operativos y las aplicaciones principales con el Generador de imágenes de EC2.
- Amazon Inspector puede identificar las vulnerabilidades y todos los resultados de seguridad se envían a Amazon GuardDuty para su gestión centralizada.
- Los mecanismos establecidos se utilizan para actualizar las reglas de control de las aplicaciones, responder a los eventos de ciberseguridad y revisar las vulneraciones del cumplimiento normativo.
- AWS CloudTrail se utiliza para el registro y la supervisión.
- Los eventos de seguridad, tales como el inicio de sesión del usuario raíz, inician las alertas.
- SCPs y las políticas de puntos finales de VPC establecen perímetros de datos para sus entornos. AWS
- SCPs impiden que los equipos de aplicaciones deshabiliten los servicios de seguridad y registro, como y. CloudTrail AWS Config
- AWS Config los resultados de toda la AWS organización se agrupan en uno solo Cuenta de AWS por motivos de seguridad.
- El paquete de conformidad AWS Config ACSC Essential 8 está disponible Cuentas de AWS en toda la organización.

Ejemplo de carga de trabajo: lago de datos sin servidor

Esta carga de trabajo es un ejemplo de Tema 1: uso de servicios administrados.

El lago de datos utiliza Amazon S3 para el almacenamiento y AWS Lambda para el ETL. Estos recursos se definen en una AWS Cloud Development Kit (AWS CDK) aplicación. Los cambios en el sistema se implementan mediante AWS CodePipeline. Esta canalización está restringida al equipo de aplicaciones. Cuando el equipo de aplicaciones hace una solicitud de extracción al repositorio de código, se utiliza la regla de dos personas.

En el caso de esta carga de trabajo, el equipo de aplicaciones toma las medidas siguientes para abordar las estrategias Essential Eight.

Control de aplicaciones

- El equipo de aplicaciones habilita Lambda Protection y el escaneo GuardDuty Lambda en Amazon Inspector.
- El equipo de aplicaciones implementa mecanismos para inspeccionar y administrar los resultados de Amazon Inspector.

Revisiones para las aplicaciones

- El equipo de aplicaciones habilita el escaneo de Lambda en Amazon Inspector y configura las alertas para las bibliotecas en desuso o vulnerables.
- El equipo de aplicaciones permite realizar un seguimiento AWS Config de AWS los recursos para el descubrimiento de activos.

Restricción de los privilegios administrativos

- Como se describe en la sección Arquitectura principal, el equipo de aplicaciones ya restringe el acceso a las implementaciones de producción mediante una regla de aprobación en su canalización de implementaciones.
- El equipo de aplicaciones confía en las soluciones de federación de identidades y registro centralizados que se describen en la sección Arquitectura principal.
- El equipo de la aplicación crea una AWS CloudTrail ruta y Amazon CloudWatch filtra.
- El equipo de aplicaciones configura las alertas del Amazon Simple Notification Service (Amazon SNS) CodePipeline para las implementaciones AWS CloudFormation y las eliminaciones de pilas.

Aplicación de revisiones a sistemas operativos

- El equipo de aplicaciones habilita el escaneo de Lambda en Amazon Inspector y configura las alertas para las bibliotecas en desuso o vulnerables.

Autenticación multifactor

- El equipo de aplicaciones confía en la solución de federación de identidades centralizada que se describe en la sección Arquitectura principal. Esta solución aplica la MFA, registra las autenticaciones y las alertas o responde de manera automática a los eventos de MFA sospechosos.

Copias de seguridad periódicas

- El equipo de aplicaciones almacena el código, como AWS CDK las aplicaciones y las funciones y configuraciones de Lambda, en un repositorio de código.
- El equipo de aplicaciones habilita el control de versiones y el bloqueo de objetos de Amazon S3 para evitar que se eliminen o modifiquen los objetos.

- El equipo de aplicaciones confía en la durabilidad integrada de Amazon S3 en lugar de replicar todo su conjunto de datos en otra Región de AWS.
- El equipo de aplicaciones ejecuta una copia de la carga de trabajo en otro equipo Región de AWS que cumple con sus requisitos de soberanía de datos. Utilizan las tablas globales de Amazon DynamoDB y la replicación entre regiones de Amazon S3 para replicar los datos de manera automática de la región principal a la región secundaria.

Ejemplo de carga de trabajo: servicio web en contenedores

Esta carga de trabajo es un ejemplo de Tema 2: gestión de la infraestructura inmutable mediante canalizaciones seguras.

El servicio web se ejecuta en Amazon ECS y utiliza una base de datos en Amazon RDS. El equipo de aplicaciones define estos recursos en una CloudFormation plantilla. Los contenedores se crean con el Generador de imágenes de EC2 y se almacenan en Amazon ECR. El equipo de aplicaciones implementa los cambios en el sistema mediante AWS CodePipeline. Esta canalización está restringida al equipo de aplicaciones. Cuando el equipo de aplicaciones hace una solicitud de extracción al repositorio de código, se utiliza la regla de dos personas.

En el caso de esta carga de trabajo, el equipo de aplicaciones toma las medidas siguientes para abordar las estrategias Essential Eight.

Control de aplicaciones

- El equipo de aplicaciones permite buscar imágenes de contenedores de Amazon ECR en Amazon Inspector.
- El equipo de aplicaciones incorporó la herramienta de seguridad File Access Policy Daemon (fapolicyd) a la canalización del Generador de imágenes de EC2. Para más información, consulte Implementing Application Control en el sitio web de ACSC.
- El equipo de aplicaciones configura la definición de tareas de Amazon ECS para registrar los resultados en Amazon CloudWatch Logs.
- El equipo de aplicaciones implementa mecanismos para inspeccionar y administrar los resultados de Amazon Inspector.

Revisiones para las aplicaciones

- El equipo de aplicaciones permite buscar imágenes de contenedores de Amazon ECR en Amazon Inspector y configura las alertas para las bibliotecas en desuso o vulnerables.
- El equipo de aplicaciones automatiza sus respuestas a los resultados de Amazon Inspector. Los nuevos hallazgos inician su proceso de implementación a través de un EventBridge activador de Amazon, y CodePipeline es el objetivo.
- El equipo de aplicaciones permite AWS Config realizar un seguimiento de AWS los recursos para el descubrimiento de activos.

Restricción de los privilegios administrativos

- El equipo de aplicaciones ya restringe el acceso a las implementaciones de producción mediante una regla de aprobación en su canalización de implementaciones.
- El equipo de aplicaciones confía en la federación de identidades del equipo de la nube centralizada para la rotación de credenciales y el registro centralizado.
- El equipo de aplicaciones crea un CloudTrail registro y CloudWatch los filtra.
- El equipo de aplicaciones configura las alertas de Amazon SNS para las CodePipeline implementaciones y CloudFormation las eliminaciones de pilas.

Aplicación de revisiones a sistemas operativos

- El equipo de aplicaciones permite buscar imágenes de contenedores de Amazon ECR en Amazon Inspector y configura las alertas para las actualizaciones de revisiones del sistema operativo.
- El equipo de aplicaciones automatiza su respuesta a los resultados de Amazon Inspector. Los nuevos hallazgos inician su proceso de implementación mediante un EventBridge disparador, y ese CodePipeline es el objetivo.
- El equipo de aplicaciones se suscribe a las notificaciones de eventos de Amazon RDS para recibir la información acerca de las actualizaciones. Toman una decisión basada en el riesgo con el responsable de la empresa sobre si aplicar estas actualizaciones de manera manual o dejar que Amazon RDS las aplique de manera automática.
- El equipo de aplicaciones configura la instancia de Amazon RDS para que sea un clúster de varias zonas de disponibilidad con el fin de reducir el impacto de los eventos de mantenimiento.

Autenticación multifactor

- El equipo de aplicaciones confía en la solución de federación de identidades centralizada que se describe en la sección Arquitectura principal. Esta solución aplica la MFA, registra las autenticaciones y las alertas o responde de manera automática a los eventos de MFA sospechosos.

Copias de seguridad periódicas

- El equipo de aplicaciones configura su clúster de Amazon RDS AWS Backup para automatizar la copia de seguridad de los datos.
- El equipo de aplicaciones almacena las CloudFormation plantillas en un repositorio de código.
- El equipo de aplicaciones desarrolla un proceso automatizado para crear una copia de su carga de trabajo en otra región y ejecutar pruebas automatizadas (entrada del AWS blog). Una vez ejecutadas las pruebas automatizadas, la canalización destruye la pila. Esta canalización se ejecuta de manera automática una vez al mes y valida la eficacia de los procedimientos de recuperación.

Ejemplo de carga de trabajo: software COTS en Amazon EC2

Esta carga de trabajo es un ejemplo de Tema 3: administración de la infraestructura mutable con automatización.

La carga de trabajo que se ejecuta en Amazon EC2 se creó de manera manual mediante Consola de administración de AWS. Los desarrolladores actualizan el sistema de manera manual. Para ello, inician sesión en las instancias de EC2 y actualizan el software.

En el caso de esta carga de trabajo, los equipos de la nube y aplicaciones toman las medidas siguientes para abordar las estrategias Essential Eight.

Control de aplicaciones

- El equipo de la nube configura su canalización de AMI centralizada para instalar y configurar el AWS Systems Manager agente (agente SSM), CloudWatch el agente y. SELinux Comparten la AMI resultante en todas las cuentas de la organización.
- El equipo de nube usa AWS Config reglas para confirmar que todas las instancias de EC2 en ejecución son administradas por Systems Manager y tienen SSM Agent, CloudWatch agente e SELinux instalado.

- El equipo de la nube envía CloudWatch los resultados de Amazon Logs a una solución centralizada de gestión de eventos e información de seguridad (SIEM) que se ejecuta en Amazon OpenSearch Service.
- El equipo de aplicaciones implementa mecanismos para inspeccionar y gestionar los hallazgos de AWS Config Amazon Inspector. GuardDuty El equipo de la nube implementa sus propios mecanismos para detectar los resultados que no detecte el equipo de aplicaciones. Para más información sobre cómo crear un programa de administración de vulnerabilidades para abordar los resultados, consulte Building a scalable vulnerability management program on AWS.

Revisiones para las aplicaciones

- El equipo de aplicaciones aplica revisiones a las instancias según los resultados de Amazon Inspector.
- El equipo de la nube corrige la AMI base y el equipo de aplicaciones recibe una alerta cuando cambia esa AMI.
- El equipo de aplicaciones restringe el acceso directo a sus instancias de EC2 mediante la configuración de las reglas de los grupos de seguridad para permitir el tráfico solo en los puertos necesarios para la carga de trabajo.
- El equipo de aplicaciones utiliza Administrador de parches para aplicar las revisiones a las instancias en lugar de iniciar sesión en instancias individuales.
- Para ejecutar los comandos arbitrarios en grupos de instancias de EC2, el equipo de aplicaciones utiliza Run Command.
- En las pocas ocasiones en que el equipo de aplicaciones necesita acceso directo a una instancia, utiliza el Administrador de sesiones. Este enfoque de acceso utiliza las identidades federadas y registra la actividad de la sesión con fines de auditoría.

Restricción de los privilegios administrativos

- El equipo de aplicaciones configura las reglas de los grupos de seguridad para permitir el tráfico solo en los puertos necesarios para la carga de trabajo. Esto restringe el acceso directo a las instancias de Amazon EC2 y es necesario que los usuarios accedan a las instancias de EC2 a través del Administrador de sesiones.
- El equipo de aplicaciones confía en la federación de identidades del equipo de la nube centralizada para la rotación de credenciales y el registro centralizado.
- El equipo de la aplicación crea un CloudTrail registro y CloudWatch los filtra.

- El equipo de aplicaciones configura las alertas de Amazon SNS para las CodePipeline implementaciones y CloudFormation las eliminaciones de pilas.

Aplicación de revisiones a sistemas operativos

- El equipo de la nube corrige la AMI base y el equipo de aplicaciones recibe una alerta cuando cambia esa AMI. El equipo de aplicaciones implementa instancias nuevas mediante esta AMI y, a continuación, utiliza State Manager, una funcionalidad de Systems Manager, para instalar el software necesario.
- El equipo de aplicaciones utiliza Administrador de parches para aplicar las revisiones a las instancias en lugar de iniciar sesión en instancias individuales.
- Para ejecutar los comandos arbitrarios en grupos de instancias de EC2, el equipo de aplicaciones utiliza Run Command.
- En las pocas ocasiones en que el equipo de aplicaciones necesita acceso directo, utiliza el Administrador de sesiones.

Autenticación multifactor

- El equipo de aplicaciones confía en la solución de federación de identidades centralizada que se describe en la sección Arquitectura principal. Esta solución aplica la MFA, registra las autenticaciones y las alertas o responde de manera automática a los eventos de MFA sospechosos.

Copias de seguridad periódicas

- El equipo de aplicaciones crea un AWS Backup plan para sus instancias EC2 y los volúmenes de Amazon Elastic Block Store (Amazon EBS).
- El equipo de aplicaciones implementa un mecanismo para hacer una restauración de copias de seguridad de manera manual todos los meses.

Recursos

AWSDocumentación de

- Arquitectura de referencia de seguridad de AWS (SRA de AWS)
- Documentación de seguridad de AWS
- Pilar de seguridad del Marco de AWS Well-Architected

Otros recursos de AWS

- AWS Seguridad en la nube de
- AWS Cloud Adoption Framework (perspectiva de seguridad)

Recursos del Centro Australiano de Ciberseguridad

- Essential Eight Explained
- Essential Eight Maturity Model
- Essential Eight Assessment Process Guide

Colaboradores

Los colaboradores de este documento son:

- James Kingsmill, arquitecto sénior de soluciones, arquitectura de soluciones en AWS
- Chris Harding, arquitecto sénior de soluciones, arquitectura de soluciones en AWS
- Jess Modini, arquitecta de soluciones de asesoramiento, arquitectura de soluciones en AWS
- Justin Bowden, responsable de garantía de seguridad, garantía de seguridad en AWS
- Rob Powell, arquitecto sénior de soluciones, arquitectura de soluciones en AWS
- Tony Mihaljevic, arquitecto sénior de nube, AWS Professional Services
- Volker Rath, asesor principal de seguridad, servicios de seguridad global en AWS

Apéndice: Matrices de los controles de Essential Eigth

Las siguientes tablas vinculan las ocho estrategias esenciales con la guía de AWS implementación y las mejores prácticas relevantes en el Marco AWS de Buena Arquitectura. Para los ocho controles esenciales que no se aplican en el Nube de AWS, la tabla incluye un enlace a una guía adicional del Centro Australiano de Ciberseguridad (ACSC).

Matrices de controles:

- Control de aplicaciones
- Revisiones para las aplicaciones
- Configuración de los valores de macros de Microsoft Office
- Endurecimiento de las aplicaciones de usuario
- Restricción de los privilegios administrativos
- Aplicación de revisiones a sistemas operativos
- Autenticación multifactor
- Copias de seguridad periódicas

Control de aplicaciones

Control de Essential Eight	Guía para la implementación	AWS recursos	AWS Guía para Well-Architected
El control de aplicaciones se implementa en estaciones de trabajo y servidores para restringir la ejecución de archivos ejecutables, bibliotecas de software, scripts, instaladores, HTML compilado, aplicaciones HTML, applets del panel de control	Tema 2: gestión de la infraestructura inmutable mediante canalizaciones seguras: implementación de canalizaciones de creación de contenedores y AMI	Utilice Generador de imágenes de EC2 e incorpore: • AWS Systems Manager Agente (agente SSM) • Herramientas de seguridad para el control de aplicaciones, como Security Enhanced Linux	SEC06- BP02 Aprovisione cómputo a partir de imágenes reforzadas

Control de Essential Eight	Guía para la implementación	AWS recursos	AWS Guía para Well-Architected
y controladores a un conjunto aprobado por la organización.		(SELinux) (GitHub), File Access Policy Daemon (fapolicyd) (GitHub) u OpenSCAP CloudWatch Agente de Amazon Comparte AMIs con toda la organización Asegúrese de que los equipos de aplicaciones consulten las últimas AMIs Utilice la canalización de AMI para la administración de revisiones	
Las “reglas de bloque recomendadas” de Microsoft están implementadas.	Consulte Implementing Application Control (sitio web de ACSC)	No aplicable	No aplicable
Las “reglas de bloque de controlador recomendadas” de Microsoft están implementadas.			

Control de Essential Eight	Guía para la implementación	AWS recursos	AWS Guía para Well-Architected
Los conjuntos de reglas de control de aplicaciones se validan cada año o con mayor frecuencia.	Tema 8: implementación de mecanismos para los procesos manuales: implementación de un mecanismo para actualizar las políticas de seguridad	No disponible	SEC01- BP08 Evalúe e implemente nuevos servicios y funciones de seguridad con regularidad
Las ejecuciones permitidas y bloqueadas en estaciones de trabajo y servidores se registran de manera centralizada y se protegen contra modificaciones y eliminaciones no autorizadas, se supervisan para detectar señales de peligro y se toman medidas cuando se detectan incidentes de ciberseguridad.	Tema 7: centralización del registro y de la supervisión: habilitación de registros	Utilice el CloudWatch agente para publicar registros a nivel de sistema en Logs CloudWatch Configure alertas para detectar los hallazgos GuardDuty Cree un registro de la organización en CloudTrail Proteja los datos almacenados en Amazon S3 mediante el control de versiones y Bloqueo de objetos de S3	SEC04- BP01 Configurar el registro de servicios y aplicaciones SEC04- BP02 Capture registros, hallazgos y métricas en ubicaciones estandarizadas

Control de Essential Eight	Guía para la implementación	AWS recursos	AWS Guía para Well-Architected
	Tema 7: centralización del registro y de la supervisión: implementación de prácticas recomendadas de seguridad de registros	Implemente CloudTrail las mejores prácticas de seguridad Úselo SCPs para evitar que los usuarios deshabiliten los servicios de seguridad (AWS entrada del blog) Cifre los datos de registro en los CloudWatch registros mediante AWS Key Management Service	SEC04- BP01 Configure el registro de servicios y aplicaciones SEC04- BP02 Capture registros, hallazgos y métricas en ubicaciones estandarizadas

Control de Essential Eight	Guía para la implementación	AWS recursos	AWS Guía para Well-Architected
	Tema 7: centralización del registro y de la supervisión: centralización de los registros	Reciba CloudTrail registros de varias cuentas Envíe los registros a una cuenta de archivo de registros Centralice CloudWatch los registros de una cuenta para su auditoría y análisis (AWS entrada de blog) Centralice la administración de Amazon Inspector Cree un agregador para toda la organización en AWS Config (entrada de blog)AWS Centralice la gestión de Security Hub (CSPM) Centralice la gestión de GuardDuty Considere utilizar Amazon Security Lake	SEC04- BP02 Capture registros, hallazgos y métricas en ubicaciones estandarizadas

Control de Essential Eight	Guía para la implementación	AWS recursos	AWS Guía para Well-Architected
	Tema 8: implementación de mecanismos para los procesos manuales: implementación de mecanismos para revisar y solucionar los problemas de cumplimiento.	Considere la posibilidad de implementar la automatización, como las reglas de AWS Config, para reducir la carga de los procesos manuales	OPS02- BP02 Los procesos y procedimientos tienen propietarios identificados OPS02- BP03 Las actividades operativas han identificado a los propietarios responsables de su desempeño OPS02- Existen BP04 mecanismos para gestionar las responsabilidades y la propiedad

Revisiones para las aplicaciones

Control de Essential Eight	Guía para la implementación	AWS recursos	AWS Guía para Well-Architected
Se utiliza un método automatizado de detección de activos al menos cada quince días para facilitar la detección de activos para las actividades posteriores de análisis de vulnerabilidades.	Tema 1: uso de servicios administrados: escaneo para detectar vulnerabilidades Tema 2: gestión de la infraestructura inmutable mediante canalizaciones	Habilite Amazon Inspector en todas las cuentas de su organización Configure los escaneos mejorados para los repositorios de Amazon ECR	SEC06- BP01 Realice una gestión de vulnerabilidades SEC06- BP05 Automatice la protección informática

Control de Essential Eight	Guía para la implementación	AWS recursos	AWS Guía para Well-Architected
	seguras: implementación del escaneo de vulnerabilidades Tema 3: administración de la infraestructura mutable con automatización: implementación del escaneo de vulnerabilidades	mediante Amazon Inspector Cree un programa de administración de vulnerabilidades para clasificar y corregir los resultados de seguridad	

Control de Essential Eight	Guía para la implementación	AWS recursos	AWS Guía para Well-Architected
	Tema 7: centralización del registro y de la supervisión: centralización de los registros	Reciba CloudTrail registros de varias cuentas Envíe los registros a una cuenta de archivo de registros Centralice CloudWatch los registros de una cuenta para su auditoría y análisis (AWS entrada de blog) Centralice la administración de Amazon Inspector Cree un agregador para toda la organización en AWS Config (entrada de blog de AWS) Centralice la gestión de Security Hub (CSPM) Centralice la gestión de GuardDuty Considere la posibilidad de utilizar Security Lake	SEC04- BP02 Capture registros, hallazgos y métricas en ubicaciones estandarizadas

Control de Essential Eight	Guía para la implementación	AWS recursos	AWS Guía para Well-Architected
Para las actividades de análisis de up-to-date vulnerabilidades se utiliza un escáner de vulnerabilidades con una base de datos de vulnerabilidades.	Tema 1: uso de servicios administrados: escaneo para detectar vulnerabilidades Tema 2: gestión de la infraestructura inmutable mediante canalizaciones seguras: implementación del escaneo de vulnerabilidades Tema 3: administración de la infraestructura mutable con automatización: implementación del escaneo de vulnerabilidades	Habilite Amazon Inspector en todas las cuentas de su organización Configure los escaneos mejorados para los repositorios de Amazon ECR mediante Amazon Inspector Cree un programa de administración de vulnerabilidades para clasificar y corregir los resultados de seguridad	SEC06- BP01 Realizar la gestión de vulnerabilidades SEC06- BP05 Automatice la protección informática
Se utiliza un escáner de vulnerabilidades al menos una vez al día para identificar las revisiones o actualizaciones que faltan para las vulnerabilidades de seguridad en los servicios conectados a internet.			

Control de Essential Eight	Guía para la implementación	AWS recursos	AWS Guía para Well-Architected
Se utiliza un escáner de vulnerabilidades al menos una vez a la semana para identificar las revisiones o actualizaciones que faltan para las vulnerabilidades de seguridad en los conjuntos de aplicaciones ofimáticas, los navegadores web y sus extensiones, los clientes de correo electrónico, el software de PDF y los productos de seguridad.	Consulte Technical example: Patch applications (sitio web de ACSC)	No aplicable	No aplicable

Control de Essential Eight	Guía para la implementación	AWS recursos	AWS Guía para Well-Architected
Se utiliza un escáner de vulnerabilidades al menos cada quince días para identificar las revisiones o actualizaciones que faltan para las vulnerabilidades de seguridad en otras aplicaciones.	Tema 1: uso de servicios administrados: escaneo para detectar vulnerabilidades Tema 2: gestión de la infraestructura inmutable mediante canalizaciones seguras: implementación del escaneo de vulnerabilidades Tema 3: administración de la infraestructura mutable con automatización: implementación del escaneo de vulnerabilidades	Habilite Amazon Inspector en todas las cuentas de su organización Configure los escaneos mejorados para los repositorios de Amazon ECR mediante Amazon Inspector Cree un programa de administración de vulnerabilidades para clasificar y corregir los resultados de seguridad	SEC06- BP01 Realice la gestión de vulnerabilidades SEC06- BP05 Automatice la protección informática

Control de Essential Eight	Guía para la implementación	AWS recursos	AWS Guía para Well-Architected
Las revisiones, actualizaciones o mitigaciones de los proveedores para las vulnerabilidades de seguridad en los servicios conectados a internet se aplican en un plazo de dos semanas desde su publicación, o en un plazo de 48 horas si existe una vulnerabilidad.	Tema 1: uso de servicios administrados: escaneo para detectar vulnerabilidades Tema 2: gestión de la infraestructura inmutable mediante canalizaciones seguras: implementación del escaneo de vulnerabilidades Tema 3: administración de la infraestructura mutable con automatización: implementación del escaneo de vulnerabilidades	Habilite Amazon Inspector en todas las cuentas de su organización Configure los escaneos mejorados para los repositorios de Amazon ECR mediante Amazon Inspector Cree un programa de administración de vulnerabilidades para clasificar y corregir los resultados de seguridad	SEC06- BP01 Realice la gestión de vulnerabilidades
	Tema 3: administración de la infraestructura mutable con automatización: automatización de la aplicación de revisiones	Habilite Administrador de parches en todas las cuentas de su organización de AWS	SEC06- BP01 Realizar la gestión de vulnerabilidades SEC06- BP05 Automatice la protección informática

Control de Essential Eight	Guía para la implementación	AWS recursos	AWS Guía para Well-Architected
Las revisiones, actualizaciones o mitigaciones de los proveedores para las vulnerabilidades de seguridad en los conjuntos de aplicaciones ofimáticas, navegadores web y sus extensiones, clientes de correo electrónico, software de PDF y productos de seguridad se aplican en un plazo de dos semanas desde su publicación, o en un plazo de 48 horas si existe una vulnerabilidad.	Consulte Technical example: Patch applications (sitio web de ACSC)	No aplicable	No aplicable

Control de Essential Eight	Guía para la implementación	AWS recursos	AWS Guía para Well-Architected
Las revisiones, actualizaciones o mitigaciones de los proveedores para las vulnerabilidades de seguridad en otras aplicaciones se aplican en un plazo de un mes desde su publicación.	Tema 1: uso de servicios administrados: escaneo para detectar vulnerabilidades Tema 2: gestión de la infraestructura inmutable mediante canalizaciones seguras: implementación del escaneo de vulnerabilidades Tema 3: administración de la infraestructura mutable con automatización: implementación del escaneo de vulnerabilidades	Habilite Amazon Inspector en todas las cuentas de su organización Configure los escaneos mejorados para los repositorios de Amazon ECR mediante Amazon Inspector Cree un programa de administración de vulnerabilidades para clasificar y corregir los resultados de seguridad	SEC06- BP01 Realice la gestión de vulnerabilidades
	Tema 3: administración de la infraestructura mutable con automatización: automatización de la aplicación de revisiones	Habilite Administrador de parches en todas las cuentas de su organización de AWS	SEC06- BP01 Realizar la gestión de vulnerabilidades SEC06- BP05 Automatice la protección informática

Control de Essential Eight	Guía para la implementación	AWS recursos	AWS Guía para Well-Architected
Se eliminan las aplicaciones que ya no admiten los proveedores.	Tema 8: implementación de mecanismos para los procesos manuales: implementación de mecanismos para revisar y solucionar los problemas de cumplimiento.	Considere la posibilidad de utilizar Inventario de AWS Systems Manager para ver qué instancias ejecutan el software que necesita la política del software	SEC06- BP02 Aprovisione cómputo a partir de imágenes reforzadas

Configuración de los valores de macros de Microsoft Office

Control de Essential Eight	Guía para la implementación	AWS recursos	AWS Guía para Well-Architected
Las macros de Microsoft Office están inhabilitadas para los usuarios que no tienen un requisito empresarial demostrado.	Consulte Technical example: Configure macro settings (sitio web de ACSC)	No aplicable	No aplicable
Solo se permite la ejecución de macros de Microsoft Office que se ejecuten desde un entorno de pruebas, una ubicación de confianza o que estén firmadas digitalmente			

Control de Essential Eight	Guía para la implementación	AWS recursos	AWS Guía para Well-Architected
por un publicador de confianza.			
Solo los usuarios privilegiados responsables de validar que las macros de Microsoft Office no contienen código malicioso pueden escribir y modificar el contenido de las ubicaciones de confianza.			
Las macros de Microsoft Office firmadas digitalmente por un publicador que no sea de confianza no se pueden activar a través de la barra de mensajes o la vista Backstage.			
La lista de publicado res de confianza de Microsoft Office se valida cada año o con mayor frecuencia.			

Control de Essential Eight	Guía para la implementación	AWS recursos	AWS Guía para Well-Architected
Las macros de Microsoft Office de los archivos que se originan en internet están bloqueadas.			
El escaneo antivirus de macros de Microsoft Office está habilitado.			
Las macros de Microsoft Office no pueden hacer llamadas a la API de Win32.			
Los usuarios no pueden cambiar la configuración de seguridad de las macros de Microsoft Office.			

Control de Essential Eight	Guía para la implementación	AWS recursos	AWS Guía para Well-Architected
Las ejecuciones de macros de Microsoft Office permitidas y bloqueadas se registran de manera centralizada y se protegen contra modificaciones y eliminaciones no autorizadas, se supervisan para detectar señales de peligro y se toman medidas cuando se detectan incidentes de ciberseguridad.			

Endurecimiento de las aplicaciones de usuario

Control de Essential Eight	Guía para la implementación	AWS recursos	AWS Guía para Well-Architected
Los navegadores web no procesan Java desde internet.	Consulte Technical example: User application hardening (sitio web de ACSC)	No aplicable	No aplicable
Los navegadores web no procesan anuncios desde internet.			
Internet Explorer 11 se inhabilitó o eliminó.			

Control de Essential Eight	Guía para la implementación	AWS recursos	AWS Guía para Well-Architected
Microsoft Office no puede crear procesos secundarios.			
Microsoft Office no puede crear contenido ejecutable.			
Microsoft Office no puede inyectar código en otros procesos.			
Microsoft Office está configurado para evitar la activación de paquetes OLE.			
El software de PDF no puede crear procesos secundari os.			
Se implementan las directrices sobre endurecimiento de ACSC o del proveedor para los navegadores web, Microsoft Office y el software de PDF.			

Control de Essential Eight	Guía para la implementación	AWS recursos	AWS Guía para Well-Architected
Los usuarios no pueden cambiar la configuración de seguridad del navegador web, Microsoft Office y del software de PDF.			
.NET Framework 3.5 (incluye .NET 2.0 y 3.0) se inhabilitó o eliminó.			
Windows PowerShell 2.0 se inhabilitó o eliminó.			
PowerShell se configuró para utilizar el modo de idioma restringido.			

Control de Essential Eight	Guía para la implementación	AWS recursos	AWS Guía para Well-Architected
Las ejecuciones de scripts de PowerShell bloqueadas se registran de manera centralizada y se protegen contra modificaciones y eliminaciones no autorizadas, se supervisan para detectar señales de peligro y se toman medidas cuando se detectan incidentes de ciberseguridad.			

Restricción de los privilegios administrativos

Control de Essential Eight	Guía para la implementación	AWS recursos	AWS Guía para Well-Architected
Las solicitudes de acceso privilegiado a los sistemas y a las aplicaciones se validan cuando se solicitan por primera vez.	Tema 4: administración de identidades: implementación de la federación de identidades	Exija a los usuarios humanos que se federen con un proveedor de identidad para acceder a AWS mediante credenciales temporales	SEC02- BP04 Confíe en un proveedor de identidad centralizado SEC03- BP01 Defina los requisitos de acceso
El acceso privilegiado a los sistemas y aplicaciones se	Tema 4: administración de identidades: implementación	Exija a los usuarios humanos que se federen con	SEC02- BP04 Confíe en un proveedor de identidad centralizado

Control de Essential Eight	Guía para la implementación	AWS recursos	AWS Guía para Well-Architected
inhabilita de manera automática después de 12 meses, a menos que se vuelva a validar.	de la federación de identidades	un proveedor de identidad para acceder a AWS mediante credencia les temporales	
	Tema 4: administr ación de identidad es: rotación de las credenciales	Exija que las cargas de trabajo utilicen las funciones de IAM para acceder AWS Automatice la eliminación de los roles de IAM no utilizados Cambie las claves de acceso con regularid ad para los casos de uso que requieran credenciales a largo plazo AWS Summit ANZ 2023: su viaje hacia las credenciales temporales en la nube (YouTubevídeo)	SEC02- BP05 Audite y modifique las credenciales periódica mente

Control de Essential Eight	Guía para la implementación	AWS recursos	AWS Guía para Well-Architected
El acceso privilegiado a los sistemas y aplicaciones se inhabilita de manera automática después de 45 días de inactividad.	Tema 4: administración de identidades: implementación de la federación de identidades Tema 4: administración de identidades: rotación de las credenciales	Exija a los usuarios humanos que se federen con un proveedor de identidad para acceder AWS mediante credenciales temporales Exija que las cargas de trabajo utilicen las funciones de IAM para acceder AWS Automatice la eliminación de los roles de IAM no utilizados Cambie las claves de acceso con regularidad para los casos de uso que requieran credenciales a largo plazo AWS Summit ANZ 2023: su viaje hacia las credenciales temporales en la nube (YouTubevídeo)	SEC02- BP04 Confíe en un proveedor de identidad centralizado SEC02- BP05 Audite y modifique las credenciales periódicamente

Control de Essential Eight	Guía para la implementación	AWS recursos	AWS Guía para Well-Architected
El acceso privilegiado a los sistemas y las aplicaciones se limita solo a lo necesario para que los usuarios y los servicios desempeñen sus funciones.	Tema 4: administración de identidades: aplicación de permisos de privilegio mínimo	Proteja sus credenciales de usuario raíz y no las utilice para las tareas diarias Utilice IAM Access Analyzer para generar políticas de privilegios mínimos en función de la actividad de acceso Verifique el acceso público y multicuenta a los recursos con IAM Access Analyzer Utilice IAM Access Analyzer para validar las políticas de IAM con objeto de garantizar la seguridad y funcionalidad de los permisos Establezca barreras de protección de permisos en varias cuentas Utilice los límites de permisos para establecer los permisos máximos que puede conceder	SEC01- BP02 Proteja el usuario raíz y las propiedades de la cuenta SEC03- BP02 Otorgue el acceso con privilegios mínimos

Control de Essential Eight	Guía para la implementación	AWS recursos	AWS Guía para Well-Architected
		una política basada en identidades Utilice las condiciones de las políticas de IAM para restringir aún más el acceso Revise y elimine periódicamente los usuarios, funciones, permisos, políticas y credenciales no utilizados Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos Utilice la característica de conjuntos de permisos de IAM Identity Center	
Las cuentas privilegiadas no pueden acceder a internet, al correo electrónico y a los servicios web.	Consulte Technical example: Restrict administrative privileges (sitio web de ACSC)	Considere la posibilidad de implementar una SCP que evite que las VPC que aún no tengan acceso a internet lo obtengan.	No aplicable

Control de Essential Eight	Guía para la implementación	AWS recursos	AWS Guía para Well-Architected
Los usuarios con privilegios utilizan entornos operativos independientes con y sin privilegios.	Tema 5: establecimiento de un perímetro de datos	Establezca un perímetro de datos. Considere la posibilidad de implementar perímetros de datos entre entornos de distintas clasificaciones de datos, como `OFFICIAL: SENSITIVE` o `PROTECTED` con distintos niveles de riesgo, como desarrollo, pruebas o producción.	SEC06- BP03 Reduzca la gestión manual y el acceso interactivo
Los entornos operativos con privilegios no se virtualizan en entornos operativos sin privilegios.			
Las cuentas sin privilegios no pueden iniciar sesión en entornos operativos con privilegios.			
Las cuentas con privilegios (a excepción de las cuentas de administrador local) no pueden iniciar sesión en entornos operativos sin privilegios.			

Control de Essential Eight	Guía para la implementación	AWS recursos	AWS Guía para Well-Architected
Just-in-time la administración se utiliza para administrar sistemas y aplicaciones.	Tema 4: administración de identidades: implementación de la federación de identidades	Exija a los usuarios humanos que se federen con un proveedor de identidad para acceder AWS mediante credenciales temporales Implemente un acceso elevado temporal a sus AWS entornos (AWS entrada del blog)	SEC02- BP04 Confíe en un proveedor de identidad centralizado
Las actividades administrativas se llevan a cabo a través de servidores jump.	Tema 1: uso de servicios administrados Tema 3: administración de la infraestructura mutable con automatización: uso de la automatización en lugar de los procesos manuales	Utilice Administrador de sesiones o Run Command en lugar del acceso directo por SSH o RDP	SEC01- BP05 Reduzca el alcance de la gestión de la seguridad SEC06- BP03 Reduzca la gestión manual y el acceso interactivo
Las credenciales de las cuentas de administrador local y las cuentas de servicio son únicas, impredecibles y administrables.	Consulte Technical example: Restrict administrative privileges (sitio web de ACSC)	No aplicable	No aplicable

Control de Essential Eight	Guía para la implementación	AWS recursos	AWS Guía para Well-Architected
Windows Defender Credential Guard y Windows Defender Remote Credential Guard se habilitaron.			

Control de Essential Eight	Guía para la implementación	AWS recursos	AWS Guía para Well-Architected
El uso del acceso privilegiado se registra de manera centralizada y se protege contra modificaciones y eliminaciones no autorizadas, se supervisa para detectar señales de peligro y se utiliza cuando se detectan incidentes de ciberseguridad.	Tema 7: centralización del registro y de la supervisión: habilitación de registros Tema 7: centralización del registro y de la supervisión: centralización de los registros	Utilice el CloudWatch agente para publicar registros a nivel de sistema operativo en Logs CloudWatch Habilite CloudTrail para su organización Centralice CloudWatch los registros en una cuenta para su auditoría y análisis (AWS entrada de blog) Centralice la administración de Amazon Inspector Centralice la gestión de Security Hub (CSPM) Cree un agregador para toda la organización en AWS Config (entrada de blog de AWS) Centralice la gestión de GuardDuty Considere utilizar Amazon Security Lake	SEC04- BP01 Configure el registro de servicios y aplicaciones SEC04- BP02 Capture registros, hallazgos y métricas en ubicaciones estandarizadas
Los cambios en cuentas y grupos con privilegios se registran de manera centralizada y se protegen contra modificaciones y eliminaciones no autorizadas, se supervisan para detectar señales de peligro y se utilizan cuando se detectan incidentes de ciberseguridad.			

Control de Essential Eight	Guía para la implementación	AWS recursos	AWS Guía para Well-Architected
		Reciba CloudTrail registros de varias cuentas Envíe los registros a una cuenta de archivo de registros	

Aplicación de revisiones a sistemas operativos

Control de Essential Eight	Guía para la implementación	AWS recursos	AWS Guía para Well-Architected
Las revisiones, actualizaciones o mitigaciones de los proveedores para las vulnerabilidades de seguridad en sistemas operativos de los servicios conectados a internet se aplican en un plazo de dos semanas desde su publicación, o en un plazo de 48 horas si existe una vulnerabilidad.	Tema 2: gestión de la infraestructura inmutable mediante canalizaciones seguras: implementación de canalizaciones de creación de contenedores y AMI	Utilice Generador de imágenes de EC2 e incorpore: • AWS Systems Manager Agente (agente SSM) • Herramientas de seguridad para el control de aplicaciones, como Security Enhanced Linux (SELinux) (GitHub), File Access Policy Daemon (fapolicyd) (GitHub) u OpenSCAP • CloudWatch Agente de Amazon	SEC01- BP05 Reducir el alcance de la gestión de la seguridad SEC06- BP01 Realizar la gestión de vulnerabilidades SEC06- BP03 Reduzca la gestión manual y el acceso interactivo

Control de Essential Eight	Guía para la implementación	AWS recursos	AWS Guía para Well-Architected
		Comparte AMIs con toda la organización Asegúrese de que los equipos de aplicaciones consulten las últimas AMIs Utilice la canalización de AMI para la administración de revisiones	
	Tema 1: uso de servicios administrados: habilitación de la aplicación de revisiones Tema 3: administración de la infraestructura mutable con automatización: automatización de la aplicación de revisiones	Habilite Administrador de parches en todas las cuentas de su organización de AWS	SEC06- BP01 Realice la gestión de vulnerabilidades SEC06- BP05 Automatice la protección informática

Control de Essential Eight	Guía para la implementación	AWS recursos	AWS Guía para Well-Architected
Las revisiones, actualizaciones o mitigaciones de los proveedores para las vulnerabilidades de seguridad en sistemas operativos de las estaciones de trabajo, los servidores y los dispositivos de red se aplican en un plazo de dos semanas desde su publicación, o en un plazo de 48 horas si existe una vulnerabilidad.	Tema 2: gestión de la infraestructura inmutable mediante canalizaciones seguras: implementación de canalizaciones de creación de contenedores y AMI	Utilice Generador de imágenes de EC2 e incorpore: • AWS Systems Manager Agente (agente SSM) • Herramientas de seguridad para el control de aplicaciones, como Security Enhanced Linux (SELinux) (GitHub), File Access Policy Daemon (fapolicyd) (GitHub) u OpenSCAP • CloudWatch Agente de Amazon Comparte AMIs con toda la organización Asegúrese de que los equipos de aplicaciones consulten las últimas AMIs Utilice la canalización de AMI para la administración de revisiones	SEC01- BP05 Reducir el alcance de la gestión de la seguridad SEC06- BP01 Realizar la gestión de vulnerabilidades SEC06- BP02 Aprovisione cómputo a partir de imágenes reforzadas

Control de Essential Eight	Guía para la implementación	AWS recursos	AWS Guía para Well-Architected
	Tema 1: uso de servicios administrados: habilitación de la aplicación de revisiones Tema 3: administración de la infraestructura mutable con automatización: automatización de la aplicación de revisiones	Habilite Administrador de parches en todas las cuentas de su organización de AWS	SEC06- BP01 Realice la gestión de vulnerabilidades SEC06- BP05 Automatice la protección informática

Control de Essential Eight	Guía para la implementación	AWS recursos	AWS Guía para Well-Architected
Se utiliza un escáner de vulnerabilidades al menos una vez al día para identificar las revisiones o actualizaciones que faltan para las vulnerabilidades de seguridad en los sistemas operativos de los servicios conectados a internet.	Tema 1: uso de servicios administrados: escaneo para detectar vulnerabilidades Tema 2: gestión de la infraestructura inmutable mediante canalizaciones seguras: implementación del escaneo de vulnerabilidades Tema 3: administración de la infraestructura mutable con automatización: implementación del escaneo de vulnerabilidades	Habilite Amazon Inspector en todas las cuentas de su organización Configure los escaneos mejorados para los repositorios de Amazon ECR mediante Amazon Inspector Cree un programa de administración de vulnerabilidades para clasificar y corregir los resultados de seguridad	SEC01- BP05 Reduzca el alcance de la gestión de la seguridad SEC06- BP01 Realizar la gestión de vulnerabilidades SEC06- BP02 Aprovisione cómputo a partir de imágenes reforzadas
Se utiliza un escáner de vulnerabilidades al menos una vez a la semana para identificar las revisiones o actualizaciones que faltan para las vulnerabilidades de seguridad en los sistemas operativos de las estaciones de trabajo, los servidores y los dispositivos de red.			

Control de Essential Eight	Guía para la implementación	AWS recursos	AWS Guía para Well-Architected
La última versión, o la versión anterior, de los sistemas operativos se utilizan para las estaciones de trabajo, los servidores y los dispositivos de red. Se sustituyen los sistemas operativos que ya no admiten los proveedores.	Tema 2: gestión de la infraestructura inmutable mediante canalizaciones seguras: implementación del escaneo de vulnerabilidades	Utilice Generador de imágenes de EC2 e incorpore: • AWS Systems Manager Agente (agente SSM) • Herramientas de seguridad para el control de aplicaciones, como Security Enhanced Linux (SELinux) (GitHub), File Access Policy Daemon (fapolicyd) (GitHub) u OpenSCAP • CloudWatch Agente de Amazon Comparte AMIs con toda la organización Asegúrese de que los equipos de aplicaciones consulten las últimas AMIs Utilice la canalización de AMI para la administración de revisiones	SEC01- BP05 Reducir el alcance de la gestión de la seguridad SEC06- BP01 Realizar la gestión de vulnerabilidades SEC06- BP02 Aprovisione cómputo a partir de imágenes reforzadas

Autenticación multifactor

Control de Essential Eight	Guía para la implementación	AWS recursos	AWS Guía para Well-Architected
Los usuarios de una organización utilizan la autenticación multifactor si se autentican en los servicios de internet de la organización.	Tema 4: administración de identidades: implementación de la federación de identidades	Exija a los usuarios humanos que se federen con un proveedor de identidad para acceder AWS mediante credenciales temporales Implemente un acceso elevado temporal a los entornos de AWS	SEC02- BP04 Confíe en un proveedor de identidad centralizado
	Tema 4: administración de identidades: aplicación de la MFA	Exija la MFA para el usuario raíz Requiere MFA a través de AWS IAM Identity Center Considere la posibilidad de exigir la MFA para las acciones de API específicas del servicio	SEC02- BP01 Utilice mecanismos de inicio de sesión sólidos
Los usuarios de una organización utilizan la autenticación multifactor cuando se autentican en servicios externos	Consulte Implementing Multi-Factor Authentication (sitio web de ACSC)	No aplicable	No aplicable

Control de Essential Eight	Guía para la implementación	AWS recursos	AWS Guía para Well-Architected
conectados a internet que procesan, almacenan o comunican informaci ón confidencial de su organización.			
Los usuarios de una organización utilizan la autenticación multifactor (si está disponible) cuando se autentican en servicios externos conectados a internet que procesan, almacenan o comunican informaci ón no confidencial de su organización.			
La autenticación multifactor está habilitada de manera predeterminada para los usuarios que no pertenecen a la organización (pero pueden optar por no utilizarla) si se autentican en los servicios de internet de una organización.			

Control de Essential Eight	Guía para la implementación	AWS recursos	AWS Guía para Well-Architected
La autenticación multifactor se utiliza para autenticar a los usuarios con privilegios de los sistemas.	Tema 4: administración de identidades: implementación de la federación de identidades	Exija a los usuarios humanos que se federen con un proveedor de identidad para acceder AWS mediante credenciales temporales Implemente un acceso elevado temporal a los entornos de AWS	SEC02- BP04 Confíe en un proveedor de identidad centralizado
	Tema 4: administración de identidades: aplicación de la MFA	Exija la MFA para el usuario raíz Exija la MFA a través de IAM Identity Center Considere la posibilidad de exigir la MFA para las acciones de API específicas del servicio	SEC02- BP01 Utilice mecanismos de inicio de sesión sólidos
La autenticación multifactor se utiliza para autenticar a los usuarios que acceden a los repositorios de los datos importantes.	Tema 4: administración de identidades: aplicación de la MFA	Considere la posibilidad de exigir la MFA para las acciones de API específicas del servicio	SEC02- BP01 Utilice mecanismos de inicio de sesión potentes

Control de Essential Eight	Guía para la implementación	AWS recursos	AWS Guía para Well-Architected
La autenticación multifactor es resistente a la suplantación de identidad de verificadores y utiliza algo que los usuarios tienen y algo que los usuarios saben, o bien algo que los usuarios tienen y que se desbloquea mediante algo que los usuarios saben o son.	Consulte Implementing Multi-Factor Authentication (sitio web de ACSC)	No aplicable	No aplicable

Control de Essential Eight	Guía para la implementación	AWS recursos	AWS Guía para Well-Architected
Las autenticaciones multifactor correctas e incorrectas se registran de manera centralizada y se protegen contra modificaciones y eliminaciones no autorizadas, se supervisan en busca de signos de compromiso y se toman medidas cuando se detectan incidentes de ciberseguridad.	Tema 7: centralización del registro y de la supervisión: habilitación de registros Tema 7: centralización del registro y de la supervisión: centralización de los registros	Centralice CloudWatch los registros en una cuenta para su auditoría y análisis (AWS entrada de blog) Centralice la administración de Amazon Inspector Centralice la gestión de Security Hub (CSPM) Cree un agregador para toda la organización en AWS Config (entrada de blog de AWS) Centralice la gestión de GuardDuty Considere la posibilidad de utilizar Security Lake Reciba CloudTrail registros de varias cuentas Envíe los registros a una cuenta de archivo de registros	SEC04- BP01 Configure el registro de servicios y aplicaciones SEC04- BP02 Capture registros, hallazgos y métricas en ubicaciones estandarizadas

Copias de seguridad periódicas

Control de Essential Eight	Guía para la implementación	AWS recursos	AWS Guía para Well-Architected
Las copias de seguridad de los datos importantes, del software y de los valores de configuración se hacen y conservan de manera coordinada y resistente, de acuerdo con los requisitos de continuidad del negocio.	Tema 6: automatización de las copias de seguridad: automatización de la copia de seguridad y la recuperación de datos	Implemente el respaldo de datos en AWS Automatice el respaldo de datos a escala (AWS entrada del blog)	REL09- BP01 Identifique y haga copias de seguridad de todos los datos de los que es necesario hacer copias de seguridad, o reproduzca los datos de las fuentes REL09- BP02 Proteja y cifre las copias de seguridad REL09- BP03 Realice copias de seguridad de datos automáticamente
La restauración de sistemas, software y datos importantes a partir de copias de seguridad se prueba de manera coordinada como parte de los ejercicios de recuperación ante desastres.	Tema 6: automatización de las copias de seguridad: automatización de la copia de seguridad y la recuperación de datos Tema 6: automatización de las copias de seguridad: implementación de la gobernanza en todos los resultados de AWS Backup	Automate data recovery validation with AWS Backup (entrada de blog de AWS) Utilice AWS Backup Audit Manager para auditar el cumplimiento de sus AWS Backup políticas	REL09- BP04 Realice una recuperación periódica de los datos para verificar la integridad y los procesos de la copia de seguridad

Control de Essential Eight	Guía para la implementación	AWS recursos	AWS Guía para Well-Architected
Las cuentas sin privilegios y las cuentas con privilegios (a excepción de los administradores de copias de seguridad) no pueden acceder a las copias de seguridad.	Tema 6: automatización de las copias de seguridad: Implemente la gobernanza en todos sus AWS Backup resultados	Las 10 mejores prácticas de seguridad para proteger las copias de seguridad en AWS (AWS entrada del blog) Utilice AWS Backup Vault Lock para mejorar la seguridad de sus bóvedas de respaldo Utilice AWS Backup Audit Manager para auditar el cumplimiento de sus AWS Backup políticas	SEC08- BP04 Aplique el control de acceso
Las cuentas sin privilegios y las cuentas con privilegios (a excepción de las cuentas de emergencia de copias de seguridad) no pueden modificar ni eliminar las copias de seguridad.			

Avisos

Es responsabilidad de los clientes realizar su propia evaluación independiente de la información que contiene este documento. El presente documento: (a) tiene solo fines informativos, (b) representa las ofertas y prácticas actuales de los productos de AWS, que están sujetas a cambios sin previo aviso, y (c) no supone ningún compromiso ni garantía por parte de AWS ni sus empresas filiales, proveedores o licenciantes. Los productos o servicios de AWS se proporcionan “tal cual”, sin garantías, declaraciones ni condiciones de ningún tipo, ya sean expresas o implícitas. Las responsabilidades y obligaciones de AWS con respecto a sus clientes se controlan mediante los acuerdos de AWS y este documento no forma parte ni modifica ningún acuerdo entre AWS y sus clientes.

Historial de documentos

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

Cambio	Descripción	Fecha
Actualizaciones de las prácticas recomendadas	Actualizamos esta guía para reflejar las prácticas recomendadas más recientes en el pilar de seguridad del Marco de AWS Well-Arch itected.	6 de noviembre de 2024
Publicación inicial	—	20 de octubre 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:

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

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

A

A2A () Agent-to-Agent

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

ABAC

Consulte control de acceso basado en atributos.

servicios abstractos

Consulte servicios administrados.

ACID

Consulte atomicidad, consistencia, aislamiento, durabilidad.

migración activa-activa

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

migración activa-pasiva

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

Agente

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

Agent Ops

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

función de agregación

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

IA

Consulte inteligencia artificial.

AIOps

Consulte operaciones de inteligencia artificial

anonimización

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

antipatrones

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

control de aplicaciones

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

cartera de aplicaciones

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

inteligencia artificial (IA)

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

operaciones de inteligencia artificial (AIOps)

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

cifrado asimétrico

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

atomicidad, consistencia, aislamiento, durabilidad (ACID)

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

control de acceso basado en atributos (ABAC)

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

origen de datos fidedigno

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

Zona de disponibilidad

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

AWS Marco de adopción de la nube (AWS CAF)

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

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

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

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

B

bot malicioso

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

BCP

Consulte planificación de la continuidad del negocio.

gráfico de comportamiento

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

sistema big-endian

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

clasificación binaria

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

filtro de floración

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

blue/green despliegue

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

bot

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

botnet

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

branch

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

acceso de emergencia

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

estrategia de implementación sobre infraestructura existente

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

caché de búfer

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

capacidad empresarial

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

planificación de la continuidad del negocio (BCP)

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

C

CAF

Consulte AWS Cloud Adoption Framework.

implementación canario

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

CCoE

Consulte Centro de excelencia en la nube.

CDC

Consulte captura de datos de cambios.

captura de datos de cambio (CDC)

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

ingeniería del caos

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

CI/CD

Consulte integración continua y entrega continua.

clasificación

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

Desarrollador ciudadano

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

cifrado del cliente

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

Centro de excelencia en la nube (CCoE)

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

computación en la nube

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

modelo operativo en la nube

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

etapas de adopción de la nube

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

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

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

CMDB

Consulte base de datos de administración de configuración.

repositorio de código

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

caché en frío

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

datos fríos

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

visión artificial (CV)

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

deriva de configuración

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

base de datos de administración de configuración (CMDB)

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

paquete de conformidad

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

integración y entrega continuas () CI/CD

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

CV

Consulte visión artificial.

D

datos en reposo

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

clasificación de datos

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

deriva de datos

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

datos en tránsito

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

malla de datos

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

minimización de datos

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

perímetro de datos

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

preprocesamiento de datos

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

procedencia de los datos

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

titular de los datos

Persona cuyos datos se recopilan y procesan.

almacenamiento de datos

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

lenguaje de definición de datos (DDL)

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

lenguaje de manipulación de datos (DML)

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

DDL

Consulte lenguaje de definición de bases de datos.

conjunto profundo

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

aprendizaje profundo

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

defensa en profundidad

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

administrador delegado

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

Implementación

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

entorno de desarrollo

Consulte entorno.

control de detección

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

asignación de flujos de valor para el desarrollo (DVSM)

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

gemelo digital

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

tabla de dimensiones

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

desastre

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

recuperación de desastres (DR)

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

DML

Consulte lenguaje de manipulación de bases de datos.

diseño basado en el dominio

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

DR

Consulte recuperación ante desastres.

Detección de desviaciones

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

DVSM

Consulte asignación de flujos de valor para el desarrollo.

E

EDA

Consulte análisis de datos de tipo exploratorio.

EDI

Consulte intercambio electrónico de datos.

computación en la periferia

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

intercambio electrónico de datos (EDI)

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

cifrado

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

clave de cifrado

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

endianidad

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

punto de conexión

Consulte punto de conexión de servicio.

servicio de punto de conexión

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

planificación de recursos empresariales (ERP)

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

cifrado de sobre

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

entorno

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

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

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

epopeya

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

ERP

Consulte planificación de recursos empresariales.

análisis de datos de tipo exploratorio (EDA)

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

F

tabla de hechos

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

Fail Fast

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

límite de aislamiento de errores

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

rama de característica

Consulte rama.

características

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

importancia de las características

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

transformación de funciones

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

peticiones con pocos pasos

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

FGAC

Consulte control de acceso detallado.

control de acceso preciso (FGAC)

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

migración relámpago

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

FM

Consulte modelo fundacional.

Modelo fundacional (FM)

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

Puerta de enlace FM

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

G

IA generativa

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

bloqueo geográfico

Consulte restricciones geográficas.

restricciones geográficas (bloqueo geográfico)

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

Flujo de trabajo de Gitflow

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

imagen dorada

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

estrategia de implementación desde cero

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

barrera de protección

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

barandas (AI)

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

H

HA

Consulte alta disponibilidad.

migración heterogénea de bases de datos

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

alta disponibilidad (HA)

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

modernización histórica

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

datos de reserva

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

human-in-the-loop (HiTL)

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

migración homogénea de bases de datos

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

datos recientes

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

hotfix

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

periodo de hiperatención

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

I

IaC

Consulte infraestructura como código.

políticas basadas en identidades

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

aplicación inactiva

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

IIoT

Consulte Internet de las cosas industrial.

infraestructura inmutable

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

VPC entrante (de entrada)

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

migración gradual

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

Industria 4.0

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

infraestructura

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

infraestructura como código (IaC)

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

Internet de las cosas industrial (IIoT)

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

VPC de inspección

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

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

Internet de las cosas (IoT)

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

interpretabilidad

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

IoT

Consulte Internet de las cosas.

biblioteca de información de TI (ITIL)

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

administración de servicios de TI (ITSM)

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

ITIL

Consulte biblioteca de información de TI.

ITSM

Consulte administración de servicios de TI.

L

control de acceso basado en etiquetas (LBAC)

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

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

zona de aterrizaje

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

modelo de lenguaje de gran tamaño (LLM)

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

migración grande

Migración de 300 servidores o más.

LBAC

Consulte control de acceso basado en etiquetas.

privilegio mínimo

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

migrar mediante lift-and-shift

Consulte Las 7 R.

sistema little-endian

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

LLM

Consulte modelo de lenguaje de gran tamaño.

entornos inferiores

Consulte entorno.

M

machine learning (ML)

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

rama principal

Consulte rama.

malware

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

Servicios administrados

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

sistema de ejecución de fabricación (MES)

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

MAP

Consulte Programa de aceleración de la migración.

MCP

Consulte Model Context Protocol.

Protocolo de contexto para modelos (MCP)

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

Servidor MCP

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

mecanismo

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

cuenta de miembro

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

MES

Consulte sistema de ejecución de fabricación.

Message Queuing Telemetry Transport (MQTT)

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

microservicio

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

arquitectura de microservicios

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

Programa de aceleración de la migración (MAP)

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

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

migración a escala

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

fábrica de migración

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

metadatos de migración

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

patrón de migración

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

Migration Portfolio Assessment (MPA)

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

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

Evaluación de la preparación para la migración (MRA)

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

estrategia de migración

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

ML

Consulte machine learning.

modernización

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

evaluación de la preparación para la modernización

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

aplicaciones monolíticas (monolitos)

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

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

MPA

Consulte Migration Portfolio Assessment.

MQTT

Consulte Message Queuing Telemetry Transport.

clasificación multiclase

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

infraestructura mutable

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

O

OAC

Consulte control de acceso de origen.

OAI

Consulte identidad de acceso de origen.

OCM

Consulte administración del cambio organizacional.

migración fuera de línea

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

OI

Consulte integración de operaciones.

OLA

Consulte acuerdo de nivel operativo.

migración en línea

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

OPC-UA

Consulte Open Process Communications: arquitectura unificada.

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

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

acuerdo de nivel operativo (OLA)

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

revisión de la preparación operativa (ORR)

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

tecnología operativa (TO)

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

integración de operaciones (OI)

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

registro de seguimiento organizativo

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

administración del cambio organizacional (OCM)

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

control de acceso de origen (OAC)

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

identidad de acceso de origen (OAI)

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

ORR

Consulte revisión de la preparación operativa.

OT

Consulte tecnología operativa.

VPC saliente (de salida)

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

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

P

límite de permisos

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

información de identificación personal (PII)

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

PII

Consulte información de identificación personal.

manual de estrategias

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

PLC

Consulte controlador lógico programable.

PLM

Consulte administración del ciclo de vida del producto.

policy

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

persistencia políglota

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

evaluación de cartera

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

predicate

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

inserción de predicados

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

control preventivo

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

entidad principal

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

Privacidad desde el diseño

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

zonas alojadas privadas

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

control proactivo

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

administración del ciclo de vida del producto (PLM)

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

entorno de producción

Consulte entorno.

controlador lógico programable (PLC)

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

encadenamiento de peticiones

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

seudonimización

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

publish/subscribe (pub/sub)

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

Q

plan de consulta

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

regresión del plan de consulta

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

R

Matriz RACI

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

RAG

Consulte generación aumentada por recuperación.

ransomware

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

Matriz RASCI

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

RCAC

Consulte control de acceso por filas y columnas.

réplica de lectura

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

rediseñar

Consulte Las 7 R.

objetivo de punto de recuperación (RPO)

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

objetivo de tiempo de recuperación (RTO)

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

refactorizar

Consulte Las 7 R.

Region

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

regresión

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

volver a alojar

Consulte Las 7 R.

versión

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

reubicar

Consulte Las 7 R.

redefinir la plataforma

Consulte Las 7 R.

recomprar

Consulte Las 7 R.

resiliencia

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

política basada en recursos

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

matriz responsable, confiable, consultada e informada (RACI)

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

control receptivo

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

retain

Consulte Las 7 R.

retirar

Consulte Las 7 R.

Generación aumentada de recuperación (RAG)

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

rotación

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

control de acceso por filas y columnas (RCAC)

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

RPO

Consulte objetivo de punto de recuperación.

RTO

Consulte objetivo de tiempo de recuperación.

manual de procedimientos

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

S

SAML 2.0

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

SCADA

Consulte control de supervisión y adquisición de datos.

SCP

Consulte política de control de servicio.

secreta

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

seguridad desde el diseño

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

control de seguridad

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

refuerzo de la seguridad

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

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

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

automatización de la respuesta de seguridad

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

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

cifrado del servidor

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

política de control de servicio (SCP)

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

punto de enlace de servicio

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

acuerdo de nivel de servicio (SLA)

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

indicador de nivel de servicio (SLI)

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

objetivo de nivel de servicio (SLO)

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

modelo de responsabilidad compartida

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

Shadow AI

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

SIEM

Consulte sistema de administración de eventos e información de seguridad.

único punto de error (SPOF)

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

SLA

Consulte acuerdo de nivel de servicio.

SLI

Consulte indicador de nivel de servicio.

SLO

Consulte objetivo de nivel de servicio.

modelo de dividir y sembrar

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

SPOF

Consulte único punto de error.

esquema en estrella

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

patrón de higo estrangulador

Un enfoque para modernizar los sistemas monolíticos mediante la reescritura y el reemplazo gradual de las funciones del sistema hasta que se pueda desmantelar el sistema heredado.

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

subred

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

control de supervisión y adquisición de datos (SCADA)

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

cifrado simétrico

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

pruebas sintéticas

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

petición del sistema

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

T

etiquetas

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

variable de destino

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

lista de tareas

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

entorno de prueba

Consulte entorno.

entrenamiento

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

herramienta

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

puerta de enlace de tránsito

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

flujo de trabajo basado en enlaces troncales

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

acceso de confianza

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

ajuste

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

equipo de dos pizzas

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

U

incertidumbre

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

tareas indiferenciadas

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

entornos superiores

Consulte entorno.

V

succión

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

control de versión

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

Emparejamiento de VPC

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

vulnerabilidad

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

W

caché caliente

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

datos templados

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

función de ventana

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

carga de trabajo

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

flujo de trabajo

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

WORM

Consulte escritura única y lectura múltiple.

WQF

Consulte AWS Workload Qualification Framework.

escritura única y lectura múltiple (WORM)

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

Z

ataque de día cero

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

vulnerabilidad de día cero

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

peticiones desde cero

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

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

aplicación zombi

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

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