AWS Arquitectura de referencia de seguridad (AWS SRA): arquitectura principal

AWS Guía prescriptiva

AWS Guía prescriptiva: AWS Arquitectura de referencia de seguridad (AWS SRA): arquitectura principal

Table of Contents

AWS Arquitectura de referencia de seguridad (AWS SRA): arquitectura principal

Equipo de seguridad de servicios globales, Amazon Web Services (colaboradores)

Diciembre de 2025 (historial del documento)

Influya en el futuro de la arquitectura de referencia de AWS seguridad (AWS SRA) realizando una breve encuesta.

La arquitectura de referencia de seguridad (AWS SRA AWS) de Amazon Web Services () es un conjunto integral de directrices para implementar la gama completa de servicios de AWS seguridad en un entorno de cuentas múltiples. Úselo para ayudar a diseñar, implementar y administrar los servicios de AWS seguridad de modo que se ajusten a las prácticas AWS recomendadas. Las recomendaciones se basan en una arquitectura de una sola página que incluye los servicios de AWS seguridad: cómo ayudan a alcanzar los objetivos de seguridad, dónde se pueden implementar y gestionar mejor en su Cuentas de AWS entorno y cómo interactúan con otros servicios de seguridad. Esta guía arquitectónica general complementa las recomendaciones detalladas y específicas de cada servicio, como las que se encuentran en el sitio web de documentación de AWS seguridad.

La arquitectura y las recomendaciones que la acompañan se basan en nuestras experiencias colectivas con clientes AWS empresariales. Este documento es una referencia (un conjunto completo de directrices Servicios de AWS para proteger un entorno determinado) y los patrones de solución del repositorio de códigos de la AWS SRA se diseñaron para la arquitectura específica que se ilustra en esta referencia. Cada cliente tendrá requisitos diferentes. Como resultado, el diseño de su AWS entorno puede diferir de los ejemplos que se proporcionan aquí. Tendrá que modificar y adaptar estas recomendaciones para adaptarlas a sus necesidades individuales de entorno y seguridad. A lo largo del documento, cuando procede, sugerimos opciones para los escenarios alternativos más frecuentes.

La AWS SRA es un conjunto de directrices dinámicas y se actualiza periódicamente en función de las nuevas versiones de servicios y funciones, los comentarios de los clientes y el panorama de amenazas en constante cambio. Cada actualización incluirá la fecha de revisión y el registro de cambios asociado.

Si bien nos basamos en un diagrama de una página como base, la arquitectura va más allá de un diagrama de un solo bloque y debe construirse sobre una base bien estructurada de fundamentos y principios de seguridad. Puede utilizar este documento de dos maneras: como narración o como referencia. Los temas están organizados en forma de historia, por lo que puede leerlos desde el principio (guía básica de seguridad) hasta el final (análisis de los ejemplos de código que puede implementar). Como alternativa, puede navegar por el documento para centrarse en los principios de seguridad, los servicios, los tipos de cuentas, las directrices y los ejemplos que mejor se adapten a sus necesidades.

Este documento se divide en las siguientes secciones y un apéndice:

- Acerca de la biblioteca de la AWS SRA proporciona una descripción general de las directrices técnicas y el código incluidos en la colección de publicaciones de la AWS SRA.
- El valor de la AWS SRA analiza la motivación para crearla, describe cómo puede utilizarla para ayudar a mejorar su seguridad y enumera las principales conclusiones. AWS
- Security Foundations revisa el Marco de Adopción de la AWS Nube (AWS CAF), el AWS Marco Well-Architected y AWS el Modelo de Responsabilidad Compartida, y destaca los elementos que son especialmente relevantes para la SRA. AWS
- AWS Organizations, cuentas e IAM Guardrails presenta el AWS Organizations servicio, analiza las capacidades de seguridad fundamentales y las barreras de protección y ofrece una descripción general de nuestra estrategia de cuentas múltiples recomendada.
- La arquitectura AWS de referencia de seguridad es un diagrama de arquitectura de una sola página que muestra las funciones y los servicios y funciones de seguridad que Cuentas de AWS están disponibles de forma general.
- La inteligencia artificial y el aprendizaje automático (AI/ML) para la seguridad describen las distintas formas de Servicios de AWS utilizar la inteligencia artificial y el aprendizaje automático (AI/ML) en segundo plano para ayudarle a alcanzar objetivos de seguridad específicos. Puede incluirlos Servicios de AWS en su diseño para aprovechar las funciones de seguridad avanzadas.
- Creación de su arquitectura de seguridad: un enfoque gradual proporciona orientación sobre cómo puede crear su propia arquitectura de seguridad en seis fases iterativas, según la referencia proporcionada por la AWS SRA.
- AWS La lista de verificación de mejores prácticas de la SRA resume las recomendaciones que se analizan a lo largo de la guía en una lista de verificación que puede seguir a medida que crea su versión de la arquitectura de seguridad.

- Los recursos de IAM presentan un resumen y un conjunto de consejos orientativos AWS Identity and Access Management (IAM) que son importantes para su arquitectura de seguridad.
- El repositorio de código para ejemplos de AWS SRA proporciona una descripción general del GitHub repositorio asociado que ayudará a los desarrolladores e ingenieros a implementar algunas de las pautas y patrones de arquitectura que se presentan en este documento. Puede implementar los ejemplos utilizando Terraform AWS CloudFormation o utilizando Terraform. HashiCorp Son compatibles tanto con entornos como AWS Control Tower con otros entornos.AWS Control Tower

El apéndice contiene una lista de los servicios individuales de AWS seguridad, identidad y cumplimiento, y proporciona enlaces a más información sobre cada servicio. La sección Historial del documento proporciona un registro de cambios para realizar un seguimiento de las versiones de este documento. También puede suscribirse a una fuente RSS para recibir notificaciones de cambios.

Acerca de la AWS biblioteca SRA

Influya en el futuro de la arquitectura de referencia de AWS seguridad (AWS SRA) realizando una breve encuesta.

Esta guía forma parte de una biblioteca que proporciona planos arquitectónicos y orientación técnica para diseñar y crear arquitecturas de seguridad sobre las que basarse. AWS La biblioteca consta de un código de implementación (biblioteca de códigos AWS SRA), una herramienta de validación (SRA Verify) y dos categorías de guías complementarias que cubren la arquitectura principal y las arquitecturas de análisis profundo.

AWS SRA: arquitectura básica (esta guía)

Esta guía representa la base de la arquitectura de AWS seguridad recomendada. Es el punto de partida que se aplica a todas las organizaciones, independientemente de su sector, tipo de aplicación o cualquier otra consideración. Esta base le ayuda a construir una arquitectura sólida y escalable AWS y a crear una sólida base de seguridad para AWS múltiples cuentas que se amplía de forma segura a medida que su empresa crece.

AWS SRA: profundiza en las arquitecturas

La guía de arquitectura principal de la AWS SRA se complementa con publicaciones adicionales que proporcionan patrones de arquitectura alineados con las capacidades de seguridad específicas, los tipos de aplicaciones y los requisitos de cumplimiento o reglamentarios específicos. Estos patrones amplían la arquitectura principal y deben usarse junto con la AWS SRA (guía de arquitectura básica).

Las siguientes guías proporcionan patrones arquitectónicos alineados con capacidades de seguridad específicas:

- AWS SRA: la gestión de identidades proporciona orientación sobre cómo implementar una solución de administración de identidades y accesos escalable, sólida y centralizada. AWS
- AWS SRA (seguridad perimetral) analiza los patrones de arquitectura y la implementación Servicios de AWS de la seguridad perimetral en una cuenta central o en cuentas individuales.
- AWS SRA (Cyber Forensics) describe cómo configurar una cuenta AWS forense como punto de partida para desarrollar las capacidades forenses de su organización y ayudar a mejorar su preparación para responder a los incidentes de seguridad (IR).

Las siguientes guías proporcionan patrones de arquitectura para tipos de aplicaciones específicos. Es posible que desee centrarse en ellos después de crear su arquitectura de seguridad básica:

- AWS SRA: AI security proporciona recomendaciones de arquitectura de seguridad para diseñar y crear aplicaciones que incorporen capacidades de IA generativa mediante el uso de servicios de IA AWS generativa.
- AWS SRA: IoT proporciona recomendaciones de arquitectura de seguridad para diseñar y construir aplicaciones de IoT. AWS

Además, en la siguiente guía se describen los patrones de arquitectura que se ajustan a marcos normativos o de cumplimiento específicos:

- AWS La arquitectura de referencia de privacidad (AWS PRA) proporciona una arquitectura de seguridad para las aplicaciones que procesan datos personales y debe cumplir con amplios requisitos de cumplimiento de la privacidad, como el Reglamento General de Protección de Datos (GDPR), la Ley de Privacidad del Consumidor de California (CCPA) o la Ley General de Protección de Datos de Brasil (LGPD). La AWS PRA proporciona un conjunto de directrices específicas para el diseño y la configuración de los controles de privacidad en. Servicios de AWS

Le recomendamos que comience con la AWS SRA (guía de arquitectura básica) para comprender la arquitectura fundamental y, después, consulte las guías complementarias para aprovechar las funcionalidades e implementaciones avanzadas. Para obtener más información sobre este conjunto de contenido, consulte Arquitectura de referencia AWS de seguridad.

> **Diagramas de arquitectura**
>
> Para personalizar los diagramas de arquitectura de referencia de la biblioteca AWS SRA en función de las necesidades de su empresa, puede descargar el siguiente archivo.zip y extraer su contenido.
>
> Descarga el archivo fuente del diagrama (PowerPointformato Microsoft)

El valor de la AWS SRA

Influya en el futuro de la arquitectura de referencia de AWS seguridad (AWS SRA) realizando una breve encuesta.

AWS cuenta con un amplio (y creciente) conjunto de servicios de seguridad y relacionados con la seguridad. Los clientes han expresado su agradecimiento por la información detallada disponible en la documentación de nuestro servicio, las publicaciones de blog, los tutoriales, las cumbres y las conferencias. También nos dicen que quieren entender mejor el panorama general y obtener una visión estratégica de los servicios de AWS seguridad. Cuando trabajamos con los clientes para comprender mejor lo que necesitan, surgen tres prioridades:

- Los clientes desean más información y patrones recomendados sobre cómo pueden implementar, configurar y operar los servicios de AWS seguridad de manera integral. ¿En qué cuentas y con qué objetivos de seguridad se deben implementar y administrar los servicios? ¿Hay una cuenta de seguridad en la que deban operar todos o la mayoría de los servicios? ¿Cómo influye la elección de la ubicación (unidad organizativa o unidad organizativa Cuenta de AWS) en los objetivos de seguridad? ¿Qué ventajas y desventajas (consideraciones de diseño) deben tener en cuenta los clientes?
- Los clientes están interesados en ver diferentes perspectivas para organizar de forma lógica los numerosos servicios de seguridad. AWS Más allá de la función principal de cada servicio (por ejemplo, los servicios de identidad o los servicios de registro), estos puntos de vista alternativos ayudan a los clientes a planificar, diseñar e implementar su arquitectura de seguridad. Un ejemplo que se comparte más adelante en este documento agrupa los servicios según los niveles de protección alineados con la estructura recomendada de su AWS entorno.
- Los clientes buscan orientación y ejemplos para integrar los servicios de seguridad de la manera más eficaz. Por ejemplo, ¿cuál es la mejor manera de alinearse y conectarse AWS Config con otros servicios para hacer el trabajo pesado de los procesos automatizados de auditoría y supervisión? Los clientes solicitan orientación sobre la forma en que cada servicio de AWS seguridad depende de otros servicios de seguridad o los apoya.

Abordamos cada uno de estos aspectos en la AWS SRA. La primera prioridad de la lista (a dónde van las cosas) es centrarse en el diagrama de arquitectura principal y en las discusiones que lo acompañan en este documento. Proporcionamos una AWS Organizations arquitectura recomendada

y una account-by-account descripción de qué servicios van a cada lugar. Para empezar con la segunda prioridad de la lista (cómo pensar en el conjunto completo de servicios de seguridad), lea la sección Aplicar los servicios de seguridad en toda AWS la organización. En esta sección se describe una forma de agrupar los servicios de seguridad según la estructura de los elementos de AWS la organización. Además, esas mismas ideas se reflejan en el análisis de la cuenta de aplicaciones, que destaca cómo se pueden operar los servicios de seguridad para centrarse en determinadas capas de la cuenta: las instancias de Amazon Elastic Compute Cloud (Amazon EC2), las redes de Amazon Virtual Private Cloud (Amazon VPC) y la cuenta más amplia. Por último, la tercera prioridad (la integración de servicios) se refleja en toda la guía, especialmente en la discusión de los servicios individuales en las guías de análisis detallado de la biblioteca AWS SRA y el código en el repositorio de códigos de la AWS SRA.

¿Cómo usar la SRA AWS

Existen diferentes formas de utilizar la AWS SRA en función del punto en el que se encuentre en el proceso de adopción de la nube. Esta es una lista de formas de obtener el máximo conocimiento de los activos de la AWS SRA (diagrama de arquitectura, orientación escrita y ejemplos de código).

- Defina el estado objetivo de su propia arquitectura de seguridad.

  Tanto si acaba de empezar su Nube de AWS viaje (configurar su primer conjunto de cuentas) como si planea mejorar un AWS entorno establecido, la AWS SRA es el lugar ideal para empezar a crear su arquitectura de seguridad. Comience con una base integral de estructura contable y servicios de seguridad y, a continuación, ajústelos en función de su conjunto tecnológico, sus habilidades, sus objetivos de seguridad y sus requisitos de conformidad específicos. Si sabe que va a crear y lanzar más cargas de trabajo, puede utilizar su versión personalizada de la AWS SRA como base para la arquitectura de referencia de seguridad de su organización. Para saber cómo puede alcanzar el estado objetivo descrito por la AWS SRA, consulte la sección Creación de su arquitectura de seguridad: un enfoque gradual.
- Revise (y revise) los diseños y las capacidades que ya ha implementado.

  Si ya tiene un diseño e implementación de seguridad, vale la pena tomarse un tiempo para comparar lo que tiene con la AWS SRA. La AWS SRA está diseñada para ser integral y proporciona una base de diagnóstico para revisar su propia seguridad. Si sus diseños de seguridad se ajustan a la AWS SRA, puede estar más seguro de que está siguiendo las mejores prácticas a la hora de utilizarla. Servicios de AWS Si sus diseños de seguridad difieren o incluso no están de acuerdo con las directrices de la AWS SRA, esto no es necesariamente una señal

de que esté haciendo algo mal. En cambio, esta observación le brinda la oportunidad de revisar su proceso de toma de decisiones. Existen razones comerciales y tecnológicas legítimas por las que podría desviarse de las mejores prácticas de la AWS SRA. Es posible que sus requisitos particulares de conformidad, normativa o seguridad de la organización requieran configuraciones de servicio específicas. O bien, en lugar de utilizarlas Servicios de AWS, es posible que prefiera una función para un producto AWS Partner Network o una aplicación personalizada que haya creado y gestionado. A veces, durante esta revisión, es posible que descubra que sus decisiones anteriores se basaron en tecnologías, AWS funciones o limitaciones empresariales antiguas que ya no se aplican. Es una buena oportunidad para revisar las actualizaciones, priorizarlas y añadirlas al lugar correspondiente de su cartera de tareas de ingeniería. Independientemente de lo que descubra al evaluar su arquitectura de seguridad a la luz de la AWS SRA, le resultará útil documentar ese análisis. Tener ese registro histórico de las decisiones y sus justificaciones puede ayudar a informar y priorizar las decisiones futuras.

- Inicie la implementación de su propia arquitectura de seguridad.

  AWS Los módulos de infraestructura como código (IaC) de SRA proporcionan una forma rápida y fiable de empezar a crear e implementar su arquitectura de seguridad. Estos módulos se describen con más detalle en la sección del repositorio de código y en el repositorio público GitHub . No solo permiten a los ingenieros basarse en ejemplos de alta calidad de los patrones de la guía de la AWS SRA, sino que también incorporan los controles de seguridad recomendados, como las políticas de contraseñas de IAM, el acceso público a las cuentas bloqueadas del Amazon Simple Storage Service (Amazon S3), el acceso público a las cuentas bloqueadas, el cifrado predeterminado de EC2 Amazon Elastic Block Store (Amazon EBS) y la integración AWS Control Tower para aplicar o eliminar los controles a medida que se incorporan nuevos controles. o fuera de servicio. Cuentas de AWS

- Obtenga más información sobre los servicios y capacidades de seguridad. AWS

  Las directrices y los debates de la AWS SRA incluyen características importantes, así como consideraciones sobre la implementación y la administración de los servicios individuales de AWS seguridad y relacionados con la seguridad. Una característica de la AWS SRA es que proporciona una introducción de alto nivel sobre la variedad de los servicios de AWS seguridad y cómo funcionan juntos en un entorno de múltiples cuentas. Esto complementa el análisis profundo de las funciones y la configuración de cada servicio que se encuentra en otras fuentes. Un ejemplo de ello es el análisis de cómo AWS Security Hub Cloud Security Posture Management (AWS Security Hub CSPM) incorpora los hallazgos de seguridad de una variedad de Servicios de AWS AWS Partner productos e incluso de sus propias aplicaciones.

- Organice un debate sobre el gobierno de la organización y las responsabilidades en materia de seguridad.

  Un elemento importante al diseñar e implementar cualquier arquitectura o estrategia de seguridad es comprender qué miembros de la organización tienen qué responsabilidades relacionadas con la seguridad. Por ejemplo, la cuestión de dónde agrupar y supervisar los hallazgos de seguridad está vinculada a la cuestión de qué equipo será responsable de esa actividad. ¿Todos los hallazgos de la organización son supervisados por un equipo central que necesita acceder a una cuenta específica de Security Tooling? ¿O son los equipos de aplicaciones individuales (o unidades de negocio) responsables de determinadas actividades de supervisión y, por lo tanto, necesitan acceder a determinadas herramientas de alerta y supervisión? Como otro ejemplo, si su organización tiene un grupo que administra todas las claves de cifrado de forma centralizada, eso influirá en quién tiene permiso para crear AWS Key Management Service (AWS KMS) claves y en qué cuentas se administrarán esas claves. Comprender las características de su organización (los distintos equipos y responsabilidades) le ayudará a diseñar la SRA para que se adapte mejor a sus necesidades. AWS Por el contrario, a veces, el debate sobre la arquitectura de seguridad se convierte en el impulso para analizar las responsabilidades organizativas existentes y considerar los posibles cambios. AWS recomienda un proceso de toma de decisiones descentralizado en el que los equipos de carga de trabajo sean responsables de definir los controles de seguridad en función de sus funciones y requisitos de carga de trabajo. El objetivo de un equipo centralizado de seguridad y gobierno es crear un sistema que permita a los propietarios de la carga de trabajo tomar decisiones informadas y a todas las partes obtener visibilidad de la configuración, los hallazgos y los eventos. La AWS SRA puede ser un medio para identificar e informar estas discusiones.

Directrices clave de implementación de la SRA AWS

Estas son ocho conclusiones clave de la AWS SRA que debe tener en cuenta al diseñar e implementar su seguridad.

- AWS Organizations y una estrategia multicuenta adecuada son elementos necesarios de su arquitectura de seguridad. La separación adecuada de las cargas de trabajo, los equipos y las funciones constituye la base para separar las tareas y defense-in-depth las estrategias. La guía trata este tema con más detalle en una sección posterior.
- Defense-in-depth es una consideración de diseño importante a la hora de seleccionar los controles de seguridad para su organización. Le ayuda a introducir los controles de seguridad adecuados

en las diferentes capas de la AWS Organizations estructura, lo que ayuda a minimizar el impacto de un problema: si hay un problema en una capa, existen controles que aíslan otros recursos de TI valiosos. La AWS SRA demuestra cómo Servicios de AWS funcionan las diferentes capas del conjunto de AWS tecnologías y cómo el uso combinado de esos servicios le ayuda a lograrlo. defense-in-depth Este defense-in-depth concepto AWS se analiza con más detalle en una sección posterior con ejemplos de diseño que se muestran en la cuenta de aplicaciones.

- Utilice la amplia variedad de componentes básicos de seguridad en múltiples Servicios de AWS y funciones para crear una infraestructura de nube sólida y resistente. Al adaptar la AWS SRA a sus necesidades particulares, tenga en cuenta no solo la función Servicios de AWS y las características principales (por ejemplo, la autenticación, el cifrado, la supervisión o la política de permisos), sino también la forma en que se integran en la estructura de su arquitectura. En una sección posterior de la guía se describe cómo funcionan algunos servicios en toda AWS la organización. Otros servicios funcionan mejor en una sola cuenta, y algunos están diseñados para conceder o denegar permisos a directores individuales. Tener en cuenta estas dos perspectivas le ayuda a crear un enfoque de seguridad por capas más flexible.
- Siempre que sea posible (tal y como se detalla en secciones posteriores), utilice esta opción, Servicios de AWS que se pueda implementar en todas las cuentas (distribuidas en lugar de centralizadas) y cree un conjunto coherente de barreras de protección compartidas que puedan ayudar a proteger sus cargas de trabajo contra el uso indebido y a reducir el impacto de los eventos de seguridad. La AWS SRA utiliza AWS Security Hub CSPM (monitoreo centralizado de búsquedas y controles de cumplimiento), Amazon GuardDuty (detección de amenazas y detección de anomalías), AWS Config (monitoreo de recursos y detección de cambios), IAM Access Analyzer (monitoreo de acceso a los recursos), AWS CloudTrail (registro de la actividad de la API del servicio en todo su entorno) y Amazon Macie (clasificación de Servicios de AWS datos) como conjunto base que se implementará en todos. Cuenta de AWS
- Utilice la función de administración delegada de AWS Organizations, cuando sea compatible, como se explica más adelante en la sección de administración delegada de la guía. Esto le permite registrar una cuenta de AWS miembro como administrador de los servicios compatibles. La administración delegada proporciona flexibilidad para que los distintos equipos de la empresa utilicen cuentas independientes, según corresponda a sus responsabilidades, para gestionar Servicios de AWS todo el entorno. Además, el uso de un administrador delegado le ayuda a limitar el acceso a la cuenta de administración y a administrar la sobrecarga de permisos de la cuenta de AWS Organizations administración.
- Implemente la supervisión, la administración y la gobernanza centralizadas en todas sus AWS organizaciones. Al utilizar estas funciones Servicios de AWS compatibles con la agregación

de varias cuentas (y, a veces, de varias regiones), junto con las funciones de administración delegada, permite a sus equipos centrales de ingeniería de seguridad, redes y nube tener una amplia visibilidad y control sobre la configuración de seguridad y la recopilación de datos adecuadas. Además, los datos se pueden devolver a los equipos de carga de trabajo para que puedan tomar decisiones de seguridad eficaces en una fase temprana del ciclo de vida del desarrollo del software (SDLC).

- Úselo AWS Control Tower para configurar y administrar su AWS entorno de múltiples cuentas con la implementación de controles de seguridad prediseñados para impulsar su arquitectura de referencia de seguridad. AWS Control Tower proporciona un plan para proporcionar administración de identidades, acceso federado a las cuentas, registro centralizado y flujos de trabajo definidos para el aprovisionamiento de cuentas adicionales. A continuación, puede utilizar la solución Customizations for AWS Control Tower (cFCT) para basar las cuentas gestionadas AWS Control Tower con controles de seguridad, configuraciones de servicio y gobernanza adicionales, como lo demuestra el repositorio de códigos de la SRA. AWS La función de fábrica de cuentas aprovisiona automáticamente las nuevas cuentas con plantillas configurables basadas en la configuración de cuentas aprobada para estandarizar las cuentas de sus organizaciones. AWS También puede extender la gobernanza a una persona existente Cuenta de AWS inscribiéndola en una unidad organizativa (OU) que ya esté regida por ella. AWS Control Tower
- Los ejemplos de código de la AWS SRA muestran cómo se puede automatizar la implementación de los patrones de la guía de la AWS SRA mediante el uso de la infraestructura como código (IaC). Al codificar los patrones, puede tratar la IaC como cualquier otra aplicación de su organización y automatizar las pruebas antes de implementar el código. La IaC también ayuda a garantizar la coherencia y la repetibilidad mediante la implementación de barreras de protección en varios entornos (por ejemplo, SDLC o específicos de una región). Los ejemplos de código SRA se pueden implementar en un entorno de varias cuentas, con o sin él. AWS Organizations AWS Control Tower Las soluciones de este repositorio que se requieren se AWS Control Tower han implementado y probado en un AWS Control Tower entorno mediante AWS CloudFormation el uso de personalizaciones para AWS Control Tower (cFCT). Las soluciones que no lo requieren se AWS Control Tower han probado en un AWS Organizations entorno mediante el uso.AWS CloudFormation Si no la usa AWS Control Tower, puede usar la solución de implementación AWS Organizations basada en datos.

Aspectos básicos de seguridad

Influya en el futuro de la arquitectura de referencia de AWS seguridad (AWS SRA) realizando una breve encuesta.

La AWS SRA se alinea con tres fundamentos de AWS seguridad: el Marco de Adopción de la AWS Nube (AWS CAF), AWS Well-Architected y el Modelo de Responsabilidad Compartida. AWS

AWS Professional Services creó el AWS CAF para ayudar a las empresas a diseñar y seguir un camino acelerado hacia una adopción exitosa de la nube. La orientación y las mejores prácticas que ofrece el marco le ayudan a desarrollar un enfoque integral de la computación en nube en toda su empresa y durante todo su ciclo de vida de TI. La AWS CAF organiza la orientación en seis áreas de enfoque, denominadas perspectivas. Cada perspectiva abarca distintas responsabilidades que pertenecen a las partes interesadas relacionadas con la funcionalidad o que las administran. En general, las perspectivas de negocio, personas y gobernanza se centran en las capacidades empresariales, mientras que las perspectivas de plataforma, seguridad y operaciones se centran en las capacidades técnicas.

La perspectiva de seguridad de la AWS CAF le ayuda a estructurar la selección e implementación de los controles en toda su empresa. Seguir las AWS recomendaciones actuales del pilar de seguridad puede ayudarle a cumplir sus requisitos empresariales y normativos.

AWS WellArchitected ayuda a los arquitectos de la nube a crear una infraestructura segura, de alto rendimiento, resiliente y eficiente para sus aplicaciones y cargas de trabajo. El marco se basa en seis pilares (excelencia operativa, seguridad, confiabilidad, eficiencia del rendimiento, optimización de costos y sostenibilidad) y proporciona un enfoque coherente para que los AWS clientes y socios evalúen las arquitecturas e implementen diseños que puedan ampliarse con el tiempo. Creemos que contar con cargas de trabajo de Well-Architected aumenta en gran medida la probabilidad de éxito empresarial.

El pilar de seguridad de Well-Architected Framework describe cómo aprovechar las tecnologías en la nube para ayudar a proteger los datos, los sistemas y los activos de una manera que pueda mejorar su postura de seguridad. Esto le ayudará a cumplir sus requisitos empresariales y normativos siguiendo las recomendaciones actuales AWS . Hay áreas de enfoque adicionales de Well-Architected Framework que proporcionan más contexto para dominios específicos, como la

gobernanza, la tecnología sin servidores, la inteligencia artificial y el aprendizaje automático y los juegos. Se conocen como lentes AWS Well-Architected.

La seguridad y el cumplimiento son una responsabilidad compartida entre el cliente AWS y el cliente. Este modelo compartido puede ayudarlo a aliviar la carga operativa, ya que AWS opera, administra 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. Por ejemplo, usted asume la responsabilidad y la administración del sistema operativo huésped (incluidas las actualizaciones y los parches de seguridad), el software de la aplicación, el cifrado de datos del lado del servidor, las tablas de rutas del tráfico de la red y la configuración del firewall del grupo AWS de seguridad proporcionado. En el caso de los servicios abstractos, como Amazon S3 y Amazon AWS DynamoDB, opera la capa de infraestructura, el sistema operativo y las plataformas, y usted accede a los puntos de enlace para almacenar y recuperar datos. Usted es responsable de administrar sus datos (incluidas las opciones de cifrado), clasificar sus activos y utilizar las herramientas de IAM para aplicar los permisos adecuados. Este modelo compartido suele describirse diciendo que AWS es responsable de la seguridad de la nube (es decir, de proteger la infraestructura en la que se ejecutan todos los servicios que se ofrecen en ella Nube de AWS) y que usted es responsable de la seguridad en la nube (según lo determinen los Nube de AWS servicios que seleccione).

Dentro de las directrices que proporcionan estos documentos fundamentales, dos conjuntos de conceptos son particularmente relevantes para el diseño y la comprensión de la AWS SRA: las capacidades de seguridad y los principios de diseño de la seguridad.

Capacidades de seguridad

La perspectiva de seguridad de la AWS CAF describe nueve capacidades que le ayudan a lograr la confidencialidad, integridad y disponibilidad de sus datos y cargas de trabajo en la nube.

- La gobernanza de la seguridad permite desarrollar y comunicar las funciones, responsabilidades, políticas, procesos y procedimientos de seguridad en todo el entorno de AWS su organización.
- Garantía de seguridad para supervisar, evaluar, gestionar y mejorar la eficacia de sus programas de seguridad y privacidad.
- Gestión de identidades y accesos para gestionar las identidades y los permisos a escala.
- Detección de amenazas para comprender e identificar posibles errores de configuración de seguridad, amenazas o comportamientos inesperados.
- Gestión de vulnerabilidades para identificar, clasificar, corregir y mitigar de forma continua las vulnerabilidades de seguridad.

- Protección de la infraestructura para ayudar a validar que los sistemas y servicios de sus cargas de trabajo estén protegidos.
- Protección de datos para mantener la visibilidad y el control de los datos y de cómo se accede a ellos y se utilizan en su organización.
- Seguridad de las aplicaciones para ayudar a detectar y abordar las vulnerabilidades de seguridad durante el proceso de desarrollo del software.
- Respuesta a incidentes para reducir los posibles daños mediante una respuesta eficaz a los incidentes de seguridad.

Principios de diseño de seguridad

El pilar de seguridad del Well-Architected Framework recoge un conjunto de siete principios de diseño que convierten áreas de seguridad específicas en una guía práctica que puede ayudarlo a fortalecer la seguridad de sus cargas de trabajo. Mientras que las capacidades de seguridad enmarcan la estrategia de seguridad general, estos principios del Marco de Well-Architected describen lo que puede empezar a hacer. Están reflejados de manera muy deliberada en este AWS SRA y consisten en lo siguiente:

- Implemente una base de identidad sólida: implemente el principio de privilegios mínimos y exija la separación de funciones con la autorización adecuada para cada interacción con sus AWS recursos. Centralice la administración de identidades y busque eliminar la dependencia de las credenciales a largo plazo.
- Habilite la trazabilidad: supervise, genere alertas y audite las acciones y los cambios en su entorno en tiempo real. Integre la recopilación de registros y métricas con sistemas para investigar y tomar medidas automáticamente.
- Aplique la seguridad en todos los niveles – Aplique un defense-in-depth enfoque con varios controles de seguridad. Aplique varios tipos de controles (por ejemplo, controles preventivos y de detección) a todas las capas, incluidos el borde de la red, la nube privada virtual (VPC), el equilibrio de carga, los servicios de instancia y procesamiento, el sistema operativo, la configuración de aplicaciones y el código.
- Automatice las mejores prácticas de seguridad: los mecanismos de seguridad automatizados y basados en software mejoran su capacidad de escalar de forma segura de forma más rápida y rentable. Cree arquitecturas seguras e implemente controles que se definan y administren como código en plantillas con control de versiones.

- Proteja los datos en tránsito y en reposo: clasifique los datos según sus niveles de confidencialidad y utilice mecanismos como el cifrado, la tokenización y el control de acceso, cuando proceda.
- Mantenga a las personas alejadas de los datos – Utilice mecanismos y herramientas para reducir o eliminar la necesidad de acceder directamente a los datos o procesarlos manualmente. De esta forma, se reducen los errores humanos y el riesgo de una mala gestión o modificación al gestionar información confidencial.
- Prepárese para los eventos de seguridad: prepárese para un incidente con políticas y procesos de gestión e investigación de incidentes que se ajusten a los requisitos de su organización. Ejecute simulaciones de respuesta frente a incidencias y use herramientas con automatización para aumentar la velocidad de detección, investigación y recuperación.

Cómo utilizar la AWS SRA con AWS CAF y Well-Architected Framework AWS

AWS CAF, AWS Well-Architected Framework AWS y SRA son marcos complementarios que funcionan juntos para respaldar sus esfuerzos de migración y modernización a la nube.

- La AWS CAF aprovecha la AWS experiencia y las mejores prácticas para ayudarlo a alinear los valores de la adopción de la nube con los resultados empresariales deseados. Utilice la AWS CAF para identificar y priorizar las oportunidades de transformación, evaluar y mejorar la preparación para la nube y desarrollar de forma iterativa su hoja de ruta de transformación.
- El AWS Well-Architected Framework AWS proporciona recomendaciones para crear una infraestructura segura, de alto rendimiento, resiliente y eficiente para una variedad de aplicaciones y cargas de trabajo que cumplan con los resultados de su negocio.
- La AWS SRA le ayuda a comprender cómo implementar y gobernar los servicios de seguridad de una manera que se alinee con las recomendaciones de la AWS CAF y el Well-Architected AWS Framework.

Por ejemplo, la perspectiva de seguridad de la AWS CAF sugiere que evalúe cómo administrar de forma centralizada las identidades de sus empleados y su autenticación. AWS En función de esta información, puede decidir utilizar una solución de proveedor de identidad corporativa (IdP) nueva o existente, como Okta, Active Directory o Ping Identity para este fin. Sigue las instrucciones del AWS Well-Architected Framework y decide integrar su IdP con el para ofrecer a sus empleados una experiencia de inicio de sesión único que pueda sincronizar AWS IAM Identity Center las

membresías y permisos de sus grupos. Debe revisar la recomendación de la AWS SRA de habilitar el Centro de Identidad de IAM en la cuenta de administración de su AWS organización y administrarlo a través de una cuenta de herramientas de seguridad utilizada por su equipo de operaciones de seguridad. Este ejemplo ilustra cómo la AWS CAF le ayuda a tomar las decisiones iniciales sobre la postura de seguridad deseada, el AWS Well-Architected Framework proporciona orientación sobre cómo evaluar Servicios de AWS los que están disponibles para cumplir ese objetivo y, a continuación, AWS la SRA proporciona recomendaciones sobre cómo implementar y gobernar los servicios de seguridad que seleccione.

Componentes básicos de la SRA: AWS Organizations cuentas y barandas

Influya en el futuro de la arquitectura de referencia de AWS seguridad (AWS SRA) realizando una breve encuesta.

AWS La mejor forma de utilizar los servicios de seguridad, sus controles y sus interacciones es con una estrategia AWS multicuenta y con barreras de gestión de identidades y accesos. Estas barreras permiten implementar los privilegios mínimos, la separación de funciones y la privacidad, y sirven de apoyo a la hora de decidir qué tipos de controles son necesarios, dónde se gestiona cada servicio de seguridad y cómo pueden compartir los datos y los permisos en la SRA. AWS

An Cuenta de AWS establece límites de seguridad, acceso y facturación para sus AWS recursos y le permite lograr la independencia y el aislamiento de los recursos. El uso de varias cuentas Cuentas de AWS desempeña un papel importante a la hora de cumplir con los requisitos de seguridad, tal como se explica en la Cuentas de AWS sección Ventajas de utilizar varias cuentas del documento técnico Cómo organizar el AWS entorno con varias cuentas. Por ejemplo, puede organizar sus cargas de trabajo en cuentas independientes y cuentas grupales dentro de una unidad organizativa (OU) en función de la función, los requisitos de conformidad o un conjunto común de controles, en lugar de reflejar la estructura de informes de su empresa. Tenga en cuenta la seguridad y la infraestructura para que su empresa pueda establecer barreras comunes a medida que crecen sus cargas de trabajo. Este enfoque proporciona límites y controles sólidos entre las cargas de trabajo. La separación a nivel de cuenta, en combinación con AWS Organizations, se utiliza para aislar los entornos de producción de los entornos de desarrollo y prueba, o para proporcionar un límite lógico sólido entre las cargas de trabajo que procesan datos de diferentes clasificaciones, como el Estándar de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS) o la Ley de Portabilidad y Responsabilidad de los Seguros de Salud (HIPAA). Si bien puede comenzar su AWS viaje con una sola cuenta, le AWS recomienda que configure varias cuentas a medida que sus cargas de trabajo aumenten de tamaño y complejidad.

Los permisos le permiten especificar el acceso a AWS los recursos. Los permisos se conceden a las entidades de IAM conocidas como principales (usuarios, grupos y roles). De forma predeterminada, los directores comienzan sin permisos. Los directores de IAM no pueden hacer nada AWS hasta que usted les conceda los permisos, y usted puede configurar barreras que se apliquen de manera tan

amplia como toda la AWS organización o tan detalladas como una combinación individual de capital, acción, recurso y condiciones.

AWS Organizations Se utiliza por motivos de seguridad

Influya en el futuro de la arquitectura de referencia de AWS seguridad (AWS SRA) realizando una breve encuesta.

AWS Organizationsle ayuda a administrar y gobernar su entorno de forma centralizada a medida que crece y escala sus AWS recursos. Al AWS Organizations utilizarlos, puede crear nuevos, asignar recursos Cuentas de AWS, agrupar cuentas para organizar sus cargas de trabajo mediante programación y aplicar políticas a las cuentas o grupos de cuentas para su control. Una AWS organización consolida las tuyas Cuentas de AWS para que puedas administrarlas como una sola unidad. Tiene una cuenta de administración y cero o más cuentas de miembros. La mayoría de las cargas de trabajo residen en las cuentas de los miembros, a excepción de algunos procesos gestionados de forma centralizada que deben residir en la cuenta de administración o en cuentas asignadas como administradores delegados, por ejemplo. Servicios de AWS Puede proporcionar herramientas y acceso desde una ubicación central para que su equipo de seguridad gestione las necesidades de seguridad en nombre de una AWS organización. Puede reducir la duplicación de recursos al compartir los recursos críticos dentro de su AWS organización. Puede agrupar las cuentas en unidades AWS organizativas (OUs), que pueden representar diferentes entornos en función de los requisitos y el propósito de la carga de trabajo. AWS Organizations también proporciona varias políticas que le permiten aplicar de forma centralizada controles de seguridad adicionales a todas las cuentas de los miembros de sus organizaciones. Esta sección se centra en las políticas de control de servicios (SCPs), las políticas de control de recursos (RCPs) y las políticas declarativas.

Con AWS Organizations, puede usar SCPsy aplicar barreras de permisos RCPsa nivel de AWS organización, unidad organizativa o cuenta. SCPs son barreras que se aplican a los directores de la cuenta de una organización, con la excepción de la cuenta de administración (que es una de las razones para no ejecutar cargas de trabajo en esta cuenta). Al conectar un SCP a una OU, el SCP lo heredan el SCP y las cuentas incluidas en esa OU. OUs SCPs no conceda ningún permiso. En su lugar, especifican los permisos máximos disponibles para los directores de una AWS organización, unidad organizativa o cuenta. Aún así, debe adjuntar políticas basadas en la identidad o en los recursos a los directores o recursos de su empresa para Cuentas de AWS poder concederles

permisos. Por ejemplo, si un SCP deniega el acceso a todo Amazon S3, el principal afectado por el SCP no tendrá acceso a Amazon S3 aunque se le conceda el acceso de forma explícita a través de una política de IAM. Para obtener más información sobre cómo se evalúan las políticas de SCPs IAM, su función y cómo se concede o deniega el acceso en última instancia, consulte la lógica de evaluación de políticas en la documentación de IAM.

RCPs son barreras que se aplican a los recursos de las cuentas de una organización, independientemente de si los recursos pertenecen a la misma organización. Por ejemplo SCPs, RCPs no afectan a los recursos de la cuenta de administración ni conceden ningún permiso. Al adjuntar un RCP a una OU, el RCP lo hereda el RCP OUs y las cuentas de la OU lo heredan. RCPs proporcionan un control central sobre los permisos máximos disponibles para los recursos de su organización y, actualmente, admiten un subconjunto de. Servicios de AWS Cuando diseñe SCPs para usted OUs, le recomendamos que evalúe los cambios mediante el simulador de políticas de IAM. También deberías revisar los datos del servicio a los que se accedió por última vez en IAM y utilizarlos AWS CloudTrail para registrar el uso del servicio a nivel de la API a fin de comprender el impacto potencial de los cambios en el SCP.

SCPs y RCPs son controles independientes. Puede optar por habilitar solo SCPs o RCPs usar ambos tipos de políticas juntas en función de los controles de acceso que desee aplicar. Por ejemplo, si quiere impedir que los directores de su organización accedan a recursos ajenos a ella, aplique este control mediante SCPs. Si desea restringir o impedir que las identidades externas accedan a sus recursos, aplique este control mediante RCPs. Para obtener más información y casos de uso de RCPs y SCPs, consulte Uso SCPs y RCPs en la AWS Organizations documentación.

Puede utilizar políticas AWS Organizations declarativas para declarar y aplicar de forma centralizada la configuración que desee para una determinada escala Servicio de AWS en toda la organización. Por ejemplo, puede bloquear el acceso público a Internet a los recursos de Amazon VPC en su organización. A diferencia de las políticas de autorización, como SCPs y RCPs, las políticas declarativas se aplican en el plano de control de un AWS servicio. Las políticas de autorización regulan el acceso al servicio APIs, mientras que las políticas declarativas se aplican directamente a nivel de servicio para garantizar una intención duradera. Estas políticas ayudan a garantizar que la configuración básica de an Servicio de AWS se mantenga siempre, incluso cuando el servicio introduzca nuevas funciones o APIs. La configuración básica también se mantiene cuando se agregan nuevas cuentas a una organización o cuando se crean nuevas entidades principales y recursos. Las políticas declarativas se pueden aplicar a toda la organización o a cuentas específicas OUs .

Cada uno Cuenta de AWS tiene un único usuario raíz que, de forma predeterminada, tiene todos los permisos para acceder a todos AWS los recursos. Como práctica recomendada de seguridad, te recomendamos que no utilices el usuario root, excepto en algunas tareas que requieren explícitamente un usuario root. Si gestionas varios de ellos AWS Organizations, puedes deshabilitar de forma centralizada el inicio de sesión root y, Cuentas de AWS a continuación, realizar acciones con privilegios root en nombre de todas las cuentas de los miembros. Tras gestionar de forma centralizada el acceso raíz de las cuentas de los miembros, puede eliminar la contraseña del usuario raíz, las claves de acceso y los certificados de firma, y desactivar la autenticación multifactor (MFA) para las cuentas de los miembros. Las cuentas nuevas que se crean mediante un acceso raíz gestionado de forma centralizada no tienen credenciales de usuario raíz de forma predeterminada. Las cuentas de los miembros no pueden iniciar sesión con su usuario raíz ni recuperar la contraseña de su usuario raíz.

AWS Control Towerofrece una forma simplificada de configurar y gestionar varias cuentas. Automatiza la configuración de las cuentas en su AWS organización, automatiza el aprovisionamiento, aplica controles (que incluyen controles preventivos y de detección) y le proporciona un panel de control para mayor visibilidad. Hay una política de administración de IAM adicional, un límite de permisos, que se vincula a entidades de IAM específicas (usuarios o funciones) y establece los permisos máximos que una política basada en la identidad puede conceder a una entidad principal de IAM.

AWS Organizations le ayuda a configurarlos para que se apliquen a todas sus Servicios de AWScuentas. Por ejemplo, puede configurar el registro central de todas las acciones realizadas en su AWS organización utilizando CloudTrail el registro y evitar que las cuentas de los miembros lo deshabiliten. También puede agregar de forma centralizada los datos de las reglas que haya definido mediante el uso AWS Config, de modo que pueda auditar sus cargas de trabajo para comprobar su conformidad y reaccionar rápidamente ante los cambios. Puede utilizarlos AWS CloudFormation StackSetspara gestionar de forma centralizada las CloudFormation pilas en todas las cuentas y OUs en su AWS organización, de forma que pueda aprovisionar automáticamente una nueva cuenta que cumpla con sus requisitos de seguridad.

La configuración predeterminada AWS Organizations admite el uso de listas de denegación SCPs como listas de rechazo. Al utilizar una estrategia de lista de rechazados, los administradores de las cuentas de los miembros pueden delegar todos los servicios y acciones hasta que se cree y adjunte un SCP que deniegue un servicio o conjunto de acciones específicos. Las declaraciones de rechazo requieren menos mantenimiento que una lista de permitidos, ya que no es necesario actualizarlas cuando se AWS añaden nuevos servicios. Las sentencias Deny suelen tener una

longitud de caracteres más corta, por lo que es más fácil mantenerlas dentro del tamaño máximo de SCPs. En una declaración en la que el `Effect` elemento tenga un valor de`Deny`, también puede restringir el acceso a recursos específicos o definir las condiciones para cuando SCPs estén en vigor. Por el contrario, una `Allow` declaración de un SCP se aplica a todos los recursos (`"*"`) y no puede restringirse mediante condiciones. Para obtener más información y ejemplos, consulte Estrategias de uso SCPs en la AWS Organizations documentación.

Consideraciones sobre el diseño

- Como alternativa, para usarlo SCPs como lista de permitidos, debe reemplazar el `FullAWSAccess` SCP administrado por AWS por un SCP que permita explícitamente solo los servicios y acciones que desee permitir. Para habilitar un permiso para una cuenta específica, todos los SCP (desde la raíz hasta cada unidad organizativa en la ruta directa a la cuenta e incluso los adjuntos a la propia cuenta) deben permitir ese permiso. Este modelo es de naturaleza más restrictiva y podría ser adecuado para cargas de trabajo delicadas y altamente reguladas. Este enfoque requiere que permita de forma explícita todos los servicios o acciones de IAM que se interpongan en el trayecto desde la unidad organizativa Cuenta de AWS hasta la unidad organizativa.
- Lo ideal sería utilizar una combinación de estrategias de listas de rechazos y listas de permitidos. Utilice la lista de permitidos para definir la lista de Servicios de AWS permitidos que se pueden utilizar en una AWS organización y adjunte este SCP a la raíz de su AWS organización. Si su entorno de desarrollo permite un conjunto de servicios diferente, adjuntará el correspondiente SCPs a cada unidad organizativa. A continuación, puede utilizar la lista de denegaciones para definir las barreras empresariales denegando de forma explícita determinadas acciones de IAM.
- RCPs se aplican a los recursos de un subconjunto de. Servicios de AWS Para obtener más información, consulte la lista de Servicios de AWS ese soporte RCPs en la AWS Organizations documentación. La configuración predeterminada de las listas de rechazo AWS Organizations admite el uso RCPs de listas de rechazo. Al activarla RCPs en su organización, una política AWS gestionada denominada `RCPFullAWSAccess` se adjunta automáticamente a la raíz de la organización, a todas las unidades organizativas y a todas las cuentas de la organización. No se puede desvincular esta política. Este RCP predeterminado permite que el acceso a todos los principios y acciones pase por una evaluación del RCP. Esto significa que, hasta que comience a crear y adjuntar RCPs, todos sus permisos de IAM actuales seguirán funcionando igual que antes. Esta política

AWS gestionada no concede el acceso. A continuación, puede crear una nueva RCPs lista de sentencias de denegación para bloquear el acceso a los recursos de su organización.

La cuenta de administración, el acceso de confianza y los administradores delegados

Influya en el futuro de la arquitectura de referencia de AWS seguridad (AWS SRA) realizando una breve encuesta.

La cuenta de administración (también llamada cuenta de administración de la AWS organización o cuenta de administración de la organización) es única y se diferencia de todas las demás cuentas existentes. AWS Organizations Es la cuenta que crea la AWS organización. Desde esta cuenta, puede crear cuentas Cuentas de AWS en la AWS organización, invitar a otras cuentas existentes a la AWS organización (ambos tipos se consideran cuentas de miembros), eliminar cuentas de la AWS organización y aplicar las políticas de IAM a la raíz o a las cuentas de la AWS organización. OUs

La cuenta de administración implementa barreras de seguridad universales y despliegues de servicios (por SCPs ejemplo CloudTrail) que afectarán a todas las cuentas de los miembros de la organización. RCPs AWS Para restringir aún más los permisos en la cuenta de administración, esos permisos se pueden delegar en otra cuenta adecuada, como una cuenta de seguridad, siempre que sea posible.

La cuenta de administración tiene las responsabilidades de una cuenta de pago y es responsable de todos los cargos devengados por las cuentas miembro. No puede cambiar la cuenta de administración de una AWS organización. Un solo Cuenta de AWS puede ser miembro de una AWS organización a la vez.

Debido a la funcionalidad y el alcance de la influencia que tiene la cuenta de administración, le recomendamos que limite el acceso a esta cuenta y conceda permisos solo a los roles que los necesiten. Dos funciones que le ayudan a hacerlo son el acceso confiable y el administrador delegado. Puede utilizar el acceso de confianza para permitir Servicio de AWS que un servicio que especifique, denominado servicio de confianza, realice tareas en su AWS organización y sus cuentas en su nombre. Esto implica la concesión de permisos al servicio de confianza, pero no afecta de ninguna otra manera a los permisos para los usuarios o roles de IAM. Puede usar el acceso de confianza para especificar los ajustes y los detalles de configuración que desea que el servicio de

confianza mantenga en las cuentas de su AWS organización en su nombre. Por ejemplo, en la sección de cuentas de administración de la organización de la AWS SRA se explica cómo conceder al CloudTrail servicio un acceso confiable para crear un registro CloudTrail organizativo en todas las cuentas de AWS la organización.

Algunas Servicios de AWS admiten la función de administrador delegado en. AWS Organizations Con esta función, los servicios compatibles pueden registrar una cuenta de AWS miembro en la AWS organización como administrador de las cuentas de la AWS organización en ese servicio. Esta capacidad proporciona flexibilidad a los distintos equipos de la empresa para que utilicen cuentas independientes, según corresponda a sus responsabilidades, y las administren Servicios de AWS en todo el entorno. Los servicios de AWS seguridad de la AWS SRA que actualmente admiten el administrador delegado incluyen IAM Identity Center, AWS Firewall Manager Amazon AWS Config, IAM Access GuardDuty Analyzer, Amazon Macie, Cloud Security Posture Management () AWS Security Hub , Amazon Detective AWS Security Hub CSPM, AWS Audit Manager Amazon Inspector y. AWS Systems Manager La AWS SRA hace hincapié en el uso de la función de administrador delegado como práctica recomendada, y delegamos la administración de los servicios relacionados con la seguridad en la cuenta Security Tooling.

Estructura de cuentas dedicadas

Influya en el futuro de la arquitectura de referencia de AWS seguridad (AWS SRA) realizando una breve encuesta.

An Cuenta de AWS proporciona límites de seguridad, acceso y facturación para sus AWS recursos, y le permite lograr la independencia y el aislamiento de los recursos. De forma predeterminada, no se permite el acceso entre cuentas.

Al diseñar su unidad organizativa y su estructura contable, comience teniendo en cuenta la seguridad y la infraestructura. Recomendamos crear un conjunto de elementos fundamentales OUs para estas funciones específicas, divididos en infraestructura y seguridad OUs. Estas recomendaciones sobre cuentas y unidades organizativas reflejan un subconjunto de nuestras directrices más amplias AWS Organizations y completas para el diseño de estructuras multicuentas. Para obtener un conjunto completo de recomendaciones, consulte Cómo organizar el AWS entorno con varias cuentas en la AWS documentación y en la entrada del blog Prácticas recomendadas para las unidades organizativas con. AWS Organizations

La AWS SRA utiliza las siguientes cuentas para llevar a cabo operaciones de seguridad eficaces en. AWS Estas cuentas dedicadas ayudan a garantizar la separación de funciones, respaldan diferentes políticas de gobierno y acceso para diferentes aplicaciones y datos confidenciales y ayudan a mitigar el impacto de un incidente de seguridad. En los debates que siguen, nos centraremos en las cuentas de producción (de producción) y sus cargas de trabajo asociadas. Las cuentas del ciclo de vida del desarrollo de software (SDLC) (que suelen denominarse cuentas de desarrollo y de prueba) están diseñadas para organizar los resultados y pueden funcionar con un conjunto de políticas de seguridad diferente al de las cuentas de producción.

Cuenta	OU	Función de seguridad
Administración	—	Gobierno y administración centrales de todas Regiones de AWS las cuentas terrestres. El Cuenta de AWS que aloja la raíz de la AWS organización.
Herramientas de seguridad	Seguridad	Dedicado a Cuentas de AWS operar servicios de seguridad de amplia aplicación (como GuardDuty Security Hub CSPM, Audit Manager, Detective, Amazon Inspector y AWS Config) Cuentas de AWS, monitorear y automatizar las alertas y respuestas de seguridad. (En AWS Control Tower, el nombre predeterminado de la cuenta en la OU de seguridad es Cuenta de auditoría).
Archivo de registro	Seguridad	Cuentas de AWS Dedicada a ingerir y archivar todos los registros y copias de seguridad para todos

		Regiones de AWS y. Cuentas de AWS Esto debe diseñarse como un almacenamiento inmutable.
Network	Infraestructura	La puerta de enlace entre su aplicación y el resto de Internet. La cuenta de red aísla los servicios de red, la configuración y el funcionamiento más generales de las cargas de trabajo de las aplicaciones individuales, la seguridad y otras infraestructuras.
Servicios compartidos	Infraestructura	Esta cuenta admite los servicios que utilizan varias aplicaciones y equipos para ofrecer sus resultados. Algunos ejemplos son los servicios de directorio de Identity Center (Active Directory), los servicios de mensajería y los servicios de metadatos.

Aplicación	Cargas de trabajo	Cuentas de AWS que alojan las aplicaciones de la AWS organización y realizan las cargas de trabajo. (A veces se denominan cuentas de carga de trabajo). Las cuentas de aplicaciones deben crearse para aislar los servicios de software, en lugar de asignarla s a sus equipos. Esto hace que la aplicación implement ada sea más resistente a los cambios organizativos.

AWS organización y estructura contable de la AWS SRA

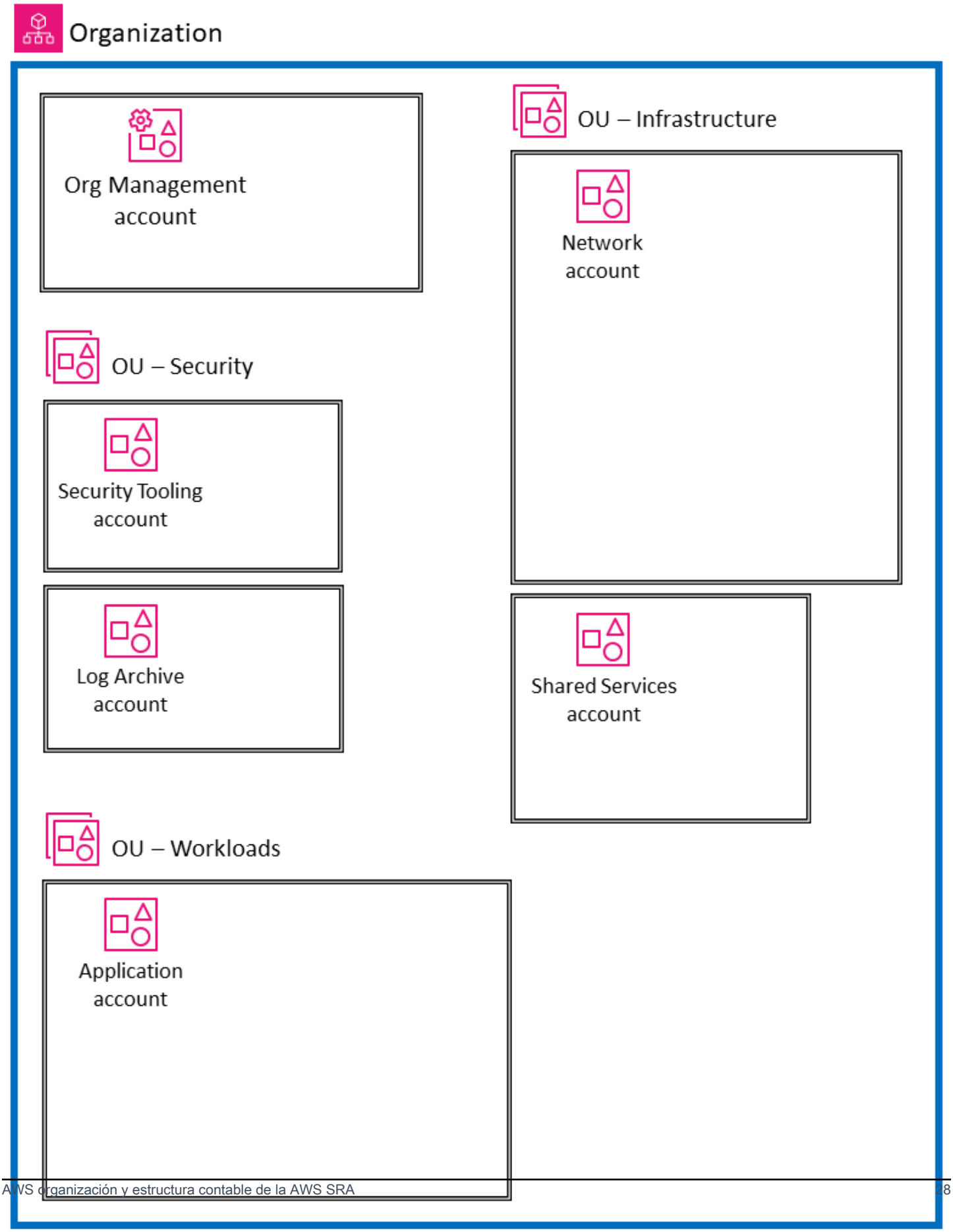
Influya en el futuro de la arquitectura de referencia de AWS seguridad (AWS SRA) realizando una breve encuesta.

El siguiente diagrama captura la estructura de alto nivel de la AWS SRA sin mostrar servicios específicos. Refleja la estructura de cuentas dedicadas analizada en la sección anterior, e incluimos el diagrama aquí para orientar el análisis en torno a los componentes principales de la arquitectura:

- Todas las cuentas que se muestran en el diagrama forman parte de una sola AWS organización.
- En la parte superior izquierda del diagrama se encuentra la cuenta de administración de la organización, que se utiliza para crear la AWS organización.
- Debajo de la cuenta de administración de la organización se encuentra la unidad organizativa de seguridad con dos cuentas específicas: una para Security Tooling y otra para Log Archive.
- En el lado derecho se encuentra la unidad organizativa de infraestructura con la cuenta de red y la cuenta de Shared Services.
- En la parte inferior del diagrama se encuentra la unidad organizativa Workloads, que está asociada a una cuenta de aplicación que aloja la aplicación empresarial.

Según esta guía, todas las cuentas se consideran cuentas de producción (producción) que funcionan en una sola cuenta. Región de AWS La mayoría Servicios de AWS (excepto los servicios globales) tienen un ámbito regional, lo que significa que los planos de control y datos del servicio existen de forma independiente en cada uno de ellos. Región de AWS Por este motivo, debe replicar esta arquitectura en todos los dispositivos Regiones de AWS que vaya a utilizar, a fin de garantizar la cobertura de todo AWS su entorno. Si no tiene ninguna carga de trabajo en un lugar específico Región de AWS, debe deshabilitar la región utilizando SCPso utilizando mecanismos de registro y supervisión. Puede usar Security Hub CSPM para agregar hallazgos y puntuaciones de seguridad de varias regiones de agregación Regiones de AWS a una sola para obtener una visibilidad centralizada.

Cuando se aloja una AWS organización con un gran conjunto de cuentas, resulta beneficioso contar con una capa de organización que facilite el despliegue y el gobierno de las cuentas. AWS Control Tower ofrece una forma sencilla de configurar y gestionar un entorno de AWS múltiples cuentas. Los ejemplos de código AWS SRA del GitHub repositorio muestran cómo se puede utilizar la solución Customizations for AWS Control Tower (cFCT) para implementar AWS las estructuras recomendadas por la SRA.

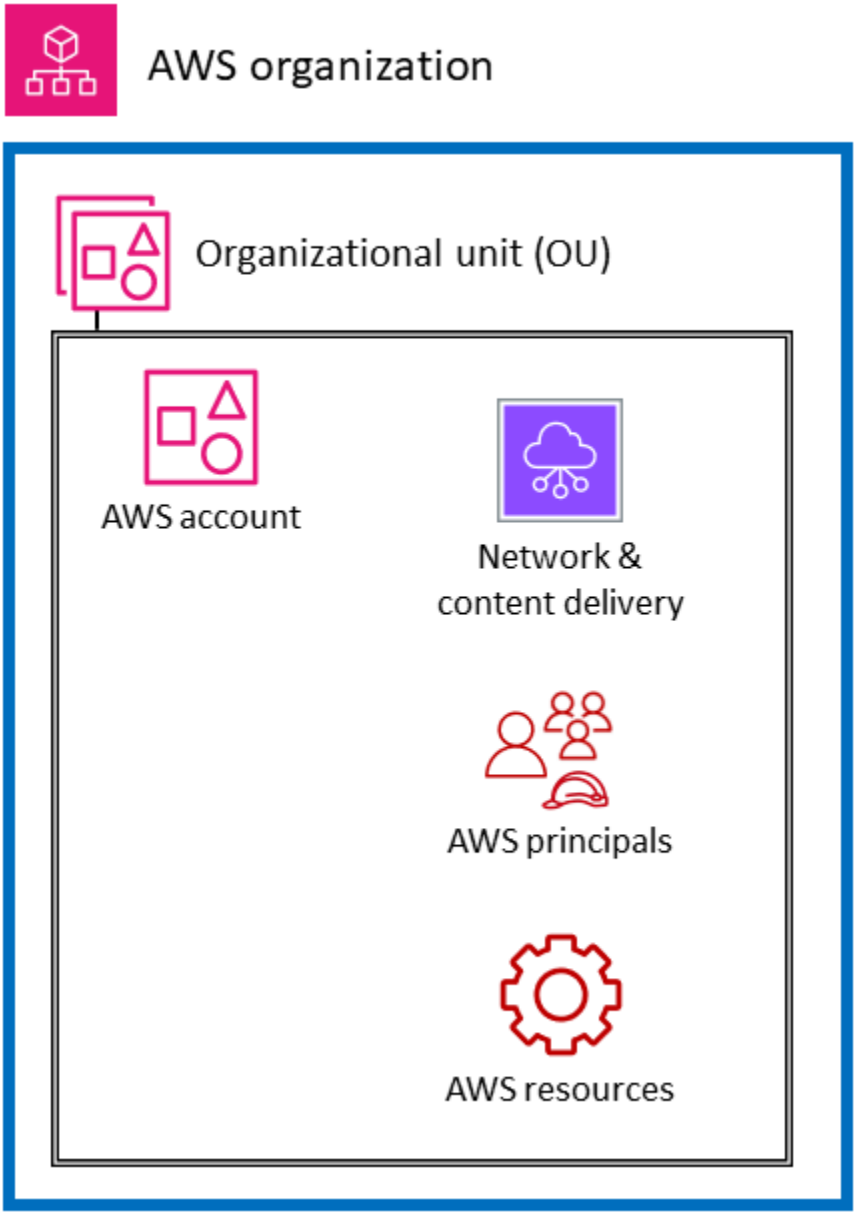

Organization
Org Management account
OU – Infrastructure
Network account
OU – Security
Security Tooling account
Log Archive account
Shared Services account
OU – Workloads
Application account

Aplique servicios de seguridad en toda su organización AWS

Influya en el futuro de la arquitectura de referencia de AWS seguridad (AWS SRA) realizando una breve encuesta.

Como se describió en una sección anterior, los clientes buscan una forma adicional de pensar y organizar estratégicamente el conjunto completo de servicios de AWS seguridad. El enfoque organizativo más común en la actualidad consiste en agrupar los servicios de seguridad por función principal, según la función que desempeñe cada servicio. La perspectiva de seguridad de la AWS CAF enumera nueve capacidades funcionales, que incluyen la administración de identidades y accesos, la protección de la infraestructura, la protección de datos y la detección de amenazas. La Servicios de AWS combinación de estas capacidades funcionales es una forma práctica de tomar decisiones de implementación en cada área. Por ejemplo, cuando se analiza la gestión de identidades y accesos, hay que tener en cuenta la IAM y el IAM Identity Center. A la hora de diseñar la arquitectura de su enfoque de detección de amenazas, esa GuardDuty podría ser su primera consideración.

Como complemento de esta visión funcional, también puede ver su seguridad con una vista estructural transversal. Es decir, además de preguntarse: «¿Cuáles Servicios de AWS debo usar para controlar y proteger mis identidades, mi acceso lógico o mis mecanismos de detección de amenazas?» , también puedes preguntarte: «¿Cuál Servicios de AWS debo aplicar en toda mi AWS organización? ¿Cuáles son los niveles de defensa que debo implementar para proteger las instancias de Amazon EC2 en el núcleo de mi aplicación?» En esta vista, mapea las capas de su AWS entorno Servicios de AWS y las características de las mismas. Algunos servicios y características son ideales para implementar controles en toda la organización de AWS . Por ejemplo, bloquear el acceso público a los buckets de Amazon S3 es un control específico de esta capa. Es preferible hacerlo en la organización raíz en lugar de formar parte de la configuración de la cuenta individual. Es mejor utilizar otros servicios y funciones para ayudar a proteger los recursos individuales dentro de un Cuenta de AWS. La implementación de una autoridad de certificación (CA) subordinada en una cuenta que requiere certificados TLS privados es un ejemplo de esta categoría. Otra agrupación igualmente importante consiste en los servicios que afectan a la capa de red virtual de la infraestructura. AWS El siguiente diagrama muestra seis capas en un AWS entorno típico: AWS organización, unidad organizativa (OU), cuenta, infraestructura de red, entidades principales y recursos.



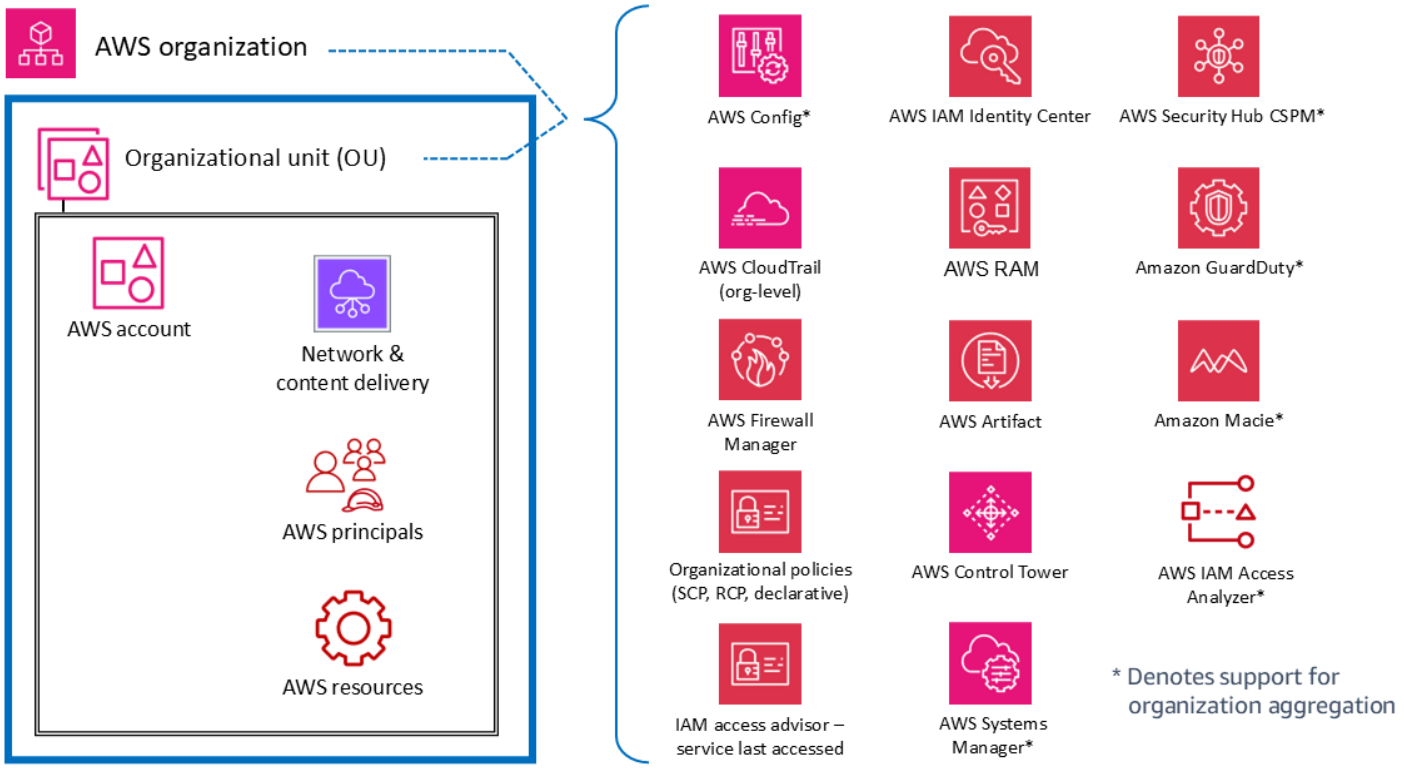
Comprender los servicios en este contexto estructural, incluidos los controles y las protecciones de cada capa, le ayuda a planificar e implementar una defense-in-depth estrategia en todo su AWS entorno. Desde esta perspectiva, puede responder a las preguntas de arriba hacia abajo (por ejemplo, «¿Qué servicios utilizo para implementar controles de seguridad en toda mi AWS organización?») y de abajo hacia arriba (por ejemplo, «¿Qué servicios gestionan los controles en esta instancia de EC2?»). En esta sección, analizamos los elementos de un AWS entorno e identificamos los servicios y características de seguridad asociados. Por supuesto, algunos Servicios de AWS tienen amplios conjuntos de funciones y admiten varios objetivos de seguridad. Estos servicios pueden ser compatibles con varios elementos de su AWS entorno.

Para mayor claridad, proporcionamos breves descripciones de cómo algunos de los servicios se ajustan a los objetivos establecidos. La siguiente sección ofrece un análisis más detallado de los servicios individuales de cada uno de ellos Cuenta de AWS.

Cuentas de toda la organización o cuentas múltiples

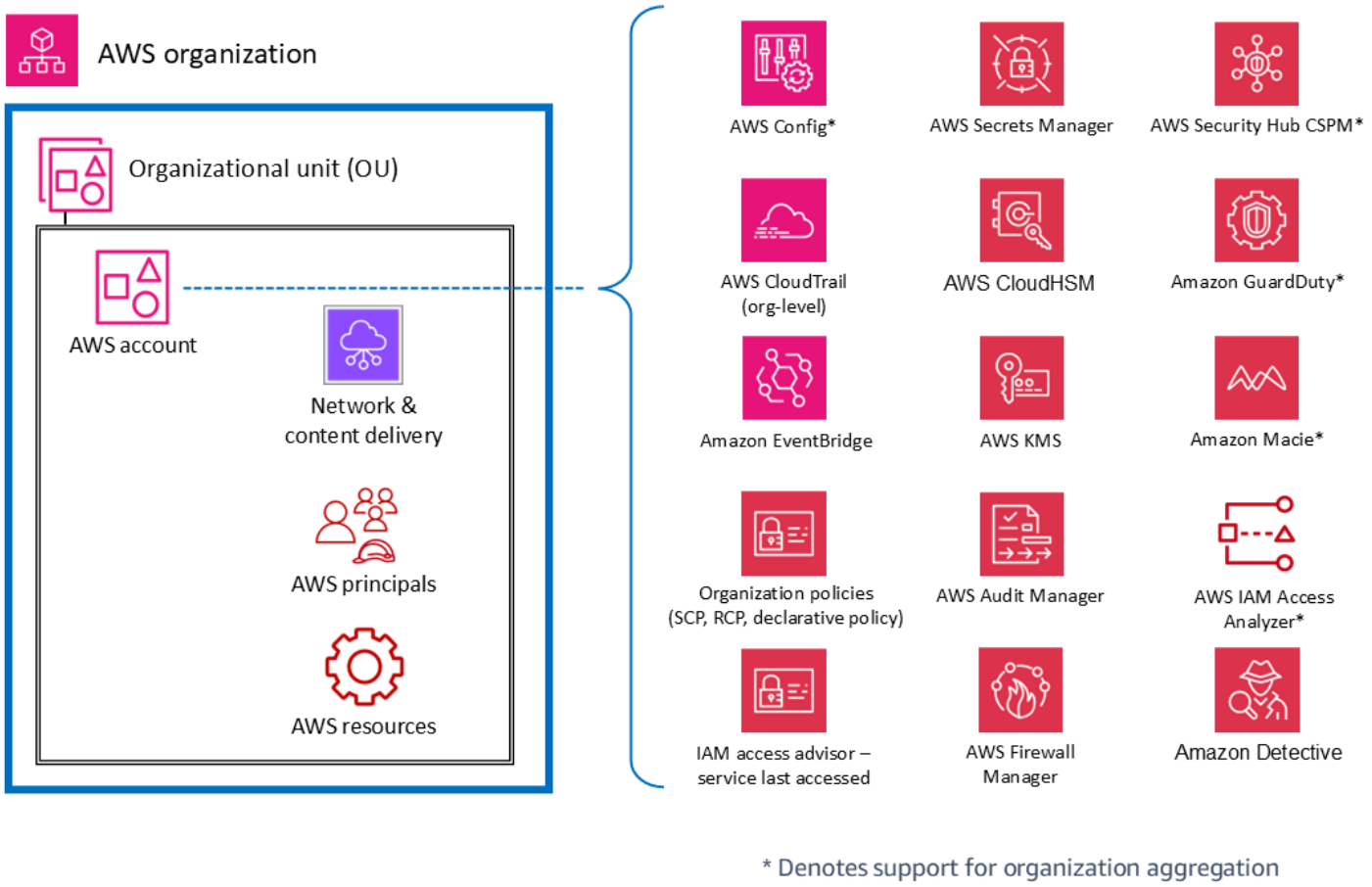
En el nivel superior, hay Servicios de AWS funciones diseñadas para aplicar funciones o barreras de gobierno y control en varias cuentas de una AWS organización (incluida toda la organización o en concreto). OUs Las políticas de control de servicios (SCPs) y las políticas de control de recursos (RCPs) son buenos ejemplos de funciones de IAM que proporcionan barreras preventivas a toda la organización. AWS AWS Organizations también proporciona una política declarativa que define y aplica de forma centralizada la configuración básica a escala. Servicios de AWS Otro ejemplo es el CloudTrail monitoreo a través de un registro de la organización que registra todos los eventos de todos los miembros de esa AWS organización. Cuentas de AWS Este registro completo es distinto de los senderos individuales que se pueden crear en cada cuenta. Un tercer ejemplo es AWS Firewall Manager el que puede utilizar para configurar, aplicar y gestionar varios recursos en todas las cuentas de su AWS organización: AWS WAF reglas, reglas AWS WAF clásicas, AWS Shield Advanced protecciones, grupos de seguridad de Amazon Virtual Private Cloud (Amazon VPC), AWS Network Firewall políticas y políticas de firewall de Amazon Route 53 Resolver DNS.

Los servicios marcados con un asterisco (*) en el siguiente diagrama funcionan con un doble ámbito: se extienden a toda la organización y se centran en las cuentas. Básicamente, estos servicios supervisan o ayudan a controlar la seguridad de una cuenta individual. Sin embargo, también permiten agregar los resultados de varias cuentas en una cuenta de toda la organización para centralizar la visibilidad y la administración. Para mayor claridad, considere SCPs que esto se aplica a toda una unidad organizativa o AWS unidad organizativa. Cuenta de AWS Por el contrario, puede configurar y administrar GuardDuty tanto a nivel de cuenta (donde se generan los hallazgos individuales) como a nivel de AWS organización (mediante la función de administrador delegado), donde los hallazgos se pueden ver y administrar en conjunto.



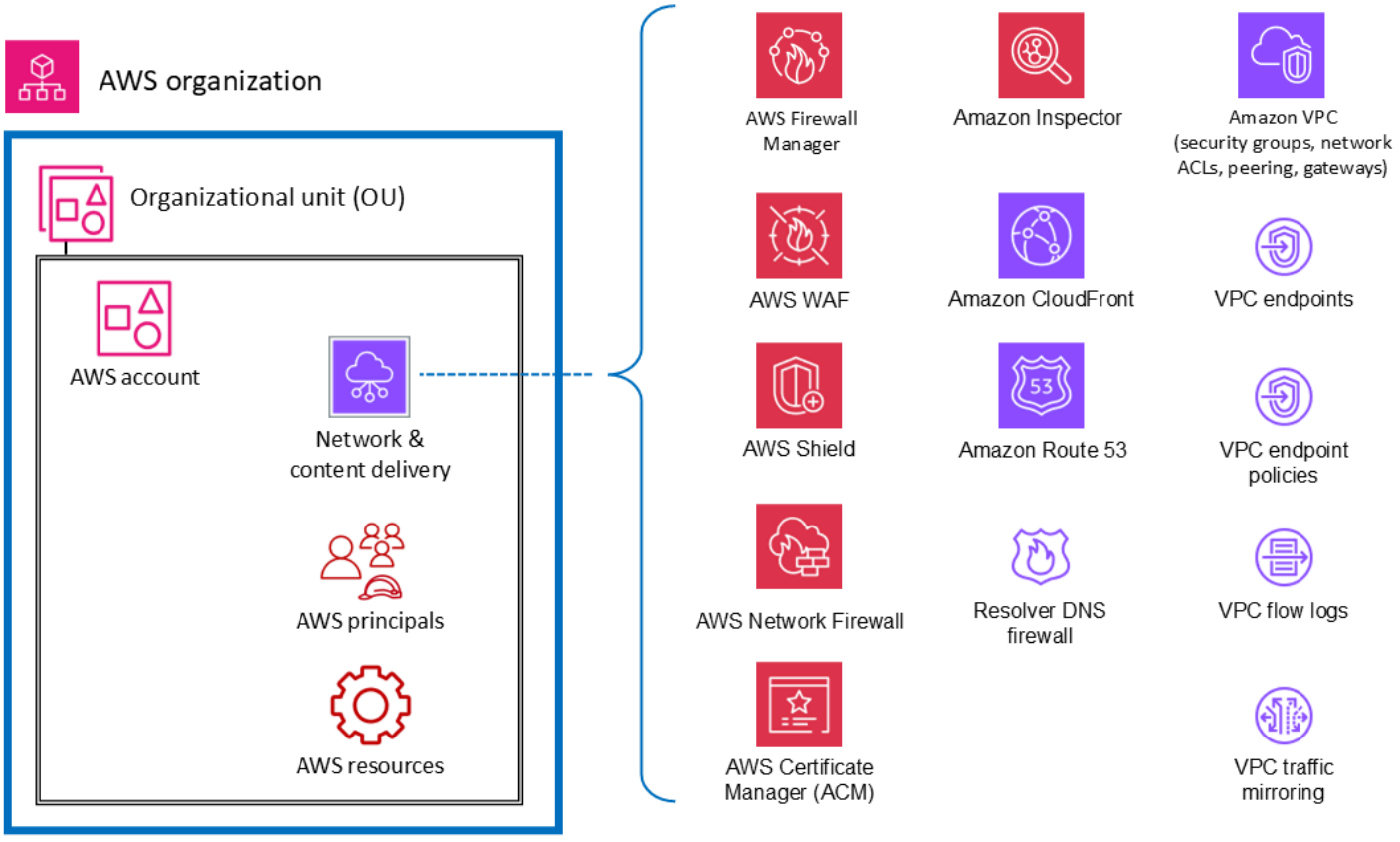
AWS cuentas

Dentro OUs, hay servicios que ayudan a proteger varios tipos de elementos dentro de un Cuenta de AWS. Por ejemplo, AWS Secrets Manager suele administrarse desde una cuenta específica y protege los recursos (como las credenciales de la base de datos o la información de autenticación), las aplicaciones y los Servicios de AWS contenidos en esa cuenta. El analizador de acceso de IAM se puede configurar para generar resultados cuando personas ajenas a ella puedan acceder a determinados recursos. Cuenta de AWS Como se mencionó en la sección anterior, muchos de estos servicios también se pueden configurar y administrar desde dentro AWS Organizations, de modo que se puedan administrar en varias cuentas. Estos servicios están marcados con un asterisco (*) en el diagrama. También facilitan la agregación de los resultados de varias cuentas y su entrega a una sola cuenta. Esto proporciona a los equipos de aplicaciones individuales la flexibilidad y la visibilidad necesarias para gestionar las necesidades de seguridad específicas de su carga de trabajo y, al mismo tiempo, permite la gobernanza y la visibilidad para los equipos de seguridad centralizados. GuardDuty es un ejemplo de este tipo de servicio. GuardDuty supervisa los recursos y la actividad asociados a una sola cuenta, y GuardDuty los resultados de las cuentas de varios miembros (como todas las cuentas de una AWS organización) se pueden recopilar, ver y gestionar desde una cuenta de administrador delegado.



Red virtual, computación y entrega de contenido

Dado que el acceso a la red es fundamental para la seguridad y la infraestructura informática es un componente fundamental de muchas AWS cargas de trabajo, existen muchos servicios y funciones de AWS seguridad dedicados a estos recursos. Por ejemplo, Amazon Inspector es un servicio de administración de vulnerabilidades que analiza continuamente sus AWS cargas de trabajo en busca de vulnerabilidades. Estos escaneos incluyen comprobaciones de accesibilidad de la red que indican que hay rutas de red permitidas a las instancias de Amazon EC2 en su entorno. Amazon VPC le permite definir una red virtual en la que puede lanzar AWS recursos. Esta red virtual se parece mucho a una red tradicional e incluye una variedad de características y ventajas. Los puntos de enlace de la VPC le permiten conectar de forma privada su VPC a los servicios de punto final compatibles Servicios de AWS y a los que funcionan AWS PrivateLink sin necesidad de una ruta a Internet. El siguiente diagrama ilustra los servicios de seguridad que se centran en la infraestructura de red, computación y entrega de contenido.



Principios y recursos

AWS los principios y los AWS recursos (junto con las políticas de IAM) son los elementos fundamentales de la gestión de identidades y accesos en Internet. AWS Un director autenticado AWS puede realizar acciones y acceder a los recursos. AWS Un principal se puede autenticar como usuario Cuenta de AWS raíz y usuario de IAM, o asumiendo una función.

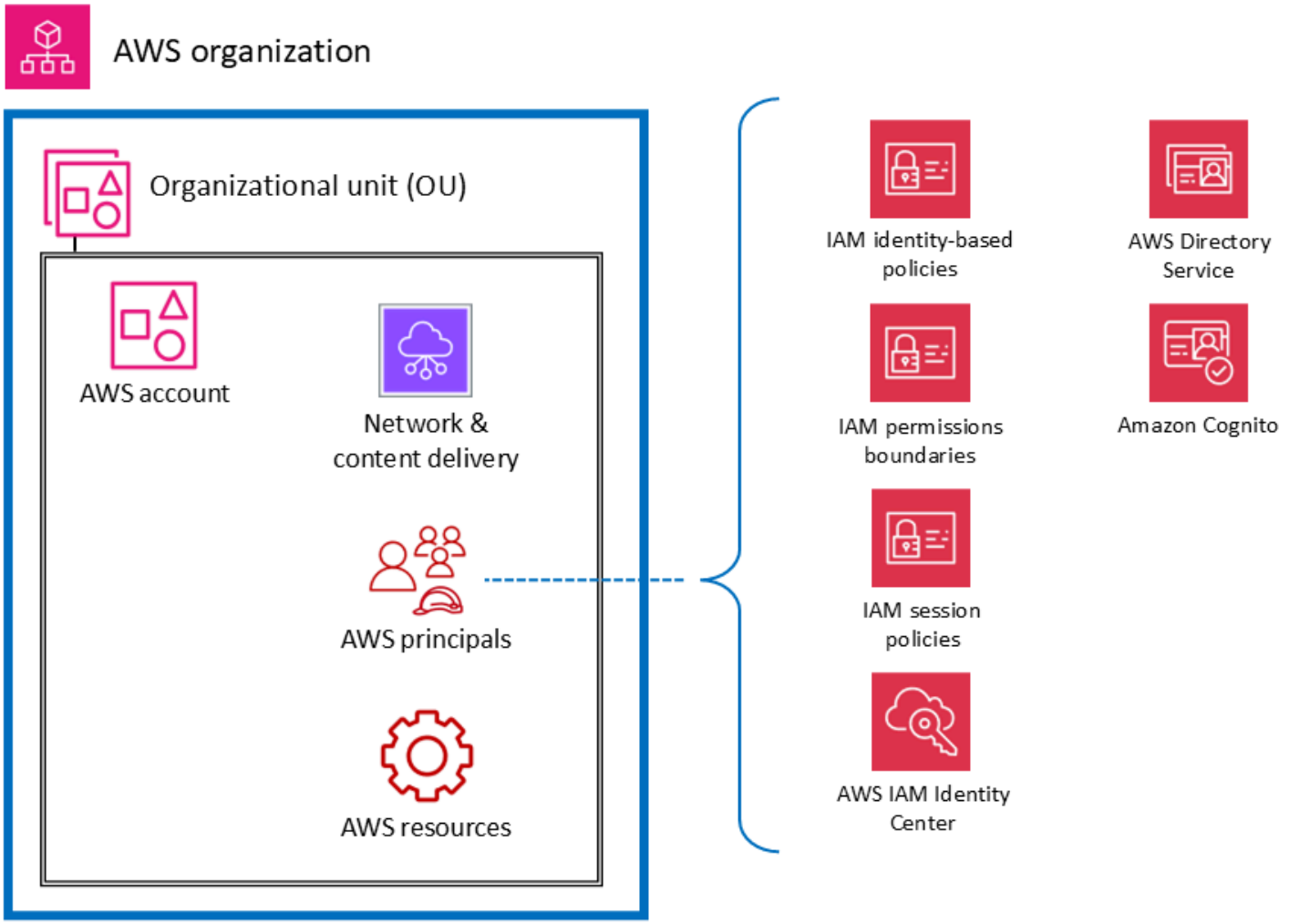
> **Note**
>
> No cree claves de API persistentes asociadas a la cuenta de usuario AWS raíz. El acceso a la cuenta de usuario raíz debe limitarse únicamente a las tareas que requieren un usuario raíz y, en ese caso, únicamente mediante un riguroso proceso de excepción y aprobación. Para conocer las prácticas recomendadas para proteger al usuario raíz de tu cuenta, consulta la documentación de IAM.

Un AWS recurso es un objeto que existe dentro de un objeto con el Servicio de AWS que puedes trabajar. Los ejemplos incluyen una instancia EC2, una CloudFormation pila, un tema de Amazon

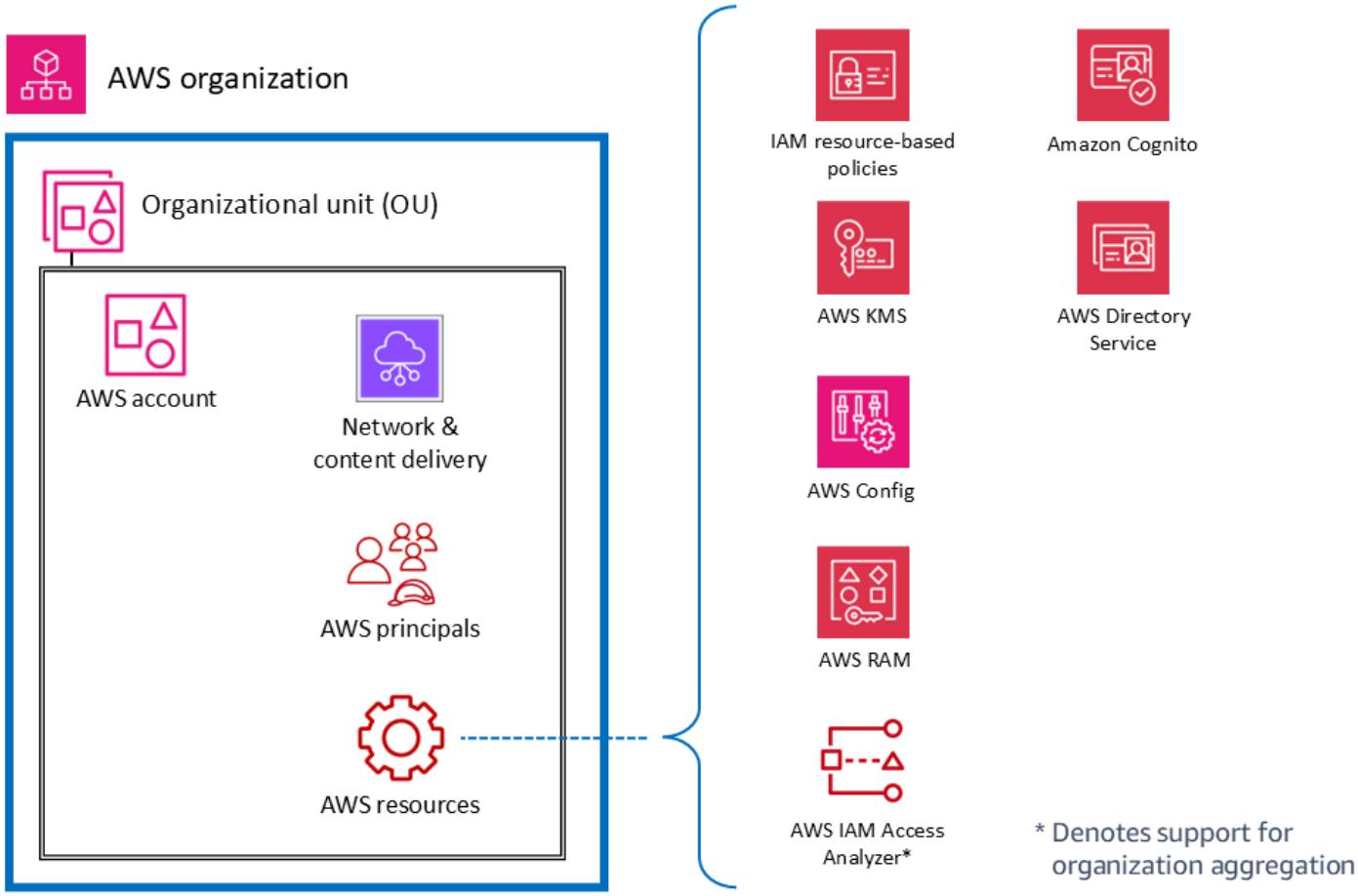
Simple Notification Service (Amazon SNS) y un bucket de S3. Las políticas de IAM son objetos que definen los permisos cuando están asociados a un recurso principal (usuario, grupo o rol) de IAM. AWS Las políticas basadas en la identidad son documentos de política que se adjuntan a un responsable (funciones, usuarios y grupos de usuarios) para controlar qué acciones puede realizar un responsable, con qué recursos y en qué condiciones. Las políticas basadas en recursos son documentos de políticas que se adjuntan a un recurso, como un bucket de S3. Estas políticas otorgan el permiso principal especificado para realizar acciones específicas en ese recurso y definen las condiciones de ese permiso. Las políticas basadas en recursos son políticas en línea. La sección de recursos de IAM profundiza en los tipos de políticas de IAM y en cómo se utilizan.

Para simplificar este análisis, enumeramos los servicios y funciones de AWS seguridad para los directores de IAM cuyo objetivo principal es operar con los directores de cuentas o solicitarlos. Mantenemos esa simplicidad y, al mismo tiempo, reconocemos la flexibilidad y la amplitud de los efectos de las políticas de permisos de IAM. Una sola declaración en una política puede afectar a varios tipos de AWS entidades. Por ejemplo, si bien una política de IAM basada en la identidad está asociada a una entidad principal de IAM y define los permisos (permitir o denegar) para esa entidad, la política también define implícitamente los permisos para las acciones, los recursos y las condiciones especificadas. De este modo, una política basada en la identidad puede ser un elemento fundamental a la hora de definir los permisos de un recurso.

El siguiente diagrama ilustra los servicios y características AWS de seguridad para AWS los directores. Las políticas basadas en identidad se asocian a un rol, grupo o usuario de IAM. Estas políticas le permiten especificar lo que esa identidad puede hacer (sus permisos). Una política de sesión de IAM es una política de permisos en línea que los usuarios aprueban en la sesión cuando asumen el rol. Puede aprobar la política usted mismo o configurar su agente de identidad para que la inserte cuando sus identidades se federen en ellas. AWS Esto permite a los administradores reducir la cantidad de funciones que tienen que crear, ya que varios usuarios pueden asumir la misma función y tener permisos de sesión únicos. El servicio IAM Identity Center está integrado con las operaciones de la AWS API AWS Organizations y le ayuda a gestionar el acceso SSO y los permisos de usuario en todo su Cuentas de AWS entorno. AWS Organizations



En el siguiente diagrama, se muestran los servicios y las características de los recursos de la cuenta. Las políticas basadas en recursos se asocian a un recurso. Por ejemplo, puede adjuntar políticas basadas en recursos a los buckets de S3, a las colas de Amazon Simple Queue Service (Amazon SQS), a los puntos de enlace de VPC y a las claves de cifrado. AWS KMS Puede usar políticas basadas en recursos para especificar quién tiene acceso al recurso y qué acciones puede realizar en él. Las políticas de bucket de S3, las políticas AWS KMS clave y las políticas de puntos finales de VPC son tipos de políticas basadas en recursos. IAM Access Analyzer le ayuda a identificar los recursos de su organización y sus cuentas, como buckets de S3 o roles de IAM, que se comparten con una entidad externa. Esto le permite identificar el acceso no deseado a sus recursos y datos, lo que constituye un riesgo para la seguridad. AWS Config le permite evaluar, auditar y evaluar las configuraciones de los AWS recursos compatibles en su Cuentas de AWS. AWS Config supervisa y registra continuamente las configuraciones AWS de los recursos y evalúa automáticamente las configuraciones registradas comparándolas con las configuraciones deseadas.


AWS organization
Organizational unit (OU)
AWS account
Network & content delivery
AWS principals
AWS resources
IAM resource-based policies
Amazon Cognito
AWS KMS
AWS Directory Service
AWS Config
AWS RAM
AWS IAM Access Analyzer*
* Denotes support for organization aggregation

La arquitectura AWS de referencia de seguridad

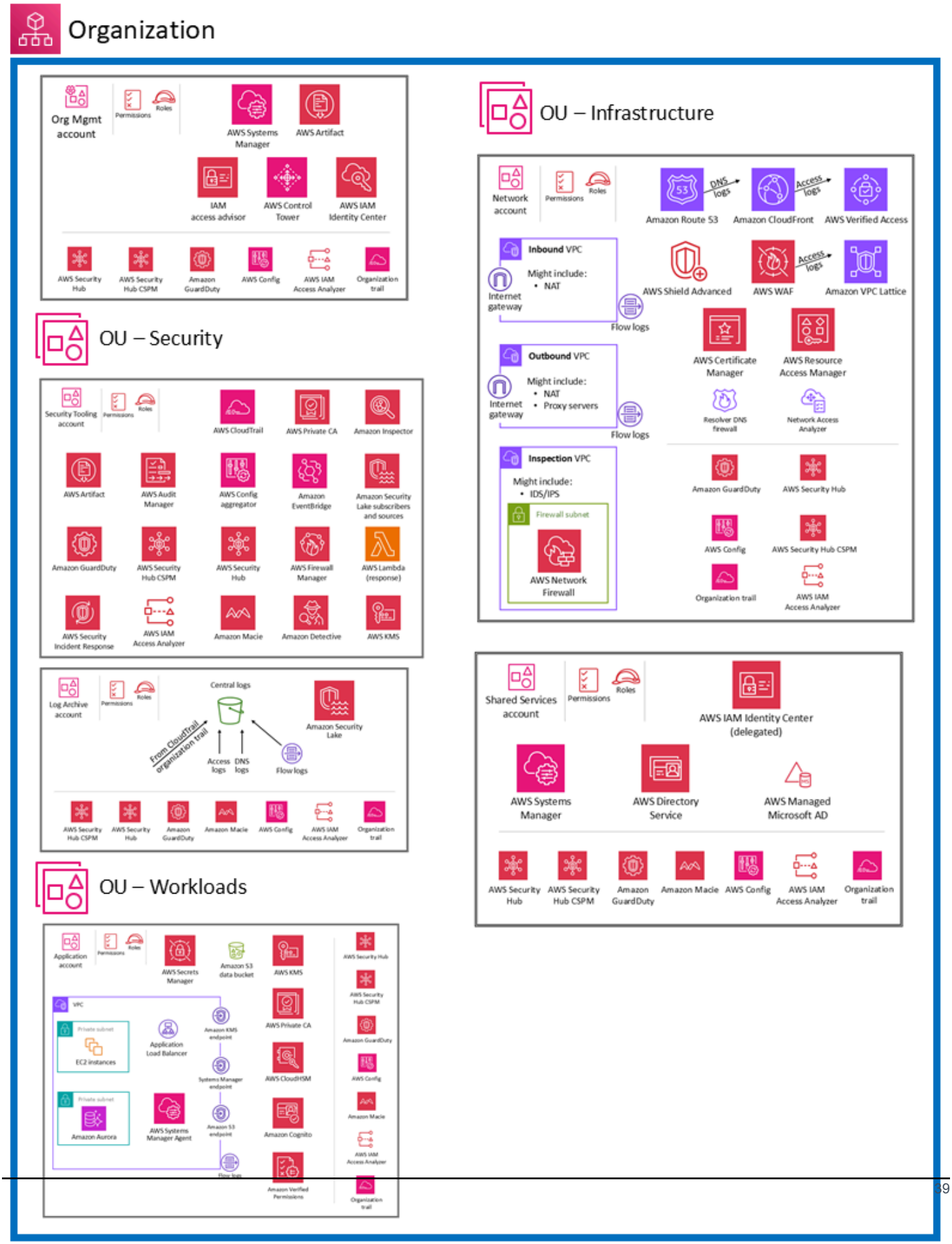
Influya en el futuro de la arquitectura de referencia de AWS seguridad (AWS SRA) realizando una breve encuesta.

El siguiente diagrama ilustra la AWS SRA. Este diagrama arquitectónico reúne todos los servicios relacionados con la AWS seguridad. Se basa en una arquitectura web simple de tres niveles que puede caber en una sola página. En una carga de trabajo de este tipo, existe un nivel web a través del cual los usuarios se conectan e interactúan con el nivel de aplicación, que se encarga de la lógica empresarial real de la aplicación: toma las entradas del usuario, realiza algunos cálculos y genera los resultados. El nivel de aplicación almacena y recupera información del nivel de datos. La arquitectura es deliberadamente modular y proporciona una abstracción de alto nivel para muchas aplicaciones web modernas.

Diagramas de arquitectura

Para personalizar los diagramas de arquitectura de referencia de esta guía en función de las necesidades de su empresa, puede descargar el siguiente archivo.zip y extraer su contenido.

Descarga el archivo fuente del diagrama (PowerPoint formato Microsoft)


Organization
Org Mgmt account
Permissions
Roles
AWS Systems Manager
AWS Artifact
IAM access advisor
AWS Control Tower
AWS IAM Identity Center
AWS Security Hub
AWS Security Hub CSPM
Amazon GuardDuty
AWS Config
AWS IAM Access Analyzer
Organization trail
OU – Security
Security Tooling account
AWS CloudTrail
AWS Private CA
Amazon Inspector
AWS Artifact
AWS Audit Manager
AWS Config aggregator
Amazon EventBridge
Amazon Security Lake subscribers and sources
Amazon GuardDuty
AWS Security Hub CSPM
AWS Security Hub
AWS Firewall Manager
AWS Lambda (response)
AWS Security Incident Response
AWS IAM Access Analyzer
Amazon Macie
Amazon Detective
AWS KMS
Log Archive account
Central logs
From CloudTrail and organization trail
Access logs
DNS logs
Flow logs
Amazon Security Lake
OU – Workloads
Application account
AWS Secrets Manager
Amazon S3 data bucket
AWS KMS
VPC
Private subnet
EC2 instances
Application Load Balancer
Amazon KMS endpoint
AWS Private CA
Systems Manager endpoint
AWS CloudHSM
Amazon Aurora
AWS Systems Manager Agent
Amazon S3 endpoint
Amazon Cognito
Flow logs
Amazon Verified Permissions
OU – Infrastructure
Network account
Amazon Route 53
DNS logs
Amazon CloudFront
Access logs
AWS Verified Access
Inbound VPC
Might include:
• NAT
Internet gateway
Flow logs
AWS Shield Advanced
AWS WAF
Access logs
Amazon VPC Lattice
Outbound VPC
Might include:
• NAT
• Proxy servers
Internet gateway
Flow logs
AWS Certificate Manager
AWS Resource Access Manager
Resolver DNS firewall
Network Access Analyzer
Inspection VPC
Might include:
• IDS/IPS
Firewall subnet
AWS Network Firewall
Amazon GuardDuty
AWS Security Hub
AWS Config
AWS Security Hub CSPM
Organization trail
AWS IAM Access Analyzer
Shared Services account
AWS IAM Identity Center (delegated)
AWS Systems Manager
AWS Directory Service
AWS Managed Microsoft AD
AWS Security Hub
AWS Security Hub CSPM
Amazon GuardDuty
Amazon Macie
AWS Config
AWS IAM Access Analyzer
Organization trail

Para esta arquitectura de referencia, la aplicación web y el nivel de datos reales se representan deliberadamente de la forma más sencilla posible, mediante EC2 instancias de Amazon y una base de datos de Amazon Aurora, respectivamente. La mayoría de los diagramas de arquitectura se centran y profundizan en los niveles web, de aplicaciones y de datos. Para facilitar la lectura, a menudo omiten los controles de seguridad. Este diagrama invierte ese énfasis para mostrar la seguridad siempre que sea posible y mantiene los niveles de aplicaciones y datos tan simples como sea necesario para mostrar las características de seguridad de manera significativa.

La AWS SRA contiene todos los servicios AWS relacionados con la seguridad disponibles en el momento de su publicación. (Consulte el historial de documentos). Sin embargo, no todas las cargas de trabajo o entornos, en función de su exposición única a las amenazas, tienen que implementar todos los servicios de seguridad. Nuestro objetivo es proporcionar una referencia para una variedad de opciones, incluidas descripciones de cómo estos servicios se integran entre sí desde el punto de vista arquitectónico, de modo que su empresa pueda tomar las decisiones más adecuadas para sus necesidades de infraestructura, carga de trabajo y seguridad, en función del riesgo.

En las siguientes secciones se explica cada unidad organizativa y cada cuenta para comprender sus objetivos y los servicios de AWS seguridad individuales asociados a ella. Para cada elemento (normalmente uno Servicio de AWS), este documento proporciona la siguiente información:

- Breve descripción del elemento y su propósito de seguridad en la AWS SRA. Para obtener descripciones más detalladas e información técnica sobre los servicios individuales, consulte el apéndice.
- Ubicación recomendada para habilitar y administrar el servicio de la manera más eficaz. Esto se refleja en los diagramas de arquitectura individuales de cada cuenta y unidad organizativa.
- Vínculos de configuración, administración e intercambio de datos a otros servicios de seguridad. ¿Cómo se basa este servicio en otros servicios de seguridad o los apoya?
- Consideraciones de diseño. En primer lugar, el documento destaca las características o configuraciones opcionales que tienen importantes implicaciones de seguridad. En segundo lugar, si bien la experiencia de nuestros equipos incluye variaciones comunes en las recomendaciones que hacemos (normalmente como resultado de requisitos o restricciones alternativos), en el documento se describen esas opciones.

OUs y cuentas

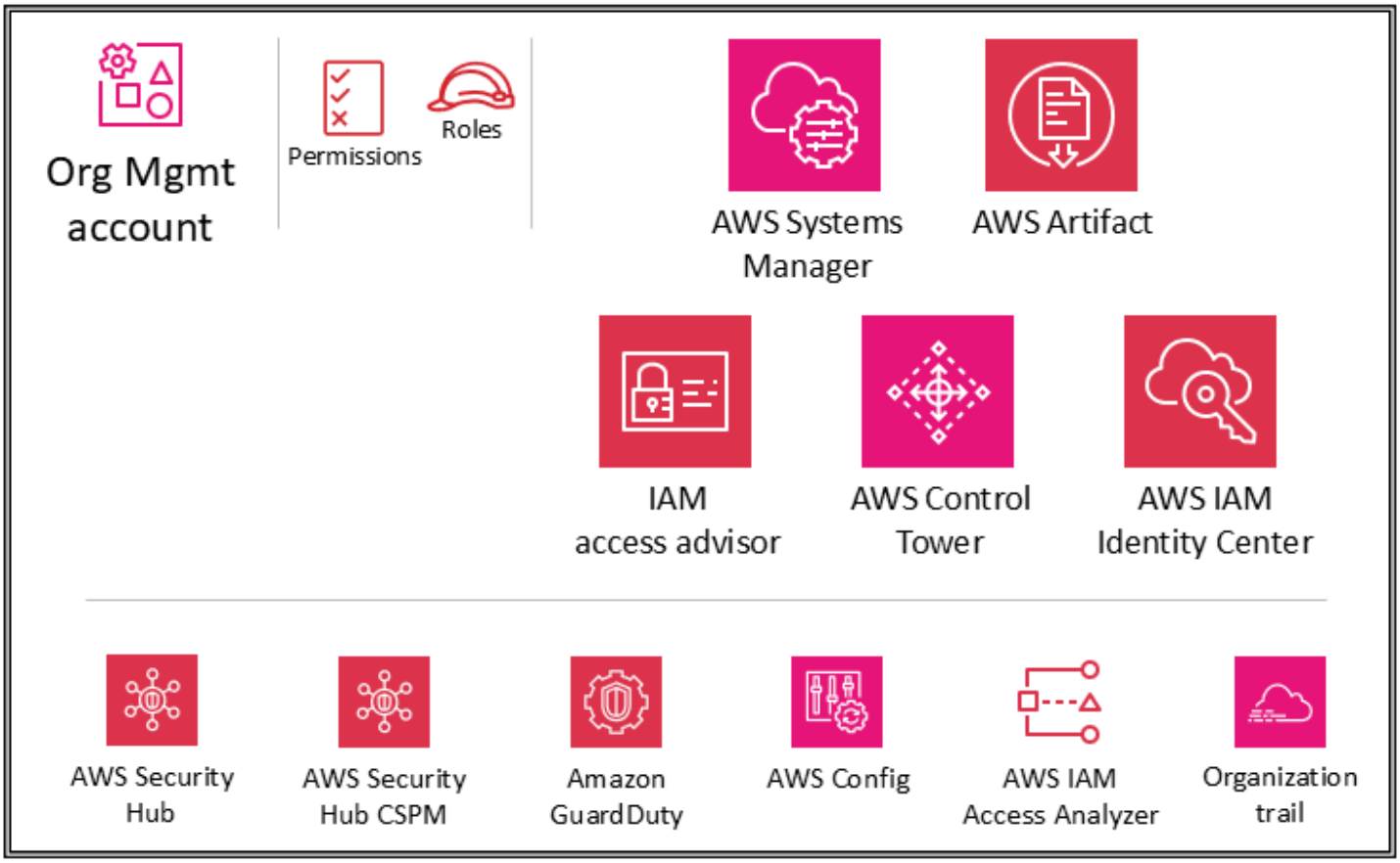
- Cuenta de administración de la organización
- UO de seguridad: cuenta de herramientas de seguridad

- UO de seguridad: cuenta de archivos de registro
- Unidad organizativa de infraestructura: cuenta de red
- Infrastructure OU: cuenta de servicios compartidos
- Workloads OU: cuenta de aplicación

Cuenta de administración de la organización

Influya en el futuro de la arquitectura de referencia de AWS seguridad (AWS SRA) realizando una breve encuesta.

El siguiente diagrama ilustra los servicios de AWS seguridad que están configurados en la cuenta de administración de la organización.



En las secciones Uso AWS Organizations por motivos de seguridad y La cuenta de administración, el acceso confiable y los administradores delegados, que aparecen anteriormente en esta guía, se

analizan en profundidad el propósito y los objetivos de seguridad de la cuenta de administración de la organización. Siga las prácticas recomendadas de seguridad para su cuenta de administración de la organización. Estas incluyen usar una dirección de correo electrónico administrada por su empresa, mantener la información de contacto administrativa y de seguridad correcta (como adjuntar un número de teléfono a la cuenta en caso de que AWS necesite contactar con el propietario de la cuenta), habilitar la autenticación multifactorial (MFA) para todos los usuarios y revisar periódicamente quién tiene acceso a la cuenta de administración de la organización. Los servicios implementados en la cuenta de administración de la organización deben configurarse con las funciones, políticas de confianza y otros permisos adecuados para que los administradores de esos servicios (que deben acceder a ellos en la cuenta de administración de la organización) tampoco puedan acceder de manera inapropiada a otros servicios.

Políticas de control de servicios

Con él AWS Organizations, puede gestionar de forma centralizada las políticas de varios Cuentas de AWS tipos. Por ejemplo, puede aplicar políticas de control de servicios (SCPs) Cuentas de AWS a varios miembros de una organización. SCPs le permiten definir cuáles Servicio de AWS APIs pueden y qué no pueden administrar los directores de IAM (como los usuarios y las funciones de IAM) de los miembros de su organización. Cuentas de AWS SCPs se crean y aplican desde la cuenta de administración de la organización, que es la Cuenta de AWS que utilizó al crear su organización. Obtenga más información al respecto SCPs en la sección Uso AWS Organizations por motivos de seguridad, que aparece anteriormente en esta referencia.

Si lo utiliza AWS Control Tower para administrar su AWS organización, esta implementará un conjunto de SCPs barreras preventivas (clasificadas como obligatorias, altamente recomendadas u optativas). Estas barreras le ayudan a controlar sus recursos al aplicar controles de seguridad en toda la organización. Utilizan SCPs automáticamente una aws-control-tower etiqueta que tiene un valor de. managed-by-control-tower

> **Consideración del diseño**
>
> SCPs afectan únicamente a las cuentas de los miembros de la AWS organización. Aunque se aplican desde la cuenta de administración de la organización, no afectan a los usuarios ni a las funciones de esa cuenta. Para obtener información sobre cómo funciona la lógica de evaluación del SCP y ver ejemplos de estructuras recomendadas, consulte la entrada del AWS blog Cómo utilizar las políticas de control de servicios en AWS Organizations.

Políticas de control de recursos

Las políticas de control de recursos (RCPs) ofrecen un control centralizado sobre el máximo de permisos disponibles para los recursos de su organización. Un RCP define una barrera de permisos o establece límites a las acciones que las identidades pueden realizar con los recursos de la organización. Puedes utilizarla RCPs para restringir quién puede acceder a tus recursos y hacer cumplir los requisitos sobre cómo los miembros de tu organización pueden acceder a tus recursos. Cuentas de AWS Puedes asociarlos RCPs directamente a cuentas individuales o a la raíz de la organización. OUs Para obtener una explicación detallada de cómo RCPs funciona, consulte la evaluación del RCP en la AWS Organizations documentación. Obtenga más información al respecto RCPs en la sección Uso AWS Organizations por motivos de seguridad, que aparece anteriormente en esta referencia.

Si lo utiliza AWS Control Tower para administrar su AWS organización, esta implementará un conjunto de barreras preventivas (clasificadas RCPs como obligatorias, altamente recomendadas u optativas). Estas barreras le ayudan a controlar sus recursos al aplicar controles de seguridad en toda la organización. Utilizan SCPs automáticamente una `aws-control-tower` etiqueta que tiene un valor de. `managed-by-control-tower`

Consideraciones sobre el diseño

- RCPs afectan únicamente a los recursos de las cuentas de los miembros de la organización. No tienen ningún efecto en los recursos de la cuenta de administración. Esto también significa que RCPs se aplican a las cuentas de los miembros designadas como administradores delegados.
- RCPs se aplican a los recursos de un subconjunto de. Servicios de AWS Para obtener más información, consulte la lista de Servicios de AWS ese soporte RCPs en la AWS Organizations documentación. Puede utilizar AWS Lambda las funciones Reglas de AWS Configy funciones para supervisar y automatizar la aplicación de los controles de seguridad en los recursos que actualmente no son compatibles con RCPs.

Políticas declarativas

Una política declarativa es un tipo de política de AWS Organizations administración que le ayuda a declarar y aplicar de forma centralizada la configuración deseada para una determinada escala Servicio de AWS en toda la organización. Las políticas declarativas son compatibles actualmente con

los servicios de Amazon EC2, Amazon VPC y Amazon EBS. Los atributos del servicio disponibles incluyen la aplicación de la versión 2 del Servicio de Metadatos de Instancia (IMDSv2), la posibilidad de solucionar problemas a través de la consola serie EC2, la configuración de Amazon Machine Image (AMI) y el bloqueo del acceso público a las instantáneas de Amazon EBS, Amazon EC2 AMIs y los recursos de Amazon VPC. Para obtener información sobre los servicios y atributos compatibles más recientes, consulte las políticas declarativas en la documentación. AWS Organizations

Para hacer cumplir la configuración básica de Servicio de AWS an, seleccione algunas opciones en las AWS Control Tower consolas AWS Organizations y o utilice algunos comandos AWS Command Line Interface (AWS CLI) y AWS del SDK. Las políticas declarativas se aplican en el plano de control del servicio, lo que significa que la configuración básica de an siempre Servicio de AWS se mantiene, incluso cuando el servicio introduce nuevas funciones o APIs cuando se agregan nuevas cuentas a una organización o cuando se crean nuevos directores y recursos. Las políticas declarativas se pueden aplicar a toda la organización o a cuentas específicas OUs . La política efectiva es el conjunto de reglas que se heredan de la raíz de la organización y OUs junto con las políticas que se asocian directamente a la cuenta. Si se separa una política declarativa, el estado del atributo volverá a su estado anterior a la incorporación de la política declarativa.

Puede usar políticas declarativas para crear mensajes de error personalizados. Por ejemplo, si una operación de la API falla debido a una política declarativa, puedes configurar el mensaje de error o proporcionar una URL personalizada, como un enlace a un wiki interno o un enlace a un mensaje que describa el error. Esto ayuda a proporcionar a los usuarios más información para que puedan solucionar el problema por sí mismos. También puede auditar el proceso de creación de políticas declarativas, actualización de políticas declarativas y eliminación de políticas declarativas mediante. AWS CloudTrail

Las políticas declarativas proporcionan informes sobre el estado de las cuentas, que permiten revisar el estado actual de todos los atributos compatibles con las políticas declarativas de las cuentas incluidas en el ámbito de aplicación. Puede elegir las cuentas e OUs incluirlas en el ámbito del informe o elegir una organización completa seleccionando la raíz. Este informe le ayuda a evaluar si está preparado, ya que proporciona un desglose Región de AWS y especifica si el estado actual de un atributo es uniforme en todas las cuentas (a través del `numberOfMatchedAccounts` valor) o incoherente en todas las cuentas (a través del `numberOfUnmatchedAccounts` valor).

> **Consideración del diseño**
>
> Al configurar un atributo de servicio mediante una política declarativa, la política puede afectar a varios APIs. Cualquier acción no conforme generará un error. Los administradores

de cuentas no podrán modificar el valor del atributo de servicio al nivel de una cuenta individual.

Acceso raíz centralizado

Todas las cuentas de los miembros AWS Organizations tienen su propio usuario raíz, que es una identidad que tiene acceso completo a todos Servicios de AWS los recursos de esa cuenta de miembro. IAM proporciona una gestión centralizada del acceso raíz para gestionar el acceso raíz en todas las cuentas de los miembros. Esto ayuda a evitar el uso por parte de los usuarios raíz de los miembros y a proporcionar una recuperación a escala. La función de acceso raíz centralizado tiene dos capacidades esenciales: la administración de credenciales raíz y las sesiones raíz.

- La capacidad de administración de credenciales raíz permite la administración centralizada y ayuda a proteger al usuario raíz en todas las cuentas de administración. Esta capacidad incluye la eliminación de las credenciales raíz de larga duración, la prevención de la recuperación de las credenciales raíz por parte de las cuentas de los miembros y el aprovisionamiento de nuevas cuentas de miembros sin credenciales raíz de forma predeterminada. También proporciona una forma sencilla de demostrar el cumplimiento. Cuando la administración de usuarios raíz está centralizada, puede eliminar las contraseñas de los usuarios raíz, las claves de acceso y los certificados de firma, y desactivar la autenticación multifactor (MFA) de todas las cuentas de los miembros.
- La función de sesiones raíz le permite realizar acciones de usuario raíz con privilegios mediante el uso de credenciales de corta duración en las cuentas de los miembros desde la cuenta de administración de la organización o desde cuentas de administrador delegado. Esta capacidad le ayuda a habilitar el acceso root a corto plazo, sujeto a acciones específicas y siguiendo el principio del privilegio mínimo.

Para una administración centralizada de las credenciales raíz, debe habilitar las capacidades de administración de credenciales raíz y sesiones raíz a nivel de la organización desde la cuenta de administración de la organización o en una cuenta de administrador delegado. Siguiendo las prácticas recomendadas de la AWS SRA, delegamos esta capacidad a la cuenta Security Tooling. Para obtener información sobre la configuración y el uso del acceso centralizado de los usuarios raíz, consulte la entrada del blog sobre AWS seguridad titulada Gestión centralizada del acceso raíz para los clientes que lo utilizan. AWS Organizations

IAM Identity Center

AWS IAM Identity Centeres un servicio de federación de identidades que le ayuda a gestionar de forma centralizada el acceso SSO a todas sus cargas de trabajo Cuentas de AWS, las principales y las de la nube. El IAM Identity Center también le ayuda a gestionar el acceso y los permisos a las aplicaciones de software como servicio (SaaS) de terceros que se utilizan habitualmente. Los proveedores de identidad se integran con el IAM Identity Center mediante SAML 2.0. El just-in-time aprovisionamiento y el aprovisionamiento masivos se pueden realizar mediante el Sistema de Gestión de Identidad entre Dominios (SCIM). El IAM Identity Center también se puede integrar con dominios de Microsoft Active Directory (AD) locales o AWS administrados como proveedor de identidades mediante el uso de. AWS Directory Service El Centro de identidad de IAM incluye un portal de usuarios en el que los usuarios finales pueden encontrar y acceder al centro de identidad de Cuentas de AWS IAM asignado, las funciones, las aplicaciones en la nube y las aplicaciones personalizadas desde un solo lugar.

El Centro de Identidad de IAM se integra de forma nativa con la cuenta de administración de la organización AWS Organizations y se ejecuta en ella de forma predeterminada. Sin embargo, para tener el mínimo de privilegios y controlar estrictamente el acceso a la cuenta de administración, la administración del IAM Identity Center se puede delegar en una cuenta de miembro específica. En la AWS SRA, la cuenta de Shared Services es la cuenta de administrador delegado del IAM Identity Center. Antes de habilitar la administración delegada en el Centro de identidades de IAM, revise estas consideraciones. Encontrará más información sobre la delegación en la sección de cuentas de Shared Services. Incluso después de activar la delegación, el Centro de Identidad de IAM seguirá ejecutándose en la cuenta de gestión de la organización para realizar determinadas tareas relacionadas con el Centro de identidades de IAM, entre las que se incluye la gestión de los conjuntos de permisos que se aprovisionan en la cuenta de gestión de la organización.

En la consola del IAM Identity Center, las cuentas se muestran según su unidad organizativa encapsulada. Esto le permite descubrir rápidamente los suyos Cuentas de AWS, aplicar conjuntos de permisos comunes y gestionar el acceso desde una ubicación central.

El centro de identidad de IAM incluye un almacén de identidades en el que se debe almacenar información específica del usuario. Sin embargo, el Centro de Identidad de IAM no tiene por qué ser la fuente autorizada de información sobre la fuerza laboral. En los casos en los que su empresa ya cuente con una fuente autorizada, el Centro de Identidad de IAM admite los siguientes tipos de proveedores de identidad (). IdPs

- Almacén de identidades del IAM Identity Center: elija esta opción si las dos opciones siguientes no están disponibles. Se crean los usuarios, se realizan las asignaciones de grupos y se asignan los permisos en el almacén de identidades. Incluso si la fuente autorizada es externa al Centro de identidades de IAM, se almacenará una copia de los atributos principales en el almacén de identidades.
- Microsoft Active Directory (AD): elija esta opción si desea seguir administrando los usuarios de su directorio AWS Directory Service for Microsoft Active Directory o del directorio autoadministrado de Active Directory.
- Proveedor de identidad externo: elija esta opción si prefiere administrar los usuarios en un IdP externo de terceros basado en SAML.

Puede confiar en un IdP existente que ya existe en su empresa. De este modo se facilita la administración del acceso en varias aplicaciones y servicios, pues crea, administra y revoca el acceso desde un único lugar. Por ejemplo, si alguien deja tu equipo, puedes revocar su acceso a todas las aplicaciones y servicios (incluidos Cuentas de AWS) desde un solo lugar. Esto reduce la necesidad de tener varias credenciales y te brinda la oportunidad de integrarte con tus procesos de recursos humanos (RRHH).

> **Consideración del diseño**
>
> Utilice un IdP externo si esa opción está disponible para su empresa. Si su IdP es compatible con el Sistema de gestión de identidades entre dominios (SCIM), aproveche la capacidad SCIM del IAM Identity Center para automatizar el aprovisionamiento (sincronización) de usuarios, grupos y permisos. Esto permite que el AWS acceso se mantenga sincronizado con el flujo de trabajo corporativo para los nuevos empleados, los empleados que se mudan a otro equipo y los empleados que se van de la empresa. En un momento dado, solo puede tener un directorio o un proveedor de identidades de SAML 2.0 conectado al Centro de identidades de IAM. Sin embargo, puede cambiar a otro proveedor de identidad.

Asesor de acceso de IAM

El asesor de acceso de IAM proporciona datos de trazabilidad en forma de información sobre el último servicio al que se accedió para usted y. Cuentas de AWS OUs Utilice este control detectivesco para contribuir a una estrategia de privilegios mínimos. Para los directores de IAM, puede ver dos tipos de información a la que se accedió por última vez: la información permitida y la Servicio de

AWS información sobre las acciones permitidas. Esta información incluye la fecha y la hora en que se realizó el intento.

El acceso a la IAM dentro de la cuenta de administración de la organización le permite ver los datos del servicio al que se accedió por última vez para la cuenta de administración de la organización, la unidad organizativa, la cuenta de miembro o la política de IAM de su organización. AWS Esta información está disponible en la consola de IAM de la cuenta de administración y también se puede obtener mediante programación mediante el asesor APIs de acceso de IAM o un cliente programático. AWS CLI Se indica qué entidades principales de una organización o cuenta intentaron acceder por última vez al servicio y cuándo lo hicieron. La información consultada por última vez proporciona información sobre el uso real del servicio (consulte los escenarios de ejemplo), por lo que puede reducir los permisos de IAM únicamente a los servicios que se utilizan realmente.

AWS Systems Manager

Quick Setup y Explorer, que son capacidades de AWS Systems Manager, admiten AWS Organizations y funcionan desde la cuenta de administración de la organización.

La configuración rápida es una función de automatización de Systems Manager. Permite que la cuenta de administración de la organización defina fácilmente las configuraciones para que Systems Manager interactúe en su nombre en todas las cuentas de su AWS organización. Puede activar la configuración rápida en toda AWS la organización o elegir una específica OUs. Quick Setup puede programar el AWS Systems Manager Agent (SSM Agent) para que ejecute actualizaciones quincenales en sus instancias de EC2 y puede configurar un análisis diario de esas instancias para identificar los parches que faltan.

Explorer es un panel de operaciones personalizable que proporciona información sobre sus recursos. AWS Explorer muestra una vista agregada de los datos de operaciones de sus AWS cuentas y de todas ellas Regiones de AWS. Esto incluye datos sobre sus instancias EC2 y detalles sobre el cumplimiento de los parches. Después de completar la configuración integrada (que también incluye Systems Manager OpsCenter) AWS Organizations, puede agregar datos en Explorer por unidad organizativa o para toda AWS la organización. Systems Manager agrega los datos a la cuenta de administración de la AWS organización antes de mostrarlos en el Explorador.

En la sección Workloads OU, que aparece más adelante en esta guía, se analiza el uso del agente SSM en las instancias EC2 de la cuenta de la aplicación.

AWS Control Tower

AWS Control Towerproporciona una forma sencilla de configurar y gobernar un AWS entorno seguro de múltiples cuentas, que se denomina landing zone. AWS Control Tower crea tu landing zone mediante el uso y proporciona una gestión y gobierno continuos de las cuentas AWS Organizations, así como las mejores prácticas de implementación. Se puede utilizar AWS Control Tower para aprovisionar nuevas cuentas en unos pocos pasos y, al mismo tiempo, garantizar que las cuentas se ajusten a las políticas de la organización. Incluso puede añadir las cuentas existentes a un nuevo AWS Control Tower entorno.

AWS Control Tower tiene un conjunto de funciones amplio y flexible. Una característica clave es su capacidad para organizar las capacidades de varios otros Servicios de AWS AWS Organizations, AWS Service Catalog incluido el IAM Identity Center, para crear una landing zone. Por ejemplo, de forma predeterminada, AWS Control Tower utiliza AWS CloudFormation políticas de control del AWS Organizations servicio (SCPs) para evitar cambios en la configuración y Reglas de AWS Config reglas para detectar continuamente las no conformidades. AWS Control Tower emplea esquemas que le ayudan a alinear rápidamente su AWS entorno de múltiples cuentas con los principios de diseño básicos de seguridad de AWS Well Architected. Entre las características de gobierno, AWS Control Tower ofrece barreras que impiden el despliegue de recursos que no se ajusten a las políticas seleccionadas.

Puede empezar a implementar las directrices de la AWS SRA con. AWS Control Tower Por ejemplo, AWS Control Tower establece una AWS organización con la arquitectura de cuentas múltiples recomendada. Proporciona planes para gestionar la identidad, proporcionar acceso federado a las cuentas, centralizar el registro, establecer auditorías de seguridad entre cuentas, definir un flujo de trabajo para el aprovisionamiento de nuevas cuentas e implementar líneas base de cuentas con configuraciones de red.

En la AWS SRA, AWS Control Tower se encuentra dentro de la cuenta de administración de la organización porque AWS Control Tower usa esta cuenta para configurar una AWS organización automáticamente y designa esa cuenta como cuenta de administración. Esta cuenta se utiliza para facturar en toda la organización. AWS También se usa para el aprovisionamiento de cuentas en Account Factory, para administrar OUs y administrar barandas. Si vas a lanzarlo AWS Control Tower en una AWS organización existente, puedes usar la cuenta de administración existente. AWS Control Tower usará esa cuenta como la cuenta de administración designada.

Consideración del diseño

Si quieres establecer una base adicional de controles y configuraciones en tus cuentas, puedes usar las personalizaciones para AWS Control Tower (cFCT). Con cFCT, puedes personalizar tu AWS Control Tower landing zone mediante una CloudFormation plantilla y SCPs. Puede implementar la plantilla y las políticas personalizadas en cuentas individuales y OUs dentro de su organización. cFCT se integra con los eventos AWS Control Tower del ciclo de vida para garantizar que los despliegues de recursos estén sincronizados con tu landing zone.

AWS Artifact

AWS Artifactproporciona acceso bajo demanda a los informes AWS de seguridad y cumplimiento y a determinados acuerdos en línea. Los informes disponibles AWS Artifact incluyen informes de controles de sistemas y organizaciones (SOC), informes del sector de tarjetas de pago (PCI) y certificaciones de organismos de acreditación de diferentes regiones geográficas y verticales de cumplimiento que validan la implementación y la eficacia operativa de los controles de seguridad. AWS AWS Artifact le ayuda a llevar a cabo la diligencia debida y, AWS con una mayor transparencia, en nuestro entorno de control de seguridad. También le permite supervisar continuamente la seguridad y el cumplimiento, AWS con acceso inmediato a nuevos informes.

AWS Artifact Los acuerdos le permiten revisar, aceptar y realizar un seguimiento del estado de AWS los acuerdos, como el apéndice de socios comerciales (BAA), para una cuenta individual y para las cuentas que forman parte de su organización. AWS Organizations

Puede proporcionar los artefactos de AWS auditoría a sus auditores o reguladores como prueba de los controles de AWS seguridad. También puede utilizar la guía de responsabilidad proporcionada por algunos de los dispositivos de AWS auditoría para diseñar su arquitectura de nube. Esta guía ayuda a determinar los controles de seguridad adicionales que puede implementar para respaldar los casos de uso específicos de su sistema.

AWS Artifact está alojado en la cuenta de administración de la organización para proporcionar una ubicación central en la que puede revisar, aceptar y gestionar los acuerdos AWS. Esto se debe a que los acuerdos que se aceptan en la cuenta de administración se transfieren a las cuentas de los miembros.

> **Consideración del diseño**
>
> Los usuarios de la cuenta de administración de la organización deben estar restringidos a utilizar únicamente la función de acuerdos AWS Artifact y nada más. Para implementar la segregación de funciones, también AWS Artifact se aloja en la cuenta Security Tooling, donde puede delegar permisos a las partes interesadas en el cumplimiento y a auditores externos para acceder a los artefactos de auditoría. Puede implementar esta separación definiendo políticas de permisos de IAM detalladas. Para ver ejemplos, consulte los ejemplos de políticas de IAM en la documentación. AWS

Barandillas de servicios de seguridad distribuidas y centralizadas

En la AWS SRA, Amazon AWS Security Hub, AWS Security Hub CSPM IAM Access Analyzer GuardDuty AWS Config, las rutas AWS CloudTrail organizativas y, a menudo, Amazon Macie se implementan con el conjunto de barreras de protección delegadas adecuadas en todas las cuentas y también proporciona supervisión, administración y gobierno centralizados en toda la organización. AWS Encontrará este grupo de servicios en todos los tipos de cuentas representadas en la SRA. AWS Estos deben formar parte de los Servicios de AWS que se deben aprovisionar como parte del proceso de incorporación y creación de bases de tu cuenta. El repositorio GitHub de código proporciona un ejemplo de implementación de servicios AWS centrados en la seguridad en sus cuentas, incluida la cuenta de administración de la organización. AWS

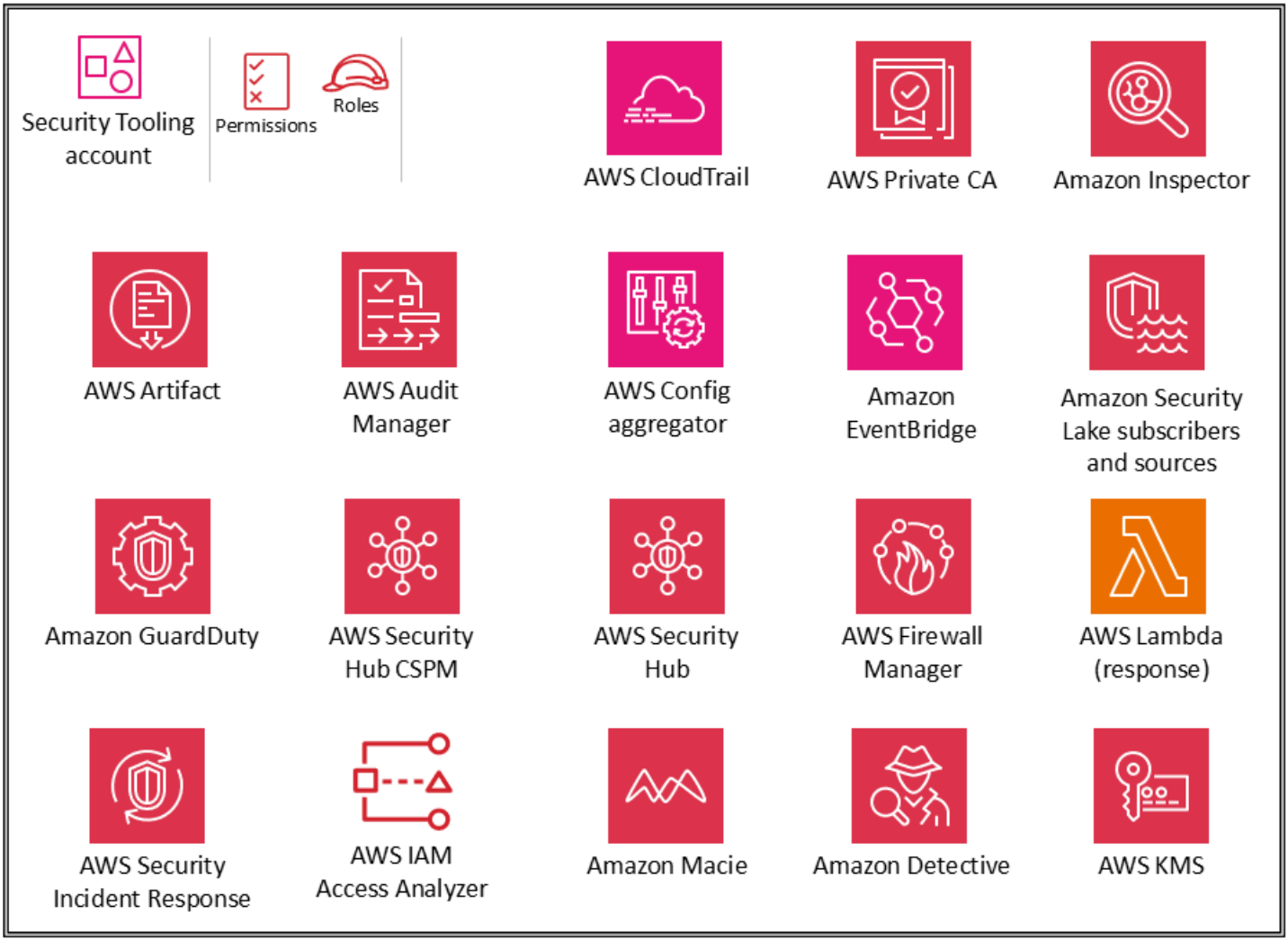
Además de estos servicios, AWS SRA incluye dos servicios centrados en la seguridad, Amazon Detective y AWS Audit Manager, que admiten la integración y la funcionalidad de administrador delegado de. AWS Organizations Sin embargo, no se incluyen como parte de los servicios recomendados para la creación de cuentas de referencia. Hemos visto que estos servicios se utilizan mejor en los siguientes escenarios:

- Cuenta con un equipo o grupo de recursos dedicados que realizan esas funciones de análisis forense digital y auditoría de TI. Los equipos de analistas de seguridad utilizan mejor Detective, y Audit Manager es útil para sus equipos de auditoría interna o cumplimiento.
- Desea centrarse en un conjunto básico de herramientas AWS Config, como Amazon GuardDuty AWS Security Hub, y AWS Security Hub CSPM al principio de su proyecto, y luego desarrollarlas mediante el uso de servicios que proporcionan capacidades adicionales.

UO de seguridad: cuenta de herramientas de seguridad

Influya en el futuro de la arquitectura de referencia de AWS seguridad (AWS SRA) realizando una breve encuesta.

El siguiente diagrama ilustra los servicios AWS de seguridad que están configurados en la cuenta Security Tooling.



La cuenta Security Tooling está dedicada a operar los servicios de seguridad Cuentas de AWS, monitorear y automatizar las alertas y respuestas de seguridad. Los objetivos de seguridad incluyen los siguientes:

- Proporcione una cuenta dedicada con acceso controlado para gestionar el acceso a las barandillas de seguridad, la supervisión y la respuesta.
- Mantenga la infraestructura de seguridad centralizada adecuada para monitorear los datos de las operaciones de seguridad y mantener la trazabilidad. La detección, la investigación y la respuesta son partes esenciales del ciclo de vida de la seguridad y se pueden utilizar para respaldar un proceso de calidad, una obligación legal o de cumplimiento y para las iniciativas de identificación y respuesta a las amenazas.
- Respalde aún más defense-in-depth la estrategia de la organización manteniendo otro nivel de control sobre la configuración y las operaciones de seguridad adecuadas, como las claves de cifrado y la configuración de los grupos de seguridad. Se trata de una cuenta en la que trabajan los operadores de seguridad. Las funciones de solo lectura o de auditoría para ver la información de AWS toda la organización son habituales, mientras que las write/modify funciones son limitadas en número y están estrictamente controladas, supervisadas y registradas.

Consideraciones sobre el diseño

- AWS Control Tower De forma predeterminada, asigna a la cuenta el nombre de cuenta de seguridad ou de auditoría. Puede cambiar el nombre de la cuenta durante la AWS Control Tower configuración.
- Podría ser adecuado tener más de una cuenta de Security Tooling. Por ejemplo, la supervisión y la respuesta a los eventos de seguridad suelen asignarse a un equipo especializado. La seguridad de la red puede requerir su propia cuenta y funciones en colaboración con la infraestructura de la nube o el equipo de red. Estas divisiones mantienen el objetivo de separar los enclaves de seguridad centralizados y hacen aún más hincapié en la separación de funciones, los privilegios mínimos y la posible simplicidad de las tareas en equipo. Si lo está utilizando AWS Control Tower, restringe la creación de otros en Cuentas de AWS virtud de la unidad organizativa de seguridad.

Administrador delegado de los servicios de seguridad

La cuenta Security Tooling sirve como cuenta de administrador para los servicios de seguridad que se administran en una administrator/member estructura en todo el. Cuentas de AWS Como se ha mencionado anteriormente, esto se gestiona mediante la función de administrador AWS Organizations delegado. Los servicios de la AWS SRA que actualmente admiten el administrador

delegado incluyen la administración centralizada de IAM del acceso raíz, AWS Firewall Manager Amazon AWS Config, IAM Access GuardDuty Analyzer, Amazon Macie,, Amazon Detective AWS Security Hub, AWS Security Hub CSPM AWS Audit Manager Amazon Inspector y. AWS CloudTrail AWS Systems Manager Su equipo de seguridad administra las funciones de seguridad de estos servicios y supervisa cualquier evento o hallazgo específico de seguridad.

AWS IAM Identity Center admite la administración delegada en la cuenta de un miembro. AWS SRA utiliza la cuenta de Servicios Compartidos como cuenta de administrador delegado para el Centro de Identidad de IAM, tal y como se explica más adelante en la sección Centro de Identidad de IAM de la cuenta de Servicios Compartidos.

Acceso raíz centralizado

La cuenta Security Tooling es la cuenta de administrador delegado para la administración centralizada de la capacidad de acceso raíz de IAM. Esta capacidad debe habilitarse a nivel de la organización al permitir la administración de credenciales y la acción raíz privilegiada en las cuentas de los miembros. Los administradores delegados deben disponer de `sts:AssumeRoot` permisos explícitos para poder realizar acciones de raíz privilegiadas en nombre de las cuentas de los miembros. Este permiso solo está disponible después de habilitar la acción raíz privilegiada en la cuenta de un miembro en la cuenta de administración de la organización o de administrador delegado. Con este permiso, los usuarios pueden realizar tareas de usuario raíz con privilegios en las cuentas de los miembros de forma centralizada desde la cuenta Security Tooling. Tras iniciar una sesión privilegiada, puede eliminar una política de bucket de S3 mal configurada, eliminar una política de colas de SQS mal configurada, eliminar las credenciales de usuario raíz de una cuenta de miembro y volver a habilitar las credenciales de usuario raíz de una cuenta de miembro. Puede realizar estas acciones desde la consola, mediante () o mediante. AWS Command Line Interface AWS CLI APIs

AWS CloudTrail

AWS CloudTrailes un servicio que respalda la gobernanza, el cumplimiento y la auditoría de la actividad de su empresa Cuenta de AWS. Con CloudTrail él, puede registrar, monitorear continuamente y retener la actividad de la cuenta relacionada con las acciones en toda su AWS infraestructura. CloudTrail está integrado con AWS Organizations, y esa integración se puede utilizar para crear un registro único que registre todos los eventos de todas las cuentas de la AWS organización. Esto es lo que se denomina registro de seguimiento de organización. Puede crear y administrar un registro de la organización solo desde la cuenta de administración de la organización o desde una cuenta de administrador delegado. Al crear un registro de la organización, se crea

un registro con el nombre que especifique en cada uno de los registros Cuenta de AWS que pertenezcan a su AWS organización. El registro registra la actividad de todas las cuentas de la AWS organización, incluida la cuenta de administración, y almacena los registros en un único depósito de S3. Debido a la sensibilidad de este depósito de S3, debe protegerlo siguiendo las prácticas recomendadas que se describen en la sección Amazon S3 como almacén de registros central, más adelante en esta guía. Todas las cuentas de la AWS organización pueden ver el registro de la organización en su lista de registros. Sin embargo, los miembros Cuentas de AWS tienen acceso de solo lectura a este sendero. De forma predeterminada, al crear un registro de la organización en la CloudTrail consola, el registro es multirregional. Para obtener más información sobre las mejores prácticas de seguridad, consulte la CloudTraildocumentación.

En la AWS SRA, la cuenta Security Tooling es la cuenta de administrador delegado para la administración. CloudTrail El depósito de S3 correspondiente para almacenar los registros de seguimiento de la organización se crea en la cuenta Log Archive. Esto sirve para separar la administración y el uso de los privilegios de CloudTrail registro. Para obtener información sobre cómo crear o actualizar un bucket de S3 para almacenar los archivos de registro para el registro de una organización, consulte la CloudTrail documentación. Como práctica recomendada de seguridad, añada la clave de `aws:SourceArn` condición del registro de la organización a la política de recursos del bucket de S3 (y a cualquier otro recurso, como las claves de KMS o los temas de SNS). Esto garantiza que el bucket de S3 solo acepte los datos asociados al registro específico. El rastro se configura con la validación del archivo de registro para validar la integridad del archivo de registro. Los archivos de registro y resumen se cifran mediante SSE-KMS. El registro de la organización también está integrado con un grupo de CloudWatch registros en Logs para enviar los eventos y conservarlos a largo plazo.

> **Note**
>
> Puede crear y administrar registros de la organización desde cuentas de administración y de administrador delegado. Sin embargo, como práctica recomendada, debes limitar el acceso a la cuenta de administración y utilizar la funcionalidad de administrador delegado cuando esté disponible.

> **Consideraciones sobre el diseño**
>
> - CloudTrail no registra los eventos de datos de forma predeterminada, ya que suelen ser actividades de gran volumen. Sin embargo, debe capturar los eventos de datos para AWS

recursos críticos específicos, como los depósitos de S3, las funciones de Lambda, los eventos de registro AWS externos que se envían al lago y CloudTrail los temas de SNS. Para ello, configure el registro de su organización para que incluya eventos de datos de recursos específicos especificando los ARNs de cada recurso individual.

- Si la cuenta de un miembro necesita acceder a los archivos de CloudTrail registro de su propia cuenta, puede compartir los archivos de CloudTrail registro de la organización de forma selectiva desde el depósito central de S3. Sin embargo, si las cuentas de los miembros requieren grupos de CloudWatch registros locales de Amazon para CloudTrail los registros de sus cuentas o si desean configurar la administración de registros y los eventos de datos (solo lectura, solo de escritura, eventos de administración, eventos de datos) de manera diferente al registro de la organización, pueden crear un registro local con los controles adecuados. Los registros específicos de las cuentas locales conllevan un coste adicional.

AWS Security Hub CSPM

AWS Security Hub La gestión de la postura de seguridad en la nube (AWS Security Hub CSPM), anteriormente conocida como AWS Security Hub, le proporciona una visión completa de su postura de seguridad AWS y le ayuda a comparar su entorno con los estándares y las mejores prácticas del sector de la seguridad. Security Hub CSPM recopila datos de seguridad de todos los servicios AWS integrados, productos de terceros compatibles y otros productos de seguridad personalizados que pueda utilizar. Le ayuda a supervisar y analizar continuamente sus tendencias de seguridad e identificar los problemas de seguridad de mayor prioridad. Además de las fuentes ingeridas, Security Hub CSPM genera sus propios hallazgos, que están representados por controles de seguridad que se ajustan a uno o más estándares de seguridad. Estos estándares incluyen las mejores prácticas de seguridad AWS fundamentales (FSBP), el Center for Internet Security (CIS) AWS Foundations Benchmark v1.20 y v1.4.0, el SP 800-53 Rev. 5 del Instituto Nacional de Estándares y Tecnología (NIST), el Estándar de seguridad de datos de la industria de tarjetas de pago (PCI DSS) y los estándares de administración de servicios. Para obtener una lista de los estándares de seguridad actuales y detalles sobre controles de seguridad específicos, consulte la referencia de estándares para Security Hub CSPM en la documentación de Security Hub CSPM.

Security Hub con el que CSPM se integra AWS Organizations para simplificar la administración del estado de seguridad en todas las cuentas actuales y futuras de su AWS organización. Puede utilizar la función de configuración central CSPM de Security Hub desde la cuenta de administrador delegado (en este caso, Security Tooling) para especificar cómo se configuran el servicio CSPM de

Security Hub, los estándares de seguridad y los controles de seguridad en las cuentas y unidades organizativas de su organización () en todas las regiones. OUs Puede configurar estos ajustes en unos pocos pasos desde una región principal, que se denomina región de origen. Si no utiliza la configuración central, debe configurar Security Hub CSPM por separado en cada cuenta y región. El administrador delegado puede designar las cuentas OUs como autoadministrables, de forma que el miembro puede configurar los ajustes por separado en cada región, o bien administrarlas de forma centralizada, donde el administrador delegado puede configurar la cuenta del miembro o la unidad organizativa en todas las regiones. Puede designar todas las cuentas de su organización como OUs administradas de forma centralizada, todas autogestionadas o como una combinación de ambas. Esto simplifica la aplicación de una configuración coherente y, al mismo tiempo, proporciona la flexibilidad de modificarla para cada unidad organizativa y cuenta.

La cuenta de administrador delegado CSPM de Security Hub también puede ver los hallazgos, ver información y controlar los detalles de todas las cuentas de los miembros. Además, puede designar una región de agregación dentro de la cuenta de administrador delegado para centralizar los hallazgos en sus cuentas y en las regiones vinculadas. Sus resultados se sincronizan de forma continua y bidireccional entre la región agregadora y todas las demás regiones.

Security Hub CSPM admite integraciones con varios. Servicios de AWS Amazon GuardDuty AWS Config, Amazon Macie, IAM Access Analyzer, Amazon AWS Firewall Manager Inspector, Amazon Route 53 Resolver DNS Firewall y AWS Systems Manager Patch Manager pueden enviar los resultados a Security Hub CSPM. Security Hub CSPM procesa las conclusiones mediante un formato estándar denominado AWS Security Finding Format (ASFF). Security Hub CSPM correlaciona los hallazgos entre los productos integrados para priorizar los más importantes. Puede enriquecer los metadatos de las conclusiones del CSPM de Security Hub para ayudar a contextualizar mejor las conclusiones de seguridad, priorizarlas y tomar medidas al respecto. Este enriquecimiento agrega etiquetas de recursos, una nueva etiqueta de AWS aplicación e información sobre el nombre de la cuenta a cada hallazgo que se ingiera en Security Hub CSPM. Esto le ayuda a ajustar los resultados para las reglas de automatización, a buscar o filtrar los hallazgos y la información y a evaluar el estado de la seguridad por aplicación. Además, puede utilizar las reglas de automatización para actualizar automáticamente los hallazgos. A medida que Security Hub CSPM ingiere los hallazgos, puede aplicar una variedad de acciones de reglas, como suprimir los hallazgos, cambiar su gravedad y añadir notas a los hallazgos. Estas reglas entran en vigor cuando los resultados coinciden con los criterios especificados, como el recurso o la cuenta a los que está asociado IDs el hallazgo o su título. Puede utilizar las reglas de automatización para actualizar los campos de búsqueda seleccionados en el ASFF. Las reglas se aplican tanto a los hallazgos nuevos como a los actualizados.

Durante la investigación de un incidente de seguridad, puedes ir del Security Hub CSPM a Amazon Detective para investigar un GuardDuty hallazgo. Security Hub CSPM recomienda alinear las cuentas de administrador delegado para servicios como Detective (donde existan) para una integración más fluida. Por ejemplo, si no alinea las cuentas de administrador entre Detective y Security Hub CSPM, no funcionará pasar de los hallazgos a Detective. Para obtener una lista completa, consulte Descripción general de Servicio de AWS las integraciones con Security Hub CSPM en la documentación de Security Hub CSPM.

Puede utilizar Security Hub CSPM con la función Network Access Analyzer de Amazon VPC para supervisar de forma continua el cumplimiento de la configuración de la red. AWS Esto le ayudará a bloquear el acceso no deseado a la red y a evitar el acceso externo a sus recursos críticos. Para obtener más detalles sobre la arquitectura y la implementación, consulte la entrada del AWS blog Verificación continua del cumplimiento de la red mediante Amazon VPC Network Access Analyzer y. AWS Security Hub CSPM

Además de sus funciones de monitoreo, Security Hub CSPM admite la integración con Amazon EventBridge para automatizar la corrección de hallazgos específicos. Puede definir las acciones personalizadas que se llevarán a cabo cuando se reciba un hallazgo. Por ejemplo, puede configurar acciones personalizadas para enviar resultados a un sistema de tickets o a un sistema de corrección automático. Para obtener más información y ejemplos, consulte las publicaciones del AWS blog Automated Response and remediation with AWS Security Hub CSPM y Cómo implementar la AWS solución para Security Hub CSPM Automated Response and remediation.

Security Hub CSPM utiliza servicios vinculados Reglas de AWS Config para realizar la mayoría de las comprobaciones de seguridad de los controles. Para admitir estos controles, AWS Config debe estar habilitado en todas las cuentas, incluidas la cuenta de administrador (o administrador delegado) y las cuentas de los miembros, en todas las que Security Región de AWS Hub CSPM esté habilitado.

Consideraciones sobre el diseño

- Si un estándar de cumplimiento, como PCI-DSS, ya está presente en el Security Hub CSPM, el servicio CSPM de Security Hub totalmente gestionado es la forma más sencilla de ponerlo en funcionamiento. Sin embargo, si desea crear su propio estándar de cumplimiento o seguridad, que puede incluir comprobaciones de seguridad, operativas o de optimización de costes, los paquetes de conformidad ofrecen un proceso de personalización simplificado. AWS Config (Para obtener más información sobre los paquetes de conformidad AWS Config y los paquetes de conformidad, consulte la AWS Configsección).

- Los casos de uso más comunes de Security Hub CSPM incluyen los siguientes:
  - Como panel que proporciona visibilidad a los propietarios de aplicaciones sobre la postura de seguridad y cumplimiento de sus recursos AWS
  - Como punto de vista central de las conclusiones de seguridad que utilizan las operaciones de seguridad, el personal de respuesta a incidentes y los cazadores de amenazas para clasificar las conclusiones en materia de AWS seguridad y conformidad y tomar medidas al respecto en todas las regiones Cuentas de AWS
  - Para agrupar y canalizar los hallazgos en materia de seguridad y conformidad de todas Cuentas de AWS las regiones a un sistema centralizado de gestión de eventos e información de seguridad (SIEM) u otro sistema de coordinación de la seguridad

  Para obtener orientación adicional sobre estos casos de uso, incluido cómo configurarlos, consulte la entrada del blog Tres patrones de uso recurrentes de CSPM de Security Hub y cómo implementarlos.

Ejemplo de implementación

La biblioteca de códigos AWS SRA proporciona un ejemplo de implementación de Security Hub CSPM. Incluye la activación automática del servicio, la administración delegada a una cuenta de miembro (Security Tooling) y la configuración para habilitar Security Hub CSPM para todas las cuentas existentes y futuras de la organización. AWS

AWS Security Hub

AWS Security Hubes una solución de seguridad en la nube unificada que prioriza sus amenazas de seguridad críticas y le ayuda a responder a gran escala. Security Hub detecta los problemas de seguridad casi en tiempo real al correlacionar y enriquecer automáticamente las señales de seguridad de múltiples fuentes, como la gestión de la postura (AWS Security Hub CSPM), la gestión de vulnerabilidades (Amazon Inspector), los datos confidenciales (Amazon Macie) y la detección de amenazas (Amazon). GuardDuty Esta capacidad permite que los equipos de seguridad identifiquen y prioricen los riesgos activos en los entornos en la nube mediante análisis automatizados e información contextual. Security Hub proporciona una representación visual de la posible ruta de ataque que los atacantes pueden aprovechar para acceder a los recursos asociados a una detección

de exposición. Esto transforma las señales de seguridad complejas en información procesable, para que pueda tomar decisiones informadas sobre su seguridad rápidamente.

Security Hub se ha rediseñado estratégicamente para simplificar la habilitación de los componentes básicos de los servicios de seguridad asociados a fin de llegar a un resultado de seguridad. Al correlacionar los hallazgos de seguridad en una matriz de amenazas entre diferentes señales de seguridad prácticamente en tiempo real, puede priorizar primero los riesgos más críticos. Los hallazgos se correlacionan para detectar la exposición asociada AWS a los recursos. Las exposiciones representan debilidades más amplias en los controles de seguridad, errores de configuración u otras áreas que podrían ser aprovechadas por las amenazas activas. Por ejemplo, una exposición podría ser una instancia de EC2 a la que se pueda acceder desde Internet y que presente vulnerabilidades de software con una alta probabilidad de explotación.

Security Hub y Security Hub CSPM son servicios complementarios. Security Hub CSPM proporciona una visión completa de su postura de seguridad y le ayuda a evaluar su entorno de nube con respecto a los estándares y las mejores prácticas del sector de la seguridad. Security Hub proporciona una experiencia unificada que le ayuda a priorizar y responder a los problemas de seguridad críticos. Los resultados del CSPM de Security Hub se envían automáticamente a Security Hub, donde se correlacionan con resultados de otros servicios de seguridad, como Amazon Inspector, para generar exposiciones. Esto ayuda a identificar los riesgos más críticos en el entorno.

Security Hub también proporciona un resumen de los recursos de su AWS entorno por tipo y las conclusiones asociadas. Los recursos se priorizan según las exposiciones y las secuencias de ataque. Al elegir un tipo de recurso, puede revisar todos los recursos asociados a ese tipo de recurso.

Para una experiencia óptima, recomendamos habilitar Security Hub y Security Hub CSPM, así como habilitar estos otros servicios de seguridad: Amazon GuardDuty, Amazon Inspector y Amazon Macie. Puede ver si estos servicios y funciones están habilitados de manera uniforme en todas las cuentas de los miembros de su organización mediante los resultados de cobertura de Security Hub.

En la AWS SRA, la cuenta Security Tooling actúa como administradora delegada de Security Hub, Security Hub CSPM y otros servicios de seguridad. AWS En la cuenta Security Tooling, puede ver todos los recursos asociados a las cuentas de los miembros. También puedes ver todos los recursos de tu hogar Región de AWS desde Linked Regiones de AWS.

Nota de implementación

La activación de Security Hub requiere tres pasos, incluidos los procedimientos que tienen en cuenta si se ha activado previamente el Security Hub CSPM. Security Hub está integrado de forma nativa con AWS Organizations, lo que simplifica el proceso de configuración e implementación, y centraliza y agrega todos los hallazgos en una sola ubicación. De acuerdo con las prácticas recomendadas de la AWS SRA, utilice la cuenta Security Tooling como cuenta de administrador delegado para gestionar y configurar Security Hub. Usa los ajustes de configuración de Security Hub para habilitar automáticamente todas las regiones y cuentas, incluidas las futuras regiones y cuentas. OUs También debe configurar la agregación entre regiones para agregar hallazgos, recursos y tendencias de varias regiones Regiones de AWS en una sola región de origen. Durante la configuración, también puedes habilitar cualquier integración nativa, como Jira Cloud o. ServiceNow

Consideraciones sobre el diseño

- Los resultados de Security Hub están formateados en el Open Cybersecurity Schema Framework (OCSF). Security Hub genera hallazgos en OCSF y recibe hallazgos en OCSF de Security Hub, CSPM y otros. Servicios de AWS Estos hallazgos de OCSF se pueden enviar a través de Amazon EventBridge para automatizarlos o se pueden almacenar en una cuenta central de agregación de registros para realizar el análisis y la retención de los registros de seguridad.
- La cuenta de administración de la AWS organización no puede designarse a sí misma como la administradora delegada en Security Hub. Esto se ajusta a la práctica recomendada de la AWS SRA de designar la cuenta Security Tooling como administradora delegada. Tenga en cuenta también lo siguiente:
  - La cuenta de administrador designada para Security Hub CSPM se convierte automáticamente en el administrador designado para Security Hub.
  - Al eliminar la administración delegada a través de Security Hub, también se elimina la administración delegada de Security Hub CSPM. Del mismo modo, al eliminar la administración delegada a través de Security Hub (CSPM), también se elimina para Security Hub.

- Security Hub incluye funciones que modifican automáticamente los hallazgos y toman medidas en función de sus especificaciones. Security Hub admite los siguientes tipos de automatizaciones:
  - Reglas de automatización, que actualizan automáticamente los hallazgos, los suprimen y los envían a las herramientas de emisión de tickets casi en tiempo real en función de criterios definidos.
  - Respuesta y corrección automatizadas, que crean EventBridge reglas personalizadas que definen las acciones automáticas que se deben tomar en función de hallazgos e información específicos.
- Security Hub puede configurar Amazon Inspector en todas las cuentas y regiones de los miembros mediante políticas, y puede configurar GuardDuty un Security Hub CSPM durante la implementación. Las políticas generan AWS Organizations políticas para cuentas y regiones. Los despliegues son acciones que se realizan una sola vez y que permiten una funcionalidad de seguridad en determinadas cuentas y regiones. Las implementaciones no se aplican a las cuentas recién habilitadas. Como alternativa, puede habilitar automáticamente las funciones para las cuentas de los nuevos miembros en GuardDuty Security Hub CSPM.

Amazon GuardDuty

Amazon GuardDuty es un servicio de detección de amenazas que monitorea continuamente la actividad maliciosa y el comportamiento no autorizado para proteger tus cargas de trabajo Cuentas de AWS y las tuyas. Siempre debe capturar y almacenar los registros adecuados para fines de supervisión y auditoría, pero GuardDuty extrae flujos de datos independientes directamente de los registros de AWS CloudTrail flujo de Amazon VPC AWS y los registros de DNS. No tiene que gestionar las políticas de bucket de Amazon S3 ni modificar la forma en que recopila y almacena los registros. GuardDutylos permisos se administran como funciones vinculadas al servicio que puede revocar en cualquier momento desactivándolas. GuardDuty Esto facilita la activación del servicio sin una configuración compleja y elimina el riesgo de que una modificación de los permisos de IAM o un cambio en la política del bucket de S3 afecten al funcionamiento del servicio.

Además de proporcionar fuentes de datos fundamentales, GuardDuty ofrece funciones opcionales para identificar los hallazgos de seguridad. Estas incluyen EKS Protection, RDS Protection, S3 Protection, Malware Protection y Lambda Protection. En el caso de los detectores nuevos, estas

funciones opcionales están habilitadas de forma predeterminada, excepto la protección EKS, que debe activarse manualmente.

- Con GuardDuty S3 Protection, GuardDuty supervisa los eventos de datos de Amazon S3 CloudTrail además de los eventos CloudTrail de administración predeterminados. La supervisión de los eventos de datos GuardDuty permite supervisar las operaciones de la API a nivel de objeto para detectar posibles riesgos de seguridad para los datos contenidos en sus depósitos de S3.
- GuardDuty Malware Protection detecta la presencia de malware en las instancias de Amazon EC2 o en las cargas de trabajo de contenedores al iniciar escaneos sin agente en los volúmenes adjuntos de Amazon Elastic Block Store (Amazon EBS). GuardDuty también detecta el posible malware en los depósitos de S3 escaneando los objetos recién cargados o las nuevas versiones de los objetos existentes.
- GuardDuty La protección RDS está diseñada para perfilar y monitorear la actividad de acceso a las bases de datos de Amazon Aurora sin afectar al rendimiento de las bases de datos.
- GuardDuty EKS Protection incluye EKS Audit Log Monitoring y EKS Runtime Monitoring. Con EKS Audit Log Monitoring, GuardDuty supervisa los registros de auditoría de Kubernetes de los clústeres de Amazon EKS y los analiza para detectar posibles actividades maliciosas y sospechosas. EKS Runtime Monitoring utiliza el agente de GuardDuty seguridad (que es un complemento de Amazon EKS) para proporcionar visibilidad en tiempo de ejecución de las cargas de trabajo individuales de Amazon EKS. El agente GuardDuty de seguridad ayuda a identificar contenedores específicos dentro de sus clústeres de Amazon EKS que puedan estar en peligro. También puede detectar los intentos de escalar los privilegios de un contenedor individual al host Amazon EC2 subyacente o al AWS entorno más amplio.

GuardDuty también proporciona una función conocida como detección extendida de amenazas que detecta automáticamente los ataques en varias etapas que abarcan fuentes de datos, varios tipos de AWS recursos y tiempos dentro de un mismo espacio. Cuenta de AWS GuardDutycorrelaciona estos eventos, que se denominan señales, para identificar los escenarios que se presentan como posibles amenazas para su AWS entorno y, a continuación, genera una búsqueda de la secuencia de ataque. Esto abarca los escenarios de amenazas que implican un compromiso relacionado con el uso indebido de AWS las credenciales y los intentos de comprometer sus Cuentas de AWS datos. GuardDuty considera críticos todos los tipos de búsqueda de secuencias de ataques. Esta función está habilitada de forma predeterminada y no conlleva ningún coste adicional.

En la AWS SRA, GuardDuty está habilitada en todas las cuentas y AWS Organizations los equipos de seguridad correspondientes pueden ver y procesar todas las conclusiones en la cuenta del

administrador GuardDuty delegado (en este caso, la cuenta Security Tooling). GuardDuty Los resultados activos se exportan a un depósito central de S3 en la cuenta de Log Archive, para que pueda conservarlos durante más de 90 días. Los resultados se exportan desde la cuenta de administrador delegado y también incluyen todos los hallazgos de las cuentas de los miembros asociadas en la misma región. Los resultados del depósito de S3 se cifran con una clave gestionada por el AWS KMS cliente. La política de bucket de S3 y la política de claves de KMS están configuradas para permitir el uso exclusivo de los recursos. GuardDuty

Cuando AWS Security Hub CSPM está habilitada, GuardDuty los resultados fluyen automáticamente al Security Hub (CSPM) y al Security Hub. Cuando Amazon Detective está activado, GuardDuty los hallazgos se incluyen en el proceso de ingesta de registros de Detective. GuardDuty y Detective admiten flujos de trabajo de usuarios multiservicio, donde GuardDuty proporciona enlaces desde la consola que lo redirigen desde un hallazgo seleccionado a una página de Detectives que contiene un conjunto de visualizaciones seleccionadas para investigar ese hallazgo. Por ejemplo, también puedes integrarte GuardDuty con Amazon EventBridge para automatizar las mejores prácticas GuardDuty, como la automatización de las respuestas a los nuevos GuardDuty hallazgos.

> **Ejemplo de implementación**
>
> La biblioteca de códigos AWS SRA proporciona un ejemplo de implementación de GuardDuty. Incluye la configuración de buckets S3 cifrados, la administración delegada y la GuardDuty activación de todas las cuentas existentes y futuras de la organización. AWS

AWS Config

AWS Configes un servicio que le permite evaluar, auditar y evaluar las configuraciones de los AWS recursos compatibles en su empresa. Cuentas de AWS AWS Config supervisa y registra continuamente las configuraciones AWS de los recursos y evalúa automáticamente las configuraciones registradas comparándolas con las configuraciones deseadas. También puede integrarlo AWS Config con otros servicios para realizar el trabajo pesado de los procesos automatizados de auditoría y supervisión. Por ejemplo, AWS Config puede monitorear los cambios en los secretos individuales de. AWS Secrets Manager

Puede evaluar los ajustes de configuración de sus AWS recursos mediante Reglas de AWS Config. AWS Config proporciona una biblioteca de reglas predefinidas y personalizables denominadas reglas administradas. También puede escribir sus propias reglas personalizadas. Puede ejecutar Reglas de AWS Config en modo proactivo (antes de que se hayan desplegado los recursos) o en modo

detective (después de que se hayan desplegado los recursos). Los recursos se pueden evaluar cuando hay cambios de configuración, de forma periódica o en ambos casos.

Un paquete de conformidad es un conjunto de AWS Config reglas y acciones correctivas que se pueden implementar como una sola entidad en una cuenta y una región, o en toda la organización. AWS Organizations Los paquetes de conformidad se crean mediante la creación de una plantilla YAML que contiene la lista de reglas AWS Config administradas o personalizadas y acciones de corrección. Para empezar a evaluar su AWS entorno, utilice una de las plantillas de paquetes de conformidad de ejemplo.

AWS Config se integra AWS Security Hub CSPM para enviar los resultados de las evaluaciones de reglas AWS Config gestionadas y personalizadas como hallazgos al Security Hub CSPM.

Reglas de AWS Config se puede usar junto con para corregir eficazmente los recursos AWS Systems Manager que no cumplen con las normas. Utiliza Systems Manager Explorer para recopilar el estado de conformidad de AWS Config las reglas en su interfaz Regiones de AWS y, Cuentas de AWS a continuación, utiliza los documentos de automatización de Systems Manager (manuales de ejecución) para resolver las reglas no conformes AWS Config . Para obtener información detallada sobre la implementación, consulte la entrada del blog Remedie AWS Config las reglas no conformes con los manuales de automatización. AWS Systems Manager

El AWS Config agregador recopila datos de configuración y cumplimiento de varias cuentas, regiones y organizaciones en. AWS Organizations El panel del agregador muestra los datos de configuración de los recursos agregados. Los paneles de inventario y cumplimiento ofrecen información esencial y actualizada sobre las configuraciones de sus AWS recursos y el estado de cumplimiento en toda la organización Cuentas de AWS, dentro de Regiones de AWS ella o dentro de ella. AWS Le permiten visualizar y evaluar su inventario de AWS recursos sin necesidad de escribir consultas AWS Config avanzadas. Puede obtener información esencial, como un resumen del cumplimiento por recursos, las 10 cuentas principales que tienen recursos que no cumplen con las normas, una comparación de las instancias de EC2 en ejecución y detenidas por tipo y de los volúmenes de EBS por tipo y tamaño de volumen.

Si lo utiliza AWS Control Tower para administrar su AWS organización, esta implementará un conjunto de AWS Config reglas como barreras de detección (clasificadas como obligatorias, altamente recomendadas o optativas). Estas barreras le ayudan a controlar sus recursos y a supervisar el cumplimiento en todas las cuentas de su organización. AWS Estas AWS Config reglas utilizarán automáticamente una `aws-control-tower` etiqueta con un valor de. `managed-by-control-tower`

AWS Config debe estar habilitada para cada cuenta de miembro de la AWS organización y Región de AWS debe contener los recursos que desee proteger. Puede administrar de forma centralizada las AWS Config reglas (por ejemplo, crear, actualizar y eliminar) en todas las cuentas de su AWS organización. Desde la cuenta de administrador AWS Config delegado, puede implementar un conjunto común de AWS Config reglas en todas las cuentas y especificar las cuentas en las que no se deben crear AWS Config reglas. La cuenta de administrador AWS Config delegado también puede agregar los datos de conformidad y configuración de los recursos de todas las cuentas de los miembros para ofrecer una vista única. Utilice los APIs datos de la cuenta de administrador delegado para reforzar la gobernanza y garantizar que las cuentas de los miembros de su AWS organización no puedan modificar las AWS Config reglas subyacentes. AWS Config está integrado de forma nativa para enviar las conclusiones si Security Hub CSPM está habilitado y existe al menos una regla AWS Config gestionada o personalizada. AWS Security Hub CSPM

En la AWS SRA, la cuenta de administrador AWS Config delegado es la cuenta Security Tooling. El canal AWS Config de entrega está configurado para entregar instantáneas de la configuración de los recursos en un depósito S3 centralizado en la cuenta de Log Archive. Como la cuenta Log Archive es el almacén central del repositorio de registros, se utiliza para almacenar la configuración de los recursos.

Consideraciones sobre el diseño

- AWS Config transmite las notificaciones de cambios de configuración y conformidad a Amazon EventBridge. Esto significa que puede utilizar las capacidades de filtrado nativas EventBridge para filtrar AWS Config eventos y así dirigir tipos específicos de notificaciones a destinos específicos. Por ejemplo, puede enviar notificaciones de conformidad para reglas o tipos de recursos específicos a direcciones de correo electrónico específicas, o enrutar las notificaciones de cambios de configuración a una herramienta externa de administración de servicios de TI (ITSM) o base de datos de administración de la configuración (CMDB). Para obtener más información, consulte la entrada del blog sobre las AWS Config mejores prácticas.
- Además de utilizar una evaluación AWS Config proactiva de las reglas, puede utilizar AWS CloudFormation Guardla herramienta de policy-as-code evaluación que comprueba de forma proactiva el cumplimiento de la configuración de los recursos. La interfaz de línea de AWS CloudFormation Guard comandos (CLI) le proporciona un lenguaje declarativo de dominio específico (DSL) que puede utilizar para expresar la política como código. Además, puede usar AWS CLI comandos para validar datos estructurados con formato

JSON o con formato YAML, como conjuntos de CloudFormation cambios, archivos de configuración de Terraform basados en JSON o configuraciones de Kubernetes. Puede ejecutar las evaluaciones localmente mediante la AWS CloudFormation Guard CLI como parte del proceso de creación o ejecutarlas dentro de su proceso de implementación. Si tiene AWS Cloud Development Kit (AWS CDK)aplicaciones, puede utilizar cdk-nag para comprobar proactivamente las mejores prácticas.

Ejemplo de implementación

La biblioteca de códigos AWS SRA proporciona un ejemplo de implementación que implementa paquetes de AWS Config conformidad en todas Cuentas de AWS las regiones de una organización. AWS El módulo AWS Config Aggregator le ayuda a configurar un AWS Config agregador al delegar la administración a una cuenta de miembro (Security Tooling) dentro de la cuenta de administración de la organización y, a continuación, configurar AWS Config Aggregator dentro de la cuenta de administrador delegado para todas las cuentas existentes y futuras de la organización. AWS Puede usar el módulo de cuentas de administración de la Torre de AWS Config Control para activarlo AWS Config dentro de la cuenta de administración de la organización; no está habilitado por. AWS Control Tower

Amazon Security Lake

Amazon Security Lake es un servicio de lago de datos de seguridad totalmente gestionado. Puede usar Security Lake para centralizar automáticamente los datos de seguridad de AWS entornos, proveedores de software como servicio (SaaS), locales y fuentes de terceros. Security Lake le ayuda a crear una fuente de datos normalizada que simplifica el uso de herramientas de análisis en relación con los datos de seguridad, de modo que pueda comprender mejor su postura de seguridad en toda la organización. El lago de datos está respaldado por buckets de Amazon Simple Storage Service (Amazon S3) y usted retiene la propiedad de sus datos. Security Lake recopila automáticamente los registros de Servicios de AWS Amazon VPC AWS CloudTrail, Amazon Route 53, Amazon S3 y los registros de auditoría, AWS Security Hub CSPM hallazgos y AWS WAF registros de AWS Lambda Amazon EKS.

AWS La SRA recomienda que utilice la cuenta Log Archive como cuenta de administrador delegado de Security Lake. Para obtener más información sobre la configuración de la cuenta de administrador delegado, consulte Amazon Security Lake en la sección Security OU – Cuenta de Log Archive. Los

equipos de seguridad que deseen acceder a los datos de Security Lake o que necesiten la capacidad de escribir registros no nativos en los buckets de Security Lake mediante funciones personalizadas de extracción, transformación y carga (ETL) deben operar dentro de la cuenta de Security Tooling.

Security Lake puede recopilar registros de diferentes proveedores de nube, registros de soluciones de terceros u otros registros personalizados. Le recomendamos que utilice la cuenta Security Tooling para realizar las funciones de ETL a fin de convertir los registros al formato Open Cybersecurity Schema Framework (OCSF) y generar un archivo en formato Apache Parquet. Security Lake crea el rol multicuenta con los permisos adecuados para la cuenta de Security Tooling y la fuente personalizada respaldada por funciones o AWS Glue rastreadores de Lambda, para escribir datos en los buckets de S3 de Security Lake.

El administrador de Security Lake debe configurar los equipos de seguridad que usen la cuenta de Security Tooling y requieran acceso a los registros que Security Lake recopila como suscriptores. Security Lake admite dos tipos de acceso de suscriptores:

- Acceso a los datos: los suscriptores pueden acceder directamente a los objetos de Amazon S3 para Security Lake. Security Lake administra la infraestructura y los permisos. Al configurar la cuenta de Security Tooling como suscriptora de acceso a datos de Security Lake, la cuenta recibe una notificación de los nuevos objetos en los buckets de Security Lake a través de Amazon Simple Queue Service (Amazon SQS), y Security Lake crea los permisos para acceder a esos nuevos objetos.
- Acceso a consultas: los suscriptores pueden consultar los datos de origen de AWS Lake Formation las tablas de su bucket de S3 mediante servicios como Amazon Athena. El acceso entre cuentas se configura automáticamente para el acceso a las consultas mediante Lake Formation. Al configurar la cuenta de Security Tooling como suscriptora de acceso a consultas de Security Lake, la cuenta tiene acceso de solo lectura a los registros de la cuenta de Security Lake. Cuando utiliza este tipo de suscriptor, Athena y AWS Glue las tablas se comparten desde la cuenta Security Lake Log Archive con la cuenta Security Tooling mediante AWS Resource Access Manager ().AWS RAM Para habilitar esta función, debe actualizar la configuración del intercambio de datos entre cuentas a la versión 3.

Para obtener más información sobre la creación de suscriptores, consulte Gestión de suscriptores en la documentación de Security Lake.

Para conocer las prácticas recomendadas para la ingesta de fuentes personalizadas, consulte Recopilación de datos de fuentes personalizadas en la documentación de Security Lake.

Puede utilizar Amazon Quick Sight, Amazon OpenSearch Service y Amazon SageMaker para configurar los análisis de los datos de seguridad que almacena en Security Lake.

> **Consideración del diseño**
>
> Si un equipo de aplicaciones necesita acceder mediante consultas a los datos de Security Lake para cumplir con un requisito empresarial, el administrador de Security Lake debe configurar esa cuenta de aplicación como suscriptor.

Amazon Macie

Amazon Macie es un servicio de seguridad y privacidad de datos totalmente gestionado que utiliza el aprendizaje automático y la coincidencia de patrones para descubrir y proteger sus datos confidenciales en él. AWS Debe identificar el tipo y la clasificación de los datos que procesa su carga de trabajo para garantizar que se apliquen los controles adecuados. Puede utilizar Macie para automatizar el descubrimiento y la presentación de informes sobre datos confidenciales de dos maneras: mediante la detección automática de datos confidenciales y mediante la creación y ejecución de tareas de descubrimiento de datos confidenciales. Gracias a la detección automática de datos confidenciales, Macie evalúa su inventario de depósitos de S3 a diario y utiliza técnicas de muestreo para identificar y seleccionar objetos representativos de S3 de sus depósitos. A continuación, Macie recupera y analiza los objetos seleccionados, inspeccionándolos en busca de datos confidenciales. Los trabajos de descubrimiento de datos confidenciales proporcionan un análisis más profundo y específico. Con esta opción, puede definir la amplitud y la profundidad del análisis, incluidos los segmentos de S3 que se van a analizar, la profundidad de muestreo y los criterios personalizados que se derivan de las propiedades de los objetos de S3. Si Macie detecta un posible problema con la seguridad o la privacidad de un bucket, crea un resultado de política para usted. La detección automática de datos está habilitada de forma predeterminada para todos los nuevos clientes de Macie, y los clientes actuales de Macie pueden activarla con un solo clic.

Macie está activado en todas las cuentas de forma automática. AWS Organizations Los directores que dispongan de los permisos adecuados en la cuenta de administrador delegado (en este caso, la cuenta Security Tooling) pueden activar o suspender a Macie en cualquier cuenta, crear tareas de descubrimiento de datos confidenciales para los grupos que son propiedad de las cuentas de los miembros y consultar todos los resultados de las políticas de todas las cuentas de los miembros. Los hallazgos de datos confidenciales solo los puede ver la cuenta que creó el trabajo de hallazgos

confidenciales. Para obtener más información, consulte Administrar varias cuentas de Macie como una organización en la documentación de Macie.

Los hallazgos de Macie van a parar a ser revisados y AWS Security Hub CSPM analizados. Macie también se integra con Amazon EventBridge para facilitar las respuestas automatizadas a hallazgos como las alertas, las transmisiones a los sistemas de información de seguridad y gestión de eventos (SIEM) y la remediación automática.

Consideraciones sobre el diseño

- Si los objetos de S3 se cifran con una clave AWS Key Management Service (AWS KMS) que usted administra, puede añadir el rol vinculado al servicio de Macie como usuario clave a esa clave de KMS para que Macie pueda escanear los datos.
- Macie está optimizado para escanear objetos en Amazon S3. Como resultado, cualquier tipo de objeto compatible con MACIE que se pueda colocar en Amazon S3 (de forma permanente o temporal) se puede escanear en busca de datos confidenciales. Esto significa que los datos de otras fuentes (por ejemplo, exportaciones periódicas de instantáneas de bases de datos Amazon Relational Database Service (Amazon RDS) o Amazon Aurora, tablas exportadas de Amazon DynamoDB o archivos de texto extraídos de aplicaciones nativas o de terceros, se pueden mover a Amazon S3 y Macie puede evaluarlos.

Ejemplo de implementación

La biblioteca de códigos AWS SRA proporciona un ejemplo de implementación de Amazon Macie. Incluye delegar la administración a una cuenta de miembro y configurar Macie dentro de la cuenta de administrador delegado para todas las cuentas existentes y futuras de la organización. AWS Macie también está configurado para enviar los resultados a un depósito central de S3 cifrado con una clave gestionada por el cliente. AWS KMS

Analizador de acceso de IAM

A medida que se acelera el proceso de Nube de AWS adopción y se sigue innovando, es fundamental mantener un control estricto sobre los accesos detallados (permisos), contener la proliferación de accesos y garantizar que los permisos se utilicen de forma eficaz. El acceso excesivo

y no utilizado presenta desafíos de seguridad y dificulta que las empresas apliquen el principio de privilegios mínimos. Este principio es un pilar importante de la arquitectura de seguridad que implica ajustar continuamente el tamaño de los permisos de IAM para equilibrar los requisitos de seguridad con los requisitos operativos y de desarrollo de aplicaciones. En este esfuerzo participan múltiples partes interesadas, incluidos los equipos centrales de seguridad y del Centro de Excelencia (CCoE) de la nube, así como los equipos de desarrollo descentralizados.

AWS Identity and Access Management Access Analyzer proporciona herramientas para establecer permisos detallados de manera eficiente, verificar los permisos previstos y refinar los permisos eliminando el acceso no utilizado para ayudarlo a cumplir con los estándares de seguridad de su empresa. Le brinda visibilidad del acceso externo e interno a los AWS recursos y de los hallazgos de acceso no utilizados a través de paneles y. AWS Security Hub CSPM Además, es compatible con Amazon EventBridge para flujos de trabajo de notificación y corrección personalizados basados en eventos.

La función de resultados del analizador de acceso externo de IAM Access Analyzer le ayuda a identificar los recursos de su AWS organización y sus cuentas, como los buckets de Amazon S3 o las funciones de IAM, que se comparten con una entidad externa. La AWS organización o cuenta que elija se conoce como zona de confianza. El analizador utiliza un razonamiento automatizado para analizar todos los recursos admitidos dentro de la zona de confianza y genera conclusiones para los directores que pueden acceder a los recursos desde fuera de la zona de confianza. Estos resultados ayudan a identificar los recursos que se comparten con una entidad externa y le ayudan a obtener una vista previa de cómo afecta su política al acceso público y multicuenta a su recurso antes de implementar los permisos de los recursos. Está disponible sin coste adicional.

Del mismo modo, la función de búsqueda del analizador de acceso interno de IAM Access Analyzer le ayuda a identificar los recursos de su AWS organización y las cuentas que se comparten con los directores internos de su organización o cuenta. Este análisis respalda el principio del privilegio mínimo al garantizar que solo puedan acceder a los recursos especificados los responsables de la organización. Se trata de una función de pago y su inspección requiere una configuración explícita de los recursos. Utilice esta función con prudencia para monitorear recursos sensibles específicos que, por diseño, deben estar bloqueados incluso internamente.

Las conclusiones de IAM Access Analyzer también le ayudan a identificar los accesos no utilizados que se han concedido a sus AWS organizaciones y cuentas, como los siguientes:

- Funciones de IAM no utilizadas: funciones que no tienen actividad de acceso dentro del período de uso especificado.

- Usuarios, credenciales y claves de acceso de IAM no utilizados: credenciales que pertenecen a los usuarios de IAM y se utilizan para acceder Servicios de AWS a los recursos.
- Políticas y permisos de IAM no utilizados: permisos de nivel de servicio y de acción que un rol no utilizó dentro de un período de uso específico. IAM Access Analyzer utiliza políticas basadas en la identidad que se adjuntan a las funciones para determinar los servicios y las acciones a los que pueden acceder esas funciones. El analizador proporciona una revisión de los permisos no utilizados para todos los permisos de nivel de servicio.

Puede utilizar las conclusiones generadas por IAM Access Analyzer para obtener visibilidad y corregir cualquier acceso no deseado o no utilizado en función de las políticas y los estándares de seguridad de su organización. Tras la corrección, estos resultados se marcarán como resueltos la próxima vez que se ejecute el analizador. Si el hallazgo es intencional, puede marcarlo como archivado en IAM Access Analyzer y priorizar otros hallazgos que supongan un mayor riesgo de seguridad. Además, puede configurar reglas de archivado para archivar automáticamente los hallazgos específicos. Por ejemplo, puede crear una regla de archivado para archivar automáticamente los resultados de un bucket de Amazon S3 específico al que conceda acceso de forma periódica.

Como creador, puede utilizar IAM Access Analyzer para realizar comprobaciones automatizadas de las políticas de IAM en una fase temprana del proceso de desarrollo e implementación (CI/CD), a fin de cumplir con los estándares de seguridad corporativos. Puede integrar las comprobaciones y revisiones de políticas personalizadas de IAM Access Analyzer AWS CloudFormation para automatizar las revisiones de políticas como parte de los procesos de su equipo de desarrollo. CI/CD Esto incluye:

- Validación de políticas de IAM: IAM Access Analyzer valida sus políticas según la gramática de las políticas de IAM y las mejores prácticas. AWS Puede ver los resultados de las comprobaciones de validación de políticas, incluidas las advertencias de seguridad, los errores, las advertencias generales y las sugerencias para su política. Actualmente hay más de 100 comprobaciones de validación de políticas disponibles y se pueden automatizar mediante AWS Command Line Interface (AWS CLI) y APIs.
- Comprobaciones de políticas personalizadas de IAM: las comprobaciones de políticas personalizadas de IAM Access Analyzer validan sus políticas según los estándares de seguridad especificados. Las comprobaciones de políticas personalizadas utilizan un razonamiento automatizado para ofrecer un mayor nivel de seguridad en cuanto al cumplimiento de los

estándares de seguridad corporativos. Los tipos de comprobaciones de políticas personalizadas incluyen:

- Compare con una política de referencia: al editar una política, puede compararla con una política de referencia, como una versión existente de la política, para comprobar si la actualización concede un nuevo acceso. La CheckNoNewAccessAPI compara dos políticas (una política actualizada y una política de referencia) para determinar si la política actualizada introduce un nuevo acceso con respecto a la política de referencia y devuelve una respuesta de aprobación o rechazo.
- Compruébalo con una lista de acciones de IAM: puedes usar la CheckAccessNotGrantedAPI para asegurarte de que una política no dé acceso a una lista de acciones críticas definidas en tu estándar de seguridad. Esta API toma una política y una lista de hasta 100 acciones de IAM para comprobar si la política permite al menos una de las acciones, y devuelve una respuesta de aprobación o rechazo.

Los equipos de seguridad y otros autores de políticas de IAM pueden utilizar IAM Access Analyzer para crear políticas que cumplan con los estándares gramaticales y de seguridad de las políticas de IAM. La creación manual de políticas del tamaño correcto puede ser propensa a errores y llevar mucho tiempo. La función de generación de políticas de IAM Access Analyzer ayuda a crear políticas de IAM que se basan en la actividad de acceso del director. IAM Access Analyzer revisa AWS CloudTrail los registros de los servicios compatibles y genera una plantilla de políticas que contiene los permisos que utilizó el director en el intervalo de fechas especificado. A continuación, puede utilizar esta plantilla para crear una política con permisos detallados que conceda solo los permisos necesarios.

- Debe tener una CloudTrail ruta habilitada en su cuenta para poder generar una política basada en la actividad de acceso.
- IAM Access Analyzer no identifica la actividad a nivel de acción de los eventos de datos, como los eventos de datos de Amazon S3, en las políticas generadas.
- Las `iam:PassRole` políticas generadas no rastrean la CloudTrail acción ni la incluyen.

El analizador de acceso de IAM se implementa en la cuenta de Security Tooling a través de la funcionalidad de administrador delegado de. AWS Organizations El administrador delegado tiene permisos para crear y gestionar analizadores con la AWS organización como zona de confianza.

Consideración del diseño

Para obtener resultados relacionados con la cuenta (donde la cuenta sirve como límite de confianza), debe crear un analizador con el ámbito de la cuenta en cada cuenta de un miembro. Esto se puede hacer como parte de la canalización de cuentas. Los hallazgos relacionados con la cuenta llegan al CSPM de Security Hub a nivel de cuenta de miembro. Desde allí, fluyen a la cuenta de administrador delegado CSPM de Security Hub (Security Tooling).

Ejemplos de implementación

- La biblioteca de códigos AWS SRA proporciona un ejemplo de implementación de IAM Access Analyzer. Muestra cómo configurar un analizador a nivel de organización dentro de una cuenta de administrador delegado y un analizador a nivel de cuenta dentro de cada cuenta.
- Para obtener información sobre cómo integrar las comprobaciones de políticas personalizadas en los flujos de trabajo de los creadores, consulte la entrada del AWS blog Introducción a las comprobaciones de políticas personalizadas de IAM Access Analyzer.

AWS Firewall Manager

AWS Firewall Managerayuda a proteger su red al simplificar las tareas de administración y mantenimiento de los AWS WAF grupos AWS Network Firewall de seguridad de Amazon VPC y el firewall de DNS en varias cuentas Amazon Route 53 Resolver y recursos. AWS Shield Advanced Con Firewall Manager, solo puede configurar las reglas de AWS WAF firewall, las protecciones de Shield Advanced, los grupos de seguridad de Amazon VPC, los firewalls de Network Firewall y las asociaciones de grupos de reglas de DNS Firewall una sola vez. El servicio aplica automáticamente las reglas y las protecciones en todas las cuentas y recursos, incluso cuando se agregan recursos nuevos.

Firewall Manager es especialmente útil cuando desea proteger toda su AWS organización en lugar de un número reducido de cuentas y recursos específicos, o si agrega con frecuencia nuevos recursos que desea proteger. Firewall Manager utiliza políticas de seguridad para permitirle definir un conjunto de configuraciones, incluidas las reglas, protecciones y acciones relevantes que se deben

implementar y las cuentas y los recursos (indicados mediante etiquetas) que se deben incluir o excluir. Puede crear configuraciones granulares y flexibles y, al mismo tiempo, ampliar el control a un gran número de cuentas y VPCs. Estas políticas hacen cumplir de forma automática y coherente las reglas que usted configura, incluso cuando se crean nuevas cuentas y recursos. El Firewall Manager está habilitado en todas las cuentas AWS Organizations y la configuración y la administración las realizan los equipos de seguridad correspondientes en la cuenta de administrador delegado de Firewall Manager (en este caso, la cuenta Security Tooling).

Debe habilitar cada una AWS Config de las Región de AWS que contengan los recursos que desee proteger. Si no desea habilitarla AWS Config para todos los recursos, debe habilitarla para los recursos que estén asociados al tipo de políticas de Firewall Manager que utilice. Si utiliza ambos AWS Security Hub CSPM y Firewall Manager, Firewall Manager envía automáticamente los resultados al Security Hub CSPM. Firewall Manager detecta los recursos que no cumplen con las normas y los ataques que detecta, y los envía a Security Hub (CSPM). Al configurar una política de Firewall Manager para AWS WAF, puede habilitar de forma centralizada el registro en las listas de control de acceso web (web ACLs) para todas las cuentas incluidas en el ámbito y centralizar los registros en una sola cuenta.

Con Firewall Manager, puede tener uno o varios administradores que pueden administrar los recursos de firewall de su organización. Al asignar varios administradores, puede aplicar condiciones de ámbito administrativo restrictivas para definir los recursos (cuentas OUs, regiones, tipos de políticas) que cada administrador puede administrar. Esto le da la flexibilidad de tener diferentes funciones de administrador en su organización y le ayuda a mantener el principio de acceso con privilegio mínimo. La AWS SRA utiliza un administrador con todo el alcance administrativo delegado en la cuenta Security Tooling.

Consideración del diseño

Los administradores de cuentas de los miembros individuales de la AWS organización pueden configurar controles adicionales (como AWS WAF reglas y grupos de seguridad de Amazon VPC) en los servicios gestionados por Firewall Manager según sus necesidades particulares.

Ejemplo de implementación

La biblioteca de códigos AWS SRA proporciona un ejemplo de implementación de Firewall Manager. Muestra la administración delegada (herramientas de seguridad), implementa

un grupo de seguridad máximo permitido, configura una política de grupo de seguridad y configura varias políticas. AWS WAF

Amazon EventBridge

Amazon EventBridge es un servicio de bus de eventos sin servidor que facilita la conexión de sus aplicaciones con datos de diversas fuentes. Se utiliza con frecuencia en la automatización de la seguridad. Puede configurar reglas de enrutamiento para determinar dónde enviar sus datos para crear arquitecturas de aplicaciones que reaccionen en tiempo real a todas sus fuentes de datos. Puede crear un bus de eventos personalizado para recibir eventos de sus aplicaciones personalizadas, además de utilizar el bus de eventos predeterminado en cada cuenta. Puede crear un bus de eventos en la cuenta de Security Tooling que pueda recibir eventos específicos de seguridad de otras cuentas de la organización. AWS Por ejemplo, al vincular Reglas de AWS Config Amazon y AWS Security Hub CSPM con GuardDuty EventBridge, se crea una canalización flexible y automatizada para enrutar los datos de seguridad, generar alertas y gestionar las acciones para resolver los problemas.

Consideraciones sobre el diseño

- EventBridge es capaz de enrutar eventos a varios objetivos diferentes. Un patrón valioso para automatizar las acciones de seguridad consiste en conectar determinados eventos con los equipos de AWS Lambda respuesta individuales, que toman las medidas adecuadas. Por ejemplo, en determinadas circunstancias, es posible que desee EventBridge enrutar la búsqueda de un bucket público de S3 a un respondedor Lambda que corrija la política del bucket y elimine los permisos públicos. Estos socorristas se pueden integrar en sus guías y manuales de investigación para coordinar las actividades de respuesta.
- Una buena práctica para que un equipo de operaciones de seguridad tenga éxito es integrar el flujo de eventos y hallazgos de seguridad en un sistema de notificación y flujo de trabajo, como un sistema de venta de entradas, un sistema u otro bug/issue sistema de información de seguridad y gestión de eventos (SIEM). Esto elimina el flujo de trabajo del correo electrónico y los informes estáticos, y le ayuda a enrutar, escalar y gestionar los eventos o hallazgos. Las capacidades de enrutamiento flexibles EventBridge que ofrece son un poderoso facilitador de esta integración.

Amazon Detective

Amazon Detective apoya su estrategia de control de seguridad responsivo al facilitar el análisis, la investigación y la rápida identificación de la causa raíz de los hallazgos de seguridad o las actividades sospechosas para sus analistas de seguridad. Detective extrae automáticamente los eventos en función del tiempo, como los intentos de inicio de sesión, las llamadas a la API y el tráfico de red, de AWS CloudTrail los registros y los registros de flujo de Amazon VPC. Detective consume estos eventos mediante flujos de CloudTrail registros independientes y registros de flujo de Amazon VPC. Puede usar Detective para acceder a datos de eventos históricos de hasta un año. Detective utiliza el aprendizaje automático y la visualización para crear una vista unificada e interactiva del comportamiento de sus recursos y las interacciones entre ellos a lo largo del tiempo, lo que se denomina gráfico de comportamiento. Puede explorar el gráfico de comportamiento para examinar acciones dispares, como los intentos fallidos de inicio de sesión o las llamadas sospechosas a la API.

Detective se integra con Amazon Security Lake para permitir a los analistas de seguridad consultar y recuperar los registros almacenados en Security Lake. Puede utilizar esta integración para obtener información adicional de CloudTrail los registros y los registros de flujo de Amazon VPC que se almacenan en Security Lake mientras realiza investigaciones de seguridad en Detective.

Detective también analiza los hallazgos detectados por Amazon GuardDuty, incluidas las amenazas detectadas por GuardDuty Runtime Monitoring. Cuando una cuenta habilita Detective, se convierte en la cuenta de administrador del gráfico de comportamiento. Antes de intentar activar Detective, asegúrate de que tu cuenta ha estado inscrita GuardDuty durante al menos 48 horas. Si no cumples este requisito, no podrás activarla DetectiveDetective.

Las fuentes de datos opcionales adicionales para Detective incluyen los registros de auditoría de Amazon EKS y AWS Security Hub CSPM. La fuente de datos del registro de auditoría de Amazon EKS mejora la información proporcionada sobre los siguientes tipos de entidades: clústeres de Amazon EKS, pods de Kubernetes, imágenes de contenedores y asuntos de Kubernetes. La fuente de datos del Security Hub forma parte de los hallazgos de AWS seguridad, donde correlaciona los hallazgos de los productos en Security Hub y los incorpora a Detective.

Detective agrupa automáticamente varios hallazgos relacionados con un único evento de compromiso de seguridad en grupos de búsqueda. Los actores de las amenazas suelen realizar una secuencia de acciones que conducen a múltiples hallazgos de seguridad repartidos en el tiempo y los recursos. Por lo tanto, encontrar grupos debe ser el punto de partida para las investigaciones que involucren múltiples entidades y hallazgos. Detective también proporciona resúmenes de grupos de

búsqueda mediante el uso de IA generativa que analiza automáticamente la búsqueda de grupos y proporciona información en lenguaje natural para ayudarlo a acelerar las investigaciones de seguridad.

Detective se integra con AWS Organizations. La cuenta de administración de la organización delega una cuenta de miembro como cuenta de administrador de Detective. En la AWS SRA, se trata de la cuenta Security Tooling. La cuenta de administrador de Detective tiene la capacidad de habilitar automáticamente todas las cuentas de los miembros actuales de la organización como cuentas de miembros de Detective y también agregar nuevas cuentas de miembros a medida que se agregan a la AWS organización. Las cuentas de los administradores de Detectives también tienen la capacidad de invitar a las cuentas de miembros que actualmente no residen en la AWS organización, pero que se encuentran dentro de la misma región, a contribuir con sus datos al gráfico de comportamiento de la cuenta principal. Cuando una cuenta de miembro acepta la invitación y está habilitada, Detective comienza a ingerir y extraer los datos de la cuenta de miembro en ese gráfico de comportamiento.

> **Consideración del diseño**
>
> Puede navegar hasta Detective buscando perfiles desde las AWS Security Hub CSPM consolas GuardDuty y. Estos enlaces pueden ayudar a agilizar el proceso de investigación. Tu cuenta debe ser la cuenta administrativa tanto de Detective como del servicio desde el que estás cambiando (GuardDutyo Security Hub CSPM). Si las cuentas principales son las mismas para los servicios, los enlaces de integración funcionan sin problemas.

AWS Audit Manager

AWS Audit Managerle ayuda a auditar continuamente su AWS uso para simplificar la gestión de las auditorías y el cumplimiento de las normativas y los estándares del sector. Le permite pasar de la recopilación, revisión y gestión manual de las pruebas a una solución que automatiza la recopilación de pruebas, proporciona una forma sencilla de rastrear la fuente de las pruebas de auditoría, permite la colaboración en equipo y ayuda a gestionar la seguridad e integridad de las pruebas. Llegado el momento de una auditoría, Audit Manager le ayuda a gestionar las revisiones de sus controles por parte de las personas interesadas.

Con Audit Manager, puede realizar auditorías con marcos prediseñados, como el punto de referencia Center for Internet Security (CIS), el CIS AWS Foundations Benchmark, System and Organization Controls 2 (SOC 2) y el Estándar de seguridad de datos de la industria de tarjetas de pago (PCI

DSS). También le permite crear sus propios marcos con controles estándar o personalizados en función de sus requisitos específicos de auditoría interna.

Audit Manager recopila cuatro tipos de pruebas. Se automatizan tres tipos de pruebas: las pruebas de control de conformidad procedentes de las llamadas a la AWS service-to-service API AWS Config y procedentes de ellas AWS Security Hub CSPM, las pruebas de AWS CloudTrail los eventos de gestión y las pruebas de configuración procedentes de ellas. Para las pruebas que no se pueden automatizar, Audit Manager le permite cargar pruebas manuales.

De forma predeterminada, los datos de Audit Manager se cifran mediante claves AWS gestionadas. La AWS SRA utiliza una clave administrada por el cliente para el cifrado a fin de proporcionar un mayor control sobre el acceso lógico. También debe configurar un bucket de S3 en el Región de AWS que Audit Manager publique el informe de evaluación. Estos depósitos deben estar cifrados con una clave gestionada por el cliente y tener una política de depósitos configurada para permitir que solo Audit Manager publique informes.

> **Note**
>
> Audit Manager ayuda a recopilar pruebas relevantes para verificar el cumplimiento de normas y reglamentos de cumplimiento específicos. Sin embargo, no evalúa su cumplimiento. Por lo tanto, es posible que las pruebas recopiladas a través de Audit Manager no incluyan detalles de los procesos operativos necesarios para las auditorías. Audit Manager no sustituye a los asesores legales ni a los expertos en cumplimiento. Le recomendamos que contrate los servicios de un evaluador externo que esté certificado para cumplir con los marcos de cumplimiento con los que se lo evalúa.

Las evaluaciones de Audit Manager pueden ejecutarse en varias cuentas de sus AWS organizaciones. Audit Manager recopila y consolida las pruebas en una cuenta de administrador delegado en. AWS Organizations Esta funcionalidad de auditoría la utilizan principalmente los equipos de cumplimiento y auditoría interna, y solo requiere acceso de lectura a la suya. Cuentas de AWS

> **Consideraciones sobre el diseño**
>
> - Audit Manager complementa otros servicios de AWS seguridad AWS Security Hub CSPM, como AWS Security Hub, y ayuda AWS Config a implementar un marco de gestión de

riesgos. Audit Manager proporciona una funcionalidad de control de riesgos independiente, mientras que Security Hub CSPM le ayuda a supervisar sus riesgos y los paquetes de AWS Config conformidad ayudan a gestionar sus riesgos. Los profesionales de auditoría que estén familiarizados con el modelo de tres líneas desarrollado por el Instituto de Auditores Internos (IIA) deben tener en cuenta que esta combinación Servicios de AWS ayuda a cubrir las tres líneas de defensa. Para obtener más información, consulte la serie de blogs de dos partes en el blog Nube de AWS Operaciones y migraciones.

- Para que Audit Manager recopile las pruebas de CSPM de Security Hub, la cuenta de administrador delegado de ambos servicios debe ser la misma. Cuenta de AWS Por este motivo, en la AWS SRA, la cuenta Security Tooling es el administrador delegado de Audit Manager.

AWS Artifact

AWS Artifactestá alojada en la cuenta Security Tooling para separar la funcionalidad de gestión de artefactos de conformidad de la cuenta de gestión de la organización. AWS Esta separación de funciones es importante porque le recomendamos que evite utilizar la cuenta de administración de la AWS organización para las implementaciones, a menos que sea absolutamente necesario. En su lugar, transfiera las implementaciones a las cuentas de los miembros. Como la administración de artefactos de auditoría se puede realizar desde la cuenta de un miembro y la función se alinea estrechamente con el equipo de seguridad y cumplimiento, la cuenta Security Tooling se designa como la cuenta de administrador de. AWS Artifact Puede utilizar AWS Artifact los informes para descargar documentos de AWS seguridad y conformidad, como las certificaciones AWS ISO, los informes del sector de las tarjetas de pago (PCI) y de los controles de sistemas y organizaciones (SOC).

AWS Artifact no es compatible con la función de administración delegada. En su lugar, puede restringir esta capacidad a solo las funciones de IAM de la cuenta de Security Tooling que pertenezcan a sus equipos de auditoría y cumplimiento, de modo que puedan descargar, revisar y proporcionar esos informes a los auditores externos según sea necesario. Además, puede restringir funciones específicas de IAM para tener acceso únicamente a AWS Artifact informes específicos mediante las políticas de IAM. Para ver ejemplos de políticas de IAM, consulta la documentación.AWS Artifact

> **Consideración del diseño**
>
> Si opta Cuenta de AWS por tener una cuenta dedicada a los equipos de auditoría y cumplimiento, puede alojarla AWS Artifact en una cuenta de auditoría de seguridad, que es independiente de la cuenta de herramientas de seguridad. AWS Artifact los informes proporcionan pruebas que demuestran que una organización sigue un proceso documentado o cumple un requisito específico. Los artefactos de auditoría se recopilan y archivan a lo largo del ciclo de vida de desarrollo del sistema y se pueden utilizar como evidencia en auditorías y evaluaciones internas o externas.

AWS KMS

AWS Key Management Service(AWS KMS) le ayuda a crear y administrar claves criptográficas y a controlar su uso en una amplia gama de aplicaciones Servicios de AWS y dentro de ellas. AWS KMS es un servicio seguro y resistente que utiliza módulos de seguridad de hardware para proteger las claves criptográficas. Sigue los procesos de ciclo de vida estándar del sector para el material clave, como el almacenamiento, la rotación y el control de acceso a las claves. AWS KMS puede ayudar a proteger sus datos con claves de cifrado y firma, y se puede utilizar tanto para el cifrado del lado del servidor como para el cifrado del lado del cliente mediante el SDK de cifrado.AWS Para mayor protección y flexibilidad, AWS KMS admite tres tipos de claves: claves administradas por el cliente, claves AWS administradas y claves propias. AWS Las claves administradas por el cliente son AWS KMS claves Cuenta de AWS que usted crea, posee y administra. AWS las claves gestionadas son AWS KMS claves de tu cuenta que se crean, gestionan Servicio de AWS y utilizan en tu nombre y están integradas en ella AWS KMS. AWS las claves propias son un conjunto de AWS KMS claves que una persona Servicio de AWS posee y administra para utilizarlas en múltiples ocasiones Cuentas de AWS. Para obtener más información sobre el uso de AWS KMS claves, consulte la AWS KMS documentación y los detalles AWS KMS criptográficos.

Una opción de implementación consiste en centralizar la responsabilidad de la administración de AWS KMS claves en una sola cuenta y, al mismo tiempo, delegar la capacidad de usar las claves de la cuenta de la aplicación por parte de los recursos de la aplicación mediante una combinación de políticas clave y de IAM. Este enfoque es seguro y sencillo de administrar, pero puede encontrar obstáculos debido a la AWS KMS limitación de los límites, a los límites de servicio de las cuentas y a la sobrecarga de tareas operativas del equipo de seguridad por parte del equipo de seguridad. Otra opción de implementación es tener un modelo descentralizado en el que se permita AWS KMS residir en varias cuentas y permitir que los responsables de la infraestructura y las cargas de

trabajo de una cuenta específica administren sus propias claves. Este modelo proporciona a sus equipos de carga de trabajo un mayor control, flexibilidad y agilidad a la hora de utilizar las claves de cifrado. También ayuda a evitar los límites de las API, limita el alcance del impacto a uno Cuenta de AWS solo y simplifica la elaboración de informes, la auditoría y otras tareas relacionadas con el cumplimiento. En un modelo descentralizado, es importante implementar y reforzar las barreras de seguridad para que las claves descentralizadas se administren de la misma manera y el uso de las AWS KMS claves se audite de acuerdo con las mejores prácticas y políticas establecidas. Para obtener más información, consulte el documento técnico AWS Key Management Service Mejores prácticas. AWS La SRA recomienda un modelo de administración de claves distribuidas en el que las AWS KMS claves residan localmente en la cuenta en la que se utilizan. Le recomendamos que evite usar una sola clave en una cuenta para todas las funciones criptográficas. Las claves se pueden crear en función de los requisitos de función y protección de datos, y para hacer cumplir el principio del privilegio mínimo. En algunos casos, los permisos de cifrado se mantendrían separados de los permisos de descifrado y los administradores gestionarían las funciones del ciclo de vida, pero no podrían cifrar ni descifrar los datos con las claves que administran.

En la cuenta Security Tooling, AWS KMS se utiliza para gestionar el cifrado de los servicios de seguridad centralizados, como el registro organizativo gestionado por la AWS CloudTrail organización. AWS

AWS Private CA

AWS Private Certificate Authority(AWS Private CA) es un servicio de CA privado gestionado que le ayuda a gestionar de forma segura el ciclo de vida de sus certificados TLS de entidades finales privadas para instancias EC2, contenedores, dispositivos IoT y recursos locales. Permite las comunicaciones TLS cifradas con las aplicaciones en ejecución. Con él AWS Private CA, puede crear su propia jerarquía de entidades de certificación (desde una CA raíz, hasta una subordinada CAs, hasta los certificados de la entidad final) y emitir certificados con ella para autenticar a los usuarios internos, los ordenadores, las aplicaciones, los servicios, los servidores y otros dispositivos, así como para firmar el código de la computadora. Los certificados emitidos por una entidad emisora de certificados privada solo son de confianza en su AWS organización, no en Internet.

Una infraestructura de clave pública (PKI) o un equipo de seguridad pueden ser responsables de administrar toda la infraestructura de la PKI. Esto incluye la administración y la creación de la CA privada. Sin embargo, debe haber una disposición que permita a los equipos de carga de trabajo cumplir por sí mismos sus requisitos de certificación. La AWS SRA describe una jerarquía de CA centralizada en la que la CA raíz se aloja en la cuenta de Security Tooling. Esto permite a los equipos de seguridad aplicar controles de seguridad estrictos, ya que la CA raíz es la base de

toda la PKI. Sin embargo, la creación de certificados privados desde la CA privada se delega en los equipos de desarrollo de aplicaciones, que comparten la CA con una cuenta de aplicación mediante AWS Resource Access Manager ()AWS RAM. AWS RAM administra los permisos necesarios para compartir entre cuentas. Esto elimina la necesidad de una CA privada en cada cuenta y proporciona una forma de implementación más rentable. Para obtener más información sobre el flujo de trabajo y la implementación, consulte la entrada del blog Cómo usar AWS RAM para compartir AWS Private CA cuentas múltiples.

Note

AWS Certificate Manager (ACM) también le ayuda a aprovisionar, administrar e implementar certificados TLS públicos para usarlos con ellos. Servicios de AWS Para admitir esta funcionalidad, el ACM debe residir en el lugar donde Cuenta de AWS se utilizará el certificado público. Esto se explica más adelante en esta guía, en la sección Cuenta de la aplicación.

Consideraciones sobre el diseño

- Con AWS Private CA ella, puede crear una jerarquía de autoridades de certificación de hasta cinco niveles. También puede crear varias jerarquías, cada una con su propia raíz. La AWS Private CA jerarquía debe ajustarse al diseño de la PKI de su organización. Sin embargo, tenga en cuenta que al aumentar la jerarquía de las entidades emisoras de certificados aumentará el número de certificados en la ruta de certificación, lo que, a su vez, aumentará el tiempo de validación de un certificado de la entidad final. Una jerarquía de CA bien definida ofrece beneficios que incluyen un control de seguridad granular adecuado para cada CA, la delegación de la CA subordinada a una aplicación diferente, lo que lleva a la división de las tareas administrativas, el uso de una CA con una confianza revocable limitada, la capacidad de definir diferentes períodos de validez y la capacidad de hacer cumplir los límites de las rutas. Lo ideal es que la raíz y la subordinada estén separadas. CAs Cuentas de AWS Para obtener más información sobre cómo planificar una jerarquía de CA mediante el uso AWS Private CA, consulte la AWS Private CA documentación y la entrada del blog Cómo proteger una AWS Private CA jerarquía a escala empresarial para la automoción y la fabricación.
- AWS Private CA se puede integrar con su jerarquía de CA existente, lo que le permite utilizar la capacidad de automatización e AWS integración nativa de ACM junto con la

base de confianza existente que utiliza en la actualidad. Puede crear una CA subordinada AWS Private CA respaldada por una CA principal en las instalaciones. Para obtener más información sobre la implementación, consulte Instalación de un certificado de CA subordinada firmado por una CA principal externa en la AWS Private CA documentación.

Amazon Inspector

Amazon Inspector es un servicio automatizado de gestión de vulnerabilidades que descubre y escanea automáticamente las instancias de Amazon EC2, las imágenes de contenedores del Amazon Elastic Container Registry (Amazon ECR) AWS Lambda , las funciones y los repositorios de código de sus administradores de código fuente para detectar vulnerabilidades de software conocidas y exposiciones no intencionadas en la red.

Amazon Inspector evalúa continuamente su entorno a lo largo del ciclo de vida de sus recursos, escaneando automáticamente los recursos cada vez que los modifica. Los eventos que inician la redigitalización de un recurso incluyen la instalación de un nuevo paquete en una instancia de EC2, la instalación de un parche y la publicación de un nuevo informe sobre vulnerabilidades y exposiciones comunes (CVE) que afecta al recurso. Amazon Inspector admite las evaluaciones comparativas del Centro de Seguridad de Internet (CIS) para sistemas operativos en instancias EC2.

Amazon Inspector se integra con herramientas para desarrolladores, como Jenkins, y TeamCity para la evaluación de imágenes de contenedores. Puede evaluar las imágenes de sus contenedores para detectar vulnerabilidades de software en el panel de control de la CI/CD) tools, and push security to an earlier point in the software development lifecycle. Assessment findings are available in the CI/CD herramienta de integración continua y entrega continua, de forma que pueda realizar acciones automatizadas en respuesta a problemas de seguridad críticos, como el bloqueo de compilaciones o el envío de imágenes a los registros de contenedores. Si tienes uno activo Cuenta de AWS, puedes instalar el complemento Amazon Inspector desde tu tienda de CI/CD herramientas y añadir un escaneo de Amazon Inspector a tu proceso de creación sin necesidad de activar el servicio Amazon Inspector. Esta función funciona con CI/CD herramientas alojadas en cualquier lugar (de forma local AWS, local o en nubes híbridas), por lo que puedes usar una única solución de forma uniforme en todos tus procesos de desarrollo. Cuando Amazon Inspector está activado, descubre automáticamente todas las instancias de EC2, las imágenes de contenedores en Amazon ECR y CI/CD las herramientas y las funciones de Lambda a escala, y las monitorea continuamente para detectar vulnerabilidades conocidas.

Los resultados de accesibilidad de la red de Amazon Inspector evalúan la accesibilidad de sus instancias EC2 hacia o desde los bordes de la VPC, como las puertas de enlace de Internet, las conexiones de emparejamiento de VPC o las redes privadas virtuales () a través de una puerta de enlace virtual. VPNs Estas reglas ayudan a automatizar la supervisión de sus AWS redes e identificar dónde puede estar mal configurado el acceso de red a sus instancias de EC2 debido a la mala administración de los grupos de seguridad, las listas de control de acceso (), las pasarelas de Internet, etc. ACLs Para obtener más información, consulta la documentación de Amazon Inspector.

Cuando Amazon Inspector identifica vulnerabilidades o rutas de red abiertas, produce una conclusión que usted puede investigar. El hallazgo incluye detalles exhaustivos sobre la vulnerabilidad, incluida una puntuación de riesgo, el recurso afectado y recomendaciones de remediación. La puntuación de riesgo se adapta específicamente a su entorno y se calcula correlacionando la información de la up-to-date CVE con factores temporales y ambientales, como la información sobre la accesibilidad y la explotabilidad de la red, a fin de proporcionar una conclusión contextual.

Amazon Inspector Code Security analiza el código fuente de las aplicaciones propias, las dependencias de las aplicaciones de terceros y la infraestructura como código (IaC) en busca de vulnerabilidades. Después de activar Code Security, puede crear y aplicar una configuración de escaneo a su repositorio de código para determinar la frecuencia, el tipo de escaneo y los repositorios que se escanearán. Code Security admite las pruebas estáticas de seguridad de las aplicaciones (SAST), el análisis de la composición del software (SCA) y el escaneo de iAC. Para configurar la frecuencia, puede definir los escaneos a pedido, al cambiar el código o de forma periódica. El análisis de código captura fragmentos de código para resaltar las vulnerabilidades detectadas. Los fragmentos de código se almacenan cifrados con claves KMS. El administrador delegado de una organización no puede ver los fragmentos de código que pertenecen a las cuentas de miembros. Tras integrar los gestores de código fuente (SCMs) con Code Security, todos los repositorios de código se muestran como proyectos en la consola de Amazon Inspector. Code Security supervisa solo la rama predeterminada de cada repositorio. Amazon Inspector optimiza las soluciones de seguridad al proporcionar recomendaciones específicas de corrección de código directamente donde trabajan los desarrolladores. La integración bidireccional con su SCM sugiere automáticamente correcciones en forma de comentarios en las solicitudes de extracción (PRs) y en las solicitudes de fusión (MRs) en caso de hallazgos importantes o importantes, y alerta a los desarrolladores sobre las vulnerabilidades más importantes que deben abordar sin interrumpir su flujo de trabajo.

Para detectar vulnerabilidades, las instancias EC2 deben administrarse AWS Systems Manager mediante un AWS Systems Manager agente (SSMAgent). No se requieren agentes para que las

instancias EC2 puedan acceder a la red ni para escanear las vulnerabilidades de las imágenes de contenedores en las funciones de Amazon ECR o Lambda.

Amazon Inspector está integrado con la administración delegada AWS Organizations y es compatible con ella. En la AWS SRA, la cuenta Security Tooling se convierte en la cuenta de administrador delegado de Amazon Inspector. La cuenta de administrador delegado de Amazon Inspector puede gestionar los datos de los hallazgos y determinados ajustes de los miembros de la AWS organización. Esto incluye ver los detalles de los resultados agregados de todas las cuentas de los miembros, habilitar o deshabilitar los escaneos de las cuentas de los miembros y revisar los recursos escaneados dentro de la AWS organización.

Consideraciones sobre el diseño

- Amazon Inspector se integra automáticamente con AWS Security Hub CSPM el Security Hub cuando ambos servicios están habilitados. Puedes usar esta integración para enviar todas las conclusiones de Amazon Inspector a Security Hub (CSPM), que luego las incluirá en su análisis de tu postura de seguridad.
- Amazon Inspector exporta automáticamente los eventos en busca de hallazgos, cambios en la cobertura de recursos y escaneos iniciales de recursos individuales a Amazon y EventBridge, opcionalmente, a un depósito de Amazon Simple Storage Service (Amazon S3). Para exportar los hallazgos activos a un bucket de S3, necesita una AWS KMS clave que Amazon Inspector pueda utilizar para cifrar los hallazgos y un bucket de S3 con permisos que permitan a Amazon Inspector cargar objetos. EventBridgela integración le permite monitorear y procesar los hallazgos casi en tiempo real como parte de sus flujos de trabajo actuales de seguridad y cumplimiento. EventBridge los eventos se publican en la cuenta de administrador delegado de Amazon Inspector además de en la cuenta de miembro en la que se originaron.
- Las integraciones de Amazon Inspector Code Security con GitHub SaaS GitHub , Enterprise Cloud GitHub y Enterprise Server requieren acceso público a Internet.

Ejemplo de implementación

La biblioteca de códigos AWS SRA proporciona un ejemplo de implementación de Amazon Inspector. Demuestra la administración delegada (herramientas de seguridad) y configura Amazon Inspector para todas las cuentas existentes y futuras de la organización. AWS

Respuesta frente a incidencias de seguridad de AWS

Respuesta frente a incidencias de seguridad de AWSes un servicio que le ayuda a prepararse para los incidentes de seguridad de su entorno y a responder a ellos. AWS Clasifica las conclusiones, intensifica los eventos de seguridad y gestiona los casos que requieren su atención inmediata. Además, le da acceso al equipo de respuesta a incidentes del AWS cliente (CIRT), que investiga los recursos afectados. Respuesta frente a incidencias de seguridad de AWS también proporciona capacidades automatizadas de respuesta y reparación mediante AWS Systems Manager documentos (documentos SSM), que ayudan a los equipos de seguridad a responder a los incidentes de seguridad y a recuperarse de ellos de manera más eficiente. Respuesta frente a incidencias de seguridad de AWS se integra con Amazon GuardDuty y AWS Security Hub CSPM para recibir hallazgos de seguridad y organizar respuestas automatizadas.

En la AWS SRA, Respuesta frente a incidencias de seguridad de AWS se implementa en la cuenta de Security Tooling como una cuenta de administrador delegado. Se selecciona la cuenta Security Tooling porque se ajusta al propósito de la cuenta de operar los servicios de seguridad y automatizar las alertas y respuestas de seguridad. La cuenta Security Tooling también actúa como cuenta de administrador delegado para Security Hub CSPM y GuardDuty, además Respuesta frente a incidencias de seguridad de AWS, ayuda a simplificar la administración del flujo de trabajo. Respuesta frente a incidencias de seguridad de AWS está configurada para funcionar con ella AWS Organizations, de forma que pueda gestionar las respuestas a los incidentes en todas las cuentas de su organización desde la cuenta Security Tooling.

Respuesta frente a incidencias de seguridad de AWS le ayuda a implementar las siguientes fases del ciclo de vida de la respuesta a los incidentes:

- Preparación: cree y mantenga planes de respuesta y documentos SSM para las acciones de contención.
- Detección y análisis: analice automáticamente los hallazgos de seguridad y determine la gravedad de los incidentes.
- Detección y análisis: abra un caso respaldado por el servicio y póngase en contacto con el AWS CIRT para obtener asistencia adicional. El CIRT es un grupo de personas que brindan apoyo durante los eventos de seguridad activa.
- Contención y erradicación: ejecute acciones de contención automatizadas a través de documentos SSM.
- Actividad posterior al incidente: documente los detalles del incidente y lleve a cabo un análisis posterior al incidente.

También se puede utilizar Respuesta frente a incidencias de seguridad de AWS para crear casos autogestionados. Respuesta frente a incidencias de seguridad de AWS puedes crear una notificación o un caso saliente cuando necesites estar al tanto de algo que pueda afectar a tu cuenta o a tus recursos o tomar alguna medida al respecto. Esta función solo está disponible cuando habilitas los flujos de trabajo de respuesta proactiva y clasificación de alertas como parte de tu suscripción.

Consideraciones sobre el diseño

- Cuando las Respuesta frente a incidencias de seguridad de AWS implementes, revisa y prueba detenidamente las acciones de respuesta automatizadas antes de activarlas en producción. La automatización puede acelerar la respuesta a los incidentes, pero las acciones automatizadas mal configuradas podrían afectar a las cargas de trabajo legítimas.
- Considere la posibilidad de utilizar los documentos SSM Respuesta frente a incidencias de seguridad de AWS para implementar procedimientos de contención específicos de la organización y, al mismo tiempo, mantener las mejores prácticas integradas en el servicio para los tipos de incidentes más comunes.
- Si planea usarlo Respuesta frente a incidencias de seguridad de AWS en una VPC, asegúrese de tener los puntos finales de VPC adecuados configurados para Systems Manager y otros servicios integrados a fin de habilitar las acciones de contención en las subredes privadas.

Implementación de servicios de seguridad comunes en todas Cuentas de AWS

En la sección Aplicar servicios de seguridad en toda AWS la organización, que aparece anteriormente en esta referencia Cuenta de AWS, se destacaban los servicios de seguridad que protegen y se señala que muchos de estos servicios también se pueden configurar y gestionar desde dentro AWS Organizations. Algunos de estos servicios deberían implementarse en todas las cuentas y los verás en la AWS SRA. Esto permite un conjunto coherente de barreras y proporciona supervisión, administración y gobierno centralizados en toda la organización. AWS

Security Hub CSPM,, GuardDuty AWS Config, IAM Access Analyzer y los registros de la CloudTrail organización aparecen en todas las cuentas. Los tres primeros admiten la función de administrador delegado que se analizó anteriormente en la sección La cuenta de administración, el acceso

confiable y los administradores delegados. CloudTrail actualmente utiliza un mecanismo de agregación diferente.

El repositorio de GitHub código AWS SRA proporciona un ejemplo de implementación para habilitar Security Hub CSPM,, GuardDuty AWS Config, y registros organizativos en todas sus cuentas AWS Firewall Manager, incluida la cuenta de administración de la CloudTrail AWS organización.

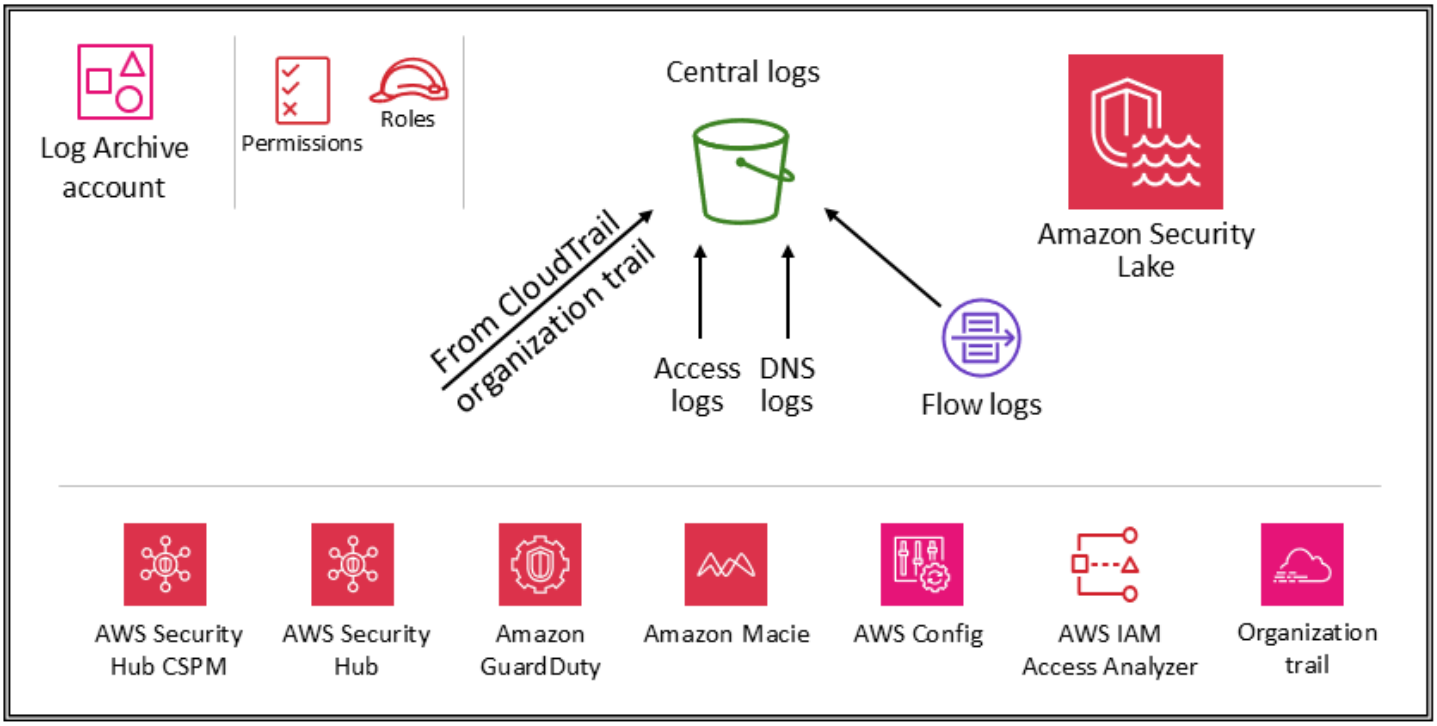
Consideraciones sobre el diseño

- Las configuraciones de cuentas específicas pueden requerir servicios de seguridad adicionales. Por ejemplo, las cuentas que administran buckets de S3 (las cuentas de Application y Log Archive) también deberían incluir Amazon Macie y considerar la posibilidad de activar CloudTrail el registro de eventos de datos de S3 en estos servicios de seguridad comunes. (Macie admite la administración delegada con una configuración y un monitoreo centralizados). Otro ejemplo es Amazon Inspector, que solo se aplica a las cuentas que alojan instancias de EC2 o imágenes de Amazon ECR.
- Además de los servicios descritos anteriormente en esta sección, la AWS SRA incluye dos servicios centrados en la seguridad, Amazon Detective y AWS Audit Manager, que admiten la AWS Organizations integración y la funcionalidad de administrador delegado. Sin embargo, no se incluyen como parte de los servicios recomendados para la creación de cuentas de referencia, ya que hemos observado que es mejor utilizarlos en los siguientes escenarios:
  - Cuenta con un equipo o grupo de recursos dedicados que realizan estas funciones. Los equipos de analistas de seguridad utilizan mejor Detective y Audit Manager es útil para sus equipos de auditoría interna o cumplimiento.
  - Al principio del proyecto, debe centrarse en un conjunto básico de herramientas, como GuardDuty Security Hub (CSPM), y luego desarrollarlas mediante el uso de servicios que proporcionan capacidades adicionales.

UO de seguridad: cuenta de archivos de registro

Influya en el futuro de la arquitectura de referencia de AWS seguridad (AWS SRA) realizando una breve encuesta.

El siguiente diagrama ilustra los servicios de AWS seguridad que están configurados en la cuenta de Log Archive.



La cuenta Log Archive se dedica a ingerir y archivar todos los registros y copias de seguridad relacionados con la seguridad. Con los registros centralizados, puede supervisar, auditar y emitir alertas sobre el acceso a objetos de Amazon S3, la actividad no autorizada por identidades, los cambios en las políticas de IAM y otras actividades críticas realizadas en recursos confidenciales. Los objetivos de seguridad son claros: debe ser un almacenamiento inmutable, al que solo se pueda acceder mediante mecanismos controlados, automatizados y monitoreados, y diseñado para ser duradero (por ejemplo, mediante el uso de los procesos de replicación y archivo adecuados). Los controles se pueden implementar en profundidad para proteger la integridad y la disponibilidad de los registros y del proceso de administración de registros. Además de los controles preventivos, como la asignación de las funciones de menor privilegio para el acceso y el cifrado de los registros con una AWS KMS clave controlada, utilice controles de detección, por ejemplo, AWS Config para supervisar (alertar y corregir) este conjunto de permisos en caso de cambios inesperados.

> **Consideración del diseño**
>
> Los datos de registro operativos que utilizan sus equipos de infraestructura, operaciones y carga de trabajo suelen superponerse con los datos de registro utilizados por los equipos de seguridad, auditoría y cumplimiento. Le recomendamos que consolide los datos de registro

operativos en la cuenta Log Archive. En función de sus requisitos específicos de seguridad y gobierno, es posible que necesite filtrar los datos del registro operativo guardados en esta cuenta. Es posible que también tengas que especificar quién tiene acceso a los datos del registro operativo de la cuenta de Log Archive.

Tipos de registros

Los registros principales que se muestran en la AWS SRA incluyen AWS CloudTrail (registro de la organización), registros de flujo de Amazon VPC, registros de acceso de CloudFront Amazon AWS WAF y registros de DNS de Amazon Route 53. Estos registros proporcionan una auditoría de las acciones emprendidas (o intentadas) por un usuario Servicio de AWS, función o entidad de red (identificadas, por ejemplo, mediante una dirección IP). También se pueden capturar y archivar otros tipos de registros (por ejemplo, registros de aplicaciones o registros de bases de datos). Para obtener más información sobre las fuentes de registro y las prácticas recomendadas de registro, consulte la documentación de seguridad de cada servicio.

Amazon S3 como almacén de registros central

Muchos Servicios de AWS registran información en Amazon S3, ya sea de forma predeterminada o exclusiva. AWS CloudTrail, Amazon VPC Flow Logs, Elastic Load Balancing GuardDuty AWS Config, Amazon y AWS WAF son algunos ejemplos de servicios que registran información en Amazon S3. Esto significa que la integridad del registro se logra mediante la integridad de los objetos de S3; la confidencialidad del registro se logra mediante los controles de acceso a los objetos de S3; y la disponibilidad del registro se logra mediante el bloqueo de objetos de S3, las versiones de los objetos de S3 y las reglas de ciclo de vida de S3. Al registrar la información en un depósito de S3 dedicado y centralizado que reside en una cuenta dedicada, puede gestionar estos registros en unos pocos depósitos y aplicar estrictos controles de seguridad, acceso y separación de funciones.

En la AWS SRA, los registros principales almacenados en Amazon S3 provienen CloudTrail, por lo que en esta sección se describe cómo proteger esos objetos. Esta guía también se aplica a cualquier otro objeto de S3 creado por sus propias aplicaciones o por terceros Servicios de AWS. Aplique estos patrones siempre que tenga datos en Amazon S3 que necesiten una alta integridad, un control de acceso sólido y una retención o destrucción automatizadas.

Todos los objetos nuevos (incluidos los CloudTrail registros) que se cargan en los buckets de S3 se cifran de forma predeterminada mediante el cifrado del lado del servidor de Amazon con claves de cifrado administradas por Amazon S3 (SSE-S3). Esto ayuda a proteger los datos en reposo, pero

el control de acceso está controlado exclusivamente por las políticas de IAM. Para proporcionar una capa de seguridad gestionada adicional, puede utilizar el cifrado del lado del servidor con AWS KMS claves que usted gestione (SSE-KMS) en todos los depósitos de seguridad de S3. Esto añade un segundo nivel de control de acceso. Para leer los archivos de registro, un usuario debe tener permisos de lectura de Amazon S3 para el objeto de S3 y una política o función de IAM aplicada que le permita descifrar mediante la política de claves asociada.

Dos opciones le ayudan a proteger o verificar la integridad de los objetos de CloudTrail registro que se almacenan en Amazon S3. CloudTrail proporciona una validación de la integridad del archivo de registro para determinar si un archivo de registro se modificó o eliminó después de CloudTrail entregarlo. La otra opción es S3 Object Lock.

Además de proteger el propio depósito de S3, puedes seguir el principio de privilegios mínimos para los servicios de registro (por ejemplo CloudTrail) y para la cuenta de Log Archive.
Por ejemplo, los usuarios con permisos concedidos por la política de IAM AWS gestionada `AWSCloudTrail_FullAccess` pueden deshabilitar o reconfigurar las funciones de auditoría más importantes y sensibles de sus usuarios. Cuentas de AWS Limite la aplicación de esta política de IAM al menor número posible de personas.

Utilice controles de detección, como los que proporciona IAM Access Analyzer, para supervisar (y alertar y corregir) este conjunto más amplio de controles preventivos en caso de cambios inesperados. AWS Config

Para obtener más información sobre las mejores prácticas de seguridad para los buckets S3, consulte la documentación de Amazon S3, las charlas técnicas en línea y la entrada del blog Las 10 mejores prácticas de seguridad para proteger los datos en Amazon S3.

> **Ejemplo de implementación**
>
> La biblioteca de códigos AWS SRA proporciona un ejemplo de implementación del acceso público a las cuentas de bloqueo de Amazon S3. Este módulo bloquea el acceso público a Amazon S3 para todas las cuentas existentes y futuras de la AWS organización.

Amazon Security Lake

AWS La SRA recomienda que utilice la cuenta Log Archive como cuenta de administrador delegado para Amazon Security Lake. Al hacerlo, Security Lake recopila los registros compatibles en depósitos S3 dedicados en la misma cuenta que otros registros de seguridad recomendados por la SRA.

Para proteger la disponibilidad de los registros y el proceso de administración de registros, solo el servicio Security Lake o las funciones de IAM administradas por Security Lake para las fuentes o los suscriptores deben acceder a los depósitos de S3 de Security Lake. Además de utilizar controles preventivos (como asignar funciones de acceso con privilegios mínimos y cifrar los registros con una AWS KMS clave controlada), utilice controles de detección AWS Config para supervisar (alertar y corregir) este conjunto de permisos en caso de cambios inesperados.

El administrador de Security Lake puede habilitar la recopilación de registros en toda la organización. AWS Estos registros se almacenan en depósitos S3 regionales de la cuenta Log Archive. Además, para centralizar los registros y facilitar el almacenamiento y el análisis, el administrador de Security Lake puede elegir una o más regiones acumulativas en las que se consoliden y almacenen los registros de todos los depósitos regionales de S3. Los registros compatibles Servicios de AWS se convierten automáticamente en un esquema estandarizado de código abierto denominado Open Cybersecurity Schema Framework (OCSF) y se guardan en formato Apache Parquet en depósitos de Security Lake S3. Gracias a la compatibilidad con OCSF, Security Lake normaliza y consolida de manera eficiente los datos de seguridad procedentes AWS y otras fuentes de seguridad empresariales para crear un repositorio unificado y fiable de información relacionada con la seguridad.

Security Lake puede recopilar registros asociados a eventos AWS CloudTrail de administración y eventos de CloudTrail datos para Amazon S3 y AWS Lambda. Para recopilar los eventos CloudTrail de administración en Security Lake, debe tener al menos un registro organizativo CloudTrail multirregional que recopile los eventos de CloudTrail administración de lectura y escritura. El registro debe estar habilitado para el registro de seguimiento. Un registro multirregional entrega los archivos de registro de varias regiones a un único depósito de S3 para una sola. Cuenta de AWS Si las regiones se encuentran en diferentes países, tenga en cuenta los requisitos de exportación de datos para determinar si se pueden habilitar los senderos multirregionales.

AWS Security Hub CSPM es una fuente de datos nativa compatible con Security Lake, y debería añadir los hallazgos de CSPM de Security Hub a Security Lake. Security Hub CSPM genera hallazgos a partir de muchas integraciones diferentes Servicios de AWS y de terceros. Estos hallazgos le ayudan a obtener una visión general de su postura de cumplimiento y a determinar si está siguiendo las recomendaciones y soluciones de seguridad. AWS AWS Partner

Para obtener visibilidad e información procesable a partir de registros y eventos, puede consultar los datos mediante herramientas como Amazon Athena, Amazon Service, OpenSearch Amazon Quick y soluciones de terceros. Los usuarios que necesiten acceder a los datos de registro de Security Lake no deberían acceder directamente a la cuenta de Log Archive. Solo deben acceder a los datos

desde la cuenta de Security Tooling. O bien, pueden utilizar otras ubicaciones Cuentas de AWS o ubicaciones locales que proporcionen herramientas de análisis, como OpenSearch Service, Quick, o herramientas de terceros, como herramientas de gestión de eventos e información de seguridad (SIEM). Para proporcionar acceso a los datos, el administrador debe configurar los suscriptores de Security Lake en la cuenta de Log Archive y configurar la cuenta que necesita acceder a los datos como suscriptor de acceso a consultas. Para obtener más información, consulte Amazon Security Lake en la sección Seguridad OU – Cuenta de herramientas de seguridad de esta guía.

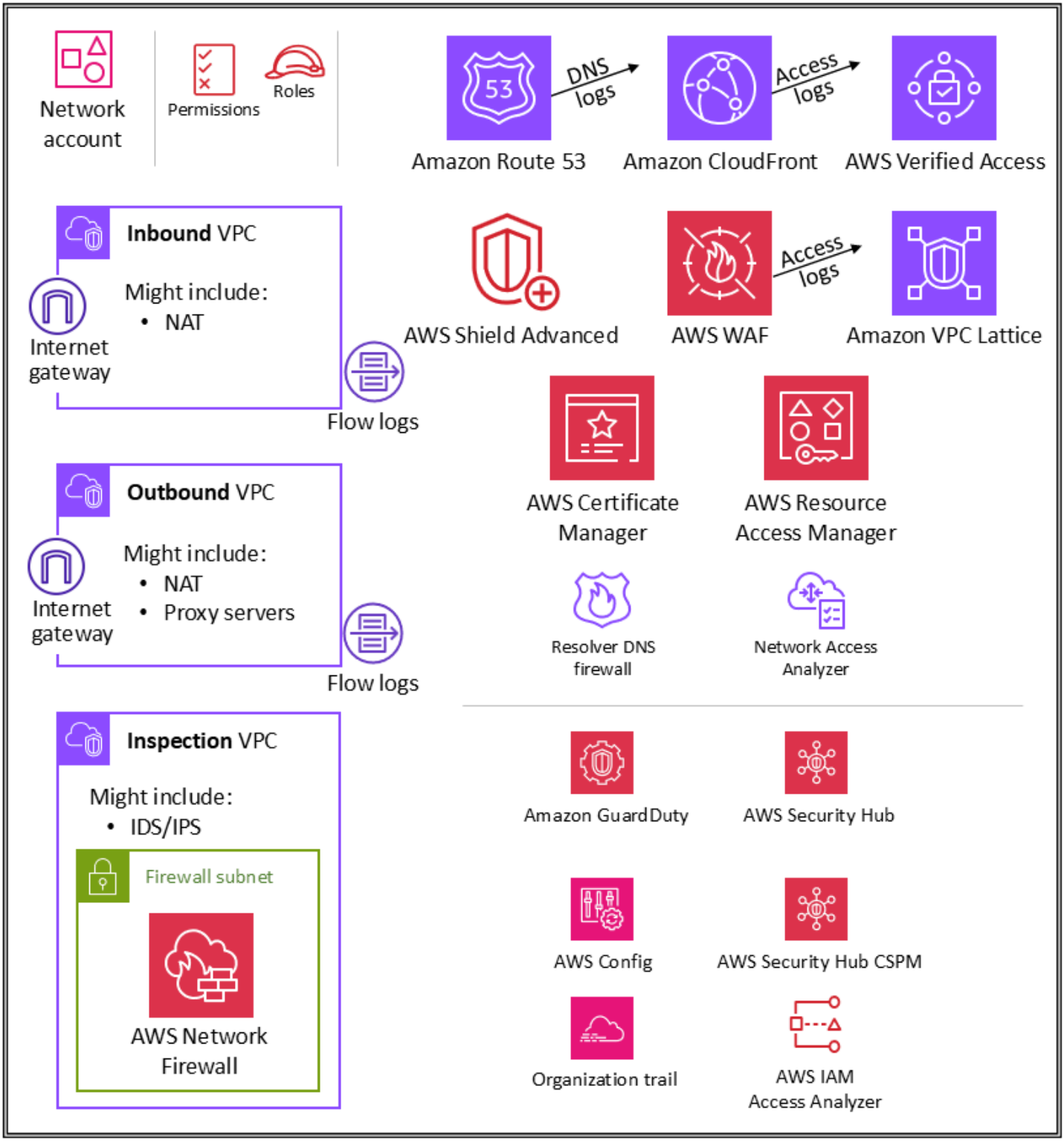
Security Lake proporciona una política AWS administrada que le ayuda a administrar el acceso de los administradores al servicio. Para obtener más información, consulte la Guía del usuario de Security Lake. Como práctica recomendada, le recomendamos que restrinja la configuración de Security Lake a través de los procesos de desarrollo y evite los cambios de configuración a través de las AWS consolas o AWS Command Line Interface (AWS CLI). Además, debe configurar políticas de IAM y políticas de control de servicios (SCPs) estrictas para proporcionar únicamente los permisos necesarios para administrar Security Lake. Puede configurar las notificaciones para detectar cualquier acceso directo a estos depósitos de S3.

> **Consideración del diseño**
>
> Cuando habilita los eventos CloudTrail de administración en Security Lake, se cobran cargos por parte de Security Lake. La recopilación de eventos de CloudTrail administración en Security Lake requiere un registro organizativo CloudTrail multirregional que recopile los eventos de CloudTrail administración de lectura y escritura. Esta primera ruta está disponible sin costo alguno para usted. CloudTrail Los eventos de gestión suelen representar un pequeño porcentaje (alrededor del 5%) del total de CloudTrail eventos. Esto se aplica a los clientes que utilizan AWS Control Tower o tienen CloudTrail registros centralizados en una cuenta de Log Archive.

Unidad organizativa de infraestructura: cuenta de red

Influya en el futuro de la arquitectura de referencia de AWS seguridad (AWS SRA) realizando una breve encuesta.

El siguiente diagrama ilustra los servicios AWS de seguridad que están configurados en la cuenta de red.



La cuenta de red administra la puerta de enlace entre la aplicación y el resto de Internet. Es importante proteger esa interfaz bidireccional. La cuenta de red aísla los servicios, la configuración y el funcionamiento de la red de las cargas de trabajo de las aplicaciones individuales, la seguridad

y otras infraestructuras. Este mecanismo no solo limita la conectividad, los permisos y el flujo de datos, sino que también permite la separación de tareas y el uso de privilegios mínimos para los equipos que necesitan operar en estas cuentas. Al dividir el flujo de la red en nubes privadas virtuales entrantes y salientes independientes (VPCs), puede proteger la infraestructura y el tráfico confidenciales del acceso no deseado. Por lo general, la red entrante se considera de mayor riesgo y merece un enrutamiento y una supervisión adecuados y la mitigación de posibles problemas. Estas cuentas de infraestructura heredarán las barreras de protección de permisos de la cuenta de administración de la organización y de la unidad organizativa de infraestructura. Los equipos de redes (y seguridad) administran la mayor parte de la infraestructura de esta cuenta.

Arquitectura de redes

Si bien el diseño y las especificaciones de la red van más allá del alcance de este documento, recomendamos estas tres opciones para la conectividad de red entre las distintas cuentas: interconexión de VPC y. AWS PrivateLink AWS Transit Gateway A la hora de elegir una de estas opciones, es importante tener en cuenta las normas operativas, los presupuestos y las necesidades específicas de ancho de banda.

- Emparejamiento de VPC: la forma más sencilla de conectar dos VPCs es utilizar el emparejamiento de VPC. Una conexión permite una conectividad bidireccional total entre. VPCs VPCs que están en cuentas separadas y que también Regiones de AWS se pueden emparejar entre sí. A gran escala, cuando se tienen decenas o cientos de ellas VPCs, interconectarlas con la interconexión se traduce en una malla de cientos o miles de conexiones entre pares, lo que puede resultar difícil de gestionar y escalar. El emparejamiento de VPC se utiliza mejor cuando los recursos de una VPC deben comunicarse con los recursos de otra VPC, el entorno de ambas VPCs está controlado y protegido y el número de personas a conectar es inferior VPCs a 10 (para permitir la administración individual de cada conexión).
- AWS PrivateLink– PrivateLink proporciona conectividad privada entre servicios y VPCs aplicaciones. Puede crear su propia aplicación en su VPC y configurarla como un servicio PrivateLink con tecnología (denominado servicio de punto final). Otros AWS principales pueden crear una conexión desde su VPC a su servicio de punto final mediante un punto final de interfaz de VPC o un punto final de Gateway Load Balancer, según el tipo de servicio. Cuando lo usas PrivateLink, el tráfico del servicio no pasa a través de una red enrutable públicamente. Úselo PrivateLink cuando tenga una configuración cliente-servidor en la que desee dar a uno o más consumidores acceso VPCs unidireccional a un servicio o conjunto de instancias específicos en la VPC del proveedor de servicios. Esta también es una buena opción cuando los clientes y los servidores de los dos VPCs tienen direcciones IP superpuestas, ya que PrivateLink utiliza

interfaces de red elásticas dentro de la VPC del cliente para que no haya conflictos de IP con el proveedor de servicios.

- AWS Transit Gateway– Transit Gateway ofrece un hub-and-spoke diseño para la conexión VPCs y las redes locales como un servicio totalmente gestionado sin necesidad de aprovisionar dispositivos virtuales. AWS gestiona la alta disponibilidad y la escalabilidad. Una pasarela de tránsito es un recurso regional y puede conectar miles de personas VPCs dentro de la misma Región de AWS. Puede conectar su conectividad híbrida (VPN y AWS Direct Connect conexiones) a una única pasarela de tránsito, consolidando y controlando así toda la configuración de enrutamiento de su AWS organización en un solo lugar. Una puerta de enlace de tránsito resuelve la complejidad que implica la creación y administración de múltiples conexiones de emparejamiento de VPC a escala. Es la opción predeterminada para la mayoría de las arquitecturas de red, pero las necesidades específicas en cuanto al costo, el ancho de banda y la latencia pueden hacer que la interconexión de VPC se adapte mejor a sus necesidades.

VPC entrante (de entrada)

La VPC entrante está diseñada para aceptar, inspeccionar y enrutar las conexiones de red iniciadas desde fuera de la aplicación. Según las características específicas de la aplicación, puede esperar ver alguna que otra traducción de direcciones de red (NAT) en esta VPC. Los registros de flujo de esta VPC se capturan y almacenan en la cuenta de archivo de registro.

VPC saliente (de salida)

La VPC saliente está destinada a administrar las conexiones de red iniciadas desde la aplicación. Según las características específicas de la aplicación, puede esperar ver tráfico NAT, puntos de enlace de Servicio de AWS VPC específicos y alojamiento de puntos de enlace de API externos en esta VPC. Los registros de flujo de esta VPC se capturan y almacenan en la cuenta de archivo de registro.

VPC de inspección

Una VPC de inspección dedicada proporciona un enfoque simplificado y central para gestionar las inspecciones entre Internet y las redes locales VPCs (en la misma o en diferentes Regiones de AWS). Para la AWS SRA, asegúrese de que todo el tráfico intermedio VPCs pase por la VPC de inspección y evite utilizar la VPC de inspección para cualquier otra carga de trabajo.

AWS Network Firewall

AWS Network Firewalles un servicio de firewall de red gestionado y de alta disponibilidad para su VPC. Le permite implementar y gestionar sin esfuerzo la inspección de estado, la prevención y detección de intrusiones y el filtrado web para proteger sus redes virtuales. AWS Puede usar Network Firewall para descifrar las sesiones de TLS e inspeccionar el tráfico entrante y saliente. Para obtener más información sobre la configuración de Network Firewall, consulte la AWS Network Firewall entrada del blog «New Managed Firewall Service in VPC».

El firewall se utiliza por zona de disponibilidad en la VPC. Para cada zona de disponibilidad, elige una subred para alojar el punto de conexión del firewall que filtra su tráfico. El punto de conexión del firewall de una zona de disponibilidad puede proteger todas las subredes de la zona, excepto la subred en la que se encuentra. Según el caso de uso y el modelo de implementación, la subred del firewall puede ser pública o privada. El firewall es completamente transparente en cuanto al flujo de tráfico y no traduce direcciones de red (NAT). Conserva la dirección de origen y destino. En esta arquitectura de referencia, los puntos de conexión del firewall se alojan en una VPC de inspección. Todo el tráfico de la VPC entrante y hacia la VPC saliente se enruta a través de esta subred de firewall para su inspección.

Network Firewall hace que la actividad del firewall sea visible en tiempo real a través de CloudWatch las métricas de Amazon y ofrece una mayor visibilidad del tráfico de red mediante el envío de registros a Amazon Simple Storage Service (Amazon S3) CloudWatch y Amazon Data Firehose. Network Firewall es interoperable con su enfoque de seguridad actual, incluidas las tecnologías de AWS los socios. También puede importar los conjuntos de reglas de Suricata existentes, que pueden haber sido redactados internamente o extraídos externamente de otros proveedores o plataformas de código abierto.

En la AWS SRA, Network Firewall se usa dentro de la cuenta de red porque la funcionalidad del servicio centrada en el control de la red se alinea con la intención de la cuenta.

Consideraciones sobre el diseño

- AWS Firewall Manager es compatible con Network Firewall, por lo que puede configurar e implementar de forma centralizada las reglas de Network Firewall en toda su organización. (Para obtener más información, consulte Uso de AWS Network Firewall políticas en Firewall Manager en la AWS documentación). Al configurar el Firewall Manager, se crea automáticamente un firewall con conjuntos de reglas en las cuentas y VPCs que usted

especifique. También implementa un punto de conexión en una subred dedicada para cada zona de disponibilidad que contenga subredes públicas. Al mismo tiempo, cualquier cambio que se efectúa en el conjunto de reglas configurado centralmente se propaga de forma automática a los firewalls de Network Firewall implementados.

- Existen varios modelos de implementación disponibles con Network Firewall. El modelo correcto depende de su caso de uso y sus requisitos. Algunos ejemplos son los siguientes:
  - Un modelo de despliegue distribuido en el que Network Firewall se despliega de forma individual VPCs.
  - Un modelo de implementación centralizada en el que Network Firewall se implementa en una VPC centralizada para el tráfico este-oeste (de VPC a VPC) o norte-sur (entrada y salida de Internet, en las instalaciones).
  - Un modelo de implementación combinado en el que Network Firewall se implementa en una VPC centralizada para el tráfico este-oeste y un subconjunto del tráfico norte-sur.
- Como recomendación, no utilice la subred de Network Firewall para implementar cualquier otro servicio. Esto se debe a que Network Firewall no puede inspeccionar el tráfico de orígenes o destinos dentro de la subred de un firewall.

Analizador de acceso a la red

Analizador de acceso a la red es una característica de Amazon VPC que identifica el acceso de red no deseado a sus recursos. Puede usar Analizador de acceso a la red para validar la segmentación de la red, identificar los recursos a los que se puede acceder desde Internet o a los que solo se puede acceder desde rangos de direcciones IP confiables y validar que cuenta con los controles de red adecuados en todas las rutas de red.

El analizador de acceso a la red utiliza algoritmos de razonamiento automatizados para analizar las rutas de red que un paquete puede recorrer entre los recursos de una AWS red y produce resultados para las rutas que coinciden con el alcance de acceso a la red definido. Analizador de acceso a la red realiza un análisis estático de una configuración de red, lo que significa que no se transmite ningún paquete en la red como parte de este análisis.

Las reglas de Accesibilidad de la red de Amazon Inspector proporcionan una característica relacionada. Los resultados generados por estas reglas se utilizan en la cuenta de aplicación. Tanto Network Access Analyzer como Network Reachability utilizan la tecnología más reciente de la iniciativa de seguridad AWS demostrable y aplican esta tecnología en diferentes áreas de enfoque.

El paquete Network Reachability se centra específicamente en las instancias y su accesibilidad a Internet EC2 .

La cuenta de red define la infraestructura de red crítica que controla el tráfico que entra y sale de su AWS entorno. Este tráfico debe supervisarse rigurosamente. En la AWS SRA, el analizador de acceso a la red se usa dentro de la cuenta de red para ayudar a identificar el acceso no deseado a la red, identificar los recursos accesibles a Internet a través de las puertas de enlace de Internet y verificar que los controles de red adecuados, como los firewalls de red y las puertas de enlace NAT, estén presentes en todas las rutas de red entre los recursos y las puertas de enlace de Internet.

> **Consideración del diseño**
>
> El analizador de acceso a la red es una función de Amazon VPC y se puede usar en Cuenta de AWS cualquier VPC que tenga una VPC. Los administradores de red pueden asignar funciones de IAM específicas y multicuentas para validar que las rutas de red aprobadas se apliquen en cada una de ellas. Cuenta de AWS

AWS RAM

AWS Resource Access Manager(AWS RAM) le ayuda a compartir de forma segura los AWS recursos que cree en uno Cuenta de AWS con otro. Cuentas de AWSAWS RAM proporciona un lugar central para gestionar el uso compartido de recursos y estandarizar esta experiencia en todas las cuentas. Esto simplifica la administración de los recursos al mismo tiempo que se aprovecha el aislamiento administrativo y de facturación, y reduce el alcance de las ventajas de la contención del impacto que una estrategia de múltiples cuentas puede ofrecer. Si tu cuenta está gestionada por AWS Organizations, te AWS RAM permite compartir recursos con todas las cuentas de la organización o solo con las cuentas de una o más unidades organizativas específicas (OUs). También puedes compartirlos con un identificador Cuentas de AWS de cuenta específico, independientemente de si la cuenta forma parte de una organización. También puede compartir algunos tipos de recursos compatibles con roles y usuarios de IAM específicos.

AWS RAM le permite compartir recursos que no son compatibles con las políticas de IAM basadas en recursos, como las subredes de VPC y las reglas de Route 53. Además AWS RAM, los propietarios de un recurso pueden ver qué directores tienen acceso a los recursos individuales que han compartido. Los directores de IAM pueden recuperar directamente la lista de recursos que han compartido con ellos, lo que no pueden hacer con los recursos compartidos por las políticas de

recursos de IAM. Si AWS RAM se utiliza para compartir recursos fuera de la AWS organización, se inicia un proceso de invitación. El destinatario debe aceptar la invitación antes de conceder el acceso a los recursos. Esto proporciona controles y contrapesos adicionales.

AWS RAM lo invoca y administra el propietario del recurso, en la cuenta en la que se implementa el recurso compartido. Un caso de uso común que AWS RAM se ilustra en la AWS SRA es que los administradores de red compartan las subredes de VPC y las puertas de enlace de tránsito con toda la organización. AWS Esto proporciona la posibilidad de separar las funciones de administración de la red Cuenta de AWS y ayuda a lograr la separación de funciones. Para obtener más información sobre el uso compartido de VPC, consulte la AWS entrada del blog Uso compartido de VPC: un nuevo enfoque para la administración de múltiples cuentas y VPC y el documento técnico sobre la infraestructura de red.AWS

> Consideración del diseño
>
> Si bien AWS RAM un servicio se implementa solo dentro de la cuenta de red de la AWS SRA, normalmente se implementa en más de una cuenta. Por ejemplo, puede centralizar la administración de su lago de datos en una sola cuenta de lago de datos y, a continuación, compartir los recursos del catálogo de AWS Lake Formation datos (bases de datos y tablas) con otras cuentas de su AWS organización. Para obtener más información, consulte la AWS Lake Formation documentación y la entrada del AWS blog Comparta sus datos de forma segura entre usuarios Cuentas de AWS . AWS Lake Formation Además, los administradores de seguridad pueden AWS RAM seguir las mejores prácticas a la hora de crear una AWS Private Certificate Authority jerarquía. CAs se puede compartir con terceros externos, que pueden emitir certificados sin tener acceso a la jerarquía de CA. Esto permite a las organizaciones de origen limitar y revocar el acceso de terceros.

Acceso verificado de AWS

Acceso verificado de AWSproporciona un acceso seguro a las aplicaciones y los recursos corporativos sin una VPN. Mejora la postura de seguridad y ayuda a aplicar un acceso de confianza cero al evaluar cada solicitud de acceso en tiempo real comparándola con los requisitos predefinidos. Puede definir una política de acceso única para cada aplicación con condiciones basadas en los datos de identidad y en la posición del dispositivo. Verified Access proporciona acceso seguro a aplicaciones HTTP (S), como aplicaciones basadas en navegador y aplicaciones que no son HTTP (S) a través de protocolos TCP, SSH y RDP para aplicaciones como repositorios, bases de datos

y grupos de instancias de Git. EC2 Se puede acceder a ellos mediante un terminal de línea de comandos o desde una aplicación de escritorio. Acceso verificado también simplifica las operaciones de seguridad al ayudar a los administradores a establecer y supervisar las políticas de acceso de manera eficiente. Esto libera tiempo para actualizar las políticas, responder a los incidentes de seguridad y conectividad y auditar los estándares de cumplimiento. Verified Access también admite la integración AWS WAF para ayudarlo a filtrar las amenazas más comunes, como la inyección de SQL y las secuencias de comandos entre sitios (XSS). Verified Access se integra perfectamente con AWS IAM Identity Center, lo que permite a los usuarios autenticarse con proveedores de identidad externos basados en SAML (). IdPs Si ya tiene una solución de IdP personalizada que sea compatible con OpenID Connect (OIDC), Acceso verificado también puede autenticar a los usuarios mediante la conexión directa con su IdP. Además, Acceso verificado registra todos los intentos de acceso para ayudarlo a responder rápidamente a los incidentes de seguridad y a las solicitudes de auditoría. Verified Access admite el envío de estos registros a Amazon Simple Storage Service (Amazon S3), Amazon Logs y CloudWatch Amazon Data Firehose.

Acceso verificado admite dos patrones comunes de aplicaciones corporativas: internas y con acceso a Internet. Acceso verificado se integra con las aplicaciones mediante equilibradores de carga de aplicación o interfaces de red elásticas. Si utilizas un Application Load Balancer, Verified Access requiere un balanceador de carga interno. Dado que Verified Access es compatible AWS WAF a nivel de instancia, una aplicación existente que se AWS WAF integre con un Application Load Balancer puede mover políticas del balanceador de carga a la instancia de Verified Access. Una aplicación corporativa se representa como un punto de conexión de Acceso verificado. Cada punto de conexión está asociado a un grupo de Acceso verificado y hereda la política de acceso del grupo. Un grupo de Acceso verificado es un conjunto de puntos de conexión de Acceso verificado y una política de Acceso verificado a nivel de grupo. Los grupos simplifican la administración de políticas y permiten a los administradores de TI establecer criterios básicos. Los propietarios de las aplicaciones pueden definir con más detalle las políticas detalladas en función de la sensibilidad de la aplicación.

En la AWS SRA, el acceso verificado se aloja en la cuenta de red. El equipo central de TI establece las configuraciones administradas de forma centralizada. Por ejemplo, puede conectar proveedores de confianza, como proveedores de identidad (por ejemplo, Okta) y proveedores de confianza de dispositivos (por ejemplo, Jamf), crear grupos y determinar la política a nivel de grupo. Luego, estas configuraciones se pueden compartir con decenas, cientos o miles de cuentas de carga de trabajo mediante AWS RAM el uso de. Esto permite a los equipos de aplicaciones gestionar los puntos finales subyacentes que gestionan sus aplicaciones sin sobrecargar a otros equipos. AWS RAM proporciona una forma escalable de aprovechar el acceso verificado para las aplicaciones corporativas alojadas en diferentes cuentas de carga de trabajo.

> **Consideración del diseño**
>
> Puede agrupar los puntos de conexión para aplicaciones que tengan requisitos de seguridad similares para simplificar la administración de políticas y luego compartir el grupo con las cuentas de aplicación. Todas las aplicaciones del grupo comparten la política de grupo. Si una aplicación del grupo requiere una política específica debido a un caso extremo, puede aplicar una política a nivel de aplicación para esa aplicación.

Amazon VPC Lattice

Amazon VPC Lattice es un servicio de redes de aplicaciones que conecta, supervisa y protege las comunicaciones. service-to-service Un servicio, que suele denominarse microservicio, es una unidad de software que se puede implementar de forma independiente y que realiza una tarea específica. VPC Lattice administra automáticamente la conectividad de la red y el enrutamiento de la capa de aplicaciones entre los servicios a través de VPCs y Cuentas de AWS sin necesidad de administrar la conectividad de red subyacente, los balanceadores de carga frontend o los proxies sidecar. Proporciona un proxy de capa de aplicación totalmente administrado que proporciona un enrutamiento a nivel de aplicación en función de las características de las solicitudes, como las rutas y los encabezados. VPC Lattice está integrado en la infraestructura de VPC, por lo que proporciona un enfoque coherente en una amplia gama de tipos de procesamiento, como Amazon Elastic Compute Cloud (Amazon), Amazon Elastic Kubernetes Service (Amazon EKS EC2) y. AWS Lambda VPC Lattice también admite el enrutamiento ponderado para blue/green despliegues tipo canario. Puede usar VPC Lattice para crear una red de servicios con un límite lógico que implemente automáticamente la detección y la conectividad de los servicios. VPC Lattice se integra con IAM para la service-to-service autenticación y la autorización mediante políticas de autenticación.

VPC Lattice se integra AWS RAM para permitir el uso compartido de servicios y redes de servicios. AWS SRA describe una arquitectura distribuida en la que los desarrolladores o propietarios de servicios crean servicios de VPC Lattice en su cuenta de aplicación. Los propietarios de los servicios definen los oyentes, las reglas de enrutamiento y los grupos objetivo junto con las políticas de autenticación. A continuación, comparten los servicios con otras cuentas y los asocian a las redes de servicios de VPC Lattice. Los administradores de red crean estas redes en la cuenta de red y las comparten con la cuenta de aplicación. Los administradores de red configuran las políticas de autenticación y el monitoreo a nivel de la red de servicios. Los administradores asocian VPCs los servicios de VPC Lattice a una o más redes de servicios. Para obtener un recorrido detallado de esta

arquitectura distribuida, consulte la entrada del AWS blog Cree una conectividad segura de múltiples cuentas y múltiples VPC para sus aplicaciones con Amazon VPC Lattice

Consideraciones sobre el diseño

- Según el modelo operativo de servicio de su organización o la visibilidad de la red de servicios, los administradores de red pueden compartir sus redes de servicios y dar a los propietarios de los servicios el control necesario para asociar sus servicios y a estas redes de servicios. VPCs O bien, los propietarios de los servicios pueden compartir sus servicios y los administradores de red pueden asociar los servicios a las redes de servicios.
- Un cliente puede enviar solicitudes a servicios asociados con una red de servicios solo si el cliente está en una VPC asociada con la misma red de servicios. Se deniega el tráfico de clientes que atraviesa una conexión de emparejamiento de VPC o una puerta de enlace de tránsito.

Seguridad de la periferia

La seguridad perimetral generalmente implica tres tipos de protecciones: la entrega segura de contenido, la protección de la red y la capa de aplicaciones y la mitigación de las denegaciones de servicio distribuidasDDo. El contenido, como datos, vídeos y APIs aplicaciones, debe entregarse de forma rápida y segura, utilizando la versión recomendada de TLS para cifrar las comunicaciones entre los puntos finales. El contenido también debe tener restricciones de acceso mediante cookies URLs firmadas y autenticadas mediante token. La seguridad a nivel de aplicación debe diseñarse para controlar el tráfico de bots, bloquear los patrones de ataque más comunes, como la inyección de código SQL o scripting entre sitios (XSS), y proporcionar visibilidad del tráfico web. En la periferia, DDo la mitigación de las emisiones de carbono proporciona una importante capa de defensa que garantiza la disponibilidad continua de las operaciones y los servicios empresariales fundamentales para la misión. Las aplicaciones APIs deben estar protegidas contra las inundaciones de SYN, las inundaciones de UDP u otros ataques de reflexión, y contar con una mitigación integrada para detener los ataques básicos a la capa de red.

AWS ofrece varios servicios para ayudar a proporcionar un entorno seguro, desde la nube central hasta el borde de la red. AWS Amazon CloudFront AWS Certificate Manager (ACM) y Amazon Route 53 trabajan juntos para ayudar a crear un perímetro de seguridad flexible y en capas. AWS Shield AWS WAF El contenido o las aplicaciones se pueden entregar a través de HTTPS mediante TLSv1 0.3 para cifrar y proteger la comunicación entre los espectadores, los clientes y. CloudFront

APIs CloudFront Puede usar ACM para crear un certificado SSL personalizado e implementarlo en una CloudFront distribución de forma gratuita. ACM maneja automáticamente la renovación del certificado. Shield es un servicio de protección DDo S gestionado que ayuda a proteger las aplicaciones que se ejecutan en ellas AWS. Proporciona una detección dinámica y mitigaciones automáticas en línea que minimizan el tiempo de inactividad y la latencia de las aplicaciones. AWS WAF permite crear reglas para filtrar el tráfico web en función de condiciones específicas (direcciones IP, encabezados y cuerpo HTTP o personalizadas URIs), ataques web habituales y bots generalizados. Route 53 es un servicio web de sistema de nombres de dominio (DNS) escalable y de alta disponibilidad. Route 53 conecta las solicitudes de los usuarios con las aplicaciones de Internet que se ejecutan de forma local AWS o local. La AWS SRA adopta una arquitectura de entrada a la red centralizada AWS Transit Gateway, alojada en la cuenta de red, por lo que la infraestructura de seguridad perimetral también está centralizada en esta cuenta.

Amazon CloudFront

Amazon CloudFront es una red de entrega de contenido (CDN) segura que proporciona una protección inherente contra los intentos comunes de transporte y capa de red DDo. Puede entregar su contenido o aplicaciones mediante certificados TLS, y las funciones TLS avanzadas se activan automáticamente. APIs Puedes usar AWS Certificate Manager (ACM) para crear un certificado TLS personalizado y reforzar las comunicaciones HTTPS entre los espectadores CloudFront, tal y como se describe más adelante en la sección ACM. También puede exigir que las comunicaciones entre CloudFront y su origen personalizado implementen el end-to-end cifrado en tránsito. En este caso, debe instalar un certificado TLS en su servidor de origen. Si su origen es un equilibrador de carga elástico, puede usar un certificado generado por ACM o un certificado validado por una entidad de certificación (CA) externa e importado a ACM. Si los puntos de enlace del sitio web del bucket de S3 sirven como origen CloudFront, no puede configurarlo CloudFront para usar HTTPS con su origen, ya que Amazon S3 no admite HTTPS para los puntos de enlace del sitio web. (Sin embargo, puede seguir requiriendo HTTPS entre los espectadores y CloudFront.) Para todos los demás orígenes que admiten la instalación de certificados HTTPS, debe utilizar un certificado firmado por una CA de terceros confiable.

CloudFront ofrece varias opciones para proteger y restringir el acceso a su contenido. Por ejemplo, puede restringir el acceso a su origen de Amazon S3 mediante el uso de cookies firmadas URLs y firmadas. Para obtener más información, consulte Configurar el acceso seguro y restringir el acceso al contenido en la CloudFront documentación.

La AWS SRA ilustra CloudFront las distribuciones centralizadas en la cuenta de red porque se alinean con el patrón de red centralizada que se implementa mediante el uso. AWS Transit Gateway

Al implementar y administrar CloudFront las distribuciones en la cuenta de red, obtiene los beneficios de los controles centralizados. Puede administrar todas CloudFront las distribuciones en un solo lugar, lo que facilita el control del acceso, la configuración de los ajustes y la supervisión del uso en todas las cuentas. Además, puede administrar los certificados ACM, los registros de DNS y los CloudFront registros desde una cuenta centralizada.

El panel CloudFront de seguridad proporciona AWS WAF visibilidad y controles directamente en su CloudFront distribución. Obtendrá visibilidad de las principales tendencias de seguridad de su aplicación, del tráfico permitido y bloqueado y de la actividad de los bots. Puede utilizar herramientas de investigación, como analizadores visuales de registros y controles de bloqueo integrados, para aislar los patrones de tráfico y bloquear el tráfico sin consultar los registros ni escribir reglas de seguridad.

Consideraciones sobre el diseño

- Como alternativa, puede implementarla CloudFront como parte de la aplicación en la cuenta de la aplicación. En este escenario, el equipo de aplicaciones toma decisiones como la forma de implementar las CloudFront distribuciones, determina las políticas de caché adecuadas y asume la responsabilidad de la gobernanza, la auditoría y la supervisión de las CloudFront distribuciones. Al distribuir CloudFront las distribuciones entre varias cuentas, puede beneficiarse de cuotas de servicio adicionales. Como otra ventaja, puede utilizar CloudFront la configuración de identidad de acceso de origen (OAI) y control de acceso de origen (OAC) inherente y automatizada para restringir el acceso a los orígenes de Amazon S3.
- Cuando publica contenido web a través de una CDN, por ejemplo CloudFront, debe evitar que los espectadores pasen por alto la CDN y accedan directamente a su contenido original. Para lograr esta restricción de acceso al origen, puedes usar CloudFront y AWS WAF añadir encabezados personalizados y verificar los encabezados antes de reenviar las solicitudes a tu origen personalizado. Para obtener una explicación detallada de esta solución, consulta la entrada del blog sobre AWS seguridad Cómo mejorar la seguridad de Amazon CloudFront Origin con AWS WAF y AWS Secrets Manager. Un método alternativo consiste en limitar únicamente la lista de CloudFront prefijos del grupo de seguridad asociado al Application Load Balancer. Esto ayudará a garantizar que solo una CloudFront distribución pueda acceder al balanceador de cargas.

AWS WAF

AWS WAFes un firewall de aplicaciones web que ayuda a proteger sus aplicaciones web de las vulnerabilidades web, como las vulnerabilidades más comunes y los bots, que podrían afectar a la disponibilidad de las aplicaciones, comprometer la seguridad o consumir recursos excesivos. Se puede integrar con una CloudFront distribución de Amazon, una API REST de Amazon API Gateway, un Application Load Balancer, una API de AWS AppSync GraphQL, un grupo de usuarios de Amazon Cognito y el servicio. AWS App Runner

AWS WAF utiliza listas de control de acceso web (ACLs) para proteger un conjunto de recursos. AWS Una ACL web es un conjunto de reglas que define los criterios de inspección y la acción asociada que se debe realizar (bloquear, permitir, contar o ejecutar el control de bots) si una solicitud web cumple con los criterios. AWS WAF proporciona un conjunto de reglas administradas que proporcionan protección contra las vulnerabilidades más comunes de las aplicaciones. Estas reglas están seleccionadas y administradas por AWS AWS nuestros socios. AWS WAF también ofrece un potente lenguaje de reglas para crear reglas personalizadas. Puede usar reglas personalizadas para redactar criterios de inspección que se ajusten a sus necesidades específicas. Los ejemplos incluyen las restricciones de IP, las restricciones geográficas y las versiones personalizadas de las reglas administradas que se adapten mejor al comportamiento específico de su aplicación.

AWS WAF proporciona un conjunto de reglas inteligentes gestionadas por niveles para bots comunes y específicos y para la protección contra el robo de cuentas (ATP). Se le cobrará una cuota de suscripción y una cuota de inspección de tráfico cuando utilice los grupos de reglas de ATP y control de bots. Por lo tanto, le recomendamos que primero supervise su tráfico y luego decida qué utilizar. Puedes utilizar los paneles de administración de bots y de apropiación de cuentas que están disponibles de forma gratuita en la AWS WAF consola para supervisar estas actividades y, a continuación, decidir si necesitas un grupo de reglas de nivel inteligente. AWS WAF

En la AWS SRA, AWS WAF está integrado CloudFront en la cuenta de red. En esta configuración, el procesamiento de AWS WAF reglas se realiza en las ubicaciones de borde en lugar de dentro de la VPC. Esto permite filtrar el tráfico malintencionado más cerca del usuario final que solicitó el contenido y ayuda a impedir que dicho tráfico entre en la red principal.

Puede enviar AWS WAF registros completos a un bucket de S3 de la cuenta de Log Archive configurando el acceso multicuenta al bucket de S3. Para obtener más información, consulte el artículo de AWS Re:post sobre este tema.

Consideraciones sobre el diseño

- Como alternativa a la implementación AWS WAF centralizada en la cuenta de red, algunos casos de uso se resuelven mejor si la implementación se realiza AWS WAF en la cuenta de aplicación. Por ejemplo, puede elegir esta opción cuando implemente sus CloudFront distribuciones en su cuenta de aplicación o tenga balanceadores de carga de aplicaciones públicos, o si usa API Gateway delante de sus aplicaciones web. Si decide realizar la implementación AWS WAF en cada cuenta de aplicación, úsela AWS Firewall Manager para administrar AWS WAF las reglas de estas cuentas desde la cuenta centralizada de Security Tooling.
- También puede agregar AWS WAF reglas generales en la CloudFront capa y reglas adicionales específicas de la aplicación AWS WAF en un recurso regional, como Application Load Balancer o la puerta de enlace de API.

AWS Shield

AWS Shieldes un servicio de protección DDo S gestionado que protege las aplicaciones que se ejecutan en él. AWS Hay dos niveles de Shield: Shield Standard y Shield Advanced. Shield Standard proporciona AWS a todos los clientes protección contra los eventos de infraestructura más comunes (capas 3 y 4) sin cargo adicional. Shield Advanced proporciona mitigaciones automáticas más sofisticadas para eventos no autorizados que se dirigen a aplicaciones en zonas alojadas protegidas de Amazon EC2, Elastic Load Balancing (Elastic Load Balancing) y Route 53. CloudFront AWS Global Accelerator Si posee sitios web de alta visibilidad o es propenso a sufrir ataques DDo S frecuentes, puede considerar las funciones adicionales que ofrece Shield Advanced.

Puede usar la función de mitigación automática de la capa DDo S de aplicaciones de Shield Advanced para configurar Shield Advanced para que responda automáticamente y mitigue los ataques de la capa de aplicaciones (capa 7) contra sus CloudFront distribuciones protegidas, los balanceadores de carga de Elastic Load Balancing (Elastic Load Balancing) (Application, Network y Classic), las zonas alojadas de Amazon Route 53, las direcciones IP de Amazon EC2 Elastic y los aceleradores AWS Global Accelerator estándar. Al activar esta función, Shield Advanced genera automáticamente AWS WAF reglas personalizadas para mitigar los ataques DDo S. Shield Advanced también te da acceso al equipo de AWS Shield respuesta (SRT). Puede ponerse en contacto con SRT en cualquier momento para crear y gestionar mitigaciones personalizadas para su aplicación o durante un ataque S activo. DDo Si desea que SRT supervise de forma proactiva sus

recursos protegidos y se ponga en contacto con usted durante un DDo intento de ataque, considere la posibilidad de habilitar la función de participación proactiva.

Consideraciones sobre el diseño

- Si tiene cargas de trabajo gestionadas por recursos con acceso a Internet en la cuenta de la aplicación, como un Application Load Balancer o un Network Load Balancer CloudFront, configure Shield Advanced en la cuenta de la aplicación y añada esos recursos a la protección Shield. Puede utilizarlas para configurar estas opciones AWS Firewall Manager a escala.
- Si tiene varios recursos en el flujo de datos, como una CloudFront distribución delante de un Application Load Balancer, utilice solo el recurso de punto de entrada como recurso protegido. Esto garantizará que no pague dos veces las tarifas de transferencia de datos salientes (DTO) de Shield por dos recursos.
- Shield Advanced registra las métricas que puedes supervisar en Amazon CloudWatch. (Para obtener más información, consulte Monitorización con Amazon CloudWatch en la AWS documentación). Configure CloudWatch alarmas para recibir notificaciones de SNS en su centro de seguridad cuando se detecte un evento DDo S. En caso de sospecha de un caso DDo S, póngase en contacto con el equipo de AWS Enterprise Support presentando un ticket de soporte y asignándole la máxima prioridad. El equipo de Enterprise Support incluirá al equipo de respuesta de Shield (SRT) cuando se encargue del evento. Además, puede preconfigurar la función Lambda de AWS Shield contratación para crear un ticket de soporte y enviar un correo electrónico al equipo de SRT.

AWS Certificate Manager (ACM)

AWS Certificate Manager(ACM) le permite aprovisionar, administrar e implementar certificados TLS públicos y privados para usarlos con Servicios de AWS sus recursos internos conectados. Con ACM, puede solicitar rápidamente un certificado, implementarlo en AWS recursos integrados con ACM, como los balanceadores de carga de Elastic Load Balancing, CloudFront las distribuciones y en Amazon API APIs Gateway, y dejar que ACM se encargue de las renovaciones de los certificados. Al solicitar certificados públicos de ACM, no es necesario generar un key pair ni una solicitud de firma de certificado (CSR), enviar una CSR a una autoridad de certificación (CA) ni cargar e instalar el certificado cuando se reciba. ACM también ofrece la opción de importar certificados TLS emitidos por terceros CAs e implementarlos con los servicios integrados de ACM. Cuando utiliza ACM para

administrar certificados, las claves privadas de los certificados se protegen y almacenan de forma segura mediante un cifrado sólido y las mejores prácticas de administración de claves. Con ACM no hay ningún cargo adicional por el aprovisionamiento de certificados públicos y ACM gestiona el proceso de renovación.

El ACM se utiliza en la cuenta de red para generar un certificado TLS público que, a su vez, lo utilizan CloudFront las distribuciones para establecer la conexión HTTPS entre los espectadores y. CloudFront Para obtener más información, consulte la Documentación de CloudFront .

> **Consideración del diseño**
>
> En el caso de los certificados externos, ACM debe residir en la misma cuenta que los recursos para los que aprovisiona los certificados. Los certificados no se pueden compartir entre cuentas.

Amazon Route 53

Amazon Route 53 es un servicio web de sistema de nombres de dominio (DNS) escalable y de alta disponibilidad. Puede utilizar Route 53 para realizar tres funciones principales: registro de dominio, direccionamiento de DNS y comprobación de estado.

Puede usar Route 53 como un servicio de DNS para asignar nombres de dominio a sus EC2 instancias, depósitos de S3, CloudFront distribuciones y otros recursos. AWS La naturaleza distribuida de los servidores AWS DNS ayuda a garantizar que los usuarios finales se dirijan a la aplicación de forma coherente. Características como el flujo de tráfico de Route 53 y el control de enrutamiento le ayudan a mejorar la confiabilidad. Si el punto de conexión de su aplicación principal deja de estar disponible, puede configurar la conmutación por error para redirigir a los usuarios a una ubicación alternativa. Route 53 Resolver proporciona un DNS recursivo para su VPC y sus redes locales a AWS Direct Connect través AWS de una VPN administrada o gestionada.

Al usar el servicio de IAM con Route 53, tienes un control detallado sobre quién puede actualizar tus datos de DNS. Puede habilitar la firma de extensiones de seguridad de DNS (DNSSEC) para permitir que los solucionadores de DNS validen que una respuesta de DNS provino de Route 53 y no haya sido manipulada.

El firewall DNS de Route 53 Resolver brinda protección para las solicitudes de DNS salientes de su. VPCs Estas solicitudes pasan por Route 53 Resolver para la resolución de nombres de dominio.

Un uso principal de las protecciones de DNS Firewall es ayudar a evitar la filtración de datos DNS. Con DNS Firewall, puede monitorear y controlar los dominios que las aplicaciones pueden consultar. Puede denegar el acceso a los dominios que sabe que son malos y permitir que pasen el resto de las consultas. También puede denegar el acceso a todos los dominios, excepto a aquellos en los que confía explícitamente. También puede utilizar DNS Firewall para bloquear las solicitudes de resolución a los recursos de zonas alojadas privadas (compartidas o locales), incluidos los nombres de los puntos de conexión de VPC. También puede bloquear las solicitudes de nombres de EC2 instancias públicas o privadas.

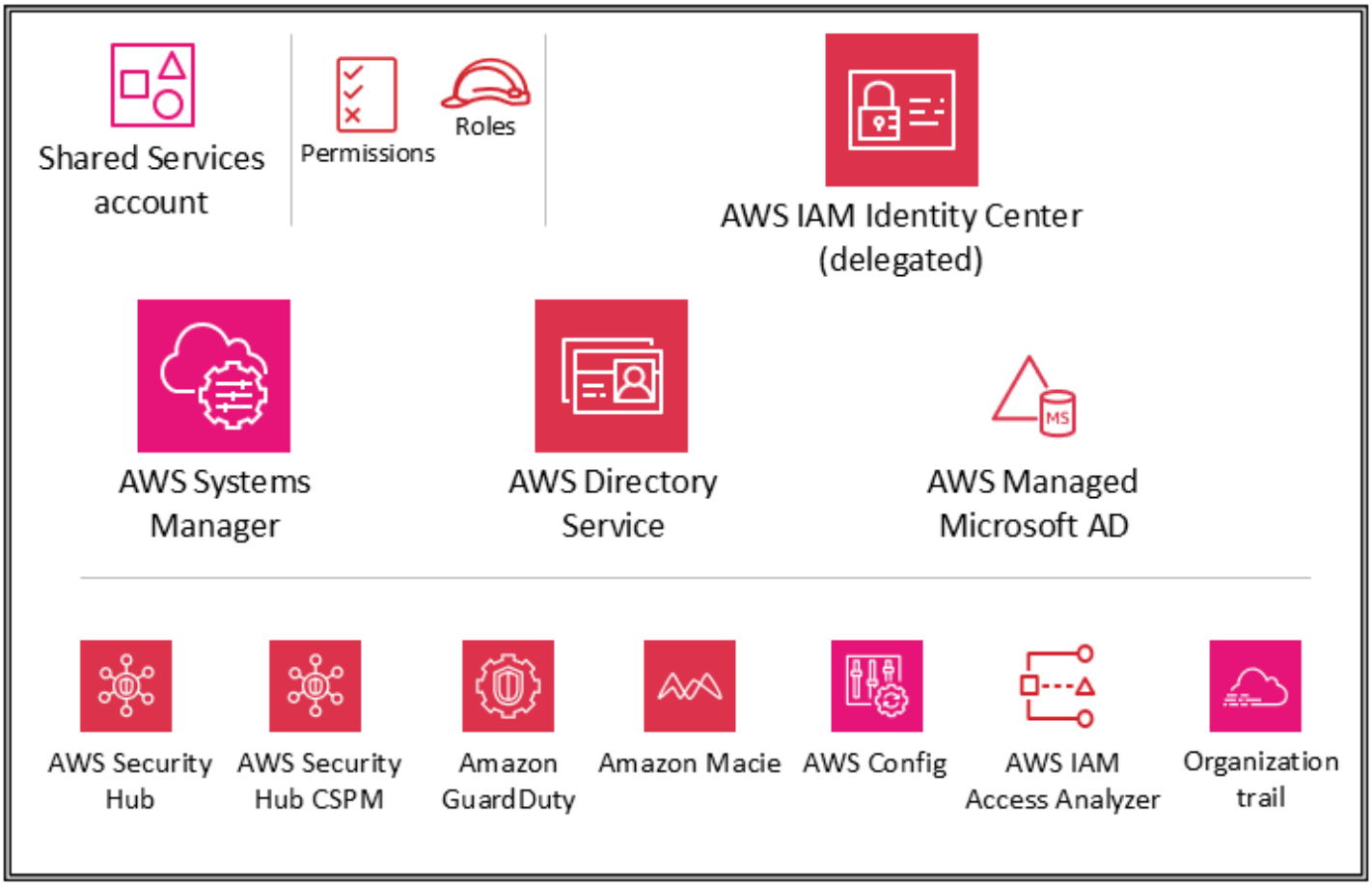
Los solucionadores de Route 53 se crean de forma predeterminada como parte de cada VPC. En la AWS SRA, Route 53 se usa en la cuenta de red principalmente para la función de firewall de DNS.

> **Consideración del diseño**
>
> Tanto el firewall de DNS AWS Network Firewall como ambos ofrecen filtrado de nombres de dominio, pero para distintos tipos de tráfico. Puede usar DNS Firewall y Network Firewall juntos para configurar el filtrado basado en el dominio para el tráfico de la capa de aplicaciones en dos rutas de red diferentes:
>
> - El firewall de DNS filtra las consultas de DNS salientes que pasan por el Route 53 Resolver desde las aplicaciones de su servidor. VPCs También puede configurar DNS Firewall a fin de enviar respuestas personalizadas para las consultas a nombres de dominio bloqueados.
> - Network Firewall proporciona filtrado para el tráfico de la capa de red y de aplicación, pero no tiene visibilidad de las consultas que realiza Route 53 Resolver.

Infrastructure OU: cuenta de servicios compartidos

Influya en el futuro de la arquitectura de referencia de AWS seguridad (AWS SRA) realizando una breve encuesta.

El siguiente diagrama ilustra los servicios AWS de seguridad que están configurados en la cuenta de Shared Services.



La cuenta de servicios compartidos forma parte de la OU de infraestructura y su propósito es respaldar los servicios que utilizan varias aplicaciones y equipos para ofrecer sus resultados. Por ejemplo, los servicios de directorio (Active Directory), los servicios de mensajería y los servicios de metadatos pertenecen a esta categoría. La AWS SRA destaca los servicios compartidos que admiten los controles de seguridad. Si bien las cuentas de red también forman parte de la unidad organizativa de infraestructura, se eliminan de la cuenta de servicios compartidos para facilitar la separación de funciones. Los equipos que administrarán estos servicios no necesitan permisos ni acceso a las cuentas de la red.

AWS Systems Manager

AWS Systems Manager(que también se incluye en la cuenta de administración de la organización y en la cuenta de la aplicación) proporciona un conjunto de funciones que permiten la visibilidad y el control de sus AWS recursos. Una de estas capacidades, Systems Manager Explorer, es un panel de operaciones personalizable que proporciona información sobre sus AWS recursos. Puede sincronizar los datos de operaciones en todas las cuentas de su AWS organización mediante el explorador

AWS Organizations de Systems Manager. Systems Manager se implementa en la cuenta de Shared Services mediante la funcionalidad de administrador delegado de AWS Organizations.

Systems Manager le ayuda a mantener la seguridad y el cumplimiento mediante el análisis de las instancias gestionadas y la notificación (o la adopción de medidas correctivas) sobre cualquier infracción de las políticas que detecte. Al combinar Systems Manager con las implementaciones adecuadas en un miembro individual Cuentas de AWS (por ejemplo, la cuenta de la aplicación), puede coordinar la recopilación de datos de inventario de instancias y centralizar la automatización, como la aplicación de parches y las actualizaciones de seguridad.

AWS Managed Microsoft AD

AWS Directory Service for Microsoft Active Directory, también conocida como AWS Managed Microsoft AD, permite que sus cargas de trabajo y AWS recursos compatibles con directorios utilicen Active Directory administrado en él. AWS Puede utilizar AWS Managed Microsoft AD para unir instancias de Amazon EC2 for Windows Server, Amazon EC2 para Linux y Amazon RDS for SQL Server a su dominio, y AWS utilizar servicios de informática de usuario final (EUC), como WorkSpacesAmazon, con usuarios y grupos de Active Directory.

AWS Managed Microsoft AD le ayuda a ampliar su Active Directory actual AWS y a utilizar sus credenciales de usuario locales existentes para acceder a los recursos en la nube. También puede administrar sus usuarios, grupos, aplicaciones y sistemas locales sin la complejidad de ejecutar y mantener un Active Directory local de alta disponibilidad. Puede unir sus ordenadores, portátiles e impresoras existentes a un AWS Managed Microsoft AD dominio.

AWS Managed Microsoft AD se basa en Microsoft Active Directory y no requiere que sincronice o replique los datos de su Active Directory existente en la nube. Puede utilizar herramientas y funciones de administración de Active Directory que ya conoce, como los objetos de política de grupo (GPOs), las confianzas de dominio, las políticas de contraseñas detalladas, las cuentas de servicios gestionados grupales (gMSAs), las extensiones de esquema y el inicio de sesión único basado en Kerberos. También puede delegar tareas administrativas y autorizar el acceso mediante grupos de seguridad de Active Directory.

La replicación multirregional le permite implementar y usar un único AWS Managed Microsoft AD directorio en varios Regiones de AWS. Esto hace que sea más fácil y rentable implementar y administrar sus cargas de trabajo de Microsoft Windows y Linux en todo el mundo. Cuando utiliza la capacidad de replicación multirregional automatizada, obtiene una mayor resiliencia, mientras que sus aplicaciones utilizan un directorio local para lograr un rendimiento óptimo.

AWS Managed Microsoft AD admite el Protocolo ligero de acceso a directorios (LDAP) sobre SSL/TLS, también conocido como LDAPS, tanto en funciones de cliente como de servidor. Cuando actúa como servidor, AWS Managed Microsoft AD admite el LDAPS a través de los puertos 636 (SSL) y 389 (TLS). Para habilitar las comunicaciones LDAPS del lado del servidor, instale un certificado en los controladores de AWS Managed Microsoft AD dominio procedente de una entidad de certificación (CA) AWS basada en los Servicios de Certificación de Active Directory (AD CS). Cuando actúa como cliente, AWS Managed Microsoft AD admite LDAPS a través de los puertos 636 (SSL). Puede habilitar las comunicaciones LDAPS del lado del cliente registrando los certificados de CA de los emisores de certificados de su servidor y AWS, a continuación, habilitando LDAPS en su directorio.

En la AWS SRA, Directory Service se usa dentro de la cuenta de Shared Services para proporcionar servicios de dominio para cargas de trabajo compatibles con Microsoft en varias cuentas de miembros. AWS

> **Consideración del diseño**
>
> Puede conceder a sus usuarios de Active Directory locales acceso para iniciar sesión en Consola de administración de AWS y AWS Command Line Interface (AWS CLI) con sus credenciales de Active Directory existentes mediante el Centro de identidades de IAM y seleccionándolo como fuente de identidad. AWS Managed Microsoft AD Esto permite a los usuarios asumir una de las funciones que se les han asignado al iniciar sesión y acceder a los recursos y tomar medidas al respecto de acuerdo con los permisos definidos para la función. Una opción alternativa es utilizarla para AWS Managed Microsoft AD permitir que los usuarios asuman una función de IAM.

IAM Identity Center

La AWS SRA utiliza la función de administrador delegado que permite delegar la mayor parte AWS IAM Identity Center de la administración del IAM Identity Center a la cuenta de Shared Services. Esto ayuda a restringir la cantidad de usuarios que necesitan acceder a la cuenta de administración de la organización. El Centro de Identidad de IAM aún debe estar habilitado en la cuenta de administración de la organización para realizar determinadas tareas, incluida la administración de los conjuntos de permisos que se aprovisionan en la cuenta de administración de la organización.

El motivo principal para utilizar la cuenta de Shared Services como administrador delegado del Centro de Identidad de IAM es la ubicación de Active Directory. Si piensa utilizar Active Directory

como fuente de identidad del IAM Identity Center, tendrá que localizar el directorio en la cuenta de miembro que haya designado como cuenta de administrador delegado del IAM Identity Center. En la AWS SRA, la cuenta de Shared Services se aloja AWS Managed Microsoft AD, por lo que dicha cuenta pasa a ser la administradora delegada del IAM Identity Center.

El Centro de Identidad de IAM admite el registro de una cuenta de un solo miembro como administrador delegado al mismo tiempo. Puede registrar una cuenta de miembro solo si inicia sesión con las credenciales de la cuenta de administración. Para habilitar la delegación, debe tener en cuenta los requisitos previos que figuran en la documentación del Centro de Identidad de IAM. La cuenta de administrador delegado puede realizar la mayoría de las tareas de administración del IAM Identity Center, pero con algunas restricciones, que se indican en la documentación del IAM Identity Center. El acceso a la cuenta de administrador delegado del IAM Identity Center debe estar estrictamente controlado.

Consideraciones sobre el diseño

- Si decide cambiar la fuente de identidad del Centro de Identidad de IAM de cualquier otra fuente a Active Directory, o cambiarla de Active Directory a cualquier otra fuente, el directorio debe residir (ser propiedad de) la cuenta del miembro administrador delegado del Centro de Identidad de IAM, si existe; de lo contrario, debe estar en la cuenta de administración.
- Puede alojarla AWS Managed Microsoft AD en una VPC dedicada en una cuenta diferente y, a continuación, usar AWS Resource Access Manager (AWS RAM) para compartir subredes de esta otra cuenta con la cuenta de administrador delegado. De esta forma, la AWS Managed Microsoft AD instancia se controla en la cuenta de administrador delegado, pero desde la perspectiva de la red actúa como si estuviera desplegada en la VPC de otra cuenta. Esto resulta útil cuando tiene varias AWS Managed Microsoft AD instancias y desea implementarlas localmente en el lugar donde se ejecuta su carga de trabajo, pero administrarlas de forma centralizada a través de una cuenta.
- Si tiene un equipo de identidades dedicado que realiza actividades habituales de administración de identidades y accesos o si tiene requisitos de seguridad estrictos para separar las funciones de administración de identidades de otras funciones de servicios compartidos, puede alojar un equipo dedicado a Cuenta de AWS la administración de identidades. En este escenario, designa esta cuenta como su administradora delegada para el Centro de Identidad de IAM y también aloja su AWS Managed Microsoft AD directorio. Puede lograr el mismo nivel de aislamiento lógico entre sus cargas de trabajo de

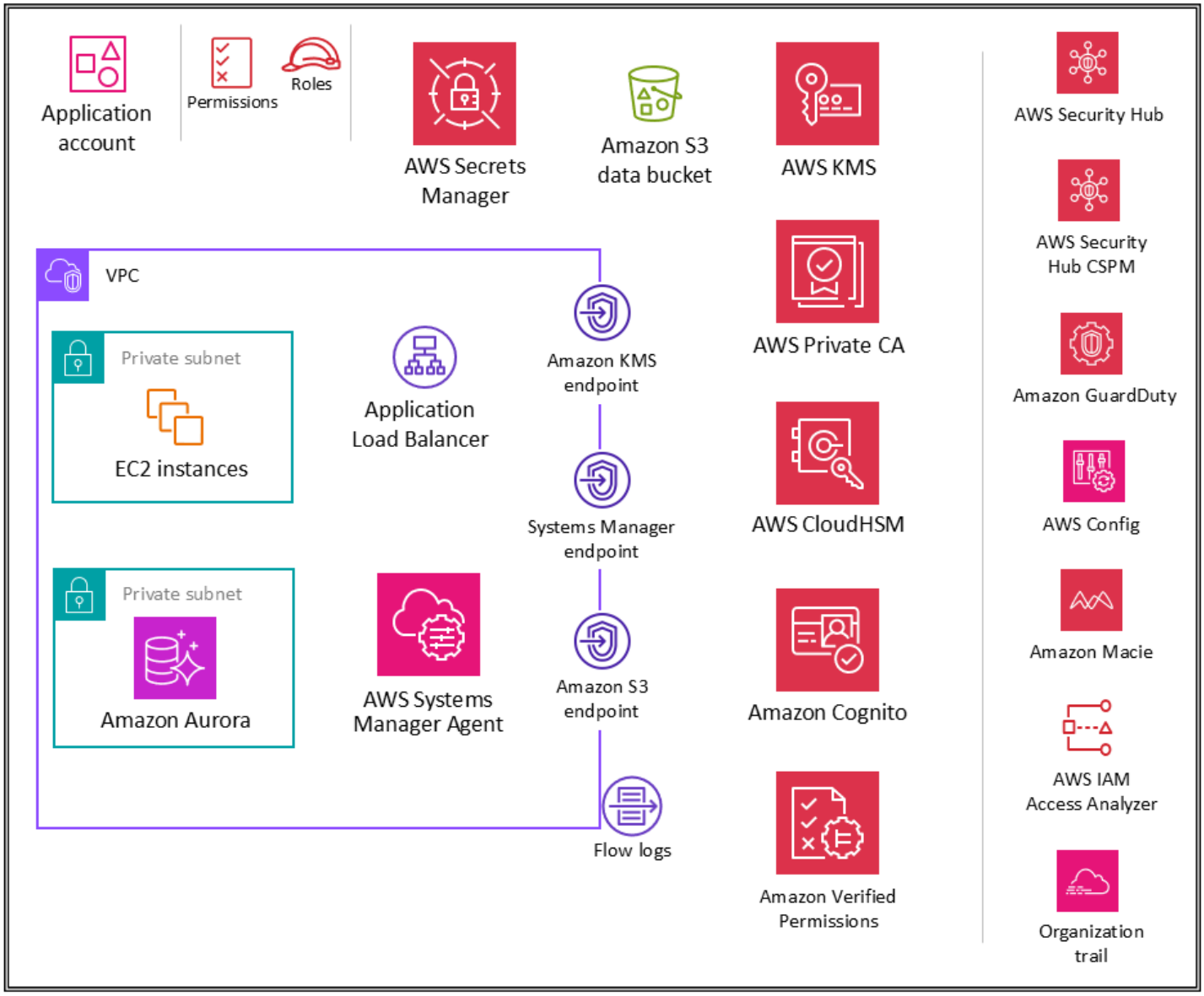
administración de identidades y otras cargas de trabajo de servicios compartidos mediante el uso de permisos de IAM detallados en una sola cuenta de servicio compartido.

- En la actualidad, el IAM Identity Center no ofrece soporte multirregional. (Para habilitar el Centro de Identidad de IAM en una región diferente, primero debe eliminar la configuración actual del Centro de Identidad de IAM). Además, no admite el uso de diferentes fuentes de identidad para diferentes conjuntos de cuentas ni permite delegar la administración de permisos en diferentes partes de la organización (es decir, varios administradores delegados) o en diferentes grupos de administradores. Si necesita alguna de estas funciones, puede usar la federación de IAM para administrar sus identidades de usuario dentro de un proveedor de identidades (IdP) externo y conceder permiso a estas identidades AWS de usuarios externos para AWS usar los recursos de su cuenta. Soportes de IAM IdPs compatibles con OpenID Connect (OIDC) o SAML 2.0. Como práctica recomendada, utilice la federación de SAML 2.0 con proveedores de identidad de terceros, como Active Directory Federation Service (AD FS), Okta, Azure Active Directory (Azure AD) o Ping Identity, para ofrecer a los usuarios la función de inicio de sesión único que les permita iniciar sesión en las operaciones de la API o realizar llamadas a ellas. Consola de administración de AWS AWS Para obtener más información sobre los proveedores de identidad y federación de IAM, consulte Acerca de la federación basada en SAML 2.0 en la documentación de IAM.

Workloads OU: cuenta de aplicación

Influya en el futuro de la arquitectura de referencia de AWS seguridad (AWS SRA) realizando una breve encuesta.

El siguiente diagrama ilustra los servicios AWS de seguridad que están configurados en la cuenta de la aplicación (junto con la propia aplicación).



La cuenta de aplicación aloja la infraestructura y los servicios principales para ejecutar y mantener una aplicación empresarial. La cuenta de aplicación y la unidad organizativa Workloads cumplen algunos objetivos de seguridad principales. En primer lugar, debe crear una cuenta independiente para cada aplicación a fin de establecer límites y controles entre las cargas de trabajo y evitar problemas relacionados con la combinación de funciones, permisos, datos y claves de cifrado. Desea proporcionar un contenedor de cuentas independiente en el que el equipo de aplicaciones pueda disponer de amplios derechos para gestionar su propia infraestructura sin que ello afecte a los demás. A continuación, añada un nivel de protección al proporcionar un mecanismo para que el equipo de operaciones de seguridad supervise y recopile los datos de seguridad. Utilice un registro organizativo y despliegues locales de los servicios de seguridad de cuentas (Amazon GuardDuty

AWS Config, AWS Security Hub CSPM, Amazon EventBridge, IAM Access Analyzer), configurados y supervisados por el equipo de seguridad. Por último, permite a su empresa establecer los controles de forma centralizada. Para alinear la cuenta de la aplicación con la estructura de seguridad más amplia, se convierte en miembro de la unidad organizativa Workloads, a través de la cual hereda los permisos de servicio, las restricciones y las barreras de protección adecuados.

> **Consideración del diseño**
>
> En su organización, es probable que tenga más de una aplicación empresarial. La OU Workloads está diseñada para albergar la mayoría de las cargas de trabajo específicas de su empresa, incluidos los entornos de producción y no producción. Estas cargas de trabajo pueden ser una combinación de aplicaciones comerciales off-the-shelf (COTS) y sus propias aplicaciones y servicios de datos personalizados desarrollados internamente. Existen pocos patrones para organizar las diferentes aplicaciones empresariales junto con sus entornos de desarrollo. Un patrón consiste en tener varios elementos secundarios en OUs función del entorno de desarrollo, como los de producción, puesta en escena, pruebas y desarrollo, y utilizar elementos secundarios separados para Cuentas de AWS los OUs que pertenezcan a distintas aplicaciones. Otro patrón común es tener un elemento secundario diferente para OUs cada aplicación y, a continuación, utilizar un elemento secundario diferente Cuentas de AWS para los entornos de desarrollo individuales. La estructura exacta de la unidad organizativa y la estructura contable dependen del diseño de la aplicación y de los equipos que gestionen esas aplicaciones. Tenga en cuenta los controles de seguridad que desea aplicar, ya sean específicos del entorno o de la aplicación, ya que es más fácil implementar esos controles a medida que avanzan. SCPs OUs Para obtener más información sobre la organización orientada a las cargas de trabajo OUs, consulte la OUs sección Aplicaciones del documento AWS técnico Cómo organizar el entorno mediante varias cuentas. AWS

Aplicación VPC

La nube privada virtual (VPC) de la cuenta de la aplicación necesita acceso entrante (para los servicios web simples que está modelando) y acceso saliente (para las necesidades o necesidades de la aplicación). Servicio de AWS De forma predeterminada, los recursos de una VPC se pueden enrutar entre sí. Hay dos subredes privadas: una para alojar las EC2 instancias (capa de aplicación) y otra para Amazon Aurora (capa de base de datos). La segmentación de la red entre diferentes niveles, como el nivel de aplicación y el nivel de base de datos, se logra mediante grupos de

seguridad de VPC, que restringen el tráfico a nivel de instancia. Para garantizar la resiliencia, la carga de trabajo abarca dos o más zonas de disponibilidad y utiliza dos subredes por zona.

> **Consideración del diseño**
>
> Puede usar Traffic Mirroring para copiar el tráfico de red desde una interfaz de red elástica de EC2 instancias. A continuación, puede enviar el tráfico a los dispositivos out-of-band de seguridad y supervisión para inspeccionar el contenido, supervisar las amenazas o solucionar problemas. Por ejemplo, es posible que desee supervisar el tráfico que sale de la VPC o el tráfico cuyo origen está fuera de la VPC. En este caso, reflejará todo el tráfico, excepto el tráfico que pasa dentro de su VPC, y lo enviará a un único dispositivo de supervisión. Los registros de flujo de Amazon VPC no capturan el tráfico reflejado; por lo general, solo capturan información de los encabezados de los paquetes. La duplicación del tráfico proporciona una visión más profunda del tráfico de la red al permitirle analizar el contenido real del tráfico, incluida la carga útil. Habilite la duplicación de tráfico solo para la interfaz de red elástica de las EC2 instancias que puedan estar funcionando como parte de cargas de trabajo confidenciales o para las que espere necesitar un diagnóstico detallado en caso de que se produzca un problema.

Puntos de conexión de VPC

Los puntos finales de VPC proporcionan otro nivel de control de seguridad, además de escalabilidad y confiabilidad. Úselos para conectar la VPC de su aplicación a otra. Servicios de AWS(En la cuenta de aplicación, la AWS SRA emplea puntos de enlace de VPC AWS KMS para AWS Systems Manager Amazon S3 y Amazon S3). Los puntos de conexión son dispositivos virtuales. Son componentes de VPC escalados horizontalmente, redundantes y de alta disponibilidad. Permiten la comunicación entre instancias de su VPC y servicios sin imponer riesgos de disponibilidad o restricciones de ancho de banda en el tráfico de red. Puede usar un punto de enlace de VPC para conectar de forma privada su VPC a los servicios de punto final de Servicios de AWS VPC compatibles y con tecnología AWS PrivateLink sin necesidad de una puerta de enlace a Internet, un dispositivo NAT, una conexión VPN o una conexión. AWS Direct Connect Las instancias de su VPC no requieren direcciones IP públicas para comunicarse con otras. Servicios de AWS El tráfico entre tu VPC y la otra Servicio de AWS no sale de la red de Amazon.

Otra ventaja del uso de puntos de enlace de VPC es permitir la configuración de políticas de puntos de conexión. Una política de punto de conexión de VPC es una política de recursos de IAM que

puede asociar a un punto de conexión cuando crea o modifica el punto de conexión. Si no adjuntas una política de IAM al crear un punto final, AWS adjunta una política de IAM predeterminada que te permita un acceso total al servicio. Una política de punto de enlace no invalida ni reemplaza las políticas de usuario de IAM ni las políticas específicas de servicios (como las políticas de bucket de S3). Se trata de una política de IAM independiente para controlar el acceso desde el punto final al servicio especificado. De esta forma, añade otro nivel de control sobre el cual AWS los principales pueden comunicarse con los recursos o servicios.

Amazon EC2

Las EC2 instancias de Amazon que componen nuestra aplicación utilizan la versión 2 del Instance Metadata Service (IMDSv2). IMDSv2 añade protecciones para cuatro tipos de vulnerabilidades que podrían utilizarse para intentar acceder al IMDS: firewalls de aplicaciones web, proxies inversos abiertos, vulnerabilidades de falsificación de solicitudes del lado del servidor (SSRF), firewalls abiertos de capa 3 y. NATs Para obtener más información, consulte la entrada del blog Mejore la protección contra los firewalls abiertos, los proxies inversos y las vulnerabilidades de la SSRF con mejoras en el servicio de metadatos de instancias. EC2

Úselo por separado VPCs (como subconjunto de los límites de las cuentas) para aislar la infraestructura por segmentos de carga de trabajo. Utilice subredes para aislar los niveles de la aplicación (por ejemplo, web, aplicación y base de datos) en una VPC individual. Utilice subredes privadas para las instancias si no se debe acceder a ellas directamente desde Internet. Para llamar a la EC2 API de Amazon desde tu subred privada sin usar una puerta de enlace de Internet, usa AWS PrivateLink. Restrinja el acceso a sus instancias mediante grupos de seguridad. Usa los registros de flujo de VPC para monitorear el tráfico que llega a tus instancias. Usa el administrador de sesiones, una funcionalidad que ofrece AWS Systems Manager, para acceder a tus instancias de forma remota, en lugar de abrir los puertos SSH entrantes y administrar las claves SSH. Utilice volúmenes independientes de Amazon Elastic Block Store (Amazon EBS) para el sistema operativo y los datos. Puede configurarlos Cuenta de AWS para aplicar el cifrado de los nuevos volúmenes y copias instantáneas de EBS que cree.

> **Ejemplo de implementación**
>
> La biblioteca de códigos AWS SRA proporciona un ejemplo de implementación del cifrado Amazon EBS predeterminado en Amazon. EC2 Demuestra cómo puede habilitar el cifrado de Amazon EBS predeterminado a nivel de cuenta en cada una de ellas Cuenta de AWS y Región de AWS en la organización. AWS

AWS Nitro Enclaves

AWS Nitro Enclaves es una EC2 función de Amazon que permite crear entornos de ejecución aislados, denominados enclaves, a partir de instancias. EC2 Los enclaves son máquinas virtuales independientes, reforzadas y altamente restringidas. La CPU y la memoria de una sola EC2 instancia principal se dividen en enclaves aislados. Cada enclave ejecuta un núcleo independiente. Los enclaves solo proporcionan una conectividad segura de sockets locales con su instancia principal. No tienen almacenamiento persistente, acceso interactivo ni red externa. Los usuarios no pueden usar SSH en un enclave y los procesos, las aplicaciones o los usuarios (root o administrador) de la instancia principal no pueden acceder a los datos y las aplicaciones que se encuentran dentro del enclave. Puede proteger sus datos más confidenciales, como la información de identificación personal (PII) y los datos de salud, financieros y de propiedad intelectual, dentro EC2 de unas cuantas instancias. Nitro Enclaves le permite centrarse en su aplicación en lugar de preocuparse por la integración con servicios externos. Nitro Enclaves incluye una certificación criptográfica para su software, de modo que puede estar seguro de que solo se está ejecutando el código autorizado, y la integración con el software para que solo sus enclaves AWS KMS puedan acceder a material confidencial. Esto ayuda a reducir la superficie de ataque de sus aplicaciones de procesamiento de datos más confidenciales. El uso de Nitro Enclaves no conlleva ningún coste adicional.

La certificación criptográfica es un proceso que se utiliza para probar la identidad de un enclave. El proceso de certificación se lleva a cabo a través del Hypervisor Nitro, que produce un documento de certificación firmado para que el enclave demuestre su identidad a otro tercero o servicio. Los documentos de certificación contienen detalles clave del enclave, como la clave pública del enclave, los códigos hash de la imagen y las aplicaciones del enclave, etc.

Con AWS Certificate Manager (ACM) para Nitro Enclaves, puede utilizar certificados públicos y privados. SSL/TLS certificates with your web applications and web servers running on EC2 instances with Nitro Enclaves. SSL/TLS certificates are used to secure network communications and to establish the identity of websites over the internet and resources on private networks. ACM for Nitro Enclaves removes the time-consuming and error-prone manual process of purchasing, uploading, and renewing SSL/TLS ACM for Nitro Enclaves crea claves privadas seguras, distribuye el certificado y su clave privada en su enclave y gestiona las renovaciones de los certificados. Con ACM para Nitro Enclaves, la clave privada del certificado permanece aislada en el enclave, lo que impide que la instancia y sus usuarios accedan a ella. Para obtener más información, consulte AWS Certificate Manager la sección sobre Nitro Enclaves en la documentación de Nitro Enclaves.

Equilibrador de carga de aplicación

Los balanceadores de carga de aplicaciones distribuyen el tráfico de aplicaciones entrante entre varios destinos, como EC2 instancias, en varias zonas de disponibilidad. En la AWS SRA, el grupo objetivo del equilibrador de carga son las instancias de la aplicación. EC2 La AWS SRA utiliza agentes de escucha HTTPS para garantizar que el canal de comunicación esté cifrado. El Application Load Balancer utiliza un certificado de servidor para finalizar la conexión front-end y, a continuación, para descifrar las solicitudes de los clientes antes de enviarlas a los destinos.

AWS Certificate Manager (ACM) se integra de forma nativa con los balanceadores de carga de aplicaciones, y la AWS SRA usa el ACM para generar y administrar los certificados públicos X.509 (servidor TLS) necesarios. Puede aplicar TLS 1.2 y cifrados seguros para las conexiones front-end mediante la política de seguridad de Application Load Balancer. Para obtener más información, consulte la Documentación de Elastic Load Balancing.

Consideraciones sobre el diseño

- Para situaciones comunes, como aplicaciones estrictamente internas que requieren un certificado TLS privado en el Application Load Balancer, puede usar ACM en esta cuenta para generar un certificado privado desde. AWS Private CAEn la AWS SRA, la CA privada raíz de ACM está alojada en la cuenta de Security Tooling y se puede compartir con toda la AWS organización o con una entidad específica Cuentas de AWS para emitir certificados de entidad final, tal y como se ha descrito anteriormente en la sección de cuentas de Security Tooling.
- En el caso de los certificados públicos, puede utilizar ACM para generarlos y gestionarlos, incluida la rotación automática. Como alternativa, puede generar sus propios certificados mediante SSL/TLS herramientas para crear una solicitud de firma de certificado (CSR), conseguir que una entidad de certificación (CA) firme la CSR para producir un certificado y, a continuación, importar el certificado a ACM o cargar el certificado en IAM para usarlo con Application Load Balancer. Si importa un certificado a ACM, debe controlar la fecha de caducidad del certificado y renovarlo antes de que caduque.
- Para niveles de defensa adicionales, puede implementar AWS WAF políticas para proteger el Application Load Balancer. Contar con políticas periféricas, políticas de aplicaciones e incluso capas de aplicación de políticas privadas o internas aumenta la visibilidad de las solicitudes de comunicación y proporciona una aplicación unificada de las políticas. Para

obtener más información, consulte la entrada del blog Deplying defense in depth using Reglas administradas de AWS for AWS WAF.

AWS Private CA

AWS Private Certificate Authority(AWS Private CA) se usa en la cuenta de la aplicación para generar certificados privados que se utilizarán con un Application Load Balancer. Es habitual que los balanceadores de carga de aplicaciones ofrezcan contenido seguro a través de TLS. Esto requiere que los certificados TLS estén instalados en Application Load Balancer. Para las aplicaciones que son estrictamente internas, los certificados TLS privados pueden proporcionar el canal seguro.

En la AWS SRA, AWS Private CA se aloja en la cuenta de Security Tooling y se comparte con la cuenta de la aplicación mediante el uso de. AWS RAM Esto permite a los desarrolladores de una cuenta de aplicación solicitar un certificado a una entidad emisora de certificados privada compartida. El hecho de compartir información CAs en toda la organización o entre ellas Cuentas de AWS ayuda a reducir el coste y la complejidad de crear y gestionar los duplicados CAs en todos sus ámbitos Cuentas de AWS. Cuando utiliza ACM para emitir certificados privados desde una entidad de certificación compartida, el certificado se genera localmente en la cuenta solicitante y ACM proporciona una gestión y renovación completas del ciclo de vida.

Amazon Inspector

La AWS SRA utiliza Amazon Inspector para detectar y escanear automáticamente las EC2 instancias y las imágenes de contenedores que se encuentran en el Amazon Elastic Container Registry (Amazon ECR) para detectar vulnerabilidades de software y exposiciones no intencionadas en la red.

Amazon Inspector se coloca en la cuenta de la aplicación porque proporciona servicios de gestión de vulnerabilidades a EC2 las instancias de esta cuenta. Además, Amazon Inspector informa sobre las rutas de red no deseadas hacia y desde EC2 las instancias.

Amazon Inspector en las cuentas de los miembros se gestiona de forma centralizada mediante la cuenta de administrador delegado. En la AWS SRA, la cuenta Security Tooling es la cuenta de administrador delegado. La cuenta de administrador delegado puede gestionar las conclusiones, los datos y determinados ajustes de los miembros de la organización. Esto incluye ver los detalles agregados de las conclusiones de todas las cuentas de los miembros, habilitar o deshabilitar los escaneos de las cuentas de los miembros y revisar los recursos escaneados dentro de la AWS organización.

> **Consideración del diseño**
>
> Puede utilizar el Administrador de parches, una función de AWS Systems Manager, para activar la aplicación de parches bajo demanda y corregir las vulnerabilidades de seguridad críticas de Amazon Inspector o de otro tipo. Patch Manager le ayuda a corregir esas vulnerabilidades sin tener que esperar a que se aplique el programa habitual de parches. La corrección se lleva a cabo mediante el manual de automatización de Systems Manager. Para obtener más información, consulte la serie de blogs de dos partes Automatice la gestión y la corrección de vulnerabilidades AWS con Amazon Inspector y. AWS Systems Manager

AWS Systems Manager

AWS Systems Manageres una herramienta Servicio de AWS que puede utilizar para ver los datos operativos de varios recursos Servicios de AWS y automatizar las tareas operativas en todos sus AWS recursos. Con flujos de trabajo y manuales de aprobación automatizados, puede trabajar para reducir los errores humanos y simplificar las tareas de mantenimiento e implementación de los AWS recursos.

Además de estas capacidades generales de automatización, Systems Manager admite una serie de funciones de seguridad preventivas, de detección y con capacidad de respuesta.AWS Systems Manager El agente (SSM Agent) es un software de Amazon que se puede instalar y configurar en una EC2 instancia, un servidor local o una máquina virtual (VM). El SSM Agent posibilita que Systems Manager actualice, administre y configure estos recursos. Systems Manager le ayuda a mantener la seguridad y el cumplimiento mediante el análisis de estas instancias gestionadas y la notificación (o la adopción de medidas correctivas) sobre cualquier infracción que detecte en sus políticas de parches, configuración y personalizadas.

La AWS SRA utiliza Session Manager, una capacidad de Systems Manager, para proporcionar una experiencia de CLI y shell interactiva y basada en navegador. Esto proporciona una administración de instancias segura y auditable sin necesidad de abrir los puertos de entrada, mantener los hosts bastiones ni administrar las claves SSH. La AWS SRA utiliza Patch Manager, una función de Systems Manager, para aplicar parches a las EC2 instancias tanto de los sistemas operativos como de las aplicaciones.

La AWS SRA también utiliza la automatización, una capacidad de Systems Manager, para simplificar las tareas comunes de mantenimiento e implementación de las EC2 instancias de Amazon y otros

AWS recursos. Automation puede simplificar tareas de TI habituales, como cambiar el estado de uno o más nodos (mediante la automatización de la aprobación) y administrar los estados de los nodos de acuerdo con una programación. Systems Manager incluye características que lo ayudan a indicar grupos grandes de instancias como destino mediante el uso de etiquetas, así como controles de velocidad que le permitan implementar cambios de acuerdo con los límites que defina. La automatización ofrece automatizaciones con un solo clic para simplificar tareas complejas, como la creación de Amazon Machine Images (AMIs) de gran calidad y la recuperación de instancias inalcanzables. EC2 Además, puede mejorar la seguridad operativa dando a los roles de IAM acceso a manuales específicos para realizar determinadas funciones, sin necesidad de conceder permisos directos a esos roles. Por ejemplo, si quieres que un rol de IAM tenga permisos para reiniciar EC2 instancias específicas tras la actualización de los parches, pero no quieres conceder el permiso directamente a ese rol, puedes crear un manual de automatización y conceder permisos al rol para que solo ejecute el runbook.

Consideraciones sobre el diseño

- Systems Manager se basa en los metadatos de la EC2 instancia para funcionar correctamente. Systems Manager puede acceder a los metadatos de la instancia mediante la versión 1 o la versión 2 del Servicio de metadatos de la instancia (IMDSv1 y IMDSv2).
- El agente SSM debe comunicarse con diferentes Servicios de AWS recursos, como Amazon EC2 Messages, Systems Manager y Amazon S3. Para que se produzca esta comunicación, la subred requiere conectividad a Internet saliente o el aprovisionamiento de los puntos finales de VPC adecuados. La AWS SRA utiliza puntos finales de VPC para que el agente SSM establezca rutas de red privadas a varias. Servicios de AWS
- Con Automation, puede compartir las prácticas recomendadas con los demás miembros de su organización. Puede crear las mejores prácticas para la administración de recursos en los manuales de ejecución y compartirlos entre grupos. Regiones de AWS También puede restringir los valores permitidos para los parámetros del runbook. Para estos casos de uso, puede que tengas que crear manuales de automatización en una cuenta central, como Security Tooling o Shared Services, y compartirlos con el resto de la organización. AWS Los casos de uso más comunes incluyen la capacidad de implementar parches y actualizaciones de seguridad de forma centralizada, corregir las desviaciones en las configuraciones de VPC o las políticas de bucket de S3 y administrar EC2 las instancias a escala. Para obtener detalles sobre la implementación, consulte la documentación de Systems Manager.

Amazon Aurora

En la AWS SRA, Amazon Aurora y Amazon S3 forman el nivel de datos lógico. Aurora es un motor de base de datos relacional completamente administrado compatible con MySQL y PostgreSQL. Una aplicación que se ejecuta en las EC2 instancias se comunica con Aurora y Amazon S3 según sea necesario. Aurora se configura con un clúster de base de datos dentro de un grupo de subredes de base de datos.

> **Consideración del diseño**
>
> Como en muchos servicios de bases de datos, la seguridad de Aurora se administra en tres niveles. Para controlar quién puede realizar acciones de administración de Amazon Relational Database Service (Amazon RDS) en clústeres e instancias de base de datos Aurora, utilice IAM. Para controlar qué dispositivos e EC2 instancias pueden abrir conexiones al punto final del clúster y al puerto de la instancia de base de datos para los clústeres de base de datos Aurora en una VPC, utilice un grupo de seguridad de VPC. Para autenticar los inicios de sesión y los permisos de un clúster de base de datos Aurora, puede adoptar el mismo enfoque que con una instancia de base de datos independiente de MySQL o PostgreSQL, o puede utilizar la autenticación de bases de datos de IAM para Aurora MySQL Compatible Edition. Con este último enfoque, se autentica en su clúster de base de datos compatible con Aurora MySQL mediante un rol de IAM y un token de autenticación.

Amazon S3

Amazon S3 es un servicio de almacenamiento de objetos que ofrece escalabilidad, disponibilidad de datos, seguridad y rendimiento líderes del sector. Es la columna vertebral de datos de muchas aplicaciones integradas AWS, y los permisos y controles de seguridad adecuados son fundamentales para proteger los datos confidenciales. Para obtener información sobre las prácticas recomendadas de seguridad para Amazon S3, consulte la documentación, las charlas técnicas en línea y las publicaciones de blog más detalladas. La mejor práctica más importante es bloquear el acceso excesivamente permisivo (especialmente el acceso público) a los buckets de S3.

AWS KMS

La AWS SRA ilustra el modelo de distribución recomendado para la administración de claves, en el que AWS KMS key residen en el mismo lugar que el recurso que Cuenta de AWS se va a cifrar. Por

este motivo, AWS KMS se utiliza en la cuenta de la aplicación además de estar incluido en la cuenta de herramientas de seguridad. En la cuenta de la aplicación, AWS KMS se usa para administrar las claves que son específicas de los recursos de la aplicación. Puede establecer una separación de funciones mediante políticas clave para conceder permisos de uso de las claves a las funciones de las aplicaciones locales y restringir los permisos de administración y supervisión a los custodios de las claves.

> **Consideración del diseño**
>
> En un modelo distribuido, la responsabilidad AWS KMS clave de la administración recae en el equipo de aplicaciones. Sin embargo, su equipo de seguridad central puede ser responsable del gobierno y la supervisión de eventos criptográficos importantes, como los siguientes:
>
> - El material clave importado de una clave KMS se acerca a su fecha de vencimiento.
> - El material clave de una clave KMS se rotó automáticamente.
> - Se ha eliminado la clave AKMS.
> - Hay una alta tasa de errores de descifrado.

AWS CloudHSM

AWS CloudHSMproporciona módulos de seguridad de hardware gestionados (HSMs) en. Nube de AWS Le permite generar y utilizar sus propias claves de cifrado AWS mediante el FIPS 140-2 de nivel 3 validado y al HSMs que usted controla el acceso. Puede utilizarla AWS CloudHSM para reducir la carga de SSL/TLS procesamiento de sus servidores web. Esto reduce la carga del servidor web y proporciona seguridad adicional al almacenar la clave privada del servidor web. AWS CloudHSM Del mismo modo, puede implementar un HSM desde AWS CloudHSM la VPC entrante de la cuenta de red para almacenar sus claves privadas y firmar las solicitudes de certificado si necesita actuar como autoridad de certificación emisora.

> **Consideración del diseño**
>
> Si tiene requisitos estrictos para el nivel 3 de FIPS 140-2, también puede optar por configurarlo AWS KMS para usar el AWS CloudHSM clúster como almacén de claves personalizado en lugar de usar el almacén de claves de KMS nativo. De este modo, se beneficia de la integración entre los sistemas Servicios de AWS que cifran sus datos AWS

KMS y, al mismo tiempo, es responsable de proteger sus claves de HSMs KMS. Esto combina un único propietario HSMs bajo su control con la facilidad de uso e integración de. AWS KMS Para administrar su AWS CloudHSM infraestructura, debe emplear una infraestructura de clave pública (PKI) y contar con un equipo con experiencia en la administración. HSMs

AWS Secrets Manager

AWS Secrets Managerle ayuda a proteger las credenciales (secretos) que necesita para acceder a sus aplicaciones, servicios y recursos de TI. El servicio le permite rotar, administrar y recuperar de manera eficiente las credenciales de las bases de datos, las claves de API y otros datos secretos a lo largo de su ciclo de vida. Puedes sustituir las credenciales codificadas de tu código por una llamada a la API a Secrets Manager para recuperar el secreto mediante programación. Esto ayuda a garantizar que alguien que esté examinando tu código no pueda comprometer el secreto, ya que el secreto ya no existe en el código. Además, Secrets Manager le ayuda a mover sus aplicaciones entre entornos (desarrollo, preproducción, producción). En lugar de cambiar el código, puede asegurarse de que en el entorno esté disponible un secreto con el nombre y la referencia adecuados. Esto promueve la coherencia y la reutilización del código de la aplicación en diferentes entornos y, al mismo tiempo, requiere menos cambios e interacciones humanas una vez probado el código.

Con Secrets Manager, puede gestionar el acceso a los secretos mediante políticas de IAM detalladas y políticas basadas en recursos. Puede ayudar a proteger los secretos cifrándolos con claves de cifrado que puede administrar mediante el uso. AWS KMS Secrets Manager también se integra con los servicios de AWS registro y supervisión para una auditoría centralizada.

Secrets Manager utiliza el cifrado de sobres con AWS KMS keys claves de datos para proteger cada valor secreto. Al crear un secreto, puede elegir cualquier clave simétrica gestionada por el cliente en la región Cuenta de AWS y, si lo prefiere, puede utilizar la clave AWS gestionada para Secrets Manager.

Como práctica recomendada, puedes supervisar tus datos secretos para registrar cualquier cambio que se produzca en ellos. Esto le ayuda a garantizar que se pueda investigar cualquier uso o cambio inesperado. Los cambios no deseados se pueden revertir. Secrets Manager admite actualmente dos Servicios de AWS que le permiten monitorear su organización y actividad: AWS CloudTrail y AWS Config. CloudTrail captura todas las llamadas a la API de Secrets Manager como eventos, incluidas las llamadas desde la consola de Secrets Manager y las llamadas en código a Secrets Manager

APIs. Además, CloudTrail captura otros eventos relacionados (ajenos a la API) que podrían afectar a la seguridad o el cumplimiento de normas Cuenta de AWS o que podrían ayudarle a solucionar problemas operativos. Entre ellos se incluyen determinados eventos de rotación de secretos y la eliminación de versiones secretas. AWS Config puede proporcionar controles detectivescos mediante el seguimiento y la supervisión de los cambios en los secretos de Secrets Manager. Estos cambios incluyen la descripción de un secreto, la configuración de rotación, las etiquetas y la relación con otras AWS fuentes, como la clave de cifrado KMS o las AWS Lambda funciones utilizadas para la rotación del secreto. También puede configurar Amazon EventBridge, que recibe notificaciones de cambios en la configuración y la conformidad AWS Config, para que enrute eventos secretos específicos para que se adopten medidas de notificación o corrección.

En la AWS SRA, Secrets Manager se encuentra en la cuenta de la aplicación para respaldar los casos de uso de aplicaciones locales y administrar los secretos cercanos a su uso. Aquí, se adjunta un perfil de instancia a las EC2 instancias de la cuenta de la aplicación. Luego, se pueden configurar secretos separados en Secrets Manager para permitir que ese perfil de instancia recupere secretos; por ejemplo, para unirse al dominio de Active Directory o LDAP correspondiente y acceder a la base de datos Aurora. Secrets Manager se integra con Amazon RDS para administrar las credenciales de los usuarios al crear, modificar o restaurar una instancia de base de datos de Amazon RDS o un clúster de base de datos Multi-AZ. Esto le ayuda a gestionar la creación y rotación de claves y sustituye las credenciales codificadas de su código por llamadas programáticas a la API a Secrets Manager.

> **Consideración del diseño**
>
> En general, configure y administre Secrets Manager en la cuenta que esté más cerca de donde se usarán los secretos. Este enfoque aprovecha el conocimiento local del caso de uso y proporciona velocidad y flexibilidad a los equipos de desarrollo de aplicaciones. En el caso de información estrictamente controlada en la que pueda resultar adecuado un nivel de control adicional, Secrets Manager puede gestionar los secretos de forma centralizada en la cuenta de Security Tooling.

Amazon Cognito

Amazon Cognito le permite añadir el registro, el inicio de sesión y el control de acceso de los usuarios a sus aplicaciones web y móviles de forma rápida y eficaz. Amazon Cognito se amplía a millones de usuarios y admite el inicio de sesión con proveedores de identidad social, como Apple,

Facebook, Google y Amazon, y con proveedores de identidad empresarial mediante SAML 2.0 y OpenID Connect. Los dos componentes principales de Amazon Cognito son los grupos de usuarios y los grupos de identidades. Los grupos de usuarios son directorios de usuarios que proporcionan opciones de registro e inicio de sesión para los usuarios de la aplicación. Los grupos de identidades le permiten conceder a sus usuarios acceso a otros. Servicios de AWS Puede utilizar los grupos de identidades y los grupos de usuarios juntos o por separado. Para ver los escenarios de uso más comunes, consulte la documentación de Amazon Cognito.

Amazon Cognito proporciona una interfaz de usuario integrada y personalizable para el registro e inicio de sesión de los usuarios. Puede usar Android, iOS y Amazon Cognito JavaScript SDKs para añadir páginas de registro e inicio de sesión de usuarios a sus aplicaciones. Amazon Cognito Sync es una Servicio de AWS biblioteca de clientes que permite la sincronización entre dispositivos de los datos de usuario relacionados con la aplicación.

Amazon Cognito admite la autenticación multifactorial y el cifrado de los datos en reposo y en tránsito. Los grupos de usuarios de Amazon Cognito ofrecen funciones de seguridad avanzadas para ayudar a proteger el acceso a las cuentas de usuario de la aplicación. Estas funciones de seguridad avanzadas proporcionan una autenticación adaptativa basada en los riesgos y la protección contra el uso de credenciales comprometidas.

Consideraciones sobre el diseño

- Puede crear una AWS Lambda función y, a continuación, activarla durante las operaciones del grupo de usuarios, como el registro, la confirmación y el inicio de sesión (autenticación) de los usuarios con un activador Lambda. Puede agregar los desafíos de autenticación, migrar usuarios, y personalizar los mensajes de verificación. Para obtener información sobre las operaciones comunes y el flujo de usuarios, consulte la documentación de Amazon Cognito. Amazon Cognito llama a las funciones de Lambda de forma sincrónica.
- Puede usar los grupos de usuarios de Amazon Cognito para proteger aplicaciones pequeñas y de varios inquilinos. Un caso de uso común del diseño multiusuario es ejecutar cargas de trabajo para poder probar varias versiones de una aplicación. El diseño de varios inquilinos también es útil para probar una sola aplicación con diferentes conjuntos de datos, lo que permite el uso completo de los recursos del clúster. Sin embargo, asegúrese de que el número de inquilinos y el volumen esperado coincidan con las cuotas de servicio de Amazon Cognito correspondientes. Todos los inquilinos de la aplicación las comparten.

Amazon Verified Permissions

Amazon Verified Permissions es un servicio escalable de administración de permisos y autorización detallado para las aplicaciones que cree. Los desarrolladores y administradores pueden usar Cedar, un lenguaje de políticas de código abierto diseñado específicamente y centrado en la seguridad, con funciones y atributos para definir controles de acceso más detallados, sensibles al contexto y basados en políticas. Los desarrolladores pueden crear aplicaciones más seguras con mayor rapidez mediante la externalización de la autorización y la centralización de la gestión y la administración de las políticas. Los permisos verificados incluyen definiciones de esquemas, gramática de las declaraciones de políticas y un razonamiento automatizado que abarca millones de permisos, para que pueda aplicar los principios predeterminados de denegación y mínimo privilegio. El servicio también incluye una herramienta de simulación de evaluación que le ayuda a poner a prueba sus decisiones de autorización y sus políticas de autor. Estas funciones facilitan la implementación de un modelo de autorización exhaustivo y detallado para respaldar sus objetivos de confianza cero. Verified Permissions centraliza los permisos en un almacén de políticas y ayuda a los desarrolladores a utilizarlos para autorizar las acciones de los usuarios en sus aplicaciones.

Puede conectar su aplicación al servicio a través de la API para autorizar las solicitudes de acceso de los usuarios. Para cada solicitud de autorización, el servicio recupera las políticas pertinentes y las evalúa para determinar si un usuario puede realizar una acción en un recurso, en función de las entradas del contexto, como los usuarios, las funciones, la pertenencia a un grupo y los atributos. Puede configurar los permisos verificados y conectarlos a ellos para enviar sus registros de autorización y administración de políticas. AWS CloudTrail Si utiliza Amazon Cognito como almacén de identidades, puede integrarlo con Verified Permissions y utilizar el identificador y los tokens de acceso que Amazon Cognito devuelve en las decisiones de autorización de sus aplicaciones. Usted proporciona los tokens de Amazon Cognito a Verified Permissions, que utiliza los atributos que contienen los tokens para representar al principal e identificar sus derechos. Para obtener más información sobre esta integración, consulte la entrada del AWS blog Cómo simplificar la autorización detallada con Amazon Verified Permissions y Amazon Cognito.

Los permisos verificados le ayudan a definir el control de acceso basado en políticas (PBAC). El PBAC es un modelo de control de acceso que utiliza permisos expresados como políticas para determinar quién puede acceder a qué recursos de una aplicación. El PBAC combina el control de acceso basado en roles (RBAC) y el control de acceso basado en atributos (ABAC), lo que da como resultado un modelo de control de acceso más potente y flexible. Para obtener más información sobre el PBAC y sobre cómo diseñar un modelo de autorización mediante permisos

verificados, consulte la entrada del AWS blog Control de acceso basado en políticas en el desarrollo de aplicaciones con Amazon Verified Permissions.

En la AWS SRA, los permisos verificados se encuentran en la cuenta de la aplicación para facilitar la administración de permisos de las aplicaciones mediante su integración con Amazon Cognito.

Defensa por capas

La cuenta de la aplicación brinda la oportunidad de ilustrar los principios de defensa estratificados que AWS permiten. Tenga en cuenta la seguridad de las EC2 instancias que constituyen el núcleo de una aplicación de ejemplo sencilla representada en la AWS SRA y verá cómo se Servicios de AWS trabaja en conjunto en una defensa por capas. Este enfoque se ajusta a la visión estructural de los servicios de AWS seguridad, tal como se describe en la sección Aplicar los servicios de seguridad en toda la AWS organización, que aparece anteriormente en esta guía.

- La capa más interna son las instancias. EC2 Como se mencionó anteriormente, EC2 las instancias incluyen muchas funciones de seguridad nativas de forma predeterminada o como opciones. Algunos ejemplos incluyen IMDSv2el sistema Nitro y el cifrado de almacenamiento de Amazon EBS.
- La segunda capa de protección se centra en el sistema operativo y el software que se ejecutan en las EC2 instancias. Servicios como Amazon Inspector le AWS Systems Managerpermiten monitorear, informar y tomar medidas correctivas en estas configuraciones. Amazon Inspector supervisa el software en busca de vulnerabilidades y Systems Manager le ayuda a mantener la seguridad y la conformidad mediante el análisis de las instancias gestionadas para comprobar el estado de los parches y la configuración y, a continuación, informar y tomar las medidas correctivas que especifique.
- Las instancias y el software que se ejecuta en ellas forman parte de su infraestructura AWS de red. Además de utilizar las características de seguridad de Amazon VPC, la AWS SRA también utiliza puntos de enlace de la VPC para proporcionar conectividad privada entre la VPC y la compatible Servicios de AWS, y para proporcionar un mecanismo para colocar las políticas de acceso en los límites de la red.
- La actividad y la configuración de las EC2 instancias, el software, la red y las funciones y los recursos de IAM se supervisan aún más mediante Cuenta de AWS servicios específicos AWS Security Hub CSPM, como AWS Security Hub Amazon,, GuardDuty AWS CloudTrail AWS Config, IAM Access Analyzer y Amazon Macie.

- Por último, más allá de la cuenta de la aplicación, AWS RAM ayuda a controlar qué recursos se comparten con otras cuentas, y las políticas de control de los servicios de IAM ayudan a aplicar permisos coherentes en toda la organización. AWS

AI/ML para la seguridad

Influya en el futuro de la arquitectura de referencia de AWS seguridad (AWS SRA) realizando una breve encuesta.

La inteligencia artificial y el aprendizaje automático (Amazon se AI/ML) is transforming businesses. AI/ML ha centrado durante más de 20 años), y muchas de las capacidades que utilizan los clientes AWS, incluidos los servicios de seguridad, están impulsadas por la IA y el aprendizaje automático. Esto crea un valor diferenciado integrado, ya que puede construir sobre él de forma segura AWS sin necesidad de que sus equipos de seguridad o desarrollo de aplicaciones tengan experiencia en inteligencia artificial y aprendizaje automático.

La IA es una tecnología avanzada que permite que las máquinas y los sistemas adquieran capacidades de inteligencia y predicción. Los sistemas de IA aprenden de la experiencia pasada a través de los datos que consumen o con los que se entrenan. El aprendizaje automático es uno de los aspectos más importantes de la IA. El aprendizaje automático es la capacidad de los ordenadores de aprender de los datos sin necesidad de programarlos de forma explícita. En la programación tradicional, el programador escribe reglas que definen cómo debe funcionar el programa en una computadora o máquina. En el aprendizaje automático, el modelo aprende las reglas a partir de los datos. Los modelos de aprendizaje automático pueden descubrir patrones ocultos en los datos o realizar predicciones precisas a partir de nuevos datos que no se utilizaron durante el entrenamiento. Se pueden Servicios de AWS usar varias AI/ML veces para aprender de enormes conjuntos de datos y hacer inferencias de seguridad.

- Amazon Macie es un servicio de seguridad de datos que utiliza el aprendizaje automático y la coincidencia de patrones para detectar y proteger sus datos confidenciales. Macie detecta automáticamente una lista cada vez mayor de tipos de datos confidenciales, que incluye información de identificación personal (PII), como nombres, direcciones e información financiera, como números de tarjetas de crédito. También le proporciona una visibilidad constante de los datos almacenados en Amazon Simple Storage Service (Amazon S3). Macie utiliza modelos de procesamiento del lenguaje natural (NLP) y aprendizaje automático que se entrenan en distintos tipos de conjuntos de datos para comprender los datos existentes y asignar valores empresariales a fin de priorizar los datos esenciales para la empresa. Luego, Macie genera hallazgos de datos confidenciales.

- Amazon GuardDuty es un servicio de detección de amenazas que utiliza el aprendizaje automático, la detección de anomalías y la inteligencia de amenazas integrada para supervisar de forma continua la actividad maliciosa y el comportamiento no autorizado, a fin de proteger sus instancias Cuentas de AWS, cargas de trabajo sin servidor y contenedores, usuarios, bases de datos y almacenamiento. GuardDuty incorpora técnicas de aprendizaje automático que son muy eficaces a la hora de diferenciar entre la actividad potencialmente maliciosa de los usuarios y su comportamiento operativo anómalo pero benigno. Cuentas de AWS Esta capacidad modela continuamente las invocaciones a las API dentro de una cuenta e incorpora predicciones probabilísticas para aislar con mayor precisión el comportamiento altamente sospechoso de los usuarios y alertar sobre ellos. Este enfoque ayuda a identificar las actividades maliciosas asociadas a las tácticas de amenazas conocidas, como la detección, el acceso inicial, la persistencia, la escalada de privilegios, la evasión de la defensa, el acceso a las credenciales, el impacto y la exfiltración de datos. Para obtener más información sobre cómo se GuardDuty utiliza el aprendizaje automático, consulta la sesión temática de AWS Re:inForce 2023 Desarrollando nuevos hallazgos mediante el aprendizaje automático en Amazon GuardDuty (0). TDR31

Seguridad demostrable

AWS desarrolla herramientas de razonamiento automatizadas que utilizan la lógica matemática para responder a preguntas críticas sobre su infraestructura y detectar errores de configuración que podrían exponer sus datos. Esta capacidad se denomina seguridad demostrable porque proporciona una mayor seguridad en la nube y en la nube. La seguridad demostrable utiliza el razonamiento automatizado, que es una disciplina específica de la IA que aplica la deducción lógica a los sistemas informáticos. Por ejemplo, las herramientas de razonamiento automatizado pueden analizar las políticas y las configuraciones de la arquitectura de red y demostrar la ausencia de configuraciones no deseadas que puedan exponer datos vulnerables. Este enfoque proporciona el mayor nivel de garantía posible para las características de seguridad críticas de la nube. Para obtener más información, consulte Provable Security Resources en el AWS sitio web. Actualmente, Servicios de AWS las siguientes funciones utilizan el razonamiento automatizado para ayudarlo a lograr una seguridad demostrable para sus aplicaciones:

- Amazon Verified Permissions es un servicio escalable de administración de permisos y autorización detallado para las aplicaciones que cree. Verified Permissions utiliza Cedar, un lenguaje de código abierto para el control de acceso que se creó mediante el razonamiento automatizado y las pruebas diferenciales. Cedar es un lenguaje para definir los permisos como políticas que describen quién debe tener acceso a qué recursos. También es una especificación

para evaluar esas políticas. Utilice las políticas de Cedar para controlar lo que cada usuario de su aplicación puede hacer y a qué recursos puede acceder. Las políticas de Cedar son declaraciones que permiten o prohíben que un usuario puede utilizar un recurso. Las políticas están asociadas a los recursos y puede adjuntar varias políticas a un recurso. Las políticas de prohibición anulan las políticas de permisos. Cuando un usuario de su aplicación intenta realizar una acción en un recurso, la aplicación realiza una solicitud de autorización al motor de políticas de Cedar. Cedar evalúa las políticas aplicables y devuelve una `DENY` decisión de `ALLOW` denegación. Cedar respalda las reglas de autorización para cualquier tipo de capital y recurso, permite un control de acceso basado en roles y atributos, y apoya el análisis mediante herramientas de razonamiento automatizadas que pueden ayudar a optimizar sus políticas y validar su modelo de seguridad.

- AWS Identity and Access Management Access Analyzerle ayuda a agilizar la gestión de permisos. Puede usar esta función para establecer permisos detallados, verificar los permisos previstos y refinar los permisos eliminando el acceso no utilizado. IAM Access Analyzer genera una política detallada basada en la actividad de acceso capturada en sus registros. También proporciona más de 100 comprobaciones de políticas para ayudarle a crear y validar sus políticas. IAM Access Analyzer utiliza una seguridad comprobada para analizar las rutas de acceso y proporcionar conclusiones exhaustivas para el acceso público y entre cuentas a sus recursos. Esta herramienta se basa en Zelkova, que traduce las políticas de IAM en declaraciones lógicas equivalentes y utiliza un conjunto de soluciones lógicas especializadas y de uso general (teorías de los módulos de adaptabilidad) para solucionar el problema. El Analizador de acceso de IAM aplica Zelkova repetidamente a una política con consultas cada vez más específicas para caracterizar las clases de comportamientos que permite la política, en función del contenido de la política. El analizador no examina los registros de acceso para determinar si una entidad externa ha accedido a un recurso dentro de su zona de confianza. Genera un resultado cuando una política basada en recursos permite el acceso a un recurso, incluso si la entidad externa no accedió al recurso. Para obtener más información sobre las teorías de los módulos de satisfactibilidad, consulte las teorías de los módulos de satisfactibilidad en el Manual de satisfactibilidad. *
- Amazon S3 Block Public Access es una función de Amazon S3 que le permite bloquear posibles errores de configuración que podrían provocar el acceso público a sus depósitos y objetos. Puede habilitar Amazon S3 Block Public Access para los puntos de acceso, los buckets, las cuentas y la AWS organización (lo que afecta tanto a los buckets existentes como a los nuevos de la cuenta). El acceso público se concede a los depósitos y objetos mediante listas de control de acceso (ACLs), políticas de depósitos o ambas opciones. Para determinar si una determinada política o ACL se considera pública, se utiliza el sistema de razonamiento automatizado Zelkova. Amazon S3 utiliza Zelkova para comprobar la política de cada bucket y le avisa si un usuario no autorizado puede leer o escribir en su bucket. Si un bucket está marcado como público, se permite

que algunas solicitudes públicas accedan al bucket. Si un depósito está marcado como no público, se rechazan todas las solicitudes públicas. Zelkova puede hacer estas determinaciones porque tiene una representación matemática precisa de las políticas de IAM. Crea una fórmula para cada política y demuestra un teorema sobre esa fórmula.

- El analizador de acceso a la red Amazon VPC es una función de Amazon VPC que le ayuda a comprender las posibles rutas de red a sus recursos e identifica el posible acceso no deseado a la red. El analizador de acceso a la red lo ayuda a verificar la segmentación de la red, identificar la accesibilidad a Internet y verificar las rutas de red confiables y el acceso a la red. Esta función utiliza algoritmos de razonamiento automatizados para analizar las rutas de red que un paquete puede recorrer entre los recursos de una AWS red. A continuación, obtiene información sobre las rutas que coinciden con los ámbitos de acceso a la red, que definen los patrones de tráfico entrante y saliente. Analizador de acceso a la red realiza un análisis estático de una configuración de red, lo que significa que no se transmite ningún paquete en la red como parte de este análisis.
- El Reachability Analyzer de Amazon VPC es una función de Amazon VPC que le permite depurar, comprender y visualizar la conectividad de su red. AWS Reachability Analyzer es una herramienta de análisis de configuración que le permite realizar pruebas de conectividad entre un recurso de origen y un recurso de destino en sus nubes privadas virtuales (). VPCs Cuando se puede alcanzar el destino, el Reachability Analyzer hop-by-hop produce detalles de la ruta de red virtual entre el origen y el destino. Cuando no se puede acceder al destino, el Reachability Analyzer identifica el componente de bloqueo. Reachability Analyzer utiliza el razonamiento automatizado para identificar rutas factibles mediante la creación de un modelo de la configuración de la red entre un origen y un destino. A continuación, comprueba la accesibilidad en función de la configuración. No envía paquetes ni analiza el plano de datos.

[*] Biere, A. M. Heule, H. van Maaren y T. Walsh. 2009. Manual de satisfactoriedad. IOS Press, NLD.

Creación de su arquitectura de seguridad: un enfoque gradual

Influya en el futuro de la arquitectura de referencia de AWS seguridad (AWS SRA) realizando una breve encuesta.

La arquitectura de seguridad multicuenta recomendada por la AWS SRA es una arquitectura básica que le ayudará a incorporar la seguridad en las primeras etapas del proceso de diseño. La transición de cada organización a la nube es única. Para que su arquitectura de seguridad en la nube evolucione satisfactoriamente, debe visualizar el estado objetivo deseado, comprender su nivel actual de preparación para la nube y adoptar un enfoque ágil para cerrar cualquier brecha. La AWS SRA proporciona un estado objetivo de referencia para su arquitectura de seguridad. La transformación gradual le permite demostrar su valor rápidamente y, al mismo tiempo, minimizar la necesidad de hacer predicciones de gran alcance.

El Marco de Adopción de la AWS Nube (AWS CAF) recomienda cuatro fases de transformación de la nube iterativas e incrementales: visualizar, alinear, lanzar y escalar. Al entrar en la fase de lanzamiento y centrarse en lanzar iniciativas piloto en producción, debería centrarse en crear una arquitectura de seguridad sólida como base para la fase de ampliación, de modo que tenga la capacidad técnica necesaria para migrar y operar las cargas de trabajo más críticas para la empresa con confianza. Este enfoque gradual es aplicable si es una empresa emergente, una empresa pequeña o mediana que quiere expandir su negocio o una empresa que está adquiriendo nuevas unidades de negocio o realizando fusiones y adquisiciones. La AWS SRA lo ayuda a lograr esa arquitectura básica de seguridad para que pueda aplicar los controles de seguridad de manera uniforme en toda su organización en expansión. AWS Organizations La arquitectura básica consta de varios servicios Cuentas de AWS Y. La planificación y la implementación deben ser un proceso de varias fases, de modo que pueda ir repasando hitos más pequeños para alcanzar el objetivo más amplio de configurar su arquitectura de seguridad básica. En esta sección, se describen las fases típicas de su transición a la nube en función de un enfoque estructurado. Estas fases se alinean con los principios de diseño de seguridad de AWS Well-Architected Framework.

Fase 1: Cree su OU y su estructura contable

Un requisito previo para una base de seguridad sólida es una AWS organización y una estructura de cuentas bien diseñadas. Como se explicó anteriormente en la sección de componentes básicos de la SRA de esta guía, tener varias Cuentas de AWS permite aislar diferentes funciones empresariales y de seguridad por diseño. Al principio, esto puede parecer un trabajo innecesario, pero se trata de una inversión que le ayudará a escalar de forma rápida y segura. En esa sección también se explica cómo AWS Organizations administrar varias Cuentas de AWS cuentas y cómo usar las funciones de acceso confiable y administrador delegado para administrar estas Servicios de AWS múltiples cuentas de forma centralizada.

Puedes usar AWS Control Towerlo descrito anteriormente en esta guía para organizar tu landing zone. Si actualmente utilizas una sola cuenta Cuenta de AWS, consulta la Cuentas de AWS guía sobre la transición a varias cuentas para migrar a varias cuentas lo antes posible. Por ejemplo, si su empresa emergente está ideando y creando prototipos de su producto en una sola Cuenta de AWS, debería pensar en adoptar una estrategia de cuentas múltiples antes de lanzar su producto al mercado. Del mismo modo, las organizaciones pequeñas, medianas y empresariales deberían empezar a desarrollar su estrategia de cuentas múltiples tan pronto como planifiquen sus cargas de trabajo de producción iniciales. Comience con su base OUs y Cuentas de AWS, a continuación, añada las cuentas y las cuentas relacionadas con la carga de trabajo OUs .

Para obtener Cuenta de AWS recomendaciones sobre la estructura de unidades organizativas más allá de lo que se proporciona en la AWS SRA, consulta la entrada del blog sobre la estrategia de múltiples cuentas para pequeñas y medianas empresas. Al finalizar la estructura de la unidad organizativa y la estructura de cuentas, tenga en cuenta los controles de seguridad de alto nivel que afectan a toda la organización y que le gustaría aplicar mediante políticas de control de servicios (SCPs), políticas de control de recursos () y políticas RCPs declarativas.

> **Consideración del diseño**
>
> No replique la estructura jerárquica de su empresa al diseñar la estructura organizativa y contable. OUs Debe basarse en las funciones de la carga de trabajo y en un conjunto común de controles de seguridad que se apliquen a las cargas de trabajo. No intentes diseñar tu estructura contable completa desde el principio. Céntrese en lo fundamental y OUs, a continuación, añada la carga de trabajo a OUs medida que la necesite. Puedes cambiar de una cuenta OUs a otra para experimentar con enfoques alternativos durante las primeras etapas del diseño. Sin embargo, esto podría generar algunos gastos generales

relacionados con la administración de los permisos lógicos SCPs RCPs, en función de las políticas declarativas y las condiciones de la IAM que se basan en las rutas de las cuentas y las unidades organizativas.

Ejemplo de implementación

La biblioteca de códigos AWS SRA proporciona un ejemplo de implementación de Account Alternate Contacts. Esta solución establece los contactos alternativos de facturación, operaciones y seguridad para todas las cuentas de una organización.

Fase 2: Implemente una base de identidad sólida

En cuanto hayas creado varias Cuentas de AWS, debes permitir que tus equipos accedan a los AWS recursos de esas cuentas. Existen dos categorías generales de gestión de la identidad: la gestión de la identidad y el acceso de los empleados y la gestión de la identidad y el acceso de los clientes (CIAM). Workforce IAM es para organizaciones en las que los empleados y las cargas de trabajo automatizadas necesitan iniciar sesión AWS para realizar su trabajo. El CIAM se utiliza cuando una organización necesita una forma de autenticar a los usuarios para proporcionar acceso a las aplicaciones de la organización. Lo primero que necesita es una estrategia de IAM para el personal, de modo que sus equipos puedan crear y migrar aplicaciones. Siempre debe utilizar funciones de IAM en lugar de usuarios de IAM para proporcionar acceso a usuarios humanos o de máquinas. Siga las instrucciones de la AWS SRA sobre cómo utilizarlas AWS IAM Identity Center en las cuentas de administración de la organización y de servicios compartidos para administrar de forma centralizada el acceso a su cuenta mediante el inicio de sesión único (SSO). Cuentas de AWS La guía también proporciona consideraciones de diseño para utilizar la federación de IAM cuando no se puede utilizar el IAM Identity Center.

Al trabajar con las funciones de IAM para proporcionar a los usuarios acceso a AWS los recursos, debe utilizar el analizador de acceso de IAM y el asesor de acceso de IAM, tal y como se describe en las secciones sobre herramientas de seguridad y gestión de la organización de esta guía. Estos servicios le ayudan a conseguir los privilegios mínimos, lo que constituye un importante control preventivo que le ayuda a adoptar una buena postura de seguridad.

Consideración del diseño

Para lograr el mínimo de privilegios, diseñe procesos que revisen y comprendan periódicamente las relaciones entre sus identidades y los permisos que requieren para funcionar correctamente. A medida que vaya aprendiendo, vaya ajustando esos permisos y redúzcalos gradualmente hasta que tengan el menor número posible de permisos. Para garantizar la escalabilidad, esta debe ser una responsabilidad compartida entre sus equipos centrales de seguridad y aplicaciones. Utilice funciones como las políticas basadas en los recursos, los límites de los permisos, los controles de acceso basados en los atributos y las políticas de sesión para ayudar a los propietarios de las aplicaciones a definir un control de acceso detallado.

Ejemplos de implementación

La biblioteca de códigos AWS SRA proporciona dos ejemplos de implementaciones que se aplican a esta fase:

- La política de contraseñas de IAM establece la política de contraseñas de las cuentas para que los usuarios se ajusten a las normas de conformidad comunes.
- Access Analyzer configura un analizador a nivel de organización dentro de una cuenta de administrador delegado y un analizador a nivel de cuenta dentro de cada cuenta.

Fase 3: Mantener la trazabilidad

Cuando sus usuarios tengan acceso AWS y comiencen a crear, querrá saber quién hace qué, cuándo y desde dónde. También querrá tener visibilidad sobre posibles errores de configuración de seguridad, amenazas o comportamientos inesperados. Una mejor comprensión de las amenazas a la seguridad le permite priorizar los controles de seguridad adecuados. Para supervisar la AWS actividad, siga las recomendaciones de la AWS SRA para configurar un registro de la organización mediante el uso AWS CloudTraily la centralización de los registros en la cuenta de Log Archive. Para la supervisión de eventos de seguridad AWS Security Hub CSPM, utilice Amazon y Amazon Security Lake GuardDuty AWS Config, tal y como se indica en la sección de cuentas de herramientas de seguridad.

Consideración del diseño

Cuando empiece a utilizar los nuevos Servicios de AWS, asegúrese de habilitar los registros específicos del servicio y de almacenarlos como parte de su repositorio de registros central.

Ejemplos de implementación

La biblioteca de códigos AWS SRA proporciona los siguientes ejemplos de implementaciones que se aplican a esta fase:

- La organización CloudTrail crea un registro de la organización y establece los valores predeterminados para configurar los eventos de datos (por ejemplo, en Amazon S3 y AWS Lambda) a fin de reducir la duplicación de CloudTrail los configurados por. AWS Control Tower Esta solución ofrece opciones para configurar los eventos de administración.
- AWS Config La cuenta de administración de la Torre de Control permite AWS Config en la cuenta de administración monitorear el cumplimiento de los recursos.
- Las reglas de organización del paquete de conformidad implementan un paquete de conformidad en las cuentas y regiones específicas de una organización.
- AWS Config El agregador implementa un agregador al delegar la administración a una cuenta de miembro que no sea la cuenta de auditoría.
- La organización Security Hub CSPM configura Security Hub CSPM dentro de una cuenta de administrador delegado para las cuentas y las regiones gobernadas de la organización.
- GuardDuty La organización se configura GuardDuty dentro de una cuenta de administrador delegado para las cuentas de una organización.

Fase 4: Aplicar la seguridad en todos los niveles

En este punto, deberías tener:

- Los controles de seguridad adecuados para su Cuentas de AWS.
- Una estructura de cuentas y unidades organizativas bien definidas con controles preventivos definidos mediante SCPs políticas declarativas y funciones y políticas de IAM con privilegios mínimos. RCPs

- La capacidad de registrar AWS las actividades mediante el uso AWS CloudTrail; de detectar eventos de seguridad mediante AWS Security Hub CSPM Amazon GuardDuty y AWS Config; y de realizar análisis avanzados en un lago de datos diseñado específicamente para la seguridad mediante Amazon Security Lake.

En esta fase, planifique aplicar la seguridad en otros niveles de su AWS organización, tal y como se describe en la sección Aplicar servicios de seguridad en toda su AWS organización. Puede crear controles de seguridad para su capa de red mediante servicios como AWS WAF,, AWS Shield, AWS Certificate Manager (ACM) AWS Firewall Manager AWS Network Firewall, Amazon CloudFront, Amazon Route 53 y Amazon VPC, tal y como se describe en la sección Cuenta de red. A medida que avance en su gama de tecnologías, aplique controles de seguridad específicos para su carga de trabajo o conjunto de aplicaciones. Utilice los puntos de enlace de VPC AWS Systems Manager, AWS Secrets Manager Amazon Inspector y Amazon Cognito tal y como se describe en la sección Cuenta de aplicación.

Consideración del diseño

Al diseñar los controles de seguridad de Defense in Depth (DiD), tenga en cuenta los factores de escalabilidad. Su equipo de seguridad central no tendrá el ancho de banda ni una comprensión completa del comportamiento de cada aplicación en su entorno. Capacite a sus equipos de aplicaciones para que asuman la responsabilidad de identificar y diseñar los controles de seguridad adecuados para sus aplicaciones. El equipo de seguridad central debe centrarse en proporcionar las herramientas y las consultas adecuadas para capacitar a los equipos de aplicaciones. Para comprender los mecanismos de escalamiento que se AWS utilizan para adoptar un enfoque de seguridad más inclinado hacia la izquierda, consulte la entrada del blog Cómo se AWS creó el programa Security Guardians, un mecanismo para distribuir la propiedad de la seguridad.

Ejemplos de implementación

La biblioteca de códigos AWS SRA proporciona los siguientes ejemplos de implementaciones que se aplican a esta fase:

- El cifrado EBS predeterminado de EC2 configura el cifrado de Amazon EBS predeterminado en Amazon EC2 para utilizar el predeterminado dentro del proporcionado. AWS KMS key Regiones de AWS

- S3 Block Account Public Access configura los ajustes de Block Public Access (BPA) a nivel de cuenta en Amazon S3 para las cuentas de la organización.
- Firewall Manager muestra cómo configurar una política de grupo de seguridad y AWS WAF políticas para las cuentas de una organización.
- Inspector Organization configura Amazon Inspector dentro de una cuenta de administrador delegado para las cuentas y regiones gobernadas dentro de la organización.

Fase 5: Proteja los datos en tránsito y en reposo

Los datos de su empresa y de sus clientes son activos valiosos que debe proteger. AWS proporciona varios servicios y funciones de seguridad para proteger los datos en movimiento y en reposo. Usa Amazon CloudFront con AWS Certificate Manager, tal y como se describe en la sección Cuenta de red, para proteger los datos en movimiento que se recopilan a través de Internet. Para los datos en movimiento dentro de las redes internas, utilice un Application Load Balancer con AWS Private Certificate Authority, tal y como se explica en la sección Cuenta de la aplicación. AWS KMS y le AWS CloudHSM ayudan a gestionar las claves criptográficas para proteger los datos en reposo.

Fase 6: Prepárese para los eventos de seguridad

A medida que opere su entorno de TI, se producirán incidentes de seguridad, que son cambios en el funcionamiento diario de su entorno de TI que indican una posible infracción de la política de seguridad o un fallo en el control de seguridad. La trazabilidad adecuada es fundamental para detectar un incidente de seguridad lo antes posible. Es igualmente importante estar preparado para clasificar estos eventos de seguridad y responder a ellos, de modo que pueda tomar las medidas adecuadas antes de que el problema de seguridad se agrave. La preparación le ayuda a clasificar rápidamente un evento de seguridad para comprender su posible impacto.

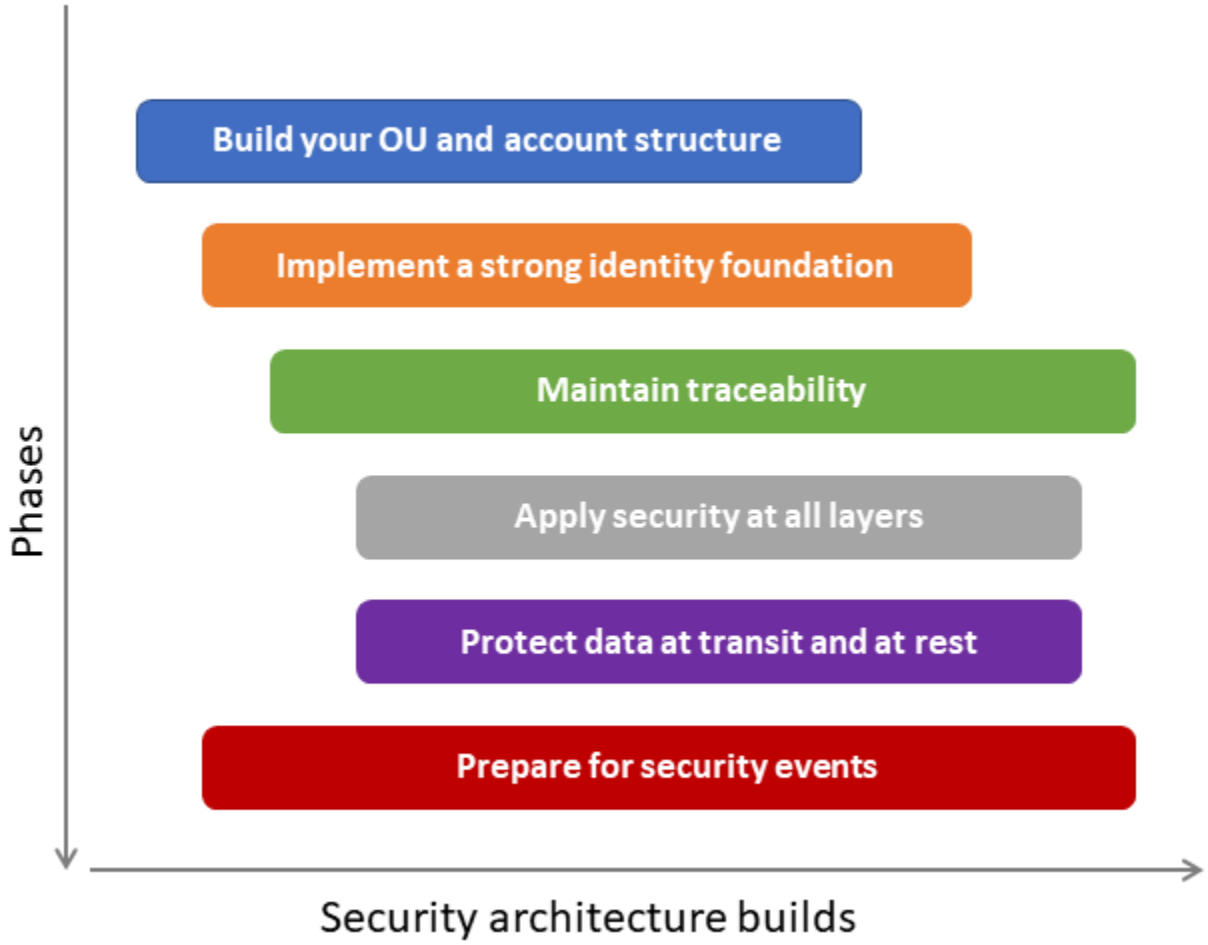
La AWS SRA, mediante el diseño de la cuenta de herramientas de seguridad y el despliegue de servicios de seguridad comunes en todas ellas Cuentas de AWS, le permite detectar eventos de seguridad en toda su organización. AWS Amazon Detective, incluido en la cuenta de herramientas de seguridad, le ayuda a clasificar un evento de seguridad e identificar la causa raíz. Durante una investigación de seguridad, debe poder revisar los registros pertinentes para registrar y comprender el alcance completo y la cronología del incidente. Los registros también son necesarios para generar alertas cuando se producen acciones específicas de interés. La AWS SRA recomienda una cuenta central de archivo de registros para el almacenamiento inmutable de todos los registros operativos

y de seguridad. Puede consultar los CloudWatch registros mediante Logs Insights para los datos almacenados en grupos de CloudWatch registros, y Amazon Athena y Amazon OpenSearch Service para los datos almacenados en Amazon S3. Utilice Amazon Security Lake para centralizar automáticamente los datos de seguridad del AWS entorno, los proveedores de software como servicio (SaaS), las instalaciones y otros proveedores de nube. Configure los suscriptores en la cuenta de Security Tooling o en cualquier cuenta dedicada, según lo establecido en la AWS SRA, para que consulten esos registros a fin de investigarlos.

Respuesta frente a incidencias de seguridad de AWSle ayuda a automatizar la respuesta, la investigación y la reparación de los incidentes de seguridad. Proporciona guías de trabajo y flujos de trabajo prediseñados para ayudarle a responder a los eventos de seguridad de forma rápida y coherente. Cuando la función de respuesta proactiva está habilitada, Security Incident Response se integra con Security Hub CSPM y activa automáticamente GuardDuty los flujos de trabajo de respuesta cuando se detectan hallazgos de seguridad. El servicio le ayuda a estandarizar y automatizar los procesos de respuesta a incidentes en toda la organización. AWS Si necesita más ayuda, puede abrir un caso respaldado por el servicio para contactar con el equipo de respuesta a incidentes del AWS cliente (CIRT).

Consideraciones sobre el diseño

- Debe empezar a prepararse para detectar y responder a los eventos de seguridad desde el principio de su transición a la nube. Para aprovechar mejor los recursos limitados, asigne la importancia de los datos y la importancia empresarial a sus AWS recursos para que, cuando detecte un incidente de seguridad, pueda priorizar la clasificación y la respuesta en función de la importancia de los recursos involucrados.
- Las fases de creación de la arquitectura de seguridad en la nube, tal como se describe en esta sección, son de naturaleza secuencial. Sin embargo, no tiene que esperar a que se complete por completo una fase para comenzar la siguiente. Le recomendamos que adopte un enfoque iterativo, en el que comience a trabajar en varias fases en paralelo y evolucione cada fase a medida que evolucione su postura de seguridad en la nube. A medida que vaya pasando por las diferentes fases, su diseño irá evolucionando. Considere la posibilidad de adaptar la secuencia sugerida que se muestra en el siguiente diagrama a sus necesidades particulares.



Ejemplo de implementación

La biblioteca de códigos AWS SRA proporciona un ejemplo de implementación de una organización de detectives, que habilita automáticamente Amazon Detective al delegar la administración en una cuenta (por ejemplo, herramientas de auditoría o seguridad) y configura Detective para las cuentas existentes y futuras. AWS Organizations

AWS Lista de verificación de mejores prácticas de la SRA

Influya en el futuro de la arquitectura de referencia de AWS seguridad (AWS SRA) realizando una breve encuesta.

En esta sección, se resumen las prácticas recomendadas de la AWS SRA que se detallan a lo largo de esta guía en una lista de comprobación que puede seguir a medida que vaya creando su versión de la arquitectura de seguridad. AWS Utilice esta lista como punto de referencia y no como sustituto de la revisión de la guía. La lista de verificación está agrupada por Servicio de AWS. Si desea validar mediante programación su AWS entorno actual según la lista de prácticas recomendadas de la AWS SRA, puede utilizar SRA Verify.

SRA Verify es una herramienta de evaluación de la seguridad que le ayuda a evaluar la alineación de su organización con la SRA en varias regiones. AWS Cuentas de AWS Se ajusta directamente a las recomendaciones de la AWS SRA al proporcionar comprobaciones automatizadas que validan su implementación según las directrices de la AWS SRA. La herramienta le ayuda a verificar que sus servicios de seguridad estén configurados correctamente de acuerdo con la arquitectura de referencia. Proporciona conclusiones detalladas y medidas de corrección prácticas para garantizar que su AWS entorno siga las mejores prácticas de seguridad. SRA Verify está diseñado para ejecutarse AWS CodeBuild en la cuenta de auditoría de la organización (herramientas de seguridad). También puede ejecutarlo localmente o ampliarlo mediante la biblioteca SRA Verify.

> **Note**
>
> SRA Verify contiene comprobaciones para varios servicios, pero es posible que no contenga una verificación para cada consideración de la AWS SRA. Para obtener más información, consulte las guías de la biblioteca de la AWS SRA.

AWS Organizations

- AWS Organizations está habilitado con todas las funciones.
- Las políticas de control de servicios (SCPs) se utilizan para definir las directrices de control de acceso para los directores de IAM.

- Las políticas de control de recursos (RCPs) se utilizan para definir las pautas de control de acceso de los AWS recursos.
- Las políticas declarativas se utilizan para declarar y aplicar de forma centralizada la configuración deseada para una determinada escala Servicio de AWS en toda la organización.
- Se OUs crean tres bases (seguridad, infraestructura y carga de trabajo) para agrupar las cuentas de los miembros que prestan servicios básicos.
- La cuenta Security Tooling se crea en la OU de seguridad. Esta cuenta proporciona una administración centralizada de los servicios de AWS seguridad y otras herramientas de seguridad de terceros.
- La cuenta Log Archive se crea en la OU de seguridad. Esta cuenta proporciona un repositorio central de registros Servicios de AWS y registros de aplicaciones estrictamente controlado.
- La cuenta de red se crea en la OU de infraestructura. Esta cuenta administra la puerta de enlace entre su aplicación e Internet en general. Aísla los servicios de red, la configuración y el funcionamiento de las cargas de trabajo de las aplicaciones individuales, de la seguridad y de otras infraestructuras.
- La cuenta de servicio compartido se crea en la OU de infraestructura. Esta cuenta admite los servicios que utilizan varias aplicaciones y equipos para ofrecer sus resultados.
- La cuenta de la aplicación se crea en la OU de Workloads. Esta cuenta aloja la infraestructura y los servicios principales para ejecutar y mantener una aplicación empresarial. Esta guía proporciona una representación, pero en el mundo real habrá varias cuentas OUs y cuentas de miembros segregadas por aplicaciones, entornos de desarrollo y otras consideraciones de seguridad.
- Se ha configurado información de contacto alternativa para la facturación, las operaciones y la seguridad de todas las cuentas de los miembros.

AWS CloudTrail

- Se configura un registro de la organización que permite la entrega de eventos de CloudTrail administración en la cuenta de administración y en todas las cuentas de los miembros de una AWS organización.
- El registro de la organización está configurado como un registro multirregional.
- El registro de la organización está configurado para capturar los eventos de los recursos globales.
- Los registros adicionales para capturar eventos de datos específicos se configuran según sea necesario para monitorear las actividades AWS de recursos confidenciales.

- La cuenta Security Tooling está configurada como administradora delegada del registro de la organización.
- El registro de la organización está configurado para activarse automáticamente en todas las cuentas de los miembros nuevos.
- El registro de la organización está configurado para publicar los registros en un depósito de S3 centralizado que está alojado en la cuenta de Log Archive.
- El registro de la organización tiene habilitada la validación de los archivos de registro para verificar la integridad de los archivos de registro.
- El registro de la organización está integrado con CloudWatch los registros para conservar los registros.
- El registro de la organización se cifra mediante una clave gestionada por el cliente.
- El depósito central de S3 que se utiliza para el repositorio de registros de la cuenta de Log Archive se cifra con una clave gestionada por el cliente.
- El depósito S3 central que se utiliza para el repositorio de registros de la cuenta de Log Archive está configurado con S3 Object Lock para garantizar la inmutabilidad.
- El control de versiones está habilitado para el depósito S3 central que se utiliza para el repositorio de registros de la cuenta de Log Archive.
- El depósito central de S3 que se utiliza para el repositorio de registros de la cuenta de Log Archive tiene definida una política de recursos que restringe la carga de objetos únicamente mediante el seguimiento de la organización a través del recurso Amazon Resource Name (ARN).

AWS Security Hub CSPM

- El CSPM de Security Hub está habilitado para todas las cuentas de los miembros y para la cuenta de administración.
- AWS Config está habilitado para todas las cuentas de los miembros como requisito previo para el CSPM de Security Hub.
- La cuenta Security Tooling está configurada como administrador delegado de Security Hub CSPM.
- Amazon GuardDuty y Amazon Detective tienen la misma cuenta de administrador delegado que Security Hub CSPM para una integración de servicios fluida.
- La configuración central se utiliza para configurar y administrar el Security Hub CSPM en múltiples Cuentas de AWS y. Regiones de AWS

- El administrador delegado de Security Hub CSPM designa todas las OU y las cuentas de los miembros como administradas de forma centralizada.
- El CSPM de Security Hub se habilita automáticamente para todas las cuentas de los miembros nuevos.
- Security Hub CSPM se habilita automáticamente para la configuración de nuevos estándares.
- Los resultados del CSPM de Security Hub de todas las regiones se agregan a una sola región de origen.
- Los resultados del CSPM de Security Hub de todas las cuentas de los miembros se agregan a la cuenta de Security Tooling.
- El estándar AWS Foundational Best Practices (FSBP) de Security Hub CSPM está habilitado para todas las cuentas de los miembros.
- El estándar CIS AWS Foundation Benchmark en Security Hub CSPM está habilitado para todas las cuentas de los miembros.
- Otros estándares CSPM de Security Hub están habilitados según corresponda.
- Se utiliza una regla de automatización CSPM de Security Hub para enriquecer los hallazgos con el contexto de los recursos.
- La función de respuesta y corrección automatizadas CSPM de Security Hub se utiliza para crear EventBridge reglas personalizadas para tomar medidas automáticas en caso de hallazgos específicos.

AWS Config

- La AWS Config grabadora está habilitada para todas las cuentas de los miembros y para la cuenta de administración.
- La AWS Config grabadora está habilitada para todas las regiones.
- El depósito S3 del canal de AWS Config entrega está centralizado en la cuenta de Log Archive.
- La cuenta de administrador AWS Config delegado se establece en la cuenta Security Tooling.
- AWS Config tiene un agregador de organizaciones configurado. El agregador incluye todas las regiones.
- AWS Config Los paquetes de conformidad se implementan de manera uniforme en todas las cuentas de los miembros desde la cuenta de administrador delegado.
- AWS Config las conclusiones de las reglas se envían automáticamente a Security Hub CSPM.

Amazon GuardDuty

- GuardDuty El detector está activado para todas las cuentas de los miembros y para la cuenta de administración.
- GuardDuty el detector está activado en todas las regiones.
- GuardDuty el detector se activa automáticamente para todas las cuentas de los miembros nuevos.
- GuardDuty la administración delegada se establece en la cuenta Security Tooling.
- GuardDuty Las fuentes de datos fundamentales, como los eventos CloudTrail de administración, los registros de flujo de VPC y los registros de consultas DNS de Route 53 Resolver, están habilitadas.
- GuardDuty La protección S3 está habilitada.
- GuardDuty La protección contra malware para los volúmenes de EBS está habilitada.
- GuardDuty La protección contra malware para S3 está habilitada.
- GuardDuty La protección RDS está habilitada.
- GuardDuty La protección Lambda está habilitada.
- GuardDuty La protección EKS está habilitada.
- GuardDuty La monitorización del tiempo de ejecución de EKS está habilitada.
- GuardDuty La detección extendida de amenazas está habilitada.
- GuardDuty Los resultados se exportan a un depósito central de S3 en la cuenta de Log Archive para su conservación.

IAM

- No se utilizan usuarios de IAM.
- Se aplica una administración centralizada del acceso raíz a las cuentas de los miembros.
- La tarea centralizada de usuario raíz con privilegios para la cuenta de administración la ejecuta el administrador delegado.
- La administración centralizada del acceso raíz se delega en la cuenta Security Tooling.
- Se eliminan todas las credenciales raíz de la cuenta de miembro.
- Todas las políticas de Cuenta de AWS contraseñas de los miembros y de la administración se establecen de acuerdo con el estándar de seguridad de la organización.

- El asesor de acceso de IAM se utiliza para revisar la última información utilizada para los grupos, usuarios, funciones y políticas de IAM.
- Los límites de permisos se utilizan para restringir el máximo de permisos posibles para las funciones de IAM.

Analizador de acceso de IAM

- El analizador de acceso de IAM está activado para todas las cuentas de los miembros y para la cuenta de administración.
- El administrador delegado de IAM Access Analyzer está configurado en la cuenta Security Tooling.
- El analizador de acceso externo de IAM Access Analyzer está configurado con la zona de confianza de la organización en cada región.
- El analizador de acceso externo de IAM Access Analyzer está configurado con la zona de confianza de la cuenta en cada región.
- El analizador de acceso interno de IAM Access Analyzer está configurado con la zona de confianza de la organización en cada región.
- El analizador de acceso interno de IAM Access Analyzer está configurado con la zona de confianza de la cuenta en cada región.
- Se crea el analizador de acceso no utilizado de IAM Access Analyzer para la cuenta corriente.
- Se crea el analizador de acceso no utilizado de IAM Access Analyzer para la organización actual.

Amazon Detective

- Detective está activado para todas las cuentas de los miembros.
- Detective se activa automáticamente para todas las cuentas de miembros nuevos.
- Detective está activado en todas las regiones.
- El administrador delegado del Detective está configurado en la cuenta Security Tooling.
- El administrador delegado de CSPM de Detective y Security Hub está configurado en la misma cuenta de Security Tooling. GuardDuty
- Detective está integrado con Security Lake para almacenar y analizar registros sin procesar.
- Detective está integrado GuardDuty para ingerir los hallazgos.
- El Detective está ingiriendo los registros de auditoría de Amazon EKS para analizarlos.

- El Detective está ingiriendo los registros CSPM de Security Hub para analizarlos.

AWS Firewall Manager

- Se han establecido las políticas de seguridad de Firewall Manager.
- El administrador delegado de Firewall Manager está configurado en la cuenta Security Tooling.
- AWS Config está habilitada como requisito previo.
- Se configuran varios administradores de Firewall Manager con un alcance restringido por unidad organizativa, cuenta y región.
- Se define una política AWS WAF de seguridad de Firewall Manager.
- Se define una política de registro AWS WAF centralizada de Firewall Manager.
- Se define una política de seguridad avanzada de Firewall Manager Shield.
- Se define una política de seguridad del grupo de seguridad de Firewall Manager.

Amazon Inspector

- Amazon Inspector está activado para todas las cuentas de los miembros.
- Amazon Inspector se activa automáticamente para cualquier cuenta de miembro nuevo.
- El administrador delegado de Amazon Inspector está configurado en la cuenta Security Tooling.
- El escaneo de EC2 vulnerabilidades de Amazon Inspector está activado.
- El escaneo de vulnerabilidades de imágenes ECR de Amazon Inspector está activado.
- El escaneo de vulnerabilidades de capas y funciones de Amazon Inspector Lambda está activado.
- El escaneo de código Lambda de Amazon Inspector está activado.
- El escaneo de seguridad del código de Amazon Inspector está activado.

Amazon Macie

- Macie está activado para las cuentas de los miembros correspondientes.
- Macie se habilita automáticamente para las nuevas cuentas de miembros aplicables.
- El administrador delegado de Macie está configurado en la cuenta Security Tooling.
- Los resultados de Macie se exportan a un depósito S3 central en la cuenta de log Archive.

- Los depósitos de S3 que almacenan los hallazgos de Macie están cifrados con una clave gestionada por el cliente.
- La política de Macie y la política de clasificación se publican en Security Hub CSPM.

Amazon Security Lake

- La configuración de la organización de Security Lake está habilitada.
- El administrador delegado de Security Lake está configurado en la cuenta Security Tooling.
- La configuración de la organización de Security Lake está habilitada para las cuentas de los nuevos miembros.
- La cuenta Security Tooling está configurada como suscriptora de acceso a datos para analizar los registros.
- La cuenta Security Tooling está configurada como suscriptora de consultas de datos para analizar los registros.
- Hay una fuente CloudTrail de registro de administración habilitada para Security Lake en todas las cuentas de los miembros activos o en algunas de ellas.
- Se habilita una fuente de registro de flujo de VPC para Security Lake en todas las cuentas de los miembros activos o en las especificadas.
- Hay una fuente de registro de Route 53 habilitada para Security Lake en todas las cuentas de los miembros activos o en las específicas.
- CloudTrail El evento de datos de una fuente de registro de S3 está habilitado para Security Lake en todas las cuentas de los miembros activos o en algunas de ellas.
- Se habilita una fuente de registro de ejecución de Lambda para Security Lake en todas las cuentas de los miembros activos o en las especificadas.
- Hay una fuente de registro de auditoría de Amazon EKS habilitada para Security Lake en todas las cuentas de miembros activos o en determinadas cuentas.
- Hay una fuente de registro de hallazgos de Security Hub habilitada para Security Lake en todas las cuentas de los miembros activos o en las especificadas.
- Hay una fuente de AWS WAF registro habilitada para Security Lake en todas las cuentas de los miembros activos o en las específicas.
- Las colas SQS de Security Lake de la cuenta de administrador delegado se cifran con una clave gestionada por el cliente.

- La cola de letras muertas SQS de Security Lake de la cuenta de administrador delegado está cifrada con una clave gestionada por el cliente.
- El depósito S3 de Security Lake está cifrado con una clave gestionada por el cliente.
- El depósito S3 de Security Lake tiene una política de recursos que solo restringe el acceso directo de Security Lake.

AWS WAF

- Todas las CloudFront distribuciones están asociadas a. AWS WAF
- Todos los REST de Amazon API Gateway APIs están asociados a AWS WAF.
- Todos los balanceadores de carga de aplicaciones están asociados AWS WAF a.
- Todos los AWS AppSync GraphQL APIs están asociados a. AWS WAF
- Todos los grupos de usuarios de Amazon Cognito están asociados a. AWS WAF
- Todos los AWS App Runner servicios están asociados AWS WAF a.
- Todas las Acceso verificado de AWS instancias están asociadas a AWS WAF.
- Todas AWS Amplify las aplicaciones están asociadas a AWS WAF.
- AWS WAF el registro está activado.
- AWS WAF los registros están centralizados en un depósito de S3 en la cuenta de Log Archive.

AWS Shield Advanced

- La suscripción Shield Advanced está habilitada y configurada para renovarse automáticamente en todas las cuentas de aplicaciones que tengan recursos públicos.
- Shield Advanced está configurado para todas las CloudFront distribuciones.
- Shield Advanced está configurado para todos los balanceadores de carga de aplicaciones.
- Shield Advanced está configurado para todos los balanceadores de carga de red.
- Shield Advanced está configurado para todas las zonas alojadas en Route 53.
- Shield Advanced está configurado para todas las direcciones IP elásticas.
- Shield Advanced está configurado para todos los aceleradores globales.
- CloudWatch las alarmas están configuradas para CloudFront los recursos de Route 53 que están protegidos por Shield Advanced.

- El acceso a Shield Response Team (SRT) está configurado.
- La interacción proactiva de Shield Advanced está habilitada.
- Los contactos de participación proactiva de Shield Advanced están configurados.
- Los recursos protegidos de Shield Advanced tienen una AWS WAF regla personalizada configurada.
- Los recursos protegidos de Shield Advanced tienen habilitada la mitigación automática de la capa DDo S de aplicación.

AWS Respuesta a incidentes de seguridad

- AWS La respuesta a incidentes de seguridad está habilitada para toda la AWS organización.
- El administrador delegado AWS de la respuesta a incidentes de seguridad está configurado en la cuenta Security Tooling.
- El flujo de trabajo de respuesta proactiva y clasificación de alertas está activado.
- AWS Se autorizan las acciones de contención del equipo de respuesta a incidentes del cliente (CIRT).

AWS Audit Manager

- Audit Manager está activado para todas las cuentas de los miembros.
- Audit Manager se activa automáticamente para las cuentas de los nuevos miembros.
- El administrador delegado de Audit Manager está configurado en la cuenta Security Tooling.
- AWS Config está activado como requisito previo para Audit Manager.
- Se utiliza una clave gestionada por el cliente para los datos almacenados en Audit Manager.
- El destino predeterminado del informe de evaluación está configurado.

Recursos de IAM

Influya en el futuro de la arquitectura de referencia de AWS seguridad (AWS SRA) realizando una breve encuesta.

Si bien AWS Identity and Access Management (IAM) no es un servicio que se incluya en un diagrama de arquitectura tradicional, abarca todos los aspectos de la AWS organización Cuentas de AWS, y. Servicios de AWS No puede implementar ninguno Servicios de AWS sin crear entidades de IAM y conceder primero los permisos. Una explicación completa de la IAM va más allá del alcance de este documento, pero en esta sección se proporcionan resúmenes importantes de las recomendaciones de mejores prácticas y sugerencias sobre recursos adicionales.

- Para conocer las prácticas recomendadas de IAM, consulte las prácticas recomendadas de seguridad en la AWS documentación, los artículos sobre IAMen el blog de AWS seguridad y las presentaciones de re:Invent.AWS
- El AWS pilar de seguridad de Well-Architected describe los pasos clave del proceso de administración de permisos: definir las barreras de protección de los permisos, conceder el acceso con privilegios mínimos, analizar el acceso público y entre cuentas, compartir los recursos de forma segura, reducir los permisos de forma continua y establecer un proceso de acceso de emergencia.
- La siguiente tabla y las notas adjuntas ofrecen una descripción general de alto nivel de las directrices recomendadas sobre los tipos de políticas de permisos de IAM disponibles y cómo utilizarlas en su arquitectura de seguridad. Para obtener más información, consulte el vídeo AWS re:Invent 2020 sobre cómo elegir la combinación adecuada de políticas de IAM.

Caso de uso o política	Effect	Administrado por	Finalidad	Pertenece a	Afecta	Desplegado en
Políticas de control de	Restrict	Equipo central, como el equipo de	Barandillas, gobernanza	Organización, unidad organizativa, cuenta	Todos los elementos principales de la	Cuenta de administración de la

servicios (SCPs)		plataforma o seguridad [1]			organización, la unidad organizativa y las cuentas	organización [2]
Políticas de control de recursos (RCPs)	Restrict	Equipo central, como el equipo de plataforma o seguridad [1]	Barandillas, gobernanza	Organización, unidad organizativa, cuenta	Recursos en las cuentas de los miembros [12]	Cuenta de administración de la organización [2]
Políticas básicas de automatización de cuentas (las funciones de IAM que utiliza la plataforma para gestionar una cuenta)	Otorgar y restringir	Equipo central, como el equipo de plataforma, seguridad o IAM [1]	Permisos para funciones (básicas) ajenas a la automatización de la carga de trabajo [3]	Cuenta única [4]	Principales utilizados por la automatización en una cuenta de miembro	Cuentas de miembros

Políticas humanas básicas (las funciones de IAM que otorgan a los usuarios permisos para realizar su trabajo)	Otorga y restringe	Equipo central, como el equipo de plataforma, seguridad o IAM [1]	Permisos para funciones humanas [5]	Cuenta única [4]	Directores federados [5] y usuarios de IAM [6]	Cuentas de miembros
Límites de permisos (permisos máximos que un desarrollador autorizado puede asignar a otro director)	Restrict	Equipo central, como el equipo de plataforma, seguridad o IAM [1]	Barandillas para las funciones de aplicación (deben estar colocadas)	Cuenta única [4]	Funciones individuales para una aplicación o carga de trabajo en esta cuenta [7]	Cuentas de miembros

Políticas de funciones de máquina para las aplicaciones (función asociada a la infraestructura implementada por los desarrolladores)	Otorgar y restringir	Delegado a los desarrolladores [8]	Permiso para la aplicación o la carga de trabajo [9]	Cuenta única	Un principal de esta cuenta	Cuentas de miembros
Políticas de recursos	Otorgar y restringir	Delegado a los desarrolladores [8,10]	Permisos a los recursos	Cuenta única	El principal de una cuenta [11]	Cuentas de miembros
Administración central de usuarios raíz	Otorgar y restringir	Equipo central, como el equipo de plataforma, seguridad o IAM [1]	Administre de forma centralizada los usuarios raíz de las cuentas de los miembros a escala	Organización	Todos los usuarios raíz de las cuentas de los miembros	Cuenta de administración de la organización, cuenta de administrador delegado

Notas de la tabla:

1. Las empresas cuentan con muchos equipos centralizados (como los equipos de plataformas en la nube, de operaciones de seguridad o de gestión de identidades y accesos) que dividen las responsabilidades de estos controles independientes y revisan las políticas de los demás por pares. Los ejemplos de la tabla son marcadores de posición. Deberá determinar la separación de funciones más eficaz para su empresa.
2. Para usarlo SCPs, debe habilitar todas las funciones que contiene AWS Organizations.
3. Por lo general, se necesitan funciones y políticas básicas comunes para permitir la automatización, como los permisos para la canalización, las herramientas de implementación, las herramientas de monitoreo (por ejemplo, AWS Lambda y Reglas de AWS Config) y otros permisos. Esta configuración suele entregarse cuando se aprovisiona la cuenta.
4. Si bien se refieren a un recurso (como un rol o una política) de una sola cuenta, se pueden replicar o implementar en varias cuentas mediante el uso de. AWS CloudFormation StackSets
5. Defina un conjunto básico de políticas y funciones humanas básicas que un equipo central implemente en todas las cuentas de los miembros (por lo general, durante el aprovisionamiento de las cuentas). Algunos ejemplos son los desarrolladores del equipo de plataformas, el equipo de IAM y los equipos de auditoría de seguridad.
6. Utilice la federación de identidades (en lugar de los usuarios de IAM locales) siempre que sea posible.
7. Los administradores delegados utilizan los límites de los permisos. Esta política de IAM define los permisos máximos y anula otras políticas (incluidas las `"*:*"` políticas que permiten realizar todas las acciones en los recursos). Las políticas humanas básicas deberían exigir límites de permisos como condición para crear funciones (como las funciones de desempeño de la carga de trabajo) y adjuntar políticas. Configuraciones adicionales, como SCPs la imposición de adjuntar el límite de permisos.
8. Esto supone que se han desplegado suficientes barandillas (por ejemplo, SCPs y límites de permisos).
9. Estas políticas opcionales se pueden implementar durante el aprovisionamiento de la cuenta o como parte del proceso de desarrollo de la aplicación. El permiso para crear y adjuntar estas políticas se regirá por los propios permisos del desarrollador de la aplicación.
10. Además de los permisos de las cuentas locales, un equipo centralizado (como el equipo de la plataforma en la nube o el equipo de operaciones de seguridad) suele gestionar algunas políticas basadas en los recursos para permitir el acceso entre cuentas para gestionar las cuentas (por ejemplo, para proporcionar acceso a los depósitos de S3 para el registro).

11. Una política de IAM basada en recursos puede hacer referencia a cualquier responsable de cualquier cuenta para permitir o denegar el acceso a sus recursos. Incluso puede hacer referencia a directores anónimos para permitir el acceso público.
12. RCPs se aplican a los recursos de un subconjunto de. Servicios de AWS Para obtener más información, consulte la lista de Servicios de AWS ese soporte RCPs en la AWS Organizations documentación.

Garantizar que las identidades de IAM solo tengan los permisos necesarios para un conjunto de tareas bien definido es fundamental para reducir el riesgo de abuso malintencionado o no intencionado de los permisos. Establecer y mantener un modelo de privilegios mínimos requiere un plan deliberado para actualizar, evaluar y mitigar continuamente el exceso de privilegios. Estas son algunas recomendaciones adicionales para ese plan:

- Utilice el modelo de gobierno de su organización y la propensión al riesgo establecida para establecer barreras y límites de permisos específicos.
- Implemente los privilegios mínimos mediante un proceso continuo e iterativo. No se trata de un ejercicio de una sola vez.
- Úselo SCPs para reducir el riesgo procesable. Se pretende que sean barreras amplias, no controles específicos.
- Utilice los límites de los permisos para delegar la administración de IAM de una manera más segura.
  - Asegúrese de que los administradores delegados adjunten la política de límites de IAM adecuada a los roles y usuarios que creen.
- Como defense-in-depth enfoque (junto con las políticas basadas en la identidad), utilice políticas de IAM basadas en los recursos para denegar el acceso generalizado a los recursos.
- Utilice el asesor de acceso de IAM AWS CloudTrail, el analizador de acceso de IAM y las herramientas relacionadas para analizar periódicamente el uso histórico y los permisos concedidos. Corrija inmediatamente los excedentes de permisos evidentes.
- Limite las acciones generales a recursos específicos, cuando proceda, en lugar de utilizar un asterisco como comodín para indicar todos los recursos.
- Implemente un mecanismo para identificar, revisar y aprobar rápidamente las excepciones a las políticas de IAM en función de las solicitudes.

Repositorio de código para AWS ejemplos de SRA

Influya en el futuro de la arquitectura de referencia de AWS seguridad (AWS SRA) realizando una breve encuesta.

Para ayudarle a empezar a crear e implementar las directrices de la AWS SRA, esta guía incluye un repositorio de infraestructura como código (IaC) en https://github.com/aws-samples/aws-security-reference-architecture-examples. Este repositorio contiene código para ayudar a los desarrolladores e ingenieros a implementar algunas de las guías y patrones de arquitectura que se presentan en este documento. Este código se basa en la experiencia de primera mano de los consultores de servicios AWS profesionales con los clientes. Las plantillas son de naturaleza general; su objetivo es ilustrar un patrón de implementación en lugar de proporcionar una solución completa. Las Servicio de AWS configuraciones y los despliegues de recursos son deliberadamente muy restrictivos. Es posible que necesite modificar y adaptar estas soluciones para adaptarlas a sus necesidades de entorno y seguridad.

El repositorio de código AWS SRA proporciona ejemplos de código con ambas opciones de implementación AWS CloudFormation y las de Terraform. Los patrones de solución admiten dos entornos: uno requiere AWS Control Tower y el otro se usa AWS Organizations sin él. AWS Control Tower Las soluciones de este repositorio que se requieren se AWS Control Tower han implementado y probado en un AWS Control Tower entorno mediante AWS CloudFormation el uso de Customizations for AWS Control Tower (cFCT). Las soluciones que no lo requieren se AWS Control Tower han probado en un AWS Organizations entorno mediante el uso de. AWS CloudFormation La solución cFCT ayuda a los clientes a configurar rápidamente un AWS entorno seguro y multicuenta basado en las AWS mejores prácticas. Ayuda a ahorrar tiempo al automatizar la configuración de un entorno para ejecutar cargas de trabajo seguras y escalables, al tiempo que implementa una base de seguridad inicial mediante la creación de cuentas y recursos. AWS Control Tower también proporciona un entorno básico para empezar con una arquitectura multicuenta, la gestión de identidades y accesos, la gobernanza, la seguridad de los datos, el diseño de redes y el registro. Las soluciones del repositorio AWS SRA proporcionan configuraciones de seguridad adicionales para implementar los patrones descritos en este documento.

Este es un resumen de las soluciones del repositorio de la AWS SRA. Cada solución incluye un `README.md` archivo con detalles.

- La solución CloudTrail Organization crea un registro de la organización dentro de la cuenta de administración de la organización y delega la administración en una cuenta de miembro, como la cuenta de auditoría o de herramientas de seguridad. Este registro se cifra con una clave gestionada por el cliente creada en la cuenta de Security Tooling y envía los registros a un depósito de S3 de la cuenta de Log Archive. Opcionalmente, los eventos de datos se pueden habilitar para Amazon S3 y AWS Lambda sus funciones. Un registro de la organización registra los eventos de todos Cuentas de AWS los miembros de la AWS organización e impide que las cuentas de los miembros modifiquen las configuraciones.
- La solución GuardDuty Organization permite a Amazon GuardDuty delegar la administración en la cuenta de Security Tooling. Se configura GuardDuty dentro de la cuenta Security Tooling para todas las cuentas de la AWS organización existentes y futuras. Los GuardDuty resultados también se cifran con una clave KMS y se envían a un bucket de S3 en la cuenta de Log Archive.
- La solución Security Hub CSPM Organization configura el Security Hub CSPM delegando la administración en la cuenta Security Tooling. Configura el Security Hub CSPM dentro de la cuenta Security Tooling para todas las cuentas de la organización existentes y futuras. AWS La solución también proporciona parámetros para sincronizar los estándares de seguridad habilitados en todas las cuentas y regiones, así como para configurar un agregador de regiones dentro de la cuenta de Security Tooling. La centralización de Security Hub CSPM en la cuenta Security Tooling proporciona una visión transversal del cumplimiento de las normas de seguridad y de las conclusiones de las integraciones tanto de terceros como de otras integraciones. Servicios de AWS AWS Partner
- La solución Inspector configura Amazon Inspector dentro de la cuenta del administrador delegado (Security Tooling) para todas las cuentas y regiones gobernadas por la organización. AWS
- La solución Firewall Manager configura las políticas de AWS Firewall Manager seguridad delegando la administración en la cuenta Security Tooling y configurando el Firewall Manager con una política de grupo de seguridad y varias políticas. AWS WAF La política de grupo de seguridad requiere un grupo de seguridad máximo permitido dentro de una VPC (existente o creada por la solución), que la solución implementa.
- La solución Macie Organization permite a Amazon Macie delegar la administración en la cuenta Security Tooling. Configura Macie dentro de la cuenta Security Tooling para todas las cuentas de la organización existentes y futuras. AWS Además, Macie está configurado para enviar los resultados de su descubrimiento a un depósito S3 central que está cifrado con una clave KMS.
- AWS Config:
  - La solución Config Aggregator configura un AWS Config agregador al delegar la administración en la cuenta de Security Tooling. A continuación, la solución configura un AWS Config agregador

dentro de la cuenta de Security Tooling para todas las cuentas existentes y futuras de la organización. AWS

  - La solución Conformance Pack Organization Rules se implementa al delegar la administración en la Reglas de AWS Config cuenta de Security Tooling. A continuación, crea un paquete de conformidad de la organización dentro de la cuenta de administrador delegado para todas las cuentas existentes y futuras de la AWS organización. La solución está configurada para implementar la plantilla de ejemplo del paquete de conformidad con las mejores prácticas operativas para el cifrado y la administración de claves.
  - La solución AWS Config Control Tower Management Account habilita AWS Config la cuenta de AWS Control Tower administración y actualiza el AWS Config agregador dentro de la cuenta de Security Tooling en consecuencia. La solución utiliza la AWS Control Tower CloudFormation plantilla de habilitación AWS Config como referencia para garantizar la coherencia con las demás cuentas de la AWS organización.
- IAM:
  - La solución Access Analyzer permite el uso de IAM Access Analyzer al delegar la administración en la cuenta Security Tooling. A continuación, configura un analizador de acceso IAM a nivel de organización dentro de la cuenta Security Tooling para todas las cuentas existentes y futuras de la organización. AWS La solución también implementa IAM Access Analyzer en todas las cuentas de los miembros y regiones para facilitar el análisis de los permisos a nivel de cuenta.
  - La solución de política de contraseñas de IAM actualiza la política de Cuenta de AWS contraseñas de todas las cuentas de una organización. AWS La solución proporciona parámetros para configurar los ajustes de la política de contraseñas a fin de ayudarle a cumplir con los estándares de conformidad del sector.
- La solución EC2 Default EBS Encryption permite el cifrado predeterminado de Amazon EBS a nivel de cuenta dentro de cada una Cuenta de AWS y Región de AWS dentro de la organización. AWS Aplica el cifrado de los nuevos volúmenes e instantáneas de EBS que cree. Por ejemplo, Amazon EBS cifra los volúmenes de EBS que se crean al lanzar una instancia y las instantáneas que se copian de una instantánea no cifrada.
- La solución S3 Block Account Public Access permite la configuración a nivel de cuenta de Amazon S3 dentro de cada miembro de Cuenta de AWS la AWS organización. La característica Block Public Access de Amazon S3 proporciona la configuración de los puntos de acceso, los buckets y las cuentas, con el fin de ayudarle a administrar el acceso público a los recursos de Amazon S3. De forma predeterminada, los buckets, puntos de acceso y objetos nuevos no permiten el acceso público. Sin embargo, los usuarios pueden modificar las políticas de bucket, las políticas de punto de acceso o los permisos de objeto para permitir el acceso público. La configuración de bloqueo

de acceso público de Amazon S3 anula estas políticas y permisos para que pueda limitar el acceso público a estos recursos.

- La solución Detective Organization automatiza la activación de Amazon Detective al delegar la administración en una cuenta (como la cuenta de auditoría o de herramientas de seguridad) y la configuración de Detective para todas las cuentas existentes y futuras. AWS Organizations
- La solución Shield Advanced automatiza la implementación AWS Shield Advanced para proporcionar una protección DDo S mejorada para sus aplicaciones en AWS.
- La solución AMI Bakery Organization ayuda a automatizar el proceso de creación y gestión de imágenes reforzadas y estándares de Amazon Machine Image (AMI). Esto garantiza la coherencia y la seguridad en todas sus AWS instancias y simplifica las tareas de implementación y mantenimiento.
- La solución Patch Manager ayuda a agilizar la administración de parches en múltiples Cuentas de AWS aplicaciones. Puede usar esta solución para actualizar el AWS Systems Manager agente (SSM Agent) en todas las instancias administradas y para escanear e instalar parches de seguridad y correcciones de errores críticos e importantes en las instancias etiquetadas para Windows y Linux. La solución también configura la configuración de administración de hosts predeterminada para detectar la creación de nuevas Cuentas de AWS soluciones e implementarlas automáticamente en esas cuentas.

Colaboradores

Autor principal:

- Avik Mukherjee, sénior de seguridad de SA AWS

Colaboradores:

- Jason Hurst, investigador sénior AWS de seguridad del CIRT
- Abhishek Panday, AWS gerente principal de productos de tecnología
- Itay Meller, especialista sénior de SA AWS
- Jonathan VanKim, AWS director de seguridad de SA
- Josh Du Lac, estratega de seguridad AWS empresarial
- James Thompson, arquitecto AWS sénior de soluciones
- Jeremy Girven, AWS especialista en SA
- Rodney Underkoffler, especialista sénior de SA AWS
- Farhan Farooq, arquitecto sénior de soluciones AWS
- Prashob Krishnan, gerente técnico de cuentas AWS
- Meg Peddada, consultora sénior de seguridad AWS
- Ashwin Phadke, arquitecto sénior de soluciones AWS
- Sowjanya Rajavaram, sénior de seguridad de SA AWS
- Tomek Jakubowski, consultor AWS sénior
- Arun Thomas, arquitecto de soluciones sénior AWS
- Ross Warren, arquitecto de soluciones de AWS productos
- Scott Conklin, consultor sénior AWS
- Ilya Epshteyn, gerente sénior de Identity Solutions AWS
- Michael Haken, tecnólogo principal AWS
- Mehial Mendrin, consultor sénior AWS
- Christopher Evensen, gerente técnico sénior de cuentas AWS

Revisando:

- Eric Rose, AWS director de seguridad de SA
- Manoj Kumar, AWS consultor de entregas

Redacción técnica:

- Handan Selamoglu, redactor técnico sénior AWS

Apéndice: servicios de AWS seguridad, identidad y cumplimiento

Influya en el futuro de la arquitectura de referencia de AWS seguridad (AWS SRA) realizando una breve encuesta.

Para obtener una introducción o un repaso, consulte Seguridad, identidad y conformidad en el AWS AWS sitio web para obtener una lista de los elementos Servicios de AWS que le ayudan a proteger sus cargas de trabajo y aplicaciones en la nube. Estos servicios se agrupan en cinco categorías: protección de datos, gestión de identidades y accesos, protección de redes y aplicaciones, detección de amenazas y supervisión continua, y cumplimiento y privacidad de los datos.

Protección de datos: AWS proporciona servicios que le ayudan a proteger sus datos, cuentas y cargas de trabajo del acceso no autorizado.

- Amazon Macie: descubra, clasifique y proteja los datos confidenciales con funciones de seguridad basadas en el aprendizaje automático.
- AWS KMS— Cree y controle las claves que se utilizan para cifrar sus datos.
- AWS CloudHSM— Administre sus módulos de seguridad de hardware (HSMs) en el Nube de AWS.
- AWS Certificate Manager— Aprovisione, administre e implemente SSL/TLS certificados para usarlos con Servicios de AWS.
- AWS Secrets Manager— Rote, gestione y recupere las credenciales de las bases de datos, las claves de API y otros datos secretos a lo largo de su ciclo de vida.

Gestión de identidades y accesos: los servicios de AWS identidad le permiten gestionar de forma segura las identidades, los recursos y los permisos a escala.

- IAM: controle de forma segura el acceso a los recursos Servicios de AWS y a los mismos.
- IAM Identity Center: administre de forma centralizada el acceso SSO a múltiples aplicaciones Cuentas de AWS y aplicaciones empresariales.
- Amazon Cognito: añada el registro, el inicio de sesión y el control de acceso de los usuarios a sus aplicaciones web y móviles.

- AWS Directory Service— Utilice Microsoft Active Directory administrado en Nube de AWS.
- AWS RAM— Comparta AWS recursos de forma sencilla y segura.
- AWS Organizations— Implemente una gestión basada en políticas para múltiples. Cuentas de AWS
- Permisos verificados de Amazon: administre permisos y autorizaciones escalables y detallados en sus aplicaciones personalizadas.

Protección de redes y aplicaciones: estas categorías de servicios le permiten aplicar una política de seguridad detallada en los puntos de control de la red de toda su organización. Servicios de AWS le ayudan a inspeccionar y filtrar el tráfico para evitar el acceso no autorizado a los recursos en los límites de host, red y aplicación.

- AWS Shield— Proteja sus aplicaciones web que se ejecutan con la protección S gestionada. AWS DDo
- AWS WAF— Proteja sus aplicaciones web de las vulnerabilidades web más comunes y garantice la disponibilidad y la seguridad.
- AWS Firewall Manager— Configure y gestione AWS WAF las reglas Cuentas de AWS y las aplicaciones desde una ubicación central.
- AWS Systems Manager— Configure y gestione Amazon EC2 y los sistemas locales para aplicar parches de sistema operativo, crear imágenes de sistemas seguros y configurar sistemas operativos seguros.
- Amazon VPC: aprovisione una sección aislada de forma lógica en la AWS que pueda lanzar AWS los recursos en una red virtual que usted defina.
- AWS Network Firewall— Implemente las protecciones de red esenciales para su. VPCs
- Firewall DNS Amazon Route 53: proteja sus solicitudes de DNS salientes de su VPCs.
- Acceso verificado de AWS— Proporcione un acceso seguro a sus aplicaciones sin necesidad de redes privadas virtuales (VPNs).
- Amazon VPC Lattice: simplifique la service-to-service conectividad, la seguridad y la supervisión.

Detección de amenazas y monitoreo continuo: los servicios de AWS monitoreo y detección proporcionan orientación para ayudar a identificar posibles incidentes de seguridad en su AWS entorno.

- AWS Security Hub CSPM— Vea y gestione las alertas de seguridad y automatice las comprobaciones de cumplimiento desde una ubicación central.
- AWS Security Hub— Correlacione y enriquezca los hallazgos de seguridad para priorizar los problemas de seguridad críticos en sus cuentas y Regiones de AWS.
- Amazon GuardDuty: proteja sus cargas de trabajo Cuentas de AWS y las suyas con la detección inteligente de amenazas y la supervisión continua.
- Amazon Inspector: automatice las evaluaciones de seguridad para ayudar a mejorar la seguridad y el cumplimiento de las aplicaciones en las que se despliegan AWS.
- AWS Config— Registre y evalúe las configuraciones de sus AWS recursos para permitir la auditoría de conformidad, el seguimiento de los cambios en los recursos y el análisis de seguridad.
- Reglas de AWS Config— Cree reglas que actúen automáticamente en respuesta a los cambios en su entorno, por ejemplo, aislando los recursos, enriqueciendo los eventos con datos adicionales o restaurando la configuración a un estado de funcionalidad comprobada.
- Respuesta frente a incidencias de seguridad de AWS— Automatice la respuesta, la investigación y la solución de los incidentes de seguridad con manuales y flujos de trabajo prediseñados.
- AWS CloudTrail— Realice un seguimiento de la actividad de los usuarios y del uso de las API para permitir la gobernanza y la auditoría operativa y de riesgos de su empresa. Cuenta de AWS
- Amazon Detective: analice y visualice los datos de seguridad para llegar rápidamente a la causa raíz de los posibles problemas de seguridad.
- AWS Lambda— Ejecute código sin aprovisionar ni administrar servidores para poder escalar su respuesta programada y automatizada a los incidentes.

Cumplimiento y privacidad de los datos: AWS le ofrece una visión completa de su estado de conformidad y supervisa continuamente su entorno mediante comprobaciones de conformidad automatizadas basadas en las AWS mejores prácticas y los estándares del sector que sigue su empresa.

- AWS Artifact— Utilice un portal de autoservicio gratuito para obtener acceso bajo demanda a los informes de AWS seguridad y cumplimiento y a determinados acuerdos en línea.
- AWS Audit Manager— Audite continuamente su AWS uso para simplificar la evaluación del riesgo y el cumplimiento de las normativas y los estándares del sector.

Historial del documento

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

Cambio	Descripción	Fecha
Reestructuración y actualizaciones del contenido	• Se agregó una guía para Security Hub y AWS Nitro Enclaves. • Reestructuró la AWS SRA para centrarse en la arquitectura principal y trasladó las secciones de análisis profundo a guías independientes para la gestión de identidades, la seguridad perimetral, la ciberciencia forense, la IA generativa y el IoT. • Se actualizó la guía existente para AWS CloudTrail incluir detalles adicionales sobre Amazon Detective AWS Firewall Manager, Amazon GuardDuty, IAM Access Analyzer AWS Shield Advanced, Amazon Security Lake y. AWS Config AWS Audit Manager	22 de diciembre de 2025
Actualizaciones importantes	• Se agregó información sobre la nueva administr	29 de agosto de 2025

ación centralizada del acceso de los usuarios raíz de IAM, las políticas de control de recursos (RCPs) y las políticas declarativas.

- El CSPM de Security Hub actualizado hace referenci a al nuevo Security Hub CSPM.
- Incluye nuevas funciones de servicio para Amazon GuardDuty y Security Hub CSPM.
- Se agregó una guía Respuesta frente a incidenci as de seguridad de AWS de servicio.
- Se actualizó la guía de análisis profundo de IAM para incluir VPC Lattice machine-to-machine para la gestión de identidades.
- Se agregó una nueva guía de análisis profundo: SRA para IoT.

Adiciones y aclaraciones	• En la sección de cuentas de Security Tooling, se actualizó la AWS KMS guía. • En la sección de administración de identidades de clientes, amplié la información sobre la autorización de API Gateway. • Se actualizó la sección de IA generativa para añadir una consideración de diseño al diseño de la OU y de la cuenta. • En la sección del repositorio de códigos de la AWS SRA, se agregó información sobre la nueva solución de administración de parches.	12 de septiembre de 2024

Actualizaciones importantes	• Se agregaron dos secciones para obtener una guía arquitectónica profunda: IA generativa con Amazon Bedrock y administración de identidades. • Se actualizaron las AWS Identity and Access Management Access Analyzer CloudFron tsecciones Amazon Detective AWS ArtifactAWS Config, Amazon Inspector AWS Security Hub CSPMhttps://docs.aws.amazon.com/prescriptive-guidance/latest/security-reference-architecture/security-tooling.html#tool-security-hub, Amazon Security Lake y Amazon con nuevas funciones de servicio. • Se actualizó la sección del repositorio de código AWS SRA para incluir la nueva opción de implementación de Terraform y la adición de soluciones AWS Shield Advanced AMI Bakery.	7 de junio de 2024

Actualizaciones importantes	• Se actualizaron las secciones Cuenta de red y Cuenta de aplicación para añadir una guía de arquitectura para Amazon Verified Permissions y Amazon VPC Lattice. Acceso verificado de AWS • Se agregó una guía arquitectónica detallada basada en la funcionalidad de seguridad. • Se han añadido nuevas directrices sobre cómo Servicios de AWS AI/ML utilizarlas para ofrecer mejores resultados de seguridad. • Se agregó una guía sobre cómo planificar la arquitectura de seguridad de forma gradual.	4 de noviembre de 2023
Adición a Security Lake	Se actualizaron las secciones de cuentas de Security Tooling y Log Archive para añadir una guía de diseño relacionada con Amazon Security Lake.	22 de septiembre de 2023

Actualizaciones menores	• Se actualizó la guía existente para reflejar Servicios de AWS las nuevas funciones y las mejores prácticas. • Guía arquitectónica actualizada para la AWS CloudTrail seguridad perimetral y perimetral. AWS IAM Identity Center	10 de mayo de 2023
Encuesta	Se agregó una breve encuesta para comprender mejor cómo se usa la AWS SRA en su organización.	14 de diciembre de 2022
Archivos fuente para diagramas de arquitectura de referencia	En la sección Arquitectura de referencia de AWS seguridad , se agregó un archivo de descarga que proporciona los diagramas de arquitectura de esta guía en PowerPoint formato editable.	17 de noviembre de 2022
Actualizaciones de la sección de fundamentos de la seguridad	En la sección Fundamentos de la seguridad, se actualizó la información sobre los pilares y los principios de diseño de seguridad del Well-Architected Framework.	27 de septiembre de 2022

Principales adiciones y actualizaciones	• Se agregó información sobre cómo usar la AWS SRA y las principales pautas de implementación. • Se agregó una guía de arquitectura para otros AWS Artifact, Servicios de AWS como Amazon Inspector AWS RAM, Amazon Route 53 AWS Control Tower, AWS Audit Manager, Directory Service, Amazon Cognito y Network Access Analyzer. • Se actualizó la guía existente para reflejar las nuevas Servicio de AWS funciones y las mejores prácticas.	25 de julio de 2022
—	Publicación inicial	23 de junio de 2021

AWS Glosario de orientación prescriptiva

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

Números

Las 7 R

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

- Refactorizar/rediseñar: traslade una aplicación y modifique su arquitectura mediante el máximo aprovechamiento de las características nativas en la nube para mejorar la agilidad, el rendimiento y la escalabilidad. Por lo general, esto implica trasladar el sistema operativo y la base de datos. Ejemplo: Migrar la base de datos de Oracle en las instalaciones a Amazon Aurora PostgreSQL-Compatible Edition.
- Redefinir la plataforma (transportar y redefinir): traslade una aplicación a la nube e introduzca algún nivel de optimización para aprovechar las capacidades de la nube. Ejemplo: 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: Migrar el sistema de administración de las relaciones con los clientes (CRM) a Salesforce.com.
- Volver a alojar (migrar mediante lift-and-shift): traslade una aplicación a la nube sin realizar cambios para aprovechar las capacidades de la nube. Ejemplo: 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

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.

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 AIOps se utiliza en la estrategia de AWS migración, consulte la guía de integración de operaciones.

cifrado asimétrico

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

atomicidad, consistencia, aislamiento, durabilidad (ACID)

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

control de acceso basado en atributos (ABAC)

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

implementación azul/verde

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 más información, consulte el indicador Implement break-glass procedures en la guía de AWS Well-Architected.

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.

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 CCo E 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: realizar inversiones fundamentales para escalar su adopción de la nube (p. ej., crear una landing zone, definir una CCo E, establecer un modelo de operaciones)

- Migración: migración de aplicaciones individuales
- Reinvención: optimización de productos y servicios e innovación en la nube

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

CMDB

Consulte 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 canalización de CI/CD puede utilizar varios repositorios.

caché en frío

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

datos fríos

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

visión artificial (CV)

Campo de la IA que utiliza el 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, compilación, 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 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.

defense-in-depth

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

administrador delegado

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

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

Implementación

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

entorno de desarrollo

Consulte entorno.

control de detección

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

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 ante desastres de cargas de trabajo en AWS: Recovery in the Cloud in the AWS Well-Architected Framework.

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. Este concepto lo introdujo Eric Evans en su libro, Diseño impulsado por el dominio: abordando la complejidad en el corazón del software (Boston: Addison-Wesley Professional, 2003). Para obtener información sobre cómo utilizar el diseño basado en dominios con el patrón de higos estranguladores, consulte Modernización gradual de los servicios web antiguos de Microsoft ASP.NET (ASMX) mediante contenedores y Amazon API Gateway.

DR

Consulte recuperación ante desastres.

Detección de 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. Los sistemas big-endianos almacenan primero el byte más significativo. Los sistemas Little-Endian 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 AWS PrivateLink y conceder permisos a otros Cuentas de AWS o a responsables AWS Identity and Access Management (de IAM). Estas cuentas o entidades principales pueden conectarse a su servicio de punto de conexión de forma privada

mediante la creación de puntos de conexión de VPC de interfaz. Para obtener más información, consulte Creación de un servicio de punto de conexión en la documentación de Amazon Virtual Private Cloud (Amazon VPC).

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, mediante el que los modelos aprenden a partir de ejemplos (pasos) incrustados en las peticiones. La técnica de peticiones con pocos pasos puede ser eficaz para las 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)

Una gran red neuronal de aprendizaje profundo que se ha estado entrenando con conjuntos de datos masivos de datos generalizados y sin etiquetar. FMs son capaces de realizar 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?

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 la sección Restringir la distribución geográfica del contenido en la CloudFront documentación.

Flujo de trabajo de Gitflow

Un enfoque en el que los entornos inferiores y superiores utilizan diferentes ramas en un repositorio de código fuente. El flujo de trabajo de Gitflow se considera heredado, 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 el cumplimiento en todas las unidades organizativas (OUs). Las barreras de protección preventivas aplican políticas para garantizar la alineación con los estándares de conformidad. Se implementan mediante políticas de control de servicios y límites de 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.

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.

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 de DevOps publicación típico.

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 más información, consulte la práctica recomendada Implementación mediante una infraestructura inmutable en el Marco de 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 AWS de referencia de seguridad recomienda configurar la cuenta de red con entradas, salidas e inspección VPCs para proteger la interfaz bidireccional entre la aplicación y el resto de Internet.

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

Término que introdujo Klaus Schwab en 2016 para referirse a la modernización de los procesos de fabricación mediante los avances en la conectividad, los datos en tiempo real, la automatización, el análisis, la IA y el 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 (T) IIo

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 de la Internet de las cosas (IIoT) industrial.

VPC de inspección

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

Internet de las cosas (IoT)

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

interpretabilidad

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

IoT

Consulte Internet de las cosas.

biblioteca de información de TI (ITIL)

Conjunto de prácticas recomendadas para ofrecer servicios de TI y alinearlos con los requisitos empresariales. 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 obtener más información, consulte Qué son. LLMs

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 para lo cual 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.

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 Framework.

cuenta de miembro

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

MES

Consulte sistema de ejecución de fabricación.

Message Queuing Telemetry Transport (MQTT)

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

microservicio

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

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

arquitectura de microservicios

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

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

Equipos multifuncionales que agilizan la migración de las cargas de trabajo mediante enfoques automatizados y ágiles. Los equipos de las fábricas de migración suelen incluir a analistas y propietarios de operaciones, empresas, 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 fiabilidad y la previsibilidad, el AWS Well-Architected Framework 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.

Open Process Communications: arquitectura unificada (OPC-UA)

Un protocolo de machine-to-machine comunicación (M2M) para la automatización industrial. OPC-UA establece un estándar de interoperabilidad con esquemas de autenticación, autorización y cifrado 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 más información, consulte Operational Readiness Reviews (ORR) en el Marco de AWS Well-Architected.

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 para todos los miembros 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 AWS KMS (SSE-KMS) y las solicitudes dinámicas `PUT` y `DELETE` dirigidas 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 AWS de referencia de seguridad recomienda configurar la cuenta de red con entradas, salidas e inspección VPCs para proteger la interfaz bidireccional entre la aplicación e Internet en general.

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

Un contenedor que contiene información sobre cómo desea que Amazon Route 53 responda a las consultas de DNS de un dominio y sus subdominios dentro de uno o más VPCs. 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 la sección 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)

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

punto de enlace de servicio

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.

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.

split-and-seed modelo

Un patrón para escalar y acelerar los proyectos de modernización. A medida que se definen las nuevas funciones y los lanzamientos de los productos, el equipo principal se divide para

crear nuevos equipos de productos. Esto ayuda a ampliar las capacidades y los servicios de su organización, mejora la productividad de los desarrolladores y apoya la innovación rápida. Para 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 con la aplicación de este patrón, consulte Modernización gradual de los servicios web antiguos de Microsoft ASP.NET (ASMX) mediante contenedores y Amazon API Gateway.

subred

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

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

Pares clave-valor que actúan como metadatos para organizar los recursos. AWS 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.

puerta de enlace de tránsito

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

flujo de trabajo basado en enlaces troncales

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

acceso de confianza

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

ajuste

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

equipo de dos pizzas

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

U

incertidumbre

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

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

Una conexión entre dos VPCs que le 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.