SUPERVISIÓN Y ANÁLISIS EN AWS

CONTENIDO

SUPERVISIÓN Y ANÁLISIS EN AWS

INTRODUCCIÓN

Para explicar los servicios de supervisión y análisis de AWS, continuaremos poniendo como ejemplo la cafetería, usado en clases anteriores.

Como propietario de la cafetería, quiero ver lo que sucede a lo largo del día, asegurándome de que las cosas funcionen correctamente. En la cafetería, veo que la gente está recibiendo sus cafés y las cosas en general se ven bien, pero no puedo quedarme sentado mirando cosas todo el día. Me gustaría irme y eventualmente, tal vez volver al final del día y poder validar cómo le fue a la tienda cuando no estaba. Por ejemplo, me gustaría saber cuántos cafés se han vendido hoy, cuánto fue el tiempo de espera promedio para alguien que ha ordenado un café. ¿Se nos habrá agotado el inventario de algo el día de hoy?
O aún mejor, me encantaría poder ser alertado automáticamente si los tiempos de espera se vuelven demasiado largos. De esa manera, podría llamar a otro empleado o colaborar yo mismo.

Todas las empresas, incluida esta cafetería, pueden usar métricas para medir qué también están funcionando los sistemas y los procesos.
Esta idea de observar sistemas, recopilar métricas, evaluar esas métricas y a lo largo del tiempo, luego usarlas para tomar decisiones o tomar acciones, es lo que llamamos ***supervisión***.

Es importante configurar supervisión en la nube. Con la naturaleza elástica de los servicios de AWS que escalan de forma dinámica vertical y horizontalmente, querrá estar al tanto de sus recursos de AWS para garantizar que los sistemas funcionen según lo previsto.
Por ejemplo, si una instancia de EC2 está siendo sobre utilizada, puede desencadenar un evento de escalado que iniciaría automáticamente otra instancia de EC2. O si una aplicación comienza a enviar respuestas de error a un ritmo inusualmente alto, puede alertar a un empleado para que eche un vistazo a lo que está pasando.

En esta clase veremos una variedad de herramientas que lo ayudarán a supervisar su entorno de AWS. Esta supervisión ayudará a medir cómo funcionan los sistemas, alertará cuando las cosas no van bien e incluso le ayudará a depurar y solucionar problemas a medida que aparecen.

AMAZON CLOUDWATCH

Amazon CloudWatch es un servicio que supervisa las aplicaciones, responde a los cambios de rendimiento, optimiza el uso de los recursos y proporciona información sobre el estado operativo. Al recopilar datos en todos los recursos de AWS, CloudWatch brinda visibilidad del rendimiento de todo el sistema y permite a los usuarios configurar alarmas, reaccionar automáticamente a los cambios y obtener una visión unificada del estado operativo.

Ahora estamos preparando mucho café, atendemos a los clientes y todo parece ir bien en nuestra cafetería. Pero a medida que usamos cada vez más las máquinas de café expreso, usamos tazas, abrimos y cerramos constantemente la nevera, quisiéramos asegurarnos de que estaremos alerta ante algo que podría haber salido mal. Tal vez sea necesario limpiar o reparar una máquina de café expreso.

El punto es que, como propietario de un negocio, necesita visibilidad del estado de sus sistemas. ¿Las cosas funcionan correctamente? ¿Hay algún cliente con una mala experiencia? ¿Con frecuencia se entrega la bebida equivocada a los clientes? ¿Todos reciben sus pedidos como se esperaba? Usted tendrá tantos tipos de preguntas relacionadas al éxito de sus operaciones. Y esta misma idea aplica a los sistemas creados en AWS. Necesita una forma de supervisar el estado y las operaciones de sus soluciones. Por suerte, no necesita crear su propia plataforma de supervisión, AWS hace eso por usted.

Amazon CloudWatch le permite supervisar su infraestructura de AWS y las aplicaciones que ejecuta en AWS en tiempo real.
CloudWatch funciona mediante el seguimiento y la supervisión de métricas. Piense en las métricas como variables vinculadas a los recursos. Por ejemplo, la cantidad de expresos que hace la máquina de café expreso o el uso de CPU de una instancia de EC2.
Tomemos un enfoque de cliente para nuestra cafetería. Supongamos que tenemos una máquina de café expreso y necesitamos limpiarla después de hacer 100 expresos. CloudWatch nos permitirá crear una métrica personalizada llamada "Contador de Expresos". Y una vez que llegue a 100, queremos alertar al personal para que limpie la máquina. Simple, ¿no?

Bueno, con CloudWatch, puede lograr esto creando lo que se llama alarma de CloudWatch. Usted establece un umbral para una métrica y cuando se alcanza, CloudWatch puede generar una alerta y detonar una acción. Esto significa que podemos alertar sobre la métrica personalizada, en este caso, llegar a 100 y, a continuación, realizar una acción.

ALARMAS DE CLOUDWATCH

Con CloudWatch, puede crear alarmas que realicen acciones de forma automática si el valor de su métrica superó o es inferior a un umbral predefinido.

Por ejemplo, imagine que los desarrolladores de su empresa utilizan instancias de Amazon EC2 con fines de desarrollo o pruebas de aplicaciones. Si los desarrolladores olvidan ocasionalmente detener las instancias, las instancias se seguirán ejecutando e incurrirán en cargos.

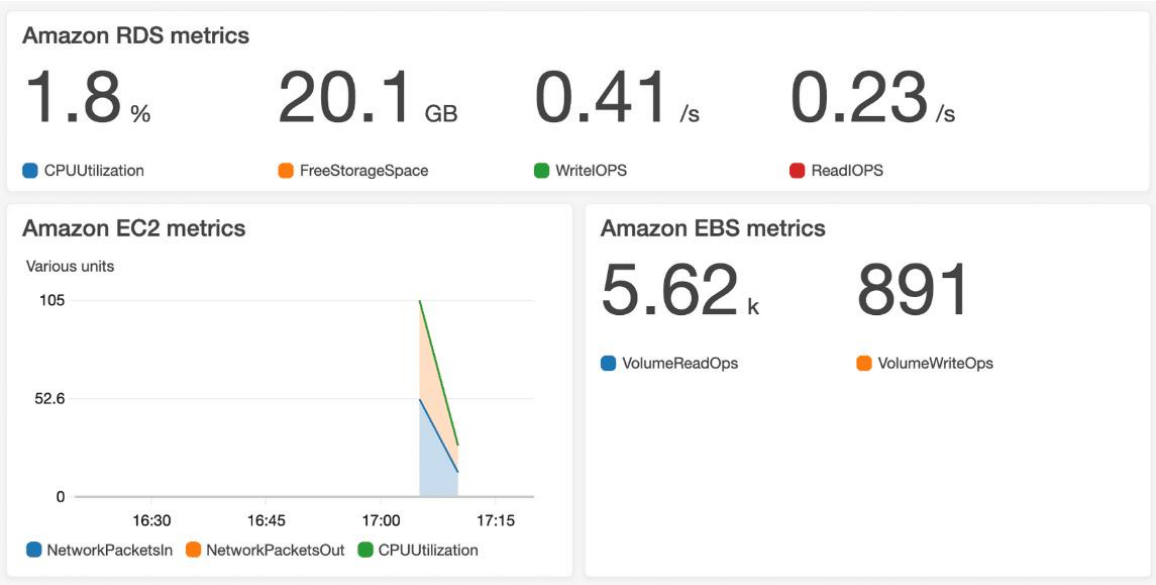
En este escenario, podría crear una alarma de CloudWatch que detenga de forma automática una instancia de Amazon EC2 cuando el porcentaje de utilización de la CPU se mantuvo por debajo de un determinado umbral durante un periodo determinado. Al configurar la alarma, puede especificar que se reciba una notificación cada vez que se active esta alarma.

Aún mejor, las alarmas de CloudWatch están integradas con SNS. Así que podemos enviar un mensaje de texto al administrador para decirle que limpie la máquina.
Puede crear todo tipo de alarmas personalizadas para métricas de todos los diferentes tipos de recursos en AWS.

PANEL DE CLOUDWATCH

Ahora, ¿qué pasa si queremos agregar todas esas métricas en un solo panel de monitoreo? Bueno, podemos usar la función de panel de CloudWatch. Piense en un panel como una pantalla que enumera las métricas casi en tiempo real. En nuestro caso, podemos crear un panel de CloudWatch que nos mostrará todas nuestras máquinas de café expreso y sus conteos de café para que podamos supervisarlas de manera proactiva. Los paneles se actualizarán automáticamente cuando están abiertos para que podamos observar una vista actualizada de nuestros recursos.

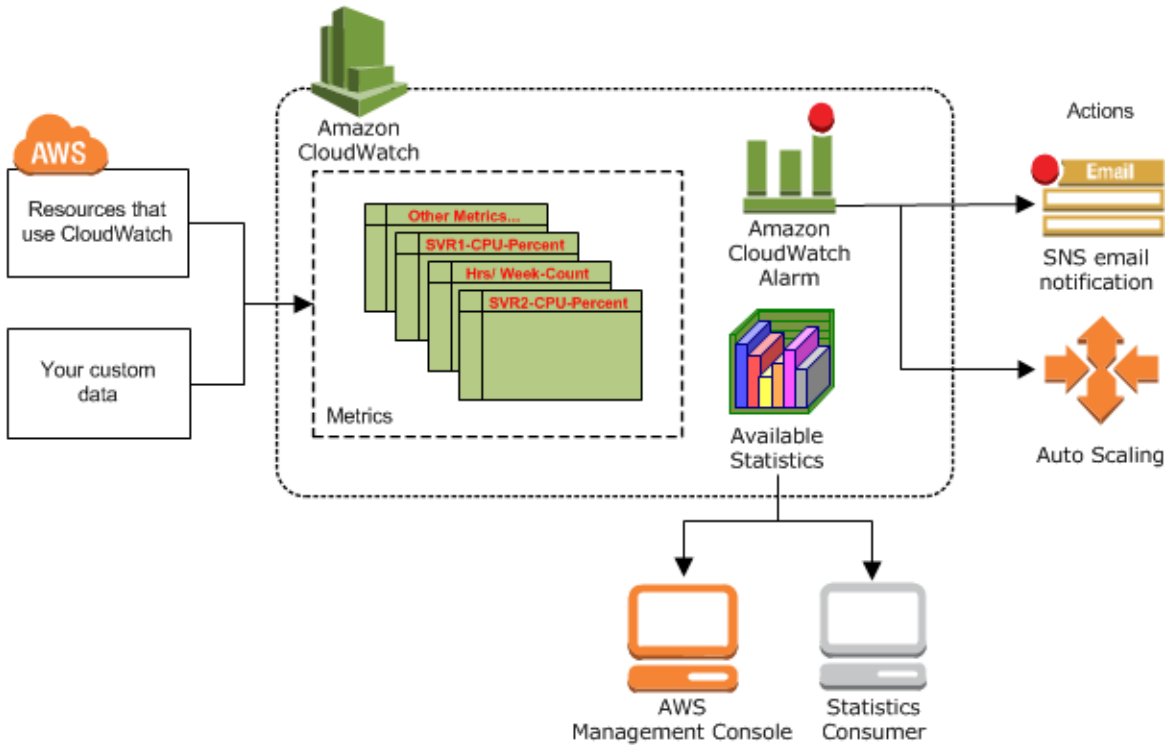
La función de panel de CloudWatch le permite acceder a todas las métricas de los recursos desde una única ubicación. Por ejemplo, puede utilizar un panel de CloudWatch para supervisar el uso de la CPU de una instancia de Amazon EC2, el número total de solicitudes realizadas a un bucket de Amazon S3 y mucho más. Incluso puede personalizar paneles independientes para distintos fines empresariales, aplicaciones o recursos.



FUNCIONAMIENTO DE AMAZON CLOUDWATCH

Amazon CloudWatch es un servicio web que le permite supervisar y administrar diversas métricas y configurar acciones de alarma en función de los datos de esas métricas.
CloudWatch utiliza métricas para representar los puntos de datos de los recursos. Los servicios de AWS envían métricas a CloudWatch. Luego, CloudWatch utiliza estas métricas para crear gráficos automáticamente que muestran cómo ha cambiado el rendimiento a lo largo del tiempo.

Amazon CloudWatch es básicamente un repositorio de métricas. Un servicio de AWS, como Amazon EC2, coloca las métricas en el repositorio, lo que logrará que recupere las estadísticas en función de dichas métricas. Si coloca sus propias métricas personalizadas en el repositorio, puede recuperar estadísticas sobre estas métricas también.



Puede utilizar las métricas para calcular estadísticas y, a continuación, presentar los datos gráficamente en la consola de CloudWatch.

Puede configurar acciones de alarma para detener, comenzar o terminar una instancia de Amazon EC2 cuando se cumplen determinados criterios. Por ejemplo, puede crear alarmas que inicien acciones de Amazon EC2 Auto Scaling y Amazon Simple Notification Service (Amazon SNS) en su nombre.

Los recursos de informática en la nube de se alojan en centros de datos de alta disponibilidad. Para proporcionar más escalabilidad y fiabilidad, cada instalación de centro de datos se encuentra en una zona geográfica específica, conocida como región. Cada región está diseñada para estar totalmente aislada de las demás regiones, para lograr la máxima estabilidad y aislamiento en caso de error. Las métricas se almacenan por separado en las Regiones, pero puede utilizar la funcionalidad para diversas regiones de CloudWatch para agregar estadísticas de diferentes Regiones.

VENTAJAS DE AMAZON CLOUDWATCH

Por último, ¿cuáles son las ventajas de utilizar un servicio como CloudWatch? Bueno, la primera es que puede ***tener acceso a todas las métricas desde una ubicación central***. Le permitirá recopilar métricas y registros de todos los recursos aplicaciones y servicios de AWS que se ejecutan tanto en AWS, así como en sus centros de datos.
Esto le ayuda a romper los silos y que pueda obtener fácilmente visibilidad en todos los sistemas.

También puede ***obtener visibilidad de sus aplicaciones, infraestructura y servicios***, lo que significa que obtendrá información de todo el conjunto distribuido para correlacionar y visualizar métricas y registros con el fin de localizar y resolver problemas rápidamente.

Esto, a su vez, significa que puede ***reducir el tiempo promedio de resolución, o MTTR, y mejorar el costo total de propiedad, o TCO***. Así que, en nuestra cafetería, si el MTTR de horas de limpieza de las máquinas de restaurante es más corto, entonces podemos ahorrar en TCO con ellas.
Esto se traduce en la liberación de recursos importantes, como los desarolladores, permitiéndoles centrarse así en agregar valor empresarial.

Por último, puede ***generar información para optimizar aplicaciones y recursos operativos***. Por ejemplo, agregando el uso de toda una flota de instancias de EC2 para obtener información operativa y sobre el uso.

Y ahora nuestro personal puede centrarse en servir café en lugar de limpiar todo el tiempo las máquinas antes de que llegue el momento de limpiarlas.

CASOS DE USO DE AMAZON CLOUDWATCH

Supervise el rendimiento de las aplicaciones: Visualice los datos de rendimiento, cree alarmas y correlacione datos para comprender y resolver la causa raíz de los problemas de rendimiento en sus recursos de AWS.

Realice un análisis de la causa raíz: Analice las métricas, los registros, el análisis de registros y las solicitudes de los usuarios para acelerar la depuración y reducir el tiempo medio general de resolución.

Optimice los recursos de forma proactiva: Automatice la planificación de recursos y reduzca los costos mediante la configuración de acciones que se producirán cuando se alcancen los umbrales en función de sus especificaciones o modelos de aprendizaje automático.

Pruebe los impactos en el sitio web: Averigüe exactamente cuándo se ve afectado su sitio web y durante cuánto tiempo viendo capturas de pantalla, registros y solicitudes web en cualquier momento.

AWS CLOUDTRAIL

AWS CloudTrail es un servicio de AWS que le ayuda a habilitar la auditoría operativa y de riesgos, la gobernanza y el cumplimiento de sus normas en su cuenta de AWS.

Las acciones realizadas por un usuario, un rol o un servicio de AWS se registran como eventos en CloudTrail. La información registrada incluye la identidad de quien llama a la API, la hora de la llamada a la API, la dirección IP de origen de quien llama a la API y más.
Puede pensar en CloudTrail como un "rastro" de migas de pan (o un registro de acciones) que alguien dejó atrás.
Con CloudTrail, puede ver un historial completo de la actividad de los usuarios y las llamadas a la API de las aplicaciones y recursos.

CloudTrail está activo en su cuenta de AWS cuando la crea. Cuando se produce una actividad en su cuenta de AWS, esa actividad se registra en un evento de CloudTrail.
Por lo general, los eventos se actualizan en CloudTrail dentro de un periodo de 15 minutos después de una llamada API. Puede filtrar los eventos especificando la hora y la fecha en que se produjo una llamada a la API, el usuario que solicitó la acción, el tipo de recurso que participó en la llamada a la API y mucho más.

Volvamos a la cafetería: La caja registradora es uno de los primeros dispositivos de auditoría personal del mundo. El principio es simple: Confiar, pero verificar.
Imagine que tiene toda su tienda gestionada por un empleado en el que confía, pero quiere asegurarse de que el efectivo de la caja coincida con las ventas reales, entonces todas las transacciones se registran y se contabilizan. Así, al final del día, sabe exactamente lo que debería haber ahí.
Poder auditar transacciones en TI es un elemento crítico en la mayoría de las estructuras de cumplimiento, pero en un centro de datos físicos, hay tantos lugares donde una persona puede, incluso por accidente, hacer cambios sin que se consigne ningún registro de ese cambio. En AWS, el problema desaparece porque todo es programático.

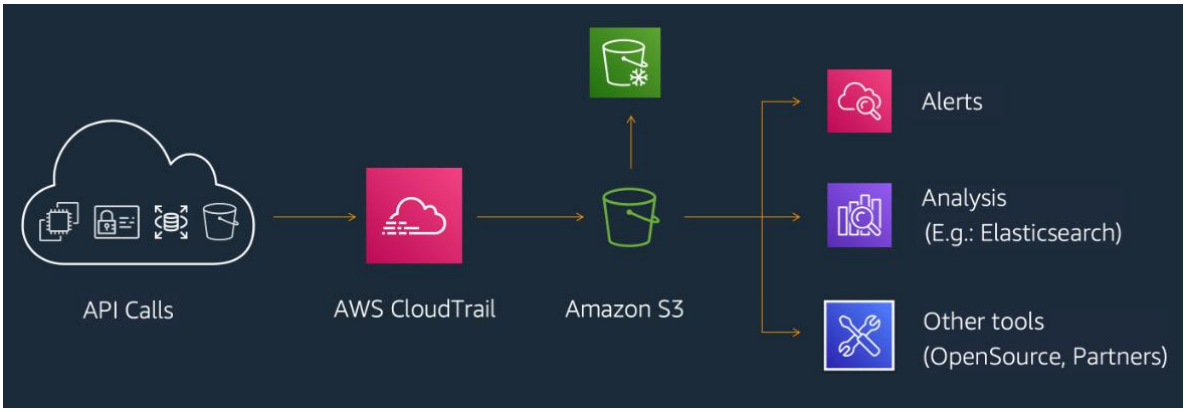
AWS CloudTrail es la herramienta completa de auditoría de APIs. El motor es sencillo, cada solicitud hecha a AWS, no importa si va a lanzar una instancia de EC2 o agregar una fila a una tabla de DynamoDB o cambiar los permisos de un usuario, cada una de las solicitudes se registran en el motor de CloudTrail.
El motor registra exactamente quién hizo la solicitud, qué operador y cuándo enviaron la llamada API, dónde estaban, cuál era la dirección IP, cuál fue la respuesta, si ha cambiado algo, cuál es el estado nuevo, si se denegó la solicitud.
Desde el punto de vista de auditoría, esto es fantástico.

Imagine que está tratando con un auditor que está comprobando que nadie desde el exterior pueda acceder a su base de datos. Está bien crear un grupo de seguridad que bloquee el tráfico externo, pero recuerde que un administrador de usuario raíz todavía tiene permisos para cambiar esa configuración, ¿verdad? Bueno, ¿cómo le demuestra al auditor que la configuración del grupo de seguridad nunca cambió? La respuesta es CloudTrail.

Posteriormente, CloudTrail puede guardar esos registros indefinidamente en buckets seguros de S3.

FUNCIONAMIENTO DE AWS CLOUDTRAIL

El funcionamiento de AWS CloudTrail es sencillo. Una vez activado, comienza a registrar automáticamente todas las llamadas API. Estos logs, conocidos como eventos, se almacenan y entregan en un bucket Amazon S3 especificado. Cada archivo de registro contiene uno o varios eventos. El usuario puede acceder a estos registros en cualquier momento para revisarlos o analizarlos.



BENEFICIOS DE AWS CLOUDTRAIL

Trazabilidad: CloudTrail permite conocer las actividades de los usuarios mediante el registro de la actividad realizada en su cuenta. CloudTrail registra información importante sobre cada acción, incluido quién ha efectuado la solicitud, qué servicios se han utilizado, qué acción se ha realizado, los parámetros de las acciones y los elementos de la respuesta enviada por el servicio de AWS. Esta información le ayuda a realizar un seguimiento de los cambios que se producen en los recursos de AWS y a solucionar problemas operativos.

Conformidad: CloudTrail lo ayuda a demostrar la conformidad, mejorar la posición de seguridad y consolidar los registros de actividad en todas las regiones y cuentas.
CloudTrail facilita la tarea de garantizar la conformidad con las políticas internas y los estándares regulatorios.

Agregue y consolide eventos de múltiples fuentes: Con CloudTrail Lake, puede recopilar eventos de actividad de AWS y de fuentes externas a AWS, incluidos otros proveedores de nube, aplicaciones internas y aplicaciones SaaS que se ejecutan en la nube o en las instalaciones.

Almacene de forma inmutable eventos dignos de auditoría: En AWS CloudTrail Lake, puede almacenar de forma inmutable eventos dignos de auditoría. Genere de forma sencilla los informes de auditoría que exigen las políticas internas y las normativas externas.

Obtenga información y analice actividades inusuales: Detecte el acceso no autorizado y analice los registros de actividad con Amazon Athena o con consultas basadas en SQL. Ahora es aún más fácil gracias a la generación de consultas en lenguaje natural (versión preliminar), la cual utiliza tecnología de IA generativa, para los usuarios con menos experiencia en la redacción de consultas SQL o CloudTrail. Responda con alertas de EventBridge basadas en reglas y flujos de trabajo automatizados.

CASOS DE USO DE AWS CLOUDTRAIL

Cumplimiento y auditoría: Proteja su organización de cualquier penalidad mediante el uso de registros de CloudTrail de modo que se demuestre la conformidad con las distintas normativas, como SOC, PCI e HIPAA.

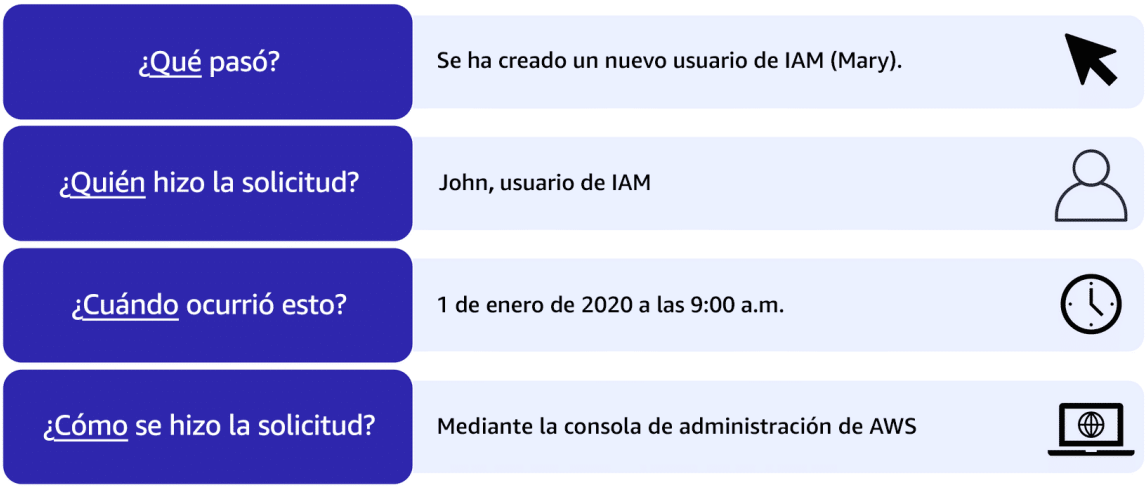
Seguridad: Mejore la posición de seguridad mediante el registro de las actividades y los eventos de los usuarios, y configure reglas de flujos de trabajo automatizadas con Amazon EventBridge.

Operaciones: Responda a las preguntas operativas, facilite la depuración e investigue problemas como la limitación de velocidad con las consultas basadas en SQL, la generación de consultas en lenguaje natural, Amazon Athena o la visualización de las tendencias con paneles en CloudTrail Lake.

EJEMPLO: EVENTO DE AWS CLOUDTRAIL

Supongamos que el propietario de la cafetería navega por la sección AWS Identity and Access Management (IAM) de la consola de administración de AWS. Descubren que se creó un nuevo usuario de IAM llamado Mary, pero no saben quién, cuándo ni qué método creó el usuario.

Para responder a estas preguntas, el propietario se desplaza a AWS CloudTrail:



En la sección Historial de eventos de CloudTrail, el propietario aplica un filtro para mostrar solo los eventos de la acción de API “CreateUser” (Crear usuario) en IAM. El propietario localiza el evento de la llamada a la API que creó un usuario de IAM para Mary. Este registro de eventos proporciona detalles completos sobre lo que ocurrió:

El 1 de enero de 2020 a las 9:00 a. m., el usuario de IAM John creó un nuevo usuario de IAM (Mary) a través de la consola de administración de AWS.

AWS TRUSTED ADVISOR

AWS Trusted Advisor lo ayuda a optimizar los costos, aumentar el rendimiento, mejorar la seguridad y la resiliencia, y operar a escala en la nube. Trusted Advisor evalúa continuamente su entorno de AWS mediante comprobaciones de prácticas recomendadas en las categorías de optimización de costos, rendimiento, resiliencia, seguridad, excelencia operativa y límites de servicio de la nube, y recomienda medidas para corregir cualquier desviación de las prácticas recomendadas.

Realiza en tiempo real una serie de comprobaciones para cada pilar en su cuenta, según las prácticas recomendadas de AWS y para las verificaciones de cada categoría, Trusted Advisor ofrece una lista de acciones recomendadas y recursos adicionales para obtener más información sobre las prácticas recomendadas de AWS.

Además, categoriza y agrupa elementos para que pueda verlos directamente en la consola de AWS. Algunas comprobaciones son gratuitas y ya se incluyen en su cuenta de AWS. Otras estarán disponibles en función del nivel de su plan de soporte. Un ejemplo de comprobación es que, si no tiene activada la autenticación multifactor para el usuario raíz, Trusted Advisor se lo hará saber.

Todos los planes de cuentas de AWS tienen acceso a 56 comprobaciones de AWS Trusted Advisor. A partir de Business Support y superior se desbloquean 426 comprobaciones adicionales, lo que suma un total de 482 comprobaciones de Trusted Advisor.

Al dirigir un negocio, es posible que necesite algunos asesores que puedan entrar desde afuera y decir: "Hey, este proceso se tendría que simplificar", o: "Tengo algunos buenos consejos sobre cómo ahorrar dinero en los gastos generales", o incluso: "Noté que puedo entrar, ir a la caja registradora y abrir el cajón sin que nadie se diera cuenta".
A veces es bueno tener a alguien que conozca las prácticas recomendadas de la industria y sepa qué buscar, entrar y le diga lo que se necesita cambiar para funcionar de manera más eficiente, estar más protegido o ahorrar algo de dinero. AWS tiene un asesor automatizado denominado AWS Trusted Advisor.

Si tiene instancias de EC2 subutilizadas que podrían apagarse para ahorrar dinero, o si tiene volúmenes de EBS de los que no se haya hecho respaldos en un tiempo razonable, también se lo hará saber.

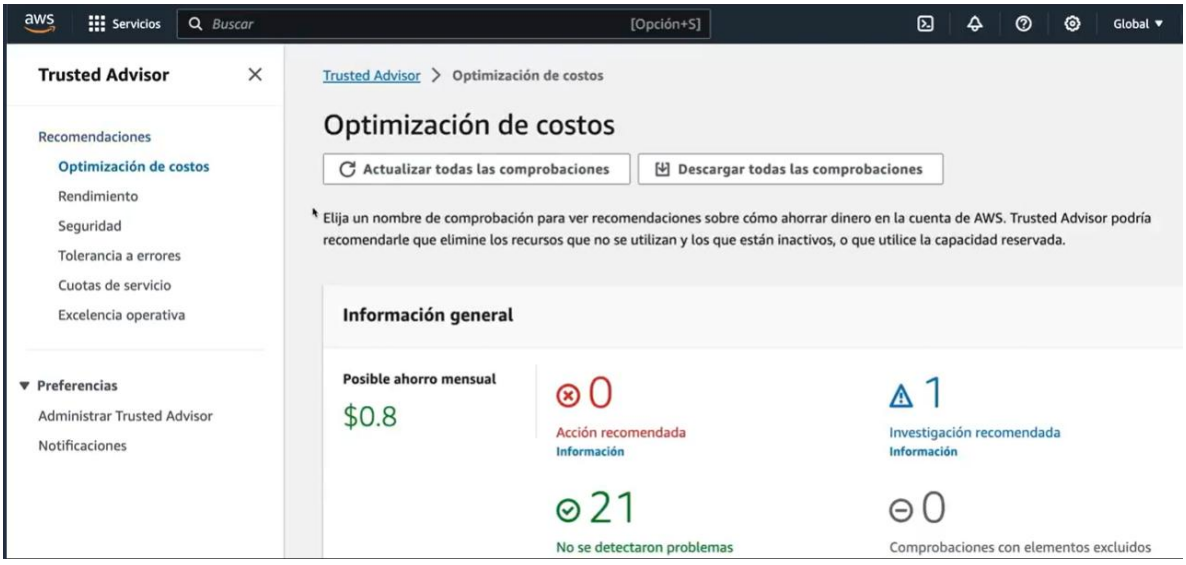
El asesoramiento que proporciona AWS Trusted Advisor puede beneficiar a su empresa en todas las etapas de la implementación. Por ejemplo, puede utilizar AWS Trusted Advisor para ayudarle a crear nuevos flujos de trabajo y desarrollar nuevas aplicaciones. También, puede utilizarlo cuando realiza mejoras continuas en las aplicaciones y los recursos existentes.

PANEL DE TRUSTED ADVISOR

Al acceder al panel de Trusted Advisor en la consola de administración de AWS, puede revisar las comprobaciones completadas de optimización de costos, rendimiento, seguridad, tolerancia a errores y límites de servicio.
Para cada categoría:

- La marca de comprobación verde indica el número de elementos para los que no se detectaron problemas.
- El triángulo naranja representa el número de investigaciones recomendadas.
- El círculo rojo representa el número de acciones recomendadas.

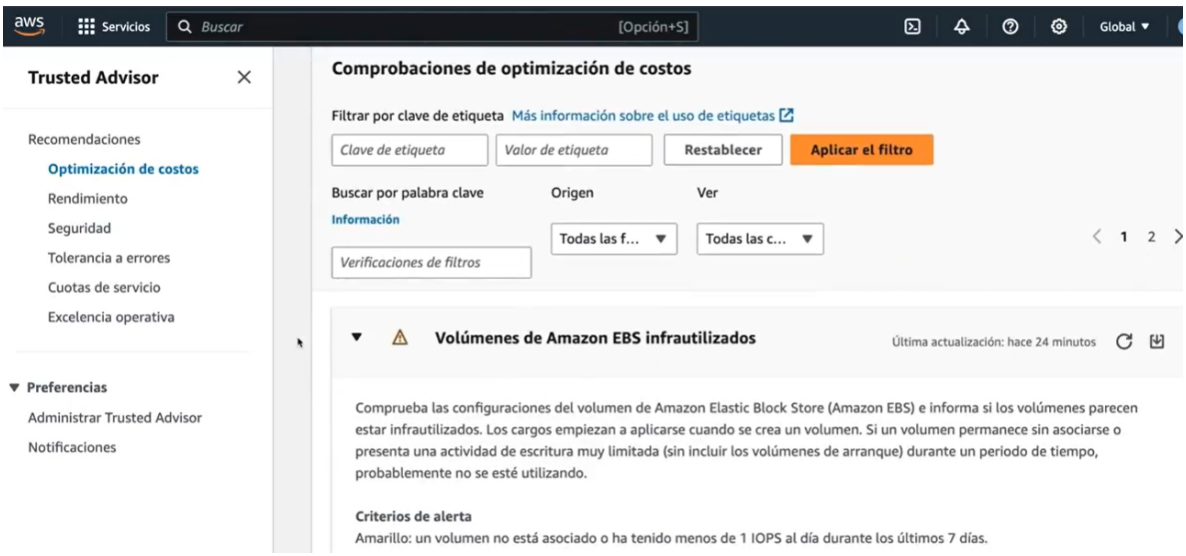
Así se ve el panel de AWS Trusted Advisor, en la consola de AWS:



En este caso, dando clic en el pilar de optimización de costos, podemos ver de inmediato que me muestra tres niveles de elementos: Está el círculo rojo, lo que significa que se recomienda una acción, el triángulo naranja, lo que significa que se recomienda una investigación y el cuadrado verde, lo que significa que no se detectaron problemas.

Aquí, por suerte, no tenemos ningún elemento rojo para la optimización de costos, pero tenemos algunos elementos naranjas. En las comprobaciones de optimización de costos, podemos leer más sobre cada comprobación que ejecutó Trusted Advisor.

En esta cuenta, hay volúmenes de EBS infrautilizados. Podríamos decidir reducir estas instancias verticalmente para ahorrar en costos, o si no se están utilizando podríamos decidir eliminar esas instancias y esos volúmenes de EBS. Sería necesario investigar un poco para determinar qué hacer aquí.



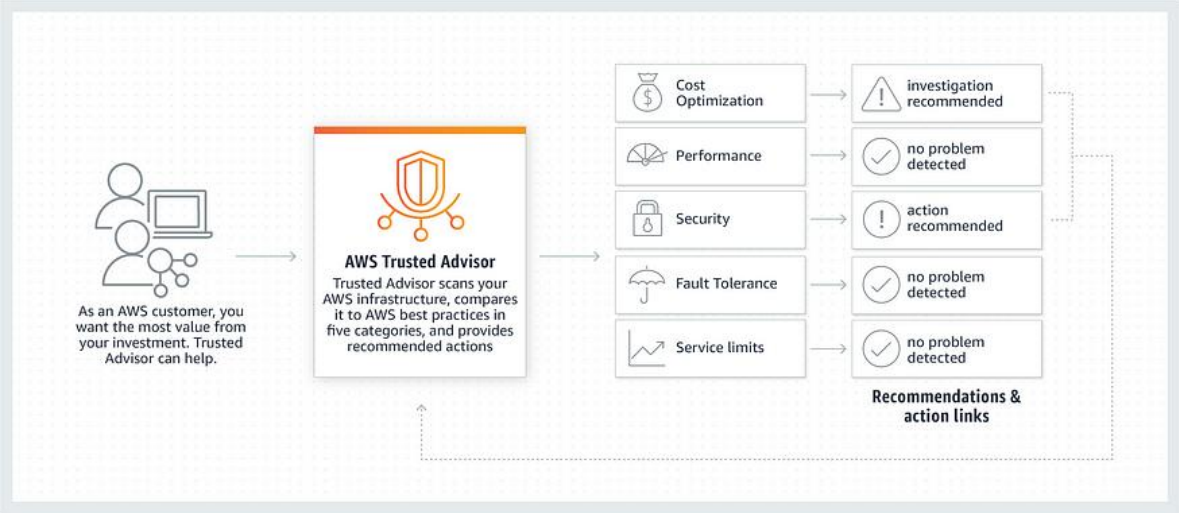
Ahora, si seleccionamos el pilar de Seguridad en esta cuenta de demostración, podemos ver que hay cuatro alertas que se encuentran en el nivel de acción recomendada:

Trusted Advisor está intentando avisarnos que tenemos políticas de contraseñas débiles para los usuarios de IAM, la autenticación multifactor no está activada para el usuario raíz, y que hay grupos de seguridad que permiten el acceso público a instancias de EC2. Todos estos elementos ponen en riesgo los recursos de esta cuenta y deben resolverse lo antes posible:

Asegúrese de haber activado Trusted Advisor para que también pueda empezar a tomar medidas para optimizar su cuenta de AWS.

FUNCIONAMIENTO DE AWS TRUSTED ADVISOR

AWS Trusted Advisor es un servicio de AWS que proporciona recomendaciones personalizadas para optimizar y mejorar tu infraestructura en la nube. Utiliza datos de tu cuenta de AWS para realizar un análisis proactivo y ofrecerte consejos sobre cómo mejorar la seguridad, la confiabilidad, el rendimiento y los costos de tu entorno.



Las recomendaciones de AWS Trusted Advisor se basan en las mejores prácticas de AWS y en la experiencia acumulada en la gestión de miles de cuentas de clientes. El servicio realiza un análisis constante de tu cuenta de AWS y te proporciona informes que contienen alertas y sugerencias para abordar posibles problemas o ineficiencias en tu configuración.

AWS Trusted Advisor proporciona recomendaciones en las siguientes áreas:

1. **Cost Optimization (Optimización de costos):** Ofrece consejos para optimizar tus recursos de AWS y reducir los gastos. Puede sugerir instancias de EC2 con menor costo, eliminar recursos infrautilizados o recomendar reservas de instancias para ahorrar en costos a largo plazo.

2. **Performance (Rendimiento):** Proporciona recomendaciones para mejorar el rendimiento de tus aplicaciones y recursos de AWS. Puede sugerir ajustes en configuraciones o recomendaciones para equilibrar la carga de trabajo.

3. **Security (Seguridad):** Identifica posibles problemas de seguridad en tu entorno y ofrece recomendaciones para mejorar la protección y mitigar riesgos. Puede sugerir el uso de políticas de acceso más estrictas, la configuración de autenticación de múltiples factores o la habilitación de cifrado. Por ejemplo, sus inspecciones incluyen controles de seguridad, como depósitos de Amazon S3 con permisos de acceso abierto.

4. **Fault Tolerance (Tolerancia a fallos):** Ofrece recomendaciones para mejorar la disponibilidad y la resistencia a fallos en tu infraestructura. Puede sugerir el uso de grupos de Auto Scaling, la distribución de cargas de trabajo en múltiples zonas de disponibilidad o la configuración de alarmas de CloudWatch.

5. **Service Limits (Límites de servicio):** Monitorea tus límites de servicio y te alerta cuando te estás acercando a los límites máximos de los servicios de AWS. Esto te ayuda a evitar problemas de rendimiento y planificar el escalado adecuado de tus recursos.

AWS Trusted Advisor está disponible en diferentes niveles de soporte de AWS y proporciona informes detallados que te ayudan a tomar decisiones informadas para optimizar tus operaciones en la nube.

BENEFICIOS DE AWS TRUSTED ADVISOR

Siga las prácticas recomendadas de AWS: Identifique desviaciones respecto a las prácticas recomendadas de AWS y descubra las medidas recomendadas para corregirlas.

Priorice las recomendaciones importantes: Las recomendaciones priorizadas de su equipo de cuentas de AWS, basadas en sus prioridades empresariales, las aplicaciones críticas y la urgencia de la recomendación, están disponibles para los clientes de Enterprise Support.

Optimice la colaboración en toda su organización: Consiga una mejor alineación en sus equipos mediante una mayor visibilidad, supervisión y seguimiento de las recomendaciones priorizadas, disponibles para los clientes de Enterprise Support.

Optimice sus recursos de AWS a escala: Obtenga una vista agregada de las recomendaciones de toda su organización o intégrelas mediante programación con las API de Trusted Advisor.

CASOS DE USO DE AWS TRUSTED ADVISOR

Optimice los costos y la eficiencia: Identifique los recursos no utilizados y las oportunidades para reducir sus costos. Evalúe su entorno de AWS y tome medidas para optimizar de forma continua la eficiencia.

Solucione brechas de seguridad: Evalúe su entorno de AWS con respecto a los estándares de seguridad y las prácticas recomendadas.

Mejore el rendimiento: Analice el uso y la configuración de su entorno de AWS para mejorar la velocidad y la capacidad de respuesta de sus aplicaciones.

Mejore la resiliencia: Examine su entorno de AWS para comprobar si hay deficiencias de redundancia y recursos sobre utilizados.

Realice un seguimiento de los límites de servicio: Compruebe el uso de la cuenta y reciba notificaciones cuando la cuenta se acerque o supere los límites de servicio.

CARACTERÍSTICAS DE AWS TRUSTED ADVISOR

Algunas de las características clave de AWS Trusted Advisor son:

Recomendaciones personalizadas: AWS Trusted Advisor analiza los datos de tu cuenta de AWS y proporciona recomendaciones específicas y personalizadas basadas en las necesidades y el uso de tus recursos.

Mejores prácticas de AWS: Las recomendaciones de Trusted Advisor se basan en las mejores prácticas de AWS, lo que garantiza que las sugerencias sean confiables y alineadas con los estándares de seguridad, rendimiento y optimización de AWS.

Análisis continuo: Trusted Advisor realiza un análisis constante y proactivo de tu cuenta de AWS para identificar oportunidades de mejora y posibles problemas en tiempo real.

Categorías de recomendaciones: Trusted Advisor proporciona recomendaciones en varias categorías importantes, incluyendo optimización de costos, rendimiento, seguridad, tolerancia a fallos y límites de servicio.

Alertas y notificaciones: Cuando se detectan problemas o se generan recomendaciones, Trusted Advisor puede enviar notificaciones y alertas por correo electrónico, lo que te permite tomar medidas inmediatas.

Informes detallados: Trusted Advisor ofrece informes detallados con una descripción clara de cada recomendación, explicando cómo implementar los cambios sugeridos.

Acciones automatizadas (con soporte Business y Enterprise): En los niveles de soporte Business y Enterprise de AWS, Trusted Advisor puede ofrecer acciones automatizadas para aplicar las recomendaciones sin intervención manual.

Fácil integración: Trusted Advisor está integrado en la consola de administración de AWS, lo que permite acceder fácilmente a las recomendaciones y los informes desde un único lugar.

Conocimiento en tiempo real: Aprovechando la vasta experiencia de AWS, Trusted Advisor te ayuda a mantener tu infraestructura actualizada con las últimas prácticas y recomendaciones.

Beneficios para el rendimiento y la seguridad: Al seguir las recomendaciones de Trusted Advisor, puedes mejorar el rendimiento, aumentar la seguridad y reducir costos innecesarios.

EN RESUMEN

Comprender lo que sucede en su entorno es clave para mantener aplicaciones eficientes, seguras y en cumplimiento.

En esta clase hablamos de cómo CloudWatch puede proporcionar comprensión casi en tiempo real de cómo se comporta su sistema, incluyendo recibir alertas de condiciones que requieren su atención.
CloudWatch también le da la capacidad de analizar esas métricas a lo largo del tiempo a medida que ajusta su sistema para obtener el máximo rendimiento.

Hablamos de cómo CloudTrail puede ayudarle a saber exactamente quién hizo qué, cuándo y desde dónde. Responde a todas sus preguntas de auditoría de AWS, excepto por qué lo hicieron.

Y finalmente, analizamos Trusted Advisor que compila un panel rápido de más de 40 comprobaciones comunes relacionadas a costos, rendimiento, seguridad y resiliencia en un panel de control comprensible.

Por supuesto, hay muchas herramientas de supervisión adicionales y herramientas de analítica disponibles para usar, pero esto le ayudará a tener una buena idea de la variedad de soluciones que AWS ofrece a su empresa.