centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 887G

Guía de Configuración segura para monitorización y gestión en AWS

Marzo 2024

MINISTERIO DE DEFENSA

Catálogo de Publicaciones de la Administración General del Estado https://cpage.mpr.gob.es

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2024.03.26 16:53:21 +01'00'

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-24-125-0

Fecha de Edición: marzo de 2024

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

ÍNDICE

1. GUÍA DE MONITORIZACIÓN EN AWS

1.1 DESCRIPCIÓN DEL USO DE ESTA GUÍA

El objetivo de la presente guía es documentar las recomendaciones de seguridad para la implementación segura de las herramientas de monitorización y gestión de la nube de AWS. Las recomendaciones incluidas en esta guía son específicas para estas herramientas y se deberán, en su caso, complementar con los requisitos y recomendaciones de seguridad explicados, para cualquier entorno AWS en la guía ***CCN-STIC 887A – Guía de Configuración Segura para AWS***, especialmente cuando se busque el cumplimiento del Esquema Nacional de Seguridad en el sistema desplegado en AWS.

Es por ello, por lo que el uso de esta guía se recomienda para aquellas entidades que utilicen los servicios de monitorización en la nube de AWS.

Partiendo del modelo de responsabilidad compartida en materia de seguridad, entre el cliente y AWS, en esta guía se presentan las herramientas de monitorización y gestión, así como el uso de estas en servicios específicos.

Los asuntos relacionados con la seguridad y la conformidad son una responsabilidad compartida entre AWS, la cual puede ser consultada en la guía CCN-STIC 887A Guía de Configuración Segura para AWS en la sección 1.3.

1.3 DEFINICIÓN DEL SERVICIO

AWS es un conjunto de servicios complementarios en la nube que permite la creación y ejecución de una amplia gama de aplicaciones y servicios en un entorno escalable y de alta disponibilidad.

AWS brinda servicios funcionales para la monitorización y gestión del rendimiento tanto de las aplicaciones como de la infraestructura de un sistema. Además, permite, a través de los servicios de monitorización, la recopilación de datos y métricas estableciendo una comunicación interactiva entre AWS y cualquier otro destino.

En la monitorización y gestión, AWS se convierte en una plataforma evolucionada basada en un conjunto de herramientas, que permite la proactividad en la gestión de la infraestructura. No solo se trata de mecanismos que recopilan datos y métricas para elaborar tendencias, patrones y estadísticas, sino que permite la interacción mediante las alertas que automatizan acciones correctivas.

El conjunto de herramientas de monitorización y gestión permite una clasificación general de sus funciones en los distintos ámbitos en los que operan. Así pues, dentro de la monitorización y gestión de alertas se puede encontrar la recopilación de métricas, la definición de canales de notificación y la personalización de las alertas adaptadas a las necesidades de la infraestructura.

Por otro lado, en el ámbito de la gestión de logs se puede encontrar la recopilación de logs de sistema, auditoría y logs personalizados que definen las alertas.

A la hora de gestionar los datos y las métricas, existen herramientas de monitorización y gestión que permiten la elaboración de estadísticas y tendencias que detectan anomalías y patrones mediante un panel de control centralizado.

2. SERVICIOS DE MONITORIZACIÓN Y GESTIÓN

A continuación, se describen los principales servicios de AWS asociados a las tareas de monitorización y gestión de eventos. En caso de estar familiarizado con estos servicios y sus conceptos se puede continuar directamente con la sección 3.

2.1 AMAZON CLOUDWATCH

Funcionamiento general de Amazon CloudWatch

Amazon CloudWatch es un servicio de monitorización y administración que suministra datos e información procesable de aplicaciones y recursos de infraestructura locales, híbridos y de AWS. Amazon CloudWatch funciona como un repositorio de métricas de uso y rendimiento de los recursos y aplicaciones en tiempo real. Las métricas son los datos sobre el desempeño de los sistemas.

De forma predeterminada, diversos servicios ofrecen métricas gratuitas para recursos (tales como instancias de Amazon EC2, volúmenes de Amazon EBS e instancias de base de datos de Amazon RDS). Cuando se empieza a utilizar alguno de estos servicios, se habilita automáticamente la supervisión básica. Se puede obtener una lista de los servicios que ofrecen supervisión básica en este enlace.

Además, algunos servicios ofrecen una supervisión detallada que incurre en cargos. Su habilitación se debe hacer de forma concreta para cada servicio de AWS. Para obtener más información sobre los precios, puede consultar este enlace.

Amazon CloudWatch puede cargar todas las métricas en la cuenta para búsquedas, representación de gráficos y para alarmas, pudiendo interactuar con los paneles de todos los servicios de AWS que se están utilizando.

Para una mejor visualización de las métricas asociadas a servicios, se puede utilizar el explorador de métricas, que es una herramienta basada en etiquetas que permite filtrar, agregar y visualizar las métricas por etiquetas y propiedades de recurso. Los datos de las métricas se guardan durante 15 meses, lo que permite ver datos actualizados y datos históricos. Las métricas de Amazon CloudWatch se almacenan por separado en las regiones, pero es posible utilizar la funcionalidad para diversas regiones para agregar estadísticas de diferentes regiones. Cada región está totalmente aislada de las demás regiones para lograr la mayor estabilidad y aislamiento en caso de error.

Para representar métricas en la consola, se puede utilizar Amazon CloudWatch Metrics Insights, un potente motor de consultas SQL de alto rendimiento para identificar tendencias y patrones dentro de los resultados todas las métricas en tiempo real.

Además, es posible crear alarmas para la vigilancia de las métricas y el envío de notificaciones o realizar cambios automáticamente en los recursos que se están monitoreando cuando se infringe un umbral. Por ejemplo, es posible monitorear el uso de la CPU y las lecturas y escrituras de disco de las instancias de Amazon EC2 y utilizar esos datos para determinar si se deben lanzar instancias adicionales para gestionar el aumento de la carga, detener instancias infrautilizadas o lanzar notificaciones a través de Amazon SNS.

Puede consultarse más información sobre el servicio de Amazon CloudWatch en este enlace.

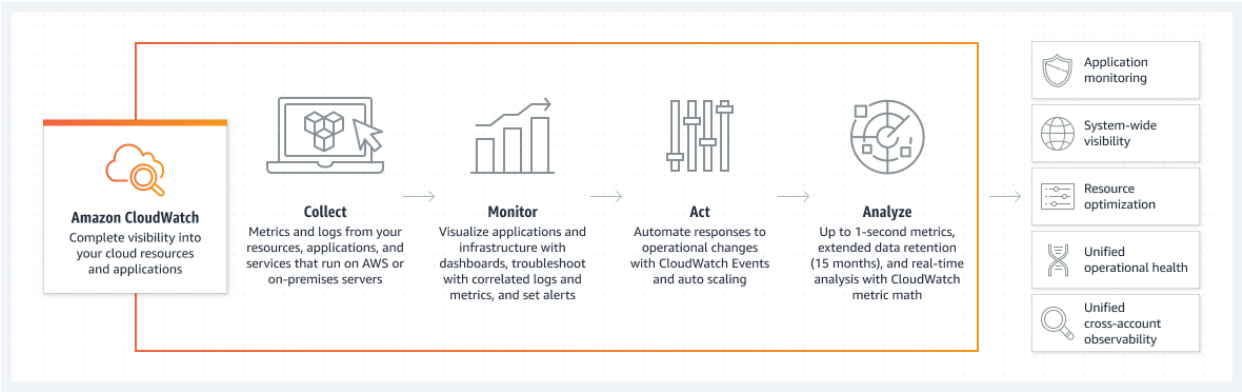

Fig. 2 Funcionamiento de Amazon CloudWatch

Permisos necesarios para utilizar la consola de Amazon CloudWatch.

Para poder trabajar con la consola de Amazon CloudWatch, cada usuario debe tener un conjunto mínimo de permisos que le permitan describir otros recursos de AWS en las cuentas. La consola Amazon CloudWatch requiere permisos de los siguientes servicios:

- Amazon EC2 Auto Scaling
- AWS CloudTrail
- Amazon CloudWatch Events
- Amazon CloudWatch Logs
- Amazon EC2
- Servicio de Amazon OpenSearch
- AWS IAM
- Amazon Kinesis
- AWS Lambda
- Simple Storage Service (Amazon S3)
- Amazon SNS
- Amazon SQS

- Amazon SWF
- X-Ray, si se utiliza la característica de ServiceLens

Para conocer el conjunto completo de permisos necesarios para trabajar con la consola de Amazon CloudWatch puede consultar este enlace.

Configuración inicial

Para utilizar Amazon CloudWatch, se necesita una cuenta de AWS. La cuenta de AWS permite utilizar servicios (por ejemplo, Amazon EC2) para generar métricas que se pueden visualizar en la consola de Amazon CloudWatch, una interfaz de selección y activación basada en la web. Además, se puede instalar y configurar la interfaz de línea de comandos (CLI) de AWS.

- Registrarse en AWS,
- Iniciar sesión en la consola de Amazon CloudWatch,
- Configuración de Amazon CLI.

Para obtener información detallada de la configuración inicial puede consultar este enlace.

Uso de paneles de Amazon CloudWatch

Los paneles de Amazon CloudWatch permiten crear gráficos reutilizables y ver las aplicaciones y recursos de la nube en una vista unificada. Se pueden visualizar en un gráfico los datos de logs y métricas en un único panel para obtener rápidamente el contexto y pasar de diagnosticar problemas a entender causas raíz. También se puede correlacionar el patrón de logs de una métrica específica y definir alarmas para que avisen de manera proactiva acerca de problemas operativos y de rendimiento. Esto otorga una visibilidad completa del sistema sobre el estado de las operaciones y la capacidad para resolver errores rápidamente, lo que reduce el tiempo de resolución de problemas.

Para obtener más información de la creación y configuración de paneles puede consultar este enlace.

Categorías principales de logs

Existen tres categorías principales de logs de Amazon CloudWatch Logs.

- Registros distribuidos: Los servicios de AWS publican originalmente estos logs por parte del cliente. Actualmente, Amazon VPC Flow Logs y los registros de Amazon Route 53 son los dos tipos admitidos.
- Logs que publican los servicios de AWS: Actualmente, 31 servicios de AWS publican logs en Amazon CloudWatch. Estos servicios incluyen Amazon API Gateway, AWS Lambda, AWS CloudTrail y muchos otros.

- Logs personalizados: Estos son los logs de las aplicaciones propias de cada organización y recursos locales. Se puede usar AWS Systems Manager para instalar un agente de CloudWatch o recurrir a la acción de la API PutLogData para publicar logs fácilmente.

Uso de Amazon CloudWatch Synthetics

Es posible utilizar Amazon CloudWatch Synthetics para la creación de Canaries, que son scripts configurables escritos en Node.js o en Python que se ejecutan según sean programados, y son utilizados para monitorizar los Endpoints (puntos de enlace final que responden a una petición de alguna instancia) y las API.

El uso de Canaries siguen las mismas rutas y realizan las mismas acciones que un cliente, lo que permite verificar continuamente la experiencia del cliente, incluso cuando no existe tráfico de clientes en las aplicaciones, de esta manera es posible descubrir problemas antes que los clientes lo hagan.

Los Canaries comprueban la disponibilidad y latencia de sus endpoints, y pueden almacenar datos de tiempo de carga y capturas de pantalla de interfaz de usuario. Estos monitorean las API REST, las URL y el contenido del sitio web, y pueden comprobar si hay cambios no autorizados de suplantación de identidad, inyección de código y scripts entre sitios.

Puede consultarse más información sobre el servicio de Amazon CloudWatch Synthetics en este enlace.

Tipos de alarmas de Amazon CloudWatch

- Alarmas compuestas: Las alarmas compuestas de Amazon CloudWatch permiten combinar varias alarmas y reducir el ruido. Si el problema de una aplicación afecta a varios recursos de la aplicación, se recibirá solo una única notificación de alarma que corresponde a toda la aplicación, en lugar de recibir una notificación por cada recurso, componente o servicio afectado. Se permite proporcionar un estado general de un grupo de recursos, como una aplicación, una región de AWS o una zona de disponibilidad.
- Alarmas de alta resolución: Las alarmas de Amazon CloudWatch permiten definir un umbral de métricas y activar una acción. Se pueden crear alarmas de alta resolución, definir un percentil y, a continuación, especificar una acción u omisión, según corresponda.

Detección de anomalías en Amazon CloudWatch

La detección de anomalías de Amazon CloudWatch aplica algoritmos de aprendizaje automático para analizar los datos de las métricas de manera permanente y detectar los comportamientos anormales. Permite crear alarmas que ajustan automáticamente los umbrales basándose en patrones de métricas naturales, como el momento del día, los días de la semana, las estaciones o las tendencias cambiantes.

Esto permite monitorear, aislar y solucionar los cambios inesperados en las métricas.

2.2 AWS CLOUDTRAIL

Funcionamiento general de AWS CloudTrail

AWS CloudTrail es un servicio que ayuda habilitar el gobierno, la conformidad y la auditoría de operaciones y riesgo de las cuentas de AWS. Proporciona un log de las acciones de los usuarios, los roles o un servicio de AWS, que se registran como eventos en AWS CloudTrail. AWS CloudTrail captura las llamadas a la API que se realizaron desde su cuenta AWS o en su nombre. Las llamadas capturadas incluyen las llamadas realizadas desde la consola y llamadas de código a las operaciones de la API. Amazon CloudWatch y CloudWatch Synthetics están integrados en AWS CloudTrail.

Al crear un seguimiento, es posible habilitar la entrega continua de eventos de AWS CloudTrail a un bucket de Amazon S3, incluyendo los eventos de Amazon CloudWatch. Si no se configura un log de seguimiento, es posible ver los eventos más recientes en el Historial de Eventos de la consola de AWS CloudTrail. Mediante la información que AWS CloudTrail recopila, se puede determinar la petición que fue enviada a Amazon CloudWatch, la dirección IP desde la que se ha realizado la petición, quién la realizó, cuando se realizó y otros detalles adicionales.

Dentro de los aspectos clave de seguridad y prácticas recomendadas operativas se encuentra la visibilidad de la actividad de la cuenta de AWS, y para esto se puede utilizar AWS CloudTrail, para ver, buscar, descargar, archivar, analizar y responder a la actividad de la cuenta en la infraestructura. Es posible identificar quién o qué tuvo que actuar, sobre que recursos se actuó, cuando se produjo el evento y otros detalles que ayudan a analizar y responder a una actividad en la cuenta de AWS. Además, se puede usar AWS CloudTrail para detectar actividad inusual en las cuentas de AWS. Estas funciones ayudan a simplificar los análisis operativos y la solución de problemas.

Puede consultarse más información sobre el servicio de AWS CloudTrail en este enlace.

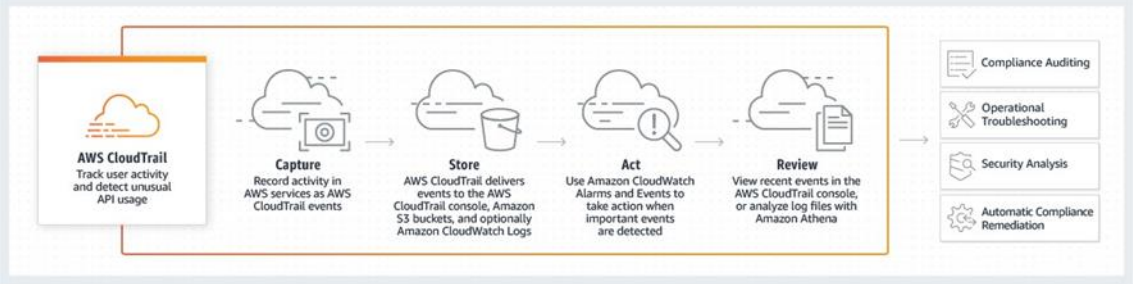

Fig. 3 Funcionamiento de AWS CloudTrail

Tipos de logs de AWS CloudTrail

Es posible crear dos tipos de logs de seguimiento para una cuenta de AWS:

- Un log de seguimiento aplicable a todas las regiones. AWS CloudTrail registra los eventos de cada región y envía los archivos de logs de eventos de AWS CloudTrail al bucket de Amazon S3 que se configure. Si se añade una región después de crear un log de seguimiento que se aplica a todas las regiones, la nueva región se incluye automáticamente, y también se registran sus eventos.
- Un log de seguimiento aplicable a una región. En este caso AWS CloudTrail solo registra los eventos de esa región, los cuales son entregados al bucket de Amazon S3 que se especifique. Solo puede crear un log de seguimiento de una sola región. El resto de los logs de seguimiento individuales adicionales, se pueden enviar al mismo bucket de Amazon S3 o a buckets separados.

Validación de los logs de AWS CloudTrail

Se recomienda activar la validación de los logs de AWS CloudTrail. La validación de logs de AWS CloudTrail crea un archivo de resumen firmado digitalmente mediante algoritmos estándar: SHA-256 para el hash y SHA-256 con RSA para la firma digitalpara cada log que AWS CloudTrail que escribe en Amazon S3. Estos archivos de resumen se pueden usar para determinar si un archivo de log se cambió, eliminó o no cambió después de que AWS CloudTrail entregó el log.

Cifrado y protección de los logs de AWS CloudTrail

AWS CloudTrail utiliza de forma predeterminada el cifrado del servidor (SSE) S3 para cifrar los archivos de logs, aunque se puede configurar para utilizar las claves maestras creada por el cliente (CMK) de KMS para proteger aún más los logs de AWS CloudTrail. Además, se recomienda implementar las siguientes protecciones:

- Que los buckets de Amazon S3 para AWS CloudTrail se configuren con MFA Delete, esto evitará la eliminación de logs de AWS CloudTrail sin una autorización explícita.
- Utilizar una política de bucket que imponga restricciones sobre cuáles de los usuarios de pueden eliminar objetos de Amazon S3.
- Activar acceso por MFA a los archivos de logs.
- Que el almacén de logs de AWS CloudTrail no sea accesible de forma pública.

Control de acceso en CloudTrail con IAM

AWS CloudTrail se integra con AWS Identity and Access Management (IAM) y de esta manera permite controlar el acceso a AWS CloudTrail y a otros recursos de AWS que solicita AWS CloudTrail, incluidos los buckets de Amazon S3 y los temas de Amazon Simple Notification Service (Amazon SNS). Se puede utilizar AWS Identity and Access Management para controlar qué usuarios de AWS pueden crear, configurar o eliminar

logs de seguimiento de AWS CloudTrail, comenzar y detener el registro y tener acceso a los buckets que contienen información de logs.

Con las políticas basadas en identidad de IAM, se pueden especificar las acciones y recursos permitidos o denegados, así como las condiciones en las que se permiten o deniegan las acciones. AWS CloudTrail admite acciones y recursos específicos. No hay claves de condición específicas del servicio de AWS CloudTrail que se puedan utilizar en el elemento Condition de las instrucciones de la política.

Las acciones de políticas de AWS CloudTrail utilizan el siguiente prefijo antes de la acción: cloudtrail: Por ejemplo, para conceder a alguien permiso para crear una lista de las etiquetas de un log de seguimiento con la operación ListTags de la API, hay que incluir la acción cloudtrail:ListTags en la política.

```
"Action": [
      "cloudtrail:AddTags",
      "cloudtrail:ListTags",
      "cloudtrail:RemoveTags
```

Fig. 4 Ejemplo de una política de CloudTrail

Control de acceso en AWS CloudTrail con listas de control de acceso (ACL)

Las listas de control de acceso (ACL) son listas de beneficiarios que se pueden adjuntar a los recursos. Conceden a las cuentas permisos de acceso al recurso al que están adjuntadas. Aunque AWS CloudTrail no admite las ACL, Amazon S3 sí. De este modo, es posible adjuntar las ACL a un recurso de bucket de Amazon S3 en el que se almacenan los archivos de logs de uno o varios logs de seguimiento.

En general AWS recomienda el uso de políticas de S3 para la protección de acceso a este recurso, pero el uso de ACLs sigue siendo válido en los entornos que todavía lo emplean.

Para obtener más información sobre cómo adjuntar las ACL a los buckets, se puede consultar este enlace.

Uso de AWS CloudTrail Lake

AWS CloudTrail Lake permite ejecutar consultas basadas en SQL sobre los eventos. Estos eventos se agregan en almacenes de datos de eventos, que son colecciones inmutables de eventos basados en criterios que se seleccionan aplicando sectores de eventos avanzados. Es posible conservar los datos de los eventos en un almacén de eventos hasta 7 años de forma predeterminada o hasta un máximo de 10 años. Los selectores que se aplican a un almacén de datos de eventos controlan los eventos que perduran y están disponibles para la consulta.

Estas consultas ofrecen una visión más detallada y personalizable de los eventos que las simples búsquedas de claves y valores en el Historial de eventos, o ejecutando LookupEvents. Las búsquedas en el Historial de eventos están limitadas a una sola cuenta de AWS, solo devuelve eventos de una única región no puede consultar múltiples

atributos. Con AWS CloudTrail Lake, se puede ejecutar consultas complejas en SQL en múltiples campos de búsqueda, y realizar búsquedas en todas las regiones simultáneamente.

Puede consultarse más información del servicio AWS CloudTrail Lake en este enlace.

2.3 AWS CONFIG

Funcionamiento general de AWS Config

AWS Config proporciona una vista detallada de la configuración de los recursos de AWS. Los recursos son entidades con las que se puede trabajar en AWS, como instancias de EC2 o volúmenes EBS. La vista que proporciona AWS Config incluye cómo se relacionan los recursos entre sí y cómo se han configurado en el pasado, de manera que es posible ver cómo las configuraciones y las relaciones cambian a lo largo del tiempo.

Puede consultarse la lista completa de recursos de AWS admitidos por AWS Config en este enlace:

En AWS Config, se tienen las siguientes opciones:

- Evaluar las configuraciones de recursos de AWS para los ajustes que se desee.
- Obtener una instantánea de las configuraciones actuales de los recursos admitidos que están asociados a su cuenta de AWS.
- Recuperar configuraciones de uno o más recursos existentes en la cuenta.
- Recuperar configuraciones históricas de uno o más recursos.
- Recibir una notificación cuando se crea, se modifica o se elimina un recurso.
- Ver las relaciones entre los recursos. Por ejemplo, es posible que se desee encontrar todos los recursos que utilizan un grupo de seguridad determinado.

Puede consultarse más información sobre el servicio de AWS Config en este enlace.

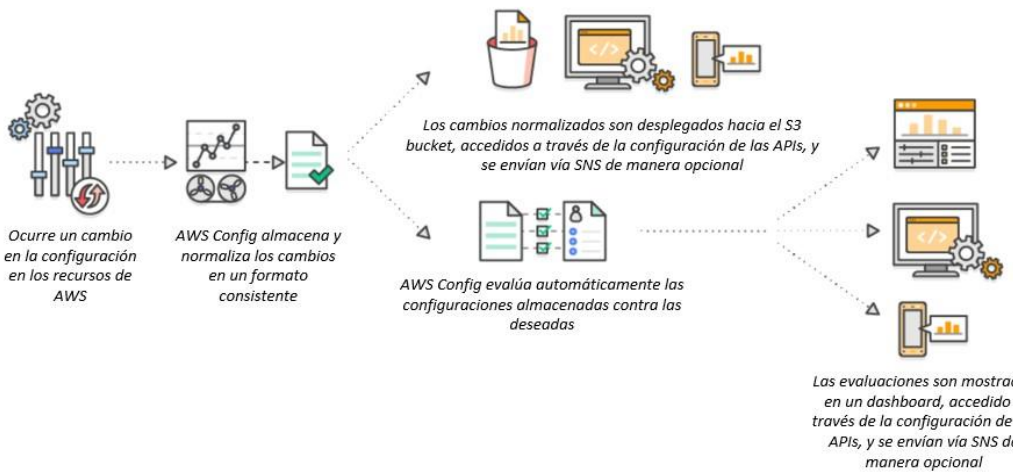

Fig. 5 Funcionamiento AWS Config

Permisos de administración de AWS Config

Para permitir que los usuarios administren AWS Config se deben conceder permisos de manera explícita a los usuarios de IAM para realizar las acciones necesarias asociadas. Para la mayoría de las situaciones, se puede hacer a través de una política administrada de AWS que tenga los permisos predefinidos.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "config.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "AWS:SourceAccount": "sourceAccountID"
        }
      }
    }
  ]
}
```

Fig. 6 Ejemplo de una política de confianza para roles de AWS Config

Puede consultarse más información de los permisos de administración de AWS Config en este enlace.

Administración de la configuración de recursos con las reglas de AWS Config

Es posible utilizar las reglas de AWS Config para evaluar los ajustes de configuración de los recursos de AWS. Cuando AWS Config detecta que un recurso infringe las condiciones en una de las reglas, AWS Config marca el recurso como no conforme y envía una notificación. Este mecanismo puede ser utilizado para que se notifique en los eventos de creación, modificación o eliminación de recursos sin tener que supervisar estos cambios sondeando las llamadas realizadas a cada recurso.

De esta manera se ejerce un mejor control de las configuraciones de los recursos y se puede detectar configuraciones erróneas en los mismos brindando una visibilidad minuciosa sobre los recursos existentes.

Administración y resolución de problemas de cambios de configuración

AWS Config es esencial para identificar y evaluar el impacto de un cambio al momento de modificar un recurso, o en su configuración, evitando tener consecuencias imprevistas en los recursos relacionados.

Cuantos más recursos de AWS dependen unos de otros, es mayor la necesidad de gestión unificada, utilizando también las configuraciones históricas de los recursos y

pudiendo de esta manera solucionar problemas y acceder a la última configuración correcta conocida de un recurso que esté fallando.

Auditoría y conformidad

AWS Config proporciona la información de las configuraciones históricas para poder demostrar y garantizar la conformidad de las políticas internas para los datos que requieren auditoría, se puede monitorear constantemente y registrar los cambios de configuración de sus recursos de AWS.

Análisis de seguridad

Para analizar posibles deficiencias de seguridad, es necesaria la información histórica detallada sobre las configuraciones de los recursos, tales como las políticas IAM que se otorgan a los usuarios o las reglas de grupo de seguridad de Amazon EC2 que controlan el acceso a los recursos. Esta información puede ayudar a determinar los permisos que pertenecían a un usuario en un momento específico o a determinar si un grupo de seguridad ha bloqueado el tráfico entrante de TCP a un puerto específico.

2.4 CONFORMANCE PACKS

Funcionamiento general de Conformance Packs

Un Conformace Pack (Paquete de conformidad) es un conjunto de reglas y acciones de corrección de AWS Config que se implementa como una entidad en una cuenta y una región o en toda una organización. La implementación de estos paquetes de conformidad se realiza a través de plantillas YAML que contienen las reglas administradas o personalizadas y las acciones de corrección de AWS Config, que son ejecutadas utilizando la consola de AWS Config o la AWS CLI.

AWS desarrolla y mantiene Conformance Packs para las diferentes categorías del Esquema Nacional de seguridad. Puede consultar la información relativa a dichos Conformance Packs en los siguientes enlaces:

- Nivel alto.
- Nivel medio.
- Nivel bajo.

Requisitos previos para utilizar un paquete de conformidad con corrección

Antes de implementar paquetes de conformidad utilizando plantillas de ejemplo con corrección, se deben crear los recursos adecuados, como el rol de automatización y otros recursos de AWS basados en el objetivo de corrección. Si ya se tiene un rol de automatización que se está utilizando para la corrección con documentos SSM (AWS Systems Manager), es posible proporcionar directamente el ARN (Amazon Resource Name) de ese rol. Si se tiene algún recurso, es posible incluirlo en la plantilla.

AWS Config no admite las funciones intrínsecas de AWS CloudFormation con el rol de ejecución de automatización. Se debe proporcionar el ARN exacto del rol en forma de cadena.

Para obtener más información acerca de cómo pasar el ARN exacto puede consultarse este enlace.

Además, previo a desplegar un paquete de conformidad es necesaria la activación de AWS Config Recording.

Requisitos previos para utilizar un paquete de conformidad con una o varias reglas de AWS Config

Antes de implementar un paquete de conformidad con una o varias reglas de AWS Config personalizadas, es necesario crear los recursos adecuados, como la función de AWS Lambda y el rol de ejecución correspondiente.

Si ya se cuenta con una regla de AWS Config personalizada, es posible proporcionar directamente el ARN de la función de AWS Lambda para crear otra instancia de esa regla personalizada como parte del paquete, pero si no se dispone de una regla AWS Config personalizada, se puede crear una función AWS Lambda y utilizar el ARN de la función de Lambda.

Para obtener más información acerca de Reglas personalizadas de AWS Config puede consultarse este enlace.

Requisitos previos de los paquetes de conformidad de la organización

Si la plantilla de entrada tiene una configuración de corrección automática, es necesario especificar el ARN del rol de ejecución de automatización de esa corrección en la plantilla. Comprobar que existe un rol con el nombre especificado en todas las cuentas (cuenta maestra y cuentas miembro) de una organización. Se debe crear este rol en todas las cuentas antes de llamar a la API *PutOrganizationConformancePack*. Se puede crear este rol en cada cuenta manualmente o utilizando los conjuntos de pilas de AWS CloudFormation.

Si la plantilla utiliza la función intrínseca Fn::ImportValue de AWS CloudFormation para importar una determinada variable, esa variable debe definirse como Export Value en todas las cuentas miembro de esa organización.

Comprobaciones de procesos en un paquete de conformidad

Las comprobaciones de proceso son un tipo de regla de AWS Config que permite realizar un seguimiento de las tareas externas e internas que requieren verificación como parte de los paquetes de conformidad. Estas comprobaciones se pueden agregar a un paquete de conformidad existente o a uno nuevo. Es posible realizar un seguimiento de

todo el cumplimiento que incluye las configuraciones de AWS y comprobaciones manuales en una única ubicación.

Con las comprobaciones de procesos, se puede enumerar el cumplimiento de los requisitos y las acciones en una única ubicación. Estas comprobaciones de procesos ayudan a aumentar la cobertura de los paquetes de conformidad basados en regímenes de cumplimiento. Se puede ampliar aún más el paquete de conformidad añadiendo nuevas comprobaciones de procesos que rastrean los procesos y las acciones que requieren verificación y seguimiento manuales. Esto permite que el paquete de conformidad se convierta en la plantilla que proporciona detalles sobre las configuraciones de AWS y de procesos manuales para un régimen de cumplimiento.

```
###############################################################################
#
#  Conformance Pack template for process check
#
###############################################################################
Resources:
  AWSConfigProcessCheck:
    Properties:
      ConfigRuleName: RuleName
      Description: Description of Rule
      Source:
        Owner: AWS
        SourceIdentifier: AWS_CONFIG_PROCESS_CHECK
    Type: AWS::Config::ConfigRule
```

Fig. 7 Ejemplo de plantilla de paquete de conformidad para crear comprobaciones de procesos

Se realiza un seguimiento y administra el cumplimiento de los procesos no asociados con los cambios de configuración de recursos dentro de los paquetes de conformidad como comprobaciones de procesos. Por ejemplo, agregar una comprobación del proceso para realizar un seguimiento del requisito de cumplimiento de PCI-DSS para almacenar copias de seguridad de medios en una ubicación fuera del sitio. Evaluará manualmente el cumplimiento de esto, de acuerdo con las directrices de PCI-DSS (Payment Card Industry – Data Security Standard) o de acuerdo con las directrices de su organización.

Para obtener más información de las comprobaciones de procesos en un paquete de conformidad de AWS Config, puede consultarse este enlace.

2.5 VPC FLOW LOGS

Funcionamiento general de VPC Flow Logs

El servicio de VPC Flow Logs permite capturar información acerca del tráfico IP que entra y sale de los interfaces de red en la VPC, red o instancia. Los datos de los logs de estos flujos de red pueden publicarse en Amazon CloudWatch Logs o Amazon S3. Una vez creado un log de flujo, es posible recuperarlo y ver los datos en el destino elegido.

Los logs de flujo son útiles en una serie de tareas, tales como:

- Diagnosticar reglas de grupo de seguridad muy restrictivas

- Monitorizar el tráfico que llega a su instancia
- Determinar la dirección del tráfico hacia y desde las interfaces de red

Los datos de logs de flujo se recopilan fuera de la ruta del tráfico de red y, por lo tanto, no afectan al rendimiento ni a la latencia de la red. Se pueden crear o eliminar logs de flujo sin ningún riesgo de impacto en el rendimiento de la red. Esta funcionalidad se incluye como control de cumplimiento para la medida Detección de intrusión descrita en la siguiente sección de esta guía

En el siguiente ejemplo observamos el log (fl-aaa) que captura el tráfico aceptado para la interfaz de la instancia A1 y publica las entradas de logs de flujo en un bucket de Amazon S3. Se observa una segunda entrada de logs de flujo que captura todo el tráfico de la subred B que publica las entradas de un log de flujo en Amazon CloudWatch Logs en el flujo (flbbb).

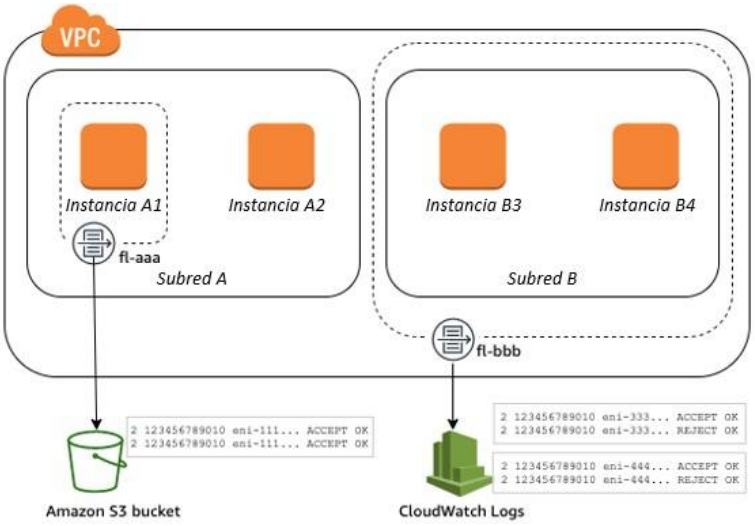

Fig. 8 Captura de tráfico con AWS Flow Log

Un log de AWS Flow Log representa un flujo de red en la VPC. Predeterminadamente, cada log captura un flujo de tráfico del protocolo de internet (IP) de red, que tiene lugar dentro de un período de captura o intervalo de agregación. Los logs de AWS Flow Logs se pueden trabajar desde las consolas de Amazon EC2, Amazon VPC, ClowdWatch y Amazon S3.

Los datos de una interfaz de red monitoreada se registran como logs de flujo, que son eventos que se componen de una serie de campos que describen el flujo del tráfico.

Puede consultarse más información sobre el servicio VPC Flow Logs en este enlace.

Permisos de control del uso de logs de VPC Flow Logs

De forma predeterminada, los usuarios de IAM no tienen permiso para trabajar con logs de flujo. Se puede crear una política de usuarios de IAM que conceda permisos a los usuarios para crear, describir y eliminar logs de flujo.

Fig. 9 Ejemplo de una política de permisos completos para crear, describir y eliminar.

Puede consultar más información sobre la configuración de VPC Flow Logs en este enlace.

2.6 AMAZON GUARDDUTY

Funcionamiento general de Amazon GuardDuty

Amazon GuardDuty es un servicio de detección de amenazas que monitorea continuamente la actividad maliciosa y el comportamiento no autorizado para proteger sus cuentas de AWS, las cargas de trabajo de Amazon Elastic Compute Cloud (EC2), las aplicaciones en contenedores, las bases de datos de Amazon Aurora (Preview) y los datos almacenados en Amazon Simple Storage Service (S3). Mediante el uso de fuentes de AWS y de terceros líderes del sector, Amazon GuardDuty combina machine learning, la detección de anomalías, el monitoreo de la red y el descubrimiento de archivos maliciosos para ayudar a proteger la carga de trabajo y los datos en AWS. Amazon GuardDuty es capaz de analizar decenas de miles de millones de eventos de múltiples orígenes de datos de AWS, como logs de eventos de AWS CloudTrail, logs de flujo de la nube virtual privada (VPC) de Amazon, logs de auditoría de Amazon Elastic Kubernetes Service (EKS) y logs de consultas de DNS.

Amazon GuardDuty identifica la actividad inusual dentro de las cuentas, analiza la relevancia para la seguridad de la actividad y proporciona el contexto en el que se invocó. Esto permite a quien responde determinar si es necesario dedicar más tiempo para investigar. A los hallazgos de Amazon GuardDuty se les asigna una gravedad, y las acciones se pueden automatizar mediante la integración con AWS Security Hub.

Para más información sobre Amazon GuardDuty y su activación puede consultar este enlace.

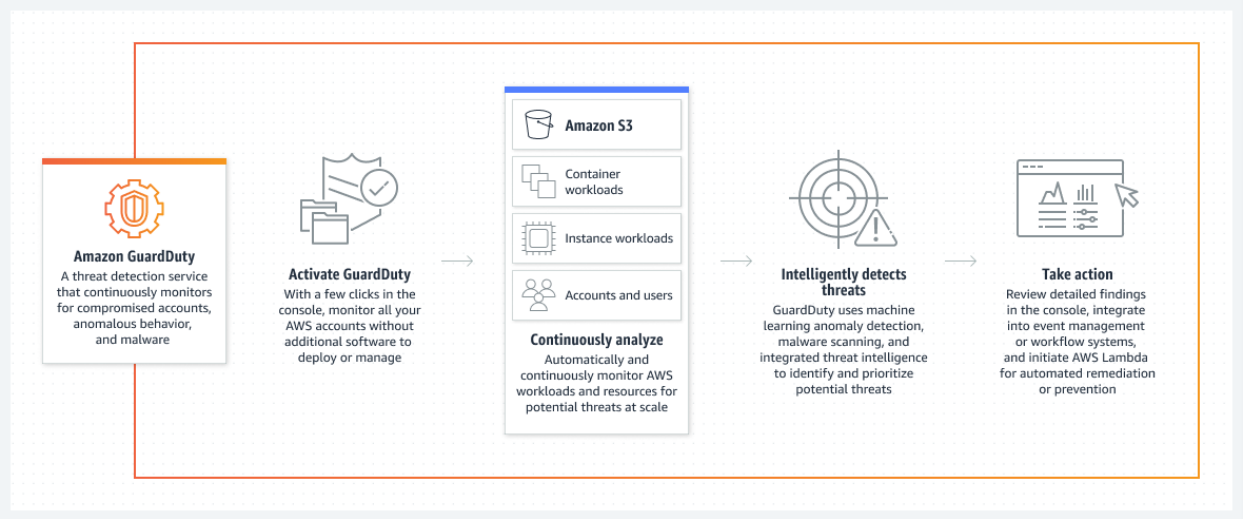

Fig. 10 Funcionamiento de Amazon GuardDuty

Detección de amenazas

Amazon GuardDuty ofrece detección de amenazas precisa de cuentas vulnerables realizando una monitorización continua de los factores en casi tiempo real. Amazon GuardDuty puede detectar señales de cuentas vulnerables, como el acceso a recursos de AWS a partir de una ubicación geográfica inusual en un momento atípico del día. Amazon GuardDuty controla las llamadas a la API inusuales, como los intentos de ocultar actividad en cuentas mediante la desactivación del log de AWS CloudTrail o la captura de instantáneas de una base de datos a partir de una dirección IP malintencionada.

Las principales categorías de detección incluyen:

- Reconocimiento: Algunos ejemplos son una actividad de API inusual, el escaneo de puertos en el interior de una VPC, patrones inusuales de solicitudes de inicio de sesión incorrectas o el sondeo de puertos no bloqueados a partir de una IP maliciosa conocida.
- Vulnerabilidad de instancias: Algunos ejemplos son una actividad que indica la vulnerabilidad de una instancia, como la minería de criptomonedas, actividad de comando y control (C&C) de puerta trasera, malware que utiliza algoritmos de generación de dominios (DGA), actividad de salida de denegación de servicios, volúmenes altos inusuales del tráfico de red, protocolos de red inusuales, comunicación de salida de instancias con una IP malintencionada conocida, credenciales temporales de Amazon EC2 utilizadas por una dirección IP externa y exfiltración de datos con DNS.
- Vulnerabilidad de cuentas: Algunos ejemplos son llamadas a la API desde una ubicación geográfica inusual o un proxy anónimo, intentos de desactivar los logs de AWS CloudTrail, cambios que debilitan la política de contraseña de la cuenta, lanzamientos inusuales de infraestructuras o de instancias, implementaciones de infraestructura en una región inusual y llamadas a la API desde direcciones IP malintencionadas conocidas.
- Vulnerabilidad de buckets: Algunos ejemplos son una actividad que indique la vulnerabilidad de un bucket, como patrones de acceso a datos que

muestren un mal uso de credenciales, actividad no usual de la API de S3 desde un host remoto, acceso a S3 no autorizado desde direcciones de IP confirmadas como maliciosas y llamadas a la API para recuperar datos en buckets de S3 de un usuario que no cuenta con un historial previo de acceso al bucket o invocadas desde una ubicación inusual. Amazon GuardDuty monitorea y analiza de manera continua eventos de datos de S3 de AWS CloudTrail para detectar actividad sospechosa en todos los buckets de Amazon S3.

Se puede consultar la lista entera de los tipos de hallazgos que localiza Amazon GuardDuty en este documento del fabricante.

Dentro del control de amenazas se dispone de tres niveles de gravedad:

- Bajo: Indica una actividad sospechosa o malintencionada que se bloqueó antes de poner en peligro al recurso.
- Medio: Indica actividad sospechosa. Por ejemplo, actividad que no se ajusta al comportamiento observado normalmente.
- Alto: Indica que el recurso en cuestión está en peligro y que se está utilizando activamente para fines no autorizados.

Monitorización continua

Amazon GuardDuty se encarga de monitorizar y analizar continuamente datos de eventos de cargas de trabajo y cuentas de AWS que se encuentran en AWS CloudTrail, en el log de flujo de VPC y logs de DNS. Amazon GuardDuty se enfoca en cómo responder rápidamente y cómo mantener la organización protegida.

Para la detección de intrusiones se recomienda el uso de Amazon GuardDuty, el cual es un servicio de detección de amenazas que monitoriza continuamente para identificar actividades maliciosas y comportamientos no autorizados con el fin de proteger datos, cargas de trabajo y cuentas de AWS almacenados en Amazon S3.

El servicio utiliza aprendizaje automático, detección de anomalías e inteligencia contra amenazas integrada para identificar y priorizar las posibles amenazas. Amazon GuardDuty analiza miles de millones de eventos a través de varios orígenes de datos de AWS, como los logs de eventos de AWS CloudTrail, los logs de flujo de Amazon VPC y los logs de DNS. Mediante la integración con Amazon CloudWatch Events, las alertas de Amazon GuardDuty son procesables, fáciles de agregar a diferentes cuentas y fáciles de insertar en los sistemas existentes de flujos de trabajo y administración de eventos. Amazon GuardDuty utiliza fuentes de información de amenazas, como listas de direcciones IP y dominios maliciosos, y aprendizaje automático para identificar la actividad anómala y potencialmente no permitida, así como la actividad malintencionada en su entorno de AWS.

2.7 AWS SECURITY HUB

AWS Security Hub proporciona una visión completa del estado de seguridad en AWS, y ayuda a contrastar el entorno con los estándares y las prácticas recomendadas del sector de la seguridad.

Security Hub recopila datos de seguridad de todas las cuentas de AWS, de los servicios y de los productos de terceros que son compatibles con AWS y ayuda a analizar las tendencias y comportamientos de seguridad, identificando de esta manera, los problemas de seguridad que tengan mayor prioridad.

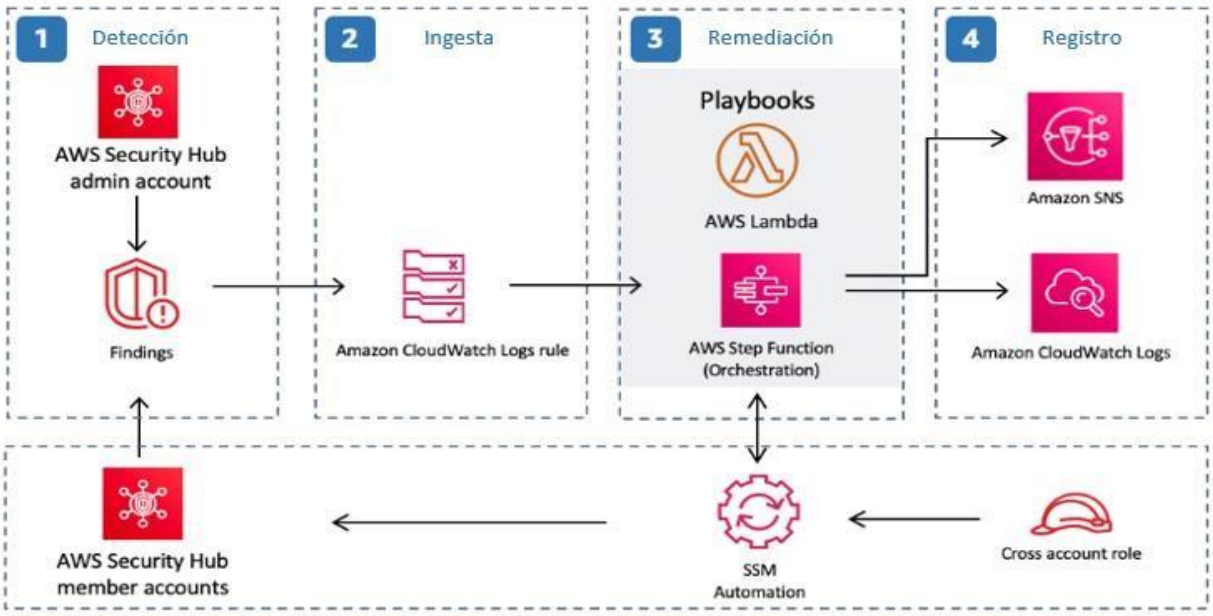

Fig. 11 Arquitectura de la solución de respuesta y resolución de problemas automatizadas de AWS Security Hub

Puede encontrar más información sobre AWS Security Hub en este enlace.

2.8 SERVICIOS INTEGRADOS DE MONITORIZACIÓN

Además de los ya expuestos, existen otros servicios que nos ayudan a gestionar de una manera más segura tanto las cuentas pertenecientes a una región o varias regiones como las acciones de los usuarios.

2.8.1 IAM ACCESS ANALYZER

AWS IAM Access Analyzer proporciona las herramientas necesarias para identificar los recursos de la organización y todas las cuentas, como buckets de Amazon S3 o roles de IAM, que se comparten con una entidad externa. Esto permite identificar el acceso no deseado a los recursos y datos, lo que constituye un riesgo para la seguridad. Access Analyzer identifica los recursos compartidos con entidades principales externas mediante el uso de un razonamiento lógico para analizar las políticas basadas en recursos en el entorno de AWS.

Cuando se habilita AWS IAM Access Analyzer, se crea un analizador para toda la organización o una cuenta. La organización o cuenta que se elija se conoce como la zona de confianza del analizador. El analizador monitoriza todos los recursos admitidos dentro de esa zona de confianza. Cualquier acceso a los recursos por parte de entidades principales que se encuentren dentro de su zona de confianza se considera de confianza.

Al analizar las políticas, si AWS IAM Access Analyzer identifica una que concede acceso a una entidad principal externa que no está dentro de la zona de confianza, genera un hallazgo. Cada hallazgo incluye detalles sobre el recurso, la entidad externa que tiene acceso al mismo y los permisos concedidos para que se puedan tomar las medidas adecuadas.

AWS IAM Access Analyzer analiza solo las políticas que se aplican a los recursos de la misma región de AWS en la que está habilitada. Para monitorear todos los recursos del entorno de AWS, se debe crear un analizador para habilitar AWS IAM Access Analyzer en cada región en la que se utilicen los recursos de AWS admitidos. AWS IAM Access Analyzer analiza los siguientes tipos de recursos:

- Buckets de Amazon Simple Storage Service Batch
- Roles de AWS Identity and Access Management
- Llaves AWS Key Management Service
- Funciones y capas de AWS Lambda
- Colas de Amazon Simple Queue Service
- Secretos de AWS Secrets Manager

Para configurar AWS IAM Access Analyzer, se puede agregar una cuenta de miembro a la organización como administrador delegado para administrar AWS IAM Access Analyzer en su organización. Este administrador tiene permisos para crear y administrar analizadores con la organización como confianza. Solo la cuenta de administración puede agregar un administrador delegado.

Para conocer más sobre la configuración de IAM Access Analyzer puede consultar este enlace.

2.8.2 IAM ACCESS ADVISOR

En la administración de AWS se puede conceder permisos a entidades (usuarios o roles) más allá de lo que requieren. AWS IAM Access Advisor proporciona información que ayuda a definir barreras y políticas de protección. La información que proporciona este servicio es:

- Información de IAM sobre los últimos accesos. Cuando se consulte la información de IAM sobre los últimos accesos se podrá encontrar dos tipos de información de las entidades de IAM: información sobre los servicios de AWS permitidos e información sobre las acciones permitidas. Esta información incluye la fecha y la hora en que se realizó el intento. La información de última acción a la que se accede está disponible para las

acciones de administración de Amazon EC2, IAM, Lambda y Amazon S3, que incluyen acciones de creación, eliminación y modificación.

Se puede conocer más sobre la información de acceso reciente de IAM en este enlace.

- Información de acceso reciente de AWS Organizations. Si se inicia sesión con las credenciales de la cuenta de administración de la organización, se podrá ver información sobre los últimos accesos a servicios de una política o entidad de AWS Organizations de la organización. Las entidades de AWS Organizations pueden ser cuentas, unidades organizativas o la raíz de la organización. En la información de acceso reciente de AWS Organizations, se incluyen los servicios permitidos por una política de control de servicios (SCP). Se indica qué entidades principales de una organización o cuenta intentaron acceder por última vez al servicio y cuándo lo hicieron.

Para conocer más sobre la información de último acceso de AWS Organizations se puede consultar este enlace.

2.8.3. NETWORK ACCESS ANALYZER

Network Access Analyzer, es una característica que identifica el acceso a la red no atendido para los recursos en AWS. Se puede utilizar para especificar los requisitos de acceso a la red e identificar las posibles rutas que no cumplan dichos requisitos. Es posible especificar los requisitos de acceso a la red como el alcance del acceso a la red, lo que determina los tipos de hallazgos que el análisis produce. Es posible agregar entradas a MatchPaths como a ExcludePaths para incluir o excluir los tipos de rutas de la red respectivamente.

- MatchPaths. En esta sección se definen los valores especificados de los campos para las rutas de red que resultan de un análisis. Estos son utilizados para especificar las rutas de red que se consideren una violación a la seguridad o el cumplimiento de requisitos.
- ExcludePaths. Aquí se incluyen todos los valores especificados para prevenir que ciertas rutas de red aparezcan en los hallazgos. Esta sección se emplea para especificar las rutas de red que sean consideradas una excepción legítima a la seguridad de red o requisitos de cumplimiento.

```
{
    "MatchPaths": [
        {
            "Source": {
                "ResourceStatement": {
                    "Resources": [
                        "vpc-abcd12e3"
                    ]
                }
            }
        }
    ],
    "ExcludePaths": [
        {
            "Source": {
                "ResourceStatement": {
                    "ResourceTypes": [
                        "AWS::EC2::InternetGateway"
                    ]
                }
            }
        }
    ]
}
```

Fig 12 Ejemplo de configuración de un origen para incluir y excluir elementos de red

2.8.4 REACHABILITY ANALYZER

Reachability Analyzer es una herramienta de análisis de configuración que permite realizar pruebas de conectividad entre un recurso origen y un recurso destino en las VPC. Cuando el destino es alcanzable, Reachability Analyzer produce un detalle de la traza de los saltos de la red virtual entre el origen y el destino. Cuando el destino no es alcanzable, Reachability Analyzer identifica el componente que lo bloquea. Por ejemplo, caminos que son bloqueados por problemas de configuración en un grupo de seguridad, ACL de red, tabla de ruta o balanceador de carga.

Es posible utilizar Reachability Analyzer para determinar, ya sea si un recurso destino es alcanzable en una VPC desde un recurso origen. Para iniciar se especifica un origen y un destino. Si tiene una traza alcanzable entre el origen y el destino, Reachability Analyzer despliega los detalles, de otra manera, identifica el componente bloqueante.

Para conocer las tareas a ejecutar para configurar Reachability Analyzer, se puede consultar este enlace.

2.8.5 AWS TRUSTED ADVISOR

AWS Trusted Advisor es una aplicación que usa las prácticas recomendadas aprendidas mediante el historial operativo total de AWS que se ha originado a partir de la atención suministrada a cientos de miles de clientes de AWS. AWS Trusted Advisor inspecciona el entorno AWS del cliente y ofrece recomendaciones cuando surge la oportunidad de ahorrar dinero, mejorar el rendimiento y la disponibilidad del sistema o ayudar a cerrar deficiencias de seguridad.

Concretamente, las categorías de verificación que incluye AWS Trusted Advisor son:

- Optimización de costos: recomendaciones que pueden hacer que el cliente ahorre dinero. Resaltan los recursos no utilizados y las posibilidades de reducir la factura.
- Rendimiento: Pueden mejorar la velocidad y la capacidad de respuesta de las aplicaciones.
- Seguridad: Recomendaciones para la configuración de seguridad que pueden hacer que la solución e AWS sea más segura.
- Tolerancia a errores: recomendaciones que ayudan a aumentar la resiliencia de la solución de AWS.
- Cuotas de servicio: verifica el uso de la cuenta y si la cuenta se acerca al límite o lo supera para los servicios y recursos de AWS.
- Excelencia operativa: recomendaciones para ayudar a operar el entorno AWS de manera eficaz y a escala.

Asimismo, las verificaciones se clasifican en:

- Acción recomendada: Por ejemplo, problemas de seguridad para los recursos de IAM, en los que se recomienda llevar a cabo una acción de carácter urgente.
- Investigación recomendada: Por ejemplo, una verificación que alcanza una cuota para un recurso, por lo que se recomienda eliminar recursos no utilizados.
- Comprobaciones con elementos excluidos: Verificaciones que incluyen elementos excluidos, es decir, recursos que se desea ignorar en las comprobaciones, como puede ser una instancia Amazon EC2 que no se desea que se evalúe.

Se puede ampliar la información de este servicio en la documentación oficial en el siguiente recurso: AWS Trusted Advisor

3. MONITORIZACIÓN DE SERVICIOS ESPECÍFICOS

Antes de comenzar a monitorear los recursos de AWS, se recomienda crear un plan de monitorización que responda a preguntas como.

- ¿Cuáles son los objetivos del monitoreo?
- ¿Qué recursos va a monitorizar?
- ¿Con qué frecuencia va a monitorizar estos recursos?
- ¿Qué herramientas de monitoreo va a utilizar?
- ¿Quién se encargará de realizar las tareas de monitoreo?
- ¿Quién debería recibir una notificación cuando surjan problemas?

A continuación, se detallan las acciones de monitorización para algunos de los servicios más comunes de AWS.

3.1 MONITORIZACIÓN DE AMAZON EC2

Después de definir los objetivos y de crear el plan de monitoreo, el paso siguiente consistirá en establecer un punto de referencia para el desempeño normal de Amazon EC2 en el entorno. Conviene medir el desempeño de Amazon EC2 en varias ocasiones y con diferentes condiciones de carga. A medida que monitorea Amazon EC2, guarde un historial de los datos de monitoreo que recopila. Puede comparar el desempeño actual de Amazon EC2 con los datos históricos para identificar patrones de desempeño normal y anomalías en el desempeño, así como desarrollar métodos para solucionarlos. Por ejemplo, puede monitorizar el uso de la CPU, la E/S de disco y el uso de la red de las instancias EC2. Si el desempeño no alcanza los valores del punto de referencia establecido, es posible que deba volver a configurar u optimizar la instancia para reducir la utilización de la CPU, mejorar la E/S de disco o reducir el tráfico de red.

Para establecer un punto de referencia se recomienda, como mínimo, monitorizar los elementos siguientes:

- Utilización de la CPU.
- Utilización de la red.
- Desempeño de disco.
- Escrituras/lecturas en disco.
- Utilización de memoria, utilización de intercambio de disco, utilización de espacio de disco, utilización de archivo de página, recopilación de logs.

AWS proporciona varias herramientas que puede usar para monitorear Amazon EC2. Se pueden configurar algunas de estas herramientas para que monitoreen automáticamente, pero otras herramientas requieren intervención manual.

Herramientas de monitoreo automatizadas

Se pueden utilizar las siguientes herramientas de monitoreo automatizada para vigilar Amazon EC2 y recibir información cuando algo va mal:

- Comprobaciones de estado de sistemas: monitorea los sistemas de AWS necesarios para usar la instancia y garantiza que funcionan correctamente. Estas comprobaciones detectan problemas con la instancia que requieren la intervención de AWS para su reparación. Cuando una comprobación de estado del sistema da error, puede elegir entre esperar a que AWS corrija el problema o solucionarlo manualmente (por ejemplo: al parar y reiniciar la instancia, o bien, al terminar y reemplazar una instancia). Entre los ejemplos de problemas que provocan errores en las comprobaciones de estado del sistema se incluyen:
    - Pérdida de conectividad de red,
    - Pérdida de potencia del sistema,

- Problemas de software en el host físico,
- Problemas de hardware en el host físico que afectan a la accesibilidad a la red.

- Comprobaciones de estado de instancias: monitorear la configuración de software y de red de la instancia individual. Estas comprobaciones detectan problemas que requieren su implicación para la reparación. Cuando una comprobación de estado de instancias da error, por lo general, se deberá resolver el problema manualmente (por ejemplo, reiniciando la instancia o efectuando modificaciones en el sistema operativo). Entre los ejemplos de problemas que pueden provocar errores en las comprobaciones de estado de la instancia se incluyen:
  - Error de las comprobaciones de estado del sistema
  - Configuración de red o de inicio incorrecta
  - Memoria agotada
  - Sistema de archivos dañado
  - Kernel incompatible

Para obtener más información, puede consultar: Comprobaciones de estado para sus instancias.

- Alarmas de Amazon CloudWatch: vigilar una única métrica durante el período especificado y realizar una o varias acciones según el valor de la métrica relativo a un determinado umbral durante varios períodos de tiempo. La acción es una notificación que se envía a un tema de Amazon Simple Notification Service (Amazon SNS) o a una política de Amazon EC2 Auto Scaling. Las alarmas invocan acciones únicamente para los cambios de estado prolongados. Las alarmas de Amazon CloudWatch no invocarán acciones tan solo por tener un estado determinado; es necesario que el estado haya cambiado y se mantenga durante un número específico de periodos.

  Para obtener más información, se puede consultar: Monitorear las instancias con Amazon CloudWatch.

- Amazon EventBridge: automatizar los servicios de AWS y responder automáticamente a los eventos del sistema. Los eventos de los servicios de AWS llegan a Amazon EventBridge prácticamente en tiempo real y puede especificar acciones automatizadas para cuando un evento coincide con una de las reglas que ha escrito.

  Para obtener más información, se puede consultar: ¿Qué es Amazon EventBridge?

- Amazon CloudWatch Logs: monitorear, almacenzar y tener acceso a los archivos de log desde instancias de Amazon EC2, AWS CloudTrail u otras fuentes.

  Para obtener más información, sepuede consultar la Guía del usuario de Amazon CloudWatch Logs.

- Agente de CloudWatch: recopilar logs y métricas de nivel de sistema tanto desde hosts como invitados en las instancias EC2 y servidores en las instalaciones.

  Para obtener más información, se puede consultar: Recopilación de métricas y logs de instancias Amazon EC2 y servidores locales con el agente de CloudWatch en la Guía del usuario de Amazon CloudWatch.

- AWS Management Pack para Microsoft System Center Operations Manager: vincula las instancias de Amazon EC2 con los sistemas operativos Windows o Linux que ejecutan. AWS Management Pack es una extensión de Microsoft System Center Operations Manager. Utiliza un equipo designado en el centro de datos (llamado nodo de monitor) y las API de Amazon Web Services para detectar y recopilar de forma remota información sobre los recursos de AWS. Para obtener más información, se puede consultar:consulte AWS Management Pack para Microsoft System Center.

Herramientas de monitoreo manuales.

Otra parte importante del monitoreo de Amazon EC2 implica el monitoreo manual de los elementos que no cubren los scripts, las comprobaciones de estado y las alarmas de Amazon CloudWatch. Los paneles de consola de Amazon EC2 y de Amazon CloudWatch proporcionan una vista rápida del entorno de Amazon EC2.

- El panel de Amazon EC2 muestra:
  - El estado del servicio y los eventos programados por región.
  - El estado de la instancia.
  - Las comprobaciones de estado.
  - El estado de la alarma.
  - Detalles de las métricas de la instancia (en el panel de navegación, elija Instances [Instancias], seleccione una instancia y elija la pestaña Monitoring [Monitoreo]).
  - Detalles de las métricas del volumen (en el panel de navegación, elija Volumes [Volúmenes], seleccione un volumen y elija la pestaña Monitoring [Monitoreo]).
- El panel de Amazon CloudWatch muestra:
  - Alarmas y estado actual.
  - Gráficos de alarmas y recursos.
  - Estado de los servicios.

Además, se puede utilizar Amazon CloudWatch para hacer lo siguiente:

- Gráfico con los datos de monitoreo de Amazon EC2 para solucionar problemas y descubrir tendencias.
- Buscar y examinar todas sus métricas de recursos de AWS.

- Crear y editar las alarmas de notificación de problemas.
- Consultar información general sobre alarmas y recursos de AWS.

3.2 MONITORIZACIÓN DE AMAZON S3

La monitorización es una parte importante a la hora de mantener la fiabilidad, la disponibilidad y el rendimiento de Amazon S3 y las soluciones de AWS. Recomendamos que recopile los datos de supervisión de todas las partes de la solución de AWS para que le resulte más sencillo depurar un error multipunto en caso de que se produzca.

AWS proporciona herramientas de monitorización que pueden ser automatizadas, pero otras requieren de intervención manual. Se recomienda que se automaticen las tareas de monitorización en la medida de lo posible.

Herramientas de monitoreo automatizadas

Las siguientes herramientas de monitoreo automatizadas se puede utilizar para vigilar Amazon S3 e informar cuando haya algún problema:

- Métricas de Amazon CloudWatch: Las métricas de Amazon CloudWatch para Amazon S3 pueden ayudar a comprender y mejorar el rendimiento de las aplicaciones que utilizan Amazon S3. Existen varias formas de utilizar Amazon CloudWatch con Amazon S3.
    - Métricas de almacenamiento diario para buckets. Pueden monitorear el almacenamiento de buckets mediante Amazon CloudWatch, que recopila y procesa datos de almacenamiento de Amazon S3 en métricas diarias legibles. El informe de estas métricas de almacenamiento para Amazon S3 se realiza una vez al día.
    - Métricas de solicitudes. Permiten monitorear las solicitudes de Amazon S3 para identificar rápidamente los problemas operativos y actuar en consecuencia. Las métricas están disponibles en intervalos de 1 minuto después de un breve periodo de latencia para procesarlas.

      Para saber cómo activar la obtención de estas métricas, consulte Configuraciones de métricas de CloudWatch.
    - Métricas de replicación. Monitorizar el número total de operaciones de la API de S3 que están pendientes de replicación, el tamaño total de los objetos pendientes de replicación y el tiempo máximo de replicación en la región de destino. Las reglas de replicación que tengan activado el control de tiempo de replicación de S3 (S3 RTC) o las métricas de replicación de S3 habilitadas publicarán métricas de replicación.

      Para obtener más información, se puede consultar: Monitorización del progreso con métricas de replicación y notificaciones de eventos de Amazon S3.

- Métricas de Amazon S3 Storage Lens. Puede publicar métricas de actividad y uso de S3 Storage Lens en Amazon CloudWatch para crear una vista unificada del estado operativo en los paneles de Amazon CloudWatch. Las métricas de S3 Storage Lens están disponibles en el espacio de nombres de AWS/S3/Storage-Lens. La opción de publicación de Amazon CloudWatch está disponible para los paneles de S3 Storage Lens actualizados a métricas y recomendaciones avanzadas. Puede habilitar la opción de publicación de Amazon CloudWatch para una configuración de panel nueva o existente en S3 Storage Lens.

  Para obtener más información, se puede consultar: Monitoreo de métricas de S3 Storage Lens en CloudWatch.

- Monitoreo de logs de AWS CloudTrail: compartir archivos de logs entre cuentas, monitorear los archivos de logs de AWS CloudTrail en tiempo real enviándolos a Amazon CloudWatch Logs, escribir aplicaciones de procesamiento de logs en Java y compruebar que los archivos de logs no hayan cambiado después de que AWS CloudTrail los entregara.

  Para obtener más información, se puede consultar: Registro de llamadas a la API de Amazon S3 mediante AWS CloudTrail.

Herramientas de monitoreo manuales.

Otra parte importante del monitoreo de Amazon S3 implica la monitorización manual de los elementos que no cubren las alarmas de Amazon CloudWatch. Amazon S3, Amazon CloudWatch, AWS Trusted Advisor y otros paneles de AWS Management Console proporcionan una vista rápida del estado de su entorno de AWS. Es posible que se desee habilitar el log de acceso al servidor, que se realice un seguimiento de las solicitudes de acceso al bucket. Cada entrada del log de acceso contiene detalles de la solicitud de acceso tales como el solicitante, el nombre del bucket, la hora de la solicitud, la acción solicitada, el estado de la respuesta y el código de error, si hay alguno. Para obtener más información, se puede consultar: Registro de solicitudes mediante el log de acceso al servidor.

El panel de Amazon S3 muestra los buckets, los objetos y las propiedades que contienen.

- La página principal de Amazon CloudWatch muestra:
  - Alarmas y estado actual.
  - Gráficos de alarmas y recursos.
  - Estado de los servicios.

  Además, se puede utilizar Amazon CloudWatch para:

  - Crear paneles personalizados para monitorear los servicios que le interesan.
  - Realizar un gráfico con los datos de las métricas para resolver problemas y descubrir tendencias.
  - Buscar y examinar todas sus métricas de recursos de AWS.

- Crear y editar las alarmas de notificación de problemas.

Por otra parte, también se puede utilizar AWS Trusted Advisor (descrito en la sección 2.8.5) para la monitorización de Amazon S3. Concretamente, las verificaciones relacionadas con Amazon S3 son:Comprobaciones de la configuración de logs de los buckets de Amazon S3.

- Comprobaciones de seguridad de los buckets de Amazon S3 que tienen permisos de acceso abierto.
- Comprobaciones de la tolerancia a errores de los buckets de Amazon S3 que no tienen activado el control de versiones, o que lo tienen suspendido.

3.3 MONITORIZACIÓN DE AMAZON EKS

Amazon Elastic Kubernetes Service (Amazon EKS) se integra con Amazon CloudWatch Logs para el plano de control de Kubernetes. Amazon EKS proporciona el plano de control como un servicio administrado y puede activar el log sin instalar un agente de CloudWatch, aunque el agente de Amazon CloudWatch también se puede implementar para capturar logs de nodos y contenedores de Amazon EKS.

Se puede instalar y configurar el agente de Amazon CloudWatch en los nodos de Amazon EKS para alinear los nodos de Amazon EKS con las configuraciones estándar de log y supervisión del sistema.

Kubernetes proporciona una API de métricas que permite acceder a las métricas de uso de recursos (por ejemplo, uso de CPU y memoria para nodos y pods), pero la API solo proporciona información puntual y no métricas históricas.

El log de Kubernetes se puede dividir en log de planos de control, log de nodos y log de aplicaciones.

Log de plano de control de Amazon EKS.

El plano de control de Kubernetes es un conjunto de componentes que administran clústeres de Kubernetes y producen logs utilizados para fines de auditoría y diagnóstico. Con Amazon EKS, se pueden activar logs para distintos componentes del plano de control y enviarlos a Amazon CloudWatch.

Un clúster de Amazon EKS consta de un plano de control de un solo tenant de alta disponibilidad para el clúster de Kubernetes y los nodos de Amazon EKS que ejecutan los contenedores. Los nodos del plano de control se ejecutan en una cuenta administrada por AWS. Los nodos de plano de control de clúster de Amazon EKS están integrados con Amazon CloudWatch y se puede activar el registro para componentes de planos de control específicos.

Se proporcionan logs para cada instancia de componente del plano de control de Kubernetes. AWS administra el estado de los nodos del plano de control y proporciona un acuerdo de nivel de servicio (SLA) para el endpoint de Kubernetes.

Logs de nodos y aplicaciones de Amazon EKS

Se recomienda que se utilice Amazon CloudWatch Container Insights para capturar logs y métricas para Amazon EKS. Información sobre contenedores implementa métricas de nivel de clúster, nodo y pod con el agente de Amazon CloudWatch y Fluent Bit o Fluente para la captura de logs en Amazon CloudWatch. Container Insights también proporciona paneles automáticos con vistas en capas de las métricas de Amazon CloudWatch capturadas. Container Insights se implementa como Amazon CloudWatch DaemonSet y Fluent Bit DaemonSet que se ejecuta en todos los nodos de Amazon EKS.

3.4 MONITORIZACIÓN DE AWS SYSTEMS MANAGER

AWS proporciona varias herramientas para monitorear sus recursos de AWS Systems Manager y otros recursos, y responder a posibles incidentes.

Logs de AWS CloudTrail

AWS CloudTrail proporciona un log de las acciones que realiza un usuario, un rol o un Servicio de AWS en AWS Systems Manager. Mediante la información recopilada por AWS CloudTrail, puede determinar la solicitud que se realizó a AWS Systems Manager, la dirección IP desde la que se realizó, quién la realizó y cuándo, etc.

Para obtener más información, se puede consultar: Registrar llamadas a la API de AWS Systems Manager con AWS CloudTrail .

Paneles de Amazon CloudWatch

Los paneles de Amazon CloudWatch son páginas de inicio personalizables en la consola de Amazon CloudWatch que se pueden utilizar para monitorear sus recursos en una vista única, incluso aquellos que se reparten entre diferentes Regiones de AWS. Se pueden utilizar los paneles de Amazon CloudWatch para crear vistas personalizadas de las métricas y las alarmas para sus recursos de AWS.

Para obtener más información, se puede consultar: Paneles de Amazon CloudWatch alojados por AWS Systems Manager .

Amazon EventBridge

Con Amazon EventBridge, se pueden configurar reglas para recibir una alerta de los cambios que se produzcan en los recursos de AWS Systems Manager y para dirigir a Amazon EventBridge para que realice acciones basadas en el contenido de esos eventos. Amazon EventBridge admite una serie de eventos emitidos por varias capacidades de AWS Systems Manager.

Para obtener más información, se puede consultar: Monitoreo de eventos de AWS Systems Manager con Amazon EventBridge

Conformidad de AWS Systems Manager

Se puede utilizar Compliance, una capacidad de AWS Systems Manager, para analizar la flota de nodos administrados en busca de conformidad de revisiones e incoherencias de configuración. Se puede recopilar y agregar datos de varias Cuentas de AWS y Regiones de AWS, y luego desglosarlas en recursos específicos que no sean conformes. De forma predeterminada, Compliance muestra datos de conformidad actuales sobre la aplicación de revisiones en Patch Manager, una capacidad de AWS Systems Manager, y asociaciones en State Manager, una capacidad de AWS Systems Manager.

Para obtener más información, se puede consultar: Conformidad de AWS Systems Manager .

AWS Systems Manager Explorer

Explorer, una capacidad de AWS Systems Manager, es un panel de operaciones personalizable que transmite información sobre sus recursos de AWS. Explorer muestra una vista agregada de los datos de operaciones (OpsData) de sus Cuentas de AWS y en todas las Regiones de AWS. En Explorer, OpsData incluye metadatos sobre instancias EC2, detalles de conformidad de parches y elementos de trabajo operativos (OpsItems). Explorer proporciona un contexto sobre cómo OpsItems se distribuyen entre las unidades de negocio o las aplicaciones, cómo se presentan a lo largo del tiempo y cómo varían según la categoría. Se puede agrupar y filtrar la información en Explorer para centrarse en los elementos que son relevantes y que requieren que se tomen medidas. Para obtener más información, se puede consultar: AWS Systems Manager Explorer .

AWS Systems Manager OpsCenter

OpsCenter, una capacidad de AWS Systems Manager, proporciona una ubicación central en la que los ingenieros de operaciones y los profesionales de TI pueden ver, investigar y resolver elementos de trabajo operativos (OpsItems) relacionados con los recursos de AWS. OpsCenter agrega y estandariza OpsItems en todos los servicios, al tiempo que proporciona datos de investigación contextuales sobre cada OpsItem, OpsItems relacionados y recursos relacionados. OpsCenter también proporciona manuales de procedimientos de Automation, una capacidad de AWS Systems Manager, que se pueden utilizar para resolver problemas rápidamente. OpsCenter se integra a Amazon EventBridge. Esto significa que se pueden crear reglas de Amazon EventBridge que generan automáticamente OpsItems para cualquier Servicio de AWS que publica eventos en Amazon EventBridge.

Para obtener más información, se puede consultar: AWS Systems Manager OpsCenter .

Amazon Simple Notification Service

Se puede configurar Amazon Simple Notification Service (Amazon SNS) para que envíe notificaciones sobre el estado de los comandos que envía a través de Run Command o Maintenance Windows, capacidades de AWS Systems Manager. Amazon SNS coordina y administra el envío y la entrega de las notificaciones a los clientes o puntos de enlace

que estén suscritos a temas de Amazon SNS.Se puede recibir una notificación siempre que un comando cambie a un nuevo estado o a un estado específico, como, por ejemplo, Failed o Timed Out. En los casos en que un comando se envía a varios nodos, se puede recibir una notificación por cada copia del comando enviada a un nodo concreto.

Para obtener más información, se puede consultar: Monitoreo de los cambios de estado de AWS Systems Manager mediante las notificaciones de Amazon SNS.

3.5 MONITORIZACIÓN DE RECURSOS DE DIRECT CONNECT

Monitorización de los recursos de DirectConnect con Amazon CloudWatch

Las conexiones físicas y las interfaces virtuales de AWS Direct Connect se pueden monitorizar mediante Amazon CloudWatch. De forma predeterminada, AWS Direct Connect proporciona datos a Amazon CloudWatch en intervalos de 5 minutos.

Algunas de las métricas que se ofrecen para las conexiones son:

- ConnectionState: El estado de la conexión. 1 indica “activa” y 0 “inactiva”.
- ConnectionBpsEgress: Velocidad de bits de los datos de salida del extremo de AWS de la conexión.
- ConnectionBpsIngress: Velocidad de bits de los datos de entrada del extremo de AWS de la conexión.
- ConnectionPpsEgress: Velocidad del paquete de datos de salida del extremo de AWS de la conexión.
- ConnectionPpsIngress: La velocidad del paquete de datos de entrada del extremo de AWS de la conexión.
- ConnectionErrorCount: El recuento total de errores de todos los tipos a nivel de MAC en el dispositivo de AWS.
- ConnectionLightLevelTx: Indica el estado de la conexión de fibra para el tráfico de salida del extremo de AWS de la conexión.
- ConnectionLightLevelRx: Indica el estado de la conexión de fibra para el tráfico de entrada del extremo de AWS de la conexión.
- ConnectionEncryptionState: Indica el estado de cifrado de la conexión. 1 indica que el estado es “up” y 0 indica que el estado es “down”.

En cuanto a las métricas disponibles desde las interfaces virtuales de AWS DirectConnect, encontramos:

- VirtualInterfacesBpsEgress: La velocidad de bits de los datos de salida del extremo de AWS de la interfaz virtual.
- VirtualInterfacesBpsIngress: La velocidad de bits de los datos de entrada del extremo de AWS de la interfaz virtual.
- VirtualInterfacesPpsEgress: La velocidad del paquete de datos de salida del extremo de AWS de la interfaz virtual.

- VirtualInterfacesPpsIngress: La velocidad del paquete de datos de entrada del extremo de AWS de la interfaz virtual.

Log de llamadas a la API de AWS Direct Connect con AWS CloudTrail

Todas las acciones de DirectConnect se registran en CloudTrail. Por ejemplo, las llamadas a la API para la creación de interfaces virtuales privadas o para la creación de conexiones. Cada entrada de registro contiene información sobre quién generó la solicitud, y permite identificar aspectos como si la solicitud se realizó con credenciales raíz o de IAM, si fue un rol o un usuario federado o si se realizó a través de otro servicio de AWS.

3.6. MONITORIZACIÓN DE RECURSOS DE AWS LAMBDA

Lambda funciona automáticamente con las métricas y los logs de Amazon CloudWatch sin más configuración o instrumentación del código de la aplicación.

Log de funciones de AWS Lambda

Lambda transmite automáticamente la salida y los mensajes de error estándar desde las funciones AWS Lambda a Amazon CloudWatch. También aprovisiona automáticamente los contenedores que ejecutan la función Lambda y los configura para generar mensajes de log en flujos de logs independientes.

Lambda crea automáticamente un grupo de logs cuando se invoca por primera vez la función Lambda y se crea un flujo de logs independiente en el grupo de logs para cada instancia de función de Lambda. Todos los logs de las invocaciones de la función Lambda se almacenan en el mismo grupo de logs. El nombre no se puede cambiar y se encuentra en almacenada con el formato aws/lambda/<nombredelafunciónLambda>.

Es recomendable utilizar una biblioteca de logs para dar formato y clasificar los mensajes de logs. También se recomienda registrar los mensajes en formato JSON para poder consultarlos desde Amazon CloudWatch Log Insights.

Otra práctica recomendada es establecer el nivel de salida del log mediante una variable y ajustarla según el entorno y los requisitos. El código de la función Lambda, además de las bibliotecas utilizadas, podría generar una gran cantidad de datos de log según el nivel de salida del log, lo que puede afectar los costes de almacenamiento y al rendimiento.

Envío de logs a otros destinos desde Amazon CloudWatch

Se puede enviar logs a otros destinos, como Amazon OpenSearch, mediante filtros de suscripción. Si no se utiliza Amazon OpenSearch, se puede utilizar una función de Lambda para procesar los logs y enviarlos a un servicio de AWS mediante el SDK.

También se puede utilizar SDK para destinos fuera de la nube de AWS. Si se elige esta opción, es recomendable considerar el impacto de la latencia, el tiempo de

procesamiento adicional, la gestión de errores y reintentos y el acoplamiento de la lógica operativa a la función Lambda.

Métricas de funciones de AWS Lambda

Comprender las métricas de rendimiento e invocación a nivel de sistema para las funciones Lambda ayuda a optimizar la configuración de los recursos y a mejorar el rendimiento del código. Supervisar y medir eficazmente el rendimiento puede mejorar la experiencia del usuario y reducir los costes mediante el tamaño adecuado de las funciones de Lambda. Normalmente, las cargas de trabajo que se ejecutan como funciones de Lambda también tienen métricas a nivel de aplicación que deben capturarse y analizarse. Lambda admite directamente el formato métrico integrado para hacer la captura a nivel de aplicación más fáciles.

- Métricas a nivel de sistema: Amazon CloudWatch proporciona Amazon CloudWatch Lambda Insights, que recopila, agrega y resume las métricas de nivel de sistema (por ejemplo, tiempo de CPU, memoria, disco y uso de red). Lambda Insights también recopila, agrega y resume información de diagnóstico para ayudar a aislar y resolver problemas rápidamente.
- Métricas de aplicación: También se pueden crear y capturar métricas de aplicación en Amazon CloudWatch utilizando el formato de métricas integradas. La instalación de Amazon CloudWatch y su integración con Lambda está configurada para procesar y extraer sentencias de formato métrico con el formato adecuado.

4. GLOSARIO

A continuación de describen una serie de términos, acrónimos y abreviaturas en materia de seguridad utilizados en esta guía.

Término	Definición
ACL	Access Control List (Lista de Control de Acceso)
Amazon WorkDocs	Es un servicio completamente administrado y seguro de creación de contenido, almacenamiento y colaboración.
API	Application Programming Interface (Interfaz de Programación de Aplicaciones)

Bucket	Contenedor para almacenar objetos (archivos) pertenecientes al servicio S3
DNS	Sistema de nombres de dominio.
EC2	Servicio web para lanzar y administrar instancias Linux/UNIX y Windows Server en los centros de datos de Amazon.
ENS	Esquema Nacional de Seguridad.
IAM	Identity and Access Management (gestión de accesos e identidades).
Instancia	Servidor virtual en la nube de AWS.
IAM	Identity and Access Management (gestión de accesos e identidades).
Instancia	Servidor virtual en la nube de AWS.
MFA	Multi-factor Authentication (autenticación multi factor).
PCoIP	PC over IP.
Instancia	Servidor virtual en la nube de AWS.
Security Group	Un grupo de seguridad funciona como un firewall virtual para las instancias EC2 para controlar el tráfico entrante y saliente.

TCP	Protocolo de control de transmisión.
Security Group	Un grupo de seguridad funciona como un firewall virtual para las instancias EC2 para controlar el tráfico entrante y saliente.
VPC	Red virtual privada.
WorkSpaces	Escritorio como servicio (DaaS).
WSP	Amazon WorkSpaces Streaming Protocol

5. GLOSARIO DE SERVICIOS AWS

A continuación, se reúnen los diferentes servicios mencionados a lo largo de esta guía incluyendo enlaces a la documentación concreta de cada uno de ellos. Como complemento de estos documentos se recomienda el uso del siguiente recurso enfocado a los aspectos de seguridad de cada uno de ellos:

Servicio	URL de documentación del servicio
Amazon CloudTrail	https://docs.aws.amazon.com/es_es/awscloudtrail/latest/userguide/cloudtrail-user-guide.html
Amazon CloudWatch	https://docs.aws.amazon.com/es_es/AmazonCloudWatch/latest/monitoring/WhatIsCloudWatch.html
Amazon EC2	https://docs.aws.amazon.com/es_es/config/latest/developerguide/how-does-config-work.html
Amazon Identity & Access Management (IAM)	https://docs.aws.amazon.com/es_es/IAM/latest/UserGuide/introduction.html
Amazon Macie	https://docs.aws.amazon.com/es_es/macie/latest/userguide/what-is-macie.html
Amazon S3	https://docs.aws.amazon.com/es_es/AmazonS3/latest/userguide/Welcome.html

Amazon SNS	https://docs.aws.amazon.com/es_es/sns/latest/dg/welcome.html
Amazon VPC	https://docs.aws.amazon.com/es_es/vpc/latest/userguide/what-is-amazon-vpc.html
AWS Config	https://docs.aws.amazon.com/es_es/config/latest/developerguide/WhatIsConfig.html
AWS Control Tower	https://docs.aws.amazon.com/es_es/controltower/latest/userguide/what-is-control-tower.html
AWS Key Management Service (KMS)	https://aws.amazon.com/es/kms/
AWS Lambda	https://docs.aws.amazon.com/es_es/lambda/latest/dg/welcome.html
AWS Security Hub	https://docs.aws.amazon.com/es_es/securityhub/latest/userguide/what-is-securityhub.html
AWS VPN	https://docs.aws.amazon.com/es_es/vpn/latest/s2svpn/VPC_VPN.html
AWS WAF	https://docs.aws.amazon.com/es_es/waf/latest/developerguide/what-is-aws-waf.html

PUBLICACIONES DE DEFENSA

GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA
SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL