COLOMBIA POTENCIA DE LA VIDA

TIC

# LECCIÓN 2: SERVICIOS DE AWS QUE ADMITEN LA FASE DE DESCUBRIMIENTO Y RECONOCIMIENTO

TALENTO TECH | AZ PROYECTOS EDUCATIVOS | UTP Universidad Tecnológica de Pereira

COLOMBIA POTENCIA DE LA VIDA

TIC

# FASE DE DESCUBRIMIENTO Y RECONOCIMIENTO

TALENTO TECH

AZ | PROYECTOS EDUCATIVOS

UTP Universidad Tecnológica de Pereira

## Observe que estos no son todos los servicios de AWS disponibles.

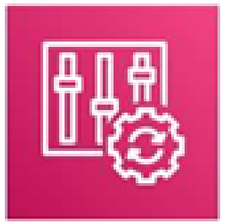
AWS Trusted Advisor

Amazon CloudWatch

Amazon Inspector

Amazon GuardDuty

AWS Shield



AWS Config

AWS ofrece varios servicios que admiten el descubrimiento y el reconocimiento de incidentes. Estos servicios ayudan a una empresa a identificar un ataque.

En esta lección, se describirán los siguientes servicios con más detalle y cómo respaldan esta fase de respuesta ante incidentes:

- AWS Trusted Advisor
- Amazon CloudWatch
- Amazon Inspector
- Amazon GuardDuty
- AWS Shield
- AWS Config

# AWS TRUSTED ADVISOR

- Se basa en las prácticas recomendadas aprendidas al atender a cientos de miles de clientes de AWS.

- Inspecciona su entorno de AWS y luego hace recomendaciones cuando existen oportunidades para mejorar el rendimiento y ayudar a cerrar las fallas de seguridad.

El servicio AWS Trusted Advisor se basa en las prácticas recomendadas aprendidas al atender a cientos de miles de clientes de AWS. Trusted Advisor inspecciona su entorno de AWS y luego hace recomendaciones cuando surgen oportunidades para mejorar el rendimiento y ayudar a solucionar las brechas de seguridad.

Si tiene un plan de AWS Basic Support o Developer Support, puede utilizar la consola de administración de AWS para acceder a las comprobaciones de seguridad principales y todas las comprobaciones de las cuotas de servicio. Si tiene un plan Business, Enterprise On-Ramp o Enterprise Support, puede usar la consola, la API de AWS Support y la Command Line Interface de AWS (AWS CLI) para acceder a todas las comprobaciones, incluida la optimización de costos, la seguridad, la tolerancia a errores, el rendimiento y las cuotas de servicio.

También puede usar Amazon EventBridge para supervisar el estado de las verificaciones de Trusted Advisor.

Para más información, consulte AWS Trusted Advisor en la Guía del usuario de AWS Support en https://docs.aws.amazon.com/awssupport/latest/user/trusted-advisor.html

# AMAZON CLOUDWATCH

- **Proporciona una solución de supervisión confiable, escalable y flexible que puede comenzar a usar en minutos.**

- **Muestra automáticamente métricas sobre cada servicio de AWS que utiliza.**

- **Brinda la capacidad de crear alarmas que observan métricas y envían notificaciones.**

Amazon CloudWatch proporciona una solución de monitoreo confiable, escalable y flexible que podrá iniciar en cuestión de minutos. Al usar este servicio, no tendrá que configurar, administrar ni escalar sus propios sistemas de supervisión ni su propia infraestructura.

La página de inicio de la consola de CloudWatch muestra automáticamente métricas sobre cada servicio de AWS que utiliza. Además, puede crear paneles personalizados para mostrar métricas sobre sus aplicaciones personalizadas y mostrar colecciones personalizadas de métricas que elija.

Puede crear alarmas para vigilar las métricas y enviar notificaciones, o realizar cambios automáticamente en los recursos que está supervisando cuando se supera un umbral.

Con CloudWatch, obtiene visibilidad de todo el sistema respecto de la utilización de los recursos, el rendimiento de las aplicaciones y el estado operativo.

Para más información, consulte la Guía del usuario de Amazon CloudWatch en https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/WhatIsCloudWatch.html.

# AMAZON INSPECTOR

- Es un servicio de administración de vulnerabilidades que escanea continuamente sus cargas de trabajo de AWS en busca de vulnerabilidades.

- Detecta y escanea automáticamente instancias de Amazon Elastic Compute Cloud (Amazon EC2) e imágenes de contenedores que residen en Amazon Elastic Container Registry (Amazon ECR).

- Crea un hallazgo cuando descubre una vulnerabilidad o un problema de red.

Amazon Inspector es un servicio de administración de vulnerabilidades que escanea continuamente sus cargas de trabajo de AWS en busca de vulnerabilidades. Amazon Inspector descubre y analiza automáticamente instancias de Amazon Elastic Compute Cloud (Amazon EC2) e imágenes de contenedor ubicadas en Amazon Elastic Container Registry (Amazon ECR) en busca de vulnerabilidades y exposición de red no intencionadas.

Cuando Amazon Inspector descubre una vulnerabilidad de software o un problema de red, el servicio crea un hallazgo. Un hallazgo describe la vulnerabilidad, identifica el recurso afectado, califica la gravedad de la vulnerabilidad y brinda orientación para la corrección.

Para más información, consulte la Guía del usuario de Amazon Inspector en https://docs.aws.amazon.com/inspector/latest/user/what-is-inspector.html

# AMAZON GUARDDUTY

- **Es un servicio de monitoreo de seguridad continuo.**

- **Identifica actividades inesperadas y potencialmente no autorizadas o malintencionadas.**

- **Utiliza fuentes de inteligencia sobre amenazas.**

**Amazon GuardDuty es un servicio de supervisión de seguridad continuo. Puede ayudar a identificar actividad inesperada o potencialmente malintencionada o no autorizada en el entorno de AWS.**

El servicio utiliza fuentes de inteligencia sobre amenazas, como listas de direcciones IP y dominios malintencionados, y machine learning para identificar actividades inesperadas y potencialmente no autorizadas y maliciosas dentro de su entorno de AWS. Esto puede incluir problemas como aumentos de privilegios, uso de credenciales expuestas o comunicación con direcciones IP o dominios malintencionados. Por ejemplo, GuardDuty puede detectar instancias de EC2 comprometidas que sirven malware o extraen bitcoins. El servicio también supervisa el comportamiento de acceso a la cuenta de AWS en busca de signos de compromiso, como implementaciones de infraestructura no autorizadas (por ejemplo, instancias que se implementan en una región que nunca se ha utilizado) y llamadas API inusuales (por ejemplo, un cambio de política de contraseñas para reducir la seguridad de la contraseña).

Para más información, consulte la Guía del usuario de Amazon GuardDuty en https://docs.aws.amazon.com/guardduty/latest/ug/what-is-guardduty.html

# AWS SHIELD

- **Protege automáticamente una red empresarial de un ataque por denegación de servicio distribuido (DDoS).**

- **Ofrece el servicio de protección contra amenazas administrado de AWS Shield Advanced para mejorar su postura de seguridad con capacidades adicionales de detección, mitigación y respuesta de DDoS.**

AWS Shield ayuda a proteger una red empresarial contra un ataque por denegación de servicio distribuido (DDoS). Un ataque DDoS es un intento malintencionado de interrumpir el tráfico normal de un servidor, servicio o red dirigidos mediante la sobrecarga del objetivo o de su infraestructura circundante con una inundación de tráfico de Internet. Desde un nivel alto, un ataque DDoS es como un embotellamiento de tráfico inesperado que obstruye la carretera e impide que el tráfico regular llegue a su destino.

Cuando crea su aplicación en AWS, recibe protección automática contra ataques DDoS comunes. Además, puede utilizar el servicio de protección contra amenazas administrado AWS Shield Advanced para mejorar su postura de seguridad con capacidades adicionales de detección, mitigación y respuesta ante ataques de DDoS.

Para más información, consulte AWS Shield en la Guía del Desarrollador de AWS WAF, AWS Firewall Manager y AWS Shield Advanced en https://docs.aws.amazon.com/waf/latest/developerguide/shield-chapter.html.

# AWS CONFIG

- Es un servicio de supervisión y evaluación continuos.

- Brinda la capacidad de ver las configuraciones actuales e históricas de un recurso y usar esta información para solucionar problemas de interrupciones.

- Envía notificaciones cuando se producen cambios.

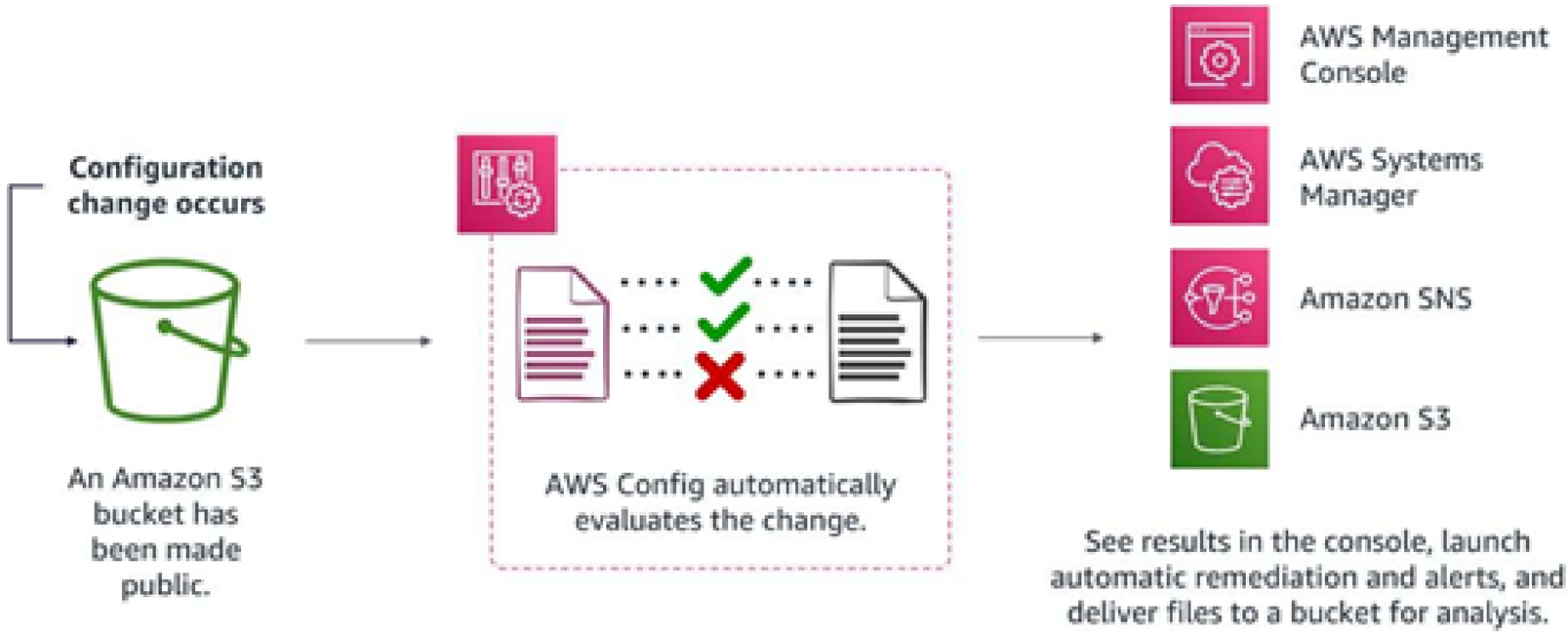
- Se integra en otros servicios de AWS para solucionar problemas.

AWS Config es un servicio continuo de supervisión y evaluación que le proporciona un inventario de sus recursos de AWS y registra los cambios en la configuración de dichos recursos. Puede ver las configuraciones actuales e históricas de un recurso y usar esta información para solucionar problemas de interrupciones y realizar análisis de ataques de seguridad. También puede ver la configuración en cualquier momento y usar esa información para reconfigurar sus recursos y llevarlos a un estado estable durante una situación de interrupción.

AWS Config envía notificaciones cuando se producen cambios y se integra con otros servicios de AWS para solucionar problemas.

Para más información, consulte la Guía del usuario de AWS Config en https://docs.aws.amazon.com/config/latest/developerguide/WhatIsConfig.html.

# REGLAS DE EVALUACIÓN

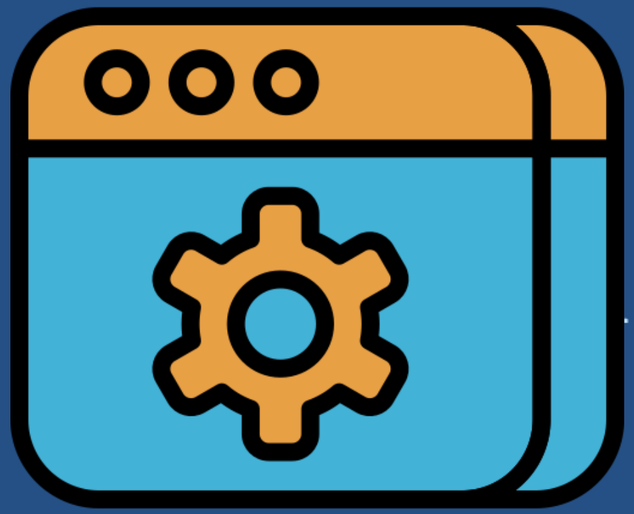


COLOMBIA POTENCIA DE LA VIDA

TIC

## Diagrama de evaluación de las reglas de AWS Config.

Se produce un cambio de configuración. En este ejemplo, se ha hecho público un bucket de S3. AWS Config evalúa automáticamente el cambio. Los resultados se pueden ver en la consola. Systems Manager y Amazon SNS se utilizan para invocar alertas y corrección automática. Los archivos se envían a un bucket de S3 para su análisis.



TALENTO TECH

AZ | PROYECTOS EDUCATIVOS

UTP Universidad Tecnológica de Pereira

A medida que se producen cambios de configuración en sus recursos de AWS, AWS Config registra y normaliza los cambios en un formato coherente. AWS Config evalúa automáticamente los cambios registrados con respecto a las reglas que ha establecido. A continuación, puede acceder al historial de cambios y a los resultados de cumplimiento mediante la consola o la API. Puede configurar Systems Manager o Amazon SNS para que se invoque y corregir o alertarle cuando se produzcan cambios. También puede enviar el historial de cambios y los archivos de instantáneas de los recursos supervisados a un bucket de S3 para su análisis.

# UNA CONCLUSIÓN CLAVE DE ESTA LECCIÓN ES QUE AWS OFRECE VARIOS SERVICIOS QUE RESPALDAN LA FASE DE DESCUBRIMIENTO Y RECONOCIMIENTO, INCLUIDOS LOS SIGUIENTES:

**Amazon Inspector es un servicio de administración de vulnerabilidades que escanea continuamente sus cargas de trabajo de AWS en busca de vulnerabilidades.**

**Shield ofrece protección contra ataques DDoS.**

**GuardDuty es un servicio de monitoreo de seguridad continuo que puede ayudar a identificar actividades inesperadas y potencialmente no autorizadas o malintencionadas en su entorno de AWS.**

**Trusted Advisor inspecciona su entorno de AWS y luego hace recomendaciones cuando existen oportunidades para ahorrar dinero, mejorar la disponibilidad y el rendimiento del sistema o ayudar a cerrar las fallas de seguridad.**

**CloudWatch proporciona una solución de supervisión confiable, escalable y flexible.**

**AWS Config es un servicio continuo de supervisión y evaluación que le proporciona un inventario de sus recursos de AWS y registra los cambios en la configuración de dichos recursos.**

•