

Módulo 6: Seguridad

Introducción

1.1 Introducción al módulo (resumen vídeo).

Modelo de Responsabilidad Compartida

AWS protege la infraestructura (centros de datos, hardware, seguridad de servicios).

Los clientes son responsables de la seguridad de sus datos, configuraciones y cargas de trabajo en la nube.

Servicios y mecanismos de seguridad en AWS

AWS ofrece herramientas para mejorar la protección de los datos y recursos en la nube.

Es fundamental configurar correctamente los permisos y controles de acceso.

Modelo de responsabilidad compartida de AWS

1.1 Modelo de responsabilidad compartida (resumen vídeo).

¿Quién es responsable de la seguridad en AWS?

- Tanto AWS como el cliente tienen responsabilidades en la seguridad.
- AWS protege la infraestructura y los servicios.
- El cliente protege sus datos, configuraciones y sistemas operativos.

Ejemplo: Seguridad en EC2

- AWS: Protege el centro de datos, la red y el hipervisor.
- Cliente: Es responsable del sistema operativo, aplicaciones y datos.

Comparación con una casa

- AWS es como la constructora que asegura paredes y puertas.
- El cliente es quien cierra la puerta con llave y protege su interior.

Responsabilidades específicas

- AWS no tiene acceso a los sistemas operativos ni a los datos del cliente.
- El cliente debe gestionar actualizaciones, accesos y cifrado.
- AWS proporciona herramientas para proteger datos y controlar accesos.

Conclusión

- AWS es responsable de la seguridad DE la nube.
- El cliente es responsable de la seguridad EN la nube.

1.2 El modelo de responsabilidad compartida de AWS

La seguridad en AWS es una responsabilidad compartida entre el cliente y AWS. No es un sistema único, sino un conjunto de componentes donde cada parte tiene tareas específicas.

- **Cliente (Seguridad en la nube):** Responsable de la protección de los datos, configuración de sistemas, redes, firewalls y administración de accesos (IAM).
- **AWS (Seguridad de la nube):** Encargado de la infraestructura física y virtual, incluyendo hardware, redes, centros de datos y cumplimiento de normativas de seguridad.

Entidad responsable	Parte del entorno de AWS
Cliente	Datos del cliente
	Plataformas, aplicaciones, Identity and Access Management (IAM)
	Configuración de sistemas operativos, red y firewall
	Cifrado de datos en el lado del cliente, cifrado de datos en el lado del cliente y protección del tráfico de la red
Amazon Web Services (AWS)	Software: computación, almacenamiento, base de datos y redes
	Hardware: regiones, zonas de disponibilidad, ubicaciones periféricas

El modelo de responsabilidad compartida de AWS se compara con la relación entre un constructor y un propietario de vivienda. AWS, como constructor, es responsable de proporcionar una infraestructura segura y bien diseñada, mientras que el cliente, como propietario, debe encargarse de proteger y gestionar lo que almacena y configura en la nube.

Responsabilidades del cliente (Seguridad en la nube)

El cliente es responsable de la seguridad de todo lo que crea y almacena en AWS. Esto incluye:

- Control total sobre los datos almacenados, decidiendo qué contenido subir, qué servicios utilizar y quién tiene acceso.
- Gestión de permisos, asegurando que solo usuarios autorizados puedan acceder a los recursos.
- Configuración de medidas de seguridad, como grupos de seguridad, firewalls y cifrado de datos.
- Aplicación de parches y actualizaciones en los sistemas operativos de sus instancias de Amazon EC2.
- Administración de cuentas de usuario y gestión de accesos mediante IAM.

Responsabilidades de AWS (Seguridad de la nube)

AWS es responsable de la seguridad de la infraestructura subyacente que soporta los servicios en la nube. Esto incluye:

- Protección física de los centros de datos donde se alojan los servidores.
- Administración del hardware, software y redes que permiten el funcionamiento de la nube.
- Seguridad en la infraestructura de virtualización y en la capa de computación.
- Mantenimiento de la disponibilidad y fiabilidad de las regiones de AWS, zonas de disponibilidad y ubicaciones periféricas.
- Cumplimiento de estándares y regulaciones de seguridad, con auditorías realizadas por terceros para garantizar la protección de la infraestructura.

Aunque AWS se encarga de la seguridad global de la nube, los clientes deben implementar sus propias medidas de protección para garantizar la seguridad de sus datos y configuraciones.

Permisos y acceso de usuarios

1.1 Permisos y acceso de usuario (resumen vídeo)

Identidades y permisos en una cafetería

Cada empleado tiene un inicio de sesión único con permisos específicos. Por ejemplo, Vicente puede usar la caja, pero no acceder al inventario. De la misma manera, en AWS, los permisos deben asignarse de forma granular según las responsabilidades de cada usuario.

Usuario raíz en AWS

Cuando creas una cuenta en AWS, te conviertes en el usuario raíz, con acceso total a todos los recursos. Es recomendable activar la autenticación multifactor (MFA) para mayor seguridad y evitar usar este usuario para tareas diarias.

AWS IAM: Control de accesos

AWS Identity and Access Management (IAM) permite gestionar accesos. Se basa en:

- **Usuarios de IAM:** No tienen permisos por defecto; deben recibir autorizaciones explícitas.
- **Principio de mínimo privilegio:** Se otorgan solo los permisos estrictamente necesarios.
- **Políticas de IAM:** Son documentos JSON que describen qué acciones puede realizar un usuario sobre recursos específicos.

Grupos y roles en IAM

- **Grupos de IAM:** Facilitan la gestión de permisos asignando políticas a un grupo en lugar de usuarios individuales.
- **Roles de IAM:** Permiten otorgar permisos temporales según la necesidad del momento, sin requerir credenciales permanentes.

Federación de identidades

IAM permite integrar credenciales corporativas para acceder a AWS sin necesidad de crear usuarios adicionales, facilitando la autenticación y autorización.

1.2 AWS Identity and Access Management (IAM)

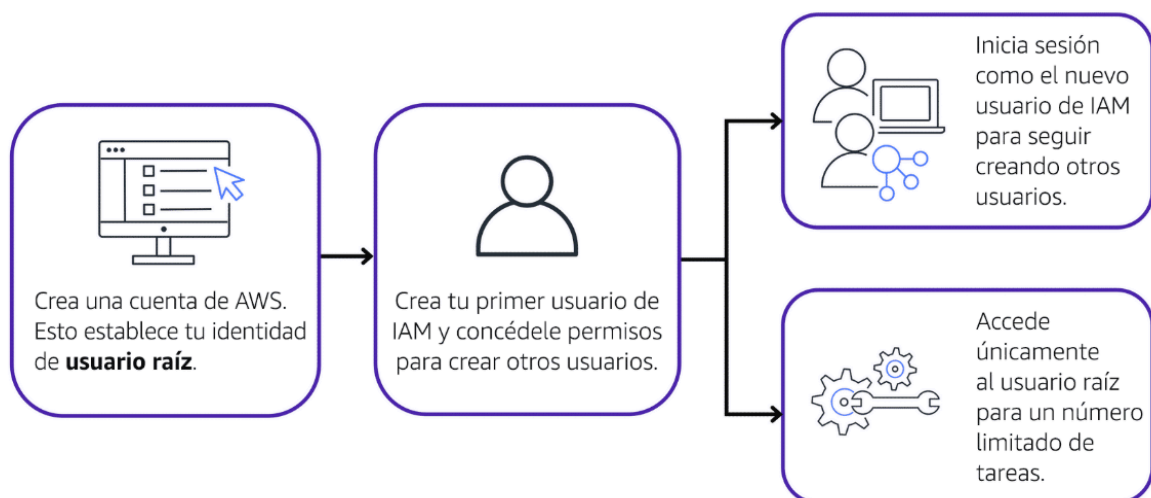
AWS Identity and Access Management (IAM) permite gestionar de forma segura el acceso a los recursos y servicios de AWS. Ofrece flexibilidad para configurar el acceso según las necesidades operativas y de seguridad de la empresa. Las funciones clave de IAM incluyen:

- Usuarios, grupos y roles de IAM
- Políticas de IAM
- Autenticación multifactor (MFA)

1.3 Usuario raíz de la cuenta de AWS

El usuario raíz de AWS es la identidad principal que se crea al iniciar una cuenta. Este usuario tiene acceso completo a todos los servicios y recursos de la cuenta, como el propietario de una cafetería. El usuario raíz debe crear el primer usuario de IAM y otorgarle permisos para crear otros usuarios.

Práctica recomendada: No uses el usuario raíz para tareas cotidianas. Utiliza este usuario solo para tareas específicas que requieren acceso exclusivo, como cambiar la dirección de correo electrónico del usuario raíz. Crea usuarios de IAM para las tareas diarias y accede a esos usuarios para gestionar la cuenta de AWS.



1.4 Usuarios de IAM

Un usuario de IAM en AWS es una identidad que se crea para representar a una persona o aplicación que interactúa con los recursos de AWS. Cada usuario tiene un nombre y credenciales, pero, por defecto, no tiene permisos asignados. Para que pueda realizar acciones específicas, como iniciar una instancia de EC2 o crear un bucket de S3, es necesario otorgarle permisos.

Práctica recomendada: Crea usuarios de IAM individuales para cada persona que necesite acceder a AWS, incluso si varios empleados requieren el mismo nivel de acceso. Esto mejora la seguridad al asignar credenciales únicas a cada usuario.

1.5 Políticas de IAM y ejemplo

Las políticas de IAM son documentos que definen los permisos que los usuarios tienen sobre los servicios y recursos de AWS. Permiten personalizar el acceso, por ejemplo, otorgando permisos para acceder a todos los buckets de Amazon S3 o solo a uno específico.

Práctica recomendada: Aplica el principio de mínimo privilegio, otorgando solo los permisos necesarios para que los usuarios puedan realizar sus tareas. Por ejemplo, si un empleado solo necesita acceder a un bucket específico, asigna permisos solo para ese bucket, no para todos los buckets de la cuenta.

Ejemplo de política de IAM:

El propietario de una cafetería crea un usuario de IAM para un cajero que necesita acceso a los recibos en un bucket de S3 con el ID `AWSDOC-EXAMPLE-BUCKET`. La política de IAM asignada permite al cajero ver los objetos en ese bucket específico (acción `ListObject`).

Si el cajero necesita acceder a otros servicios, se le asignan políticas adicionales. En lugar de asignar permisos a cada cajero individual, el propietario puede crear un grupo de IAM y asignar permisos a todo el grupo.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "s3:ListObject",
    "Resource": "arn:aws:s3:::
AWSDOC-EXAMPLE-BUCKET"
  }
}
```

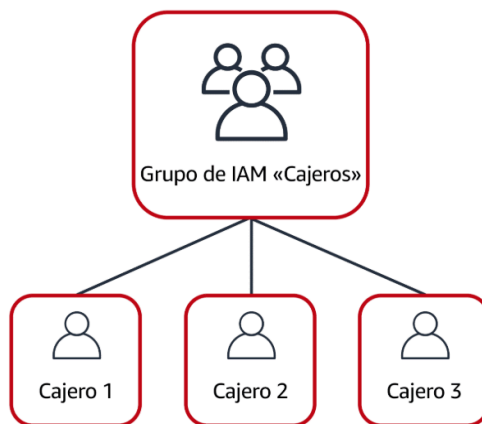
Este ejemplo de política de IAM habilita el permiso para acceder a los objetos del bucket de Amazon S3 con ID: `AWSDOC-EXAMPLE-BUCKET`.

1.6 Grupos de IAM

Un grupo de IAM es un conjunto de usuarios al que se le asigna una política de permisos. En lugar de asignar permisos a cada usuario individualmente, se asignan al grupo, lo que facilita la gestión.

Por ejemplo, en la cafetería, el propietario puede crear un grupo llamado "Cajeros" y asignar permisos a todos los cajeros al mismo tiempo. Si un empleado cambia de puesto, se le puede mover a otro grupo con los permisos adecuados.

Si un empleado necesita permisos temporales para diferentes tareas, se pueden usar roles de IAM.



1.6 Roles de IAM

Un rol de IAM es una identidad que permite obtener acceso temporal a permisos específicos. En situaciones donde un empleado cambia de tarea, como en la cafetería, puede adoptar un rol diferente para acceder a los permisos necesarios para su nueva tarea.

En AWS, un usuario, aplicación o servicio debe tener permisos para asumir un rol. Al adoptar un rol, se reemplazan los permisos anteriores por los del nuevo rol.

Práctica recomendada: Los roles de IAM son útiles para accesos temporales a recursos o servicios, en lugar de permisos permanentes.

Ejemplo de uso de Roles de IAM en la cafetería:

Paso 1:

El propietario de la cafetería concede al empleado permisos para asumir los roles de "**Cajero**" e "**Inventario**". Esto le permite alternar entre estos dos roles a lo largo del día, dependiendo de la tarea que deba realizar.

Paso 2:

El empleado comienza su día asumiendo el rol de "**Cajero**". Esto le otorga acceso al sistema de cajas registradoras, lo que le permite realizar tareas relacionadas con las ventas en la cafetería.

1.7 Autenticación multifactor

La autenticación multifactor (MFA) agrega una capa extra de seguridad a tu cuenta de AWS. Requiere que proporciones dos formas de autenticación para verificar tu identidad, como una contraseña y un código aleatorio enviado a tu teléfono, garantizando que solo tú puedas acceder a tu cuenta.

ID de usuario de IAM:	<input type="text" value="AIDACKCEVSQ6C2EXAMPLE"/>
Contraseña:	<input type="password" value="*****"/>

En primer lugar, un usuario introduce su ID de usuario de IAM y contraseña para iniciar sesión en un sitio web de AWS.



A continuación, se solicita al usuario una respuesta de autenticación desde su dispositivo MFA de AWS. Este dispositivo podría ser una clave de seguridad de hardware, un dispositivo de hardware o una aplicación MFA en un dispositivo como un smartphone.

AWS Organizations

1.1 AWS organizations (resumen vídeo)

AWS Organizations: Gestión de Cuentas y Permisos

Cuando una empresa comienza a usar AWS, puede acabar con una gran cantidad de cuentas, lo que dificulta la gestión de permisos y recursos. AWS Organizations ayuda a organizar y gestionar todas las cuentas de AWS de manera centralizada. Algunas de sus características clave incluyen:

1. **Administración centralizada:** Permite gestionar múltiples cuentas de AWS de forma centralizada, lo que facilita la supervisión.
2. **Facturación unificada:** Permite consolidar el pago de todas las cuentas miembros, aprovechando descuentos por volumen.
3. **Estructura jerárquica:** Agrupa cuentas en unidades organizativas (por ejemplo, por unidad de negocio o requisitos normativos), facilitando la gestión de recursos y seguridad.
4. **Control de permisos:** A través de políticas de control de servicios (SCP), puedes restringir el acceso a servicios y acciones específicas de la API de AWS según las necesidades de cada cuenta.

En resumen, AWS Organizations facilita la gestión de cuentas y la asignación de permisos, mejorando la seguridad, el control y la eficiencia en el uso de AWS.

1.2 AWS organizations

AWS Organizations permite unificar y administrar múltiples cuentas de AWS desde una ubicación central. Al crear una organización, se genera automáticamente una raíz que contiene todas las cuentas. Con AWS Organizations, puedes controlar los permisos de las cuentas mediante políticas de control de servicios (SCP), que imponen restricciones a los servicios, recursos y acciones de API accesibles por los usuarios y roles de cada cuenta. Además, ofrece facturación unificada, facilitando la gestión de los precios de todas las cuentas.

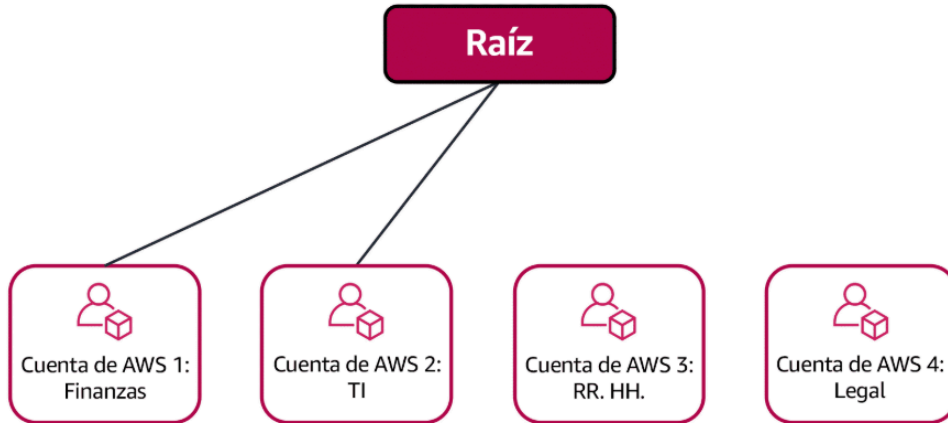
1.3 Unidades organizativas

En AWS Organizations, las cuentas se pueden agrupar en unidades organizativas (UO) para facilitar su administración según requisitos empresariales o de seguridad similares. Al aplicar una política a una UO, todas las cuentas dentro de ella heredan automáticamente los permisos especificados. Esto permite aislar cargas de trabajo o aplicaciones con requisitos específicos, como cumplir con normativas. Por ejemplo, cuentas que solo pueden acceder a servicios normativos se agrupan en una UO, y se les aplica una política que restringe el acceso a otros servicios que no cumplan dichos requisitos.



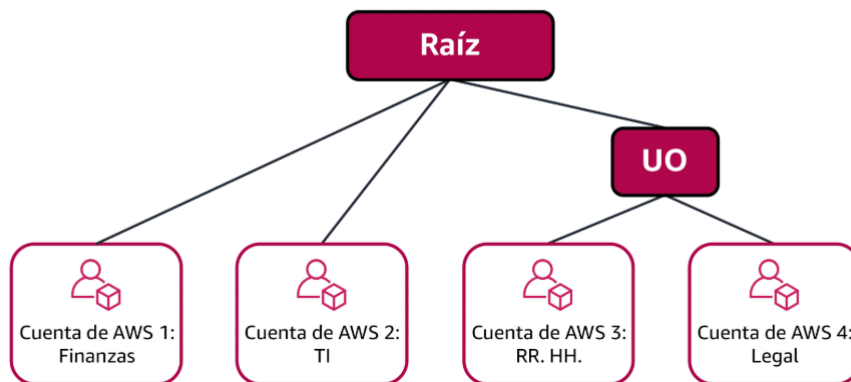
Imagina que tu empresa tiene cuentas de AWS para diferentes departamentos como finanzas, TI, RR.HH. y legal. Decides consolidarlas en una sola organización para gestionarlas desde un único lugar, creando una raíz. Al diseñar la organización, se consideran las necesidades empresariales, de seguridad y reglamentarias de cada departamento para determinar cómo agruparlos en unidades organizativas (UO).

Paso 2



Los departamentos de finanzas y de TI tienen requisitos que no se solapan con los de ningún otro departamento. Incorpora estas cuentas a tu organización para aprovechar beneficios como la facturación unificada, pero no las coloques en ninguna unidad organizativa (UO).

Paso 3



Los departamentos de recursos humanos y legal necesitan acceder a los mismos servicios y recursos de AWS, de modo que debes colocarlos juntos en una unidad organizativa. El hecho de colocarlos en una unidad organizativa te permite adjuntar políticas que se aplican a las cuentas de AWS tanto del departamento de recursos humanos como del legal.

Conclusión

Aunque hayas colocado estas cuentas en las UO, puedes seguir proporcionando acceso a usuarios, grupos y roles a través de IAM.

Al agrupar sus cuentas en UO, puedes darles acceso más fácilmente a los servicios y recursos que necesitan. De esta manera, también impides que accedan a los servicios o recursos que no necesitan.

Conformidad

1.1 Resumen vídeo

Para cumplir con la normativa y pasar auditorías en AWS, debes asegurarte de que las soluciones que alojas en AWS cumplan con los estándares aplicables. AWS ya aplica prácticas recomendadas de seguridad en su infraestructura, pero como cliente, debes asegurarte de cumplir con normativas específicas como el RGPD o HIPAA. AWS ofrece herramientas como AWS Artifact para acceder a documentos y auditorías de conformidad de terceros.

AWS permite elegir regiones que te ayuden a cumplir con requisitos locales de almacenamiento de datos. Además, puedes aplicar mecanismos de cifrado para proteger tus datos, y AWS te proporciona documentación técnica para cumplir con los estándares de conformidad.

Recuerda que, aunque AWS facilita la seguridad, la responsabilidad de la conformidad de las arquitecturas y soluciones creadas en AWS es tuya.

1.2 AWS Artifact

AWS Artifact es un servicio que proporciona acceso a informes de seguridad y conformidad de AWS, así como a acuerdos en línea. Se divide en dos secciones principales:

1. AWS Artifact Agreements: Permite gestionar y firmar acuerdos relacionados con el uso de información en AWS, especialmente para empresas que deben cumplir con regulaciones

específicas, como HIPAA. Puedes revisar, aceptar y administrar estos acuerdos tanto a nivel individual como en AWS Organizations.

Ejemplo: Supongamos que tu empresa necesita firmar un acuerdo con AWS en relación con el uso de determinados tipos de información en los servicios de AWS. Puedes hacerlo a través de **AWS Artifact Agreements**.

2. AWS Artifact Reports: Proporciona informes de conformidad de auditores de terceros, que validan que AWS cumple con estándares y regulaciones de seguridad globales y del sector. Estos informes se actualizan regularmente y pueden ser utilizados como prueba de los controles de seguridad de AWS.

Ejemplo: supongamos que un miembro del equipo de desarrollo de tu empresa está creando una aplicación y necesita más información sobre la responsabilidad de cumplir con ciertos estándares regulatorios. Puedes aconsejarle que acceda a esta información en **AWS Artifact Reports**.



AWS Artifact proporciona acceso a los documentos de seguridad y conformidad de AWS, como las certificaciones ISO de AWS, los informes del sector de pagos con tarjeta (PCI) y los informes de control de organización de servicios (SOC).

1.3 Centro de conformidad para clientes

El Centro de conformidad para clientes de AWS proporciona recursos para entender la conformidad en AWS. Incluye historias de clientes que muestran cómo empresas de sectores regulados han resuelto desafíos de conformidad y auditoría. Además, ofrece documentos técnicos sobre temas como:

- Respuestas de AWS a preguntas clave sobre conformidad.
- Información general sobre riesgo y conformidad de AWS.
- Listas de verificación de seguridad de auditoría.

También incluye una ruta de aprendizaje del auditor dirigida a profesionales de auditoría y conformidad, que desean conocer cómo sus operaciones pueden demostrar conformidad al usar AWS.

Ataques de denegación del servicio

1.1 Resumen vídeo

El ataque DDoS (Denegación de Servicio Distribuida) busca sobrecargar la infraestructura de una aplicación para hacerla inoperativa, utilizando un ejército de bots distribuidos que envían solicitudes masivas. Los ataques pueden ser simples, como la inundación UDP, donde se envía una solicitud con una dirección falsa para inundar el servidor con datos innecesarios, o más sofisticados, como el Slowloris, que simula conexiones lentas para bloquear las solicitudes legítimas.

Para defenderse de estos ataques, AWS ofrece soluciones integradas sin costos adicionales. Los grupos de seguridad bloquean tráfico no deseado, mientras que los ataques masivos son manejados por la infraestructura de AWS, que es capaz de filtrar grandes volúmenes de tráfico. El Elastic Load Balancer (ELB) ayuda a mitigar ataques como Slowloris al gestionar el tráfico de manera eficiente. Para ataques más complejos, AWS ofrece AWS Shield y AWS WAF, que emplean tecnologías de aprendizaje automático para identificar y bloquear amenazas avanzadas.

En resumen, una buena arquitectura en AWS ya proporciona una defensa sólida contra la mayoría de los ataques DDoS, y con herramientas como AWS Shield Advanced, puedes fortalecer aún más la protección.

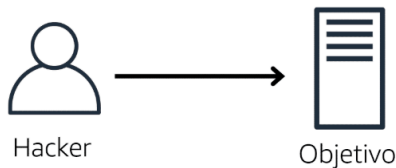
Ejemplo:

Un bromista llama repetidamente a una cafetería para hacer pedidos que nunca recoge, lo que impide que el cajero atienda a otros clientes. La cafetería podría bloquear el número del bromista para detener las solicitudes falsas. Este comportamiento es similar a un **ataque de denegación de servicio (DoS)**, donde un atacante sobrecarga un sistema con solicitudes maliciosas para impedir su funcionamiento normal.

1.2 Ataques de denegación del servicio

Un ataque de denegación de servicio (DoS) es un intento malintencionado de hacer que un sitio web o una aplicación no estén disponibles para los usuarios. Un atacante puede inundar un sitio web o aplicación con tráfico excesivo, sobrecargando el sistema y evitando que responda a las solicitudes legítimas de los usuarios.

Ataque de denegación de servicio

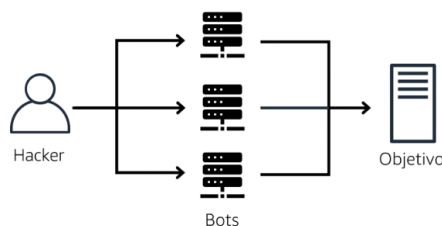


El ataque proviene de una **sola** fuente.

1.3 Ataques de denegación de servicio distribuidos

Un ataque de denegación de servicio distribuido (DDoS) implica a un atacante que utiliza múltiples fuentes, como varios equipos infectados (bots), para inundar un sitio web o una aplicación con tráfico excesivo. Esto hace que sea difícil bloquear todas las solicitudes y provoca que el servicio no esté disponible para los usuarios legítimos. Para mitigar estos ataques, se puede usar AWS Shield.

Ataque de denegación de servicio distribuido



El ataque proviene de **múltiples** fuentes.

1.4 AWS Shield

AWS Shield es un servicio que protege las aplicaciones contra ataques DDoS, ofreciendo dos niveles de protección:

1. **AWS Shield Standard:** Proporciona protección automática y gratuita para todos los clientes de AWS, defendiendo los recursos contra los ataques DDoS más comunes mediante técnicas de análisis en tiempo real.
2. **AWS Shield Advanced:** Es un servicio de pago que ofrece diagnósticos detallados de ataques, detecta y mitiga ataques DDoS sofisticados, y se integra con servicios como Amazon CloudFront, Route 53, y Elastic Load Balancing. Además, permite personalizar reglas con AWS WAF para mitigar ataques más complejos.

Servicios de seguridad adicionales

1.1 Resumen vídeo

En este vídeo se abordan diferentes medidas de seguridad para proteger los datos y la infraestructura en AWS:

1. **Cifrado:** Se compara con cerrar con llave para proteger el café en grano. Hay dos tipos de cifrado:
 - **Cifrado en reposo:** Protege los datos almacenados (por ejemplo, en DynamoDB) para evitar accesos no autorizados.
 - **Cifrado en tránsito:** Protege los datos mientras se transfieren entre servicios o entre un cliente y un servicio, usando conexiones SSL y certificados de servicio.
2. **Amazon Inspector:** Es un servicio que evalúa automáticamente la seguridad de las aplicaciones en AWS, verificando la exposición de instancias EC2 y otras vulnerabilidades.
3. **Amazon GuardDuty:** Detecta amenazas analizando los metadatos de la cuenta y la actividad de red, usando inteligencia de amenazas y machine learning para identificar anomalías y amenazas, sin afectar el rendimiento de los servicios.

1.2 AWS Key Management Service (AWS KMS)

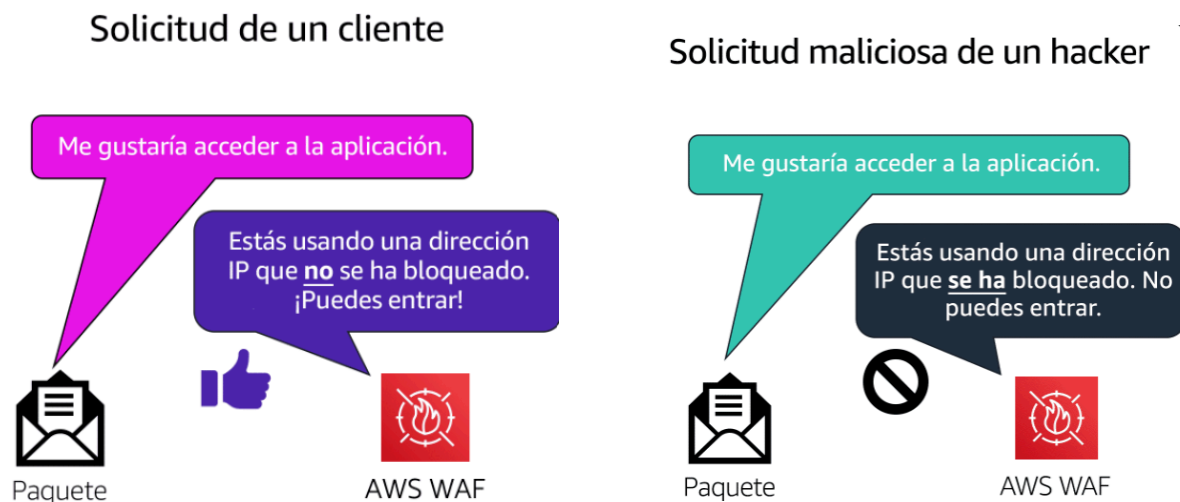
AWS Key Management Service (AWS KMS) es un servicio que permite realizar operaciones de cifrado mediante el uso de claves criptográficas para proteger los datos, tanto en reposo como en tránsito. Similar a cómo una cafetería protegería sus artículos valiosos, AWS KMS asegura los datos de las aplicaciones mediante claves aleatorias que cifran y descifran la información.

Con AWS KMS, los usuarios pueden crear, gestionar y usar claves criptográficas, controlando el acceso a ellas mediante roles de IAM. Además, se pueden desactivar temporalmente las claves para evitar su uso no autorizado, garantizando que las claves nunca salgan de AWS KMS y manteniendo el control total sobre ellas.

1.3 AWS WAF

AWS WAF (Web Application Firewall) es un servicio que protege tus aplicaciones web supervisando las solicitudes de red entrantes. Funciona junto con Amazon CloudFront y un Application Load Balancer, utilizando una lista de control de acceso web (ACL) para bloquear o permitir el tráfico.

Por ejemplo, si una aplicación recibe solicitudes maliciosas de ciertas direcciones IP, puedes configurar AWS WAF para bloquear estas direcciones mientras permites el acceso a usuarios legítimos. Al llegar una solicitud, AWS WAF la compara con las reglas de la ACL, permitiendo o denegando el acceso según corresponda.

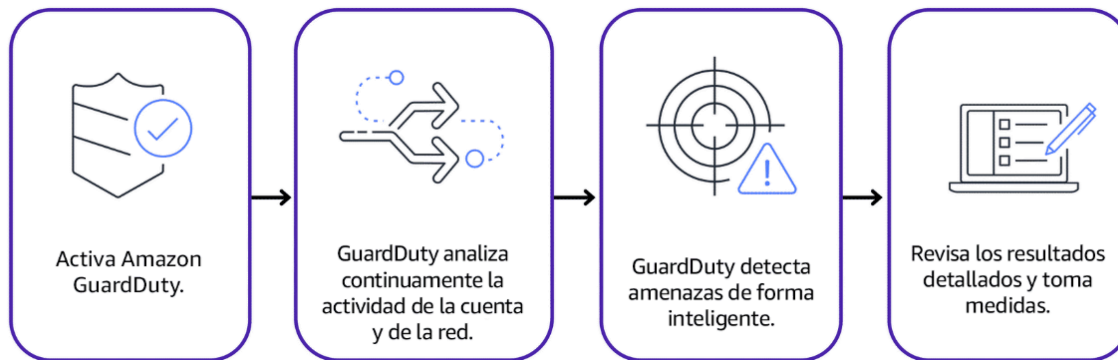


1.4 Amazon Inspector

Amazon Inspector es un servicio que realiza evaluaciones de seguridad automatizadas para mejorar la seguridad y la conformidad de las aplicaciones. Ayuda a identificar vulnerabilidades y desviaciones de las mejores prácticas de seguridad, como el acceso no autorizado a instancias EC2 o el uso de versiones de software vulnerables. Después de una evaluación, proporciona una lista de resultados ordenados por severidad, con detalles de los problemas de seguridad y recomendaciones para solucionarlos. Sin embargo, AWS no garantiza que las recomendaciones solucionen todos los problemas, ya que los clientes son responsables de la seguridad de sus aplicaciones.

1.5 Amazon GuardDuty

Amazon GuardDuty es un servicio de detección inteligente de amenazas para infraestructura y recursos de AWS. Supervisa continuamente la actividad de la red y el comportamiento de la cuenta para identificar amenazas. Los pasos principales son: activar el servicio, analizar la actividad, detectar amenazas de forma inteligente y revisar los hallazgos para tomar medidas. GuardDuty analiza los datos de diversas fuentes de AWS, como los registros de flujo de VPC y DNS, y, si detecta amenazas, proporciona resultados detallados y pasos recomendados para la corrección, permitiendo configurar AWS Lambda para acciones automáticas de corrección.



RESUMEN MÓDULO 6

En AWS, la responsabilidad de seguridad es compartida: AWS es responsable de la seguridad de la nube, mientras que tú eres responsable de la seguridad en la nube. IAM (Identity and Access Management) gestiona usuarios, grupos, roles y políticas, permitiendo controlar accesos. Los usuarios inician sesión con contraseñas y deben tener permisos asignados mediante políticas. IAM también admite identidad federada y autenticación multifactor, especialmente para el usuario raíz.

AWS Organizations ayuda a gestionar múltiples cuentas, organizándolas jerárquicamente. La conformidad es importante, y AWS utiliza auditores externos para asegurar el cumplimiento de normativas, accesibles mediante AWS Artifact.

Para proteger contra ataques DDoS, AWS ofrece herramientas como ELB, grupos de seguridad, AWS Shield y AWS WAF. El cifrado es clave, y eres responsable de cifrar tus datos en tránsito y en reposo.

La seguridad es fundamental en AWS. Se recomienda aplicar el principio de mínimo privilegio al asignar permisos y usar los servicios de AWS para proteger tus recursos, asegurando siempre la protección de los datos.

Módulo 7: Supervisión y análisis

Introducción

1.1 Introducción (resumen vídeo)

Como dueña de la cafetería, quieres poder supervisar cómo van las operaciones sin tener que estar presente todo el día. Deseas conocer métricas como la cantidad de cafés vendidos, el tiempo de espera promedio de los clientes y si te has quedado sin inventario. Además, te gustaría recibir alertas automáticas si el tiempo de espera se alarga demasiado para poder intervenir.

Este tipo de supervisión, que involucra recopilar métricas y utilizarlas para tomar decisiones, se llama **seguimiento**. Es esencial configurar el seguimiento en la nube, ya que los servicios de AWS son elásticos y se escalan dinámicamente. Así, si una instancia de EC2 se sobrecarga, se puede activar un evento de escalado para lanzar otra instancia, o si una aplicación genera demasiados errores, puedes recibir un aviso.

En resumen, el seguimiento en AWS te ayudará a medir el rendimiento, recibir alertas cuando algo salga mal y solucionar problemas rápidamente.

Amazon CloudWatch

1.1 Introducción (resumen vídeo)

En la cafetería, el propietario necesita monitorear el estado de los sistemas, como las cafeteras y otros recursos, para asegurarse de que todo funciona bien. La misma necesidad aplica a los sistemas en AWS, y para esto, existe Amazon CloudWatch, que permite supervisar en tiempo real la infraestructura de AWS y las aplicaciones que usas.

CloudWatch rastrea métricas, como el uso de la CPU de una instancia de EC2 o el número de cafés preparados por una cafetera. Puedes crear métricas personalizadas, como un "Recuento de expresos", para recibir alertas cuando, por ejemplo, se haya alcanzado el límite de 100 cafés y se necesite limpiar la cafetera. Las alertas pueden enviarse a través de SNS, como un SMS al gerente.

Además, puedes crear un panel de CloudWatch para visualizar todas las métricas en un solo lugar y en tiempo real. Esto facilita la supervisión proactiva de los recursos y ayuda a identificar y resolver

problemas rápidamente, reduciendo el tiempo de resolución (MTTR) y mejorando el coste total de propiedad (TCO). Esto permite optimizar recursos, como los desarrolladores, para centrarse en tareas que añadan más valor empresarial.

En resumen, CloudWatch facilita la supervisión y optimización de tus recursos en AWS y puede ser muy útil para mejorar la eficiencia y reducir costos.

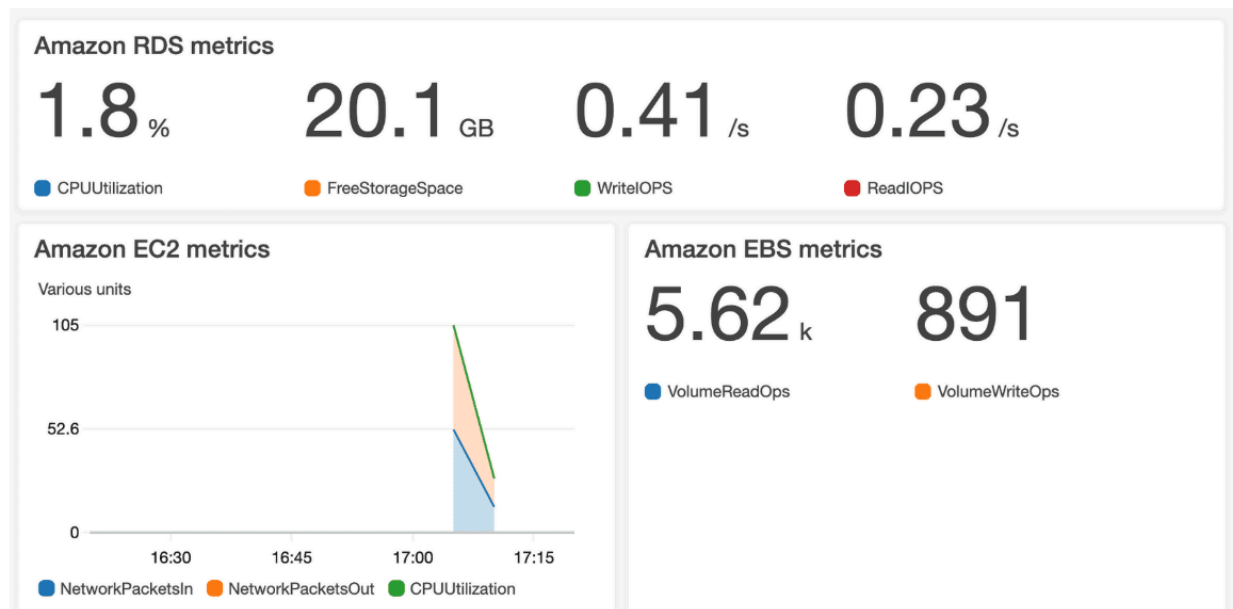
1.2 Amazon CloudWatch

Amazon CloudWatch es un servicio web que permite supervisar y gestionar métricas, así como configurar alarmas basadas en los datos de esas métricas. Los servicios de AWS envían métricas a CloudWatch, que luego crea gráficos automáticamente para mostrar cómo ha cambiado el rendimiento de los recursos a lo largo del tiempo.

1.3 CloudWatch alarms

CloudWatch Alarms permite crear alarmas que ejecuten acciones automáticamente cuando el valor de una métrica supera o queda por debajo de un umbral predefinido. Por ejemplo, si los desarrolladores dejan instancias de Amazon EC2 en ejecución sin usarlas, se puede configurar una alarma para detener automáticamente la instancia cuando su uso de CPU caiga por debajo de un umbral durante un período determinado, y recibir una notificación cuando se active la alarma.

1.4 Panel de CloudWatch



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

AWS Cloud Trail

1.1 Introducción (resumen vídeo)

AWS CloudTrail es una herramienta de auditoría de API que registra todas las solicitudes realizadas a AWS, como lanzar instancias EC2, modificar tablas de DynamoDB o cambiar permisos de usuarios. Registra detalles como quién hizo la solicitud, qué operación se realizó, cuándo, desde qué ubicación, la IP, la respuesta, el cambio realizado y si la solicitud fue denegada. Esto permite auditar y verificar transacciones de manera efectiva, lo que es crucial para la conformidad y la seguridad. CloudTrail guarda estos registros en buckets de S3 seguros, lo que permite demostrar la integridad de la configuración y evitar manipulaciones, facilitando la auditoría, especialmente en procesos de seguridad.





1.2 AWS CloudTrail

AWS CloudTrail registra todas las llamadas a la API de tu cuenta, incluyendo detalles como la identidad del solicitante, la hora, la dirección IP de origen y más. Funciona como un "rastreo" de acciones realizadas, permitiendo consultar un historial completo de actividad. Los eventos se actualizan aproximadamente 15 minutos después de una llamada a la API y puedes filtrarlos por hora, fecha, usuario y tipo de recurso involucrado, entre otros parámetros.

Ejemplo: Evento de AWS CloudTrail

En este ejemplo, el propietario de la cafetería descubre que se ha creado un nuevo usuario de IAM llamado Mary, pero no sabe quién lo hizo, cuándo ni cómo. Para obtener esta información, consulta AWS CloudTrail.

En el Historial de eventos de CloudTrail, el propietario filtra los eventos para ver solo aquellos relacionados con la acción API "CreateUser" en IAM. El registro muestra que el 1 de enero de 2020, a las 9:00, el usuario de IAM llamado John creó el usuario Mary utilizando la consola de administración de AWS. Esto le proporciona todos los detalles necesarios para resolver la duda.

¿Qué ha pasado?	Se ha creado un nuevo usuario de IAM (Mary).	
¿Quién ha presentado la solicitud?	Juan, usuario de IAM	
¿Cuándo ha ocurrido?	1 de enero de 2020 a las 9:00 a.m.	
¿Cómo se ha presentado la solicitud?	Mediante la consola de administración de AWS	

1.3 Información de CloudTrail

CloudTrail Insights es una función opcional dentro de CloudTrail que permite detectar automáticamente actividades inusuales en tu cuenta de AWS. Por ejemplo, podría identificar un aumento inesperado en el número de instancias de Amazon EC2 iniciadas. Una vez detectado el comportamiento inusual, puedes revisar los detalles del evento para tomar las medidas necesarias y abordar la situación.

AWS Trusted Advisor

1.1 Introducción (resumen vídeo)

AWS Trusted Advisor es un servicio automatizado que evalúa los recursos de tu cuenta de AWS según cinco pilares: optimización de costos, rendimiento, seguridad, tolerancia a fallos y límites de servicio. Este servicio verifica en tiempo real diversas prácticas recomendadas de AWS, alertando sobre áreas que necesitan atención. Por ejemplo, puede avisarte si no has activado la autenticación multifactor para el usuario raíz, si hay instancias EC2 subutilizadas que podrían desactivarse para ahorrar, o si hay volúmenes EBS sin copias de seguridad.

En la consola de AWS, puedes ver los resultados agrupados en categorías de "rojo" (problemas críticos), "azul" (recomendaciones) y "verde" (sin problemas). Además, Trusted Advisor permite configurar alertas para que los contactos de facturación, operaciones y seguridad reciban notificaciones sobre las verificaciones. Es una herramienta útil para optimizar recursos, mejorar la seguridad y asegurar la eficiencia en la cuenta de AWS.

1.2 Amazon Trusted Advisor

AWS Trusted Advisor es un servicio web que analiza tu entorno de AWS y ofrece recomendaciones en tiempo real basadas en las prácticas recomendadas de AWS. Examina cinco áreas clave: optimización de costos, rendimiento, seguridad, tolerancia a fallos y límites de servicio. Para cada área, proporciona una lista de acciones recomendadas y recursos adicionales para profundizar en las mejores prácticas.

Este servicio es útil en todas las fases del despliegue de tu infraestructura, desde la creación de nuevos flujos de trabajo y aplicaciones hasta la mejora continua de los recursos y aplicaciones existentes.

1.3 Panel de Amazon Trusted Advisor



El panel de AWS Trusted Advisor muestra un resumen de los problemas, investigaciones y acciones recomendadas en cinco categorías: optimización de precios, rendimiento, seguridad, tolerancia a fallos y límites de servicio.

Para cada categoría:

- La marca de verificación verde indica que no se han detectado problemas.
- El triángulo naranja señala las investigaciones recomendadas.
- El círculo rojo representa las acciones recomendadas para resolver problemas.

RESUMEN MÓDULO 7

Para garantizar que las aplicaciones sean eficientes, seguras y conformes, es crucial saber qué sucede en tu entorno. AWS ofrece varias herramientas para lograrlo:

- **CloudWatch** proporciona información casi en tiempo real sobre el comportamiento del sistema, alertando sobre problemas y mostrando métricas a lo largo del tiempo para optimizar el rendimiento.
- **CloudTrail** te permite saber exactamente quién hizo qué, cuándo y desde dónde, respondiendo a preguntas clave de auditoría.
- **Trusted Advisor** evalúa aspectos relacionados con el precio, el rendimiento, la seguridad y la resiliencia, mostrando recomendaciones a través de un panel práctico.

Aunque AWS tiene muchas otras herramientas de seguimiento y análisis, estas tres te dan una buena idea de las capacidades que ofrece para mejorar la gestión de tu entorno.

Módulo 8: Precios y soporte

Introducción

1.1 Introducción (resumen vídeo)

Mar, ahora propietaria de una cafetería, debe gestionar diversos costes como alquiler, empleados, impuestos y electricidad. Para estimar el gasto del próximo mes, especialmente con la temporada alta acercándose, es necesario analizar cada elemento y hacer una previsión en una tabla. También se plantea la comparación de costes en otra ciudad. En la siguiente sección, se explorará cómo AWS ofrece herramientas gratuitas para planificar y analizar presupuestos en entornos de AWS.

Nivel gratuito de AWS

1.1 Introducción (resumen vídeo)

Si has creado una cuenta de AWS y quieres probar servicios sin preocuparte por los precios, puedes aprovechar el **nivel gratuito**, que ofrece tres opciones:

1. **Siempre gratis:** disponible sin límite de tiempo.
2. **12 meses gratis:** acceso gratuito durante el primer año tras el registro.

3. **Periodos de prueba:** pruebas gratuitas por tiempo limitado.

Ejemplos incluyen **AWS Lambda** (1 millón de invocaciones gratis al mes sin caducidad), **S3** (5 GB gratis por 12 meses) y **Lightsail** (1 mes con hasta 750 horas). Otros servicios gratuitos incluyen **SageMaker**, **DynamoDB**, **Cognito**, entre otros.

1.2 Nivel gratuito de AWS

El nivel gratuito de AWS permite usar ciertos servicios sin costos durante un tiempo determinado. Hay tres tipos de ofertas:

1. **Gratis para siempre:** no caducan, como AWS Lambda (1 millón de solicitudes gratis al mes) y DynamoDB (25 GB de almacenamiento gratuito).
2. **12 meses gratis:** válido durante el primer año tras registrarse, como almacenamiento en S3, tiempo de computación en EC2 y transferencia de datos en CloudFront.
3. **Pruebas gratuitas:** de duración limitada, como Amazon Inspector (90 días) y Lightsail (750 horas en 30 días).

Conceptos relacionados con los precios de AWS

1.1 Cómo funcionan los precios de AWS

Los precios de AWS funcionan con un modelo de pago por uso, sin contratos a largo plazo. Hay tres formas de optimizar costos:

1. **Pago por consumo:** solo pagas por los recursos que utilizas.
2. **Reservas con descuento:** algunos servicios, como EC2 Instance Savings Plans, permiten ahorrar hasta un 72 % al comprometerse a un uso prolongado.
3. **Descuentos por volumen:** cuanto más usas ciertos servicios, como S3, menor es el costo por unidad.

Este modelo ofrece **flexibilidad** y **ahorro** según las necesidades del usuario.

1.2 Calculadora de precios de AWS

La calculadora de precios de AWS permite estimar los costos de los servicios en función de tus necesidades. Puedes organizar estimaciones por grupos, reflejando la estructura de tu empresa, y compartirlas mediante un enlace.

Por ejemplo, si evalúas Amazon EC2, la calculadora te ayuda a comparar regiones, tipos de instancias, sistema operativo y requisitos de memoria o E/S para encontrar la opción más rentable.

1.3 Ejemplos de precios de AWS

AWS Lambda

Los precios de **AWS Lambda** dependen del número de solicitudes y del tiempo de ejecución de las funciones.

- **Nivel gratuito:** 1 millón de solicitudes y hasta 3,2 millones de segundos de computación gratis al mes.
- **Ahorro:** Se pueden reducir costos con un **Compute Savings Plan**, comprometiéndose a un uso constante por 1 o 3 años.
- **Ejemplo:** Una factura en **Virginia del Norte** con 680 solicitudes y 255 segundos de ejecución no genera costo, ya que está dentro del nivel gratuito.

Amazon EC2

Los precios de **Amazon EC2** se basan en el tiempo de ejecución de las instancias.

- **Instancias de spot:** permiten ahorrar hasta un **90 %** en cargas de trabajo flexibles.
- **Ahorro adicional:** se pueden reducir costos con **Savings Plans** e **instancias reservadas**.
- **Ejemplo:** Una instancia en **Virginia del Norte** con **107 horas de uso, 11 GB de EBS y 268 horas de Load Balancer** estaría dentro del nivel gratuito, sin generar costos.

Amazon S3

Los precios de **Amazon S3** se determinan según varios factores:

- **Almacenamiento:** Solo se paga por el espacio utilizado, considerando el tamaño de los objetos, la clase de almacenamiento y el tiempo de almacenamiento en el mes.
- **Solicitudes y recuperación de datos:** Se cobra por cada solicitud para acceder a los objetos o para agregarlos a los buckets de S3. Por ejemplo, si almacenas imágenes en S3 y las sirves en un sitio web, cada acceso cuenta como una solicitud facturable.
- **Transferencia de datos:** La transferencia de datos dentro de la misma región o desde Internet a S3 es gratuita. Sin embargo, mover datos entre regiones o fuera de AWS tiene un costo.
- **Administración y replicación:** Si activas funciones como inventario, análisis o replicación de objetos, también generan costos adicionales.

Ejemplo de precios

Un usuario ha utilizado **Amazon S3** en las regiones de **Virginia del Norte y Ohio**.

- En **Virginia del Norte**, hubo 185 solicitudes de almacenamiento y 923 de recuperación, usando 0,159 GB.
- En **Ohio**, hubo 4 solicitudes de recuperación y 0,000001 GB de almacenamiento.

Todo este uso está por debajo del límite del **nivel gratuito de AWS**, por lo que no generó costos adicionales.

Panel de facturación

1.1 Introducción vídeo

El video explica cómo revisar la facturación de AWS. Al ingresar, puedes ver el gasto mensual, los servicios más usados, y detalles del gasto actual y el mes pasado. También puedes acceder a herramientas como Cost Explorer y Budgets, y ver las facturas desglosadas por servicio y región. En resumen, muestra cómo monitorear el uso y controlar los costes en tu cuenta de AWS.

Facturación unificada

1.1 Introducción (resumen vídeo)

El video explica la facturación unificada en AWS Organizations, que permite gestionar varias cuentas de AWS bajo una sola factura, facilitando el seguimiento y control de los gastos. Al igual que una empresa con varias cafeterías que recibe una sola factura por los servicios comunes, AWS permite agrupar el uso de recursos de todas las cuentas y aplicar descuentos por volumen. Además, los planes de ahorro y las instancias reservadas de EC2 pueden compartirse entre cuentas. Esta característica es gratuita y simplifica la gestión de la facturación.

1.2 Facturación unificada

La facturación unificada en AWS Organizations permite recibir una única factura mensual para todas las cuentas de la organización, facilitando el seguimiento de los costes combinados. Puedes revisar los cargos detallados de cada cuenta y mantener la transparencia en la facturación. Además, permite compartir descuentos por volumen, planes de ahorro e instancias reservadas entre las cuentas, lo que beneficia a las cuentas con menor uso. El número predeterminado de cuentas en una organización es 4, pero se puede aumentar contactando con AWS Support.

Paso 1

En el Paso 1, se añaden tres cuentas de AWS a una cuenta principal para facilitar la gestión de la facturación. Supongamos que la empresa usa tres cuentas para diferentes departamentos: la cuenta 1 debe 19,64 USD, la cuenta 2 debe 19,96 USD y la cuenta 3 debe 20,06 USD. En lugar de pagar tres facturas separadas, se crea una organización en AWS y se gestionan todas las cuentas desde la cuenta principal.

Paso 2

En el Paso 2, AWS cobra a la cuenta principal por todas las cuentas vinculadas en una factura unificada cada mes. La cuenta principal también recibe un informe detallado de los costes de cada cuenta vinculada. Además, la factura incluye los costes de uso de la propia cuenta principal, que en este caso son 14,14 USD. El total de la factura, que abarca las tres cuentas vinculadas y la cuenta principal, es de 73,80 USD.

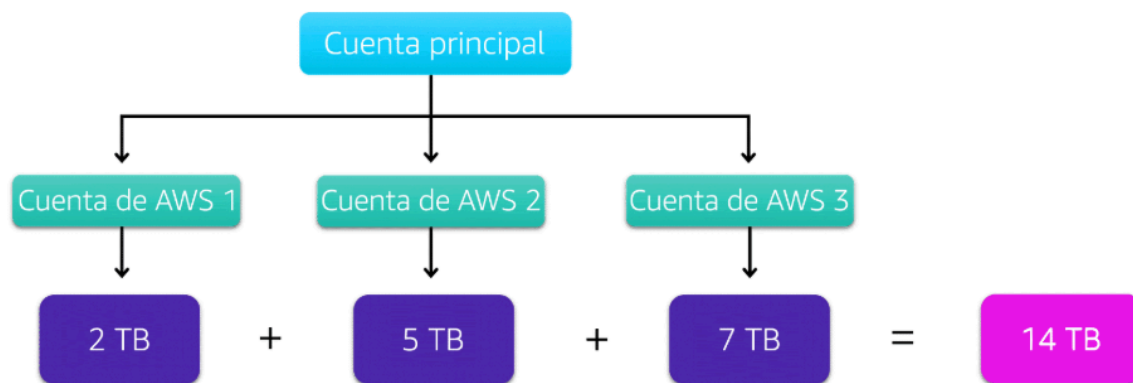
Paso 3

En el Paso 3, la facturación unificada permite compartir descuentos por volumen entre las cuentas. Algunos servicios de AWS, como Amazon S3, ofrecen precios más bajos cuanto más se usa el servicio. En este ejemplo, tres cuentas han transferido diferentes cantidades de datos en Amazon S3 durante el mes: la cuenta 1 ha transferido 2 TB, la cuenta 2 ha transferido 5 TB y la cuenta 3 ha

transferido 7 TB. Ninguna cuenta ha superado el umbral de 10 TB, por lo que ninguna puede acceder al descuento en el precio de transferencia por GB para los próximos 40 TB.

Conclusión

En la conclusión, tres cuentas de AWS se vinculan bajo una organización y usan la facturación unificada, con un uso total de 14 TB en Amazon S3. Al combinar el uso de todas las cuentas, se supera el umbral de 10 TB, lo que permite aplicar un descuento por volumen. AWS distribuye el descuento según el uso de cada cuenta. En este caso, la cuenta 3, que transfirió 7 TB, recibiría una mayor parte del descuento, ya que usó más datos que la cuenta 1 (2 TB) y la cuenta 2 (5 TB).



AWS Budgets

1.1 Introducción (resumen vídeo)

AWS Budgets permite crear presupuestos personalizados para supervisar los gastos y el uso en AWS. Al igual que un presupuesto personal, puedes establecer límites y recibir alertas cuando los costes o el uso superen el presupuesto establecido. Por ejemplo, si tu presupuesto es de 1000 dólares, puedes configurar una alerta para que te notifiquen al llegar al 80% de ese monto. En la demostración, se muestra cómo crear un presupuesto, establecer un umbral de alerta y recibir notificaciones por correo cuando el gasto se acerque al límite.

1.2 AWS Budgets

AWS Budgets te permite crear presupuestos personalizados para planificar el uso de servicios, costes y reservas de instancias en AWS. La información se actualiza tres veces al día, lo que permite monitorear si el uso está dentro del presupuesto o el nivel gratuito de AWS. También puedes configurar alertas personalizadas para recibir notificaciones cuando el uso o el coste se acerque o supere el límite establecido. Por ejemplo, si estableces un presupuesto de 200 USD para Amazon EC2, puedes recibir una alerta cuando el uso alcance los 100 USD, dándote tiempo para ajustar el uso.

AWS Cost Explorer

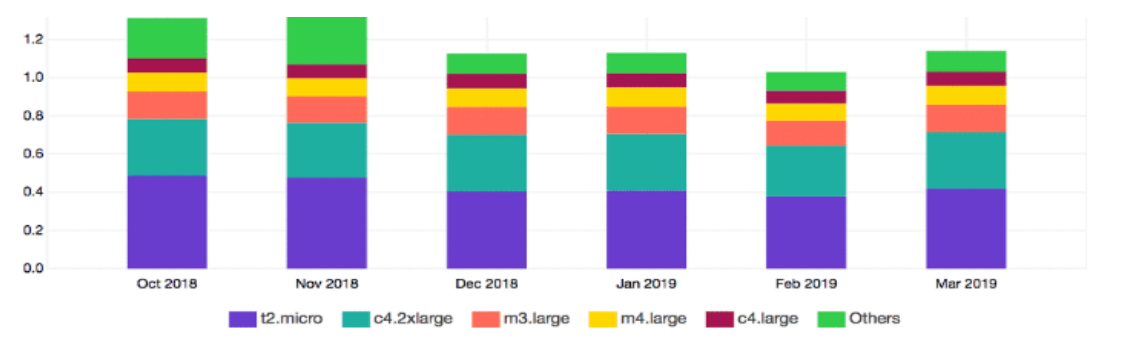
1.1 Introducción (resumen vídeo)

AWS Cost Explorer es una herramienta que permite analizar visualmente los costes de los servicios en AWS, permitiendo identificar en qué se está invirtiendo más. Puedes ver un historial de 12 meses y desglosar los gastos por servicio, región o etiquetas. Las etiquetas son pares clave-valor que se asignan a recursos como instancias EC2, lo que facilita el seguimiento de costes por proyectos específicos. Además, puedes crear informes personalizados para revisar detalles específicos, como los gastos diarios. Cost Explorer ayuda a identificar aumentos de gasto y optimizar el uso de los recursos en AWS.

1.2 AWS Cost Explorer

AWS Cost Explorer es una herramienta que permite visualizar, comprender y gestionar los costes y el uso de AWS a lo largo del tiempo. Incluye un informe predeterminado con los costes acumulados de los cinco servicios principales de AWS, y permite aplicar filtros y personalizar agrupaciones para un análisis detallado, incluso a nivel por hora.

Por ejemplo, puedes analizar los costes mensuales de instancias de Amazon EC2, desglosados por tipo de instancia, para tomar decisiones informadas sobre presupuestos y planificación futura de costes.



[Download CSV](#)

Instance Type	Oct 1, 2018	Nov 1, 2018	Dec 1, 2018	Jan 1, 2019
Total cost (\$)	1,312.71	1,328.54	1,125.99	1,129.65
t2.micro (\$)	486.75	475.89	405.63	409.27
c4.2xlarge (\$)	296.11	286.56	296.11	296.11

Planes de AWS Suport

1.1 Introducción (resumen vídeo)

AWS ofrece varios niveles de soporte técnico:

1. **Basic Support:** Acceso gratuito a atención al cliente, documentación y herramientas como AWS Trusted Advisor.
2. **Developer Support:** Soporte por correo electrónico con respuestas en 24 horas, ideal para pruebas y desarrollo.
3. **Business Support:** Soporte telefónico, tiempos de respuesta rápidos (1-4 horas) y gestión de eventos.
4. **Enterprise On-Ramp:** Respuesta en 30 minutos para cargas críticas y acceso a un Technical Account Manager (TAM).
5. **Enterprise Support:** Respuesta en 15 minutos, TAM dedicado y revisiones proactivas de la infraestructura.

Los TAM ayudan a optimizar la infraestructura usando el Well-Architected Framework.

1.2 Basic Support

Basic Support es gratuito para todos los clientes de AWS y ofrece:

- Acceso a documentación técnica y comunidades de soporte.
- Asistencia para preguntas sobre facturación y límites de servicio.
- Acceso limitado a comprobaciones de AWS Trusted Advisor.
- Uso de AWS Personal Health Dashboard para alertas sobre problemas que puedan afectarte.

Si se necesita soporte adicional, se pueden considerar planes como Developer Support, Business Support, Enterprise On-Ramp o Enterprise Support.

1.3 Developer Support, Business Support, Enterprise On-Ramp y Enterprise Support

AWS ofrece los siguientes planes de soporte adicionales al Basic Support:

1. **Developer Support:**
 - Guía de prácticas recomendadas y herramientas de diagnóstico.
 - Soporte para la arquitectura de creación de bloques, ayudando a combinar servicios de AWS para crear aplicaciones.
2. **Business Support:**

- Guía de casos de uso y acceso completo a todas las comprobaciones de AWS Trusted Advisor.
- Soporte limitado para software de terceros, como sistemas operativos en Amazon EC2.

3. Enterprise On-Ramp Support:

- Incluye todo lo del plan Business Support, más acceso a un grupo de administradores técnicos de cuentas (TAM).
- Talleres anuales de optimización de costes y soporte proactivo.
- Tiempo de respuesta de 30 minutos para problemas críticos.

4. Enterprise Support:

- Incluye todo lo de Enterprise On-Ramp, más un administrador técnico de cuentas dedicado y herramientas avanzadas de supervisión.
- Soporte para eventos de infraestructura y formación para impulsar la innovación.
- Tiempo de respuesta de 15 minutos para problemas críticos.

Cada plan tiene un costo mensual, con Developer Support siendo el más económico, los planes Business Support y Enterprise On-Ramp tienen un precio intermedio y Enterprise Support el más costoso.

1.4 Administrador técnico de cuenta (TAM)

El Administrador Técnico de Cuenta (TAM) es un recurso clave en los planes Enterprise On-Ramp y Enterprise Support. El TAM actúa como el principal punto de contacto en AWS, proporcionando:

- Guía experta en ingeniería para diseñar soluciones eficientes y rentables.
- Asistencia en la integración de servicios de AWS y en la creación de arquitecturas resilientes.
- Acceso directo a programas de AWS y a una comunidad de expertos.

El TAM ayuda a las empresas a optimizar su transición a la nube, como por ejemplo, ofreciendo recomendaciones sobre cómo integrar diversos servicios de AWS para desarrollar aplicaciones que satisfagan necesidades específicas.

AWS Marketplace

1.1 Introducción (resumen vídeo)

AWS Marketplace es un catálogo digital que facilita la búsqueda, despliegue y gestión de software de terceros en AWS. Ayuda a las empresas a implementar soluciones rápidamente, reduciendo los costos y mejorando la innovación.

Los beneficios clave de AWS Marketplace incluyen:

- **Despliegue rápido:** Ofrece opciones como "desplegar con un clic", permitiendo adquirir y usar productos de software de diversos proveedores sin necesidad de crear y mantener infraestructura adicional.
- **Flexibilidad en los pagos:** Muchos proveedores ofrecen opciones de pago por uso, evitando costes innecesarios por licencias no utilizadas. También permite usar licencias anuales en AWS.
- **Pruebas gratuitas:** Algunos proveedores ofrecen planes de prueba o inicio rápido para evaluar sus productos.
- **Funcionalidades empresariales:** Marketplace proporciona opciones como acuerdos personalizados de licencia, catálogos privados de software preaprobado y herramientas de gestión de costos.

En resumen, AWS Marketplace facilita la adopción de software de terceros, ahorra tiempo y dinero, y mejora la agilidad y flexibilidad en la nube.

1.2 AWS Marketplace

AWS Marketplace es un catálogo digital que ofrece miles de productos de software de proveedores independientes para ejecutar en AWS. Permite buscar, probar y comprar software, y proporciona información detallada sobre precios, soporte y opiniones de otros usuarios.

Las soluciones se pueden explorar por sector y caso práctico. Por ejemplo, en el sector sanitario, se pueden encontrar soluciones para proteger registros de pacientes o usar machine learning para predecir riesgos de salud.

Categorías principales incluyen infraestructura, DevOps, datos, aplicaciones empresariales, machine learning, IoT, entre otras, con subcategorías para facilitar las búsquedas, como desarrollo de aplicaciones, supervisión y pruebas en DevOps.



RESUMEN MÓDULO 8

En el **módulo 8** se trataron los siguientes conceptos clave:

1. **Tipos de ofertas en el nivel gratuito de AWS:** 12 meses gratis, Gratis para siempre y Pruebas.
2. **Beneficios de la facturación unificada** en AWS Organizations.
3. **Herramientas para planificar y revisar los costes de AWS.**
4. **Diferencias entre los planes de AWS Support:** Basic, Developer, Business, Enterprise On-Ramp y Enterprise.
5. **Descubrimiento de software en AWS Marketplace.**

El módulo cubrió la facturación unificada a través de AWS Organizations, el uso de herramientas como AWS Budgets y Cost Explorer, y los diferentes planes de soporte para el traspaso a la nube. Además, se abordó el ecosistema de socios de AWS y cómo encontrar soluciones listas en AWS Marketplace.

Módulo 9: Migración e innovación

Introducción

1.1 Introducción (resumen vídeo)

En este módulo, los objetivos de aprendizaje son:

1. Comprender la migración y la innovación en la nube de AWS.
2. Resumir el AWS Cloud Adoption Framework (AWS CAF).
3. Explicar los seis factores clave de una estrategia de migración a la nube.
4. Describir los beneficios de las soluciones de migración de datos de AWS, como AWS Snowcone y AWS Snowball.
5. Resumir las soluciones innovadoras que ofrece AWS.

El módulo se enfoca en herramientas y estrategias para la migración de datos a AWS, incluyendo el uso de dispositivos físicos (como los de la Snow Family) y el marco de adopción de la nube de AWS.

AWS Cloud Adoption Framework (AWS CAF)

1.1 Introducción (resumen vídeo)

La migración a la nube de AWS es un proceso complejo que requiere esfuerzo y experiencia, no es algo que suceda de forma mágica. Aunque muchas empresas ya lo han logrado, es importante comprender que diferentes roles dentro de una organización tienen perspectivas distintas sobre la migración. Los desarrolladores, arquitectos en la nube, y analistas empresariales o financieros aportan enfoques distintos, por lo que es fundamental trabajar en equipo y aprovechar todos los conocimientos disponibles.

Además, es esencial contar con el talento adecuado para facilitar la migración, lo que puede implicar contratar nuevos perfiles para cubrir todas las necesidades del proceso.

El AWS Cloud Adoption Framework está diseñado para guiar a las empresas en esta migración, organizándose en seis áreas clave: negocios, personal, gobernanza, plataforma, seguridad y operaciones. Cada área se enfoca en aspectos específicos de la migración, tanto desde una perspectiva empresarial como técnica. El marco ayuda a identificar carencias en capacidades y procesos, y a crear un plan de acción para gestionar la transición a la nube.

En resumen, aunque la migración es desafiante, el AWS Cloud Adoption Framework ofrece recursos valiosos para facilitar el proceso y garantizar una transición fluida.

1.2 Seis perspectivas principales de Cloud Adoption Framework

El AWS Cloud Adoption Framework (AWS CAF) ofrece directrices en seis áreas clave llamadas perspectivas, que abordan diferentes responsabilidades en el proceso de migración a la nube. Estas perspectivas se dividen en dos grupos: capacidades empresariales (negocio, personal y gobernanza) y capacidades técnicas (plataforma, seguridad y operaciones).

1. **Perspectiva de negocio:** Alinea las TI con las necesidades empresariales y vincula las inversiones tecnológicas a los resultados clave. Ayuda a crear un caso de negocio sólido para la adopción de la nube. Roles comunes: administradores de negocio, responsables de finanzas, y responsables de presupuestos.
2. **Perspectiva de personal:** Desarrolla una estrategia de gestión del cambio para adoptar la nube con éxito. Evalúa estructuras organizativas, requisitos de habilidades y procesos. Roles comunes: recursos humanos y administradores de personal.
3. **Perspectiva de gobernanza:** Asegura la alineación de las TI con la estrategia empresarial y maximiza el valor mientras minimiza los riesgos. Se enfoca en actualizar habilidades y procesos para gestionar las inversiones en la nube. Roles comunes: CIO, administradores de programas, arquitectos de empresas.

4. **Perspectiva de plataforma:** Define principios y patrones para implementar soluciones en la nube y migrar cargas de trabajo. Establece modelos arquitectónicos para describir la estructura de los sistemas de TI. Roles comunes: CTO, administradores de TI, arquitectos de soluciones.
5. **Perspectiva de seguridad:** Garantiza que la organización cumpla con los objetivos de seguridad. Ayuda a seleccionar e implementar controles de seguridad adecuados. Roles comunes: CISO, administradores de seguridad de TI, analistas de seguridad.
6. **Perspectiva de operaciones:** Ayuda a gestionar las operaciones diarias, trimestrales y anuales. Define los procedimientos operativos y la formación necesarios para una adopción exitosa de la nube. Roles comunes: administradores de operaciones de TI y soporte de TI.

Estas perspectivas guían a las organizaciones en la planificación y ejecución de la migración a la nube.

Estrategias de migración

1.1 Introducción (resumen vídeo)

El proceso de migrar aplicaciones a AWS no es automático ni fácil, pero existen seis tipos de migración que puedes considerar según tus necesidades de tiempo, costo, prioridad e importancia:

1. **Realojar (Lift and Shift):** Consiste en mover las aplicaciones tal cual están a AWS sin cambios significativos. Es una opción fácil y rápida que puede ahorrar hasta un 30% de los costos, aunque sin aprovechar completamente los beneficios de la nube.
2. **Redefinir la plataforma (Lift, Tinker and Shift):** Similar al "lift and shift", pero se realizan algunas optimizaciones en la nube sin cambiar el código de la aplicación, como adaptar bases de datos a servicios como Amazon RDS.
3. **Retirar:** Elimina aplicaciones obsoletas que ya no se usan o que tienen alternativas funcionales, ahorrando costos y esfuerzos. Se estima que entre el 10 y el 20% de las aplicaciones de una empresa pueden retirarse.
4. **Retener:** Algunas aplicaciones aún no están obsoletas, pero podrían ser migradas más tarde, lo que permite posponer su migración a AWS.
5. **Volver a comprar:** Implica cambiar a nuevos proveedores de software, como migrar de un CRM antiguo a uno basado en la nube. Aunque puede aumentar los costos iniciales, los beneficios a largo plazo pueden ser significativos.
6. **Refactorizar:** Reescribir el código de las aplicaciones para mejorar su rendimiento o agregar nuevas características que no eran viables en las instalaciones. Es una opción costosa y que requiere más tiempo, pero puede ser muy beneficiosa a largo plazo.

Elegir la opción adecuada para cada aplicación es crucial para una migración exitosa a AWS.

1.2 Seis estrategias de migración

Las seis estrategias de migración más comunes son:

1. **Volver a alojar (Lift-and-Shift):** Implica mover aplicaciones tal como están a la nube sin hacer cambios. Es una opción rápida para escalar aplicaciones sin modificaciones.
2. **Redefinir la plataforma (Lift, Tinker and Shift):** Consiste en realizar algunas optimizaciones en la nube sin cambiar la arquitectura principal de la aplicación, para obtener beneficios tangibles.
3. **Refactorizar/Rearquitectura:** Implica rediseñar una aplicación utilizando funciones nativas en la nube para mejorar características, escalabilidad o rendimiento, especialmente cuando las necesidades empresariales son mayores.
4. **Volver a comprar:** Consiste en cambiar de un modelo tradicional a uno basado en software como servicio (SaaS), como migrar de un CRM tradicional a Salesforce.com.
5. **Retener:** Mantiene aplicaciones esenciales en el entorno actual, que pueden necesitar refactorización o que pueden migrarse en el futuro.
6. **Retirar:** Elimina aplicaciones que ya no son necesarias.

Familia de productos AWS Snow

1.1 Introducción (resumen vídeo)

En este video, se presenta la **AWS Snow Family**, una solución para transferir grandes cantidades de datos a la nube de manera eficiente. Debido a las limitaciones de ancho de banda, transferir grandes volúmenes de datos por internet puede llevar días o incluso meses. Para solucionar esto, AWS ofrece dispositivos como **AWS Snowcone** y **AWS Snowball Edge**.

- **AWS Snowcone** admite hasta 8 terabytes de datos y permite copiar estos datos a AWS a través de un dispositivo que se envía al cliente, quien luego lo devuelve para que AWS cargue los datos en su cuenta, generalmente en S3.
- **AWS Snowball Edge** tiene versiones **Compute Optimized** y **Storage Optimized**. Estos dispositivos, que se pueden agrupar en clústeres, permiten procesar y almacenar más datos. Son útiles en ubicaciones remotas y para tareas como captura de datos IoT, compresión de imágenes, o transcodificación de vídeo.

Los dispositivos Snow son seguros: incluyen cifrado automático de datos y firmas criptográficas, con claves gestionadas por el cliente mediante **AWS Key Management Service**.

1.2 Miembros de la familia de productos AWS Snow



La **AWS Snow Family** es un conjunto de dispositivos físicos diseñados para transferir grandes volúmenes de datos dentro y fuera de AWS, hasta alcanzar escalas de exabytes. Los dispositivos de esta familia incluyen AWS Snowcone, AWS Snowball y AWS Snowmobile. Todos estos dispositivos están gestionados y son propiedad de AWS, integrándose con sus servicios de seguridad, almacenamiento, computación y supervisión.

1. AWS Snowcone

- Características: Dispositivo pequeño, robusto y seguro para transferencia de datos y computación periférica.
- Especificaciones:
 - 2 CPU
 - 4 GB de memoria
 - 14 TB de almacenamiento utilizable

2. AWS Snowball

- Tipos:
 - **Snowball Edge Storage Optimized:** Ideal para migraciones de datos a gran escala y transferencias recurrentes, con capacidad para computación local.
 - Almacenamiento: 80 TB HDD, 1 TB SSD
 - Computación: 40 vCPU, 80 GiB de memoria
 - **Snowball Edge Compute Optimized:** Proporciona poderosos recursos de computación para tareas como *machine learning* y análisis de vídeo.
 - Almacenamiento: 80 TB HDD, 28 TB SSD NVMe
 - Computación: 104 vCPU, 416 GiB de memoria, y opción de GPU NVIDIA Tesla V100

3. AWS Snowmobile

- Características: Servicio para la transferencia masiva de datos a escala de exabytes, permitiendo mover hasta 100 petabytes de datos a AWS.

Cada dispositivo está diseñado para ser seguro, con capacidades integradas de cifrado, y se utiliza para diferentes niveles de capacidad, desde pequeños hasta grandes volúmenes de datos.

Innovación con AWS

1.1 Introducción (resumen vídeo)

AWS ofrece una amplia gama de servicios para diversas necesidades tecnológicas. Algunos de los aspectos destacados incluyen:

1. **VMware en AWS:** La infraestructura VMware local puede trasladarse a AWS mediante VMware Cloud en AWS, facilitando la migración a la nube.
2. **Machine Learning e Inteligencia Artificial:** AWS ofrece un conjunto robusto de servicios de IA, incluyendo herramientas preentrenadas para visión artificial, recomendaciones lingüísticas y predicciones empresariales. Con Amazon SageMaker, las empresas pueden crear, entrenar y desplegar modelos de machine learning. También están disponibles servicios como Amazon Lex (para crear bots de chat) y Amazon Textract (para extraer datos de documentos).
3. **Plataforma optimizada para Machine Learning:** AWS proporciona una infraestructura de computación de alto rendimiento y seguridad, utilizando herramientas como Amazon SageMaker y Amazon Augmented AI (A2I) para facilitar el uso de machine learning incluso sin expertos en la empresa.
4. **AWS DeepRacer:** Permite a los desarrolladores experimentar con el aprendizaje por refuerzo en un entorno de carreras.
5. **Internet de las Cosas (IoT):** AWS soporta dispositivos conectados globalmente.
6. **AWS Ground Station:** Permite a las empresas usar satélites, pagando solo por el tiempo de uso, eliminando la necesidad de tener un satélite propio.

AWS ofrece tecnologías innovadoras y actualiza constantemente sus servicios, además de ofrecer formación a través de AWS Training and Certification.

1.2 Innovar con los servicios de AWS

Para innovar con los servicios de AWS, es esencial enfocarse en los resultados deseados, considerando el estado actual, el estado deseado y los problemas a resolver. Al trasladarse a la nube, se deben explorar varios caminos posibles:

1. **Aplicaciones sin servidor:** AWS permite crear aplicaciones sin necesidad de administrar servidores, ya que se encarga de la disponibilidad y la tolerancia a fallos. AWS Lambda es un

ejemplo que ejecuta código sin la necesidad de gestionar servidores, permitiendo a los desarrolladores centrarse en su producto.

2. **Machine Learning:** AWS facilita el desarrollo de modelos de machine learning mediante Amazon SageMaker, que simplifica la creación, entrenamiento e implementación de modelos rápidamente. El machine learning puede usarse para analizar datos, resolver problemas complejos y hacer predicciones.
3. **Inteligencia Artificial:** AWS ofrece varios servicios de IA, como Amazon CodeWhisperer (sugerencias de código y detección de errores de seguridad), Amazon Transcribe (convertir voz a texto), Amazon Comprehend (análisis de texto), Amazon Fraud Detector (detección de fraudes) y Amazon Lex (creación de chatbots de voz y texto).

1.3 Amazon CodeWhisperer

Amazon **CodeWhisperer** es un complemento de programación basado en inteligencia artificial que ayuda a los desarrolladores a analizar el código y los comentarios mientras programan. Utiliza el procesamiento de lenguaje natural para generar automáticamente funciones y bloques de código, adaptándose a las descripciones y estilo del desarrollador. Además, asegura la calidad del código al verificar que cumpla con estándares de seguridad como OWASP y las prácticas recomendadas de AWS.

Este servicio simplifica el desarrollo al automatizar tareas repetitivas, ahorrando tiempo y permitiendo a los desarrolladores centrarse en aspectos más críticos del proyecto. También mejora la calidad del código, acelera el desarrollo de aplicaciones y mitiga vulnerabilidades de seguridad. **CodeWhisperer** asegura la propiedad intelectual al mostrar el origen del código abierto sugerido, mejorando la fiabilidad y manteniendo las aplicaciones seguras ante nuevas amenazas.

RESUMEN MÓDULO 9

En el **módulo 9** se trataron los siguientes conceptos:

1. **Cloud Adoption Framework:** Este marco ayuda a identificar los roles y enfoques necesarios para la migración a la nube, con perspectivas tanto técnicas (plataforma, seguridad, operaciones) como no técnicas (negocios, personal, gobernanza).
2. **Seis estrategias de migración:** Incluye estrategias como volver a alojar, redefinir la plataforma, volver a comprar, refactorizar, retirar (jubilar) y retener para trasladar soluciones a la nube.
3. **Familia de productos AWS Snow:** Se presentan dispositivos físicos que facilitan la transferencia masiva de datos a AWS sin utilizar la red, proporcionando una solución segura y eficiente para evitar problemas de rendimiento.
4. **Innovación con servicios de AWS:** Se exploran servicios innovadores que pueden optimizar la migración y el uso de AWS para las empresas.

Módulo 10: El traspaso a la nube

Introducción

1.1 Introducción (resumen vídeo)

En este módulo aprenderás a:

1. **Resumir los seis pilares de Well-Architected Framework:** Este marco ayuda a evaluar arquitecturas y alcanzar la excelencia en áreas como: excelencia operativa, seguridad, fiabilidad, eficiencia de rendimiento, optimización de costes y sostenibilidad.
2. **Explicar los seis beneficios de la computación en la nube:** El curso aborda cómo AWS ofrece opciones para crear soluciones a través de servicios, y cómo herramientas como el Well-Architected Framework permiten mejorar arquitecturas, garantizando su fiabilidad y rendimiento.

AWS Well-Architected Framework

1.1 Introducción (resumen vídeo)

Well-Architected Framework ayuda a crear infraestructuras seguras, de alto rendimiento, resistentes y eficientes en AWS. Está compuesto por seis pilares:

1. **Excelencia operativa:** Se enfoca en el funcionamiento y supervisión de los sistemas, y en la mejora continua, como la automatización de cambios.
2. **Seguridad:** Garantiza la integridad de los datos y la protección de los sistemas, incluyendo el cifrado.
3. **Fiabilidad:** Planifica la recuperación ante fallos y gestiona los cambios para satisfacer las demandas empresariales.
4. **Eficiencia del rendimiento:** Impulsa el uso eficiente de recursos, como elegir el tipo adecuado de EC2 según la carga de trabajo.
5. **Optimización de costes:** Busca reducir los gastos, como ajustar el tamaño de servidores para optimizar el costo total.
6. **Sostenibilidad:** Minimiza el impacto medioambiental, centrado en reducir el consumo de energía y aumentar la eficiencia.

Well-Architected Tool es una herramienta de autoservicio para evaluar cargas de trabajo en AWS, generando informes con un sistema de semáforos (verde, naranja, rojo) para identificar áreas de mejora y sugerir soluciones siguiendo las mejores prácticas.

1.2 The AWS Well-Architected Framework

El AWS Well-Architected Framework ayuda a diseñar y operar sistemas confiables, seguros, eficientes y rentables en AWS, evaluando las arquitecturas según las mejores prácticas y principios de diseño. Se compone de seis pilares:

1. **Excelencia operativa:** Enfocada en ejecutar y supervisar sistemas para aportar valor y mejorar procesos de manera continua, mediante prácticas como cambios pequeños y reversibles.
2. **Seguridad:** Protege información y sistemas con evaluaciones de riesgos y estrategias de mitigación. Incluye automatización de prácticas de seguridad y protección de datos en todas las capas.
3. **Fiabilidad:** Asegura la capacidad de los sistemas para recuperarse de interrupciones, escalar dinámicamente y mitigar problemas como configuraciones erróneas.
4. **Eficiencia de rendimiento:** Optimiza el uso de recursos para satisfacer los requisitos del sistema y mantener la eficiencia a medida que cambian la demanda y la tecnología.
5. **Optimización de costes:** Permite ejecutar sistemas al menor costo posible mediante un modelo de consumo y el uso de servicios administrados.
6. **Sostenibilidad:** Introducido en 2021, este pilar mejora el impacto ambiental mediante la reducción del consumo de energía y la maximización de la eficiencia de los recursos, con un enfoque en la adopción de tecnologías más eficientes.

Estos pilares guían la creación de arquitecturas que mejoren el rendimiento y reduzcan costos y el impacto medioambiental.

Beneficios de la nube de AWS

1.1 Introducción (resumen vídeo)

El curso sobre AWS te proporciona los conocimientos necesarios para comprender los servicios de la nube de AWS y cómo combinarlos para crear soluciones flexibles y escalables. A medida que avanzas, conocerás términos clave de AWS y los beneficios de usar su infraestructura.

Las seis principales ventajas de usar AWS son:

1. **Costos variables:** A diferencia de los centros de datos tradicionales, AWS cobra solo por lo que consumes, lo que permite ajustar el presupuesto mes a mes.
2. **Economías de escala:** AWS compra hardware en grandes volúmenes, lo que reduce costos y permite una mayor eficiencia operativa.

3. **No necesidad de estimar la capacidad:** Con AWS, solo pagas por los recursos que usas y puedes escalarlos según tus necesidades, evitando sobrecostos o falta de capacidad.
4. **Velocidad y agilidad:** Puedes probar nuevas soluciones rápidamente, sin los altos costos de infraestructura, acelerando el tiempo de salida al mercado.
5. **Sin inversión en mantenimiento de centros de datos:** AWS maneja la infraestructura, permitiendo que te concentres en el valor y la innovación de tu negocio.
6. **Globalización rápida:** Puedes expandir tu infraestructura a nivel mundial en minutos, con la capacidad de replicar tu arquitectura en diferentes regiones automáticamente.

En resumen, AWS te permite crear soluciones escalables, flexibles y globales sin necesidad de grandes inversiones iniciales o preocupaciones sobre la infraestructura, lo que facilita la innovación y mejora la eficiencia operativa.

1.2 Beneficios de la Computación en la nube

Los beneficios de la computación en la nube de AWS incluyen:

1. **Gasto variable en lugar de gasto inicial:** No necesitas invertir en centros de datos o servidores antes de usarlos; solo pagas por los recursos que consumes.
2. **Economías de escala masiva:** AWS logra precios más bajos debido a su escala global, lo que se traduce en costos más bajos para los usuarios.
3. **Eliminación de la necesidad de adivinar la capacidad:** Puedes ajustar los recursos según la demanda, sin tener que prever cuánta capacidad necesitarás con antelación.
4. **Mayor velocidad y agilidad:** La nube permite desarrollar, implementar y ajustar aplicaciones rápidamente, lo que fomenta la innovación.
5. **Reducción de costos operativos:** Ya no necesitas gestionar centros de datos; AWS se encarga de la infraestructura, permitiéndote concentrarte en el desarrollo y los clientes.
6. **Alcance global en minutos:** AWS permite desplegar aplicaciones globalmente, ofreciendo baja latencia y acceso rápido para usuarios en todo el mundo.

RESUMEN MÓDULO 10

En el Módulo 10, se cubren dos temas principales. Primero, los seis pilares de AWS Well-Architected Framework: excelencia operativa, seguridad, fiabilidad, eficiencia de rendimiento, optimización de costes y sostenibilidad. Segundo, las seis ventajas de la computación en la nube: pasar de gasto inicial a gasto variable, aprovechar economías de escala, no tener que adivinar la capacidad, aumentar la velocidad y agilidad, reducir el gasto en mantenimiento de centros de datos y lograr un alcance global en minutos.

