Cloud Computing - AWS

ACADEMIA CONSULTEC

Presentado por **Alejandro Chacón**
www.consultec-ti.com

Alejandro Chacón

Ingeniero DevOps @Consultec

Alejandro es Licenciado en Computación con certificaciones relacionadas con tecnologías de IAC, Kubernetes y Arquitectura en la Nube (AWS, Azure y GCP). Además, posee experiencia en Administración de Sistemas GNU/Linux, Soporte Técnico y herramientas CI/CD.

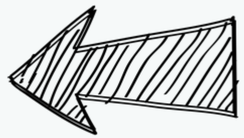
Proyectos:

- Sr DevOps en AES Energy Corp
- Sr DevOps en Yappy/BG

ACADEMIA CONSULTEC

Agenda

- Intro



- Almacenamiento S3
- Networking
- Cómputo y Almacenamiento
- Integración y Monitoreo
- Bases de Datos
- Seguridad
- Despliegues y Gestión de Infraestructura

ACADEMIA CONSULTEC

Cloud Computing

Generalidades - Costos/Labs

En el desarrollo del curso estaremos usando máquinas virtuales con el conjunto de herramientas necesarias para elaborar nuestras actividades propuestas, donde estaremos configurando mediante un terminal el acceso a la cuenta AWS que hospedará nuestras pruebas.

- La mayoría de los servicios que usaremos están comprendidos en la capa de gratuita de AWS Free-Tier.
- En caso de que hagamos uso de servicios alternativos que no estén comprendidos, lo mencionaremos con tiempo para tenerlo en cuenta en las prácticas.
- Recordemos al culminar el día, limpiar todos los cambios que originan costos al dejarlo encendidos.
- Podemos obtener mayor información en:
  - https://aws.amazon.com/free/

ACADEMIA CONSULTEC

Cloud Computing

Terminologia

- Client
- Server
- Network
- Router
- Switch
- Host
- Database
- ...

Cloud Computing

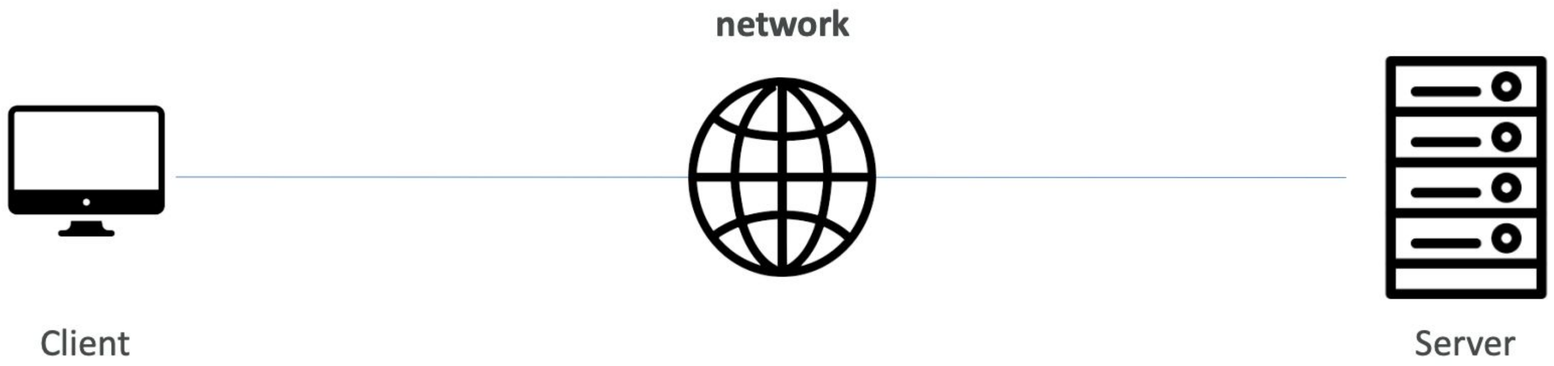
- Cloud vs On-premise
- Modelos de despliegues en la nube
- Caracteristicas del Cloud Computing
- Modelo de servicios en la nube
- Modelo de responsabilidad compartida

ACADEMIA CONSULTEC

Cloud Computing

¿Cómo funciona?

IP Cliente / IP Servidor



Cloud Computing
Esquema Tradicional

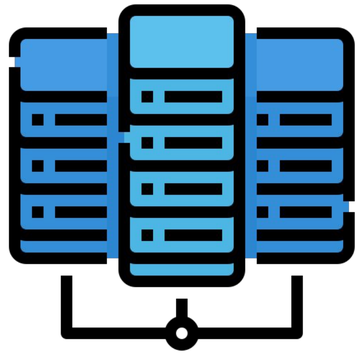
¿Cómo está compuesto un servidor?

- Computo
- Memoria
- Almacenamiento
- Red
- OS/App

Cloud Computing
Esquema Tradicional - Motivaciones

- Al pasar los años, más gente requiere computadoras
- Eventualmente se necesita conectividad
- Almacenar datos centralizados
- Alto costo en compras de equipos
- En pocos años, nuevas tecnologías
- App nuevas, mayor consumo de HW

Mantenerse actualizado,
se vuelve una carrera sin fin!

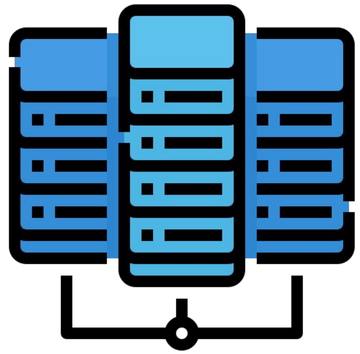


ACADEMIA CONSULTEC

Cloud Computing

Esquema Tradicional - Problemas

- Pagos de rentas en centros de datos
- Pagos al servicio eléctrico, climatización (A/C) y mantenimiento.
- Agregar y reemplazar equipamiento, consume tiempo.
- El escalamiento es limitado.
- Se debe tener personal 24/7 para monitoreo de la infraestructura.
- Manejo ante desastres naturales ...



ACADEMIA CONSULTEC

Cloud Computing

Concepto

La computación en la nube es un modelo para la prestación de servicios informáticos a través de Internet. Permite que las personas y las organizaciones utilicen potentes recursos informáticos, como servidores, almacenamiento y aplicaciones, sin tener que invertir en hardware e infraestructura.

Video Conceptual - 1:38 min

ACADEMIA CONSULTEC

Cloud Computing
Concepto

- Nos ofrece entrega on-demand en cómputo, almacenamiento, aplicaciones y otros servicios IT, con el foco de que pagas por lo que usas (pay-as-you-go).
- Es posible aprovisionar tipo y tamaño en recursos que necesites en todo momento.
- Se puede acceder casi instantáneamente a muchos recursos en la nube, ganando tiempo en estar en el mercado.

  Por ejemplo, AWS es dueño y mantiene todo el equipamiento conectado a la red, para ofrecer todos estos servicios, mientras nosotros configuramos y usamos vía una aplicación web.

ACADEMIA CONSULTEC

Cloud Computing

Modelos desplegados en la Nube

- Nube Privada
  - Servicios usados por una simple organización, no expuesta públicamente
  - Completo control
  - Seguridad para aplicaciones sensitivas
  - Cumple necesidades específicas del negocio
- Nube Pública
  - Todos los recursos pertenecen y son operados por terceros, expuestos en internet para quien lo necesite.
- Nube Híbrida
  - Mantiene un mix, con on-premise y se extiende en algunas capacidades a la nube.

ACADEMIA CONSULTEC

Cloud Computing

Características

- Servicios a demanda
  - Usuarios puede aprovisionar recursos y usarlos sin interacción humana.
- Acceso a la gran red
  - Recursos disponibles en la red, pueden ser accedidos desde diversas plataformas del cliente.
- Multiple tenencia y agrupación de recursos
  - Múltiples clientes pueden compartir la misma infraestructura; aplicaciones con seguridad y privacidad.
- Elasticidad y escalabilidad
  - Automáticamente y rápidamente dispone de recursos necesarios; fácilmente escala basado en la demanda.
- Servicios cuantificados
  - El uso es medido, los usuarios pagan correctamente lo que es usado en recursos.

Cloud Computing

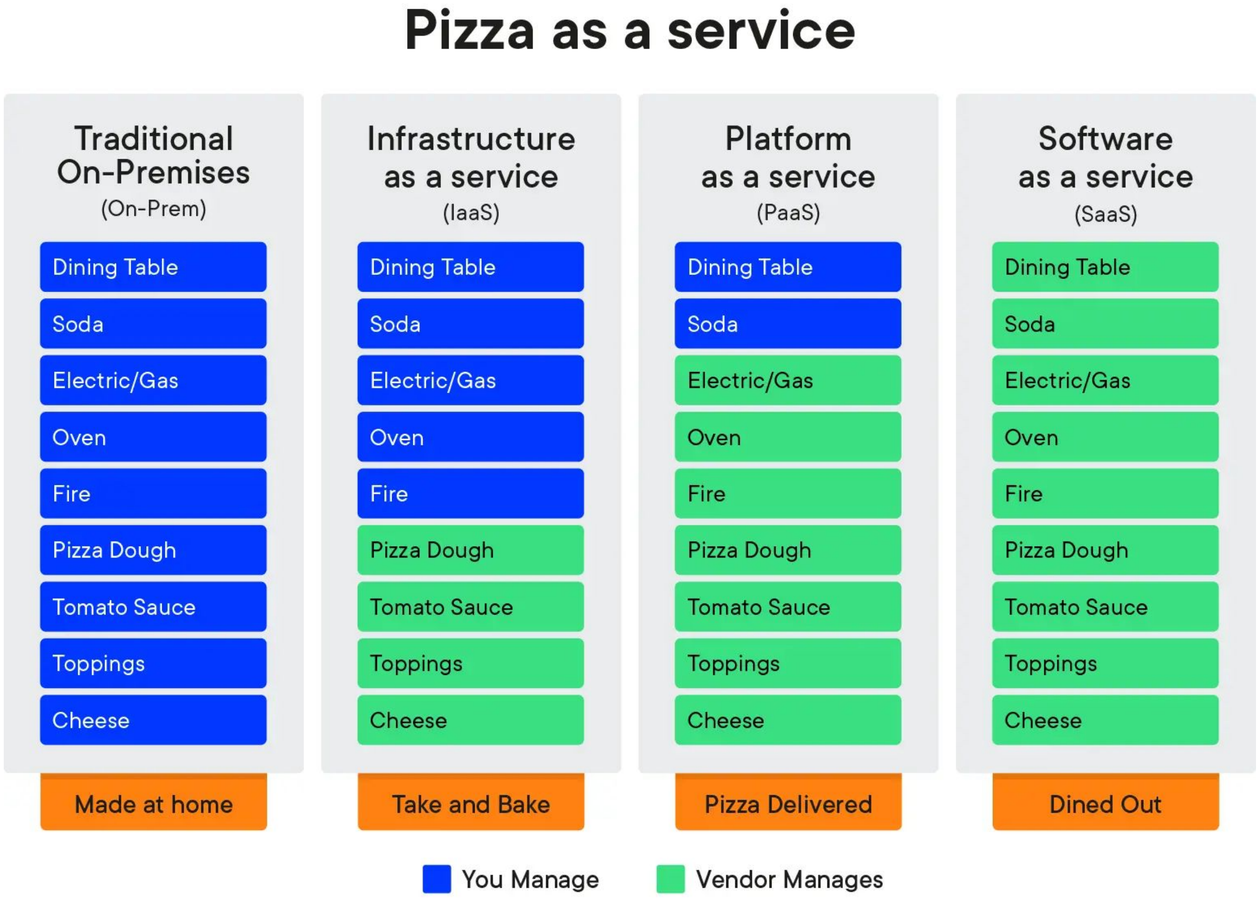
Ventajas

- CAPEX (Capital Expense) sobre OPEX (Operational Expense)
    - Reducción del costo total de equipos (TCO) y el OPEX
- Economía de escala
- No hay necesidad de adivinar la capacidad
- Crece con velocidad y agilidad
- No más dinero en levantar y mantener centros de datos
- Ser globales en minutos.
- Está demostrado que se gana: flexibilidad, escalabilidad, costo beneficio, elasticidad, agilidad, alta disponibilidad y tolerancia a fallos.

ACADEMIA CONSULTEC

Cloud Computing

Modelos de Servicios Cloud



Cloud Computing

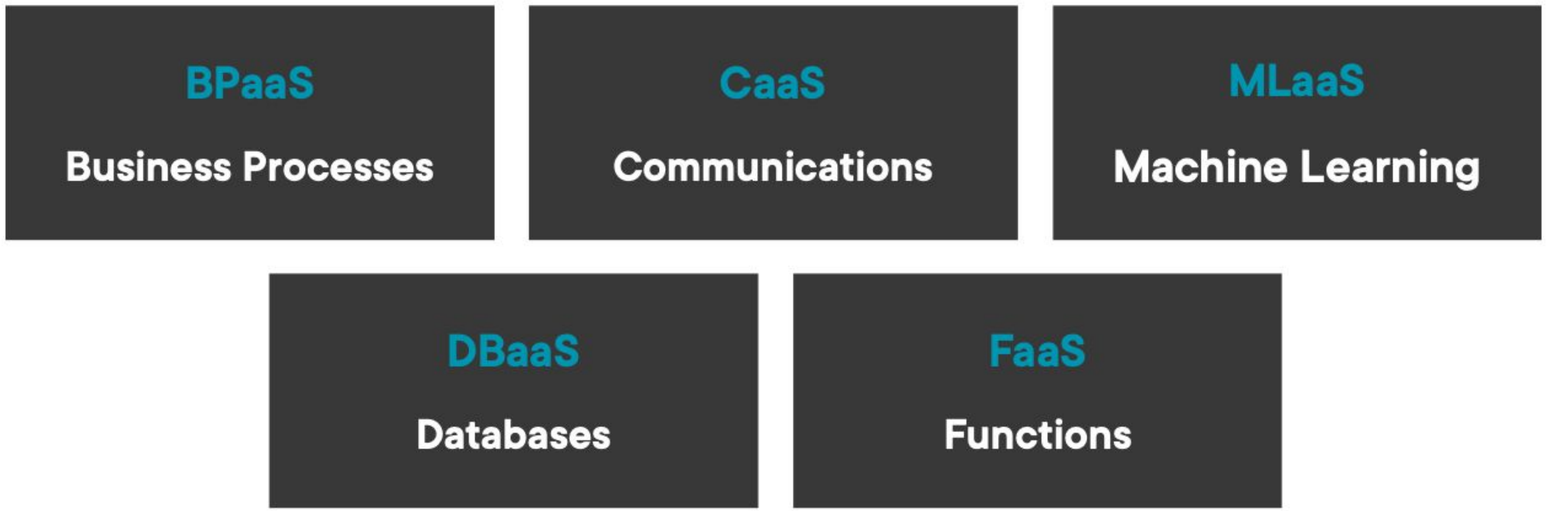
Modelos de Servicios Cloud

- Infrastructure as a Service (IaaS)
  - Provee networking, cómputo, almacenamiento
  - Alto nivel de flexibilidad
  - EC2 AWS / Linode / DRoplets DO/ Compute GCP
- Platform as a Service (PaaS)
  - Sin responsabilidad en la infraestructura
  - Enfocado en despliegues y administrar las apps
  - Elastic Beanstalk AWS / Heroku/ App Engine GCP
- Software as a Service (SaaS)
  - Producto administrado completamente por un tercero o service provider
  - Rekognition ML AWS / Gmail / Zoom

ACADEMIA CONSULTEC

Cloud Computing

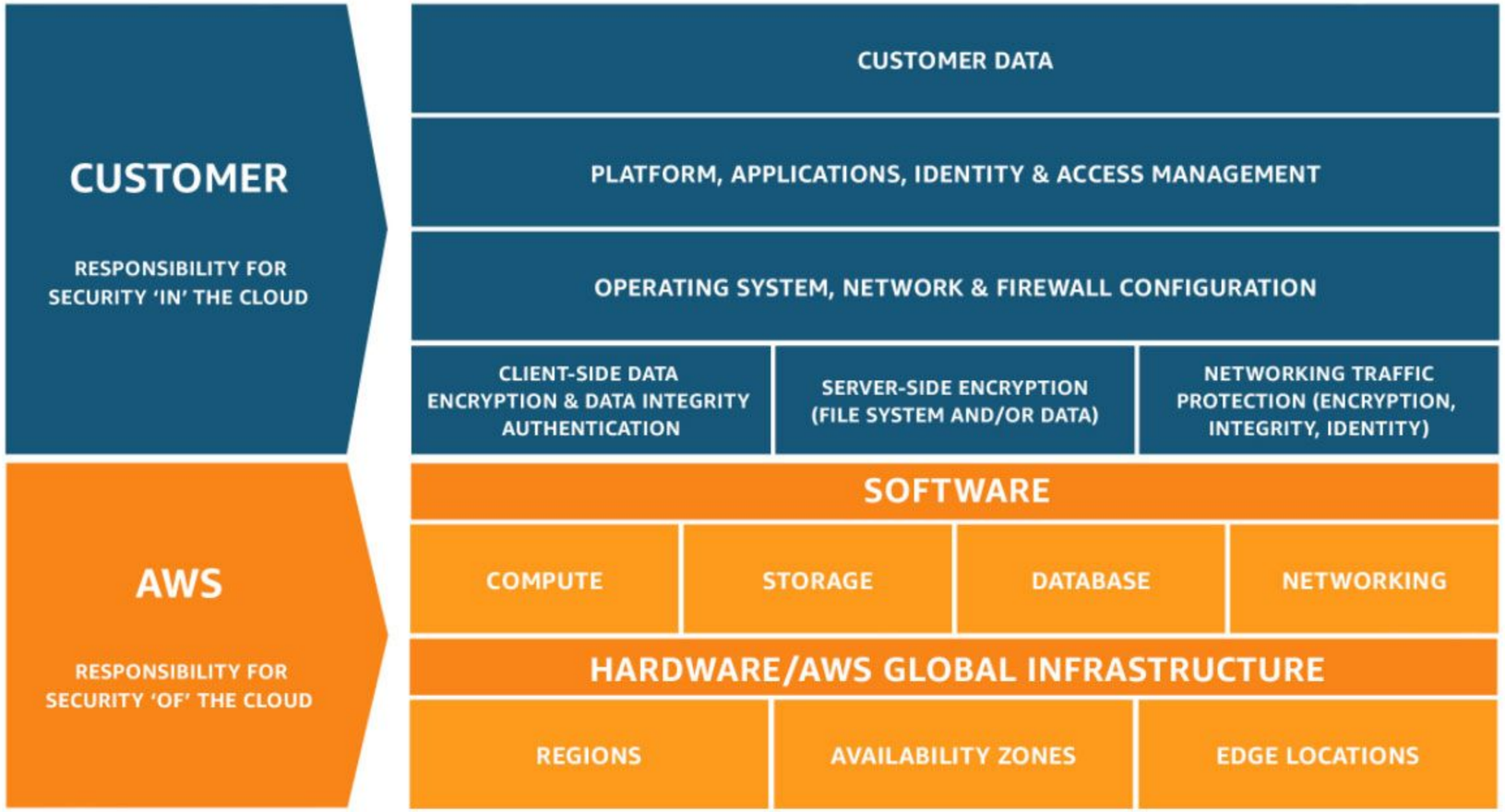
Otros Modelos de Servicios Cloud



ACADEMIA CONSULTEC

Cloud Computing

Modelo de Responsabilidad Compartida



ACADEMIA CONSULTEC

Ya Volvemos!
Un pequeño descanso.

Cloud Computing - AWS

ACADEMIA CONSULTEC

AWS Ecosistema

- Aventura de las Certificaciones
- Well Architected Framework
- Infraestructura AWS
- Comparativa en abanico de servicios en la nube

ACADEMIA CONSULTEC

AWS Ecosistema

Camino de certificaciones

FOUNDATIONAL

Certificación basada en conocimientos para obtener conocimiento básico de la nube de AWS.
No se necesita experiencia previa.

ASSOCIATE

Certificaciones basadas en roles que demuestran su conocimiento y habilidades de AWS y que construyen su credibilidad como profesional de la nube de AWS. **Se recomienda tener experiencia previa sólida en TI local o en la nube.**

PROFESIONAL

Certificaciones basadas en roles que validan habilidades y conocimientos avanzados necesarios para diseñar aplicaciones seguras, optimizadas y modernas, y automatizar procesos en AWS. **Se recomienda tener 2 años de experiencia previa en la nube de AWS**

SPECIALTY

Aprenda a profundidad y posiciónese como un asesor de confianza para las partes interesadas o clientes de estas áreas estratégicas. **Consulte las guías de examen en las páginas de exámenes para saber la experiencia recomendada.**

ACADEMIA CONSULTEC

AWS Ecosistema

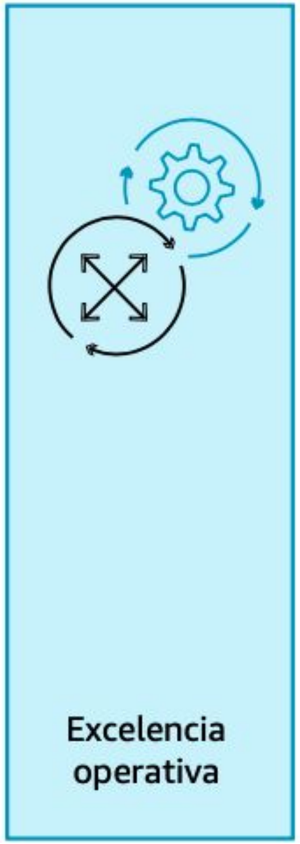
Well Architected y los 6 Pilares

ACADEMIA CONSULTEC

AWS Ecosistema

Excelencia Operativa

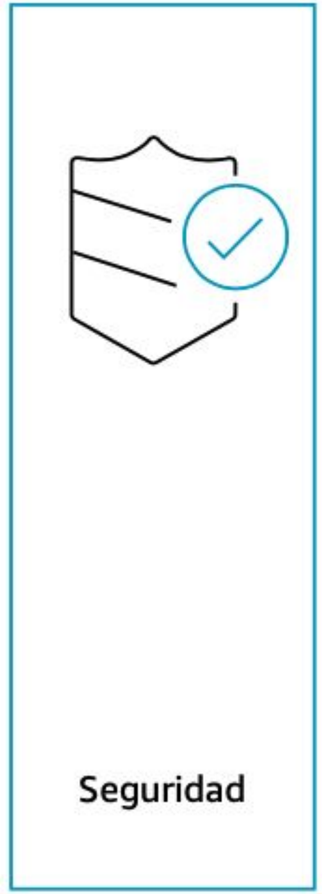
El pilar de la excelencia operativa se concentra en ejecutar y monitorear los sistemas y en mejorar constantemente los procesos y los procedimientos. Entre los temas clave se incluyen la automatización de cambios, la respuesta a eventos y la definición de estándares para administrar las operaciones diarias.



AWS Ecosistema

Seguridad*

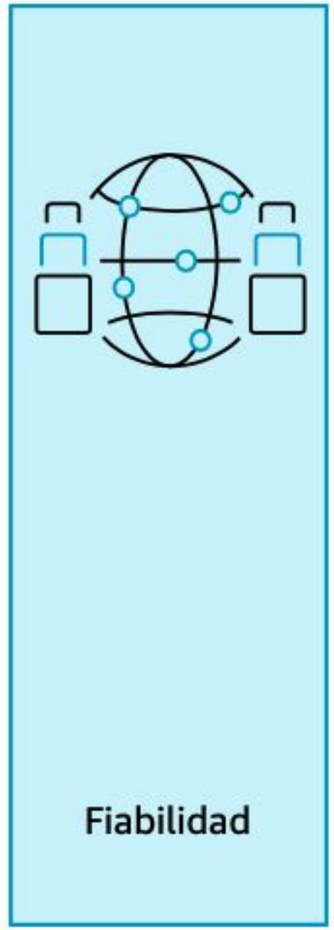
El pilar de la seguridad se concentra en proteger la información y los sistemas. Entre los temas clave se incluyen la confidencialidad y la integridad de los datos, la administración de los permisos de usuarios y el establecimiento de controles para detectar eventos de seguridad.



AWS Ecosistema

Fiabilidad

El pilar de fiabilidad se centra en las cargas de trabajo que realizan las funciones previstas y en cómo recuperarse rápidamente de los errores para cumplir con las demandas. Entre los temas clave se incluyen el diseño de sistemas distribuidos, la planificación de la recuperación y cómo adaptarse a los requisitos cambiantes.

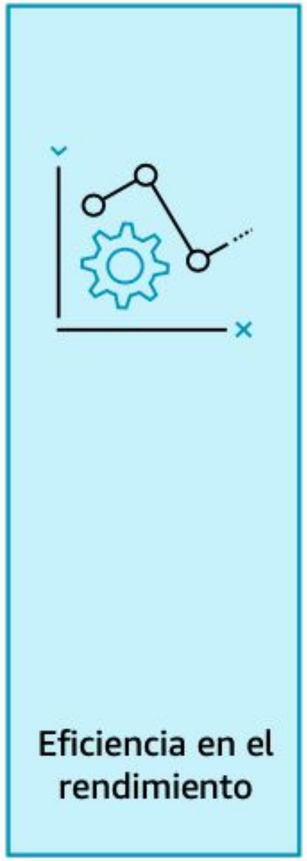


ACADEMIA CONSULTEC

AWS Ecosistema

Eficiencia en el Rendimiento

El pilar de eficacia del rendimiento se centra en la asignación estructurada y simplificada de TI y en los recursos informáticos. Entre los temas clave se incluyen la selección de los tipos y tamaños de recursos optimizados para los requisitos de la carga de trabajo, la supervisión del rendimiento y el mantenimiento de la eficacia a medida que evolucionan las necesidades de la empresa.

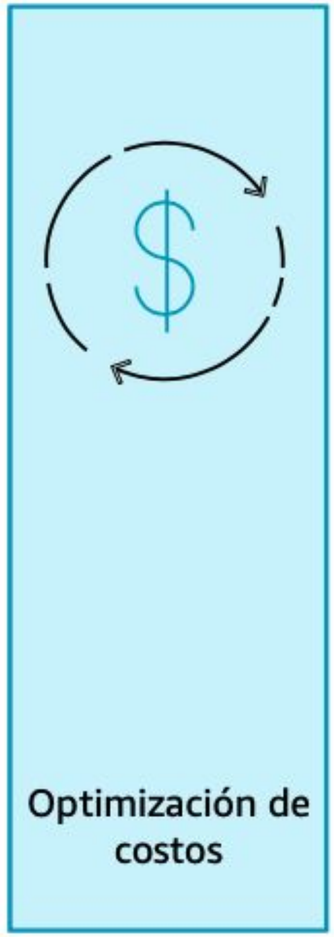


ACADEMIA CONSULTEC

AWS Ecosistema

Optimización de Costos

El pilar de optimización de costos se centra en evitar gastos innecesarios. Entre los temas clave se incluyen la comprensión del tiempo dedicado y el control de la asignación de fondos, la selección correcta del tipo de recursos y cantidad adecuada, y escalar para satisfacer las necesidades comerciales sin gastar de más.

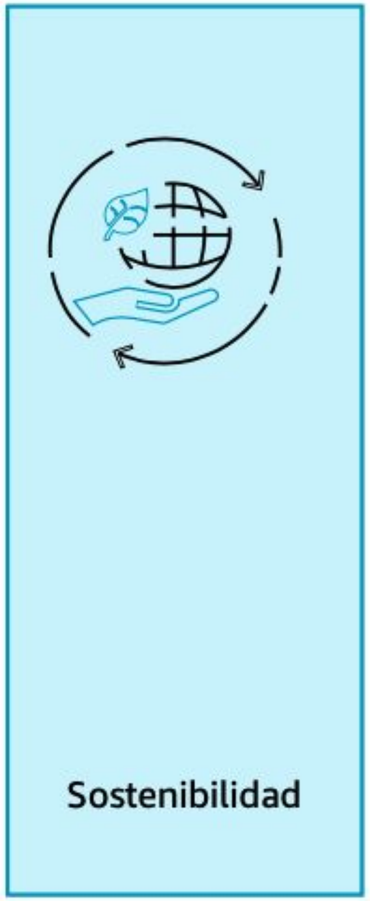


ACADEMIA CONSULTEC

AWS Ecosistema

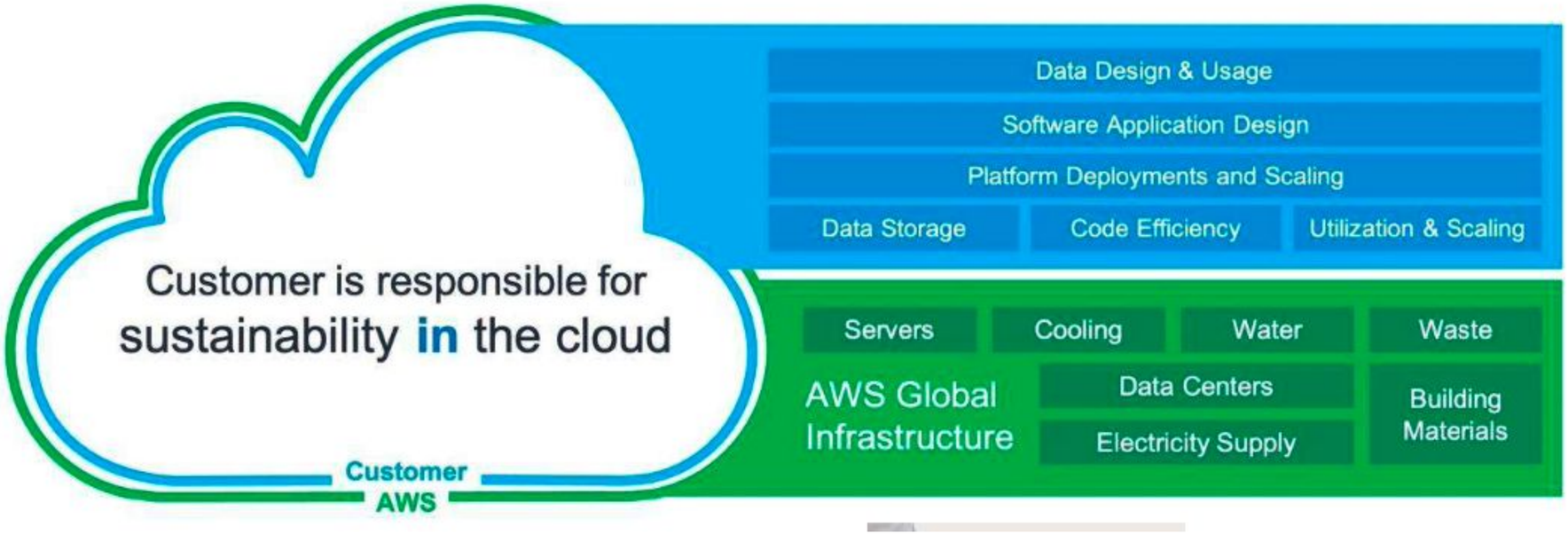
Sostenibilidad

El pilar de sostenibilidad se centra en minimizar los impactos ambientales de ejecutar cargas de trabajo en la nube. Entre los temas clave se incluyen un modelo de responsabilidad compartida para la sostenibilidad, la comprensión del impacto y la maximización del uso para minimizar los recursos necesarios y reducir los impactos posteriores.



AWS Ecosistema

Sostenibilidad



ACADEMIA CONSULTEC

AWS Ecosistema

Infraestructura Global

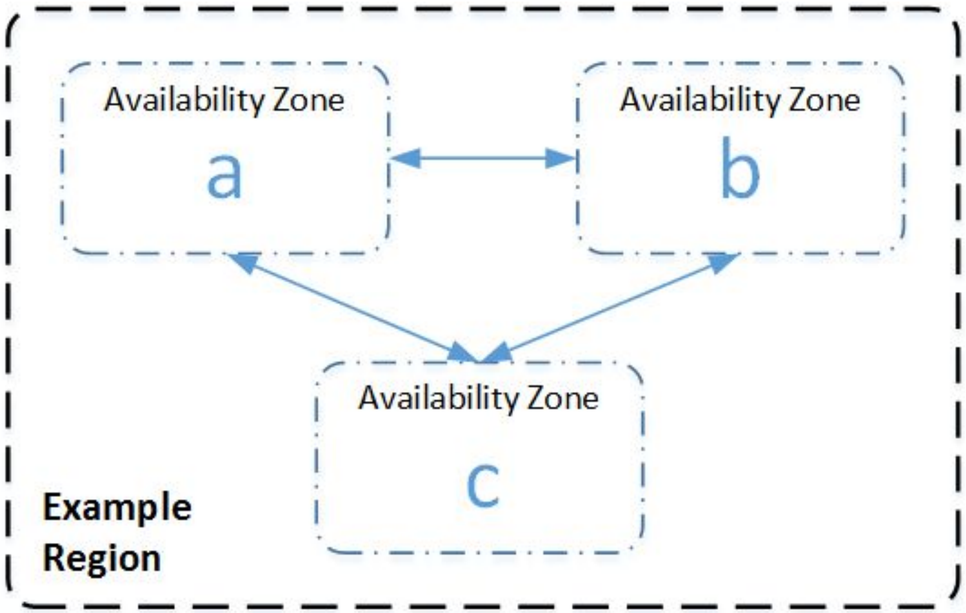
- AWS Regiones
- AWS Zonas de Disponibilidad
- AWS Centro de Datos
- AWS Edge Locations
  - Puntos de Presencia

ACADEMIA CONSULTEC

AWS Ecosistema

Regiones

- AWS tiene regiones alrededor de todo el mundo.
- Su nomenclatura está relacionada con la región y zona: us-east-1, eu-west-3.
- Una región es un cluster de centro de datos.
- La mayoría de los servicios AWS, están centrados en regiones.
- Algunos criterios de selección:
  - Compliance, relacionado con requerimientos legales en manejo de datos.
  - Proximidad con los clientes, menor latencia.
  - Servicios disponibles, no todos los servicios están disponibles en las regiones.
  - Precios, pueden variar por zonas.

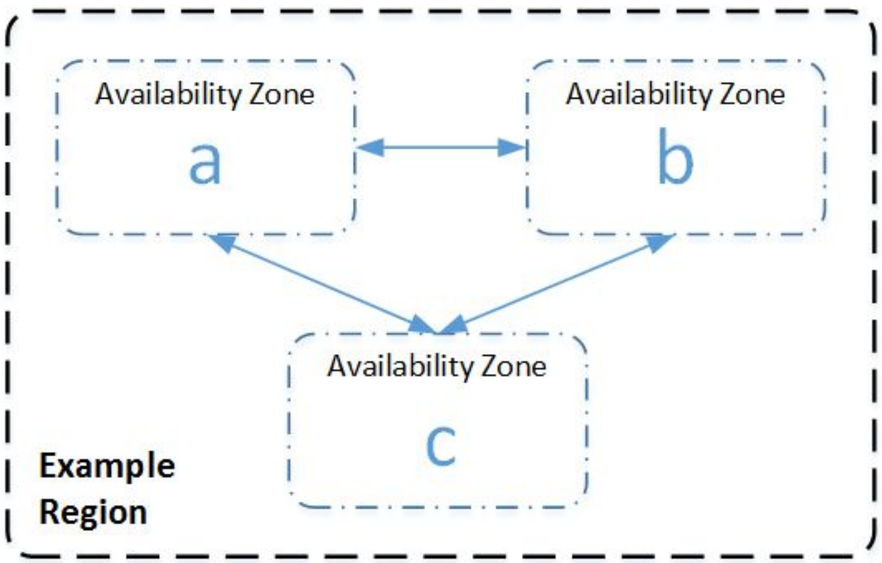


ACADEMIA CONSULTEC

AWS Ecosistema

Zonas de Disponibilidad AZ

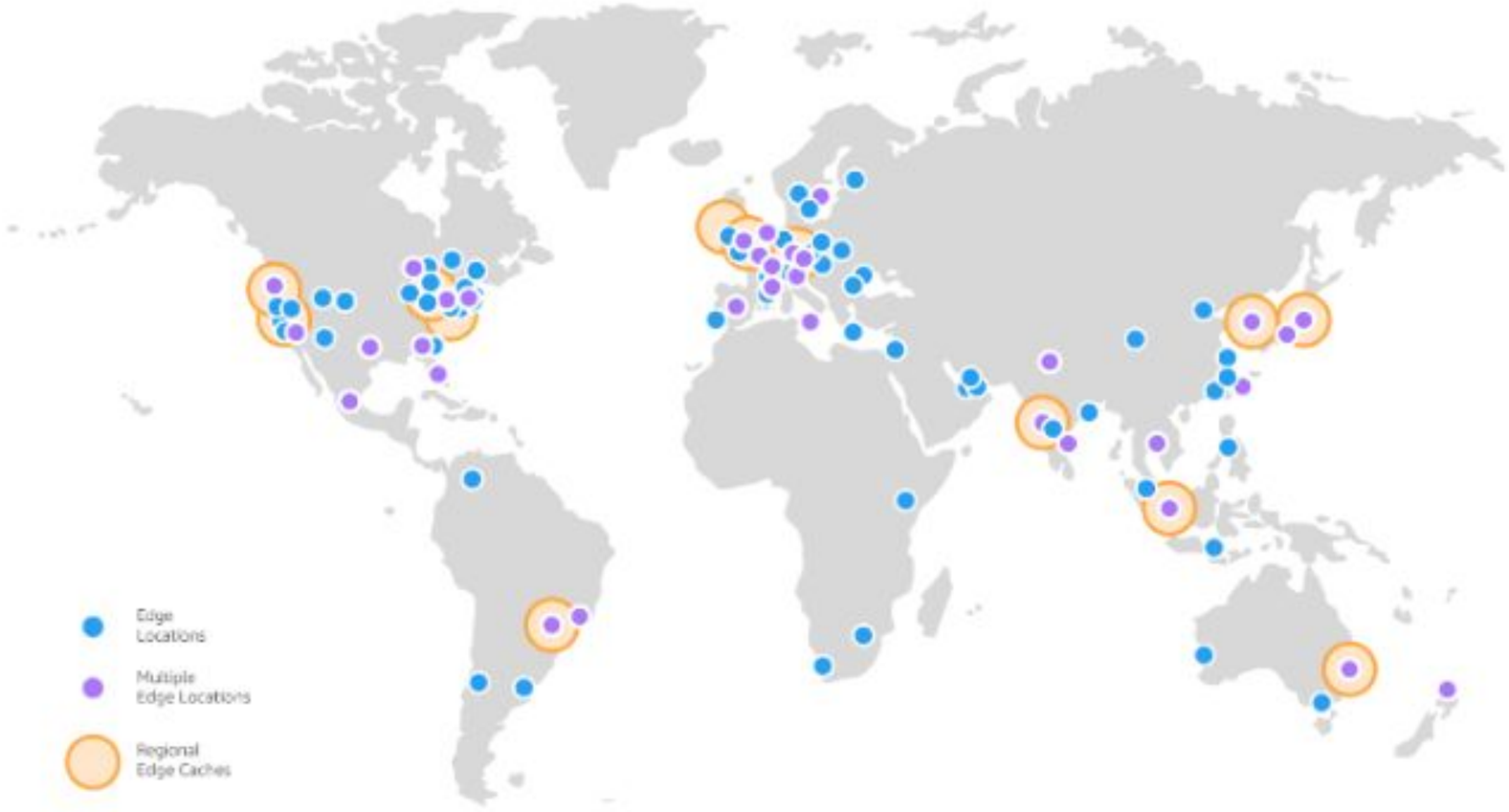
- Cada región tiene varias AZ, usualmente 3, con mínimo 2 y máximo 6; nombradas de la siguiente manera:
  - us-east-1a / us-east-1b /us-east-1c.
- Cada Zona tiene uno o más data centers con redundancia en poder, red y conectividad.
- Están separadas y aisladas para evitar los desastres naturales.
- Conectadas con alto ancho de banda y baja latencia.



ACADEMIA CONSULTEC

AWS Ecosistema

Edge Locations / Puntos de Presencia

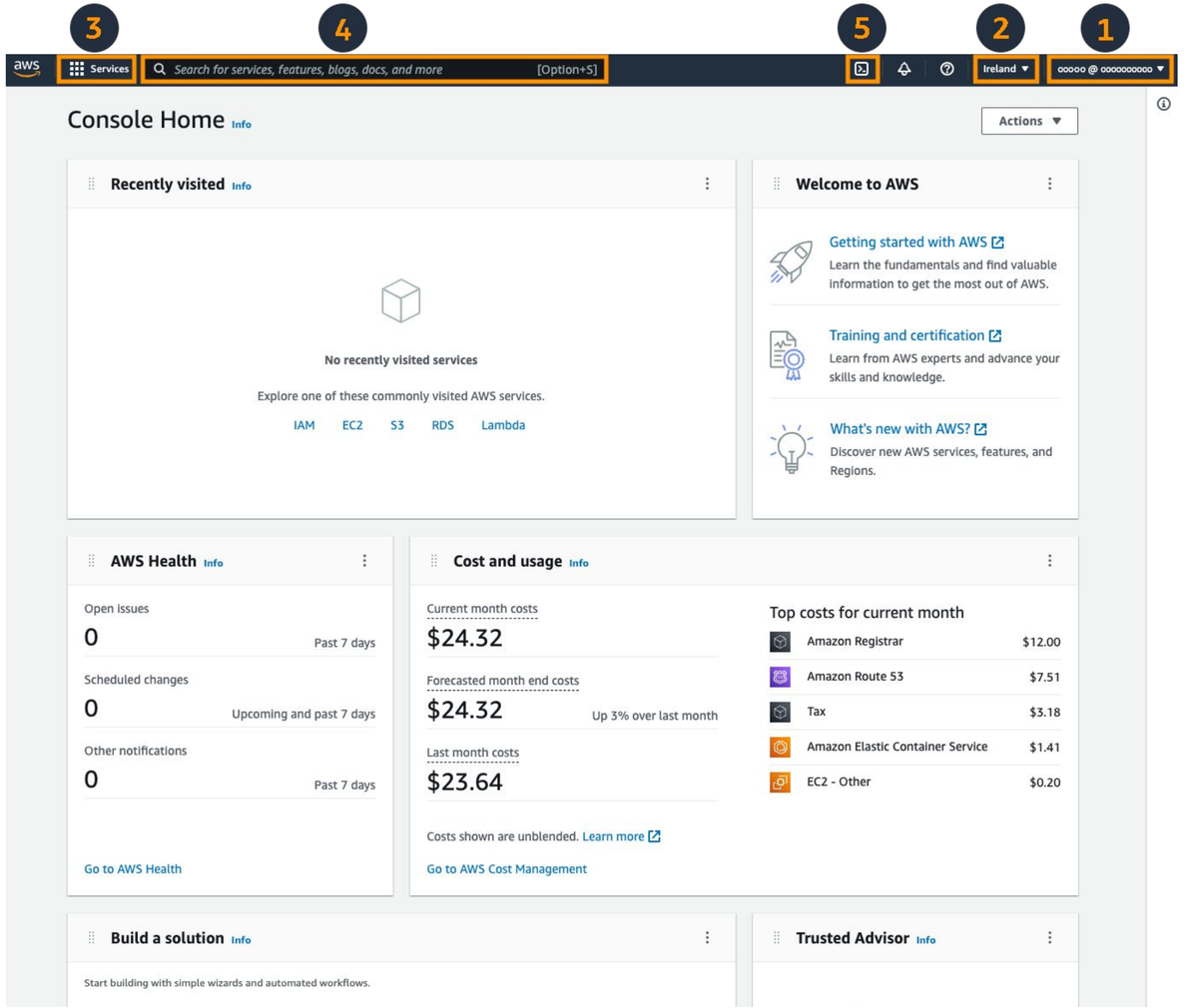


ACADEMIA CONSULTEC

AWS Ecosistema

Tour por la Consola WEB

- Global Services:
  - IAM - Users and policies managements
  - Route 53 - DNS services
  - Cloudfront - CDN Content Delivery Network
  - WAF - Web Application Firewall
- Servicios por Región:
  - EC2 - IaaS
  - Elastic Beanstalk - PaaS
  - Lambda - FaaS
  - Rekognition - SaaS



ACADEMIA CONSULTEC

AWS Ecosistema

Comparativa de servicios en nubes públicas

Service	AWS	Azure	GCP
Compute	Amazon EC2, AWS Lambda, Amazon ECS, AWS Fargate	Azure Virtual Machines, Azure Functions, Azure Kubernetes Service (AKS)	Google Compute Engine, Cloud Functions, Google Kubernetes Engine (GKE)
Storage	Amazon S3, Amazon EBS, Amazon Glacier, Amazon Elastic File System (EFS)	Azure Blob Storage, Azure Files, Azure Disk Storage	Google Cloud Storage, Cloud SQL, Cloud Spanner
Database	Amazon RDS, Amazon DynamoDB, Amazon Redshift, Amazon Neptune	Azure SQL Database, Azure Cosmos DB, Azure Database for PostgreSQL, Azure Database for MySQL	Google Cloud SQL, Cloud Spanner, Cloud Bigtable
Networking	Amazon VPC, Amazon Route 53, Elastic Load Balancing (ELB), AWS Direct Connect	Azure Virtual Network, Azure DNS, Azure Load Balancer, Azure ExpressRoute	Google Virtual Private Cloud (VPC), Cloud DNS, Cloud Load Balancing, Cloud Interconnect
Analytics	Amazon EMR, Amazon Kinesis, Amazon Redshift, AWS Glue	Azure HDInsight, Azure Stream Analytics, Azure Data Factory, Azure Databricks	Google Cloud Dataproc, Cloud Dataflow, BigQuery
Security	AWS Identity and Access Management (IAM), Amazon Inspector, Amazon GuardDuty, AWS WAF	Azure Active Directory (AD), Azure Security Center, Azure Sentinel, Azure Firewall	Google Cloud Identity and Access Management (IAM), Cloud Security Command Center, Cloud Armor

ACADEMIA CONSULTEC

Ya Volvemos!
Un pequeño descanso.

Cloud Computing - AWS

ACADEMIA CONSULTEC

AWS IAM

- Intro
- Usuarios y Grupos
- Políticas y Roles
- Security - MFA
- Acceso CLI / SDK

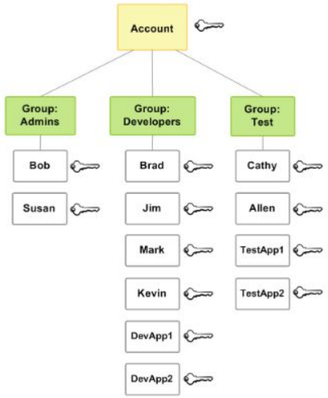
AWS IAM
Identity & Access Management

Es donde se especifica quién o qué puede acceder a los servicios y recursos en AWS, administrar de forma centralizada los permisos específicos y analizar el acceso para perfeccionar los permisos en todo AWS.

ACADEMIA CONSULTEC

AWS IAM
Users & Groups

- IAM es un servicio global
- Cuenta Root es creada por default y no debería ser usada o compartida.
- Usuarios son personas dentro de la organización que pueden ser agrupadas.
- Grupos sólo pueden contener usuarios, no otros grupos.
- Usuarios pueden estar sin grupos, o pueden pertenecer a varios.
- Se recomienda el uso de grupos para diferentes perfiles de usuarios en AWS.



ACADEMIA CONSULTEC

AWS IAM
Permisos

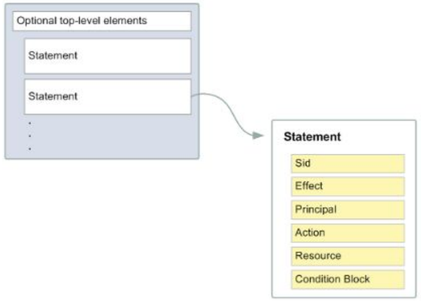
- Una política es un objeto de AWS que, cuando se asocia a una identidad o un recurso, define sus permisos. AWS evalúa estas políticas cuando una entidad principal de IAM (usuario o rol) realiza una solicitud. Los permisos en las políticas determinan si la solicitud se permite o se deniega. La mayoría de políticas se almacenan en AWS como documentos JSON.
- Usuarios o grupos se les puede asignar políticas.
- Estas políticas definen los permisos de los usuarios.
- Se introduce el concepto del principio de menor privilegio (Least privilege principle) donde no daremos más permisos de los que se necesitan.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "s3:ListBucket",
    "Resource": "arn:aws:s3:::example_bucket"
  }
}
```

ACADEMIA CONSULTEC

AWS IAM
Estructura de los Permisos

- *Version* – Especifica la versión del idioma de la política que desea utilizar. Le recomendamos que utilice la última versión de 2012-10-17.
- *Statement* – Utilice este elemento de política principal como contenedor de los siguientes elementos. Puede incluir varias instrucciones en una política.
- *Sid* (Opcional) – Incluye un *ID* de instrucción opcional para diferenciar entre las instrucciones.
- *Effect* – Utilice *Allow* o *Deny* para indicar si la política permite o deniega el acceso.
- *Principal* (Obligatorio únicamente en algunas circunstancias): si crea una política basada en recursos, debe indicar la cuenta, el usuario, el rol o el usuario federado al que desea permitir o denegar el acceso. Si va a crear una política de permisos de IAM para asociarla a un usuario o un rol, no puede incluir este elemento. La entidad principal está implícita como ese usuario o rol.
- *Action* – Lista de acciones que la política permite o deniega.
- *Condition* (Opcional) - Especifica las circunstancias bajo las cuales la política concede permisos.

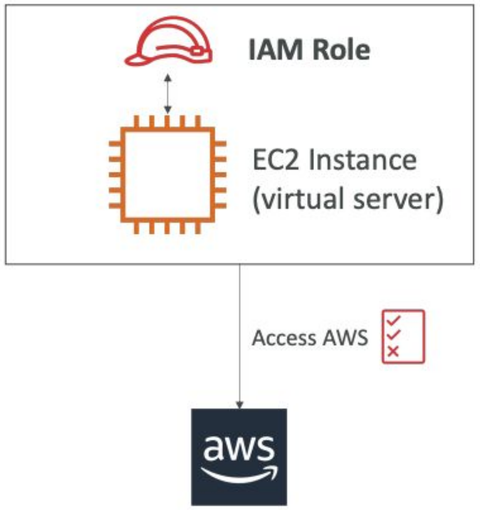



```
{
    "Version": "2012-10-17",
    "Id": "S3-Account-Permissions",
    "Statement": [
        {
            "Sid": "1",
            "Effect": "Allow",
            "Principal": {
                "AWS": ["arn:aws:iam::123456789012:root"]
            },
            "Action": [
                "s3:GetObject",
                "s3:PutObject"
            ],
            "Resource": ["arn:aws:s3:::mybucket/*"]
        }
    ]
}
```

ACADEMIA CONSULTEC

AWS IAM
Roles

- Un *rol* de IAM es una identidad de IAM que puede crear en su cuenta y que tiene permisos específicos. Un rol de IAM es similar a un usuario de IAM en que se trata de una identidad de AWS con políticas de permisos que determinan lo que la identidad puede hacer y lo que no en AWS. No obstante, en lugar de asociarse exclusivamente a una persona, la intención es que cualquier usuario pueda asumir un rol que necesite. Además, un rol no tiene asociadas credenciales a largo plazo estándar, como una contraseña o claves de acceso. En su lugar, cuando se asume un rol, este proporciona credenciales de seguridad temporales para la sesión de rol.



ACADEMIA CONSULTEC

AWS IAM
Security

- Políticas en passwords; fuertes políticas de implementación, incrementan la seguridad de nuestra cuenta.
  - Configurar mínimo en longitud
  - Requerir específicos tipos de caracteres
    - mayusculas
    - minusculas
    - numeros
    - no alfanumericos
- Permitir a cada usuario rotar y actualizar su contraseña.
- Requerir a los usuarios cambiar su contraseña cada cierto tiempo (password expiration).
- Prevenir re-usar contraseñas
- Forzar la activación de Autenticación con Multifactor (MFA)
- Activar registros de eventos con CloudTrail (AWS API events)

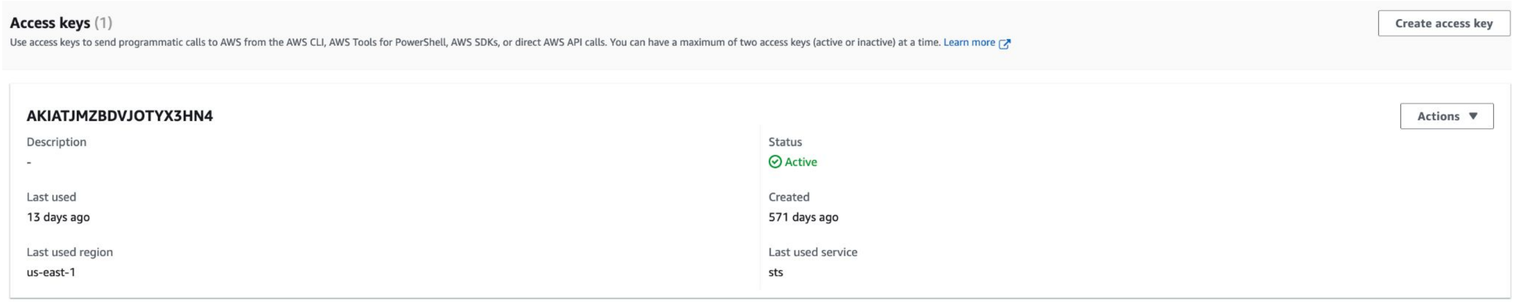
Google Authenticator
(phone only)

YubiKey by Yubico (3rd party)

ACADEMIA CONSULTEC

AWS IAM
¿Cómo accedemos en AWS?

- Tenemos tres opciones:
  - Consola Web (Contrasena y MFA)
  - Línea de comandos (AWS CLI - llaves de acceso + MFA)
  - Kit de desarrollo AWS (SDK - para usar en código)
- Las llaves de acceso son generadas en la consola
- Los usuarios pueden administrar sus llaves de acceso.
  - Son secretos, no se pueden compartir.
    - Access Key ID - Username
    - Secret Access Key - Contraseña



ACADEMIA CONSULTEC

AWS IAM
AWS CLI

- La interfaz de la línea de comandos de AWS (AWS CLI) es una herramienta unificada para administrar los servicios de AWS. Solo tendrá que descargar y configurar una única herramienta, para poder controlar varios servicios de AWS desde la línea de comandos y automatizarlos mediante scripts.
- La AWS CLI v2 ofrece varias funciones nuevas que incluyen instaladores mejorados, nuevas opciones de configuración como AWS IAM Identity Center (sucesor de AWS SSO) y varias funciones interactivas.

```
aws [options] <command> <subcommand> [parameters]
```

```
aws ec2 describe-regions
```

Output:


```
{
    "Regions": [
        {
            "Endpoint": "ec2.eu-north-1.amazonaws.com",
            "RegionName": "eu-north-1",
            "OptInStatus": "opt-in-not-required"
        },
        {
            "Endpoint": "ec2.ap-south-1.amazonaws.com",
            "RegionName": "ap-south-1",
            "OptInStatus": "opt-in-not-required"
        },
        {
            "Endpoint": "ec2.eu-west-3.amazonaws.com",
            "RegionName": "eu-west-3",
            "OptInStatus": "opt-in-not-required"
        },
```


ACADEMIA CONSULTEC

AWS IAM
AWS SDK

- Es el kit de desarrollo de software de AWS
- Set de librerías disponibles en los lenguajes de programación más usados, para acceder y administrar servicios AWS de manera programática.
- Embebido dentro de las aplicaciones, con soporte en:
  - Javascript, python, PHP, .NET, ruby, Java, Go, Node.js, C++, otros.
  - Mobile: Android/IOS
  - IoT - C y arduino
- Ejemplo: https://aws.amazon.com/es/sdk-for-python/


```
for i in ec2.instances.all():
    if i.state['Name'] == 'stopped':
        i.start()
```

ACADEMIA CONSULTEC

AWS IAM
Buenas Prácticas

- No usar la cuenta raíz, solo para la configuración inicial de cuentas.
- Una cuenta de usuario AWS para cada persona física.
- Asignar usuarios a grupos y políticas a grupos.
- Crear una política de contraseñas robusta.
- Usar y forzar el uso de MFA
- Crear y usar roles para dar acceso a servicios AWS
- Usar llaves para acceso programático (CLI/SDK)
- Auditar permisos frecuentemente con el IAM Credential Reports
- Nunca Compartir User y Llaves de acceso.

Ya Volvemos!
Un pequeño descanso.

Cloud Computing - AWS

ACADEMIA CONSULTEC

Contacto

achacon@consultec-ti.com

info@consultec-ti.com

@consulteclatam

@consultec-ti

consultec-ti.com

Gracias

¡Nos vemos pronto!