REGION

AZs

Cual y como elegir?

Compilance: Data Governance and legal requirements

Proximity: Latency services

Avaible services: New Services and new features aren't avaible in every regions

Pricing: Maybe, variable pricing between region. Ref Docs

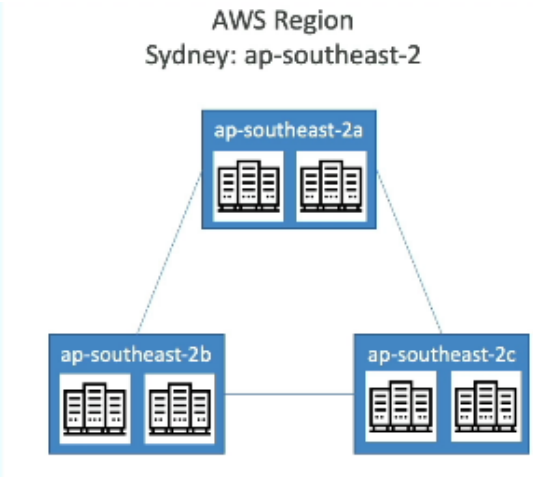
REGION

AZ -> Usually 3, min 3 , MAX 6

- Cada AZ , tiene mas de uno o mas datacenters con energia , conectividad y redes.

- Estan separados estrategicamente para evitar desastres

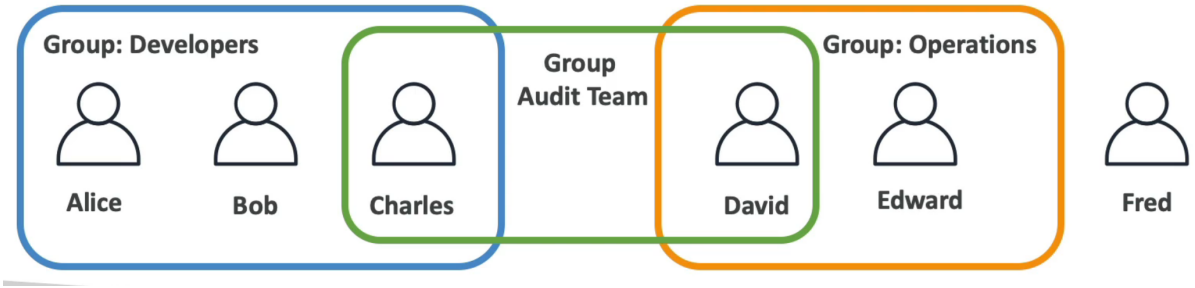
- Interconectados (Cada AZ de la region) con bandaancha de alto rendimiento y super baja latencia.



IAM

Users, people within my organization, and CAN BE GROUPED

Groups: ONLY CONTAIN USERS, not other groups.

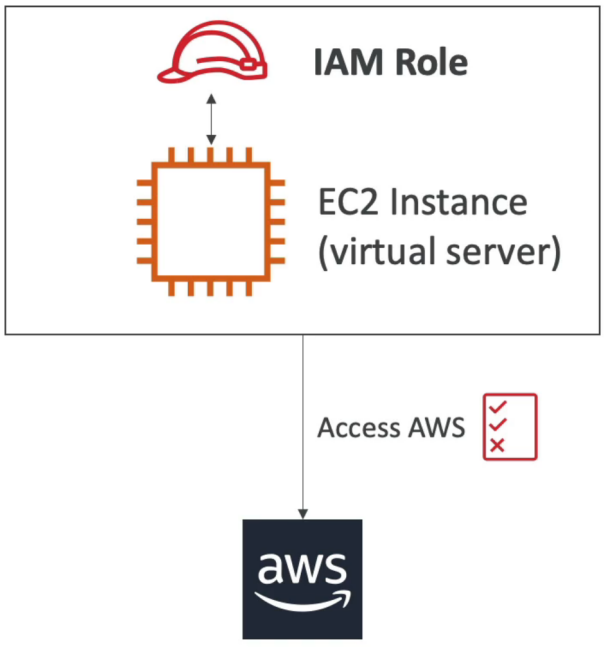


*Fred: No pertenece a ningun grupo, una mala practica, pero es posible en AWS.

Policies :Permisos defininos para usar recursos para cada grupo/usuario.
>>> Principio Min Privilegio <<<

- IAM es un servicio GLOBAL, si genera un user/politica, estara disponible en cualquier region.

ROLES: es la "interface" / "usuario" que se le asigna al servicio, donde se le asocia policies con los permisos necesarios para que el servicio cumpla su funcion.

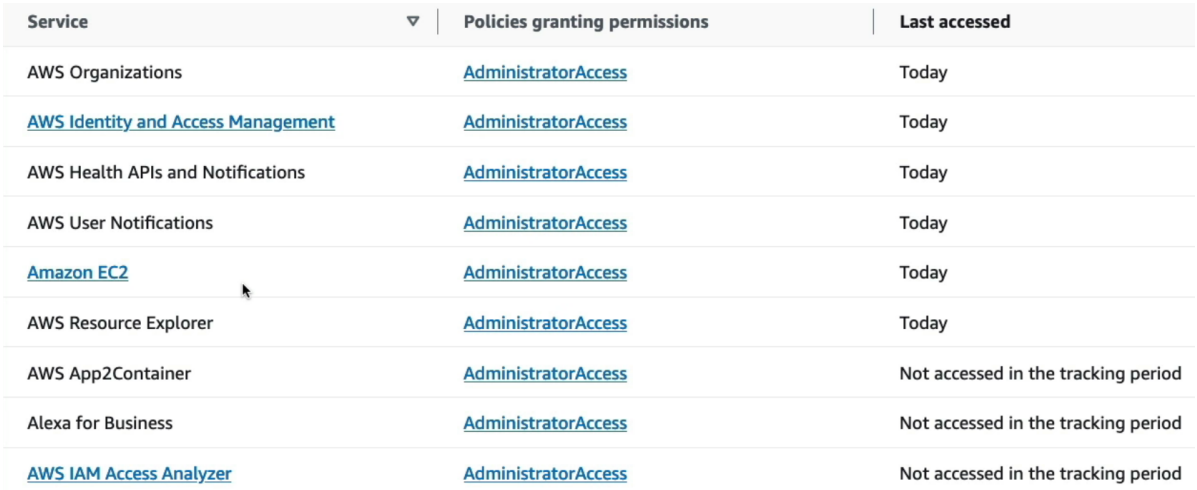


Herramientas para gestion del servicio IAM

1. Informe de Credenciales de IAM :
   Herramienta de seguridad a nivel de cuenta.
   Contiene información sobre todos los usuarios y el estado de sus credenciales.
   Útil para auditar y gestionar las credenciales en la cuenta.

2. IAM Access Advisor :

   - Herramienta de seguridad a nivel de usuario.
   - Muestra los permisos de servicio otorgados a un usuario y cuándo se accedió a esos servicios por última vez.
   - Ayuda a aplicar el principio de privilegio mínimo , permitiendo identificar y eliminar permisos no utilizados, reduciendo así el acceso innecesario.



Service	Policies granting permissions	Last accessed
AWS Organizations	AdministratorAccess	Today
AWS Identity and Access Management	AdministratorAccess	Today
AWS Health APIs and Notifications	AdministratorAccess	Today
AWS User Notifications	AdministratorAccess	Today
Amazon EC2	AdministratorAccess	Today
AWS Resource Explorer	AdministratorAccess	Today
AWS App2Container	AdministratorAccess	Not accessed in the tracking period
Alexa for Business	AdministratorAccess	Not accessed in the tracking period
AWS IAM Access Analyzer	AdministratorAccess	Not accessed in the tracking period

Buenas Practicas IAM

1. Evitar el uso de la cuenta root :
   - Utiliza la cuenta root solo para configurar tu cuenta AWS.
   - Crea cuentas personales separadas para el día a día.

2. Un usuario de AWS = Un usuario físico :
   - No compartas tus credenciales con otros.
   - Si alguien más necesita acceso, crea un usuario adicional para ellos.

3. Gestión de usuarios y grupos :
   - Asigna usuarios a grupos y gestiona permisos a nivel de grupo para simplificar la administración de seguridad.

4. Política de contraseñas seguras :
   - Implementa una política robusta para garantizar que las contraseñas sean seguras.

5. Autenticación multifactor (MFA) :
   - Usa MFA para añadir una capa extra de seguridad y proteger tu cuenta contra accesos no autorizados.

RESUMEN

1. Usuarios IAM :
   - Asigna un usuario IAM a una persona real.
   - Cada usuario tiene una contraseña para la consola de AWS.

2. Grupos y Políticas :
   - Agrupa usuarios para simplificar la gestión.
   - Adjunta políticas (JSON) a usuarios o grupos para definir permisos.

3. Roles :
   - Usa roles para otorgar permisos a servicios de AWS (como EC2) sin compartir credenciales.

4. Seguridad :
   - Activa MFA (autenticación multifactor) para mayor seguridad.
   - Establece una política de contraseñas seguras .

5. CLI/SDK :
   - Usa la CLI o SDK para gestionar AWS mediante programación.
   - Genera claves de acceso para CLI/SDK y manténlas seguras.

6. Auditoría :
   - Usa el Informe de Credenciales IAM para auditar credenciales.
   - Utiliza IAM Access Advisor para revisar permisos y su uso reciente.

EC2 Fundamentals

¿Qué es EC2? :

- EC2 (Elastic Compute Cloud) es un servicio de Infraestructura como Servicio (IaaS) en AWS.
- Permite alquilar instancias virtuales (máquinas virtuales) bajo demanda.

Componentes clave de EC2 :

- Instancias EC2 : Máquinas virtuales que puedes configurar y usar.
- Volúmenes EBS : Almacenamiento virtual para tus instancias.
- Balanceadores de carga : Distribuyen el tráfico entre instancias.
- Grupos de Autoescalado (ASG) : Escalan automáticamente tus recursos según la demanda.

Configuración de una instancia EC2 :

- Sistema operativo : Linux, Windows o Mac OS.
- CPU, RAM y almacenamiento : Elige según tus necesidades.
- Red : Configura IPs públicas y tarjetas de red rápidas.
- Firewall : Usa grupos de seguridad para controlar el acceso.
- Bootstrap : Script que se ejecuta al arrancar la instancia para automatizar configuraciones iniciales.

BootTasks (User Data) EC2 :

- Se ejecuta una vez durante el primer arranque con permisos de root .
- Automatiza tareas como instalación de software, actualizaciones, descargas, etc.

Tipos de instancias EC2 :

Ejemplos:

- t2.micro : 1 vCPU, 1 GB RAM, bajo rendimiento de red (parte de la capa gratuita de AWS).
- t2.xlarge : 4 vCPU, 16 GB RAM, rendimiento moderado.
- c5d.4xlarge : 16 vCPU, 32 GB RAM, almacenamiento NVMe SSD, alto rendimiento de red.

Capa gratuita de AWS :

- Puedes usar t2.micro gratis hasta 750 horas/mes durante un año.

Instance	vCPU	Mem (GiB)	Storage	Network Performance	EBS Bandwidth (Mbps)
t2.micro	1	1	EBS-Only	Low to Moderate	
t2.xlarge	4	16	EBS-Only	Moderate	
c5d.4xlarge	16	32	1 x 400 NVMe SSD	Up to 10 Gbps	4,750
r5.16xlarge	64	512	EBS Only	20 Gbps	13,600
m5.8xlarge	32	128	EBS Only	10 Gbps	6,800

t2.micro is part of the AWS free tier (up to 750 hours per month)

Instancia EC2 :

- Es una máquina virtual en la nube que puedes configurar y usar para ejecutar aplicaciones.
- Se lanza desde una AMI (Amazon Machine Image) , que es una plantilla preconfigurada con un sistem

Configuración Inicial :

- Nombre y Etiquetas : Asigna un nombre a tu instancia (ej., "Mi Primera Instancia").
- AMI : Usa imágenes como Amazon Linux 2 (compatible con la capa gratuita).
- Tipo de Instancia : Elige t2.micro (1 vCPU, 1 GB RAM) para aprovechar la capa gratuita.
- Claves SSH : Crea un par de claves (.pem o .ppk) para acceder a la instancia de forma segura.

Grupo de Seguridad :

- Controla el tráfico de entrada y salida.
- Configura reglas para permitir:
  - SSH (puerto 22) : Acceso remoto.
  - HTTP (puerto 80) : Para servidores web.

- La IP pública puede cambiar al detener e iniciar la instancia, pero la IP privada permanece igual.

Almacenamiento :

- Usa volúmenes EBS (Elastic Block Store) para almacenamiento persistente.
- Configura un volumen raíz (por defecto, 8 GB en la capa gratuita).
- Activa la opción "Eliminar al Terminar" si deseas que el volumen se elimine junto con la instancia.

Datos de Usuario (Bootstrap) :

- Permite ejecutar scripts al lanzar la instancia por primera vez.
- Ejemplo: Actualizar el sistema, instalar un servidor web (HTTPD) y crear un archivo HTML básico.

Acceso y Funcionamiento :

- Usa la IP pública para acceder a la instancia desde internet.
- Asegúrate de usar http:// en lugar de https:// para acceder al servidor web.
- Si la instancia se detiene, la IP pública puede cambiar; verifica la nueva dirección.

Estados de la Instancia :

- En ejecución : La instancia está activa y consumiendo recursos.
- Detenida : No se factura por la instancia, pero el almacenamiento sigue existiendo.
- Terminada : La instancia y sus recursos asociados se eliminan permanentemente.

Beneficios de EC2 :

- Escalabilidad: Lanza múltiples instancias rápidamente.
- Flexibilidad: Personaliza el tipo de instancia según tus necesidades.
- Ahorro de costos: Usa la capa gratuita (t2.micro) para aprender y experimentar.

Conceptos Adicionales :

- Capa gratuita de AWS : Ofrece hasta 750 horas/mes de uso de t2.micro durante el primer año.
- Servidor Web : Puedes configurar un servidor básico con un mensaje "Hola Mundo" usando scripts en los Datos de Usuario.

Tipos de Instancias EC2 :
- AWS ofrece diferentes tipos de instancias EC2 optimizadas para diversos casos de uso.
- Las categorías principales son:
  - Propósito General ,
  - Computación Optimizada ,
  - Memoria Optimizada ,
  - y Almacenamiento Optimizado .

Convención de Nomenclatura :
Ejemplo: m5.2xlarge
m : Clase de instancia (Propósito General).
5 : Generación de la instancia.
2xlarge : Tamaño de la instancia (mayor tamaño = más CPU y memoria).

Categorías de Instancias :
Propósito General :
- Equilibrio entre CPU, memoria y red.
- Ideal para servidores web y aplicaciones generales.
- Ejemplo: t2.micro (capa gratuita).

Computación Optimizada :
Optimizadas para tareas intensivas en CPU.
Usadas en transcodificación de medios, aprendizaje automático, juegos, etc.
Ejemplo: Familia C (c5, c6).

Memoria Optimizada :
Enfocadas en aplicaciones que requieren mucha RAM.
Ideales para bases de datos en memoria, caché, y análisis de datos.
Ejemplo: Familia R (r5), X (alta memoria).

Almacenamiento Optimizado :
Diseñadas para acceso rápido a grandes volúmenes de datos almacenados localmente.
Usadas en bases de datos OLTP, sistemas de archivos distribuidos, etc.
Ejemplo: Familias I, G, H.

Comparación de Tipos de Instancias :
Ejemplo: t2.micro vs. r5.16xlarge vs. c5d.4xlarge.
t2.micro: 1 vCPU, 1 GB RAM (bajo costo, capa gratuita).
r5.16xlarge: 16 vCPU, 512 GB RAM (memoria intensiva).
c5d.4xlarge: 16 vCPU, 32 GB RAM (CPU intensiva).

Capa Gratuita de AWS :
t2.micro es parte de la capa gratuita, con hasta 750 horas/mes disponibles.

¿Qué son los Grupos de Seguridad? :

- Actúan como firewalls para controlar el tráfico de red entrante y saliente de las instancias EC2.
- Contienen reglas de permiso que especifican qué tráfico está permitido (entrada y salida).
- Pueden referenciar direcciones IP o otros grupos de seguridad .

Funcionamiento Básico :

- Entrada : Define qué tráfico externo puede llegar a la instancia (por ejemplo, acceso SSH, HTTP).
- Salida : Por defecto, todo el tráfico saliente está permitido.
- Si el tráfico está bloqueado por el grupo de seguridad, la instancia ni siquiera lo "ve".

Ejemplo Práctico :

- Una regla típica permite tráfico SSH (puerto 22) desde una dirección IP específica.
- Otra regla permite tráfico HTTP (puerto 80) desde cualquier IP (0.0.0.0/0).

Características Importantes :

- Asociación múltiple : Un grupo de seguridad puede adjuntarse a múltiples instancias, y una instancia puede tener múltiples grupos de seguridad.
- Ámbito regional : Los grupos de seguridad están vinculados a una región y VPC específicas.
- Fuera de la instancia : No es una aplicación dentro de la instancia; es un firewall externo.

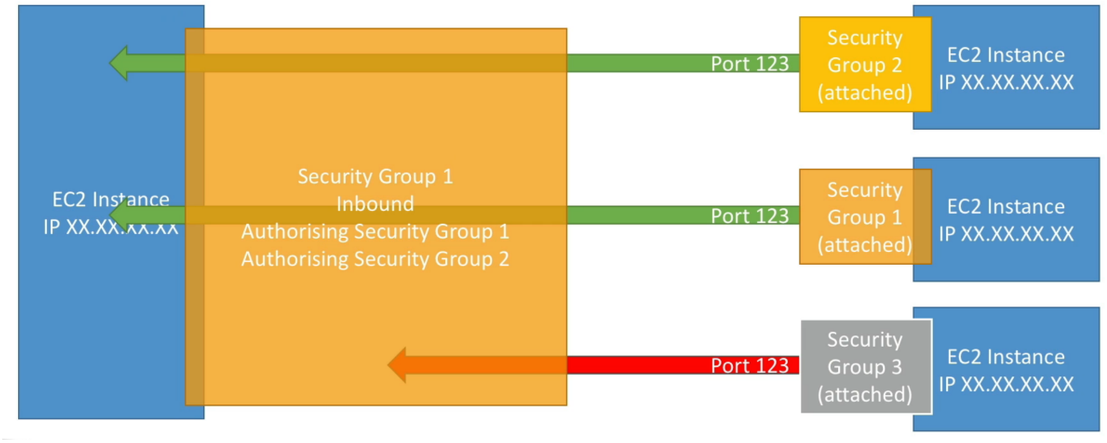
Consejos Prácticos :

- Mantén un grupo de seguridad separado solo para SSH para mayor seguridad.
- Si hay problemas de conectividad:
  Tiempo de espera : Probablemente un problema del grupo de seguridad.
  Conexión denegada : El tráfico llegó a la instancia, pero la aplicación falló.

Reglas de Referencia entre Grupos de Seguridad :

- Puedes autorizar tráfico entre instancias basándote en sus grupos de seguridad (útil con balanceadores de carga).

Ejemplo: Si una instancia tiene el "Grupo 1" y otra el "Grupo 2", puedes permitir que se comuniquen directamente sin preocuparte por IPs.



Puertos Clave para el Examen AWS :

22 : SSH (acceso seguro a instancias Linux).
21 : FTP (transferencia de archivos no segura).
22 : SFTP (transferencia de archivos segura usando SSH).
80 : HTTP (sitios web no seguros).
443 : HTTPS (sitios web seguros).
3389 : RDP (acceso remoto a instancias Windows).

Comportamiento por Defecto :

Entrada : Todo el tráfico está bloqueado a menos que se especifique lo contrario.
Salida : Todo el tráfico está permitido a menos que se restrinja.