IAM AND AWS CLI

AKIAR2VVJX67ADEZ7LGI

zuY5MSq8wwbE/JqmNht4VX/EIENaLEStS2UqABxR

aws iam list-access-keys

aws iam list-users

IAM ROLES FOR SERVICES

Some services will need to perform actions on your behalf, to do so, we will assign permissions to aws services with **IAM Roles.**

**Common roles:**

EC2 instance roles.

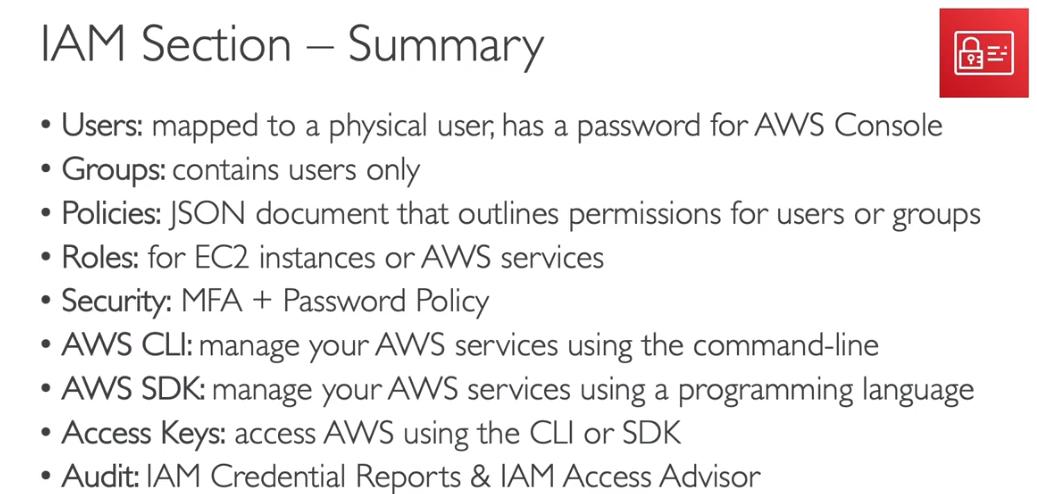
Lambda function roles.

Roles for CloudFormation.

IAM CREDENTIAL REPORTS shows IAM users and status of their credentials (mfa,last pas change, etc).

ACCESS ADVISOR

Help to identify what services are being user by a user and what services no. It shows Last access details.



EC2 FUNDAMENTALS

AWS BUDGETS track cost monthly, control cost, receive alerts.

AMAZON EC2 IaaS

Renting virtual machine EC2

Storing data on virtual drive EBS

Distributing load across machines ELB

Scaling the services using an auto-scaling group ASG

**EC2 instance types:**

General purpose, diversity for workloads such web servers or code repositories.

Compute optimized, intensive task that need high performance.

Memory optimized, fast performance for workloads that process large data sets in memory.

Storage optimized, intensive task requires high read and write access.

**Security groups**

Works like a firewall.

Locked down to a region, if you switch you need to create a new security group in that region.

By default, all inbound traffic is blocked.

By default, all outbound traffic is authorized.

Referencia de grupo de seguridad, regla que permite el tráfico de otro grupo de seguridad.

**Iam role**

Accediendo a una instancia EC2 a través de una instancia si queremos acceder a iam list-users no podremos hacerlo a menos que aws configure nuestras keys pero eso seria peligroso. Lo ideal es attachar un IAM role a la instancia que contenga una política de readonly.

**EC2 instance purchasing options**

On demand,

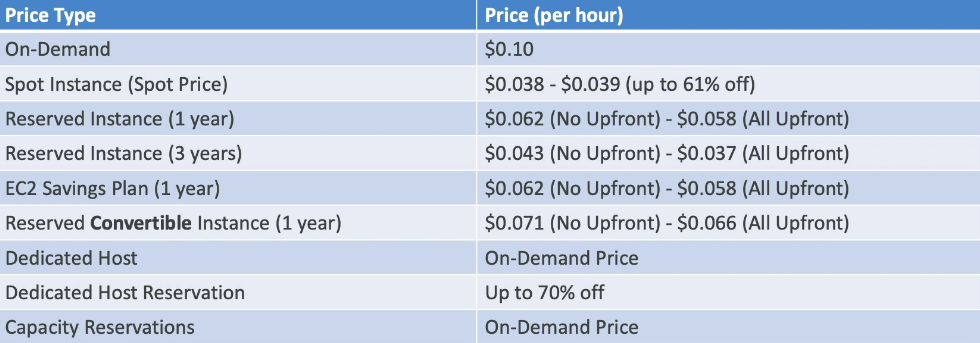
Reserved,

Savings plans.

Spot instances,

Dedicated hosts,

Capacity reservations,



ELASTIC IP ofrece una IP fija, puede obtener hasta 5 por account. Se tiene que adjuntar rápido porque estando sin adjuntar va cobrando.

PLACEMENT GROUPS

Cluster Todas las instancias en una misma AZ, high performance.

Spread Hasta 7 instancias por AZ placement group.

Partition hasta 7 partitions per AZ en la misma región. Hasta 100s de EC2 instancias.

EC2 SOLUTIONS ARCHITECT LEVEL

**ELASTIC NETWORK INTERFACE** Es como una tarjeta de red virtual.

**-**Disponible para cada AZ.

-Asociar a instancias en cualquier momento.

- Se puede asociar a grupos de seguridad.

-Conexión a VPC.

EC2 HIBERNATE Es como hinbernar una computadora.

Inicio más rápido.

RAM menor a 150GB.

Root volumen, must be EBS, encrypted.

Disponible en instancias on demand, reserved y Spot.

No se puede hinbernar más de 60 dias.

EC2 INSTANCE STORAGE

EBS(Elastic block store)

* It’s a network drive.
* Locked in one AZ. (practitioner level)
* Have a provisioned capcity.

By default EBS creation no deletion but creation through instance by default it going to be deleted after instance terminated.

EBS snapshot

* Snapshots is like backup.
* Can copy across az or region

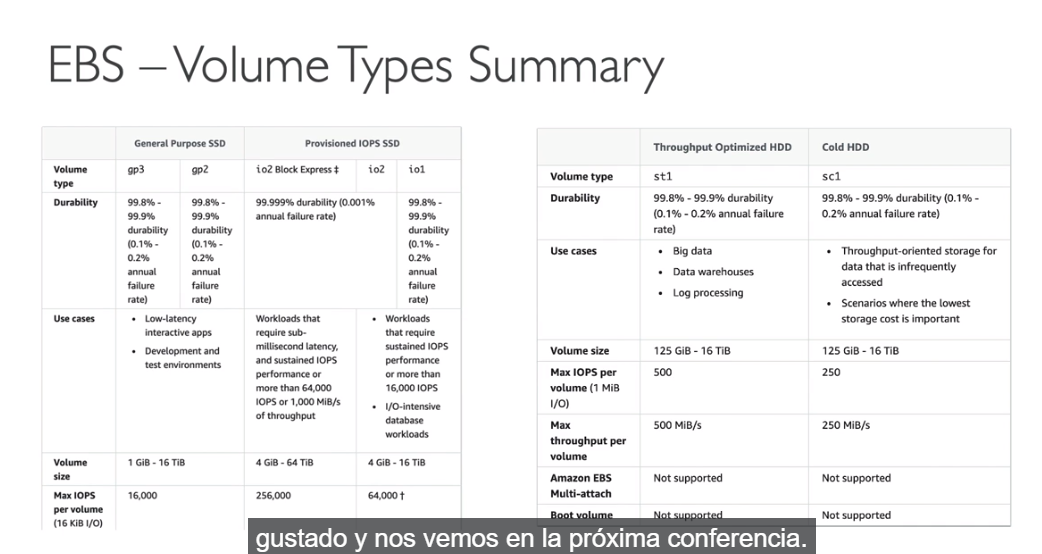
Features:

* EBS Snapshot archive
* Recycle bin for EBS snapshot
* Fast Snapshot Restore (FSR)

AMI (Amazon machine image)

* AMI public provided by amazon.
* Your own AMI you make.
* AMI Marketplace provided by someone else.

EBS VOLUME TYPES



EBS MULTI ATTACH – io1/io2 family

* Attach the same EBS volume to multiple instances in the same AZ.
* Only available for volumes EBS IO1 e IO2.
* Up to 16 instances at a time.
* Must use a file system that’s cluster-aware.

Amazon EFS Elastic file system

* EFS works with EC2 instances in multi AZ.
* Like managed Networks file system can mounted on many EC2.
* Autoscaling.
* Pay for each GB, pay for use.

HIGH AVAILABILITY AND SCABILITY: ELB & ASG

* Vertical scaling: Increase instances size
* Horizontal scaling: Increase number of instances. (Autoscaling group, load balancer)
* High availability: Run instances for the same application across multi AZ (Autoscaling group multi AZ, Load balance multi AZ)

Elastic load balancer

* Servers that forward traffic to multiple servers (eg instances)
* Expose single point of access (DNS) to your application.
* Provide SSL termination (HTTPS) for your websites.
* High availability across zones
* Separate public traffic from private traffic.
* It is a managed load balancer.
* AWS guarantees it will be working, takes care of upgrades and provides few configurations knobs.

Types of ELB

* **Application load balancer**
* **Network load balancer**
* **Gateway load balancer.**

**Application load balancer v2**

Layer 7 HTTP

Load balancing to multiple HTTP applications across machines (target groups).

Load balancing to multiple applications on the same machine (ex:containers).

Support for HTTP/2 and WebSocket.

Supoort redirects (from HTTP to HTTPS for example).

Network load balancer

* Layer 4.
* Forward TCP & UDP traffic yo your instances.
* Handle millions of requests per seconds,
* Less latency -100ms (vs 400 ms for ALB)
* NLB has one static IP per AZ and support Elastic IP.
* Used for extreme performance.

Target groups:

* EC2
* IP addresses (private Ips)
* I could be front an ALB.

Gateway load balancer

* Layer 3
* Deploy, scale and manage a fleet of 3erd party networks virtual appliances in AWS.
* Example: Firewall, IDS, etc.
* Combines two functions:
  + Transparent network gateway (single entry/exit for all traffic)
  + Load balancer (distributes traffic you your virtual appliance)

ELB Sticky sessions

* Used to redirect the user to the same instance behind a load balancer.
* It works for Classic load balancer, ALB, NLB.
* It works with cookies.
  + Application-base cookies (The following cookie names are reserved by the ELB (AWSALB, AWSALBAPP, AWSALBTG)).
  + Duration-based cookies

Cross-zone load balancing

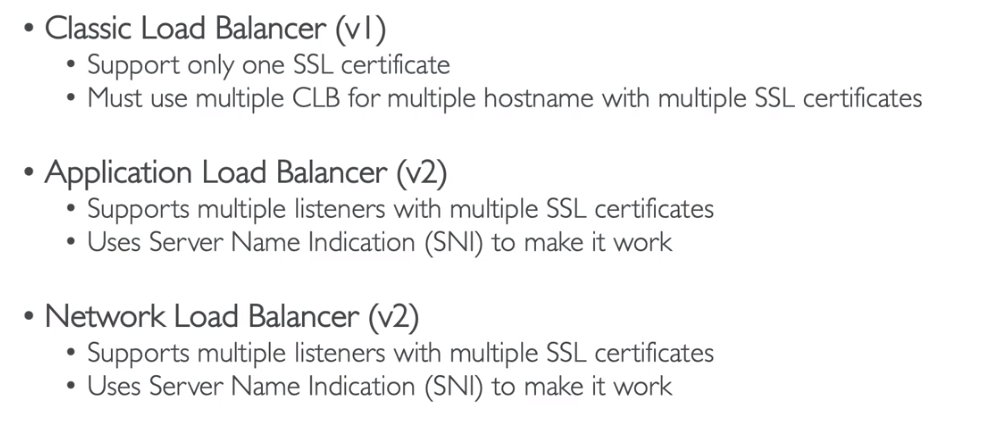
Distribuye el tráfico a través de todas las instancias de forma igual. Se puede habilitar.

SSL/TLS – Basics

Traffic in transit encrypted.

Load balancer – SSL certificates

* The load balancer uses an X.509 certificate (SSL/TLS server certificate)
* You can manage certificates using ACM (AWS Certificate Manager).
* You can create upload your own certificate alternatively.



Auto scaling groups