IAM

- Users, Groups (users heritage its policies), Roles (for aws resources) and Policies (json)
- Global
- Root Account (never use it) + MFA
- By default new users have no permissions
    - Programmatic access
    - AWS Management console access
- IAM password policy
- Roles:
    - AWS Service Role - The usual one, and the one we are interested in
    - AWS service-linked role: for Alexa
    - Role for cross-account access: allow IAM users to access to another AWS accounts
    - Role for identity provider access: grant access from Cognito, or OpenID (facebook, google, amazon), SAML, etc

S3

- Key-Value Object Storage. Files from 0 byte to 5TB. Unlimited storage
- S3 buckets: universal namespace. Default: max 100 buckets/account
- Read after write for PUTs of new objects
- Eventual consistency for overwrite PUTS and DELETES

S3 object consists on:

- Key: nombre del fichero
- Value: el contenido del fichero (secuencia de bytes)
- Version ID
- Metadata
- Subresources
- Access Control List

S3 tiers

- **S3 standard**: Objeto mínimo 0 bytes
- **S3 IA**: accedes 1 vez al mes (o cada 6 meses). Pero necesitas acceso rápido
    - Objeto mínimo 128Kb. Es la opción más barata de S3
- **RRS**: para ficheros que puedes permitirte perder. Thumbnails
- **Glacier**: para archivar. Tardas de 3 a 5h en recurarar un fichero
    - Restauras via S3 API o via la consola de AWS.

	Standard	Standard - Infrequent Access	Reduced Redundancy Storage
Durability	99.999999999%	99.999999999%	99.99%
Availability	99.99%	99.9%	99.99%
Concurrent facility fault tolerance	2	2	1

Bucket URL formats:
http://s3-<region>.amazonaws.com/<bucket> o http://<bucket>.s3-<region>.amazonaws.com

Versioning

- No puede deshabilitarse, solo suspenderse
- Cada update es un fichero por sí mismo, con su propio ID
- Eliminar un fichero es marcarlo (**delete marker**) como eliminado > desaparece del bucket, no del histórico > Sólo el propietario del bucket puede eliminarlos de verdad
- Puedes habilitar MFA para los deletes

Cross region replication (CRR)

- Require "**versioning**" habilitado.
    - Permite subconjuntos via prefijos. Tb replica metadatos y ACL
- Al subir algo nuevo (o update) al bucket, se replica a otro bucket (en otra región) – tb requiere **versioning** pero acepta otro tipo de S3 (IA, RRS…). Requiere IAM roles.

Lifecicle & Glacier

- Sin versioning
    - **30 días de S3 > IA** (sólo para objetos mayores de 128KB)
    - **30 días de IA > Glacier**
- Con versioning
    - Tengo 2 LC, uno para el objeto actual y otro para las versiones antiguas

S3 Security & Encryption

- Por defecto los buckets son privados
- Control de acceso via bucket policies (aplica a todos los objetos) o ACL
- Puedes habilitar logging > lo guarda en otro bucket
- Encryption
    - In transit (SSL/HTTPS) – SSL/HTTP endpoints using HTTS protocol
    - At rest
        - Server Side Encryption (SSE)
            - S3 Managed Keys (SSE-S3). Amazon se encarga de todo.
            - AWS Key Management Service (SSE-KMS) **Permite Audit Trail**
            - Customer Provided Keys (SSE-C): Tú controlas las claves
        - Client Side Encryption

S3 Transfer Acceleration

- Usa las edge locations de CloudFront para subir los datos desde el más cercano a ti
    - Coste adicional. Debes usar la URL proporcionada para esas transferencias

S3 Static Website Hosting

- Si usas Route53 con S3, el nombre del bucket debe ser el del dominio (sin el ".com")
- **http://<bucketname>.s3-website-<region>.amazonaws.com**
- Puedes especificar index/error pages y redirect rules

CloudFront

- Edge location: caché, TTL (default 24h), puedes habilitar la escritura/update en edge locations que updatean el origin
    - Puedes elegir "Allowed HTTP methods" (GET, HEAD, PUT, DELETE…)
- Origin (permite múltiples orígenes para la misma distribution)
    - S3 bucket: puedes restringir el bucket para que sólo se pueda acceder desde el CDN -> Origin Access Identity
    - EC2 instance
    - ELB
    - Route53
    - Fuera de AWS
- Distribution
    - Web distribution: para websites
    - RTMP: media streaming

S3 multipart upload API > abort or failed uploads via lifecycle policies. Puede usarse con tx acc

- Recommended for files > 100MB

Storage Gateway
- VM que instalas en tu datacenter y replica a S3.
- 3 tipos
    - **Gateway Storage Volumes**: tus datos en local, SGW replica a S3 (bkp)
    - **Gateway Cached Volumes**: tus datos en S3, SGW sirve de caché local
    - **Gateway Virtual Tape Library** (VTL): reemplaza los bkps en cinta > usa S3

Import/Export
- Actualmente reemplazado por Snowball. Permite:
- Exportar desde S3
- Importar a S3, Glacier y EBS

Snowball
- Importar/Exportar hacia/desde S3.
- Snowball: Petabyte scale data transport solution
- Snowball edge: + compute cababilities. i.e gather data during a flight
- Snowmobile: el camión. Exabyte scale

EC2

Pricing
- On demand
- Reserved: 1 or 3 years. Predictable usage or Reserved Capacity
- Spot: flexible start/end, only feasible at low prices, urgent compute needs
    - Si la termina AWS, no pagas por esa fracción de hora
- Dedicated hosts: Por hora o Reserved. Licencias o for Regulatory Requirements

Types
- Dr Mc Gift Px

EBS (Elastic Block Storage)
- General Purpose SSD (gp2). 3iops/GiB max 10K iops
- Provisioned iops SSD (io1). Por si necesitas más de 10K iops (hasta 20K)
- Throughtput optimized HDD (ST1). Frequent Access. Large amount of data in sequence as Data warehousing, log processing. Cannot boot
- Cold HDD (SC1). Less frequent access. Typical: fileserver. Cannot boot
- Magnetic (Standard). Infrequent access, lowest cost
- Por defecto: root volumen terminated al terminar la instancia
- Los volúmenes deben estar en la AZ de la instancia que los quiere usar
    - EBS guarda copias redundantes dentro de la misma AZ

EBS: upgrading volumes (cambiar tamaño o tipo)
- BEST PRACTICE: parar instancia, dettach, hacer snapshot, crear new volumen, attach.
- EBS pueden updatearse on the fly (excepto magnetic standard)
    - Sólo un cambio en 6 horas
- El tamaño sólo puede incrementarse (incluso desde snapshot)

RAID & EBS
- Aumentar iops = Raid 0 (stripped) o 10
- **Application Consistent Snapshots**:
    - Necesita 1) parar escrituras a disco desde la aplicación 2) flush caché
    - 3 métodos para hacer esto:
        - Freeze the filesystem
        - Unmount the RAID array
        - (BEST OPTION) Parar la instancia, tomar snapshot, iniciar instancia

EBS Snapshots:
- Puedo: Crear Volumen, AMI, copiarlo a otra región y/o crear una copia “cifrada”
- No puedo eliminar un snapshot usado por una AMI (creada a partir de él)
- Los snapshots se almacenan en S3, y son incrementales (allow point-in-time recover)

Encrypt Root device volume and create AMI

- No puedo crear un snapshot cifrado de un volumen no cifrado
- Los snapshots hechos de volúmenes cifrados, están cifrados automáticamente
- Los volúmenes restaurados desde snapshot cifrados, están cifrados automáticamente
- Sólo puedes compartir AMIs NO cifradas (con otras cuentas AWS o públicamente)
- Las AMIs son “por región” pero puedo copiarlas

EBS root vs instance (ephemeral) storage

- Si el root device es EBS, éste creó lanza desde una AMI creada de un snapshot EBS
- Si es instance store, éste se creó desde una AMI creada desde un template en S3 (slow)
- Las instancias con instance storage no se pueden parar (si el host falla, la info se pierde)
- Puedes escoger no terminatar los EBS root volumes, pero NO los instance storage.
- No puedes desatachar el root EBS sin parar la instancia, claro

Security Groups

- Por defecto: inbound denied, outbound allowed
- Cambios applicados immediatamente
- Son stateful: crean reglas (no visible) para el tráfico relacionado

ALB/ELB y Healthchecks -> self-sanitazion of instances

- Tienen su propio security group
- LB asociado a una VPC. Puede (debe) trabajar en varias AZ
- No tienen IP, sólo un DNS record
- Cross-Zone enabled = Balancea entre instancias, independientemente de las AZ
- ELB (capa 4)
    - No permiten instancias creadas desde Amazon DevPay site
    - SSL Termination: has de instalar el certificado en el ELB
    - Puedes loggear la actividad con CloudTrail
- ALB (capa 7) + Barato
    - Internet facing o internal
    - Routing > target groups = path based routing! (ie. /a > target1, /b > target2)
    - Healthcheck opcionalmente puede checkear el HTTP success code
    - Parar SSL termination en las instancias

CloudWatch for EC2

- Default metrics on EC2 instances: CPU, disk, Network, Instance status
- Standard monitoring (5min) vs detailed (1min)
- Dashboards, alarms, events (responde a cambios en los recursos de AWS) and logs (requiere un agente instalado en la instancia. Permiten agregar y almacenar logs)
- Cloudwatch (monitoring y logging) VS CloudTrial (para auditar)
- Tipos de alarma: OK, Alarm, insuficient-data

Userdata & Metadata

- Bootstrap scripts: user data section (max 16KB)
- Instance Metadata: http://169.254.169.254/latest/meta-data/

Launch configuration & ASG

- Launch configuration: plantilla con la creación de imágenes
- ASG: size, VPC y subnets donde crear las instancias, ELB, Healthcheck (ELB o EC2)
    - + Scaling Policies: min/max & increase/decrease when…
    - termination: selects AZ with most instances > delete the one using the oldest lc
    - cooldown: seconds after another scaling event can happen

EC2 termination protection deshabilitado por defecto

EC2 Placement groups

- Grupo lógico de instancias que necesitan **low latency** y/o **high network throughtput**
    - 10Gbps. Misma AZ
- El nombre del PG debe ser único en tu cuenta AWS
- Sólo para cierto tipo de instancias (cpu, ram, storage y gpu)
- No puedes juntar PG. Tampoco mover una instancia de un PG a otro.

EFS

- Soporta NFSv4 y miles de conexiones simultáneas
- Petabytes. Data stored in multiple AZ in a región
- **Read after write consistency**
- Tiene su propio sg para cada punto de montaje = subnet = AZ
- Puede almacenar datos de una bbdd (al igual que EBS)

Lambda

- Puedes usarlo:
    - Event-drive compute service: en respuesta a eventos
    - En respuesta a HTTP requests via API Gateway
- Lenguajes: Java, NodeJS, Python, C#
- Triggers:
    - API Gateway
    - IoT
    - Alexa
    - CloudFront
    - CloudWatch
    - CodeCommit
    - Cognito
    - DynamoDB
    - Kinesis
    - S3
    - SNS
- Máxima duración 5 min
- Las ejecuciones son independientes
- Escala horizontalmente (scale out) automáticamente

API Gateway

- Publish, maintain, monitor and secure APIs to EC2 or Lambda
- You can enable API caching to cache (for a TTL) the API response
  You can throttle (estrangular) API GW to prevent attacks
- You can log results to CloudWatch
- CORS (Cross-Origin Resource Sharing) > permite servir contenido de un dominio diferente al original

Route53

- ELB do not have IPv4, you resolve to them via DNS name
- Understand Alias (you can resolve individual AWS resources) vs CNAME
- Routing policies:
    - Simple (default): round robin
    - Weighted: A/B
    - Latency: lowest network latency (ms) to a region > latency
    - Failover: active/passive setup -> healthchecks
    - Geolocation: latency & show a geo-customized web
- Default limit of 50 domain names (can be increase contacting support)

Databases

RDS for OLTP

- Have to select instance type, EBS size (max 6TB/16TB for SSD), VPC, etc.
  - SQL Express max 300GB disk size
- **Backups**: Automated (enable 1 by default 1-35 days) VS Database snapshots > impact performance! -> Backup window (changes to it applied immediately)
  - Automatic backups are deleted when terminate (only latest snap could be)
- **Encryption** only at creation time!!! Not even from snapshots (I think)
- **Multi-AZ**: only for disaster recovery. Does not improve performance. AWS Handles failover -> Sync replication
- **Read Replica**: Read performance. Requires auto backups on. Max 5, same AZ. Async
  - Available for MySQL and PostgreSQL engines
- Permite aplicar particionado de tablas para usar varias instancias RDS
- Aurora: 5x faster than MySQL
  - Maintains 2 copies of physical data in 3 AZ (min 6 copies)
    - Can fail 2 for writes, 3 for reads
  - 2 Types of replica: Aurora (max 15, fault tolerance) & MySQL Read Replicas

DynamoDB – NoSQL

- Really scalable (no downtimes!), fast (SSD) and flexible
- Spread across 3 data centers
- Eventual Consistent Reads (if you can wait 1 second)
- vs Strong Consistent Reads (if you can't) -> increases cost
- Very cheap for reads
- Provisioned capacity = ios per table
- Exists an option for Cross Region Replication

Redshift for OLAP (& BI)

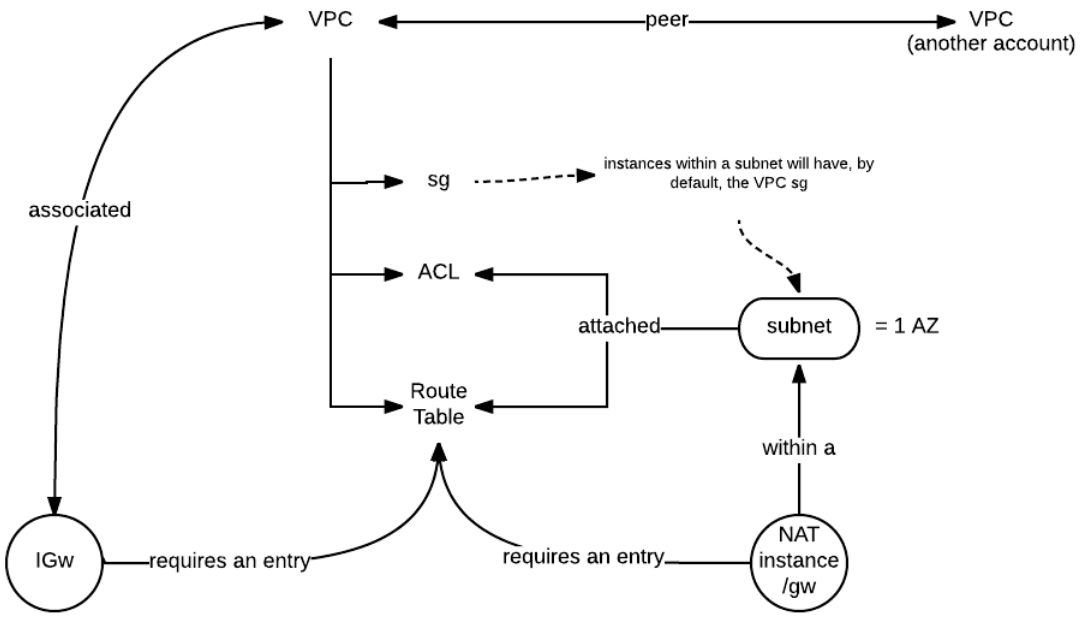
- Single node (160G)
- vs Multi-node, consists on
  - Leader Node
  - up to 128 Compute Nodes
- Fast because
  - Columnar data storage (block size = 1MB)
  - Advanced compression (by columns)
  - Massive Parallel Processing (MPP) across all nodes

Elasticcache

- Memcached and Redis

SSD better performance than magmetic for DBs in EC2 instances
RDS troubleshooting > look for "error nodes" in XML RDS API response

VPC



VPC

- Private datacenter
- Max 1 IGW per VPC. After created, detached
  - Route table has to have a route through IGW
- VPC peering, even with another AWS accounts (NO TRANSITIVE PEERING)
  - IP ranges cannot overlap!!
- Custom VPC creates
  - Default ACL > all denied by default
  - Default SG
  - Main Route Table > allow local (private) connections > so by default, all subnets within the VPC can communicate to each other
- By default, max 5 VPCs per region
- Instances in default VPC will have public and private IP
- VPC endpoints to access to AWS resources
- VPC Flow logs: capture traffic within the VPC and sends it to CloudWatch

Subnet

- 1 subnet = 1AZ
- Only can be attached to 1 ACL, and associated to 1 Route Table
- Public means the route table where is associated has an IGw, and its instances has a public IP

NAT

  - To allow instances within a private subnet to reach internet (for yum, i.e.)
  - Be placed in a **public subnet** (so with an IGw attached)
  - Needs an entry in the route table associated with the private subnet
- Nat instance is just a regular EC2 instance with a specific AMI
  - Needs a public IP
  - Needs disable “source/destination check”
  - HA via ASG, multiple subnets and a script to automate failover
  - Throughtput depends on instance type
- Nat GW
  - Scale automatically up to 10Gbps, across a single AZ

ACLS

Sg	ACL
Instance level (1st)	Subnet level (2nd)
Allow rules	Allow/Deny
Stateful	Stateless
All rules evaluated before deciding	FW: Rules in asc order > first match
Only applies to the instance if attached	Applies to all instances in the subnet

- Ephemeral ports for outbound connections (1024-65535)
- Your VPC automatically have a default ACL, with by default all inbount/outbount traffic is enabled
- But when you create your custom network ACL, all inbount/outbount traffic is denied

Application Services

SQS: pull. queue. message oriented API
- Simple Queue Service: Pull queue message system
- To **decouple** your components < EXAM!!
- Message size 256KB any format (text, json, xml)
- Messages in queue from 1min to 14 days. Default 4 days
- **Visibility timeout**: tiempo que tiene un consumer para procesar el mensaje (max 12h)
    - Si da timeout, el mensaje vuelve a la cola > Puede duplicarse!
- **Long Polling**: en lugar de preguntar cada X seg si hay mensajes, preguntas y te avisa al entrar mensajes, o cuando de el long poll timeout (ReceiveMessageWaitTimeSeconds>0)
- 2 tipos: default (**puede haber duplicados, no en orden**) y fifo

SWF: task oriented API
- Simple Workflow Service. Can include **human interaction**
- **Workflows max 1 year**
- **A task is assigned only once, never duplicated, and in order**
- SWF tracks all events. With SQS you have to implement your app-level tracking
- Parameters in JSON
- "Domains" are a collection of related workflows.
    - Includes "workflow starters", "deciders" and "activity workers".

SNS: push. message oriented API
- Simple Notification Message: publish-subscribe service
- **mobile push notifications, Email/Email-JSON, SMS, SQS or Lambda**
- **SNS topics**: access points for clients to allow to subscribe to notifications (also HTTP(S))
- Data format in JSON

Elastic Transcoder: media converter

Kinesis
- Stream: consists on **shards**. **Data retained** max 7 days (default 1)
    - Producer > Shards within the stream > Consumers
- Firehouse: no shards, streams or consumers. Data send to S3. **Optional Lambda** analysis
    - Producer > Firehouse (optional Lambda) > S3
- Analytics: encima de Streams/Firehouse añade SQL analytics

Withepapers: Security

Shared security model
- AWS is responsible for the security config of its **managed services** products (DynamoDB, RDS, Redshift, EMR, WorkSpaces, etc.) and the underlaying infra
- YOU: IAAS (EC2, VPC, S3) are under your control
- YOU are responsible for account & user access.
    - Recommend MFA, SSL/TLS for communications and CloudTrial for user activity logging

Storage Decommissioning
- AWS uses DoD 5220.22 (National Industrial Security Media Sanitization) or NIST 800-88 (Guideless for Media Sanitization) to destroy data.
- Magnetic storage devices are physically destroyed

Network Security
- You can connect to AWS via HTTP or HTTPS using SSL
- VPC allows to use IPSec VPNs to tunnel between AWS and your datacenter
- AWS network is segregated from the Amazon Corporate (.com) network

Network Monitoring & Protection
- By default, AWS provides protection for
    - DDoS
    - Man in the middle
    - IP Spoofing: the AWS host-based firewall will not allow instances to send traffic with a source IP or MAC other than its own.
    - Port Scanning
    - Packet Sniffing by other tenants (inquilinos)
- Unauthorized port/vulnerability scans by EC2 users are a violation of AWS Acceptable Use Policy. You may request permission before!

AWS Credentials
- Passwords
- MFA
- Access Key
- Key Pairs: SSH login to EC2. Cloudfront signed URLs
- X.509 Certificates: SSL certificates for HTTPS/ SOAP-based requests to AWS API

Trusted Advisor
- Inspects your AWS environment and makes recommendations to
    - Save money
    - Improve performance
    - Close security gaps
    - Fault Tolerance
- Provides alerts of common security misconfigurations

Instance Isolation
- Instances running on the same box, are isolated from each other via the Xen hypervisor.
    - AWS firewall in the hypervisor layer between physical and EC2 NICs
- Physical RAM is separated using similar mechanisms
    - Memory allocated to guest is scrubbed (set to zero) when unallocated.
- Instances have no raw access to disk, but a virtual disk.
    - AWS automatically resets (disk zeroing) every customer's block of storage

Other considerations

- Gest OS:
  - virtual instances are completely controlled by you. No backdoors for AWS!
  - good security practice: EBS volumes and snapshots encrypted with AES-256
- ELB: Supports SSL Termination on the LB > intances can identify the source IP address
- Direct Connect: dedicated connection from your datacenter to your AWS VPC, using 802.1q VLAN standard, allowing you to connect to AWS public resources (S3) and private ones (EC2 in a private subnet)

Exam feedback

Virtualization types

- Paravirtual (PV)
- Hardware Virtual Machine (HVM)
  - Better performance
  - Can take advantadge on hardware extensions and run in top of hw

AD

- Directory Service's AD Connector: let's you connect your existing AD to AWS
- Simple AD: inexpensive AD compatible with the common AD features
- You can authenticate with AD to AWS using SAML
  - Authenticate to AD first, then to STS

AWS Organization & Consolidation Billing

- Account Management service to manage multiple AWS accounts from a central location
- Consolidated billing: 1 billing-only account. Up to 20 linked accounts. Global discounts

Resource Groups & Tagging

- Groups resources that share one or more tags

Security Token Services (STS)

- Federation (tipically AD) – means join groups –
  - Uses SAML
  - Allows users to login to AWS without IAM credentials (but AD)
- Federation with Mobile Apps
  - Uses Fb, Google, OpenID lo login
- Cross Account Access

Workspaces

- VDIs. Are persistent.
- Runs Win7. By default users are local admins (allow to install applications)
- All data on D: is backed up every 12h

ECS

- ECR: EC2 Container Registry
- ECS Tasks definitions are JSON files describing one or more containers that conform your application (include CPI, RAM, links, etc)
- ECS service is like ASG using Task Definitions
- Clusters (region specific) are logical groups of container instances to place tasks in
- Service Scheduler: ensures a specific number of tasks is constantly running (ELB reg)
- Custom Scheduler: third party
- ECS Agent (docker agent)
- EC2 uses IAM roles to access ECS (Security groups still at host (EC2) level)
- ECS tasks uses IAM roles to access services and resources

More info:
https://acloud.guru/forums/aws-certified-solutions-architect-associate/discussion/-KSDNs4nfg5ikp6yBN9l/exam_feedback

Extra

- 44 AZ, 17 regions
    - AZ names are assigned randomly per account!!!
- For new AWS accounts > max 20 EC2 instances per region
- 4 support levels: basic, developer, business, enterprise
- Por defecto, max 5 EIP por región > las EIP estarán atachadas a la instancia hasta que explícitamente las detaches (no se detachan si la instancia se para)
- CloudTrail permite registrar el histórico de llamadas a la API de AWS
- AWS Config permite guardar el histórico de cambios en las configuraciones de recursos de AWS > y enviar notificaciones de cambios via SNS
- 1GIB <= EBS size <= 16TiB
- RPO (Recovery Point Objective): datos que estoy dispuesto a perder (ej. 1h)
  RTO (Recovery Time Objective): tiempo en volver a dar servicio (ej. 20j)

EXAM QUESTIONS

- for sure: 1 subnet = 1AZ -> you cannot spread 1 subnet across AZ
- NO VPC Transitive peering: if A – B – C, A cannot talk with C throught A. You have to create a peer between A and C.