Cloud Practioner

Introduction:

You only pay want you use. AWS follow.

Client Server Architecture → in which shopkeeper Morgan is a server and the customers are the clients. You have to only pay what you need.

Cloud Computing →

- On demand delivery of resources over the internet.
  Pay as you go pricing.
- On demand delivery of IT resources and applications through internet with pay-as-you go pricing

Compute in Cloud

Hypervisor is responsible for the sharing the underlying physical resources of the host machine between the virtual machine.
This idea of sharing resources is known as Multitenancy. Hypervisor is responsible for the multitenancy

You can also scale up your instances in terms of processors or memory.
It is done by.

1. Vertical scaling →

(Caas) Compute as a service.

Instance types:

Availability Zone → Run across at the least two Availability Zones in a Region.

Module 5 :

Storage and Databases :

Instance store and (EBS) : Block storage :

* Instance store :
  - Temporary block level storage for an EC2 instance.
  - When instance terminated, data lossed.

* Amazon Elastic Block store (EBS) :
  - Provide block level storage volumes that you can use with EC2 instance.
  - If you stop or terminate EC2 instance the data remains available in attached EBS volume.
  - For incremental backups the EC2 creates the snapshots of the data

Amazon Simple store Service (S3) : (Object storage)

- In object storage, each object consist of data, metadata and key.
- The data might be an image, video, text document, or any other type of file.

(i) Recall that when you modify a file in block storage, only the pieces that changed are updated. When a file in object storage is modified, the entire object is updated.

* Amazon Simple storage Service (S3) →
  - Provide the object level storage.
  - S3 store data in buckets.
  - S3 provide unlimited storage space for backups.
  - The maximum file size of an object is 5 TB in S3.
  - You can also set permissions to control visibility and access in S3.
  - You can also use S3 versioning to track changes to your object over time.

* Amazon S3 Storage classes :

You can select from a range of storage classes to select a fit for your business and cost needs. Two factors:
- How often you plan to retrieve your data.
- How available you need your data to be.

1) Amazon S3 Standard :-
- Designed for frequently accessed data
- Stores data in a minimum of three Availability Zone.
- Provide high availability.
- But has higher cost than other storage classes
- Good choice for wide range of use cases such as website, content distribution and data analytics.

2.) Amazon S3 Standard Infrequent Access (S3 IA) :-
- Ideal for infrequent accessed data
- Similar to S3 Standard but has lower storage price and higher retrieval price.
- Also store data in minimum three AZs.

3.) Amazon S3 one zone - IA :-
- Store data in single AZs.
- Has a lower price than Amazon S3 Standard IA.
- It saves cost on storage.
- You can easily reproduce your data in the event of AZs failure.

4.) S3 Intelligent Tiering →
5. S3 Glacier Instant Retrieval → Instant Retrieval in milliseconds
6.) " " Flexible " → in minutes or hour
7.) " " Deep Archive " → 12 hours to 48 hours
8. Amazon outposts. → Get the S3 storage on your on premises storage.

EBS	S3
1. Size up to 16 TiB	1. Unlimited storage
2. Survive termination of their EC2 instance	2. Individual object up To 5000 GB (5TB)
3. solid state by default	3. Write once / read many
4. HDD option	4. 99.999999999% durability
use case :- 80 GB video file to and you have to change edit some part of that video. - Block storage store in blocks so engine can only make edit on the specific blocks and not need to update the whole file.	use case :- Face recognition in which several images of animal are seen by several people. Secure S3 bucket - Versioning enabled - Regionally distributed - Data GC - Offer cost savings - Serverless

EFS elastic File System :>

- multiple users can access data that is stored in shared file folder.
- It is use in case in which a large number of servers and resources need to access the data at the same time.

EFS →
- is a scalable File system.
- As you add files it grow and shrink automatically

EBS	EFS
1. An Amazon EBS volume stores data in a single AZs.	1. EFS is a regional service. It stores data in multiple AZs
2. To attach an EC2 instance to an EBS volume, both must reside with same AZs.	2. The duplicate storage enables you to access data concurrently from all AZs in the Region where a file system is located. Additionally, on premises servers can access EFS using AWS DirectAccess

Module 1 :

Cloud computing :

Deployment models :

1) Cloud Based Deployment → a) Run all parts of app in cloud. b) Migrate existing app to cloud. c) Design and build new app on cloud.

2) On premises Deployment :
- Private cloud
- Deploy resources by using virtualization and resource management tool.

3) Hybrid Deployment →
- Connect cloud based resources to on premises infrastructure
- Integrate cloud based resources with legacy IT applications

Benefits of cloud

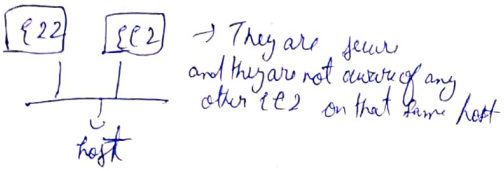
1. Trade upfront expense for variable expense →
Variable expense means you only pay for computing resource you consume.
2. Stop spending money to run and maintain data centers
3. Stop guessing capacity :
4) Benefits from massive economies of scale : scale of cloud computing help you to have lost
pay as you go prices means pay only for what you use. So economies of scale lower the pay as you go pricing. The aggregated cloud usage from a large no of customers result in lower pay as you go prices.
5) Speed and agility →
agility means ability to deploy, test application on cloud.

Module 2 : Compute in Cloud :

* EC2 supports vertical scaling.

Launch → Connect → Use

Multitenancy → Sharing underlying hardware between virtual machines.
Hypervisor is responsible for virtualization and coordinated the multitenancy



→ They are secure and they are not aware of any other EC2 on that same host

* Types of EC2 :

1.) General purpose instance :
- Balance of compute, memory, network resources.

2.) Compute optimized instance → For high performance processor
- Also for batch processing workloads.

3.) Memory optimized instances → RAM
- Deliver fast performance of workloads.
- Best for high performance database or a workload that involves performing real time processing of a large amount of unstructured data.

4.) Accelerated computing instances →
- use Hardware accelerator, coprocessor
- For floating points number calculation, graphics application processing and data pattern matching.

5.) Storage optimized instances →
- Require for high read and write access to large datasets on local storage.
- For Distributed file systems, data warehousing applications and high frequency online transaction processing (OLTP) system.

* EC2 pricing =>

1. On demand Instances →
- Ideal for short term, irregular workloads that cannot be interrupted.
- Pay only as you use.
- For developing and testing application.

2.) EC2 saving plans →
- Reduce cost by committing to a consistent amount of usage for 1 - 3 years term.
  It saves 72% over on Demand costs.

3.) Reserved Instance →
- Purchase standard Reserve and convertible Reserved Instances for 1 and 3 years.

4.) Spot Instance →
- Have start and end times, or that can withstand interruption.
- It save 90% off on Demand prices.

5. Dedicated Hosts →
- Fully dedicated servers for the customer use.
- License maintenance
- It is more expensive.

Scaling Amazon EC2 →

- Dynamic scaling → responds to changing demand
- Predictive scaling → schedules the right number of EC2 instance based on predicted demand.

Vertically → By resizing the instance
Horizontally → By launching new instances in addition to the pool.

Load Balancer works on Horizontal scaling

For scaling you have to define minimum, desired and maximum capacity of EC2 instances

Messaging and Queuing →

Tightly coupled, Monolithic application → If one component fail, other also fail
Publish, subscribe service → SNS (Simple Notification Service)

Loosely coupled, If one fail whole component doesn't fail
without losing messages, Send message in queue
User retrieve message from queue, read it and delete → SQS (Simple Queue Service)

Serverless computing :

AWS Lambda :

(Scaling can apply on it)

- No need to manage the underlying servers
- No need to provision the servers
- Pay only for the compute time.

1. Upload code to Lambda → 2. Set trigger from an event source → 3. Lambda runs your code only when triggered. 4. Pay only for compute time.

containerized application :-

ECS →

- Help to run and scale containerized application.
- ECS support Docker. Docker is a software platform that enable you to build, test and deploy application quickly.

EKS :-

- Help to run kubernetes on AWS.
- Used to Manage containerized application at scale.

All Summary VIMP

AWS Fargate →

- Serverless compute engine for containers.
- Works for both ECS and EKS

Server less on AWS

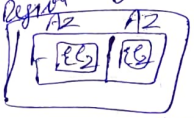
Module 3 ⇒ Global Infrastructure and Reliability :

AWS Regions ⇒ Selection Region four (business) factors should be considered :

1. **Compliance** → If specific region then select region within that area.
2. **Proximity** ⇒ Near to your customer. Depending on customer location, then choose the region according to customer or near to customer.
3. **Available service within a Region** →
4. **Pricing** → Choose region according your budget.

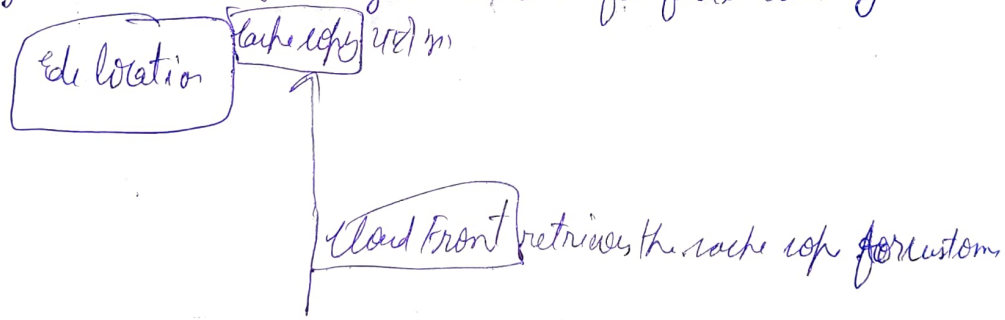
- Regions are geographically isolated areas
- Region contain AZs

Availability Zone → It is a single or more data centres saves from disaster. Run your EC2 at least two availability zone



Edge location → (Content) Delivery Network (CDN) ⇒ CloudFront (AWS named it)

- Edge locations runs CloudFront. CloudFront is a content delivery service.
- It is a site that Amazon CloudFront uses to store cached copies of your content closer to your customer for faster delivery.



Edge location are seprated from regions.

Edge location also runs DNS (Domain Nam servers) known as Amazon Route 53 helps direct the customers to correct web locations with reliably low latency

Outpost ⇒ When a customer wants AWS services in his own building. AWS install mini region in your own data centre owned fully by AWS but isolated in your own building.

Ways to Interact with AWS services / How to provision AWS resources

AWS Management Console → Call API

AWS Command Line Interface → ~~Call API~~ save time by calling command again and again

Software Development Kit → To save time

AWS Manage Tools :- (Automated and Repeated Deployment)

1) AWS Beanstalk → You can provide your application code and desired configuration to the AWS Elastic Beanstalk. When then take your information and built your application environment for you. It also save the configuration Environment so that they can be deploy again easily. It works for EC2 instances
- Adjust capacity, Load Balancer, Automatic scaling, Application health monitoring.

2) AWS Cloud Formation → It is a Infrastructure as code tool used to define a wide variety of AWS resources in a declared way using JSON and YAML text based document called cloud formation templates.

It is works of also in ~~You have to provide code~~
- Storage
- Database
- Analytics
- Machine learning

Template → Cloud Formation → Provision the Resources

We can use that Cloud Formation in different regions and accounts and it create identical environment across them.

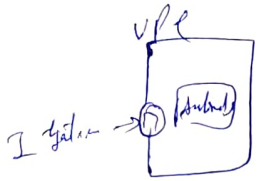
Less human errors because it is automated process.

Module - 4 Networking

Amazon Virtual Privat. Cloud (VPC) :-

- Establish boundaries around your AWS resources.
- It enables you to provision an isolated section of AWS cloud.
- In isolated section you can launch resources in a virtual network that you define.
- Within VPC you can organize your resources into subnets.

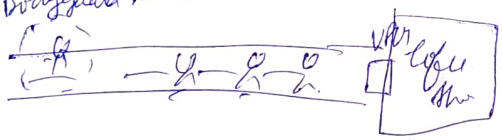
Internet Gateway :- To allow public traffic from the internet to your VPC, you attach an Internet Gateway (IGW).



Virtual Private Gateway :- The VPG is the component that allows protected internet traffic to enter into the VPC.

- A virtual private gateway enables you to establish a virtual private network (VPN) connection between your VPC and a private network.
- A virtual private gateway allow traffic into VPC only if it is coming from an approved network.

Analogy like VPN



AWS Direct Connect :-

- Dedicated private connection between your data center and VPC.

Eg private hallway directly links to coffee shop which allow only that building people to travel through it to the coffee shop without needing to ~~share~~ use the public road shared with other customers

---

Subnets :-

- Section of VPC in which you can group resources based on security or operational needs. It can be public or private.

Public and Private subnets can communicate with each other.

VPC component that checks package permission for subnets is a Network Access Control List (ACL) & stateless packet filtering

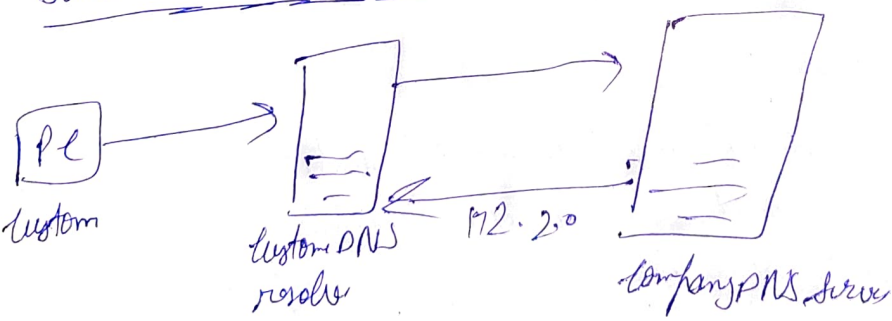
- It is a virtual firewall.
- By default all inbound and outbound traffic is allowed
- But in custom all outbound, inbound are deny. All network ACLs has an explicit deny rule

The component that check packet permission for an EC2 instance is a security group & stateful packet filtering

- It is a virtual firewall.
- By default security group denies all inbound traffic and allow all outbound traffic.
- If you have multiple EC2 instance within a subnet, you can associate them the same security group or use different security group for each instance

Global Networking :

Domain Name System (DNS) :



Amazon Route 53 :

- DNS web service
- Give a reliable way to developers and business to route end user to internet application hosted in AWS.
- It connects user request to infrastructure running in AWS.
- It also manages the DNS records for domain name.
- You can register new domains names directly in Route 53.

- This enable you to manage all your domain names within a single location.

How Route 53 and CloudFront works together:

1. A customer request data from the application by go to company.com
2. Amazon Route 53 uses DNS resolution to identify Any company.com's corresponding IP address. This information is sent back to the customer.
3. The customer's request is sent to the nearest edge location through CloudFront.
4. CloudFront connects to the Application Load Balancer, which sends the incoming packets to an Amazon EC2 instances.

Module 6. Security:

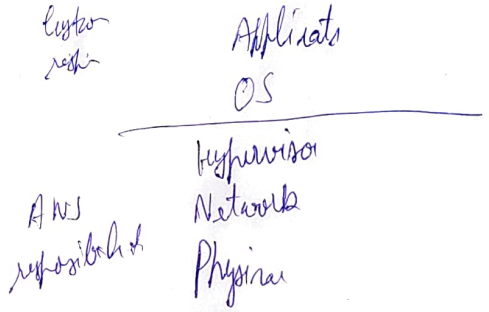
Shared responsibility model → AWS is responsible for some part and you are responsible for other part. This concept is shared responsibility model

Customer responsibility is → Security in the cloud.
AWS " is → Security of the cloud.

Customer responsibility → Platform, Application, Identity and Access Management, operating system, Network and firewall configuration.
Giving Access and Patch work of application

AWS responsibility → Compute, storage, Database, networking.

- Physical security of data centre
- Hardware and software infrastructure
- Network infrastructure
- Virtualization infrastructure



User permission and Access :

AWS Identity and Access Management :

- Enable you to manage access to AWS services

1. IAM Root user : owner, access to all the services.

- When you first create an AWS account, you begin with an identity known as root user.

2. IAM users :

- An IAM user is an identity you create in AWS
- By default when you create an IAM user in AWS, it has no permission.

3. IAM policy :

- An document that allows or denies permission to AWS services and resources.

Follow the principle of least privilege.

IAM group ⇒

- It is a collection of IAM users.
- When assign permission to group
- All group user have permission accordig granted in policy.

IAM role ⇒

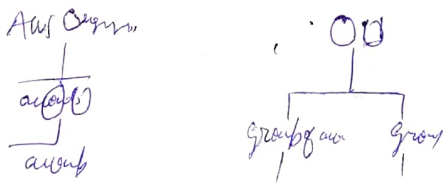
- It is an identity that you can assume to gain temporary access to permission.
- IAM role are idial for situation in which access to servic or resource needs to be granted temporarily, instead of long term.
- It switches to different in coffle step in a single day.
- But on access to ~~a~~ role at one time.

Multi factor Authentication ⇒

- It provide an extra layer of security for your AWS account.
- grand MFA to root user and IAM user.

AWS organization ⇒

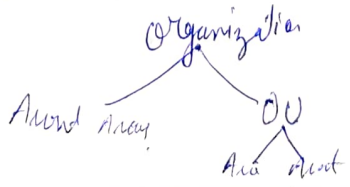
- When company has multiple AWS accounts. Then you can use AWS organizati. to consolidate and manage multiple account within a central location.
- It first create root, which is parent containe of all accounts.
- You can centrally control permission by using service control policies (SCP).



Consolidated billing

Organizational Unit ⇒

- In AWS organization, you can group accounts in OUs to make it easier to manage accounts with similar busines or security requirements
- When you apply a policy to an OU, all accounts in OU automatically inherit the permission specified to policy.



Module 12 Monitoring

Amazon CloudWatch →

- Service that enable to monitor and manage various metrics and configure alarm
- It use metrics to represent the data
- AWS send that metrics to CloudWatch.

CloudWatch Alarm → You can create alarm that automatically perform action when the value of your metrics has gone above or below a predefined threshold.

CloudWatch dashboard →
- Access all metrics from a single location.

AWS CloudTrail →

- Record API call for your account
- Record identity of API caller, time of API call, source IP address of API caller;
- You can ~~review~~ view a history of user activity and API calls for your application and resources.

Review details for user activities and API call

Updated within 15 minutes after an API call.

CloudTrail Insights :

- Allow CloudTrail to automatically detect unusual API ~~call~~ activities in your AWS account.

Key Point :
- Tracks user Activities and API request
- Filter logs to assist with operation analysis

AWS Trusted Advisor :

- Inspects your AWS environment and provide real time recommendation.

Five categories → cost optimization, performance, security, fault tolerance and service limits.

Module 6 ⇒ Continue

Compliance :

AWS Artifact ⇒ on demand

- Access to AWS security and compliance reports
- Select online Agreement

Review, accept, manage agreement with AWS

AWS Artifact Agreement ⇒

- Company use artifact agreement to sign an agreement with AWS.
- You can review, accept, manage agreement for an individual account or for all account in AWS organization.

AWS Artifact Report :- Information of responsibility of company.

DDOS ⇒ Distributed denial of service

- Multiple transistor call at coffee shop.
- It is difficult to block them all
- They make site unavailable.

DDoS :

- Make site flood with fuel of network traffic, make it unavailable for use

AWS Shield ⇒

- Protect application against DDOS. Two level protection

1. AWS shild standard : available

- Automatically protect all customer at no cost.

2. AWS shild Advance ⇒

- It is a paid service to detect and mitigate sophisticated DDoS Attack.
- It also intrent with other services like, Amazon cloud Front, Amazon Route 53 and Elastic load Balancer.
- You can also integrate AWS shield with AWS WAF (web Application Firewall) by writing custom rules.

Additional security services =>

AWS Key Management servic :

- Perform encryption operation through the use of cryptographic keys.
- A cryptographic is a random string of digit used for locking and unlocking data.

AWS WAF :

- Web App Firewall lets you monitor network request that comes into your web application
- It work with Amazon CloudFront and Load Balancer.

Amazon Inspector :

- To automate security assessment, vulnerability of new App Amazon Inspector is use.
- It improve security and compliance of application, check security vulnerabilities

Amazon Guard Duty :

- Provid intelligent threat detection
- continuously monitoring the network activity and account behaviour

Module 8 Pricing and Support :

AWS Free Tier :

1. Always Free → Do not expire
   DynamoDB → give 25 GB per month.

2. 12 months Free :

3. Trials → Amazon Inspector provide 90 days free trial
   Amazon Lightsail → 750 free hours over 30 day period.

How AWS pricing works)

1. Pay for what you use.
2. Pay less when you reserve → Lambda give 1 million requests & 3.2 million seconds of compute free.
3. Pay less with volume-based discounts when you use more

AWS pricing calculator → Give you estimate cost

AWS Budget :

- You can create budget.
- The information in AWS Budget update 3 times a day.
- You can also use custom alerts when your usage exceeds.

Cost Explorer :

- Helps you to visualize, understand, manage your AWS costs and usage over time.
- It also provides a report by default.

AWS support Plan:

Basic support:

- Free for all AWS customer.
- Include Access to whitepaper, documentation and support communities.
- You can also use AWS personal Health Dashboard.

Developer support ⇒

- Best practice guidance
- Client side diagnostic tools
- Building block architecture support, which consist guidance of for how to use AWS offering. Lower cost

Business support ⇒

- ALL AWS Trusted Advisor Checks.
- Limited support for third-party software, such as common OS and application stack component. Middle level cost

Enterprise On Ramp support ⇒

- Feature of all above support
- A pool of Technical Account Manager
- 30 minute for business critical use

Middle

Enterprise

- All feature of above
- 15 minutes or less response
- A designated Technical Account Manager.

Highest cost

TAM Technical Account Manager:

- Comes comes you take support of enterprise on Ramp, or Enterprise
- Education, empower, envole your cloud journey across the full range of AWS services.

Module-3 Migration

Cloud Adoption Framework :

Business Strategy :

- Business and IT strategy is in a business model that integrate IT strategy

People perspective ⇒

- Supports development of an organization wide change management strategy for successful cloud adoption.
- Evaluate organizational structures.

Governance perspective ⇒

- Focuses skill and process to align IT strategy with business strategy
- How to update the staff skill

Platform perspective ⇒

- Help to design, implement, optimize your AWS infrastructure

Security perspective ⇒

Security objective for visibility, auditability, control and agility.

Operation perspective ⇒

- Used to run, use, operate and recover IT workloads to the level agreed upon with your business stakeholders.

6R's of Migration strategy

1. Rehosting :
- Migrating the app without changes. Known as lift and shift

2. Replatforming :
- Known as lift, tinker, shift
- Make a few cloud optimizations to realize a tangible benefits.
- Optimization is achieved without changing the core architecture of the application.

3. Refactoring / Rearchitecting :
- used to add features, scale or performance, which would be difficult to achieve in application existing environment.

4. Repurchasing :
- Moving from a traditional license to software as a service model

5. Retaining :
- Keeping app that are critical for the business in the source environment

6. Retiring :
Process of removing app that are no longer needed.

Snow family :
- Collection of physical devices that help to physically transport upto exabytes of data into and out of AWS

1. AWS Snowcone :
- Small, rugged, secure edge computing and data transfer device.
- It feature 2CPU, 4GB of memory, 8 TB of usable storage.

AWS Snowball :

1. Snowball Storage optimized ⇒ used for large scale data migrations
   - Storage: 80 TB of harddisk, 1 TB of SATA solid state drive.
   - Compute: 40 vCPU, 80 GiB of memory to support

2. Snowball Edge Compute Optimized ⇒ Provide powerful computing for machine learning, full motion video analysis.
   - Storage: 42 TB of harddisk, 7.68 TB of SSD
   - Compute: 52 vCPU, 208 GiB of memory, Nvidia Tesla GPU100.

AWS Snowmobile ⇒

- Used to move large amounts of data to AWS
- Transfer upto 100 petabyte of data per snowmobile, pulled by semi trailer truck.

Interaction with AWS ⇒

Machine learning by sagemaker

Module - 10

Well Architected Framework:

- Help you to understand how to design and operate reliable, secure, efficient, cost effective system in the AWS cloud.

1. Operational excellence :-
   - Ability to run and monitor systems to deliver business value.
   - Design to perform operations as code, annotating documentation, anticipate failure, reversible changes.

2. Security :-
   - Protect information, system and assets.

3. Reliability :-
   - Recover from infrastructure or service disruption
   - Dynamically acquire computing resources to meet demand.
   - Mitigate disruptions such as misconfigurations or transient network issues

4. Performance efficiency :-
   - Ability to use computing resources efficiently to meet system requirements

5. Cost optimization :-
   - Run systems to deliver business value at lowest price point.
   - Cost optimization includes adopting a consumption model.

6. Sustainability :-

Benefits of cloud ⇒

Database ⇒

Relational Database Service ⇒

- Data relate to each other.
- RDS uses query lang (SQL)

- RDS is a service that enable you to run relational database in the AWS cloud.
- RDS automate the hardware provision, database setup, patching and bac

Amazon RDS database engine ⇒

- Amazon Aurora
- Postgre SQL
- MySQL
- Oracle
- ~~Dynamo DB~~ Maria DB
- Microsoft SQL Server.

- Amazon Aurora ⇒
  - Enterprise - class relational database.
  - compatible with MySQL and PostgreSQL.

5X MySQL
3X PostgreSQL