65 question 118 dollar 90 minites.
Northern Virginia region.
AWS Cloud

S3 - Dropbox.
→ Module 4 - Cloud architecting most important.
→ White paper.
→ 0 to 1024 are for http services.
→ Compliances program?
→ 1969 was the
* Cloud computing is the on demand delivery of computer power, database, storage, application and other IT resources through a cloud service platform via the internet with pay-as-you-go pricing.

* Cluster computing and Grid computing.

→ Cloud computing is used for content delivery, Enterprise IT, database, web hosting.

→ Cloud terminology :- High availability.
Fault tolerance
Scalibility.
Elasticity.

Adv1 → Capital Expense (Fees) and Variable expense (Pocket money).
Adv2 → Economics of Scale.
Adv3 → Eliminate guessing.
Adv4 → Speed and agility.
Stop wasting money spending money on data centers.
Adv5 → Go global.

Intro to cloud Economics:-

Three fundamental drivers of cost with AWS:-
- Compute.
- Storage.
- Outbound data transfer.

(In most of the cases) No charge:-
- Inbound data transfer
- Data transfer between services within the same region.

→ TCO - Total Cost of Ownership.

TCO consideration:-
- Server cost
- Storage cost
- Network cost
- IT labour Cost.

→ Reserved instance are available in AURI, NURI and PURI.

⇒ ~~AWS Global~~

→ Pay less when you reserve.
AURI, PURI and NURI

Benefits
- Minimize risk
- Predictably manage budgets
- comply with policies that require longer-term commitments.

→ AWS services for no additional charge:-
- Amazon VPC
- Amazon IAM
- Consolidated billing.

→ The general cost of doing business is reduced and saving are passed back to the customer, due to economies of scale

Date
Page

- AWS Elasting Beanstalk
- AWS Cloud formation
- Automatic Scaling
- AWS OPS work.

→ Global Cloud Front uses AWS Edge location to ensure low latency delivery.

→ AWS highly recommends provisioning your compute resources across multiple availability zone.

Module 2 AWS Core Services:-

Compute services
- Amazon Elastic compute Cloud (Amazon EC2)
- AWS Lambda:
  Fully managed serverless compute
- Auto-scaling:
- Elastic load balancer - distribute incoming traffic
  - help achieve higher level of fault tolerance.
- AWS Elastic Beanstalk - Paas that quickly deploys, scales and manages web app.s . No charge for Elastic Beanstalk.
- Amazon Lightsail
  Everything needed to jump start a project
  Manage simple web and app servers.
- Amazon (ECS) Elastic Containes service
- Aws Fargate.

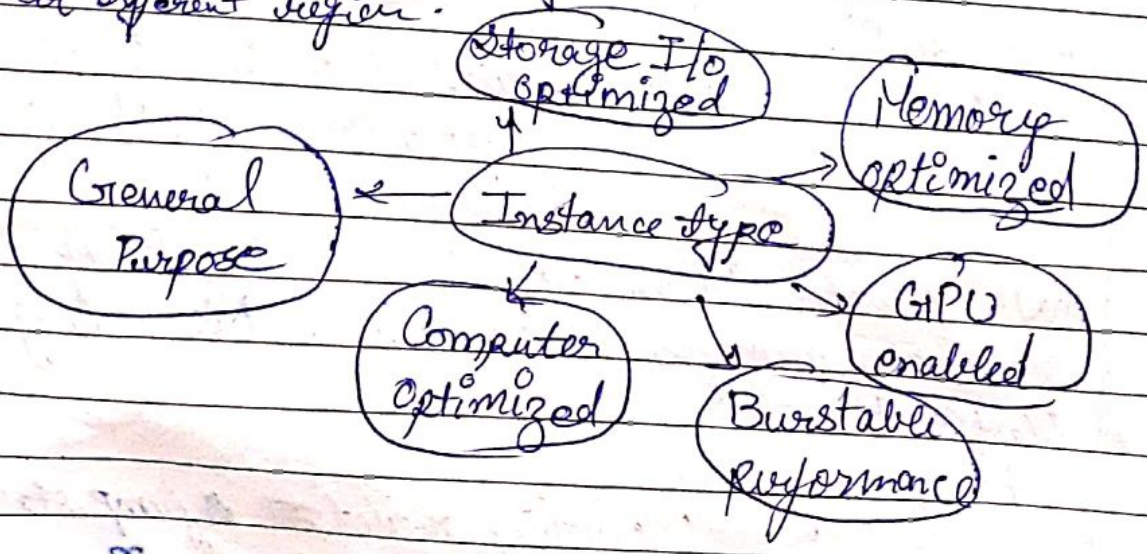
Amazon Elastic Container services for Kubernetes (EKS)

→ Choosing the right Amazon EC2 instance?
→ AWS uses intel Xeon processors, providing custom with high performance and value.

→ While choosing your instances consider:
- Core count
- Memory size
- Storage size and type
- Network performance
- CPU technologies.

→ AMI life cycle and uses.
- Create and register an AMI.
- Uses:
- Launch a new instance
- Copy within the same region or different region.

→



EC2 Pricing :-

On demand | Spot Instances | Reserved Instances

Dedicated host (Per-hour billing)
Per-second billing (Amazon Linux and Ubuntu only)
Per-hour billing (All other OSs)

Amazon EC2 instance types are optimized for different use-cases and workload requirement. They come in multiple sizes.

Billing and instance configuration

Instance configuration: Physical capacity of instance.
Pricing varies with:
AWS region
OS
Number of cores
Memory.

Amazon Cloudwatch to monitor instances:
- Basic monitoring (default, no additional cost)
- Detailed monitoring.
  - Fixed monthly rate for seven pre-selected metrics recorded once a minute.
  - Prorated partial months.

Auto Scaling:
automatically adjusts number of Amazon EC2 instances in your deployment.

- Incurs no additional charge beyond cloudwatch fees.

8. Elastic IP address.

* Spot instance Interruption.

→ An on demand instance specified in an EC2 fleet or spot fleet cannot be interrupted.

* Reasons for interuption :-
  - Price, Capacity and Constraints.

* Stoping interrupted spot instances.

Requirement :-
- For a spot instance request, the type must be persistent.
- For an EC2 fleet or spot fleet request, the type must be maintain.
- The root volume must be EBS volume, not an instance store volume.

+ The four pillars of cost optimization

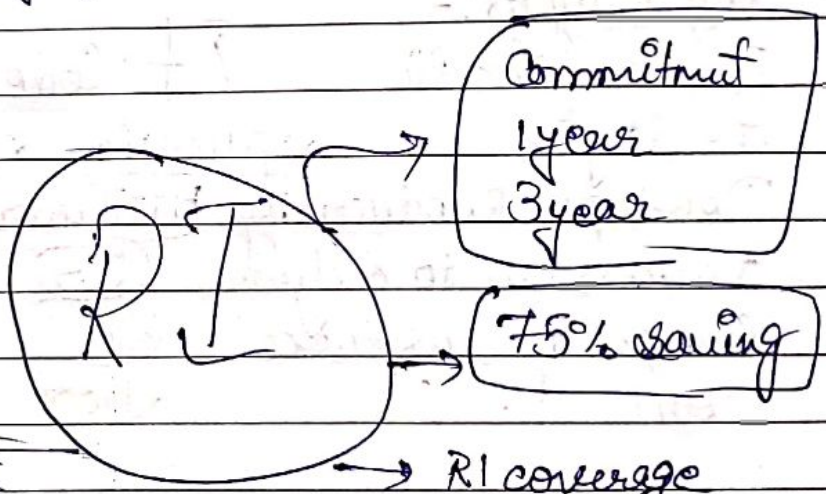
- Right sizing allows you to choose the right balance of instance types.
- Reserved Instances leverage reserved instances when you have long-term workloads with predictable usage patterns.
- Increase elasticity using auto scaling.

And monitor and improve by measuring and analyzing your system.

Right sizing :-

On demand	Reserved	Spot	Dedicated
- Pay by the hour - No long term commitments	- Pay upfront - 50-75% lower hourly rate.	Bid for unused Amazon EC2 capacity.	- In your VPC - Isolated steady state workload

Ondemand : Spiky workloads
Reserved : Steady-state workload.
Spot : Time insensitive workload.
Dedicated : Highly sensitive workload.



RI utilization
95% utilization

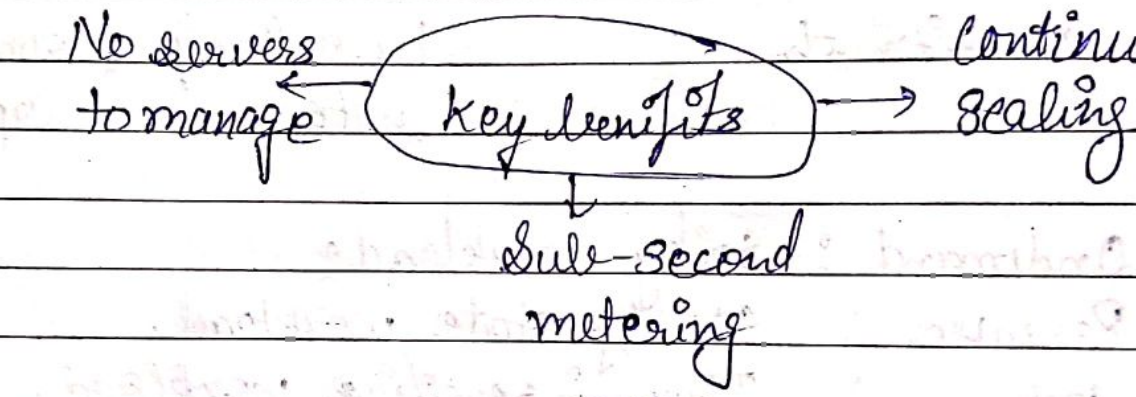
RI coverage
cover always-on resources
Target 70-80% always-on coverage

Use more smaller instances vs fewer, larger instances.

Auto tag resources, identify always-on non production systems, identify instances to downsize

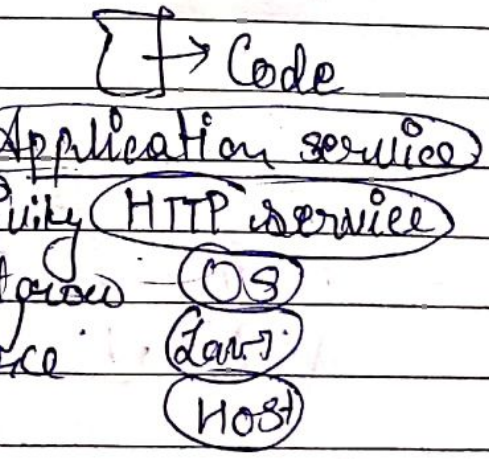
- recomended RI to purchase
- consolidate your billing
- Dashboard your status
- Report on savings.

AWS Lambda (Part 5)



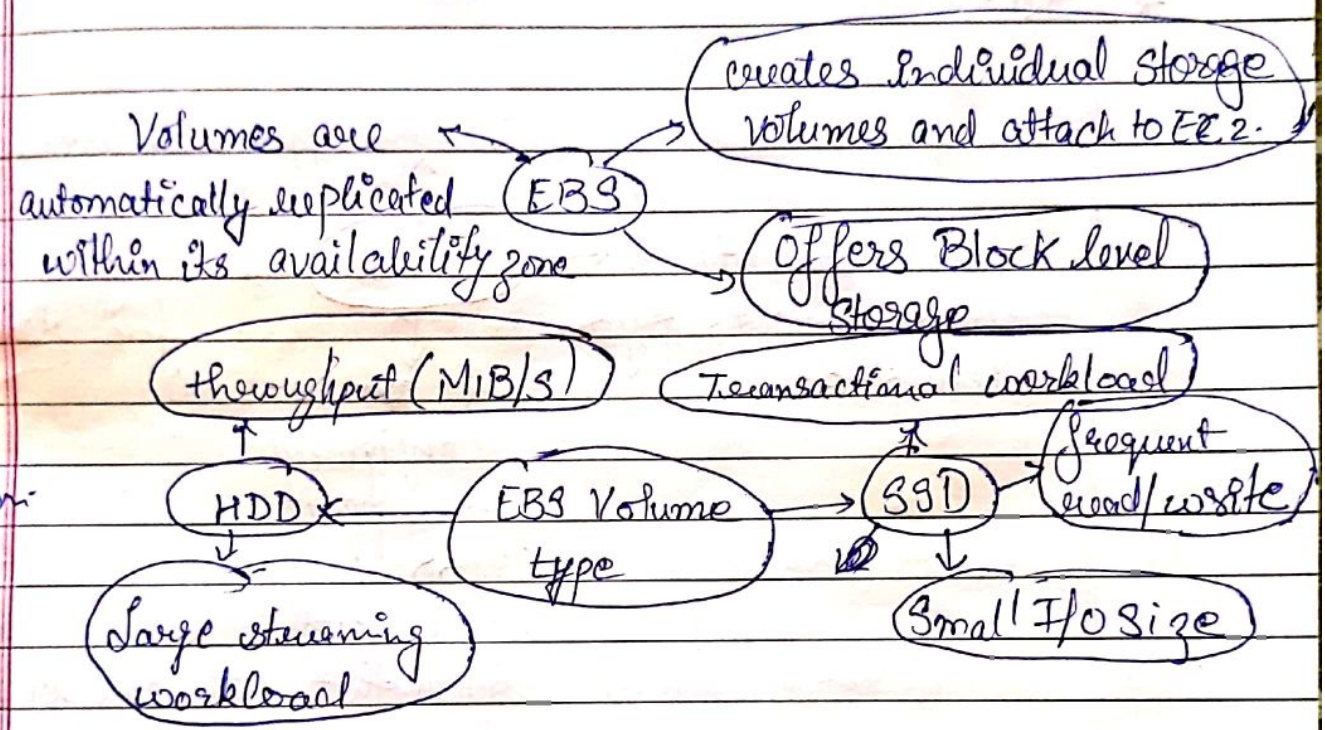
(Part 6) Elastic Beanstalk.

→ Key benifits:-
- Fast and simple to begin
- Developer productivity
- Impossible to outgrow
- Complete resource control.



Storage

- Instance store is temporary storage
- EBS is Resistent, mountable storage which can be mounted as a device to Amazon EC2 instance.
  NOTE - Amazon EBS can only be mounted to an Amazon EC2 instance within the same availability zone.
- Amazon S3 is Resistent Storage, however it can be accessed from anywhere.



SSD		HDD	
General Purpose	Provisioned IOPS	Throughput-optimized	Cold.
- System boot volume - Virtual Desktop - Low-latency interactive apps - Development and test environment.	- Apps needing 1600 IOPS or 250 MiB/s of throughput per volume. - Large Database.	- Streaming workload, fast throughput at low cost. - Big data - Data warehouse - Log processing * Cannot be a boot volume	- Throughput required but not frequently * Lowest storage cost. * Cannot be a boot volume.

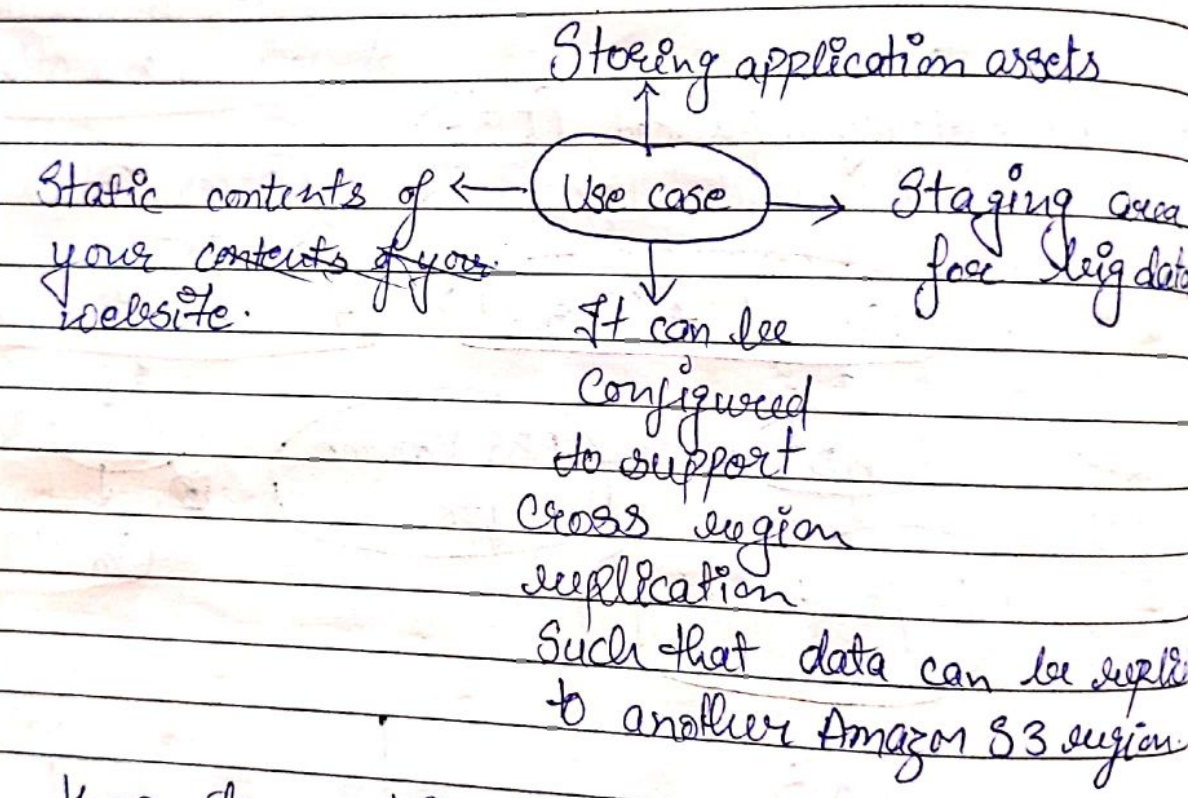
→ gp2 and io1 can only be used as boot volume.

IOPS SSD (General Purpose)
- Charged by amount you provision.

Magnetic
- Charged by the no. of req. to volume.

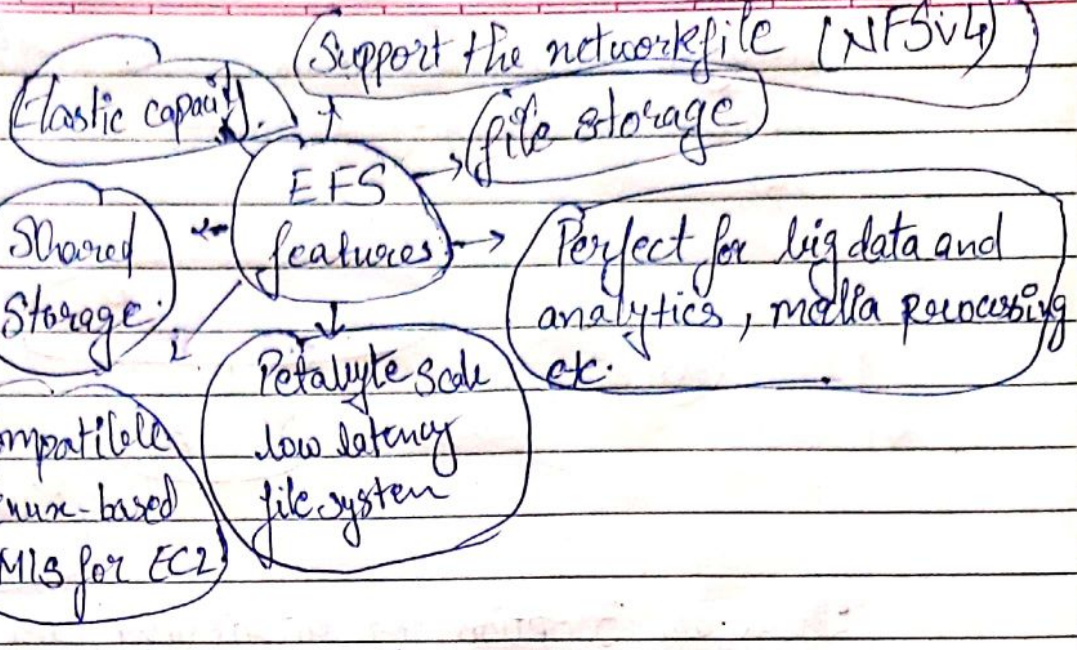
Provisioned IOPS (SSD)
- Charged by the amount you provision.

* S3.



→ How do estimate storage pricing :-

1. Types of storage class
2. Amount of storage. No and size of objects
3. Request
4. Data transfer

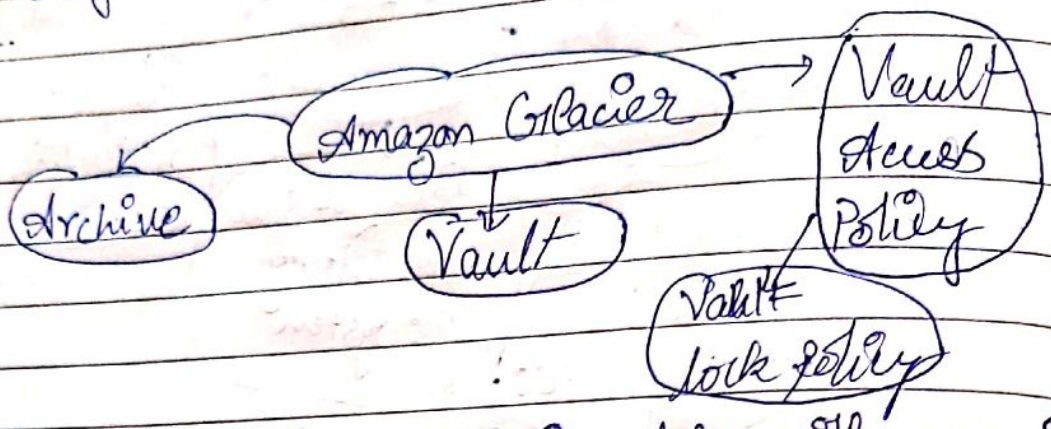


→ EFS resources is having file system as primary resource. Filesystem have ID, creation token, creation time, file system size in bytes, number of mount targets created for the file system, filesystem state.

Mount target
- Subnet ID
- Security groups
- One or more per file system
- Create in a VPC subnet.
- One per availability zone
- must be in same VPC.

Tags - key value pair.

* Amazon Glacier :- It is a data archiving service designed for security, durability, and an extremely low cost.



There are 3 option for retrieving data with varying access time and cost:

1) Expediated - Available in 1-5 mins.
2) Standard - Available in 3 to 4 hours.
3) Bulk - Retrieval complete in 5 to 12 hour

→ How to use?

1) Amazon management console → Creating, Deleting → Managing and Policies.
2) Restful web services, JAVA or .NET SDKs
3) Amazon S3 with lifecycle policies.

* What is life cycle policies?
- It allows you to delete or move object based on age

* A life cycle configuration is a set of rules that define actions that Amazon S3 applies to a group of objects. archive objects to the GLACIER storage class ~~one after~~ creating them.

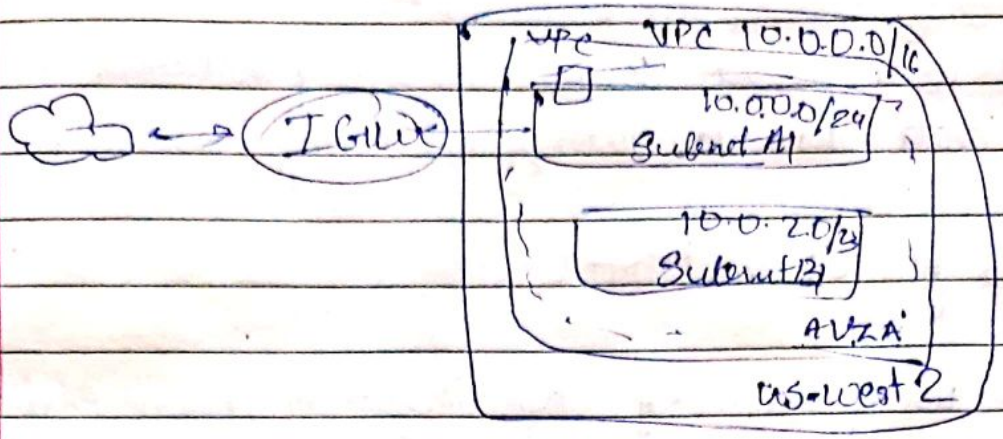
Module 2 Section 3:
AWS Core Services VPC

→ VPC lives within region, as they can exist only in a single region. There are ways to connect VPC in different regions.

* Amazon VPC components: Segment of an Amazon VPC's IP address range where you can launch AWS services.
. Subnet within a zone cannot span a one subnet equal to one availability zone.
. Can be classified as public, private or VPN only.
* Security group
* NACL
(optional) * Internet gateway is a horizontally scaled, redundant and highly available Amazon VPC component. Allows access to the internet from Amazon VPC.
(Optional) * Elastic IP addresses - Static, public IP addresses that can be pulled from a pool for use on a temporary basis.
(Optional) * Elastic network interface - Virtual network interface.
* Endpoints - Direct conn. to other AWS service.
* Peering - Allows 2 VPC to communicate.
* NAT and NAT gateways accepts, translates and forward traffic within a private subnet.

* VPC are logically isolated from other network
* VPC can span across multiple AZ's but subnet cannot.

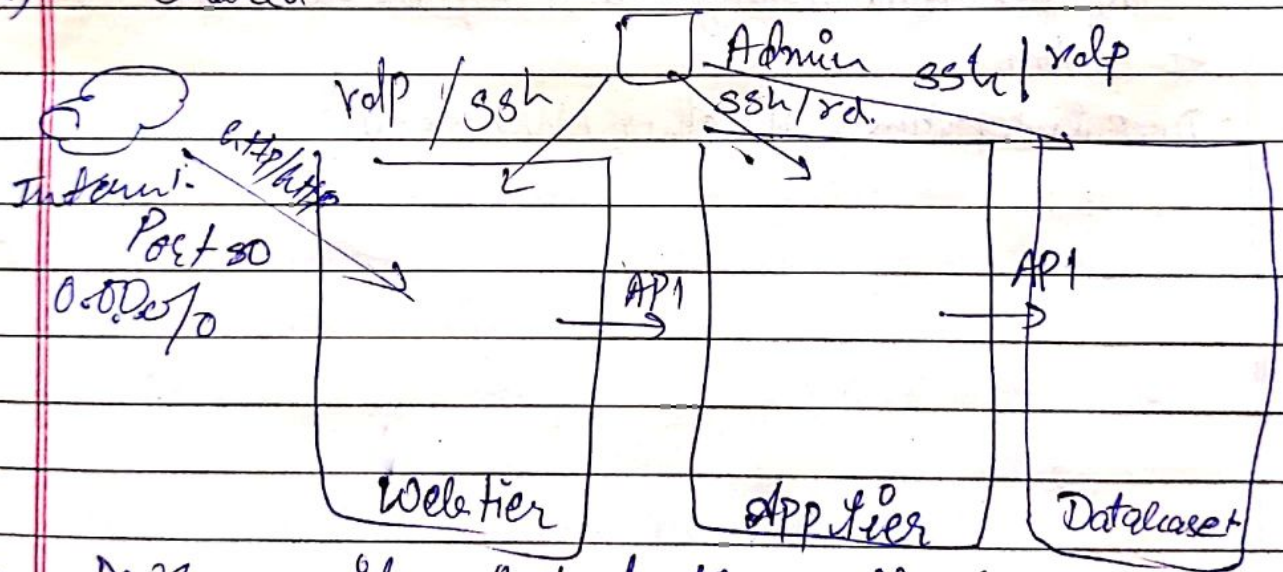
Amazon VPC Example



* Aws security Groups :-

→ Security groups are stateful while NACL are stateless.

1) Shared.



→ AWS provide virtual firewall that can control traffic for one or more instances.

→ Control accessibility by making security groups.

Part 3 AWS Cloud front :- It allows you to scale out, save money, improve app. performance.

→ It is a global content delivery network that deliver data with low latency and transfer speeds.

→ Benifits of Cloud Front :-

→ Global using network of Edge location to ensure that app. deliver high availability, scalability and performance
→ Secure content at edge location.
→ Programmable content delivery network
→ High performance: low latency and high data transfer spe
→ Cost effective : No upfront or minimum commitments
• Pay for data transfer and requests to deliver content to customer.
→ Deep integration with other AWS services.

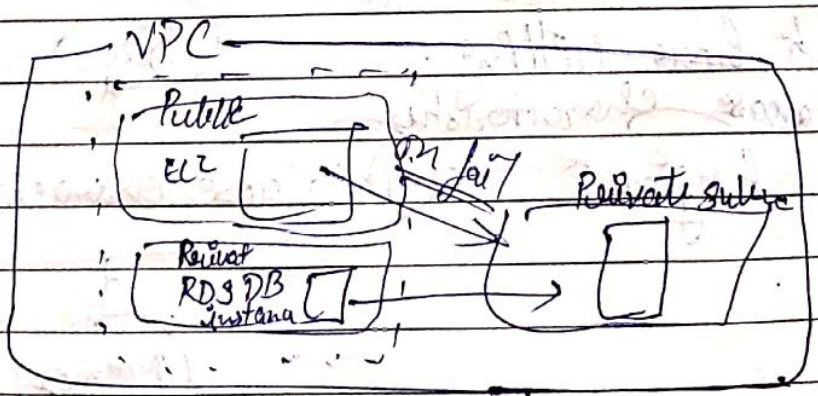
Module 2 - Section 4

→ Unmanaged and managed services.
→ Scaling, fault tolerance and availability are managed by you.
→ Scaling, fault tolerance and availability are typically built in to the service.

* Challenges of RD:
- Server maintainance and energy footprint.
- Software installation and patches
- Backups and high availability
- Limit on scalability.
- Data security
- OS.

* Amazon RDS DB instance -
→ DB instance Class.
CPU, Memory and Network performance
→ DB instance storage.
Magnetic, General purpose, Provisional IOPS.

→ High availability with multiple AZ.



→ Because your application inference the databases by name using RDS DNS endpoint, you don't need to change anything in your application code.

Date
Page

Read replica of Amazon RDS.

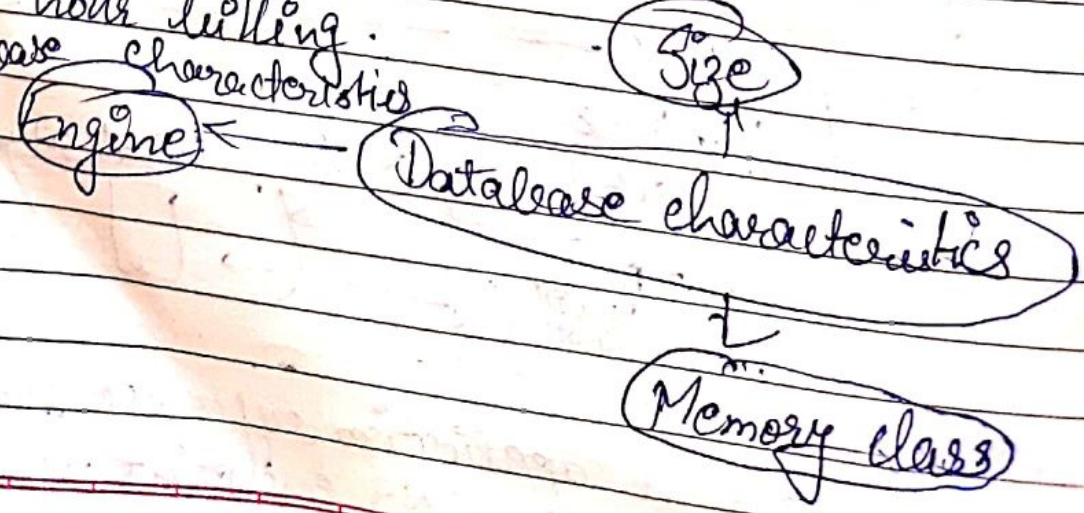
Features - asynchronous replication
- promote to master if needed.

→ Read replica can be created in different region than the master database. This feature can help satisfy disaster recovery requirement or cut down latency.

→ When to use RDS:-
- Complex transaction and complex queries.
- A medium to high query rate - upto 30K IOPs.
- No more than a single worker
- High durability.

→ Do not use Amazon RDS when your app requires:
- Massive read/write rates
- Sharding
- Simple GET/PUT request and queries that a NoSQL database can handle.
- RDMS customization.

1. Clock hour billing.
2. Database characteristics



3. DB purchase type:
   - On demand database instance
     - compute capacity by the hour.
   - Reserved database instance.
     - Low, one time, up-front payment for database instance reserved with 1 or 3 year term.

4. Number of DB instance.
   - Provision multiple DB instances to handles peak loads.

5. Provision and storage:
   - No. charge
     - Backup storage of up to 100% of DB storage of active instance
   - Charge (GB/month)
     - Backup storage of terminated DB instance.

6. Additional storage:
   - Charge (GB/month)
     - Backup storage in addition to provisioned storage.

7. Request: Number of input and output request made to the database.

8. Deployment type - Storage and I/O charge vary depending
   - Single AZ or Multiple AZ.

9. Data transfer - No charge for inbound data transfer
   Tiered charges for outbound data transfer.

Amazon DynamoDB

→ DynamoDB is a fully managed NoSQL database service.

→ Amazon redundantly stores data across multiple facilities within a native US region as part of the fault tolerant architecture.

→ You can have newer format items stored side by side with older formatted items in the same table without needing to perform schema migration

→ SSD.

→ DynamoDB also allows you to provision the amount of read or write throughput you need for your table

* Partioning :-

- As the data grows the table data is partioned and indexed by the primary key.
- Two ways of retriving data :-
- query operation takes advantage of partioning to effectively and locate items by using the primary key
- Scan from other attribute.

Part 3: Amazon Redshift. (Data warehouse)

Leader node
↓
Compute node
↓
Amazon S3 / Dynamo DB

- The amazon redshift Spectrum features enables you to run queries against exabytes of data directly in Amazon S3.

→ Amazon Redshift use cases :-
- Many customers migrate their traditional enterprise datawarehouse to Amazon Redshift with the primary goal of agility.
→ Smaller customers typically don't have the money to purchase the amount of hardware and expertise to run these systems.

→ Saas :- Scale the DW capacity as demand grows.
Add analytic functionality to applications.
Reduce the hardware and software cost exponentially.

Summary :- - Fast, fully managed DW
- Easily scaled with no downtime.
- Columnar storage and parallel processing
- Automatic and continuous monitoring cluster.
- Encryption is built in.

Amazon Aurora

Amazon Aurora is a MySQL and PostgreSQL compatible relational database build for the cloud.

→ It is highly available 5 times better performance of My

→ It has drop-in compatibility with MySQL 5.6 using the InnoDB storage engine.

→ Amazon Aurora is highly available and resilient design. It stores six copies of your data across 3 availability zone with continuous backups to S3.

→ Upto 15 read replicas can be used to help you ensure that your data is not lost.

→ Instant crash recovery.

* Resilient Design - Amazon Aurora does not need to replay the redo log from the last database checkpoint. This reduces the restart time after database crash to less than 60 sec..

Date
Page

Assesment

→ NoSQL database like DynamoDB excel at scaling to 100 of thousands of request with key/value to user se

→ Amazon Redshift is best suited for traditional OLAP transaction.

→ You need to scan to find an item in a DynamoDB table using an attribute other than the item's PK.

Load Balancer

ALB	NLB	CLB
HTTP/HTTPS	TCP	Previous gen: HTTP, HTTPS.
- Flexible application management	- Extreme performance and static IP for your app	- Existing app. that was built within EC2-classic
- Advance load balancing of HTTP and HTTPS traffic	- Load balancing of tcp traffic	- Operates at both request and connection level.
- Operates at the layer 7. (request level)	- operates at layer 4.	

→ Use cases: Access through a single point, Decouple application environment, provide high availability and fault tolerance, increase elasticity and scalability.

→ Classic Load Balancer:
- Access servers through single point
- Decouple the application environment.
- Provide high availability and fault tolerance.
- increase elasticity and scalability.

→ Application Load Balancer - It offers the feature of classic load balancer.
- It offers path based routing and host based routing.
- native IPv6 support
- additional supported request protocols -
- deletion protection.
- request tracking
- Enhanced metrics and enhanced access log.
- Target health check.

→ Use case of ALB: use container to host your micro services and route to those application from a single load balancer.

- allows to route different request to same instance. but differ the path based on port.
- You can setup routing rules to distribute to distribute traffic to only the desired backend application.

- We create rules in order to direct how the request received by the load balancer will be routed to the backend targets.

- To register those targets to the load balancer and configure the health check the LB will use for the targets.

→ Usecase of Network Load Balancer-
Handle sudden and volatile traffic pattern while using a single static IP address per AZ.
- Ideal for application that requires extreme performance.

* In general use cases: High availability and fault tolerant containerized application, Elasticity and Scalability VPC, Hybrid environments, Invoke functions of lambda.

Cloud watch.

- Track resource and application performance.
- Collect and monitor log files.
- Get notified when an alarm gets off.

(Basic monitoring) (Cloud watch) → (Detailed monitoring)

→ Basic monitoring : 7 pre selected metrics at 5 min frequency and three status check metrics at one minute frequency without any charge.

→ Detailed monitoring : All metrics are available to less monitoring at 1 min frequency, for an additional charge.
- Detailed monitoring enabled allows data aggregation by Amazon EC2 AMI ID and instance type.
- It retain metrics for 15 months, free of charge.

CloudWatch metrics support three retention schedules
- 1 min datapoint - 15 days
- 5 min datapoint - 63 days
- 1 hour datapoint - 455 days.

(Metrics) ← (Amazon CloudWatch) → (Event)

(Alarm)

Metric - specific datapoint for one of the resources or application you are monitoring.

Alarm - Alarm sends out a notification message when a tracked metric reaches a specified value for a specified period of time.

Event - Event can monitor AWS resources and deliver a near real time stream of events that describes the changes in resources.

Auto Scaling :-

Three components are required for automatic scaling.
- First, create a launch configuration.
- Create automatic scaling group.
- define atleast one automatic scaling policy.

→ What is lauch configuration?
- defines what to be launched.

→ What is an auto scaling group?
- Defines where the deployment take place and some boundaries for the deployment.

→ What is an autoscaling policy?
- This is to specify when to launch ~~and~~ or terminate Amazon EC2 instance.

Do knowledge assesment again

AWS Cloud Security

AWS is responsible for security of the cloud.

- Secures :- Physical security of data centers with controlled, need leased access, located in nondescript facilities, 24/7 security guards, two factor authentication access logging and review, video surveillance, and disk degaussing and destruction.

- Hardware → Servers, storage devices etc.
- Software → Host OS, service application and virtualization
- Network infrastructure - Routers, switches, firewall etc.
- Virtualization infrastructure including instance isolation

Unmanaged service	Managed service
EC2	DynamoDB
EBS	RDS
	Redshift
	EMR
	Workspaces

- AWS will handle basic security task of OS and database patching, firewall configuration, disaster recovery

- Customer need to configure logical access controls and protect account credential.

Example of Control :-

Inherited Controls - Controls that apply to both the infrastructure layer and customer layers but in completely separate context or perspective in a shared control.

Patch management, Configuration management.

- AWS is responsible for patching and fixing flaws in infrastructure. Customer responsible for patching the guest OS and application.

- Awareness and training.
- Customer specific
- Service and communication protection or Zone security.

* Shared responsibility:
  Customer respon - Guest OS, Applications, Security groups.
  AWS respons:- Physical security, HW/SW Netwo, Virt infrastructure.

Part 2 IAM Identity and Access Management.

* IAM allows you to:
- manage IAM users and their access.
- manage IAM roles and their permission.
- manage federated users and their permission.

Type of security credentials:
- Email address and password - Associated with your AWS account
- IAM username and password - used to access AWS management console.
- Access and secret Access key - used with cli and programatic request like API and SDK.
- MFA - Can be enabled for root account and IAM users.
- Key pairs - Used only for specific AWS service like Amazon EC2.

- IAM allows you to follow the least privilege principle
- Programmatic access
- Management console
- All permissions are denied by default.
- If something is explicitly denied, it can never be allowed.
- IAM is global. It is not on a per region basis. It applies access all regions.

Trusted Advisor Checks, in five categories including: Cost optimization, performance, Security, Fault tolerance, Service limits.

→ Six best practise available to all customers :-
- Service limits
- Security groups - specific ports unrestricted
- IAM use
- MFA
- EBS
- RDS public snapshot.

→ Features and functionalities

Notification

AWS SupportAPI

Action links

Recent changes

Access management

Exclude items

5 minute refresh

CloudTrail is a web service that records API calls for your account and deliver log files to you.

Benifits of CloudTrail ← Always on
- User and resource activity
- Simplified Compliance
- Security automation
- Analysis and troubleshooting

By default, the logs are stored for 7 days.
The activity log can be sent to other AWS services, so the activity history can be retained for as long as you.

Activity happens
↓
Captures and call
- Cloud trail event
  - Who performed request
  - the date
  - the time
  - Source IP
  - how the request was made
  - the region
  - action taken.

AWS config - AWS config is a fully managed service that enables you to assess, audit and evaluate the configuration of your AWS resources.
- continous monitoring
- continous assessment
- Change management
- Operation Troubleshooting.

If you want to track changes to resource configu... answer question about resource configuration, demonstrate compliance, trouble shoot or Perfo... security analysis, use AWS config.

AWS config overview :-

Config change → Config record ← Changes stored in S3 b...

Config automatically evaluates the recor... configuration against yo... desired configuration

Displayed by config API, optionally via SNS.

* IAM practises :-

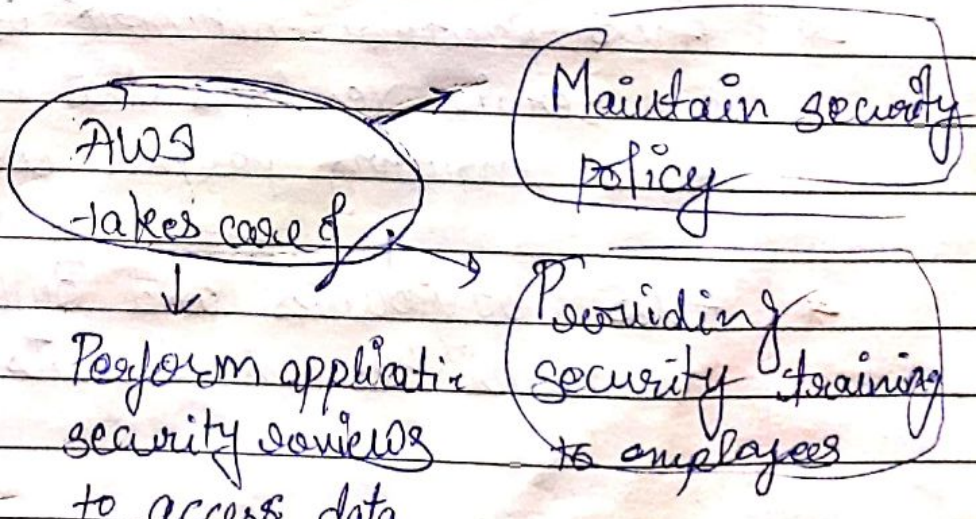
- Delete AWS root account access keys.
- Create individual IAM user.
- Use groups to assign permission to IAM users.
- Grant least privilege.
- Config a strong password policy.
- Enable MFA for privileged users.
- Use roles for application.
- Delegate by using roles.
- Use policy condition.
- Rotate credential
- Remove unnecessary users and credentials.
- Monitor activity in your AWS account.

* AWS Service Catalog can be integrated with AWS CloudFormation for stack development to ensure compliance with corporate standards.

→ Components of AWS Risk and Compliance programs
- Risk management
- Control environment
- Information security.

* Risk management :- Identifies risk.
- implement appropriate measures to address risks.
- Assess various internal/external risk.

→ Information security framework and policies based on
- Control objectives for information and related technology
- American institute of certified Public accountants.
- National institute of standards and technology.



Policies

↓

Process ← (AWS Control Environment) → Technology

* Customer compliance basic approach:
  - Review, Design, Identify, Verify

AWS security resources

- AWS account teams provide
  - First point of contact.
  - Guide deployment
  - Point towards the right resource to resolve security issues.

- AWS Enterprise Support provides 15 minute response time. 24/7 by phone, chat or Email. or Dedicated TAM.

* AWS partner network is a group of cloud software and service vendors that has hundreds of certified AWS consulting partner worldwide.

* AWS advisories and Bulletins provided on current vulnerabilities and threats.

Cloud Architecture

Aws well architected Frame work-

→ Why?
increase awareness of architectural best practices.
Address foundational areas
Evaluate architecture using consistent set of principles.

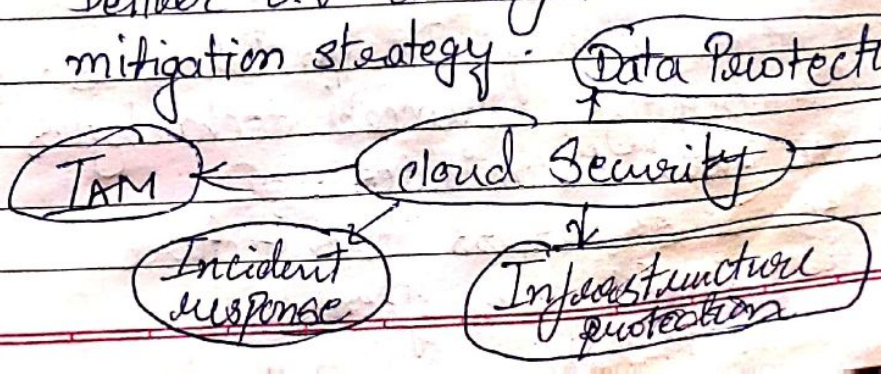
→ Not Provides
Implementation details
Architectural patterns
Relevant case studies

Does not provides
- Critically understand architectural decision
- Services and solution relevant to each question.
- Reference to relevant resources.

Pillars of well architected framework

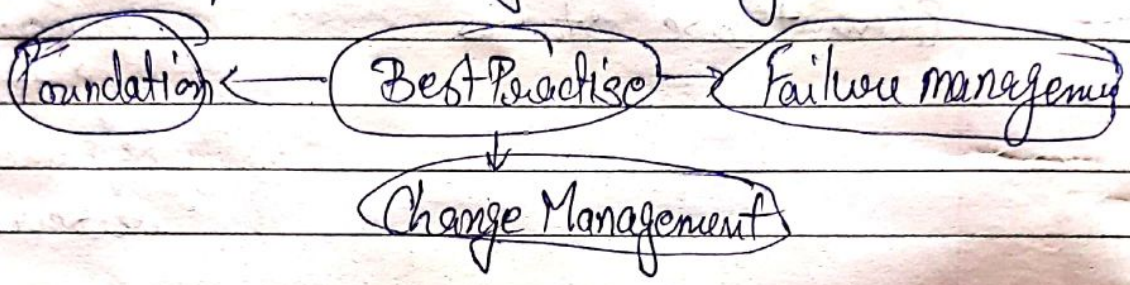
1. Operational Excellence
2. Security
3. Reliability
4. Performance efficiency
5. Cost optimization.

→ Operational Excellence - Deliver Bv. and improve supportprocesses
→ Security - Protect information, Systems, Assets.
Deliver b.v through Risk assessment and mitigation strategy.



Security : Design Principles:
Implement security at all layers.
Enable traceability
Implement principle of least privilege
Focus on securing your system.
Automate

Reliability : Ability of a system to :
Recover from infrastructure or service failure.
Dynamic acquirement of computing resource.

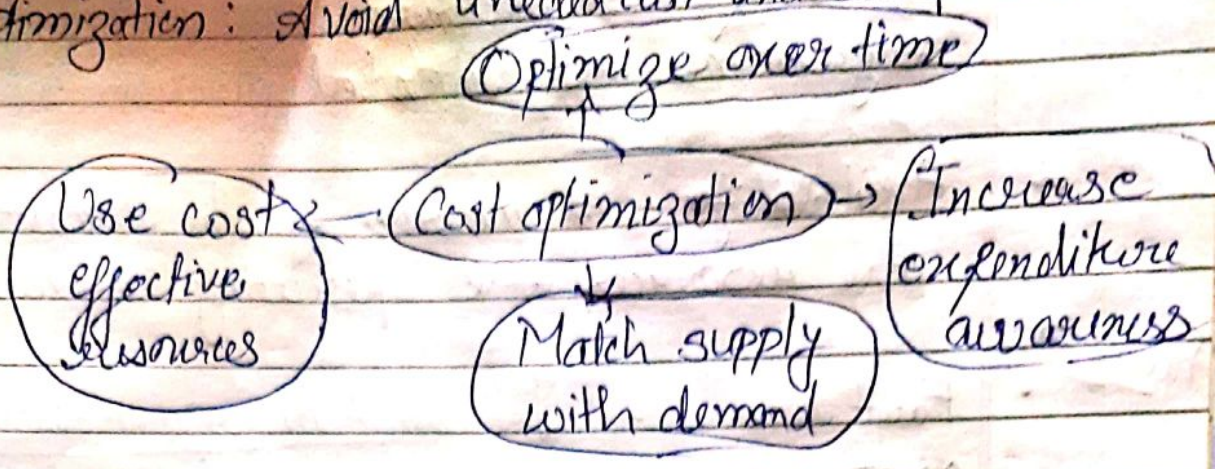


Reliability : Design Principles:
Test recovery procedure
Automatically recover
Scale horizontally
Stop guessing capacity
Manage change in automation.

Performance efficiency: Fulfill system requirement and maintain efficiency as demand changes and tech. evolves.

Performance efficiency : Design Principles.
Democratize advanced technologies.
Go global in minutes.
Use a serverless architecture
Experiment more often.
Have mechanical sympathy.

Cost optimization: Avoid unneeded cost and suboptimal resources.



Cost optimization: Design Principles.
Adopt a consumptional mode
Measure overall efficiency
Reduce spending on data center operation
Analyze and attribute expenditure.
Use managed services.

Part 2 Well-architected design Principle

Stop guessing your capacity needs.
Test system at production scale.
Automate to make architectural experimentation easier.
~~Automat~~ Allow for evolutionary architectures.
Drive architecture using data.
Improve through game days.

Part 3

Reliability - Probability that entire system functions for a specified period of time.
Includes hardware, software, and firmware.
Measures how long the item performs its intended funct

Measures → Mean time Between failure
→ failure rate.

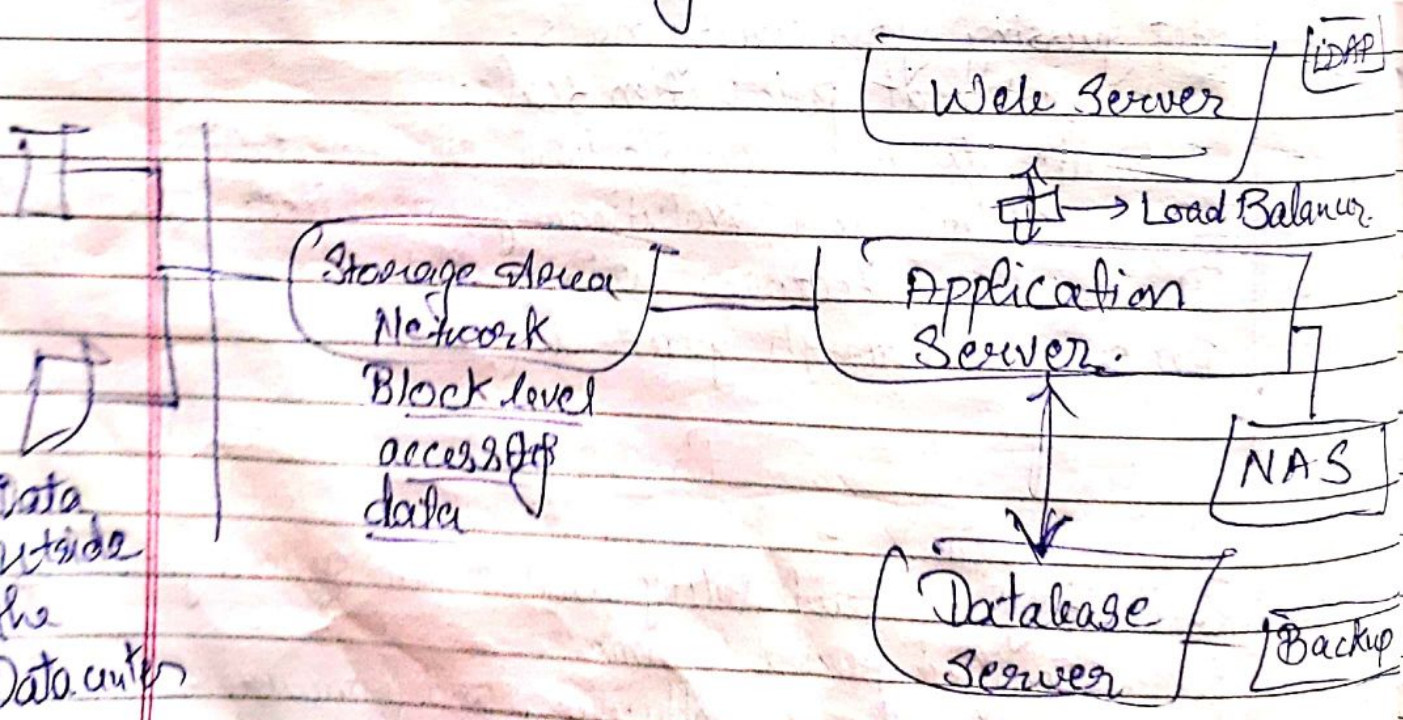
Reliability Vs Availability

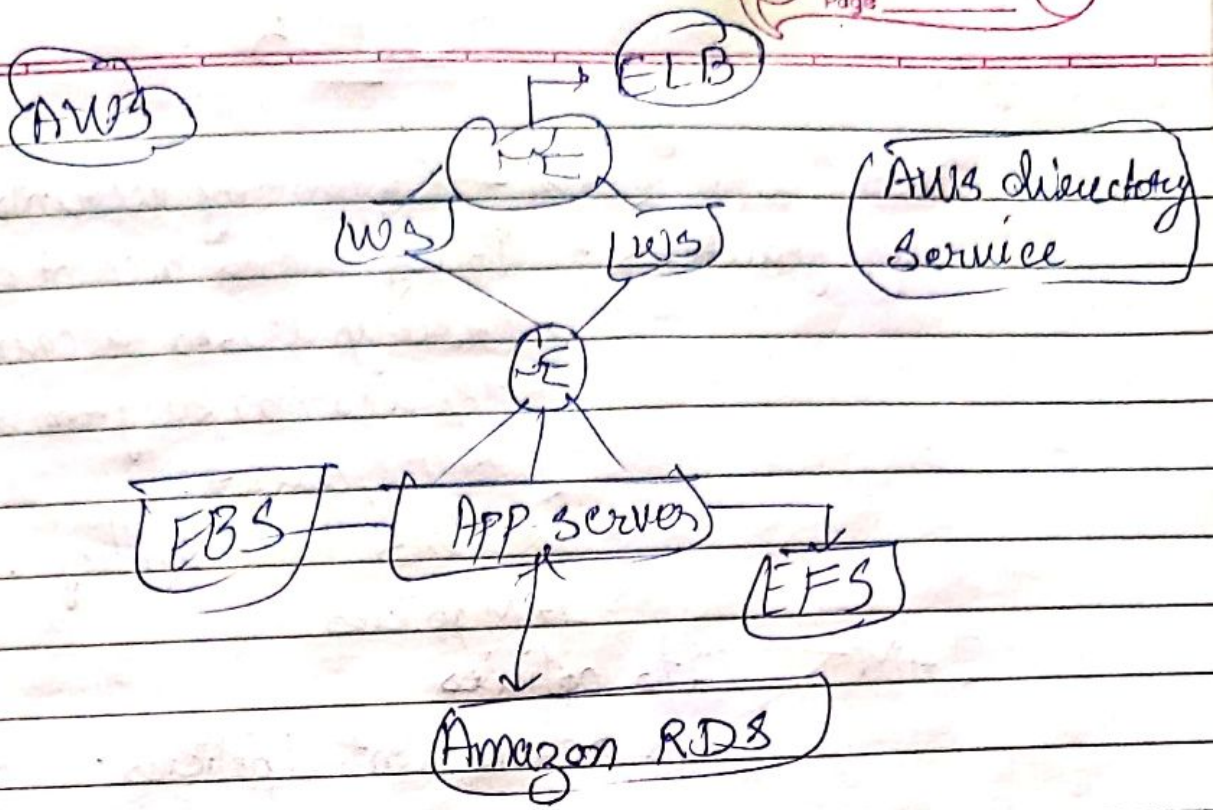
- Reliability - A measure how long a resource performance its intended function.
- Availability - A measure of the percentage of time the resources are operating normally.

- Fault tolerance - The built-in redundancy of an application component and is ability to remain operational.
  - It addresses to the hardware failures.
- Scalability - The ability of an application to accommodate growth without changing design.
- Recoverability - The process, policies and procedures related to restoring service after a catastrophic event.

Part 4

Example - Transitioning a Data center to the Cloud:

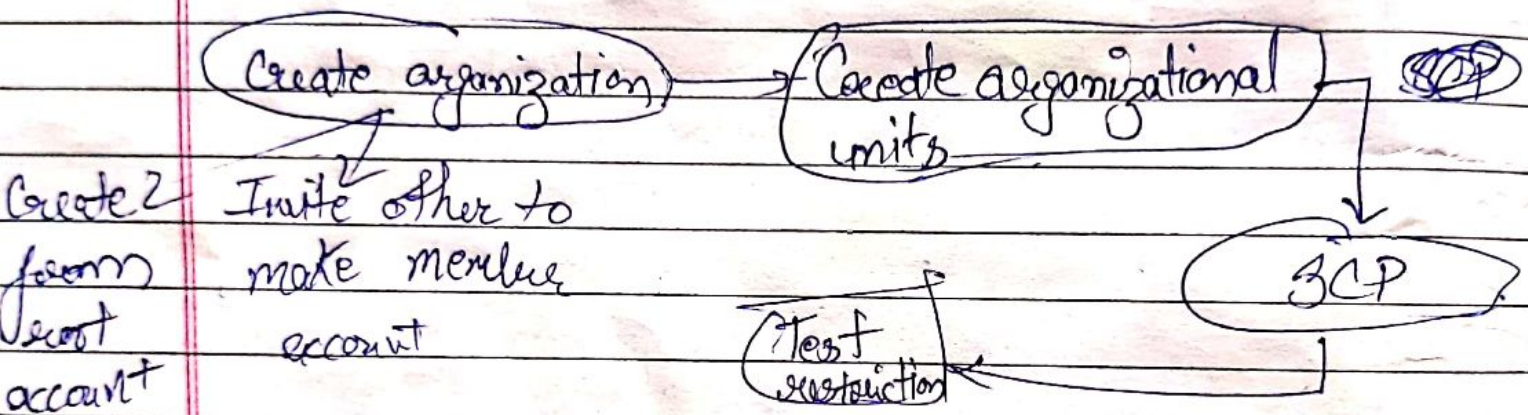




AWS Organization – Organizing accounts.

Key features – Policy-based account management.
- Group based account management
- Application program to automate the management.
- Consolidate billing.

IAM → IAM policies.
→ Its policies
→ Service Control policies.



Limits in AWS Organization.
- Names must be composed of unicode character.
- Names must not exceed 250 character in lenght.

* Access – AMC, CLI, SDK, HTTPS Query application.

Part-2

Tools on AWS billing dashboard.
- AWS Bills
- AWS Cost explorer
- AWS Budgets
- AWS cost and usage reports.

AWS Support Services :-

Support < Experimenting
Production
Business critical

Proactive guidance - TAM
Best Practices - Trusted Advisor
Account assistance - AWS Support Concierge

AWS support offer 4 plans
Basic support - Resource center access, Service health dashboard, Product FAQ's, Discussion forum, Support and health check.

Developer support - Development support : early development.
Business Support - Customers running production wl
Enterprise Support - Customers running business and mission critical workload.

TAM is the point of contact for all the ongoing support in Enterprise.
Response depends on case severity see 3.6. module

AWS Trusted Advisor :-

- Core checks and recommended
- Full trusted Advisor benifits available with Bussiness or enterprise support Plans.

→ Locate the management tool section of the console.

New Syllabus

→ Compute ← Fundamental drivers of cost on AWS → Data transfer
↓
Storage

- Pay for what you use
- Pay less when you reserve.
- Pay less when you use more and as AWS grows.

* Global Infrastructure

1. Data governance, Legal requirements
2. Latency
3. Service available within the region
4. Cost (vary by region)

- Not all the services are available in all the region.
- AWS recommend replicating accross several AZs for resiliency.
- Resources in one region are not automatically copied in other region.
- It is our responsibility if we want.

→ AWS Storage Services :-
1) Simple Storage Service.
2) Elastic Block Storage
3) Elastic file System
4) Amazon Glacier.

→ AWS Compute category :-
1) Amazon EC2
2) Amazon EC2 auto scaling
3) Amazon Elastic container service
4) Amazon EC2 Container registrey
5) EBS
6) AWS Lambda
7) Elastic kubernet service.
8) AWS Fargate.

→ AWS Database services :-
1) Amazon Relational database service.
2) Amazon Aurora
3) Amazon redshift. (Work fast at any scale)
4) Amazon DynamoDB (one ms response at any scale)

→ AWS Networking and content delivery servic
1) Amazon VPC.
2) Elastic loadbalancing
3) Amazon Cloudfront (CDN)
4) Amazon Transit gateway.
5) Amazon route 53.
6) Amazon Direct connect
7) AWS VPN.

→ AWS security, identity and compliance services
1) IAM
2) AWS organization
3) AWS Cognito
4) AWS artifact
5) AWS key management service
6) AWS Shield.

→ AWS Cost Management
1) AWS Cost and usage report
2) AWS Budgets
3) AWS Cost Explorer

→ AWS management and governance services
1) AWS management console
2) AWS config
3) AWS Cloudwatch
4) AWS autoscaling
5) AWS CLI
6) AWS Trusted advisor
7) AWS well architect tool
8) AWS Cloud trail.

* IAM Policies :- Identity based and resource based.
→ If there is a competition between allow and deny then deny wins.

→ Characteristic of resource based policies :-
- Specifies who can access to the resource and what action they can perform on it.
- The policies are inline only not managed.

NOTE Resource based policies are supported only by some AWS services.

Secure your new AWS Account :-

→ Do not use the AWS account root user except when necessary.

→ Stop using the account root user as soon as possible. How?
- Create IAM user
- IAM group with full administrator permission and add user to the group.
- Disable and remove your account root user access keys
- Enable password policy for user.
- Sing in with new user and save root user credential in a secure place.

2.→ Enable MFA.

3.→ Use AWS Cloud Trail :-
- Maintain log for 90 days.
- all stored in S3 bucket.

4.→ Enable a billing report, such as the AWS Cost and usage report.

- Billing reports provide information about your use of AWS resources and estimated cost for that use.
- Details go to S3 bucket and are updated atleast once a year.
- AWS cost and usage report tracks your AWS usage and provides estimated charges, either by hour or by day.

AWS Shield.

* AWS Shield :-
- Is manged DDOS protection service.
- Safeguard application running on AWS.
- Provides always-on detection and automatic Inline mitigation.
- AWS Shield standard enabled for at any cost.
- AWS shield advanced is an optional paid service.

Q. Why we use :-
✓ Minimize downtime and latency.

IMP To contact DDOS response team customers need to have either business or enterprise support.

* AWS compliance programs :-
- Certification and attestation
- law regulation and privacy General Data protection regu

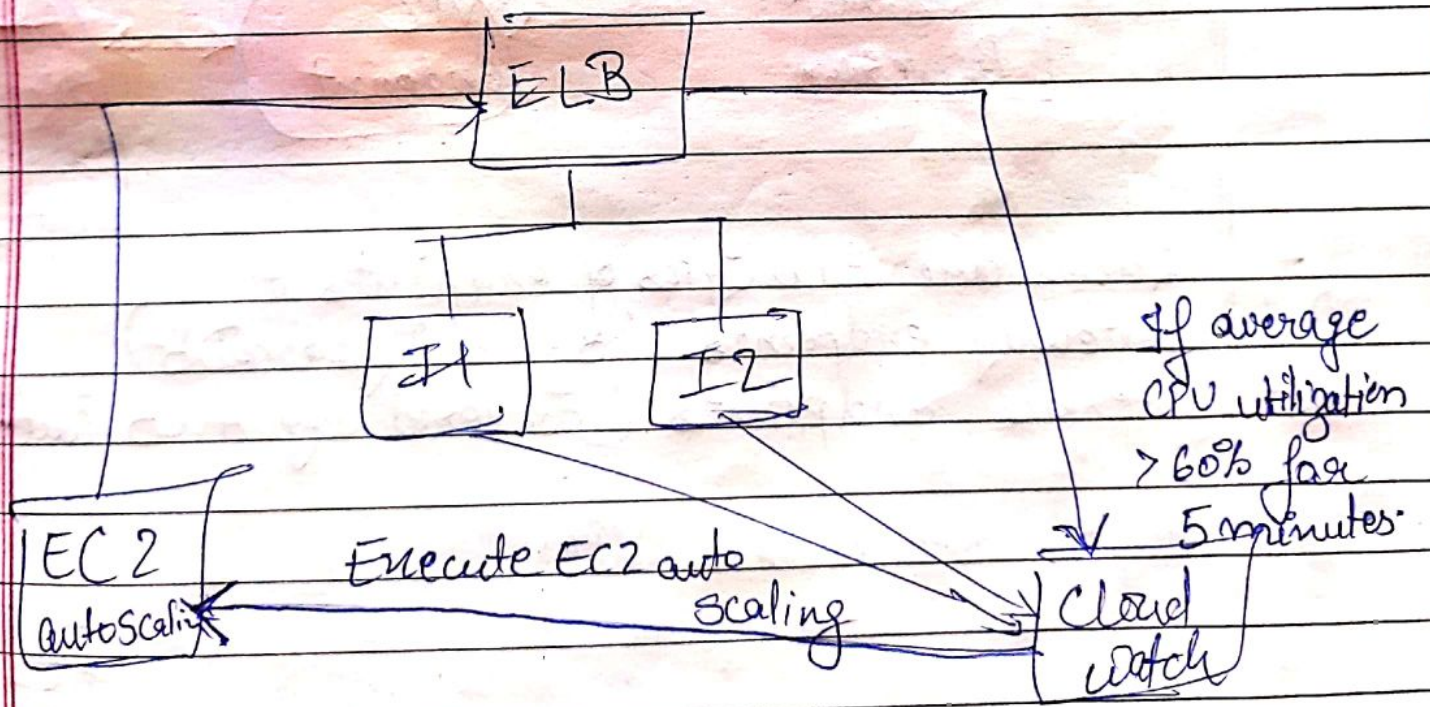
* Module 4 Summary :-
- Recognize Shared responsibility model
- responsibility of the customer on AWS
- Recognize IAM users, groups and roles
- Different credential.
- Secure new account
- Explore groups and users
- secure aws data
- AWS compliance program.

Important: Changing the AWS Support Plan can only be done by the AWS account root user. The other tasks are alone with IAM.

* How AWS EC2 auto Scaling works?

Launch configuration → Auto scaling group

- Maintain current number
- Manual Scaling
- Scheduled Actions
- Dynamic Scaling
- Auto Scaling

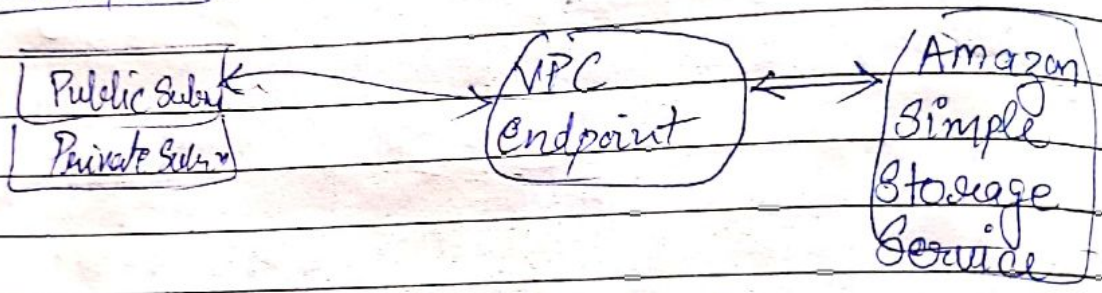


* Amazon VPC peering.

- You can connect VPC in your own AWS account between AWS accounts, are between AWS region.

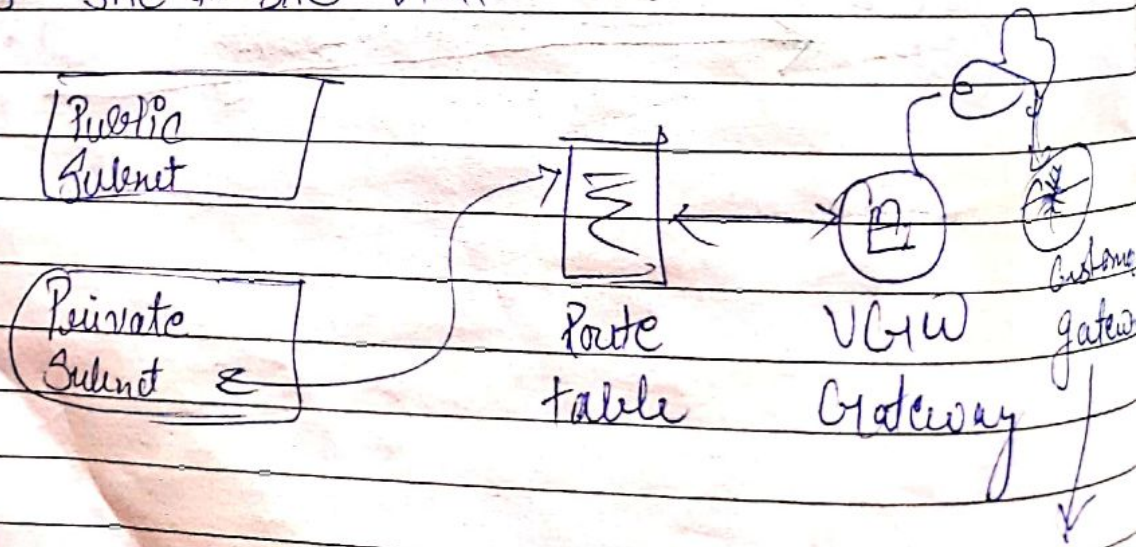
Restriction- IP spaces can't overlap.
Transitive peering is not supported.
You can have one peering resource between the same two VPC's.

VPC Endpoints :-



- There are two types of endpoints :-
1)- Gateway endpoints (S3 and DynamoDB)
2)- Interface endpoints (powered by AWS Privatelink)

* AWS site to site VPN



VPC Securities

Security groups:- Have rules to manage instance traffic
- Default security groups are sealed shut to inbound traffic. We need to define rules.
- Security groups are stateful. The outbound traffic is always allowed.

ACL has separate inbound and outbound rules and each rule either allows or deny traffic.
- Default network ACL allows all inbound & outbound IPv4 traffic.
- Network ACL's are stateless.

Categorizing compute service

EC2 — Iaas, Instance based/ Vertual machine

Lambda — Serverless computing Function based, Low cost.

ECS

EKS — Container leased

Fragate — computing -

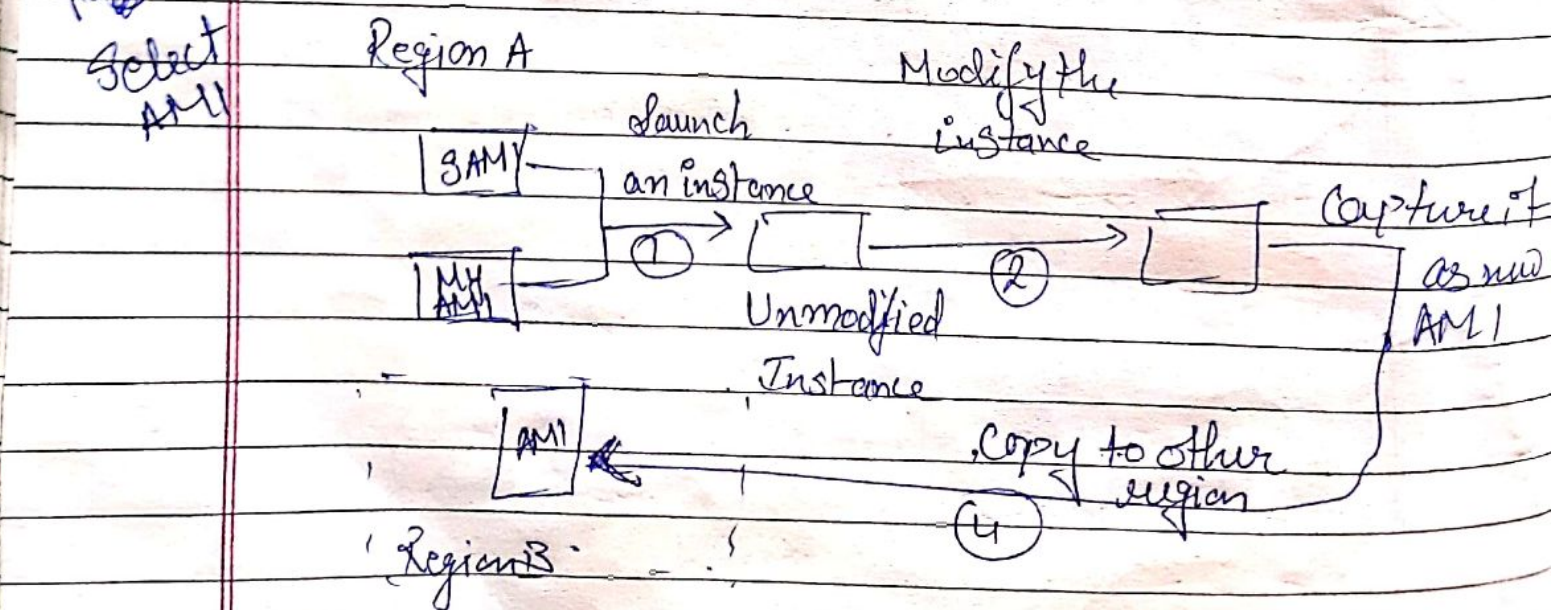
ECR — Instance leased.

EBS — Paas, for web application.

→ Some aspects to consider -

- What is your application design?
- What are the usage patterns?
- What configuration settings will you want to manage?

* Creating new AMI: (EC2 → launching)



2. Instance type :- RAM, CPU, Storage, Network performance.

Instance type naming : (t3) . (large) → size
↓ family
↓ generation

Select instance type : Based on use cases.

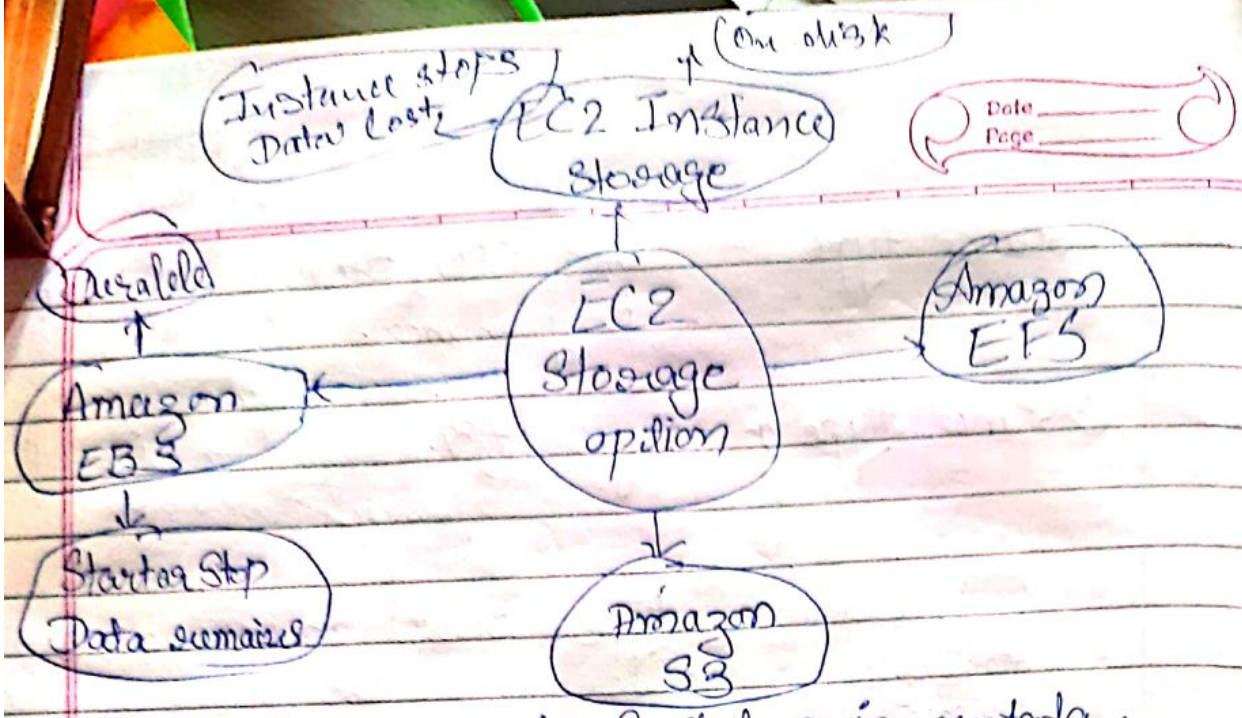
	Instance type	Usecase		Instance type	Usecase
1.	m1, m4, m5 t2, t3	Broad	2.	c4, c5	High performance
3.	r4, r5 x1, x1	In memory databases	4.	f1, g3, g4, p2, p3	HC
5.	d2, h1, i3	Distributed file system			

3. Network settings :- Identify the VPC and optionally the subnet.
→ When in default VPC the instance is getting public IP address.

4. Attach IAM role :- If yes attach an appropriate IAM role.
- The role is kept in instance profile.
- You can also attach a role to an instance that already exist.

5. User data script :- Scripts executes the first time the instance starts.

6. configure storage volume - For each volume specify :
1) Encryption. 2) Size 3) Volume type



Tag - A tag is a label that is metada.

Security group.

Key Pair - A key pair consist of -
- A public key that AWS stores.
- A private key file that you store.

* EC2 instance metadata is data about your instance while you are connected to the instance, you can view it - at 169.254.169.254/latest/meta-data.
It can be only accessed from the instance only.

→ It can be used to configure and manage a running instances.

* For ex, author a configuration script that reads the metadata and uses it to configure application and OS settings.

Benifits of EC2 pricing model:-

On demand Instance
Low cost and flexibility

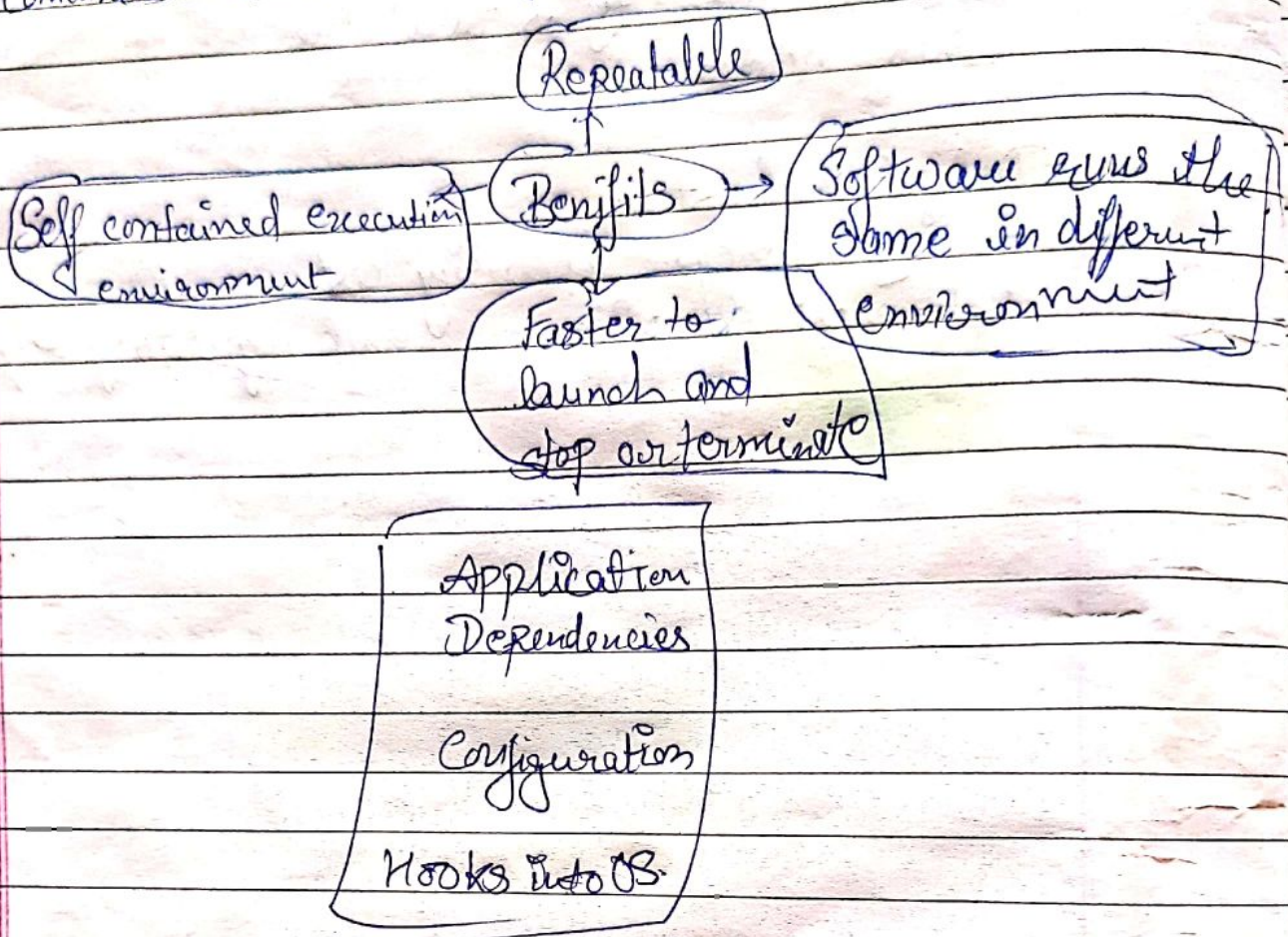
Spot Instance
Large scale,
Dynamic workload.

Reserved Instances
Predictability ensures
compute capacity is available
when needed.

Dedicated host.
- Saving money on licensing cost
- Help meet compliance and regulatory requirements

AWS Container Service

Containers are a method of operating system virtualization



* Docker is a software platform that enables you to build, test and deploy your application.

→ Container run on Docker.

Container are created from a template called image

→ A container have everything a software application needs to run.

Q. What it needs?

A. Libraries, System tools, Code, Runtime.

→ Virtual machine needs hypervisor while Container can run on any OS if/appropriate Support Software are shared with the OS host for Docker.

Amazon ECS cluster Options :-

Key question: Do you want to manage the Amazon ECS cluster that runs the container?

- If yes, create an Amazon ECS cluster backed by EC2
- If no, create an Amazon ECS cluster backed by AWS Fargate

Now let's see an alternative to ECS.

- Kubernet is a open source software for container orchestration.
  - Deploy and manage containerized application at scale.
  - The same toolset can be used on premis and in the cloud.
- It complement docker, it orchestrates multiple Docker host (nodes).
- Automates
  - container provisioning
  - Networking
  - Load distribution
  - Scaling.

If none of EC2 instance are connected to EFS then performance mode is Max I/O.

Date
Page

S3

- Data is stored as object in buckets
- Virtually unlimited storage
  - Single object is limited to 5TB
- Designed for 11 9s of durability
- Granular access to bucket and objects

Amazon S3 bucket URL

Access object:
- Bucket path-style URL endpoint:
  - https://s3.Region code.amazonaws.com/bucket name
- Bucket virtual-hosted-style URL endpoint
  - https://Bucket name.s3.Region code.

Note: Data → Redundantly stored.

Data transfer:
- Amazon S3 pricing -
- Pay only for what you use, including -
  - GB per month
  - Transfer out to other region
  - PUT, COPY, POST, LIST and GET request.
- You do not pay for -
  - Transfer in to Amazon S3.
  - Transfer out from Amazon S3 to Amazon CloudFront or an Amazon EC2 instance in same region

When to use Amazon RDS.

Use it when:

Complex Transaction

High query or write rate.

Single working node and high durability

Massive read/write rates

use Amazon RDS.

Sharding due to high data size or through-put design.

-SIMPLE GET or PUT
- RDMS customization

Design Principle of Cloud architect

Operational Excellence - Key topics - Managing and automating changes
- Responding to events
- Defining standards to successfully manage daily operation

Principles:
- Perform operation as code
- annotate document
- Make frequent, small, reversible changes
- Refine operation procedures frequently
- Anticipate failure
- learn from all operational events and failures.

Operational excellence → Prepare, Operate, Evolve.

Security: Identifying and managing who can do what
Establishing controls to detect security events
Protecting system and services.
Protecting confidentiality and integrity of data.

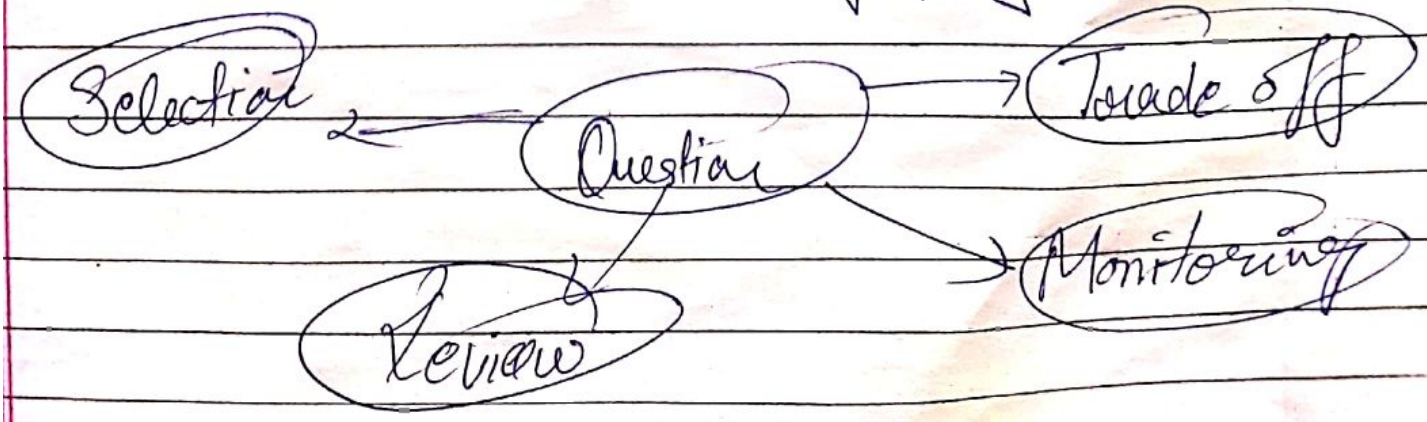
Principles: Implement identity foundation.
Enable traceability
Security at all layers
Security best practice
Protect data in transit and at rest.
Keep people away from data.
Prepare for securing events

Reliability : key topics
Setting up
Cross Project requirements
Recovery Planning
Handling change

Principles: Test recovery Procedures
automatic recovery
Scale horizontally
Stop guessing capacity
manage change in automation.

Performance efficency - Selecting the right resource types and sizes based on work load requirement.
- Monitoring performance
Making informed decision to maintain efficency as business nee evolve.

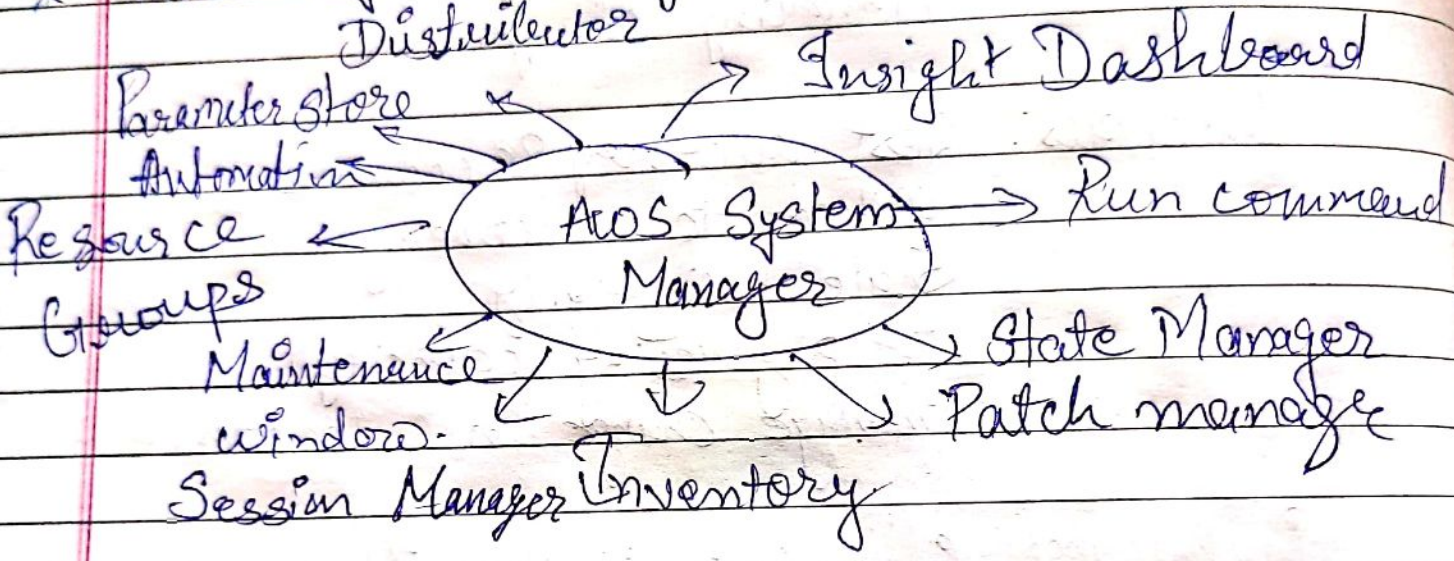
Principles - Democratize advance technologies ✓
Go global in minutes ✓
Use serveless architecture ✓
Experiment more often ✓
Have mechanical sympathy ✓



7, Third party Database?

Performance, cost optimization, security, fault tolerance and service limits are the five categories.

* AWS System Manager's Distributor



→ AWS Personal Health Dashboard - Provides alerts and remediation guidance when AWS is experiencing events that might affect you

→ AWS well-architected framework, developed to help cloud architects build secure, high-performing resilient and efficient application infrastructure