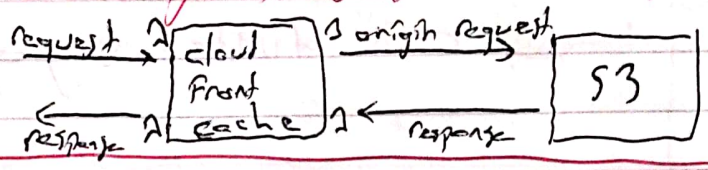
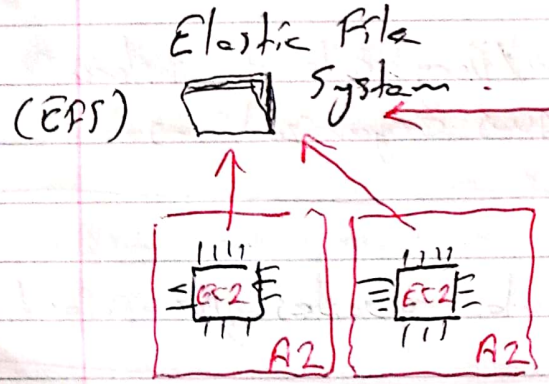
- Amazon Kinesis Firehose is the easiest way to load streaming data into AWS. (into S3, Redshift)

- Lambda@Edge is an extension of AWS Lambda, compute service execute functions the content cloudfront deliver.



- Signed URL a user gets access only a single file
  Signed cookie " " " multiple files.



∴ EFS provides simple, scalable fully managed use AW service and on-premises simultaneously.

- cloudfront geo restriction for banned countries.

- Network Load Balancer distribute traffic to the instances at Layer 4

- Permissions for a specific task on ECS, you should use IAM Roles, The "taskRoleArn" is specify the policy.

EBS Volume Types

(SSD) : Transactional workload, frequent read/write with small I/O size, dominant attribute IOPS

(HDD) : Large streaming workloads, attribute is throughput (500 GiB – 16 TiB)
- ↳ Throughput optimized HDD : frequently accessed (st1)
- ↳ Cold HDD : Less frequently accessed workload

- ↳ General Purpose SSD : Balance price and performance (gp2) (1 GiB – 16 TiB, Max IOPS : 16000)
- ↳ Provisioned IOPS SSD : High performance, mission critical (io1) (4 GiB – 16 TiB, Max IOPS 64000)

(SCP) Service Control Policy : Allow/Deny rule to instance in AWS Organizations.

- SQS queue, use seperate queues for prioritize

- With the copy of (AMI) able to launch instance from the same EBS volume in another Region.

Note: (AMI) stored in S3 but cannot view S3 console.

- AWS DataSync move large data online b/w premises storage and S3 or EFS.

- Scaling Policy:

Schedule Scaling: When and for how long need additional capacity.

Step Scaling: Lead unpredictable, adjustment vary the alarm breach.

Simple Scaling: Unpredictable Load, after scaling waiting health check & replacement, to additional alarm (step scaling)

- AWS Direct Connect: (DX) (Regional service)

- Speeds from 50 Mbps – 500 Mbps accessed APN partner also
- DX connection not encrypted. → if you want, the DX
- ★ Use IPSec 525 VPN over connection to add encryption in transit

---

- Transit Gateway:

- Birden çok multiple VPC ayrı ayrı VPC peering yerine Transit Gateway hub gibi görür.
- On premise den DX için direk Transit GW bağlanarak bütün VPC ler ile connection kurulmuş olur.

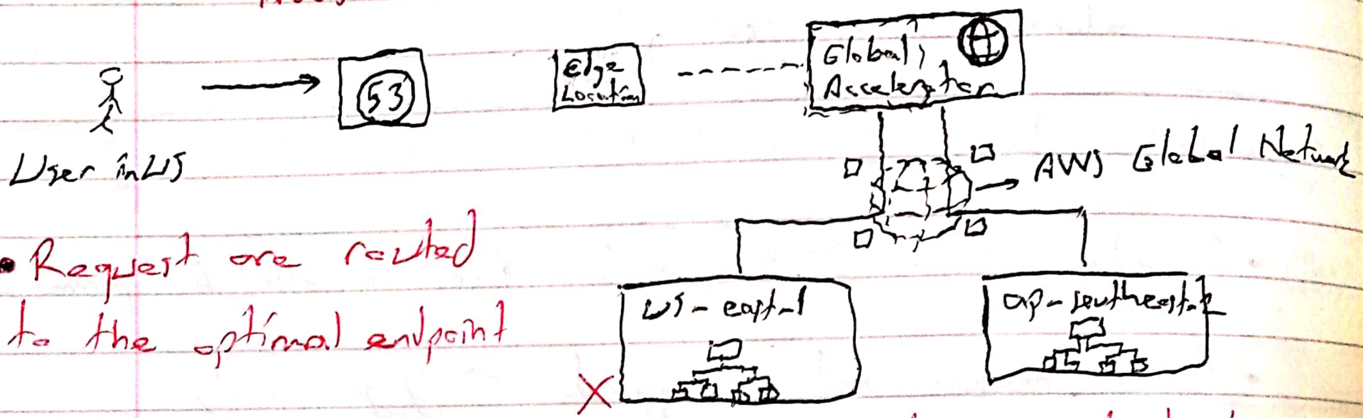
- VPCs are region wide, create up to 5 VPCs per region
- ★ Egress-only Int. Gateway for IPv6 traffic
- VPN connection b/w VPC (Virtual Private Gateway) to on premise (Customer Gateway)
- Sec Grp (Stateful) Network ACL (Stateless)

- Private Connectivity b/w VPCs different region, VPC peering

- Several remote office connect to an VPC and eachother over the internet with full encryption;
  Creat VPG and attach remote locations using AWS CloudHub.

★ Cloudfront certificate must be issued in US-east-1

AWS Global Accelerator:



- Request are routed to the optimal endpoint

- US-east de problem olsa ap-southeast'e yönlendirilecek ancak long latency olmasın diye Global Accelerator var.

CNAME	Alias Records.
can use subdomain	- Maps the domain name to the ELB
	- Resolving apex or naked domain names (example.com)

★ File system with S3 integration is FSX for Lustre

★ EBS Volumes AZ specific but snapshots region specific bc they are on S3.

- Simple Queue Service (SQS): decoupled
- Simple Notification Service (SNS): Notification Cloudwatch triggered
- Step functions: Processing workflow.
- Amazon Kinesis: real-time streaming
- Amazon MQ: Message Broker, migrate queues to AWS.

ElastiCache: Two types, high availability, multi-AZ

Some app. such as media catalog updates → Not supported

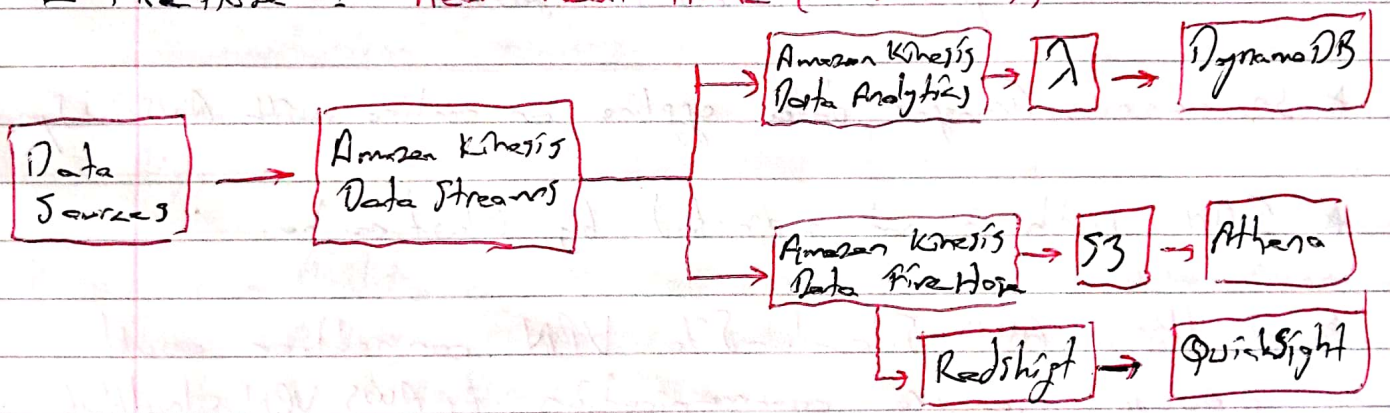
Memcached: No data persistence, simple data, No encryption
required high frequency reads and consistent throughput. No backup, restore, and snapshots.
- in-memory database, support multiple cores or threads

Redis: Data persistance, complex data, encryption available
support high availability multi-AZ automatic backup and restore, manual snapshots.
- Does not support multiple cores or threads.

★ Storing session state → Elasticache or dynamodb
→ Reduce the S3 retrieval cost, improve performance.

DynamoDB - Serverless, performance milisecond, DynamoDB Accelerator (DAX) microsecond latency
35 days on demand backup

- Data Stream : real
- FireHose : near real time (~200 ms)



Amazon QuickSight: Diff is in case for data visualization.

- Pricing per query and data scanned each query.

Amazon Athena: - Queries data in S3 using SQL
- Connect other data with Lambda
- Querying Network Load Balancer Logs.

AWS Glue: Fully managed, used for data analytics.

- Discovers data and stores metada in Glue Data Catalog.

- Works → S3, Redshift, RDS and Ec2 database

Serverless Database: → No-SQL → DynamoDB
→ MySQL, PostgreSQL → Aurora Serverless

AWS WAF: - Key words (Web exploit and cross site scripting)

- WAF is rules to filter web traffic.

Amazon Macie: Security, data privacy service on S3. Also API keys and secret keys.

AWS Migration Tools:

- AWS Application Discovery Service: When you decide to migrate from on premise first need to discover requirements
- AWS Server Migration Service: Servers.
  " Database " " : Database
  " DataSync : NAS / File Server

---

* Snowcone: Transfer data offline or online with AWS DataSync agent
* IAM Auth is not supported by Elasticache
* Multiple AWS Site-to-Site VPN connection could provide secure communication by AWS VPN CloudHub.

- Heterogeneous Database migrations:

STEP-1

Oracle Database → AWS Schema Conversion Tool → AMAZON AURORA

MySQL Database → AWS Database migration Service → AMAZON AURORA

STEP-2

- cloud trail: Who → when → what did with resources.
  CloudTrail logs API actions (90 days)

- To improve application performance:

★ Enable DynamoDB accelerator (DAX) for DynamoDB and CloudFront for S3.

DAX is a fully managed, in-memory cache for DynamoDB from milisec to microsec.

cloudfront is a delivers static and dynamic web content, video streams and APIs around the world.

- Redis for DynamoDB is real-time transactional and real time analytics.

Diff. Amazon Kinesis Data Streams and SQS:

Kinesis: - Ability for multiple app. to consume same stream
- Ability consume records in the same order a few hours later
- Routing related records and ordering of records.

SQS:
- Messaging semantics and visibility timeout.
- Message delay.
- Dynamically increase throughput at read time.
- Ability to scale transparently

Amazon Neptune: - Highly interactive graph queries with (Social Networking) high throughput to bring social features into your app.
- Quickly sets of user-profiles and interaction to build social networking
- Graph database service for storing billions of relationship and queries in milliseconds

- VPC Sharing (Resource Access Manager) allows multiple AWS accounts create their app. resources (EC2, RDS, Lambda etc)

- VPC owner shares one or more subnets with each other.

- By default, the root volume for an AMI backed by Amazon EBS is deleted when instance terminated.
However Non-root EBS volumes remain available.

- Network Load Balancer operates at the connection level (Layer-4) and can not be used route traffic based on the content of the request.

	NAT GATEWAY	NAT INSTANCE
Supports port forwarding	✗	✓
Can be used as a bastion server	✗	✓
SecGrp can be associated	✗	✓

- Amazon GuardDuty: Threat detection, continuously monitors for malicious activity. Analyze AWS data sources;

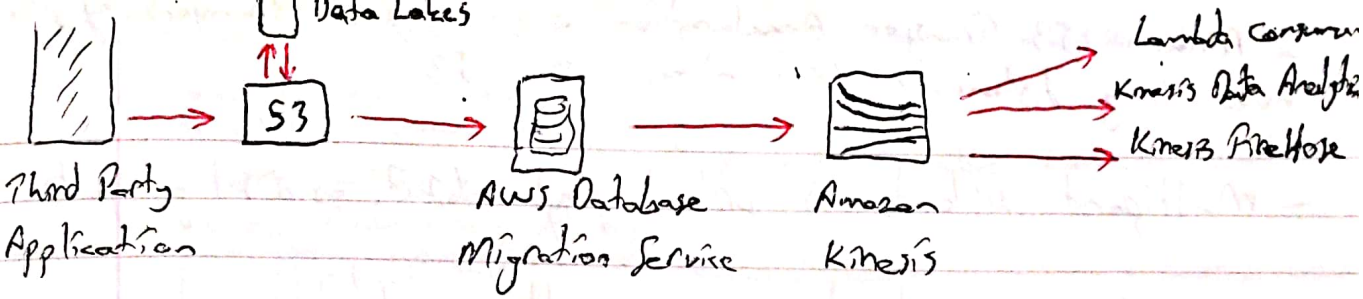
- AWS CloudTrail Events - VPC Flow Logs - DNS Logs.

- AWS S3 sync command: Copy objects b/w S3 buckets

- Amazon FSx for Lustre provides process of "cold data" on S3 and "hot data" distributes
- It is high performance file system.

- AWS Global Accelerator fit non-HTTP, such as. UDP, IOT (MQTT), Voice over IP

- CloudFront supports HTTP/RTMP



Amazon Redshift Spectrum: Query and retrieve structured and semi structured data from S3.

Amazon Athena: Query to analyze data directly in S3 using SQL, it is serverless, no infrastructure to set up, manage, only pay queries to run.

Allow Lambda Execution role to access S3 bucket:

Step 1: Create IAM role for the lambda

Step 2: Configure IAM role as Lambda function's execution role

Step 3: Verify S3 bucket policy doesn't deny access and execution of Lambda function.

A Network Load Balancer, route the traffic to the instances by using "Private IP" Address, Not "Public IP" or "Elastic IP" or "Instance ID."

Launch Template is similar to Launch Configuration, Also Launch Temp instead of Launch config. allows to have multiple versions of template, to scale performance and cost.

- FIFO Support up to 3000 messages/sec with batching
  " " up to 300 " without "
- The name of FIFO must end with .fifo suffix.

- Amazon S3 Transfer Acceleration enables fast, easy, and secure transfers of files over long distances b/w clients and S3.

- Multipart uploads is upload single object as a set of parts.

- AWS Global Accelerator improves the availability and performance of applications but it will not help accelerating file transfer speed to S3.
- It uses IP (static) addresses, migrate up to two /24 IPv4 addresses ranges.

- AWS services can be used for buffering or throttling to handle traffic;
  Throttling: limiting the number of request
  Buffering: ~~queue~~, areas, assistant, temporary

  - API Gateway → throttling.
  - SQS → Buffering.
  - Amazon Kinesis → ingest, buffer and process streaming data in real time.

- Two types VPC Endpoints;
  Interface Endpoints: ENI with Private IP
  Gateway Endpoints: You specify target in your route table.
  Gateway Endpoints supported; S3 and DynamoDB.
  ↳ Not for a private service.

- EBS Volume Encryption;
  * Data rest inside the volume
  * Data moving b/w volume and instance
  * Snapshot created from volume

  } Encrypted

- Autoscaling Lifecycle Hook puts the instance into a wait state until timeout periods end.
  Instance remain wait state 1 hour (default), ASG continues launch or terminate process.

- S3 can publish notifications for the events;
  - New object created
  - Object removal
  - Restore object
  - Reduced Redundancy Storage
  - Replication Events

  } Events invoke Lambda Function

Charge Price ECS : a ECS with EC2 : Used EC2 and EBS Volumes
b ECS with Fargate : CPU and memory resources

- AWS Global Accelerator can shift traffic gradually or once b/w blue and green environment.

Amazon Macie : Discover and protect sensitive data in S3

Guard Duty : Monitor any malicious activity on data in S3

- EC2 Reboot CloudWatch Alarm Action used to reboot instance

*** Importing Data into MySQL DB Instance;

There are diff techniques depends on source of data, amount of data, whether import is done or is going.

* If source Existing MySQL on premises or on EC2; Create backup and store on S3 then restore back up file to new RDS DB instance running MySQL.

* Copy Existing Database, one time or ongoing, minimal down time; Use Database Migration Service

* Existing MySQL DB instance; create read replica for one-time creation of new DB instance

* Existing MariaDB or MySQL, small amount; copy data directly to MySQL using command line

- The AWS Storage Gateway Hardware Appliance;

Physical configured server for on-premises deployments.

- File Gateway
- Volume Gateway
- Tape Gateway

} File Gateway suitable mounting via NFS and SMB protocols.

Volume Gateway: Used block-based storage.

---

* Cloudfront geo restrictions deny access blocked countries.

* cloudfront can use to cache files in edge locations to improve the performance of the webpages.

For the high availability for web tier and database tier:

- For Web tier; Auto Scaling Grp across multiple AZs

- For database tier; Migration from EC2 to RDS to take advantage of Multi-AZ functionality.

- Microsoft SQL server from on-premise server can directly migrate into Amazon RDS.

- Geolocation Routing: Based on the location of user

- Geoproximity Routing: Based on the location of your resources.

- Developer stored database username and password in a config file on the root EBS.
  This is not secure way. Best practice;
- IAM Role permission to access database and attach this role to the EC2.

- Amazon CloudFront with a custom origin pointing to the on-premises servers able to cache content for dynamic websites

---

- SQS is service, decoupling app, reducing interdependencies
- SQS is pull based, not push based.
- SQS supports resource-based policies. (Send message permission to partner AWS accounts.)

- Amazon RDS creates SSL certificate and installs the certificate on the DB instance.

Storage Gateway: On-Premises → AWS

1) File Gateway: (NFS/SMB) → Encryption in Transit (Direct Connect or Internet)
2) Volume Gateway: (iSCSI)
3) Tape Gateway: (iSCSI VTL)

★ Hybrid cloud storage services

★ There is no direct create or copy b/w EBS and S3

★ AWS recommend using separate queues for prioritization

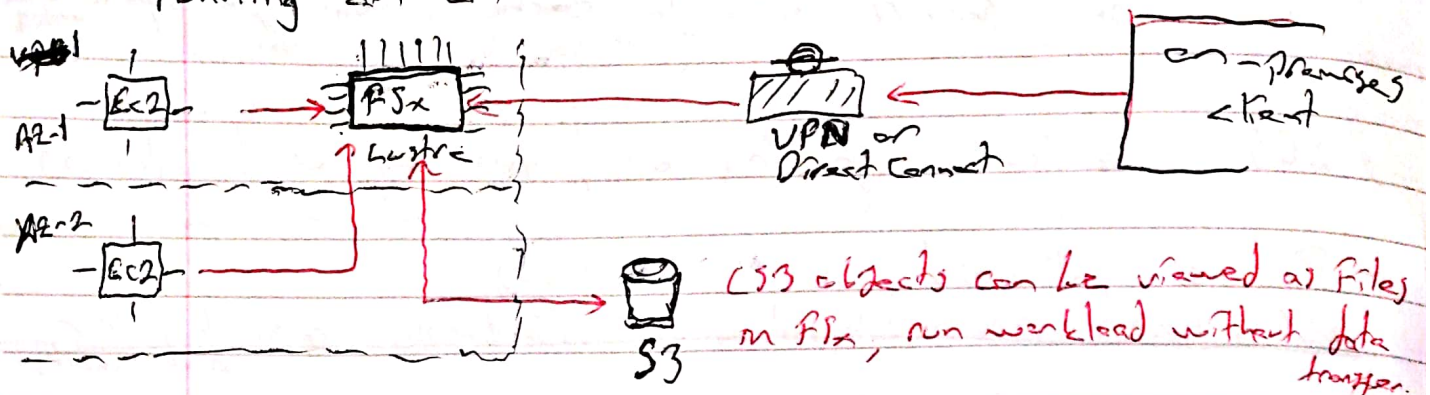
S3 - Encryption:

- Server-Side Encryption: - Protect data at rest. (Not metadata)
  - Encrypt each obj. with a unique key.

1) S3 managed keys: Unique object keys, Master keys, AES 256
2) KMS Managed keys: Customer Master keys, CMK (Customer Managed Key)
3) Client provided keys: (SSE-C), Client managed, Not stored on AWS

- Client-Side Encryption: Object encrypted before uploaded.
  1. Customer master key (CMK) from KMS by AWS.
  2. Client managed keys.

- Amazon FSx for Lustre: (HPC) High Performance Computing running on Linux instances.



- AWS Transit Gateway connects VPCs and on-premises networks through a central hub.

- Origin Access Identity (OAI) restrict access to content in S3 but not on EC2 or ELB.

Amazon ECS Service Auto Scaling: ECS uses as a service to scale tasks. based on target value for a specific metric. as reported by cloudWatch alarm breached

- For the "cost-effective" requirement, in the options choose AWS Lambda, S3, cloudfront but EC2, ELB ongoing cost. ×$$ ×$$

- After creating a file system, by default only root user has read-write execution permissions.
For the other users, root user must grant them access.

★ You can not transition to Standard IA to S3 standard within 30 days.

- A Kinesis data stream is a set of shards. Each shards contains a sequence of data records.

- Amazon DynamoDB supports near-real time performance and millisecond responsiveness.

DynamoDB — near-real time, milliseconds response

SQS — Not near-real time.

Redshift : Not millisecond responsiveness.

- The data stored both EBS and RDS must be encrypted at rest by AWS KMS keys.

- AWS WAF (Web Application Firewall) available on ALB
  Not on NLB, and it can protect against XSS attacks.

★ Amazon EFS establish IAM role allows Fargate.
S3 uses Rest API, Not EFS
EBS
FSx for Lustre } Not connected Fargate.
EFS — Not (S3)

- MySQL need to access a service on the internet and maximum secure and minimum operational overhead is.
  NAT Gateway.

- CloudWatch agent to collect both system metrics and log files from EC2 and on-premises.
- Agent support both Windows, Linux

- Amazon Aurora Replicas independent endpoints and no caching. Replicas create Multi-Zone and total 15 Replicas across Zones.

- For high performance / low latency EC2 Instance Stores also cost-effective.
  → S3 not High Perform Computing

- Lambda; has a maximum execution time of 900 sec, (15 min)

- API in a your VPC can
interface VPC Endpoint.

- This configuration powered by AWS PrivateLink, do not need IGW, Nat Device, VPN or Direct Connection nor public IP.

- Another option VPC Peering

- Amazon FSx for Windows file use both Windows and Linux instances.

- You can not use Amazon EFS for Windows instance.

- CloudWatch Container Insights, collect, aggregate, summarized metrics, and logs from containerized application and microservices

- Snowball Edge can transferring data (offline) b/w your local env. and the AWS Cloud.
Snowball Edge local processing and edge computing.

→ Manages all the infrastructure, provisioning, managing, monitoring and scaling your computing jobs.

AWS Batch Multi-node parallel jobs, enable run single jobs span multiple EC2 instances.

Run large scale, tightly coupled, HPC app, without need launch, configure, manage EC2 resources. directly.

most efficient approach to deploy resources

- AWS Step Functions; A workflow orchestration service, not a message bus

- Athena; ad hoc data discovery and SQL querying
- Easily query encrypted data and write encrypted result back to S3 bucket.
- Redshift Spectrum; more complex queries where large number of data lake users run concurrent BI and reporting workloads

- Amazon Cognito identity pools: provide temporary AWS credentials for users (unauthenticated) and received token.

- DynamoDB can scale without downtime and minimal operational overhead. often used eCommerce solutions

---

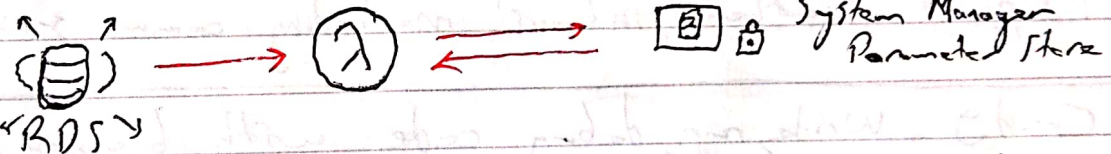
- VPC Endpoints: Connect VPC to AWS services. and it powered by AWS PrivateLink not requiring NAT, VPN, Direct Connect

Two types of VPC Endpoint: Interface Endpoint, Gateway Endpoint

API Gateway, cloudformation, cloud Watch ⇓ Security Groups ⇓ ENI with a Private IP

S3, DynamoDB ⇓ VPC Endpoints Policies ⇓ Route Table.

- Create trail in Cloud Trail in management account with organizational trails option enabled. Member accounts can see trail but can't modify, delete, access logfiles in S3



Lambda ~~for~~ authenticate to MySQL, need credentials store in Parameter Store.

A RAID array uses multiple EBS Volumes to improve performance and redundancy.

Raid 0 : Performance is important, loss of single volume results complete data loss,

Raid 1 : Fault tolerance is important

- AWS allow "test penetration" for some resources without prior authorization.

- Events in Cloud Trail: 1) Data Events (Data plane OPP)
2) management Events

- Amazon Polly → Text to lifelike speech
- Amazon Transcribe → Speech to text

- Textract: Printed text, handwriting, forms, tables to Read, extracts.

- Rekognition: Identify image, scenes, objects.

- MQ: Message Brokers, set up maintenance of message.
- AWS. AppSync: Develop GraphQL APIs to the data sources. DynamoDB Lambda
- AWS App Mesh: Networking to services communicate eachother
- Cloud Map: Microservices to locate one another, by service name and locations.
  Microservice need connect API but needs locations and names.

- Pinpoint: Outbound, inbound marketing comm. service.

- Cloud9: Write, run, debug code with browser.
  It is packed Java, Python, PHP... no need installation.

- Launch wizard: Sizing, configuring, deploying AWS resources for third party application

Storage Types

- CloudFront which is a Content Delivery Network (CDN) that caches content to improve performance. with a custom origin pointing (S3, EC2, ELB, Route53)

- RDS instance create → Need to be publicly accessible
  → and Sec. Grp. need to assigned.

- When EBS volume encrypted with a custom key, you need share it with the account and modify permission on snapshot.

- You can not share encrypted volumes created by CMK key. and you can not change the CMK key used to encrypted volume

---

- Athena serverless, easy to analyze data in S3 by SQL you pay only queries you run.

- Updating Stacks in Cloud formation;

  1) Direct update 2) Creating and executing change

- MySQL authentication is handled by AWS Authentication Plugin with AWS provided IAM

- RDS Replication: Nc Continious and Scheduled Replication
  - Synchronous Replication: Physical, logical replication
  - Usynchpounous Replication: Used for Read Replicas.

- CloudWatch: Performance monitoring
  Trusted Adviser: Current usage, limits

Lambda function metrics, lambda tracks: (CloudWatch)

1) Number of requests
2) Latency per request
3) Number of requests resulting in an error.

- To enable your Lambda function to access resources inside VPC must provide configurations;
  1) VPC Subnet IDs 2) VPC Security Group IDs

Alias Records used to map resource in your hosted zone to;
- ELB - API GW - cloudfront Dist - Elastic Beanstalk - S3

- ASG can be edited once created
- You can attach running EC2 to ASG.
- If adding instances result exceeding max capacity of ASG request will fail.

- AWS Step Functions; Orchestrating serverless work flows.
- Amazon API Gateway with Lambda; Executing business logic.

Amazon CloudFront, you can enforce secure end-to-end connections to origin servers by using HTTPS.
Field-level encryption ~~allows~~ adds an additional layer of security lets you protect specific data.

AWS IoT Core is a managed cloud service lets connected devices, easily and securely.

SQS: 1) Long Polling: - Uses fewer requests and reduces cost
Eliminate empty responses
- Eliminate false empty responses.
- Waits until message available in the que before sending a reponse

2) Short Polling: - Do not wait for messages to appear in the queue
- It is default, ReceiveMessageWaitTime is 0
Return all messages

---

* Enhanced Networking provides higher bandwidth, higher packet per second (PPS)

ELB Feature: - Connection Draining provides for connections to close cleanly.

- Sticky Sessions: Uses cookies
- Proxy Protocol: Identify the IP address uses TCP
- Deletion Protection: Protect the ELB from deletion.

AWS Serverless Application Model (SAM) is an extension of CloudFormation is used to package, test and deploy application

---

Default VPC Sec. Grp: Deny ALL Inbound and allow outbound traffic
Default ACL: Allows All inbound/outbound traffic.
Custom NACL: Denies " " ".

AWS ~~B~~ Access Logs on an ALB process the log files using a hosted Hadoop service. EMR is a web service enables business, researchers, analyst and developers process vast amounts data.
EMR utilizes a Hadoop framework on EC2 and S3.

- POSIX permissions allows you to restrict access from hosts by user and group.

- EFS Sec. Grp. act as a firewall, rules add define the traffic flow.

- Elastic Beanstalk used to deploy and manage app. on AWS.
- It is not suitable for long process, (EC2 can be for long)
- Elastic Beanstalk "capacity provisioning and load balancing of website."

- Through the "Range" header in HTTP Get Request, a specified portion of the objects can be downloaded instead of whole objects

---

- Cloud Trail used to monitor API activity and delivers logs files to S3.

* ELBs can only balance traffic one region, not across multiple regions.

* Sharing AWS resources: (AWS Organization)
  - Only own resources can be shared.
  - Sharing needs to enabled with master account in AWS organization.

---

* Cloudfront Origin Access Identity used to control access to content in S3 bucket.

  Object ACL's provide granular control on each file in S3...

Elastic Beanstalk supports the deployment of web app. from Docker containers.

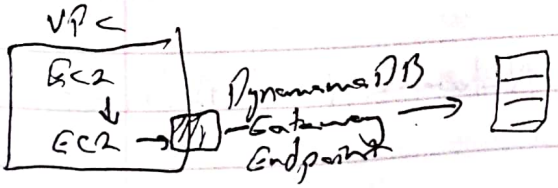
- VPN is for an IPsec connection. AWS Direct Connect is for private connection with high bandwidth throughput.

Weighted Routing Policy: Testing new versions of software or Blue-Green deployments. It lets you associate multiple resources with a single domain name- or sub domain.

AWS Config: AWS Resource Configuration
- Get a snapshot of current config.
- Receive notification when resource created/modified/delete

AWS CloudHSM enables you to easily generate and use your own encryption keys. Are isolated on their own encryption module

KMS is a shared, your keys in their own partition of an encryption module share with other AWS customers.



- By the route table entry to endpoint.

★ Microsoft SQL server database migrate Amazon RDS
- AWS Database Migration Service ★ migrate directly to RDS.

★ EC2 is better than EBS for maximum performance

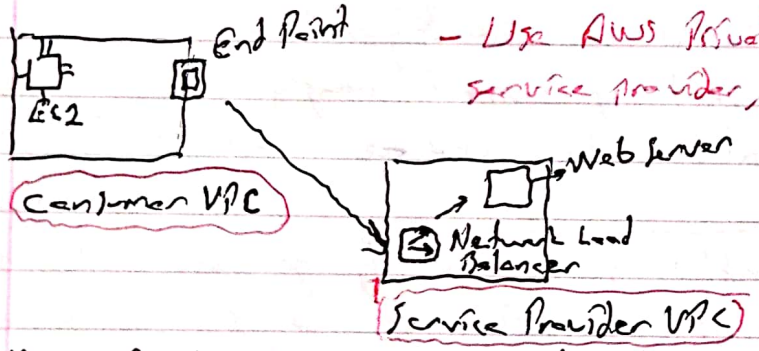
★ DynamoDB is best for near-real time performance with max. responsiveness.

★ Instance Store best for high I/O performance and very low latency.
EBS is good for fault tolerant, data persist.

★ You can create static website by S3 with custom domain name but to connect using HTTPS you need cloudfront uses S3 as the origin.

- Read Replica for RDS, there is no Read Replica DynamoDB.
- Cross Region replication is S3 concept not for not for dynamic data.

- Service Provider Model:



- Use AWS PrivateLink - Network Load Balancer service provider, PrivateLink Endpoint created in consumer VPC.
★ VPC's can be shared among multiple AWS Accounts.
★ To restrict access instance of others, PrivateLink to create endpoint for the app.

- Web Application Firewall (WAF) is available on ALB, in a VPC to protect website and website service. (XSS Attacks)

- You can not use WAF with Network Load Balancer.

- Redis for long complex queries, also it improve performance
- But it is not serverless, for repeat queries by caching result.

* To prevent or control users to reach website running on EC2, on CloudFront (WAF or pre-signed URL, / signed cookies) and origin access identity (OAI) to reach S3.

With WAF you can create ACL that includes IP restrictions

Elasticache Redis: in-memory database that supports data replication.

Elasticache Memcached: Not in-memory database.

RDS PostgreSQL and MySQL

Amazon Macie: Detecting and protecting sensitive data in S3

Amazon GuardDuty: Detect and remediate compromise of services.

* RDS use snapshot for the backup.

Parameter Store: provides secure storage for the keys, passwords, IDs, AMI, license codes

* Launch RDS instance with encryption enabled, logs and backups automatically encrypted.

* S3 manages encryption and decryption automatically when Amazon S3 server side encryption (SSE)

* AWS Config conformance packs: set of evaluations and remediations across in AWS Organizations.

Trusted Advisor online tool with real-time guidance provision resources.

- EFS not supported Windows Instances.

- AWS Code Commit is a version control service in AWS.

- EFS : * POSIX permissions to control access from hosts by user or group.
  * EFS Sec. grp to control network traffic.

- AWS Batch eliminates need to operate third-party commercial, it is manages infrastructure for provision managing, monitoring and scaling.