Accn and Administration

- AWS SSM System MANAGER
  3rd party Workload → Syst MGR Run Command

(1) System Manager → SSM Session Manager
↓
Log Data → (S3) | Cloud Watch

(2) Run Command (Run script)
Trigger → Cloud Event bridge → 3rd Party → Run Command
Send Notification to SNS } Patch

(3) Patch Manager → Patching (on Managed Nodes)

(4) Maintenance Window → Main (Schedule) → Run → EC2

(5) Automation → Simplify common Maint task
Ex → Restart instance, Create AMI, EBS Snapshot
Automation Runbook (Rule based → SSM Document)

- AMAZON Simple Email Service [SES]
  - Fully Managed, secure, Global
  - Use case: Marketing Email !

Amazon Pin Point.
2 way communication (Inbound/outbound)
Msg / Email / Voice / Inapp Msg

Security Hub ↑ Event Bridge → EC2 and VPC only

Amazon Inspector (Automated Security Monitoring)

↓

EC2

↓

AWS System Manager (Remote SSH session)

↓

Secure Shell

AWS Macie

- ML + Pattern Matching
- Identify Sensitive info (personal info)

AWS Secret Mgr → Password + Rotation (RDS)

AWS Certificate mgr → Provision, Manage, deploy TSL certificate

Free ↑ API Gateway
- Edge optimized
- Regional (Same Region)
- Private (VPC)

AWS Web App Firewall (WAF) → ALB | API GW | Cloud Front | Also for access content

layer 7 = HTTPS

- Regional

DDOS

↓ ↓

AWS Shield | AWS Shield Standard | $3000 / Month

AWS Fire Wall Manager
- Org firewall

Amazon Guard duty (ML)
- Account threat protect

Setup = Eventbridge
- Crypto currency attack

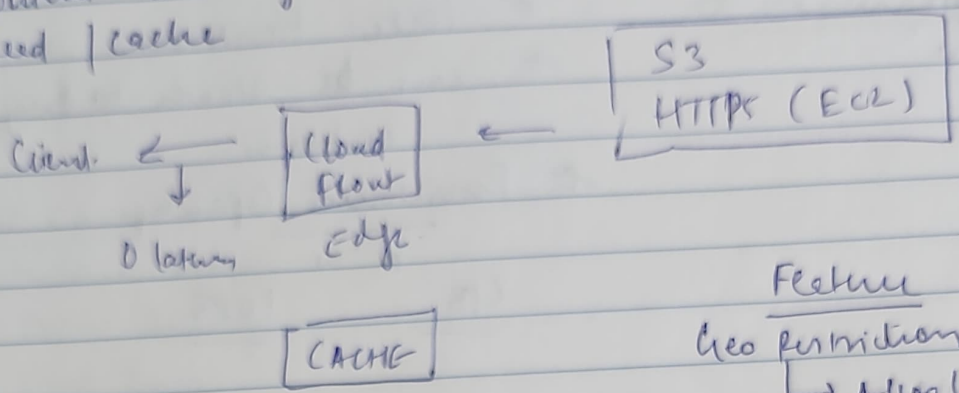
AWS X-RAY → Insight gathering
Trace application
S (SNS) (EC2) (Gateway) (λ) (ECS) (Beanstalk)
SQS

AWS AppSync → GRAPHQL / front end data fetching

AWS org
Restriction → Service control policy (Root)

AWS Cloud FRONT [DDOT Protection]

- Content delivering Network
- Read | cache



Feature
Geo Restriction
→ Allow List | Blocklist

Website
Static Content → Cloud Front
Dynamic Content → Cross-Region Replication

AWS Global Accelerator [Elastic EC2, ALB, NLB, Public/Private]

INTERNAL network to Application

Anycast IP → Edge location → Application

- DDOS Protection (Both have DDOS)

Global Accelerator VIS → Application
- Gaming
- IOT
- Voip

Cloud Front → Website (Static Content) Cache → Image/video. API etc

ELASTIC BLOCK STORAGE

NETWORK DRIVE (USB)

↓

"Specific Zone"

EBS Volume (USB)

- locked to A-Z
- Can be attach to Any EC2 instance.
- Provisioned Capacity
  - GB
  - IOPS

EBS SNAPshot → copy of EBS Volume

- Snapshot Archive — Restore 1-3 day
- Recycle Bin — retention — 1 - 1year
- FAST Snapshot Restore (FSR) — No latency

Network DRIVE → EC2 INSTANCE STORAGE

- Better I/O — Risk of Data loss

EBS Volume TYPE

- SIZE
- Throughput
- IOPS

SSD (gp2) → HP + Workload
SSD (io1) → low latency + HP
HDD (st1) → Fay Acess
HDD (sc1) → lowest cost

IOPS → Provisioned input Outputs for,
: → Database Workload

EBS Encryption → KMS (AES-256)

Data At Rest | Flight | Snapshot | Volume.

Elastic File System (Network file system) on EC2

- Highly Available
- Scalable
- Expensive

USE CASE
- content mgt
- Data Sharing
- Word Pres

EBS vs EFS

1 instance

100 of instance
Word Pres
Linux (POSIX)

EFS-IA → Cost saving

AMAZON APP FLOW

Software as a Service [Salesforce, Service Now] ⟷ AWS S3, Redshift

6 Pillar → AWS well Architected Tool → Advise!

1. Operational Excellence
2. Security
3. Reliability
4. Performance Efficiency
5. Cost optimization
6. Sustainability

TRusted Advisor

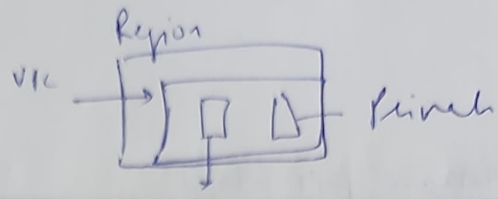
Basic Plan → Service Limit, S3

Enterprise
- Cloud watch
- 5 Category

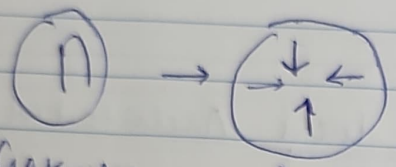
5 Category advise

- Cost optimization (P)
- Performance
- Security (P)
- Fault tolerance
- Service limit

VIRTUAL PRIVATE Cloud



Internet Gateway → Connect VPC to Public Internet
→ Horizontal Scale
→ Edit Route Table



Gateway Router

BASTION HOST → Always in Public Subnet and Connects with Private Subnet

NAT (Network Addrss TRANSLATION)
EC2 instance in Private Subnet ⟷ Internet

NAT GATEAWAY (AWS Managed)

NAT GW - with high availability → Resilient with single AZ

Network Acess control list (NACL) = Firewall to Subnet

| NACL | Subnet
| NACL → Blocks Specific I|P.

NAT instance → Fail over Management

Security GRP	NACL
Instance Allow Stateful	Subnet Allow/block Stateless

Stateful → Return traffic Regardless of Rule

Stateless → Return traffic based on Rule

VPC Pairing • 2 VPC (private connect) Using AWS Network

• Must not have overlaping CIDR

VPC Endpoint → Publically exposed Service → AWS private Network

Interface Endpoint (S) | Gateway Endpoint (Free)

↓ | ↓

Private Link | S3 | DynDB

VPC Flow log → IP address Traffic

↓

CloudWatch / S3

↓

Amazon Athena (Query)

↓

Quick Sight

Site to Site VPN

↙ ↘

Private GW | Customer GW

Cloud formation → Infr as code (IAC)
Declarative (Template) to create Infrastructure
Right ORDER + Exact Configuration

Support almost all AWS services

Activity
Create
Delete
Program

AWS Budget → Usage Alert

AWS Trusted Advisor (Business / Enterprise account)
best practice auditing tool
- Cost optimization
- Performance
- Security
- Fault Tolerance
- Service limits

AWS Control Tower

AWS Health

Cost explorer → AWS cost / Usage over time

- Custom Report
- Forecast → 12 Month Report

Amazon Elastic Transcoder

Media File → format friendly for Device (Phone | Laptop)

AWS Batch

- 100,000 computing Job
- Cost Optimization
- ~~Run on Docker~~ BATCH Job = Docker Image Run on ECS

Batch	LAMBDA
No Runtime limit	Time limit
EC2 | EBS	Serverless

MACHINE LEARNING

1. AMAZON REKOGNITION

Object / People / Text / in Image / video using ML

Use case
- labeling
- Content Moderation
- Text detection
- Face search

Manual review → Amazon Augmented AI (A2I)

2. Amazon Transcribe

Speech → Text

Automatic Speech Recognition (ASR)

Remove → Personal identifiable Info. Redaction

3. Amazon Polly

Text → Speech

★ Speech Synthesis Markup Language

4. Amazon Translate

English - French

5. Amazon lex - Connect

lex → Alexa
- Chatbot (NLU)

Connect → Virtual Contact Center.

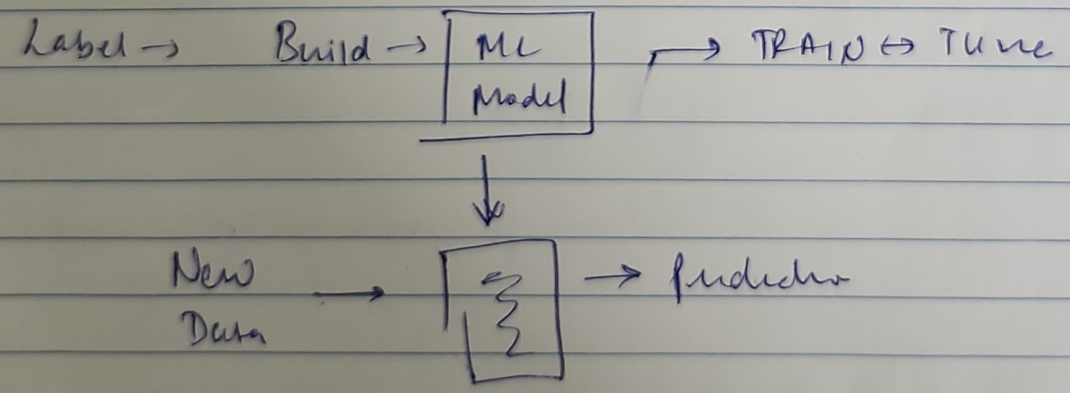
80% cheaper than traditional Contact Center

6. Amazon comprehend
- NLP
-

Medical (Personal Health Info PHI) → Pelod

7 SAGE Maker

Developer / Data Scientist to build ML - Model



8 Forecast → Product Demand Planning

9. Amazon Kendra

- Document Search Servie
- Extract Answer from document.

10. Personalize (Recomendation System)

↓

Email Marketing

11. Amazon Textract

Extract information from document

AWS Monitoring Audit Performance

- Cloud watch
- TRAIL
- CONFIG

Cloud Watch → Metrics → Namespace
↳ CPU utilization
↳ TimeStamp

Dashboard → Metrics
↳ Custom

Near Real time + Low Latency

CW | ECS | API | Route 53
↳ Logs → S3 | Kinesis | λ

CW → Kinesis → S3 → Red Shift, Open Search
↓
Athena

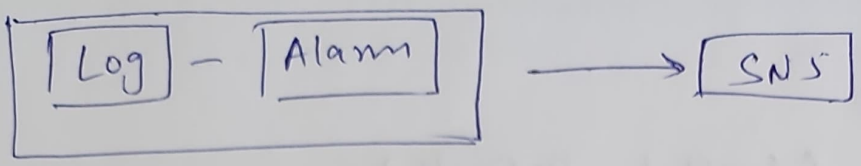
→ Cloud Watch Dashboard

Cloud Watch → Create Export Task → S3

Watch Log
↙ CW log agent (Old)
↘ Unified Agent
- System level Metrics → RAM, Proc, CPU

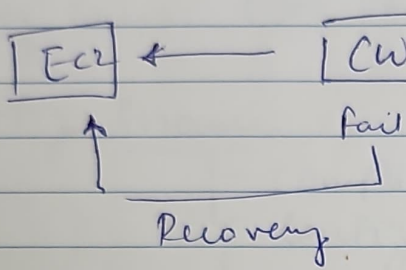
~~Alarm~~ Alarms → Trigger Notification

Alarms Target (Action)
- Stop / Terminate EC2
- Start Auto Scaling (A)
- SNS



Composite Alarm → Single Metric (AND | OR)

★ EC2 Instance Recovery



Amazon Event bridge (Cloud Watch Event)

CRON Jobs → Schedule Scripts
Event pattern

Trigger → λ | SQS | SNS

Event Bridge Rules

Event Bus | custom | Partner Event bus

★ Schema Registry → Allow to generate code for application → Structure Event Bus
★ Resource based policy → Allow / Deny.
★ CW container insight → ECS | EKS | Fargate | K8s on EC2

Lambda insight

Contributor Insight (top 10 IP address)
Application insight (Sage Maker)

CCTV

Cloud TRAIL (Enabled – Default)

✓ Compliance / Audit / Governance

log

↓

Cloud TRAIL

↓

Cloud Watch Logs

Event

Mngt Event → Read, Write

Data Event (λ/API)

Insight → Cloud Trail Insight → Detect Unusual Activity

→ Event Retention → 90 Days in Cloud Trail

→ Event Bridge – Intercept API Calls

AWS Config

Auditing | Record Compliance

SNS Notification of Any change

Config Rules (No Deny)

Config Resource
- Compliance
- Config
- API Call (Cloud trail API call)

CR - Remediation → SSM Automation

Config Rule Notification
- change
- Non compliance

Watch	TRAIL	Config
Monitoring Alerting Analysis	Record API call	Config changes Timeline of change | compliance

AWS Organization → free governance tool that allows you to create and manage multiple AWS ~~or~~ account

- Consolidated billing
- Service control Policy
- Centralize log | no one can edit | delete logs

AWS RAM

- Share Resource with other AWS Account

AWS Config → Inventory Management and control tool

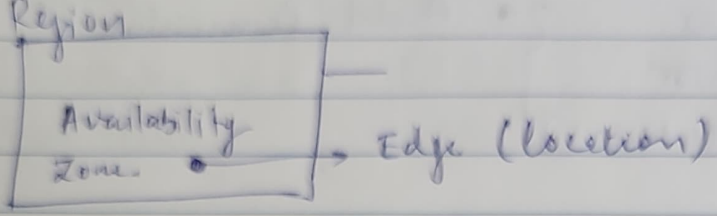
AWS Activedirectory

Managed Microsoft AD

AD Connector

Region (Selection) – {compliance; Price}

- Cluster of data centers
- Services = Region Scoped



Global	Regional
IAM	EC2
DNS (53)	Elastic Beanstalk
Cloud Front	λ
WAF	Rekognition

IAM

Root (Default) (MFA*)
User
Group
] Permission → Least Privilege Principle

Password policy
- Strong
- Specific Chars
- IAM User to change pwd

] + MFA → Google Aut (Single User)
→ Yubikey (Multi User)

Access AWS

1. AWS MNGT Console — PWD + MFA
2. CLI
3. SDK

Console → Access key = Username
Secret key = Pwd.

IAM Security Tools

- Credential Report (account-level)
- Access Advisor (user-level)

→ Audit Permission ✓

EC2 = Infra as service

Virtual Machine → EC2
Storage → EBS
Distributing load → ELB
Auto scaling → ASG

EC2 Instance type

1. Compute optimized - Media Transcoding
   Gaming | Workload
2. Memory optimized - Database | BI | Real time Processing
3. Storage optimized - OLTP - Online transaction processing
   - Relational | No Relational
   - Cache (In Memory - Redis)

Security Group (Only Allow Rules) = FIREWALL

1 Sec Group = 1 SSH

By Default
- Inbound → Block
- Outbound → Allow

EC2 Purchase option

1. On Demand → short $/second
2. Reserved
   - Reserved → Long
   - Convertible → flexible
3. Saving Plan (1-3yr)
4. Spot Instance → short less Reliable → Cost effective
5. Dedicated Host → Entire Physical Server → Most Expensive
6. Dedicated instance → NO other customer use Hardware
7. Cap Reservation → Reserved for Any duration

- Elastic IP → Fixed Public IP (Avoid)
- Placement Group
  Define { Cluster - Spread - Partition }
  - Big Data Job
- Elastic Network Interface (ENI) # EC2
  = Virtual Network Card - Specific AZ

EC2 Hibernate [Stop - Terminate]
↓ Data on Disk is intact
↓ Data is lost!

In-Memory (RAM)

Use case → Long Running processing

Limit → 60 DAYS

EC2 Instance STORAGE

1. EBS Volume = Network DRIVE (Specific AZ)

   To Move Vol → Snapshot Detach from Any A→Z

   4GB | IOPS

2. EBS Snapshot → Backup.

   Copy Across AZ

   - Archive 1-3 day
   - Recycle bin 1-1 year
   - Fast Snapshot Restore → No latency ($$)

3. AMI = Amazon Machine Image ⇒ Laptop (Dell) (Customize / Configure)

   { Public, Own, Marketplace }

4. EC2 Instance Storage → High performance (your Responsibility)

5. EBS < SSD, HDD

   Encryption

   KMS - ~~(SSE256)~~ AES 256.

   EFS → Elastic File System (Highly Available - Scalable $$)

6. EFS – Storage Class (90-1% Saving)

* Scalability.

(AutoScaling / Load balancer)

Vertical

Size
Database
(RDS, Elastic Cache)
Limit

Horizontal

> No. of instance
> Web application
EC2 (Easy scaling)

↓

High Availability = Avail Zone

* Load Balancer

Traffic to Multiple Server

* Elastic Load Balancer (AWS Managed)

↳ EC2 / ASG / ECS
↳ Certificate Manager
↳ R-53 / WAF / Global Accelerator

* Health Check (Port and Route)

HC = 200 (Not Okay)

Type of ELB

"Sticky Affinity"

Application
Micro (Docker / ECS)
Target group
+ Website

1. Classic → HTTP is / TCP / ICL
2. Application → Websocket
3. Network → TCP / TLS
4. Gateway → IP Protocol

↓

Network / Firewall

ters
Gateway

Sticky Affinity → Same Client directed to Same Instance

Cookie

Custom

Application

AWS ALB APP

→ Duration Band

APP

AWS ALB (ALB)

AWS ELB L (CLB)

Classic

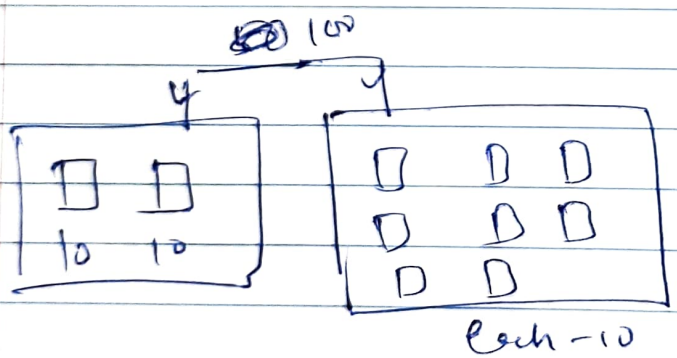
Cross Zone load Balancing

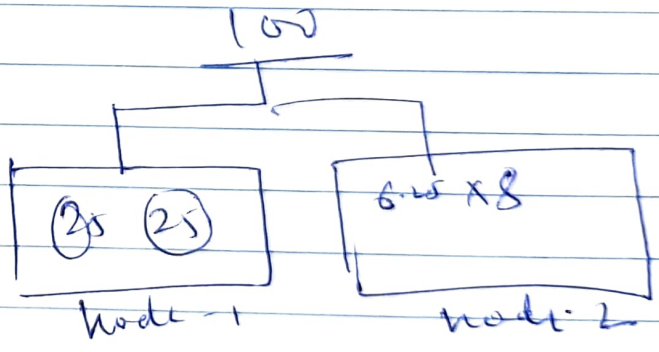
With

Without

(Even distribution)

Node Distribution





(146)

RDS → Relational Database (SQL)

- Postgre
- MSQL
- MariaDB
- ORACLE
- Aurora

NO SSH

STORAGE (S3)

99.999999999%

1. S3 Standard - low latency | High throughput
   - 2 concurrent failure
   - Big Data Analytics
2. S3 standard - Infrequent Access
   - low cost
   - Secondary backup
   - Disaster Recovery | Backup
3. 1 zone - IA
4. Glacier - Instant Retrival (90 Days)
   - Milisecond Retrival
5. Glacier - Flexible Retrival (90 Days)
6. Glacier → Deep Archive (180 Days) → long term storage
7. S3 Intelligent Tiering

Moving between S3

Manual

"Lifecycle Rules"

Transition Action → Move

Expiration Action → Delete

S3
- Infinite Scaling
- Backbone of Website

Use
- Backup
- DR
- Hybrid cloud Storage
- Software delivery
- Static website

Best practice
1. Version Bucket
2. Allow Public Read.
3. Proper IAM Permission

S3
File Repository

{Object} → Key : full path + obj Name

Max obj size = 5TB

- Metadata
- tag | ~~Uid~~. Version Id

Security
- Userband → IAM (API GW)
- Resource based
  - Bucket policies
  - Object Access Control list
  - Bucket Access Control list

Bucket policy → JSON
- Persona
- Effect ✓/✗
- Action

Replication
- Cross Region Replication CRR
  - Compliance / low latency / Replica across
- Same Region Replication SRR
  - Live Replication from Test to Prod env.

- No chaining Replication

S3 Event Notification — SNS | SQS | λ

Performance

3500 Put | Copy | Post | Delete
5000 Get | Head

✓ Multipart load (Parallelize load)
✓ S3 Transfer Acceleration (Fast and Private)

Server side Filtering → Retrive less data (SQL)
- Row
- Column
- ⊖ less CPU cost (Client Side)

S3 (Select) → 400% faster
→ 80% cheaper

Encryption
- Server Side
- Client Side

AWS λ ⇒ 15 Min Execution-time

API Gateway ↕ WAF → Security
- DDOS

AWS Batch

- Batch Computing Workload (EC2 | ECS | Fargate)

Lambda vs Batch

15 Min Time
Fully serverless
10 GB RAM

Docker

Amazon MQ

Support Apache ActiveMQ
Rabbit MQ

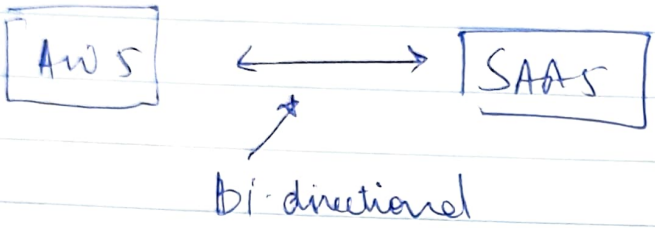
- Existing Application
- Private Network

AWS Step Function → State Machine [Every single step = Task]

- Serverless
- Orchestration

Standard Express

Amazon AppFlow



- Aurora Serverless Database use Aurora Capacity Units to set scaling unit

Redshift

✓ 15 PB

- Big data Application
- Relational

✗ highly Available
need separate deployment.

Elastic Map Reduce

✓ ETL TOOL

Kinesis

Real time data processing

DATA Stream

DATA Firehouse

Real time → 60 second (S3 | Redshift | Elastic search)

Need config Plug n play

AWS Athena

S3 ← SQL processing

AWS quicksight → BI

AWS Glue

ETL

AWS Data pipeline

- ETL
- Fully Managed

★ Amazon Redshift spectrum → Run SQL queries on unstructured data, NO ETL required

Kinesis Data Analytics allow you to Transform data using SQL.

Amazon Managed Streaming for Amazon KAFKA (MSK)

- You Manage servers.

Amazon Open Search

Run and search various Analytics engine

- Logs

CONTAINERS

ECS → All in AWS + Simple (Preffered)

EKS → Open Source Kubernetes + Configuration Required
↓
Can Run on premise

fargate = { ECS | EKS } ~~&~~ Linux Only workload.

Env

ECR → Elastic Container Registry
~~&~~ Managed Container Registry

ECR Public → Public Image Repository

Container Image → Docker file

Automatic Key Rotation

AWS generated AWS Import

AWS KMS → Key Management Service

∫ [EBS] [S3] [RDS]

- Controlling Keys
- Customer Master Key - CMK

HSM → Hardware Security Module (Physical computing)

CloudHSM → Generate / use own key for cloud.

- No automatic key Rotation

Secret Manager

Store / encrypt and rotates your Database Credentials

RDS
Non RDS

(free) Parameter Store → AWS System Manager

★ Password, database string, AMI, ID's and Lisc code

AWS Certificate Manager

→ Create, Manage and deploy public and private SSL certificates for use with other AWS Service

Audit Manager

- audit AWS usage [PCI | GDPR]
- Automated Service → automated Report.

AWS Artifact

Compliance Related Information

- SOC
- Payment Card Industry PCI
- GDPR
- ISO | HIPAA

Amazon Cognito → AppSync

authentication / authorization and user Management for your web and Mobile App

User Pool — Identity Pool → Access to other AWS service

↓

Sign in | Sign up

Amazon Detective

Analyze, identify root cause of potential security issue or suspicious activities

AWS Security Hub

Single place to view all security updates from Amazon Guard duty, Amazon Inspector, Amazon Macie and AWS Firewall Manager.

Cache

↙ → Elastic Cache → Any database

DAX

↓

DynamoDB