Created by: Filipe Braga linkedin.com/in/filbraga/

Management & Governance

Organizational unit (OU) → Organizations (aaaaaa) → (SCP) Service Control Policies

Apply:
- Users (also root)
- Roles

Don't Apply:
- Master Acc

"My Advisor is PerFaCSS"

Trusted Advisor — Checklist

Per Fa C S S

Insight & checklist → Performance, Fault tolerant, Cost, Security, Service limits

"Well PORCSS architecture"

Well-Archtected — Review your architectures

P O R C S S

Health Dashboard — AWS service status

Personal Health Dashboard → may impact you

resource change hist

Config — Config & Compliance Over time

Service Catalog — Self-service products pre-defined

perform. / evnt / alert

CloudWatch — Metrics Dashboard

account activity

CloudFormation — IaaC — Deploy stacks

CloudTrail — Record API calls

Performance Efficiency → Advanced technologies, Global in minutes, SLS architectures, Experiment more often, Mechanical sympathy

Operational Excellence → Operations as code, Document code, Make frequent, small, reversible changes, Refine operations, Learn from and Anticipate failure

Reliability → Test recovery, automatically recover from failure, scale horizontally, stop guessing capacity, automate changes to infrastructure

Cost Optimization → Pay only for what you use, measure efficiency, analyze expenses

Security → Traceability, Layers, Protect data

Sustainability → Understand Impact, Reduce amout of energy

7 Core Checks
- S3 Bucket Permissions
- SG - Specific Ports Unrestricted
- IAM Use (one IAM user min)
- MFA on Root Account
- EBS Public Snapshots
- RDS Public Snapshots
- Service Limits

Full Checks
- Ability to set CloudWatch alarms when reaching limits
- Programmatic Access using AWS Support API

Cloud Adoption Framework (AWS CAF)
- Business - Strategy Management
- People - Workforce
- Governance - Risk Management
- Platform - Architecture
- Security - Protection
- Operations - Observability

Compute

Instance = Amazon Machine Image (AMI) (Linux, macOS, Windows) + Instance Type t3.micro + Network Settings VPC / SSH / HTTPs + Security Group (Firewall) + Storage 1× 8GiB gp3 + User data Bootstrap Script (OPTIONAL) + Role

build, test and deploy

EC2 — Elastic Compute Cloud (60s)

EC2 Image Builder — Automate creation of AMI

Lambda — Virtual function (SLS, Event-Driven)

ASG — Auto Scaling Group

Outpost — on-premises AWS Infrastructure

Batch — Large data jobs (EC2)

network traffic logs → Flow logs

private access to AWS Services → Endpoints

fixed public IPv4 → Elastic IP address

Connect two VPC → Peering connection

Stateless, subnet rules for inbound and outbound → NACL → Network access control list

Network Address Translation → NAT gateway

Give internet access to private subnets → provide Internet Access → Internet gateway

Public subnet

Private subnet

Route table (172.16.0.0, 172.16.1.0, 172.16.2.0) → Set of rules that determine where network traffic from your subnet or gateway is directed

Storage

S3 — Simple Storage Service (Glacier)

EBS — Elastic Block Storage (Single ec2)

EFS — Elastic File System (Multiple ec2)

FSx — 3rd Party

Snowcone — 8 TB HDD / 14 SSD (data transfer)

Edge Computing

Snowball — 80 TB < 10 PB (data transfer)

Storage GW — Bridge on-premise data & cloud data

Snowmobile — > 10 PB < 100 PB (data transfer)

OpsHub to manage snow family

Database

RDS — Relational Database Service (OLTP)

DynamoDB — Key/Value & DAX cache (SLS, a-a global tables)

Aurora — Relational DB Management System (OLTP)

DocumentDB — JSON (Aurora for MongoDB) (NoSQL)

Neptune — Graph DB

ElastiCache — In-memory

DMS — Database Migration Service

Analytics

Redshift — Warehouse data analyze (OLAP, SQL)

EMR — Elastic MapReduce (Hadoop, Cluster)

Athena — serverless S3 Query (SLS)

Glue — Extract Transform Load

QuickSight — dashboards (SLS)

App Integration

API GW — create, publish, monitor, and secure APIs (SLS)

EventBridge — Schedules, Event, Trigger, Rules

SNS — Simple Notification Service

Step Functions — Visual workflow to orchestrate Lambda f

SQS — Message Queue

MQ — Messaging Queue

Kinesis — Real-time Streaming

AppSync — sync mobile & web apps data (GraphQL)

Pinpoint — Marketing communications (email sms push, 2-way)

Connect — Virtual Contact Center

Business App

Security OF the Cloud
- Infrastructure (Hardware, facilities, network)
- Managed Services (S3, Dynamo, RDS)

Sared Responsibility
- Patch Management
- Configuration Management
- Awareness & Training

Security IN the Cloud
- EC2 patches and updates, firewall, IAM
- Encrypting application data (client and server side)
- Customer data
- Networking traffic protection

AWS Partner Network (APN)

Consulting Partners are professional services firms that help customers to migrate to AWS cloud

Technology Partners provide hardware, connectivity, or software solutions hosted or integrated w/ AWS

Network

VPC — Virtual Private Cloud

ELB — Distribute traffic

CloudFront — CDN (Content Delivery Network) (cache)

Route 53 — DNS (Domain Name System)

Edge location → site that CloudFront uses to cache copies of the content for faster delivery to users at any location

Private Link — Expose a service (Network Load Balancer, Elastic Network Interface)

Transit GW — Peering thousands of VPC / on-premises

Direct Connect — on-premises and AWS (over private network)

Site-to-Site VPN — on-premises VPN to AWS (over public internet)

Client VPN — Connect your PC to AWS & on-premises (over public internet)

Global Accelerator — Use AWS global network

Security, Identity, & Compliance

IAM — Identity Access Management

Security Tools Audit: Credentials Report (Account), Access Advisor (User)

Root User privileges

User, Groups, Policy, Access Keys, Token (MFA) (STS: Temporary credentials) → U2F=USB, Virtual, Hardware

Roles → AWS Services

AWS Abuse → Report suspected AWS resources used for abusive or illegal purposes

Shield — DDoS

WAF — Web App Firewall

GuardDuty — Malicious Behavior in VPC, DNS

Security Hub — Central security tool

Network Firewall — VPC Firewall

Secrets Manager — Storing and rotate secrets every x day

Cognito — App users

KMS — Key Management Service (encryption)

CloudHSM — encryption Hardware Security Module

Identity Center — Single sign-on (SSO, aws console)

Directory Service — Microsoft Active Directory (db of obj, user acc, pc, printers)

Inspector — Find software vulnerabilities (Workloads)

Detective — Root cause and suspicious activities (Logs, ML)

Resource Access Manager (RAM) — Share Resources w/ other AWS accounts

ACM — AWS Certificate Manager

Artifact — Security and Compliance Reports

Macie — Discovers sensitive data (ML)

Developer Tools

CodeCommit — Git Repo

CodeBuild — Build & test

CDK — Cloud Development Kit (provision, IaaC)

CodeDeploy — to instances or functions

SDK — Software Development Kit (interact)

CLI — Command Line Interface (SSH (Secure Shell))

CodePipeline — Orchestration (build to deploy)

CodeArtifact — packages / dependencies

Cloud9 — IDE (VSCode)

CodeStar — CICD view

CloudShell — Browser shell

WorkSpace — Provision desktops (DaaS, VDI)

AppStream — Desktop Streaming (with browse)

End User Computing

OpsWorks — Chef and Puppet

Control Tower — Easy Account Setup

Compute Optimizer — ↓ costs ↑ perf (Recommendations, ML)

Managed Blockchain — No need authority (Ethereum, Hyperledger)

QLDB — Quantum Ledger (Immutable journal, crypto verifiable)

SSM — Systems Manager (operational insights, Manage & operate)

Management Console — Web App Console

Beanstalk — Deploying an app (PaaS)

EKS — Elastic Kubernetes Service

ECS — Elastic Container Service

Containers / Kubernetes

Support — AWS Plans Pricing

Marketplace — Independent software vendors (sell SaaS)

Lightsail — little cloud experience

Fargate — Serverless containers (SLS)

ECR — Elastic Container Registry

Basic
free, documentation

Developer
email

Response times:
- General: < 24 business hours
- System: < 12 business hours

Business
phone / chat access

Response times:
- Production impaired: < 4 hours
- Production down: < 1 hour

Enterprise
TAM (Technical Account Manager)

Response times:
- Business down: < 15 minutes

Financial

Billing Dashboard: high level overview + free tier dashboard

Cost Allocation Tags: tag resources to create detailed reports

Cost Anomaly Detection: detect unusual spends using ML

Service Quotas: notify when close to service quota threshold

Cost Explorer — High level custom reports (forecast)

Cost and Usage Reports — most comprehensive set

Budgets — Budget Alarm (forecast)

Savings Plans — Long-term 1-3 years

Compute

Local Zones — compute & storage, providing low latency (closer to users, Extend VPC)

Wavelenght — 5G networks

Storage Backup

Backup — automate backups

Strategies:
- Backup and Restore
- Pilot Light
- Warm standby
- Multi-site/ Hot-Site

DRS — Elastic Disaster Recovery (Block replication, outside into aws)

Front-end

Amplify — develop & deploy

Device Farm — tests app with pc, mobile, tablet...

Migration & Transfer

App Migration Service (MGN) — Migrating applications to AWS

Migration Evaluator — data-driven business case for migration

App Discovery Service — On-premises migration plan

DataSync — Data from on-premises to AWS (incremental)

Satellite

Ground Station — Satellite

IoT Core — Internet of Things

Machine Learning

Use

Rekognition — face detection, labeling

SageMaker — Dev machine learning

Transcribe — audio to text

Textract — Detect text and data in documents

Polly — text to audio

Kendra — ML-powered search engine

Translate — Translations

Forecast — highly accurate forecasts

Lex — Chatbots

CodeGuru — automated code reviews

Comprehend — Natural language processing (NLP)

Personalize — recommendations