AWS Cloud Practitioner Cheat Sheet

Last Updated: September, 2025

IAM

MFA Multi Factor Authentication

- Virtual MFA Mobile MFA apps like Duo Mobile
- U2F USB
- Hardware MFA Small physical devices that generate MFA code

IAM Credentials Report Account-level, a csv file that lists all IAM users and the status of their credentials

IAM Access Advisor User-level, shows which services a user can access and when they were last accessed

IAM Access Analyzer Find out which resources are shared cross account or organization, define a Zone of Trust

IAM Identity Center SSO, one login for all accounts in Organizations + 3rd party SaaS apps

EC2

EC2 Image Builder Automate and maintain AMIs

EC2 Pricing

- On-Demand Pay as you go
- Reserved Instances Up to 72% discount, 1 or 3 years
- Spot Instances Up to 90% discount, good fit for workload that can be interrupted
- Dedicated Instances Your instance runs on dedicated hardware (not shared with any other customer). AWS manages placement and may move the instance between servers
- Dedicated Hosts Reserve an entire physical server Keywords: Server-bound licenses

EC2 Storage

- EC2 Instance Store
- EBS Network drive, locked to an AZ, attached to one instance at a time (multi-attach is possible but not tested in Cloud Practitioner)
- EFS Managed Network File System, can be mounted on 100s of EC2 instances
- FSx for Windows File Server SMB
- FSx for Lustre (Linux Cluster) HPC

S3

Static Website Hosting

Versioning Maintain versions of same key overwrites

Cross-Region/Same-Region Replication

Storage Class

- Standard No retrieval fee
- Intelligent Tiering Move between ACCESS tiers (frequent, infrequent, …), No retrieval fee
- Standard-IA
- One Zone-IA
- Glacier Instant Retrieval
- Glacier Flexible Retrieval Retrieval may take minutes to 12 hours
- Glacier Deep Archive Retrieval may take 12~48 hours

S3 Lifecycle Configurations Move between STORAGE classes

Storage Gateway Hybrid storage solution, gateway between on-premise servers and S3

Snow Family (Edge Computing)

Snowcone

Snowball Transfer petabytes of data

Snowcone and Snowball can be used for both data migration (storage optimized) and edge computing (compute optimized)

Snowmobile Transfer exabytes of data

OpsHub Client-side software to manage snow family devices

ELB & ASG

Application Load Balancer Layer 7, HTTP/HTTPS

Network Load Balancer Layer 4, TCP/UDP

Gateway Load Balancer Layer 3, GENEVE Protocol

Keywords: Route traffic to firewalls, intrusion detection

Auto Scaling Group

Database & Analytics

RDS Relational DB

Aurora AWS proprietary, supports MySQL and PostgreSQL, can opt serverless

ElastiCache In-memory cache, Redis/Memcached in AWS

DynamoDB NoSQL DB

DAX In-memory cache for DynamoDB

DynamoDB Global Tables Global read/write, active-active

Redshift OLAP, Data warehouse

EMR Map Reduce in AWS

Athena Analyze data stored in S3

Quicksight Interactive dashboards

DocumentDB MongoDB

Neptune Graph DB

Timestream Time series DB

QLDB Quantum Ledger DB, record financial transactions and track all changes, cryptographically verifiable that data has not been modified

Glue ETL (Extract, Transform, and Load), prepare and transform data for analytics

DMS Database Migration Service

Managed Blockchain Blockchain in AWS

Other Compute Services

ECS Containers in AWS

Fargate Serverless ECS

ECR Image registry

EKS Kubernetes in AWS

Lambda FaaS, serverless compute

API Gateway Often used together with Lambda and DynamoDB, supports both RESTful and WebSocket APIs

Batch Run large and parallel batch jobs

Lightsail Beginner-friendly website/app deployment

Deployments & Infrastructure at Scale

CloudFormation IaC, Terraform in AWS

CDK Development kit for provisioning AWS resources

Beanstalk PaaS

Developer-friendly service for deploying apps, developers can focus on writing code instead of managing infrastructure

Still have control over underlying resources (EC2, ASG, ELB, RDS, etc.)

CodeCommit Code repository

CodeBuild Compiles code, runs tests, and produce code builds

CodeDeploy Automates deployments to EC2, ECS, and Lambda, supports rolling and blue/green strategies

CodePipeline Orchestrate a pipeline e.g., CodeCommit -> CodeBuild -> CodeDeploy -> Elastic Beanstalk

CodeArtifact Manage dependencies, developers can download dependencies from CodeArtifact using tools like npm and yarn

CodeStar Unified UI for CodeCommit, CodeBuild, etc.

Cloud9 Web-based IDE

Systems Manager (SSM) Manage a fleet of EC2 instances.

A central hub to automate, view, and operate your EC2 fleet (and other resources) without having to SSH into them

Mostly for EC2 instances, but can be used for on-prem servers & VMs if you install an SSM agent.

Keywords: “Centralize operational insights”

SSM Session Manager Enable SSH access without opening up port 22

SSM Parameter Store Store configuration data & secrets

Global Infrastructure

Route53 *Managed DNS*

Route53 Routing Policies

- Simple routing
- Weighted routing
- Latency routing
- Failover routing Active-Passive

CloudFront CDN, also good for DDoS protection

S3 Transfer Acceleration Accelerate S3 global uploads & downloads

AWS Global Accelerator

Can be used for both UDP/TCP and HTTP

Global Accelerator typically targets EC2, ALB, and NLB, it does not target S3 buckets or DynamoDB

Keywords: AWS Global Network, improve global application's availability and performance

AWS Outposts Hybrid cloud solution, you get physical server racks with AWS services available

AWS Wavelength Edge-computing at telecom provider's node

Keywords: 5G networks

AWS Local Zones Extension to regions, e.g., have local zones for major cities like Boston, Chicago, Dallas, …

Keywords: Latency-sensitive applications

Cloud Integrations

SQS Decouple app components, queue model

Keywords: "Loosely-coupled" applications

Kinesis Real-time big data streaming

SNS Notification service, pub-sub model

MQ 3rd party message broker services

Cloud Monitoring

CloudWatch Metrics Numeric time-series data

- EC2 instances: CPU utilization, status checks
- EBS: Disk read/writes
- Service Limits: API usage
- Billing: Total estimated charges

CloudWatch Logs Raw text data, usually app or system logs, can be filtered and monitored in real-time

CloudWatch Alarms

Tied to metrics (or by filtering logs)

Trigger following actions:

- Auto Scaling
- Stop, terminate, or reboot EC2 instances
- Send a SNS notification

EventBridge (CloudWatch Events) Discrete events (e.g., an API call) trigger Lambda or SQS/SNS

CloudTrail History of events/API calls made by an AWS account

Account-based - who did what?

Keywords: Governance, compliance, and audit

CloudTrail Event Types

- Management Events Provided by default
- Data Events Resource operations e.g., S3
- Insights Events Detect unusual API events

X-Ray Visual analysis of microservices dependencies, debug distributed services

CodeGuru Automated code review

AWS Health Dashboard Dashboard to check if any AWS services are down (ALL regions and services)

AWS Account Health Dashboard Dashboard to check if YOUR account and resources are impacted

VPC & Networking

VPC Your private network in AWS, spans AZ

Subnet A subset of IPs inside a VPC, locked to a single AZ, can be public or private

Internet Gateway Expose VPC to the internet, for resources with public IPs

NAT Gateway Translate private IP to public IP, enable resources in private subnets to access the internet without being exposed to inbound traffic

Security Groups Instance level, stateful, ALLOW rules only

NACL Network ACL Subnet level, stateless, both ALLOW and DENY rules, rules applied in specified order

AWS Network Firewall VPC level security

VPC Flow Logs Log of IP traffic

VPC Peering Connect two VPCs

VPC Endpoint Connects your VPC privately to AWS services (e.g., S3, DynamoDB) without using the public internet

PrivateLink Expose your service privately to other VPCs or on-prem, requires NLB to front your service

Use Case: A SaaS company wants customers to access its service securely from their own VPCs, without going over the public internet

Connect On-premise and AWS

- DirectConnect Establish physical connection between on-prem data center and AWS
- Site-to-Site VPN Connection over the internet but encrypted
  Need to set up Customer Gateway on client side, Virtual Private Gateway on AWS side

Client VPN Allow end-users (e.g., laptops or remote workers) to securely connect to VPC over the internet

Transit Gateway Connect thousands of VPCs + on-premise networks using one interface, hub-and-spoke model

Security & Compliance

Shield Protect against DDoS at lower layer

Shield Advanced 24/7 premium DDoS protection, paid service

Works with Route53, CloudFront, Global Accelerator, ELB, and EC2

Web Application Firewall (WAF) Protection against web-based threats e.g., SQL Injection, Cross-Site Scripting, Geo-match (block certain countries)

Works with CloudFront, ALB, API Gateway, and AppSync

AWS Firewall Manager Central security management across multiple accounts

Works with WAF, Shield Advanced, Security Groups, and Network Firewall

Data at rest vs. in transit Best practice is to encrypt both

Encryption

- Encrypted by default: CloudTrail logs, S3 server-side, S3 Glacier, S3 Storage Gateway
- Encrypted manually: S3 client-side, EBS, EFS, RDS, Redshift

KMS Managed key service used by AWS and customers to create, manage, and use encryption keys

CloudHSM Store keys on hardware devices called HSM (Hardware Security Module)

Types of Customer Master Keys (CMKs)

- Customer Managed CMKs Created, managed, and used by customers
- AWS Managed CMKs AWS creates, manages, and uses on customer's behalf
- AWS Owned CMKs AWS owns and manages, used in multiple accounts, invisible to users

- CloudHSM Keys Keys generated from your own HSM device

AWS Certificate Manager (ACM) Manages SSL/TLS certificates

Secrets Manager Secrets can be anything e.g., database credentials, API keys, etc.

Rotation of secrets, Integration with RDS

Artifact AWS compliance and agreement documents

GuardDuty ML-powered intelligent threat discovery

Inspector Inspect vulnerabilities and security of EC2, container images, and Lambda

Config Audit and compliance, resource-specific: how has the resource configuration changed over time?

Macie Identify and protect sensitive information stored in S3

Security Hub Central security tool that aggregates information from multiple accounts

Dashboard with data from GuardDuty, Inspector, etc.

Amazon Detective Identify root causes of security issues

AWS Abuse Report suspected AWS resources involved in abusive or illegal activities

Machine Learning

Rekognition Object recognition

Transcribe Speech-to-text

Polly Text-to-speech

Translate

Lex Chatbot

Connect Call center

Comprehend NLP

SageMaker Managed notebook service

Kendra ML-powered document search engine

Personalize

Textract OCR

Account Management, Billing & Support

Organizations Manage multiple accounts

Consolidated billing, pricing benefits from aggregated usage, pool reserved instances among accounts

Service Control Policies (SCPs) Set guardrails - what services/actions accounts in the org can or cannot use

Control Tower Runs on top of Organizations, quickly set up multi-account environment + guardrails

Resource Access Manager Share AWS resources within organization

Service Catalog Quick way to launch a set of authorized services that have been pre-defined by admins

Compute Optimizer Mostly for EC2, EBS, and Lambda. Helps you right-size e.g., if EC2 instances are under-utilized, downscale

Free Services in AWS

- IAM, VPC, Consolidated Billing
- ELB, CloudFormation, and ASG Free, but you pay for the underlying resources

Savings Plans

- Compute Savings Plans More flexible
- EC2 Instance Savings Plans Less flexible, fixed instance type, higher discount

Estimating Costs

- Pricing Calculator

Tracking Costs

- Billing Dashboard
- Cost Allocation Tags
- Cost Explorer Forecast usage up to 12 months based on previous usage, choose an optimal savings plan
- Cost and Usage Reports Most detailed, raw billing data in csv format

Monitoring

- Billing Alarms Simple alarm, not as powerful as Budgets, billing data stored in us-east-1
- Budgets Keywords: Send alarms when cost exceeds budget

AWS Cost Anomaly Detection Use ML to detect unusual spends

AWS Service Quotas Get notified when you're close to service quota e.g., you can have max 5 VPCs in a region

AWS Trusted Advisor High-level account assessment, assess the following categories:

- Cost optimization
- Performance
- Security
- Fault tolerance
- Service limits

7 core checks are provided in all plans

Full checks and API access is only available to business and enterprise plans

Support Plans

Basic	24/7 access to customer service
Developer	Business hour email access to Cloud Support Associates
Business Support	24/7 access to Cloud Support Associates Trusted Advisor full set of checks + API access
Enterprise On-Ramp	Access to Technical Account Managers Concierge Support Team
Enterprise	Access to a designated TAM Business critical system down time is less than 15 mins

Advanced identity

Security Token Service Create temporary, limited credentials, used by AWS internally

Cognito Authentication in web or mobile apps

Directory Services Microsoft Active Directories in AWS

Other Services

WorkSpaces Desktop-as-a-Service, access Windows or Linux desktop environment via browser or client app

AppStream Apps delivered/streamed from browser

IoT Core

Elastic Transcoder Convert media files stored in S3 into file formats required by consumer playback devices e.g., phones

AppSync GraphQL, store and sync data across mobile and web apps in real time

Amplify Develop and deploy full stack web and mobile apps

AWS Infrastructure Composer Visual design tool for building AWS architectures, uses CloudFormation templates under the hood

Device Farm Tests apps on various devices (android, ios, etc.)

DataSync Large data transfer, supports incremental transfers

Step Functions Serverless visual workflow, orchestrate lambda functions

Ground Station Satellite solution

AWS Pinpoint Marketing solution
AWS Fault Injection Simulation Chaos engineering

AWS Backup Centrally manage and automate backups for different services
AWS Elastic Disaster Recovery Formerly known as CloudEndure Disaster Recovery

Application Migration Service Lift-and-shift migration
Application Discovery Service Plan migration by gathering information about on-prem data centers, results can be viewed in Migration Hub
AWS Migration Evaluator Helps estimate migration costs
AWS Migration Hub Central dashboard for migration progress

Database Migration Strategies

- Rehost Migrate to cloud without making any changes
- Replatform Migrate to cloud with some optimizations e.g., switch from self-managed to managed
- Repurchase Replacing the existing database with a new one from a different vendor or a cloud-native solution.
- Refactor Involves changing the codebase
- Retire Shut down applications that are no longer needed
- Retain Keep certain applications on-prem e.g., due to compliance
- Relocate Moving the database within the AWS cloud, such as from one VPC to another or from one AWS account to another

Disaster Recovery Strategy

Backup & Restore	● $, Active-Passive ● For low priority use case
Pilot Light	● $$, Active-Passive ● Data is live but service is idle ● Core components (e.g., database) are live, but some components (e.g., load balancer) might be idle. ● Since the core parts are live, easier to restore
Warm Standby	● $$$, Active-Passive ● Full system always running but at a smaller scale. ● Think of it like a scaled-down clone of the production environment running 24/7 in another region. ● For business critical services
Multi-site Active-Active	● $$$$, Active-Active ● Zero downtime and near zero data loss ● For mission critical services

Active-Active All environments live and serving traffic simultaneously
Active-Passive One site is active while the other is on standby (idle or lightly running)

Architecting & Ecosystem

Well Architected Framework (WAF)

- Operational Excellence
- Security
- Reliability
- Performance Efficiency
- Cost Optimization
- Sustainability

AWS Well-Architected Tool Select your workload and answer questions to check if it follows best practice
AWS Customer Carbon Footprint Tool

AWS Cloud Adoption Framework (CAF)

- Business
- People
- Governance
- Platform
- Security
- Operations

AWS Professional Services & Partner Network

- APN Technology Partners Hardware, connectivity, or software providers
- APN Consulting Partners
- APN Training Partners Help learn AWS
- AWS Competency Program Granted by AWS to APN partners
- AWS Navigate Program Help partners become better partners

AWS Marketplace Buy or sell third-party software, data, and services that run on AWS
AWS Knowledge Center Most frequent and common questions and requests
AWS IQ Find and employ 3rd party AWS experts
AWS re:Post Q&A