AMAZON WEB SERVICES CHEAT SHEET 1

AWS Basics

Amazon Web Service

Amazon Web Services (AWS) is a collection of various cloud computing services and applications that offer flexible, reliable, easy to use and cost-effective solutions.

Cloud Computing

It is an internet-based computing service in which various remote servers are networked to allow centralized data storage and online access to computer services and resources.

Types of cloud: There are three types of clouds

- Public cloud: The resources and services provided by the 3rd party service providers are available to the customers via internet
- Private cloud: Here the resources and services are managed by the organizations or by the third party only for the customers organization.
- Hybrid cloud: It is a combination of both Public and Private Cloud. The decision to run the services on public or private depends on the parameters like sensitivity of the data and applications, industry certifications and required standards, etc.

Elastic Block Store

Elastic Block Store (EBS): an easy-to-use, scalable, high-performance block-storage service designed for EC2. It is a persistent storage device that can be attached to a **single** EC2 instance to be used as a file system for databases, application hosting, and storage.

Elastic File System

Elastic File System (EFS): a managed network file system that can be shared across **multiple** EC2 instances and is scalable depending on workload. Uses: big data and analytics, media processing workflows, content management, web serving, and home directories.

Elastic Cloud Compute

EC2 (Elastic Compute Cloud) is a virtual server for running applications on **AWS**. EC2 instance types:

Type:

- General Instances: provide a balance of compute, memory and networking resources, and can be used for a variety of diverse workloads.
- Compute Instances: are ideal for compute bound applications that benefit from high performance processors.
- Accelerated Compute Instances (GPU): use hardware accelerators, or co-processors, to perform functions, such as floating-point number calculations, graphics processing, or data pattern matching, more efficiently than is possible in software running on CPUs.
- Memory Instances: are designed to deliver fast performance for workloads that process large data sets in memory.
- Storage Instances: are designed for workloads that require high, sequential read and write access to very large data sets on local storage.

Family:	Use Cases:
M, T micro	websites and web applications, development environments, build servers, code repositories, services, test and staging environments, and line of business applications.
C, HPC performance machine	batch processing workloads, media transcoding, high performance web servers, high computing (HPC), scientific modeling, dedicated gaming servers and ad server engines, learning inference and other compute intensive applications.
P, D, T, I, G, F, VT computational finance, discovery.	machine learning, high performance computing, computational fluid dynamics, seismic analysis, speech recognition, autonomous vehicles, and drug
R, X time big	memory-intensive applications such as open-source databases, in-memory caches, and real data analytics (e.g. SAP HANA, Apache Spark)
I, D, H business-critical performance and high PostgreSQL), and NoSQL for workloads that require very engines and data analytics	maximize the number of transactions processed per second (TPS) for I/O intensive and workloads which have medium size data sets and can benefit from high compute network throughput such as relational databases (MySQL, MariaDB, and databases (KeyDB, ScyllaDB, and Cassandra). They are also an ideal fit fast access to medium size data sets on local storage such as search workloads.

Simple Storage Service

S3 is an object storage service offering industry-leading scalability, data availability, security, and performance. Data is stored as objects within resources called "buckets", and a single object can be up to 5 terabytes in size.

Characteristics:

- Designed for durability of 99.999999999% (11 9s) of objects across multiple Availability Zones
- Designed for 99.99% availability over a given year

Name:	Type:	Product Description:
S3 Standard	Storage	offers high durability, availability, and performance object storage for frequently accessed data.
S3 Intelligent-Tiering	Storage	automatically reduces your storage costs on a granular object level by automatically moving data to the most cost-effective access tier based on access frequency, without performance impact, retrieval fees, or operational overhead.
S3 Standard-Infrequent Access (S3 Standard-IA)	Storage	for data that is accessed less frequently but requires rapid access when needed. It offers the high durability, high throughput, and low latency of S3 Standard, with a low per GB storage price and per GB retrieval charge.
S3 One Zone-Infrequent Access (S3 One Zone-IA)	Storage	for data that is accessed less frequently but requires rapid access when needed. Unlike other S3 Storage Classes which store data in a minimum of three Availability Zones (AZs), S3 One Zone-IA stores data in a single AZ and costs 20% less than S3 Standard-IA.
S3 Outpost	Storage	delivers object storage to your on-premises AWS Outposts environment.
S3 Glacier Instant Retrieval	Archive	is an archive storage class that delivers the lowest-cost storage for long-lived data that is rarely accessed and requires retrieval in milliseconds.
S3 Glacier Flexible Retrieval	Archive	delivers low-cost storage for archive data that is accessed 1-2 times per year and is retrieved asynchronously.
S3 Glacier Deep Archive	Archive	is Amazon S3's lowest-cost storage class and supports long-term retention and digital preservation for data that may be accessed once or twice in a year.

AMAZON WEB SERVICES

CHEAT SHEET 2

AWS Basics

EC2 Pricing Models

EC2 usage is billed on one second increments, with a minimum of 60 seconds. Similarly, provisioned storage for EBS volumes will be billed per-second increments, with a 60 second minimum. Available for On-Demand, Reserved and Spot forms.

Pricing Models:

Free Tier: includes 750 hours of Linux and Windows t2.micro instances, (t3.micro for the regions in which t2.micro is unavailable) each month for one year. To stay within the Free Tier, use only EC2 Micro instances.

On Demand: pay for compute capacity by the hour or the second depending on which instances you run. No longer-term commitments or upfront payments are needed. You can increase or decrease your compute capacity depending on the demands of your application and only pay the specified per hourly rates for the instance you use.

Spot: allow you to request spare Amazon EC2 computing capacity for up to 90% off the On-Demand price.

Savings Plans: are a flexible pricing model that offer low prices on EC2 and Fargate usage, in exchange for a commitment to a consistent amount of usage (measured in $/hour) for a 1 or 3 year term.

Standard Reserved Instance: provide a significant discount (up to 72%) compared to On-Demand Instance pricing and can be purchased for a 1-year or 3-year term.

Convertible Reserved Instance: if you need additional flexibility, such as the ability to use different instance families, operating systems, or tenancies over the Reserved Instance term. Convertible Reserved Instances provide you with a significant discount (up to 66%) compared to On-Demand Instances and can be purchased for a 1-year or 3-year term.

Dedicated Hosts: is a physical EC2 server dedicated for your use. Dedicated Hosts can help you reduce costs by allowing you to use your existing server-bound software licenses, including Windows Server, SQL Server, and SUSE Linux Enterprise Server (subject to your license terms), and can also help you meet compliance requirements.

AWS Services

Compute

- EC2: **Elastic Compute Cloud** provides secure, resizable compute capacity in the cloud. It makes we-scale cloud computing easer for developers.
- EC2 Auto Scaling: Helps maintain application availability which can automatically add or remove EC2 instances according to conditions.
- Amazon Container Registry: Fully-managed Docker container registry that helps to store, manage and deploy Docker container images.
- Amazon Elastic Container Service: Highly scalable, high-performance container orchestration service supporting Docker containers, which makes it easy to run and scale containerized applications on AWS.
- Amazon Elastic Kubernetes Service: Makes it easy to deploy, manage, and scale containerized applications using Kubernetes on AWS.
- Amazon Fargate: is a serverless, pay-as-you-go compute compatible with both Amazon Elastic Container Service (ECS) and Amazon Kubernetes Services (EKS).
- Amazon Lightsail: Designed to be the easiest way to launch and manage a virtual private server with AWS.
- Elastic Beanstalk: It is an application container used for deploying and managing containers.
- Lambda: It is a serverless computing service that runs the code in response to events.

Storage

- AWS S3: It refers to **Simple Storage Service**. Allows storage of data objects.
- AWS Backup: is an externally-accessible backup provider that makes it easier to align and optimize the backup of data across AWS services in the cloud.
- Amazon Elastic Block Store (EBS): is a web service that provides block-level storage volumes.
- Amazon Elastic File System (EFS): offers file storage for the user's EC2 instances. Blob Storage.

Storage (Continued)

- Amazon FSx: supplies a fully managed third-party file systems with the native compatibility and characteristic sets for workloads.
- Amazon S3 Glacier: Amazon Simple Storage Service Glacier (Amazon S3 Glacier) is a storage service tailored for infrequently used data, or "cold data."
- Snowball: AWS Snowball is a service for users who wish to transport terabytes or petabytes of data to and from AWS.
- Storage Gateway: is a service which connects an on-premises software appliance with cloud-based storage.

Database

- Aurora: is a fully managed RDS MySQL and PostgreSQL compatible relational database that is both cost effective and extremely quick.
- DocumentDB: is a quick, dependable, and fully-managed database service that makes it easy for you to set up, operate, and scale MongoDB-compatible databases.
- DynamoDB: is a fully administered NoSQL database service that offers quick and reliable performance with integrated scalability.
- Elasticache: helps in setting up, managing, and scaling in-memory cache conditions.
- Cassandra Service: Amazon Managed Apache Cassandra Service (MCS) is an extensible, highly available, and secured Apache Cassandra–compatible database provider.
- Neptune: is a fast, reliable, fully-managed graph database service that makes it easy to build and run applications that work with highly connected datasets.
- Quantum Ledger Database (QLDB): is a fully managed ledger database functioned by a central trusted authority that offers a transparent, immutable, and cryptographically verifiable transaction log of all application changes.
- Relational Database Service (RDS): is a managed service that makes it simple to set up, operate, and scale databases in the cloud.

Database (Continued)

- Redshift: is a rapid, fully accessible, petabyte-scale data warehouse service that makes it easy and cost-effective to effectively evaluate data with the existing business intelligence tools.

Security, Identify, & Compliance

- Identity and Access Management (IAM): is a web service for safely controlling access to AWS services.
- Artifact: provides on-demand access to AWS' security and compliance reports and select online agreements.
- Cognito: is an authentication management SDK and management service covering user sign-up, sign-in, and access control for web and mobile applications.
- Detective: enables quick analysis and investigation of potential security issues.
- Directory Service: offers various methods to set up and operates Amazon Cloud Directory, Amazon Cognito, and Microsoft AD with other AWS services.
- Firewall Manager: is a service that simplifies the management of web application firewalls and maintenance activities over multiple accounts and resources.
- GuardDuty: is a threat detection service that continuously monitors for malicious activity and anomalous behavior.
- Inspector: is an automated security vulnerability management service that continually evaluates your resources for software vulnerabilities and unintended network exposure.
- Macie: is a fully managed data security and data privacy service that uses machine learning and pattern matching to discover and protect sensitive data
- Resource Access Manager: securely share resources across AWS accounts, within your organization or organizational units (OUs) in AWS Organizations, and with IAM roles and IAM users for supported resource types.
- Secrets Manager: assists the user to safely encode, store, and recover credentials for any user's database and other services.

Security, Identify, & Compliance (Continued)

- Security Hub: allows viewing the security state of the AWS resources.
- Single Sign-In: is a cloud-based service that helps in simplifying, managing SSO access to AWS accounts and business applications.
- Data Migration Service (DMS): is a service to quickly and securely migrate to the cloud.
- Web Application Firewall (WAF):is a web application firewall that protects web applications from common web exploits.
- Cloud HSM: provides a secure cryptographic key storage for all users by allowing administrated hardware security modules in the AWS Cloud.
- Key Management Service: is functionality utilized by other AWS services, which can also be utilized to secure data.
- Crypto Tools: libraries engineered to assist users to do cryptography right, even without a specialist.
- Certificate Manager: the **ACM** helps to easily provision, manage, and deploy SSL/TLS certificates on AWS managed resources.

Management & Governance

- Auto-Scaling: service to set up as well as manage dynamic and imminent scaling of scalable AWS resources.
- Chatbot: is an interactive agent that makes it easy to monitor, operate, and troubleshoot AWS workloads in Slack channels or Amazon Chime chatrooms.
- CloudFormation: Is a service that models a collection of related AWS and third-party resources, provision them quickly and consistently, and manage them throughout their lifecycles, by treating infrastructure as code.
- CloudTrail: With AWS CloudTrail, any user can control the AWS deployments in the cloud by accepting a history of AWS API calls for the account, including API calls made through the AWS Management Console, the AWS SDKs, the command line tools, and higher-level AWS services.

AMAZON WEB SERVICES CHEAT SHEET 3

AWS Basics

Storage Services

Service Name	Use Case
Simple Storage Service	Data storage for unstructured data.
Elastic Block Store	System storage for EC2 VMs.
Elastic File System	Scalable data storage for EC2 VMs

Relational Database Service

Amazon Relational Database Service (RDS) is a collection of managed services that makes it simple to set up, operate, and scale databases in the cloud. Choose from **Amazon Aurora with MySQL** compatibility, **Amazon Aurora with PostgreSQL** compatibility, **MySQL**, **MariaDB**, **PostgreSQL**, **Oracle**, and **SQL Server**. Deployments can be to either AWS or on-premises with Amazon RDS on AWS Outposts.

RDS	is a fully managed database service. [7 DBs]
RDS Custom	is a managed database service for applications that require customization of the underlying operating system and database environment. [Oracle, SQL]
RDS on AWS Outposts	is a fully managed AWS Outpost deployed database using secure connections. [SQL, MySQL, PostgreSQL]
RDS Proxy	is a fully managed, highly available database proxy feature for Amazon RDS. RDS Proxy makes applications more scalable, more resilient to database failures, and more secure. [Aurora, MySQL, PostgreSQL]

AWS Services

Management & Governance (Continued)

- **CloudWatch**: is a monitoring service for cloud resources and applications. It can be used to collect and track metrics, collect and monitor log files, and set alarms.
- **Command Line Interface (CLI)**: is a unified tool to manage your AWS services. It can control multiple AWS services from the and automate them through scripts.
- **Compute Optimizer**: recommends optimal resources for your workloads to reduce costs and improve performance by using machine learning to analyze historical utilization metrics.
- **Config**: is a service that enables you to assess, audit, and evaluate the configurations of your resources.
- **Control Tower**: is assistance that permits the user to implement and control governance rules for protection, operations, and compliance at scale across all the companies and accounts.
- **Data Lifecycle Manager**: manages the lifecycle of resources. Lifecycle policies are created and used to automate operations on the specified resources. Amazon DLM supports Amazon EBS volumes and snapshots.
- **Health**: grants personalized data about events that can affect the AWS infrastructure, conducts the scheduled changes, and stimulates the troubleshooting of problems that influence the AWS resources and accounts.
- **License Manager**: streamlines the method of carrying software vendor licenses to the cloud.
- **OpsWorks**: presents a simple and flexible way to create and maintain stacks and applications.
- **Organizations**: is an account administration service that allows the user to incorporate multiple AWS accounts into an association that the user creates and centrally manages.
- **Resource Groups**: permits the user to organize AWS resources into groups, tag supplies employing essentially any criteria, and maintain, proctor, and automate assignments on grouped resources.

Management & Governance (Continued)

- **Service Catalog**: facilitates IT administrators to organize, maintain, and share portfolios of recommended products to end-users.
- **Systems Manager**: is a secure end-to-end management solution for hybrid cloud environments.
- **Storage Gateway**: is a service which connects an on-premises software appliance with cloud-based storage.
- **Tool for PowerShell**: are PowerShell modules, developed on functionality exposed by the AWS SDK for .NET, that allow the user to script services on AWS resources from the PowerShell command line.
- **Well-Architected Tool**: is designed to help review applications and workloads, and it provides a central place for architectural best practices and guidance. It is based on the Well-Architected Framework, which was developed to help cloud architects build secure, high-performing, resilient, and efficient application infrastructures.

Migration & Transfer

- **Application Discovery Service**: improves systems integrators promptly by automatically classifying applications.
- **Database Migration Service**: is a web service that helps to transfer data from a user DB to AWS using a RDS instance.
- **DataSync**: is a data-transfer service that simplifies, automates, and accelerates moving and replicating data.
- **Migration Hub**: a single place to store IT asset inventory data while tracking migrations to any AWS Region.
- **Schema Conversion Tool**: generates a heterogeneous database migration simple by automatically transforming the source database schema.
- **Server Migration Service**: unites data collection tools with automated server replication to advance the journey of on-premises servers to AWS.

Migration & Transfer (Continued)

- **Snowball**: AWS Snowball is an aid for consumers who need to transport terabytes or petabytes of data to and from AWS, or who desire to obtain the storage and measure the power of the AWS Cloud locally and cost-effectively.
- **Transfer for SFTP**: is a reliable transfer service that saves the users data in Amazon S3 and clarifies the movement of Secure File Transfer Protocol (SFTP) workflows to AWS.

Networking & Content Delivery

- **API Gateway**: allows the user to design and expand REST and WebSocket APIs at any scale.
- **App Mesh**: makes it accessible to guide and control microservices on AWS.
- **Cloud Map**: is a cloud resource discovery service. You define custom names for your application resources, and ACM maintains the updated location of these dynamically changing resources.
- **CloudFront**: expedites distribution of static and dynamic web content.
- **Direct Connect**: connects the internal interface to an AWS Direct Connect location over a standard 1 gigabit or 10 gigabit Ethernet fiber-optic cable.
- **Elastic Load Balancing**: automatically assigns the incoming administration business beyond multiple targets, such as EC2 instances.
- **Global Accelerator**: is a network layer service in which the user creates accelerators to enhance availability and performance for internet purposes managed by a global audience.
- **Route 53**: is an extremely convenient and scalable Domain Name System (DNS) web service.
- **Virtual Private Cloud**: lets the user begin Amazon Web Services (AWS) resources within a virtual network that users defined.
- **Virtual Private Network**: enables protected and separate tunnel from the network or equipment to the AWS Cloud.

Analytics

- **Athena**: is an automated query service that makes it simple to examine data in Amazon S3 with the help of standard SQL.
- **CloudSearch**: is a fully administrate service in the cloud that makes it effortless to set up, maintain, and scurf a search solution for the website.
- **Data Exchange**: is a service that makes it simple for customers to discover, subscribe to and use third-party data in AWS.
- **Data Pipeline**: is a web service that user can utilize to optimize the movement and restructuring of data.
- **Elastic Search (ES)**: is an enabled service that makes it comfortable to allocate, function, and scale Elasticsearch, a popular open-source search and analytics engine.
- **Data Pipeline**: is a web service that user can utilize to optimize the movement and restructuring of data.
- **EMR**: is a web service that makes it simple to litigate a large amount of data efficiently.
- **Glue**: is a fully enabled ETL (extract, transform, and load) service that makes it easy and cost-effective to classify the data, clean it, enhance it, and propel it reliably between different data stores.
- **Kinesis**: makes it effortless to gather, process, and examine video and data streams in real-time.
- **Lake Formation**: is a administrate service that makes it simple to set up, safe, and maintain the user's data lakes.
- **Managed Streaming for Apache Kafka MSK**: is a fully maintained service that allows it easy for the user to construct and operate applications that utilize Apache Kafka to process streaming data.
- **QuickSight**: is a quick business analytics service to develop visualizations, execute ad hoc analysis, and instantly get business observations from the data.

AMAZON WEB SERVICES CHEAT SHEET 4

AWS Basics

Elastic Load Balancing

ELB automatically distributes incoming application traffic across multiple targets and virtual appliances in one or more Availability Zones (AZs). There are 4 types of load balancers available:

- **Application Load Balancer**: operates at the request level (layer 7), routing traffic to targets (EC2 instances, containers, IP addresses, and Lambda functions) based on the content of the request.
- **Network Load Balancer**: operates at the connection level (Layer 4), routing connections to targets (Amazon EC2 instances, microservices, and containers) within Amazon VPC, based on IP protocol data. Ideal for load balancing of both TCP and UDP traffic. Network Load Balancer is capable of handling millions of requests per second while maintaining ultra-low latencies.
- **Gateway Load Balancer**: helps to deploy, scale, and manage third-party virtual appliances. It provides one gateway for distributing traffic across multiple virtual appliances while scaling them up or down, based on demand.
- **Classic Load Balancer**: is a web service that allows applications, end-users, and devices to immediately send and accept notifications from the cloud.

ElastiCache

Amazon ElastiCache is a fully managed, in-memory caching service supporting flexible, real-time use cases. It can be used to accelerate application and database performance, or as primary data stores that don't require durability.

Use Cases:

- Real-Time Transactions
- Chat
- Business Intelligence & Analytics
- Session Store
- Gaming Leaderboards
- Cache [Compatible with Redis and Memcached]

AWS Services

Application Integration

- **EventBridge**: is a serverless function bus service that makes it straightforward to unite the applications with data from a variety of sources.
- **Messaging Queue (MQ)**: is a guided message broker service for Apache ActiveMQ to set up and administer message brokers in the cloud.
- **Simple Notification Service (SNS)**: is a web service that allows applications, end-users, and devices to immediately send and accept notifications from the cloud.
- **Simple Workflow Service (SWF)**: makes it simple to create applications that parallel work over-allocated components.

Machine Learning

- **Apache MXNet**: is an open-source deep learning framework that offers all the users to define, train, and utilize deep neural networks on a wide variety of platforms, from cloud infrastructure to mobile devices.
- **CodeGuru**: offers intelligent suggestions for enhancing application performance, efficiency, and code quality in your Java applications.
- **Deep Learning**: offers intelligent suggestions for enhancing application performance, efficiency, and code quality in your Java applications.
- **DeepComposer**: is artificial intelligence (AI)-enabled music keyboard that equips the user with a hands-on learning exposure to explore generative learning.
- **DeepLens**: matches a connected HD camera developer kit to assist developers to learn machine learning concepts utilising hands-on computer vision use cases.
- **DeepRacer**: a reinforcement learning (RL)-enabled autonomous 1/18th-scale vehicle with maintaining services in the AWS Machine Learning ecosystem.
- **Elastic Inference**: is a service that allows you to attach low-cost GPU-powered acceleration to Amazon machine instances in order to reduce the cost of running deep learning inference by up to 75%.

Machine Learning (Continued)

- **Forecast**: is a fully guided deep knowledge service for time-series forecasting.
- **Fraud Detector**: is a fully maintained service that supports the user to recognize suspicious online activities such as the creation of fake accounts and online payment fraud.
- **Kendra**: is a search service, powered by machine learning, that allows users to explore unstructured text utilizing natural language.
- **Lex**: is an AWS assistance for building conversational interfaces into applications applying voice and text.
- **Machine Learning**: helps to develop smart applications, including applications for fraud detection, demand forecasting, targeted marketing, and click prediction.
- **Polly**: is a Text-to-Speech (TTS) cloud service that switches text into lifelike speech.
- **Rekognition**: makes it effortless to attach the image and video analysis to the applications.
- **SageMaker**: is a fully distributed machine learning service. With the help of Amazon SageMaker, data scientists and developers can instantly develop and exercise machine learning models and then deploy them into a production-ready hosted environment.
- **Textract**: allows the user to add document text detection and analysis to any application.
- **Transcribe**: equips transcription services for any audio files. It utilizes exceptional machine learning technologies to recognize spoken words and transcribe them into text.
- **Translate**: is a neural machine translation assistance for altering the text to and from English across a breadth of supported languages.
- **Athena**: is an automated query service that makes it simple to examine data in Amazon S3 with the help of standard SQL.

Mobile

- **Amplify**: facilitates developers to produce and deploy cloud-powered mobile and web applications.
- **AppSync**: is an enterprise-level, completely supervised GraphQL support with real-time data synchronization and offline programming characteristics.
- **Device Farm**: is an app testing service that equips the user to test the iOS, Android and Fire OS apps on actual, physical phones and tablets that are entertained by AWS.
- **Amplify Android**: Android SDK executes libraries, code samples, and documentation for developers to produce relevant mobile applications employing AWS.
- **Amplify IOS**: iOS SDK presents an institution, code samples, and documentation for developers to produce connected mobile applications using AWS.
- **Mobile SDK for Unity**: SDK for Unity includes a set of .NET domains that facilitates games written with Unity to utilize AWS services.
- **Pinpoint**: supports the user to engage with customers by sending them email, SMS and voice messages, and push notifications.
- **Simple Notification Service (SNS)**: s a web service that allows applications, end-users, and devices to immediately send and accept notifications from the cloud.

Media Services

- **Elastic Transcoder**: allows the user to switch media files that the user have stored in Amazon S3 into media files in the setups demanded by consumer playback devices.
- **MediaConnect**: is a safe, guarded and resilient transport assistance for live video.
- **Elemental Media Convert**: is a service that formats and compresses offline video content for distribution to televisions or connected appliances.

Media Services (Continued)

- **Elemental MediaLive**: is video assistance that provides easy and secure creation of live productions for broadcast and streaming delivery.
- **Elemental MediaPackage**: is a just-in-time video packaging and origination service that produces extremely strong, scalable, and stable video streams to an extensive variety of playback devices.
- **Elemental MediaStore**: is a video origination and storage assistance that allows the high execution, expected low latency, and fast consistency required for live origination.
- **Elemental Appliances & Software**: encodes, packages, and delivers video assets on-premises and seamlessly connects with cloud-based video infrastructure.

Internet of Things (IoT)

- **IoT**: enables secure, a bi-directional interface between Internet-connected things as well as the AWS Cloud over MQTT and HTTP.
- **FreeRTOS**: is an operating system that helps microcontroller-based edge devices simple to program, deploy, protect, and sustain.
- **IoT Analytics**: presents advanced data analysis for AWS IoT.
- **IoT Device Defender**: is an AWS IoT security service that enables the user to audit the arrangement of the devices, monitor the connected devices to recognize abnormal behavior, and to relieve security risks.
- **IoT Device Management**: is a cloud-based device administration service that makes it accessible for consumers to securely operate IoT devices throughout their lifecycle.
- **IoT Events**: enables the user to control the equipment or device fleets for malfunctions or changes in operation and to trigger actions whenever such events transpire.

AMAZON WEB SERVICES CHEAT SHEET 5

AWS Basics

AWS IAM - Best Practice

Listed below are several AWS IAM best practices aimed at securing AWS resources.

Best Practice Recommendations:

1. Avoid the use of root account unless strictly necessary.
2. Use temporary credentials.
3. Embrace the least privilege principle and review all IAM permissions periodically.
4. Enforce bi-directional least privilege principle.
5. Monitor account activity.
6. Use Multi-Factor Authentication (MFA.
7. Enforce strong passwords.

Cloud Migration Strategies

The complexity of migrating existing applications varies, depending on the architecture and existing licensing arrangements. The 6 most common application migration strategies are (The 6Rs):

- **Rehosting**: Lift & Shift
- **Replatforming**: Lift - Tinker - and - Shift (Example: change DB from Oracle to RDS or changing the JVM from WebSphere to Apache Tomcat).
- **Repurchasing**: Moving to a different product. Such as a move to a SaaS platform. (Example: migrating a CRM system to SalesForce, a HR system to Workday, or a CMS to Drupal.
- **Refactoring/Re-architecting**: Re-imagining how the application is architected and developed, typically using cloud-native features.
- **Retire**: Get rid of.
- **Retain**: Usually this means "revisit" or do nothing (for now). An example of this would be riding out some depreciation, not being ready to prioritize an application that was recently upgraded, or otherwise not inclined to migrate some applications.

AWS Services

Internet of Things (IoT) (Continued)

- **IoT Greengrass**: seamlessly stretches AWS onto physical devices with the help of the cloud for management, analytics, and durable storehouse.
- **IoT SiteWise**: easily assemble, design, and examine data from industrial facilities at scale.

Internet of Things (IoT) (Continued)

- **IoT Things Graph**: is an integrated set of instruments that allow developers to produce IoT applications utilizing devices and services.
- **IoT 1-Click**: is a service that helps devices to trigger AWS Lambda functions that perform a specific action.

Robotics

- **RoboMaker**: is a service that makes it accessible to generate, copy, and extend intelligent robotics applications at scale.

Blockchain

- **Managed Blockchain**: is a fully distributed service that makes it comfortable to organize and operate scalable blockchain networks with the help of popular open-source frameworks.

Game Tech

- **GameLift**: is a fully accomplished service for extending, conducting, and balancing session-based multiplayer game servers in the cloud.
- **Lumberyard**: is an independent AAA game engine deeply blended with AWS and Twitch—with full source.
- **Open 3D Engine**: an Apache 2.0 licensed multi-platform 3D engine.

AWS Cloud Adoption Framework

AWS Cloud Adoption Framework helps digitally transform and accelerate business outcomes through innovative use of AWS. AWS CAF identifies specific organizational capabilities that underpin successful cloud transformations. These capabilities provide best practice guidance that helps you improve your cloud readiness.

Capabilities & Perspectives

Business

- The **Business** perspective helps ensure that your cloud investments accelerate your digital transformation ambitions and business outcomes. Common stakeholders include chief executive officer (CEO), chief financial officer (CFO), chief operations officer (COO), chief information officer (CIO), and chief technology officer (CTO).

Platform

- The **Platform** perspective helps you build an enterprise-grade, scalable, hybrid cloud platform, modernize existing workloads, and implement new cloud-native solutions. Common stakeholders include CTO, technology leaders, architects, and engineers.

Governance

- The **Governance** perspective helps you orchestrate your cloud initiatives while maximizing organizational benefits and minimizing transformation-related risks. Common stakeholders include chief transformation officer, CIO, CTO, CFO, chief data officer (CDO), and chief risk officer (CRO).

People

- The **People** perspective serves as a bridge between technology and business, accelerating the cloud journey to help organizations more rapidly evolve to a culture of continuous growth, learning, and where change becomes business-as-normal, with focus on culture, organizational structure, leadership, and workforce. Common stakeholders include CIO, COO, CTO, cloud director, and cross-functional and enterprise-wide leaders.

Security

- The **Security** perspective helps you achieve the confidentiality, integrity, and availability of your data and cloud workloads. Common stakeholders include chief information security officer (CISO), chief compliance officer (CCO), internal audit leaders, and security architects and engineers.

Operations

- The **Operations** perspective helps ensure that your cloud services are delivered at a level that meets the needs of your business. Common stakeholders include infrastructure and operations leaders, site reliability engineers, and information technology service managers.

Use Cases

Technology

Migrate and modernize legacy infrastructure, applications, and data and analytics platforms. Cloud Value Benchmarking shows that migrating from on-premises to AWS leads to a 27% reduction in cost per user, a 58% increase in VMs managed per admin, a 57% decrease in downtime, and a 34% decrease in security incidents.

Process

Digitize, automate, and optimize your business operations. This may include leveraging new data and analytics platforms to create actionable insights or using machine learning (ML) to improve your customer service experience, employee productivity and decision-making, business forecasting, fraud detection and prevention, and industrial operations.

Organization

Reimagine how your business and technology teams create customer value and meet your strategic intent. Organizing your teams around products and value streams while leveraging agile methods to rapidly iterate and evolve will help you become more responsive and customer centric.

Product

Reimagine your business model by creating new value propositions and revenue models. Cloud Value Benchmarking shows that adopting AWS leads to a 37% reduction in time-to-market for new features and applications, a 342% increase in code deployment frequency, and a 38% reduction in the time it takes to deploy new code.

Benefits:

- Reduce business risk
- Improve environmental, social, and governance performance
- Grow revenue
- Increase operational efficiency

How it Works:

- **Envision**: Identify and prioritize transformation opportunities in line with your strategic objectives.

How it Works (Continued):

- **Align**: Identify capability gaps and cross-organizational dependencies.
- **Launch**: Deliver pilots in production and demonstrate incremental business value.
- **Scale**: Expand pilots and business value to desired scale and ensure that the business benefits associated with your cloud investments are realized and sustained.

AMAZON WEB SERVICES CHEAT SHEET 6

AWS Basics

AWS CloudTrail

AWS CloudTrail is a service that enables governance, compliance, and operational and risk auditing of AWS account. Actions taken by a user, role, or an AWS service are recorded as events as either control plane (actions on resources) or data plane events (actions within a resource) in CloudTrail.

- Records AWS account activity.
- Detects user activity and API usage.
- Delivers log files to Amazon S3 bucket.
- Enables data event logging.
- Identifies unusual activity in AWS accounts.

CloudTrail uses these events in **three features**:

- **Trails**: enable delivery and storage of events in Amazon S3, with optional delivery to Amazon CloudWatch Logs and EventBridge.
- **Insights**: analyzes control plane events for anomalous behavior in API call volumes.
- **Event History**: provides a 90-day history of control plane actions for free. As part of its core audit capabilities, CloudTrail provides customer managed keys for encryption and log file validation to guarantee immutability.

Use Cases:

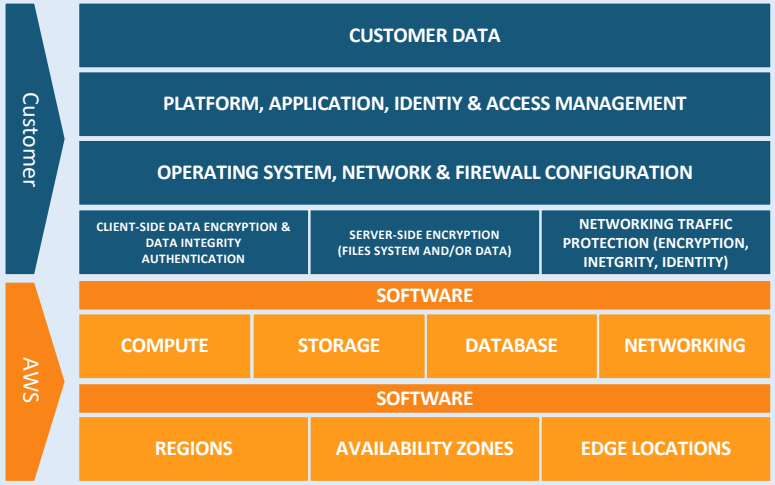
- **Audit Activity** - Monitor, store, and validate activity events for authenticity. Easily generate audit reports required by internal policies and external regulations.
- **Identity and Security Incident** - Detect unauthorized access using the Who, What, and When information in CloudTrail Events. Respond with rules-based EventBridge alerts and automated workflows.
- **Trouble Shooting Operational Issues** - Continuously monitor API usage history using machine learning (ML) models to spot unusual activity in your AWS accounts and determine root cause.

6 Advantages of Cloud

Key advantages of leveraging AWS include:

1. **Trade capital expense for variable expense**: Instead of having to invest heavily in data centers and servers before you know how you're going to use them, you can pay only when you consume computing resources, and pay only for how much you consume.
2. **Benefit from massive economies of scale**: By using cloud computing, you can achieve a lower variable cost than you can get on your own. Because usage from hundreds of thousands of customers is aggregated in the cloud, providers such as AWS can achieve higher economies of scale, which translates into lower pay as-you-go price.
3. **Stop guessing about capacity**: Eliminate guessing on your infrastructure capacity needs. When you make a capacity decision prior to deploying an application, you often end up either sitting on expensive idle resources or dealing with limited capacity. With cloud computing, these problems go away. You can access as much or as little capacity as you need and scale up and down as required.
4. **Increase speed and agility**: In a cloud computing environment, new IT resources are only a click away, which means that you reduce the time to make those resources available to your developers from weeks to just minutes. This results in a dramatic increase in agility for the organization since the cost and time it takes to experiment and develop is significantly lower.
5. **Stop spending money running and maintaining data centers**: Focus on projects that differentiate your business, not the infrastructure. Cloud computing lets you focus on your own customers, rather than on the heavy lifting of racking, stacking, and powering servers.
6. **Go global in minutes**: Easily deploy your application in multiple regions around the world with just a few clicks. This means you can provide lower latency and a better experience for your customers at minimal cost.

Shared Responsibility Model



Customer: Responsible for Security 'in' the cloud.
AWS: Responsible for Security 'of' the cloud.

AWS Config

AWS Config is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources.

- Evaluates AWS resource configurations.
- Tracks resource relationships.
- Manages compliance of AWS resource configurations.
- Captures point-in-time resource information.

AWS CloudWatch

AWS CloudWatch is the native monitoring service for resources and applications running in AWS. It gathers logs and monitors metrics for key resources like:

- Amazon EC2 instances.
- Amazon DynamoDB tables.
- Amazon RDS DB instances.
- Custom application and service generated metrics

AWS GuardDuty

AWS GuardDuty: is a threat detection service that continuously monitors for malicious activity and unauthorized behavior to protect your AWS accounts and workloads. Amazon GuardDuty exposes notifications via Amazon CloudWatch so you can trigger an automated response or notify a human.

AWS CLI (Command Line Interface): Basic Commands

- **rm <filename>**: removes file with specified filename from the current directory.
- **cat /proc/mounts**: lists mounted drives.
- **rpm -ql '<package name>'**: lists utilities contained within a package with specified name.
- **sudo yum update**: performs required AWS updates.
- **sudo chmod <options>**: changes access mode for the current directory.
- **sudo mkdir <directory name>**: creates a new directory.
- **sudo rmdir <directory name>**: removes the specified directory.
- **sudo reboot**: reboots the remove AWS system so that you can see the results of any changes made.
- **sudo yum groupinstall "<group package name>"**: installs the specified group of packages.
- **sudo yum search '<package name>'**: searches for package with specified package name.
- **sudo yum –y install <service or feature>**: installs required support service or feature.

AMAZON WEB SERVICES CHEAT SHEET 7

AWS Basics

Network ACL .vs Security Groups

The primary difference between Network Access Control Lists (NACL) and Security Groups (SG) are highlighted below:

Network Access Control List (NACL)

- **Scope:** NACL is the firewall of the **VPC Subnets.** They are applicable at the subnet level, so any instance in the subnet with an associated NACL will follow the rules of the NACL.
- **Stateful or Stateless**: NACL are stateless, which means any changes applied to an incoming rule will not be applied to the outgoing rule. E.G. If you allow an incoming port 80, an outgoing traffic rule would separately be required.
- **Rules (Allow/Deny)**: NACL supports allow and deny rules. By deny rules, it means it is possible to explicitly deny a certain IP address to establish a connection. E.G. Block IP address 123.201.57.39 from establishing a connection to an EC2 Instance.
- **Rules (Order)**: Rules are applied in their order (the rule with the lower number gets processed first).
- **Rules (Destination)**: Rules only allow **CIDR** [Classless Inter-Domain Routing] as destination.
- **Defense Order**: First layer of defense [inbound traffic] and Second layer defense [outbound traffic].
- **Occurrence**: Subnet can have only one NACL

Security Group (SG):

- **Scope:** SG a firewall for **EC2 Instances**.
- **Stateful or Stateless**: SG are stateful, which means any changes applied to an incoming rule will automatically be applied to the outgoing rule. E.G. If you allow an incoming port 80, an outgoing traffic rule would automatically be opened.
- **Rules (Allow/Deny)**: SG supports allow only (by default all rules are denied). It means that it is not possible to deny a certain IP address from establishing a connection.
- **Rules (Order)**: All rules in a security group are applied.
- **Rules (Destination)**: Rule allow CIDR, IP, SG as destination.
- **Defense Order**: Second layer of defense [inbound traffic] and First layer defense [outbound traffic].
- **Occurrence**: Instance can have multiple SG.

AWS Well Architected Framework

AWS Well-Architected Framework helps cloud architects build secure, high-performing, resilient, and efficient infrastructure for a variety of applications and workloads. Built around six pillars:

Operational excellence pillar focuses on running and monitoring systems, and continually improving processes and procedures. Key topics include automating changes, responding to events, and defining standards to manage daily operations.

1. Organization (Operational Priorities, Operating Model, Organizational Culture)
2. Prepare (Design Telemetry, Improve Flow, Mitigate Deployment Risks, Operational Readiness)
3. Operate (Understanding Workload Health, Understanding Operations Health)
4. Evolve (Learn from Experience, Make Improvements, Share Learnings)

Security pillar focuses on protecting information and systems. Key topics include confidentiality and integrity of data, managing user permissions, and establishing controls to detect security events.

1. Identity & Access Management
2. Detection
3. Infrastructure Protection
4. Data Protection
5. Incident Response

Reliability pillar focuses on workloads performing their intended functions and how to recover quickly from failure to meet demands. Key topics include distributed system design, recovery planning, and adapting to changing requirements.

1. Foundations
2. Workload Architecture
3. Change Management
4. Failure Management

Performance efficiency pillar focuses on structured and streamlined allocation of IT and computing resources. Key topics include selecting resource types and sizes optimized for workload requirements, monitoring performance, and maintaining efficiency as business needs evolve.

1. Selection
2. Review
3. Monitoring
4. Trade-offs

AWS Support Plans

	BASIC	DEVELOPER	BUSINESS	ENTERPRISE
Cost	FREE	$29.00/Mo	$100.00/Mo	$15,000/Mo
Use Case		Experimenting	Production Use	Mission-Critical Use
Tech Support	NO	Business hours via email	24x7 via email, chat & phone	24x7 via email, chat & phone
SLA		12-24 h at local business hours	1 h response to urgent support cases	15 min to critical support cases w/ priority.
TAM & Support Concierge	NO	NO	NO	YES
Support Cases	NONE	1 Person, Unlimited Cases.	Unlimited Contacts/Cases.	Unlimited Contacts/Cases

Cost optimization pillar focuses on avoiding unnecessary costs. Key topics include understanding spending over time and controlling fund allocation, selecting resources of the right type and quantity, and scaling to meet business needs without overspending.

1. Practice Cloud Financial Management
2. Expenditure and usage awareness
3. Cost effective resources
4. Management demand and supply resources
5. Optimize over time

Sustainability pillar focuses on minimizing the environmental impacts of running cloud workloads. Key topics include a shared responsibility model for sustainability, understanding impact, and maximizing utilization to minimize required resources and reduce downstream impacts.

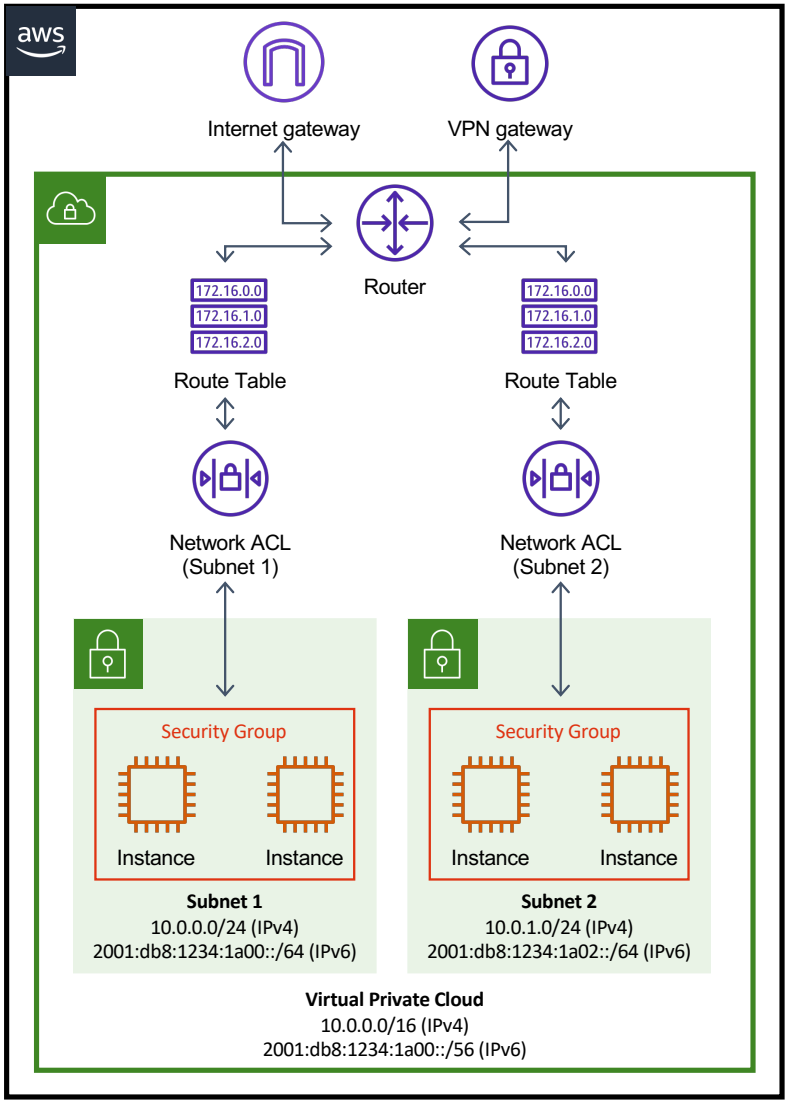
Goal: The AWS Well-Architected framework provides a consistent approach to evaluate architectures and implement scalable designs.

AMAZON WEB SERVICES

CHEAT SHEET 8

AWS Basics

Security



AMAZON WEB SERVICES

CHEAT SHEET 9

AWS Basics

IAM best practices to secure your AWS resources:

- **Authentication** - create and manage identities such as users, groups, and roles as well as authentication for resources, people, services, and apps within an AWS account.
- **Authorization** - primary components **Policies** and **Permissions.**
- **Fine-Grained Permissions** - permission users based on needs.
- **Shared Access to AWS Accounts** - Simplified multi-account access without sharing credentials.
- **AWS Organizations** - Fine grained control for multiple AWS accounts.
- **Identity Federation** - federated access from other identify providers like Active directory.

•**Authentication:** AWS IAM lets you create and manage identities such as users, groups, and roles, meaning you can issue and enable authentication for resources, people, services, and apps within your AWS account. In the next section, we'll look at authentication in detail.
•**Authorization:** Access management or authorization in IAM is made of two primary components: **Policies** and **Permissions**. In the next section, we'll also look at each of these.
•**Fine-grained permissions:** Consider this — you want to provide the sales team in your organization access to billing information, but also need to allow the developer team full access to the EC2 service, and the marketing team access to selected S3 buckets. Using IAM, you can configure and tune these permissions as per the needs of your users.
•**Shared access to AWS accounts:** Most organizations have more than one AWS account, and at times need to delegate access between them. IAM lets you do this without sharing your credentials, and more recently, AWS released ControlTower to further simplify multi-account configurations. We also published a quick, hands-on tutorial on Securing Multi-Account Access on AWS.
•**AWS Organizations:** For fine-grained control for multiple AWS accounts, you can use AWS Organizations to segment accounts into groups and assign permission boundaries.
•**Identity Federation:** Many times, your organization will need to federate access from other identity providers such as Okta, G Suite, or Active Directory. IAM enables you to do this with a feature called Identity Federation.

•**Avoid the use of root account unless strictly necessary:** Do not use the root account for day to day administration activities. By default, the root account user has access to all resources for all AWS services and it's best practice to create IAM users with least privilege access. Additionally, do not create access keys for the root account unless strictly necessary. Finally, set up monitoring to detect and alert on root account activity, and ensure hardware-based MFA is set up for root account access.
•**Use temporary credentials:** Never share your credentials with anyone. It's advisable to create individual users for anyone who has access requirements and even better use temporary credentials. Dynamically generated credentials that expire after a configurable interval, are a great way to tackle this. You can visit our practical tutorial on Securing Multi-Account Access on AWS for detailed instructions on this.
•**Embrace the least privilege principle and review all IAM permissions periodically:** It is important to follow the security principle of least privilege, which means that if a user doesn't need to interact with a resource, then it is best not to provide them access to that resource. IAM permissions allow for very granular access controls, so avoid the use of policy statements that grant access to all actions, all principals, or all resources. Additionally, use the IAM Access Advisor regularly to ensure that all permissions assigned to a particular user are indeed being used.
•**Enforce the least privilege principle to be implemented bi-directionally**: Many AWS resources (such as S3 buckets) can have their access policy attached directly. Don't fall into the trap of thinking that because access is tightly controlled in one direction (i.e. an IAM Role that grants very specific permissions), that you should be less rigid in the other direction (for example, when an S3 bucket access policy grants read access to all entities in your account). Optimally use both sides of the least privilege principle to achieve favorable outcomes.
•**Monitor account activity regularly using IAM Access Analyzer and AWS CloudTrail:** In addition to what we discussed about the newly released IAM Access Analyzer, the good old AWS CloudTrail is an excellent tool to monitor all activities in your account. You can easily use CloudTrail logs to identify suspicious activity and take necessary actions depending on your findings. You will find our deep-dive, practical tutorial on AWS Security Logging with CloudTrail interesting with step by step instructions to help you do this.
•**Use Multi-Factor Authentication (MFA)**: Enable MFA to build an additional layer of security for interaction with the AWS API.
•**Enforce strong passwords:** Enforce strong passwords by configuring account password policy that involves password rotation, discourages the use of old passwords, only allows alphanumeric characters, and more.