**AWS**

**General**

[AWS Well Architected framework](https://docs.aws.amazon.com/wellarchitected/latest/framework/welcome.html)

[AWS Professional Services](https://aws.amazon.com/professional-services/)

[AWS Support](https://docs.aws.amazon.com/awssupport/latest/user/getting-started.html)

[AWS Support Plan](https://aws.amazon.com/premiumsupport/plans/)

[6 advantages of CC](https://docs.aws.amazon.com/whitepapers/latest/aws-overview/six-advantages-of-cloud-computing.html)

**Identity and Access Management**

IAM User

4 ways in which a user can access AWS

* Console Password
* Access Keys
* SSH keys for use with CodeCommit
* Server Certificates

Each IAM user is associated with one and only one AWS account. Because users are defined within your AWS account, they don't need to have a payment method on file with AWS. Any AWS activity performed by users in your account is billed to your account.

[Change permission for IAM User](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_users_change-permissions.html)

IAM Security Groups

IAM User Group

IAM Role

IAM Policy

2 types – Resource based and Identity Based

Always use managed policies instead of inline)

IAM Access Analyzer

Best Security Practices

* Lock away your AWS account root user access keys
* Use roles to delegate permissions
* Grant least privilege
* Get started using permissions with AWS managed policies
* Validate your policies
* Use customer managed policies instead of inline policies
* Use access levels to review IAM permissions
* Configure a strong password policy for your users
* Enable MFA
* Use roles for applications that run on Amazon EC2 instances
* Do not share access keys
* Rotate credentials regularly
* Remove unnecessary credentials
* Use policy conditions for extra security
* Monitor activity in your AWS account
* A Security Group is stateful, that is, it automatically allows the return traffic.
* MFA can be done either with Virtual MFA Device (Google Authenticator) or physical hardware device like Hardware MFA devices or U2F security key (plug into USB port).

**Compute**

EC2

AMI

[EC2 Pricing](https://aws.amazon.com/ec2/pricing/)

EC2 Reserve Types

AWS Lightsail (small compute, storage and network capability)

ECS

ECR

Fargate

Lambda

* AMI should be from the same region as EC2.
* EC2 instance user data is the data that you specified in the form of a bootstrap script or configuration parameters while launching your instance.
* AWS Lambda is Event Driven service and there is pay per request/call and compute time model.

**Storage**

S3

[S3 Lifecycle Management](https://docs.aws.amazon.com/AmazonS3/latest/userguide/object-lifecycle-mgmt.html)

EBS

The fundamentals charges for EBS volumes are:

* the volume type (based on performance)
* the storage volume in GB per month provisioned
* the number of IOPS provisioned per month
* the storage consumed by snapshots
* outbound data transfer

[Types of EBS volumes](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-volume-types.html)

EFS

FSx

EC2 Instance Store – Temporary, fast performance. It is physically connected to the host computer. Since data is ephemeral, good use case if buffer/cache/scratch data.

[AWS Storage Gateway](https://aws.amazon.com/storagegateway/)

It is a hybrid cloud storage service that provide on-premises access to virtually unlimited cloud storage.

Datasync

* Usually for DB, use Provisioned IOPS SSD EBS. These are specifically designed for database workloads and offer the lowest latency storage options for an ec2 instance.
* EBS offers root volume (for booting OS) not EFS.
* Amazon EC2 and other AWS compute instances running in multiple Availability Zones within the same AWS Region can access the EFS, so that many users can access and share a common data source.
* In S3, there are no charges for (1) Data transferred in from the internet, (2) Data transferred out to an EC2 instance, when the instance is in the same AWS Region as the S3 bucket, (3) Data transferred out to Amazon CloudFront (CloudFront).
* All S3 storage classes (except One Zone) stores data in a minimum of 3 AZ.
* Out of all storage services, only EFS can be used directly with on-premise systems that too only with the help of AWS Direct Connect or AWS VPN.

**Database**

RDS

Aurora

DynamoDB

DynamoDB Accelerator ()

DynamoDB Global Tables

ElastiCache

Redshift (OLAP)

EMR (Big Data)

Athena (SQL to S3)

Quicksight

Neptune (GraphDB)

DocumentDB (Managed MongoDB)

Database Migration Service

QLDB

Managed Blockchain

Glue (ETL)

[DB MultiAZ Deployments](https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.MultiAZ.html)

* Currently, all DB instances in a multi-master cluster must be in the same AWS Region. You can't enable cross-Region replicas from multi-master clusters.
* RDS DB exists on 1 AZ only, whereas DynamoDB is there on multiple.
* You can do both homogeneous and heterogeneous database migration using Database Migration Service.

**Deployment and Managing Infra at Scale**

CloudFormation

AWS Quick Starts references

Quick Starts are built by AWS solutions architects and partners to help you deploy popular technologies on AWS, based on AWS best practices for security and high availability. These accelerators reduce hundreds of manual procedures into just a few steps, so you can build your production environment quickly and start using it immediately.

Each Quick Start includes AWS CloudFormation templates that automate the deployment and a guide that discusses the architecture and provides step-by-step deployment instructions.

AWS CDK - CloudFormation in custom programming language instead of yaml

Beanstalk - Elastic Beanstalk is an example of a PaaS service. You can simply upload your code and Elastic Beanstalk automatically handles the deployment, from capacity provisioning, load balancing, auto-scaling to application health monitoring.

CodeDeploy - Deploy your code on ec2 or onprem - hybrid

CodeCommit (like Github)

CodeBuild

CodePipeline

CodeArtifact

CodeStar - Unified UI to easily manage software development activities in one place

Cloud9 (Cloud IDE)

AWS System Manager (SSM)

Hybrid Service - Systems Manager provides a central place to view and manage your AWS resources, so you can have complete visibility and control over your operations.

SSM Session Manager

Through this, you can SSH into EC2/Onprem, without opening Port 22, need to have SSM Agent installed

Opsworks - Managed Chef and puppet service – used for configuration mgmt. It’s alternative to SSM

**AWS Global Infrastructure**

AWS Route 53 - DNS, can also perform health check & monitoring

AWS CloudFront

Edge Locations

[S3 Transfer Acceleration](https://aws.amazon.com/s3/transfer-acceleration/)  
[AWS Global Accelerator](https://aws.amazon.com/global-accelerator/?blogs-global-accelerator.sort-by=item.additionalFields.createdDate&blogs-global-accelerator.sort-order=desc&aws-global-accelerator-wn.sort-by=item.additionalFields.postDateTime&aws-global-accelerator-wn.sort-order=desc) (For TCP/UDP/VoIP, not HTTP)  
[AWS Outpost](https://docs.aws.amazon.com/outposts/latest/userguide/what-is-outposts.html)

AWS Wavelength – 5G  
AWS Local Zone  
Global Application Architecture

Single Region, Single AZ/ Single Region, Multi AZ/Multi Region Active-Passive/Multi Region Active-Active

**Cloud Integration**

AWS SQS

AWS SNS

AWS Kinesis (real time big data streaming)

Amazon MQ (managed RabbitMQ and ApacheMQ)

**Cloud Monitoring**

CloudWatch

Amazon CloudWatch is a monitoring service for AWS cloud resources and the applications you run on AWS. You can use Amazon CloudWatch to collect and track metrics, collect and monitor log files, and set alarms. Amazon CloudWatch can monitor AWS resources such as Amazon EC2 instances, Amazon DynamoDB tables, and Amazon RDS DB instances, as well as custom metrics generated by your applications and services, and any log files your applications generate.

You can use Amazon CloudWatch to gain system-wide visibility into resource utilization, application performance, and operational health. You can use these insights to react and keep your application running smoothly.)

CloudWatch Metrics

CloudWatch Alarm

CloudWatch Logs

Can be collected from Beanstalk, ECS, Lambda, CloudTrail, Route 53, CloudWatch Log Agents. For getting logs from EC2, install CloudWatch Logs Agent)

CloudWatch Events (EventBridge – next version of this)

CloudTrail

API access

There are three types of events that can be logged in CloudTrail: management events, data events, and CloudTrail Insights events.

By default, CloudTrail logs all management events and does not include data events or Insights events. Additional charges apply for data and Insights events.)

AWS CloudTrail Insights

AWS X-Ray (Debugging applications on Production)

CodeGuru

An ML powered service for automated code reviews and application performance recommendations

Service Health Dashboard

Can be used to subscribe to an RSS feed to be notified of the status of all AWS service interruptions)

Personal Health Dashboard

**Virtual Private Cloud**

AWS VPC

Subnet (public and private)

Internet Gateway

Access internet from an instance in private VPC, it is a logical connection not physical. Only one can be associated with a VPC.

NAT Gateway (AWS managed) & NAT Instance (self-managed)

Allow your instance in your Private Subnet to access internet while remaining private.

NACL

Works as a firewall at subnet level, has both allow and deny rules

[VPC Flow Logs](https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs.html)

VPC Peering

Connects two VPC’s together, it is non transitive.

VPC Endpoint

Allow you to connect to AWS services using a private network instead of public www – this gives you enhanced security and lower latency.

VPC Endpoint Gateway can be used to connect to S3 and DynamoDB. VPC Endpoint Interface, for all rest of the services.

[Site to Site VPN](https://docs.aws.amazon.com/vpn/latest/s2svpn/VPC_VPN.html)

There are 2 ways of connecting your onprem data center to AWS, first is Site to Site VPN and second is Direct Connect.

AWS Site-to-Site VPN enables you to securely connect your on-premises network or branch office site to your Amazon Virtual Private Cloud (Amazon VPC). VPN Connections are a good solution if you have an immediate need and have low to modest bandwidth requirements. This connection goes over the public internet. A virtual private gateway is the VPN concentrator on the Amazon side of the Site-to-Site VPN connection. A customer gateway is a resource in AWS that provides information to AWS about your Customer gateway device.

AWS Direct Connect

Transit Gateway - Star topology

Difference between Internet gateway and NAT gateway is that IG allows instances with public IP to access internet, while NAT gateway allows for a private subnet. Another difference is that Internet Gateway works 2 ways, while NAT Gateway works one way by default.

**Security**

Shared Responsibility Model

DDos Protection: WAF and Shield

Penetration Testing

AWS allows security assessment or penetration tests against their AWS infra without prior approval for 8 services – Ec2 instances NAT Gateway and Elastic Load Balancer, RDS, Beanstalk, Aurora, CloudFront, Lambda and Lambda edge functions, API Gateway, Fargate

AWS KMS - AWS manages the encryption keys for us  
CloudHSM - Here we manage our keys ourselves, AWS provisions an encryption hardware

AWS Certficate Manager

AWS Certificate Manager is a service that lets you easily provision, manage, and deploy public and private Secure Sockets Layer/Transport Layer Security (SSL/TLS) certificates for use with AWS services and your internal connected resources. SSL/TLS certificates are used to secure network communications and establish the identity of websites over the Internet as well as resources on private networks. AWS Certificate Manager removes the time-consuming manual process of purchasing, uploading, and renewing SSL/TLS certificates.

AWS Secret Manager

AWS Secrets Manager helps you protect secrets needed to access your applications, services, and IT resources. The service enables you to easily rotate, manage, and retrieve database credentials, API keys, and other secrets throughout their lifecycle.

AWS GuardDuty - Intelligent threat discovery service. AWS Guard Duty works on EC2 and S3. It is a security monitoring service that processes logging info from services such as CloudTrail, VPC flow logs, DNS logs and Kubernetes Audit logs

AWS Inspector – Automated Security Assessment service which works on EC2 and ECR.

AWS Config

Macie

Amazon Macie is a fully managed data security and data privacy service that uses machine learning and pattern matching to discover and protect your sensitive data in AWS.

Security Hub

AWS Security Hub provides you with a comprehensive view of your security state in AWS and helps you check your environment against security industry standards and best practices. Security Hub collects security data from across AWS accounts, services, and supported third-party partner products and helps you analyze your security trends and identify the highest priority security issues.

Amazon Detective

AWS Shield – Free service

AWS Shield Advanced

It includes intelligent DDoS attack detection and mitigation for not only for network layer (layer 3) and transport layer (layer 4) attacks but also for application layer (layer 7) attacks. AWS Shield Advanced provides expanded DDoS attack protection for web applications running on the following resources: Amazon Elastic Compute Cloud, Elastic Load Balancing (ELB), Amazon CloudFront, Amazon Route 53, AWS Global Accelerator.

AWS Web Application Firewall  
WAF protects Amazon API Gateway API, Amazon CloudFront or an Application Load Balancer. It works on Layer 7 and monitors HTTP and HTTPS. AWS WAF also lets you control access to your content. AWS WAF has to be enabled by the customer and comes under the customer's responsibility. It protects against SQL Injection and XSS attacks and gives you control on how traffic reaches your app.

**Billing**

[AWS budgets](https://docs.aws.amazon.com/cost-management/latest/userguide/budgets-managing-costs.html)

[Cost Explorer](https://docs.aws.amazon.com/cost-management/latest/userguide/ce-what-is.html)

AWS Organizations

AWS Organizations offers policy-based management for multiple AWS accounts. With Organizations, you can create groups of accounts, automate account creation, apply and manage policies for those groups. Organizations enables you to centrally manage policies across multiple accounts, without requiring custom scripts and manual processes. It is not used to send, store, and receive message between software components.

[AWS Security Token S](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_temp.html)ervice (Global Service)

Amazon Cognito

Lets you add user sign-up, sign-in, and access control to your web and mobile apps quickly and easily. Amazon Cognito scales to millions of users and supports sign-in with social identity providers, such as Apple, Facebook, Google, and Amazon, and enterprise identity providers via SAML 2.0 and OpenID Connect.

**Compute Optimizer –** It recommends optimal AWS resource for your workloads to reduce cost & improve performance by using ML. It works on 3 resources: EC2, EBS, Lamda.

Its algo is same as that of AWS Cost Explorer, but there the focus is on cost, here it is on correct resource (Only EC2).

[AWS Savings Plan](https://docs.aws.amazon.com/savingsplans/latest/userguide/what-is-savings-plans.html) (3 types)

**Compute Savings Plan(Amazon EC2, AWS Lambda, and AWS Fargate)** - Upto 66% discount compared to On-Demand for a commitment to a consistent amount of usage of 1 or 3 years and offers possibility to change EC2 instance family type.

**EC2 Instance saving plan** – Upto 72% discount compared to On-Demand for a commitment to a consistent amount of usage of 1 or 3 years and but does not offer possibility to change EC2 instance family type. Can change size, OS and tenancy (host, dedicated, default).

**SageMaker Savings Plan** - SageMaker Savings Plans provide savings up to 64 percent off of On-Demand rates. These plans automatically apply to your SageMaker instance usage regardless of instance family (for example, ml.m5, ml.c5, etc.), instance sizes (for example ml.c5.large, ml.c5.xlarge, etc.), Region (for example, us-east-1, us-east-2, etc.), and component (for example, Notebook, Training, etc.)

* To get the benefits of idle reserved instance in AWS Organizations, they must be launched in same AZ.
* The AWS account must be able to operate as a standalone account. Only then it can be removed from AWS organizations.

**Machine Learning**

Amazon Rekognition

With Amazon Rekognition, you can identify objects, people, text, scenes, and activities in images and videos, as well as to detect any inappropriate content

Amazon SageMaker

Amazon SageMaker is a fully-managed platform that enables developers and data scientists to quickly and easily build, train, and deploy machine learning models at any scale.

Amazon Comprehend

Amazon Comprehend is a natural language processing (NLP) service that uses machine learning to find meaning and insights in text.

Amazon Lex

Amazon Lex is a service for building conversational interfaces using voice and text. Powered by the same conversational engine as Alexa, Amazon Lex provides high-quality speech recognition and language understanding capabilities, enabling the addition of sophisticated, natural language ‘chatbots’ to new and existing applications.

Amazon Polly - Converts text to speech

Amazon Transcribe - Converts speech to text

Amazon Translate – Language Translation

Amazon Connect – AWS public cloud customer contact center

Amazon Forecast

It is a fully managed service that uses machine learning to deliver highly accurate forecasts. Based on the same technology used at Amazon.com, Forecast uses machine learning to combine time series data with additional variables to build forecasts.

Amazon Kendra

It is an intelligent search service powered by machine learning (ML). Kendra reimagines enterprise search for your websites and applications so your employees and customers can easily find the content they’re looking for, even when it’s scattered across multiple locations and content repositories within your organization.

Amazon Personalize

Enables developers to build applications with the same machine learning (ML) technology used by Amazon.com for real-time personalized recommendations – no ML expertise required.

Amazon Textract

It is a machine learning (ML) service that automatically extracts text, handwriting, and data from scanned documents. It goes beyond simple optical character recognition (OCR) to identify, understand, and extract data from forms and tables.

**Others**

Amazon Sumerian (3D)

[Audit Manager](https://aws.amazon.com/audit-manager/)

[AWS Acceptable Use policy](https://aws.amazon.com/aup/)

Amazon WorkSpaces

It is a managed, secure Desktop-as-a-Service (DaaS) solution. You can use Amazon WorkSpaces to provision either Windows or Linux desktops in just a few minutes and quickly scale to provide thousands of desktops to workers across the globe.

APN Technology Partner

APN Technology Partners provide hardware, connectivity services, or software solutions that are either hosted on or integrated with, the AWS Cloud.

**General Notes**  
**AWS Services which are global:**

* IAM
* CloudFront
* Route 53
* WAF

\*\*S3 is a regional service

**An online gaming company wants to block users from certain geographies from accessing its content. Which AWS services can be used to accomplish this task?**

AWS Route53 and WAF

**Which of the AWS services can be used to prevent Distributed Denial-of-Service (DDoS) attack?**

AWS Shield, WAF, CloudFront with Route53

**You will pay a fee each time you read from or write data stored on the EFS - Infrequent Access storage class** - The Infrequent Access storage class is cost-optimized for files accessed less frequently. Data stored on the Infrequent Access storage class costs less than Standard and you will pay a fee each time you read from or write to a file.

**Amazon EBS Snapshots are stored incrementally, which means you are billed only for the changed blocks stored** - Amazon EBS Snapshots are a point in time copy of your block data. For the first snapshot of a volume, Amazon EBS saves a full copy of your data to Amazon S3. EBS Snapshots are stored incrementally, which means you are billed only for the changed blocks stored.

**Notes**

* AWS follows “save when you reserve” policy.
* CloudTrail Logs, S3 Glacier, AWS Storage Gateway have encryption supported by default.
* Security Group has allow rules only, while NACL has allow and deny rules both.
* Credits are applied in the following order:
* Soonest expiring
* Least number of applicable products
* Oldest credit
* Only AWS Business and Enterprise Support plans have programmatic access to AWS Support Center features.
* Reservations provide you with greater discounts, up to 75%, by paying for capacity ahead of time. Some of the services you can reserve include: EC2, DynamoDB, ElastiCache, RDS, and RedShift.







