



KodeKloud

Bringing it all together





Summary of Cloud Computing



What Is Cloud Computing? - Summary



Cloud Computing is the on-demand delivery of IT resources, particularly compute power, application hosting, database application, networking, and more



Three models of deployment: Cloud, On-Premises, and Hybrid



Works on a Client-Server model



Provides almost instant pay-as-you-go access to compute resources/ app hosting





What Is AWS?



What Is AWS? - Summary



Amazon Web Services or AWS was the first large-scale cloud provider



AWS was launched in 2006, with S3 as the first service



Since then, AWS has grown to 300+ services



Signing up is free; all services usually are pay-to-use



AWS has one of the largest communities, market positioning, and growth in the industry





Benefits of Cloud



Benefits of Cloud - Summary



Trade upfront expense for variable expense



Stop focusing on data centers



Stop guessing capacity



Benefit from economies of scale



Increase your speed and agility



Go global in minutes





Cloud Economics



Cloud Economics - Summary



Free Tier means that certain services are always free, and some are free for 12 months after new account creation



On-Demand is full pricing and pay-as-you-go, but no contract and very flexible



Reservations are contracts that you enter with Amazon for 1-3 years



Volume Discounts are pay less per unit as you use more

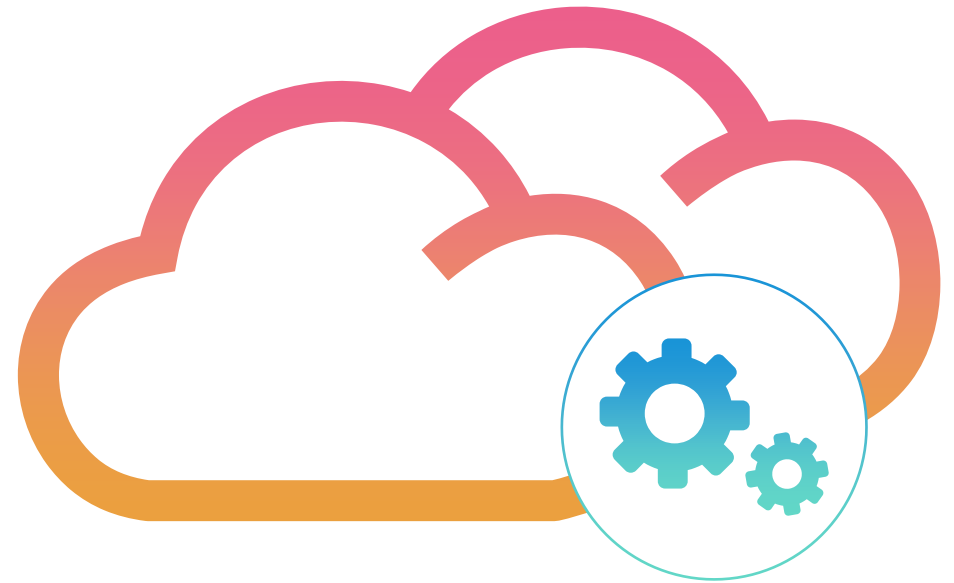


Price Drops are random price cuts that AWS does every few years on its services





Cloud Native Design Principles



Cloud Native Design Principles - Summary



Design for failure



Decouple components



Implement elasticity



Think parallel



Summary on Security and Compliance





AWS Shared Responsibility Model



AWS Shared Responsibility Model - Summary



The shared responsibility model delineates the customer's responsibilities and AWS's responsibilities



Unmanaged services need to be secured by users



Managed services offload some of the security responsibility onto AWS



AWS Shared Responsibility Model - Summary



Compliance and regulatory frameworks are sets of guidelines and best practices that organizations must follow



AWS compliance reports can be accessed on-demand from AWS Artifact



The AWS Compliance Center is a central location to research cloud-related regulatory requirements and how they impact your industry.



Audit manager continuously collects data to prepare for audits and ensures that you are achieving compliance with regulatory standards



AWS config monitors the configuration state of AWS resources over time



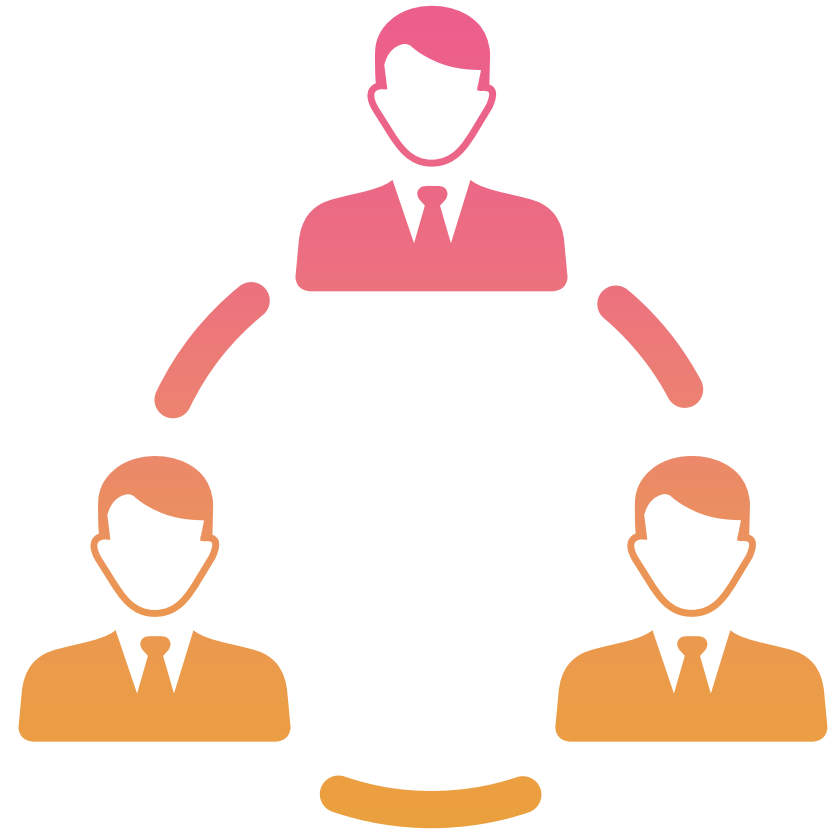
AWS Shared Responsibility Model

On-Premises	IaaS	PaaS	SaaS
Application	Application	Application	Application
Data	Data	Data	Data
Runtime	Runtime	Runtime	Runtime
Middleware	Middleware	Middleware	Middleware
OS	OS	OS	OS
Virtualization	Virtualization	Virtualization	Virtualization
Servers	Servers	Servers	Servers
Storage	Storage	Storage	Storage
Network	Network	Network	Network





Identity Access Management (IAM) Users, Groups, Roles



Identity Access Management **Users, Groups, Roles**

- Summary



Root user has unlimited access and no restrictions



IAM is responsible for managing access to AWS resources



An IAM user represents a person or application that needs access to AWS or a subset of services



Policies are documents that either grant or deny access to specific AWS services/resources



Identity Access Management Users, Groups, Roles

- Summary



Groups are a collection of IAM users



Roles allow a user to get temporary access to a service or resource



Least-privilege permissions – Grant users or entities the minimum level of access required to perform their specific tasks, reducing the risk of unauthorized actions or potential security breaches



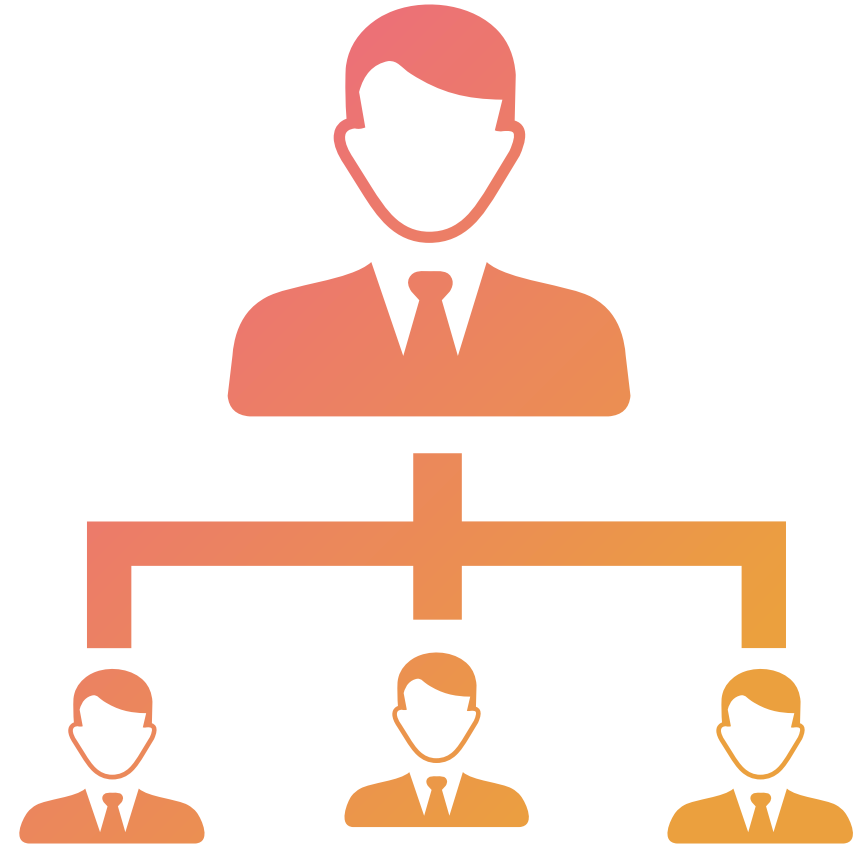
Policy

```
Terminal
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "SecondStatement",
      "Effect": "Allow",
      "Action": "ec2:*",
      "Resource": "*"
    },
    {
      "Sid": "ThirdStatement",
      "Effect": "Allow",
      "Action": [
        "s3:List*",
        "s3:Get*"
      ],
      "Resource": [
        "arn:AWS:s3:::bucket1",
        "arn:AWS:s3:::bucket1/*"
      ]
    }
  ]
}
```





AWS Organizations



AWS Organizations - Summary



Organizations help manage multiple AWS accounts



Organizational units (OUs) allow you to group accounts with similar business or security requirements



Service Control Policies (SCPs) restrict what an account can do



SCPs can be applied to individual accounts or OUs





Security Resources



Security Resources - Prevention - Summary



WAF prevents applications from common attacks like SQL injection and XSS attack



Shield prevents apps and services from DDoS attacks



Network Firewalls monitor traffic entering and leaving VPCs



Security Resources – Detection - Summary



GuardDuty monitors and detects suspicious activity and potential threats in your AWS environment



Detective helps analyze and investigate security-related events by collecting and visualizing data



CloudTrail logs and monitors all user and API activity within an AWS account



AWS Config tracks and audits the configuration of AWS resources over time



Security Hub automates security checks and brings alerts to a central location. Also performs validation on AWS best practices



Security Lake collects logs from a variety of locations and transforms them into a query-efficient format



AWS Macie scans S3 buckets for sensitive data and notifies users of findings



Security Resources – Management - Summary



Firewall Manager helps manage security configurations across multiple AWS accounts



Resource Access Manager helps you securely share resources across accounts, organizations, and organizational units



Cognito provides authentication (with social logins), authorization, and user management for web and mobile applications



IAM enables you to manage user identities and their access to AWS resources



Identity Center provides a central location for managing user authentication across multiple AWS accounts



Secrets Manager allows you to securely store and manage sensitive information like passwords and credentials



Security Resources – Management - Summary



AWS Certificate Manager (ACM) provisions, manages, and deploys SSL/TLS certificates for AWS resources



Private Certificate Authority manages your own private certificate authority within AWS



Key Management Service (KMS) creates and manages encryption keys used to encrypt data



Hardware Security Module (HSM) – AWS provides a dedicated hardware to store and operate cryptographic keys

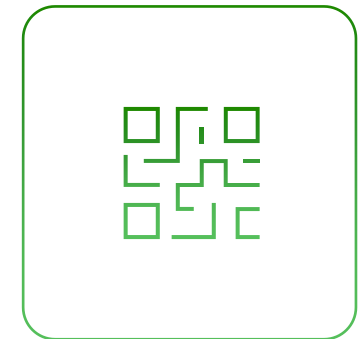
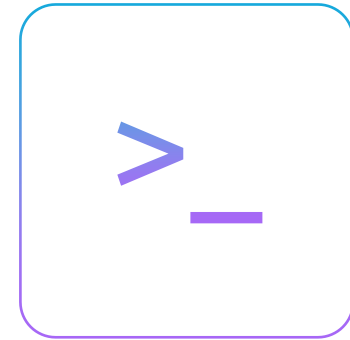


Summary on Technology





Deployment Methods



Deployment Methods - Summary



Console



CLI



SDK





Global infrastructure



Global Infrastructure - Summary



Regions are locations to which certain services can be deployed



Not all services are available in all Regions



Availability Zones (AZ) are isolated and independent datacenters inside Regions



Edge locations are smaller Points of Presence where services are run closer to customers



Local Zones are extensions of AWS regions located near users in select metropolitan areas





Networking



Networking - Summary



VPC isolates computing resources from other computing resources available in the cloud



VPCs are isolated to a region



VPC CIDR block defines the ip addresses a VPC can use



Subnets are a range of ip addresses within a VPC



Subnets reside within a single Availability Zone



Networking - Summary



Subnets can be made public/private using Internet Gateways & Nat Gateways



Internet Gateways allow subnets to communicate with internet & vice versa



NAT Gateways allow subnets to talk to the internet but connections must be initiated from within the VPC



Virtual Private Gateway enable secure access to private resources over the internet



Direct Connect(DX) is a direct connection into an aws regions that provide low latency + high speeds



Default VPC - Summary



Every region has a Default VPC with default subnets, Security Groups, and NACLs



The CIDR block for the Default is 172.31.0.0/16



The Default VPC and its subnets have outbound access to the Internet by default.



One default subnet in each Availability Zone



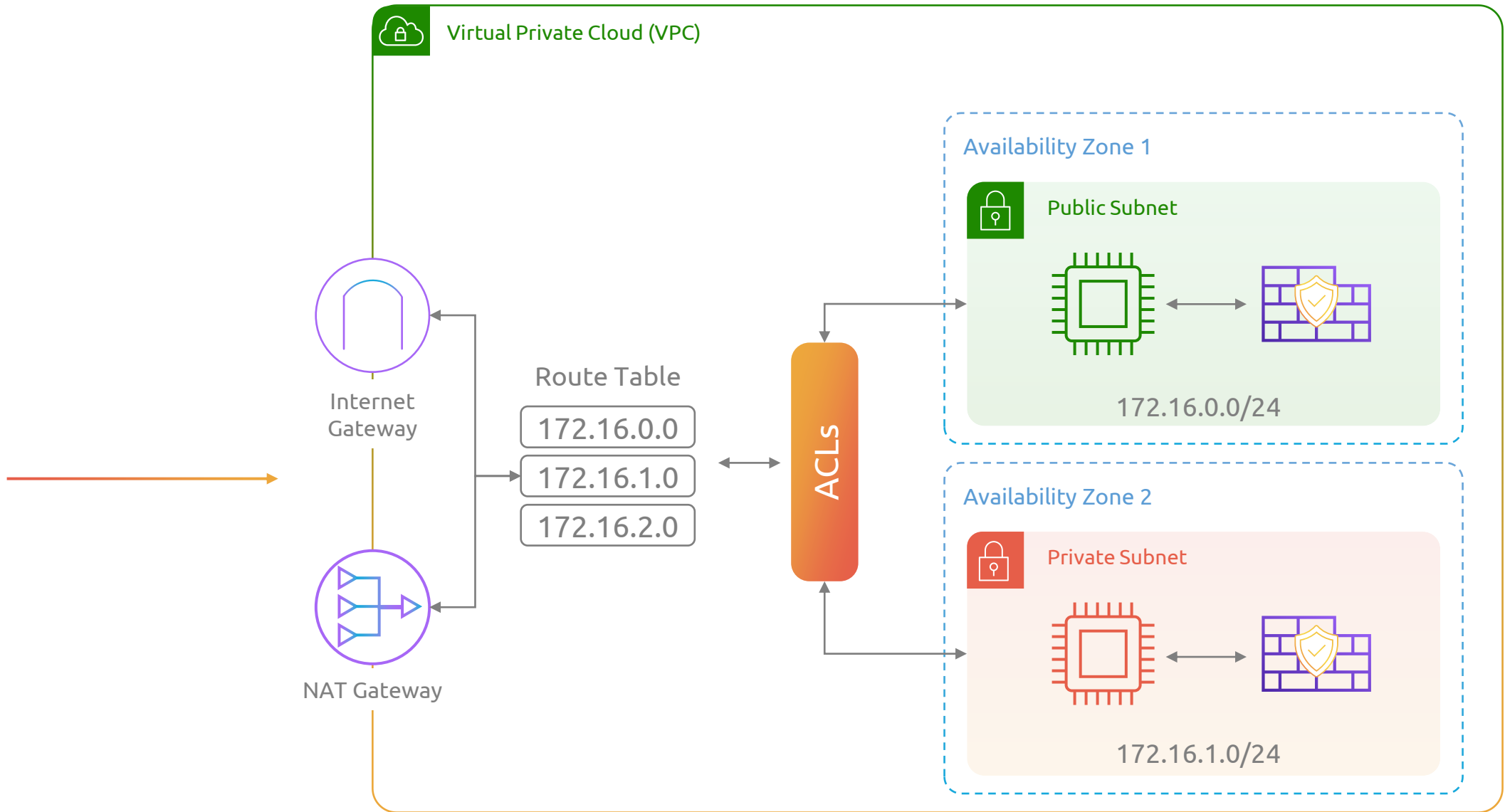
The Security Groups allow outbound and the NACLs are open in both inbound and outbound directions.



Firewalls - Summary

- ✓ Stateless firewalls require traffic to be explicitly permitted inbound & outbound
- ✓ Stateful firewalls are intelligent firewalls that track requests and allow response
- ✓ Network ACLs filter traffic entering & leaving a subnet
- ✓ Network ACLs are stateless firewalls
- ✓ Security Groups act as firewalls for individual resources such as EC2, NICs, and other network objects
- ✓ Security Groups are stateful firewalls







Storage



Block Storage - Summary



A collection of blocks can be presented to the OS as a volume



EBS Volumes can be mounted & booted



EBS Volumes are within an Availability Zone



Instance Stores are removed when EC2 instances are stopped/started



File Storage - Summary



File Storage services like EFS store data in a hierarchical structure of files and folders



It is accessible over the network



EFS can be mounted as a file system inside an OS



It cannot be used as a boot volume (can't install OS)



Object Storage - Summary



Objects are just files



Flat file structure (no folders); but they look like folders



Great for storing media files, logs, audit reports or basically any file you want.



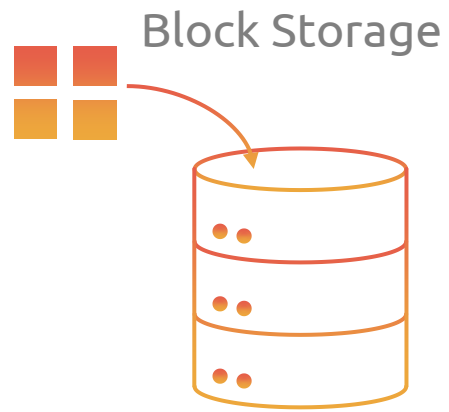
API storage so it cannot be and should not be mounted or boot.



Storage classes impact accessibility, resiliency, and cost



Types of Storage



Amazon Elastic Block Store (Amazon EBS)



Amazon Elastic File System (Amazon EFS)



Amazon Simple Storage Service (Amazon S3)





Compute



Elastic Compute Cloud (EC2) - Summary



EC2 allows you to provision a server in AWS within minutes



AMIs are templates for deploying EC2 instances



AWS has a variety of instance types to support all your computing needs(Memory, Compute, Storage optimized)



AWS supports a wide variety of Operating Systems from RHEL, SUSE, Ubuntu, Amazon Linux and Windows



AWS also offers a variety of processors from ARM to AMD to Intel.



AWS marketplace has thousands of AMIs that offer a variety of prebuilt services(NGINX, Palo Alto Firewall, MongoDB)



Elastic Compute Cloud (EC2) - Summary



OnDemand Pricing – Pay for what you use, only billed when instance is running



Spot Pricing – discounted rates when Amazon has spare capacity



Workloads on Spot Pricing need to tolerate interruptions



Reserved Pricing – Discounted rates when reserved for long periods of time(1-3 years)



Dedicated Host – Reserves an entire host(physical server) for you.



Dedicated instance – Only your instances run on a server, but that server can change if instances are stopped/started





Lambda - Summary



AWS Lambda is a compute service that lets you run code without having to provision or manage servers



AWS manages the server maintenance, scaling, capacity provisioning, and logging



Use cases include file processing, mobile and web backend



Autoscales to handle spike in traffic



Pay per invocation, only pay for what you use



Containers – Summary

- ✓ Containers are a tool that allows you to package an application and all of the necessary files, libraries, and dependencies the application needs to run
- ✓ Container orchestrators deploy, manage, and scale containerized applications
- ✓ ECS is simple managed container orchestrator provided by AWS
- ✓ Kubernetes is an open source container orchestrator
- ✓ EKS is a managed Kubernetes service – where AWS manages the control plane for you





Database



Self-Hosted Database Service



Self-Managed is an option if you need management and control



RDS and Redshift are the primary SQL database systems



RDS has five engines it supports: Oracle, MySQL, MariaDB, MS SQL, and PostgreSQL



DynamoDB, DocumentDB, and others are NoSQL services that are fully managed.



Make sure you look at the last slide for use cases for each service.



SQL Database Services



RDS is the RDBMS SQL database service in AWS



Aurora is a sub-service of RDS that supports PostgreSQL and MySQL cloud-natively



Aurora Serverless v2 is an Aurora variation, but without any VM management + Autoscaling



All of the RDS services feature encryption, replication, some type of scaling, and more



RedShift is unlike the others in that is it for reporting (OLAP)



Redshift has a serverless version and can handle Petabytes of data.



NoSQL Database Services



Most of the AWS NoSQL collection is based on Open Source Products



DynamoDB is the primary NoSQL service and has a ton of features



Remember that AWS has several NoSQL options that fit different use cases like Search, Security, and more



DynamoDB, DocumentDB, and others are NoSQL services that are fully managed.



Review the use cases slide to ensure you know the general use of each service.



Another way to think about the database

My Applications

What Kind of data does my application need?

Structured
Relational
Transactions



Amazon (RDS)



Amazon Aurora

Structured
Relational Reporting



Amazon Redshift

Unstructured Fast
Data Blobs



Amazon DynamoDB

Semi-structured
Fast Data



Amazon Keyspaces
(for Apache Cassandra)

Semi-structured
Fast Timestamped
data



Amazon Timestream

Caching



Amazon
ElastiCache



Amazon
MemoryDB for
Redis

Search



Amazon OpenSearch
Service

Relationships of the
Data



Amazon Neptune

Collections of
Documents



Amazon DocumentDB
(with MongoDB compatibility)

Very Secure
Transactions

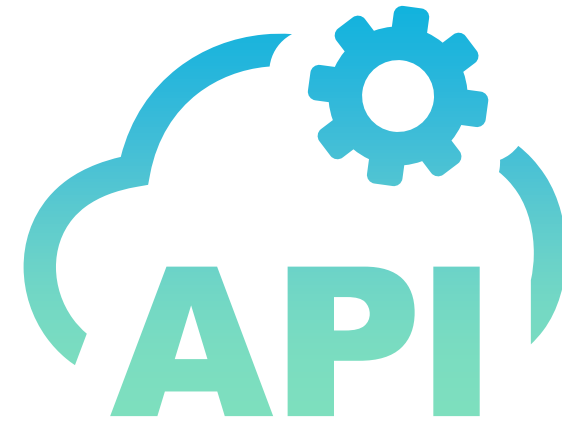


Amazon Quantum Ledger
Database (Amazon QLDB)





Application Integration



Application Integration



Simple Notification Service is to duplicating multiple messages to many different sources like email, text, other applications, etc.



Simple Queue system is built to receive messages and hold them for processing



Elastic Load Balancing distributes network connections over a pool of applications



Autoscaling handles add and removing capacity whether servers or read/write units

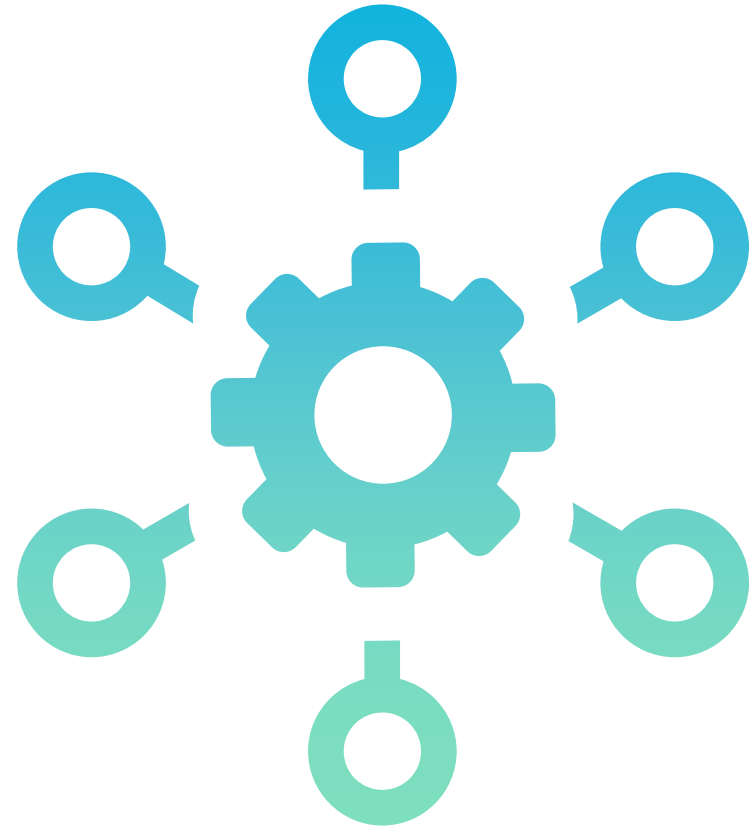


A variety of other services will be covered in the practice exams.





Management Services



Management – Summary

- ✓ Many Management Services used to manage AWS services
- ✓ CloudFormation and OpsWorks are used to create AWS service objects, while Systems Manager is configuration
- ✓ Organizations and Control Tower are all about multi-account management and setup
- ✓ AWS Config and AWS CloudTrail are configuration tracking and API tracking
- ✓ There are other Management services, but these are the main ones.





Migration Services



Migration Services – Summary



Migration starts with a good plan; remember the Cloud Adoption Framework



Migration Hub allows you to centralize your migration tools and plans on AWS



Data transfer happens with the Snowcone, Snowball (edge), or SnowMobile



AWS supports FTPS, SFTP, FTP, and AS2 for transfer as well



Application discovery is used for scanning inventory of migratable servers/apps



Application/Database/Data Center all have Migration services available on AWS



Mainframe Modernization is a service/framework for engineering Mainframe migration



Summary on Billing





General Billing



General Billing - Summary



Most services charge based on usage and capacity (always over time)



Compute, Storage, and Requests/Network are the common dimensions



Understand billing to optimize you spend



Scale up and down as needed

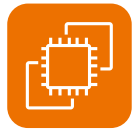


Use the appropriate billing model for your workload

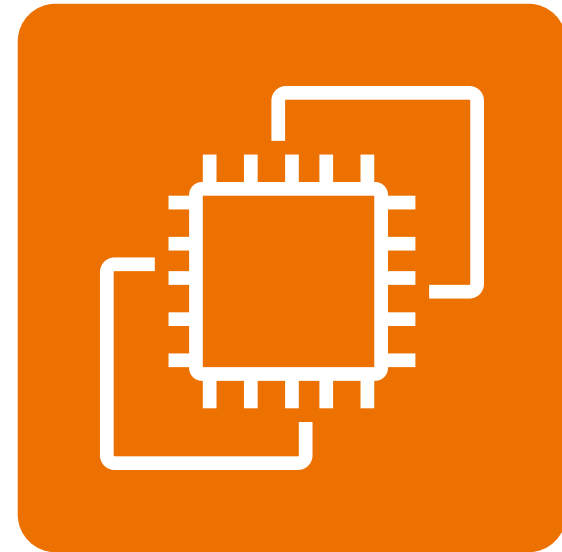


Use the Free tier when you can if learning





EC2 Billing



EC2 Billing - Summary



With EC2, you only pay when the machine is running



Compute, Storage, Requests/Network are the common dimensions even with EC2



Five models - On-demand, Reserved, Spot, Dedicated, and Savings Plans



The Fifth Model - Dedicated to both instance and host



Sizing is the biggest dimension



Enabling Features or Service Integrations can increase costs





RDS Billing



RDS Billing - Summary



Which RDS service are you running - Aurora, “main” RDS, or Aurora Serverless?



What Database engine are you using?



What Size of DB engine are you using - DB.t3.large, DB.t3.xlarge, or others?



How big and how fast are the disks?



Are you using On-demand RDS/ you get Reservations for your RDS instances?



Did you enable other features like Multi-AZ (failover) or long back-up retention?





VPC Billing



VPC Billing - Summary



VPC components are mostly free



Data, particularly outbound data = Not free



Same region, same AZ, with private IP = Free



Different region or AZ or public IP = Paid



Add-on components add extra cost, particularly when data is run through them



AWS does not test on specific numbers but does only general comparisons





Lambda Billing



Lambda Billing - Summary



Lambda pricing is based on size, duration, and frequency



The more often you run it, the more you pay (frequency)



The larger the memory and the longer it runs, the more you pay



Lambda functions have a maximum memory limit up to 10 GB and/or execution time up to 15 minutes



Additional features can be added but not required for Cloud Practitioner level

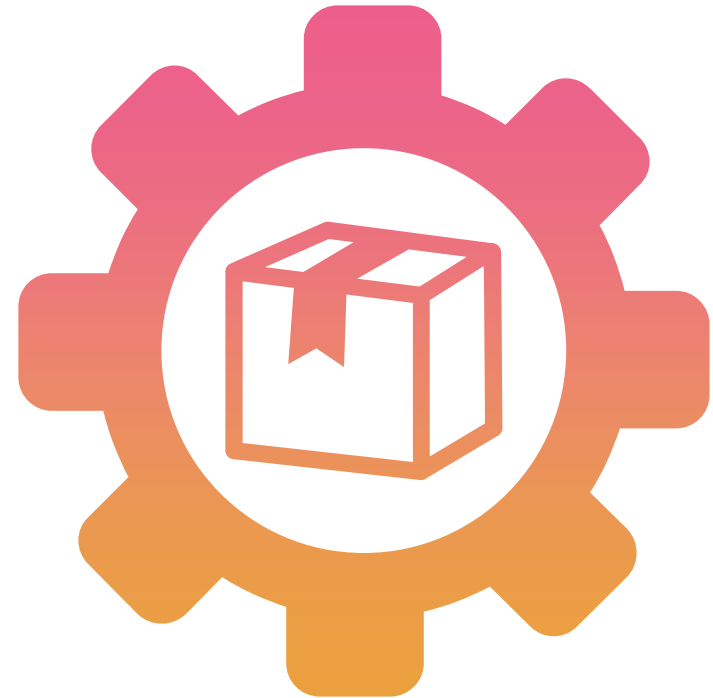


AWS does not test on specific numbers and does only general comparisons. Did we say this already?





Billing - Other Services



Other Services and their Billing - Summary

- ✓ Not required to know the specifics of billing for every service
- ✓ EBS charges based on type, size, and storage duration of virtual hard drive
- ✓ S3 charges based on number of objects, number of requests, storage class, and outbound pull
- ✓ DynamoDB charges based on table type, number of data, and read/write capacity units
- ✓ CloudFront charges based on data pulled/actions against “cached” objects
- ✓ Kinesis charges like DDB/Macie charges based on data scanned (number of objects)





Billing Account Structure



Account Structures on Billing - Summary



Solo AWS accounts have their own bills, details, and savings



Two/More accounts can designate a payer account with Consolidated Billing



Biller account ready if it is part of an AWS Organization



Control Tower is a practiced way to deploy a multi-account “Meta” account



All three Consolidated Billing options allow for billing by account





Tools for Billing



Tools for Billing - Summary



Billing, Cost Explorer, and CUR are tools for Billing Analysis



AWS Budgets is focused on soft and hard limits and notifications for billing



The “bill” or billing dashboard is great for skimming



Cost Explorer is more about visualization of billing data



CUR is the most detailed in terms of usage report



Modify AWS Budgets to “restrict” service launch and send notifications based on thresholds/alarms





KodeKloud