AWS Cloud practinioner notes

1. Cloud computing

Different types of cloud computing

IAM - Identity and Access Management

Definitions

root user IAM Users: IAM User Groups: IAM Policies IAM Roles

IAM Best practices

Shared responsibilty model

2. EC2 - Elastic Compute Cloud

3. Storage for EC2 Instance

EBS

EFS

4. ELB & ASG - Elastic Load Balancing & Auto Scaling Groups

5. Amazon S3

6. Databases & Analytics

RDS (Relational Database Service)

- RDS - Managed relational database service that supports multiple database engines: MySQL, PostgreSQL, MariaDB, Oracle, SQL Server, and Aurora
- suited for OLTP workloads: Online Transaction Processing

RDS Deployments options

1. Read replicas

- scale the read workload of your DB (in the same AZ)
- can create oup to 15 read replicas
- data is only written to the main DB

2. Multi-AZ

- failover DB in cas of AZ outage (high availability)
- data is only read & written to the main database
- can only have 1 other AZ as failover, failover is used only when main is down

3. Multi-Region (Read replicas)

- Disater recovery in cas of region issue
- local performance for global reads (application reads in db replica of nearest AZ)
- write is done in main DB (1 AZ)
- replication cost

Amazon Elasticache

ElastiCache is to get managed Redis or Memcached in-memory databases with high performance and low latency. --> Helps to reduce the load of databases (RDS DB: Postgres, or other) for read intensive workloads by storing cache in in-memory database

insert schema architecture

DynamoDB

keywords: serverless, low latency

- Fully managed highly available with replication across 3 AZ
- NoSQL database -> not a relational database -> stores primary key and product pairs (cfr key value)
- scales to massive worklaods because it is a distributes serverless database (no instances of the db are required)
- millions of requests per sections, trillions of rows, 100s of TB of storage
- single digit millisecond latency - low latency retrieval

DynamoDB is a flagship product of AWS

DynamoDB Global Tables

DynamoDB Global Tables makes DynamoDB table accessible with low latency in multiple-regions by using Active-Active replciation 2-way replication --> users can read and write in any table specific to the AZ

insert schema architecture

DynamoDB Accelerator - DAX

- same as Elasticache but for `DynamoDB` only: in-memory cache for DynamoDB only
- 10x performance improvement

DAX

- Amazon DynamoDB Accelerator (DAX) is a fully managed, highly available, in-memory cache for Amazon DynamoDB that delivers up to a 10 times performance improvement—from milliseconds to microseconds—even at millions of requests per second.

Redshift

- Redshift - Fully managed, petabyte-scale data warehouse service and analytics tool.
- data is stored in colnmar format (columns instead of rows)
- exam keywords: analytics, data warehouse, colunmar, OLAP

- OLAP (Online Analytical Processing) is used for complex queries and data analysis

Redshift serverless

- Redshift serverless - Serverless data warehouse that automatically scales the datawarehouse based on the workload.
- pay only for compute and storage used during analysis -> very cost efficient to run Redshift
- use cases: reporting, dashboards, real-time analytics

Amazon EMR (Elastic MapReduce)

- Amazon EMR - helps creating Hadoop clusters to analyze and process large amounts of data (Big Data)
- cluster can be made up of EC2 instances and EMR takes care of the provisioning and configuration of the cluster
- automatically scales the cluster based on the workload
- supports Apache Spark, HBasem Presto, Flink, and other big data frameworks
- exam keywords: Hadoop clusters, Big Data, data processing

Amazon Athena

- Amazon Athena - serverless query service that makes it easy to analyze data in Amazon S3 using standard SQL
- S3 objects supported are CSV, JSON, ORC, Avro, and Parquet (built on Presto)
- no need to set up or manage any infrastructure
- use cases: Business intelligence, analytics, reportingm ELB Logs, CloudTrail Logs, VPC Flow Logs
- Amazon QuickSight can be used to visualize the data
- pricing: $5 per TB of data scanned
- cost saving: use compressed or columnar data formats(Parquet, ORC) to reduce the amount of data scanned

exam keywords: analyze data in S3, serverless, SQL

Amazon QuickSight

- Amazon QuickSight - Serverless machine learning-powered Business Intelligence tool that allows you to create interactive dashboards and reports
- integrates with AWS services like RDS, Redshift, Athena, Aurora and S3
- pay per session or per user
- exam keywords: Business Intelligence, dashboards, reports, machine learning

Neptune

- Neptune - Fully managed graph database service that supports both RDF and property graph models
- use cases: social networking, fraud detection, recommendation engines, network security, knowledge graphs (Wikipedia)
- exam keywords: graph database, RDF, property graph
- build and rund applications working with highly connected datasets - optimized for these complex and hard querries

- highly available with replication across 3 AZs

TimeStream

- TimeStream - Fully managed, serverless, time-series database service for IoT and operational applications
- optimized for IoT and operational applications
- store and analyze trillions of events per day at 1/10th the cost of relational databases
- exam keywords: time-series data, IoT, operational applications

QLDB

- QLDB - Fully managed ledger database that provides a transparent, immutable, and cryptographically verifiable transaction log
- Quantun Ledger Database
- A ledger is a record of (financial) transactions
- immutable system: no entry can be removed or modified
- cryptographically verifiable: you can verify the integrity of the data -> because of the cryptographic hash of the data after each transaction
- difference with Amazon Managed Blockchain: QLDB is a ledger database, not a blockchain and it is not decentralized (all data is stored at AWS) -> in accordance with financial regulations
- manipulate data using PartiQL (SQL-compatible query language)
- 2-3x faster than common ledger blockchain frameworks
- exam keywords: ledger database, financial transactions, (immutable, cryptographically verifiable)

Managed Blockchain

- Managed Blockchain - Create and manage scalable blockchain networks using popular open-source frameworks: Hyperledger Fabric and Ethereum
- join public blockhain networks or create your own private blockchain networks
- exam keywords: blockchain, Hyperledger Fabric, Ethereum

Glue

- Glue - Fully managed extract, transform, and load (ETL) service that makes it easy to prepare and load your data for analytics
- fully serverless
- exam keywords: ETL, extract, transform, load
- use case example: EXTRACT data from S3 and RDS -> TRANSFORM data with Glue script -> LOAD data into Redshift

Glue Data Catalog

- Glue Data Catalog - Fully managed metadata repository that makes it easy to discover, search, and query metadata across your data lake and data warehouse
- catalog of datasets in AWS structure
- can be used with Athena, Redshift, EMR, and other services to build schemas for data
- probably not on exam

DMS (Database Migration Service)

- DMS - Migrate your databases to AWS with minimal downtime
- supports homogeneous migrations (Oracle to Oracle) and heterogeneous migrations (Microsoft SQL to Aurora)
- Quickly and securly migrate databases to AWS
- Source database remains available during the migration
- exam keywords: database migration

Overview

- Relational Databases: RDS and Aurora
  - Difference between multi-AZ, read replicas, multi-region
- In-memory Database: ElastiCache
- Key/Value Database: DynamoDB (serverless) & DAX (cache for DynamoDB) if cache is needed
- Data Warehouse or OLAP: Redshift(SQL)
- Hadoop Cluster: EMR
- Athena: query data on Amazon S3 (serverless & SQL)
- Quicksight: dashboards and visualization of data (serverless)
- DocumentDB: "Aurora of MongoDB" (JSON type of datasets - NoSQL database)
- Amazon QLDB: Financial transactions ledger (immutable journal, cryptographically verifiable): centralized!
- Amazon Managed Blockchain: managed Hyperledger Fabric and Ethereum blockchains
- Glue: Managed ETL (Extract, Transform, Load) and Data Catalog service
- DMS: Database Migration Service
- Neptune: Graph database
- TimeStream: Time-series database

Other compute services: ECS, lambda, Batch and Lightsail

ECS (Elastic Container Service)

- ECS - Highly scalable, high-performance container orchestration service that supports Docker containers
- ECS is a container management service that makes it easy to run, stop, and manage Docker containers on a cluster
- You must provision the infrastructure (EC2 instances) that run the containers

Fargate

- Fargate - Serverless compute engine for containers that works with both ECS and EKS
- With Fargate, you no longer have to provision, configure, or scale clusters of virtual machines to run containers --> fully serverless

ECR (Elastic Container Registry)

- ECR - Fully managed Docker container registry that makes it easy to store, manage, and deploy Docker container images
- Private Docker container registry on AWS

Lambda

- Lambda - Serverless compute service that lets you run code without provisioning or managing servers
- Lambda runs your code only when needed and scales automatically
- Functions are triggered by events -> event driven : S3 upload, DynamoDB update, API Gateway request
- Pioneer of serverless computing on AWS
- Supports multiple programming languages: Node.js, Python, Ruby, Java, Go, .NET
- Pricing:
  - pay per request (number of invocations)
  - compute time (GB-seconds) = memory in GB provisioned * total runtime in seconds
- Easy monitoring with CloudWatch Logs
- use cases:
  - create thumbnails from images uploaded to S3
  - run serverless CRON jobs
- exam keywords: serverless, event-driven, functions

API Gateway

- API Gateway - Fully managed service that makes it easy for developers to create, publish, maintain, monitor, and secure APIs at any scale
- Create serverless RESTful APIs and WebSocket APIs
- Integrates with Lambda, DynamoDB, and other AWS services
- Proxies requests from endpoint to other services. Eg: Allow users to upload files to S3 or access data in DynamoDB or trigger Lambda functions from HTTP requests
- exam keywords: serverless RESTful APIs, WebSocket APIs

Batch

- Batch - Fully managed batch processing at any scale
- Is not serverless, relies on EC2 instances
- Batch computing is the processing of a large amount of data in a programmatic way

Batch vs. Lambda

- Lambda is serverless, Batch is not
- Lambda is event-driven, Batch is not
- Lambda has limited runtime (15 minutes), Batch can run for hours or days
- Lambda has limited storage (512MB), Batch can use EBS volumes
- Lambda is for small, short-lived functions, Batch is for long-running batch jobs

Lightsail

- Lightsail - Virtual private server (VPS) service that offers everything needed to build an application or website
- For people with no cloud experience
- low and predictable pricing

- use cases:
  - simple websites: Wordpress, Joomla, Drupal
  - Dev/Test environments
  - simple webapps: has templates for MEAN, LAMP, Nginx, Node.js

Overview

- ECS: Run Docker containers on EC2 instances (not serverless)
- Fargate: Serverless compute engine for containers
- ECR: Docker container registry for storing, managing, and deploying Docker container images
- Lambda: Serverless compute service
- API Gateway: Serverless RESTful APIs
- Batch: Run batch jobs on AWS using EC2 instances (not serverless)
- Lightsail: Virtual private server (VPS) service

Deployments

CloudFormation

- CloudFormation - Infrastructure as Code (IaC) service that helps you model and set up your AWS resources so you can spend less time managing those resources and more time focusing on your applications
- CloudFormation templates are written in YAML or JSON
- repeat architecture in different environments, regions or AWS accounts
- exam keywords: Infrastructure as Code, templates, YAML, JSON,

CDK (Cloud Development Kit)

- CDK - Software development framework for defining cloud infrastructure in code and provisioning it through AWS CloudFormation
- Define cloud infrastructre through code (Python, TypeScript, Java, C#)
- Code is then synthesized into CloudFormation templates
- Deploy infrastructure and application runtime together
- Great of Lambda functions or Docker containers in ECS / EKS
- exam keywords: Infrastructure as Code, CloudFormation, Python, TypeScript, Java, C#

Elastic Beanstalk

- Elastic Beanstalk - Platform as a Service (PaaS) that allows you to deploy and manage web applications and services
- Supports multiple programming languages: Java, .NET, PHP, Node.js, Python, Ruby, Go, Docker
- Platform as a Service (PaaS)
- You upload your code and Elastic Beanstalk automatically handles the deployment using the architecture model you choose
- Health monitoring is also built-in (health agent pushes metrics to CloudWatch)
- 3 architecture models:
  - Single instance : good for dev environments
  - ELB + ALB : great for web applications

  - ALB only : good for workers, microservices
- exam keywords: PaaS, multiple programming languages

CodeDeploy

- CodeDeploy - Automates code deployments to any instance, including Amazon EC2 instances and instances running on-premises
- exam keywords: code deployments, hybrid(On-premises and AWS)

Systems Manager (SSM)

- Systems Manager - Gives you visibility and control of your infrastructure on AWS
- Patch, configure and run commands at scale (at multiple instances at the same time)
- exam keywords: patching, configuration, automation

SSM Session Manager

- SSM Session Manager - Provides a secure and auditable instance management
- No need for SSH keys, bastion hosts, or open inbound ports
- exam keywords: secure, auditable, instance management

SSM Parameter Store

- SSM Parameter Store - Securely store configuration data and secrets
- exam keywords: secure, configuration, secrets

Developer services

CodeCommit

- CodeCommit - Fully managed source control service that makes it easy for teams to host secure and highly scalable private Git repositories
- exam keywords: source control, Git
- No longer supported in the future

CodeBuild

- CodeBuild - Fully managed build service that compiles source code, runs tests, and produces software packages that are ready to deploy
- exam keywords: build service, compile, tests

CodePipeline

- CodePipeline - Continuous integration and continuous delivery (CI/CD) service for fast and reliable application and infrastructure updates
- from code commit to build to deployment
- exam keywords: CI/CD, continuous integration, continuous delivery

12 Global appplications

Route 53

- Route 53 - Scalable Domain Name System (DNS) web service
- routing policies:
  - simple : one record with multiple IP addresses (no health checks)
  - failover : primary and secondary record (health checks)
  - latency-based : direct users to the region with the lowest latency (health checks)
  - weighted : split traffic based on pre-defined weights (health checks)
- exam keywords: DNS, latency-based routing, failover routing

CloudFront

- CloudFront - Content Delivery Network (CDN) service that securely delivers data, videos, applications, and APIs to customers globally with low latency and high transfer speeds
- Replicate part of your application or S3 bucket content to edge locations - decrease latency
- Cache content of frequent requests at edge locations - improved user experience by decreasing latency
- exam keywords: CDN, edge locations, low latency

Cloudfront vs S3 Cross Region Replication

- CloudFront:
  - caches content at edge locations to decrease latency
  - great for static content that needs to be available everywhere
- S3 Cross Region Replication:
  - replicates all data to another region for disaster recovery
  - great for dynamic content that needs to be available in another region

##3 S3 Transfer Acceleration

- S3 Transfer Acceleration - Speeds up transferring files to and from Amazon S3 using the AWS CloudFront globally distributed edge locations
- exam keywords: S3, CloudFront, edge locations

##3 AWS Global Accelerator

- AWS Global Accelerator - Improve global application availability and performance AWS global network
- traffic is routed to the nearest AWS edge location and then to the application (can be running in a different region)
- exam keywords: availability, performance, local, global

CloudFront vs Global Accelerator

Both use edge locations to decrease latency and protection against DDoS attacks

- CloudFront:
  - caches content at edge locations to decrease latency
  - great for static content that needs to be available everywhere

- Global Accelerator:
  - no caching: routes traffic to the nearest AWS edge location and then to the application
  - improves global application availability and performance

AWS Outposts

- AWS Outposts - Fully managed service that extends AWS infrastructure, AWS services, APIs, and tools to virtually any datacenter, co-location space, or on-premises facility for a truly consistent hybrid experience
- AWS provides servers, storage, and networking equipment to run AWS services on-premises
- benfits: low latency, local data processing, data residency, and seamless integration with AWS services
- exam keywords: hybrid, on-premises, consistent

AWS Wavelength

- AWS Wavelength - Deliver ultra-low latency applications for 5G devices using AWS compute and storage at the edge of the 5G network
- AWS Wavelength embeds AWS compute and storage services at the edge of telecommunications providers' 5G networks
- Goal: reduce latency for 5G applications
- exam keywords: ultra-low latency, 5G, edge

AWS Local Zones

- AWS Local Zones - AWS infrastructure deployment that places compute, storage, database, and other select services closer to large population, industry, and IT centers
- Extend AWS region to a Local Zone in a specific geographic location so you can run applications that require single-digit millisecond latency directly at the Local Zone
- exam keywords: latency-sensitive, large population, industry centers

Global application architecture

- Single Region + single AZ :
  - low availability
  - low latency
  - low difficulty
- Single Region + multiple AZs :
  - high availability
  - low latency
  - medium difficulty
- Multi-Region - Active/Passive :
  - high availability
  - medium latency
  - higher difficulty

- Multi-Region - Active/Active :
  - high availability
  - low latency
  - highest difficulty

13 Cloud Integrations

SQS (Simple Queue Service)

- SQS - Fully managed message queuing service that enables you to decouple and scale microservices, distributed systems, and serverless applications
- exam keywords: message queuing, decouple, microservices

SNS (Simple Notification Service)

- SNS - Fully managed messaging service for both application-to-application and application-to-person communication
- exam keywords: messaging service, application-to-application, application-to-person, topics

Kinesis

- Kinesis - Fully managed service for real-time processing of streaming data at massive scale
- exam keywords: real-time processing, streaming data

Amazon MQ

- Amazon MQ - Managed message broker service for Apache ActiveMQ and RabbitMQ that makes it easy to set up and operate message brokers in the cloud
- exam keywords: message broker, Apache ActiveMQ, RabbitMQ

14 Cloud Monitoring

CloudWatch Metrics & Alarms

- CloudWatch - Monitor AWS resources and applications in real-time
- CloudWatch Metrics: collect and track metrics, monitor log files, set alarms
- CloudWatch Alarms: send notifications or take actions based on defined rules
- exam keywords: monitoring, metrics, alarms

CloudWatch Logs

- CloudWatch Logs - Monitor, store, and access log files from Amazon EC2 instances, AWS CloudTrail, Route 53, and other sources
- exam keywords: log files, monitoring

EventBridge

- EventBridge - Serverless event bus that makes it easy to connect applications together using data from your own applications, integrated SaaS applications, and AWS services
- default event bus: receive events from AWS services

- partner event bus: receive events from SaaS applications (AWS parntners: Zendesk, Datadog, PagerDuty)
- custom event bus: receive events from your own applications
- ex: Cron jobs, S3 uploads, CodePipeline, CloudWatch Alarms trigger events that are sent to EventBridge and then to Lambda functions or other services
- exam keywords: serverless, event bus

CloudTrail

- CloudTrail - Record API calls for your account and delivers log files to you
- CloudTrail is enabled by default
- log files can be stored in S3 or CloudWatch Logs
- exam keywords: API calls, log files, tracking activity

X-Ray

- X-Ray - Analyze and debug distributed applications in production or under development
- allows you to trace requests from beginning to end with a visual map and latency data
- troubleshooting performance issues (latency, errors)
- exam keywords: analyze, debug, distributed applications

Amazon CodeGuru

- Amazon CodeGuru - Automated code reviews and application performance recommendations
- like: SonarQube, Checkmarx, Lint
- ML-powered powered service that helps you write better code and troubleshoot issues
- 2 components:
  - CodeGuru Reviewer: automated code reviews
  - CodeGuru Profiler: application performance recommendations: eg. reduce CPU usage, remove unused code
- exam keywords: code reviews, performance recommendations

AWS Health Dashboard

- AWS Health Dashboard - Provides alerts and remediation guidance for AWS services
- provides alerts and remediation guidance when AWS is experiencing events that may impact you
- exam keywords: alerts, remediation guidance

15 VPC - Virtual Private Cloud

VPC

- VPC - Virtual network that you create in an AWS region
- exam keywords: virtual network, region

Subnets

- Subnets - Range of IP addresses in your VPC
- subnets can be public or private
- subnets are defined per AZ

- subnets can be associated with route tables
- internet gateway is required for public subnets
- NAT gateway (AWS managed) or NAT instance (self managed) is required for private subnets to access the internet while remaining private(outbound only)
- exam keywords: IP addresses, public, private, AZ

NACLs

- NACLs - Act as a firewall for associated subnets, controlling inbound and outbound traffic
- NACLs are stateless: return traffic is not automatically allowed
- can have allow and deny rules
- are attached at the Subnet level
- exam keywords: firewall, inbound, outbound, stateless, subnet

Security Groups

- Security Groups - Act as a firewall for associated EC2 instances, controlling inbound and outbound traffic
- Security Groups are stateful: return traffic is automatically allowed, regardless of any rules
- can have allow rules only
- are attached at the EC2 instance level
- exam keywords: firewall, inbound, outbound, stateful, EC2 instance

VPC Flow Logs

- VPC Flow Logs - Capture information about the IP traffic going to and from network interfaces in your VPC
- VPC flow log, subnet flow log or Elastic Network Interface (ENI) flow log
- Help, monitor and troubleshoot connectivity issues in your VPC
- VPC Flow Logs can be published to CloudWatch Logs, S3, or Kinesis Data Firehose
- captures network information from AWS managed interfaces (eg. RDS, ElastiCache), Elastic Load Balancers, ENI's, etc.
- exam keywords: IP traffic, network interfaces, monitor, troubleshoot

VPC Peering

- VPC Peering - Connect two VPCs to route traffic between them using private IP addresses, so they behave as if they are on the same network
- Must not have overlapping CIDR blocks (IP ranges)

VPC Endpoints

- VPC Endpoints - Enables you to privately connect your VPC to supported AWS services and VPC endpoint services powered by PrivateLink without requiring an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection
- VPC Enpoint Gateway: S3 and DynamoDB only
- VPC Endpoint Interface: rest of the services
- exam keywords: private connection, VPC, AWS services

PrivateLink

- PrivateLink - Enables you to privately connect your VPC to services hosted by other AWS accounts (SaaS providers) and services hosted by other VPCs in your own account
- exam keywords: private connection, VPC, AWS services, SaaS providers

Direct Connect

- Direct Connect - Establish a dedicated network connection from your premises to AWS
- exam keywords: dedicated, network connection, on-premises

Site-to-Site VPN

- Site-to-Site VPN - Connect your on-premises network to your VPC over an IPsec VPN tunnel
- on premise you need a Custumer Gateway (CGW) and on AWS a Virtual Private Gateway (VGW) to establish the VPN connection
- exam keywords: on-premises, network, IPsec, VPN, fast implementation, public internet

Direct Connect(DAX) vs. Site-to-Site VPN

- Direct Connect:
  - dedicated network connection from your premises to AWS
  - private connection
  - higher bandwidth
  - more expensive
  - time-consuming to set up
- Site-to-Site VPN:
  - connect your on-premises network to your VPC over an IPsec VPN tunnel
  - uses the public internet
  - lower bandwidth
  - less expensive
  - faster to set up

Client VPN

- Client VPN - Managed client-based VPN service that enables you to securely access your AWS resources and resources in your on-premises network
- Connect to your VPC from your computer using OpenVPN
- exam keywords: client-based, VPN, secure

Transit Gateway

- Transit Gateway - Connect thousands of VPCs and on-premises networks using a single gateway
- hub-and-spoke model (star): connect multiple VPCs and on-premises networks to a central hub (Transit Gateway)
- exam keywords: thousands of VPCs, on-premises networks, single gateway

VPC Summary

- VPC: Virtual network in an AWS region

- Subnets: Range of IP addresses in your VPC
- NACLs: Firewall for subnets, stateless
- Security Groups: Firewall for EC2 instances, stateful
- VPC Flow Logs: Capture IP traffic going to and from network interfaces
- VPC Peering: Connect two VPCs to route traffic between them
- VPC Endpoints: Privately connect your VPC to supported AWS services
- PrivateLink: Privately connect your VPC to services hosted by other AWS accounts
- Direct Connect: Dedicated network connection from your premises to AWS
- Site-to-Site VPN: Connect your on-premises network to your VPC over an IPsec VPN tunnel
- Client VPN: Managed client-based VPN service
- Transit Gateway: Connect thousands of VPCs and on-premises networks using a single gateway

16 Security & Compliance

Shared responsibility model

- AWS is responsible for security of the cloud -> hardware, software, networking, and facilities that run AWS services
- Customer is responsible for security in the cloud -> data, identity, access management, platform, applications, and network configuration

AWS Shield

- AWS Shield is a managed DDoS protection service that safeguards applications running on AWS
- DDoS protection
- Standard: protection against most common DDoS attacks
- Advanced: protection against more sophisticated attacks
- exam keywords: DDoS protection

AWS WAF - Web Application Firewall

- Protects web applications from common web exploits
- Filter specific requests based on rules
- Rules can be based on IP addresses, HTTP headers, HTTP body, or URI strings
- exam keywords: WAF, web application firewall, protect web applications

AWS Network Firewall

- Managed firewall service that makes it easy to deploy essential network protections for all of your Amazon Virtual Private Clouds (VPCs)
- From Layer 3 to Layer 7 protection
- exam keywords: protect entire VPC, network firewall

AWS Firewall Manager

- Manage security rules in all accounts of an AWS Organization
- exam: manage VPC security groups on multiple accounts in an organisation --> AWS Firewall Manager
- Security policy: common set of security rules:

- VPC Security Groups for EC2, ALB, RDS, ElastiCache, etc.
- WAF rules for API Gateway, CloudFront, App Load Balancer
- AWS Shield Advanced for DDoS protection
- AWS Network Firewall for VPCs

Penetration Testing

- AWS customers are allowed to perform penetration testing on their AWS infrastructure within certain limits
- DDOS testing other attacks that can harm the AWS infrastructure are not allowed

Encryption in rest vs in transit

- Encryption in rest: data is encrypted when it is stored (data is not moving)
- Encryption in transit: data is encrypted when it is moving from one place to another (eg data moving from EC2 to S3)

Encryption with KMS

- AWS Key Management Service (KMS) is a managed service that makes it easy for you to create and control the encryption keys used to encrypt your data
- AWS manages the encryption keys for you, you define the policies
- type of KMS keys:
  - Customer Managed Keys: you create and manage the keys
  - AWS Managed Keys: AWS creates and manages the keys (aws/s3, aws/ebs)
  - AWS Owned Keys: Collection of CMKs (Customer Master Keys) that an AWS service owns and manages to use in multiple accounts
  - CloudHSM Keys: keys are stored in a hardware security module (CloudHSM)
- exam keywords: KMS, encryption, key management service

CloudHSM

- CloudHSM is a cloud-based hardware security module (HSM) that enables you to easily generate and use your own encryption keys on the AWS Cloud
- you manage the encryption keys entirely
- exam keywords: CloudHSM, hardware security module, encryption keys

KMS vs CloudHSM

- KMS: AWS manages the software for encryption, pay per use
- CloudHSM: AWS provisions encryption hardware, dedicated hardware, pay per hour

AWS Certificate Manager (ACM)

- 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

AWS Secrets Manager

- AWS Secrets Manager helps you protect access to your applications, services, and IT resources without the upfront investment and on-going maintenance costs of operating your own infrastructure
- Integration with Amazon RDS
- Possibility to rotate secrets automatically
- exam keywords: Secrets Manager, rotate secrets, RDS secrets

AWS Artifact

- AWS Artifact is your go-to, central resource for compliance-related information that matters to you
- eg. PCI DSS, HIPAA, ISO, SOC, etc.
- exam keywords: compliance, AWS Artifact

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
- uses Machine Learning to detect anomalies
- input data: VPC Flow Logs, CloudTrail Logs, DNS Logs
- exam tip: can protect against CryptoCurrency attacks
- exam keywords: GuardDuty, threat detection, malicious activity

Amazon Inspector

- Amazon Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS
- For EC2 instances:
  - leveraging the AWS System Manager (SSM) agent
  - Analyze against unintended network accessibility, vulnerabilities, and deviations from best practices
  - analyze the running OS against known vulnerabilities
- For container image push to Amazon ECR:
  - assesment of the container image as they are pushed
- for Lambda functions:
  - assesment of the Lambda function code and package dependencies as it is deployed
- Reporting & integration with AWS Security Hub
- send findings to Amazon Event bridge
- exam keywords: Amazon Inspector, security assessment, compliance

AWS Config

- AWS Config is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources
- Helps with auditing and recording compliance of your AWS resources based on the configurations you have set
- Helpful for big enterprises to make sure all resources are compliant with the company's security policies
- exam keywords: AWS Config, compliance, audit

Amazon Macie

- Amazon Macie is a security service that uses machine learning to automatically discover, classify, and protect sensitive data in AWS
- Macie helps and alerts you to sensitive data such as personally identifiable information (PII)
- can be integrated with Amazon EventBridge
- exam keywords: Macie, sensitive data, PII

AWS Security Hub

- Central security tool to manage security across multiple AWS accounts and automate security checks
- Integrated dashboards showing current security and compliance status to quickly take actions
- Automatically aggregate alerts in predefined or personal findings format from various AWS serivces & AWS partner tools:
  - Config
  - GuardDuty
  - Inspector
  - Macie
  - IAM Access Analyzer
  - AWS Systems Manager
  - AWS Firewall Manager
  - AWS Health
- must enable AWS Config Service to use Security Hub
- exam keywords: Security Hub, security checks, compliance

Amazon Detective

- GuardDuty, Macie and Security Hub are great tools to detect security issues, but they do not provide a full investigation
- Amazon Detective is a service that helps you to investigate and identify the root cause of potential security issues or suspicious activities
- automatically collects and process events from VPC Flow Logs, CloudTrail, GuardDuty to create a visual graph of the resources and the interactions between them. So you can easily identify the root cause of the issue.
- exam keywords: Detective, investigate, root cause

AWS Abuse

- AWS Abuse is a service that helps you to report any abuse of the AWS services
- eg. phishing, malware, spam, DoS or DDoS etc. that is hosted on AWS
- exam keywords: AWS Abuse, report abuse

Root user privileges

- Root user has full access to all AWS services and resources in the account
- Some actions can only be performed by the root user:
  - `change account settings( account name, email, root user password, root user access keys)`
  - `close the account`
  - `change or cancel AWS support plan`

    - restore IAM user permissions
    - view certain tax invoices
    - `register as a seller in the Reserved Instance Marketplace`
    - Configure and Amazon S3 bucket to enable MFA
    - edit or delete an Amazon S3 bucket policy that includes an invalid VPC ID or VPC endopoint ID
    - sign up for GovCloud

IAM Access Aanlyzer

- IAM Access Analyzer helps identify which resources are shared externally:
    - S3 Buckets
    - KMS Keys
    - IAM Roles
    - Lambda Functions
    - SQS Queues
    - Secrets Manager Secrets
- Define Zone of Trust = AWS account or AWS Organization
- Access outiside zone of trust is flagged as a finding
- exam keywords: IAM Access Analyzer, shared resources, Zone of Trust, analyze access