AWS Cloud concepts

- **AWS Well-Architected Framework**
  - **Operational Excellence** - running and managing systems to deliver business value, ensuring operations are efficient, predictable and resilient. **Perform operations as code, make frequent, small, reversible changes, refine operations procedures frequently, anticipate failure, learn from all operational failures.**
  - **Security** - protecting information and systems. **Implement a strong identity foundation, enable traceability, apply security best practices, protect data in transit and at rest, keep people away from data, prepare for security events.**
  - **Reliability** - systems can recover from failures and continue to function in the face of disruption. **Automatically recover from failure, test recovery procedures, scale horizontally to increase aggregate workload availability, stop guessing capacity, manage change in automation**
  - **Performance Efficiency** - using IT resources efficiently and effectively, ensuring systems deliver necessary performance with minimal waste
  - **Cost Optimisation** - managing costs and resources efficiently, maximising value of IT investments

- **Decoupling** components ensures the different components of applications can be managed and maintained separately. If all components are tightly coupled, the entire application would go down when one component goes down.

Security and compliance within the AWS Cloud

- **AWS Artifact** to download AWS security & Compliance documents. AWS Artifacts consists of reports such as AWS ISO certifications, Payment Card Industry, Payment Card Industry (PCI) and System and Organisation Control (SOC).

- **AWS Config** can be used to audit and evaluate configurations of AWS resources. Helps ensure resources remain compliant. Can't alert you about sign-in events. Use Cloud watch for this.

- **Amazon CloudWatch Anomaly Detection** is a ML feature limited to Amazon CloudWatch metrics. CloudWatch provides a centralised view of AWS resources and their performance. Collect and analyse metrics and logs, set alarms, and troubleshoot issues.

- **AWS CloudTrail** provides a record of the actions taken by a user, role or an AWS service in your account. Can check logs on the S3 bucket.

- **AWS License Manager** serves the purpose of differentiating, maintaining third-party software provisioning vendor licenses. It also decreases the risk of license expirations and the penalties.

- **AWS Systems Manager Parameter Store** can be used to store configuration data and secrets securely in a plain or encrypted format (Amazon KMS). **Amazon KMS** cannot be used to store data. It is integrated with AWS Systems Manager Parameter Store for encrypting data stored.

- **Amazon Secrets Manager** can be used to store secrets in an encrypted format with AWS KMS. NOT FREE. Allows users to replace authentication information in code with an API call to Secrets Manager. Secret is removed from code. Automatically rotates the secret in accordance with specified schedules.

AWS Access Management Capabilities

- **AWS Single Sign-On** is best suited for authenticating employees for accessing AWS services.

- **AWS Identity and Access Management (IAM)** is used to control access to AWS services or resources.

- **IAM policies** are attached to **IAM roles** and IAM roles get attached to the EC2 **instances**.

- **IAM roles** are temporary credentials that expire.

- **AWS Lifecycle Manager** creates lifecycle policies for specified resources to automate operations.

- **IAM Group** is a collection of IAM users.

- **IAM user** is an entity representing the person or application that uses it to interact with AWS.

- **Meta data information** is available to EC2 instances by default without the need to provide an IAM role. Get the instance ID by querying Meta Data.

- An **Organisational unit** can have only one parent.

- **Organisational level policies** are known as **Service Control Policies**. A policy applied at the Root is applied throughout the Organisation.

- Accounts that are managed by Root are called **Member Accounts**.

- There is only **one root account** in an AWS Organisation and should be used only for admin and management account

- **IAM is primarily focused on managing access to AWS resources within an AWS account**

- **Cognito is designed to provide user management and authentication for web and mobile applications,** and can be integrated with other AWS services to build serverless applications.

- **Amazon Cognito User Pools** manages user authentication to mobile applications.

- **Amazon Cognito Identity Pools** are used to provide privileged credentials for accessing AWS services.

- **Resource Access Manager (AWS RAM)** allows users to share resources with other AWS accounts or via AWS Organisations.

- **AWS Systems Manager** allows users to control their AWS resources by unifying services into a user interface. One in which they can view, atomate and monitor operational tasks.

- **AWS Systems Manager Session Manager** is an interactive shell and CLI that helps to provide secure, access-controlled, and audited Windows and Linux EC2 instance management. Session Manager removes the need to open inbound ports, manage SSH keys, or use bastion hosts.

- To connect a mobile app that needs to access AWS resources, use security token service (STS) with Identity Federation that will allow the user to access the resource within a session.

Security Support

- **AWS Trusted Advisor** provides recommendations to follow AWS best practices which will enhance performance and security, provide fault tolerance, reduce cost and monitor service limits.

- **AWS Detective** is a persistent ML service that automatically collates log data from all AWS resources. This log data is then applied into ML algorithms to derive data patterns between AWS services and resources, graph theory and statistical analysis. This information allows the user to **proactively visualise their AWS environment from a security standpoint**, thereby allowing them to quickly and efficiently conduct security investigations when they occur. Root cause finder.

- **AWS Macie** matches and discovers **sensitive** data such as personally identifiable information- detect credit card information that has been erroneously uploaded by a user into one of the **S3 buckets** during an online questionnaire.

- **AWS Shield** is a **DDoS** protection service that applies to applications running in the AWS environment.

- **AWS GuardDuty** is a threat detection service that monitors logs from AWS CloudTrail Event logs, Amazon VPC Flow Logs, and DNS Logs to detect any malicious activity.

- **AWS Security Hub** aggregates alerts from various services like Amazon GuardDuty, Amazon Inspector, Amazon Macie, and AWS Partner solutions in a single place.

- **Amazon Inspector** is a security assessment service that helps you to automate security assessments, identify security issues and vulnerabilities, and prioritise remediation efforts to improve the security posture of your applications and infrastructure in AWS. Performs **network accessibility checks** on Amazon EC2 instance.

- **AWS CloudHSM** is a managed hardware model for generating and managing encryption keys on the AWS cloud.

- **Virtual Private Cloud** is a VNet that lets us launch AWS resources in the defined VNet.

- **Network Access Control List (NACL)** can be configured to enhance the security at the subnet level.

- **Security Group** acts as a firewall by controlling the traffic. Acts at the instance level.

- **AWS WAF** is a web application firewall that lets you monitor the HTTP and HTTPS requests that are forwarded to CloudFront or Application Load Balancer. Used to create a custom rule that blocks SQL injection attacks.

Technology

AWS global infrastructure

- **AWS Global Accelerator** does not include the content caching capability that CloudFront does. Global Accelerator is suitable for applications that are **non-HTTP/s** such as VoIP, MTTQ and gaming.

- **CloudFront enhances the performance of HTTP-based content such as dynamic web applications, images and videos.** Can use EC2, ELB etc. It filters requests to ensure that only valid HTTP/S requests will be forwarded to backend hosts. Also supports geo-blocking.

- **Global Accelerator** uses the AWS global network of PoPs (Points of Presence) to route traffic to the optimal regional endpoint based on health, client location, and policies you configure, which increases availability. **Global Accelerator** can find the optimal path from the end user to your web-servers. Deployed within Edge Locations so you send user traffic to an Edge Location instead of directly to your web-application.

- **Route 53** is a cloud-based DNS. It provides latency-based routing which selects a region that may be relatively faster for the user to send traffic to, based on certain factors like internet traffic and proximity to the user's location. Does not provide a fast network path. DOES NOT PERMIT PENERTRATION TESTS.

- **CloudFront Distribution** improves performance for cacheable content (images, videos) and dynamic content (API, dynamic site delivery) using edge locations.

AWS compute services

- **Spot request** is the price which a customer is willing to pay for a specific instance type in an AZ. When spot price > spot request, instance gets terminated.

- **Amazon Fargate (Azure Container Instances)** allows serverless compute platform without managing underlying infrastructure.

- **AWS Lambda** allows run code without provisioning or managing servers. Pay only for compute time consumed.

- **Elastic Beanstalk** provides a fast way to deploy a web application on AWS. Automatically handles resource provisioning, autoscaling, and monitoring when configured. Use Java, .Net, PHP, Node.js, Python, Ruby, Go, and Docker on Apache and others

- **Amazon WorkSpaces** provides a secure managed service for virtual desktops for remote users. It supports both Windows and Linux based machines for a large number of users.

- **Amazon AppStream 2.0** provides access to applications or a non-persistent desktop from any location.

- **Amazon WorkLink** can be used by internal employees to securely access internal websites and applications using mobile phones.

- **Application Load Balancer is for HTTPS** and supports a feature named Path-based routing that will route requests based on URL patterns provided in the request.

- **Network Load balances** are for extreme performance as operates on layer 4 and below. Does not take into consideration anything at the application layer such as content type, cookie data, custom headers, user location, or the application behaviour.

- **Classic Load Balancer** is simple and distributes network traffic across multiple EC2 instances in one or more AZ.

- **Job Definitions** can be used to specify how a job runs in a compute environment. It can be used to define memory, CPU requirements, IAM roles required for running the Jobs, container properties, environment variables, and mount points for persistent storage. **A job** is a script or executable file which is submitted to AWS Batch. **Job Queue** can be used to specify priority of the jobs which are submitted to AWS Batch.

- Must use an EC2 Dedicated Host if reusing existing server-bound software licensing.

AWS storage services

- **S3** allow you to store virtually unlimited amounts of data and each object is accessible via a URL but cannot store an object of an unlimited size. S3 supports both server-side and client-site encryptions. Self-created S3 resources are only accessible to the user by default. By default both S3 buckets and objects are private.

- **Amazon S3 Transfer Acceleration** allows you to generate a special URL that can be used by end users to upload files to a nearby Edge Location.

- **S3 Standard** - frequency accessed data

- **S3 Intelligent Tiering** - optimises costs by storing in frequent and infrequent access

- **S3 Standard IA** - infrequent access

- **S3 One Zone IA** - stores data in single AZ as opposed to the 3 AZ of the other ones BUT not fault tolerant

- **S3 Glacier** - long term archive data

- **EBS Volume** directly attaches to an EC2 instance to provide persistent storage. Optimised for low-latency, high throughput access. EBS Volume replication replicates the volume in the same AZ.

- **Amazon S3** stores and retrieves large amounts of data, such as backups, archives, and static assets.

- **Amazon S3 Glacier console** cannot be used to upload data on Glacier. The console can only be used to create a Glacier vault which can be used to store data. Can use REST API calls, Amazon SDK and S3 Lifecycle Policies to upload data.

- **Amazon RDS** databases are useful for heavy transaction processing systems. Restrict database access by using a security group. Can use RDS to created and read replicas across Regions.

- **EFS** is a regional service!

AWS networking services

- **Need an Internet gateway** to enable a VPC to have inbound internet access

- The components involved in a **Site-to-Site VPN connection to an AWS VPC** are: **A Customer Gateway (CGW)** on the local network, **A Virtual Private Gateway** (VGW) on the AWS network, **A VPN tunnel to connect CGW and VGW.**

- **Verify security certificate from AWS Certificate Manager** by creating a CNAME record or email confirmation.

- **AWS Firewall Manager** makes it possible to manage VPC security groups.

- VPC infrastructure hosting Application and Database. Want only application accessible so use a **subnet configured for the ELB with a NAT Gateway.** Have the ELB within the Public Subnet which allows you to expose your application to the internet whilst ensuring that traffic is distributed evenly across servers and have the Application and Database in the Private Subnet. The user can access application through ELB.

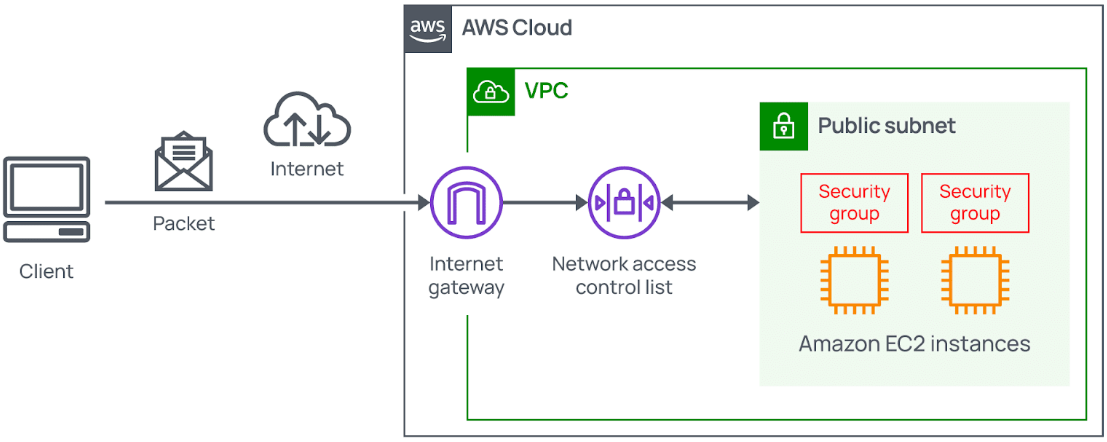
- **VPC** lets you provision a logically isolated section of the AWS Cloud where you can launch AWS resources in a VNet that you define. You have complete control over your VNet environment, including selection of your own IP address range, creation of subnets, and configuration of route tables and network gateways. IPv4 and IPv6 can be used.

- **Primary (Elastic Network Interface) ENI** of an instance cannot be detached form the instance. By default, the primary ENI is created with the creation of the EC2 instance and deleted when then instance is terminated.

- **Route53** is a Domain Name System. Route traffic to various AWS services or other infrastructure outside of AWS. Traffic Management - implement advanced routing policies such as: **Weighted routing** - distribute traffic across multiple endpoints in proportion to their assigned weights. Test new versions of your application or distribute traffic to different regions of AZs. **Latency-based routing** - directs traffic to the endpoint that provides the lowest latency (shortest round-trip) from user's location. **Geolocation-based routing** - direct users to the endpoint that is closest to their location or route traffic to different region based on user location

- **Key Pair** is a set of public and private keys which are security credentials used to connect to EC2 instances. **Using EC2 instance** - create using console, AWS CLI or PowerShell. Public Key is stored in EC2 instance. **Using third-party tools** - generate key using third party tool and store securely, these need to be imported into EC2.

- **NACLs** are stateless whereas **Subnets** are stateful (remember)



AWS database services

- **Amazon Redshift** service is a **data warehouse** for operational analytics on business events.

- **Amazon Athena** is a query service in Amazon S3 by using standard **SQL**. Uses SQL only. It is compatible with data formats such as CSV, JSON, ORC, AVRO and Parquet. It queries data directly from S3.

- **Amazon DynamoDB** for huge volume, data retrieval. Enable real-time capture of data changes using event notifications. **NoSQL**.

AWS Developer Tools

- **AWS CloudFormation** provides an easy way to model a collection of AWS resources, provision them quickly and consistently and manage them throughout their lifecycle by treating **infrastructure as code.**

- **AWS CodeCommit** is a managed source control service. It can be used as a data store to store source code, binaries, scripts, HTML pages and images which are accessible over the internet. CodeCommit encrypts files in transit and at rest. Works will with Git tools.

- **AWS Code Deploy** is a deployment service that automates application deployments to Amazon EC2 instances, on premises instances, serverless Lambda functions, or Amazon ECS services.

- **AWS CodePipeline** is used when **orchestrating and automating the various phases involved in the release of application updates** in-line with a release model that the developer defines. It does not provision IT infrastructure.

- **AWS CodeStar** provides a unified user interface, enabling you to manage your software development activities in one place. Set up entire continuous delivery toolchain in minutes, allowing you to start releasing code faster. It is a software development management tool.

AWS Support

- **Basic** - free, AWS whitepapers, documentation and support forums
- **Developer** - technical support for development and testing environments **Service quota and basic security checks. Does not include chat and phone calls. Provides email support during business hours only.**
- **Business** - technical support for production environments and AWS Trusted Advisor **Full set of checks. Provides phone, email and chat access 24/7. Response time of less than one hour if a production system has a service interruption.**
- **Enterprise** - Dedicated Technical Account Manager (TAM) **Less than 15 mins support service.**

AWS Professional services is a global team of experts providing assistance for deploying high performance computing systems using various services in AWS cloud.

AWS Connect is an omnichannel cloud contact centre. Telephone as a service. High Quality Audio.

Billing and Pricing

- **Pricing calculator has replaced TCO**

- **On-Demand Instances** for short durations and uninterruptedly running.

- **Regional Reserved instances** are not guaranteed to have capacity!

- **Tenancy and capacity reservation are different.** Tenancy is security if have strict regulatory compliance while placing resources in the Public Cloud.

- **AWS Burst Capacity** allows for temporarily burst above baseline performance level.

- **AWS Kinesis** collecting, processes, and analyses streaming data.

- **Amazon QuickSight** allows for insightful business intelligence reporting with creative data delivery methods, including graphical and interactive dashboards.

- **AWS Personal Health Dashboard** provides detailed information about performance and availability of AWS services which may impact customers' resources. It is a service that prompts the user with alerts and notifications on AWS scheduled activities, pending issues, and planned changes.

- **AWS Lamda and Email** can subscribe to an SNS Topic.