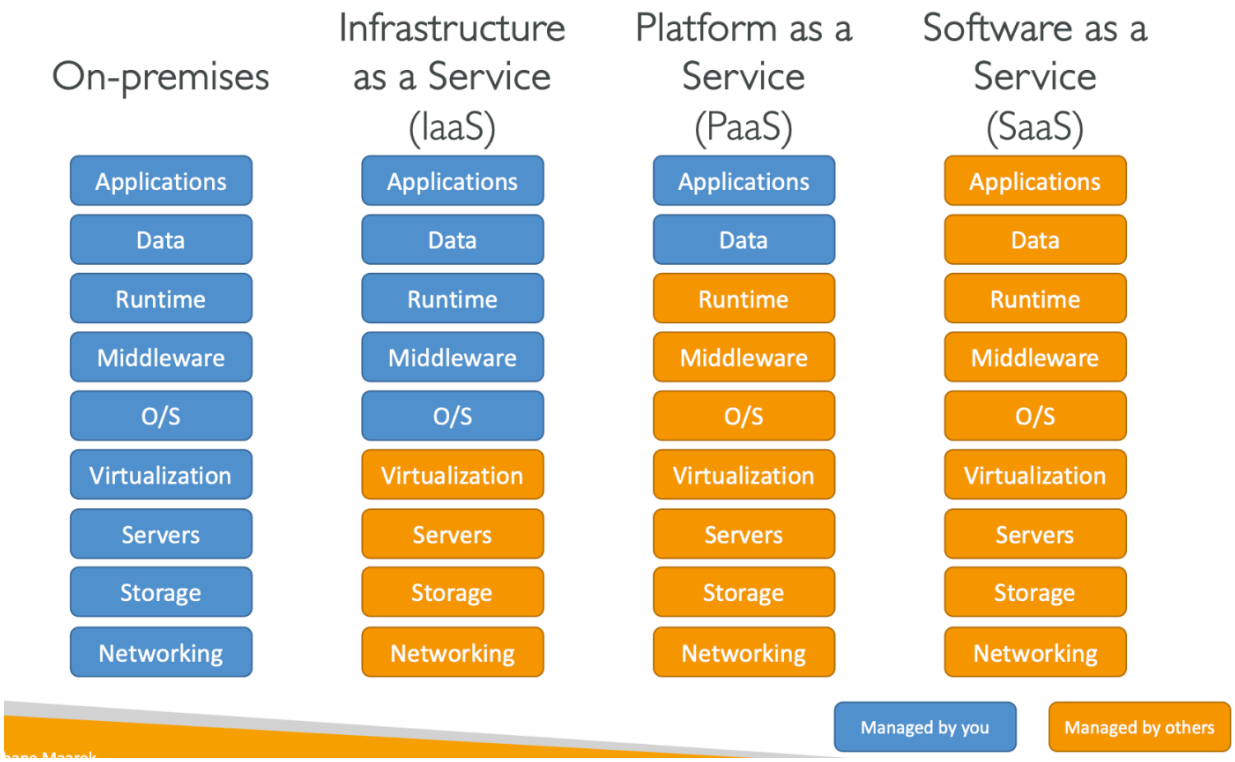
Udemy CCP Notes



- **ELB**: automatically distributes incoming application traffic across multiple resources
  - healthy check
- **SQS**: **decoupling and scaling of app**. can send, store, and receive messages between software components, without losing messages or requiring other services to be available
- **SNS**: **decoupling,** publishes messages to subscribers. (Subscribers can be web servers, email addresses, AWS Lambda functions, or several other options.)
- **Lambda**: run code without needing to provision or manage servers.
- Container Orchestration Tool:
  - **ECS**-Elastic Container Service: highly scalable, high-performance container management system that enables you to run and scale containerized applications on AWS.
  - **EKS**-Elastic Kubernetes Service: fully managed service that you can use to run Kubernetes on AWS.
- **Fargate**: **serverless** compute engine for containers. It works with both Amazon ECS and Amazon EKS.
- **Outposts**: run AWS infrastructure in your own data center
- **CloudTrail**: enables governance, compliance, operational auditing, and auditing of your AWS account.
  - cloudTrail Logs has **encryption default**
  - management events logged default
- **Elastic Beanstalk**: provide code and configuration settings, and Elastic Beanstalk deploys the resources necessary to perform: adjust capacity, load balancing, auto scaling, application health monitoring.
- **CloudFormation**: treat your infrastructure as code, deploy a collection of related resources

- **CloudFront**(CDN) : use Edge locations around the world to cache content for accelerating
- **VPC**: Define and launch AWS resources in a logically **isolated** virtual network
    - support **VPC endpoint gateway** for private connection: **S3, DynamonDB**(data not leave amazon)
    - Internet gateway:
    - **NAT gateway**: managed by AWS
- **VPN**: connection between your data center(on premises) and a VPC.
- ***Direct connect***: establish a dedicated **private** connection between your data center(on premises) and a VPC, 1 month to establish

I Both connect **on-premises VPN to AWS**,

- **Site to Site VPN**: **public** internet, connection is **encrypted**
- **Transit Gateway**: connect thousand VPC
- **Control Tower**:
    - run on top of AWS organization.
    - set up and govern a secure and compliant multi-account AWS environment based on best practices
- **Network ACL**(control access list):
    - for subnet, They are stateless and **allow** all inbound traffic by default.
    - **both deny and allow rule!**
    - contains a numbered list of rules and evaluates these rules in the increasing order while deciding whether to allow the traffic

I ***both check packet in and out, but SG is stateful, and NACL is stateless*** (https://explore.skillbuilder.aws/learn/course/134/play/99519/aws-cloud-practitioner-essentials)

- **Security group**:
    - for instances, They are stateful and **deny** all inbound traffic by default.
    - **only have allow rule!**
- Region has **at least 3 AZ**, each AZ **one or more data center**
- **Route53**(DNS domain name service): translating a domain name to an IP address. Able to use relocation-related routing policies.
    - SIMPLE ROUTING POLICY
    - WEIGHTED ROUTING POLICY
    - LATENCY ROUTING POLICY
    - FAILOVER ROUTING POLICY
- ***Example How Route 53 and CloudFront deliver content****: Client request→ Route53 translate domain to IP→ Client get Ip address → CloudFront(edge locations) → ELB → EC2 instances.*
- **EMR**: Hadoop clusters
- **Kendra**: document search service
- **Local Zone**: allow you to use select AWS services run **latency-sensitive applications**
    - extend of region
- **Encryption Automatically enabled:**
    - CloudTrail Logs, S3 Glacier, Storage Gateway
- **Dedicated host** support business **license** and **dedicated instance not.**
- **EFS- Elastic file system**: Multiple instances can access the data in EFS same time, **as long as in same region, EC2**

can access EFS! Auto scales, can access **up to 1000 EC2**

- **EBS** elastic block store: attach block-level storage volumes for EC2 instances, **EC2 and EBS need to be in the same AZ! Not auto scales**
    - Database, Enterprise software, file systems
    - mount OS and application files
    - cannot access simultaneously by multiple EC2 instances
- **EBS snapshots**: is an **incremental** backup, which means update items change instead of whole block
    - able to across AZ or region
- **EC2 Instance store**: **high performance, low latency, fault-tolerant architectures, physically attached**, provides temporary **block-level** storage for an Amazon EC2 instance. Terminate = lose data

Object storage *consists of data, metadata, key*

reservation option: DynamoDB, RDS, EC2

- **S3 standard**: 11-9's%, frequently accessed data, store data in a min of three AZ
- **S3 standard-IA**:
- **S3 Intelligent tiering**: Ideal for data with unknown or changing access patterns
- **S3 One Zone-IA**: in single availability zone
- **S3 Glacier instant retrieval**: data requires immediate access, retrieve objects within a few milliseconds
- **S3 Glacier Flexible Retrieval**: low-cost, within few mins to hours
- **S3 Glacier deep archive**: lowest-cost, retrieve within 12 hours
- **S3 outposts**: Creates S3 buckets on Amazon S3 Outposts, Makes it easier to retrieve, store, and access data on AWS Outposts
- **Storage Gateway**:
    - Hybrid storage service to allow on- premises to seamlessly use the AWS Cloud
    - Tape Gateway, File Gateway and Volume Gateway
    - **encryption auto**
- **AWS Health - Service Health Dashboard** displays the **general** status of AWS services
- **AWS Health - Your Account Health Dashboard** gives you a **personalized** view of the performance and availability of the AWS services underlying your AWS resources.
- **Compute Optimizer**: EBS, Lambda, EC2, ASG
- **Elastic Container Registry:** used to store, manage, and deploy Docker container images
- **ECS**: highly scalable, fast, container management service that makes it easy to run, stop, and manage Docker containers on a cluster
- **QuickSight: BI,** Serverless machine learning-powered business intelligence service to create interactive dashboards
- **Glue**: Serverless, Useful to prepare and transform data for analytics
- **API GateWay**: serverless, scale
- **Lightsail**:
    - simple web app
    - Great for people with little cloud experience
- **CodeStar**: manage software development activities in one place
- **CodeGuru**: automated code reviews and application performance recommendations

- **Macie**: identify and alert you to **sensitive** data, such as personally identifiable information (**PII**)
- Amazon **Detective analyzes:** investigates, and quickly identifies the root cause of security issues or suspicious activities (using ML and graphs)
    - Automatically collects and processes events from VPC Flow Logs
- **RDS**: run relational databases in the AWS Cloud. Business analytics
    - **Supported database engines**: aurora, PostgreSQL, MySQL, MariaDB, Oracle DB, MS SQL server
    - **Aurora serverless**: enterprise-class relational database, compatible with MySQL and PostgreSQL relational databases
    - **Read Replicas: Scale**
    - **Multi-AZ**: **Failover**, Can only have 1 other AZ as failover
    - **Multi-Region**: Disaster recovery, local performance for global read
- **DynamoDB**: **serverless** DB, NoSQL, key-value database service, **Auto Scaling**
    - **flexible schema and supports document data models**
    - **DynamoDB global tables(actitve-active)** replicate data automatically across your choice of AWS Regions and automatically scale capacity to accommodate your workloads
- **Redshift**: **SQl**. a data warehousing service that you can use for big data analytics
- **DMS** Database migration service: migrate relational databases, non-relational databases, and other types of data stores.
    - **Use cases:**
        - Development and test DB migrations
        - DB consolidation: all into one
        - Continuous replication.
- **Other**:
    - **DocumentDB**: **Fully managed NoSQL**. document database service that supports MongoDB workloads
    - **Neptune:** a graph database service.
    - **QLDB** Quantum Ledger DB: a ledger database service.
    - **Managed Blockchain:** use to create and manage blockchain networks with open-source frameworks.
    - **ElasticCache**: **in-memory DB**, adds caching layers on top of your databases to help improve the read times of common requests.
    - **DynamoDB Accelerator**: in-memory cache for DynamoDB
- **MQ**: managed message broker service
- **CloudHSM - Hardware** security Module: generate and use your encryption keys on the AWS Cloud
- **KMS** Key Management services: enables you to perform encryption operations through the use of cryptographic keys
- **Cloud Foundations**: help customers **deploy**, configure, and secure their new workloads while ensuring they are ready for **on-going** operations in the cloud
- **AWS Acceptable Use Policy:** prohibited uses of the web services
- **Shared Responsibility Model:**
    - Both: **AWS and Customer**
        - Patch & Configuration Management, Awareness & Training
    - **AWS:** Security of the cloud
        - Edge Location Management
        - updating firmware
        - Physical and Environmental controls

    - **Customer:** Security in the cloud
        - Server-side Encryption
        - Database encription
        - patch guest OS and app
        - Service and Communications Protection or Zone Security
- **IAM**: enables you to manage access to AWS services and resources securely.
    - **Users (**default user without any permissions): an identity created in AWS
    - **Policies(least privilege):** a document that allows or denies permissions to AWS services and resources.
    - **Groups**: a collection of IAM users. When you assign an IAM policy to a group, all users in the group are granted permissions specified by the policy.
    - **Roles**: an identity that you can assume to gain **temporary** access to permissions*. (When someone assumes an IAM role, they abandon all previous permissions that they had under a previous role and assume the permissions of the new role.)*
- **IAM Credentials report (account-level)**
    - List all account's users and the status of their various credentials
- **IAM Access Advisor(user-level)**
    - Show the service permissions granted to a user and when those service were last accessed
- **MFA**: provides an extra layer of security for your AWS account.
- **Organization**: A central location to manage multiple AWS accounts
    - The AWS account must be able to operate as a standalone account. Only then it can be removed from AWS organizations
    - When creating an org, auto creates a root
    - **SCP** service control policies: **can limit the permission of the root user.** centrally control permissions for the accounts in org.
    - **OU** org units: to manage accounts with similar business or security requirements*. (When you apply a policy to an OU, all the accounts in the OU automatically inherit the permissions specified in the policy.)*
- **Artifact**: provides on-demand access to AWS security and compliance reports and select online agreements.
    - **AWS Artifact Agreements**: can review, accept, and manage agreements for an individual account and for all your accounts in AWS Organizations.
    - **AWS Artifact Reports**: provide compliance reports from third-party auditors
- **DDoS** distributed denial-of-service: a deliberate attempt to make a website or application unavailable to users.
    - **for: EC2, ELB, CDN, Route53, Global Accelerator**
    - **Shield:** protects applications against DDoS attacks.
        - **Shield Standard:** Auto protects all AWS customers at no cost
        - **Shield Advanced:** paid to provide detailed attack diagnostics and the ability to detect ad mitigate sophisticated DDoS attacks.
- **System manager**: Hybrid service, deploy security patches at regular monthly intervals automatically.
    - run commands, patch & configure our servers
- **Firewall Manager**: centrally configure and **manage firewall rules across all accounts** in your AWS **Organization**
- **WAF** web app firewall: monitor network requests that come into your web app.
    - Work with ELB and CloudFront
    - Web ACL, similar with NACL
- **Trusted Advisor**: inspects your AWS environment and provides **real-time** recommendations in accordance with AWS best

practices.

    - **Five pillars**: Cost optimization, performance, security, fault tolerance, service limits
    - check s3 permission
    - MFA for RU
- **Inspector**: improve the **security(network)** and compliance of applications by running automated security **assessments**. *(checks applications for security **vulnerabilities** and **deviations** from security best practices, such as open access to Amazon EC2 instances and installations of vulnerable software versions.)*
    - **only** for EC2 instances, Container Images & Lambda functions
- **GuardBody**: provides **intelligent** threat **detection** for your AWS infrastructure and resources.
- **Athena**: analyze data in S3 using SQL queries
- **CloudWatch**: monitor and manage various metrics and configure alarm actions based on data from those metrics.
    - **MTTR**: Mean time to resolution
    - **TCO**: Total cost of ownership
- **CloudTrail**: records API calls for account(provision, manage, and configure)
- **X-Ray:** analyze and debug **serverless** and distributed applications such as those built using a **microservices** architecture
- **Free Tier**: enables you to begin using certain services without having to worry about incurring costs for the specified period.
    - Types: always free, 12 months free, trials
- **Pricing 3 categories**: Pay for what you use, Pay less when you reserve, Pay less with volume-based discount when you use more
- **Billing Dashboard**: pay your AWS bill, monitor your usage, and analyze and control your costs.
    - **Consolidated billing**: receive a single bill for all AWS accounts in your organization. Default min account is 4.
    - **Budgets**: create budgets to plan your service usage, service costs, and instance reservations.
    - **Cost explorer**: lets you forecast usage up to 12 months, visualize, understand, and manage your AWS **costs and usage over time**.
- **Support Plan**:
    - provide access to guidance, configuration, and troubleshooting of AWS interoperability with third-party software
        - Enterprise, Business
    - lowest price trusted advisor, provides architectural guidance contextual to your specific use-cases, 24x7 contact
        - Business
    - provide access to only core checks from the AWS Trusted Advisor Best Practice Checks
        - Basic, Developer
    - **Basic -**
        - One-on-one responses to account and billing questions
        - Support forums
        - Service health checks
        - Documentation, technical papers, and best practice guides
    - **AWS Developer Support** -
        - testing or doing early development on AWS
        - email-based technical support during business hours
        - only supports general architectural guidance.
    - **AWS Business Support**

        - 24x7 phone, email and chat access to technical support and architectural guidance in the context of your specific use-cases.
        - Full access to AWS Trusted Advisor Best Practice Checks.
        - Access to Infrastructure Event Management for an additional fee.
    - **AWS Enterprise On-Ramp Support**
        - production/business critical workloads in AWS
        - 24x7 access to technical support and need expert guidance to grow and optimize in the Cloud.
        - supports architectural guidance contextual to your application (one per year).
    - **AWS Enterprise Support** -
        - provides customers with concierge - achieve their outcomes and find success in the cloud.
        - 24x7 technical support from high-quality engineers, tools and technology to automatically manage the health of your environment, consultative review and guidance based on your applications,
        - TAM to coordinate access to proactive/preventative programs and AWS subject matter experts.
        - supports architectural guidance contextual to your application.

- **CAF** Cloud Adoption Framework: advice to enable a quick and smooth **migration to AWS** *(https://explore.skillbuilder.aws/learn/course/134/play/99519/aws-cloud-practitioner-essentials)*
    - **business capabilities**: People, business, governance
    - **technical capabilities**: platform, security, operation
    - Do it before move migration:
        - Leverage agile methods to rapidly iterate and evolve
          Organize your teams around products and value streams

    - **Business:** ensures that **IT aligns with business** needs and that IT investments link to key business results.
    - **People: connect technology and business**. support development of an org-wide change management strategy for successful cloud adoption
    - **Governance: risk management.** focuses on the skills and processes to align **IT strategy** with **business strategy**, max the business value and min risk
    - **Platform:** includes **principles** and **patterns** for implementing new solutions on the cloud, and migrating on-premises workloads to the cloud.
    - **Security:** ensure that the org meets **security** objectives for visibility, auditability, control, and agility.
    - **Operations:** helps you to enable, run use, operate, and recover IT **workloads** to the level agreed upon with your business stakeholders.

- **Well-architected framework**: ensure AWS workloads and system follow best practices.
    - **Operational excellence**: run and monitor systems to deliver business value and to continually improve supporting processes and procedures.
    - **Security**: protect information, systems, and assets while delivering business value through risk assessments and mitigation strategies.
    - **Reliability**:
        - CloudTrail, CloudWatch, Config
    - **performance efficiency**:
    - **cost optimization**:

    - **sustainability**: continually improve sustainability impacts by **reducing energy consumption**
- **Migration Evaluator**: compare current env cost to the cost of running in the AWS cloud
- **Miragtion 7's R**
    - Retire, Retain, relocate, rehost, replatform, repurchase, refactor
- **Step function** : Build serverless visual workflow to orchestrate your Lambda functions
- **Snow Family**: use **OpsHub** managed Snow Family
    - **Snow cone**: 2 CPU, 4GB memory, up to 14 TB
    - **Snowball**: 80 - 210 TB
    - **Snowmobile**: 100 PB
- Other:
    - Amazon Textract is a machine learning service that automatically extracts text and data from scanned documents.
    - Amazon Lex is a service that enables you to build conversational interfaces using voice and text.
    - AWS DeepRacer is an autonomous 1/18 scale race car that you can use to test reinforcement learning models.
- **Config:**
    - access, audit, monitor, and evaluate the configuration of AWS resources.
    - recording compliance of your AWS resources
- **Partner Network: third party** support you in AWS cloud