AWS CCP notes

22 January 2023 00:03

Amazon Cloud practitioner exam

What is Cloud Computing ?

Traditional IT: On-Premises
Types of Cloud Computing:
1. IaaS (Infrastructure as a Service):
-Providing Building blocks of cloud IT
example: GCP,AWS,Azure
2. Paas (Platform as a Service)
ex: Elastic Beanstalk,
Heroku, Google App engine
3. SaaS (Software as a Service)
ex: Gmail, Zoom, AWS Machine Learning

AWS Availability Zones :
-Each region has min 2 AZs
-Each AZ has 1 or more data centres

Pricing Model:
-Compute: Pay for compute time
-Storage: Pay for data stored in cloud
-Network: Pay for data transfer OUT of the cloud

Shared Responsibility Model:
Customer : Responsible for Security of Data IN the cloud
AWS: Responsible of Security OF the Cloud

AWS Acceptable Use Policy:
No Illegal Usage
No Email abuse

IAM - Identity & Access Management:

IAM is a global service
Root account
->Admin Account
-> Users (for each person)

Group: Collection of Users
User can/cannot belong to a Group
User can be part of Multiple Group

IAM Permissions:
Users or Groups can be assigned JSON documents called policies
Apply Least privilege permission

IAM Policies:
Policies attached to Group level.
All Users in that Group inherit that policy
User without Group can be attached "in-line policy"

IAM Policies Structure:
  Version:
  Id: (optional)
  Statement:
    Sid: (optional)
    Effect:
    Principal:
    Action:
    Resource:
    Condition: (optional)

IAM Password Policy:

IAM MFA: Multi Factor Authentication
  -Recommended to use
  -Protect Root accounts with MFA device
    -Virtual MFA Device (Google Authenticator, Microsoft Authenticator)
    -U2F Security Key: USB type physcial device
    -Hardware Key MFA Device:

AWS Access Keys:
  How to access AWS Management console:
    -Protected by password + MFA
    -AWS CLI
    -AWS SDK

  Access keys generated through AWS Console
    Can be used in AWS CLI to login (Programmatic access)
    Can be used in AWS SDK to login (Programmatic access)

AWS Cloudshell:
  Terminal in Cloud of AWS
  Free to use

IAM Roles for Services:
 Roles are where you can attach Policies (Permissions)
 Now these Roles can be attached to Users, AWS Services, 3rd party services

 Can be attached to a EC2 instance
 example IAM Role: DemoRoleForEC2 , Policy: IAMReadOnlyAccess

 Common Roles:
  EC2 Instance Roles
  Lambda Fucntion Roles
  Roles for CloudFormation

IAM Security Tool:
  IAM Credentials Report - account level
    -list all users of the account
    -status of their credentials

  IAM Access Advisor - User level
    -shows service permission granted to the user
    -used to revise the policies

Shared Responsibility:

AWS:
-Infrastructure (Global Network Security)
-Compliance Validation
-configuration

You:
-User, Groups, Policies management & monitoring
-Enable MFA
-Analyze access patterns & Permissions

Summary:
-Users:
-Groups:
-Policies:
-Roles:
-Security:
-AWS CLI:
-AWS SDK:
-Access Keys:
-Audit: IAM Credentials Report & IAM Access advisor

EC2 : Elastic Cloud Compute
aws iam list-users

AWS Budgets Setup:
Create a AWS Budget for Cost type
Set a Target budget
Triggert email is 80% acheived of the target budget

EC2 Basics:
-Elastic Compute Cloud
-Infrastructure as a Service
-Virtual server in a the cloud
-Consists of:
-Renting virtual machines (EC2)
-Storing data on virtual drives (EBS)
-Distributing Load across machines (ELB)
-Scaling the services using auto-scaling (ASG)

EC2 Sizing & configuration:
-OS : Linux, Windows, Mac
-RAM
-Compute Power & cores (CPU)
-Storage Space:
-Network attached (EBS, EFS)
-hardware attached (EC2 Instance store)
-Firewall rules (Security Group)
-Bootstrap Script (EC2 User Data)
-Network Card: speed of the card

EC2 instance types:
-t2.micro , t2.xlarge, c5d.4xlarge , m5.8xlarge
example: m5.2xlarge
m: instance class
5: version
2xlarge: size within the instance class

Types:
-General Purpose (Free tier - t2micro)
-Compute Optimized
-Memory Optimized
-Storage Optimized

Security Groups:
-Only contain ALLOW rules
-Rules by IP address/ or other security groups
-Applies to Network Traffic of EC2 instance
-Controls inbound and outbound network to & from EC2 instance

-Locked down to a Region/VPC

-Good to have separate Security Group for SSH access.
-"Time-Out" -> then a security Group issue
-"Connection Refused" -> application issue
-All inbound traffic is blocked by default
-All outbound traffic is allowed by default

Classic Ports to know:
SSH: 22
FTP: 21
SFTP: 22 (upload using SSH)
HTTP: 80
HTTPS:443
RDP: 3389 (log in to a Windows instance)

SSH overview:
We can use Putty in Windows to connect
Windows 10 or above can access SSH via Powershell
Mac or Linux can access via Terminal

EC Instance Connect: SSH to EC2 via AWS console
Operating System Independent

EC2 instance types:
-On demand :
60s minimum billing
Linux: per second
Windows: per second
Any Other OS: per hour

-Reserved instances:
1 or 3 year reservation
75% savings over On demand
Reserve a specific instance type

-Spot instances:
90% savings over On demand
Can be lost if anyone overbids for that instance
Use for workload resilient to failure
Ex: batch jobs, Data analysis, distributed workloads

-Dedicated Instances:
EC2 instancs running on hardware dedicated to you
Don't get access to that hardware

No control over instance placement

-Dedicated Hosts:
for server licence - BYOL (Bring Your Own License)
for compliance requirements
3 year period reservation

Shared Responsibility Model:
AWS:
-Infrastructure (Global network security)
-Isolation on Physical host
-Replacing Faulty hardware
-Complaince validation

User:
-Security Group rules
-Operating System patches
-Software & Utilities installed in EC2
-Data security on your instance

Summary:
EC2 Instance: AMI (OS) + Instance Size (CPU+RAM) + Storage+ security groups+ EC2 user Data
Security Groups: Firewall attached to EC2 instance
EC2 User Data: Script launched at first start of instance
SSH: start a terminal into the instance via (port 22)
EC2 Instance Roles: Link to IAM roles
Purchasing Options:
On Demand, Spot, Reserved (1 or 3 years)

EC2 Instance Storage:

EBS Volume:
Elastic Block Volume - network drive which can be attached to EC2 instance
Can be only mounted to 1 or No instance at a time.
1 instance can have multiple EBS volumes

Locked to a AZ (Availability Zone)
EC2 instance must be in the same AZ as EBS

Have a provisined capacity
Billed for the provisioned capacity

EBS Snapshots:
Backup of the EBS volume
The snapshots are automatically saved to Amazon Simple Storage Service (Amazon S3) for long-term retention.
Can copy snapshots across AZs or Regions

AMI (Amazon Machine Image) Overview:
-customization of an EC2 instance
-Built for a Specific Region
-An EC2 instance can be built from:
-A Public AMI:
-Custom AMI:
-AMI from AWS Marketplace

Question:An AWS user is trying to launch an EC2 instance in a given region.
What is the region-specific constraint that the Amazon Machine Image (AMI) must meet so that it can be used for this EC2 instance?

Ans: You must use an AMI from the same region as that of the EC2 Instance
The region of AMI doesn't impact performance of EC2 instance

You can launch EC2 instances from AMI:
Existing Instance --> Custom AMI---> New Instance

EC2 Image Builder Overview:
-Automate creation, maintain, validate and test EC2 AMIS

EC2 Instance Store:
-Hardware Disk attached to the EC2 instance
-Extreme High Performace storage
-Better I/O performance
-Could loss the storage if stopped

EFS - Elastic File System:
-Managed network file system
-Can be mounted on 100s of EC2 instances
-Works in Multi AZs
-Highly available, expensive
-Can be mounted on On-premise Servers

EFS - IA: Infrequent Access
92% lower cost compared to EFS Standard
Files will be moved automatically to IA , based on usage
Define a Lifecycle policy

Amazon File systems:
Amazon FSx for Windows:
- Windows, Microsoft Server files

Amazon Fsx for Lustre:
Linux File server
High Performance Computing (HPC)

Shared Responsibility Model:
AWS:
-Infrastructure
-Replication for Data for EBS & EFS
-Replacing Faulty hardware
-Ensuring AWS employees don't see user data

User:
-Setting up backup/snapshot
-Setting up data encryption
-Understanding risk of Instance Store

Summary:
-EBS Volumes:
-network drives attached to EC2 instances
-Mapped to AZ (availability zone)
-EBS snapshots : Backups/transferring EBS volumes across AZs
-AMI:

-ready to use EC2 instances with customizations
-EC2 Image Builder:
-automatically build, test and distribute AMIs
-EC2 Instance Store:
-High Performance hardware disk attached to EC2 instance
-Lost if instance is stopped/terminated
-EFS:
-network file systems can be attached to 100s of instance in a Region
-EFS-IA:
-cost optimized storage for Infrequent Access files
-FSx for Windows:
-Network file systems for Windows servers
-FSx for Lustre:
-Network file systems for Linux servers

ELB & ASG - Elastic Load Balancing & Auto Scaling Groups

Scalability & High Availability
High Availability
-running instance in >= 2 AZs
-In case of a disaster in any Data centre , the app will still be available
-Run Instances of same application in Multi AZ
-Auto Scaling Group Multi AZ

Scalability:
- Vertical Scaling: Increasing instance size (scale up/down)
- Horzontal Scaling: Increasing number of instances (scale in/out)
    - Auto Scaling Group
    - Load Balancer
- High Availability: Run instances for same application in multiple Azs
    - Auto Scaling Group in Multi AZ
    - Load Balancer in Multi AZ

Scalability vs Elasticity (vs Agility)

Scalability:
-Ability to accomodate larger load my making hardware stronger (scale up)
,or by adding more nodes (scale out)

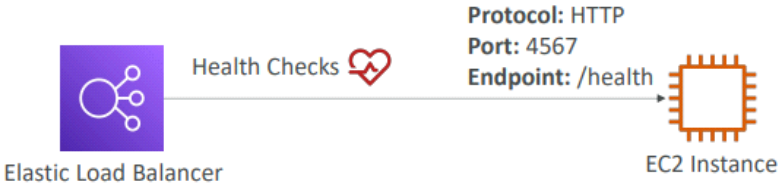
Elasticity:
-Once a system is scalable , there should be some sort of
"Auto scaling", so that system can scale based on Load.
System must be pay per use and "cloud-friendly"

Agility (not related to Scalability - distractor)
Ability to add new Cloud resouces in minutes
Reducing the time to add new Cloud resources

Load Balancers :
- Load balancers are servers that forward internet traffic to multiple servers (EC2 Instances) downstream.
- Expose a single point of access (DNS)
- Do regular **health checks**
- Provide SSL termination (HTTPS) for websites
- Handle failures of downstream systems

- Enforce stickiness of cookies
- Separate public traffic from private traffic
- High Availability acrosss zones

Health checks of ELB:



ELB - Elastic Load Balancer
AWS Managed Load Balancer

Types of Load Balancers: (AWS managed LB)

- ALB (Application Load balancer) - Http/HTTPS L7
  - -Layer 7
- NLB (network load balancer)- TCP -L4
  - ultra high performance, allows for TCP
  - Layer 4
- Gateway Load Balancer

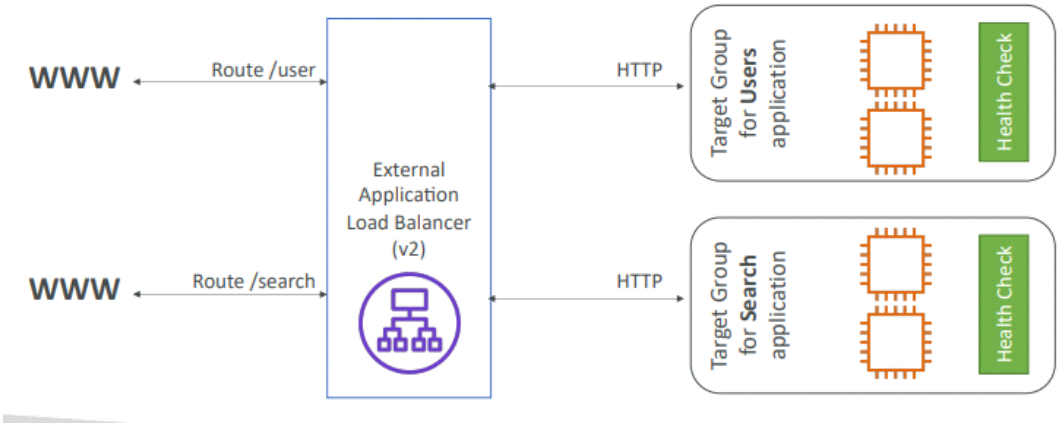
- CLB (Classic Load Balancer)
  - -Layer 4 and Layer 7
  - -Service is retired from AWS

Load Balancer Security Groups :

EC2 instances will accept the traffic only from Load balancer security Group

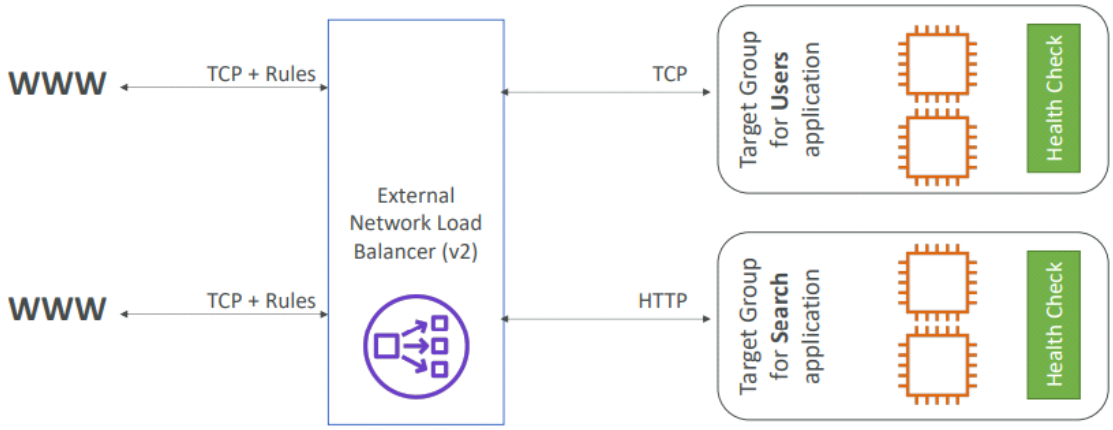
Application Load Balancer:

- Layer 7 (HTTP) load balancer
- Supports redirects (HTTP to HTTPs)
- Load balancing to multiple applications in the same machine
- Routing based on target groups
- Good fit for microservice & dockerize containers



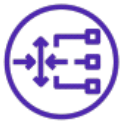
Network Load Balancer:

- Layer 4 (Transport Layer) load balancer
- Forwards TCP and UDP traffic to our instances
- High performance (millions of requests)
- 1 static IP per AZ
- Health check supports: TCP, HTTP, HTTPs



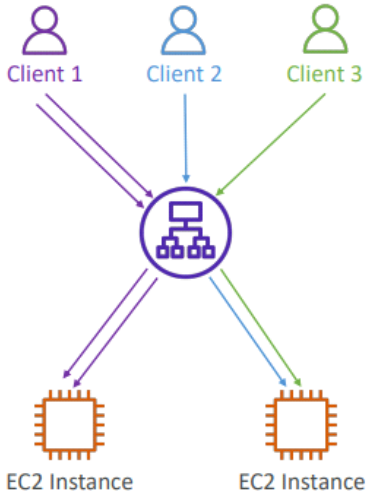
Gateway Load Balancer:

- Operates at Layer 3 (Network layer) - IP Packets
- Deploy, scale and manage a fleet of 3rd party network virtual appliances
- Firewall, Intrusion detection systems, Deep packet inspection systems
- Uses **GENEVE** protocol on port 6081



Elastic Load Balancer: Sticky Sessions (Session Affinity)

- Same client is redirected to the same instance behind the load balancer



- This is implemented with the help of Cookie

Cookies:

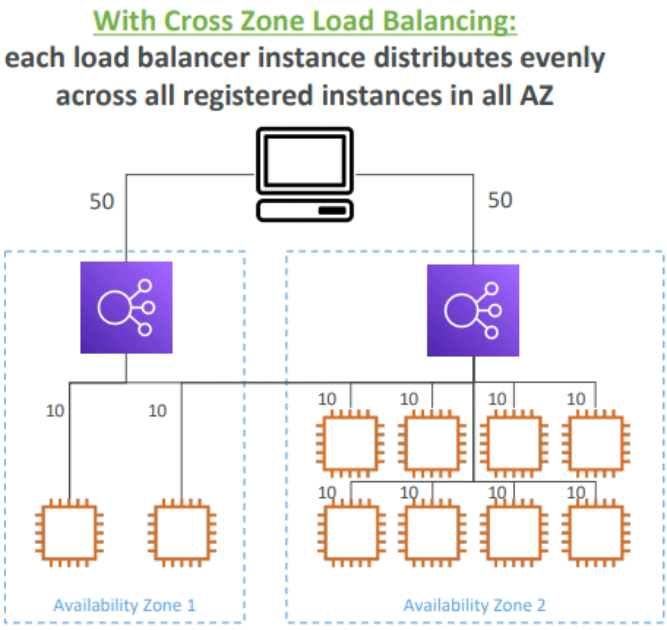
- Application Based Cookie
- Duration Based Cookie

Cookies can be configured in the Target group. Enable the Stickiness.

Elastic Load Balancer : Cross Zone Load Balancing

With cross zone load-balancing :

Traffic is evenly distributed to all instances spread across all AZs



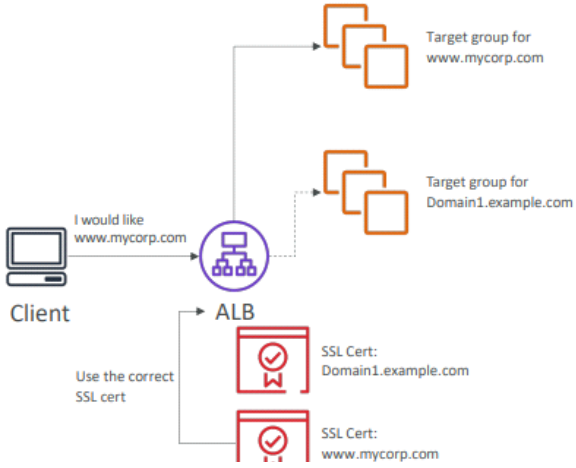
Elastic Load Balancer: SSL/TLS

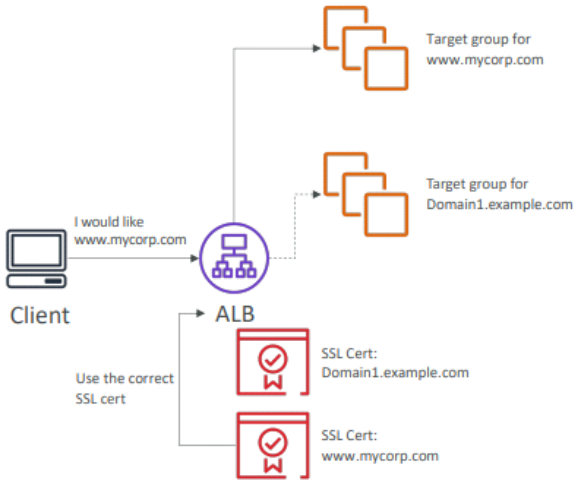
- Traffic between Client and Load Balancer is encrypted
- SSL is secure Sockers Layer ,used for encrypting connections
- TLS is Transport Layer Security is a newer version of SSL
- Public SSL certitificates are issued by Certificates Authority(CA) ex: GoDaddy, Digicert

- Load Balancer loads a X.509 certificate (SSL/TLS certificate)

SSL - Server Name Indication (SNI)

- To Load Multiple SSL certificates into a web server
- Client requires to indicate the "hostname" to initiate SSL handshake
- Works only for ALB, NLB and CloudFront





- How to Add SSL certiifcates ?
  - Go to the ALB console
  - Add a HTTPS listener
  - Forward Requests to a Target Group
  - Secure Listener Settings:
    - Mention a Security Policy
    - Load the SSL/TLS certiifcates from ACM/import/load
  - In case of NLB, add a TLS listener

Connection Draining:

- When an EC2 instance is being de-registered or taken off , then it's given time to complete all the "in-flight" requests
- This time to drain all the existing connections can be set in the LoadBalancer.
- Stops sending new requests to the EC2 instance which is getting de-registered
- New users will be automatically connected to other healthy instances by LoadBalancer
- Deregistration Delay naming NLB, ALB

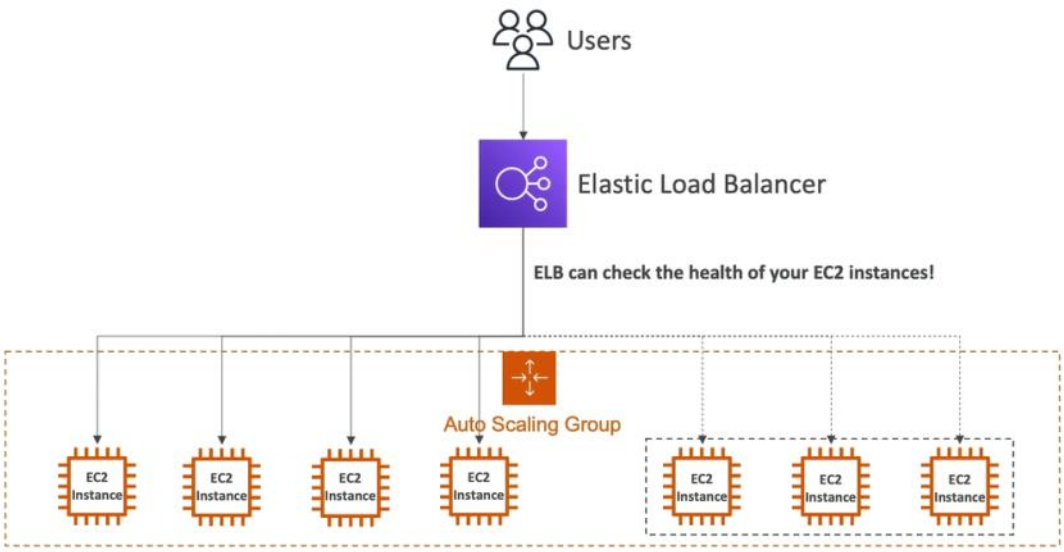
Auto Scaling Group (ASG) strategies :

We have a application that can be load balanced by Elastic Load Balancer
Goal of ASG groups:

- -Scale out (add EC2 instances) to match increase load
- -Scale in (remove EC2 instances) to match decrease load
- -Ensure min/max number of machines running
- -Automatically register new instance to Load Balancer
- -Replace unhealthy instances
- -Cost savings : Only Run at Optimal Capacity (Main Goal)

Auto Scaling Group (ASG) works Hand-inHand with Elastic Load balancer (ELB)

Minimum Capacity
Desired Capacity (Optimal)
Maximum Capacity

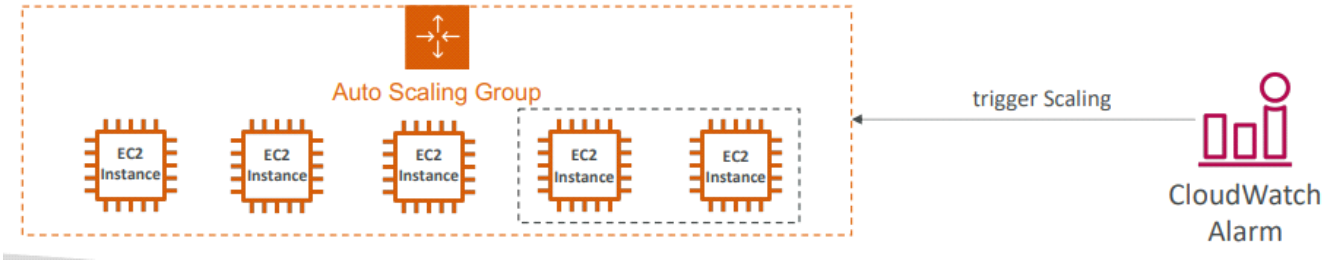


Auto Scaling Group: Attributes

- Launch Template
- Min/Max/Initial capacity
- Scaling Policies

Auto Scaling : CloudWatch Alarms

- Based on alarms we can have scale-out/scale in policies
- Metrics can be CPU usage



Hands-on:

- Create a Target Group
- Create a Load balancer and attach the target group
- Create a security group for Load-Balancer and for EC2 instances
- Ec2-instance's security group should allow all HTTP traffic from Load-Balancer security group
- Create a Launch template
- Attach it to ASG
- Follow the default configurations
- Launch ASG

Auto Scaling Group (ASG) Strategy:

Manual Scaling

-update the size of ASG manually

Dynamic Scaling

-respond to changing demand automatically:

1. Simple/Step scaling
2. Target Tracking scaling
3. Scheduled Scaling

Predictive Scaling

-Uses ML to predict future traffic

-Scaling happens before the event

Summary:
-High Availability vs Scalability vs Elasticity vs Agility:
High Availability: Having instances in multiple AZs
Scalability: Vertical (increasing the size of the instance) &
Horizontal (increasing the number of instances)
Elasticity: Ability to scale up/down
Agility: Work faster by creating/deleting instance faster

-Elastic Load Balancer (ELB):
Distribute traffic accross backend EC2 instances
Multi AZ instances
Supports health checks
3 types: Application LB (Http L7) , Network LB (TCP L4), Classic LB

-Auto Scaling Groups (ASG):
Implement Elasticity for instances , across Multi AZ
Scale EC2 instance based on demand
Replace unhealthy instances
Integrate with ELB

Amazon S3 service:

Store objects (files) in buckets (directories)
Bucket - globally unique name for all accounts
Infinite Scaling
Region specific
Has proper naming convention
Objects have Key-Value
Key is the object path , Value is the object data
Metadata - list of key/value pairs
Stores Data in Flat non-hierarchical structure

S3 Bucket
-bucket name has to be globally unique
Buckets are region specific
Objects are stored in Buckets

S3 object:
Max object size: 5 TB
Objects Greater than 5 GB has to be upload in multi-part
Object location -> key
key is the FULL path:
-s3://my-bucket/myfile.txt
-> key: myfile.txt
-s3://my-bucket/my_folder/my_subgoler/myfile.txt
-> key: my_folder/my_subgoler/myfile.txt

S3 Security:
User Based
-IAM policies : Which API calls should be allowed for a specific IAM user
Resource Based
-Bucket Policies

User responsible for S3 encryption

Bucket Policy:

TO make objects accessible to the public internet
We need to turn off "Block public access"
And define a bucket policy :
(mention resource as arn_number/*)

```
{
  "Id": "Policy1639227397127",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1639227392849",
      "Action": [
        "s3:GetObject"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::ashutosh-ccp-bucket-1/*",
      "Principal": "*"
    }
  ]
}
```

"Effect" this "Action" on this "Resource" for "Principal"
=>Allow this GetObject on this bucket for All.

S3 Encryption:
User is reponsible for encryption of files
Types:
No Encryption
Server-Side encryption
-server encrpts file after receiving it
Client-Side encryption
-user encrpts the file before uploading it

S3 Websites:
S3 can host static websites and accessible on www
User gets 403 (Forbidden) if bucket policy doen't allow public reads

S3 Versioning:
Git lke versioning on objects at bucket level

S3 Server Access Logs:
For audit process
Log all access requests made to S3 bucket
Access logs to 1 S3 bucket will be logged to another S3 bucket

S3 Replication :
Types:
Cross Region Replication
Same Region Replication

S3 storage classes:
-S3 general purpose
No retrieval fee
Sustain 2 concurrent facility failures
Use cases: Big Data analytics , Gaming

-S3 Intelligent Tiering
moves data between frequent/infrequent access

based on usage patterns
No retrieval fee
Use cases: Resiliency against events that impact an entire AZ

-S3 Infrequent Access (IA)
Retieval fee required
Sustain 2 concurrent facility failures
Lower cose than S3-IA
Use case: Primary backup datastore for any Disaster recovery

-S3 One Zone IA
Data stored in One AZ
Retieval fee required
Use case: Secondary backup copies of on-premise data

-Amazon Glacier
Retieval fee required (Cheap)

-Amazon Glacier Deep archive
Retieval fee required (cheapest)

S3 Durability and Availability:
High Durability
-Loss of single object once in 10,000 years
Availability:
-S3 Standard has 99.99% availability
-it will not be availble for 53 minutes in a year
-Vaires depending on storage classes

AWS Snow Family:
If Data transfer takes over a week.
Offline Devices to perform
Data Migration usages in/out of AWS
Edge Computing purposes

Edge computing: Snowball Edge, Snowcone

Snow Family Devices :
1. Snowcone
-Small potable, rugged devices
-withstand harsh environment
-Good for remote research facilities
- Can Hold a storage of max: 8 TBs
Data migration: upto 24 TB, online and offline

2. Snowball Edge
- Use this to move data > 8TB && < 10 PB
- DataCentre decommissioning
- Huge data migrations
Data migration: upto petabytes

3. Snowmobile:
-Use this to move data > 10 PB
-Entire truck
-High Security
-For transfering > 10 PB of data
Data migration: utp exabytes

AWS Datasync:
This is a agent installed in Snowcone
to tranfer data back to AWS cloud

What is Edge Computing ?
-Process Data at remote location with no Internet connectivity
-Setup Snowball edge/Snowcone device
-Ship to AWS facility
Devices:
-Snowcone
-Snowball Edge - Compute Optimized
-Snowball Edge - Storage Optimized
Long term deployments (1 and 3 years)

AWS OpsHub:
-Software to use and manage Snow Family Devices
-Installed on On-Premise servers

Hybrid Cloud for Storage:
-Part of infra is on-prem & rest on cloud
How to expose S3 data to on-premises ?

-AWS Storage Gateway
Bridge between On-prem data and Cloud data in S3

AWS Storage Cloud Native Options:
BLOCK: Amazon EBS, EC2 Instance store
FILE: Amazon EFS
OBJECT: Amazon S3, Glacier

Native On-prem Servers has these Storage Types:
-File
-Volume
-Tape

Shared Responsibility Model:
AWS:
-Infrastructure (Global security)
-Durability
-Sustain concurrent loss of data in 2 facilities
-configuration and vulnerability analysis
-Compliance validation
User:
-S3 Versioning
-S3 Bucket Policies
-S3 Replication Setup
-S3 Storage Classes
-Data encryption at rest and in transit
-Logging and monitoring

Summary:
Buckets vs Objects:
Global unique name
Tied to a region
S3 security:
IAM Policy , S3 Bucket Policy, S3 Encryption

S3 Websites:
Host static websites
S3 Versioning:
Similar to git technology, prevent accidental deletes
S3 Access Logs:
Log requests made within S3 bucket
S3 Replication:
Same region , Cross region replication
Must enable versioning
S3 Storage Classes:
Standard
IA:
IZ-IA:
Intelligent:
Glacier:
Glacier Deep Archive:
S3 Lifecycle Rules:
Transition objects between storage classes
S3 Glacier Vault Lock/Object Lock:
WORM (Write Once Read Many) - Objects never need to be deleted, only read
Snow Family:
Data migration via physical device , Edge Computing
OpsHub:
Desktop app to manage AWS Snow Family devices
Storage Gateway:
Bridge between On premises storage to S3 storage

Databases & Analytics:
Relational Databases
No SQL database
-JSON format data

AWS RDS :
create databases in the cloud that are managed by AWS
• Postgres
• MySQL
• MariaDB
• Oracle
• Microsoft SQL Server
• Aurora (AWS Proprietary database)
-managed service with SQL capability suited for Online Transaction Processing (OLTP)

Aurora DB:
PostGreSQL , MySQL supported as AWS Aurora DB
Aurora costs more than RDS

RDS Deployments:
Read Replicas, Multi AZs
Multi Region (Read replica)
-Read replicas:
Scale the read workload of DB
Writing is done to the main DB
-Multi AZ:
Failover in case of AZ outage(high availability)
Replication is done in a different AZ
When Main DB fails, Data written to failover DB
-Multi Region:

Same as Read replicas
But deployed in different regions
Disaster recovery in case of region outage
Low latency
Replication cost

AWS Elastic Cache :
Managed Redis or Memcached

DynamoDB:
Fully Managed Highly available with replication across 3 AZ
NoSQL database
serverless database

DynamoDB Accelerator (DAX)
-In memory Cache for DynamoDB

DynamoDB GLobal Tables
Accessible in mulitple regions
Active-Active replication => read/write to any AWS region

Amazon Redshift:
Based on PostGreSQL
Used for OLAP (Online analytical processing)
Data Warehousing and Analytics
Columnar storage of Data

Amazon EMR:
Elastic Map Reduce
Hadoop Cluster: Big Data
Analyze and process vast amount of data
-data processing , machine learning, big data , web indexing
enables businesses, researchers, data analysts, and developers to easily
and cost-effectively process vast amounts of data

Amazon Athena:
-Analyze data in S3 using serverless SQL query

Amazon Quicksight
-Dashboards on Databases
-Serverless ML powered BI service to create interactive dashboards
-ML: Machine Learning, BI: Business Intelligence

DocumentDB :
-AWS managed implementation of MongoDB
-NoSQL database

Amazon Neptune:
-Fully managed graph database
-Social networking platforms

Amazon QLDB:
Quantum Financial Ledger Database
-recording financial transactions
-review history of changes made in application data
-Immutable system (no entry can be removed or modified)

Amazon Managed Blockchain:
-managed Hyperledger Fabric & Ethereum blockchains
-create and manage scalable blockchain networks
-create decentralized blockchain

Amazon Glue:
-ETL (Extract Transform Load) service - Amazon managed
-Data catalogue service
-makes it easy for customers to prepare and load their data for analytics
-AWS Glue Data Catalog is a central repository to store structural
and operational metadata for all your data assets

Amazon Database Migration:
Migrate databases to AWS
This Service helps you migrate databases to AWS quickly and securely.
The source database remains fully operational during the migration
minimizing downtime to applications

AWS Shared responsibility for Databases & Cache:
AWS :
takes care of OS maintenance / patching, optimizations, setup,
configuration, monitoring, failure recovery and backup
User:
If non managed Databases then
Resilency, backup, patching, high availability,
fault tolerance & scaling

Summary:
Relational Database: OLTP - RDS, Aurora (SQL)
Diff btw Multi AZ, Read Replicas, Multi Region:
In memory Database: ElastiCache
Key/Value Database: DynamoDB(serverless), DAX (cache for DynamoDB)
Warehouse- OLAP : Redshift (SQL)
Hadoop Cluster: EMR
Athena: Query data on Amazon S3 (serverless SQL)
Quicksight: dashboards on your data (serverless)
DocumentDB: Json-NoSQL DB (Aurora for MongoDB)
Amazon QLDB: Finacial Transaction Ledger
Amazon managed blockchain: Ethereum blockchain, Hyperledger fabric
Glue: Managed ETL (Extract Transform Load)
Database Migration: DMS
Neptune: Graph Database

Other Compute Services:
What is Docker ?
-Docker is a software development platform that allows you to run applications the same way,
regardless of where they are run. It can scale containers up and down within seconds.

ECS : Elastic Container Service
-Launch docker container on AWS
-need to provision infrastructure
-we create/manage the ec2 instances

Fargate:
-Launch docker containers in AWS
-serverless offering

-no need to provision infrastructure
-AWS runs containers based on CPU/RAM requirements

ECR: Elastic Container Resgistry
-Private docker registry in AWS
-Fargate creates container from images in ECR

Serverless:
  Just deploy code
  No need to provision servers or manage servers
  There are servers that End users dont have to manage.
  Example:
    S3, DynamoDB, Fargate, Lambda

Lamda:
-Serverless
-pay per calls
-pay per duration
-can run for a maximum duration of 15 mins
-Function as a Service (FaaS)
-Event driven
-Seamless scaling, reactive
-supports multiple programming language
-Invocation time: 15mins
 Use case:
  -Thumbnails creation
  -Serverless CRON job

Amazon API Gateway:
  -Build Serverless HTTP/S API
  -Client --> API Gateway --> Lambda --> DB
  -Supports security, user authentication, API throttling

AWS Batch:
  -Serverless
  -Efficeintly run 100,000s of computing batch jobs in AWS
  -it will dynamically launch EC2 instances or Spot instances

AWS Lightsail:
  People with little cloud experience
  To get started quickly with predictive pricing
  High availability but No autoscaling

Summary:
  Docker:
  ECS:
  Fargate:
  ECR:
  Batch:
  Lightsail:
  Lamda:
    -Serverless
    -BillingLanguage Support:
    -Invocation Time:
    -Use Cases:
    -API Gateway:

Deployments & Managing Infrastructure at Scale:

CloudFormation :

Declarative way of outlining the AWS infrastructure

Example within a Cloud formation you can have:
-a security group
-EC2 instances
-S3 bucket
-load balancer (ELB)

-Infrastructure as a code
-yaml format OR json format
-Easier cost analysis

Cloud formation stack designer : Gives a diagramatic presentation of architecture
stack template has to be created in us-east-1 (for the course)

AWS Cloud Development Kit (CDK)

Deploy Cloud as Infrastructure as a Code using programming language
-Java, Python, NodeJS
Then use CDK CLI to convert into a CloudFormation template (JSON/YAML)
This helps to use type safety in AWS

AWS Beanstalk:

-Developer centric view of Deploying apps on AWS
-Web 3 tier -> (ALB + ASG)
-Paas (Platform as a service)
-Free but pay for underlying resources

Can choose from different programming platforms
Application code can be uploaded
Behind the scenes, CloudFormation is used

Health Monitoring
Inbuilt inside beanstalk
Checks application health

AWS CodeDeploy:

Deploy applications automatically
Works with EC2 instances.
Works with On-Premises servers
Hybrid service
Server/Instances must be provisioned

AWS CodeCommit:

Similar to Github repository
Codes can be version controlled using codecommit

AWS CodeBuild:

Serlervess service Pulls from CodeCommit, Build and test the code
and make Ready-to-Deploy artifacts
Similar to Jenkins Build Tool
Pay for usage : time to build
It builds the code and stores the artifacts securely

AWS CodeArtifact:

AWS managed artifact management system

like maven central repository

AWS CodePipeline:
CICD pipeline
Automating the pipeline from code to Elastic Beanstalk
Continuous Delivery
Code->Build->Test->Provision->Deploy
Source: Github/CodeCommit
Build: CodeBuild/Jenkins
Testing: 3rd party tools
Deploy: CodeDeploy
Entire orchestration by CodePipeline

AWS Cloud9:
Development IDE in AWS

AWS CodeStar:
Unified UI to easily manage software development activities
Quick way to:
CodeCommit
CodeBuild
CodeDeploy
CloudFormation stack
Elastic Beanstalk
EC2

AWS Systems Manager (SSM)
Manage EC2, On-Premise infra on scale
Patch EC2 instances
Run commands across all servers

AWS System Manager(SSM)- Session Manager:
For secure shell on EC2 or on-prem servers

AWS OpsWork:
Managed Chef & Puppet
Works with EC2 & On-Premise VM
Server configuration

Global Infrastructure Section:
Why global ?
-Multiple geographies
-Multiple regions/Edge locations
-Decreased Latency
-Disaster Recovery plan
-Attack protection (Hacker)

Regions: For deploying applications & infra
Availability Zones: Made of multiple data centres
Edge Locations: Content delivery as close as possible
to users

Global apps:
Route 53: Global DNS
CloudFront: Global CDN(Content Delivery Network)
S3 Transfer acceleration

AWS Global Accelerator

Route 53:
Managed DNS service
Process flow:
Web Browser --->Makes DNS Request for that domain --> Route 53
<---Sends back IP address for that domain --

Web Browser --->Makes HTTP Request on that IP --> Application Server
<------HTTP Response----------
Host (Domain): myapp.mydomain.com
Record: hostname to IP

Routing Policies:
Simple Routing Policy : No Health Checks
Weighted Routing Policy: Based on priority assigned
Latency Routing Policy : Based on geographical location
Failover Routing Policy: Based on Primary & Failover server (Disaster Recovery)

Route 53 features are (non exhaustive list):
Domain Registration, DNS, Health Checks, Routing Policy

AWS CloudFront
Content Delivery Network (CDN)
Improves Read performance , content is cached at edge
DDOS protection -Integration with WAF and Shield
Use AWS Global Network
Which services does CloudFront integrate to protect against web attacks?
WAF & Shield

Caching done in S3 bucket
Cloudfront vs S3 Cross Region Replication
(Static content) (dynamic content)

S3 Transfer Acceleration:
Increase upload/download speed of file in S3 bucket
File is first uploaded in Edge location
Then File uploaded from Edge location to S3 bucket via AWS private net

AWS Global Accelerator:
Improve global application Availability
Client will connect to Edge location
Edge location will redirect to ALB
Use AWS Global Network
Integrate Shield for DDos Protection
Provides static IP address
Good fit for non-Http use cases

AWS Outposts:
Hybrid Cloud use cases
AWS will setup on premises infra
These servers will have preloaded AWS services
Client is responsible for physical security of the server
Benefits:
Fully managed services
Low latency
Data Residency (Privacy)

AWS Wavelength:
5G Datacentres
Ultra low latency to apps through 5G networks
deploy ultra-low latency applications to 5G devices
No Additional charges

AWS Local Zones:
Place AWS compute,storage services closer to end users
Local Zones are closer than AZs (Availability Zones)

Global Application architecture:
Multi Region, Active-Passive : Active(Read/Write), Passive(read)
Multi Region, Active-Active:

Cloud Integration Section
Application Communication
1. Synchronous Communication : Source service -> Destination service
2. Asynchronous/Event Based : Source -> Queue -> Destination
-SQS model
-SNS model

Amazon SQS:
Simple Queue Service
Producer/s -> SQS -> Consumer/s
Serverless service
Decouple application
Retention: upto to 14days
Messages deleted after read by Consumers

Amazon SNS:
Simple Notification Service
Send one message to many receivers
Pub/Sub model
No Retention of messages
we can have SNS topics
Publishers only sends message to 1 SNS topic
Subscribers can listen to that SNS topic notifications
subscriber to that topic will get all the messages

SNS subscribers can be:
Email, HTTP, HTTPS, AWS SQS, Lambda

Amazon Kinesis:
Real time Big Data streaming (Exam purpose)
Managed service to collect, process and analyze realtime
streamind data

Amazon MQ:
Messaging Queue
SNS,SQS are aws Proprietary protocols
Companies use Open source protocols (Apache active MQ)
Amazon MQ= managed Apache ActiveMQ
Not serverless

Cloud Monitoring Section:

Amazon CloudWatch metrics:
Monitor usages of aws services
Important metrics :
EC2 instances
EBS volumes
S3 Buckets
Billing (only available in us-east-1)
Service Limits
Custom Metrics

Amazon CloudWatch Alarms:
Trigger notification for any metric
Can be used to set up billing alarms to monitor estimated charges on your AWS account
Alarm action:
-Auto Scaling
-restart, stop a EC2 instance
-SNS notifications

Amazon CloudWatch Logs:
Can collect log from:
Elastic Beanstalk
ECS: collection from containers
AWS Lambda
CloudTrail
Route53
EC2 : (via CloudWatch Log agent)
On Premises : (via CloudWatch Log agent)
Enable Real time monitoring of logs
CloudWatch log agents : EC2 instances/on-prem servers

Amazon CloudWatch Events:
React to event happening within AWS infra services
Schedule Pattern: (Serverless Cron job)
Event Pattern : IAM user sign in event
Trigger : emails

Amazon EventBridge:
Next version of CloudWatch Events
Default event bus
Partner event bus

CloudWatch Events & EventBridge are used interchangibly

AWS CloudTrail:
Governance, Compliance, Audit of AWS account
Hisotry of events made within AWS account
Enabled by default
Event Types:
Management Events
Data Events
CloudTrail Insight Events (pay service)
-to detect unusual activities
Retention: 90 days

AWS X-Ray:

Debugging in Production
Useful for Microservice architecture apps
Visual analysis of Application
Are we meeting time SLA ?
Troubleshooting performance

Amazon CodeGuru:
Machine Learning service for Automated code review
CodeGuru reviewer:
-automated bugs finder in code, code review
-coding best pracices
CodeGuru Profiler:
-recommend application performance improvement

Supports Java & Python

AWS Status - Service Health Dashboard:
-UI to see service health of all AWS services
-Shows for all Regions

AWS Personal Health Dashboard:
-Alerts & recommendations about services you deployed
-For events that Affects you
-phd.aws.amazon.com/
-AWS outages that directly impacts you

Exam Alert:

You may see use-cases asking you to select one of CloudWatch vs CloudTrail vs Config. Just remember this thumb rule -
Think resource performance monitoring, events, and alerts; think CloudWatch.
Think account-specific activity and audit; think CloudTrail.
Think resource-specific change history, audit, and compliance; think Config.

VPC & Networking Section:

VPC & Subnets Primer:
VPC (Virtual Private Cloud) -
Region Level - across Multiple AZ
One Region can have multiple VPCs
Logically isolated section of the AWS Cloud

-Subnets - each for AZ
-Private Subnet (not accessible from Internet)
-Public Subnet (accessible from Internet)
Route tables - Define access to internet from Subnets
EC2 instances can be launched from Subnet

Internet Gateway:
Connects Public Subnet's EC2 instance to Internet

NAT Gateway:
Connects Private Subnet's EC2 instance to Internet

Network ACL and Security Groups:
-Network ACL (NACL):
Present at Subnet level

Firewall which controls traffic from and to the subnet
Can have ALLOW and DENY rules
Stateless

-Security Groups:
Present at EC2 instance level
Firewall which controls traffic from and to EC2 instances
Can only have ALLOW rules
Stateful

VPC Flow Logs:
logs network traffic logs
logs can be exported to CloudWatch logs

VPC Peering:
Connect 2 VPC privately using AWS network
IP address range donot overlap

VPC Endpoints:
To connect to AWS services using a private network instead of the public network
For Enhanced Security of AWS services
Two types
-VPC Endpoint Gateway (For S3 and DynamoDB)
-VPC Enpoint Interface (For rest)

Hybrid Cloud - When Client has to connect On-premise resources to Cloud resources:

Direct Connect: (DX)
-Hybrid Cloud use case
-Goes over private network
-Establish a physical connection
-Takes Time to setup

Site to Site VPN:
-Hybrid Cloud case
-Goes over Public Internet
-Connect on-premise VPN to AWS
-Faster setup
-Customer Gateway(on prem) --> Virtual Private Gateway (AWS)

Transit Gateway:
Connect hundreds/thousands of VPC with on-premise data centers

For Exam:
VPC, Subnets, Internet Gateways, NAT Gateways
Security Groups, Network ACLs, VPC Flow
VPC Peering, VPC Endpoints
Site to Site VPN, Direct Connect
Transit Gateway

IP range, CIDR range

Summary:
VPC: Virtual Private Cloud
Subnets: Tied to AZs, network partition of the VPC
Internet Gateway: at VPC level, provide internet access
NAT Gateway: at subnet level, gives internet access to

private subnets
NACL: Stateless subnet rules for inbound/outbound traffics
Security Groups: Stateful, operates at EC2 level
VPC Peering: Connects 2 VPCs with non-overlapping IP ranges
VPC Endpoints: Provides private access to AWS Services within VPC (DynamoDB,S3)
VPC Flow Logs: network traffic logs
Site-to-Site VPN: VPN over public internet between on-premises & AWS
Direct Connect: direct physical private network btw on-prem & AWS
Transit Gateway: Connect hundreds of VPCs and your on-premises data centers together

Security & Compliance Section

AWS Shared Responsibility Model:
AWS:
Security of the Cloud
Protecting Infrastructure
Managed services like S3, DynamoDB, RDS etc.
User:
Security IN the cloud
For EC2 instances - OS update/patches, firewall
Encryption of app data

For RDS:
AWS responsibility:
Manage underlying EC2 instance
Automate DB patching , OS patching
Audit underlying instance
User responsibility:
Security group
DB encryption setting

For S3:
AWS responsibility:
-Unlimited storage
-encryption
-data privacy
User responsibility:
-Bucket configuration
-Bucket policy
-IAM user and roles
-enabling encryption

DDOS protection:
Distributed Denial of Services

-Amazon Shield Standard:
It is activated on all AWS services by default

Shield Standard with CloudFront and Route 53:
-provides attack mitigation at edge
-you receive comprehensive availability protection against all known infrastructure (Layer 3 and 4) attacks.

-Amazon Shield Advanced (Premium)
It covers the below services:
EC2, Elastic Load Balancing, CloudFront, Global Accelerator, Route 53
Provides Protection to Network layer (L3), Transport Layer (L4), Application Layer (L7)

-Amazon WAF: (Web Application Firewall)
Monitors web requests forwarded to below services.
CloudFront, API Gateway, Application Load Balancers
Charges for Number of Web requests received and number of Web ACL created

WAF checks for the presence of malicious SQL code in requests (SQL Injection)
WAF can block ALL requests except the one you specify

-Leverage Auto scaling under attack

Penetration Testing
Without prior approval from AWS customers can
carry out security assessment of certain services

Cannot Perform DDoS attack on AWS services

Encryption:
Encryption of Data at Rest vs Data in Transit
Rest: S3, EFs, EBS
Transit: Data transferred over network

AWS KMS (Key Management Service):
-for encrypting data in various AWS services
-we don't have access to keys
-AWS manages the keys

Default Encrypted services:
-CloudTrail Logs
-Glacier
-Storage Gateway

Encryption opt-in services:
-S3 bucket
-EFS
-EBS
-RDS
-Redshift

AWS CloudHSM:
-AWS provisions Hardware encryption
-End user manages the encryption keys

Customer Master keys (CMK)
Customer Managed CMK:
-Created, managed and used by Customer
AWS managed CMK
-Created managed used by AWS on customer's behalf
-End users don't have access to it
AWS owned CMK
-AWS owns the keys , customer can't see the keys
-End users dont' have access to view it
CloudHSM keys (custom keystore)
-Keys generated from you own CloudHSM hardware

AWS Certificate Manager (ACM):
- -SSL/TLS Certificate (provision, manage and deployed by AWS)
- -In flight encryption (HTTPS endpoints)

AWS Secret Manager:
- -Rotation of secrets every X days
- -Integration with Amazon RDS
- -Secrets will be encrypted using KMS

AWS Artifact:
- -Provides customer with AWS compliance and agreements
- -Artifact Agreements (HIIPA, BIA)
- -Account agreements, Organization agreements

AWS GuardDuty:
- -Use to Protect AWS account using ML algorithms
- -Can be integrated with CloudTrail
- -threat detection service that continuously monitors for malicious activity

AWS Inspector:
- -Automate Security Assessments on EC2 instances
- -Analyze running OS vulnerability against known threats
- -Track configuration changes

AWS Config:
- -Recording configuration changes
- -For Auditing and Recording compliance of AWS resources
- -Store the config data in S3 buckets (analyze by Athena)
- -Integrate with SNS topic

AWS Macie:
- -Fully managed data security and data privacy service
- -Uses ML and pattern matching to discover and protect sensitive data & Intellectual Property & Peronally Identifiable Information (PII)
- -Can be used to identify sensitive data in S3 bucket

AWS Security Hub:
- -Central Security Tool
- -Manage security across several AWS accounts
- -Integrated Dashboard
- -Enable AWS config
- -Analyzes data from : Macie, GuardDuty, Inspector, Firewall Manager , System Manager

AWS Detective:
- -Invesigate logs from AWS Security Hub
- -Root cause analysis

AWS Abuse:
- -Report suspected/illegal activites to AWS abuse mail
- -abuse@amazonaws.com

Root User Privileges:
-Account Owner
-Has complete access to all AWS resources
-Actions by Root user:

-Change account settings
-Close AWS account
-Change or Cancel AWS Support plan
-Register as a Seller in Amazon Marketplace in Reserved Instance Marketplace

Summary:
Shared Responsibility Model on AWS
Sheild: DDos Protection
WAF:
-Firewall for web applications
KMS:
-Encryption keys managed by AWS
CloudHSM:
-Handware encryption, customer manager encryption keys
AWS Certificate Manager:
-for SSL/TLS certificates
Aritifact:
-Get access to compliance reports (PCI,ISO)
GuardDuty:
-Find malicious behavior with CloudTrail logs
Inspector: (for EC2 only)
-Find vulnerability within EC2 instance
Config:
-Track config changes and compliance against rules
Macie:
-Find sesnitive data (Intellectual Property) in S3 bucket
CloudTrail:
-Track API calls made by users within account
AWS Security Hub:
-Gather security findings accross multiple AWS accounts
Amazon Detective:
-find root cause of security issues
AWS Abuse:
-report illegal AWS usages
Root User Privileges:
-Change account settings
-Close AWS account
-Change or Cancel AWS Support plan
-Register as a Seller in Amazon Marketplace

Machine Learning Section:

Amazon Rekognition:
Facial Recogtition
Object recognition
Content moderation
Text detection

Amazon Transcribe:
Converts Speech to Text
Subtitles generation

Amazon Polly:
Converts Text to Speech

Amazon Translate:
natural and accurate language translation

Amazon Lex:
Automatic Speech Recognition (ASR) to convert speech to text
Recognize intent of the speech
Same tech that powers Alexa

Amazon Connect:
Virtual Contact Centre (Call centre)

Use case:
Phone call -> Connect -> Lex -> Lamda -> CRM DB

Amazon Comprehend:
Natural Language Processing
identify language of text
Sentiment analysis

Amazon SageMaker:
Fully managed service to Build ML models
For developers/Scientist

Amazon Forcast:
Uses ML to predict forcasting models
Future forcast, Future financial planning

Amazon Kendra:
Document search service powered by Machine Learning

Amazon Personalize:
Real time Personalize recommendation service
Personalize product recommendation

Summary:
Rekognition: face detection, celbrity recognition
Transcribe: audio to text (subtitles)
Polly: text to audio
Translate: translations
Lex: conversational bots
Connect: cloud contact centres
Comprehend: natural language processing
SageMaker: build ML models
Forecast: make highly accurate forcasts
Kendra: ML-pwered search engine
Personalize: personalized recommendations

Account Management , Billing and Support:

AWS Organizations:
Global Service
Main account is master account
Manage multiple AWS accounts
Cost Benefits:
-Consolidated Billing - single payment
-Aggregated usage - discounts

-Pooling of reserved instances
Automate AWS account creation
Restrict account privileges using SCP

Multi Account Strategies:
Organizations Units (OU)
-Business Unit
-Environment Lifecycle

Root OU (Master account)
-> Dev OU (Account A)
-> Prod OU (Account B)
-> Finance OU (Account C)
-> HR OU (Account D)

Service Control Policies (SCP)
-doesnot apply to Master Account
-Applied to OU levels
-Whitelist or Blacklist IAM Actions

AWS Organization: Consolidating Billing
-Combined Usages : share volume pricing, share Reserved Instances
-One Bill

AWS Control Tower:
setup and manage AWS organizations automatically
No pay for Control tower -pay for underlying resources
Get complaint info about the accounts
Has a SSO

Pricing Models in AWS Cloud:
-Pay as you Go
Start, Delete resources when necessary

-Save when you reserve
Reservations are available for
EC2 Reserved Instances,
DynamoDB Reserved Capacity,
ElastiCache Reserved Nodes,
RDS Reserved Instance,
Redshift Reserved Nodes

-Pay less by using more
Volume based discounts

-Pay less as AWS grows
Discounts as AWS expands in market

Always Free Services in AWS:
IAM
VPC
Consolidated Biling
Elastic Beanstalk
CloudFormation
Auto Scaling Group

Compute Pricing - EC2 :

On demand instances
-Minimum billing time: 60s
-Linux: pay per second
-Windows: pay per hour
Reserved instances:
-75% compared to On demand
-1 or 3 year commitment
Spot instances:
-90% discount compared to On-demand
-Bid for unused capacity
Dedicated hosts:
-On demand
-1 or 3 years commitment
AWS Savings Plan

Compute Pricing - Lambds & ECS:
Lambda: Pay per call & per duration
ECS: Pay for underlying EC2 instances
Fargate: Pay for vCPU and memory allocated

Storage Pricing : S3
Pay as per Storage class
Number and size of objects
Number and Type of Request in/out of S3
Data Transfer OUT of the S3 region
Number and type of requests
S3 Transfer Acceleration
Lifecycle transition

Same applies for EFS

Storage Pricing: EBS
Storage volume in GB per month as provisioned
Data transfer OUT of EBS
Snapshots : cost per GB per month

Database Pricing - RDS
Per hour biling
Database charecteristics
Purchase type: On demand/Reserved type
Backup Storage
Additional Storage (per GB per month)
Number of requests (input/output) per month
Deployment type (Single AZ/Multi AZ)
Data Transfer: OUT of RDS

Content Delivery - CloudFront
Since Global service - pricing different for each regions
Aggregated bill- more usage more discounts
Pay for Data transfer OUT
Number of HTTP/HTTPS requests

Networking Costs in AWS per GB
-Free traffic IN to EC2 instance (AZ1)
-Free traffic EC2 - EC2 within same AZ
-EC2 - EC2 across Inter-AZs via private IP ($0.01) , via Public IP ($0.02)
-EC2 - EC2 across Inter-region ($0.02)

-Use Private IP instead of Public IP for good savings and better network performance
-Use same AZ for maximum cost savings (trade-off with high availability)

AWS Savings Plan:
Commit $ for per hour or 1/3 years

EC2 Savings Plan:
-72% savings compared to On demand
-Commit instance family, region
-regardless of AZ, size , OS

Compute Savings Plan:
-66% discounts compared to On-demand
-Compute Options: EC2, Fargate, Lambda
-Can change EC2 instance family, size, AZ, OS , region

Setup savings plan in AWS Cost Explorer Console

AWS Compute Optimizer:
-Reduce costs and Improve performance
-by recommending optimal AWS resources
-EC2, Auto Scaling Groups, EBS, Lambda

Billing and Costing Tools:

Estimating costs:
-TCO Calculator
-Simple Monthly Calculator/ AWS Pricing Calculator

Tracking Costs:
-Billing Dashboards
-Cost Allocation Tags
-Cost and Usage Reports
-AWS Cost Explorer

Monitoring against Cost Plans:
-Billing Alarms
-AWS Budgets

Estimating Cost---------

AWS TCO (Total Cost of Ownership):
Estimate Cost savings when using AWS
Compare cost of application in on-premise to AWS based on:
Server, Storage, Network, IT Labor

AWS Pricing Calculator/Simply Monthly Calculator
-Replaced by AWS Pricing Calculator
-Cost of an actual architecture solution
-It tells you Total monthly most and Upfront cost(1/3 years)

Tracking Cost-------

AWS Billing Dashboard:
-Higher level overview

-Shows cost spend for the current month
-Shows spends per service

Cost Allocation Tags:
-To get cost by category
-AWS generated tags
-User defined tags

Tags and Resource Groups:
-Resources can be Tagged
-Resource Groups can have multiple Tags

Cost and Usage Report:
-most detailed report
-most granular cost usage reports (hoursly/Daily)

AWS Cost Explorer:
-choose an optimal Savings Plan
-Forcast usage upto 12 months based on previous uasage

Monitoring Cost----------

Biling Alarms
Billing Data is stored in CloudWatch in us-east-1
Billing data are for overall AWS regions

AWS Budgets:
Create Budget Send alarm when costs exceeds the budget
Can send 5 SNS notifications
2 Budgets are free then $0.02/Bday/Budget
3 types: Usage, Cost, Reservation
Can filter by Service

AWS Trusted Advisor:
Analyze your AWS account and provided recommendation
Identifies low utilization of EC2 resources
based on 5 categories:
-Cost Optimization
-Performance
-Security
-Fault Tolerance
-Service Limits

Basic and Developer support plan get access to 7 Core Trusted advisor checks .
-S3 Bucket permission
-Security Groups
-IAM Permission
-MFA on Root Account
-EBS Public snapshots
-RDS Public Snapshots
-Service Limits

Business and Enterprise support plans have Full access to Trusted advisor checks
-Important to know check
:Programmatic Access to AWS Support API

AWS Support Plans:

Basic Support: (incl for all AWS accounts)

Developer Support:
+ Basic Support Plan
Business hours email access to Cloud Support Associates
Unlimited Cases/1 contact
Architectural Guidance: General
Case Severity:
General Guidance < 24 business hours
System Impaired < 12 business hours

Business Support:
(for production workload)
+ Developer Support Plan
24*7 phone/chat/email access to Cloud Support Engineers
Programmatic access - AWS Support API
Unlimited cases/Unlimited contacts
Architectural Guidance:
Guidance to contextual use cases
Infrastructure Event Management (addtn fee)
Case Severity:
General Guidance < 24 business hours
System Impaired < 12 business hours
Production System Impaired < 4hrs
Production System Down < 1hr

Enterprise On-Ramp:
+ Business Support plan features
Pool of TAM
Conceirge Support Team
Consultatie review and guidance based on apps
Infrastructure Event Management (incl)
Architectural Guidance:
Consultative review Based on your applications
Case Severity/Response Time:
+ Same as Business Plan
Business Critical systems down: < 30 mins

Enterprise Support:
+ Business Support plan features
Designated TAM
Conceirge Support team
Infrastructure Event Management
Well Architected & Operational Reviews
Architectural Guidance:
Consultative review Based on your applications
Case Severity/Response Time:
+ Same as Business Plan
Business Critical systems down: <15 mins

Account Best Practices - Summary:
Use AWS Organizations
Use SCP to restrict account power
Easy setup for multiple accounts - AWS Control Tower
Use Tags, & Cost Allocation Tags
IAM guidelines
AWS Config - compliance and audit trail

CloudFormation to deploy stacks across regions
AWS Trusted Advisor for account recommendation
CloudTrail - record all API calls within the account
If AWS account compromised:
change root password,
rotate all password ,
contact AWS support

Billing - Summary
AWS Compute Optimizer
AWS TCO
AWS Pricing calculator
Billing Dashbaord
COst Allocation tags
AWS Cost and Usage reports
AWS Cost explorer
Billing Alarms
AWS Budgets
AWS Savings Plans

Advanced Identity:

AWS Security Token Service (STS):
-Create temporary, limited privileges credentials
to access AWS resources
-Same concept as Oauth token identification

Amazon Cognito
-Identify your Web and Mobile app users
-millions of users
-Login with Google/Facebook
-lets you add user sign-up, sign-in, and access control
to your web and mobile apps quickly and easily.

Directory Services:
Integrate Microsoft Active Directory in AWS
Centralized storage of Username/password

AWS Directory Services:
-AWS Managed Microsoft AD
-AD connector (Proxy)
-Simple AD (managed AWS active directory)

AWS SSO (single sign on):
Integrated with AWS organizations
Can be integrated with on prem Active Directory
Manage multiple AWS accounts and other Business applications

Summary:
IAM: Identity and Access management within AWS account
Organizations: manage multiple AWS accounts
STS:
Cognito:
Directory Services:
Single Sign On(SSO):

Other Services:

Amazon WorkSpaces:
Alternate to VDI (Virtual Desktop Infrastructure)
Pay as you go, Hourly rates

Amazon AppSream 2.0:
Desktop Applciation streaming service
Stream any particular app
No need to connect via VDI

Amazon Sumerian:
Virtual Reality (VR)
Augmented Relaity (AR)

AWS IoT Core:
Internet Of Things
Allows IoT device to connect to AWS cloud

Amazon Elastic Transcoder:
Converts Media Files in s3 bucket TO
Media Files in formats requried by playback devices

AWS Device Farm:
Run tests concurrently on multiple devices
Fully managed service that tests web and mobile apps
To tests application on multiple devices

AWS Backup:
Cross region backup
Cross account backup
Centrally automate Backup of AWS services

Disaster Recovery Strategies:
-Cheapest Strategy $: Backup and restore

-Core functions available, Minimal setup, ready to scale $$:
Pilot Light

-Full version of the app, but at Minimum size $$$:
Warm Standby

-Full Version of the app, at full size: Most expensive $$$$
Multi-Site/Hot-Site

CloudEndure Disaster Recovery:
Protect most critical Databases
Use CloudEndure services to backup your physical servers to AWS cloud
It creates a backup of on-premise/Any Cloud infra in AWS Cloud (Staging area)
When there is a Failure in Existing on-prem infra, the AWS Cloud backup converts into a Production scale infra
When the Failure is mitigated the AWS Cloud infra becomes Secondary and hands ove control to On-premise infra

AWS DataSync:
Move large amount of data from on premises to AWS Cloud

Replication tasks are incremental after the first load

AWS Fault Injection Simluator:
Chaos Engineering
Observing application performance by creating a disruption

AWS Architecting & Ecosystems:

General Guiding Principals:
Stop guessing capacity
Test system at production scale
Drive architecture using data
Simulate applications for Flash sale days

Design Principles - Best Practices :
Scalability:
Disposable Resources:
Automation:
Loose Coupling:
Think Services, not Servers:

Well Architected Framework:
1. Operational Execellence
2. Security
3. Reliability
4. Performance Efficiency
5. Cost Optimization

1. Operational Execellence:
-Perform Operations as a Code - Infrastructure as a Code
-Annotate Documentation
-Make frequent small reversible changes
-Refine operations procedures frequently
-Anticipate failures
-Learn from all failures

Services Backbone:
AWS CloudFormation

2. Security:
-Implement a strong Identity
-Enable tracebility
-Apply security at all layers
-Automate security best practices
-Protect data in transit and rest
-Keep people away from data
-Prepare for security events

Services Backbone:
IAM, AWS Organizations
AWS Config, AWS CloudTrail, AWS CloudWatch
AWS Shield, AWS WAF , AWS Inspector
KMS

3. Reliability:
-Test recovery procedures

-Automatically recover from failures
-Scale horizantally to increase availability
-Stop guessing capacity
-Manage change in automation

Services Backbone:
IAM, Amzon VPC , AWS Trusted Advisor
Auto Scaling

4. Performance Efficiency:
-Use advanced technology
-Go global in minutes
-Use serverless architecture
-Experiment more often
-Be aware of all AWS services

Services Backbone:
Auto Scaling, AWS CloudFormation
CloudWatch

5. Cost Optimization:
-Adopt consumption model - Pay only for what u use
-Measure overall efficiency
-Stop spending money on data centre operations
-Analyze and attribute expenditure
-Use managed and application level services to reduce cost of ownership

Services Backbone:
AWS Lambda , Fargate , Beanstalk
AWS Budgets, AWS Cost and Usage Reports, AWS Cost Explorer
Spot Instances, Reserved Instances
Auto Scaling, AWS Trusted Advisor

AWS Well Architected Tool:
Review your architecture
Adopt best architectural practices
Free to use
Define a workload and it Reviews the architecture against AWS 5 pillars of Well architected tool

AWS Right Sizing:
Scaling UP is easy so Start SMALL
Tools: CloudWatch, Cost Explorer
Trusted Advisor

AWS Ecosystems:
Free resources:
AWS Blogs
AWS Forums
AWS Whitepapers

AWS QuickStarts:
-Automated Gold standard deployment in Cloud

AWS Solutions:

AWS Support: (Basic, Developer,Business, Enterprise)
AWS Marketplace:
AWS Training:

AWS Professional Services & Partner network
-Global team of experts
-Chosen member of APN

APN Technology Partner:
-Provides Hardware, connectivity and software

APN Consulting Partner:
-Professional service to migrate/build on AWS cloud

APN Training Partner :
-Who can help you learn on AWS

AWS Competency Programs:
-Partners who demostrate technical proficiency

AWS Navigate Program:
-Help partners become better at their game

AWS Knowledge Centre:
Troubleshooting on various services
Best practices and Documentation

Serverless Services in AWS:

Compute:
-AWS Lambda
-AWS Fargate

Application Integration:
-EventBridge
-Step Function
-SQS
-SNS
-Amazon API Gateway
-AppSync

Data Store:
-Amazon S3
-Amazon DynamoDB
-Amazon RDS proxy
-Amazon Aurora Serverless

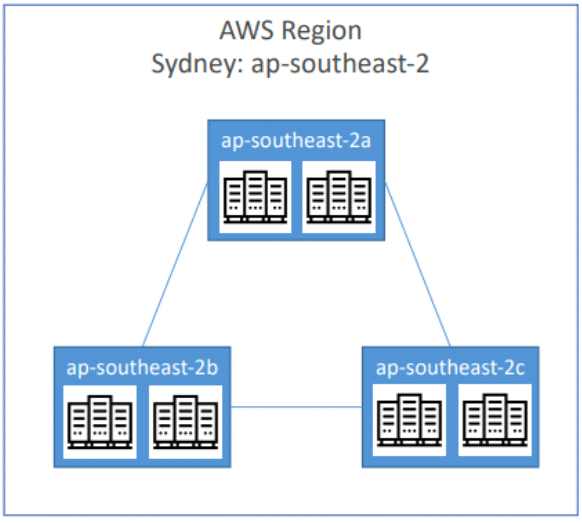
IAM & AWS CLI

09 January 2023 13:15

AWS Regions and Availability Zones:

AWS Region can have min 3 and maximum 6 Availability Zones (AZ).
AZs are where datacentres are kept.
Each AZ can have 1 or more datacentres inside it.
Each AZ is separated from each other, and have redundant power, networking capabilities.
Any issues in one AZ will not cascade into the other.
All the AZs are connected with each other using high bandwith low latency network, so that they behave as a single region.

Example:



IAM: Identity & Access Management - Global service
Root account is created by default - not to be shared

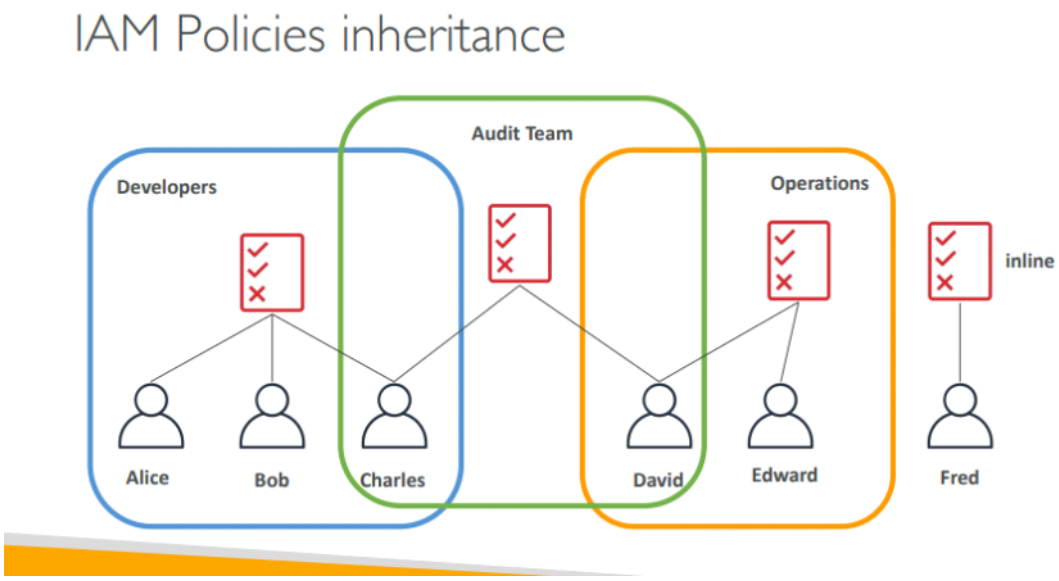
We should create different IAM users, which can be grouped in User Groups for daily activities

Users / Groups can be linked to IAM permissions
IAM permissions are developed through Policies

Users login:
https://ashutosh-root-aws.signin.aws.amazon.com/console

IAM Policies:

Policy inheritance:



Policies can be attached to a Group. One user can belong to multiple group.
In that case that User will inherit policy from those groups.

Policy can be created by Users.
Policies can be attached as 'in-line policy' to Users.

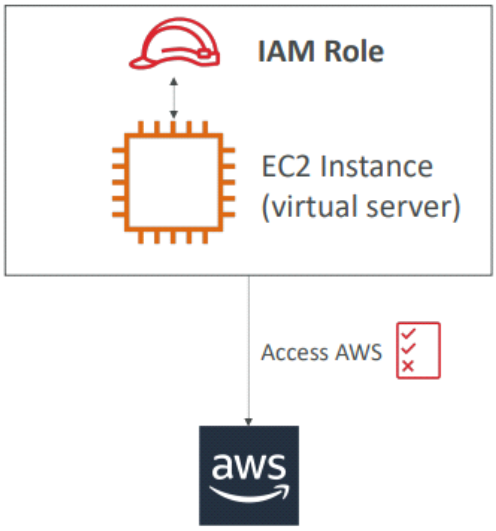
Policy Structure (JSON):

```
{
        "verison" :
        "id":
        "Statement" : {
                "Sid" :
                "Effect" :
                "Principal" : {
                        "AWS" : [ … ]
                                },
                "Action" : [ .. ],
                "Resource" : [ … ],
                }
}
```

IAM Roles for AWS services:

Some AWS service will perform functions on your behalf.
To do so, we assign **permissions** to AWS services, with **IAM Roles.**

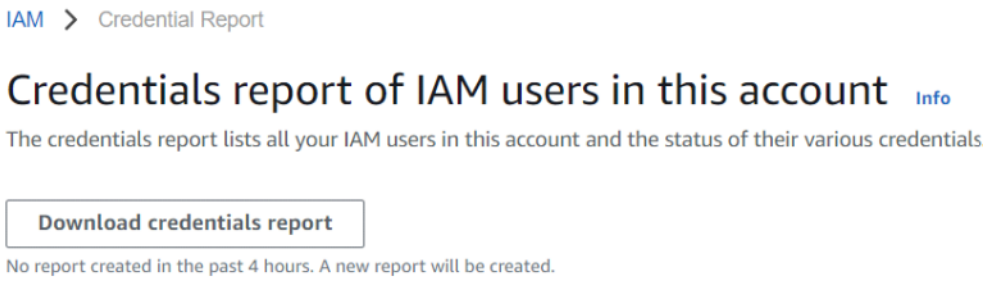
Example: We are using a EC2 instance to connect to our AWS.
EC2 instance needs some IAM Roles to get the permission to access the AWS.
ex: **DemoRoleForEC2** (policy: IAMReadOnlyAccess)
Those are IAM Roles for AWS services.



IAM Security Tool:

These reports can also be used for Audit purposes.

IAM Credentials Report - account level
-list all users of the account
-status of their credentials



IAM Access Advisor - User level
-shows service permission granted to the user
-used to revise the policies

Users > aws_dev_1

Summary

User ARN	arn:aws:iam::874263642285:user/aws_dev_1
Path	/
Creation time	2023-01-09 14:05 UTC+0530

Permissions | Groups (1) | Tags (1) | Security credentials | Access Advisor

Access Advisor shows the services that this user can access and when those services were last accessed. Review this data to remove unused permissions. Learn

Allowed services (346)

Access Advisor reports activity for services and EC2, IAM, Lambda, and S3 management actions. To view actions, choose the service name from the list. Recent se
the past 400 days. Learn More

Last accessed information is available for EC2, IAM, Lambda, and S3 management actions.

Search | No Filter

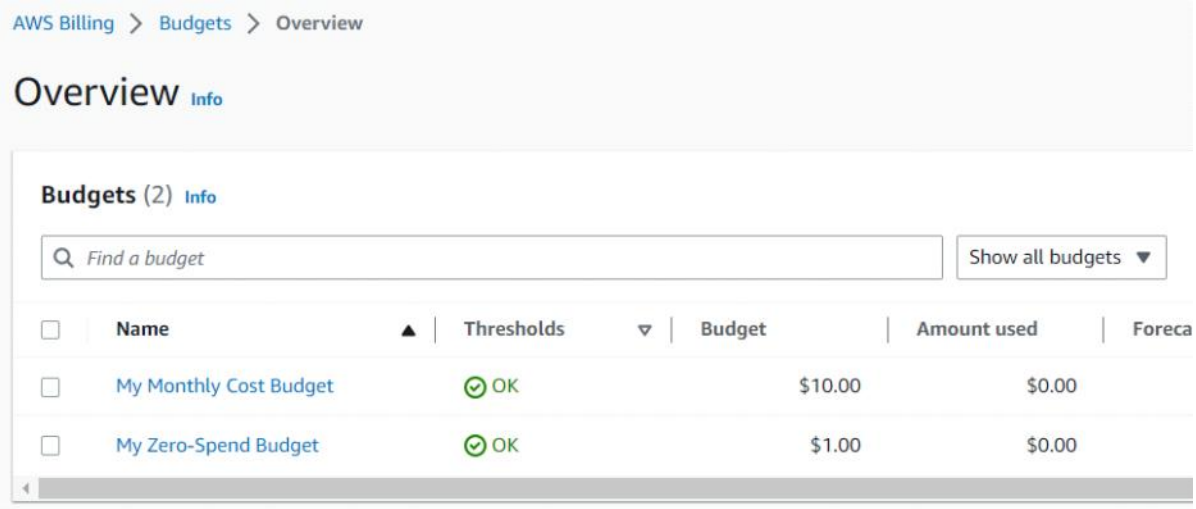
Service	Policies granting permissions	Last accessed
AWS Identity and Access Management	AdministratorAccess	Today
AWS Health APIs and Notifications	AdministratorAccess	Yesterday
Amazon EC2	AdministratorAccess	Yesterday
AWS Cost Explorer Service	AdministratorAccess	2 days ago

EC2 Fundamentals

12 January 2023 01:57

AWS Budget Setup:

We need to approve the Billing Dashboard permission for IAM users from Root account.
In the AWS Budget section we can create various budgets according to our requirement.



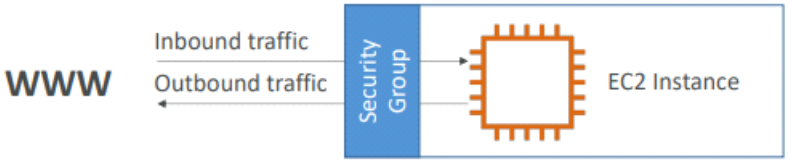
EC2 Basics:

-Elastic Compute Cloud
-Infrastructure as a Service (IaaS)
-Virtual server in a the cloud

-Consists of:
  -Renting virtual machines (EC2)
  -Storing data on virtual drives (EBS)
  -Distributing Load across machines (ELB)
  -Scaling the services using auto-scaling (ASG)

Security Groups:

Security Groups only contain ALLOW rules.



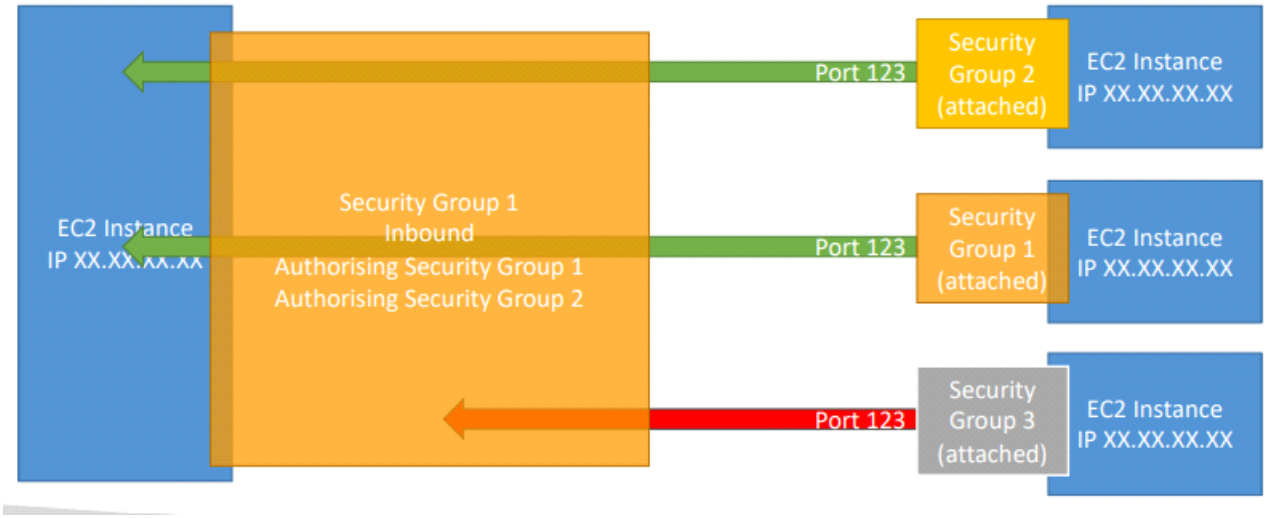
They control how traffic is allowed into or out of the EC2 instance

-Can be attached to multiple EC2 instances
-Locked to a Region
-If application is not accessible ("timed out") then, it's a sceurity group issue
-If application gives "connection refused" error, then security group is working, app is not working
-All **INBOUND** traffic is **blocked** by default
-All **OUTBOUND** traffic is **authorized** by default.

Referencing other security Groups:

We have a EC2-0 instance which has the following Security Group (Inbound)
-Authorising Security Group 1
-Authorising Security Group 2

Now, Security Group 1 is attached to EC2-a , Security Group 2 is attached to EC2-b
So, both EC2-a & EC2-b can access to EC2-0 instance.



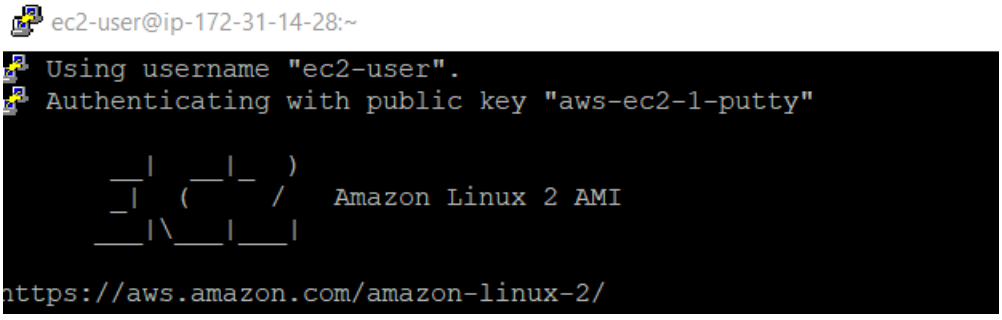
Classic Ports to know:

22 -> SSH (Secure Shell Host) : log into a Linux instance
21 -> FTP (File transfer protocol)
22 -> SFTP (Secured FTP)
80 -> Unsecured Websites (Http)
443 -> Secured Websites (Https)
3389 -> RDP (Remote Desktop Protocol) : log into an Windows instance

SSH into EC2 instance:

Putty:
Hostname: ec2-user@{**Public IPv4 address**}
example: Hostname: ec2-user@65.2.57.216

In SSH->Auth->Credentials
Load the ppk file into Private Key



EC2 instance Purchasing options:

TCP UDP HTTP HTTPS

04 February 2023 14:11

Network protocols brings in a set of rules and guidelines for communication between two devices.
It makes sure both the devices is communicating with each other in a compatible language.

Network Protocols :

- Internet Protocols
  - TCP
  - UDP
  - HTTP
  - SSL
  - TLS
- Wireless Network Protocols
  - WiFi
  - LTE
  - Bluetooth
- Routing Protocols
  - Decides which is the fastest path to download a file

TCP : Transmission Control Protocol

The protocol for communication between 2 computers over a network within a defined session.
Source sends a SYN command.
Dest sends a ACK response
Source sends a ACK Received command.

UDP: User Datagram Protocol

This protocol is used for communication between 2 computers but without creating a session.
Also known as fire and forget method.

HTTP: Hyper Text Transfer Protocol
This protocol sends data in simple text from Sender's computer to the Web Server.

HTTP: Secure HTTP
This protocol encrypts the data which being sent from Soruce to Destinaton computer.
It secures the communication using the below protocols:

- SSL: Secure Sockets Layer.
  - An SSL certificate is used to authenticate the identity of a website

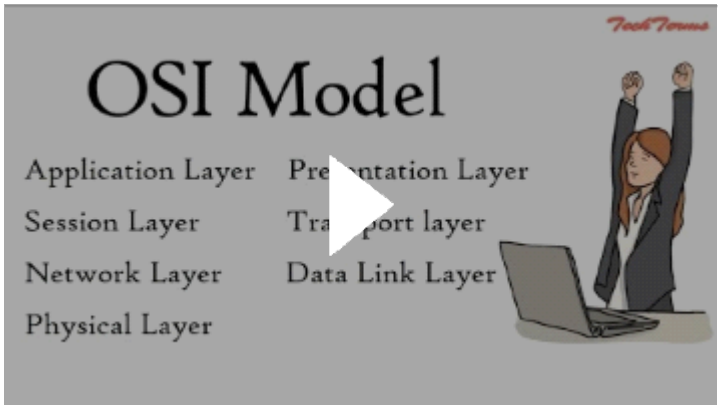
- TLS: Transport Layer Security
  - The latest industry standard for cryptographic protocol
  - It's a successor to SSL
  - Authenticates the server, client and encrypts the data

OSI Model (7 Layers)

05 February 2023 01:47

Layer 7: Application layer
Layer 6: Presentation layer
Layer 5: Session Layer
Layer 4: Transport Layer
Layer 3: Network Layer
Layer 2: Data Link Layer
Layer 1: Physical layer

[OSI Model Explained | OSI Animation | Open System Interconnection Model | OSI 7 layers | TechTerms]



Layer 7: Application Layer

Application Layer Protocols are used by Network applications for communication.
Network services such as:

- File Transfer : FTP (File Transfer protocol)
- Web Surfing: HTTP/S (Hyper Text Transfer Protocol Secure)
- Emails: SMTP (Simple Message Transfer Protocol), POP3, IMAP
- Virtual Terminals: TelNet

Layer 6: Presentation Layer:

- Translation
- Compression
- Encryption

Layer 5: Session Layer

- Authentication
- Authorization

Layer 4: Transport Layer

- Connection Oriented transmission : TCP (Transmission Control Protocol)
- Connection-less transmission : UDP(User Datagram Protocol)
- TCP is used for Emails, File transfer
- UDP is used for Online Movie streaming, VoIP, Video streaming