AWS Technical Essentials – Day 1 (1 October 2025)

2-day AWS Technical Essentials

Instructor Yuen San

Day #1

-IAM

-Compute, server and serverless

-Storage, object-level and block-level storage

-Database, RDS and DynamoDB

-Cloud Economics

-Elastic load balancing

-Resilience Availability

-Monitoring, scaling and load balancing

History of Amazon Web Services

-Amazon started an ecommerce platform, attracted interest of M&S

-Breakdown merchant platform into components

-Lazada-like platform created (Amazon)

Benefits of cloud computing

-Need unlimited storage/bandwidth

-Private cloud, e.g. database

-GTM (Go To Market) faster enables companies to capture larger market share.

-ROI (Return On Investment) KPI for datacentres

-Shifting to cloud is not cheap

-TCO (Total Cost of Ownership)

-Rapid scaling required, use Cloud

AWS Technical Essentials – Day 1 (1 October 2025)

-Eg. Netflix streaming uses CloudFront >8000 datacentres (Edge locations) around the world

-Going global in minutes

-Pay as you go

Breadth of AWS Services

-Application (Virtual desktops, Collaboration/sharing)

AWS Global Infrastructure

-AWS Regions

New regional datacentres are announced every year.

-Latency sensitivity (how close the resource needs to be to users)

-Alexa assistant service only available in US.

-Availability zones are clusters of databases (3 az in Singapore)

-Edge locations store cache of image files in worldwide locations

Security is a shared responsibility of AWS and customer

AWS does not protect data or application

EC2 is a virtual machine

Lambda is a serverless compute service

AWS SLA is available in AWS Artifacts

Cloud native apps are apps built

AWS Technical Essentials – Day 1 (1 October 2025)

AWS Identity and Access Management (IAM)

Permission is given by the root user by policies.

Policies are written in JSON format

Policies are allowed to start and stop EC2 instances, unable to create.

Best practice is to follow the security of least privilege.

4 key concepts,

Create Role, do not need to add Admin and Developer to Group

Role has permission policy, but no associated credentials (i.e. ID and PW)

Assume role > provide account ID and

Principle of least privilege

Lab #1

https://991474125288.signin.aws.amazon.com/console

Lab #2

Lab #3

Lab #4

AWS Technical Essentials – Day 1 (1 October 2025)

3 Evaluations - Day #2

2 Assessments - Day #2

Compute lesson

Compute includes management and

Public AMI (Amazon Machine Image) versus private AMI

EC2 Instance Types

-General purpose (e.g. Bursty apps)

-Compute optimized

-Memory optimized

-Accelerated computing

-Storage optimized

EC2 pricing

-AWS Free Tier

-Savings Plan

-Dedicated Instance

-Dedicated Hosts

-On-Demand Instances

-Reserved Instances

-Spot Instances

When terminating EC2, storage is not deleted.

Spot Instances is useful for batch analytics

-e.g. analyzing DNA sequences

AWS Technical Essentials – Day 1 (1 October 2025)

1. CPU/Memory
2. Storage capacity
3. Storage IOps
4. Bandwidth

Load balancing of Containers

1. Amazon ECS (Elastic Container)
2. Amazon EKS (Elastic Kubernetes Server)

Serverless Compute

-AWS Fargate

-AWS Lambda

Use DNS to load balance traffic to instances.

For example, for private ride app, use Lambda to handle request, rather than a continuous running server.

Limitation of Lambda is 15 minutes.

Fargate does not have 15-minute limitation.

Choose between Fargate only or Fargate and EC2

Network Lesson

AWS Technical Essentials – Day 1 (1 October 2025)

Amazon VPC (Virtual Private Cloud) and subnets

-Private IP addresses are not Internet routable

-Only Public IP address can be routed

VPC (10.0.0.0/16) gives 65,536 unique IP addresses.

VPC (10.0.0.0/28)

3 types of gateway

-Internet gateway, attached to VPC (Virtual Private Cloud)

-Virtual Private gateway, used to enter on-prem datacentre, using VPN connection (e.g. SSL VPN, encrypted VPN)

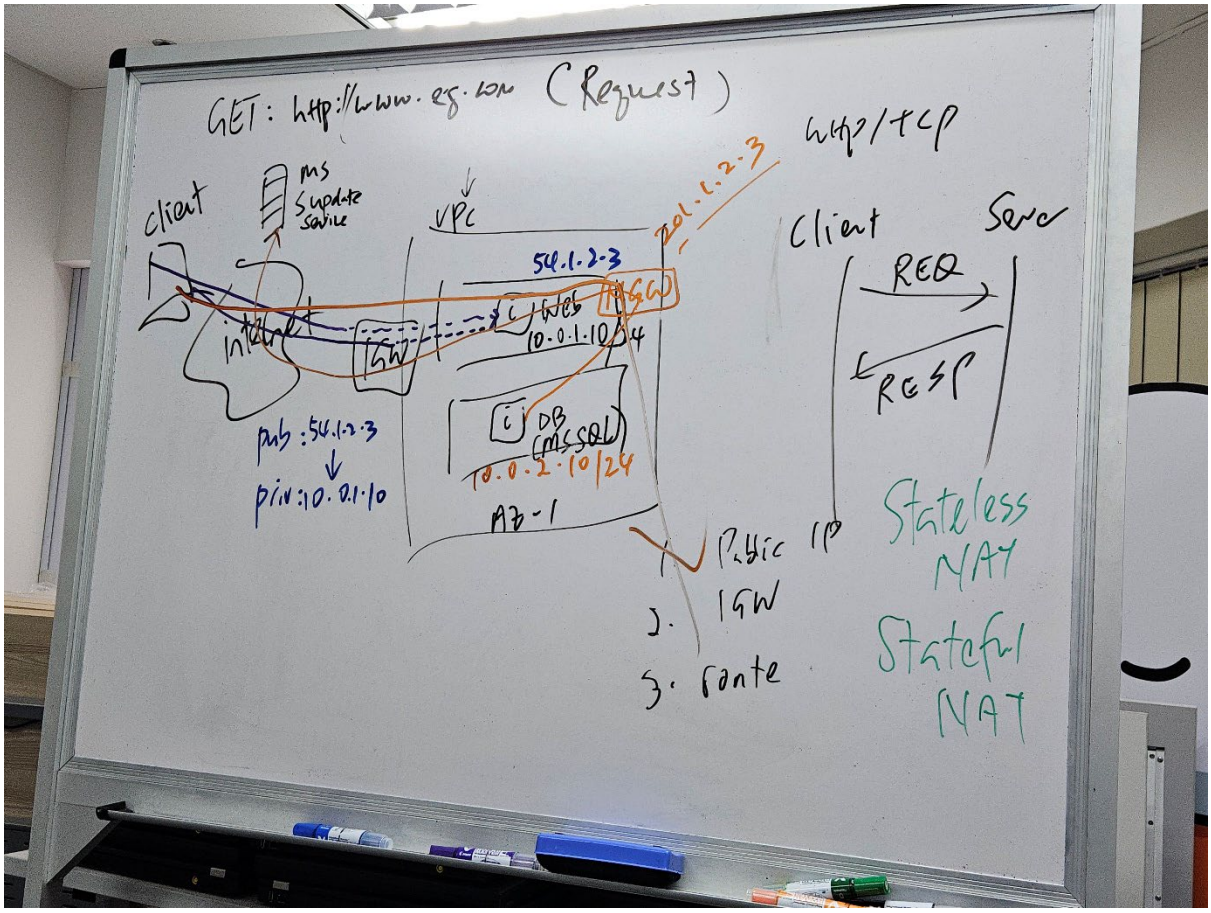
NAT - Network Address Translation

Do not give server a public IP address.

Server uses a private subnet behind firewall

Multi-layer netting

1. Internet gateway
2. Network Gateway
3. Virtual private network gateway



AWS Direct Connect

Whole environment is private.

Route tables

Distinct public and private subnet.

Subnet associated with 1 table at a time.

Custom route table (public)

Main route table (private)

Access control

-Network level

-Network Access Control List (ACL) - stateless (i.e. create a separate outbound rule)

-In/Out from the Firewall's perspective

Stateful versus Stateless

Default NACL

-Inbound (allowed)

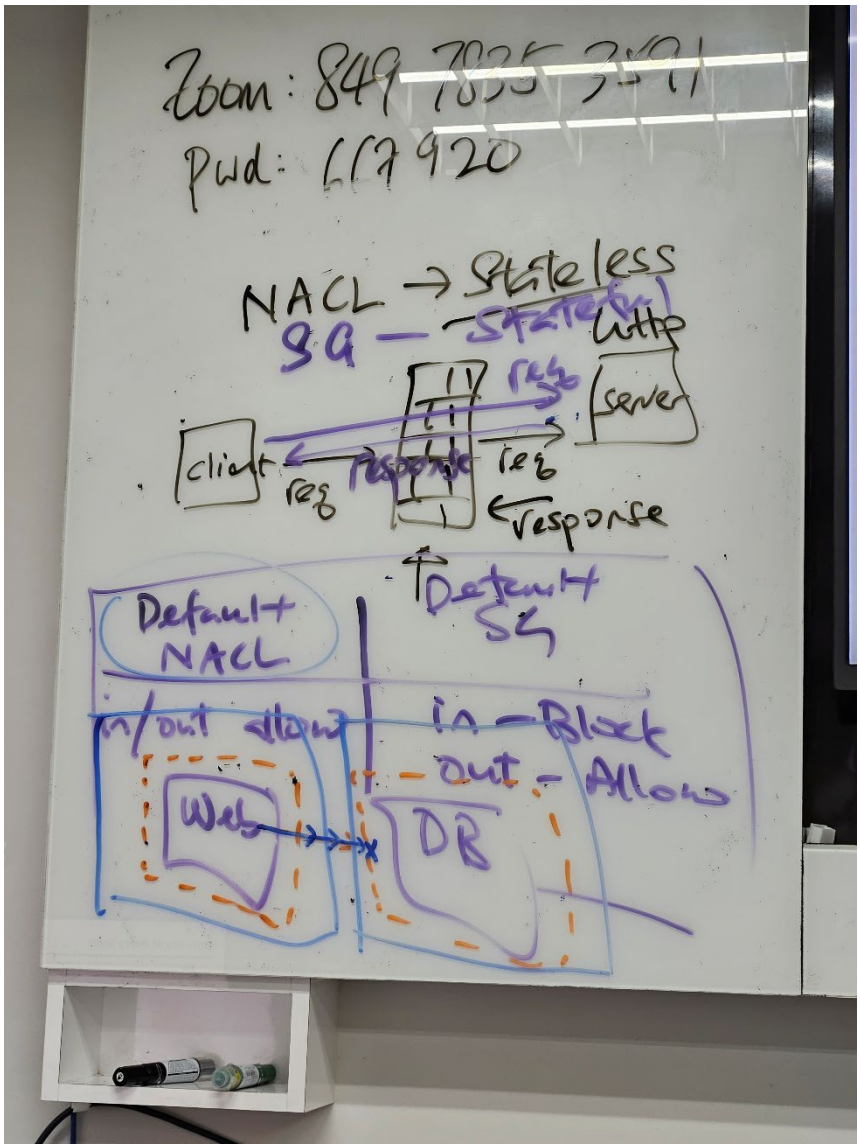
-Outbound (allowed)

Default security groups

-Inbound (blocked)

-Outbound (allowed)

AWS Technical Essentials – Day 1 (1 October 2025)



Storage Lesson

-Block storage

Fragmentation when the file is stored.

Metadata of the block is captured

Instance store is temporary, is available with some AMI (Amazon Machine Image)

EBS (Elastic Block Store) is persistent, io2 will replace Instance store

SSD versus HDD

- Consider data access pattern (random or sequential?)

AWS Technical Essentials – Day 1 (1 October 2025)

For sequential data access, HDD is better

For random data access, SSD is favoured

-File storage (EFS - Elastic File Storage, span across regional datacentres, serverless, provision folder, infinite in iOps)

-Object level storage (e.g. OneDrive, Google Drive, has a generated key)

Global, regional and zonal

AWS

1. Unmanaged
2. Managed - RDS
3. Fully managed

For Windows, use Amazon FSx

Cloud Native app is a mixture of S3 and Lambda

Amazon S3 storage classes

-Amazon S3 standard

-S3 Standard-Infrequent access

-S3 One-zone Infrequent access

-S3 Glacier: Instant Retrieval, Flexible Retrieval and Deep Archive