AWS Cloud Practitioner Certification Bootcamp

Week - 7

Session 7 - VPC, Well-Architected Framework, Shared Responsibility

26th Feb, Saturday
7:00 PM to 8:30 PM IST

WOMEN iN BIG DATA
BANGLADESH

aws USER GROUP
BANGLADESH

AWS
User Groups

Speakers

Sanchit Jain

Lead Architect - AWS at Quantiphi

AWS APN Ambassador

Agenda

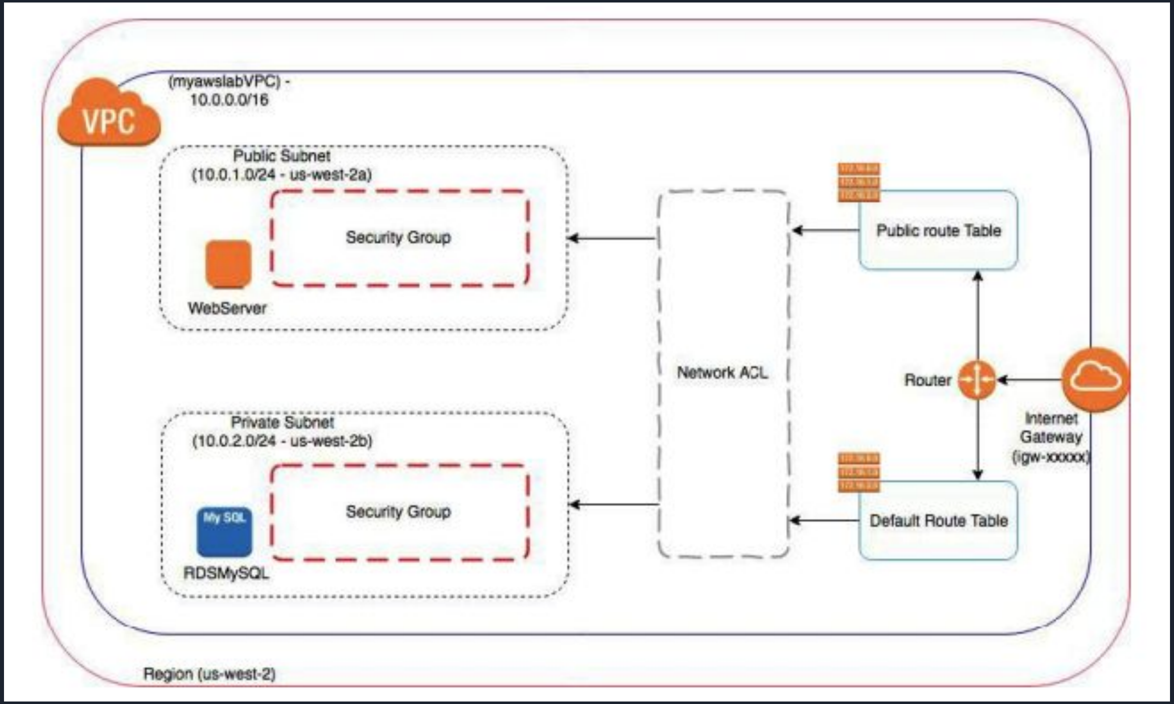
AWS
Virtual Private Cloud(VPC)

AWS
Shared Responsibility

AWS
Well Architected Framework

AWS VPC

AWS VPC


VPC
(myawslabVPC) -
10.0.0.0/16
Public Subnet
(10.0.1.0/24 - us-west-2a)
Security Group
WebServer
Private Subnet
(10.0.2.0/24 - us-west-2b)
My SQL
Security Group
RDSMySQL
Network ACL
Public route Table
Router
Internet
Gateway
(igw-xxxxx)
Default Route Table
Region (us-west-2)

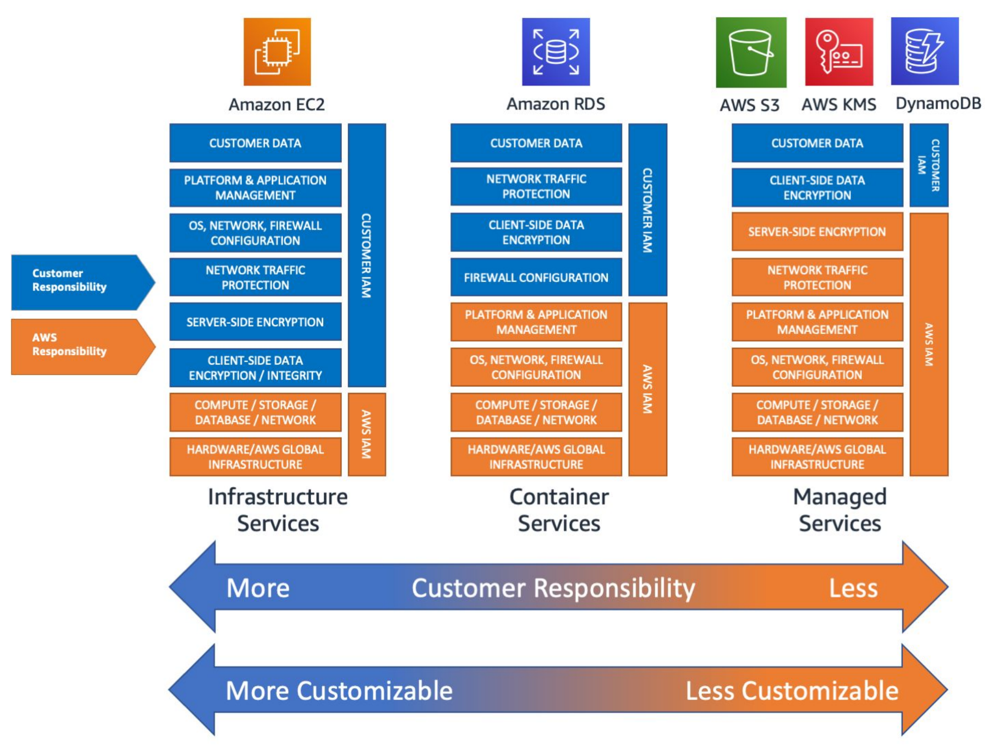
AWS VPC Components

- Subnet - A subnet (short for “subnetwork”) is an identifiably separate part of an organization’s network. These are the logical subdivisions of an IP network.
- Public Subnet - A logical subnet whose instance can be reachable over the internet directly.
- Private Subnet - A logical subnet whose instance cannot be reachable over the internet directly.
- Security group - A security group acts as a virtual firewall for your instance to control inbound and outbound traffic.
- Network ACL - A network access control list (ACL) is an optional layer of security for your VPC that acts as a firewall for controlling traffic in and out of one or more subnets.
- Route Table - A route table contains a set of rules, called routes, that are used to determine where network traffic is directed.
- Internet Gateway - An Internet gateway is a horizontally scaled, redundant, and highly available VPC component that allows communication between instances in your VPC and the Internet.

AWS
Shared Responsibility

AWS Shared Responsibility

- To help clarify the division of responsibilities and ease the burden of cloud security, Amazon Web Services (AWS) has established the AWS Shared Responsibility Model.
- Put simply, the AWS Shared Responsibility Model explains what AWS is responsible for securing in the cloud and what the customer is responsible for securing.



Customer Responsibility

AWS Responsibility

Amazon EC2

- CUSTOMER DATA
- PLATFORM & APPLICATION MANAGEMENT
- OS, NETWORK, FIREWALL CONFIGURATION
- NETWORK TRAFFIC PROTECTION
- SERVER-SIDE ENCRYPTION
- CLIENT-SIDE DATA ENCRYPTION / INTEGRITY
- COMPUTE / STORAGE / DATABASE / NETWORK
- HARDWARE/AWS GLOBAL INFRASTRUCTURE
- CUSTOMER IAM
- AWS IAM

Infrastructure Services

Amazon RDS

- CUSTOMER DATA
- NETWORK TRAFFIC PROTECTION
- CLIENT-SIDE DATA ENCRYPTION
- FIREWALL CONFIGURATION
- PLATFORM & APPLICATION MANAGEMENT
- OS, NETWORK, FIREWALL CONFIGURATION
- COMPUTE / STORAGE / DATABASE / NETWORK
- HARDWARE/AWS GLOBAL INFRASTRUCTURE
- CUSTOMER IAM
- AWS IAM

Container Services

AWS S3 AWS KMS DynamoDB

- CUSTOMER DATA
- CLIENT-SIDE DATA ENCRYPTION
- SERVER-SIDE ENCRYPTION
- NETWORK TRAFFIC PROTECTION
- PLATFORM & APPLICATION MANAGEMENT
- OS, NETWORK, FIREWALL CONFIGURATION
- COMPUTE / STORAGE / DATABASE / NETWORK
- HARDWARE/AWS GLOBAL INFRASTRUCTURE
- CUSTOMER IAM
- AWS IAM

Managed Services

More Customer Responsibility Less

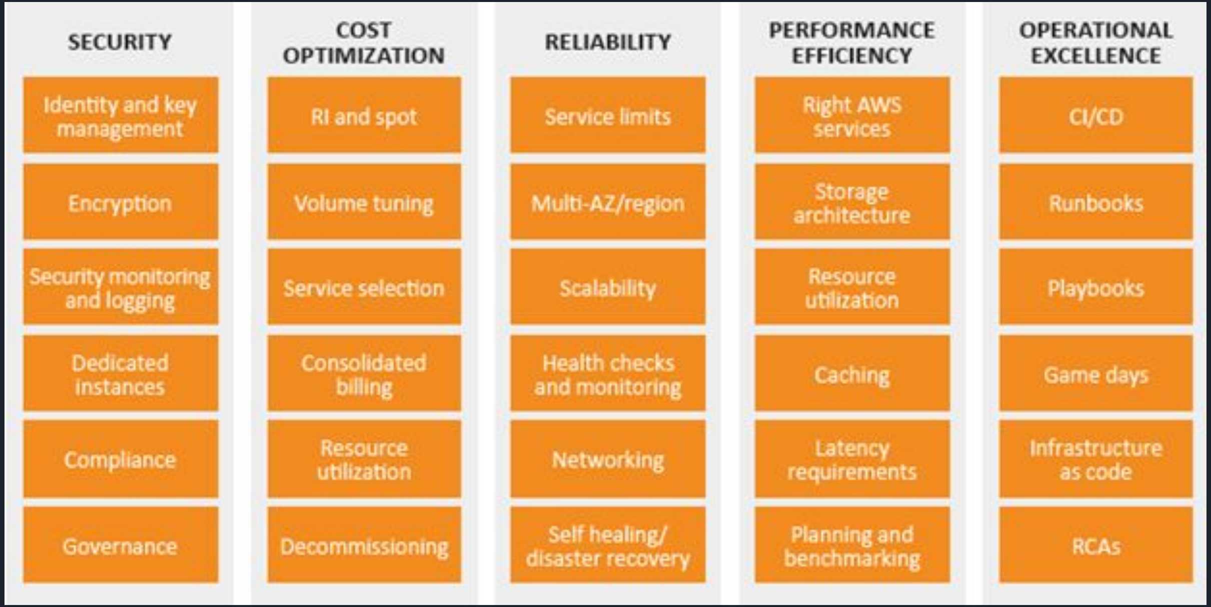
More Customizable Less Customizable

AWS
User Groups

AWS
Well Architected Framework

AWS Well Architected Framework

- AWS Well-Architected helps cloud architects build secure, high-performing, resilient, and efficient infrastructure for their applications and workloads. Based on five pillars operational excellence, security, reliability, performance efficiency, and cost optimization



SECURITY	COST OPTIMIZATION	RELIABILITY	PERFORMANCE EFFICIENCY	OPERATIONAL EXCELLENCE
Identity and key management	RI and spot	Service limits	Right AWS services	CI/CD
Encryption	Volume tuning	Multi-AZ/region	Storage architecture	Runbooks
Security monitoring and logging	Service selection	Scalability	Resource utilization	Playbooks
Dedicated instances	Consolidated billing	Health checks and monitoring	Caching	Game days
Compliance	Resource utilization	Networking	Latency requirements	Infrastructure as code
Governance	Decommissioning	Self healing/ disaster recovery	Planning and benchmarking	RCAs

Operational Excellence

- The Operational Excellence pillar includes the ability to support development and run workloads effectively, gain insight into their operation, and continuously improve supporting processes and procedures to delivery business value

- Design Principles - There are five design principles for operational excellence in the cloud
    - Perform operations as code
    - Make frequent, small, reversible changes
    - Refine operations procedures frequently
    - Anticipate failure
    - Learn from all operational failures

Security

- The Security pillar includes the ability to protect data, systems, and assets to take advantage of cloud technologies to improve your security
- Design Principles - There are seven design principles for security in the cloud:
    - Implement a strong identity foundation
    - Enable traceability
    - Apply security at all layers
    - Automate security best practices
    - Protect data in transit and at rest
    - Keep people away from data
    - Prepare for security events

Reliability

- The Reliability pillar encompasses the ability of a workload to perform its intended function correctly and consistently when it’s expected to

- Design Principles - There are five design principles for reliability in the cloud:
  - Automatically recover from failure
  - Test recovery procedures
  - Scale horizontally to increase aggregate workload availability
  - Stop guessing capacity
  - Manage change in automation

Performance Efficiency

- The Performance Efficiency pillar includes the ability to use computing resources efficiently to meet system requirements, and to maintain that efficiency as demand changes and technologies evolve.
- Design Principles - There are five design principles for performance efficiency in the cloud:
  - Democratize advanced technologies
  - Go global in minutes
  - Use serverless architectures
  - Experiment more often
  - Consider mechanical sympathy

Cost Optimization

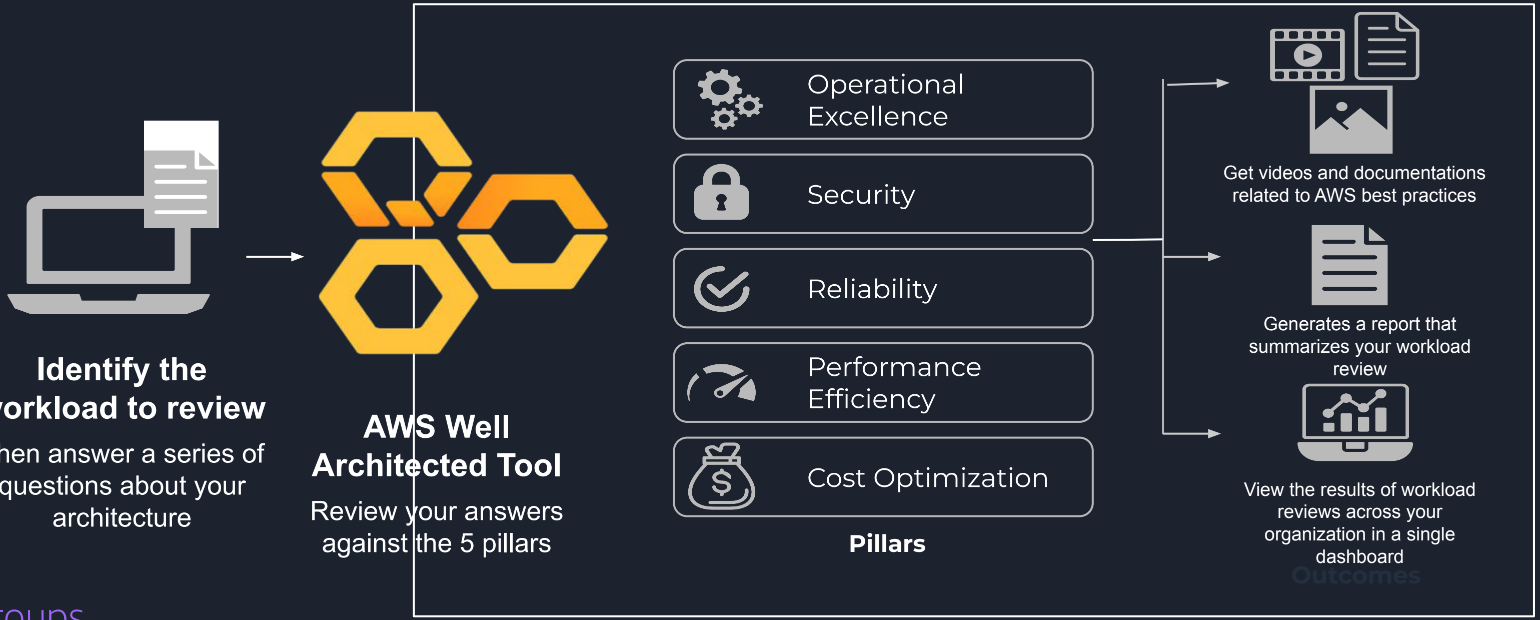
- The Cost Optimization pillar includes the ability to run systems to deliver business value at the lowest price point

- Design Principles - There are five design principles for cost optimization in the cloud:
  - Implement cloud financial management
  - Adopt a consumption model
  - Measure overall efficiency
  - Stop spending money on undifferentiated heavy lifting
  - Analyze and attribute expenditure

AWS Well Architected Review

AWS Well-Architected Review helps you review the state of your workloads and compares them to the latest AWS architectural best practices.

It is based on the AWS Well Architected Framework, developed to help cloud architects build secure, high-performing, resilient, and efficient infrastructure.



Identify the workload to review

Then answer a series of questions about your architecture

AWS Well Architected Tool

Review your answers against the 5 pillars

- Operational Excellence
- Security
- Reliability
- Performance Efficiency
- Cost Optimization

Pillars

Get videos and documentations related to AWS best practices

Generates a report that summarizes your workload review

View the results of workload reviews across your organization in a single dashboard

Outcomes

Thank you!

WOMEN iN BIG DATA

BANGLADESH

aws USER GROUP

BANGLADESH

AWS

User Groups