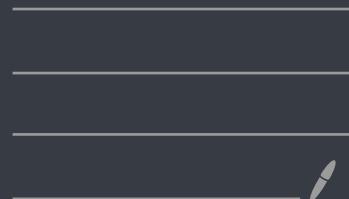


AWS CLOUD

PRACTITIONER
COURSE

Ritesh Bhattacharyya



Exam Guide – Content Outline



Cloud Concepts	28%
Security	24%
Technology	36%
Billing and Pricing	12%

Important: The content of the examination has a specific weighting, so some sections have more questions than others. This table contains the breakdown of the exam content and its relative weight.

Content Outline

The exam guide includes weighting, test objectives and descriptions only. It is not a comprehensive listing of the content of the exam. To determine what to study, refer to the exam content outline and the sample questions.

Domain	Details	% of Exam
Domain 1: Cloud Concepts	1.1 Explain the concept of cloud and its value to a organization 1.2 Identify concepts of AWS Cloud architecture 1.3 Explain the AWS Cloud computing model 1.4 Explain the AWS Cloud delivery model	24%
Domain 2: Security	2.1 Explain the AWS security principles 2.2 Define the AWS shared responsibility model 2.3 Define AWS Cloud security best practices concepts	31%
Domain 3: Technology	3.1 Explain the AWS Lambda function execution model 3.2 Explain the AWS Lambda invoke interface 3.3 Explain the AWS Lambda trigger interface	17%
Domain 4: Billing and Pricing	4.1 Explain the AWS Cloud pricing model 4.2 Explain the AWS Cloud cost management tools for AWS	18%
TOTAL:		100%

Version 1.1-CDF-021

Page | 2

2.3 Identify AWS storage management capabilities
2.4 Identify resources for security request
Detailed description: Explain how AWS Cloud provides security using the AWS Cloud security principles and the AWS shared responsibility model.
3.1 Define the AWS Lambda function execution model
3.2 Explain the AWS Lambda invoke interface
3.3 Explain the AWS Lambda trigger interface
Detailed description: Explain the AWS Lambda function execution model, invoke interface, trigger interface, and the AWS Lambda API.
4.1 Explain the AWS Cloud pricing model
4.2 Explain the AWS Cloud cost management tools for AWS
4.3 Explain the AWS Cloud cost management concepts



What is Cloud Computing?

cloud com·put·ing

noun

the practice of using a network of remote servers hosted on the Internet to store, manage, and process data, rather than a local server or a personal computer.



-GCP, AWS, AZURE

Cloud Providers

- Someone else owns the servers
- Someone else hires the IT people
- Someone else pays or rents the real-estate
- You are responsible for your configuring cloud services and code, someone else takes care of the rest.

On-Premise

- You own the servers
- You hire the IT people
- You pay or rent the real-estate
- You take all the risk

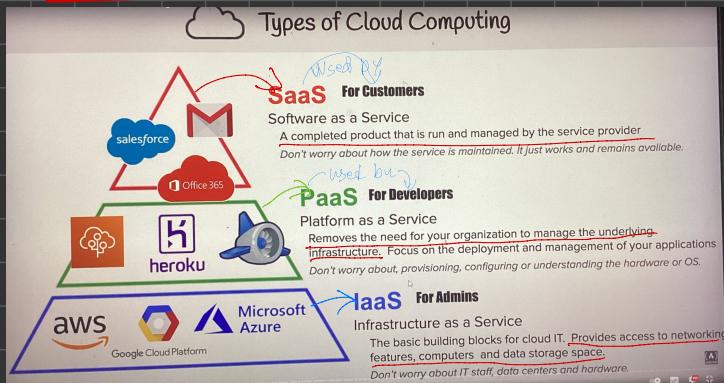
ADVANTAGES AND BENEFITS!



Six Advantages and Benefits of Cloud Computing

Why go with a Cloud Provider over On-Premise?

- 1 Trade capital expense for variable expense No upfront-cost instead of paying for data centers and servers Pay On-Demand Pay only when you consume computing resources
- 2 Benefit from massive economies of scale Usage from hundreds of thousands of customers aggregated in the cloud. You are sharing the cost with other customers to get unbeatable savings
- 3 Stop guessing capacity Eliminate guesswork about infrastructure capacity needs. Instead of paying for idle or underutilized servers, you can scale up or down to meet the current need
- 4 Increase speed and agility Launch resources within a few clicks in minutes instead of waiting days or weeks of your IT to implement the solution on-premise
- 5 Stop spending money on running and maintaining data centers Focus on your own customers, rather than on the heavy lifting of racking, stacking, and powering servers
- 6 Go global in minutes Deploy your app in multiple regions around the world with a few clicks. Provide lower latency and a better experience for your customers at minimal cost.



AWS Global Infrastructure

Where does all this Cloud Computing Run?

69 Availability Zones within **22 Geographic Regions** around the world
Way More Edge Locations than AZs!

AWS serves over a million active customers in more than 190 countries

Steadily expanding global infrastructure to help customers achieve lower latency and higher throughput

Regions physical location in the world with multiple Availability Zones

Availability Zones one or more discrete data centers

Edge Location datacenter owned by a trusted partner of AWS



Regions



A **geographically distinct** location which has multiple datacenters (AZs)

Every region is **physically isolated** from and independent of every other region in terms of location, power, water supply

Each region has at least  two AZs \Rightarrow 2 AZs available

AWS largest region is **US-EAST**

NEW services almost always become available first in **US-EAST**

Not all services are available in all regions.

US-EAST-1 is the region where you see all your billing information.

Availability Zones :-

Availability Zones (AZs)



An AZ is a datacenter owned and operated by AWS in which AWS services run

Each region has at least two AZs

AZs are represented by a Region Code, followed by a letter identifier eg. **us-east-1a**

Multi-AZ Distributing your instances across multiple AZs allows failover configuration for handling requests when one goes down.

< 10ms latency between AZs

Edge Locations :-



Edge Locations

Get Data Fast or Upload Data Fast to AWS

An Edge Location is a datacenter owned by a trusted partner of AWS which has a **direct connection** to the AWS network.



These locations serve requests for **CloudFront** and **Route 53**. Requests going to either of these services will be routed to the nearest edge location automatically.



S3 Transfer Acceleration traffic and **API Gateway** endpoint traffic also use the AWS Edge Network.

This allows for **low latency** no matter where the end user is geographically located.

This is why edge location is needed!

CloudFront
Route 53
S3 Transfer Acceleration
API Gateway

GovCloud Regions :- Available for US only and US Govt use it for Controlled Unclassified Information.

 GovCloud (US)

AWS GovCloud Regions allow customers to host sensitive **Controlled Unclassified Information** and other types of regulated workloads.

GovCloud Regions are only operated by employees who are U.S. citizens, on U.S. soil.

They are **only** accessible to U.S. entities and root account holders who pass a screening process.

Customers can architect secure cloud solutions that comply with:

-  FedRAMP High baseline
-  DOJ's Criminal Justice Information Systems (CJIS) Security Policy
-  U.S. International Traffic in Arms Regulations (ITAR)
-  Export Administration Regulations (EAR)
-  Department of Defense (DoD) Cloud Computing Security Requirements Guide

Cost Management Preferences :-

Receive free tier Usage Alerts [Free]

Receive Billing Alerts [Free]

Detailed Billing Reports [You have to pay for this → Can be stored in S3 Bucket.
This is not free]

The screenshot shows the 'Identity and Access Management' blade in the Azure portal. The left sidebar lists 'Identity Management (1)', 'Azure Active Directory (1)', 'Groups', 'Users', 'Roles', 'Identity providers', 'Account settings', 'Conditional access', 'Dashboard report', and 'Delete AAD'. The main area has a title 'Welcome to Identity and Access Management' and a sub-section 'AAD Tenant (1)'. Below that is 'AAD Resources' with sections for 'Users (0)', 'Groups (0)', and 'Custom Managed Policies (0)'. On the right, there's a 'Role assignments (0)' section with a 'Resets 2' link and a 'Identity Providers (0)' section. At the bottom, a progress bar indicates '1 out of 5 complete'.

Android, iPhone → Google Authenticator
Windows Phone → Google Authenticator

Your Security Credential

Use this page to manage the credentials for your AWS account.

To learn more about the types of AWS credentials:

- Password
- Multi-factor authentication (MFA)

User MFA increases the security of your AWS account.

[Activate MFA](#)

– Access keys (access key ID and secret access key)

– CloudFront key pairs

– X.509 certificate

– Account identifiers

Set up virtual MFA device

1. Install a compatible app on your mobile device or computer. See list of compatible applications.

2. Use your virtual MFA app and your device's camera to scan the QR code.



Alternatively, you can type the secret key. Show secret key

3. Type two consecutive MFA codes below.

MFA code 1:

MFA code 2:

[Cancel](#) [Previous](#) [Assign MFA](#)

Add user

Set user details

You can add multiple users at once with the same access type and permissions. [Learn more](#)

User name*

Add another user

Select AWS access type

Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step. [Learn more](#)

Access type* Programmatic access

Enables an access key ID and secret access key for the AWS API, CLI, SDK, and other development tools.

AWS Management Console access

Enables a password that allows users to sign-in to the AWS Management Console.

Console password* Autogenerated password

Custom password

Require password reset User must create a new password at next sign-in

Users automatically get the IAMUserChangePassword policy to allow them to change their own password.

PASSWORD POLICY:-

The screenshot shows the AWS IAM Password Policy settings page. The left sidebar navigation includes Identity and Access Management (IAM), AWS Account (111111111111), Dashboard, Groups, Users, Roles, Policies, Identity providers, Account settings, Credential report, and a search bar for IAM. The main content area is titled "Password policy". It states: "A password policy is a set of rules that define the type of password an IAM user can set. Learn more". Below this is a "Password policy" section with the message: "The AWS account does not have a password policy set." A "Set password policy" button is present. The "Endpoints" section lists session tokens from the global STS endpoint and regional STS endpoints. The "Regions" section lists various AWS regions with their respective endpoints and status. The "Endpoints" table has columns: Region name, Endpoint, STS status, and Actions. The "Regions" table has columns: Region name, Endpoint, Status, and Actions.

Region name	Endpoint	STS status	Actions
Global Endpoint	https://sts.amazonaws.com	Always active	<input type="button" value="Edit"/>
US East (N. Virginia)	https://sts.us-east-1.amazonaws.com	Always active	<input type="button" value="Edit"/>
Asia Pacific (Hong Kong)	https://sts.ap-southeast-1.amazonaws.com	Active	<input type="button" value="Deactivate"/>
Asia Pacific (Mumbai)	https://sts.ap-south-1.amazonaws.com	Active	<input type="button" value="Deactivate"/>
Asia Pacific (Seoul)	https://sts.ap-northeast-2.amazonaws.com	Active	<input type="button" value="Deactivate"/>
Asia Pacific (Sydney)	https://sts.ap-northeast-1.amazonaws.com	Active	<input type="button" value="Deactivate"/>
Asia Pacific (Singapore)	https://sts.ap-southeast-2.amazonaws.com	Active	<input type="button" value="Deactivate"/>
Australia (Wellington)	https://sts.ap-southeast-1.amazonaws.com	Active	<input type="button" value="Deactivate"/>

The screenshot shows the "Set password policy" configuration page. The top navigation bar includes Services, Resource Groups, and a search bar for IAM. The main content area is titled "Set password policy". It states: "A password policy is a set of rules that define complexity requirements and mandatory rotation periods for your IAM users' passwords. Learn more". Below this is a "Select your account password policy requirements" section. The "Enforce minimum password length" field is set to 6 characters. The "Complexity requirements" section contains several checkboxes: "Requires at least one uppercase letter from Latin alphabet (A-Z)" (checked), "Requires at least one lowercase letter from Latin alphabet (a-z)" (checked), "Requires at least one number" (checked), "Requires at least one non-alphanumeric character ([!@#\$%^&*(),_---])" (checked), "Enable password expiration" (unchecked), "Password expression requires administrator review" (unchecked), "Allow users to change their own password" (unchecked), and "Prevent password reuse" (unchecked).

