Module Completion and Exam Hints
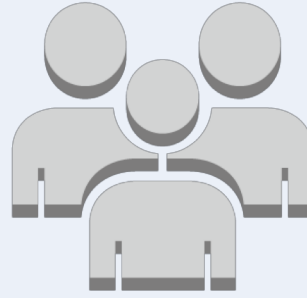
Identity Access Management (IAM)

Identity Access Management

- AWS Identity and Access Management (IAM) helps you securely control access to AWS resources

- You use IAM to control *who* is authenticated (signed in) and authorized (has permissions) to use *what* resources

- IAM authentication and authorization

Identity Access Management
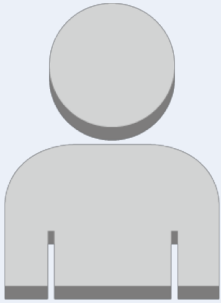
USER   GROUP   ROLE

AUTHENTICATION

POLICY DOCUMENT

AUTHORIZATION

AWS Certified Cloud Practitioner

IAM Key Concepts

- A USER is a permanent named operator, human or AWS service, with PERMANENT auth. CREDENTIALS

- A GROUP is a collection of users and usually contains multiple users; a user can belong to multiple groups

- A ROLE is an operator, just like a user; a role can be as well a human or another AWS service, with TEMPORARY auth. CREDENTIALS

- POLICY DOCS enforce authorization (permissions)

Virtual Private Cloud (VPC)

Virtual Private Cloud (VPC)

- A virtual private cloud (VPC) is a virtual network dedicated to your AWS account (i.e. 10.0.0.0/16)

- Amazon Virtual Private Cloud enables you to launch AWS resources into the virtual network that you define

- AWS VPC is literally your Data Center in the AWS Cloud

Data Center

Elastic Compute Cloud (EC2)

Elastic Compute Cloud (EC2)

- AWS Elastic Compute Cloud (EC2) provides scalable computing capacity in the Amazon Web Services (AWS) cloud – Virtual Machines in AWS -> INSTANCES

- There are four ways to pay for Amazon EC2 instances:
    - On-Demand Instances
    - Reserved Instances
    - Spot Instance
    - Dedicated Hosts

EC2

Pricing models for Amazon EC2

- With *On-Demand Instances*, you pay for compute capacity per hour or per second, depending on which instances you run

- Amazon *EC2 Spot Instances* allow you to request spare Amazon EC2 computing capacity for up to 90% off the On-Demand price

Pricing models for Amazon EC2

- Amazon *EC2 Reserved Instances* provide you with a significant discount (up to 75%) compared to On-Demand Instance pricing

- Amazon *Dedicated Host* is a physical EC2 server dedicated for your use

Security Groups (SGs)

Security Groups (SG) Basics

- AWS security groups act as a virtual firewall for your EC2 instances to control inbound and outbound traffic

- Security groups enforce security at the instance level, not the subnet; different EC2 instances can have different SGs applied

- In a SG you add rules that control inbound traffic to instances and separate rules that control outbound traffic

Security Group

Elastic Block Store (EBS)

Elastic Block Store (EBS) Basics

- Amazon Elastic Block Store (EBS) provides block level storage volumes for use with EC2 instances

- EBS volumes are highly available and reliable storage volumes that can be attached to any running instance that is in the same AZ

- EBS volumes that are attached to an EC2 instance are exposed as storage volumes that persist independently from the life of the instance

Amazon EBS

Amazon EBS Volume Types

- SSD volumes types:
  - General Purpose SSD (gp2)
    - Balance between price & performance
  - Provisioned IOPS SSD (io1)
    - Highest performance SSD volume

- HDD volumes types:
  - Throughput optimized HDD (st1)
    - Low-cost; frequently accessed, throughput-intensive
  - Cold HDD (sc1)
    - Lowest cost; less frequently accessed workloads

Amazon EBS

Amazon EBS Pricing

- Amazon EBS pricing depends on the following:

- Volumes
  - Total storage of all EBS volumes, charged as GB/month

- Snapshots
  - Total snapshot storage consumed in AWS S3
  - EBS snapshot copying between regions is charged

- Data Transfer – inbound is free, outbound is charged

Simple Storage Service (S3)

What is Amazon S3 ?

- Amazon S3 or Amazon Simple Storage Service provides object storage through a web service interface

- With Amazon S3 you can store and retrieve any amount of data, at any time, from anywhere on the web

Amazon S3

- You can use S3 to store files, documents, pictures, etc (object storage) and not OS (Elastic Block Store – EBS purpose)

Amazon S3 Concepts

- A Bucket is a container for objects stored in Amazon S3

- Every object in S3 is contained in a bucket

- Think of a bucket as a folder where you can store objects (files)

- Bucket names are globally unique !
(DNS Compliant)
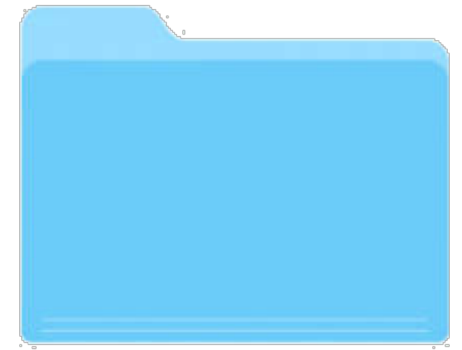
Folder

Amazon S3 Data Consistency Model

- Amazon S3 provides read-after-write consistency for PUTS of new objects in your S3 bucket in all regions

- This means you can access the object immediately, after it was copied (PUT) in an S3 bucket

- Amazon S3 offers eventual consistency for overwrite PUTS and DELETES in all regions

- If you update or delete an object in S3 bucket, the change will *eventually* be propagated and visible everywhere
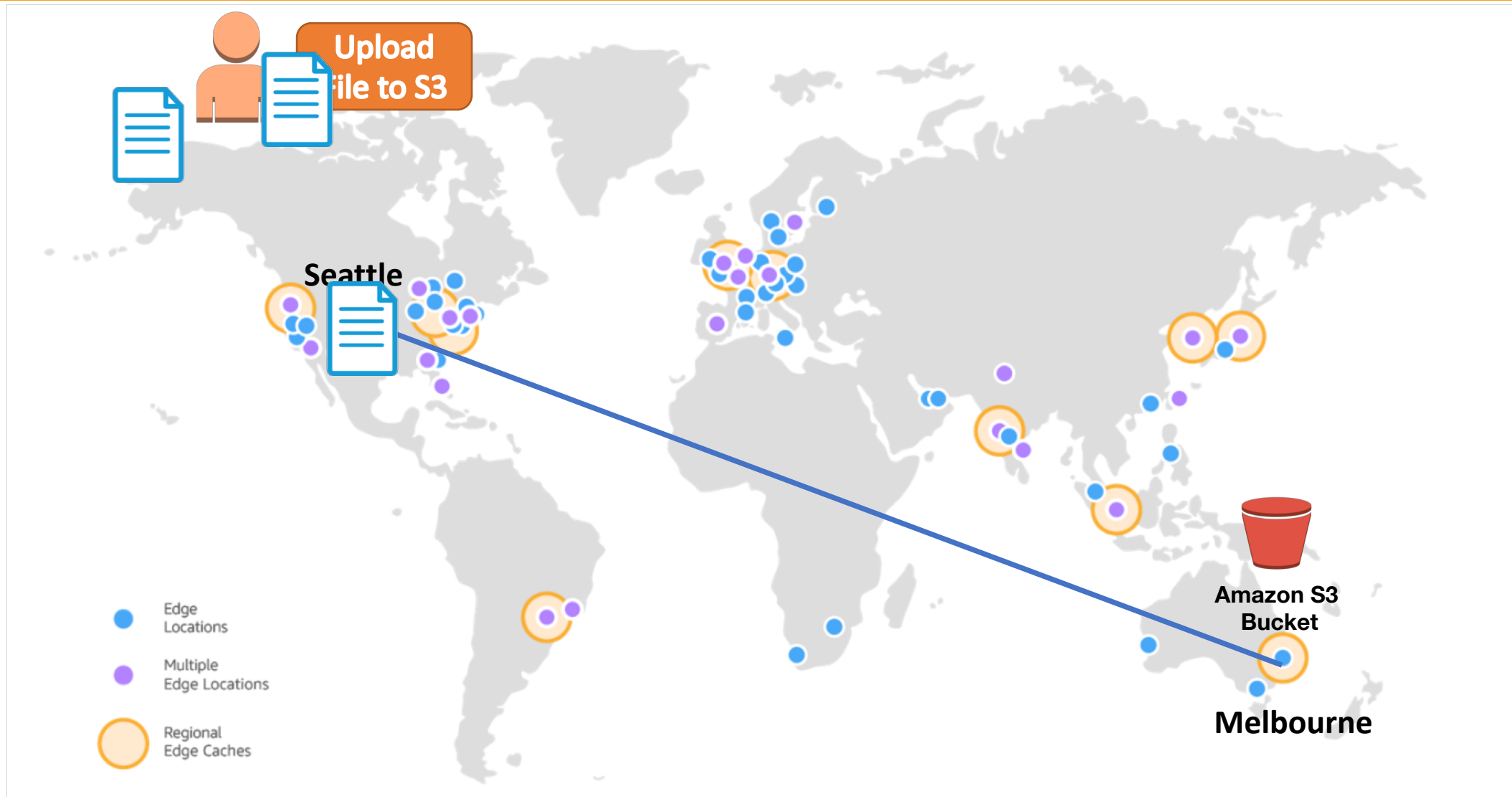
Amazon S3 Features – Storage Classes

- *Standard Storage Class* is used for performance-sensitive use cases (those that require millisecond access time) and frequently accessed data

- *Standard_IA* and *Onezone_IA* – Infrequently Accessed
  - Designed for long-lived & infrequently accessed data
  - Plan to store data for minimum 30 days

- *Standard_IA* - Amazon S3 stores the object data redundantly across multiple geographically separated AZs ; objects are resilient to the loss of an AZ
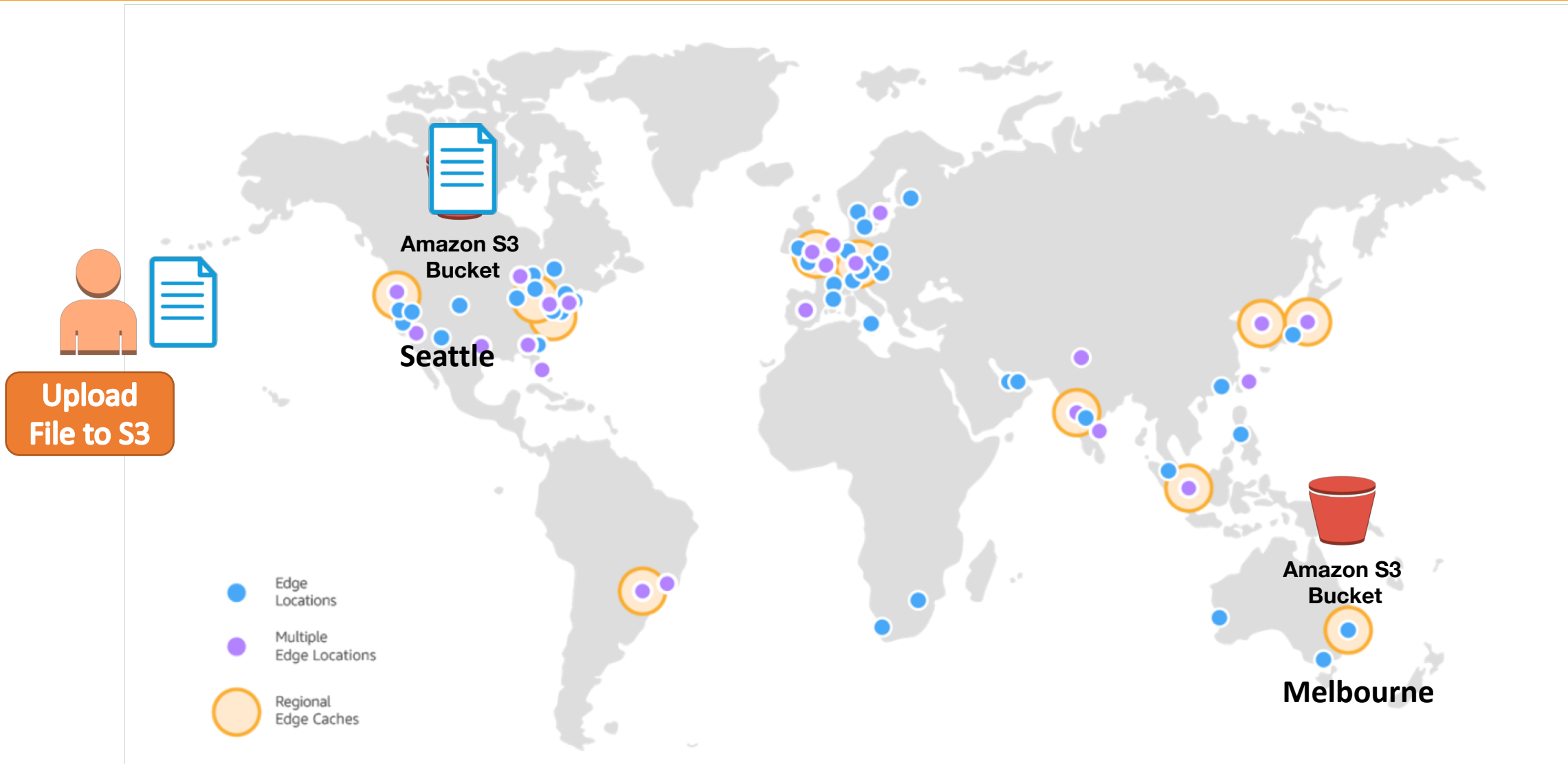
Amazon S3 Features – Storage Classes

- *Standard Onezone_IA* - Amazon S3 stores the object data in only one AZ; however, the data is not resilient to the physical loss of the Availability Zone

- *Glacier* - data stored in this storage class has a minimum storage duration period of 90 days and can be accessed in 1-5 minutes using expedited retrieval

- *Deep_Archive* - Minimum storage duration period of 180 days and a default retrieval time of 12 hours; lowest cost storage option in AWS

AWS S3 Transfer Acceleration

Upload File to S3

Seattle

Edge Locations

Multiple Edge Locations

Regional Edge Caches

Amazon S3 Bucket

Melbourne

AWS Certified Cloud Practitioner

Amazon S3 Pricing

- Amazon S3 provides the simplicity and cost-effectiveness of pay-as-you-go pricing

- You pay only for the storage you use, no minimum fee

- Price will depend on the following:
  - Storage Class
  - Storage – number and size of objects
  - Requests – GET requests come with charges
  - Data Transfer – data transferred out of Amazon S3

What's next ?

Thank you