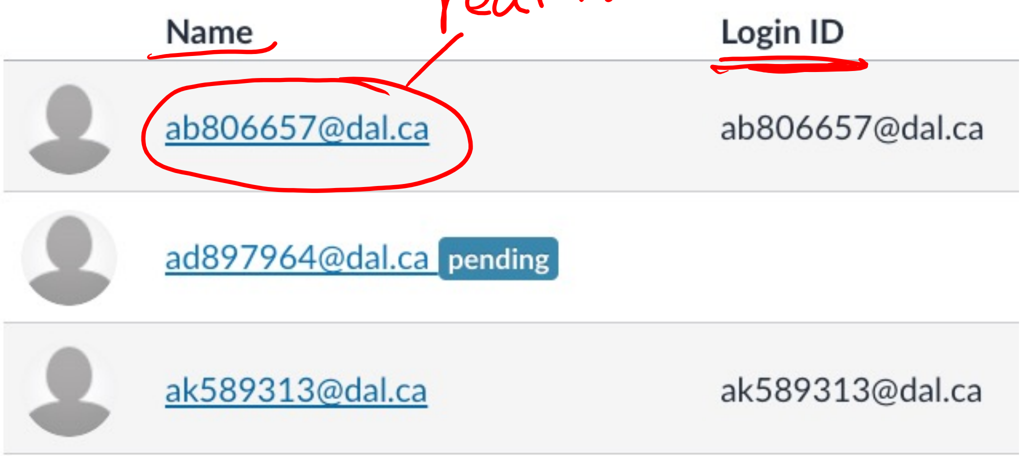
CSCI 5902 Adv. Cloud Architecting
Fall 2023
Instructor: Lu Yang

Modules 3 Adding Storage Layer (Sections 4 - 5)
Sep 22, 2023

Housekeeping and feedback (1/3)

1. You can start working on the first challenge lab today. The due date is 11:59pm, Sep 29.
2. First cloud architecting assignment released today. The due date is 11:59pm, Oct 6.
3. Newly registered students please ask me to add you to the Teams channel and ASW Academy resources.
4. Everyone must change your email address to your real name on the AWS Academy Cloud Architecting course.

real name



Name	Login ID
ab806657@dal.ca	ab806657@dal.ca
ad897964@dal.ca pending	
ak589313@dal.ca	ak589313@dal.ca

Housekeeping and feedback (2/3)

Key features of AWS KMS

- **Fully Managed:** You access the encrypted data by assigning permissions to use the keys while AWS Key Management Service deals with the long-lasting and physical security of your keys, hence enforcing your permissions.
- **Centralized Key Management:** AWS KMS provides a single point and defines policies continuously across AWS services and also your own applications. By using AWS CLI and SDK or AWS management console you can easily create, rotate, delete, and manage permissions on the keys.
- **Manage Encryption for AWS Service:** AWS KMS is integrated with AWS services to simplify the encryption of data. KMS monitors the use of keys to AWS CloudTrail to give you a view of who accessed your encrypted data, including AWS services using them on your behalf.
- **Encrypt Data In your Applications:** Using simple APIs you can also build encryption and key management into your own applications wherever they run. Using AWS SDK you can encrypt data locally within your application.
- **Digitally Sign Data:** To maintain the integrity of your data, AWS Key Management Service enables you to perform digital signing using asymmetric key pairs.
- **Low Cost:** As such there are no charges to use AWS Key Management Service. You are only charged when you use or manage the keys beyond the free tier.
- **Secure:** AWS KMS uses hardware security modules that have been validated under FIPS 140-2(Federal Information Processing Standard Publication) or are in the process of being validated, to generate and protect keys. Your keys are only used inside these devices and can never leave them unencrypted. KMS keys are never shared outside the AWS region in which they were created.
- **Compliance:** The security and quality controls in AWS KMS have been certified under multiple compliance schemes AWS KMS is also integrated with AWS CloudTrail for monitoring key usage so that your regulatory and compliance needs are met.

permission

Housekeeping and feedback (3/3)

- A fun question. What's the difference of AWS services and Amazon services?

  The key convention:

  - If the service is a foundational stand-alone service, the service name is prefixed with "Amazon"
  - However, if the service is a packaged solution service, or more like a utility service, its name is prefixed with "AWS"

Examples of stand-alone services:

- Amazon EC2
- Amazon S3
- Amazon Aurora
- Amazon DynamoDB
- Amazon CloudWatch

Examples of packaged or utility-type services:

- AWS Lambda – a utility serverless service , with EC2 servers in the back
- AWS Elastic Beanstalk – a packaged solution that manages foundational elements under the hood
- AWS Backup – a centralized packaged solution that you use for (backing up) other Amazon / AWS services
- AWS Build, AWS CodeCommit, AWS CodeDeploy, AWS CodePipeline – all of these are utilities to help you implement DevSecOps (or parts of it)

- A question for the next week's feedback:
  What's the difference of cloud services and cloud resources?

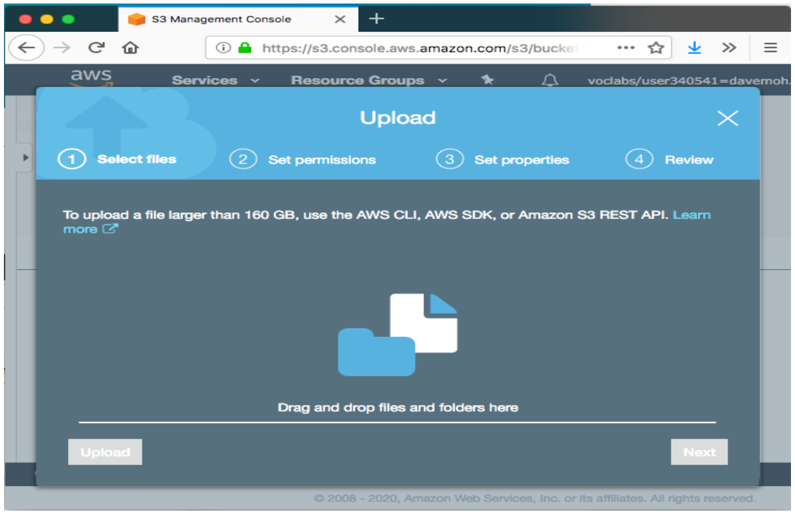
Module 3: Adding a Storage Layer

Section 4: Moving data to and from Amazon S3

Moving objects to Amazon S3

1 AWS Management Console

Upload or download by using a browser.



To upload a file larger than 160 GB, use the AWS CLI, AWS SDK, or Amazon S3 REST API. Learn more

Drag and drop files and folders here

© 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

2 AWS Command Line Interface

Upload or download from a terminal command prompt or in a call from a script.

scp

- Example upload command:

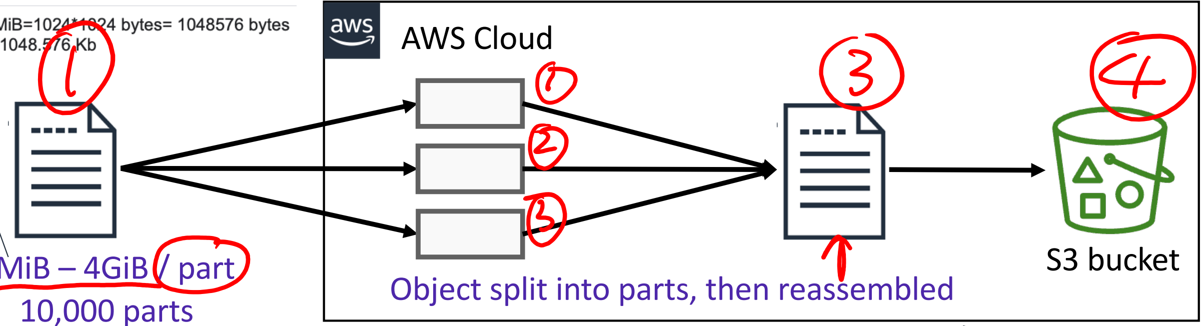
```
$aws s3 cp test.txt \
s3://AWSDOC-EXAMPLE-BUCKET/test.txt
```

3 AWS SDKs

Move objects programmatically by using AWS SDKs.

Multipart upload

Megabyte	Mebibyte
1 MB=1000*1000 bytes= 1000000 bytes or 1000Kb	1 MiB=1024*1024 bytes= 1048576 bytes or 1048.576 Kb



5MiB – 4GiB / part
10,000 parts

Object split into parts, then reassembled

Multipart upload is a three-step process:

1. Initiate the upload
2. Upload the object parts
3. Complete the multipart upload

- Files can be uploaded by using the Multipart Upload API
  - You can upload a single object as a set of parts → ids
  - Each part is a contiguous portion of the object's data
  - After all parts of your object are uploaded, Amazon S3 assembles these parts and creates the object
- Typically, only used for files larger than 100 MB
- Advantages –
  - Quick recovery from network issues: If transmission of any part fails, only need to retransmit that part
  - Ability to pause and resume object uploads
  - Improved throughput: Upload parts in parallel to improve throughput
- Professional: You can setup lifecycle policy to abort/delete incomplete multipart uploads after X days

Multipart upload – Optional readings

1

- Official AWS doc: https://docs.aws.amazon.com/AmazonS3/latest/userguide/mpuoverview.html

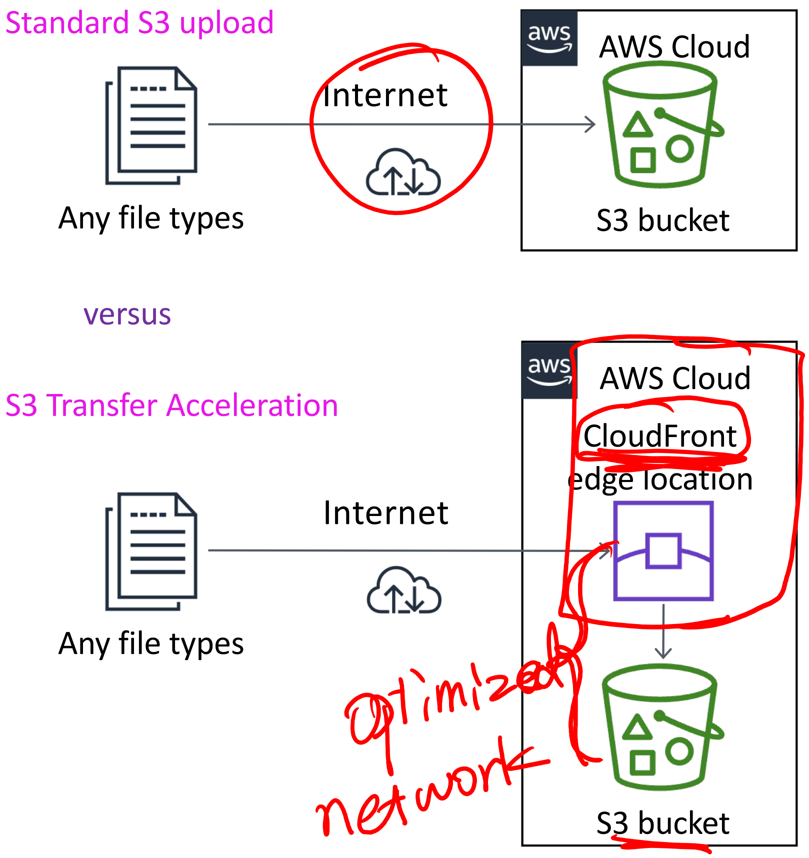
2

- Optional lab: https://aws.amazon.com/blogs/compute/uploading-large-objects-to-amazon-s3-using-multipart-upload-and-transfer-acceleration/#:~:text=Using%20S3%20multipart%20upload%20to%20upload%20large%20objects&text=Breaking%20a%20large%20object%20upload,upload%20for%20

AWS Blog

- How to set up a CloudFront distribution for Amazon S3: https://aws.amazon.com/cloudfront/getting-started/S3/
- How to use Python to upload files to S3 in parallel: https://www.linkedin.com/pulse/using-python-upload-files-s3-parallel-tom-reid/

Amazon S3 Transfer Acceleration



console

- Accelerates Amazon S3 data transfers
- Uses optimized network protocols and the AWS edge infrastructure
- Typical speed improvement:
  - 50–500% for cross-country transfer of larger objects
  - Can go even higher under certain conditions
- When to use transfer acceleration:
  - You have customers all around the world who upload to a centralized bucket
  - You transfer gigabytes or terabytes of data across continents on a regular basis
  - You underutilize the available bandwidth when you upload files to Amazon S3 over the internet
- Can be combined with multipart upload

Demonstration: S3 Transfer Acceleration

Moving large amounts of data into Amazon S3: AWS Snowball

Snow family

compute

AWS Snowball

AWS Snowball

Petabyte-scale data transport

1 thousand terabytes

- Can transport multiple terabytes of data into or out of Amazon S3
  - Multiple devices can be used to transfer petabytes
- Addresses concerns of large data transfers (network costs, transfer times, security)
  - *Example*: To transfer 10 petabytes (10 million GB) over the internet with a 10 Gbps upload speed would take over 100 days
- To use –
  - Create a job in the AWS Management Console and a Snowball will be shipped to you.
  - Attach to your local network, then download and run the Snowball Client
  - Select the file directories to transfer (encrypted) to the device
  - Ship the device back and track the status

Moving large amounts of data into Amazon S3: AWS Snowmobile

AWS Snowmobile

AWS Snowmobile

Exabyte-scale data transport

1 million terabytes or 1 billion gigabytes

- A 45-foot-long (13.7 meters) shipping container, pulled by a semi-trailer truck
- Can transfer up to 100 PB per Snowmobile
- Offers multiple layers of security –
  - Dedicated security personnel
  - GPS tracking, alarm monitoring, 24/7 video surveillance
  - Optional escort security vehicle while in transit
  - Data encrypted with 256-bit encryption keys

How should I choose between Snowmobile and Snowball?

To migrate large datasets of 10PB or more in a single location, you should use Snowmobile. For datasets less than 10PB or distributed in multiple locations, you should use Snowball.

(https://aws.amazon.com/snowmobile/faqs/#:~:text=AWS%20Snowmobile%20is%20the%20first,from%20on%2Dpremises%20to%20AWS)

Section 4 key takeaways

- The S3 multipart upload option is a good option for files larger than 100 MB and in situations where network connectivity might be inconsistent
- Amazon S3 Transfer Acceleration uses edge locations and can significantly increase the speed of uploads
- AWS Snowball provides a way to transfer *petabytes* of data, and AWS Snowmobile provides a way to transfer *exabytes* of data to AWS

Module 3: Adding a Storage Layer

Section 5: Choosing Regions for your architecture

aws academy

Choosing a Region: Compliance and latency considerations

This principle applies to not only S3 but also all other cloud services

- Data residency and regulatory compliance
  - Are there relevant Region data privacy laws?
  - Can customer data be stored outside the country?
  - Can you meet your governance obligation?

- Proximity of users to data
  - Small differences in latency can impact customer experience
  - Choose the Region closest to your users

Choosing a Region: Service availability and cost considerations

- Service and feature availability
  - Not all AWS services are available in all Regions
    - Consult the AWS Region Table for details
    - Services expand to new Regions regularly
  - Can use some services cross-Region, but at increased latency

- Cost-effectiveness
  - Costs vary by Region
  - Some services like Amazon S3 have costs for transferring data out
  - Consider the cost-effectiveness of replicating the entire environment in another Region

Why is S3 so powerful?

Powerful Features with Minimal Complexity

Major Users

- Airbnb.
- Pinterest.
- Netflix.
- Spotify.
- Amazon.
- Udemy.
- Instacart.
- Reddit.

ETL

Use Cases

- **Data lake creation.** An S3 data lake enables users to unlock insights to maximize the full value of their data.
- **Critical data backup and restoration.** Robust replication features make it easier for organizations to meet Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) in the event of a disaster.
- **Low-cost data archiving.** Moving data archives to certain levels of AWS S3 service, allow businesses to save money.
- **Operation of cloud-native applications.** Developers in particular will enjoy the ability to build robust, speedy mobile and web-based cloud-native apps that are configured to be highly available and scale automatically.

cost

Work with S3

- **Data structure.** AWS S3 is a key-value store. Features such as metadata support, prefixes, and object tags allow users to organize data according to their needs.
- **APIs and integrations.** The REST API for managing Amazon S3 buckets allows developers to connect stored data to other web applications and services. Objects are available to HTTP clients (S3 can be used as a static website host), and URLs can point directly to stored resources.
- **Data ingestion and analysis.** S3 integrates with AWS analytics services — no additional data migration or processing is required. Analysts can perform data mining directly on stored objects, metadata, tags, and S3 log information.

https://www.cloudwards.net/amazon-s3-review/#:~:text=Unlike%20classic%20cloud%20file%20storage,organization%20and%20accurate%20deep%20searches.
https://www.stitchdata.com/resources/aws-s3/

Professional level (1/3)

1. Do not store a lot of small files in S3

- **Cost**: Amazon S3 charges for storage space, data transfer, and requests. If you have a large number of small files, the cost can add up quickly.
  - Transferring a large number of small files to S3 can be inefficient due to network latency and the overhead of individual HTTP requests per file. The key to overcoming this challenge is to [redacted] before transferring them.
- **Limited Metadata Search**: Amazon S3 provides limited metadata search capabilities, which can make it difficult to locate specific files in a large bucket.

Professional level (1/3)

1. Do not store a lot of small files in S3

- **Cost**: Amazon S3 charges for storage space, data transfer, and requests. If you have a large number of small files, the cost can add up quickly.
  - Transferring a large number of small files to S3 can be inefficient due to network latency and the overhead of individual HTTP requests per file. The key to overcoming this challenge is to batch or package files before transferring them.
- **Limited Metadata Search**: Amazon S3 provides limited metadata search capabilities, which can make it difficult to locate specific files in a large bucket.

2. S3 is not a good solution for frequently and rapidly changing data

3. Cross Regin Replication (CRR)
   Can be combined with lifecycle policies to reduce latency and disaster recovery

4. S3 event notifications
   S3:ObjectCreated, S3:ObjectRemoved, S3:ObjectRestore, S3:Replication …
   The events can be sent to SNS, SQS, and Lambda function
   The events can also to sent to EventBridge to set up very complex rules to work with over 18 AWS services

CloudWatch

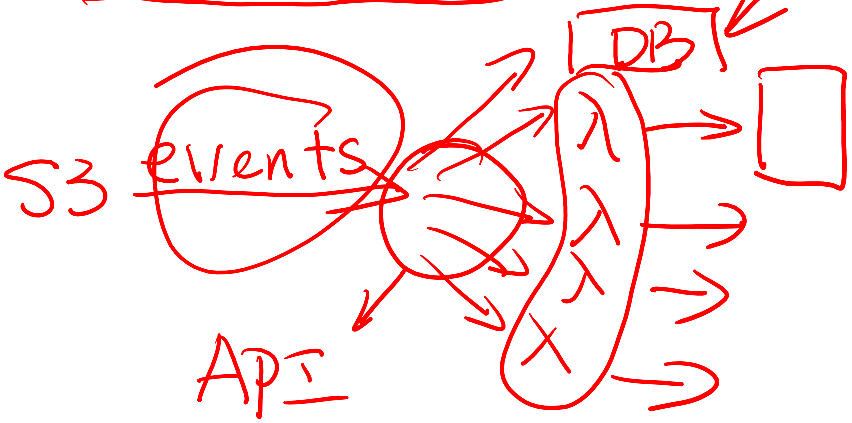
Professional level (2/3)

5. Byte-Range Fetches
   Using the Range HTTP header in a GET Object request, you can fetch a byte-range from an object, transferring only the specified portion. You can use concurrent connections to Amazon S3 to fetch different byte ranges from within the same object. This helps you achieve higher aggregate throughput versus a single whole-object request. Fetching smaller ranges of a large object also allows your application to improve retry times when requests are interrupted.
   (https://docs.aws.amazon.com/AmazonS3/latest/userguide/optimizing-performance-guidelines.html#optimizing-performance-guidelines-get-range)
6. S3 Select & Glacier Select
   (https://aws.amazon.com/blogs/aws/s3-glacier-select/#:~:text=Glacier%20Select%20allows%20you%20to,pass%20in%20initiate%20job%20request)
   - Filtering and retrieving data
     - Use SQL statements to filter the contents of an Amazon S3 object and retrieve only the subset of data that you need.
     - Reduce the amount of data that Amazon S3 transfers, which reduces the cost and latency to retrieve this data
     - Works on objects stored in CSV, JSON, or Apache Parquet format, with server-side encrypted objects

Professional level (3/3)

7. S3 Storage Lens
   Amazon S3 Storage Lens is a cloud-storage analytics feature that you can use to gain organization-wide visibility into object-storage usage and activity. You can use S3 Storage Lens metrics to generate summary insights, such as finding out how much storage you have across your entire organization, or which are the fastest-growing buckets and prefixes.

8. Thinking about architecting
   - S3 is often behind CloudFront for content delivery
   - S3 is great for static contents, but it can be integrated with a lot of services or trigger events to make a lot dynamic actions happen



API Gateway

Module 3: Adding a Storage Layer

Module wrap-up

Module summary

In summary, in this module, you learned how to:

- Recognize the problems that Amazon Simple Storage Service (Amazon S3) can solve
- Describe how to store content efficiently using Amazon S3
- Recognize the various Amazon S3 storage classes and cost considerations
- Describe how to move data to and from Amazon S3
- Describe how to choose a Region
- Create a static website

prefix