

Experiment 6

Aim

Study and Implement of Storage as a Service (STaaS)

Theory

1. Prepare a detailed study of Storage as a Service (STaaS)

Ans: Storage as a Service or STaaS is cloud storage that you rent from a Cloud Service Provider (CSP) and that provides basic ways to access that storage. Enterprises, small and medium businesses, home offices, and individuals can use the cloud for multimedia storage, data repositories, data backup and recovery, and disaster recovery. There are also higher-tier managed services that build on top of STaaS, such as Database as a Service, in which you can write data into tables that are hosted through CSP resources.

The storage you choose will typically depend on how often you intend to access the data. Cold data storage is data that you leave alone or access infrequently, whereas warm or hot data is accessed regularly and repeatedly. Pricing by quantity tends to be more cost efficient but isn't intended to support fast and frequent access for day-to-day business productivity. For hot or warm data, an SLA will be crucial to leveraging data storage in support of current projects or ongoing processes.

Many CSPs make it easy to onboard and upload data into their STaaS infrastructure for little to no cost at all. However, there may be hidden fees and it can be extremely costly to migrate or transfer your data to a different cloud platform.

2. Advantages and Limitation of STaaS for S3 & S3 Glacier service

Ans: **Advantages of STaaS**

Key advantages to STaaS in the enterprise include the following:

Storage costs. Personnel, hardware and physical storage space expenses are reduced.

- **Disaster recovery.** Having multiple copies of data stored in different locations can better enable disaster recovery measures.
- **Scalability.** With most public cloud services, users only pay for the resources that they use.
- **Syncing.** Files can be automatically synced across multiple devices.
- **Security.** Security can be both an advantage and a disadvantage, as security methods may change per vendor. Data tends to be encrypted during transmission and while at rest.

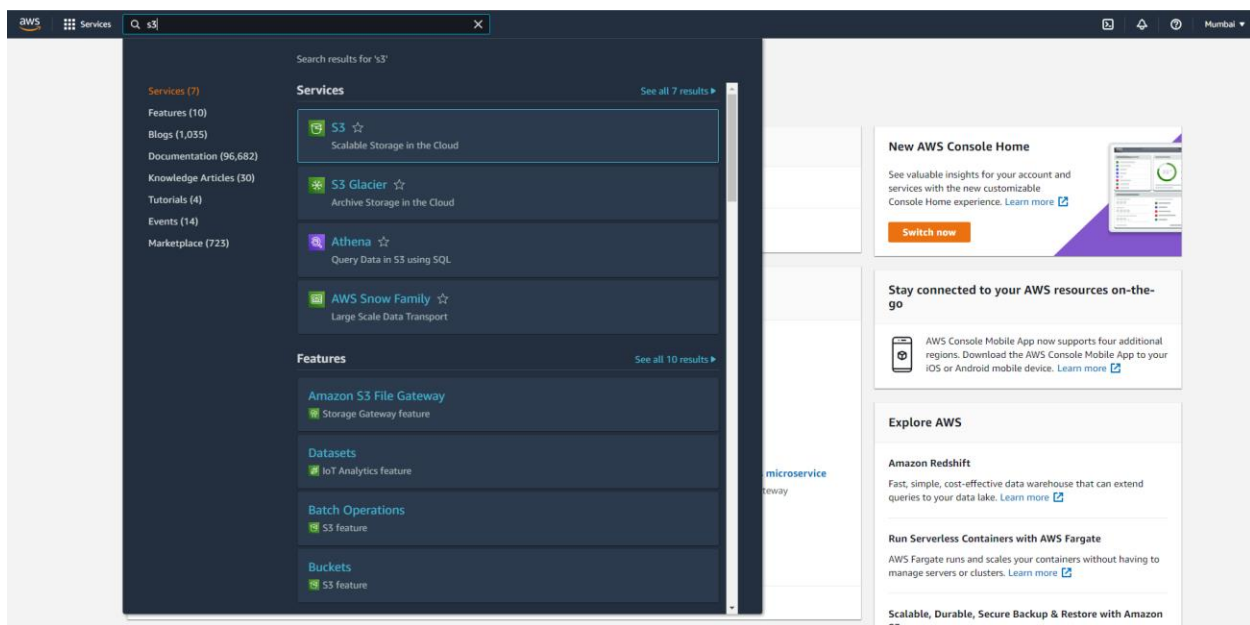
Disadvantages of STaaS

Common disadvantages of STaaS include the following:

- **Security.** Users may end up transferring business-sensitive or mission-critical data to the cloud, which makes it important to choose a service provider that's reliable.
- **Potential storage costs.** If bandwidth limitations are exceeded, these could be expensive.
- **Potential downtimes.** Vendors may go through periods of downtime where the service is not available, which can be trouble for mission-critical data.
- **Limited customization.** Since the [cloud infrastructure](#) is owned and managed by the service provider, it is less customizable.
- **Potential for vendor lock-in.** It may be difficult to migrate from one service to another.

Activity

1. With the help of any suitable cloud service (S3 & S3 Glacier Service) Perform STaaS
2. Use of S3 & S3 Glacier service in AWS (STaaS)



PID: 192120

We're continuing to improve the S3 console to make it faster and easier to use. If you have feedback on the updated experience, choose [Provide feedback](#).

Object Ownership Info

Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.

☒ **ACLs disabled (recommended)**
 All objects in this bucket are owned by this account.
 Access to this bucket and its objects is specified using only policies.

☐ **ACLs enabled**
 Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.

Object Ownership
Bucket owner enforced

Block Public Access settings for this bucket

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to this bucket and its objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to this bucket or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

- ☒ **Block all public access**
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.
 - ☒ **Block public access to buckets and objects granted through new access control lists (ACLs)**
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.
 - ☒ **Block public access to buckets and objects granted through any access control lists (ACLs)**
S3 will ignore all ACLs that grant public access to buckets and objects.
 - ☒ **Block public access to buckets and objects granted through new public bucket or access point policies**
S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.
 - ☒ **Block public and cross-account access to buckets and objects through any public bucket or access point policies**
S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

Name: Keegan Vaz

SEC: TE CMPTN B

Roll No.: 28

PID: 192120

aws

Services

Search for services, features, blogs, docs, and more

[Alt+S]

Global

We're continuing to improve the S3 console to make it faster and easier to use. If you have feedback on the updated experience, choose [Provide feedback](#).

Provide feedback

Amazon S3 > exp6bucket > Upload

Upload

info

Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDK or Amazon S3 REST API. [Learn more](#)

Drag and drop files and folders you want to upload here, or choose [Add files](#), or [Add folders](#).

Files and folders (0)

Remove

Add files

Add folder

All files and folders in this table will be uploaded.

Find by name

< 1 >

Name

Folder

Type

Size

No files or folders

You have not chosen any files or folders to upload.

Destination

Destination

s3://exp6bucket

Destination details

Bucket settings that impact new objects stored in the specified destination.

aws

Services

Search for services, features, blogs, docs, and more

[Alt+S]

Global

We're continuing to improve the S3 console to make it faster and easier to use. If you have feedback on the updated experience, choose [Provide feedback](#).

Provide feedback

Amazon S3 > exp6bucket > Upload

Upload

info

Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDK or Amazon S3 REST API. [Learn more](#)

Drag and drop files and folders you want to upload here, or choose [Add files](#), or [Add folders](#).

Files and folders (1 Total, 8.0 B)

Remove

Add files

Add folder

All files and folders in this table will be uploaded.

Find by name

< 1 >

☐

Name

Folder

Type

Size

☐ abc.txt-

text/plain

8.0 B

Destination

Destination

s3://exp6bucket

Destination details

Bucket settings that impact new objects stored in the specified destination.

Permissions

Grant public access and access to other AWS accounts.

Properties

Specify storage class, encryption settings, tags, and more.

PID: 192120

Services

Search for services, features, blogs, docs, and more

[Alt+S]

Global ▾

We're continuing to improve the S3 console to make it faster and easier to use. If you have feedback on the updated experience, choose [Provide feedback](#).

Upload succeeded

View details below.

Upload: status

The information below will no longer be available after you navigate away from this page.

Summary

Destination
s3://jexp6bucket

Succeeded
✔ 1 file, 8.0 B (100.00%)

Failed
○ 0 files, 0 B (0%)

Files and folders

Configuration

Files and folders (1 Total, 8.0 B)

Find by name

< 1

Name	Folder	Type	Size	Status	Error
abc.txt	-	text/plain	8.0 B	✔ Succeeded	-

Name: Keegan Vaz

SEC: TE CMPN B

Roll No.: 28

PID: 192120

aws

Services

Search for services, features, blogs, docs, and more

[Alt+S]

Global

Amazon S3

Buckets

Access Points

Object Lambda Access Points

Multi-Region Access Points

Batch Operations

Access analyzer for S3

Block Public Access settings for this account

Storage Lens

Dashboards

AWS Organizations settings

Feature spotlight

AWS Marketplace for S3

We're continuing to improve the S3 console to make it faster and easier to use. If you have feedback on the updated experience, choose [Provide feedback](#).

Amazon S3 > exp6bucket > abc.txt

abc.txt

Copy S3 URI

Download

Open

Object actions

Properties

Permissions

Versions

Object overview

Owner

41bcb29b961757a03ff61058ed1895c33a388cedfb9f0f5d85c1fbbd735babcc

AWS Region

Asia Pacific (Mumbai) ap-south-1

Last modified

February 15, 2022, 13:46:22 (UTC+05:30)

Size

8.0 B

Type

txt

Key

abc.txt

S3 URI

s3://exp6bucket/abc.txt

Amazon Resource Name (ARN)

arn:aws:s3::exp6bucket/abc.txt

Entity tag (ETag)

4ff8b4c6ae916f462edad65f84c9fa00

Object URL

https://exp6bucket.s3.ap-south-1.amazonaws.com/abc.txt

Object management overview

The following bucket properties and object management configurations impact the behavior of this object.

Amazon S3

Buckets

Access Points

Object Lambda Access Points

Multi-Region Access Points

Batch Operations

Access analyzer for S3

Block Public Access settings for this account

Storage Lens

Dashboards

AWS Organizations settings

Feature spotlight

AWS Marketplace for S3

We're continuing to improve the S3 console to make it faster and easier to use. If you have feedback on the updated experience, choose [Provide feedback](#).

Amazon S3 > Block Public Access settings for this account

Block Public Access settings for this account

Use Amazon S3 Block public access settings to control the settings that allow public access to your data.

Block Public Access settings for this account

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply account-wide for all current and future buckets and access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

Edit

Block all public access

OFF

Block public access to buckets and objects granted through new access control lists (ACLs)

OFF

Block public access to buckets and objects granted through any access control lists (ACLs)

OFF

Block public access to buckets and objects granted through new public bucket or access point policies

OFF

Block public and cross-account access to buckets and objects through any public bucket or access point policies

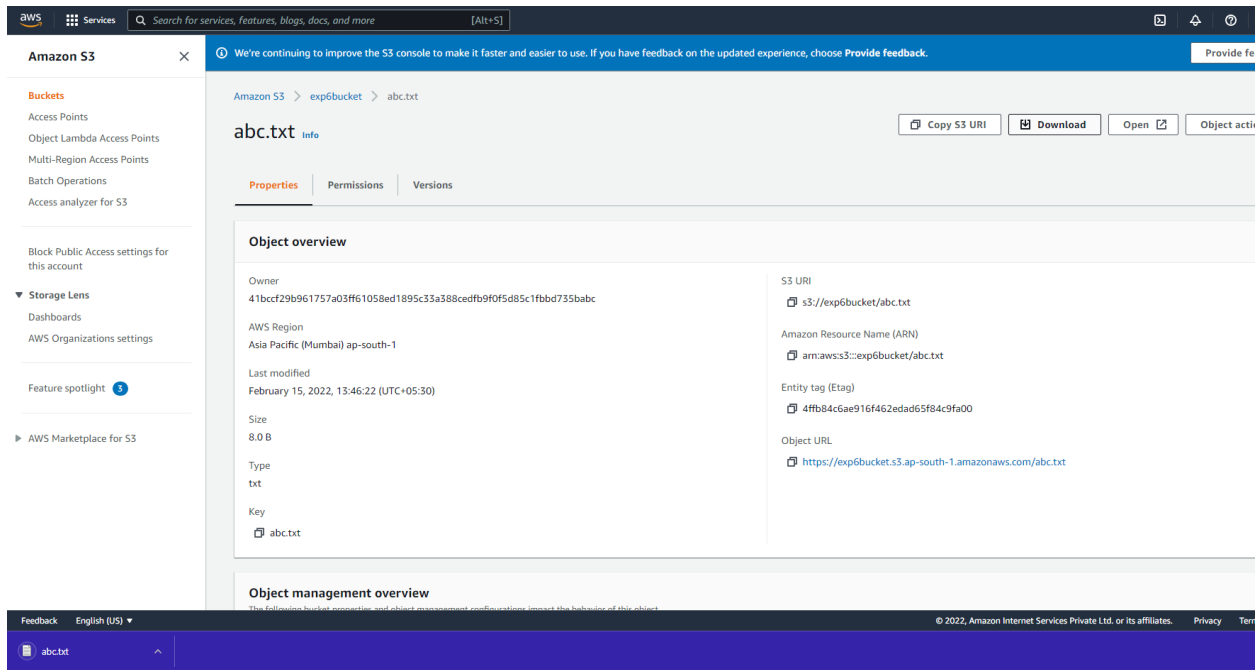
OFF

https://s3.console.aws.amazon.com/s3/settings?region=ap-south-1

© 2022, Amazon Internet Services Private Ltd. or its affiliates. [Privacy](#) [Terms](#) [Cookie p](#)

abc.txt

Share



Conclusion

Demonstrate the CRUD operations on different SQL and NoSQL databases running on cloud

Ans:

SQL databases - MySQL databases:

CREATE -

```
CREATE TABLE table_name (  
    column1 datatype,  
    column2 datatype,  
);
```

READ -

```
CREATE VIEW view_name AS  
SELECT column1, column2, ...  
FROM table_name  
WHERE condition;
```

UPDATE -

```
UPDATE table_name  
SET column1 = value1, column2 = value2, ...  
WHERE condition;
```

DELETE -

```
DELETE FROM table_name  
WHERE condition;
```


NoSQL databases - MongoDB:**CREATE -**

```
{
  create: <collection or view name>,
  capped: <true|false>,
  timeseries: {
    timeField: <string>,
    metaField: <string>,
    granularity: <string>
  },
  expireAfterSeconds: <number>,
  autoIndexId: <true|false>,
  size: <max_size>,
  max: <max_documents>,
  storageEngine: <document>,
  validator: <document>,
  validationLevel: <string>,
  validationAction: <string>,
  indexOptionDefaults: <document>,
  viewOn: <source>,
  pipeline: <pipeline>,
  collation: <document>,
  writeConcern: <document>,
  comment: <any>
}
```

READ -

Use the `db.createCollection()` method or the create command:

```
db.createCollection(
  "<viewName>",
  {
    "viewOn" : "<source>",
    "pipeline" : [<pipeline>],
    "collation" : { <collation> }
  }
)
```

Use the [db.createView\(\)](#) method:

```
db.createView(
  "<viewName>",
  "<source>",
  [<pipeline>],
  {
    "collation" : { <collation> }
  }
)
```

)

UPDATE -

db.collection.update(query, update, options)

DELETE -

```
db.collection.remove(  
  <query>,  
  {  
    justOne: <boolean>,  
    writeConcern: <document>,  
    collation: <document>,  
    let: <document> // Added in MongoDB 5.0  
  }  
)
```

REFERENCES

1. <https://www.intel.com/content/www/us/en/cloud-computing/storage-as-a-service.html>
2. <https://www.techtarget.com/searchstorage/definition/Storage-as-a-Service-SaaS>