Ishita Hardasmalani

C14-2103058

# EXPERIMENT NO . 6

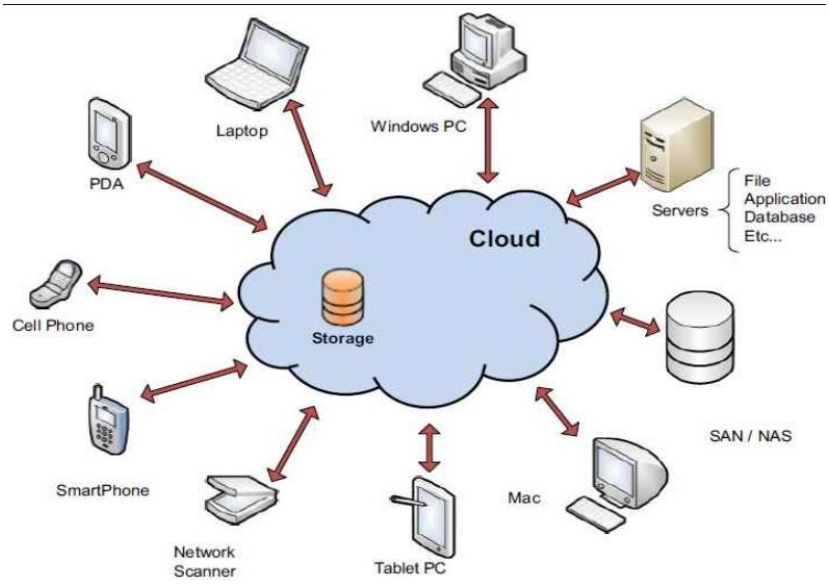
**Aim:** To study and implement Storage as a Service using Own Cloud

## Theory:

Cloud storage is a service model that provides users with the capability to store and access their data over the internet from remote servers, rather than storing it locally on physical hardware such as hard drives or storage devices. It enables users to store large amounts of data, access it from anywhere with an internet connection, and scale their storage needs dynamically without the hassle of managing physical infrastructure.

Key aspects and concepts of cloud storage include:

1. Remote Data Storage: Cloud storage involves storing data on remote servers maintained by cloud service providers. These servers are typically housed in data centers located in various geographic regions around the world.




2. Accessibility: Users can access their stored data from anywhere with an internet connection, using various devices such as computers, smartphones, or tablets. This accessibility facilitates collaboration among distributed teams and enables users to access their data on the go.

3. Scalability: Cloud storage offers scalability, allowing users to increase or decrease their storage capacity as needed without the constraints of physical hardware. This scalability is particularly useful for businesses with fluctuating storage requirements.

4. Redundancy and Reliability: Cloud storage providers implement redundancy measures to ensure data durability and availability. Data is often replicated across multiple servers and data centers to protect against hardware failures, natural disasters, or other disruptions.

5. Security: Cloud storage services typically employ robust security measures to protect data from unauthorized access, including encryption, access controls, and authentication mechanisms. Users can also implement additional security measures such as encryption of data at rest and in transit for added protection.

6. Cost-effectiveness: Cloud storage services operate on a pay-as-you-go or subscription model, allowing users to pay only for the storage resources they consume. This cost-effective pricing model eliminates the need for upfront investment in hardware and allows businesses to align their storage costs with their actual usage.

7. Integration with Other Cloud Services: Cloud storage often integrates seamlessly with other cloud services, such as compute, analytics, and backup services, enabling users to build comprehensive cloud-based solutions tailored to their specific needs.

Overall, cloud storage provides a flexible, scalable, and cost-effective solution for storing and managing data, offering businesses and individuals the ability to leverage the benefits of remote storage without the complexity of managing physical infrastructure.

OwnCloud is an open-source software platform that provides a self-hosted solution for file synchronization and sharing. It allows users to store, access, and share files and folders securely over the internet, providing an alternative to commercial cloud storage services like Dropbox or Google Drive. Here are some of the key features of OwnCloud:

1. File Synchronization: OwnCloud enables users to synchronize files and folders across multiple devices, including desktop computers, laptops, smartphones, and tablets. This ensures that users have access to their files from anywhere, on any device.

2. File Sharing and Collaboration: Users can easily share files and folders with others, both internally within their organization and externally with clients, partners, or collaborators. OwnCloud provides flexible sharing options, allowing users to set permissions and access levels for shared files and folders.

3. Versioning and File Recovery: OwnCloud maintains version history for files, allowing users to track changes and revert to previous versions if needed. This feature is particularly useful for collaboration and ensures data integrity and consistency.

4. Security and Encryption: OwnCloud prioritizes data security and offers robust encryption mechanisms to protect files both in transit and at rest. It supports encryption of data stored on the server and provides options for end-to-end encryption for enhanced privacy and security.

5. User Management and Access Controls: OwnCloud provides comprehensive user management capabilities, allowing administrators to create and manage user accounts, set permissions, and enforce access controls. This ensures that sensitive data remains secure and accessible only to authorized users.

6. Integration with Existing Infrastructure: OwnCloud can be integrated with existing IT infrastructure, including authentication systems such as LDAP or Active Directory, as well as external storage systems like NAS devices or external cloud storage providers. This flexibility makes it easy to deploy OwnCloud in a variety of environments and adapt it to existing workflows.

7. Customization and Extensibility: OwnCloud is highly customizable and extensible, allowing users to tailor the platform to their specific needs and requirements. It supports a wide range of plugins and extensions, as well as custom themes and branding options.

8. Compliance and Data Sovereignty: OwnCloud offers features to help organizations comply with regulatory requirements and maintain data sovereignty. It supports on-premises deployment, giving organizations full control over their data and ensuring compliance with data protection regulations.

Storage as a Service (STaaS) offers various advantages and limitations, which are important to consider when evaluating whether it's the right solution for your storage needs.

**Advantages:**

1. **Scalability**: STaaS allows users to scale their storage resources up or down based on their needs without the hassle of managing physical infrastructure. This scalability ensures that organizations can accommodate growing data volumes without disruptions.

2. **Cost-effectiveness**: STaaS operates on a pay-as-you-go or subscription model, allowing organizations to pay only for the storage resources they consume. This cost-effective pricing model eliminates the need for upfront investment in hardware and reduces operational expenses associated with maintaining and managing storage infrastructure.

3. **Flexibility and Accessibility**: STaaS enables users to access their stored data from anywhere with an internet connection, using various devices such as computers, smartphones, or tablets. This flexibility facilitates collaboration among distributed teams and allows users to access their data on the go.

4. **Redundancy and Reliability**: STaaS providers typically implement redundancy measures to ensure data durability and availability. Data is often replicated across multiple servers and data centers to protect against hardware failures, natural disasters, or other disruptions, ensuring high levels of reliability and data integrity.

5. **Security**: STaaS providers prioritize data security and implement robust security measures to protect data from unauthorized access, including encryption, access controls, and authentication mechanisms. Users can also implement additional security measures such as encryption of data at rest and in transit for added protection.

**Limitations:**

1. **Data Privacy and Compliance Concerns**: Organizations may have concerns about storing sensitive or confidential data in a third-party cloud environment due to regulatory compliance requirements or data privacy concerns. It's essential to ensure that the STaaS provider complies with relevant regulations and standards and offers adequate security and privacy protections.

2. **Dependence on Service Provider**: Organizations relying on STaaS are dependent on the service provider for the availability, performance, and security of their data. Any disruptions or outages on the provider's end could impact access to data and business operations.

3. **Data Transfer Costs**: Transferring large volumes of data in and out of the STaaS environment may incur additional costs, especially if data needs to be migrated between different cloud providers or regions. It's essential to consider data transfer costs when estimating the total cost of ownership.

4. **Limited Control Over Infrastructure**: With STaaS, organizations relinquish control over the underlying storage infrastructure to the service provider. While this reduces the burden of managing physical hardware, it also means that organizations have limited visibility and control over the infrastructure supporting their data.

5. **Potential Vendor Lock-in: Migrating data between different STaaS providers or back to an on-premises environment can be complex and costly, leading to vendor lock-in. Organizations should carefully consider their long-term storage strategy and evaluate the implications of vendor lock-in when choosing a STaaS provider.

Different types of storage technologies serve various purposes and have unique characteristics suited to different use cases. Here's an explanation of some common types of storage:

1. **Object Storage**:

- Object storage is a storage architecture that manages data as objects rather than as blocks or files. Each object typically includes the data itself, metadata, and a unique identifier.

- Objects are stored in a flat hierarchy, making it easy to scale and manage large volumes of data efficiently.

- Object storage is highly scalable and suitable for storing large amounts of unstructured data, such as multimedia files, documents, and backups.

- Examples of object storage services include Amazon S3, Google Cloud Storage, and Azure Blob Storage.

2. **Block Storage**:

- Block storage is a storage architecture that divides data into fixed-sized blocks and stores them as separate volumes.

- Each block is typically treated as an individual hard drive and is accessed through a storage area network (SAN).

- Block storage is ideal for applications that require high-performance and low-latency access to data, such as databases and virtual machines.

- It offers features like data replication, snapshots, and cloning for data protection and management.

- Examples of block storage solutions include Amazon EBS (Elastic Block Store), Google Persistent Disk, and Azure Managed Disks.

3. **File Storage**:

- File storage is a storage architecture that organizes data into hierarchical structures of files and folders, similar to how data is organized on a traditional file system.

- File storage systems typically use network-attached storage (NAS) or distributed file systems to provide shared access to files over a network.

- File storage is suitable for storing and sharing documents, media files, and other types of structured data.

- It supports features like file-level access control, quotas, and file locking for collaborative workloads.

- Examples of file storage solutions include NFS (Network File System), SMB (Server Message Block), and distributed file systems like Hadoop HDFS and Lustre.

4. **Object-Block-File Hybrid Storage**:

- Some storage solutions combine elements of object, block, and file storage to provide a versatile and flexible storage platform.

- These hybrid storage systems offer the benefits of object storage scalability, block storage performance, and file storage simplicity.

- Hybrid storage solutions are often used in environments with diverse storage requirements, allowing users to tailor storage configurations to specific workloads.

- Examples of hybrid storage solutions include Ceph, OpenStack Swift, and EMC Isilon.

Certainly! Here are five popular storage-as-a-service vendors along with their services, including Amazon S3:

1. **Amazon Web Services (AWS)**:

- **Amazon S3 (Simple Storage Service)**: Amazon S3 is an object storage service that offers scalable storage for data storage and retrieval. It provides highly durable, available, and secure storage for a wide variety of use cases, including data lakes, backup and restore, content distribution, and application data storage.

- **Amazon EBS (Elastic Block Store)**: Amazon EBS provides block-level storage volumes that can be attached to EC2 instances for persistent storage. It is suitable for databases, transactional workloads, and applications that require low-latency access to data.

- **Amazon EFS (Elastic File System)**: Amazon EFS offers fully managed, scalable file storage for EC2 instances and on-premises servers. It provides shared access to files across multiple instances and supports NFSv4 protocol, making it suitable for file-based workloads, content management, and data analytics.

- **Amazon Glacier**: Amazon Glacier is a low-cost storage service designed for long-term archival and backup of data. It offers three retrieval options (Expedited, Standard, and Bulk) with varying retrieval times and costs, making it suitable for data archiving, compliance, and regulatory requirements.

- **Amazon FSx**: Amazon FSx provides fully managed file storage services for Windows and Lustre file systems. It offers high-performance file storage with features like data deduplication, encryption, and automatic backups, making it suitable for Windows applications, HPC workloads, and data processing.

2. **Microsoft Azure**:

- **Azure Blob Storage**: Azure Blob Storage is a scalable object storage service for storing and serving large amounts of unstructured data, including documents, images, videos, and backups. It offers multiple storage tiers, including hot, cool, and archive, with varying performance and cost characteristics.

- **Azure Disk Storage**: Azure Disk Storage provides managed disk storage for virtual machines in Azure. It offers different disk types (Standard HDD, Standard SSD, Premium SSD) and sizes, suitable for a wide range of workloads, including databases, analytics, and virtual machines.

- **Azure Files**: Azure Files offers fully managed file shares in the cloud, accessible via SMB (Server Message Block) protocol. It provides shared access to files across multiple VMs and on-premises servers, making it suitable for file-based applications and shared storage scenarios.

- **Azure Archive Storage**: Azure Archive Storage is a low-cost storage tier for long-term data retention and archival. It offers low storage costs and retrieval fees, making it suitable for compliance, regulatory, and backup/archival use cases.

- **Azure NetApp Files**: Azure NetApp Files provides high-performance, enterprise-grade file storage powered by NetApp technology. It offers features like snapshots, replication, and data encryption, making it suitable for performance-sensitive workloads, databases, and enterprise applications.

3. **Google Cloud Platform (GCP)**:

- **Google Cloud Storage (GCS)**: Google Cloud Storage is an object storage service for storing and accessing data in the cloud. It offers multiple storage classes, including Standard, Nearline, Coldline, and Archive, with varying availability, durability, and cost characteristics.

- **Google Persistent Disk**: Google Persistent Disk provides block storage for virtual machine instances in GCP. It offers SSD and HDD options with different performance levels and features like snapshots and encryption, suitable for databases, analytics, and virtual machines.

- **Google Filestore**: Google Filestore offers managed file storage services for applications that require shared file systems. It supports both

NFS and SMB protocols, providing high throughput and low latency access to files for compute instances.

- **Google Cloud Storage for Firebase**: Google Cloud Storage for Firebase is a scalable object storage solution for mobile and web applications. It offers features like user authentication, access controls, and integration with Firebase services, making it suitable for app development and content management.

- **Google Cloud Storage Transfer Service**: Google Cloud Storage Transfer Service allows users to securely transfer data from on-premises or other cloud providers to Google Cloud Storage. It supports one-time transfers, periodic transfers, and transfers with scheduling and monitoring capabilities.

4. **IBM Cloud**:

- **IBM Cloud Object Storage**: IBM Cloud Object Storage is a scalable object storage service for storing and accessing unstructured data. It offers features like data encryption, geo-dispersed data protection, and integration with other IBM Cloud services, suitable for analytics, AI, and data-intensive workloads.

- **IBM Cloud Block Storage**: IBM Cloud Block Storage provides block-level storage volumes for virtual servers in IBM Cloud. It offers different performance tiers and replication options, suitable for databases, transactional workloads, and enterprise applications.

- **IBM Cloud File Storage**: IBM Cloud File Storage offers fully managed file storage services for cloud-native applications. It provides NFS and SMB file shares with high availability, scalability, and data encryption, suitable for file-based applications and collaboration workloads.

- **IBM Cloud Object Storage for Archiving**: IBM Cloud Object Storage for Archiving is a low-cost storage solution for long-term data retention and archival. It offers immutable object locking, data encryption, and compliance features, making it suitable for regulatory compliance and data governance.

- **IBM Cloud VPC Block Storage**: IBM Cloud VPC Block Storage provides high-performance block storage volumes for virtual servers in IBM Cloud Virtual Private Clouds (VPCs). It offers features like encryption, snapshots,

and replication, suitable for mission-critical workloads and enterprise applications.

5. **Oracle Cloud Infrastructure (OCI)**:

- **Oracle Cloud Object Storage**: Oracle Cloud Object Storage is a scalable, durable, and highly available object storage service for storing and managing data in the cloud. It offers features like data encryption, lifecycle management, and versioning, suitable for data backup, archive, and content management.

- **Oracle Cloud Block Volume**: Oracle Cloud Block Volume provides high-performance block storage for compute instances in Oracle Cloud Infrastructure. It offers different performance tiers, encryption, and backup options, suitable for databases, analytics, and enterprise applications.

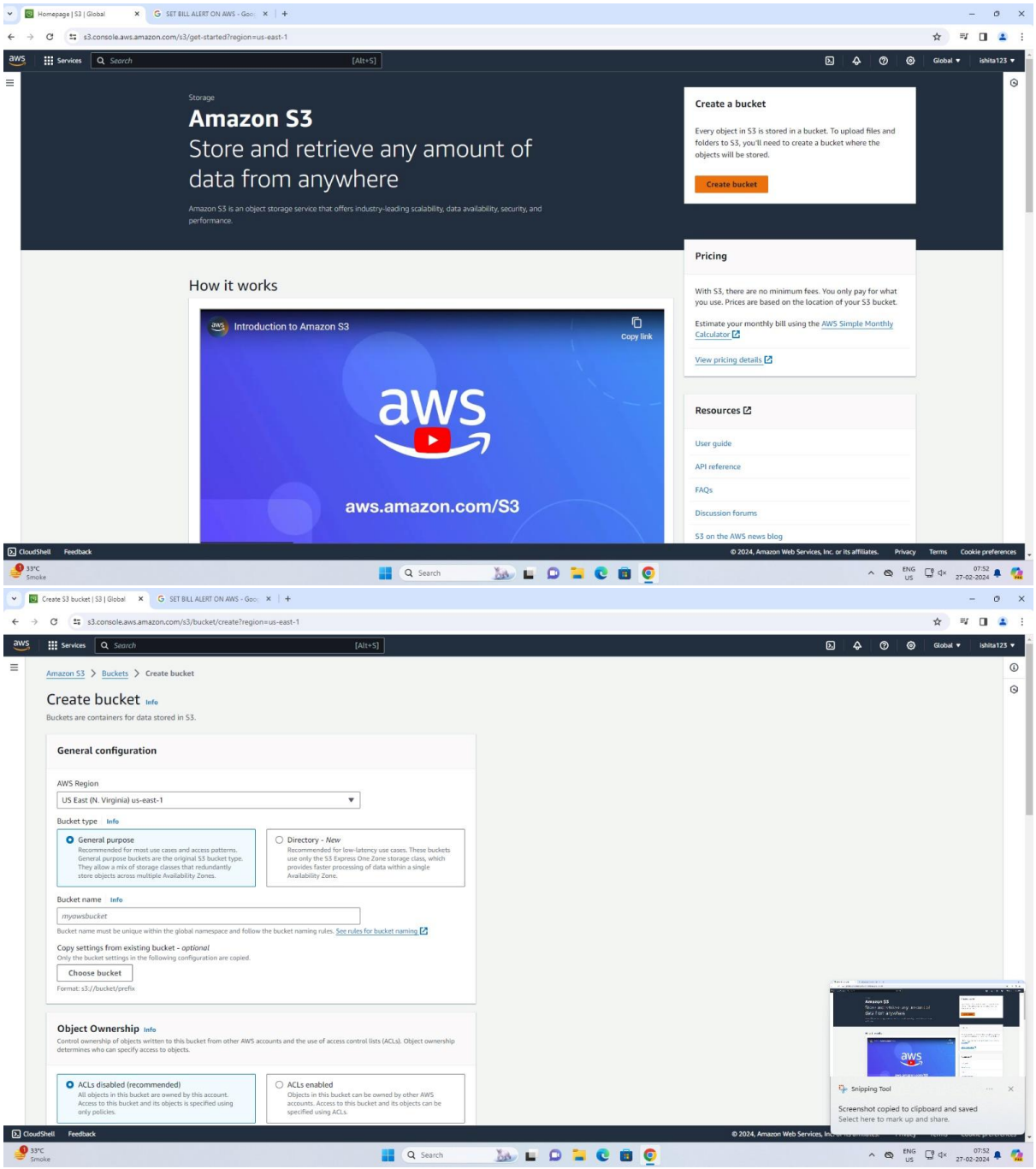
- **Oracle Cloud File Storage**: Oracle Cloud File Storage offers fully managed, NFS-based file storage services for applications and workloads that require shared file systems. It provides features like snapshots, encryption, and access controls, suitable for file-based applications and collaboration workloads.

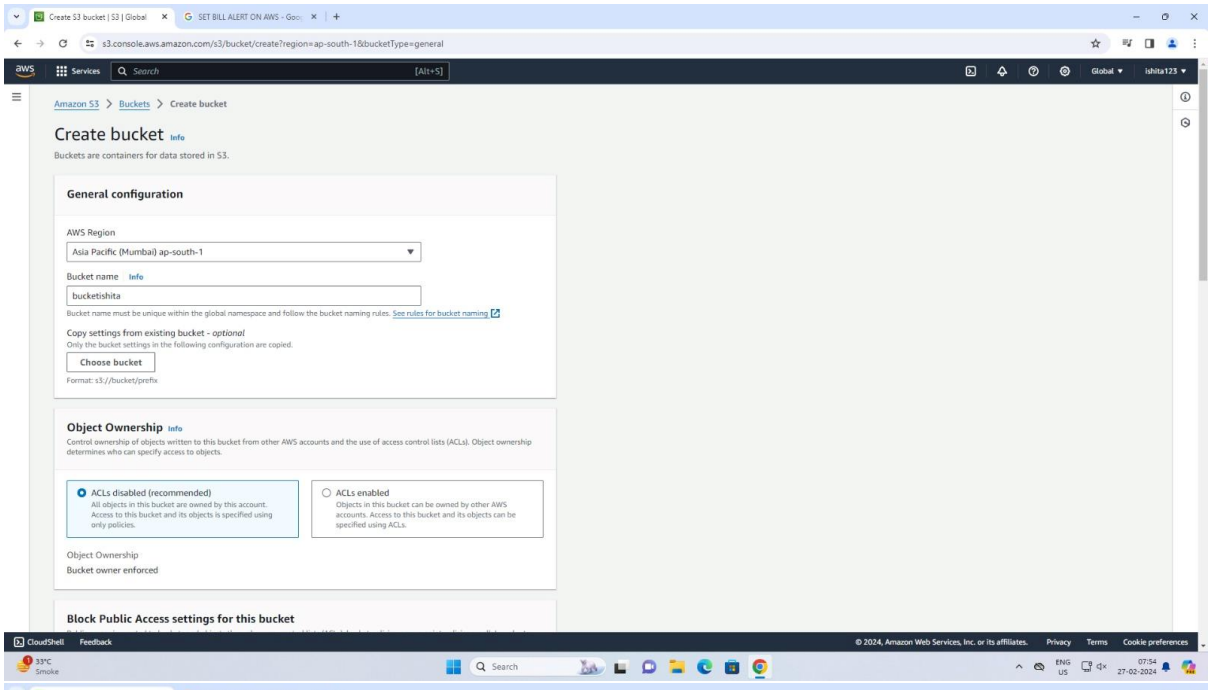
- **Oracle Cloud Archive Storage**: Oracle Cloud Archive Storage is a low-cost storage solution for long-term data retention and archival. It offers low storage costs, retrieval fees, and durability, making it suitable for compliance, regulatory, and backup/archival use cases.

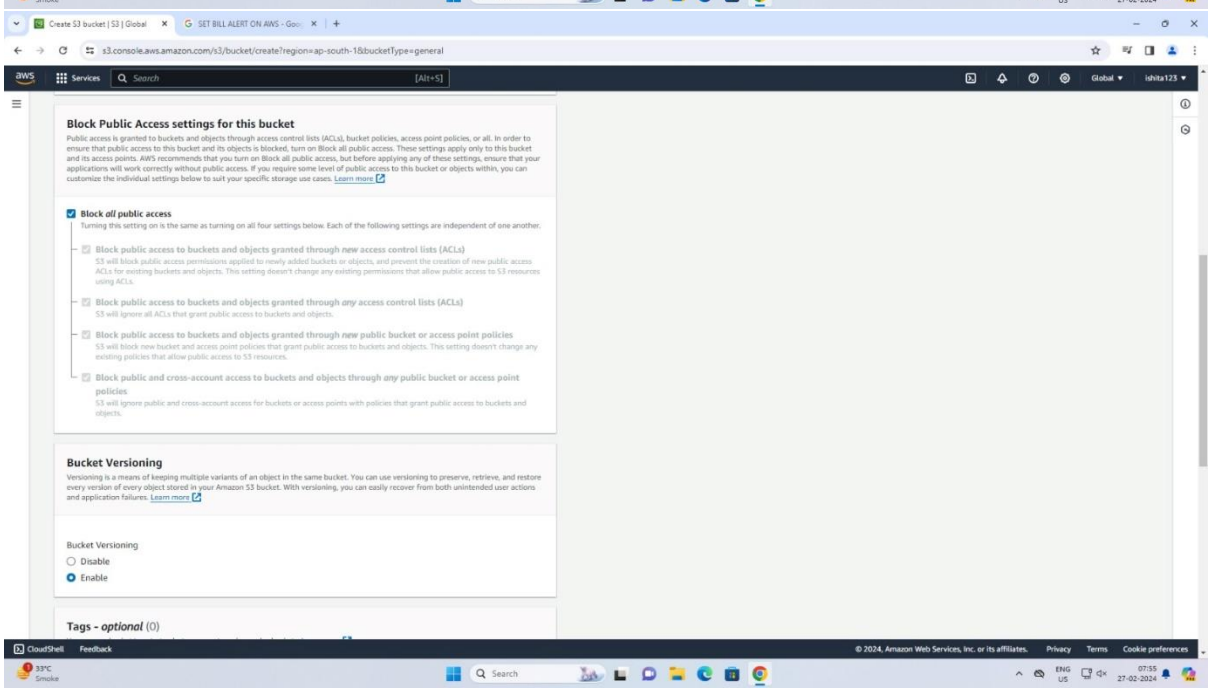
- **Oracle Cloud Storage Gateway**: Oracle Cloud Storage Gateway enables hybrid cloud storage deployments by providing seamless integration between on-premises environments and Oracle Cloud Storage. It supports file, block, and object storage protocols, enabling data migration, backup, and disaster recovery scenarios.

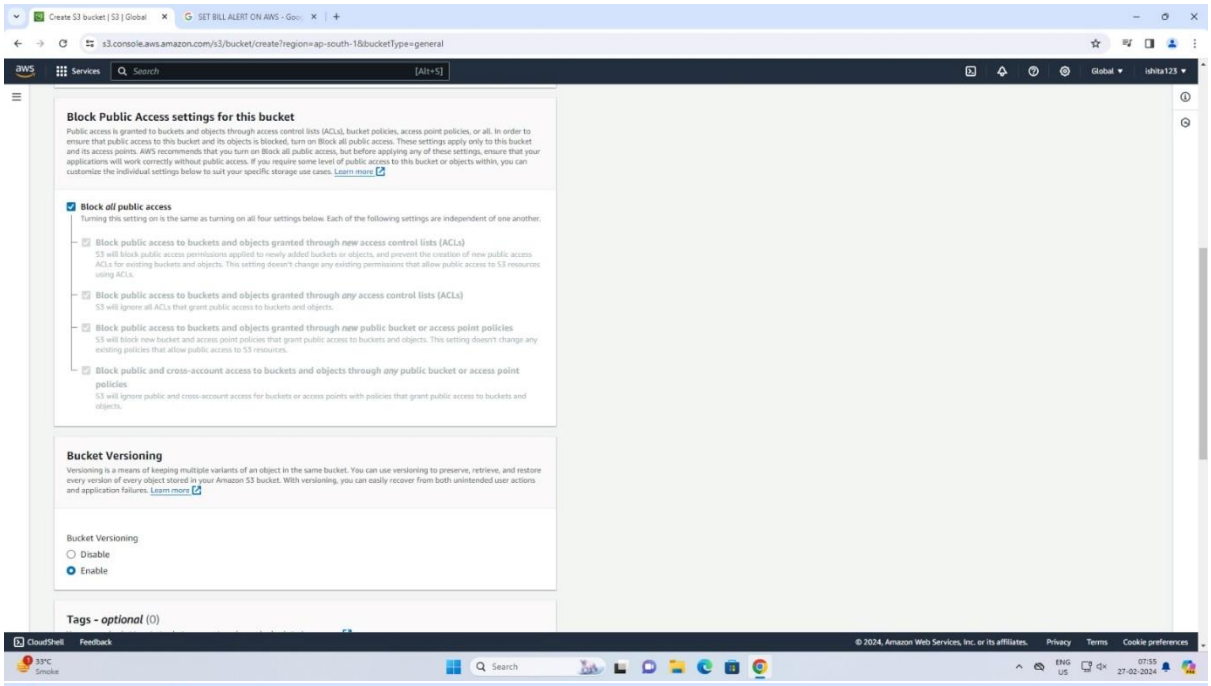
Implementation:

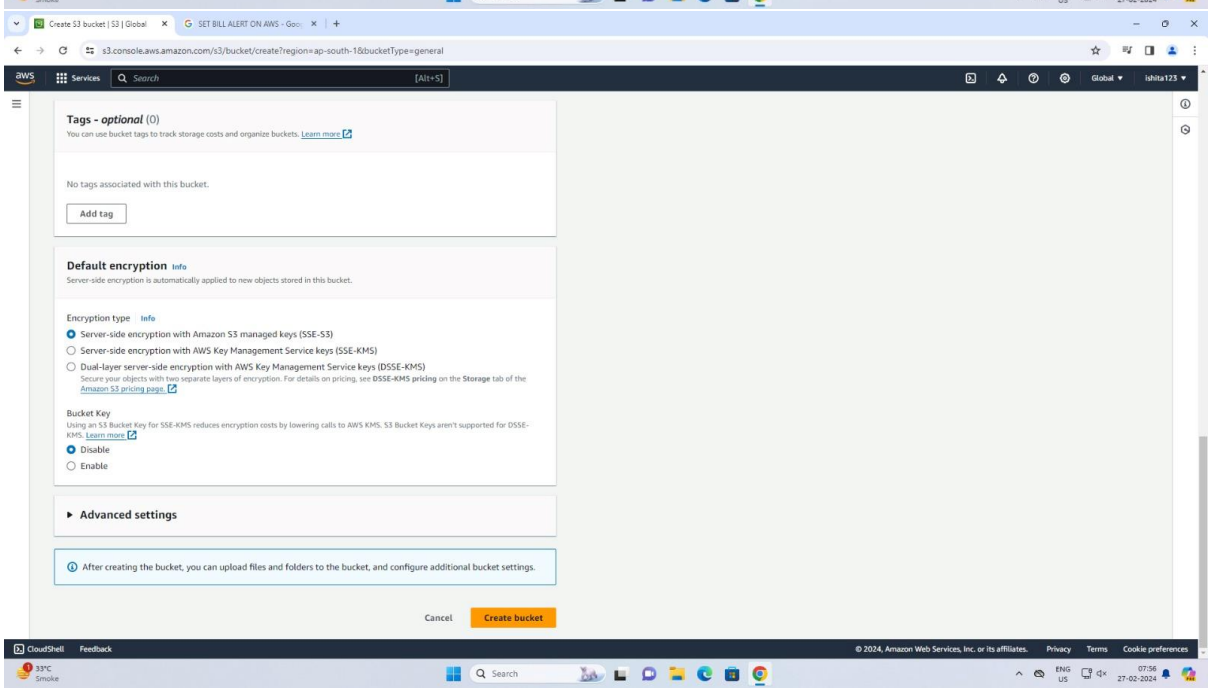
1. Craete S3 bucket

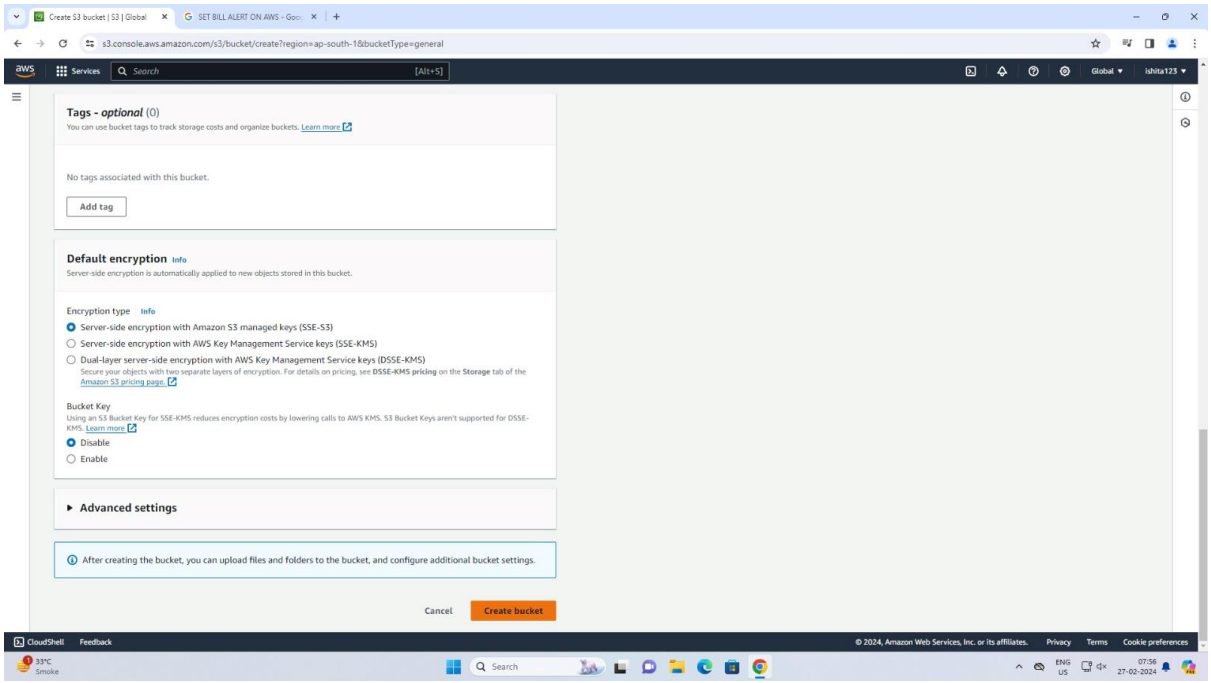



Create S3 bucket | S3 | Global
SET BILL ALERT ON AWS - Goo
s3.console.aws.amazon.com/s3/bucket/create?region=ap-south-1&bucketType=general
Services
Search
[Alt+S]
Global
ishita123
Amazon S3 > Buckets > Create bucket
Create bucket Info
Buckets are containers for data stored in S3.
General configuration
AWS Region
Asia Pacific (Mumbai) ap-south-1
Bucket name Info
bucketishita
Bucket name must be unique within the global namespace and follow the bucket naming rules. See rules for bucket naming
Copy settings from existing bucket - optional
Only the bucket settings in the following configuration are copied.
Choose bucket
Format: s3://bucket/prefix
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
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
33°C
Smoke
Search
ENG
US
07:54
27-02-2024

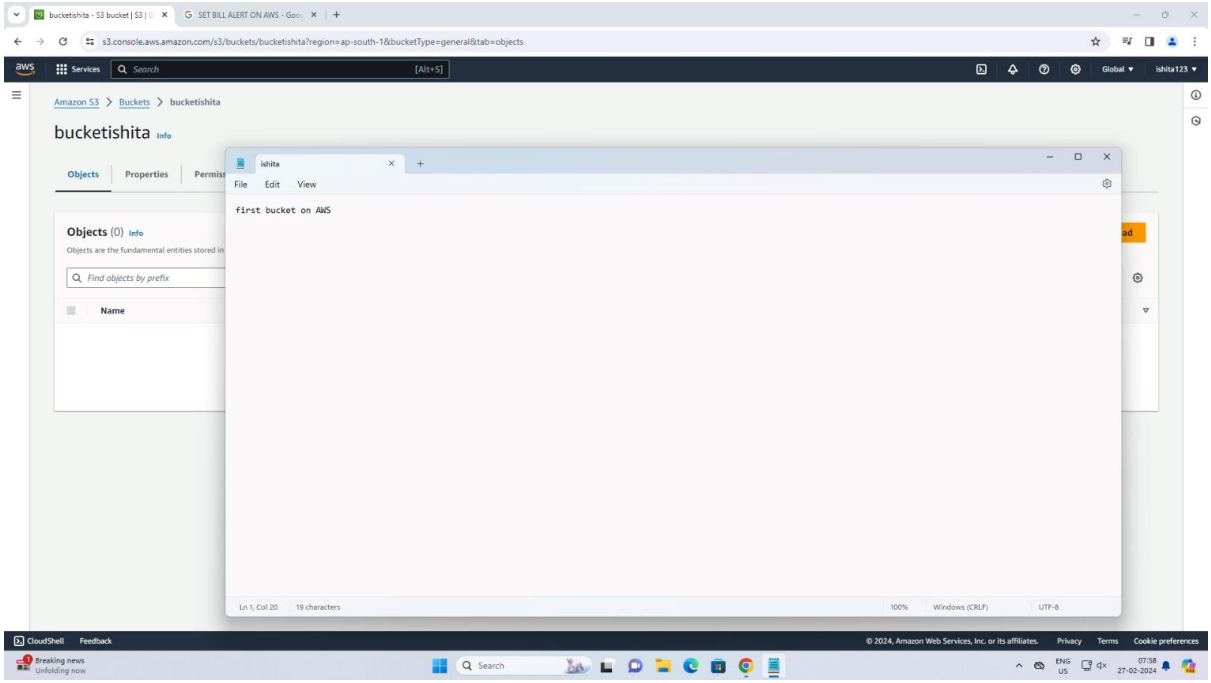

Create S3 bucket | S3 | Global
SET BILL ALERT ON AWS - Goo
s3.console.aws.amazon.com/s3/bucket/create?region=ap-south-1&bucketType=general
Services
Search
[Alt+S]
Global
ishita123
Block Public Access settings for this bucket
Public access is granted to buckets and objects through access control lists (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.
Bucket Versioning
Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. Learn more
Bucket Versioning
Disable
Enable
Tags - optional (0)
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
33°C
Smoke
Search
ENG
US
07:55
27-02-2024

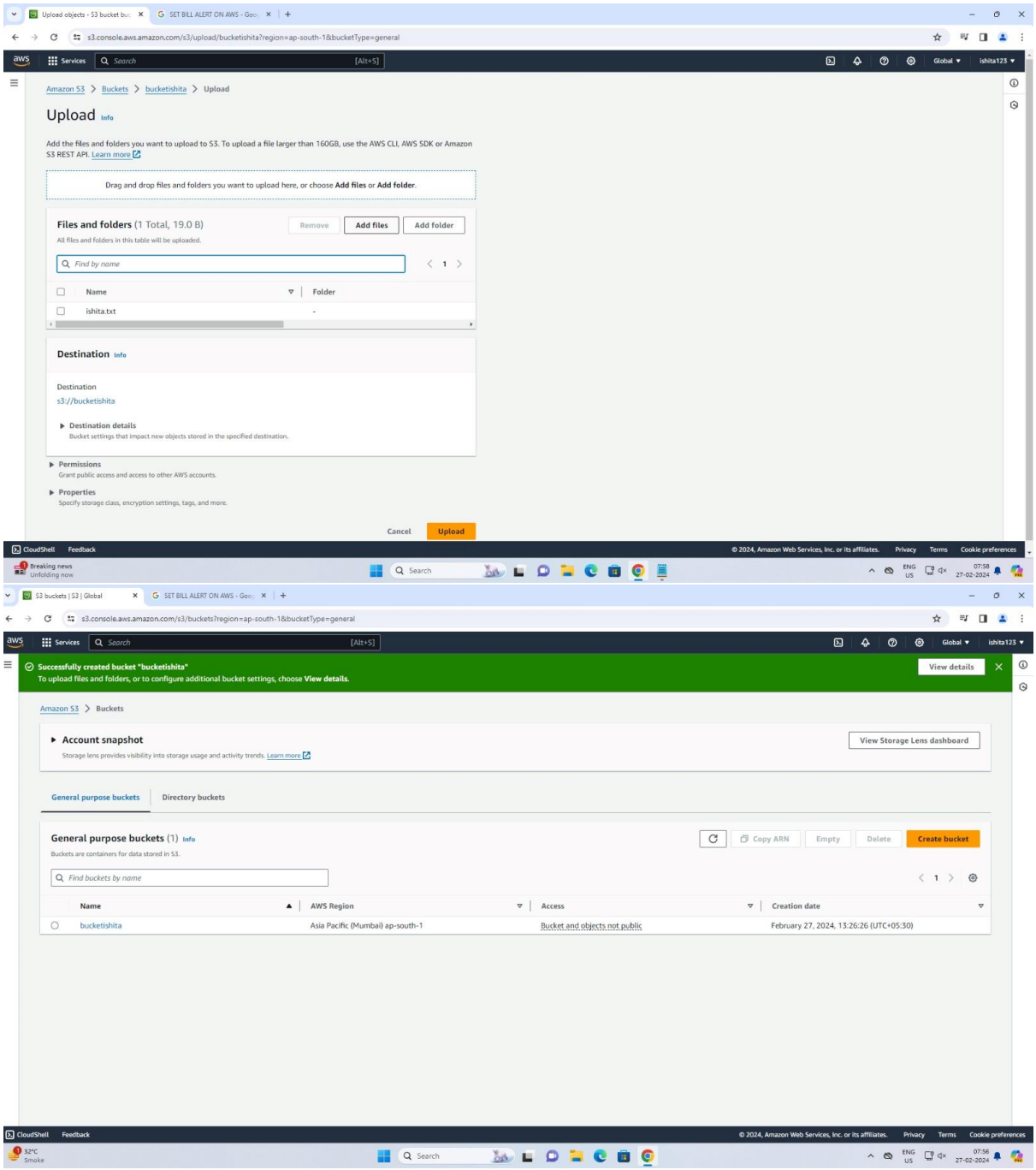

Create S3 bucket | S3 | Global
SET BILL ALERT ON AWS - Goo
s3.console.aws.amazon.com/s3/bucket/create?region=ap-south-1&bucketType=general
Services
Search
[Alt+S]
Global
ishita123
Block Public Access settings for this bucket
Public access is granted to buckets and objects through access control lists (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.
Bucket Versioning
Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. Learn more
Bucket Versioning
Disable
Enable
Tags - optional (0)
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
33°C
Smoke
Search
ENG
US
07:55
27-02-2024


Create S3 bucket | S3 | Global
SET BILL ALERT ON AWS - Goo
s3.console.aws.amazon.com/s3/bucket/create?region=ap-south-1&bucketType=general
Services
Search
[Alt+S]
Global
ishita123
Tags - optional (0)
You can use bucket tags to track storage costs and organize buckets. Learn more
No tags associated with this bucket.
Add tag
Default encryption Info
Server-side encryption is automatically applied to new objects stored in this bucket.
Encryption type Info
Server-side encryption with Amazon S3 managed keys (SSE-S3)
Server-side encryption with AWS Key Management Service keys (SSE-KMS)
Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)
Secure your objects with two separate layers of encryption. For details on pricing, see DSSE-KMS pricing on the Storage tab of the Amazon S3 pricing page.
Bucket Key
Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSSE-KMS. Learn more
Disable
Enable
Advanced settings
After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.
Cancel
Create bucket
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
33°C
Smoke
Search
ENG
US
07:56
27-02-2024

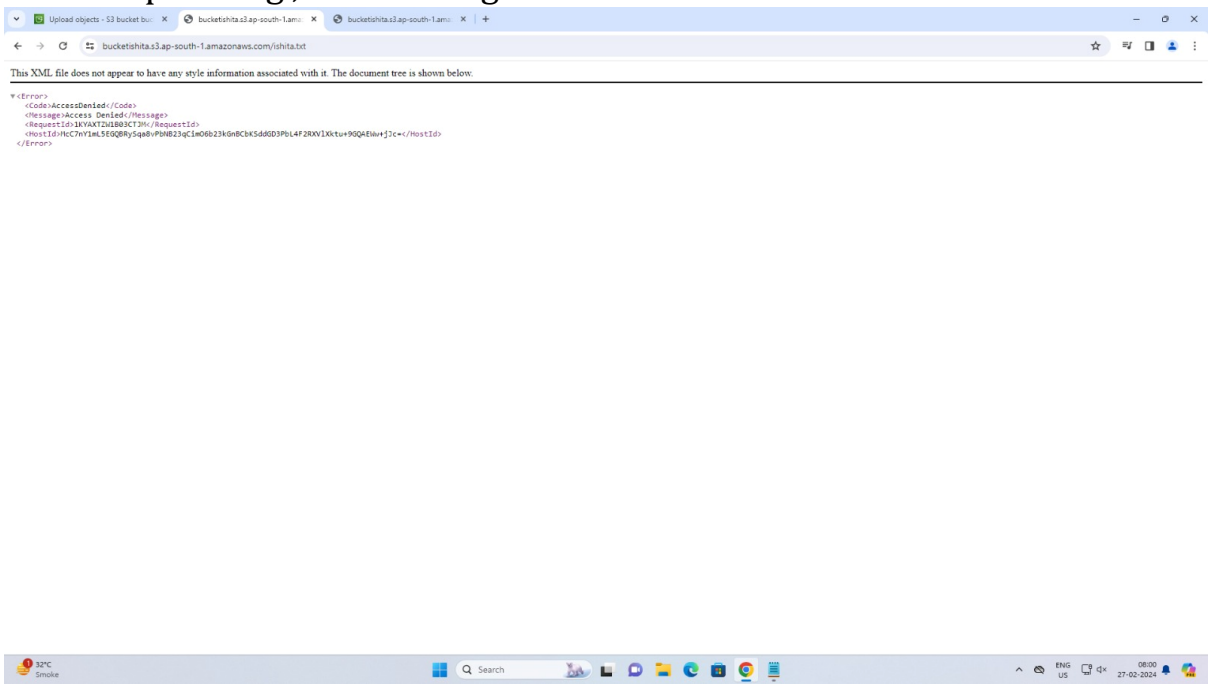



# 2.create a text file to be uploaded

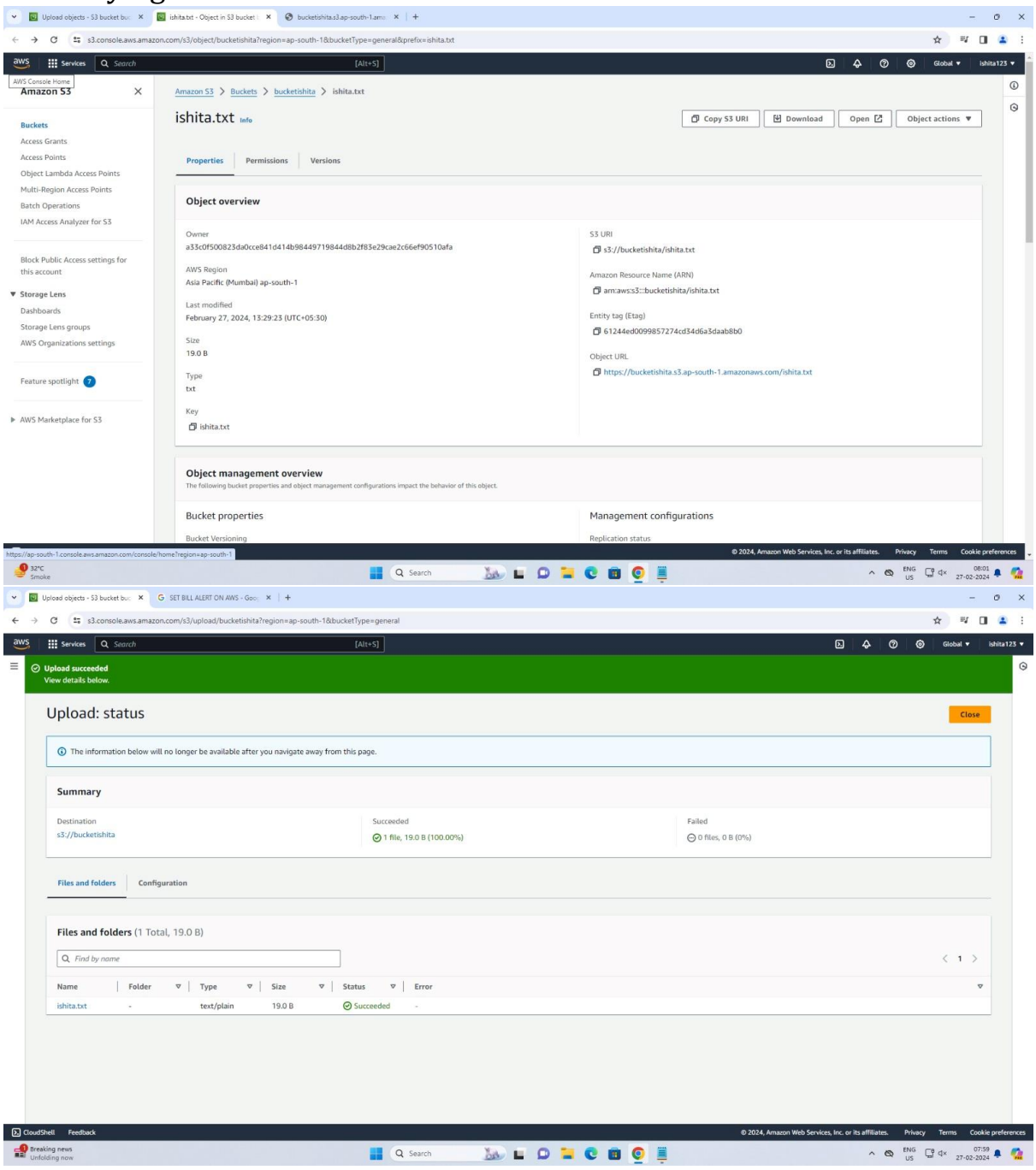



Upload objects - S3 bucket buc
SET BILL ALERT ON AWS - Goo
s3.console.aws.amazon.com/s3/upload/bucketishita?region=ap-south-1&bucketType=general
Services
Search
[Alt+S]
Global
ishita123
Amazon S3 > Buckets > bucketishita > Upload
Upload Info
Add the files and folders you want to upload to S3. To upload 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 folder.
Files and folders (1 Total, 19.0 B)
Remove
Add files
Add folder
All files and folders in this table will be uploaded.
Find by name
Name
Folder
ishita.txt
Destination Info
Destination
s3://bucketishita
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.
Cancel
Upload
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Breaking news
Unfolding now
Search
ENG
US
07:58
27-02-2024
S3 buckets | S3 | Global
SET BILL ALERT ON AWS - Goo
s3.console.aws.amazon.com/s3/buckets?region=ap-south-1&bucketType=general
Services
Search
[Alt+S]
Global
ishita123
Successfully created bucket "bucketishita"
To upload files and folders, or to configure additional bucket settings, choose View details.
View details
Amazon S3 > Buckets
Account snapshot
Storage lens provides visibility into storage usage and activity trends. Learn more
View Storage Lens dashboard
General purpose buckets
Directory buckets
General purpose buckets (1) Info
Buckets are containers for data stored in S3.
Copy ARN
Empty
Delete
Create bucket
Find buckets by name
Name
AWS Region
Access
Creation date
bucketishita
Asia Pacific (Mumbai) ap-south-1
Bucket and objects not public
February 27, 2024, 13:26:26 (UTC+05:30)
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
32°C
Smoke
Search
ENG
US
07:56
27-02-2024

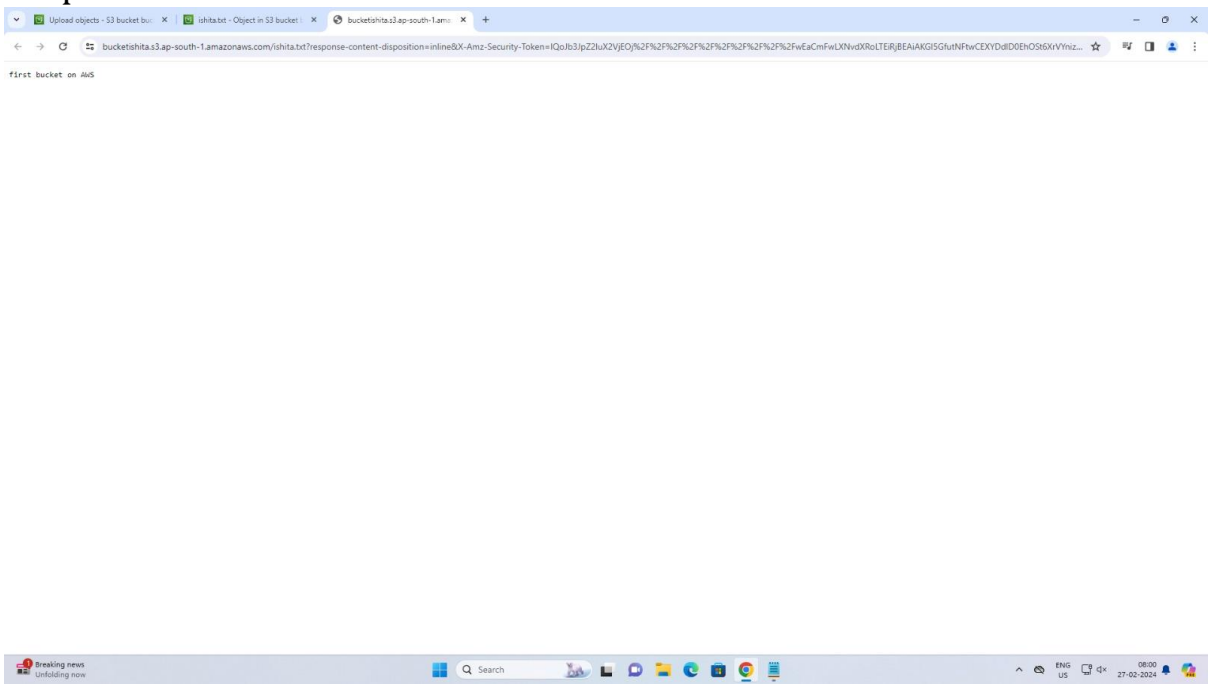
3. after uploading , error for rights



# 4.Modifying it



# Output:


Upload objects - S3 bucket buc
ishita.txt - Object in S3 bucket
bucketishita.s3.ap-south-1.ama
bucketishita.s3.ap-south-1.amazonaws.com/ishita.txt?response-content-disposition=inline&X-Amz-Security-Token=IQoJb3JpZ2luX2VjEOj%2F%2F%2F%2F%2F%2F%2F%2F%2F%2FwEaCmFwLXNvdXRoLTEiRjBEAiAKGI5GfutNFtwCEXYDdlD0EhOSt6XrVYniz...
first bucket on AWS
Breaking news
Unfolding now
Search
ENG
US
08:00
27-02-2024