



Create S3 bucket | S3 | Global Pipelines - Recent Upload files : janardhana.papolu

s3.console.aws.amazon.com/s3/bucket/create?region=ap-south-1&bucketType=general

aws Services Search [Alt+S] Global janardhana.papolu

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 (1)

You can use bucket tags to track storage costs and organize buckets. [Learn more](#)

Key Value - optional
Mybucket Dotnet

CloudShell Feedback Type here to search © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences 30°C 12:27 18-01-2024

Create S3 bucket | S3 | Global Pipelines - Recent Upload files : janardhana.papolu

s3.console.aws.amazon.com/s3/bucket/create?region=ap-south-1&bucketType=general

aws Services Search [Alt+S] Global janardhana.papolu

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.

CloudShell Feedback Type here to search © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences 30°C 12:27 18-01-2024

Create S3 bucket | S3 | Global Pipelines - Recent Upload files : janardhana.papolu

s3.console.aws.amazon.com/s3/bucket/create?region=ap-south-1&bucketType=general

aws Services Search [Alt+S] Global janardhana.papolu

Advanced settings

Object Lock

Store objects using a write-once-read-many (WORM) model to help you prevent objects from being deleted or overwritten for a fixed amount of time or indefinitely. Object Lock works only in versioned buckets. [Learn more](#)

Disable Enable
Permanently allows objects in this bucket to be locked. Additional Object Lock configuration is required in bucket details after bucket creation to protect objects in this bucket from being deleted or overwritten.

Object Lock works only in versioned buckets. Enabling Object Lock automatically enables Versioning.

After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.

CloudShell Feedback Type here to search © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences 30°C 12:29 18-01-2024

Screenshot of the AWS S3 console showing the creation of a new bucket named "janasbucket".

General configuration:

- AWS Region: Asia Pacific (Mumbai) ap-south-1
- Bucket name: janasbucket
- Copy settings from existing bucket - optional: Only the bucket settings in the following configuration are copied.
- Choose bucket: Format: s3://bucket/prefix

Object Ownership:

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.

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.

Success message: Successfully created bucket "janasbucket". To upload files and folders, or to configure additional bucket settings, choose [View details](#).

Buckets Overview:

Amazon S3 > Buckets

Account snapshot: Storage lens provides visibility into storage usage and activity trends. [Learn more](#)

General purpose buckets:

Name	AWS Region	Access	Creation date
janasbucket	Asia Pacific (Mumbai) ap-south-1	Objects can be public	January 18, 2024, 12:30:00 (UTC-05:30)

S3 buckets | S3 | Global Pipelines - Recent Upload files :janardhana-pap... +

s3.console.aws.amazon.com/s3/buckets?region=ap-south-1&bucketType=general

aws Services Search [Alt+S] Global janardhana.papolu

Successfully created bucket "janasbucket". To upload files and folders, or to configure additional bucket settings, choose View details.

View details

Account snapshot

Storage lens provides visibility into storage usage and activity trends. Learn more

General purpose buckets Directory buckets

General purpose buckets (1) Info Buckets are containers for data stored in S3. Learn more

Find buckets by name

Name AWS Region Access Creation date

janasbucket Asia Pacific (Mumbai) ap-south-1 Objects can be public January 18, 2024, 12:30:00 (UTC+05:30)

CloudShell Feedback Type here to search Pipelines - Recent Upload files :janardhana-pap... +

s3.console.aws.amazon.com/s3/buckets/janasbucket?region=ap-south-1&bucketType=general&tab=objects

aws Services Search [Alt+S] Global janardhana.papolu

Amazon S3 > Buckets > janasbucket

janasbucket Info

Objects (0) Info

Copy Copy S3 URI Copy URL Download Open Delete Actions Create folder Upload

Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

Find objects by prefix Show versions

Name Type Last modified Size Storage class

No objects You don't have any objects in this bucket.

CloudShell Feedback Type here to search Pipelines - Recent Upload files :janardhana-pap... +

s3.console.aws.amazon.com/s3/upload/janasbucket?region=ap-south-1&bucketType=general

aws Services Search [Alt+S] Global janardhana.papolu

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, 1.7 MB)

All files and folders in this table will be uploaded.

Find by name

Folder Type Size

dhana-Aws-instance.pdf application/pdf 1.7 MB

Destination Info

Destination c://janardhanabucket

CloudShell Feedback Type here to search Pipelines - Recent Upload files :janardhana-pap... +

Upload objects - S3 bucket Jan... Pipelines - Recent Upload files - janardhana-pap... +

s3.console.aws.amazon.com/s3/upload/janabucket?region=ap-south-1&bucketType=general

aws Services Search [Alt+S] Global janardhana.papolu

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.

Storage class [Info](#)
Amazon S3 offers a range of storage classes designed for different use cases. [Learn more](#) or see [Amazon S3 pricing](#)

Storage class	Designed for	Bucket type	Availability Zones
S3 Express One Zone	Single-digit millisecond response times for the most frequently accessed data.	Directory	1
Standard	Frequently accessed data (more than once a month) with milliseconds access	General purpose	≥ 3
Intelligent-	Data with changing or unknown access	General	≥ 3

CloudShell Feedback Type here to search © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences 30°C 12:33 ENG 18-01-2024

Upload objects - S3 bucket Jan... Pipelines - Recent Upload files - janardhana-pap... +

s3.console.aws.amazon.com/s3/upload/janabucket?region=ap-south-1&bucketType=general

aws Services Search [Alt+S] Global janardhana.papolu

Server-side encryption [Info](#)
Server-side encryption protects data at rest.

Server-side encryption

- Do not specify an encryption key**
The bucket settings for default encryption are used to encrypt objects when storing them in Amazon S3.
- Specify an encryption key**
The specified encryption key is used to encrypt objects before storing them in Amazon S3.

If your bucket policy requires objects to be encrypted with a specific encryption key, you must specify the same encryption key when you upload objects. Otherwise, uploads will fail.

Additional checksums [Info](#)
Checksum functions are used for additional data integrity verification of new objects. [Learn more](#)

Additional checksums

CloudShell Feedback Type here to search © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences 30°C 12:33 ENG 18-01-2024

Upload objects - S3 bucket Jan... Pipelines - Recent Upload files - janardhana-pap... +

s3.console.aws.amazon.com/s3/upload/janabucket?region=ap-south-1&bucketType=general

aws Services Search [Alt+S] Global janardhana.papolu

Tags - optional
You can use object tags to analyze, manage, and specify permissions for objects. [Learn more](#)

No tags associated with this resource.

Add tag

Metadata - optional
Metadata is optional information provided as a name-value (key-value) pair. [Learn more](#)

No metadata associated with this resource.

Add metadata

Cancel **Upload**

CloudShell Feedback Type here to search © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences 30°C 12:33 ENG 18-01-2024

Upload objects - S3 bucket Janardhana-Aws-instance

Pipelines - Recent

Upload files - janardhana-papolu

s3.console.aws.amazon.com/s3/upload/janabucket?region=ap-south-1&bucketType=general

aws Services Search [Alt+S]

Global janardhana.papolu

Upload succeeded
View details below.

Destination: s3://janabucket
Succeeded: 1 file, 1.7 MB (100.00%)
Failed: 0 files, 0 B (0%)

Files and folders | Configuration

Files and folders (1 Total, 1.7 MB)

Name	Folder	Type	Size	Status	Error
Janardhana-Aws-...	-	application/...	1.7 MB	Succeeded	-

CloudShell Feedback

Type here to search

Janabucket - S3 bucket [S3] | **Pipelines - Recent** | **Upload files - janardhana-papolu**

s3.console.aws.amazon.com/s3/buckets/janabucket?region=ap-south-1&bucketType=general&tab=objects

aws Services Search [Alt+S]

Global janardhana.papolu

Amazon S3 > Buckets > janabucket

janabucket Info

Objects (1) Info

Name	Type	Last modified	Size	Storage class
Janardhana-Aws-...	pdf	January 18, 2024, 12:33:55 (UTC+05:30)	1.7 MB	Standard

CloudShell Feedback

Type here to search

Edit Block Public Access setting | **Pipelines - Recent** | **Upload files - janardhana-papolu** | **janabucket.s3.ap-south-1.amazonaws.com**

s3.console.aws.amazon.com/s3/bucket/janabucket/property/bpa/edit?region=ap-south-1&bucketType=general

aws Services Search [Alt+S]

Global janardhana.papolu

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.

Cancel **Save changes**

CloudShell Feedback

Type here to search

Janasbucket - S3 bucket | S3 | Pipelines - Recent | janasbucket.s3.ap-south-1.amazonaws.com | Upload files - janardhana.papolu | +

aws Services Search [Alt+S] Global janardhana.papolu

Successfully edited Block Public Access settings for this bucket.

Permissions overview

Access Objects can be public

Block public access (bucket settings)

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 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 your buckets or objects within, you can customize the individual settings below to suit your specific storage use case. [Learn more](#)

Block all public access

Off Individual Block Public Access settings for this bucket

Edit

CloudShell Feedback Type here to search 30°C 12:44 18-01-2024

Janardhana-Aws-Instance.pdf | Pipelines - Recent | janasbucket.s3.ap-south-1.amazonaws.com | Upload files - janardhana.papolu | +

s3.console.aws.amazon.com/s3/object/janasbucket?region=ap-south-1&bucketType=general&prefix=Janardhana-Aws-Instance.pdf&tab=permissions

aws Services Search [Alt+S] Global janardhana.papolu

Grant basic read/write permissions to AWS accounts. [Learn more](#)

This bucket has the bucket owner enforced setting applied for Object Ownership. When bucket owner enforced is applied, use bucket policies to control access. [Learn more](#)

Grantee	Object	Object ACL
Object owner (your AWS account) Canonical ID: cac5e50d3f61972cf230c1cf34775d253e6cd51328e6a5d022e02291571014ac	Read	Read, Write
Everyone (public access) Group: http://acs.amazonaws.com/groups/global/AllUsers	-	-
Authenticated users group (anyone with an AWS account) Group: http://acs.amazonaws.com/groups/global/AuthenticatedUsers	-	-

CloudShell Feedback Type here to search 30°C 12:44 18-01-2024

Janardhana-Aws-Instance.pdf | Pipelines - Recent | janasbucket | janardhana-Aws-Instance.pdf | Upload files - janardhana.papolu | +

s3.console.aws.amazon.com/s3/object/janasbucket?region=ap-south-1&bucketType=general&prefix=Janardhana-Aws-Instance.pdf&tab=versions

aws Services Search [Alt+S] Global janardhana.papolu

Amazon S3 > Buckets > janasbucket > Janardhana-Aws-Instance.pdf

Janardhana-Aws-Instance.pdf [Info](#)

Properties | Permissions | **Versions**

Versions (1)

Version ID	Type	Last modified	Size	Storage class
LnFNNvd9StiaLi71XpBGH0U9xy3q9Xo (Current version)	pdf	January 18, 2024, 12:33:55 (UTC+05:30)	1.7 MB	Standard

CloudShell Feedback Type here to search 30°C 12:44 18-01-2024

File Explorer (Windows) showing the file structure:

```

    Janardhana-Aws-instance
    └── Janardhana-Aws-Instance
        ├── dotnet.ppk
        ├── Dotnet
        ├── index
        ├── index.html
        └── RoleBasedAuthentication

```

Upload files dialog (Windows File Explorer):

File name: Janardhana-Aws-instance

Add files Add folder

Find by name

No files or folders

You have not chosen any files or folders to upload.

CloudShell Feedback

Type here to search

Upload objects - S3 bucket Janasbucket

Pipelines - Recent

janasbucket.s3.ap-south-1.amazonaws.com

Upload files - janardhana-papolu

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

aws Services Search [Alt+S]

Find by name

Name Folder Type

Destination Info

Destination s3://janasbucket

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

Type here to search

Janardhana-Aws-instance.pdf

Pipelines - Recent

janasbucket.s3.ap-south-1.amazonaws.com

Upload files - janardhana-papolu

s3.console.aws.amazon.com/s3/object/janasbucket?region=ap-south-1&bucketType=general&prefix=Janardhana-Aws-instance.pdf&tab=versions

aws Services Search [Alt+S]

Amazon S3 > Buckets > janasbucket > Janardhana-Aws-instance.pdf

Janardhana-Aws-instance.pdf Info

Properties Permissions Versions

Versions (2)

Version ID	Type	Last modified	Size	Storage class
kGxluVyxJP8j7PWHaZvkQ7TwYzhx3OW6 (Current version)	pdf	January 18, 2024, 12:45:59 (UTC+05:30)	1.7 MB	Standard
LnfNNvd9SliaLi71XpBGh0U9xy3q9Xo	pdf	January 18, 2024, 12:33:55 (UTC+05:30)	1.7 MB	Standard

Download Open Delete Actions

CloudShell Feedback

Type here to search

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Bucket policy

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. [Learn more](#)

Bucket ARN

arn:aws:s3:::janasbucket

Policy

```

1  {
2    "Version": "2012-10-17",
3    "Id": "ExamplePolicy01",
4    "Statement": [
5      {
6        "Sid": "ExampleStatement01",
7        "Effect": "Allow",
8        "Principal": [
9          "AWS": "arn:aws:iam::123456789012:user/Dave"
10        ],
11        "Action": [
12          "s3:GetObject",
13          "s3:GetBucketLocation",
14        ]
15      }
16    ]
17  }

```

Edit statement Statement1 Remove

Add actions Choose a service

Available AMP API Gateway

Create lifecycle rule - S3

Policies and Permissions Policies and Permissions Pipelines - Recent janasbucket.s3.ap-south-1 Upload files - janardhana CloudShell Feedback Type here to search © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences 30°C ENG 12:51 18-01-2024

Create lifecycle rule

Lifecycle rule configuration

Lifecycle rule name bucket Up to 255 characters

Choose a rule scope

- Limit the scope of this rule using one or more filters
- Apply to all objects in the bucket

Filter type You can filter objects by prefix, object tags, object size, or whatever combination suits your usecase.

Prefix Add filter to limit the scope of this rule to a single prefix. Enter prefix

Prefix Add filter to limit the scope of this rule to a single prefix. Enter prefix

Object tags You can limit the scope of this rule to the key/value pairs added below. Add tag

Object size You can limit the scope of this rule to apply to objects based on their size. For example, you can filter out objects that might not be cost effective to transition to Glacier Flexible Retrieval (formerly Glacier) because of per-object fees.

- Specify minimum object size
- Specify maximum object size

Lifecycle rule actions Choose the actions you want this rule to perform. Per-request fees apply. [Learn more](#) or see [Amazon S3 pricing](#)

Screenshot of the AWS S3 Lifecycle Rule configuration page for creating a new rule.

Actions:

- Move current versions of objects between storage classes
- Move noncurrent versions of objects between storage classes
- Expire current versions of objects
- Permanently delete noncurrent versions of objects
- Delete expired object delete markers or incomplete multipart uploads

Transition current versions of objects between storage classes:

Choose transitions to move current versions of objects between storage classes based on your use case scenario and performance access requirements. These transitions start from when the objects are created and are consecutively applied. [Learn more](#)

Choose storage class transitions:

Days after object creation
Standard-IA

Review transition and expiration actions:

Current version actions:

Day 0	Noncurrent versions actions
Objects uploaded	No actions defined.

Day 30

Noncurrent versions actions:

Day 0	Noncurrent versions actions
30	The integer value for One Zone-IA must be at least 30 more than the value for Standard-IA.

Add transition

Review transition and expiration actions:

Current version actions:

Day 0	Noncurrent versions actions
Objects uploaded	No actions defined.

Day 30

Noncurrent versions actions:

Day 0	Noncurrent versions actions
30	The integer value for One Zone-IA must be at least 30 more than the value for Standard-IA.

Add transition

Review transition and expiration actions:

Current version actions:

Day 0	Noncurrent versions actions
Objects uploaded	No actions defined.

Day 30

Noncurrent versions actions:

Day 0	Noncurrent versions actions
30	The integer value for One Zone-IA must be at least 30 more than the value for Standard-IA.

Add transition

Warning: Transitioning small objects to Glacier Flexible Retrieval (formerly Glacier) or Glacier Deep Archive will incur a per object cost. You will be charged for each object you transition to S3 Glacier Flexible Retrieval (formerly Glacier) or S3 Glacier Deep Archive. A fixed amount of storage is also added to each object to accommodate metadata for managing the object which increases storage costs. You can reduce these costs by limiting the number of objects to transition (by prefix, tag, or version), or by aggregating objects before transitioning them. Learn more about [Glacier Flexible Retrieval \(formerly Glacier\) cost considerations](#) or review the table on Requests and data retrievals tab on the [Amazon S3 pricing page](#).

I acknowledge that this lifecycle rule will incur a one-time lifecycle request cost per object if it transitions small objects.

Screenshot of the AWS S3 Lifecycle configuration page for a bucket named "janasbucket".

Current version actions:

- Day 0: Objects uploaded.
- Day 30: Objects move to Standard-IA.
- Day 60: Objects move to One Zone-IA.
- Day 183: Objects move to Glacier Flexible Retrieval (formerly Glacier).

Noncurrent versions actions:

- Day 0: No actions defined.

Lifecycle rule name: bucket

Choose a rule scope:
 Limit the scope of this rule using one or more filters
 Apply to all objects in the bucket

Apply to all objects in the bucket:
 If you want the rule to apply to specific objects, you must use a filter to identify those objects. Choose "Limit the scope of this rule using one or more filters". [Learn more](#)

 I acknowledge that this rule will apply to all objects in the bucket.

 You must check this check box to apply this rule to all objects in the bucket.

Lifecycle rule actions:

Choose the actions you want this rule to perform. Per-request fees apply. [Learn more](#) or see [Amazon S3 pricing](#)

Move current versions of objects between storage classes

 Move noncurrent versions of objects between storage classes

Lifecycle configuration was updated. Lifecycle rule "bucket" was successfully added.

It may take some time for the configuration to be updated. Press the refresh button if changes to the rule are not displayed.

Lifecycle configuration

To manage your objects so that they are stored cost effectively throughout their lifecycle, configure their lifecycle. A lifecycle configuration is a set of rules that define actions that Amazon S3 applies to a group of objects. Lifecycle rules run once per day.

Lifecycle rules (1)

Use lifecycle rules to define actions you want Amazon S3 to take during an object's lifetime such as transitioning objects to another storage class, archiving them, or deleting them after a specified period of time. [Learn more](#)

	View details	Edit	Delete	Actions	Create lifecycle rule
<input type="text"/> Find lifecycle rules by name					
Lifecycle rule... Status Scope Current ver... Noncurrent ... Expired obj... Incomplete m... <input checked="" type="radio"/> bucket Enabled Entire bucket Transition to Stand...					

The screenshot shows the AWS S3 Bucket Management interface for the 'janasbucket' bucket. The 'Management' tab is selected. Under the 'Lifecycle rules' section, there is one rule named 'bucket' with the status 'Enabled'. The 'Scope' is set to 'Entire bucket' and the 'Transition to Standard' option is selected. The 'Replication rules' section shows 0 replication rules.

Lifecycle rules (1)

Use lifecycle rules to define actions you want Amazon S3 to take during an object's lifetime such as transitioning objects to another storage class, archiving them, or deleting them after a specified period of time. [Learn more](#)

Lifecycle rule ...	Status	Scope	Current versio...	Nonconcurrent ve...	Expired object...	Incomplete m...
bucket	Enabled	Entire bucket	Transition to Standard	-	-	-

[View lifecycle configuration](#)

Replication rules (0)

Use replication rules to define options you want Amazon S3 to apply during replication such as server-side encryption, replica ownership, transitioning replicas to another storage class, and more. [Learn more](#)

The screenshot shows the AWS S3 Bucket Management interface for the 'janasbucket' bucket. The 'Management' tab is selected. Under the 'Objects' section, there is 1 object named 'Janardhana-Aws-instance.pdf' which is a PDF file. It was uploaded on January 18, 2024, at 12:45:59 (UTC+05:30) and has a size of 1.7 MB. The storage class is set to Standard.

Objects (1) Info

Actions	Name	Type	Last modified	Size	Storage class
Copy S3 URI	Janardhana-Aws-instance.pdf	pdf	January 18, 2024, 12:45:59 (UTC+05:30)	1.7 MB	Standard

The taskbar shows several open browser tabs related to AWS services, including CloudShell, Feedback, Policies and Permissions, Pipelines - Recent, janasbucket.s3.ap-south..., Upload files - janardhan..., and s3.console.aws.amazon.com. The system tray indicates it is 13:08 on January 18, 2024, with a temperature of 30°C and ENG selected.

Screenshot of the AWS S3 console showing the process of deleting objects from a bucket.

The browser tabs are:

- Delete objects - S3 buck...
- Policies and Permissions
- Pipelines - Recent
- janasbucket.s3.ap-south...
- Upload files - janardhan...

The main content area shows the "Delete objects" interface for the "janasbucket" bucket.

Delete objects (Info)

Specified objects

Name	Type	Last modified	Size
Janardhana-Aws-instance.pdf	pdf	January 18, 2024, 12:45:59 (UTC+05:30)	1.7 MB

Delete objects?

To confirm deletion, type **delete** in the text input field.

delete

Delete objects (Delete objects button highlighted)

Successfully deleted objects

Delete objects: status

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

Summary

Source	Successfully deleted	Failed to delete
s3://janasbucket	1 object, 1.7 MB	0 objects

Failed to delete (0)

CloudShell Feedback Type here to search Privacy Terms Cookie preferences © 2024, Amazon Web Services, Inc. or its affiliates. 30°C ENG 13:09 18-01-2024

The image consists of three vertically stacked screenshots of the AWS S3 console.

Screenshot 1: Bucket List

The first screenshot shows the "General purpose buckets" section of the S3 console. It displays a single bucket named "janasbucket" located in the "Asia Pacific (Mumbai) ap-south-1" region. The bucket is set to "Objects can be public" and was created on "January 18, 2024, 12:30:00 (UTC+05:30)".

Name	AWS Region	Access	Creation date
janasbucket	Asia Pacific (Mumbai) ap-south-1	Objects can be public	January 18, 2024, 12:30:00 (UTC+05:30)

Screenshot 2: Empty Bucket Warning

The second screenshot shows a modal dialog titled "Emptying the bucket deletes all objects in the bucket and cannot be undone." It contains the following text:

- Emptying the bucket deletes all objects in the bucket and cannot be undone.
- Objects added to the bucket while the empty bucket action is in progress might be deleted.
- To prevent new objects from being added to this bucket while the empty bucket action is in progress, you might need to update your bucket policy to stop objects from being added to the bucket.

[Learn more](#)

Screenshot 3: Confirmation Dialog

The third screenshot shows a confirmation dialog titled "Permanently delete all objects in bucket "janasbucket"" with the message: "To confirm deletion, type *permanently delete* in the text input field." A text input field contains the text "permanently delete".

[Cancel](#) [Empty](#)

Empty bucket - S3 buckets Policies and Permissions Pipelines - Recent janasbucket.s3.ap-south-1 Upload files - janardhana...

Successfully emptied bucket "janasbucket". View details below. If you want to delete this bucket, use the [delete bucket configuration](#).

Empty bucket: status

The details below are no longer available after you navigate away from this page.

Summary

Source	Successfully deleted	Failed to delete
s3://janasbucket	3 objects, 3.4 MB	0 objects

Failed to delete (0)

Name	Prefix	Version ID	Type	Last modified	Size	Error
© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences						

CloudShell Feedback Type here to search © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences 13:10 18-01-2024

Delete bucket - S3 buckets Policies and Permissions Pipelines - Recent janasbucket.s3.ap-south-1 Upload files - janardhana...

Delete bucket "janasbucket". To confirm deletion, enter the name of the bucket in the text input field. janasbucket

Cancel Delete bucket

CloudShell Feedback Type here to search © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences 13:10 18-01-2024