

S3 Storage Cloud Service

Some of the slides has been adapted from Prof. Sandeep Kumar Singh Slides

BUCKETS



Containers for objects stored in S3

Serve several purposes:

- Organise the Amazon S3 namespace at the highest level

- Identify the account responsible for charges

- Play a role in access control

- Serve as the unit of aggregation for usage reporting

OBJECTS



Fundamental entities stored in Amazon S3

Consist of data & metadata

Data portion is opaque to Amazon S3

Metadata is a set of name-value pairs that describe the object

Object is uniquely identified within a bucket by a key (name) and a version ID

KEYS

Unique identifier for an object within a bucket.

Every object in a bucket has exactly one key

Combination of a bucket, key & version ID
uniquely identify each object

Some Use Cases on Storage Cloud Service

- Heavy media files to be used on EC2 hosted website wordpress
- Versioning
- Cross Region Replication
- Static website hosting like brochure, contact lists, email
- Synchronisation
- Cost effective backup of data

Use Case -1: Data Storage

Amazon S3



We're gradually updating the design of the Amazon S3 console. You will notice some updated screens as we improve the performance and user interface. To help us improve the experience, give [feedback](#) on the recent updates.



Buckets

Batch Operations

Access analyzer for S3

Block public access (account settings)

Feature spotlight 2

Amazon S3

Buckets (0)

Buckets are the fundamental container in Amazon S3 for data storage. For others to access the objects in your buckets, you'll need to explicitly grant them permissions. [Learn more](#)

Find bucket by name

< 1 >

Name	Region	Access	Bucket created
No buckets			
You don't have any buckets.			
Create bucket			

You can host in any Geo-Regions

REGIONS



The geographical region where Amazon S3 will store the buckets that you create

Choose a region to optimise latency, minimise costs, or address regulatory requirements.

ⓘ We're gradually updating the design of the Amazon S3 console. You will notice some updated screens as we improve the performance and user interface. To help us improve the experience, [give feedback](#) on the recent updates.

Amazon S3 > Create bucket

Create bucket

General configuration

Bucket name

`masksbucket`

Bucket name must be unique and must not contain spaces or uppercase letters. [See rules for bucket naming](#)

Region

Asia Pacific (Mumbai) ap-south-1

Bucket settings for Block Public Access

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)



Feedback



English (US)

© 2008 - 2020, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.

Privacy Policy

Terms of Use



Type here to search



21:56
23-04-2020

Amazon S3

X

ⓘ We're gradually updating the design of the Amazon S3 console. You will notice some updated screens as we improve the performance and user interface. To help us improve the experience, give [feedback](#) on the recent updates.

ⓘ Successfully created bucket "mysksbucket"

To upload files and folders, or to configure additional bucket settings such as Bucket Versioning, tags, and default encryption, choose [Go to bucket details](#).

[Go to bucket details](#)

X

Buckets

Batch Operations

Access analyzer for S3

Block public access (account settings)

Feature spotlight 2

Amazon S3

Buckets (1)

Buckets are the fundamental container in Amazon S3 for data storage. For others to access the objects in your buckets, you'll need to explicitly grant them permissions. [Learn more](#)

[Copy ARN](#)

[Empty](#)

[Delete](#)

[Create bucket](#)

Find bucket by name

< 1 > |

Name	Region	Access	Bucket created
mysksbucket	Asia Pacific (Mumbai) ap-south-1	Not public	2020-04-23T16:24:57.000Z

mysksbucket

Overview

Properties

Permissions

Management

Access points

Upload

+ Create folder

Download

Actions ▾

Asia Pacific (Mumbai) 

No Hierarchy in S3
Create a hierarchy on root

This bucket is empty. Upload new objects to get started.



Upload an object

Buckets are globally unique containers for everything that you store in Amazon S3.



Set object properties

After you create a bucket, you can upload your objects (for example, your photo or video files).



Set object permissions

By default, the permissions on an object are private, but you can set up access control policies to grant permissions to others.

mysksbucket

Overview

Properties

Permissions

Management

Access points

Block public access

Access Control List

Bucket Policy

CORS configuration

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 cases. [Learn more](#)

Block all public access

On

Edit

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

On

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

On

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

On

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

On

[Overview](#)[Properties](#)[Permissions](#)[Management](#)[Access points](#)[Block public access](#)[Access Control List](#)[Bucket Policy](#)[CORS configuration](#)

Block public access (bucket settings)

Public access is granted to buckets and objects through bucket policies and access point policies. To prevent public access from being granted to your buckets and objects, you can turn on bucket-level public access settings. These settings apply only to the bucket and its objects. If you require site-wide or account-wide changes, turn on AWS CloudTrail or AWS CloudWatch Metrics to track and analyze access requests, and then use AWS Lambda to automatically block public access.

Block all public access

Turning this setting on is the same as turning on all four other settings.

Block public access to buckets and objects using ACLs

S3 will block public access permissions applied to objects using ACLs. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.

Block public access to buckets and objects using bucket policies

S3 will ignore all ACLs that grant public access to objects.

Block public access to buckets and objects using access point policies

S3 will block new bucket and access point policies that grant public access to buckets and objects.

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.

Edit block public access (bucket settings)



Turn on this setting if you want to prevent all public access to your bucket and objects. If you want to prevent public access to all your S3 buckets and objects, turn on this setting and then turn on the Block all public access setting. If you want to prevent public access to some of your buckets and objects, turn on this setting and then turn on one or more of the other three settings. If you turn on any of these settings, ensure that your applications will still work correctly without public access. If you require site-wide or account-wide changes, turn on AWS CloudTrail or AWS CloudWatch Metrics to track and analyze access requests, and then use AWS Lambda to automatically block public access.

This will result in public access being blocked for this bucket and all objects in the bucket.

To confirm the settings, type *confirm* in the field.

[Cancel](#)[Confirm](#)[Cancel](#) [Save](#)

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 cases.

[Learn more](#)

Block all public access
Turning this setting on is the same as turning on all the other settings listed here.

Block public access to buckets and objects
S3 will block public access permissions applied to this bucket and all objects within. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.

Block public access to buckets and objects
S3 will ignore all ACLs that grant public access to this bucket and all objects within.

Block public access to buckets and objects
S3 will block new bucket and access point policies that grant public access to this bucket and all objects within.

Block public and cross-account access
S3 will ignore public and cross-account access policies that grant public access to this bucket and all objects within.

Edit block public access (bucket settings) X

Updating the block public access (bucket settings) will affect this bucket and all objects within. This may result in some objects becoming public.

To confirm the settings, type **confirm** in the field.

confirm

Cancel Confirm

Cancel Save

Block public access

Access Control List

Bucket Policy

CORS configuration

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 cases. [Learn more](#)

 Public access settings updated successfully



Block all public access

Off

Edit

— 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

On

[Overview](#)[Properties](#)[Permissions](#)[Management](#)[Access points](#)[Block public access](#)[Access Control List](#)[Bucket Policy](#)[CORS configuration](#)

Access for bucket owner

Canonical ID i	List objects i	Write objects i	Read bucket permissions i	Write bucket permissions i
<input type="radio"/> 2436635ec1ff0eb4452fde92935328e396b669a41fa c52611fd013c049c818cb (Your AWS account)	Yes	Yes	Yes	Yes

Access for other AWS accounts

+ Add account	Delete
-------------------------------	------------------------

Canonical ID i	List objects i	Write objects i	Read bucket permissions i	Write bucket permissions i

Public access

The block public access settings turned on for this bucket prevent granting public access.

Group i	List objects i	Write objects i	Read bucket permissions i	Write bucket permissions i
<input type="radio"/> Everyone	-	-	-	-

[Overview](#)[Properties](#)[Permissions](#)[Management](#)[Access points](#)[Block public access](#)[Access Control List](#)[Bucket Policy](#)[CORS configuration](#)

Access for bucket owner

[Canonical ID](#)[List objects](#)[Write objects](#)[Read bucket permissions](#)2436635ec1ff0eb4452fde92935328e396b669a41fa
c52611fd013c049c818cb (Your AWS account)

Yes

Yes

Yes

Access for other AWS accounts

[+ Add account](#)[Delete](#)[Canonical ID](#)[List objects](#)[Write objects](#)[Read bucket permissions](#)

Public access

The block public access settings turned on for this bucket prevent granting public access.

[Group](#)[List objects](#)[Write objects](#)[Read bucket permissions](#) Everyone

Everyone

**This bucket will have public access**

Everyone will have access to one or all of the following: list objects, write objects, read and write permissions.

Access to the objects

 List objects Write objects

Access to this bucket's ACL

 Read bucket permissions Write bucket permissions[Cancel](#)[Save](#)

This bucket has public access

You have provided public access to this bucket. We highly recommend that you never grant any kind of public access to your S3 bucket.

Access for bucket owner

Canonical ID 	List objects 	Write objects 	Read bucket permissions 	Write bucket permissions 
<input type="radio"/> 2436635ec1ff0eb4452fde92935328e396b669a41fa c52611fd013c049c818cb (Your AWS account)	Yes	Yes	Yes	Yes

Access for other AWS accounts

[+ Add account](#)[Delete](#)

Canonical ID 	List objects 	Write objects 	Read bucket permissions 	Write bucket permissions 

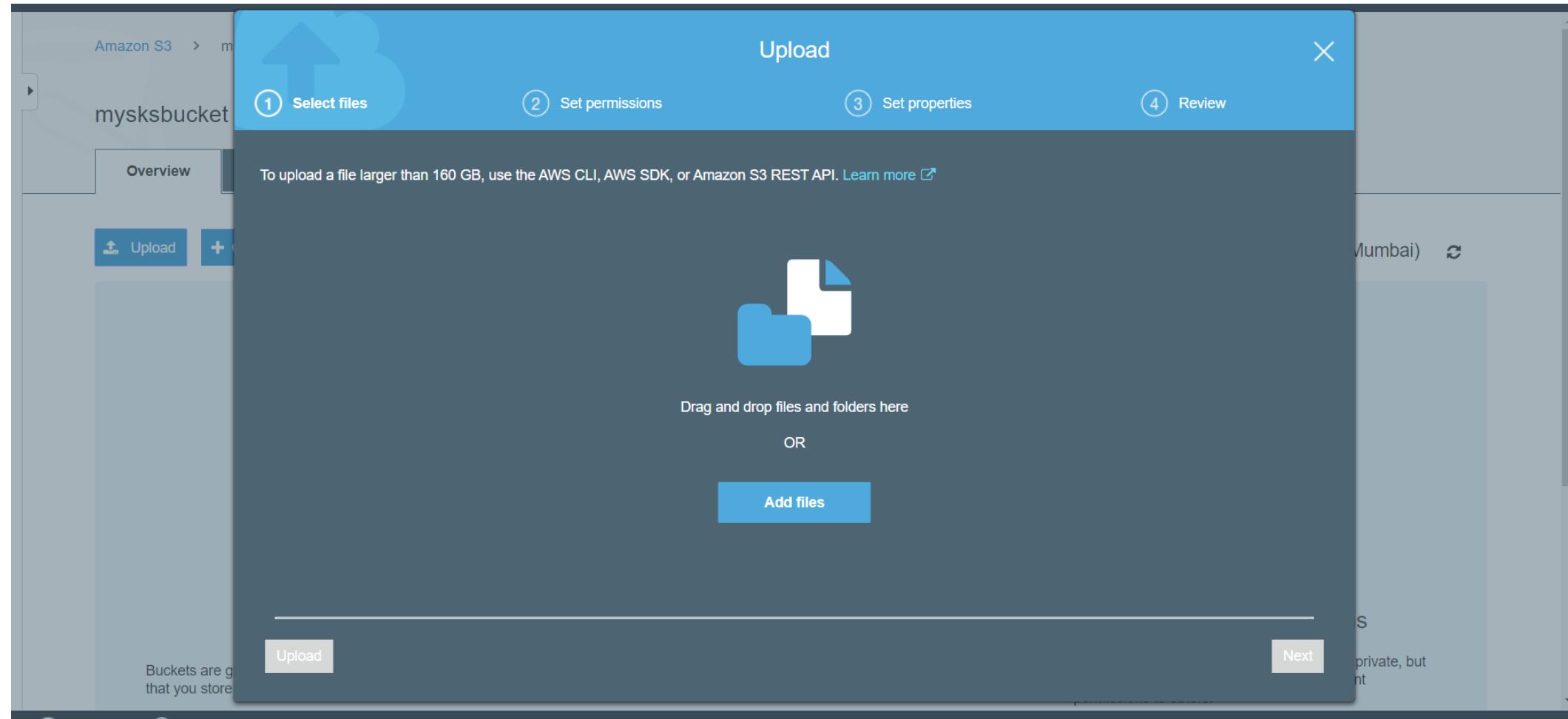
Public access

Group 	List objects 	Write objects 	Read bucket permissions 	Write bucket permissions 
<input type="radio"/> Everyone	Yes	-	Yes	-

S3 log delivery group

Group 	List objects 	Write objects 	Read bucket permissions 	Write bucket permissions 
<input type="radio"/> Log Delivery	-	-	-	-

Use Case-2 Upload data in S3



Durability (99.99%) avg yr and Availability [Upload](#)

X

Select files

Set permissions

3 Set properties

4 Review

Choose a storage class based on your use case and access requirements. [Learn more](#) or see [Amazon S3 pricing](#)

Storage class	Designed for	Availability Zones	Min storage duration	Min billable object size	Monitoring and automation fees	Retrieval fees
<input type="radio"/>	Standard	Frequently accessed data	≥ 3	-	-	-
<input type="radio"/>	Intelligent-Tiering	Long-lived data with changing or unknown access patterns	≥ 3	30 days	Per-object fees apply	-
<input type="radio"/>	Standard-IA	Long-lived, infrequently accessed data	≥ 3	30 days	128KB	Per-GB fees apply
<input type="radio"/>	One Zone-IA	Long-lived, infrequently accessed, non-critical data	≥ 1	30 days	128KB	Per-GB fees apply
<input type="radio"/>	Glacier	Archive data with retrieval times ranging from minutes to hours	≥ 3	90 days	40KB	Per-GB fees apply
<input type="radio"/>	Glacier Deep Archive	Archive data that rarely, if ever, needs to be accessed with retrieval times in hours	≥ 3	180 days	40KB	Per-GB fees apply
<input type="radio"/>	Reduced Redundancy (Not recommended)	Frequently accessed, non-critical data	≥ 3	-	-	-

[Upload](#)

[Previous](#)

[Next](#)

Buckets are g
that you store

private, but
nt

Upload

to be accessed with retrieval times in hours

apply

Reduced Redundancy (Not recommended) Frequently accessed, non-critical data ≥ 3 ≥ 10 ≥ 30

Encryption

Protect data at rest by using Amazon S3 master-key or by using AWS KMS master-key.

None Amazon S3 master-key AWS KMS master-key

Metadata

Metadata is a set of name-value pairs. You cannot modify object metadata after it is uploaded.

Header	Value
Select a key	<input type="text"/>

Tag

Add tags to search, organize and manage access

Key	Value
<input type="text"/>	<input type="text"/>

Upload **Previous** **Next**

Overview

Upload

Upload

X

1 Select files Set permissions Set properties Review

Files

1 Files Size: 1.2 MB Edit

Permissions

1 grantees Edit

Properties

Encryption No **Storage class** Standard Edit

Metadata

Tag

Previous Upload

Buckets are g that you store

Mumbai

mysksbucket

[Overview](#)[Properties](#)[Permissions](#)[Management](#)[Access points](#) Type a prefix and press Enter to search. Press ESC to clear.[Upload](#)[+ Create folder](#)[Download](#)[Actions ▾](#)

Asia Pacific (Mumbai)



Viewing 1 to 1

 Name ▾

Last modified ▾

Size ▾

Storage class ▾

 Vivaan singh IV G Poster.jpg

Apr 23, 2020 10:02:32 PM GMT+0530

1.2 MB

Standard

Viewing 1 to 1

 Type a prefix and press Enter to search. Press ESC to clear.

 Upload  Create folder  Download  Actions

<input checked="" type="checkbox"/> Name ▾	Last modified ▾
 Vivaan singh IV G Poster.jpg	Apr 23, 2020 10:02:32 PM GMT+0530

Asia Pacific (Mumbai) 

Vivaan singh IV G Poster.jpg 

 Download  Copy path  Select from

Latest version ▾

Overview Key Vivaan singh IV G Poster.jpg
Size 1.2 MB
Expiration date N/A
Expiration rule N/A
ETag 25413164836b23e5025e3f3bab90d349
Last modified Apr 23, 2020 10:02:32 PM GMT+0530
Object URL <https://mysksbucket.s3.ap-south-1.amazonaws.com/Vivaan+singh+IV+G+Poster.jpg>

Properties Storage class Standard
Encryption None
Metadata 1
Tags 0 Tags
Object lock Disabled

Permissions Owner

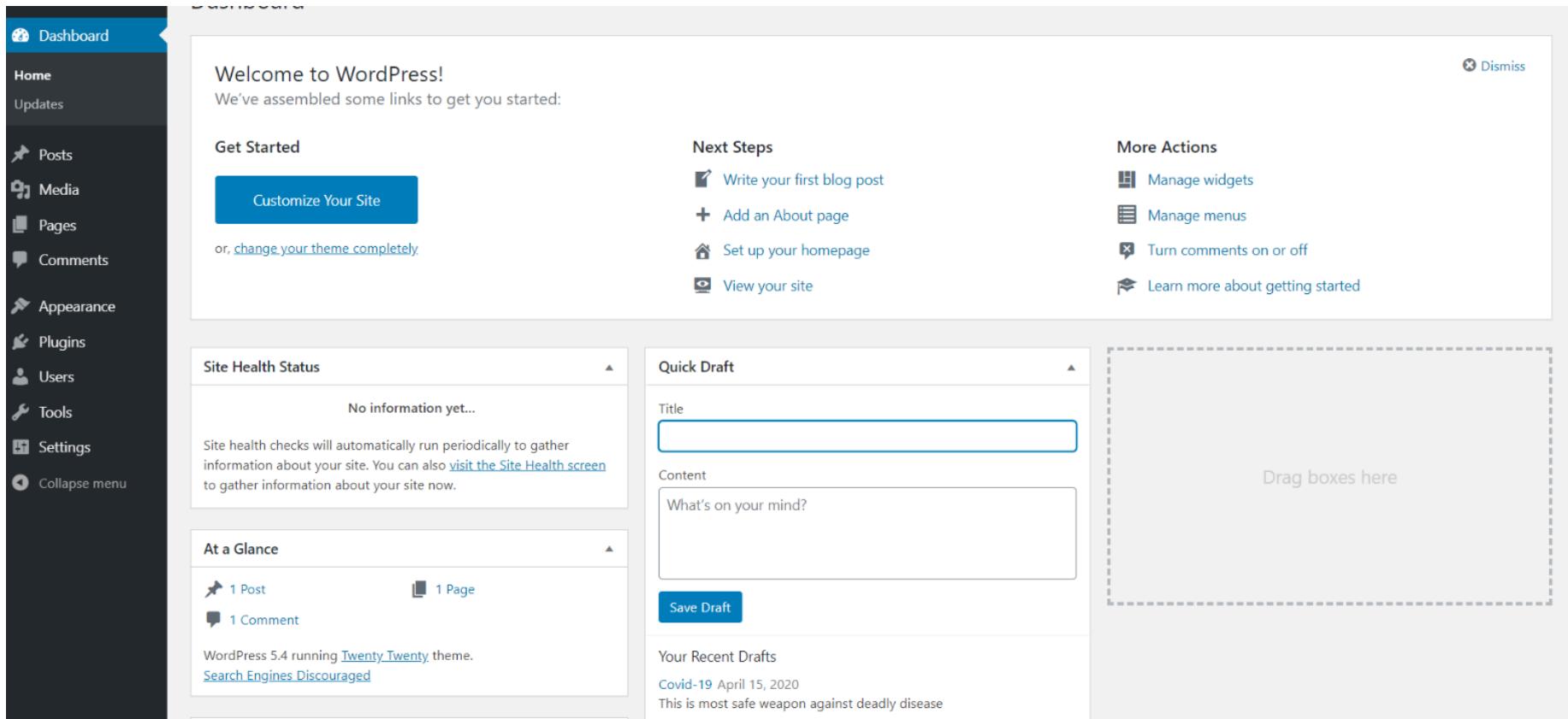
Object URL for use

Operations 0 In progress 1 Success 0 Error

Use Case- Integrate S3 object in EC2 running Website

a) Use Posts and add media

b) Use HTML code and add video tag with source



The screenshot shows the WordPress 'Edit Post' screen. On the left is the navigation sidebar with 'Bootstrap IT' selected. The main area has a title 'Edit Post' and a 'Save Draft' button. The content area contains a video URL: <https://s3.amazonaws.com/bootstrap-it/linux-network-security-lpic-3-303-m3-04.mp4>. A checkmark indicates the endpoint is inserted. The right side features a 'Publish' section with 'Status: Draft' and 'Visibility: Public'. It also includes 'Save Draft', 'Preview', 'Publish immediately', 'Move to Trash', and a 'Publish' button. A 'Categories' section lists 'Uncategorized' with a checked checkbox and a '+ Add New Category' link. A 'Tags' section has a checked checkbox. A 'Visual' and 'Text' switch is at the top right of the content area, with 'Text' currently selected.

The endpoint is already inserted into the page.

Toggle between Visual and Text views.

```
<div align="center">
<br><br>
<hr>
<b>
<video width="640" height="480" controls>
    <source src="https://s3.amazonaws.com/bootstrap-it/linux-network-
        security-
        ↪lpic-3-303-m3-04.mp4" type="video/mp4">
</video>
<hr>
```

b) Use HTML code and add video tag with source

Delete bucket

- ⚠ • Deleting a bucket cannot be undone.
• Bucket names are unique. If you delete a bucket, another AWS user can use the name.

[Learn more !\[\]\(c7774dea93eb10ead3ed0542c77a8534_img.jpg\)](#)

Delete bucket mysecondregion2020

To confirm deletion, type the name of the bucket.

mysecondregion2020

Cancel

Delete bucket

Delete bucket



This bucket is not empty

Buckets must be empty before they can be deleted. To delete all objects in the bucket, use the [empty bucket configuration](#).

Delete bucket myclassbucket2020

To confirm deletion, type the name of the bucket.

myclassbucket2020

Cancel

Delete bucket

Use Case -5 Bucket Protection

<https://docs.aws.amazon.com/AmazonS3/latest/dev/example-bucket-policies.html>

Bucket Policies

Fine grained
Apply policies at the bucket level in S3
Incorporate user restrictions without using IAM

Allow
Bob, Jane
Actions
PutObject
Resource
arn:aws:s3:::mybucket/*

Other Example Use-Cases for Bucket Policies

- Granting Permissions to Multiple Accounts with Added Conditions
- Restricting Access to a Specific HTTP Referrer
- Granting Permission to an Amazon CloudFront Origin Identity
- Adding a Policy to Require MFA Authentication
- Granting Cross-Account Permissions to Upload Objects While Ensuring the Bucket Owner Has Full Control

myclassbucket2020

[Overview](#) [Properties](#) [Permissions](#)

Public

[Management](#)[Access points](#)[Block public access](#)[Access Control List](#)

Public

[Bucket Policy](#)[CORS configuration](#)

Bucket policy editor ARN: arn:aws:s3:::myclassbucket2020

Type to add a new policy or edit an existing policy in the text area below.

[Delete](#)[Cancel](#)[Save](#)

The block public access settings turned on for this bucket prevent granting public access.

```
1 {
2     "Version": "2012-10-17",
3     "Id": "S3PolicyId1",
4     "Statement": [
5         {
6             "Sid": "IPAllow",
7             "Effect": "Deny",
8             "Principal": "*",
9             "Action": "s3:*",
10            "Resource": "arn:aws:s3:::myclassbucket2020/*",
11            "Condition": {
12                "NotIpAddress": {
13                    "aws:SourceIp": "192.168.0.103/24"
14                }
15            }
16        }
17    ]
18 }
```

Use Case 6- Versioning Data in Bucket

mysksbucket

Overview

Properties

Permissions

Management

Access points

Versioning

Keep multiple versions of an object in the same bucket.

[Learn more](#)

 Disabled

Server access logging

Set up access log records that provide details about access requests.

[Learn more](#)

 Disabled

Static website hosting

Host a static website, which does not require server-side technologies.

[Learn more](#)

 Disabled

Object-level logging

Record object-level API activity using the CloudTrail data events feature (additional cost).

[Learn more](#)

 Disabled

Default encryption

Automatically encrypt objects when stored in Amazon S3

[Learn more](#)

myclassbucket2020

Overview

Properties

Permissions

Public

Management

Access points

Versioning

Enable versioning
 Suspend versioning
This suspends the creation of object versions for all operations but preserves any existing object versions.
 Disabled

[Cancel](#) [Save](#)

Server access logging

Set up access log records that provide details about access requests.

[Learn more](#)

Disabled

Static website hosting

Host a static website, which does not require server-side technologies.

[Learn more](#)

Disabled

Object-level logging

Record object-level API activity using the

Default encryption

Automatically encrypt objects when

Operations

0 In progress

1 Success

0 Error

myclassbucket2020

SKS_W3Lab.docx file first uploaded
at 6:39 and modified and reuploaded

Overview

Properties

Permissions

Public

Management

Access points

 Type a prefix and press Enter to search. Press ESC to clear.

Upload

+ Create folder

Download

Actions ▾

Versions

Hide

Show

Asia Pacific (Mumbai)

Viewing 1 to 3

<input type="checkbox"/> Name ▾	Last modified ▾	Size ▾	Storage class ▾
SKS.pdf	Apr 27, 2020 7:03:55 PM GMT+0530	71.7 KB	Standard-IA
SKS_W3Lab.docx	Apr 27, 2020 6:41:06 PM GMT+0530	15.8 KB	Standard
Week 4 DNS Assignment.txt	Apr 27, 2020 7:07:18 PM GMT+0530	481.0 B	Standard

Viewing 1 to 3

Operations

0 In progress

1 Success

0 Error

myclassbucket2020

[Overview](#)[Properties](#)[Permissions](#)

Public

[Management](#)[Access points](#) Type a prefix and press Enter to search. Press ESC to clear.[Upload](#)[+ Create folder](#)[Download](#)[Actions ▾](#)[Versions](#)[Hide](#)[Show](#)

Asia Pacific (Mumbai)

Viewing 1 to 2

<input type="checkbox"/>	Name	Version ID	Last modified	Size	Storage class
	SKS_W3Lab.docx		Apr 27, 2020 6:41:06 PM		
<input type="checkbox"/>	Apr 27, 2020 6:41:06 PM (Latest version)	.zzXUMQ_BVSMjoKovED2MUyj3.s.4H6b		15.8 KB	Standard
<input type="checkbox"/>	Apr 27, 2020 6:39:36 PM	null		15.9 KB	Standard

Viewing 1 to 2

myclassbucket2020

[Overview](#)[Properties](#)[Permissions](#)

Public

[Management](#)[Access points](#) Type a prefix and press Enter to search. Press ESC to clear.[Upload](#)[+ Create folder](#)[Download](#)[Actions ▾](#)[Versions](#)[Hide](#)[Show](#)

Asia Pacific (Mumbai)



Viewing 1 to 3

<input type="checkbox"/>	Name	Version ID	Last modified	Size	Storage class
	SKS_W3Lab.docx		Apr 27, 2020 6:50:32 PM		
<input type="checkbox"/>	Apr 27, 2020 6:50:32 PM (Delete marker)	YCStvZfpODbluSvnz7_7LyC6iUv3cKw		--	--
<input type="checkbox"/>	Apr 27, 2020 6:41:06 PM	.zzXUMQ_BVSMjoKovED2MUyj3.s.4H6b		15.8 KB	Standard
<input type="checkbox"/>	Apr 27, 2020 6:39:36 PM	null		15.9 KB	Standard

Viewing 1 to 3

Operations

0 In progress

2 Success

0 Error

myclassbucket2020

[Overview](#)[Properties](#)[Permissions](#)

Public

[Management](#)[Access points](#) Type a prefix and press Enter to search. Press ESC to clear.[Upload](#)[+ Create folder](#)[Download](#)[Actions](#) ▾[Versions](#)[Hide](#)[Show](#)

Asia Pacific (Mumbai)



Viewing 1 to 3

<input type="checkbox"/> Name
SKS_W3Lab.docx
<input checked="" type="checkbox"/> Apr 27, 2020 6:50:32 PM (Delete mark)
<input type="checkbox"/> Apr 27, 2020 6:41:06 PM

[Open](#)[Download as](#)[Get total size](#)[Change storage class](#)[Restore](#)[Change encryption](#)[Change metadata](#)[Add tags](#)[Make public](#)[Rename](#)

Last modified	Size	Storage class
Apr 27, 2020 6:50:32 PM	–	–
bluSvnz7_7LyC6iUv3cKw	15.8 KB	Standard
SMjoKovED2MUyj3.s.4H6b	15.9 KB	Standard

Viewing 1 to 3

[Delete](#)[Operations](#)

0 In progress

2 Success

Use Case7

Cross-region replication (CRR)

mysksbucket

Overview

Properties

Permissions

Management

Access points

Lifecycle

Replication

Analytics

Metrics

Inventory

+ Add lifecycle rule

Edit

Delete

Actions ▾



There is no lifecycle rule applied to this bucket.
Here is how to get started.



Use lifecycle rules to manage your objects



Automate transition to tiered storage



Expire your objects

Create bucket

General configuration

Bucket name

Bucket name must be unique and must not contain spaces or uppercase letters. [See rules for bucket naming](#)

Region

Bucket settings for Block Public Access

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

mysecondregion2020

Overview Properties Permissions Management Access points

Lifecycle

Replication

Analytics

Metrics

Inventory

+ Add rule

Edit priorities

Edit

Delete

Actions ▾



You haven't created any replication rules for this bucket.

Cross-Region Replication

Cross-Region replication enables automatic and asynchronous copying of objects across buckets in different AWS Regions. Buckets configured for object replication can be owned by the same AWS account or by different accounts.

Same-Region Replication

Same-Region replication enables automatic and asynchronous copying of objects across buckets in the same AWS Region. Buckets configured for object replication can be owned by the same AWS account or by different accounts.

Operations

0 In progress

1 Success

0 Error

mysecondregion2020

[Overview](#)[Properties](#)[Permissions](#)[Lifecycle](#)[Replication](#)[+ Add rule](#)[Edit priorities](#)[Edit](#)[Delete](#)

Cross-Region

Cross-Region replication enables automatic and asynchronous copying of objects across buckets in different AWS Regions. Buckets configured for cross-region replication can be owned by the same AWS account or by different accounts.

Operations

0 In progress

1 Success

Replication rule

1 Set source 2 Set destination 3 Configure rule options 4 Review

Set source

Entire bucket  mysecondregion2020
 Prefix or tags 

Replication criteria

Replicate objects encrypted with AWS KMS 

 Your replication rule will be created using the new schema

Replication now has a new schema that supports replication based on prefixes, one or more object tags or a combination of the two. As part of the new schema, you can set overlapping rules with priorities. The new schema does not support delete marker replication, which would prevent any delete actions from replicating.

[Learn more](#)

[Cancel](#)

[Next](#)

mysecondregion2020

[Overview](#)[Properties](#)[Permissions](#)[Lifecycle](#)[Replication](#)[+ Add rule](#)[Edit priorities](#)[Edit](#)[Delete](#)

Cross-Region

Cross-Region replication enables automatic and asynchronous copying of objects across buckets in different AWS Regions. Bucket replication can be owned by the same AWS account or by different accounts.

Operations

0 In progress

1 Success

Replication rule

 Set source ② Set destination ③ Configure rule options ④ Review

Destination bucket

You can replicate objects across buckets in different AWS Regions (cross-Region replication) or you can replicate objects across buckets in the same AWS Region (same-Region replication).

[Learn more](#) or see [Amazon S3 pricing](#)

Select bucket

 Buckets in this account Buckets in another account[Select or enter bucket name](#)

Create new bucket

▶ myclassbucket2020

Region: Asia Pacific (Mumbai)

[Previous](#)[Next](#)

mysecondregion2020

[Overview](#)[Properties](#)[Permissions](#)[Lifecycle](#)[Replication](#)[+ Add rule](#)[Edit priorities](#)[Edit](#)[Delete](#)

Cross-Region

Cross-Region replication enables automatic replication of objects across buckets in different AWS Regions. Object replication can be owned by the source or destination account.

Operations

0 In progress

1 Success

Replication rule

 Set source ② Set destination ③ Configure rule options ④ Review

Destination options

Storage class

 Change the storage class for the replicated objects

Choose a storage class based on your use case and access requirements. There are **per-request fees** when replicating data to any S3 or S3 Glacier storage class. [Learn more](#) or see [Amazon S3 pricing](#)

[Standard-IA](#)

Object ownership

 Change object ownership to destination bucket owner [i](#)

Replication time control settings

 S3 Replication Time Control

Replication Time Control replicates 99.99% of your new objects within 15 minutes. Additional per-GB Data Transfer fees and CloudWatch metrics fees apply. [Learn more](#)

[Previous](#)[Next](#)

mysecondregion2020

[Overview](#)[Properties](#)[Permissions](#)[Lifecycle](#)[Replication](#)[+ Add rule](#)[Edit priorities](#)[Edit](#)[Delete](#)

Cross-Region

Cross-Region replication enables automatic and asynchronous copying of objects across buckets in different AWS Regions. Buckets configured for cross-region replication can be owned by the same AWS account or by different accounts.

Operations

0 In progress

1 Success

Replication rule

X

Set source Set destination **3 Configure rule options** 4 Review

IAM role

Create new role

Rule name

Canada to Mumbai Region

Status

Enabled

Disabled

Previous Next

mysecondregion2020

Overview Properties Permissions Management Access points

Lifecycle

Replication

Analytics

Metrics

Inventory

✓ Replication configuration updated successfully.

x

Source	Destination	Permissions	 Edit global settings
Bucket mysecondregion2020	Bucket myclassbucket2020	IAM role s3crr_role_for_mysecondregion2020_to_myclassbucket2020	
Region Canada (Central)	Region Asia Pacific (Mumbai)	Bucket policy Copy	

Operations

0 In progress

1 Success

0 Error

mysecondregion2020

Overview

Properties

Permissions

Management

Access points

 Type a prefix and press Enter to search. Press ESC to clear.

 Upload

 Create folder

 Download

 Actions ▾

Versions

 Hide

 Show

Canada (Central) 

 Viewing 1 to 2

Name ▾

Last modified ▾

Size ▾

Storage class ▾

 Lecture Plan.txt

Apr 27, 2020 6:59:02 PM GMT+0530

660.0 B

Standard

 SKS.pdf

Apr 27, 2020 7:03:55 PM GMT+0530

71.7 KB

Standard

 Viewing 1 to 2

mysecondregion2020

[Overview](#)[Properties](#)[Permissions](#)[Management](#)[Access points](#) Type a prefix and press Enter to search. Press ESC to clear.[Upload](#)[+ Create folder](#)[Download](#)[Actions ▾](#)[Versions](#)[Hide](#)[Show](#)

Canada (Central)

Viewing 1 to 2

 Name ▾

Last modified ▾

Size ▾

Storage class ▾

 Lecture Plan.txt

Apr 27, 2020 6:59:02 PM GMT+0530

660.0 B

Standard

 SKS.pdf

Apr 27, 2020 7:03:55 PM GMT+0530

71.7 KB

Standard

Viewing 1 to 2

Operations

0 In progress

2 Success

0 Error

myclassbucket2020

[Overview](#)[Properties](#)[Permissions](#)

Public

[Management](#)[Access points](#) Type a prefix and press Enter to search. Press ESC to clear.[Upload](#)[+ Create folder](#)[Download](#)[Actions ▾](#)[Versions](#)[Hide](#)[Show](#)

Asia Pacific (Mumbai)

Viewing 1 to 3

 Name ▾

Last modified ▾

Size ▾

Storage class ▾

 SKS.pdf

Apr 27, 2020 7:03:55 PM GMT+0530

71.7 KB

Standard-IA

 SKS_W3Lab.docx

Apr 27, 2020 6:41:06 PM GMT+0530

15.8 KB

Standard

 Week 4 DNS Assignment.txt

Apr 27, 2020 7:07:18 PM GMT+0530

481.0 B

Standard

Viewing 1 to 3

Operations

0 In progress

1 Success

0 Error

Use Case 8- Static Web site Hosting

<https://docs.aws.amazon.com/AmazonS3/latest/dev/WebsiteHosting.html>

<https://docs.aws.amazon.com/AmazonS3/latest/dev/HowDoIWebsiteConfiguration.html>

<https://docs.aws.amazon.com/AmazonS3/latest/dev/ManagingBucketWebsiteConfig.html>

<https://docs.aws.amazon.com/AmazonS3/latest/dev/ConfigWebSiteREST.html>

1. Register a domain on free or paid services. Fetch the domain name assigned.
2. Create a S3 bucket with the same name as the domain.
3. In Properties , enable static website hosting option.
4. Create the contents of your website including the index page. Upload contents in your bucket.
5. Make appropriate pages publicly accessible.(Refer Previous Slides)
6. Write appropriate bucket policy for making website accessible read-only to anonymous user.(Refer Previous Slides)
7. Avail a Rout 53 Service and follow the DNS management
8. Copy the newly created NS records to nameservers at your respective domain provider site.
9. Create IP rule record and set alias to S3 bucket
10. Test your website from different places and browsers.

mysksbucket

Overview

Properties

Permissions

Management

Access points

Versioning

Keep multiple versions of an object in the same bucket.

[Learn more](#)

Disabled

Server access logging

Set up access log records that provide details about access requests.

[Learn more](#)

Disabled

Static website hosting



Endpoint : <http://mysksbucket.s3-website.ap-south-1.amazonaws.com>

Use this bucket to host a website [Learn more](#)

Redirect requests [Learn more](#)

Disable website hosting

Disabled

[Cancel](#)

[Save](#)

Object-level logging

Default encryption

Versioning

Keep multiple versions of an object in the same bucket.

[Learn more](#)

Disabled

Server access logging

Set up access log records that provide details about access requests.

[Learn more](#)

Disabled

Static website hosting



Endpoint : <http://mysksbucket.s3-website.ap-south-1.amazonaws.com>

Use this bucket to host a website [Learn more](#)

Index document [i](#)

`index.html`

Error document [i](#)

`error.html`

Redirection rules (optional) [i](#)

Redirect requests [Learn more](#)

Disable website hosting

Disabled

[Cancel](#)

[Save](#)

Use Case 9: S3 as Backup Device

Goal- To build replica of your instance

Recommended Stopping instance

New EC2 Experience
[Tell us what you think](#)

Create Snapshot Actions ▾

Owned By Me ▾ Filter by tags and attributes or search by keyword

None found

You do not have any snapshots in this region.

Click the Create Snapshot button to create your first snapshot.

Create Snapshot

IMAGES

- AMIs
- Bundle Tasks

ELASTIC BLOCK STORE

- Volumes

Snapshots

- Lifecycle Manager

NETWORK & SECURITY

- Security Groups [New](#)
- Elastic IPs [New](#)
- Placement Groups [New](#)
- Key Pairs [New](#)
- Network Interfaces

Select a snapshot above

⋮ ⋯ ⋮

Create Snapshot

Select resource type Volume Instance

Volume*  

Description 

Encrypted Not Encrypted 

Key (128 characters maximum)

Value (256 characters maximum)

This resource currently has no tags

Choose the Add tag button or [click to add a Name tag](#)

Add Tag

50 remaining (Up to 50 tags maximum)

Cancel

Create Snapshot

Create Snapshot

✓ Create Snapshot Request Succeeded

[snap-0485aed3dca7f36ef](#)

[Manage Fast Snapshot Restore](#)

[Close](#)

New EC2 Experience
Tell us what you think

Create Snapshot

Actions ▾

- Delete
- Create Volume
- Manage Fast Snapshot Restore
- Create Image
- Copy
- Modify Permissions
- Add/Edit Tags

EC2 Dashboard New

Events New

Tags

Reports

Limits

▼ INSTANCES

Instances

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts New

Capacity Reservations

▼ IMAGES

AMIs

Bundle Tasks

▼ ELASTIC BLOCK
STORE

Volumes

Snapshots New

Search by keyword

?



1 to 1 of 1



Description	Status	Started	Progress
WordpressInstancebackupsks	completed	April 29, 2020 at 7:59:38 AM...	available (100%)

Snapshot ID	snap-0485aed3dca7f36ef	Progress	100%
Status	completed	Capacity	8 GiB
Volume	vol-0fba02bd8e1a22a3f	Encryption	Not Encrypted
Started	April 29, 2020 at 7:59:38 AM UTC+5:30	KMS Key ID	
Owner	951169881444	KMS Key Aliases	
Product codes	-	KMS Key ARN	
Description	WordpressInstancebackupsks	Fast Snapshot Restore	-

New EC2 Experience
Tell us what you think

Create Snapshot

Actions ▾



Owned By Me ▾



Filter by tags and attributes or search by keyword



1 to 1 of 1



EC2 Dashboard New

Events New

Tags

Reports

Limits

▼ INSTANCES

Instances

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts New

Capacity Reservations

▼ IMAGES

AMIs

Bundle Tasks

▼ ELASTIC BLOCK STORE

Volumes

Snapshots

Name	Snapshot ID	Size	Description	Status	Started	Progress
	snap-0485aed3dca...	8 GiB	WordpressInstancebackupsks	completed	April 29, 2020 at 7:59:38 AM...	available (100%)

Snapshot ID	snap-0485aed3dca7f36ef	Progress	100%
Status	completed	Capacity	8 GiB
Volume	vol-0fba02bd8e1a22a3f	Encryption	Not Encrypted
Started	April 29, 2020 at 7:59:38 AM UTC+5:30	KMS Key ID	
Owner	951169881444	KMS Key Aliases	
Product codes	-	KMS Key ARN	
Description	WordpressInstancebackupsks	Fast Snapshot Restore	-

New EC2 Experience
Tell us what you think

Create Snapshot

Actions ▾

- Delete
- Create Volume
- Manage Fast Snapshot Restore
- Create Image
- Copy
- Modify Permissions
- Add/Edit Tags

EC2 Dashboard New

Events New

Tags

Reports

Limits

▼ INSTANCES

Instances

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts New

Capacity Reservations

▼ IMAGES

AMIs

Bundle Tasks

▼ ELASTIC BLOCK STORE

Volumes

Snapshots

Search by keyword

?



1 to 1 of 1



Description	Status	Started	Progress
WordpressInstancebackupsks	completed	April 29, 2020 at 7:59:38 AM...	available (100%)

Snapshot ID	snap-0485aed3dca7f36ef	Progress	100%
Status	completed	Capacity	8 GiB
Volume	vol-0fba02bd8e1a22a3f	Encryption	Not Encrypted
Started	April 29, 2020 at 7:59:38 AM UTC+5:30	KMS Key ID	
Owner	951169881444	KMS Key Aliases	
Product codes	-	KMS Key ARN	
Description	WordpressInstancebackupsks	Fast Snapshot Restore	-

New EC2 Experience
Tell us what you think

Create Snapshot

Actions ▾



Owned By Me ▾

Filter by tags and attributes or search by keyword

?



1 to 1 of 1



Create Image from EBS Snapshot

Name

Description

Architecture

Virtualization type

Root device name

Kernel ID

RAM disk ID

Block Device Mappings

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)	Delete on Termination	Encrypted
Root	/dev/sda1	snap-0485aed3dca7f36ef	8	General Purpose SSD (gp2)	100 / 3000	N/A	<input checked="" type="checkbox"/>	Not Encrypted

Add New Volume

Cancel Create

Started April 29, 2020 at 7:59:38 AM UTC+5:30

KMS Key ID

Owner 951169881444

KMS Key Aliases

Product codes -

KMS Key ARN

Description WordpressInstancebackupsks

Fast Snapshot Restore -

New EC2 Experience
Tell us what you think

Create Snapshot

Actions ▾



Owned By Me ▾



Filter by tags and attributes or search by keyword



1 to 1 of 1



EC2 Dashboard New

Events New

Tags

Reports

Limits

▼ INSTANCES

Instances

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts New

Capacity Reservations

▼ IMAGES

AMIs

Bundle Tasks

▼ ELASTIC BLOCK STORE

Volumes

Snapshots

Name	Snapshot ID	Size	Description	Status	Started	Progress
	snap-0485aed3dca...	8 GiB	WordpressInstancebackupsks	completed	April 29, 2020 at 7:59:38 AM...	available (100%)

Create Image from EBS Snapshot



Create Image request received.

[View pending image ami-069223cf9a8e45c25](#)

Close

Snapshot ID	snap-0485aed3dca7f36ef	Progress	100%
Status	completed	Capacity	8 GiB
Volume	vol-0fba02bd8e1a22a3f	Encryption	Not Encrypted
Started	April 29, 2020 at 7:59:38 AM UTC+5:30	KMS Key ID	
Owner	951169881444	KMS Key Aliases	
Product codes	-	KMS Key ARN	
Description	WordpressInstancebackupsks	Fast Snapshot Restore	-

 New EC2 Experience
Tell us what you think

EC2 Dashboard New

Events New
Tags
Reports
Limits

INSTANCES
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts New
Capacity Reservations

IMAGES
AMIs
Bundle Tasks

ELASTIC BLOCK STORE
Volumes

Welcome to the new EC2 console!
We're redesigning the EC2 console to make it easier to use and improve performance. We'll release new screens periodically. We encourage you to try them and let us know where we can make improvements. To switch between the old console and the new console, use the New EC2 Experience toggle.

EC2

Resources

You are using the following Amazon EC2 resources in the Asia Pacific (Mumbai) Region:

Running instances	0	Elastic IPs	0
Dedicated Hosts	0	Snapshots	1
Volumes	1	Load balancers	0
Key pairs	7	Security groups	8
Placement groups	0		

Account attributes

Supported platforms Checkmark
• VPC
Default VPC Checkmark
vpc-cdac89a5
Console experiments
Settings

Explore AWS

Save up to 90% on EC2 with Spot Instances
Optimize price-performance by combining EC2 purchase options in a single EC2 ASG. [Learn more](#) Checkmark

Save 10% with AMD EPYC-Powered Instances

Launch instance **Service health**

New EC2 Experience
Tell us what you think

Launch

Actions



Owned by me

Filter by tags and attributes or search by keyword



< >

1 to 1 of 1

EC2 Dashboard

Events

Tags

Reports

Limits

▼ INSTANCES

Instances

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts

Capacity Reservations

▼ IMAGES

AMIs

Bundle Tasks

▼ ELASTIC BLOCK STORE

Volumes

Snapshots

Name	AMI Name	AMI ID	Source	Owner	Visibility	Status	Creation Date	Platform	Root De
	mysksimage	ami-069223cf9a8e45c25	951169881444/...	951169881444	Private	available	April 29, 2020 at 8:03:46 AM...	Other Linux	ebs

Image: ami-069223cf9a8e45c25

Details

Permissions

Tags

Edit

AMI ID: ami-069223cf9a8e45c25

Owner: 951169881444

Status: available

AMI Name: mysksimage

Source: 951169881444/mysksimage

State Reason: -

[1. Choose AMI](#)[2. Choose Instance Type](#)[3. Configure Instance](#)[4. Add Storage](#)[5. Add Tags](#)[6. Configure Security Group](#)[7. Review](#)

Step 2: Choose an Instance Type

Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. [Learn more](#) about instance types and how they can meet your computing needs.

Filter by: [All instance types](#) [Current generation](#) [Show/Hide Columns](#)

Currently selected: t2.micro (Variable ECUs, 1 vCPUs, 2.5 GHz, Intel Xeon Family, 1 GiB memory, EBS only)

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance	IPv6 Support
<input type="checkbox"/>	General purpose	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
<input checked="" type="checkbox"/>	General purpose	t2.micro <small>Free tier eligible</small>	1	1	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	General purpose	t2.small	1	2	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	General purpose	t2.medium	2	4	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	General purpose	t2.large	2	8	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	General purpose	t2.xlarge	4	16	EBS only	-	Moderate	Yes
<input type="checkbox"/>	General purpose	t2.2xlarge	8	32	EBS only	-	Moderate	Yes
<input type="checkbox"/>	General purpose	t3a.nano	2	0.5	EBS only	Yes	Up to 5 Gigabit	Yes

[Cancel](#)[Previous](#)[Review and Launch](#)[Next: Configure Instance Details](#)

[1. Choose AMI](#)[2. Choose Instance Type](#)[3. Configure Instance](#)[4. Add Storage](#)[5. Add Tags](#)[6. Configure Security Group](#)[7. Review](#)

Step 7: Review Instance Launch

Please review your instance launch details. You can go back to edit changes for each section. Click **Launch** to assign a key pair to your instance and complete the launch process.



Improve your instances' security. Your security group, launch-wizard-6, is open to the world.

Your instances may be accessible from any IP address. We recommend that you update your security group rules to allow access from known IP addresses only.

You can also open additional ports in your security group to facilitate access to the application or service you're running, e.g., HTTP (80) for web servers. [Edit security groups](#)

AMI Details

[Edit AMI](#)**mysksimage - ami-069223cf9a8e45c25**

Root Device Type: ebs Virtualization type: hvm

Instance Type

[Edit instance type](#)

Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
t2.micro	Variable	1	1	EBS only	-	Low to Moderate

Security Groups

[Edit security groups](#)**Security group name**

launch-wizard-6

Description

launch-wizard-6 created 2020-04-29T08:09:07.610+05:30

[Cancel](#)[Previous](#)[Launch](#)[Define key pair and launch](#)

New EC2 Experience
Tell us what you think

EC2 Dashboard [New](#)

Events [New](#)

Tags

Reports

Limits

INSTANCES

Instances

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts

Capacity Reservations

IMAGES

AMIs

Bundle Tasks

ELASTIC BLOCK STORE

Volumes

Snapshots

Feedback

Launch Instance

Connect

Actions

Filter by tags and attributes or search by keyword

?

1 to 6 of 6

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)
az-1b-sks2	i-00d3111cd3b35c0d0	t2.micro	ap-south-1b	stopped		None	
az-1a-sks2	i-03acd8bd91c906f78	t2.micro	ap-south-1a	stopped		None	
az-1a-sks	i-066e9948d76d36a87	t2.micro	ap-south-1a	stopped		None	
az-1b-sks	i-0b3840e322346400d	t2.micro	ap-south-1b	stopped		None	
	i-0bd974128fabf906e	t2.micro	ap-south-1a	stopped		None	
	i-024dff4066548cfb9	t2.micro	ap-south-1b	running	2/2 checks ...	None	ec2-13-233-157-240.ap...

ubuntu@ip-172-31-4-43: ~

login as: ubuntu

[Authenticating with public key "imported-openssh-key"]

Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-1065-aws x86_64)

* Documentation: <https://help.ubuntu.com>

* Management: <https://landscape.canonical.com>

* Support: <https://ubuntu.com/advantage>

System information as of Wed Apr 29 02:44:49 UTC 2020

System load: 0.16 Processes: 95

Usage of /: 27.9% of 7.69GB Users logged in: 0

Memory usage: 33% IP address for eth0: 172.31.4.43

Swap usage: 0%

* Ubuntu 20.04 LTS is out, raising the bar on performance, security, and optimisation for Intel, AMD, Nvidia, ARM64 and z15 as well as AWS, Azure and Google Cloud.

ubuntu.amazonaws.com

Public DNS (IPv4) ec2-13-233-157-240.ap-south-1.compute.amazonaws.com

IPv4 Public IP 13.233.157.240

IPv6 IPs -

Elastic IPs

Availability zone ap-south-1b

© 2008 - 2020, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. [Privacy Policy](#) [Terms of Use](#)