



VIT[®]
BHOPAL
www.vitbhopal.ac.in

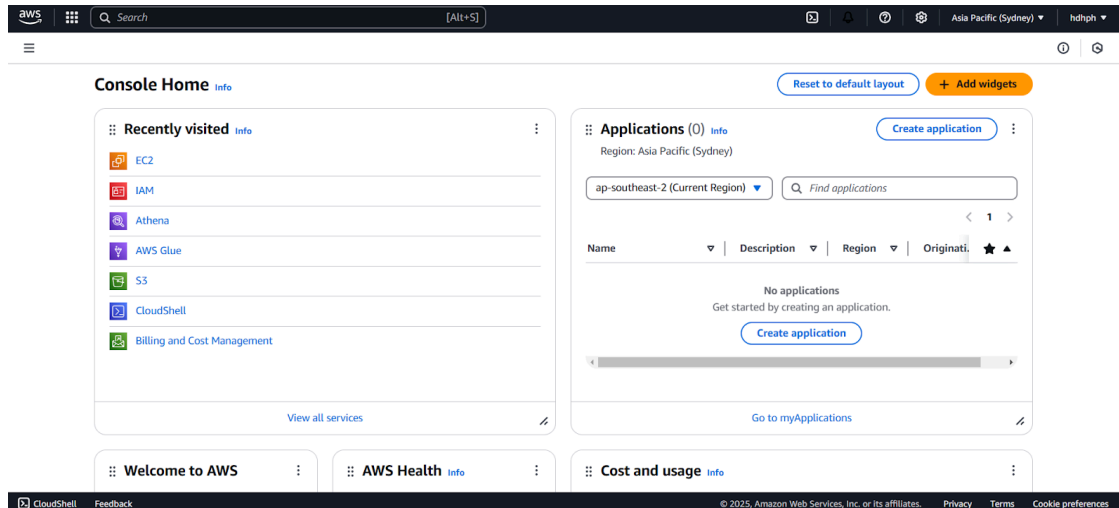
Practical 3

(Create an S3 bucket and Configure bucket policies, versioning, and encryption. Upload and download objects to/from the S3 bucket.)

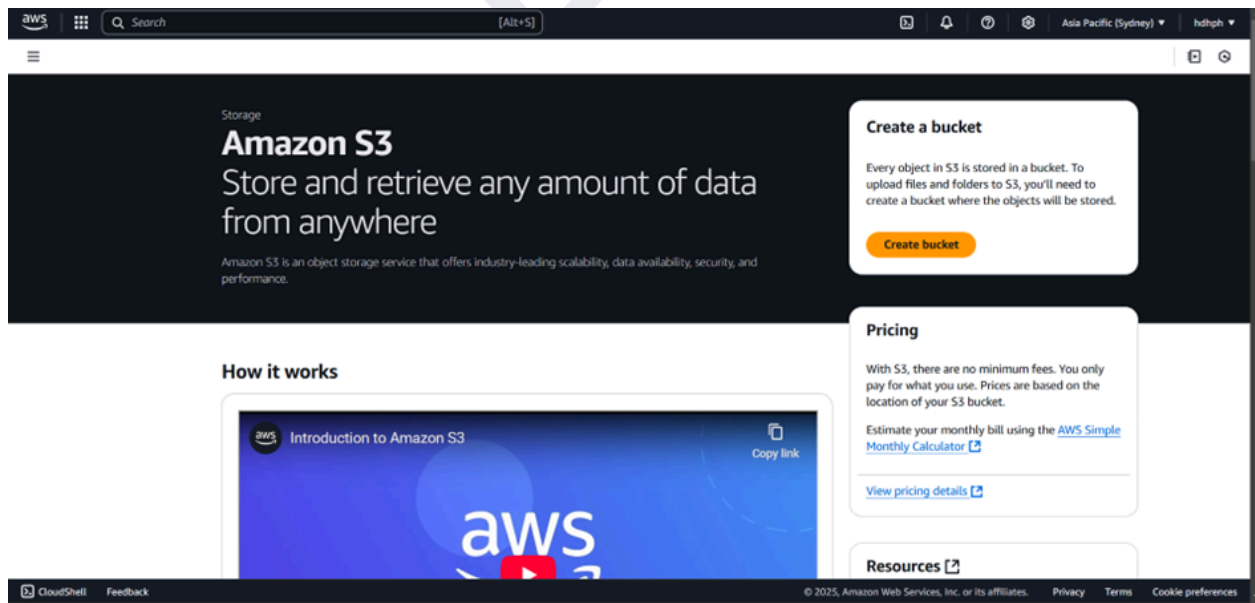
Name: Arpita Rajput
Reg. No. 22MIP10001

Windows instance

Step 1: Sign in to the AWS Management Console & Go to Services S3



Step 2: Click on “Create Bucket”



Step 3: Choose Connect -> RDP connection Choose Get Password, and then choose Choose File (demo2.pem) and generate one password.

Create bucket [Info](#)

Buckets are containers for data stored in S3.

General configuration

AWS Region
Asia Pacific (Seoul) ap-northeast-2

Bucket name [Info](#)
arpitarajpu

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

Step 4: Download the remote desktop file (demo2.rdp).

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.

Turning off block all public access might result in this bucket and the objects within becoming public
AWS recommends that you turn on block all public access, unless public access is required for specific and verified use cases such as static website hosting.

☒ I acknowledge that the current settings might result in this bucket and the objects within becoming public.

Step 5: Choose Connect. You will get the windows screen of your Instance with the EC2 instance information. Remote Desktop Protocol (RDP): RDP is the go-to method for connecting to Windows instances.

aws

Search

[Alt+S]

Asia Pacific (Seoul)

hdhph

Amazon S3

Buckets

Successfully created bucket "arpitarajput"

To upload files and folders, or to configure additional bucket settings, choose [View details](#).

View details

Account snapshot - updated every 24 hours

All AWS Regions

View Storage Lens dashboard

Storage lens provides visibility into storage usage and activity trends. Metrics don't include directory buckets. [Learn more](#)

General purpose buckets

Directory buckets

General purpose buckets (2)

Info

All AWS Regions

Copy ARN

Empty

Delete

Create bucket

Buckets are containers for data stored in S3.

Find buckets by name

< 1 >

Name	AWS Region	IAM Access Analyzer	Creation date
arpitarajput	Asia Pacific (Seoul) ap-northeast-2	View analyzer for ap-northeast-2	February 27, 2025, 10:55:40 (UTC+05:30)
simple-devops-demo1	Asia Pacific (Seoul) ap-northeast-2	View analyzer for ap-northeast-2	February 25, 2025, 10:40:59 (UTC+05:30)

aws

Search

[Alt+S]

Asia Pacific (Seoul)

hdhph

Amazon S3

Buckets

arpitarajput

arpitarajput

Info

ObjectsPropertiesPermissionsMetricsManagementAccess Points

Objects (0)

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

< 1 >

Name

Type

Last modified

Size

Storage class

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

Upload

ap-northeast-2.console.aws.amazon.com/s3/upload/arpitarajput?region=ap-northeast-2&bucketType=general

aws

Search

[Alt+S]

Asia Pacific (Seoul)

hdhph

Amazon S3

Buckets

arpitarajput

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 SDKs 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, 4.6 KB)

Remove

Add files

Add folder

All files and folders in this table will be uploaded.

Find by name

< 1 >

Name

Folder

Type

Size

hack.html

-

text/html

4.6 KB

Destination

Info

Destination

[s3://arpitarajput](#)

Destination details

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

Permissions

CloudShell

Feedback

© 2025, Amazon Web Services, Inc. or its affiliates.

Privacy

Terms

Cookie preferences

26°C

Sunny

Search

10:57

27-02-2025

aws

Search

[Alt+S]

Asia Pacific (Seoul)

hdhph

Upload succeeded

For more information, see the Files and folders table.

Close

Upload: status

After you navigate away from this page, the following information is no longer available.

Summary

Destination

s3://arpitarajput

Succeeded

1 file, 4.6 KB (100.00%)

Failed

0 files, 0 B (0%)

Files and folders

Configuration

Files and folders (1 total, 4.6 KB)

Find by name

Name	Folder	Type	Size	Status	Error
hack.html	-	text/html	4.6 KB	Succeeded	-

aws

Search

[Alt+S]

Asia Pacific (Seoul)

hdhph

Amazon S3

Buckets

arpitarajput

hack.html

hack.html

Copy S3 URI

Download

Open

Object actions

Properties

Permissions

Versions

Object overview

Owner

78b4a971717b08f909935e86de4635022c0c5e0eb42735a96a051e98a6d5a3f8

AWS Region

Asia Pacific (Seoul) ap-northeast-2

Last modified

February 27, 2025, 10:58:00 (UTC+05:30)

Size

4.6 KB

Type

html

Key

hack.html

S3 URI

s3://arpitarajput/hack.html

Amazon Resource Name (ARN)

arn:aws:s3:::arpitarajput/hack.html

Entity tag (Etag)

5af3248d972cd8d50e81150e84cd8a17

Object URL

https://arpitarajput.s3.ap-northeast-2.amazonaws.com/hack.html

Object management overview

Amazon S3> Buckets> arpitaraiput> hack.html

hack.htmlInfo

Copy S3 URIDownloadOpenObject actions

PropertiesPermissionsVersions

Access control list (ACL)Edit

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: 78b4a971717b08f909935e86de4635022c0c5e0eb42735a96a051e98a6d5a3f8	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	-	-

CloudShellFeedback© 2025, Amazon Web Services, Inc. or its affiliates. PrivacyTermsCookie preferences26°C11:2027.02.2023

aws

Search[Alt+S]

Asia Pacific (Seoul)hdhph

Amazon S3> Buckets> arpitaraiput> Edit Block public access (bucket settings)

Edit Block public access (bucket settings)Info

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 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

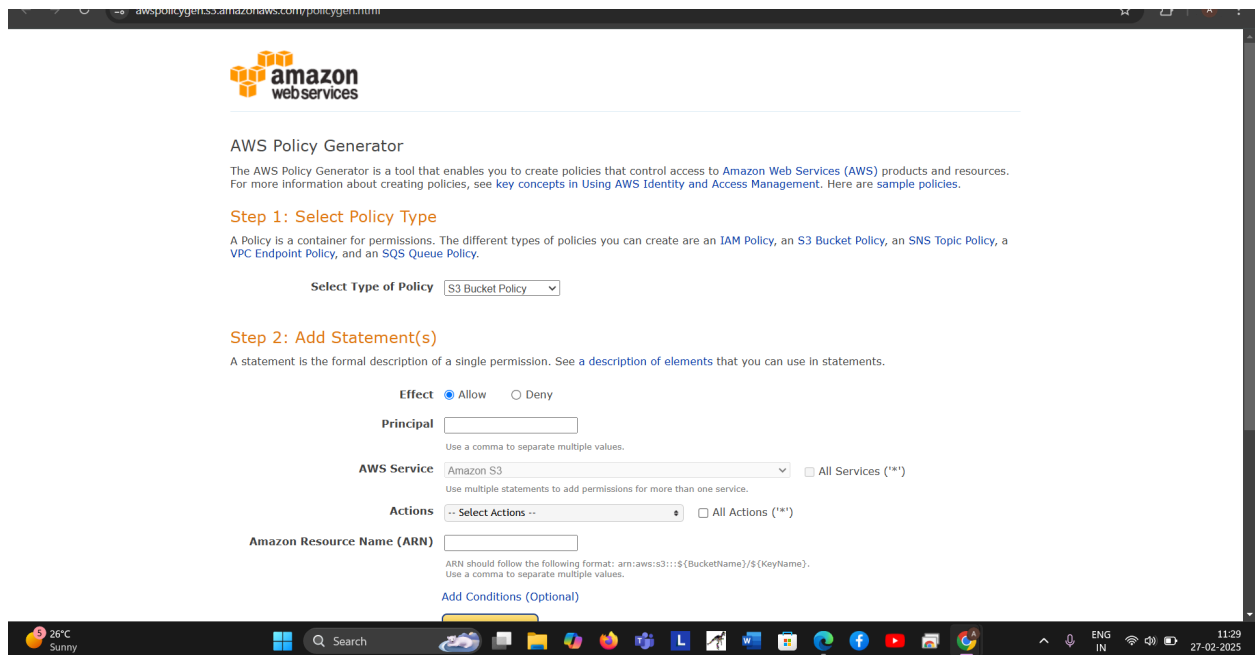
S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.

☒ 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.

CancelSave changes

aws:policygenerator:amazonaws.com/policygenerator.html



amazon
webservices

AWS Policy Generator

The AWS Policy Generator is a tool that enables you to create policies that control access to [Amazon Web Services \(AWS\)](#) products and resources. For more information about creating policies, see [key concepts in Using AWS Identity and Access Management](#). Here are [sample policies](#).

Step 1: Select Policy Type

A Policy is a container for permissions. The different types of policies you can create are an [IAM Policy](#), an [S3 Bucket Policy](#), an [SNS Topic Policy](#), a [VPC Endpoint Policy](#), and an [SQS Queue Policy](#).

Select Type of Policy

Step 2: Add Statement(s)

A statement is the formal description of a single permission. See a [description of elements](#) that you can use in statements.

Effect ☒ Allow ☐ Deny

Principal

Use a comma to separate multiple values.

AWS Service ☐ All Services (**)

Use multiple statements to add permissions for more than one service.

Actions ☐ All Actions (**)

Amazon Resource Name (ARN)

ARN should follow the following format: `arn:aws:s3:::{BucketName}/{Key}`.
Use a comma to separate multiple values.

[Add Conditions \(Optional\)](#)

Step 1: Select Policy Type

A Policy is a container for permissions. The different types of policies you can create are an [IAM Policy](#), an [S3 Bucket Policy](#), an [SNS Topic Policy](#), a [VPC Endpoint Policy](#), and an [SQS Queue Policy](#).

Select Type of Policy

Step 2: Add Statement(s)

A statement is the formal description of a single permission. See a [description of elements](#) that you can use in statements.

Effect ☒ Allow ☐ Deny

Principal

Use a comma to separate multiple values.

AWS Service ☐ All Services (**)

Use multiple statements to add permissions for more than one service.

Actions ☐ All Actions (**)

Amazon Resource Name (ARN)

☐ GetBucketLocation
☐ GetBucketLogging
☐ GetBucketMetadataTableConfiguration
☐ GetBucketNotification
☐ GetBucketObjectLockConfiguration
☐ GetBucketOwnershipControls
☒ GetBucketPolicy
☐ GetBucketPolicyStatus

[Add Conditions \(Optional\)](#)

Use a comma to separate multiple values.

ARN should follow the following format: `arn:aws:s3:::{BucketName}/{Key}`.
Use a comma to separate multiple values.

[Add Conditions \(Optional\)](#)

Step 3: Generate Policy

A *policy* is a document (written in the [Access Policy Language](#)) that acts as a container for one or more statements.

Add one or more statements above to generate a policy.