

S3 Versioning, CRR, Static Web Hosting

The screenshot shows the AWS Console Home page. It includes sections for Recently visited (EC2, S3), Applications (0), and Cost and usage. The Applications section shows a message to 'Get started by creating an application.' and a 'Create application' button. The Cost and usage section displays current month costs (\$0.37) and forecasted month end costs (\$1.07). A sidebar on the left provides links to Welcome to AWS, AWS Health, and Storage.

The screenshot shows the Amazon S3 landing page. It features a large heading 'Amazon S3' with the subtext 'Store and retrieve any amount of data from anywhere'. Below this, it says 'Amazon S3 is an object storage service that offers industry-leading scalability, data availability, security, and performance.' A 'Create a bucket' button is prominently displayed. Other sections include 'How it works' (with a video thumbnail for 'Introduction to Amazon S3'), 'Pricing' (mentioning no minimum fees), and 'Resources' (links to User guide and API reference).

S3 Versioning, CRR, Static Web Hosting

The screenshot shows the 'Create bucket' page in the AWS S3 console. Under 'General configuration', the 'Bucket name' is set to 'myawsbucket'. The 'Bucket type' is selected as 'General purpose', which is described as recommended for most use cases. A note states that bucket names must be 3 to 63 characters long and unique. There is also a section for 'Copy settings from existing bucket - optional' with a 'Choose bucket' button.

General configuration

AWS Region
US East (N. Virginia) us-east-1

Bucket type [Info](#)

General purpose
Recommended for most use cases and access patterns. General purpose buckets are the original S3 bucket type. They allow a mix of storage classes that redundantly store objects across multiple Availability Zones.

Directory
Recommended for low-latency use cases. These buckets use only the S3 Express One Zone storage class, which provides faster processing of data within a single Availability Zone.

Bucket name [Info](#)
myawsbucket

Bucket names must be 3 to 63 characters and unique within the global namespace. Bucket names must also begin and end with a letter or number. Valid characters are a-z, 0-9, periods (.), and hyphens (-). [Learn More](#)

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.

© 2025, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

The screenshot shows the 'Create bucket' page in the AWS S3 console. Under 'Object Ownership', the 'ACLs enabled' option is selected, which is described as allowing objects to be owned by other AWS accounts. A note recommends disabling ACLs unless individual object access control is needed. There is also a section for 'Object Ownership' with 'Bucket owner preferred' selected.

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.

⚠️ We recommend disabling ACLs, unless you need to control access for each object individually or to have the object writer own the data they upload. Using a bucket policy instead of ACLs to share data with users outside of your account simplifies permissions management and auditing.

Object Ownership

Bucket owner preferred
If new objects written to this bucket specify the bucket-owner-full-control canned ACL, they are owned by the bucket owner. Otherwise, they are owned by the object writer.

Object writer
The object writer remains the object owner.

ⓘ If you want to enforce object ownership for new objects only, your bucket policy must specify that the bucket-owner-full-control canned ACL is required for object uploads. [Learn more](#)

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
Blocks public access to this bucket and its objects through access control lists (ACLs).

© 2025, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

S3 Versioning, CRR, Static Web Hosting

The screenshot shows the 'Create bucket' step of the AWS S3 wizard. Under 'Block Public Access settings for this bucket', several options are listed:

- 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.

A warning message in a box states: "⚠️ 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." A checkbox labeled "I acknowledge that the current settings might result in this bucket and the objects within becoming public." is checked.

The screenshot shows the 'Create bucket' step of the AWS S3 wizard. Under 'Bucket Versioning', it says: "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." A link to "Learn more" is provided. Below this, a section titled "Bucket Versioning" has a radio button for "Enable" which is selected, while "Disable" is unselected.

The screenshot shows the 'Create bucket' step of the AWS S3 wizard. Under 'Tags - optional (0)', it says: "You can use bucket tags to track storage costs and organize buckets." A link to "Learn more" is provided. It shows "No tags associated with this bucket." and a blue "Add tag" button.

The screenshot shows the 'Create bucket' step of the AWS S3 wizard. Under 'Default encryption', it says: "Server-side encryption is automatically applied to new objects stored in this bucket." A section titled "Encryption type" has a radio button for "Server-side encryption with Amazon S3 managed keys (SSE-S3)" which is selected, while "Server-side encryption with AWS Key Management Service keys (SSE-KMS)" and "Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)" are unselected. A note states: "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](#)." A section titled "Bucket Key" notes: "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." A radio button for "Disable" is shown.

S3 Versioning, CRR, Static Web Hosting

The screenshot shows the AWS S3 Buckets page. A green success message at the top states: "Successfully created bucket 'kmittankbund'. To upload files and folders, or to configure additional bucket settings, choose View details." Below this, an "Account snapshot" section provides storage usage and activity trends. At the bottom, there are tabs for "General purpose buckets" and "Directory buckets", with "General purpose buckets" selected. A table lists one bucket: "kmittankbund" (Name), "US East (N. Virginia) us-east-1" (AWS Region), "View analyzer for us-east-1" (IAM Access Analyzer), and "March 15, 2025, 14:41:33 (UTC+05:30)" (Creation date). Action buttons include "Copy ARN", "Empty", "Delete", and "Create bucket".

The screenshot shows the AWS S3 Objects page for the "kmittankbund" bucket. The top navigation bar includes CloudShell, Feedback, and links for CC-3-2-CS-3C-2024_25, CC-3-2-CS-3C-2024_25, CC-3-2-CS, Launch AWS Academy Learner Lab, and kmittankbund - S3 bucket | S3. The main content area shows the "Objects" tab selected, displaying a table with no objects. The table has columns for Name, Type, Last modified, Size, and Storage class. Buttons for Actions, Create folder, and Upload are available. A note at the top says: "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](#)".



S3 Versioning, CRR, Static Web Hosting

The screenshot shows the AWS S3 'Upload' interface. At the top, there are tabs for 'CC-3-2-CS-3C-2024_25: CC-3-2-CS-' and 'Launch AWS Academy Learner Lab'. The main navigation bar includes 'Search' (Alt+S), a bell icon, a gear icon, and 'United States (N. Virginia)'. The user's email, 'voclabs/user3879096=reddyprasad.kmit@gmail.com @ 8269-1826-5081', is also visible.

The page title is 'Upload objects - S3 bucket km...'. The breadcrumb navigation shows 'Amazon S3 > Buckets > kmittankbund > 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, 1.0 MB)

All files and folders in this table will be uploaded.

<input type="checkbox"/>	Name	Folder	Type	Size
<input type="checkbox"/>	Background (1).png	-	image/png	1.0 MB

[Remove](#) [Add files](#) [Add folder](#)

Destination Info

Destination [s3://kmittankbund](#)

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.

Access control list (ACL)

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

AWS recommends using S3 bucket policies or IAM policies for access control. [Learn more](#)

Access control list (ACL)

Choose from predefined ACLs

Specify individual ACL permissions

Predefined ACLs

Private (recommended)
Only the object owner will have read and write access.

Grant public-read access
Anyone in the world will be able to access the specified objects. The object owner will have read and write access. [Learn more](#)

Granting public-read access is not recommended

Anyone in the world will be able to access the specified objects. [Learn more](#)

I understand the risk of granting public-read access to the specified objects.

© 2025, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

S3 Versioning, CRR, Static Web Hosting

The screenshot shows the AWS S3 console with a success message: "Upload succeeded". It displays a summary of upload status: 1 file succeeded (1.0 MB) and 0 files failed (0 B). A table lists the uploaded file "Background (1).png" with details: Name, Folder, Type (image/png), Size (1.0 MB), Status (Succeeded), and Error (-). A note at the top says: "After you navigate away from this page, the following information is no longer available."

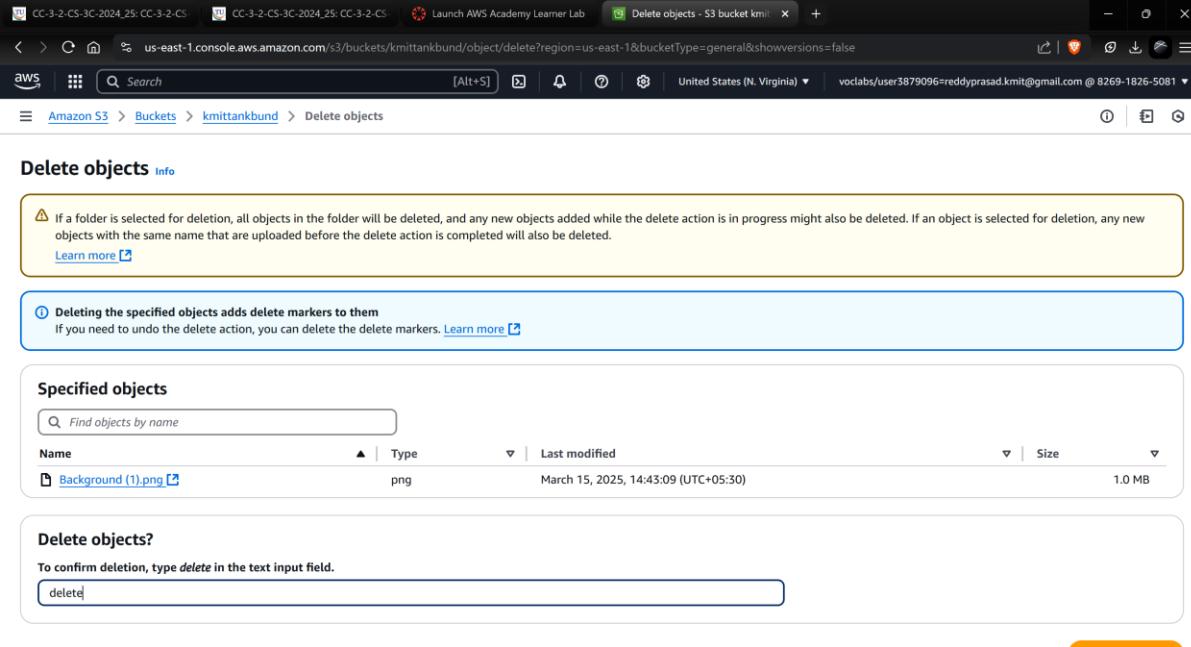
Name	Folder	Type	Size	Status	Error
Background (1).png	-	image/png	1.0 MB	Succeeded	-

The screenshot shows the AWS S3 console for the bucket "kmittankbund". It displays a list of objects: "Background (1).png" (1.0 MB, Standard storage class). The interface includes tabs for Objects, Metadata, Properties, Permissions, Metrics, Management, and Access Points. Buttons for Actions (Create folder, Upload) and object-specific actions (Copy S3 URI, Copy URL, Download, Open) are visible.

Name	Type	Last modified	Size	Storage class
Background (1).png	png	March 15, 2025, 14:43:09 (UTC+05:30)	1.0 MB	Standard



S3 Versioning, CRR, Static Web Hosting



Delete objects Info

Specified objects

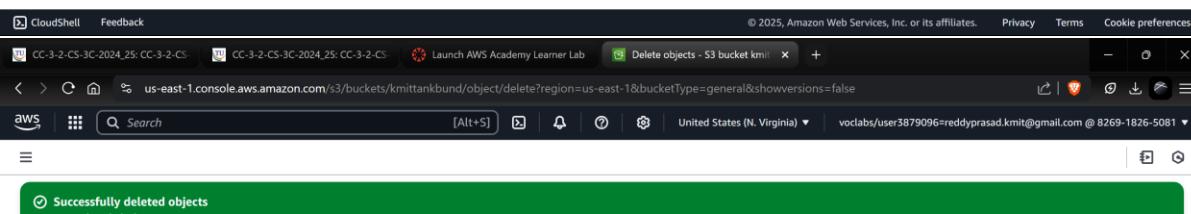
Name	Type	Last modified	Size
Background (1).png	png	March 15, 2025, 14:43:09 (UTC+05:30)	1.0 MB

Delete objects?

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

delete

Cancel **Delete objects**



Successfully deleted objects
View details below.

Delete objects: status Close

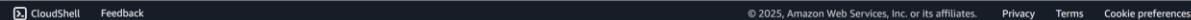
Summary

Source	Successfully deleted	Failed to delete
s3://kmittankbund	1 object, 1.0 MB	0 objects

Failed to delete Configuration

Failed to delete (0)

Name	Type	Last modified	Size	Error
No objects failed to delete.				



Successfully deleted objects

S3 Versioning, CRR, Static Web Hosting

The screenshot shows the AWS S3 console interface. The top navigation bar includes tabs for 'CC-3-2-CS-3C-2024_25: CC-3-2-CS-' and 'Launch AWS Academy Learner Lab'. The main title is 'kmittankbund - S3 bucket | \$3'. The search bar contains 'Search [Alt+S]'. The location bar shows 'us-east-1.console.aws.amazon.com/s3/buckets/kmittankbund?region=us-east-1&bucketType=general&tab=objects'. The user information is 'voclabs/user3879096=reddyprasad.kmit@gmail.com @ 8269-1826-5081'. Below the header, the breadcrumb navigation shows 'Amazon S3 > Buckets > kmittankbund'. The main content area is titled 'kmittankbund Info'. A navigation bar at the top of the content area includes 'Objects', 'Metadata', 'Properties', 'Permissions', 'Metrics', 'Management', and 'Access Points'. The 'Objects' tab is selected. Below this is a toolbar with actions: Copy S3 URI, Copy URL, Download, Open, Delete, Actions (dropdown), Create folder, and Upload. A search bar says 'Find objects by prefix'. A table header for 'Objects (0)' includes columns for Name, Type, Last modified, Size, and Storage class. A message states 'No objects' and 'You don't have any objects in this bucket.' A prominent blue 'Upload' button is at the bottom.

This screenshot shows the same AWS S3 console interface as the previous one, but now the 'Objects' table contains two entries. The table header is identical: 'Name', 'Type', 'Version ID', 'Last modified', 'Size', and 'Storage class'. The first entry is 'Background (1).png', which is a 'Delete marker' with a Version ID of '_tOV_CMnllyrmSgUlgAMaJ75_3_yKsxaU3' and was last modified on March 15, 2025, at 14:44:32 (UTC+05:30). It has a size of 0 B and is in the Standard storage class. The second entry is another 'Background (1).png' file, which is a 'png' file with a Version ID of 'D19THpXD4xyQN9wEiPoOj33BzIOIEWXb' and was last modified on March 15, 2025, at 14:43:09 (UTC+05:30). It has a size of 1.0 MB and is in the Standard storage class.



S3 Versioning, CRR, Static Web Hosting

Name	Type	Version ID	Last modified	Size	Storage class
Background (1).png	Delete marker	_tOV_CMnlyrmSgUlgAMaJ75_3_yKsxaU3	March 15, 2025, 14:44:32 (UTC+05:30)	0 B	-
Background (1).png	png	D19THpXD4xyQN9wEiPoOI3_3BzIOIEWx	March 15, 2025, 14:43:09 (UTC+05:30)	1.0 MB	Standard

Name	Version ID	Type	Last modified	Size
Background (1).png	_tOV_CMnlyrmSgUlgAMaJ75_3_yKsxaU3	Delete marker	March 15, 2025, 14:44:32 (UTC+05:30)	0 B

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

Cancel **Delete objects**

S3 Versioning, CRR, Static Web Hosting

The screenshot shows the AWS S3 console with a green header bar indicating "Successfully deleted objects". Below it, a summary table shows one object successfully deleted and zero failed. Under the "Failed to delete" tab, there are no entries. A note at the bottom says "After you navigate away from this page, the following information is no longer available.".

The screenshot shows the AWS S3 console with a header for "Upload objects - S3 bucket kmittankbund". The main area is titled "Upload" and contains a "Files and folders (0)" section with a table showing zero files or folders. It also includes sections for "Destination" (set to s3://kmittankbund) and "Permissions".

S3 Versioning, CRR, Static Web Hosting

The screenshot shows the AWS S3 console interface for uploading files to a bucket named 'kmittankbund'. The top navigation bar includes tabs for 'CC-3-2-CS-3C-2024_25: CC-3-2-CS-' and 'CC-3-2-CS-3C-2024_25: CC-3-2-CS-', 'Launch AWS Academy Learner Lab', and 'Upload objects - S3 bucket km...'. The main content area shows a file upload dialog with a message: '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'.

Files and folders (1 total, 3.1 KB)

Name	Type	Size
portfolio using Bootstrap.html	text/html	3.1 KB

Destination [Info](#)
Destination: <s3://kmittankbund>

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.

Upload (Orange button)

Upload succeeded
For more information, see the [Files and folders](#) table.

Upload: status

Summary

Destination	Succeeded	Failed
s3://kmittankbund	1 file, 3.1 KB (100.00%)	0 files, 0 B (0%)

Files and folders (1 total, 3.1 KB)

Name	Folder	Type	Size	Status	Error
portfolio using Bootstrap.html	-	text/html	3.1 KB	Succeeded	-

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

S3 Versioning, CRR, Static Web Hosting

Objects (1/2)

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](#)

Name	Type	Last modified	Size	Storage class
Background (1).png	png	March 15, 2025, 14:43:09 (UTC+05:30)	1.0 MB	Standard
portfolio using Bootstrap.html	html	March 15, 2025, 14:48:08 (UTC+05:30)	3.1 KB	Standard

Bucket overview

AWS Region: US East (N. Virginia) us-east-1

Amazon Resource Name (ARN): arn:aws:s3:::kmittankbund

Creation date: March 15, 2025, 14:41:33 (UTC+05:30)

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
Enabled

Multi-factor authentication (MFA) delete
An additional layer of security that requires multi-factor authentication for changing Bucket Versioning settings and permanently deleting object versions. To modify MFA delete settings, use the AWS CLI, AWS SDK, or the Amazon S3 REST API. [Learn more](#)

Disabled

Tags (0)

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

Key	Value
No tags associated with this resource.	

S3 Versioning, CRR, Static Web Hosting

The screenshot shows the AWS S3 Bucket Properties page for the bucket 'kmittankbund'. It includes sections for Object Lock (disabled), Requester pays (disabled), and Static website hosting (disabled). A note recommends using AWS Amplify Hosting for static website hosting.

Object Lock
Disabled

Requester pays
Disabled

Static website hosting
Disabled

We recommend using AWS Amplify Hosting for static website hosting

The screenshot shows the 'Edit static website hosting' configuration page for the 'kmittankbund' bucket. It includes sections for enabling static website hosting, specifying the index document as 'portfolio using Bootstrap.html', and setting the error document as 'error.html'. A note states that customers must make all content publicly readable.

Enable

Hosting type

Host a static website
Use the bucket endpoint as the web address. [Learn more](#)

Redirect requests for an object
Redirect requests to another bucket or domain. [Learn more](#)

For your customers to access content at the website endpoint, you must make all your content publicly readable. To do so, you can edit the S3 Block Public Access settings for the bucket. For more information, see [Using Amazon S3 Block Public Access](#).

Index document
Specify the home or default page of the website.
portfolio using Bootstrap.html

Error document - optional
This is returned when an error occurs.
error.html

S3 Versioning, CRR, Static Web Hosting

The screenshot shows the AWS S3 Bucket Properties page for the bucket 'kmittankbund'. The 'Properties' tab is selected. Key details include:

- AWS Region:** US East (N. Virginia) us-east-1
- Amazon Resource Name (ARN):** arn:aws:s3:::kmittankbund
- Creation date:** March 15, 2025, 14:41:33 (UTC+05:30)

Bucket Versioning: Enabled. 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](#)

Multi-factor authentication (MFA) delete: Disabled. An additional layer of security that requires multi-factor authentication for changing Bucket Versioning settings and permanently deleting object versions. To modify MFA delete settings, use the AWS CLI, AWS SDK, or the Amazon S3 REST API. [Learn more](#)

Tags (0): You can use bucket tags to track storage costs and organize buckets. [Learn more](#)

The screenshot shows the AWS S3 Upload page for the 'kmittankbund' bucket. The 'Upload' tab is selected. Key features include:

- Upload:** Add files and folders to upload to S3. A large dashed blue box allows dragging and dropping files or choosing files/folders.
- Files and folders:** (1 total, 10.0 B)

Name	Type	Size
error.html	text/html	10.0 B
- Destination:** s3://kmittankbund
- 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.

S3 Versioning, CRR, Static Web Hosting

The screenshot shows the AWS S3 'Upload' interface. The 'Destination' field is set to `s3://kmittankbund`. Under 'Destination details', it says 'Bucket settings that impact new objects stored in the specified destination.' Below this is a 'Permissions' section with the note 'Grant public access and access to other AWS accounts.' A 'Access control list (ACL)' section follows, with the note 'Grant basic read/write permissions to other AWS accounts.' A blue callout box contains the text 'AWS recommends using S3 bucket policies or IAM policies for access control.' Under 'Access control list (ACL)', there are two options: 'Choose from predefined ACLs' (selected) and 'Specify individual ACL permissions'. The 'Predefined ACLs' section includes 'Private (recommended)' (unchecked) and 'Grant public-read access' (checked). The checked option allows anyone in the world to access the specified objects. A warning message 'Granting public-read access is not recommended' is shown, stating 'Anyone in the world will be able to access the specified objects.' A checkbox labeled 'I understand the risk of granting public-read access to the specified objects.' is checked.

The screenshot shows the AWS S3 'Upload: status' page. A green banner at the top says 'Upload succeeded' and 'For more information, see the Files and folders table.' A 'Close' button is in the top right. Below is a 'Summary' section with 'Destination' set to `s3://kmittankbund`. It shows 'Succeeded' (1 file, 10.0 B (100.00%)) and 'Failed' (0 files, 0 B (0%)). Below is a 'Files and folders' table with one entry: 'error.html' (text/html, 10.0 B, Status: Succeeded). The table has columns: Name, Folder, Type, Size, Status, and Error.

This is a continuation of the screenshot above, showing the 'Files and folders' table in the 'Upload: status' section. The table lists one file: 'error.html' (text/html, 10.0 B, Status: Succeeded).

S3 Versioning, CRR, Static Web Hosting

Object Lock
Disabled

Requester pays
When enabled, the requester pays for requests and data transfer costs, and anonymous access to this bucket is disabled. [Learn more](#)

Requester pays
Disabled

Static website hosting
Use this bucket to host a website or redirect requests. [Learn more](#)

We recommend using AWS Amplify Hosting for static website hosting
Deploy a fast, secure, and reliable website quickly with AWS Amplify Hosting. Learn more about [Amplify Hosting](#) or [View your existing Amplify apps](#)

S3 static website hosting
Enabled

Hosting type
Bucket hosting

Bucket website endpoint
When you configure your bucket as a static website, the website is available at the AWS Region-specific website endpoint of the bucket. [Learn more](#)
<http://kmittankbund.s3-website-us-east-1.amazonaws.com>

REDDY LEELA VENKATA KRISHNA PRASAD

About
Skilled in developing optimized code for enhanced performance and scalability. Possesses strong problem-solving abilities and thrives as a collaborative team player, committed to delivering high-quality results.

Skills
• **Languages:** Java, C++, SQL, C, Python
• **Technologies & Frameworks:** MERN, GitHub, Spring
• **Soft skills:** Communication, Leadership

Projects
• [Image Steganography](#) | Python, Bootstrap, Tkinter
• [Speech Emotion Recognition on Calls](#) | Python, Flask, HTML, CSS, JavaScript, Neural Networks

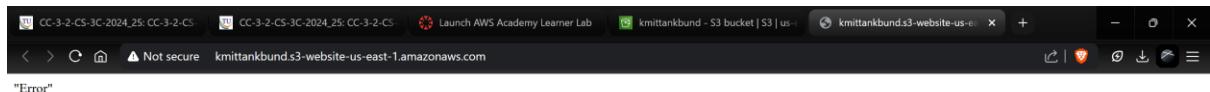
Achievements
• Improved Google Maps algorithm performance by 12%.
• Contributed to open-source projects on GitHub.

S3 Versioning, CRR, Static Web Hosting

The screenshot shows the 'Delete objects' page in the AWS S3 console. A single object, 'portfolio_using_Bootstrap.html', is selected for deletion. The object is listed in the 'Specified objects' table with details: Name: portfolio_using_Bootstrap.html, Type: html, Last modified: March 15, 2025, 14:56:38 (UTC+05:30), Size: 3.1 KB. Below the table, a confirmation step asks 'Delete objects?' with a text input field containing 'delete'. At the bottom right are 'Cancel' and 'Delete objects' buttons.

The screenshot shows the 'Objects' page in the AWS S3 console for the 'kmittankbund' bucket. There are two objects listed: 'Background (1).png' (Type: png, Last modified: March 15, 2025, 14:43:09 (UTC+05:30), Size: 1.0 MB, Storage class: Standard) and 'error.html' (Type: html, Last modified: March 15, 2025, 14:54:40 (UTC+05:30), Size: 10.0 B, Storage class: Standard). The page includes tabs for Objects, Metadata, Properties, Permissions, Metrics, Management, and Access Points. At the top, there are buttons for Actions (with options like Copy S3 URI, Copy URL, Download, Open, Delete, Create folder, and Upload), and a 'Show versions' link. The bottom of the page includes standard AWS footer links: CloudShell, Feedback, © 2025, Amazon Web Services, Inc. or its affiliates., Privacy, Terms, and Cookie preferences.

S3 Versioning, CRR, Static Web Hosting

A screenshot of the AWS S3 console. The URL in the address bar is 'us-east-1.console.aws.amazon.com/s3/bucket/kmittankbund/empty?region=us-east-1&bucketType=general'. The page title is 'Empty bucket - S3 bucket kmittankbund'. The navigation path is 'Amazon S3 > Buckets > kmittankbund > Empty bucket'.

Empty bucket Info

⚠ • 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](#)

ⓘ If your bucket contains a large number of objects, creating a lifecycle rule to delete all objects in the bucket might be a more efficient way of emptying your bucket. [Go to lifecycle rule configuration](#)

Permanently delete all objects in bucket "kmittankbund"?

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

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

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

S3 Versioning, CRR, Static Web Hosting

The screenshot shows the 'Delete bucket' confirmation step in the AWS S3 console. The URL is us-east-1.console.aws.amazon.com/s3/bucket/kmittankbund/delete?region=us-east-1&bucketType=general. The page displays a warning box with bullet points about the不可逆性 of deleting buckets. Below it, a text input field contains 'kmittankbund'. At the bottom right are 'Cancel' and 'Delete bucket' buttons.

The screenshot shows the main Amazon S3 landing page. The URL is us-east-1.console.aws.amazon.com/s3/get-started?region=us-east-1&bucketType=general. A green success message at the top states 'Successfully deleted bucket "kmittankbund"'. The page features sections for 'Amazon S3' (with a 'Store and retrieve any amount of data from anywhere' callout), 'Create a bucket' (with a 'Create bucket' button), 'Pricing' (with a note about no minimum fees), and 'How it works' (with a video player showing an 'Introduction to Amazon S3' video). Navigation links at the bottom include CloudShell, Feedback, Privacy, Terms, and Cookie preferences.

S3 Versioning, CRR, Static Web Hosting

The screenshot shows the AWS S3 'Create bucket' interface across three main sections: General configuration, Object ownership, and Block public access settings.

General configuration: Set the AWS Region to 'US East (N. Virginia) us-east-1'. The 'Bucket type' is set to 'General purpose', which is described as recommended for most use cases. A bucket name 'kmittankbund' is entered. There is also a 'Copy settings from existing bucket - optional' section with a 'Choose bucket' button.

Object Ownership: The 'ACLs disabled (recommended)' option is selected, indicating that all objects in the bucket are owned by the account owner. A note suggests disabling ACLs unless specific access control is required. Under 'Object Ownership', the 'Bucket owner preferred' option is selected, stating that new objects will have the bucket-owner-full-control canned ACL if not specified.

Block Public Access settings for this bucket: The 'Block all public access' setting is turned on, which applies to all four settings below. It prevents public access to buckets and objects granted through new access control lists (ACLS). A note states that this setting doesn't change existing permissions.

S3 Versioning, CRR, Static Web Hosting

The screenshot shows the 'Create S3 bucket' page in the AWS console. Under the 'Block Public Access Settings for this bucket' section, there are four checkboxes: 'Block all public access', 'Block public access to buckets and objects granted through new access control lists (ACLs)', 'Block public access to buckets and objects granted through any access control lists (ACLs)', and 'Block public access to buckets and objects granted through new public bucket or access point policies'. The first checkbox is checked. A note below says: 'Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.' A warning box states: '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.' A checkbox labeled 'I acknowledge that the current settings might result in this bucket and the objects within becoming public.' is checked.

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

The screenshot shows the 'Create S3 bucket' page. Under the 'Default encryption' section, it says: 'Server-side encryption is automatically applied to new objects stored in this bucket.' It includes an 'Encryption type' dropdown with three options: 'Server-side encryption with Amazon S3 managed keys (SSE-S3)' (selected), 'Server-side encryption with AWS Key Management Service keys (SSE-KMS)', and 'Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)'. A note says: '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

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

[Cancel](#) [Create bucket](#)

S3 Versioning, CRR, Static Web Hosting

The screenshot shows the AWS S3 console interface. A green success message at the top left states: "Successfully created bucket 'kmittankbund'. To upload files and folders, or to configure additional bucket settings, choose View details." Below this, an "Account snapshot" box indicates "updated every 24 hours" and "Storage lens provides visibility into storage usage and activity trends. Metrics don't include directory buckets". The main area displays "General purpose buckets" (1) and "Directory buckets". A table lists the single bucket "kmittankbund" with its name, region (US East (N. Virginia)), and ARN. On the right, a sidebar lists AWS regions with their corresponding endpoint names. A modal window for the bucket "kmittankbund" shows its creation date as March 15, 2025, 15:06:07 (UTC+05:30).

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

▶ Account snapshot - updated every 24 hours All AWS Regions

Storage lens provides visibility into storage usage and activity trends. Metrics don't include directory buckets.

[General purpose buckets](#) [Directory buckets](#)

General purpose buckets (1) [Info](#) All AWS Regions

Buckets are containers for data stored in S3.

Name	AWS Region
kmittankbund	US East (N. Virginia) us-east-1

There are 15 Regions that are not enabled.

[Manage Regions](#) [Manage Local Zones](#)

View Storage Lens dashboard

ARN Empty Delete Create bucket

Creation date March 15, 2025, 15:06:07 (UTC+05:30)

Region Endpoint

United States N. Virginia us-east-1

Ohio us-east-2

N. California us-west-1

Oregon us-west-2

Asia Pacific Mumbai ap-south-1

Osaka ap-northeast-3

Seoul ap-northeast-2

Singapore ap-southeast-1

Sydney ap-southeast-2

Tokyo ap-northeast-1

Canada Central ca-central-1

Europe Frankfurt eu-central-1

Ireland eu-west-1

London eu-west-2

Paris eu-west-3

Stockholm eu-north-1

South America São Paulo sa-east-1

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

The screenshot shows the AWS S3 console interface for the US West (Oregon) region. It displays the same "General purpose buckets" list with one item: "kmittankbund" from the US East (N. Virginia) region. The sidebar on the left includes sections for "Amazon S3", "General purpose buckets" (with links to "Directory buckets", "Table buckets", etc.), "Storage Lens" (with "Dashboards", "Storage Lens groups", and "AWS Organizations settings"), and "AWS Marketplace for S3". The bottom of the page includes standard AWS footer links: CloudShell, Feedback, Privacy, Terms, and Cookie preferences.

https://us-west-2.console.aws.amazon.com/s3/buckets?region=us-west-2&bucketType=general

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

▶ Account snapshot - updated every 24 hours All AWS Regions

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 (1) [Info](#) All AWS Regions

Buckets are containers for data stored in S3.

Name	AWS Region	IAM Access Analyzer	Creation date
kmittankbund	US East (N. Virginia) us-east-1	View analyzer for us-east-1	March 15, 2025, 15:06:07 (UTC+05:30)

Copy ARN Empty Delete Create bucket

Creation date March 15, 2025, 15:06:07 (UTC+05:30)

Region Endpoint

United States (Oregon) us-west-2

CloudShell Feedback

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

S3 Versioning, CRR, Static Web Hosting

The screenshot shows the AWS S3 'Create bucket' wizard. The first step, 'Bucket type', is selected. It offers two options: 'General purpose' (selected) and 'Directory'. The 'General purpose' option is described as recommended for most use cases. The second step, 'Object Ownership', is shown below, with 'Bucket owner enforced' selected. The third step, 'Block Public Access settings for this bucket', is also visible.

Bucket type

General purpose
Recommended for most use cases and access patterns. General purpose buckets are the original S3 bucket type. They allow a mix of storage classes that redundantly store objects across multiple Availability Zones.

Directory
Recommended for low-latency use cases. These buckets use only the S3 Express One Zone storage class, which provides faster processing of data within a single Availability Zone.

Bucket name **Info**
kmittankbund1

Bucket names must be 3 to 63 characters and unique within the global namespace. Bucket names must also begin and end with a letter or number. Valid characters are a-z, 0-9, periods (.), and hyphens (-). [Learn More](#)

Copy settings from existing bucket - optional
Only the bucket settings in the following configuration are copied.
[Choose bucket](#)

Format: s3://bucket/prefix

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

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

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

Object Ownership
Bucket owner enforced

Block Public Access settings for this bucket
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](#)

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.

⚠️ We recommend disabling ACLs, unless you need to control access for each object individually or to have the object writer own the data they upload. Using a bucket policy instead of ACLs to share data with users outside of your account simplifies permissions management and auditing.

Object Ownership

Bucket owner preferred
If new objects written to this bucket specify the bucket-owner-full-control canned ACL, they are owned by the bucket owner. Otherwise, they are owned by the object writer.

Object writer
The object writer remains the object owner.

ⓘ If you want to enforce object ownership for new objects only, your bucket policy must specify that the bucket-owner-full-control canned ACL is required for object uploads. [Learn more](#)

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 **existing** access control lists (ACLs)

© 2025, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

S3 Versioning, CRR, Static Web Hosting

The screenshot shows the 'Block Public Access settings for this bucket' section. It includes a note about turning off block all public access and a checkbox for acknowledging the consequences.

Block Public Access settings for this bucket

Bucket 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 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.

The screenshot shows the 'Bucket Versioning' section. It includes a note about recovering from unintended user actions and application failures, and a checkbox for acknowledging the consequences.

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](#)

Disable

Enable

The screenshot shows the 'Default encryption' section. It includes a note about server-side encryption being automatically applied to new objects, and a checkbox for acknowledging the consequences.

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

The screenshot shows the 'Advanced settings' section. It includes a note about uploading files and folders to the bucket, and a checkbox for acknowledging the consequences.

Advanced settings

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

Create bucket

S3 Versioning, CRR, Static Web Hosting

The screenshot shows the AWS S3 buckets page. A green success message at the top states: "Successfully created bucket 'kmittankbund1'. To upload files and folders, or to configure additional bucket settings, choose View details." Below this, an account snapshot is displayed, updated every 24 hours. A link to the Storage Lens dashboard is available. The navigation bar shows "Amazon S3 > Buckets". The main table lists two general purpose buckets: "kmittankbund" and "kmittankbund1". The "Create bucket" button is visible on the right.

The screenshot shows the AWS S3 Management tab for the "kmittankbund" bucket. The left sidebar includes links for General purpose buckets, Storage Lens, and AWS Marketplace. The main content area is titled "Lifecycle configuration" and "Lifecycle rules". It states there are no lifecycle rules for this bucket and provides a "Create lifecycle rule" button. Below this is the "Replication rules (0)" section, which also includes a "Create replication rule" button. The navigation bar shows "Amazon S3 > Buckets > kmittankbund".

S3 Versioning, CRR, Static Web Hosting

The screenshot shows the 'Create replication rule' configuration page in the AWS Management Console. The URL in the browser is us-east-1.console.aws.amazon.com/s3/management/kmittankbund/replication/create?region=us-east-1&bucketType=general. The page is titled 'Create replication rule' with an 'Info' link.

Replication rule configuration

Replication rule name: Enter rule ID

Status: Choose whether the rule will be enabled or disabled when created.
Enabled (radio button selected)
Disabled

Priority: The priority value resolves conflicts that occur when an object is eligible for replication under multiple rules to the same destination. The rule is added to the configuration at the highest priority and the priority can be changed on the replication rules table.
0

Source bucket:

Source bucket name: kmittankbund

Source Region: US East (N. Virginia) us-east-1

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

CloudShell Feedback

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

S3 Versioning, CRR, Static Web Hosting

The screenshot shows the 'Create replication rule' configuration page for an S3 bucket named 'kmittankbund'. The 'Destination' section is active, showing options to choose a bucket in the same account ('Choose a bucket in this account') or another account ('Specify a bucket in another account'). A 'Bucket name' field contains 'kmittankbund1', and a 'Destination Region' dropdown is set to 'US West (Oregon) us-west-2'. The 'IAM role' section shows 'Choose from existing IAM roles' selected, with a dropdown menu containing 'LabRole'. The 'Encryption' section has a checkbox for 'Replicate objects encrypted with AWS Key Management Service (AWS KMS)', which is unchecked. The 'Destination storage class' section notes that Amazon S3 offers various storage classes and includes a checkbox for 'Change the storage class for the replicated objects', which is also unchecked. The 'Additional replication options' section contains a checkbox for 'Replication Time Control (RTC)', which is unchecked.

Destination

Destination
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). You can also specify a different bucket for each rule in the configuration. [Learn more](#) or see [Amazon S3 pricing](#)

Choose a bucket in this account
 Specify a bucket in another account

Bucket name
Choose the bucket that will receive replicated objects.
kmittankbund1 [Browse S3](#)

Destination Region
US West (Oregon) us-west-2

IAM role

Permission to access the specified resources

Create new role
 Choose from existing IAM roles
 Enter IAM role ARN

IAM role
Choose IAM role [View](#)

Encryption
Server-side encryption protects data at rest.

Replicate objects encrypted with AWS Key Management Service (AWS KMS)
Replicate SSE-KMS and DSSE-KMS encrypted objects.

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

Change the storage class for the replicated objects

Additional replication options

Replication Time Control (RTC)
Replication Time Control replicates 99.99% of new objects within 15 minutes and includes replication metrics. Additional fees will apply. [Learn more](#)

S3 Versioning, CRR, Static Web Hosting

The screenshot displays two main sections of the AWS S3 console:

Replication rules (1)

Replication configuration successfully updated
If changes to the configuration aren't displayed, choose the refresh button. Changes apply only to new objects. To replicate existing objects with this configuration, choose [Create replication job](#).

Replication configuration settings

Configuration settings affect all replication rules in the bucket.

Source bucket	IAM role
kmittankbund	LabRole

Source Region
US East (N. Virginia) us-east-1

Actions View details Edit rule Delete Create replication rule

Replication rules (1)

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](#)

Replication rule name	Status	Destination bucket	Destination Region	Priority	Scope	Storage class	Replica owner	Replication Time Control	KMS-encrypted objects (SSE-KMS or DSSE-KMS)	Replica modification sync

Upload

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, 7.1 MB)

All files and folders in this table will be uploaded.

Name	Type	Size
Background.png	image/png	7.1 MB

Destination

Destination
<s3://kmittankbund>

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

Permissions
Grant public access and access to other AWS accounts.

Access control list (ACL)
Grant basic read/write permissions to other AWS accounts. [Learn more](#)

S3 Versioning, CRR, Static Web Hosting

The screenshot shows the 'Access control list (ACL)' section of the S3 bucket properties. It includes a note from AWS recommending S3 bucket policies or IAM policies for access control. The 'Grant public-read access' option is selected, allowing anyone in the world to access the objects. A warning message states that granting public-read access is not recommended because anyone in the world will be able to access the specified objects. A checkbox for accepting the risk is checked.

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

kmittankbund [Info](#)

[Objects](#) [Metadata](#) [Properties](#) [Permissions](#) [Metrics](#) [Management](#) [Access Points](#)

Objects (1)

Name	Type	Last modified	Size	Storage class
Background (1).png	png	March 15, 2025, 15:23:15 (UTC+05:30)	1.0 MB	Standard

S3 Versioning, CRR, Static Web Hosting

The screenshot shows the AWS S3 console interface. At the top, there are several tabs and links: 'CC-3-2-CS-3C-2024_25: CC-3-2-CS...', 'CC-3-2-CS-3C-2024_25: CC-3-2-CS...', 'Launch AWS Academy Learner Lab', 'kmittankbund1 - S3 bucket | S3', 'S3 buckets | S3 | us-east-1', and 'voclabs/user3879096=reddyprasad.kmit@gmail.com @ 8269-1826-5081'. Below this is a search bar with '[Alt+S]' and a navigation bar with 'Amazon S3 > Buckets > kmittankbund1'.

The main area is titled 'kmittankbund1 Info' and shows the 'Objects' tab selected. It displays one object: 'Background (1).png'. The object details are as follows:

Name	Type	Last modified	Size	Storage class
Background (1).png	png	March 15, 2025, 15:23:15 (UTC+05:30)	1.0 MB	Standard

Below the table are buttons for 'Actions' (Copy S3 URI, Copy URL, Download, Open, Delete, Create folder, Upload), a search bar ('Find objects by prefix'), and a 'Show versions' link. At the bottom of the page, there are links for 'CloudShell', 'Feedback', and copyright information: '© 2025, Amazon Web Services, Inc. or its affiliates.' followed by 'Privacy', 'Terms', and 'Cookie preferences'.