

Lab24

S3 Restriction for Specific Bucket

Click "S3" service

The screenshot shows the AWS Management Console homepage. The URL is https://console.aws.amazon.com/console/home?region=us-east-1. The top navigation bar includes 'Services' (dropdown), 'Resource Groups' (dropdown), and user information (siva1n82, N. Virginia, Support). The main content area is titled 'AWS services' with a search bar. It lists 'Recently visited services' (Billing, EC2, CloudFormation, IAM) and 'All services' categorized by type: Compute, Storage, Database, Migration, Services (Management Tools, Mobile Services, AR & VR, Application Integration, Media Services, Customer Engagement, Machine Learning, Business Productivity), and Tools (CloudWatch, AWS Auto Scaling, CloudFormation, CloudTrail, Config, OpsWorks, Service Catalog, Systems Manager, Trusted Advisor, Managed Services). The 'Storage' category is expanded, showing S3, EFS, Glacier, and Storage Gateway. The 'S3' icon is highlighted with a yellow box. On the right side, there are 'Helpful tips' (Manage your costs, Create an organization) and 'Explore AWS' sections (Amazon RDS, Amazon Kinesis, Amazon ECS, AWS Marketplace).

Click “Create bucket” with unique name.

The screenshot shows the AWS S3 Management Console interface. At the top, there's a navigation bar with links for Services, Resource Groups, and a search bar. Below the navigation bar, a banner reads "Identify optimal storage classes with S3 Analytics - Storage Class Analysis. Learn More »". On the left, there's a sidebar titled "Amazon S3" with a "Search for buckets" input field and buttons for "+ Create bucket", "Delete bucket", and "Empty bucket". The main area displays a table of buckets. The table has columns for Bucket name, Access, Region, and Date created. There are 5 Buckets listed, all of which are "Not public". The buckets are:

Bucket name	Access	Region	Date created
elasticbeanstalk-ap-south-1-297111308396	Not public *	Asia Pacific (Mumbai)	Dec 20, 2017 5:48:27 PM GMT+0530
elasticbeanstalk-us-east-1-297111308396	Not public *	US East (N. Virginia)	Jan 23, 2018 10:42:40 AM GMT+0530
elasticbeanstalk-us-east-2-297111308396	Not public *	US East (Ohio)	Dec 15, 2017 10:52:13 AM GMT+0530
elasticbeanstalk-us-west-1-297111308396	Not public *	US West (N. California)	Jan 25, 2018 7:04:06 AM GMT+0530
elasticbeanstalk-us-west-2-297111308396	Not public *	US West (Oregon)	Jan 27, 2018 6:23:50 PM GMT+0530

* Objects might still be publicly accessible due to object ACLs. [Learn more](#)

At the bottom of the screen, there's a taskbar showing various application icons and system status indicators like battery level and network connection.

Type aws.sansbound.com

The screenshot shows the 'Create bucket' wizard on the 'Name and region' step. The title 'Create bucket' is at the top right, with a close button 'X'. Below it are four tabs: 1) Name and region (selected), 2) Set properties, 3) Set permissions, and 4) Review. The main area is titled 'Name and region'. It has a 'Bucket name' field containing 'aws.sansbound' with an info icon. A 'Region' dropdown menu is set to 'US East (N. Virginia)'. Below this is a section for 'Copy settings from an existing bucket' with a 'Select bucket (optional)' dropdown showing '5 Buckets'. At the bottom are 'Create', 'Cancel', and 'Next' buttons.

Create bucket

1 Name and region 2 Set properties 3 Set permissions 4 Review

Name and region

Bucket name ⓘ

aws.sansbound

Region

US East (N. Virginia)

Copy settings from an existing bucket

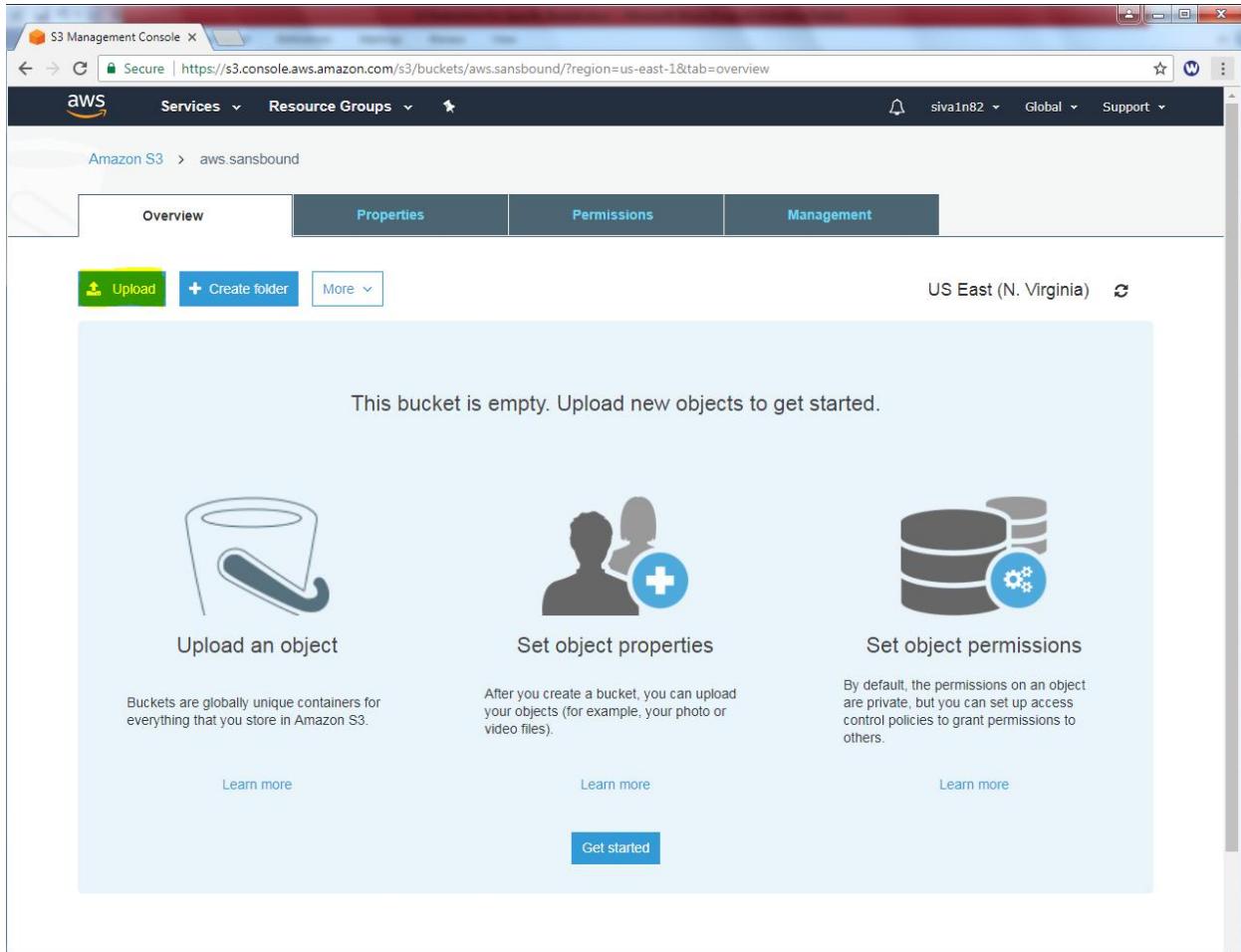
Select bucket (optional)

5 Buckets

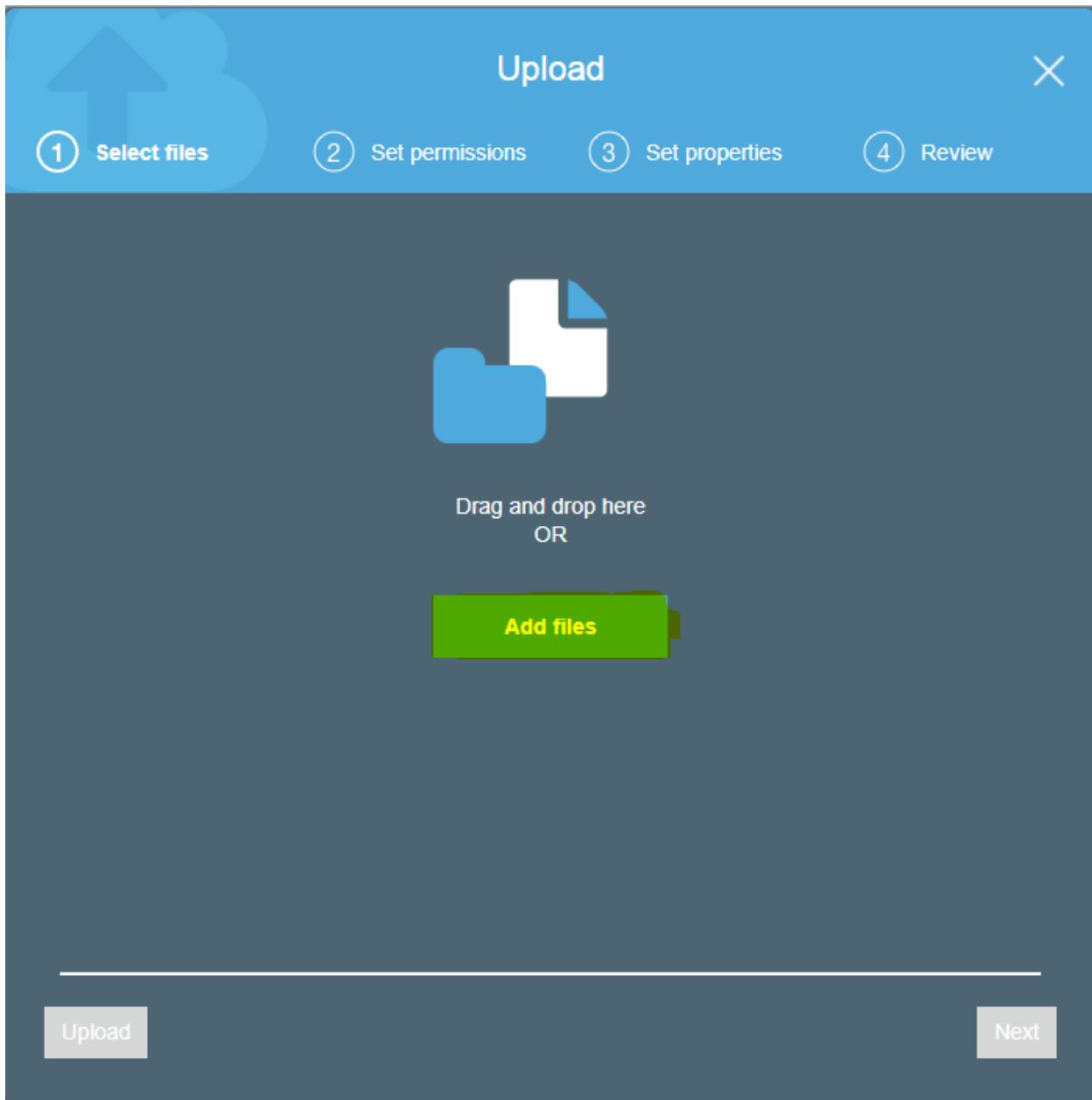
Create Cancel Next

Click "Create".

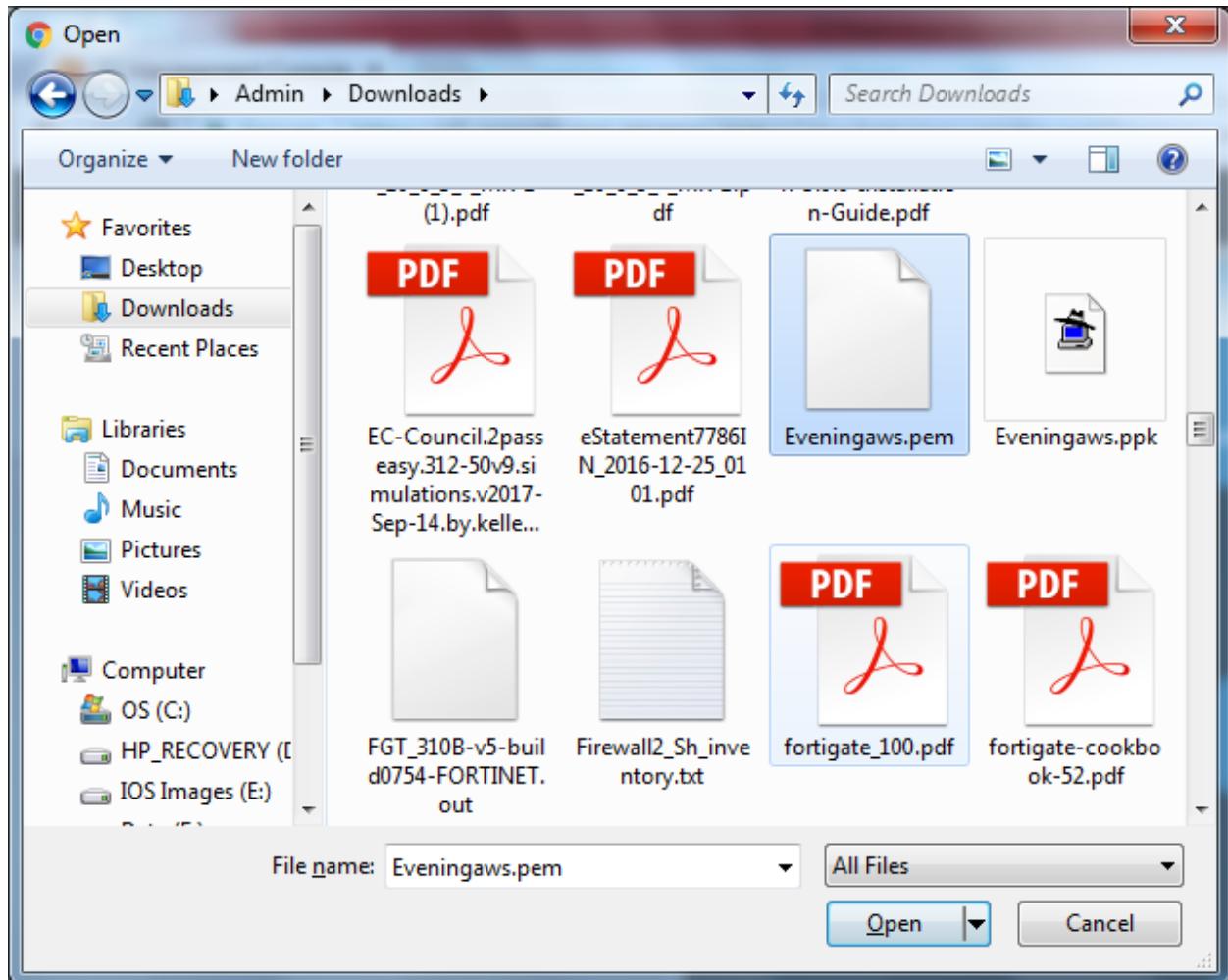
Click “Upload”.



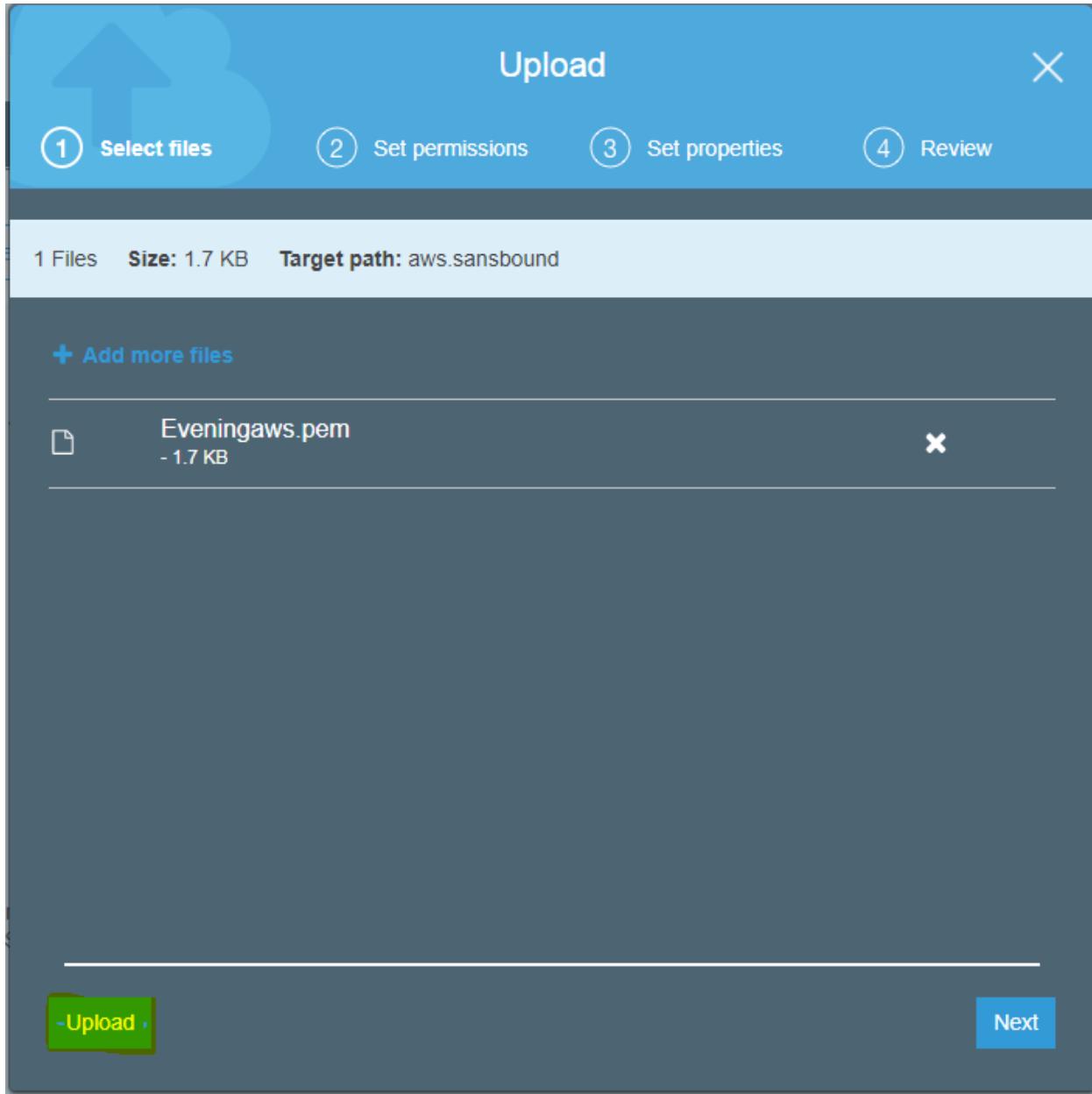
Click “Add files”.



Locate the file and click open.



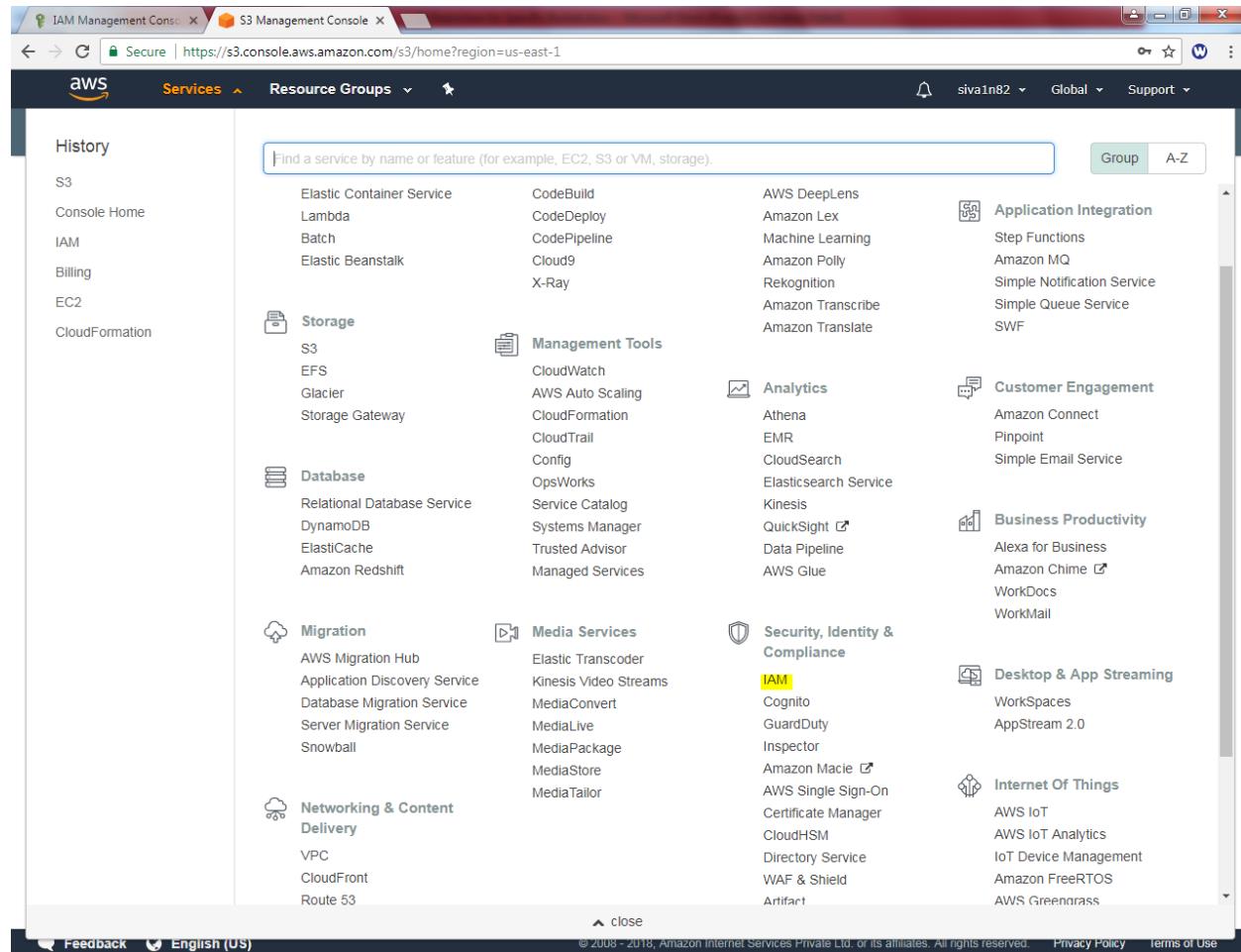
Click “Upload” to upload the file.



We can able view the file.

The screenshot shows the AWS S3 Management Console interface. At the top, there's a navigation bar with links for 'Services', 'Resource Groups', and user information ('siva1n82', 'Global', 'Support'). Below the navigation bar, the URL is https://s3.console.aws.amazon.com/s3/buckets/aws.sansbound/?region=us-east-1&tab=overview. The main area displays the contents of the 'aws.sansbound' bucket. A search bar at the top says 'Type a prefix and press Enter to search. Press ESC to clear.' Below it, there are buttons for 'Upload', '+ Create folder', and 'More'. On the right, it shows the region as 'US East (N. Virginia)' with a refresh icon. The table lists one file: 'Eveningaws.pem'. The file details are: Name: Eveningaws.pem, Last modified: Feb 6, 2018 7:24:07 AM GMT+0530, Size: 1.7 KB, Storage class: Standard. The table has columns for Name, Last modified, Size, and Storage class. At the bottom of the list, it says 'Viewing 1 to 1'.

Click "IAM" Role.

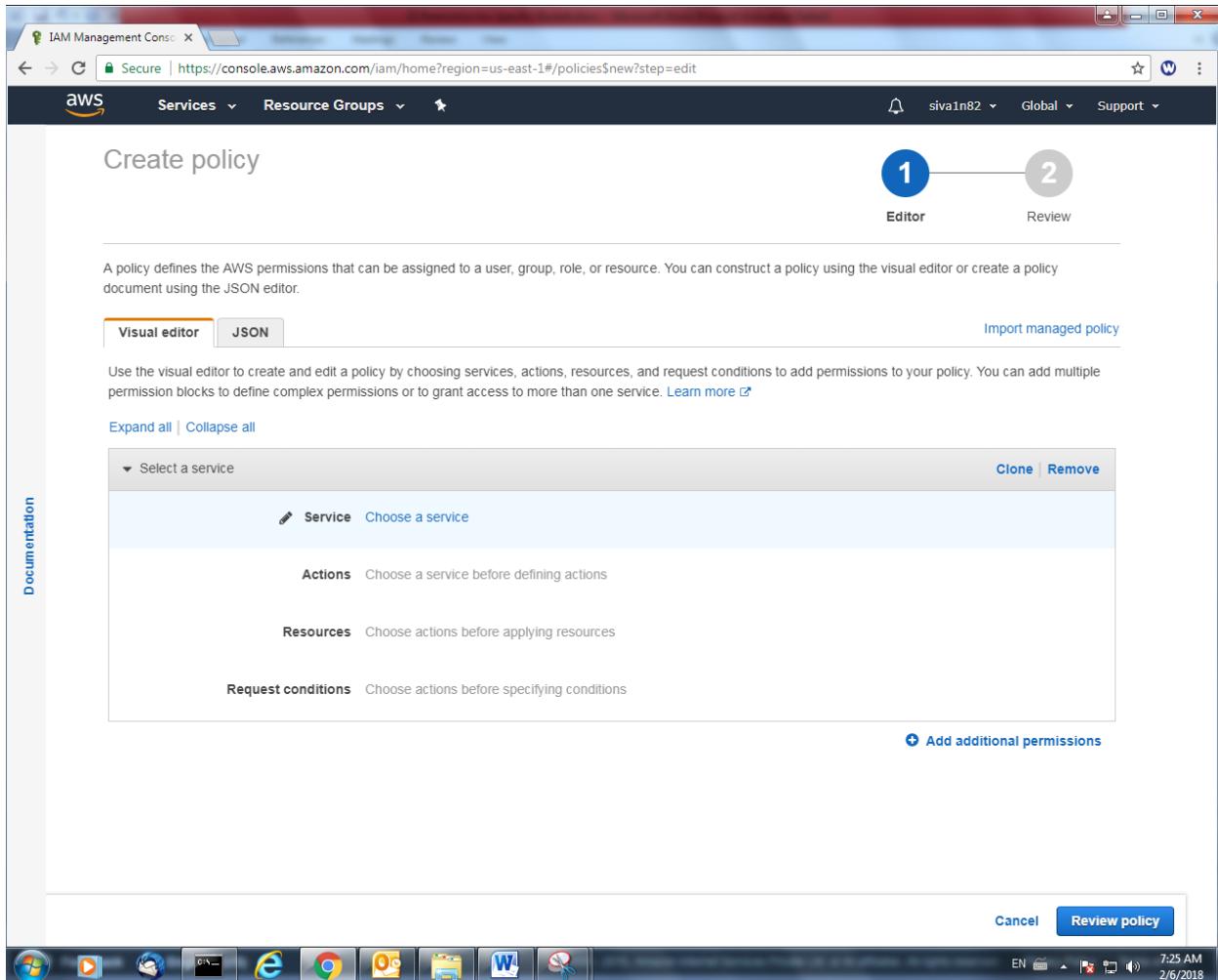


Click “Create Policy”.

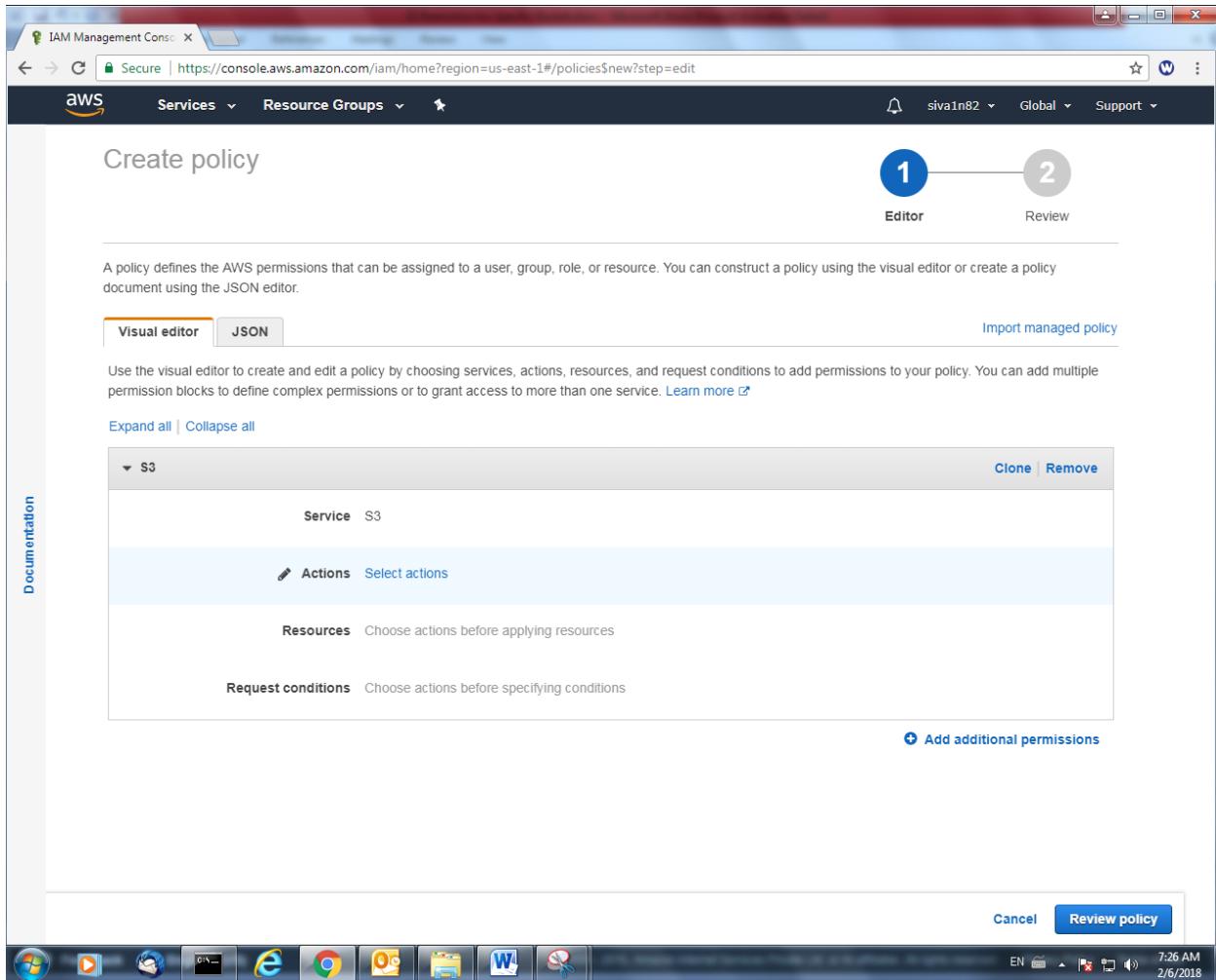
The screenshot shows the AWS IAM Management Console interface. The left sidebar has a 'Policies' section selected, which is highlighted with an orange border. The main content area displays a table of managed policies. The columns in the table are 'Policy name', 'Type', 'Attachments', and 'Description'. The table lists numerous AWS-managed policies, each with a small icon and a brief description of its access scope.

Policy name	Type	Attachments	Description
AdministratorAccess	Job function	0	Provides full access to AWS services and resources.
AlexaForBusinessDeviceSetup	AWS managed	0	Provide device setup access to AlexaForBusiness services
AlexaForBusinessFullAccess	AWS managed	0	Grants full access to AlexaForBusiness resources and access to related services
AlexaForBusinessGatewayExecution	AWS managed	0	Provide gateway execution access to AlexaForBusiness services
AlexaForBusinessReadOnlyAccess	AWS managed	0	Provide read only access to AlexaForBusiness services
AmazonAPIGatewayAdministrator	AWS managed	0	Provides full access to create/edit/delete APIs in Amazon API Gateway
AmazonAPIGatewayInvokeFullAccess	AWS managed	0	Provides full access to invoke APIs in Amazon API Gateway
AmazonAPIGatewayPushToCloudWatchLogs	AWS managed	0	Allows API Gateway to push logs to user's account
AmazonAppStreamFullAccess	AWS managed	0	Provides full access to Amazon AppStream via the AWS Management Console
AmazonAppStreamReadOnlyAccess	AWS managed	0	Provides read only access to Amazon AppStream via the AWS Management Console
AmazonAppStreamServiceAccess	AWS managed	0	Default policy for Amazon AppStream service role
AmazonAthenaFullAccess	AWS managed	0	Provide full access to Amazon Athena and scoped access to the developer's account
AmazonChimeFullAccess	AWS managed	0	Provides full access to Amazon Chime Admin Console via the AWS Management Console
AmazonChimeReadOnly	AWS managed	0	Provides read only access to Amazon Chime Admin Console via the AWS Management Console
AmazonChimeUserManagement	AWS managed	0	Provides user management access to Amazon Chime Admin Console via the AWS Management Console
AmazonCloudDirectoryFullAccess	AWS managed	0	Provides full access to Amazon Cloud Directory Service
AmazonCloudDirectoryReadOnlyAccess	AWS managed	0	Provides read only access to Amazon Cloud Directory Service
AmazonCognitoDeveloperAuthentication	AWS managed	0	Provides access to Amazon Cognito APIs to support developer authentication
AmazonCognitoPowerUser	AWS managed	0	Provides administrative access to existing Amazon Cognito resources
AmazonCognitoReadOnly	AWS managed	0	Provides read only access to Amazon Cognito resources

Click "Choose a service" and



choose the S3 service and click Select actions.



Access level groups, check “List” and click “There are action in your policy that support the bucket resource type.”

A policy defines the AWS permissions that can be assigned to a user, group, role, or resource. You can construct a policy using the visual editor or create a policy document using the JSON editor.

Use the visual editor to create and edit a policy by choosing services, actions, resources, and request conditions to add permissions to your policy. You can add multiple permission blocks to define complex permissions or to grant access to more than one service. [Learn more](#)

Expand all | Collapse all

S3 (4 actions) ⚠ 1 warning

Service S3

Actions Specify the actions allowed in S3 [?](#) [Close](#) [Filter actions](#)

[Switch to deny permissions](#)

Manual actions (add actions)

All S3 actions (s3:*)

Access level groups

▶ List (4 selected)

▶ Read

▶ Write

▶ Permissions management

Resources There are actions in your policy that support the **bucket** resource type.

Request conditions Specify request conditions (optional)

[Add additional permissions](#)

[Clone](#) | [Remove](#)

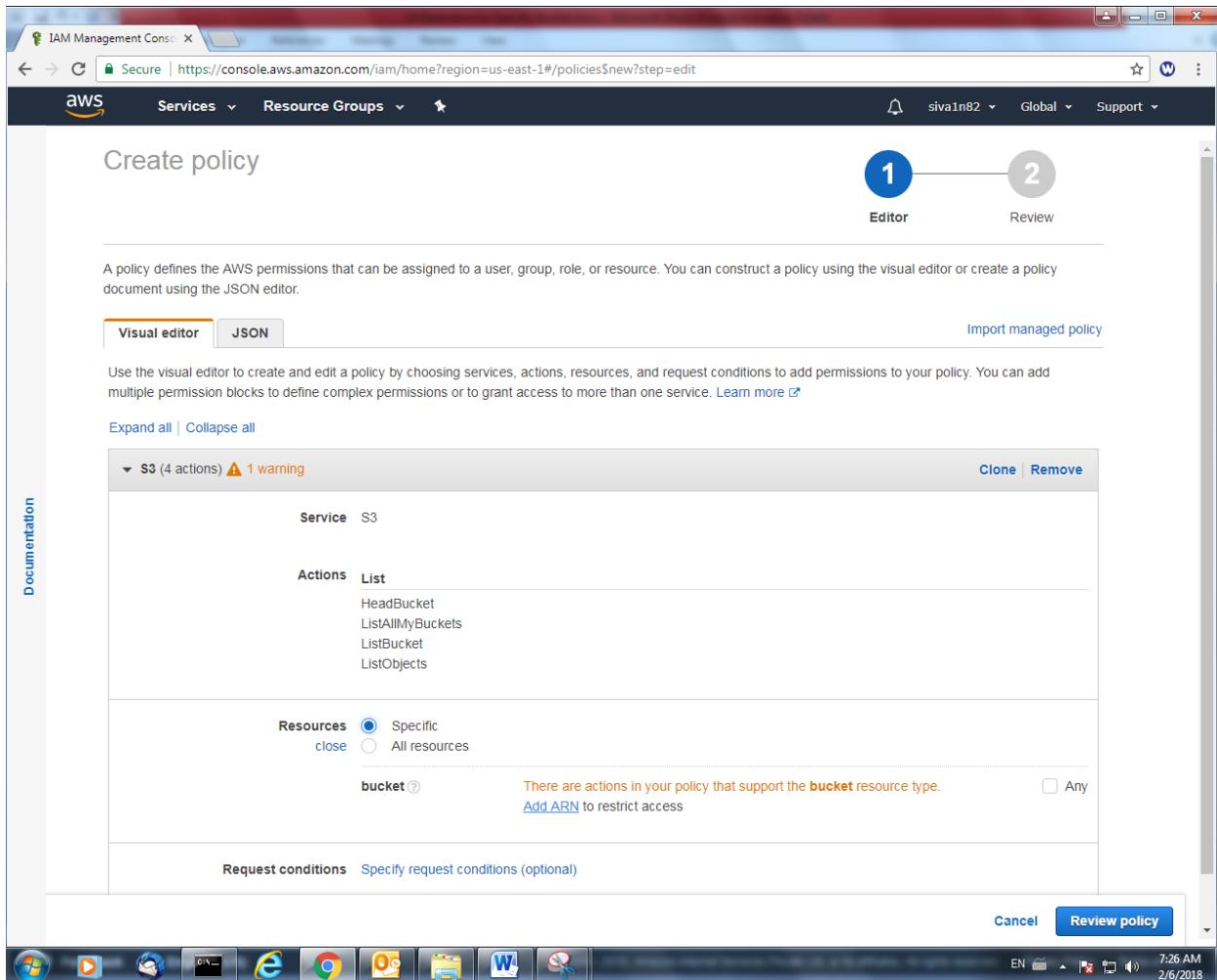
[Expand all](#) | [Collapse all](#)

[Cancel](#) | [Review policy](#)

Documentation

EN 7:26 AM 2/6/2018

Click specific option and click “Add ARN” to add the bucket name.



Type the bucket name and click “Add”.

Add ARN(s) ×

Amazon Resource Names (ARNs) uniquely identify AWS resources. Resources are unique to each service. [Learn more ↗](#)

Specify ARN for bucket [List ARNs manually](#)

Bucket name Any

[Cancel](#) Add

Click “Review Policy”.

The screenshot shows the AWS IAM Management Console with the URL [https://console.aws.amazon.com/iam/home?region=us-east-1#/policies\\$new?step=edit](https://console.aws.amazon.com/iam/home?region=us-east-1#/policies$new?step=edit). The page title is "Policy Editor". The top navigation bar includes "Services", "Resource Groups", "Editor", "Review", and user information "siva1n82". A sidebar on the left is titled "Documentation". The main content area is titled "A policy defines the AWS permissions that can be assigned to a user, group, role, or resource. You can construct a policy using the visual editor or create a policy document using the JSON editor." It features tabs for "Visual editor" (selected) and "JSON". Below this, a note says: "Use the visual editor to create and edit a policy by choosing services, actions, and resources, and request conditions to add permissions to your policy. You can add multiple permission blocks to define complex permissions or to grant access to more than one service." A link "Learn more" is provided. Buttons "Import managed policy", "Clone", and "Remove" are at the top right of the policy editor panel. The policy editor itself shows an "S3 (4 actions)" block. Under "Service" is "S3". Under "Actions" is "List" with items: HeadBucket, ListAllMyBuckets, ListBucket, ListObjects. Under "Resources" is "Specific" selected. A "bucket" field contains "arn:aws:s3:::aws.sansbound" with an "EDIT" button and a "close" link. An "Add ARN to restrict access" link is below. At the bottom of the editor is a "Request conditions" section with "Specify request conditions (optional)". A "Add additional permissions" button is at the bottom right. At the very bottom of the window are standard Windows taskbar icons and system status indicators.

Type Name of Policy and Description.

Create policy

1 Editor 2 Review

Review policy

Before you create this policy, provide the required information and review this policy.

Name* S3ListAccess

Maximum 128 characters. Use alphanumeric and '+=_@-' characters.

Description S3ListAccess

Maximum 1000 characters. Use alphanumeric and '+=_@-' characters.

Summary

Service	Access level	Resource	Request condition
S3	Full: List	Multiple	None

Allow (1 of 129 services) Show remaining 128

* Required Cancel Previous Create policy EN 7:30 AM 2/6/2018

Click “Create Policy”.

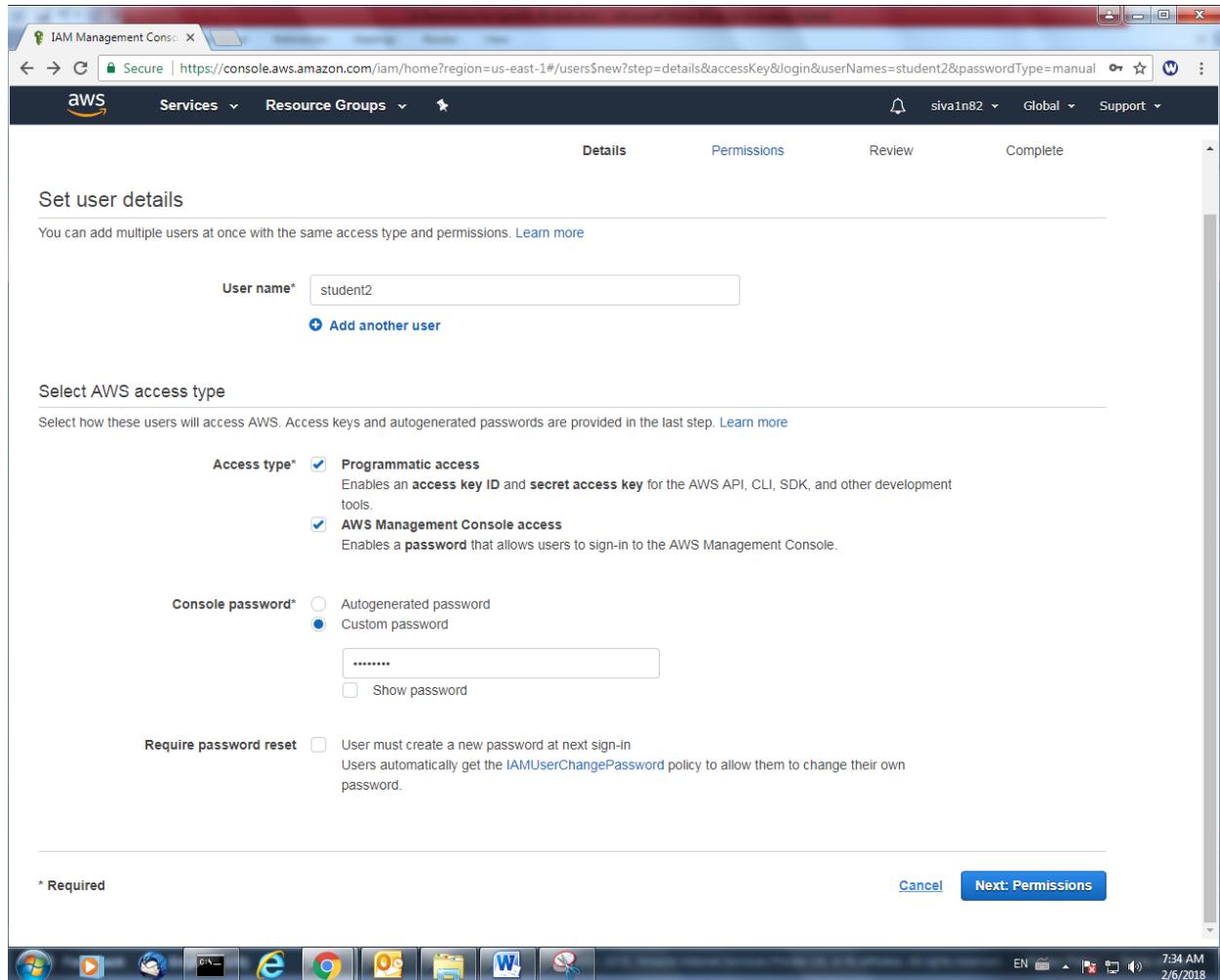
We need to create a user to assign the policy.

Click “Add user”.

The screenshot shows the AWS IAM Management Console interface. The left sidebar has a navigation menu with options like Dashboard, Groups, Users (which is selected), Roles, Policies, Identity providers, Account settings, Credential report, and Encryption keys. The main content area displays a table titled "Find users by username or access key". The table has columns: User name, Groups, Access key age, Password age, Last activity, and MFA. One row is shown, representing a user named "student1" who is part of the "S3ReadOnlyAccess" group, with access keys created today, no password age, no last activity, and no MFA enabled. There are "Add user" and "Delete user" buttons at the top of the table area.

Username: student2

Access type : Programmatic access and AWS management console access.



Click "Next".

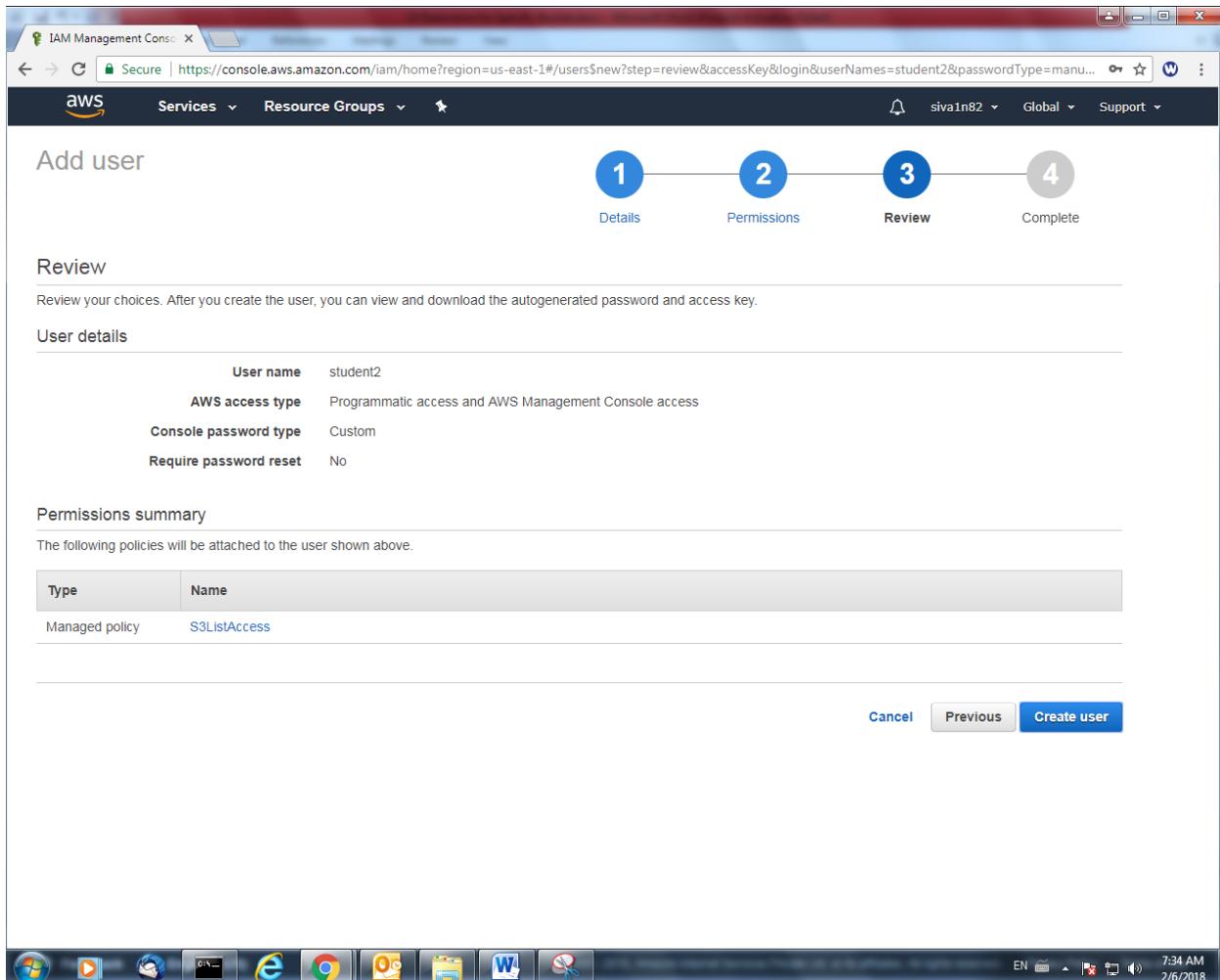
In Policy type, type “s3” to filter the s3 policies. Select the policy which we created.

The screenshot shows the AWS IAM Management Console with the URL [https://console.aws.amazon.com/iam/home?region=us-east-1#/users\\$new?step=permissions&accessKey&login&userNames=student2&passwordType=...](https://console.aws.amazon.com/iam/home?region=us-east-1#/users$new?step=permissions&accessKey&login&userNames=student2&passwordType=...). The window title is "IAM Management Console". The top navigation bar includes "Services", "Resource Groups", and "Support". The main title is "Add user" and the sub-step is "Permissions". There are four numbered steps: 1 (Details), 2 (Permissions), 3 (Review), and 4 (Complete). Below the steps, it says "Set permissions for student2". Three options are shown: "Add user to group" (disabled), "Copy permissions from existing user" (disabled), and "Attach existing policies directly" (selected). A note below says "Attach one or more existing policies directly to the users or create a new policy. [Learn more](#)". A "Create policy" button and a "Refresh" button are available. A search bar at the top right is set to "Filter: Policy type" and contains "s3". The results table shows five policies:

	Policy name	Type	Attachments	Description
<input type="checkbox"/>	AmazonDMSRedshiftS3Role	AWS managed	0	Provides access to manage S3 settings for Redshift endpoints for DMS.
<input type="checkbox"/>	AmazonS3FullAccess	AWS managed	0	Provides full access to all buckets via the AWS Management Console.
<input type="checkbox"/>	AmazonS3ReadOnlyAccess	AWS managed	1	Provides read only access to all buckets via the AWS Management Con...
<input type="checkbox"/>	QuickSightAccessForS3Storag...	AWS managed	0	Policy used by QuickSight team to access customer data produced by S...
<input checked="" type="checkbox"/>	S3ListAccess	Customer managed	0	S3ListAccess

Click “Next”.

Click “Create user”.



User successfully created. Please note that URL as below in box.

The screenshot shows the AWS IAM Management Console interface. At the top, there's a navigation bar with links for Services, Resource Groups, and Support. Below the navigation bar, a progress bar indicates four steps: Details (step 1), Permissions (step 2), Review (step 3), and Complete (step 4). Step 4 is highlighted with a blue circle and labeled 'Complete'. A success message box is displayed, stating: 'Success: You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download. However, you can create new credentials at any time.' It also provides a sign-in URL: <https://297111308396.sigin.aws.amazon.com/console>. Below the message, there's a table with columns: User, Access key ID, Secret access key, and Email login instructions. One row is visible for the user 'student2', showing the Access key ID as 'AKIAIQLGWR4HLOEN4ECQ' and a 'Show' link for the Secret access key. There's also a 'Send email' link. At the bottom right of the message box is a 'Close' button. The taskbar at the bottom of the screen shows various application icons and the date/time: 7:34 AM, 2/6/2018.

Click Users, and select student2 user.

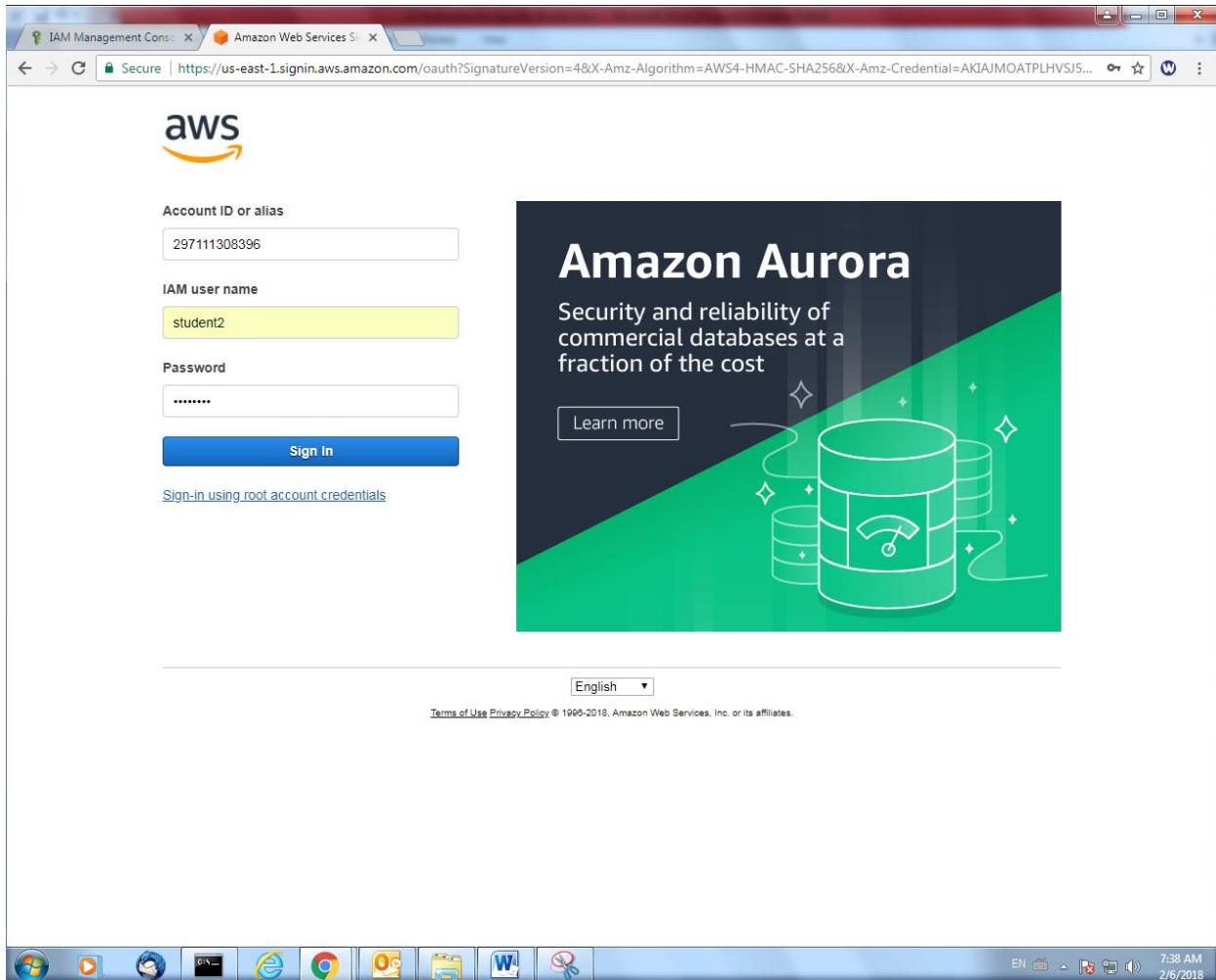
The screenshot shows the AWS IAM Management Console interface. The left sidebar has a 'Users' section selected, which is highlighted in orange. The main content area displays a table of users. The table has columns: User name, Groups, Access key age, Password age, Last activity, and MFA. There are two entries:

User name	Groups	Access key age	Password age	Last activity	MFA
student1	S3ReadonlyAccess	Today	Today	None	Not enabled
student2	None	Today	Today	Today	Not enabled

Click Security Credentials, copy the console login link and open that URL in new window.

The screenshot shows the AWS IAM Management Console interface. The left sidebar is titled 'Users' and lists various options: Dashboard, Groups, Users (selected), Roles, Policies, Identity providers, Account settings, Credential report, and Encryption keys. The main content area is titled 'Summary' for the user 'student2'. It displays the User ARN (arn:aws:iam::297111308396:user/student2), Path (/), and Creation time (2018-02-06 07:34 UTC+0530). Below this, there are tabs for 'Permissions', 'Groups (0)', 'Security credentials' (which is selected), and 'Access Advisor'. The 'Sign-in credentials' section shows that the console password is enabled, the console login link is https://297111308396.signin.aws.amazon.com/console, and the last login was on 2018-02-06 07:36 UTC+0530. It also indicates that no assigned MFA device or signing certificates are present. The 'Access keys' section includes a 'Create access key' button and a table showing one active access key: AKIAIQLGWR4HLOEN4ECQ, created on 2018-02-06 07:34 UTC+0530, last used N/A, and in Active status. The 'SSH keys for AWS CodeCommit' section includes an 'Upload SSH public key' button. The bottom of the screen shows the Windows taskbar with various icons and the system tray indicating the date and time (7:37 AM, 2/6/2018).

Type the login credentials of Student2.



Click "S3".

The screenshot shows the AWS Management Console homepage. At the top, there are two tabs: 'IAM Management Console' and 'AWS Management Console'. The URL in the address bar is <https://console.aws.amazon.com/console/home?region=us-east-1>. The top navigation bar includes 'Services', 'Resource Groups', a user dropdown for 'student2 @ 2971-1130-8396', a location dropdown for 'N. Virginia', and a 'Support' link.

The main content area is divided into several sections:

- AWS services**: A search bar with placeholder text 'Find a service by name or feature (for example, EC2, S3 or VM, storage)' and a 'Recently visited services' list. Items listed include IAM, S3, Billing, EC2, and CloudFormation. A 'All services' link is also present.
- Helpful tips**: Two cards:
 - Manage your costs**: Describes real-time billing alerts based on cost and usage budgets. Includes a 'Start now' button.
 - Create an organization**: Describes AWS Organizations for policy-based management of multiple AWS accounts. Includes a 'Start now' button.
- Build a solution**: A section for simple wizards and automated workflows. It includes six items:
 - Launch a virtual machine**: With EC2 or Lightsail, ~1-2 minutes.
 - Build a web app**: With Elastic Beanstalk, ~6 minutes.
 - Host a static website**: With S3, CloudFront, Route 53, ~5 minutes.
 - Connect an IoT device**: With AWS IoT, ~5 minutes.
 - Start a development project**: With CodeStar, ~5 minutes.
 - Register a domain**: With Route 53, ~3 minutes.A 'See more' link is located below these items.
- Explore AWS**: A section with links to other AWS services:
 - Amazon Relational Database Service (RDS)**: Describes RDS managing databases. Includes a 'Learn more' link.
 - Real-Time Analytics with Amazon Kinesis**: Describes stream analysis. Includes a 'Learn more' link.
 - Get Started with Containers on AWS**: Describes Amazon ECS for container management. Includes a 'Learn more' link.
 - AWS Marketplace**: Describes discovering, procuring, and deploying software products. Includes a 'Learn more' link.
- Learn to build**: A section for step-by-step guides, labs, and videos. It includes three categories:
 - Websites**: 3 videos, 3 tutorials, 3 labs.
 - DevOps**: 6 videos, 2 tutorials, 3 labs.
 - Backup and recovery**: 3 videos, 2 tutorials, 3 labs.A 'See all' link is located above the DevOps category.

At the bottom of the screen, the Windows taskbar is visible with icons for File Explorer, Task View, Start, Taskbar settings, Edge, Google Chrome, File Explorer, Word, and Snipping Tool. The system tray shows the date and time as '7:38 AM 2/6/2018'.

Click "aws.sansbound" bucket.

The screenshot shows the AWS S3 Management Console interface. At the top, there are tabs for 'IAM Management Console' and 'S3 Management Console'. The URL in the address bar is <https://s3.console.aws.amazon.com/s3/home?region=us-east-1#>. The header includes the AWS logo, 'Services' dropdown, 'Resource Groups' dropdown, user info ('student2 @ 2971-1130-8396'), 'Global' dropdown, and 'Support' dropdown. A banner at the top says 'Identify optimal storage classes with S3 Analytics - Storage Class Analysis. [Learn More »](#)' and 'Documentation'.

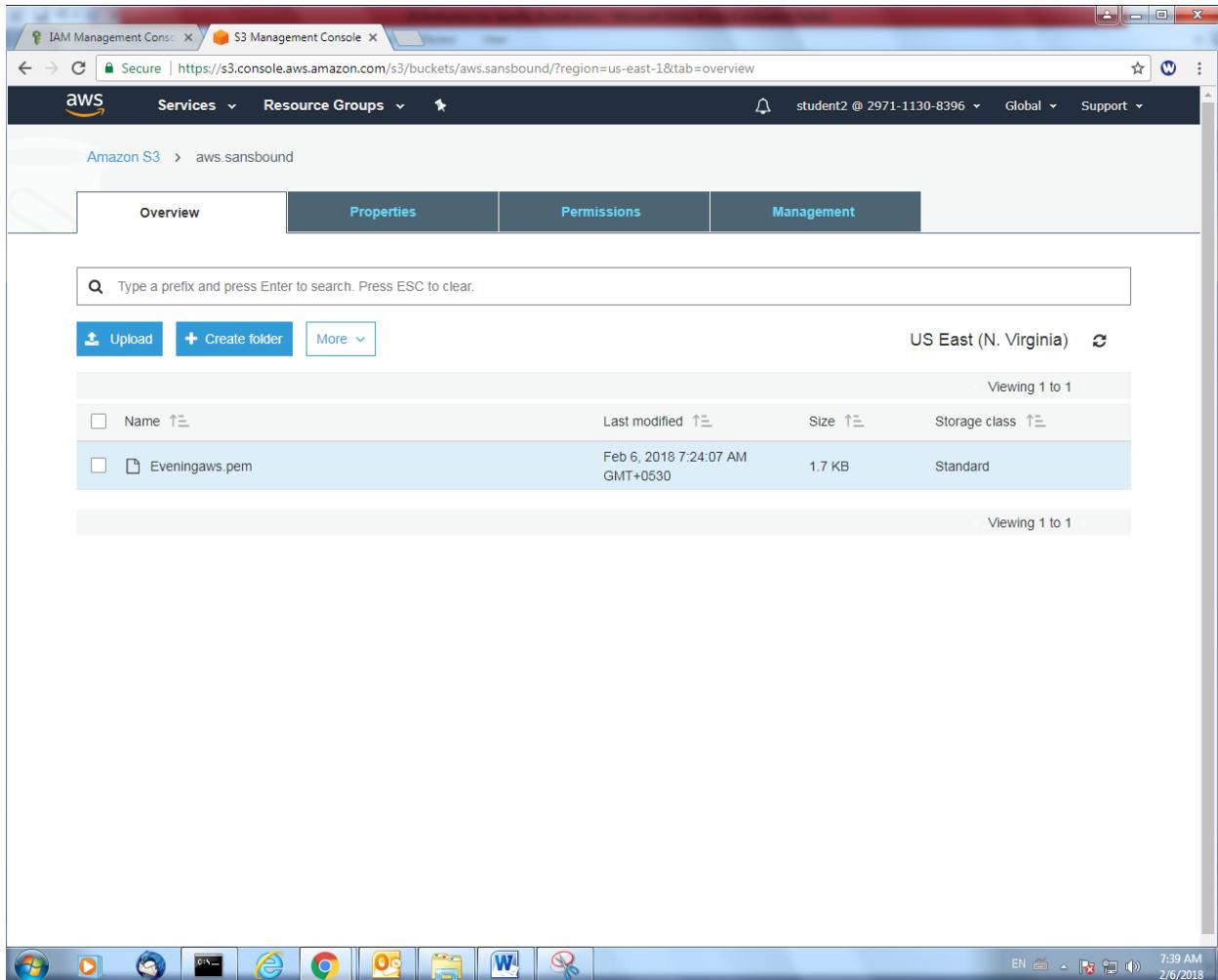
The main area is titled 'Amazon S3' with a search bar 'Search for buckets'. Below it are buttons for '+ Create bucket', 'Delete bucket', and 'Empty bucket'. It displays 6 Buckets and 5 Regions. The table lists the following buckets:

Bucket name	Access	Region	Date created
aws.sansbound	Error	US East (N. Virginia)	Feb 6, 2018 7:21:56 AM GMT+0530
elasticbeanstalk-ap-south-1-297111308396	Error	Asia Pacific (Mumbai)	Dec 20, 2017 5:48:27 PM GMT+0530
elasticbeanstalk-us-east-1-297111308396	Error	US East (N. Virginia)	Jan 23, 2018 10:42:40 AM GMT+0530
elasticbeanstalk-us-east-2-297111308396	Error	US East (Ohio)	Dec 15, 2017 10:52:13 AM GMT+0530
elasticbeanstalk-us-west-1-297111308396	Error	US West (N. California)	Jan 25, 2018 7:04:06 AM GMT+0530
elasticbeanstalk-us-west-2-297111308396	Error	US West (Oregon)	Jan 27, 2018 6:23:50 PM GMT+0530

A note at the bottom states: '* Objects might still be publicly accessible due to object ACLs. [Learn more](#)'.

The taskbar at the bottom shows various icons for Windows applications like File Explorer, Task View, and Control Panel, along with system status icons for battery, signal, and volume, and the date and time '7:38 AM 2/6/2018'.

We can able to view the file.



Try to access another bucket “elasticbeanstalk”. But we are not able to access the bucket. Because we have provided access to student2 user only for aws.sansbound bucket only.

