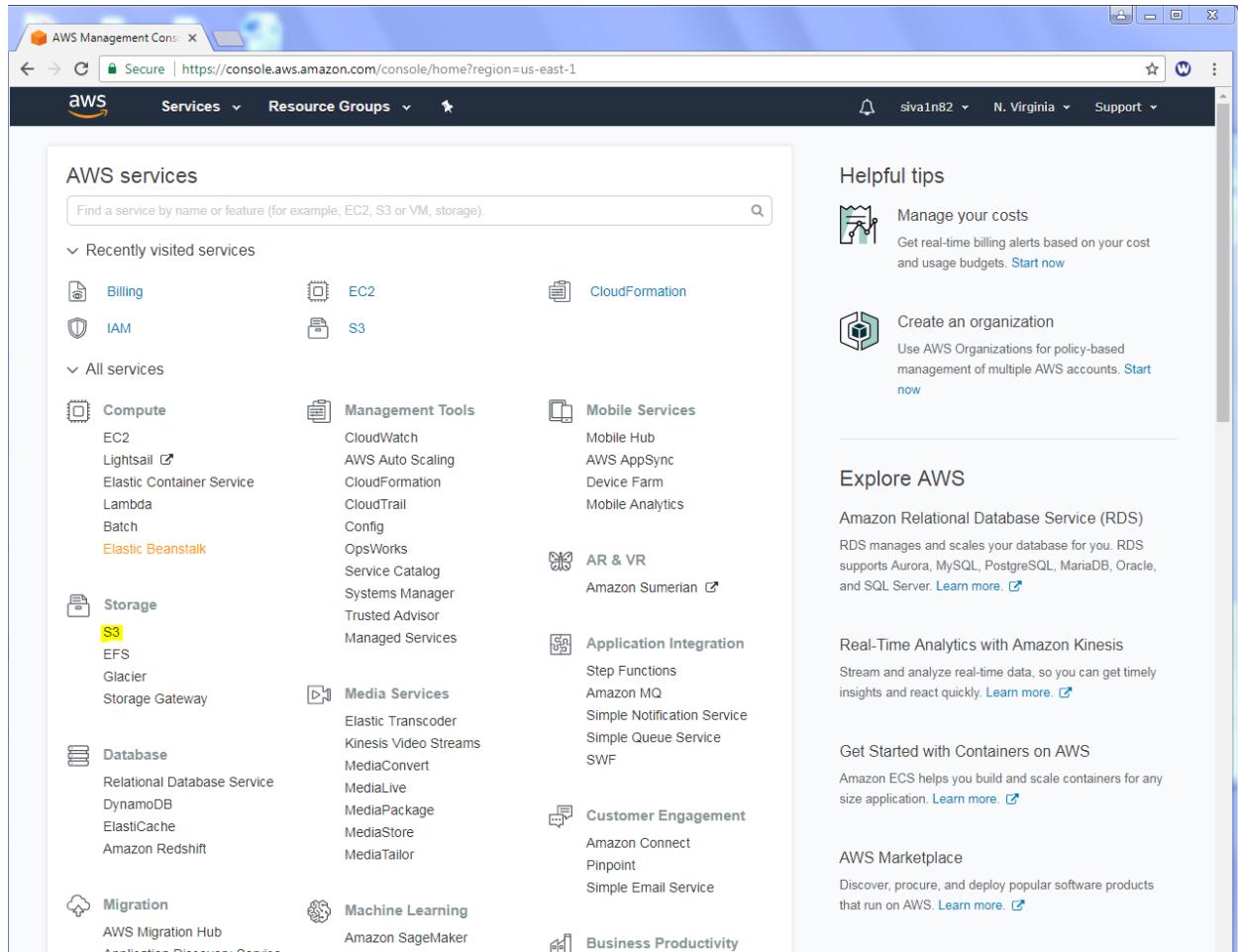


## Lab24

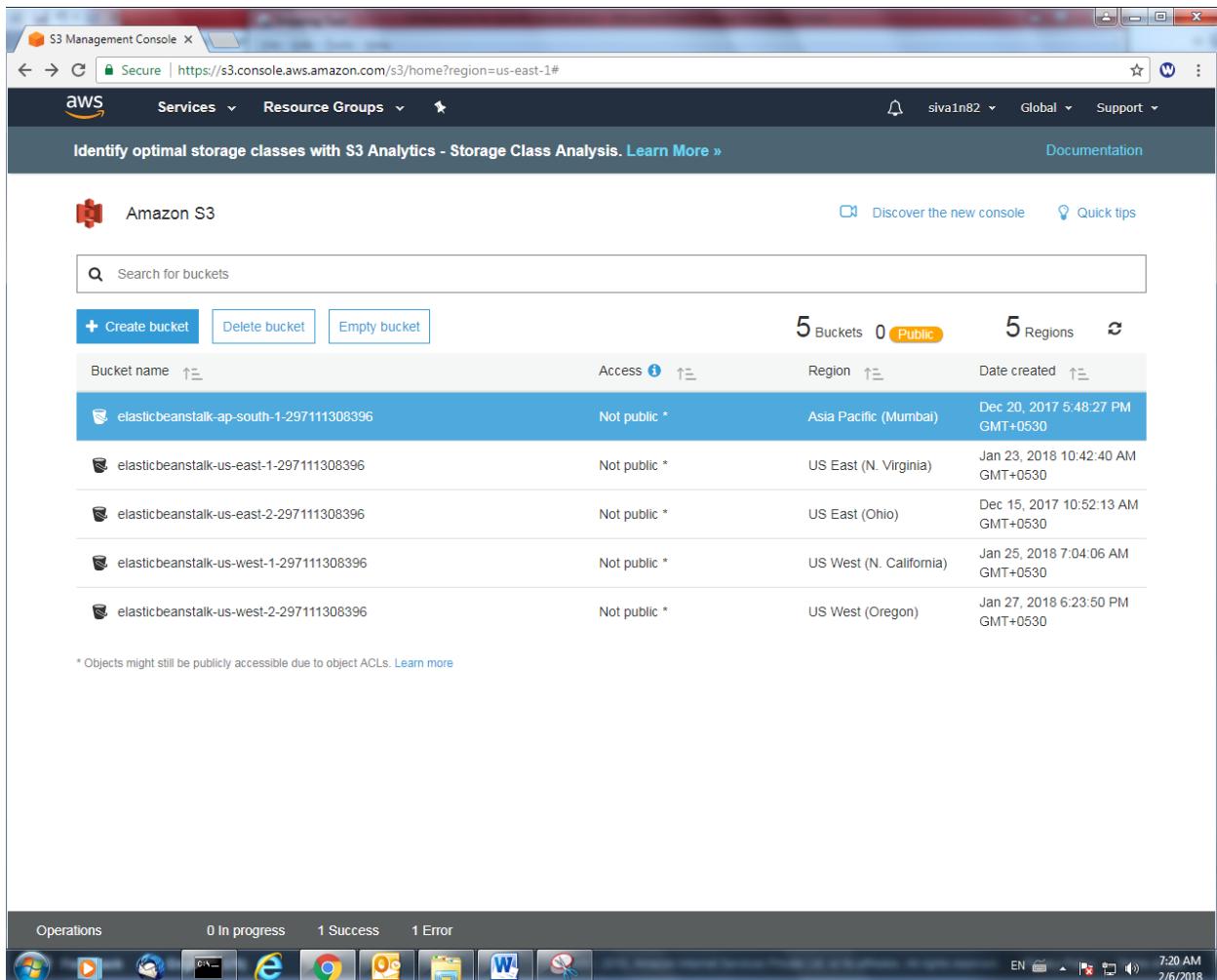
### S3 Restriction for Specific Bucket

Click "S3" service



The screenshot shows the AWS Management Console homepage. The top navigation bar includes the AWS logo, a search bar, and account information (sivaIn82, N. Virginia, Support). Below the navigation is a section titled "AWS services" with a search bar. A sidebar on the left lists "Recently visited services" (Billing, EC2, CloudFormation, IAM, S3) and "All services" categorized into Compute, Storage, Database, Migration, Services (Management Tools, Mobile Services, AR & VR, Application Integration, Media Services, Customer Engagement, Machine Learning, Business Productivity), and AWS Marketplace. The "S3" icon in the Storage category is highlighted with a red box. To the right of the services list are "Helpful tips" for managing costs and creating organizations, and sections for exploring AWS services like RDS, Kinesis, ECS, and Marketplace.

Click “Create bucket” with unique name.



The screenshot shows the AWS S3 Management Console interface. At the top, there's a header bar with the AWS logo, a Services dropdown, Resource Groups dropdown, user information (siva1n82), Global dropdown, and Support dropdown. Below the header, a banner reads "Identify optimal storage classes with S3 Analytics - Storage Class Analysis. Learn More »" and "Documentation". The main area is titled "Amazon S3" and features a search bar with the placeholder "Search for buckets". Below the search bar are three buttons: "+ Create bucket", "Delete bucket", and "Empty bucket". To the right of these buttons, it shows "5 Buckets" and "0 Public" buckets. Further right, it shows "5 Regions" and a refresh icon. The main content area displays a table of buckets:

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 with icons for various Windows applications like File Explorer, Word, and Task Manager. The system tray shows the date and time as "2/6/2018 7:20 AM".

Type aws.sansbound.com

### Create bucket

X

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

Name and region

Bucket name ⓘ

Region

US East (N. Virginia) ▾

---

Copy settings from an existing bucket

Select bucket (optional)

5 Buckets ▾

---

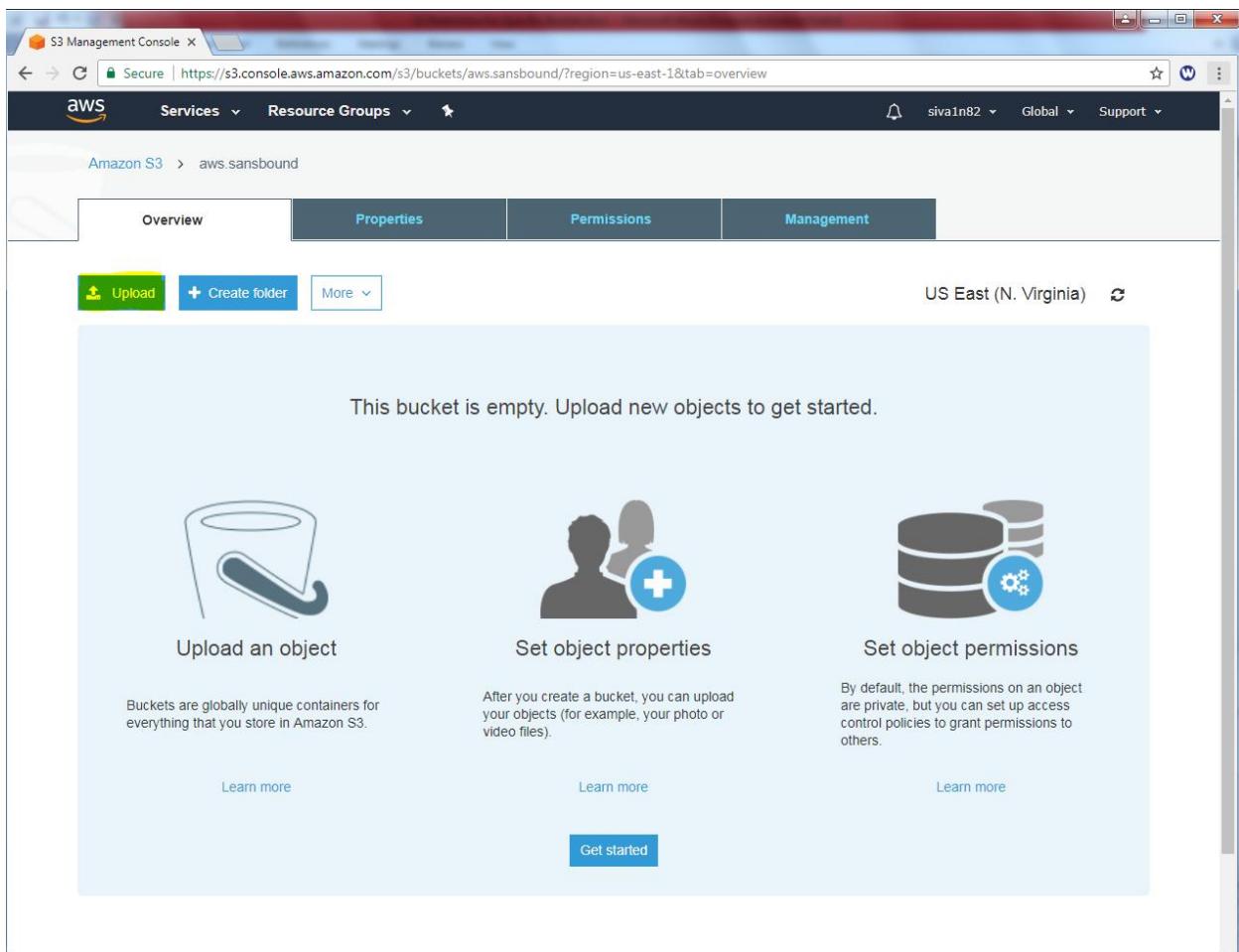
Create

Cancel

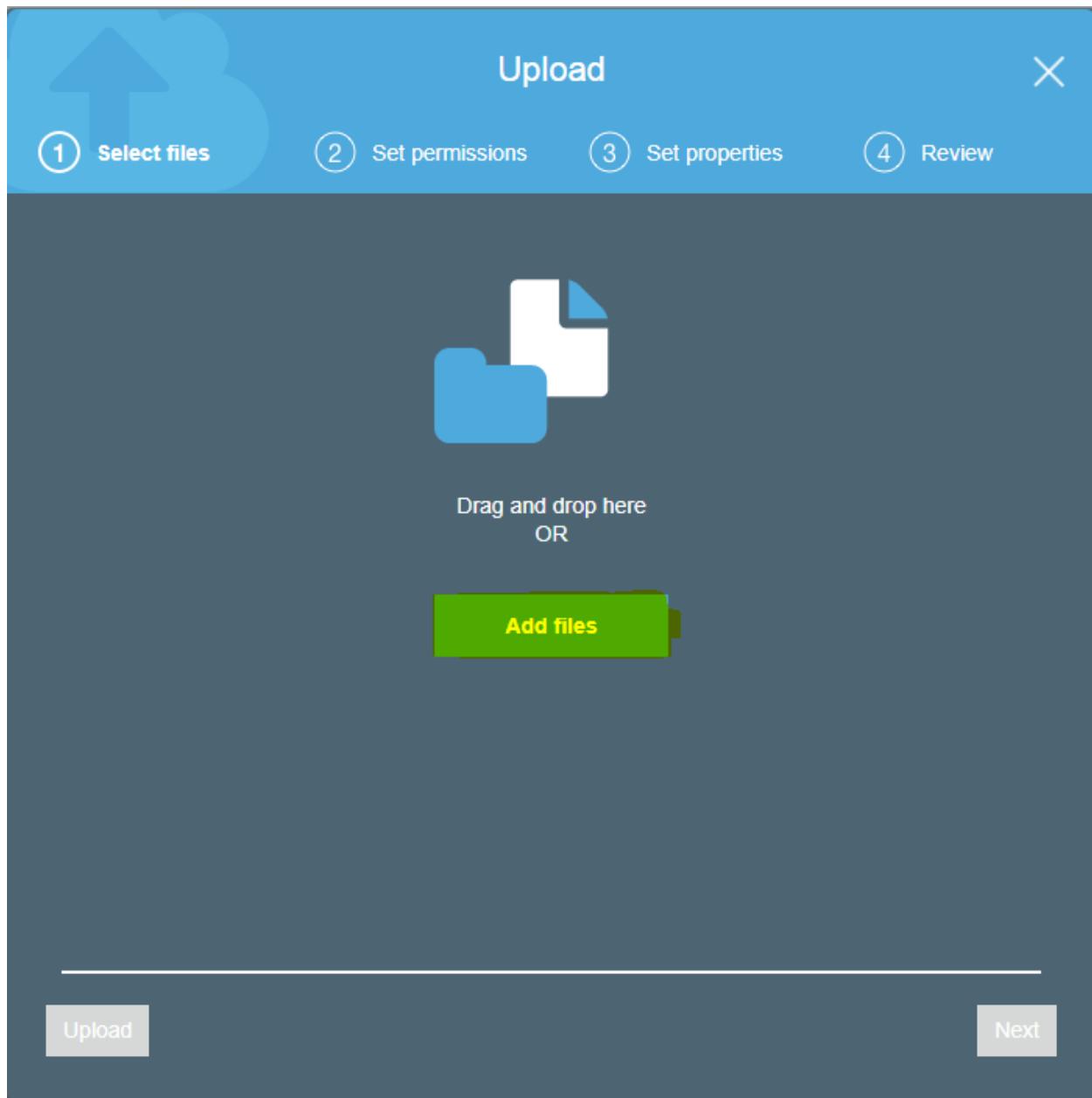
Next

Click "Create".

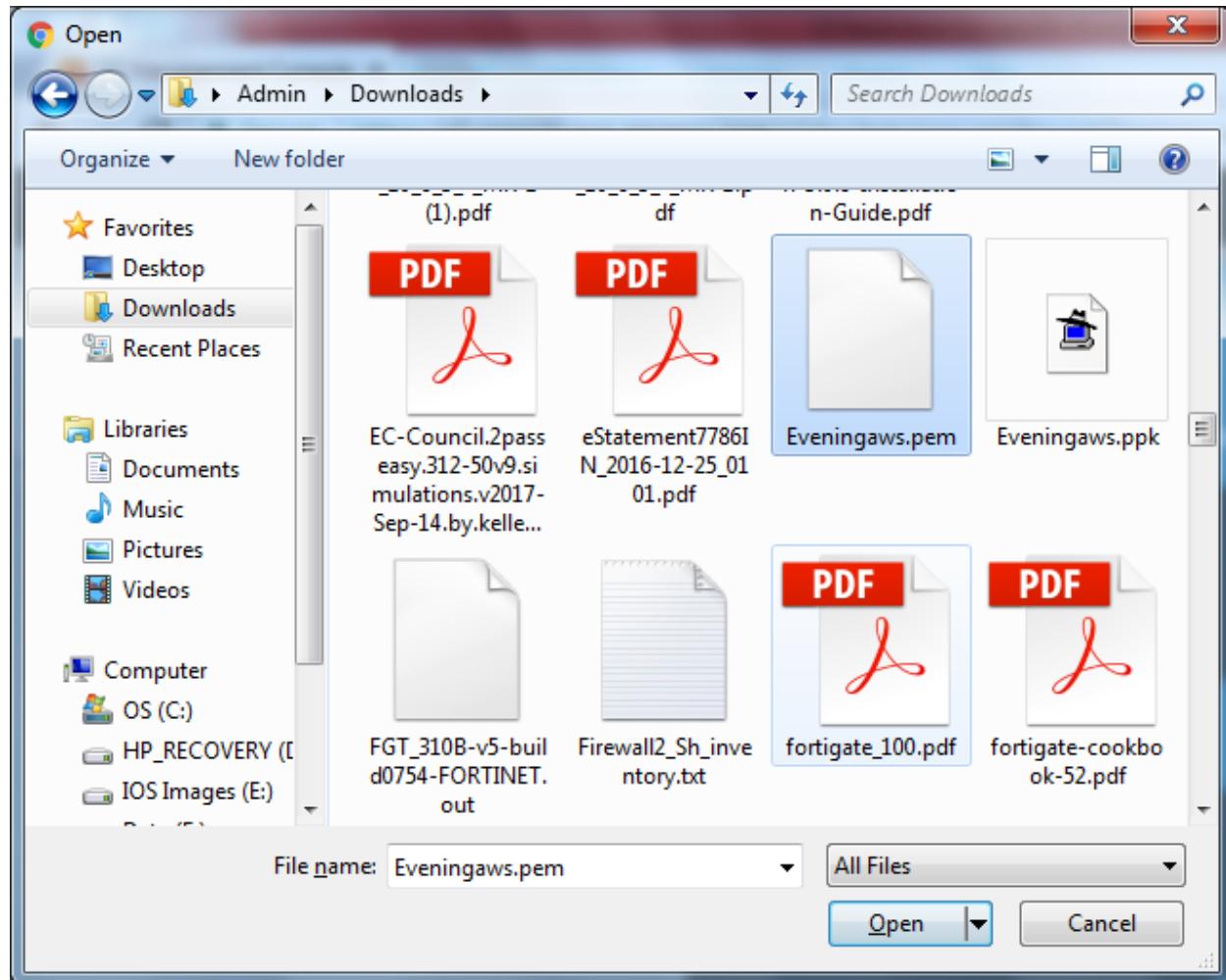
Click "Upload".



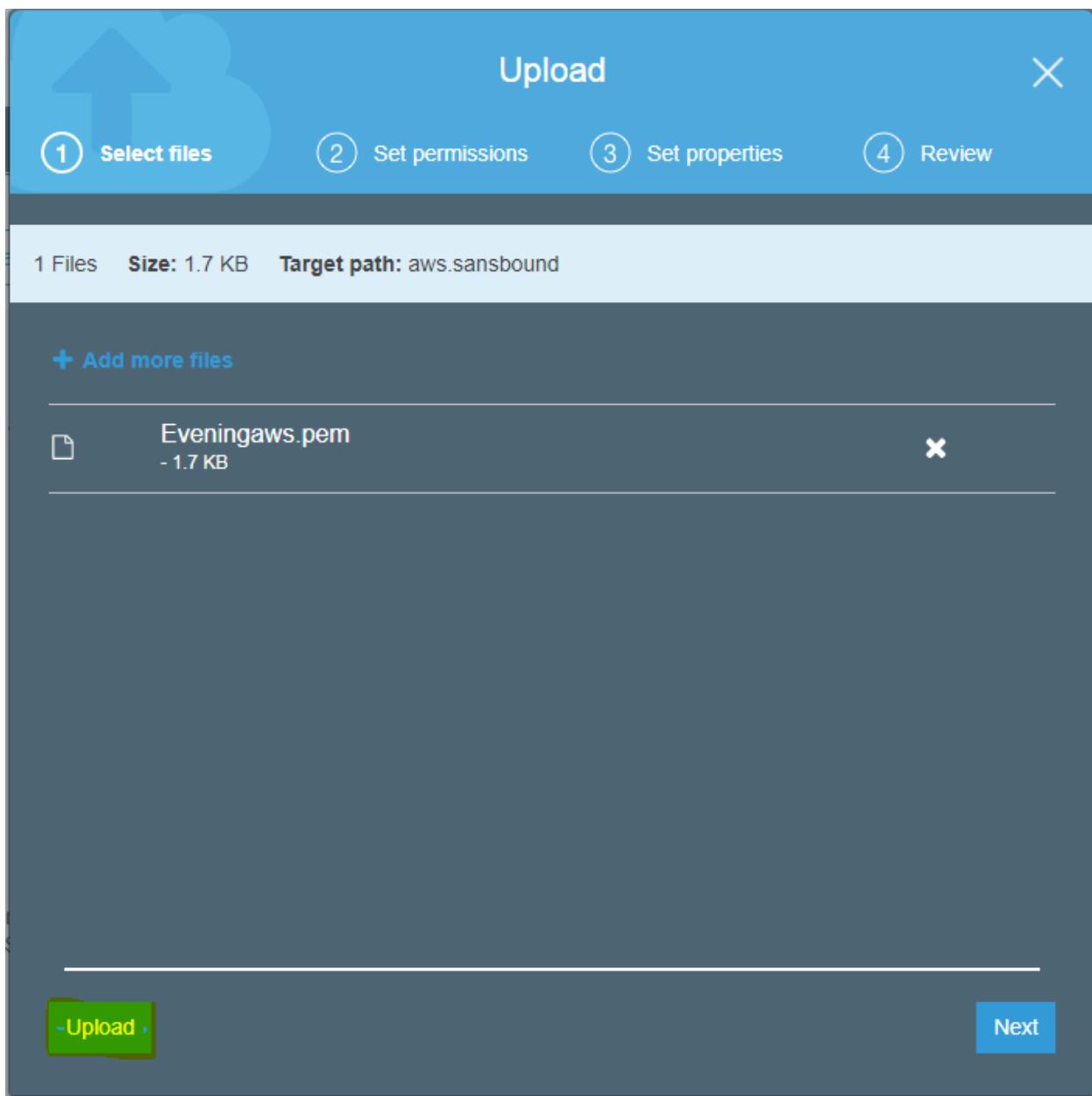
Click “Add files”.



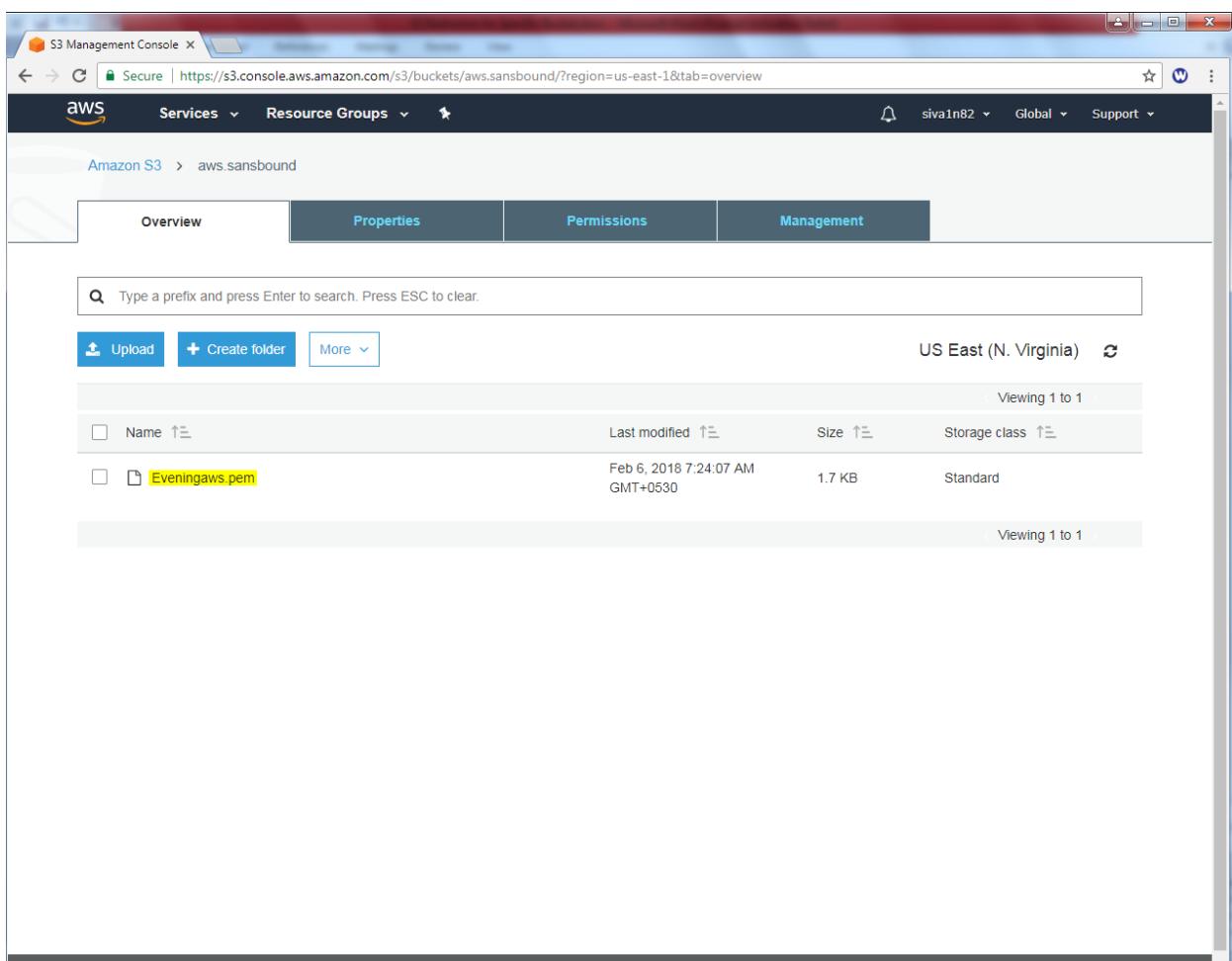
Locate the file and click open.



Click “Upload” to upload the file.



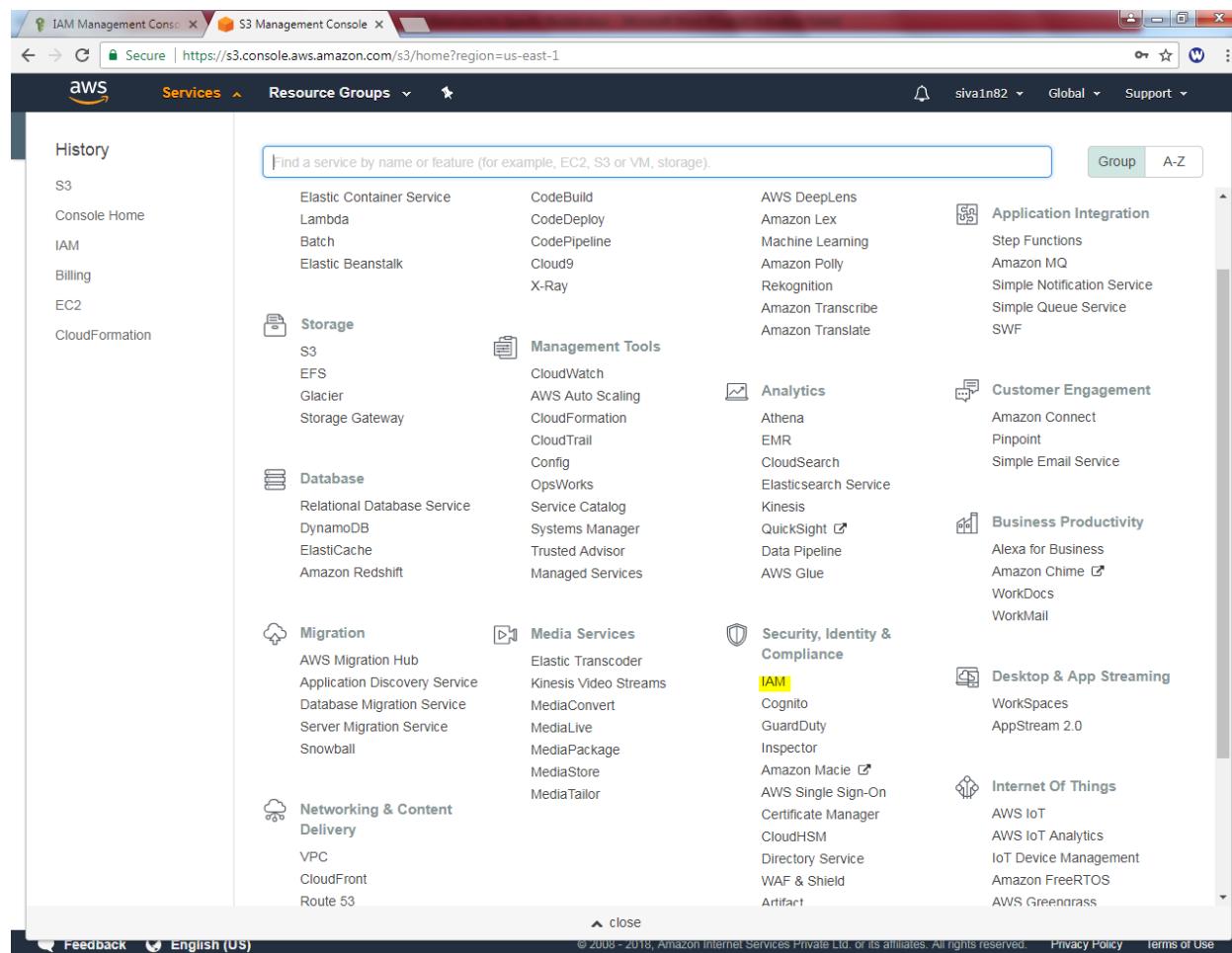
We can able view the file.



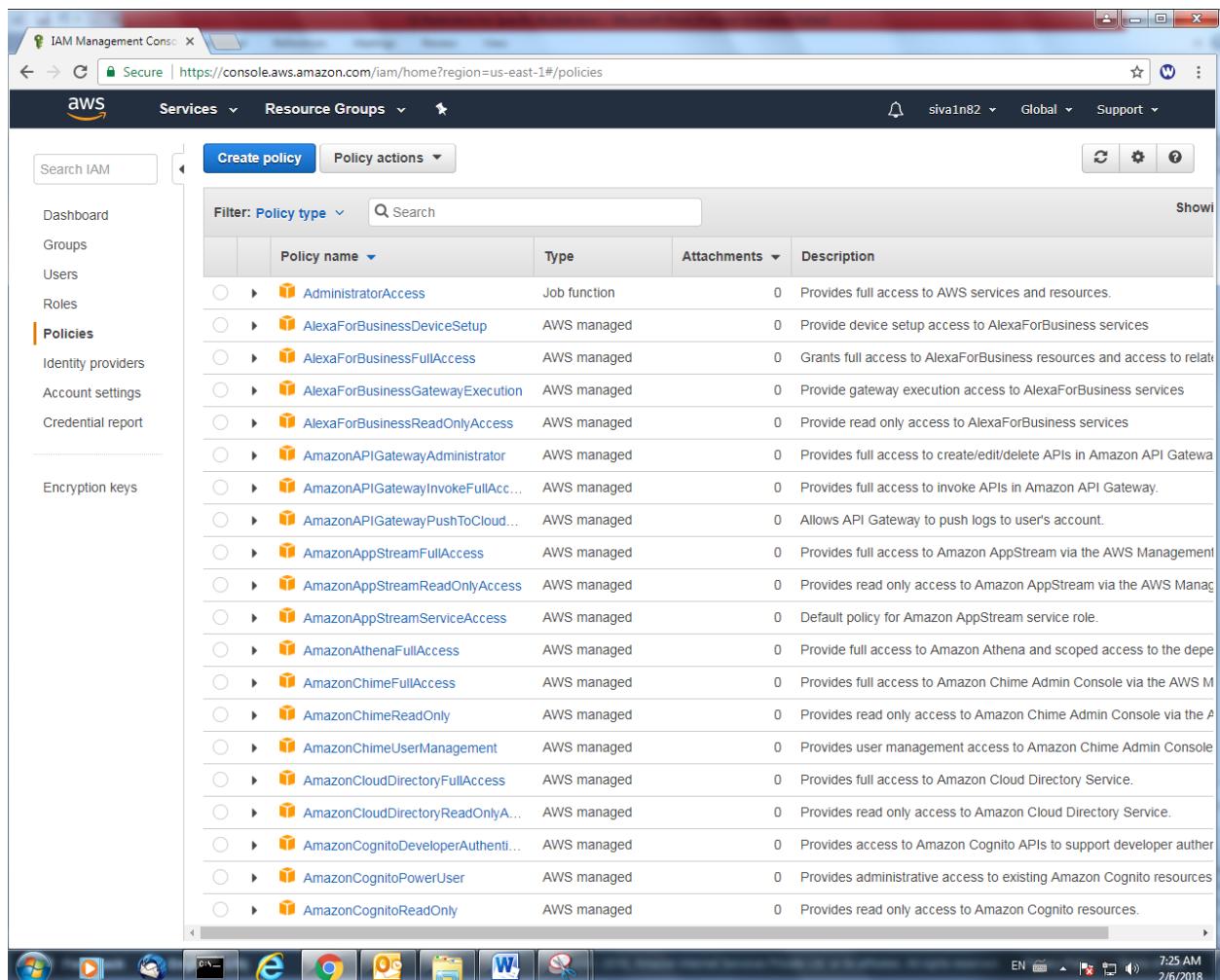
The screenshot shows the AWS S3 Management Console interface. The URL in the address bar is <https://s3.console.aws.amazon.com/s3/buckets/aws.sansbound/?region=us-east-1&tab=overview>. The page displays the contents of the 'aws.sansbound' bucket in the 'US East (N. Virginia)' region. A single file, 'Eveningaws.pem', is listed. The file was last modified on Feb 6, 2018, at 7:24:07 AM (GMT+0530) and has a size of 1.7 KB. It is stored in the Standard storage class. The file name is highlighted in yellow.

Name	Last modified	Size	Storage class
Eveningaws.pem	Feb 6, 2018 7:24:07 AM GMT+0530	1.7 KB	Standard

Click “IAM” Role.



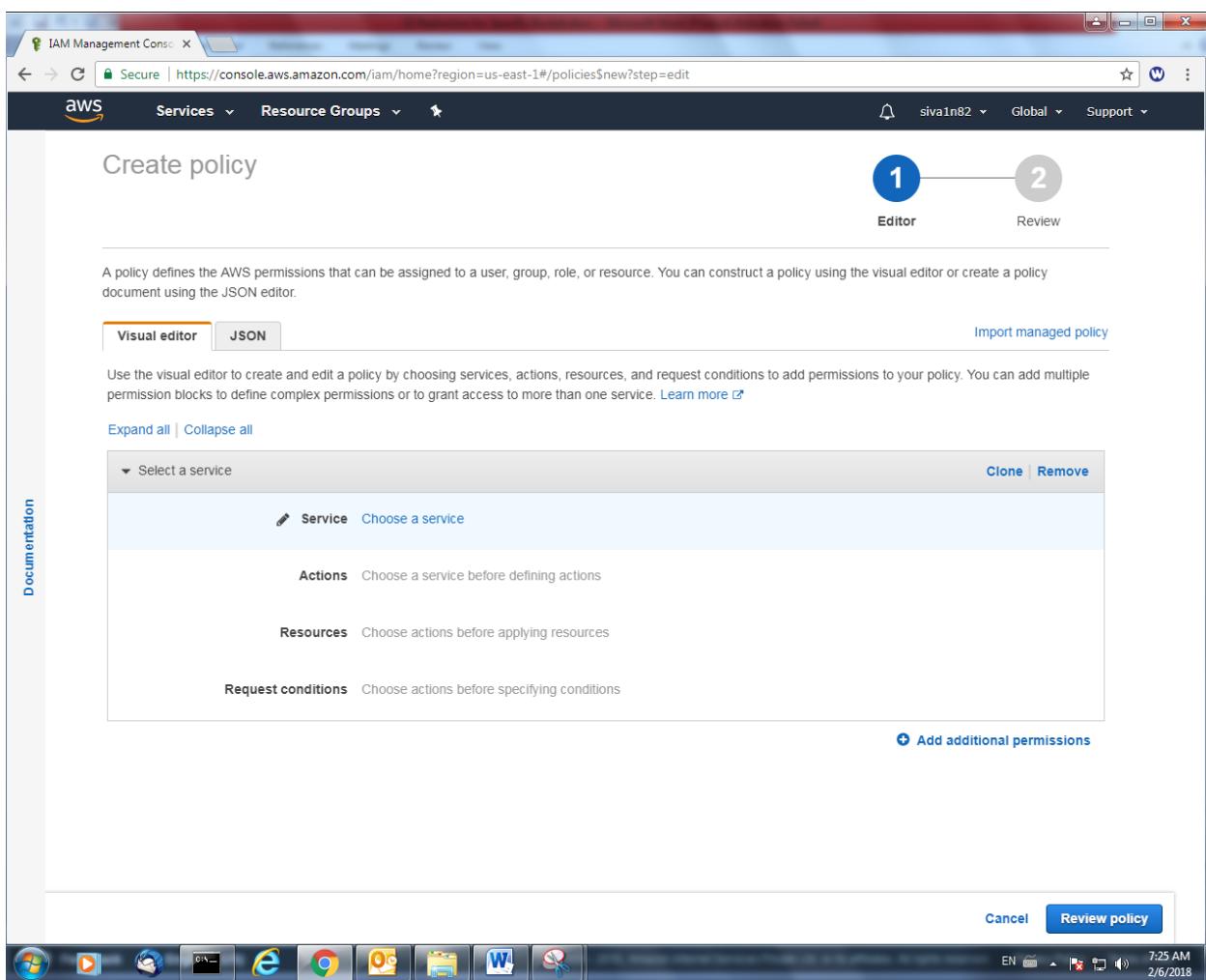
Click “Create Policy”.



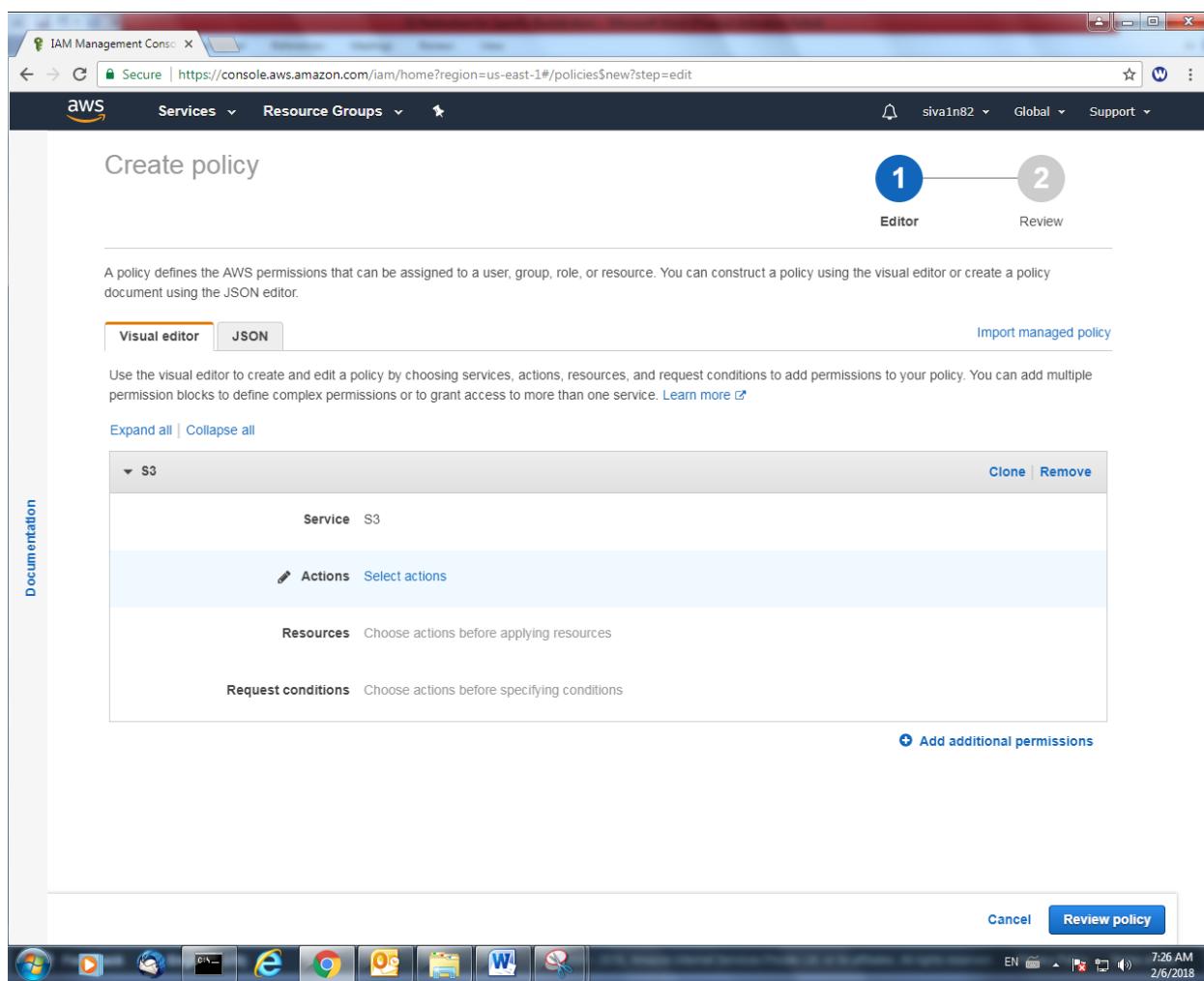
The screenshot shows the AWS IAM Management Console with the URL <https://console.aws.amazon.com/iam/home?region=us-east-1#/policies>. The left sidebar is collapsed, and the main area displays a table of AWS managed policies. The table has columns for Policy name, Type, Attachments, and Description. The 'Policies' option in the sidebar is selected, indicated by a blue border.

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



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**

Service S3

Actions **Select actions**

Resources Choose actions before applying resources

Request conditions Choose actions before specifying conditions

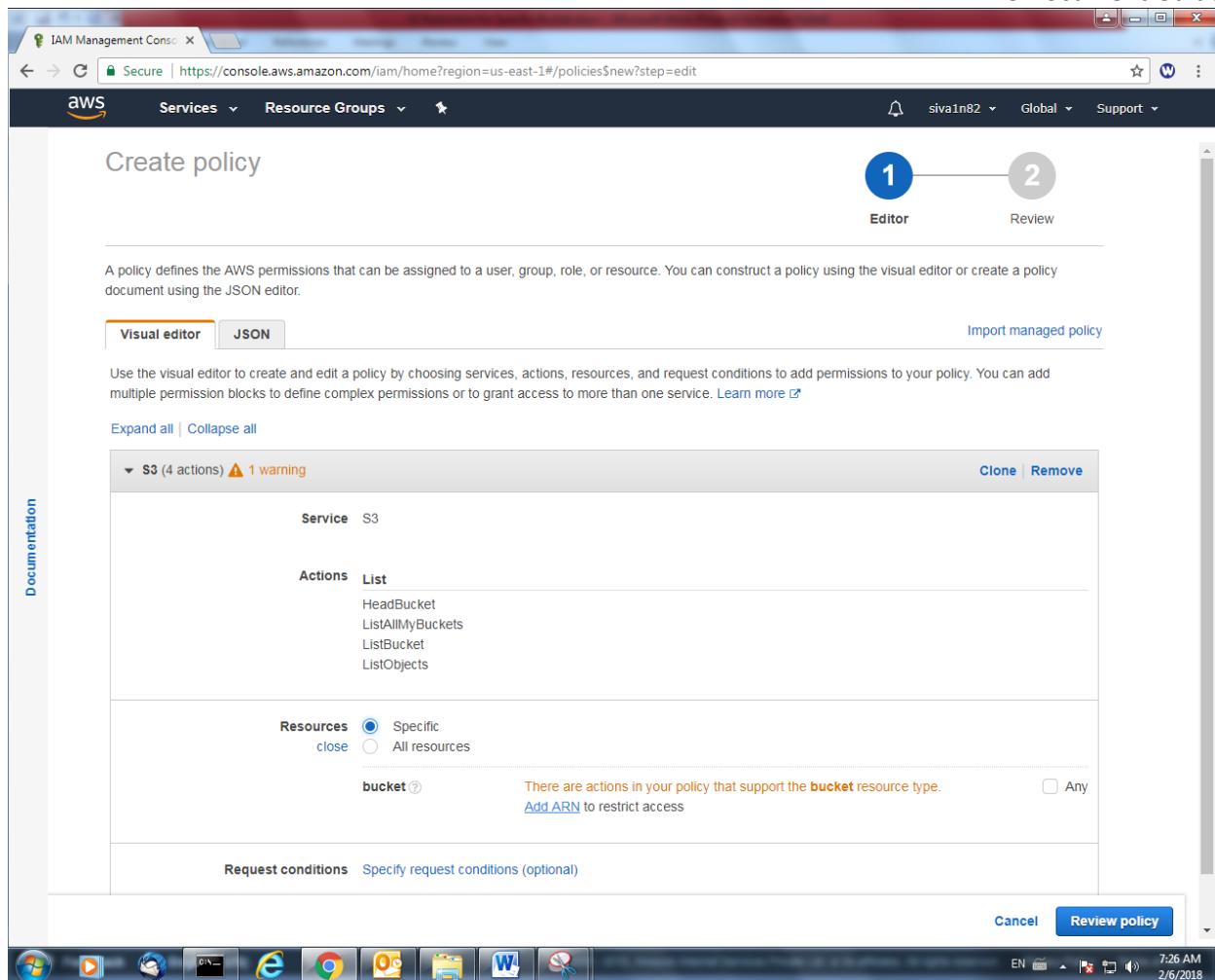
Add additional permissions

Cancel Review policy

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

The screenshot shows the AWS IAM Management Console interface. The URL in the address bar is [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 main content area displays the Visual editor tab selected. It shows a policy for the S3 service with four actions selected: List, Read, Write, and Permissions management. A note at the bottom states: "There are actions in your policy that support the **bucket** resource type." The browser taskbar at the bottom shows various open tabs and icons.

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



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** List

- HeadBucket
- ListAllMyBuckets
- ListBucket
- ListObjects

**Resources**  Specific  All resources

**bucket** There are actions in your policy that support the **bucket** resource type.  Any [Add ARN](#) to restrict access

**Request conditions** Specify request conditions (optional)

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

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](#)

arn:aws:s3:::aws.sansbound

**Bucket name**   Any

[Cancel](#) Add

Click “Review Policy”.

IAM Management Console X

Secure | https://console.aws.amazon.com/iam/home?region=us-east-1#policies\$new?step=edit

aWS Services Resource Groups siva1n82 Global Support

Editor Review

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.

**Visual editor** **JSON** **Import managed policy**

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

Service S3

**Actions** List

- HeadBucket
- ListAllMyBuckets
- ListBucket
- ListObjects

**Resources**  Specific  All resources

**bucket** [Edit](#)  Any

arn:aws:s3:::aws.sansbound

Add ARN to restrict access

**Request conditions** Specify request conditions (optional)

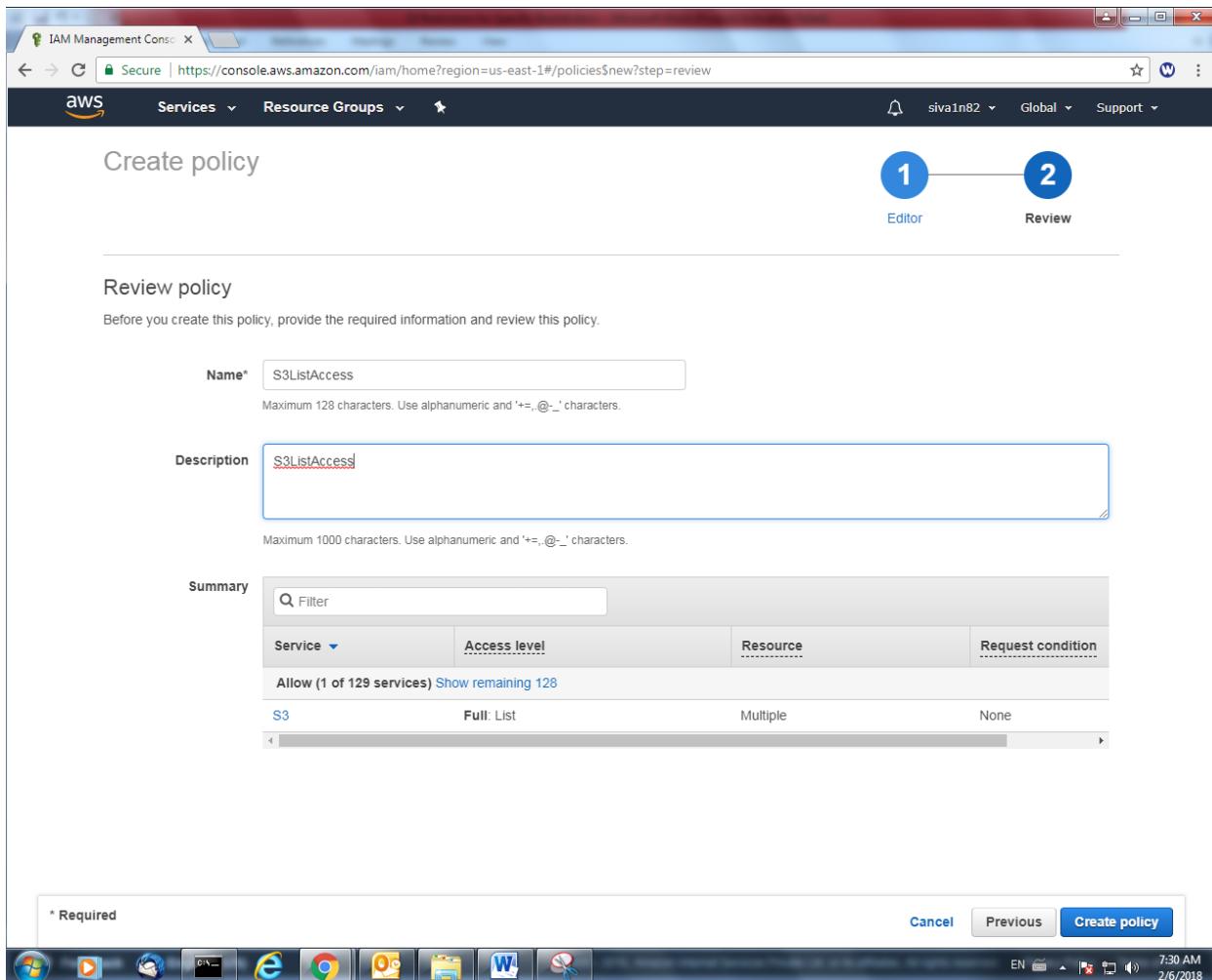
[Add additional permissions](#)

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

EN 7:28 AM 2/6/2018



Type Name of Policy and Description.



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**

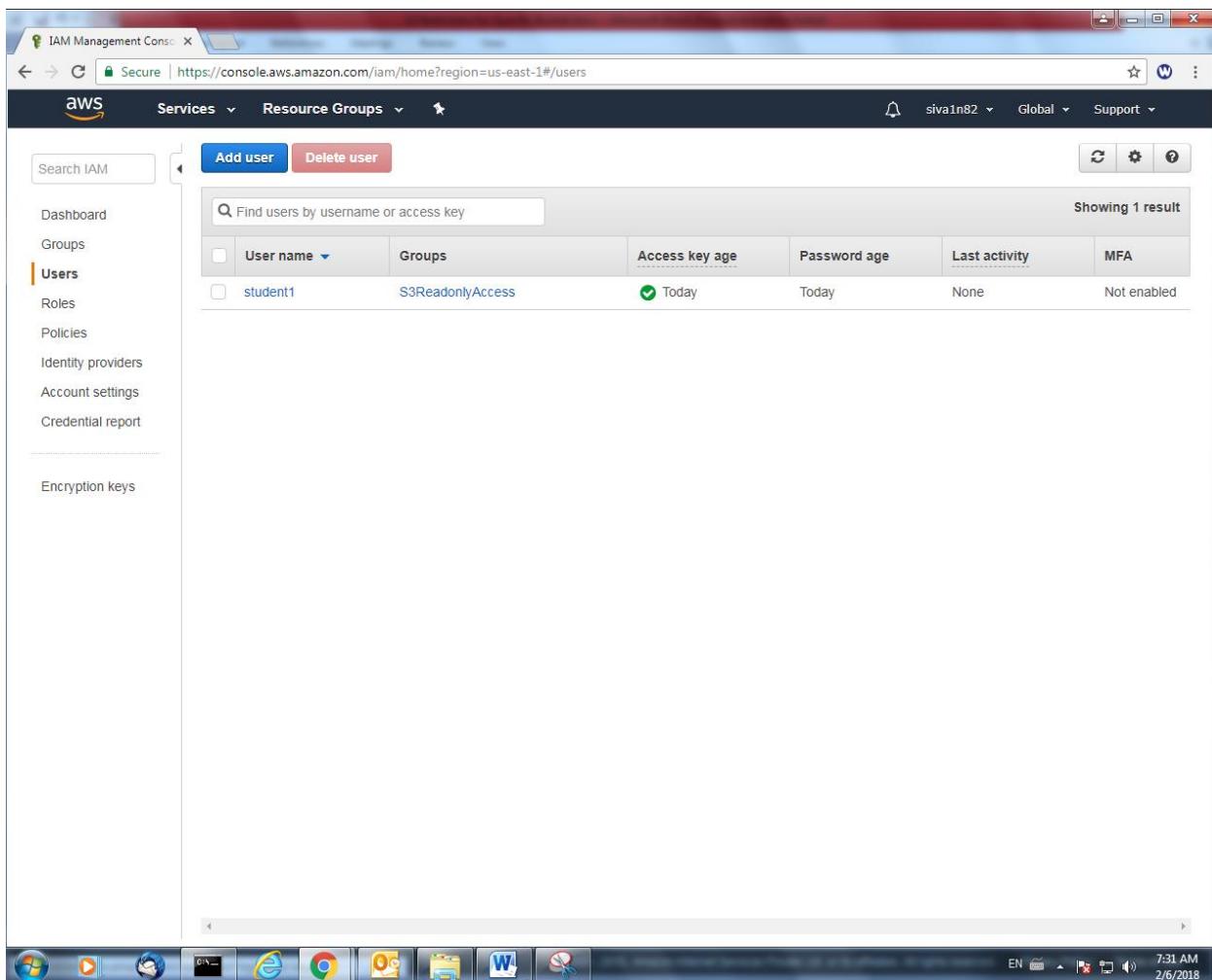
Service	Access level	Resource	Request condition
Allow (1 of 129 services) Show remaining 128			
S3	Full: List	Multiple	None

\* Required      Cancel      Previous      Create policy

Click "Create Policy".

We need to create a user to assign the policy.

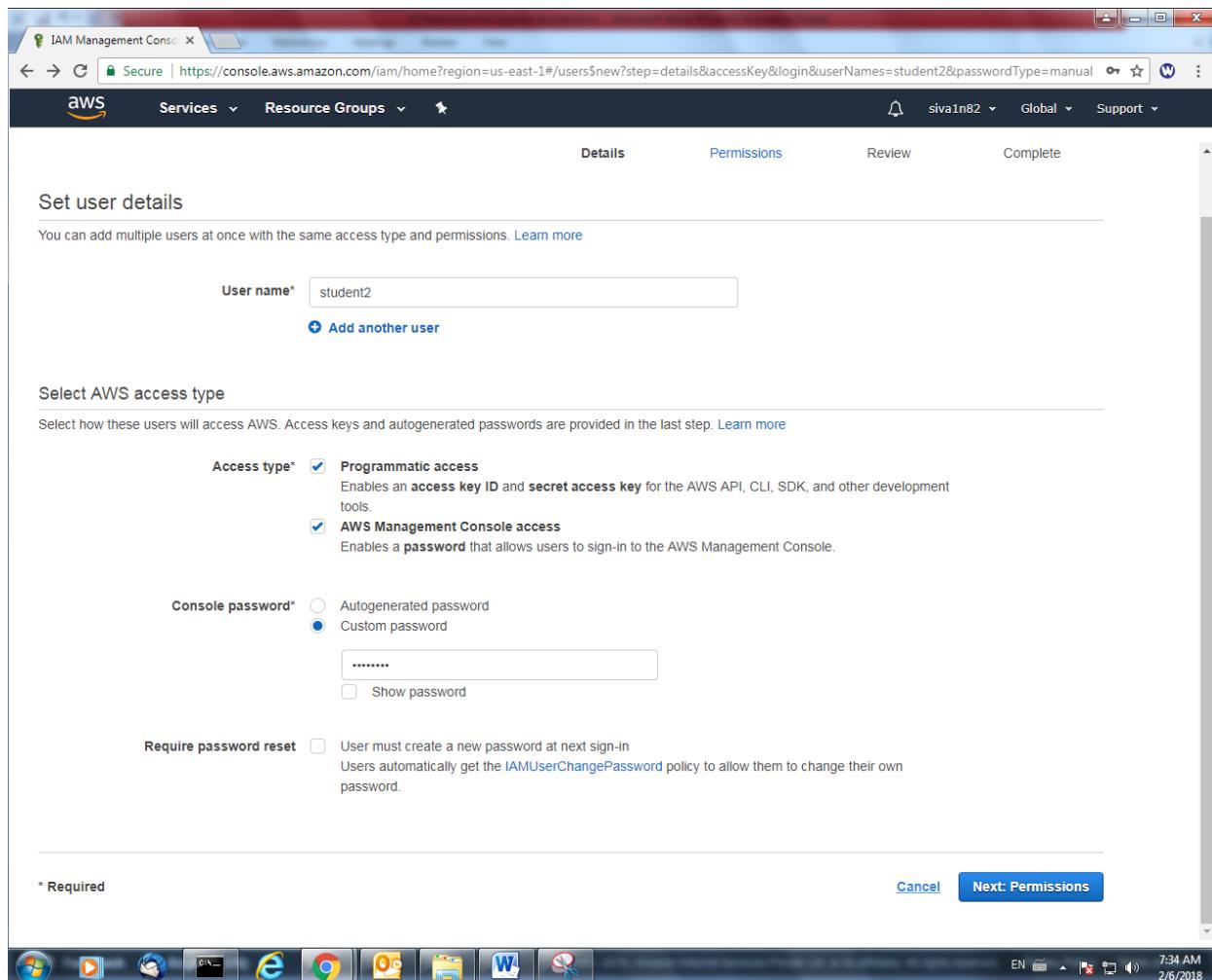
Click "Add user".



User name	Groups	Access key age	Password age	Last activity	MFA
student1	S3ReadOnlyAccess	Today	Today	None	Not enabled

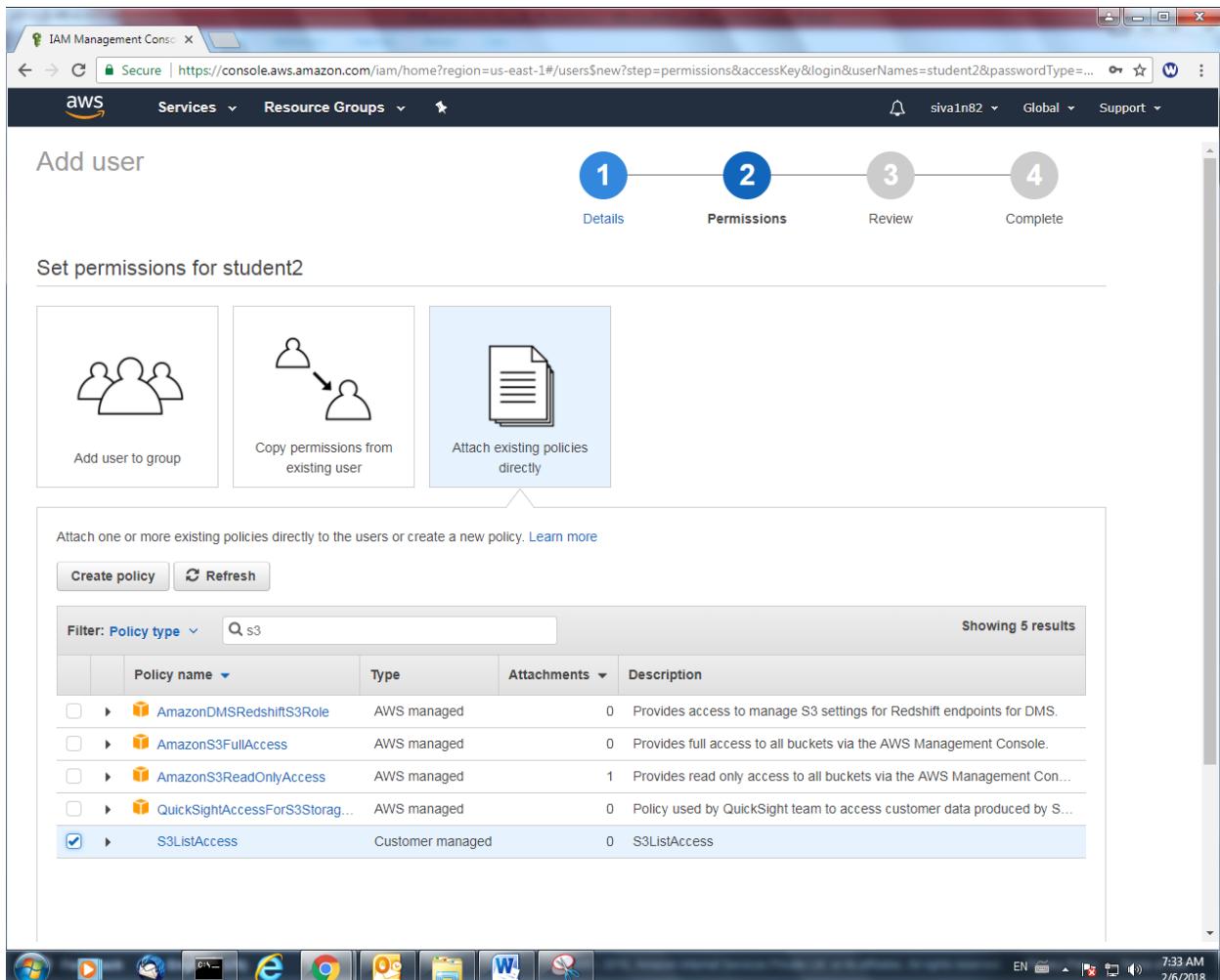
Username: student2

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 browser title is "JAM Management Conso". The navigation bar includes "Services", "Resource Groups", "sivaIn82", "Global", and "Support".

The main heading is "Add user" and the sub-step is "Permissions" (marked with a blue circle labeled "2"). Below it are "Details" (blue circle labeled "1"), "Review" (grey circle labeled "3"), and "Complete" (grey circle labeled "4").

The section "Set permissions for student2" contains three options:

- Add user to group
- Copy permissions from existing user
- Attach existing policies directly

A callout arrow points from the "Attach existing policies directly" option to the search results table below.

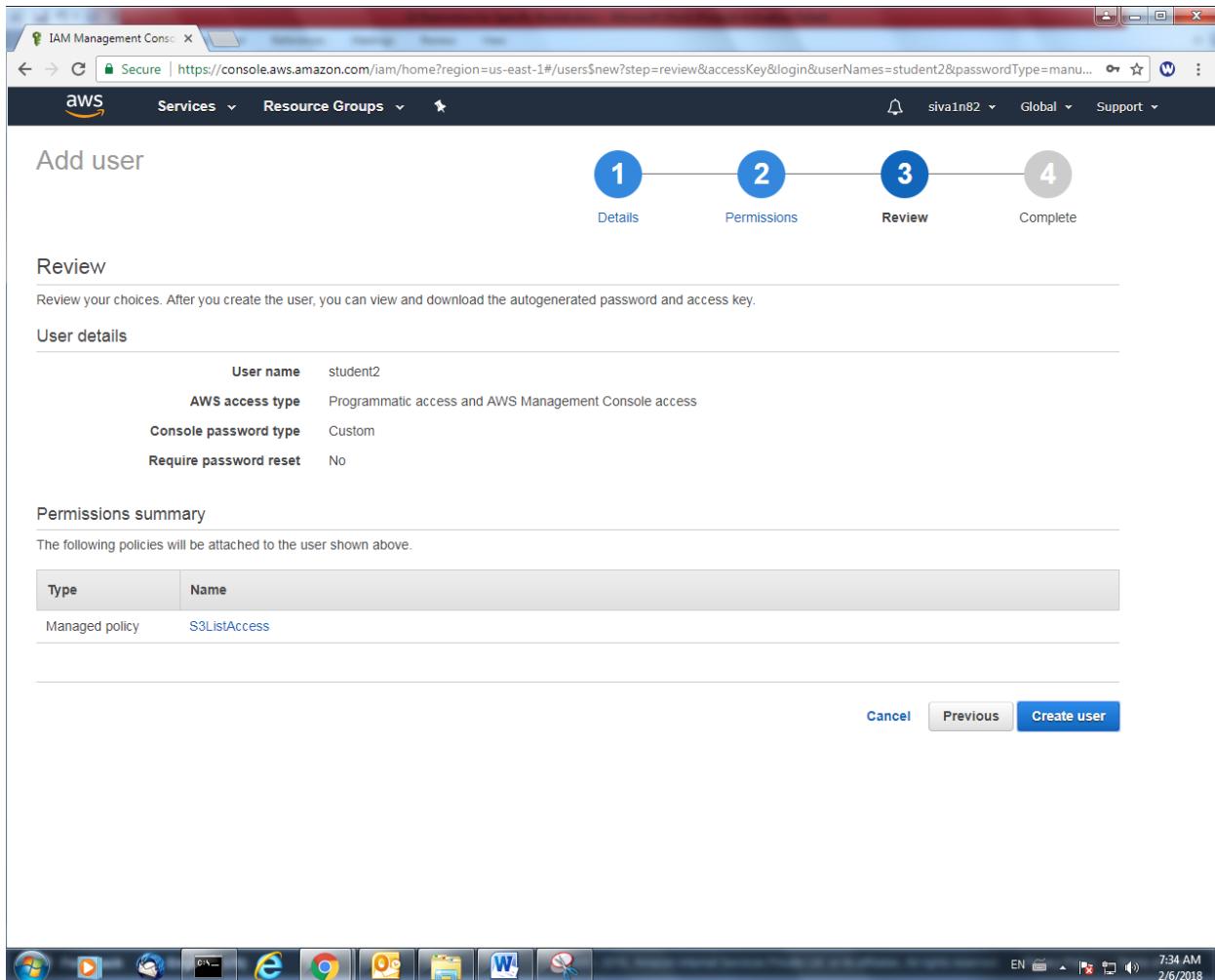
The search results table is titled "Showing 5 results" and has columns: Policy name, Type, Attachments, and Description. It lists five policies, with "S3ListAccess" being the selected one (indicated by a checked checkbox). The table includes a "Filter: Policy type" dropdown set to "s3" and a "Refresh" button.

	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

The taskbar at the bottom shows various icons for Windows applications like File Explorer, Internet Explorer, and Microsoft Word, along with system status icons. The date and time are shown as "7:33 AM 2/6/2018".

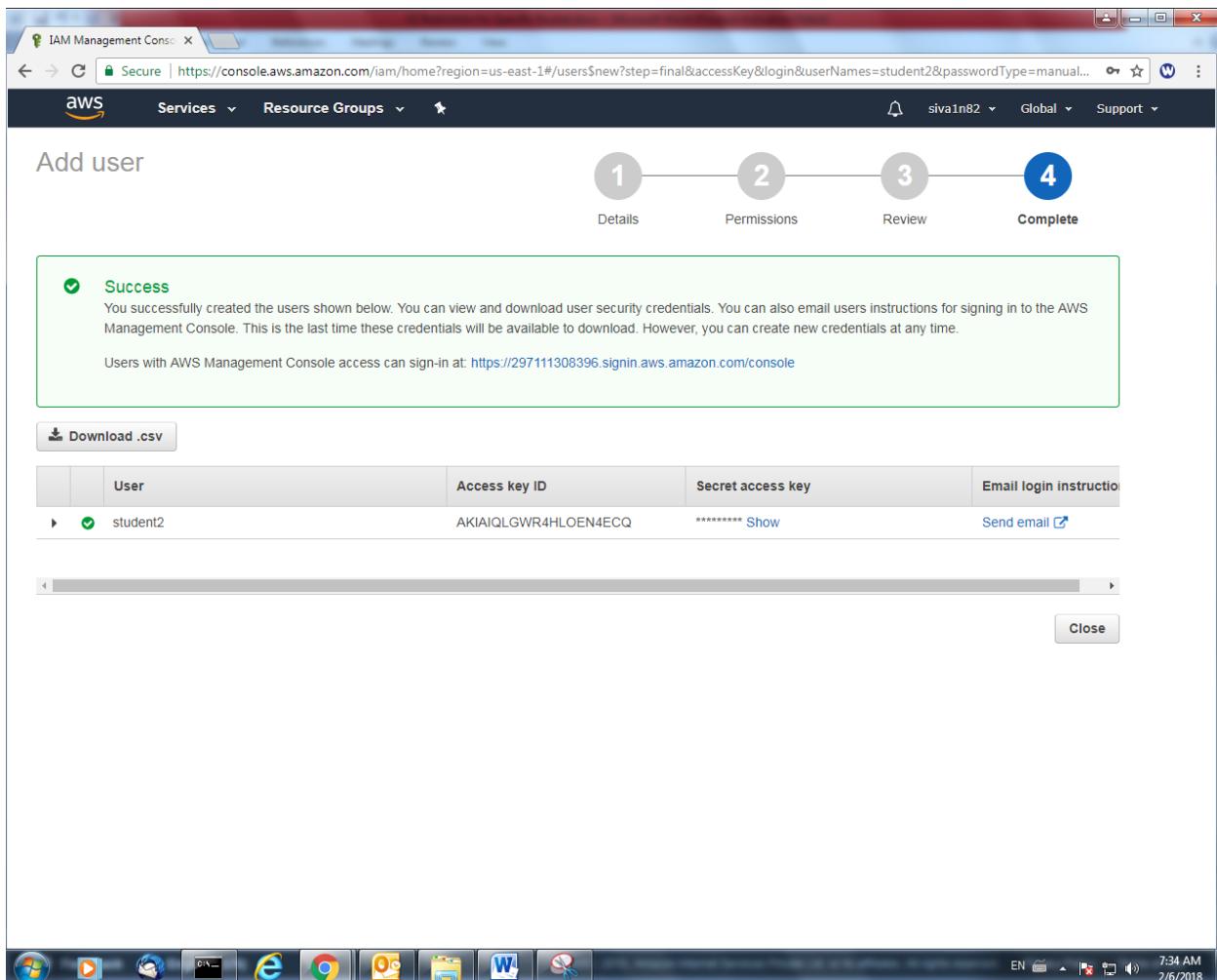
Click "Next".

Click "Create user".



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=review&accessKey&login&userNames=student2&passwordType=manu...](https://console.aws.amazon.com/iam/home?region=us-east-1#/users$new?step=review&accessKey&login&userNames=student2&passwordType=manu...). The page is titled "Add user" and displays four steps: Details (1), Permissions (2), Review (3), and Complete (4). Step 3 is highlighted with a blue circle. The "Review" section shows the user details: User name (student2), AWS access type (Programmatic access and AWS Management Console access), Console password type (Custom), and Require password reset (No). The "Permissions summary" section lists a single managed policy: S3ListAccess. At the bottom right, there are "Cancel", "Previous", and "Create user" buttons, with "Create user" being the active button.

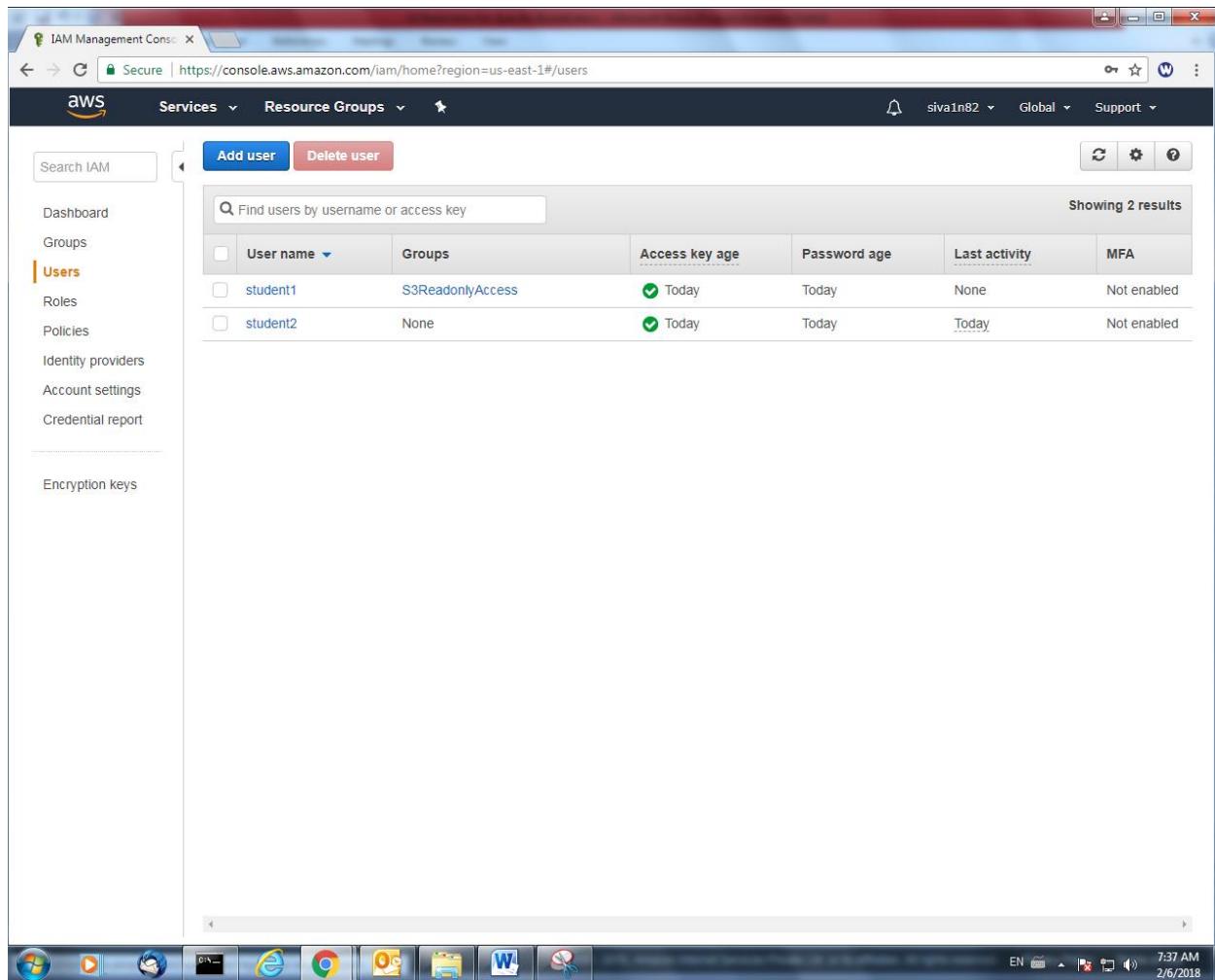
User successfully created. Please note that URL as below in box.



The screenshot shows the AWS IAM Management Console interface. The title bar reads "IAM Management Console". The navigation bar includes "Services", "Resource Groups", and "Global". The main heading is "Add user". A progress bar at the top right shows four steps: 1. Details (grey), 2. Permissions (grey), 3. Review (grey), and 4. Complete (blue). A "Success" message box is displayed, stating: "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 includes a link: "Users with AWS Management Console access can sign-in at: <https://297111308396.signin.aws.amazon.com/console>". Below this is a table with columns: User, Access key ID, Secret access key, and Email login instructions. One row is shown for "student2", with "Access key ID" as "AKIAIQLGWR4HLOEN4ECQ" and "Secret access key" as "\*\*\*\*\* Show". A "Send email" button is next to the secret key. At the bottom right of the modal is a "Close" button. The taskbar at the bottom of the screen shows various icons for Windows applications like File Explorer, Internet Explorer, and Microsoft Word, along with system status icons.

User	Access key ID	Secret access key	Email login instructions
student2	AKIAIQLGWR4HLOEN4ECQ	***** Show	<a href="#">Send email</a>

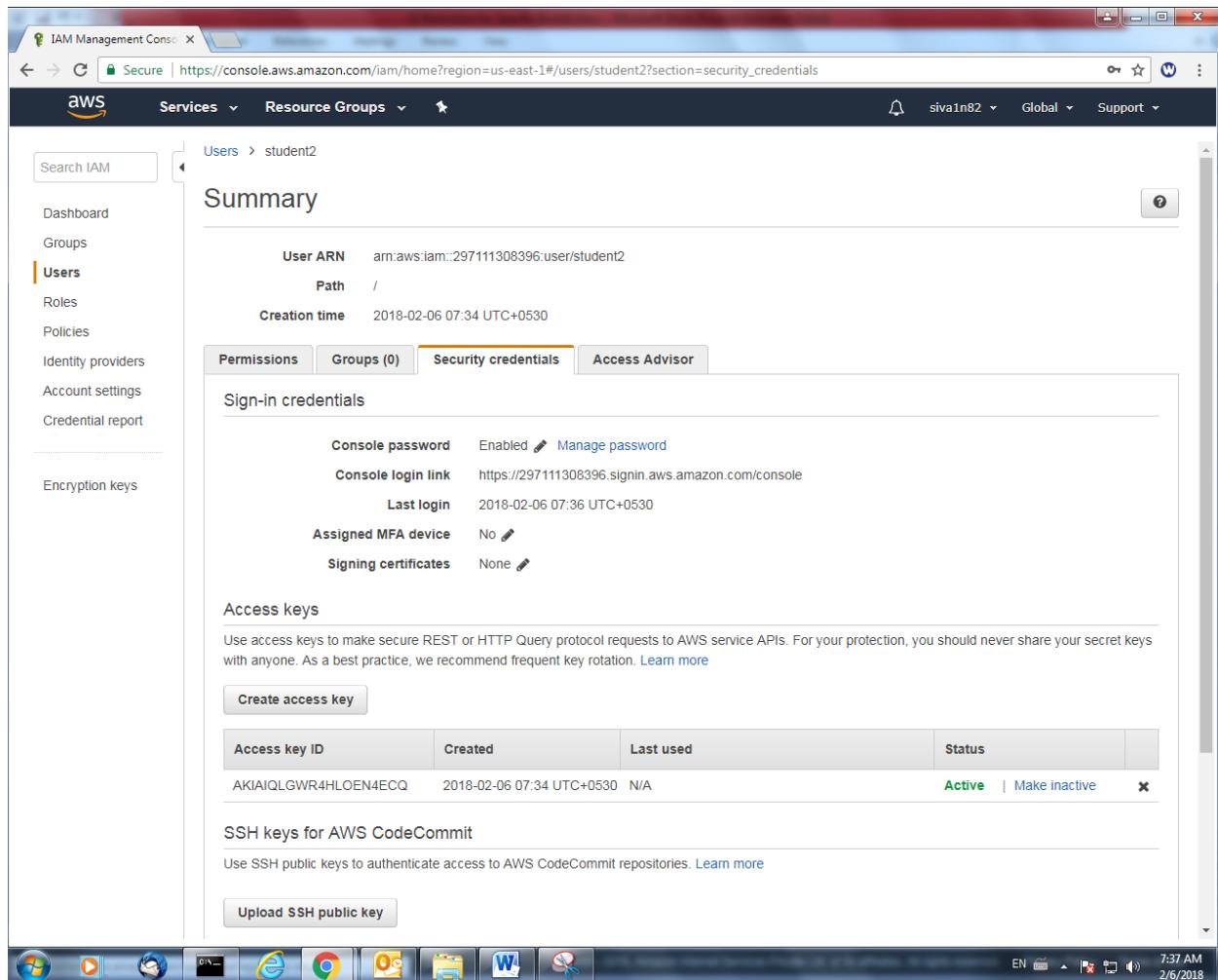
Click Users, and select student2 user.



The screenshot shows the AWS IAM Management Console interface. The left sidebar is titled "Search IAM" and contains links for Dashboard, Groups, **Users**, Roles, Policies, Identity providers, Account settings, and Credential report. The main content area has tabs for "Add user" and "Delete user". A search bar at the top says "Find users by username or access key" and displays "Showing 2 results". The user list table has columns: User name, Groups, Access key age, Password age, Last activity, and MFA. Two users are listed: "student1" and "student2".

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 collapsed, and the main area displays the 'Summary' for the user 'student2'. The 'Security credentials' tab is active, showing the following details:

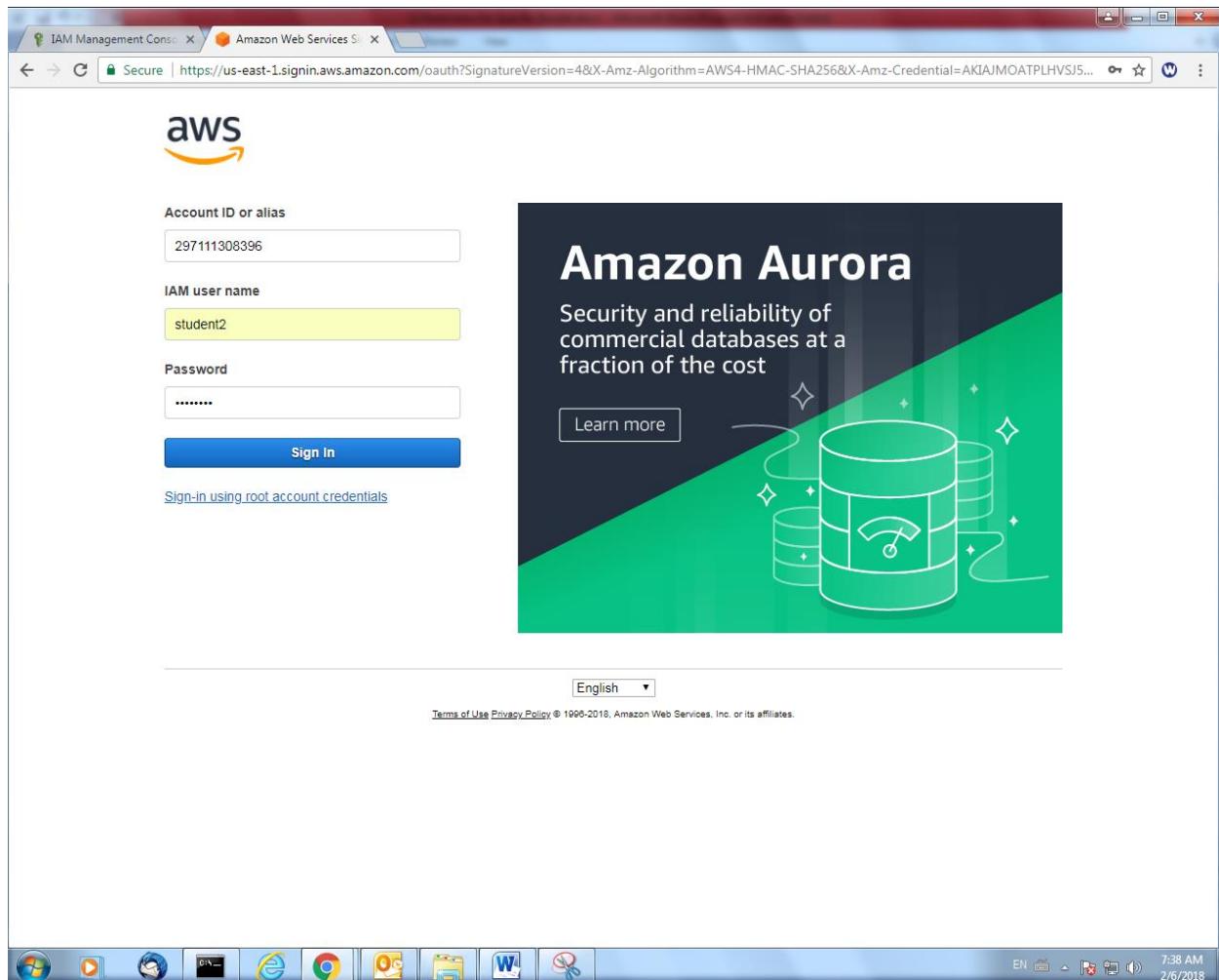
Attribute	Value
Console password	Enabled <a href="#">Manage password</a>
Console login link	<a href="https://297111308396.signin.aws.amazon.com/console">https://297111308396.signin.aws.amazon.com/console</a>
Last login	2018-02-06 07:36 UTC+0530
Assigned MFA device	No <a href="#">Edit</a>
Signing certificates	None <a href="#">Edit</a>

Below this, there is a section for 'Access keys' with a note about using them securely and a 'Create access key' button. A table shows existing access keys:

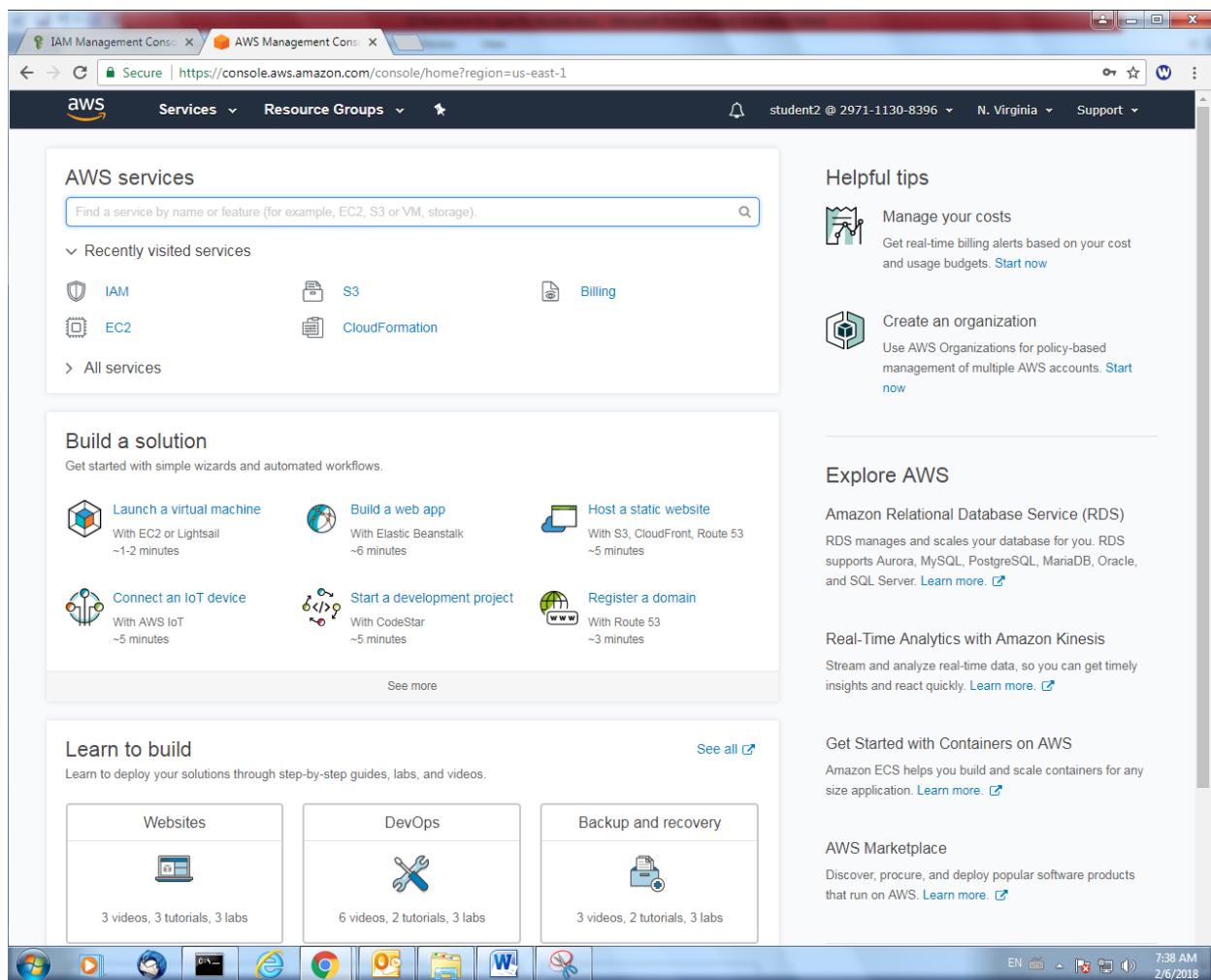
Access key ID	Created	Last used	Status
AKIAIQLGWR4HLOEN4ECQ	2018-02-06 07:34 UTC+0530	N/A	<a href="#">Active</a>   <a href="#">Make inactive</a> <a href="#">Edit</a>

Finally, there is a section for 'SSH keys for AWS CodeCommit' with a 'Upload SSH public key' button.

Type the login credentials of Student2.



Click "S3".



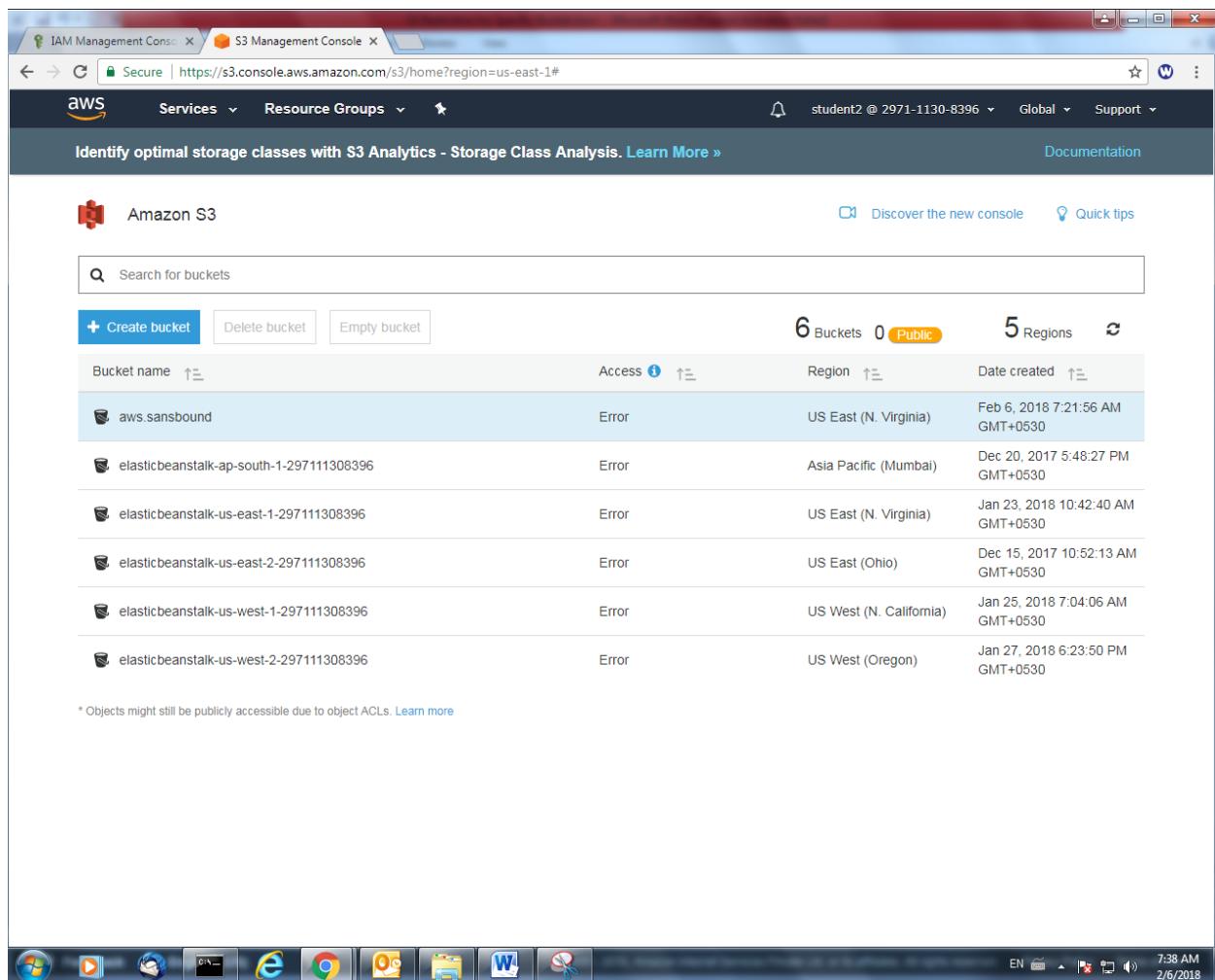
The screenshot shows the AWS Management Console homepage. The top navigation bar includes links for IAM Management Console, AWS Management Console, Services (selected), Resource Groups, and Support. The user is signed in as student2 @ 2971-1130-8396 in the N. Virginia region.

The main content area is titled "AWS services" and features a search bar. Recently visited services listed are IAM, S3, EC2, and CloudFormation. Below this is a section titled "Build a solution" with six quick-start options: Launch a virtual machine, Build a web app, Host a static website, Connect an IoT device, Start a development project, and Register a domain. Each option includes a small icon, a title, and a note about the estimated time required.

On the right side, there is a "Helpful tips" section with two items: "Manage your costs" (with a link to start real-time billing alerts) and "Create an organization" (with a link to use AWS Organizations for policy-based management). Below this is an "Explore AWS" section featuring "Amazon Relational Database Service (RDS)" and "Real-Time Analytics with Amazon Kinesis", each with a brief description and a "Learn more" link. Further down are sections for "Get Started with Containers on AWS" (Amazon ECS) and "AWS Marketplace", both with descriptions and "Learn more" links.

At the bottom, there is a toolbar with various icons for different AWS services like Lambda, CloudWatch, and S3, followed by the system tray which shows the date and time as 7:38 AM 2/6/2018.

Click “aws.sansbound” bucket.

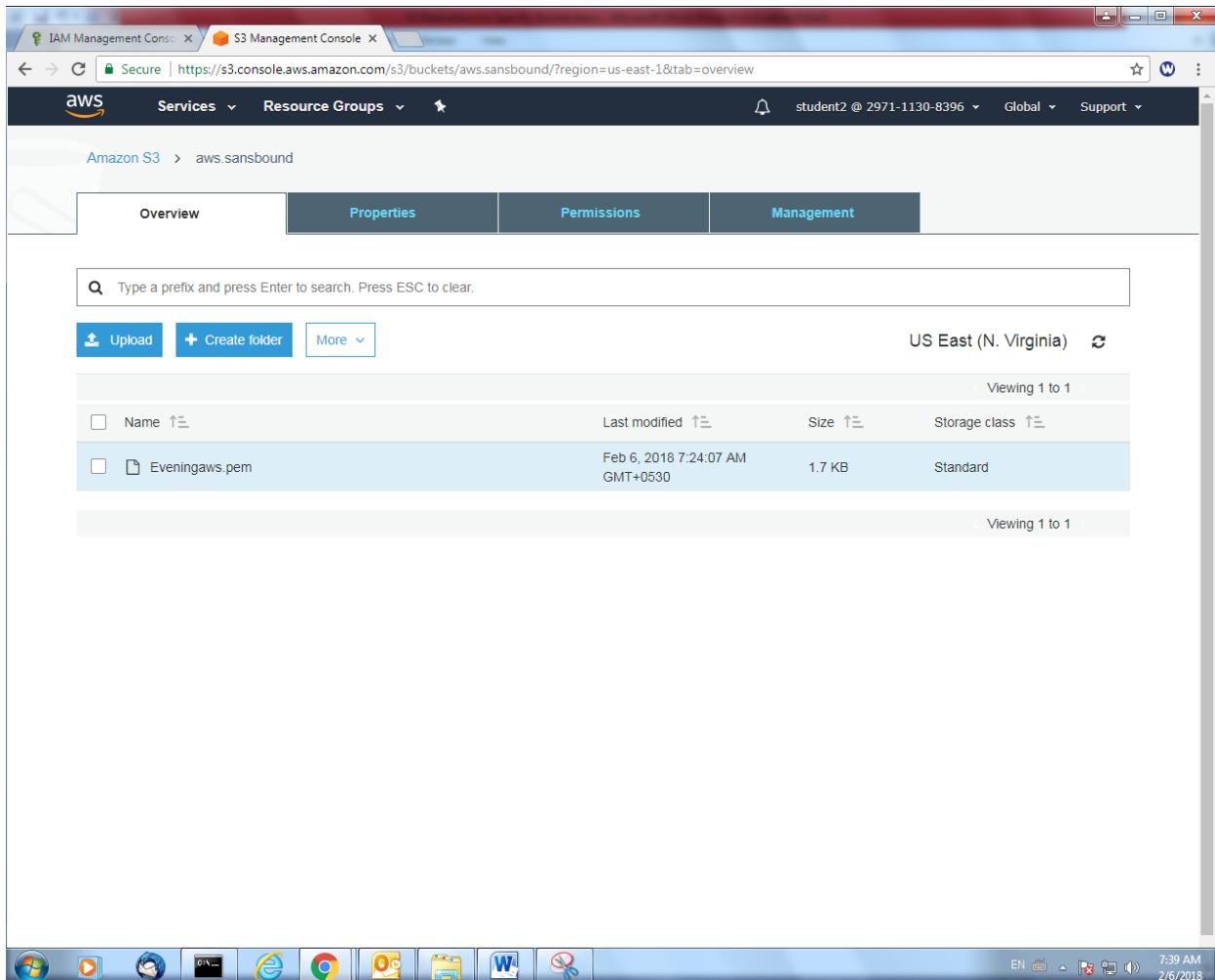


The screenshot shows the AWS S3 Management Console interface. At the top, there are tabs for IAM Management Console and S3 Management Console. The URL in the address bar is https://s3.console.aws.amazon.com/s3/home?region=us-east-1#. The header includes the AWS logo, Services dropdown, Resource Groups dropdown, a user icon for student2, and Global, Support dropdowns. Below the header, a banner says "Identify optimal storage classes with S3 Analytics - Storage Class Analysis. [Learn More »](#)" and "Documentation". The main area is titled "Amazon S3" with a "Discover the new console" link and a "Quick tips" link. A search bar says "Search for buckets". Below the search bar are three buttons: "+ Create bucket", "Delete bucket", and "Empty bucket". To the right, it shows "6 Buckets" and "0 Public" buckets, and "5 Regions". The table lists the 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

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

We can able to view the file.

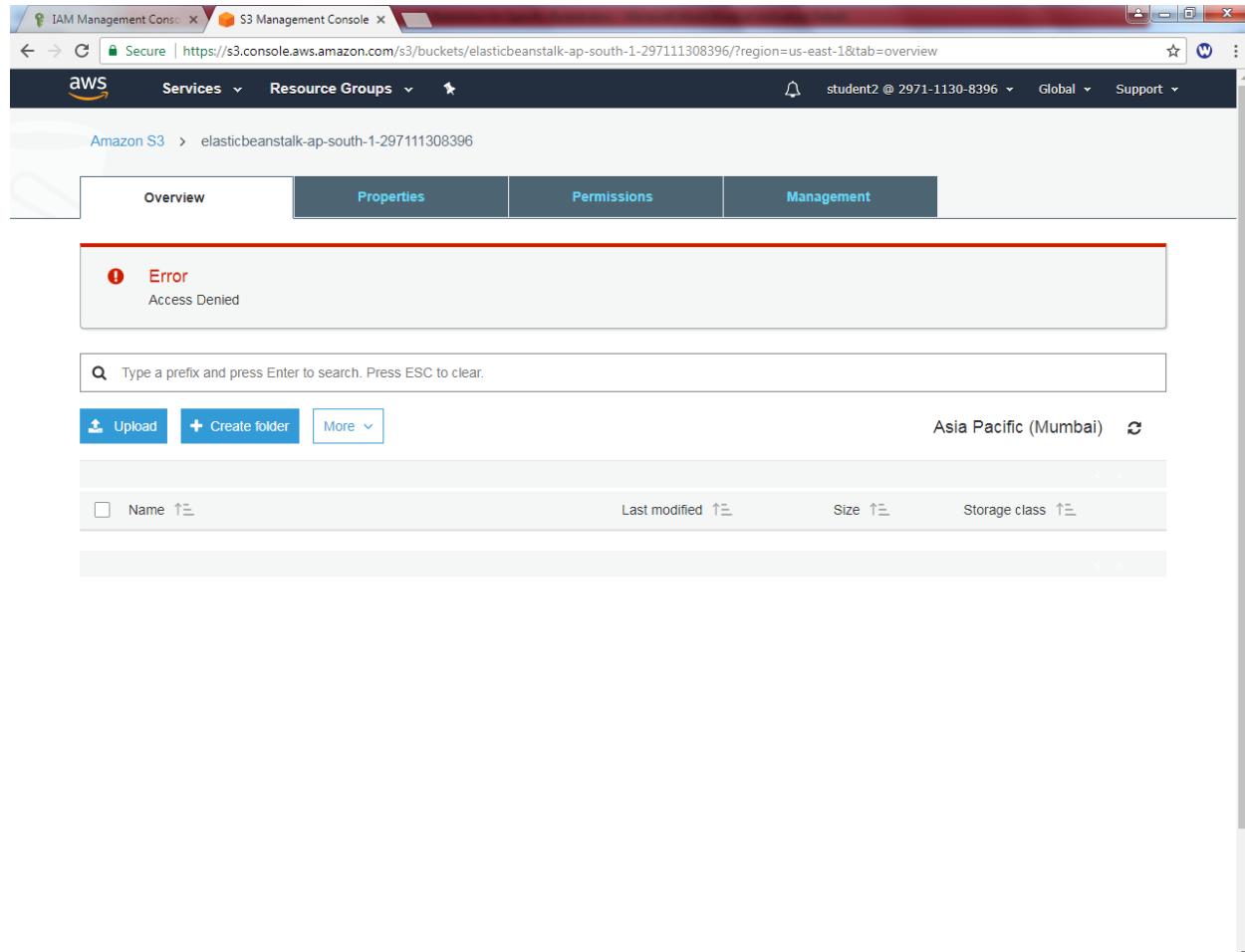


The screenshot shows the AWS S3 Management Console interface. The URL in the address bar is <https://s3.console.aws.amazon.com/s3/buckets/aws.sansbound/?region=us-east-1&tab=overview>. The navigation bar includes 'Services' (selected), 'Resource Groups', and 'Global'. The user 'student2 @ 2971-1130-8396' is logged in. The main area shows the 'Overview' tab selected for 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 are buttons for 'Upload', '+ Create folder', and 'More'. The file list table has columns: Name, Last modified, Size, and Storage class. One file is listed:

Name	Last modified	Size	Storage class
Eveningaws.pem	Feb 6, 2018 7:24:07 AM GMT+0530	1.7 KB	Standard

At the bottom, there's a taskbar with various icons and system status information: EN, 7:39 AM, 2/6/2018.

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.



The screenshot shows the AWS S3 Management Console interface. The URL in the browser is <https://s3.console.aws.amazon.com/s3/buckets/elasticbeanstalk-ap-south-1-297111308396/?region=us-east-1&tab=overview>. The user is signed in as "student2 @ 2971-1130-8396". The navigation bar includes "Services", "Resource Groups", and "Global". The main content area shows the "Overview" tab selected for the bucket "elasticbeanstalk-ap-south-1-297111308396". A prominent red error message box displays an exclamation mark icon and the text "Error" followed by "Access Denied". Below the error message is a search bar with the placeholder "Type a prefix and press Enter to search. Press ESC to clear.". At the bottom of the screen, there are buttons for "Upload", "Create folder", and "More", along with a location indicator "Asia Pacific (Mumbai)" and a refresh icon.