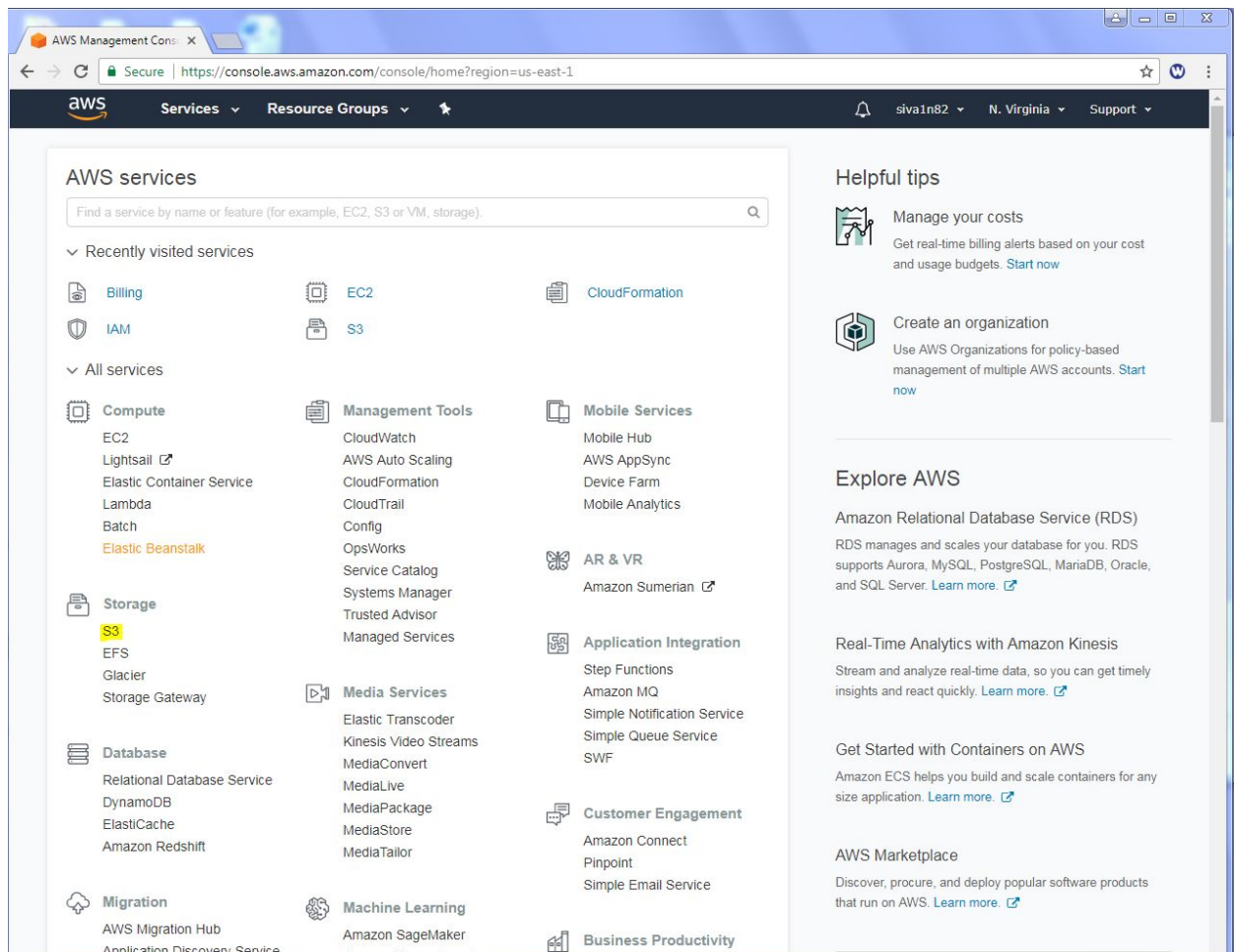


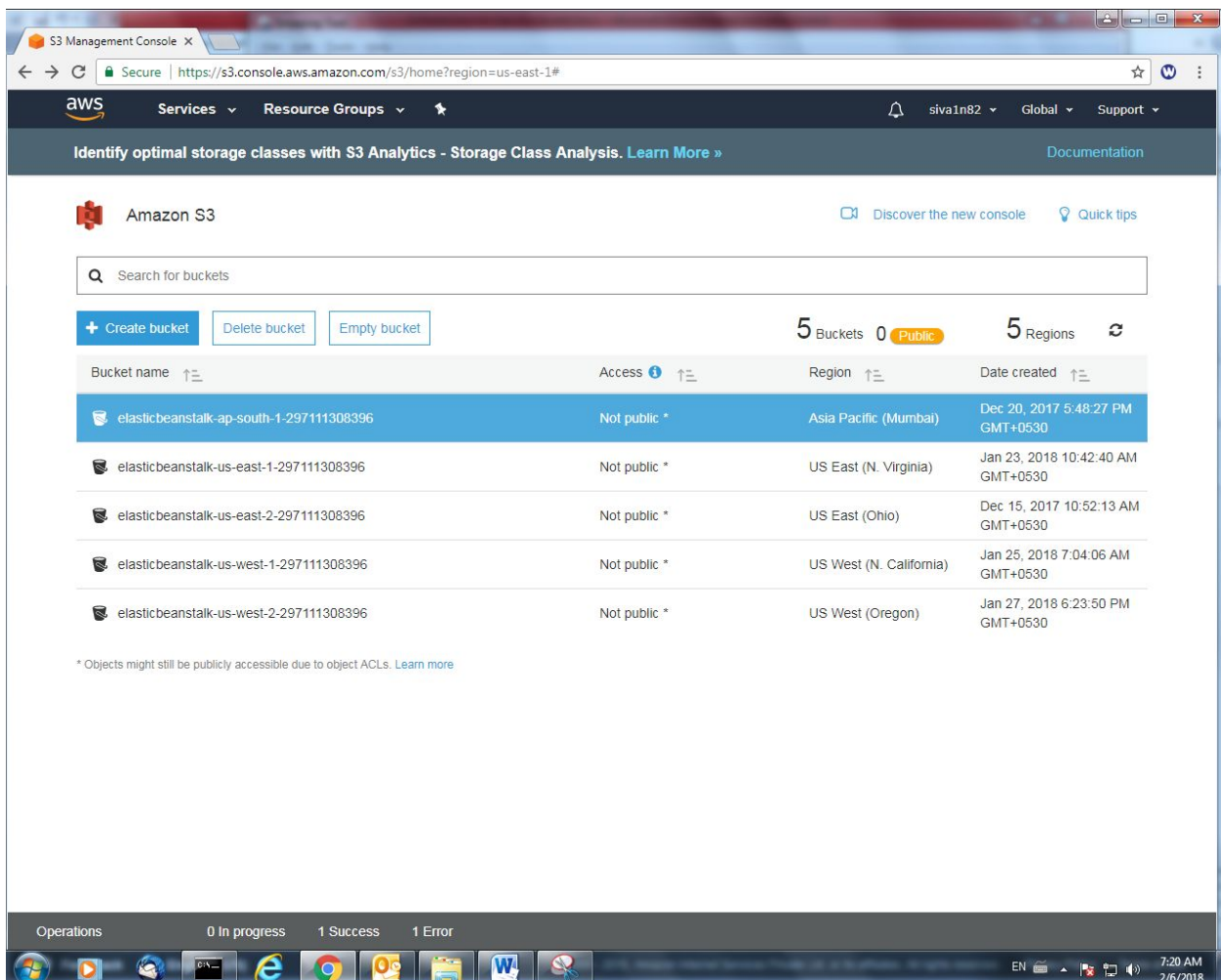
Lab24

S3 Restriction for Specific Bucket

Click “S3” service



Click “Create bucket” with unique name.



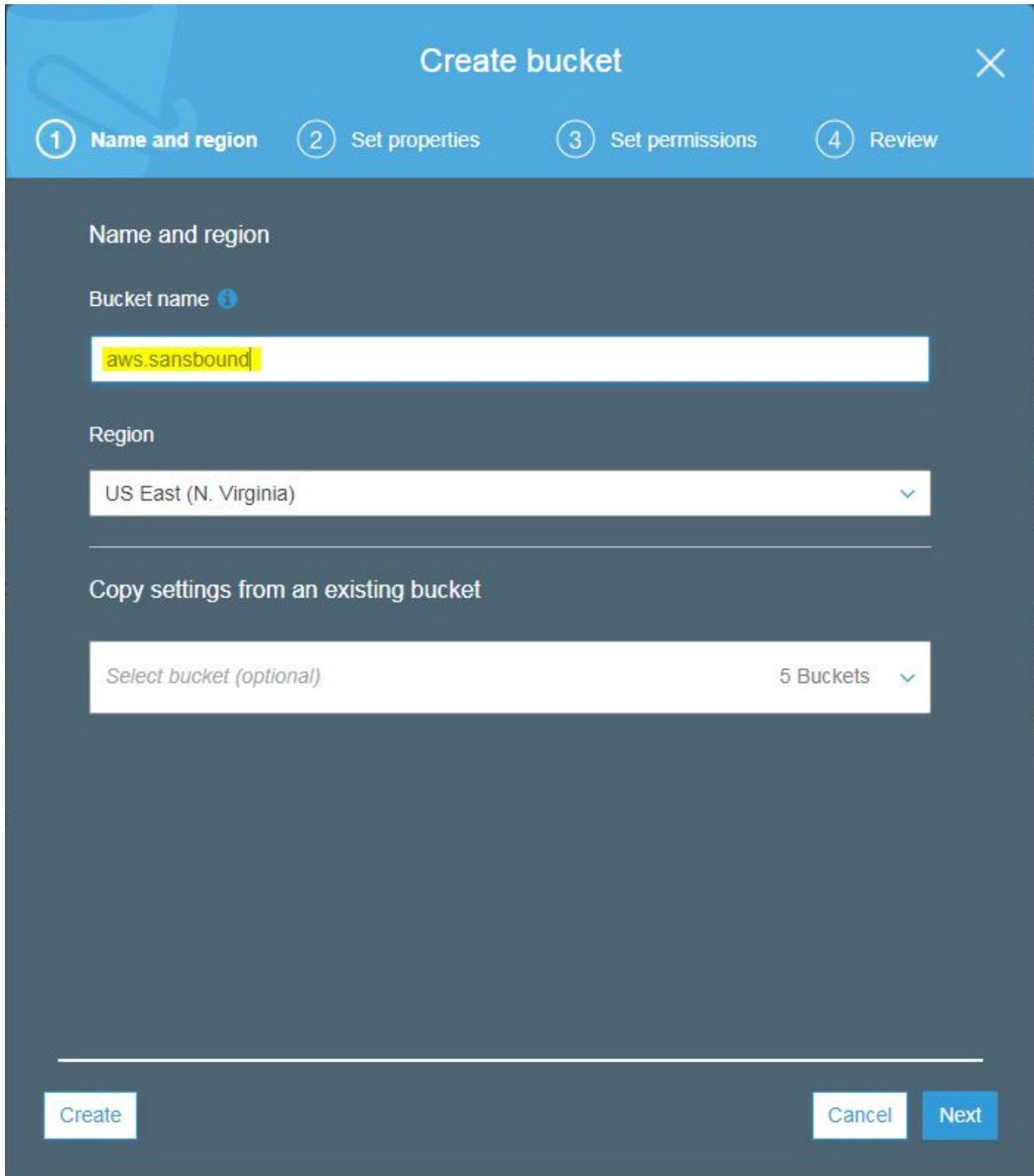
The screenshot shows the AWS S3 Management Console interface. At the top, there's a navigation bar with the AWS logo, 'Services', 'Resource Groups', and user information. Below this is a banner for 'Identify optimal storage classes with S3 Analytics - Storage Class Analysis'. The main content area is titled 'Amazon S3' and includes a search bar and buttons for 'Create bucket', 'Delete bucket', and 'Empty bucket'. A summary shows '5 Buckets', '0 Public', and '5 Regions'. A table lists the buckets with columns for 'Bucket name', 'Access', 'Region', and 'Date created'.

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](#)

Operations: 0 In progress, 1 Success, 1 Error

Type `aws.sansbound.com`



The screenshot shows the 'Create bucket' wizard in the AWS Management Console. The title bar is blue with a close button (X) in the top right. Below the title bar is a progress bar with four steps: 1. Name and region (active), 2. Set properties, 3. Set permissions, and 4. Review. The main content area is dark blue. It has a section 'Name and region' with a 'Bucket name' label and a text input field containing 'aws.sansbound'. Below this is a 'Region' label and a dropdown menu showing 'US East (N. Virginia)'. Further down is a section 'Copy settings from an existing bucket' with a text input field containing 'Select bucket (optional)' and a dropdown menu showing '5 Buckets'. At the bottom, there are three buttons: 'Create' (white with blue text), 'Cancel' (white with blue text), and 'Next' (blue with white text).

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)

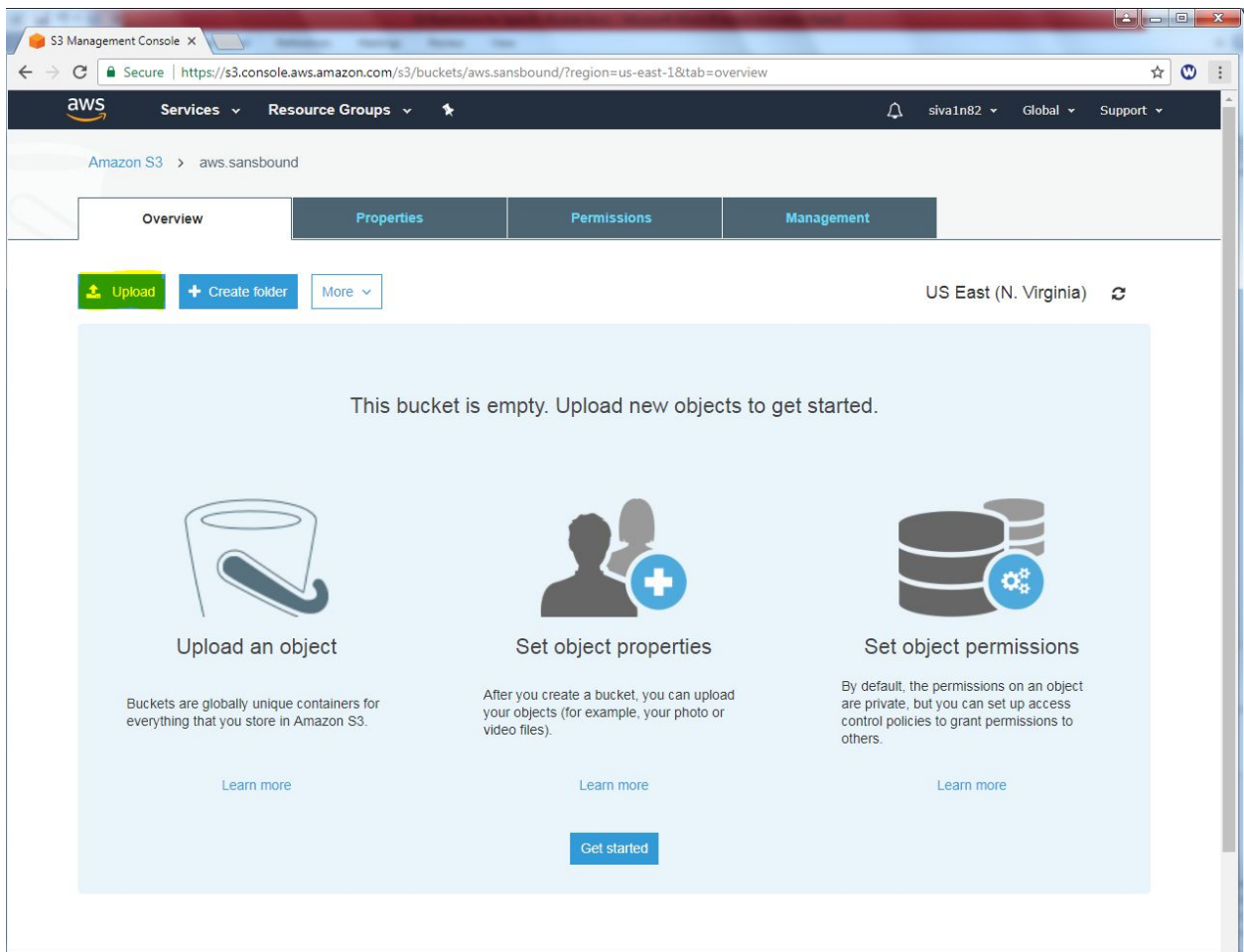
Copy settings from an existing bucket

Select bucket (optional) 5 Buckets

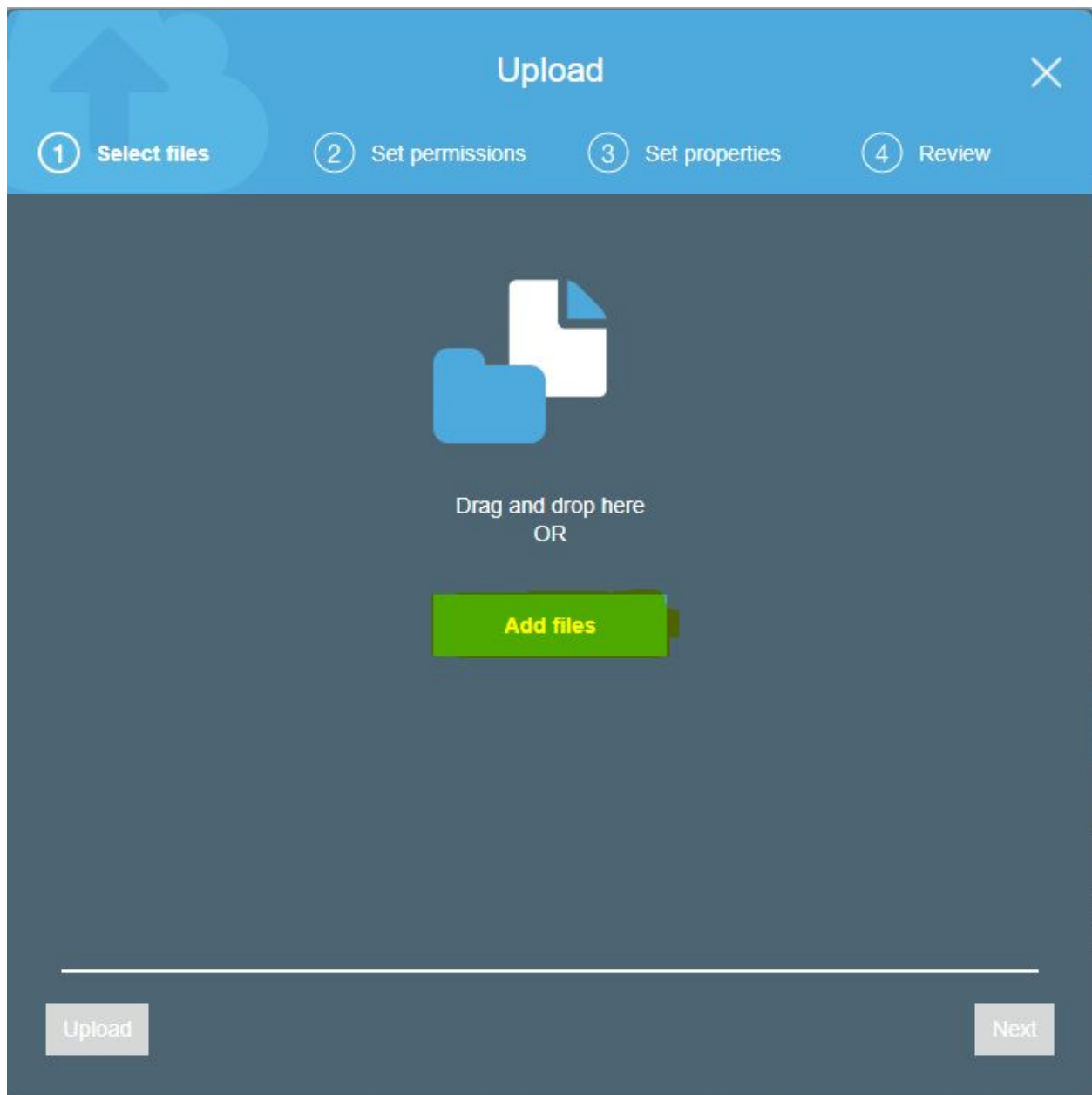
Create Cancel Next

Click "Create".

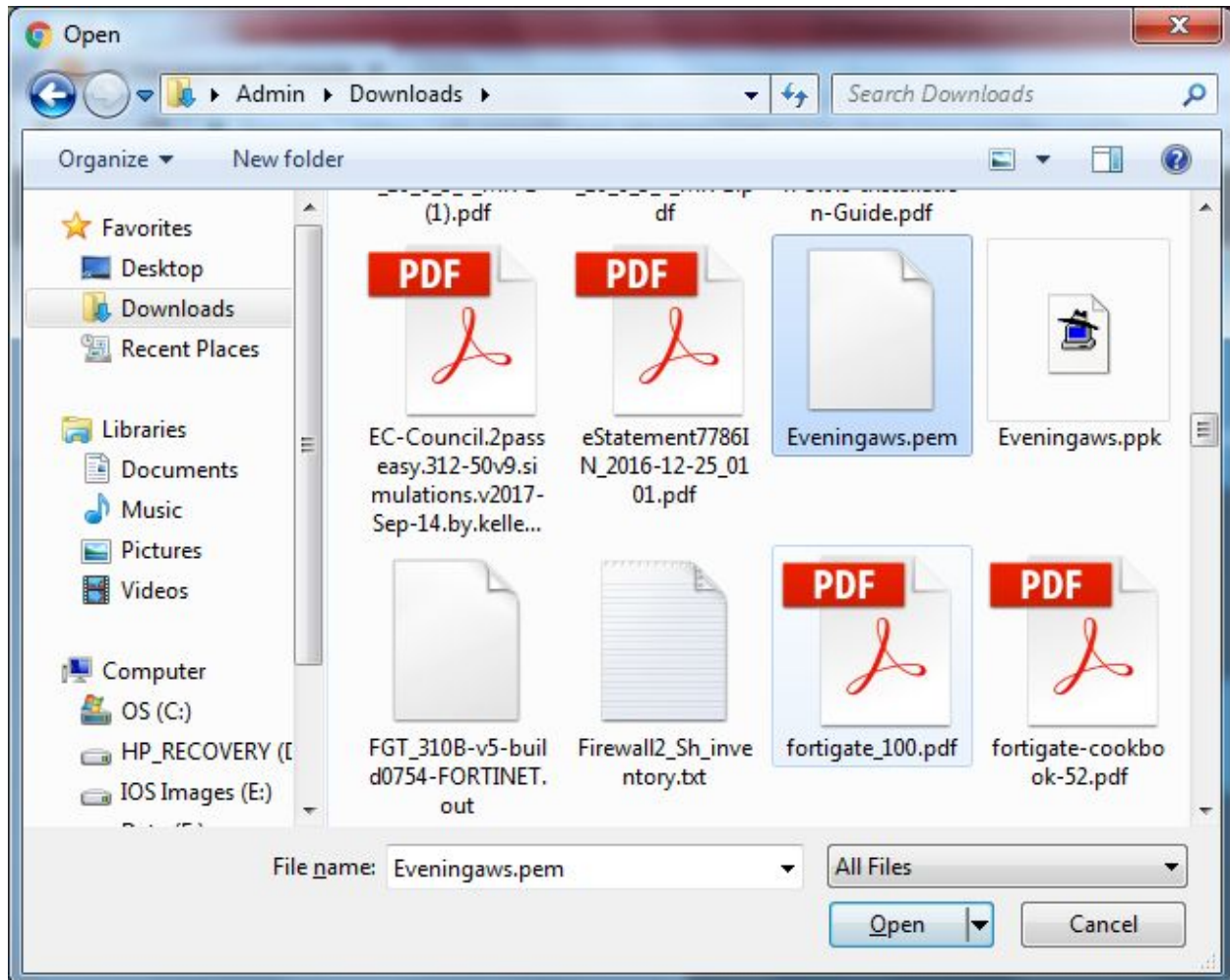
Click “Upload”.



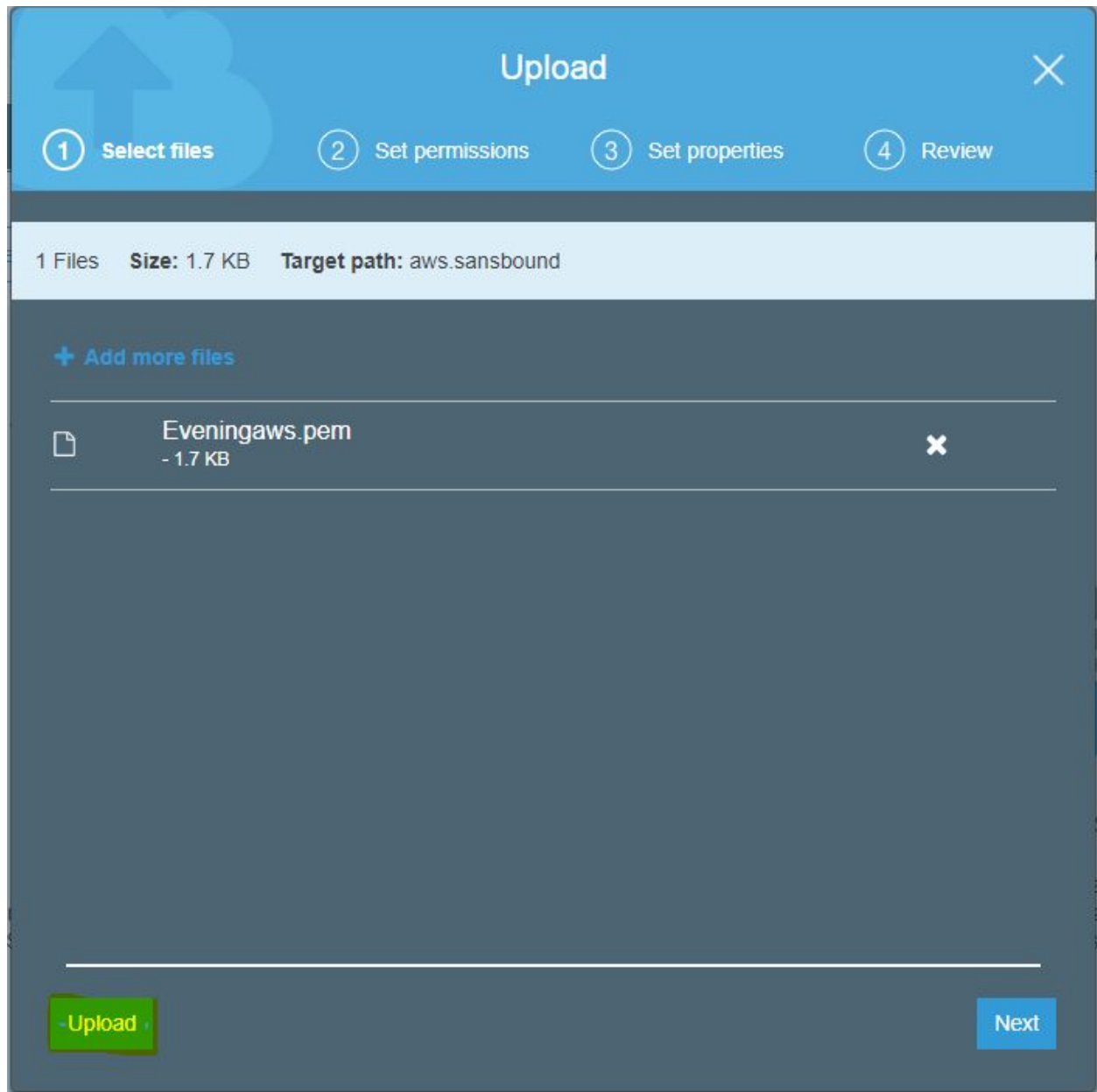
Click “Add files”.



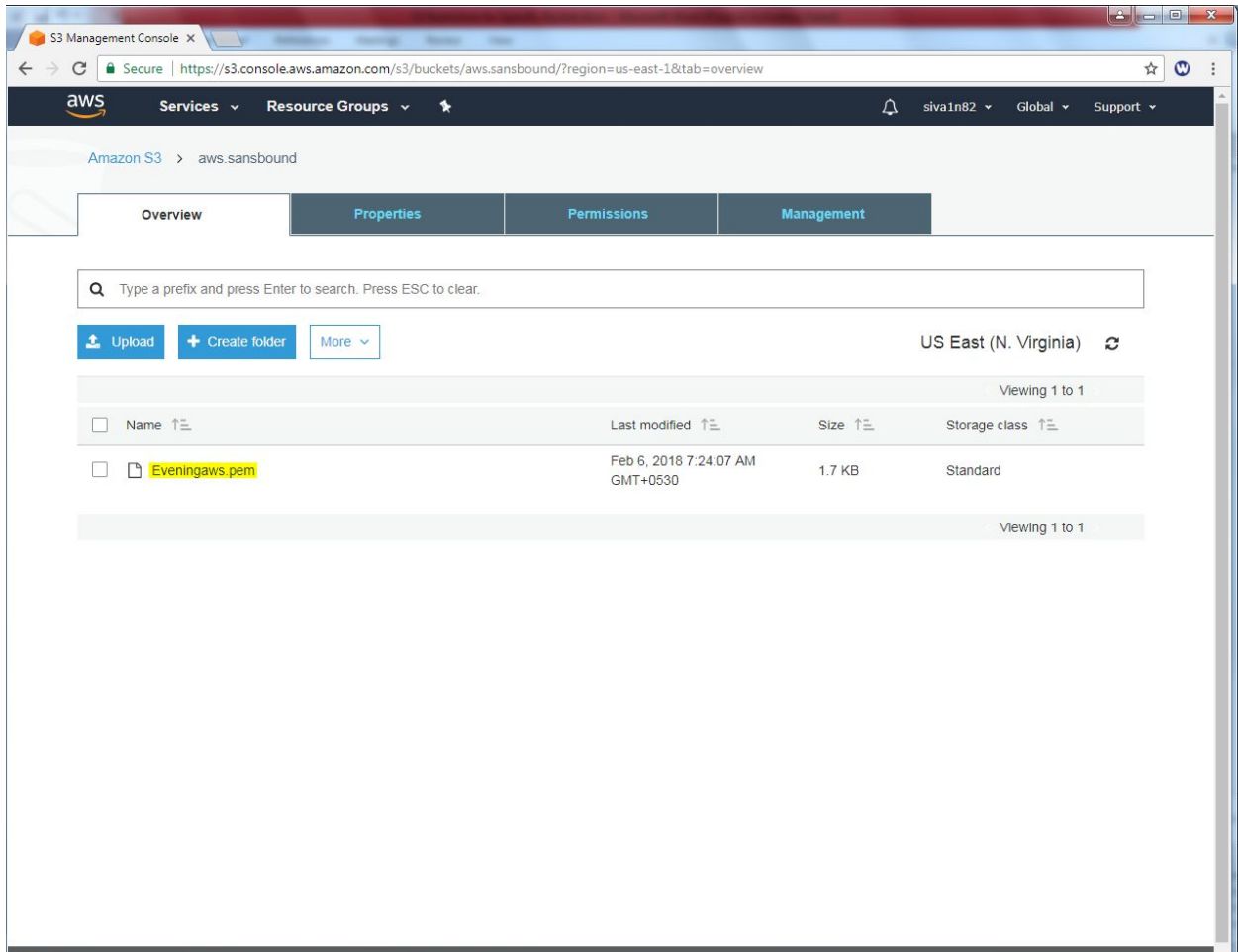
Locate the file and click open.



Click “Upload” to upload the file.



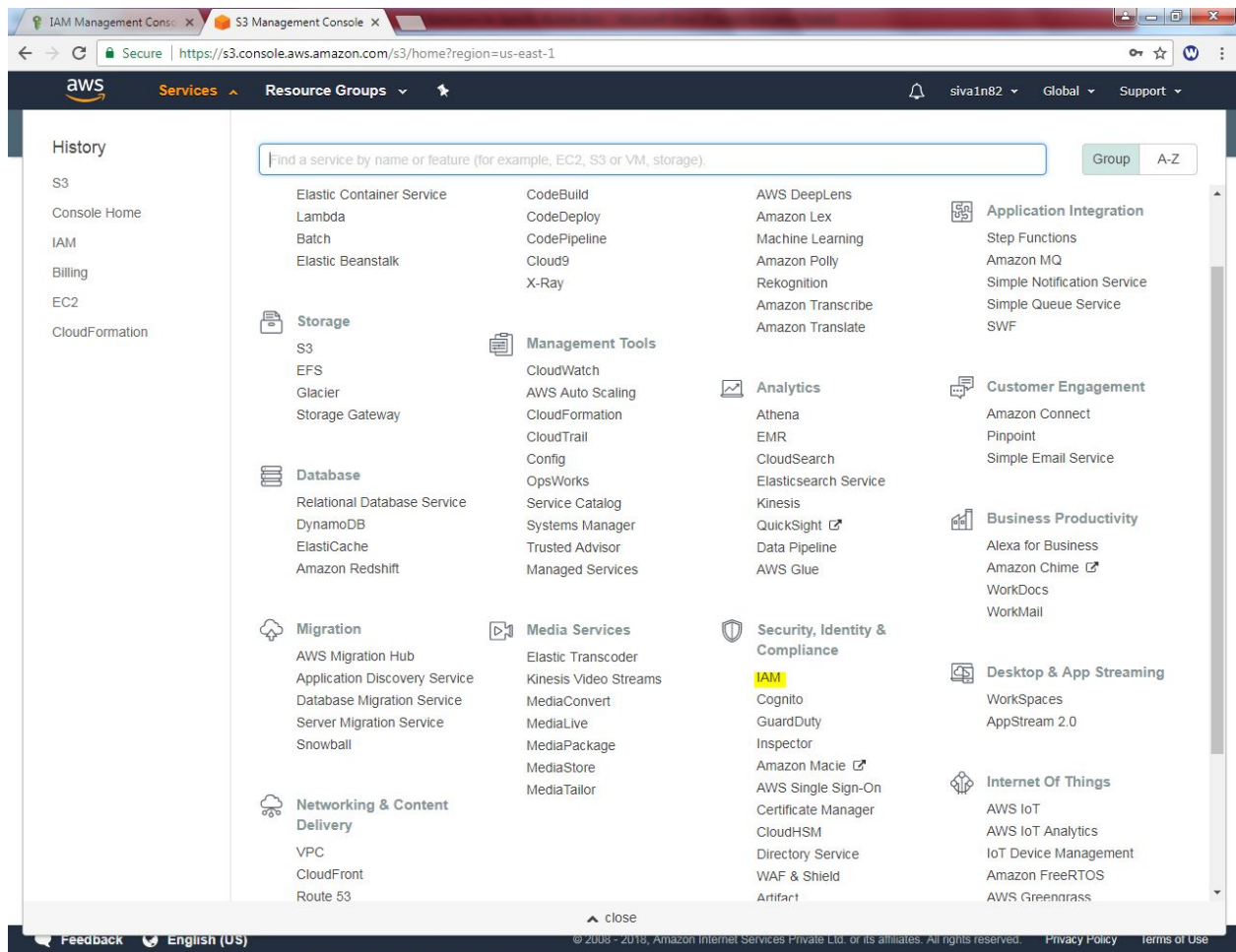
We can able view the file.



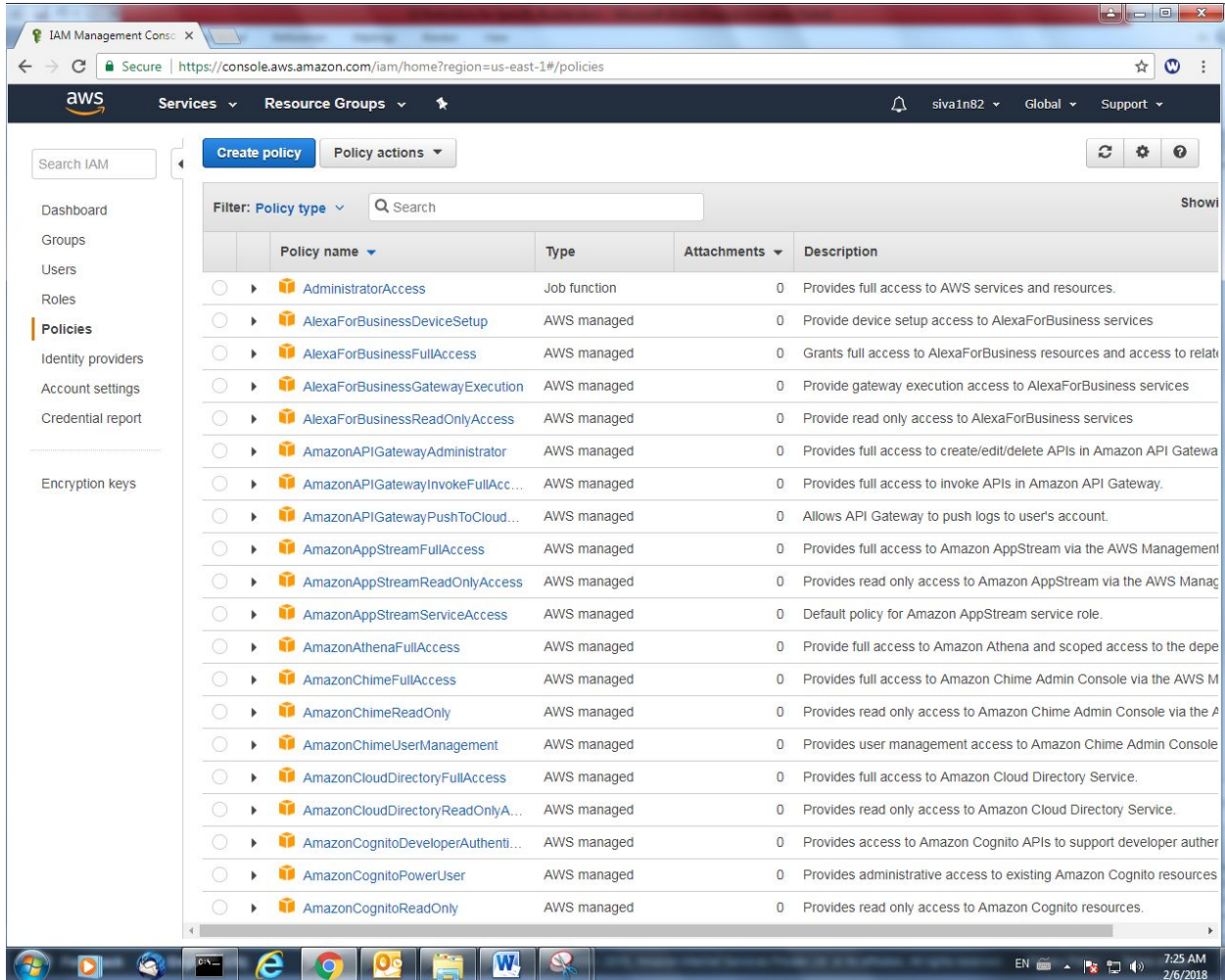
The screenshot displays the AWS S3 Management Console interface. The browser address bar shows the URL: <https://s3.console.aws.amazon.com/s3/buckets/aws.sansbound/?region=us-east-1&tab=overview>. The console header includes the AWS logo, navigation tabs for Services, Resource Groups, and a user profile for 'siva1n82'. The breadcrumb trail indicates the current location is 'Amazon S3 > aws.sansbound'. Below the breadcrumb, there are four tabs: Overview (selected), Properties, Permissions, and Management. A search bar is present with the placeholder text 'Type a prefix and press Enter to search. Press ESC to clear.' Below the search bar, there are three buttons: 'Upload', 'Create folder', and 'More'. The region is set to 'US East (N. Virginia)'. A table lists the contents of the bucket, showing one file named 'Eveningaws.pem'. The table has columns for Name, Last modified, Size, and Storage class. The file 'Eveningaws.pem' was last modified on 'Feb 6, 2018 7:24:07 AM GMT+0530', has a size of '1.7 KB', and is stored in 'Standard' storage class. The table also indicates 'Viewing 1 to 1'.

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

Click "IAM" Role.



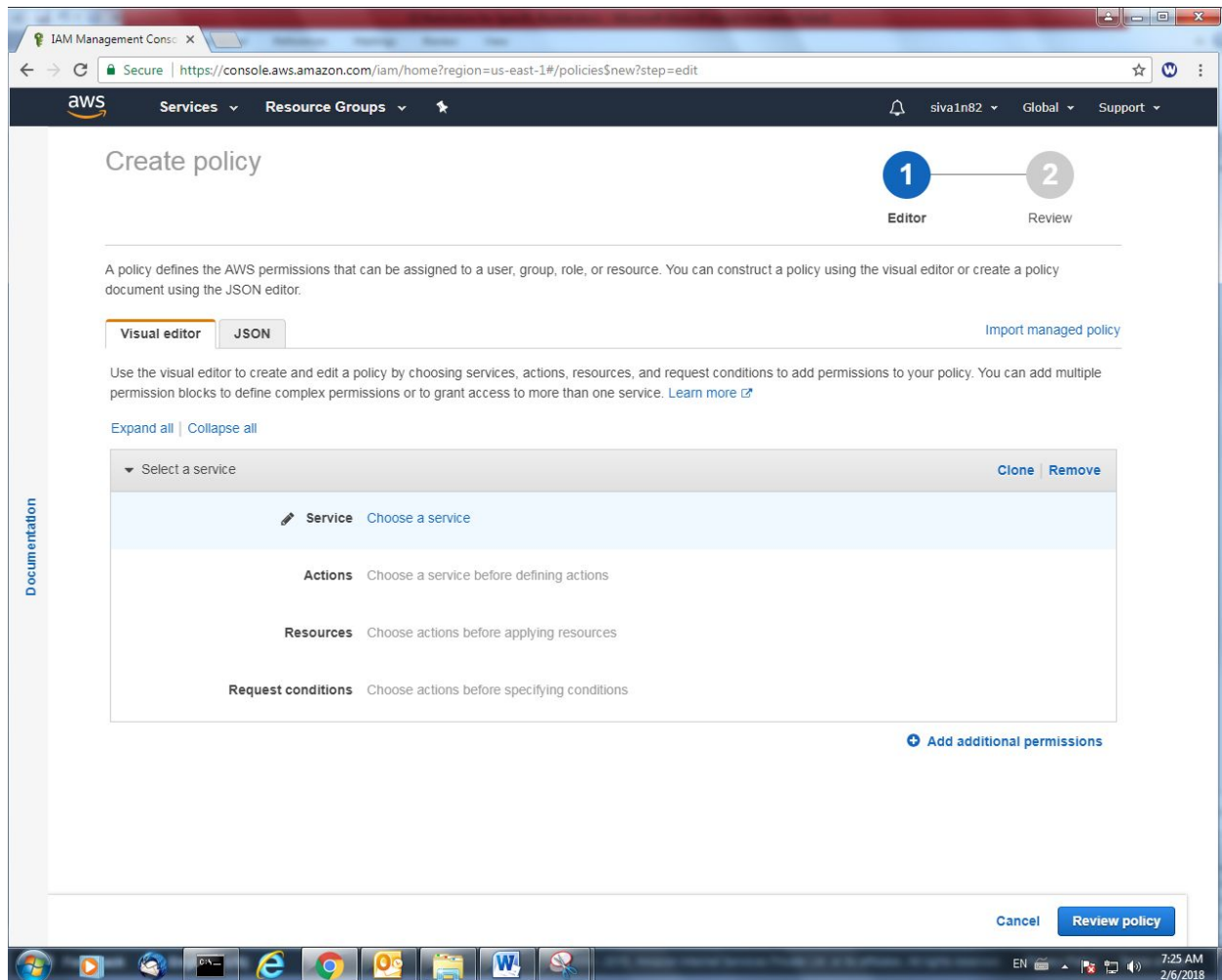
Click “Create Policy”.



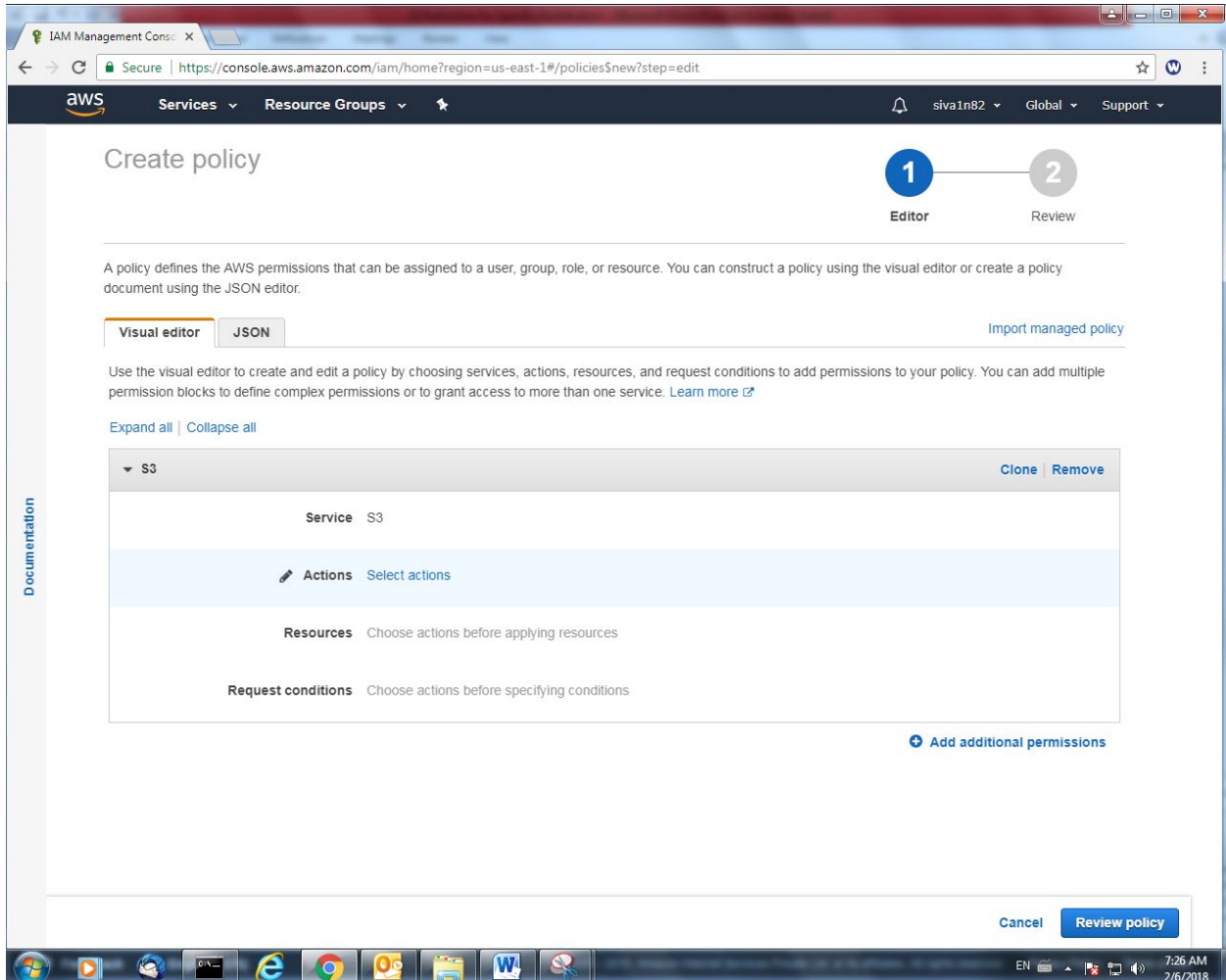
The screenshot shows the AWS IAM Management Console interface. The top navigation bar includes the 'Create policy' button. The left sidebar contains navigation links for Dashboard, Groups, Users, Roles, Policies (selected), Identity providers, Account settings, Credential report, and Encryption keys. The main content area displays a list of AWS managed policies.

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 dependent services
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
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.
AmazonCognitoDeveloperAuthenticator	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

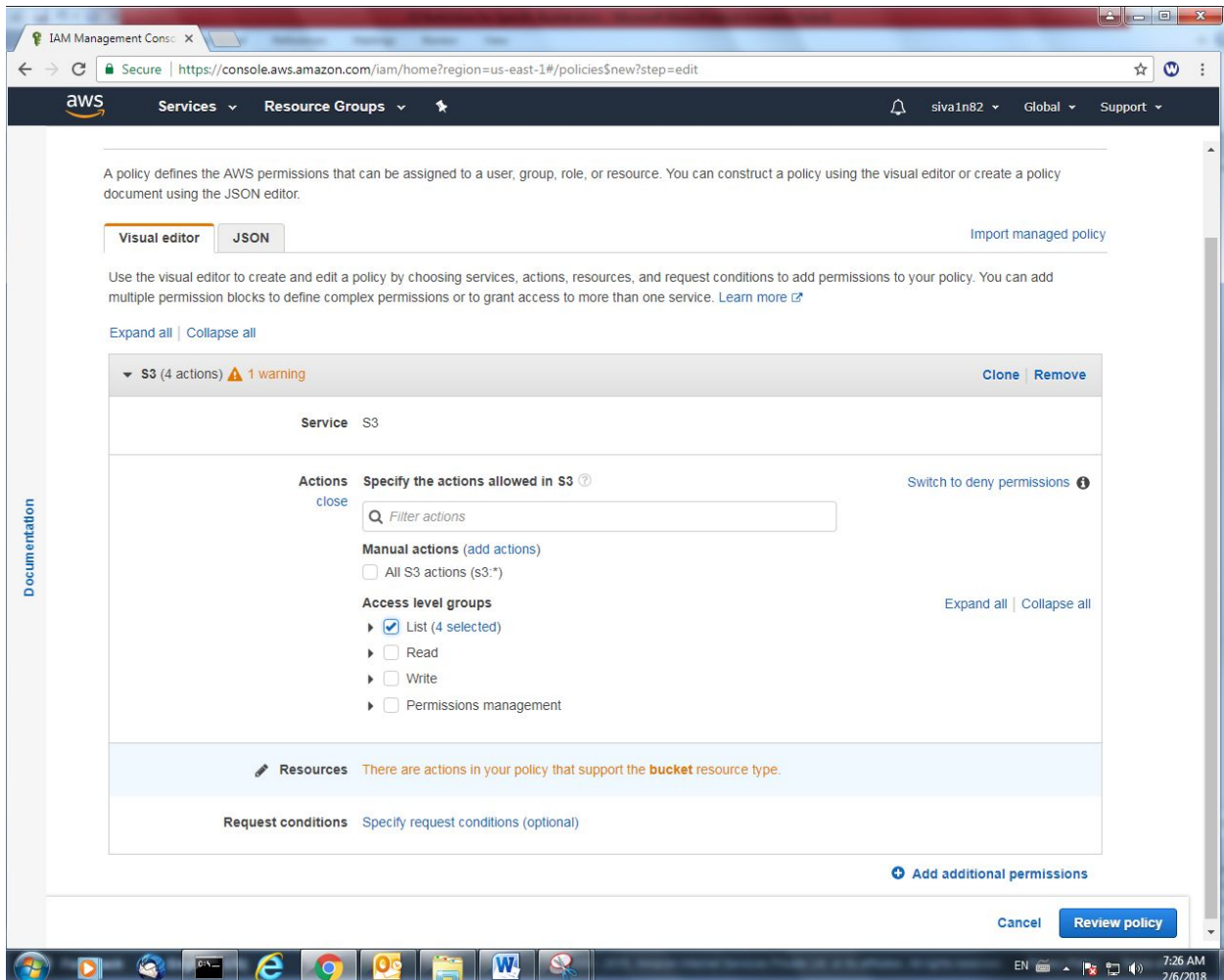


choose the S3 service and click Select actions.



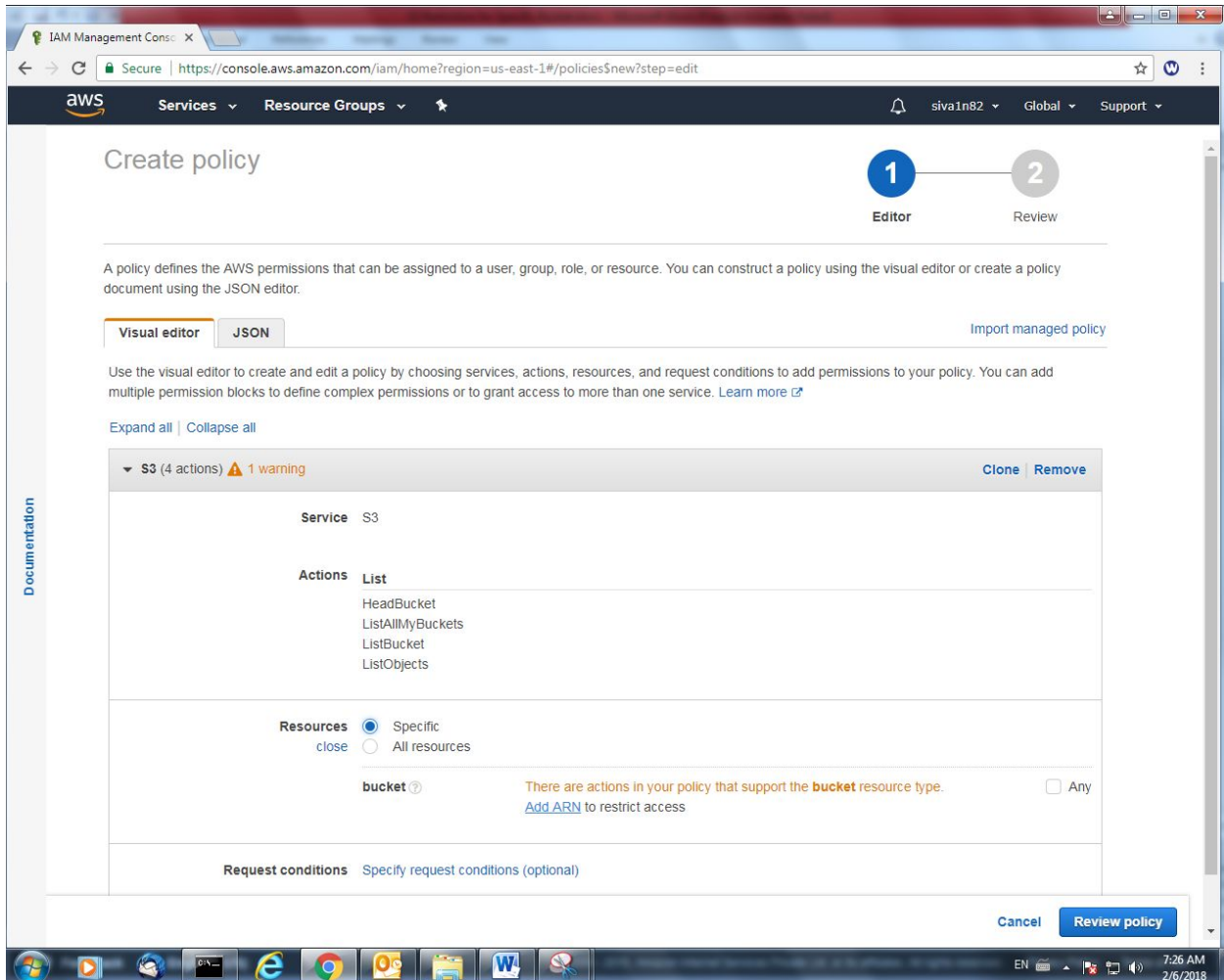
The screenshot shows the AWS IAM console's 'Create policy' page. The browser address bar indicates the URL: [https://console.aws.amazon.com/iam/home?region=us-east-1#/policies\\$new?step=edit](https://console.aws.amazon.com/iam/home?region=us-east-1#/policies$new?step=edit). The page has a dark blue header with the AWS logo, 'Services', 'Resource Groups', and user information 'siva1n82'. A progress bar at the top right shows two steps: '1 Editor' (active) and '2 Review'. Below the header, the 'Create policy' title is followed by a description: '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.' There are two tabs: 'Visual editor' (selected) and 'JSON'. A link 'Import managed policy' is on the right. The 'Visual editor' section contains instructions and links like 'Expand all' and 'Collapse all'. A table-like structure shows the policy configuration: 'Service' is 'S3', 'Actions' is 'Select actions' (with a pencil icon), 'Resources' is 'Choose actions before applying resources', and 'Request conditions' is 'Choose actions before specifying conditions'. There are 'Clone' and 'Remove' links for the S3 service. At the bottom right, there are 'Cancel' and 'Review policy' buttons. The Windows taskbar at the bottom shows various application icons and the system clock '7:26 AM 2/6/2018'.

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's Visual editor for a policy. The policy is named "S3 (4 actions)" and has a warning icon. The "Actions" section is expanded, showing a search bar and a list of actions. The "Access level groups" section is also expanded, showing a list of groups with "List (4 selected)" checked. The "Resources" section shows a message: "There are actions in your policy that support the bucket resource type." The "Request conditions" section is empty. The "Add additional permissions" button is at the bottom right.

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



The screenshot shows the AWS IAM Management Console interface for creating a new policy. The 'Visual editor' tab is active, showing a policy for the S3 service. The actions listed are List, HeadBucket, ListAllMyBuckets, ListBucket, and ListObjects. The resources are set to 'Specific' and a 'bucket' resource type is selected. A warning message indicates that the actions support the 'bucket' resource type and that an ARN should be added to restrict access. The 'Request conditions' section is set to 'Specify request conditions (optional)'. The page has a progress bar at the top with steps 1 (Editor) and 2 (Review). The bottom of the page shows a Windows taskbar with various application icons and a system clock showing 7:26 AM on 2/6/2018.

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

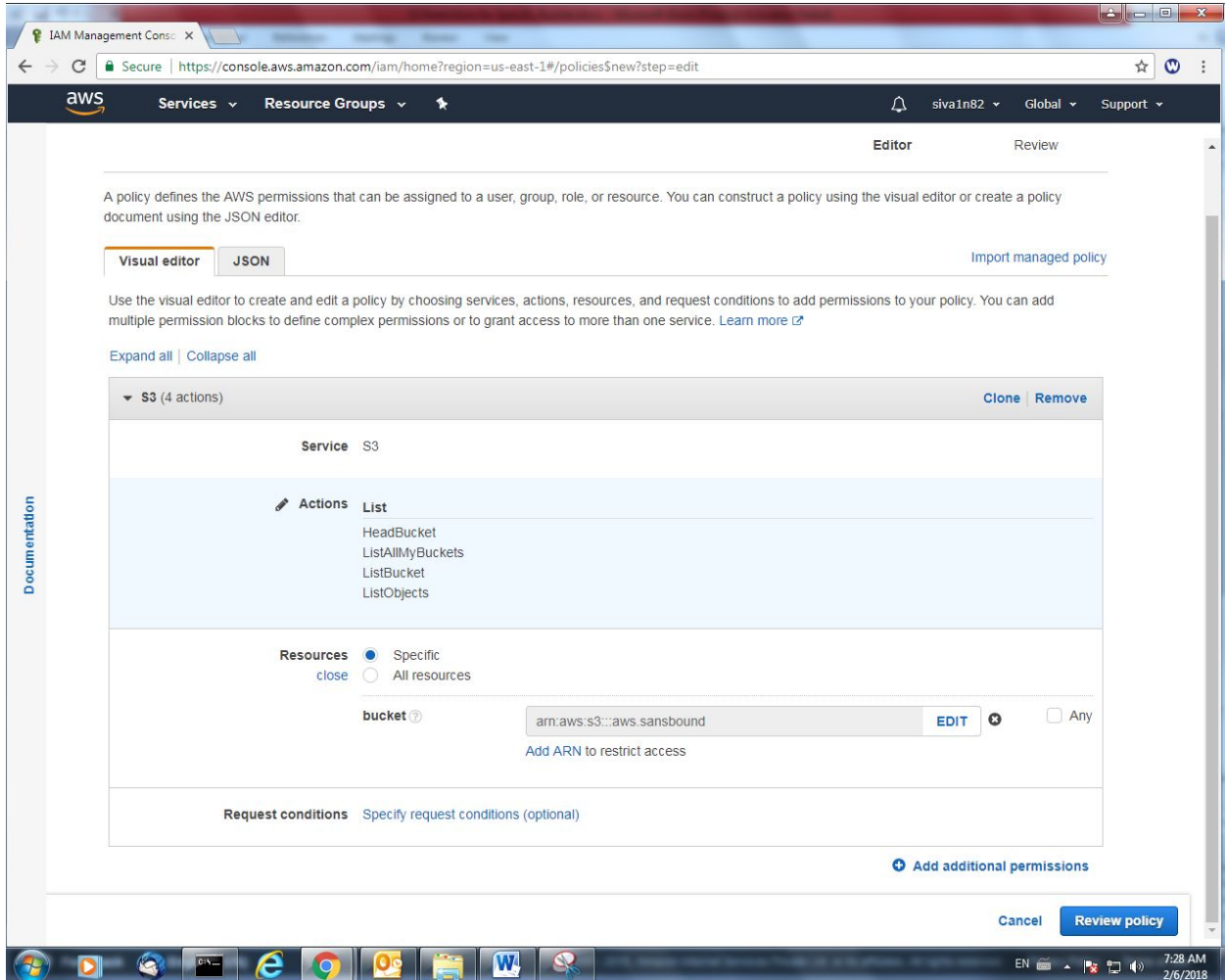
aws.sansbound

☐ Any

Cancel

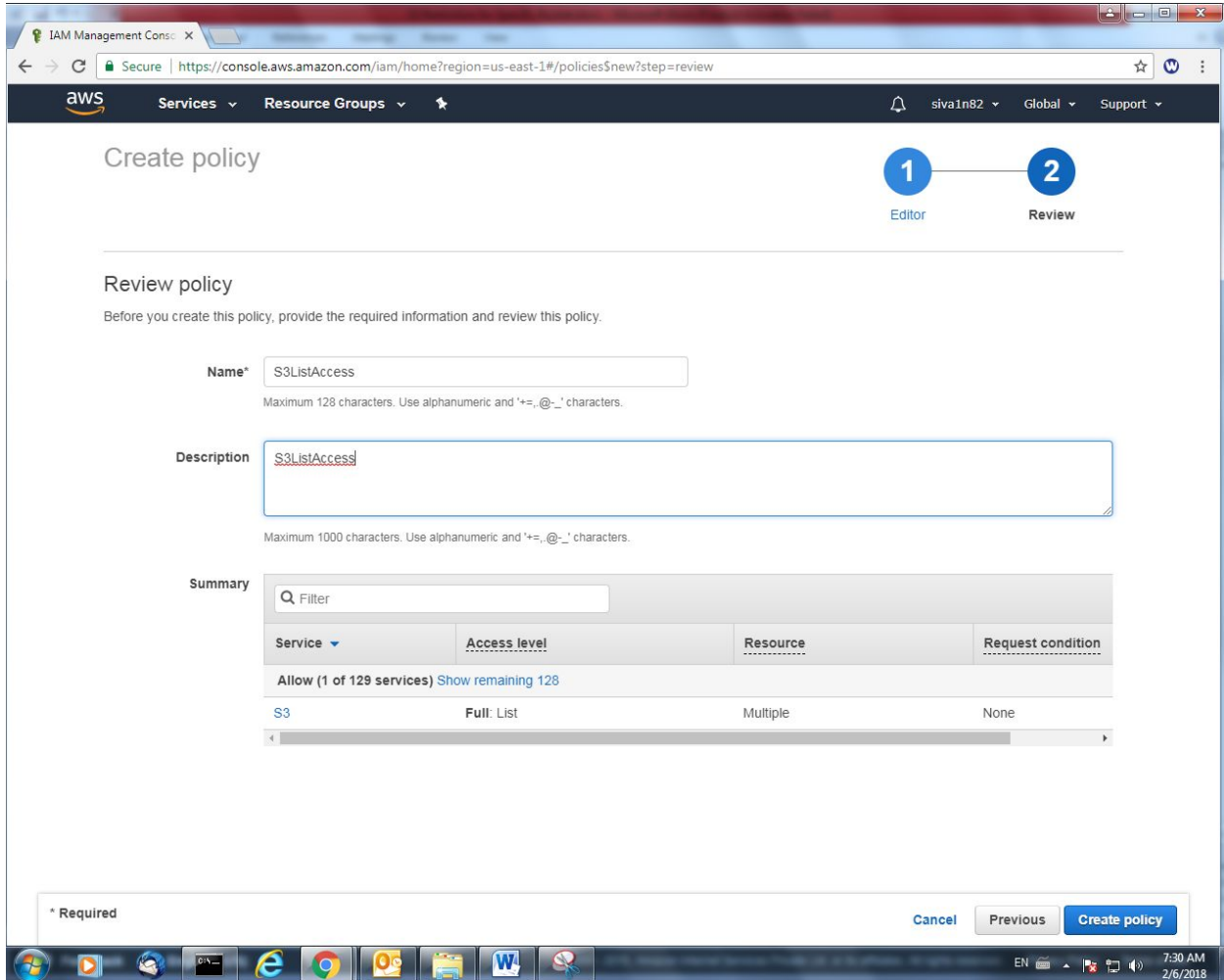
Add

Click “Review Policy”.



The screenshot shows the AWS IAM console's Visual editor for creating a policy. The interface is in the 'Editor' mode, with a 'Review' tab also visible. A sidebar on the left is labeled 'Documentation'. The main content area explains that a policy defines AWS permissions and offers two editors: 'Visual editor' (selected) and 'JSON'. Below this, instructions guide the user on how to use the visual editor to create and edit a policy by choosing services, actions, resources, and request conditions. A link 'Learn more' is provided. The 'Expand all' and 'Collapse all' options are visible. The policy configuration is shown for 'S3 (4 actions)'. The 'Service' is set to 'S3'. The 'Actions' list includes 'List', 'HeadBucket', 'ListAllMyBuckets', 'ListBucket', and 'ListObjects'. The 'Resources' section is set to 'Specific' (selected) instead of 'All resources'. The resource is specified as 'arn:aws:s3:::aws.sansbound'. There is an 'EDIT' button and a checkbox for 'Any'. A link 'Add ARN to restrict access' is also present. The 'Request conditions' section is set to 'Specify request conditions (optional)'. At the bottom right, there are 'Cancel' and 'Review policy' buttons. The bottom of the screen shows a Windows taskbar with various application icons and a system clock indicating 7:28 AM on 2/6/2018.

Type Name of Policy and Description.



The screenshot shows the AWS IAM console 'Create policy' page in the 'Review' step. The browser address bar shows the URL: [https://console.aws.amazon.com/iam/home?region=us-east-1#/policies\\$new?step=review](https://console.aws.amazon.com/iam/home?region=us-east-1#/policies$new?step=review). The page has a progress bar with two steps: '1 Editor' and '2 Review', with '2 Review' being the active step.

Create policy

Review policy

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

Name*

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

Description

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

Summary

Q Filter

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

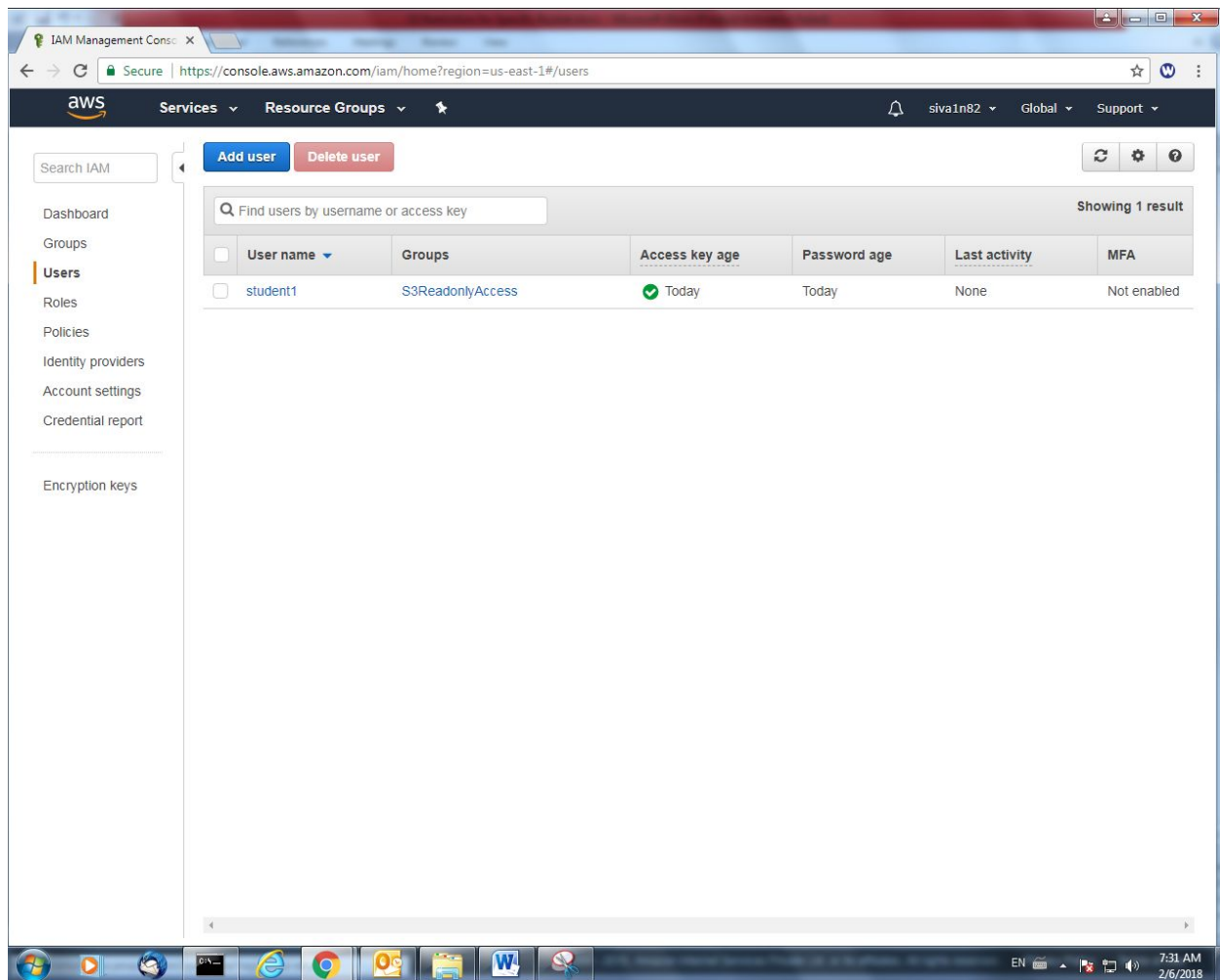
* Required

[Cancel](#) [Previous](#) [Create policy](#)

Click "Create Policy".

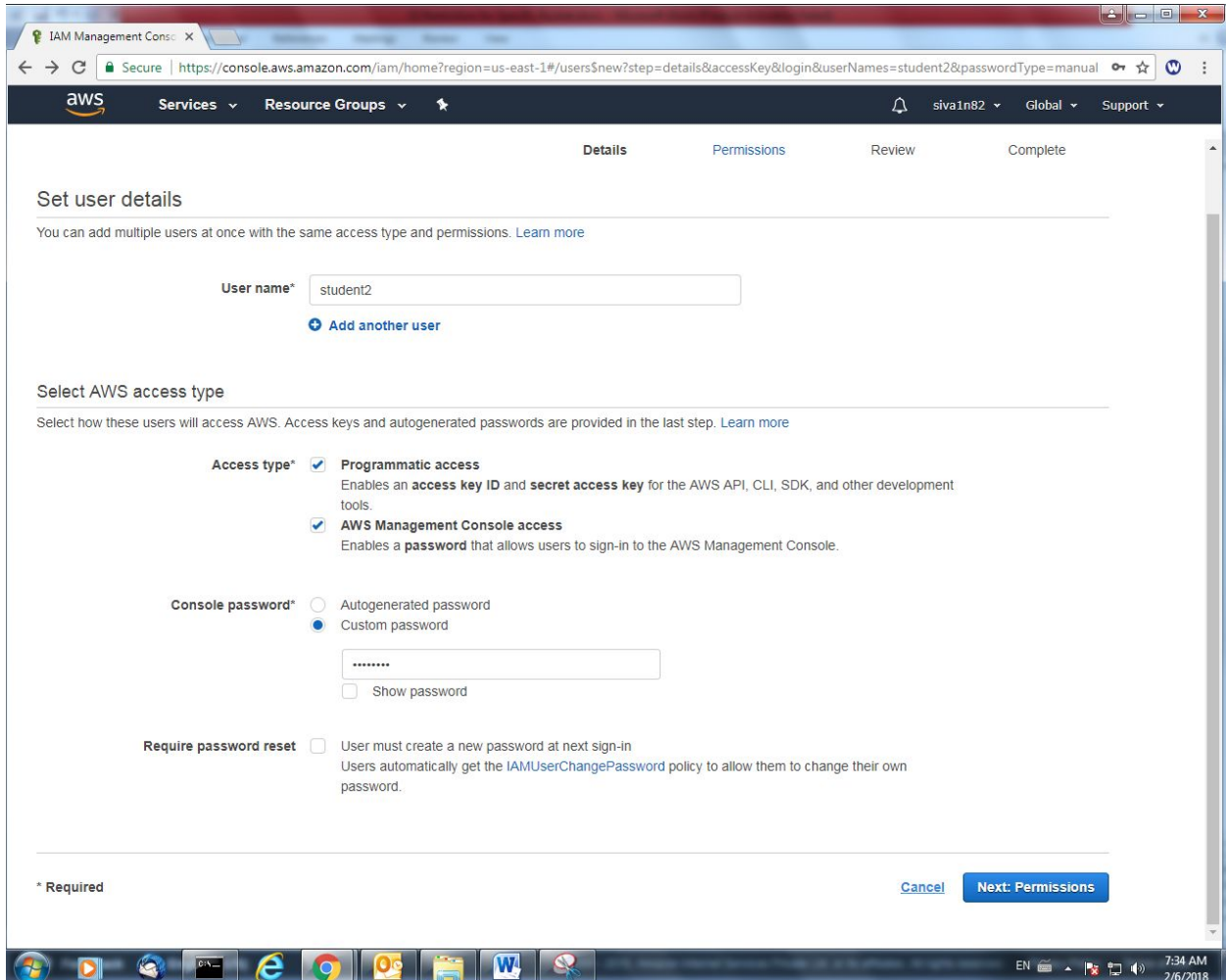
We need to create a user to assign the policy.

Click “Add user”.



Username: student2

Access type : Programmatic access and AWS management console access.



IAM Management Console

Secure | [https://console.aws.amazon.com/iam/home?region=us-east-1#/users\\$new?step=details&accessKey&login&userNames=student2&passwordType=manual](https://console.aws.amazon.com/iam/home?region=us-east-1#/users$new?step=details&accessKey&login&userNames=student2&passwordType=manual)

aws Services Resource Groups

siva1n82 Global Support

Details Permissions Review Complete

Set user details

You can add multiple users at once with the same access type and permissions. [Learn more](#)

User name*

[Add another user](#)

Select AWS access type

Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step. [Learn more](#)

Access type* ☒ **Programmatic access**
Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.

☒ **AWS Management Console access**
Enables a **password** that allows users to sign-in to the AWS Management Console.

Console password* ☐ Autogenerated password
☒ Custom password

☐ Show password

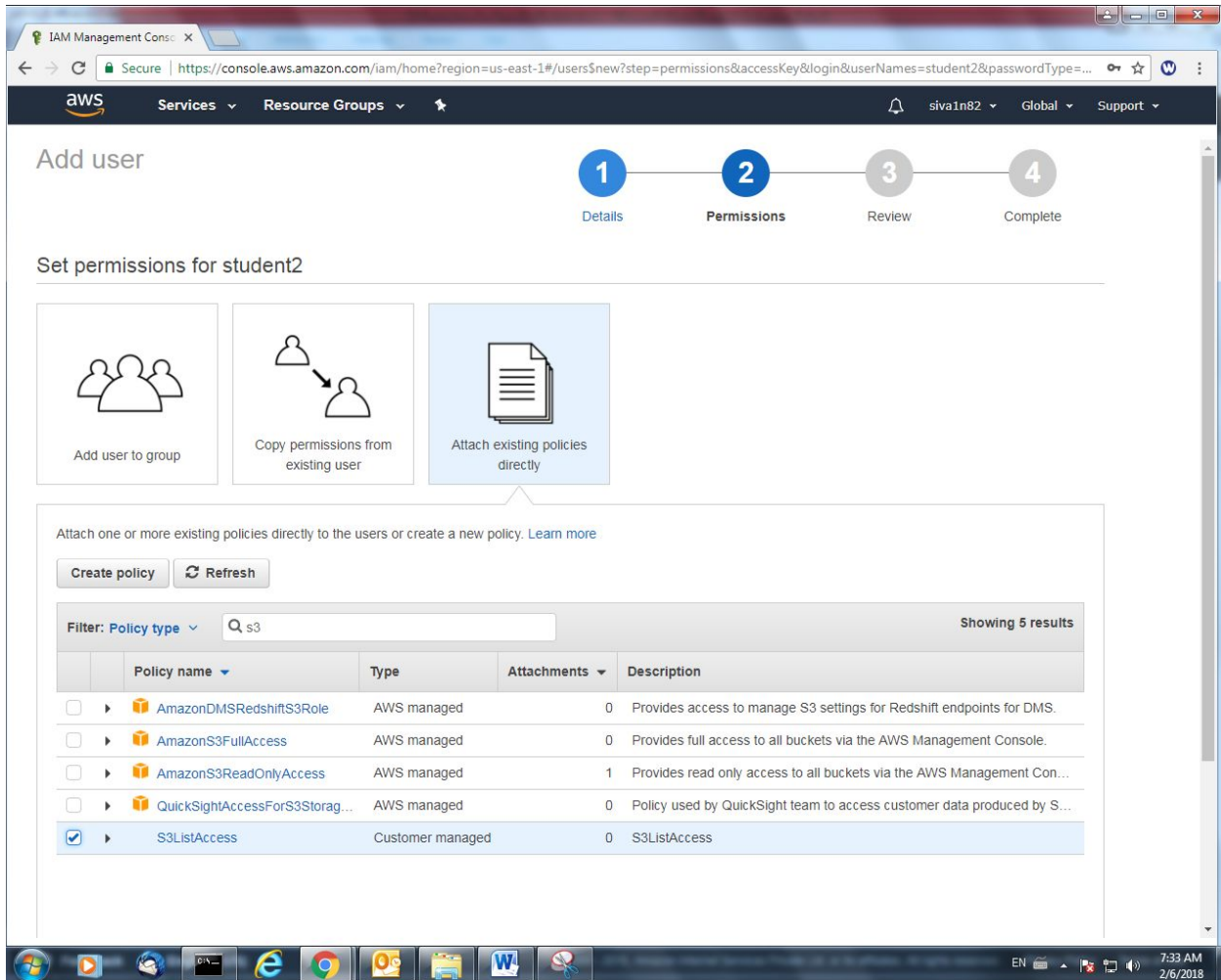
Require password reset ☐ User must create a new password at next sign-in
Users automatically get the [IAMUserChangePassword](#) policy to allow them to change their own password.

* Required

[Cancel](#) [Next: Permissions](#)

Click "Next".


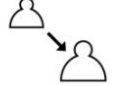

In Policy type, type “s3” to filter the s3 policies. Select the policy which we created.



Add user

1 Details 2 **Permissions** 3 Review 4 Complete

Set permissions for student2

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

Attach one or more existing policies directly to the users or create a new policy. [Learn more](#)

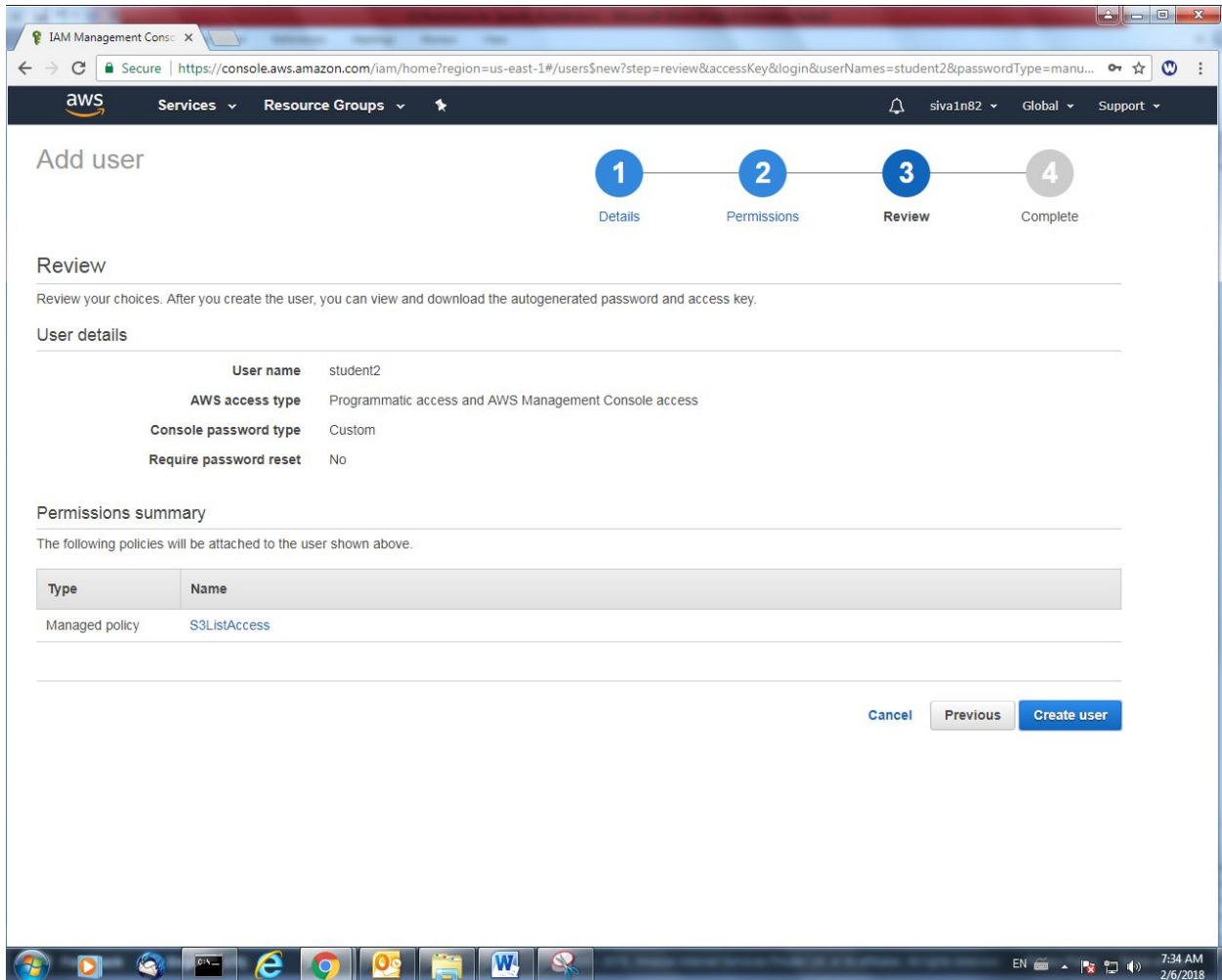
Create policy Refresh

Filter: Policy type Showing 5 results

	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”.



The screenshot shows the AWS IAM Management Console 'Add user' page, specifically the 'Review' step (Step 3 of 4). The page title is 'Add user'. The progress bar indicates the steps: 1 Details, 2 Permissions, 3 Review (current), and 4 Complete.

Review

Review your choices. After you create the user, you can view and download the autogenerated password and access key.

User details

User name	student2
AWS access type	Programmatic access and AWS Management Console access
Console password type	Custom
Require password reset	No

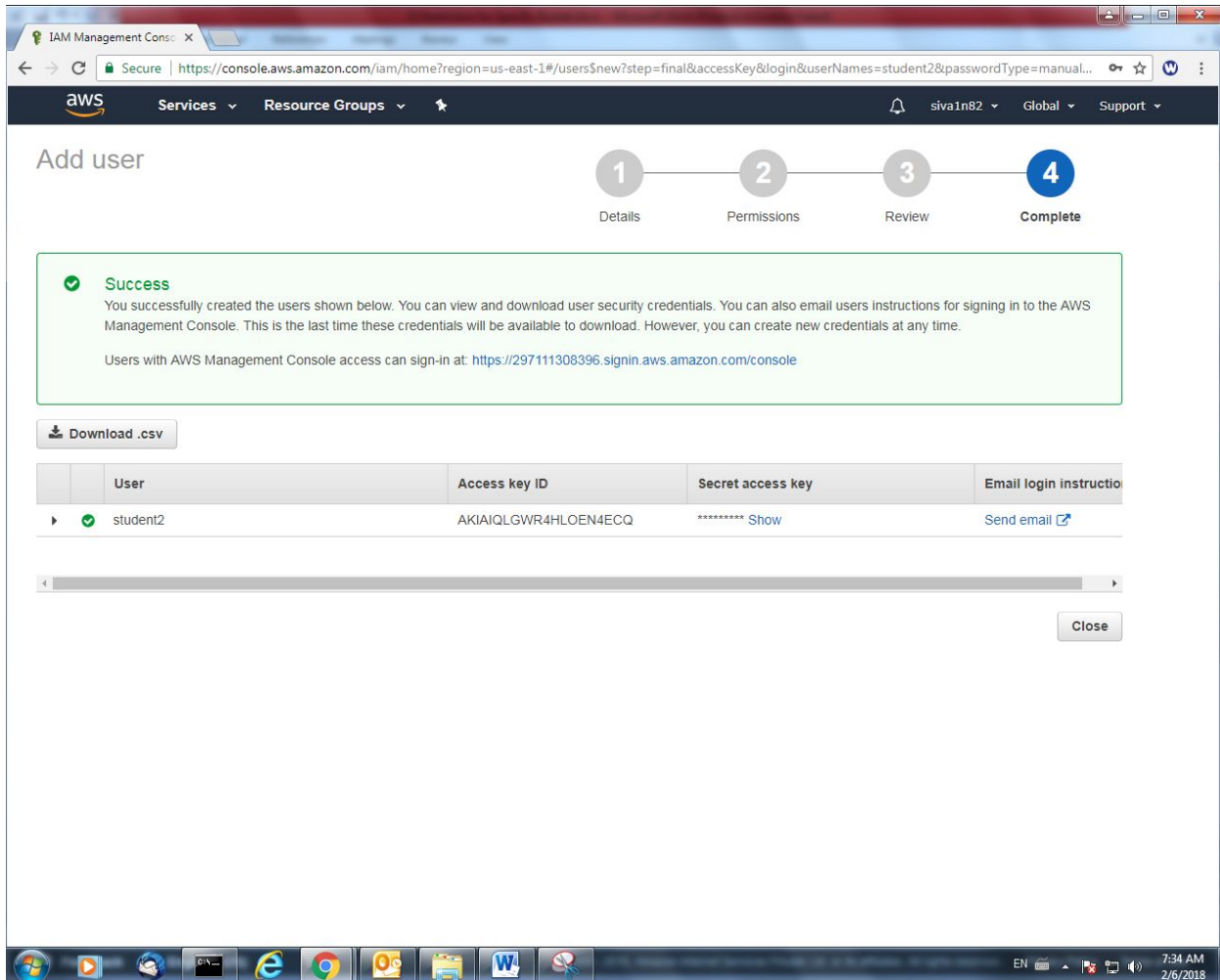
Permissions summary

The following policies will be attached to the user shown above.

Type	Name
Managed policy	S3ListAccess

At the bottom right, there are three buttons: 'Cancel', 'Previous', and '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 the AWS logo, 'Services', 'Resource Groups', and user information. Below this, the 'Add user' section is visible, with a progress indicator showing four steps: 1. Details, 2. Permissions, 3. Review, and 4. Complete (highlighted in blue). A green success message box states: '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. Users with AWS Management Console access can sign-in at: <https://297111308396.signin.aws.amazon.com/console>'. Below the message is a 'Download .csv' button. A table lists the created user:

	User	Access key ID	Secret access key	Email login instruction
▶	✓ student2	AKIAIQLGWR4HLOEN4ECQ	***** Show	Send email ↗

At the bottom right of the table area is a 'Close' button. The Windows taskbar at the very bottom shows various application icons and the system clock indicating 7:34 AM on 2/6/2018.

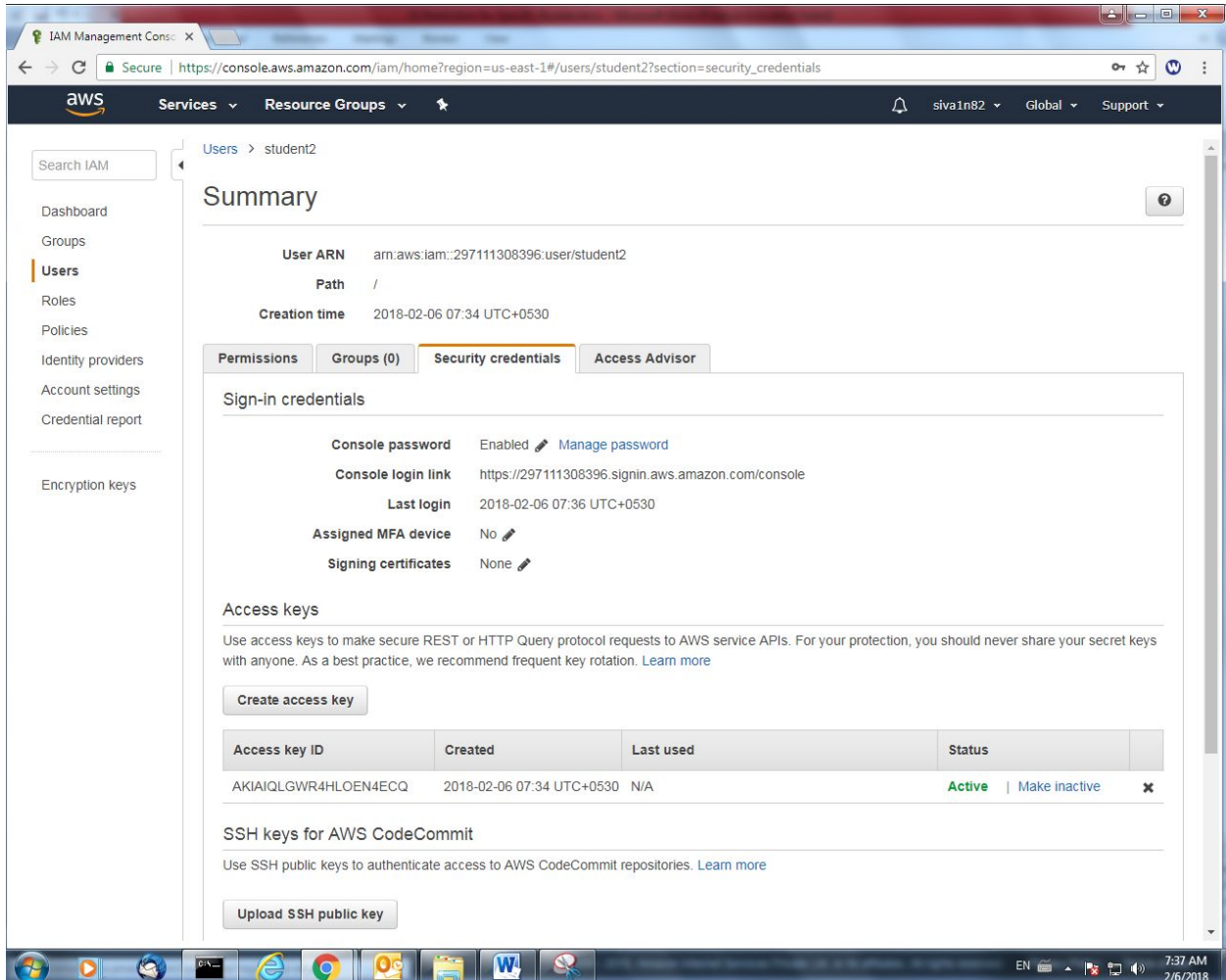


Click Users, and select student2 user.

The screenshot shows the AWS IAM Management Console interface. The left sidebar contains navigation links: Dashboard, Groups, Users (highlighted), Roles, Policies, Identity providers, Account settings, Credential report, and Encryption keys. The main content area shows the 'Users' page with a search bar and two buttons: 'Add user' and 'Delete user'. Below the search bar is a table listing users. The table has columns for User name, Groups, Access key age, Password age, Last activity, and MFA. Two users are listed: student1 and student2. student1 is associated with the S3ReadOnlyAccess group, while student2 has no group. Both users have access keys created today and MFA is not enabled for either.

	User name	Groups	Access key age	Password age	Last activity	MFA
<input type="checkbox"/>	student1	S3ReadOnlyAccess	✓ Today	Today	None	Not enabled
<input type="checkbox"/>	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 console interface. The left sidebar contains navigation links: Search IAM, Dashboard, Groups, Users (selected), Roles, Policies, Identity providers, Account settings, Credential report, and Encryption keys. The main content area is titled 'Summary' for 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 (selected), and Access Advisor. The 'Security credentials' tab shows 'Sign-in credentials' with the following details: Console password (Enabled, Manage password), Console login link (https://297111308396.signin.aws.amazon.com/console), Last login (2018-02-06 07:36 UTC+0530), Assigned MFA device (No), and Signing certificates (None). Under 'Access keys', there is a 'Create access key' button and a table with one entry: Access key ID (AKIAIQLGWR4HLOEN4ECQ), Created (2018-02-06 07:34 UTC+0530), Last used (N/A), and Status (Active). Below this, there is a section for 'SSH keys for AWS CodeCommit' with an 'Upload SSH public key' button. The bottom of the screen shows a Windows taskbar with various application icons and a system clock indicating 7:37 AM on 2/6/2018.

Summary

User ARN: arn:aws:iam::297111308396:user/student2
 Path: /
 Creation time: 2018-02-06 07:34 UTC+0530

Security credentials

Sign-in credentials

- Console password: Enabled [Manage password](#)
- Console login link: <https://297111308396.signin.aws.amazon.com/console>
- Last login: 2018-02-06 07:36 UTC+0530
- Assigned MFA device: No
- Signing certificates: None

Access keys

Use access keys to make secure REST or HTTP Query protocol requests to AWS service APIs. For your protection, you should never share your secret keys with anyone. As a best practice, we recommend frequent key rotation. [Learn more](#)

[Create access key](#)

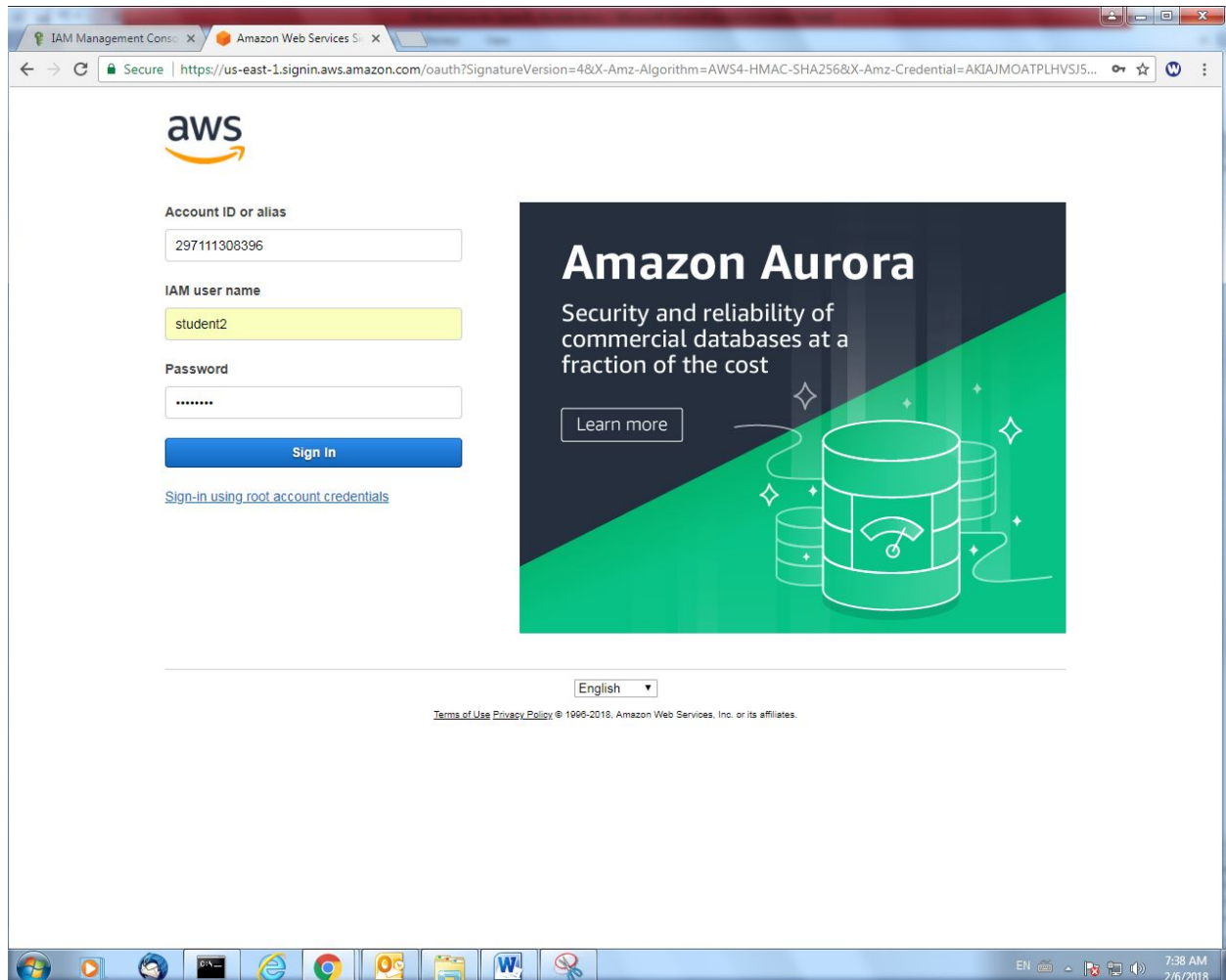
Access key ID	Created	Last used	Status
AKIAIQLGWR4HLOEN4ECQ	2018-02-06 07:34 UTC+0530	N/A	Active Make inactive Delete

SSH keys for AWS CodeCommit

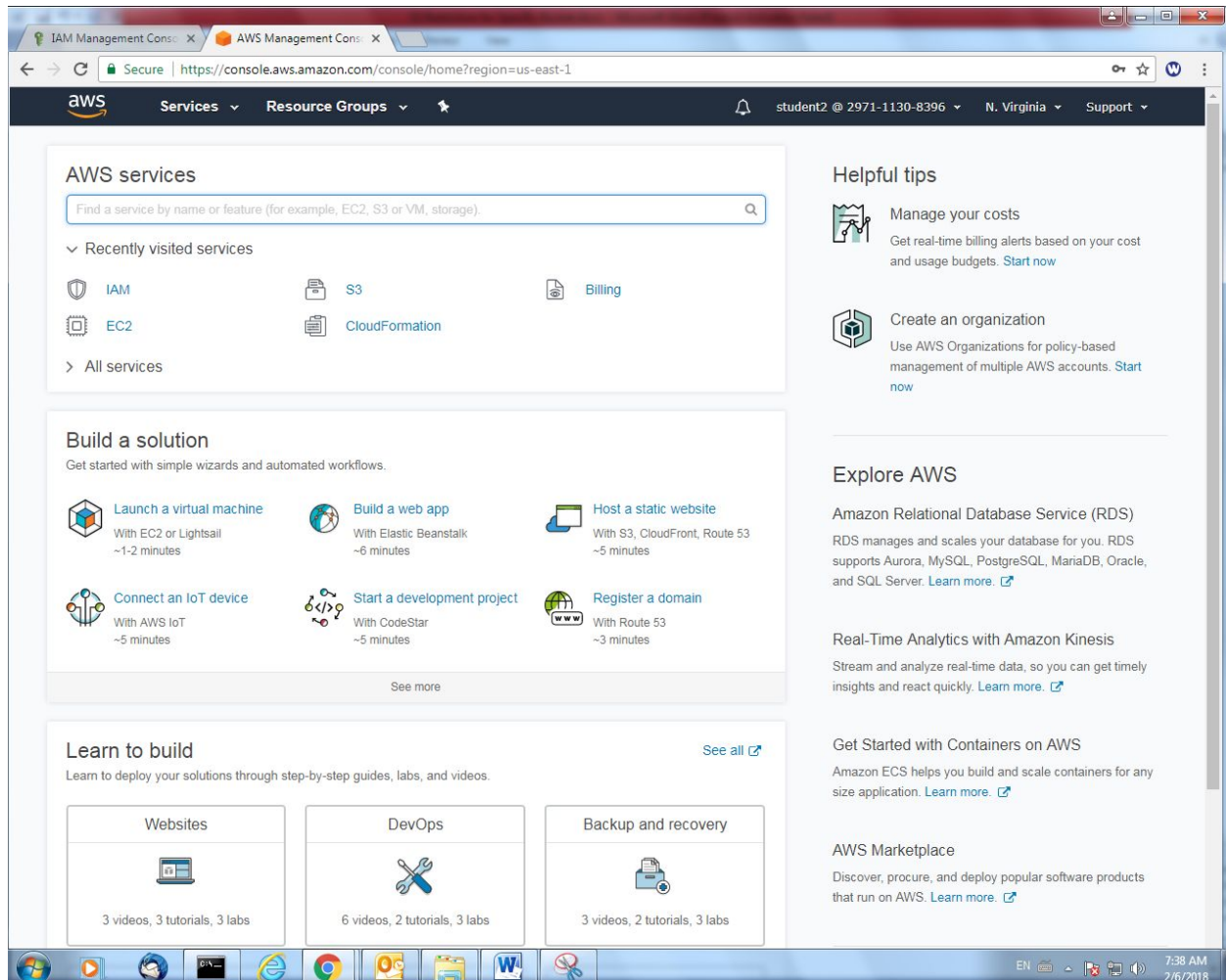
Use SSH public keys to authenticate access to AWS CodeCommit repositories. [Learn more](#)

[Upload SSH public key](#)

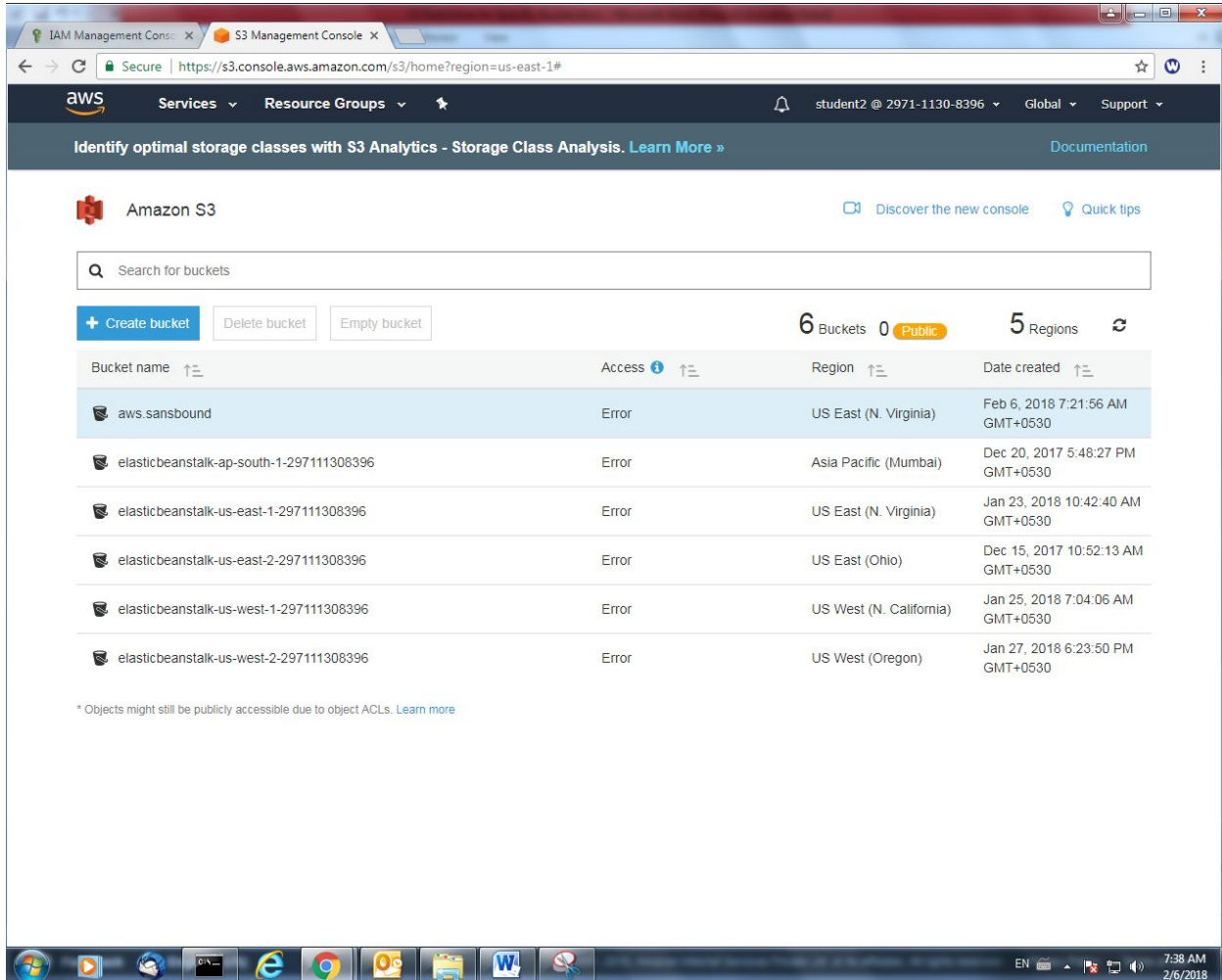
Type the login credentials of Student2.



Click "S3".



Click “aws.sansbound” bucket.









Identify optimal storage classes with S3 Analytics - Storage Class Analysis. [Learn More »](#) [Documentation](#)

Amazon S3 [Discover the new console](#) [Quick tips](#)

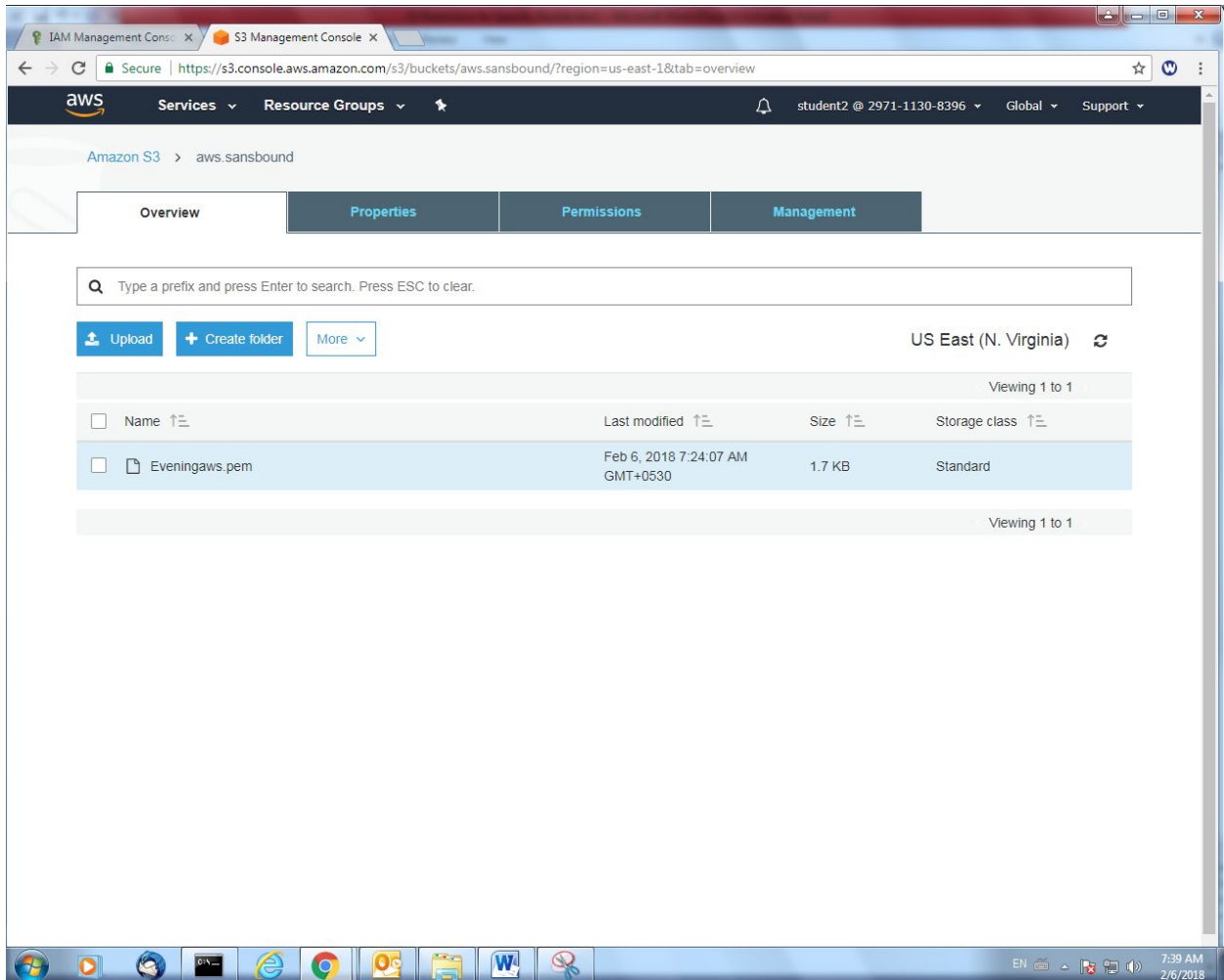
Search for buckets

[+ Create bucket](#) [Delete bucket](#) [Empty bucket](#) **6** Buckets **0** Public **5** Regions [Refresh](#)

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 console interface. The top navigation bar includes the AWS logo, 'Services', 'Resource Groups', and user information. The main content area is titled 'Amazon S3 > aws.sansbound'. Below this, there are tabs for 'Overview', 'Properties', 'Permissions', and 'Management'. A search bar is present with the placeholder text 'Type a prefix and press Enter to search. Press ESC to clear.' Below the search bar are buttons for 'Upload', 'Create folder', and 'More'. The region is set to 'US East (N. Virginia)'. A table displays the contents of the bucket:

	Name	Last modified	Size	Storage class
<input type="checkbox"/>	Eveningaws.pem	Feb 6, 2018 7:24:07 AM GMT+0530	1.7 KB	Standard

The bottom of the screenshot shows a Windows taskbar with various application icons and a system clock indicating 7:39 AM on 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.

