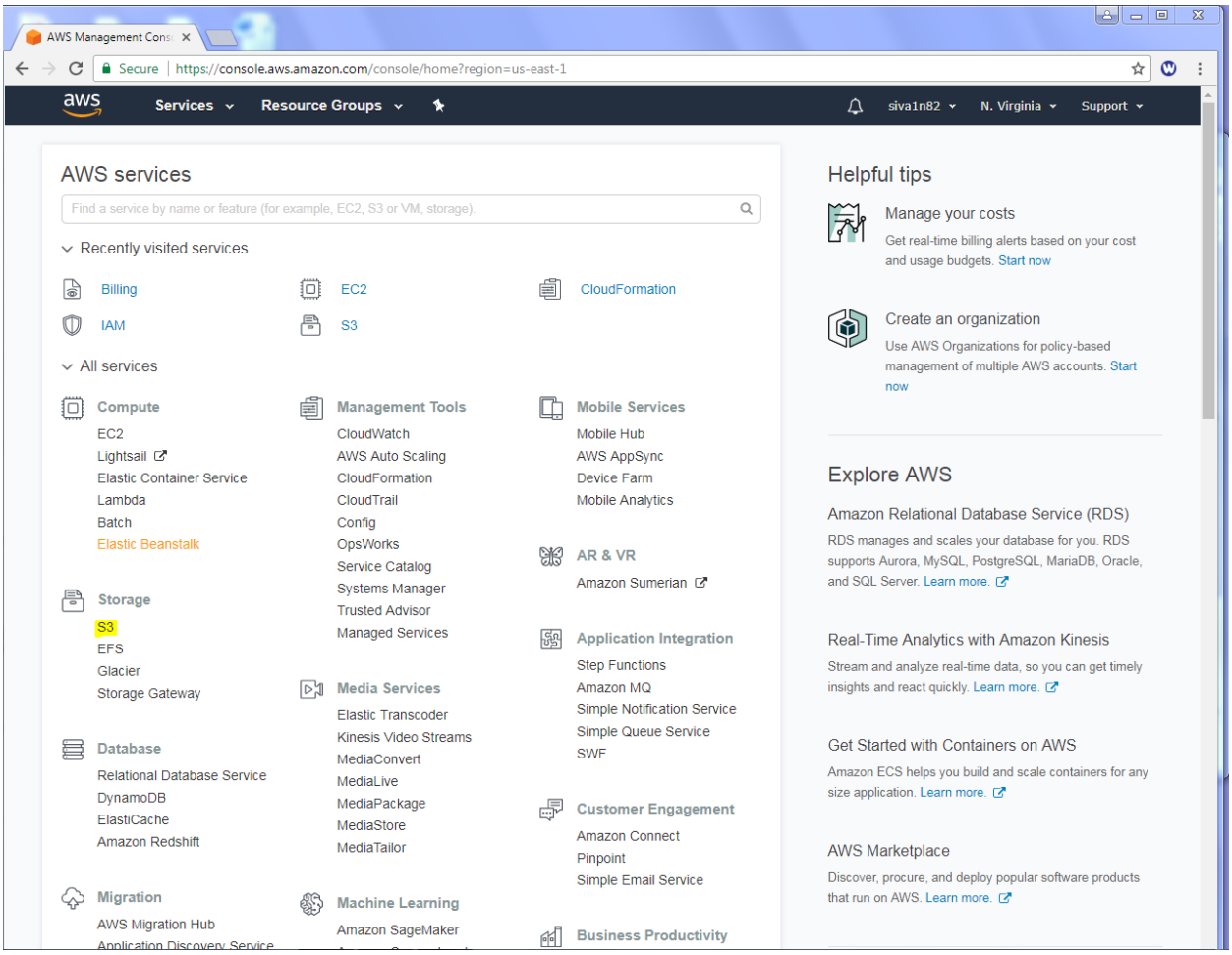
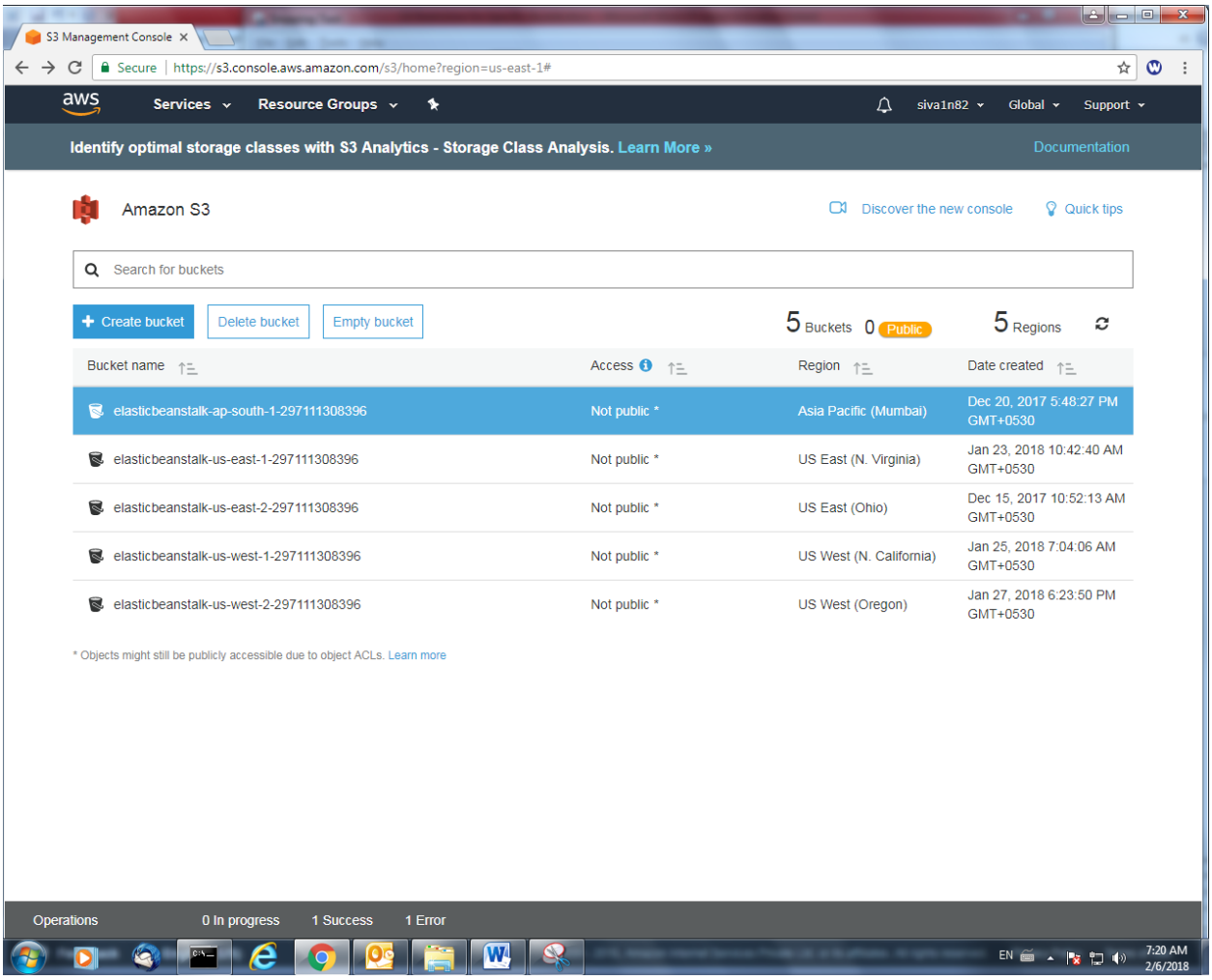
Lab24

S3 Restriction for Specific Bucket

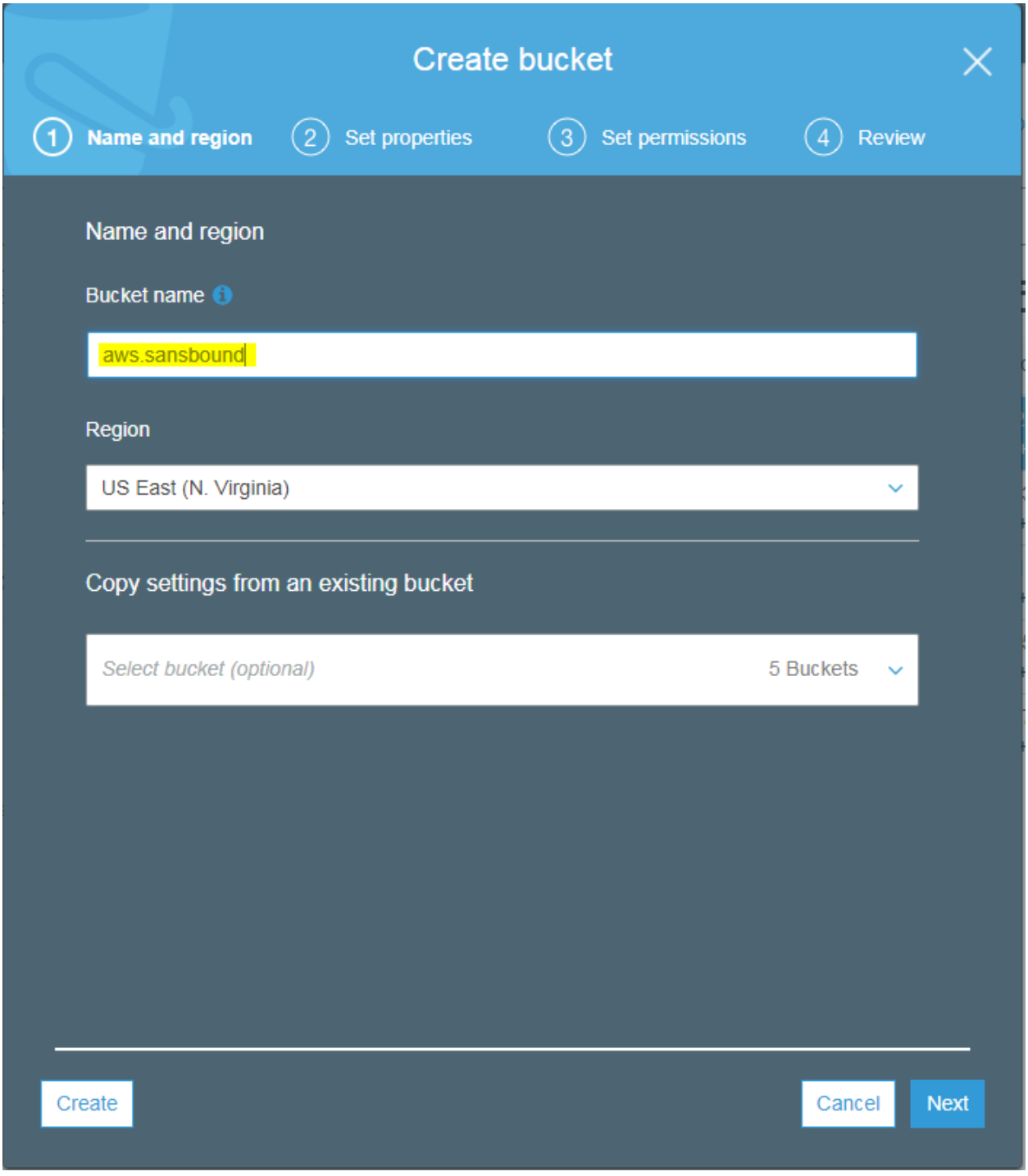
Click “S3”service



Click “Create bucket” with unique name.

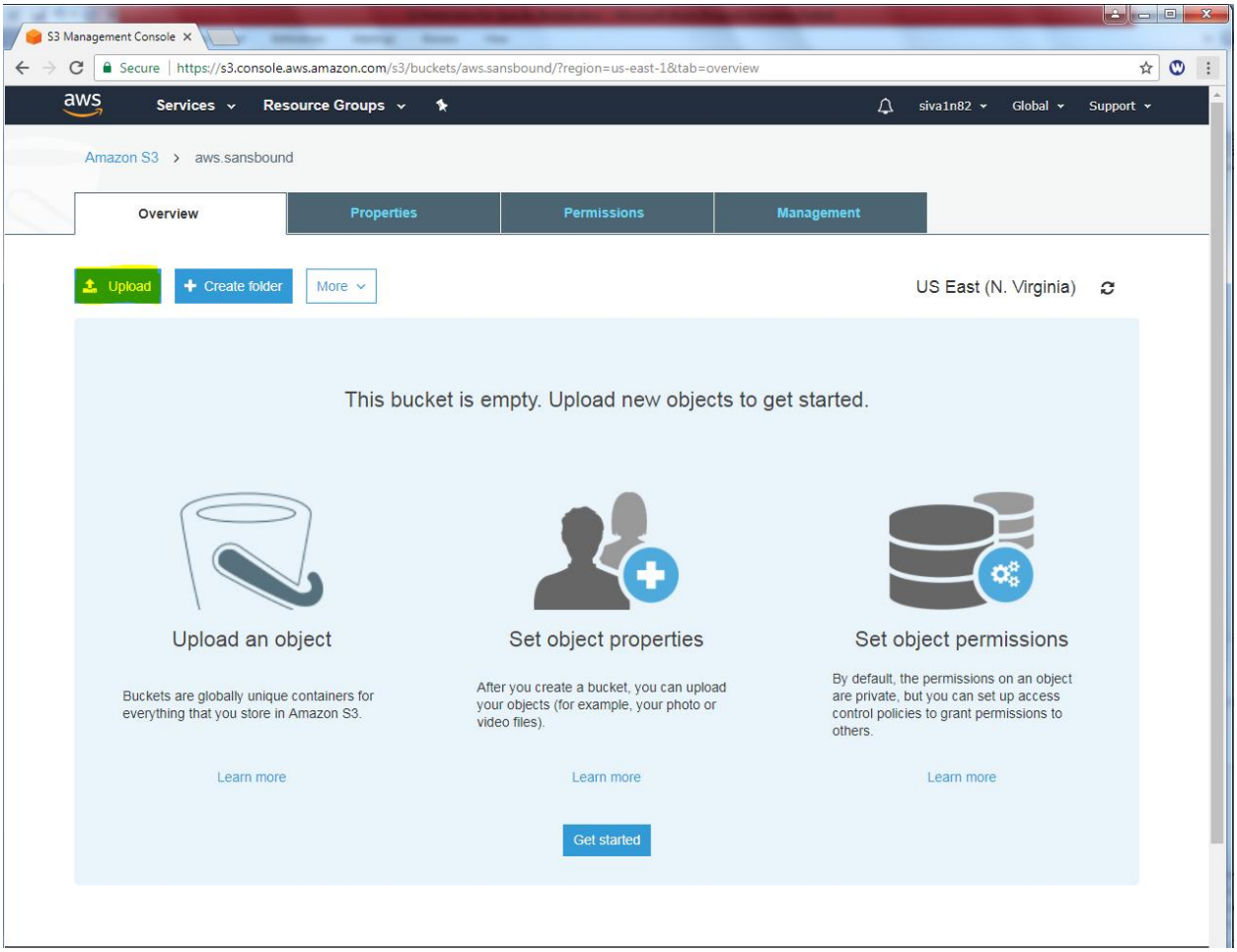


Type aws.sansbound.com

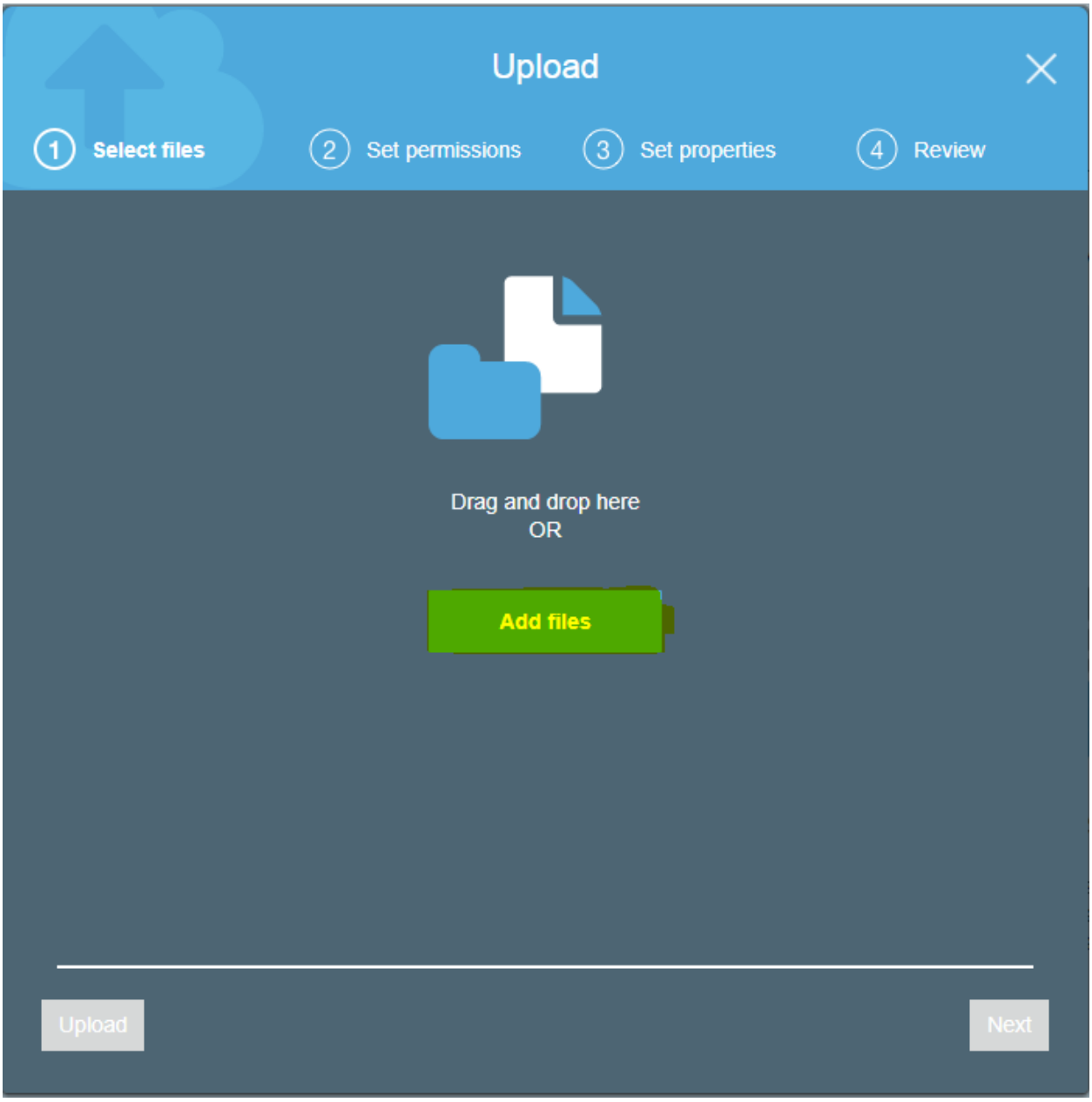


Click “Create”.

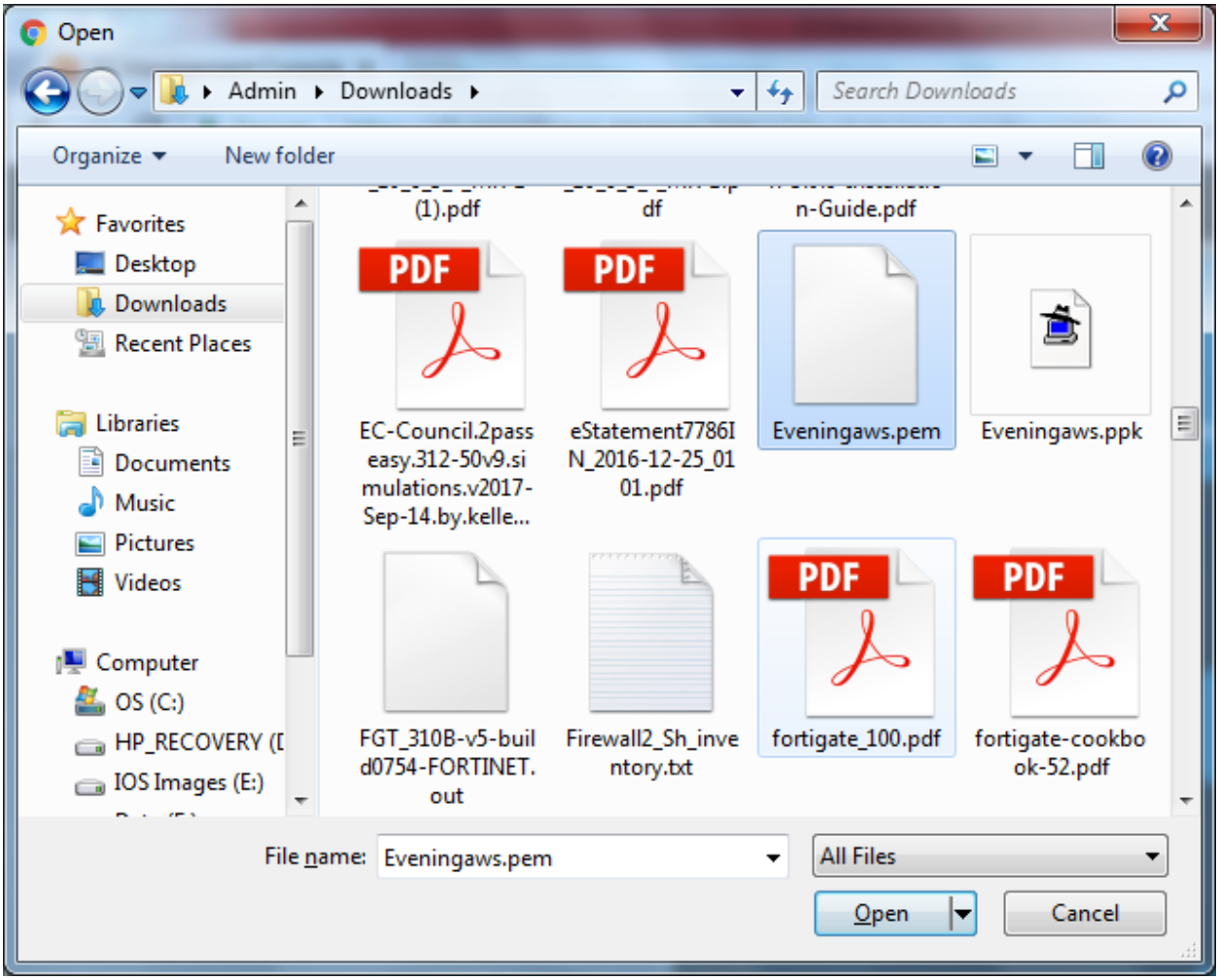
Click “Upload”.



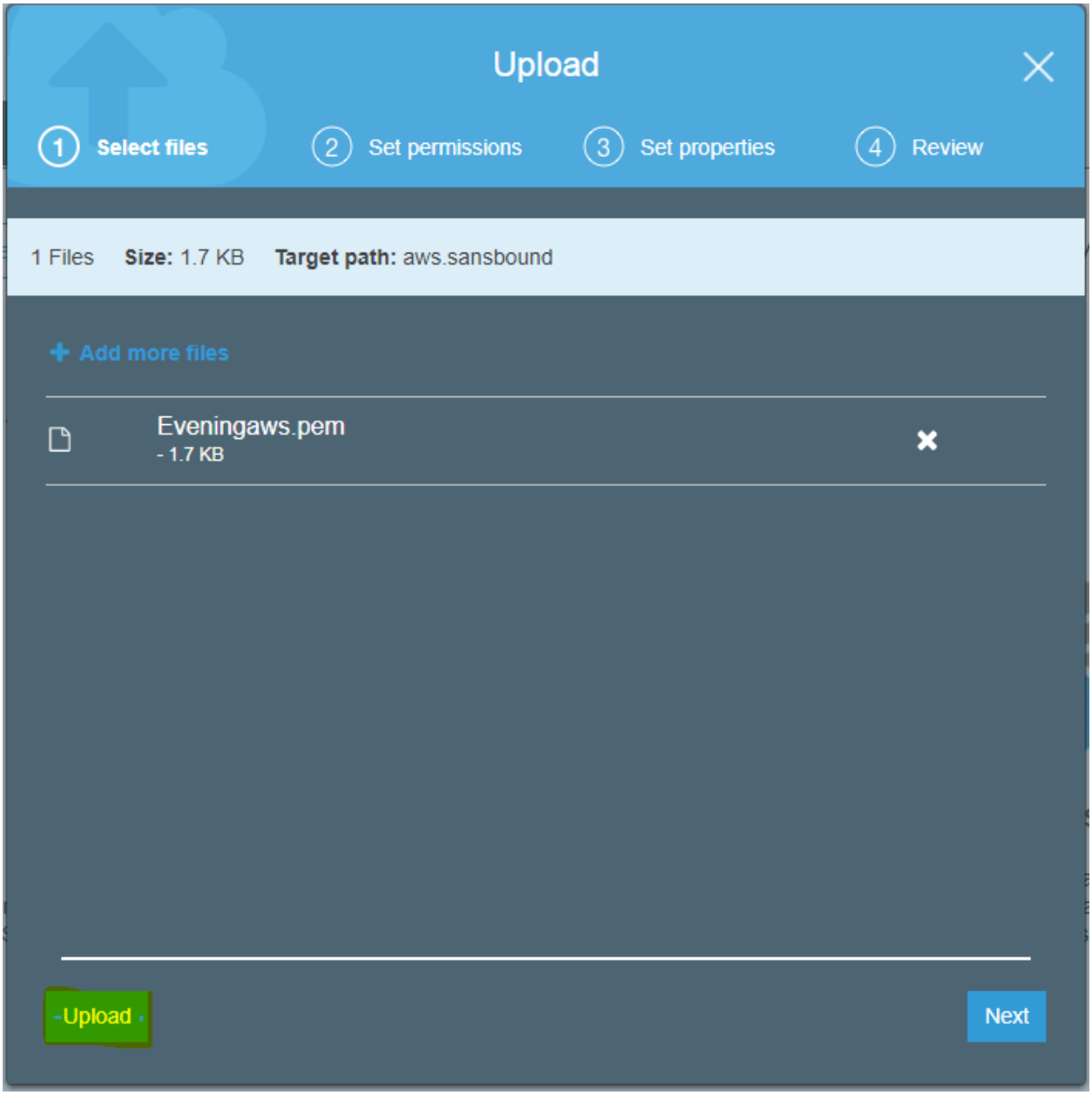
Click “Add files”.



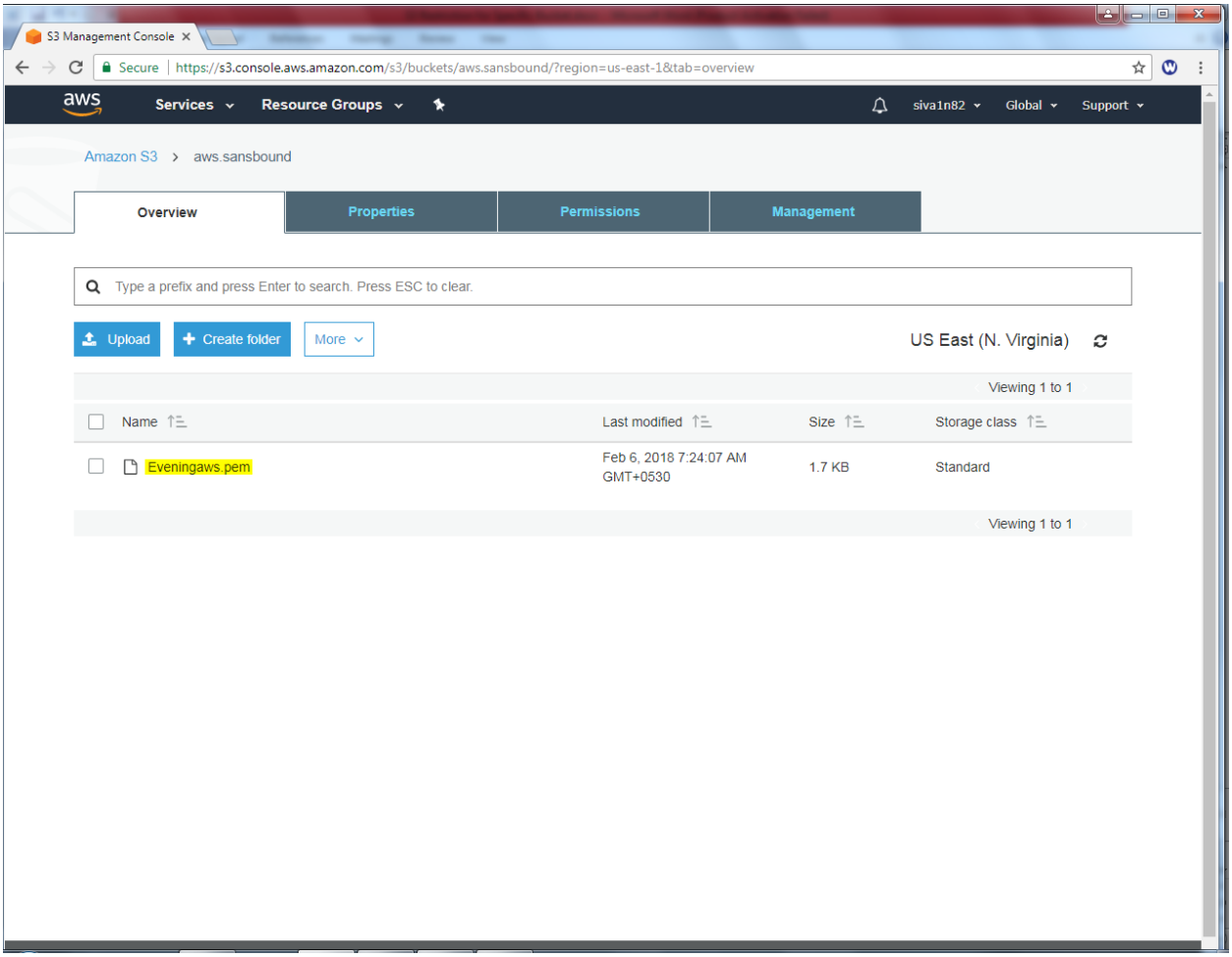
Locate the file and click open.


Open
Admin ▸ Downloads ▸
Search Downloads
Organize
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Computer
OS (C:)
HP_RECOVERY (D
IOS Images (E:)
(1).pdf
df
n-Guide.pdf
EC-Council.2passeasy.312-50v9.simulations.v2017-Sep-14.by.kelle...
eStatement7786IN_2016-12-25_0101.pdf
Eveningaws.pem
Eveningaws.ppk
FGT_310B-v5-build0754-FORTINET.out
Firewall2_Sh_inventory.txt
fortigate_100.pdf
fortigate-cookbook-52.pdf
File name: Eveningaws.pem
All Files
Open
Cancel

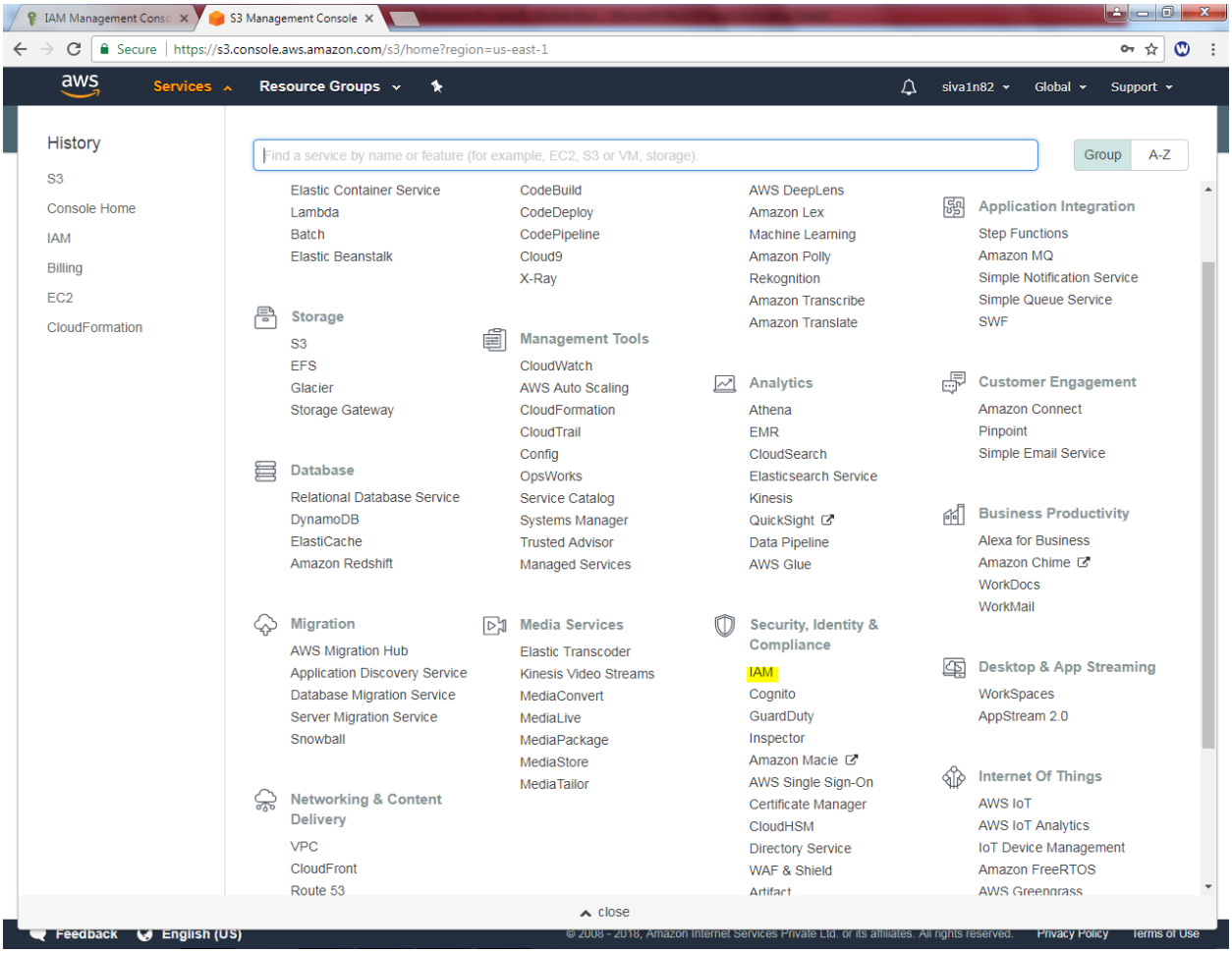
Click “Upload” to upload the file.



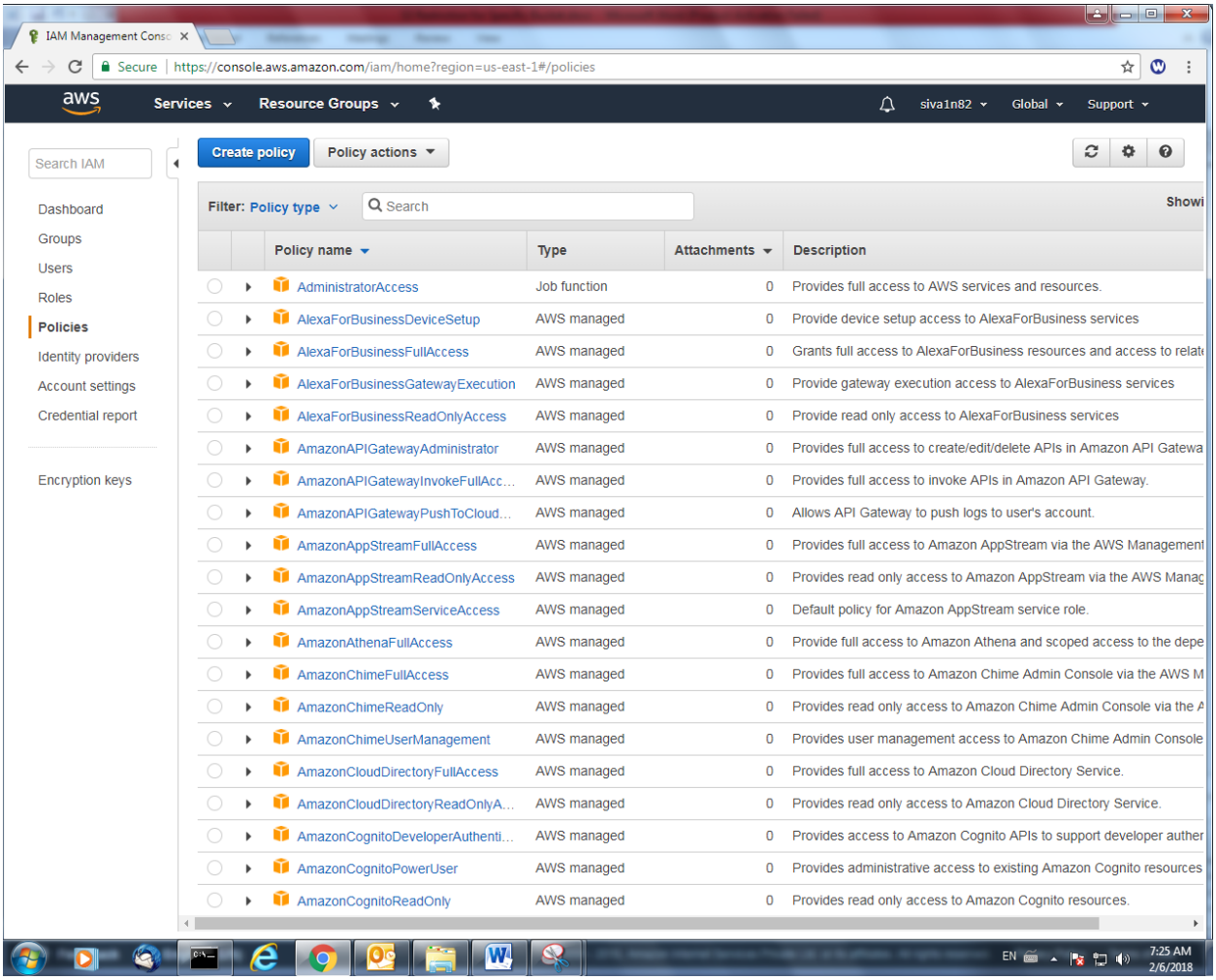
We can able view the file.



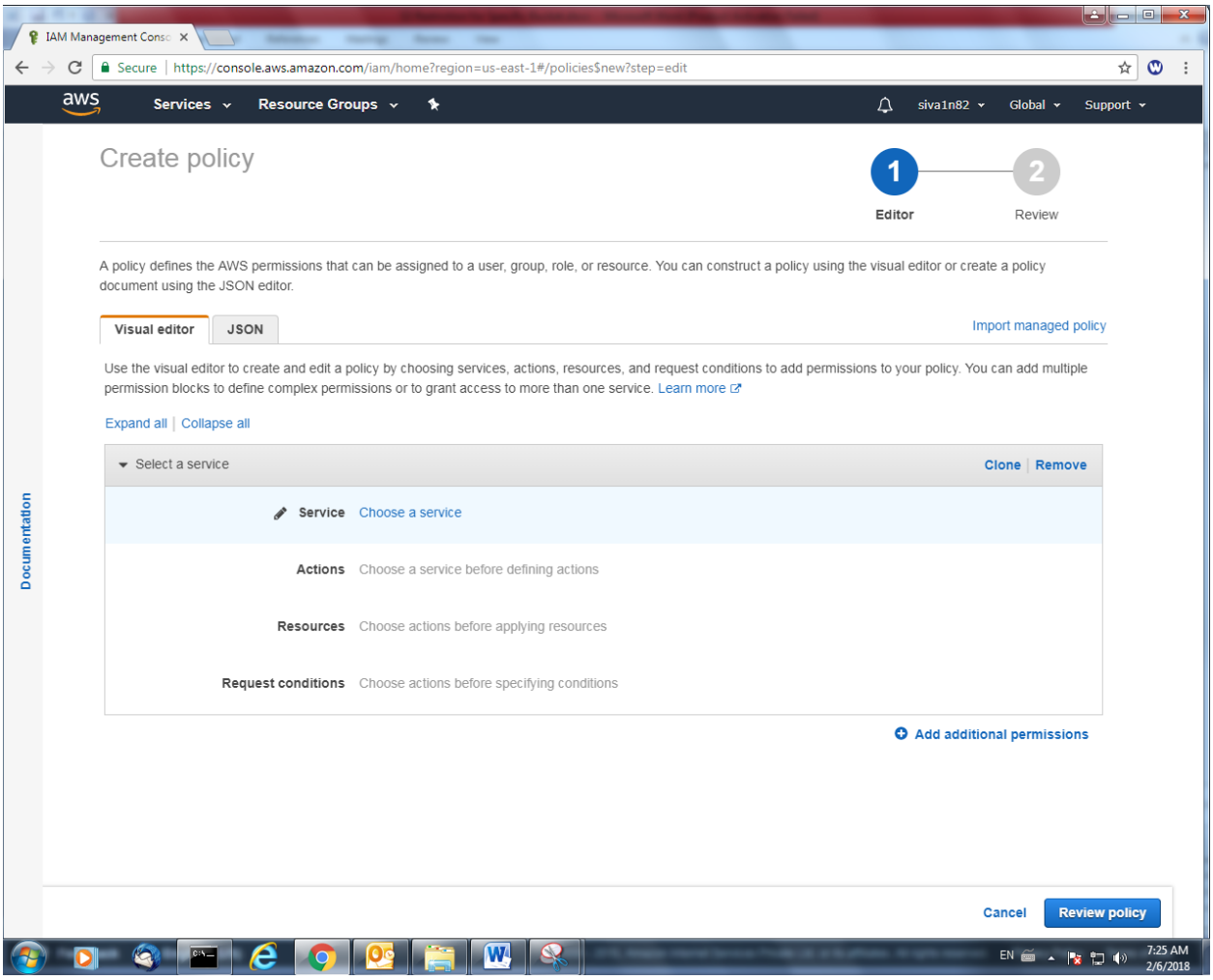
Click “IAM” Role.



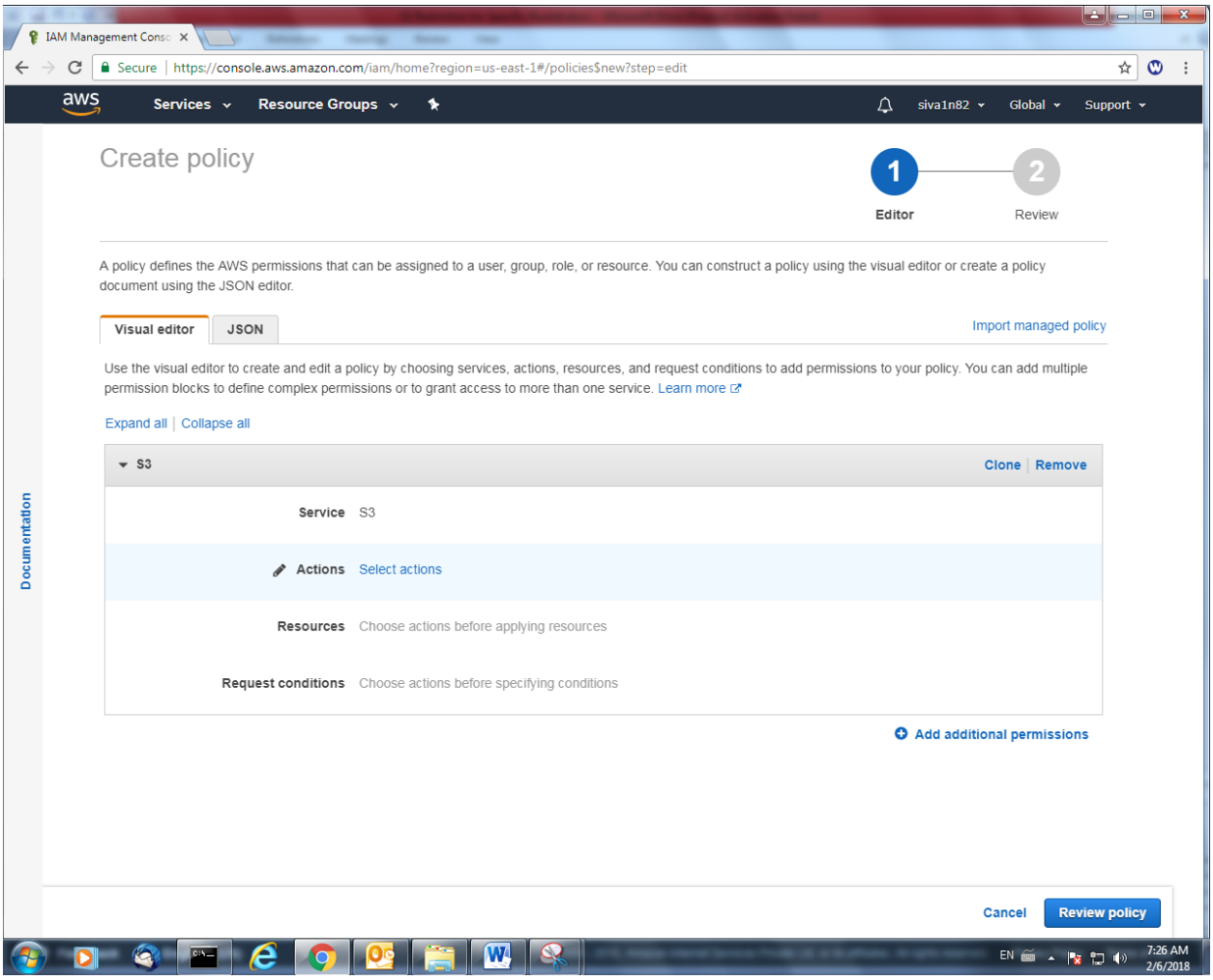
Click “Create Policy”.



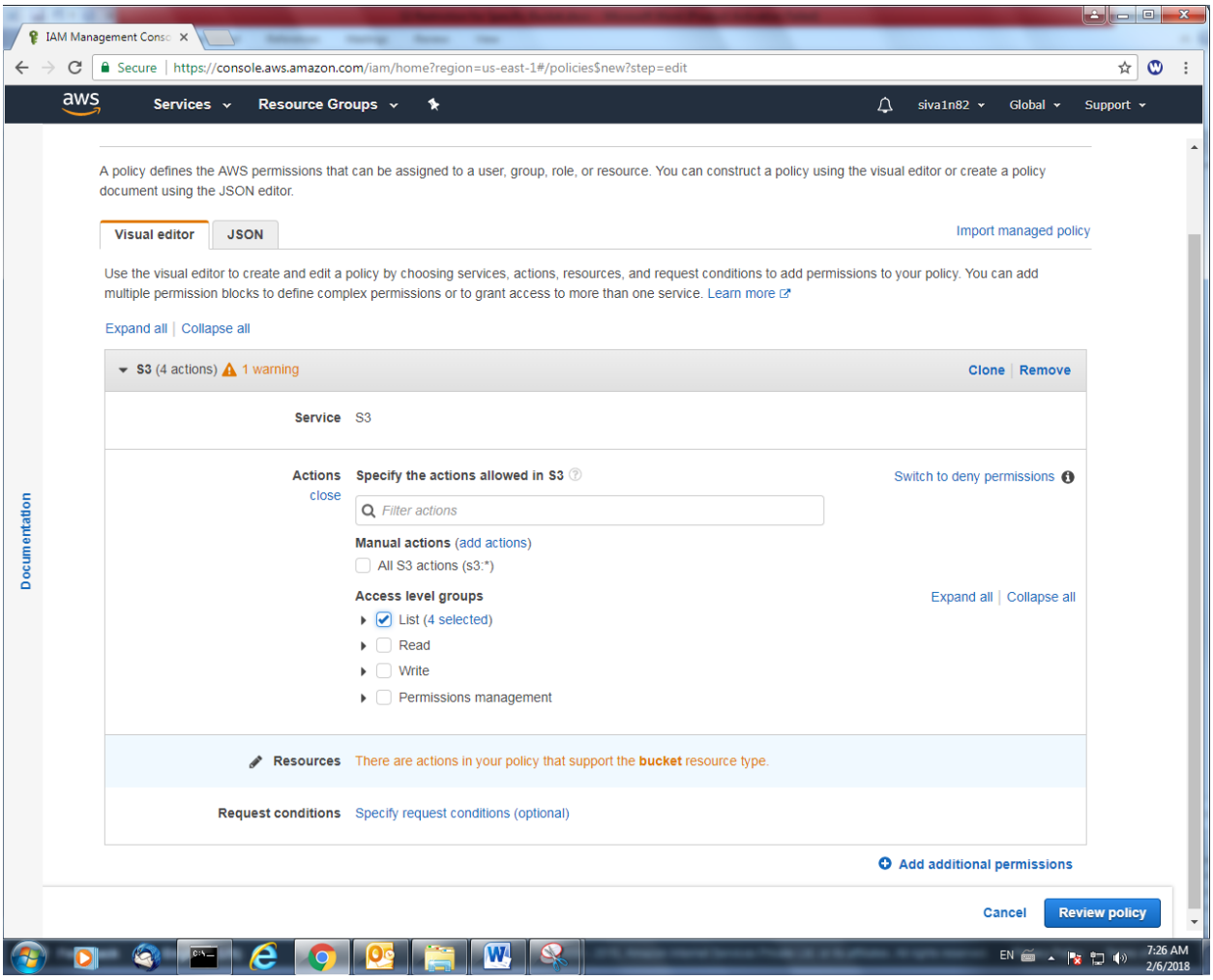
Click “Choose a service” and



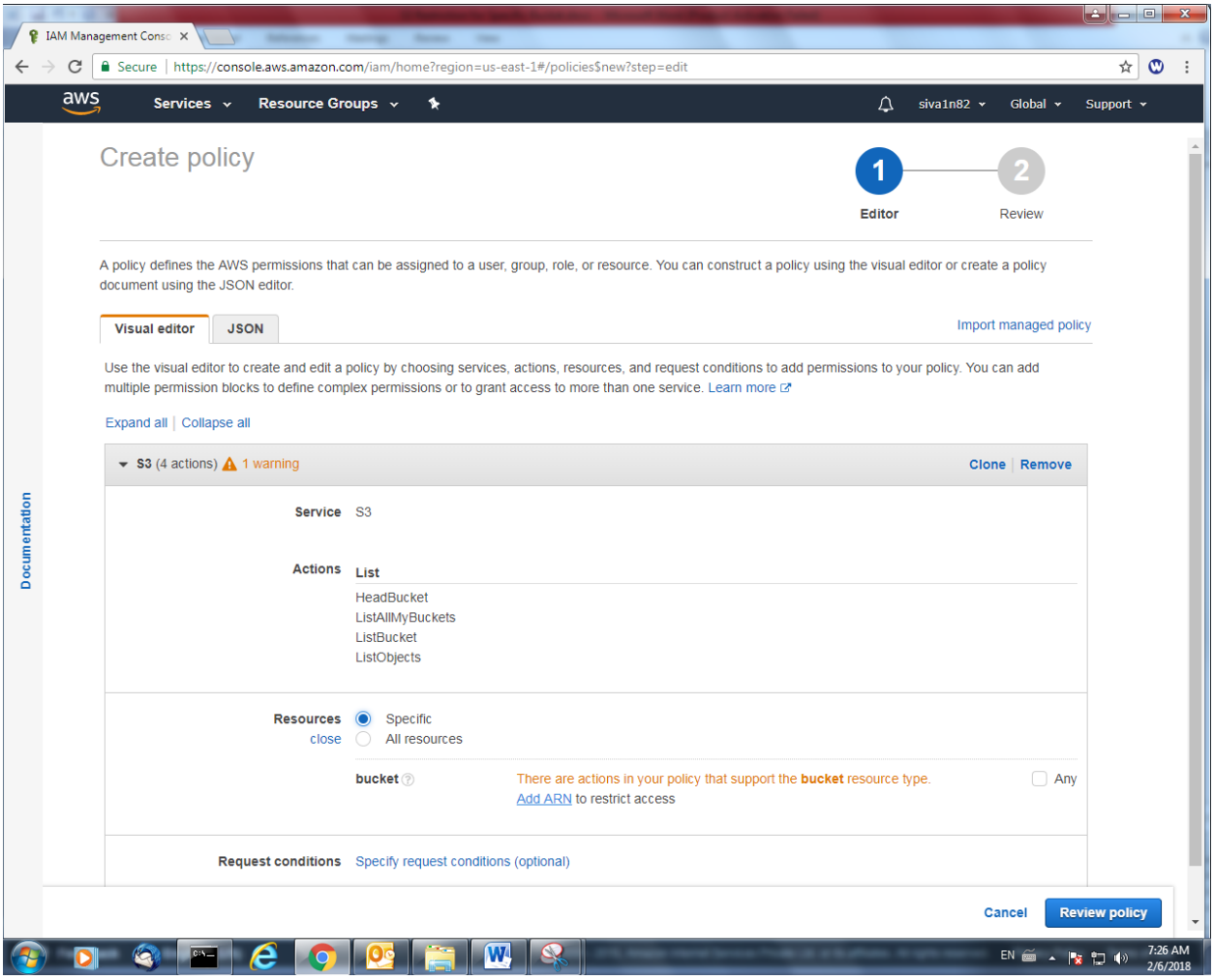
choose the S3 service and click Select actions.



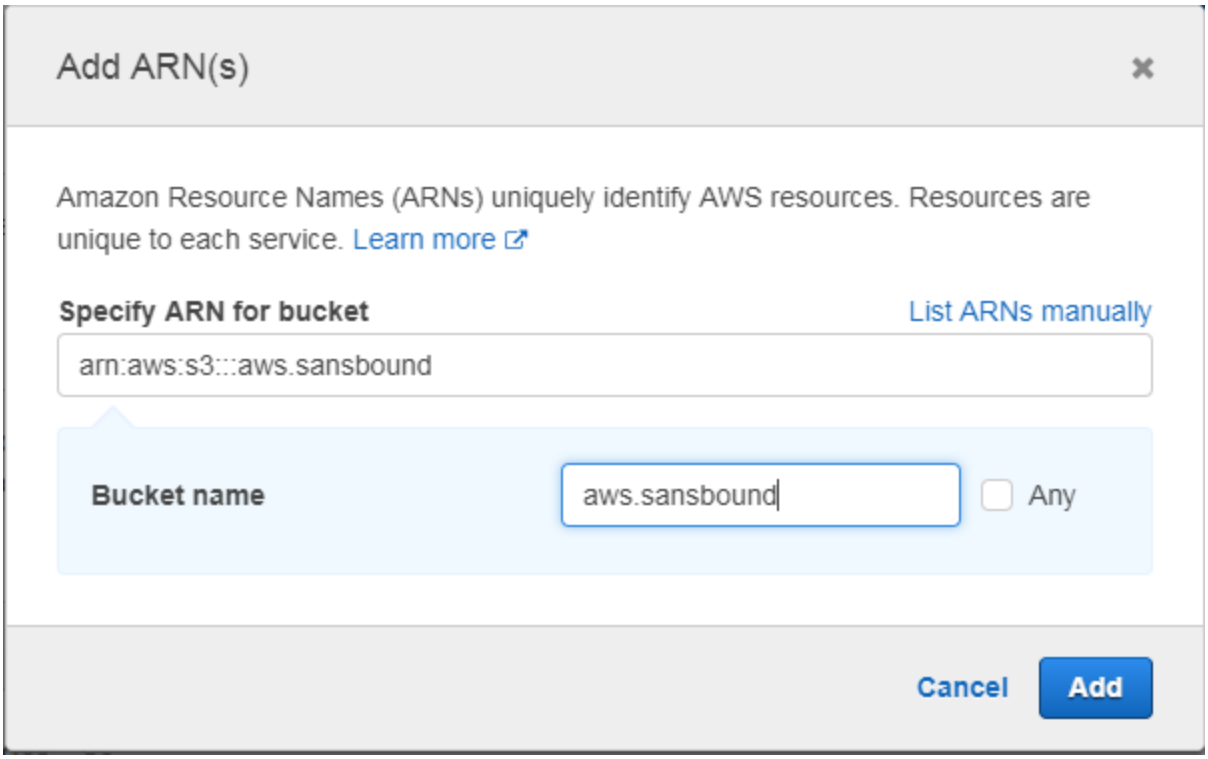
Access level groups, check “List” and click “There are action in your policy that support the bucket resource type.


IAM Management Cons
Secure | https://console.aws.amazon.com/iam/home?region=us-east-1#/policies$new?step=edit
aws
Services
Resource Groups
siva1n82
Global
Support
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) 1 warning
Clone | Remove
Service S3
Actions
close
Specify the actions allowed in S3
Switch to deny permissions
Filter actions
Manual actions (add actions)
All S3 actions (s3:*)
Access level groups
Expand all | Collapse all
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
Cancel
Review policy
Documentation
EN
7:26 AM
2/6/2018

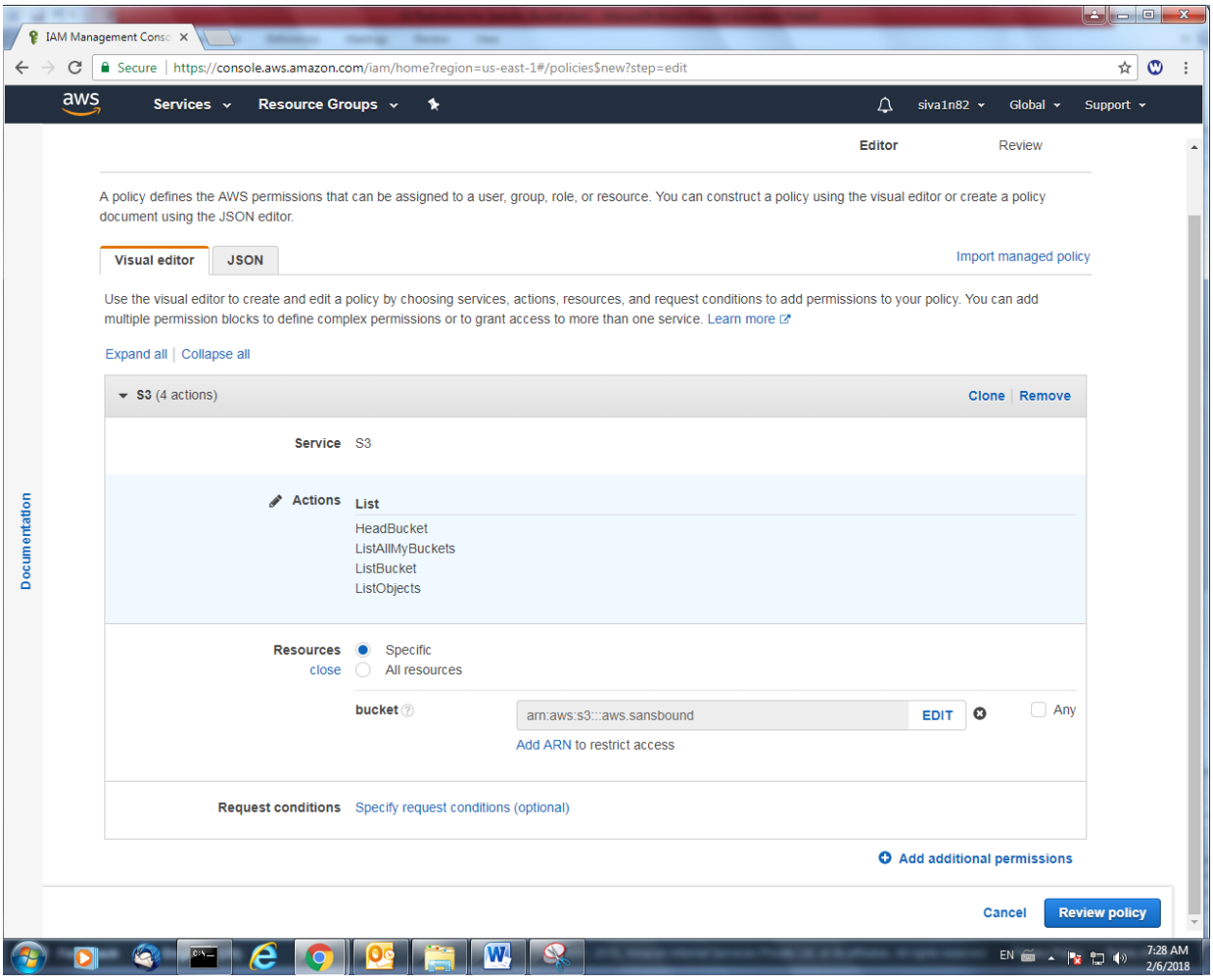
Click specific option and click “Add ARN” to add the bucket name.



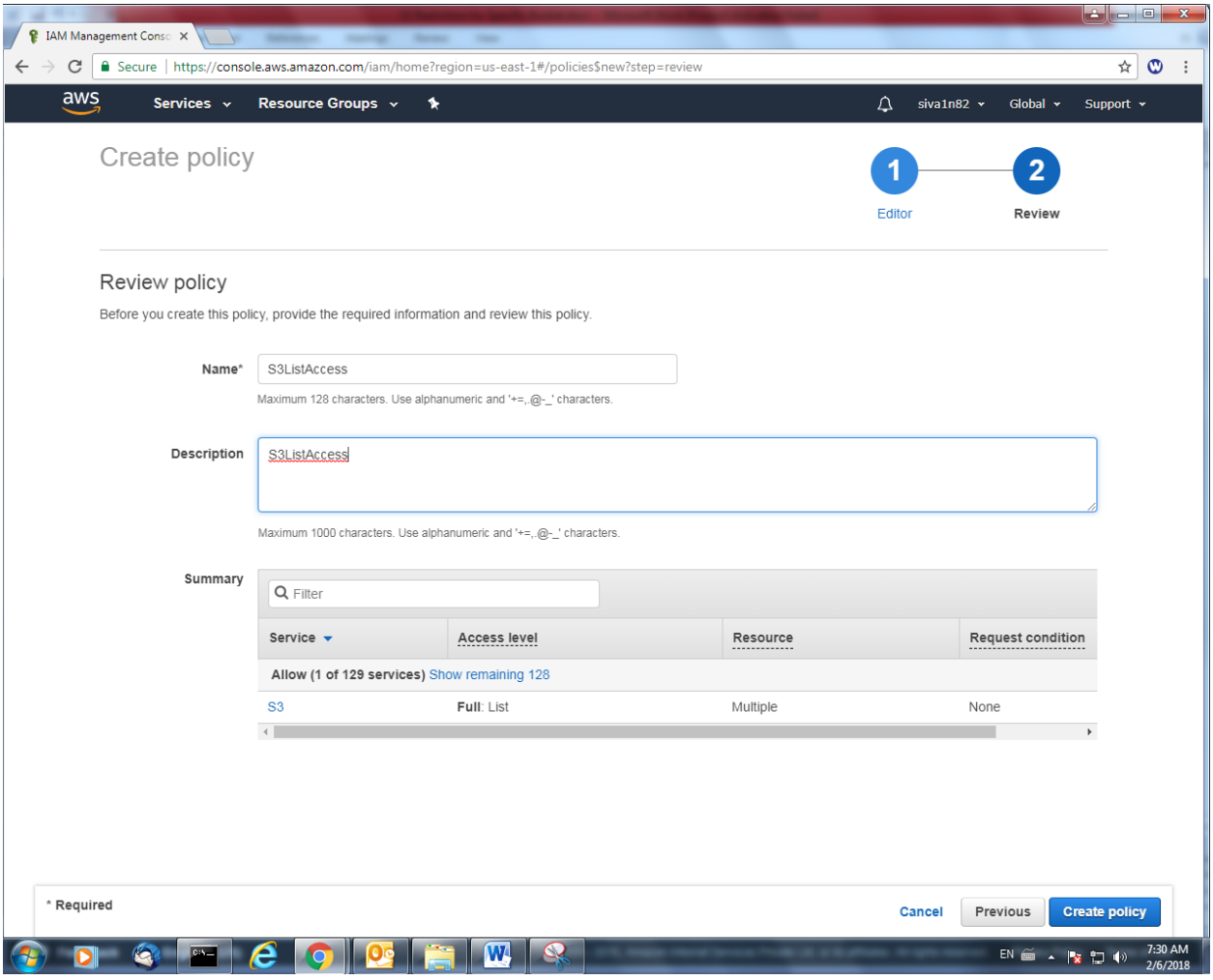
Type the bucket name and click “Add”.



Click “Review Policy”.


IAM Management Cons
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
close
Specific
All resources
bucket
arn:aws:s3:::aws.sansbound
EDIT
Any
Add ARN to restrict access
Request conditions
Specify request conditions (optional)
Add additional permissions
Cancel
Review policy
Documentation
EN
7:28 AM
2/6/2018

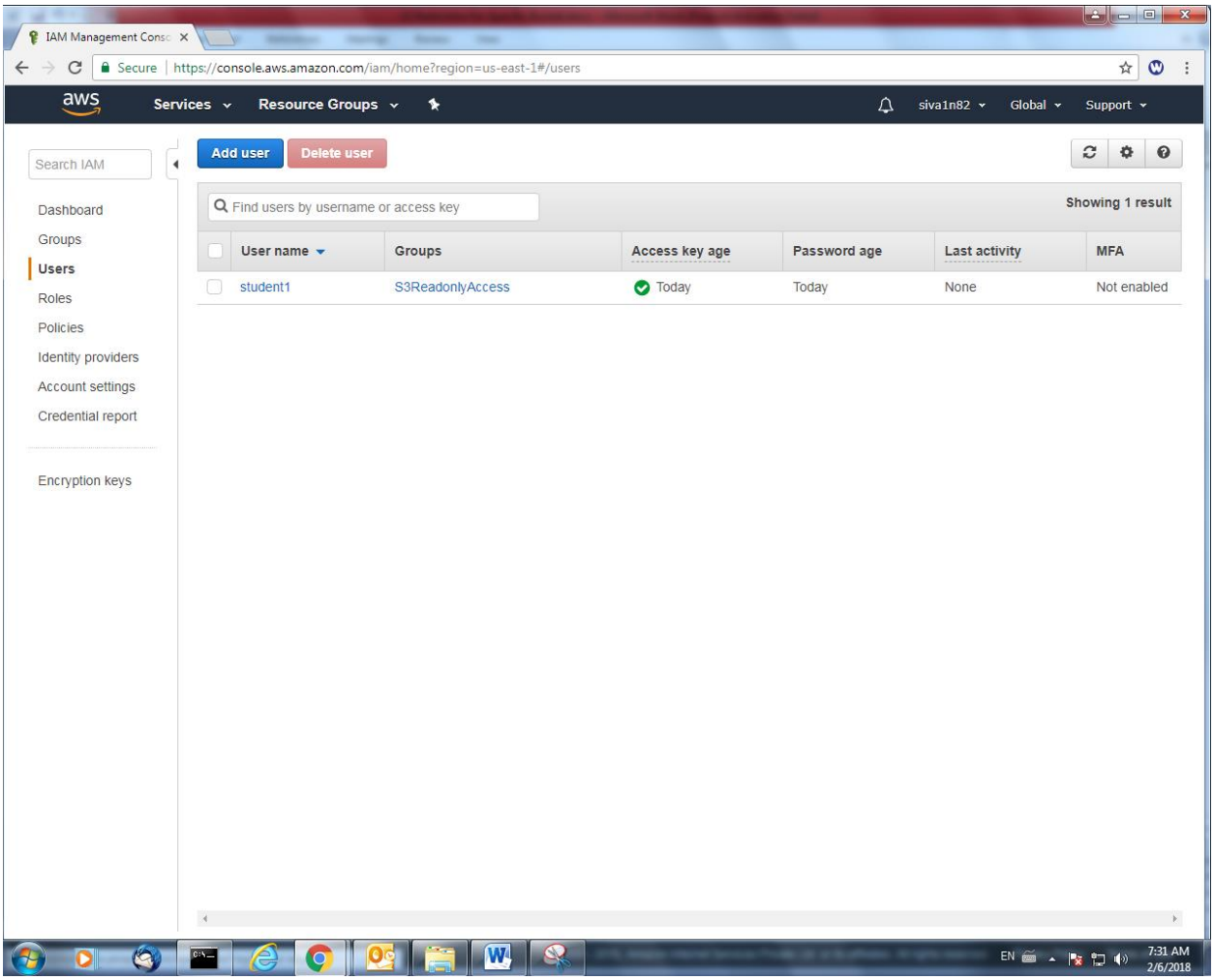
Type Name of Policy and Description.



Click “Create Policy”.

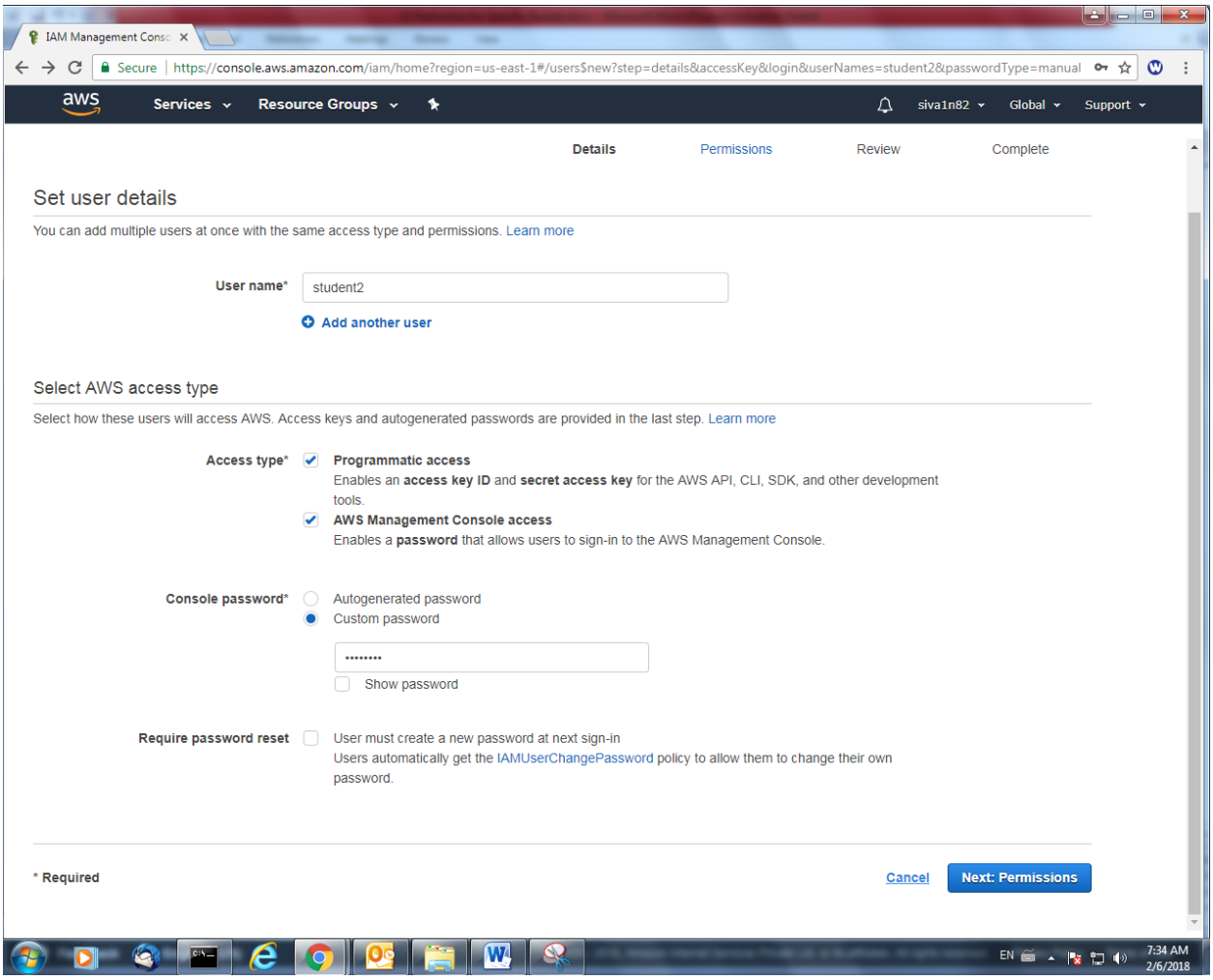
We need to create a user to assign the policy.

Click “Add user”.



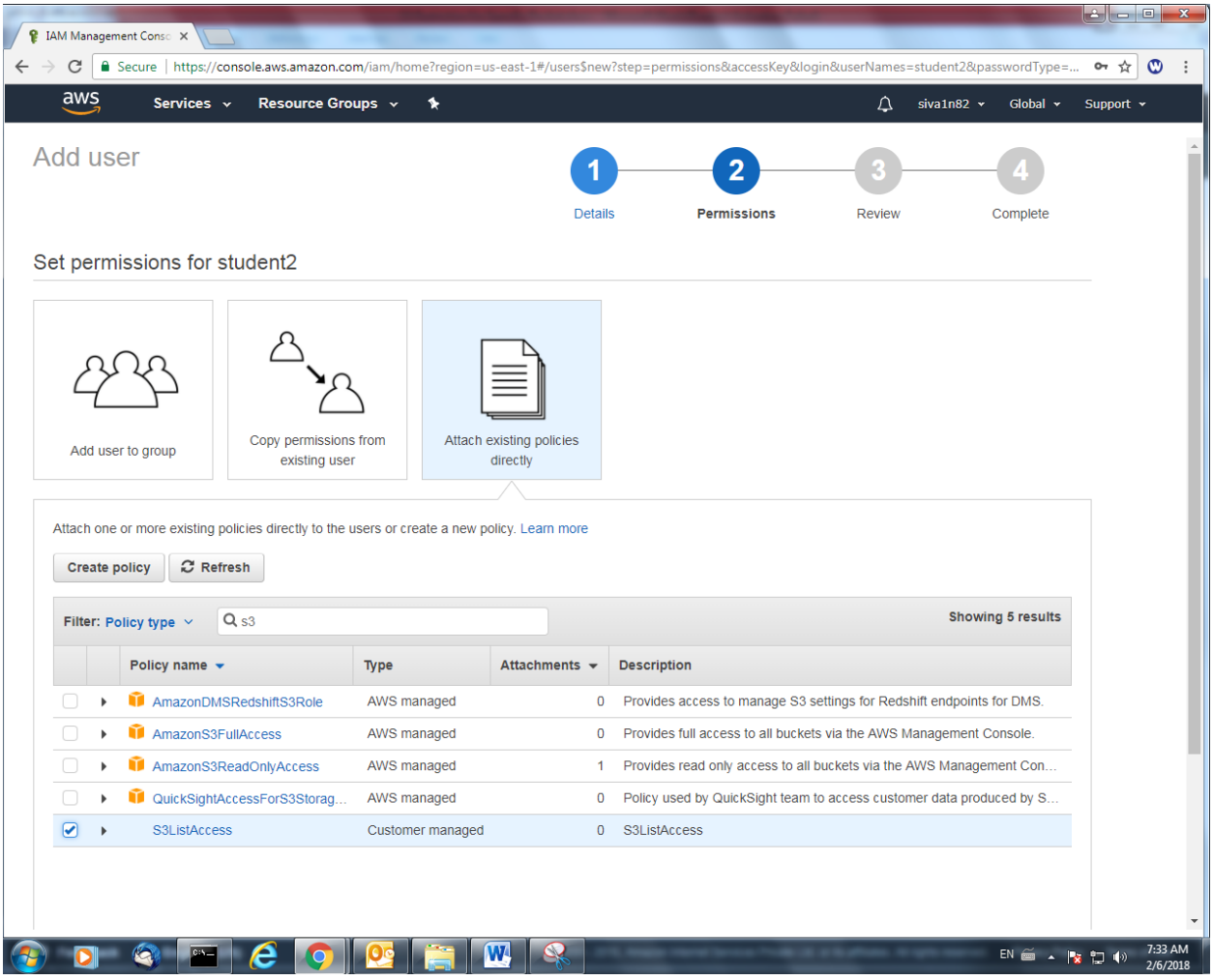
Username: student2

Access type : Programmatic access and AWS management console access.


IAM Management Conso
Secure | 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*
student2
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
EN
7:34 AM
2/6/2018

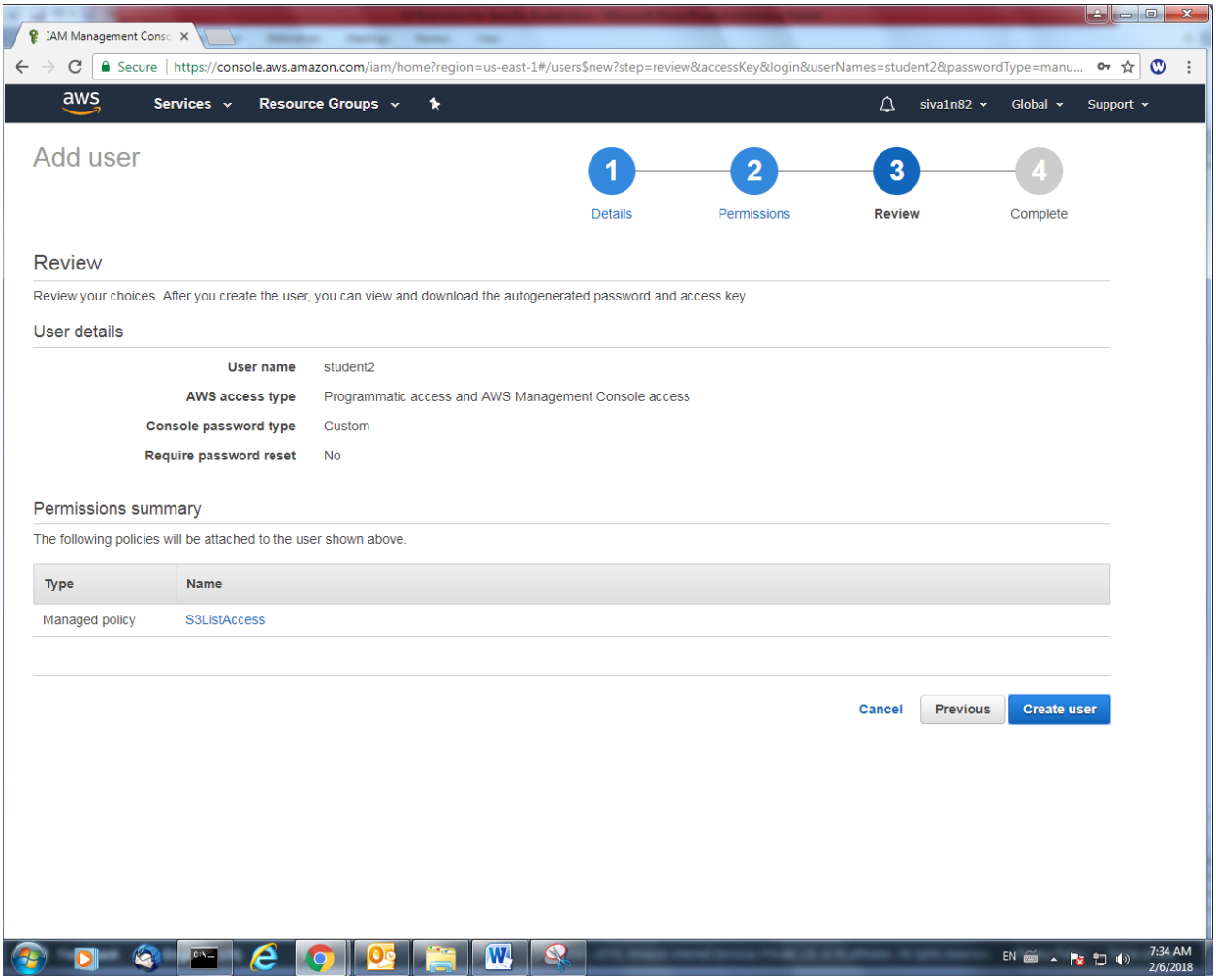
Click “Next”.

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

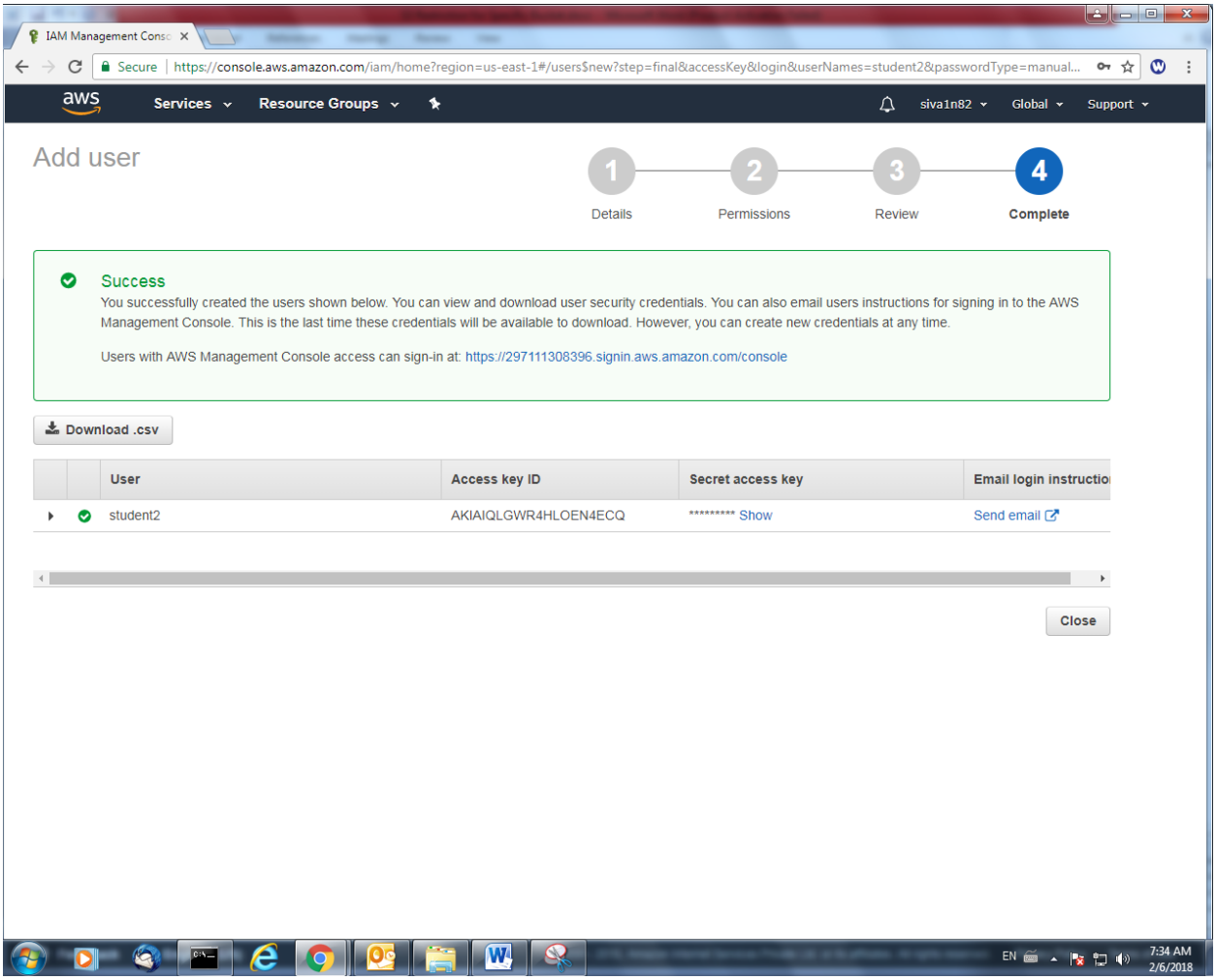


Click “Next”.

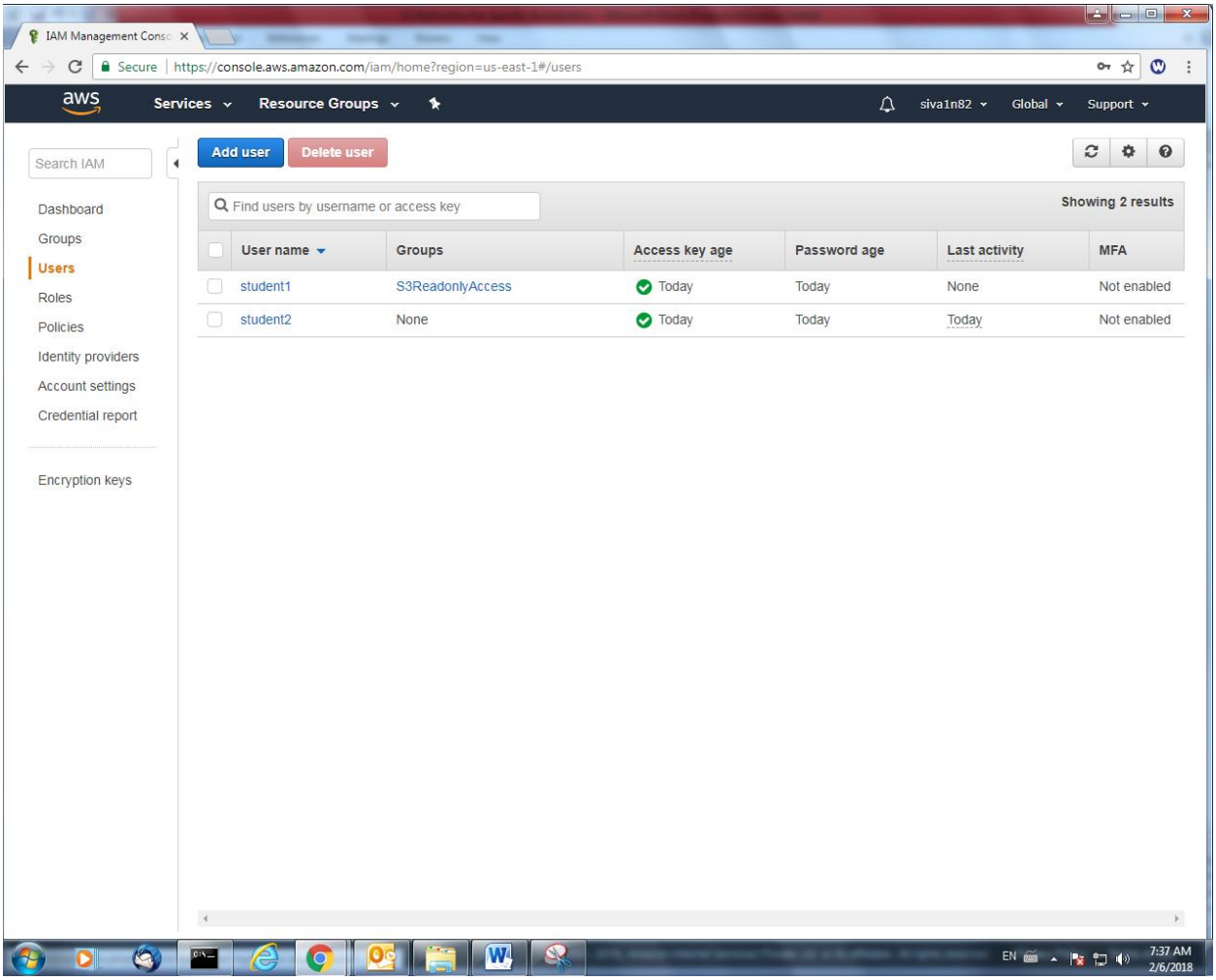
Click “Create user”.



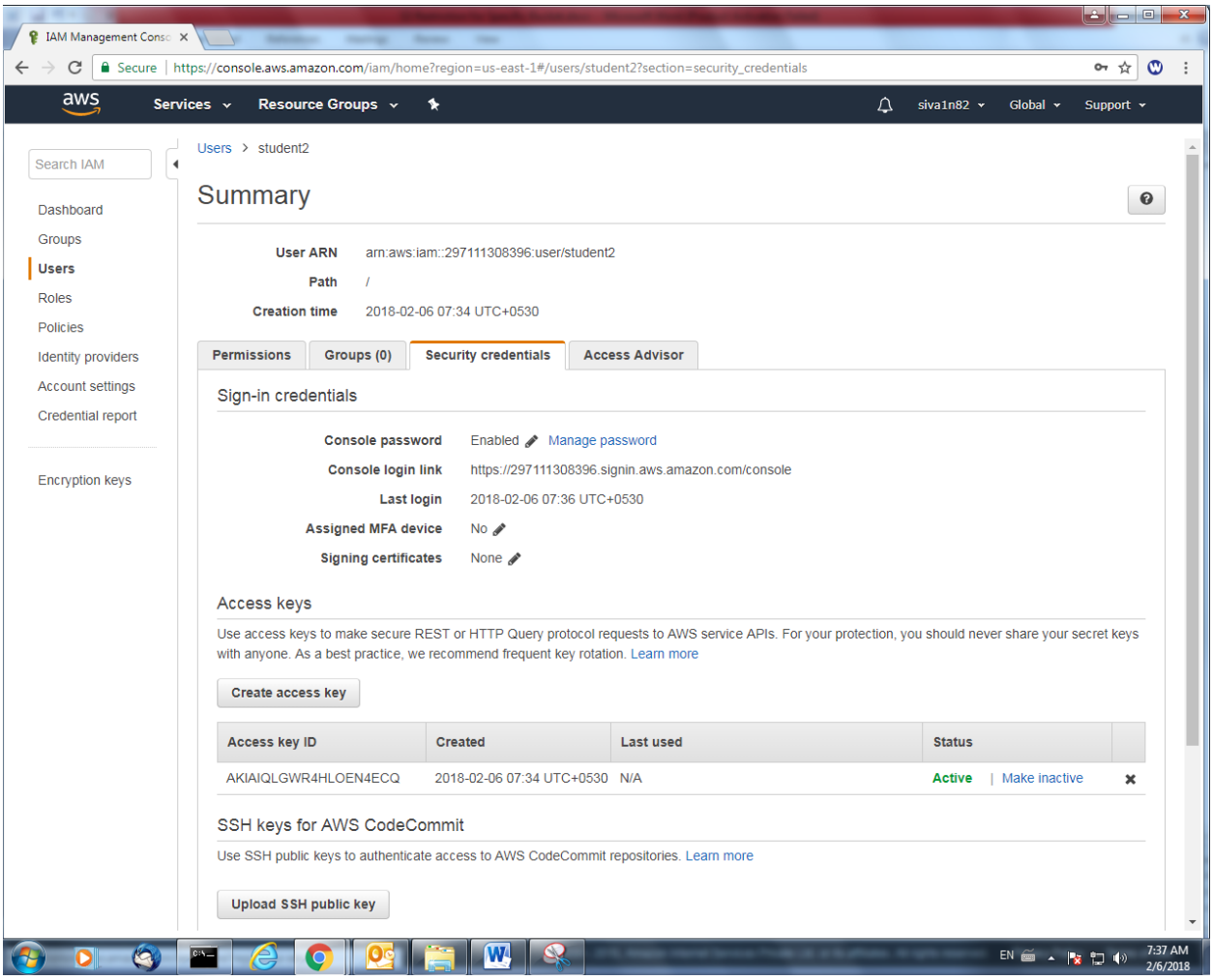
User successfully created. Please note that URL as below in box.



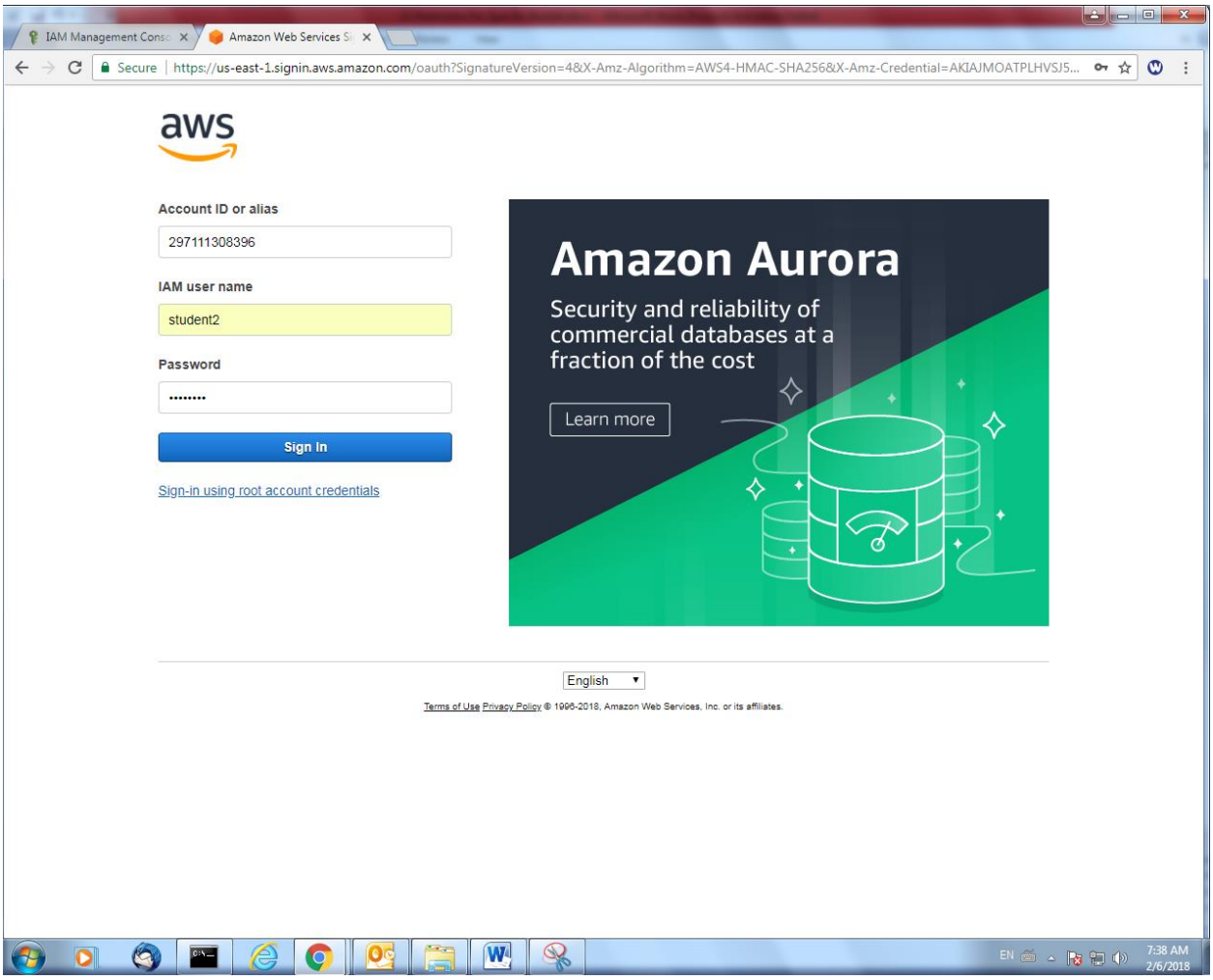
Click Users, and select student2 user.



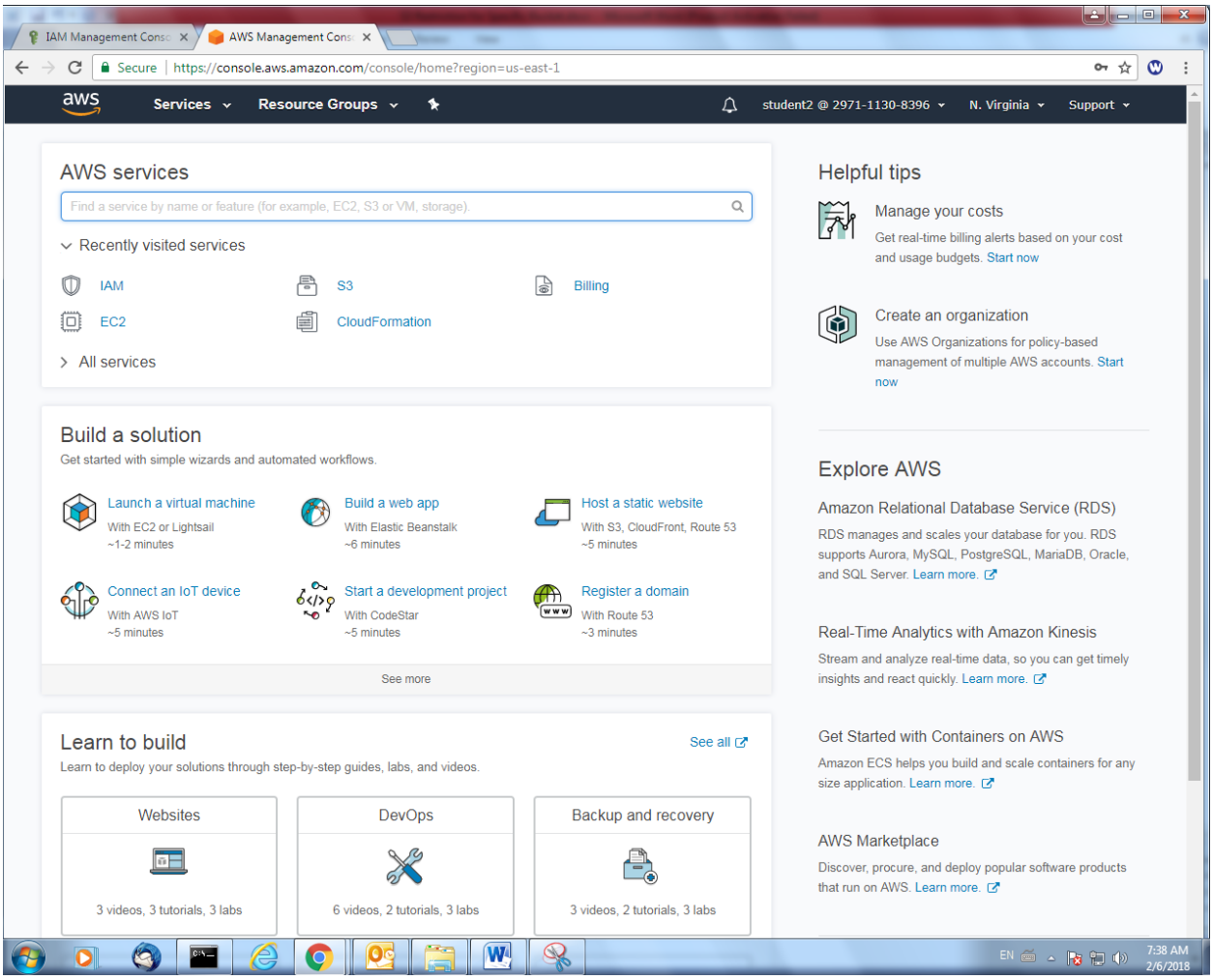
Clcik Security Credentials, copy the console login link and open that URL in new window.



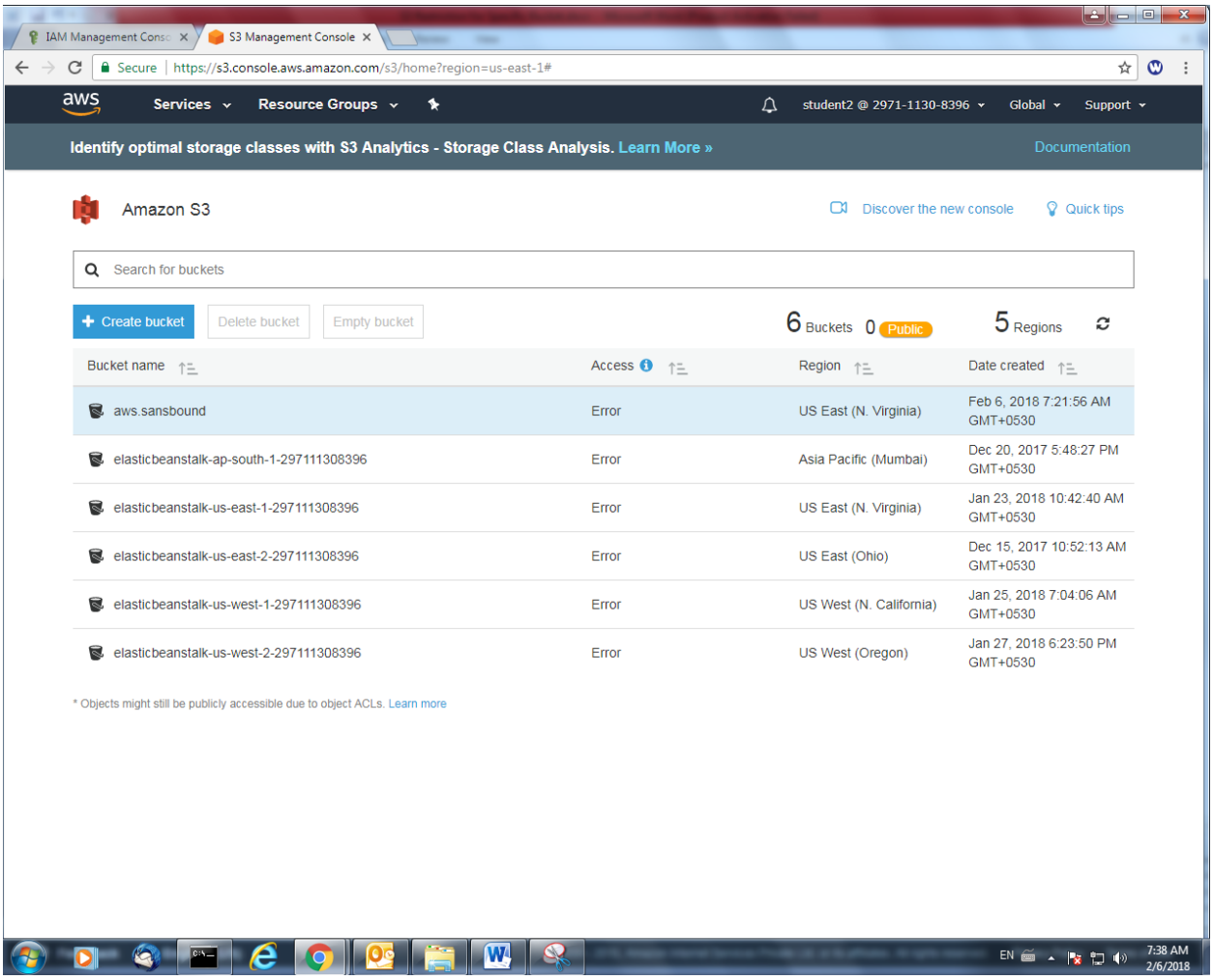
Type the login credentials of Student2.


IAM Management Cons
Amazon Web Services Si
Secure | https://us-east-1.signin.aws.amazon.com/oauth?SignatureVersion=4&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAJMOATPLHVSJ5...
aws
Account ID or alias
297111308396
IAM user name
student2
Password
Sign In
Sign-in using root account credentials
Amazon Aurora
Security and reliability of commercial databases at a fraction of the cost
Learn more
English
Terms of Use Privacy Policy © 1996-2018, Amazon Web Services, Inc. or its affiliates.
7:38 AM
2/6/2018

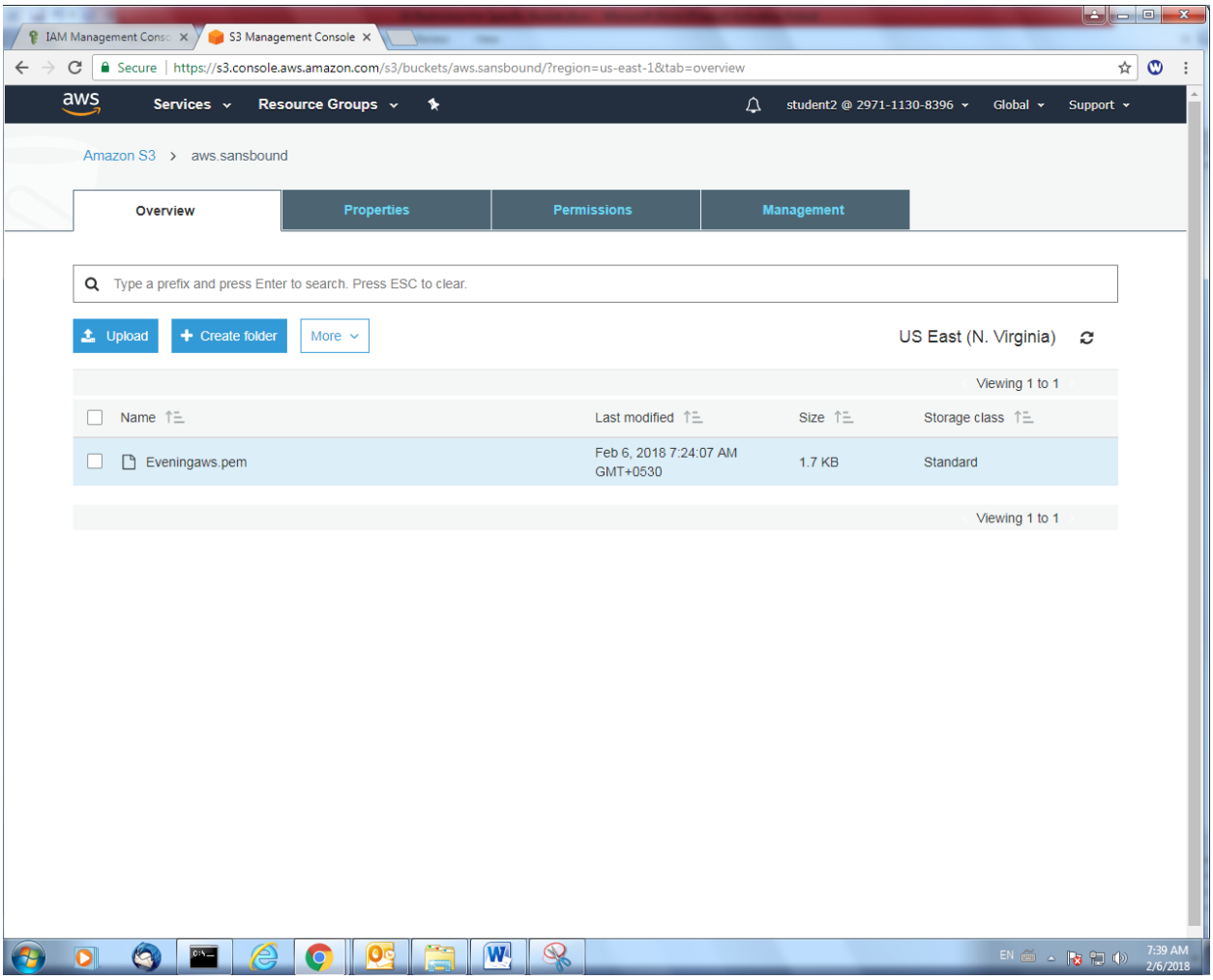
Click “S3”.



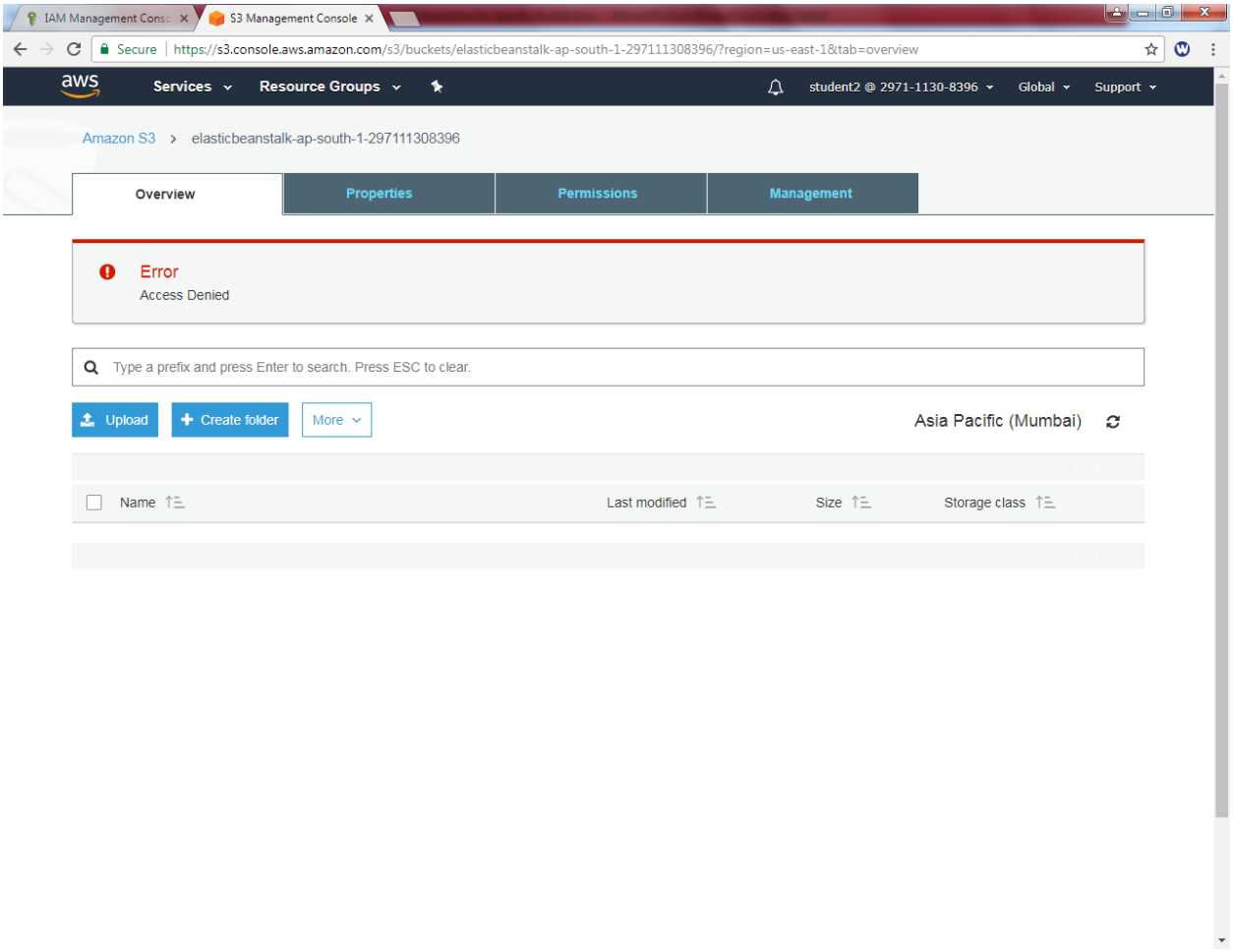
Click “aws.sansbound” bucket.



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.


IAM Management Conso
S3 Management Console
Secure | https://s3.console.aws.amazon.com/s3/buckets/elasticbeanstalk-ap-south-1-297111308396/?region=us-east-1&tab=overview
aws
Services
Resource Groups
student2 @ 2971-1130-8396
Global
Support
Amazon S3 > elasticbeanstalk-ap-south-1-297111308396
Overview
Properties
Permissions
Management
Error
Access Denied
Type a prefix and press Enter to search. Press ESC to clear.
Upload
Create folder
More
Asia Pacific (Mumbai)
Name
Last modified
Size
Storage class