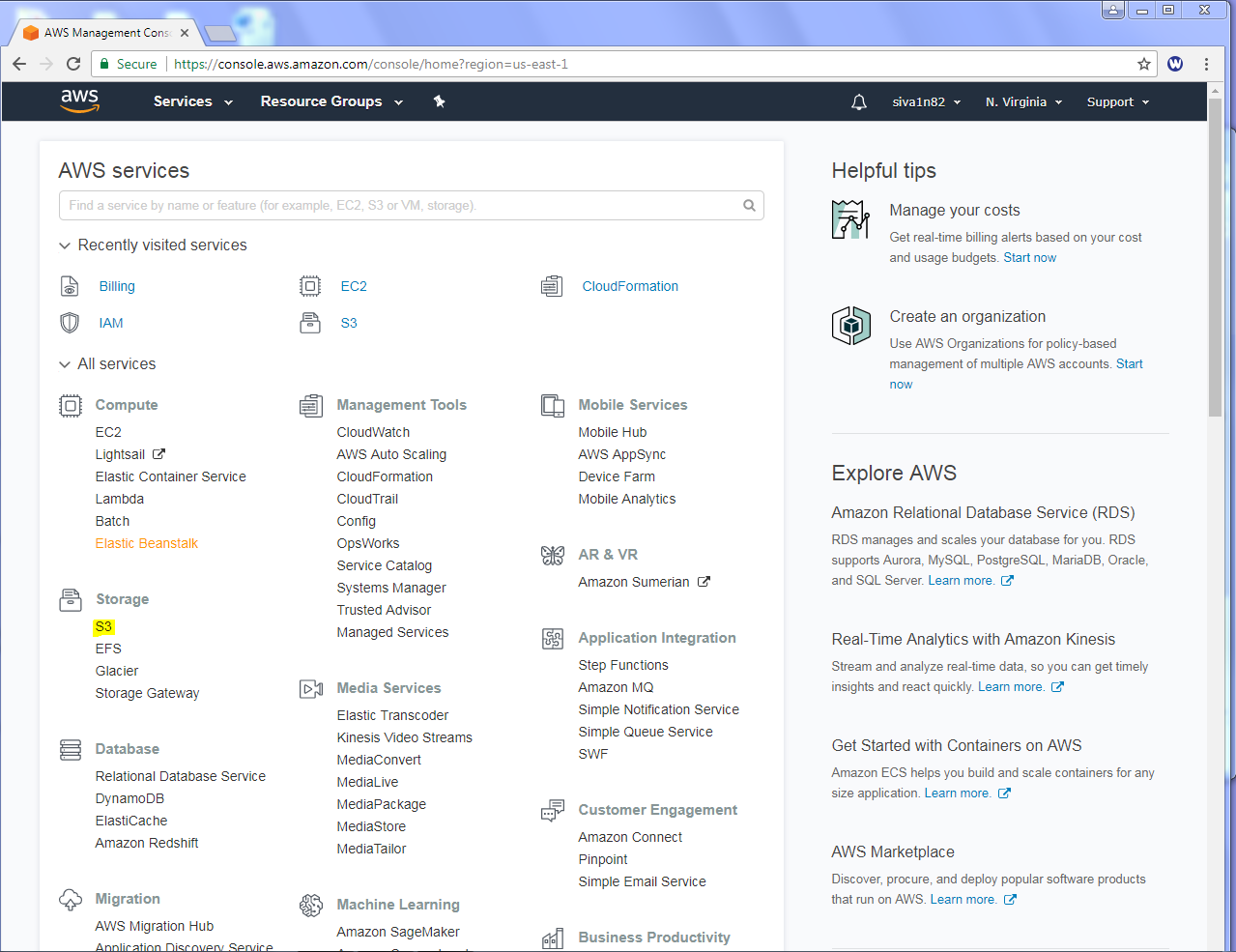
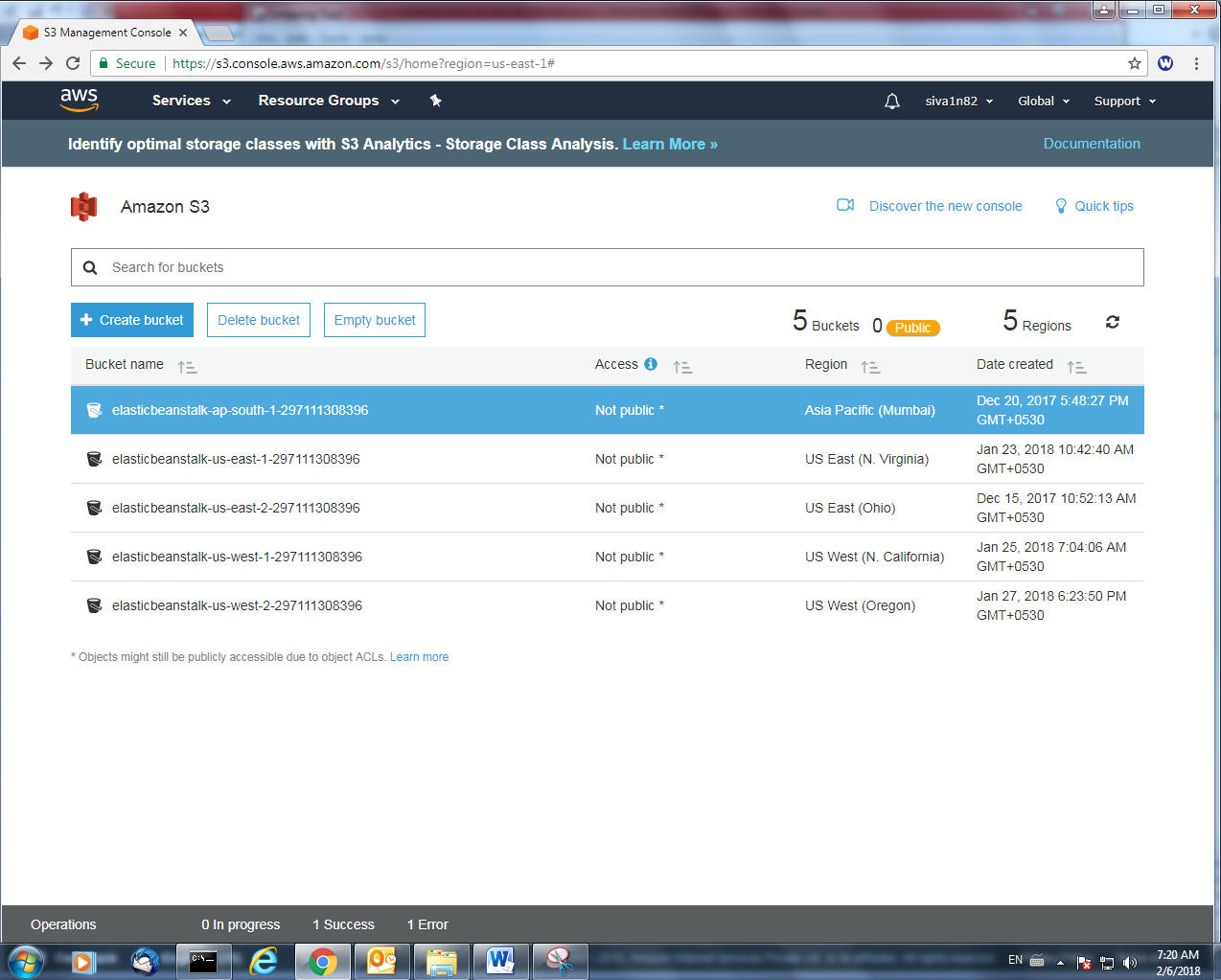
**Lab24**

**S3 Restriction for Specific Bucket**

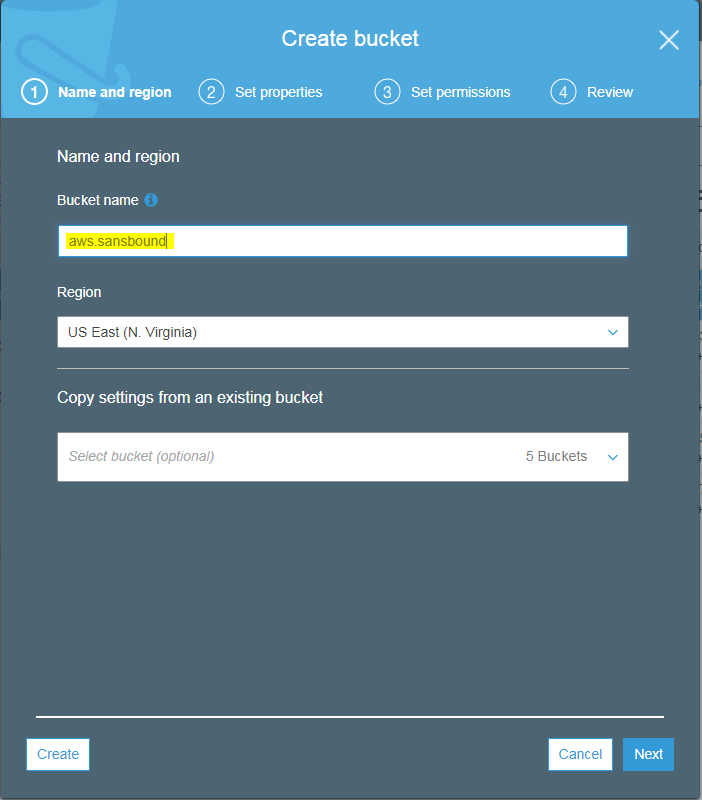
Click “S3”service



Click “Create bucket” with unique name.

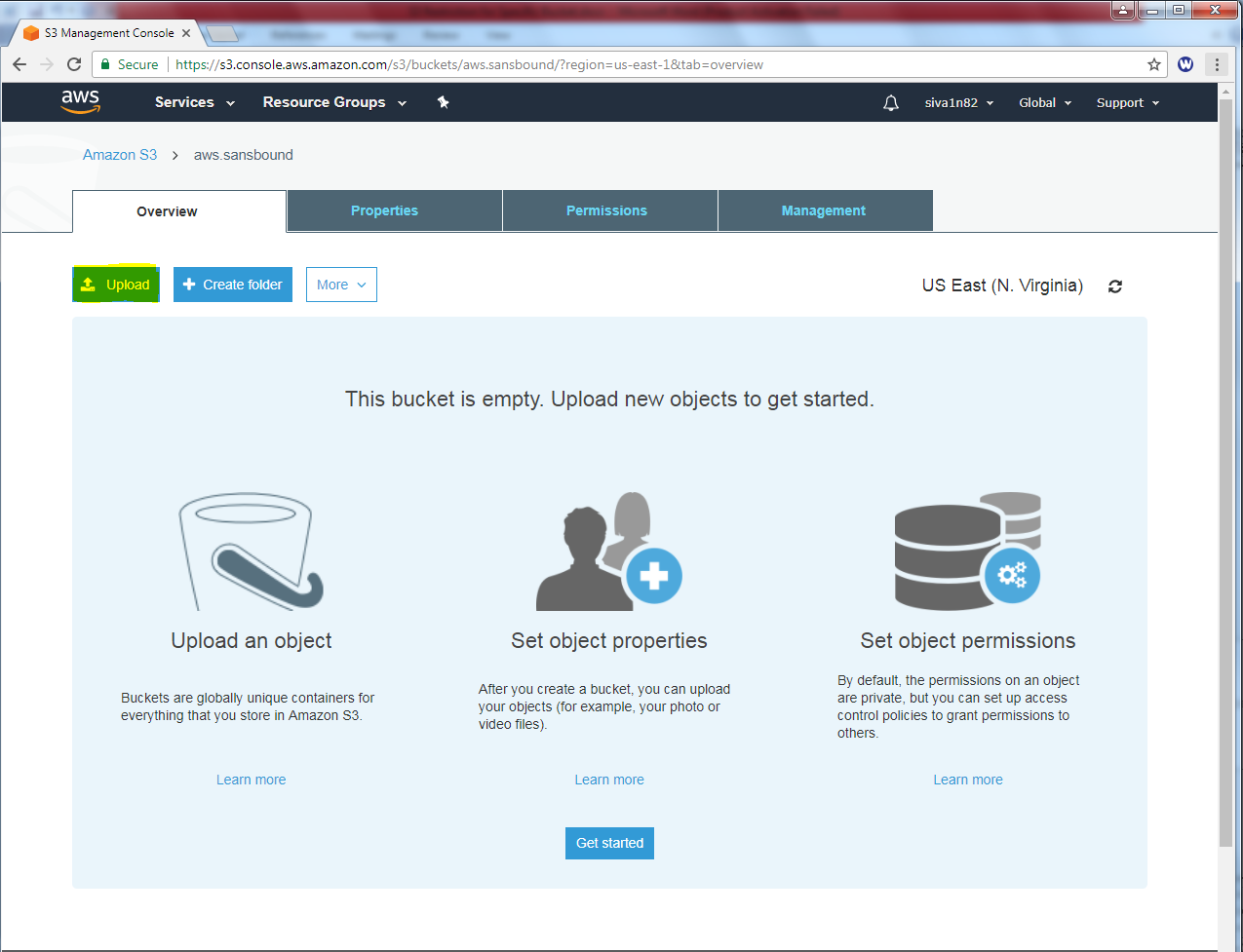


Type aws.sansbound.com

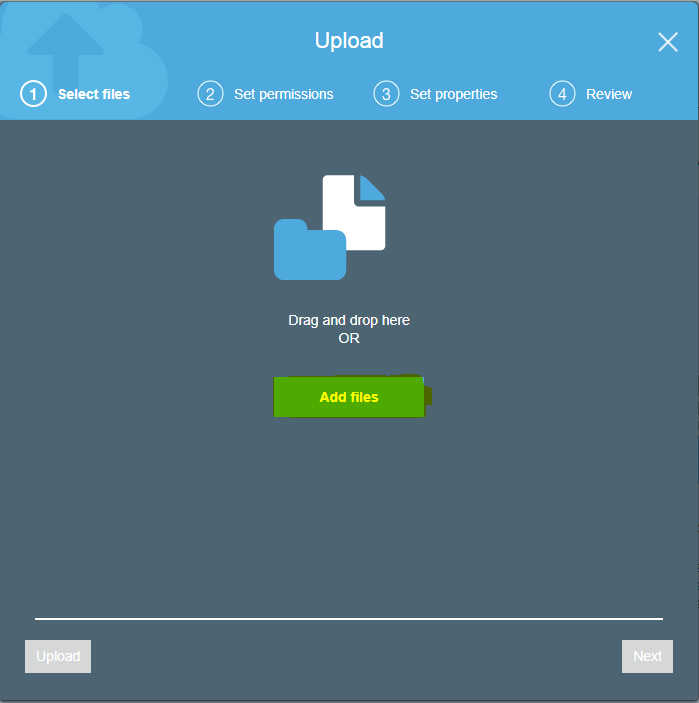


Click “Create”.

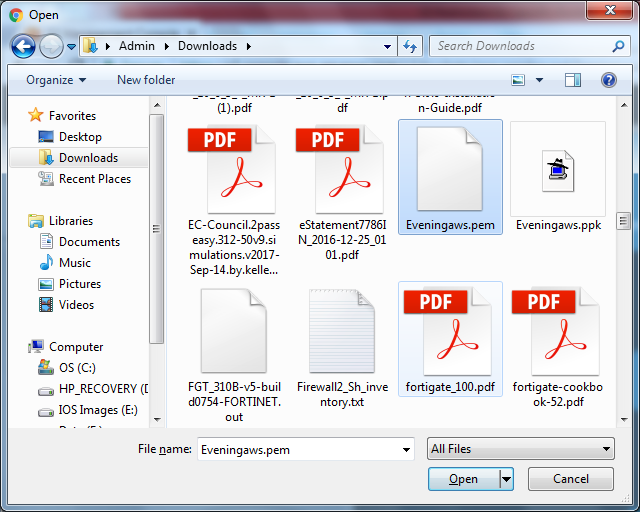
Click “Upload”.



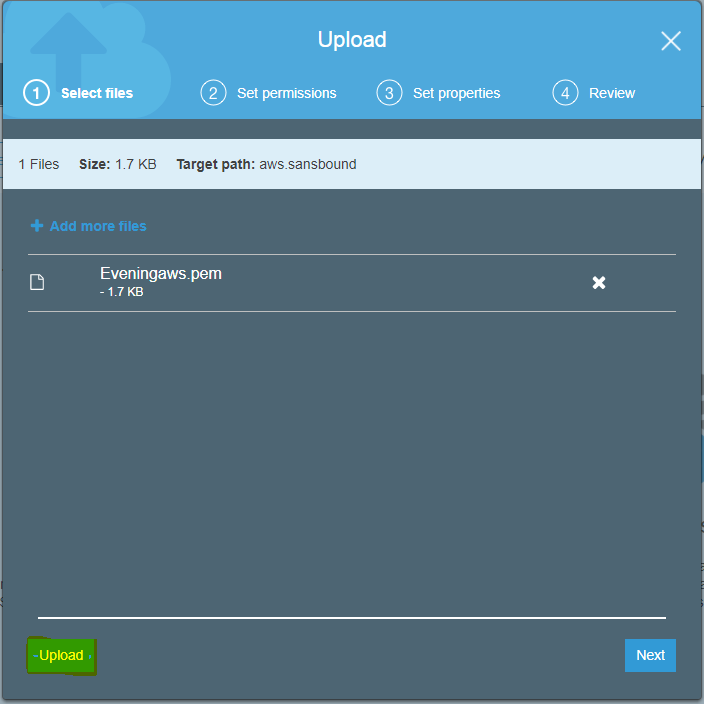
Click “Add files”.



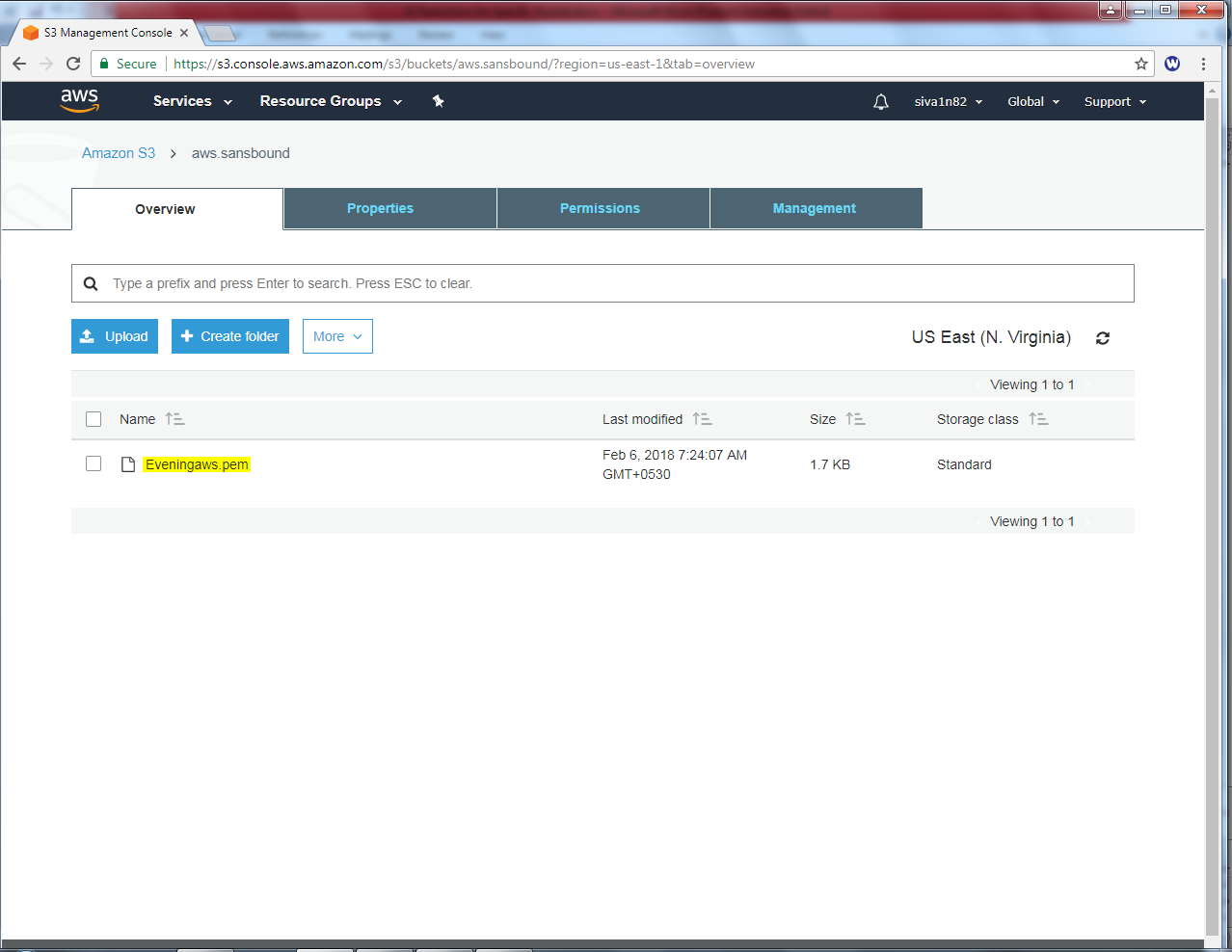
Locate the file and click open.



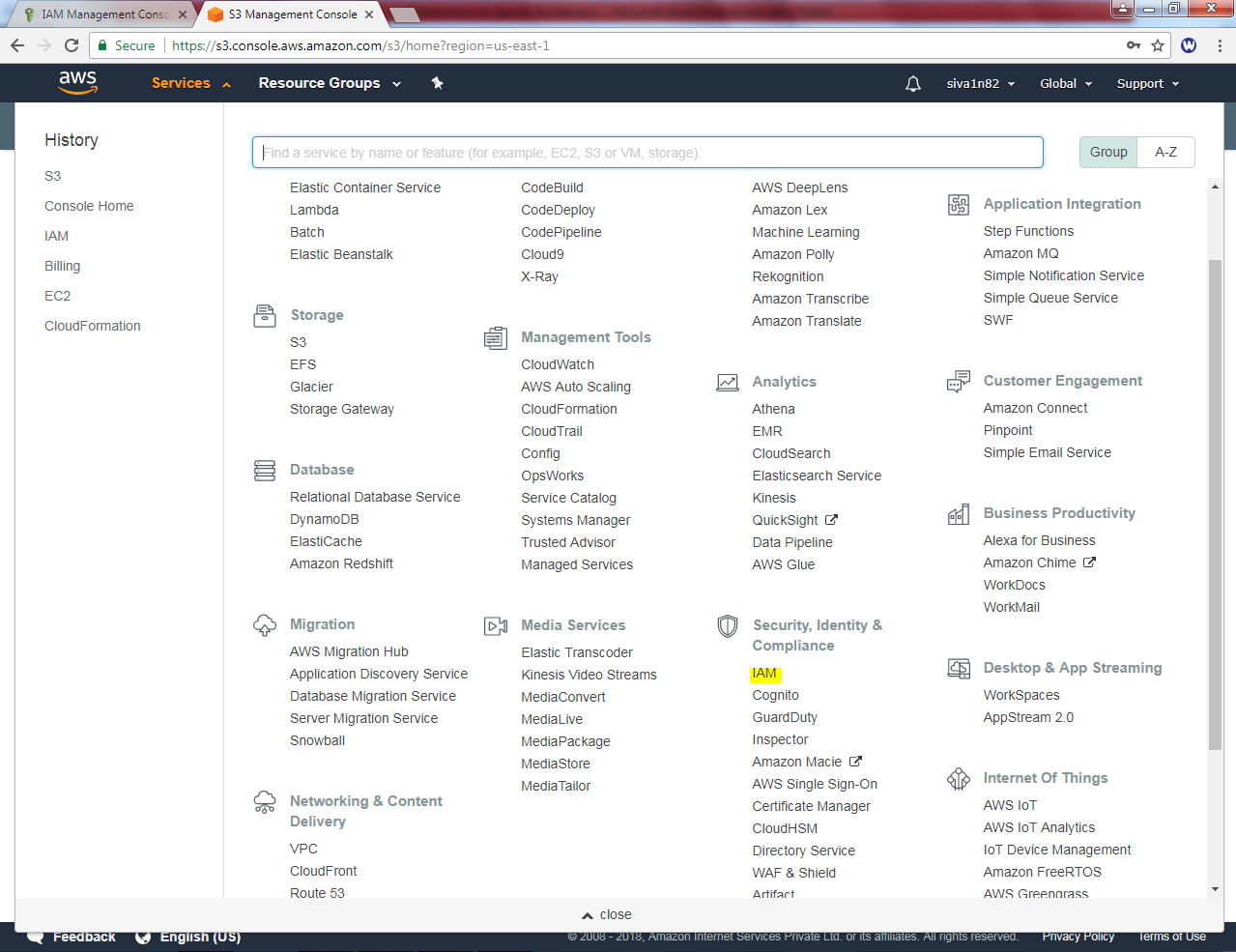
Click “Upload” to upload the file.



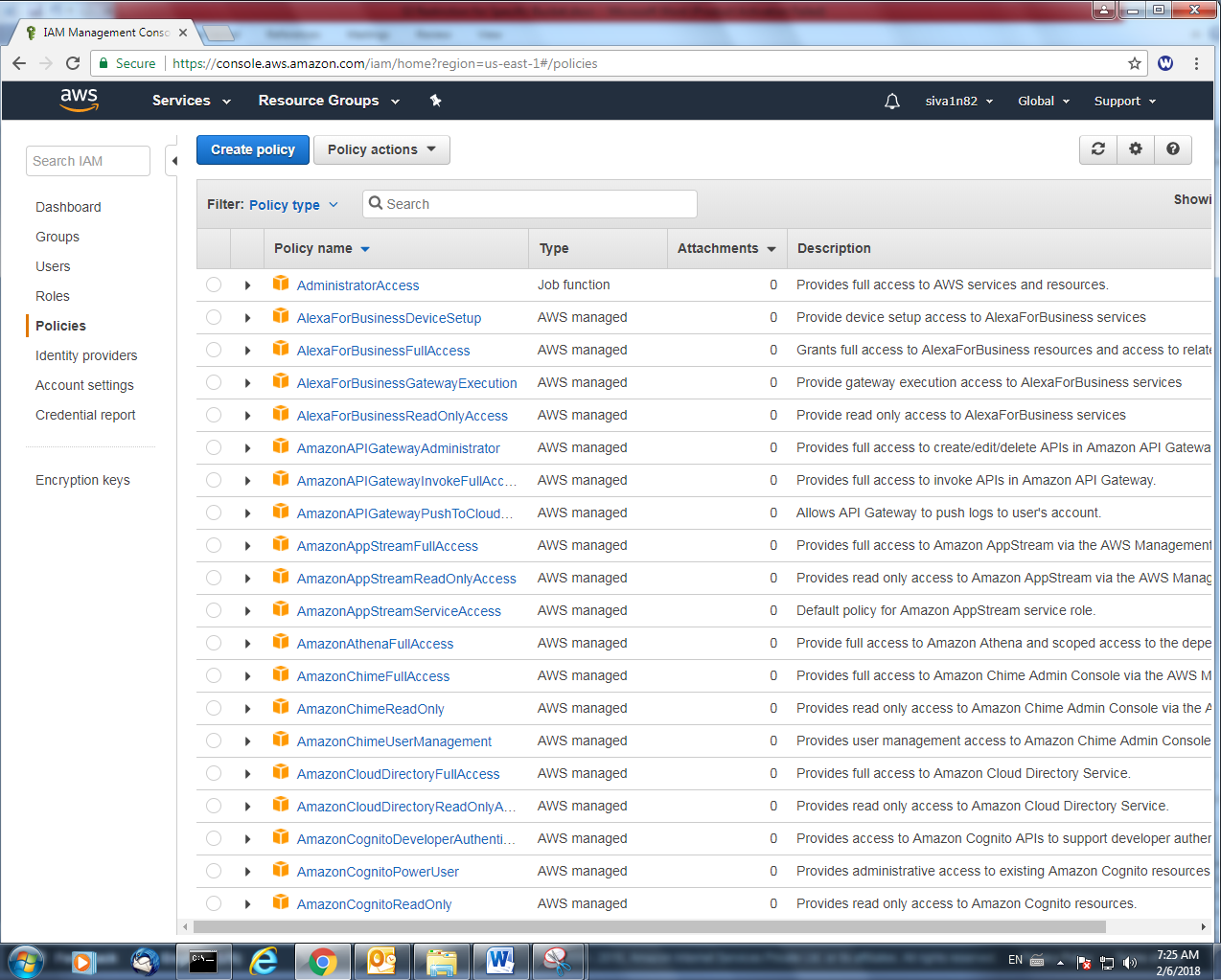
We can able view the file.



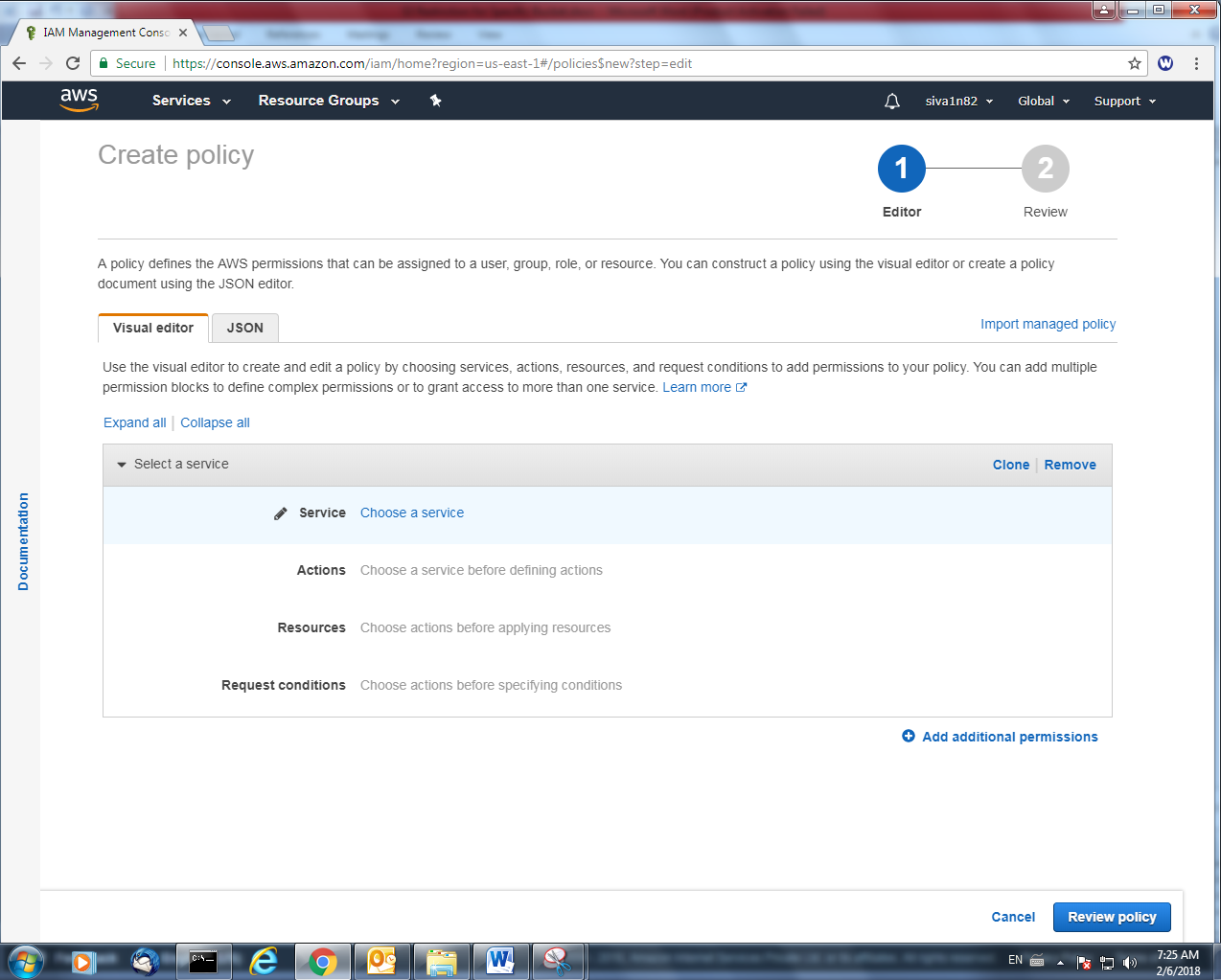
Click “IAM” Role.



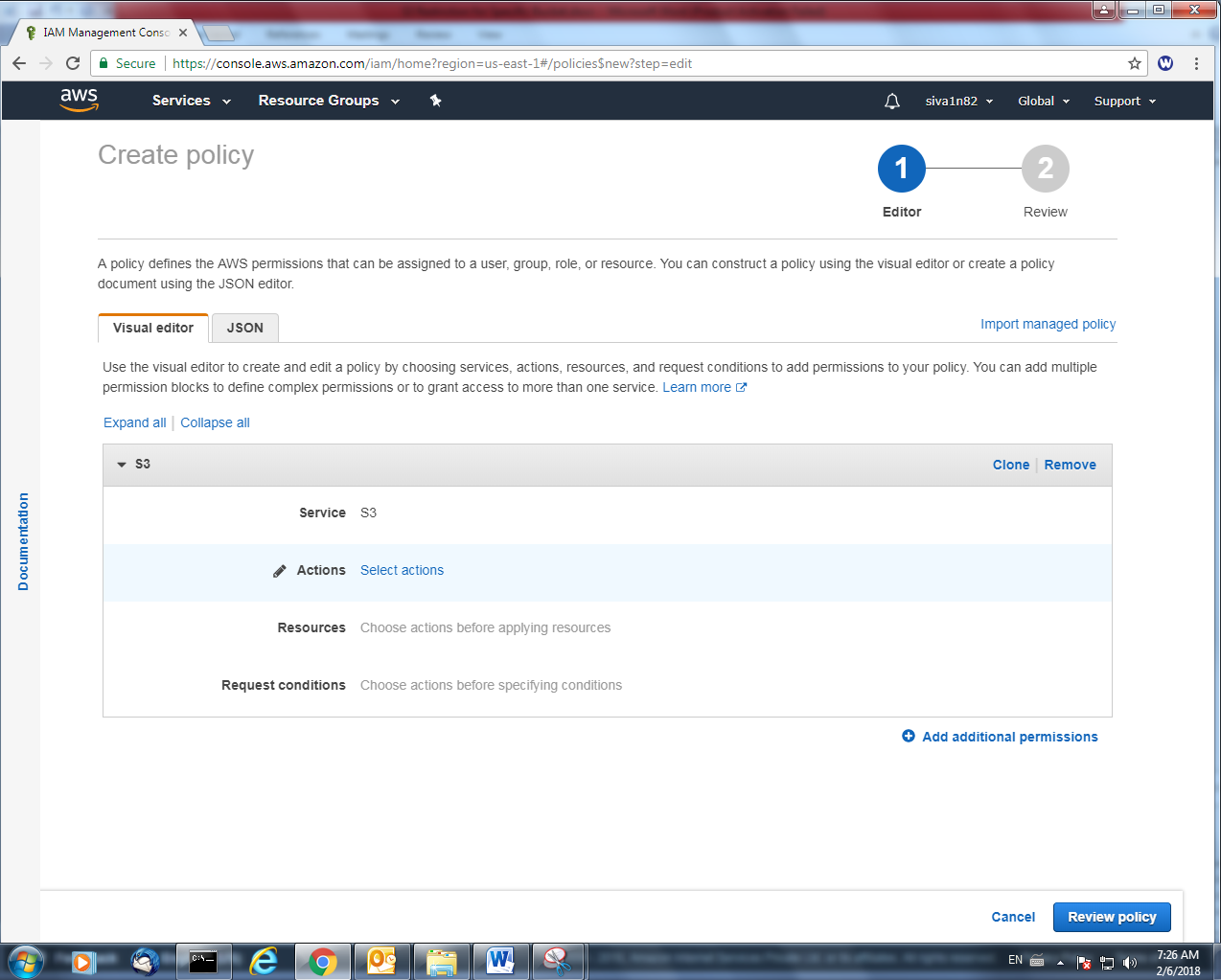
Click “Create Policy”.



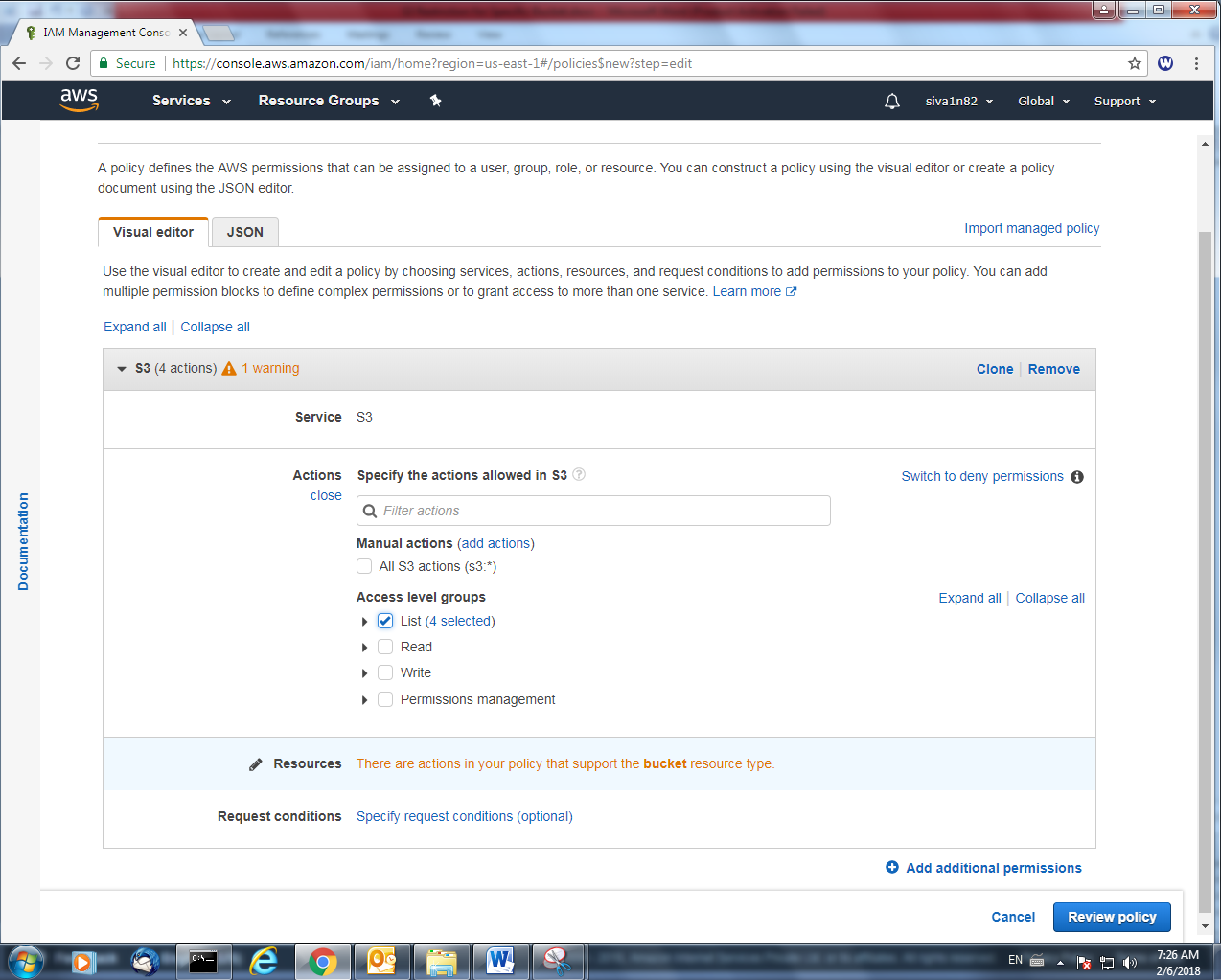
Click “Choose a service” and



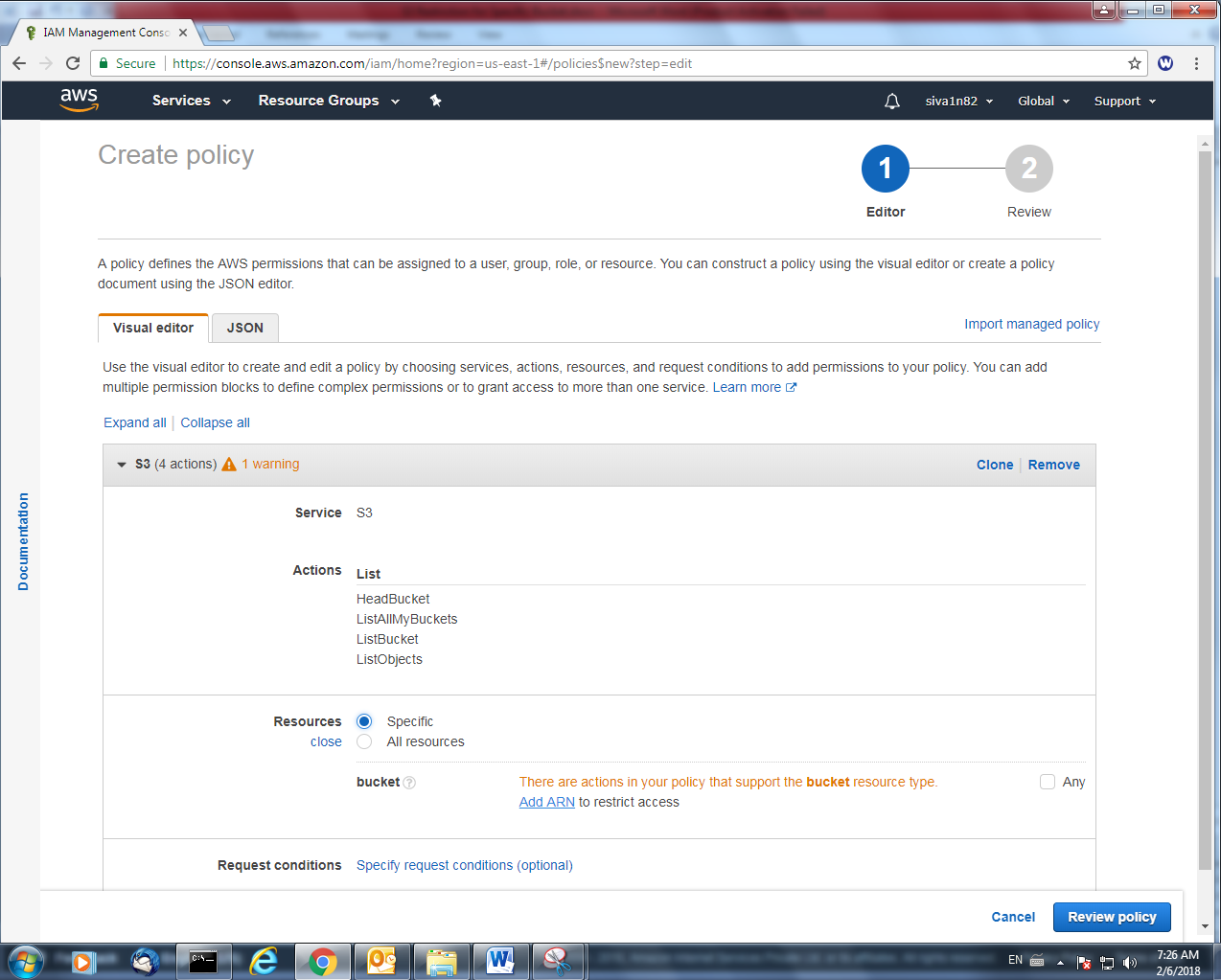
choose the S3 service and click Select actions.



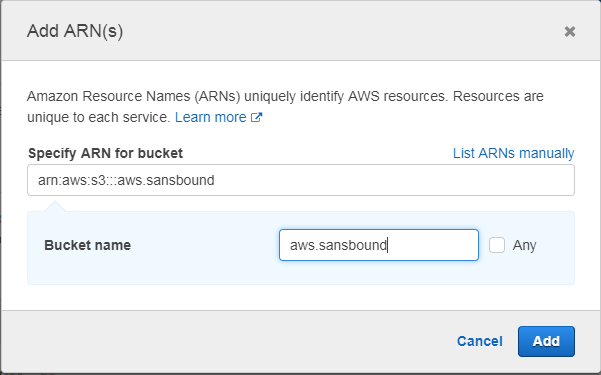
Access level groups, check “List” and click “There are action in your policy that support the bucket resource type.



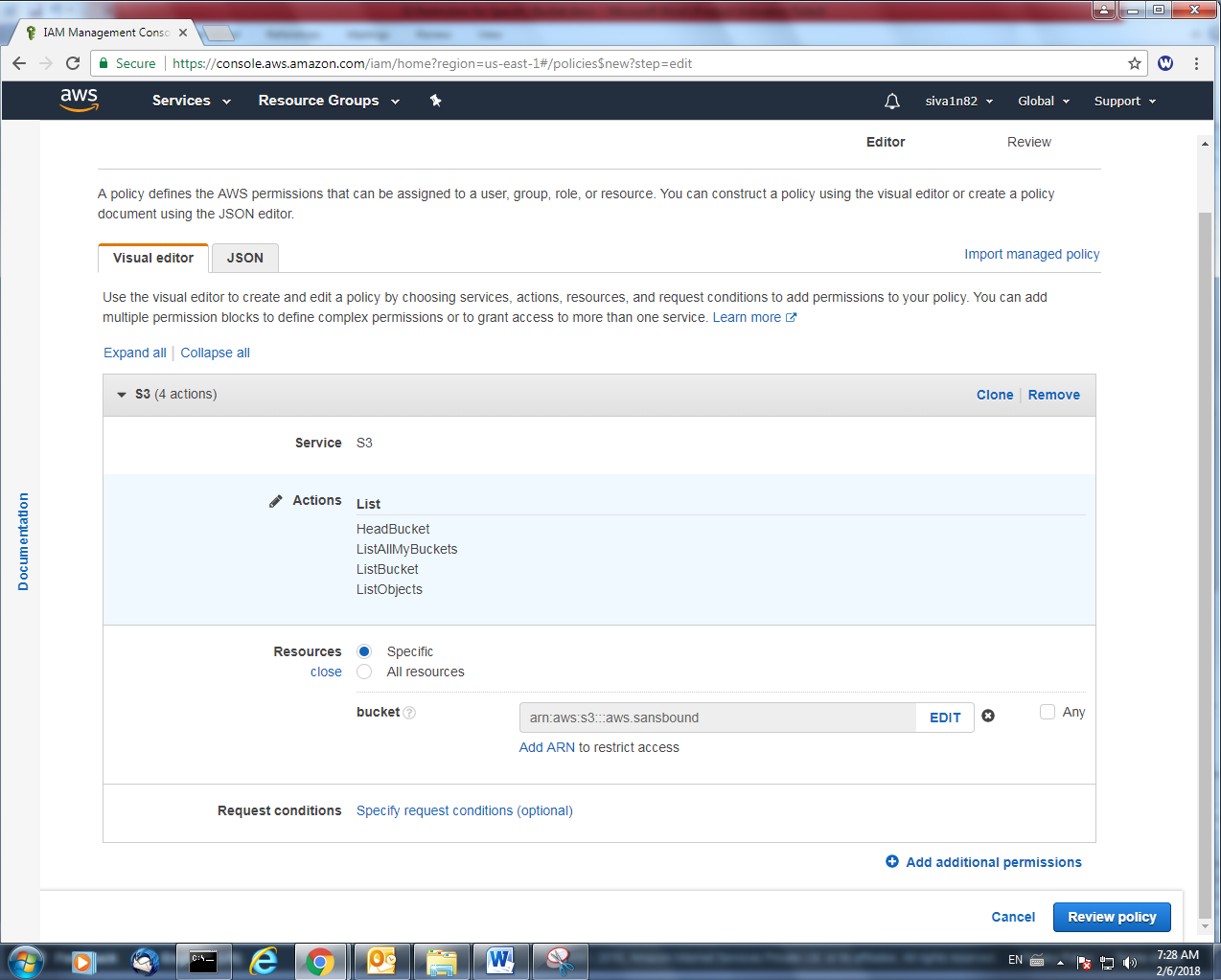
Click specific option and click “Add ARN” to add the bucket name.

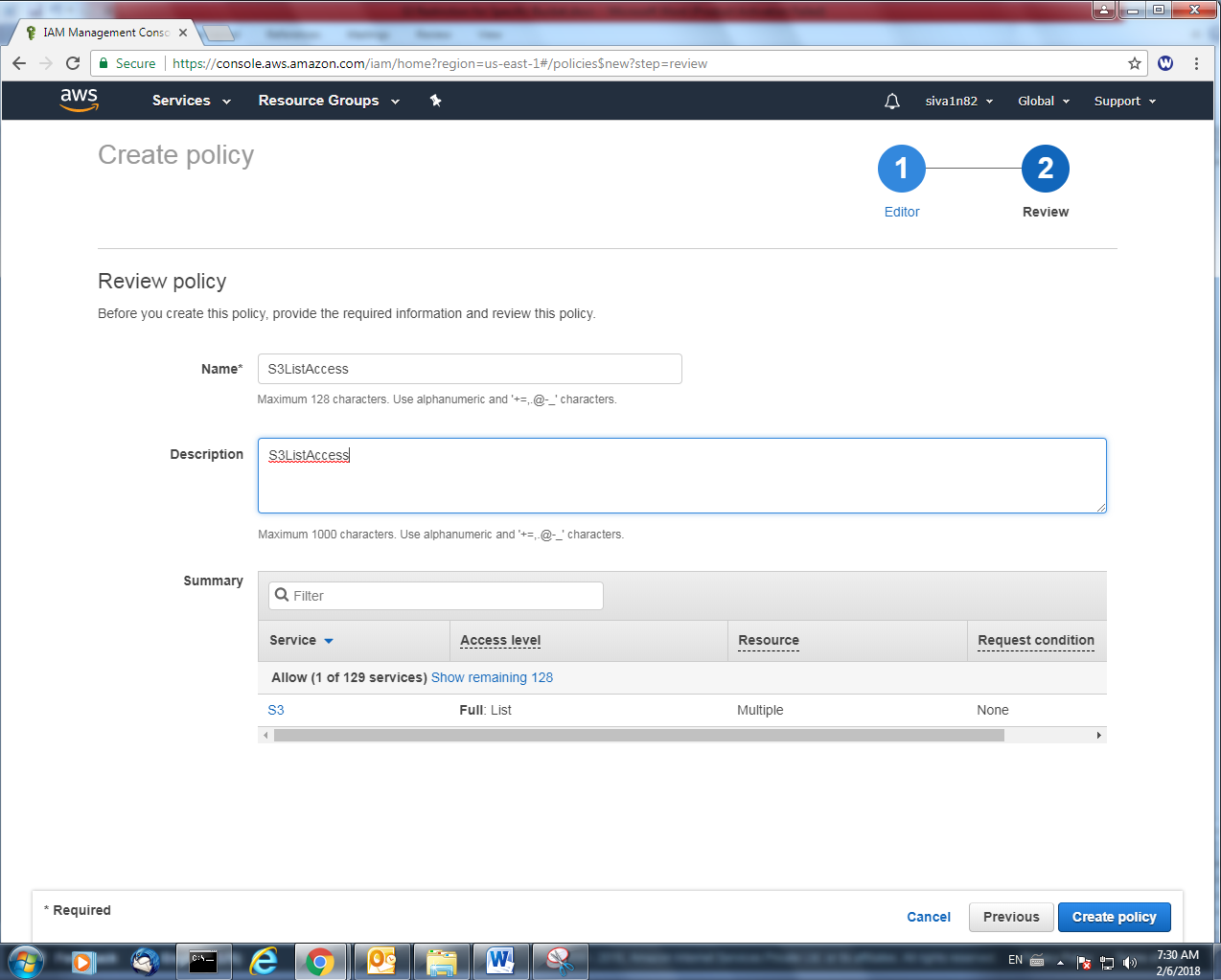


Type the bucket name and click “Add”.



Click “Review Policy”.

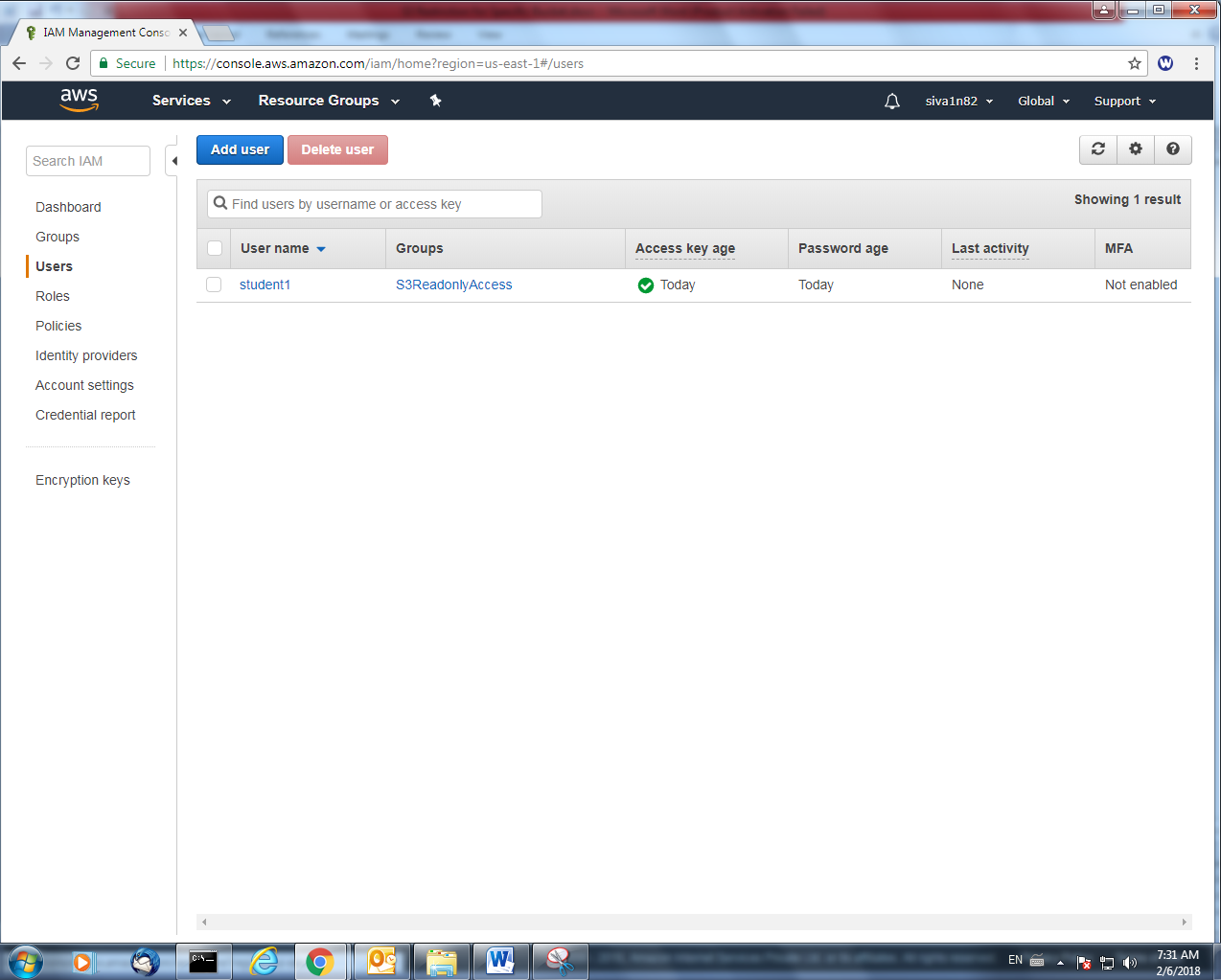


Type Name of Policy and Description.

Click “Create Policy”.

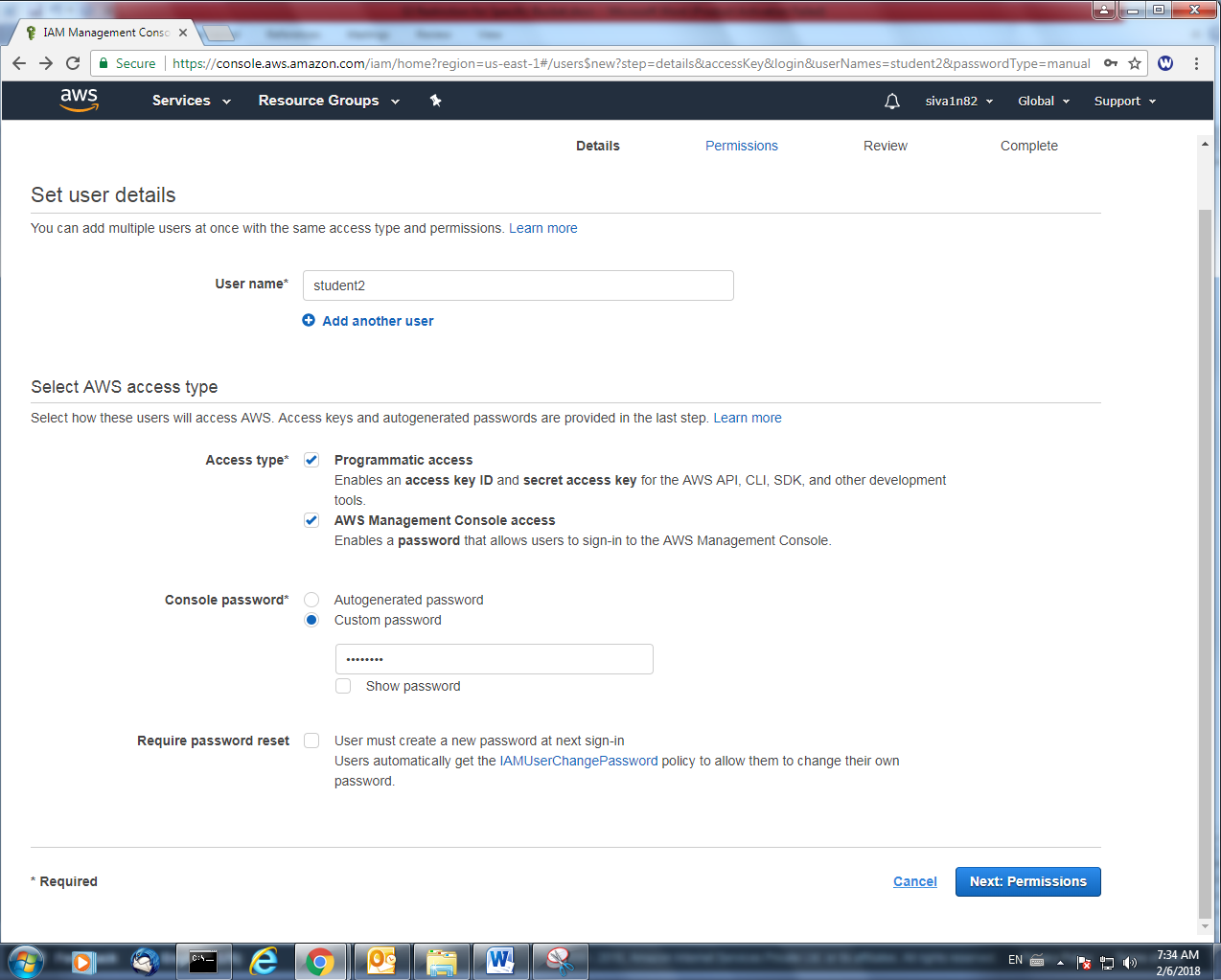
We need to create a user to assign the policy.

Click “Add user”.



Username: student2

Access type : Programmatic access and AWS management console access.

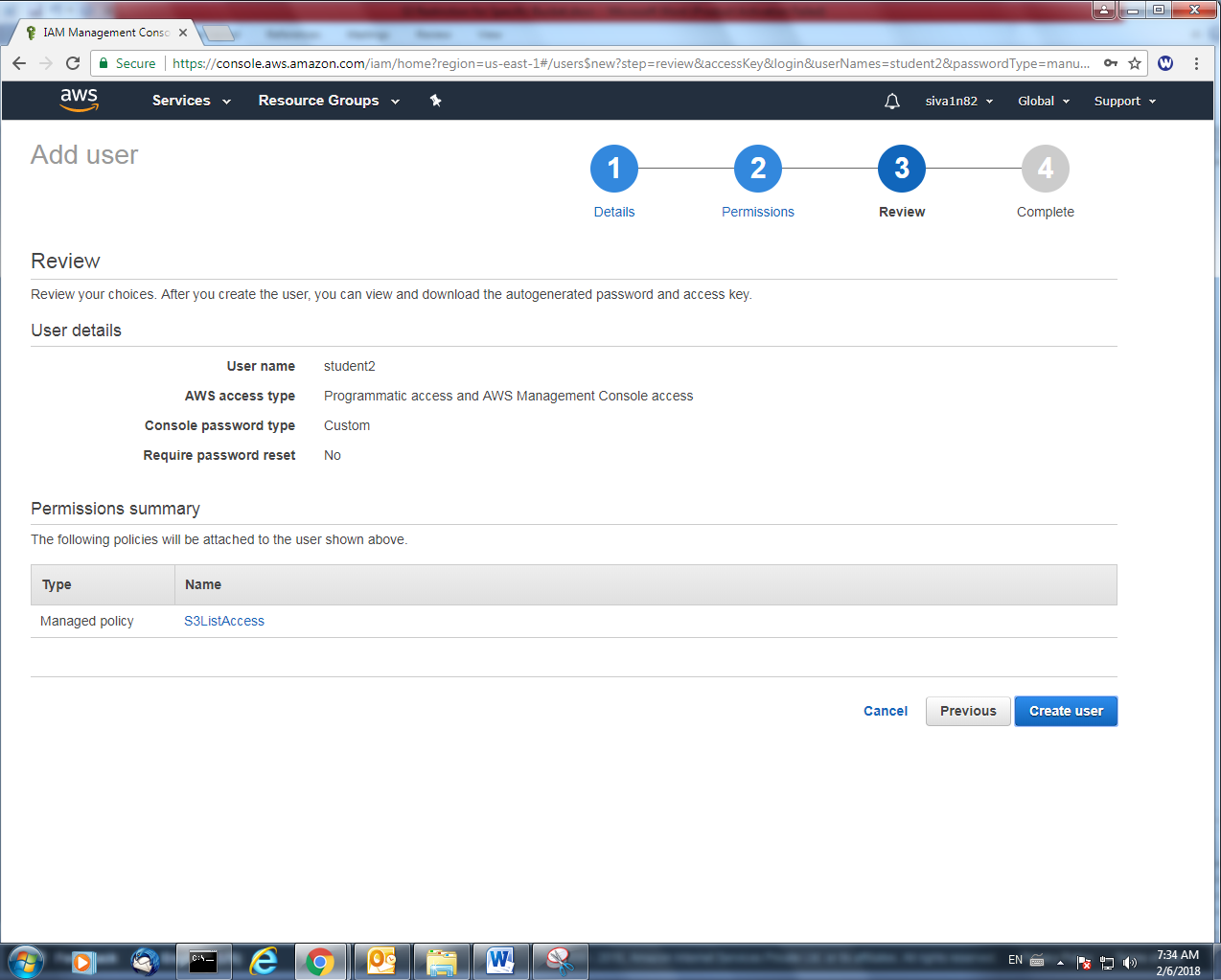


Click “Next”.

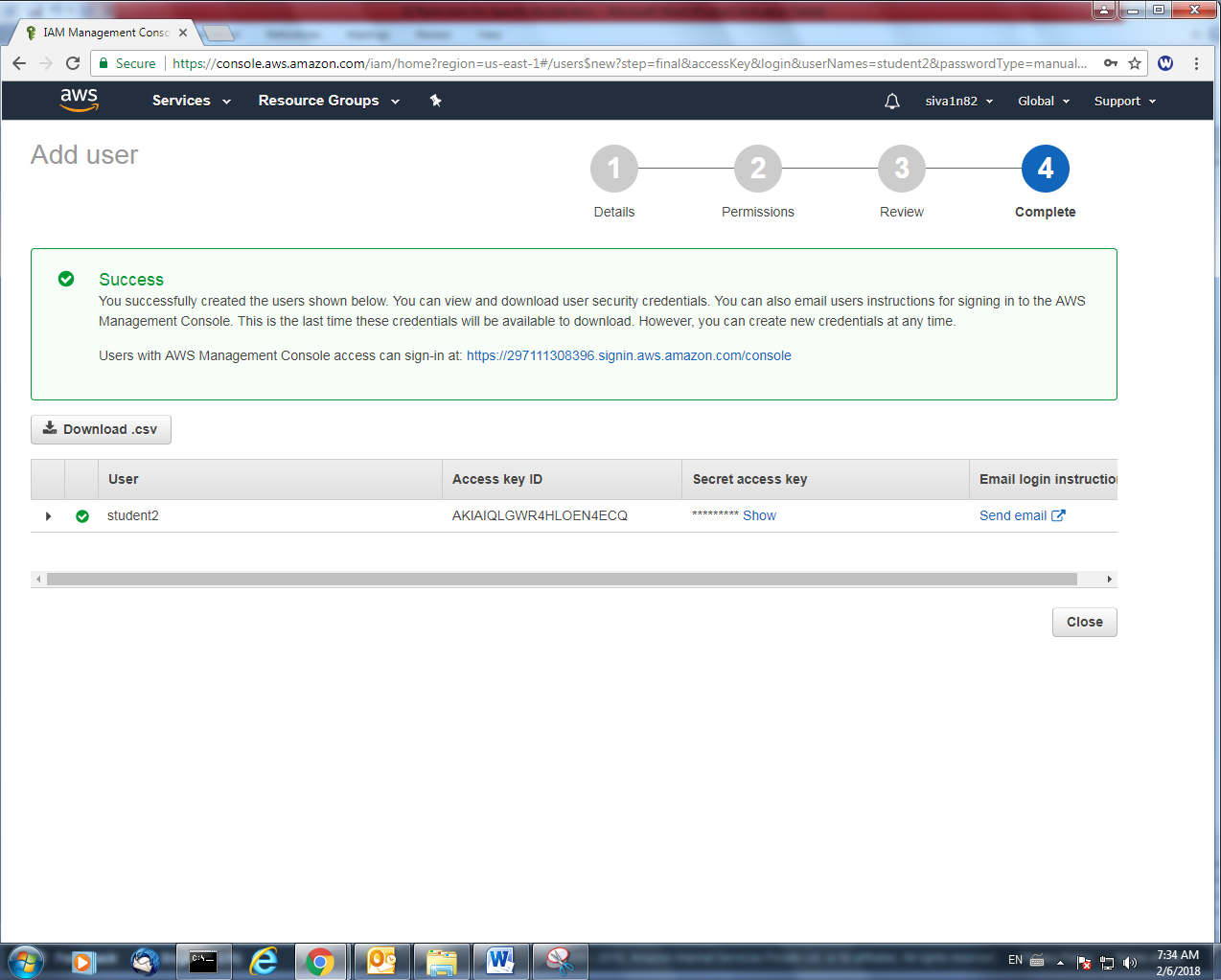
In Policy type, type “s3” to filter the s3 policies. Select the policy which we created.

Click “Next”.

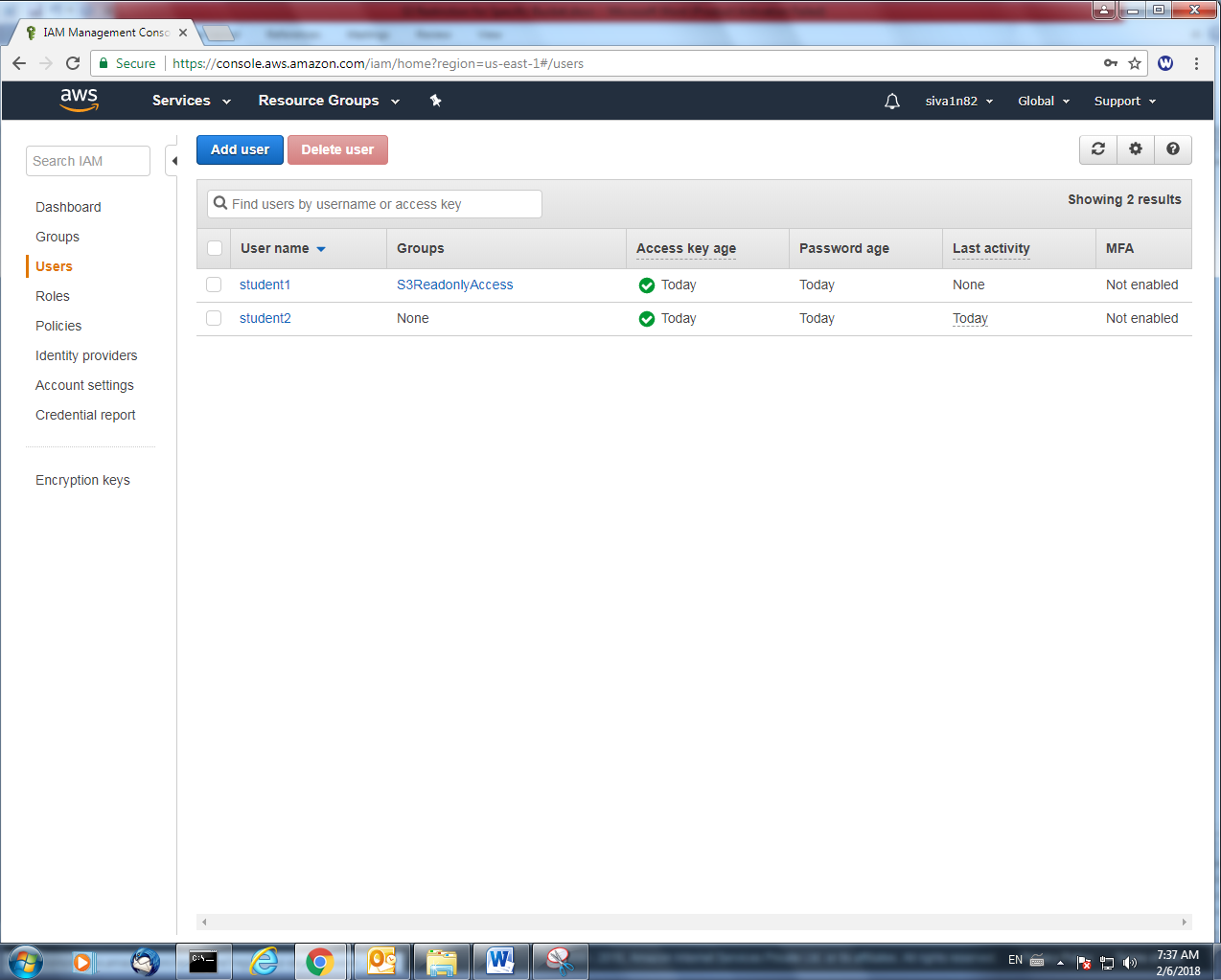
Click “Create user”.



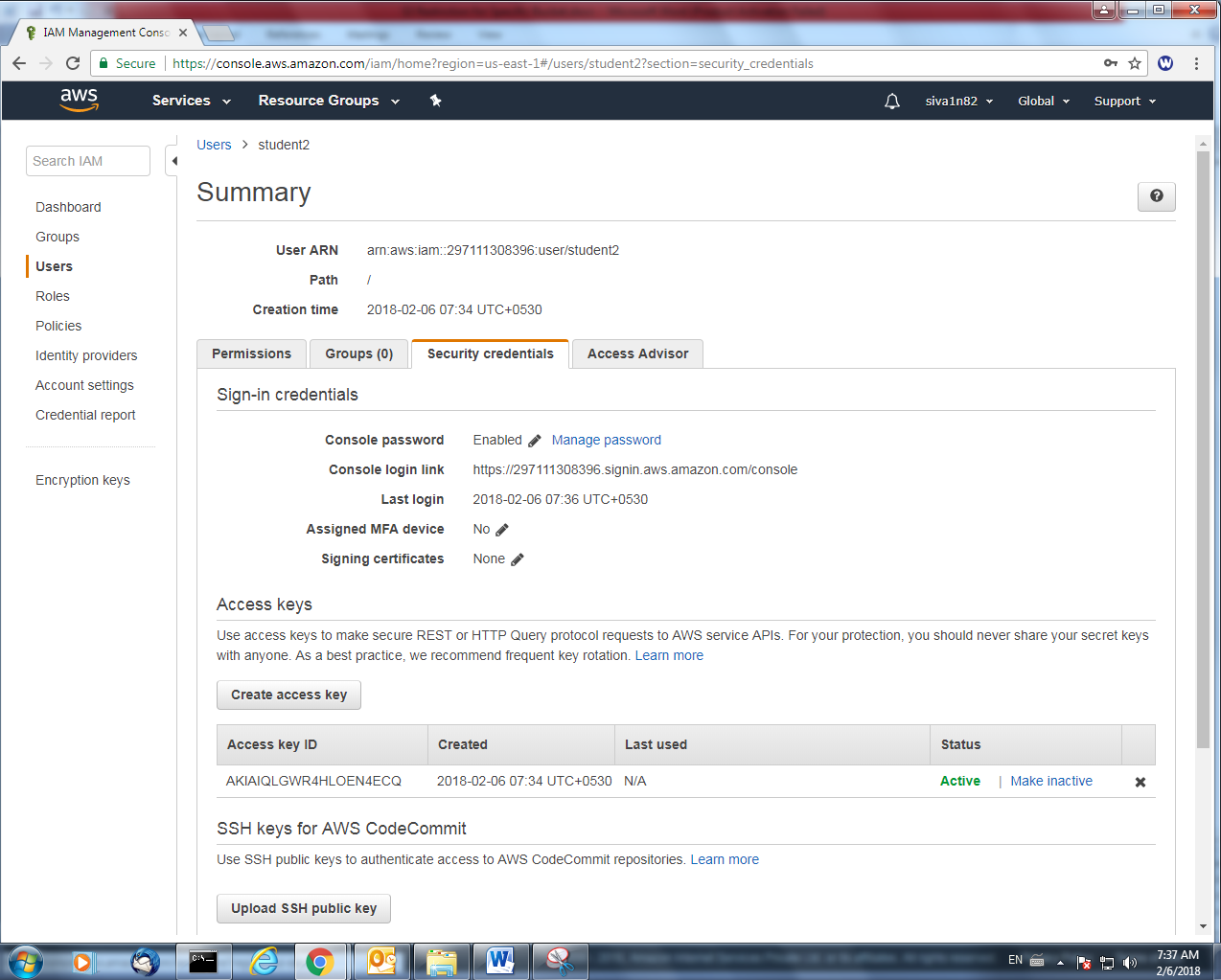
User successfully created. Please note that URL as below in box.



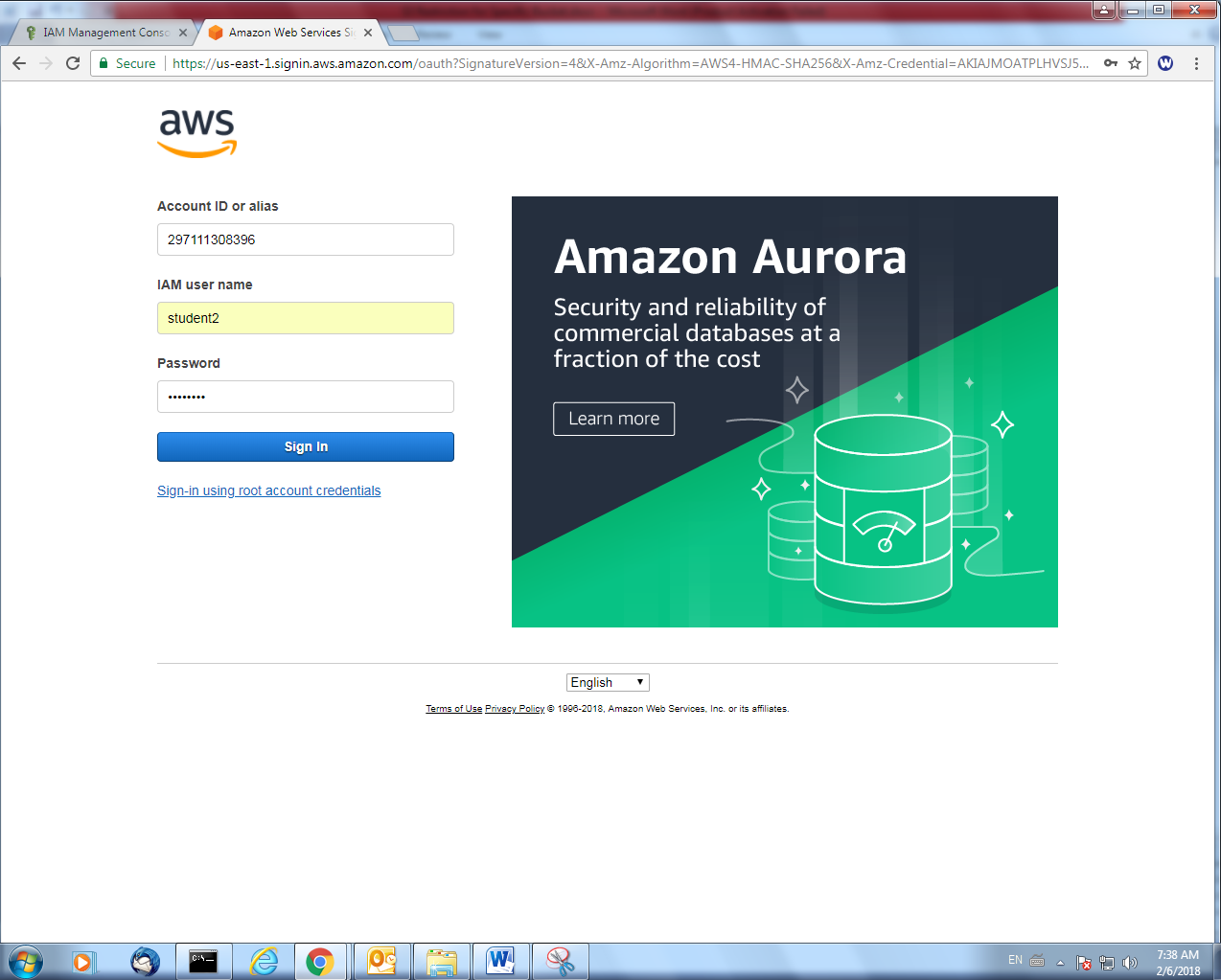
Click Users, and select student2 user.



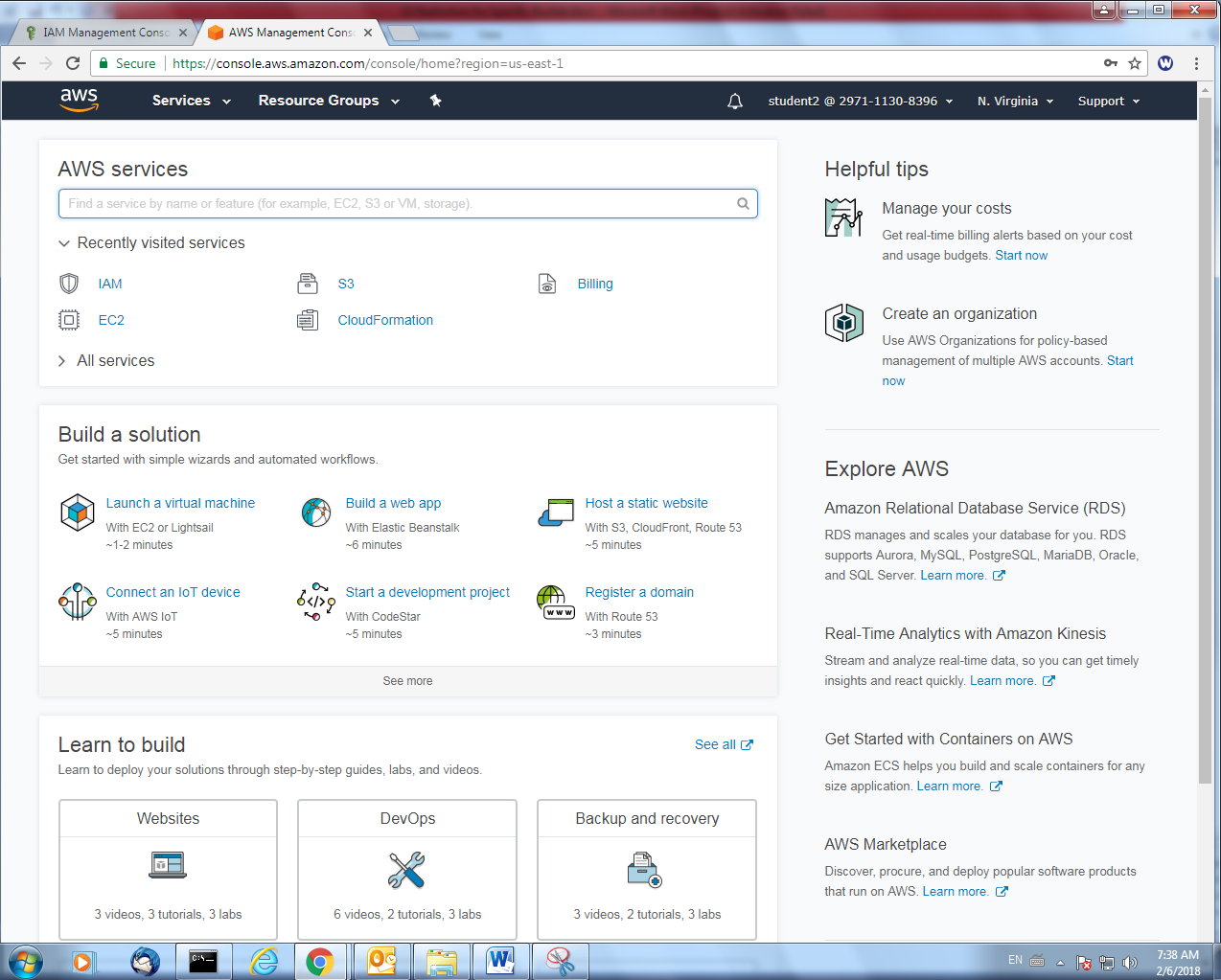
Clcik Security Credentials, copy the console login link and open that URL in new window.



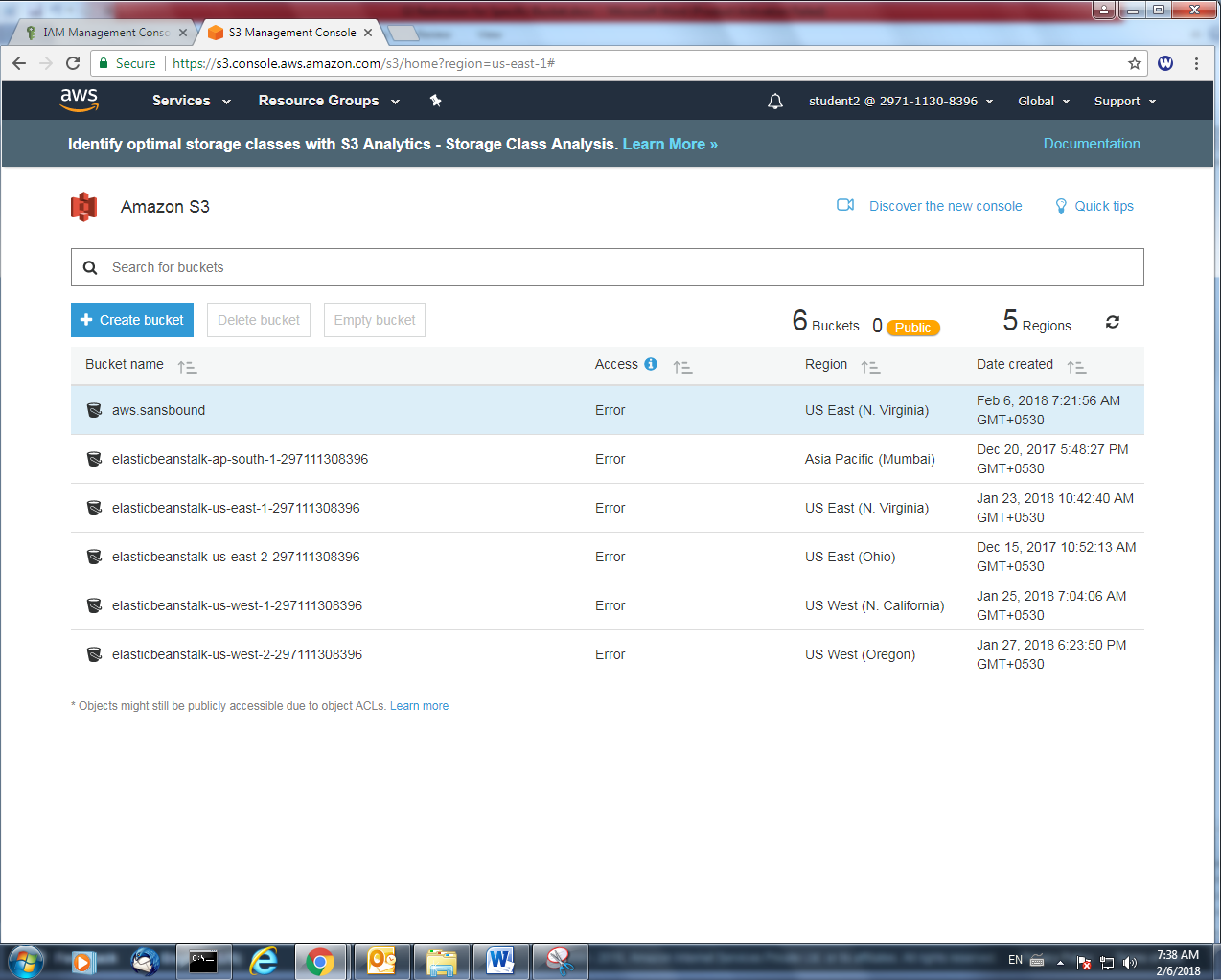
Type the login credentials of Student2.



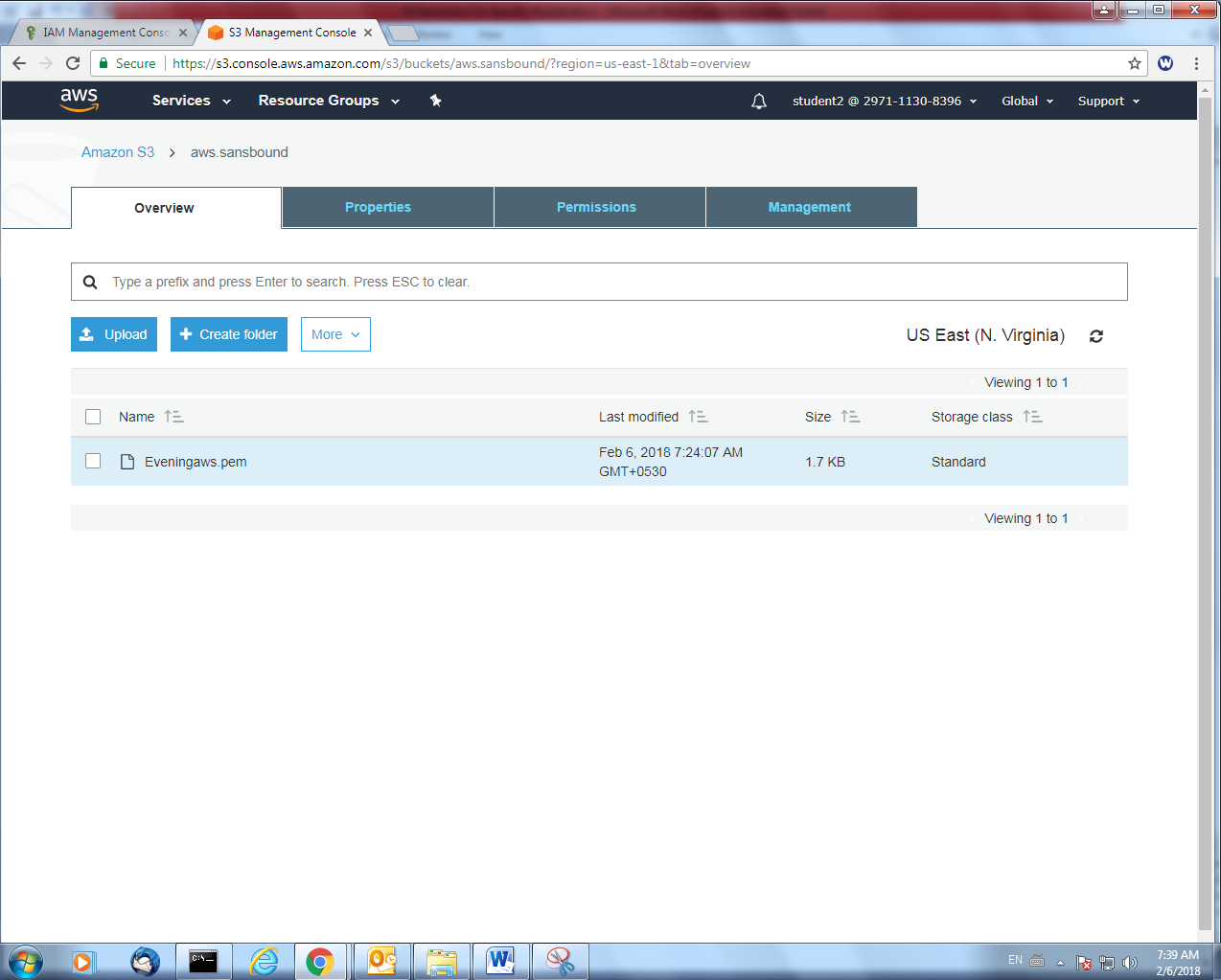
Click “S3”.



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.

