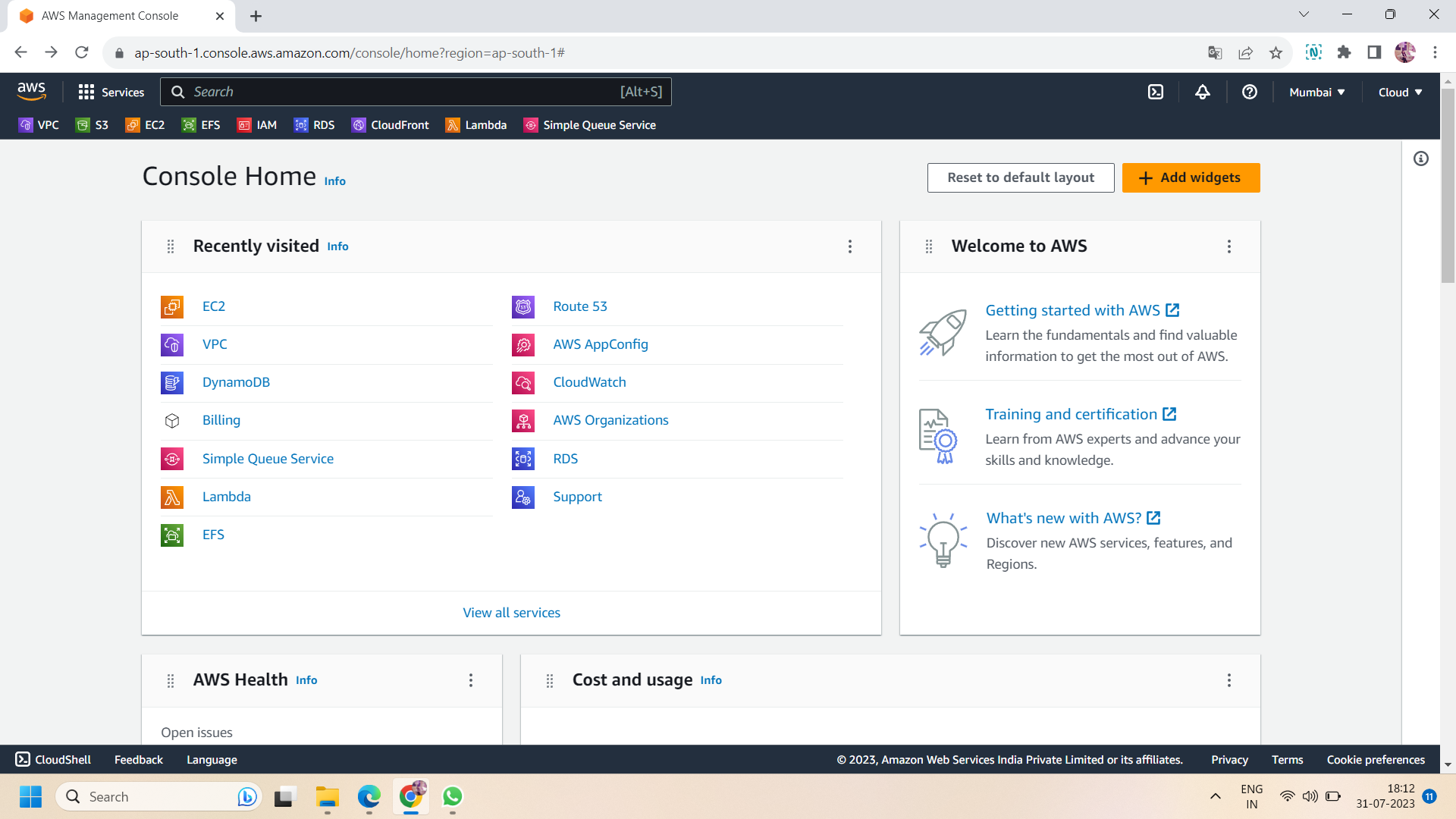
**AWS :**

**S3 Access Point :**

Step 1: login to aws management console



Step2 : Now, navigate to IAM console and go to policy and create a policy.On clicking on “create policy” ,first “specify permissions”.In permissions ,you can use visual or JSON format .here we use the JSON format.In both format, allow the following permissions :

* ListAccessPoints
* ListAllMyBuckets
* GetAccessPoint
* ListBucket
* ListMultiRegionAccessPoints

If you use the JSON format then you can directly copy and paste the following script:

{

"Version": "2012-10-17",

"Statement": [

{

"Sid": "Statement1",

"Effect": "Allow",

"Action": [

"s3:ListAccessPoints",

"s3:ListAllMyBuckets",

"s3:GetAccessPoint",

"s3:ListBucket",

"s3:ListMultiRegionAccessPoints"

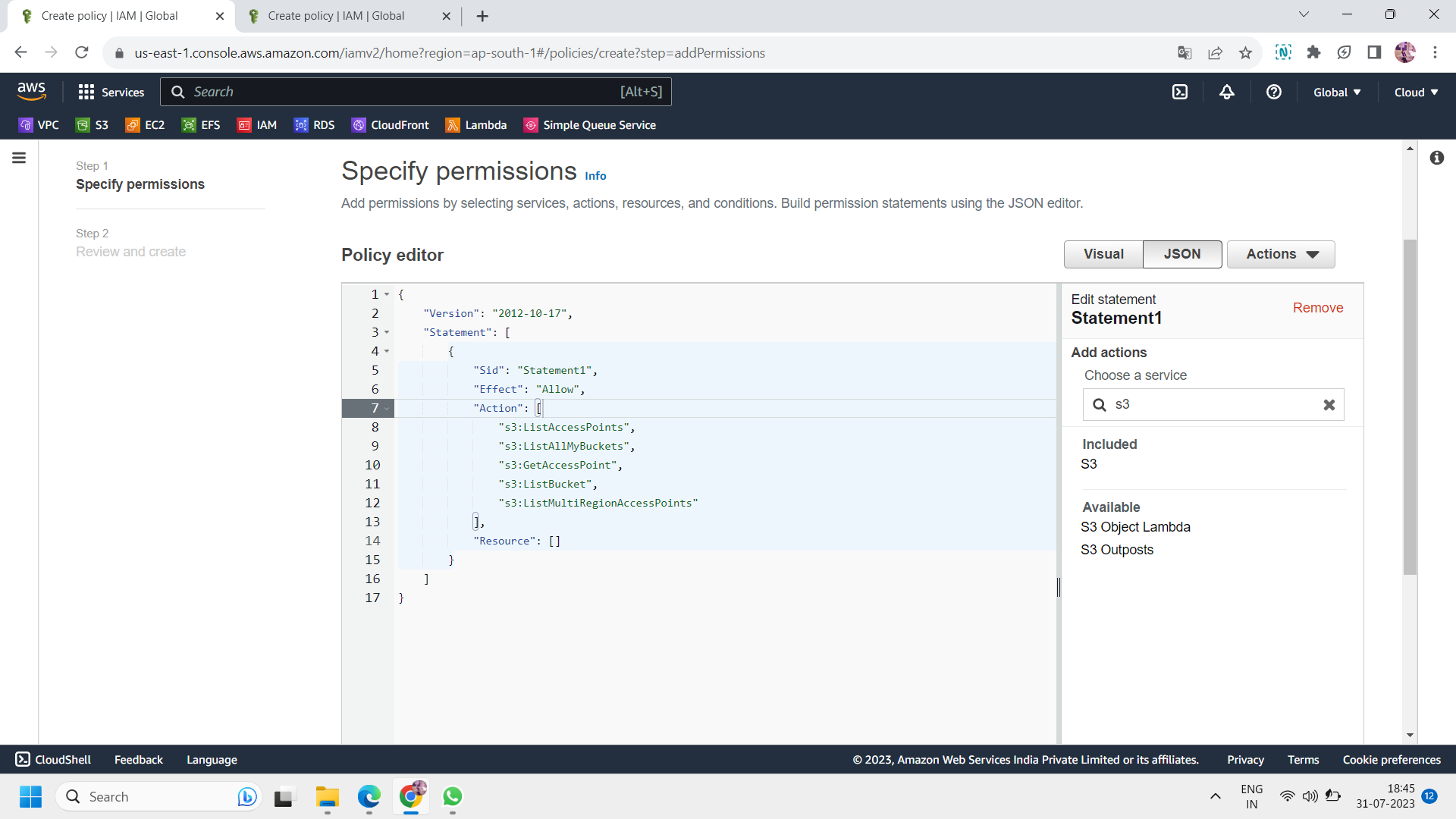
],

"Resource": "\*"

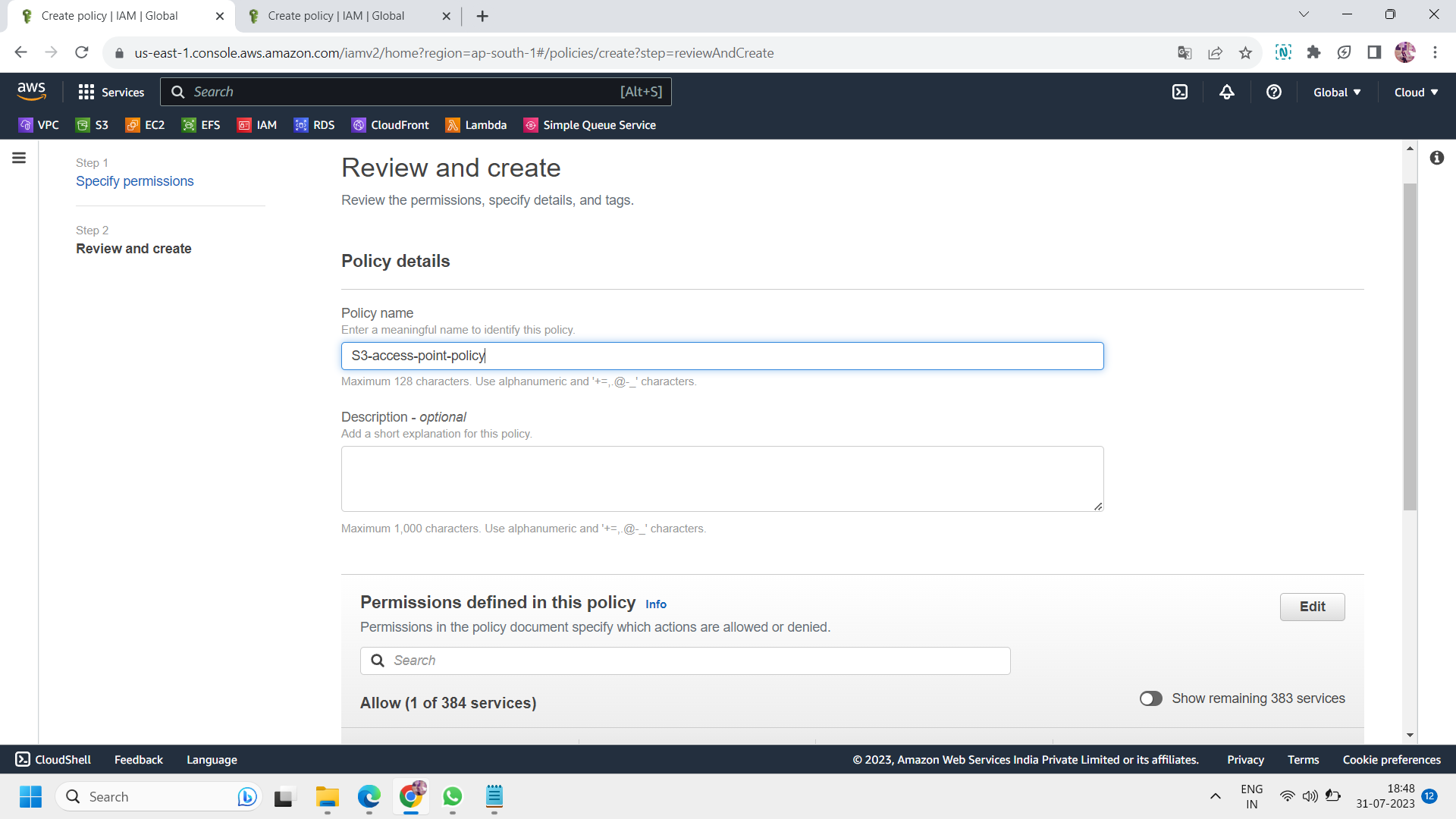
}

]

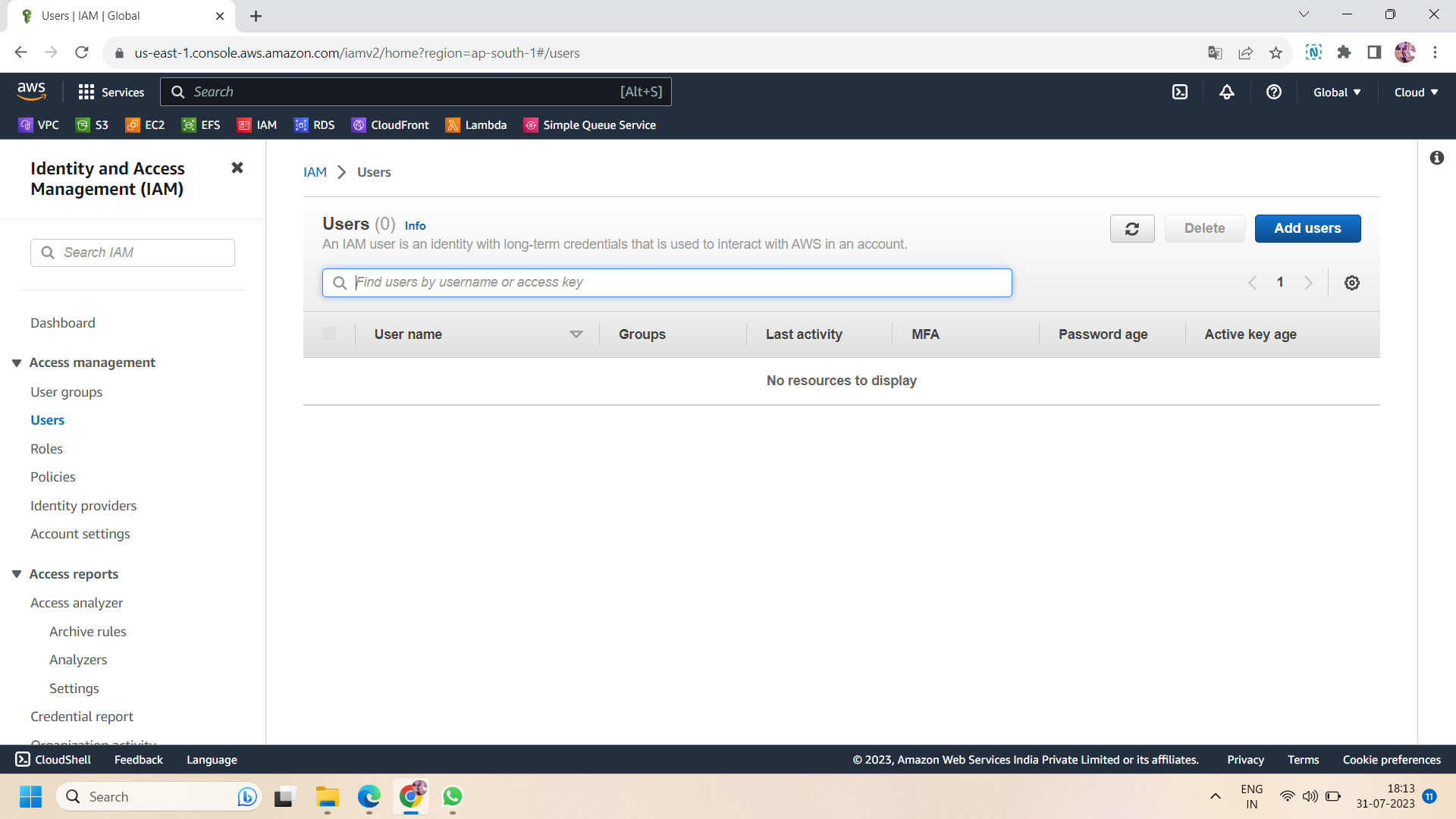
}

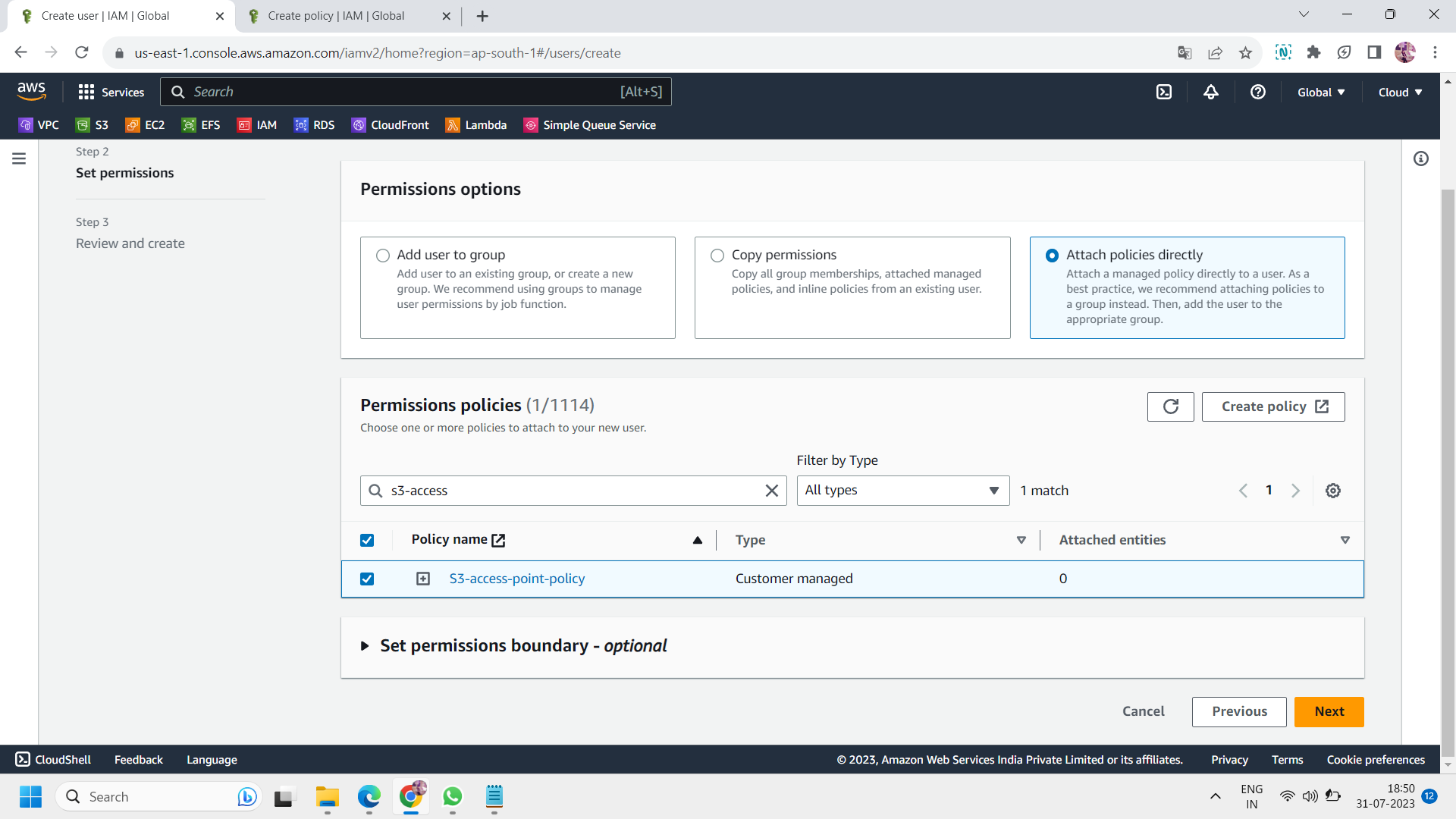


Step 3: Review and create : after specify the permissions ,name the policy and click on create policy.Here ,we use the name of the policy : s3-access-point-policy.



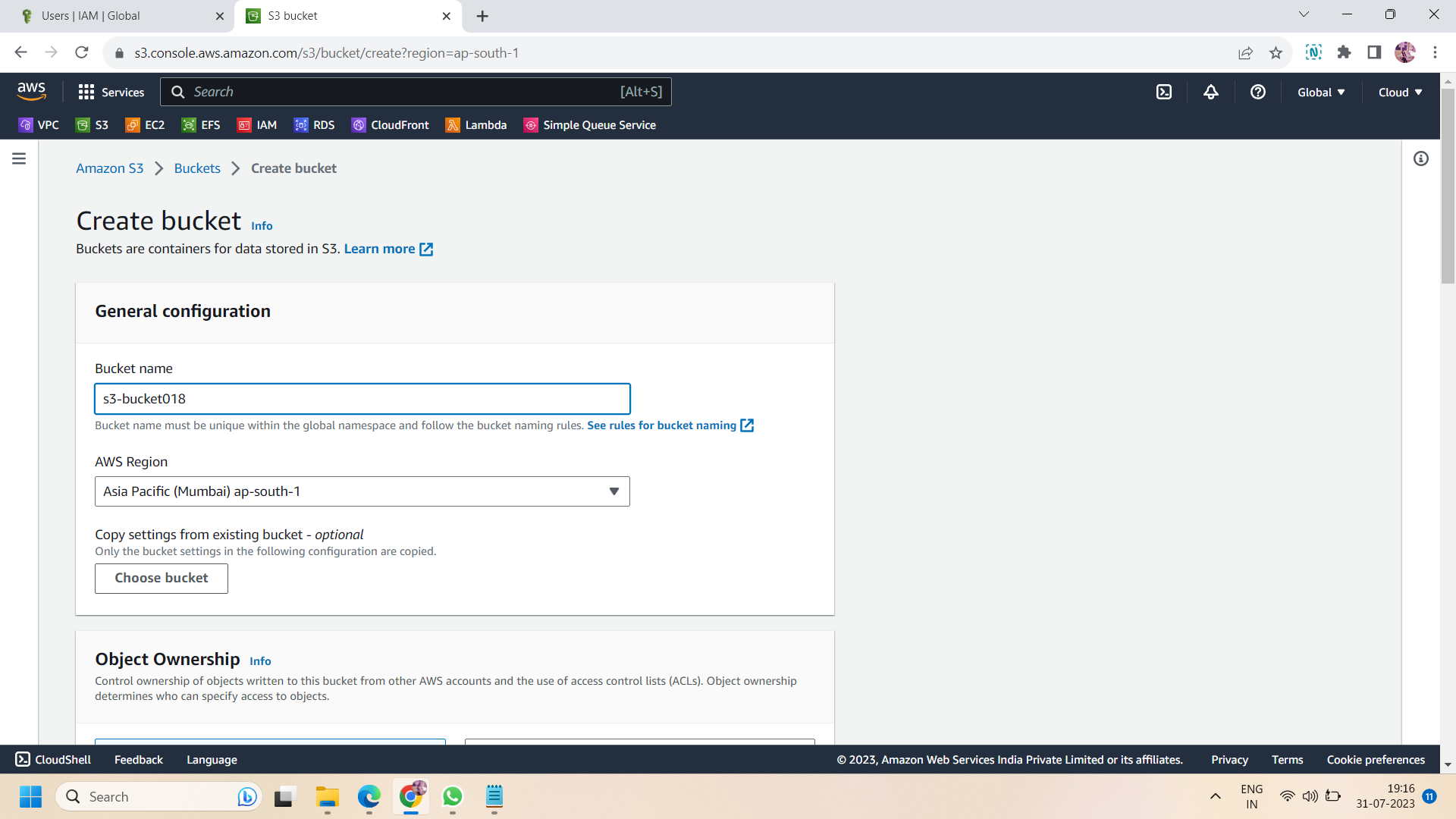
Step 4: Now ,move to users and create 3 IAM users with the same policy created above.here we create 3 users namely: IAM\_user,IAM\_user2 and IAM\_user3. For assigning the policies with users ,click on “attach policies directly”.

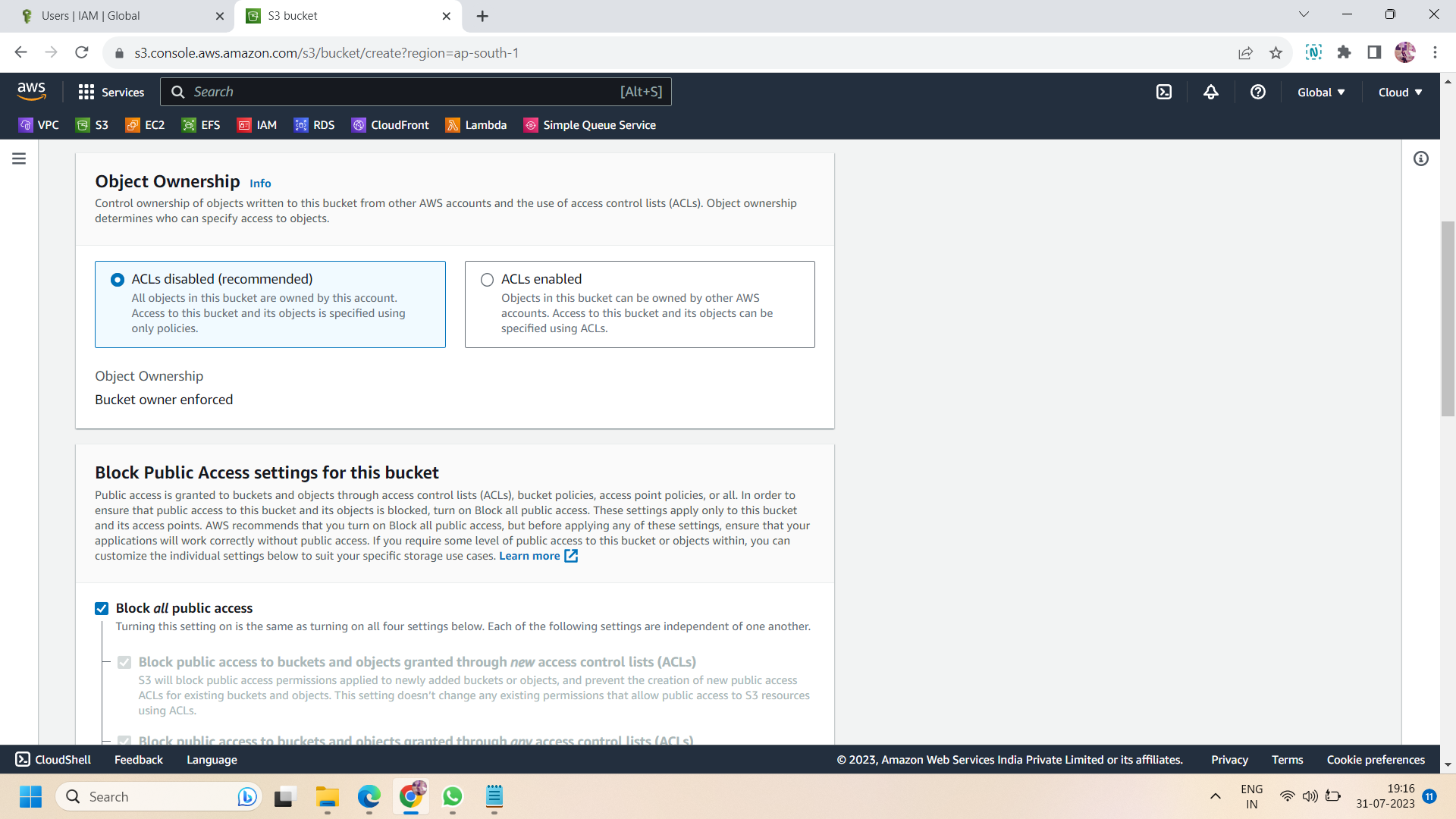


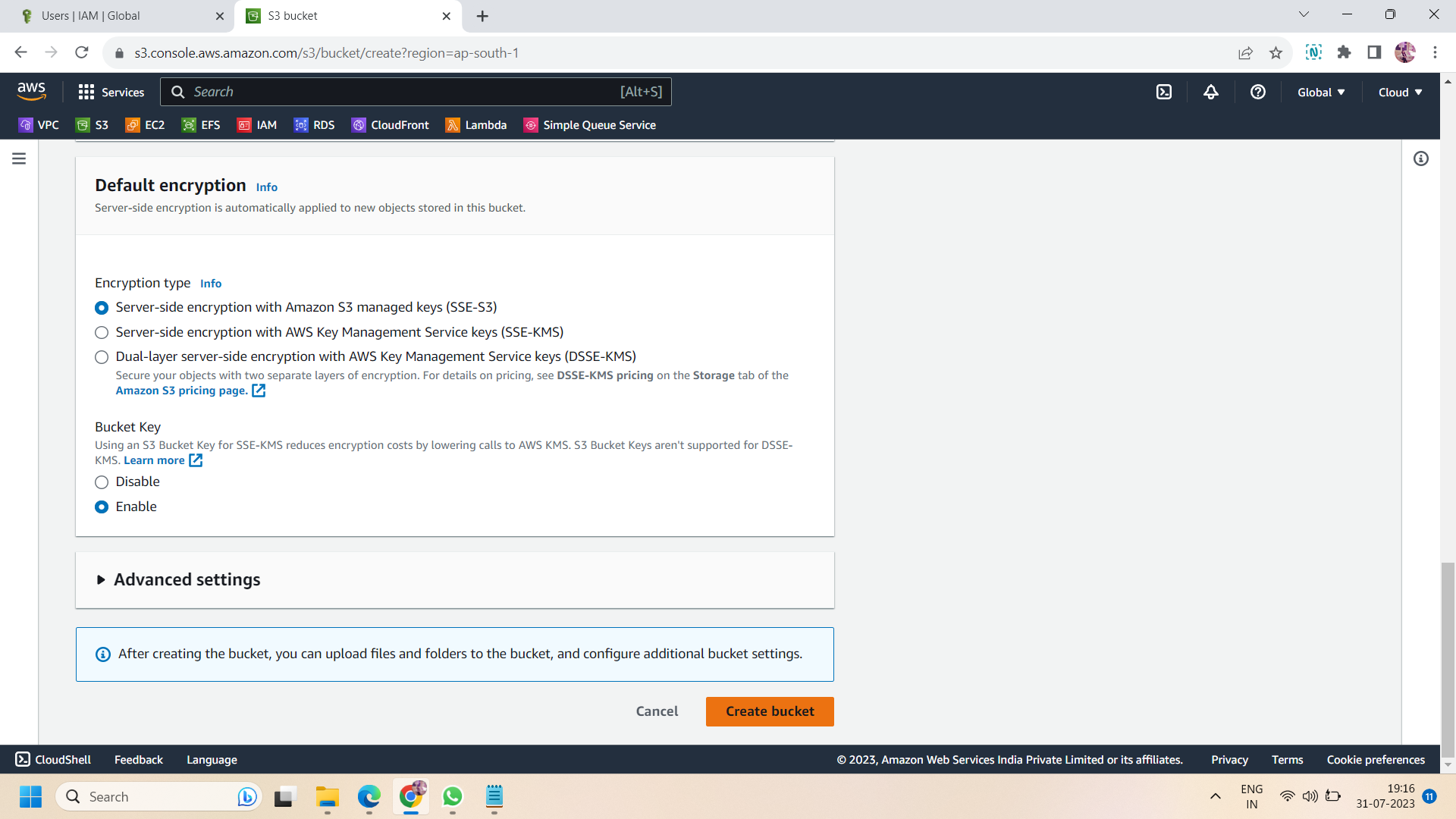
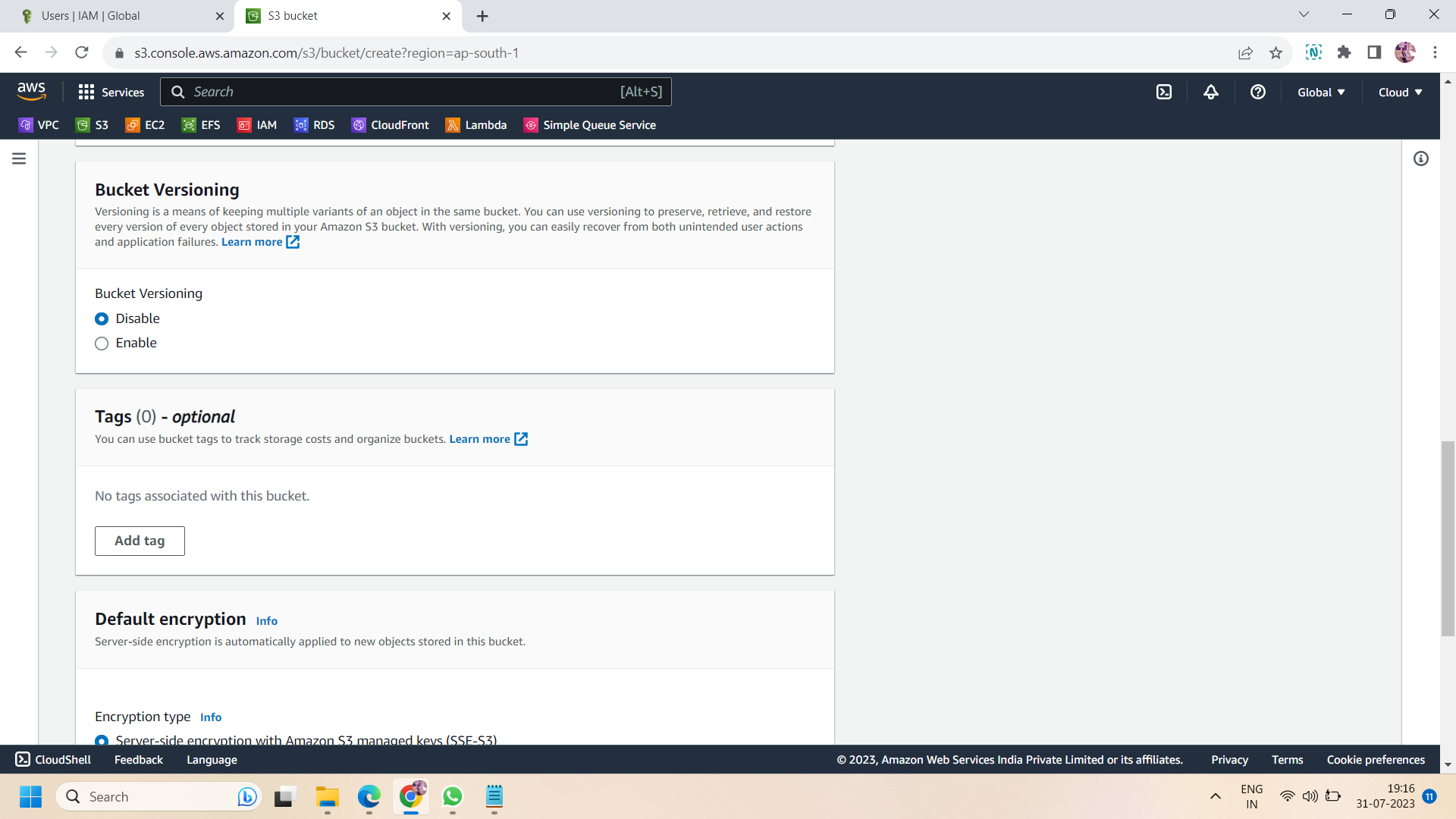




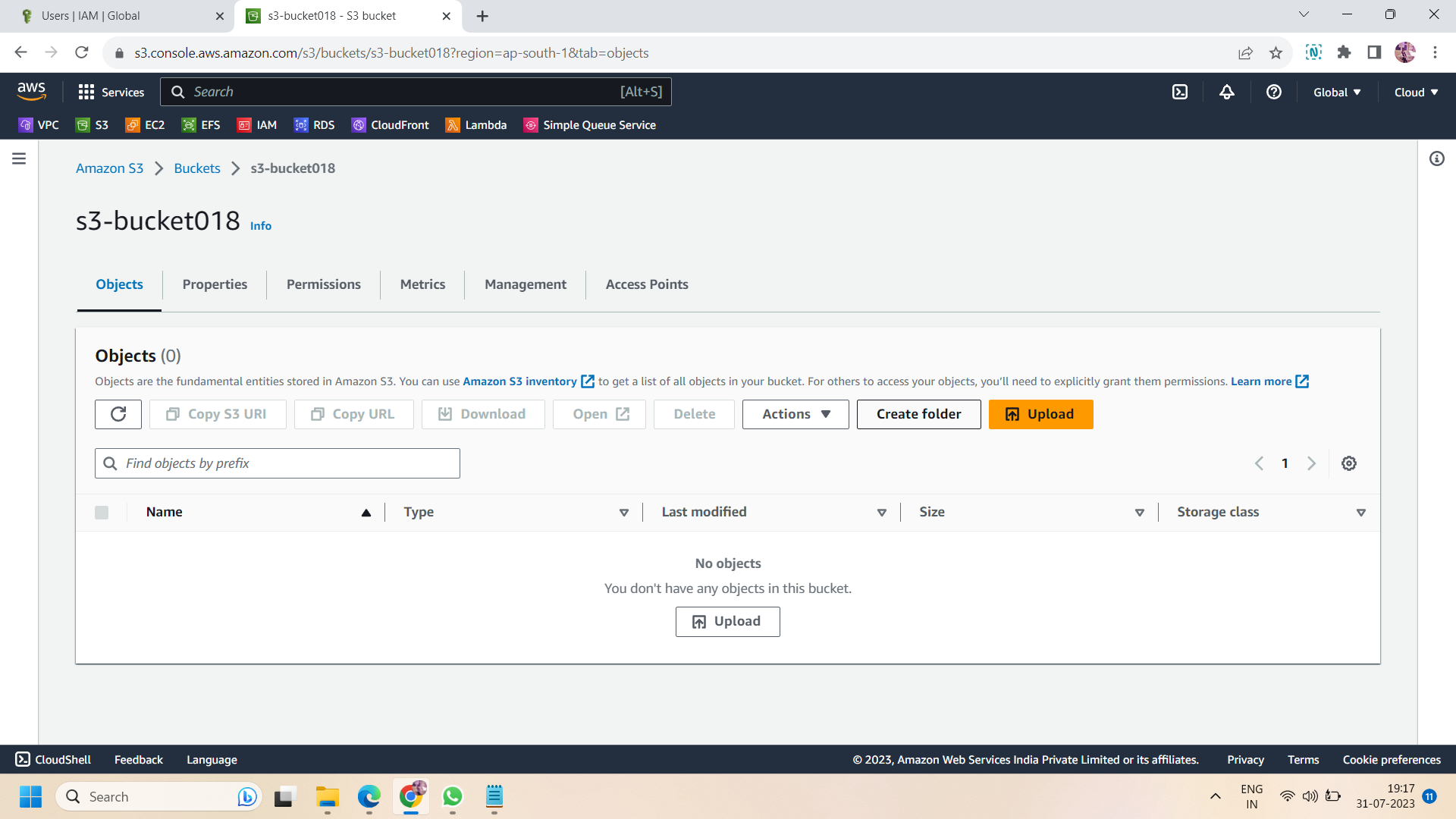
Step 5: Now ,navigate to the S3 console and create a bucket in any specified region.In object ownership,**disable the ACLs** and **block all public acces**s as because we are trying to access s3 using access points.**disable the versioning** and **enable server-side encryption with Amazon s3 managed keys(SEE-S3)**.then click on “create bucket”.

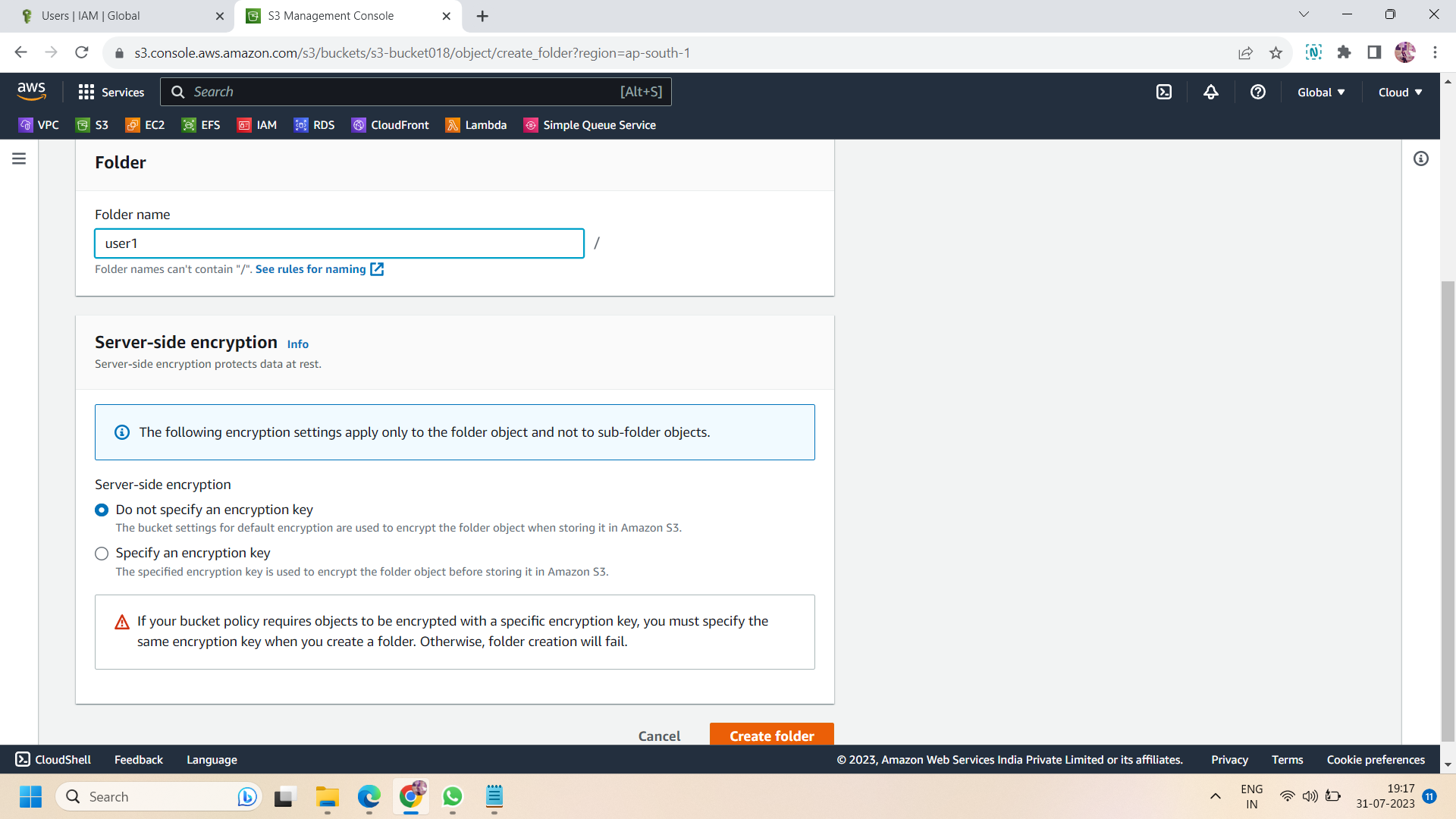






Step 6: Now, create a folder inside the created s3 bucket.here we create three folders :-user1,user2,user3.Click on “create folder” to create folders.





Step 7: after creating folders,now got ot bucket policy and create the bucket policy for your s3 bucket.here is the JSON script ,copy that JSON script and and paste into bucket policy after customized it.during customization ,**copy the arn of your s3 bucket in the resources** and **paste your aws account ID in condition section**.here is the sample json format bucket policy script:-

{

"Version": "2012-10-17",

"Statement": [{

"Effect": "Allow",

"Principal": {

"AWS": "\*"

},

"Action": "\*",

"Resource": [

"arn:aws:s3:::s3-bucket018" ,

"arn:aws:s3:::s3-bucket018/\*"

],

"Condition": {

"StringEquals": {

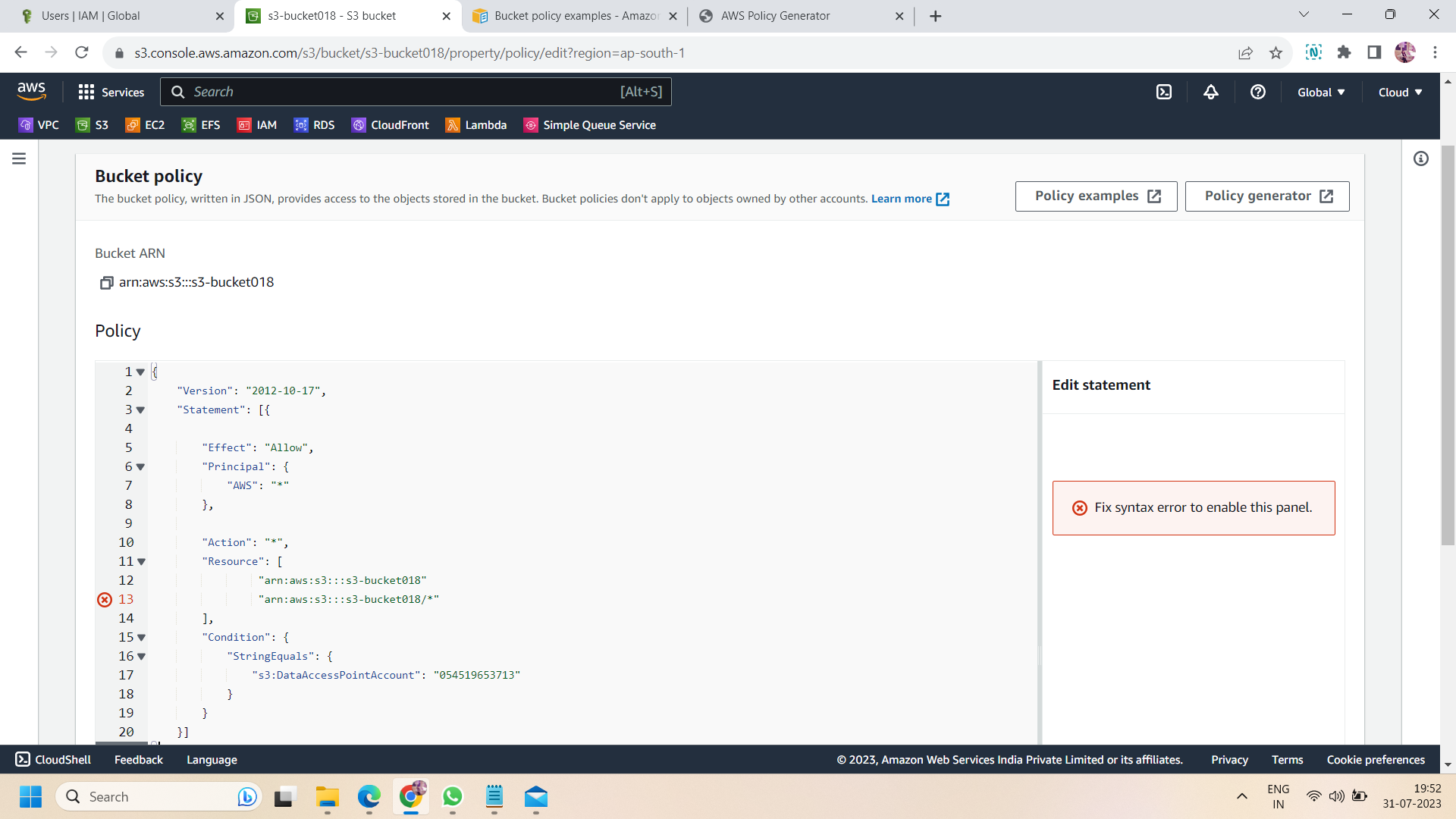
"s3:DataAccessPointAccount": "054819653713"

}

}

}]

}



Step 8: after creating the bucket policy,move to bucket access point and **create an access point** of your s3 bucket.name the access point and copy the arn generated after naming the access point.**choose the internet network origin** and **block all public level access**.then paste the following script in access point policy.the following script has to be customized according to your own s3 bucket.

**In principal section ,you have to paste the arn of one of your created IAM user**,which you have to assign permissions.next is actions ,here we assign get and put permission to the IAM user and then **in resource section,paste the arn of s3 bucket access point.**

{

"Version": "2012-10-17",

"Statement": [{

"Sid": "Statement1",

"Effect": "Allow",

"Principal":{

"AWS": "arn:aws:iam::054519653713:user/IAM\_user1"

},

"Action": [

"s3:GetObject",

"s3:PutObject"

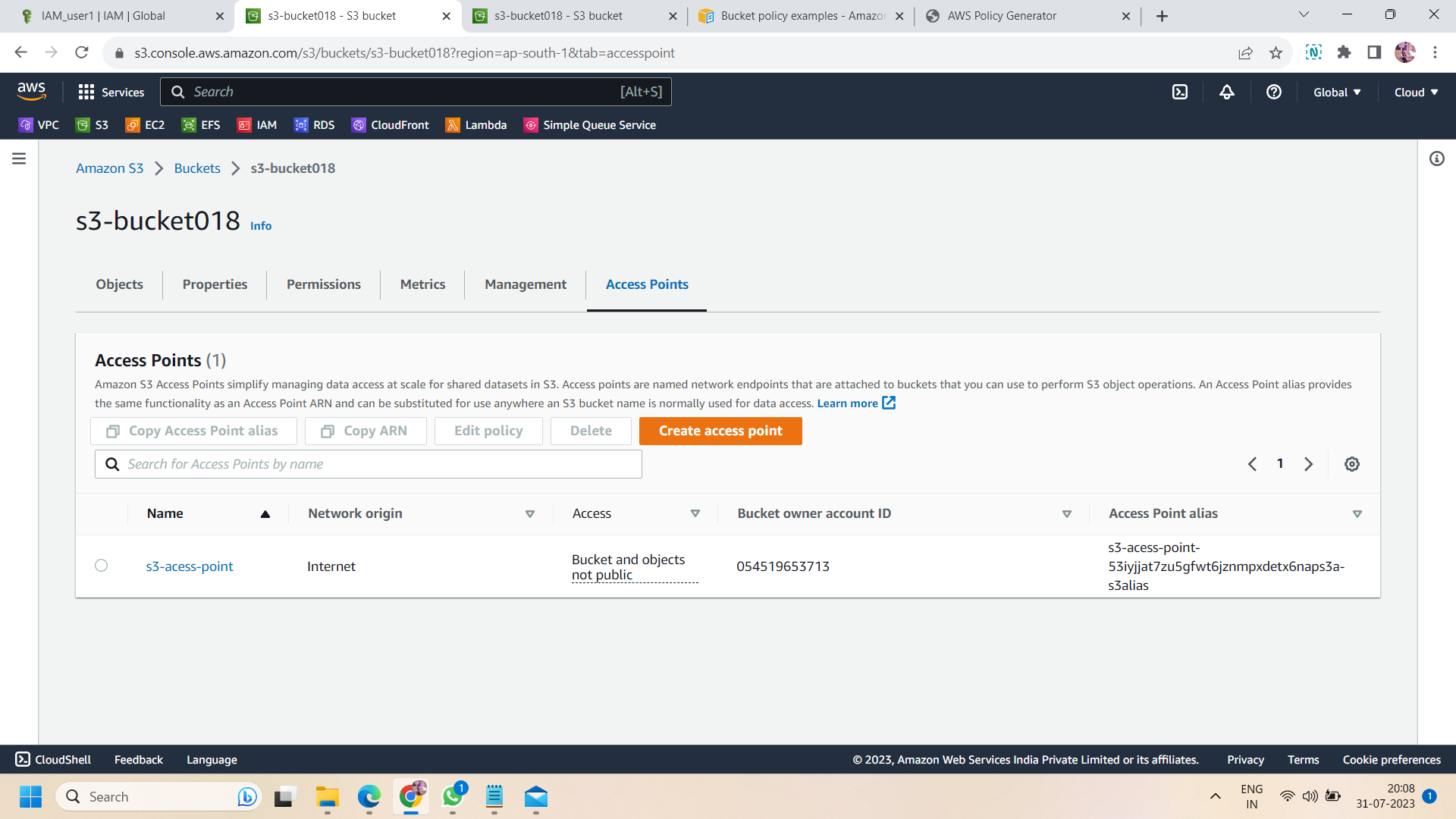
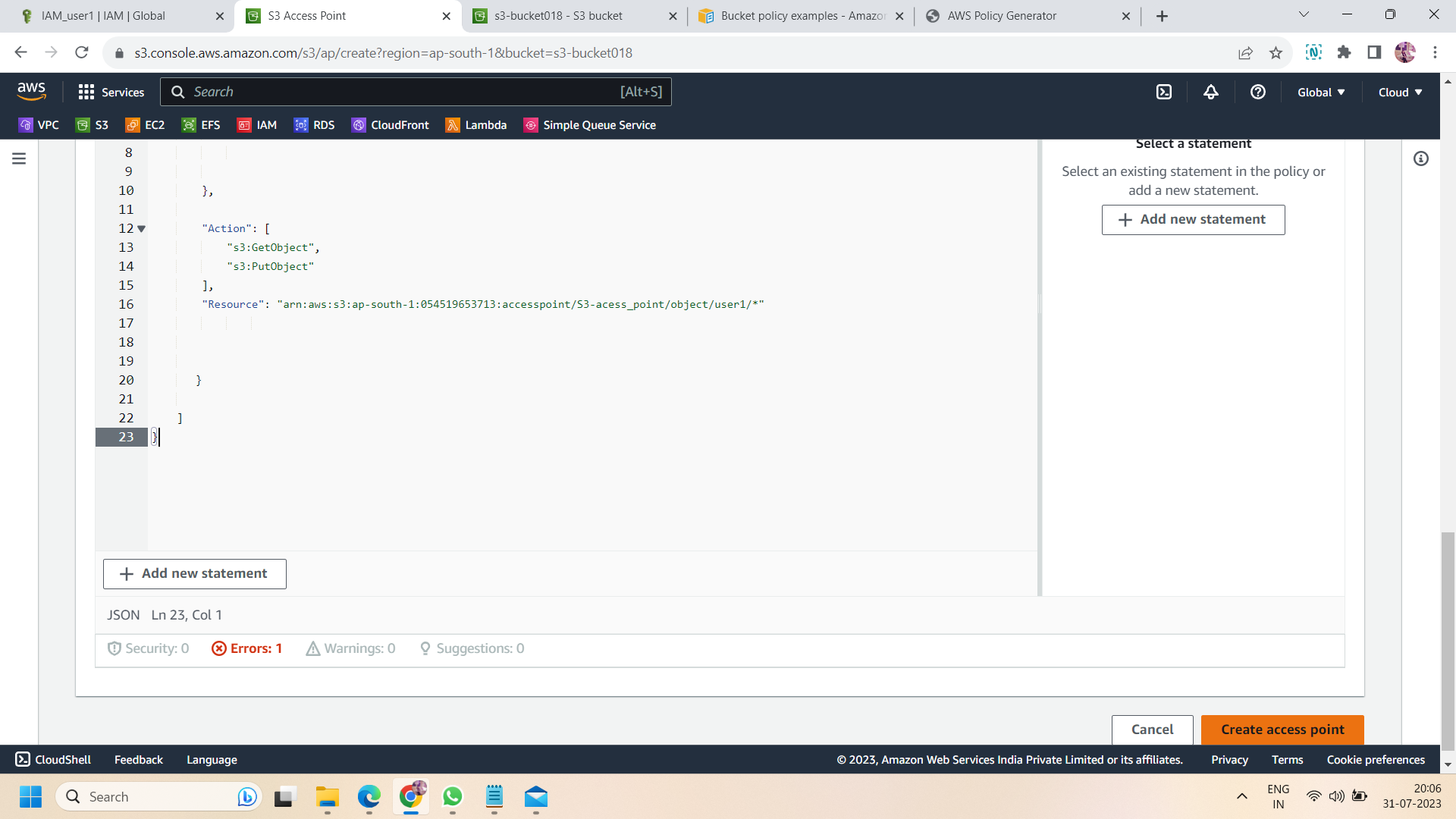
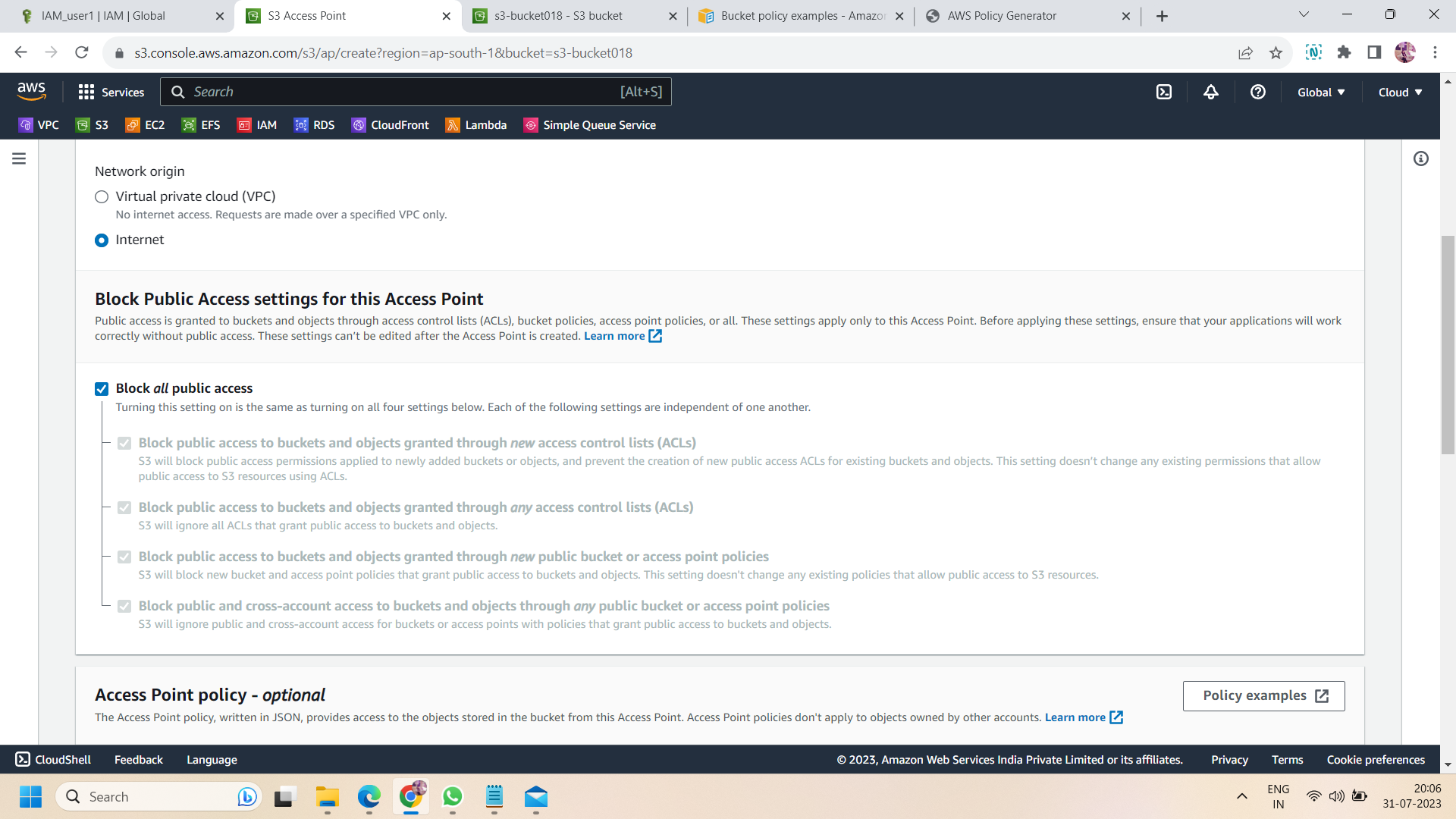
],

"Resource": "arn:aws:s3:ap-south-1:054519653713:accesspoint/S3-acess\_point/object/user1/\*"

}

]

}

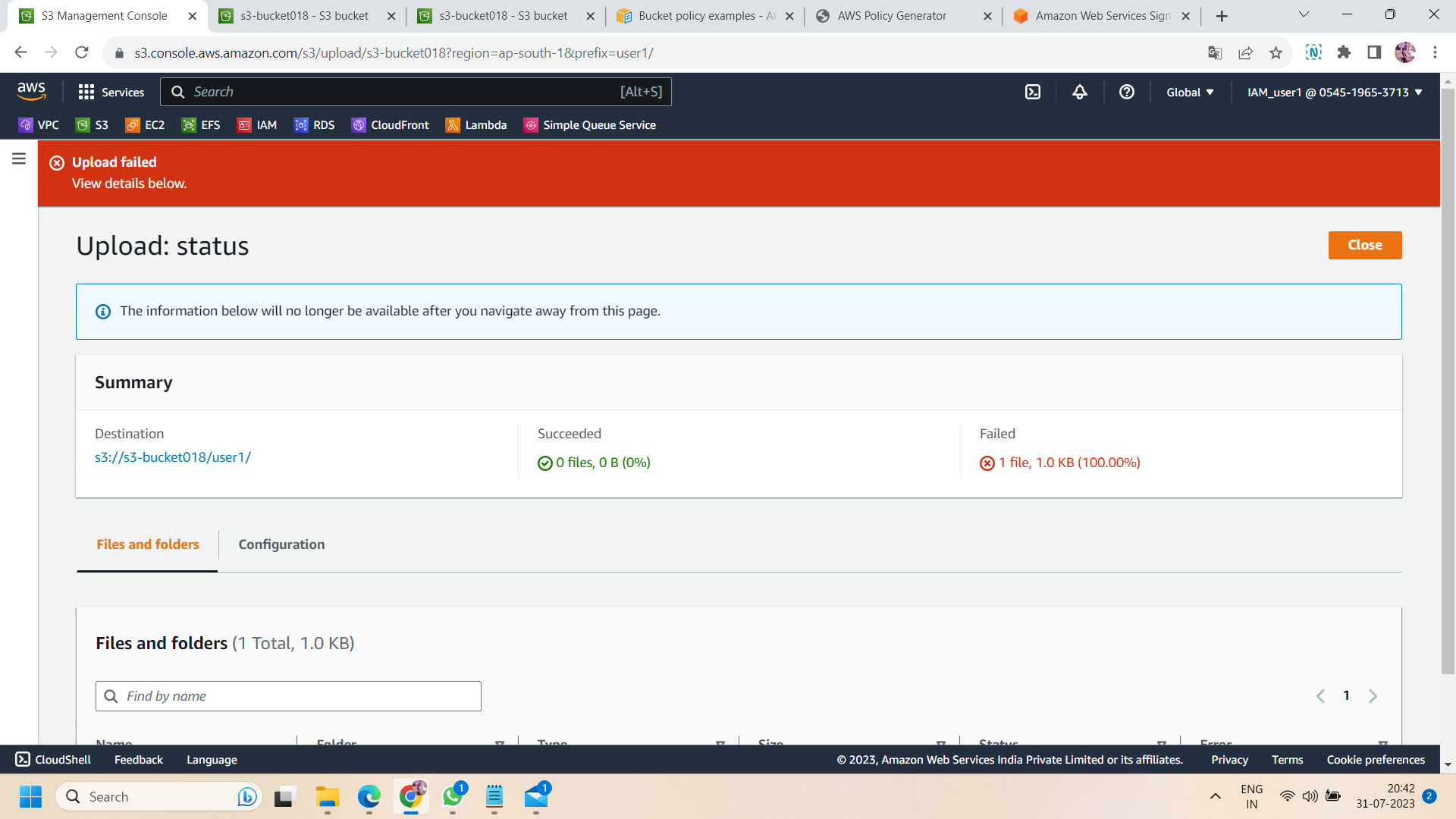


Step 9: Now, after following the above all steps ,login to aws console using the one of the IAM user which have permission to access bucket.here we assign permissions to aws IAM\_user1.



Step 10 : after login with IAM user,navigate to s3 bucket ,here you will see all the buckets created in your aws account and IAM user have permissions to access.so here we have only one bucket which IAM\_user1 can access.i.e.,s3-bucket018.

Now if we try to upload any file or folder in the bucket or inside any created folder i.e.,(user1.user2 or user3) then access denied and uploading will not be successfully.it is because in an access point,we can access or upload any object only using the access point.



Step 11: now move to access point and click on created access point,if we trying to upload any file of folder in access point then again we will get the same error.i.e., upload failed .it is because we defined policies to only one IAM user and to access the folder ‘user1’ not user2 or user3.so if we click on folder “user1” and upload any file or folder in it then it will upload and uploading will be successful.

