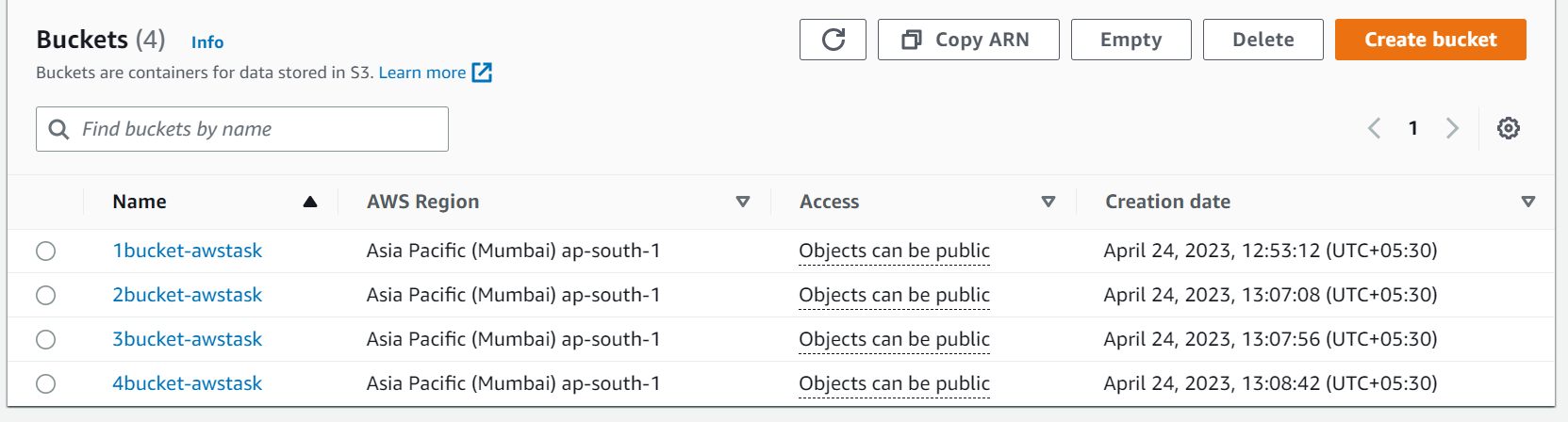
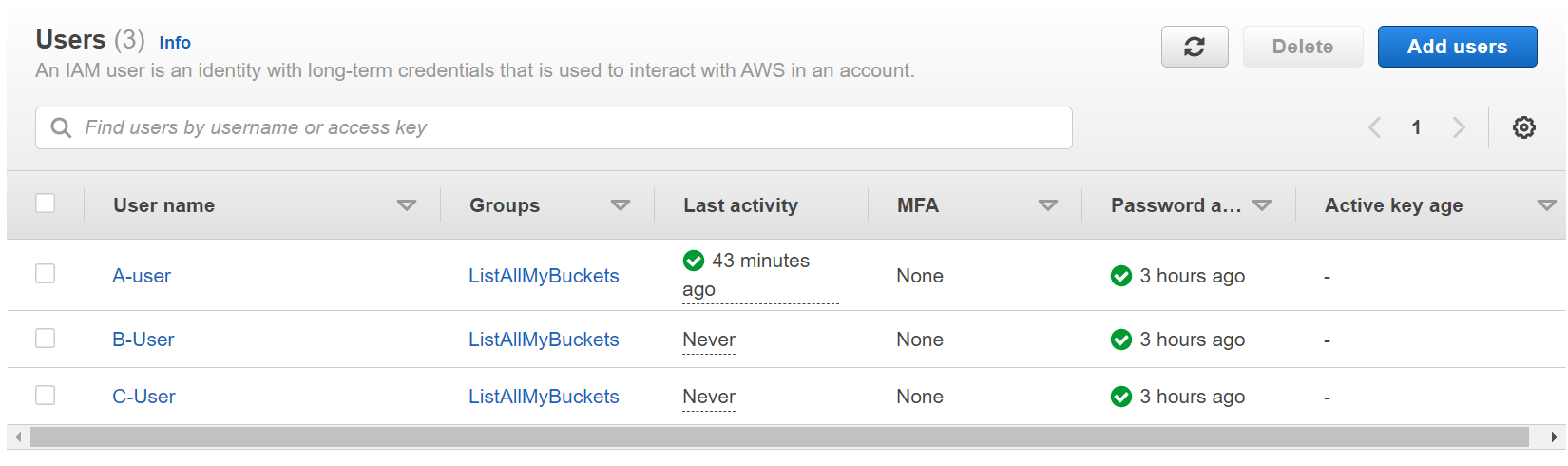
User 1 – bucket 1 access

1.Create 4 buckets and upload objects in each bucket



2.create users



3.IAM-> policies -> create policy -> JSON

To list all buckets and view objects:

{

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

"Statement": [

{

"Sid": "AllowGroupToSeeBucketListInTheConsole",

"Action": [

"s3:ListAllMyBuckets"

],

"Effect": "Allow",

"Resource": "\*"

},

{

"Sid": "Stmt1682323008869",

"Action": [

"s3:GetAccountPublicAccessBlock",

"s3:GetBucketAcl",

"s3:GetBucketLocation",

"s3:GetBucketPolicyStatus",

"s3:GetBucketPublicAccessBlock",

"s3:ListAccessPoints",

"s3:ListBucket"

],

"Effect": "Allow",

"Resource": "\*"

}

]

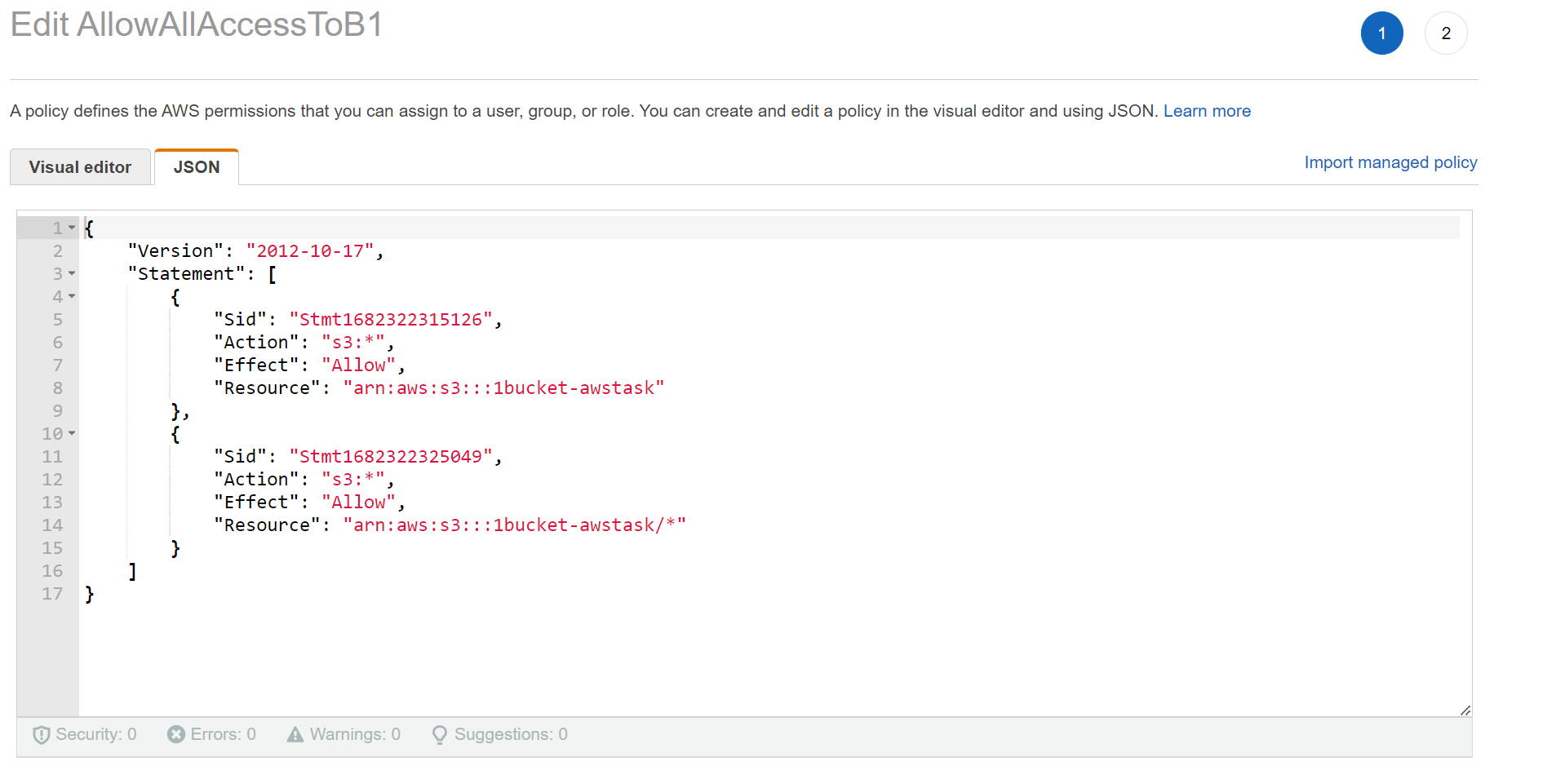
}

4.IAM -> user groups

Group name: listallmybuckets

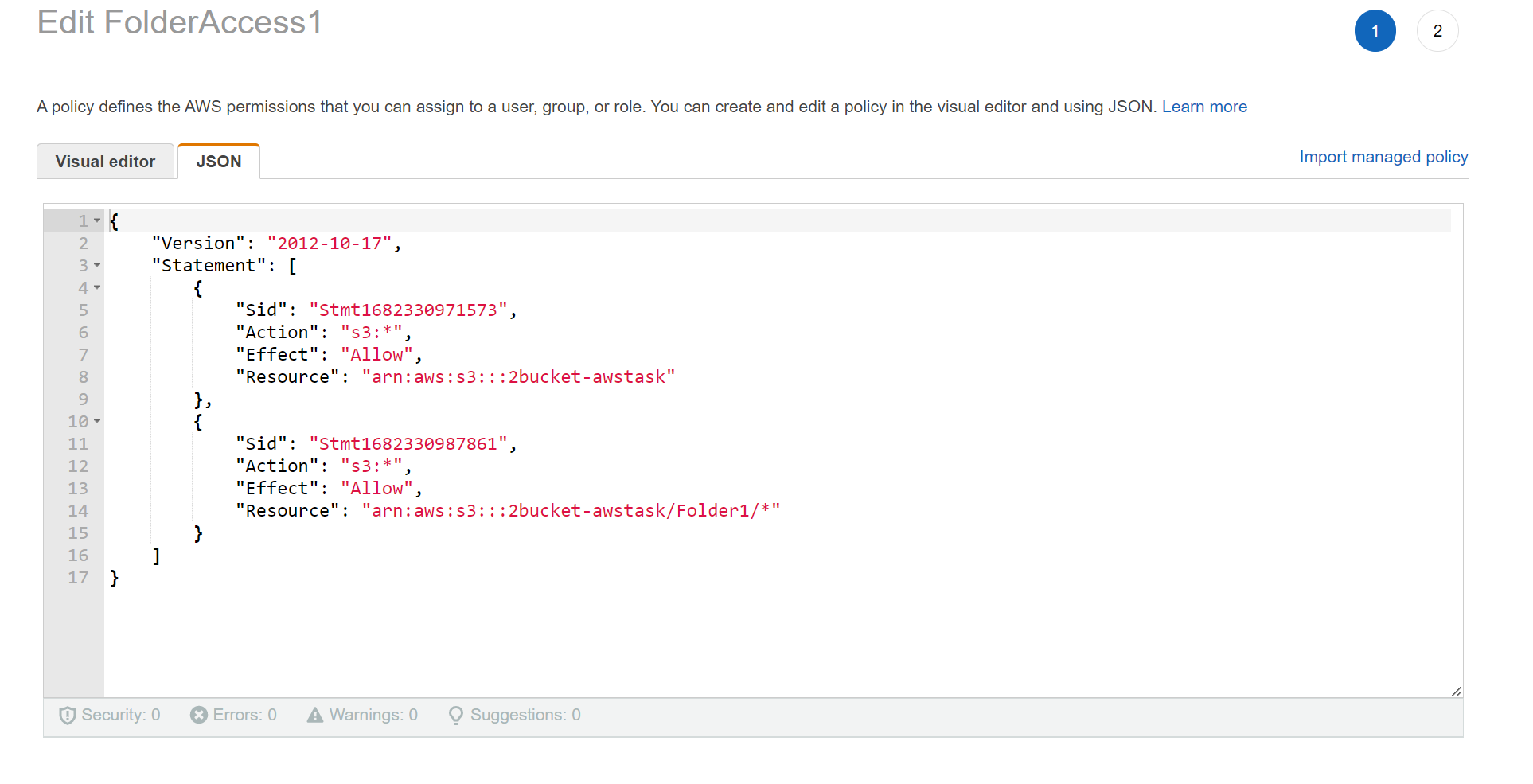
Add all the users to the group

5. create inline policy for user1 to access bucket 1



6. for first bucket to make object public use object actions and make ACL public

For folder level access:



If we did not allow below permissions it will show

{

"Sid": "Stmt1682323008869",

"Action": [

"s3:GetAccountPublicAccessBlock",

"s3:GetBucketAcl",

"s3:GetBucketLocation",

"s3:GetBucketPolicyStatus",

"s3:GetBucketPublicAccessBlock",

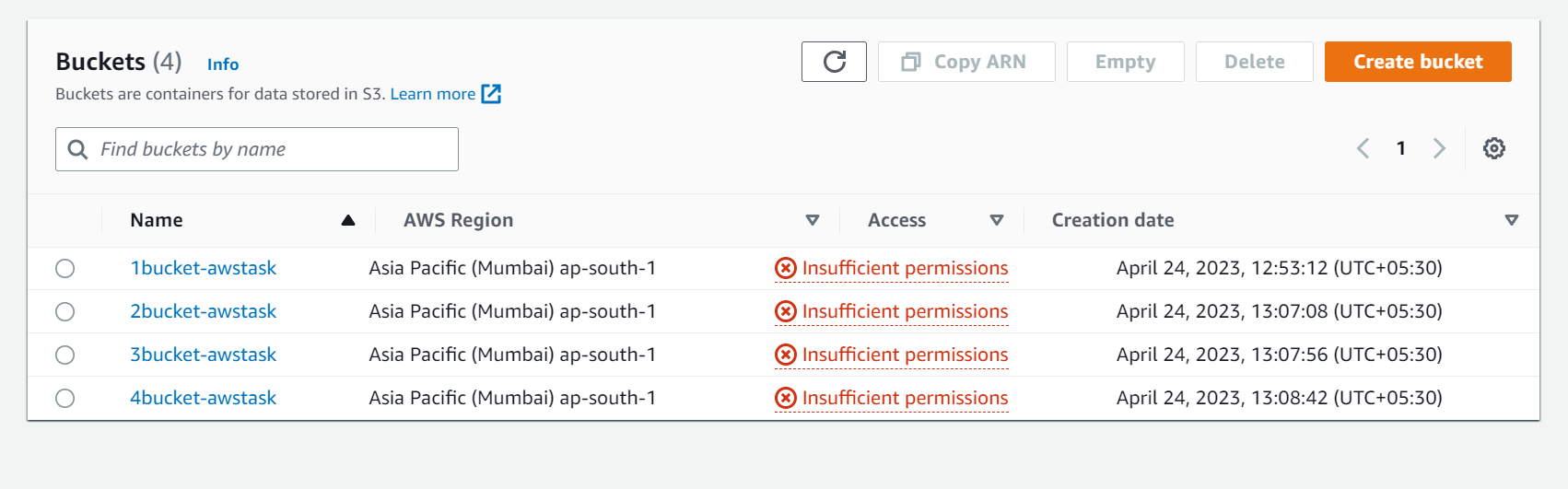
"s3:ListAccessPoints"

],

"Effect": "Allow",

"Resource": "arn:aws:s3:::1bucket-awstask"

}



Inline policy – one to one relationship b/w identity to policy.

For ref:

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/example-policies-s3.html#iam-policy-ex1>