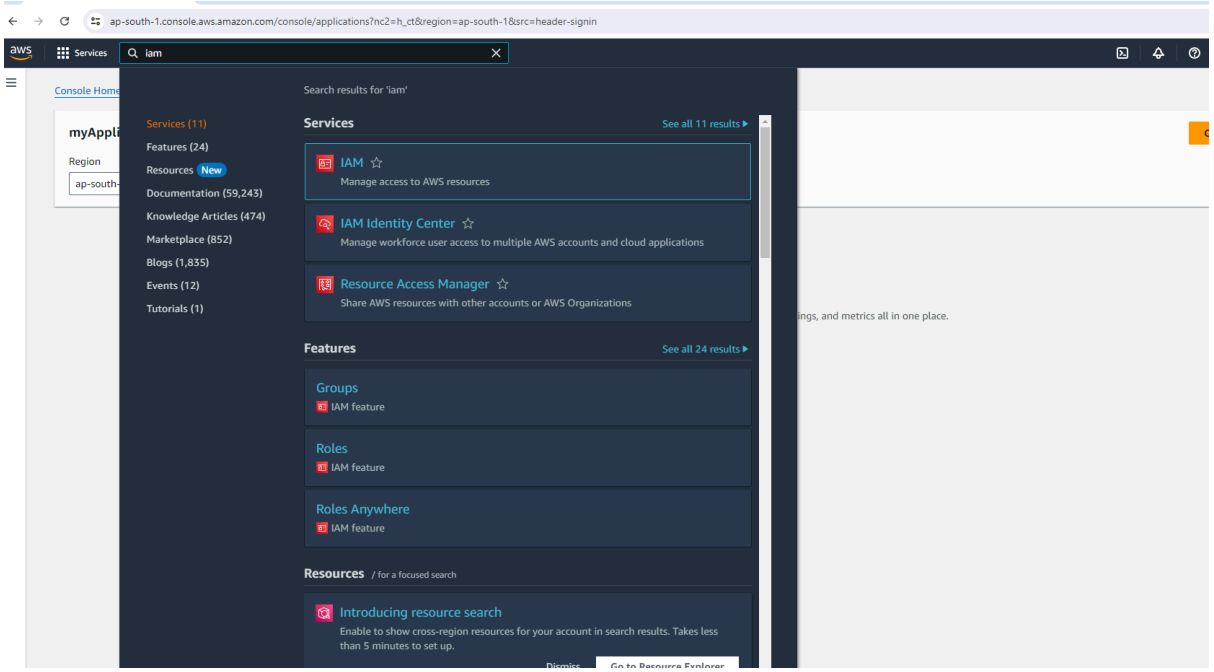
Name: Garima Joshi
Cloud Computing: Identity Access Management

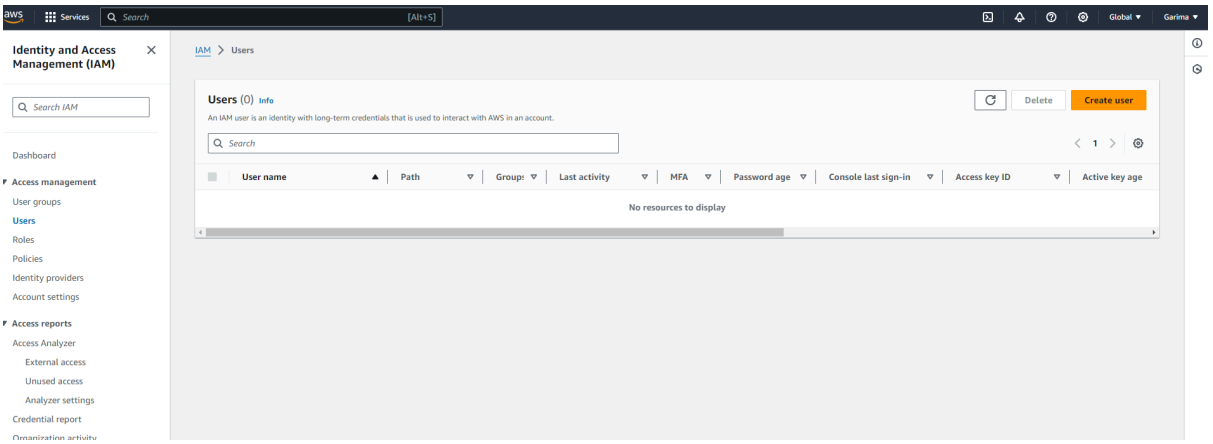
Q.Implementing policies for IAM users to access

1. S3 service
2. EC2 service

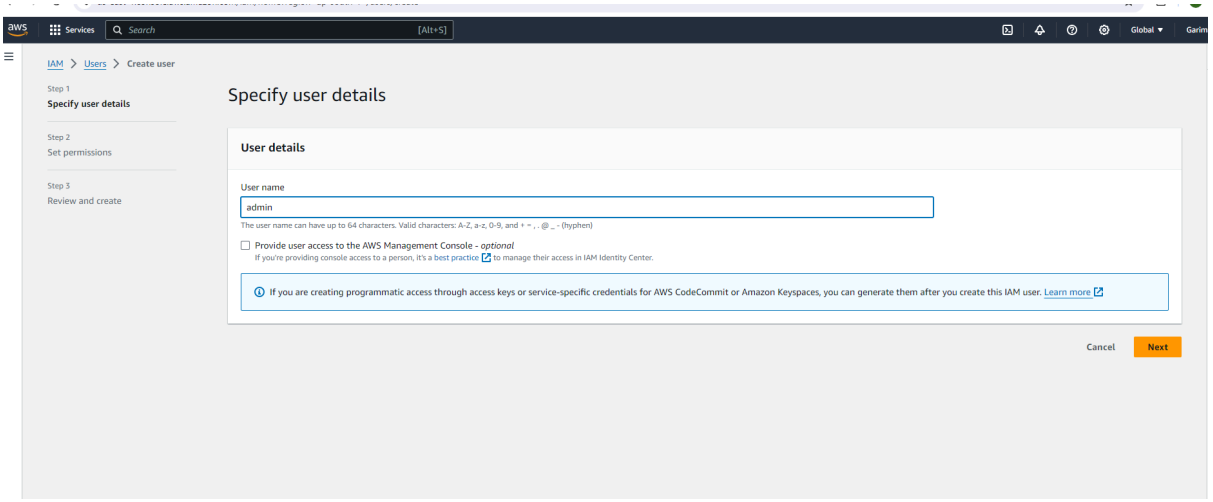
Ans:



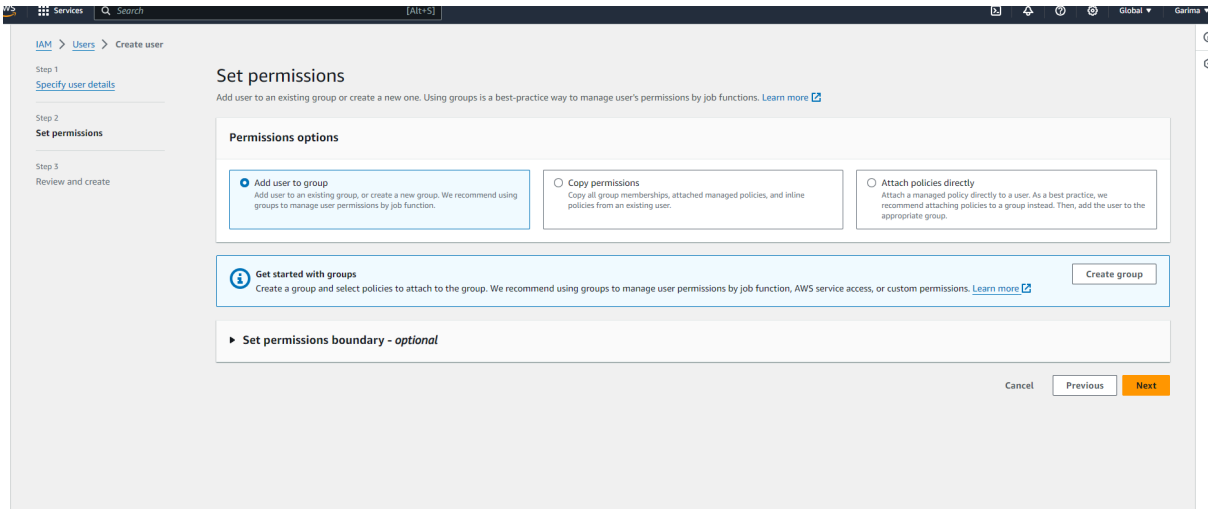
Select IAM from services.



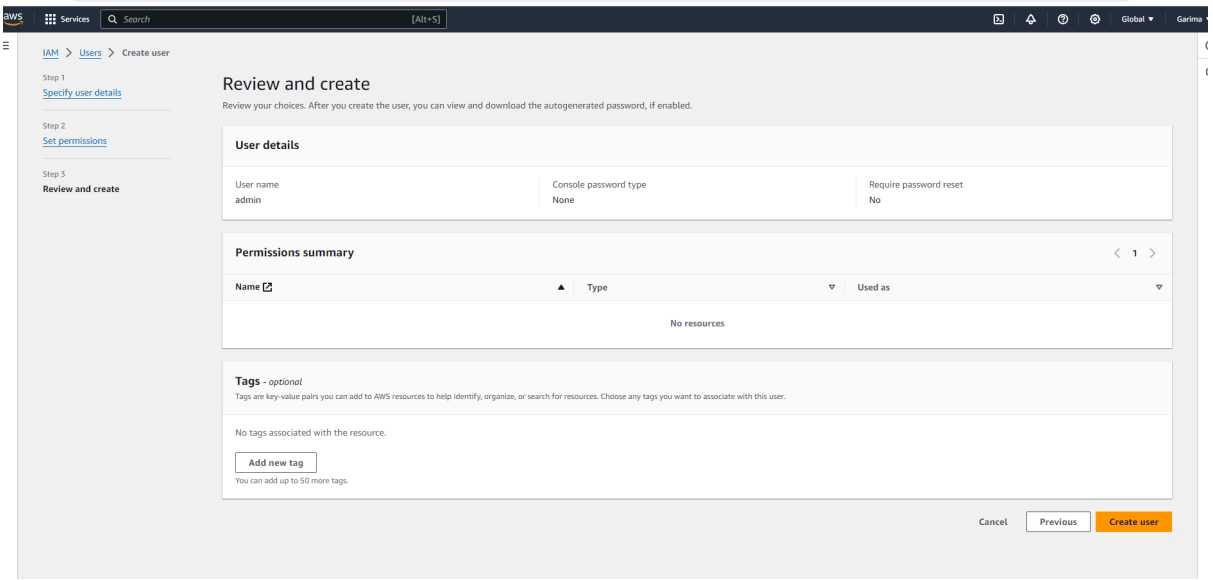
Select the “Create User” option



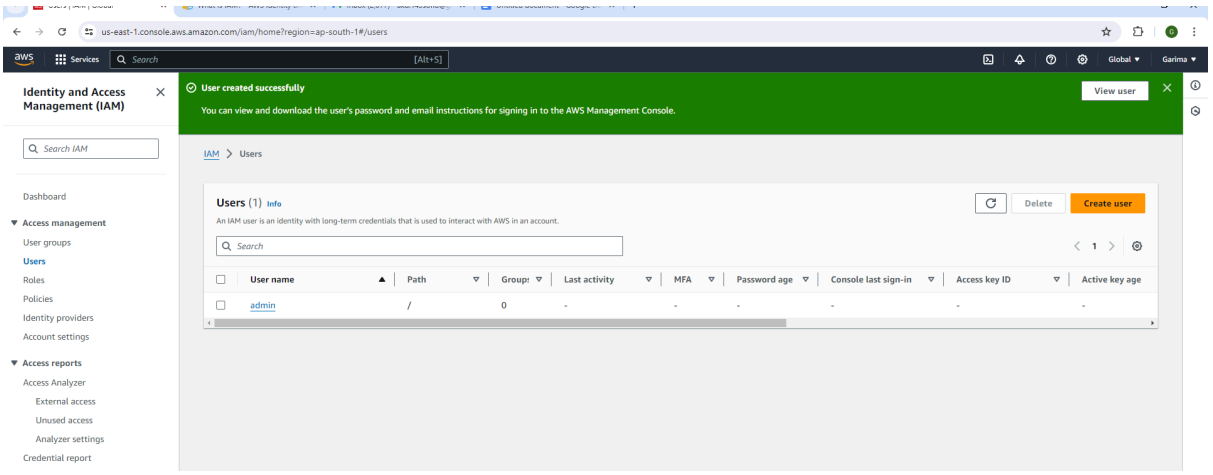
Given name to the user.



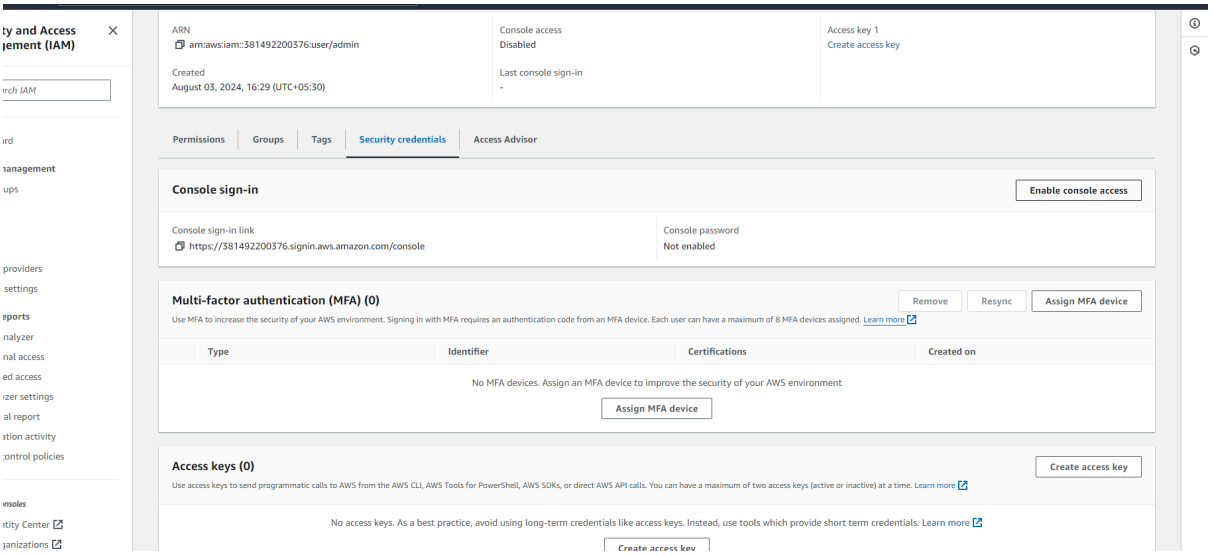
Select the first option of adding the user to the group and hit the next button



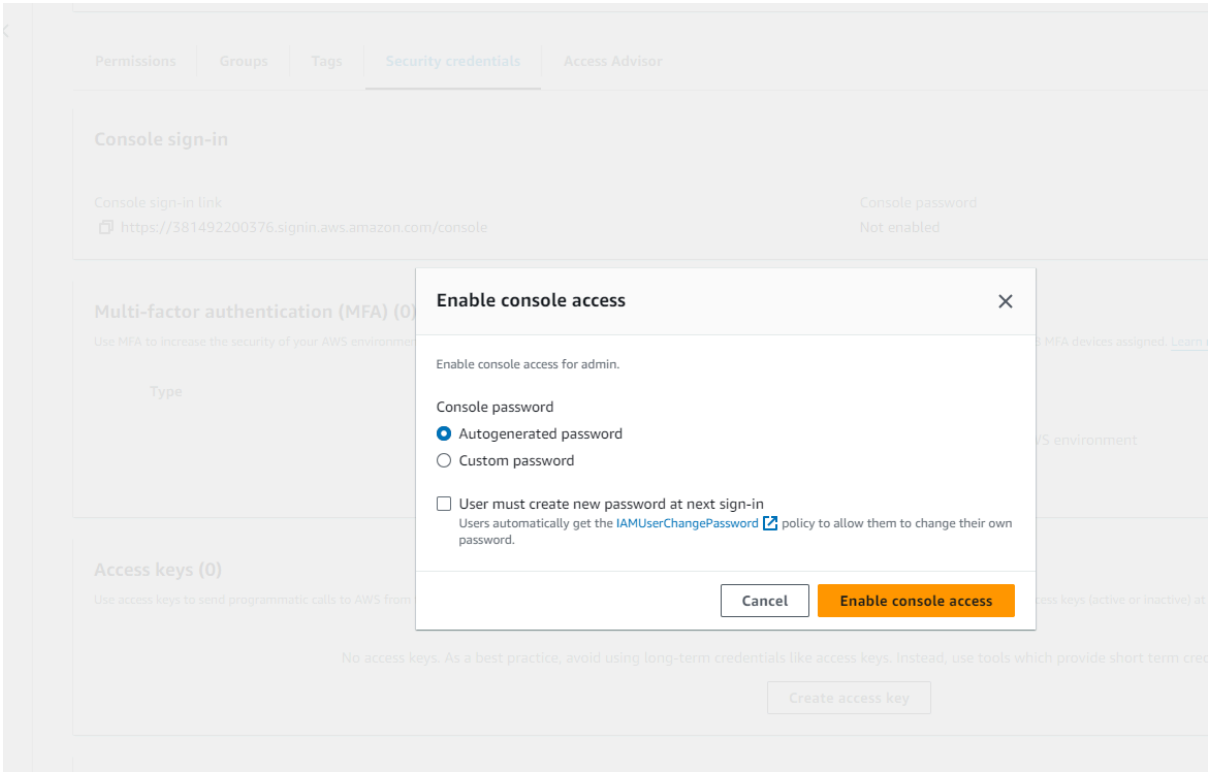
Review the details and hit the “Create User” button



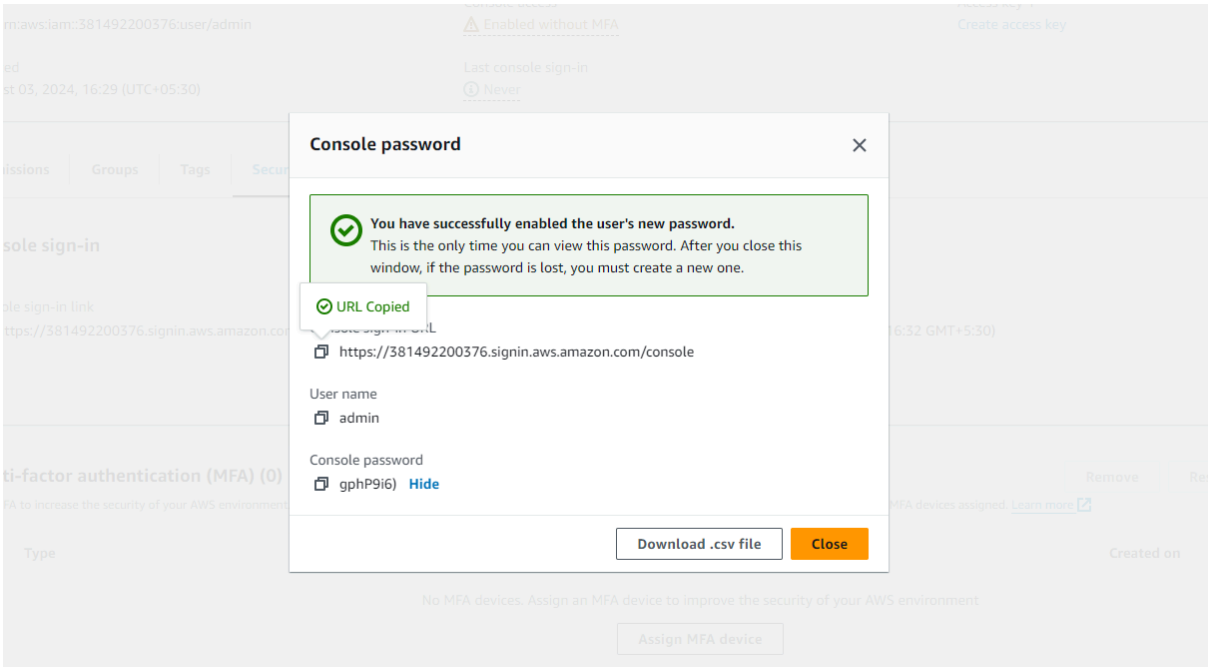
Open the user account “admin”.



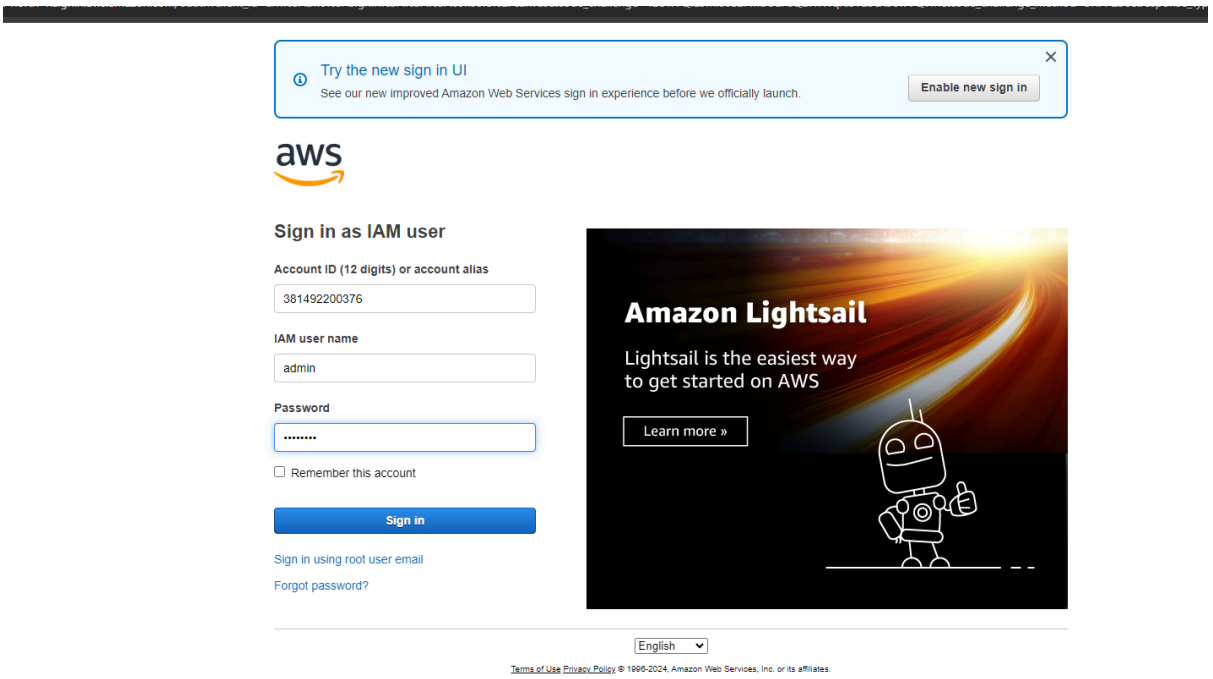
In the “Security credentials” section, in the “Console sign-in” section, click on “Enable console access”



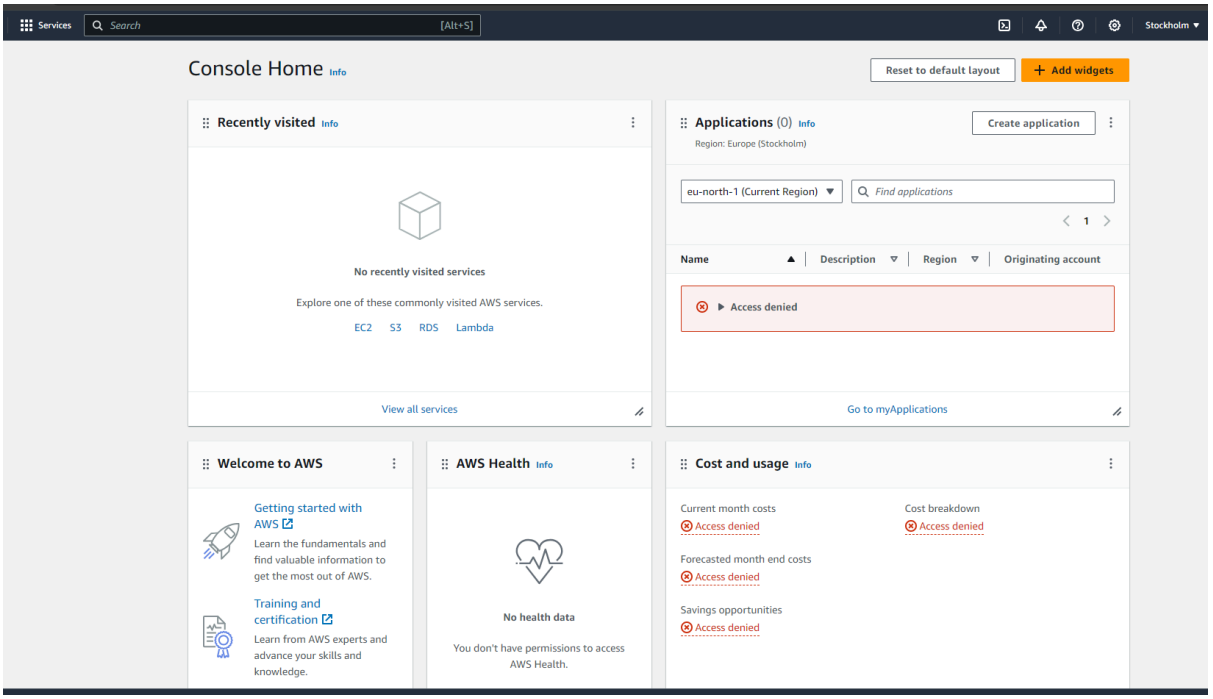
Here, select “Autogenerated password” and then click on the “Enable console access” button.



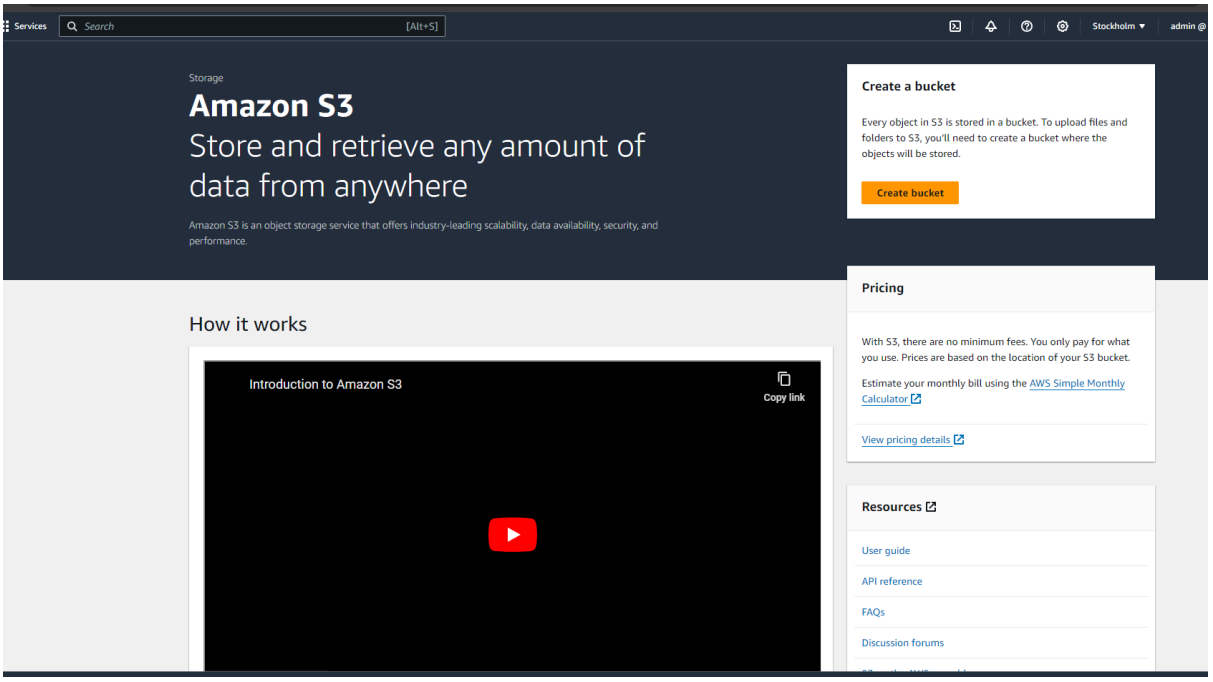
After creating the password, we get the password and the link for the admin user’s account. Download the .csv file. Copy the link and open the new account. Not to close this dialog box.



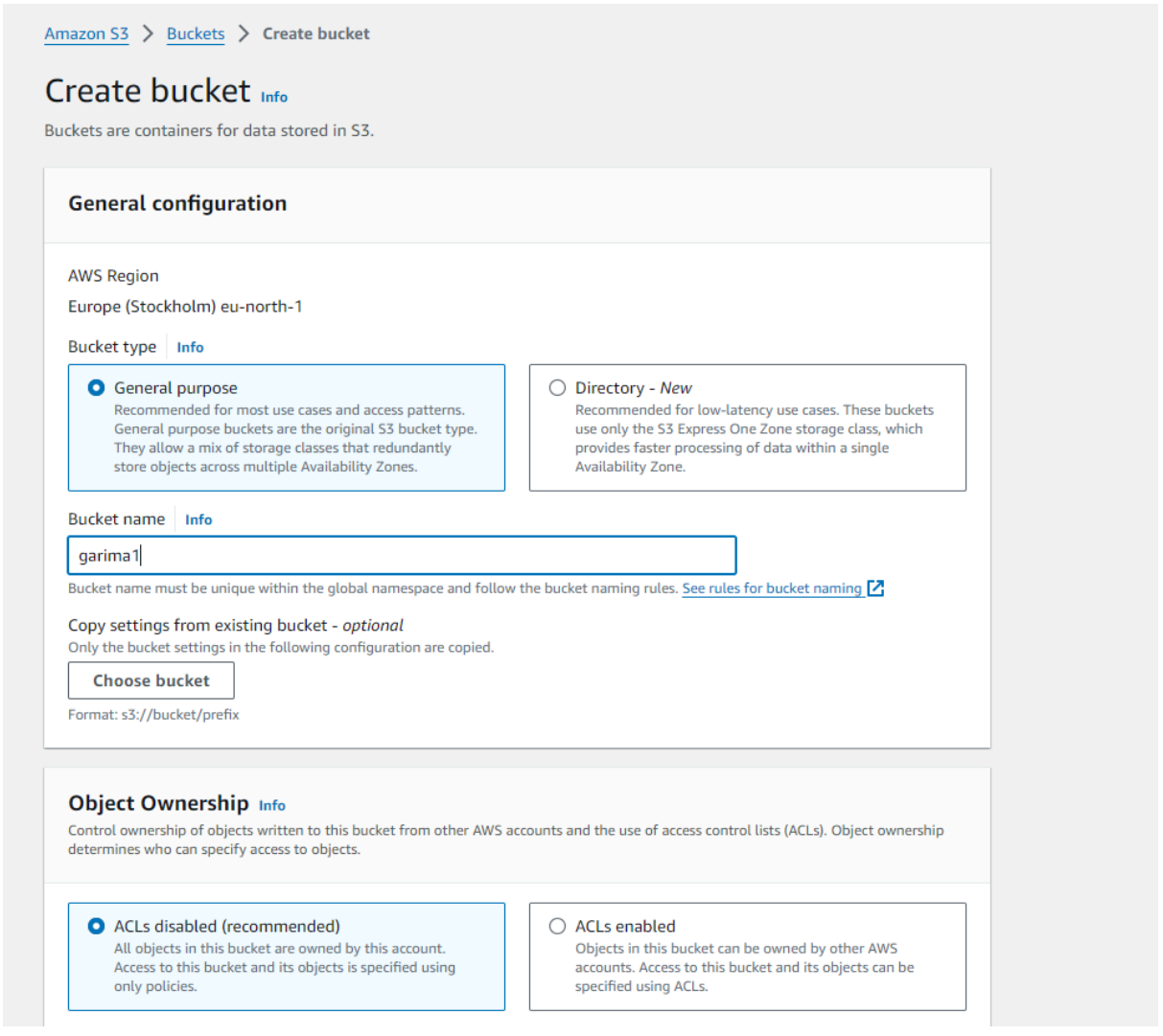
This is the page to sign in to the admin user's AWS account. From the before dialog box, copy the password and paste it here to sign in.



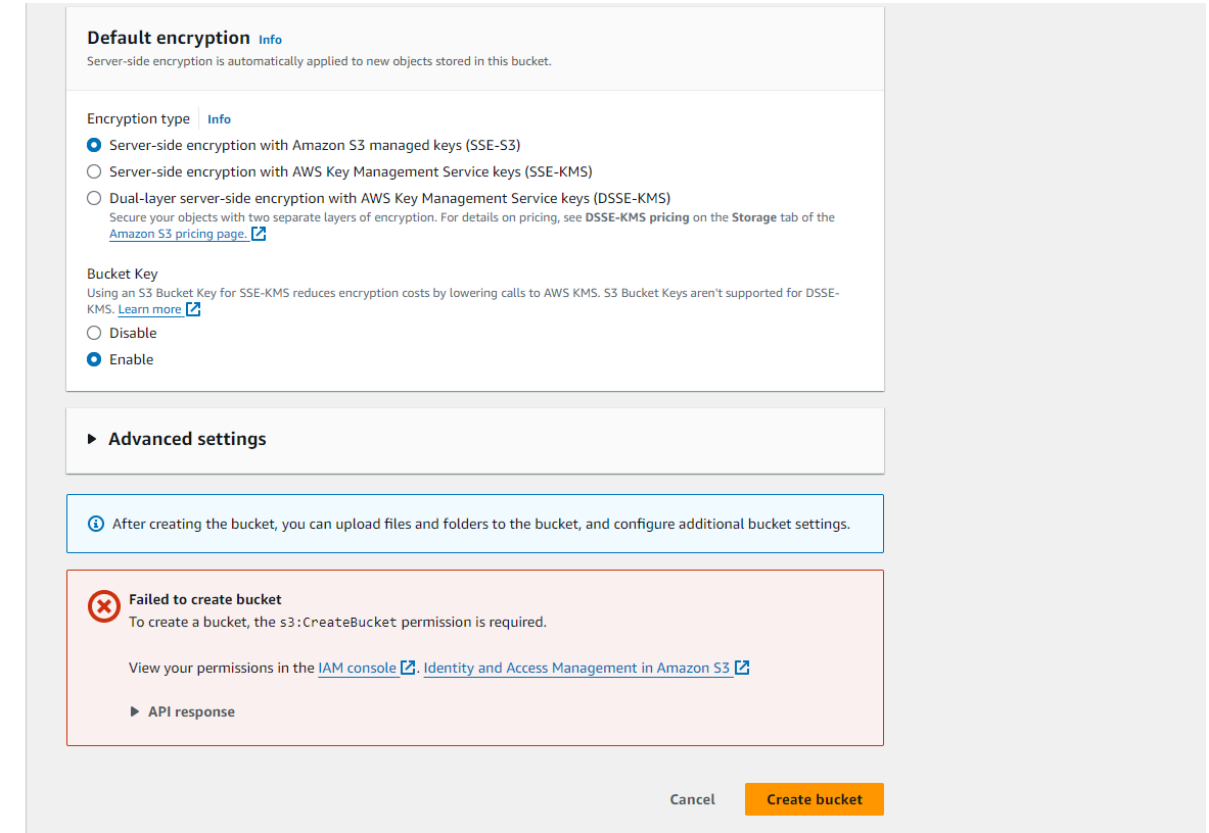
After signing in, this screen shows that the user cannot access the services, so the costs and applications section shows “Access denied”.
Eg, we try to create a bucket using the S3 service.



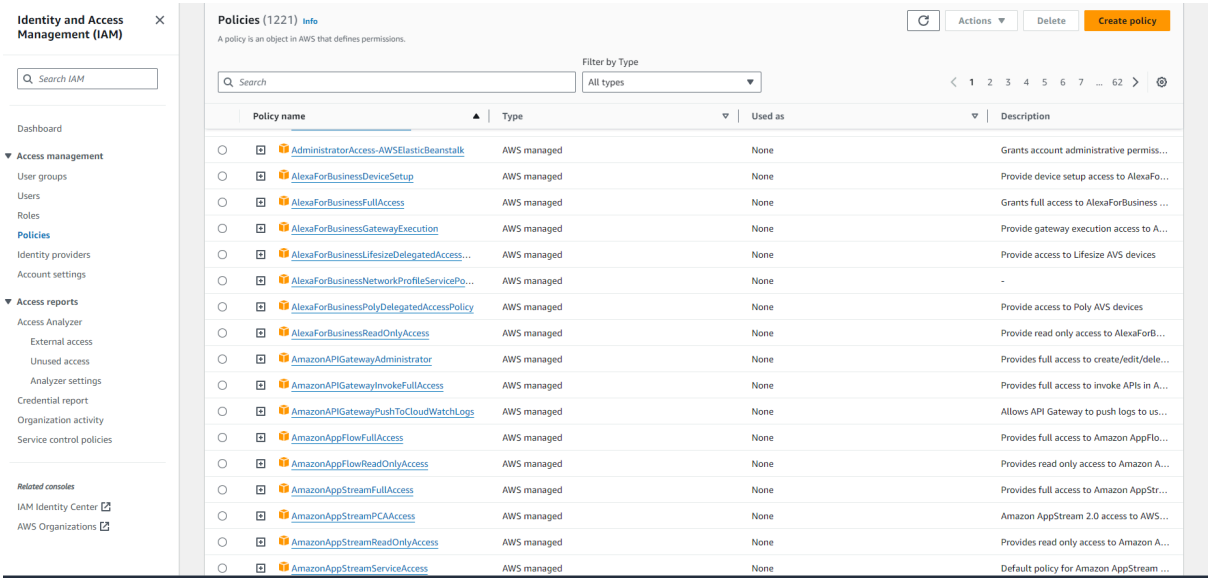
Click on the “Create Bucket” option.



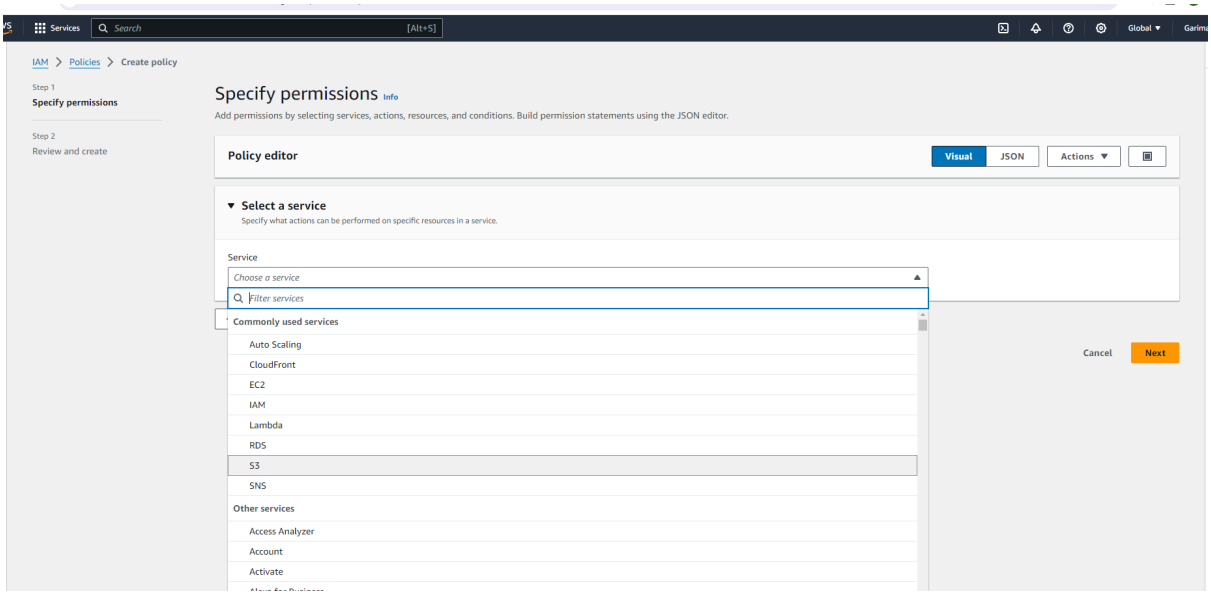
Select appropriate options for creating a bucket.



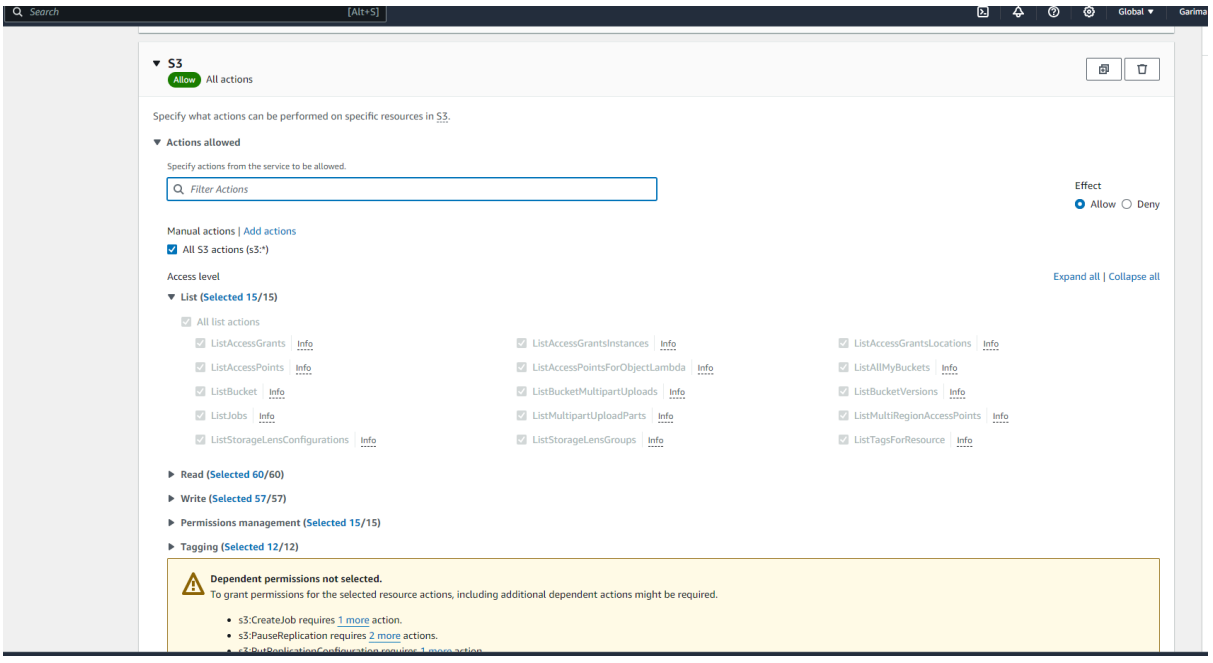
In the end, when we try to create the bucket, we get the message that the bucket cannot be made as the user “admin” doesn't have access to it.



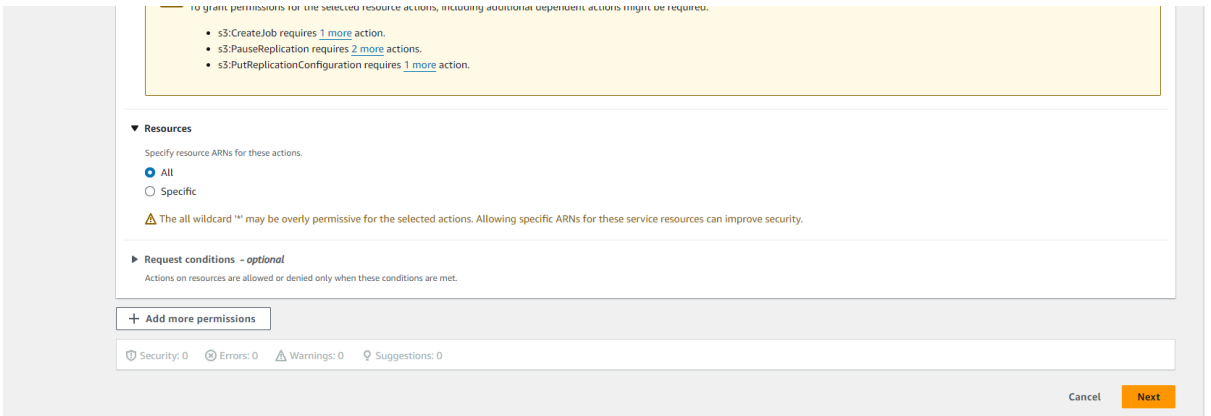
Go back to the root user’s account. On the left side, select “Policies” from the Access Management section. We get the above screen where we click on the “Create Policy” option.



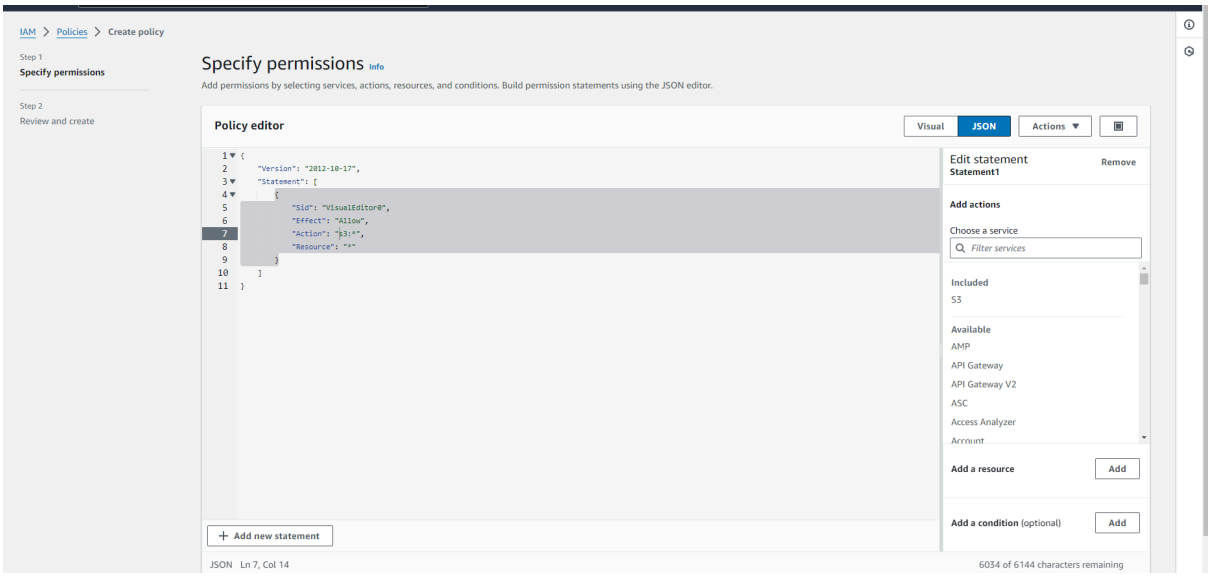
We get the above page. In the “Visual” section in the “Select a service” section, select “S3” from the drop-down list.



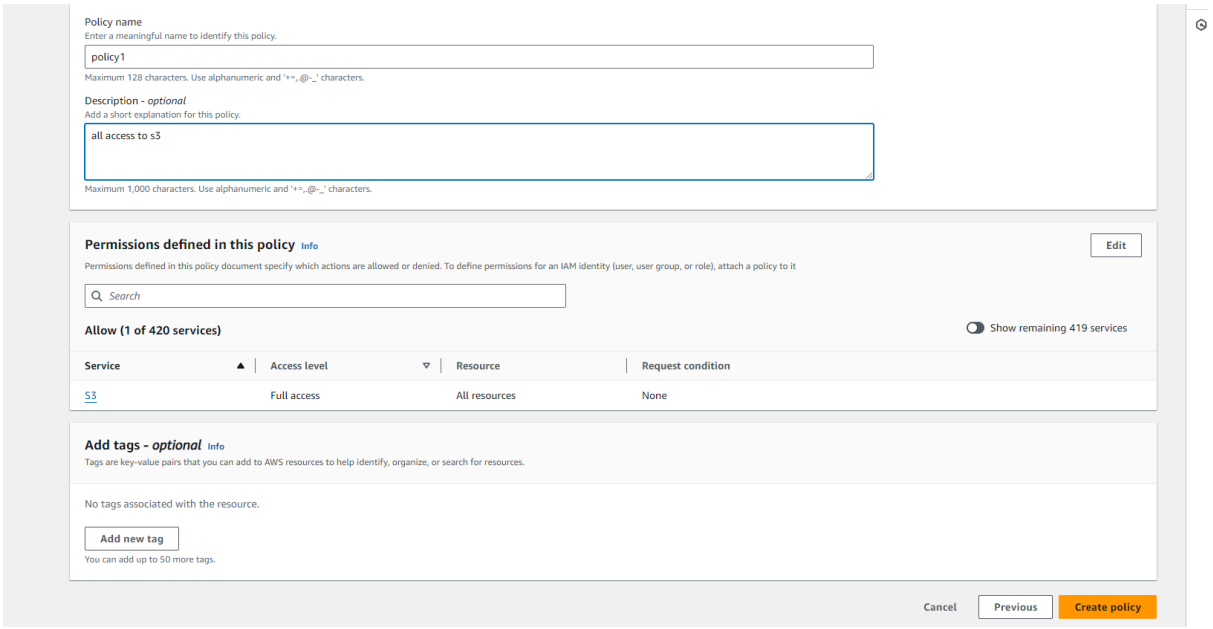
Select the checkbox for “All S3 actions”



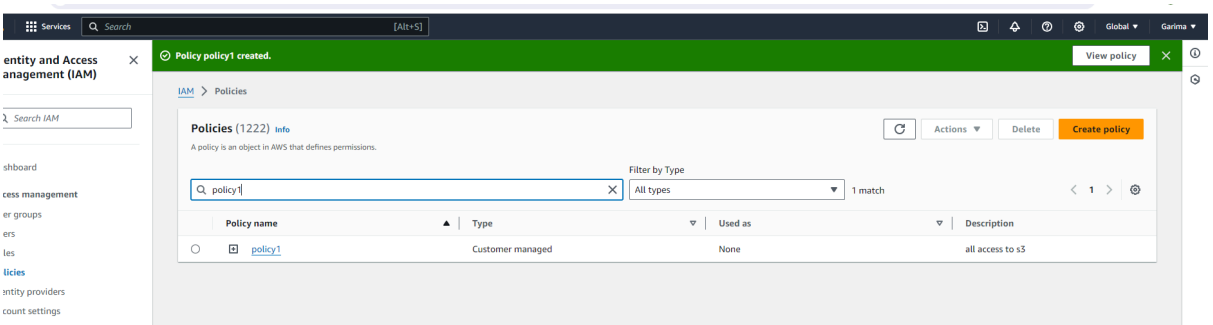
Select “All” resources. Click on Next.



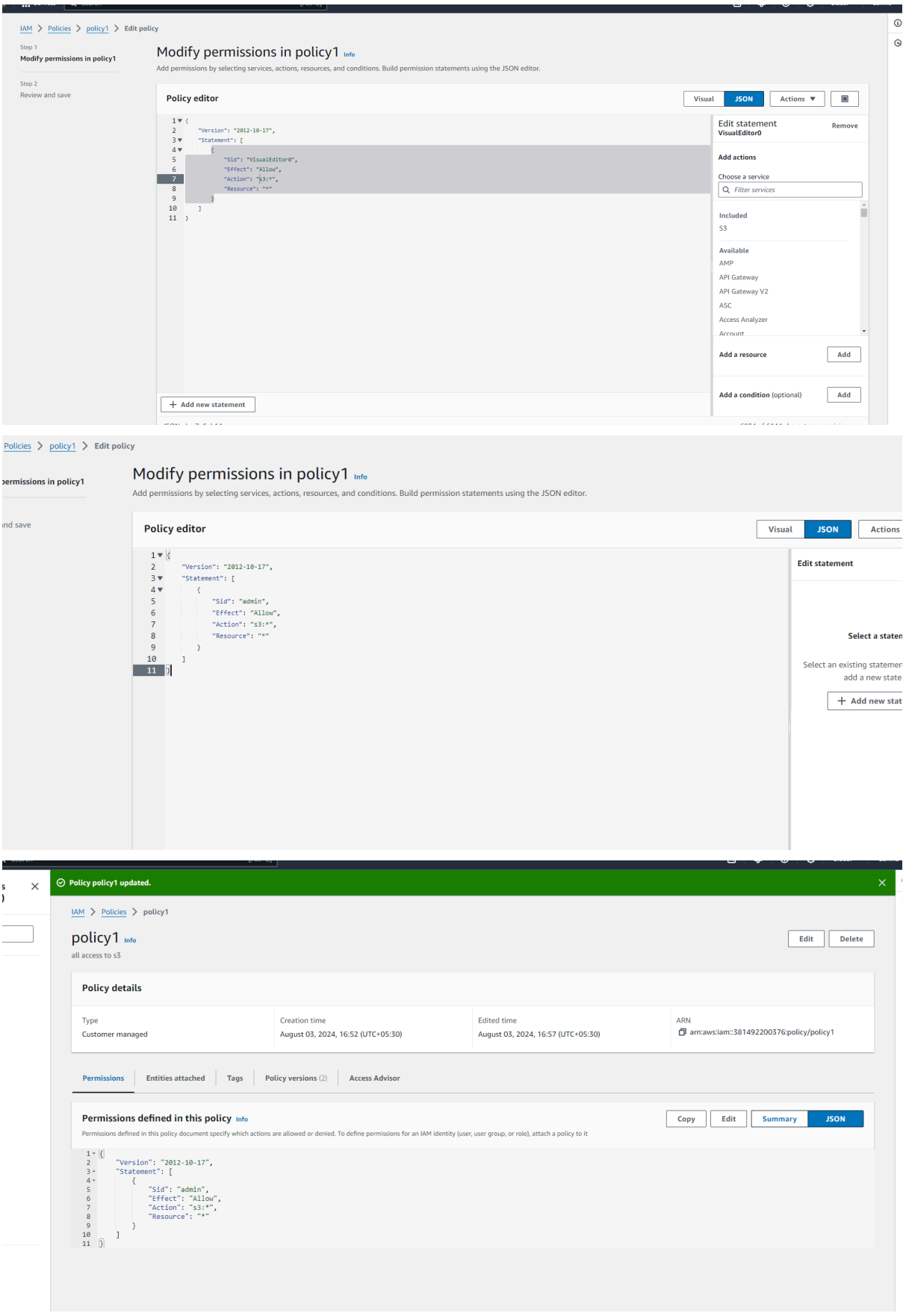
In the JSON section, change the name of “Sid” to the name of the user i.e. admin.



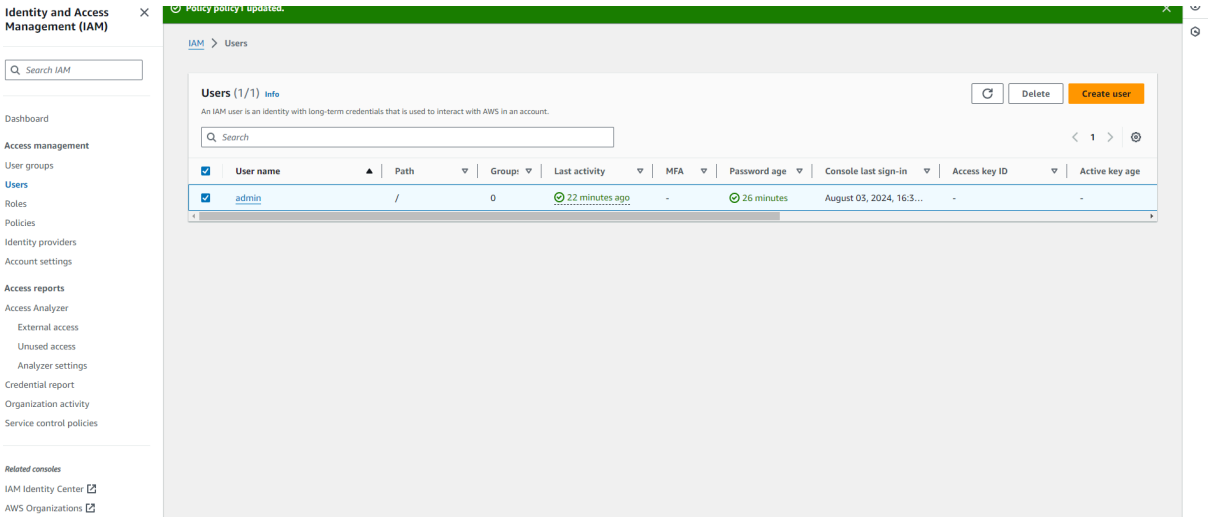
Give the policy a name and give a short description of the policy. Check the permissions defined for the policy. Then click on “Create policy”



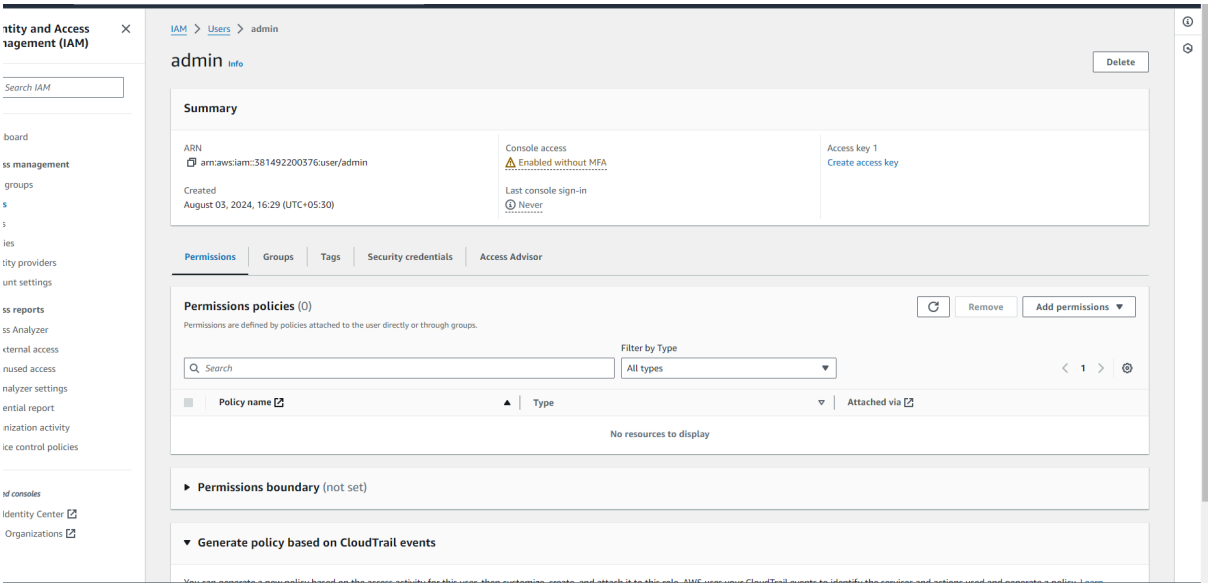
The policy is created.



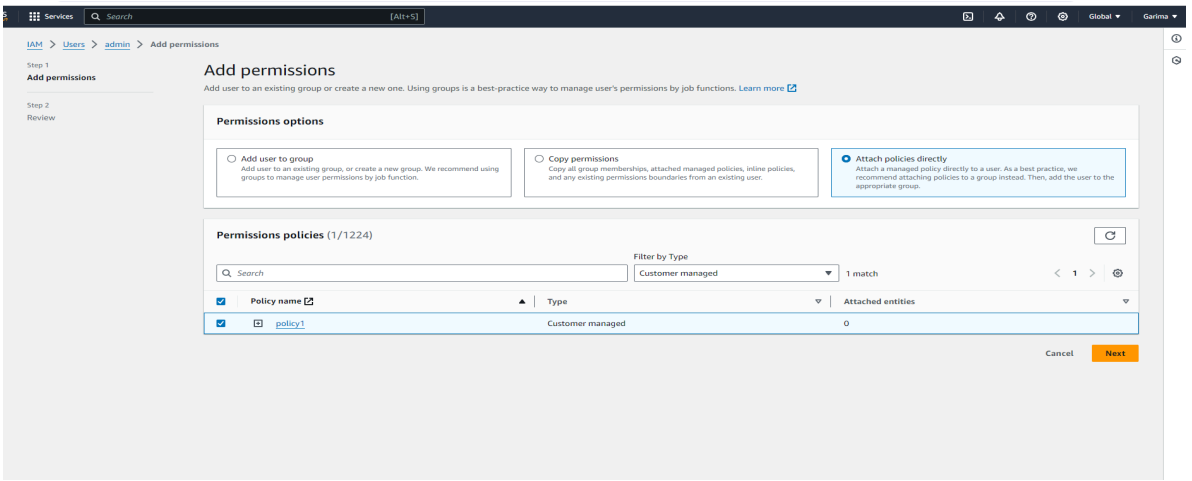
In case the policy needs to be edited, select the policy, select edit, make the edits, and update the policy.



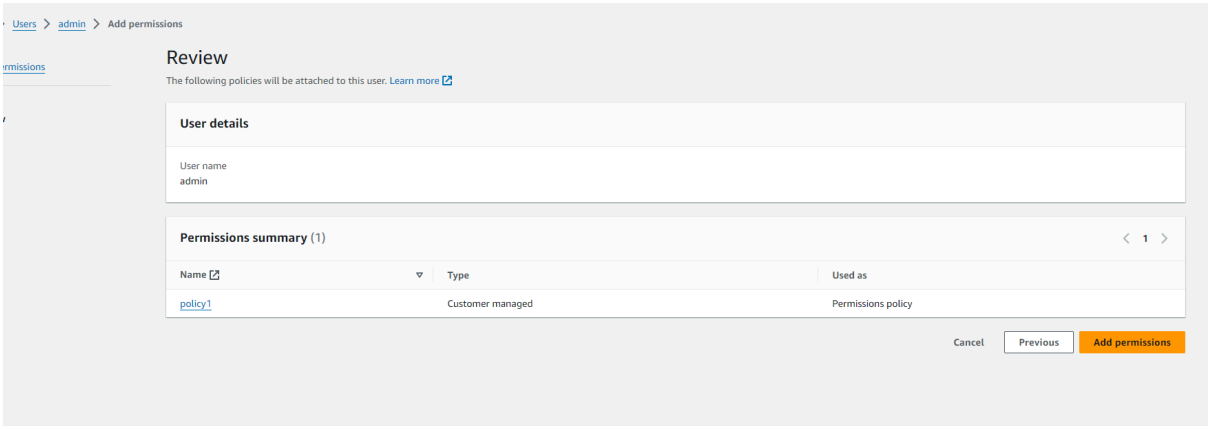
Go to users and select the admin user created before.



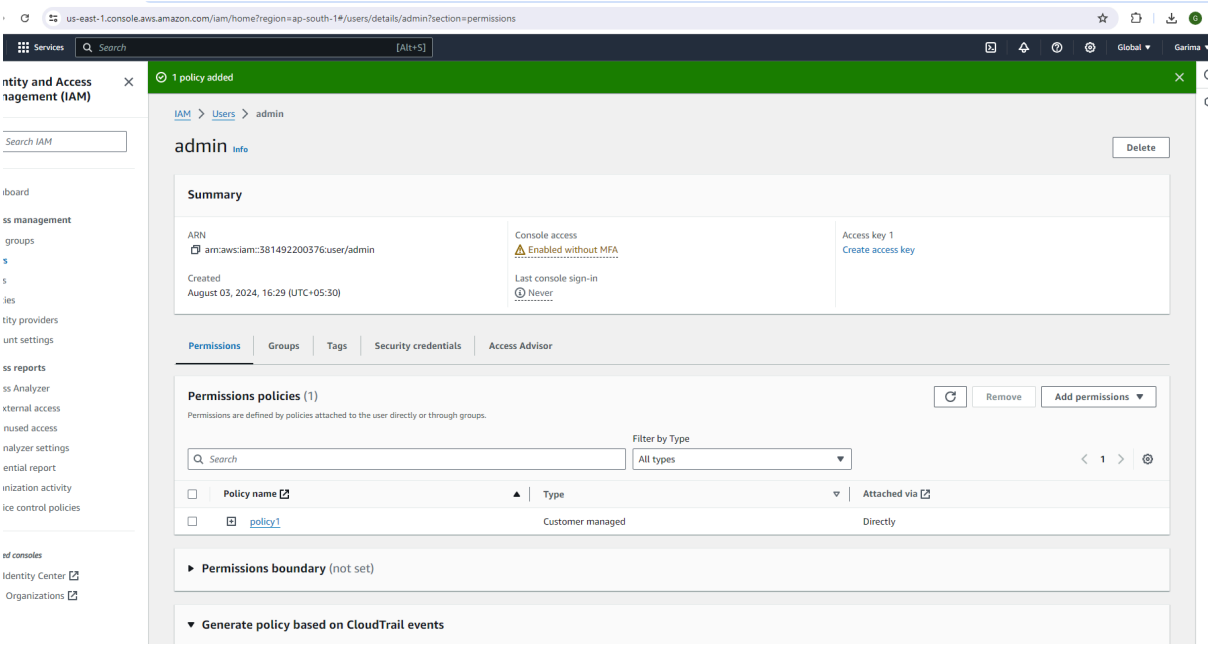
In the “Permissions policies” section, select “Add permissions” from the drop-down at the right corner.



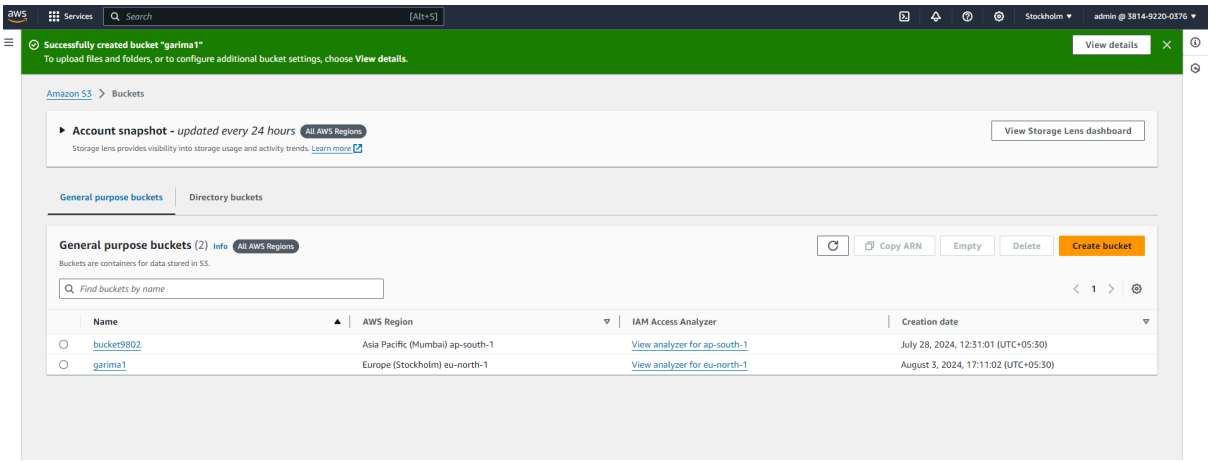
Select the policy created and above from the options, and select “Attach policies directly”. Click on “Next”



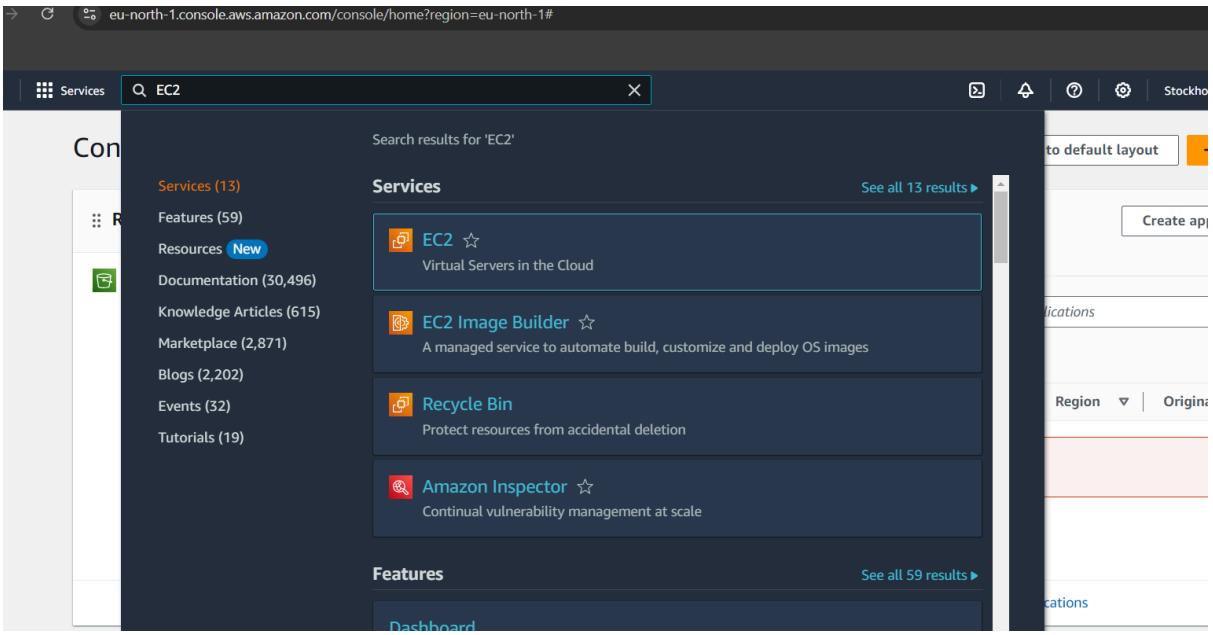
Check if the correct policy has been selected and then click on “Add permissions”.



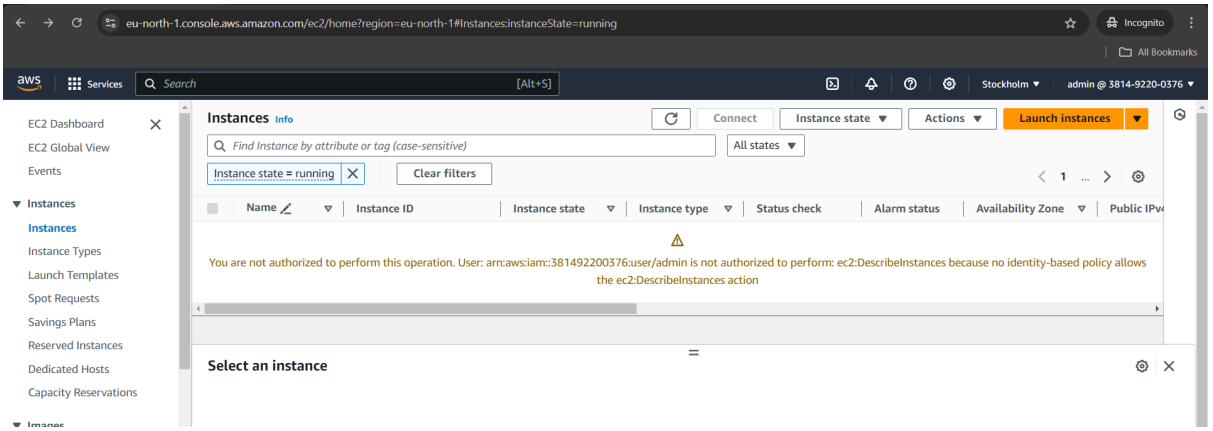
Then go back to the incognito page of the user “admin” account, and click on create bucket. This time a bucket will be created.



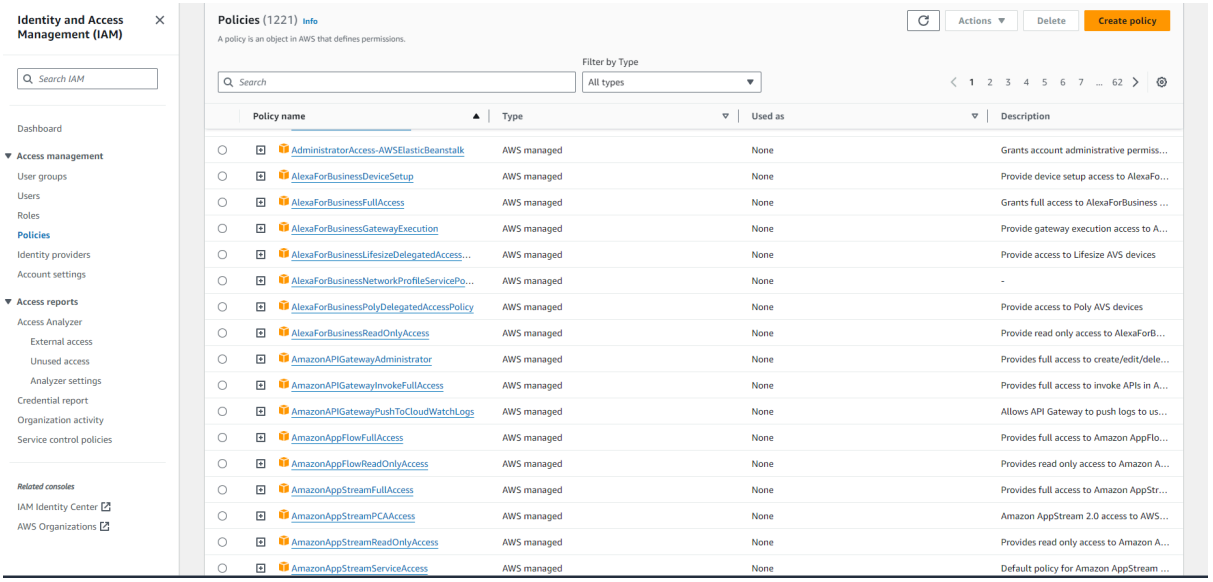
Now, we try to create an instance using the EC2 service.



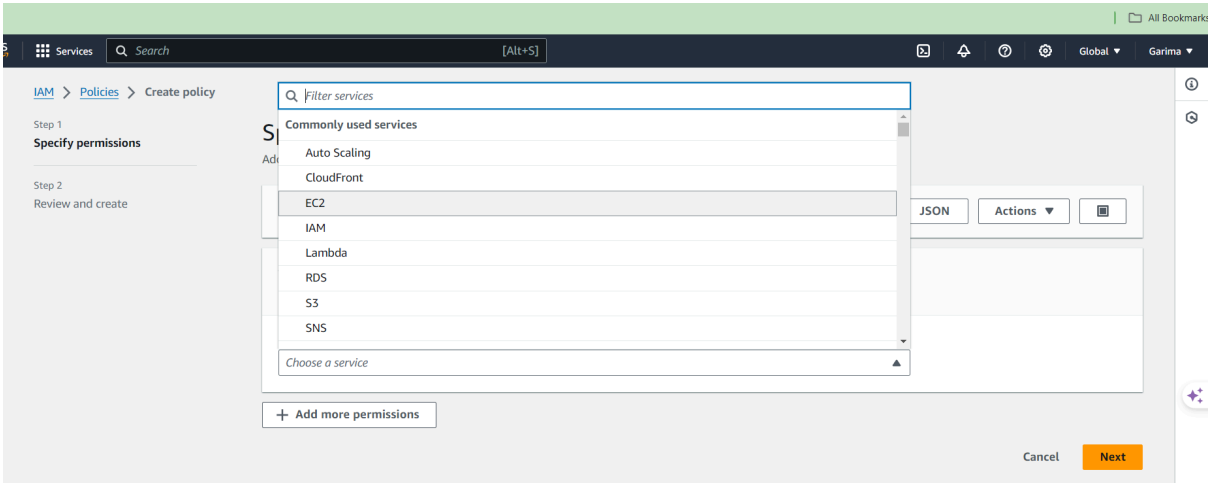
Select EC2 service.



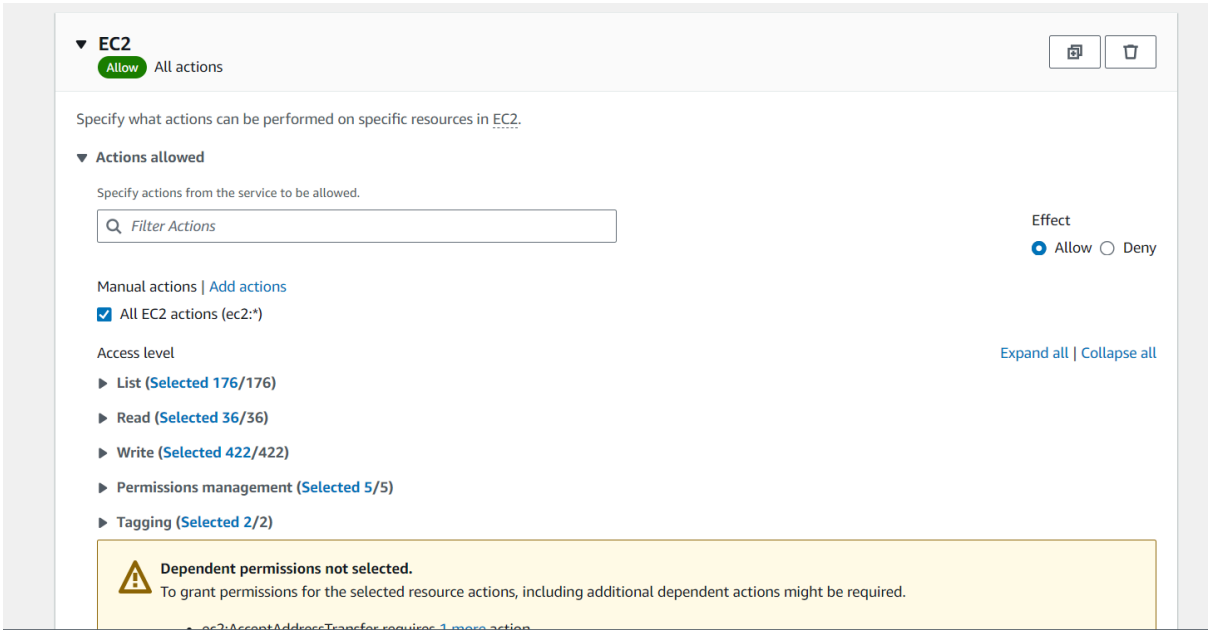
When trying to create an instance, we get the above message stating that no policy permits the user “admin” to create an instance.



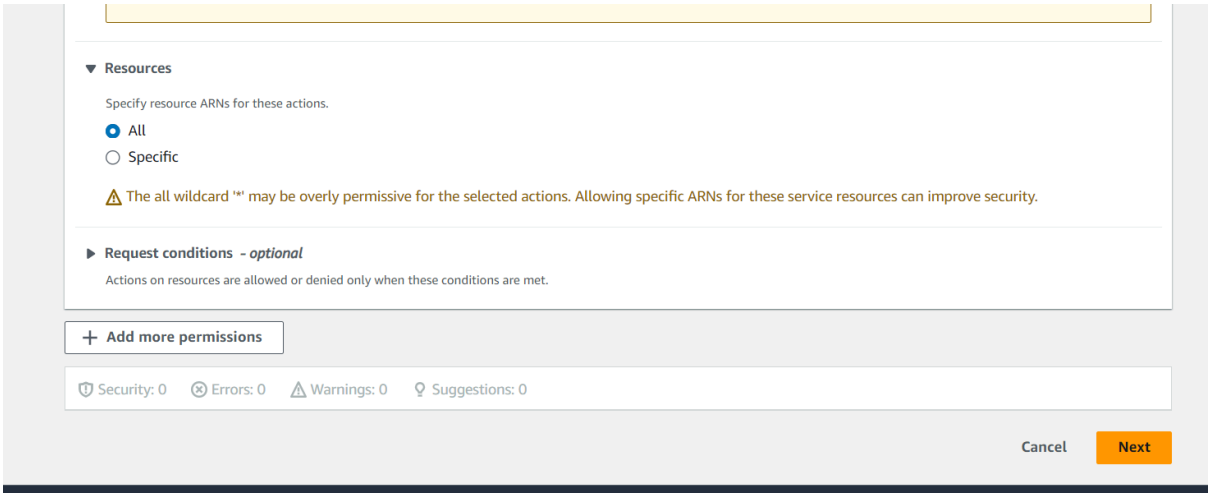
Go back to the root user's account. On the left side, select "Policies" from the Access Management section. We get the above screen where we click on the "Create Policy" option.



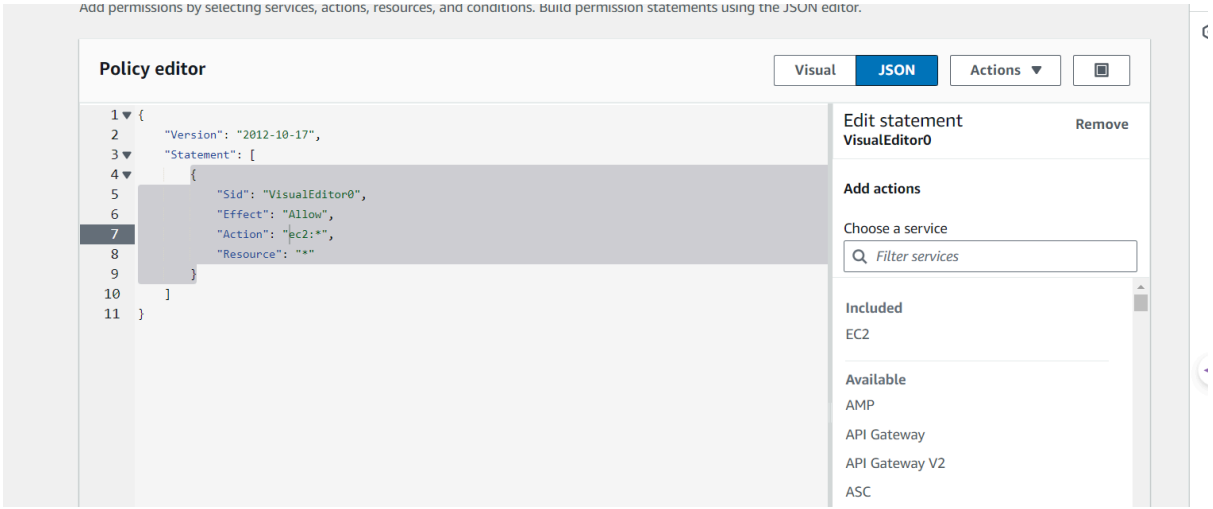
We get the above page. In the "Visual" section in the "Select a service" section, select "EC2" from the drop-down list.



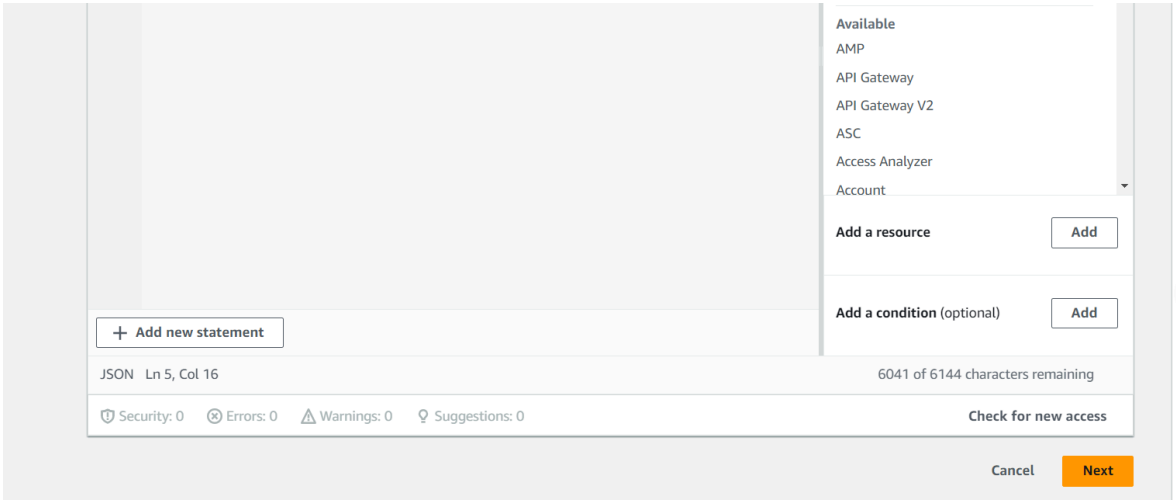
Select All EC2 actions to permit the user to perform all actions in the EC2 service.



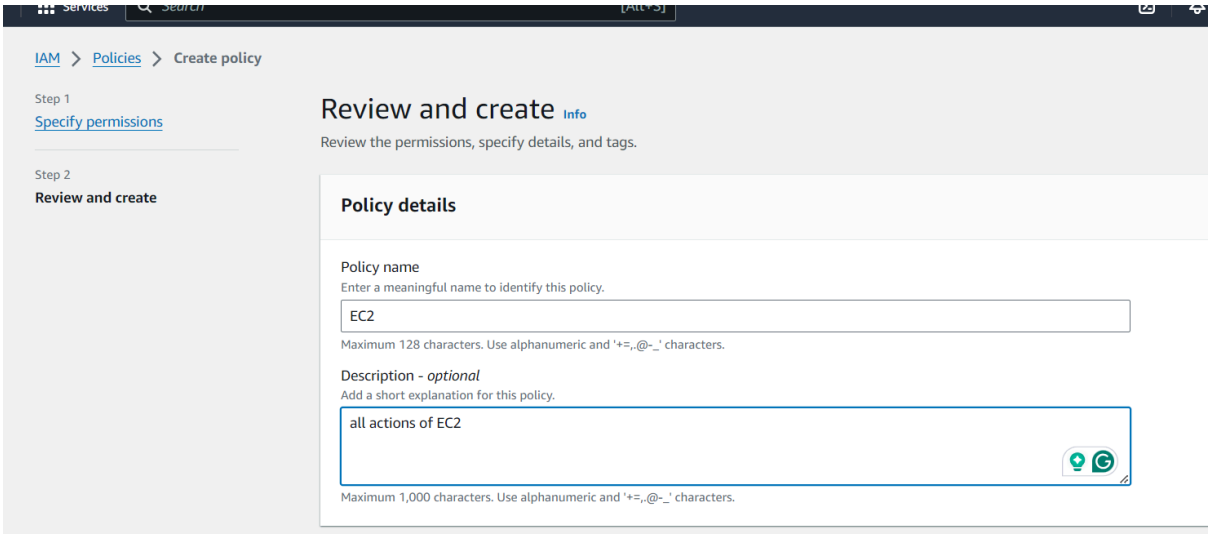
In the “Resources” section, select the “All” option. Then click “Next”.



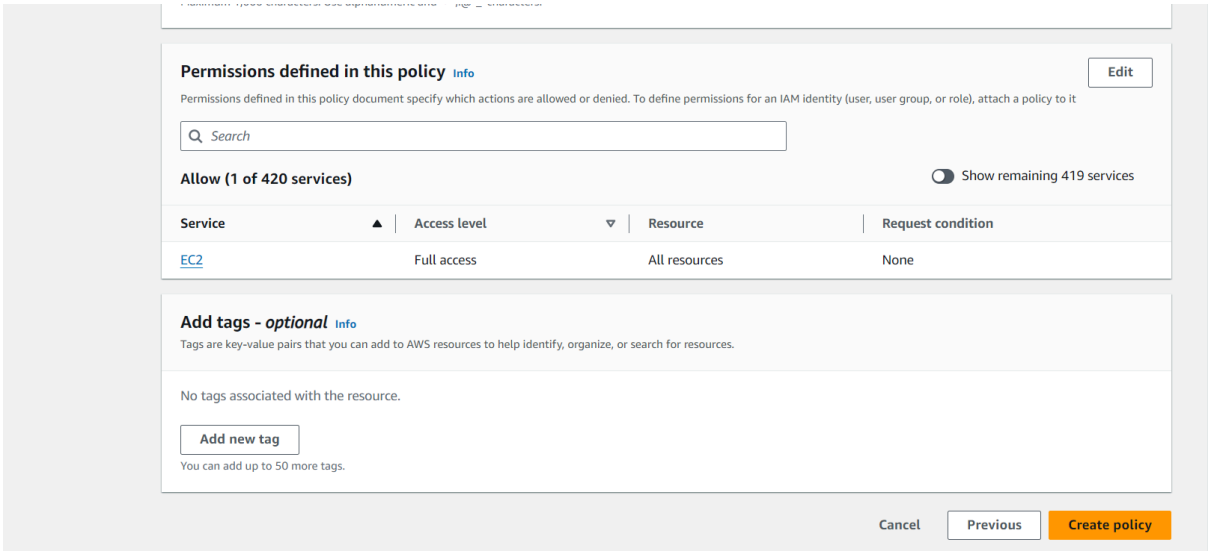
Then in the “JSON” section, change the name of Sid from “VisualEditor” to the user’s name i.e. “admin”.



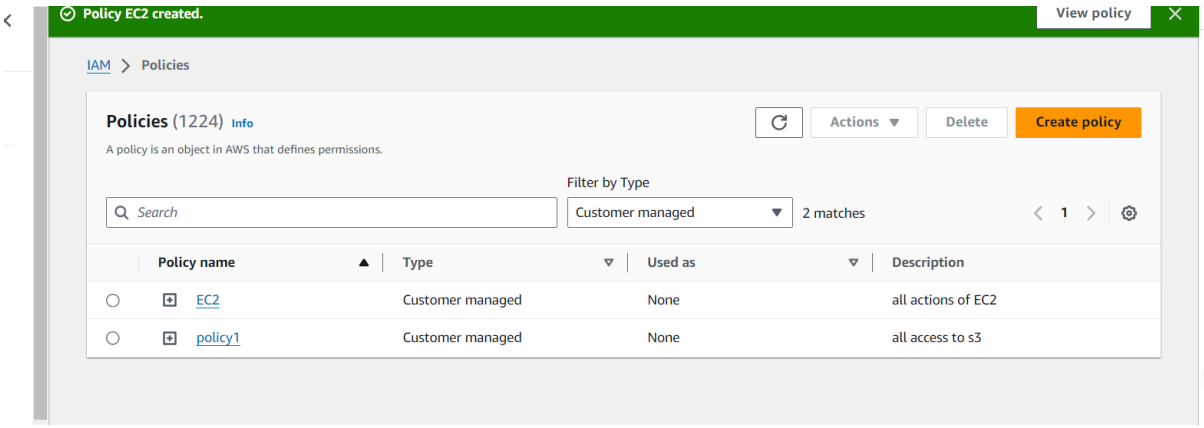
Click Next.



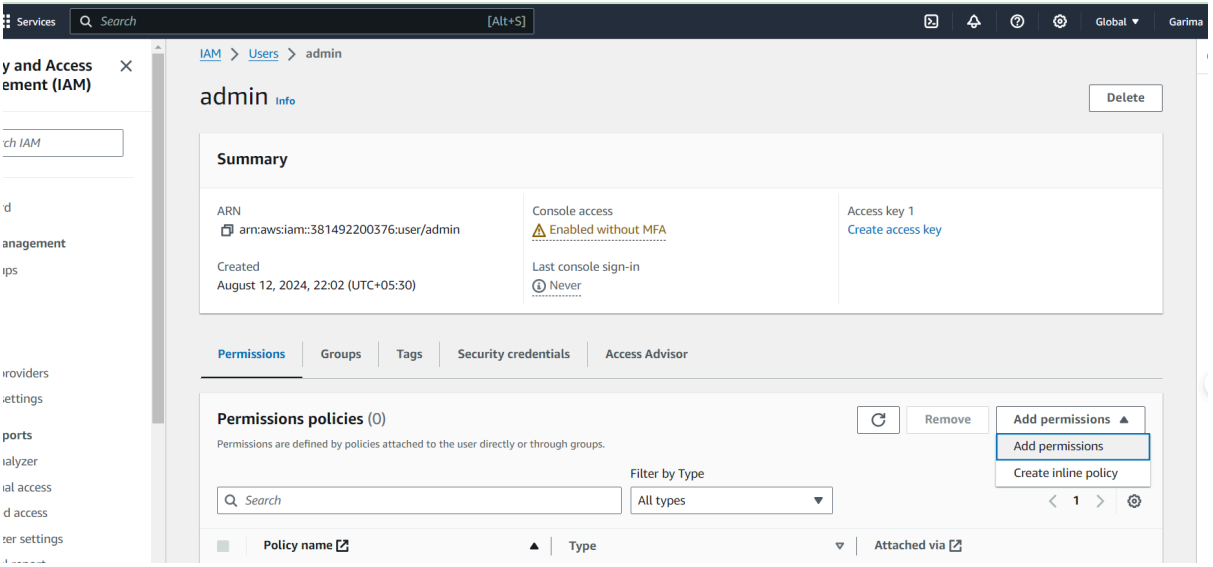
Give the policy a name and a short description.



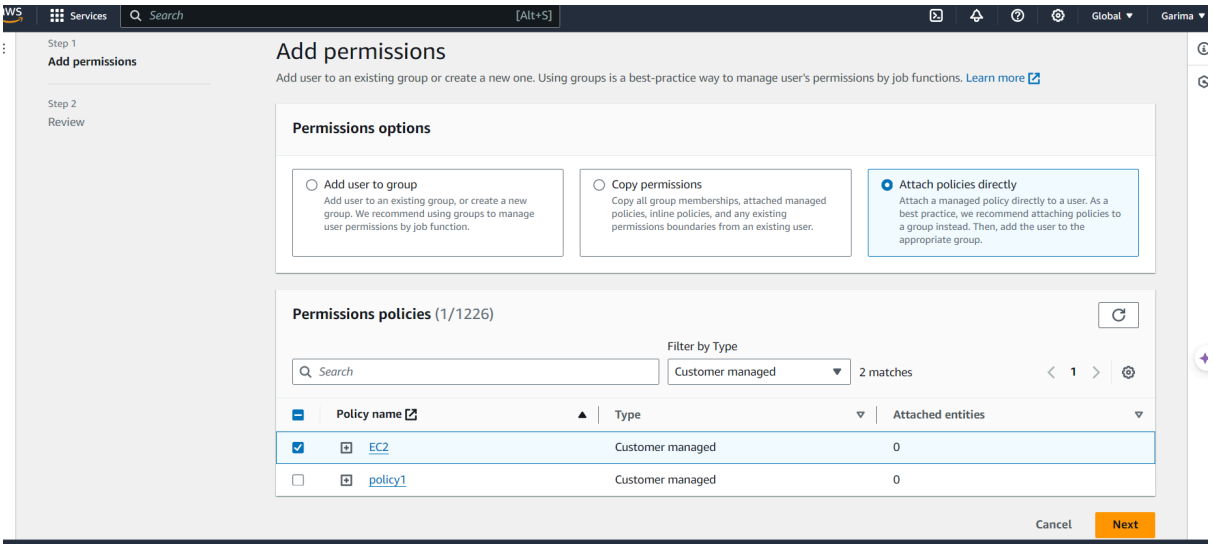
Click Create Policy.



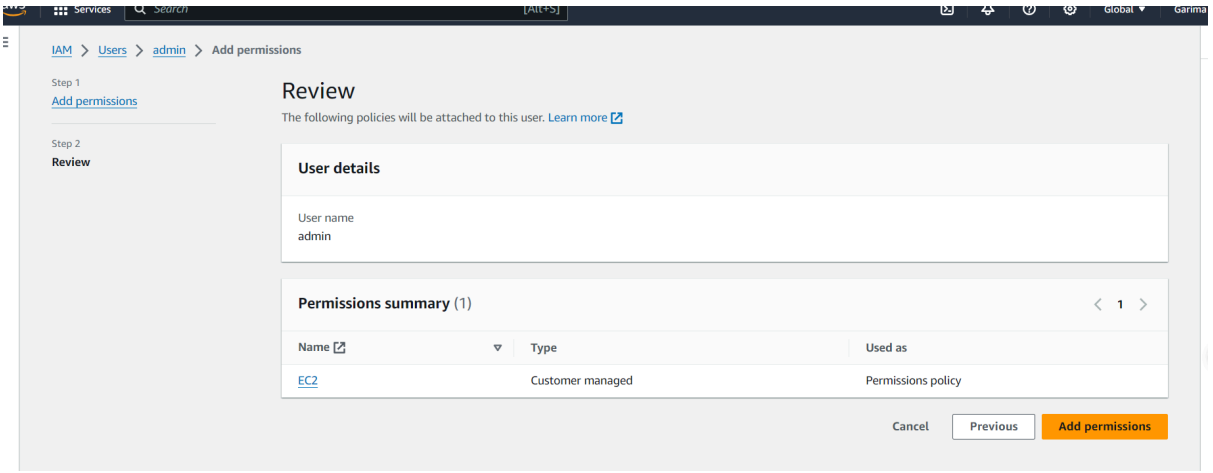
Here, we get to see the policy we created.
Go to users and select admin user.



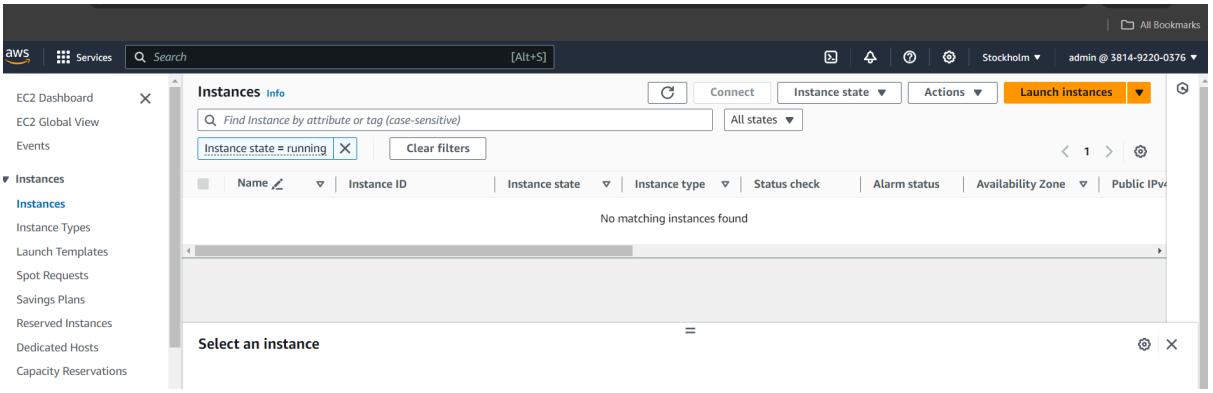
In the “Permission policies” section, select “Add permissions” from drop-down.



Select the “Attach policies directly” option. In “Permission policies” filter as “Customer managed” and select the policy “EC2”. Click “Next”.



Click on “Add permissions”.



After going back to the incognito tab where the admin user’s account is open, refresh the page. Now no message regarding permission issues is shown, indicating we can create an instance now from this account.