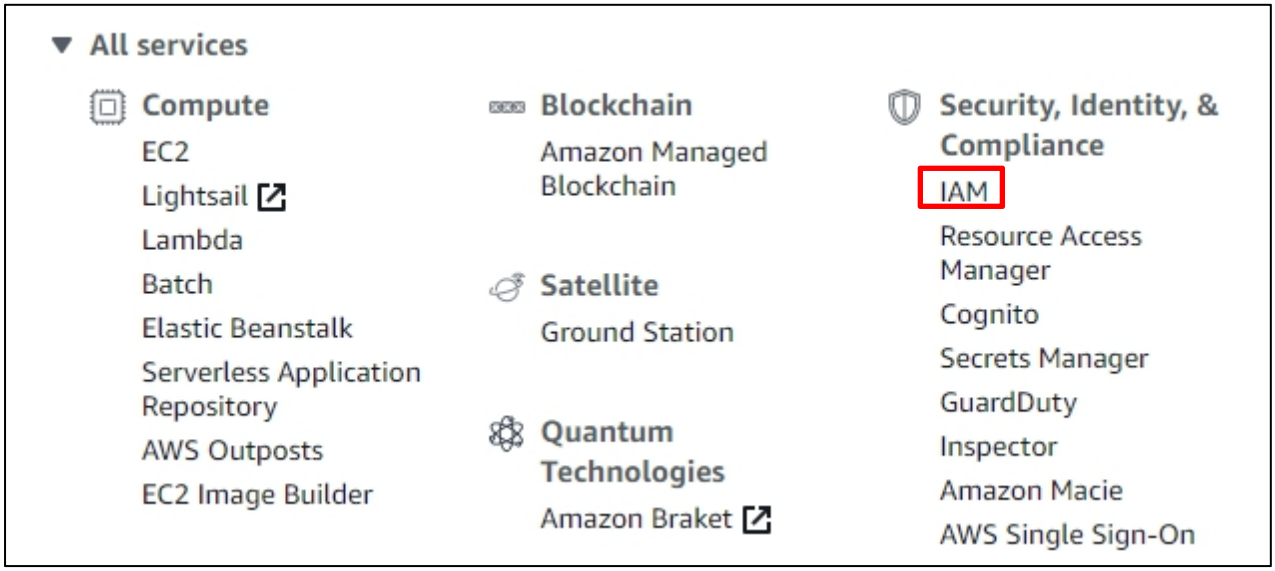
Module 2: Security Management in AWS

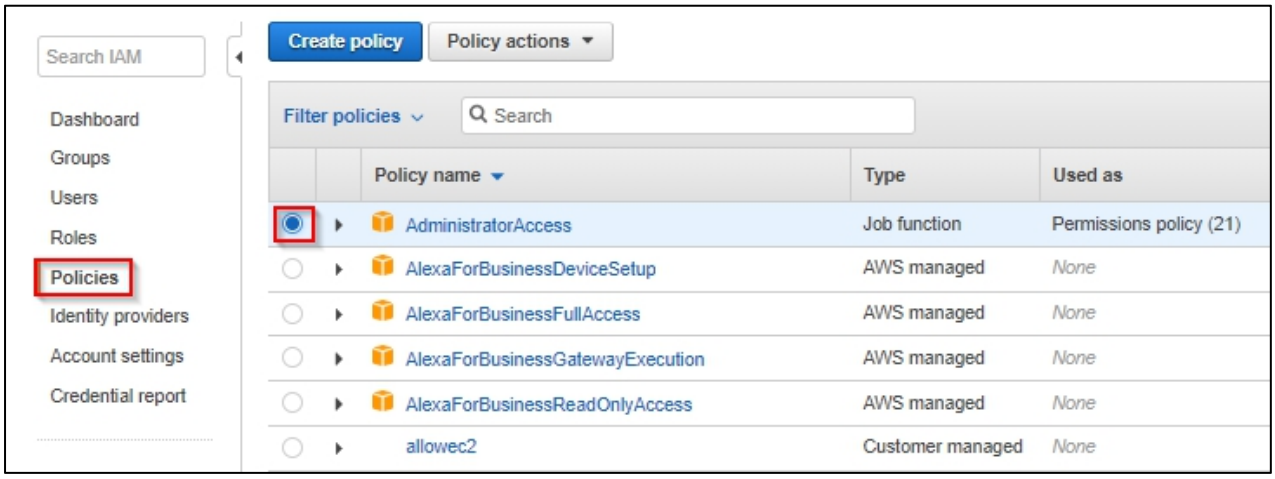
Demo Document 3

Creating Policies for New User to Have All Admin or Limited Privileges

Step1: Go to the AWS Management Console and select **IAM** under Security, Identity & Compliance.



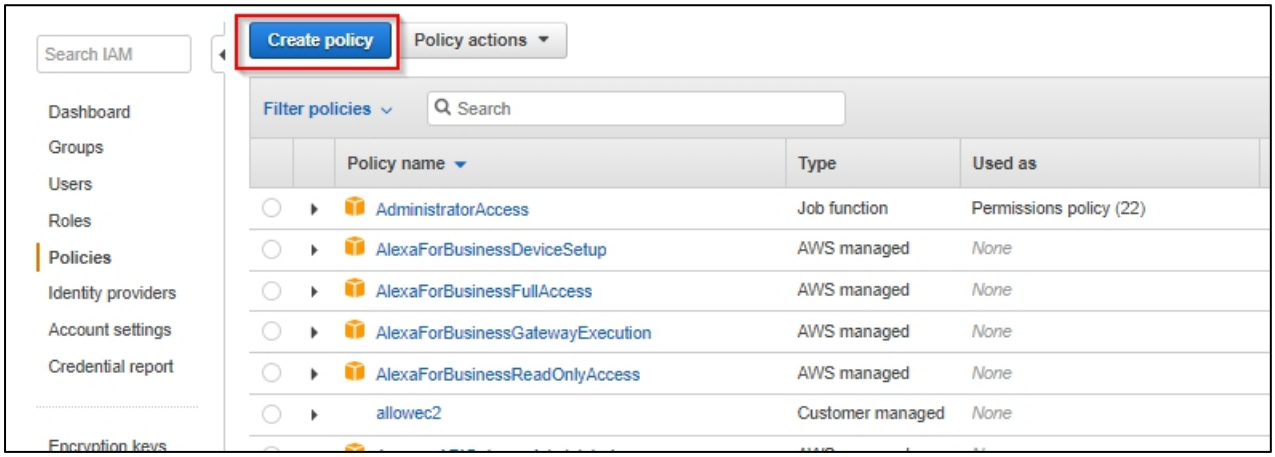
Step2: Creating Policies for New User: Move to **Policies** section under IAM and select **AdministratorAccess**. (By attaching this policy, the user gets the admin access to all the services)



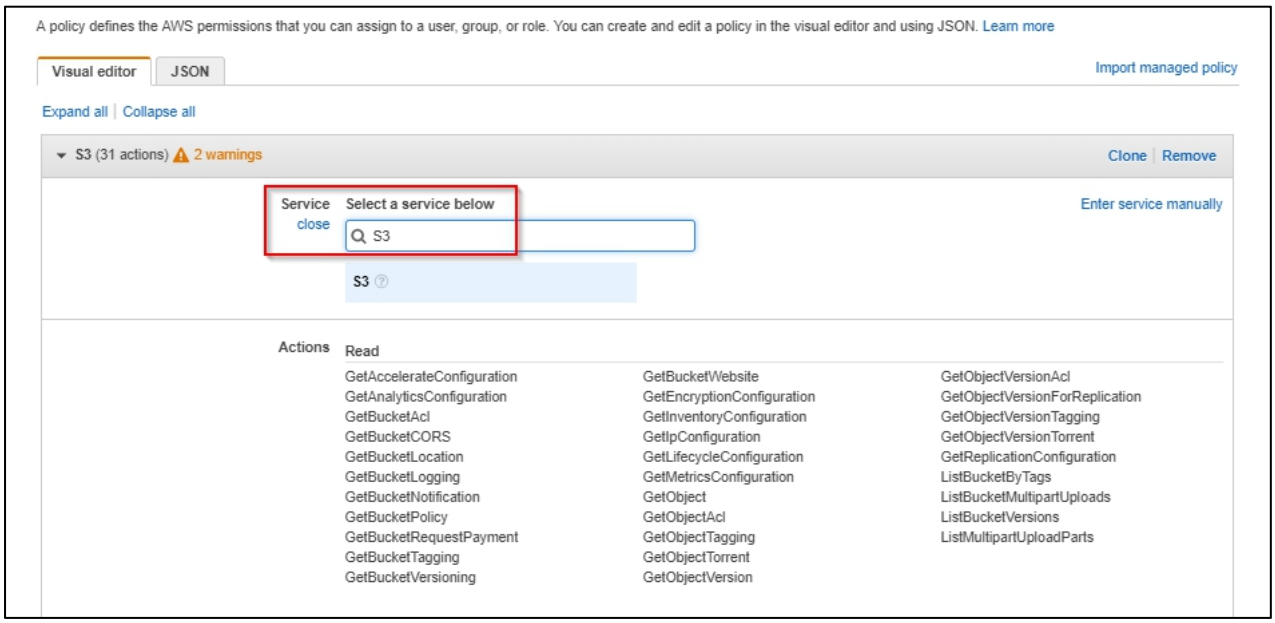
Note: *To provide limited access to the user, you can create such a policy and attach it to the user.*

For example, let us create a policy that provides the user the permissions of only the **list and read** to all objects in an Amazon S3.

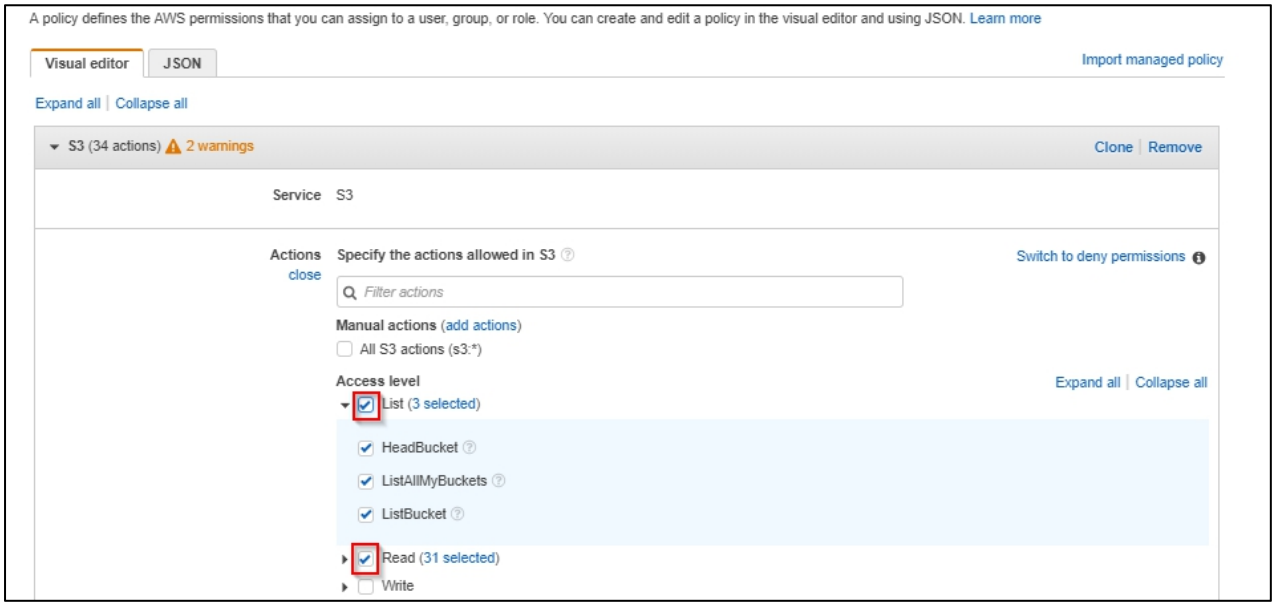
Step-3: Go to **Policies** and click on **Create policy**.



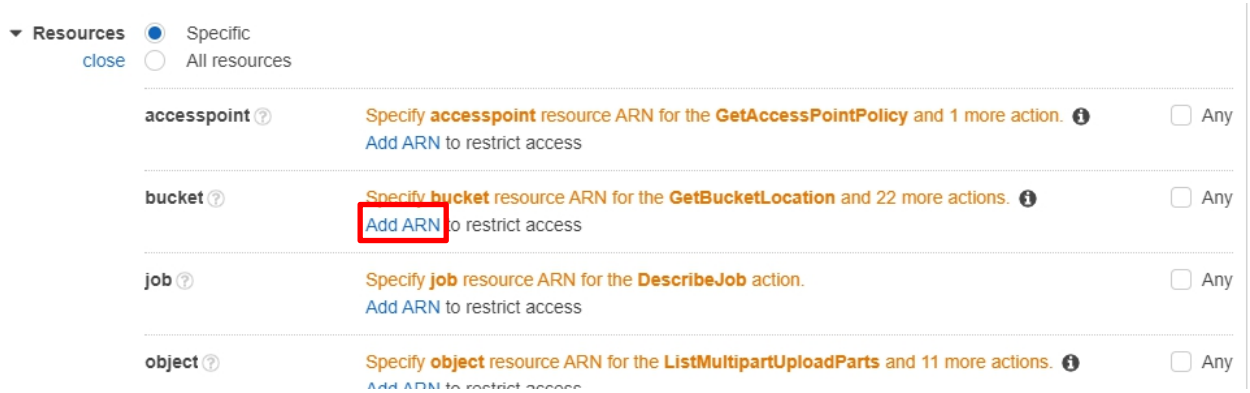
Step-4: Go to **Visual editor** under **Service** and choose ***S3*** service.

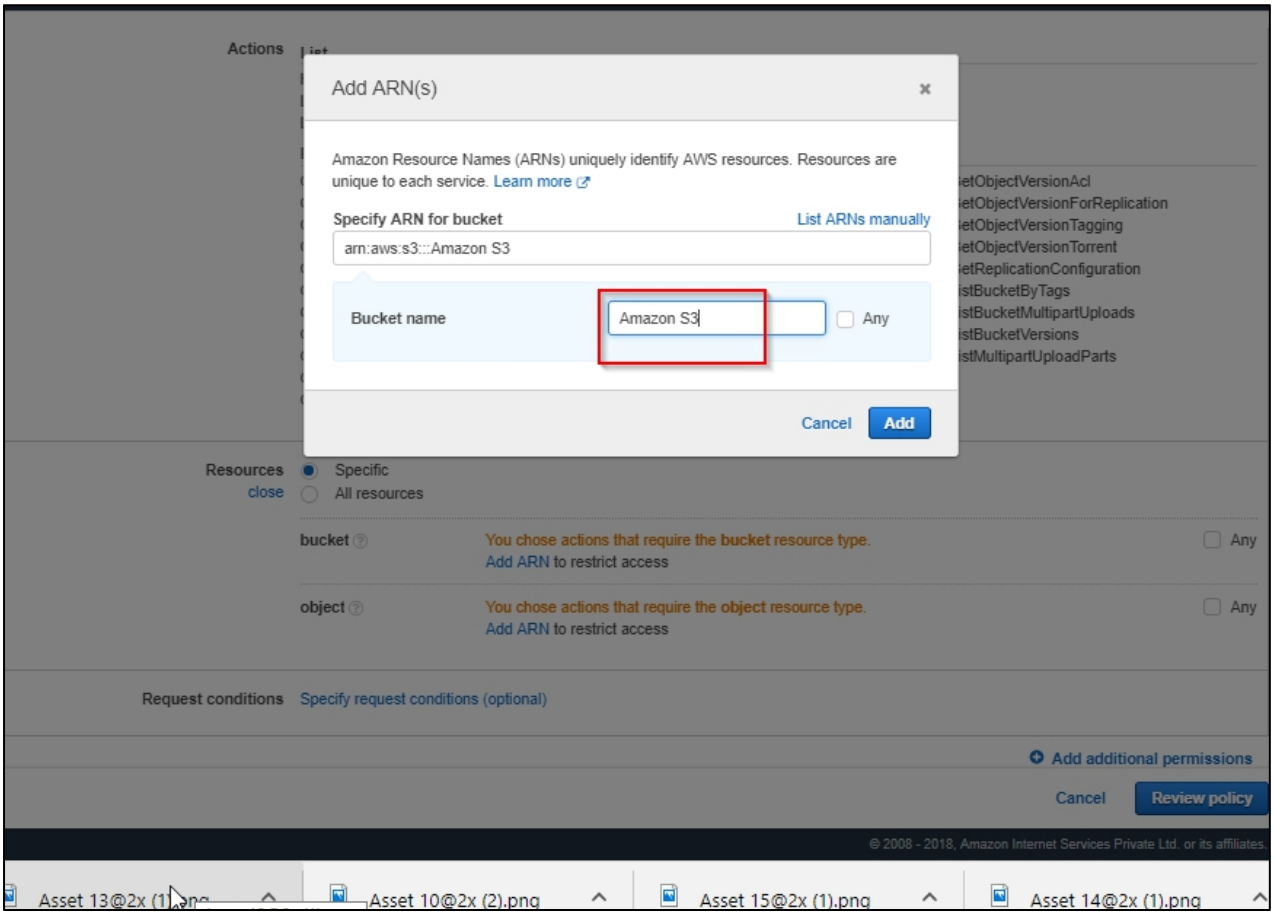


Step-5: Under **Action**, you can choose the action you want to perform. For now, let's select **List** and **Read.**

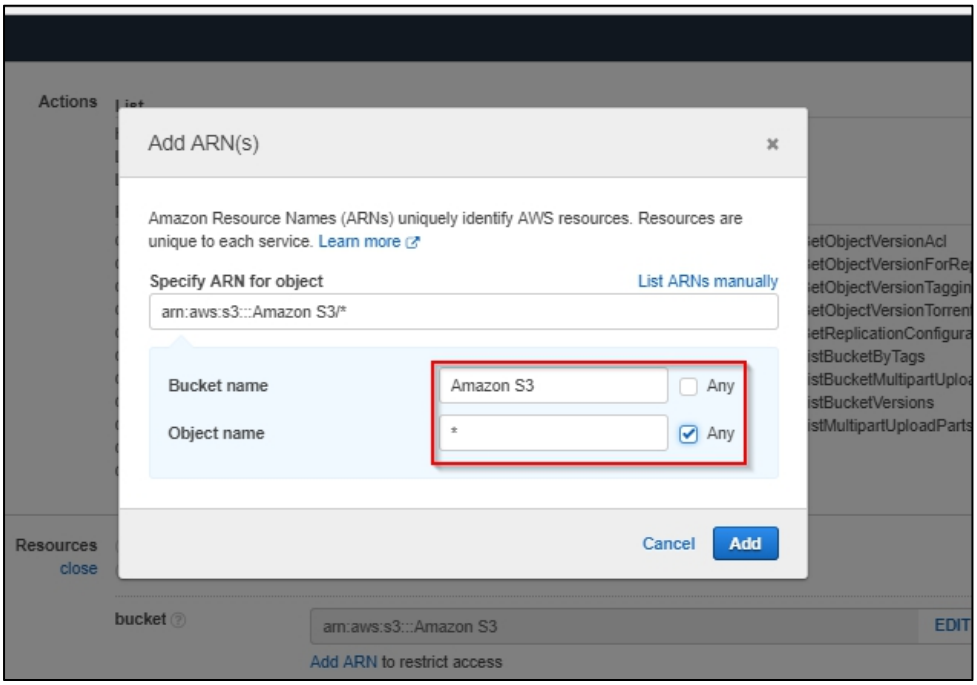


Step-6: You may find specific errors in between. To get rid of them, move to resources at the bottom; just beside the bucket, click on **Add ARN,** and specify ARN.

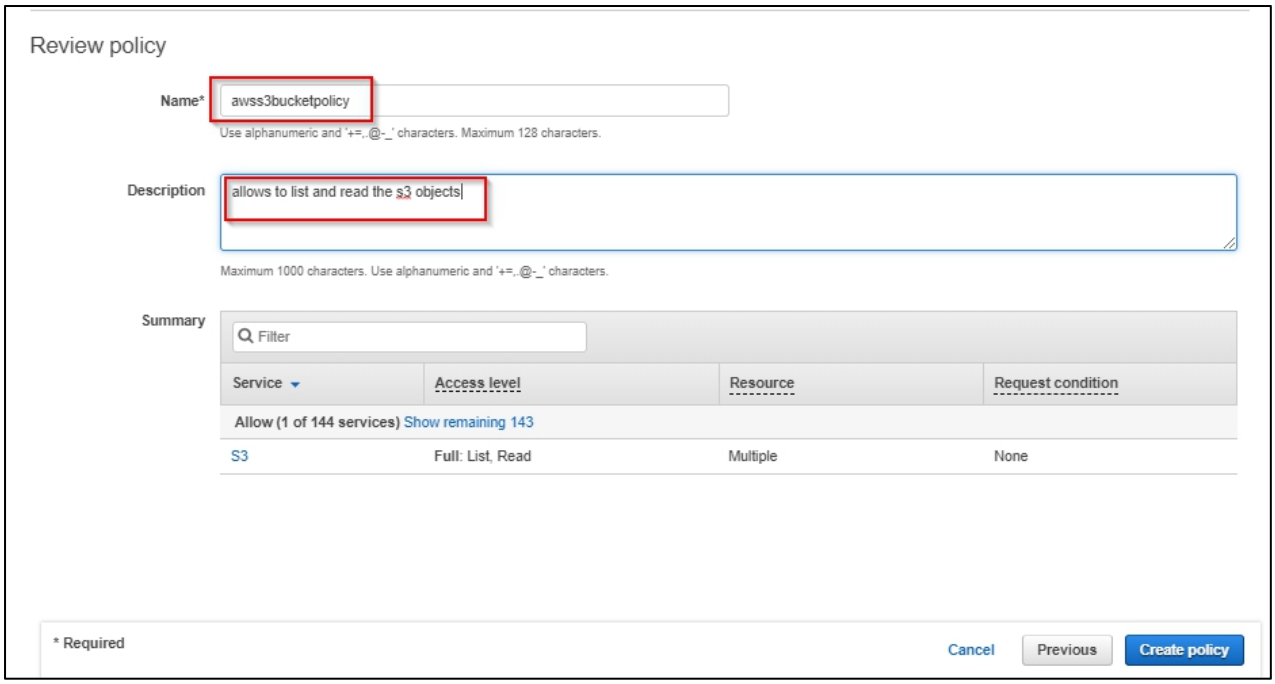




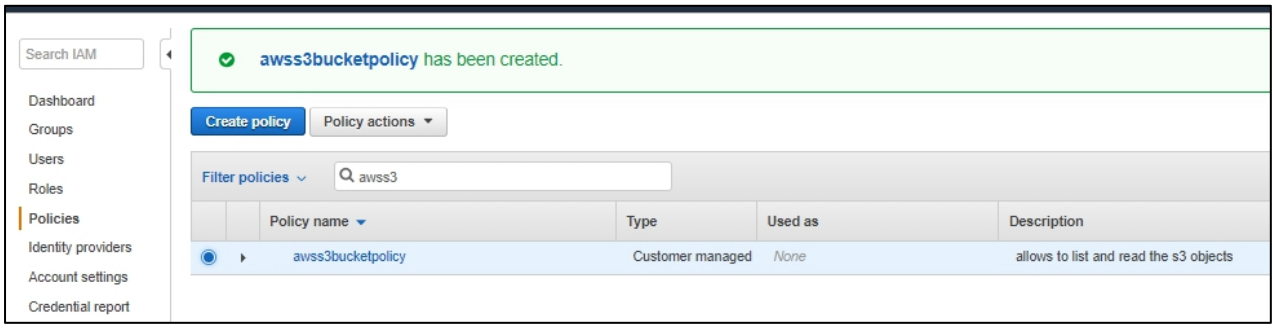
Step-7: Specify Object ARN and click on **Review policy**.



Step-8: Specify name and description and click on **Create Policy**.

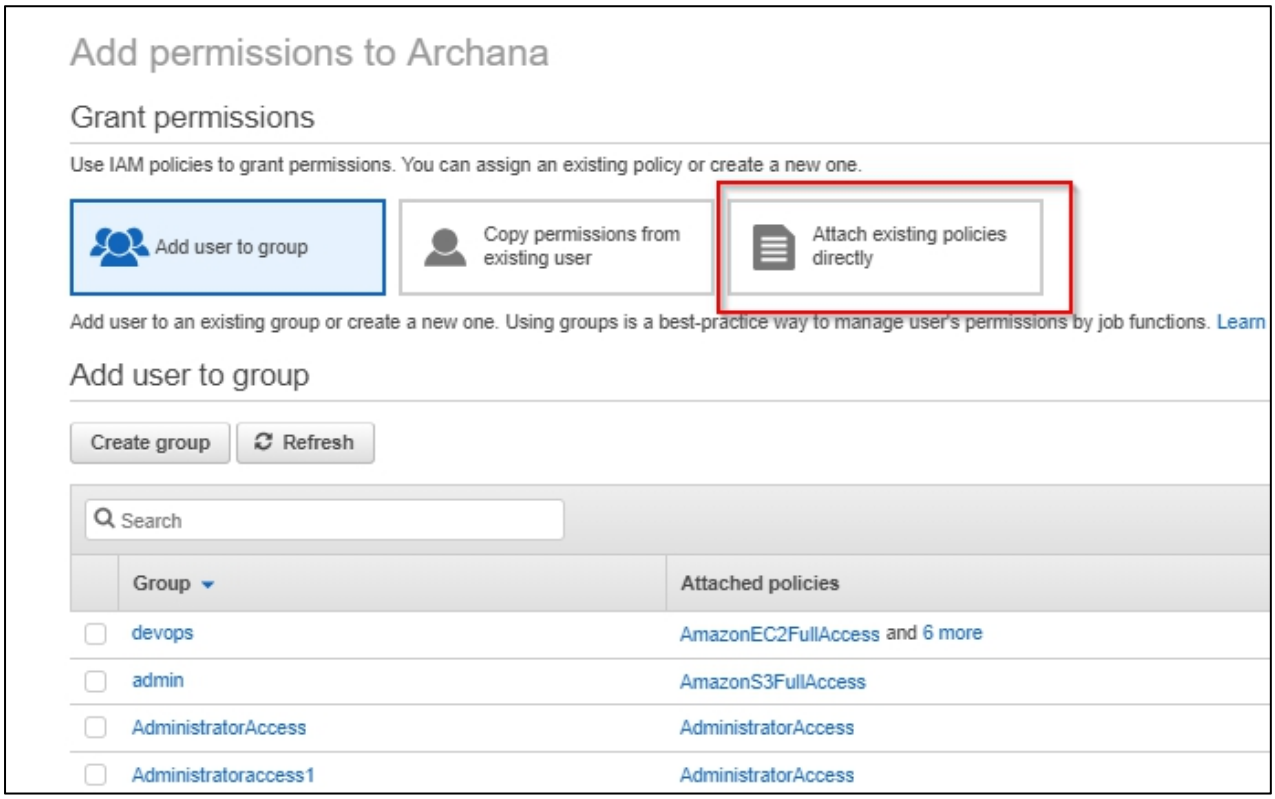


Step-9: If the policy is created successfully, it will then be added to the policy list.

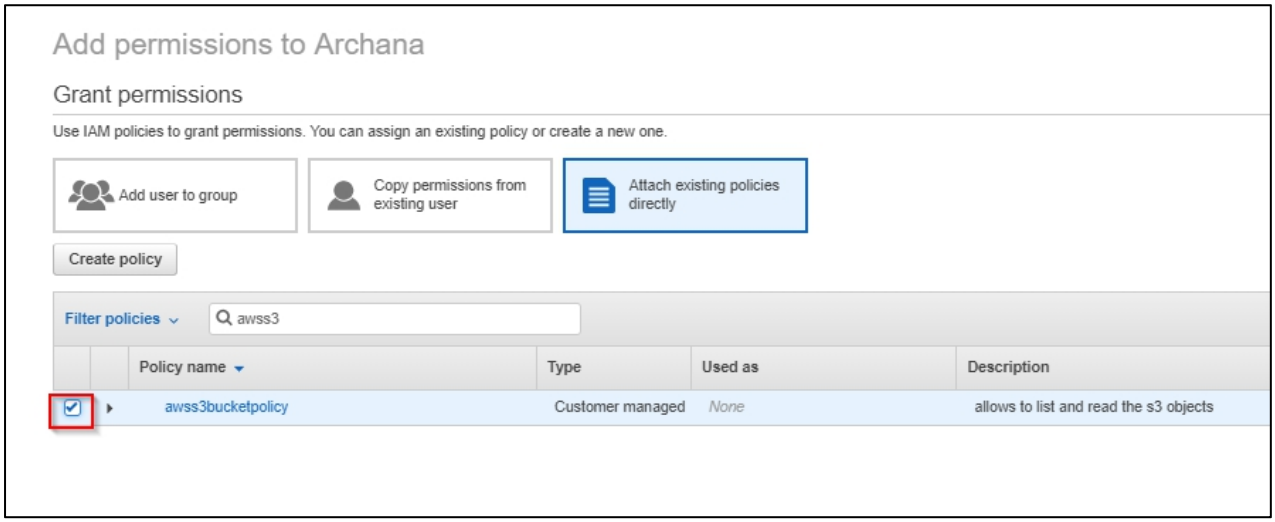


Step-10: Go to **users** and attach the **policy** to a user.

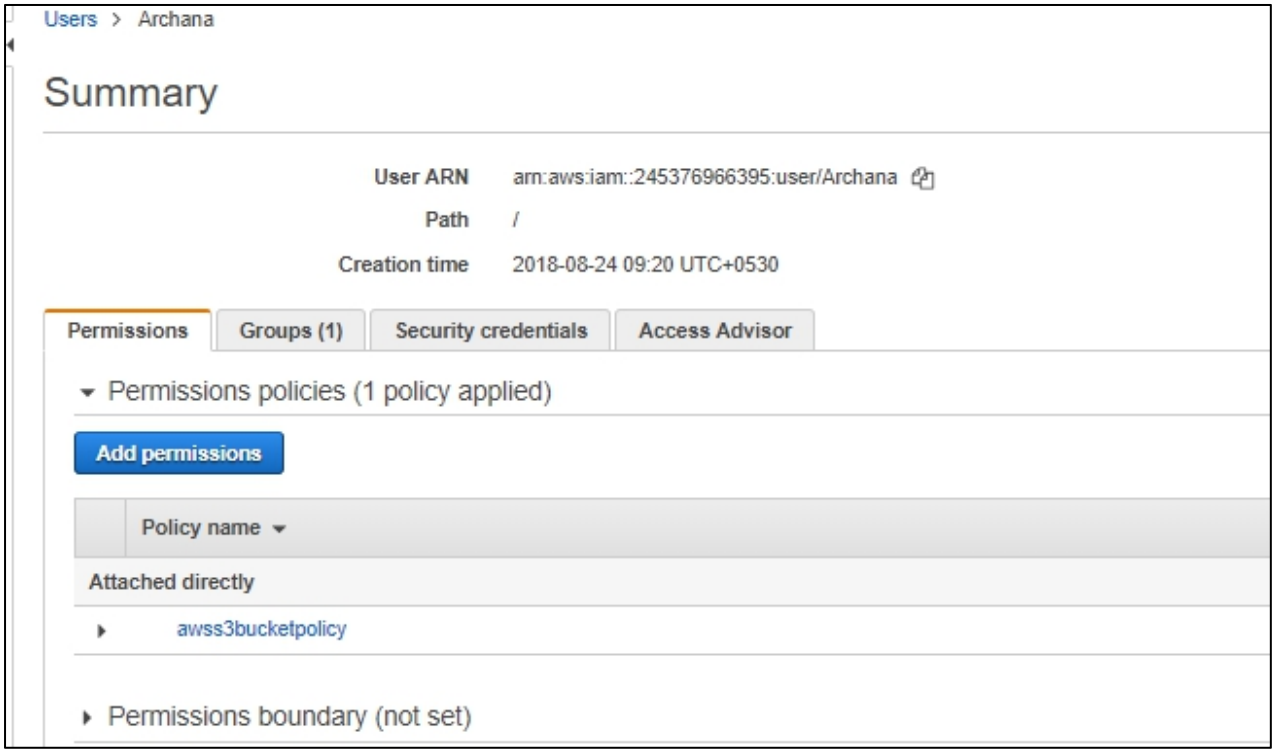
Step-11: Click on **Add Permission**, and select the **Policy attach option.**



Step-12: Attach the created policy and click on **Next Review**.



Step-13: Click on **Add Permission** to see that the policy is attached to the user. Now, the user can only read and list the **S3 bucket.**



Conclusion:

We have successfully created the **limited privileged policies** for a user.