AWS IAM Permissions Boundary Project

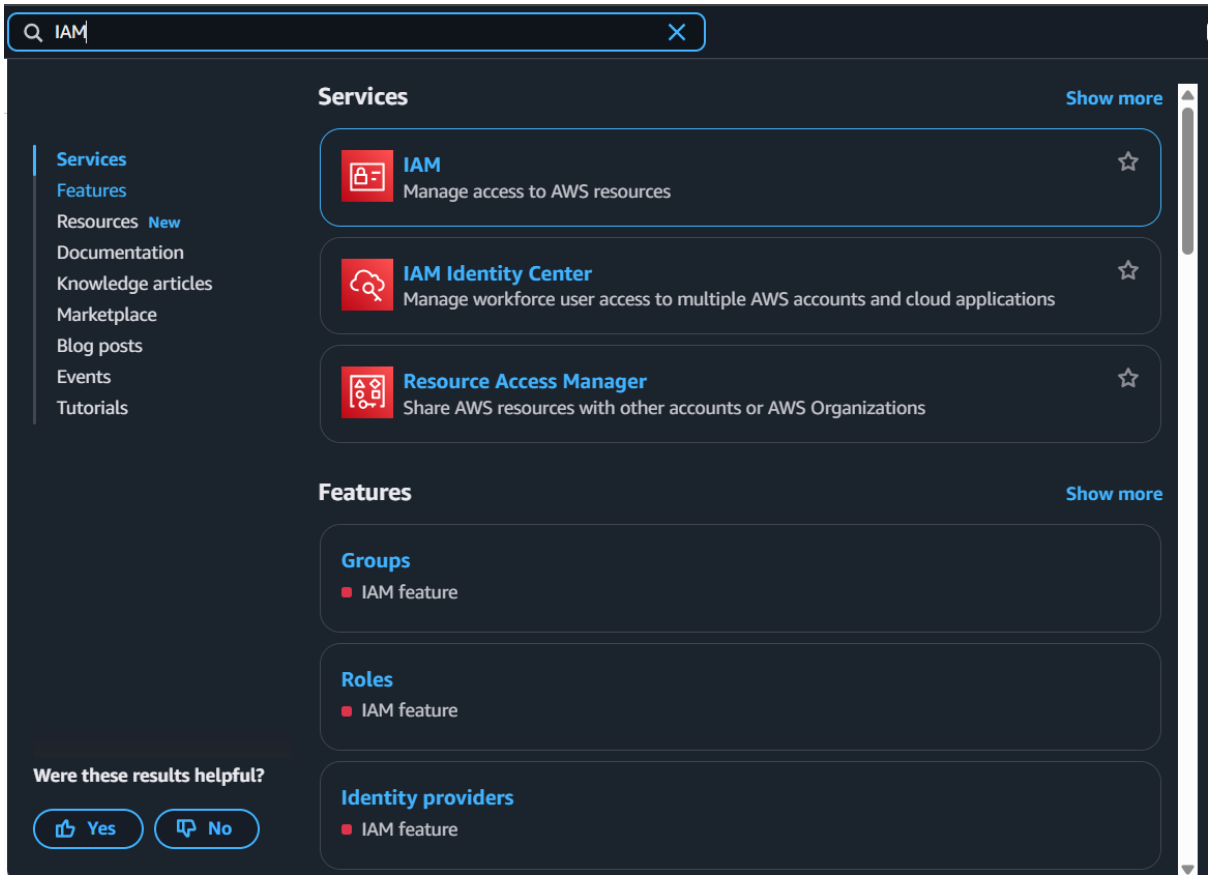
By Syeda Umaima Abeer

July 2025

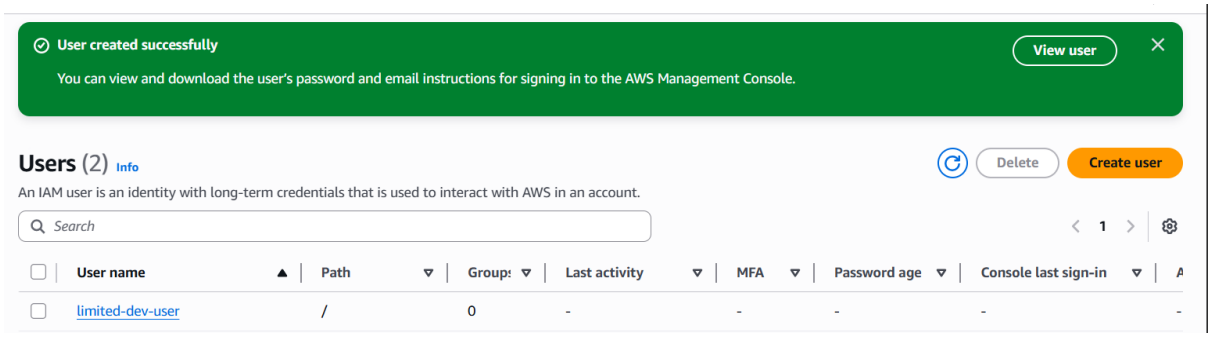
This project focuses on implementing IAM permissions boundaries in AWS to restrict the maximum permissions an IAM user can have, even if broader policies are attached.

By applying both a full-access custom policy and a tightly scoped permissions boundary, this project demonstrates how AWS enforces least privilege access using layered security controls. The purpose was to understand how permissions boundaries work and how they override standard IAM policies to limit actions such as S3 writes while still allowing reads.

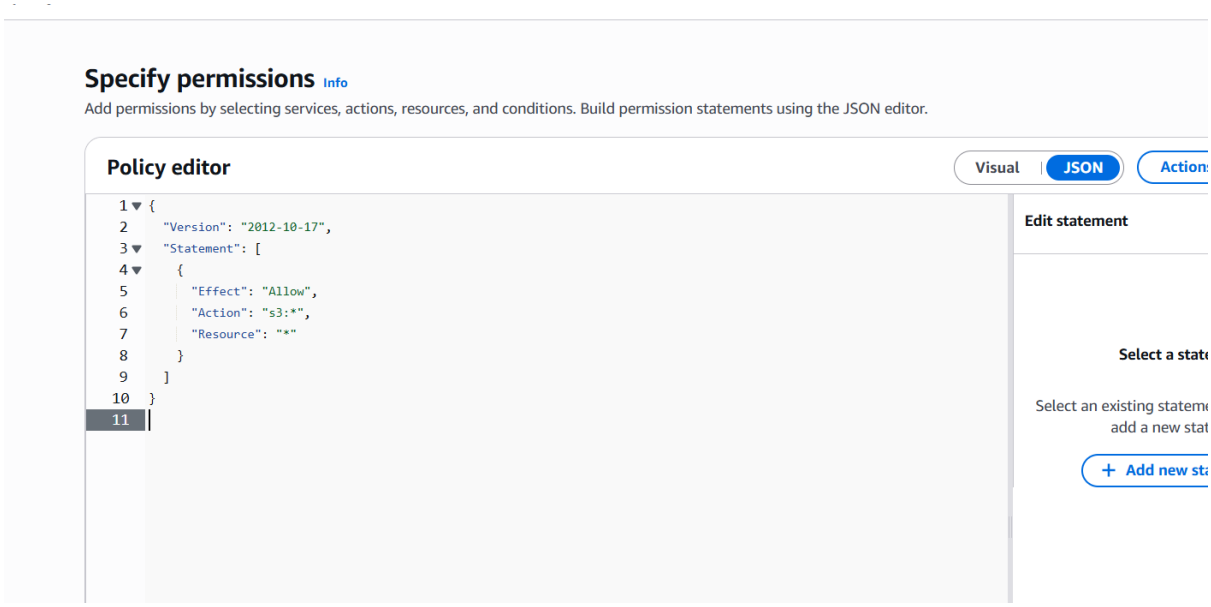
This documentation walks through each step of the setup process along with screenshots and key observations.

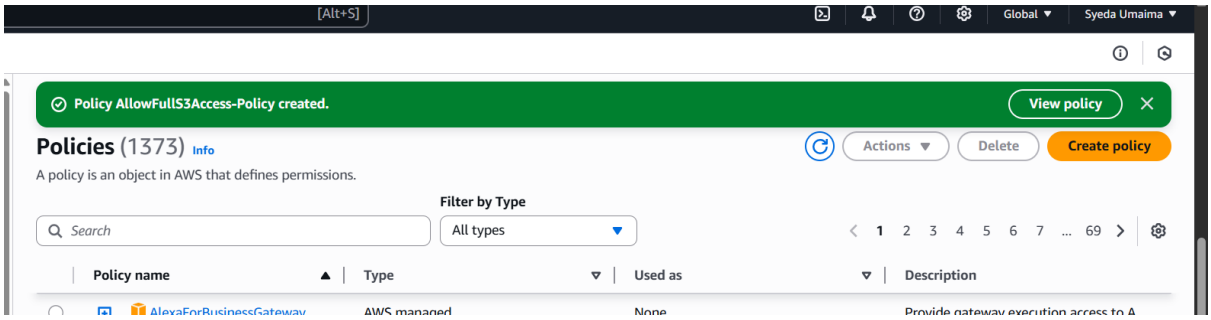


Opened the AWS IAM service from the console to start user and policy configuration.

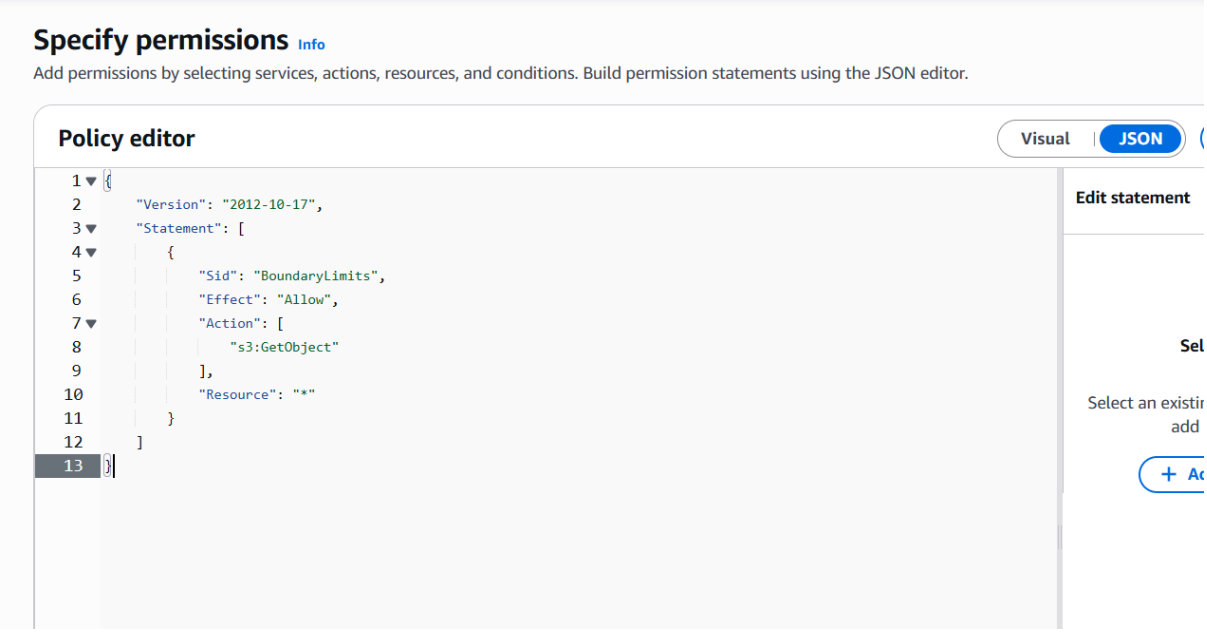


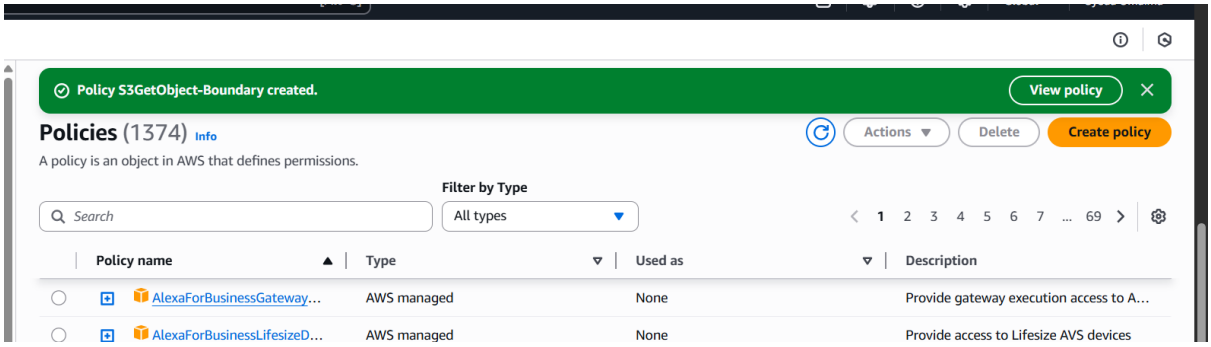
Created an IAM user with programmatic access and no direct permissions.



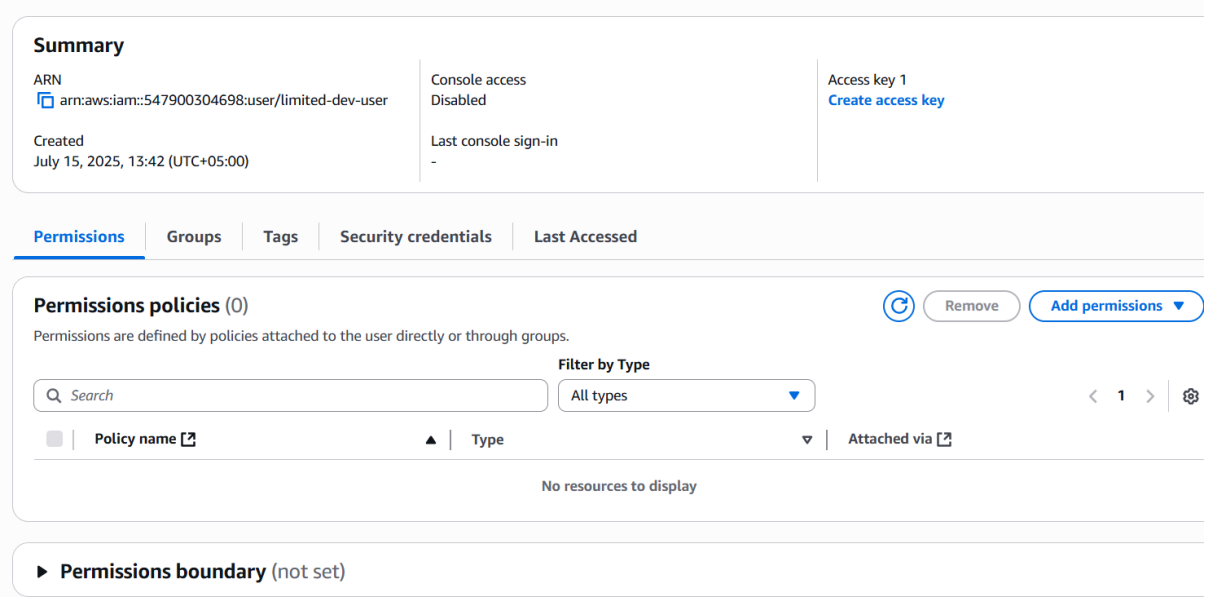


Created a policy that allows full access to all S3 actions on all resources.



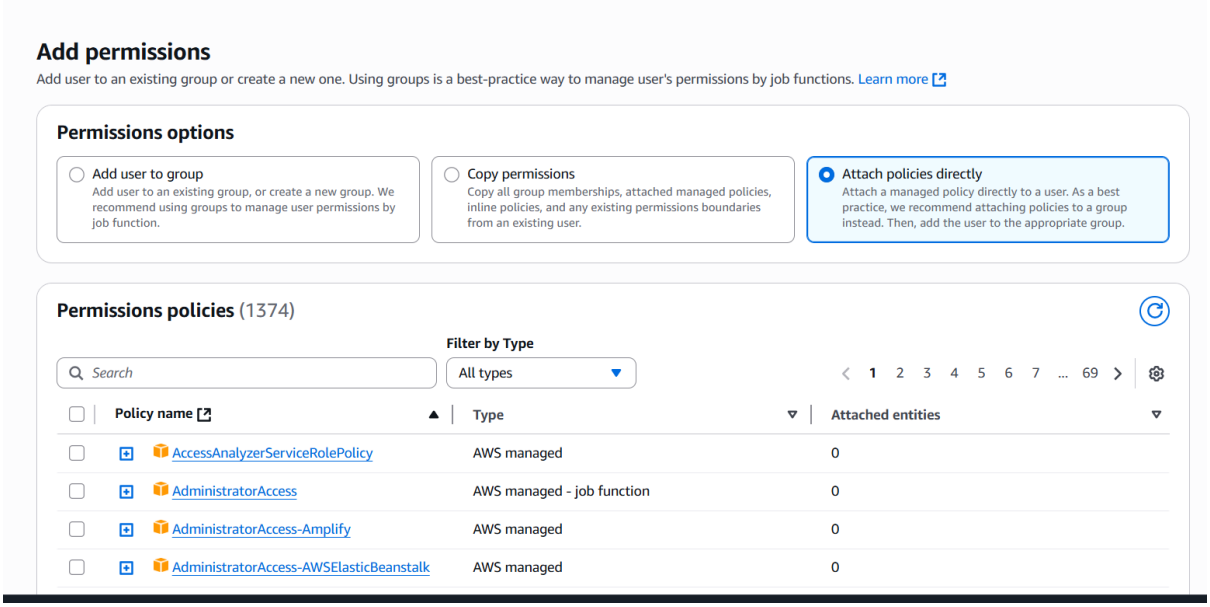


Created a permissions boundary that only allows s3:GetObject, restricting user actions even if other policies allow more.

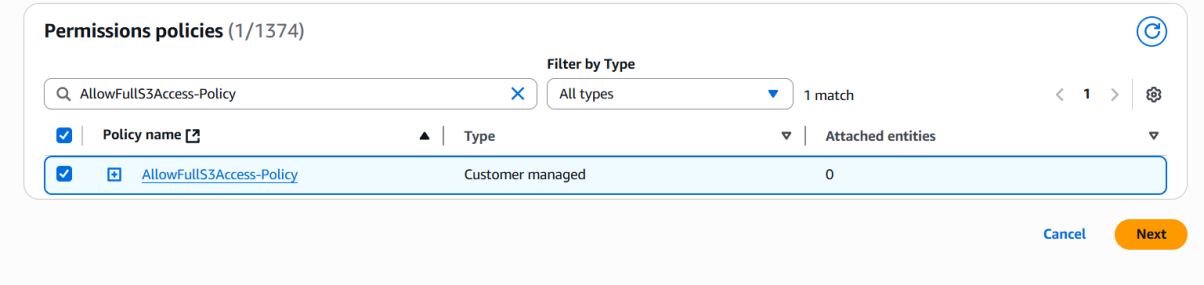


Navigated to the IAM user limited-dev-user and opened the **Permissions** tab.

IAM Console → **Users** → Click on limited-dev-user

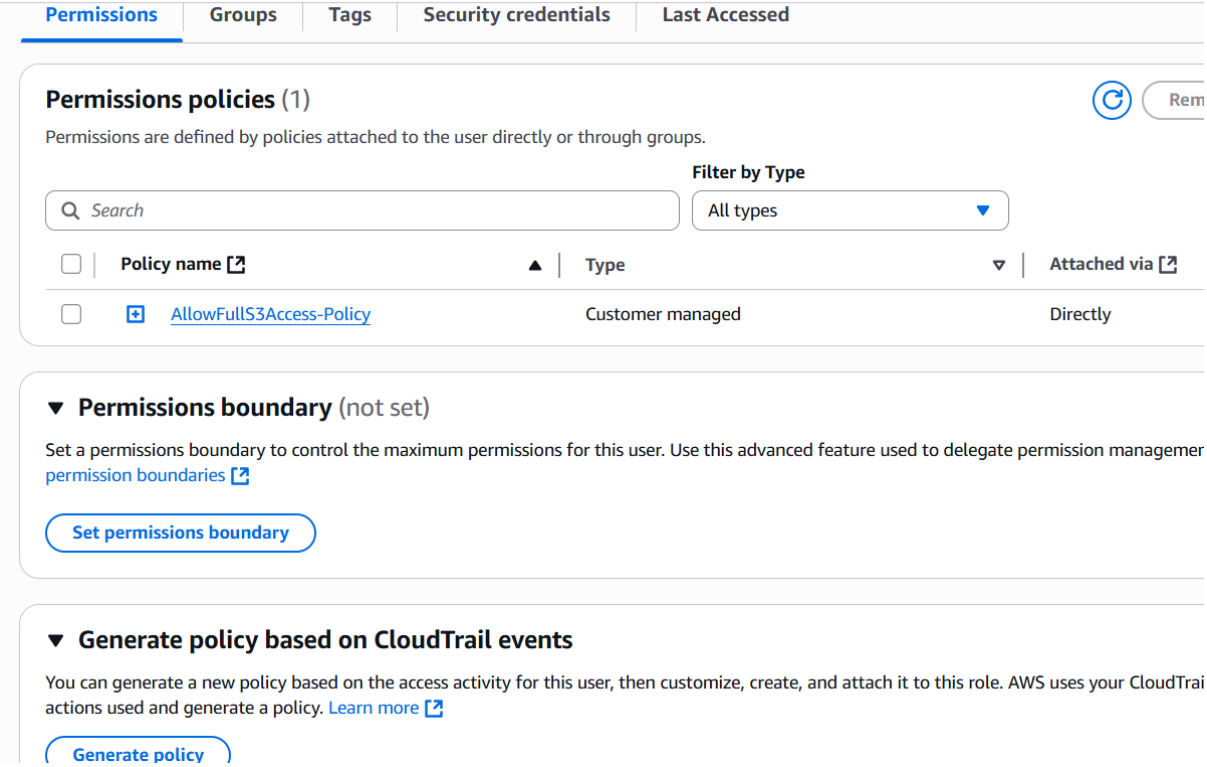


Clicked on **Add permissions** and selected **Attach policies directly**.



Searched for AllowFullS3Access-Policy and selected it.

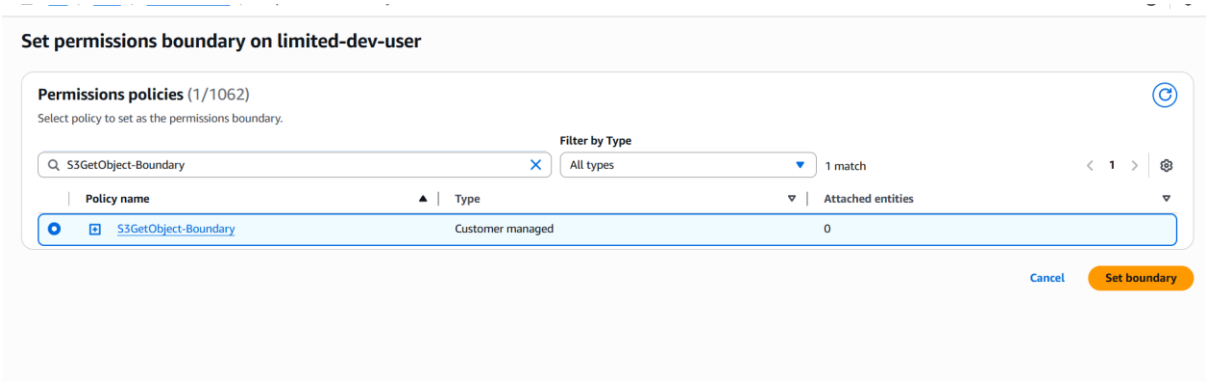
Attached custom policy that gives full S3 access to the user.



Opened the IAM user limited-dev-user in the IAM console.

Clicked on **Permissions boundary** section inside the user detail page.

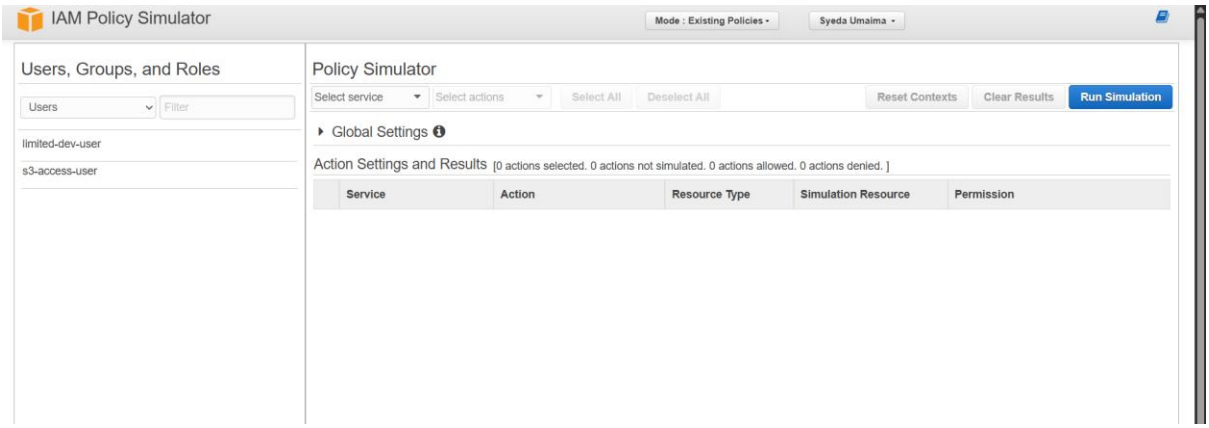
Selected **Set permissions boundary** option.



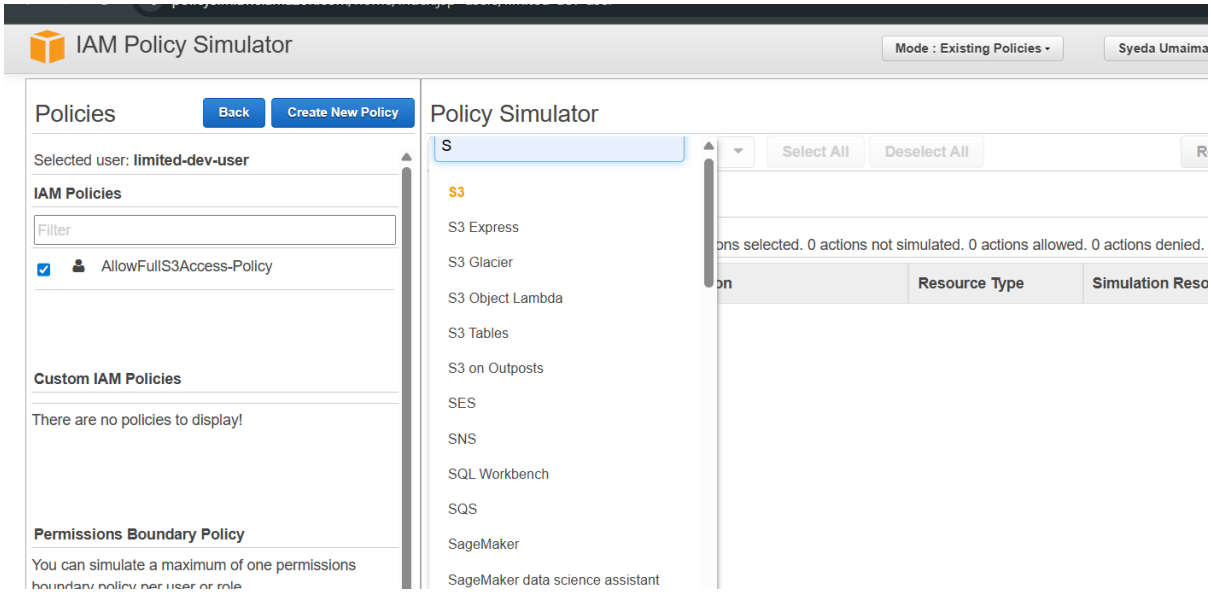
Searched for the policy named S3GetObject-Boundary.

Confirmed and saved the permissions boundary successfully.

Applied a permissions boundary to restrict the user to s3:GetObject only, despite having full S3 access policy.

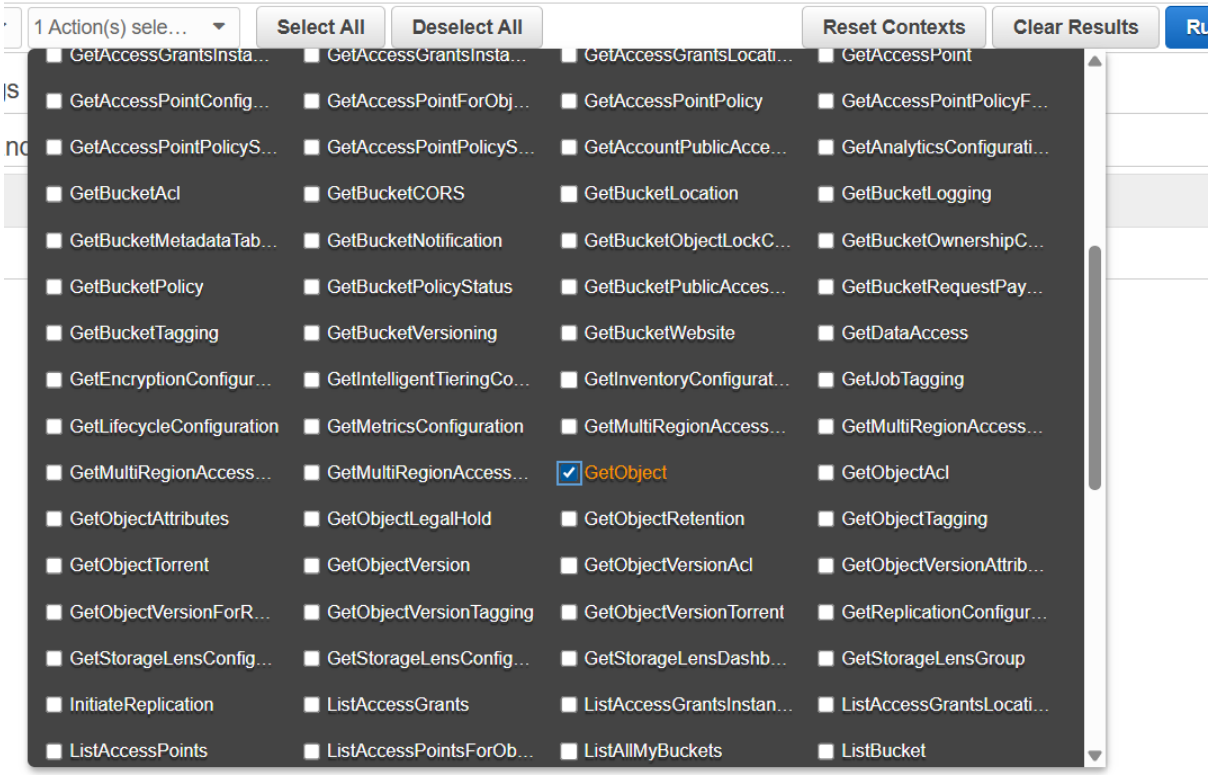


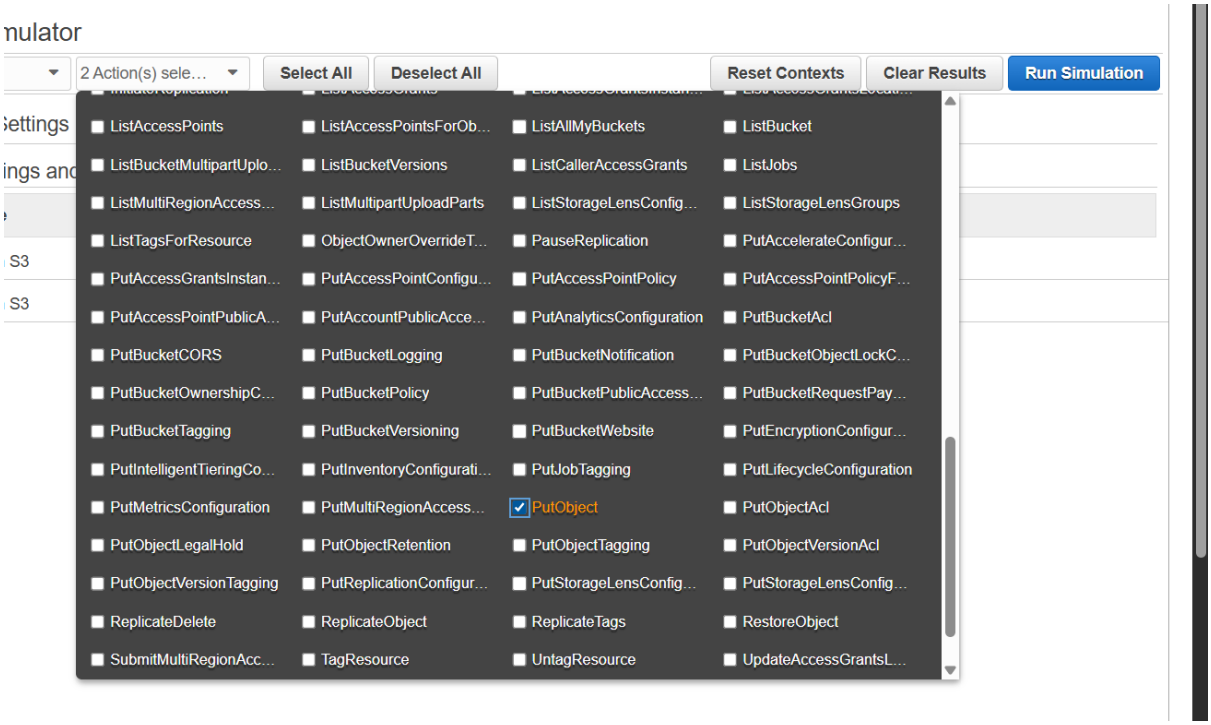
Opened the AWS IAM Policy Simulator to test the user's access permissions.



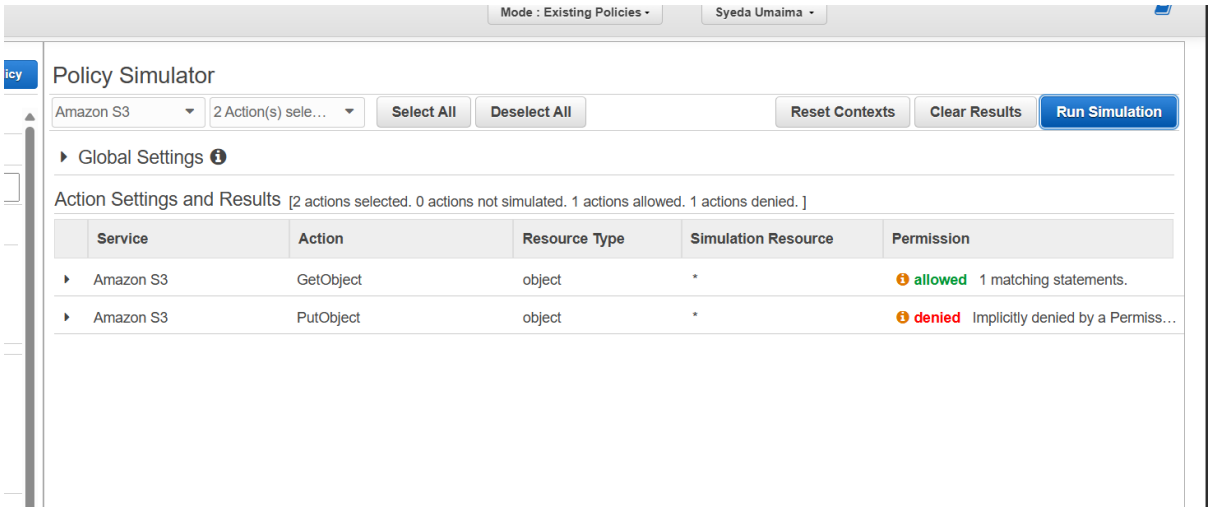
Selected limited-dev-user from the list of IAM users.

Chose Amazon S3 as the service to simulate permissions on.





Selected actions: s3:GetObject (should pass) and s3:PutObject (should fail).



Ran the simulation to verify the results.

Result: s3:GetObject was allowed, while s3:PutObject was correctly denied due to the permissions boundary.

Simulation confirmed that s3:GetObject is allowed but other actions like s3:PutObject are denied due to the applied permissions boundary

Summary:

This project demonstrates how to implement granular access control using IAM permissions boundaries in AWS.
An IAM user with full S3 access policy was created, and a permissions boundary was applied to restrict actual access to only s3:GetObject.
Testing through the IAM Policy Simulator confirmed that the boundary overrode the broader policy, ensuring limited, secure access.
This hands-on exercise improved understanding of IAM policy evaluation, privilege restriction, and cloud access control mechanisms.