1. *Now, add a policy to your IAM Administrator user with a conflicting permission. Use the policy generator to create a new policy. Create the policy with effect: Deny;AWS Service:Amazon S3;Actions:\*; and ARN:\*.*

Open AWS IAM console and click on ‘Policies’.

Click on ‘Create Policy’ button.

Select "S3" as the service for which you want to create a policy. Under "Actions", select "All S3 actions".

Under "Amazon Resource Name (ARN)", enter "\*".

This will apply the policy to all S3 resources.

Change the "Effect" as "Deny". Click on the "Add Statement" button to add the policy to the policy editor. Review the policy statement to ensure it matches your requirements. Click on the "Generate Policy" button to generate the JSON policy.

Choose Users from the access management panel in AWS IAM. Open the ‘User summary’ of the user ‘Administrator’. Add the created policy from the ‘Permissions’ tab.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*