**PROJECT - IMPLEMENTING CLOUD IDENTITY AND ACCESS MANAGEMENT (IAM) POLICIES**

*DESCRIPTION* -

1. IAM POLICIES - IAM policies define who (identities) can do what (permissions) on which resources. By setting up policies correctly, you ensure the principle of least privilege and maintain a secure cloud environment.

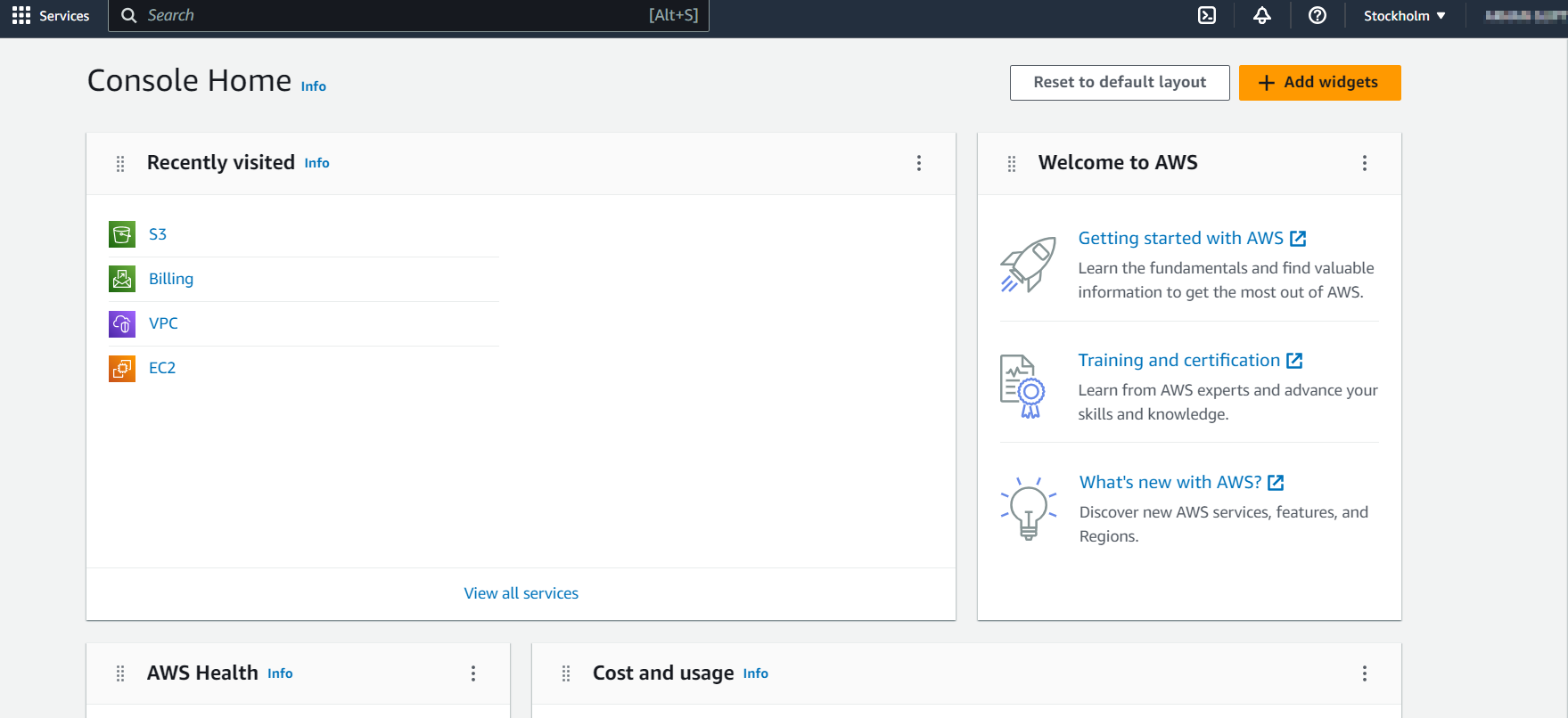
*SCENARIO* -A company with different employees needing different levels of access to resources.

*IAM TERMINOLOGY* -

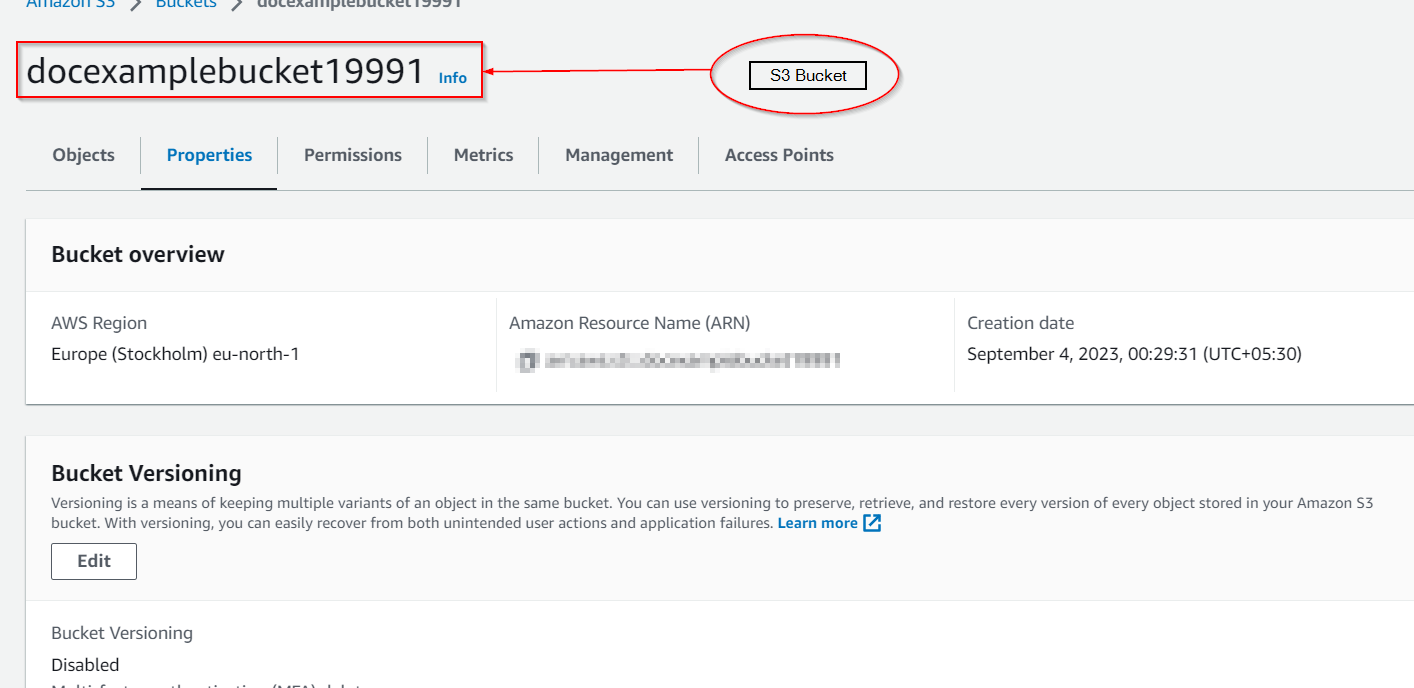
1. IAM Users - These stand for people or things that require usage of AWS resources. They have particular authentication credentials.
2. IAM Roles - Roles are like users, but they are typically assumed by AWS services or resources.
3. IAM Policies - IAM Policies are JSON Documents that define permissions.
4. IAM Groups - Groups are collections of IAM users. Policies can be attached to groups, making it easier to manage permissions for multiple users with similar roles.

*STEPS -*

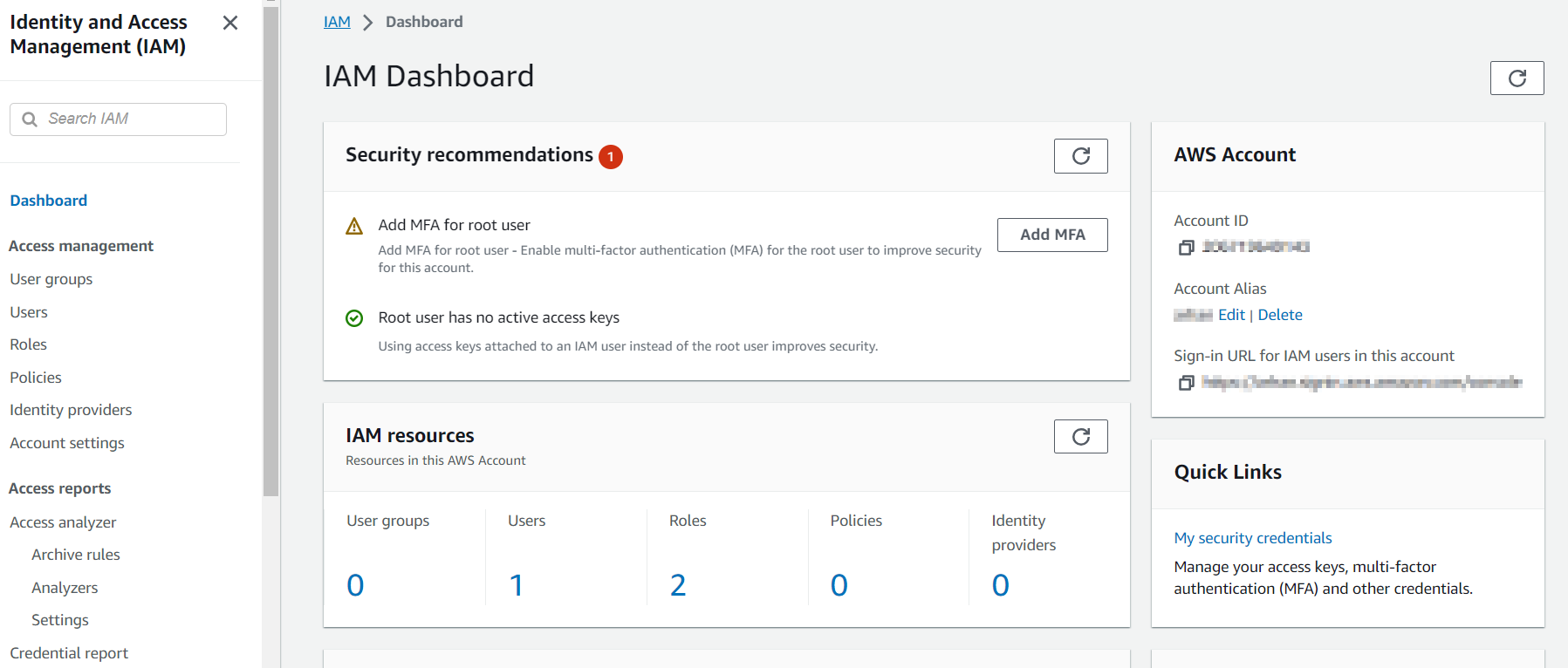
1. Opening the AWS Management Console



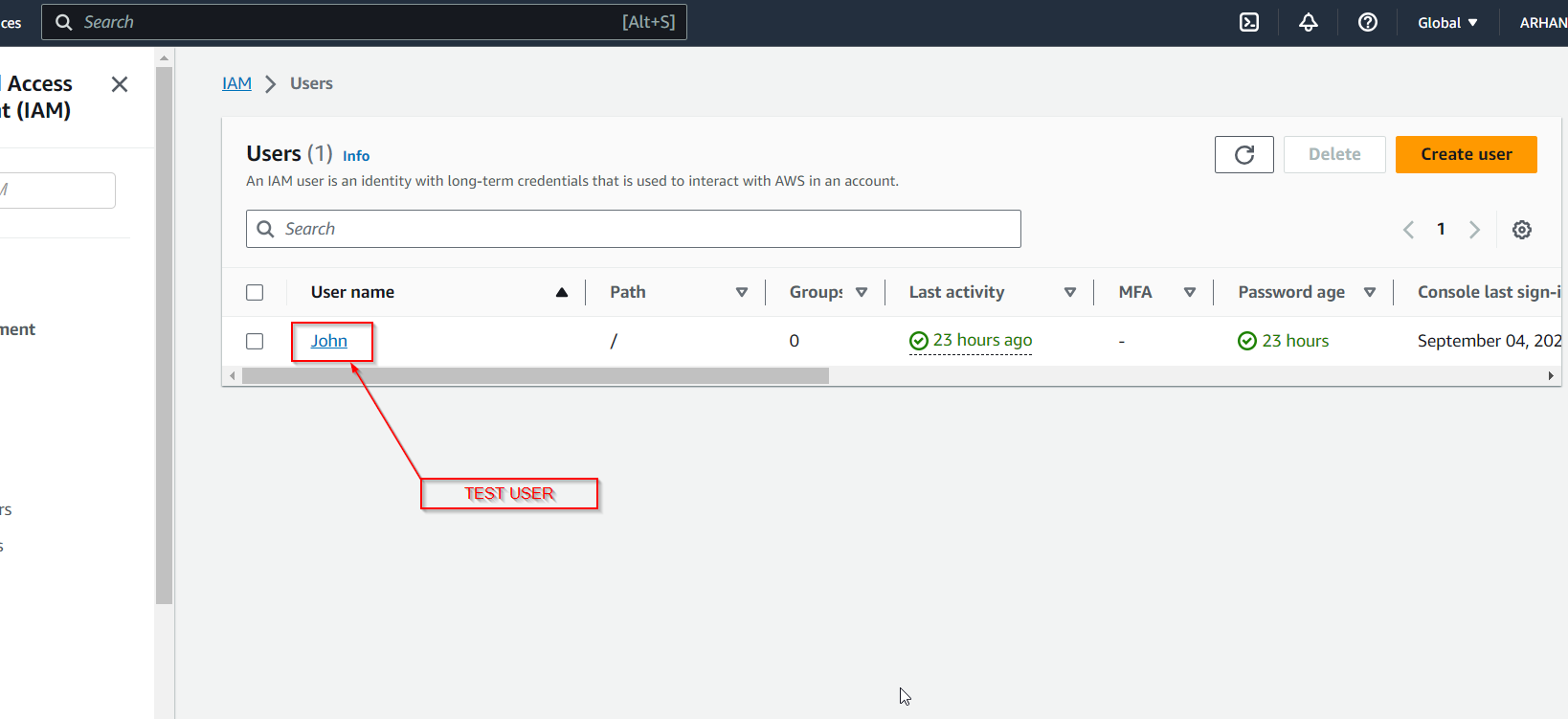
1. Setting up the S3 Buckets as the Root User



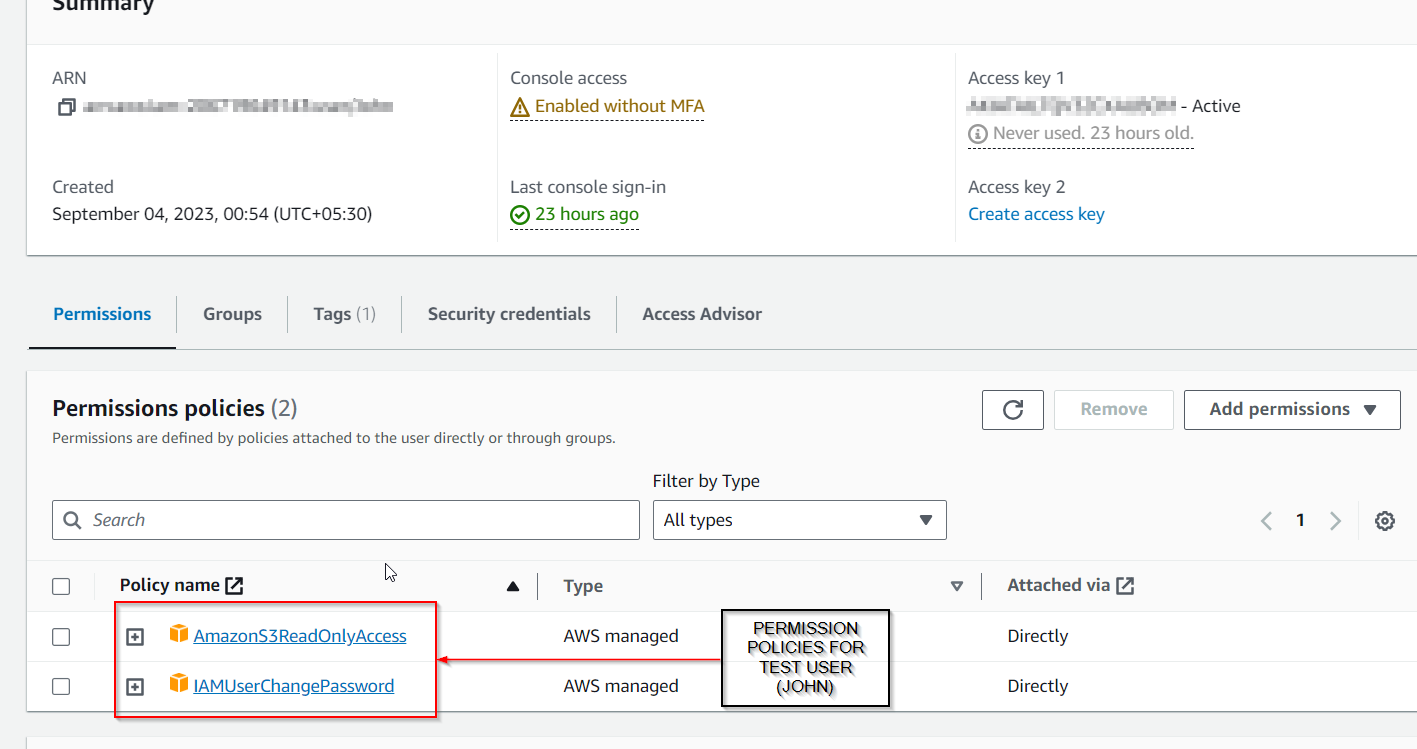
1. Accessing the IAM Dashboard



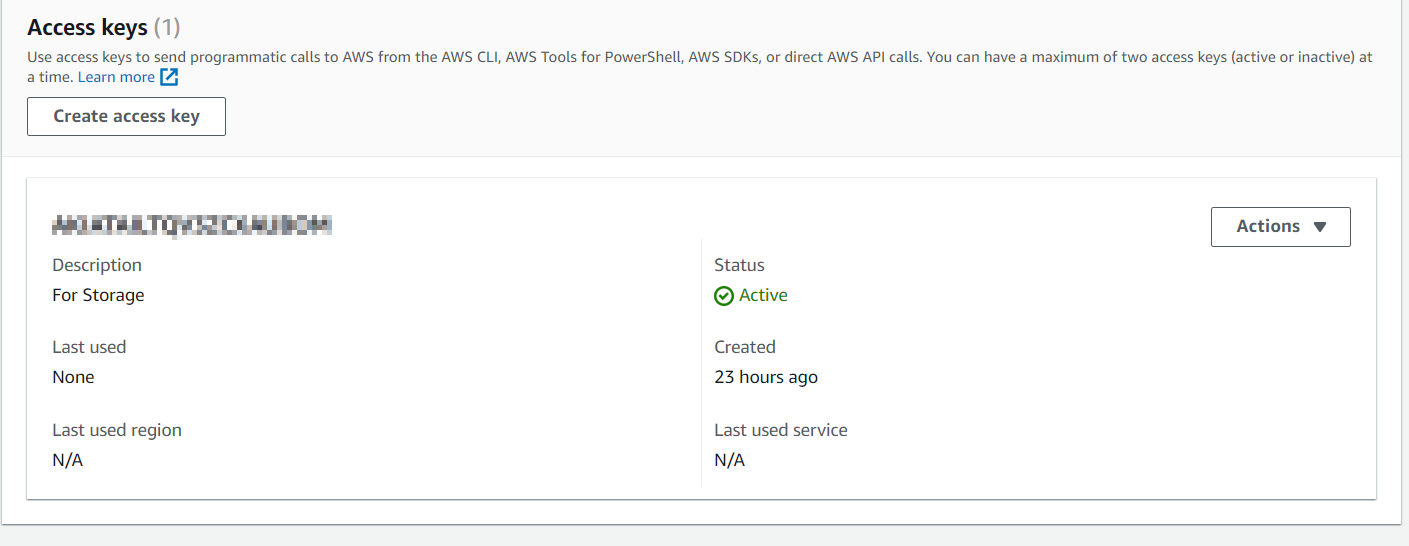
1. Setting up the Test User



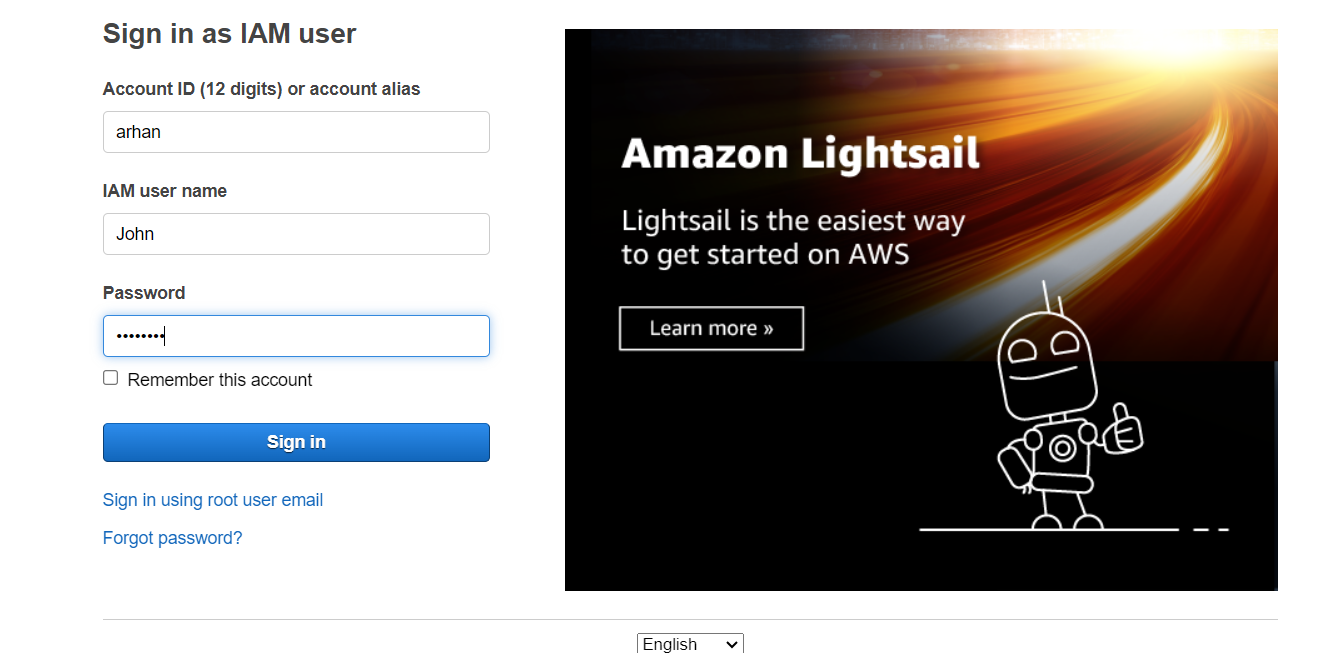
1. Setting up the Permission Policies for the Test User



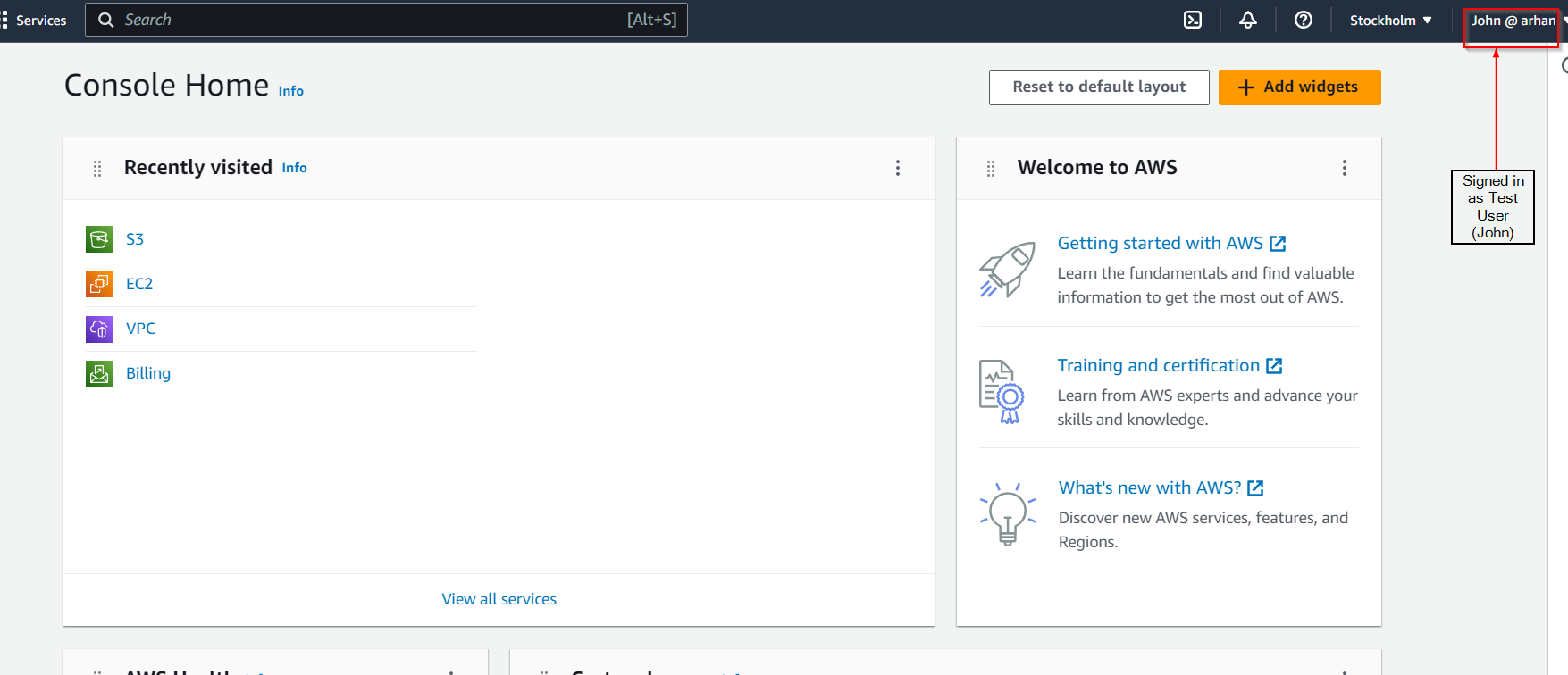
1. Creating the Access Keys



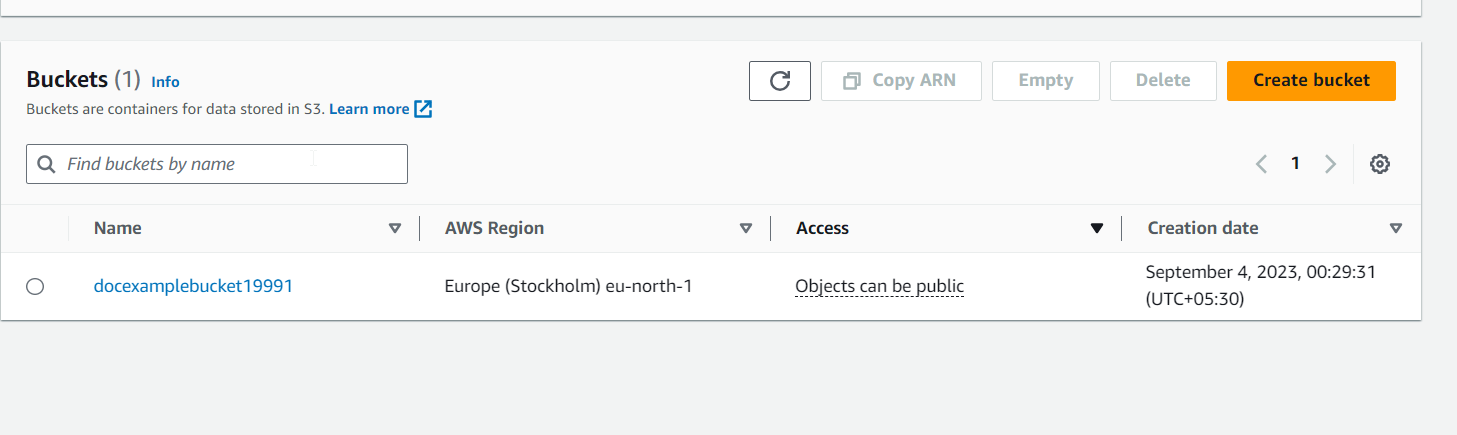
1. Signing in as IAM Test User (John)



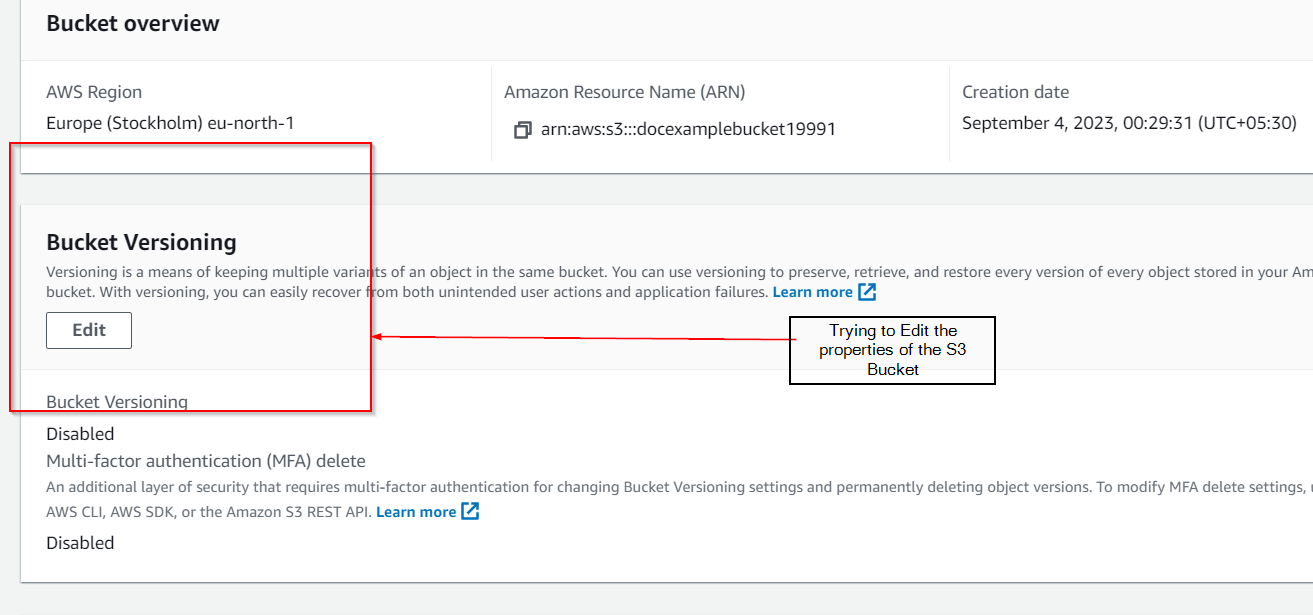
1. Signed in as Test User (John)



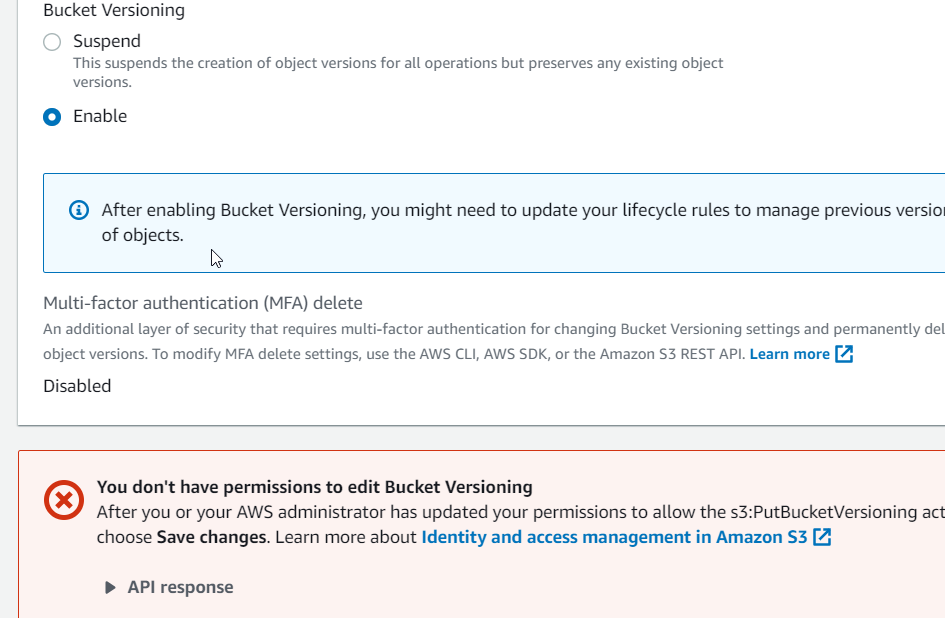
1. Accessing the Bucket that was created before in Step 2



1. Trying to edit the Properties of the S3 Bucket



1. IAM Test User Does Not have the Permission for that.



*FINAL RESULT -* This project exists to ensure that only authorized users and services have access to cloud resources, helping to prevent unauthorized access and data breaches.