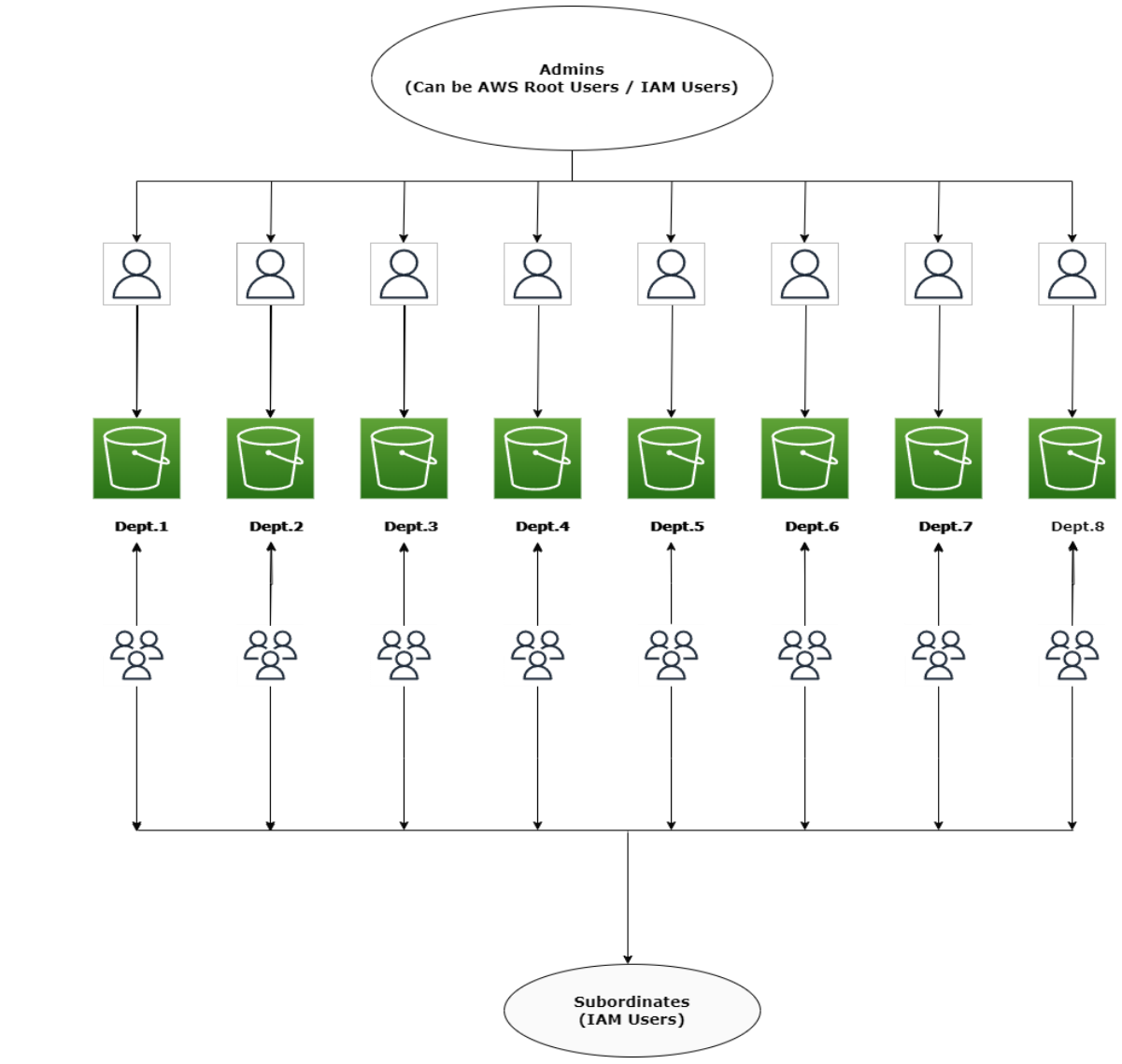
Introduction

Transfer files from local machine or any on-premise machine to AWS S3 that has a hierarchical model for adding objects to the S3 buckets with relevant permissions to the respective users.

Process Flow



As per the above diagram, there are multiple departments in an organization. In this case, we have considered the number of departments to be 8. Each department has an admin & multiple users who can add files to an AWS S3 bucket with permissions as below:

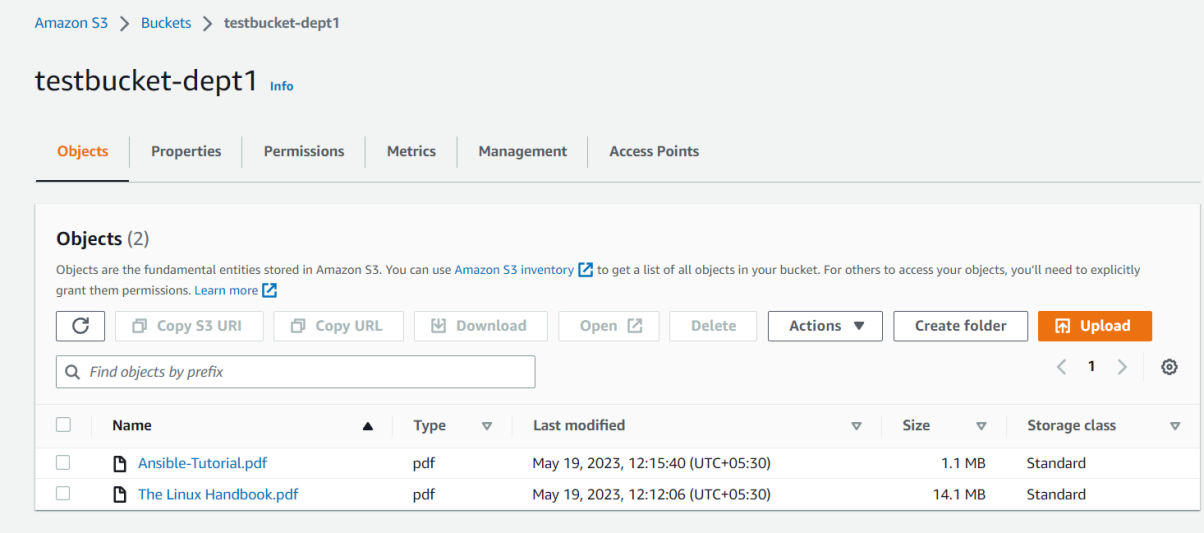
1.Admin – List, Read, Write and Delete S3 objects

2.Users – List, Read and Write S3 objects

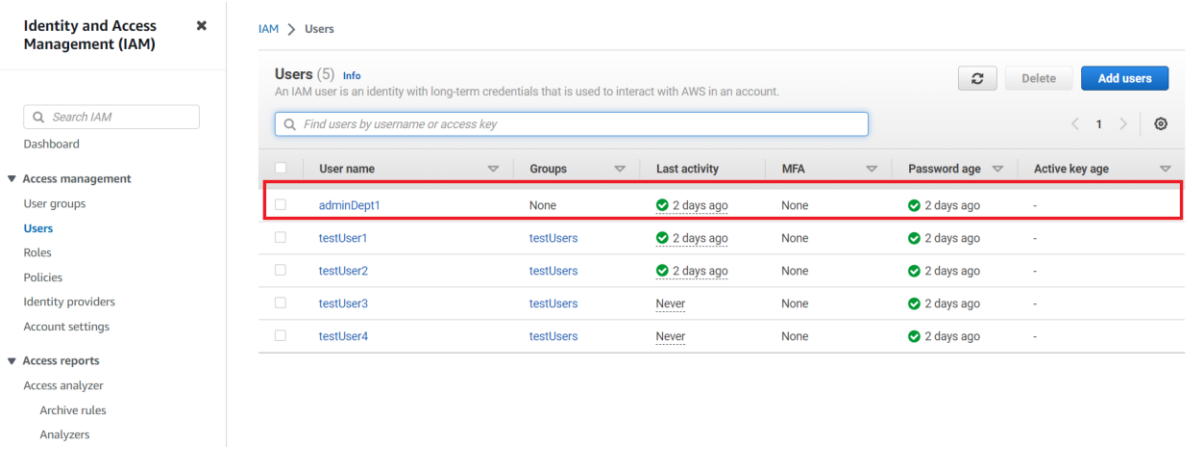
**There can be one admin to one department or a single admin can oversee multiple departments

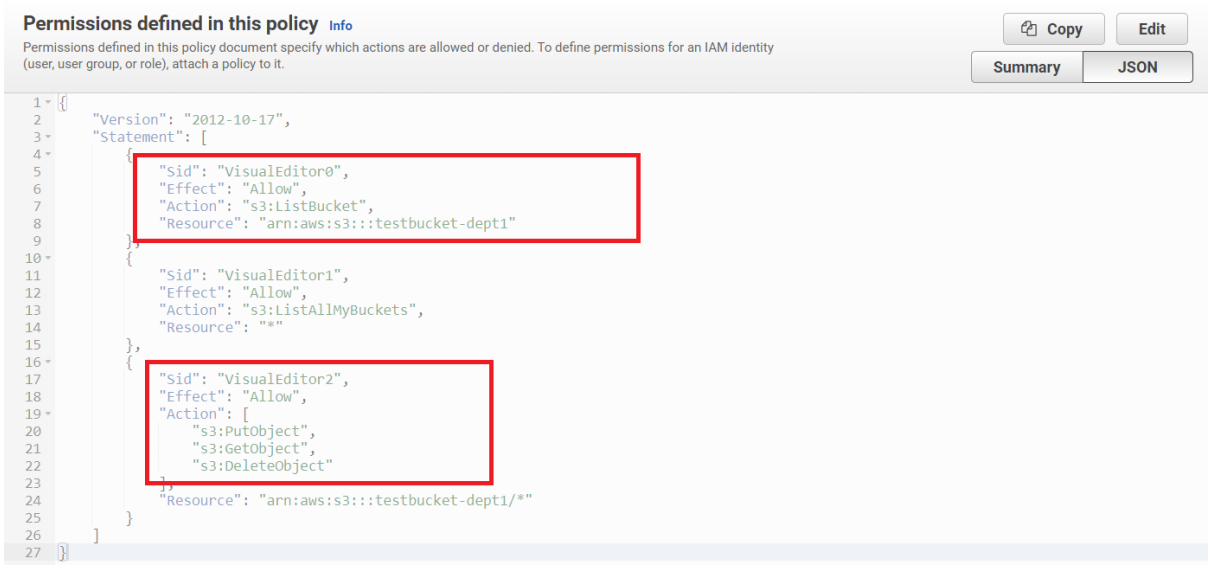
Process for achieving the above use case:

1.Create an S3 bucket under the root user

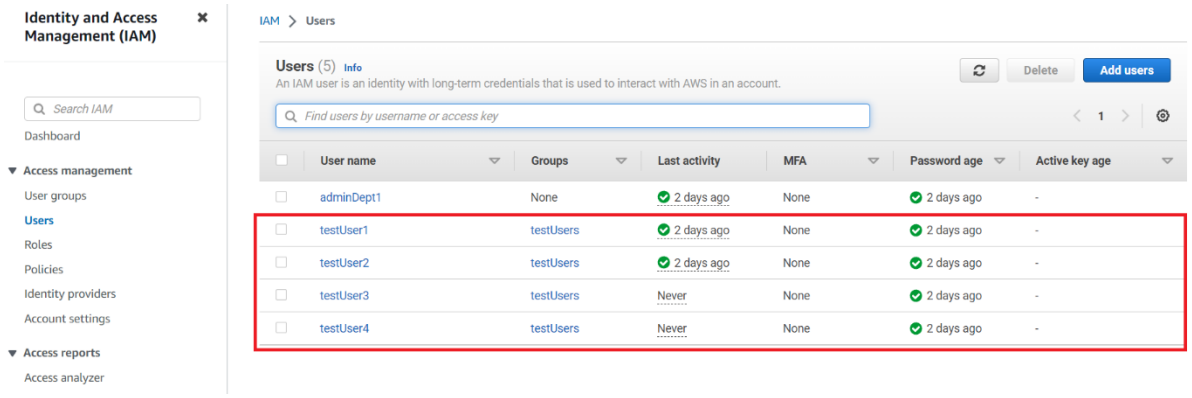


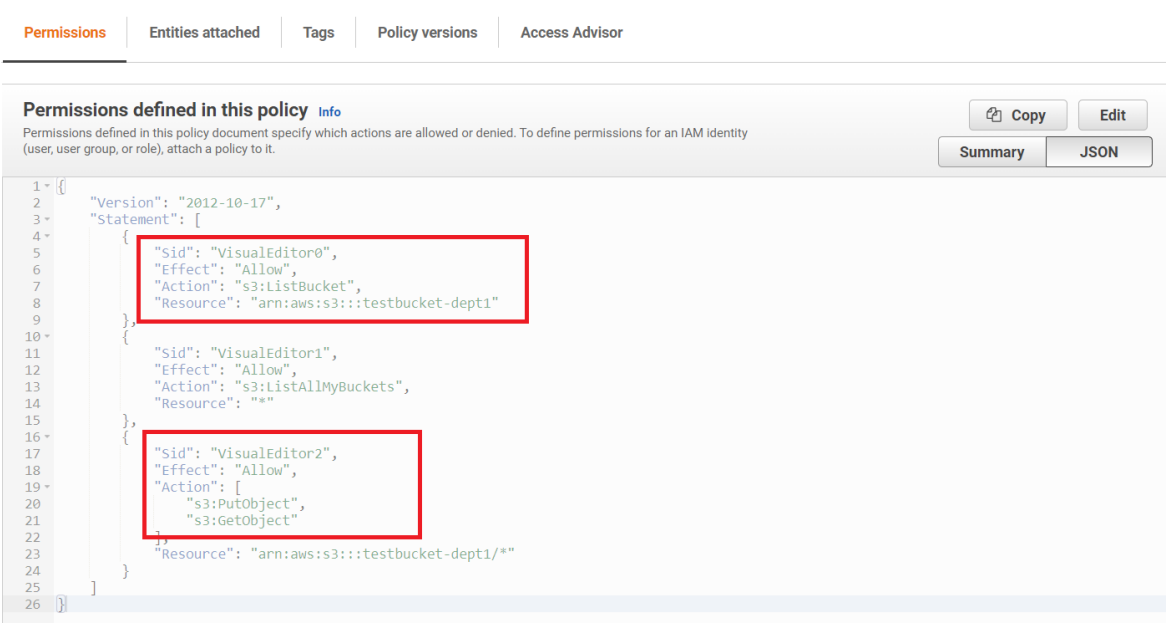
2.Create an IAM user for admin and modify the JSON document so as to provide access to a specific S3 bucket and the required permissions.



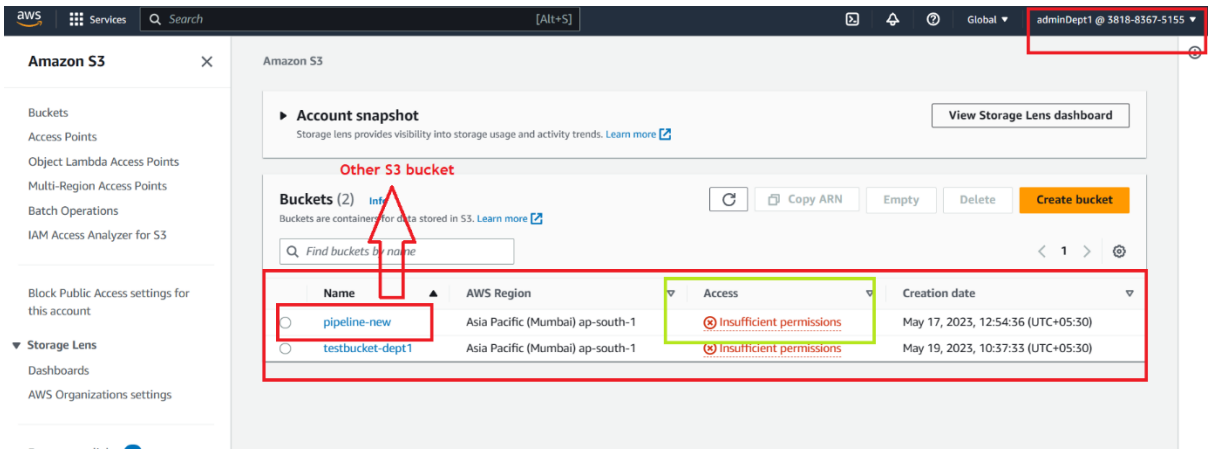


3.Create multiple IAM users for the other users or subordinates and add them to a Group and attach the policy with relevant permissions to the Group.

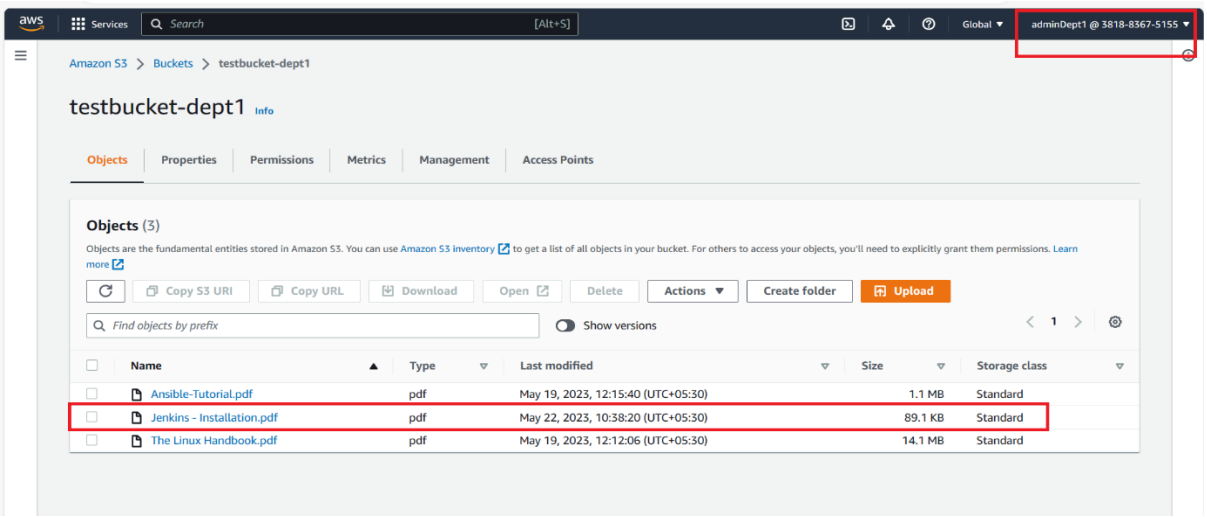


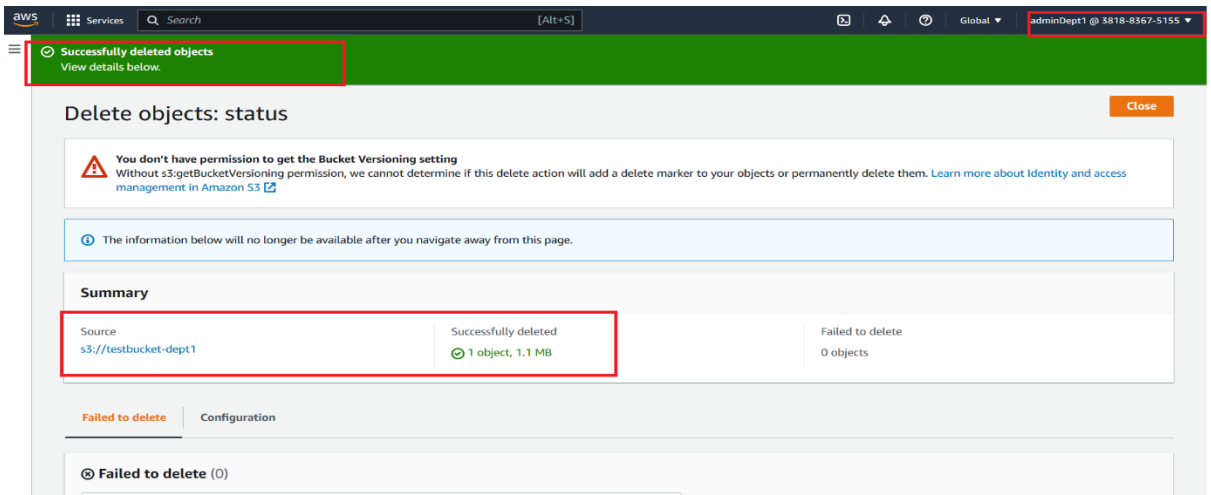


4.The admin user can list the objects, add objects, read and delete the objects in the specified S3 bucket. Even though the admin as well as the other users can view other S3 buckets, they cannot view the objects within the other buckets.

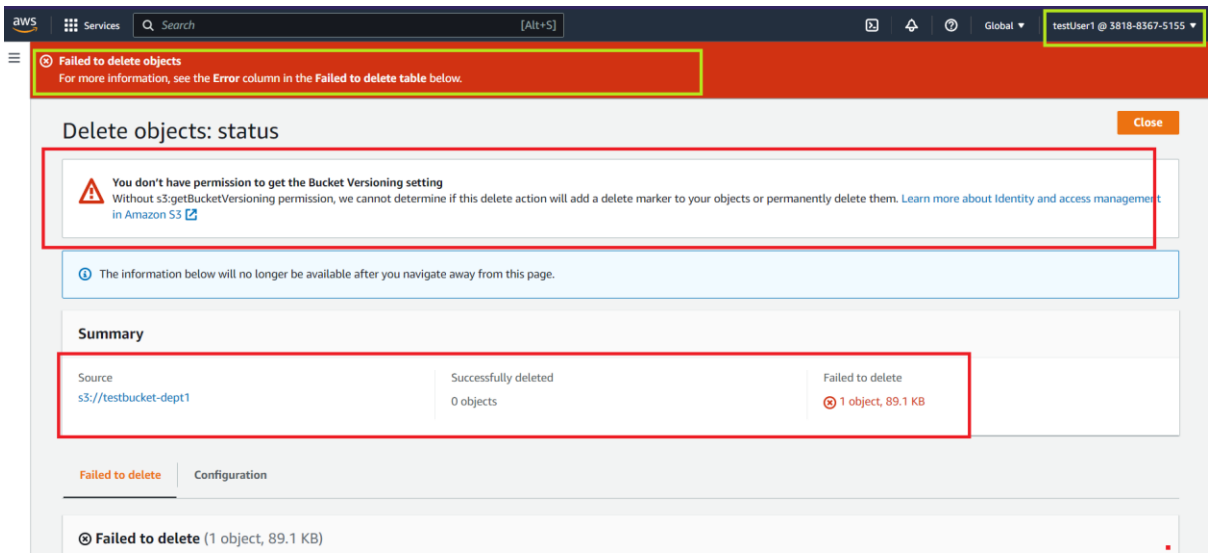


5.Perform read, write or delete operations on the created S3 bucket from the admin login. All the operations can be performed as per the assigned policy.





6.Perform read and write operations from the other user/s login. The users cannot perform delete operation and an error message will be thrown by AWS citing reason as insufficient permissions to delete the object.



Observations

We have tested all possible operations from the admin user login as well other IAM users with relevant permissions provided in the IAM policies attached to the respective users and we were able to achieve all the use cases.

Conclusion

AWS S3 offers a flexible way of granting access to the buckets for specific users. The access can be at the bucket level or at the object level depending on the requirements. This can be achieved via the visual editor on the AWS console or the access can be restricted at a granular level by editing the JSON document while creating the policy for the IAM user/s. Furthermore, it is a best practice to always create the S3 buckets by the root user and provide relevant permissions by modifying the policies and attach them to the IAM users.