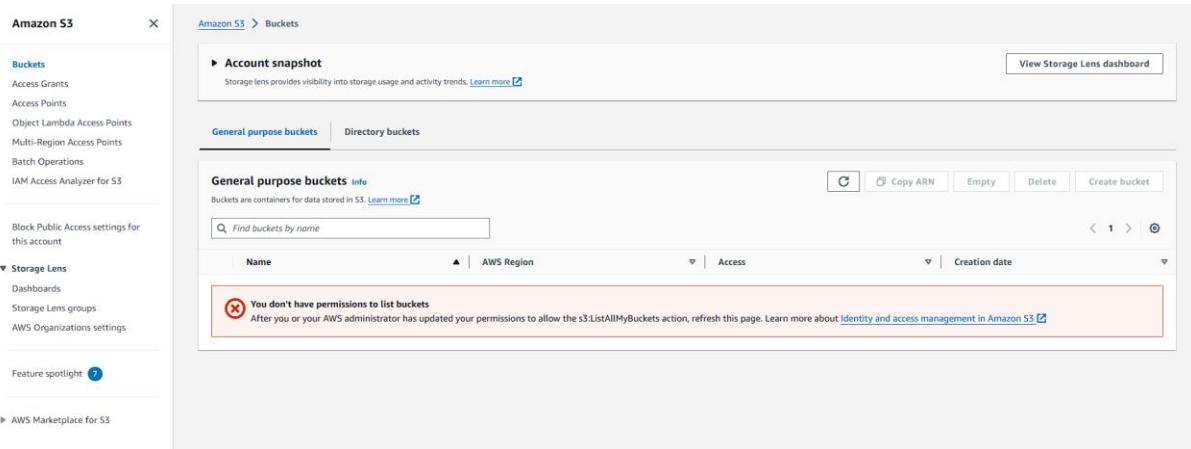


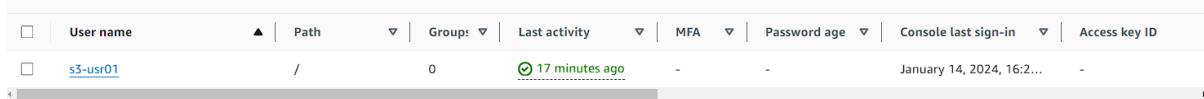
GIVING ACCESS TO IAM USER

1. In this you are going to learn how give access to your IAM user.
2. Now you will search S3 and navigate there in your IAM user account.
3. You will see that you don't have any permission or access to use S3.



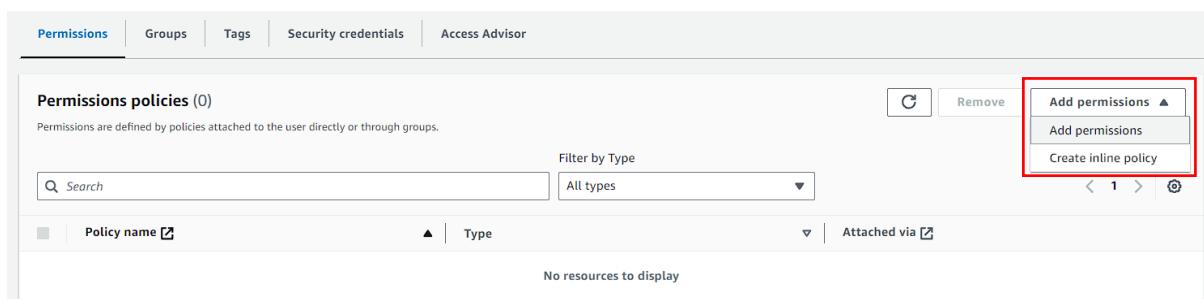
The screenshot shows the 'Amazon S3 > Buckets' page. On the left, a sidebar lists various AWS services like Buckets, Access Grants, and Storage Lens. The main area shows a table for 'General purpose buckets'. A prominent red box highlights an error message: 'You don't have permissions to list buckets. After you or your AWS administrator has updated your permissions to allow the s3>ListAllMyBuckets action, refresh this page. Learn more about Identity and access management in Amazon S3'.

4. Now you need to go back to your Root user or say to your main account.
5. There you need to navigate to IAM. Then to users.
6. You will see your user in place.
7. Now you need to open your user.



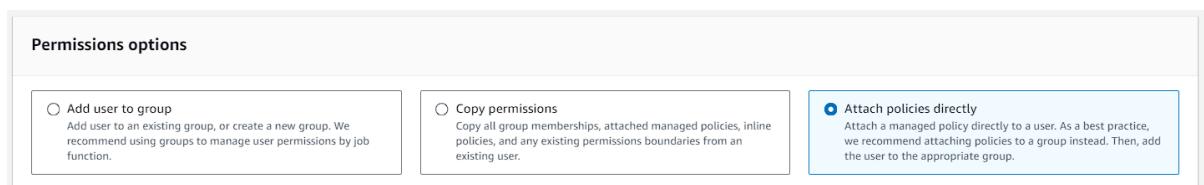
The screenshot shows the 'IAM > Users' page. It lists a single user: 's3-usr01'. The user's last activity was '17 minutes ago' on 'January 14, 2024, 16:2...'. The table includes columns for User name, Path, Groups, Last activity, MFA, Password age, Console last sign-in, and Access key ID.

8. There in the permission's tab you will see an option to add permission.
9. Click again on add permission.



The screenshot shows the 'Permissions' tab for the 's3-usr01' user. It displays a table for 'Permissions policies (0)'. A red box highlights the 'Add permissions' button in the top right corner of the table header.

10. You will see these 3 options again which you have seen while creating your IAM user.
11. But this time you have to choose **Attach Policies Directly**.



The screenshot shows the 'Permissions options' section. It contains three radio button options: 'Add user to group', 'Copy permissions', and 'Attach policies directly'. The 'Attach policies directly' option is selected and highlighted with a blue border. A tooltip for 'Attach policies directly' states: 'Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.'

12. Now if you scroll down, you will see a lot of permission policies to choose from.

13. But for the time being search for S3 permission policies.

14. You will this policy for read only access.

15. Select this and click on next.

Policy name	Type	Attached entities
AmazonS3ReadOnlyAccess	AWS managed	18

16. On the next page you will have the review page now you just need to click on Add permission.

Name	Type	Used as
AmazonS3ReadOnlyAccess	AWS managed	Permissions policy

17. You will see that your policy has been added successfully.

Name	Type	Attached via
AmazonS3ReadOnlyAccess	AWS managed	Directly

18. Now go back to your IAM user in the other browser. And navigate to S3.

19. And this time you will able to see your bucket in place.

Name	AWS Region	Access	Creation date
datausr1234	Europe (London) eu-west-2	Public	January 12, 2024, 19:46:48 (UTC+05:30)

20. You can also open its content.

21. But you can not make any changes because the policy that you issued is for read only.

datausr1234 Info Publicly accessible

Objects Properties Permissions Metrics Management Access Points

Objects (2) Info

Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)

< 1 > (1)

<input type="checkbox"/>	Name	Type	Last modified	Size	Storage class
<input type="checkbox"/>	Dockerfile	-	January 12, 2024, 23:07:36 (UTC+05:30)	113.0 B	Standard
<input type="checkbox"/>	scripts/	Folder	-	-	-