😊 IAM Permission Boundary

An IAM (Identity and Access Management) permission boundary is a feature in AWS (Amazon Web Services) that defines the maximum permissions an IAM entity (such as a user or role) can have. It acts as a policy that sets the maximum permissions that the entity can be granted regardless of any other policies attached to it.

By setting a permission boundary, you can control the maximum level of access an IAM entity can have, even if policies are attached that would otherwise grant broader permissions. This helps enforce security and compliance requirements by ensuring that certain IAM entities cannot exceed a predefined level of access.

😄 Use cases of IAM Permission Boundary:

IAM permission boundaries have several use cases:

1. **Security Control:** Permission boundaries help enforce the principle of least privilege by restricting the maximum permissions that IAM entities can have. This reduces the risk of unauthorized access and potential security breaches.
2. **Compliance Requirements:** Many regulatory standards require organizations to implement strict access controls and enforce separation of duties. IAM permission boundaries provide a mechanism to meet these compliance requirements by limiting the scope of access for IAM entities.
3. **Complex Access Requirements:** In environments with complex access requirements, where users or roles may have multiple policies attached, permission boundaries offer a way to set clear limits on access levels, ensuring that entities cannot exceed certain permissions regardless of other policies.
4. **Third-party Access:** When granting access to third-party entities, such as vendors or partners, IAM permission boundaries can be used to restrict their access to only the necessary resources and actions, reducing the risk of potential misuse or unauthorized access.
5. **Resource Isolation:** Permission boundaries can be used to isolate resources within an organization. By defining strict boundaries for different teams or departments, organizations can ensure that each group only has access to the resources required for their specific tasks, enhancing resource isolation and security.

Overall, IAM permission boundaries are a powerful tool for managing access control in AWS environments, providing granular control over permissions and helping organizations maintain security and compliance standards.

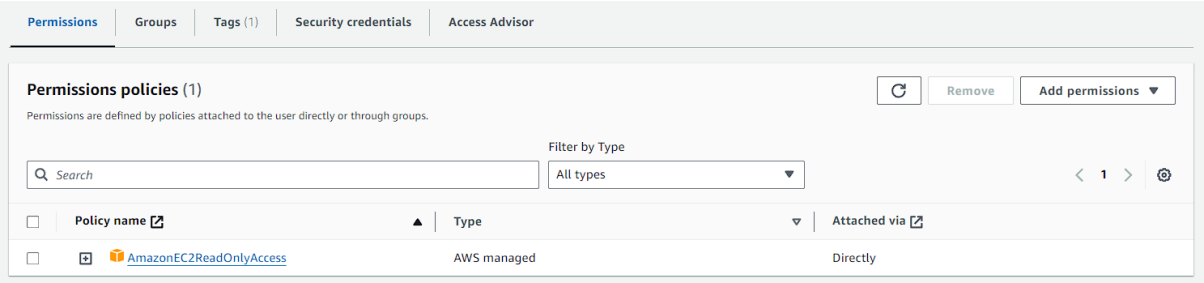
🤔 What are we doing in this Lab?

In IAM permission boundaries, we're defining the maximum permissions that an IAM entity (like a user or role) can have within AWS services. The end goal is to enhance security and compliance by limiting the scope of access for these entities, ensuring they cannot surpass predefined boundaries, even if other policies would grant broader permissions. It helps

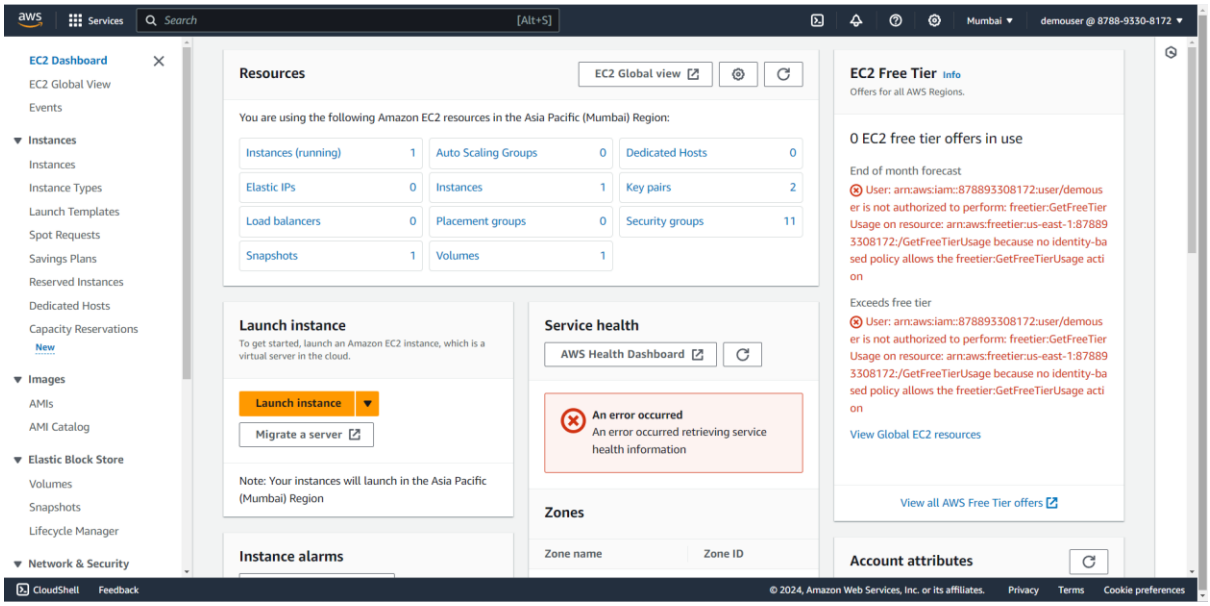
organizations maintain control over access levels and reduce the risk of unauthorized actions within their AWS environments.

😄 To begin with the Lab:

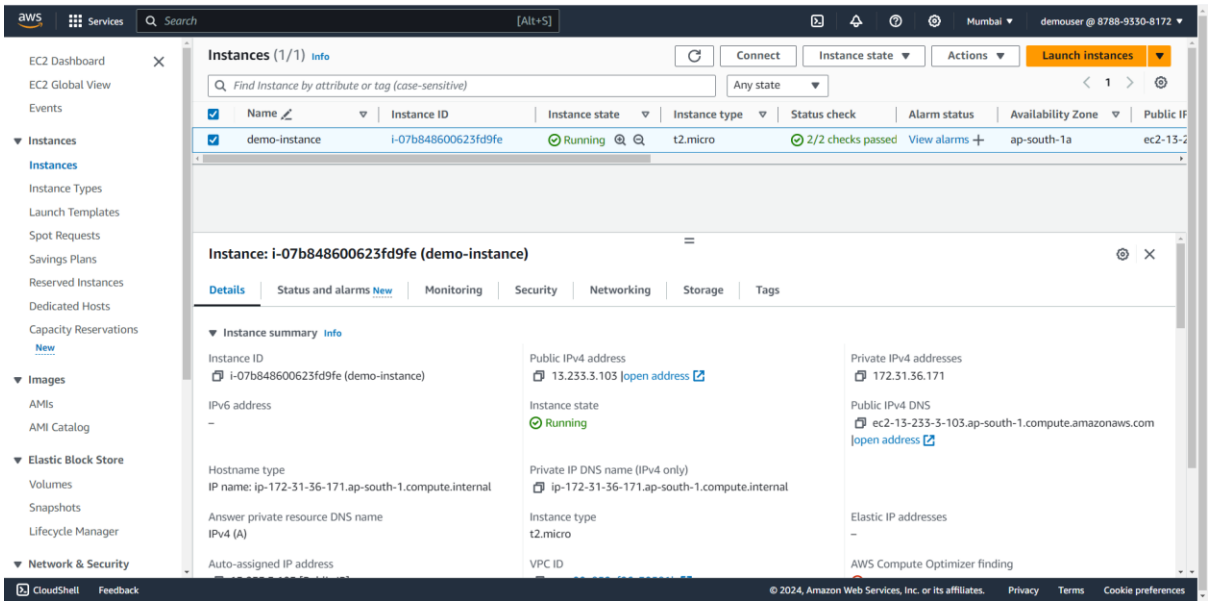
1. So, login to AWS console and navigate to EC2, there you need to launch an instance.
2. Once the instance is launched now you have to go to IAM and there you are going to create an IAM user.
3. Now attach EC2 read only permission to this IAM user.



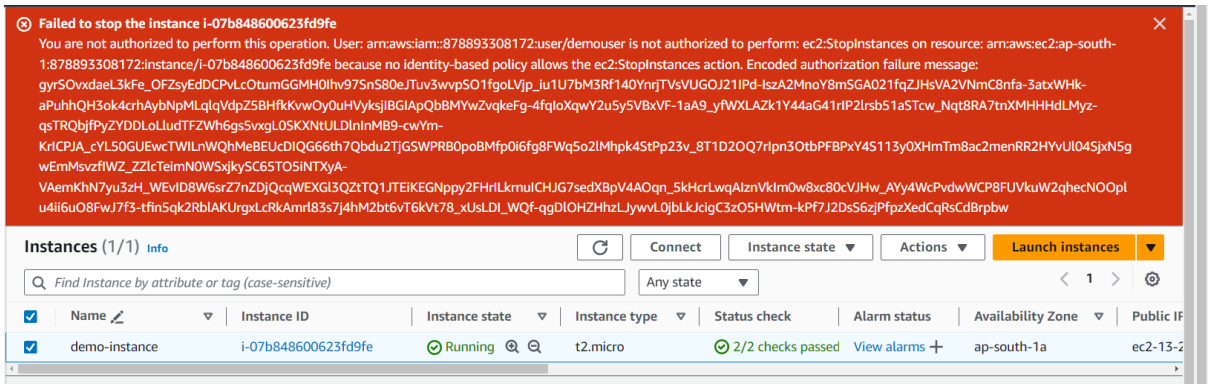
4. Now you are going to login with this IAM user in another browser. Then navigate to EC2. Here you can see that the permission is for read only so, you can only see the instance.



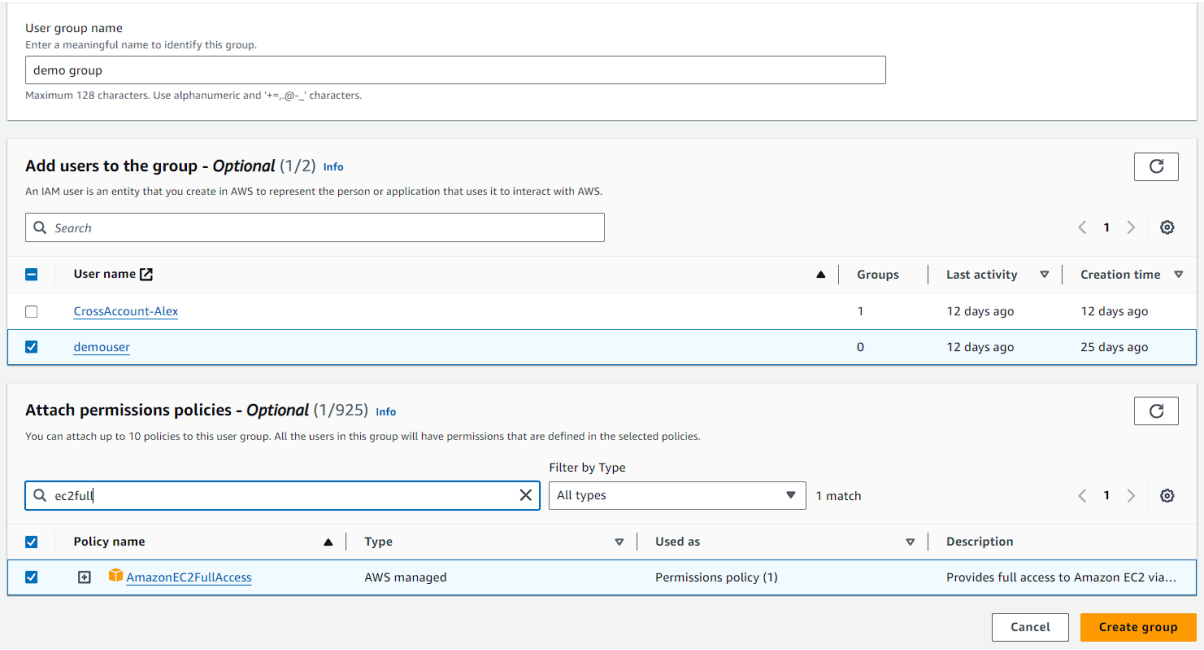
5. Here you can see this instance. But if you will try to stop this instance or terminate this instance then you will get an error.



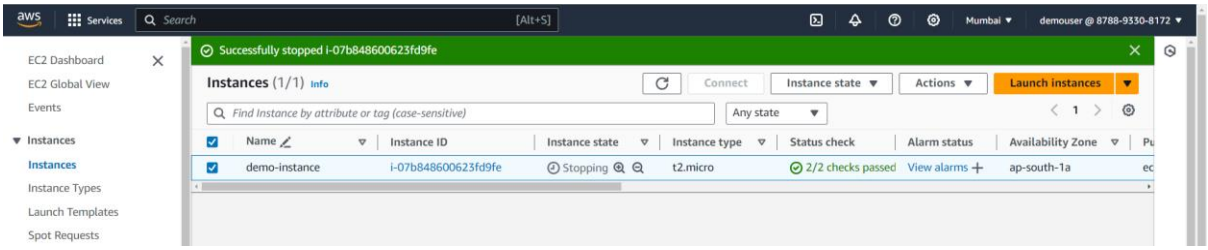
6. Below you can see the error.



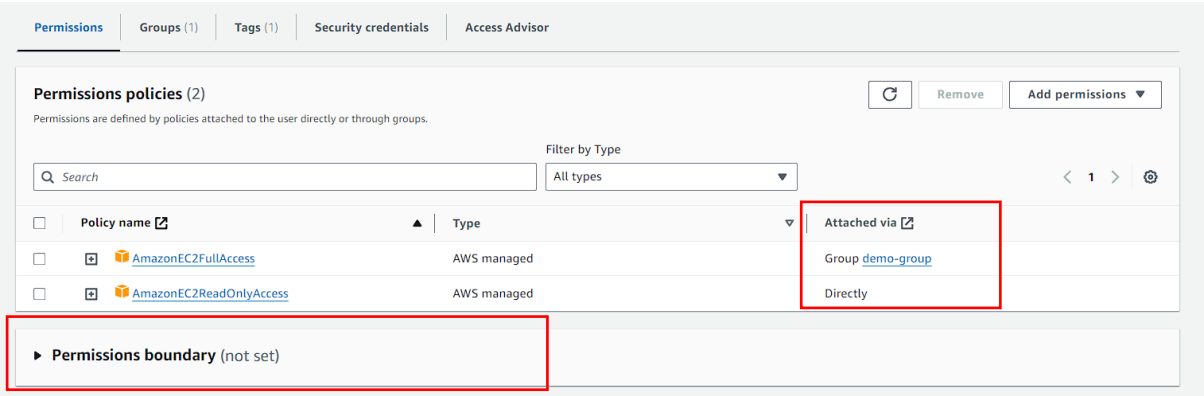
7. Now go back to your root account or main account and navigate to IAM then you are going to create a user group.
8. Here, you are going to give a name to your group then select the IAM user and attach the policy for EC2 full access. Then click on create group.



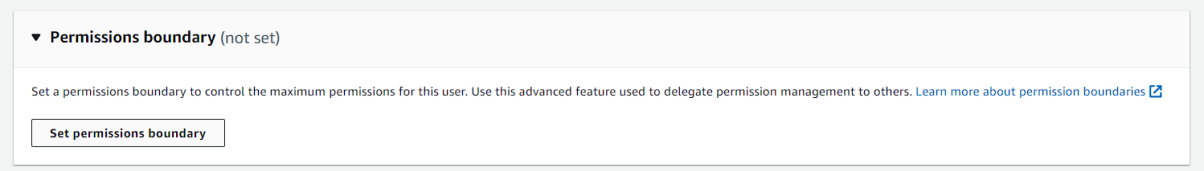
9. So, now the thing is first we attached read only permission directly to the user then we attached this user to the group and in that group, we attached EC2 full access. According to this the user has both read only and full access permission attached.
10. Now if you go back to your IAM user in another browser and again try to stop the instance. Below you can see that you are able to stop this instance.



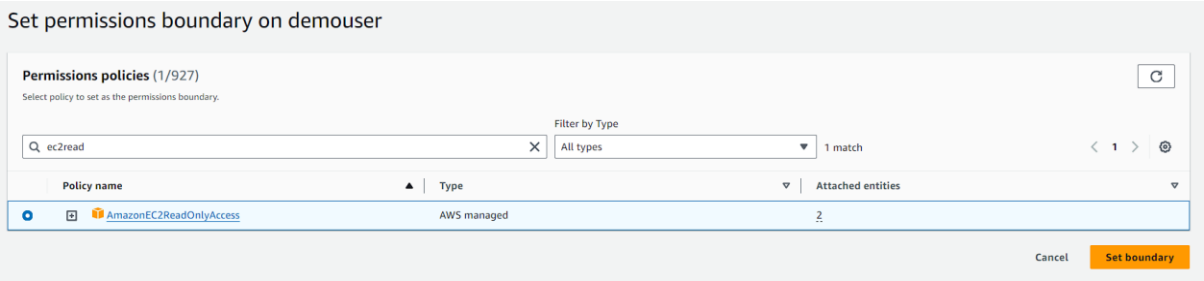
11. Come back to IAM in your root account and open your user. In the dashboard of your user if you'll scroll down a little you can see an option for permission boundary.
12. You can also see how the permissions are attached to this user.



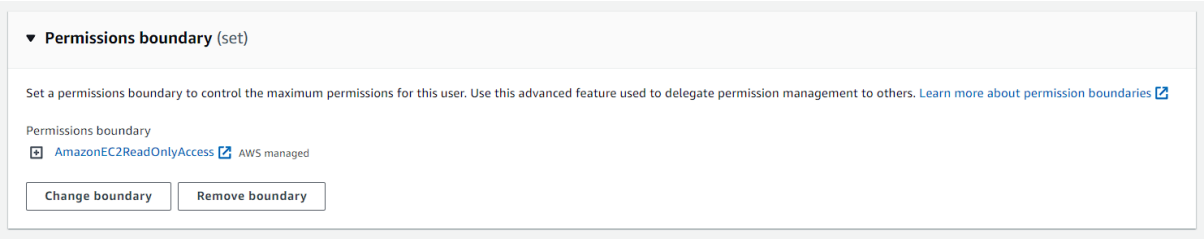
13. Now click on permissions boundary and then set permissions boundary.



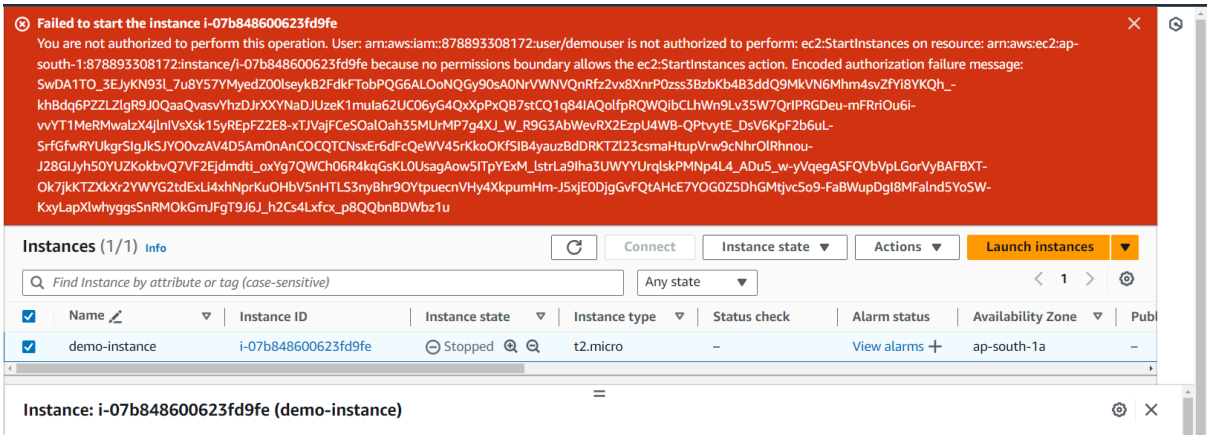
14. Now you are going to set boundary for EC2 read only permission.



15. Below you can also verify that the permission boundary has been set successfully.



16. Now you are going back to the user in another browser and try to start the instance and instantly you will get an error.



17. This means that permission boundary has set the hierarchy for the permission which you have attached to the IAM user.

In this lab exercise, we are demonstrating the implementation of IAM (Identity and Access Management) permission boundaries in an AWS (Amazon Web Services) environment. The end goal is to enhance security and compliance by setting clear limits on the maximum permissions that IAM entities (such as users or roles) can have, ensuring they cannot exceed predefined boundaries, even if other policies would grant broader permissions. This helps organizations maintain control over access levels and reduce the risk of unauthorized actions within their AWS environments.