😊 AWS Organizations

AWS Organizations is a service provided by Amazon Web Services (AWS) that allows you to centrally manage and govern multiple AWS accounts. It helps you organize your accounts into a hierarchical structure called an organization and offers tools for managing policies, permissions, and billing.

Key Features of AWS Organizations:

1. **Centralized Management**: It lets you manage multiple AWS accounts from a single location, making it easier to set up and govern your AWS environment.
2. **Consolidated Billing**: You can consolidate billing for multiple AWS accounts into a single payment, which can help simplify tracking costs and optimize spending.
3. **Policy Management**: AWS Organizations allows you to apply policies across accounts, such as security and compliance requirements. These policies can control what actions can be performed within each account.
4. **Account Grouping**: You can group accounts into organizational units (OUs) and apply policies to these units, simplifying management.
5. **Resource Sharing**: The service enables sharing resources across accounts, such as AWS License Manager licenses or AWS Transit Gateway, without needing to create duplicate resources in each account.

Why Use AWS Organizations?

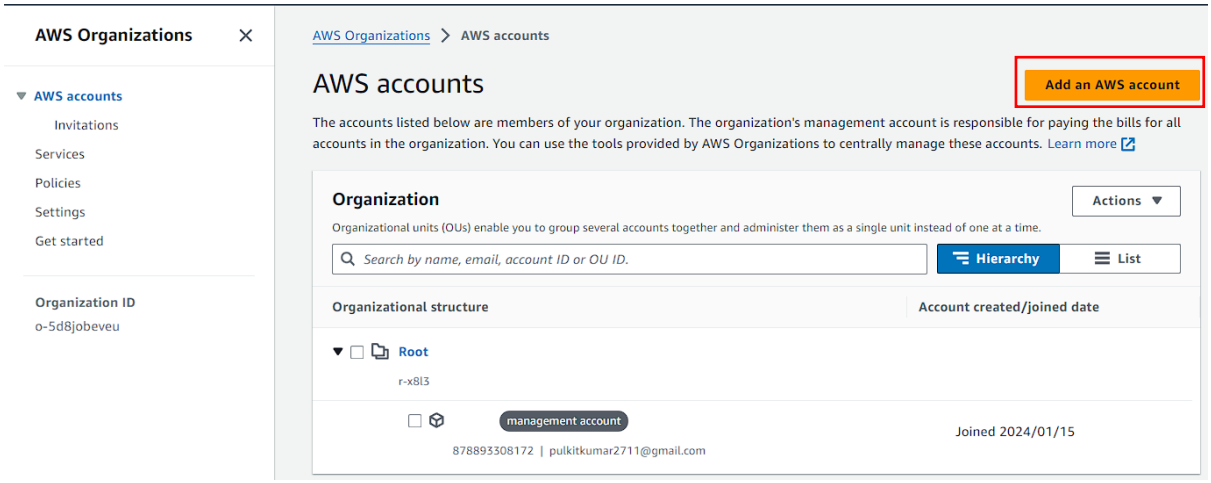
- **Simplified Management**: It simplifies the management of multiple accounts, especially for large enterprises or organizations with different departments, projects, or environments (e.g., development, testing, production).
- **Cost Efficiency**: With consolidated billing, you can benefit from volume discounts and simplified cost tracking.
- **Enhanced Security and Compliance**: By enforcing policies at the organization level, you can ensure consistent security and compliance across all accounts.
- **Scalability**: It makes it easier to scale your infrastructure by adding new accounts and resources as needed.

In simple terms, AWS Organizations helps you keep all your AWS accounts under control, ensuring they are organized, secure, and efficiently managed.

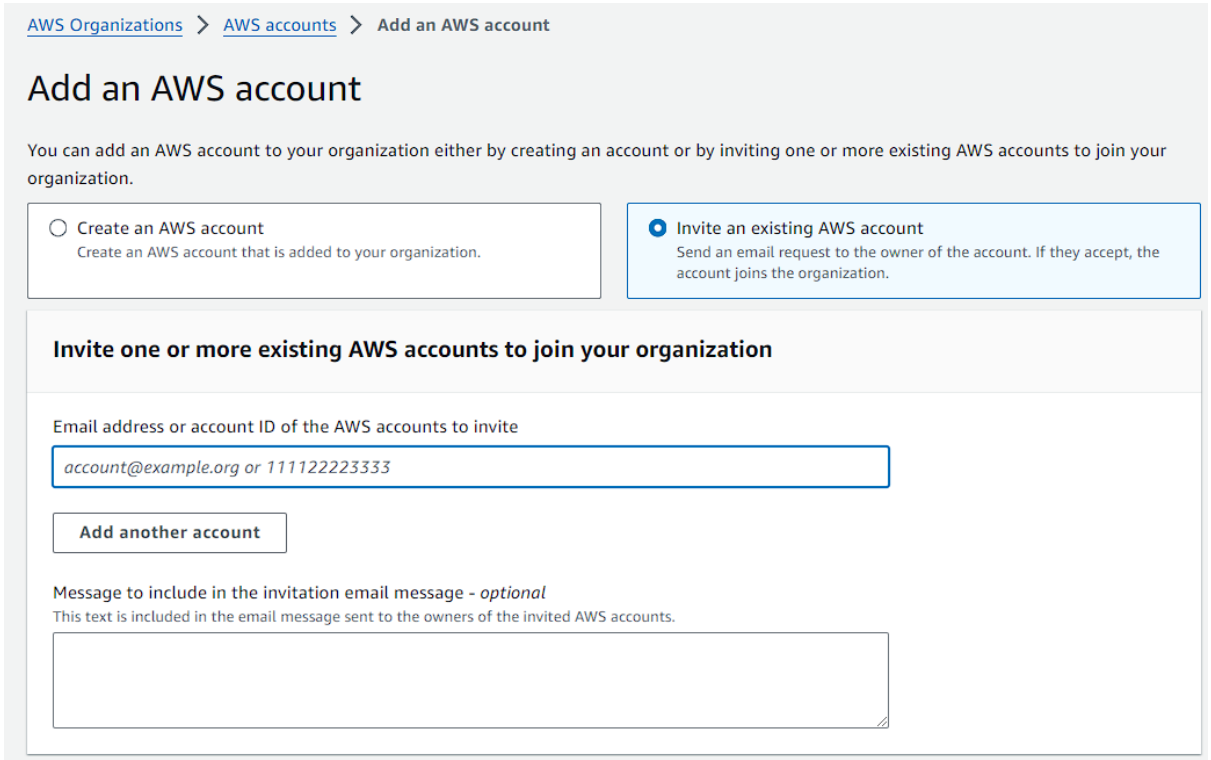
End Goal: In this lab, you're working with AWS Organizations to manage multiple AWS accounts within an organization. The goal is to invite another AWS account to join the organization, apply a service control policy (SCP) from the management account to restrict access to a specific AWS service (S3 in this case) for the member account, and then observe the effects of the policy on the member account's access permissions. Finally, you'll detach the policy to restore access to the restricted service for the member account.

😄 To begin with this Lab:

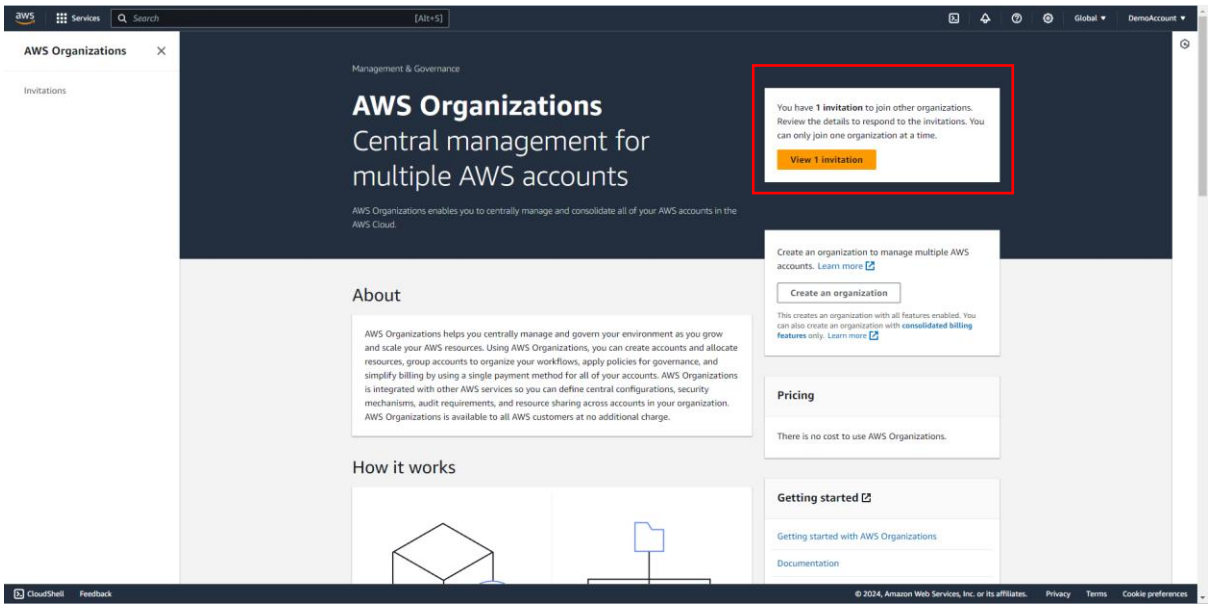
1. Now for this lab you should have AWS Organizations setup in your AWS Account.
2. Once you have setup the organizations you will see this type of dashboard for it.
3. Now at this stage you will see that you have one account and it is also showing you that this is a management account. So, from this account you can go ahead and do various things like apply policies to member account and various others.



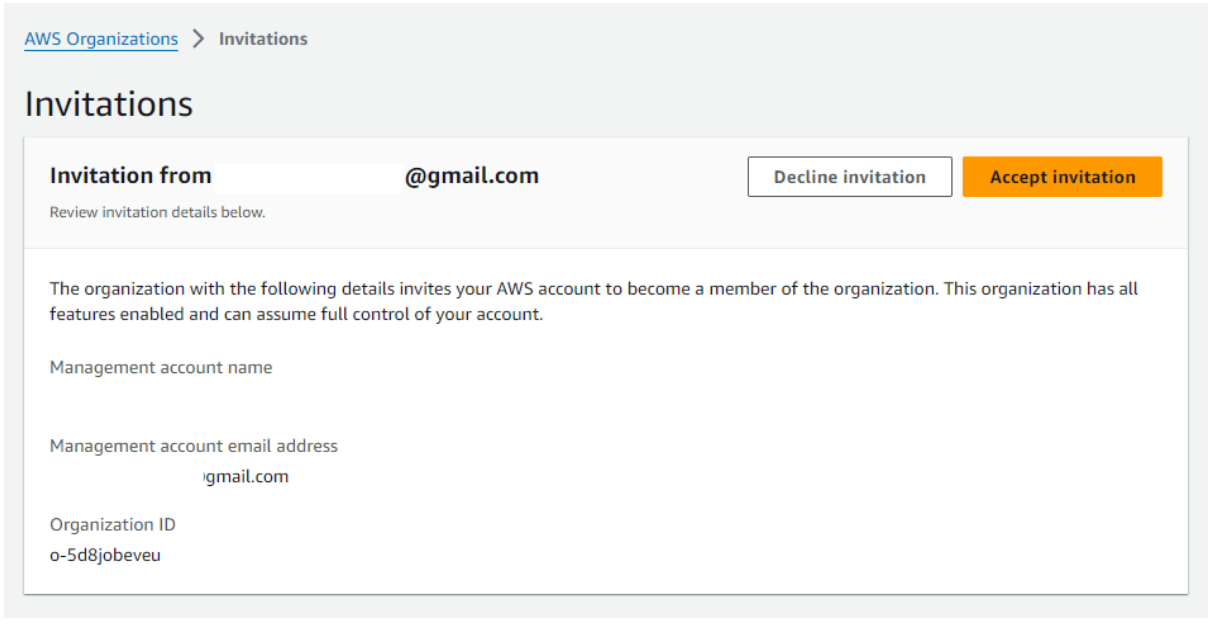
4. Now you can go ahead and invite other AWS account. For that click on Add an AWS Account.
5. You can either create an AWS account or you can add an existing account in it.
6. Now click on invite an existing AWS Account. Then paste the account ID of the other account. After that just click on send invitation.



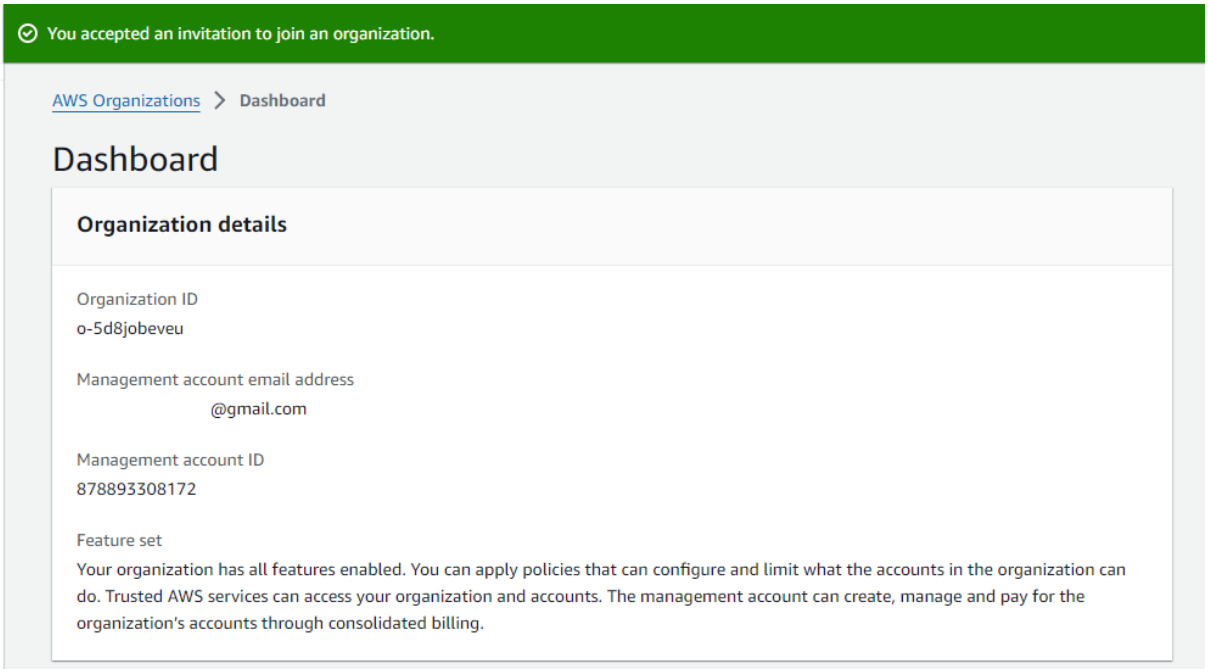
7. Now from the other account in the AWS Console navigate to Organizations. There you will see an invitation.
8. Now click on View invitation and accept the invitation.



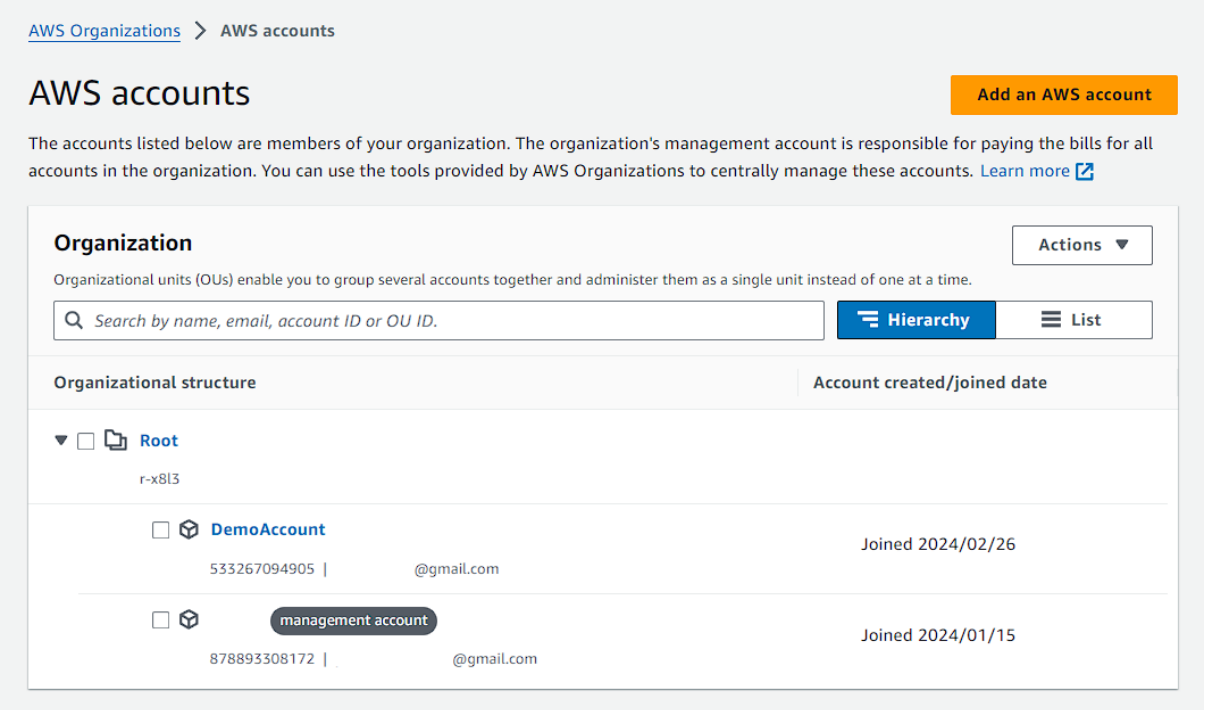
9. Here you will see the details where the invitation came from. What is the management account name and the email address.
10. Now click on accept invite.



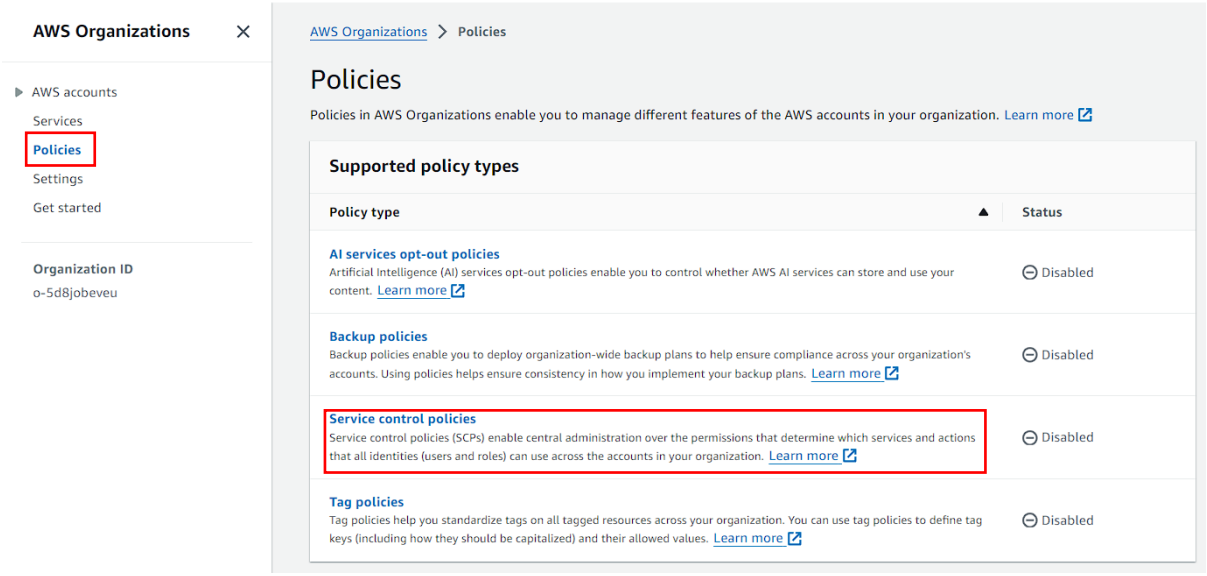
11. After that you will see this kind of dashboard.



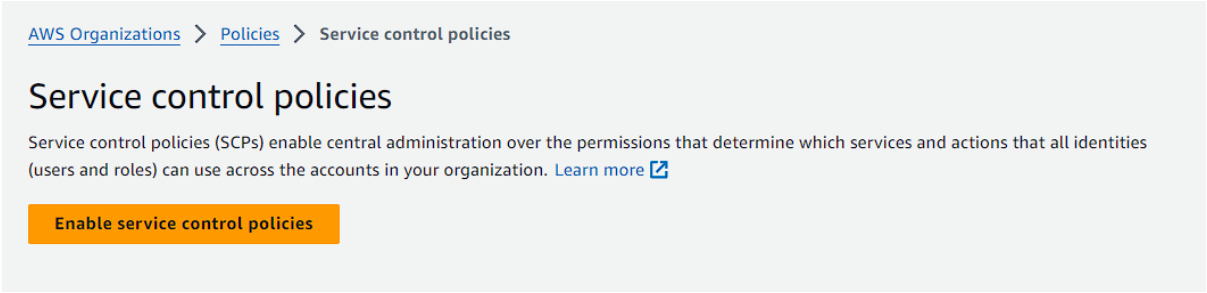
12. Now come back to your main account and refresh the organization page you will be able to see the account that you had just invited.



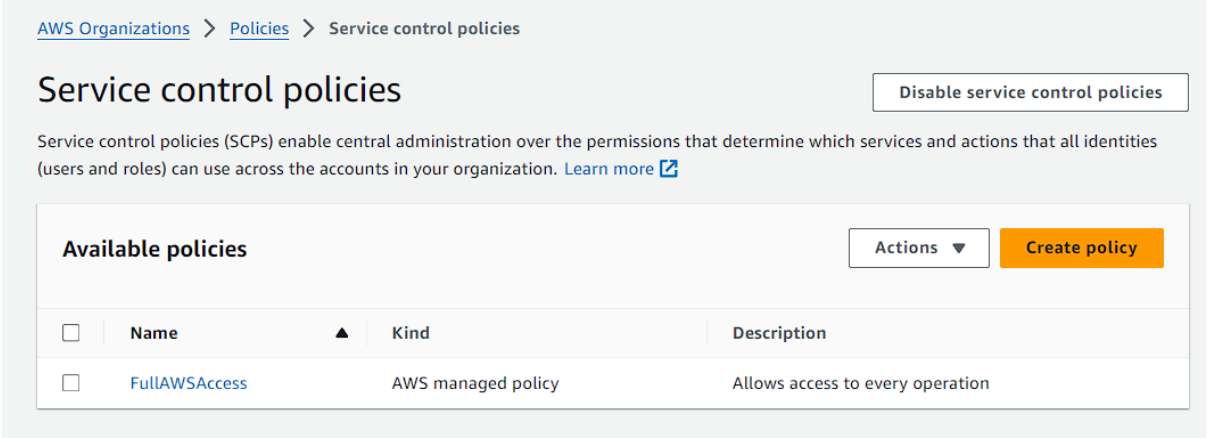
13. So, now let's do one thing similar to the policy demo that we had seen, where we go ahead and apply a specific policy to an account. And once the policy is applied, not even a root user of that account can access that service.
14. Now in your management account go to policies, from there click on service control polices.



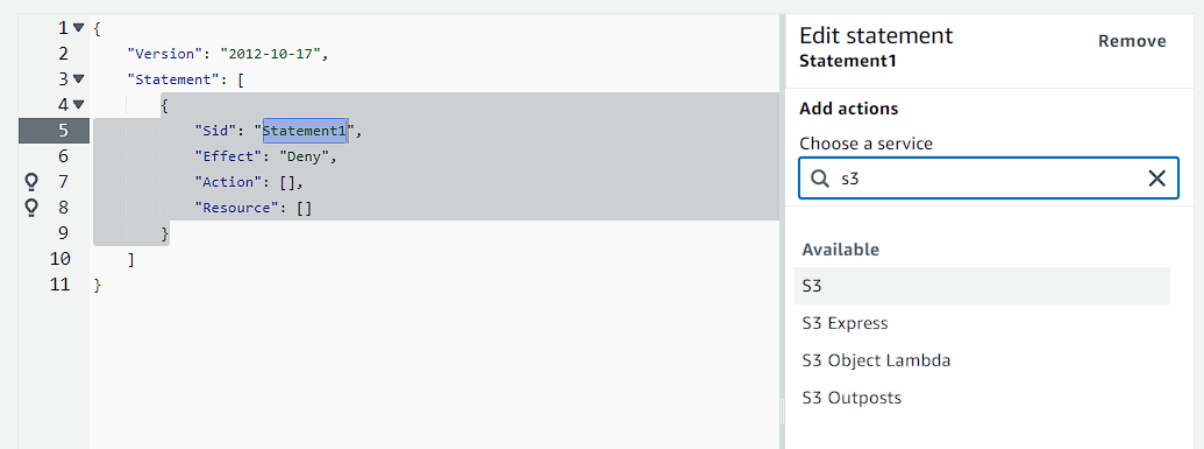
15. First you are going to enable your service control policies.



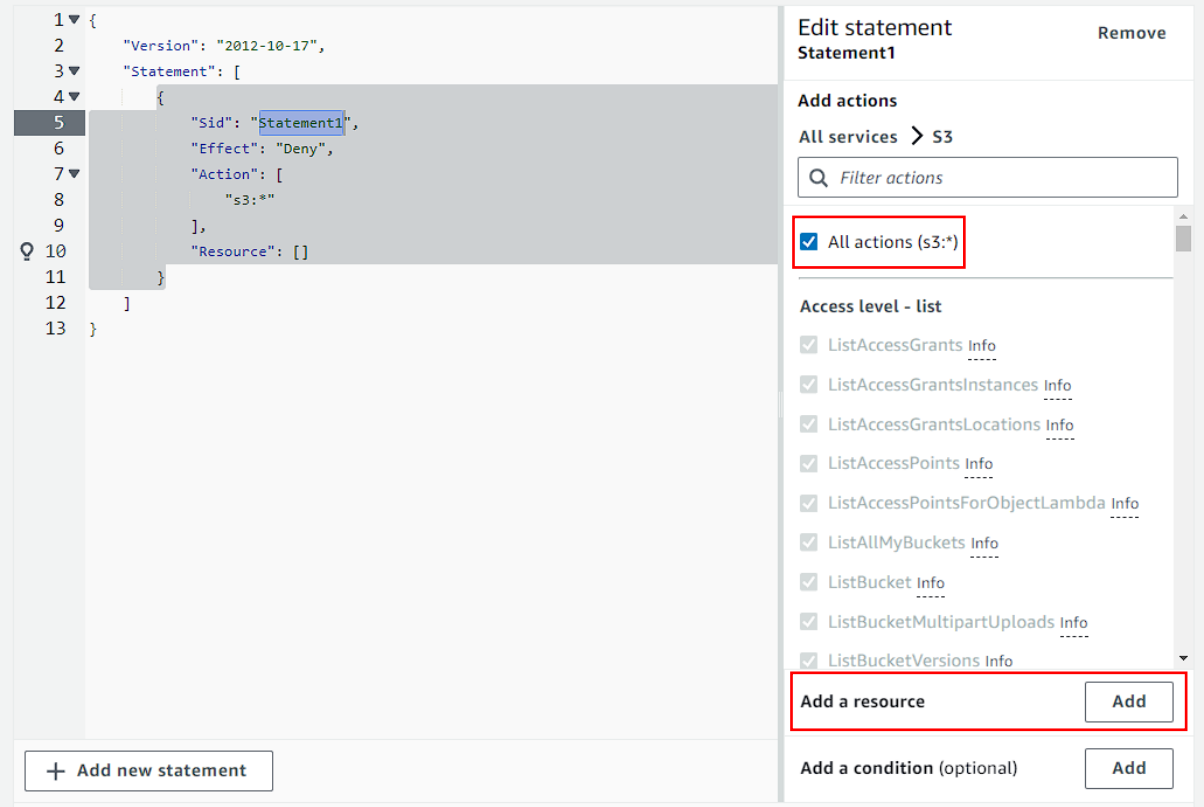
16. Then you will see that at this time you have full AWS Access.



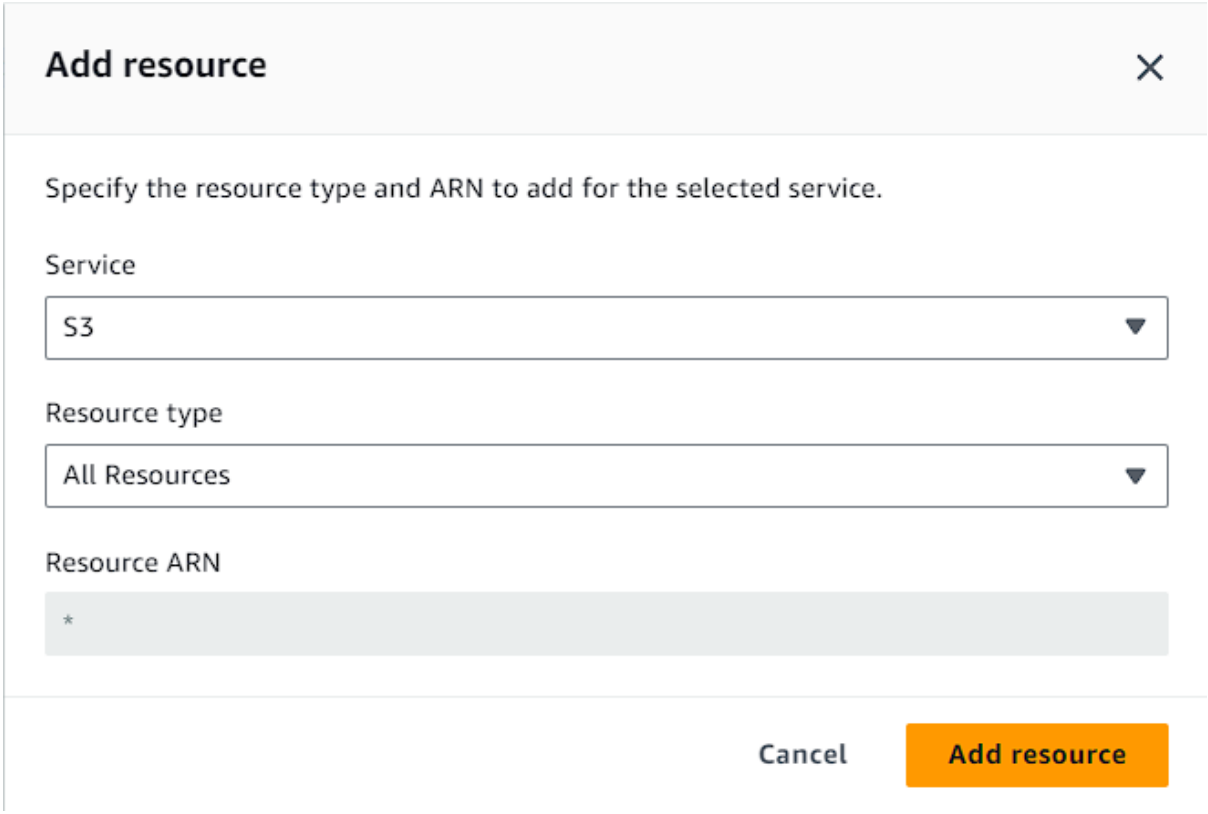
17. Now let's go ahead and create a new policy. Click on create policy.
18. Now here first you are going to specify a name for it. Then if you'll scroll down to edit statement. Here you going to choose a S3 as a service.



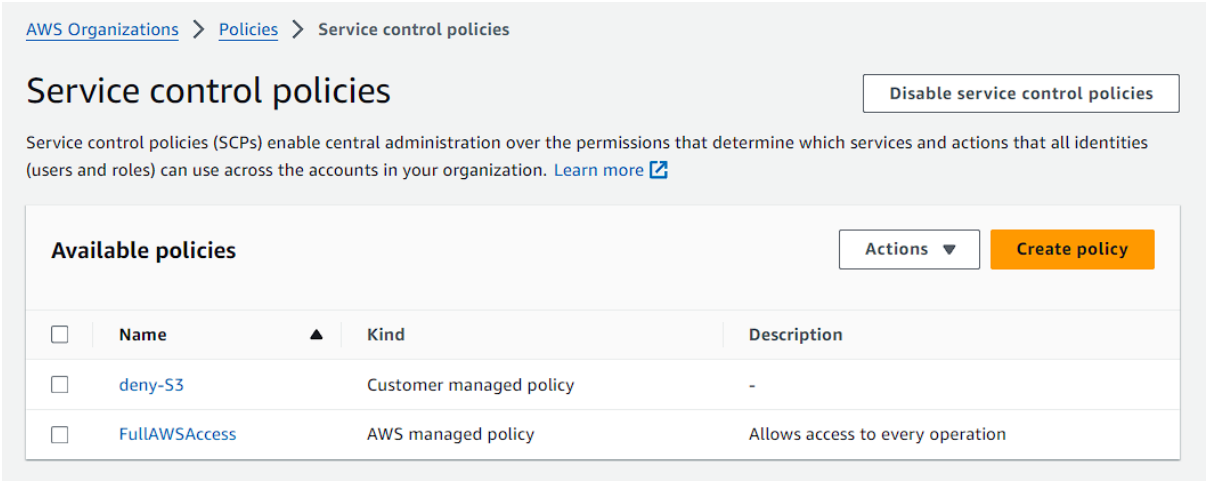
19. Then click on All actions. After that click on add resource.



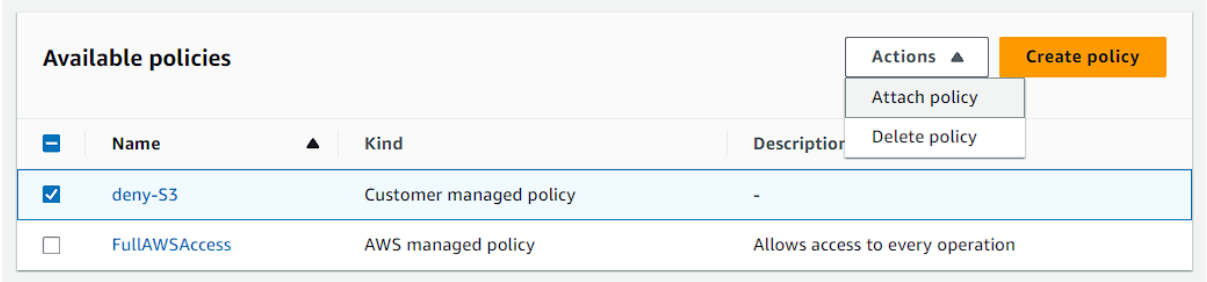
20. Select service as S3 and in the resource type choose all resources. Then click on add resource.



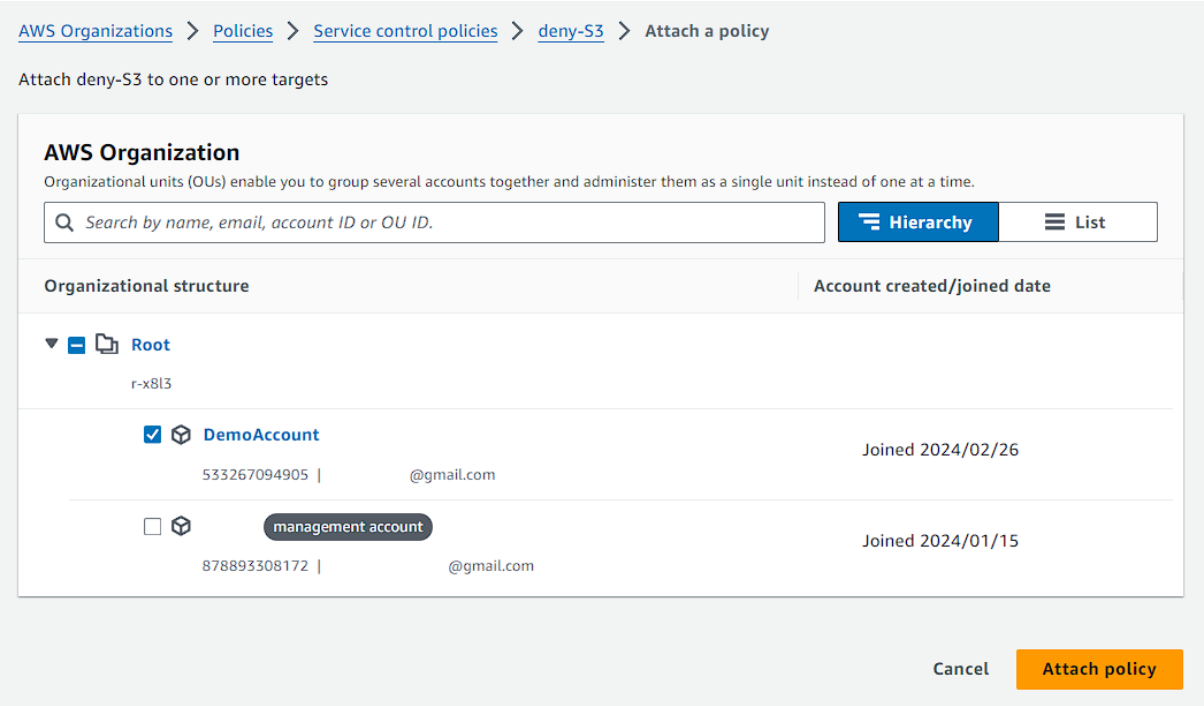
21. After that just create your policy.
22. Then you will see your policy here.



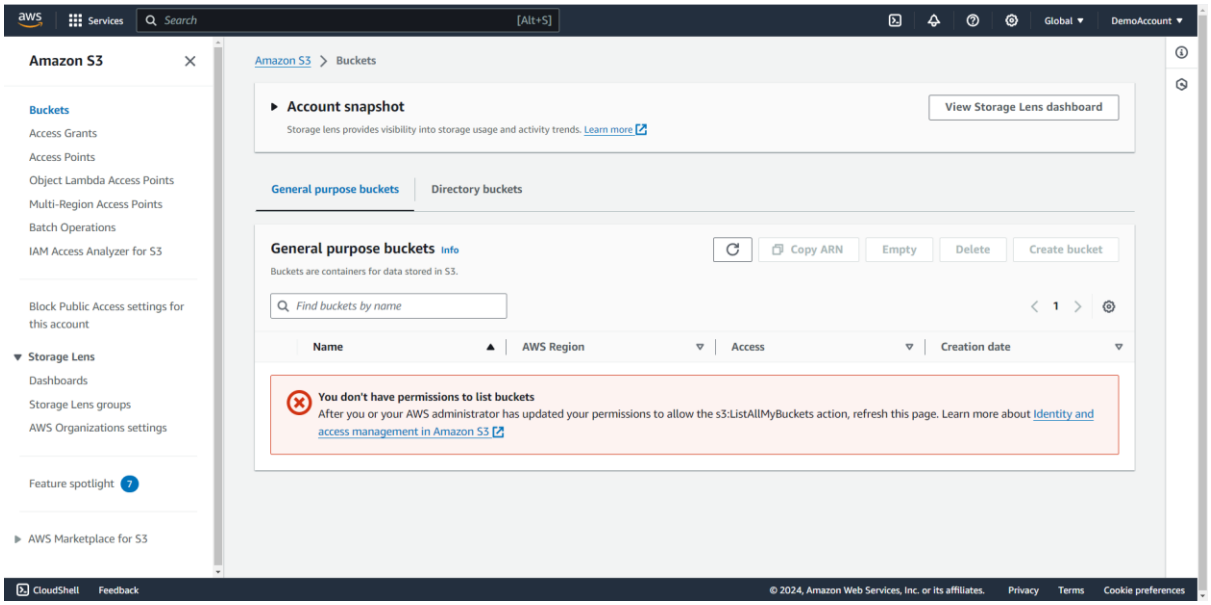
23. Now you are going to associate this policy with your member account.
24. For that select your policy and click on attach policy.



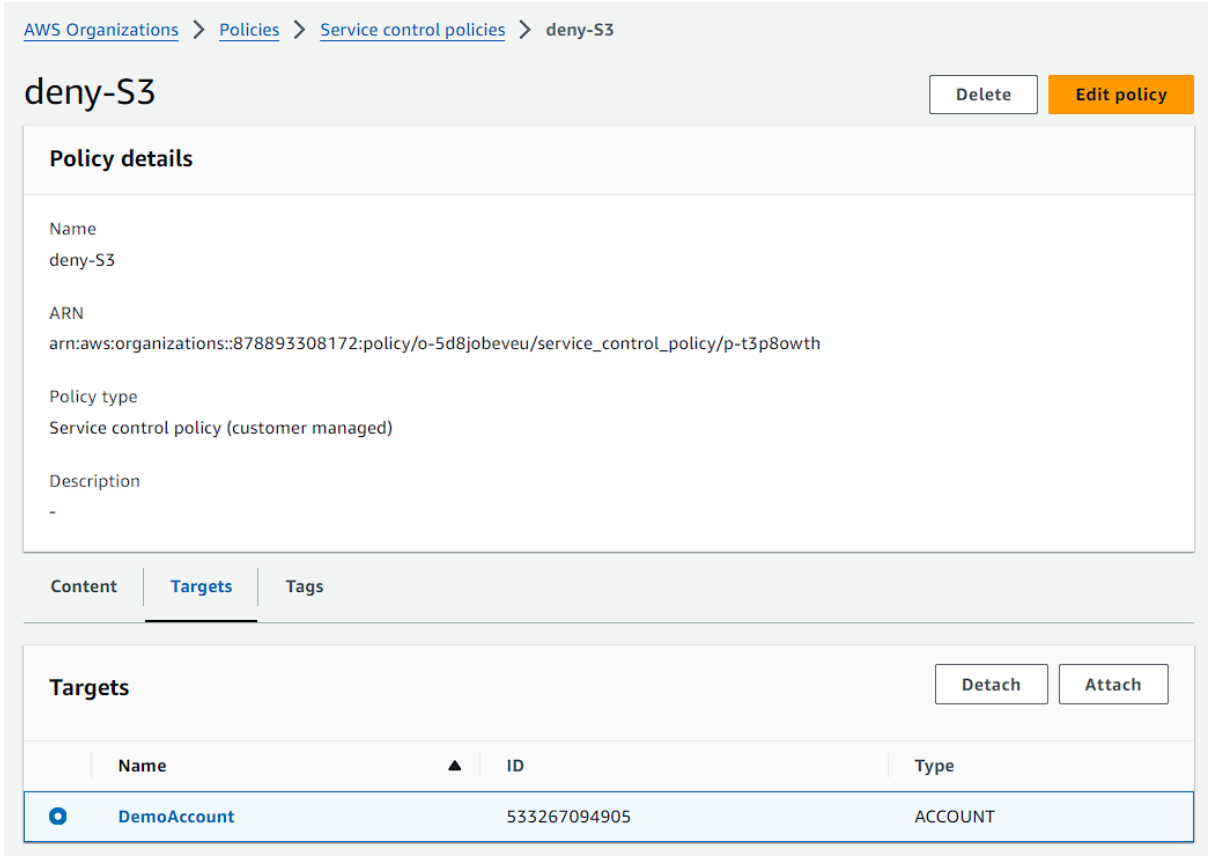
25. Once you have clicked on attach policy you will see it is asking you to select your member account. Select it and click on attach policy.



26. Now if you will go to your member account and navigate to S3 then you will see access denied.



27. Now you can also detach your policy go to your policy in your management account and open it. Then if you will targets in it and select the account then click on detach.



28. Then if you will again navigate to your member account and refresh the page you can see that you have the permission now to view S3.