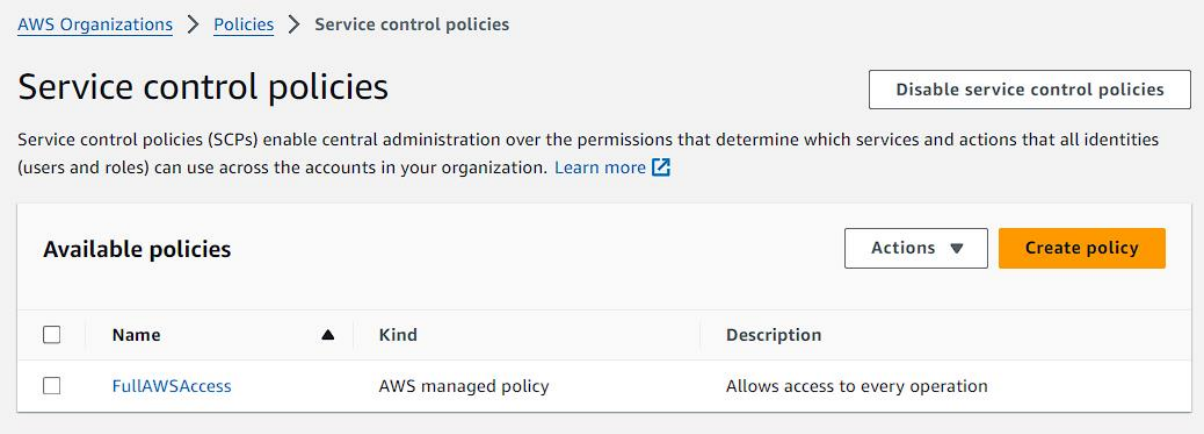
😊 Changing policy from Deny to Allow

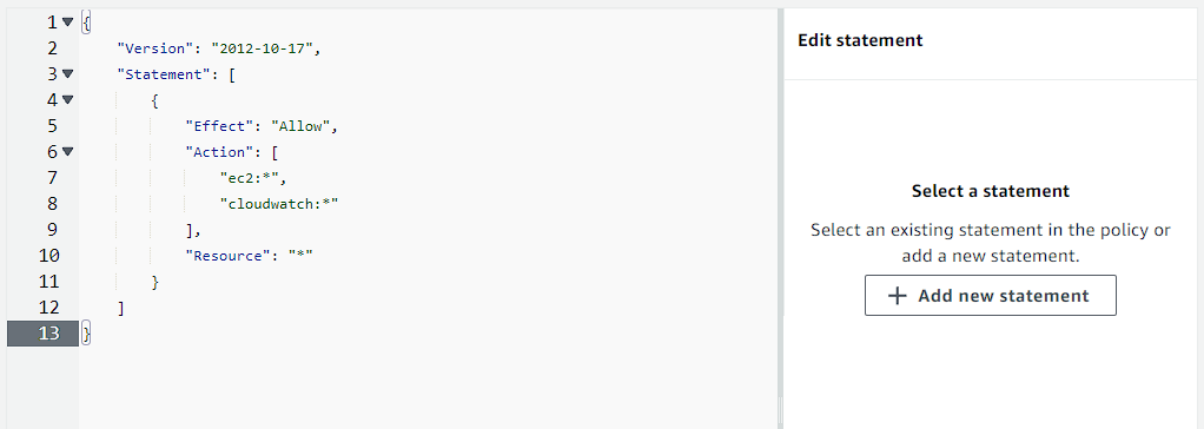
In this lab, you're exploring how to switch from a deny list policy to an allow list policy using AWS Organizations and Service Control Policies (SCPs). You start by creating an allow policy that grants full access to specific AWS services (EC2 and CloudWatch). Then, you attach this allow policy to a member account, ensuring that only the specified services are accessible. Finally, you remove the member account from the deny list policy to complete the transition. Through this process, you observe the effects of the new allow list policy on the member account's access permissions.

1. Now, in the earlier lab, we were discussing about the basics of SCP (Service Control Policies) and how by default, using the full Access SCP, the denialist strategy is taken into effect.
2. So, in this lab you are going to see how you can switch to allow list policy from deny list policy.
3. First, go to organizations and then move to policies. Here you can see by default we get Full AWS access policy.

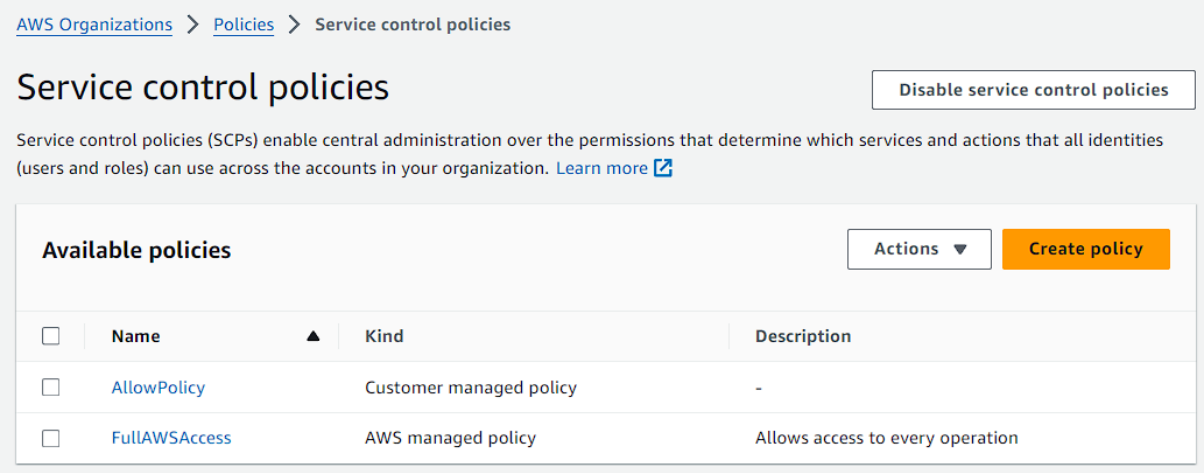


4. Now you are going to click on create policy and paste the policy below. In this policy the actions are to give EC2 full access and cloud watch full access.

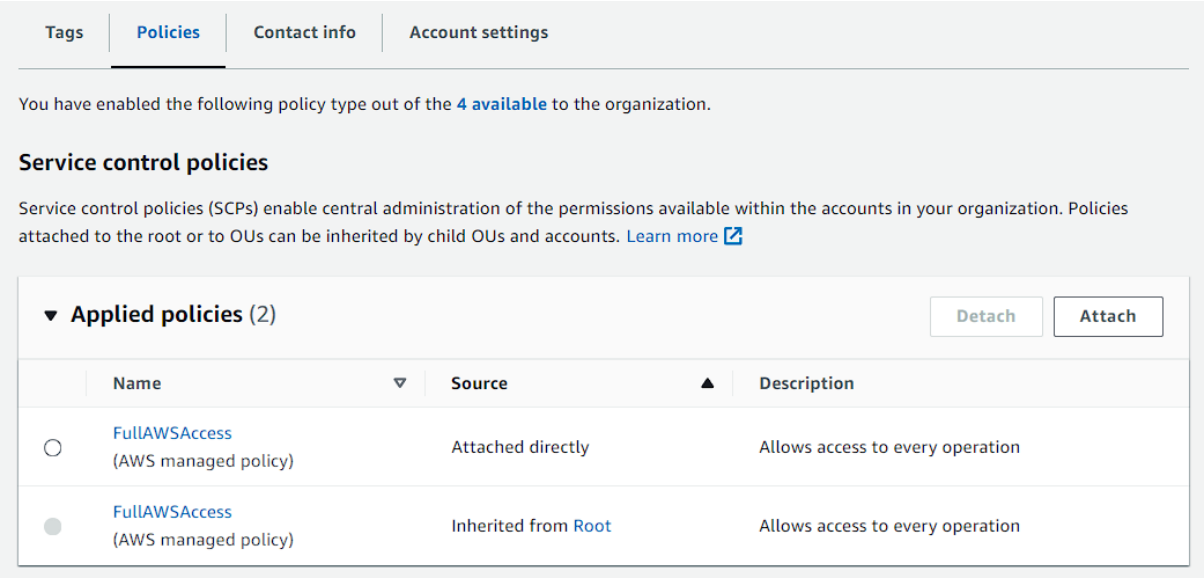
```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:*",
        "cloudwatch:*"
      ],
      "Resource": "*"
    }
  ]
}
```



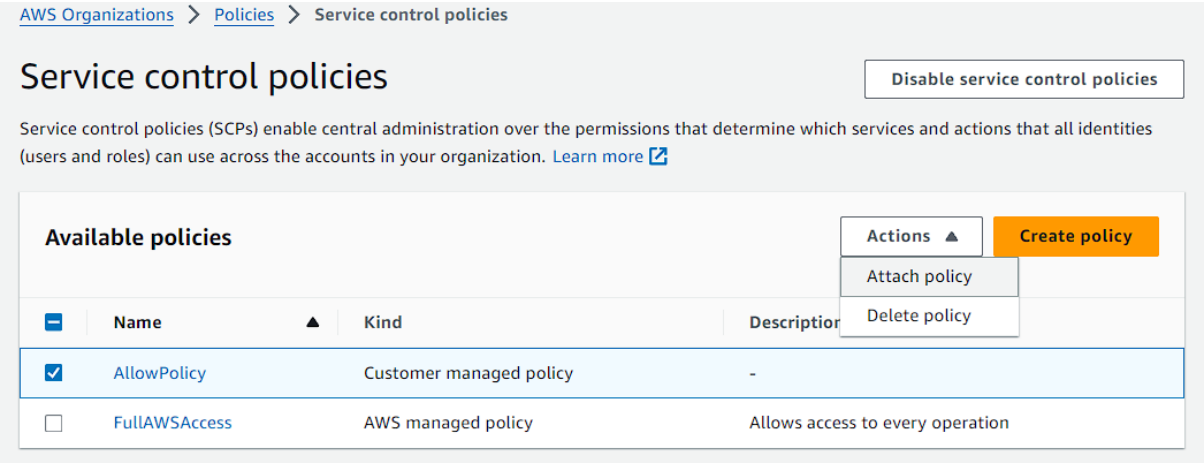
5. Once you are done just create your policy. Below you can see that you have a allow policy.



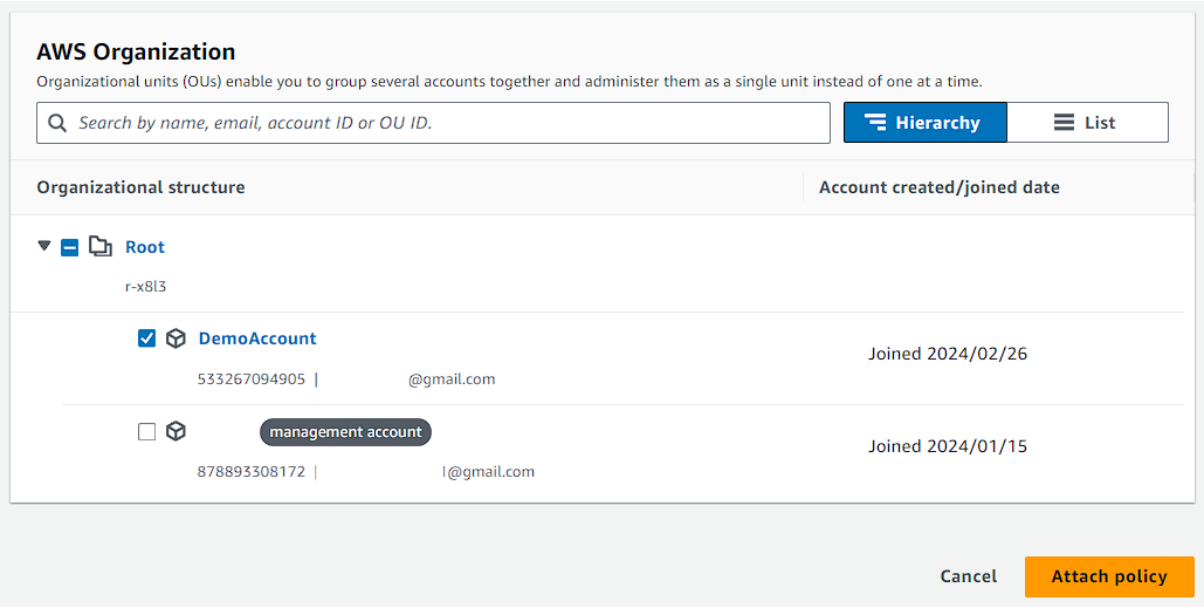
6. Now if you will open your member account.
7. And if you look there in the policies it is attached to 2 policies. One is attached directly and the other is inherited.



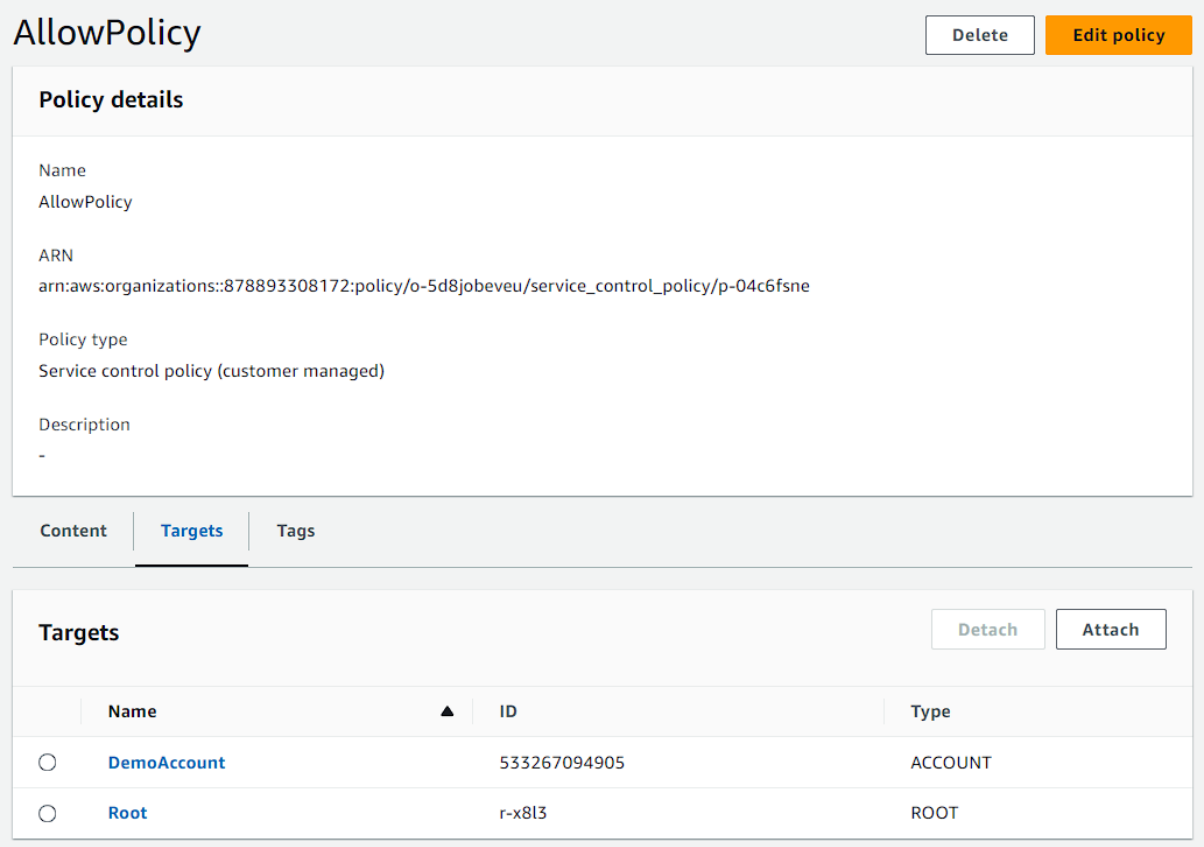
8. Now go back to your policy and attach your allow policy to member account. So, to attach your policy select your policy then click on actions and then click on attach policy.



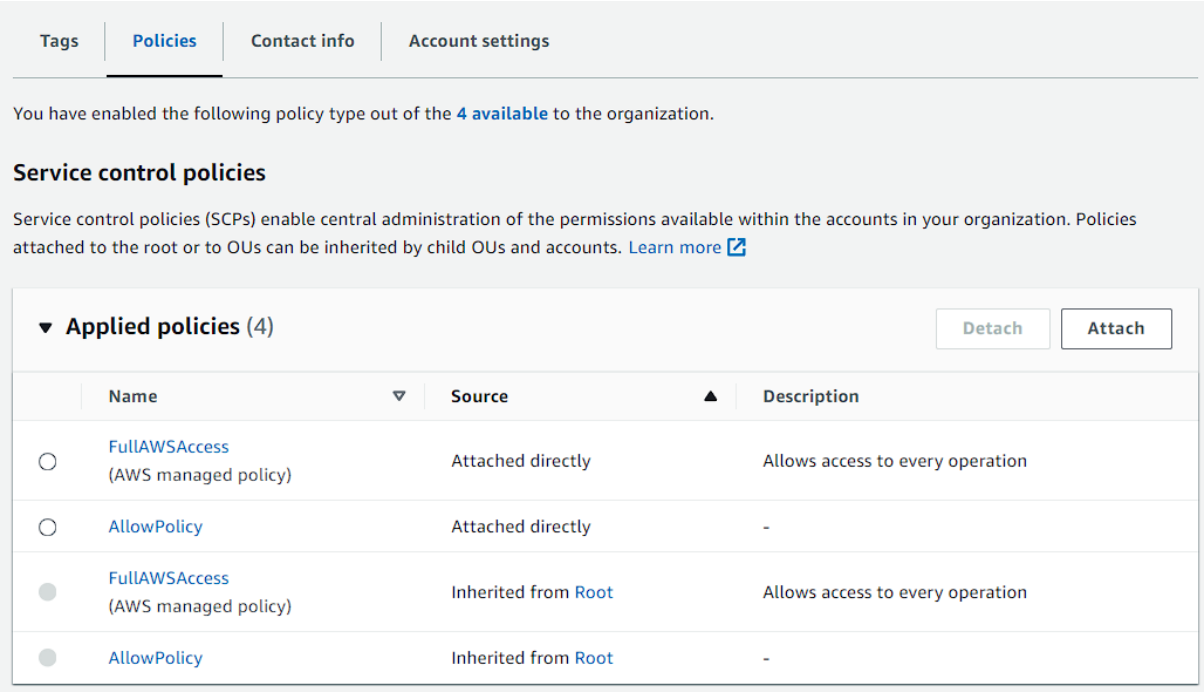
9. Now you will see that is asking you to select the account on which you want to attach this policy.
10. So, select your member account and root then click on attach policy.



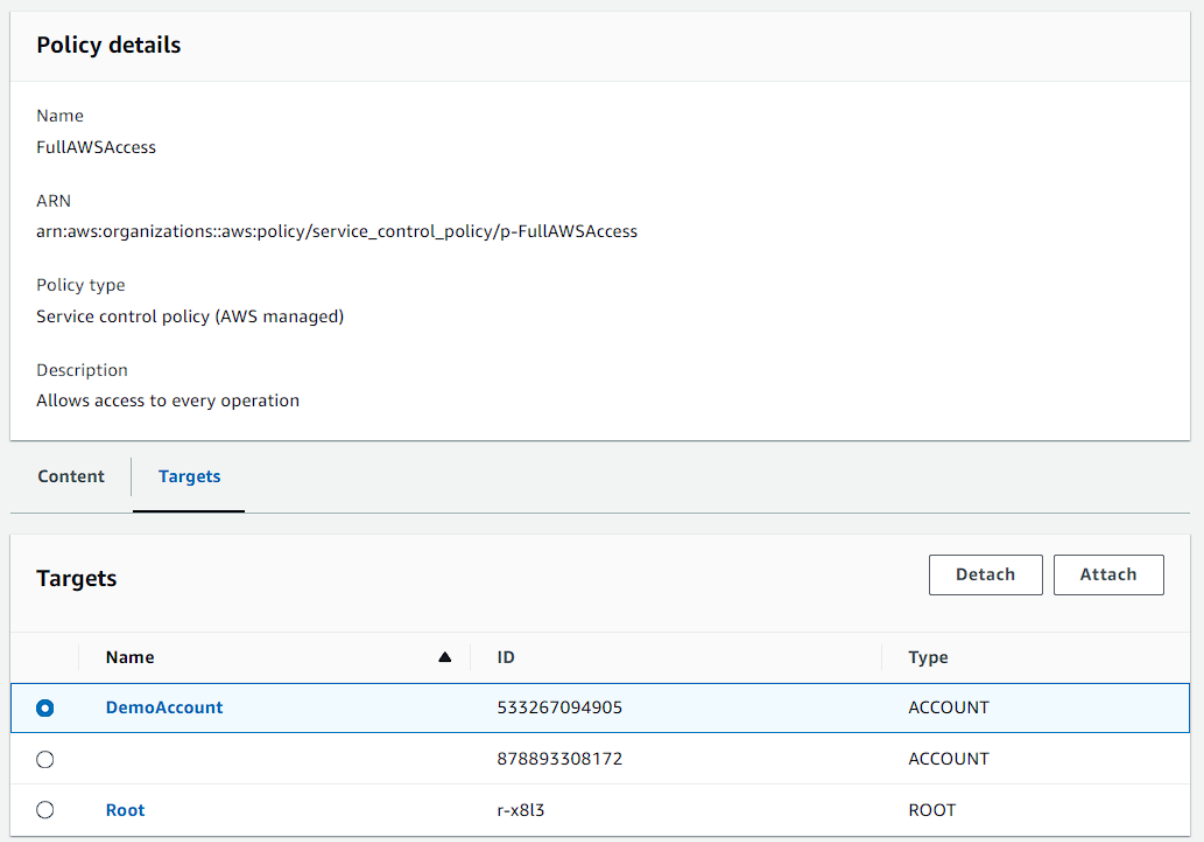
11. Now if you will open the targets of your allow policy you can see the member's account and root user.

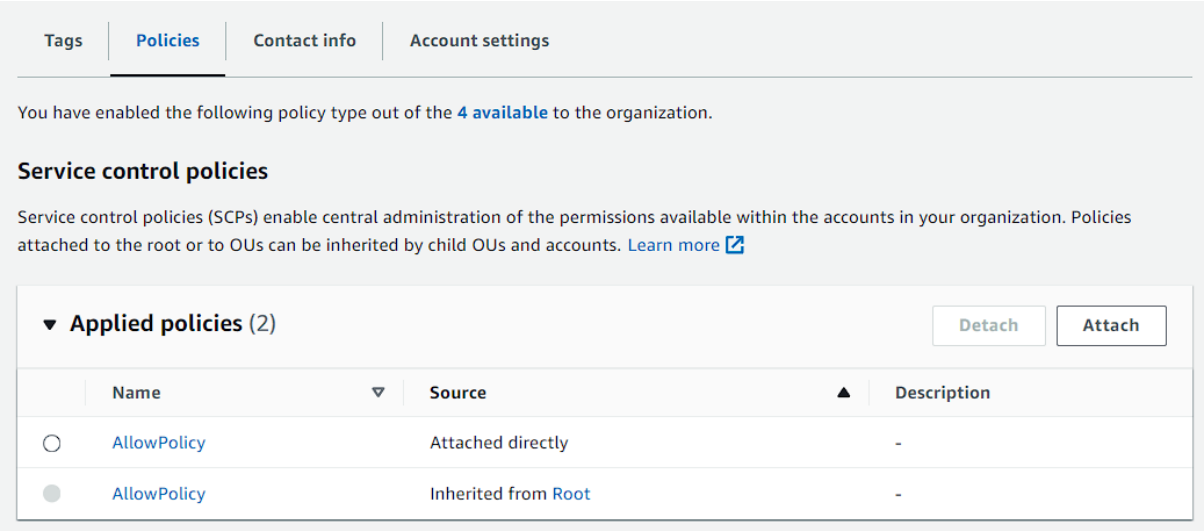


12. Plus, if you go back to member's account and open its policies you will see your allow policy which is now attach to it directly.

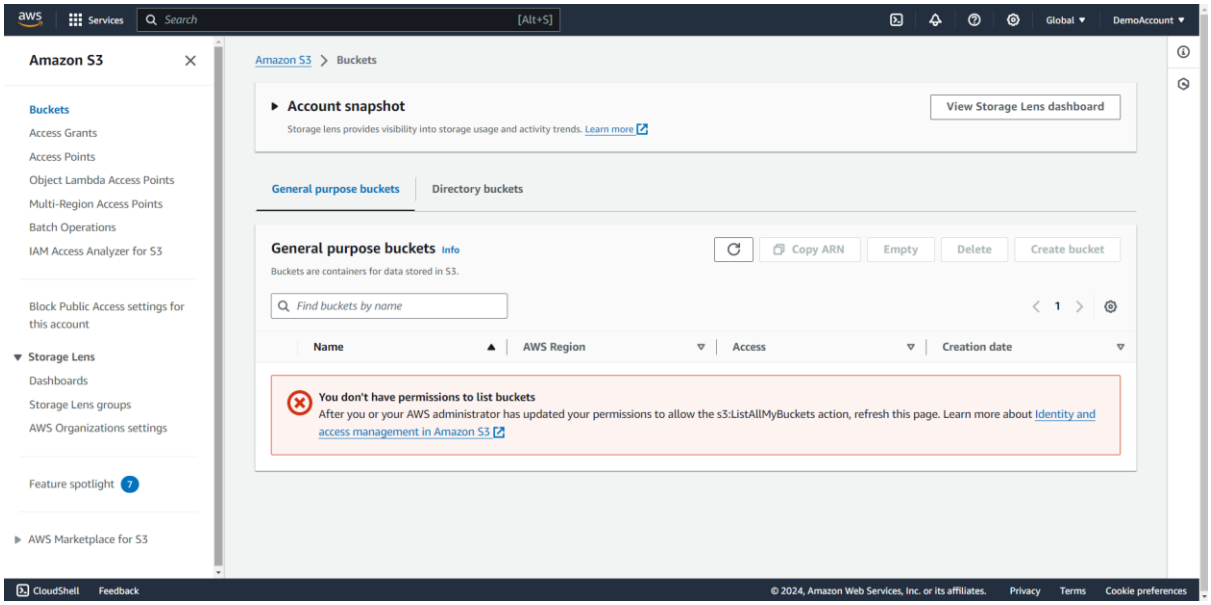


13. Now go back to policies and open your AWS full access policy and from the targets remove the member account and root from there.
14. Once this is done just reverify to check only allow policy should be attached to member account.

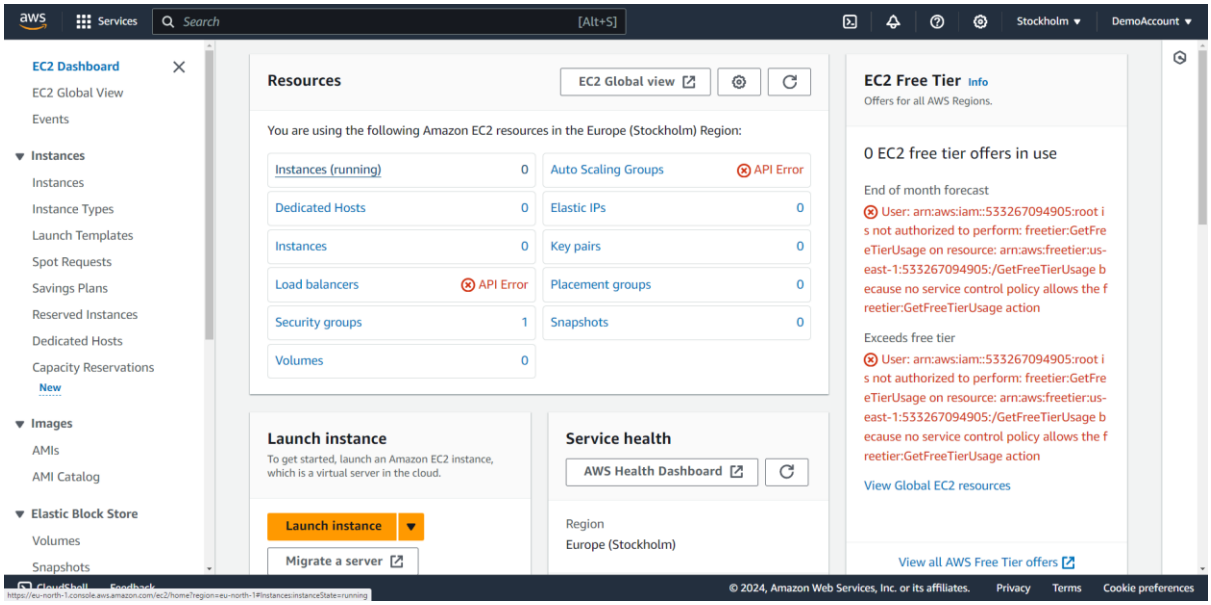


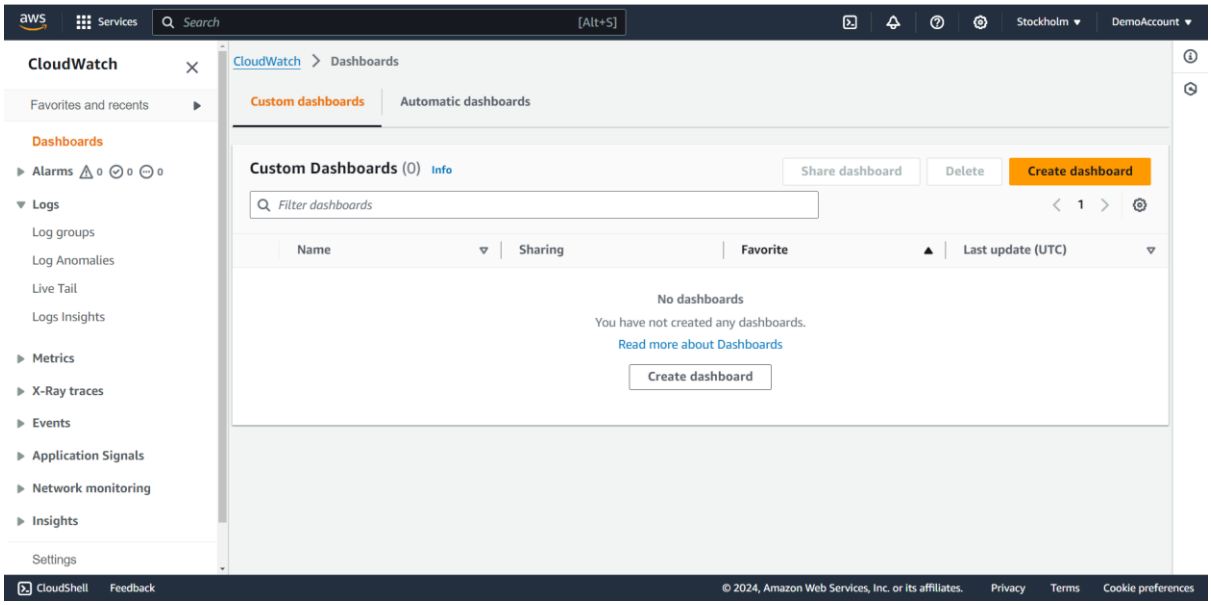


15. Now you have to login to your member account and try to visit any service other than cloud watch and EC2. You will see that you are getting permission denied.



16. But you will see that you have access to EC2 and cloud watch.




aws
Services
Search
[Alt+S]
Stockholm
DemoAccount
CloudWatch
Favorites and recents
Dashboards
Alarms 0 0 0
Logs
Log groups
Log Anomalies
Live Tail
Logs Insights
Metrics
X-Ray traces
Events
Application Signals
Network monitoring
Insights
Settings
CloudWatch > Dashboards
Custom dashboards
Automatic dashboards
Custom Dashboards (0) Info
Share dashboard
Delete
Create dashboard
Filter dashboards
1
Name
Sharing
Favorite
Last update (UTC)
No dashboards
You have not created any dashboards.
Read more about Dashboards
Create dashboard
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences