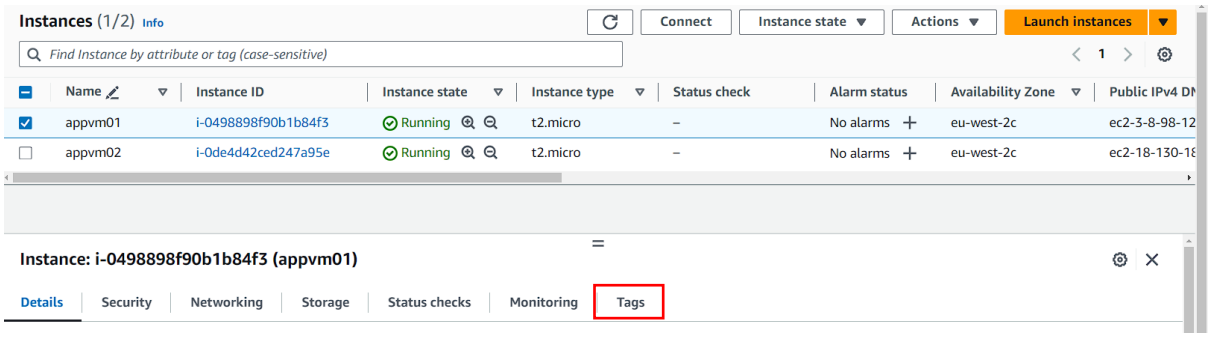
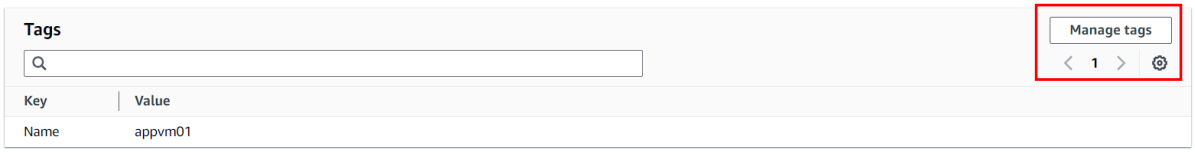
😊 IAM: Only allow permissions based on tags

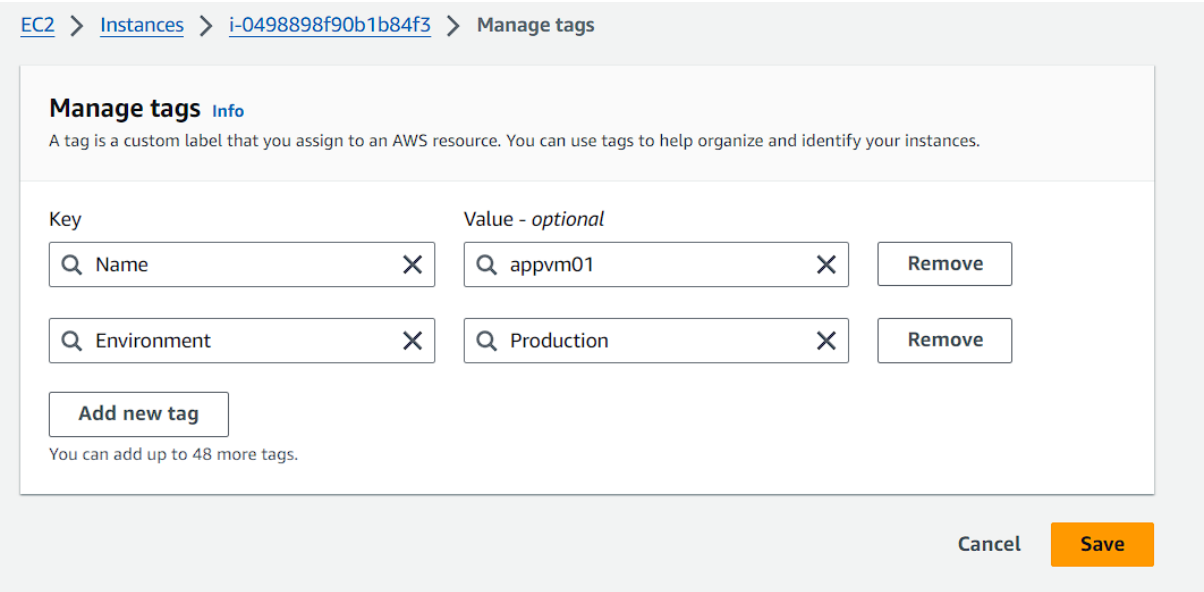
1. For this lab you are going to learn how allow permission for an EC2 instance based on tags.
2. You need to launch two EC2 instances, then you need to define tags for one of the instances.
3. For select your desired instance. Then click on tags



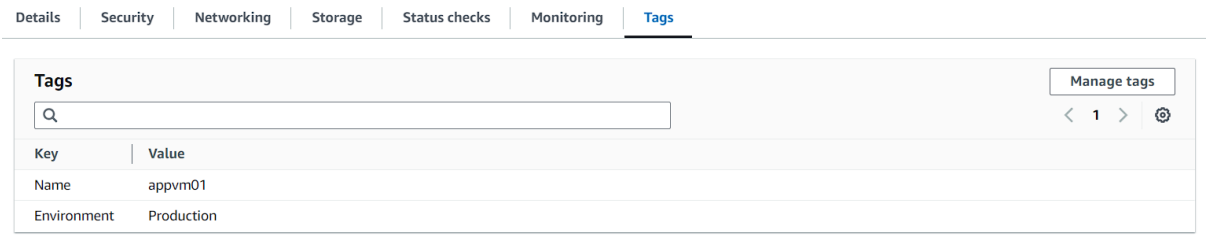
4. Now you need to define tag. For that click on manage tags.



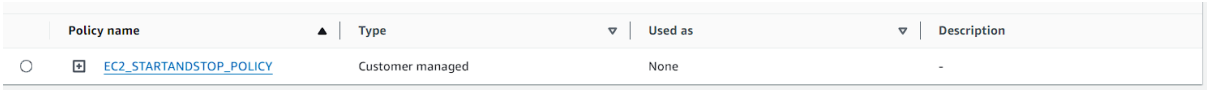
5. Now you need to click on add new tag, then write Environment in key and Production in value.
6. Then click on save.



7. Now you want to allow permission for now letting anyone start, stop or terminate the instance with tag on it.



8. For that go to IAM and then policies. Open your policy for start and stop which you created in last lab.
9. Now you need to edit the JSON code of it.

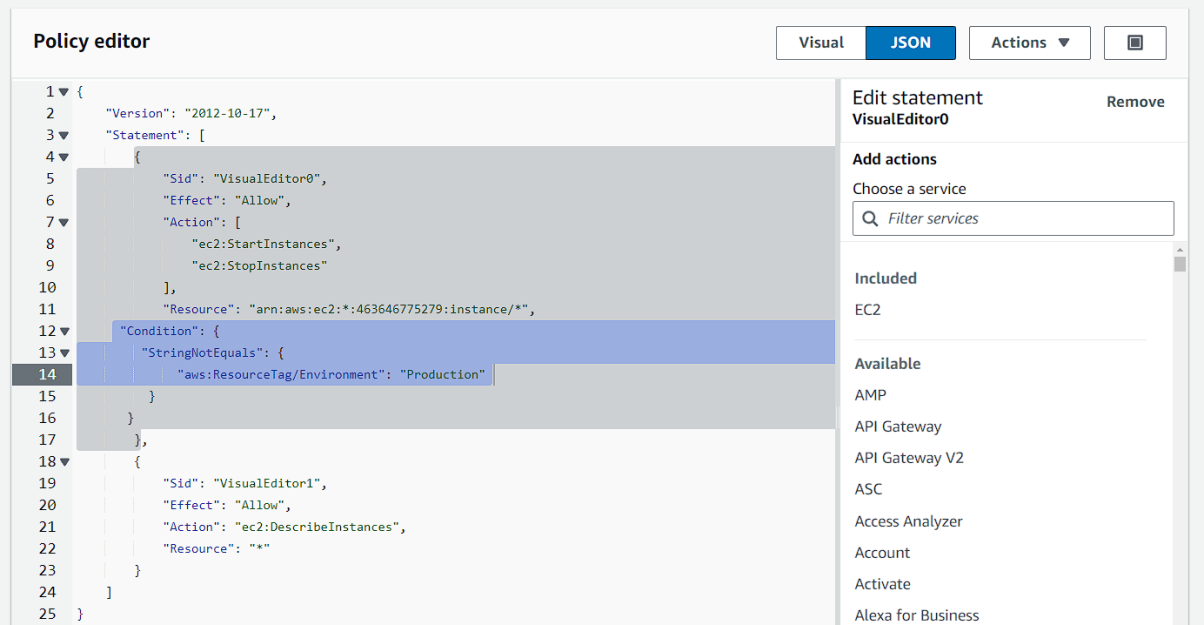


10. There you need to paste this code.

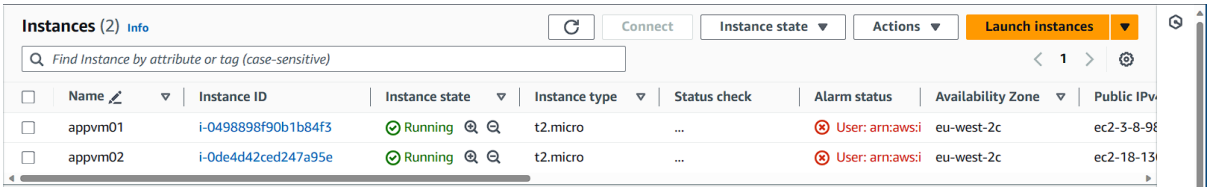
```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "ec2:StartInstances",
        "ec2:StopInstances"
      ],
      "Resource": "arn:aws:ec2:*:463646775279:instance/*",
   "Condition": {
     "StringNotEquals": {
        "aws:ResourceTag/Environment": "Production"
      }
    }
     },
     {
      "Sid": "VisualEditor1",
      "Effect": "Allow",
```

```
        "Action": "ec2:DescribeInstances",
        "Resource": "*"
    }
  ]
}
```

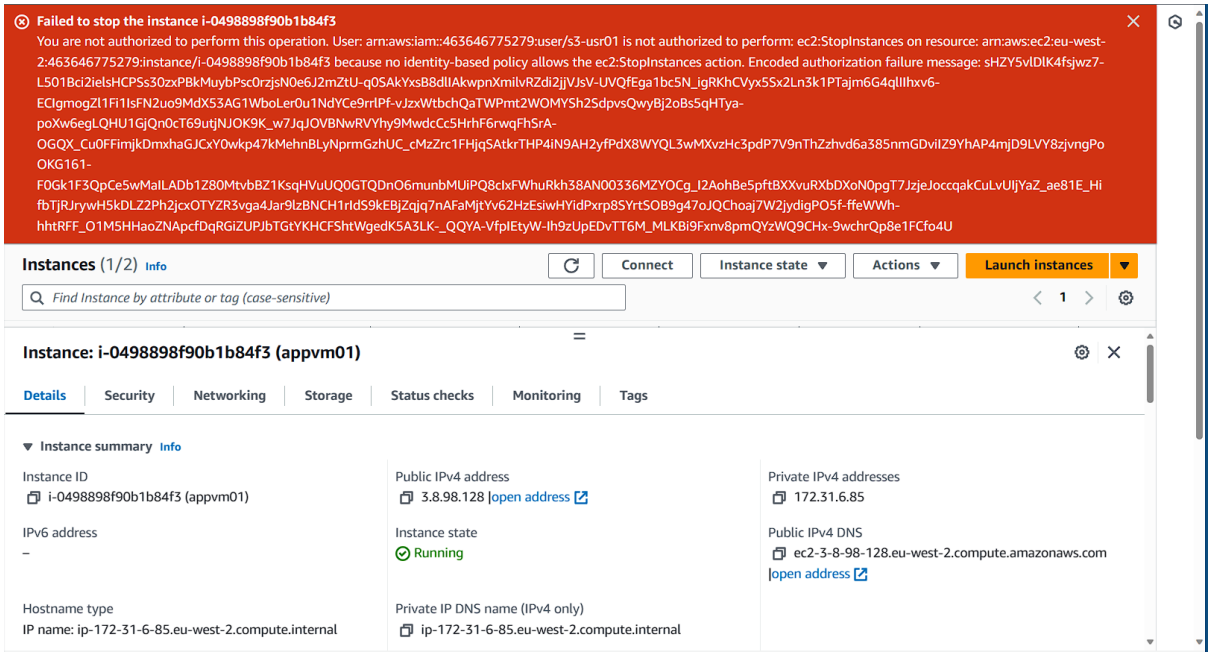
11. In this code you will see that a condition has been applied.



12. Save this policy and attach it to your instance, if not attached.
13. Once your policy is attached. Now login to a new browser with IAM user account.
14. Then navigate to EC2 instances, there you will see that your two instances are running.



15. Now if you will try to stop the instance with tag on it. Then it will refuse to stop.



16. But if you will stop the other instance with no tag, then it will get stopped.