



IAM: Only allow permissions based on tags

1. For this lab you are going to learn how to 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

The screenshot shows the AWS EC2 Instances page. There are two instances listed: 'appvm01' and 'appvm02'. Both instances are running, t2.micro type, with no alarms. They are located in eu-west-2c availability zones with public IPv4 addresses. The 'Tags' tab is highlighted with a red box at the bottom of the instance details.

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

The screenshot shows the 'Tags' section. It includes a search bar, a table with columns 'Key' and 'Value', and a single row for 'Name' with value 'appvm01'. The 'Manage tags' button is highlighted with a red box.

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

The screenshot shows the 'Manage tags' dialog box. It displays two tags: 'Name' with value 'appvm01' and 'Environment' with value 'Production'. A note says 'You can add up to 48 more tags.' At the bottom are 'Cancel' and 'Save' buttons, with 'Save' highlighted with a red box.

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

The screenshot shows the 'Tags' tab of a CloudWatch Metrics resource. It displays a table with one row containing a key 'Name' with value 'appvm01' and another row for 'Environment' with value 'Production'. A search bar at the top left and a 'Manage tags' button at the top right are also visible.

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.

The screenshot shows the 'Policies' section of the IAM console. A single policy named 'EC2_STARTANDSTOP_POLICY' is listed, showing it is a 'Customer managed' policy with no 'Used as' resources and no description.

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.

The screenshot shows the AWS IAM Policy editor interface. The policy JSON is displayed on the left, and the right side features tabs for Visual, JSON, Actions, and a preview pane. A condition block in the JSON is highlighted with a blue selection bar. The condition block contains a StringNotEquals condition on the aws:ResourceTag/Environment tag, which is set to "Production". The preview pane on the right shows the policy statement and lists available services like EC2, AMP, API Gateway, etc.

```

1 {
2     "Version": "2012-10-17",
3     "Statement": [
4         {
5             "Sid": "VisualEditor0",
6             "Effect": "Allow",
7             "Action": [
8                 "ec2:StartInstances",
9                 "ec2:StopInstances"
10            ],
11            "Resource": "arn:aws:ec2:*:463646775279:instance/*",
12            "Condition": {
13                "StringNotEquals": {
14                    "aws:ResourceTag/Environment": "Production"
15                }
16            }
17        },
18        {
19            "Sid": "VisualEditor1",
20            "Effect": "Allow",
21            "Action": "ec2:DescribeInstances",
22            "Resource": "*"
23        }
24    ]
25 }

```

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.

The screenshot shows the AWS EC2 Instances page. It displays two instances: appvm01 and appvm02. Both instances are listed as "Running" and have the t2.micro instance type. They are located in eu-west-2c availability zones and have public IPv4 addresses ec2-3-8-96 and ec2-18-131 respectively.

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IP
appvm01	i-0498898f90b1b84f3	Running	t2.micro	...	User: arn:aws:	eu-west-2c	ec2-3-8-96
appvm02	i-0de4d42ced247a95e	Running	t2.micro	...	User: arn:aws:	eu-west-2c	ec2-18-131

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

Failed to stop the instance i-0498898f90b1b84f3

You are not authorized to perform this operation. User: arn:aws:iam::463646775279:user/s3-usr01 is not authorized to perform: ec2:StopInstances on resource: arn:aws:ec2:eu-west-2:463646775279:instance/i-0498898f90b1b84f3 because no identity-based policy allows the ec2:StopInstances action. Encoded authorization failure message: sHZY5vIDK4fsjwz7-LS01Bc2ielsHCPs30zxPbkMuybPscDrjsN0e6J2m2tU-q0SAKYxsB8dIiAkwpnXmlvRZdi2jJVjv-UVQfEga1bc5N_igRKhCVyx5Sx2Ln3k1PTajm6G4qlIIhxv6-EClgmogZ11F1lsfN2uo9MdX53AG1Wb0Ler0u1NdCe9rlPf-vJxWtbcnQaTWPmt2WOMYSsh25dpvsQwyBj2oBs5qHTya-poXw6egLQHUT1GQn0cT69utNJOK9K_w7JqJOVBNwRVYhy9Mwdcc5HrhF6rwqFhSrA-OGOX_Cu0FFimjkDmxhaGJx0wkp47KMehnBlyNprmGzhUC_cmZrc1FHjq5AtkrTHP4IN9AH2yfPdX8WYQL3wMXvzHc3pdP7V9nThZzhvd6a385nmGDvifZ9YhAP4mjD9LVY8zjvngPoOKG161-F0GK1F3QpCe5wMaILAbdB1Z80MtvbBZ1KsqHVuUQ0GTQDnO6munbMUIPQ8clxFWhuRkh38AN00336MZYOCg_I2AhBe5pftBXvuRXbDxoN0pgT7JzjeJoccqakCuLvUljYaZ_ae81E_HifbTjRJrywH5kDLZ2Ph2jcxOTYZR3vga4Jar9lzBNCH1rdS9kEBjZqjg7nAFaMjtYv62HzEsiwHYidPxpr85YrtSOB9g47oJQChoaj7W2jydigPO5f-ffeWWh-hhtRFF_O1M5HHAoZNApclfDqRGIZUPJbTGtYKHCFShWgedk5A3LK_QQYA-VfpIEtyW-ih9zUpEdvTT6M_MLKBi9Fxnv8pmQyzWQ9Chx-9wchrQp8e1Fc04U

Instances (1/2) Info

Find Instance by attribute or tag (case-sensitive)

Instance: i-0498898f90b1b84f3 (appvm01)

Details | Security | Networking | Storage | Status checks | Monitoring | Tags

Instance summary

Instance ID i-0498898f90b1b84f3 (appvm01)	Public IPv4 address 3.8.98.128 [open address]	Private IPv4 addresses 172.31.6.85
IPv6 address -	Instance state Running	Public IPv4 DNS ec2-3-8-98-128.eu-west-2.compute.amazonaws.com [open address]
Hostname type IP name: ip-172-31-6-85.eu-west-2.compute.internal	Private IP DNS name (IPv4 only) ip-172-31-6-85.eu-west-2.compute.internal	

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

Successfully stopped i-0de4d42ced247a95e

Instances (1/2) Info

Find Instance by attribute or tag (case-sensitive)

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4
appvm01	i-0498898f90b1b84f3	Running	t2.micro	✖ You are not auth	✖ User: arn:aws:si	eu-west-2c	ec2-3-8-98
appvm02	i-0de4d42ced247a95e	Stopping	t2.micro	✖ You are not auth	✖ User: arn:aws:si	eu-west-2c	ec2-18-13