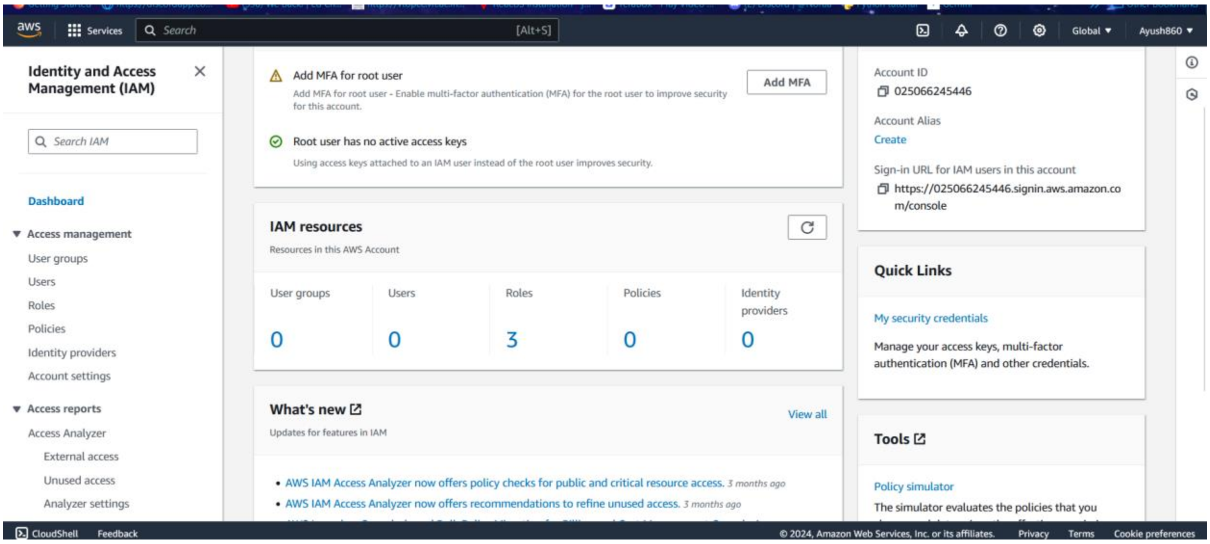
Ayush Raj

22BRS1117

Creating an Iam role and policy for a user using Jason script

First search for iam in the search bar



Add MFA for root user
Add MFA for root user - Enable multi-factor authentication (MFA) for the root user to improve security for this account.

Root user has no active access keys
Using access keys attached to an IAM user instead of the root user improves security.

Account ID
025066245446

Account Alias
Create

Sign-in URL for IAM users in this account
https://025066245446.signin.aws.amazon.com/console

IAM resources
Resources in this AWS Account

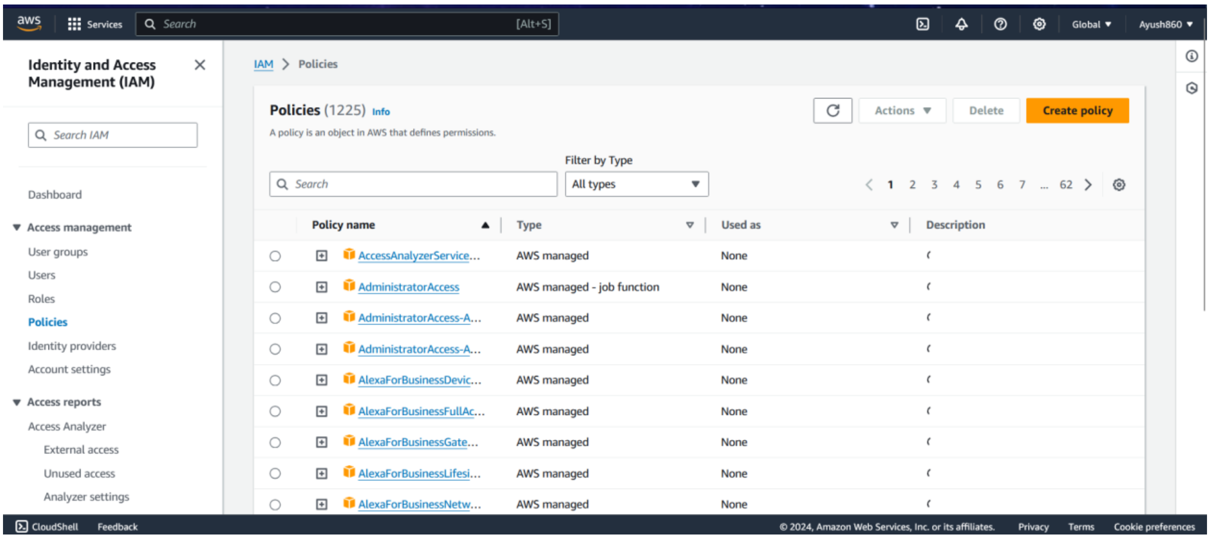
User groups	Users	Roles	Policies	Identity providers
0	0	3	0	0

Quick Links
My security credentials
Manage your access keys, multi-factor authentication (MFA) and other credentials.

What's new
Updates for features in IAM
- AWS IAM Access Analyzer now offers policy checks for public and critical resource access. 3 months ago
- AWS IAM Access Analyzer now offers recommendations to refine unused access. 3 months ago

Tools
Policy simulator
The simulator evaluates the policies that you

Click on policies

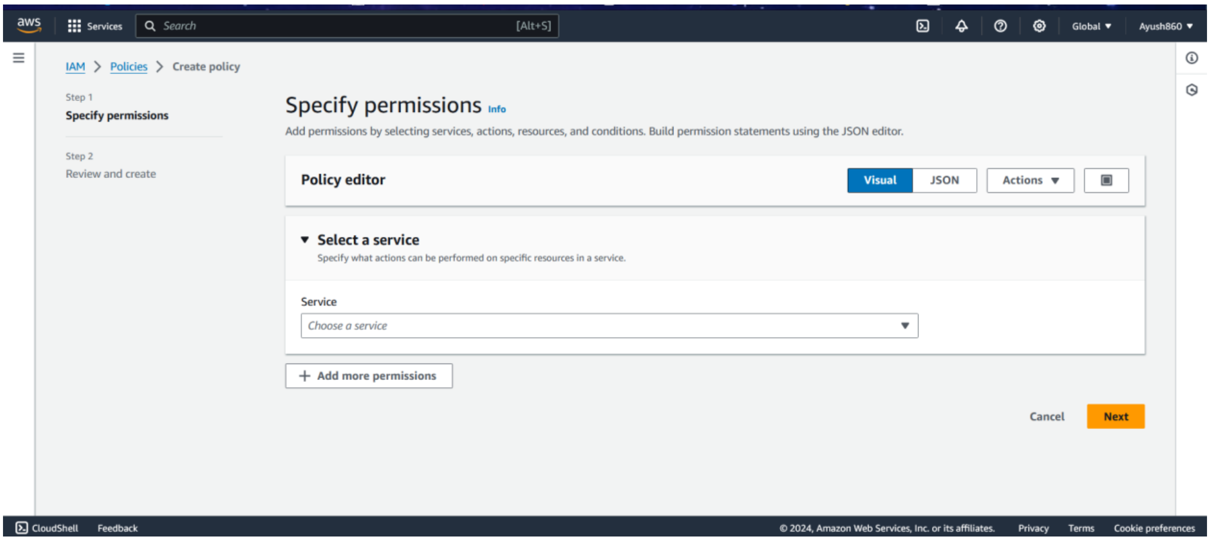


Policies (1225) Info
A policy is an object in AWS that defines permissions.

Filter by Type
All types

	Policy name	Type	Used as	Description
○	AccessAnalyzerService...	AWS managed	None	(
○	AdministratorAccess	AWS managed - job function	None	(
○	AdministratorAccess-A...	AWS managed	None	(
○	AdministratorAccess-A...	AWS managed	None	(
○	AlexaForBusinessDevic...	AWS managed	None	(
○	AlexaForBusinessFullAc...	AWS managed	None	(
○	AlexaForBusinessGate...	AWS managed	None	(
○	AlexaForBusinessLifesi...	AWS managed	None	(
○	AlexaForBusinessNetw...	AWS managed	None	(

Click on create policy



Step 1
Specify permissions

Step 2
Review and create

Specify permissions Info

Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.

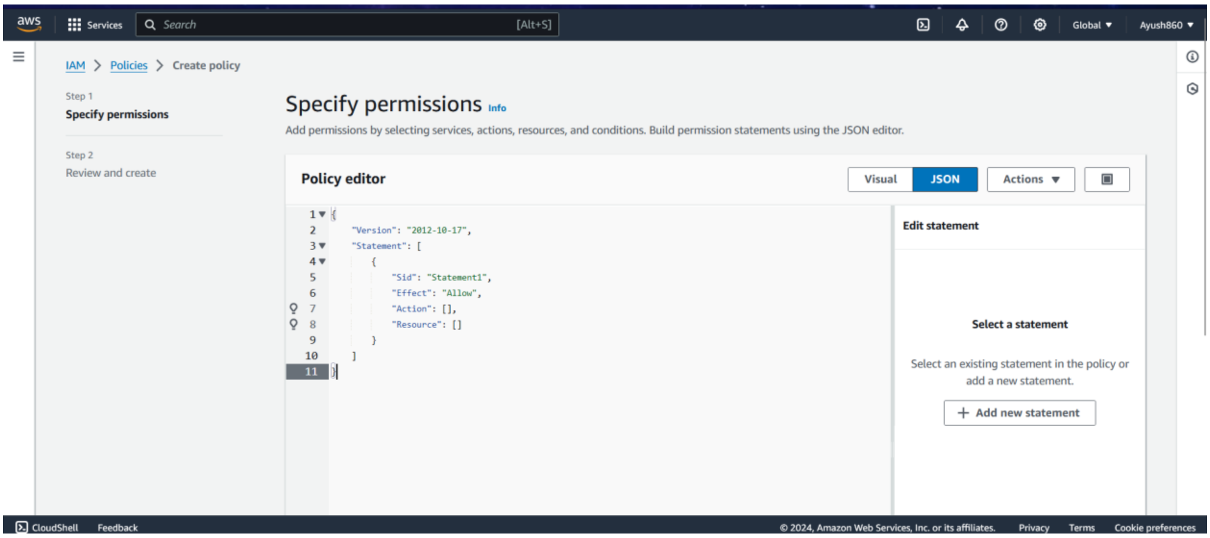
Policy editor

Select a service

Specify what actions can be performed on specific resources in a service.

Service: Choose a service

Choose Json



Step 1
Specify permissions

Step 2
Review and create

Specify permissions Info

Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.

Policy editor

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Statement1",
            "Effect": "Allow",
            "Action": [],
            "Resource": []
        }
    ]
}
```

Edit statement

Select a statement

Select an existing statement in the policy or add a new statement.

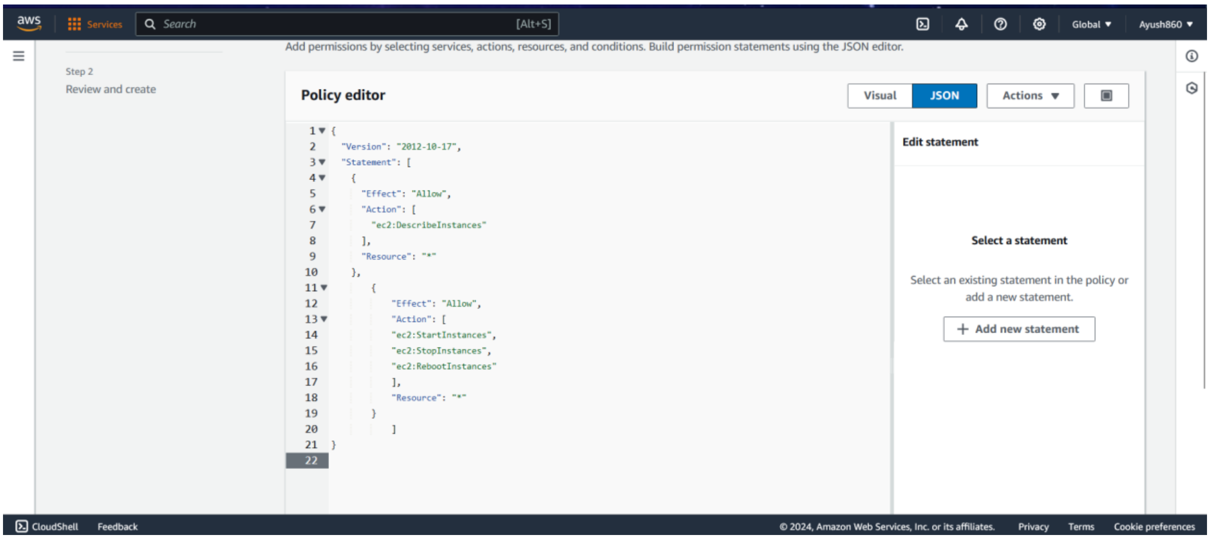
Write a Json script for allowing start and stop instance by a user

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeTags"
      ],
      "Resource": "arn:aws:ec2:us-east-
1:0123456789:instance/i-001122334455"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:RebootInstances"
      ],
      "Resource": "arn:aws:ec2:us-east-
1:0123456789:instance/i-001122334455"
```

This part means the account no 0123456789 and the region of that account

```
    }
  ]
}
```

Check for any errors , a cross sign will appear if there is a syntax error



Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.

Step 2
Review and create

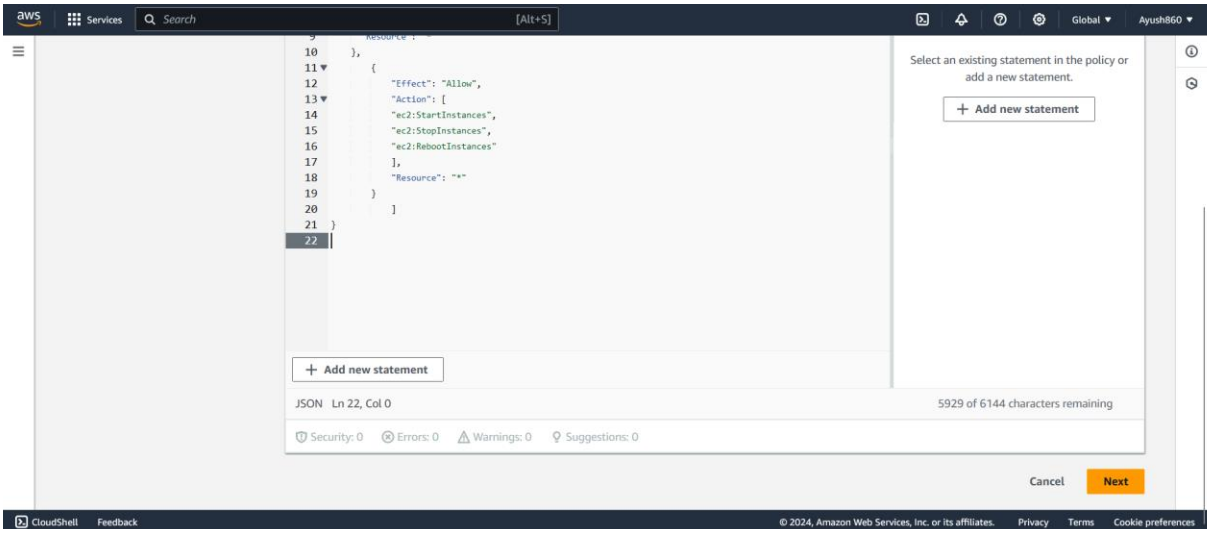
Policy editor

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

Edit statement

Select a statement

Select an existing statement in the policy or add a new statement.



```
    },
      {
          "Effect": "Allow",
          "Action": [
          "ec2:StartInstances",
          "ec2:StopInstances",
          "ec2:RebootInstances"
          ],
          "Resource": "*"
      }
          ]
}
```

Select an existing statement in the policy or add a new statement.

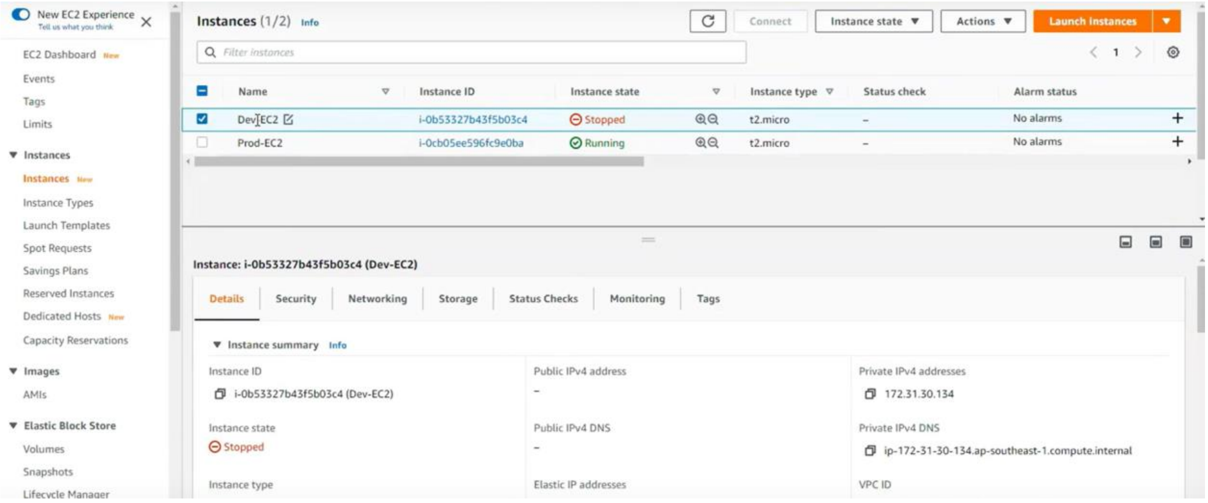
JSON Ln 22, Col 0

5929 of 6144 characters remaining

Security: 0 Errors: 0 Warnings: 0 Suggestions: 0

Click next

Choose the instance



Instances (1/2) Info

☑	Name	Instance ID	Instance state	Instance type	Status check	Alarm status
☑	Dev-EC2	i-0b53327b43f5b03c4	Stopped	t2.micro	–	No alarms
□	Prod-EC2	i-0cb05ee596fc9e0ba	Running	t2.micro	–	No alarms

Instance: i-0b53327b43f5b03c4 (Dev-EC2)

Instance summary Info

Instance ID: i-0b53327b43f5b03c4 (Dev-EC2)

Public IPv4 address: –

Private IPv4 addresses: 172.31.30.134

Instance state: Stopped

Public IPv4 DNS: –

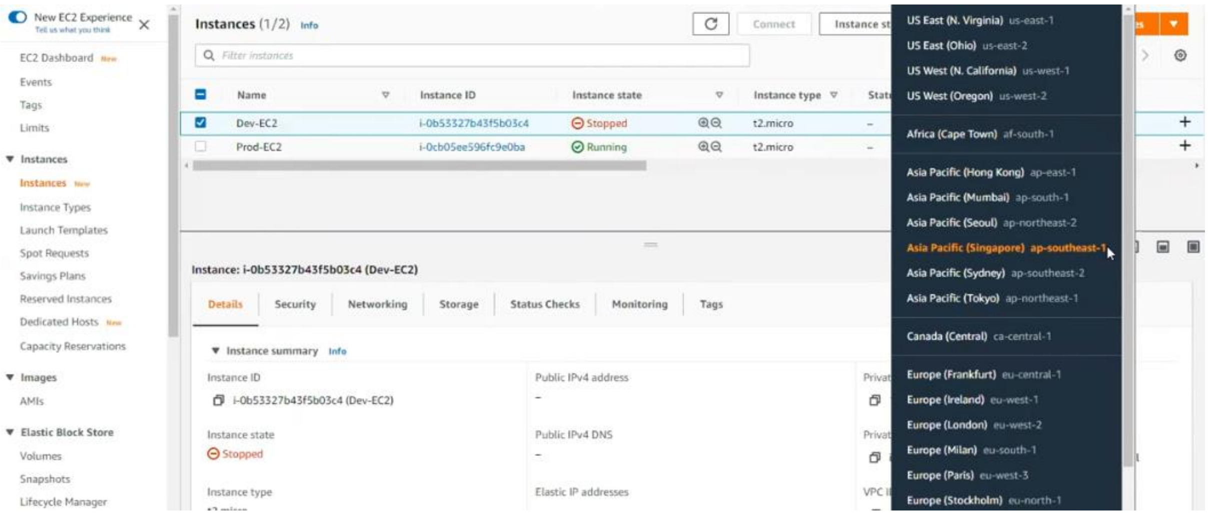
Private IPv4 DNS: ip-172-31-30-134.ap-southeast-1.compute.internal

Instance type

Elastic IP addresses

VPC ID

Check the region where the instance is


New EC2 Experience
Tell us what you think
EC2 Dashboard New
Events
Tags
Limits
Instances
Instances New
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts New
Capacity Reservations
Images
AMIs
Elastic Block Store
Volumes
Snapshots
Lifecycle Manager
Connect
Instance st
Filter instances
US East (N. Virginia) us-east-1
US East (Ohio) us-east-2
US West (N. California) us-west-1
US West (Oregon) us-west-2
Africa (Cape Town) af-south-1
Asia Pacific (Hong Kong) ap-east-1
Asia Pacific (Mumbai) ap-south-1
Asia Pacific (Seoul) ap-northeast-2
Asia Pacific (Singapore) ap-southeast-1
Asia Pacific (Sydney) ap-southeast-2
Asia Pacific (Tokyo) ap-northeast-1
Canada (Central) ca-central-1
Europe (Frankfurt) eu-central-1
Europe (Ireland) eu-west-1
Europe (London) eu-west-2
Europe (Milan) eu-south-1
Europe (Paris) eu-west-3
Europe (Stockholm) eu-north-1
Details
Security
Networking
Storage
Status Checks
Monitoring
Tags

Instances (1/2) Info

☑	Name	Instance ID	Instance state	Instance type	Stat
☑	Dev-EC2	i-0b53327b43f5b03c4	Stopped	t2.micro	–
□	Prod-EC2	i-0cb05ee596fc9e0ba	Running	t2.micro	–

Instance: i-0b53327b43f5b03c4 (Dev-EC2)

Instance summary Info

Instance ID: i-0b53327b43f5b03c4 (Dev-EC2)

Public IPv4 address: –

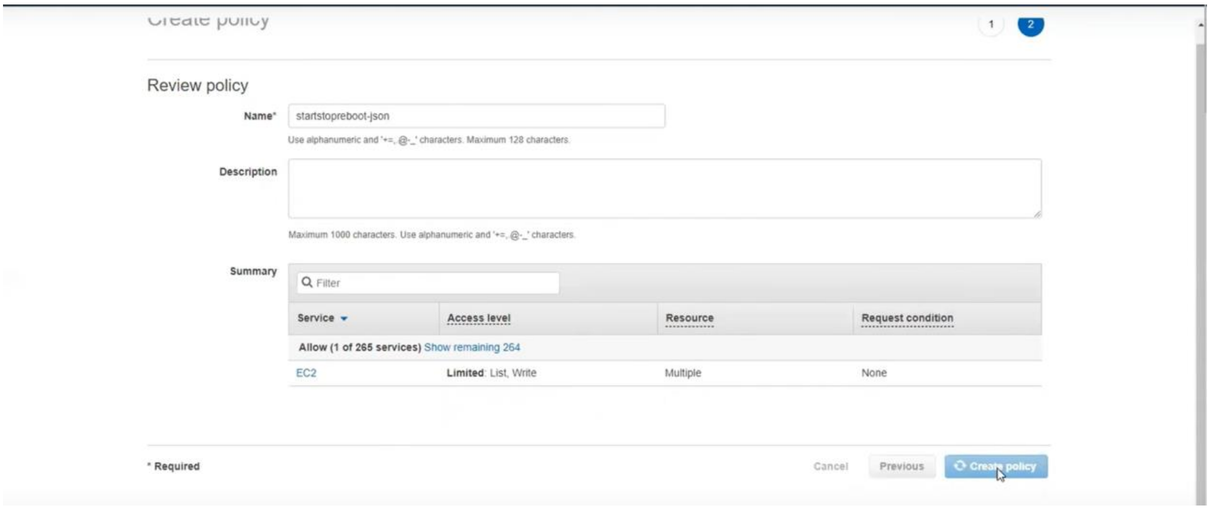
Instance state: Stopped

Public IPv4 DNS: –

Instance type

Elastic IP addresses

Review the policy and allow user



Review policy

Name* startstopreboot-json

Use alphanumeric and '+=,.@-_' characters. Maximum 128 characters.

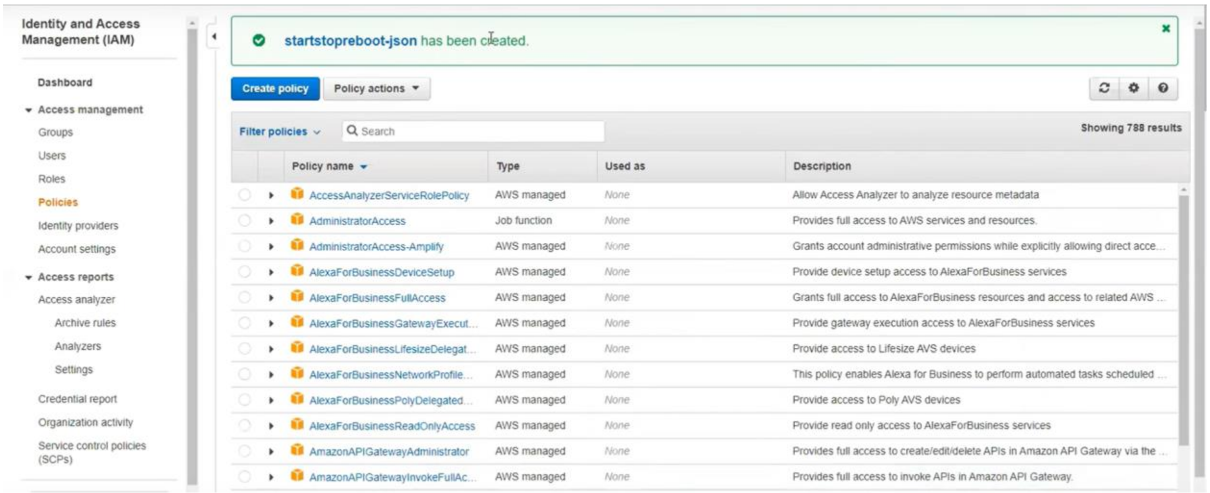
Description

Maximum 1000 characters. Use alphanumeric and '+=,.@-_' characters.

Summary

Service	Access level	Resource	Request condition
Allow (1 of 265 services) Show remaining 264			
EC2	Limited: List, Write	Multiple	None

We can see that the startstopreboot-json has been created

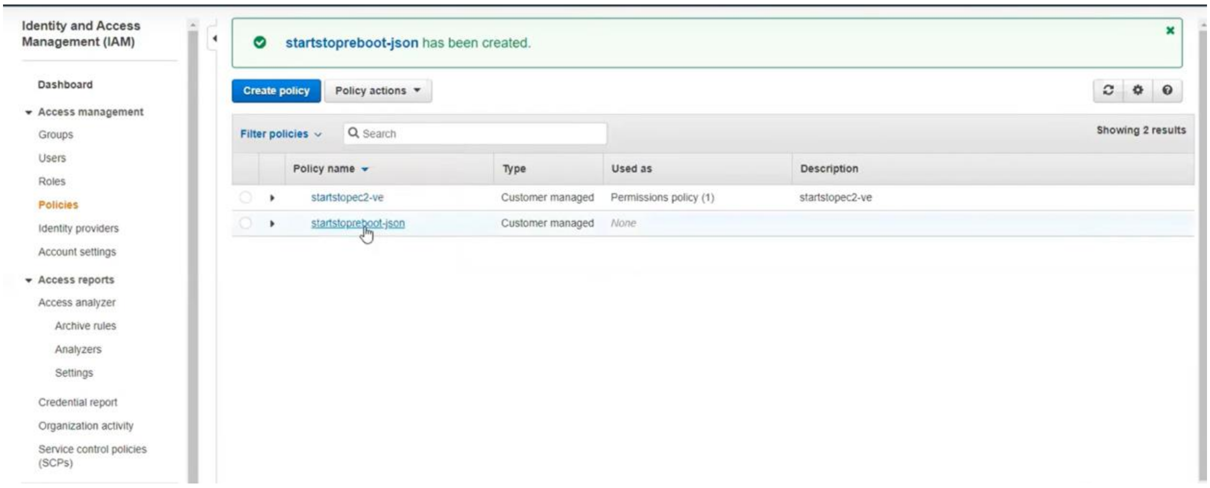


startstopreboot-json has been created.

Showing 788 results

Policy name	Type	Used as	Description
AccessAnalyzerServiceRolePolicy	AWS managed	None	Allow Access Analyzer to analyze resource metadata
AdministratorAccess	Job function	None	Provides full access to AWS services and resources.
AdministratorAccess-Amplify	AWS managed	None	Grants account administrative permissions while explicitly allowing direct acce...
AlexaForBusinessDeviceSetup	AWS managed	None	Provide device setup access to AlexaForBusiness services
AlexaForBusinessFullAccess	AWS managed	None	Grants full access to AlexaForBusiness resources and access to related AWS ...
AlexaForBusinessGatewayExecut...	AWS managed	None	Provide gateway execution access to AlexaForBusiness services
AlexaForBusinessLifesizeDelegat...	AWS managed	None	Provide access to Lifesize AVS devices
AlexaForBusinessNetworkProfile...	AWS managed	None	This policy enables Alexa for Business to perform automated tasks scheduled ...
AlexaForBusinessPolyDelegated...	AWS managed	None	Provide access to Poly AVS devices
AlexaForBusinessReadOnlyAccess	AWS managed	None	Provide read only access to AlexaForBusiness services
AmazonAPIGatewayAdministrator	AWS managed	None	Provides full access to create/edit/delete APIs in Amazon API Gateway via the ...
AmazonAPIGatewayInvokeFullAc...	AWS managed	None	Provides full access to invoke APIs in Amazon API Gateway.

We can check the policy that has been created



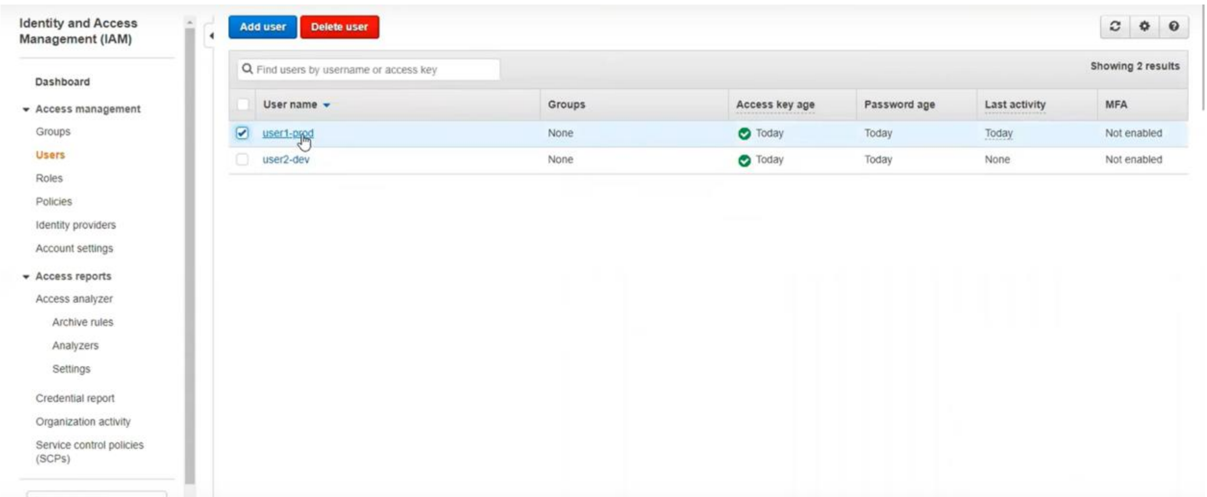
startstopreboot-json has been created.

Showing 2 results

Policy name	Type	Used as	Description
startstopec2-ve	Customer managed	Permissions policy (1)	startstopec2-ve
startstopreboot-json	Customer managed	None	

Allow the user add or create a user

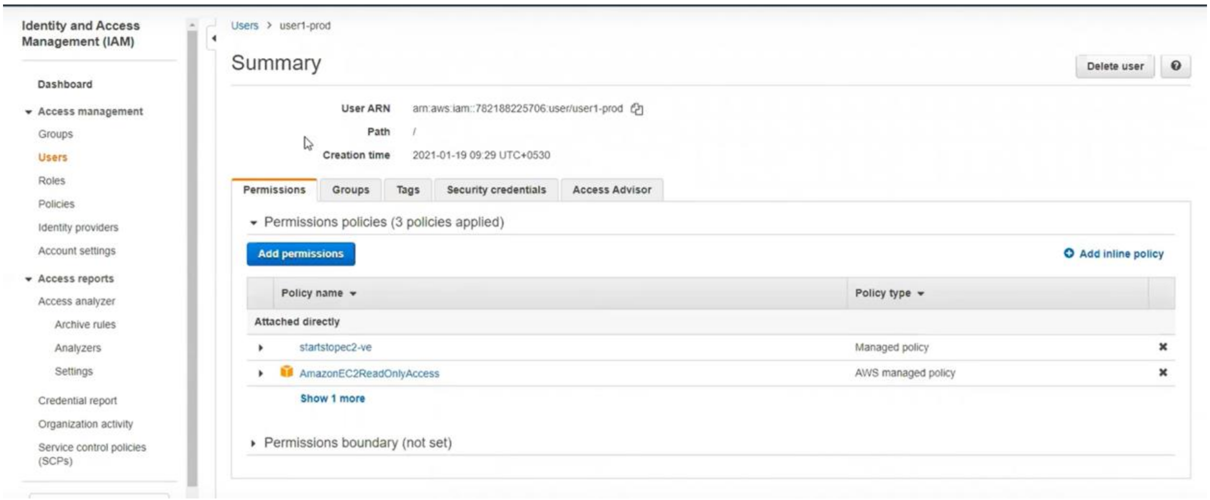
Since I already created a user we can see



Showing 2 results

	User name	Groups	Access key age	Password age	Last activity	MFA
☑	user1-prod	None	✓ Today	Today	Today	Not enabled
□	user2-dev	None	✓ Today	Today	None	Not enabled

Add permisions and policy



Summary

User ARN arn:aws:iam::782188225706:user/user1-prod

Path /

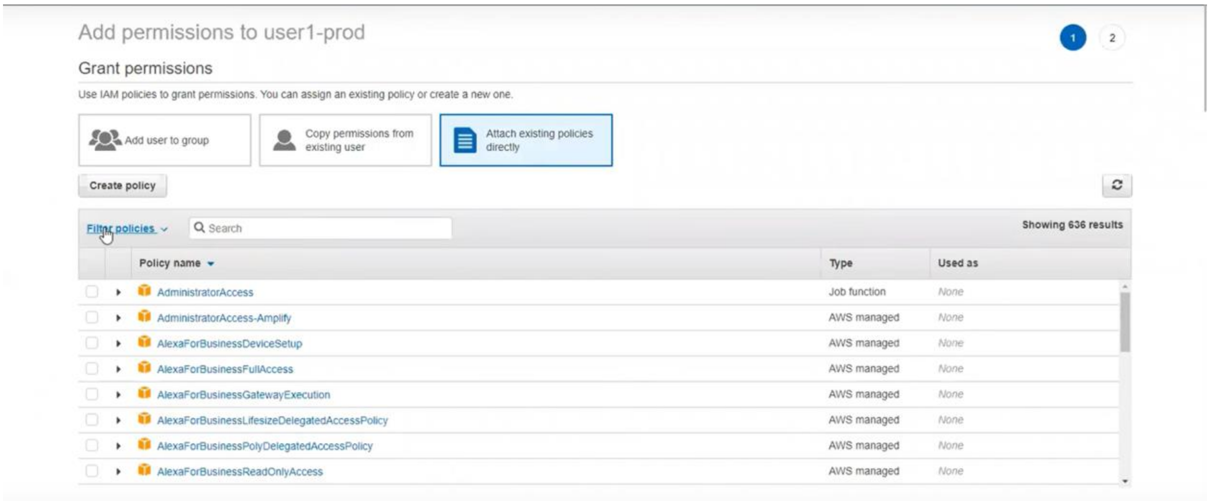
Creation time 2021-01-19 09:29 UTC+0530

Permissions policies (3 policies applied)

Policy name	Policy type
Attached directly	
startstopec2-ve	Managed policy
AmazonEC2ReadOnlyAccess	AWS managed policy

Permissions boundary (not set)

Grant permissions and attach existing policy directly option since we have a json file


1
2
Add user to group
Copy permissions from existing user
Attach existing policies directly
Create policy
Filter policies
Search

Add permissions to user1-prod

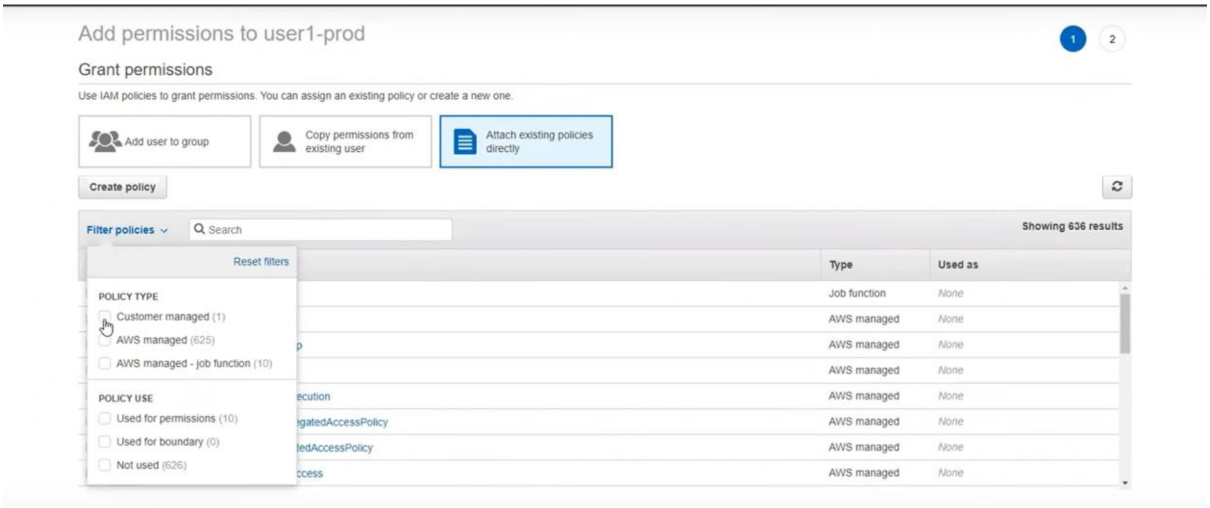
Grant permissions

Use IAM policies to grant permissions. You can assign an existing policy or create a new one.

Showing 636 results

	Policy name	Type	Used as
□	AdministratorAccess	Job function	None
□	AdministratorAccess-Amplify	AWS managed	None
□	AlexaForBusinessDeviceSetup	AWS managed	None
□	AlexaForBusinessFullAccess	AWS managed	None
□	AlexaForBusinessGatewayExecution	AWS managed	None
□	AlexaForBusinessLifesizeDelegatedAccessPolicy	AWS managed	None
□	AlexaForBusinessPolyDelegatedAccessPolicy	AWS managed	None
□	AlexaForBusinessReadOnlyAccess	AWS managed	None

Choose custom managed policy



Add permissions to user1-prod

Grant permissions

Use IAM policies to grant permissions. You can assign an existing policy or create a new one.

Add user to group
Copy permissions from existing user
Attach existing policies directly
Create policy
Filter policies
Search

Showing 636 results

POLICY TYPE

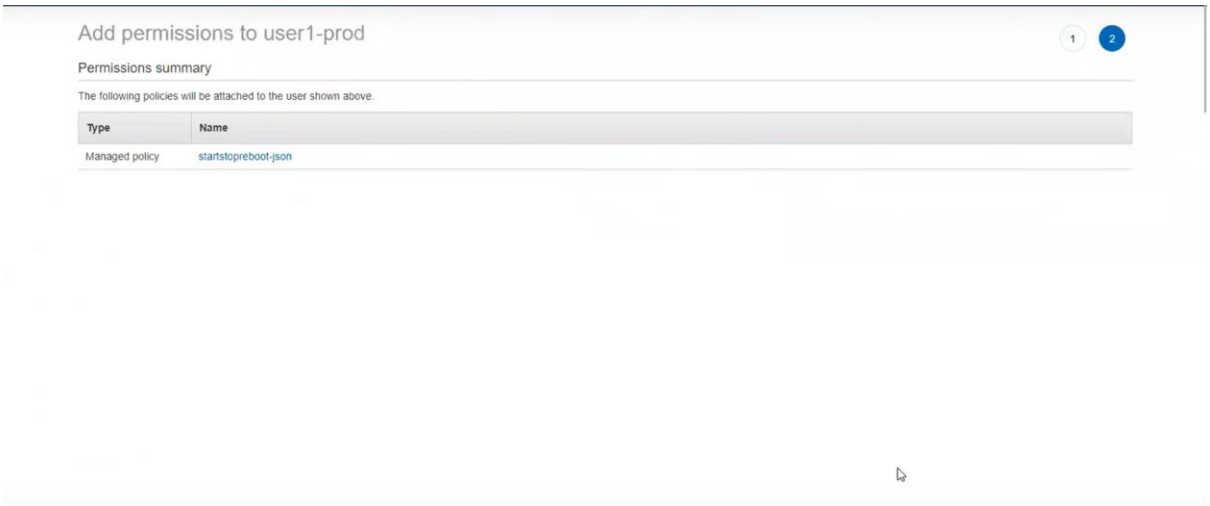
- □ Customer managed (1)
- □ AWS managed (625)
- □ AWS managed - job function (10)

POLICY USE

- □ Used for permissions (10)
- □ Used for boundary (0)
- □ Not used (626)

	Type	Used as
	Job function	None
	AWS managed	None
p	AWS managed	None
	AWS managed	None
ecution	AWS managed	None
gatedAccessPolicy	AWS managed	None
tedAccessPolicy	AWS managed	None
ccess	AWS managed	None

Select our Already existing policy on this user



Add permissions to user1-prod

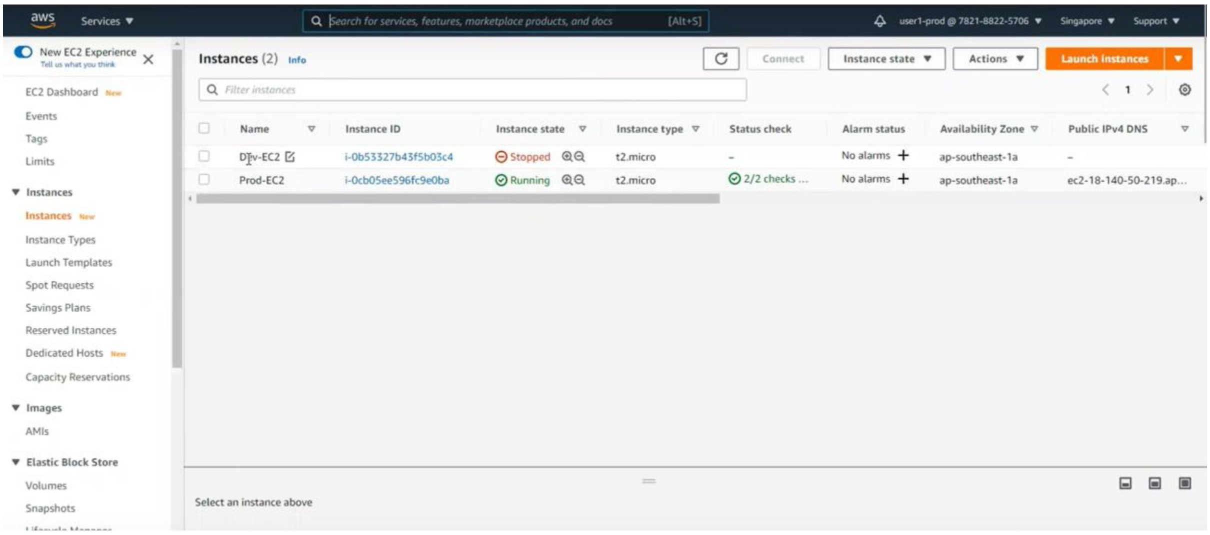
Permissions summary

The following policies will be attached to the user shown above.

Type	Name
Managed policy	startstopreboot-json

Now we will verify if it is working or not

We see that the instance can be started and stopped using this user

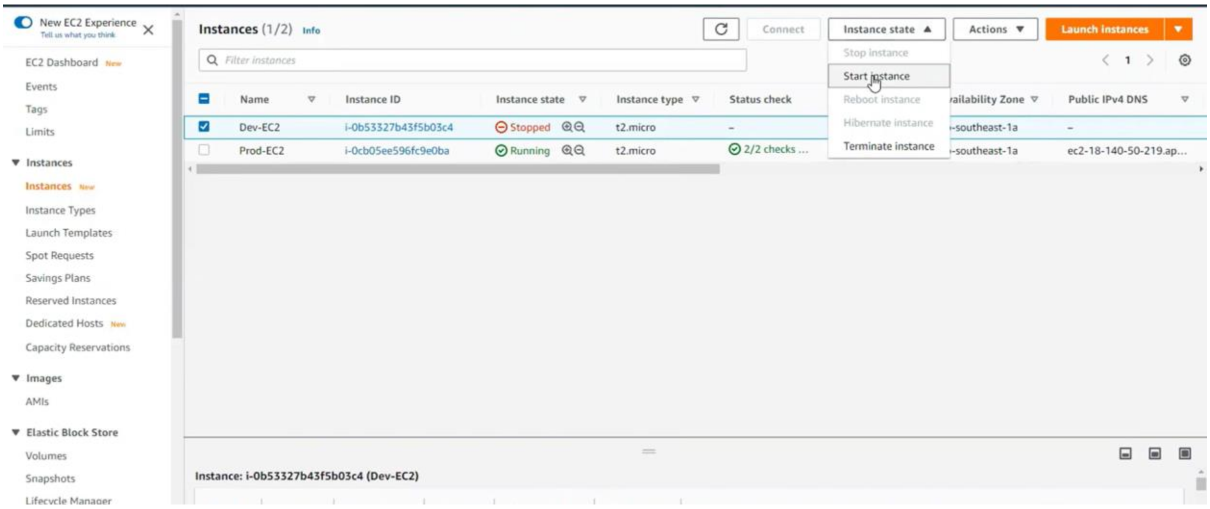


Instances (2) Info

□	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
□	Dev-EC2	i-0b53327b43f5b03c4	Stopped	t2.micro	–	No alarms +	ap-southeast-1a	–
□	Prod-EC2	i-0cb05ee596fc9e0ba	Running	t2.micro	2/2 checks ...	No alarms +	ap-southeast-1a	ec2-18-140-50-219.ap...

Select an instance above

Click on instance state

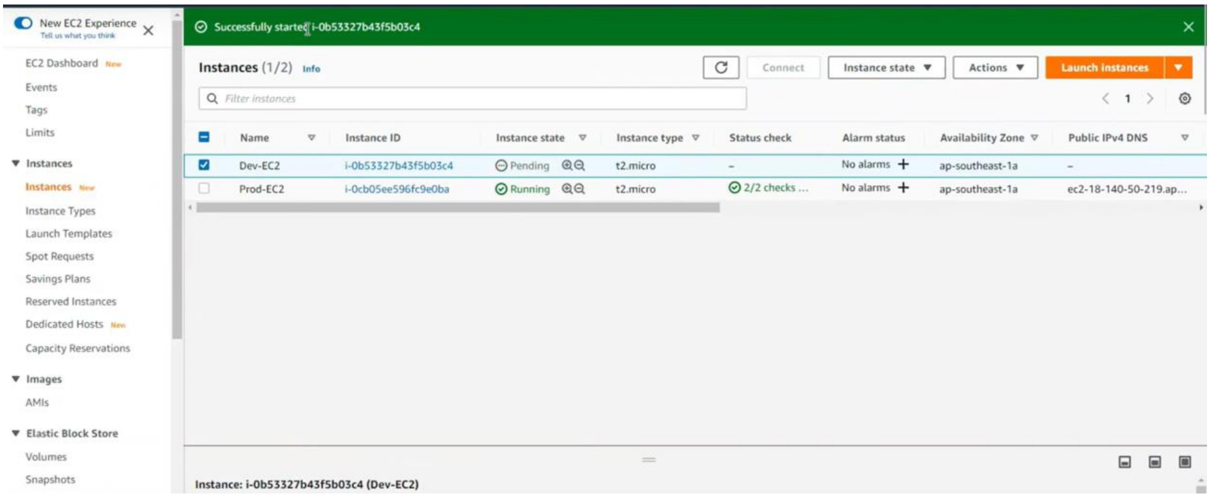


Instances (1/2) Info

☑	Name	Instance ID	Instance state	Instance type	Status check	vailability Zone	Public IPv4 DNS
☑	Dev-EC2	i-0b53327b43f5b03c4	Stopped	t2.micro	–	-southeast-1a	–
□	Prod-EC2	i-0cb05ee596fc9e0ba	Running	t2.micro	2/2 checks ...	-southeast-1a	ec2-18-140-50-219.ap...

Instance: i-0b53327b43f5b03c4 (Dev-EC2)

Successfully started instance



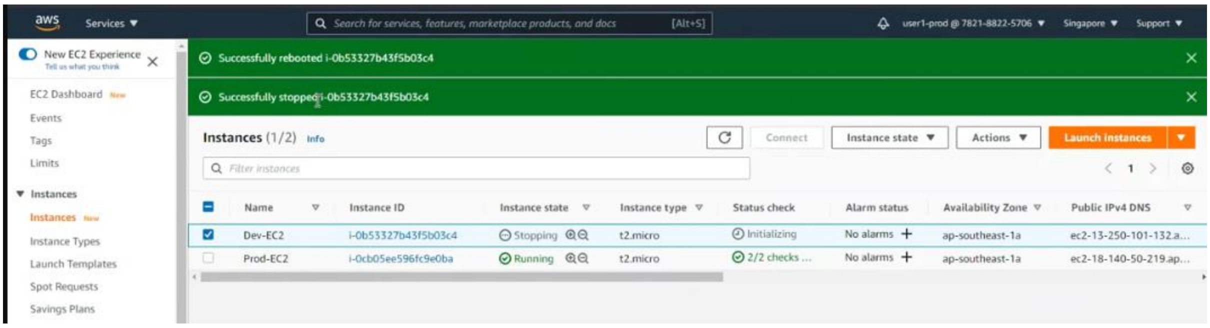
Successfully started i-0b53327b43f5b03c4

Instances (1/2) Info

☑	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
☑	Dev-EC2	i-0b53327b43f5b03c4	Pending	t2.micro	–	No alarms +	ap-southeast-1a	–
□	Prod-EC2	i-0cb05ee596fc9e0ba	Running	t2.micro	2/2 checks ...	No alarms +	ap-southeast-1a	ec2-18-140-50-219.ap...

Instance: i-0b53327b43f5b03c4 (Dev-EC2)

Successfully stopped instance



Successfully rebooted i-0b53327b43f5b03c4

Successfully stopped i-0b53327b43f5b03c4

Instances (1/2) Info

	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
☑	Dev-EC2	i-0b53327b43f5b03c4	Stopping	t2.micro	Initializing	No alarms +	ap-southeast-1a	ec2-13-250-101-132.a...
□	Prod-EC2	i-0cb05ee596fc9e0ba	Running	t2.micro	2/2 checks ...	No alarms +	ap-southeast-1a	ec2-18-140-50-219.ap...

Now we can change the Json file script to this

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

this will not allow starting of instance for this user