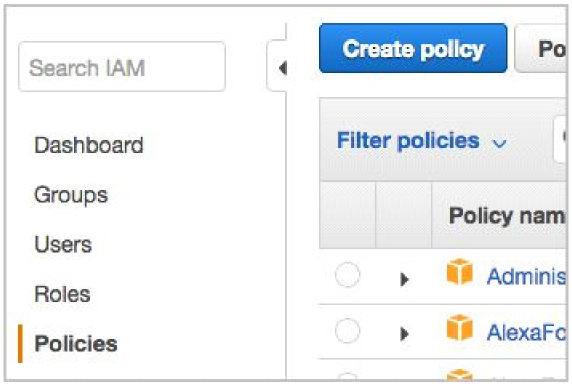
Create IAM policies

1.1 Create policy named ec2read

This policy allows read only permissions with a region condition.

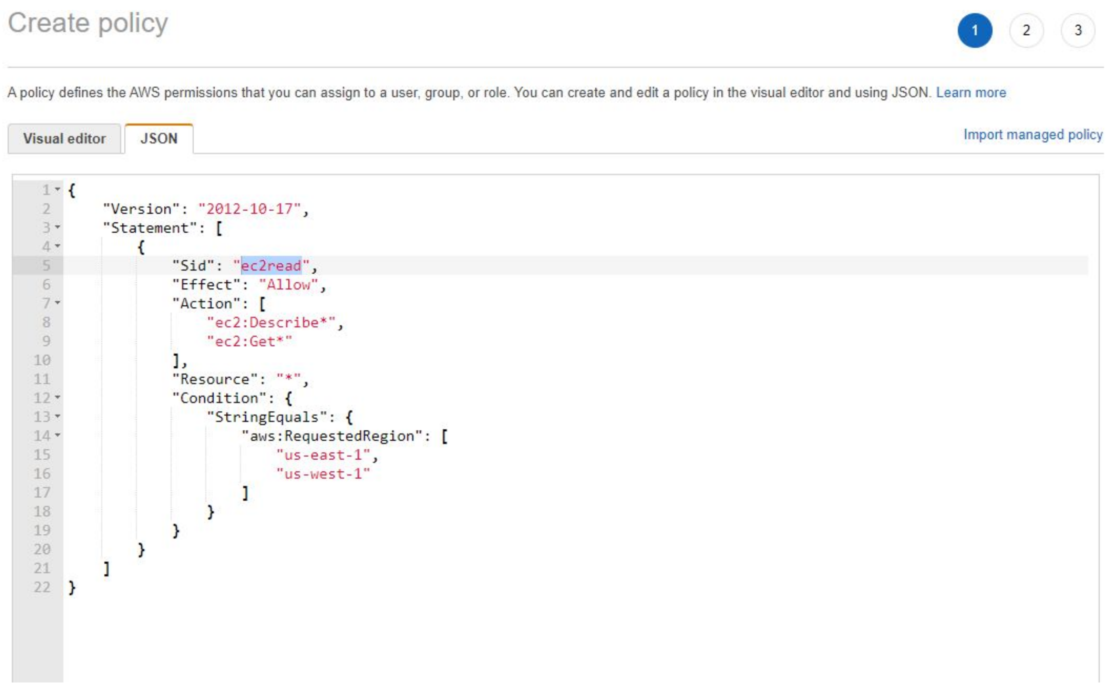
Sign in to the AWS Management Console as an IAM user with MFA enabled that can assume roles in your AWS account, and open the IAM console at https://console.aws.amazon.com/iam/ .

In the navigation pane, click Policies and then click Create policy.



On the Create policy page click the JSON tab.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ec2read",
            "Effect": "Allow",
            "Action": [
                "ec2:Describe*",
                "ec2:Get*"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestedRegion": [
                        "us-east-1",
                        "us-west-1"
                    ]
                }
            }
        }
    ]
}
```



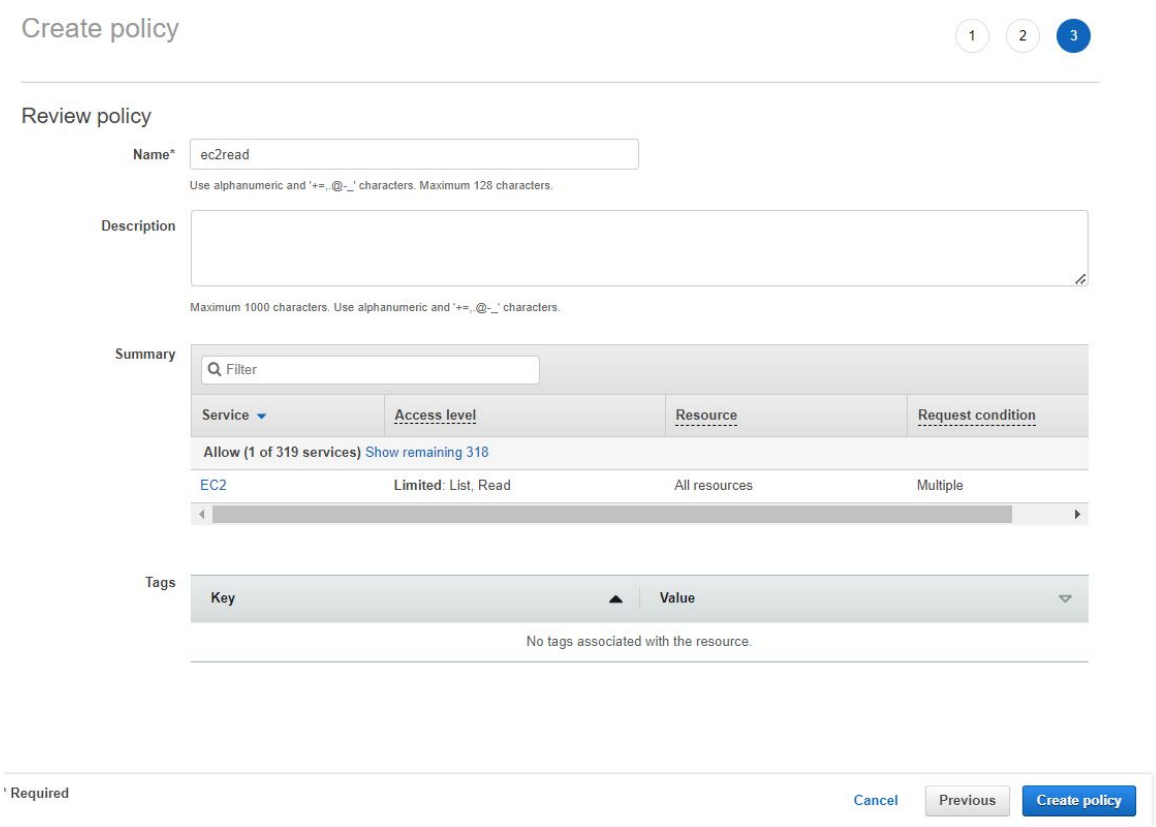
Create policy

A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the visual editor and using JSON. Learn more

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ec2read",
            "Effect": "Allow",
            "Action": [
                "ec2:Describe*",
                "ec2:Get*"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestedRegion": [
                        "us-east-1",
                        "us-west-1"
                    ]
                }
            }
        }
    ]
}
```

Click Review policy.

Enter the name of ec2read and any description to help you identify the policy, verify the summary and then click Create policy.



Create policy

Review policy

Name* ec2read

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

Description

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

Summary

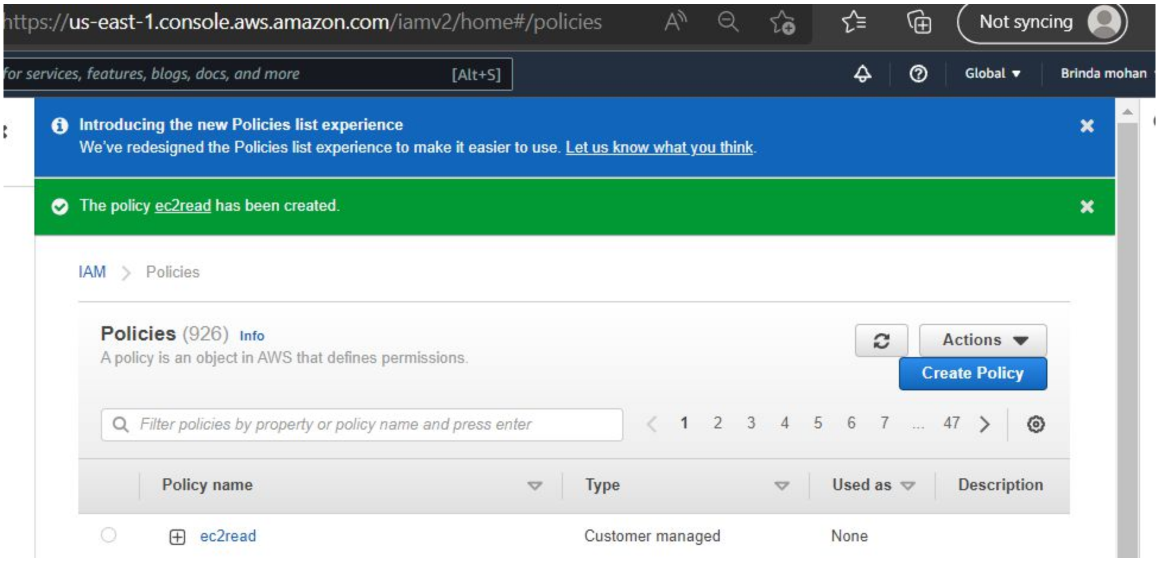
Service	Access level	Resource	Request condition
Allow (1 of 319 services) Show remaining 318			
EC2	**Limited**: List, Read	All resources	Multiple

Tags

Key	Value
No tags associated with the resource.	

' Required

Cancel
Previous
Create policy



ittps://us-east-1.console.aws.amazon.com/iamv2/home#/policies

Not syncing
for services, features, blogs, docs, and more
[Alt+S]
Global
Brinda mohan

Introducing the new Policies list experience
We've redesigned the Policies list experience to make it easier to use. Let us know what you think.

The policy ec2read has been created.

IAM > Policies

Policies (926) Info

A policy is an object in AWS that defines permissions.

Actions
Create Policy
Filter policies by property or policy name and press enter
1 2 3 4 5 6 7 ... 47

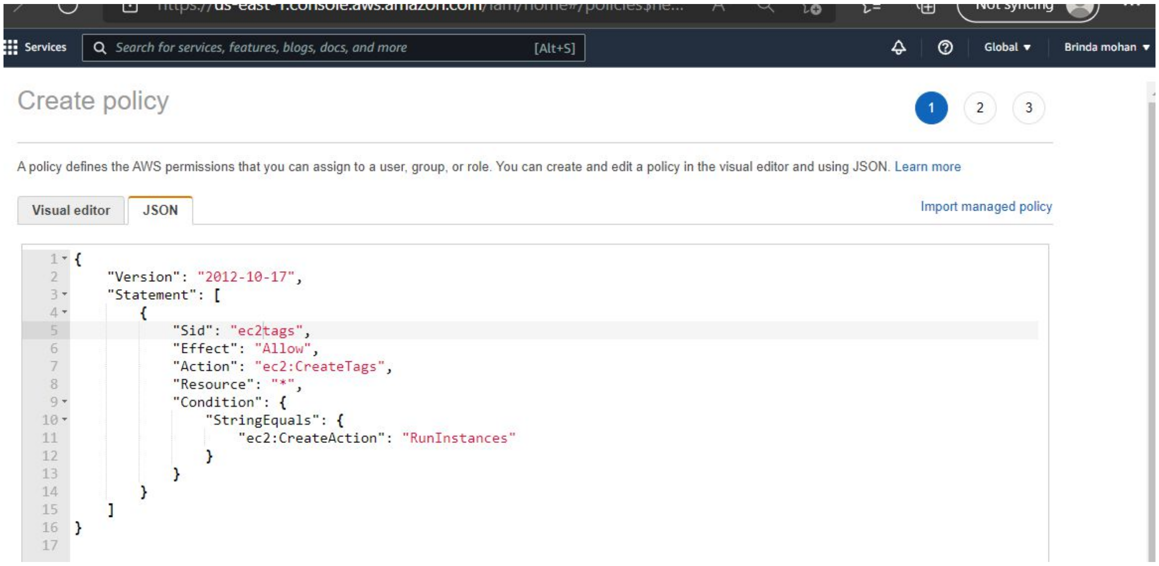
Policy name	Type	Used as	Description
ec2read	Customer managed	None	

1.2 Create policy named ec2tags

This policy allows the creation of tags for EC2, with a condition of the action being RunInstances , which is launching an instance.

Create a managed policy using the JSON policy below and name of ec2tags.

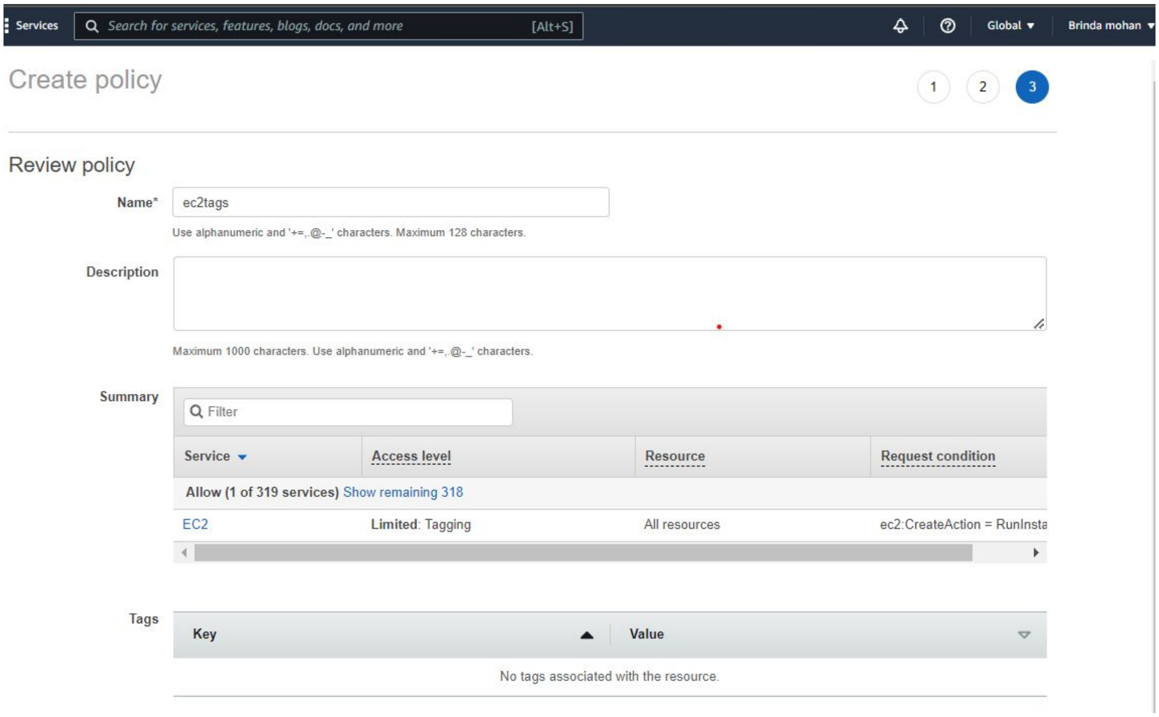
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ec2tags",
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "RunInstances"
                }
            }
        }
    ]
}
```


https://us-east-1.console.aws.amazon.com/iam/home#/policies$ne...
Not syncing
Services
Search for services, features, blogs, docs, and more [Alt+S]
Global
Brinda mohan
1
2
3
Visual editor
JSON
Import managed policy

Create policy

A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the visual editor and using JSON. Learn more

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ec2tags",
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "RunInstances"
                }
            }
        }
    ]
}
```


Services
Search for services, features, blogs, docs, and more [Alt+S]
Global
Brinda mohan
1
2
3
Filter

Create policy

Review policy

Name* ec2tags

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

Description

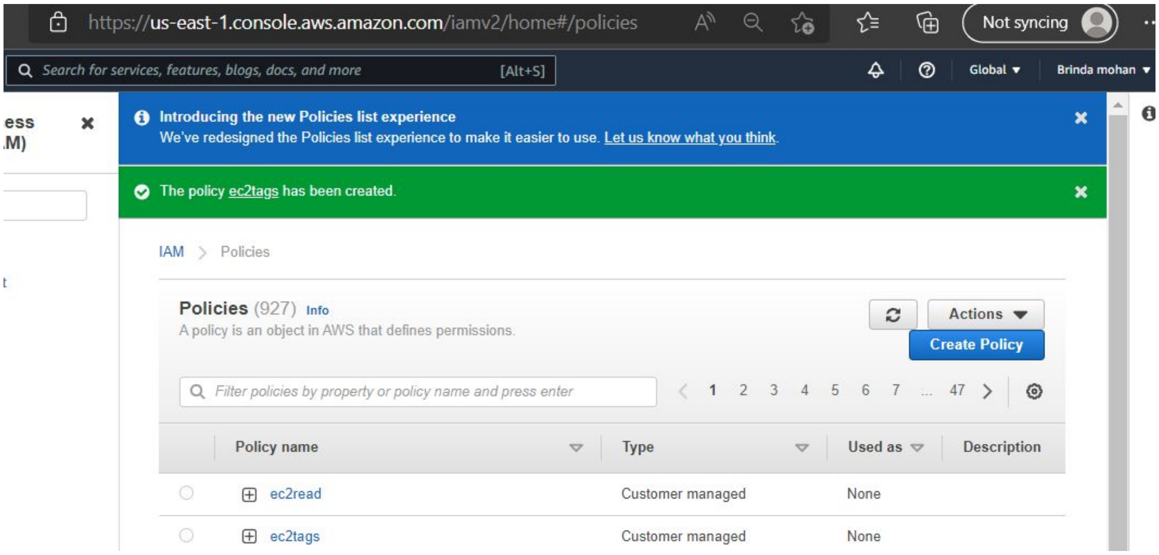
Maximum 1000 characters. Use alphanumeric and '+=,.@-_' characters.

Summary

Service	Access level	Resource	Request condition
Allow (1 of 319 services) Show remaining 318			
EC2	Limited: Tagging	All resources	ec2:CreateAction = RunInsta

Tags

Key	Value
No tags associated with the resource.	


https://us-east-1.console.aws.amazon.com/iamv2/home#/policies
Not syncing
Search for services, features, blogs, docs, and more [Alt+S]
Global ▾
Brinda mohan ▾
ess
.M)
IAM > Policies
Actions ▾
Create Policy
Filter policies by property or policy name and press enter
< 1 2 3 4 5 6 7 ... 47 >

Introducing the new Policies list experience
We've redesigned the Policies list experience to make it easier to use. Let us know what you think.

The policy ec2tags has been created.

Policies (927) Info
A policy is an object in AWS that defines permissions.

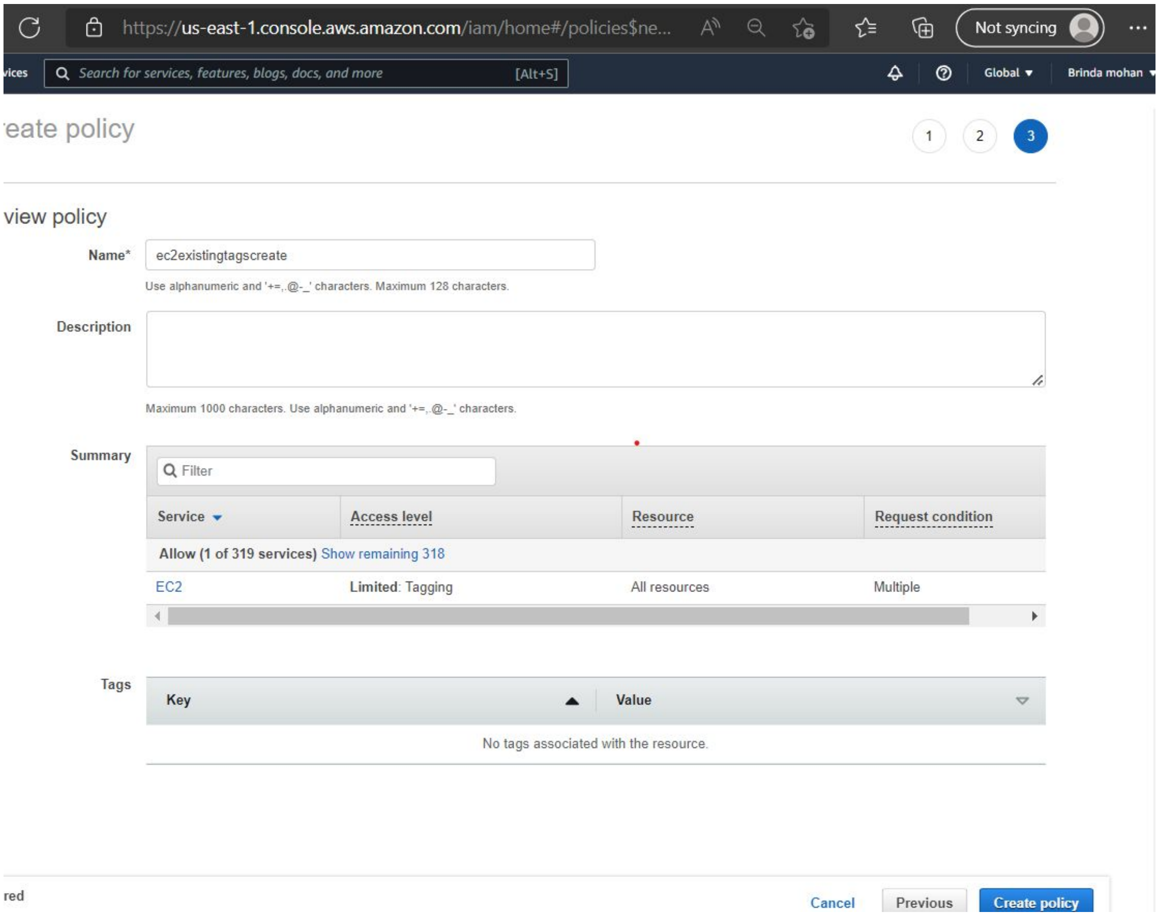
	Policy name	Type	Used as	Description
○	⊞ ec2read	Customer managed	None	
○	⊞ ec2tags	Customer managed	None	

1.3 Create policy named ec2existingtagscreate

This policy allows creation (and overwriting) of EC2 tags only if the resources are already tagged Team / Beta.

Create a managed policy using the JSON policy below and name of ec2existingtagscreate.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ec2existingtagscreate",
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/Team": "Beta"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": [
                        "Team",
                        "Name"
                    ]
                },
                "StringEqualsIfExists": {
                    "aws:RequestTag/Team": "Beta"
                }
            }
        }
    ]
}
```



https://us-east-1.console.aws.amazon.com/iam/home#/policies$ne...

Search for services, features, blogs, docs, and more [Alt+S]

eate policy

view policy

Name* ec2existingtagscreate

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

Description

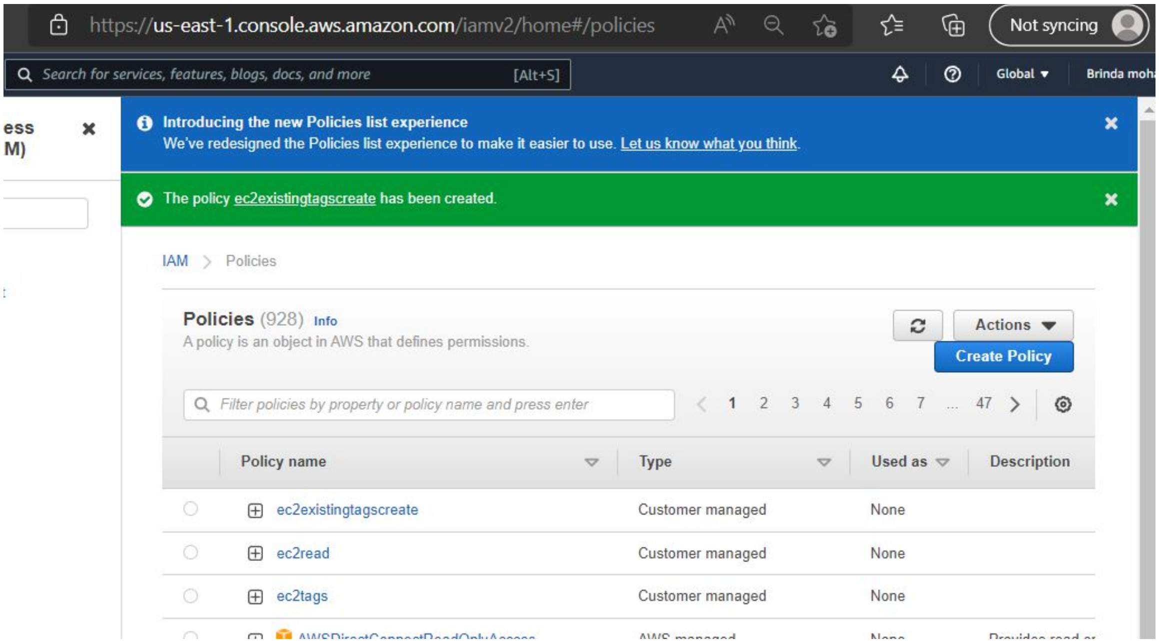
Maximum 1000 characters. Use alphanumeric and '+=,.@-_' characters.

Summary

Service	Access level	Resource	Request condition
Allow (1 of 319 services) Show remaining 318			
EC2	**Limited**: Tagging	All resources	Multiple

Tags

Key	Value
No tags associated with the resource.	



https://us-east-1.console.aws.amazon.com/iamv2/home#/policies

Search for services, features, blogs, docs, and more [Alt+S]

Introducing the new Policies list experience
We've redesigned the Policies list experience to make it easier to use. Let us know what you think.

The policy ec2existingtagscreate has been created.

IAM > Policies

Policies (928) Info
A policy is an object in AWS that defines permissions.

Filter policies by property or policy name and press enter

Policy name	Type	Used as	Description
ec2existingtagscreate	Customer managed	None	
ec2read	Customer managed	None	
ec2tags	Customer managed	None	
AWSDirectConnectReadOnlyAccess	AWS managed	None	Provides read or

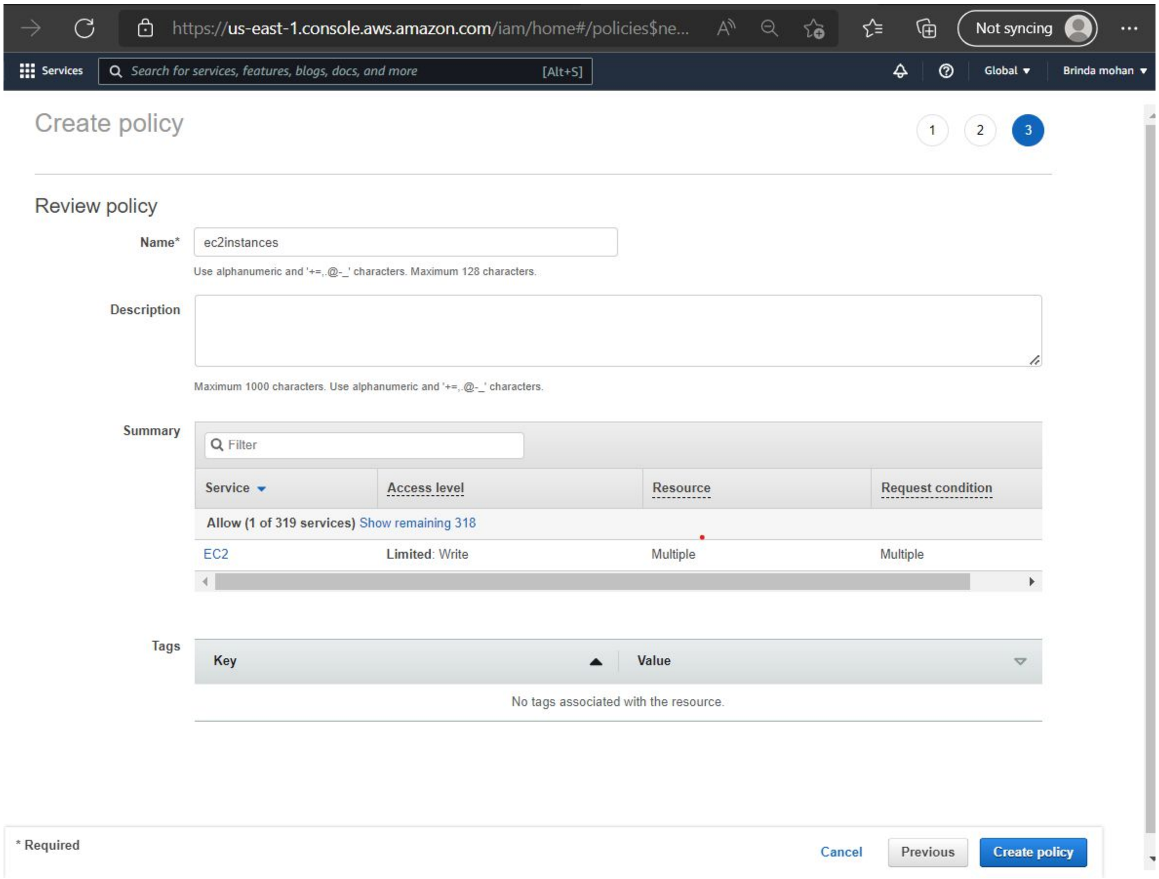
1.4 Create policy named ec2instances

This first section of this policy allows instances to be launched, only if the conditions of region and specific tag keys are matched. The second section allows other resources to be created at instance launch time with region condition.

Create a managed policy using the JSON policy below and name of ec2instances.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ec2instances",
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": "arn:aws:ec2:*:*:instance/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestedRegion": [
                        "us-east-1",
                        "us-west-1"
                    ],
                    "aws:RequestTag/Team": "Beta"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": [
                        "Name",
                        "Team"
                    ]
                }
            }
        },
        {
            "Sid": "ec2instancesother",
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": [
                "arn:aws:ec2:*:*:subnet/*",
                "arn:aws:ec2:*:*:key-pair/*",
                "arn:aws:ec2:*::snapshot/*",
                "arn:aws:ec2:*:*:launch-template/*",
                "arn:aws:ec2:*:*:volume/*",
                "arn:aws:ec2:*:*:security-group/*",
                "arn:aws:ec2:*:*:placement-group/*",
                "arn:aws:ec2:*:*:network-interface/*",
                "arn:aws:ec2:*::image/*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:RequestedRegion": [
                        "us-east-1",
                        "us-west-1"
                    ]
                }
```

```
                    }
                }
            ]
        }
```



https://us-east-1.console.aws.amazon.com/iam/home#/policies$ne...
Not syncing
Services
Search for services, features, blogs, docs, and more
[Alt+S]
Global
Brinda mohan
1
2
3

Create policy

Review policy

Name* ec2instances

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

Description

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

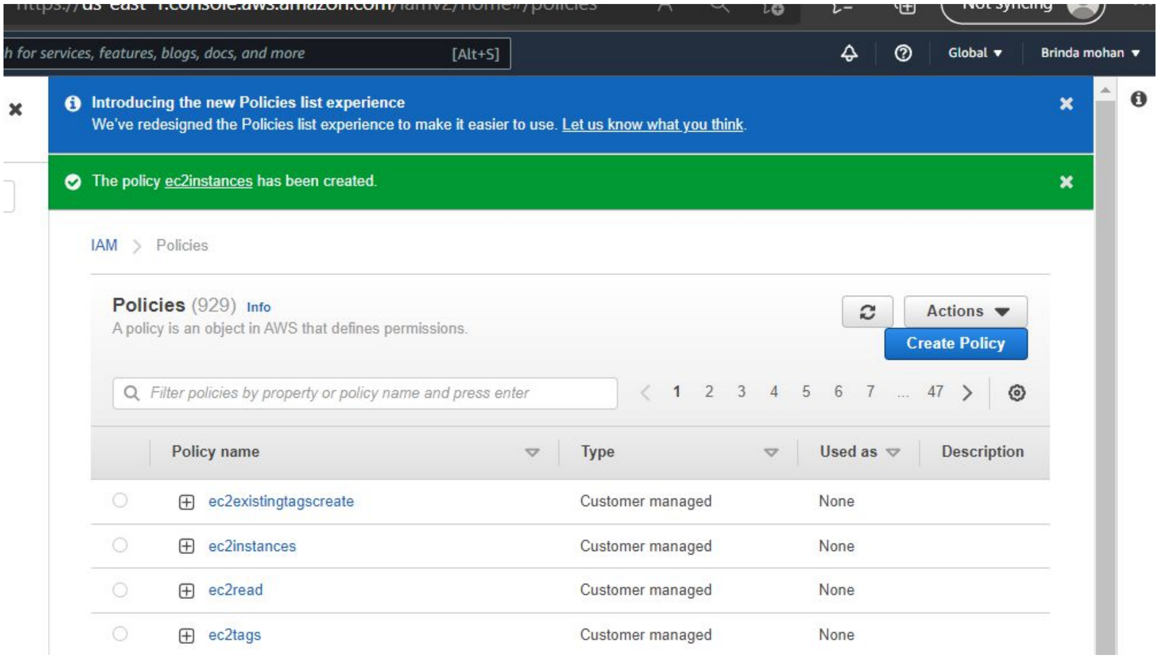
Summary

Service	Access level	Resource	Request condition
Allow (1 of 319 services) Show remaining 318			
EC2	**Limited**: Write	Multiple	Multiple

Tags

Key	Value
No tags associated with the resource.	

* Required


https://us-east-1.console.aws.amazon.com/iamv2/home#/policies
Not syncing
h for services, features, blogs, docs, and more
[Alt+S]
Global
Brinda mohan
IAM
Policies
Actions
Create Policy
Filter policies by property or policy name and press enter
1 2 3 4 5 6 7 ... 47

Introducing the new Policies list experience
We've redesigned the Policies list experience to make it easier to use. Let us know what you think.

The policy ec2instances has been created.

Policies (929) Info
A policy is an object in AWS that defines permissions.

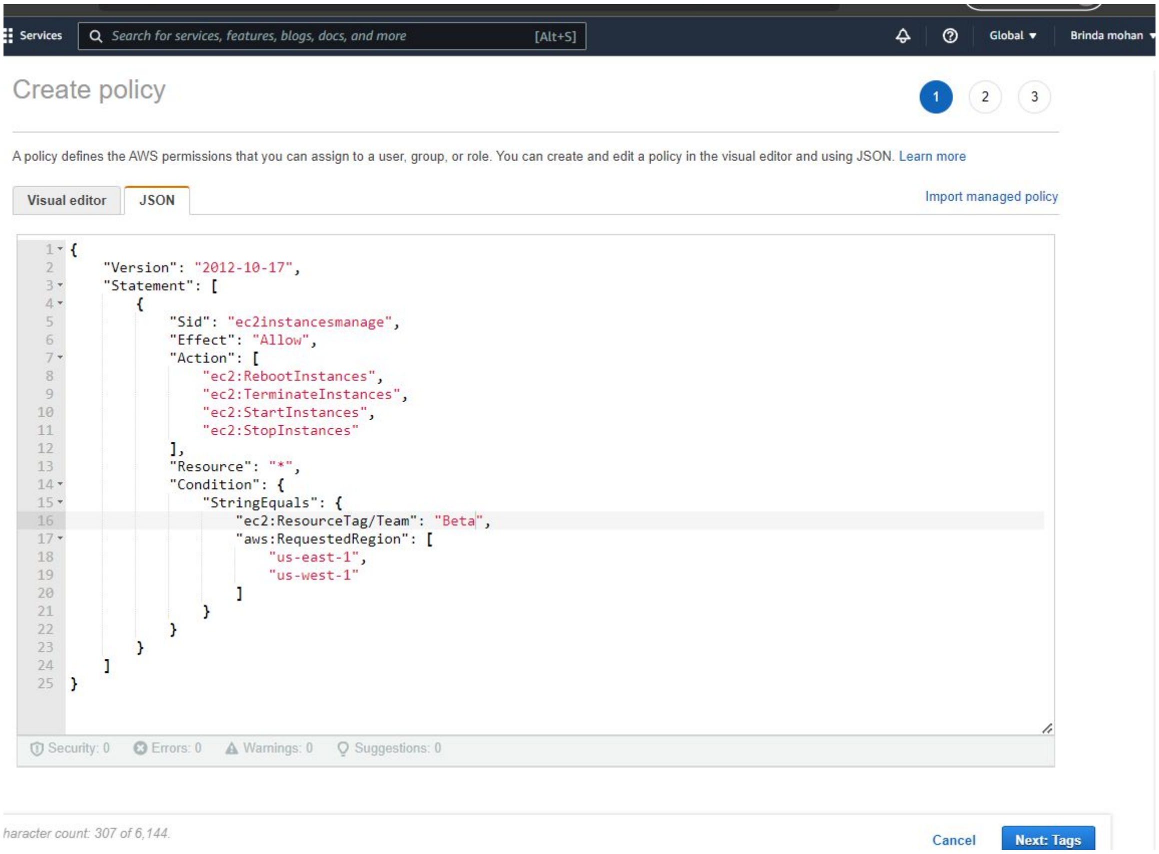
Policy name	Type	Used as	Description
○ ⊞ ec2existingtagscreate	Customer managed	None	
○ ⊞ ec2instances	Customer managed	None	
○ ⊞ ec2read	Customer managed	None	
○ ⊞ ec2tags	Customer managed	None	

1.5 Create policy named ec2instancesmanage

This policy allows reboot, terminate, start and stop of instances, with a condition of the key Team is Beta and region.

Create a managed policy using the JSON policy below and name of ec2instancesmanage.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ec2instancesmanage",
            "Effect": "Allow",
            "Action": [
                "ec2:RebootInstances",
                "ec2:TerminateInstances",
                "ec2:StartInstances",
                "ec2:StopInstances"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/Team": "Beta",
                    "aws:RequestedRegion": [
                        "us-east-1",
                        "us-west-1"
                    ]
                }
            }
        }
    ]
}
```



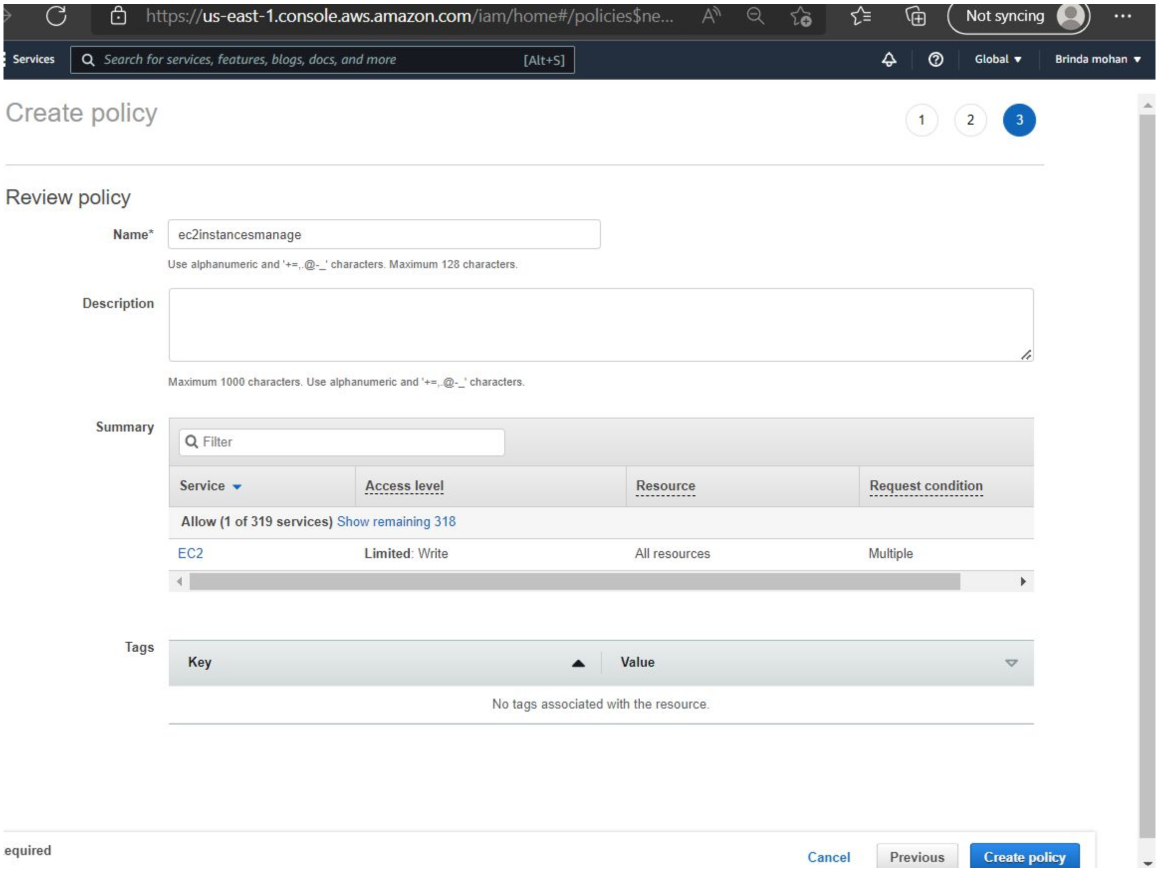
Create policy

A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the visual editor and using JSON. Learn more

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ec2instancesmanage",
            "Effect": "Allow",
            "Action": [
                "ec2:RebootInstances",
                "ec2:TerminateInstances",
                "ec2:StartInstances",
                "ec2:StopInstances"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/Team": "Beta",
                    "aws:RequestedRegion": [
                        "us-east-1",
                        "us-west-1"
                    ]
                }
            }
        }
    ]
}
```

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

haracter count: 307 of 6,144.



https://us-east-1.console.aws.amazon.com/iam/home#/policies$ne...

Create policy

Review policy

Name* ec2instancesmanage

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

Description

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

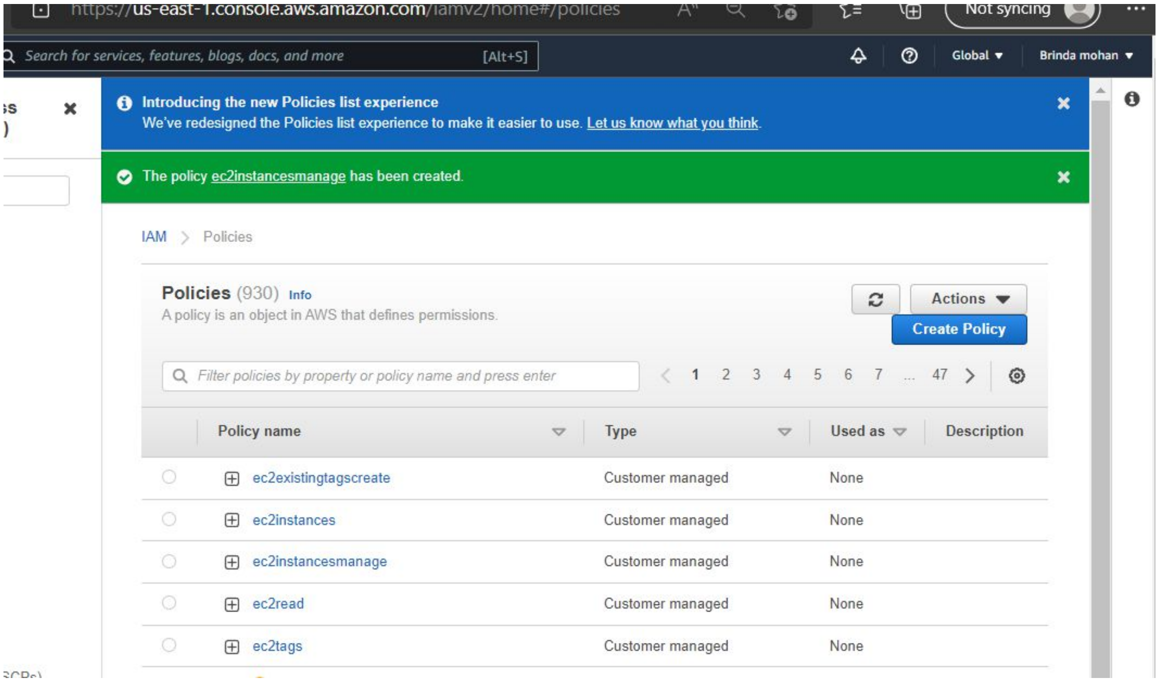
Summary

Service	Access level	Resource	Request condition
Allow (1 of 319 services) Show remaining 318			
EC2	**Limited**: Write	All resources	Multiple

Tags

Key	Value

No tags associated with the resource.



https://us-east-1.console.aws.amazon.com/iamv2/home#/policies

Introducing the new Policies list experience
We've redesigned the Policies list experience to make it easier to use. Let us know what you think.

The policy ec2instancesmanage has been created.

IAM > Policies

Policies (930) Info
A policy is an object in AWS that defines permissions.

	Policy name	Type	Used as	Description
○	⊞ ec2existingtagscreate	Customer managed	None	
○	⊞ ec2instances	Customer managed	None	
○	⊞ ec2instancesmanage	Customer managed	None	
○	⊞ ec2read	Customer managed	None	
○	⊞ ec2tags	Customer managed	None	

Not syncing
Search for services, features, blogs, docs, and more
[Alt+S]
Global
Brinda mohan
Actions
Create Policy
Filter policies by property or policy name and press enter
1 2 3 4 5 6 7 ... 47