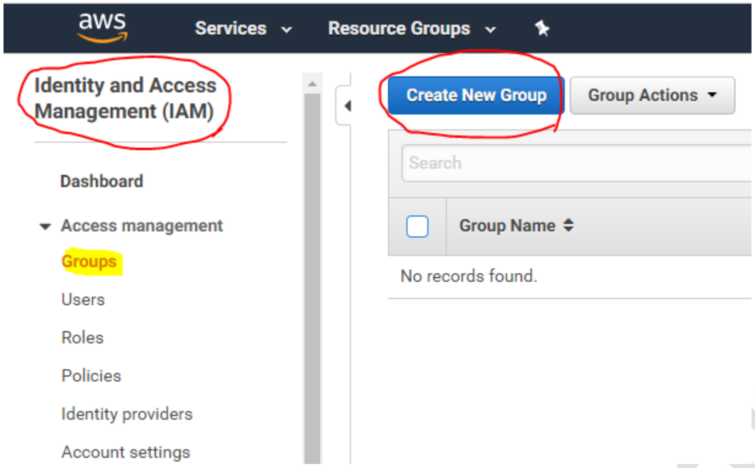
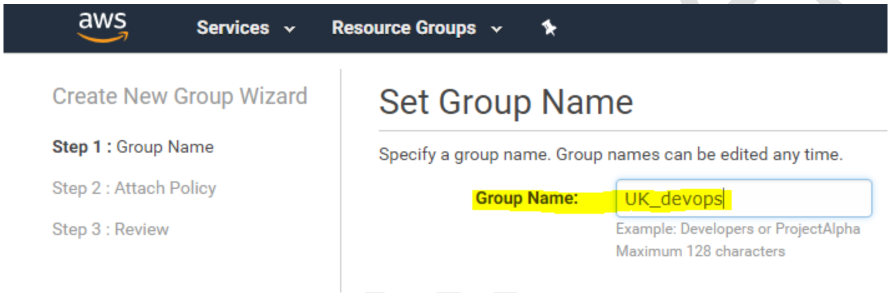
Identity and Access Management (IAM)

https://docs.aws.amazon.com/IAM/latest/UserGuide/intro-structure.html

Step1:- Create a group and attach policy for EC2 full access.
@Click Services → IAM → Expand **Access management** → select Groups → Create New Group→ enter group name



No records found.



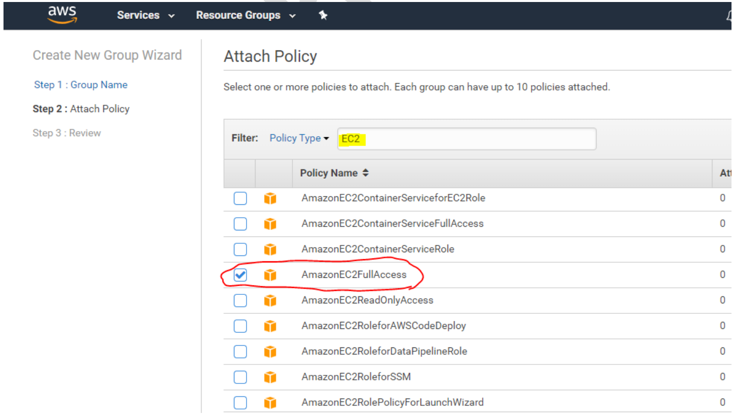
Set Group Name

Specify a group name. Group names can be edited any time.

Group Name: UK_devops

Example: Developers or ProjectAlpha
Maximum 128 characters

@Search of EC2 policy → select AmazonEC2FullAccess →then click Create Group.

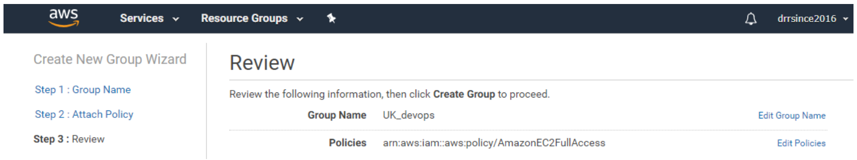


Attach Policy

Select one or more policies to attach. Each group can have up to 10 policies attached.

Filter: Policy Type EC2

	Policy Name	At
□	AmazonEC2ContainerServiceforEC2Role	0
□	AmazonEC2ContainerServiceFullAccess	0
□	AmazonEC2ContainerServiceRole	0
☑	AmazonEC2FullAccess	0
□	AmazonEC2ReadOnlyAccess	0
□	AmazonEC2RoleforAWSCodeDeploy	0
□	AmazonEC2RoleforDataPipelineRole	0
□	AmazonEC2RoleforSSM	0
□	AmazonEC2RolePolicyForLaunchWizard	0



Review

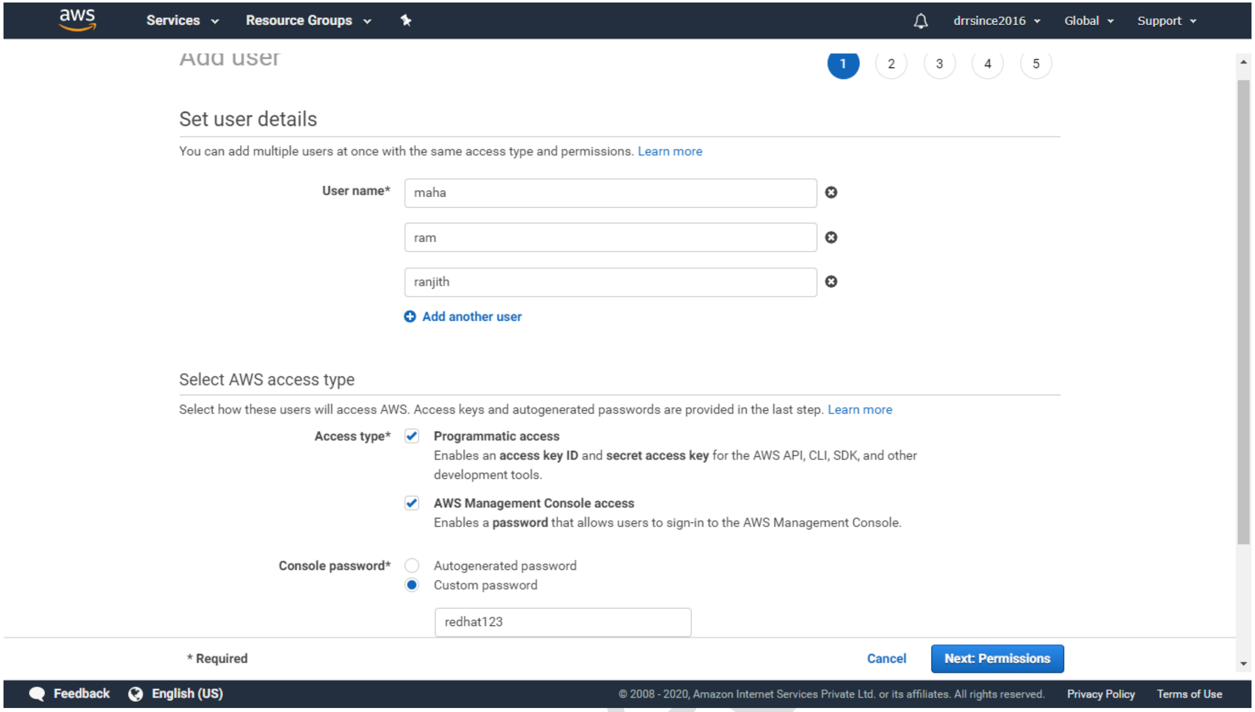
Review the following information, then click **Create Group** to proceed.

Group Name UK_devops

Policies arn:aws:iam::aws:policy/AmazonEC2FullAccess

Step2:- Create users and added the same to newly created groups (UK_Devops)

@Click Users → Add user→ then enter usernames (either one user or multiple users) → select access type →enter custom password→then click Next Permission→



Add user

Set user details

You can add multiple users at once with the same access type and permissions. Learn more

User name* maha

ram

ranjith

Add another user

Select AWS access type

Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step. Learn more

Access type* ☑ **Programmatic access**
Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.

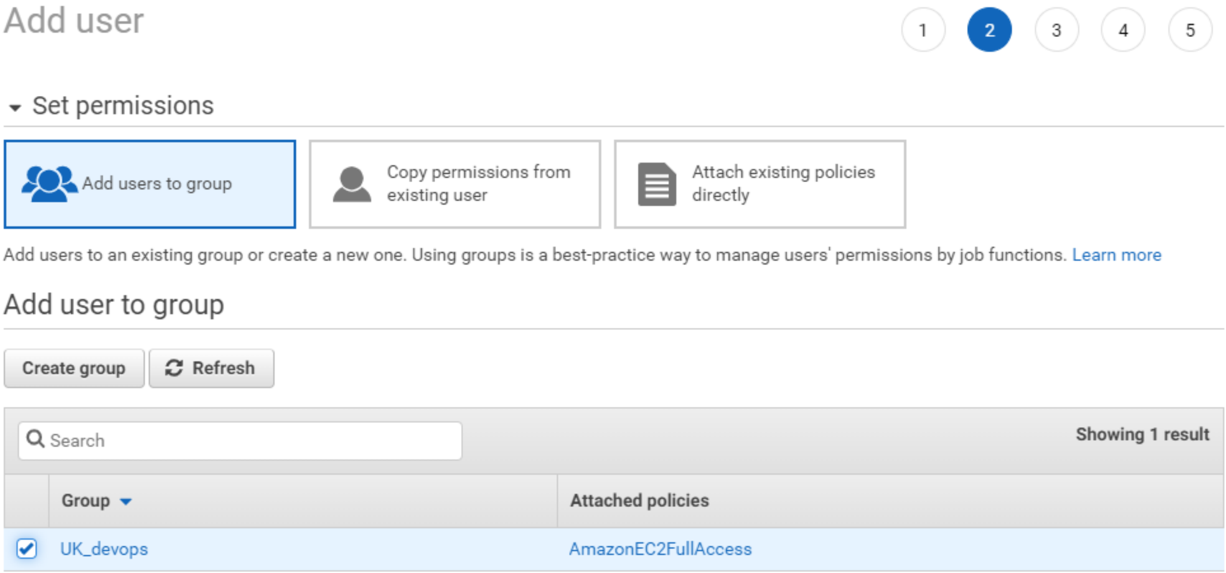
☑ **AWS Management Console access**
Enables a **password** that allows users to sign-in to the AWS Management Console.

Console password* ○ Autogenerated password
● Custom password

redhat123

* Required

@Select → UK_devops → click Next:Tags → Next:Review→Create users →


1
2
3
4
5
Add users to group
Copy permissions from existing user
Attach existing policies directly
Create group
Refresh
Search

Add user

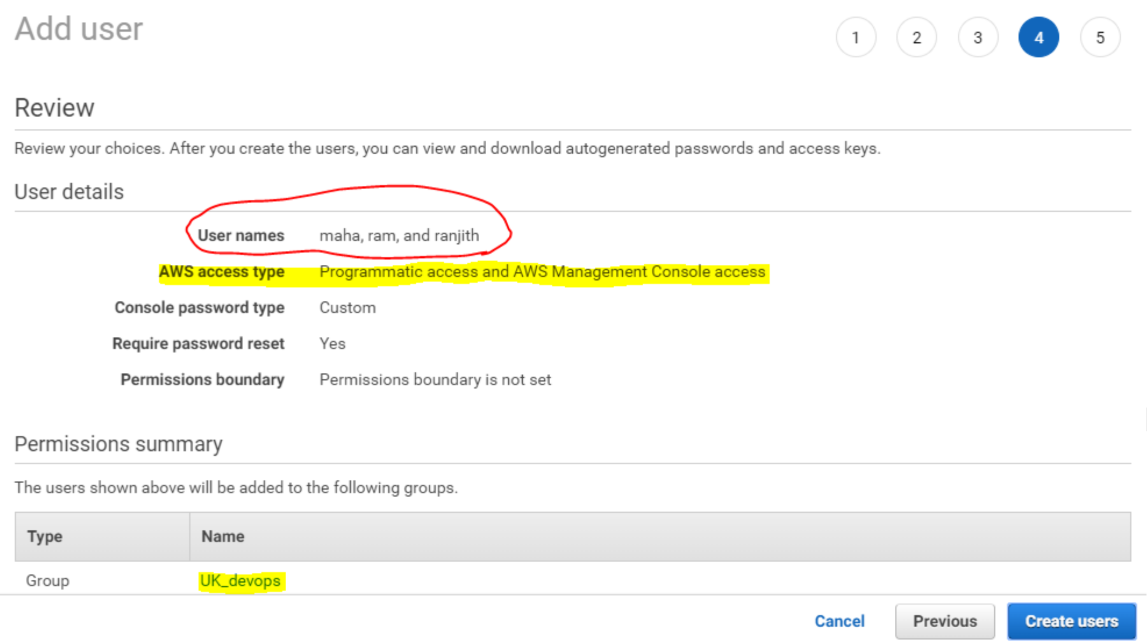
Set permissions

Add users to an existing group or create a new one. Using groups is a best-practice way to manage users' permissions by job functions. Learn more

Add user to group

Showing 1 result

	Group	Attached policies
☑	UK_devops	AmazonEC2FullAccess



Add user

Review

Review your choices. After you create the users, you can view and download autogenerated passwords and access keys.

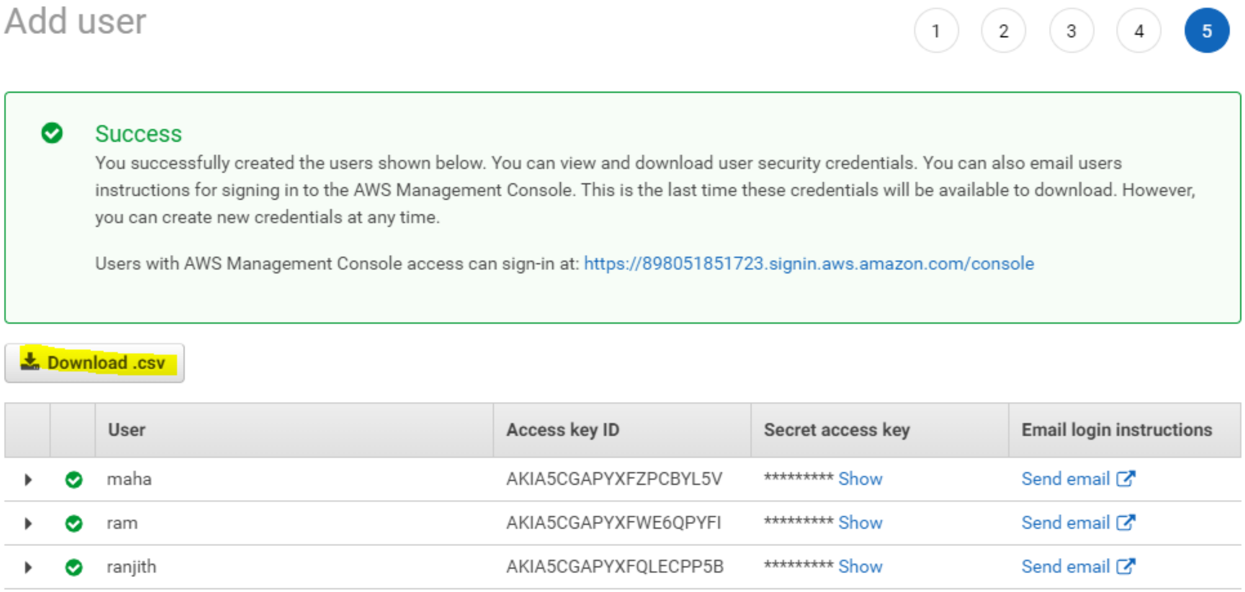
User details

User names	maha, ram, and ranjith
AWS access type	Programmatic access and AWS Management Console access
Console password type	Custom
Require password reset	Yes
Permissions boundary	Permissions boundary is not set

Permissions summary

The users shown above will be added to the following groups.

Type	Name
Group	UK_devops



Add user

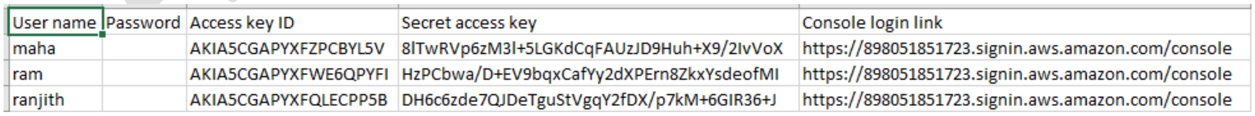
Success

You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download. However, you can create new credentials at any time.

Users with AWS Management Console access can sign-in at: https://898051851723.signin.aws.amazon.com/console

		User	Access key ID	Secret access key	Email login instructions
▸	✓	maha	AKIA5CGAPYXFZPCBYL5V	********** Show	Send email
▸	✓	ram	AKIA5CGAPYXFWE6QPYFI	********** Show	Send email
▸	✓	ranjith	AKIA5CGAPYXFQLECPP5B	********** Show	Send email

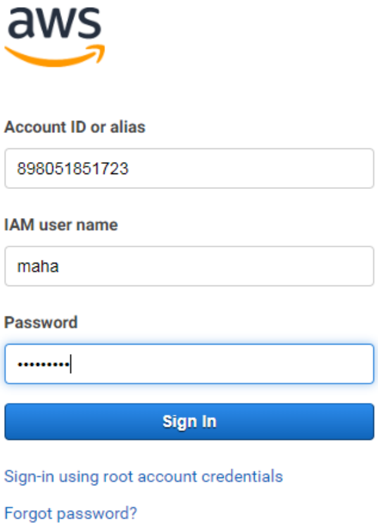
Note:- Users are created and added into group successfully, now download the .csv and save it safely for login purpose and use below console login link to access.



User name	Password	Access key ID	Secret access key	Console login link
maha		AKIA5CGAPYXFZPCBYL5V	8lTwRVp6zM3l+5LGKdCqFAUzJD9Huh+X9/2IvVoX	https://898051851723.signin.aws.amazon.com/console
ram		AKIA5CGAPYXFWE6QPYFI	HzPCbwa/D+EV9bqxCafYy2dXPErn8ZkxYsdeofMI	https://898051851723.signin.aws.amazon.com/console
ranjith		AKIA5CGAPYXFQLECPP5B	DH6c6zde7QJDeTguStVgqY2fDX/p7kM+6GIR36+J	https://898051851723.signin.aws.amazon.com/console

Step2.1:- now try to login with newly created user by using console link.

https://898051851723.signin.aws.amazon.com/console



Account ID or alias

898051851723

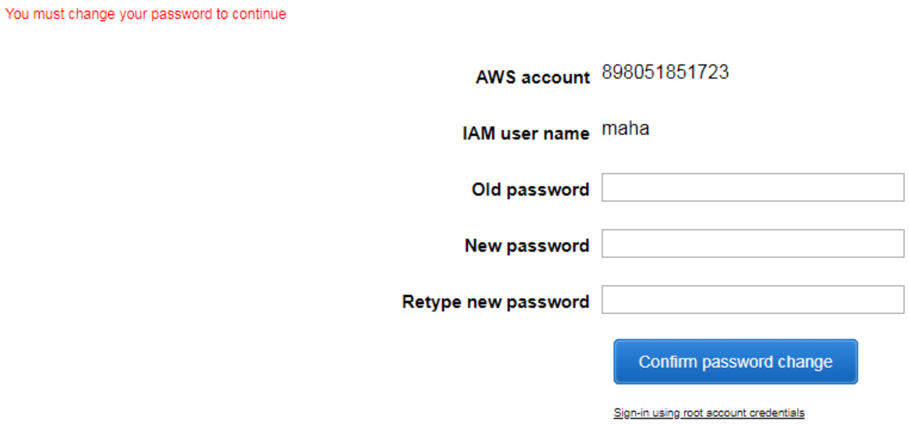
IAM user name

maha

Password

•••••••••

@Change the password at first login.



You must change your password to continue

AWS account 898051851723

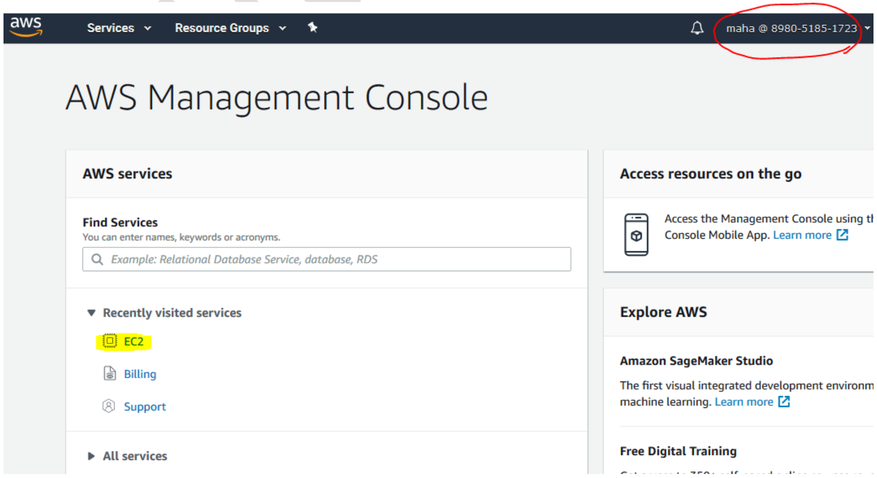
IAM user name maha

Old password

New password

Retype new password

@Now you see AWS Management Console.



AWS Management Console

AWS services

Find Services

You can enter names, keywords or acronyms.

Example: Relational Database Service, database, RDS

Recently visited services

- EC2
- Billing
- Support

All services

Access resources on the go

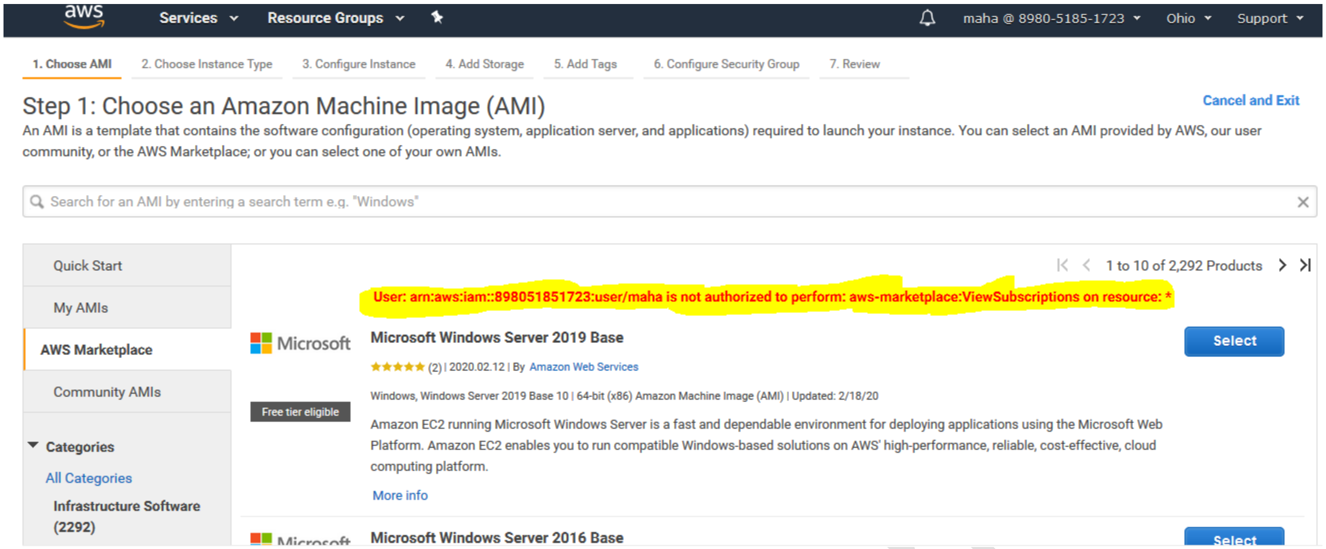
Access the Management Console using th Console Mobile App. Learn more

Explore AWS

Amazon SageMaker Studio

The first visual integrated development environm machine learning. Learn more

Free Digital Training



Step 1: Choose an Amazon Machine Image (AMI)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.

User: arn:aws:iam::898051851723:user/maha is not authorized to perform: aws-marketplace:ViewSubscriptions on resource: *

Microsoft Windows Server 2019 Base

★★★★★ (2) | 2020.02.12 | By Amazon Web Services

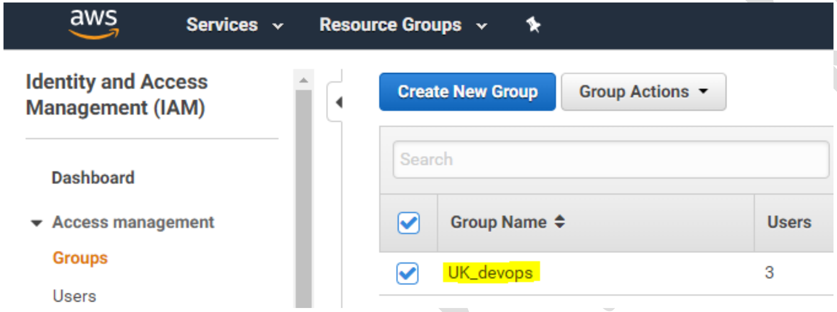
Windows, Windows Server 2019 Base 10 | 64-bit (x86) Amazon Machine Image (AMI) | Updated: 2/18/20

Amazon EC2 running Microsoft Windows Server is a fast and dependable environment for deploying applications using the Microsoft Web Platform. Amazon EC2 enables you to run compatible Windows-based solutions on AWS' high-performance, reliable, cost-effective, cloud computing platform.

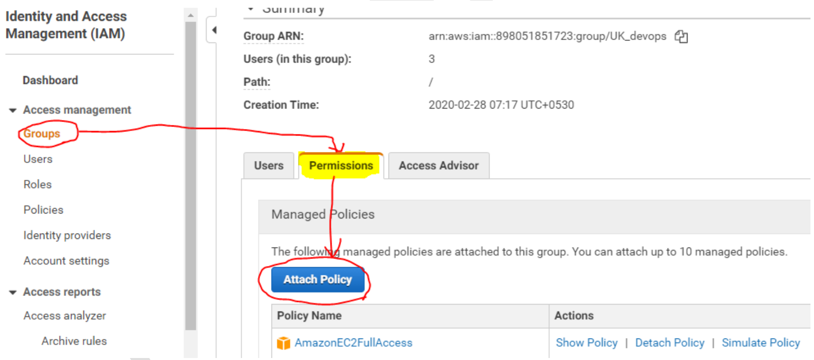
Microsoft Windows Server 2016 Base

Note:- User is not able to create instance, lets try to give access and try the same again.

Step 3:- Go to groups and attach the policy (AWSMarketplaceManageSubscription) for user to create EC2 instance.



☑	Group Name	Users
☑	UK_devops	3



Group ARN: arn:aws:iam::898051851723:group/UK_devops

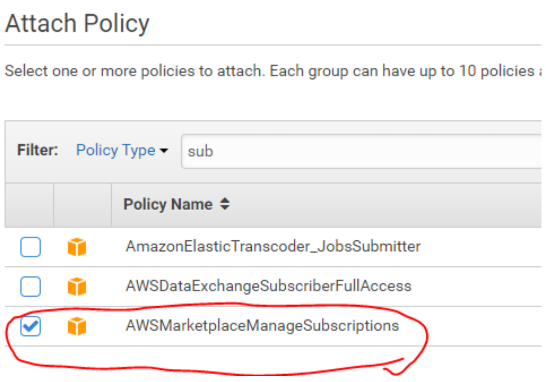
Users (in this group): 3

Path: /

Creation Time: 2020-02-28 07:17 UTC+0530

The following managed policies are attached to this group. You can attach up to 10 managed policies.

Policy Name	Actions
AmazonEC2FullAccess	Show Policy | Detach Policy | Simulate Policy

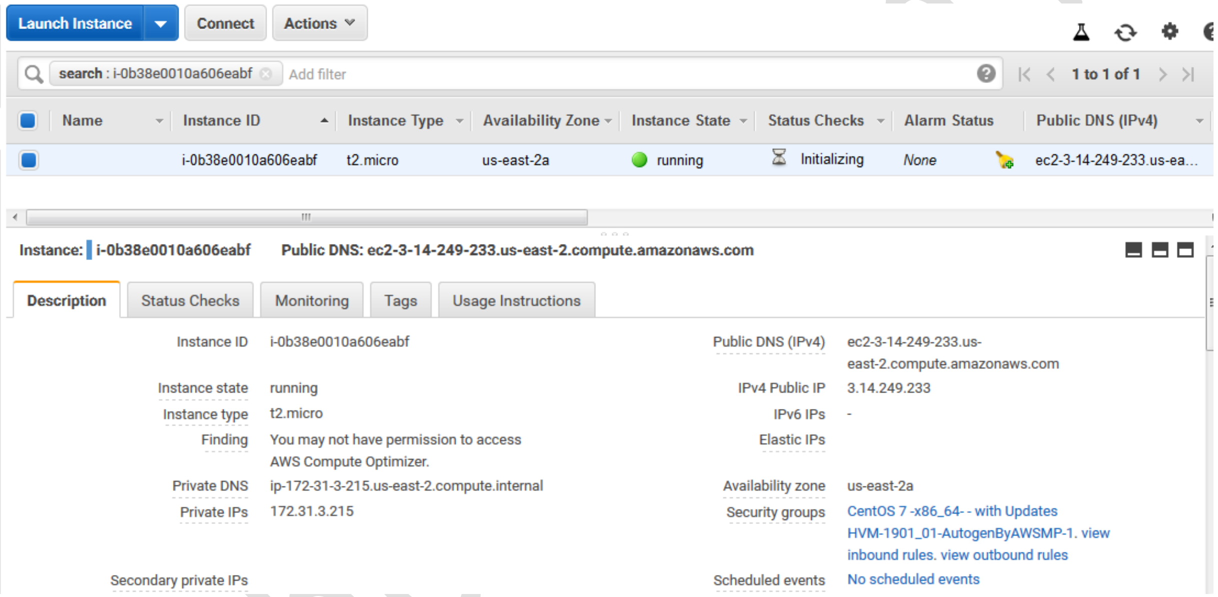


Attach Policy

Select one or more policies to attach. Each group can have up to 10 policies

		Policy Name
□		AmazonElasticTranscoder_JobsSubmitter
□		AWSDataExchangeSubscriberFullAccess
☑		AWSMarketplaceManageSubscriptions

Step 3.1:- Launch the EC2 instance with help of (AWS_Launch-EC2instance.pdf)

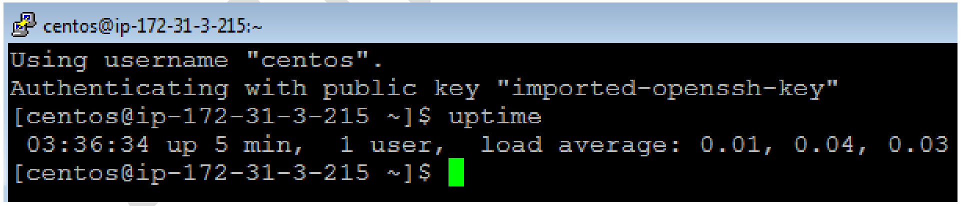


	Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)
■		i-0b38e0010a606eabf	t2.micro	us-east-2a	● running	Initializing	None	ec2-3-14-249-233.us-ea...

Instance: i-0b38e0010a606eabf Public DNS: ec2-3-14-249-233.us-east-2.compute.amazonaws.com

Instance ID	i-0b38e0010a606eabf	Public DNS (IPv4)	ec2-3-14-249-233.us-east-2.compute.amazonaws.com
Instance state	running	IPv4 Public IP	3.14.249.233
Instance type	t2.micro	IPv6 IPs	-
Finding	You may not have permission to access AWS Compute Optimizer.	Elastic IPs	
Private DNS	ip-172-31-3-215.us-east-2.compute.internal	Availability zone	us-east-2a
Private IPs	172.31.3.215	Security groups	CentOS 7 -x86_64- - with Updates HVM-1901_01-AutogenByAWSMP-1. view inbound rules. view outbound rules
Secondary private IPs		Scheduled events	No scheduled events

@With ssh key, try to login into server.



centos@ip-172-31-3-215:~

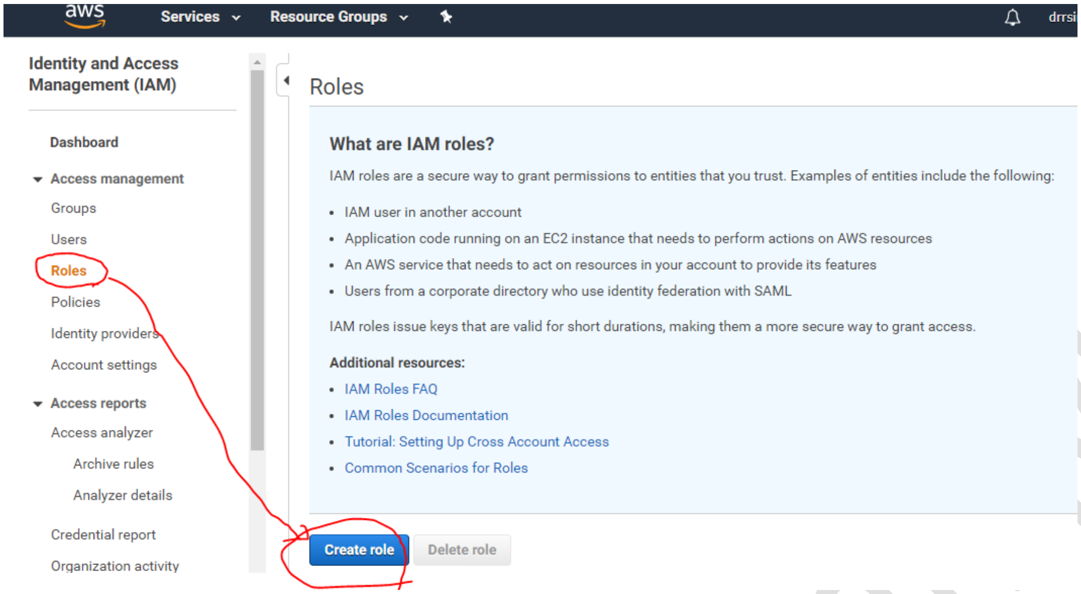
```
Using username "centos".
Authenticating with public key "imported-openssh-key"
[centos@ip-172-31-3-215 ~]$ uptime
 03:36:34 up 5 min,  1 user,  load average: 0.01, 0.04, 0.03
[centos@ip-172-31-3-215 ~]$
```

Note:-after attached the policy, now normal user can able to create/delete EC2 instances. The best way to attach the exact the policy. Kindly read out the error message whats popping up from user end while creating ec2 instance.

Step4:- How to create role and use role for access.

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html

Click on Roles → Create role →select AWS service (EC2) →attach below policies →enter role name →click create role.



Roles

What are IAM roles?

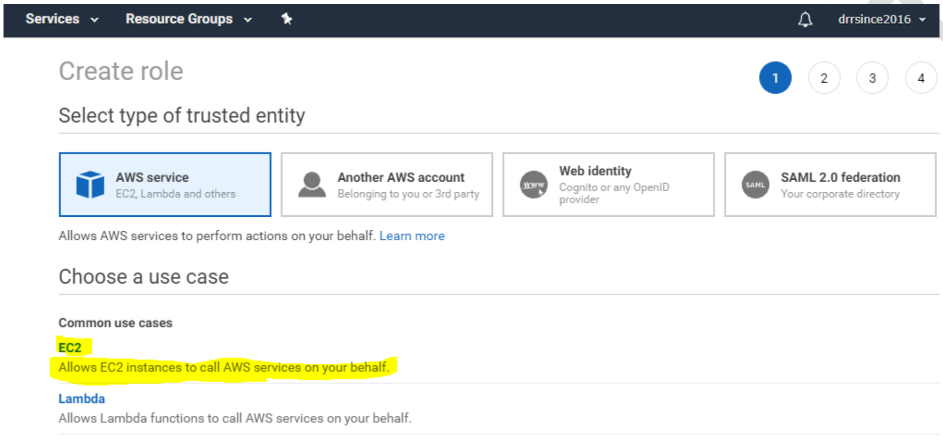
IAM roles are a secure way to grant permissions to entities that you trust. Examples of entities include the following:

- IAM user in another account
- Application code running on an EC2 instance that needs to perform actions on AWS resources
- An AWS service that needs to act on resources in your account to provide its features
- Users from a corporate directory who use identity federation with SAML

IAM roles issue keys that are valid for short durations, making them a more secure way to grant access.

Additional resources:

- IAM Roles FAQ
- IAM Roles Documentation
- Tutorial: Setting Up Cross Account Access
- Common Scenarios for Roles



Create role

Select type of trusted entity

AWS service EC2, Lambda and others	Another AWS account Belonging to you or 3rd party	Web identity Cognito or any OpenID provider	SAML 2.0 federation Your corporate directory

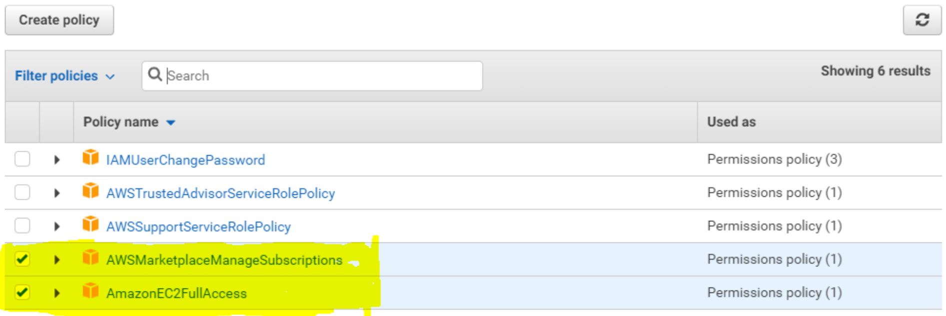
Allows AWS services to perform actions on your behalf. Learn more

Choose a use case

Common use cases

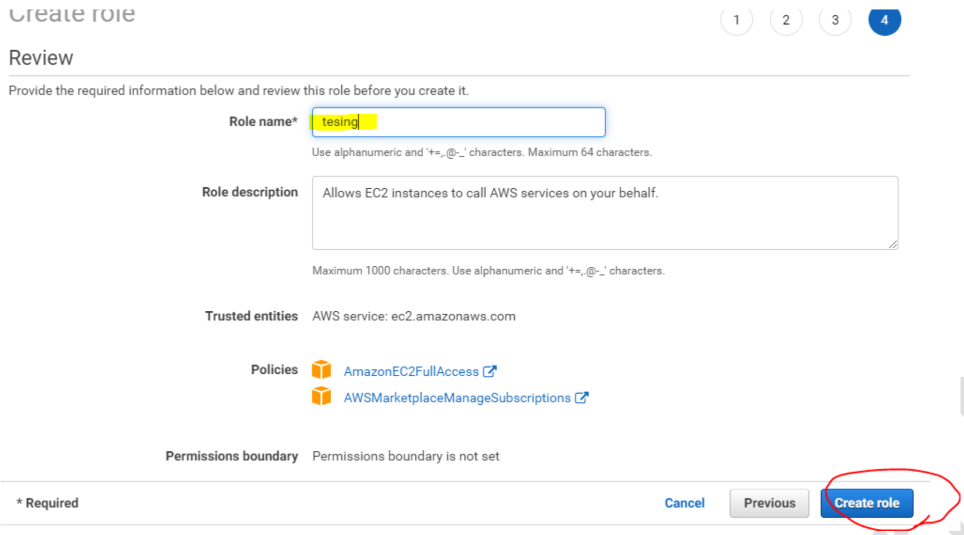
EC2
Allows EC2 instances to call AWS services on your behalf.

Lambda
Allows Lambda functions to call AWS services on your behalf.



Showing 6 results

		Policy name	Used as
□	▸	IAMUserChangePassword	Permissions policy (3)
□	▸	AWSTrustedAdvisorServiceRolePolicy	Permissions policy (1)
□	▸	AWSSupportServiceRolePolicy	Permissions policy (1)
☑	▸	AWSMarketplaceManageSubscriptions	Permissions policy (1)
☑	▸	AmazonEC2FullAccess	Permissions policy (1)



Create role

1 2 3 4

Review

Provide the required information below and review this role before you create it.

Role name* tesing

Use alphanumeric and '+=,.@-_' characters. Maximum 64 characters.

Role description: Allows EC2 instances to call AWS services on your behalf.

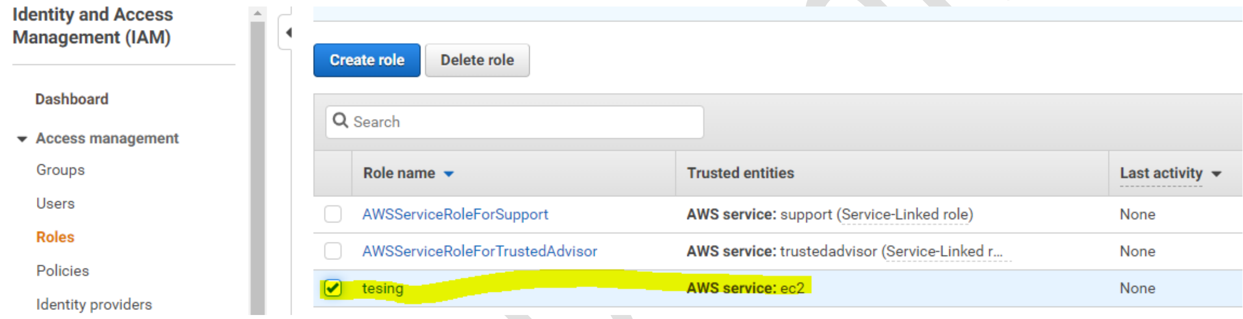
Maximum 1000 characters. Use alphanumeric and '+=,.@-_' characters.

Trusted entities: AWS service: ec2.amazonaws.com

Policies: AmazonEC2FullAccess, AWSMarketplaceManageSubscriptions

Permissions boundary: Permissions boundary is not set

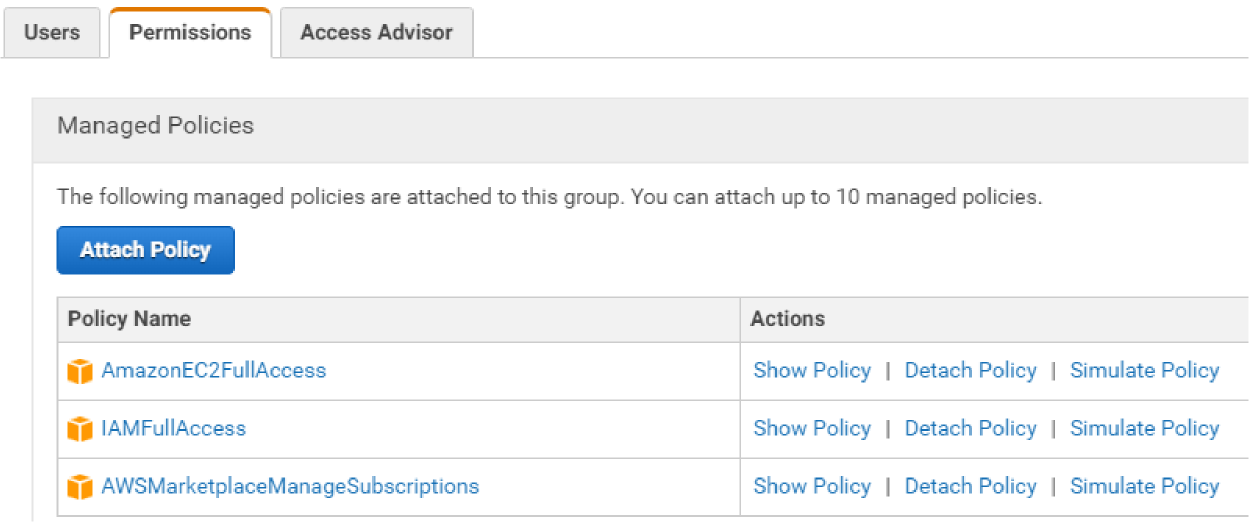
* Required



	Role name	Trusted entities	Last activity
□	AWSServiceRoleForSupport	AWS service: support (Service-Linked role)	None
□	AWSServiceRoleForTrustedAdvisor	AWS service: trustedadvisor (Service-Linked r...	None
☑	tesing	AWS service: ec2	None

Note:- Now role has been created.

Step5:-select the existing group and attach the policy (IAM full access)



Managed Policies

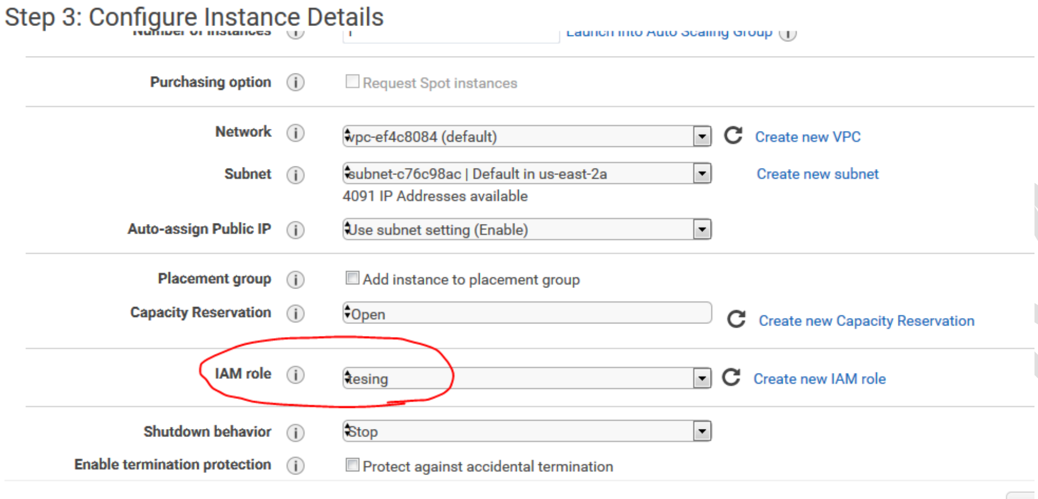
The following managed policies are attached to this group. You can attach up to 10 managed policies.

Policy Name	Actions
AmazonEC2FullAccess	Show Policy | Detach Policy | Simulate Policy
IAMFullAccess	Show Policy | Detach Policy | Simulate Policy
AWSMarketplaceManageSubscriptions	Show Policy | Detach Policy | Simulate Policy

Note:- After attaching the policy, normal user from the group can able to select IAM role.

Step5.1:- from normal user try to launch the EC2 instance with help of (AWS_Launch-EC2instance.pdf)

@While creating instance → you can select IAM role



Step 3: Configure Instance Details

Number of instances: 1 — Launch into Auto Scaling Group

Purchasing option: □ Request Spot instances

Network: vpc-ef4c8084 (default) — Create new VPC

Subnet: subnet-c76c98ac | Default in us-east-2a — Create new subnet
4091 IP Addresses available

Auto-assign Public IP: Use subnet setting (Enable)

Placement group: □ Add instance to placement group

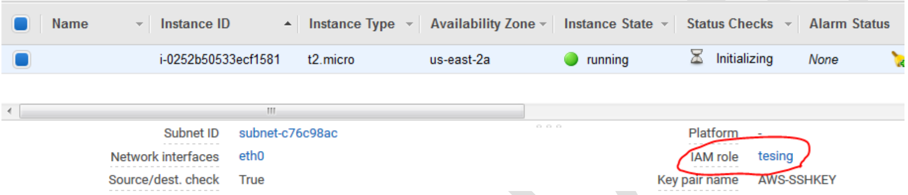
Capacity Reservation: Open — Create new Capacity Reservation

IAM role: tesing — Create new IAM role

Shutdown behavior: Stop

Enable termination protection: □ Protect against accidental termination

@you can see the IAM role on instances details.

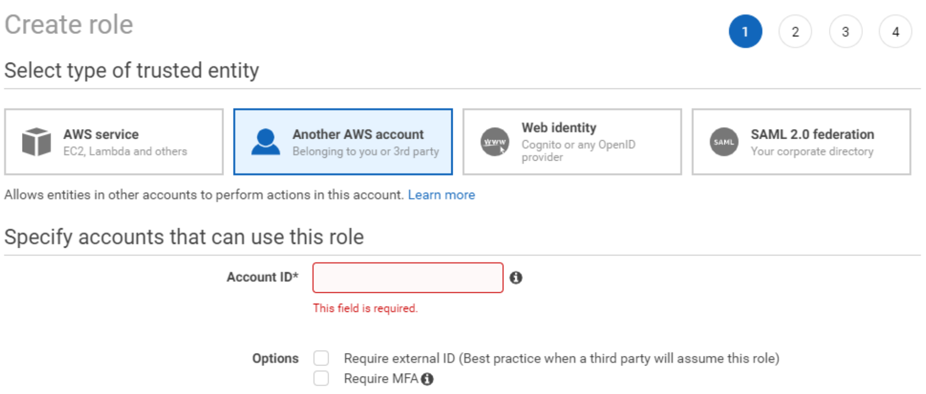


Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status
	i-0252b50533ecf1581	t2.micro	us-east-2a	running	Initializing	None

Subnet ID: subnet-c76c98ac
Network interfaces: eth0
Source/dest. check: True

Platform: -
IAM role: tesing
Key pair name: AWS-SSHKEY

@@We can allow another AWS account with role to use specific services.



Create role

1 2 3 4

Select type of trusted entity

AWS service — EC2, Lambda and others
Another AWS account — Belonging to you or 3rd party
Web identity — Cognito or any OpenID provider
SAML 2.0 federation — Your corporate directory

Allows entities in other accounts to perform actions in this account. Learn more

Specify accounts that can use this role

Account ID*:
This field is required.

Options: □ Require external ID (Best practice when a third party will assume this role)
□ Require MFA

Note:- The maximum session duration setting applies only to sessions created using the AssumeRole* API operations or assume-role* CLI commands. The setting does not limit sessions assumed by AWS services.