

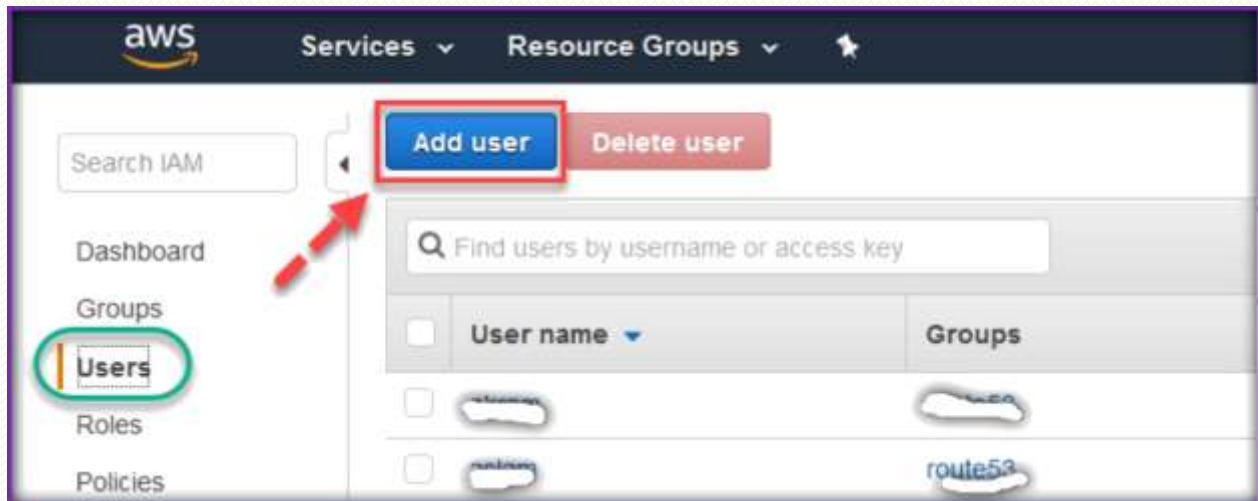
13. IDENTITY AND ACCESS MANAGEMENT

AWS Identity and Access Management (IAM) is a web service that helps you securely control access to AWS resources for your users. You use IAM to control who can use your AWS resources (*authentication*) and what resources they can use and in what ways (*authorization*).

Choose Identity & Access management under Security & Identity from the AWS console page.

CREATING USERS:

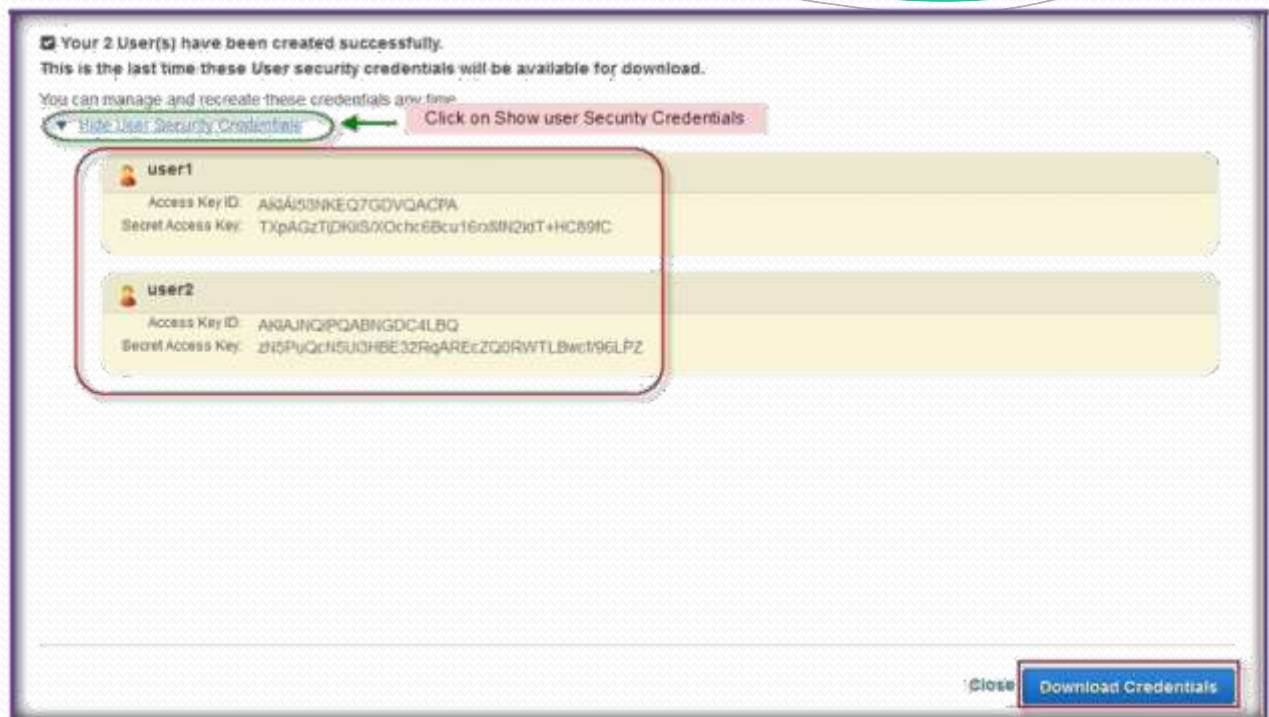
Once you are on IAM page, Click Users from left pane, then choose Add User to create a user.



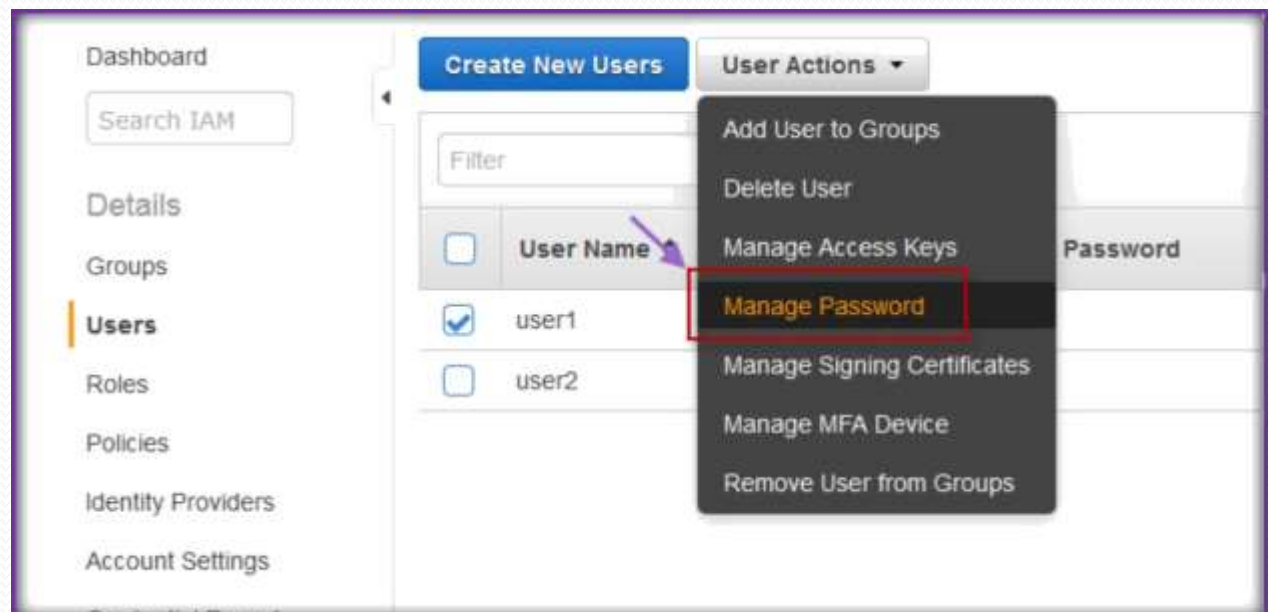
Specify user names in the text fields, if you do not want access keys for new users uncheck generate access keys, then choose Create.



On the next page, click on Show User Security Credentials to see access keys or choose Download Credentials to download them then click on close.



Under Users tab, select a user and click on User Actions, then select manage Password to create a new password.



On the next page, choose either auto-generated or a custom password, then specify a password if you choose custom password.

Check box if you want user to create a new password at next sign-in, then choose Apply.

Users who will be using the AWS Management Console require a password. Select from the options below to manage the password for user user1.

☐ Assign an auto-generated password

☒ Assign a custom password

Password:

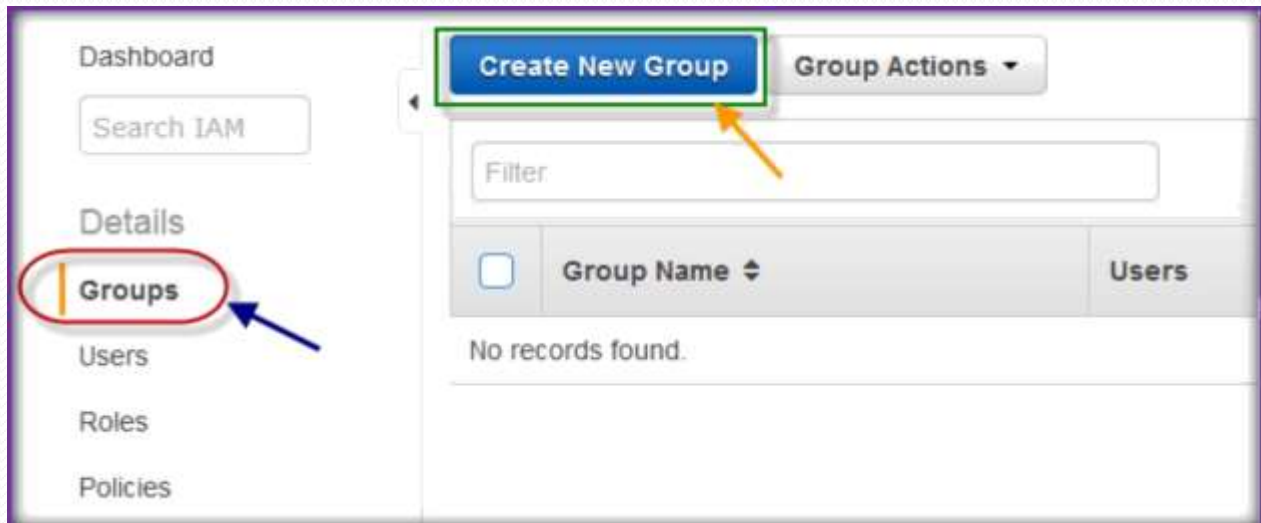
Confirm Password:

☐ Require user to create a new password at next sign-in

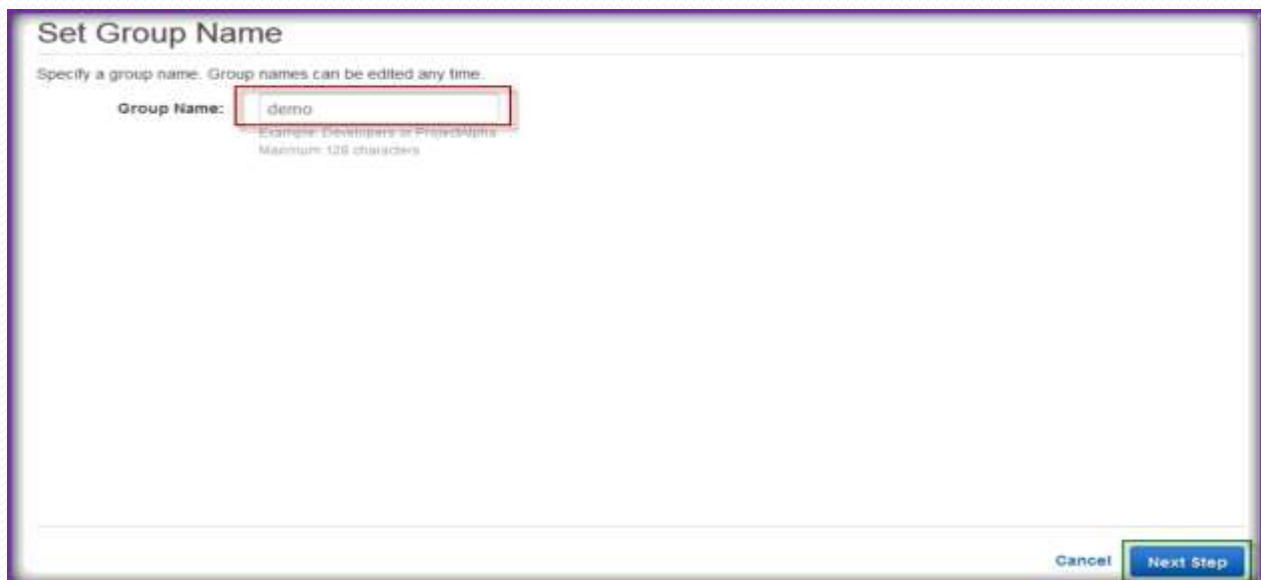
[Cancel](#) [Apply](#)

CREATING GROUPS:

Choose Groups from the left pane, then choose Create New Group to create a new one.



On next page, specify a new group name, choose next step.



On the next page, search a service name of AWS in the policy type text field, choose one or more policies for group, then choose Next Step.

Attach Policy

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

Filter: Policy Type = ec2 Showing 15 results

	Policy Name	Attached Entities	Creation Time	Edited Time
<input type="checkbox"/>	AmazonEC2ContainerService...	0	2010-04-09 21:44 UTC+0530	2010-04-09 21:44 UTC+0530
<input checked="" type="checkbox"/>	AmazonEC2FullAccess	0	2015-02-07 00:10 UTC+0530	2015-02-07 00:10 UTC+0530
<input type="checkbox"/>	AmazonEC2ReadOnlyAccess	0	2015-02-07 00:10 UTC+0530	2015-02-07 00:10 UTC+0530
<input type="checkbox"/>	AmazonEC2ReportsAccess	0	2015-02-07 00:10 UTC+0530	2015-02-07 00:10 UTC+0530
<input type="checkbox"/>	AmazonEC2RoleforAWSCode...	0	2015-05-19 23:40 UTC+0530	2015-05-19 23:40 UTC+0530
<input type="checkbox"/>	AmazonEC2RoleforDataPipel...	0	2015-02-07 00:11 UTC+0530	2016-02-22 22:54 UTC+0530
<input type="checkbox"/>	AmazonEC2RoleforSSM	0	2015-05-29 23:18 UTC+0530	2015-10-24 03:42 UTC+0530
<input type="checkbox"/>	AmazonEC2SpotFleetRole	0	2015-05-19 04:58 UTC+0530	2015-10-20 01:54 UTC+0530
<input type="checkbox"/>	AmazonElasticMapReduceforE...	0	2015-02-07 00:11 UTC+0530	2015-05-14 02:57 UTC+0530

Cancel Previous **Next Step**

On the review page, choose Create Group.

Review

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

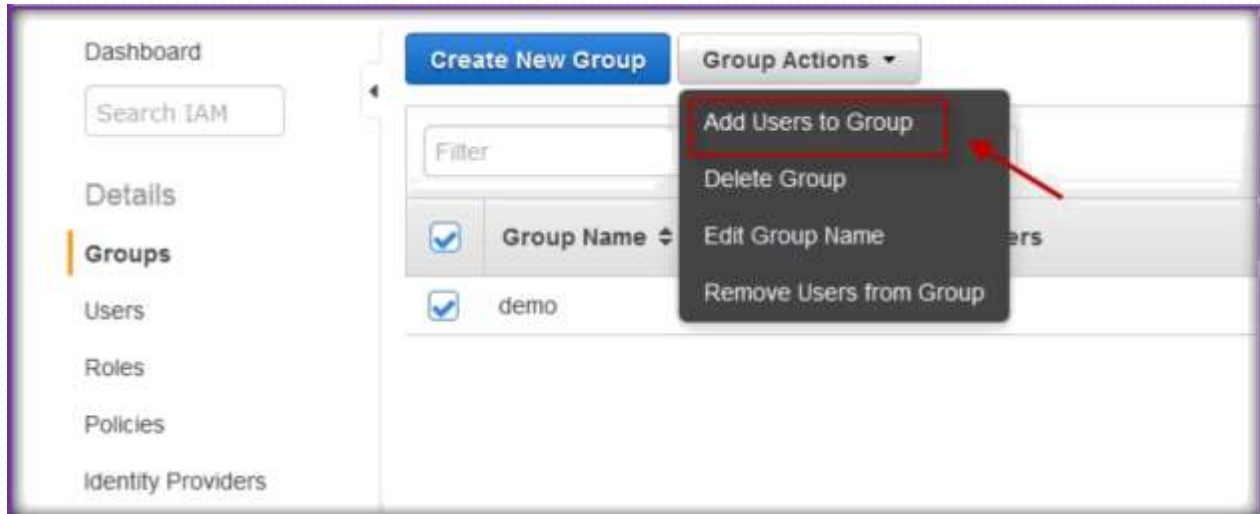
Group Name demo [Edit Group Name](#)

Policies arn:aws:iam::aws:policy/AmazonEC2FullAccess [Edit Policies](#)

Cancel Previous **Create Group**

ADDING USERS TO GROUP:

select Groups from left pane, then select the group then click Group Actions. Under group actions choose Add users to Group.



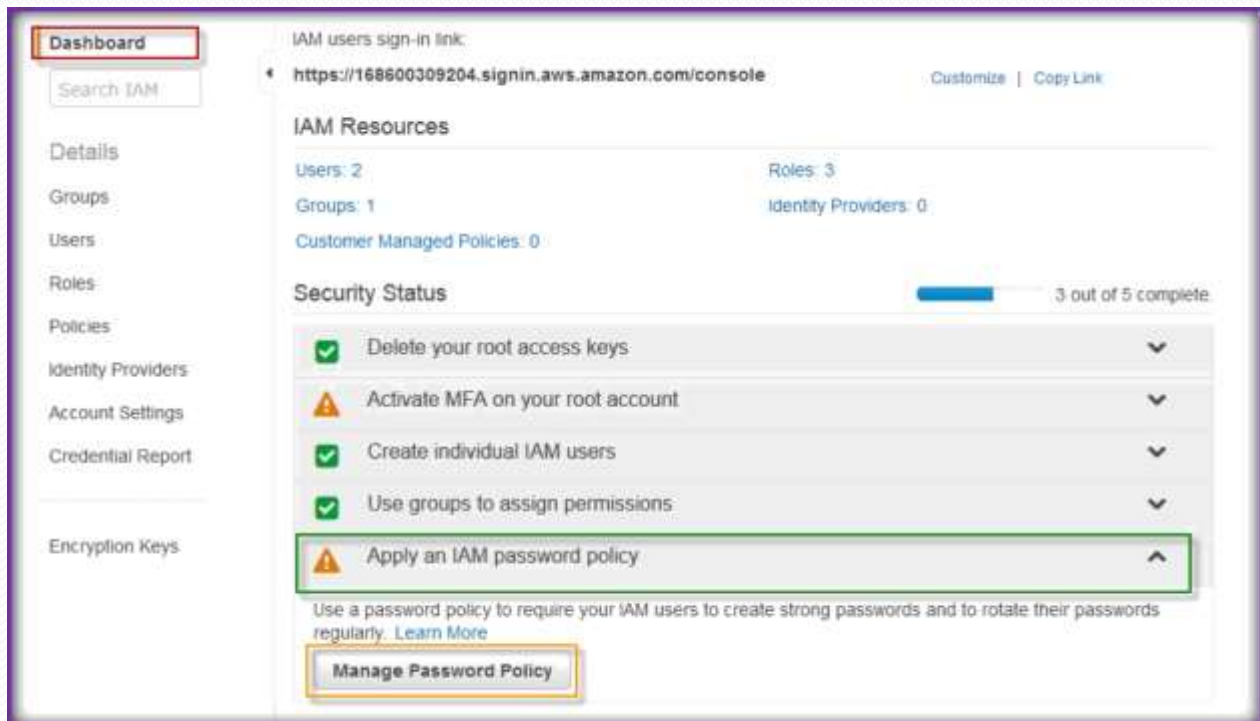
Select users from the available users list then choose Add Users.



Now selected users will be added to your group.

MANAGE PASSWORD POLICY:

Under IAM dashboard, expand Apply an IAM password policy, then choose Manage Password Policy.



Select options which you want then Apply Password policy.

▼ Password Policy

A password policy is a set of rules that define the type of password an IAM user can set. For more information about password policies, go to [Managing Passwords](#) in Using IAM.

Currently, this AWS account does not have a password policy. Specify a password policy below.

Minimum password length:

- ☒ Require at least one uppercase letter ⓘ
- ☒ Require at least one lowercase letter ⓘ
- ☒ Require at least one number ⓘ
- ☐ Require at least one non-alphanumeric character ⓘ
- ☒ Allow users to change their own password ⓘ
- ☐ Enable password expiration ⓘ
Password expiration period (in days):
- ☐ Prevent password reuse ⓘ
Number of passwords to remember:
- ☐ Password expiration requires administrator reset ⓘ

Apply password policy

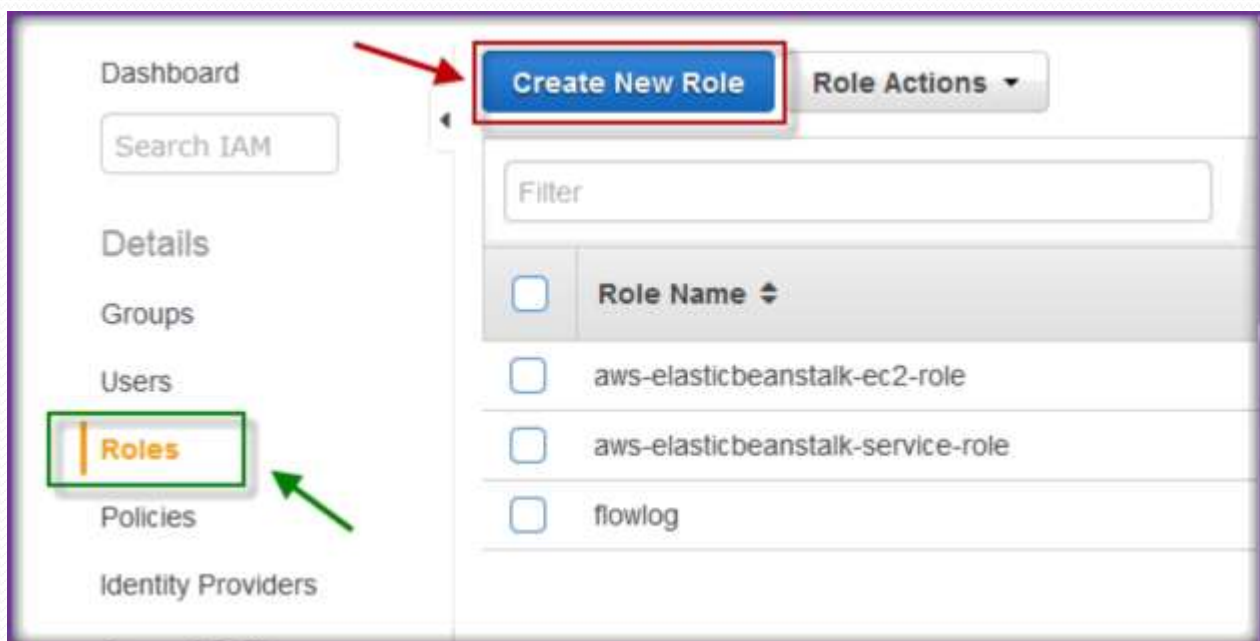
Delete password policy

ROLES: An IAM *role* is similar to a user, in that it is an AWS identity with permission policies that determine what the identity can and cannot do in AWS. However, instead of being uniquely associated with one person, a role is intended to be assumable by anyone who needs it.

Also, a role does not have any credentials (password or access keys) associated with it.

Instead, if a user is assigned to a role, access keys are created dynamically and provided to the user.

Once you are IAM dashboard, choose Roles from the left pane, then click on Create New Role.



In the next page, specify a name for role and choose Next Step.

Set Role Name

Enter a role name. You cannot edit the role name after the role is created.

Role Name

Use only alphanumeric characters, hyphens, and underscores. Do not use spaces or special characters.

Specify a name for role

Cancel Next Step

On next page, select role type, choose select button to respective AWS service.

Select Role Type

AWS Service Roles

- Amazon EC2**
Allows EC2 instances to call AWS services on your behalf. **Select**
- AWS Directory Service**
Allows AWS Directory Service to manage access for existing directory users and groups to AWS services. **Select**
- AWS Lambda**
Allows Lambda Function to call AWS services on your behalf. **Select**
- Amazon Redshift**
Allows Amazon Redshift Clusters to call AWS services on your behalf. **Select**
- Amazon API Gateway**
Allows API Gateway to call AWS resources on your behalf. **Select**

☐ Role for Cross-Account Access

☐ Role for Identity Provider Access

Cancel Previous Next Step

On the next page, search a service name of AWS in the policy type text field, choose one or more policies for group, then choose Next Step.

Attach Policy

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

Filter: Policy Type = ec2 Showing 15 results

	Policy Name	Attached Entities	Creation Time	Edited Time
<input type="checkbox"/>	AmazonEC2ContainerService...	0	2015-04-09 21:44 UTC+0530	2015-04-09 21:44 UTC+0530
<input checked="" type="checkbox"/>	AmazonEC2FullAccess	0	2015-02-07 00:10 UTC+0530	2015-02-07 00:10 UTC+0530
<input type="checkbox"/>	AmazonEC2ReadOnlyAccess	0	2015-02-07 00:10 UTC+0530	2015-02-07 00:10 UTC+0530
<input type="checkbox"/>	AmazonEC2ReportsAccess	0	2015-02-07 00:10 UTC+0530	2015-02-07 00:10 UTC+0530
<input type="checkbox"/>	AmazonEC2RoleforAWSCode...	0	2015-05-19 23:40 UTC+0530	2015-05-19 23:40 UTC+0530
<input type="checkbox"/>	AmazonEC2RoleforDataPipel...	0	2015-02-07 00:11 UTC+0530	2016-02-22 22:54 UTC+0530
<input type="checkbox"/>	AmazonEC2RoleforSSM	0	2015-05-29 23:18 UTC+0530	2015-10-24 03:42 UTC+0530
<input type="checkbox"/>	AmazonEC2SpotFleetRole	0	2015-05-19 04:58 UTC+0530	2015-10-20 01:54 UTC+0530
<input type="checkbox"/>	AmazonElasticMapReduceforE...	0	2015-02-07 00:11 UTC+0530	2015-05-14 02:57 UTC+0530

Cancel Previous **Next Step**

On the review page, choose Create Role.

Review

Review the following role information. To edit the role, click an edit link, or click **Create Role** to finish.

Role Name sandbox [Edit Role Name](#)

Role ARN arn:aws:iam::168600309204:role/sandbox

Trusted Entities The identity provider(s) ec2.amazonaws.com

Policies arn:aws:iam::aws:policy/AmazonEC2FullAccess [Change Policies](#)

Cancel Previous **Create Role**