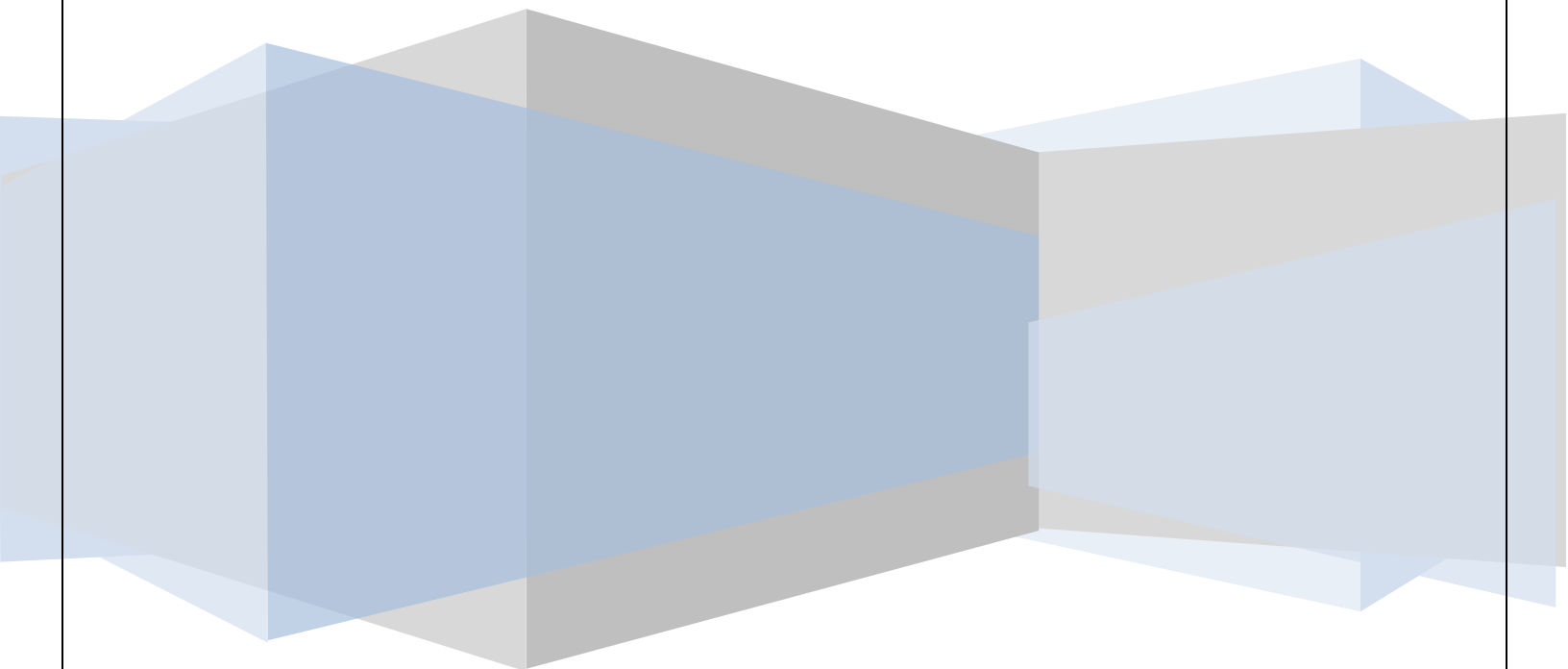


IT TOOK YOU YEARS OF EXPERIENCE
TO REACH WHERE YOU ARE TODAY.
ANOTHER **45 HOURS OF TRAINING**
WITH TACT WILL TAKE YOU HIGHER.

TACT is an online technology academy for competency training to train the IT professionals and uplift their career to discover more opportunities in the space of emerging technologies.

AWS Cloud Training

IDENTITY AND ACCESS MANAGEMENT



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*).

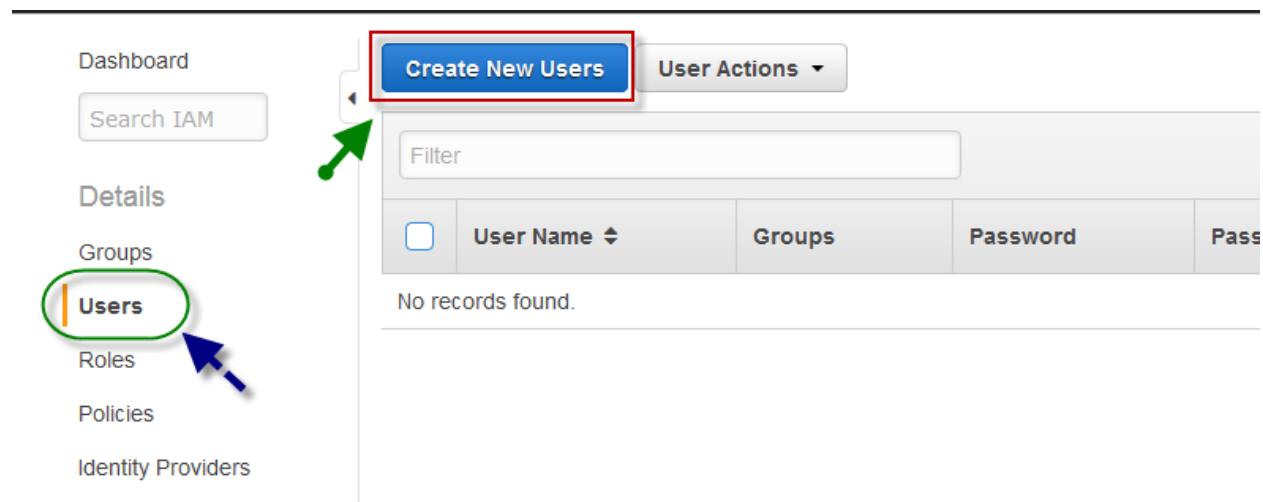
Choose Identity & Access management under Security & Identity from the AWS console page.

The screenshot displays the AWS Management Console interface, organized into several columns of service tiles. Each tile includes an icon, the service name, and a brief description. The services are categorized as follows:

- Compute:** EC2 (Virtual Servers in the Cloud), EC2 Container Service (Run and Manage Docker Containers), Elastic Beanstalk (Run and Manage Web Apps), Lambda (Run Code in Response to Events).
- Storage & Content Delivery:** S3 (Scalable Storage in the Cloud), CloudFront (Global Content Delivery Network), Elastic File System (Fully Managed File System for EC2, marked as PREVIEW), Glacier (Archive Storage in the Cloud), Snowball (Large Scale Data Transport), Storage Gateway (Hybrid Storage Integration).
- Database:** RDS (Managed Relational Database Service), DynamoDB (Managed NoSQL Database), ElastiCache (In-Memory Cache).
- Management Tools:** CodeCommit (Store Code in Private Git Repositories), CodeDeploy (Automate Code Deployments), CodePipeline (Release Software using Continuous Delivery), CloudWatch (Monitor Resources and Applications), CloudFormation (Create and Manage Resources with Templates), CloudTrail (Track User Activity and API Usage), Config (Track Resource Inventory and Changes), OpsWorks (Automate Operations with Chef), Service Catalog (Create and Use Standardized Products), Trusted Advisor (Optimize Performance and Security).
- Security & Identity:** This category is highlighted with a red circle. It includes:
 - Identity & Access Management:** Manage User Access and Encryption Keys. This service is specifically highlighted with a red arrow.
 - Directory Service:** Host and Manage Active Directory.
 - Inspector:** Analyze Application Security.
- Application Services:** AWS IoT (Connect Devices to the Cloud), Game Development (GameLift: Deploy and Scale Session-based Multiplayer Games), Mobile Services (Mobile Hub: Build, Test, and Monitor Mobile Apps; Cognito: User Identity and App Data Synchronization; Device Farm: Test Android, iOS, and Web Apps on Real Devices in the Cloud; Mobile Analytics: Collect, View and Export App Analytics; SNS: Push Notification Service), and other services like API Gateway, AppStream, CloudSearch, Elastic Transcoder, and SES.

CREATING USERS:

Once you are on IAM page, Click Users from left pane, then choose Create New Users 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.

Enter User Names:

1.
2.
3.
4.
5.

Maximum 64 characters each

☒ Generate an access key for each user

Users need access keys to make secure REST or Query protocol requests to AWS service APIs.
For users who need access to the AWS Management Console, create a password in the Users panel after completing this wizard.

Cancel

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.



✓ Your 2 User(s) have been created successfully.

This is the last time these User security credentials will be available for download.

You can manage and recreate these credentials any time

[Hide User Security Credentials](#)

Click on Show user Security Credentials

 user1	
Access Key ID: AKIAI53NKEQ7GDVQACPA	
Secret Access Key: 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	
 user2	
Access Key ID: AKIAJNQIPQABNGDC4LBQ	
Secret Access Key: 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	

Close [Download Credentials](#)

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

Dashboard

Search IAM

Details

Groups
Users
Roles
Policies
Identity Providers
Account Settings
Credential Report

Create New Users

User Actions

Filter

<input type="checkbox"/>	User Name	Password
<input checked="" type="checkbox"/>	user1	
<input type="checkbox"/>	user2	

Add User to Groups
Delete User
Manage Access Keys
Manage Password
Manage Signing Certificates
Manage MFA Device
Remove User from Groups

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:

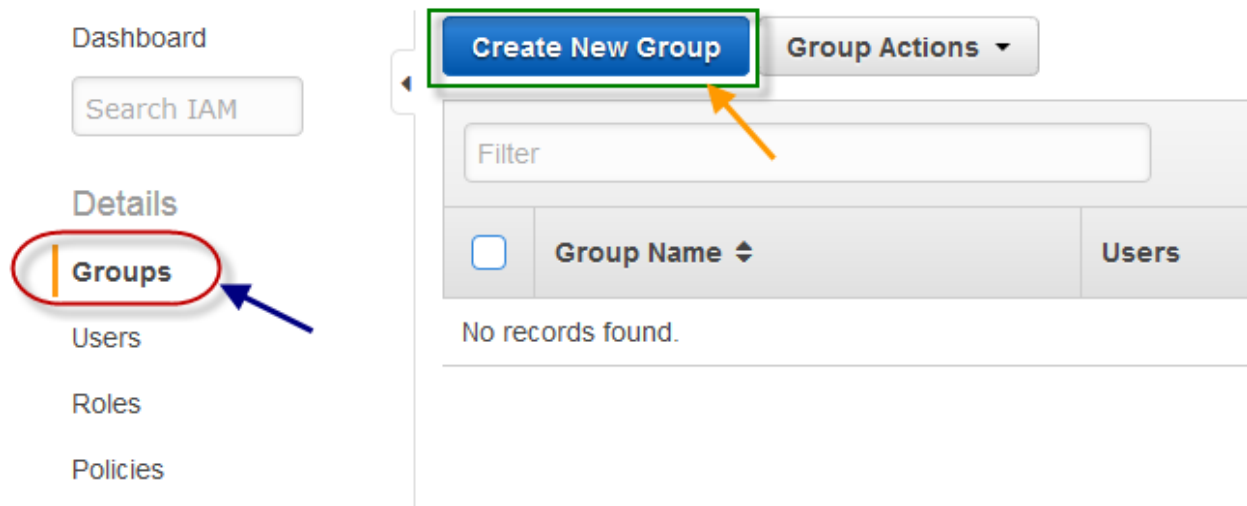
☐ Require user to create a new password at next sign-in

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.

Set Group Name

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

Group Name:

Example: Developers or ProjectAlpha
Maximum 128 characters

[Cancel](#) [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 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 Group.

Review

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

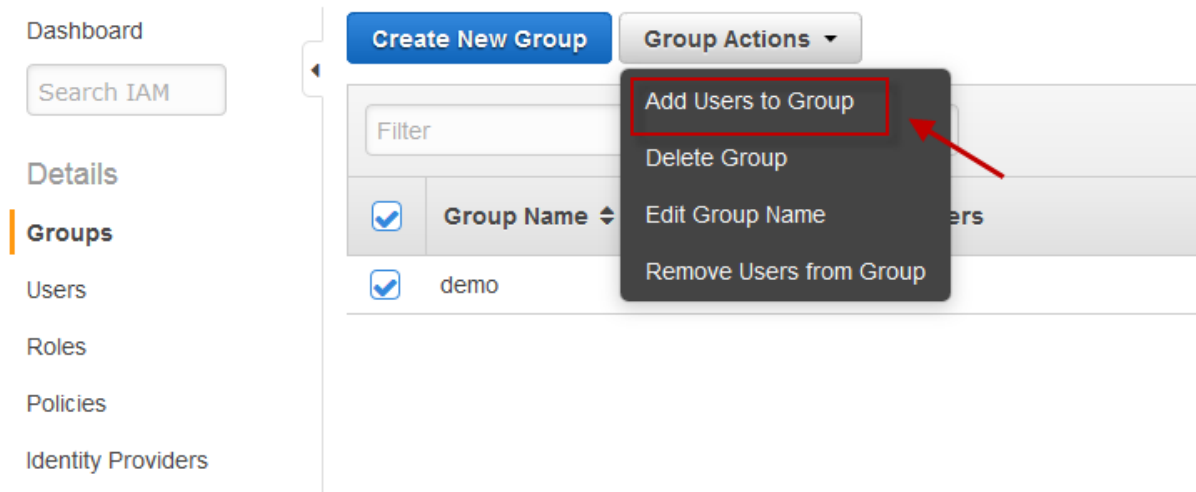
Group Name demo [Edit Group Name](#)

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.

Filter							Showing 2 results
<input type="checkbox"/>	User Name ↕	Groups	Password	Password Last Used ↕	Access Keys	Creation Time ↕	
<input checked="" type="checkbox"/>	user1	0	✓	Never	1 active	2016-04-29 21:37 U...	
<input type="checkbox"/>	user2	0		N/A	1 active	2016-04-29 21:37 U...	

Cancel **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.

The screenshot shows the AWS IAM console interface. On the left is a navigation menu with 'Dashboard' highlighted. The main content area shows the 'IAM users sign-in link' and 'IAM Resources' summary. The 'Security Status' section is expanded, showing a progress bar for '3 out of 5 complete'. A list of security checks is displayed, with 'Apply an IAM password policy' highlighted by a green box. Below this list, a 'Manage Password Policy' button is highlighted by an orange box.

Dashboard

Search IAM

Details

Groups

Users

Roles

Policies

Identity Providers

Account Settings

Credential Report

Encryption Keys

IAM users sign-in link: <https://168600309204.signin.aws.amazon.com/console> [Customize](#) | [Copy Link](#)

IAM Resources

Users: 2 Roles: 3

Groups: 1 Identity Providers: 0

Customer Managed Policies: 0

Security Status 3 out of 5 complete.

- ☒ Delete your root access keys
- ☐ Activate MFA on your root account
- ☒ Create individual IAM users
- ☒ Use groups to assign permissions
- ☐ Apply an IAM password policy

Use a password policy to require your IAM users to create strong passwords and to rotate their passwords regularly. [Learn More](#)

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

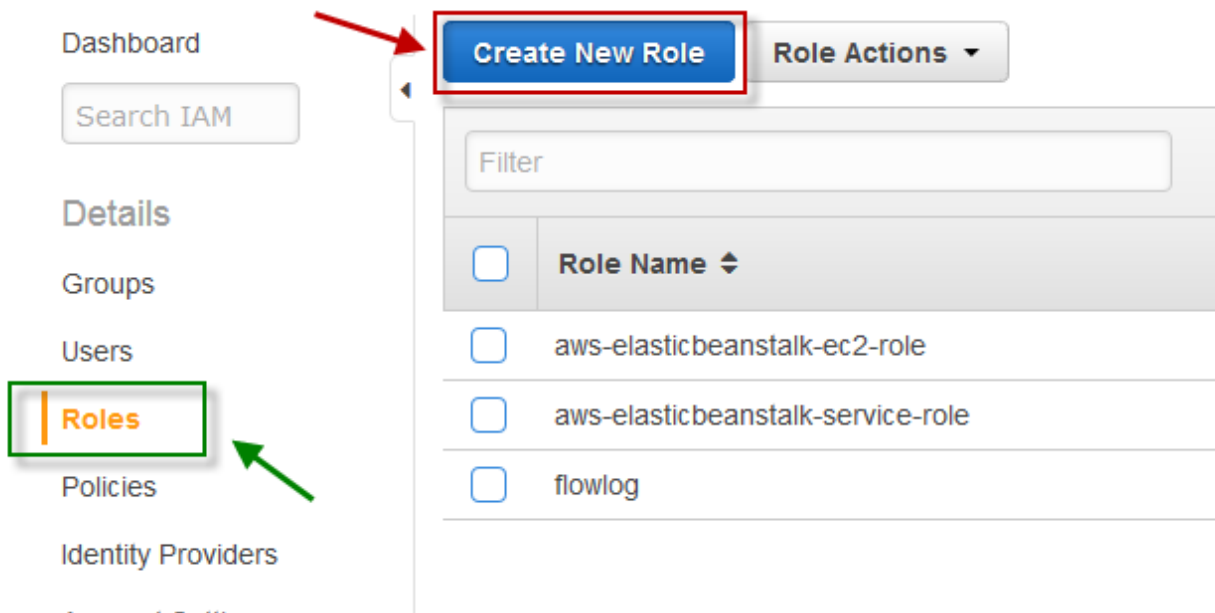
Delete password policy

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

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

:ap-southeast-1#

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 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

in-southeast-1

Cancel Previous **Create Role**