

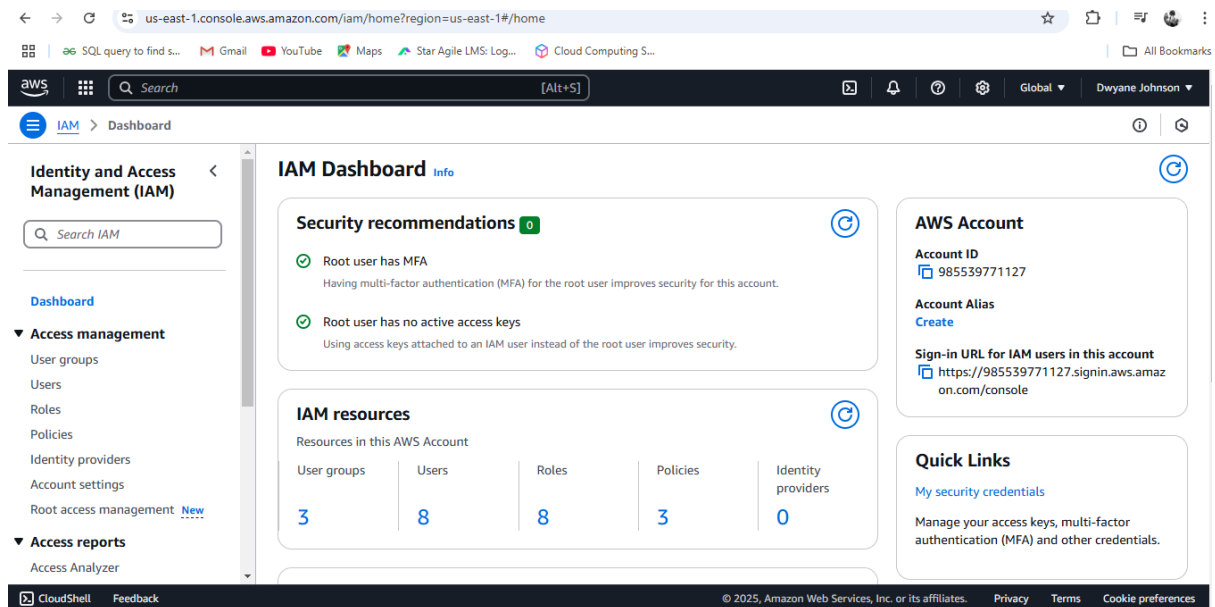
Submitted by: Mohammed Saquib

Date: 13/01/2025

Batch no: DevOps SA2412033

## L2 - Login to AWS Console and Create IAM User, Role, and Group

### Step1: Login to AWS account as a Root user



## Step2: Click on users

The screenshot shows the AWS IAM console 'Users' page. The left sidebar contains the 'Identity and Access Management (IAM)' menu with options like Dashboard, Access management, Users, Roles, Policies, Identity providers, Account settings, Root access management, Access reports, and Access Analyzer. The main content area displays a list of 8 users: Admin, Chris\_Gayle, James\_Bond, Kane, Randy-Orton, Test-new-user, and TripleH. Each user entry includes a checkbox, user name, path, group, last activity, MFA status, password age, and console access status. At the top right of the main area, there are 'Delete' and 'Create user' buttons. The bottom of the page shows the AWS logo, a search bar, and navigation links for CloudShell and Feedback.

|                          | User name                     | Path | Groups | Last activity | MFA | Password age | Cons... |
|--------------------------|-------------------------------|------|--------|---------------|-----|--------------|---------|
| <input type="checkbox"/> | <a href="#">Admin</a>         | /    | 1      | 9 days ago    | -   | 9 days       | Janua   |
| <input type="checkbox"/> | <a href="#">Chris_Gayle</a>   | /    | 1      | 4 hours ago   | -   | 4 hours      | Janua   |
| <input type="checkbox"/> | <a href="#">James_Bond</a>    | /    | 1      | 5 hours ago   | -   | 5 hours      | Janua   |
| <input type="checkbox"/> | <a href="#">Kane</a>          | /    | 0      | 9 days ago    | -   | 9 days       | Janua   |
| <input type="checkbox"/> | <a href="#">Randy-Orton</a>   | /    | 1      | 7 days ago    | -   | 9 days       | Janua   |
| <input type="checkbox"/> | <a href="#">Test-new-user</a> | /    | 0      | 7 days ago    | -   | 7 days       | Janua   |
| <input type="checkbox"/> | <a href="#">TripleH</a>       | /    | 0      | 9 days ago    | -   | 9 days       | Janua   |

## Step3: Click on Create user

The screenshot shows the AWS IAM console 'Create user' page. The left sidebar shows the 'IAM > Users > Create user' breadcrumb and a progress indicator for four steps: Step 2 (Set permissions), Step 3 (Review and create), Step 4 (Retrieve password), and a final step (Retrieve password). The main content area is titled 'User details' and contains a 'User name' field with the value 'Assignment'. Below this, there is a checkbox labeled 'Provide user access to the AWS Management Console - optional' which is checked. A note explains that if console access is provided, it's a best practice to manage access in IAM Identity Center. A section titled 'Are you providing console access to a person?' contains two radio button options: 'Specify a user in Identity Center - Recommended' and 'I want to create an IAM user'. The 'I want to create an IAM user' option is selected. Below this, there is a 'Console password' section.

**User details**

**User name**

Assignment

The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ \_ - (hyphen)

☒ **Provide user access to the AWS Management Console - optional**  
If you're providing console access to a person, it's a [best practice](#) to manage their access in IAM Identity Center.

**Are you providing console access to a person?**

**User type**

☐ Specify a user in Identity Center - Recommended  
We recommend that you use Identity Center to provide console access to a person. With Identity Center, you can centrally manage user access to their AWS accounts and cloud applications.

☒ I want to create an IAM user  
We recommend that you create IAM users only if you need to enable programmatic access through access keys, service-specific credentials for AWS CodeCommit or Amazon Keyspaces, or a backup credential for emergency account access.

**Console password**

## Step4: Give the user details

us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/users/create

SQL query to find s... Gmail YouTube Maps Star Agile LMS: Log... Cloud Computing S... All Bookmarks

aws Search [Alt+S] Global Dwayne Johnson

IAM > Users > Create user

**Console password**

☐ Autogenerated password  
You can view the password after you create the user.

☒ Custom password  
Enter a custom password for the user.

\*\*\*\*\*

- Must be at least 8 characters long
- Must include at least three of the following mix of character types: uppercase letters (A-Z), lowercase letters (a-z), numbers (0-9), and symbols ! @ # \$ % ^ & \* ( ) \_ + - (hyphen) = [ ] { } ' "

☐ Show password

☒ Users must create a new password at next sign-in - Recommended  
Users automatically get the [IAMUserChangePassword](#) policy to allow them to change their own password.

**Info** If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspaces, you can generate them after you create this IAM user. [Learn more](#)

Cancel Next

## Step5: Attach policies/permissions

us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/users/create

SQL query to find s... Gmail YouTube Maps Star Agile LMS: Log... Cloud Computing S... All Bookmarks

aws Search [Alt+S] Global Dwayne Johnson

IAM > Users > Create user

Step 1 Specify user details  
Step 2 **Set permissions**  
Step 3 Review and create  
Step 4 Retrieve password

**Set permissions**  
Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. [Learn more](#)

**Permissions options**

☐ Add user to group  
Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.

☐ Copy permissions  
Copy all group memberships, attached managed policies, and inline policies from an existing user.

☒ Attach policies directly  
Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

**Permissions policies (1/1321)** [Create policy](#)

Choose one or more policies to attach to your new user.

Filter by Type

Ec2 All types 44 matches

| Policy name | Type | Attached entities |
|-------------|------|-------------------|
|-------------|------|-------------------|

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

## Step6: Review the details and create the user

The screenshot shows the AWS IAM console 'Create user' wizard at the 'Review and create' step. The left sidebar shows the progress: Step 1 (Specify user details), Step 2 (Set permissions), Step 3 (Review and create - active), and Step 4 (Retrieve password). The main content area is titled 'Review and create' and includes a sub-header 'Review your choices. After you create the user, you can view and download the autogenerated password, if enabled.'

**User details**

|                         |  |                               |
|-------------------------|--|-------------------------------|
| User name<br>Assignment | Console password type<br>Custom password | Require password reset<br>Yes |
|-------------------------|--|-------------------------------|

**Permissions summary**

| Name                                  | Type        | Used as            |
|---------------------------------------|-------------|--------------------|
| <a href="#">AmazonEC2FullAccess</a>   | AWS managed | Permissions policy |
| <a href="#">IAMUserChangePassword</a> | AWS managed | Permissions policy |

**Tags - optional**  
Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.  
No tags associated with the resource.  
[Add new tag](#)  
You can add up to 50 more tags.

At the bottom right, there are 'Cancel' and 'Previous' buttons.

## Step7: User “Assignment” has been created

The screenshot shows the AWS IAM console 'Create user' wizard at the 'Retrieve password' step. The left sidebar shows the progress: Step 1 (Specify user details), Step 2 (Set permissions), Step 3 (Review and create), and Step 4 (Retrieve password - active). A green success message at the top states: 'User created successfully. You can view and download the user's password and email instructions for signing in to the AWS Management Console. [View user]'. The main content area is titled 'Retrieve password' and includes a sub-header 'Retrieve password. You can view and download the user's password below or email users instructions for signing in to the AWS Management Console. This is the only time you can view and download this password.'

**Console sign-in details**

[Email sign-in instructions](#)

Console sign-in URL  
<https://985539771127.signin.aws.amazon.com/console>

User name  
[Assignment](#)

Console password  
\*\*\*\*\* [Show](#)

At the bottom, there are 'Cancel', 'Download .csv file', and 'Return to users list' buttons.

us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/users

SQL query to find s... Gmail YouTube Maps Star Agile LMS: Log... Cloud Computing S... All Bookmarks

Search [Alt+S]

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Root access management

Access reports

Access Analyzer

External access

Unused access

User created successfully

You can view and download the user's password and email instructions for signing in to the AWS Management Console.

View user

Users (9)

An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

Search

| <input type="checkbox"/> | User name   | Path | Group | Last activity | MFA | Password age | Console last sign-in      | Access key ID | Active key as |
|--------------------------|-------------|------|-------|---------------|-----|--------------|---------------------------|---------------|---------------|
| <input type="checkbox"/> | Admin       | /    | 1     | 9 days ago    | -   | 9 days       | January 04, 2025, 12:2... | -             | -             |
| <input type="checkbox"/> | Assignment  | /    | 0     | 1 minute ago  | -   | -            | January 13, 2025, 16:0... | -             | -             |
| <input type="checkbox"/> | Chris_Gayle | /    | 1     | 5 hours ago   | -   | 5 hours      | January 13, 2025, 10:5... | -             | -             |
| <input type="checkbox"/> | James_Bond  | /    | 1     | 5 hours ago   | -   | 5 hours      | January 13, 2025, 10:5... | -             | -             |
| <input type="checkbox"/> | Kane        | /    | 0     | 9 days ago    | -   | 9 days       | January 04, 2025, 12:2... | -             | -             |
| <input type="checkbox"/> | Randy-Orton | /    | 1     | 7 days ago    | -   | 9 days       | January 05, 2025, 18:4... | -             | -             |

## Step8: Login to IAM user

eu-north-1.signin.aws.amazon.com/oauth?client\_id=arn%3Aaws%3Asignin%3A%3A%3Aconsole%2Fcanvas&code\_challenge=YmFRH8DTSmcWlzp0-6S4l3b1... Incognito

SQL query to find s... Gmail YouTube Maps Star Agile LMS: Log... Cloud Computing S... All Bookmarks

IAM user sign in

Account ID (12 digits) or account alias

985539771127

IAM username

Assignment

Password

.....

☐ Show Password [Having trouble?](#)

Sign in

Sign in using root user email

[Create a new AWS account](#)

☐ Remember this account

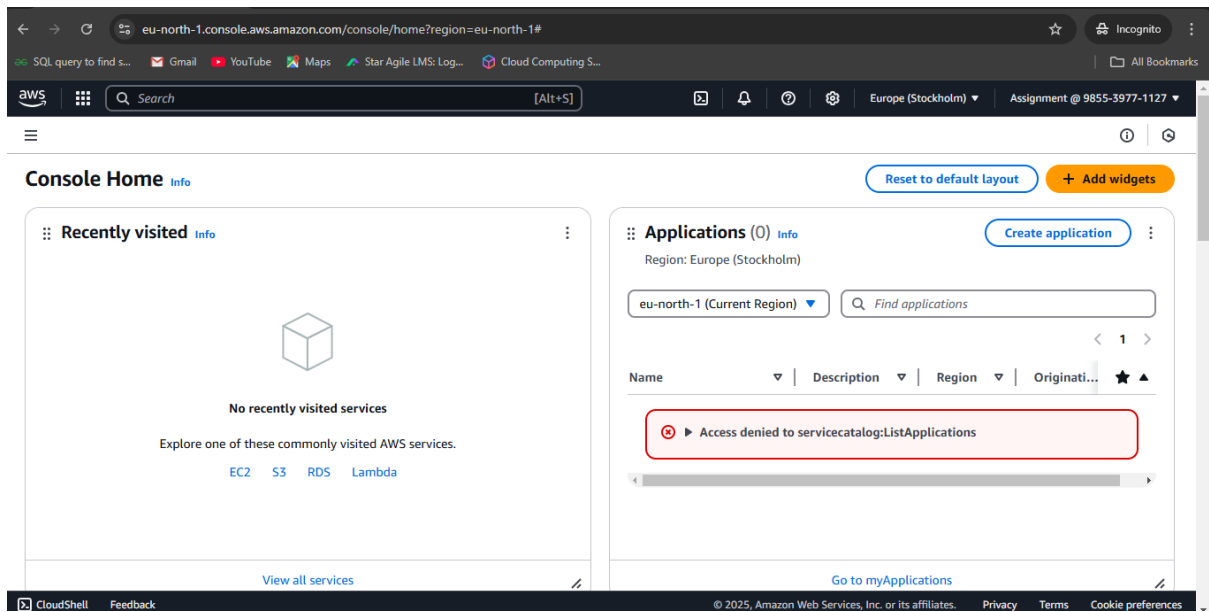
By continuing, you agree to [AWS Customer Agreement](#) or other agreement for AWS services, and the [Privacy Notice](#). This site uses essential cookies. See our [Cookie Notice](#) for more.

Amazon Lightsail

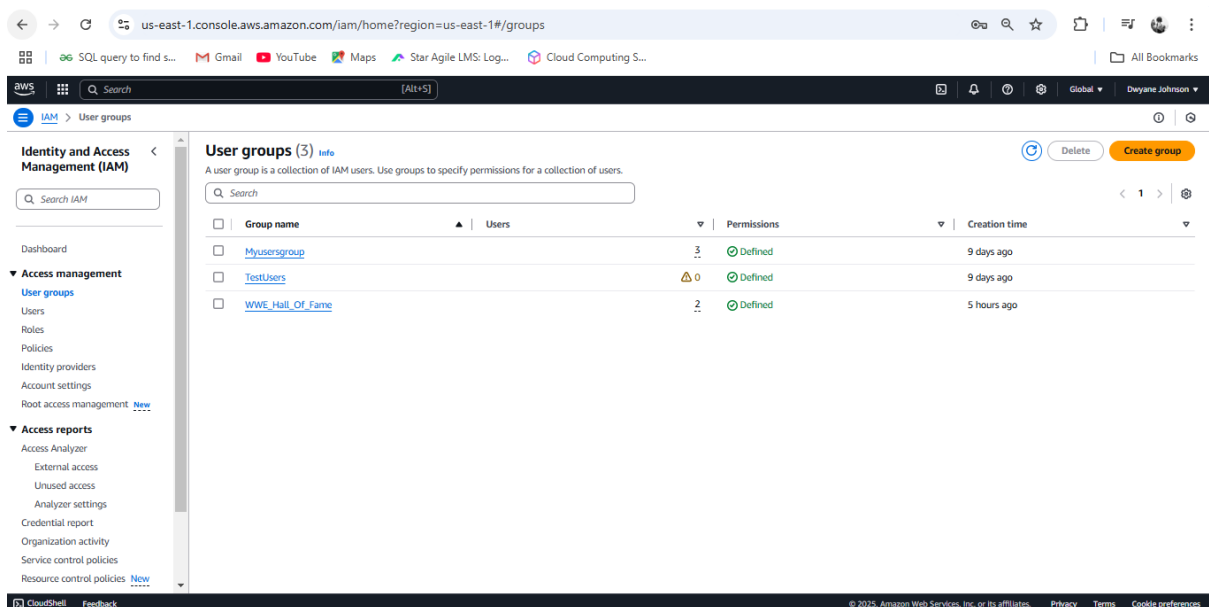
Lightsail is the easiest way to get started on AWS

[Learn more »](#)

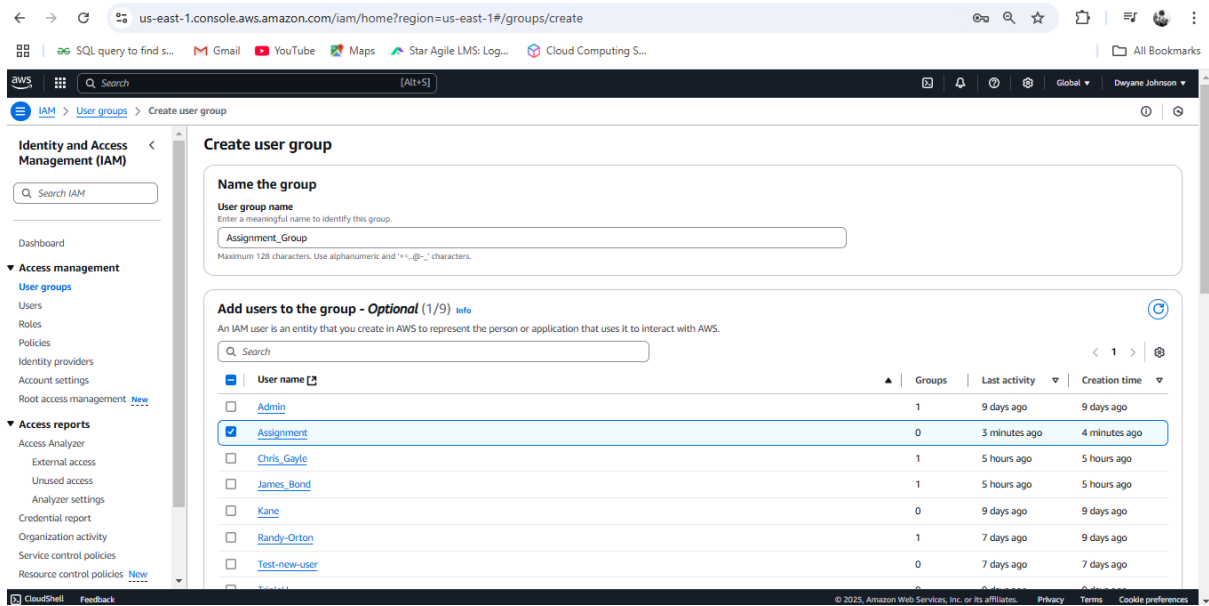
## Step9: IAM user home page



## Step 10: Creating group



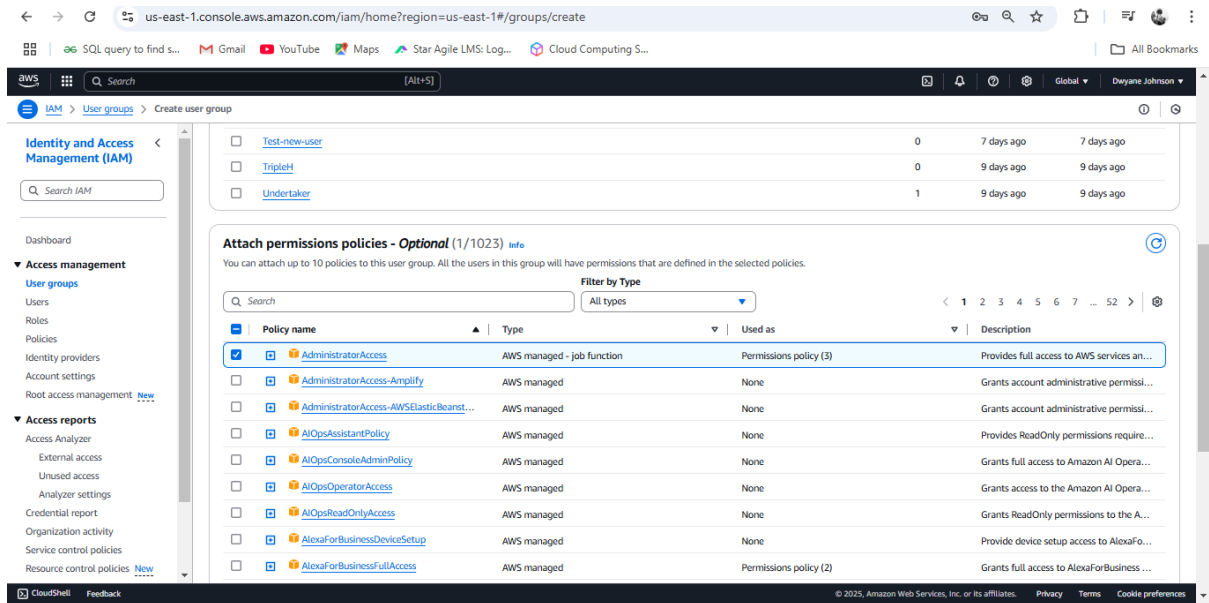
## Step 11: Filling group details



The screenshot shows the AWS IAM console 'Create user group' page. The 'Name the group' section has 'Assignment\_Group' entered. The 'Add users to the group' section shows a list of users with 'Assignment' selected.

| User name                                      | Groups | Last activity | Creation time |
|--|--------|---------------|---------------|
| <input type="checkbox"/> Admin                 | 1      | 9 days ago    | 9 days ago    |
| <input checked="" type="checkbox"/> Assignment | 0      | 3 minutes ago | 4 minutes ago |
| <input type="checkbox"/> Chris_Gayle           | 1      | 5 hours ago   | 5 hours ago   |
| <input type="checkbox"/> James_Bond            | 1      | 5 hours ago   | 5 hours ago   |
| <input type="checkbox"/> Kane                  | 0      | 9 days ago    | 9 days ago    |
| <input type="checkbox"/> Randy-Orton           | 1      | 7 days ago    | 9 days ago    |
| <input type="checkbox"/> Test-new-user         | 0      | 7 days ago    | 7 days ago    |

## Step12: Attaching policies



The screenshot shows the AWS IAM console 'Create user group' page. The 'Attach permissions policies' section shows a list of policies with 'AdministratorAccess' selected.

| Policy name  | Type                       | Used as                | Description                                |
|--|----------------------------|------------------------|--|
| <input checked="" type="checkbox"/> AdministratorAccess          | AWS managed - job function | Permissions policy (3) | Provides full access to AWS services an... |
| <input type="checkbox"/> AdministratorAccess-Amplify             | AWS managed                | None                   | Grants account administrative permissi...  |
| <input type="checkbox"/> AdministratorAccess-AWSElasticBeanst... | AWS managed                | None                   | Grants account administrative permissi...  |
| <input type="checkbox"/> AIOpsAssistantPolicy                    | AWS managed                | None                   | Provides ReadOnly permissions require...   |
| <input type="checkbox"/> AIOpsConsoleAdminPolicy                 | AWS managed                | None                   | Grants full access to Amazon AI Opera...   |
| <input type="checkbox"/> AIOpsOperatorAccess                     | AWS managed                | None                   | Grants access to the Amazon AI Opera...    |
| <input type="checkbox"/> AIOpsReadOnlyAccess                     | AWS managed                | None                   | Grants ReadOnly permissions to the A...    |
| <input type="checkbox"/> AlexaForBusinessDeviceSetup             | AWS managed                | None                   | Provide device setup access to AlexaFo...  |
| <input type="checkbox"/> AlexaForBusinessFullAccess              | AWS managed                | Permissions policy (2) | Grants full access to AlexaForBusiness ... |

## Step13: Group got created

us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/groups

Assignment\_Group user group created. View group

### User groups (4)

A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

Search

| <input type="checkbox"/> | Group name       | Users | Permissions | Creation time |
|--------------------------|------------------|-------|-------------|---------------|
| <input type="checkbox"/> | Assignment_Group | 1     | Defined     |               |
| <input type="checkbox"/> | Myusersgroup     | 3     | Defined     | 9 days ago    |
| <input type="checkbox"/> | TestUsers        | 0     | Defined     | 9 days ago    |
| <input type="checkbox"/> | WWE_Hall_Of_Fame | 2     | Defined     | 5 hours ago   |

Dashboard

Access management

- User groups
- Users
- Roles
- Policies
- Identity providers
- Account settings
- Root access management

Access reports

- Access Analyzer
- External access
- Unused access
- Analyzer settings

## Step 14: Creating Roles

us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/roles

Assignment\_Group user group created. Delete Create role

### Roles (8)

An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

Search

| <input type="checkbox"/> | Role name                                | Trusted entities               | Last activity |
|--------------------------|--|--------------------------------|---------------|
| <input type="checkbox"/> | Admin-access-for-test-new-user           | Account: 985539771127          | 4 hours ago   |
| <input type="checkbox"/> | AWSServiceRoleForAmazonElasticFileSystem | AWS Service: elasticfilesystem | 3 hours ago   |
| <input type="checkbox"/> | AWSServiceRoleForBackup                  | AWS Service: backup            | 5 hours ago   |
| <input type="checkbox"/> | AWSServiceRoleForSupport                 | AWS Service: support           | -             |
| <input type="checkbox"/> | AWSServiceRoleForTrustedAdvisor          | AWS Service: trustedadvisor    | -             |
| <input type="checkbox"/> | EC2-S3-role                              | AWS Service: ec2               | -             |
| <input type="checkbox"/> | role_for_Lambda_to_S3                    | AWS Service: lambda            | -             |
| <input type="checkbox"/> | WWE_Role_Lambda                          | AWS Service: lambda            | -             |

Roles Anywhere

Authenticate your non AWS workloads and securely provide access to AWS services.

Access AWS from your non AWS workloads

Operate your non AWS workloads using the same authentication and authorization strategy that you use within AWS.

X.509 Standard

Use your own existing PKI infrastructure or use AWS Certificate Manager Private Certificate Authority to authenticate identities.

Temporary credentials

Use temporary credentials with ease and benefit from the enhanced security of temporary credentials.

Manage

Dashboard

Access management

- User groups
- Users
- Roles
- Policies
- Identity providers
- Account settings
- Root access management

Access reports

- Access Analyzer
- External access
- Unused access
- Analyzer settings
- Credential report
- Organization activity
- Service control policies
- Resource control policies



## Step 15: Filling details

us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/roles/create

SQL query to find s... Gmail YouTube Maps Star Agile LMS: Log... Cloud Computing S... All Bookmarks

aws Search [Alt+S]

IAM > Roles > Create role

Step 1  
Step 2  
Step 3

Select trusted entity

Trusted entity type

☒ AWS service  
Allow AWS services like EC2, Lambda, or others to perform actions in this account.

☐ AWS account  
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

☐ Web identity  
Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.

☐ SAML 2.0 federation  
Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.

☐ Custom trust policy  
Create a custom trust policy to enable others to perform actions in this account.

Use case  
Allow an AWS service like EC2, Lambda, or others to perform actions in this account.

Service or use case  
Lambda

Choose a use case for the specified service.  
Use case  
☒ Lambda  
Allows Lambda functions to call AWS services on your behalf.

Cancel Next

## Step 16: Giving permission

us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/roles/create?trustedEntityType=AWS\_SERVICE&selectedService=Lambda&selecte...

SQL query to find s... Gmail YouTube Maps Star Agile LMS: Log... Cloud Computing S... All Bookmarks

aws Search [Alt+S]

IAM > Roles > Create role

Step 1  
Step 2  
Step 3

Add permissions

Permissions policies (1/1023)  
Choose one or more policies to attach to your new role.

Filter by Type  
All types 14 matches

| Policy name   | Type        | Description                                  |
|---|-------------|--|
| <input type="checkbox"/> AmazonDMSRedshiftS3Role                      | AWS managed | Provides access to manage S3 settings ...    |
| <input checked="" type="checkbox"/> AmazonS3FullAccess                | AWS managed | Provides full access to all buckets via t... |
| <input type="checkbox"/> AmazonS3ObjectLambdaExecutionRolePolicy      | AWS managed | Provides AWS Lambda functions perm...        |
| <input type="checkbox"/> AmazonS3OutpostsFullAccess                   | AWS managed | Provides full access to Amazon S3 on ...     |
| <input type="checkbox"/> AmazonS3OutpostsReadOnlyAccess               | AWS managed | Provides read only access to Amazon S...     |
| <input type="checkbox"/> AmazonS3ReadOnlyAccess                       | AWS managed | Provides read only access to all bucket...   |
| <input type="checkbox"/> AmazonS3TablesFullAccess                     | AWS managed | Provides full access to all S3 table buc...  |
| <input type="checkbox"/> AmazonS3TablesReadOnlyAccess                 | AWS managed | Provides read only access to all S3 tabl...  |
| <input type="checkbox"/> AWSBackupServiceRolePolicyForS3Backup        | AWS managed | Policy containing permissions necessar...    |
| <input type="checkbox"/> AWSBackupServiceRolePolicyForS3Restore       | AWS managed | Policy containing permissions necessar...    |
| <input type="checkbox"/> AWSQuickSetupSSMDeploymentS3BucketRolePolicy | AWS managed | This policy grants permissions for listin... |

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

## Step17: Giving Role name and creating Role

us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/roles/create?trustedEntityType=AWS\_SERVICE&selectedService=Lambda&selecte... All Bookmarks

SQL query to find s... Gmail YouTube Maps Star Agile LMS: Log... Cloud Computing S...

aws Search [Alt+S]

iam > Roles > Create role

● Add permissions  
Step 1  
● Name, review, and create

### Role details

**Role name**  
Enter a meaningful name to identify this role.  
  
Maximum 64 characters. Use alphanumeric and "+, -, @, \_" characters.

**Description**  
Add a short explanation for this role.  
  
Maximum 1000 characters. Use letters (A-Z and a-z), numbers (0-9), tabs, new lines, or any of the following characters: "\_+=~@-/\[\]{}!%\*^()~""

**Step 1: Select trusted entities** [Edit](#)

**Trust policy**

```
1- {  
2-   "Version": "2012-10-17",  
3-   "Statement": [  
4-     {  
5-       "Effect": "Allow",  
6-       "Action": [  
7-         "sts:AssumeRole"  
8-       ],  
9-       "Principal": {  
10-        "Service": [  
11-          "lambda.amazonaws.com"  
12-        ]  
13-      }  
14-    ]  
15-  }  
16- }
```

CloudShell Feedback © 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/roles/create?trustedEntityType=AWS\_SERVICE&selectedService=Lambda&selecte... All Bookmarks

SQL query to find s... Gmail YouTube Maps Star Agile LMS: Log... Cloud Computing S...

aws Search [Alt+S]

iam > Roles > Create role

8-  
9-  
10-  
11-  
12-  
13-  
14-  
15-  
16- }

**Step 2: Add permissions** [Edit](#)

**Permissions policy summary**

| Policy name                        | Type        | Attached as        |
|------------------------------------|-------------|--------------------|
| <a href="#">AmazonS3FullAccess</a> | AWS managed | Permissions policy |

**Step 3: Add tags**

**Add tags - optional** [Info](#)

Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.  
No tags associated with the resource.

[Add new tag](#)

You can add up to 50 more tags.

[Cancel](#) [Previous](#) [Create role](#)

## Stp18: Role got created

us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/roles

SQL query to find s... Gmail YouTube Maps Star Agile LMS: Log... Cloud Computing S... All Bookmarks

**Identity and Access Management (IAM)**

Search IAM

Dashboard

**Access management**

- User groups
- Users
- Roles**
- Policies
- Identity providers
- Account settings
- Root access management New

**Access reports**

- Access Analyzer
- External access
- Unused access
- Analyzer settings
- Credential report
- Organization activity
- Service control policies

**Role Assignment\_Role created.** [View role](#)

**Roles (9)** [Info](#) [Delete](#) [Create role](#)

An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

Search

| <input type="checkbox"/> | Role name  | Trusted entities                                     | Last activity |
|--------------------------|--|--|---------------|
| <input type="checkbox"/> | <a href="#">Admin-access-for-test-new-user</a>           | Account: 985539771127                                | 4 hours ago   |
| <input type="checkbox"/> | <b>Assignment_Role</b>                                   | AWS Service: lambda                                  | -             |
| <input type="checkbox"/> | <a href="#">AWSServiceRoleForAmazonElasticFileSystem</a> | AWS Service: elasticfilesystem (Service-Linked Role) | 3 hours ago   |
| <input type="checkbox"/> | <a href="#">AWSServiceRoleForBackup</a>                  | AWS Service: backup (Service-Linked Role)            | 5 hours ago   |
| <input type="checkbox"/> | <a href="#">AWSServiceRoleForSupport</a>                 | AWS Service: support (Service-Linked Role)           | -             |
| <input type="checkbox"/> | <a href="#">AWSServiceRoleForTrustedAdvisor</a>          | AWS Service: trustedadvisor (Service-Linked Role)    | -             |
| <input type="checkbox"/> | <a href="#">EC2-S3-role</a>                              | AWS Service: ec2                                     | -             |
| <input type="checkbox"/> | <a href="#">role_for_Lambda_to_S3</a>                    | AWS Service: lambda                                  | -             |
| <input type="checkbox"/> | <a href="#">WWE_Role_Lambda</a>                          | AWS Service: lambda                                  | -             |

**Roles Anywhere** [Info](#) [Manage](#)

Authenticate your non AWS workloads and securely provide access to AWS services.