

NAME - SHUBHANGI SINGH  
E-MAIL - [singh.dimp12397@gmail.com](mailto:singh.dimp12397@gmail.com)

# ASSIGNMENT - 1

The image displays two screenshots of the AWS IAM Management Console. The top screenshot shows the IAM dashboard for a user named 'shubhangi1997'. The dashboard includes sections for 'IAM resources' (Users: 0, Groups: 2, Policies: 0), 'Security alerts', 'Best practices', and 'Additional information'. The bottom screenshot shows the 'Add user' wizard, which is a multi-step process for creating a new user. The first step, 'Details', is currently active, showing the 'User name' field and the 'Access type' selection. The 'Access type' options are 'Programmatic access' (selected) and 'AWS Management Console access'. The 'Programmatic access' option is selected, and the 'Access key ID and secret access key' are provided. The 'Add user' button is visible at the bottom right of the wizard.

ServicesResource GroupsCloudWatchDynamoDBgeneralprod

Add user

1234

DetailsPermissionsReviewComplete

Set user details

You can add multiple users at once with the same access type and permissions. [Learn more](#)

User name\*

gsaul-dev-s3

gsaul-dev-ec2+ids

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

Download .csv

ServicesResource GroupsCloudWatchDynamoDBgeneralprod

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

Show password

Require password reset

☒ Users must create a new password at next sign-in

Users automatically get the IAMUserChangePassword policy to allow them to change their own password.

\* Required

CancelNext: Per

FeedbackEnglish (US)

© 2009 - 2017, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.

Download .csv

ServicesResource GroupsCloudWatchDynamoDBgeneralprod

DetailsPermissionsReviewComplete

Review

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

User details

User names

gsaul-dev-s3 and gsaul-dev-ec2+ids

AWS access type

Programmatic access and AWS Management Console access

Console password type

Custom

Require password reset

Yes

Permissions summary

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

Type	Name
Managed policy	IAMUserChangePassword

CancelPreviousComplete

FeedbackEnglish (US)

© 2009 - 2017, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.

Download .csv

ServicesResource GroupsCloudWatchDynamoDBgeneralprod

Add user

123

DetailsPermissionsReviewComplete

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 first 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://581977599153.signin.aws.amazon.com/console>

Download .csv

User	Access key ID	Secret access key	Email login instructions
gsaul-dev-s3	AKIAQFDXTNTOKAZPOMQ	***** Show	Send email
gsaul-dev-ec2+ids	AKIAJUNARCHMOEIQDMA	***** Show	Send email

FeedbackEnglish (US)

© 2009 - 2017, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.

Download .csv

BWS

Services

Resource Groups

CloudWatch

DynamoDB

general@prod

Users with AWS Management Console access can sign-in at: <https://581977599153.signin.aws.amazon.com/console>

Download .csv

User	Access key ID	Secret access key	Email login ID
gpaul-dev-v3	AKIA6FOXTN7OK4ZPOMQ	***** Show	Send email <a href="#">?</a>

Created user gpaul-dev-v3

Attached policy IAMUserChangePass-ord to user gpaul-dev-v3

Created access key for user gpaul-dev-v3

Created login profile for user gpaul-dev-v3

gpaul-dev-ec2+rds	AKIAJUNARXMOE2Q8UA	***** Show	Send email <a href="#">?</a>
-------------------	--------------------	------------	------------------------------

BWS

Services

Resource Groups

CloudWatch

DynamoDB

general@prod

Search IAM

Dashboard

Groups

Users

Roles

Policies

Identity providers

Account settings

Credential report

Encryption keys

Users

gpaul-dev-ec2+rds

Summary

User ARN: am:aws:iam:581977599153:user/gpaul-dev-ec2+rds

Path: /

Creation time: 2017-12-30 21:20 UTC+0530

Permissions: [Types \(0\)](#) [Security credentials](#) [Access Advisor](#)

Add permissions

Attached policies: 1

Policy name	Policy type
Attached directly	
<a href="#">IAMUserChangePass-ord</a>	AWS managed policy

BWS

Services

Resource Groups

CloudWatch

DynamoDB

general@prod

Add permissions to gpaul-dev-ec2+rds

1

Permissions

Rev

Grant permissions

Use IAM policies to grant permissions. You can assign an existing policy or create a new one.

Add user to group

Copy permissions from existing user

Attach existing policies directly

Get started with groups

You haven't created any groups yet. Using groups is a best-practice way to manage users' permissions by job functions, AWS service access, or your custom permissions. Get started by creating a group. [Learn more](#)

Create group

BWS

Services

Resource Groups

CloudWatch

DynamoDB

general@prod

Use IAM policies to grant permissions. You can assign an existing policy or create a new one.

Add user to group

Copy permissions from existing user

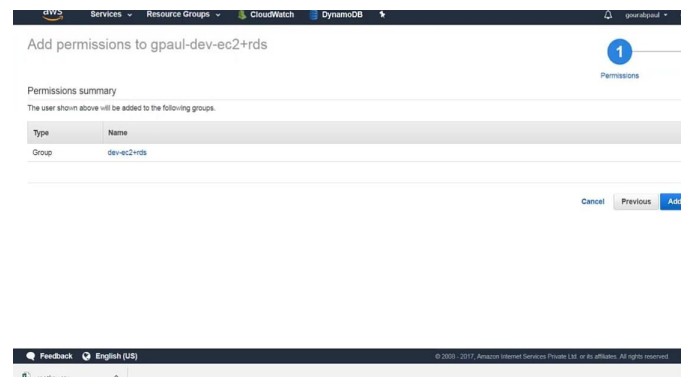
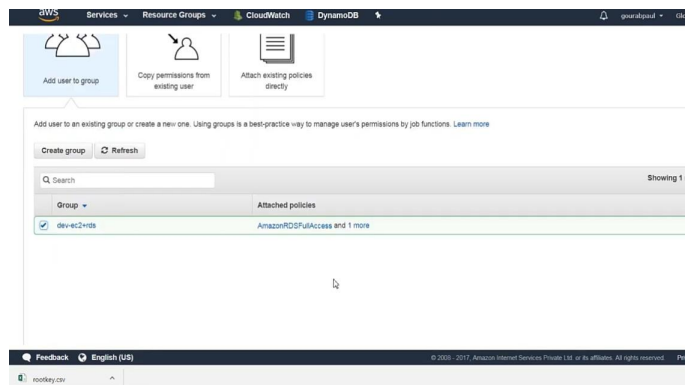
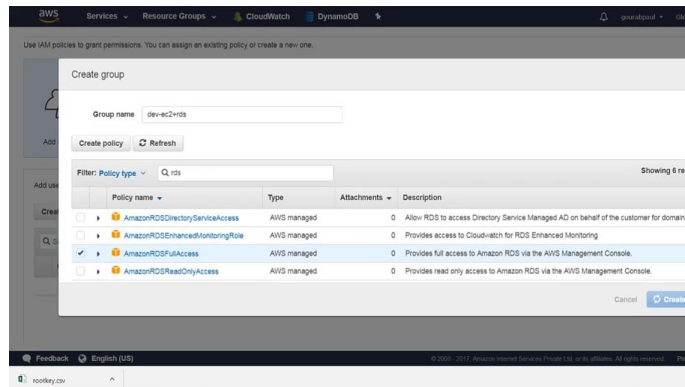
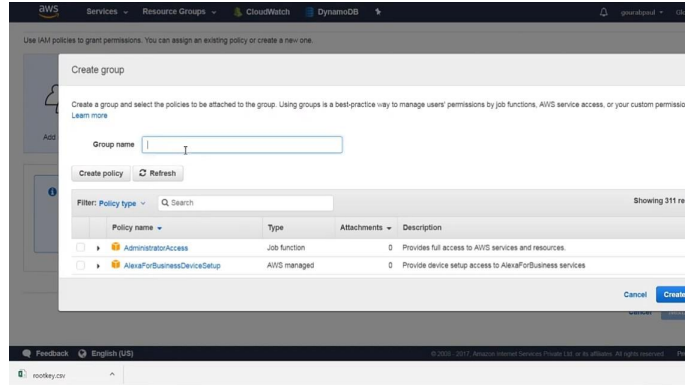
Attach existing policies directly

Get started with groups

You haven't created any groups yet. Using groups is a best-practice way to manage users' permissions by job functions, AWS service access, or your custom permissions. Get started by creating a group. [Learn more](#)

Create group

Cancel



**AWS** Services - Resource Groups - CloudWatch - DynamoDB - gpaul@paul - US

Search IAM

Dashboard  
Groups  
**Users**  
Roles  
Policies  
Identity providers  
Account settings  
Credential report

Encryption keys

Users > gpaul-dev-ec2+rds

### Summary

User ARN: `arn:aws:iam::581977599153:user/gpaul-dev-ec2+rds`  
Path: `/`  
Creation time: 2017-12-30 21:20 UTC+0530

Permissions Groups (1) Security credentials Access Advisor

[Add permissions](#) Attached policies: 3

Policy name	Policy type
Attached directly	
<a href="#">IAMUserChangePassword</a>	AWS managed policy
Attached from group	
<a href="#">AmazonRDSFullAccess</a>	AWS managed policy from group dev-ec2+rds
<a href="#">AmazonEC2ContainerRegistryFullAccess</a>	AWS managed policy from group dev-ec2+rds

Feedback English (US) © 2009 - 2017 Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. rootkey.civ

**AWS** Services - Resource Groups - CloudWatch - DynamoDB - gpaul@paul - US

Search IAM

Dashboard  
Groups  
**Users**  
Roles  
Policies  
Identity providers  
Account settings  
Credential report

Encryption keys

Users > gpaul-dev-ec2+rds

### Summary

User ARN: `arn:aws:iam::581977599153:user/gpaul-dev-ec2+rds`  
Path: `/`  
Creation time: 2017-12-30 21:20 UTC+0530

Permissions Groups (1) Security credentials Access Advisor

[Add permissions](#) Attached policies: 3

Policy name	Policy type
Attached directly	
<a href="#">IAMUserChangePassword</a>	AWS managed policy
Attached from group	
<a href="#">AmazonRDSFullAccess</a>	AWS managed policy from group dev-ec2+rds
<a href="#">AmazonEC2ContainerRegistryFullAccess</a>	AWS managed policy from group dev-ec2+rds

Policy summary [JSON](#)

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "iam:CreateServiceLinkedRole",
      "Resource": "arn:aws:iam::*:role/aws-service-role/rds.amazonaws.com/AWSServiceRoleForRDS",
      "Condition": {
        "StringEquals": {
          "iam:AWSServiceName": "rds.amazonaws.com"
        }
      }
    }
  ]
}
```

Feedback English (US) © 2009 - 2017 Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. rootkey.civ

**AWS** Services - Resource Groups - CloudWatch - DynamoDB - gpaul@paul - US

Search IAM

Dashboard  
Groups  
**Users**  
Roles  
Policies  
Identity providers  
Account settings  
Credential report

Encryption keys

Users > gpaul-dev-ec2+rds

### Summary

User ARN: `arn:aws:iam::581977599153:user/gpaul-dev-ec2+rds`  
Path: `/`  
Creation time: 2017-12-30 21:20 UTC+0530

Permissions Groups (1) Security credentials Access Advisor

Sign-in credentials

Console password	Enabled <a href="#">Manage password</a>
Console login link	<a href="https://581977599153.signin.aws.amazon.com/console">https://581977599153.signin.aws.amazon.com/console</a>
Last login	Never
Assigned MFA device	No <a href="#">Add</a>
Signing certificates	None <a href="#">Add</a>

Access keys

Use access keys to make secure REST or HTTP Query protocol requests to AWS service APIs. For your protection, you should never share your secret keys with anyone. As a best practice, we recommend frequent key rotation. [Learn more](#)

[Create access key](#)

Feedback English (US) © 2009 - 2017 Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. rootkey.civ

aws

Account ID or alias

581977599153

IAM user name


gsaul-dev-s3

Password

Sign in

[Sign in using root account credentials](#)

AWS Database Migration Service



**Over 45,000 Databases Migrated**  
Easily migrate and convert databases.  
[Learn More >](#)

English

Terms of Use Privacy Policy © 1996-2017 Amazon Web Services, Inc. or its affiliates.

Services

Resource Groups

gsaul-dev-s3 @ 581977599153

gsaul

Amazon Glacier now offers expedited retrievals, typically in 1-5 minutes. [Learn More >](#)

Amazon S3

Discover the new console

Search for buckets


+ Create bucket

Delete bucket

Empty bucket


0 Buckets 0 [objects](#) 0 [Reg](#)

You do not have any buckets. Here is how to get started with Amazon S3.




Create a new bucket

Buckets are globally unique containers for everything that you store in Amazon S3.



Upload your data

After you create a bucket, you can upload your objects (for example, your photo or video files).



Set up your permissions

By default, the permissions on an object are private. You can set up access control policies to grant permissions to others.