

Module 8

1 a. Creating an IAM user For login

Add user 1 2 3 4 5

Set user details

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

User name*

[+ Add another user](#)

Select AWS access type

Select how these users will primarily access AWS. If you choose only programmatic access, it does NOT prevent users from accessing the console using an assumed role. Access keys and autogenerated passwords are provided in the last step. [Learn more](#)

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

☒ **Password - AWS Management Console access**

* Required

[Cancel](#) [Next: Permissions](#)

➔ Adding users to the group

Add user 1 2 3 4 5

▼ **Set permissions**

[Add user to group](#) [Copy permissions from existing user](#) [Attach existing policies directly](#)

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](#)

Add user to group

[Create group](#) [Refresh](#)

Search Showing 1 result

Group	Attached policies
<input checked="" type="checkbox"/> instancePermission	launchInstanceGroups

[Cancel](#) [Previous](#) [Next: Tags](#)

[Feedback](#) [Looking for language selection? Find it in the new Unified Settings](#) © 2022, Amazon Web Services India Private Limited or its affiliates. [Privacy](#) [Terms](#)

➔ created group name is instancePermission with attached policy LaunchInstanceGroup .

Add user

1 2 3 4 5

Review

Review your choices. After you create the user, you can view and download the autogenerated password and access key.

User details

User name	instancePermission
AWS access type	Programmatic access and AWS Management Console access
Console password type	Autogenerated
Require password reset	Yes
Permissions boundary	Permissions boundary is not set

Permissions summary

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

Time	Name

Cancel Previous Create user

Feedback Looking for language selection? Find it in the new Unified Settings © 2022, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

➔ Reviewing the permission for creating user with user name InstancePermission

1b. Permission to launch and stop instance given to the IAM user

Identity and Access Management (IAM)

Dashboard

Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Access reports

Access analyzer

Archive rules

Analyzers

Policies > launchInstanceGroups

Summary

Delete policy

Policy ARN: arn:aws:iam::198578022078:policy/launchInstanceGroups

Description: group is allowed to create ,launch and stop instances only

Permissions Policy usage Tags Policy versions Access Advisor

Policy summary {} JSON Edit policy

```

5
6
7
8
9
10
11
12
{
  "Sid": "VisualEditor0",
  "Effect": "Allow",
  "Action": [
    "ec2:DescribeInstances",
    "ec2:StartInstances",
    "ec2:StopInstances"
  ],
  "Resource": "*"
}

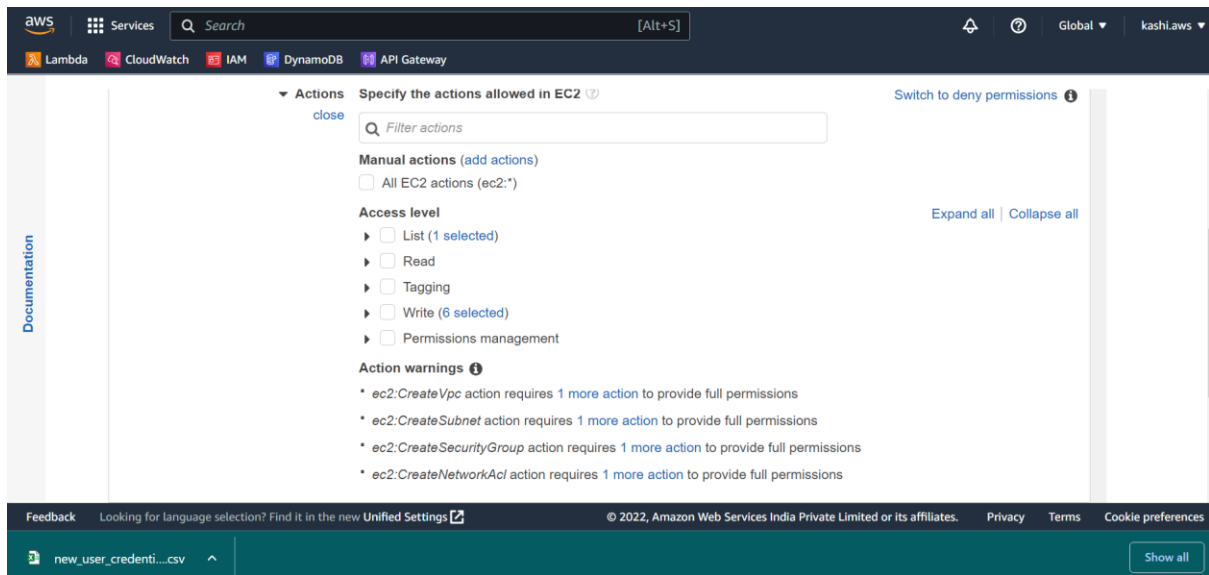
```

Feedback Looking for language selection? Find it in the new Unified Settings © 2022, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

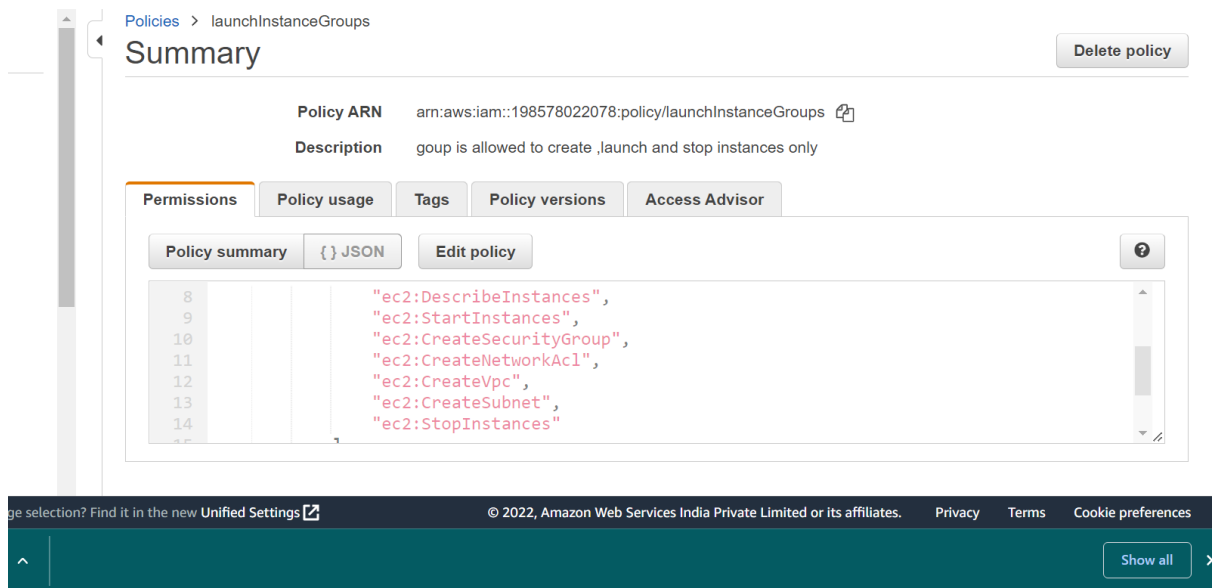
new_user_credenti...csv Show all

➔ Policy attached describeInstance and StartInstance, StopInstance

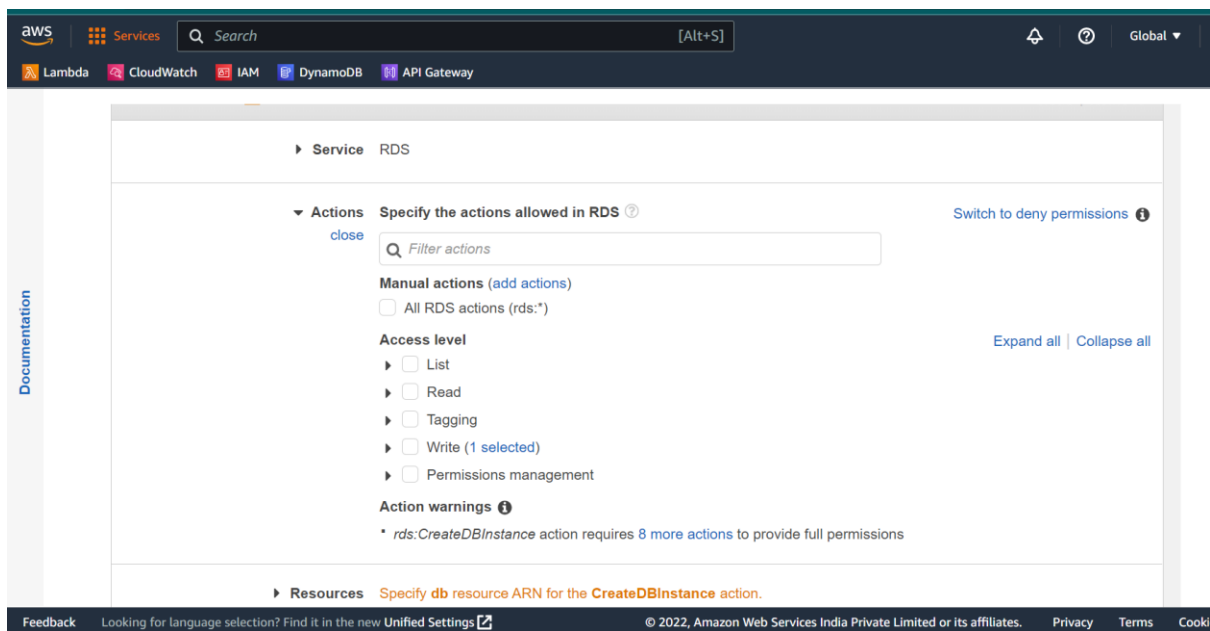
2a. Vpc , Subnet, NACL, Security groups Providing permissions



➔ Added permission for VPC, SUBNET, NACL, SECURITY GROUP

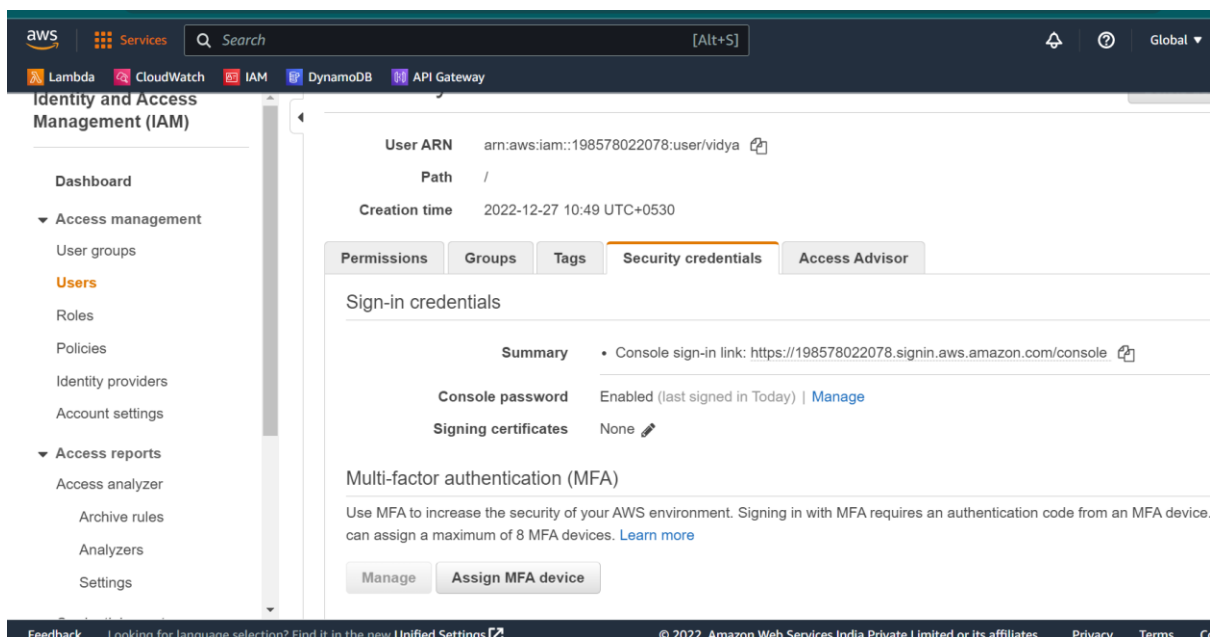


2 b. Permission to create an RDS instance

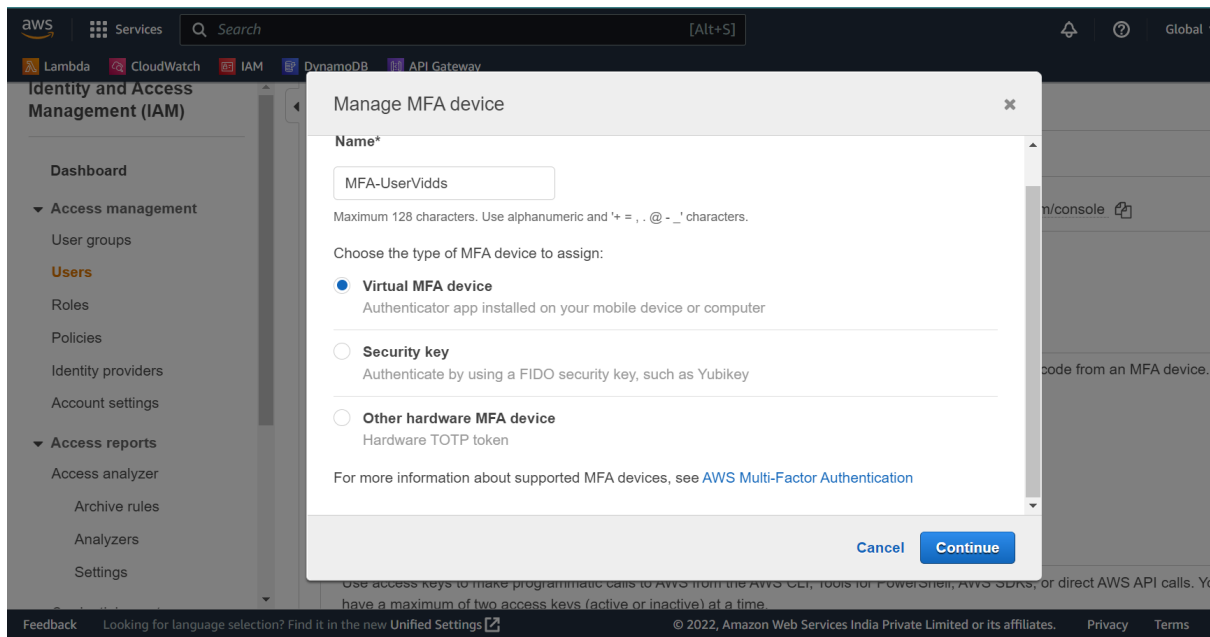


➔ Given the permission for creating an RDS instance

2c. Security for AWS Resources



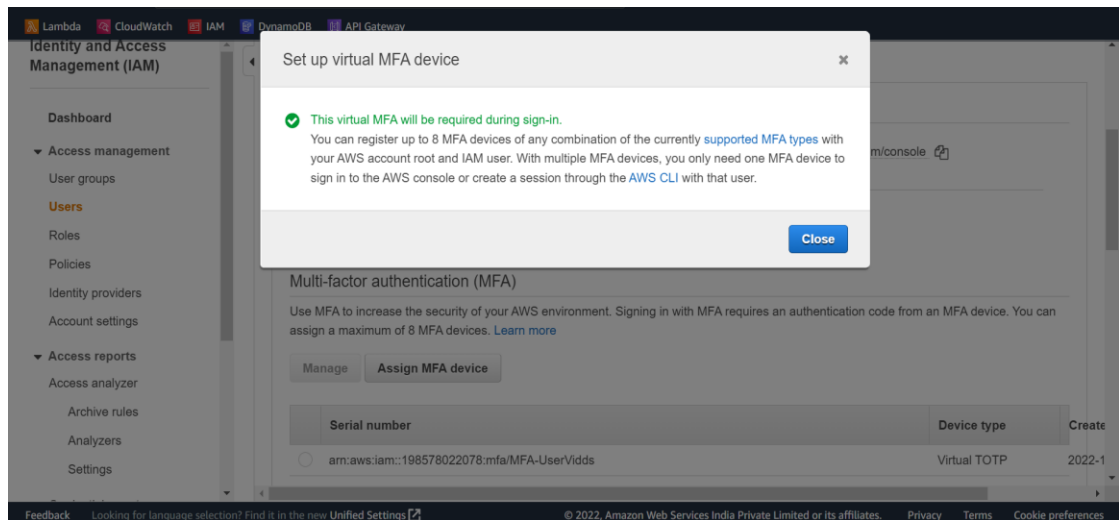
➔ Using Multi-Factor Authentication



➔ Assigning the name for MFA and setting up device by installing google authenticator application on phone



➔ Scanned QR for MFA via phone



➔ MFA device added