

LAB-2

Terraform AWS Provider and IAM User Setting

Step 1: Create a new directory

```
arnim_taliyan@device:~$ mkdir terraform
arnim_taliyan@device:~$ cd terraform
arnim_taliyan@device:~/terraform$
```

Step 2: IAM user

The screenshot displays the AWS IAM console interface for creating a new user. The top navigation bar includes the AWS logo, 'Services', a search bar, and user information for 'ArnimTaliyan'. The left sidebar shows a progress bar with four steps: Step 1 (Specify user details), Step 2 (Set permissions), Step 3 (Review and create), and Step 4 (Retrieve password). The main content area is divided into two sections: 'User details' and 'Set permissions'.

User details

- User name:** A text input field containing 'eg-lab'. Below it, a note states: '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:** A checkbox that is checked. Below it, a note states: '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?:** A section with two radio button options:
 - Specify a user in Identity Center - Recommended:** A radio button that is not selected. Below it, a note states: '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:** A radio button that is selected. Below it, a note states: '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:** A section with two radio button options:
 - Autogenerated password:** A radio button that is selected. Below it, a note states: 'You can view the password after you create the user.'
 - Custom password:** A radio button that is not selected.

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:** A radio button that is selected. Below it, a note states: 'Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.'
- Copy permissions:** A radio button that is not selected. Below it, a note states: 'Copy all group memberships, attached managed policies, and inline policies from an existing user.'
- Attach policies directly:** A radio button that is not selected. Below it, a note states: '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.'

Get started with groups: A section with a note stating: 'Create a group and select policies to attach to the group. We recommend using groups to manage user permissions by job function, AWS service access, or custom permissions. [Learn more](#)'. A 'Create group' button is located to the right of this section.

Set permissions boundary - optional: A section with a dropdown arrow and the text 'Set permissions boundary - optional'.

aws

Services

Search

[Alt+S]

Global

ArnimTaliyan

Review and create

Step 4
Retrieve password

eg-labAutogeneratedYes

Permissions summary

Name	Type	Used as
AdministratorAccess	AWS managed - job function	Permissions boundary
IAMUserChangePassword	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.

CancelPreviousCreate user

CloudShell

Feedback

© 2024, Amazon Web Services, Inc. or its affiliates.

Privacy

Terms

Cookie preferences

aws

Services

Search

[Alt+S]

Global

ArnimTaliyan

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

Step 1
Specify user details

Step 2
Set permissions

Step 3
Review and create

Step 4
Retrieve password

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

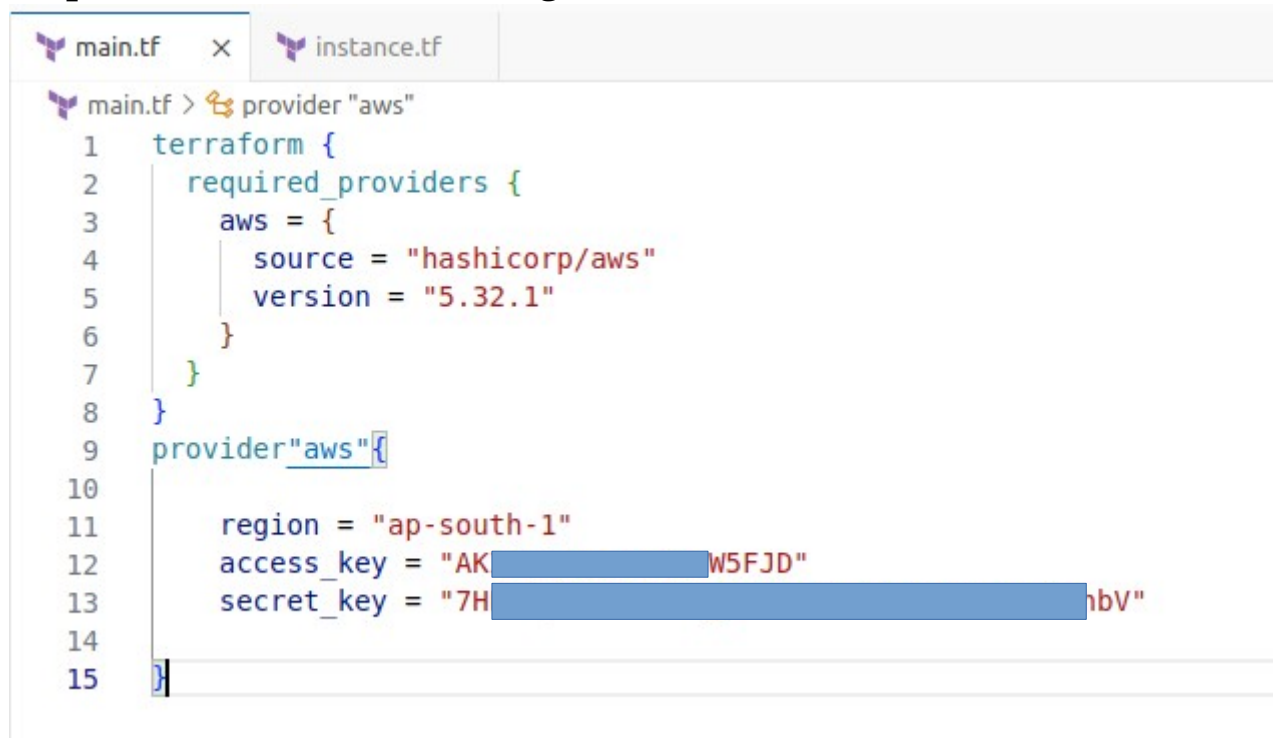
Console sign-in URL
https://533266967718.signin.aws.amazon.com/console

User name
eg-lab

Console password
 Show

CancelDownload .csv fileReturn to users list

Step 3: Create Terraform configuration file



```
main.tf > provider "aws"
1  terraform {
2      required_providers {
3          aws = {
4              source = "hashicorp/aws"
5              version = "5.32.1"
6          }
7      }
8  }
9  provider "aws" {
10
11      region = "ap-south-1"
12      access_key = "AKW5FJD"
13      secret_key = "7HhBV"
14  }
15 }
```

Step 4: Initialize Terraform

```
arnim_taliyan@device:~/Desktop/terraform$ terraform init

Initializing the backend...

Initializing provider plugins...
- Finding hashicorp/aws versions matching "5.32.1"...
- Installing hashicorp/aws v5.32.1...
- Installed hashicorp/aws v5.32.1 (signed by HashiCorp)

Terraform has created a lock file .terraform.lock.hcl to record the provider
selections it made above. Include this file in your version control repository
so that Terraform can guarantee to make the same selections by default when
you run "terraform init" in the future.

Terraform has been successfully initialized!

You may now begin working with Terraform. Try running "terraform plan" to see
any changes that are required for your infrastructure. All Terraform commands
should now work.

If you ever set or change modules or backend configuration for Terraform,
rerun this command to reinitialize your working directory. If you forget, other
commands will detect it and remind you to do so if necessary.
arnim_taliyan@device:~/Desktop/terraform$
```