

## Lab 1

### - Terraform installed successfully

```
PROBLEMS  OUTPUT  DEBUG CONSOLE  TERMINAL  PORTS

• [engy@localhost Terraform]$ terraform --version
Terraform v1.11.0
on linux_amd64
• [engy@localhost Terraform]$ which terraform
/usr/bin/terraform
○ [engy@localhost Terraform]$
```

### - Created a user name terraform-user in AWS Console and gave it Administrator 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 (1/4)** [Info](#)

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

Search

	User name	Path	Group	Last activity	MFA	Password age	Console last sign-in	Access key ID	Active key age
<input type="checkbox"/>	<a href="#">admin-1</a>	/	1	-	Virtual	11 days	-	-	-
<input type="checkbox"/>	<a href="#">admin2-prog</a>	/	1	11 days ago	-	-	-	Active - AKIAVPEYWS7...	11 days
<input type="checkbox"/>	<a href="#">dev-user</a>	/	1	11 days ago	-	11 days	-	Active - AKIAVPEYWS7...	11 days
<input checked="" type="checkbox"/>	<a href="#">terraform-user</a>	/	0	-	-	-	-	-	-

### - Generate the access keys for this user

**Access key created**  
This is the only time that the secret access key can be viewed or downloaded. You cannot recover it later. However, you can create a new access key any time.

**Retrieve access keys** [Info](#)

**Access key**  
If you lose or forget your secret access key, you cannot retrieve it. Instead, create a new access key and make the old key inactive.

Access key: AKIAVPEYWS7NCNIAKP4C | Secret access key: [Show](#)

**Access key best practices**

- Never store your access key in plain text, in a code repository, or in code.
- Disable or delete access key when no longer needed.
- Enable least-privilege permissions.
- Rotate access keys regularly.

For more details about managing access keys, see the [best practices for managing AWS access keys](#).

[Download .csv file](#) [Done](#)

### - AWS Configure

```
engy@localhost:~/Terraform — aws configure

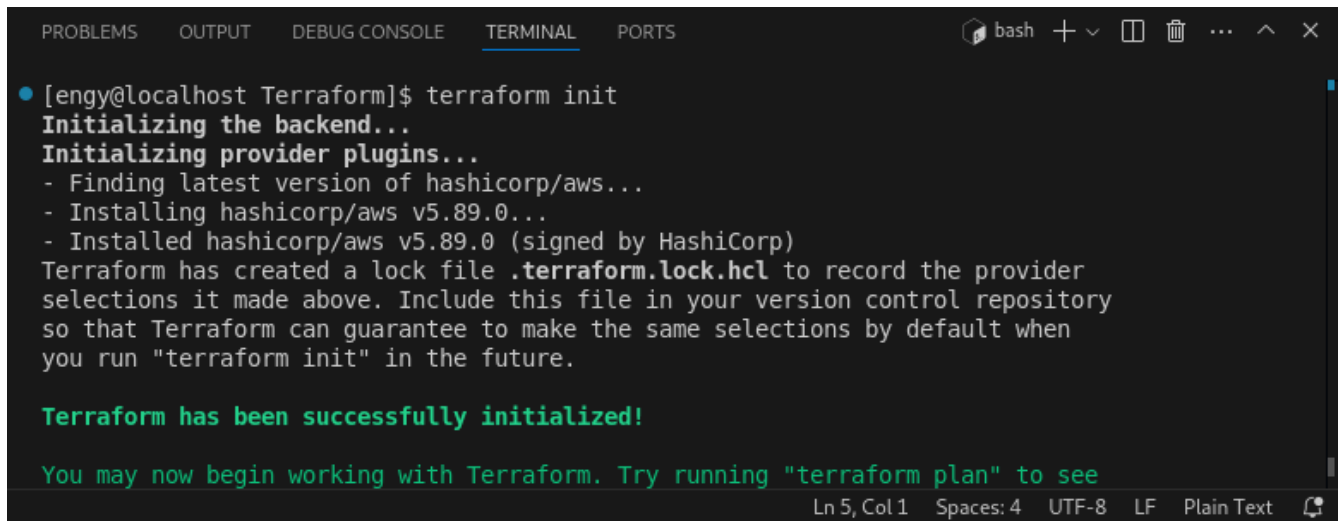
[engy@localhost Terraform]$ aws configure
AWS Access Key ID [*****KP4C]: AKIAVPEYWS7NCNIAKP4C
AWS Secret Access Key [*****HtAw]:
```

- Made a profile named terraform in my ~/.aws/credentials file

```
[engy@localhost Terraform]$ cd ~/.aws
[engy@localhost .aws]$ ls
config  credentials
[engy@localhost .aws]$ vi credentials
```

```
[terraform]
aws_access_key_id = AKIAV
aws_secret_access_key = F
```

- Used terraform init to initialize my terraform plugins

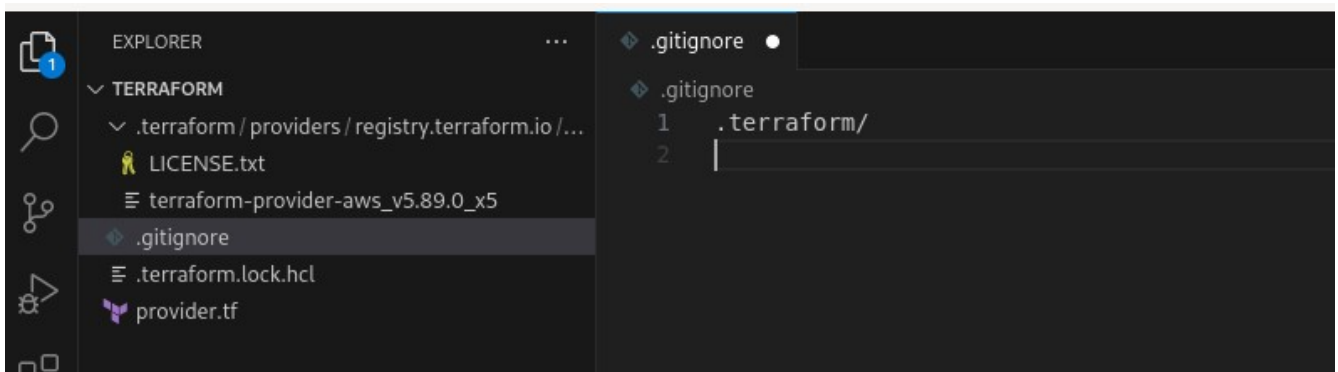


```
PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS
[engy@localhost Terraform]$ terraform init
Initializing the backend...
Initializing provider plugins...
- Finding latest version of hashicorp/aws...
- Installing hashicorp/aws v5.89.0...
- Installed hashicorp/aws v5.89.0 (signed by HashiCorp)
Terraform 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!

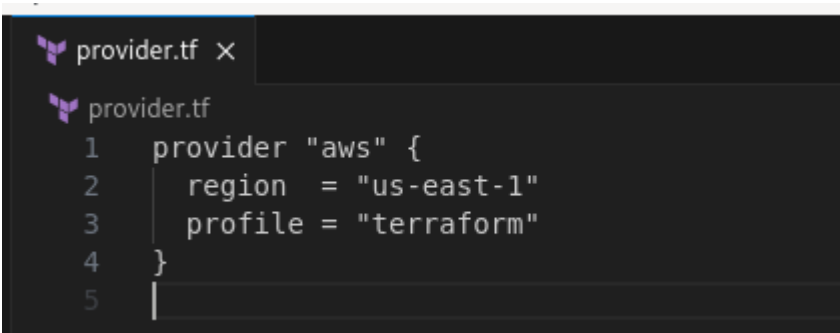
You may now begin working with Terraform. Try running "terraform plan" to see
```

- Created gitignore file and added in it all the plugins



```
EXPLORER
TERRAFORM
  .terraform/providers/registry.terraform.io/...
  LICENSE.txt
  terraform-provider-aws_v5.89.0_x5
  .gitignore
  .terraform.lock.hcl
  provider.tf
```

- Created provider file and used in it the terraform profile that has the accesskeys that we added.



```
provider.tf
provider "aws" {
  region = "us-east-1"
  profile = "terraform"
}
```

## - Created a s3 bucket named terraform-bucket-engy

Successfully created bucket "terraform-bucket-engy"  
To upload files and folders, or to configure additional bucket settings, choose [View details](#).

Account snapshot - updated every 24 hours All AWS Regions [View Storage Lens dashboard](#)  
Storage lens provides visibility into storage usage and activity trends. Metrics don't include directory buckets. [Learn more](#)

General purpose buckets | Directory buckets

General purpose buckets (1/3) All AWS Regions  
Buckets are containers for data stored in S3.

Find buckets by name

	Name	AWS Region	IAM Access Analyzer	Creation date
<input type="radio"/>	lab3-q3-s3	US East (N. Virginia) us-east-1	<a href="#">View analyzer for us-east-1</a>	March 3, 2025, 02:40:55 (UTC+02:00)
<input type="radio"/>	lab3-s3	US East (N. Virginia) us-east-1	<a href="#">View analyzer for us-east-1</a>	March 3, 2025, 01:50:30 (UTC+02:00)
<input checked="" type="radio"/>	terraform-bucket-engy	US East (N. Virginia) us-east-1	<a href="#">View analyzer for us-east-1</a>	March 3, 2025, 04:20:25 (UTC+02:00)

## - Created a backend.tf file and added my bucket name "terraform-bucket-engy" and the key that will be created inside of it.

```
backend.tf
.terraform > providers > registry.terraform.io > hashicorp > aws > 5.89.0 > linux_amd64 > backend.tf
1 terraform {
2   backend "s3" {
3     bucket = "terraform-bucket-engy"
4     key    = "terraform.tfstate"
5     region = "us-east-1"
6     profile = "terraform"
7   }
8 }
9
```

Amazon S3 > Buckets > terraform-bucket-engy

terraform-bucket-engy Info

Objects | Metadata | Properties | Permissions | Metrics | Management | Access Points

Objects (1) [Copy S3 URI](#) [Copy URL](#) [Download](#) [Open](#) [Delete](#) [Actions](#) [Create folder](#) [Upload](#)  
Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 Inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)

Find objects by prefix

<input type="checkbox"/>	Name	Type	Last modified	Size	Storage class
<input type="checkbox"/>	<a href="#">terraform.tfstate</a>	tfstate	March 3, 2025, 04:37:52 (UTC+02:00)	1.7 KB	Standard

→ was created after terraform apply command

## 1- create vpc

```
[engy@localhost Terraform]$ terraform apply
```

Terraform used the selected providers to generate the following execution plan.  
Resource actions are indicated with the following symbols:

+ create

Terraform will perform the following actions:

# aws\_vpc.main will be created

```
+ resource "aws_vpc" "main" {
  + arn                               = (known after apply)
  + cidr_block                        = "10.0.0.0/16"
  + default_network_acl_id           = (known after apply)
  + default_route_table_id           = (known after apply)
  + default_security_group_id        = (known after apply)
```

Plan: 1 to add, 0 to change, 0 to destroy.

Do you want to perform these actions?

Terraform will perform the actions described above.  
Only 'yes' will be accepted to approve.

Enter a value: yes

aws\_vpc.main: Creating...

aws\_vpc.main: Creation complete after 3s [id=vpc-0fe94fd9a0cf78341]

Apply complete! Resources: 1 added, 0 changed, 0 destroyed.

```
[engy@localhost Terraform]$
```

Your VPCs (3) <a href="#">Info</a>										Last updated less than a minute ago	<a href="#">Actions</a>	<a href="#">Create VPC</a>
<input type="checkbox"/>	Name	VPC ID	State	Block Public Access	IPv4 CIDR	IPv6 ...	DHCP option set	Main route table	Main network ACL			
<input type="checkbox"/>	-	<a href="#">vpc-0026b9817463a7da2</a>	Available	Off	172.31.0.0/16	-	<a href="#">dopt-013b78c169837f1...</a>	<a href="#">rtb-02b81d6cf2d5c75d3</a>	<a href="#">acl-075e3b5bb61872c</a>			
<input type="checkbox"/>	my-vpc-01	<a href="#">vpc-0cb8fca9cd02997cf</a>	Available	Off	10.0.0.0/16	-	<a href="#">dopt-013b78c169837f1...</a>	<a href="#">rtb-074394be6c6a20055</a>	<a href="#">acl-02a39e49396a7b5</a>			
<input type="checkbox"/>	my_terraform_vpc	<a href="#">vpc-0fe94fd9a0cf78341</a>	Available	Off	10.0.0.0/16	-	<a href="#">dopt-013b78c169837f1...</a>	<a href="#">rtb-0b4084b74b882c5f6</a>	<a href="#">acl-0d6200fa9b2b3e5c</a>			

## 2- create internet gateway

```
internet_gateway.tf
```

```
internet_gateway.tf
```

```
1 resource "aws_internet_gateway" "gw" {
2   vpc_id = aws_vpc.main.id
3
4   tags = {
5     Name = "terraform-lab-gw"
6   }
7 }
8
```

```
o [engy@localhost Terraform]$ terraform apply
aws_vpc.main: Refreshing state... [id=vpc-0fe94fd9a0cf78341]
```

Terraform used the selected providers to generate the following execution plan.  
Resource actions are indicated with the following symbols:

+ create

Terraform will perform the following actions:

```
# aws_internet_gateway.gw will be created
+ resource "aws_internet_gateway" "gw" {
  + arn      = (known after apply)
  + id       = (known after apply)
  + owner_id = (known after apply)
  + tags     = {
    + "Name" = "terraform-internet-gw"
  }
  + tags_all = {
    + "Name" = "terraform-internet-gw"
  }
}
```

Plan: 1 to add, 0 to change, 0 to destroy.

Do you want to perform these actions?

Terraform will perform the actions described above.  
Only 'yes' will be accepted to approve.

Enter a value: yes

aws\_internet\_gateway.gw: Creating...

aws\_internet\_gateway.gw: Creation complete after 2s [id=igw-0f9645cb912025f3e]

Apply complete! Resources: 1 added, 0 changed, 0 destroyed.

Internet gateways (1/3) Info						Actions	Create internet gateway
Search						< 1 >	
<input type="checkbox"/>	Name	Internet gateway ID	State	VPC ID	Owner		
<input type="checkbox"/>	my-Internet-gateway	<a href="#">igw-00211472c8b15165d</a>	Attached	<a href="#">vpc-0cb8fca9cd02997cf   my-vpc-01</a>	376129886170		
<input type="checkbox"/>	-	<a href="#">igw-03c88077f293629e3</a>	Attached	<a href="#">vpc-0026b9817463a7da2</a>	376129886170		
<input checked="" type="checkbox"/>	terraform-internet-gw	<a href="#">igw-0f9645cb912025f3e</a>	Attached	<a href="#">vpc-0fe94fd9a0cf78341   my_terraform...</a>	376129886170		

### 3- create public route table

```
public_route-table x
public_route-table
1 resource "aws_route_table" "public_route" {
2   vpc_id = aws_vpc.main.id
3
4   route {
5     cidr_block = "0.0.0.0/0"
6     gateway_id = aws_internet_gateway.gw.id
7   }
8
9   tags = {
10    Name = "public_route_table"
11  }
12 }
13
```

```
engy@localhost Terraform$ terraform apply
aws_vpc.main: Refreshing state... [id=vpc-0fe94fd9a0cf78341]
aws_internet_gateway.gw: Refreshing state... [id=igw-0f9645cb912025f3e]
```

Terraform used the selected providers to generate the following execution plan. Resource actions are indicated with the following symbols:

+ create

Terraform will perform the following actions:

```
# aws_route_table.public_route will be created
+ resource "aws_route_table" "public_route" {
  + arn                = (known after apply)
  + id                 = (known after apply)
  + owner_id           = (known after apply)
  + propagating_vgws   = (known after apply)
  + route              = [
    + {
      + cidr_block      = "0.0.0.0/0"
      + gateway_id      = "igw-0f9645cb912025f3e"
      # (11 unchanged attributes hidden)
    },
  ]
}
```

Plan: 1 to add, 0 to change, 0 to destroy.

Do you want to perform these actions?

Terraform will perform the actions described above.  
Only 'yes' will be accepted to approve.

Enter a value: yes

aws\_route\_table.public\_route: Creating...

aws\_route\_table.public\_route: Creation complete after 2s [id=rtb-016acee61139a2412]

Apply complete! Resources: 1 added, 0 changed, 0 destroyed.

Route tables (1/6) [Info](#)

Last updated less than a minute ago [Actions](#) [Create route table](#)

<input type="checkbox"/>	Name	Route table ID	Explicit subnet associations	Edge associations	Main	VPC	Owner ID
<input type="checkbox"/>	-	<a href="#">rtb-074394be6c6a20055</a>	-	-	Yes	<a href="#">vpc-0cb8fca9cd02997cf   my-vpc-01</a>	376129886170
<input type="checkbox"/>	my-route -public	<a href="#">rtb-07211bd9ae2b42807</a>	<a href="#">2 subnets</a>	-	No	<a href="#">vpc-0cb8fca9cd02997cf   my-vpc-01</a>	376129886170
<input type="checkbox"/>	-	<a href="#">rtb-0b4084b74b882c5f6</a>	-	-	Yes	<a href="#">vpc-0fe94fd9a0cf78341   my_terraform...</a>	376129886170
<input checked="" type="checkbox"/>	public_route_table	<a href="#">rtb-016acee61139a2412</a>	-	-	No	<a href="#">vpc-0fe94fd9a0cf78341   my_terraform...</a>	376129886170
<input type="checkbox"/>	-	<a href="#">rtb-02b81d6cf2d5c75d3</a>	-	-	Yes	<a href="#">vpc-0026b9817463a7da2</a>	376129886170
<input type="checkbox"/>	my-route-private	<a href="#">rtb-06276d5365effef7c</a>	<a href="#">2 subnets</a>	-	No	<a href="#">vpc-0cb8fca9cd02997cf   my-vpc-01</a>	376129886170

rtb-016acee61139a2412 / public\_route\_table

Details

Routes

Subnet associations

Edge associations

Route propagation

Tags

Details

Route table ID  
[rtb-016acee61139a2412](#)

VPC  
[vpc-0fe94fd9a0cf78341 | my\\_terraform\\_vpc](#)

Main  
☐ No

Owner ID  
[376129886170](#)

Explicit subnet associations  
-

Edge associations  
-

#### 4- create private route table

```
private_route_table.tf
private_route_table.tf
1 resource "aws_route_table" "private_route" {
2   vpc_id = aws_vpc.main.id
3
4   tags = {
5     Name = "private_route_table"
6   }
7 }
8
```

```
o [engy@localhost Terraform]$ terraform apply
aws_vpc.main: Refreshing state... [id=vpc-0fe94fd9a0cf78341]
aws_internet_gateway.gw: Refreshing state... [id=igw-0f9645cb912025f3e]
aws_route_table.public_route: Refreshing state... [id=rtb-016acee61139a2412]
```

Terraform used the selected providers to generate the following execution plan. Resource actions are indicated with the following symbols:

+ create

Terraform will perform the following actions:

```
# aws_route_table.private_route will be created
+ resource "aws_route_table" "private_route" {
+   arn                = (known after apply)
+   id                 = (known after apply)
+   owner_id           = (known after apply)
+   propagating_vgws   = (known after apply)
+   route              = (known after apply)
+   tags               = {
+     "Name" = "private_route_table"
+   }
+   tags_all           = {
+     "Name" = "private route table"
+   }
}
```

**Plan:** 1 to add, 0 to change, 0 to destroy.

**Do you want to perform these actions?**

Terraform will perform the actions described above.  
Only 'yes' will be accepted to approve.

Enter a value: yes

aws\_route\_table.private\_route: Creating...

aws\_route\_table.private\_route: Creation complete after 2s [id=rtb-0af4cfd638dab8883]

**Apply complete! Resources: 1 added, 0 changed, 0 destroyed.**

Route tables (1/7) Info		Last updated less than a minute ago		Actions	Create route table		
<input type="text" value="Find resources by attribute or tag"/>							
<input checked="" type="checkbox"/>	Name	Route table ID	Explicit subnet associations	Edge associations	Main	VPC	Owner ID
<input type="checkbox"/>	-	rtb-074394be6ca20055	-	-	Yes	vpc-0cb8fca9cd02997cf   my-vpc-01	376129886170
<input checked="" type="checkbox"/>	private_route_table	rtb-0af4cfd638dab8883	-	-	No	vpc-0fe94fd9a0cf78341   my_terraform...	376129886170
<input type="checkbox"/>	my-route-public	rtb-07211bd9aa2b42807	2 subnets	-	No	vpc-0cb8fca9cd02997cf   my-vpc-01	376129886170
<input type="checkbox"/>	-	rtb-0b4084b74b882c5f6	-	-	Yes	vpc-0fe94fd9a0cf78341   my_terraform...	376129886170
<input type="checkbox"/>	public_route_table	rtb-016acee61139a2412	-	-	No	vpc-0fe94fd9a0cf78341   my_terraform...	376129886170
<input type="checkbox"/>	-	rtb-02b81d6cf2d5c75d3	-	-	Yes	vpc-0026b9817463a7da2	376129886170
<input type="checkbox"/>	my-route-private	rtb-06276d5365effe7c	2 subnets	-	No	vpc-0cb8fca9cd02997cf   my-vpc-01	376129886170



Plan: 2 to add, 0 to change, 0 to destroy.

Do you want to perform these actions?

Terraform will perform the actions described above.

Only 'yes' will be accepted to approve.

Enter a value: yes

aws\_subnet.public\_sub: Creating...

aws\_subnet.private\_sub: Creating...

aws\_subnet.private\_sub: Creation complete after 2s [id=subnet-0ee5914bc196384ed]

aws\_subnet.public\_sub: Creation complete after 3s [id=subnet-05ce1d1d974cdc419]

Apply complete! Resources: 2 added, 0 changed, 0 destroyed.

Subnets (2/6) Info										Last updated less than a minute ago	Actions	Create subnet
Find resources by attribute or tag												
my X Clear filters												
	Name	Subnet ID	State	VPC	Block Public...	IPv4 CIDR	IPv6 CIDR	IPv6 CIDR as				
<input type="checkbox"/>	my-subnet-01 -public	subnet-04294f78ef676da36	Available	vpc-0cb8fca9cd02997cf   my-vpc-01	Off	10.0.0.0/24	-	-				
<input checked="" type="checkbox"/>	public_sub	subnet-05ce1d1d974cdc419	Available	vpc-0fe94fd9a0cf78341   my_terrafor...	Off	10.0.2.0/24	-	-				
<input type="checkbox"/>	my-subnet-02 -public	subnet-03f617ba76ac28352	Available	vpc-0cb8fca9cd02997cf   my-vpc-01	Off	10.0.2.0/24	-	-				
<input type="checkbox"/>	my-subnet-02-private	subnet-0a6c1dd55a37f14c3	Available	vpc-0cb8fca9cd02997cf   my-vpc-01	Off	10.0.3.0/24	-	-				
<input checked="" type="checkbox"/>	private_sub	subnet-0ee5914bc196384ed	Available	vpc-0fe94fd9a0cf78341   my_terrafor...	Off	10.0.1.0/24	-	-				
<input type="checkbox"/>	my-subnet-01-private	subnet-094b53af265d8f7c6	Available	vpc-0cb8fca9cd02997cf   my-vpc-01	Off	10.0.1.0/24	-	-				

## 6- Attach public route table to subnets

```
public_route-table.tf x
public_route-table.tf
1 resource "aws_route_table" "public_route" {
2   vpc_id = aws_vpc.main.id
3
4   route {
5     cidr_block = "0.0.0.0/0"
6     gateway_id = aws_internet_gateway.gw.id
7   }
8
9   tags = {
10    Name = "public_route_table"
11  }
12 }
13 resource "aws_route_table_association" "public_route_association" {
14   subnet_id      = aws_subnet.public_sub.id
15   route_table_id = aws_route_table.public_route.id
16 }
17
```

```
[engy@localhost Terraform]$ terraform apply
aws_vpc.main: Refreshing state... [id=vpc-0fe94fd9a0cf78341]
aws_route_table.private_route: Refreshing state... [id=rtb-0af4cfd638dab8883]
aws_internet_gateway.gw: Refreshing state... [id=igw-0f9645cb912025f3e]
aws_subnet.private_sub: Refreshing state... [id=subnet-0ee5914bc196384ed]
aws_subnet.public_sub: Refreshing state... [id=subnet-05ce1d1d974cdc419]
aws_route_table.public_route: Refreshing state... [id=rtb-016acee61139a2412]
```

Terraform used the selected providers to generate the following execution plan. Resource actions are indicated with the following symbols:

+ create

Terraform will perform the following actions:

```
# aws_route_table_association.public_route_association will be created
+ resource "aws_route_table_association" "public_route_association" {
  + id            = (known after apply)
  + route_table_id = "rtb-016acee61139a2412"
  + subnet_id     = "subnet-05ce1d1d974cdc419"
}
```

Plan: 1 to add, 0 to change, 0 to destroy.

Do you want to perform these actions?

Terraform will perform the actions described above.  
Only 'yes' will be accepted to approve.

Enter a value: yes

```
aws_route_table_association.public_route_association: Creating...
aws_route_table_association.public_route_association: Creation complete after 2s [id=rtbassoc-071543b81fc681ce6]
```

Apply complete! Resources: 1 added, 0 changed, 0 destroyed.

```
[engy@localhost Terraform]$
```

Route tables (1/7) [Info](#)

Last updated less than a minute ago [Actions](#) [Create route table](#)

<input type="checkbox"/>	Name	Route table ID	Explicit subnet associations	Edge associations	Main	VPC	Owner ID
<input type="checkbox"/>	-	<a href="#">rtb-074394be6c6a20055</a>	-	-	Yes	<a href="#">vpc-0cb8fca9cd02997cf   my-vpc-01</a>	376129886170
<input type="checkbox"/>	private_route_table	<a href="#">rtb-0af4cfd638dab8883</a>	-	-	No	<a href="#">vpc-0fe94fd9a0cf78341   my_terraform...</a>	376129886170
<input type="checkbox"/>	my-route -public	<a href="#">rtb-07211bd9ae2b42807</a>	2 subnets	-	No	<a href="#">vpc-0cb8fca9cd02997cf   my-vpc-01</a>	376129886170
<input type="checkbox"/>	-	<a href="#">rtb-0b4084b74b882c5f6</a>	-	-	Yes	<a href="#">vpc-0fe94fd9a0cf78341   my_terraform...</a>	376129886170
<input checked="" type="checkbox"/>	public_route_table	<a href="#">rtb-016acee61139a2412</a>	<a href="#">subnet-05ce1d1d974cdc419 / public_sub</a>	-	No	<a href="#">vpc-0fe94fd9a0cf78341   my_terraform...</a>	376129886170
<input type="checkbox"/>	-	<a href="#">rtb-02b81d6cf2d5c75d3</a>	-	-	Yes	<a href="#">vpc-0026b9817463a7da2</a>	376129886170
<input type="checkbox"/>	my-route-private	<a href="#">rtb-06276d5365effef7c</a>	2 subnets	-	No	<a href="#">vpc-0cb8fca9cd02997cf   my-vpc-01</a>	376129886170

rtb-016acee61139a2412 / public\_route\_table

[Details](#) [Routes](#) [Subnet associations](#) [Edge associations](#) [Route propagation](#) [Tags](#)

Details

Route table ID  
[rtb-016acee61139a2412](#)

VPC  
[vpc-0fe94fd9a0cf78341 | my\\_terraform\\_vpc](#)

Main  
[No](#)

Owner ID  
[376129886170](#)

Explicit subnet associations  
[subnet-05ce1d1d974cdc419 / public\\_sub](#)

Edge associations  
-

## Compute

### 7- create security group which allow ssh from 0.0.0.0/0

```
sg_1.tf X
sg_1.tf
1 resource "aws_security_group" "sg_1_terraform" {
2     name           = "allow_ssh"
3     description    = "Allow ssh inbound traffic and all outbound traffic"
4     vpc_id         = aws_vpc.main.id
5
6     tags = {
7         Name = "allow_ssh"
8     }
9 }
10
11 resource "aws_vpc_security_group_ingress_rule" "allow_ssh_ipv4" {
12     security_group_id = aws_security_group.sg_1_terraform.id
13     cidr_ipv4         = "0.0.0.0/0"
14     from_port         = 22
15     ip_protocol       = "tcp"
16     to_port           = 22
17 }
18
```

Terraform will perform the following actions:

```
# aws_security_group.sg_1_terraform will be created
+ resource "aws_security_group" "sg_1_terraform" {
+   arn                = (known after apply)
+   description        = "Allow ssh inbound traffic and all outbound traffic"
+   egress              = (known after apply)
+   id                 = (known after apply)
+   ingress             = (known after apply)
+   name                = "allow_ssh"
+   name_prefix        = (known after apply)
+   owner_id            = (known after apply)
+   revoke_rules_on_delete = false
+   tags                = {
+     "Name" = "allow_ssh"
+   }
+   tags_all            = {
+     "Name" = "allow_ssh"
+   }
+   vpc_id              = "vpc-0fe94fd9a0cf78341"
+ }

# aws_vpc_security_group_ingress_rule.allow_ssh_ipv4 will be created
+ resource "aws_vpc_security_group_ingress_rule" "allow_ssh_ipv4" {
+   arn                = (known after apply)
+   cidr_ipv4          = "0.0.0.0/0"
+   from_port          = 22
+   id                 = (known after apply)
+   ip_protocol         = "tcp"
+   security_group_id   = (known after apply)
+   security_group_rule_id = (known after apply)
+   tags_all            = {}
+   to_port             = 22
+ }
}
```

Plan: 2 to add, 0 to change, 0 to destroy.

Do you want to perform these actions?

Terraform will perform the actions described above.  
Only 'yes' will be accepted to approve.

Enter a value: yes

```
aws_security_group.sg_1_terraform: Creating...
aws_security_group.sg_1_terraform: Creation complete after 4s [id=sg-05ad2722abe586f5c]
aws_vpc_security_group_ingress_rule.allow_ssh_ipv4: Creating...
aws_vpc_security_group_ingress_rule.allow_ssh_ipv4: Creation complete after 1s [id=sgr-0ecb288e8dac7a00d]
```

Apply complete! Resources: 2 added, 0 changed, 0 destroyed.

## sg-05ad2722abe586f5c - allow\_ssh

Actions ▾

### Details

Security group name  
allow\_ssh

Security group ID  
sg-05ad2722abe586f5c

Description  
Allow ssh inbound traffic and all outbound traffic

VPC ID  
vpc-0fe94fd9a0cf78341

Owner  
376129886170

Inbound rules count  
1 Permission entry

Outbound rules count  
0 Permission entries

Inbound rules

Outbound rules

Sharing - new

VPC associations - new

Tags

### Inbound rules (1)



Manage tags

Edit inbound rules

Search

<input type="checkbox"/>	Name	Security group rule ID	IP version	Type	Protocol	Port range	Source	Description
<input type="checkbox"/>	-	sgr-0ecb288e8dac7a00d	IPv4	SSH	TCP	22	0.0.0.0/0	-

## 8- create security group that allow ssh and port 3000 from vpc cidr only

```

sg_1.tf  sg_2.tf  X
sg_2.tf
1  resource "aws_security_group" "sg_2_terraform" {
2      name           = "allow ssh private"
3      description    = "Allow ssh inbound traffic for only vpc cidr"
4      vpc_id         = aws_vpc.main.id
5
6      tags = {
7          Name = "allow_ssh_private"
8      }
9  }
10
11 resource "aws_vpc_security_group_ingress_rule" "allow_ssh_ipv4_2" {
12     security_group_id = aws_security_group.sg_2_terraform.id
13     cidr_ipv4         = aws_vpc.main.cidr_block
14     from_port         = 22
15     ip_protocol       = "tcp"
16     to_port           = 22
17 }
18
19 resource "aws_vpc_security_group_ingress_rule" "allow_3000_ipv4_2" {
20     security_group_id = aws_security_group.sg_2_terraform.id
21     cidr_ipv4         = aws_vpc.main.cidr_block
22     from_port         = 3000
23     ip_protocol       = "tcp"
24     to_port           = 3000
25 }
26

```

Plan: 3 to add, 0 to change, 0 to destroy.

Do you want to perform these actions?

Terraform will perform the actions described above.  
Only 'yes' will be accepted to approve.

Enter a value: yes

aws\_security\_group.sg\_2\_terraform: Creating...

aws\_security\_group.sg\_2\_terraform: Creation complete after 4s [id=sg-0d1d901225d8563e6]

aws\_vpc\_security\_group\_ingress\_rule.allow\_3000\_ipv4\_2: Creating...

aws\_vpc\_security\_group\_ingress\_rule.allow\_ssh\_ipv4\_2: Creating...

aws\_vpc\_security\_group\_ingress\_rule.allow\_3000\_ipv4\_2: Creation complete after 1s [id=sgr-0591e1f256c71b62b]

aws\_vpc\_security\_group\_ingress\_rule.allow\_ssh\_ipv4\_2: Creation complete after 1s [id=sgr-0adb0a728fa2b68cc]

Apply complete! Resources: 3 added, 0 changed, 0 destroyed.

jenqv@localhost: Terraform\$

## sg-0d1d901225d8563e6 - allow ssh private

Actions

### Details

Security group name  
allow ssh private

Security group ID  
sg-0d1d901225d8563e6

Description  
Allow ssh Inbound traffic for only vpc cidr

VPC ID  
vpc-0fe94fd9a0c78341

Owner  
376129886170

Inbound rules count  
2 Permission entries

Outbound rules count  
0 Permission entries

Inbound rules | Outbound rules | Sharing - new | VPC associations - new | Tags

### Inbound rules (2)



Manage tags

Edit inbound rules

<input type="checkbox"/>	Name	Security group rule ID	IP version	Type	Protocol	Port range	Source	Description
<input type="checkbox"/>	-	sgr-0591e1f256c71b62b	IPv4	Custom TCP	TCP	3000	10.0.0.0/16	-
<input type="checkbox"/>	-	sgr-0adb0a728fa2b68cc	IPv4	SSH	TCP	22	10.0.0.0/16	-

## 7- create ec2(bastion) in public subnet with security group from 7

```

ec2(bastion).tf x  sg_1.tf
ec2(bastion).tf
1 resource "aws_instance" "bastion" {
2     ami           = "ami-05b10e08d247fb927"
3     instance_type = "t2.micro"
4     subnet_id     = aws_subnet.public_sub.id
5
6     tags = {
7         Name = "bastion"
8     }
9
10    vpc_security_group_ids = [aws_security_group.sg_1_terraform.id]
11 }
12

```

Plan: 1 to add, 0 to change, 0 to destroy.

### Do you want to perform these actions?

Terraform will perform the actions described above.  
Only 'yes' will be accepted to approve.

Enter a value: yes

aws\_instance.bastion: Creating...

aws\_instance.bastion: Still creating... [10s elapsed]

aws\_instance.bastion: Creation complete after 15s [id=i-0e03885e8b9f99eba]

Apply complete! Resources: 1 added, 0 changed, 0 destroyed.

Instances (1/6) Info

Find Instance by attribute or tag (case-sensitive) All states

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...
	i-072250ba06d7ff08e	Running	t2.micro	2/2 checks passed	View alarms +	us-east-1b	-	54.144.60.78
	i-0cc4ceea9ea770d18	Running	t2.micro	2/2 checks passed	View alarms +	us-east-1b	-	-
	i-04e479ac8977cf306	Running	t2.micro	2/2 checks passed	View alarms +	us-east-1b	-	-
	i-08f638c0e7055367a	Running	t2.micro	2/2 checks passed	View alarms +	us-east-1a	-	98.80.210.246
	i-0b52d35bf7e6691e1	Running	t2.micro	2/2 checks passed	View alarms +	us-east-1a	-	-
<input checked="" type="checkbox"/> bastion	i-0e03885e8b9f99eba	Running	t2.micro	Initializing	View alarms +	us-east-1a	-	-

i-0e03885e8b9f99eba (bastion)

Details Status and alarms Monitoring Security Networking Storage Tags

▼ Instance summary info

Instance ID i-0e03885e8b9f99eba	Public IPv4 address -	Private IPv4 addresses 10.0.2.43
IPv6 address -	Instance state Running	Public IPv4 DNS -
Hostname type IP name: ip-10-0-2-43.ec2.internal	Private IP DNS name (IPv4 only) ip-10-0-2-43.ec2.internal	Elastic IP addresses -
Answer private resource DNS name -	Instance type t2.micro	AWS Compute Optimizer finding Opt-in to AWS Compute Optimizer for recommendations.   Learn more
Auto-assigned IP address -	VPC ID vpc-0fe94fd9a0cf78341 (my_terraform_vpc)	Auto Scaling Group name -
IAM Role -	Subnet ID subnet-05ce1d1d974cdc419 (public_sub)	Managed false
IMDSv2 Required	Instance ARN arn:aws:ec2:us-east-1:376129886170:instance/i-0e03885e8b9f99eba	

## 8- create ec2(application) private subnet with security group from 8

```

ec2(application).tf x sg_2.tf
ec2(application).tf
1 resource "aws_instance" "application" {
2     ami           = "ami-05b10e08d247fb927"
3     instance_type = "t2.micro"
4     subnet_id     = aws_subnet.private_sub.id
5
6     tags = {
7         Name = "application"
8     }
9
10    vpc_security_group_ids = [aws_security_group.sg_2.terraform.id]
11 }
12

```

Plan: 1 to add, 0 to change, 0 to destroy.

Do you want to perform these actions?

Terraform will perform the actions described above.  
Only 'yes' will be accepted to approve.

Enter a value: yes

aws\_instance.application: Creating...

aws\_instance.application: Still creating... [10s elapsed]

aws\_instance.application: Creation complete after 15s [id=i-097178edbec1d0b7d]

Apply complete! Resources: 1 added, 0 changed, 0 destroyed.

Instances (1/7) [Info](#)

Find Instance by attribute or tag (case-sensitive)

All states

Last updated less than a minute ago

Connect

Instance state

Actions

Launch instances

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...
	i-072250ba06d7ff08e	Running	t2.micro	2/2 checks passed	View alarms +	us-east-1b	-	54.144.60.78
	i-0cc4ecea9ea770d18	Running	t2.micro	2/2 checks passed	View alarms +	us-east-1b	-	-
	i-04e479ac8977cf306	Running	t2.micro	2/2 checks passed	View alarms +	us-east-1b	-	-
	i-08f638c0e7055367a	Running	t2.micro	2/2 checks passed	View alarms +	us-east-1a	-	98.80.210.246
	i-0b52d35bf7e6691e1	Running	t2.micro	2/2 checks passed	View alarms +	us-east-1a	-	-
bastion	i-0e03885e8b9f99eba	Running	t2.micro	2/2 checks passed	View alarms +	us-east-1a	-	-
<input checked="" type="checkbox"/> application	i-097178edbec1d0b7d	Running	t2.micro	Initializing	View alarms +	us-east-1a	-	-

i-097178edbec1d0b7d (application)

Details

Status and alarms

Monitoring

Security

Networking

Storage

Tags

▼ Instance summary [Info](#)

Instance ID

i-097178edbec1d0b7d

IPv6 address

-

Hostname type

IP name: ip-10-0-1-86.ec2.internal

Answer private resource DNS name

-

Auto-assigned IP address

-

IAM Role

-

Public IPv4 address

-

Instance state

Running

Private IP DNS name (IPv4 only)

ip-10-0-1-86.ec2.internal

Instance type

t2.micro

VPC ID

vpc-0fe94fd9a0cf78341 (my\_terraform\_vpc)

Subnet ID

subnet-0ee5914bc196384ed (private\_sub)

Private IPv4 addresses

10.0.1.86

Public IPv4 DNS

-

Elastic IP addresses

-

AWS Compute Optimizer finding

Opt-in to AWS Compute Optimizer for recommendations. | [Learn more](#)

Auto Scaling Group name

-

Finally , that's all ! :)

You can access my github repo for this Lab through :

[https://github.com/EngyElhamzawy/Terraform\\_Labs](https://github.com/EngyElhamzawy/Terraform_Labs)