**Terraform Vpc**

provider "aws" {

region = "us-east-1"

}

# 1. VPC

resource "aws\_vpc" "myvpc" {

cidr\_block = "10.0.0.0/16"

enable\_dns\_support = true

enable\_dns\_hostnames = true

tags = {

Name = "myvpc"

}

}

# 2. Subnets

resource "aws\_subnet" "my\_pub\_resource" {

vpc\_id = aws\_vpc.myvpc.id

cidr\_block = "10.0.1.0/24"

map\_public\_ip\_on\_launch = true

availability\_zone = "us-east-1a"

tags = {

Name = "my\_pub\_resource"

}

}

resource "aws\_subnet" "my\_pvt\_resource" {

vpc\_id = aws\_vpc.myvpc.id

cidr\_block = "10.0.2.0/24"

availability\_zone = "us-east-1a"

tags = {

Name = "my\_pvt\_resource"

}

}

# 3. Internet Gateway

resource "aws\_internet\_gateway" "igw" {

vpc\_id = aws\_vpc.myvpc.id

tags = {

Name = "myvpc-igw"

}

}

# 4. Route Tables

resource "aws\_route\_table" "public\_rt" {

vpc\_id = aws\_vpc.myvpc.id

tags = {

Name = "myvpc-public-rt"

}

}

resource "aws\_route" "public\_route" {

route\_table\_id = aws\_route\_table.public\_rt.id

destination\_cidr\_block = "0.0.0.0/0"

gateway\_id = aws\_internet\_gateway.igw.id

}

resource "aws\_route\_table\_association" "public\_assoc" {

subnet\_id = aws\_subnet.my\_pub\_resource.id

route\_table\_id = aws\_route\_table.public\_rt.id

}

resource "aws\_route\_table" "private\_rt" {

vpc\_id = aws\_vpc.myvpc.id

tags = {

Name = "myvpc-private-rt"

}

}

resource "aws\_route\_table\_association" "private\_assoc" {

subnet\_id = aws\_subnet.my\_pvt\_resource.id

route\_table\_id = aws\_route\_table.private\_rt.id

}

# 5. Security Groups

resource "aws\_security\_group" "public\_sg" {

name = "public\_sg"

description = "Allow public traffic"

vpc\_id = aws\_vpc.myvpc.id

ingress {

from\_port = 22

to\_port = 22

protocol = "tcp"

cidr\_blocks = ["0.0.0.0/0"]

}

ingress {

from\_port = 80

to\_port = 80

protocol = "tcp"

cidr\_blocks = ["0.0.0.0/0"]

}

ingress {

from\_port = 443

to\_port = 443

protocol = "tcp"

cidr\_blocks = ["0.0.0.0/0"]

}

ingress {

from\_port = 3389

to\_port = 3389

protocol = "tcp"

cidr\_blocks = ["0.0.0.0/0"]

}

egress {

from\_port = 0

to\_port = 0

protocol = "-1"

cidr\_blocks = ["0.0.0.0/0"]

}

}

resource "aws\_security\_group" "private\_sg" {

name = "private\_sg"

description = "Allow all TCP from public SG"

vpc\_id = aws\_vpc.myvpc.id

ingress {

from\_port = 0

to\_port = 65535

protocol = "tcp"

security\_groups = [aws\_security\_group.public\_sg.id]

}

egress {

from\_port = 0

to\_port = 0

protocol = "-1"

cidr\_blocks = ["0.0.0.0/0"]

}

}

# 6. NAT Gateway + EIP

resource "aws\_eip" "nat\_eip" {

vpc = true

}

resource "aws\_nat\_gateway" "nat\_gw" {

allocation\_id = aws\_eip.nat\_eip.id

subnet\_id = aws\_subnet.my\_pub\_resource.id

tags = {

Name = "myvpc-nat-gw"

}

}

resource "aws\_route" "private\_route" {

route\_table\_id = aws\_route\_table.private\_rt.id

destination\_cidr\_block = "0.0.0.0/0"

nat\_gateway\_id = aws\_nat\_gateway.nat\_gw.id

}