







**Terraform main.tf**

provider "aws" {

  region = "ap-south-1" # Change as needed

}

# Create an S3 bucket

resource "aws\_s3\_bucket" "my\_bucket" {

  bucket = "my-terraform-bucket-841162683682"# Change to a unique name

}

# IAM Role for EC2 to access S3

resource "aws\_iam\_role" "ec2\_role" {

  name = "ec2\_s3\_access\_role"

  assume\_role\_policy = jsonencode({

    Version = "2012-10-17"

    Statement = [

      {

        Action = "sts:AssumeRole"

        Effect = "Allow"

        Principal = {

          Service = "ec2.amazonaws.com"

        }

      }

    ]

  })

}

# IAM Policy for S3 Access

resource "aws\_iam\_policy" "s3\_policy" {

  name        = "s3\_access\_policy"

  description = "Allows EC2 to access S3"

  policy = jsonencode({

    Version = "2012-10-17"

    Statement = [

      {

        Action = [

          "s3:GetObject",

          "s3:ListBucket",

          "s3:PutObject"

        ]

        Effect   = "Allow"

        Resource = [

          aws\_s3\_bucket.my\_bucket.arn,

          "${aws\_s3\_bucket.my\_bucket.arn}/\*"

        ]

      }

    ]

  })

}

# Attach Policy to Role

resource "aws\_iam\_role\_policy\_attachment" "s3\_attachment" {

  role       = aws\_iam\_role.ec2\_role.name

  policy\_arn = aws\_iam\_policy.s3\_policy.arn

}

# IAM Instance Profile

resource "aws\_iam\_instance\_profile" "ec2\_profile" {

  name = "ec2\_instance\_profile"

  role = aws\_iam\_role.ec2\_role.name

}

# Create EC2 Instance

resource "aws\_instance" "my\_instance" {

  ami           = "ami-0ddfba243cbee3768" # Change to latest Amazon Linux 2 AMI

  instance\_type = "t2.micro"

  iam\_instance\_profile = aws\_iam\_instance\_profile.ec2\_profile.name

  tags = {

    Name = "EC2-With-S3-Access"

  }

}

# Create CloudWatch Log Group

resource "aws\_cloudwatch\_log\_group" "ec2\_log\_group" {

  name              = "/aws/ec2/my-instance-logs"

  retention\_in\_days = 7

}

# Create CloudWatch Log Stream

resource "aws\_cloudwatch\_log\_stream" "ec2\_log\_stream" {

  name           = "ec2-log-stream"

  log\_group\_name = aws\_cloudwatch\_log\_group.ec2\_log\_group.name

}

# IAM Policy for CloudWatch Logs

resource "aws\_iam\_policy" "cloudwatch\_policy" {

  name        = "cloudwatch\_logs\_policy"

  description = "Allows EC2 to write logs to CloudWatch"

  policy = jsonencode({

    Version = "2012-10-17"

    Statement = [

      {

        Action = [

          "logs:CreateLogStream",

          "logs:PutLogEvents"

        ]

        Effect   = "Allow"

        Resource = "${aws\_cloudwatch\_log\_group.ec2\_log\_group.arn}:\*"

      }

    ]

  })

}

# Attach CloudWatch Policy to EC2 Role

resource "aws\_iam\_role\_policy\_attachment" "cloudwatch\_attachment" {

  role       = aws\_iam\_role.ec2\_role.name

  policy\_arn = aws\_iam\_policy.cloudwatch\_policy.arn

}