

# **HashiCorp Certified Terraform Associate 2025**

# PPT Version

PPT Release Date = 26th December 2024

We regularly release new version of PPT when we update this course.

Please check regularly that you are using the latest version.

The Latest Version Details are mentioned in the PPT Lecture in Section 1.

# Understanding the Need

My personal journey started with implementing “AWS Hardening” guidelines.

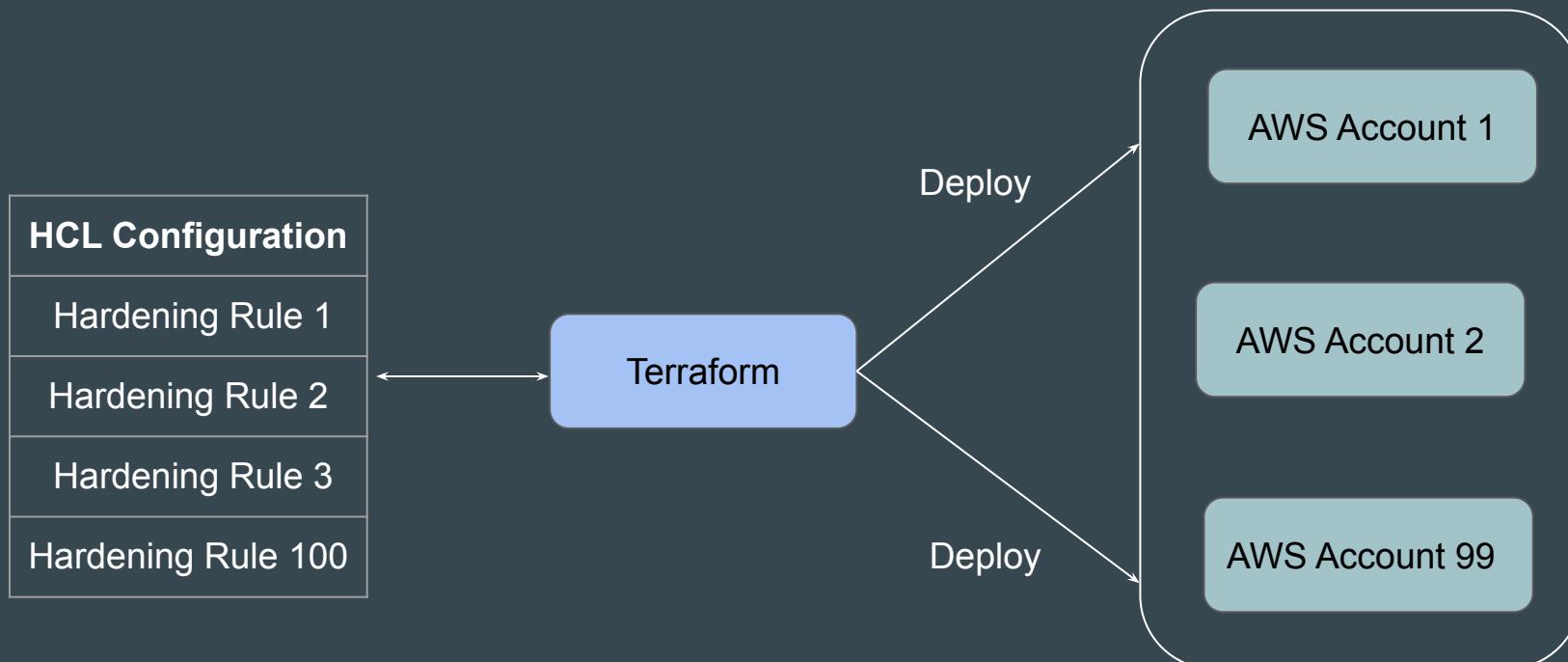
There were 100+ pages of guidelines, and it used to take 2-3 days to implement in 1 account.

Nowadays, it is more than 250+ pages.



# Challenge that Terraform Solves

Terraform allows us to create reusable code that can deploy identical set of infrastructure in a repeatable fashion.



# Amazing Terraform

One of the great benefits of Terraform is that it supports thousands of providers.

Once you learn Terraform Core concepts, you can write code to create and manage infrastructure across all the providers.



# Overview of Terraform Certification

Terraform has become one of the most popular and widely used tools to create and manage infrastructure and one of the defacto IAC tools for DevOps.

HashiCorp has released the official Terraform certification to certify students related to core Terraform concepts and skills.



# What Does this Course Cover?

We start this course of Terraform from absolute scratch and then we move ahead with advance topics.

We cover ALL the topics of the official exams.



# About Me

- DevSecOps Engineer - Defensive Security.
- Teaching is one of my passions.
- I have total of 16 courses, and around 350,000+ students now.

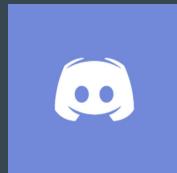
## Something about me :-

- HashiCorp Certified [Terraform, Vault, Consul] Associate.
- AWS Certified [DevOps Pro, SA Pro, Advanced Networking, Security Specialty ...]
- RedHat Certified Architect (RHCA) + 13 more Certifications
- Part time Security Consultant



# Join us in our Adventure

Be Awesome



[kplabs.in/chat](https://kplabs.in/chat)



[kplabs.in/linkedin](https://kplabs.in/linkedin)

# **About the Course**

# Understanding the Basics

This is a **certification specific course** and we cover all the pointers that are part of the official exam blueprint.

The screenshot shows a user interface for a certification exam. At the top, there's a navigation bar with 'Certification' on the left, 'Overview' in the middle, and 'Certifications' with a dropdown arrow on the right. Below this, the main content area has a title 'Exam objectives' in large white font. The objectives are listed in a table format:

<b>1</b>	<b>Understand infrastructure as code (IaC) concepts</b>
1a	Explain what IaC is
1b	Describe advantages of IaC patterns
<b>2</b>	<b>Understand the purpose of Terraform (vs other IaC)</b>
2a	Explain multi-cloud and provider-agnostic benefits
2b	Explain the benefits of state

## Point to Note

The arrangement of topics in this course is a little different from the exam blueprint to ensure this course remains beginner friendly and topics are covered in a step by step manner.

# Course Resource - GitHub

All the code that we use during practicals have been added to our GitHub page.

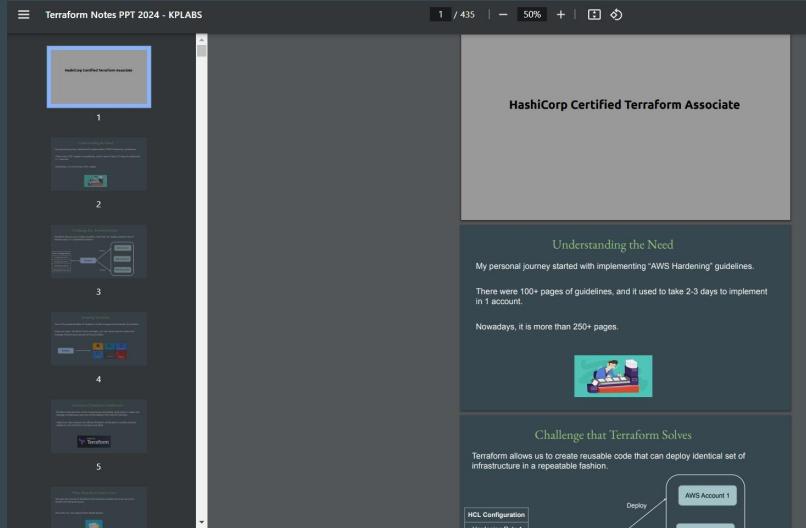
The screenshot shows a GitHub repository page for the user 'zealvora' with the repository name 'terraform-beginner-to-advanced-resource'. The repository is public and has 1 branch and 0 tags. The master branch is selected. The page displays a list of 127 commits, with the most recent commit being a merge pull request from 'vk31032022/patch-1' at 17 hours ago. The commits are organized into sections: 'Section 1 - Deploying Infrastructure with Terra...', 'Section 2 - Read, Generate, Modify Configuration...', 'Section 3 - Terraform Provisioners', 'Section 4 - Terraform Modules & Workspaces', 'Section 5 - Remote State Management', 'Section 6 - Security Primer', 'Section 7 - Terraform Cloud & Enterprise Capa...', and 'Readme.md'. The commits for 'Readme.md' and 'Section 7' are from last week, while others are from June 2023 or earlier.

Commit Details	Date
zealvora Merge pull request #22 from vk31032022/patch-1	17 hours ago
Section 1 - Deploying Infrastructure with Terra...	June 2023 Update
Section 2 - Read, Generate, Modify Configuration...	Merge pull request #22 from vk31032022/patch-1
Section 3 - Terraform Provisioners	Update remote-exec.md
Section 4 - Terraform Modules & Workspaces	Updating Year of Update in Repo
Section 5 - Remote State Management	Update eip.tf
Section 6 - Security Primer	Update multiple-providers.md
Section 7 - Terraform Cloud & Enterprise Capa...	Updating Year of Update in Repo
Readme.md	Update Readme.md

# Course Resource - PPT Slides

ALL the slides that we use in this course is available to download as PDF.

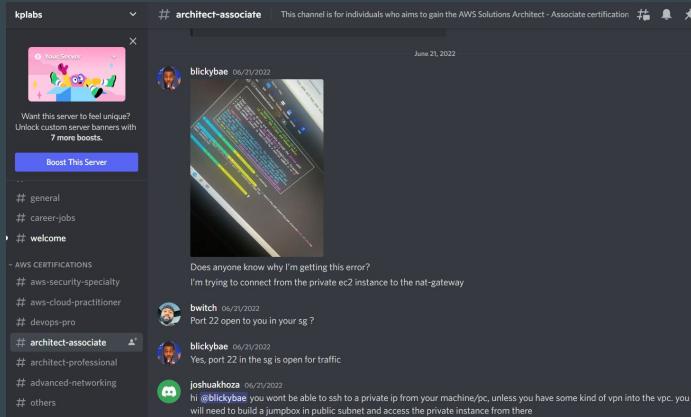
The PDF is attached as part of the lecture titled “Central PPT Notes”.



# Our Community (Optional)

We also have a Discord community that allows all the individuals who are preparing for the same certification to connect with each other for discussions as well as technical support.

<https://kplabs.in/chat>



# Important Note - Platform for This Course

Terraform supports hundreds of platforms like AWS, Azure, GCP etc.

To learn Terraform concepts, we have to choose 1 platform for our testing.

For this course we have chosen AWS.



# Clarification Regarding AWS Platform

Aim of this course is to learn Core Concepts of Terraform and not AWS.

We use very basic AWS services like Virtual Machine, AWS users to demonstrate and Learn the Core Terraform concepts.

The Terraform structure and concepts remain SAME irrespective of platform.

We have hundreds of users from different platform like Azure who have completed this course and are actively implementing Terraform for different platforms..

# **Infrastructure as Code (IAC)**

# Understanding the Basics

There are two ways in which you can create and manage your infrastructure:

- Manually approach.
- Through Automation



# Work Requirement: Database Backup

I was assigned a task to take database backup every day at 10 PM and the backup had to be stored in Amazon S3 Storage with appropriate timestamp.

- db-backup-01-01-2024.sql
- db-backup-02-01-2024.sql

Initially due to lack of time, I used to manually take DB backup at 10 PM and upload it to S3.



# Learning from this Work Requirement

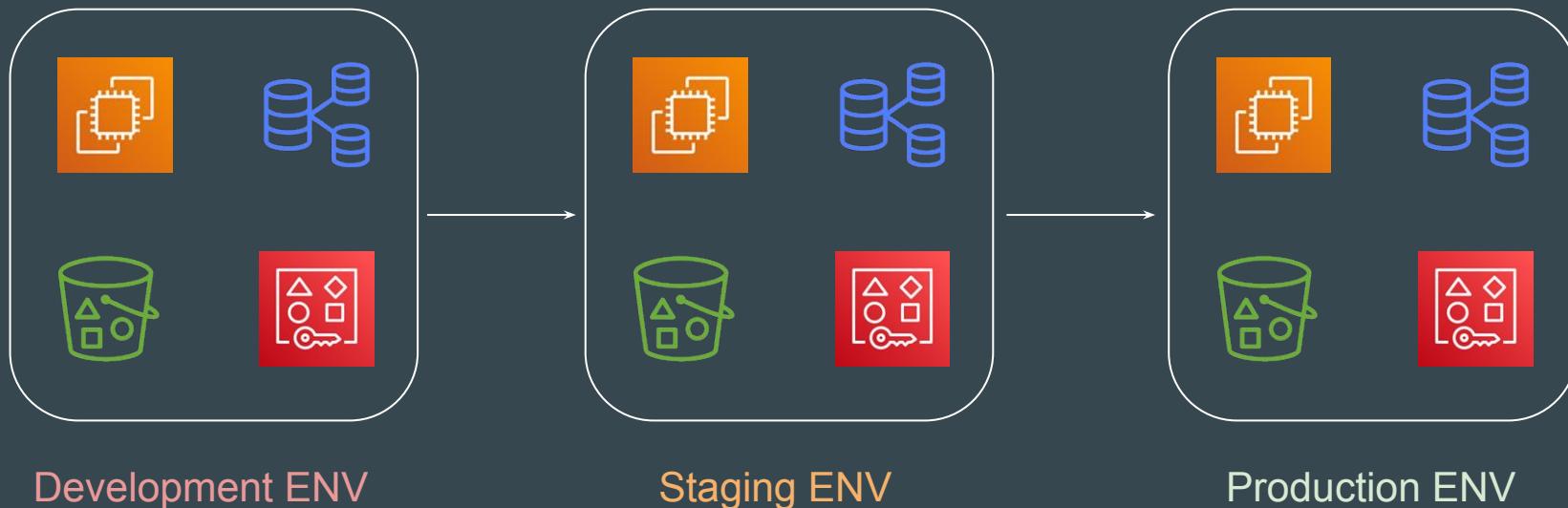
If a particular task has to be done in an repeatable manner, it MUST be automated.

## Points to Note:

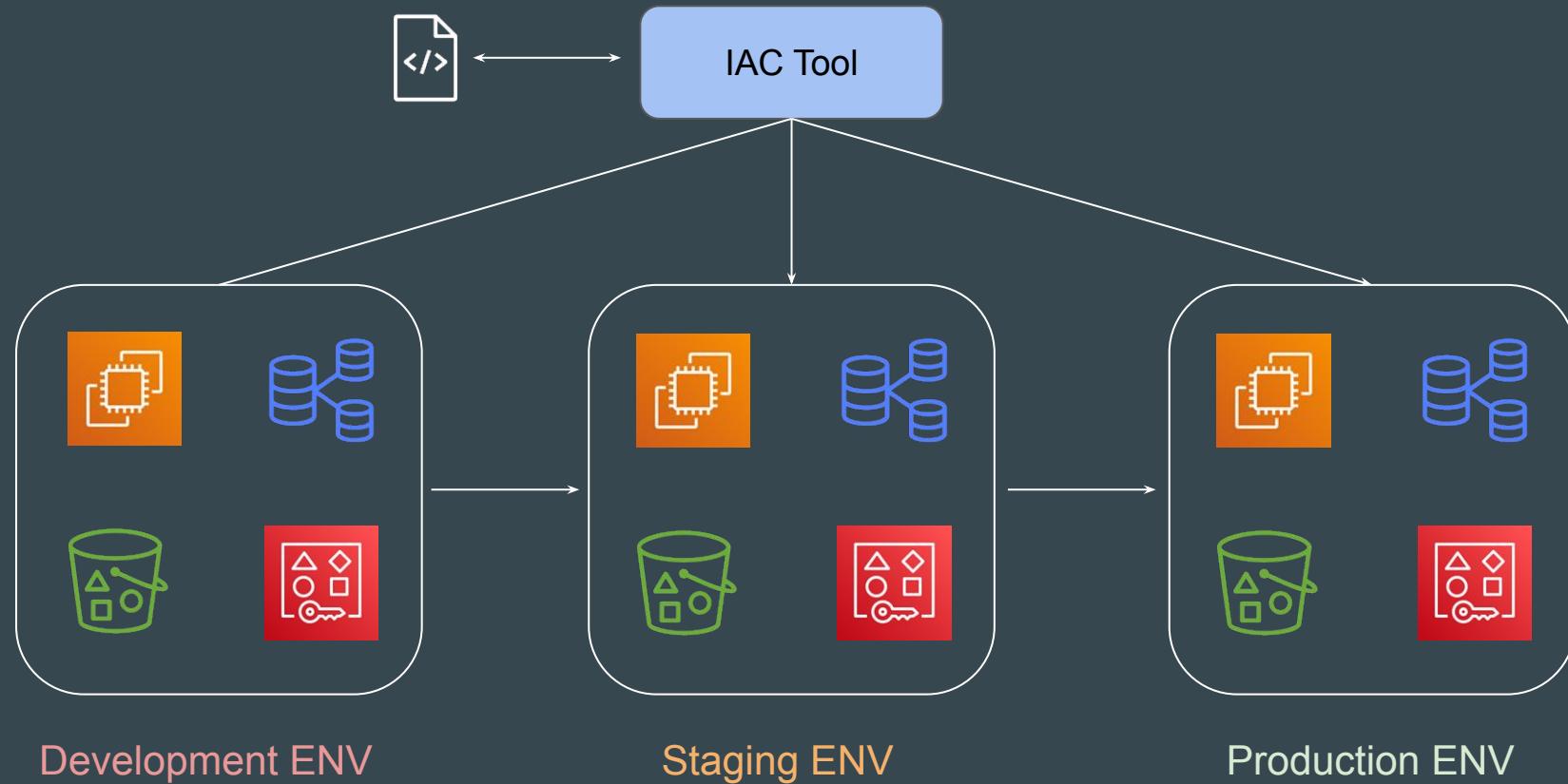
1. Depending on the type of task, the tools for automation will change.
2. There are wide variety of Tools & Technologies used for Automation like Ansible, CloudFormation, Terraform, Python etc.

# Example of a Single Service

Set of resources (Virtual Machine, Database, S3, AWS Users) must be created with exact similar configuration in Dev, Stage and Production environment.



# Example of a Single Service - Automated Way



# Basics of Infrastructure as Code

Infrastructure as Code (IaC) is the managing and provisioning of infrastructure through code instead of through manual processes.

```
! test.yaml
AWSTemplateFormatVersion: 2010-09-09
Description: Simple EC2

Resources:
  WebAppInstance:
    Type: AWS::EC2::Instance
    Properties:
      ImageId: ami-079db87dc4c10ac91
      InstanceType: t2.micro
```

```
! vm.tf > ...
resource "aws_instance" "myec2" {
  ami = "ami-079db87dc4c10ac91"
  instance_type = "t2.micro"
}
```

# Benefits of Infrastructure As Code

There are several benefits of designing your infrastructure as code:

- Speed of Infrastructure Management.
- Low Risk of Human Errors.
- Version Control.
- Easy collaboration between Teams.

# **Choosing Right IAC Tool**

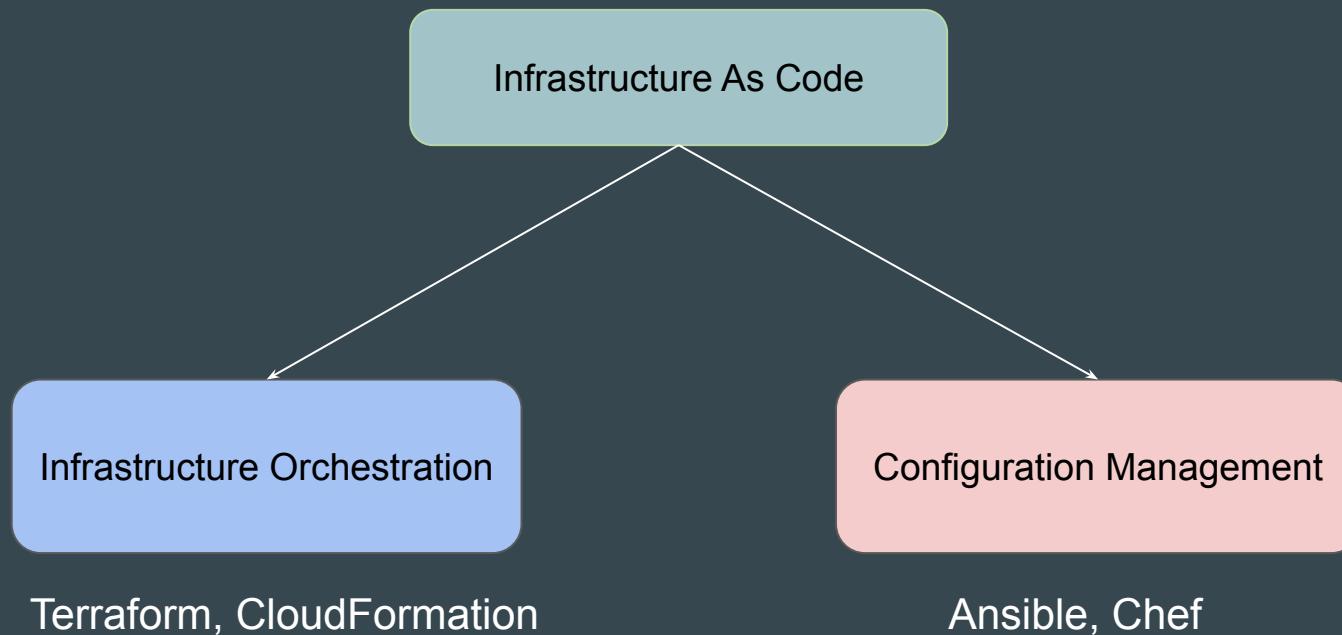
# Available Tools

There are various types of tools that can allow you to deploy infrastructure as code :

- Terraform
- CloudFormation
- Heat
- Ansible
- SaltStack
- Chef, Puppet and others

# Categories of Tools

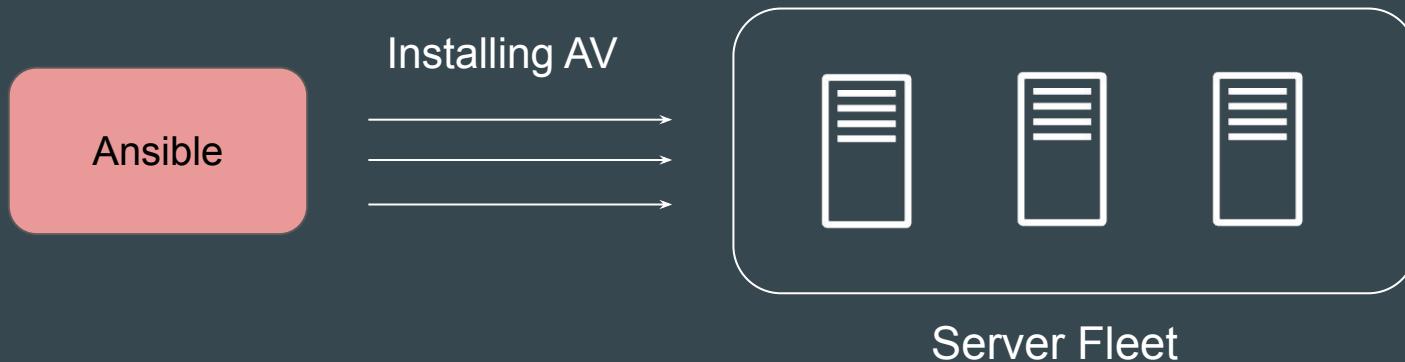
The tools are widely divided into two major categories



# Configuration Management

Configuration Management tools are primarily used to maintain desired configuration of systems (inside servers)

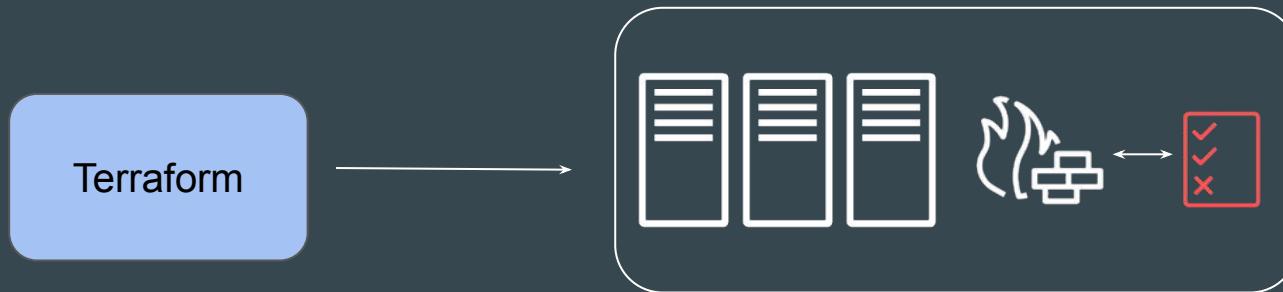
Example: ALL servers should have Antivirus installed with version 10.0.2



# Infrastructure Orchestration

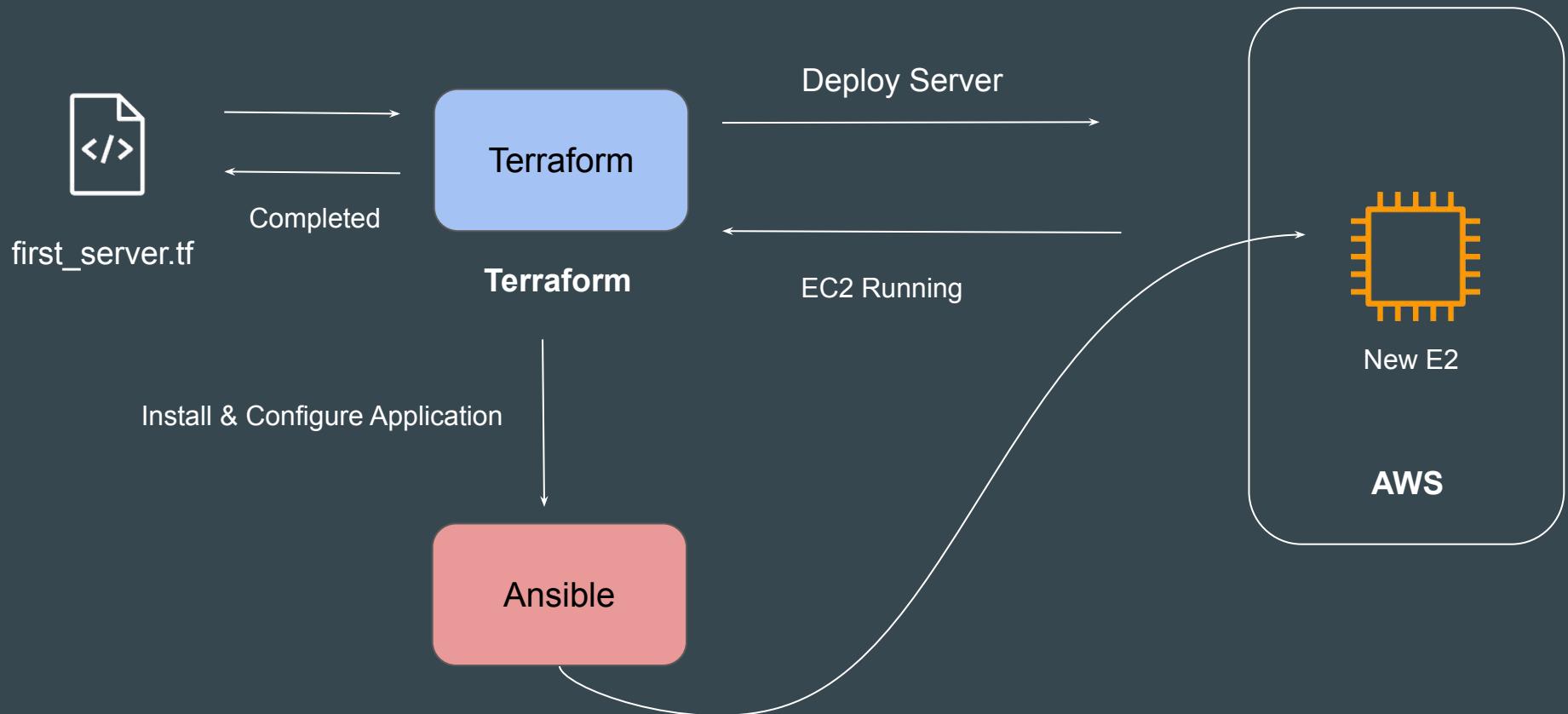
Infrastructure Orchestration is primarily used to create and manage infrastructure environments.

Example: Create 3 Servers with 4 GB RAM, 2 vCPUs. Each server should have firewall rule to allow SSH connection from Office IPs.



Infrastructure Fleet

# IAC & Configuration Management = Friends



# How to choose IAC Tool?

- i) Is your infrastructure going to be vendor specific in longer term ? Example AWS.
- ii) Are you planning to have multi-cloud / hybrid cloud based infrastructure ?
- iii) How well does it integrate with configuration management tools ?
- iv) Price and Support

# Use-Case 1 - Requirement of Organization 1

1. Organization is going to be based on AWS for next 25 years.
2. Official support is required in-case if team face any issue related to IAC tool or code itself.
3. They want some kind of GUI interface that supports automatic code generation.

## Use-Case 2 - Requirement of Organization 2

1. Organization is based on Hybrid Solution. They use VMware for on-premise setup; AWS, Azure and GCP for Cloud.
2. Official support is required in-case if IAC tool has any issues.

---

# Installing Terraform

Terraform in detail

---

# Overview of Installation Process

Terraform installation is very simple.

You have a single binary file, download and use it.



# Supported Platforms

Terraform works on multiple platforms, these includes:

- Windows
- macOS
- Linux
- FreeBSD
- OpenBSD
- Solaris

# Terraform Installation - Mac & Linux

There are two primary steps required to install terraform in Mac and Linux

- 1) Download the Terraform Binary File.
- 2) Move it in the right path.

---

# Choosing IDE For Terraform

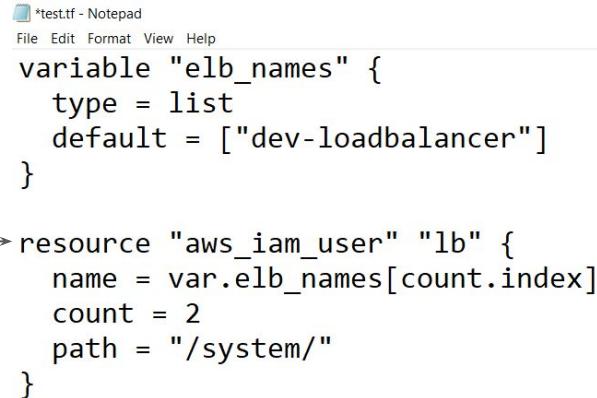
Terraform in detail

# Terraform Code in NotePad!

You can write Terraform code in Notepad and it will not have any impact.

## Downsides:

- Slower Development
- Limited Features



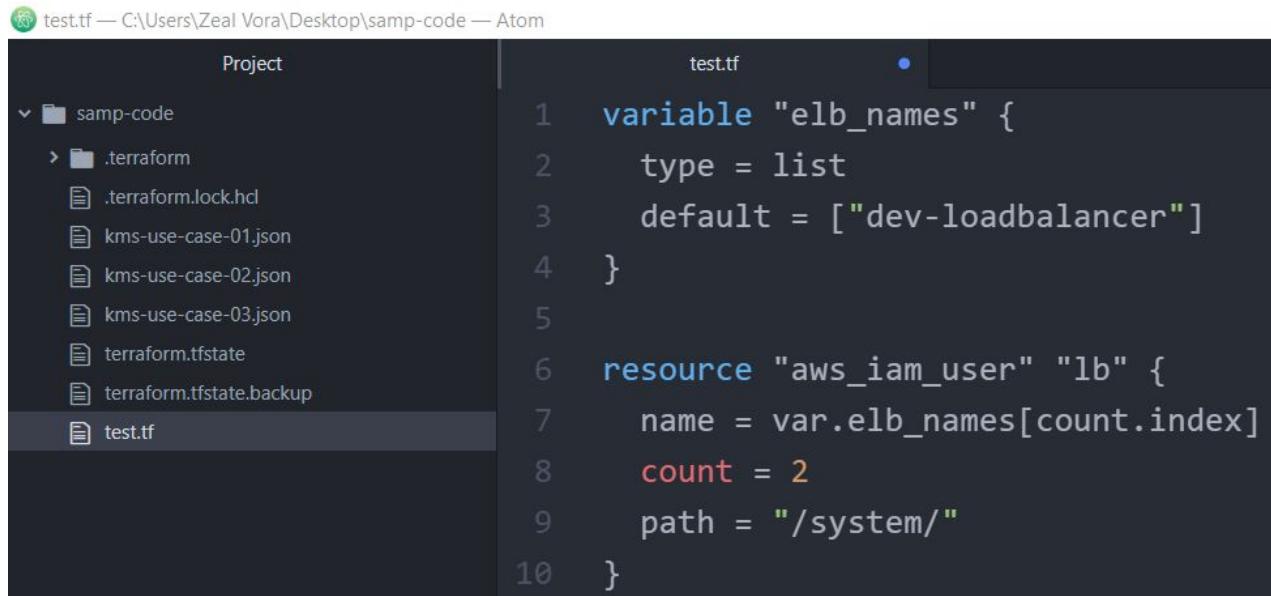
A screenshot of a Windows Notepad window titled "\*test.tf - Notepad". The menu bar includes File, Edit, Format, View, and Help. The code in the editor is:

```
variable "elb_names" {
  type = list
  default = ["dev-loadbalancer"]
}

resource "aws_iam_user" "lb" {
  name = var.elb_names[count.index]
  count = 2
  path = "/system/"
}
```

# Need of a Better Software

There is a need of a better application that allows us to develop code faster.

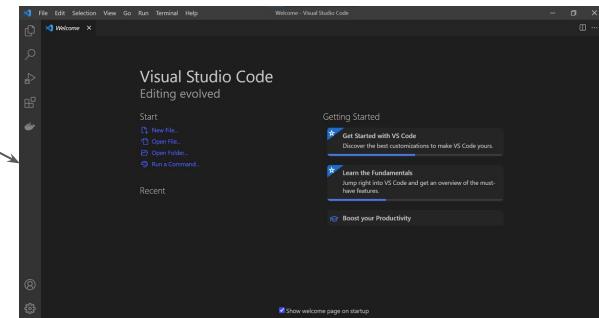


The screenshot shows the Atom code editor interface. On the left, the 'Project' sidebar lists a directory structure under 'samp-code': '.terraform', '.terraform.lock.hcl', 'kms-use-case-01.json', 'kms-use-case-02.json', 'kms-use-case-03.json', 'terraform.tfstate', 'terraform.tfstate.backup', and 'test.tf'. The 'test.tf' file is currently selected and shown in the main editor area. The code in 'test.tf' is:

```
1 variable "elb_names" {
2     type = list
3     default = ["dev-loadbalancer"]
4 }
5
6 resource "aws_iam_user" "lb" {
7     name = var.elb_names[count.index]
8     count = 2
9     path = "/system/"
10 }
```

# What are the Options!

There are many popular source code editors available in the market.

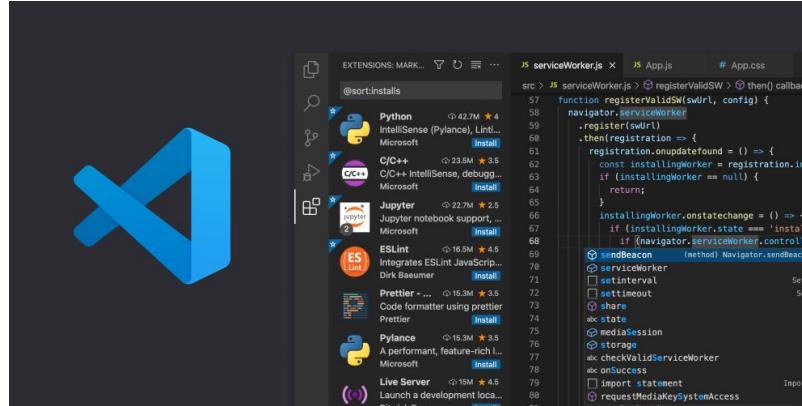


# Editor for This Course

We are going to make use of [Visual Studio Code](#) as primary editor in this course.

## Advantages:

1. Supports Windows, Mac, Linux
2. Supports Wide variety of programming languages.
3. Many Extensions.





# Using Notepad

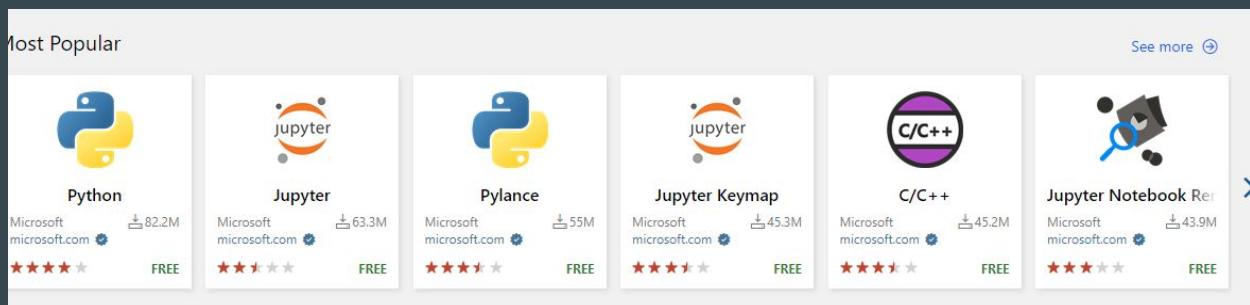
# Using Visual Studio Code

# **Visual Studio Code Extensions**

# Understanding the Basics

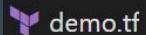
Extensions are add-ons that allow you to customize and enhance your experience in Visual Studio by adding new features or integrating existing tools

They offer wide range of functionality related to colors, auto-complete, report spelling errors etc.

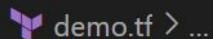


# Terraform Extension

HashiCorp also provides extension for Terraform for Visual Studio Code.



```
demo.tf
resource "aws_instance" "myec2" {
    ami = "ami-00c39f71452c08778"
    instance_type = "t2.micro"
}
```



```
demo.tf > ...
resource "aws_instance" "myec2" {
    ami = "ami-00c39f71452c08778"
    instance_type = "t2.micro"
}
```

---

# Setting up the Lab

Let's start Rolling !

---

# Let's Start

- i) Create a new AWS Account.
- ii) Begin the course



# Registering an AWS Account



The screenshot shows the AWS Free Tier landing page. At the top, there's a dark navigation bar with the AWS logo, a "Create an AWS Account" button, and language and account options. Below this is a large banner with a purple-to-yellow gradient background featuring the text "AWS Free Tier" and a "Create a Free Account" button. Underneath the banner, there are three main links: "Free Tier Details", "Get Started", and "Free Tier Software". At the bottom of the page, there's a section titled "AWS Free Tier Details" with filters for "FEATURED", "12 MONTHS FREE", "ALWAYS FREE", "TRIALS", "PRODUCT CATEGORIES", and "ALL".

AWS Free Tier

The AWS Free Tier enables you to gain free, hands-on experience with the AWS platform, products, and services.

Create a Free Account

Free Tier Details      Get Started      Free Tier Software

AWS Free Tier Details

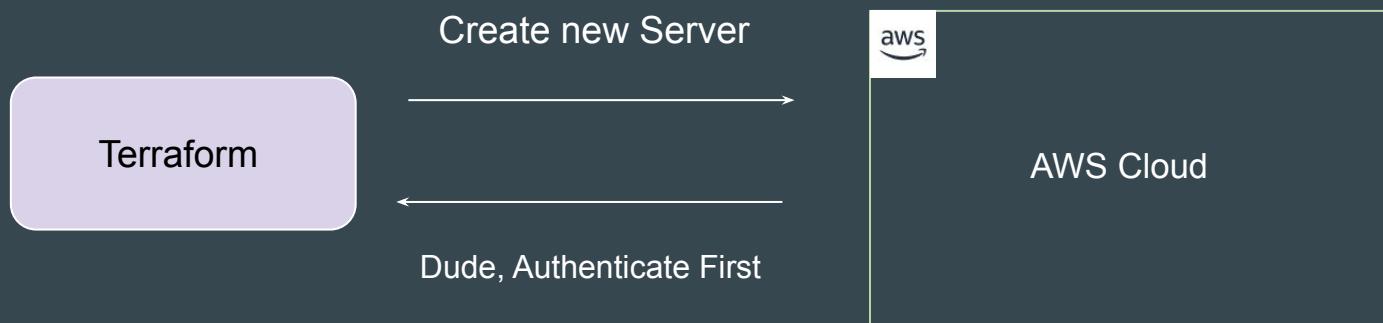
★ FEATURED    12 MONTHS FREE    ALWAYS FREE    TRIALS    PRODUCT CATEGORIES    ALL

# Authentication and Authorization



# Understanding the Basics

Before we start working on managing environments through Terraform, the first important step is related to Authentication and Authorization.



# Basics of Authentication and Authorization

Authentication is the process of verifying who a user is.

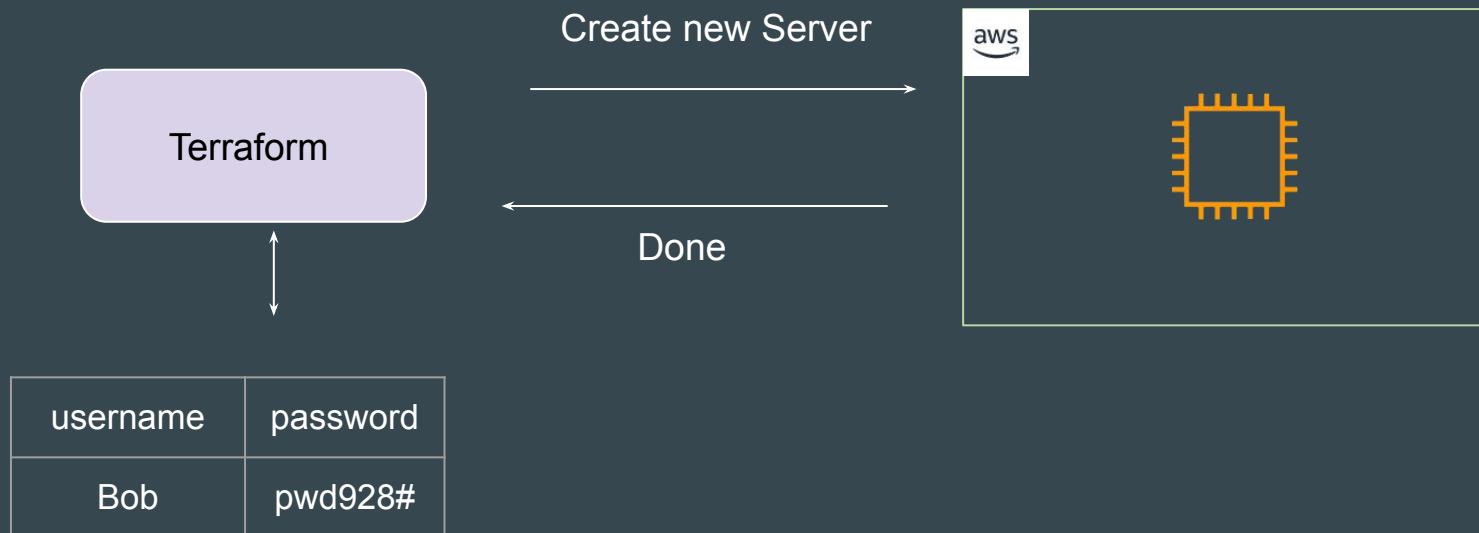
Authorization is the process of verifying what they have access to

Example:

Alice is a user in AWS with no access to any service.

# Learning for Todays' Video

Terraform needs **access credentials with relevant permissions** to create and manage the environments.

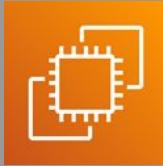


# Access Credentials

Depending on the provider, the type of access credentials would change.

Provider	Access Credentials
AWS	Access Keys and Secret Keys
GitHub	Tokens
Kubernetes	Kubeconfig file, Credentials Config
Digital Ocean	Tokens

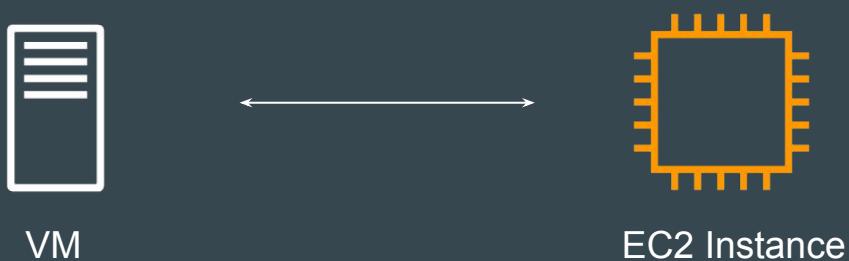
# First Virtual Machine Through Terraform



# Revising the Basics of EC2

EC2 stands for Elastic Compute Cloud.

In-short, it's a name for a virtual server that you launch in AWS.



# Available Regions

Cloud providers offers multiple regions in which we can create our resource.

You need to decide the region in which Terraform would create the resource.



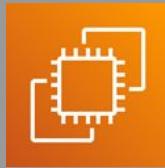
# Virtual Machine Configuration

A Virtual Machine would have it's own set of configurations.

- CPU
- Memory
- Storage
- Operating System

While creating VM through Terraform, you will need to define these.

# Providers and Resources



# Basics of Providers

Terraform supports multiple providers.

Depending on what type of infrastructure we want to launch, we have to use appropriate providers accordingly.



# Learning 1 - Provider Plugins

A provider is a plugin that lets Terraform manage an external API.

When we run `terraform init`, plugins required for the provider are automatically downloaded and saved locally to a `.terraform` directory.

```
C:\Users\zealv\Desktop\kplabs-terraform>terraform init

Initializing the backend...

Initializing provider plugins...
- Finding latest version of hashicorp/aws...
- Installing hashicorp/aws v4.60.0...
- Installed hashicorp/aws v4.60.0 (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
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.
```

# Learning 2 - Resource

Resource block describes one or more infrastructure objects

Example:

- resource aws\_instance
- resource aws\_alb
- resource iam\_user
- resource digitalocean\_droplet

```
resource "aws_instance" "myec2" {  
    ami = "ami-082b5a644766e0e6f"  
    instance_type = "t2.micro"  
}
```

# Learning 3 - Resource Blocks

A resource block declares a resource of a given type ("aws\_instance") with a given local name ("myec2").

Resource type and Name together serve as an identifier for a given resource and so must be unique.

```
resource "aws_instance" "myec2" {  
    ami = "ami-082b5a644766e0e6f"  
    instance_type = "t2.micro"  
}
```

EC2 Instance Number 1

```
resource "aws_instance" "web" {  
    ami           = ami-123  
    instance_type = "t2.micro"  
}
```

EC2 Instance Number 2

# Point to Note

You can only use the resource that are supported by a specific provider.

In the below example, provider of Azure is used with resource of aws\_instance

```
provider "azurerm" {}

resource "aws_instance" "web" {
    ami           = ami-123
    instance_type = "t2.micro"

}
```

# Important Question

The core concepts, standard syntax remains similar across all providers.

If you learn the basics, you should be able to work with all providers easily.



# Issues and Bugs with Providers

A provider that is maintained by HashiCorp does not mean it has no bugs.

It can happen that there are inconsistencies from your output and things mentioned in documentation. You can raise issue at Provider page.

The screenshot shows a GitHub Issues page with the following details:

- Open Issues:** 3,698 Open, 11,345 Closed
- Filters:** Author, Label, Projects, Milestones
- Issues:**
  - [Bug]: Provider produced inconsistent final plan [#30281](#) opened 10 minutes ago by akothawala
  - [Bug]: tags\_all is showing sensitive data [#30278](#) opened 10 hours ago by askmike1
  - [Enhancement]: Ephemeral storage support in batch [#30274](#) opened 15 hours ago by bmaisonn
  - [Docs]: Missing detail about KMS in secretsmanager\_secret.html.markdown which prevents cross-account access [#30272](#) opened 17 hours ago by v-rosa

# Relax and Have a Meme Before Proceeding

That stupid walk you do when  
someone's mopping a floor and you  
know you're gonna walk over it but you  
want them to see how sorry you are to  
be walking over it so you make  
yourself look like you're walking over  
hot lava.



It ain't much, but it's honest work

# Provider Tiers



# Provider Maintainers

There are 3 primary type of provider tiers in Terraform.

Provider Tiers	Description
Official	Owned and Maintained by HashiCorp.
Partner	Owned and Maintained by Technology Company that maintains direct partnership with HashiCorp.
Community	Owned and Maintained by Individual Contributors.

# Provider Namespace

Namespaces are used to help users identify the organization or publisher responsible for the integration

Tier	Description
Official	hashicorp
Partner	Third-party organization e.g. mongodb/mongodbatlas
Community	Maintainer's individual or organization account, e.g. DeviaVir/gsuite

# Important Learning

Terraform requires explicit source information for any providers that are not HashiCorp-maintained, using a new syntax in the required\_providers nested block inside the terraform configuration block

```
provider "aws" {  
    region      = "us-west-2"  
    access_key  = "PUT-YOUR-ACCESS-KEY-HERE"  
    secret_key  = "PUT-YOUR-SECRET-KEY-HERE"  
}
```

HashiCorp Maintained

```
terraform {  
    required_providers {  
        digitalocean = {  
            source = "digitalocean/digitalocean"  
        }  
    }  
}  
  
provider "digitalocean" {  
    token = "PUT-YOUR-TOKEN-HERE"  
}
```

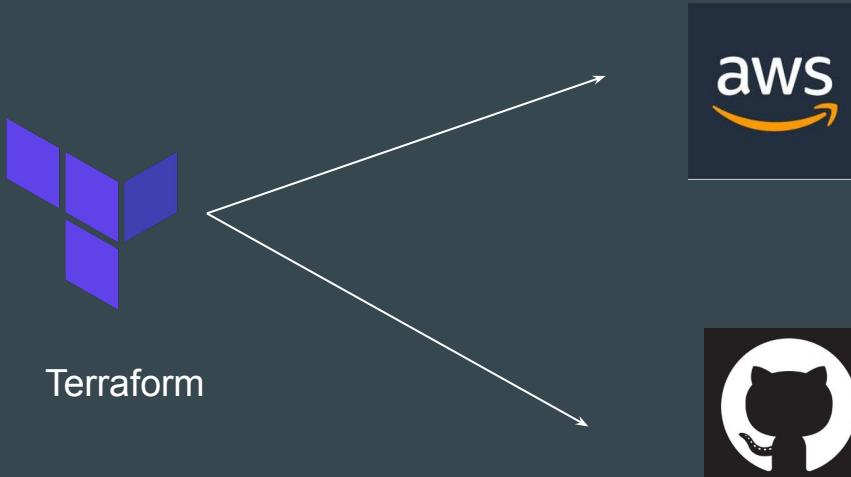
Non-HashiCorp Maintained

# **Terraform Destroy**

# Learning to Destroy Resources

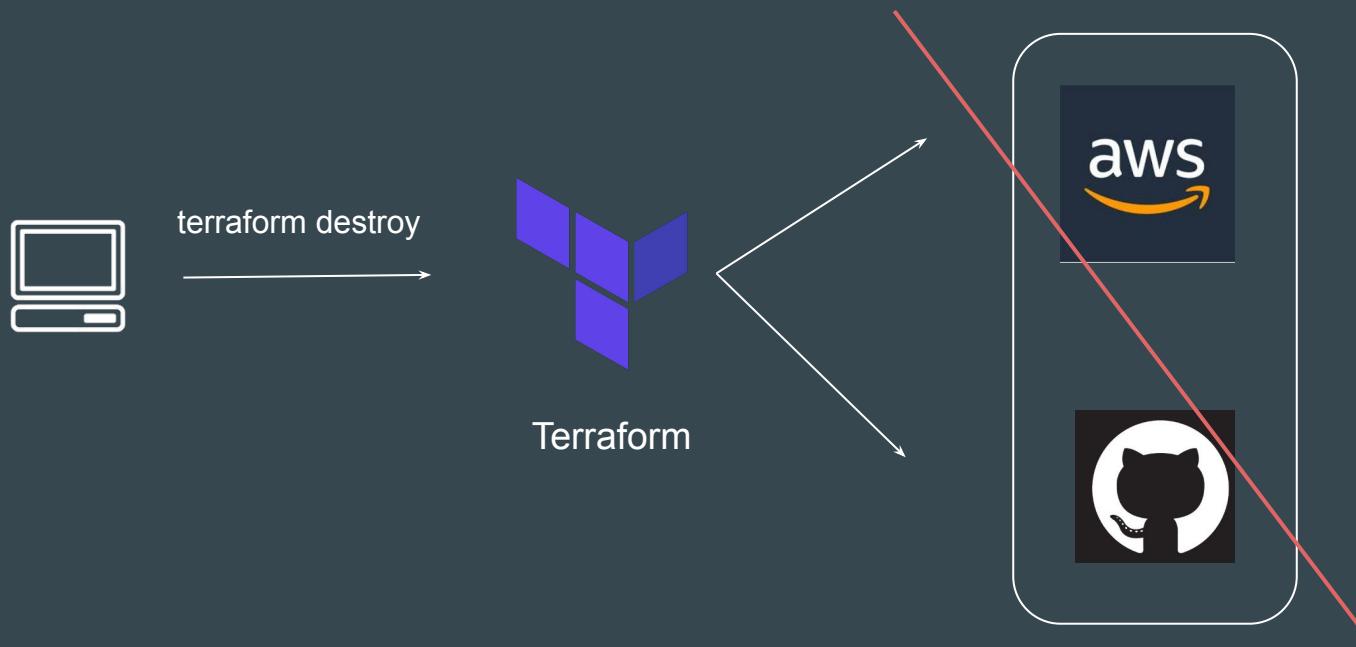
If you keep the infrastructure running, you will get charged for it.

Hence it is important for us to also know on how we can delete the infrastructure resources created via terraform.



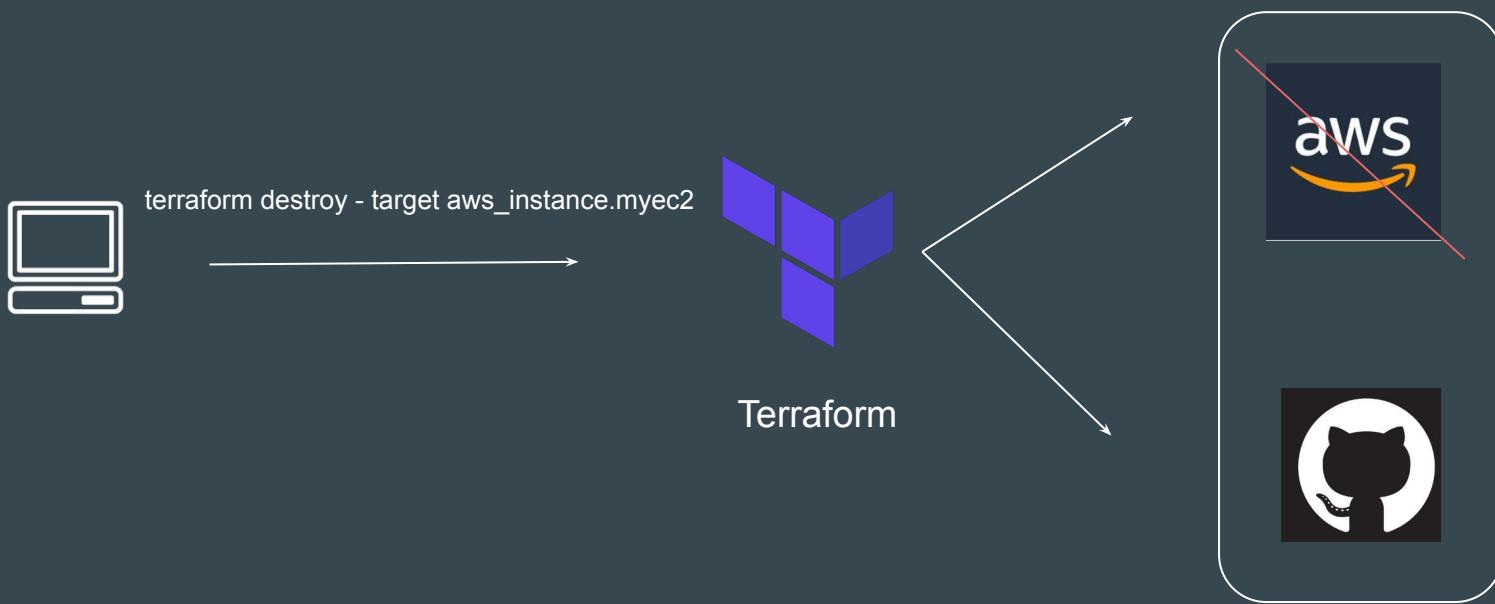
# Approach 1 - Destroy ALL

**terraform destroy** allows us to destroy all the resource that are created within the folder.



## Approach 2 - Destroy Some

terraform destroy with **-target** flag allows us to destroy specific resource.



# Terraform Destroy with Target

The **-target** option can be used to focus Terraform's attention on only a subset of resources.

Combination of : Resource Type + Local Resource Name

Resource Type	Local Resource Name
aws_instance	myec2
github_repository	example

```
resource "aws_instance" "myec2" {  
    ami = "ami-00c39f71452c08778"  
    instance_type = "t2.micro"  
}
```

```
resource "github_repository" "example" {  
    name      = "example"  
    description = "My awesome codebase"  
    visibility = "public"  
}
```

---

# Terraform State File

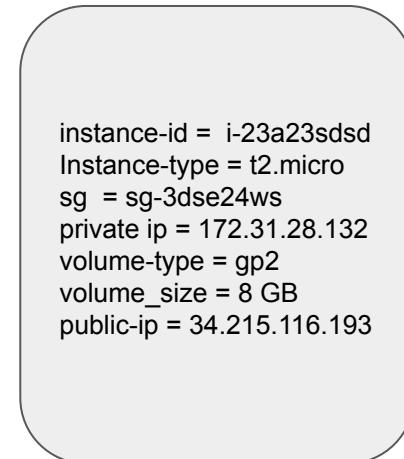
Terraform in detail

---

# State File

Terraform stores the state of the infrastructure that is being created from the TF files.

This state allows terraform to map real world resource to your existing configuration.



State File



EC2 Instance



```
instance-id = i-23a23sdsd  
Instance-type = t2.micro  
sg = sg-3dse24ws  
private ip = 172.31.28.132  
volume-type = gp2  
volume_size = 8 GB  
public-ip = 34.215.116.193
```



GitHub Repo



```
name = terraform-repo  
branch = default  
type = private
```



EC2 Instance



GitHub Repo



```
name  = terraform-repo  
branch = default  
type   = private
```

---

# Desired & Current State

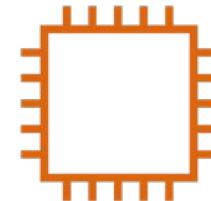
Terraform in detail

---

# Desired State

Terraform's primary function is to create, modify, and destroy infrastructure resources to match the desired state described in a Terraform configuration

```
resource "aws_instance" "myec2" {  
    ami = "ami-082b5a644766e0e6f"  
    instance_type = "t2.micro"  
}
```



EC2 - t2.micro

# Current State

Current state is the actual state of a resource that is currently deployed.

```
resource "aws_instance" "myec2" {  
    ami = "ami-082b5a644766e0e6f"  
    instance_type = "t2.micro"  
}
```



t2.medium

# Important Pointer

Terraform tries to ensure that the deployed infrastructure is based on the desired state.

If there is a difference between the two, terraform plan presents a description of the changes necessary to achieve the desired state.



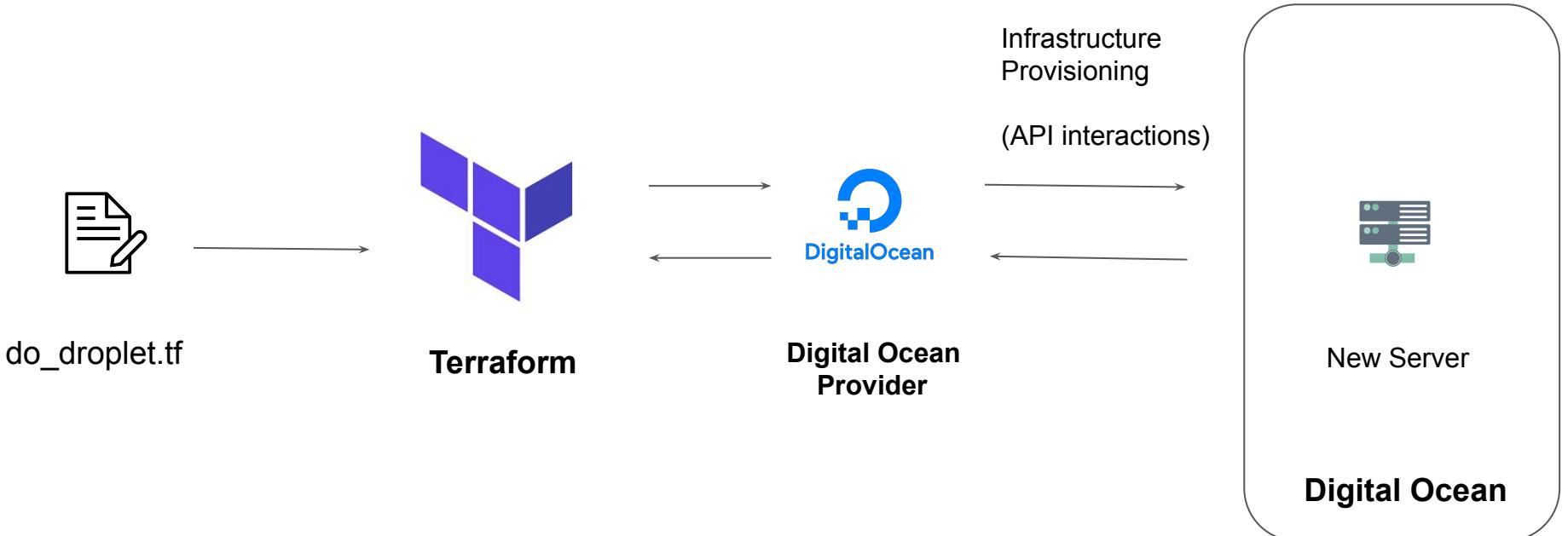
---

# Provider Versioning

Terraform in detail

---

# Provider Architecture



# Overview of Provider Versioning

Provider plugins are released separately from Terraform itself.

They have different set of version numbers.

.



Version 1



Version 2

# Explicitly Setting Provider Version

During terraform init, if version argument is not specified, the most recent provider will be downloaded during initialization.

For production use, you should constrain the acceptable provider versions via configuration, to ensure that new versions with breaking changes will not be automatically installed.

```
terraform {  
    required_providers {  
        aws = {  
            source  = "hashicorp/aws"  
            version = "~> 3.0"  
        }  
    }  
}  
  
provider "aws" {  
    region = "us-east-1"  
}
```

# Arguments for Specifying provider

There are multiple ways for specifying the version of a provider.

<b>Version Number Arguments</b>	<b>Description</b>
<code>&gt;=1.0</code>	Greater than equal to the version
<code>&lt;=1.0</code>	Less than equal to the version
<code>~&gt;2.0</code>	Any version in the 2.X range.
<code>&gt;=2.10,&lt;=2.30</code>	Any version between 2.10 and 2.30

# Dependency Lock File

Terraform dependency lock file allows us to lock to a specific version of the provider.

If a particular provider already has a selection recorded in the lock file, Terraform will always re-select that version for installation, even if a newer version has become available.

You can override that behavior by adding the `-upgrade` option when you run `terraform init`,

```
provider "registry.terraform.io/hashicorp/aws" {
    version      = "2.70.0"
    constraints = ">= 2.31.0, <= 2.70.0"
    hashes = [
        "h1:fx8tbGVwK1YIDI6UdHLnorC9PA1ZPSWEeW3V3aDCdWY=",
        "zh:01a5f351146434b418f9ff8d8cc956ddc801110f1cc8b139e01be2ff8c544605",
        "zh:1ec08abbaf09e3e0547511d48f77a1e2c89face2d55886b23f643011c76cb247",
        "zh:606d134fef7c1357c9d155aadbee6826bc22bc0115b6291d483bc1444291c3e1",
        "zh:67e31a71a5ecbbc96a1a6708c9cc300bbfe921c322320cdbb95b9002026387e1",
```

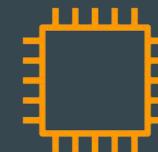
# Terraform Refresh

# Understanding the Challenge

Terraform can create an infrastructure based on configuration you specified.

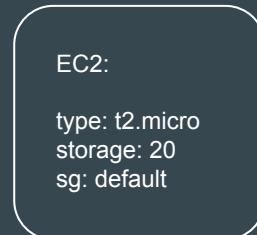
It can happen that the infrastructure gets modified manually.

```
resource "aws_instance" "web" {  
  ami           = ami-123  
  instance_type = "t2.micro"  
}
```



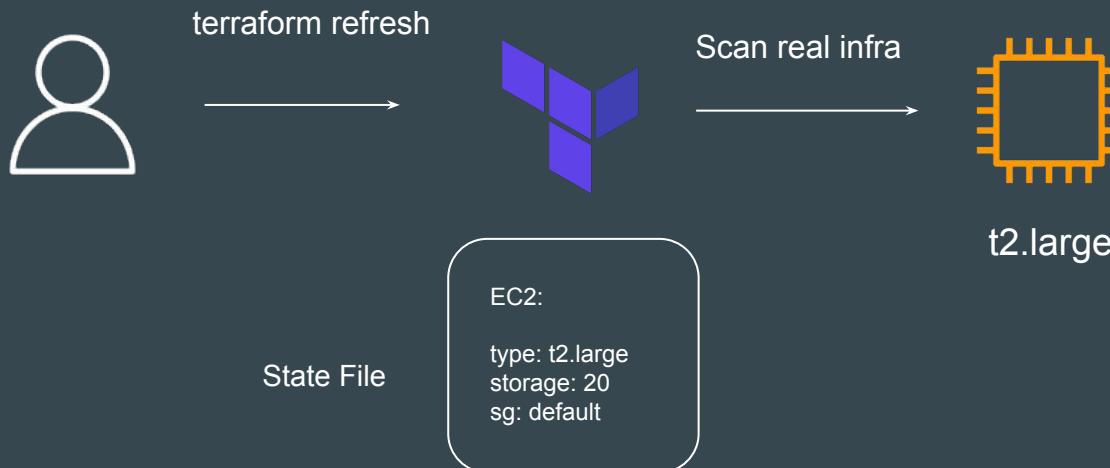
t2.micro

State File



# Understanding the Challenge

The **terraform refresh** command will check the latest state of your infrastructure and update the state file accordingly.



## Points to Note

You shouldn't typically need to use this command, because Terraform automatically performs the same refreshing actions as a part of creating a plan in both the `terraform plan` and `terraform apply` commands.

# Understanding the Usage

The `terraform refresh` command is deprecated in newer version of `terraform`.

The `-refresh-only` option for `terraform plan` and `terraform apply` was introduced in Terraform v0.15.4.

# **AWS Provider - Authentication Configuration**

# Understanding the Basics

At this stage, we have been manually hardcoding the access / secret keys within the provider block.

Although a working solution, but it is **not optimal from security point of view**.

```
VSCode Terminal: aws-provider-config.tf > ...
provider "aws" {
    region      = "us-east-1"
    access_key  = "AKIAQTS...5QJI"
    secret_key  = "8aEdYqLULVnIK1S...WmfqOP"
}

resource "aws_eip" "lb" {
    domain    = "vpc"
}
```

# Better Way

We want our code to run successfully without hardcoding the secrets in the provider block.

```
VSCode Terminal: aws-provider-config.tf > ...
provider "aws" {
    region      = "us-east-1"
}

resource "aws_eip" "lb" {
    domain      = "vpc"
}
```

# Better Approach

The AWS Provider can source credentials and other settings from the shared configuration and credentials files.

```
vim aws-provider-config.tf > ...
provider "aws" {
    shared_config_files      = [/Users/tf_user/.aws/conf"]
    shared_credentials_files = [/Users/tf_user/.aws/creds"]
    profile                  = "customprofile"
}

resource "aws_eip" "lb" {
    domain    = "vpc"
}
```

# Default Configurations

If shared files lines are not added to provider block, by default, Terraform will locate these files at \$HOME/.aws/config and \$HOME/.aws/credentials on Linux and macOS.

"%USERPROFILE%\aws\config" and "%USERPROFILE%\aws\credentials" on Windows.

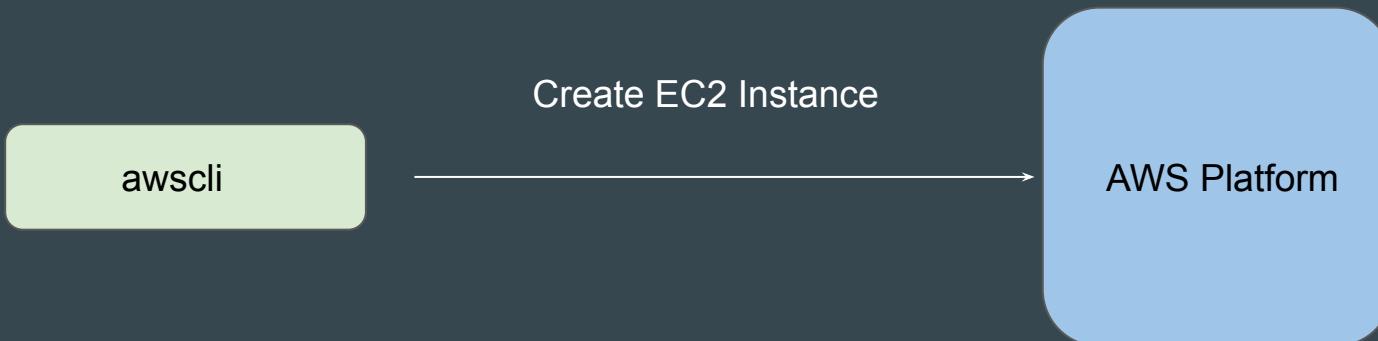
```
VS Code aws-provider-config.tf > ...
provider "aws" {
    region      = "us-east-1"
}

resource "aws_eip" "lb" {
    domain     = "vpc"
}
```

# AWS CLI

AWS CLI allows customers to manage AWS resources directly from CLI.

When you configure Access/Secret keys in AWS CLI, the location in which these credentials are stored is the same default location that Terraform searches the credentials from.



---

# Lecture Format - Terraform Course

Terraform in detail

---

# Overview of the Format

We tend to use a different folder for each practical that we do in the course.

This allows us to be more systematic and allows easier revisit in-case required.

Lecture Name	Folder Names
Create First EC2 Instance	folder1
Tainting resource	folder2
Conditional Expression	folder3

# Find the appropriate code from GitHub

Code in GitHub is arranged according to sections that are matched to the domains in the course.

Every section in GitHub has easy Readme file for quick navigation.

## Video-Document Mapper

Sr No	Document Link
1	<a href="#">Understanding Attributes and Output Values in Terraform</a>
2	<a href="#">Referencing Cross-Account Resource Attributes</a>
3	<a href="#">Terraform Variables</a>
4	<a href="#">Approaches for Variable Assignment</a>
5	<a href="#">Data Types for Variables</a>

# Destroy Resource After Practical

We know how to destroy resources by now

`terraform destroy`

After you have completed your practical, make sure you destroy the resource before moving to the next practical.

This is easier if you are maintaining separate folder for each practical.

# Relax and Have a Meme Before Proceeding



**alcohol**  
@Mandac5

What is an extreme sport?



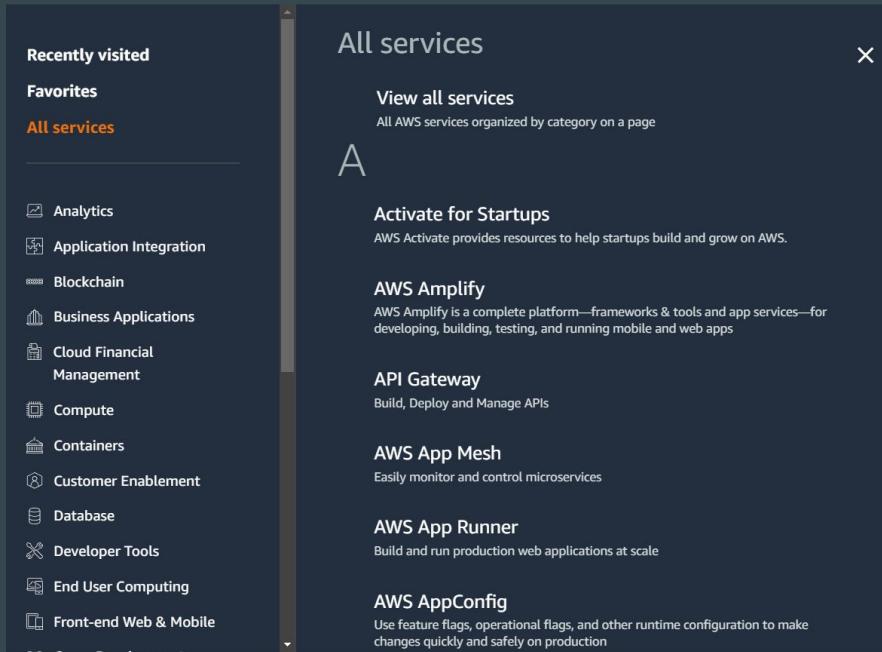
**allison**  
@amazaleax

Doing your homework while the  
teacher is collecting it

# **Learning Scope - AWS Services for Terraform Course**

# Understanding the Basics

AWS has more than 200 services available.



# Aim of the Course

Primary aim of this course is to master the core concepts of Terraform.

Terraform = Infrastructure as Code Tool.

To learn Terraform, we need to create infrastructure somewhere.



# Services that we Choose

Throughout the course, we use very basic AWS services to demonstrate Terraform concepts.

- Virtual Machine (EC2)
- Firewall (Security Groups)
- AWS Users (IAM Users)
- IP Address (Elastic IP)

# Basics of These Services are Covered

We have 100,000+ students from different background who are learning Terraform.

Some are AWS Pros, Some are from Azure/GCP, Some are students

To align everyone on same page, we also cover basics of the AWS service that we use throughout the course.

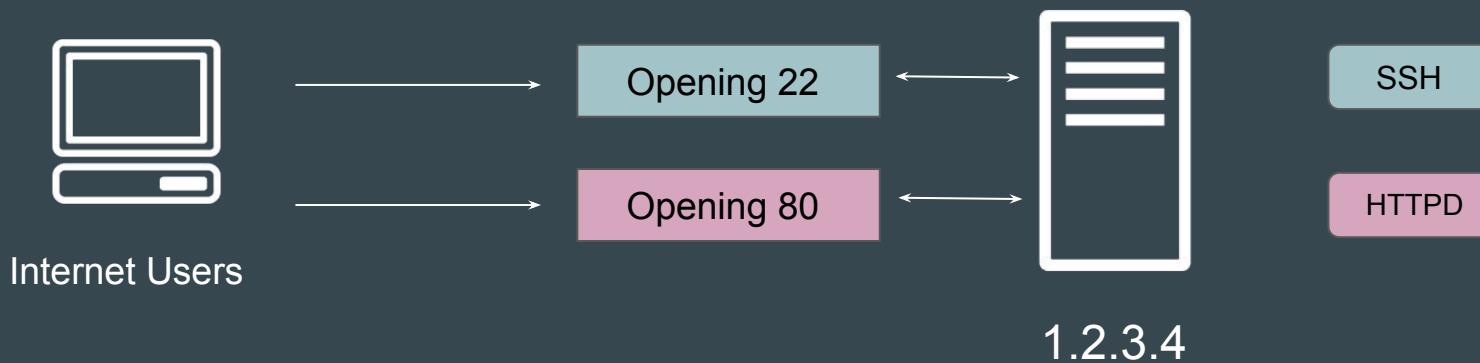
# Example - Creating Firewall Through Terraform

1. Basics of Firewalls in AWS
2. Firewall Practical in AWS (GUI Console)
3. Creating Firewall Rules Through Terraform.

# **Basics of Firewalls**

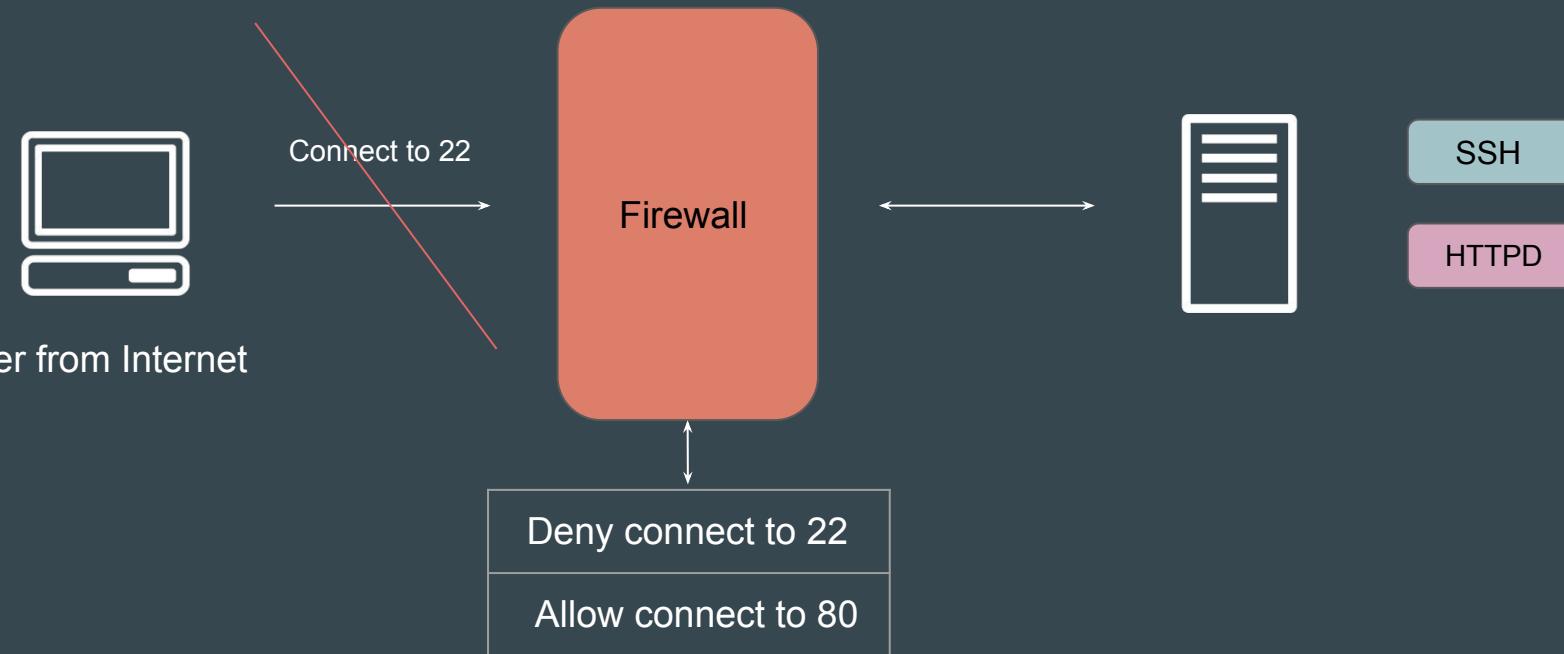
# Basics of Ports

A port acts as a **endpoint of communication** to identify a given application or process on an Linux operating system



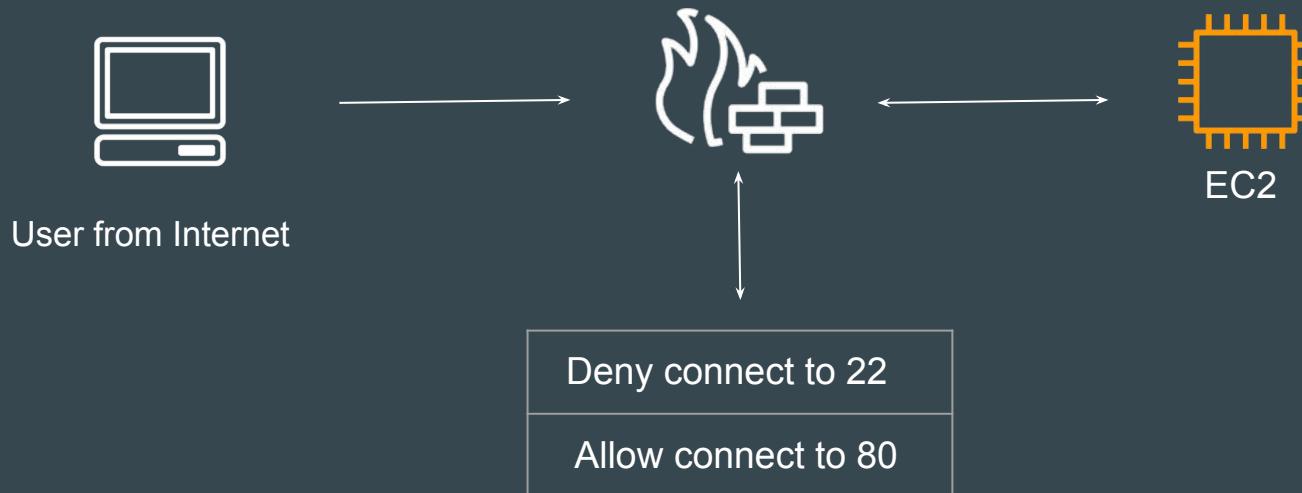
# Basics of Firewall

Firewall is a **network security system** that monitors and controls incoming and outgoing network traffic based on predetermined security rules.



# Firewall in AWS

A **security group** acts as a virtual firewall for your instance to control inbound and outbound traffic.



# Sample Security Group with Rules

### Details

Security group name <a href="#">demo-firewall</a>	Security group ID <a href="#">sg-0fcf94c6fff3977b2</a>	Description <a href="#">Demo Purpose</a>	VPC ID <a href="#">vpc-050f222846f400045</a>
Owner <a href="#">042025557788</a>	Inbound rules count 3 Permission entries	Outbound rules count 1 Permission entry	

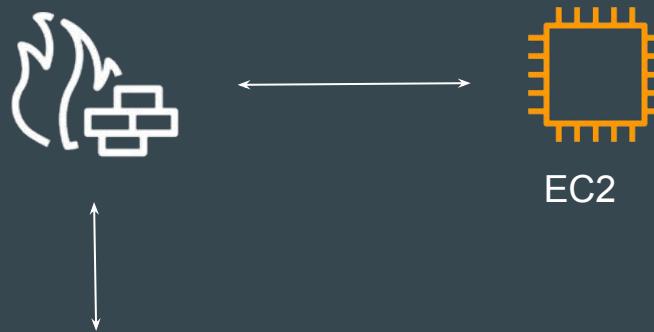
[Inbound rules](#)   [Outbound rules](#)   [Tags](#)

### Inbound rules (3)

IP version	Type	Protocol	Port range	Source
IPv4	SSH	TCP	22	172.31.0.0/16
IPv4	HTTP	TCP	80	0.0.0.0/0
IPv4	MYSQL/Aurora	TCP	3306	172.31.0.10/32

# Inbound and Outbound Rules

Firewalls control both inbound and outbound connections to and from the server.



Inbound	Outbound
Allow 80 from 0.0.0.0/0	Allow 3306 to 172.31.10.50

# **Creating Firewall Rules with Terraform**

# Architecture of Today's Video

We will create a Firewall (Security Group) in AWS with following configuration



terraform-firewall



Inbound	Outbound
Allow 80 from 0.0.0.0/0	Allow ALL

# Reference - Final Code in Video

```
firewall.tf  X
firewall.tf > resource "aws_vpc_security_group_ingress_rule" "allow_tls_ipv4"

resource "aws_security_group" "allow_tls" {
    name          = "terraform-firewall"
    description   = "Managed from Terraform"
}

resource "aws_vpc_security_group_ingress_rule" "allow_tls_ipv4" {
    security_group_id = aws_security_group.allow_tls.id
    cidr_ipv4        = "0.0.0.0/0"
    from_port         = 80
    ip_protocol      = "tcp"
    to_port           = 80
}

resource "aws_vpc_security_group_egress_rule" "allow_all_traffic_ipv4" {
    security_group_id = aws_security_group.allow_tls.id
    cidr_ipv4        = "0.0.0.0/0"
    ip_protocol      = "-1" # semantically equivalent to all ports
}
```

# **Dealing with Documentation Code Updates - Terraform**

# Understanding the Challenge

Occasionally in the newer version of Providers, you will see some changes in the way you create a resource.

```
resource "aws_security_group" "allow_tls" {
  name      = "terraform-firewall"
  description = "Managed from Terraform"
}

resource "aws_vpc_security_group_ingress_rule" "allow_tls_ipv4" {
  security_group_id = aws_security_group.allow_tls.id
  cidr_ipv4        = "0.0.0.0/0"
  from_port         = 80
  ip_protocol       = "tcp"
  to_port           = 80
}
```

New Approach

```
resource "aws_security_group" "old_approach" {
  name      = "allow_tls"
  description = "Allow TLS inbound traffic"

  ingress {
    description      = "TLS from VPC"
    from_port        = 443
    to_port          = 443
    protocol         = "tcp"
    cidr_blocks     = ["10.77.32.50/32"]
  }
}
```

Old Approach

## Points to Note

Just because a better approach is recommended, does NOT always mean that the older approach will stop working.

Organizations can continue to use the approach that suits best in it's environment.

# Switching to Older Provider Doc

You can always switch to the older version of provider documentation page to understand the changes.

The screenshot shows the HashiCorp Terraform provider documentation for AWS. The URL is `Providers / hashicorp / aws / Version 5.31.0`. The main content is titled "Resource: `aws_security_group`". It provides a brief description: "Provides a security group resource." Below this, there is a note about security group rules:

**⚠ NOTE on Security Groups and Security Group Rules:**

Terraform currently provides a Security Group resource with `ingress` and `egress` rules defined in-line and a `Security Group Rule` resource which manages one or more `ingress` or `egress` rules. Both of these resources were added before AWS assigned a `security group rule unique ID`, and they do not work well in all scenarios using the `description` and `tags` attributes, which rely on the unique ID. The `aws_vpc_security_group_egress_rule` and `aws_vpc_security_group_ingress_rule` resources have been added to address these limitations and should be used for all new security group rules. You should not use the `aws_vpc_security_group_egress_rule` and `aws_vpc_security_group_ingress_rule` resources in conjunction with an `aws_security_group` resource with in-line rules or with `aws_security_group_rule` resources defined for the same Security Group, as rule conflicts may

# Closing Pointers

For larger enterprises, it becomes difficult to upgrade their code base to the newer approach that provider recommends.

In such case, they stick with the appropriate provider version that supports the older approach of creating the resource.

# Create Elastic IP with Terraform

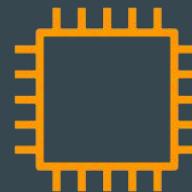
# Basics of Elastic IP in AWS

An Elastic IP address is a static IPv4 address in AWS.

You can create it and associate it with EC2 instance.



52.30.40.50



52.30.40.50

# Aim of Today's Video

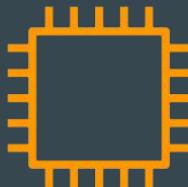
We are going to use Terraform to generate Elastic IP resource in AWS.

# **Attributes**

# Basics of Attributes

Each resource has its associated set of attributes.

Attributes are the fields in a resource that hold the values that end up in state.



Attributes	Values
ID	i-abcd
public_ip	52.74.32.50
private_ip	172.31.10.50
private_dns	ip-172-31-10-50-.ec2.internal

# Points to Note

Each resource type has a predefined set of attributes determined by the provider.

 [Attribute Reference](#)

---

This resource exports the following attributes in addition to the arguments above:

- `arn` - ARN of the instance.
- `capacity_reservation_specification` - Capacity reservation specification of the instance.
- `id` - ID of the instance.
- `instance_state` - State of the instance. One of: `pending` , `running` , `shutting-down` , `terminated` , `stopping` , `stopped` . See [Instance Lifecycle](#) for more information.
- `outpost_arn` - ARN of the Outpost the instance is assigned to.
- `password_data` - Base-64 encoded encrypted password data for the instance. Useful for getting the administrator password for instances running Microsoft Windows. This attribute is only exported if `get_password_data` is true. Note that this encrypted value will be stored in the state file, as with all exported attributes. See [GetPasswordData](#) for more information.
- `primary_network_interface_id` - ID of the instance's primary network interface.

# **Cross-Resource Attribute References**

# Typical Challenge

It can happen that in a single terraform file, you are defining two different resources.

However Resource 2 might be dependent on some value of Resource 1.



Elastic IP Address

Security group

Allow 443 from Elastic IP

# Understanding The Workflow

```
VSCode eip.tf > ...
resource "aws_eip" "lb" {
  domain    = "vpc"
}
```

```
resource "aws_vpc_security_group_ingress_rule" "allow_tls_ipv4" {
  security_group_id = aws_security_group.allow_tls.id
  cidr_ipv4        = "HOW-TO-ADD-ELASTIC-IP-ADDRESS-HERE"
  from_port         = 80
  ip_protocol       = "tcp"
  to_port           = 80
}
```

Elastic IP



52.72.30.50



Security group

Allow 443 from 52.72.30.50

# Analyzing the Attributes of EIP

We have to find which attribute stores the Public IP associated with EIP Resource.

**Attribute Reference**

---

This resource exports the following attributes in addition to the arguments above:

- `allocation_id` - ID that AWS assigns to represent the allocation of the Elastic IP address for use with instances in a VPC.
- `association_id` - ID representing the association of the address with an instance in a VPC.
- `carrier_ip` - Carrier IP address.
- `customer_owned_ip` - Customer owned IP.
- `id` - Contains the EIP allocation ID.
- `private_dns` - The Private DNS associated with the Elastic IP address (if in VPC).
- `private_ip` - Contains the private IP address (if in VPC).
- `public_dns` - Public DNS associated with the Elastic IP address.
- `public_ip` - Contains the public IP address.

# Referencing Attribute in Other Resource

We have to find a way in which attribute value of “public\_ip” is referenced to the cidr\_ipv4 block of security group rule resource.



Elastic IP

Attribute	Value
public_ip	52.72.52.72

```
resource "aws_vpc_security_group_ingress_rule" "allow_tls_ipv4" {
  security_group_id = aws_security_group.allow_tls.id
  cidr_ipv4         = "REFERENCE-PUBLIC-IP-ATTRIBUTE-HERE"
  from_port          = 80
  ip_protocol        = "tcp"
  to_port            = 80
}
```

# Cross Referencing Resource Attribute

Terraform allows us to reference the attribute of one resource to be used in a different resource.

Overall syntax:

<RESOURCE TYPE>. <NAME>. <ATTRIBUTE>

# Cross Referencing Resource Attribute

We can specify the resource address with attribute for cross-referencing.



Elastic IP

Attribute	Value
public_ip	52.72.52.72

```
resource "aws_vpc_security_group_ingress_rule" "allow_tls_ipv4" {
    security_group_id = aws_security_group.allow_tls.id
    cidr_ipv4        = "aws_eip.lb.public_ip"
    from_port         = 80
    ip_protocol       = "tcp"
    to_port           = 80
}
```

# String Interpolation in Terraform

`${...})`: This syntax indicates that Terraform will replace the expression inside the curly braces with its calculated value.

```
resource "aws_vpc_security_group_ingress_rule" "allow_tls_ipv4" {
    security_group_id = aws_security_group.allow_tls.id
    cidr_ipv4        = "${aws_eip.lb.public_ip}/32"
    from_port         = 80
    ip_protocol       = "tcp"
    to_port           = 80
}
```

# Joke Time

Why did the Terraform attribute take a break?

...It was feeling over-referenced.

---

How did the Terraform attribute become a detective?

...It followed the resource trail.

# **Output Values**

# Understanding the Basics

**Output values** make information about your infrastructure available on the command line, and can expose information for other Terraform configurations to use.



# Sample Example

## Use-Case:

Create a Elastic IP (Public IP) resource in AWS and output the value of the EIP.

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

Changes to Outputs:
+ demo = (known after apply)
aws_eip.lb: Creating...
aws_eip.lb: Creation complete after 3s [id=eipalloc-0680508decfe8c252]

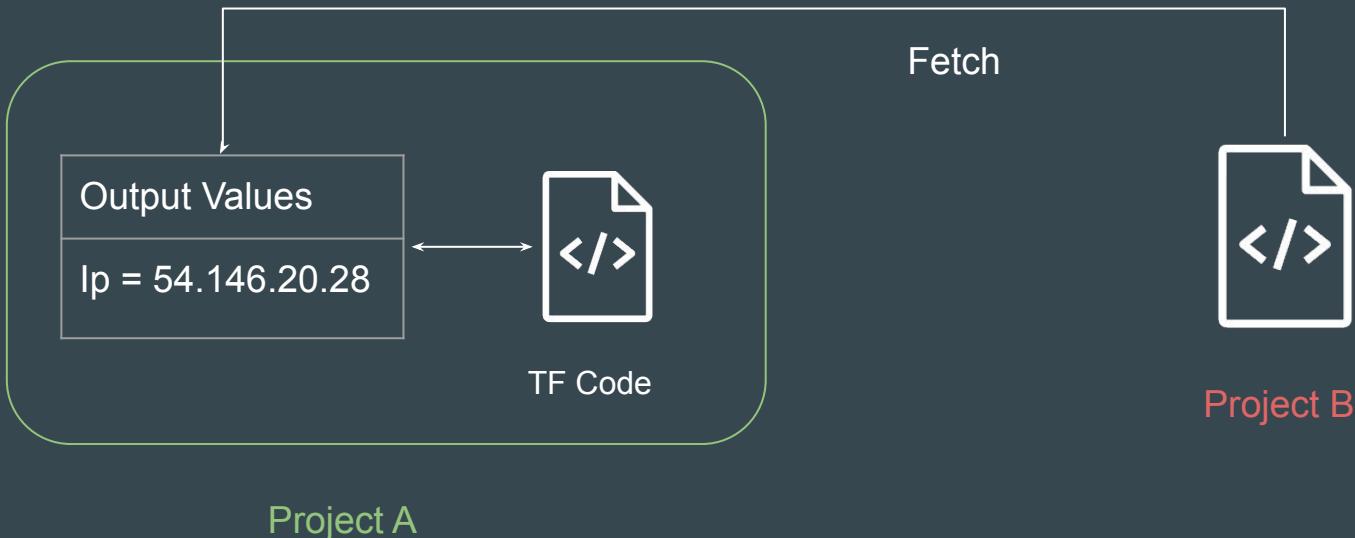
Apply complete! Resources: 1 added, 0 changed, 0 destroyed.

Outputs:

demo = "54.146.20.18"
```

# Point to Note

Output values defined in Project A can be referenced from code in Project B as well.



# Terraform Variables

# Understanding the Challenge

Repeated static values in the code can create more work in the future.

Example: VPN IP needs to be whitelisted for 5 ports through Firewall Rules.

Port Number	CIDR Block	Description
80	101.0.62.210/32	VPN IP Whitelist
443	101.0.62.210/32	VPN IP Whitelist
22	101.0.62.210/32	VPN IP Whitelist
21	101.0.62.210/32	VPN IP Whitelist
8080	101.0.62.210/32	VPN IP Whitelist

# Reference Screenshot

```
resource "aws_vpc_security_group_ingress_rule" "allow_tls_ipv4" {
    security_group_id = aws_security_group.allow_tls.id
    cidr_ipv4        = "101.0.62.210/32"
    from_port         = 80
    ip_protocol      = "tcp"
    to_port           = 80
}
```

Firewall Rule 1

```
resource "aws_vpc_security_group_ingress_rule" "allow_tls_ipv4" {
    security_group_id = aws_security_group.allow_tls.id
    cidr_ipv4        = "101.0.62.210/32"
    from_port         = 443
    ip_protocol      = "tcp"
    to_port           = 443
}
```

Firewall Rule 2

# Better Approach

A better solution would be to define repeated static value in one central place.

Key	Value
vpn_ip	101.0.62.210/32

Central Location

```
resource "aws_vpc_security_group_ingress_rule" "allow_tls_ipv4" {
  security_group_id = aws_security_group.allow_tls.id
  cidr_ipv4        = "fetch-from-central-location"
  from_port         = 443
  ip_protocol       = "tcp"
  to_port           = 443
}
```

```
resource "aws_vpc_security_group_ingress_rule" "allow_tls_ipv4" {
  security_group_id = aws_security_group.allow_tls.id
  cidr_ipv4        = "fetch-from-central-location"
  from_port         = 8080
  ip_protocol       = "tcp"
  to_port           = 8080
}
```

# Basics of Variables

Terraform input variables are used to pass certain values from outside of the configuration

Name	Value
vpn_ip	101.0.62.210/32
app_port	8080

Variable File

```
resource "aws_vpc_security_group_ingress_rule" "allow_tls_ipv4" {  
    security_group_id = aws_security_group.allow_tls.id  
    cidr_ipv4        = var.vpn_ip  
    from_port         = var.app_port  
    ip_protocol       = "tcp"  
    to_port           = var.app_port  
}
```

# Benefits of Variables

1. Update important values in one central place instead of searching and replacing them throughout your code, saving time and potential mistakes.
2. No need to touch the core Terraform configuration file. This can avoid human mistakes while editing.



# **Variable Definitions File (TFVars)**

# Understanding the Base

Managing variables in production environment is one of the very important aspect to keep code clean and reusable.

HashiCorp recommends creating a separate file with name of `*.tfvars` to define all variable value in a project.

# How Recommended Folder Structure Looks Like

1. Main Terraform Configuration File.
2. **variables.tf** file that defines all the variables.
3. **terraform.tfvars** file that defines value to all the variables.

```
resource "aws_vpc_security_group_ingress_rule" "allow_tls_ipv4" {  
    security_group_id = aws_security_group.allow_tls.id  
    cidr_ipv4        = var.vpn_ip  
    from_port         = var.app_port  
    ip_protocol      = "tcp"  
    to_port          = var.app_port  
}
```

Main Configuration File

```
variables.tf X  
└─ variable "vpn_ip" {}  
└─ variable "app_port" {}
```

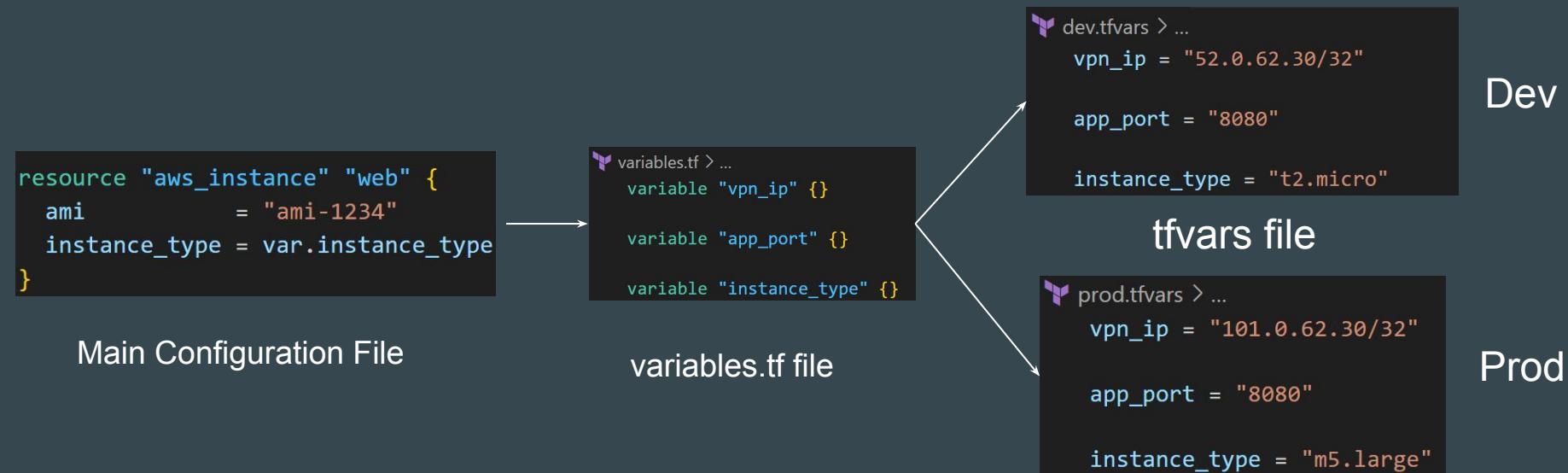
variables.tf File

```
terraform.tfvars ●  
└─ vpn_ip = "101.0.62.210/32"  
    app_port = "8080"
```

terraform.tfvars file

# Configuration for Different Environments

Organizations can have wide set of environments: Dev, Stage, Prod



# Selecting tfvars File

If you have multiple variable definitions file (\*.tfvars) file, you can manually define the file to use during command line.

```
C:\Users\zealv\kplabs-terraform>terraform plan -var-file="prod.tfvars"

Terraform used the selected providers to generate the following execution plan.
following symbols:
+ create

Terraform will perform the following actions:

# aws_instance.web will be created
+ resource "aws_instance" "web" {
    + ami                                = "ami-1234"
    + arn                                = (known after apply)
    + associate_public_ip_address        = (known after apply)
    + availability_zone                  = (known after apply)
    + cpu_core_count                     = (known after apply)
    + cpu_threads_per_core              = (known after apply)
    + disable_api_stop                  = (known after apply)
    + disable_api_termination           = (known after apply)
    + ebs_optimized                     = (known after apply)
```

# Point to Note

If file name is `terraform.tfvars` → Terraform will automatically load values from it.

If file name is different like `prod.tfvars` → You have to explicitly define the file during plan / apply operation.

```
C:\Users\zealv\kplabs-terraform>terraform plan -var-file="prod.tfvars"

Terraform used the selected providers to generate the following execution plan.
following symbols:
+ create

Terraform will perform the following actions:

# aws_instance.web will be created
+ resource "aws_instance" "web" {
    + ami                                = "ami-1234"
    + arn                                = (known after apply)
    + associate_public_ip_address        = (known after apply)
    + availability_zone                  = (known after apply)
    + cpu_core_count                     = (known after apply)
    + cpu_threads_per_core              = (known after apply)
    + disable_api_stop                  = (known after apply)
    + disable_api_termination           = (known after apply)
    + ebs_optimized                      = (known after apply)
```

# **Approach to Variable Assignment**

# Understanding the Base

By default, whenever you define a variable, you must also set a value associated with it.

```
resource "aws_instance" "web" {  
    ami           = "ami-1234"  
    instance_type = var.instance_type  
}
```

Main Configuration File

```
variables.tf > ...  
  
variable "instance_type" {}
```

variables.tf

**VARIABLE IS DEFINED**



**BUT WHERE IS THE VALUE**

# Add a Value in CLI

If you have not defined a value for a variable, Terraform will ask you to input the value in CLI Prompt when you run `terraform plan` / `apply` operation.

```
C:\Users\zealv\kplabs-terraform>terraform plan  
var.instance_type  
Enter a value:
```

# Declaring Variable Values

When variables are declared in your configuration, they can be set in a number of ways:

1. Variable Defaults.
2. Variable Definition File (\*.tfvars)
3. Environment Variables
4. Setting Variables in the Command Line.

# Variable Defaults

You can set a default value for a variable.

If there is no value supplied, the default value will be taken.

```
variables.tf > ...
variable "app_port" {
    default = "8080"
}
```

# Variable Definition File (\*.tfvars)

Variable Values can be defined in \*.tfvars file.

```
prod.tfvars > ...
vpn_ip = "101.0.62.30/32"

app_port = "8080"

instance_type = "m5.large"
```

# Setting Variable in Command Line

To specify individual variables on the command line, use the `-var` option when running the `terraform plan` and `terraform apply` commands:

```
C:\Users\zealv\kplabs-terraform>terraform plan -var="instance_type=m5.large"

Terraform used the selected providers to generate the following execution plan. Resource
following symbols:
+ create

Terraform will perform the following actions:

# aws_instance.web will be created
+ resource "aws_instance" "web" {
    + ami                                = "ami-1234"
    + arn                                = (known after apply)
    + associate_public_ip_address        = (known after apply)
    + availability_zone                  = (known after apply)
    + cpu_core_count                     = (known after apply)
    + cpu_threads_per_core              = (known after apply)
    + disable_api_stop                  = (known after apply)
    + disable_api_termination           = (known after apply)
    + ebs_optimized                     = (known after apply)
    + get_password_data                = false
    + host_id                            = (known after apply)
    + host_resource_group_arn           = (known after apply)
    + iam_instance_profile              = (known after apply)
    + id                                 = (known after apply)
    + instance_initiated_shutdown_behavior = (known after apply)
    + instance.lifecycle               = (known after apply)
    + instance.state                   = (known after apply)
    + instance_type                    = "m5.large"
```

# Setting Variable through Environment Variables

Terraform searches the environment of its own process for environment variables named `TF_VAR_` followed by the name of a declared variable.

```
C:\Users\zealv\kplabs-terraform>echo %TF_VAR_instance_type%
t2.large

C:\Users\zealv\kplabs-terraform>terraform plan

Terraform used the selected providers to generate the following execution plan
following symbols:
+ create

Terraform will perform the following actions:

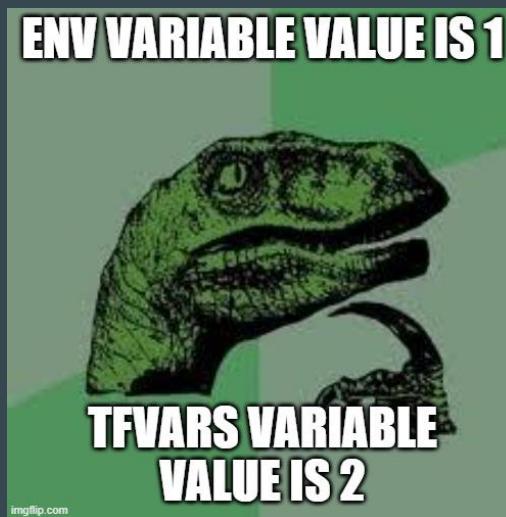
# aws_instance.web will be created
+ resource "aws_instance" "web" {
    + ami                                = "ami-1234"
    + arn                                = (known after apply)
    + associate_public_ip_address        = (known after apply)
    + availability_zone                  = (known after apply)
```

# **Variable Definition Precedence**

# Understanding the Base

Values for a variable can be defined at multiple different places.

What if values for a variable are different?



# Simple Example

```
variable "instance_type" {}
```

1. Default Value is t2.micro
2. Terraform.tfvars value is "t2.small"
3. Environment Variable TF\_VAR\_instance\_type = "t2.large"

Which value will Terraform take?

# Variable Definition Precedence

Terraform loads variables in the following order, with later sources taking precedence over earlier ones:

1. Environment variables
2. The `terraform.tfvars` file, if present.
3. The `terraform.tfvars.json` file, if present.
4. Any `*.auto.tfvars` or `*.auto.tfvars.json` files, processed in lexical order of their filenames.
5. Any `-var` and `-var-file` options on the command line

# Example 1

ENV Variable of TF\_VAR\_instance\_type = “t2.micro”

Value in terraform.tfvars = “t2.large”

Final Result = “t2.large”

## Example 2

1. ENV Variable of TF\_VAR\_instance\_type = "t2.micro"
2. Value in terraform.tfvars = "t2.large"
3. terraform plan -var="instance\_type=m5.large"

Final Result = "m5.large"

# **Data Types**

# Setting the Base

Data type refers to the **type of value**.

Depending on the requirement, you can use wide variety of values in Terraform configuration.

Example Data Type	Data Type
“Hello World”	String
7575	Number

# Restricting Variable Value to Data Type

We can restrict the value of a variable to a data type.

Example:

Only numbers should be allowed in AWS Usernames.

```
variable "username" {  
    type = number  
}
```

# Data Types in Terraform

Data Types	Description
string	a sequence of Unicode characters representing some text, like "hello".
number	A Numeric value
bool	a boolean value, either true or false
list	a sequence of values, like ["us-west-1a", "us-west-1c"]
set	a collection of unique values that do not have any secondary identifiers or ordering.
map	a group of values identified by named labels, like {name = "Mabel", age = 52}.
null	a value that represents absence or omission.

# **Data Type - List**

# List Data Type

Allows us to store **collection of values** for a single variable / argument.

Represented by a pair of square brackets containing a comma-separated sequence of values, like ["a", 15, true].

Useful when multiple values needs to be added for a specific argument

```
variable "my-list" {  
  type = list  
  default = ["mumbai","bangalore","delhi"]  
}
```

# Data Type and Documentation

Arguments for a resource requires specific data types.

Some argument requires list, some requires map and so on.

The details of data type expected for an argument is mentioned in documentation.

- `volume_tags` - (Optional) Map of tags to assign, at instance-creation time, to root and EBS volumes.

**⚠ NOTE:**

Do not use `volume_tags` if you plan to manage block device tags outside the `aws_instance` configuration, such as using `tags` in an `aws_ebs_volume` resource attached via `aws_volume_attachment`. Doing so will result in resource cycling and inconsistent behavior.

- `vpc_security_group_ids` - (Optional, VPC only) List of security group IDs to associate with.

# Use-Case 1: List Data Type

EC2 instance can have one or more security groups.

**Requirement:**

Create EC2 instance with 2 security groups attached.

# Specify the Type of Values in List

We can also specify the type of values expected in a list.

```
variable "my-list" {  
    type = list(number)  
    default  = ["1","2","3"]  
}
```

# **Map - Data Type**

# Map Data Type

A map data type represents a **collection of key-value pair elements**

```
variable "instance_tags" {  
  type = map  
  default = {  
    Name = "app-server"  
    Environment = "development"  
    Team = "payments"  
  }  
}
```

# Use-Case of Map

We can add multiple tags to AWS resources.

These tags are key-value pairs.

The screenshot shows the AWS EC2 Instances page with one instance listed:

- Name:** kplabs-ec2
- Instance ID:** i-0b8abce20ade4fe35
- Instance state:** Running
- Instance type:** t2.micro
- Status check:** Initializing

The instance details are shown in the main pane:

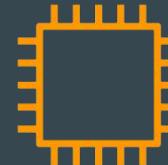
- Tags:** Environment: Production, Team: Security, Name: kplabs-ec2

# **The COUNT Meta-Argument**

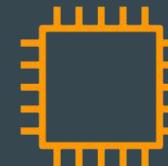
# Understanding the Challenge

By default, a resource block configures one real infrastructure object.

```
resource "aws_instance" "first_ec2" {  
    ami = "ami-00c39f71452c08778"  
    instance_type = "t2.micro"  
}
```



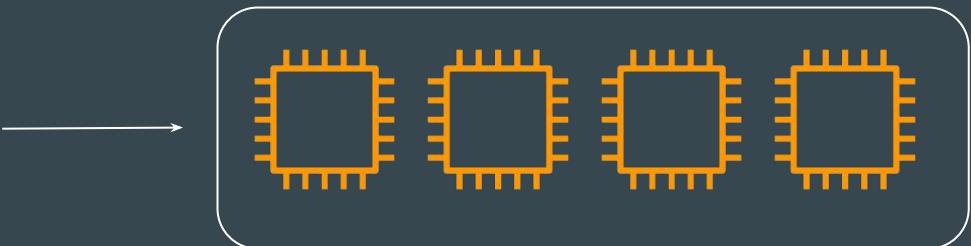
```
resource "aws_instance" "second_ec2" {  
    ami = "ami-00c39f71452c08778"  
    instance_type = "t2.micro"  
}
```



# Understanding the Use-Case

Sometimes you want to manage several similar objects (like a fixed pool of compute instances) without writing a separate block for each one.

```
resource "aws_instance" "second_ec2" {  
    ami = "ami-00c39f71452c08778"  
    instance_type = "t2.micro"  
    <something-logic-here>  
}
```

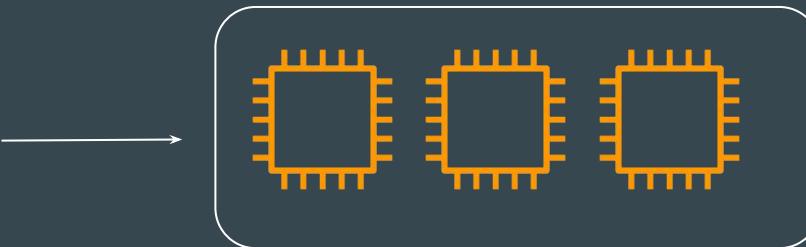


Pool of Servers

# Introducing Count Argument

The count argument accepts a whole number, and creates that many instances of the resource.

```
resource "aws_instance" "second_ec2" {  
    ami = "ami-00c39f71452c08778"  
    instance_type = "t2.micro"  
    count = 3  
}
```



Pool of Servers

# Challenges with Count

The instances created through count and identical copies, but you might want to customize certain properties for each one.

```
resource "aws_instance" "first_ec2" {  
    ami = "ami-00c39f71452c08778"  
    instance_type = "t2.micro"  
    count = 3  
}
```



Instances (3) <a href="#">Info</a>				
	Name ↴	Instance ID	Instance state	Instance type
<input type="checkbox"/>		i-0ff464aa6552b8b71	<span>Running</span>  	t2.micro
<input type="checkbox"/>		i-0cb8f1ede6e0bf880	<span>Running</span>  	t2.micro
<input type="checkbox"/>		i-09b74e79c59f8fc17	<span>Running</span>  	t2.micro

# Example - IAM User

For many resources, exact identical copies are not required and will not work.

Example: You cannot have multiple AWS Users with exact same name.

```
resource "aws_iam_user" "lb" {
    name = "developer-user"
    count = 3
}
```



```
Error: creating IAM User (developer-user): operation error IAM: CreateUser, https response error Status
: 44c3ff43-0bd4-430e-a838-ba5e43aa569a, EntityAlreadyExists: User with name developer-user already exists
with aws_iam_user.lb[0],
on iam.tf line 2, in resource "aws_iam_user" "lb":
2: resource "aws_iam_user" "lb" {
```

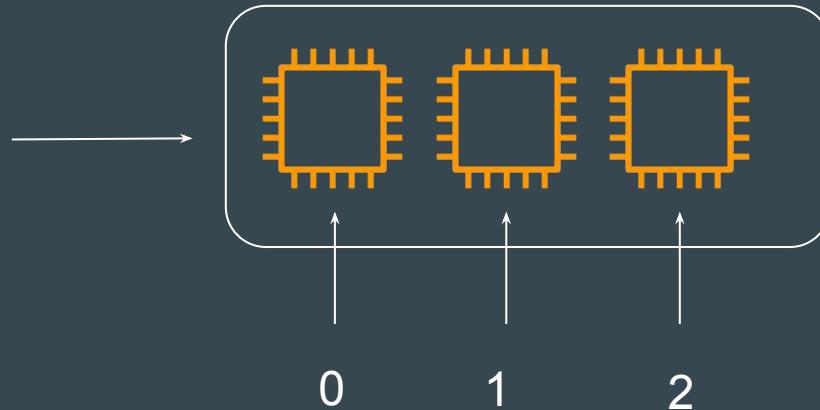
**COUNT.INDEX**

# Introducing Count Index

When using count, you can also make use of `count.index` which allows better flexibility.

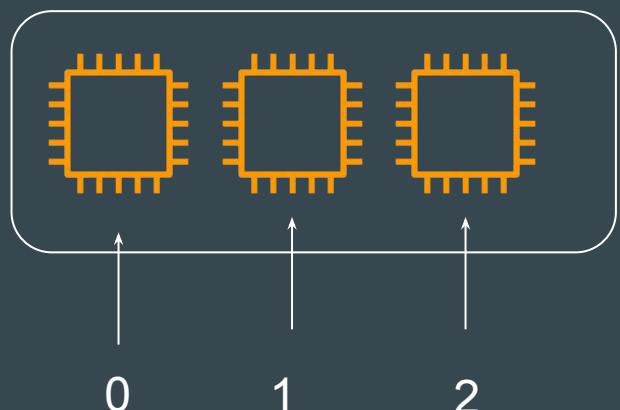
This attribute holds a distinct index number, starting from 0, that uniquely identifies each instance created by the count meta-argument.

```
resource "aws_instance" "myec2" {  
    ami = "ami-00c39f71452c08778"  
    instance_type = "t2.micro"  
    count = 3  
}
```



# Tabular Representation

Following representation shows each EC2 instance's resource address that contains the index.



Resource Address	Description
aws_instance.myec2[0]	First EC2 Instance
aws_instance.myec2[1]	Second EC2 Instance
aws_instance.myec2[2]	Third EC2 Instance

# CLI Output

Within CLI output, you will be able to see the index value of resource.

```
# aws_instance.first_ec2[0] will be created
+ resource "aws_instance" "first_ec2" {
    + ami                                = "ami-00c39f71452c08778"
    + arn                                = (known after apply)
    + associate_public_ip_address        = (known after apply)
    + availability_zone                  = (known after apply)
    + cpu_core_count                     = (known after apply)
    + cpu_threads_per_core              = (known after apply)
    + disable_api_stop                  = (known after apply)
    + disable_api_termination           = (known after apply)
    + ebs_optimized                      = (known after apply)
    + get_password_data                 = false
    + host_id                            = (known after apply)
    + host_resource_group_arn           = (known after apply)
    + iam_instance_profile              = (known after apply)
    + id                                 = (known after apply)
```

First EC2

```
# aws_instance.first_ec2[1] will be created
+ resource "aws_instance" "first_ec2" {
    + ami                                = "ami-00c39f71452c08778"
    + arn                                = (known after apply)
    + associate_public_ip_address        = (known after apply)
    + availability_zone                  = (known after apply)
    + cpu_core_count                     = (known after apply)
    + cpu_threads_per_core              = (known after apply)
    + disable_api_stop                  = (known after apply)
    + disable_api_termination           = (known after apply)
    + ebs_optimized                      = (known after apply)
    + get_password_data                 = false
    + host_id                            = (known after apply)
    + host_resource_group_arn           = (known after apply)
    + iam_instance_profile              = (known after apply)
    + id                                 = (known after apply)
```

Second EC2

# Example - IAM User Use-Case

The \${count.index} is dynamic expression that utilizes the count.index attribute so that each username will be unique.

```
resource "aws_iam_user" "lb" {
  name = "developer-user.${count.index}"
  count = 3
}
```



Users (7) <a href="#">Info</a>						
	User name	Path	Groups	Last activity		
<input type="checkbox"/>	<a href="#">developer-user.0</a>	/	0	-		
<input type="checkbox"/>	<a href="#">developer-user.1</a>	/	0	-		
<input type="checkbox"/>	<a href="#">developer-user.2</a>	/	0	-		

# Enhancing with Count Index

You can use count.index to iterate through the list to have more customization.

```
variable "dev_names" {  
  type = list  
  default = ["alice", "bob", "johncorner"]  
}  
  
resource "aws_iam_user" "lb" {  
  name = var.dev_names[count.index]  
  count = 3  
}
```

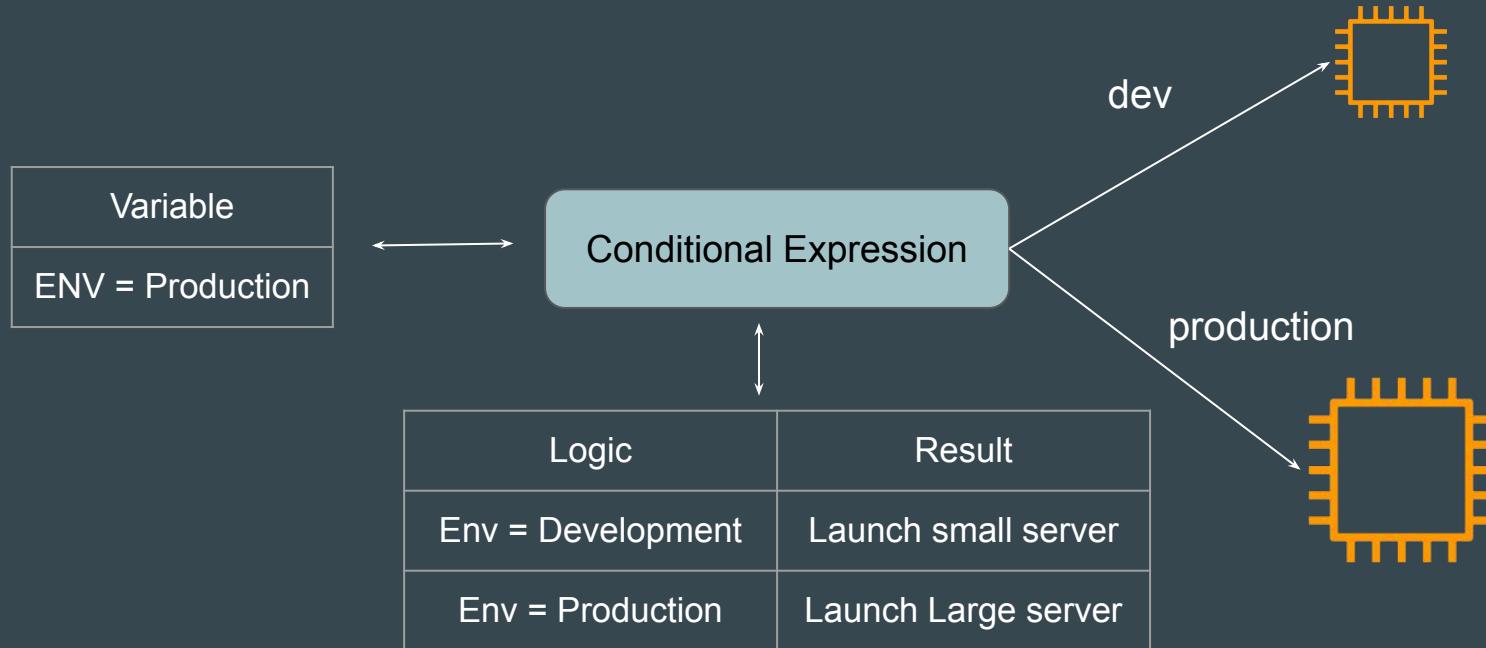


Users (7) <small>Info</small>						
	User name	Path	Groups	Last activity	Actions	
<input type="checkbox"/>	alice	/	0	-	<a href="#">Edit</a>	<a href="#">Delete</a>
<input type="checkbox"/>	bob	/	0	-	<a href="#">Edit</a>	<a href="#">Delete</a>
<input type="checkbox"/>	johncorner	/	0	-	<a href="#">Edit</a>	<a href="#">Delete</a>

# **Conditional Expressions**

# Setting the Base

Conditional expressions in Terraform allow you to choose between two values based on a condition



# Syntax of Conditional Expression

The syntax of a conditional expression is as follows:

```
condition ? true_val : false_val
```

If condition is true then the result is true\_val. If condition is false then the result is false\_val.

# Conditional Expression Based on Use-Case

If Environment is Development, t2.micro instance type should be used.

If Environment is NOT development, m5.large instance type should be used.

```
variable "environment" {
  default = "development"
}

resource "aws_instance" "example" {
  instance_type = var.environment == "development" ? "t2.micro" : "m5.large"
  ami           = "ami-12345678"
}
```

# Conditional Expression with Multiple Variables

In the following example, **only if** env=production and region=us-east-1, the larger instance type of m5.large can be used.

```
variable "environment" {
    default = "production"
}

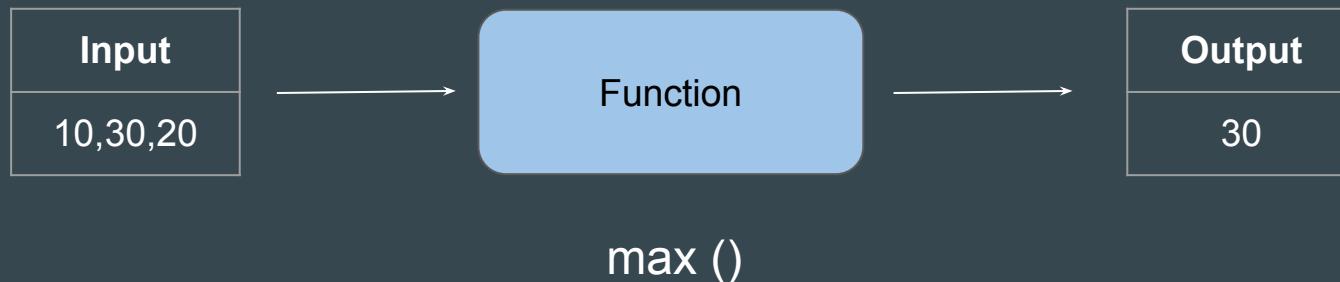
variable "region" {
    default = "ap-south-1"
}

resource "aws_instance" "example" {
    instance_type = var.environment == "production" && var.region == "us-east-1" ? "m5.large" : "t2.micro"
    ami           = "ami-12345678"
}
```

# Terraform Functions

# Basics of Function

A function is a block of code that performs a specific task.



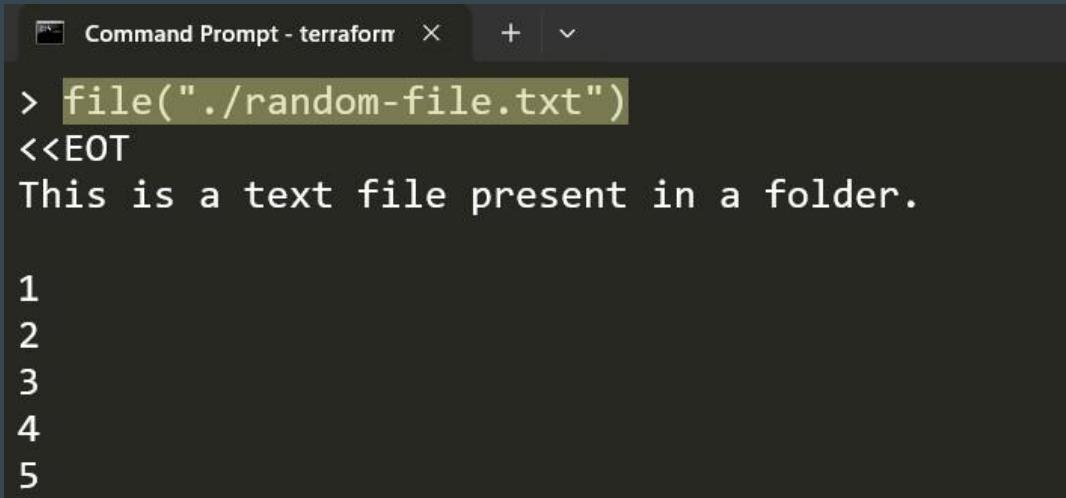
# Function 1 - MAX

max () takes one or more numbers and returns the greatest number.

```
C:\Users\zealv\kplabs-terraform>terraform console  
> max(10,20,30)  
30
```

## Function 2 - FILE

file () reads the contents of a file at the given path and returns them as a string.



```
Command Prompt - terraform > file("./random-file.txt")
<<EOT
This is a text file present in a folder.

1
2
3
4
5
```

# Introducing Terraform Console

Terraform Console provides an interactive environment specifically **designed to test functions** and experiment with expressions before integrating them into your main code.

```
C:\Users\zealv\kplabs-terraform>terraform console  
> max(10,20,30)  
30
```

# Importance of File Function

file reads the contents of a file at the given path and returns them as a string.

```
resource "aws_iam_user_policy" "lb_ro" {
  name = "demo-user-policy"
  user = aws_iam_user.this.name

  policy = jsonencode({
    "Version": "2012-10-17",
    "Statement": [
      {
        "Action": "ec2:*",
        "Effect": "Allow",
        "Resource": "*"
      },
      {
        "Effect": "Allow",
        "Action": "elasticloadbalancing:*",
        "Resource": "*"
      },
    ]
  })
}
```

Before



```
resource "aws_iam_user_policy" "lb_ro" {
  name = "demo-user-policy"
  user = aws_iam_user.this.name

  policy = file("./ec2-policy.json")
}
```

After

# Functions in Terraform

Terraform has wide variety of functions available to achieve different set of use-cases.

Functions are grouped into categories. Some of these include:

Function Categories	Functions Available
Numeric Functions	abs, ceil, floor, max, min
String Functions	concat, replace, split, tolower,toupper
Collection Functions	element, keys, length, merge, sort
Filesystem Functions:	file, filebase64, dirname

# Important Point to Note

The Terraform language **does not support user-defined functions**, and so only the functions built in to the language are available for use

The documentation includes a page for all of the available built-in functions.

# **Challenge - Analyzing Code Containing Functions**

# Setting the Base

As part of this challenge, you will be given a code that contains multiple sets of Terraform Functions.

You have to analyze what this code does without running the “apply” operation.

```
variable "ami" {
  type = map
  default = {
    "us-east-1" = "ami-08a0d1e16fc3f61ea"
    "us-west-2" = "ami-0d6621c01e8c2de2c"
    "ap-south-1" = "ami-0470e33cd681b2476"
  }
}

resource "aws_instance" "app-dev" {
  ami = lookup(var.ami,var.region)
  instance_type = "t2.micro"
  count = length(var.tags)

  tags = {
    Name = element(var.tags,count.index)
    CreationDate = formatdate("DD MMM YYYY hh:mm ZZZ",timestamp())
  }
}
```

# Overall Workflow

1. Analyze what exactly the given code in GitHub will do without running the “apply operation”.
2. Analyze the outcome by applying function using Terraform Console and reading the documentation.
3. Make a note of it.
4. Run the “terraform apply” operation to verify if it matches your findings.

# **Solution - Analyzing Code Containing Functions**

# 1- Analyzing Lookup Function

lookup retrieves the value of a single element from a map, given its key.

Format: lookup(map, key, default)

```
> lookup({a="ay", b="bee"}, "a", "what?")
ay
> lookup({a="ay", b="bee"}, "c", "what?")
what?
```

# Testing Lookup Function

To test lookup function, add the details that are part of the map associated with variable of ami and the default value of variable of region.

```
variable "ami" {  
  type = map  
  default = {  
    "us-east-1" = "ami-08a0d1e16fc3f61ea"  
    "us-west-2" = "ami-0d6621c01e8c2de2c"  
    "ap-south-1" = "ami-0470e33cd681b2476"  
  }  
}
```

```
variable "region" {  
  default = "us-east-1"  
}
```

terraform console

```
> lookup({"us-east-1" = "ami-08a0d1e16fc3f61ea", "us-west-2" = "ami-0d6621c01e8c2de2c", "ap-south-1" = "ami-0470e33cd681b2476"}  
, "us-east-1")  
"ami-08a0d1e16fc3f61ea"
```

## 2 - Analyzing Length Function

**length** determines the length of a given list, map, or string.

```
> length([])  
0  
> length(["a", "b"])  
2  
> length({"a" = "b"})  
1  
> length("hello")  
5
```

# Testing Length Function

Code: count = length(var.tags)

```
variable "tags" {  
    type = list  
    default = ["firstec2", "secondec2"]  
}
```



```
> length(["firstec2", "secondec2"])  
2
```

## 3 - Analyzing Element Function

element retrieves a single element from a list.

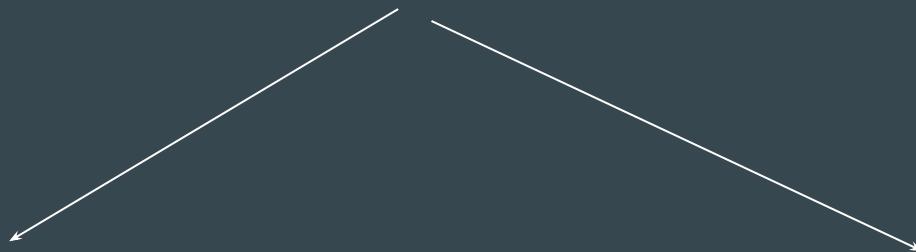
Format: element(list, index)

```
> element(["a", "b", "c"], 1)
b
```

# Testing Element Function

Code: Name = element(var.tags,count.index)

```
variable "tags" {  
    type = list  
    default = ["firstec2","secondec2"]  
}
```



```
> element(["firstec2","secondec2"],0)  
"firstec2"
```

```
> element(["firstec2","secondec2"],1)  
"secondec2"
```

## 4 - Analyzing TimeStamp Function

timestamp returns a UTC timestamp string in RFC 3339 format.

```
> formatdate("DD MMM YYYY hh:mm ZZZ", "2018-01-02T23:12:01Z")
02 Jan 2018 23:12 UTC
> formatdate("EEEE, DD-MMM-YY hh:mm:ss ZZZ", "2018-01-02T23:12:01Z")
Tuesday, 02-Jan-18 23:12:01 UTC
> formatdate("EEE, DD MMM YYYY hh:mm:ss ZZZ", "2018-01-02T23:12:01-08:00")
Tue, 02 Jan 2018 23:12:01 -0800
> formatdate("MMM DD, YYYY", "2018-01-02T23:12:01Z")
Jan 02, 2018
> formatdate("HH:mm:ss", "2018-01-02T23:12:01Z")
11:12pm
```

# Testing TimeDate Function

A simple call to the timestamp () returns the timestamp value

```
> timestamp()  
"2024-06-16T13:43:13Z"
```

## 5 - Analyzing Formatdate Function

formatdate converts a timestamp into a different time format.

```
> formatdate("DD MMM YYYY hh:mm ZZZ", "2018-01-02T23:12:01Z")
02 Jan 2018 23:12 UTC
> formatdate("EEEE, DD-MMM-YY hh:mm:ss ZZZ", "2018-01-02T23:12:01Z")
Tuesday, 02-Jan-18 23:12:01 UTC
> formatdate("EEE, DD MMM YYYY hh:mm:ss ZZZ", "2018-01-02T23:12:01-08:00")
Tue, 02 Jan 2018 23:12:01 -0800
> formatdate("MMM DD, YYYY", "2018-01-02T23:12:01Z")
Jan 02, 2018
> formatdate("HH:mm:ss", "2018-01-02T23:12:01Z")
11:12pm
```

## 5 - Testing Formatdate Function

Code Block:

```
CreationDate = formatdate("DD MMM YYYY hh:mm ZZZ",timestamp())
```

```
> formatdate("DD MMM YYYY hh:mm ZZZ",timestamp())
"16 Jun 2024 13:46 UTC"
```

# Final Result

1. Two set of EC2 instances will be created.
2. Name of EC2 will be “firstec2”, and “secondec2”
3. EC2 will have a tag of creation date with the timestamp value

# You are Awesome

Learning “Terraform Function” is a longer learning journey compared to other topics.

In today’s video, we learnt the practical aspect of Function in Terraform Code.



# **Local Values**

# Understanding the Challenge

Various resources in your project can have common values like tags.

Repeating these values across multiple resource blocks increases the code length and makes it difficult to manage in larger projects.

```
resource "aws_instance" "myec2" {
    ami = "ami-00c39f71452c08778"
    instance_type = "t2.micro"
    tags = {
        Team = "payments-team"
    }
}
```

```
resource "aws_security_group" "allow_tls" {
    name          = "firewall_sg"
    tags = {
        Team = "payments-system"
    }
}
```

# Solution using Variables

One solution is to centralize these common values using Variables

```
variable "payment_tag" {  
    type = map  
    default = {  
        Team = "payments-team"  
    }  
}
```

Variable

```
resource "aws_instance" "myec2" {  
    ami = "ami-00c39f71452c08778"  
    instance_type = "t2.micro"  
    tags = var.payment_tag  
}
```

```
resource "aws_security_group" "allow_tls" {  
    name = "firewall_sg"  
    tags = var.payment_tag  
}
```

# Introducing Local Values

Local Values are similar to Variables in a sense that it allows you to store data centrally and that can be referenced in multiple parts of configuration.

```
locals {  
    common_tags = {  
        Team = "payments-team"  
    }  
}
```

Locals

```
resource "aws_instance" "myec2" {  
    ami = "ami-00c39f71452c08778"  
    instance_type = "t2.micro"  
    tags = local.common_tags  
}
```

```
resource "aws_security_group" "allow_tls" {  
    name = "firewall_sg"  
    tags = local.common_tags  
}
```

# Additional Benefit of Locals

You can add expressions to locals, which allows you to compute values dynamically

```
locals {
    # IDs for multiple sets of EC2 instances, merged together
    instance_ids = concat(aws_instance.blue.*.id, aws_instance.green.*.id)
}

locals {
    # Common tags to be assigned to all resources
    common_tags = {
        Service = local.service_name
        Owner   = local.owner
    }
}
```

# Locals vs Variables

Variable value can be defined in wide variety of places like `terraform.tfvars`, ENV Variables, CLI and so on.

Locals are more of a private resource. You have to directly modify the code.

Locals are used when you want to avoid repeating the same expression multiple times.

# Important Points to Note

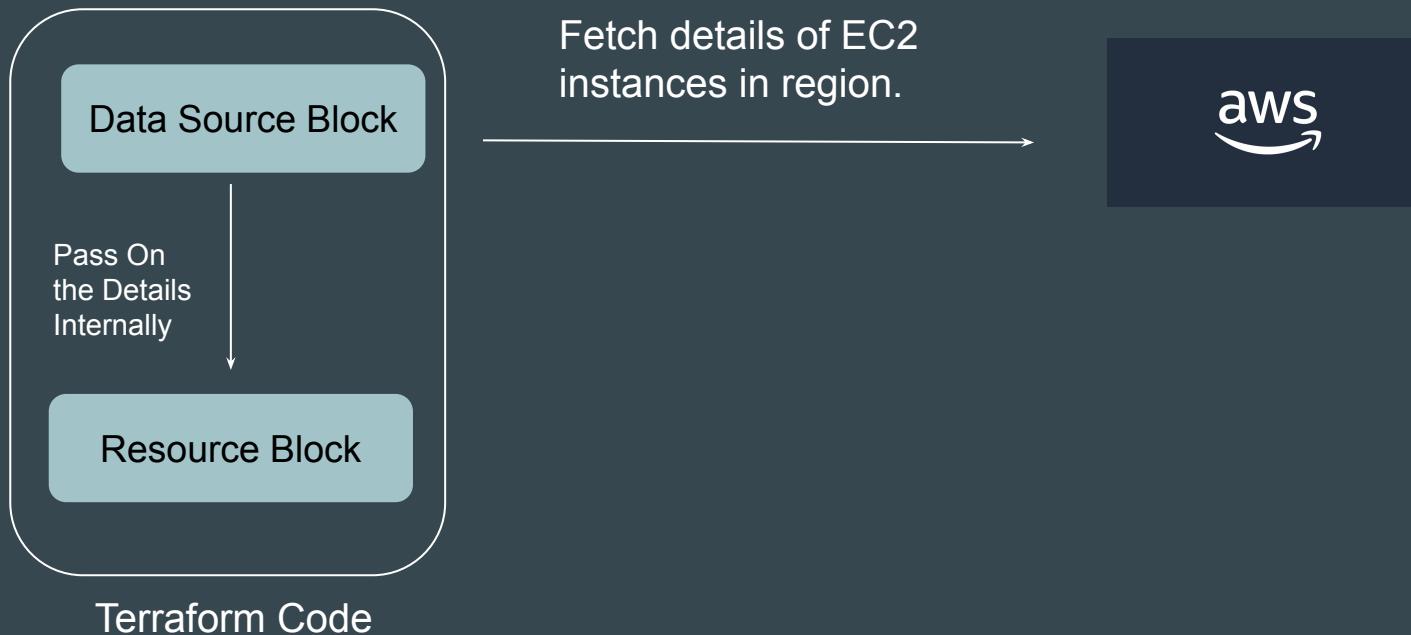
Local values are often referred to as just "locals"

Local values are created by a `locals` block (plural), but you reference them as attributes on an object named `local` (singular)

# **Data Sources**

# Introducing Data Sources

Data sources allow Terraform to **use / fetch** information defined outside of Terraform



## Example 1 - Reading Info of DO Account

Following data source code is used to get information on your DigitalOcean account.

```
data "digitalocean_account" "example" {}
```

## Example 2 - Reading a File

Following data source allows you to read contents of a file in your local filesystem.

```
data "local_file" "foo" {
    filename = "${path.module}/demo.txt"
}
```

# Clarity regarding path.module

`${path.module}` returns the current file system path where your code is located.

```
data "local_file" "foo" {
    filename = "${path.module}/demo.txt"
}
```

## Example 3 - Fetch EC2 Instance Details

Following data source code is used to fetch details about the EC2 instance in your AWS region.

```
data "aws_instances" "example" {}
```

# **Data Sources Documentation Reference**

# Finding Available Data Sources

List of available data source are associated with each resource of a provider.

The screenshot shows a documentation page for the DigitalOcean Provider. The left sidebar has a 'DIGITALOCEAN DOCUMENTATION' header and a 'Filter' search bar. Below the filter is a list of resources under 'digitalocean provider': 'Resources' (indicated by a right-pointing arrow) and 'Data Sources' (indicated by a downward-pointing arrow). Under 'Data Sources', there is a list of provider names: 'digitalocean\_account', 'digitalocean\_app', 'digitalocean\_certificate', 'digitalocean\_container\_registry', 'digitalocean\_database\_ca', 'digitalocean\_database\_cluster', 'digitalocean\_database\_connection\_pool', and 'digitalocean\_database\_replica'. The main content area is titled 'DigitalOcean Provider' and contains text explaining that the provider interacts with DigitalOcean resources and needs configuration. It also includes a 'Example Usage' section with a code snippet:

```
terraform {  
    required_providers {  
        digitalocean = {  
            source  = "digitalocean/digitalocean"  
            version = "~> 2.0"  
        }  
    }  
}
```

A 'Copy' button is located next to the code snippet.

# **Data Sources Format**

# Understanding the Basic Structure

A data source is accessed via a special kind of resource known as a **data resource**, declared using a **data** block:

Following data block requests that Terraform read from a given data source ("aws\_instance") and export the result under the given local name ("foo").

```
data "aws_instance" "foo" {}
```

# Filter Structure

Within the block body (between { and }) are query constraints defined by the data source.

```
data "aws_instance" "foo" {
  filter {
    name    = "tag:Team"
    values  = ["Production"]
  }
}
```

# **Fetching Latest OS Image Using Data Sources**

# Understanding the Requirement

You have been given a requirement to write a Terraform code that creates EC2 instance using latest OS Image of Amazon Linux.

# Approach that New User will Take

We want to use the latest OS image for creating server in AWS.

Steps that we typically follow:

1. Go to EC2 Console.
2. Fetch the latest AMI ID
3. Add that AMI ID in Terraform code.



# Sample Reference Code

```
resource "aws_instance" "web" {  
    ami              = "ami-0440d3b780d96b29d" ← Hard Coded static value  
    instance_type   = "t2.micro"  
}
```

# Static Information is Boring

Hardcoding static details in your Terraform code will lead you to repeatedly modify your code to meet changing requirements.



# Another Challenge with Static Values

In many of the cases, the static value changes depending on the region.

Example: AMI IDs are specific to region.

Hardcoded AMI in code will only work for single region.

Mumbai Region



ami-1234

Singapore Region



ami-5678

Tokyo Region

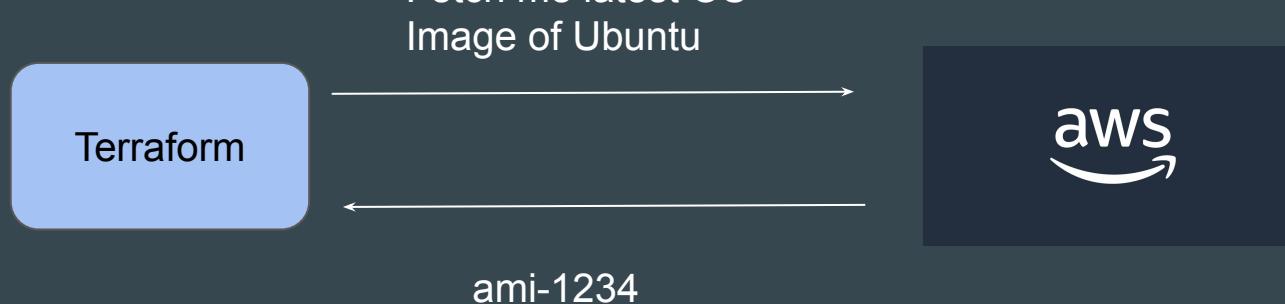


ami-9012

# Time to be Pros - Dynamic Configuration

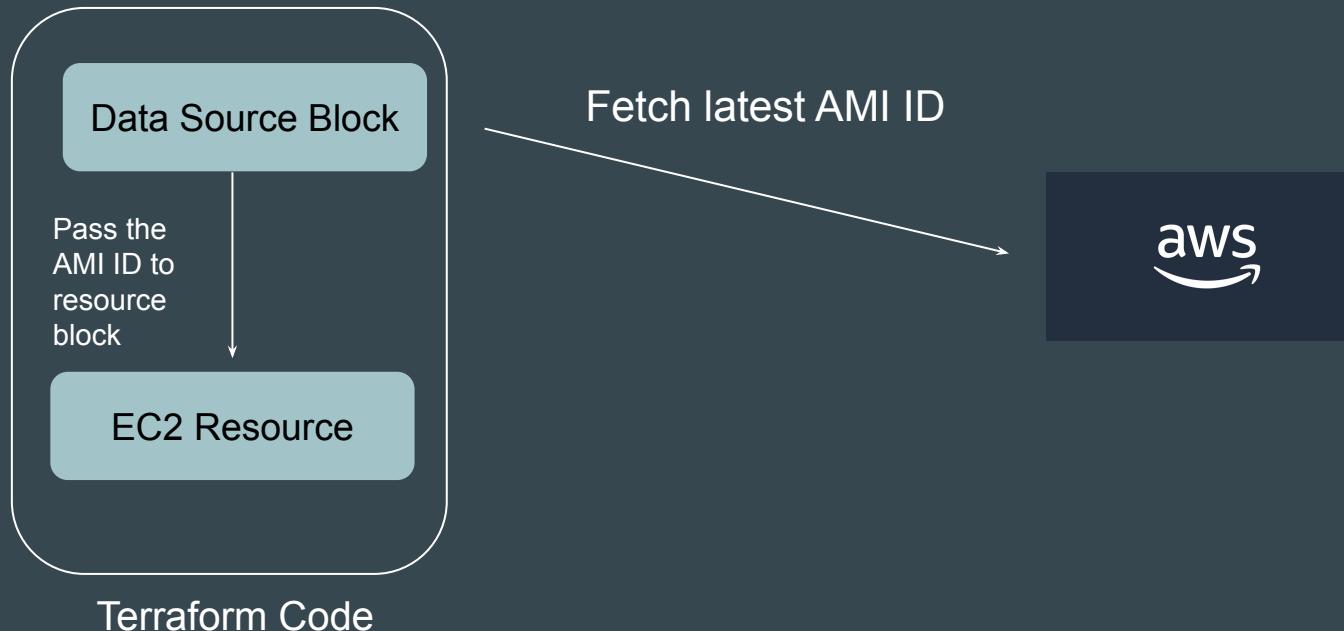
We want Terraform to automatically query the latest OS image in AWS or any other provider and use that for creating server.

We need code which works for all region without modification.



# Introducing Data Sources

Data sources allow Terraform to **use information defined outside of Terraform** and we can use that information to provision resources.



# Debugging Terraform

# Basics of Debugging

Debugging is the **process of finding the root cause** of a specific issue.

30-40% of the time of a System Administrator goes into Debugging.



# Example - SSH Verbosity

One of the important requirement in Debugging is getting detailed Log

Depending on the application, the approach to get detailed logs will differ.

```
C:\Users\zealv\OneDrive\Desktop>ssh -v -i dp_rsa root@64.227.154.149
OpenSSH_for_Windows_8.6p1, LibreSSL 3.4.3
debug1: Authenticator provider $SSH_SK_PROVIDER did not resolve; disabling
debug1: Connecting to 64.227.154.149 [64.227.154.149] port 22.
debug1: Connection established.
debug1: identity file dp_rsa type -1
debug1: identity file dp_rsa-cert type -1
debug1: Local version string SSH-2.0-OpenSSH_for_Windows_8.6
debug1: Remote protocol version 2.0, remote software version OpenSSH_9.6p1 Ubuntu-3ubuntu13.4
debug1: compat_banner: match: OpenSSH_9.6p1 Ubuntu-3ubuntu13.4 pat OpenSSH* compat 0x04000000
debug1: Authenticating to 64.227.154.149:22 as 'root'
debug1: load_hostkeys: fopen C:\\\\Users\\\\zealv/.ssh/known_hosts2: No such file or directory
debug1: load_hostkeys: fopen __PROGRAMDATA__\\\\ssh\\\\ssh_known_hosts: No such file or directory
debug1: load_hostkeys: fopen __PROGRAMDATA__\\\\ssh\\\\ssh_known_hosts2: No such file or directory
debug1: SSH2_MSG_KEXINIT sent
debug1: SSH2_MSG_KEXINIT received
debug1: kex: algorithm: curve25519-sha256
debug1: kex: host key algorithm: ssh-ed25519
debug1: kex: server->client cipher: chacha20-poly1305@openssh.com MAC: <implicit> compression: none
debug1: kex: client->server cipher: chacha20-poly1305@openssh.com MAC: <implicit> compression: none
debug1: expecting SSH2_MSG_KEX_ECDH_REPLY
```

# Debugging in Terraform

Similar to SSH Verbosity, even Terraform allows us to set wide variety of log levels for getting detailed logs for debugging purpose.

```
root@test-kplabs:~# terraform plan
2024-08-24T05:01:48.844Z [INFO]  Terraform version: 1.9.5
2024-08-24T05:01:48.845Z [DEBUG] using github.com/hashicorp/go-tfe v1.58.0
2024-08-24T05:01:48.845Z [DEBUG] using github.com/hashicorp/hcl/v2 v2.20.0
2024-08-24T05:01:48.845Z [DEBUG] using github.com/hashicorp/terraform-svchost v0.1.1
2024-08-24T05:01:48.845Z [DEBUG] using github.com/zclconf/go-cty v1.14.4
2024-08-24T05:01:48.845Z [INFO] Go runtime version: go1.22.5
2024-08-24T05:01:48.845Z [INFO] CLI args: []string{"terraform", "plan"}
2024-08-24T05:01:48.845Z [TRACE] Stdout is a terminal of width 125
2024-08-24T05:01:48.845Z [TRACE] Stderr is a terminal of width 125
2024-08-24T05:01:48.845Z [TRACE] Stdin is a terminal
2024-08-24T05:01:48.845Z [DEBUG] Attempting to open CLI config file: /root/.terraformrc
2024-08-24T05:01:48.845Z [DEBUG] File doesn't exist, but doesn't need to. Ignoring.
2024-08-24T05:01:48.845Z [DEBUG] ignoring non-existing provider search directory terraform.d/plugins
2024-08-24T05:01:48.846Z [DEBUG] ignoring non-existing provider search directory /root/.terraform.d/plugins
2024-08-24T05:01:48.846Z [DEBUG] ignoring non-existing provider search directory /root/.local/share/terraform/plugins
2024-08-24T05:01:48.846Z [DEBUG] ignoring non-existing provider search directory /usr/local/share/terraform/plugins
2024-08-24T05:01:48.846Z [DEBUG] ignoring non-existing provider search directory /usr/share/terraform/plugins
2024-08-24T05:01:48.846Z [DEBUG] ignoring non-existing provider search directory /var/lib/snapd/desktop/terraform/plugins
2024-08-24T05:01:48.848Z [INFO] CLI command args: []string{"plan"}
```

# Understanding the Basics

Terraform has detailed logs that you can enable by setting the `TF_LOG` environment variable to any value.

You can set `TF_LOG` to one of the log levels (in order of decreasing verbosity)

Log Level
TRACE
DEBUG
INFO
WARN
ERROR

# Storing the Logs to File

To persist logged output you can set `TF_LOG_PATH` in order to force the log to always be appended to a specific file when logging is enabled

```
root@test-kplabs:~# terraform plan
2024-08-24T05:01:48.844Z [INFO] Terraform version: 1.9.5
2024-08-24T05:01:48.845Z [DEBUG] using github.com/hashicorp/go-tfe v1.58.0
2024-08-24T05:01:48.845Z [DEBUG] using github.com/hashicorp/hcl/v2 2.20.0
2024-08-24T05:01:48.845Z [DEBUG] using github.com/hashicorp/terraform-svchost v0.1.1
2024-08-24T05:01:48.845Z [DEBUG] using github.com/cilicon/ci-cty v1.14.4
2024-08-24T05:01:48.845Z [INFO] Go runtime version: go1.22.5
2024-08-24T05:01:48.845Z [INFO] CLI args: []string{"terraform", "plan"}
2024-08-24T05:01:48.845Z [TRACE] Stdout is a terminal of width 125
2024-08-24T05:01:48.845Z [TRACE] Stderr is a terminal of width 125
2024-08-24T05:01:48.845Z [TRACE] Stdin is a terminal
2024-08-24T05:01:48.845Z [DEBUG] Attempting to open CLI config file: /root/.terraformrc
2024-08-24T05:01:48.845Z [DEBUG] File doesn't exist, but doesn't need to. Ignoring.
2024-08-24T05:01:48.845Z [DEBUG] ignoring non-existing provider search directory /root/.terraform.d/plugins
2024-08-24T05:01:48.846Z [DEBUG] ignoring non-existing provider search directory /root/.terraform.d/plugins
2024-08-24T05:01:48.846Z [DEBUG] ignoring non-existing provider search directory /root/.local/share/terraform/plugins
2024-08-24T05:01:48.846Z [DEBUG] ignoring non-existing provider search directory /usr/local/share/terraform/plugins
2024-08-24T05:01:48.846Z [DEBUG] ignoring non-existing provider search directory /usr/share/terraform/plugins
2024-08-24T05:01:48.846Z [DEBUG] ignoring non-existing provider search directory /var/lib/snapd/desktop/terraform/plugins
2024-08-24T05:01:48.848Z [INFO] CLI command args: []string{"plan"}
```

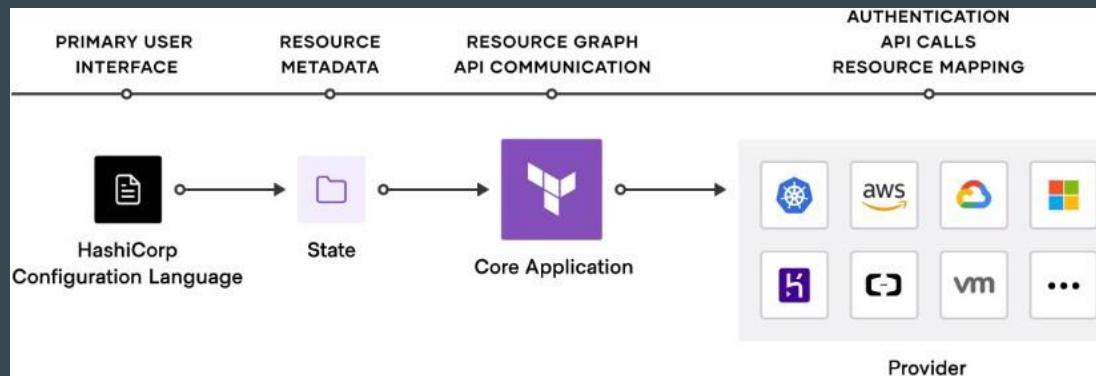


# Terraform Troubleshooting Model

# Terraform Troubleshooting Model

There are four potential types of issues that you could experience with Terraform

Language, State, Core, and Provider Errors.



# 1 - Language Errors

In most of the cases, the errors that you will face will be related to this.

When Terraform encounters a syntax error in your configuration, it prints out the line numbers and an explanation of the error.

```
C:\kplabs-terraform>terraform plan
```

```
Error: Unclosed configuration block
```

```
on demo.tf line 11, in resource "aws_iam_user" "dev":  
11: resource "aws_iam_user" "dev" {
```

```
There is no closing brace for this block before the end of the file.  
elsewhere in this file.
```

## 2 - State Errors

If state is out of sync, Terraform may destroy or change your existing resources.

If state is locked, you will also be blocked from running write operations.

```
C:\kplabs-terraform>terraform plan
```

```
Error: Error acquiring the state lock
```

```
Error message: Failed to read state file: The state file could not be read: read terraform.tfstate  
access the file because another process has locked a portion of the file.
```

```
Terraform acquires a state lock to protect the state from being written  
by multiple users at the same time. Please resolve the issue above and try  
again. For most commands, you can disable locking with the "-lock=false"  
flag, but this is not recommended.
```

# 3 - Core errors

These errors are directly related to the main Terraform application.

Errors produced at this level may be a bug.

The screenshot shows a GitHub search results page with the following filters applied:

- 311 Open
- 11,376 Closed
- Author dropdown
- Label dropdown
- Projects dropdown
- Milestones dropdown

The search results list several core errors:

- Terraform init is extremely slow** (bug, v0.13, v0.15, v1.0, v1.2, waiting for reproduction)  
#27379 opened on Dec 29, 2020 by AlmogCohen
- terraform init/apply kills Macbook Pro M1 Network connection #349** (bug, upstream, v1.1, v1.2, v1.3)  
waiting for reproduction  
#31467 opened on Jul 19, 2022 by jeff-auth0
- TrendMicro system call interception causes plugin handshake to hang for provider plugins built with Go 1.14 for Windows systems** (bug, core, explained, v0.12, windows)  
#25133 opened on Jun 4, 2020 by jf781
- configuration\_aliases in child module terraform validate fails: Provider configuration not present** (bug, config, pending project, v0.15)  
#28490 opened on Apr 23, 2021 by RobertKeyser
- Terraform does not wait for the resource to be destroyed before creating it** (bug, lifecycle, moved\_blocks)  
#24704 opened on Apr 18, 2020 by ghost
- terraform init timing out when installing AWS provider** (bug)  
#30846 opened on Apr 12, 2022 by dmandyna

## 4 - Provider errors

These set of errors are primarily related to the provider plugins.

Use the Provider GitHub page for reporting and identifying the issue.

The screenshot shows a GitHub Issues page for the 'Terraform Providers' repository. The header indicates there are 1,666 open issues and 5,180 closed issues. The page is filtered by the 'bug' label and the 'needs-triage' label. The issues listed are:

- [Bug]: Parameters or not being picked up for aws\_glue\_catalog\_table resource (#39010)
- [Bug]: aws\_lakeformation\_permissions does not save SELECT permissions in the state file (#39009)
- [Bug]: Error: failed to refresh cached credentials, no EC2 IMDS role found, operation error ec2imds: GetMetadata, exceeded maximum | number of attempts, 3, request send failed (#39003)
- [Bug]: use\_fips\_endpoint causes Terraform plan to fail with DNS resolution error in AWS provider when using a proxy (#39000)
- [Bug]: Provider bug when migrating documentdb resources from terraform 1.3 to terraform 1.8 (#38986)
- [Bug]: RDS DB upgrade from 14.9 to 16.3 and aws\_db\_parameter\_group breaks (#38984)

# **Reporting Terraform Bugs**

# Reporting Bugs

You can report bugs in the Terraform Core GitHub page or appropriate provider page.

- ⌚ **Terraform Crash** bug crash new waiting-response

#35630 opened yesterday by terrymandin
- ⌚ **503 error getting Terraform state in USA** bug cloud new waiting for reproduction waiting-response

#35613 opened 4 days ago by billnbell3
- ⌚ **Resource state not refreshed before destroy** bug new waiting for reproduction

#35568 opened last week by jooola
- ⌚ **OIDC based Azurerm backend authentication not working for Azure China Cloud** backend/azure

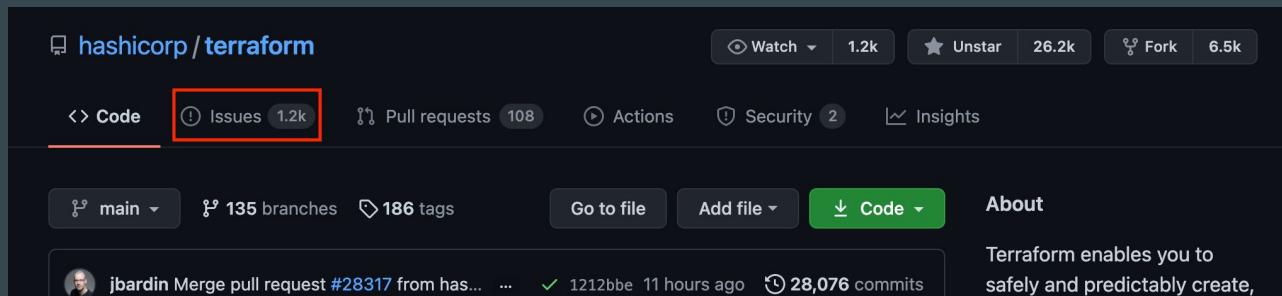
#35565 opened last week by ankitatdnav
- ⌚ **imported aws\_iam\_access\_key when using pgp\_key is destroyed** bug import new provider/aws

#35551 opened 2 weeks ago by akloss-cibo
- ⌚ **Receiving "initialising" and "initializing" in the same error message** bug new

#35536 opened 3 weeks ago by strachtenberg-hashi

# 1 - Navigate to Issues

First, navigate to the Terraform GitHub repository and choose "Issues" from the top tabs.



## 2 - Choose "New Issue".

hashicorp / **terraform**

Watch 1.2k Unstar 26.2k Fork 6.5k

Code Issues 1.2k Pull requests 108 Actions Security 2 Insights

Pinned issues

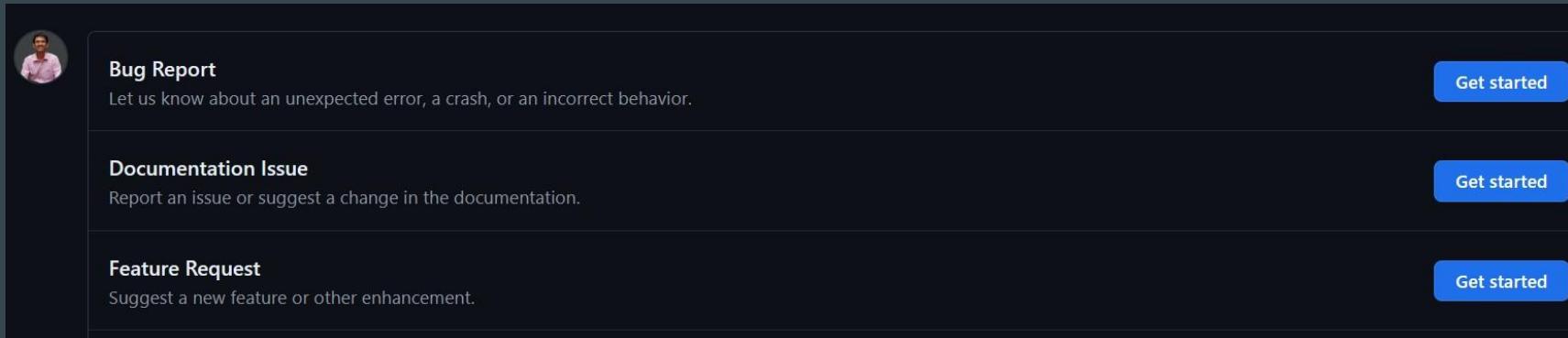
**Terraform 0.15.0-rc2 released!** #27917 opened on Feb 24 by pkolyvas Open

Filters is:issue is:open Labels 247 Milestones 4 New issue

1,243 Open 15,597 Closed Author Label Projects Milestones Assignee Sort

**Modify an RDS Aurora cluster instance size independently from the cluster instance** enhancement new

# 3 - Click “Get Started”



The image shows a dark-themed user interface with three distinct sections, each featuring a circular profile picture of a person in the top left corner. The first section is labeled "Bug Report" and contains the text "Let us know about an unexpected error, a crash, or an incorrect behavior." To its right is a blue button with the white text "Get started". The second section is labeled "Documentation Issue" and contains the text "Report an issue or suggest a change in the documentation." To its right is a blue button with the white text "Get started". The third section is labeled "Feature Request" and contains the text "Suggest a new feature or other enhancement." To its right is a blue button with the white text "Get started".

Category	Description	Action
Bug Report	Let us know about an unexpected error, a crash, or an incorrect behavior.	Get started
Documentation Issue	Report an issue or suggest a change in the documentation.	Get started
Feature Request	Suggest a new feature or other enhancement.	Get started

# 4 - Fill Core Terraform Template

## Terraform Version \*

Run `terraform version` to show the version, and paste the result below. If you are not running the latest version of Terraform, please try upgrading because your issue may have already been fixed.

```
...output of `terraform version`...
```

## Terraform Configuration Files \*

Paste the relevant parts of your Terraform configuration between the ``` marks below. For Terraform configs larger than a few resources, or that involve multiple files, please make a GitHub repository that we can clone, rather than copy-pasting multiple files in here.

```
```terraform
...terraform config...
````
```

## Debug Output \*

Full debug output can be obtained by running Terraform with the environment variable `TF_LOG=trace`. Please create a GitHub Gist containing the debug output. Please do *not* paste the debug output in the issue, since debug output is long. Debug output may contain sensitive information. Please review it before posting publicly.

```
...link to gist...
```

---

# Terraform Format

Terraform in detail

---

# Importance of Readability

Anyone who is into programming knows the importance of formatting the code for readability.

The terraform fmt command is used to rewrite Terraform configuration files to take care of the overall formatting.

```
provider "aws" {  
    region      = "us-west-2"  
    access_key  = "AKIAQIW66DN2W7WOYRGY"  
    secret_key  = "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"  
    version     = ">=2.10,<=2.30"  
}
```

**Before fmt**

```
provider "aws" {
    region      = "us-west-2"
    access_key  = "AKIAQIW66DN2W7WOYRGY"
    secret_key  = "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"
    version     = ">=2.10,<=2.30"
}
```



**After fmt**

```
provider "aws" {
    region      = "us-west-2"
    access_key  = "AKIAQIW66DN2W7WOYRGY"
    secret_key  = "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"
    version     = ">=2.10,<=2.30"
}
```

---

# Terraform Validate

Terraform in detail

---

# Overview of Terraform Validate

Terraform Validate primarily checks whether a configuration is syntactically valid.

It can check various aspects including unsupported arguments, undeclared variables and others.

```
resource "aws_instance" "myec2" {  
    ami           = "ami-082b5a644766e0e6f"  
    instance_type = "t2.micro"  
    sky          = "blue"  
}
```

```
bash-4.2# terraform validate  
  
Error: Unsupported argument  
  
on validate.tf line 10, in resource "aws_instance" "myec2":  
10:   sky = "blue"  
  
An argument named "sky" is not expected here.
```

---

# Load Order & Semantics

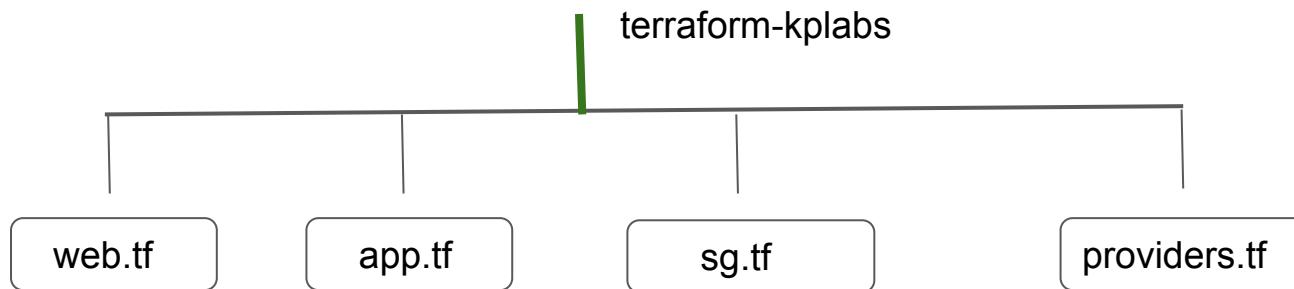
Terraform in detail

---

# Understanding Semantics

Terraform generally loads all the configuration files within the directory specified in alphabetical order.

The files loaded must end in either .tf or .tf.json to specify the format that is in use.



---

# Dynamic Block

Terraform In Depth

---

# Understanding the Challenge

In many of the use-cases, there are repeatable nested blocks that needs to be defined.

This can lead to a long code and it can be difficult to manage in a longer time.

```
ingress {  
    from_port    = 9200  
    to_port      = 9200  
    protocol     = "tcp"  
    cidr_blocks = ["0.0.0.0/0"]  
}
```

```
ingress {  
    from_port    = 8300  
    to_port      = 8300  
    protocol     = "tcp"  
    cidr_blocks = ["0.0.0.0/0"]  
}
```

# Dynamic Blocks

Dynamic Block allows us to dynamically construct repeatable nested blocks which is supported inside resource, data, provider, and provisioner blocks:

```
dynamic "ingress" {
    for_each = var.ingress_ports
    content {
        from_port    = ingress.value
        to_port      = ingress.value
        protocol     = "tcp"
        cidr_blocks = ["0.0.0.0/0"]
    }
}
```

# Iterators

The iterator argument (optional) sets the name of a temporary variable that represents the current element of the complex value

If omitted, the name of the variable defaults to the label of the dynamic block ("ingress" in the example above).

```
dynamic "ingress" {  
    for_each = var.ingress_ports  
    content {  
        from_port    = ingress.value  
        to_port      = ingress.value  
        protocol     = "tcp"  
        cidr_blocks = ["0.0.0.0/0"]  
    }  
}
```



```
dynamic "ingress" {  
    for_each = var.ingress_ports  
    iterator = port  
    content {  
        from_port    = port.value  
        to_port      = port.value  
        protocol     = "tcp"  
        cidr_blocks = ["0.0.0.0/0"]  
    }  
}
```

# **Terraform Taint**

# Understanding the Use-Case

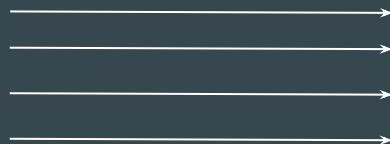
You have created a new resource via Terraform.

Users have made a lot of manual changes (both infrastructure and inside the server)

Two ways to deal with this: Import Changes to Terraform / Delete & Recreate the resource



Lots of manual changes

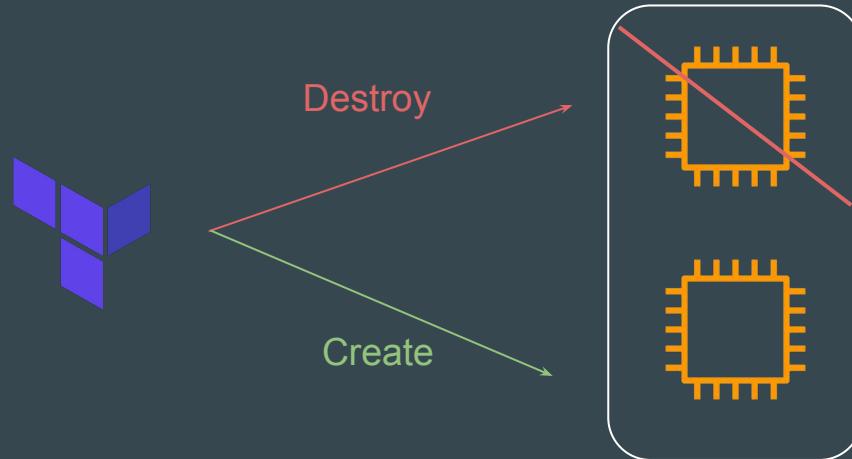


Terraform Managed Resource

# Recreating the Resource

The **-replace** option with `terraform apply` to force Terraform to replace an object even though there are no configuration changes that would require it.

```
terraform apply -replace="aws_instance.web"
```



## Points to Note

Similar kind of functionality was achieved using `terraform taint` command in older versions of Terraform.

For Terraform v0.15.2 and later, HashiCorp recommend using the `-replace` option with `terraform apply`

---

# Splat Expression

## Terraform Expressions

---

# Overview of Spalat Expression

Splat Expression allows us to get a list of all the attributes.

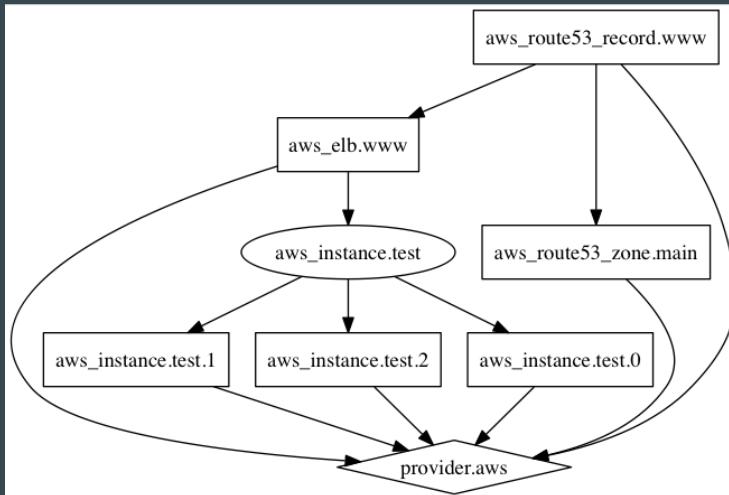
```
resource "aws_iam_user" "lb" {
    name = "iamuser.${count.index}"
    count = 3
    path = "/system/"
}

output "arns" {
    value = aws_iam_user.lb[*].arn
}
```

# Terraform Graph

# Understanding the Base Structure

Terraform graph refers to a **visual representation of the dependency relationships** between resources defined in your Terraform configuration.



# Summary and Conclusion

Terraform graphs are a valuable tool for visualizing and understanding the relationships between resources in your infrastructure defined with Terraform.

It can improve your overall workflow by aiding in planning, debugging, and managing complex infrastructure configurations.

# **Saving Terraform Plan to File**

# Setting the Base

Terraform allows saving a plan to a file.

```
terraform plan -out ec2.plan
```

```
Saved the plan to: ec2.plan
```

```
To perform exactly these actions, run the following command to apply:  
terraform apply "ec2.plan"
```

# Apply from Plan File

You can run the terraform apply by referencing the plan file.

This ensures the infrastructure state remains exactly as shown in the plan to ensure consistency.

```
C:\Users\zealv\kplabs-terraform>terraform apply infra.plan
aws_security_group.allow_tls: Creating...
aws_security_group.allow_tls: Creation complete after 4s [id=sg-02ed88b1d80a484a6]
aws_vpc_security_group_ingress_rule.app_port: Creating...
aws_vpc_security_group_ingress_rule.ssh_port: Creating...
aws_vpc_security_group_ingress_rule.ftp_port: Creating...
aws_vpc_security_group_ingress_rule.app_port: Creation complete after 1s [id=sgr-0b8f10164824c9027]
aws_vpc_security_group_ingress_rule.ssh_port: Creation complete after 1s [id=sgr-042688b669ba3d824]
aws_vpc_security_group_ingress_rule.ftp_port: Creation complete after 2s [id=sgr-0962b3406710b00ba]

Apply complete! Resources: 4 added, 0 changed, 0 destroyed.
```

# Exploring Terraform Plan File

The saved Terraform plan file will be a binary file.

You can use the `terraform show` command to read the contents in detail.

```
{  
    "format_version": "1.2",  
    "terraform_version": "1.9.1",  
    "variables": {  
        "app_port": {  
            "value": "8080"  
        },  
        "ftp_port": {  
            "value": "21"  
        },  
        "ssh_port": {  
            "value": "22"  
        },  
        "vpn_ip": {  
            "value": "200.20.30.50/32"  
        }  
    },  
    "planned_values": {  
        "root_module": {  
            "resources": [  
                {  
                    "address": "aws_security_group.allow_tls",  
                    "mode": "managed",  
                    "type": "aws_security_group",  
                    "name": "allow_tls",  
                    "provider_name": "registry.terraform.io/hashicorp/aws",  
                    "schema_version": 1,  
                    "values": {  
                        "description": "Managed from Terraform",  
                        "name": "terraform-firewall",  
                        "values": {}  
                    }  
                }  
            ]  
        }  
    }  
}
```

# Use-Cases of Saving Plan to a File

Many organizations require documented proof of planned changes before implementation.

These changes will further be reviewed and approved.

Running apply from plan ensures consistent desired outcome.

---

# Terraform Output

Terraform in detail

---

# Terraform Output

The terraform output command is used to extract the value of an output variable from the state file.

```
C:\Users\Zeal Vora\Desktop\terraform\terraform>terraform output iam_names
[
  "iamuser.0",
  "iamuser.1",
  "iamuser.2",
]
```

# Terraform Settings

# Setting the Base

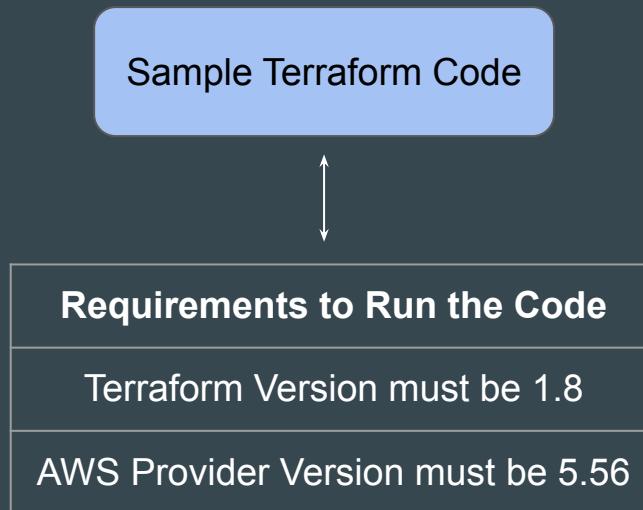
We can use the provider block to define various aspects of the provider, like region, credentials and so on.

```
provider "aws" {
    region      = "us-east-1"
    access_key  = "AKIAIOSFODNN7EXAMPLE"
    secret_key  = "wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY"
}

resource "aws_security_group" "sg_01" {
    name = "app_firewall"
}
```

# Specific Version to Run Your Code

In a Terraform project, your code might require a very specific set of versions to run.



# Introducing Terraform Settings

Terraform Settings are used to configure project-specific Terraform behaviors, such as requiring a minimum Terraform version to apply to your configuration.

Terraform settings are gathered together into **terraform blocks**:

```
terraform {  
    # <setting-1>  
    # <setting-2>  
}
```

# 1 - Specifying a Required Terraform Version

If your code is compatible with specific versions of Terraform, you can use the **required\_version** block to add your constraints.

```
terraform {  
    required_version = "1.8"  
}
```

## 2 - Specifying Provider Requirements

The `required_providers` block can be used to specify all of the providers required by your Terraform code.

You can further fine-tune to include a specific version of the provider plugins.

```
terraform {
  required_providers {
    aws = {
      version = "5.56"
      source  = "hashicorp/aws"
    }
  }
}
```

# Flexibility in Settings Block

There are a wide variety of options that can be specified in the Terraform block.

```
terraform {....}
```



## Options That Can be Defined

Required Terraform Version

Required Provider and Version

BackEnd Configuration

Experimental Features

## Point to Note

It is a good practice to include the `terraform { }` block to include details like `required_providers` as part of your project.

The `provider { }` block is still important to specify various other aspects like regions, credentials, alias and others.

---

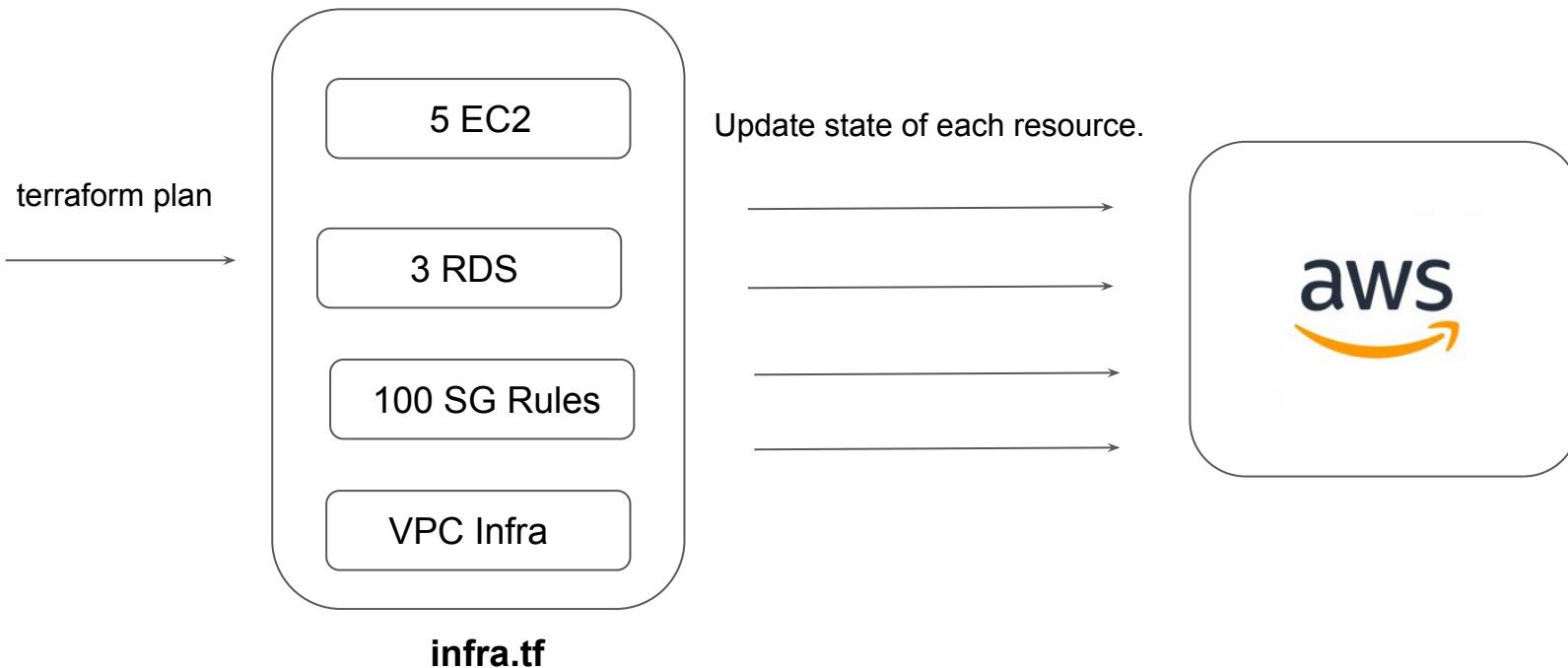
# Dealing with Larger Infrastructure

Terraform in detail

---

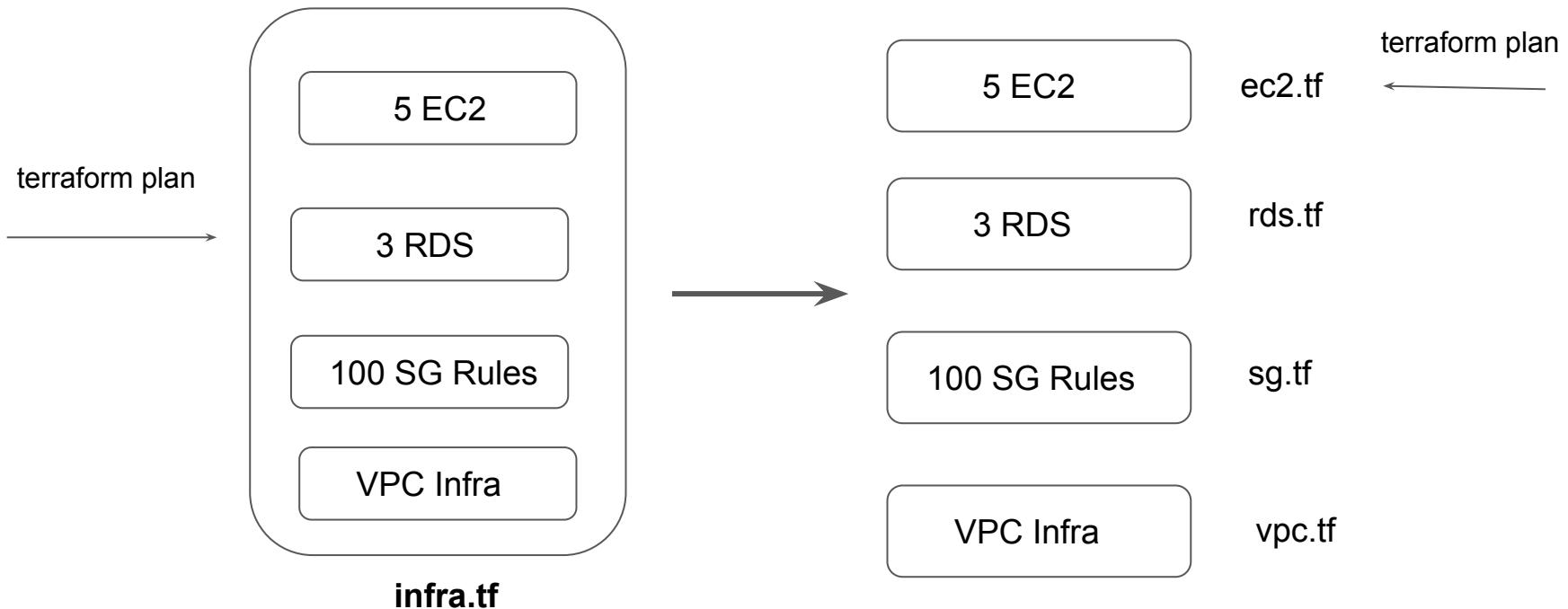
# Challenges with Larger Infrastructure

When you have a larger infrastructure, you will face issue related to API limits for a provider.



# Dealing With Larger Infrastructure

Switch to smaller configuration were each can be applied independently.



# Slow Down, My Man

We can prevent terraform from querying the current state during operations like terraform plan.

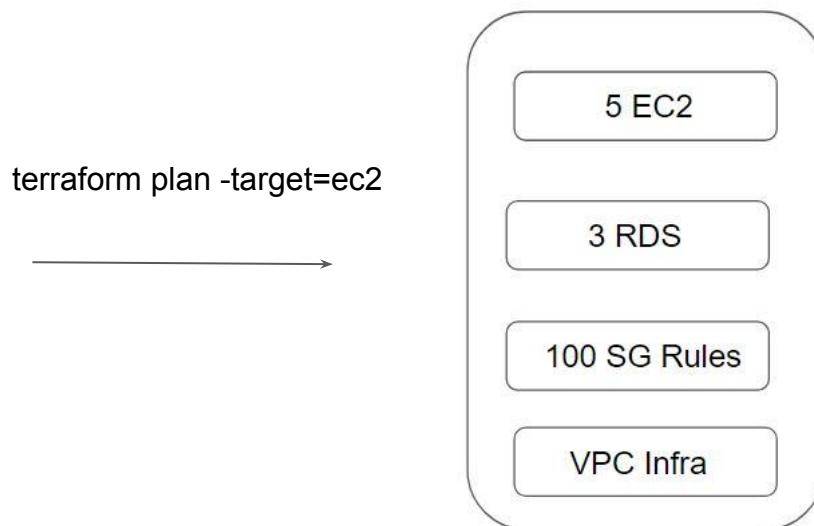
This can be achieved with the [-refresh=false flag](#)



# Specify the Target

The `-target=resource` flag can be used to target a specific resource.

Generally used as a means to operate on isolated portions of very large configurations



---

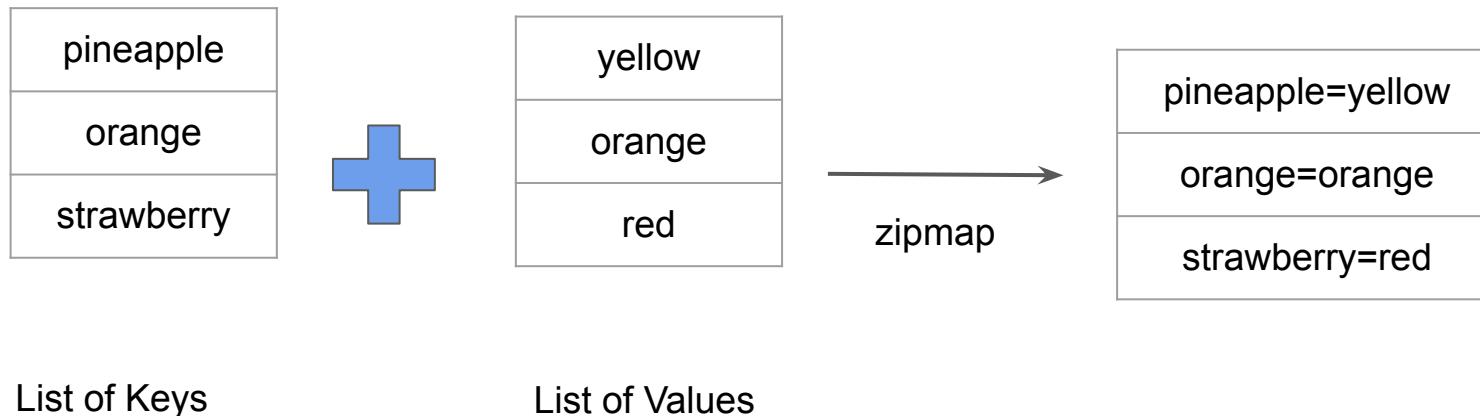
# Zipmap

Terraform Function

---

# Overview of Zipmap

The zipmap function constructs a map from a list of keys and a corresponding list of values.



# Sample Output of Zipmap Function

```
←[J]> zipmap(["pineapple","oranges","strawberry"], ["yellow","orange","red"])
{
  "oranges" = "orange"
  "pineapple" = "yellow"
  "strawberry" = "red"
}
```

# Simple Use-Case

You are creating multiple IAM users.

You need output which contains direct mapping of IAM names and ARNs

```
zipmap = {  
    "demo-user.0" = "arn:aws:iam::018721151861:user/system/demo-user.0"  
    "demo-user.1" = "arn:aws:iam::018721151861:user/system/demo-user.1"  
    "demo-user.2" = "arn:aws:iam::018721151861:user/system/demo-user.2"  
}
```

---

# Comments in Terraform Code

Commenting the Code!

# Overview of Comments

A comment is a text note added to source code to provide explanatory information, usually about the function of the code

```
'''In this program, we check if the number is positive or
negative or zero and
display an appropriate message'''

num = 3.4

# Try these two variations as well:
# num = 0
# num = -4.5

if num > 0:
    print("Positive number")
elif num == 0:
    print("Zero")
else:
    print("Negative number")
```

# Comments in Terraform

The Terraform language supports three different syntaxes for comments:

| Type      | Description                                                                     |
|-----------|---------------------------------------------------------------------------------|
| #         | begins a single-line comment, ending at the end of the line.                    |
| //        | also begins a single-line comment, as an alternative to #.                      |
| /* and */ | are start and end delimiters for a comment that might span over multiple lines. |

# **Resource Behavior and Meta-Argument**

# Understanding the Basics

A **resource block** declares that you want a particular infrastructure object to exist with the given settings

```
resource "aws_instance" "myec2" {
    ami = "ami-00c39f71452c08778"
    instance_type = "t2.micro"
}
```

# How Terraform Applies a Configuration

Create resources that exist in the configuration but are not associated with a real infrastructure object in the state.

Destroy resources that exist in the state but no longer exist in the configuration.

Update in-place resources whose arguments have changed.

Destroy and re-create resources whose arguments have changed but which cannot be updated in-place due to remote API limitations.

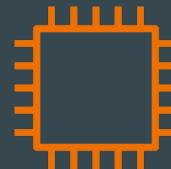
# Understanding the Limitations

What happens if we want to change the default behavior?

Example: Some modification happened in Real Infrastructure object that is not part of Terraform but you want to ignore those changes during terraform apply.

```
resource "aws_instance" "web" {
    ami           = "ami-00c39f71452c08778"
    instance_type = "t3.micro"

    tags = {
        Name = "HelloWorld"
    }
}
```



|      |            |
|------|------------|
| Name | HelloWorld |
|------|------------|

|     |            |
|-----|------------|
| Env | Production |
|-----|------------|

# Solution - Using Meta Arguments

Terraform allows us to include **meta-argument** within the resource block which allows some details of this standard resource behavior to be customized on a per-resource basis.

Inside resource block

```
resource "aws_instance" "myec2" {
    ami = "ami-00c39f71452c08778"
    instance_type = "t2.micro"

    lifecycle {
        ignore_changes = [tags]
    }
}
```

# Different Meta-Arguments

| Meta-Argument | Description                                                                                                                                            |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| depends_on    | Handle hidden resource or module dependencies that Terraform cannot automatically infer.                                                               |
| count         | Accepts a whole number, and creates that many instances of the resource                                                                                |
| for_each      | Accepts a map or a set of strings, and creates an instance for each item in that map or set.                                                           |
| lifecycle     | Allows modification of the resource lifecycle.                                                                                                         |
| provider      | Specifies which provider configuration to use for a resource, overriding Terraform's default behavior of selecting one based on the resource type name |

# **Meta Argument - LifeCycle**

# Basics of Lifecycle Meta-Argument

Some details of the default resource behavior can be customized using the special nested lifecycle block within a resource block body:

```
resource "aws_instance" "myec2" {
    ami = "ami-0f34c5ae932e6f0e4"
    instance_type = "t2.micro"

    tags = {
        Name = "HelloEarth"
    }

    lifecycle {
        ignore_changes = [tags]
    }
}
```

# Arguments Available

There are four argument available within lifecycle block.

| Arguments             | Description                                                                                                          |
|-----------------------|----------------------------------------------------------------------------------------------------------------------|
| create_before_destroy | New replacement object is created first, and the prior object is destroyed after the replacement is created.         |
| prevent_destroy       | Terraform to reject with an error any plan that would destroy the infrastructure object associated with the resource |
| ignore_changes        | Ignore certain changes to the live resource that does not match the configuration.                                   |
| replace_triggered_by  | Replaces the resource when any of the referenced items change                                                        |

# Replace Triggered By

Replaces the resource when any of the referenced items change.

```
resource "aws_appautoscaling_target" "ecs_target" {
    # ...

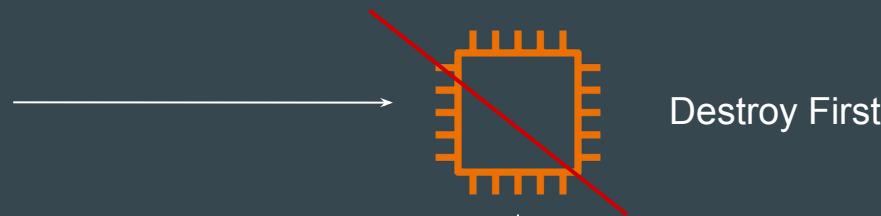
    lifecycle {
        replace_triggered_by = [
            # Replace `aws_appautoscaling_target` each time this instance of
            # the `aws_ecs_service` is replaced.
            aws_ecs_service.svc.id
        ]
    }
}
```

# **Create Before Destroy Argument**

# Understanding the Default Behavior

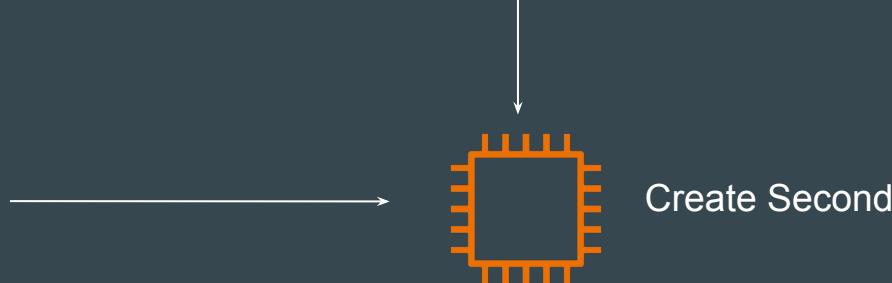
By default, when Terraform must change a resource argument that cannot be updated in-place due to remote API limitations, Terraform will instead destroy the existing object and then create a new replacement object with the new configured arguments.

```
🦄 demo.tf > ...
resource "aws_instance" "myec2" {
  ami = "ami-00c39f71452c08778"
  instance_type = "t2.micro"
}
```



Changed AMI

```
resource "aws_instance" "myec2" {
  ami           = "ami-123456789"
  instance_type = "t2.micro"
}
```



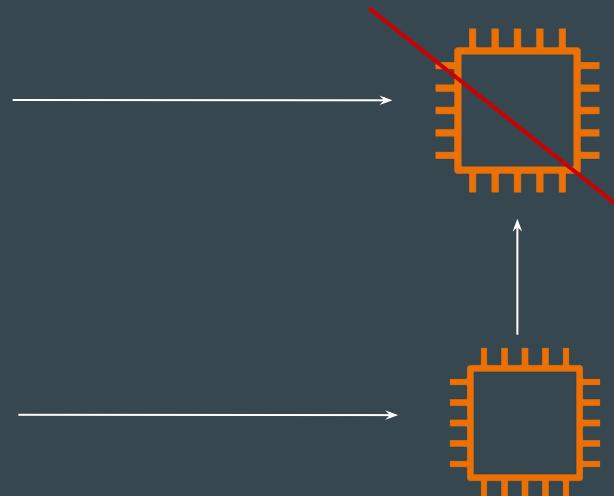
# Create Before Destroy Argument

The `create_before_destroy` meta-argument changes this behavior so that the new replacement object is created first, and the prior object is destroyed after the replacement is created.

```
resource "aws_instance" "myec2" {  
    ami = "ami-053b0d53c279acc90"  
    instance_type = "t2.micro"  
  
    lifecycle {  
        create_before_destroy = true  
    }  
}
```

↓  
Changed AMI

```
resource "aws_instance" "myec2" {  
    ami = "ami-123456789"  
    instance_type = "t2.micro"  
  
    lifecycle {  
        create_before_destroy = true  
    }  
}
```

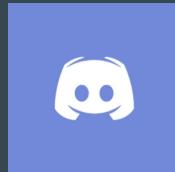


Destroy Second

Create First

# Join us in our Adventure

Be Awesome



[kplabs.in/chat](https://kplabs.in/chat)



[kplabs.in/linkedin](https://kplabs.in/linkedin)

# **LifeCycle - Prevent Destroy Argument**

# Prevent Destroy Argument

This meta-argument, when set to true, will cause Terraform to reject with an error any plan that would destroy the infrastructure object associated with the resource, as long as the argument remains present in the configuration.

```
resource "aws_instance" "myec2" {
    ami          = "ami-123456789"
    instance_type = "t2.micro"

    lifecycle {
        prevent_destroy = true
    }
}
```

## Points to Note

This can be used as a measure of safety against the accidental replacement of objects that may be costly to reproduce, such as database instances.

Since this argument must be present in configuration for the protection to apply, note that this setting does not prevent the remote object from being destroyed if the resource block were removed from configuration entirely.

# **LifeCycle - Ignore Changes Argument**

# Ignore Changes

In cases where settings of a remote object is modified by processes outside of Terraform, the Terraform would attempt to "fix" on the next run.

In order to change this behavior and ignore the manually applied change, we can make use of `ignore_changes` argument under `lifecycle`.

```
resource "aws_instance" "myec2" {
    ami = "ami-00c39f71452c08778"
    instance_type = "t2.micro"

    lifecycle {
        ignore_changes = [tags]
    }
}
```

# Points to Note

Instead of a list, the special keyword `all` may be used to instruct Terraform to ignore all attributes, which means that Terraform can create and destroy the remote object but will never propose updates to it.

```
resource "aws_instance" "myec2" {
    ami = "ami-0f34c5ae932e6f0e4"
    instance_type = "t2.micro"

    tags = {
        Name = "HelloEarth"
    }

    lifecycle {
        ignore_changes = all
    }
}
```

---

# Challenges with Count

Meta-Argument

# Revising the Basics

Resources are identified by the index value from the list.

```
variable "iam_names" {
  type = list
  default = ["user-01","user-02","user-03"]
}

resource "aws_iam_user" "iam" {
  name = var.iam_names[count.index]
  count = 3
  path = "/system/"
```



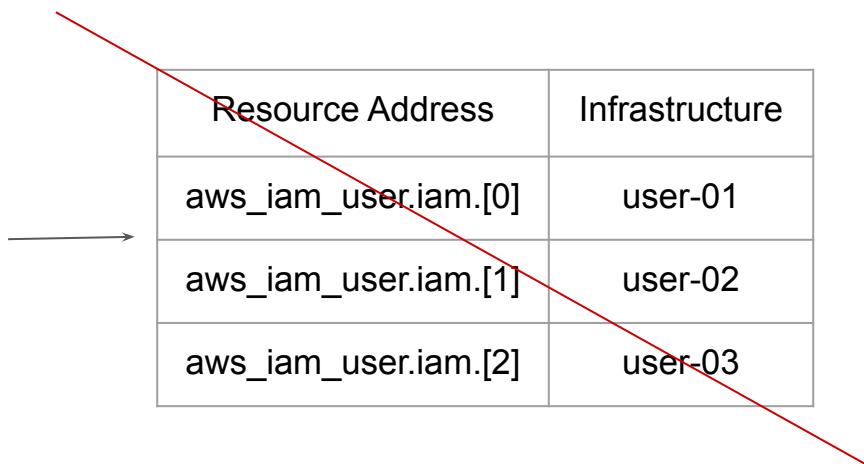
| Resource Address    | Infrastructure |
|---------------------|----------------|
| aws_iam_user.iam[0] | user-01        |
| aws_iam_user.iam[1] | user-02        |
| aws_iam_user.iam[2] | user-03        |

# Challenge - 1

If the order of elements of index is changed, this can impact all of the other resources.

```
variable "iam_names" {
  type = list
  default = ["user-0","user-01","user-02","user-03"]
}

resource "aws_iam_user" "iam" {
  name = var.iam_names[count.index]
  count = 4
  path = "/system/"
}
```



# Important Note

If your resources are almost identical, count is appropriate.

If distinctive values are needed in the arguments, usage of `for_each` is recommended.

```
resource "aws_instance" "server" {
    count = 4 # create four similar EC2 instances
    ami      = "ami-a1b2c3d4"
    instance_type = "t2.micro"
}
```

# **SET - Data Type**

# Revising List Data Type

Lists are used to store multiple items in a single variable.

These items can be duplicates as well.

```
C:\Users\zealv\kplabs-terraform>terraform apply -auto-approve
var.my-list
  Enter a value: ["hello","world","hello"]

Changes to Outputs:
+ variable_output = [
    + "hello",
    + "world",
    + "hello",
  ]

You can apply this plan to save these new output values to the Terraform
Apply complete! Resources: 0 added, 0 changed, 0 destroyed.

Outputs:

variable_output = tolist([
  "hello",
  "world",
  "hello",
])
```

# List and Index

List items are indexed, the first item has index [0], the second item has index [1] etc.

```
variable "user_names" {  
    type = list  
    default = ["alice", "bob", "john"]  
}
```

0      1      2

The diagram illustrates the indexing of the list. Three vertical arrows point upwards from the numbers 0, 1, and 2 at the bottom to the corresponding elements "alice", "bob", and "john" in the list above. This visualizes how each index corresponds to a specific item in the sequence.

# SET Data Type

Sets can only store unique elements.

Any duplicates are automatically removed.

```
C:\Users\zealv\kplabs-terraform>terraform apply -auto-approve
var.my-set
  Enter a value: ["hello","world","hello"]

Changes to Outputs:
  + variable_output = [
      + "hello",
      + "world",
    ]
You can apply this plan to save these new output values to the Terraform
Apply complete! Resources: 0 added, 0 changed, 0 destroyed.

Outputs:

variable_output = toset([
  "hello",
  "world",
])
```

# Point to Note

While defining a SET, you need to also define the type of value that is expected.

```
variable "my-set" {
    type = set(string)
}
```

# SET is Unordered

A set does not store the order of the elements.

Terraform only tracks the presence of elements, not their order.

If the elements in a set change order, Terraform won't detect that as a change. However, if an element is added or removed, Terraform will apply updates accordingly.

```
variable "user_names" {  
    type = list  
    default = ["alice","bob","john"]  
}
```

```
variable "user_names" {  
    type = set(string)  
    default = ["john","bob","alice"]  
}
```

# **The for\_each Meta-Argument**

# Setting the Base

By default, a resource block configures one real infrastructure object.

However, sometimes you want to manage several similar objects (like a fixed pool of compute instances) without writing a separate block for each one.

Terraform has two ways to do this: `count` and `for_each`.

```
resource "aws_iam_user" "lb" {
    name = "alice"
}
```

# Creating 5 IAM Users

If we want to create multiple resources with different configuration, we have to add multiple different resource blocks.



```
iam.tf
●
iam.tf > ...

resource "aws_iam_user" "lb" {
    name = "alice"
}

resource "aws_iam_user" "lb" {
    name = "bob"
}

resource "aws_iam_user" "lb" {
    name = "johh"
}

resource "aws_iam_user" "lb" {
    name = "james"
}

resource "aws_iam_user" "lb" {
    name = "will"
}
```

# Introducing for\_each

If a resource block includes a `for_each` meta argument whose value is a map or a set of strings, Terraform creates one instance for each member of that map or set.

```
variable "user_names" {  
    type = set(string)  
    default = ["alice", "bob"]  
}  
  
resource "aws_iam_user" "lb" {  
    for_each = var.user_names  
    name = each.value  
}
```



```
C:\kplabs-terraform>terraform plan  
  
Terraform used the selected providers to generate the following  
following symbols:  
+ create  
  
Terraform will perform the following actions:  
  
# aws_iam_user.lb["alice"] will be created  
+ resource "aws_iam_user" "lb" {  
    + arn          = (known after apply)  
    + force_destroy = false  
    + id           = (known after apply)  
    + name         = "alice"  
    + path          = "/"  
    + tags_all     = (known after apply)  
    + unique_id    = (known after apply)  
}  
  
# aws_iam_user.lb["bob"] will be created  
+ resource "aws_iam_user" "lb" {  
    + arn          = (known after apply)  
    + force_destroy = false  
    + id           = (known after apply)  
    + name         = "bob"  
    + path          = "/"  
    + tags_all     = (known after apply)  
    + unique_id    = (known after apply)  
}
```

# Point to Note

In blocks where `for_each` is set, an additional `each` object is available.

These object has two attributes:

| Each Object             | Description                                                 |
|-------------------------|-------------------------------------------------------------|
| <code>each.key</code>   | The map key (or set member) corresponding to this instance. |
| <code>each.value</code> | The map value corresponding to this instance                |

# Example - for\_each with Map

When `for_each` is used with map, we can make use of each object to extract both key and value from the given map.

```
variable "mymap" {
  default = {
    dev = "ami-123"
    prod = "ami-456"
  }
}

resource "aws_instance" "web" {
  for_each      = var.mymap
  ami           = each.value
  instance_type = "t3.micro"

  tags = {
    Name = each.key
  }
}
```

# Relax and Have a Meme Before Proceeding

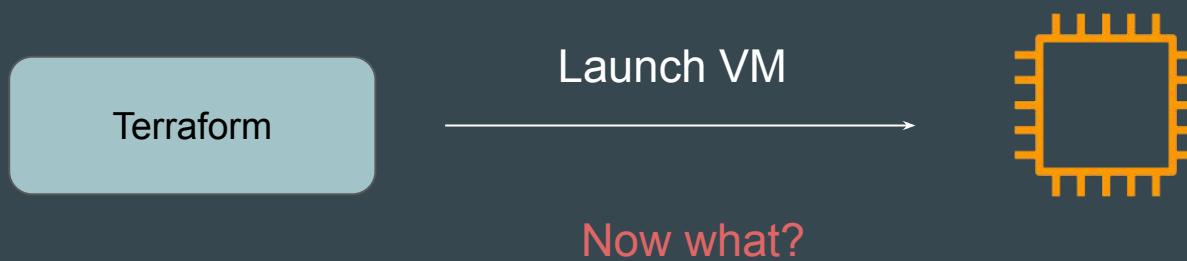


# Terraform Provisioners

# Setting the Base

We have been using Terraform to create and manage resources for a specific provider.

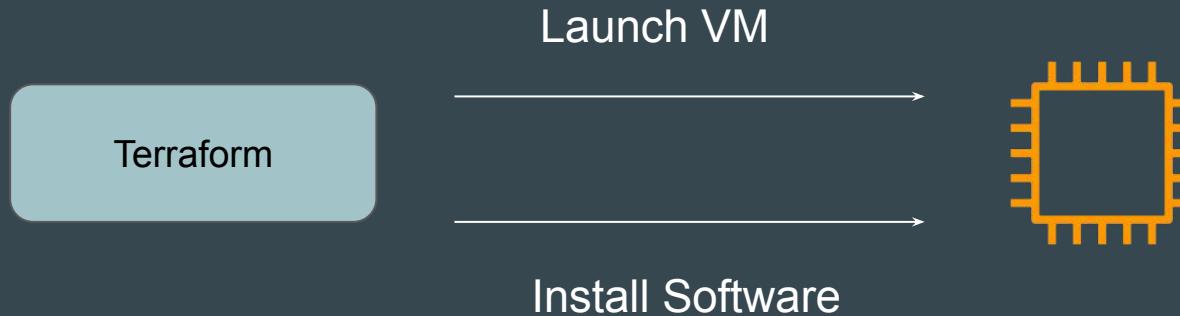
Organizations would want end-to-end solution for creation of infrastructure and configuring appropriate packages required for the application.



# Introducing Provisioners

Provisioners are used to **execute scripts on a local or remote machine** as part of resource creation or destruction.

Example: After VM is launched, install software package required for application.

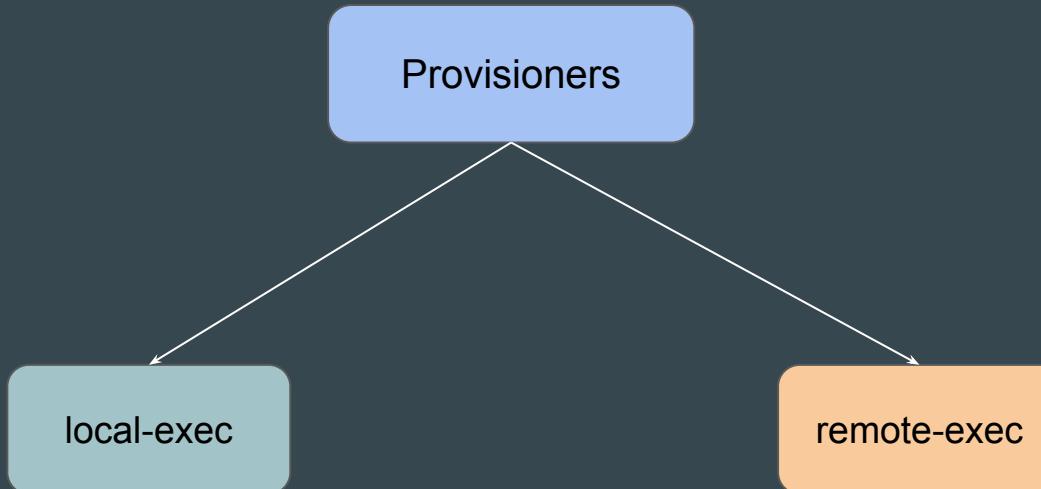


# **Types of Provisioners in Terraform**

# Setting the Base

Provisioners are used to **execute scripts on a local or remote machine** as part of resource creation or destruction.

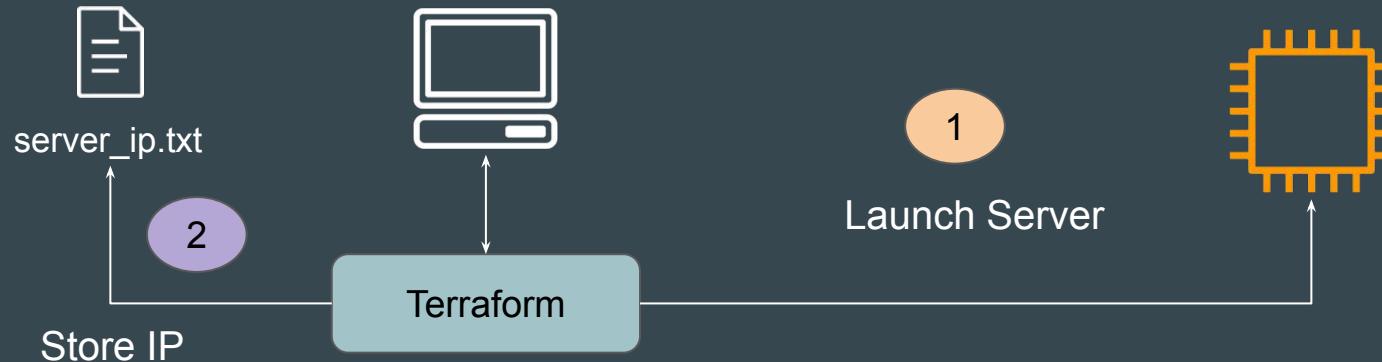
There are 2 major types of provisioners available



# Type 1 - local-exec provisioner

The local-exec provisioner **invokes a local executable** after a resource is created.

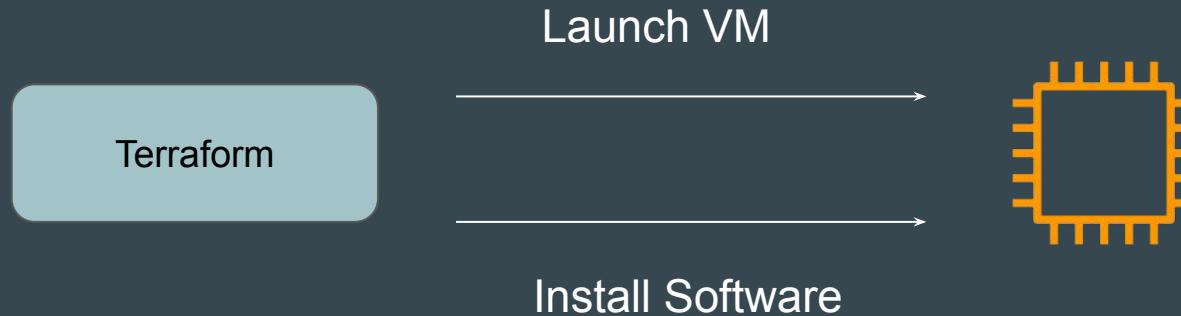
Example: After EC2 is launched, fetch the IP and store it in file `server_ip.txt`



## Type 2 - remote-exec provisioner

remote-exec provisioners allow to invoke scripts or run commands directly on the remote server.

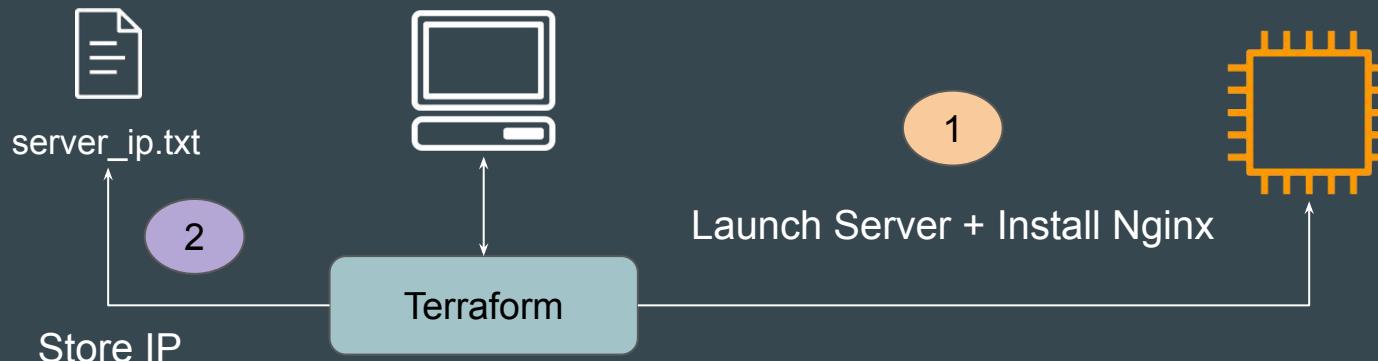
Example: After EC2 is launched, install “apache” software



# Today's Demo

For today's demo, the Terraform code will run two provisioners.

1. Remote-Exec will install Nginx software in EC2 to have basic website.
2. Local-Exec will fetch the Public IP of EC2 and store it in a new file.



# **Format of Provisioners**

# 1 - Defining Provisioners

Provisioners are defined inside a specific resource.

```
resource "aws_instance" "myec2" {  
    ami = "ami-001843b876406202a"  
    instance_type = "t2.micro"  
  
    . . . <provisioners-need-to-be-defined-inside-resource>  
}
```

## 2 - Defining provisioner

Provisioners are defined by “provisioner” followed by type of provisioner

```
resource "aws_instance" "myec2" {
    ami = "ami-001843b876406202a"
    instance_type = "t2.micro"

    provisioner "local-exec" {}
    provisioner "remote-exec" {}

}
```

## 3 - Local Provisioner Approach

For local provisioners, we have to specify command that needs to be run locally

```
resource "aws_instance" "example" {
    ami = "ami-001843b876406202a"
    instance_type = "t2.micro"

    provisioner "local-exec" {
        command = "echo Server has been created through Terraform"
    }
}
```

## 4 - Remote Exec Provisioner Approach

Since commands are executed on remote-server, we have to provide way for Terraform to connect to remote server.

Details to connect to the Server



```
resource "aws_instance" "myec2" {
    ami = "ami-001843b876406202a"
    instance_type = "t2.micro"

    connection {
        type     = "ssh"
        user     = "ec2-user"
        private_key = file("./terraform-key.pem")
        host     = self.public_ip
    }

    provisioner "remote-exec" {
        inline = [
            "sudo yum install -y nginx",
            "sudo systemctl start nginx"
        ]
    }
}
```

Commands to Run on the Server



# **Points to Note - Provisioners**

# Provisioners are Defined inside Resource Block

It is not necessary to define a `aws_instance` resource block for provisioner to run.

They can be defined inside other resource types as well.

```
resource "aws_iam_user" "lb" {
    name = "loadbalancer"

    provisioner "local-exec" {
        command = "echo local-exec provisioner is starting"
    }
}
```

# Multiple Provisioners Blocks for Single Resource

We can define multiple provisioners block in a single resource block.

```
resource "aws_iam_user" "lb" {
    name = "loadbalancer"

    provisioner "local-exec" {
        command = "echo local-exec provisioner is starting"
    }

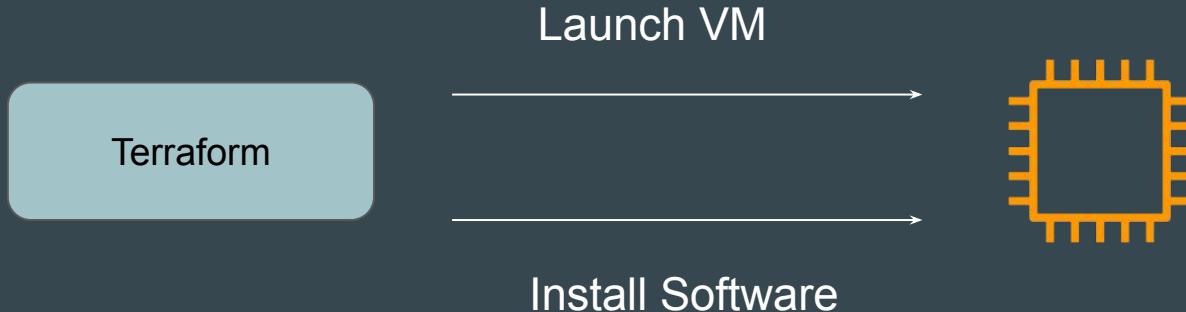
    provisioner "local-exec" {
        command = "echo local-exec-2 provisioner is starting"
    }
}
```

# **Creation-Time & Destroy-Time Provisioners**

# Basic of Creation-Time Provisioners

By default, provisioners run when the resource they are defined within is created.

Creation-time provisioners are **only run during creation**, not during updating or any other lifecycle.



# Destroy-Time Provisioner

Destroy provisioners are run before the resource is destroyed.

Example:

Remove and De-Link Anti-Virus software before EC2 gets terminated.

Define destroy-time  
provisioner

```
resource "aws_instance" "web" {
    # ...

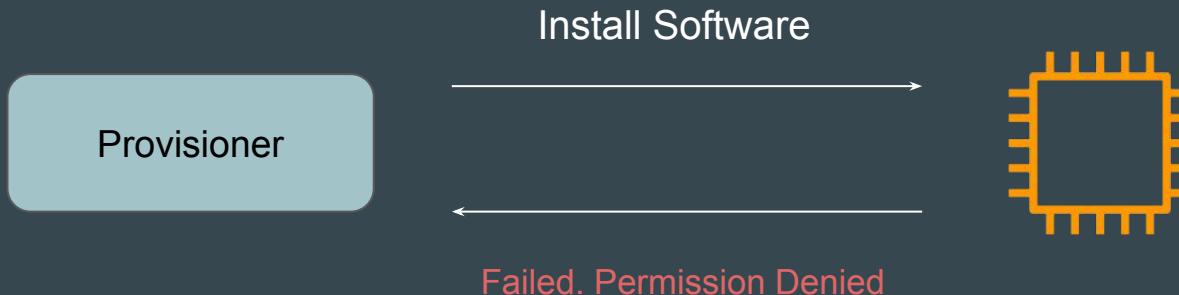
    provisioner "local-exec" {
        when      = destroy
        command  = "echo 'Destroy-time provisioner'"
    }
}
```

# Tainting Resource in Creation-Time Provisioners

If a creation-time provisioner fails, the resource is marked as **tainted**.

A tainted resource will be planned for destruction and recreation upon the next terraform apply.

Terraform does this because a failed provisioner can leave a resource in a semi-configured state.



# Reference Screenshot - Resource Marked as Tainted

Following screenshot shows state file that has marked the resource as “tainted” because the provisioner had failed.

```
Error: local-exec provisioner error  
with aws_iam_user.lb,  
on test-prov.tf line 5, in resource "aws_iam_user" "lb":  
5:   provisioner "local-exec" {  
  
Error running command 'echo1 local-exec provisioner is starting': exit status 1.  
internal or external command,  
operable program or batch file.  
  
resources": [  
  {  
    "mode": "managed",  
    "type": "aws_iam_user",  
    "name": "lb",  
    "provider": "provider[\"registry.terraform.io/hashicorp/aws\"]",  
    "instances": [  
      {  
        "status": "tainted",  
        "schema_version": 0,  
        "attributes": {  
          "arn": "arn:aws:iam::042025557788:user/loadbalancer2",  
          "force_destroy": false,  
          "id": "loadbalancer2",  
        }  
      }  
    ]  
  }  
]
```

# **Failure Behaviour in Provisioners**

# Understanding the Challenge

By default, provisoners that fail will also cause the terraform apply itself to fail.

This will lead to resource being tainted and we have to re-create the resource.

```
# aws_iam_user.lb will be created
+ resource "aws_iam_user" "lb" {
    + arn          = (known after apply)
    + force_destroy = false
    + id           = (known after apply)
    + name         = "loadbalancer2"
    + path          = "/"
    + tags_all     = (known after apply)
    + unique_id    = (known after apply)
}

Plan: 1 to add, 0 to change, 0 to destroy.
aws_iam_user.lb: Creating...
aws_iam_user.lb: Provisioning with 'local-exec'...
aws_iam_user.lb (local-exec): Executing: ["cmd" "/C" "echo1 local-exec provisioner is starting"]
aws_iam_user.lb (local-exec): 'echo1' is not recognized as an internal or external command,
aws_iam_user.lb (local-exec): operable program or batch file.

Error: local-exec provisioner error

with aws_iam_user.lb,
on test-prov.tf line 5, in resource "aws_iam_user" "lb":
  5:   provisioner "local-exec" {

Error running command 'echo1 local-exec provisioner is starting': exit status 1. Output: 'echo1' is not recognized as an
internal or external command,
operable program or batch file.
```

# Basics of On Failure Setting

The `on_failure` setting can be used to change the default behaviour.

| Allowed Values | Description                                                                                                     |
|----------------|-----------------------------------------------------------------------------------------------------------------|
| continue       | Ignore the error and continue with creation or destruction.                                                     |
| fail           | Raise an error and stop applying (the default behavior). If this is a creation provisioner, taint the resource. |

# Reference Code - On-Failure

Following screenshot shows a reference code where `on_failure` is set to `continue`.

```
resource "aws_iam_user" "lb" {
    name = "loadbalancer"

    provisioner "local-exec" {
        command = "echo1 local-exec provisioner is starting"
        on_failure = continue
    }
}
```

# Reference Screenshot - Failed Provisioner

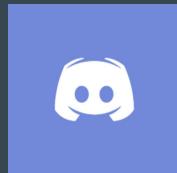
Following screenshot shows that the provisioner has failed but still the apply has completed successfully.

This is an example of `on_failure = continue`

```
Plan: 1 to add, 0 to change, 1 to destroy.  
aws_iam_user.lb: Destroying... [id=loadbalancer2]  
aws_iam_user.lb: Destruction complete after 1s  
aws_iam_user.lb: Creating...  
aws_iam_user.lb: Provisioning with 'local-exec'...  
aws_iam_user.lb (local-exec): Executing: ["cmd" "/C" "echo1 local-exec provisioner is starting"]  
aws_iam_user.lb (local-exec): 'echo1' is not recognized as an internal or external command,  
aws_iam_user.lb (local-exec): operable program or batch file.  
aws_iam_user.lb: Creation complete after 1s [id=loadbalancer2]  
  
Apply complete! Resources: 1 added, 0 changed, 1 destroyed.
```

# Join us in our Adventure

Be Awesome



[kplabs.in/chat](https://kplabs.in/chat)

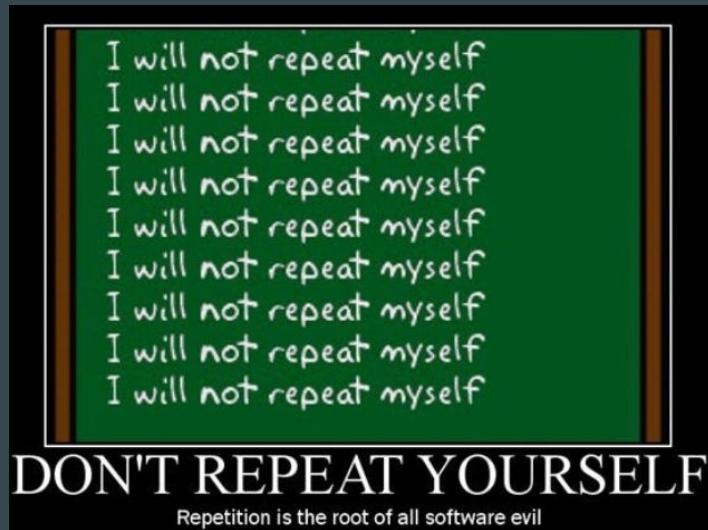


[kplabs.in/linkedin](https://kplabs.in/linkedin)

# **Terraform Modules**

# Understanding the Basic

In software engineering, **don't repeat yourself** (DRY) is a principle of software development aimed at reducing repetition of software patterns.



# Understanding the Challenge

Let's assume there are 10 teams in your organization using Terraform to create and manage EC2 instances.

```
resource "aws_instance" "web" {  
    ami          = "ami-1234"  
    instance_type = "t3.micro"  
    key_name      = "user1"  
    monitoring     = true  
    vpc_security_group_ids = ["sg-12345678"]  
}
```

Team1

```
resource "aws_instance" "web" {  
    ami          = "ami-1234"  
    instance_type = "t3.micro"  
    key_name      = "user1"  
    monitoring     = true  
    vpc_security_group_ids = ["sg-12345678"]  
}
```

Team 3

```
resource "aws_instance" "web" {  
    ami          = "ami-1234"  
    instance_type = "t3.micro"  
    key_name      = "user1"  
    monitoring     = true  
    vpc_security_group_ids = ["sg-12345678"]  
}
```

Team 5

```
resource "aws_instance" "web" {  
    ami          = "ami-1234"  
    instance_type = "t3.micro"  
    key_name      = "user1"  
    monitoring     = true  
    vpc_security_group_ids = ["sg-12345678"]  
}
```

Team 2

```
resource "aws_instance" "web" {  
    ami          = "ami-1234"  
    instance_type = "t3.micro"  
    key_name      = "user1"  
    monitoring     = true  
    vpc_security_group_ids = ["sg-12345678"]  
}
```

Team 4

```
resource "aws_instance" "web" {  
    ami          = "ami-1234"  
    instance_type = "t3.micro"  
    key_name      = "user1"  
    monitoring     = true  
    vpc_security_group_ids = ["sg-12345678"]  
}
```

Team 6

# Challenge with the Previous Example

1. Repetition of Code.
2. Change in AWS Provider specific option will require change in EC2 code blocks of all the teams.
3. Lack of standardization.
4. Difficult to manage.
5. Difficult for developers to use.

# Better Approach

In this approach, the DevOps Team has defined standard EC2 template in a central location that all can use.

```
resource "aws_instance" "web" {  
    ami           = "ami-1234"  
    instance_type = "t3.micro"  
    key_name      = "user1"  
    monitoring    = true  
    vpc_security_group_ids = ["sg-12345678"]  
    associate_public_ip_address = true  
    instance_initiated_shutdown_behavior = "stop"  
    ebs_optimized = true  
    source_dest_check = false  
    hibernation = true  
    disable_api_termination = true  
}
```

Standard Template

Team 1 Code

Team 2 Code

Team 3 Code

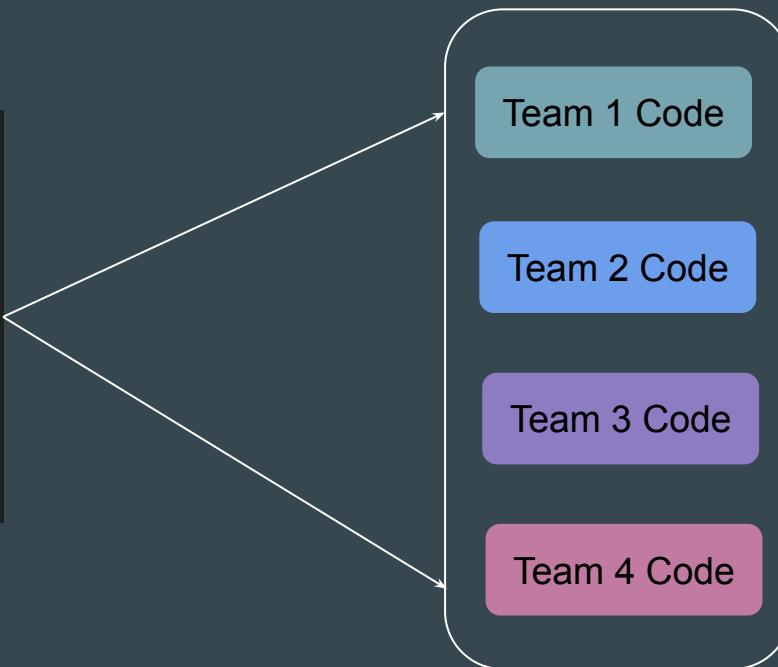
Team 4 Code

# Introducing Terraform Modules

Terraform Modules allows us to centralize the resource configuration and it makes it easier for multiple projects to re-use the Terraform code for projects.

```
resource "aws_instance" "web" {  
    ami          = "ami-1234"  
    instance_type = "t3.micro"  
    key_name      = "user1"  
    monitoring     = true  
    vpc_security_group_ids = ["sg-12345678"]  
    associate_public_ip_address = true  
    instance_initiated_shutdown_behavior = "stop"  
    ebs_optimized = true  
    source_dest_check = false  
    hibernation = true  
    disable_api_termination = true  
}
```

Terraform Module



# Multiple Modules for a Single Project

Instead of writing code from scratch, we can use multiple ready-made modules available.

```
resource "aws_instance" "web" {
    ami           = "ami-1234"
    instance_type = "t3.micro"
    key_name      = "user1"
    monitoring    = true
    vpc_security_group_ids = ["sg-12345678"]
    associate_public_ip_address = true
    instance_initiated_shutdown_behavior = "stop"
    ebs_optimized = true
    source_dest_check = false
    hibernation = true
    disable_api_termination = true
}
```

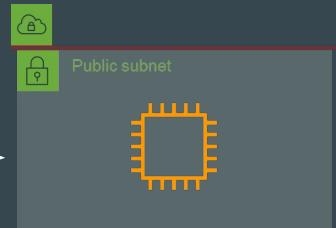
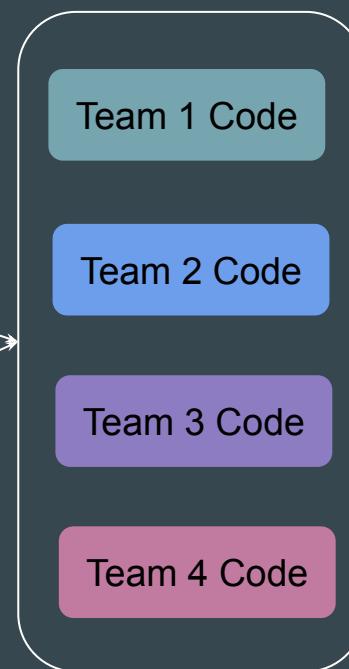
EC2 Module

```
resource "aws_vpc" "this" {
    count = local.create_vpc ? 1 : 0

    cidr_block      = var.use_ipam_pool ? null : var.cidr
    ipv4_ipam_pool_id = var.ipv4_ipam_pool_id
    ipv4_netmask_length = var.ipv4_netmask_length

    assign_generated_ipv6_cidr_block = var.enable_ipv6 && !var.use_ipam_pool ? true : null
    ipv6_cidr_block                = var.ipv6_cidr
    ipv6_ipam_pool_id              = var.ipv6_ipam_pool_id
    ipv6_netmask_length            = var.ipv6_netmask_length
    ipv6_cidr_block_network_border_group = var.ipv6_cidr_block_network_border_group
}
```

VPC Module



Infrastructure Created

# **Points to Note - Referencing Terraform Modules**

# Understanding the Base

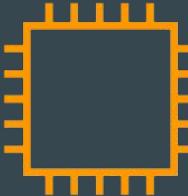
For some infrastructure resources, you can directly use the module calling code, and the entire infrastructure will be created for you.

```
VSCode ec2-module.tf > ...
```

```
module "ec2-instance" {  
  source  = "terraform-aws-modules/ec2-instance/aws"  
  version = "5.6.1"  
}
```

terra

form apply



# Avoiding Confusion

Just by referencing any module, it is not always the case that the infrastructure resource will be created for you directly.

Some modules require specific inputs and values from the user side to be filled in before a resource gets created.

# Example Module - AWS EKS

If you try to use an AWS EKS Module directly and run “terraform apply”, it will throw an **error**.

```
 eks-module.tf > ...
  module "eks" {
    source  = "terraform-aws-modules/eks/aws"
    version = "20.11.1"
  }
```

↓  
terraform apply

```
Plan: 21 to add, 0 to change, 0 to destroy.

Error: Error in function call

on .terraform\modules\eks\main.tf line 48, in resource "aws_eks_cluster" "this":
48:   subnet_ids          = coalescelist(var.control_plane_subnet_ids, var.subnet_ids)

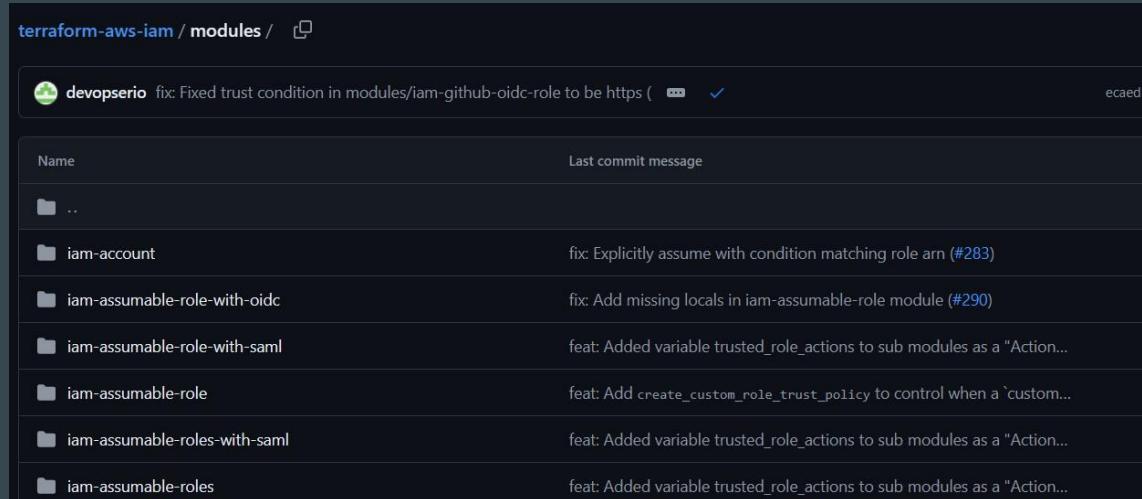
      while calling coalescelist(vals...)
      var.control_plane_subnet_ids is empty list of string
      var.subnet_ids is empty list of string

Call to function "coalescelist" failed: no non-null arguments.
```

# Module Structure Can be Different

Some module pages in GitHub can contain multiple sets of modules together for different features.

In such cases, you have to reference the exact sub-module required.



A screenshot of a GitHub repository page titled "terraform-aws-iam / modules". The page displays a list of several sub-modules under the "modules" directory. Each entry shows the folder name, the last commit message, and the commit author and date. The commits are:

| Name                          | Last commit message                                                                 |
|-------------------------------|-------------------------------------------------------------------------------------|
| ..                            |                                                                                     |
| iam-account                   | fix: Explicitly assume with condition matching role arn (#283)                      |
| iam-assumable-role-with-oidc  | fix: Add missing locals in iam-assumable-role module (#290)                         |
| iam-assumable-role-with-saml  | feat: Added variable trusted_role_actions to sub modules as a "Action..."           |
| iam-assumable-role            | feat: Add <code>create_custom_role_trust_policy</code> to control when a `custom... |
| iam-assumable-roles-with-saml | feat: Added variable trusted_role_actions to sub modules as a "Action..."           |
| iam-assumable-roles           | feat: Added variable trusted_role_actions to sub modules as a "Action..."           |

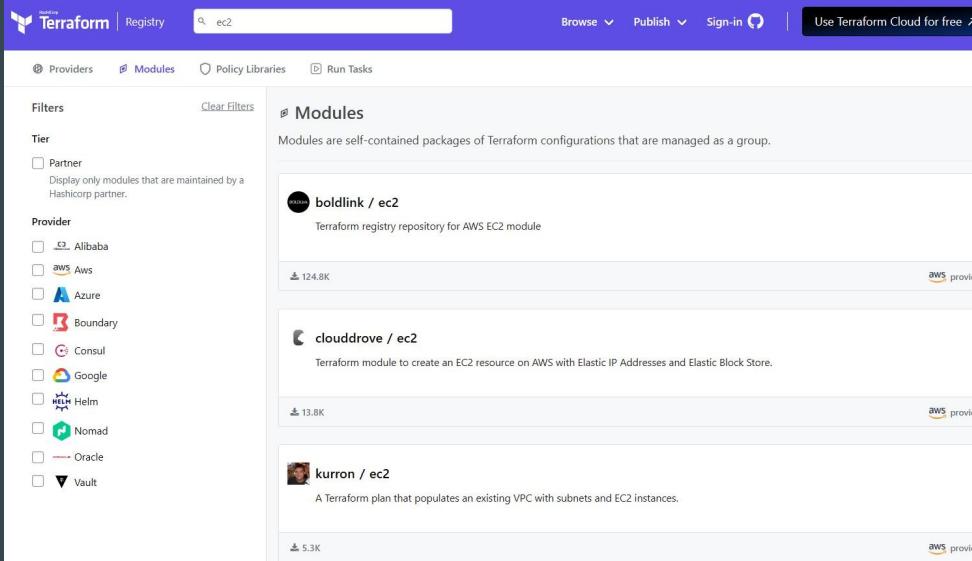
# Learnings for Today's Video

Always read the Module Documentation to understand the overall structure, important information, and what is expected from the user side when creating a resource.

# **Choosing the Right Terraform Module**

# Understanding the Base

Terraform Registry can contain multiple modules for a specific infrastructure resource maintained by different users



The screenshot shows the Terraform Registry interface. At the top, there's a search bar with the query "ec2". Below the search bar, there are navigation links for "Browse", "Publish", and "Sign-in". A button on the right says "Use Terraform Cloud for free".

The main area is titled "Modules" and contains a brief description: "Modules are self-contained packages of Terraform configurations that are managed as a group." Below this, three modules are listed:

- boldlink / ec2**: "Terraform registry repository for AWS EC2 module". It has 124.8K stars and is an "aws provider".
- clouddrove / ec2**: "Terraform module to create an EC2 resource on AWS with Elastic IP Addresses and Elastic Block Store.". It has 13.8K stars and is an "aws provider".
- kurron / ec2**: "A Terraform plan that populates an existing VPC with subnets and EC2 instances.". It has 5.3K stars and is an "aws provider".

On the left side, there are filters and a sidebar with categories like "Providers", "Modules", "Policy Libraries", and "Run Tasks". The "Filters" section includes a "Tier" filter for "Partner" modules and a "Provider" filter listing various cloud providers: Alibaba, Aws, Azure, Boundary, Consul, Google, Helm, Nomad, Oracle, and Vault.

# 1 - Check Total Downloads

Module Downloads can provide early indication about level of acceptance by users in the Terraform community

The screenshot shows the Terraform Registry page for the `ec2-instance` module. The module is categorized under the `aws provider`. It is described as a Terraform module to create AWS EC2 instance(s) resources. The module was published on March 7, 2024, by `terraform-aws-modules`, managed by `antonbabenko`, and has a GitHub source code link.

A dropdown menu shows the current version is `5.6.1 (latest)`. To the right, a summary of module downloads is displayed:

| Downloads this week     | 153,193 |
|-------------------------|---------|
| Downloads this month    | 476,217 |
| Downloads this year     | 2.8M    |
| Downloads over all time | 14.4M   |

Below the download stats, there is a section titled **Provision Instructions** containing Terraform configuration code:

```
module "ec2-instance" {  
  source = "terraform-aws-modules/ec2-instance"  
  version = "5.6.1"  
}
```

## 2 - Check GitHub Page of Module

GitHub page can provide important information related to the Contributors, Reported Issues and other data.

The screenshot shows the GitHub repository page for the "aws-ec2-instance" Terraform module. The repository has 177 commits across 2 branches and 83 tags. The README file is the active tab. The page includes sections for About, Releases, Sponsor this project, Packages, and Contributors. A prominent yellow banner at the bottom encourages users to help Ukraine.

**About**  
Terraform module to create AWS EC2 instance(s) resources. [registry.terraform.io/modules/terraform-aws-ec2-instance/](#)

**Releases** 32  
[v5.6.1 \[Latest\]](#) on Mar 7  
+ 31 releases

**Sponsor this project**  
[antonbabenko](#) /anton Babenko <https://www.paypal.me/antonbabenko>

**Packages**  
No packages published

**Contributors** 42  
+ 28 contributors

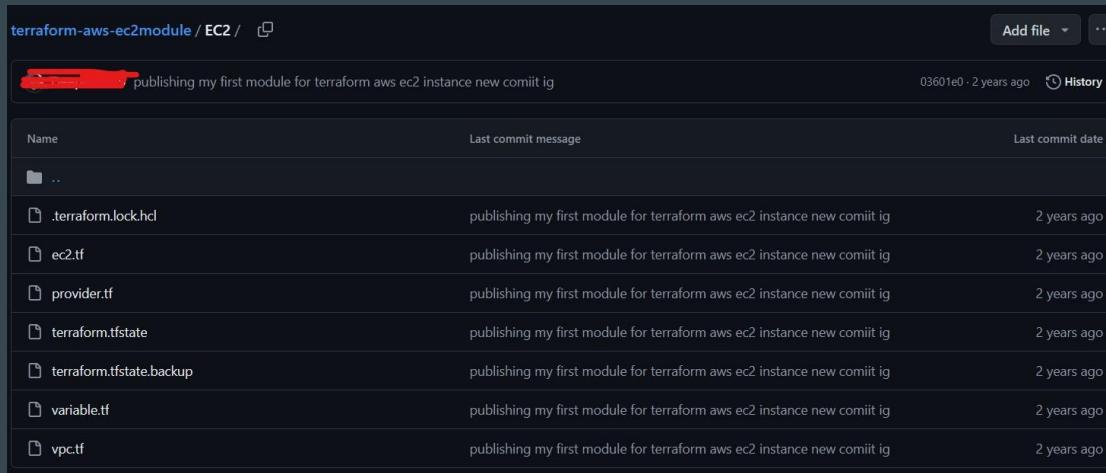
**AWS EC2 Instance Terraform module**  
Terraform module which creates an EC2 instance on AWS.

Russia invaded Ukraine, killing tens of thousands of civilians and displacing millions more. It's a genocide. Please help us defend freedom, democracy and Ukraine's right to exist.

Help Ukraine Now →

## 3 - Avoid Modules Written by Individual Participant

Avoid module that are maintained by a single contributor as regular updates, issues and other areas might not always be maintained.

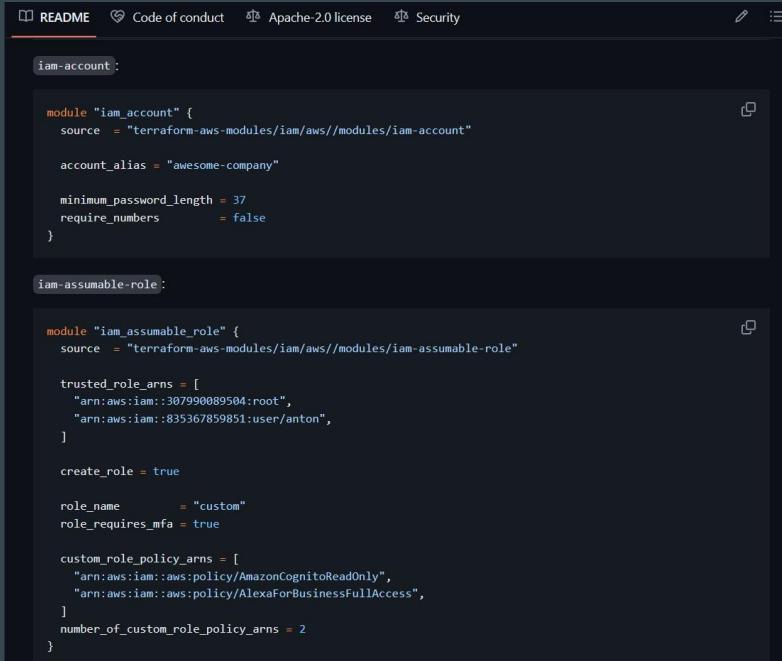


The screenshot shows a GitHub repository named "terraform-aws-ec2module / EC2". A single commit message, "publishing my first module for terraform aws ec2 instance new comitt ig", is present in all files listed in the commit history. The commit was made 2 years ago by a user whose name is partially obscured.

| Name                     | Last commit message                                                     | Last commit date |
|--------------------------|-------------------------------------------------------------------------|------------------|
| ..                       |                                                                         |                  |
| .terraform.lock.hcl      | publishing my first module for terraform aws ec2 instance new comitt ig | 2 years ago      |
| ec2.tf                   | publishing my first module for terraform aws ec2 instance new comitt ig | 2 years ago      |
| provider.tf              | publishing my first module for terraform aws ec2 instance new comitt ig | 2 years ago      |
| terraform.tfstate        | publishing my first module for terraform aws ec2 instance new comitt ig | 2 years ago      |
| terraform.tfstate.backup | publishing my first module for terraform aws ec2 instance new comitt ig | 2 years ago      |
| variable.tf              | publishing my first module for terraform aws ec2 instance new comitt ig | 2 years ago      |
| vpc.tf                   | publishing my first module for terraform aws ec2 instance new comitt ig | 2 years ago      |

# 4 - Analyze Module Documentation

Good documentation should include an overview, usage instructions, input and output variables, and examples.



The screenshot shows a GitHub README page with several tabs at the top: README (which is active), Code of conduct, Apache-2.0 license, and Security. Below the tabs, there are two code snippets:

```
iam-account :  
  
module "iam_account" {  
  source  = "terraform-aws-modules/iam/aws//modules/iam-account"  
  
  account_alias = "awesome-company"  
  
  minimum_password_length = 37  
  require_numbers         = false  
}  
  
iam-assumable-role :  
  
module "iam_assumable_role" {  
  source  = "terraform-aws-modules/iam/aws//modules/iam-assumable-role"  
  
  trusted_role_arns = [  
    "arn:aws:iam::307990089504:root",  
    "arn:aws:iam::8355367859851:user/anton",  
  ]  
  
  create_role = true  
  
  role_name        = "custom"  
  role_requires_mfa = true  
  
  custom_role_policy_arns = [  
    "arn:aws:iam::aws:policy/AmazonCognitoReadOnly",  
    "arn:aws:iam::aws:policy/AlexaForBusinessFullAccess",  
  ]  
  number_of_custom_role_policy_arns = 2  
}
```

# 5 - Check Version History of Module

Look at the version history. Frequent updates and a clear versioning strategy suggest active maintenance.

The screenshot shows the Terraform Registry interface for the "iam" module. The top navigation bar includes links for "Browse", "Publish", "Sign-in", and "Use Terraform Cloud for free". The main content area displays the "iam" module details, which is an "aws provider" used to create AWS IAM resources. It was published on May 15, 2024, by "terraform-aws-modules" and managed by "antonbabenko". The source code is available on GitHub at [github.com/terraform-aws-modules/terraform-aws-iam](https://github.com/terraform-aws-modules/terraform-aws-iam). Below this, there are buttons for "Submodules" and "Examples". A dropdown menu titled "Version 5.39.1 (latest)" lists previous versions from 5.32.1 to 5.39.1. To the right, a "Module Downloads" section shows statistics for the current week, month, year, and all time. At the bottom, "Provision Instructions" provide a Terraform configuration snippet:

```
module "iam" {  
    source = "terraform-aws-modules/iam"  
    version = "5.39.1"  
}
```

# 6 - Analyze the Code

Inspect the module's source code on GitHub or another platform. Clean, well-structured code is a good sign.

```
resource "aws_instance" "this" {
    count = local.create && !var.ignore_ami_changes && !var.create_spot_instance ? 1 : 0

    ami              = local.ami
    instance_type    = var.instance_type
    cpu_core_count   = var.cpu_core_count
    cpu_threads_per_core = var.cpu_threads_per_core
    hibernation      = var.hibernation

    user_data         = var.user_data
    user_data_base64 = var.user_data_base64
    user_data_replace_on_change = var.user_data_replace_on_change

    availability_zone = var.availability_zone
    subnet_id         = var.subnet_id
    vpc_security_group_ids = var.vpc_security_group_ids

    key_name          = var.key_name
    monitoring        = var.monitoring
    get_password_data = var.get_password_data
    iam_instance_profile = var.create_iam_instance_profile ? aws_iam_instance_profile.this[0].name : var.iam_instance_profile
```

# 7 - Check the Community Feedback

The number of stars and forks on GitHub can indicate popularity and community interest.

The screenshot shows the GitHub repository page for 'terraform-aws-ec2-instance'. The repository is public and has 735 stars and 1.8k forks. The 'Code' tab is selected, showing the master branch with 2 branches and 83 tags. The commit history lists several recent changes, including updates to CI workflows, examples, and wrappers, along with documentation and security-related commits. The repository is described as a Terraform module to create AWS EC2 instances. It includes links to the registry, AWS tags, and various contributing and licensing information.

terraformer-aws-modules / **terraform-aws-ec2-instance** Public

Type ⌘ to search

Code Issues 3 Pull requests 1 Actions Security Insights

**terraform-aws-ec2-instance** Public

Sponsor Watch 24 Fork 1.8k Star 735

master 2 Branches 83 Tags Go to file Add file Code About

semantic-release-bot chore(release): version 5.6.1 [skip ci] 4f8387d · 2 months ago 177 Commits

.github/workflows fix: Update CI workflow versions to remove deprecated runti... 2 months ago

examples feat: Add example for connecting via Session Manager witho... 9 months ago

wrappers feat: Support Private DNS name options (#370) 5 months ago

.editorconfig [ci skip] Create ".editorconfig". 4 years ago

.gitignore chore: update documentation based on latest terraform-doc... 3 years ago

.pre-commit-config.yaml fix: Update CI workflow versions to remove deprecated runti... 2 months ago

.releaserc.json chore: Update release configuration files to correctly use con... 3 years ago

Terraform module to create AWS EC2 instance(s) resources UA

registry.terraform.io/modules/terraform-aws-ec2-instance

aws aws-ec2 ec2-instance

terraform-module

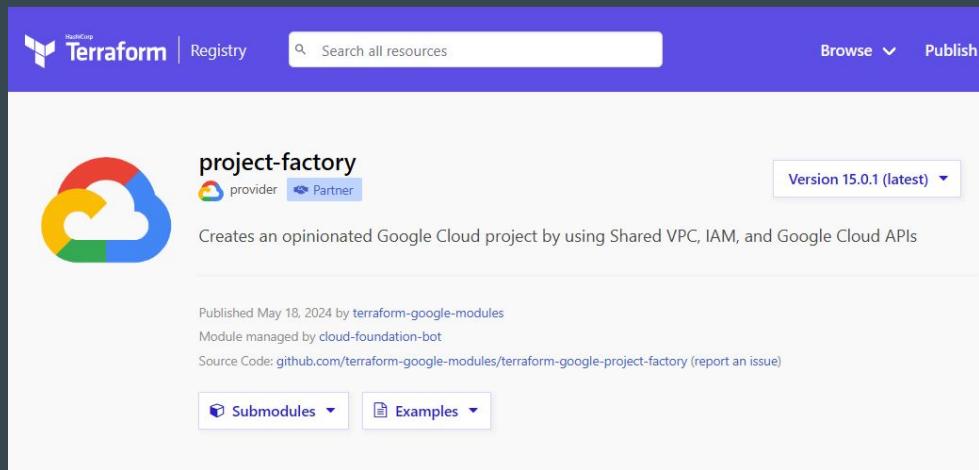
Readme Apache-2.0 license

Code of conduct Security policy

Activity Custom properties

# 8 - Modules Maintained by HashiCorp Partner

Search for modules that are maintained by HashiCorp Partners



## Important Point to Note

Avoid directly trying any random Terraform module that is not actively maintained and looks shady (primarily by sole individual contributors)

An attacker can include malicious code in a module that sends information about your environment to the attacker.

# Which Modules do Organizations Use?

In most of the scenarios, organizations maintain their own set of modules.

They might initially fork a module from the Terraform registry and modify it based on their use case.

# **Creating Base Module Structure**

# Understanding the Base Structure

A base “modules” folder.

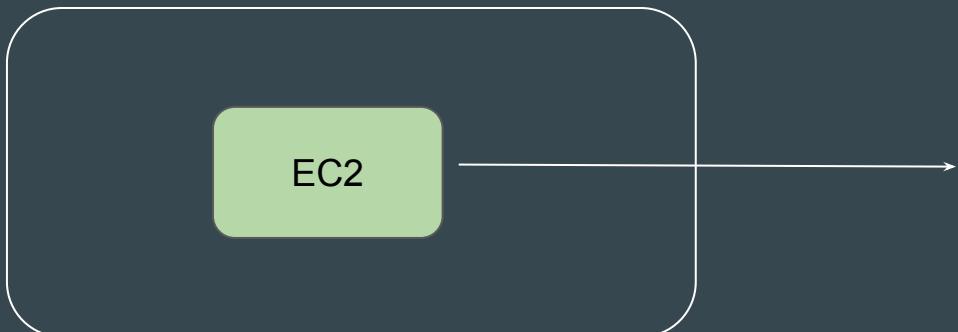
A sub-folder containing name for each modules that are available.



modules folder

# What is Inside the Sub-Folders

Each module's sub-folder contains the actual module Terraform code that other projects can reference from.



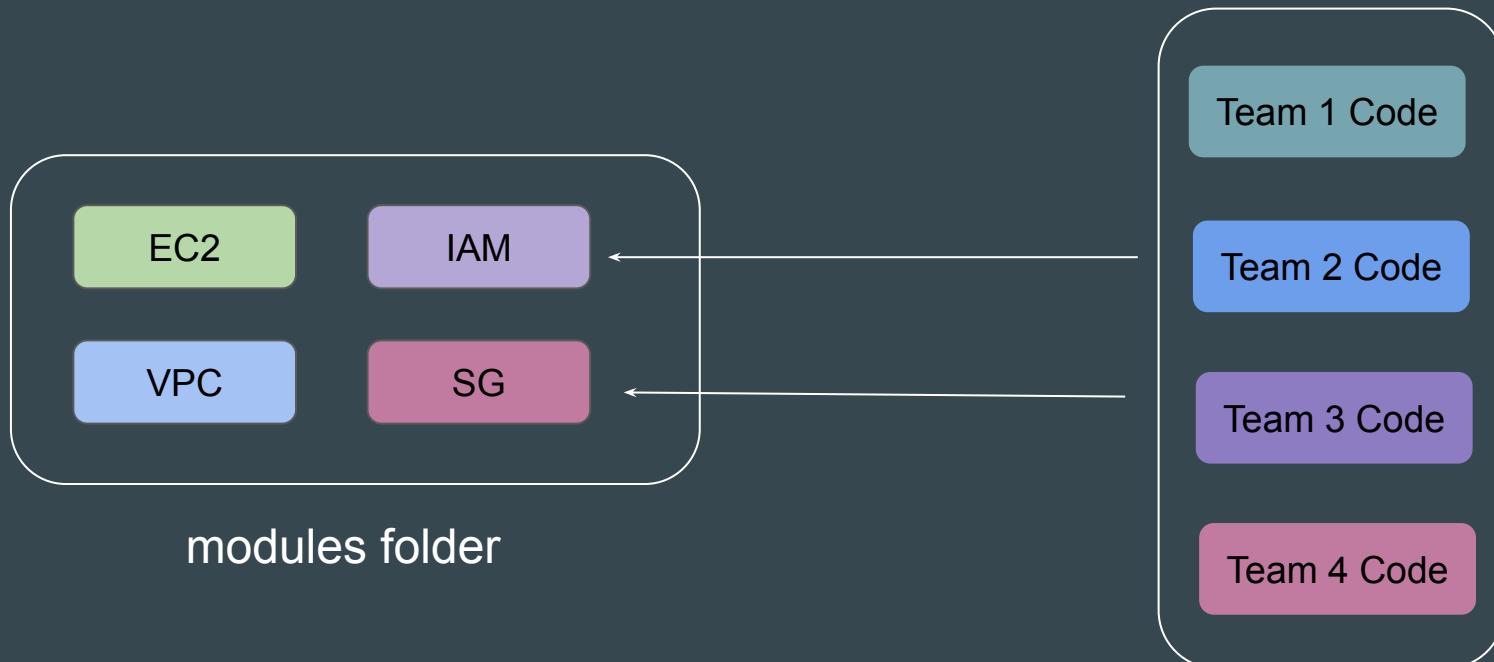
modules folder

```
resource "aws_instance" "web" {
    ami          = "ami-1234"
    instance_type = "t3.micro"
    key_name     = "user1"
    monitoring    = true
    vpc_security_group_ids = ["sg-12345678"]
    associate_public_ip_address = true
    instance_initiated_shutdown_behavior = "stop"
    ebs_optimized   = true
    source_dest_check = false
    hibernation = true
    disable_api_termination = true
}
```

main.tf

# Calling the Module

Each Team can call various set of modules that are available in the modules folder based on their requirements.

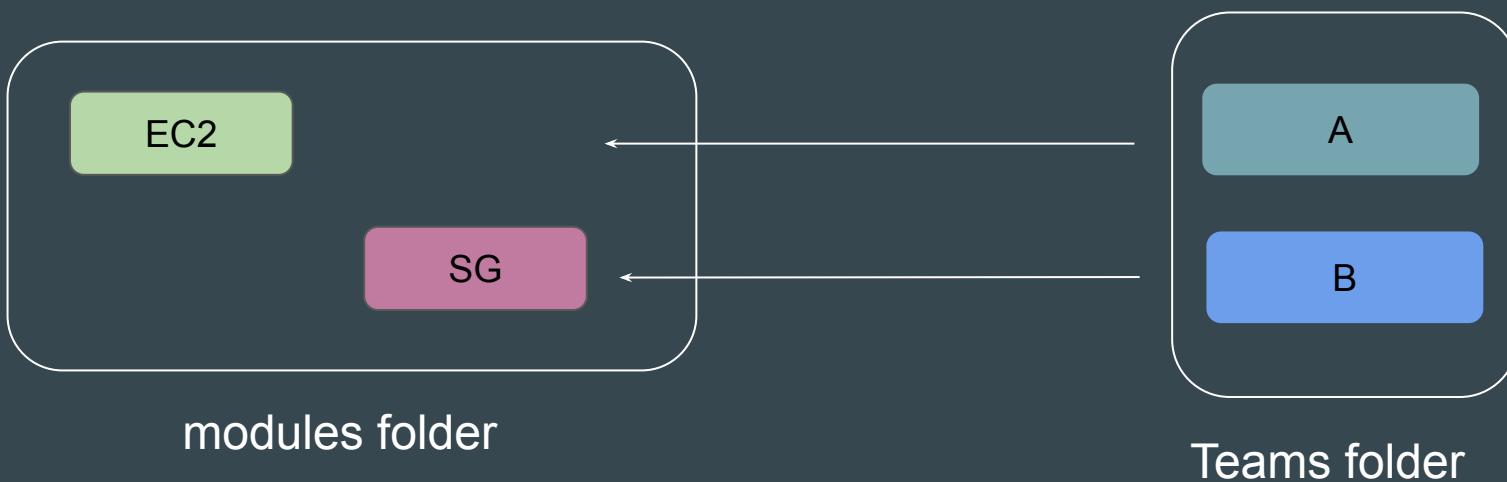


# Our Practical Structure

Our practical structure will include two main folders (modules and teams).

Modules sub-folder will contain sub-folders of modules that are available.

Teams sub-folder will contain list of teams that we want to be made available.



# **Module Sources - Calling a Module**

# Understanding the Base

Module source code can be present in wide variety of locations.

These includes:

1. GitHub
2. HTTP URLs
3. S3 Buckets
4. Terraform Registry
5. Local paths

# Base - Calling the Module

In order to reference to a module, you need to make use of **module** block

The module block must contain source argument that contains location to the referenced module.

```
module "ec2" {  
    source = "https://example.com/vpc-module.zip"  
}
```

## Example 1 - Local Paths

Local paths are used to reference to module that is available in local filesystem.

A local path must begin with either ./ or ../ to indicate that a local path

```
module "ec2" {
    source = "../modules/ec2"
}
```

## Example 2 - Generic Git Repository

Arbitrary Git repositories can be used by prefixing the address with the special `git::` prefix.

```
module "vpc" {
    source = "git::https://example.com/vpc.git"
}
```

# Module Version

A specific module can have multiple versions.

You can reference to specific version of module with the **version** block

```
module "eks" {
  source  = "terraform-aws-modules/eks/aws"
  version = "20.11.1"
}
```

# **Improvements in Custom Module Code**

# Our Simple Module

We had created a very simple module that allows developers to launch an EC2 instance when calling the module.

```
provider "aws" {
    region = "us-east-1"
}

resource "aws_instance" "myec2" {
    ami = "ami-0bb84b8ffd87024d8"
    instance_type = "t2.micro"
}
```

# Need to Analyze Shortcomings

Being a simplistic and a basic module code, there is a good room of improvements.

In today's video, we will be discussing about some of the important shortcomings with the code.



# Challenge 1 - Hardcoded Values

The values are hardcoded as part of the module.

If developer is calling the module, he will have to stick with same values.

Developer will not be able to override the hardcoded values of the module.

Hard-Coded Values

```
provider "aws" {
    region = "us-east-1"
}

resource "aws_instance" "myec2" {
    ami = "ami-0bb84b8ffd87024d8"
    instance_type = "t2.micro"
}
```

# Challenge 2 - Provider Improvements

Avoid hard-coding region in the Module code as much as possible.

A **required\_provider** block with version constraints for module to work is important.

```
provider "aws" {
  region = "us-east-1"
}

resource "aws_instance" "myec2" {
  ami      = "ami-0bb84b8ffd87024d8"
  instance_type = "t2.micro"
}
```



```
terraform {

  required_providers {
    aws = {
      source  = "hashicorp/aws"
      version = ">= 5.5"
    }
  }

  resource "aws_instance" "myec2" {
    ami      = "ami-0bb84b8ffd87024d8"
    instance_type = "t2.micro"
  }
}
```

# **Variables in Terraform Modules**

## Point to Note

As much as possible, avoid hardcoded values as part of the Modules.

This will make the module less flexible.



# Convert Hard Coded Values to Variables

For modules, it is especially recommended to convert hard-coded values to **variables** so that it can be overridden based on user requirements.

```
resource "aws_instance" "myec2" {  
    ami = "ami-0bb84b8ffd87024d8"  
    instance_type = "t2.micro"  
}
```



Bad Approach

```
resource "aws_instance" "myec2" {  
    ami = var.ami  
    instance_type = var.instance_type  
}
```

Good Approach

# Advantages of Variables in Module Code

Variable based approach will allow the teams to override the values.

```
resource "aws_instance" "myec2" {
    ami = var.ami
    instance_type = var.instance_type
}
```

Main Module

Team 1

instance\_type = t2.micro

Team 2

instance\_type = m5.large

# Reviewing Professional EC2 Module Code

Reviewing an EC2 Module code that is professionally written, we see that the values associated with arguments are not hardcoded and variables are used extensively.

```
resource "aws_instance" "this" {
  count = local.create && !var.ignore_ami_changes && !var.create_spot_instance ? 1 : 0

  ami           = local.ami
  instance_type = var.instance_type
  cpu_core_count = var.cpu_core_count
  cpu_threads_per_core = var.cpu_threads_per_core
  hibernation    = var.hibernation

  user_data      = var.user_data
  user_data_base64 = var.user_data_base64
  user_data_replace_on_change = var.user_data_replace_on_change

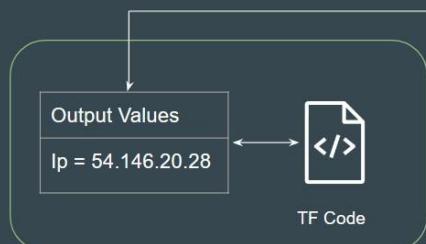
  availability_zone = var.availability_zone
  subnet_id        = var.subnet_id
  vpc_security_group_ids = var.vpc_security_group_ids

  key_name        = var.key_name
  monitoring      = var.monitoring
  get_password_data = var.get_password_data
  iam_instance_profile = var.create_iam_instance_profile ? aws_iam_instance_profile.this[0].name : var.iam_instance_profile
```

# **Module Outputs**

# Revising Output Values

**Output values** make information about your infrastructure available on the command line, and can expose information for other Terraform configurations to use.



```
resource "aws_eip" "lb" {  
    domain    = "vpc"  
}  
  
output "public-ip" {  
    value = aws_eip.lb.public_ip  
}
```

# Understanding the Challenge

If you want to create a resource that has a dependency on an infrastructure created through a module, you won't be able to implicitly call it without output values.

```
resource "aws_instance" "myec2" {  
    ami = "ami-123"  
    instance_type = "t2.micro"  
}
```



```
module "ec2" {  
    source = "../../modules/ec2"  
}  
  
resource "aws_eip" "lb" {  
    instance = module.ec2.instance_id  
    domain  = "vpc"  
}
```

# Accessing Child Module Outputs

Ensure to include output values in the module code for better flexibility and integration with other resources and projects.

**Format:** module.<MODULE NAME>.<OUTPUT NAME>

```
resource "aws_instance" "myec2" {
    ami = var.ami
    instance_type = var.instance_type
}

output "instance_id" {
    value = aws_instance.myec2.id
}
```

```
module "ec2" {
    source = "../../modules/ec2"
}

resource "aws_eip" "lb" {
    instance = module.ec2.instance_id
    domain  = "vpc"
}
```

# **Root and Child Modules**

# Root Module

Root Module resides in the **main working directory of your Terraform configuration**. This is the entry point for your infrastructure definition

```
module "ec2" {  
    source = "../../modules/ec2"  
}
```

Root Module

# Child Module

A **module that has been called by another module** is often referred to as a child module.



# **Standard Module Structure**

# Setting the Base

At this stage, we have been keeping the overall module structure very simple to understand the concepts.

In production environments, it is important to follow recommendations and best-practices set by HashiCorp.

# Basic of Standard Module Structure

The **standard module structure** is a file and directory layout HashiCorp recommends for reusable modules.

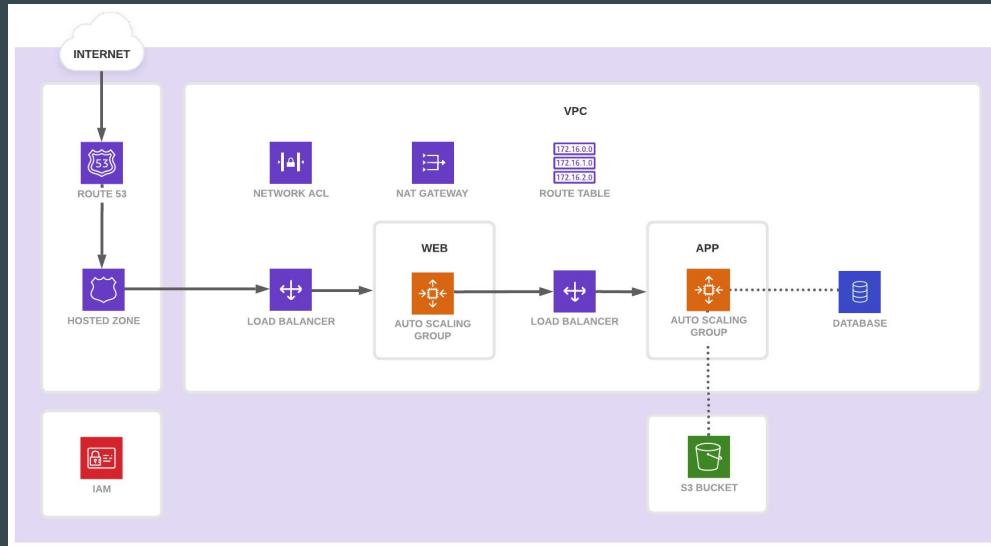
A minimal recommended module following the standard structure is shown below

```
$ tree minimal-module/
.
├── README.md
└── main.tf
    ├── variables.tf
    └── outputs.tf
```

# Scope the Requirements for Module Creation

A team wants to provision their infrastructure using Terraform.

The following architecture diagram depicts the desired outcome.



# Planning a Module Structure

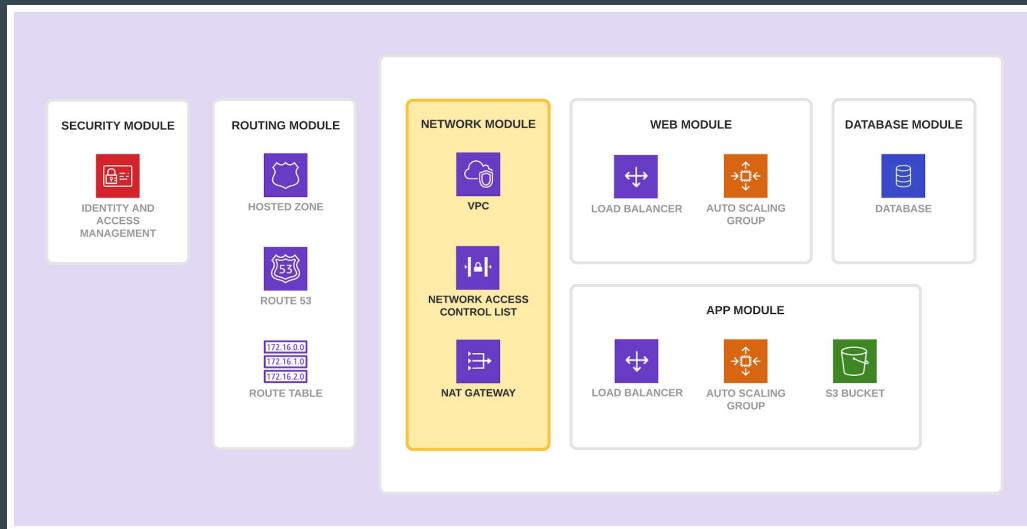
In this scenario, a team of Terraform producers, who write Terraform code from scratch, will build a collection of modules to provision the infrastructure and applications.

The members of the team in charge of the application will consume these modules to provision the infrastructure they need.

# Final Module Output

After reviewing the consumer team's requirements, the producer team has broken up the application infrastructure into the following modules:

Network, Web, App, Database, Routing, and Security.



---

# Publishing Modules

Publish Modules to Terraform Registry

---

# Overview of Publishing Modules

Anyone can publish and share modules on the Terraform Registry.

Published modules support versioning, automatically generate documentation, allow browsing version histories, show examples and READMEs, and more.



# Requirements for Publishing Module

| Requirement               | Description                                                                                                                                                                |
|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| GitHub                    | The module must be on GitHub and must be a public repo. This is only a requirement for the public registry.                                                                |
| Named                     | Module repositories must use this three-part name format<br>terraform-<PROVIDER>-<NAME>                                                                                    |
| Repository description    | The GitHub repository description is used to populate the short description of the module.                                                                                 |
| Standard module structure | The module must adhere to the standard module structure.                                                                                                                   |
| x.y.z tags for releases   | The registry uses tags to identify module versions. Release tag names must be a semantic version, which can optionally be prefixed with a v. For example, v1.0.4 and 0.9.2 |

# Standard Module Structure

The standard module structure is a file and directory layout that is recommended for reusable modules distributed in separate repositories

```
$ tree minimal-module/
.
├── README.md
├── main.tf
├── variables.tf
└── outputs.tf
```

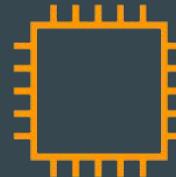
```
$ tree complete-module/
.
├── README.md
├── main.tf
├── variables.tf
├── outputs.tf
├── ...
└── modules/
    ├── nestedA/
    │   ├── README.md
    │   ├── variables.tf
    │   ├── main.tf
    │   └── outputs.tf
    ├── nestedB/
    │   ├── ...
    └── examples/
        ├── exampleA/
        │   ├── main.tf
        ├── exampleB/
        └── .../
```

# Terraform Workspace

# Setting the Base

An infrastructure created through Terraform is **tied to the** underlying Terraform configuration and a state file.

```
resource "aws_instance" "myec2" {  
    ami = "ami-00c39f71452c08778"  
    instance_type = "t2.micro"  
}
```



EC2 Instance



terraform.tfstate

# What If?

What if we have multiple state file for single Terraform configuration?

Can we manage different env's through it separately?

```
resource "aws_instance" "myec2" {  
    ami = "ami-00c39f71452c08778"  
    instance_type = "t2.micro"  
}
```



State File 1



State File 2



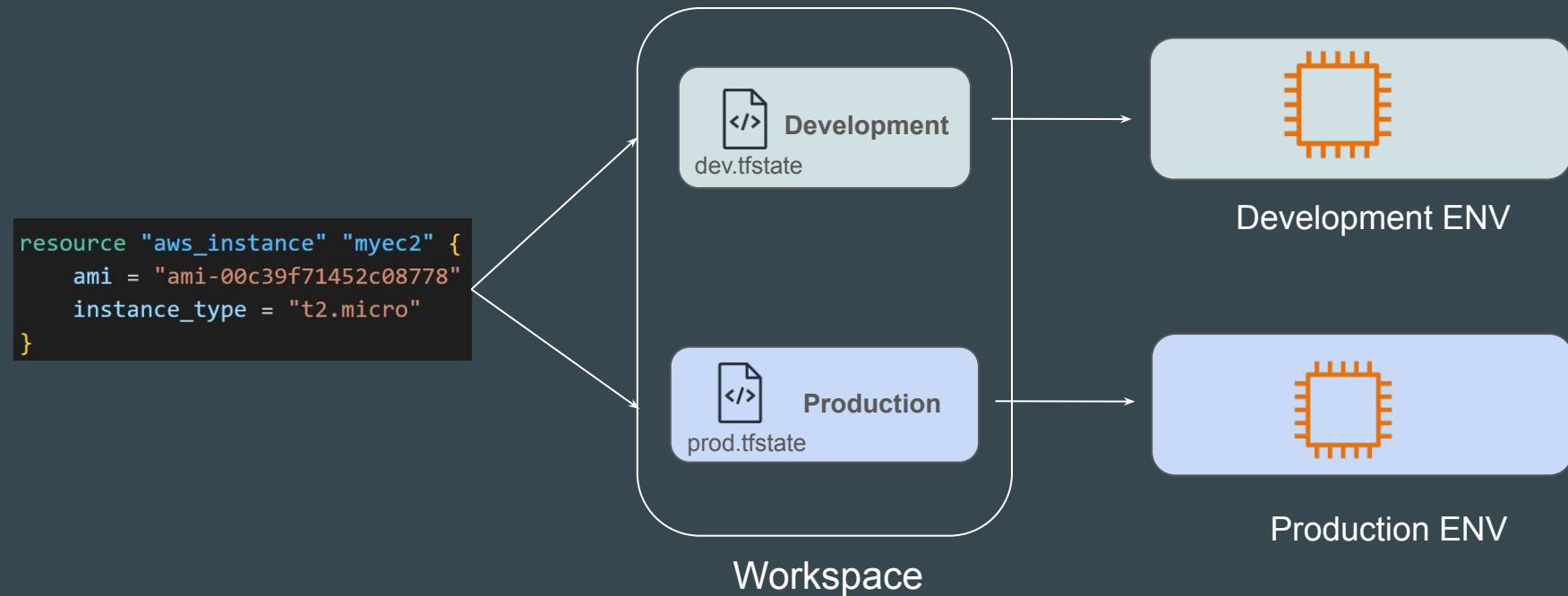
Environment 1



Environment 2

# Introducing Terraform Workspace

Terraform workspaces enable us to **manage multiple set of deployments from the same sets of configuration file.**

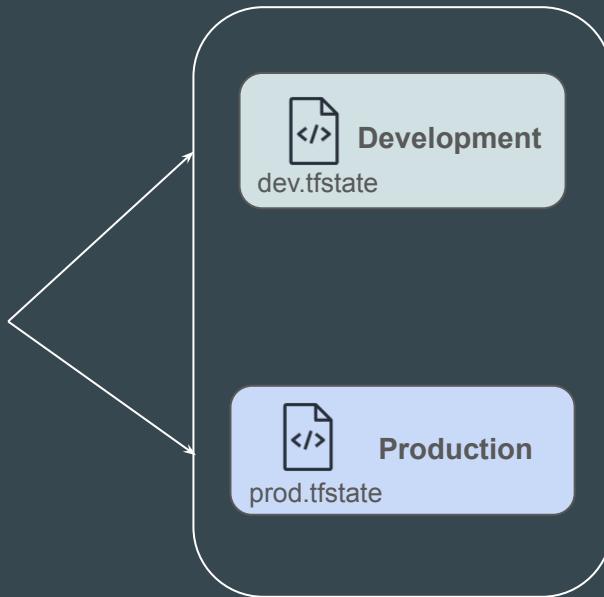


# Flexibility with Workspace

Depending on the workspace being used, the value to a specific argument in your Terraform code can also change.

```
resource "aws_instance" "myec2" {
  ami           = "ami-08a0d1e16fc3f61ea"
  instance_type = local.instance_types[terraform.workspace]
}
```

| Environment | instance_type |
|-------------|---------------|
| Development | t2.micro      |
| Production  | m5.large      |



Workspace

---

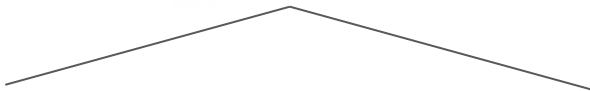
# Team Collaboration

Terraform in detail

---

# Local Changes are not always good

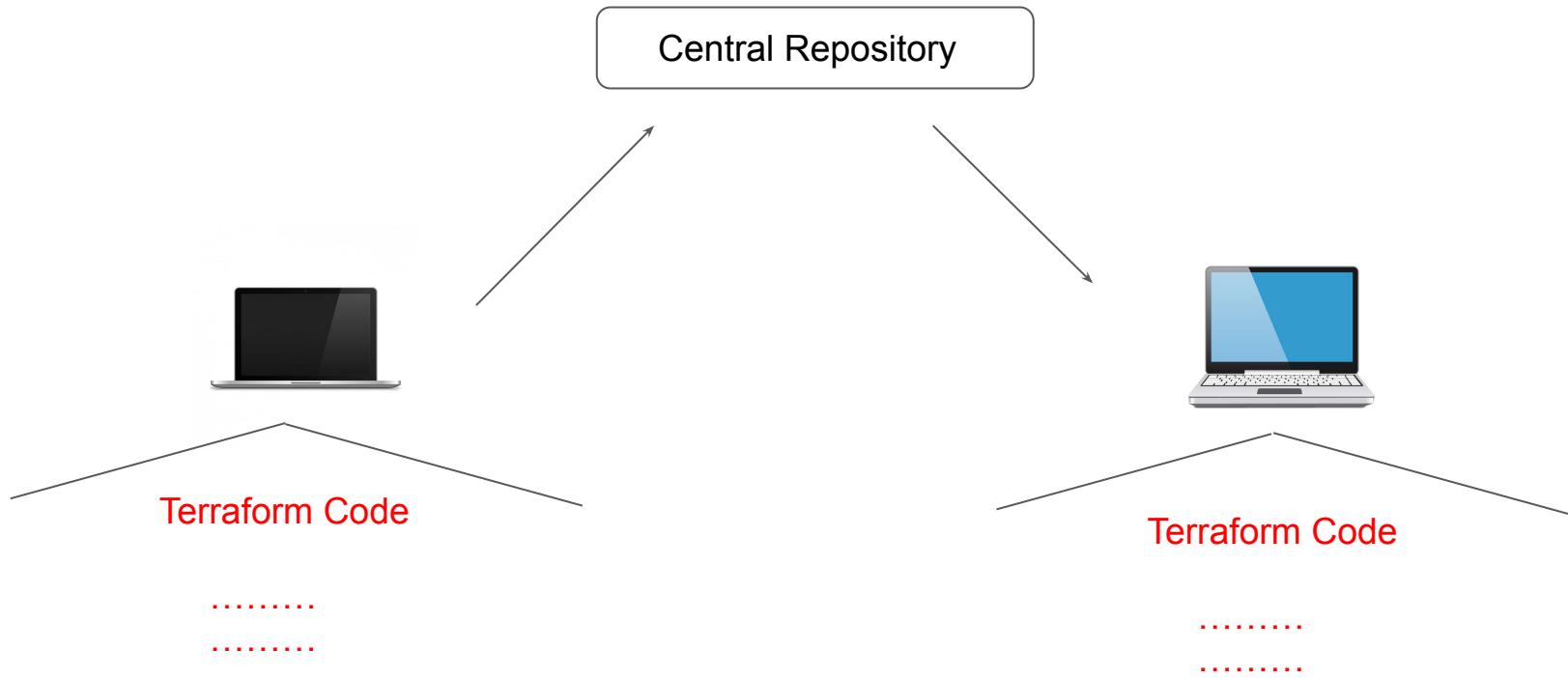
Currently we have been working with terraform code locally.



Terraform Code

.....  
.....

# Centralized Management



# Relax and Have a Meme Before Proceeding

me: i'll do it at 6

time: 6:05

me: wow looks like i gotta wait til 7 now



---

# Terraform & GitIgnore

Terraform in detail

---

# Overview of gitignore

The `.gitignore` file is a text file that tells Git which files or folders to ignore in a project.

|                          |
|--------------------------|
| <code>.gitignore</code>  |
| <code>conf/</code>       |
| <code>*.artifacts</code> |
| <code>credentials</code> |



# Terraform and .gitignore

Depending on the environments, it is recommended to avoid committing certain files to GIT.

| Files to Ignore   | Description                                                            |
|-------------------|------------------------------------------------------------------------|
| .terraform        | This file will be recreated when terraform init is run.                |
| terraform.tfvars  | Likely to contain sensitive data like usernames/passwords and secrets. |
| terraform.tfstate | Should be stored in the remote side.                                   |
| crash.log         | If terraform crashes, the logs are stored to a file named crash.log    |

---

# Terraform Backend

Terraform in detail

---

# Basics of Backends

Backends primarily determine where Terraform stores its state.

By default, Terraform implicitly uses a backend called local to store state as a local file on disk.

```
provider "vault" {
  address = "http://127.0.0.1:8200"
}

data "vault_generic_secret" "demo" {
  path = "secret/db_creds"
}

output "vault_secrets" {
  value = data.vault_generic_secret.demo.data_json
  sensitive = "true"
}
```

demo.tf



```
terraform.tfstate
1  {
2    "version": 4,
3    "terraform_version": "1.1.9",
4    "serial": 1,
5    "lineage": "f7ba581a-ab47-b03e-2e54-e683a2dc4ba2",
6    "outputs": {
7      "vault_secrets": {
8        "value": "{\"admin\":\"password123\"}",
9        "type": "string",
10       "sensitive": true
11     }
12   },
13   "resources": [
14     {
15       "mode": "data",
16       "type": "vault_generic_secret",
17       "name": "demo",
18       "provider": "provider[\"registry.terraform.io/hashicorp/vault\"]",
19       "instances": [

```

terrafrom.tfstate

# Challenge with Local Backend

Nowadays Terraform project is handled and collaborated by an entire team.

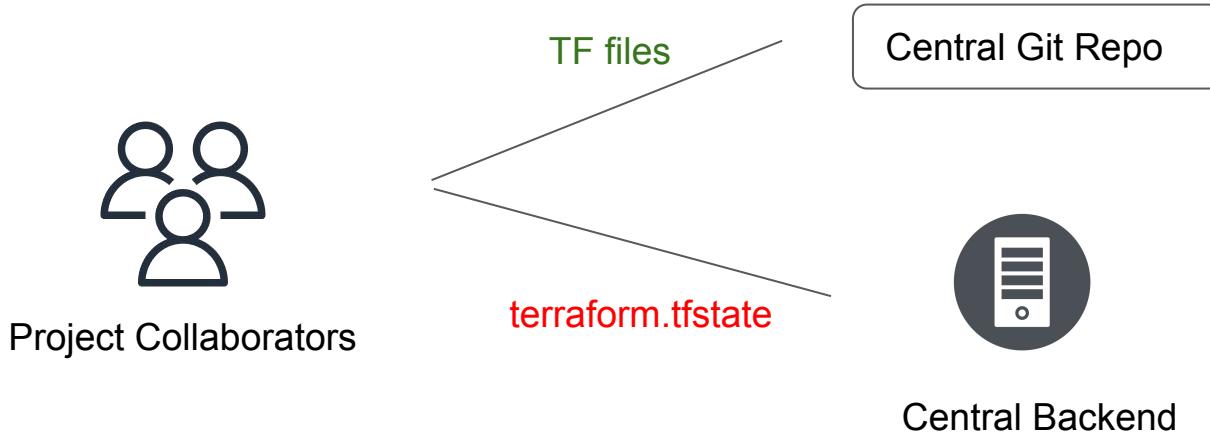
Storing the state file in the local laptop will not allow collaboration.



# Ideal Architecture

Following describes one of the recommended architectures:

1. The Terraform Code is stored in Git Repository.
2. The State file is stored in a Central backend.



# Backends Supported in Terraform

Terraform supports multiple backends that allows remote service related operations.

Some of the popular backends include:

- S3
- Consul
- Azurerm
- Kubernetes
- HTTP
- ETCD

# Important Note

Accessing state in a remote service generally requires some kind of access credentials

Some backends act like plain "remote disks" for state files; others support locking the state while operations are being performed, which helps prevent conflicts and inconsistencies.



---

# State Locking

Let's Lock the State

---

# Understanding State Lock

Whenever you are performing write operation, terraform would lock the state file.

This is very important as otherwise during your ongoing terraform apply operations, if others also try for the same, it can corrupt your state file.

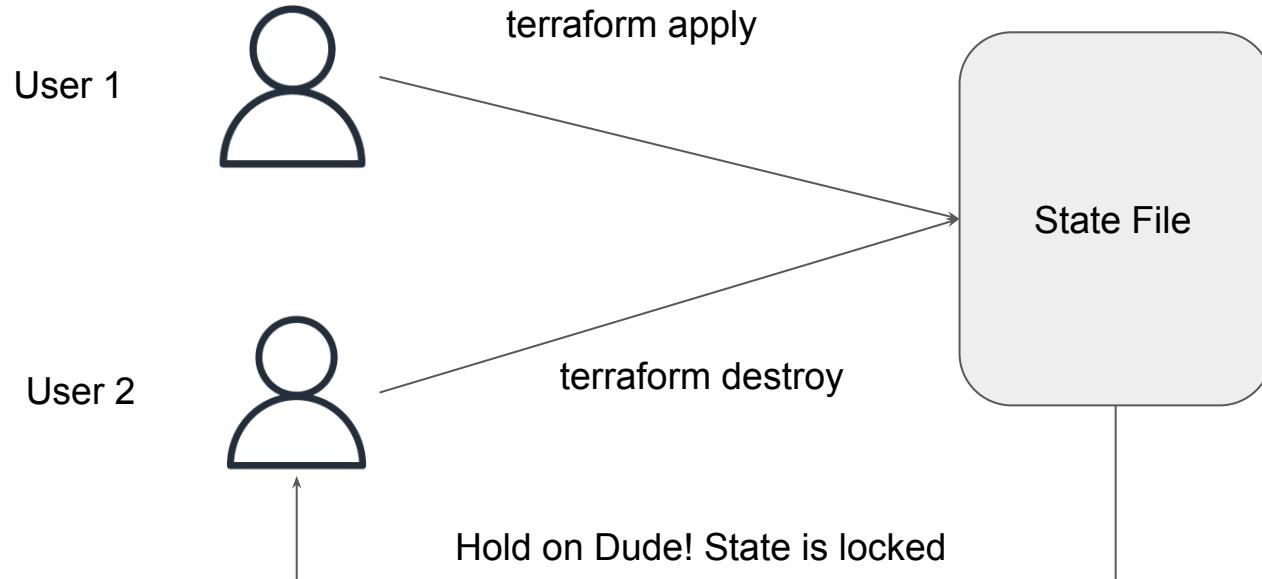
```
C:\Users\Zeal Vora\Desktop\tf-demo\remote-backend>terraform plan
```

```
Error: Error acquiring the state lock
```

```
Error message: Failed to read state file: The state file could not be read: read terraform.tfstate: The process  
cannot access the file because another process has locked a portion of the file.
```

```
Terraform acquires a state lock to protect the state from being written  
by multiple users at the same time. Please resolve the issue above and try  
again. For most commands, you can disable locking with the "-lock=false"  
flag, but this is not recommended.
```

# Basic Working



# Important Note

State locking happens automatically on all operations that could write state. You won't see any message that it is happening

If state locking fails, Terraform will not continue

Not all backends support locking. The documentation for each backend includes details on whether it supports locking or not.

# Force Unlocking State

Terraform has a [force-unlock](#) command to manually unlock the state if unlocking failed.

If you unlock the state when someone else is holding the lock it could cause multiple writers.

Force unlock should only be used to unlock your own lock in the situation where automatic unlocking failed.

---

# State Locking in S3 Backend

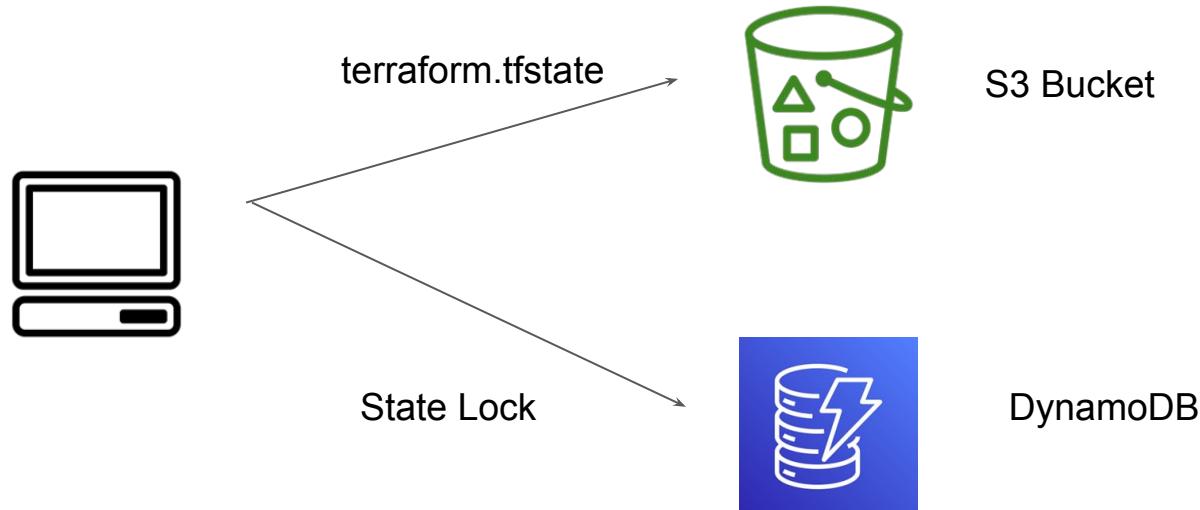
Back to Providers

---

# State Locking in S3

By default, S3 does not support State Locking functionality.

You need to make use of DynamoDB table to achieve state locking functionality.



# **Terraform State Management**

# Setting the Base

As your Terraform usage becomes more advanced, there are some cases where you may need to modify the Terraform state.

It is **NOT** recommended to modify the state file manually.



# State Management

The **terraform state** command is used for advanced state management

| Sub-Commands     | Description                                                      |
|------------------|------------------------------------------------------------------|
| list             | List resources within terraform state file.                      |
| mv               | Moves item with terraform state.                                 |
| pull             | Manually download and output the state from remote state.        |
| push             | Manually upload a local state file to remote state.              |
| rm               | Remove items from the Terraform state                            |
| show             | Show the attributes of a single resource in the state.           |
| replace-provider | Used to replace the provider for resources in a Terraform state. |

## Sub-Command 1 - List

The **terraform state list** command is used to list resources within a Terraform state.

Useful if you want to quickly view all resources managed by Terraform.

```
C:\kplabs-terraform>terraform state list
aws_iam_user.dev
aws_security_group.dev
```

## Sub-Command 2 - Show

The `terraform state show` command is used to show the attributes of a single resource in the state.

Useful for debugging and understanding the current attributes of a resource.

```
C:\kplabs-terraform>terraform state show aws_iam_user.dev
# aws_iam_user.dev:
resource "aws_iam_user" "dev" {
    arn                  = "arn:aws:iam::042025557788:user/kplabs-user-01"
    force_destroy        = false
    id                  = "kplabs-user-01"
    name                = "kplabs-user-01"
    path                = "/"
    permissions_boundary = null
    tags                = {}
    tags_all            = {}
    unique_id           = "AIDAQTSFLD4OALWEWB2AW"
}
```

# Sub-Command 3 - pull

The **terraform state pull** command is used to pull the state from a remote backend and output it to stdout.

Useful to view or backup the current state stored in a remote backend.

```
C:\kplabs-terraform>terraform state pull
{
    "version": 4,
    "terraform_version": "1.9.1",
    "serial": 6,
    "lineage": "78f3ac79-1cb9-e724-964b-37bb3dc649a8",
    "outputs": {},
    "resources": [
        {
            "mode": "managed",
            "type": "aws_iam_user",
            "name": "dev",
            "provider": "provider[\"registry.terraform.io/hashicorp/aws\"]",
            "instances": [
                {
                    "schema_version": 0,
                    "attributes": {
                        "arn": "arn:aws:iam::042025557788:user/kplabs-user-01",
                        "force_destroy": false,
                        "id": "kplabs-user-01",
                        "name": "kplabs-user-01",
                        "path": "/",
                        "permissions_boundary": ""
                    }
                }
            ]
        }
    ]
}
```

## Sub-Command 4 - rm

The `terraform state rm` command is used to remove items from the state.

Use this when you need to remove a resource from Terraform's state management without destroying it.

```
C:\kplabs-terraform>terraform state rm aws_security_group.dev
Removed aws_security_group.dev
Successfully removed 1 resource instance(s).
```

## Sub-Command 5 - mv

The **terraform state mv** command is used to move an item in the state to a different address.

```
C:\kplabs-terraform>terraform state mv aws_security_group.dev aws_security_group.prod
Move "aws_security_group.dev" to "aws_security_group.prod"
Successfully moved 1 object(s).
```

# Sub-Command 6 - replace-provider

The `terraform state replace-provider` command is used to replace the provider for resources in a Terraform state.

```
C:\kplabs-terraform>terraform state replace-provider hashicorp/local kplabs.in/internal/local
Terraform will perform the following actions:

  ~ Updating provider:
    - registry.terraform.io/hashicorp/local
    + kplabs.in/internal/local

Changing 1 resources:

  local_file.foo

Do you want to make these changes?
Only 'yes' will be accepted to continue.

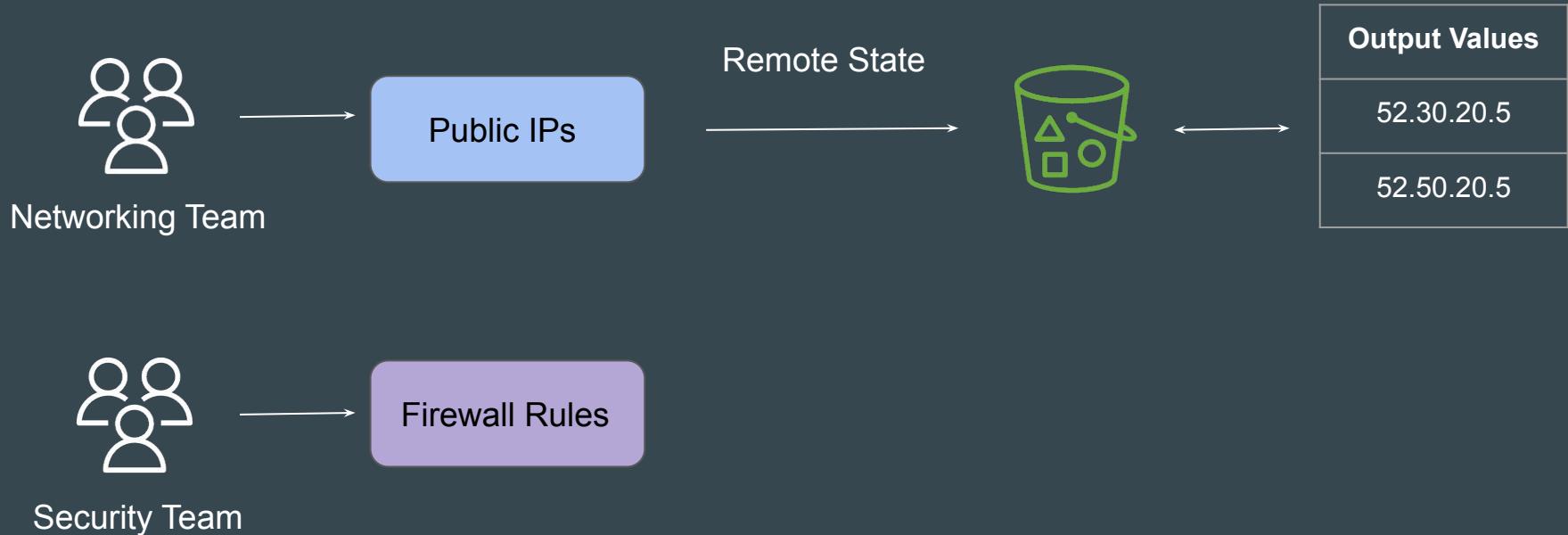
Enter a value: yes

Successfully replaced provider for 1 resources.
```

# **Remote State Data Source**

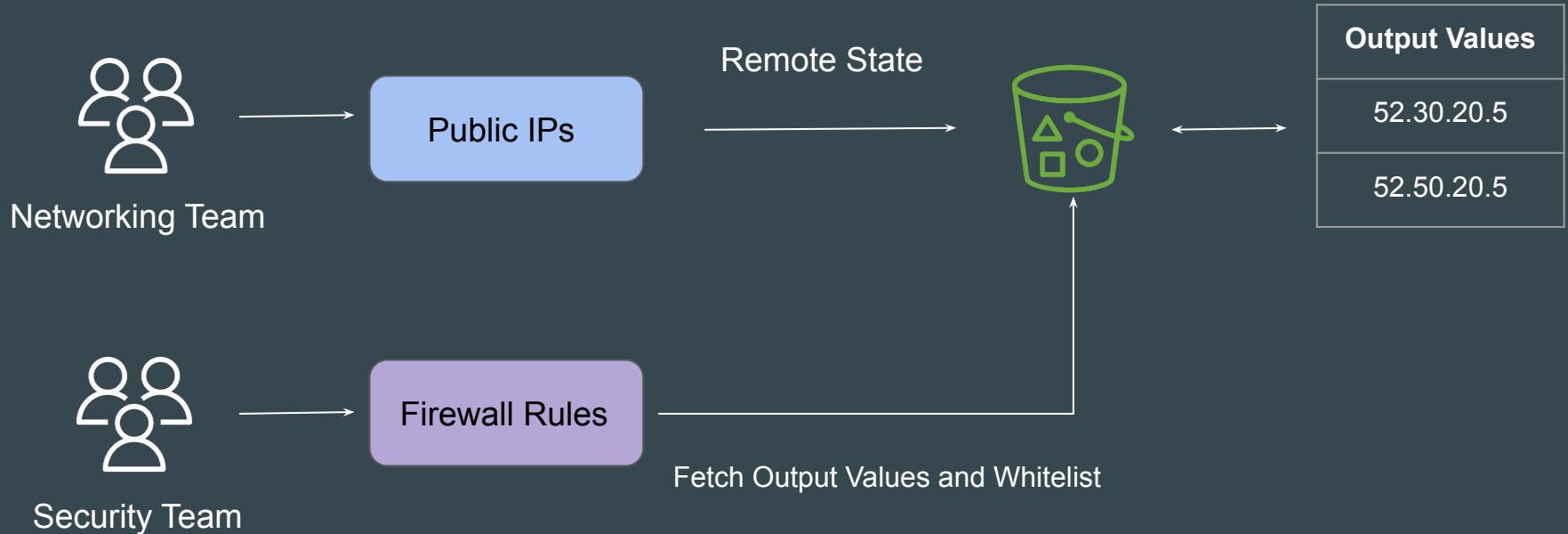
# Setting up the Base

In larger enterprises, there can be multiple different teams working on different aspects of a infrastructure resource



# Understanding the Challenge

Security Team wants that all the IP addresses added as part of Output Values in tfstate file of Networking Team project should be whitelisted in Firewall.



# What Needs to be Achieved

1. The code from Security Team project should connect to the `terraform.tfstate` file managed by the Networking team.
2. The code should fetch all the IP addresses mentioned in the output values in the state file.
3. The code should whitelist these IP addresses in Firewall rules.

# Practical Workflow Steps

1. Create two folders for networking-team and security-team
2. Create Elastic IP resource in Networking Team and Store the State file in S3 bucket. Output values should have information of EIP.
3. In Security Team, use Terraform Remote State data source to connect to the tfstate file of Networking Team.
4. Use the Remote State to fetch EIP and whitelist it in Security Group rule.

# Introducing Remote State Data Source

The `terraform_remote_state` data source allows us to fetch output values from a specific state backend

```
data "terraform_remote_state" "eip" {  
  backend = "s3"  
  config = {  
    bucket = "kplabs-team-networking-bucket"  
    key    = "eip.tfstate"  
    region = "us-east-1"  
  }  
}
```

```
resource "aws_vpc_security_group_ingress_rule" "allow_tls_ipv4" {  
  security_group_id = aws_security_group.allow_tls.id  
  cidr_ipv4        = "${data.terraform_remote_state.eip.outputs.eip_addr}/32"  
  from_port         = 443  
  ip_protocol       = "tcp"  
  to_port           = 443  
}
```

Step 1 - Define Remote State Source

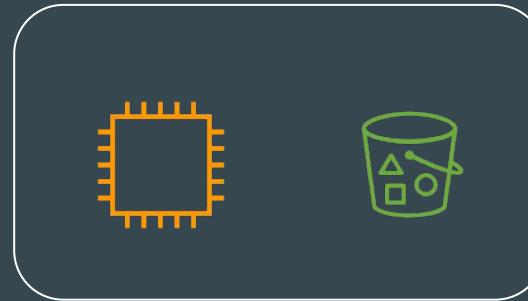
Step 2 - Define Data to Fetch

# **Terraform Import**

# Typical Challenge

It can happen that all the resources in an organization are created manually.

Organization now wants to start using Terraform and manage these resources via Terraform.

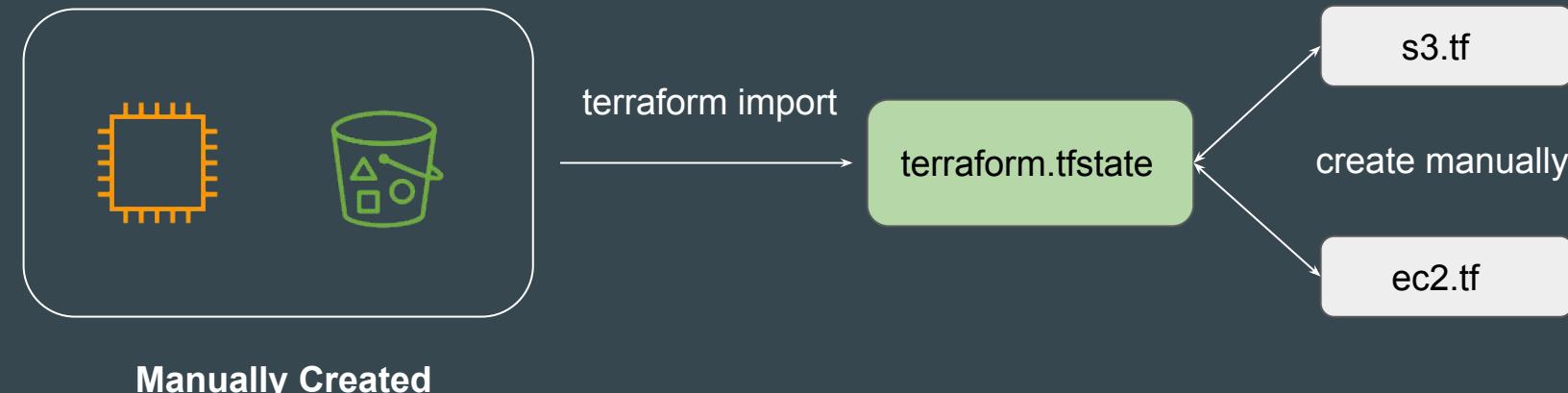


Manually Created

# Earlier Approach

In the older approach, Terraform import would create the state file associated with the resources running in your environment.

Users still had to write the tf files from scratch.



# Newer Approach

In the newer approach, **terraform import** can automatically create the terraform configuration files for the resources you want to import.



## Point to Note

Terraform 1.5 introduces automatic code generation for imported resources.

This dramatically reduces the amount of time you need to spend writing code to match the imported

This feature is not available in the older version of Terraform.

# **Multiple Provider Configuration**

# Understanding the Requirement

There can be multiple resource types in same project and you want to deploy them in different set of AWS regions.

```
resource "aws_instance" "myec2" {  
    ami           = "ami-08a0d1e16fc3f61ea"  
    instance_type = "t2.micro"  
}  
  
resource "aws_security_group" "allow_tls" {  
    name          = "staging_firewall"  
}
```



Singapore Region



Mumbai Region

# Setting the Base

At this stage, we have been dealing with single provider configuration.

In below code, both resources will be created in Singapore region.

```
provider "aws" {
    region = "ap-southeast-1"
}

resource "aws_instance" "myec2" {
    ami          = "ami-08a0d1e16fc3f61ea"
    instance_type = "t2.micro"
}

resource "aws_security_group" "allow_tls" {
    name        = "staging_firewall"
}
```

# Alias Meta-Argument

Each provider can have one default configuration, and **any number of alternate configurations** that include an extra name segment (or "alias").

```
resource "aws_instance" "myec2" {  
    ami           = "ami-08a0d1e16fc3f61ea"  
    instance_type = "t2.micro"  
}
```



```
provider "aws" {  
    region = "ap-southeast-1"  
}  
  
provider "aws" {  
    alias   = "mumbai"  
    region = "ap-south-1"  
}  
  
provider "aws" {  
    alias   = "usa"  
    region = "us-east-1"  
}
```



```
resource "aws_security_group" "allow_tls" {  
    name        = "staging_firewall"  
}
```

# Final Output Using Alias

By using the provider meta-argument, you can select an alternate provider configuration for a resource.

```
provider "aws" {
    region = "ap-southeast-1"
}

provider "aws" {
    alias  = "mumbai"
    region = "ap-south-1"
}

provider "aws" {
    alias = "usa"
    region = "us-east-1"
}
```

```
resource "aws_instance" "myec2" {
    provider = aws.mumbai
    ami       = "ami-08a0d1e16fc3f61ea"
    instance_type = "t2.micro"
}
```

```
resource "aws_security_group" "allow_tls" {
    provider    = aws.usa
    name        = "staging_firewall"
}
```

# **Sensitive Parameter**

# Setting the Base

By default, Terraform will show the values associated with defined attributes in the CLI output during plan, apply operations for most of the resources.

```
C:\kplabs-terraform>terraform plan

Terraform used the selected providers to generate the following execution plan.
following symbols:
+ create

Terraform will perform the following actions:

# local_file.foo will be created
+ resource "local_file" "foo" {
    + content              = "supersecretpassw0rd!"
    + content_base64sha256 = (known after apply)
    + content_base64sha512 = (known after apply)
    + content_md5          = (known after apply)
    + content_sha1          = (known after apply)
    + content_sha256         = (known after apply)
    + content_sha512         = (known after apply)
    + directory_permission   = "0777"
    + file_permission        = "0777"
    + filename               = "password.txt"
    + id                     = (known after apply)
}
```

# What to Expect

We should design our Terraform code in such way that no sensitive information is available and shown out of the box in CLI Output, Logs, etc.



# Basics of Sensitive Parameter

Adding sensitive parameter ensures that you do not accidentally expose this data in CLI output, log output

```
variable "sensitive_content" {
  sensitive = true
  default = "supersecretpassw0rd"
}

resource "local_file" "foo" {
  content  = var.sensitive_content
  filename = "password.txt"
}
```



```
Terraform will perform the following actions:

# local_file.foo will be created
+ resource "local_file" "foo" {
  + content          = (sensitive value)
  + content_base64sha256 = (known after apply)
  + content_base64sha512 = (known after apply)
  + content_md5      = (known after apply)
  + content_sha1     = (known after apply)
  + content_sha256   = (known after apply)
  + content_sha512   = (known after apply)
  + directory_permission = "0777"
  + file_permission   = "0777"
  + filename          = "password.txt"
  + id                = (known after apply)
}
```

# Sensitive Values AND Output Values

If you try to reference sensitive value in output values, Terraform will immediately give you an error.

```
variable "sensitive_content" {  
    sensitive = true  
    default = "supersecretpassw0rd"  
}  
  
resource "local_file" "foo" {  
    content = var.sensitive_content  
    filename = "password.txt"  
}  
  
output "content" {  
    value = local_file.foo.content  
}
```



Error: Output refers to sensitive values

on local\_file.tf line 12:  
12: output "content" {

To reduce the risk of accidentally exporting sensitive data that any root module output containing sensitive data be explicitly m

If you do intend to export this data, annotate the output value :  
sensitive = true

# Sensitive Values AND Output Values

If you still want sensitive content to be available in “output” of state file but should not be visible in CLI Output, Logs, following approach can be used.

```
variable "sensitive_content" {
  sensitive = true
  default   = "supersecretpassw0rd"
}

resource "local_file" "foo" {
  content  = var.sensitive_content
  filename = "password.txt"
}

output "content" {
  value = local_file.foo.content
  sensitive = "true"
}
```



```
Changes to Outputs:
+ content = (sensitive value)

You can apply this plan to save these new output values to the Terraform state

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

Outputs:

content = <sensitive>
```

# Important Point to Note

Sensitive parameter will NOT protect / redact information from State file.

```
variable "sensitive_content" {  
    sensitive = true  
    default = "supersecretpassw0rd"  
}  
  
resource "local_file" "foo" {  
    content  = var.sensitive_content  
    filename = "password.txt"  
}
```

Configuration File

```
...  
"resources": [  
    {  
        "mode": "managed",  
        "type": "local_file",  
        "name": "foo",  
        "provider": "provider[\\"registry.terraform.io/hashicorp/azurerm\"\"]",  
        "instances": [  
            {  
                "schema_version": 0,  
                "attributes": {  
                    "content": "supersecretpassw0rd",  
                    "content_base64": null,  
                    "content_base64sha256": "7Bj9buJUR+BnQAGN/nDad3...  
                }  
            }  
        ]  
    }  
]
```

State File

# Benefits of Mature Providers

Various providers like AWS will automatically consider the password argument for any database instance as sensitive and will redact it as a sensitive value

```
resource "aws_db_instance" "default" {  
    allocated_storage      = 10  
    db_name                = "mydb"  
    engine                 = "mysql"  
    engine_version         = "8.0"  
    instance_class          = "db.t3.micro"  
    username               = "foo"  
    password               = "foobarbaz"  
    parameter_group_name   = "default.mysql8.0"  
    skip_final_snapshot     = true  
}
```

```
C:\kplabs-terraform>terraform apply -auto-approve

Terraform will perform the following actions:

# aws_db_instance.default will be created
+ resource "aws_db_instance" "default" {
    + address                      = (known after apply)
    + allocated_storage              = 10
    + password                      = (sensitive value)
    + performance_insights_enabled = false
    + performance_insights_kms_key_id = (known after apply)
    + performance_insights_retention_period = (known after apply)
    + port                           = (known after apply)
```

---

# Overview of Vault

HashiCorp Certified: Vault Associate

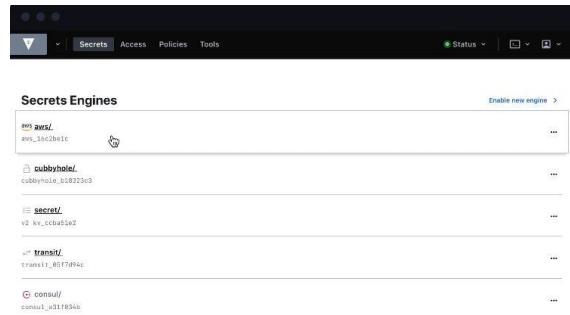
---

# Let's get started

HashiCorp Vault allows organizations to securely store secrets like tokens, passwords, certificates along with access management for protecting secrets.

One of the common challenges nowadays in an organization is “Secrets Management”

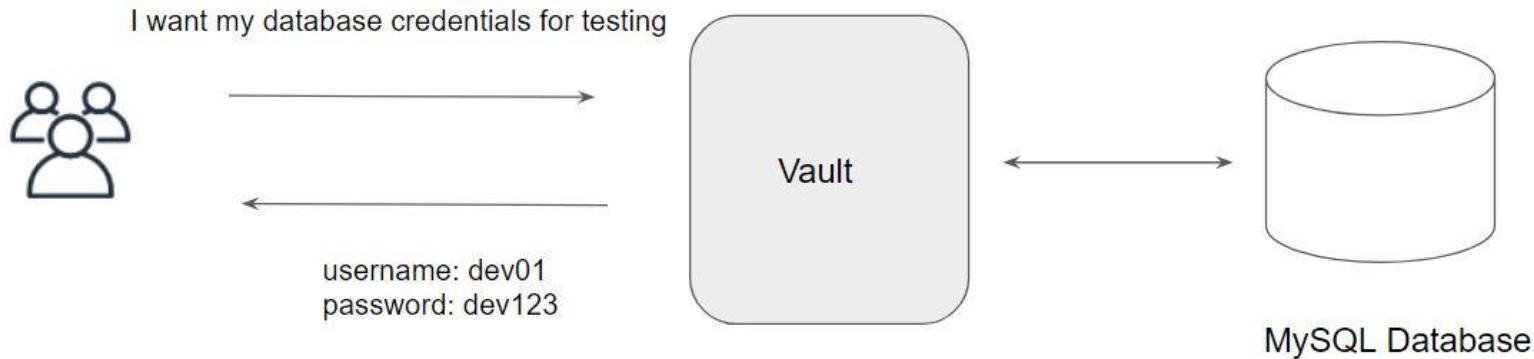
Secrets can include, database passwords, AWS access/secret keys, API Tokens, encryption keys and others.



The screenshot shows the HashiCorp Vault web interface. At the top, there is a navigation bar with tabs for "Secrets", "Access", "Policies", and "Tools". Below the navigation bar, the title "Secrets Engines" is displayed. A button "Enable new engine >" is located in the top right corner of the engine list. The list contains five entries, each with a small icon, the engine name, and a copy/paste link:

- aws/**  
aws\_16c2b0fc
- cubbyhole/**  
cubbyhole\_b1B31203
- secret/**  
v2\_kv\_cchab1e2
- transit/**  
transit\_85f7d94c
- consul/**  
consul\_a31fb34b

# Dynamic Secrets



# Life Becomes Easier

Once Vault is integrated with multiple backends, your life will become much easier and you can focus more on the right work.

Major aspect related to Access Management can be taken over by vault.



---

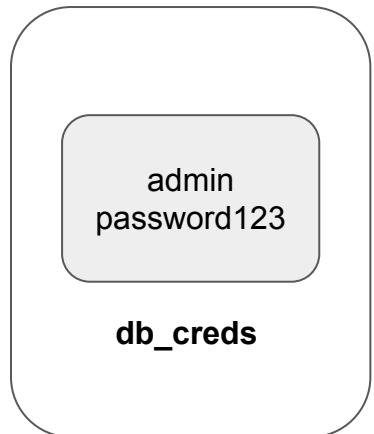
# Vault Provider

[Back to Providers](#)

---

# Vault Provider

The Vault provider allows Terraform to read from, write to, and configure HashiCorp Vault.



```
provider "vault" {
  address = "http://127.0.0.1:8200"
}

data "vault_generic_secret" "demo" {
  path = "secret/db-creds"
}
```

# Important Note

Interacting with Vault from Terraform causes any secrets that you read and write to be persisted in both Terraform's state file.

# **Dependency Lock File**

# Revising the Basics

Provider Plugins and Terraform are managed independently and have different release cycle.

AWS Plugin v1

AWS Plugin v2

AWS Plugin v3

Terraform v1.2

# Understanding the Challenge

The AWS code written in Terraform is working perfectly well with AWS Plugin v1

It can happen that same code might have some issues with newer AWS plugins.

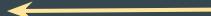


# Version Dependencies

Version constraints within the configuration itself determine which versions of dependencies are potentially compatible.

After selecting a specific version of each dependency Terraform remembers the decisions it made in a dependency lock file so that it can (by default) make the same decisions again in future.

```
≡ .terraform.lock.hcl
1 # This file is maintained automatically by "terraform init".
2 # Manual edits may be lost in future updates.
3
4 provider "registry.terraform.io/hashicorp/aws" {
5     version      = "4.62.0"
6     constraints = "~> 4.0"
7     hashes = [
8         "h1:TBu xeL RMrChr zgDhAyil3HITJhuNrL+X58QRC+FTmFQ=",
9         "zh:12059dc2b639797b9facb6397ac6aec563891634be8e5aadf3a4
10        "zh:1b3515d70b6998359d0a6d3b3c287940ab2e5c59cd02f95c7d9d
```



```
TY demo.tf •
TY demo.tf > ...
1  terraform {
2      required_providers {
3          aws = {
4              source  = "hashicorp/aws"
5              version = "~> 4.0"
6          }
7      }
8  }
9
10 # Configure the AWS Provider
11 provider "aws" {
12     region = "us-east-1"
13 }
```

# Default Behaviour

What happens if you update the TF file with version that does not match the `terraform.lock.hcl`?

```
↳ .terraform.lock.hcl
1  # This file is maintained automatically by "terraform init".
2  # Manual edits may be lost in future updates.
3
4 provider "registry.terraform.io/hashicorp/aws" {
5   version    = "4.62.0"
6   constraints = "~> 4.0"
7   hashes = [
8     "h1:TBu xeL RMr Chr zgDhAy il3HITJhuN rL+X58QRC+F TmFQ=",
9     "zh:12059dc2b639797b9facb6397ac6aec563891634be8e5aadf3a4
10    "zh:1b3515d70b6998359d0a6d3b3c287940ab2e5c59cd02f95c7d9d
```

```
demo.tf > ...
  terraform {
    required_providers {
      aws = {
        source  = "hashicorp/aws"
        version = "4.60"
      }
    }
  }

  # Configure the AWS Provider
  provider "aws" {
    region = "us-east-1"
  }
```

```
C:\Users\zealv\Desktop\kplabs-terraform>terraform init

Initializing the backend...

Initializing provider plugins...
- Reusing previous version of hashicorp/aws from the dependency lock file

Error: Failed to query available provider packages

Could not retrieve the list of available versions for provider hashicorp/aws: local configured version constraint 4.60.0; must use terraform init -upgrade to allow
```

# Upgrading Option

If there is a requirement to use newer or downgrade a provider, can override that behavior by adding the `-upgrade` option when you run `terraform init`, in which case Terraform will disregard the existing selections

```
C:\Users\zealv\Desktop\kplabs-terraform>terraform init -upgrade

Initializing the backend...

Initializing provider plugins...
- Finding hashicorp/aws versions matching "4.60.0"...
- Installing hashicorp/aws v4.60.0...
- Installed hashicorp/aws v4.60.0 (signed by HashiCorp)

Terraform has made some changes to the provider dependency selections recorded
in the .terraform.lock.hcl file. Review those changes and commit them to your
version control system if they represent changes you intended to make.
```

# Points to Note

When installing a particular provider for the first time, Terraform will pre-populate the hashes value with any checksums that are covered by the provider developer's cryptographic signature, which usually covers all of the available packages for that provider version across all supported platforms.

```
≡ .terraform.lock.hcl
  # This file is maintained automatically by "terraform init".
  # Manual edits may be lost in future updates.

  provider "registry.terraform.io/hashicorp/aws" {
    version      = "4.60.0"
    constraints = "4.60.0"
    hashes = [
      "h1:M90xusbiz/HW7zF+jLddXqdpzsFZ38Fa2S+Yaquad2g=",
      "zh:1853d6bc89e289ac36c13485e8ff877c1be8485e22f545bb32c7a30f1d1856e8",
      "zh:4321d145969e3b7ede62fe51bee248a15fe398643f21df9541eef85526bf3641",
      "zh:4c01189cc6963abfe724e6b289a7c06d2de9c395011d8d54efa8fe1aac444e2e",
      "zh:5934db7baa2eec0f9acb9c7f1c3dd3b3fe1e67e23dd4a49e9fe327832967b32b",
```

## Points to Note

At present, the dependency lock file tracks only provider dependencies.

Terraform does not remember version selections for remote modules, and so Terraform will always select the newest available module version that meets the specified version constraints.

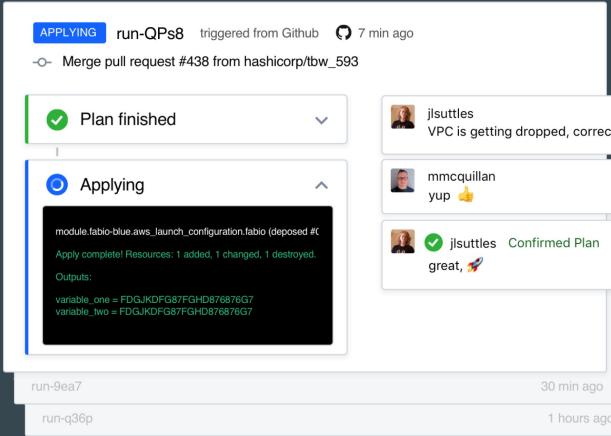
# **HashiCorp Cloud Platform - Terraform**

# Setting the Base

Till now, we have been managing Terraform through CLI

Although this approach is decent, we should also be aware that there is a GUI based offering that is available.

```
root@test-kplabs:~# terraform plan
2024-08-24T05:01:48.844Z [INFO]  Terraform version: 1.9.5
2024-08-24T05:01:48.845Z [DEBUG] using github.com/hashicorp/go-tfe v1.58.0
2024-08-24T05:01:48.845Z [DEBUG] using github.com/hashicorp/hcl/v2 v2.20.0
2024-08-24T05:01:48.845Z [DEBUG] using github.com/hashicorp/terraform-svchost v0.1.1
2024-08-24T05:01:48.845Z [DEBUG] using github.com/zclconf/go-cty v1.14.4
2024-08-24T05:01:48.845Z [INFO] Go runtime version: go1.22.5
2024-08-24T05:01:48.845Z [INFO] CLI args: []string{"terraform", "plan"}
2024-08-24T05:01:48.845Z [TRACE] Stdout is a terminal of width 125
2024-08-24T05:01:48.845Z [TRACE] Stderr is a terminal of width 125
2024-08-24T05:01:48.845Z [TRACE] Stdin is a terminal
2024-08-24T05:01:48.845Z [DEBUG] Attempting to open CLI config file: /root/.terraformrc
2024-08-24T05:01:48.845Z [DEBUG] File doesn't exist, but doesn't need to. Ignoring.
2024-08-24T05:01:48.845Z [DEBUG] ignoring non-existing provider search directory /root/.terraform.d/plugins
2024-08-24T05:01:48.845Z [DEBUG] ignoring non-existing provider search directory /root/.local/share/terraform/plugins
2024-08-24T05:01:48.846Z [DEBUG] ignoring non-existing provider search directory /usr/local/share/terraform/plugins
2024-08-24T05:01:48.846Z [DEBUG] ignoring non-existing provider search directory /usr/share/terraform/plugins
2024-08-24T05:01:48.846Z [DEBUG] ignoring non-existing provider search directory /var/lib/snapd/desktop/terraform/plugins
2024-08-24T05:01:48.848Z [INFO] CLI command args: []string{"plan"}
```



# HCP Terraform

HCP Terraform manages Terraform runs in a consistent and reliable environment with various features like access controls, private registry for sharing modules, policy controls and others.

The screenshot shows the HCP Terraform interface. At the top, it displays a message from 'mykplabs' that triggered a run from the UI a few seconds ago. Below this, the 'Run Details' section shows a green checkmark indicating the 'Plan finished' status a few seconds ago. It also shows 'Resources: 1 to add, 0 to change, 0 to destroy'. A prominent green bar indicates '+ 1 to create'. The interface includes filters for resources by address and action, and links to download raw logs and sentinel mocks. In the bottom section, a green checkmark indicates the 'Cost estimation finished' status a few seconds ago. It shows 'Resources: 1 of 1 estimated · \$8.35/mo · +\$8.35'. A table provides detailed cost information for an 'aws\_instance' named 'myec2':

| RESOURCE       | NAME  | HOURLY COST | MONTHLY COST | MONTHLY DELTA |
|----------------|-------|-------------|--------------|---------------|
| ✓ aws_instance | myec2 | \$0.012     | \$8.352      | +\$8.352      |

# Not Everything is Free

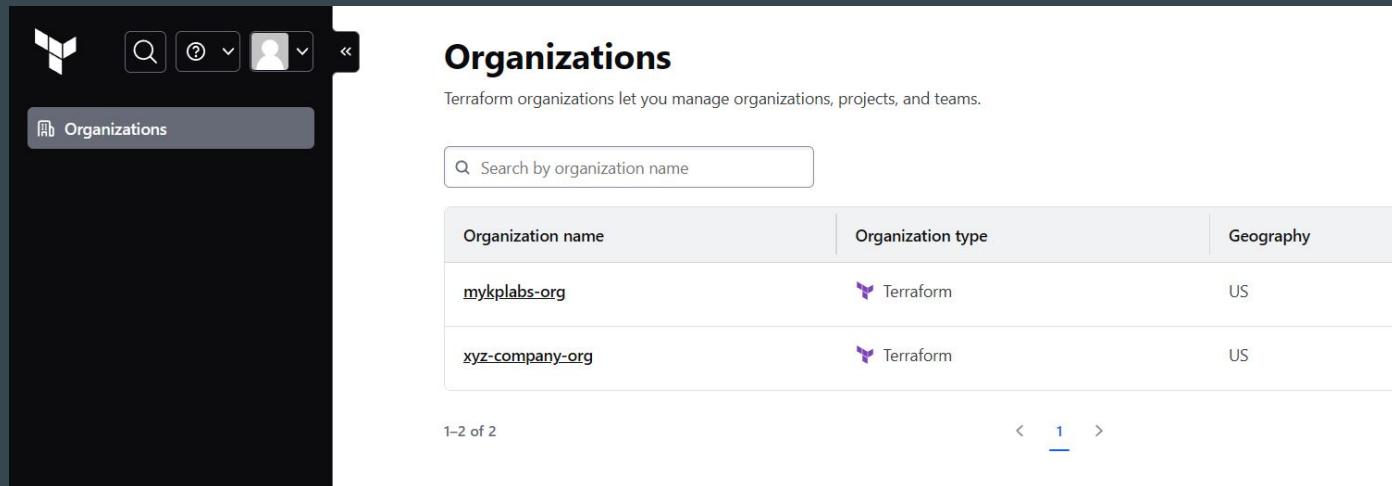
HCP Terraform is not entirely free. Depending on the usage and features needed, there are multiple pricing plans that are available.

| Terraform pricing                                                                                                     |                                                                                                                             |                                                                                                                                                 |                                                                                                                                            |
|-----------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| Free                                                                                                                  | Standard                                                                                                                    | Plus                                                                                                                                            | Enterprise                                                                                                                                 |
| UP TO<br><b>500 resources</b><br>per month                                                                            | STARTING AT<br><b>\$0.00014</b><br>per hour per resource                                                                    | Custom                                                                                                                                          | Custom                                                                                                                                     |
| Cloud<br>Get started with all capabilities needed for infrastructure as code provisioning.<br>No credit card required | Cloud<br>For professional individuals or teams adopting infrastructure as code provisioning.<br>Enterprise support included | Cloud<br>For enterprises standardizing and managing infrastructure automation and lifecycle, with scalable runs.<br>Enterprise support included | Self-managed<br>For enterprises with special security, compliance, and additional operational requirements.<br>Enterprise support included |
| <a href="#">Start for free</a>                                                                                        | <a href="#">Start for free</a>                                                                                              | <a href="#">Contact sales</a>                                                                                                                   | <a href="#">Contact sales</a>                                                                                                              |

# **HCP Terraform - Basic Structure**

# 1 - Organizations

Organizations are a shared space for one or more teams to collaborate on workspaces.



The screenshot shows the Terraform Cloud interface with the 'Organizations' page selected. The top navigation bar includes a logo, search, help, and user icons. A sidebar on the left has a 'Organizations' button. The main content area is titled 'Organizations' and contains a sub-header: 'Terraform organizations let you manage organizations, projects, and teams.' Below this is a search bar labeled 'Search by organization name'. A table lists two organizations:

| Organization name               | Organization type | Geography |
|---------------------------------|-------------------|-----------|
| <a href="#">mykplabs-org</a>    | Terraform         | US        |
| <a href="#">xyz-company-org</a> | Terraform         | US        |

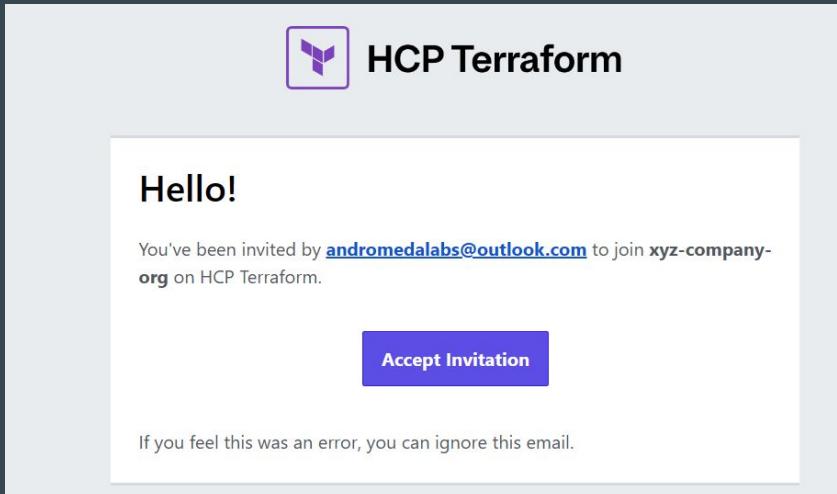
At the bottom, it shows '1-2 of 2' and a page number '1'.

| Organization name               | Organization type | Geography |
|---------------------------------|-------------------|-----------|
| <a href="#">mykplabs-org</a>    | Terraform         | US        |
| <a href="#">xyz-company-org</a> | Terraform         | US        |

# Points to Note - Organizations

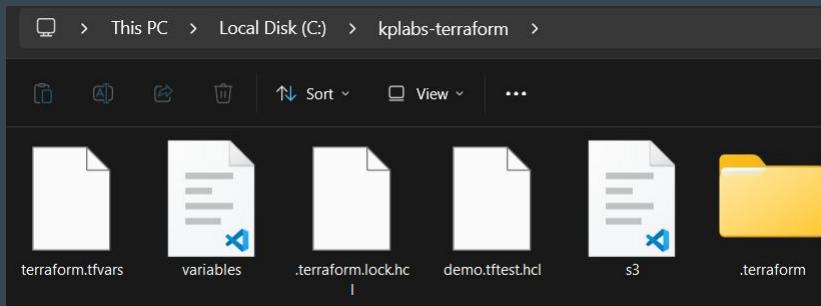
HCP Terraform manages plans and billing at the organization level.

Each HCP Terraform user can belong to multiple organizations, which might subscribe to different billing plans.



# 2 - Workspace

HCP Terraform manages infrastructure collections with workspaces instead of directories

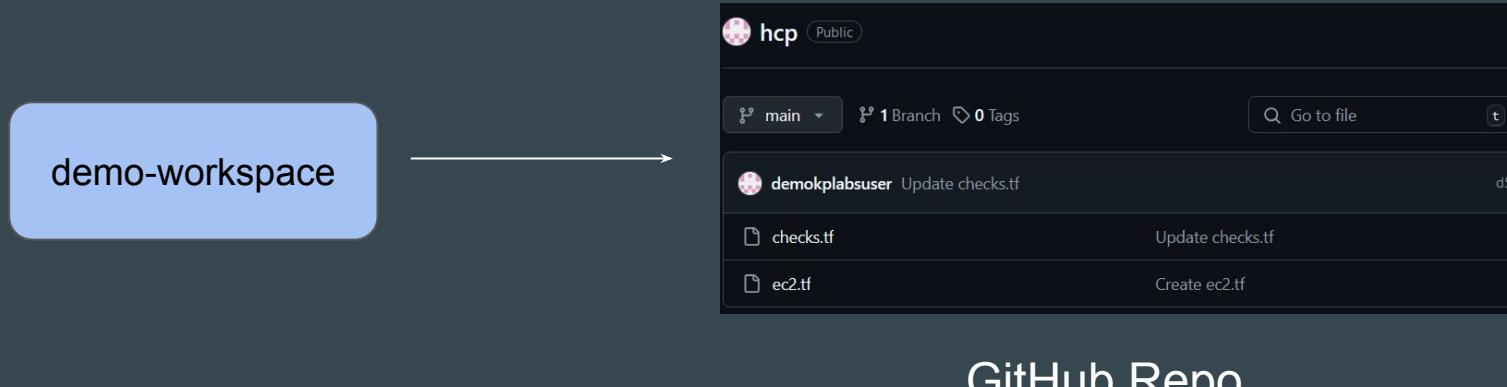


A screenshot of the HashiCorp Cloud Platform (HCP) workspace interface. The workspace is named 'hcp' with ID 'ws-SfMu8aw7NnmPzx2F'. It shows 'Running', 'Resources 1', 'Terraform v1.9.5', and 'Updated an hour ago'. The 'Latest Run' section shows a run triggered via UI by 'mykplabs' an hour ago. It details policy checks ('Add'), estimated cost increase ('\$0.35'), plan duration ('Less than a minute'), and resources to be changed ('+1 ~0 -0'). The 'Metrics' section shows the last 2 runs. On the right, there are configuration options: 'Execution mode: Remote', 'Auto-apply API, CLI, & VCS runs: Off', 'Auto-apply run triggers: Off', 'Auto-destroy: Off', and 'Project: kplabs-workspace'.

# Workspace & Configuration Files

The Terraform configuration file (sample.tf) is not directly uploaded to a workspace.

Instead, workspace is connected to GitHub repository where it can fetch code from.



# Workspace vs Directories

| Component               | Local Terraform                                                          | HCP Terraform                                                              |
|-------------------------|--------------------------------------------------------------------------|----------------------------------------------------------------------------|
| Terraform configuration | On disk                                                                  | In linked version control repository, or periodically uploaded via API/CLI |
| Variable values         | As <code>.tfvars</code> files, as CLI arguments, or in shell environment | In workspace                                                               |
| State                   | On disk or in remote backend                                             | In workspace                                                               |
| Credentials and secrets | In shell environment or entered at prompts                               | In workspace, stored as sensitive variables                                |

# 3 - Projects

HCP Terraform projects let you organize your workspaces into groups.

 **security-team-project** New ▾

ID: prj-QN8iVccxZ7ML2eE1 

[Add project description](#)

 Teams 0  Workspaces 3

| Workspace name                                                                                                                          | Repository | Health | Latest change     |
|-----------------------------------------------------------------------------------------------------------------------------------------|------------|--------|-------------------|
|  <a href="#">azure-hardening</a><br>No status reported | None       | None   | a few seconds ago |
|  <a href="#">gcp-hardening</a><br>No status reported   | None       | None   | a few seconds ago |
|  <a href="#">aws-hardening</a><br>No status reported   | None       | None   | a minute ago      |

## Point to Note - Projects

You can structure your projects based on your organization's resource usage and ownership patterns, such as teams, business units, or services.

With HCP Terraform Standard Edition, you can give teams access to groups of workspaces using projects.

# **The CLI-driven Run Workflow**

# Setting the Base

Whenever we create a new Workspace in HCP, following are the 3 types of workflow modes that are available.

The screenshot shows a web-based interface for creating a new workspace. At the top, the URL is 'mykplabs-org / Workspaces / New Workspace'. The main title is 'Create a new Workspace'. Below it, a descriptive text states: 'HCP Terraform organizes your infrastructure resources by workspaces. A workspace contains infrastructure resources, variables, state data, and run history. Learn more about workspaces in HCP Terraform.' A section titled 'Choose your workflow' presents three options:

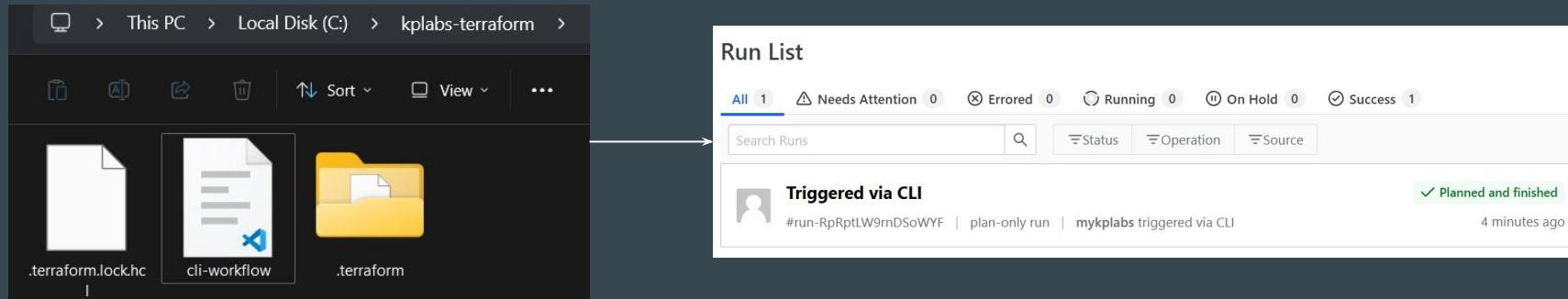
- Version Control Workflow**: Trigger runs based on changes to configuration in repositories. Best for those who need traceability and transparency.
- CLI-Driven Workflow**: Trigger runs in a workspace using the Terraform CLI. Best for those comfortable with Terraform CLI.
- API-Driven Workflow**: Trigger runs using the HCP Terraform API. Best for those with custom integrations and pipelines.

A 'Cancel' button is located at the bottom right of the form.

# Basics of CLI Driven Workflow

In this approach, the working directory on your workstation is linked with HCP Workspace.

The code file can be present in your laptop, and plan/apply operations can also be initiated from local workstation.



# **The CLI-driven Run Workflow - Practical**

# Setting the Base

Whenever we create a new Workspace in HCP, following are the 3 types of workflow modes that are available.

The screenshot shows a web-based interface for creating a new workspace. At the top, the URL is "mykplabs-org / Workspaces / New Workspace". The main title is "Create a new Workspace". Below it, a descriptive text states: "HCP Terraform organizes your infrastructure resources by workspaces. A workspace contains infrastructure resources, variables, state data, and run history. Learn more about workspaces in HCP Terraform." A section titled "Choose your workflow" presents three options:

- Version Control Workflow**: Trigger runs based on changes to configuration in repositories. Best for those who need traceability and transparency.
- CLI-Driven Workflow**: Trigger runs in a workspace using the Terraform CLI. Best for those comfortable with Terraform CLI.
- API-Driven Workflow**: Trigger runs using the HCP Terraform API. Best for those with custom integrations and pipelines.

A "Cancel" button is located at the bottom right of the form.

# Step 1 - Setup Cloud Integration

You have to add code block within your .tf file to setup cloud integration.

This code will contain details about your HCP organization and workspace name.

```
terraform {
  cloud {

    organization = "mykplabs-org"

    workspaces {
      name = "remote-operation-workspace"
    }
  }
}
```

## Step 2 - Terraform Login

Once your cloud integration code block has been added, next step is to run the **terraform login** command.

```
C:\kplabs-terraform>terraform login
Terraform will request an API token for app.terraform.io using your browser.
```

```
If login is successful, Terraform will store the token in plain text in
the following file for use by subsequent commands:
```

```
C:\Users\zealv\AppData\Roaming\terraform.d\credentials.tfrc.json
```

```
Do you want to proceed?
```

```
Only 'yes' will be accepted to confirm.
```

```
Enter a value: yes
```

---

```
Terraform must now open a web browser to the tokens page for app.terraform.io.
```

```
If a browser does not open this automatically, open the following URL to proceed:
```

```
https://app.terraform.io/app/settings/tokens?source=terraform-login
```

# Step 3 - Initialize

Run the `terraform init` command to initialize

```
C:\kplabs-terraform>terraform init
Initializing HCP Terraform...
Initializing provider plugins...
- Finding latest version of hashicorp/aws...
- Installing hashicorp/aws v5.70.0...
- Installed hashicorp/aws v5.70.0 (signed by HashiCorp)
Terraform has made some changes to the provider dependency selections recorded
in the .terraform.lock.hcl file. Review those changes and commit them to your
version control system if they represent changes you intended to make.
```

HCP Terraform has been successfully initialized!

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

If you ever set or change modules or Terraform Settings, run "terraform init"
again to reinitialize your working directory.

# Step 4 - Run the Plan / Apply Operations

Once initialized, the terraform “plan”, and “apply” commands when entered through CLI will run in HCP Terraform with output streamlined in terminal.

```
C:\kplabs-terraform>terraform plan
Running plan in HCP Terraform. Output will stream here. Pressing Ctrl-C
will stop streaming the logs, but will not stop the plan running remotely.

Preparing the remote plan...

To view this run in a browser, visit:
https://app.terraform.io/app/mykplabs-org/remote-operation-workspace/runs/run-RpRptLW9rnDSoWYF

Waiting for the plan to start...

Terraform v1.9.7
on linux_amd64
Initializing plugins and modules...

Terraform used the selected providers to generate the following execution plan. Resource actions
following symbols:
+ create
```

---

# Sentinel

Terraform Cloud In Detail

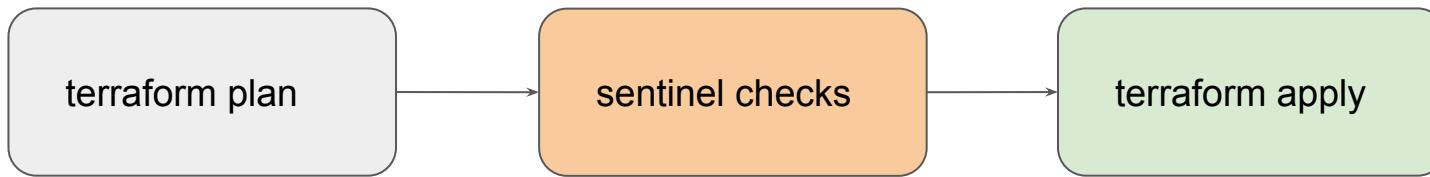
---

# Overview of the Sentinel

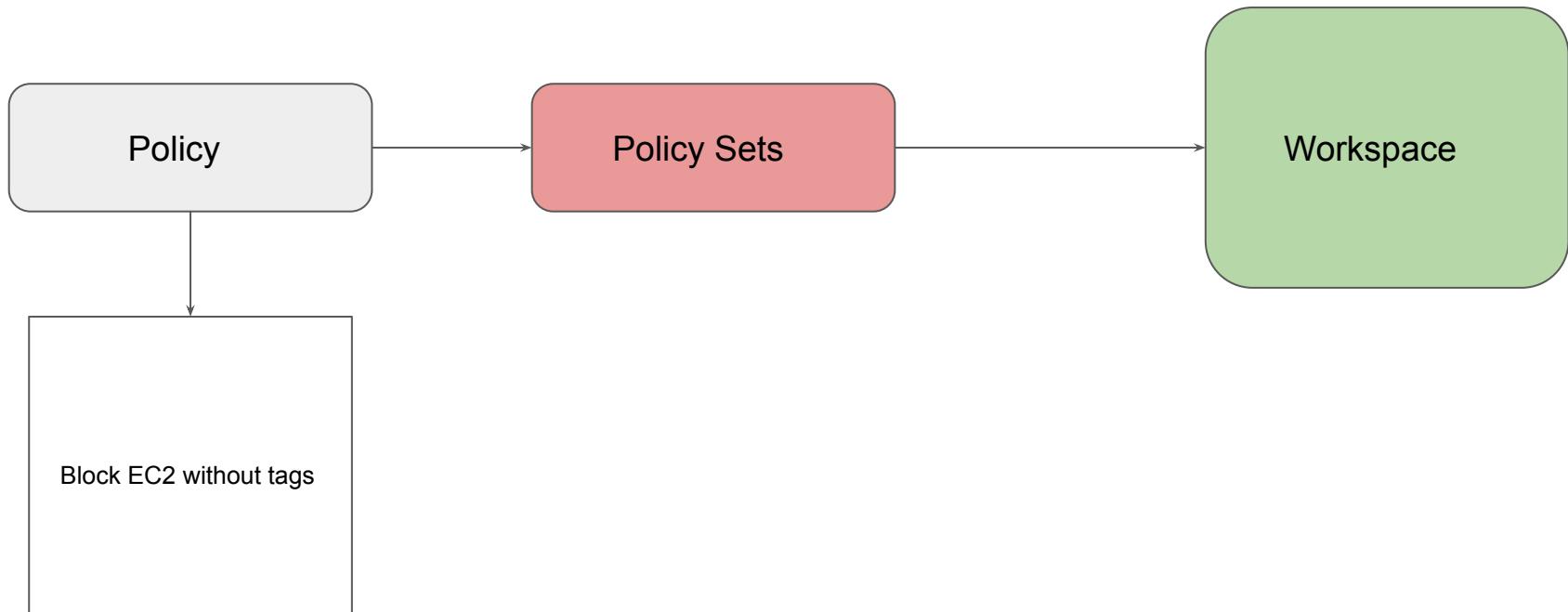
Sentinel is a policy-as-code framework integrated with the HashiCorp Enterprise products.

It enables fine-grained, logic-based policy decisions, and can be extended to use information from external sources.

Note: Sentinel policies are paid feature



# High Level Structure



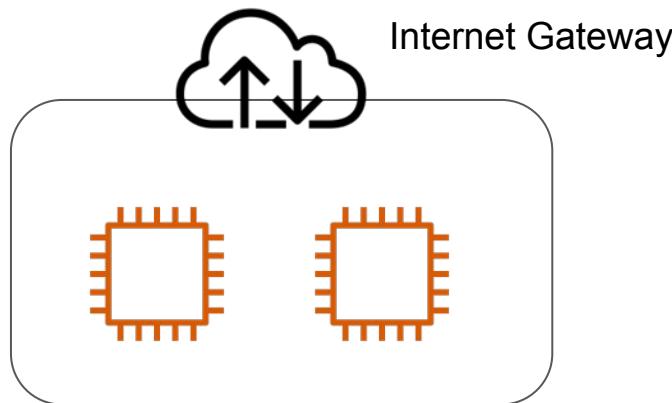
---

# Air Gapped Environments

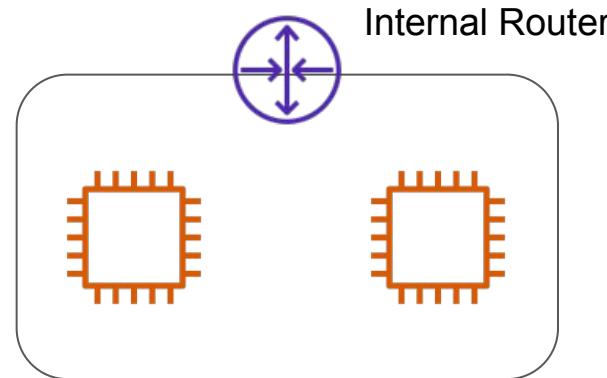
## Installation Methods

# Understanding Concept of Air Gap

An air gap is a network security measure employed to ensure that a secure computer network is physically isolated from unsecured networks, such as the public Internet.



Internet Connectivity



Air Gapped System

# Usage of Air Gapped Systems

Air Gapped Environments are used in various areas. Some of these include:

- Military/governmental computer networks/systems
- Financial computer systems, such as stock exchanges
- Industrial control systems, such as SCADA in Oil & Gas fields

# Terraform Enterprise Installation Methods

Terraform Enterprise installs using either an online or air gapped method and as the names infer, one requires internet connectivity, the other does not

| WORKSPACE NAME   | RUN STATUS           | LATEST CHANGE | RUN      | REPO                          |
|------------------|----------------------|---------------|----------|-------------------------------|
| exceed-limit     | ✓ APPLIED            | 5 months ago  | run-B8Ac | NICKF/terraform-minimum       |
| filetest-dev     | ✗ ERRORED            | 3 months ago  | run-SLSz | nfagerlund/terraform-filetest |
| migrated-default | ✓ PLANNED            | 5 months ago  | run-BVjy | nfagerlund/terraform-minimum  |
| migrated-first   | ✓ PLANNED            | 5 months ago  | run-A2sp | nfagerlund/terraform-minimum  |
| migrated-second  | ✓ PLANNED            | 5 months ago  | run-KqNV | nfagerlund/terraform-minimum  |
| migrated-solo    | ✓ APPLIED            | 5 months ago  | run-1RkX | NICKF/terraform-minimum       |
| migrated-solo2   | ✓ PLANNED            | 5 months ago  | run-Rih7 | nfagerlund/terraform-minimum  |
| migrate-first-2  | ! NEEDS CONFIRMATION | 3 months ago  | run-hR57 | nfagerlund/terraform-minimum  |

Terraform Enterprise

Air Gap Install



Isolated Server

## Choose your installation type



Online



Airgapped

Please choose an installation type to continue.

[Continue »](#)

## Provide path or upload airgap bundle

Provide absolute path on this server to archive file

e.g. ./mnt/installers/package.airgap

Continue »

Select file for upload

Upload Airgap Bundle

To upload an app bundle, file must have a `.airgap` extension.

« Back

# Relax and Have a Meme Before Proceeding



Cole  
@its\_cmillz6

when you're sleeping and your alarm  
didn't ring yet but the amount of  
sleep you're getting is suspicious



# Terraform Challenges

# Key Observations

At this stage, we have been learning core concepts of Terraform step by step.

Whenever learning a new technology, small set of practical projects are always useful to grasp the practical aspects of a technology.



# Introducing Terraform Challenges

With Terraform Challenges, we aim to reduce the gap between learning and gaining practical experience.

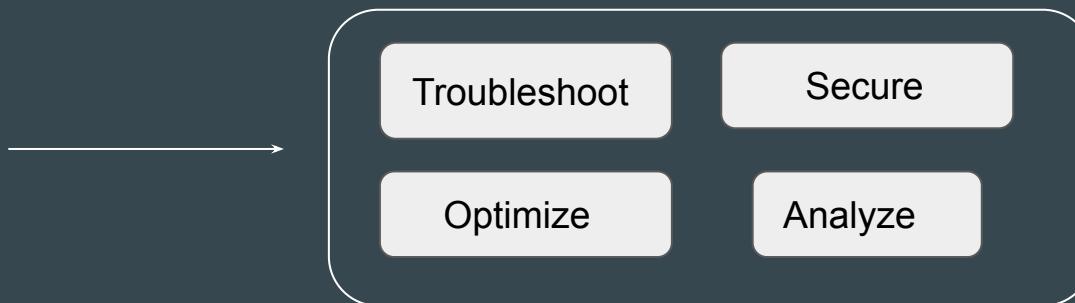


# About the Challenges

Each Challenge will test you in different areas of Terraform that will help you gain some kind of hands-on experience.



Awesome Students



Terraform

# Workflow Steps

We will have multiple sets of challenges.

After each challenge video, we will have a **Solution Hints** video and then the **Practical Solution** video.



# Terraform Challenge 1

# Understanding the Challenge

A Developer at Sample Small Corp had created a Terraform File for creating certain resources.

The code was written a few years back based on the old Terraform version.

```
provider "aws" {
    version = "~> 2.54"
    region  = "us-east-1"
    access_key = "AKIAIOSFODNN7EXAMPLE"
    secret_key = "wJalrXUtnFEMI/K7MDENG/bPxRfICYEXAMPLEKEY"
}

provider "digitalocean" {}

terraform {
    required_version = "0.12.31"
}

resource "aws_eip" "kplabs_app_ip" {
    vpc      = true
}
```

# What you need to do?

1. Create Infrastructure using the provided code (without modifications).
2. Verify if the code works in the latest version of Terraform and Provider .
3. Modify and Fix the code so that it works with latest version of Terraform.
4. Feel free to edit the code as you like.

# **TF Challenge 1 - Solution Discussion and Hints**

# Hint 1 - Create Infrastructure with Base Code

Based on the initial code given to you, use appropriate version of binaries to ensure infrastructure gets created successfully.

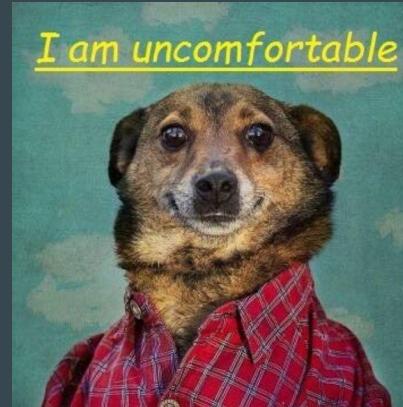
```
terraform_0.12.31
terraform_0.12.30
terraform_0.12.29
terraform_0.12.28
terraform_0.12.27
terraform_0.12.26
terraform_0.12.25
terraform_0.12.24
terraform_0.12.23
terraform_0.12.22
```

## Hint 2 - Access/Secret Keys

There are hardcoded AWS Access/Secret keys with the code.

This MUST be be fixed.

```
provider "aws" {
  version = "~> 2.54"
  region  = "us-east-1"
  access_key = "AKIAIOSFODNN7EXAMPLE"
  secret_key = "wJalrXutnFEMI/K7MDENG/bPxRfCYEXAMPLEKEY"
}
```



## Hint 3 - Provider Block

Provider Block is used to define provider version along with 3rd party providers.

Instead, use the new required\_provider block to define provider and constraints.

```
provider "aws" {  
    version = "~> 2.54"  
    region  = "us-east-1"  
    access_key = "AKIAIOSFODNN7EXAMPLE"  
    secret_key = "wJalrXutnFEMI/K7MDENG/t  
}  
  
provider "digitalocean" {}
```

```
terraform {  
    required_providers {  
        mycloud = {  
            source  = "mycorp/mycloud"  
            version = "~> 1.0"  
        }  
    }  
}
```

## Hint 4 - Terraform Core Version Requirement

Since the challenge states that latest version of Terraform should be used, you can plan to remove the required\_version block from the code.

```
terraform {  
    required_version = "0.12.31"  
}
```

## Hint 5 - Code Upgrade

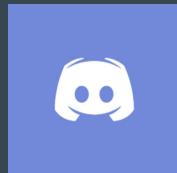
Does the resource block of “aws\_eip” work with the latest version of Terraform?

It can happen that latest AWS provider requires some changes in the aws\_eip resource block. Incorporate these changes to ensure EIP gets created.

```
resource "aws_eip" "kplabs_app_ip" {  
    vpc      = true  
}
```

# Join us in our Adventure

Be Awesome



[kplabs.in/chat](https://kplabs.in/chat)



[kplabs.in/linkedin](https://kplabs.in/linkedin)

# Terraform Challenge 2

# Understanding the Challenge

A sample code has been provided to you that creates certain resources.

You are required to optimize the code following the Best Practices.

```
resource "aws_security_group" "security_group_payment_app" {
    name          = "payment_app"
    description   = "Application Security Group"
    depends_on    = [aws_eip.example]

    # Below ingress allows HTTPS from DEV VPC
    ingress {
        from_port      = 443
        to_port        = 443
        protocol       = "tcp"
        cidr_blocks   = ["172.31.0.0/16"]
    }

    # Below ingress allows APIs access from DEV VPC

    ingress {
        from_port      = 8080
        to_port        = 8080
    }
}
```

# Conditions to Meet

1. Ensure the code is working and resource gets created.
2. Do NOT delete the existing `terraform.lock.hcl` file. File is free to be modified based on requirements.
3. Demonstrate ability to modify variable “splunk” from 8088 to 8089 without modifying the Terraform code.

# **TF Challenge 2 - Solution Discussion and Hints**

# Hint 1 - Indentation

Indentation issues are present in the code.

Make sure that code is properly indented.

```
# Below ingress allows HTTPS from DEV VPC
ingress {
    from_port      = 443
    to_port        = 443
    protocol       = "tcp"
    cidr_blocks   = ["172.31.0.0/16"]
}
```

## Hint 2 - Using Variables and TFVars

Many values are hard-coded as part of the code.

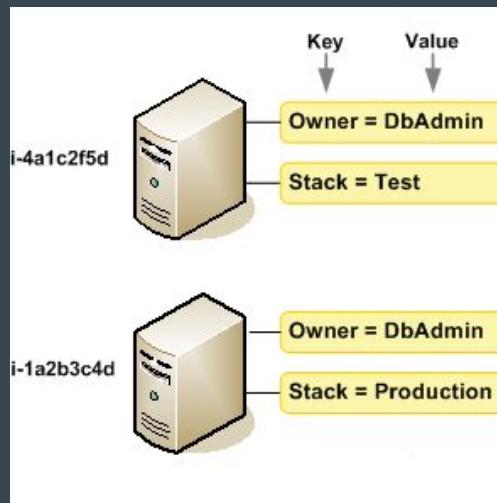
This makes it difficult to modify if code base becomes larger.

```
# Below ingress allows HTTPS from DEV VPC
ingress {
    from_port      = 443
    to_port        = 443
    protocol       = "tcp"
    cidr_blocks    = ["172.31.0.0/16"]
}
```

## Hint 3 - Using Tags

It is important that resources are properly tagged

This will make it easier to identify the resource among all others.



## Hint 4 - Variable Precedence

Consider using appropriate variable precedence to override variables from Terraform code.

## Hint 5 - Right Folder Structure

Having right naming convention for files is important.

Bad Structure: Everything in one single file named main.tf

Good Structure: providers.tf , variables.tf , ec2.tf and so on.

# **Terraform Challenge 3**

# Understanding the Requirements

You will be provided with a variable named `instance_config`

The variable type is map.

```
variable "instance_config" {
  type = map
  default = {
    instance1 = { instance_type = "t2.micro", ami = "ami-03a6eaae9938c858c" }
    instance2 = { instance_type = "t2.micro", ami = "ami-053b0d53c279acc90" }
  }
}
```

# Conditions to Meet

1. Based on the values specified in map, EC2 instances should be created accordingly.
2. If key/value is removed from map, EC2 instances should be destroyed accordingly.

# **TF Challenge 3 - Hints**

# Hint 1 - Loops

The requirement indicates that based on key/value specified in map, the resources should be created and destroyed accordingly.

We need to use some kind of loops to achieve this.

```
variable "instance_config" {  
  type = map  
  default = {  
    instance1 = { instance_type = "t2.micro", ami = "ami-03a6eaae9938c858c" }  
    instance2 = { instance_type = "t2.micro", ami = "ami-053b0d53c279acc90" }  
  }  
}
```

## Hint 2 - for\_each

If a resource block includes a `for_each` argument whose value is a **map** or a **set** of strings, Terraform creates one instance for each member of that map or set.

# **Terraform Challenge 4**

# Requirement - 1

Clients wants a code that can create IAM user in AWS account with following syntax:

admin-user-{account-number-of-aws}



## Requirement - 2

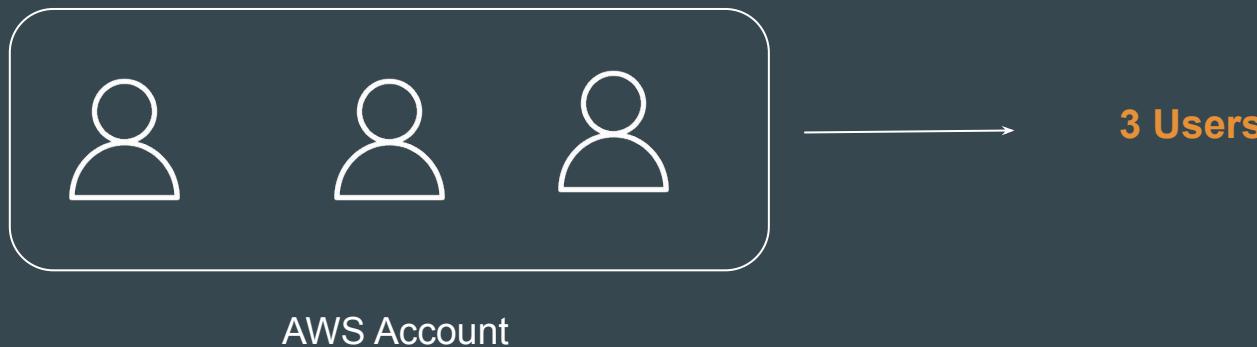
Client wants to have a logic that will show names of ALL users in AWS account in the output.



```
+ users      = [  
+ "Ankit",  
+ "DemoUser",  
+ "cloudformation-user",  
+ "demo-user",  
+ "kplabs-demo-user",  
+ "terraform",  
]
```

## Requirement - 3

Along with list of users in AWS, client also wants Terraform to show Total number of users in AWS.



# **TF Challenge 4 - Solution Hints**

## Hint 1 - Data Sources

Data Sources allows us to dynamically fetch information from the infrastructure resource or other state backends.

You can try to dynamically fetch information like AWS Account ID, User names using Data Sources.

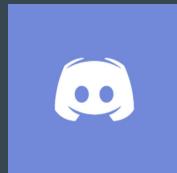
## Hint 2 - Functions

To calculate number of users is outside scope of Data Source.

You need to make use of Terraform Function that can calculate total number of users and output it.

# Join us in our Adventure

Be Awesome



[kplabs.in/chat](https://kplabs.in/chat)



[kplabs.in/linkedin](https://kplabs.in/linkedin)

---

# Overview of HashiCorp Exams

Let's Get Certified!

# Overview of HashiCorp Associate Exams

Overview of the basic exam related information.

| <b>Assessment Type</b> | <b>Description</b> |
|------------------------|--------------------|
| Type of Exams          | Multiple Choice    |
| Format                 | Online Proctored   |
| Duration               | 1 hour             |
| Questions              | 57                 |
| Price                  | 70.50 USD + Taxes  |
| Language               | English            |
| Expiration             | 2 years            |

# Multiple Choice

This includes various sub-formats, including:

- True or False
- Multiple Choice
- Fill in the blank

# Delta Type of Question

Example 1:

Demo Software stores information in which type of backend?



# Format - Online Proctored

## Important Rules to be followed:

- You are alone in the room
- Your desk and work area are clear
- You are connected to a power source
- No phones or headphones
- No dual monitors
- No leaving your seat
- No talking
- Webcam, speakers, and microphone must remain on throughout the test.
- The proctor must be able to see you for the duration of the test.

# My Experience - Before Room



# My Experience - After Room



# My Experience - My Desk

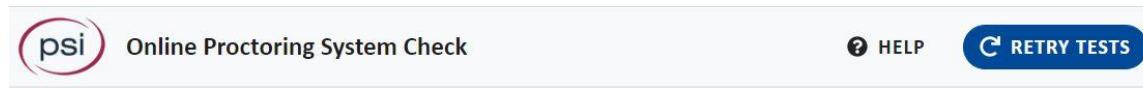


# Registration Process

The high-level steps for registering for the exams are as follows:

1. Login to the HashiCorp Certification Page.
2. Register for Exams.
3. Check System Requirements
4. Download PSI Software
5. Best of Luck & Good Luck!

# Make sure to complete system check.



The link below will install the PSI Secure Browser, complete a system check, and perform your check-in steps. This should be done at least 24 hours before your scheduled appointment to avoid possible forfeiture of exam fees due to issues with the test taker's system.

 [Download PSI Secure Browser](#)

NOTE: Please be sure to run this test on the computer that you intend to use for your exam. If you change computers for any reason, be sure to re-run this check on the computer that you will be using before taking the exam.

# Registration Process

 Online Exam

HashiCorp Certified: Consul Associate - Scheduled for Test

|                                   |                                |                                     |                                                                                                                                                                                                                                                  |                                                                                                                 |
|-----------------------------------|--------------------------------|-------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|
| EXAM DATE:<br><b>Nov 24, 2020</b> | START TIME:<br><b>05:30 PM</b> | EXAM DURATION:<br><b>60 minutes</b> | <ul style="list-style-type: none"><li>Before taking your remote online proctored exam, please check system compatibility - click <a href="#">HERE</a></li><li>You can only launch the exam within 30 minutes of your appointment time.</li></ul> | You may launch your test in...<br><b>3 Hours</b><br><a href="#">Launch Exam</a><br><a href="#">View Details</a> |
|-----------------------------------|--------------------------------|-------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|

# Registration Process

Please Select Camera and Microphone

**Cameras**

| Camera Description               | Select One                       |
|----------------------------------|----------------------------------|
| USB2.0 UVC HD Webcam (13d3:5654) | <input checked="" type="radio"/> |
| HD Pro Webcam C920 (046d:082d)   | <input type="radio"/>            |
| Logi Capture                     | <input type="radio"/>            |



**Microphones**

| Microphone Description                      | Select One                       |
|---------------------------------------------|----------------------------------|
| Microphone (HD Pro Webcam C920) (046d:082d) | <input checked="" type="radio"/> |
| Microphone (Realtek High Definition Audio)  | <input type="radio"/>            |

**QUIT** **CONTINUE**

# Registration Process

Please Test Your Microphone

Please say the following sentence out loud:

**"I am testing the volume on my microphone"**



Is your microphone working? Please speak now.

QUIT

# Registration Process

## Photo ID Capture

Please take a picture of a current Photo ID.

- It must be a current, non-expired, government-issued identification.
- Military IDs are not currently accepted.

### 💡 Photo Tips

1. Position the FRONT of your ID card in the center of the frame so that all of the corners are visible.
2. Make sure that your photo is clear.
3. Make sure that all of the text can be read.
4. When you are ready, press the camera button.



CC

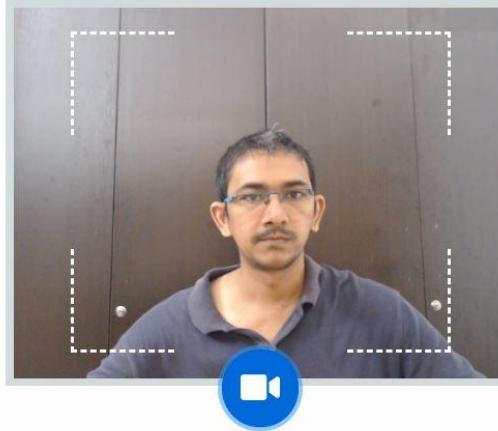
# Registration Process

## Scan Your Room and Workspace

Click the blue camera button and take a video of all four walls around your desk and your immediate workspace showing that you have no prohibited items within your reach. Click the red STOP button when you are done. Then, click CONTINUE.

### 💡 Scanning Requirements

1. Room Scan should be slow and thorough.
- 2. Conduct a 360-degree scan all the way around the room.**
3. Slowly scan from the ceiling to the floor.
- 4. Scan the entire desk/work-space area.**
5. Scan the area directly underneath where you will be placing laptop and/or keyboard.
6. After your laptop or keyboard is in place, show your cell phone to the camera and place it directly behind your seat and out of reach.
7. Roll up any sleeves and show both sides of arms up to the camera.
8. Show your ears to ensure there are no earbuds in use.
9. If wearing glasses, hold them up to the camera for visual inspection.



[CONTINUE >](#)

# **Exam Preparation - Part 1**

# Providers in AWS

A provider is responsible for understanding API interactions and exposing resources.

When we run `terraform init`, plugins required for the provider are automatically downloaded and saved locally to a `.terraform` directory.

```
C:\Users\zealv\Desktop\kplabs-terraform>terraform init

Initializing the backend...

Initializing provider plugins...
- Finding latest version of hashicorp/aws...
- Installing hashicorp/aws v4.60.0...
- Installed hashicorp/aws v4.60.0 (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
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.
```

# Interesting Question

Is provider block {..} mandatory to be added as part of your Terraform configuration? Yes/No

```
provider "aws" {
    region = "us-east-1"
}
```

# Two Pointers from Documentation

All Terraform configurations **must** declare which providers they require so that Terraform can install and use them.

A provider block may be omitted if its contents would otherwise be empty.

# Concluding this Question

If you plan to explicitly add some contents to provider {} like region, credentials, then defining this block is required.

Otherwise, even if you skip, the terraform apply will work fine.

```
demo.tf ●  
demo.tf > ...  
  
resource "aws_security_group" "sg_01" {  
    name = "app_firewall"  
}
```

# Alias in Providers

**alias** can be used for using the same provider with different configurations for different resources

```
provider "aws" {
    region = "ap-southeast-1"
}

provider "aws" {
    alias  = "mumbai"
    region = "ap-south-1"
}

provider "aws" {
    alias = "usa"
    region = "us-east-1"
}
```

```
resource "aws_instance" "myec2" {
    provider = aws.mumbai
    ami       = "ami-08a0d1e16fc3f61ea"
    instance_type = "t2.micro"
}
```



```
resource "aws_security_group" "allow_tls" {
    provider    = aws.usa
    name        = "staging_firewall"
}
```

## Point to Note - Providers

It is a good practice to store the credentials outside of Terraform configuration, such as in Environment Variables.

# Terraform Settings

Terraform Settings are used to configure project-specific Terraform behaviours, such as requiring a minimum Terraform version to apply to your configuration.

```
terraform {  
    required_version = "2.0"  
  
    required_providers {  
        aws = {  
            version = "5.54.1"  
            source  = "hashicorp/aws"  
        }  
    }  
}
```

## Options That Can be Defined

Required Terraform Version

Required Provider and Version

BackEnd Configuration

Experimental Features

## Point to Note

You cannot define configuration related to regions, Access/Secret keys inside required\_provider block.

For these, you have to use a provider {} block.

# Versioning Constraint

Version Constraint allows you to specify mix of multiple operators to select a suitable version of Terraform and Provider Plugins.

| Operators and Examples | Description                       |
|------------------------|-----------------------------------|
| >=1.0                  | Greater than equal to the version |
| <=1.0                  | Less than equal to the version    |
| ~>2.0                  | Any version in the 2.X range.     |
| >=2.10,<=2.30          | Any version between 2.10 and 2.30 |

# Provider Tiers

There are 3 primary type of provider tiers in Terraform.

| Provider Tiers | Description                                                                                  |
|----------------|----------------------------------------------------------------------------------------------|
| Official       | Owned and Maintained by HashiCorp.                                                           |
| Partner        | Owned and Maintained by Technology Company that maintains direct partnership with HashiCorp. |
| Community      | Owned and Maintained by Individual Contributors.                                             |

# Terraform Init

The `terraform init` command initializes a working directory.

Initialization includes Installing Provider Plugins, Backend initialization, Copy Source Module, etc.

This is the first command that should be run after writing a new Terraform configuration. It is safe to run multiple times.

```
C:\Users\zealv\Desktop\kplabs-terraform>terraform init

Initializing the backend...

Initializing provider plugins...
- Finding latest version of hashicorp/aws...
- Installing hashicorp/aws v4.60.0...
- Installed hashicorp/aws v4.60.0 (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
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.
```

# Terraform Init Upgrade

The `terraform init -upgrade` installs the latest module and provider versions allowed within configured constraints.

If you have latest provider plugins installed and if you define new version constraints that matches different version, you will have to run the `init -upgrade`

```
C:\kplabs-terraform>terraform plan

Error: Inconsistent dependency lock file

The following dependency selections recorded in the lock file are inconsistent with the current configuration:
  - provider registry.terraform.io/hashicorp/aws: locked version selection 5.54.1 doesn't match the updated version
    int "5.50.1"

To update the locked dependency selections to match a changed configuration, run:
  terraform init -upgrade
```

# Terraform Plan

The **terraform plan** command is used to create an execution plan.

The infrastructure is not modified as part of this plan.

The **state file is not modified** even when it detects drift in real-world and current infrastructure.

```
C:\kplabs-terraform>terraform plan

Terraform used the selected providers to generate the following
following symbols:
+ create

Terraform will perform the following actions:

# aws_security_group.sg_01 will be created
+ resource "aws_security_group" "sg_01" {
    + arn                  = (known after apply)
    + description          = "Managed by Terraform"
    + egress               = (known after apply)
    + id                   = (known after apply)
    + ingress              = (known after apply)
    + name                 = "app_firewall"
    + name_prefix          = (known after apply)
    + owner_id              = (known after apply)
```

# Saving Plan to File

You can use the optional `-out=FILE` option to save the generated plan to a file on disk, which you can later execute by passing the file to `terraform apply` as an extra argument.

This ensures consistent infrastructure as defined in the plan.

```
terraform plan -out ec2.plan
```



```
Saved the plan to: ec2.plan
```

```
To perform exactly these actions, run the following command to apply:  
  terraform apply "ec2.plan"
```

# Terraform Apply

**terraform apply** command is used to apply the changes required to reach the desired state of the configuration.

The state file gets modified in this command.

Name of state file = `terraform.tfstate`

Terraform Apply can change, destroy and provision resources but cannot import any resource.

# Terraform Destroy

`terraform destroy` command is used to destroy the Terraform-managed infrastructure.

`terraform destroy` command is not the only command through which infrastructure can be destroyed.

# Terraform Format

`terraform fmt` command is used to rewrite Terraform configuration files to a canonical format and style. It will directly perform “write” operation and not “read”

For use-case, where the all configuration written by team members needs to have a proper style of code, `terraform fmt` can be used.

```
resource "aws_instance" "myec2" {  
    ami = "ami-00c39f71452c08778"  
    instance_type = "t2.micro"  
    tags = {  
        Name = "test-ec2"  
    }  
}
```

Before

```
resource "aws_instance" "myec2" {  
    ami           = "ami-00c39f71452c08778"  
    instance_type = "t2.micro"  
    tags = {  
        Name = "test-ec2"  
    }  
}
```

After

# terraform fmt options

You have to keep a note of two important flags for terraform fmt command

| Command    | Description                                                                                                     |
|------------|-----------------------------------------------------------------------------------------------------------------|
| -check     | Check if the input is formatted. Files are not modified.                                                        |
| -recursive | Also process files in subdirectories. By default, only the given directory (or current directory) is processed. |

# **Exam Preparation - Part 2**

# Terraform Validate

`terraform validate` command validates the configuration files in a directory.

Requires an initialized working directory with any referenced plugins and modules installed.

`terraform plan` uses implied validation check.

```
C:\kplabs-terraform>terraform validate  
Success! The configuration is valid.
```

# Terraform Refresh

`terraform refresh` command reads the current settings from all managed remote objects and updates the Terraform state to match.

This won't modify your real remote objects, but it will modify the Terraform state.

This command is deprecated, because its default behavior is unsafe.

# Resource Blocks

A resource block declares a resource of a **given type** ("aws\_instance") with a **given local name** ("web").

Resource type and Name together serve as an identifier for a given resource and so must be unique.

Address of the following resource is: aws\_instance.web

```
resource "aws_instance" "web" {
    ami          = ami-123
    instance_type = "t2.micro"
}
```

# Important Terminology

```
resource "aws_instance" "myec2" {  
    ami          = "ami-123"  
    instance_type = "t2.micro"  
}
```



|              |                             |
|--------------|-----------------------------|
| aws_instance | Resource Type               |
| myec2        | Local name for the resource |
| ami          | Argument Name               |
| ami-123      | Argument value              |

# Data Types in Terraform

| Data Types | Description                                                                           |
|------------|---------------------------------------------------------------------------------------|
| string     | a sequence of Unicode characters representing some text, like "hello".                |
| number     | A Numeric value                                                                       |
| bool       | a boolean value, either true or false                                                 |
| list       | a sequence of values, like ["us-west-1a", "us-west-1c"]                               |
| set        | a collection of unique values that do not have any secondary identifiers or ordering. |
| map        | a group of values identified by named labels, like {name = "Mabel", age = 52}.        |
| null       | a value that represents absence or omission.                                          |

# Point to Note - Data Types

Array data types are not supported in Terraform

# State Management

The **terraform state** command is used for advanced state management

| Sub-Commands     | Description                                                      |
|------------------|------------------------------------------------------------------|
| list             | List resources within terraform state file.                      |
| mv               | Moves item with terraform state.                                 |
| pull             | Manually download and output the state from remote state.        |
| push             | Manually upload a local state file to remote state.              |
| rm               | Remove items from the Terraform state                            |
| show             | Show the attributes of a single resource in the state.           |
| replace-provider | Used to replace the provider for resources in a Terraform state. |

# Use-Case - Removing Item from State

There are 5 EC2 instances created through Terraform using count =5

The Team wants to destroy all the EC2 instances except the second instance with the resource address of aws\_instance.web[1].

1. This is not possible since the instance created through Count.
2. Apply taint on the EC2 instance.
3. Use terraform state rm aws\_instance.web[1]
4. Use terraform state mv aws\_instance.web[1]
5. None of the Above

# Debugging in Terraform

Terraform has detailed logs that can be enabled by setting the `TF_LOG` environment variable to any value.

You can set `TF_LOG` to one of the log levels TRACE, DEBUG, INFO, WARN or ERROR to change the verbosity of the logs.

To persist logged output, you can set `TF_LOG_PATH`

# Terraform Import

Allows importing existing infrastructure to Terraform.

Automatic code generation for imported resources is supported.

You can use **import blocks** to import more than one resource at a time.



# Import Workflow Steps

```
import {
  to = aws_security_group.mysg
  id = "sg-07f13feb262ba8b6f"
}

# terraform plan -generate-config-out="mysg.tf"

# terraform apply -auto-approve
```

# Local Values

Locals are used when you want to avoid repeating the same expression multiple times.

Local values are created by a `locals` block (plural), but you reference them as attributes on an object named `local` (singular)

Local value can reference values from other variables, locals etc.

```
locals {
    common_tags = {
        Team = "payments-team"
    }
}
```

# Terraform Workspace

Terraform workspaces enable us to manage multiple sets of deployments from the same sets of configuration files.

State File Directory = `terraform.tfstate.d`

Not suitable for isolation for strong separation between workspace (stage/prod)

| Use-Case                       | Command                                      |
|--------------------------------|----------------------------------------------|
| Create New Workspace           | <code>terraform workspace new kplabs</code>  |
| Switch to a specific Workspace | <code>terraform workspace select prod</code> |

# Terraform Modules

Terraform Modules allow us to centralize the resource configuration, and it makes it easier for multiple projects to re-use the Terraform code.

Instead of writing code from scratch, we can use multiple ready-made modules available.

```
resource "aws_instance" "web" {
    ami          = "ami-1234"
    instance_type = "t3.micro"
    key_name      = "user1"
    monitoring     = true
    vpc_security_group_ids = ["sg-12345678"]
    associate_public_ip_address = true
    instance_initiated_shutdown_behavior = "stop"
    ebs_optimized = true
    source_dest_check = false
    hibernation = true
    disable_api_termination = true
}
```

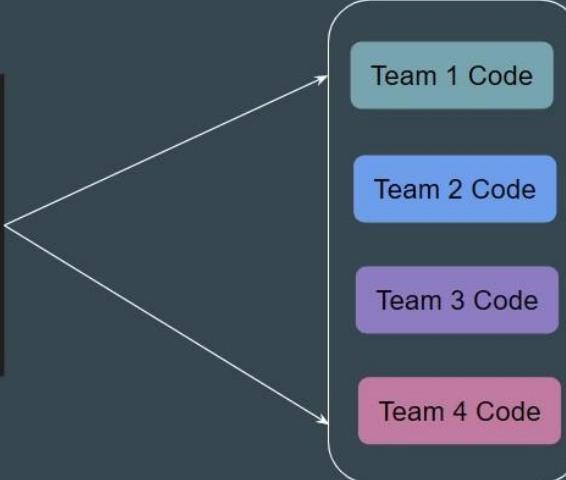
Terraform Module

Team 1 Code

Team 2 Code

Team 3 Code

Team 4 Code



# Calling a Module

Module source code can be present in a wide variety of locations including:

GitHub, Local Paths, Terraform Registry, S3 Buckets, HTTP URLs

To reference a module, you need to make use of **module** block and **source**

Terraform uses this during the module installation step of `terraform init` to download the source code to a directory on local disk so that other Terraform commands can use it.

```
module "ec2" {
    source = "https://example.com/vpc-module.zip"
}
```

## Example 1 - Local Paths

Local paths are used to reference to a module that is available in local filesystem.

A local path must begin with either ./ or ../ to indicate that a local path.

Modules sourced from local paths do NOT support versions.

```
module "ec2" {  
    source = "../modules/ec2"  
}
```

## Example 2 - Generic Git Repository

Arbitrary Git repositories can be used by prefixing the address with the special `git::` prefix.

```
module "vpc" {
    source = "git::https://example.com/vpc.git"
}
```

# Root vs Child Modules

**Root Module** resides in the main working directory of your Terraform configuration. This is the entry point for your infrastructure definition

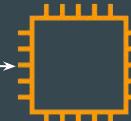
A module that has been called by another module is often referred to as a **child module**.

```
resource "aws_instance" "myec2" {  
  ami = var.ami  
  instance_type = var.instance_type  
}
```

```
module "ec2" {  
  source = "../../modules/ec2"  
}
```

Child Module

Root Module



# Module Outputs

A child module can use outputs to expose a subset of its resource attributes to a parent module.

**Format:** <MODULE NAME>.<OUTPUT NAME>

```
resource "aws_instance" "myec2" {
    ami = var.ami
    instance_type = var.instance_type
}

output "instance_id" {
    value = aws_instance.myec2.id
}
```

```
module "ec2" {
    source = "../../modules/ec2"
}

resource "aws_eip" "lb" {
    instance = module.ec2.instance_id
    domain   = "vpc"
}
```

# Module Versioning

When using modules installed from a module registry, HashiCorp recommends explicitly constraining the acceptable version numbers to avoid unexpected or unwanted changes.

It is **not mandatory** to specify a version argument.

```
module "ec2-instance" {
  source  = "terraform-aws-modules/ec2-instance/aws"
  version = "5.6.1"
}
```

# Terraform Registry

- Hosts a broad collection of publicly available Terraform modules.
- Each Terraform module has an associated address.
- A module address has the syntax `hostname/namespace/name/system`

The `hostname/` portion of a module is optional, and if omitted, it defaults to `registry.terraform.io/`.

```
module "ec2-instance" {  
    source  = "terraform-aws-modules/ec2-instance/aws"  
    version = "5.6.1"  
}
```

# Functions in Terraform

The Terraform language includes a number of built-in functions that you can use to transform and combine values.

**NO SUPPORT** for User-Defined Functions.

| Function Categories   | Functions Available                           |
|-----------------------|-----------------------------------------------|
| Numeric Functions     | abs, ceil, floor, max, min                    |
| String Functions      | concat, replace, split, join, tolower,toupper |
| Collection Functions  | element, keys, length, merge, sort, slice     |
| Filesystem Functions: | file, filebase64, dirname                     |

# Lookup function

lookup retrieves the value of a single element from a map, given its key. If the given key does not exist, the given default value is returned instead.

```
> lookup({a="ay", b="bee"}, "a", "what?")
ay
> lookup({a="ay", b="bee"}, "c", "what?")
what?
```

# Zipmap function

zipmap constructs a map from a list of keys and a corresponding list of values.

```
←[J]> zipmap(["pineapple","oranges","strawberry"], ["yellow","orange","red"])
{
    "oranges" = "orange"
    "pineapple" = "yellow"
    "strawberry" = "red"
}
```

# Index function

index finds the element index for a given value in a list.

```
C:\kplabs-terraform>terraform console  
> index(["a", "b", "c"], "b")  
1
```

# Element Function

element retrieves a single element from a list.

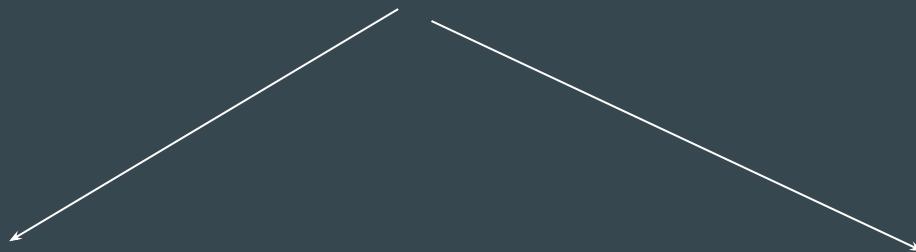
Format: element(list, index)

```
> element(["a", "b", "c"], 1)
b
```

# Testing Element Function

Code: Name = element(var.tags,count.index)

```
variable "tags" {  
    type = list  
    default = ["firstec2","secondec2"]  
}
```



```
> element(["firstec2","secondec2"],0)  
"firstec2"
```

```
> element(["firstec2","secondec2"],1)  
"secondec2"
```

# `toset` Function

`toset` function will convert the list of values to SET

```
> toset(["a", "b", "c","a"])
toset([
  "a",
  "b",
  "c",
])
```

# TimeStamp Function

timestamp returns a UTC timestamp string in RFC 3339 format.

```
> formatdate("DD MMM YYYY hh:mm ZZZ", "2018-01-02T23:12:01Z")
02 Jan 2018 23:12 UTC
> formatdate("EEEE, DD-MMM-YY hh:mm:ss ZZZ", "2018-01-02T23:12:01Z")
Tuesday, 02-Jan-18 23:12:01 UTC
> formatdate("EEE, DD MMM YYYY hh:mm:ss ZZZ", "2018-01-02T23:12:01-08:00")
Tue, 02 Jan 2018 23:12:01 -0800
> formatdate("MMM DD, YYYY", "2018-01-02T23:12:01Z")
Jan 02, 2018
> formatdate("HH:mm:ss", "2018-01-02T23:12:01Z")
11:12pm
```

# File Function

File function can reduce the overall Terraform code size by loading contents from external sources during terraform operations.

```
resource "aws_iam_user_policy" "lb_ro" {
  name = "demo-user-policy"
  user = aws_iam_user.this.name

  policy = jsonencode({
    "Version": "2012-10-17",
    "Statement": [
      {
        "Action": "ec2:*",
        "Effect": "Allow",
        "Resource": "*"
      },
      {
        "Effect": "Allow",
        "Action": "elasticloadbalancing:*",
        "Resource": "*"
      },
    ]
  })
}
```

Before



```
resource "aws_iam_user_policy" "lb_ro" {
  name = "demo-user-policy"
  user = aws_iam_user.this.name

  policy = file("./ec2-policy.json")
}
```

After

# Meta Arguments in Terraform

Terraform allows us to include meta-arguments within the resource block, which allows some details of this standard resource behaviour to be customized on a per-resource basis.

Inside resource block

```
resource "aws_instance" "myec2" {
    ami = "ami-00c39f71452c08778"
    instance_type = "t2.micro"

    lifecycle {
        ignore_changes = [tags]
    }
}
```

# Different Meta-Arguments

| Meta-Argument | Description                                                                                                                                            |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| depends_on    | Handle hidden resource or module dependencies that Terraform cannot automatically infer.                                                               |
| count         | Accepts a whole number, and creates that many instances of the resource                                                                                |
| for_each      | Accepts a map or a set of strings, and creates an instance for each item in that map or set.                                                           |
| lifecycle     | Allows modification of the resource lifecycle.                                                                                                         |
| provider      | Specifies which provider configuration to use for a resource, overriding Terraform's default behavior of selecting one based on the resource type name |

# Lifecycle Meta-Argument

Some details of the default resource behaviour can be customized using the special nested lifecycle block within a resource block body:

```
resource "aws_instance" "myec2" {
    ami = "ami-0f34c5ae932e6f0e4"
    instance_type = "t2.micro"

    tags = {
        Name = "HelloEarth"
    }

    lifecycle {
        ignore_changes = [tags]
    }
}
```

# Arguments Available for LifeCycle Block

There are four argument available within lifecycle block.

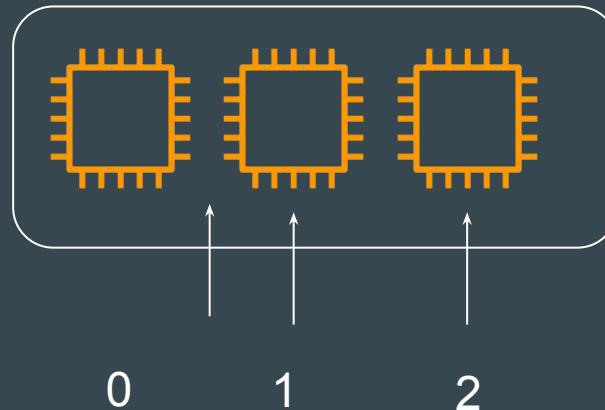
| Arguments             | Description                                                                                                          |
|-----------------------|----------------------------------------------------------------------------------------------------------------------|
| create_before_destroy | New replacement object is created first, and the prior object is destroyed after the replacement is created.         |
| prevent_destroy       | Terraform to reject with an error any plan that would destroy the infrastructure object associated with the resource |
| ignore_changes        | Ignore certain changes to the live resource that does not match the configuration.                                   |
| replace_triggered_by  | Replaces the resource when any of the referenced items change                                                        |

# Count and Count Index

The count argument accepts a whole number, and creates that many instances of the resource.

count.index — The distinct index number (starting with 0) corresponding to this instance.

```
resource "aws_instance" "myec2" {  
    ami = "ami-00c39f71452c08778"  
    instance_type = "t2.micro"  
    count = 3  
}
```



# **Exam Preparation - Part 3**

# Find the Issue - Use-Cases

You can expect a use case in exam with a sample Terraform code, and you must find what should be removed as part of Terraform best practice.

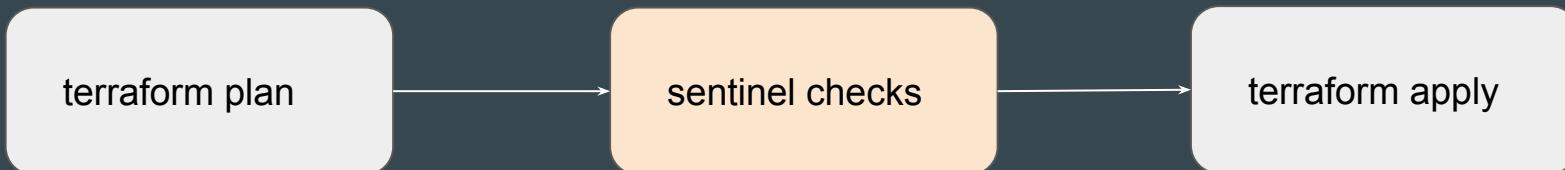
```
terraform {
  backend "s3" {
    bucket = "mybucket"
    key    = "path/to/my/key"
    region = "us-east-1"
    access_key = "AKIAIOSFODNN7EXAMPLE"
    aecret_key = "wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEK"
  }
}
```

# Sentinel

Sentinel is an embedded policy-as-code framework integrated with the HashiCorp Enterprise products. Sentinel is a proactive service.

Can be used for various use-cases like:

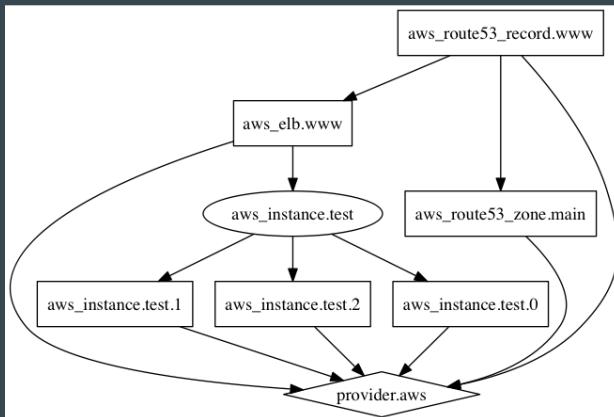
- Verify if EC2 instance has tags.
- Verify if the S3 bucket has encryption enabled.



# Terraform Graph

Terraform graph refers to a **visual representation of the dependency relationships** between resources defined in your Terraform configuration.

The output of terraform graph is in the **DOT format**, which can easily be converted to an image.



# Input Variables

Terraform input variables are used to pass certain values from outside of the configuration

| Name     | Value           |
|----------|-----------------|
| vpn_ip   | 101.0.62.210/32 |
| app_port | 8080            |

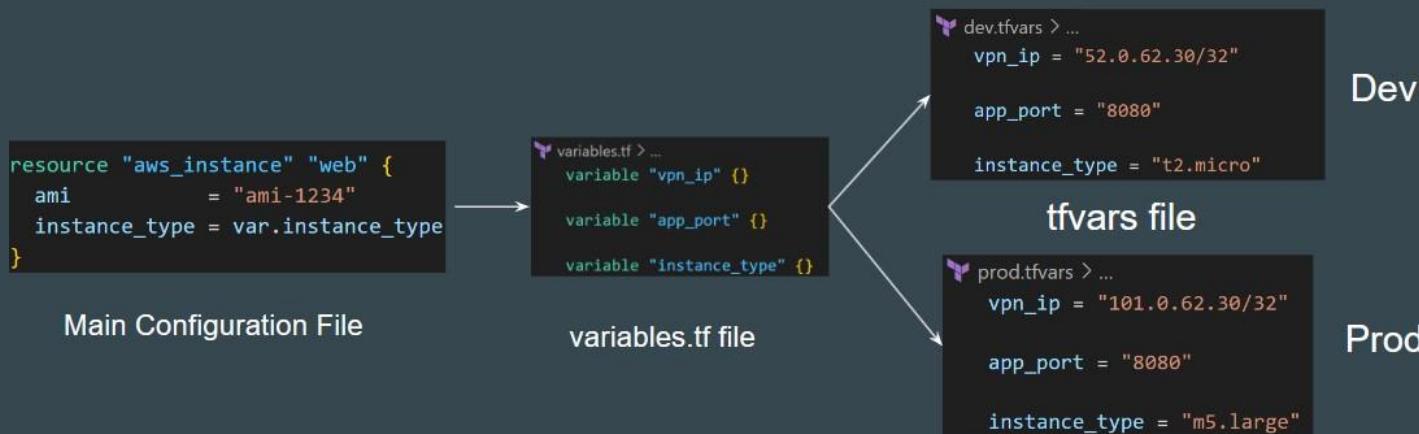
Variable File

```
resource "aws_vpc_security_group_ingress_rule" "allow_tls_ipv4" {  
    security_group_id = aws_security_group.allow_tls.id  
    cidr_ipv4        = var.vpn_ip  
    from_port         = var.app_port  
    ip_protocol       = "tcp"  
    to_port           = var.app_port  
}
```

# Terraform TFGVARS

terraform.tfvars file can be used to define value to all the variables.

This approach leads to easier setup for multi-project deployments.



# Selecting tfvars File

If you have multiple variable definitions file (\*.tfvars) file, you can manually define the file to use during the command line.

```
C:\Users\zealv\kplabs-terraform>terraform plan -var-file="prod.tfvars"

Terraform used the selected providers to generate the following execution plan.
following symbols:
+ create

Terraform will perform the following actions:

# aws_instance.web will be created
+ resource "aws_instance" "web" {
    + ami                                = "ami-1234"
    + arn                                = (known after apply)
    + associate_public_ip_address        = (known after apply)
    + availability_zone                  = (known after apply)
    + cpu_core_count                     = (known after apply)
    + cpu_threads_per_core              = (known after apply)
    + disable_api_stop                  = (known after apply)
    + disable_api_termination           = (known after apply)
    + ebs_optimized                     = (known after apply)
```

# Declaring Variable Values

When variables are declared in your configuration, they can be set in a number of ways:

1. Variable Defaults.
2. Variable Definition File (\*.tfvars)
3. Environment Variables
4. Setting Variables in the Command Line.

```
variables.tf > ...

variable "app_port" {
    default = "8080"
}
```

```
prod.tfvars > ...

vpn_ip = "101.0.62.30/32"

app_port = "8080"

instance_type = "m5.large"
```

# Setting Variable in Command Line

To specify individual variables on the command line, use the `-var` option when running the `terraform plan` and `terraform apply` commands:

```
C:\Users\zealv\kplabs-terraform>terraform plan -var="instance_type=m5.large"

Terraform used the selected providers to generate the following execution plan. Resource
following symbols:
+ create

Terraform will perform the following actions:

# aws_instance.web will be created
+ resource "aws_instance" "web" {
    + ami                                = "ami-1234"
    + arn                                = (known after apply)
    + associate_public_ip_address        = (known after apply)
    + availability_zone                  = (known after apply)
    + cpu_core_count                     = (known after apply)
    + cpu_threads_per_core              = (known after apply)
    + disable_api_stop                  = (known after apply)
    + disable_api_termination           = (known after apply)
    + ebs_optimized                     = (known after apply)
    + get_password_data                = false
    + host_id                            = (known after apply)
    + host_resource_group_arn           = (known after apply)
    + iam_instance_profile              = (known after apply)
    + id                                 = (known after apply)
    + instance_initiated_shutdown_behavior = (known after apply)
    + instance.lifecycle               = (known after apply)
    + instance.state                   = (known after apply)
    + instance_type                    = "m5.large"
```

# Setting Variable through Environment Variables

Terraform searches the environment of its own process for environment variables named `TF_VAR_` followed by the name of a declared variable.

```
C:\Users\zealv\kplabs-terraform>echo %TF_VAR_instance_type%
t2.large

C:\Users\zealv\kplabs-terraform>terraform plan

Terraform used the selected providers to generate the following execution plan
following symbols:
+ create

Terraform will perform the following actions:

# aws_instance.web will be created
+ resource "aws_instance" "web" {
    + ami                                = "ami-1234"
    + arn                                = (known after apply)
    + associate_public_ip_address        = (known after apply)
    + availability_zone                  = (known after apply)
```

# Variable Definition Precedence

Terraform loads variables in the following order, with later sources taking precedence over earlier ones:

1. Environment variables
2. The `terraform.tfvars` file, if present.
3. The `terraform.tfvars.json` file, if present.
4. Any `*.auto.tfvars` or `*.auto.tfvars.json` files, processed in lexical order of their filenames.
5. Any `-var` and `-var-file` options on the command line

# Variables with undefined values

If you have variables with undefined values, it will **NOT** directly result in an error.

Terraform will ask you to supply the value associated with them.

```
C:\Users\zealv\kplabs-terraform>terraform plan  
var.instance_type  
Enter a value:
```

# Not Allowed Variable Names

We cannot use all words within variable names.

Terraform reserves some additional names that can no longer be used as input variable names for modules. These reserved names are:

- count
- depends\_on
- for\_each
- lifecycle
- providers
- source

```
Error: Invalid variable name  
on demo.tf line 6, in variable "count":  
 6: variable "count" {  
  
The variable name "count" is reserved due to its special meaning
```

# Points to Note - State File

Terraform state file generally stores details about the resources that it manages.

Various aspects like “Input Variables” are not stored.

Output value will be stored in state file but not the description

```
variable "instance_type" {
    type =    string
    default = "t2.micro"
    description = "Default EC2 Instance type for Module"
}

output "variable" {
    value = var.instance_type
    description = "Instance Type of EC2"
}
```

# Terraform Console

Terraform Console provides an interactive environment specifically **designed to test functions** and experiment with expressions before integrating them into your main code.

```
C:\Users\zealv\kplabs-terraform>terraform console  
> max(10,20,30)  
30
```

# Dependency Lock File

Terraform dependency lock file allows us to lock to a specific version of the provider. Name is `terraform.lock.hcl`. For tracking provider dependencies.

If a particular provider already has a selection recorded in the lock file, Terraform will always re-select that version for installation, even if a newer version has become available.

You can override that behavior by running `terraform init -upgrade`

# Dependencies - Implicit

With **implicit dependency**, Terraform can automatically find references of the object, and create an implicit ordering requirement between the two resources.

In the following screenshot, Terraform will create EC2 first before EIP.

```
resource "aws_eip" "lb" {
    domain    = "vpc"
    instance = aws_instance.myec2.id
}

resource "aws_instance" "myec2" {
    ami          = "ami-123"
    instance_type = "t2.micro"
}
```

# Dependencies - Explicit

Explicitly specifying a dependency is only necessary when a resource relies on some other resource's behavior but doesn't access any of that resource's data in its arguments.

Uses the `depends_on` meta-argument

```
resource "aws_iam_role" "example" {
  name = "example"
  assume_role_policy = "..."
}

resource "aws_instance" "example" {
  ami           = "ami-a1b2c3d4"
  instance_type = "t2.micro"
  depends_on   = [aws_iam_role_policy.example]
}
```

# Data Sources

Data sources allow Terraform to use / fetch information defined outside of Terraform

```
data "aws_instances" "example" {}
```

```
data "local_file" "foo" {
  filename = "${path.module}/demo.txt"
}
```

# Terraform Enterprise

Terraform Enterprise provides several added advantages compared to Terraform Cloud.

Some of these include:

- Single Sign-On
- Auditing
- Private Data Center Networking
- Clustering

Team & Governance features are not available for Terraform Cloud Free (Paid)

# Remote Backend

The remote backend stores Terraform state and may be used to run operations in Terraform Cloud.

When using full remote operations, operations like `terraform plan` or `terraform apply` can be executed in Terraform Cloud's run environment, with log output streaming to the local terminal.

The remote backend was the primary implementation of HCP Terraform's CLI-driven run workflow for Terraform versions 0.11.13 through 1.0.x. We recommend using the native cloud integration for Terraform versions 1.1 or later, as it provides an improved user experience and various enhancements.

# Points to Note

HCP = HashiCorp Cloud Platform

Secure Variable Storage is available in Terraform Enterprise and Cloud but not in the normal version of Terraform.

Terraform Cloud / Enterprise comes with a Private Module registry which allows organizations to restrict access based on requirements.

Terraform Cloud provides the feature of Remote State storage.

Encryption of state file is available

## Points to Note

In a HCP workspace linked to a VCS repository, runs start automatically when you merge or commit changes to version control.

A workspace is linked to one branch of a VCS repository and ignores changes to other branches.

To protect secret values in HCP, you can mark any Terraform or environment variable as sensitive data by clicking its Sensitive checkbox that is visible during editing. Marking a variable as sensitive makes it write-only and prevents all users (including you) from viewing its value

# Sensitive Values in HCP

To protect secret values in HCP, you can mark any Terraform or environment variable as sensitive data by clicking its Sensitive checkbox that is visible during editing.

Marking a variable as sensitive makes it write-only and prevents all users (including you) from viewing its value

Variable set scope

Apply globally  
All current and future workspaces in this organization will access this variable set.

Apply to specific projects and workspaces

Variables

You can add any number of [Terraform](#) and [Environment](#) variables. Terraform will use these variables for all plan and apply operations in the specified workspaces.

| Key                                       | Value                  | Category  | ... |
|-------------------------------------------|------------------------|-----------|-----|
| HCP_CLIENT_ID<br><small>SENSITIVE</small> | Sensitive - write only | terraform | ... |

Select variable category

**Terraform variable**  
These variables should match the declarations in your configuration. Click the HCL box to use interpolation or set a non-string value.

**Environment variable**  
These variables are available in the Terraform runtime environment.

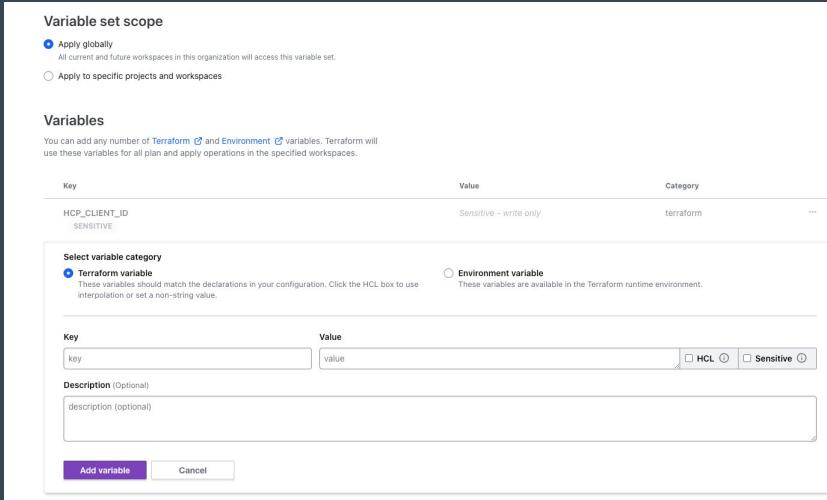
| Key | Value |
|-----|-------|
| key | value |

HCL  Sensitive

Description (Optional)

description (optional)

Add variable Cancel

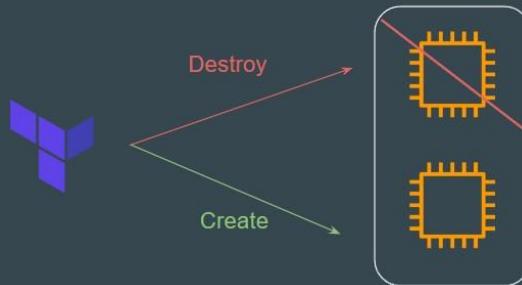


# Recreating the Resource

The **-replace** option with `terraform apply` to force Terraform to replace an object even though there are no configuration changes that would require it.

```
terraform apply -replace="aws_instance.web"
```

A similar kind of functionality was achieved using the **terraform taint** command in older versions of Terraform. Not recommended now.



# Benefits of IAC Tool

There are three primary benefits of Infrastructure as Code tools:

Automation, Versioning, and Reusability.

Various IAC Tools Available in the market:

- Terraform
- CloudFormation
- Azure Resource Manager
- Google Cloud Deployment Manager

# terraform output

The terraform output command is used to extract the value of an output variable from the state file.

```
variable "instance_type" {  
    type = "string"  
    default = "t2.micro"  
    description = "Default EC2 Instance type for Module"  
}  
  
output "instance_type" {  
    value = var.instance_type  
    description = "Instance Type of EC2"  
}
```



```
C:\kplabs-terraform>terraform output  
instance_type = "t2.small"
```

# Module Source and Git Branches

By default, Terraform will clone and use the default branch (referenced by HEAD) in the selected repository.

You can override this using the `ref` argument.

Format: `?ref=<version-number>`

```
module "vpc" {  
  source = "git::https://example.com/vpc.git?ref=v1.2.0"  
}
```

# Splat Expressions

Splat Expression allows us to get a list of all the attributes.

Resources that use the `for_each` argument will appear in expressions as a map of objects, so you can't use splat expressions with those resources.

```
resource "aws_iam_user" "lb" {
    name = "iamuser.${count.index}"
    count = 3
    path = "/system/"
}

output "arns" {
    value = aws_iam_user.lb[*].arn
}
```

# Important Documentation Reference - Splat

A *splat expression* provides a more concise way to express a common operation that could otherwise be performed with a `for` expression.

If `var.list` is a list of objects that all have an attribute `id`, then a list of the ids could be produced with the following `for` expression:

```
[for o in var.list : o.id]
```



This is equivalent to the following *splat expression*:

```
var.list[*].id
```



# Point to Note

Will this code block display the names of all the IAM usernames created?

Answer = NO

```
resource "aws_iam_user" "lb" {
    name = "iamuser.${count.index}"
    count = 3
    path = "/system/"
}

output "arns" {
    value = aws_iam_user.lb.[*].name
}
```

# Legacy Splat Expression

Earlier versions of the Terraform language had a slightly different version of splat expressions, which Terraform continues to support for backward compatibility.

The legacy "attribute-only" splat expressions use the sequence `.*`, instead of `[*]`:

```
resource "aws_iam_user" "lb" {
    name = "iamuser.${count.index}"
    count = 3
    path = "/system/"
}

output "arns" {
    value = aws_iam_user.lb.*.name
}
```

# Fetching Values from List

To fetch the `instance_type` value of `m5.xlarge` from the `list`, you can reference to the key of `1`

```
var.size[1]
```

```
variable "size" {
    type = list
    default = ["m5.large","m5.xlarge","t2.medium"]
}

resource "aws_instance" "myec2" {
    ami = "ami-082b5a644766e0e6f"
    instance_type = var.size[1]
}
```

# Fetching Values from Map

To reference the “t2.small” instance type from the below map, the following approaches need to be used:

```
var.types["ap-south-1"]
```

```
variable "types" {
  type = map
  default = {
    us-east-1 = "t2.micro"
    us-west-2 = "t2.nano"
    ap-south-1 = "t2.small"
  }
}

resource "aws_instance" "myec2" {
  ami = "ami-082b5a644766e0e6f"
  instance_type = var.types["ap-south-1"]
}
```

# Dealing with Larger Infrastructure

Cloud Providers have set a certain rate limit, so Terraform can only request a certain number of resources over a period of time.

It is important to break larger configurations into multiple smaller configurations that can be independently applied.

Alternatively, you can make use of `-refresh=false` and `target` flag for a workaround (not recommended)

# BackEnds

Backends primarily determine where Terraform stores its state.

By default, Terraform implicitly uses a backend called local to store state as a local file on disk.

If required, you can store state file in other backend as well.

```
terraform {  
  backend "s3" {  
    bucket = "mybucket"  
    key    = "path/to/my/key"  
    region = "us-east-1"  
  }  
}
```

## Points to Note - Initializing Backend

When configuring a backend for the first time (moving from no defined backend to explicitly configuring one), Terraform will give you the option to migrate your state to the new backend.

This lets you adopt new backends without losing any existing state.

# Local Backend

The local backend stores the state on the local filesystem, locks that state using system APIs, and performs operations locally.

By default, Terraform uses the "local" backend, which is the normal behavior of Terraform you're used to

```
terraform {
  backend "local" {
    path = "relative/path/to/terraform.tfstate"
  }
}
```

# Air Gapped Environments

An air gap is a network security measure employed to ensure that a secure computer network is physically isolated from unsecured networks, such as the public Internet.

The screenshot shows the Terraform Enterprise workspace management interface. At the top, there are navigation links for Workspaces, Modules, and Settings. Below that is a search bar and a button for '+ New Workspace'. The main area displays a table titled 'Workspaces' with 18 total entries. The columns are 'WORKSPACE NAME', 'RUN STATUS', 'LATEST CHANGE', 'RUN', and 'REPO'. The table lists various workspaces like 'exceed-limit', 'filetest-dev', 'migrated-default', etc., along with their run status (e.g., APPLIED, ERROR, PLANNED), latest change time, run ID, and repository information.

| WORKSPACE NAME   | RUN STATUS           | LATEST CHANGE | RUN      | REPO                          |
|------------------|----------------------|---------------|----------|-------------------------------|
| exceed-limit     | ✓ APPLIED            | 5 months ago  | run-B8Ac | NICKF/terraform-minimum       |
| filetest-dev     | * ERROR*             | 3 months ago  | run-SLSz | nfagerlund/terraform-filetest |
| migrated-default | ✓ PLANNED            | 5 months ago  | run-BVjI | nfagerlund/terraform-minimum  |
| migrated-first   | ✓ PLANNED            | 5 months ago  | run-A2sp | nfagerlund/terraform-minimum  |
| migrated-second  | ✓ PLANNED            | 5 months ago  | run-KqNV | nfagerlund/terraform-minimum  |
| migrated-solo    | ✓ APPLIED            | 5 months ago  | run-1RKX | NICKF/terraform-minimum       |
| migrated-solo2   | ✓ PLANNED            | 5 months ago  | run-Rih7 | nfagerlund/terraform-minimum  |
| migrate-first-2  | ! NEEDS CONFIRMATION | 3 months ago  | run-hR57 | nfagerlund/terraform-minimum  |

Terraform Enterprise

Air Gap Install



Isolated Server

## Choose your installation type



Please choose an installation type to continue.

[Continue »](#)

# Requirements for Publishing Module in Registry

| Core Requirements                    | Description                                                                                                                                                                                         |
|--------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| GitHub                               | The module must be on GitHub and must be a public repo. This is only a requirement for the public registry and not for private registry.                                                            |
| Named<br>terraform-<PROVIDER>-<NAME> | Example:<br>terraform-aws-ec2-instance                                                                                                                                                              |
| Repository description               | The GitHub repository description is used to populate the short description of the module.                                                                                                          |
| Standard module structure            | The module must adhere to the standard module structure. This allows the registry to inspect your module and generate documentation, track resource usage, parse submodules and examples, and more. |
| x.y.z tags for releases              | For example, v1.0.4 and 0.9.2                                                                                                                                                                       |

# Comments in Terraform

A comment is a text note added to the source code to provide explanatory information, usually about the function of the code.

```
/* This is Terraform Backend
State file stored in S3
*/

terraform {
    backend "s3" {
        bucket = "mybucket"
        key    = "path/to/my/key"
        region = "us-east-1"
    }
}

# This is single line comment
// This is single line comment
```

# Dynamic Blocks

Dynamic Block allows us to dynamically construct repeatable nested blocks, which are supported inside resource, data, provider, and provisioner blocks.

Overuse of Dynamic blocks can make configuration hard to read and maintain.

```
variable "sg_ports" {
  type    = list(number)
  description = "list of ingress ports"
  default   = [8200, 8201, 8300, 9200, 9500]
}

resource "aws_security_group" "dynamicsg" {
  name      = "dynamic-sg"

  dynamic "ingress" [
    for_each = var.sg_ports
    iterator = port
    content {
      from_port   = port.value
      to_port     = port.value
      protocol    = "tcp"
      cidr_blocks = ["0.0.0.0/0"]
    }
  ]
}
```

# Miscellaneous Pointers

GitHub is not the supported backend type in Terraform.

API and CLI access for Terraform Cloud can be managed through API tokens that can be generated from Terraform Cloud UI.

Terraform uses Parallelism to reduce the time it takes to create the resource. By default, this value is set to 10

# Code Formatting Recommended Practices

Indent two spaces for each nesting level

When multiple arguments with single-line values appear on consecutive lines at the same nesting level, align their equals signs:

```
ami          = "abc123"
instance_type = "t2.micro"
```

# Miscellaneous Pointers

Terraform does not require **go** as a prerequisite.

Terraform providers are NOT always installed through the internet. There is a different offline approach for air-gapped systems.

Terraform and Terraform Provider **NEED NOT** have the same major version for compatibility.

# Sensitive Parameter

Adding sensitive parameter ensures that you do not accidentally expose this data in CLI output, log output.

The sensitive value will be present as part of the state file.

```
variable "sensitive_content" {  
    sensitive = true  
    default = "supersecretpassw0rd"  
}  
  
resource "local_file" "foo" {  
    content = var.sensitive_content  
    filename = "password.txt"  
}
```



```
Terraform will perform the following actions:  
  
# local_file.foo will be created  
+ resource "local_file" "foo" {  
    + content          = (sensitive value)  
    + content_base64sha256 = (known after apply)  
    + content_base64sha512 = (known after apply)  
    + content_md5      = (known after apply)  
    + content_sha1     = (known after apply)  
    + content_sha256   = (known after apply)  
    + content_sha512   = (known after apply)  
    + directory_permission = "0777"  
    + file_permission   = "0777"  
    + filename          = "password.txt"  
    + id                = (known after apply)  
}
```

# Actions Forbidden When State File is Locked

When the state file is locked, the following actions are forbidden:

Running `terraform apply` or any other command that modifies the state file (e.g. `terraform plan`, `terraform destroy`, etc.)

Running `terraform refresh`, which updates the state file to reflect the current state of the infrastructure

`terraform state [push, rm, mv]`

# Miscellaneous Pointers

1. `terraform.tfstate` will NOT always match the current state infrastructure.

If you are making use of the GIT repository for committing terraform code, the `.gitignore` should be configured to ignore certain terraform files that might contain sensitive data.

Some of these can include:

`terraform.tfstate` file (this can include sensitive information)

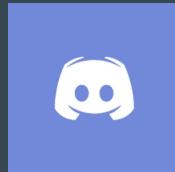
`*.tfvars` (may contain sensitive data like passwords)

## Points to Note - State

1. If supported by your backend, Terraform will lock your state for all operations that could write state.
2. Not all backends support locking functionality.
3. Terraform has a force-unlock command to manually unlock the state if unlocking failed. *terraform force-unlock LOCK\_ID [DIR]*

# Join us in our Adventure

Be Awesome



[kplabs.in/chat](https://kplabs.in/chat)



[kplabs.in/linkedin](https://kplabs.in/linkedin)