

HashiCorp Certified Terraform Associate 2024

PPT Version

PPT Release Date = 5th June 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.

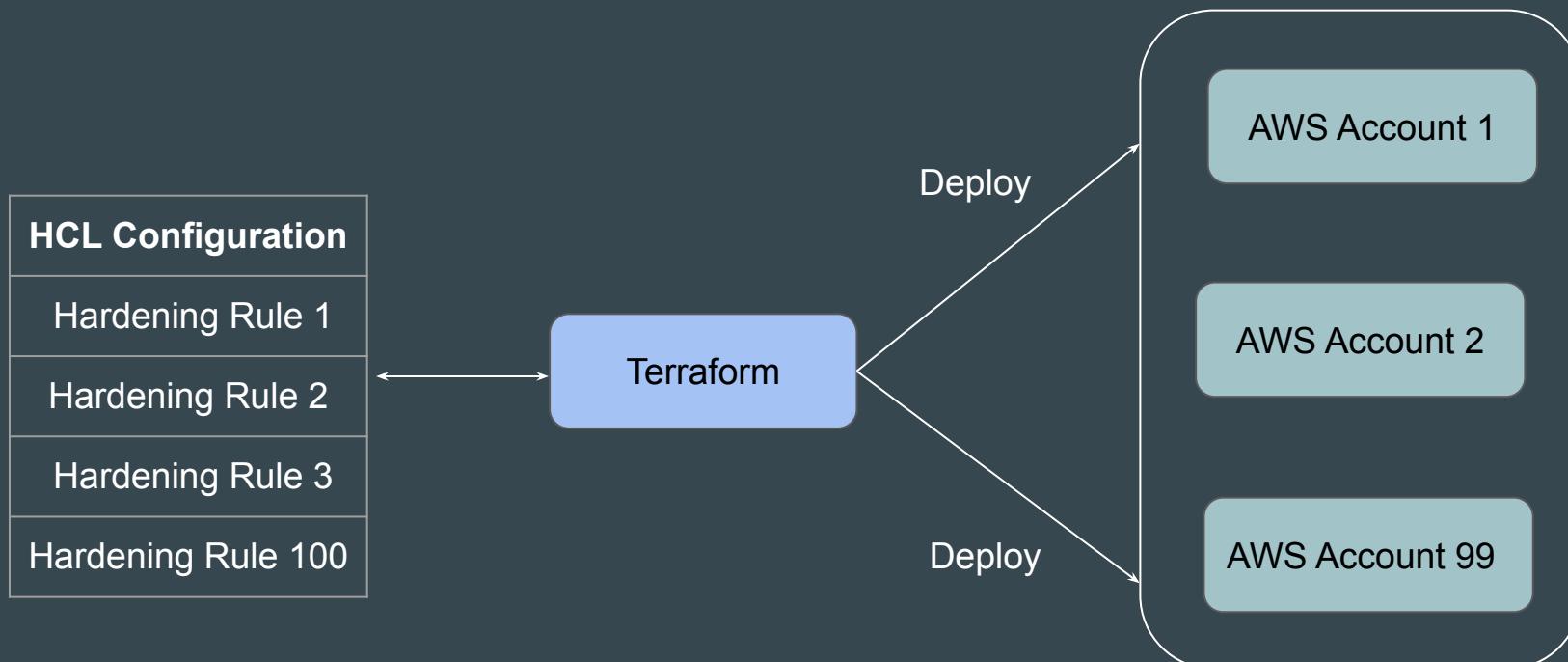
There were 100+ pages of guidelines, and it used to take 2-3 days to implement in 1 account.

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.

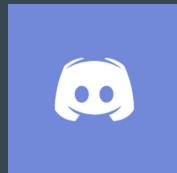
Something about me :-

- 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



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:

1	Understand infrastructure as code (IaC) concepts
1a	Explain what IaC is
1b	Describe advantages of IaC patterns
2	Understand the purpose of Terraform (vs other IaC)
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.

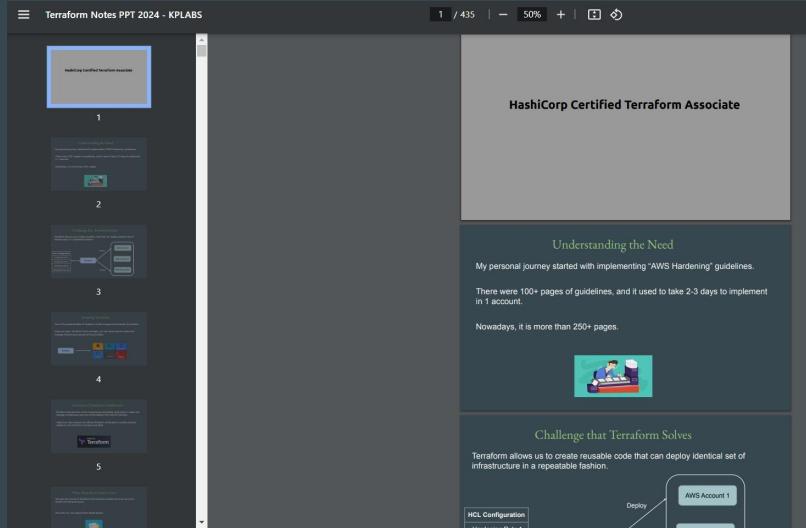
The screenshot shows a GitHub repository page for the user 'zealvora' with the repository name 'terraform-beginner-to-advanced-resource'. The repository is public and has 1 branch and 0 tags. The master branch is selected. The page displays a list of 127 commits, with the most recent commit being a merge pull request from 'vk31032022/patch-1' at 17 hours ago. The commits are organized into sections: 'Section 1 - Deploying Infrastructure with Terraform...', '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 Capabilities...', and 'Readme.md'. The commits for 'Readme.md' and 'Section 7...' are from last week, while others are from June 2023 or earlier.

Commit	Message	Time Ago
zealvora Merge pull request #22 from vk31032022/patch-1	e7f392d · 17 hours ago	127 Commits
Section 1 - Deploying Infrastructure with Terraform...	June 2023 Update	6 months ago
Section 2 - Read, Generate, Modify Configuration...	Merge pull request #22 from vk31032022/patch-1	17 hours ago
Section 3 - Terraform Provisioners	Update remote-exec.md	3 months ago
Section 4 - Terraform Modules & Workspaces	Updating Year of Update in Repo	6 months ago
Section 5 - Remote State Management	Update eip.tf	last month
Section 6 - Security Primer	Update multiple-providers.md	3 months ago
Section 7 - Terraform Cloud & Enterprise Capabilities...	Updating Year of Update in Repo	6 months ago
Readme.md	Update Readme.md	last week

Course Resource - PPT Slides

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

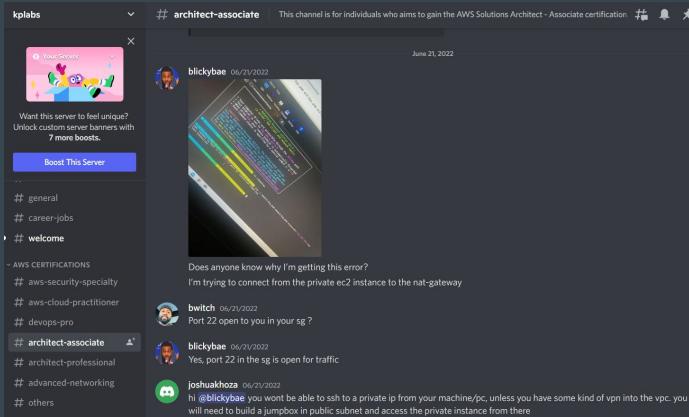
The PDF is attached as part of the lecture titled “Central PPT Notes”.



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

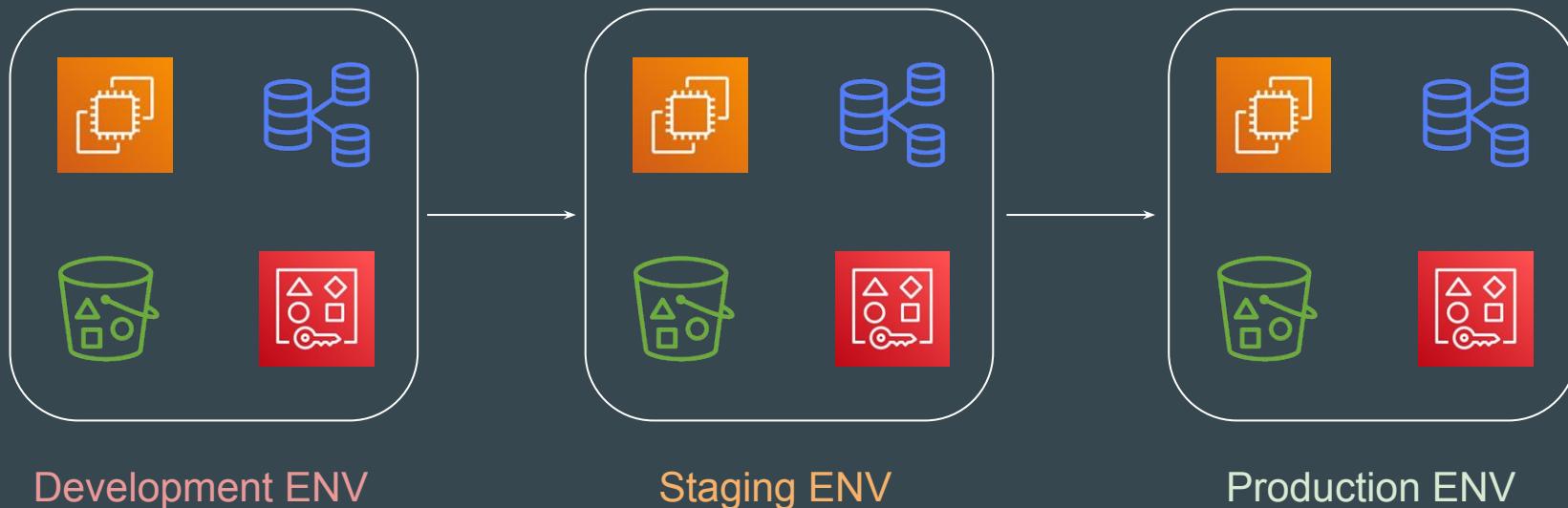
If a particular task has to be done in an repeatable manner, it MUST be automated.

Points to Note:

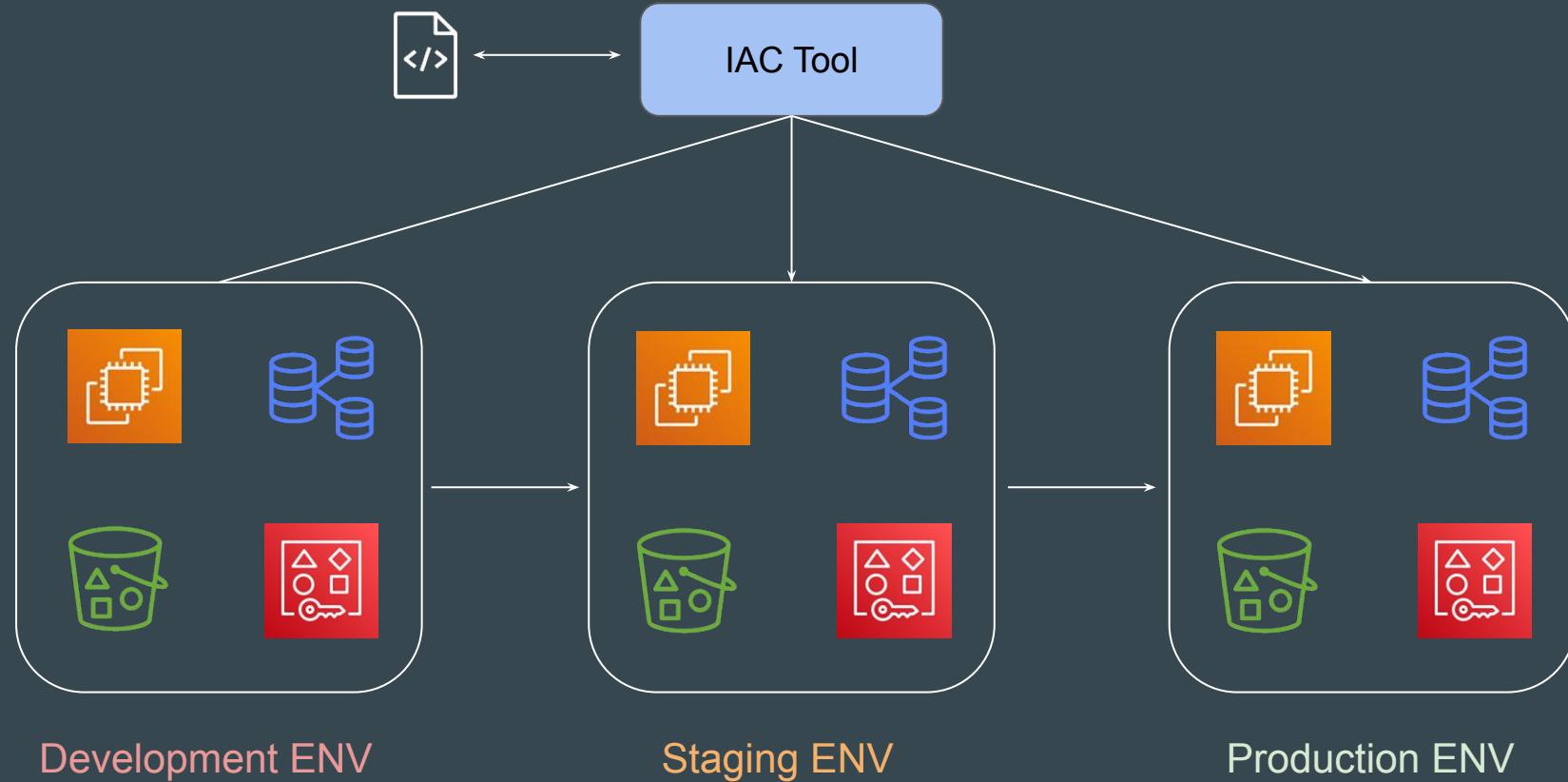
1. Depending on the type of task, the tools for automation will change.
2. There are wide variety of Tools & Technologies used for Automation like Ansible, CloudFormation, Terraform, Python etc.

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

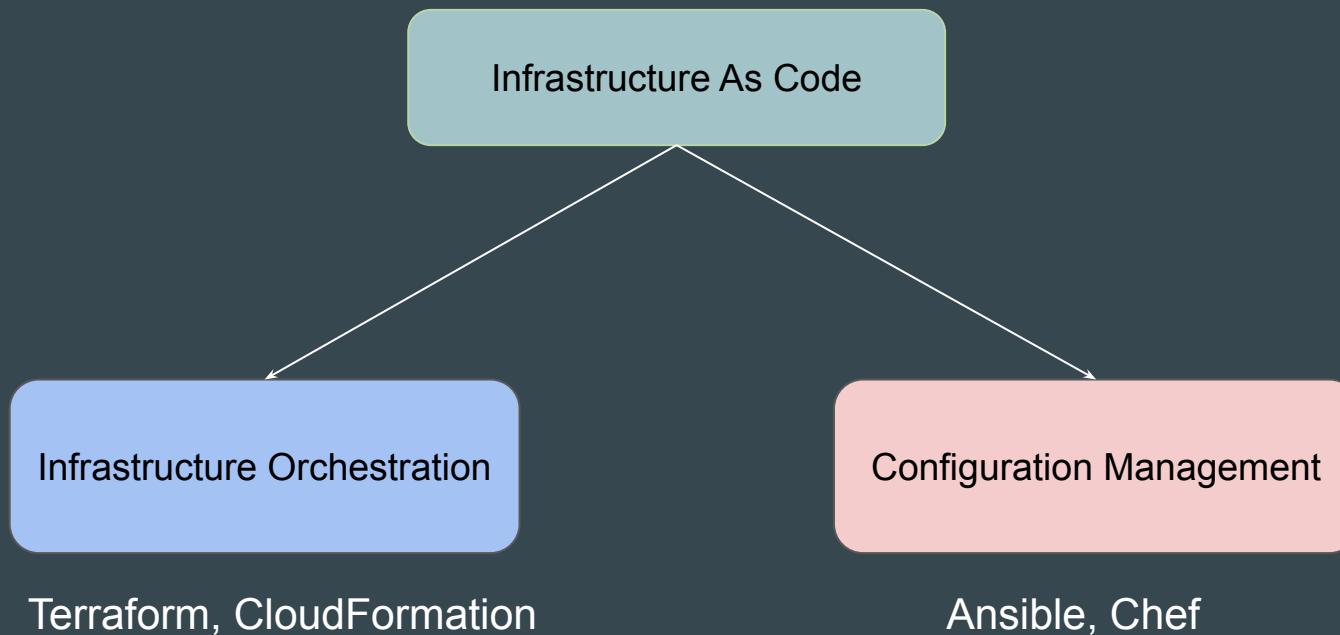
Available Tools

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

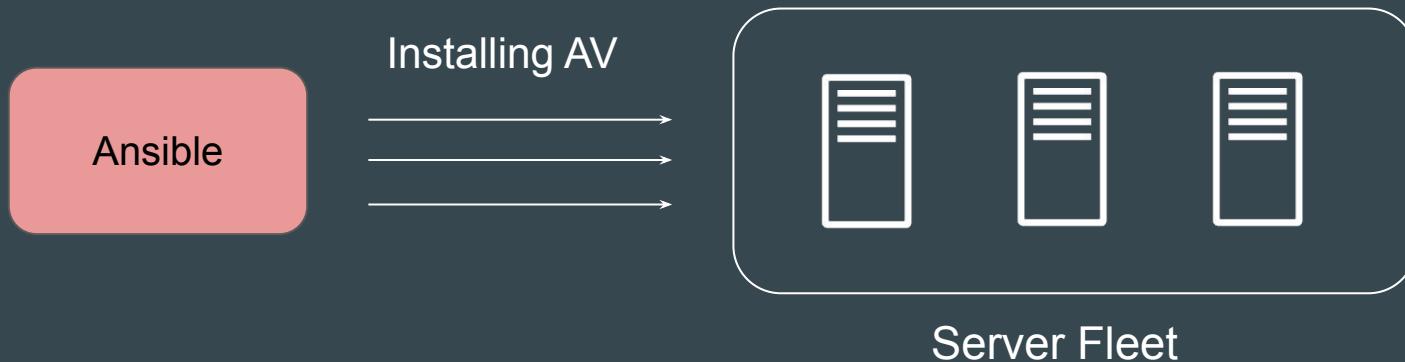
The tools are widely divided into two major categories



Configuration Management

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

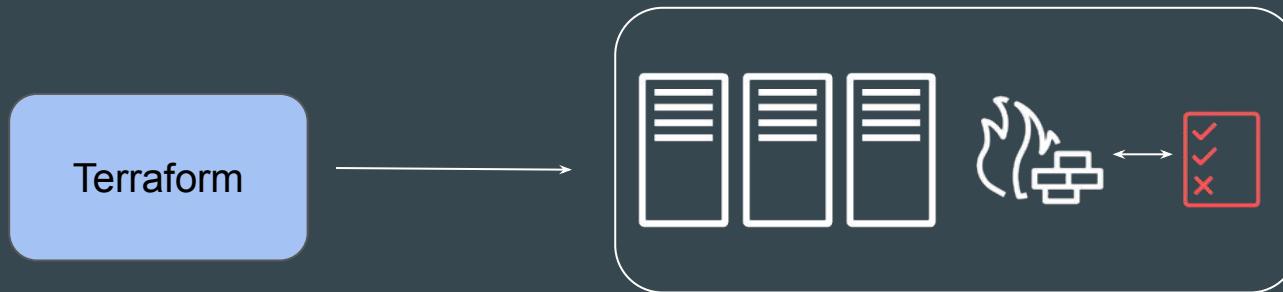
Example: ALL servers should have Antivirus installed with version 10.0.2



Infrastructure Orchestration

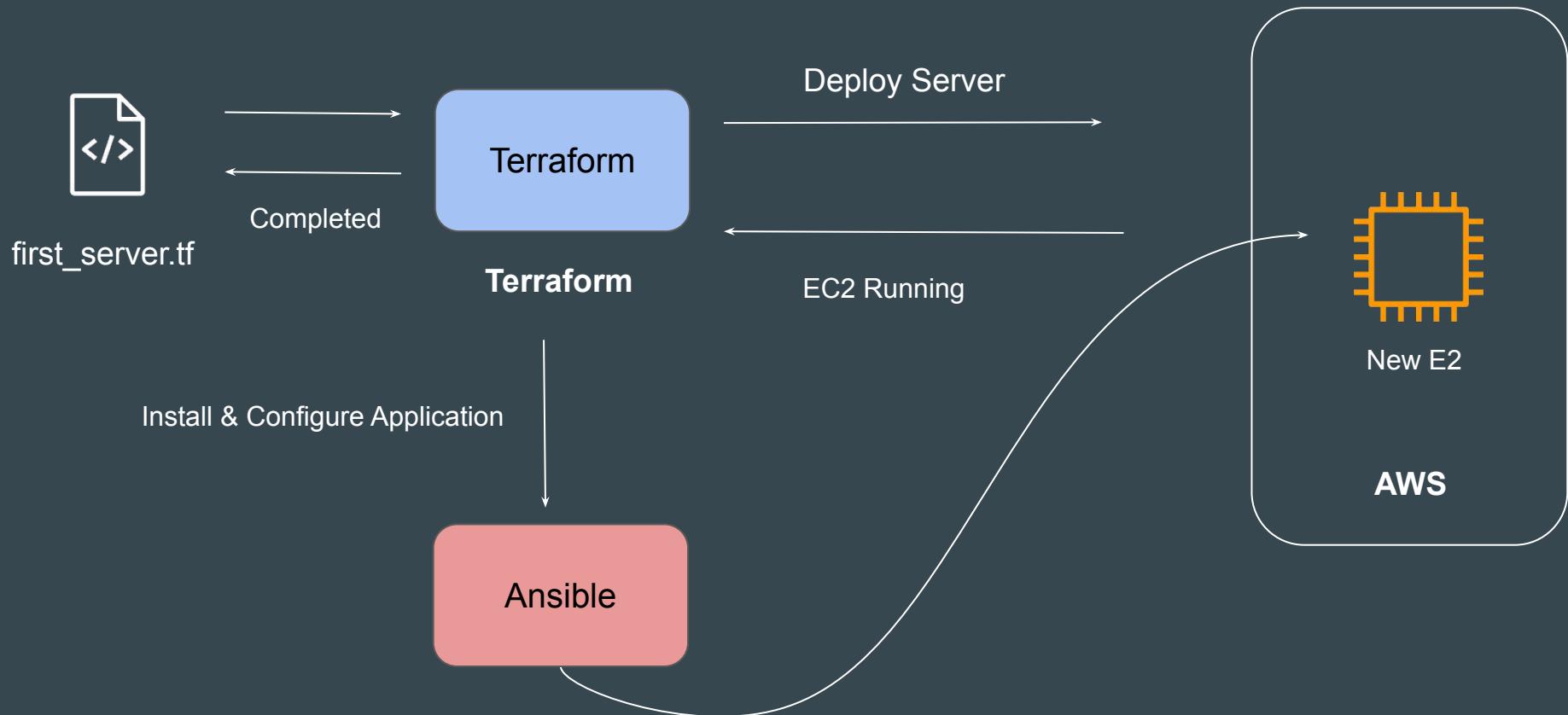
Infrastructure Orchestration is primarily used to create and manage infrastructure environments.

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

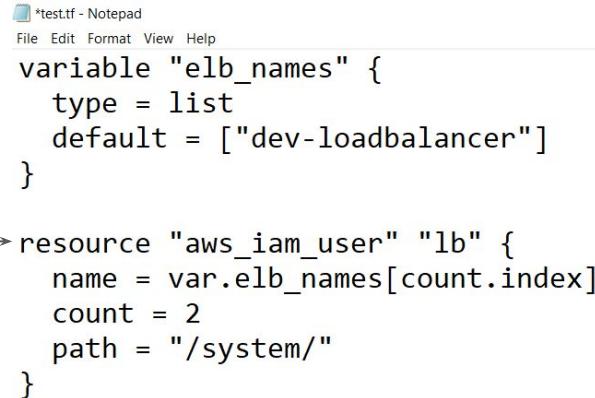
Terraform in detail

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.

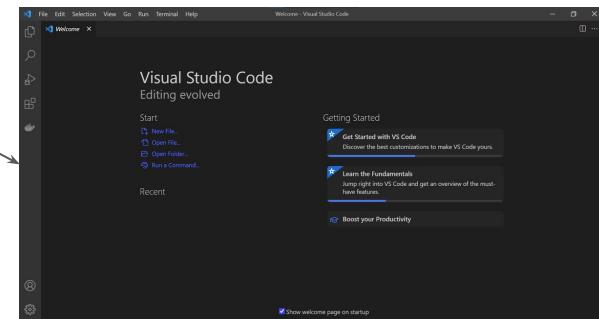


The screenshot shows the Atom code editor interface. On the left, the 'Project' sidebar lists a directory structure under 'samp-code': '.terraform', '.terraform.lock.hcl', 'kms-use-case-01.json', 'kms-use-case-02.json', 'kms-use-case-03.json', 'terraform.tfstate', 'terraform.tfstate.backup', and 'test.tf'.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

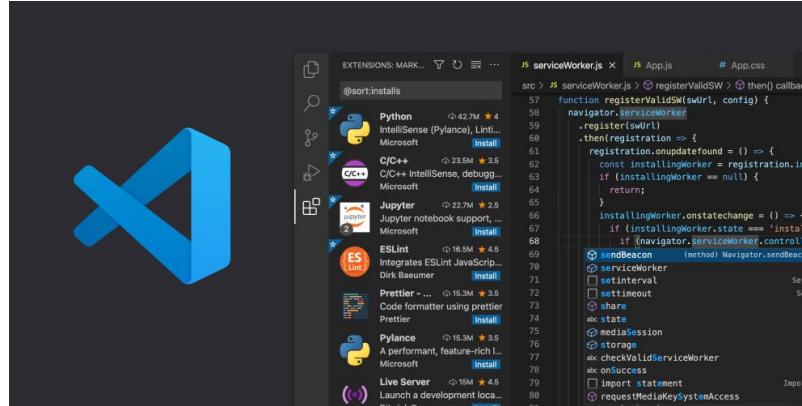


Editor for This Course

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

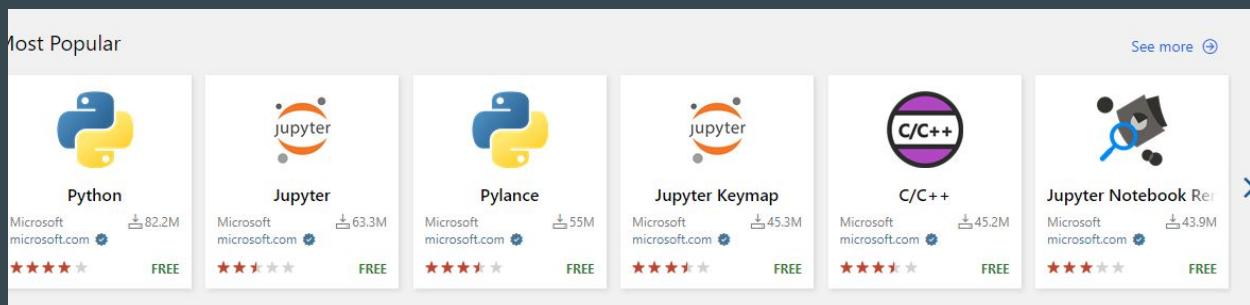
Using Visual Studio Code

Visual Studio Code Extensions

Understanding the Basics

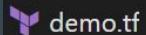
Extensions are add-ons that allow you to customize and enhance your experience in Visual Studio by adding new features or integrating existing tools

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, 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

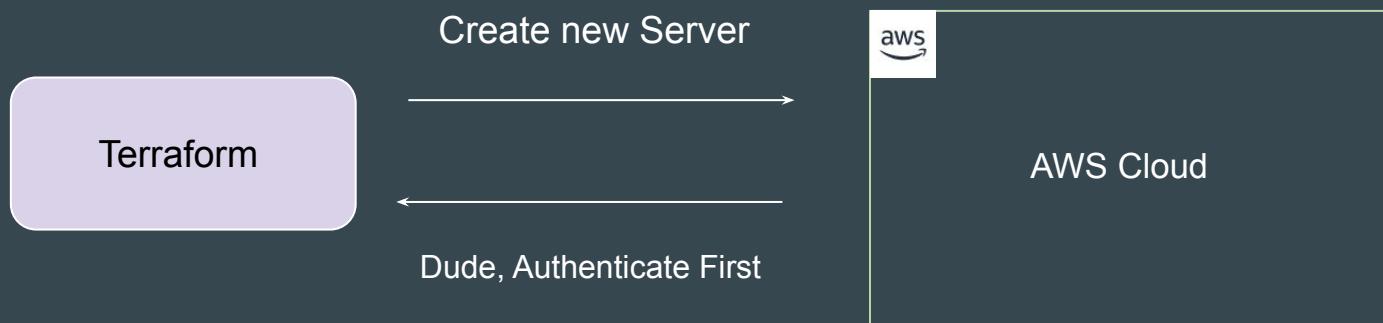
★ FEATURED 12 MONTHS FREE ALWAYS FREE TRIALS PRODUCT CATEGORIES ALL

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.

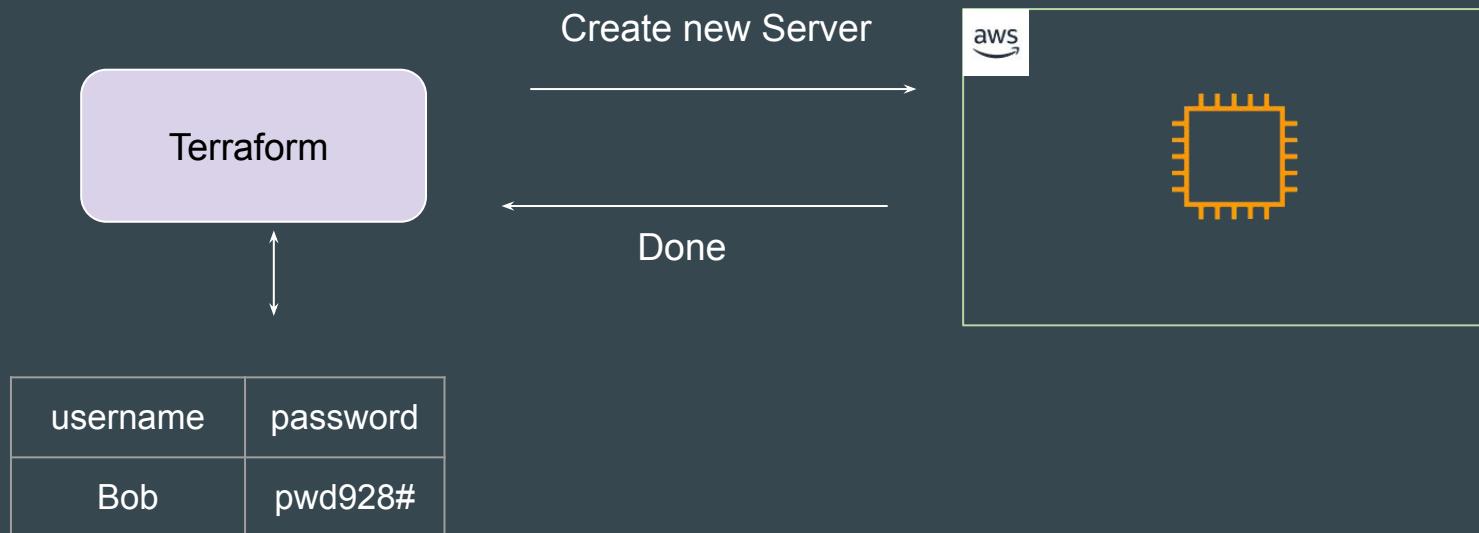
Authorization is the process of verifying what they have access to

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.

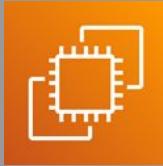


Access Credentials

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

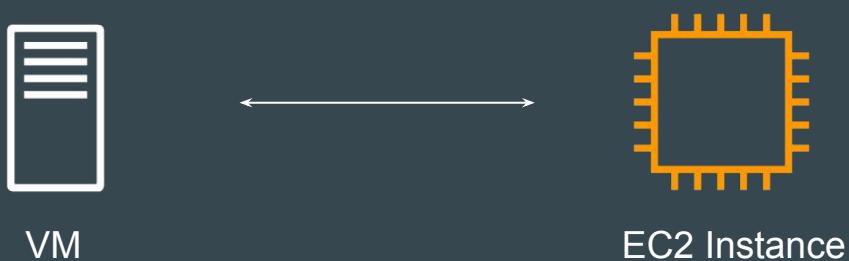
First Virtual Machine Through Terraform



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.



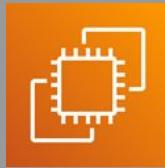
Virtual Machine Configuration

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"
}
```

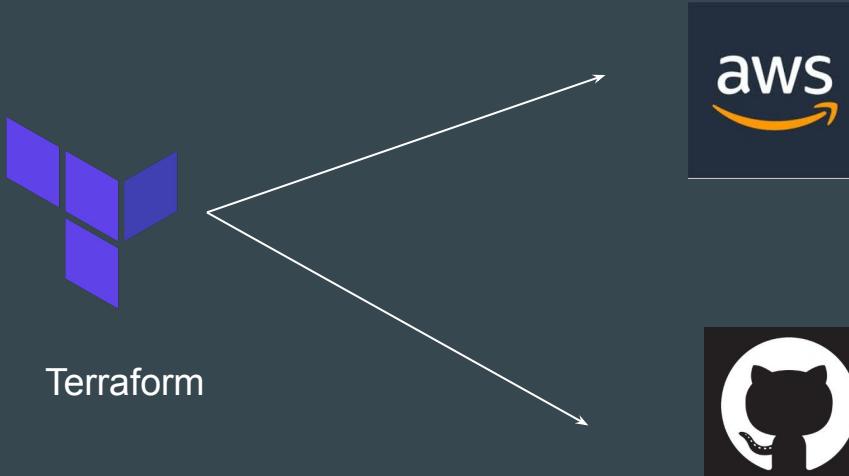
Non-HashiCorp Maintained

Terraform Destroy

Learning to Destroy Resources

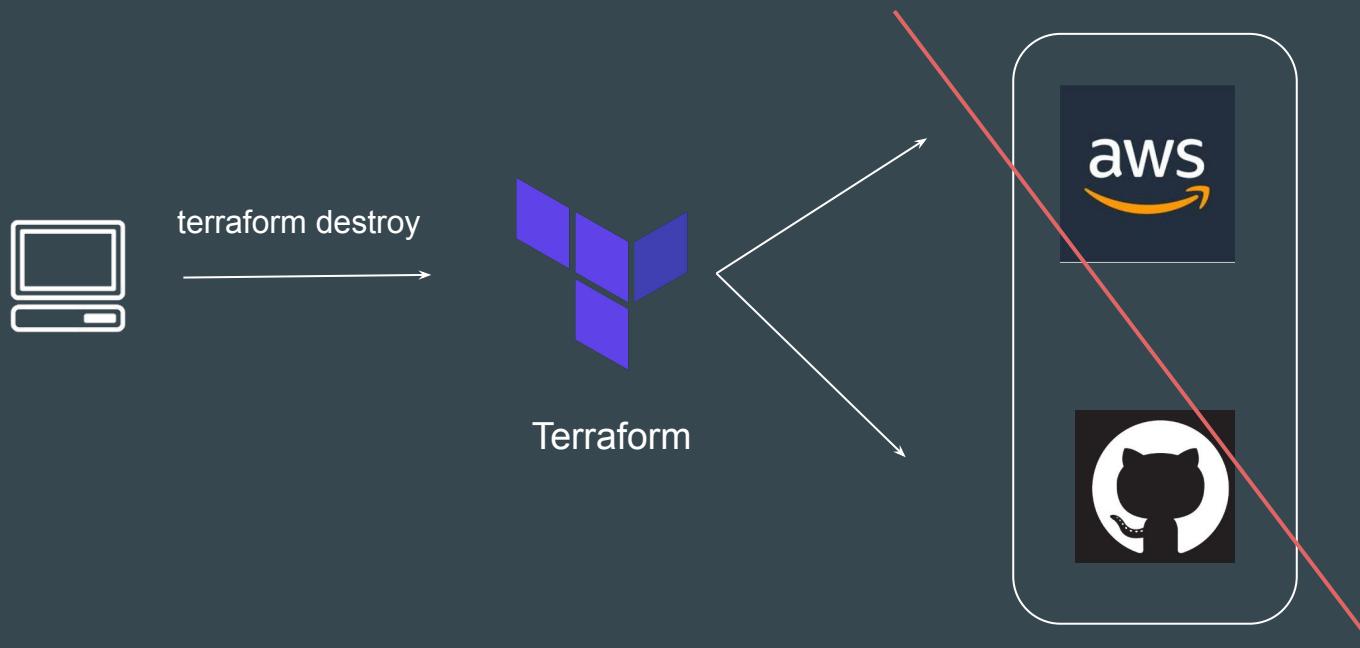
If you keep the infrastructure running, you will get charged for it.

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



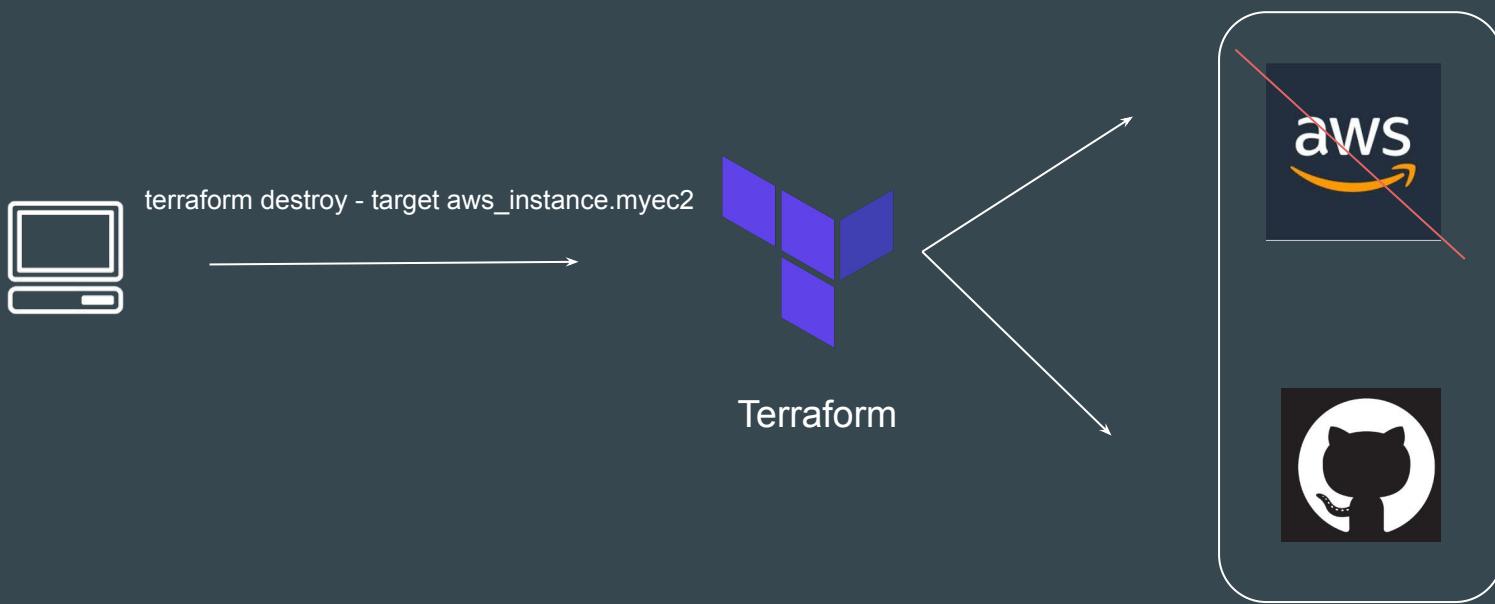
Approach 1 - Destroy ALL

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"  
}
```

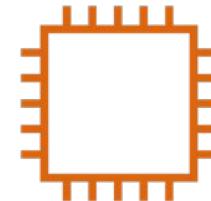
Desired & Current State

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.

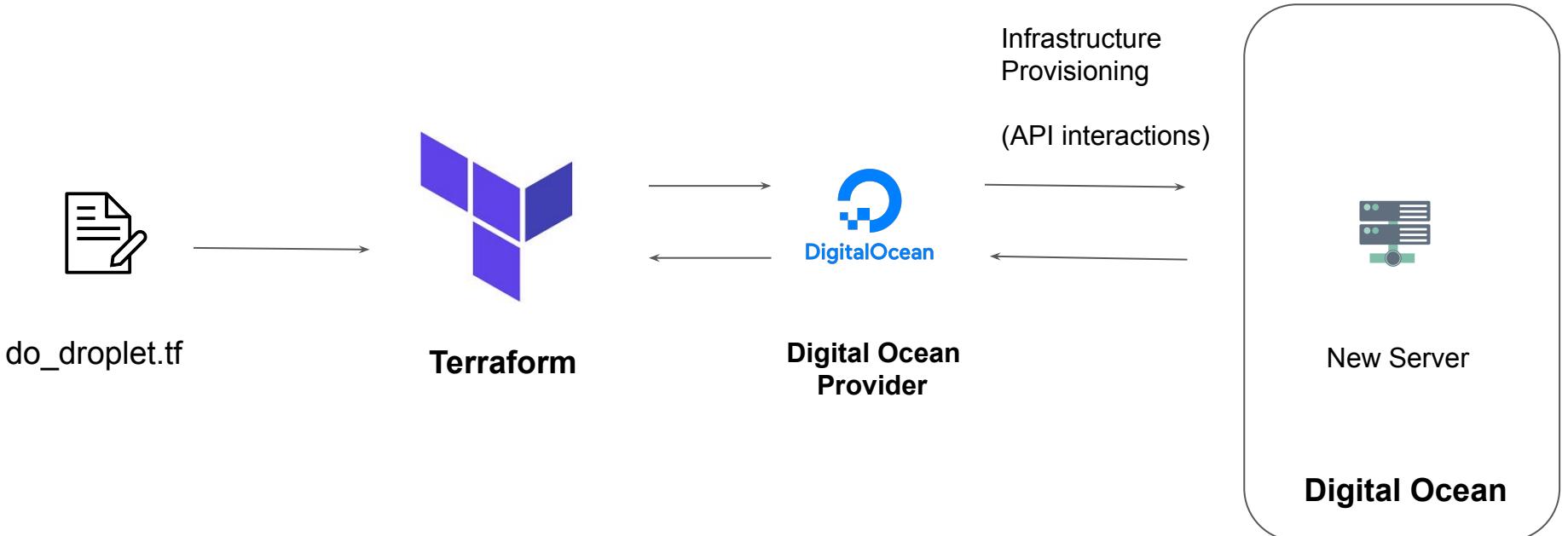
If there is a difference between the two, terraform plan presents a description of the changes necessary to achieve the desired state.



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



DigitalOcean

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.

Version Number Arguments	Description
<code>>=1.0</code>	Greater than equal to the version
<code><=1.0</code>	Less than equal to the version
<code>~>2.0</code>	Any version in the 2.X range.
<code>>=2.10,<=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:1ec08abba09e3e0547511d48f77a1e2c89face2d55886b23f643011c76cb247",
        "zh:606d134fef7c1357c9d155aadbee6826bc22bc0115b6291d483bc1444291c3e1",
        "zh:67e31a71a5ecbbc96a1a6708c9cc300bbfe921c322320cdbb95b9002026387e1",
```

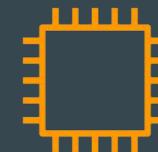
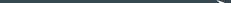
Terraform Refresh

Understanding the Challenge

Terraform can create an infrastructure based on configuration you specified.

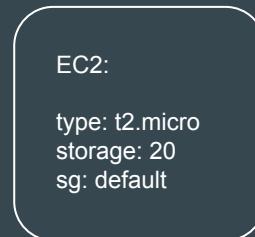
It can happen that the infrastructure gets modified manually.

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



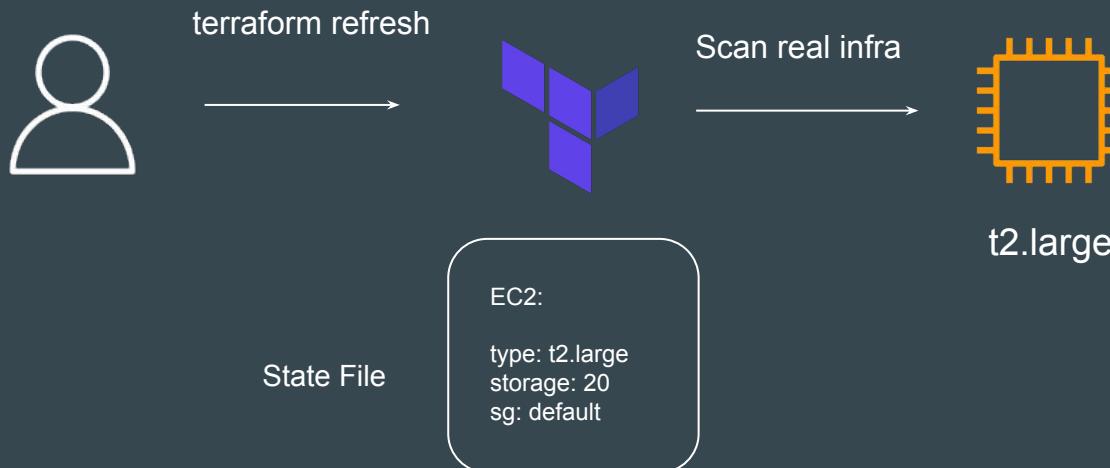
t2.micro

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...Z5QJI"
    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.

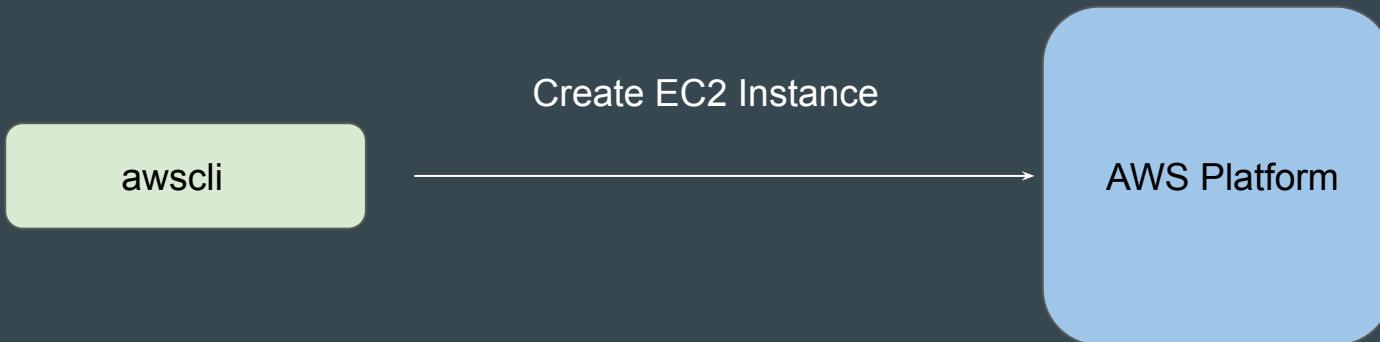
```
VS Code aws-provider-config.tf > ...
provider "aws" {
    region      = "us-east-1"
}

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	Understanding Attributes and Output Values in Terraform
2	Referencing Cross-Account Resource Attributes
3	Terraform Variables
4	Approaches for Variable Assignment
5	Data Types for Variables

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.

The screenshot shows the AWS All Services search interface. On the left, a sidebar lists 'Recently visited', 'Favorites', and 'All services' (which is highlighted in orange). Below this are various service categories with corresponding icons: Analytics, Application Integration, Blockchain, Business Applications, Cloud Financial Management, Compute, Containers, Customer Enablement, Database, Developer Tools, End User Computing, and Front-end Web & Mobile. The main panel displays search results starting with the letter 'A'. Each result includes an icon, the service name, and a brief description. The results are: **Activate for Startups** (AWS Activate provides resources to help startups build and grow on AWS.), **AWS Amplify** (AWS Amplify is a complete platform—frameworks & tools and app services—for developing, building, testing, and running mobile and web apps), **API Gateway** (Build, Deploy and Manage APIs), **AWS App Mesh** (Easily monitor and control microservices), **AWS App Runner** (Build and run production web applications at scale), and **AWS AppConfig** (Use feature flags, operational flags, and other runtime configuration to make changes quickly and safely on production).

Recently visited

Favorites

All services

Analytics

Application Integration

Blockchain

Business Applications

Cloud Financial Management

Compute

Containers

Customer Enablement

Database

Developer Tools

End User Computing

Front-end Web & Mobile

All services

X

A

View all services

All AWS services organized by category on a page

Activate for Startups

AWS Activate provides resources to help startups build and grow on AWS.

AWS Amplify

AWS Amplify is a complete platform—frameworks & tools and app services—for developing, building, testing, and running mobile and web apps

API Gateway

Build, Deploy and Manage APIs

AWS App Mesh

Easily monitor and control microservices

AWS App Runner

Build and run production web applications at scale

AWS AppConfig

Use feature flags, operational flags, and other runtime configuration to make changes quickly and safely on production

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.

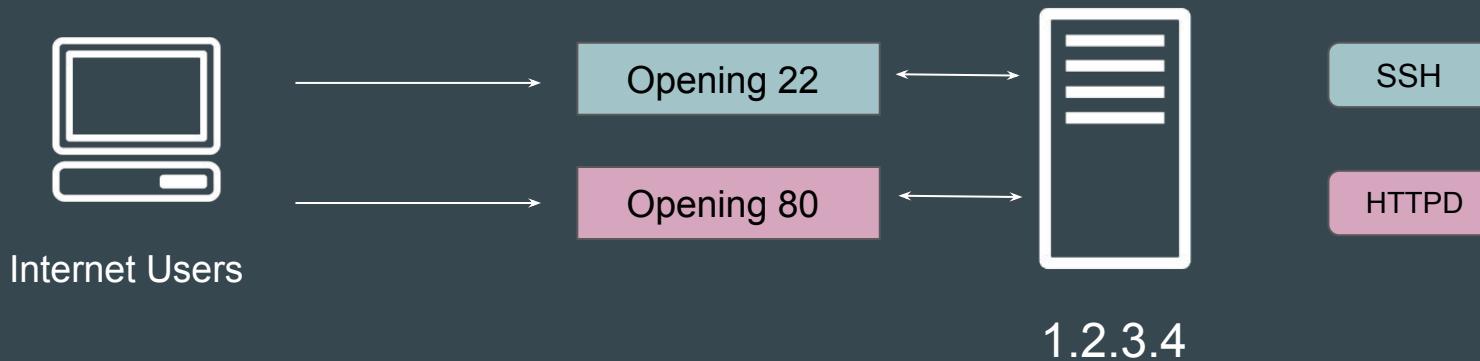
Example - Creating Firewall Through Terraform

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

Basics of Firewalls

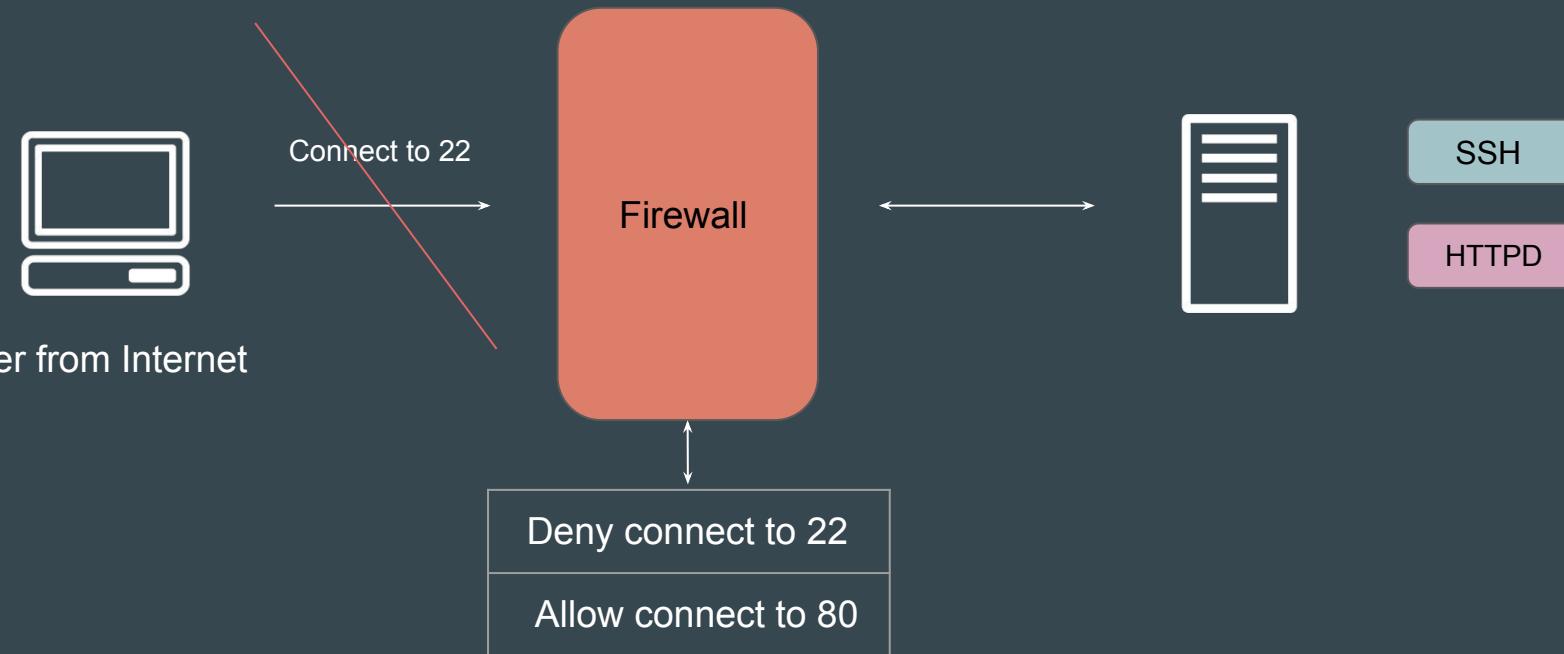
Basics of Ports

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



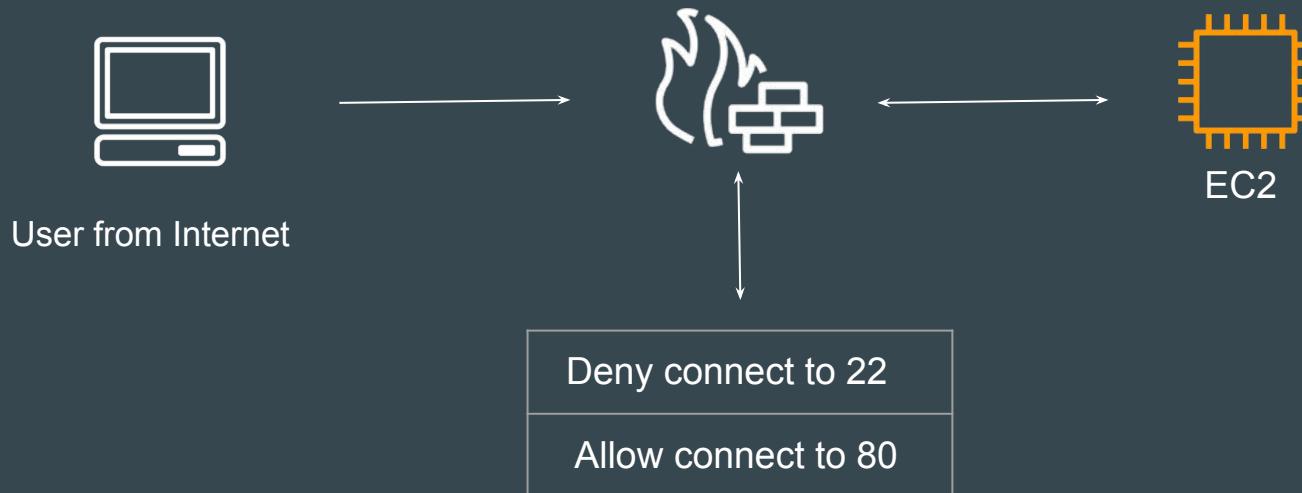
Basics of Firewall

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 demo-firewall	Security group ID sg-0fcf94c6fff3977b2	Description Demo Purpose	VPC ID vpc-050f222846f400045
Owner 042025557788	Inbound rules count 3 Permission entries	Outbound rules count 1 Permission entry	

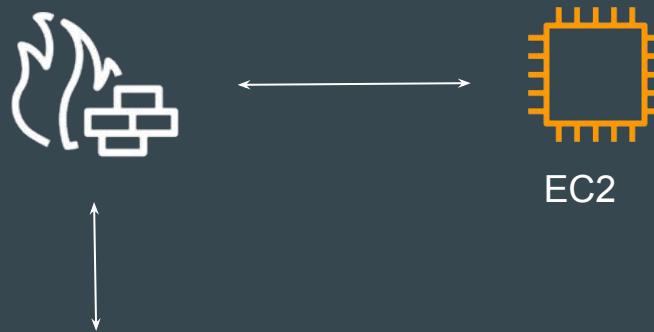
[Inbound rules](#) [Outbound rules](#) [Tags](#)

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

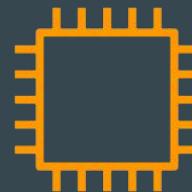
Basics of Elastic IP in AWS

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

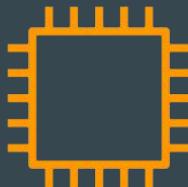
We are going to use Terraform to generate Elastic IP resource in AWS.

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

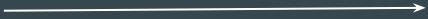
```
VSCode eip.tf > ...
resource "aws_eip" "lb" {
  domain    = "vpc"
}
```

```
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]

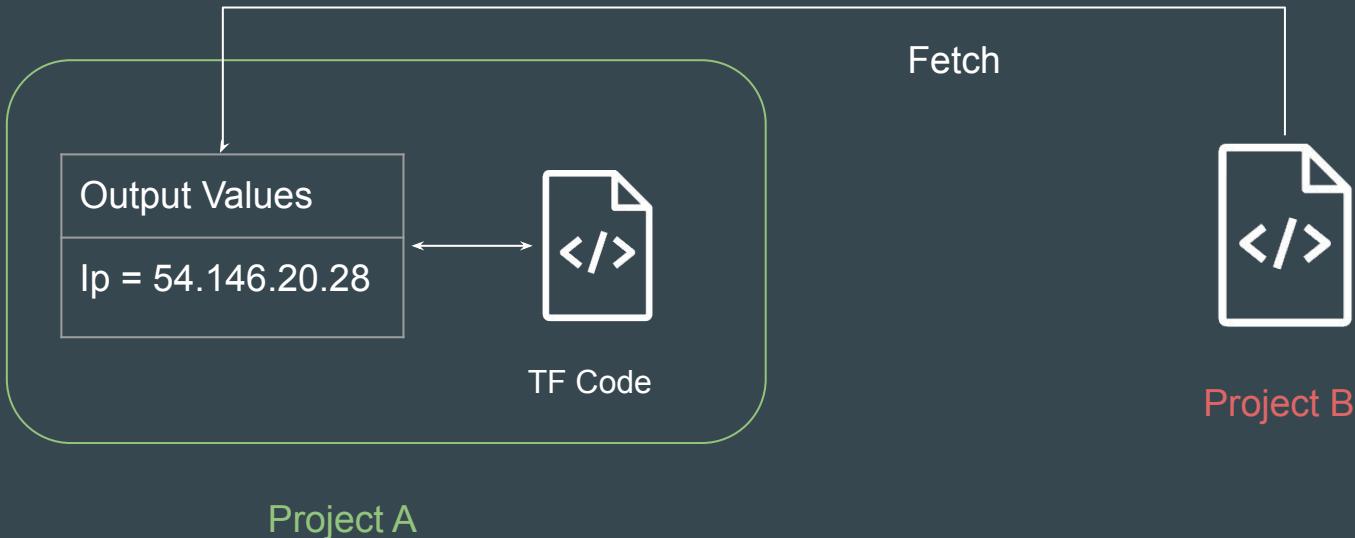
Apply complete! Resources: 1 added, 0 changed, 0 destroyed.

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" {}
```

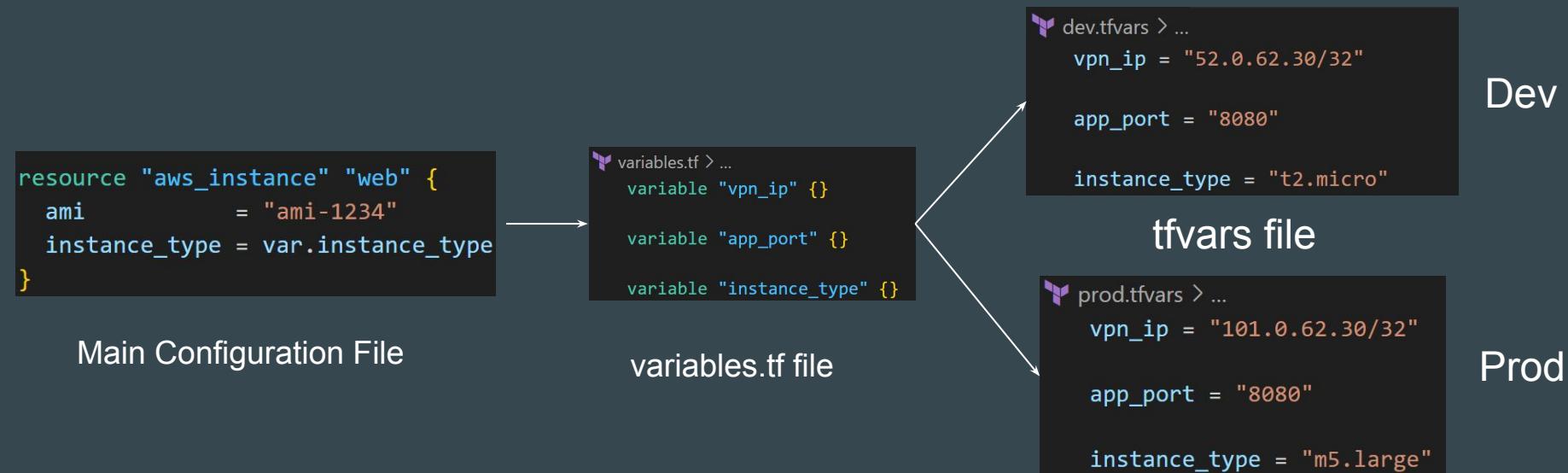
variables.tf File

```
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.

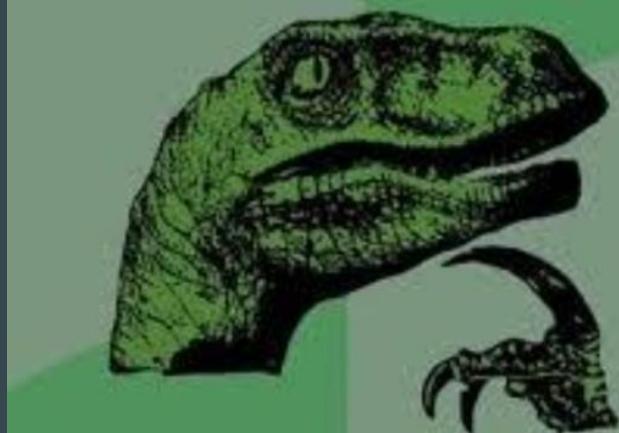
```
resource "aws_instance" "web" {  
    ami           = "ami-1234"  
    instance_type = var.instance_type  
}
```

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:

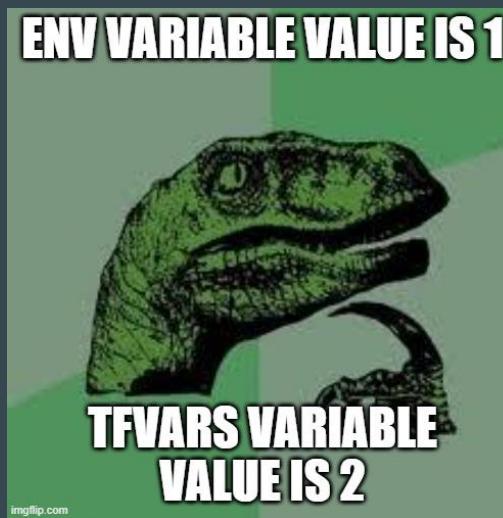
# aws_instance.web will be created
+ resource "aws_instance" "web" {
    + ami                                = "ami-1234"
    + arn                                = (known after apply)
    + associate_public_ip_address        = (known after apply)
    + availability_zone                  = (known after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

Count Parameter

Terraform in detail

Overview of Count Parameter

The count parameter on resources can simplify configurations and let you scale resources by simply incrementing a number.

Let's assume, you need to create two EC2 instances. One of the common approach is to define two separate resource blocks for aws_instance.

```
resource "aws_instance" "instance-1" {  
    ami = "ami-082b5a644766e0e6f"  
    instance_type = "t2.micro"  
}
```



```
resource "aws_instance" "instance-2" {  
    ami = "ami-082b5a644766e0e6f"  
    instance_type = "t2.micro"  
}
```

Overview of Count Parameter

With count parameter, we can simply specify the count value and the resource can be scaled accordingly.

```
resource "aws_instance" "instance-1" {
    ami = "ami-082b5a644766e0e6f"
    instance_type = "t2.micro"
    count = 5
}
```

Count Index

In resource blocks where count is set, an additional count object is available in expressions, so you can modify the configuration of each instance.

This object has one attribute:

count.index — The distinct index number (starting with 0) corresponding to this instance.

Understanding Challenge with Count

With the below code, terraform will create 5 IAM users. But the problem is that all will have the same name.

```
resource "aws_iam_user" "lb" {
    name = "loadbalancer"
    count = 5
    path = "/system/"
}
```

Understanding Challenge with Count

count.index allows us to fetch the index of each iteration in the loop.

```
resource "aws_iam_user" "lb" {
    name = "loadbalancer.${count.index}"
    count = 5
    path = "/system/"
}
```

Understanding Challenge with Default Count Index

Having a username like loadbalancer0, loadbalancer1 might not always be suitable.

Better names like dev-loadbalancer, stage-loadbalancer, prod-loadbalancer is better.

count.index can help in such scenario as well.

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

Conditional Expression

Terraform in detail

Overview of Conditional Expression

A conditional expression uses the value of a bool expression to select one of two values.

Syntax of Conditional expression:

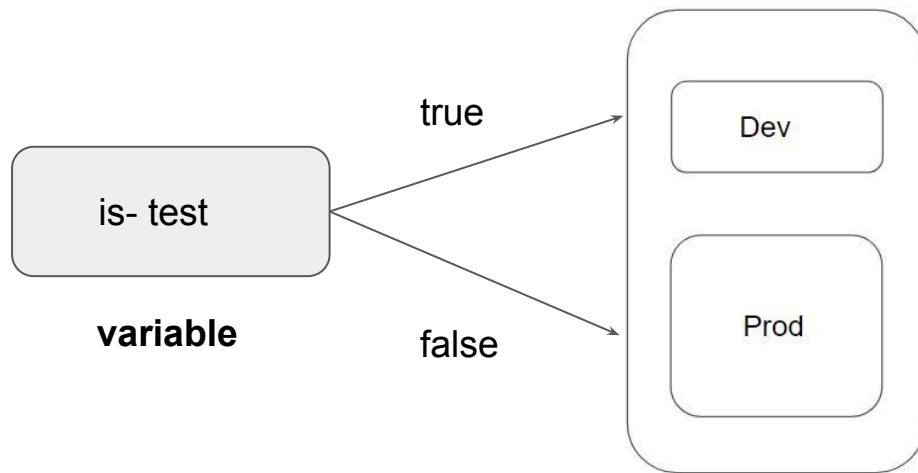
```
condition ? true_val : false_val
```

If condition is true then the result is true_val. If condition is false then the result is false_val.

Example of Conditional Expression

Let's assume that there are two resource blocks as part of terraform configuration.

Depending on the variable value, one of the resource blocks will run.



Local Values

Terraform in detail

Overview of Local Values

A local value assigns a name to an expression, allowing it to be used multiple times within a module without repeating it.

```
locals {  
    common_tags = {  
        Owner = "DevOps Team"  
        service = "backend"  
    }  
}
```

```
resource "aws_instance" "app-dev" {  
    ami = "ami-082b5a644766e0e6f"  
    instance_type = "t2.micro"  
    tags = local.common_tags  
}
```

```
resource "aws_ebs_volume" "db_ebs" {  
    availability_zone = "us-west-2a"  
    size              = 8  
    tags = local.common_tags  
}
```

Local Values Support for Expression

Local Values can be used for multiple different use-cases like having a conditional expression.

```
locals {
    name_prefix = "${var.name != "" ? var.name : var.default}"
}
```

Important Pointers for Local Values

Local values can be helpful to avoid repeating the same values or expressions multiple times in a configuration.

If overused they can also make a configuration hard to read by future maintainers by hiding the actual values used

Use local values only in moderation, in situations where a single value or result is used in many places and that value is likely to be changed in future.

Terraform Functions

Terraform in detail

Overview of Terraform Functions

The Terraform language includes a number of built-in functions that you can use to transform and combine values.

The general syntax for function calls is a function name followed by comma-separated arguments in parentheses:

function (argument1, argument2)

Example:

```
> max(5, 12, 9)
```

```
12
```

List of Available Functions

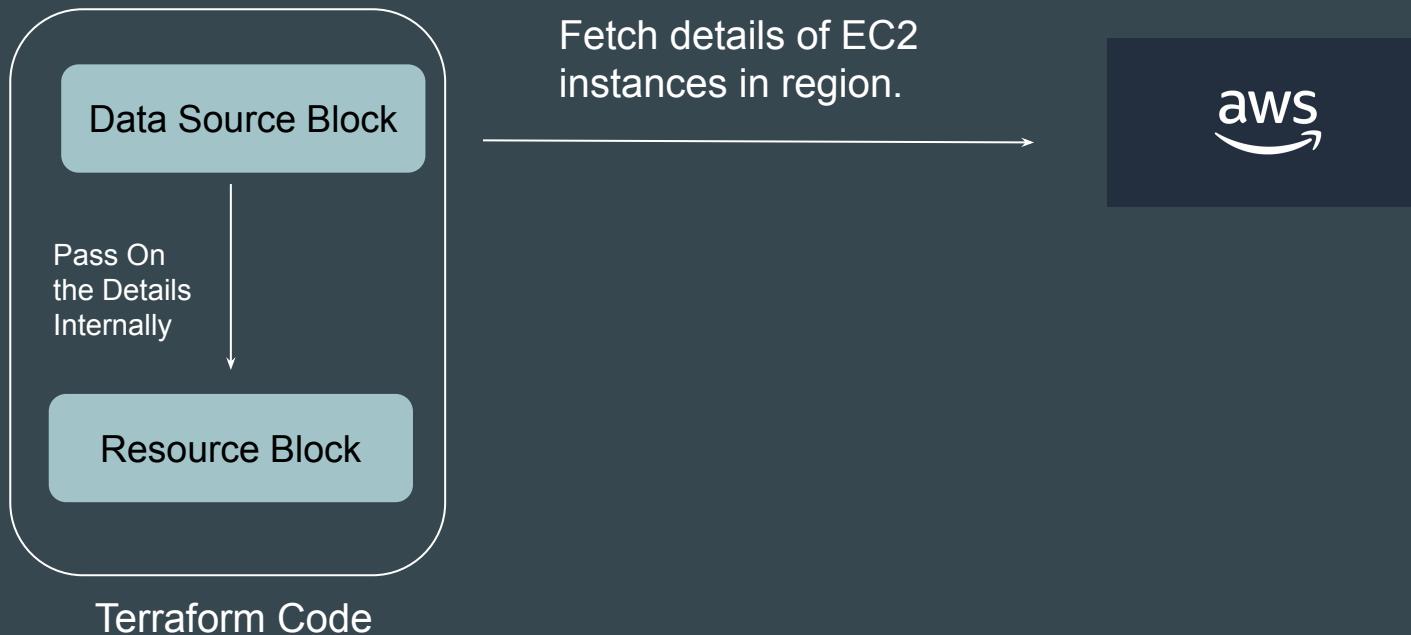
The Terraform language does not support user-defined functions, and so only the functions built in to the language are available for use

- Numeric
- String
- Collection
- Encoding
- Filesystem
- Date and Time
- Hash and Crypto
- IP Network
- Type Conversion

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

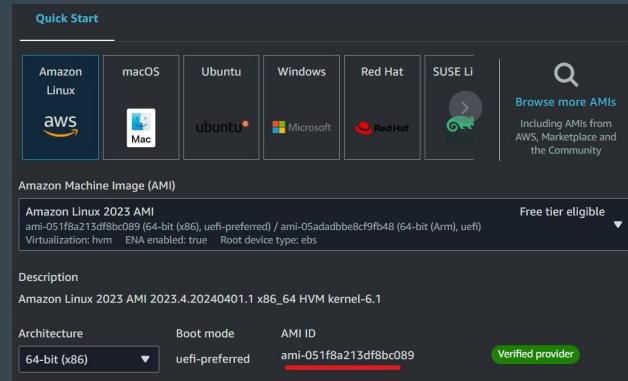
You have been given a requirement to write a Terraform code that creates EC2 instance using latest OS Image of Amazon Linux.

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

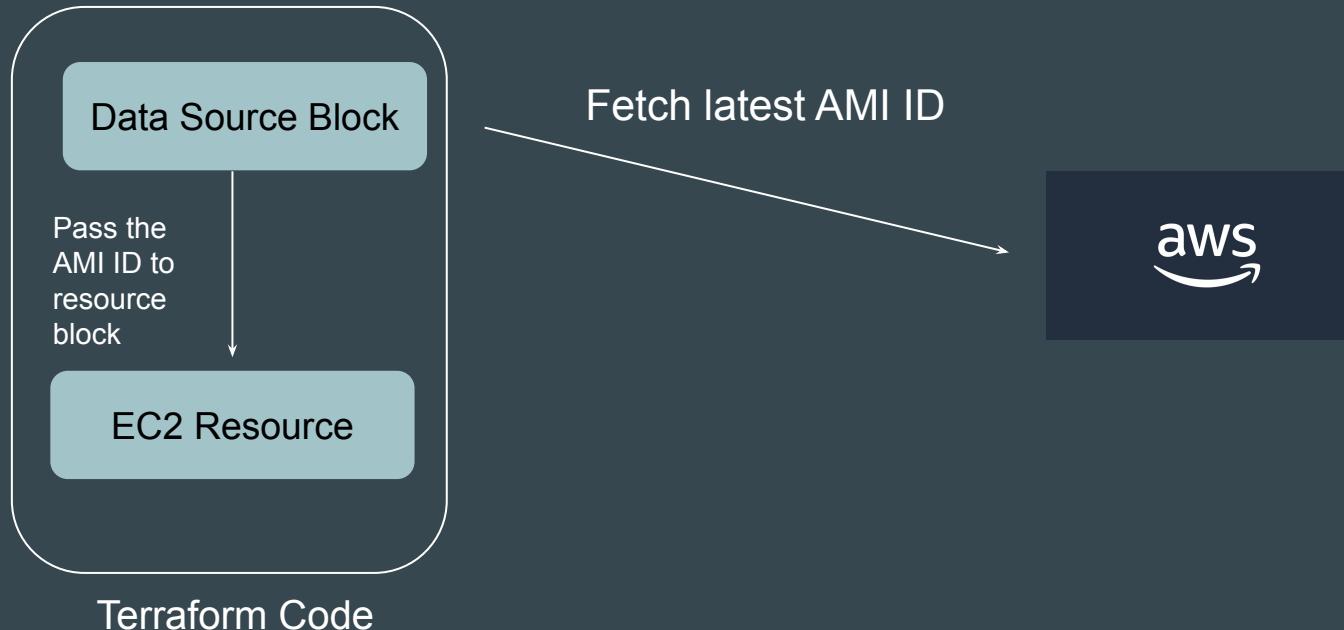
We want Terraform to automatically query the latest OS image in AWS or any other provider and use that for creating server.

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

Terraform in detail

Overview of Debugging Terraform

Terraform has detailed logs which 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

```
bash-4.2# terraform plan
2020/04/22 13:45:31 [INFO] Terraform version: 0.12.24
2020/04/22 13:45:31 [INFO] Go runtime version: go1.12.13
2020/04/22 13:45:31 [INFO] CLI args: []string{"/usr/bin/terraform", "plan"}
2020/04/22 13:45:31 [DEBUG] Attempting to open CLI config file: /root/.terraformrc
2020/04/22 13:45:31 [DEBUG] File doesn't exist, but doesn't need to. Ignoring.
2020/04/22 13:45:31 [DEBUG] checking for credentials in "/root/.terraform.d/plugins"
2020/04/22 13:45:31 [INFO] CLI command args: []string{"plan"}
2020/04/22 13:45:31 [TRACE] Meta.Backend: built configuration for "s3" backend with hash value 789489680
2020/04/22 13:45:31 [TRACE] Meta.Backend: backend has not previously been initialized in this working directory
2020/04/22 13:45:31 [DEBUG] New state was assigned lineage "a10f92bf-686d-e6cf-3e9d-755be5c8a6a3"
2020/04/22 13:45:31 [TRACE] Meta.Backend: moving from default local state only to "s3" backend
```

Important Pointers

TRACE is the most verbose and it is the default if TF_LOG is set to something other than a log level name.

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.

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	Understanding Attributes and Output Values in Terraform
2	Referencing Cross-Account Resource Attributes
3	Terraform Variables
4	Approaches for Variable Assignment
5	Data Types for Variables

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

Do you have a special talent?

Me:



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.
```

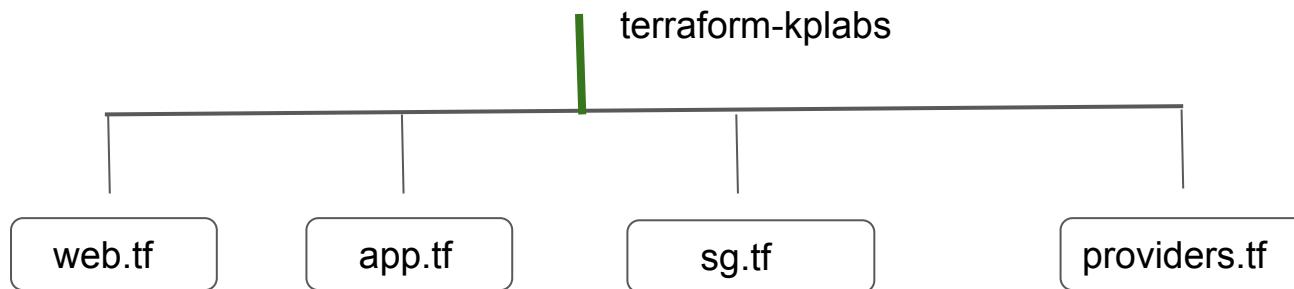
Load Order & Semantics

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

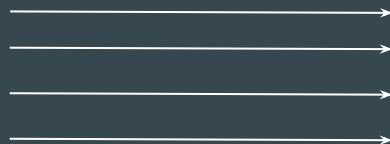
You have created a new resource via Terraform.

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

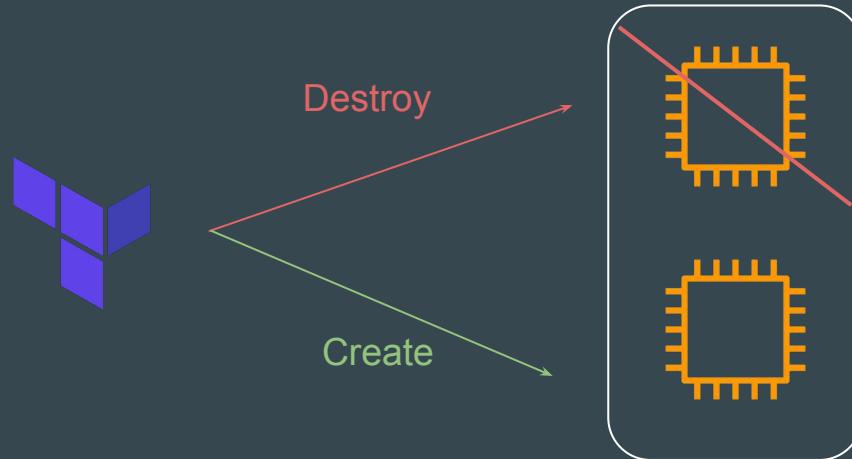


Terraform Managed Resource

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
}
```

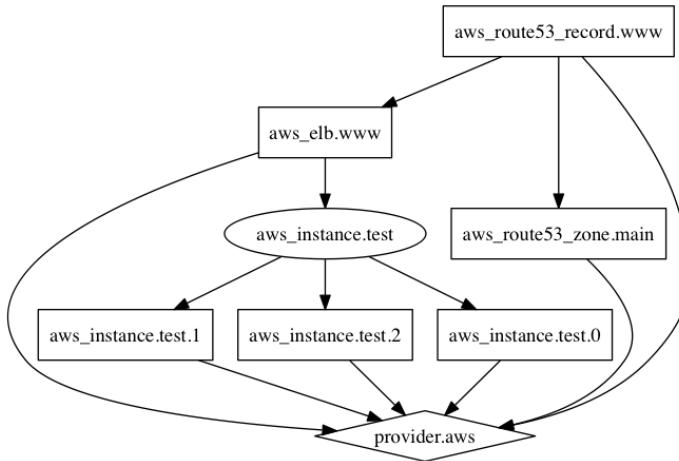
Terraform Graph

Terraform In Detail

Overview of Graph

The `terraform graph` command is used to generate a visual representation of either a configuration or execution plan

The output of `terraform graph` is in the DOT format, which can easily be converted to an image.



Saving Terraform Plan to a File

Terraform In Detail

Terraform Plan File

The generated terraform plan can be saved to a specific path.

This plan can then be used with terraform apply to be certain that only the changes shown in this plan are applied.

Example:

```
terraform plan -out=path
```

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 output>terraform output iam_names
[
  "iamuser.0",
  "iamuser.1",
  "iamuser.2",
]
```

Terraform Settings

Terraform in detail

Overview of Terraform Settings

The special `terraform` configuration block type is used to configure some behaviors of Terraform itself, such as requiring a minimum Terraform version to apply your configuration.

Terraform settings are gathered together into `terraform` blocks:

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

Setting 1 - Terraform Version

The `required_version` setting accepts a version constraint string, which specifies which versions of Terraform can be used with your configuration.

If the running version of Terraform doesn't match the constraints specified, Terraform will produce an error and exit without taking any further actions.

```
terraform {  
    required_version = "> 0.12.0"  
}
```

Setting 2 - Provider Version

The `required_providers` block specifies all of the providers required by the current module, mapping each local provider name to a source address and a version constraint.

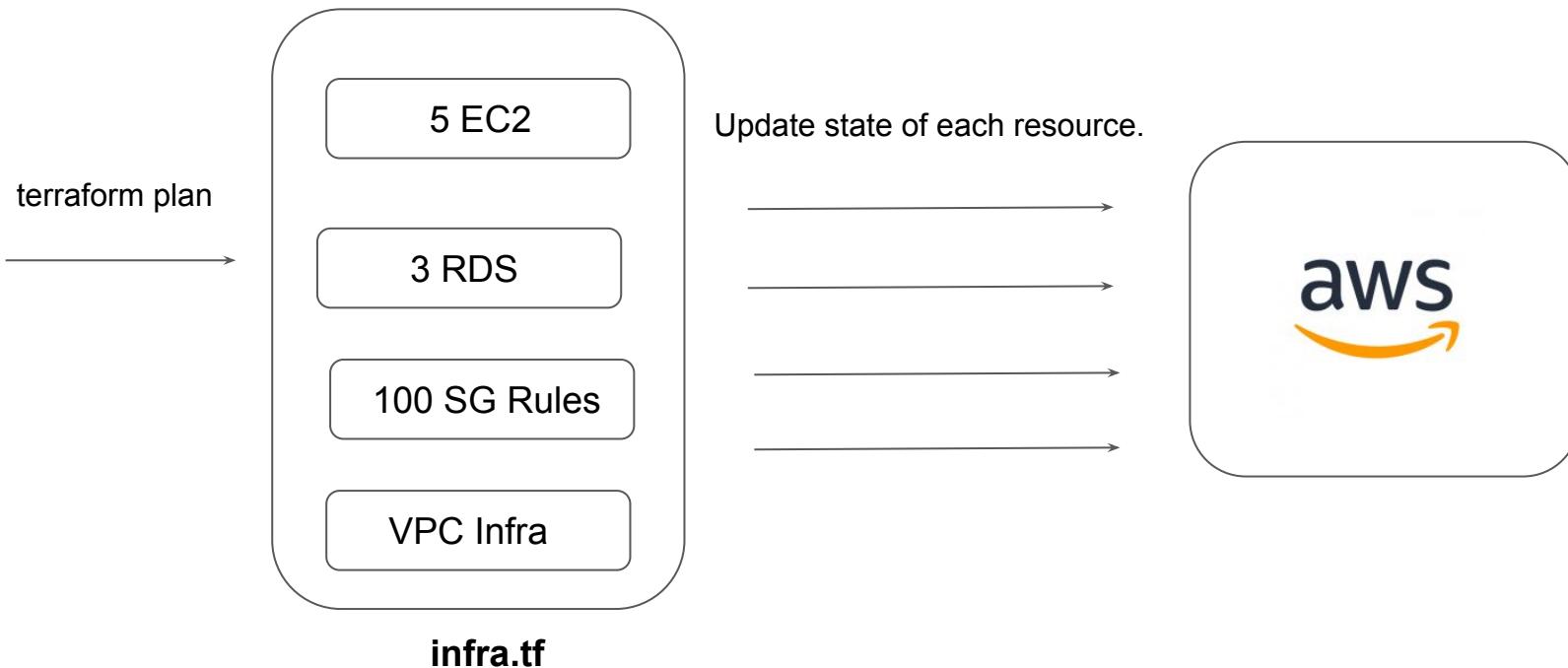
```
terraform {
  required_providers {
    mycloud = {
      source  = "mycorp/mycloud"
      version = "~> 1.0"
    }
  }
}
```

Dealing with Larger Infrastructure

Terraform in detail

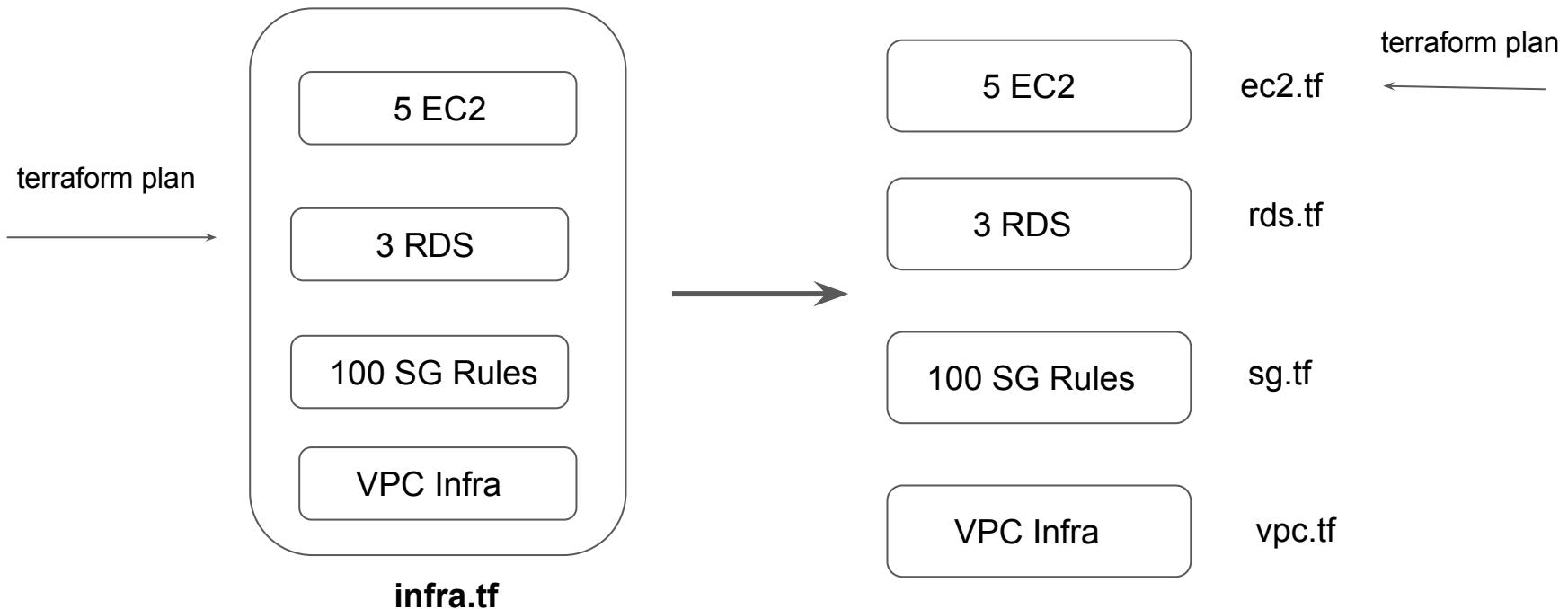
Challenges with Larger Infrastructure

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.

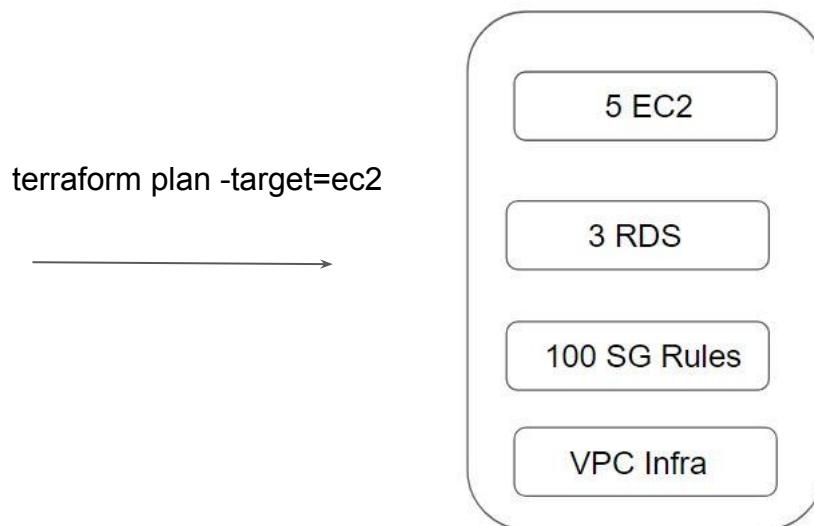
This can be achieved with the [-refresh=false flag](#)



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

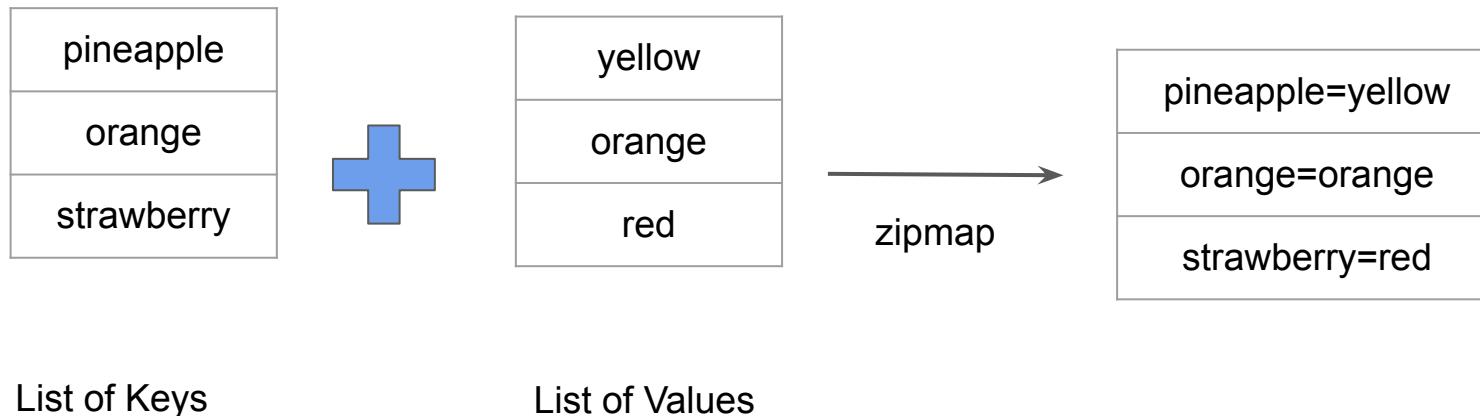


Zipmap

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.

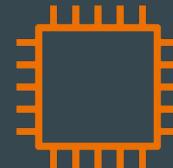
Understanding the Limitations

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" {
    # ...

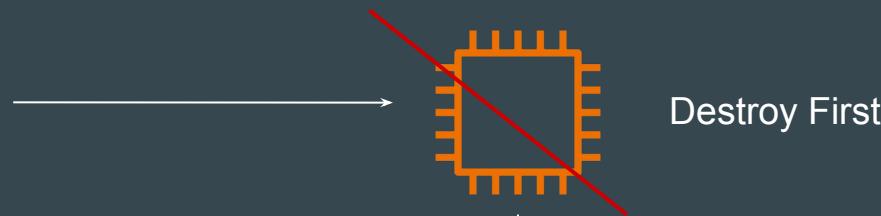
    lifecycle {
        replace_triggered_by = [
            # Replace `aws_appautoscaling_target` each time this instance of
            # the `aws_ecs_service` is replaced.
            aws_ecs_service.svc.id
        ]
    }
}
```

Create Before Destroy Argument

Understanding the Default Behavior

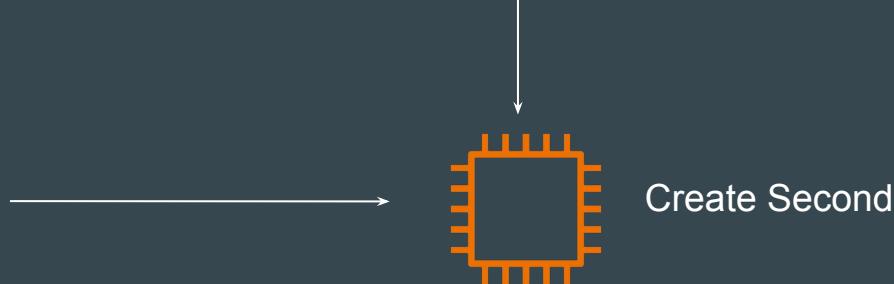
By default, when Terraform must change a resource argument that cannot be updated in-place due to remote API limitations, Terraform will instead destroy the existing object and then create a new replacement object with the new configured arguments.

```
🦄 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"
}
```



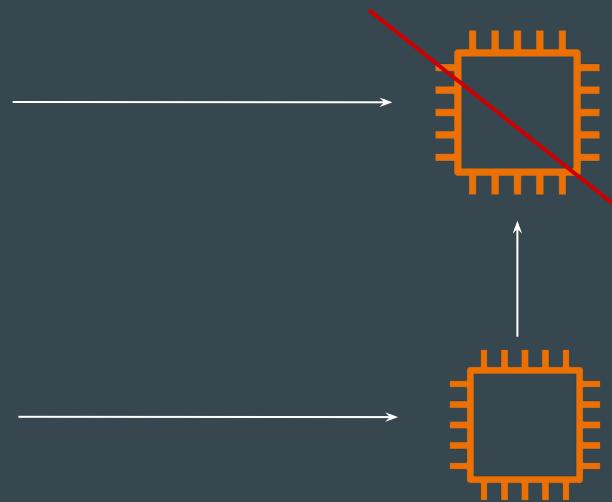
Create Before Destroy Argument

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  
    }  
}
```

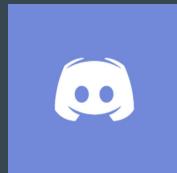


Destroy Second

Create First

Join us in our Adventure

Be Awesome



kplabs.in/chat



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/"
```



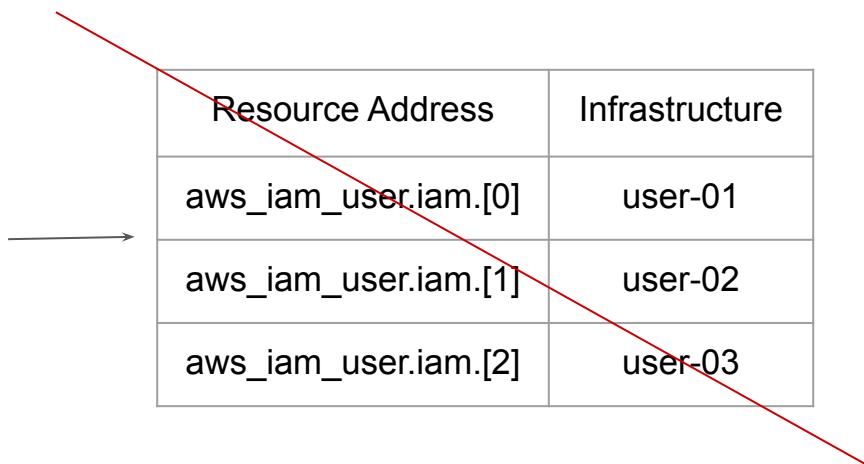
Resource Address	Infrastructure
aws_iam_user.iam[0]	user-01
aws_iam_user.iam[1]	user-02
aws_iam_user.iam[2]	user-03

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"
}
```

Data Type - SET

Let's Revise Programming

Basics of List

- Lists are used to store multiple items in a single variable.
- List items are ordered, changeable, and allow duplicate values.
- List items are indexed, the first item has index [0], the second item has index [1] etc.

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

Understanding SET

- SET is used to store multiple items in a single variable.
- SET items are unordered and no duplicates allowed.

Allowed

```
demoset = {"apple", "banana", "mango"}
```

Not-Allowed

```
demoset = {"apple", "banana", "mango", "apple"}
```

toset Function

toset function will convert the list of values to SET

```
> toset(["a", "b", "c","a"])
toset([
  "a",
  "b",
  "c",
])
```

for_each

Meta-Argument

Basics of For Each

for_each makes use of map/set as an index value of the created resource.

```
resource "aws_iam_user" "iam" {
  for_each = toset( ["user-01","user-02", "user-03"] )
  name      = each.key
}
```



Resource Address	Infrastructure
aws_iam_user.iam[user-01]	user-01
aws_iam_user.iam[user-02]	user-02
aws_iam_user.iam[user-03]	user-03

Replication Count Challenge

If a new element is added, it will not affect the other resources.

```
resource "aws_iam_user" "iam" {  
    for_each = toset( ["user-0","user-01","user-02", "user-03"] )  
    name      = each.key  
}
```

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

The each object

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

This 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

Relax and Have a Meme Before Proceeding

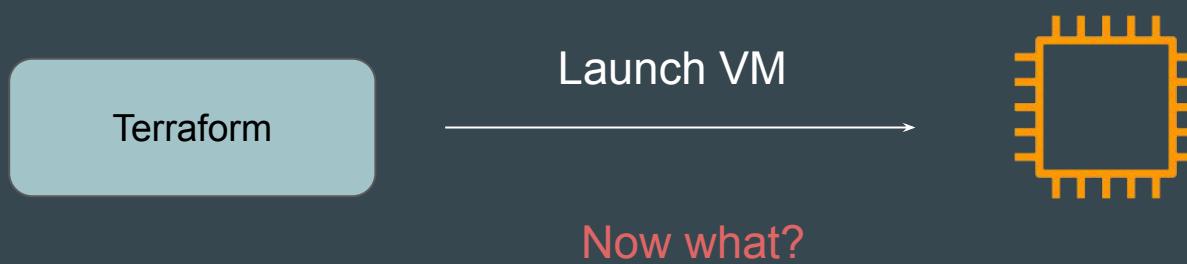


Terraform Provisioners

Setting the Base

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

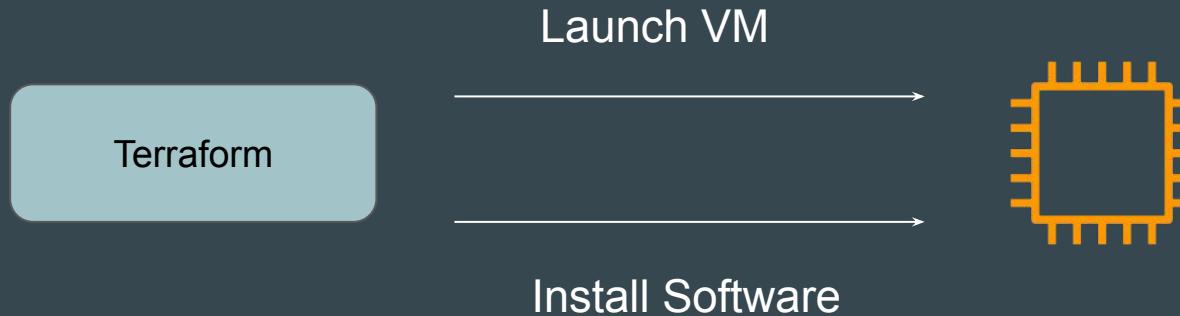
Organizations would want end-to-end solution for creation of infrastructure and configuring appropriate packages required for the application.



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.

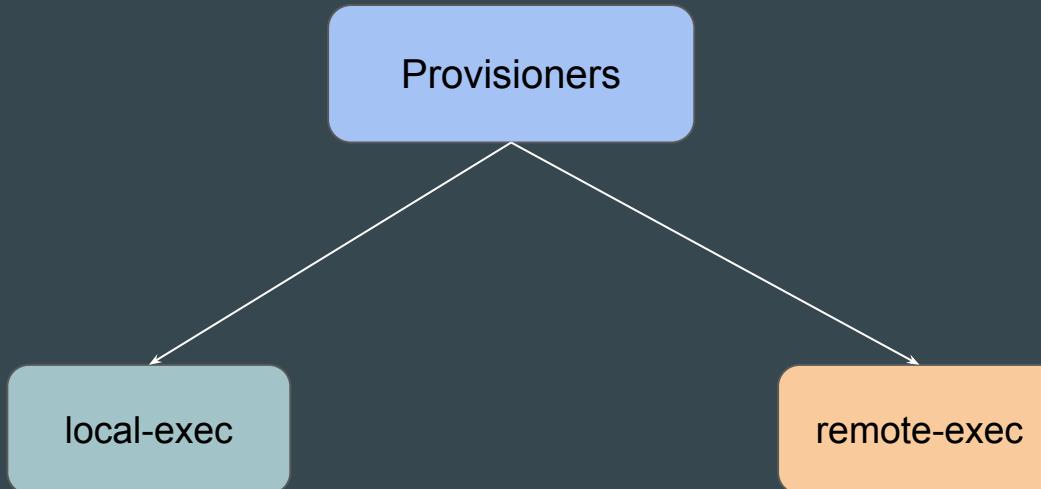


Types of Provisioners in Terraform

Setting the Base

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

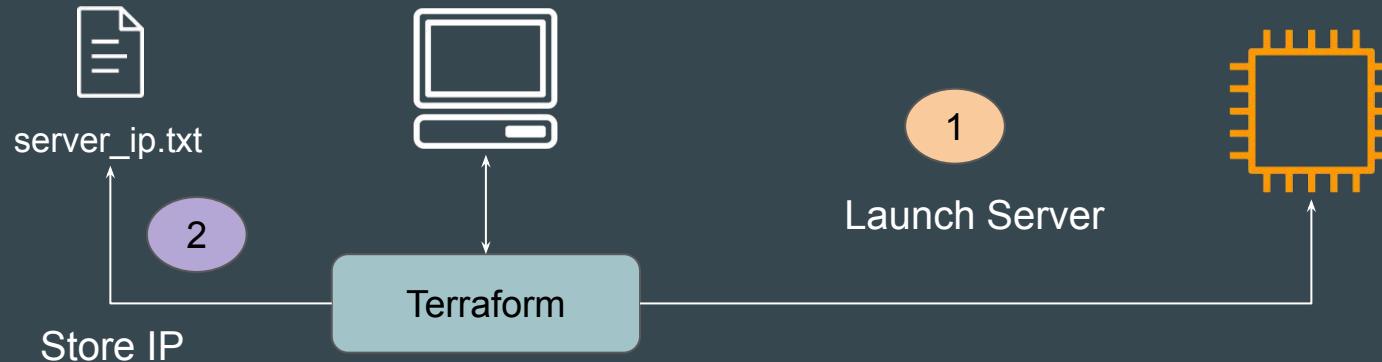
There are 2 major types of provisioners available



Type 1 - local-exec provisioner

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

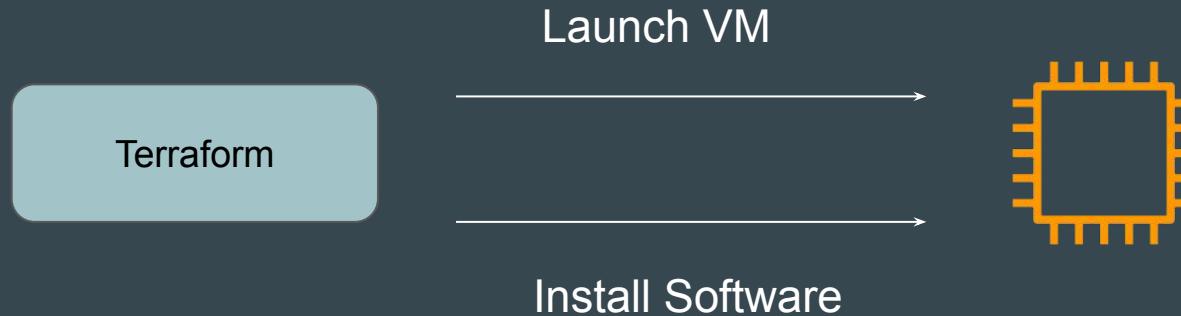
Example: After EC2 is launched, fetch the IP and store it in file `server_ip.txt`



Type 2 - remote-exec provisioner

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

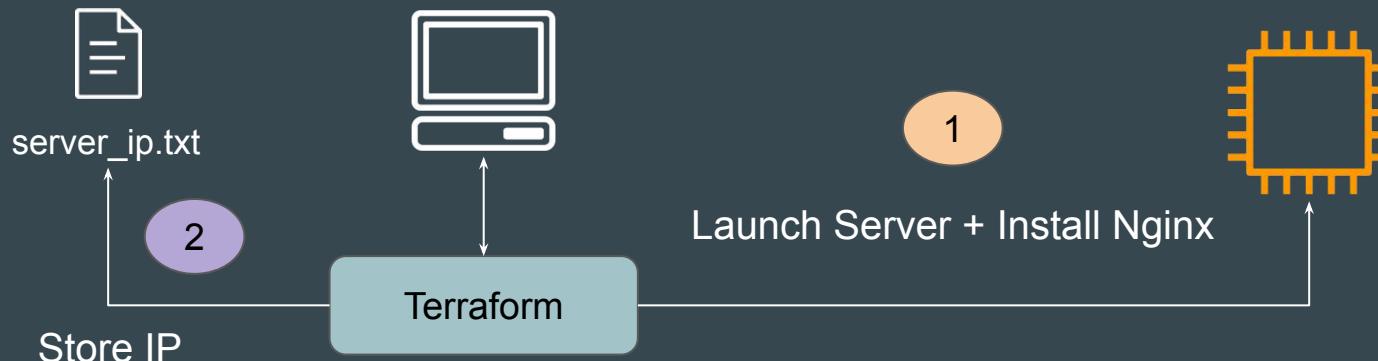
Example: After EC2 is launched, install “apache” software



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

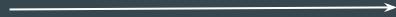
```
resource "aws_instance" "example" {
    ami = "ami-001843b876406202a"
    instance_type = "t2.micro"

    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"
    }

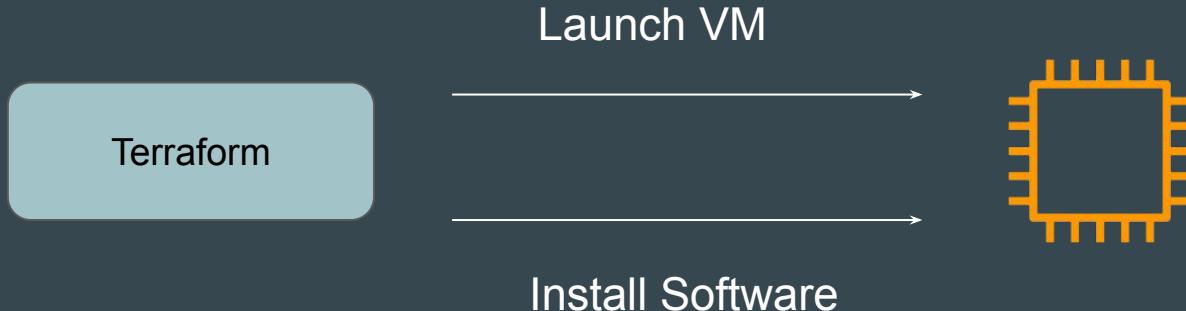
    provisioner "local-exec" {
        command = "echo local-exec-2 provisioner is starting"
    }
}
```

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

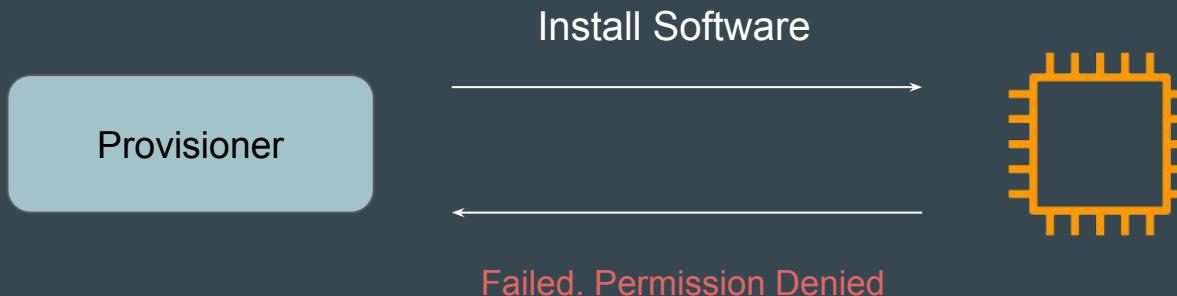
```
resource "aws_instance" "web" {
    # ...
    provisioner "local-exec" {
        when      = destroy
        command  = "echo 'Destroy-time provisioner'"
    }
}
```

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

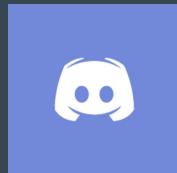
Following screenshot shows that the provisioner has failed but still the apply has completed successfully.

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

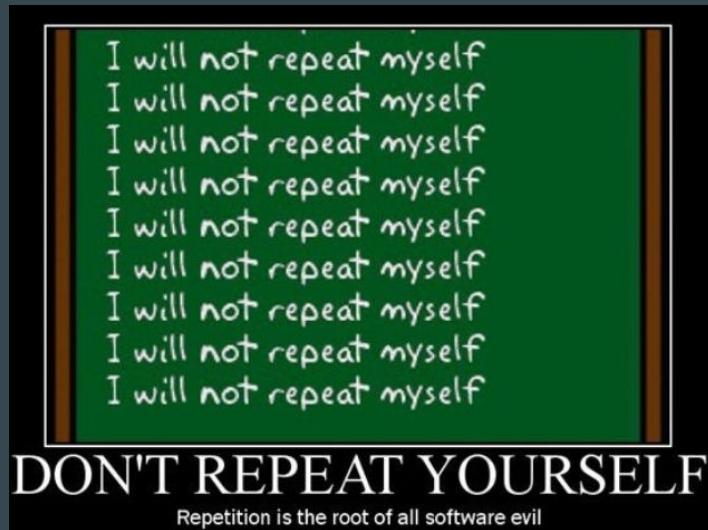


kplabs.in/linkedin

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

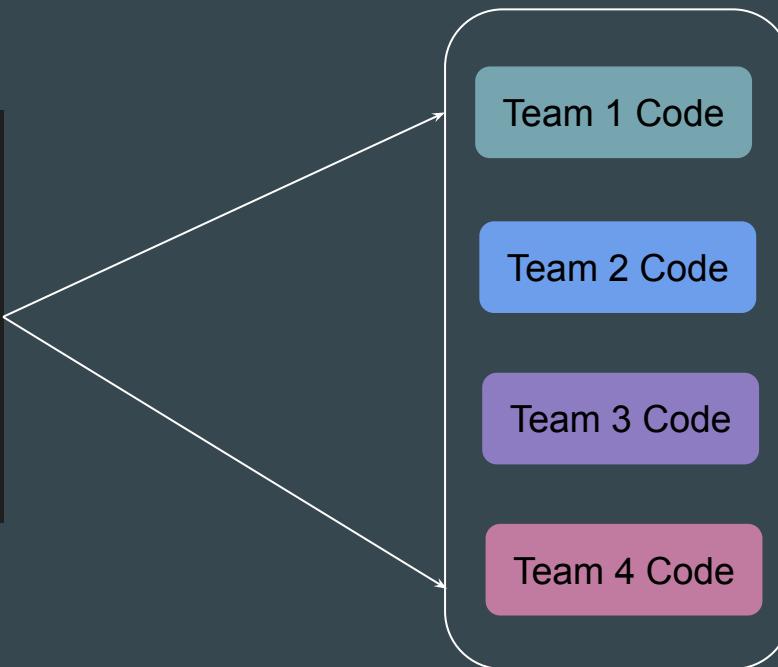
Team 4 Code

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
}
```

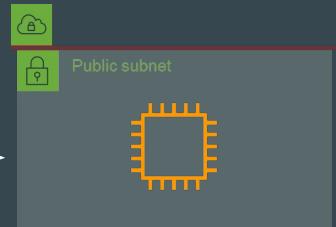
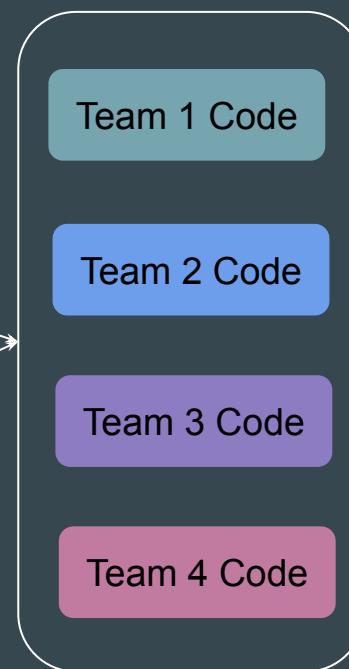
EC2 Module

```
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

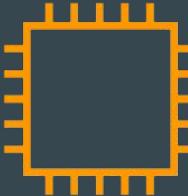
For some infrastructure resources, you can directly use the module calling code, and the entire infrastructure will be created for you.

```
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)

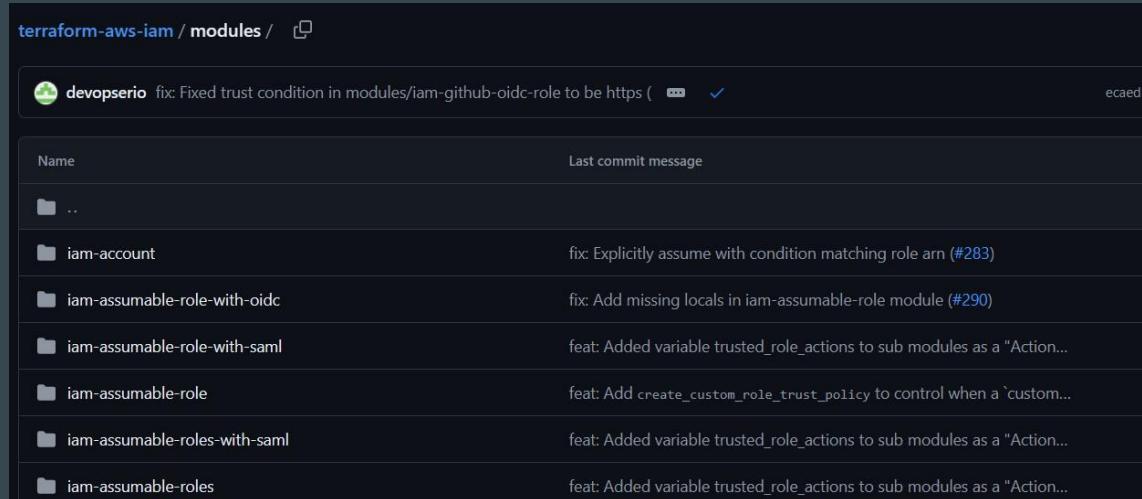
      while calling coalescelist(vals...)
      var.control_plane_subnet_ids is empty list of string
      var.subnet_ids is empty list of string

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..."

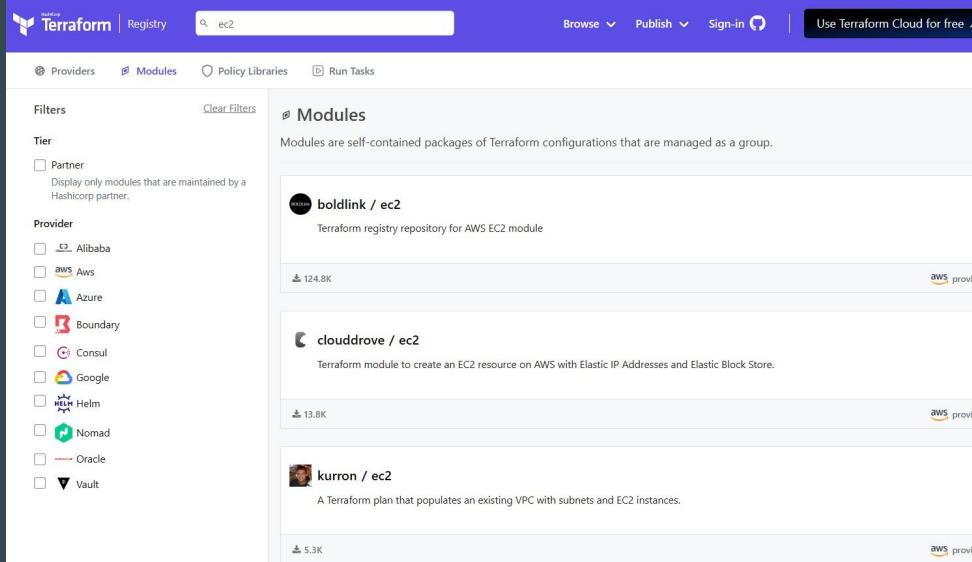
Learnings for Today's Video

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



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, there is a summary of module downloads:

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

Below the download statistics, there is a section titled **Provision Instructions** containing the 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 code tab is selected, showing a list of recent commits:

- semantic-release-bot chore(release): version 5.6.1 [skip ci] - 2 months ago
- .github/workflows fix: Update CI workflow versions to remove deprecated runtimes... - 2 months ago
- examples feat: Add example for connecting via Session Manager without... - 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-docs... - 3 years ago
- .pre-commit-config.yaml fix: Update CI workflow versions to remove deprecated runtimes... - 2 months ago
- .releaserc.json chore: Update release configuration files to correctly use con... - 3 years ago
- CHANGELOG.md chore(release): version 5.6.1 [skip ci] - 2 months ago
- LICENSE chore: update CI/CD to use stable terraform-docs release art... - 3 years ago
- README.md feat: Support Private DNS name options (#370) - 5 months ago
- UPGRADE-3.0.md BREAKING CHANGE: update module to include latest featur... - 3 years ago
- main.tf feat: Support Private DNS name options (#370) - 5 months ago
- outputs.tf feat: Add availability_zone output (#347) - 9 months ago
- variables.tf feat: Support Private DNS name options (#370) - 5 months ago
- versions.tf feat: Implementation of the cpu_options block and addition ... - last year

The repository has 735 stars, 24 watching, and 1.8k forks. It includes sections for Readme, Apache-2.0 license, Code of conduct, Security policy, Activity, Custom properties, and Report repository. A sidebar shows releases (v5.6.1 Latest), sponsor this project (antonbabenko), and packages (No packages published). The contributors section lists 42 contributors, including Anton Babenko, with a note that there are + 28 more.

AWS EC2 Instance Terraform module

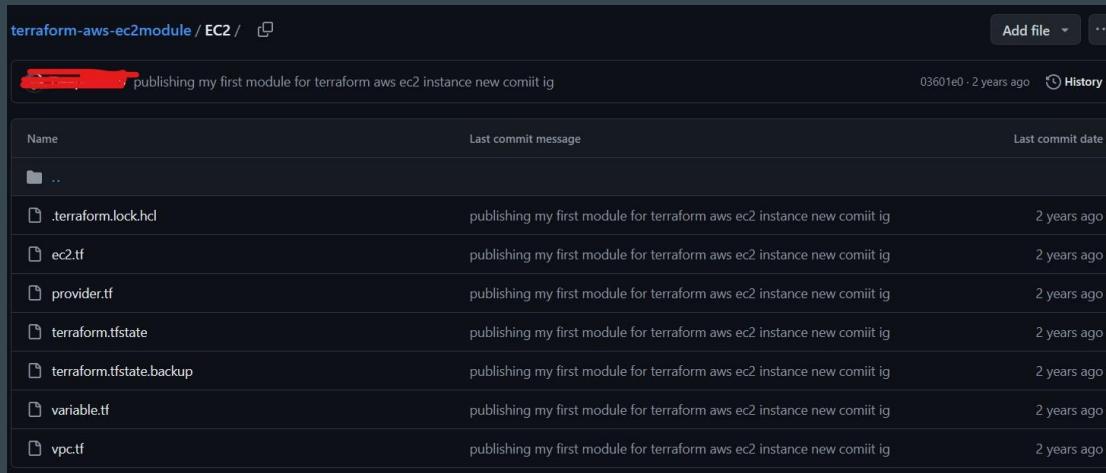
Terraform module which creates an EC2 instance on AWS.

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.

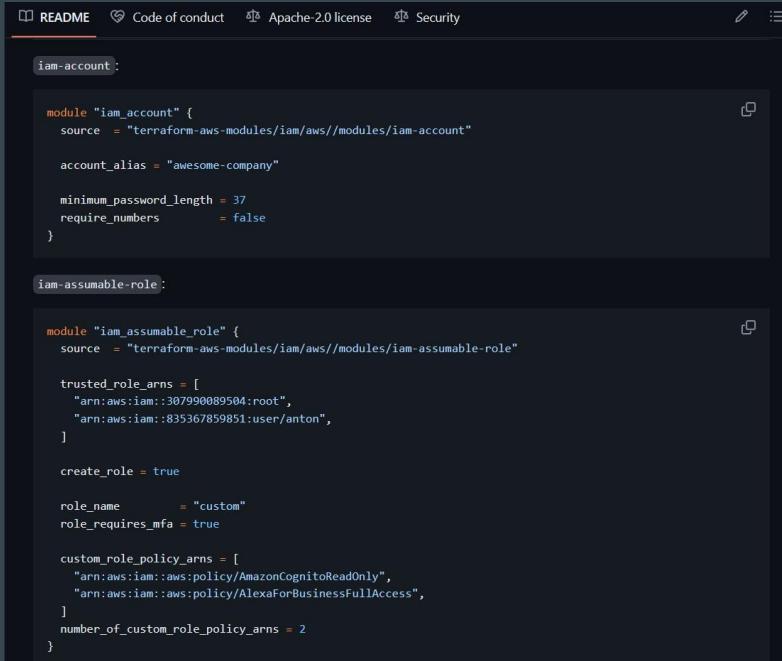


The screenshot shows a GitHub repository named "terraform-aws-ec2module / EC2". A single commit message, "publishing my first module for terraform aws ec2 instance new comitt ig", is present in all files listed in the commit history. The commit was made 2 years ago by a user whose name is partially obscured.

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, Code of conduct, Apache-2.0 license, and Security. The README tab is selected. Below the tabs, there are two code snippets. The first snippet is for the `iam-account` module:

```
module "iam_account" {
  source  = "terraform-aws-modules/iam/aws//modules/iam-account"
  account_alias = "awesome-company"
  minimum_password_length = 37
  require_numbers      = false
}
```

The second snippet is for the `iam-assumable-role` module:

```
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. Below this, there are buttons for "Submodules" and "Examples". A dropdown menu titled "Version 5.39.1 (latest)" lists all available versions from 5.32.1 to 5.39.1. To the right, a "Module Downloads" section shows statistics for the last week, month, year, and overall: 1.9M, 7.4M, 36.1M, and 110.1M respectively. 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

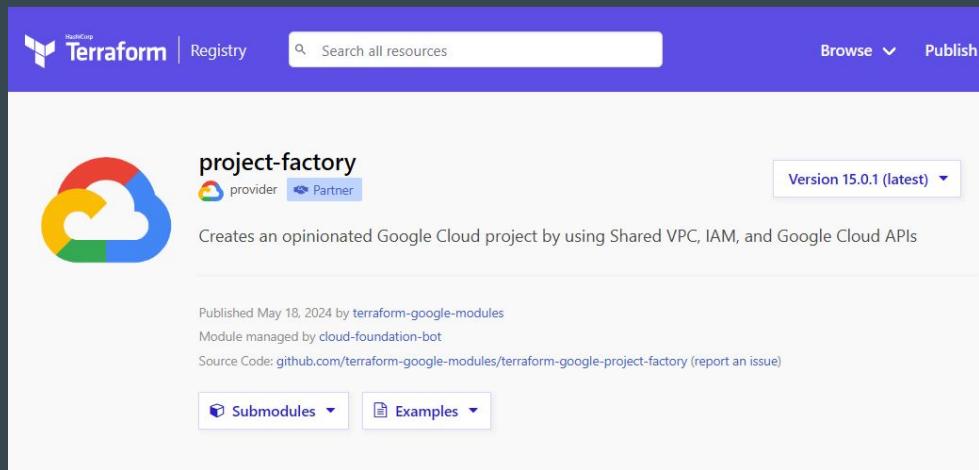
Readme Apache-2.0 license

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.

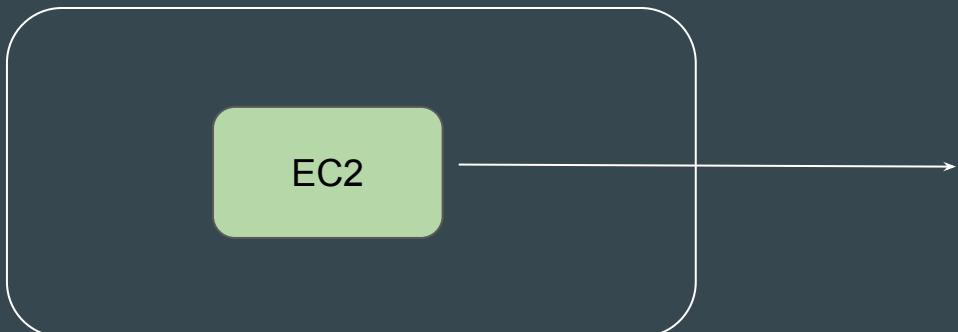
A sub-folder containing name for each modules that are available.



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.



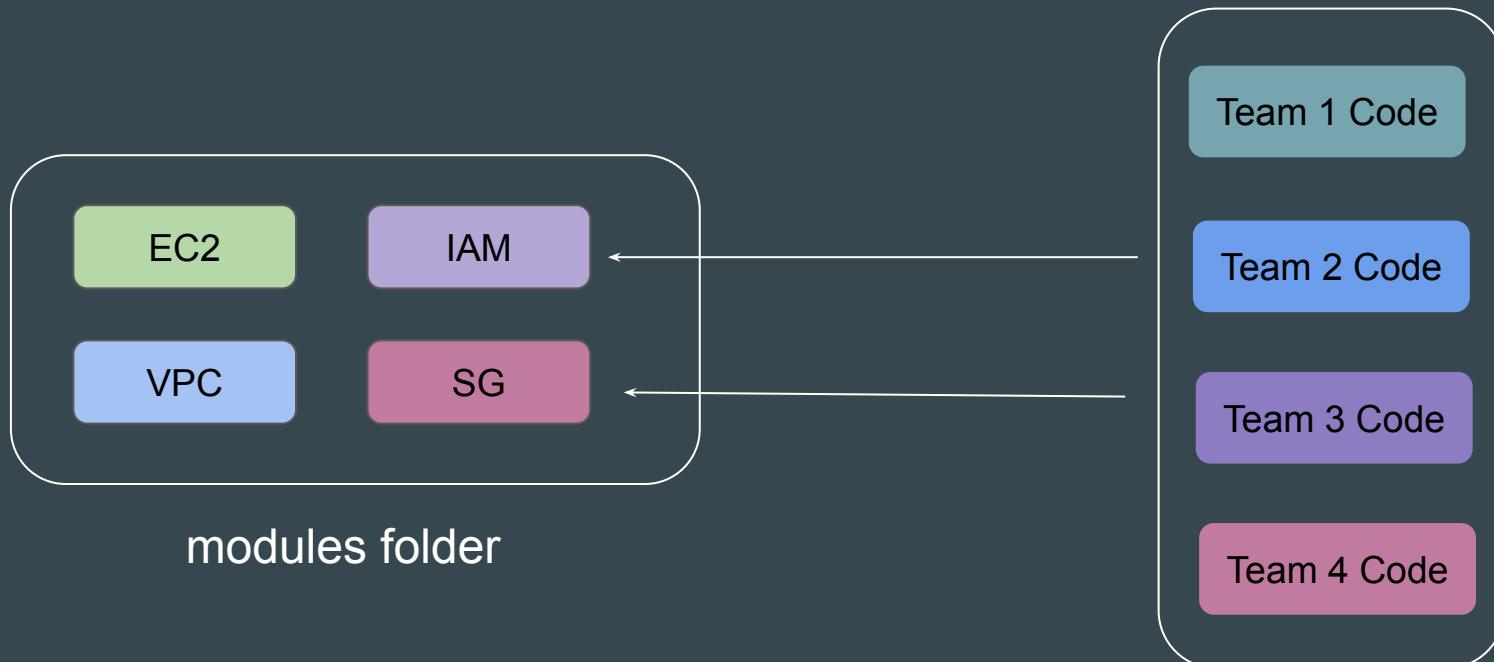
modules folder

```
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.

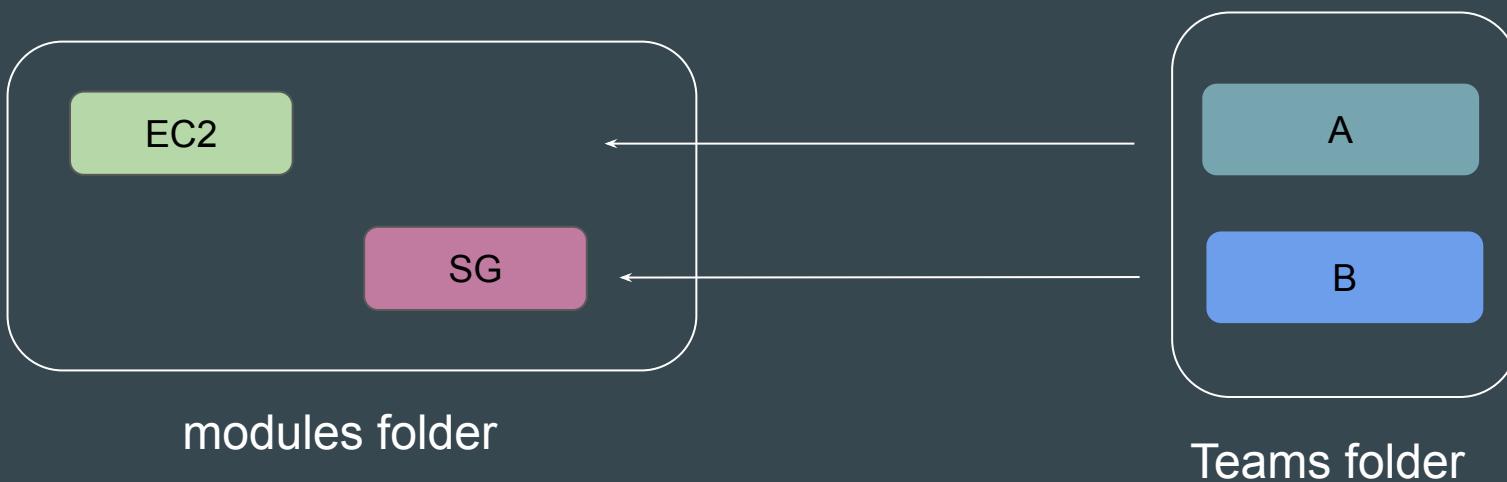


Our Practical Structure

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"
}
```

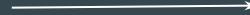
Challenge 2 - Provider Improvements

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

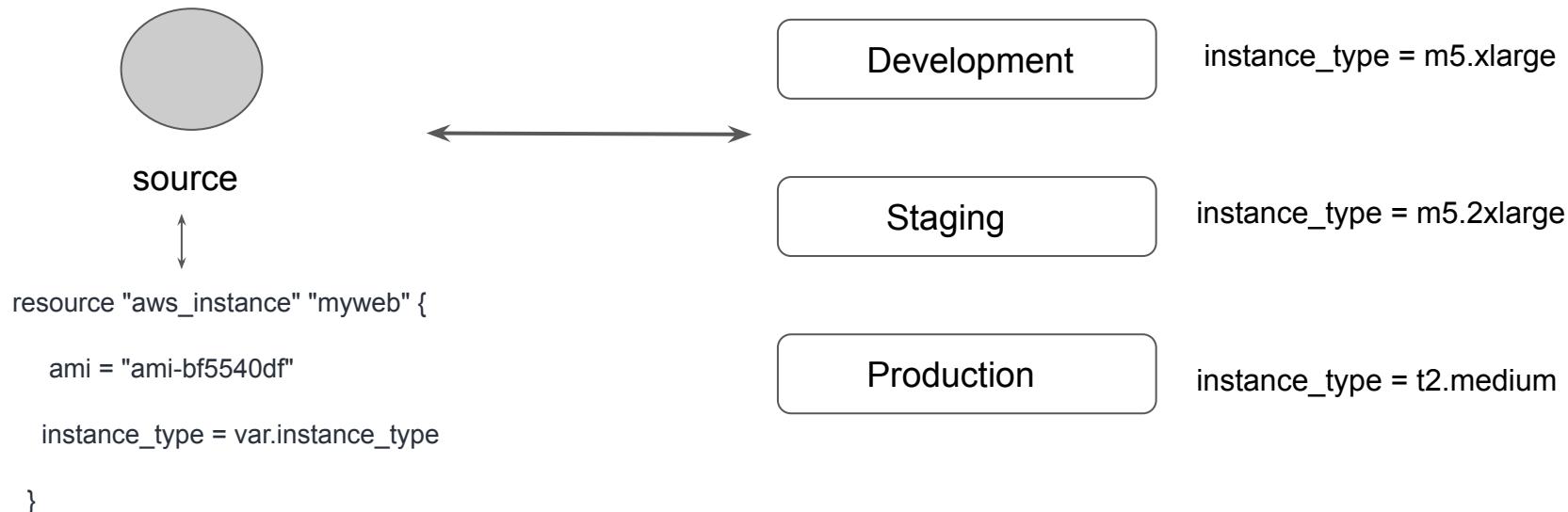
    key_name        = var.key_name
    monitoring      = var.monitoring
    get_password_data = var.get_password_data
    iam_instance_profile = var.create_iam_instance_profile ? aws_iam_instance_profile.this[0].name : var.iam_instance_profile
```

Using Locals with Modules

Terraform Function

Understanding the Challenge

Using variables in Modules can also allow users to override the values which you might not want.



Setting the Context

There can be many repetitive values in modules and this can make your code difficult to maintain.

You can centralize these using variables but users will be able to override it.

```
resource "aws_security_group" "elb-sg" {  
    name      = "myelb-sg"  
  
    ingress {  
        description      = "Allow Inbound from Secret Application"  
        from_port        = 8443  
        to_port          = 8443  
        protocol         = "tcp"  
        cidr_blocks     = ["0.0.0.0/0"]  
    }  
}
```



Hardcoded Port

```
resource "aws_security_group" "elb-sg" {  
    name      = "myelb-sg"  
  
    ingress {  
        description      = "Allow Inbound from Secret Application"  
        from_port        = var.app_port  
        to_port          = var.app_port  
        protocol         = "tcp"  
        cidr_blocks     = ["0.0.0.0/0"]  
    }  
}
```

Variable Port

Using Locals

Instead of variables, you can make use of locals to assign the values.

You can centralize these using variables but users will be able to override it.

```
resource "aws_security_group" "ec2-sg" {
    name      = "myec2-sg"

    ingress {
        description      = "Allow Inbound from Secret Application"
        from_port        = local.app_port
        to_port          = local.app_port
        protocol         = "tcp"
        cidr_blocks     = ["0.0.0.0/0"]
    }

    locals {
        app_port = 8443
    }
}
```

Module Outputs

Output the Data

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.

```
output "instance_ip_addr" {  
    value = aws_instance.server.private_ip  
}
```

Accessing Child Module Outputs

In a parent module, outputs of child modules are available in expressions as
module.<MODULE NAME>.<OUTPUT NAME>

```
resource "aws_security_group" "ec2-sg" {
    name      = "myec2-sg"

    ingress {
        description      = "Allow Inbound from Secret Application"
        from_port        = 8433
        to_port          = 8433
        protocol         = "tcp"
        cidr_blocks     = ["0.0.0.0/0"]
    }

    output "sg_id" {
        value = aws_security_group.ec2-sg.arn
    }
}
```



```
module "sgmodule" {
    source = "../../modules/sg"
}

resource "aws_instance" "web" {
    ami           = "ami-0ca285d4c2cda3300"
    instance_type = "t3.micro"
    vpc_security_group_ids = [module.sgmodule.sg_id]
}
```

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 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
```

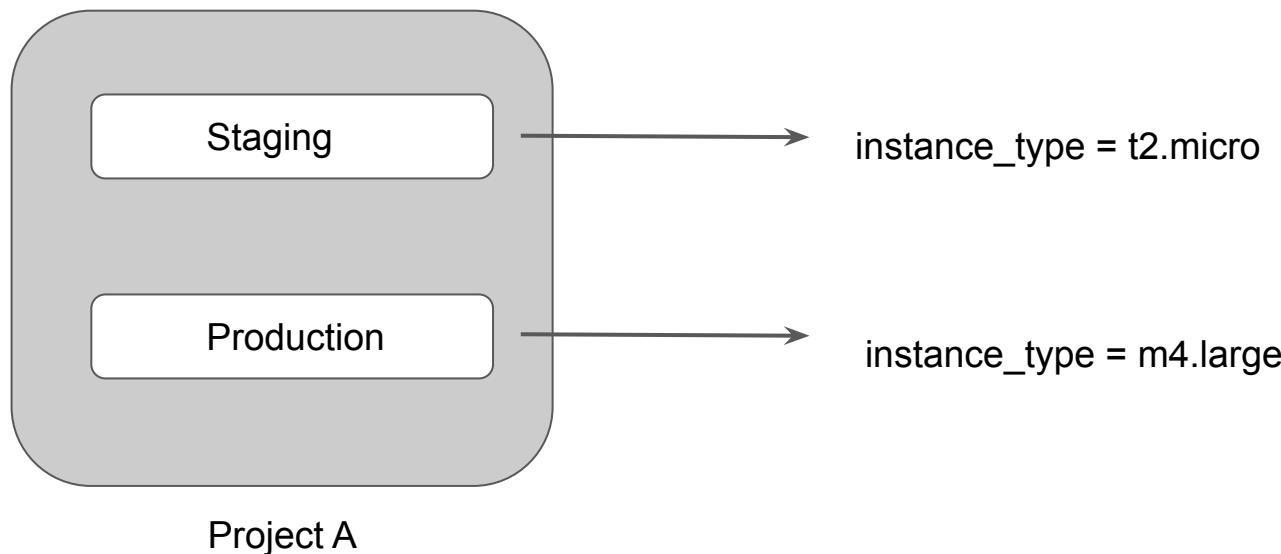
```
$ tree complete-module/
.
├── README.md
├── main.tf
├── variables.tf
├── outputs.tf
├── ...
└── modules/
    ├── nestedA/
    │   ├── README.md
    │   ├── variables.tf
    │   ├── main.tf
    │   ├── outputs.tf
    └── nestedB/
        ├── ...
    └── examples/
        ├── exampleA/
        │   ├── main.tf
        └── exampleB/
            ├── ...
        └── .../
```

Terraform Workspace

Interesting topics

Understanding WorkSpaces

Terraform allows us to have multiple workspaces, with each of the workspace we can have different set of environment variables associated



Team Collaboration

Terraform in detail

Local Changes are not always good

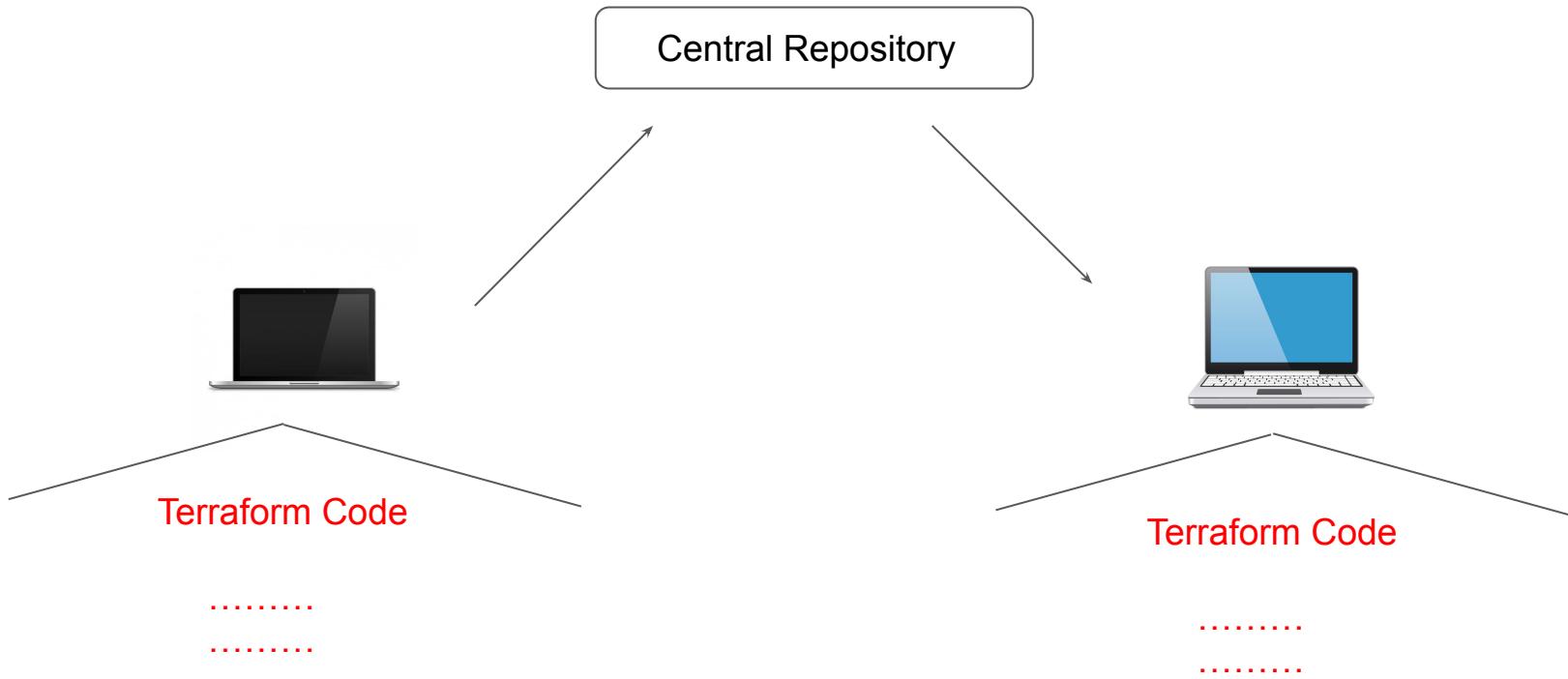
Currently we have been working with terraform code locally.



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.

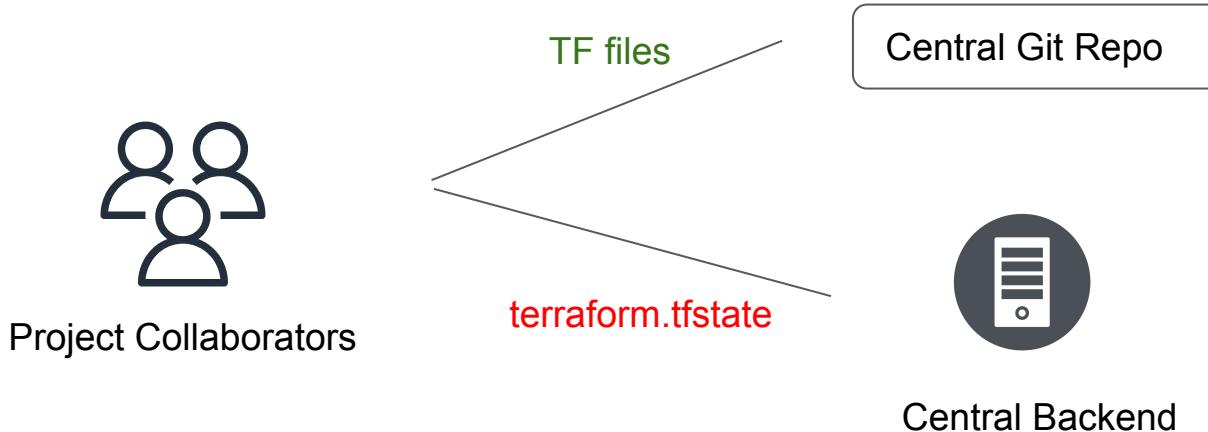
Storing the state file in the local laptop will not allow collaboration.



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.

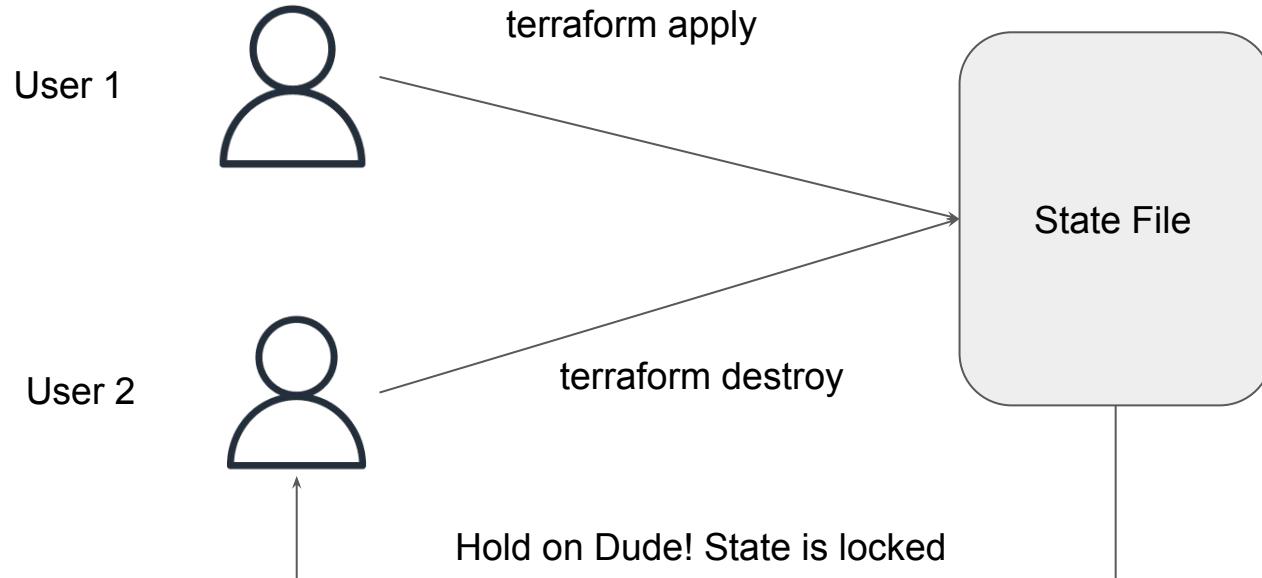
```
C:\Users\Zeal Vora\Desktop\tf-demo\remote-backend>terraform plan
```

```
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.

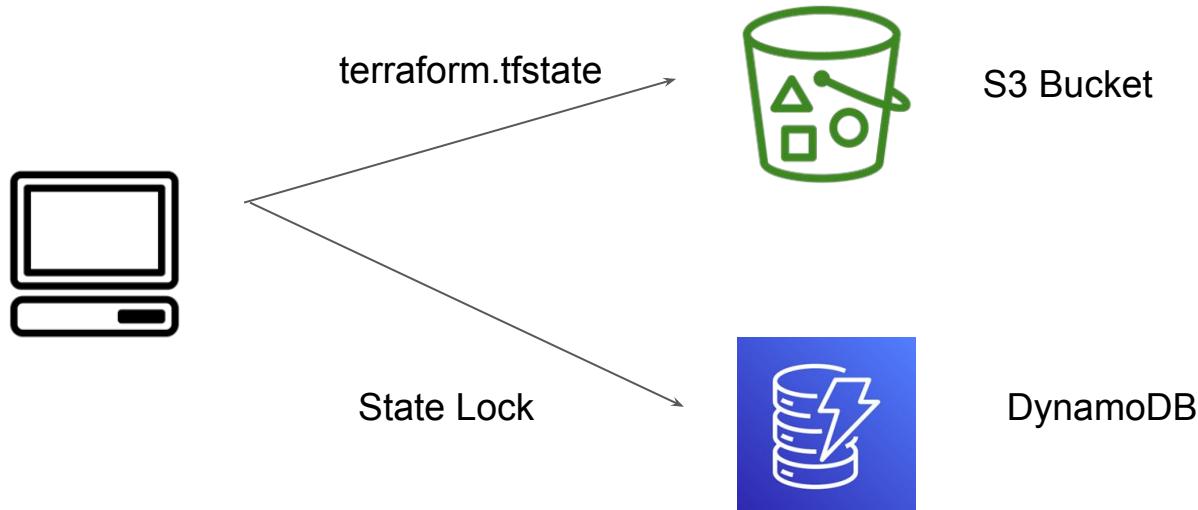
State Locking in S3 Backend

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

Advanced State Management

Overview of State Modification

As your Terraform usage becomes more advanced, there are some cases where you may need to modify the Terraform state.

It is important to never modify the state file directly. Instead, make use of `terraform state` command.

Overview of State Modification

There are multiple sub-commands that can be used with terraform state, these include:

State Sub Command	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.

Sub Command - List

The terraform state list command is used to list resources within a Terraform state.

```
bash-4.2# terraform state list
aws_iam_user.lb
aws_instance.webapp
```

Sub Command - Move

The terraform state mv command is used to move items in a Terraform state.

This command is used in many cases in which you want to rename an existing resource without destroying and recreating it.

Due to the destructive nature of this command, this command will output a backup copy of the state prior to saving any changes

Overall Syntax:

```
terraform state mv [options] SOURCE DESTINATION
```

Sub Command - Pull

The terraform state pull command is used to manually download and output the state from remote state.

This is useful for reading values out of state (potentially pairing this command with something like jq).

Sub Command - Push

The terraform state push command is used to manually upload a local state file to remote state.

This command should rarely be used.

Sub Command - Remove

The terraform state rm command is used to remove items from the Terraform state.

Items removed from the Terraform state are not physically destroyed.

Items removed from the Terraform state are only no longer managed by Terraform

For example, if you remove an AWS instance from the state, the AWS instance will continue running, but terraform plan will no longer see that instance.

Sub Command - Show

The terraform state show command is used to show the attributes of a single resource in the Terraform state.

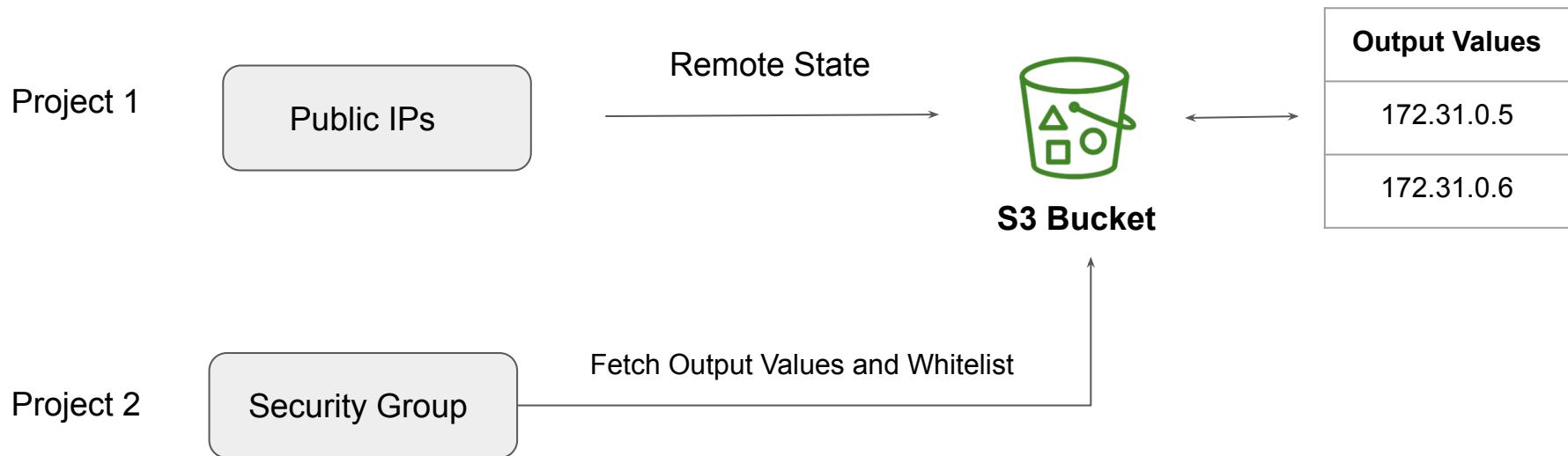
```
bash-4.2# terraform state show aws_instance.webapp
# aws_instance.webapp:
resource "aws_instance" "webapp" {
    ami                      = "ami-082b5a644766e0e6f"
    arn                      = "arn:aws:ec2:us-west-2:018721151861:instance/i-0107ea9ed06c467e0"
    associate_public_ip_address = true
    availability_zone        = "us-west-2b"
    cpu_core_count           = 1
    cpu_threads_per_core     = 1
    disable_api_termination   = false
    ebs_optimized            = false
    get_password_data         = false
    id                       = "i-0107ea9ed06c467e0"
    instance_state            = "running"
    instance_type              = "t2.micro"
```

Connecting Remote States

Terraform in detail

Basics of Terraform Remote State

The `terraform_remote_state` data source retrieves the root module output values from some other Terraform configuration, using the latest state snapshot from the remote backend.



Step 1 - Create a Project with Output Values & S3 Backend

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

output "eip_addr" {
    value = aws_eip.lb.public_ip
}
```



```
terraform {
    backend "s3" {
        bucket = "kplabs-terraform-backend"
        key    = "network/eip.tfstate"
        region = "us-east-1"
    }
}
```

Step 2 - Reference Output Values from Different Project

```
data "terraform_remote_state" "eip" {  
    backend = "s3"  
    config = {  
        bucket = "kplabs-terraform-backend"  
        key    = "network/eip.tfstate"  
        region = "us-east-1"  
    }  
}
```



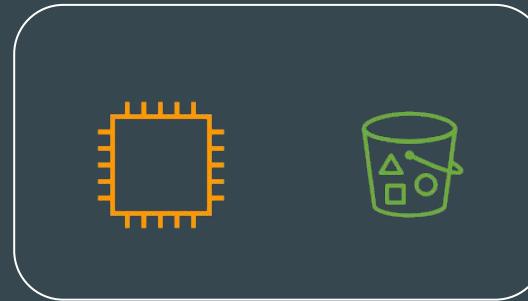
```
resource "aws_security_group" "allow_tls" {  
    name      = "allow_tls"  
    description = "Allow TLS inbound traffic"  
  
    ingress {  
        description      = "TLS from VPC"  
        from_port        = 443  
        to_port          = 443  
        protocol         = "tcp"  
        cidr_blocks     = ["${data.terraform_remote_state.eip.outputs.eip_addr}/32"]  
    }  
}
```

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.

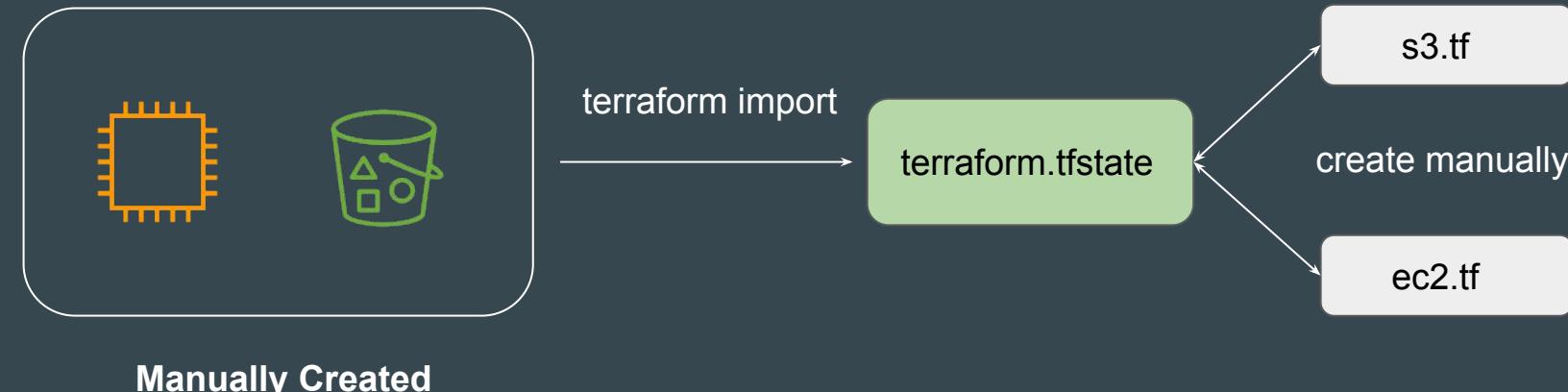


Manually Created

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.

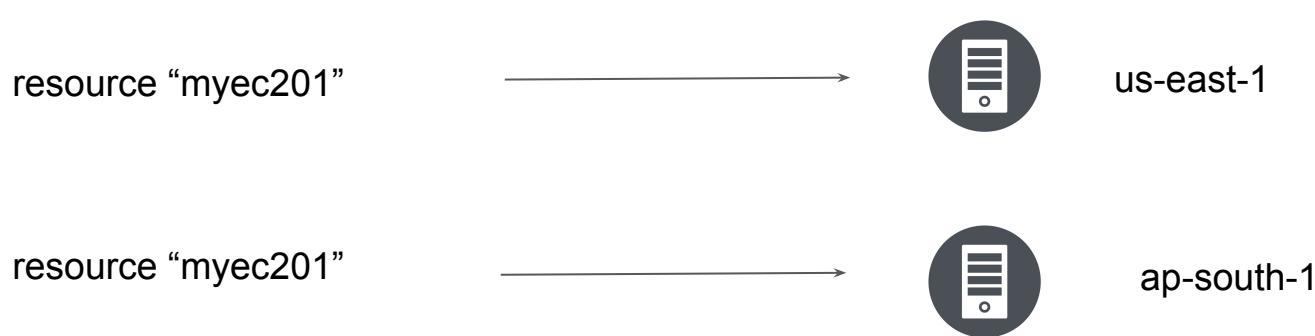
Provider Configuration

Terraform in detail

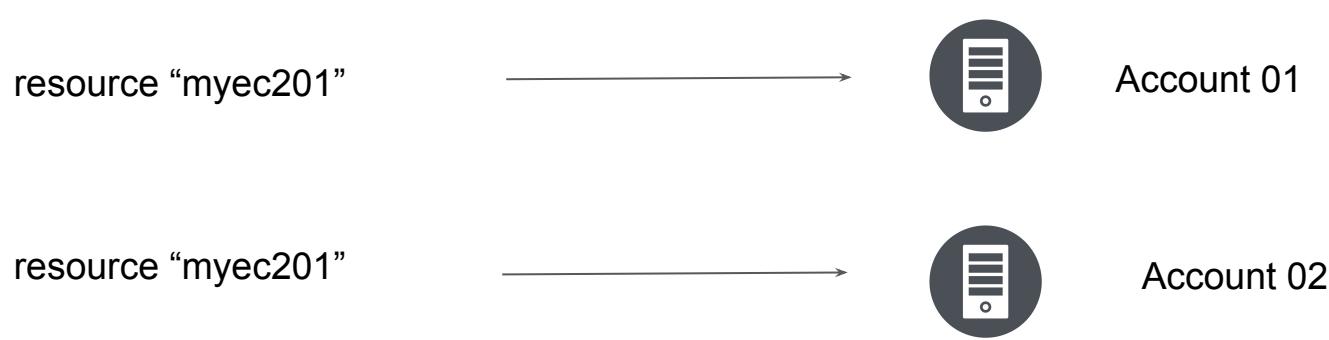
Single Provider Multiple Configuration

Till now, we have been hardcoding the aws-region parameter within the providers.tf

This means that resources would be created in the region specified in the providers.tf file.



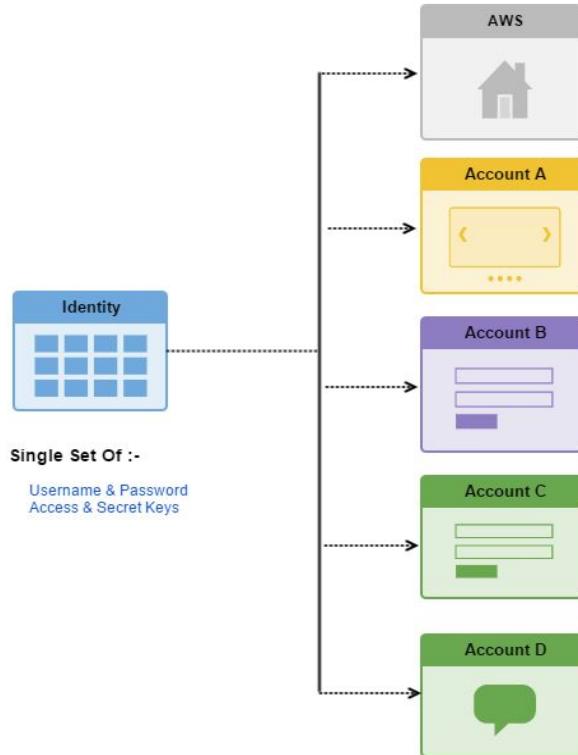
Single Provider Multiple Configuration



Terraform with STS

Terraform in detail

Definitive Use-Case



Sensitive Parameter

Terraform Security

Overview of Sensitive Parameter

With organization managing their entire infrastructure in terraform, it is likely that you will see some sensitive information embedded in the code.

When working with a field that contains information likely to be considered sensitive, it is best to set the Sensitive property on its schema to true

```
output "db_password" {
    value      = aws_db_instance.db.password
    description = "The password for logging in to the database.
    sensitive   = true
}
```

Overview of Sensitive Parameter

Setting the sensitive to “true” will prevent the field's values from showing up in CLI output and in Terraform Cloud

It will not encrypt or obscure the value in the state, however.

```
C:\Users\Zeal Vora\Desktop\terraform\sensitive data>terraform apply  
Apply complete! Resources: 0 added, 0 changed, 0 destroyed.  
  
Outputs:  
  
db_password = <sensitive>
```

Overview of Vault

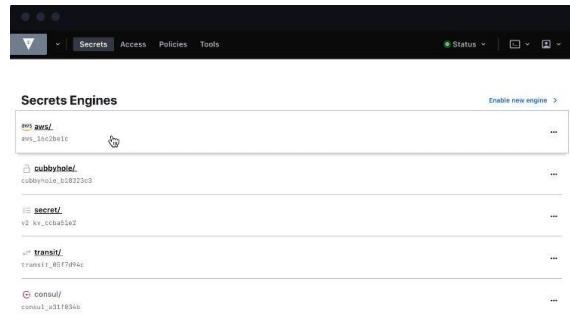
HashiCorp Certified: Vault Associate

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”

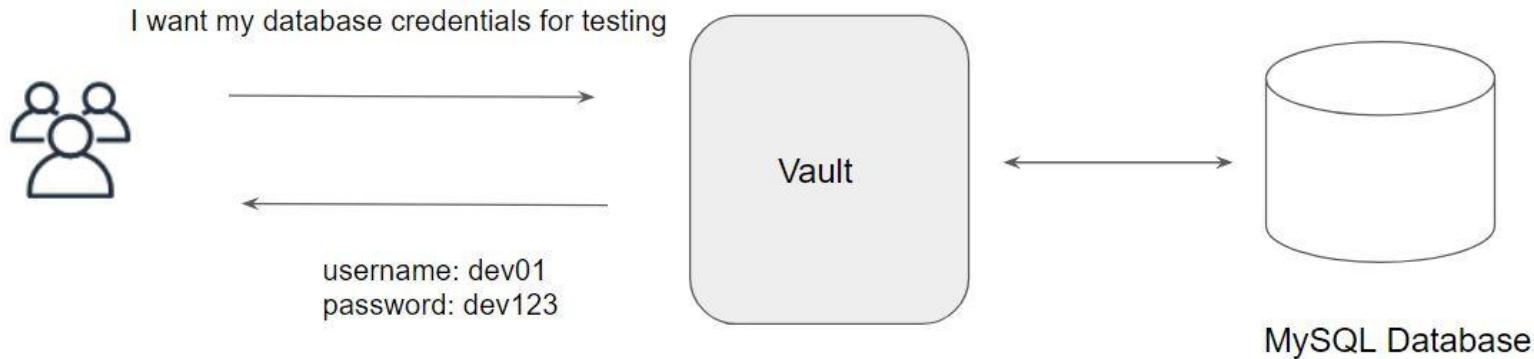
Secrets can include, database passwords, AWS access/secret keys, API Tokens, encryption keys and others.



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 this section. The main area lists several secret engines:

- aws/**
aws_16c2b0fc
- cubbyhole/**
cubbyhole_b1B31203
- secret/**
v2_kv_cchab1e2
- transit/**
transit_85f7d94c
- consul/**
consul_a31fb34b

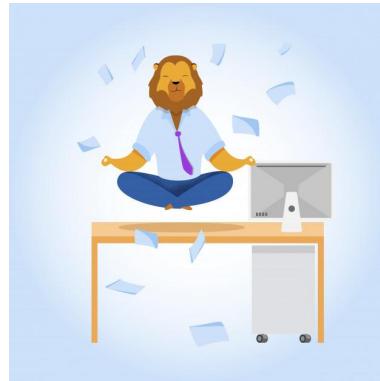
Dynamic Secrets



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.

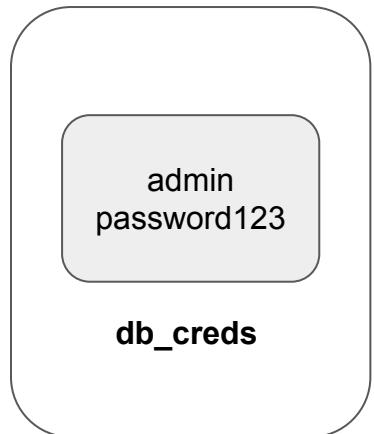


Vault Provider

[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

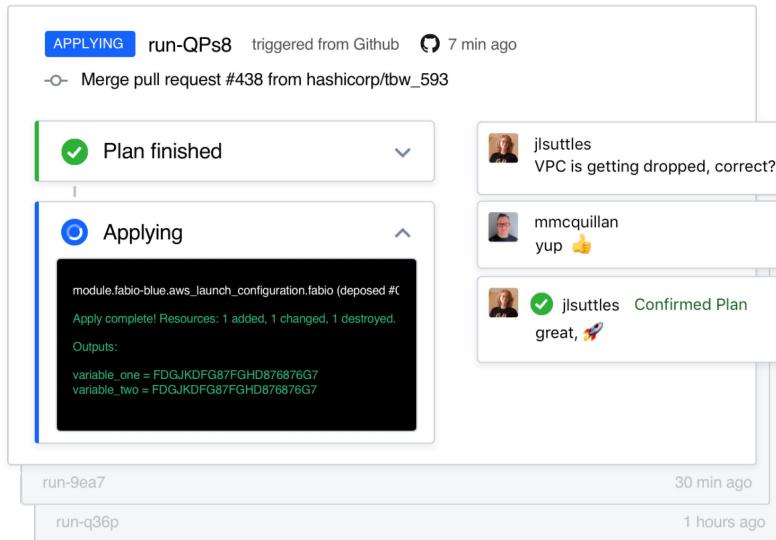
Interacting with Vault from Terraform causes any secrets that you read and write to be persisted in both Terraform's state file.

Terraform Cloud

Terraform in detail

Overview of Terraform Cloud

Terraform Cloud manages Terraform runs in a consistent and reliable environment with various features like access controls, private registry for sharing modules, policy controls and others.



Sentinel

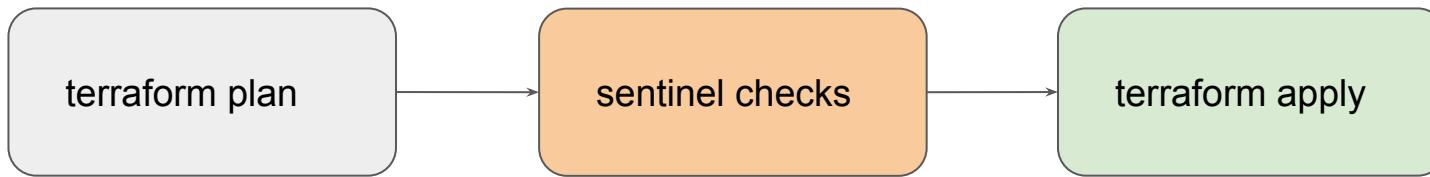
Terraform Cloud In Detail

Overview of the Sentinel

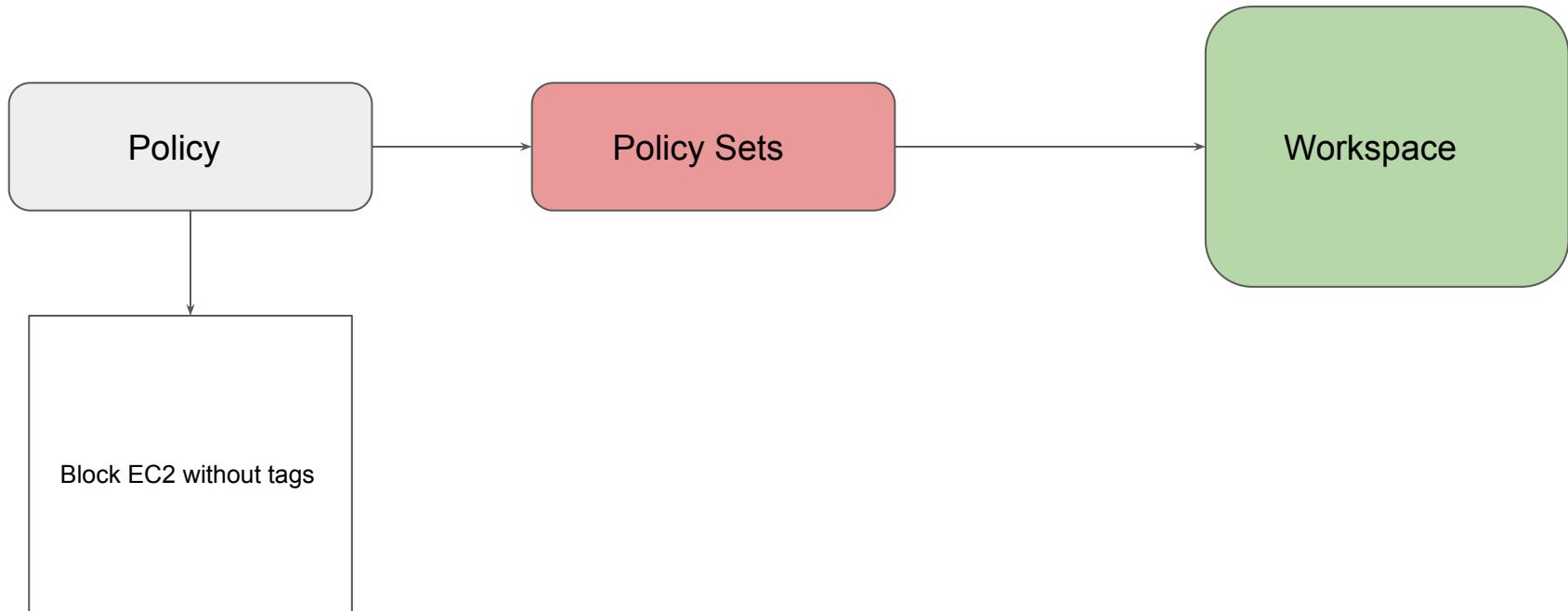
Sentinel is a policy-as-code framework integrated with the HashiCorp Enterprise products.

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



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": [

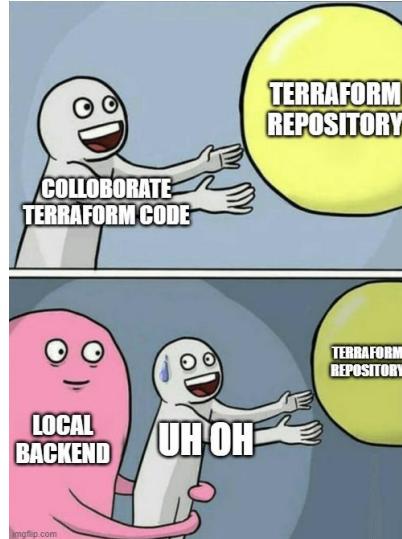
```

terrafrom.tfstate

Challenge with Local Backend

Nowadays Terraform project is handled and collaborated by an entire team.

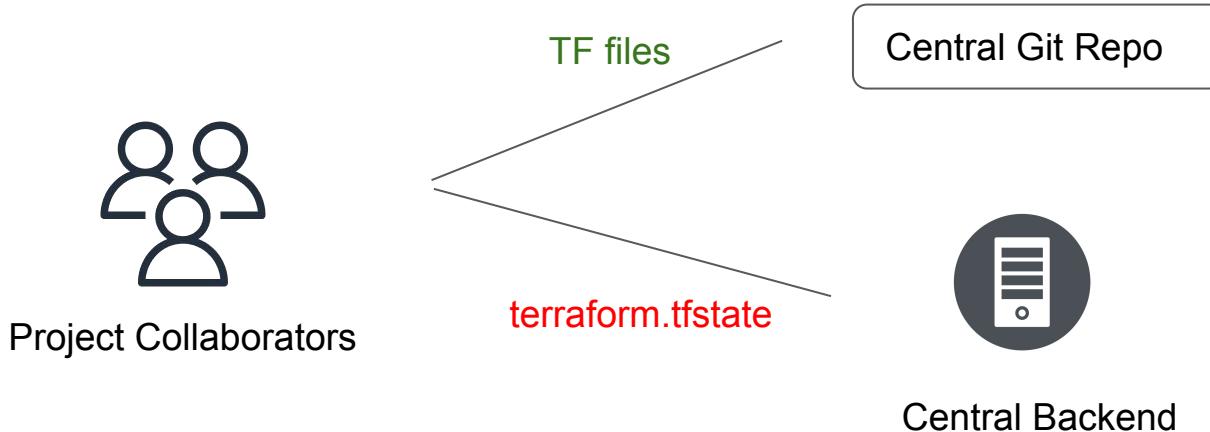
Storing the state file in the local laptop will not allow collaboration.



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.

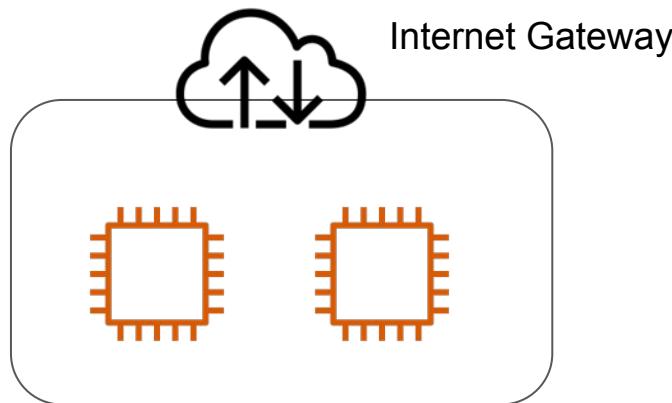


Air Gapped Environments

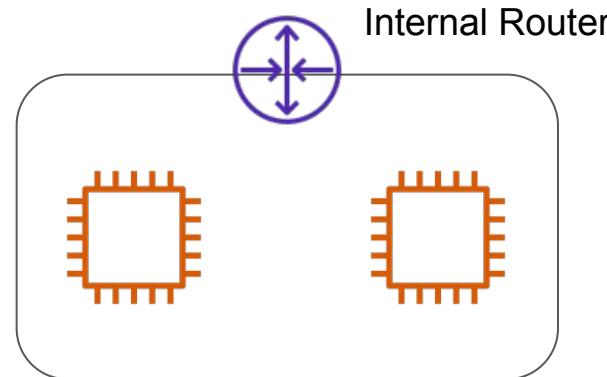
Installation Methods

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

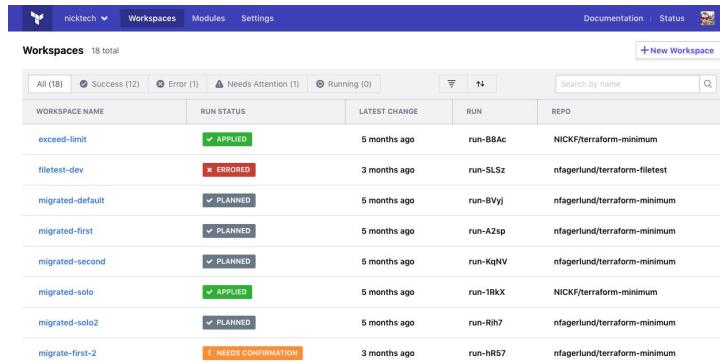
Usage of Air Gapped Systems

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



The screenshot shows the Terraform Enterprise web interface. At the top, there's a navigation bar with a logo, the user name 'nicktech', and links for 'Workspaces', 'Modules', and 'Settings'. Below the navigation is a search bar and a button for '+ New Workspace'. The main area is titled 'Workspaces' with a count of '18 total'. There are filters for 'All (18)', 'Success (12)', 'Error (1)', 'Needs Attention (1)', and 'Running (0)'. A table lists 18 workspaces with columns for 'WORKSPACE NAME', 'RUN STATUS', 'LATEST CHANGE', 'RUN', and 'REPO'. The table includes rows for 'exceed-limit', 'filetest-dev', 'migrated-default', 'migrated-first', 'migrated-second', 'migrated-solo', 'migrated-solo2', and 'migrate-first-2'. The 'migrate-first-2' row has a status of 'NEEDS CONFIRMATION'.

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-Rh7	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

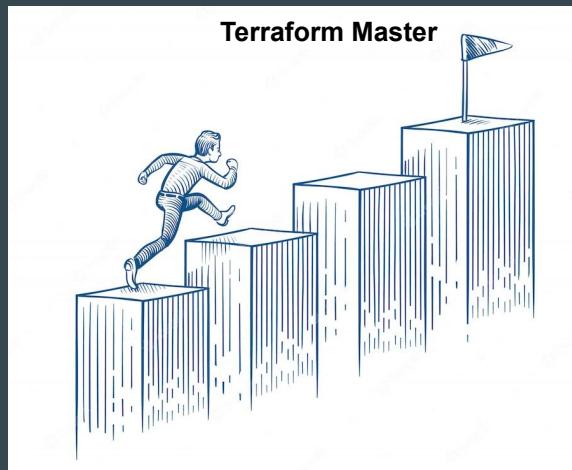
At this stage, we have been learning core concepts of Terraform step by step.

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.

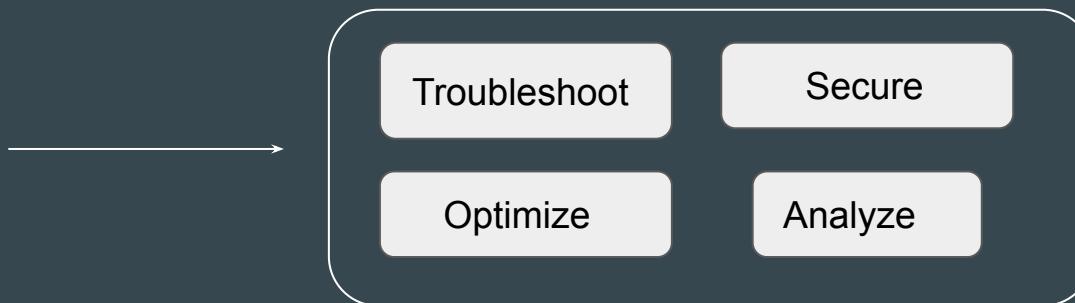


About the Challenges

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.

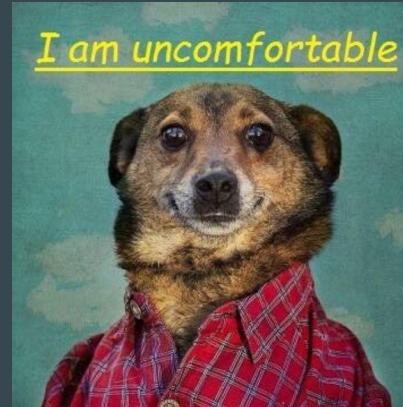
```
terraform_0.12.31
terraform_0.12.30
terraform_0.12.29
terraform_0.12.28
terraform_0.12.27
terraform_0.12.26
terraform_0.12.25
terraform_0.12.24
terraform_0.12.23
terraform_0.12.22
```

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

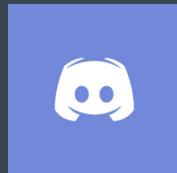
Does the resource block of “aws_eip” work with the latest version of Terraform?

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



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.

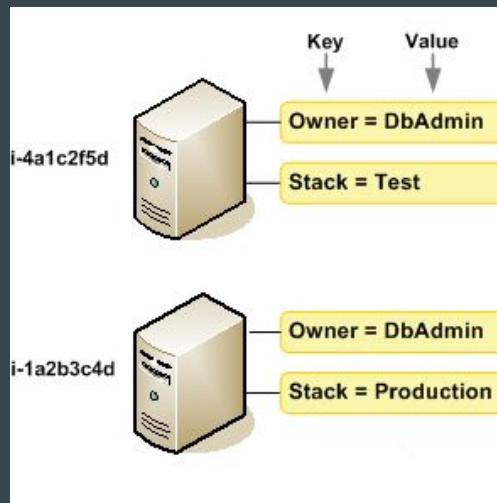
This makes it difficult to modify if code base becomes larger.

```
# 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

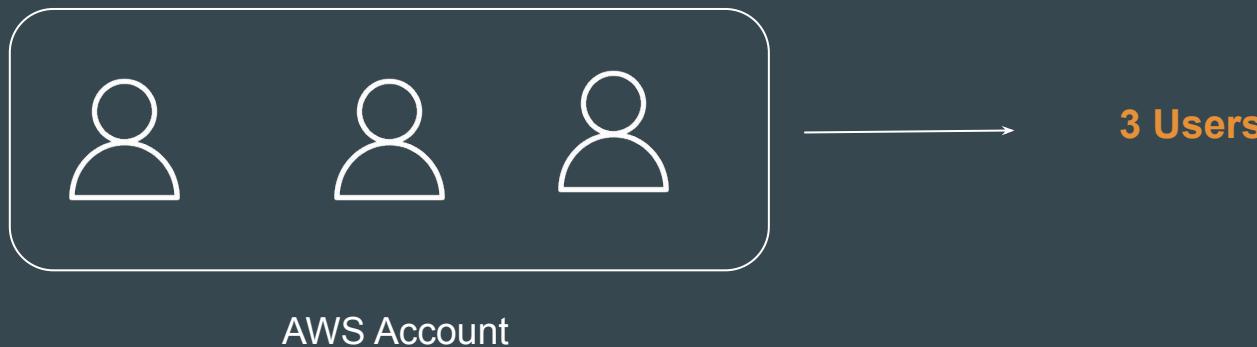
Client wants to have a logic that will show names of ALL users in AWS account in the output.



```
+ 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.

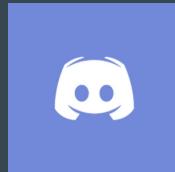
Hint 2 - Functions

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



kplabs.in/linkedin

Overview of HashiCorp Exams

Let's Get Certified!

Overview of HashiCorp Associate Exams

Overview of the basic exam related information.

Assessment Type	Description
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

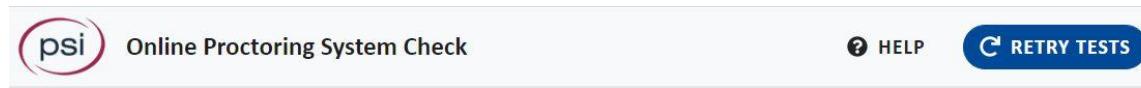


Registration Process

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: Nov 24, 2020	START TIME: 05:30 PM	EXAM DURATION: 60 minutes	<ul style="list-style-type: none">Before taking your remote online proctored exam, please check system compatibility - click HEREYou can only launch the exam within 30 minutes of your appointment time.	You may launch your test in... 3 Hours Launch Exam View Details
-----------------------------------	--------------------------------	-------------------------------------	--	---

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 >](#)

Important Pointers for Exams - 1

Let's get Certified

Terraform Providers

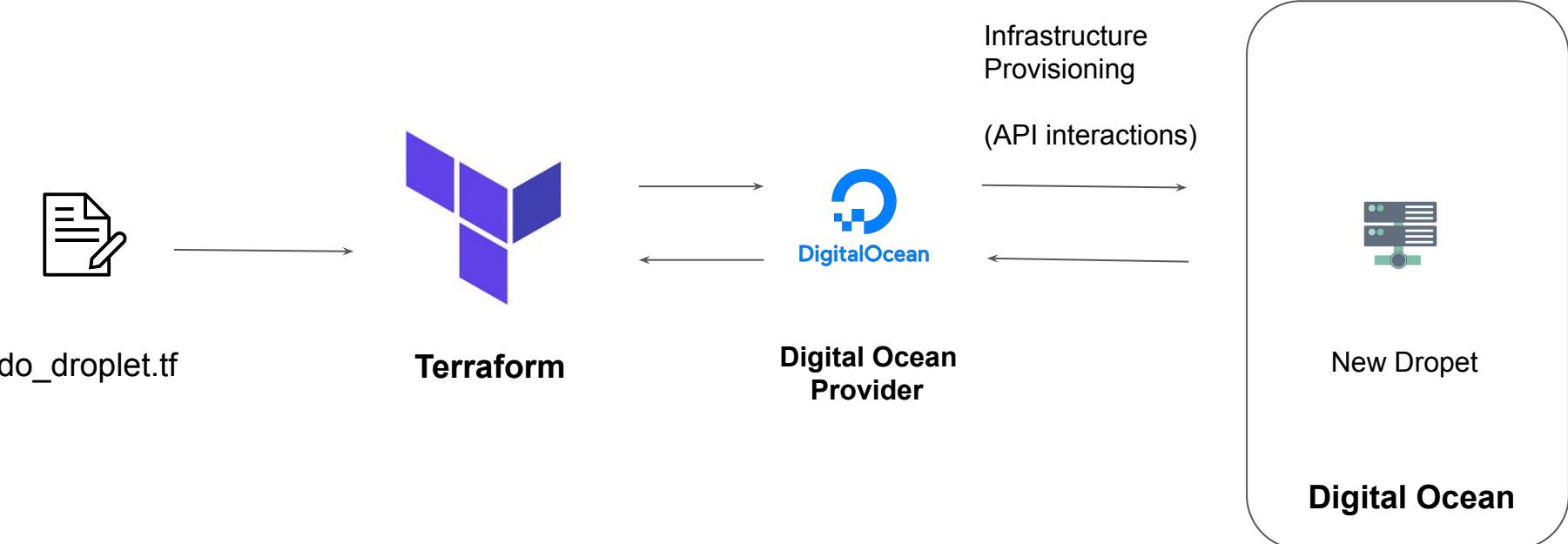
A provider is responsible for understanding API interactions and exposing resources.

Most of the available providers correspond to one cloud or on-premises infrastructure platform, and offer resource types that correspond to each of the features of that platform.

You can explicitly set a specific version of the provider within the provider block.

To upgrade to the latest acceptable version of each provider, run `terraform init -upgrade`

Provider Architecture



Terraform Providers - Part 2

You can have multiple provider instance with the help of alias

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

```
provider "aws" {  
    alias  = "west"  
    region = "us-west-2"  
}
```

The provider block without alias set is known as the default provider configuration. When an alias is set, it creates an additional provider configuration.

Terraform Init

The terraform init command is used to initialize a working directory containing Terraform configuration files.

During init, the configuration is searched for module blocks, and the source code for referenced modules is retrieved from the locations given in their source arguments.

Terraform must initialize the provider before it can be used.

Initialization downloads and installs the provider's plugin so that it can later be executed.

It will not create any sample files like example.tf

Terraform Plan

The terraform plan command is used to create an execution plan.

It will not modify things in infrastructure.

Terraform performs a refresh, unless explicitly disabled, and then determines what actions are necessary to achieve the desired state specified in the configuration files.

This command is a convenient way to check whether the execution plan for a set of changes matches your expectations without making any changes to real resources or to the state.

Terraform Apply

The terraform apply command is used to apply the changes required to reach the desired state of the configuration.

Terraform apply will also write data to the `terraform.tfstate` file.

Once apply is completed, resources are immediately available.

Terraform Refresh

The `terraform refresh` command is used to reconcile the state Terraform knows about (via its state file) with the real-world infrastructure.

This does not modify infrastructure but does modify the state file.

Terraform Destroy

The `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

The `terraform fmt` command is used to rewrite Terraform configuration files to a canonical format and style.

For use-case, where the all configuration written by team members needs to have a proper style of code, `terraform fmt` can be used.

Terraform Validate

The `terraform validate` command validates the configuration files in a directory.

Validate runs checks that verify whether a configuration is syntactically valid and thus primarily useful for general verification of reusable modules, including the correctness of attribute names and value types.

It is safe to run this command automatically, for example, as a post-save check in a text editor or as a test step for a reusable module in a CI system. It can run before `terraform plan`.

Validation requires an initialized working directory with any referenced plugins and modules installed

Terraform Provisioners

Provisioners can be used to model specific actions on the local machine or on a remote machine in order to prepare servers or other infrastructure objects for service.

Provisioners should only be used as a last resort. For most common situations, there are better alternatives.

- Provisioners are inside the resource block.
- Have an overview of local and remote provisioner

```
resource "aws_instance" "web" {  
    # ...  
  
    provisioner "local-exec" {  
        command = "echo The server's IP address is ${self.private_ip}"  
    }  
}
```

Important Pointers for Exams - 2

Let's get Certified

Overview of Debugging 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.

Example:

`TF_LOG=TRACE`

To persist logged output, you can set **TF_LOG_PATH**

Local Values

A local value assigns a name to an expression, allowing it to be used multiple times within a module without repeating it.

The expression of a local value can refer to other locals, but as usual reference cycles are not allowed. That is, a local cannot refer to itself or to a variable that refers (directly or indirectly) back to it.

It's recommended to group together logically-related local values into a single block, particularly if they depend on each other.

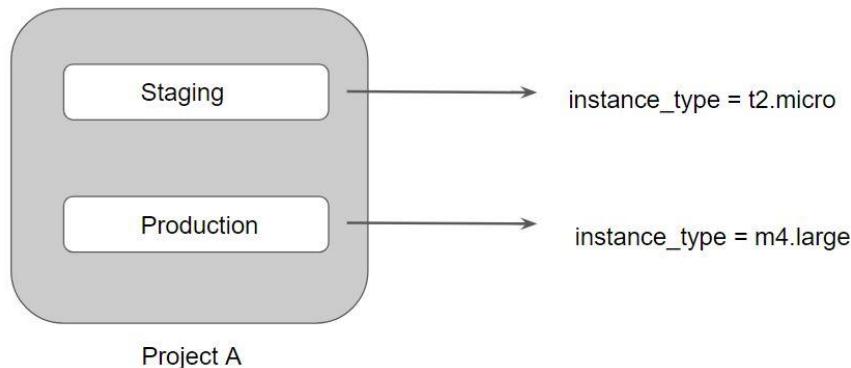
Overview of Data Types

Type Keywords	Description
string	Sequence of Unicode characters representing some text, like "hello".
list	Sequential list of values identified by their position. Starts with 0 ["mumbai", "singapore", "usa"]
map	a group of values identified by named labels, like {name = "Mabel", age = 52}.
number	Example: 200

Terraform WorkSpaces

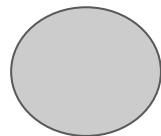
Terraform allows us to have multiple workspaces; with each of the workspaces, we can have a different set of environment variables associated.

Workspaces allow multiple state files of a single configuration.



Terraform Modules

We can centralize the terraform resources and can call out from TF files whenever required.



module “source”

source



```
resource "aws_instance" "myweb" {  
    ami = "ami-bf5540df"  
  
    instance_type = "t2.micro"  
  
    security_groups = ["default"]  
}
```

Terraform Modules - ROOT and Child

Every Terraform configuration has at least one module, known as its root module, which consists of the resources defined in the .tf files in the main working directory.

A module can call other modules, which lets you include the child module's resources into the configuration in a concise way.

A module that includes a module block like this is the calling module of the child module.

```
module "servers" {
    source = "./app-cluster"

    servers = 5
}
```

Module - Accessing Output Values

The resources defined in a module are encapsulated, so the calling module cannot access their attributes directly.

However, the child module can declare output values to selectively export certain values to be accessed by the calling module.

A module includes a module block like this in the calling module of the child module.

```
output "instance_ip_addr" {
    value = aws_instance.server.private_ip
}
```

Suppressing Values in CLI Output

An output can be marked as containing sensitive material using the optional `sensitive` argument:

```
output "db_password" {
  value      = aws_db_instance.db.password
  description = "The password for logging in to the database."
  sensitive   = true
}
```

Setting an output value in the root module as sensitive prevents Terraform from showing its value in the list of outputs at the end of `terraform apply`

Sensitive output values are still recorded in the state, and so will be visible to anyone who is able to access the state data.

Module Versions

It is recommended to explicitly constraining the acceptable version numbers for each external module to avoid unexpected or unwanted changes.

Version constraints are supported only for modules installed from a module registry, such as the Terraform Registry or Terraform Cloud's private module registry.

```
module "consul" {
    source  = "hashicorp/consul/aws"
    version = "0.0.5"

    servers = 3
}
```

Terraform Registry

The Terraform Registry is integrated directly into Terraform.

The syntax for referencing a registry module is

<NAMESPACE>/<NAME>/<PROVIDER>.

For example: hashicorp/consul/aws.

```
module "consul" {
    source = "hashicorp/consul/aws"
    version = "0.1.0"
}
```

Private Registry for Module Sources

You can also use modules from a private registry, like the one provided by Terraform Cloud.

Private registry modules have source strings of the following form:

<HOSTNAME>/<NAMESPACE>/<NAME>/<PROVIDER>.

This is the same format as the public registry, but with an added hostname prefix.

While fetching a module, having a version is required.

```
module "vpc" {
  source = "app.terraform.io/example_corp/vpc/aws"
  version = "0.9.3"
}
```

Important Pointers for Exams - 3

Let's get Certified

Terraform Functions

The Terraform language includes a number of built-in functions that you can use to transform and combine values.

```
> max(5, 12, 9)  
12
```

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

Be aware of basic functions like element, lookup.

Count and Count Index

The count parameter on resources can simplify configurations and let you scale resources by simply incrementing a number.

In resource blocks where the count is set, an additional count object (count.index) is available in expressions, so that you can modify the configuration of each instance.

```
resource "aws_iam_user" "lb" {
    name = "loadbalancer.${count.index}"
    count = 5
    path = "/system/"
}
```

Find the Issue - Use-Case

You can expect use-case with terraform code, and you have to 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 = 1234  
    asecret_key = 1234567890  
  }  
}
```

Terraform Lock

If supported by your backend, Terraform will lock your state for all operations that could write state.

Terraform has a force-unlock command to manually unlock the state if unlocking failed.

Use-Case - Resources Deleted Out of Terraform

You have created an EC2 instance. Someone has modified the EC2 instance manually. What will happen if you do terraform plan yet again?

1. Someone has changed EC2 instance type from t2.micro to t2.large?
2. Someone has terminated the EC2 instance.

Answer 1. Terraform's current state will have t2.large, and the desired state is t2.micro. It will try to change back instance type to t2.micro.

Answer 2. Terraform will create a new EC2 instance.

Resource Block

Each resource block describes one or more infrastructure objects, such as virtual networks, compute instances, or higher-level components such as DNS records.

A resource block declares a resource of a given type ("aws_instance") with a given local name ("web").

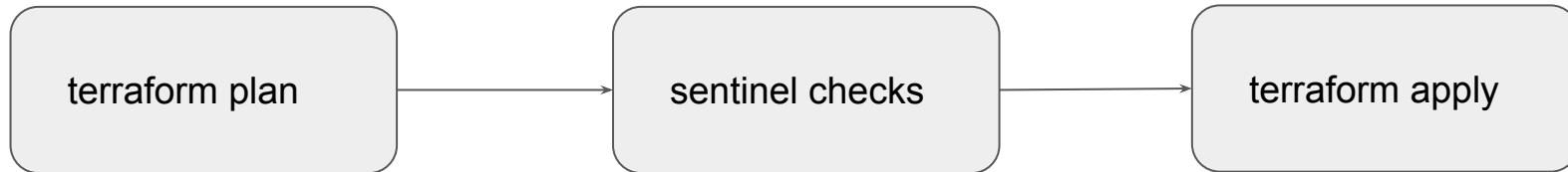
```
resource "aws_instance" "web" {
    ami          = "ami-a1b2c3d4"
    instance_type = "t2.micro"
}
```

Sentinel

Sentinel is an embedded policy-as-code framework integrated with the HashiCorp Enterprise products.

Can be used for various use-cases like:

- Verify if EC2 instance has tags.
- Verify if the S3 bucket has encryption enabled.



Sensitive Data in State File

If you manage any sensitive data with Terraform (like database passwords, user passwords, or private keys), treat the state itself as sensitive data.

Approaches in such a scenario:

Terraform Cloud always encrypts the state at rest and protects it with TLS in transit. Terraform Cloud also knows the identity of the user requesting state and maintains a history of state changes.

The S3 backend supports encryption at rest when the encrypt option is enabled.

Dealing with Credentials in Config

Hard-coding credentials into any Terraform configuration are not recommended, and risks the secret leakage should this file ever be committed to a public version control system.

You can store the credentials outside of terraform configuration.

Storing credentials as part of environment variables is also a much better approach than hard coding it in the system.

Remote Backend for Terraform Cloud

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.

Miscellaneous Pointers

Terraform does not require go as a prerequisite.

It works well in Windows, Linux, MAC.

Windows Server is not mandatory.

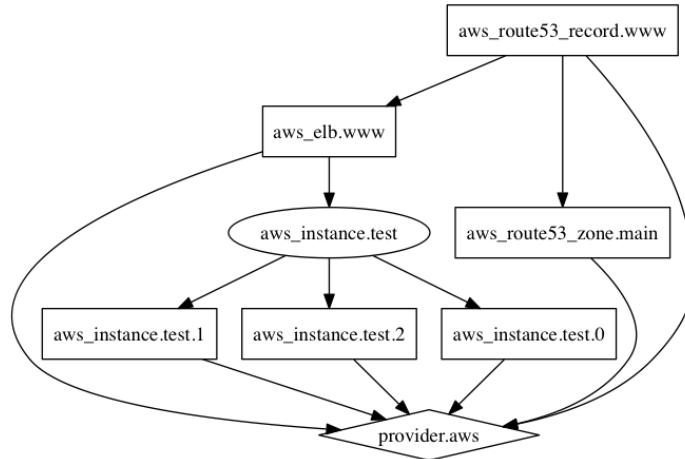
Important Pointers for Exams - 4

Let's get Certified

Terraform Graph

The `terraform graph` command is used to generate a visual representation of either a configuration or execution plan

The output of `terraform graph` is in the **DOT format**, which can easily be converted to an image.



Splat Expressions

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 Terminologies

aws_instance	Resource Type
example	Local name for the resource
ami	Argument Name
abc123	Argument value

```
resource "aws_instance" "example" {
    ami = "abc123"
}
```

Provider Configuration

Provider Configuration block is not mandatory for all the terraform configuration.

```
provider "aws" {
  region      = "us-east-1"
  access_key  = "YOUR-KEY"
  secret_key  = "YOUR-KEY"
}

resource "aws_iam_user" "iam" {
  name        = "iamuser"
  path        = "/system/"
}
```

```
locals {
  arr = ["value1", "value2"]
}

output "test" {
  value = local.arr
}
```

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 output iam_names
[
  "iamuser.0",
  "iamuser.1",
  "iamuser.2",
]
```

Terraform Unlock

If supported by your backend, Terraform will lock your state for all operations that could write state.

Not all backends supports locking functionality.

Terraform has a force-unlock command to manually unlock the state if unlocking failed.

```
terraform force-unlock LOCK_ID [DIR]
```

Miscellaneous Pointers - 1

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

Miscellaneous Pointers - 2

Sentinel is a proactive service.

Terraform Refresh does not modify the infrastructure but it modifies the state file.

Slice Function is not part of the string function. Others like join, split, chomp are part of it.

It is not mandatory to include the module version argument while pulling the code from terraform registry.

Miscellaneous Pointers - 3

Overuse of dynamic blocks can make configuration hard to read and maintain.

Terraform Apply can change, destroy and provision resources but cannot import any resource.

Join us in our Adventure

Be Awesome



kplabs.in/twitter



kplabs.in/linkedin

instructors@kplabs.in

Important Pointers for Exams - 5

Let's get Certified

Terraform Enterprise & Terraform Cloud

Terraform Enterprise provides several added advantage 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)

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.

Example Code:

```
variable custom_var { }
```

```
C:\Users\Zeal Vora\Desktop\terraform\tmp\1>terraform plan  
var.custom_var  
Enter a value:
```

Environment Variables

Environment variables can be used to set variables.

The environment variables must be in the format `TF_VAR_name`

```
export TF_VAR_region=us-west-1  
  
export TF_VAR_ami=ami-049d8641  
  
export TF_VAR_alist='[1,2,3]'
```

Structural Data Types

A structural type allows multiple values of several distinct types to be grouped together as a single value.

List contains multiple values of same type while object can contain multiple values of different type.

Structural Type	Description
object	<p>A collection of named attributes that each have their own type.</p> <pre>object({<ATTR NAME> = <TYPE>, ... }) object({ name=string, age=number })</pre> <pre>{ name = "John" age = 52 }</pre>
tuple	<pre>tuple([<TYPE>, ...])</pre>

BackEnd Configuration

Backends are configured directly in Terraform files in the `terraform` section.

After configuring a backend, it has to be initialized.

```
terraform {  
  backend "s3" {  
    bucket = "mybucket"  
    key    = "path/to/my/key"  
    region = "us-east-1"  
  }  
}
```

BackEnd Configuration Types - 1

First Time Configuration:

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 backends without losing any existing state.

BackEnd Configuration Types - 2

Partial Time Configuration:

You do not need to specify every required argument in the backend configuration. Omitting certain arguments may be desirable to avoid storing secrets, such as access keys, within the main configuration.

With a partial configuration, the remaining configuration arguments must be provided as part of the initialization process.

```
terraform {  
  backend "consul" {}  
}
```

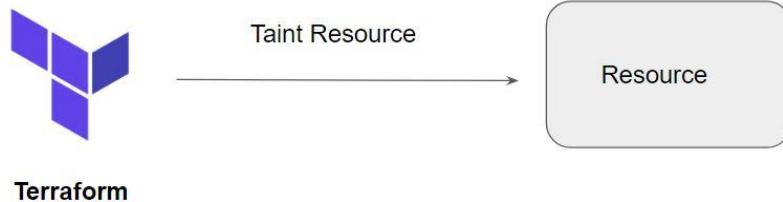


```
terraform init \  
  -backend-config="address=demo.consul.io" \  
  -backend-config="path=example_app/terraform_state" \  
  -backend-config="scheme=https"
```

Overview of Terraform Taint

The `terraform taint` command manually marks a Terraform-managed resource as tainted, forcing it to be destroyed and recreated on the next apply.

Once a resource is marked as tainted, the next plan will show that the resource will be destroyed and recreated and the next apply will implement this change.



Input Variables

The value associated with a variable can be assigned via multiple approaches.

```
variable "image_id" {  
    type = string  
}
```

Value associated with the variables can be defined via CLI as well as in tfvars file.

Following is syntax to load custom tfvars file:

```
terraform apply -var-file="testing.tfvars"
```

Variable Definition Precedence

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

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

If the same variable is assigned multiple values, Terraform uses the last value it finds.

Terraform Local Backend

The local backend stores 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"  
    }  
}
```

Required Providers

Each Terraform module must declare which providers it requires, so that Terraform can install and use them.

Provider requirements are declared in a required_providers block.

```
terraform {
  required_providers {
    mycloud = {
      source  = "mycorp/mycloud"
      version = "~> 1.0"
    }
  }
}
```

Required Version

The required_version setting accepts a version constraint string, which specifies which versions of Terraform can be used with your configuration.

If the running version of Terraform doesn't match the constraints specified, Terraform will produce an error and exit without taking any further actions.

```
terraform {  
    required_version = "> 0.12.0"  
}
```

Versioning Arguments

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

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

Important Pointers for Exams - 6

Let's get Certified

Fetching Values from Map

To reference to image-abc from the below map, following approaches needs to be used:

```
var.ami_ids["mumbai"]
```

```
variable "ami_ids" {
  type = "map"
  default = {
    "mumbai" = "image-abc"
    "germany" = "image-def"
    "states"  = "image-xyz"
  }
}
```

Terraform and GIT - Part 1

If you are making use of 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)

.

Terraform and GIT - Part 2

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

After this prefix, any valid Git URL can be specified to select one of the protocols supported by Git.

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

module "storage" {
    source = "git::ssh://username@example.com/storage.git"
}
```

Terraform and GIT - Part 3

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:

```
module "vpc" {  
    source = "git::https://example.com/vpc.git?ref=v1.2.0"  
}
```

The value of the ref argument can be any reference that would be accepted by the git checkout command, including branch and tag names.

Terraform Workspace

- Workspaces are managed with the `terraform workspace` set of commands.
- 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 workspace new bar  
Created and switched to workspace "bar"!
```

You're now on a new, empty workspace. Workspaces isolate their state, so if you run "terraform plan" Terraform will not see any existing state for this configuration.

Dependency Types - Implicit

With implicit dependency, Terraform can automatically find references of the object, and create an implicit ordering requirement between the two resources.

```
resource "aws_eip" "my_eip"{
    vpc = "true"
}

resource "aws_instance" "my_ec2" {
    instance_type = "t2.micro"
    public_ip     = aws_eip.myeip.private_ip
}
```

Dependency Types - 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.

```
resource "aws_s3_bucket" "example" {
    acl      = "private"
}

resource "aws_instance" "myec2" {
    instance_type = "t2.micro"
    depends_on   = [aws_s3_bucket.example]
}
```

State Command

Rather than modify the state directly, the terraform state commands can be used in many cases instead.

State Command	Description
terraform state list	List resources within terraform state
terraform state mv	Move items within terraform state. Can be used to resource renaming.
terraform state pull	manually download and output the state from state file.
terraform state rm	Remove Items from terraform state file.
Terraform state show	Show the attributes of a single resource in the Terraform state.

Data Source Code

- Data sources allow data to be fetched or computed for use elsewhere in Terraform configuration.
- Reads from a specific data source (aws_ami) and exports results under “app_ami”

```
data "aws_ami" "app_ami" {  
    most_recent = true  
    owners = ["amazon"]  
  
    filter {  
        name    = "name"  
        values  = ["amzn2-ami-hvm*"]  
    }  
}
```



```
resource "aws_instance" "instance-1" {  
    ami = data.aws_ami.app_ami.id  
    instance_type = "t2.micro"  
}
```

Terraform taint

Terraform Taint can also be used to taint resource within a module.

```
terraform taint [options] address
```

```
$ terraform taint "module.couchbase.aws_instance.cb_node[9]"  
Resource instance module.couchbase.aws_instance.cb_node[9] has been marked as tainted.
```

For multiple sub modules, following syntax-based example can be used

```
module.foo.module.bar.aws_instance.qux
```

Terraform Plan Destroy

The behavior of any terraform destroy command can be previewed at any time with an equivalent [terraform plan -destroy](#) command.

```
C:\Users\Zeal Vora\Desktop\terraform\tmp\1>terraform plan -destroy
Refreshing Terraform state in-memory prior to plan...
The refreshed state will be used to calculate this plan, but will not be
persisted to local or remote state storage.

-----
An execution plan has been generated and is shown below.
Resource actions are indicated with the following symbols:

Terraform will perform the following actions:

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

Changes to Outputs:
  - test = [
      - "host1",
      - "host2",
      - "host3",
    ] -> null
```

Terraform Module Sources

The module installer supports installation from a number of different source types like Local paths, Terraform Registry, GitHub, S3 buckets and others.

Local path references allow for factoring out portions of a configuration within a single source repository.

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

```
module "consul" {
    source = "../consul"
}
```

Dealing with Larger Infrastructure

Cloud Providers has certain amount of rate limiting set so Terraform can only request certain amount 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)

Miscellaneous Pointers

lookup retrieves the value of a single element from a map

```
lookup(map, key, default)
```

Various commands runs terraform refresh implicitly, some of these include:

terraform [plan, apply, destroy]

Others like terraform [init, import] do not run refresh implicitly.

Array Datatype is not supported in Terraform.

Miscellaneous Pointers -2

Various variable definition files will be loaded automatically in terraform. These include:

- `terraform.tfvars`
- `terraform.tfvars.json`
- Any files with names ending in `.auto.tfvars.json`

Both implicit and explicit dependency information is stored in `terraform.tfstate` file.

`terraform init -upgrade` updates all previously installed plugins to the newest version.

Miscellaneous Pointers -3

The terraform console command provides an interactive console for evaluating expressions.

Difference 0.11 and 0.12

- “\${var.instance_type}” → 0.11
- var.instance_type → 0.12

Miscellaneous Pointers -3

If you have multiple modules and you want to export a value from one module to be imported into another module,

Difference 0.11 and 0.12

- “\${var.instance_type}” → 0.11
- var.instance_type → 0.12