TERRAFORM : it is an open-source infrastructure as code (IaC) tool. It enables you to define, provision, and manage your infrastructure resources across various cloud providers and on premises.

A diagram of a terraform process

AI-generated content may be incorrect.

1. Write:

Before any commands are executed, you define your infrastructure's desired state in human-readable configuration files, typically ending in .tf. This code specifies the resources you want to create, such as virtual machines, networking, and databases.

2. Initialize (terraform init):

This command prepares the working directory for use with Terraform. It performs the following setup tasks:

Downloads the necessary provider plugins for the services specified in your configuration (e.g., AWS, Azure, Google Cloud).

Initializes the backend, which is where Terraform stores its state file. This file is critical for tracking your managed infrastructure.

Downloads any modules the configuration depends on.

3. Plan (terraform plan):

The plan command creates an execution plan that shows exactly what Terraform will do to match the desired state defined in your configuration files.

Compares states: It reads the current state of your resources, compares it to the desired state in your code, and identifies any differences.

Shows actions: It outputs a list of changes, such as which resources will be added, modified, or destroyed.

Does not change infrastructure: This is a dry run that allows you to review and verify the changes before they are actually applied.

4. Apply (terraform apply):

The apply command executes the changes defined in the execution plan.

Provisioning: It creates, updates, or deletes infrastructure resources according to the plan.

Updates state: It updates the state file to reflect the new state of the managed infrastructure.

Confirms changes: By default, it requires confirmation before applying the changes, which serves as a safety measure.

5. Destroy (terraform destroy):

When infrastructure is no longer needed, the destroy command is used to clean up all resources managed by a specific Terraform configuration.

Destroys all managed resources: It looks at the state file to identify and then terminate all resources that were created by that configuration.

Deletes resources permanently: This is a permanent and irreversible action that should be used with extreme caution, especially in production environments.

EC2 COMPONENTS:

The main components of an Amazon EC2 instance are the virtual machine itself, the templates used to create it, storage options, and networking and security controls. These elements work together to provide scalable and configurable compute capacity in the cloud.

VIRTUAL MACHINE AND CONFIGURATION:

1.EC2 Instance: A virtual server that you can launch, stop, and terminate as your needs change. It is defined by its core hardware components, including CPU, memory, storage, and networking capacity.

2.Amazon Machine Image (AMI): A pre-configured template that contains the operating system and any initial software or application servers needed to launch your instance. You can choose from various AMIs provided by AWS or the user community, purchase one from the AWS Marketplace, or create your own custom AMI.

3.Instance Type: Specifies the hardware profile of your instance, which includes the amount of CPU, memory, and storage. AWS offers different instance families, such as general purpose, compute optimized, and memory optimized, so you can select the most appropriate option for your application's workload.

STORAGE OPTIONS:

1.Amazon Elastic Block Store (EBS): This provides persistent, network-attached block-level storage volumes for your EC2 instance. Your data remains intact on the EBS volume even if you stop or terminate the instance, and you can attach it to another instance as needed.

2.Instance Store: This is temporary, block-level storage directly attached to the physical host computer. It offers very high input/output performance, but all data on the instance store is lost when the instance is stopped or terminated.

NETWORKINFG AND SECURITY:

1.Virtual Private Cloud (VPC): A logically isolated network where you can launch your EC2 instance. This gives you full control over your virtual networking environment, including IP address ranges, subnets, and route tables.

2.Security Group: Functions as a virtual firewall for your instance to control inbound and outbound traffic. You can set rules to specify which protocols, ports, and source/destination IP addresses are allowed to communicate with your instance.

3.Elastic IP (EIP): A static, public IPv4 address designed for dynamic cloud computing. Unlike a normal public IP address that changes when an instance is stopped and started, an EIP is associated with your account and can be remapped to a different instance to mask instance failures.

4.Key Pair: A pair of cryptographic keys used to securely connect to your instance. AWS stores the public key, and you store the private key, which is used for authentication via SSH for Linux instances or RDP for Windows.

5.EC2 User Data: A feature that allows you to provide a script that is automatically executed when an instance is first launched. This can be used to perform tasks like installing software, configuring applications, or joining the instance to a domain.

SUPPORTING SERVICES:

1.Elastic Load Balancer (ELB): A service that automatically distributes incoming application traffic across multiple EC2 instances to increase your application's availability and fault tolerance.

2.Auto Scaling: A service that helps you automatically adjust the number of EC2 instances in a group based on demand. This ensures your application can handle traffic spikes and reduces costs during quiet periods.

3Amazon CloudWatch: A monitoring service for your AWS cloud resources, including EC2 instances. It collects and tracks metrics like CPU utilization, network traffic, and disk performance, and can be used to set alarms that trigger Auto Scaling policies.