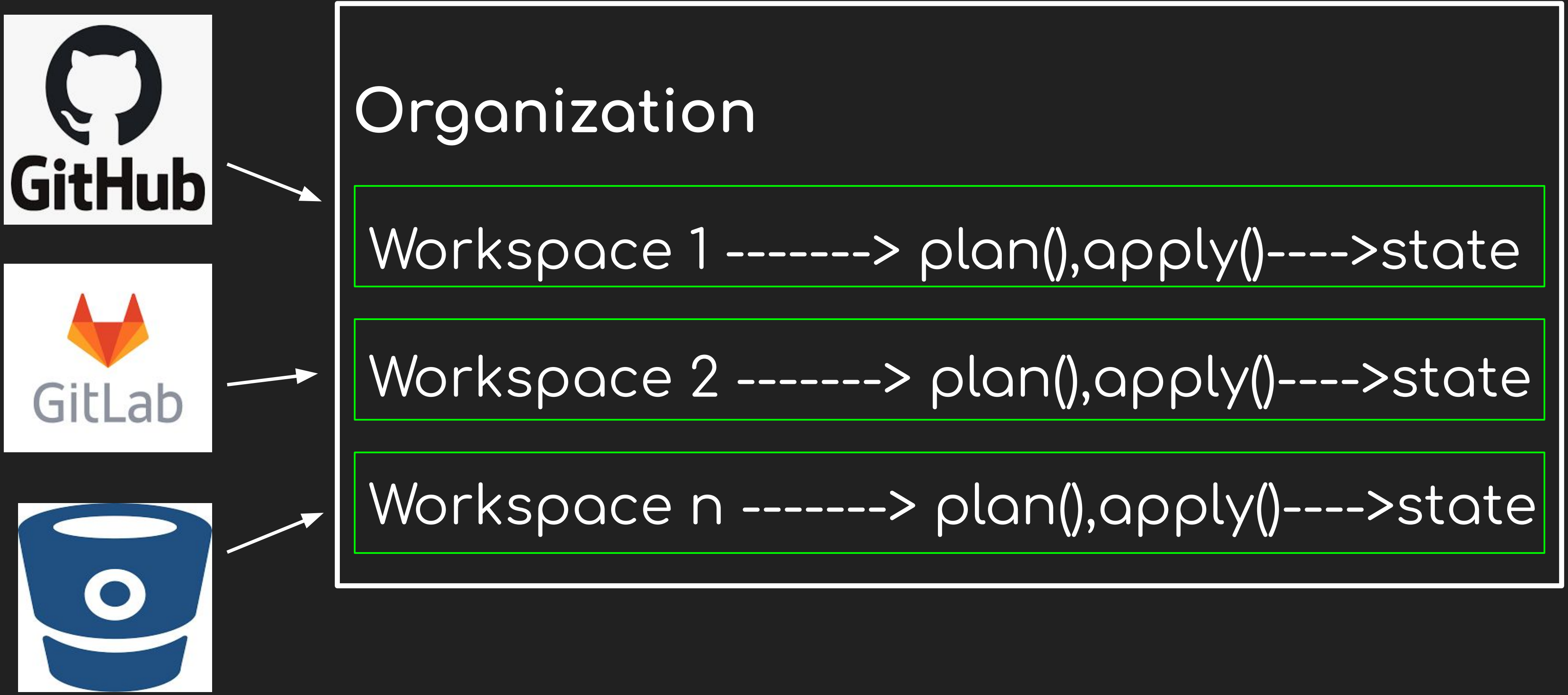
Section 9

Understanding Terraform Cloud and Enterprise

Terraform cloud overview

Terraform cloud



Organization

Workspace 1 -------> plan(),apply()---->state

Workspace 2 -------> plan(),apply()---->state

Workspace n -------> plan(),apply()---->state

Terraform cloud workspaces deconstruct an infrastructure into an organization with multiple workspaces that can be managed by multiple teams

Workspace can be seen as equivalent of a root module..

Team management with users membership and authentication and authorization can be managed by Terraform organizations as paid feature.

Terraform workspaces in Terraform cloud are composed of the following:

- Configuration .tf files
- state file
- run logs and historical state logs
- Variables ..input and environment

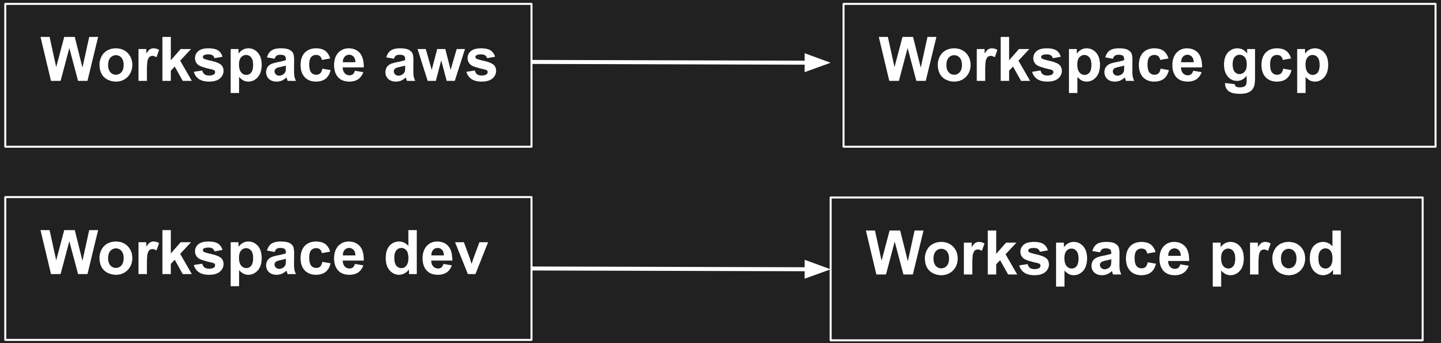
It is different from the cli workspace as it uses the same working directory with various state files associated with each cli workspace stored in the terraform.tfstate.d subdir.

Terraform runs are the Terraform remote operation in each workspace with plan() and apply() to provision terraform managed resources in a provider.

TF cloud uses it own disposable VMs to do TF runs and uses workspaces for config, variables and state files.

TF Runs are queued in the order started and will lock its workspace until the run is executed.

TF run triggers can link workspaces for teams to cowork to provisions resources in one or more infrastructures as in a multi-cloud scenario.



Workspace aws

Workspace gcp

Workspace dev

Workspace prod

Terraform cloud as remote backend with VCS driven runs

Terraform cloud as remote backend using CLI driven runs.

Private Module Registry

With Terraform cloud and enterprise, like the public module registries, the private module registry will allow the sharing of these modules but only to confines of selected teams or organizations in TF cloud or enterprise

Private module registry support the following VCS:

- GitHub, GitLab, BitBucket, Azure devops server

Migrating local backend to Terraform cloud

- Migration to terraform cloud is done using a backend configuration using remote type.

- Need to create an organization first but workspace can be created automatically using the workspace argument.

- Once the migration is complete, you have to delete or rename the local backend state.file.

Sentinel or policy-as-code

Terraform provision infrastructure in the cloud, it is critical to provide secure configuration guardrails.

Per Gartner, 99% of attacks are caused my cloud misconfigurations or too permissive IAM rules.

Terraform sentinel is a paid feature as part of the teams & governance process.

The Sentinel language is a high level programing than can be used that can be used by non-programmers.

Sentinel is a stage in a run between plan() and apply() to perform configuration compliance prior to applying the execution plan.

Sentinel allows the creation of policies on an organization level using sentinel language that are organized in policy sets and stored in VCS.

Policies are declared in .sentinel files and have to be in the same directory as the sentinel.hcl file.

Sentinel policy uses enforcement levels defined in the sentinel.hcl file

- Hard-mandatory- cannot override
- Soft-mandatory- can override
- Advisory - logging only

Policy sets enforced on all or on a per workspace basis.
NOTE: The use of individual policies is now deprecated.

cost estimation in Terraform cloud

Terraform will estimate the cost of a per run basis with an estimated average monthly cost per resource.

Not available for all resource types.

Supported clouds are AWS, Azure and Google.

Comparing Terraform cloud and Terraform enterprise

Terraform cloud is a SaaS that provide the ability for small teams to use a remote backend. It also provides authentication, team collaboration, change approval, private module registry

Terraform enterprise is a private local data center install to provide a self service infrastructure with custom security and policy controls like SSO, governance as well as audit logs.

CLOUD

- VCS Integration
- Workspace Management
- Secure Variable Storage
- Remote Runs & Applies
- Full API Coverage
- Private Module Registry
- Roles / Team Management
- Sentinel
- Cost Estimation

vs

ENTERPRISE

- VCS Integration
- Workspace Management
- Secure Variable Storage
- Remote Runs & Applies
- Full API Coverage
- Private Module Registry
- Roles / Team Management
- Sentinel
- Cost Estimation
- SAML / SSO
- Private DC Installation
- Private Network Connectivity
- Self-Hosted
- Audit Logs