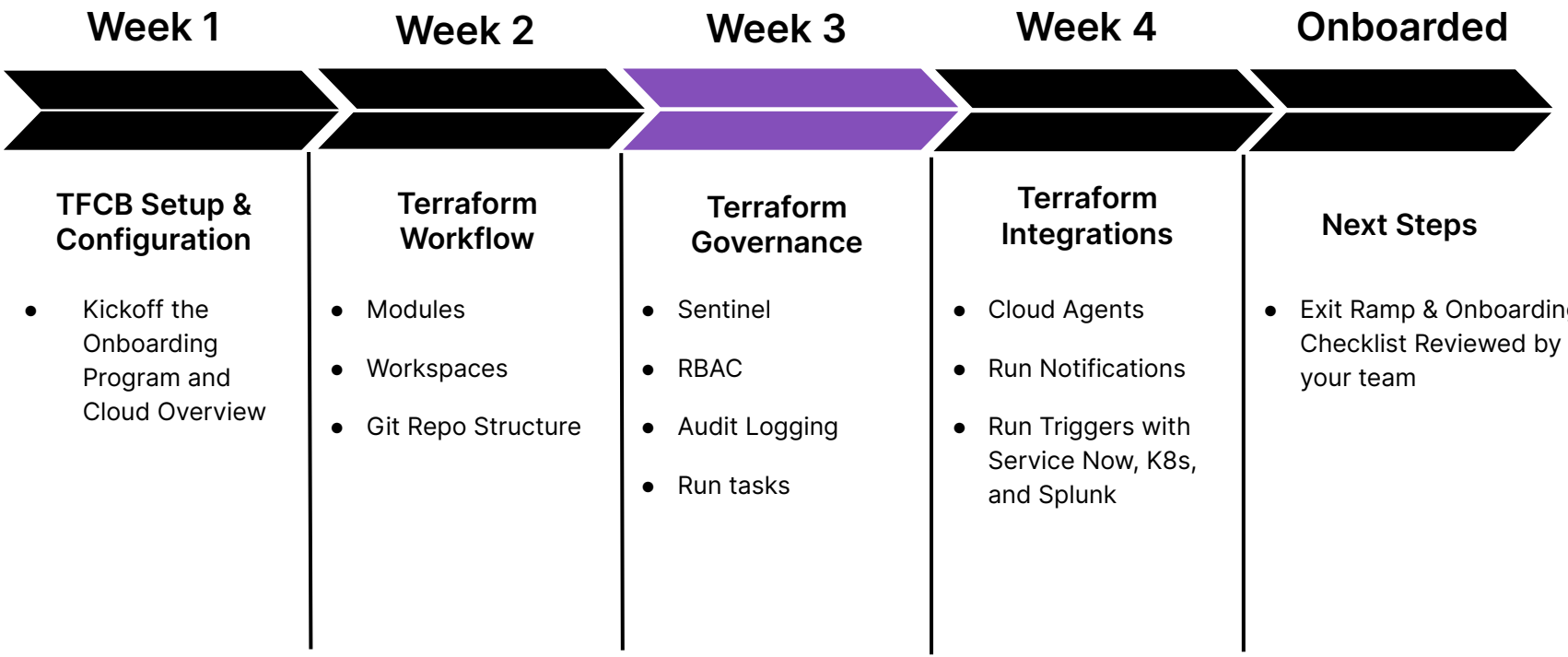
HashiCorp Terraform

TFCB Onboarding Program Week 3

HashiCorp Customer Success

TFCB Path to Production



Terraform Cloud Governance

Agenda

01

Role Based Access Controls (RBAC)

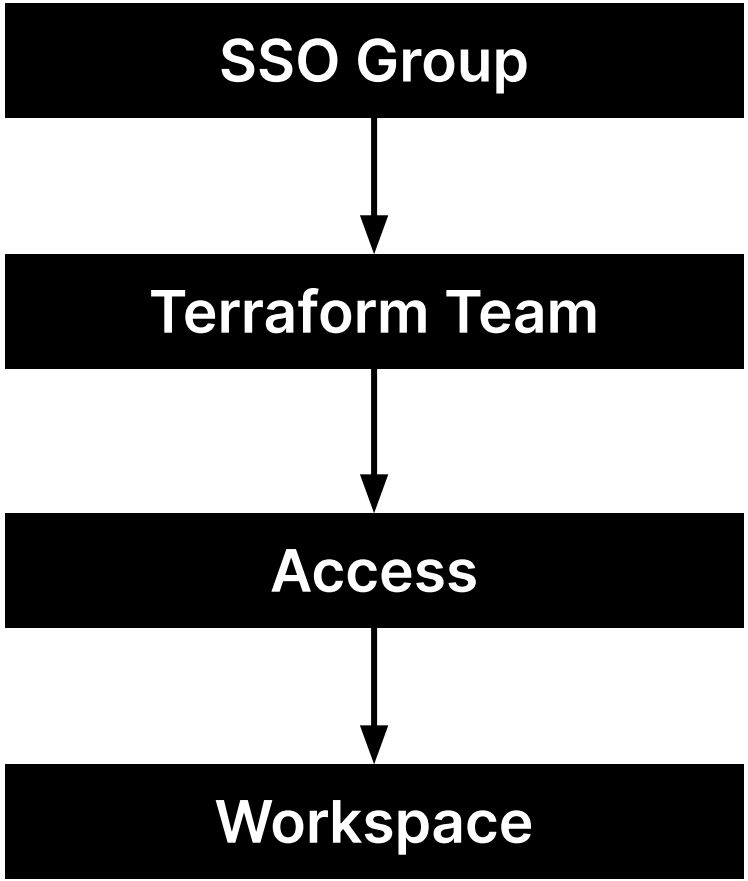
Terraform Cloud RBAC Model

- Terraform Cloud's (TFCB) access model is team-based
  - Permissions are assigned at the team level
  - Users inherit permissions based upon team assignment
- TFCB's permission model is split into organization-level & workspace-level permissions
- Every Org has an "owners" team which have every available permission in that org
- Workspace permissions allow administrators to delegate access to specific collections of infrastructure

Common Scenarios

- TFC is often used by multiple Teams (i.e. *Developers*, *QA*, *Security*, *Operations*, *Networking*, *SQL Admins*, *Filestore Admins*, *Accounting*)
- The best approach to managing permissions is:
  a. Create Groups within your Single Sign-on (SSO) service for each team
  b. Assign each group as a TFC Team
  c. Determine how Workspaces will be divided, & assign permissions accordingly
- Data can be dynamically shared between Workspaces as read-only by using the **“tfe_outputs”** data source
- `Terraform_remote_state` Data Source

TFCB Permissions Flow



Workspace Permissions

There are two ways to assign permissions to a TFCB team:

1. Custom permissions
2. Fixed permission sets - bundles of specific permissions, designed for delegated access patterns

Permission Sets

Read

- Read runs
- Read variables
- Read state versions

Plan

- Queue plans
- Read variables
- Read state versions

Admin

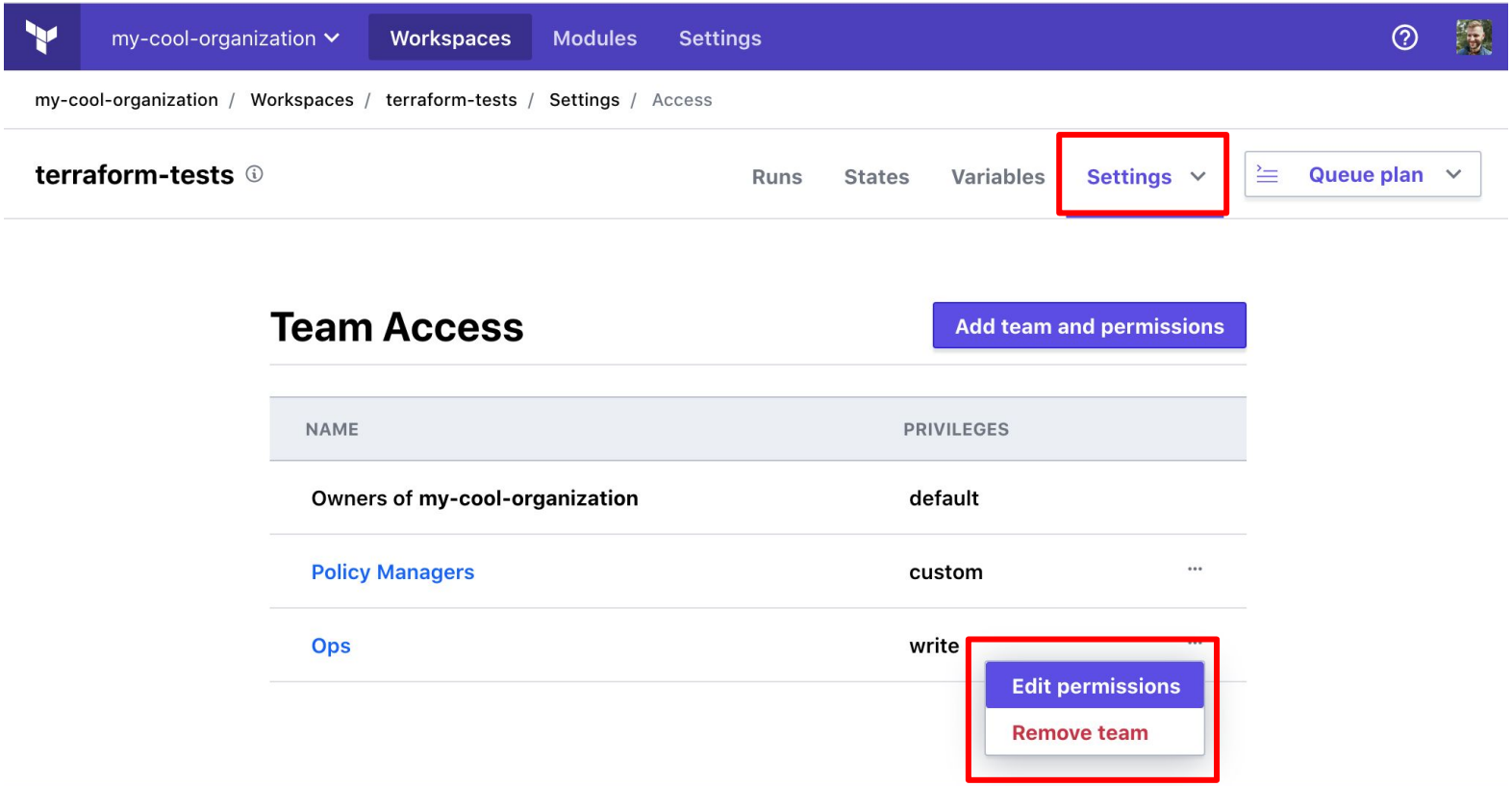
- VCS Configuration
- Manage Team Access
- Execution Mode
- Delete Workspace
- Read & write workspace settings, general settings, notification configurations, run triggers, & more

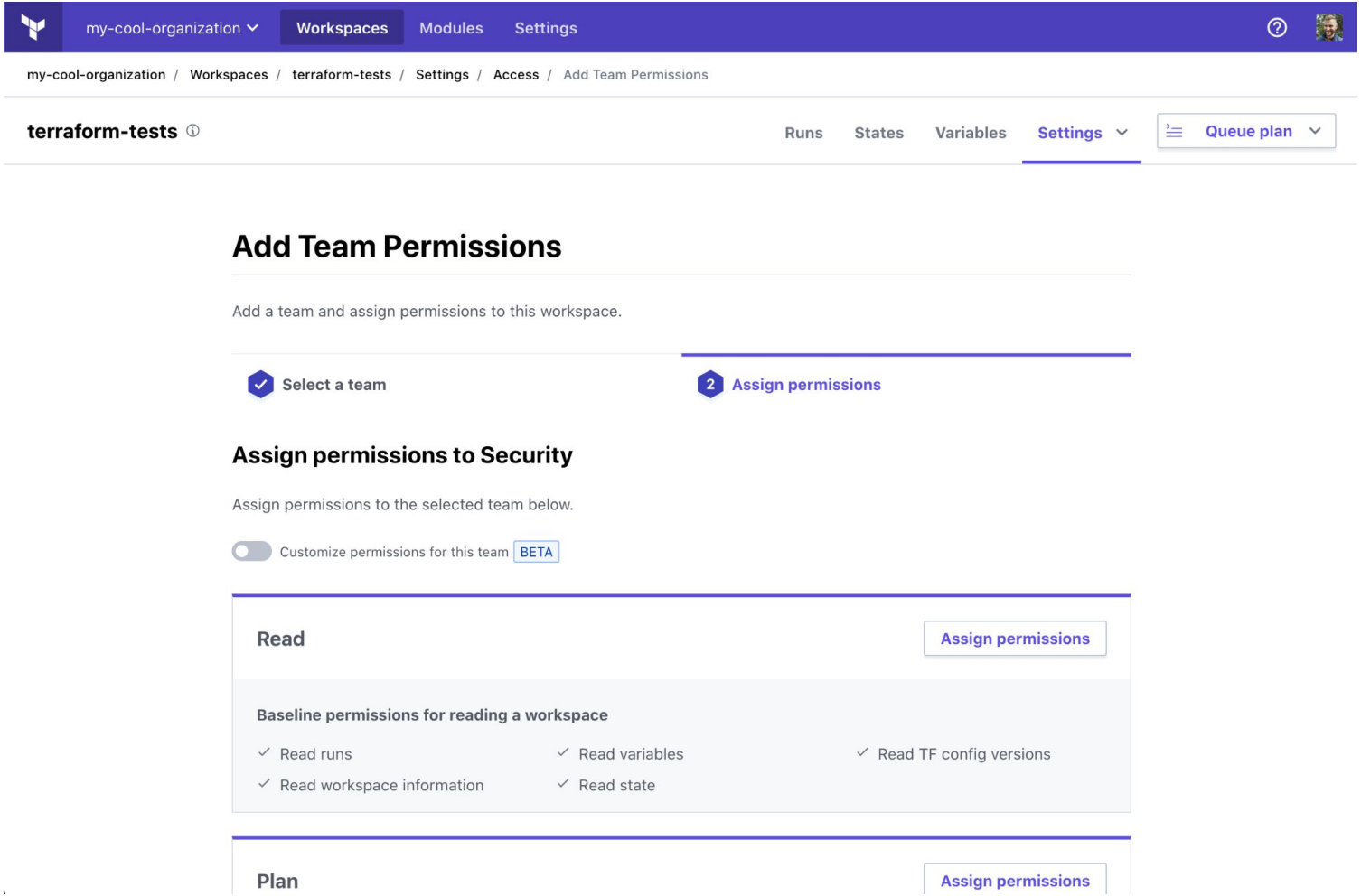
Write

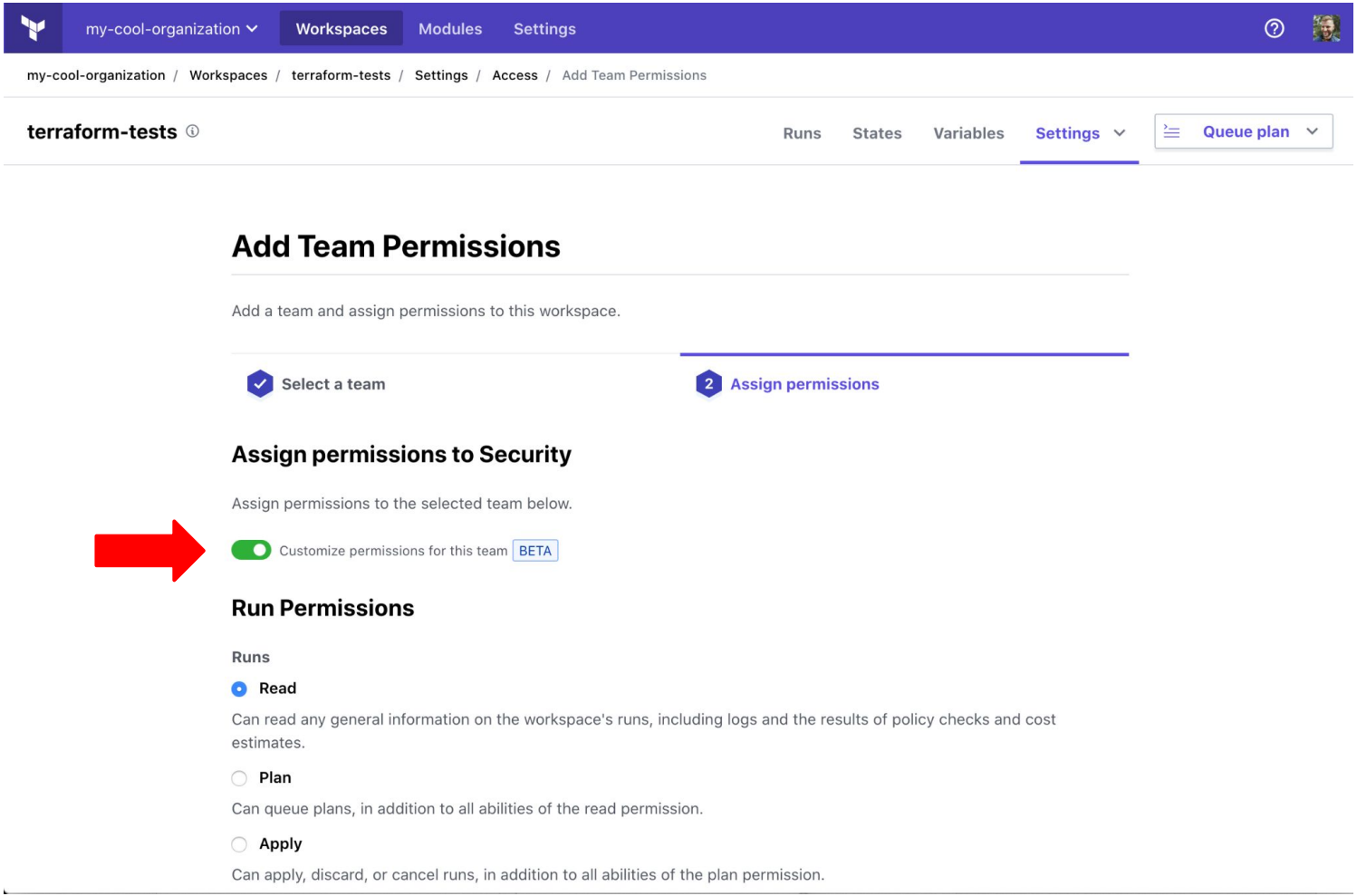
- Lock/unlock Workspace
- Download Sentinel mocks
- Read and write Variables
- Read and write State Versions
- Approve Runs

State Files

- May contain secrets, passwords, & API Tokens
- Should be handled as sensitive material when applying RBAC permissions
- Are encrypted at rest using HashiCorp Vault
- Data can still be read at runtime or directly from the TFC UI if a User has the necessary Workspace permissions


my-cool-organization
Workspaces
Modules
Settings
my-cool-organization / Workspaces / terraform-tests / Settings / Access
terraform-tests
Runs
States
Variables
Settings
Queue plan
Team Access
Add team and permissions
NAME
PRIVILEGES
Owners of my-cool-organization
default
Policy Managers
custom
Ops
write
Edit permissions
Remove team
© 2020 HashiCorp, Inc.
Support
Terms
Privacy
Security


my-cool-organization
Workspaces
Modules
Settings
my-cool-organization / Workspaces / terraform-tests / Settings / Access / Add Team Permissions
terraform-tests
Runs
States
Variables
Settings
Queue plan
Add Team Permissions
Add a team and assign permissions to this workspace.
Select a team
2
Assign permissions
Assign permissions to the selected team below.
Customize permissions for this team
BETA
Read
Assign permissions
Baseline permissions for reading a workspace
Read runs
Read variables
Read TF config versions
Read workspace information
Read state
Plan
Assign permissions


my-cool-organization
Workspaces
Modules
Settings
my-cool-organization / Workspaces / terraform-tests / Settings / Access / Add Team Permissions
terraform-tests
Runs
States
Variables
Settings
Queue plan
Add Team Permissions
Add a team and assign permissions to this workspace.
Select a team
2
Assign permissions
Assign permissions to Security
Assign permissions to the selected team below.
Customize permissions for this team
BETA
Run Permissions
Runs
Read
Can read any general information on the workspace's runs, including logs and the results of policy checks and cost estimates.
Plan
Can queue plans, in addition to all abilities of the read permission.
Apply
Can apply, discard, or cancel runs, in addition to all abilities of the plan permission.

02

Sentinel

Sentinel is: “Policy, Governance, & Security as Code”

Use Cases

1. Cloud Provider
2. Account ID
3. Limit Availability Zones
4. Cost Estimates
5. Cost Limiting
6. Resource Tagging
7. Resource Types
8. Resource Sizes
9. Resource Configuration
10. Resource Destruction

Benefits

1. Enforcement
2. Speed
3. Reproducibility
4. Reliability
5. Automation
6. Version Control
7. Auditability

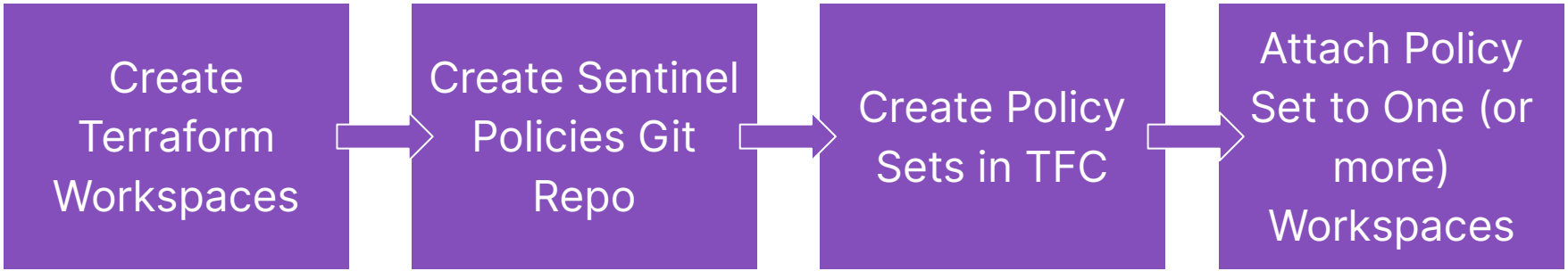
Architecture

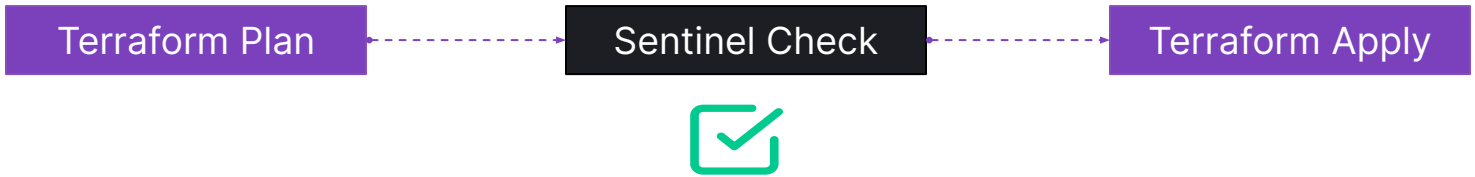
- Variables, conditionals, loops, functions
  - Sentinel Language Reference
- Validates Config and State (Create, Edit, Destroy) of Terraform resources
- terraform plan → sentinel check → terraform apply
- Enforcement Levels – all are Logged
  - **Hard-mandatory**, required, cannot bypass, fail the TF RUN (prod)
  - **Soft-mandatory**, required, TF Owner can bypass with a comment in the TF UI, will halt the TF Run
  - **Advisory**, guard-rails warning, info warnings in the TF Run

Syntax Example

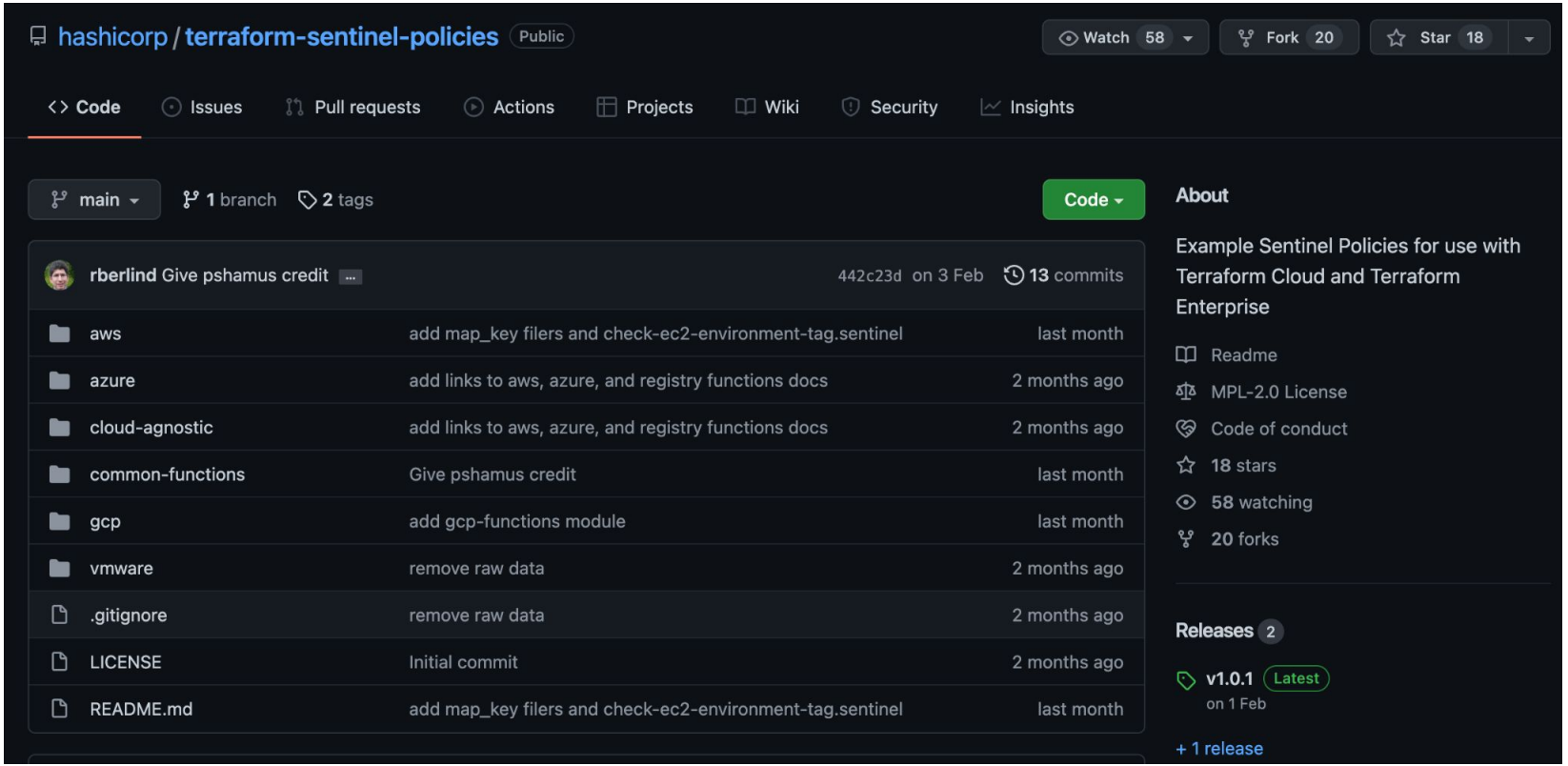
```
import "units"

memory = func(job) {
  result = 0
  for job.groups as g {
    for g.tasks as t {
      result += t.resources.memory else 0
    }
  }

  return result
}

main = rule {
  memory(job) < 1 * units.gigabyte
}
```

Workflow

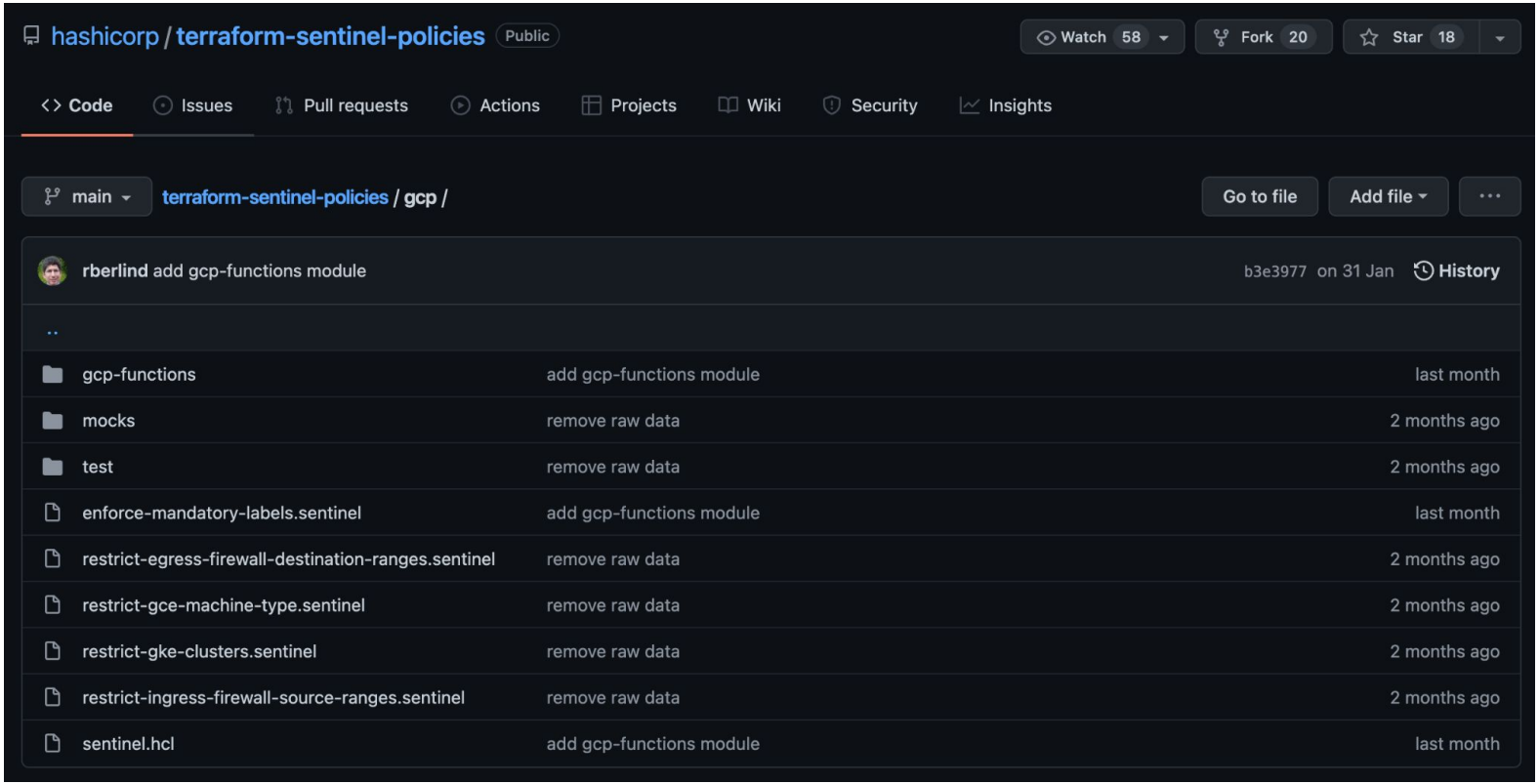




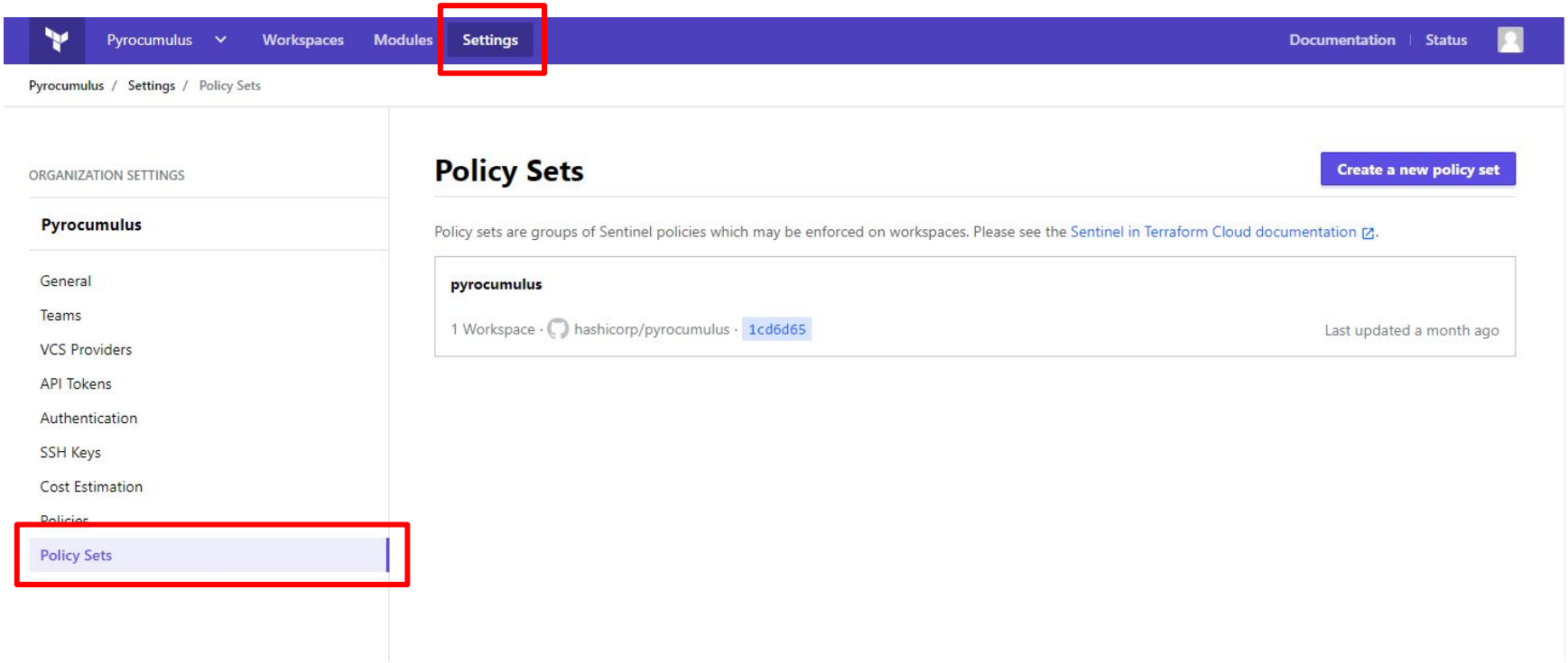
Sentinel Rule Git Repo



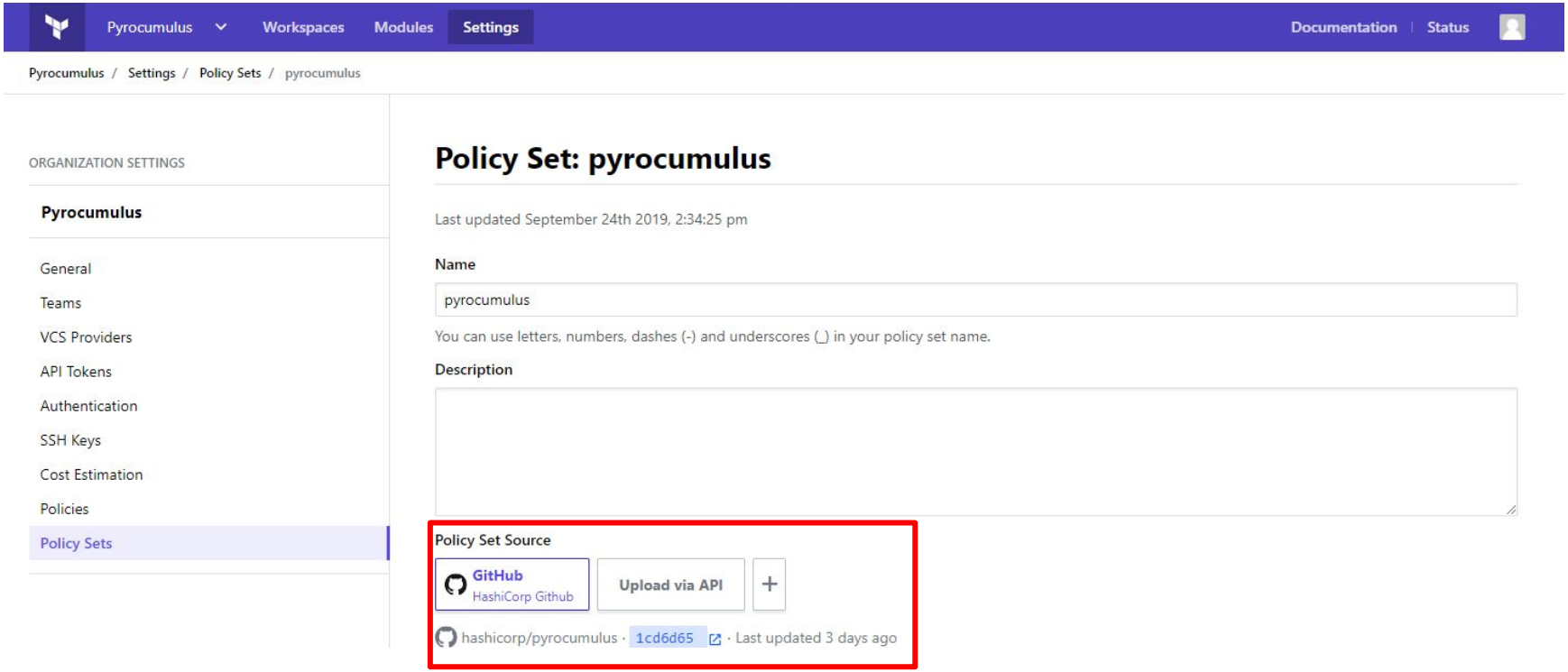
Policy Set File Structure



Policy Sets



Create Policy Set



Attach Policy Set

Automate Sentinel to Workspaces

```
# Get a list of Workspace IDs, based on matching a Regex pattern
variable "workspace_name_pattern" {
  type = string
  default = ".*_dev_vdm"
}
data "tfe_workspace_ids" "all" {
  names = ["*"]
  organization = var.tf_org_name
}
output "all_workspace_ids" { value = data.tfe_workspace_ids.all.ids }
locals {
  # filter by the Workspace Name, then return the Workspace ID, or null, then remove null entries
  filtered_workspace_ids = compact(flatten([
    for name, id in data.tfe_workspace_ids.all.ids : [
      (length(regexall(var.workspace_name_pattern, name)) > 0) ? id : null
    ]
  ]))
}
output "filtered_workspace_ids" { value = local.filtered_workspace_ids }
```

Limitations

1. Can only enforce against resources deployed & managed by Terraform
2. Cannot enforce “self-managed” services (ex: mysql on AWS EC2, Azure VM, GCP VM, VMware VM)
3. Cannot enforce against resource logs / metrics (ex: AWS CloudTrail, Azure Monitor, GCP Cloud Audit Logs)
4. Cannot continuously monitor (ex: AWS Config, Azure Policy, GCP Forseti)
5. Sentinel uses the Cloud Provider’s Cost Estimation API, which doesn’t continuously run, & does not check costs for usage-based billing (ex: AWS Athena, Azure DataBricks, GCP BigQuery, GCP Pub/Sub)

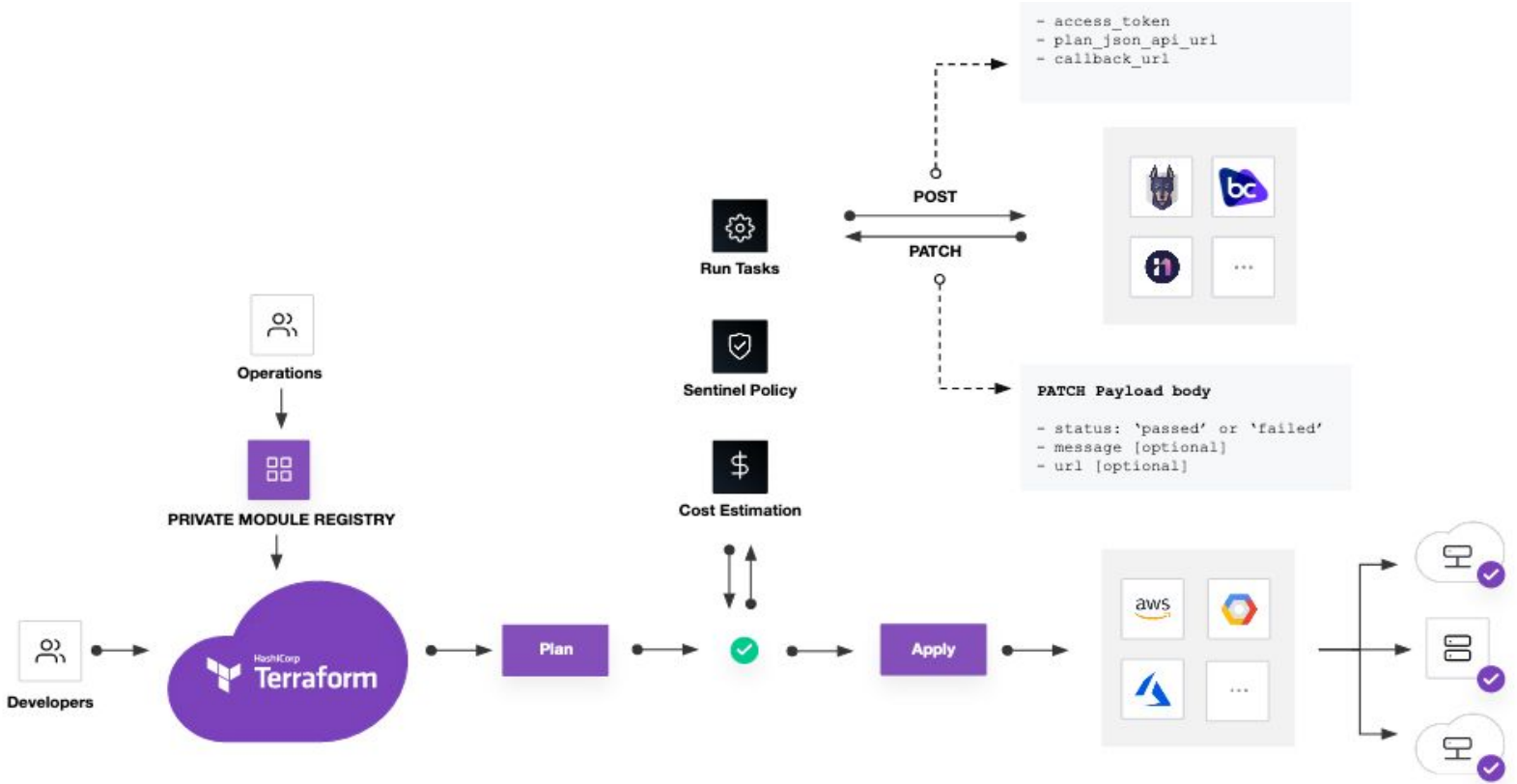
03

Run Tasks

Run Tasks

- Integrate 3rd-party tools into the pre-apply stage during a Terraform Cloud run
  - During pre-apply phase, an event hook is triggered & TFCB sends a payload containing run details
  - Terraform waits for the service to reply with either passed or failed status
- Supported integrations
  - Snyk, Bridgecrew, Infracost, Lightlytics, Vantage
  - HCP Packer

Architecture of Run Tasks



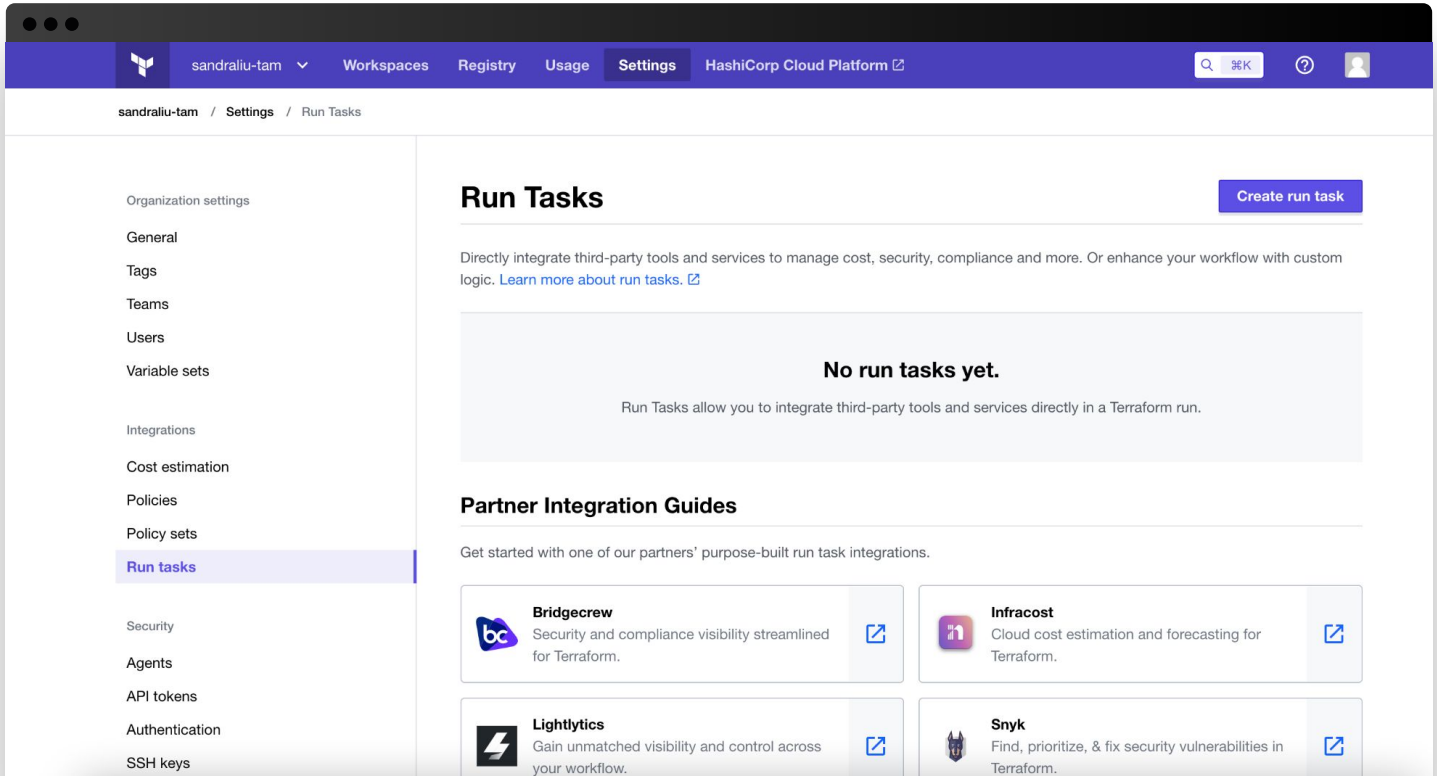
Payload from Terraform

CODE EDITOR


```
{
  "payload_version": 1,
  "access_token": "4QEuyyxug1f2rw.atlasv1.iDyxqhXGVZ0ykes53YdQyHyYtFOrdAWNBxcVUgWvzb64NFHjcquu8gJMEdUwoSLRu4Q
  "task_result_id": "taskrs-2nH5dncYoXaMVQmJ",
  "task_result_enforcement_level": "mandatory",
  "task_result_callback_url":
"https://app.terraform.io/api/v2/task-results/5ea8d46c-2ceb-42cd-83f2-82e54697bddd/callback",
  "run_app_url": "https://app.terraform.io/app/hashicorp/my-workspace/runs/run-i3Df5to9ELvibKpQ",
  "run_id": "run-i3Df5to9ELvibKpQ",
  "run_message": "Triggered via UI",
  "run_created_at": "2021-09-02T14:47:13.036Z",
  "run_created_by": "username",
  "workspace_id": "ws-ck4G5bb1Yei5szRh",
  "workspace_name": "tfr_github_0",
  "workspace_app_url": "https://app.terraform.io/app/hashicorp/my-workspace",
  "organization_name": "hashicorp",
  "plan_json_api_url": "https://app.terraform.io/api/v2/plans/plan-6AFmRJW1PFJ7qbAh/json-output",
  "vcs_repo_url": "https://github.com/hashicorp/terraform-random",
  "vcs_branch": "main",
  "vcs_pull_request_url": null,
  "vcs_commit_url":
"https://github.com/hashicorp/terraform-random/commit/7d8fb2a2d601edebdb7a59ad2088a96673637d22"
}
```

Create Run Tasks

Organization Settings → Run Tasks → Create run tasks



Run Task Integration with HCP Packer

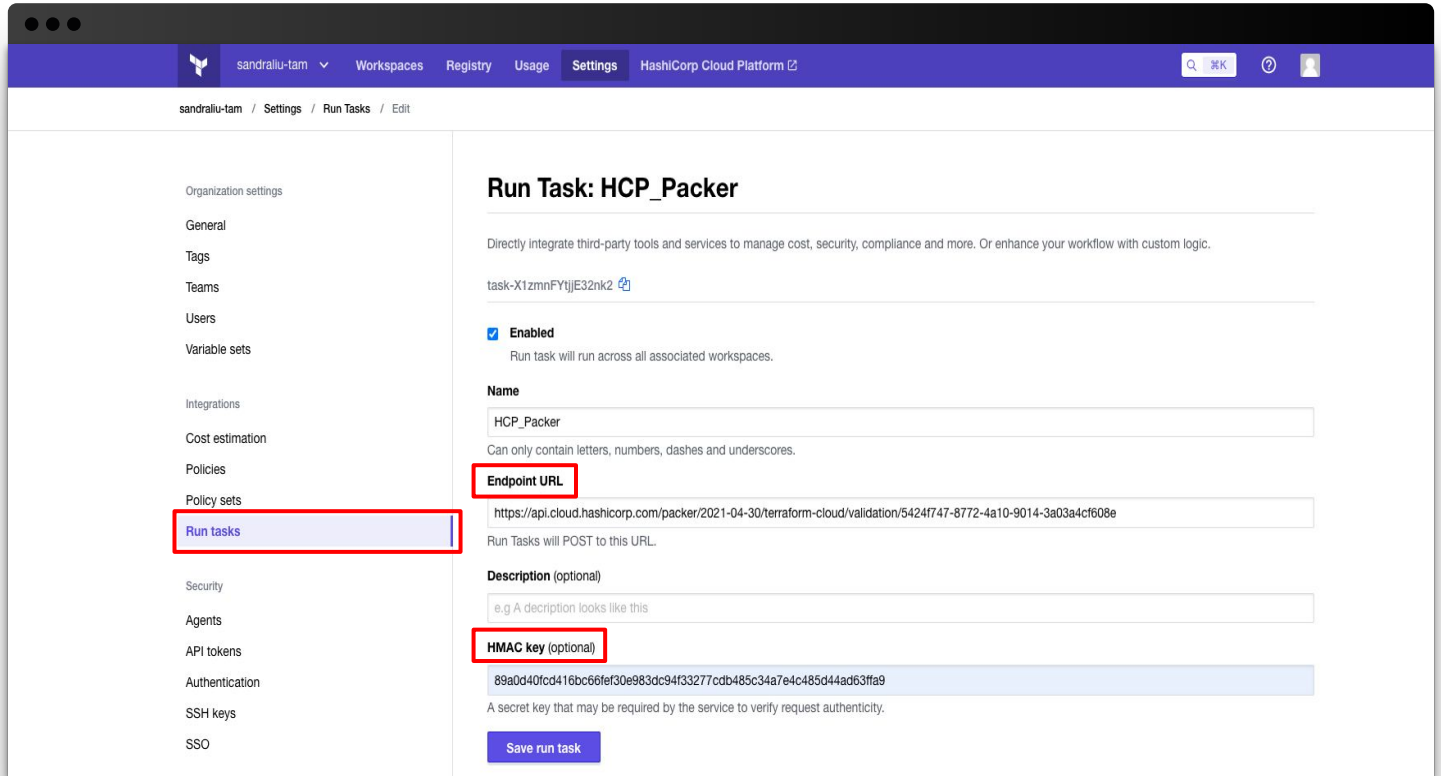
Run Task validates that machine images in your Terraform configuration are valid and haven’t been revoked for security or other reasons

Use-cases

1. Use run tasks with HCP Packer to identify compromised images with Terraform Cloud to prevent images from being outdated
2. Enforce image compliance with Terraform Cloud and let your configuration dynamically use more up to date images as you create them

Create Run Tasks with HCP Packer

Organization Settings → Run Tasks → Create run tasks



Technology Partners

Bridgecrew
Security and compliance errors in Terraform configurations.

cloudtamer.io
Cost savings or compliance findings.

Infracost
A cloud infrastructure costing, initiated right from a pull request or Terraform run.

Lightlytics
Security checks to any additional dependency changes.

Refactr
Allows users to build workflows for multiple use cases including but not limited to code scanning.

Snyk
find, track, and fix security misconfigurations in their cloud infrastructure as part of their SDLC

Future
The up-to-date list is available **here**

04

Audit Logs

Audit Logging

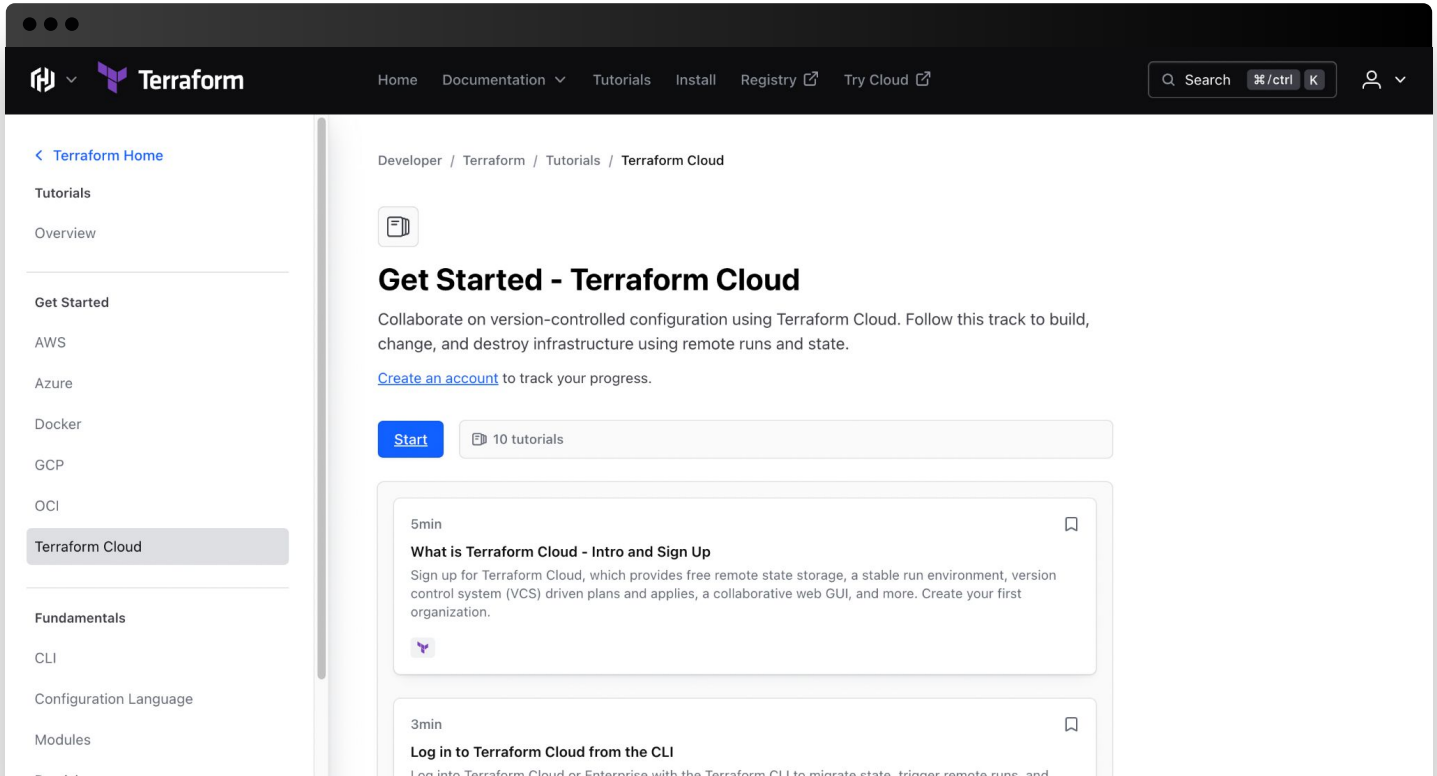
- The audit trails API exposes a stream of audit events, describing changes to the application entities (workspaces, runs, etc.) for a specific TCFB Organization
- Terraform Cloud retains 14 days of audit log information
- Retention beyond 14 days requires ingestion into an external platform or solution
- Endpoint requires an organization token, user token or team token will not work

Next Steps

Tutorials

https://developer.hashicorp.com/terraform/tutorials

Step-by-step guides to accelerate deployment of Terraform Cloud



Resources

Sentinel Policies

- Example Sentinel Policies Collection
- Terraform Foundational Policies Library
- Sentinel Tutorials

Run Tasks

- Run Tasks Documentation
- Run Tasks Integration
- Tutorial: Configure Snyk Run Task in Terraform Cloud

Audit Logging

- Audit Trails API
- Blog - Cloud Compliance & Management with Terraform
- Log Forwarding
- Terraform Cloud Audit Logging with Splunk
- Medium Post - Splunk Integration with TFC

Need Additional Help?

Customer Success

Contact our Customer Success Management team with any questions. We will help coordinate the right resources for you to get your questions answered.

customer.success@hashicorp.com

Technical Support

Something not working quite right? Engage with HashiCorp Technical Support by opening a ticket for your issue at:

support.hashicorp.com.

Discuss

Engage with the HashiCorp Cloud community including HashiCorp Architects and Engineers

discuss.hashicorp.com

Upcoming Webinars

Terraform Integrations/ Program Closing

Deep dive into Cloud Agents, Integration with K8s, ServiceNow, and Splunk, Run Triggers, Run Notifications, if your infrastructure is ready for production, and close out the program.

Q&A

Thank you

customer.success@hashicorp.com

www.hashicorp.com/customer-success