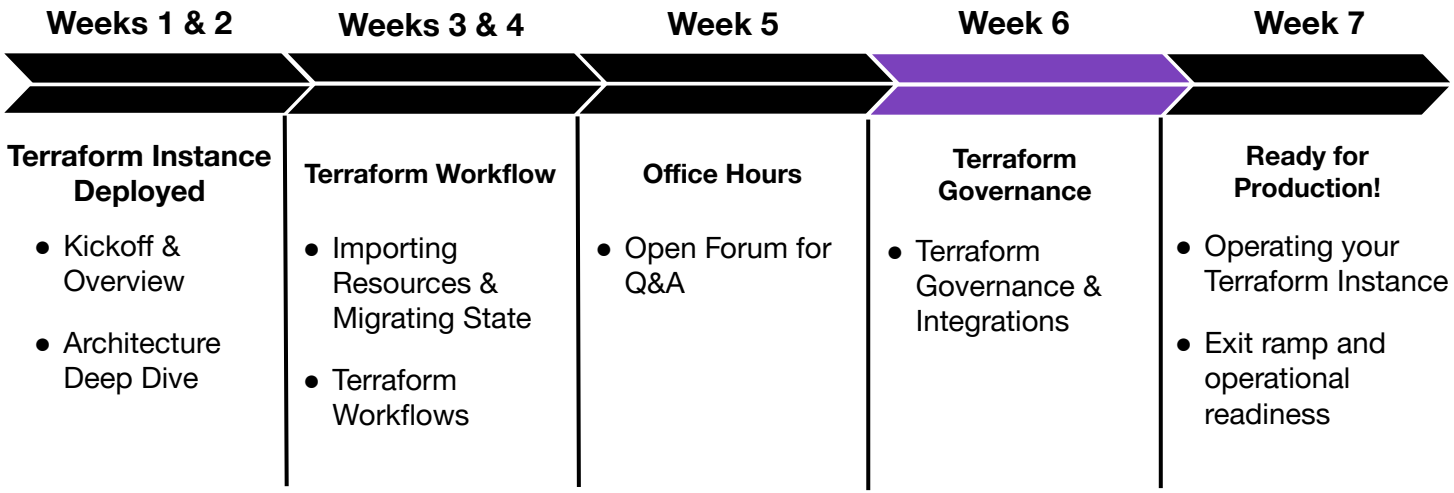
HashiCorp Terraform

Terraform Governance & Integrations

Terraform Enterprise Path to Production



Agenda

1. Role Based Access Controls
2. Cloud Agents
3. Sentinel
4. TFE & ServiceNow
5. Run Triggers & Run Notifications

01

Role Based Access Controls

Terraform Enterprise RBAC Model

- Terraform Enterprise's access model is team-based
  - Permissions are assigned at the team level
  - Users inherit permissions based upon team assignment
- TFE'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

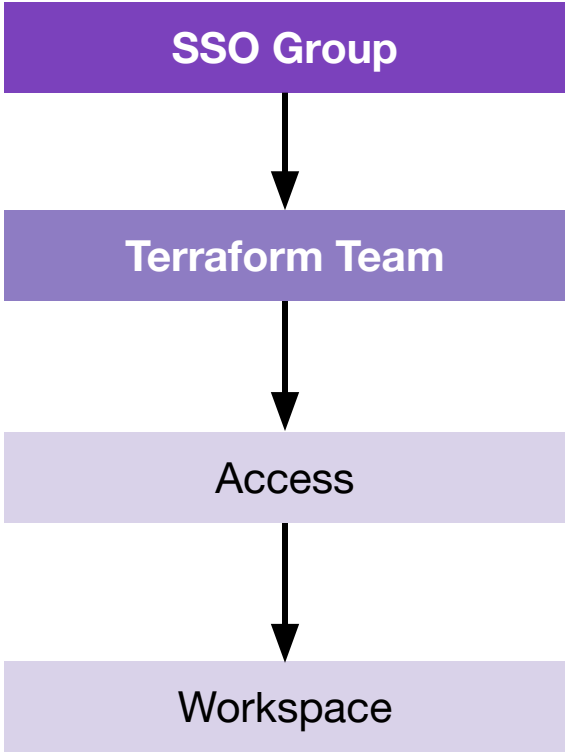
Workspaces and Projects

- Projects let you organize workspaces and scope access to workspace resources
- Each project has a separate permissions set which can be used to manage access to all workspaces in the project
- Project-level permissions
  - More granular than Org-level permissions
  - More specific than workspace-level grants
- Projects added in TFE 202302-1 (Feb 2023)

Common Scenarios

- TFE is often used by multiple Teams (i.e. *Developers, QA, Security, etc)*
- 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 TFE 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

Permissions Flowdown



Workspace & Projects Permissions

- There are two ways to assign permissions to a TFE team:
  - Custom permissions
  - Fixed permission sets - bundles of specific permissions, designed for delegated access patterns
- Each workspace has an “admin” permissions level with full control of the workspace
- Projects have specific permissions that can be assigned to teams
- Members of teams with "admin" permissions for a Project have permissions for every workspace in the project & additional permissions

Workspace Permissions Sets

Read

- Read runs
- Read variables
- Read state versions

Plan

- Queue plans
- Read variables
- Read state versions

Write

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

Admin

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

State Files

- May contain secrets, passwords, and 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 TFE UI if a User has the necessary Workspace permissions

hashicorp-training | Workspaces | Modules | Usage | Settings | HCP

hashicorp-training / Workspaces / dev-webapp / Overview

dev-webapp

No workspace description available. Add workspace description.

Resources: 0

Terraform version: 0.14.8

Updated: 2 minutes ago

Overview | Runs | States | Variables | Settings | Queue plan manually

- General
- Locking
- Notifications
- Run Triggers
- SSH Key
- Team Access
- Version Control
- Destruction and Deletion

Waiti

Checking for configuration

This wor … rm configuration files associat … aiting for the configuration to be upl …

CLI-dr

1. E … ted into Terraform Cloud by runn … e command line or by using a cre …
2. Add … configuration files to set up t … add this configuration bloc … ory where you run Terr …

Example code

```
terraform {
  backend "remote" {
    organization = "hashicorp-training"
```

Execution mode: Remote

Auto apply: Off

Metrics

Data will appear after at least one run.

Contributors (1)

o

hashicorp-training | Workspaces | Modules | Usage | Settings | HCP

hashicorp-training / Workspaces / dev-webapp / Settings / Access

dev-webapp

No workspace description available. Add workspace description.

Resources	Terraform version	Updated
0	0.14.8	2 minutes ago

Overview | Runs | States | Variables | Settings

Queue plan manually

Team Access

Add team and permissions

Heads up
Teams with organization-level permissions can also access this workspace, even if they are not listed on this page or are listed at a lower access level.

NAME	PRIVILEGES
Owners of hashicorp-training	default

hashicorp-training | Workspaces | Modules | Usage | Settings | HCP

hashicorp-training / Workspaces / dev-webapp / Settings / Access / Add Team Permissions

dev-webapp

No workspace description available. Add workspace description.

Resources	Terraform version	Updated
0	0.14.8	2 minutes ago

Overview | Runs | States | Variables | Settings

Queue plan manually

Add Team Permissions

Add a team and assign permissions to this workspace.

1 Select a team

2 Assign permissions

NAME	
Dev-Team	Select team

Plan

Assign permissions

Read permissions plus the ability to create runs

- ✓ All permissions of read
- ✓ Create runs

Write

Assign permissions

Read, plan and write permisions

- ✓ All permissions of plan
- ✓ Can read and write
- ✓ Approve runs
- ✓ Lock/unlock workspace

Team API Token

- A Team can only have a single API token
- The token can be regenerated
- The token capabilities is defined by the roles and permissions of the team
- The token can be used both by the CLI and API
- The token will bypass SSO and MFA
- Tokens can also be generated at Organisation and User level

Admin Roles

Super user roles

Manage Policies

Create, edit and delete Sentinel Policy Sets

Manage Workspaces

Create and administrate all workspaces in the organisation

Manage VCS Settings

Create and manage VCS settings and SSH Keys

Manage Policy Overrides

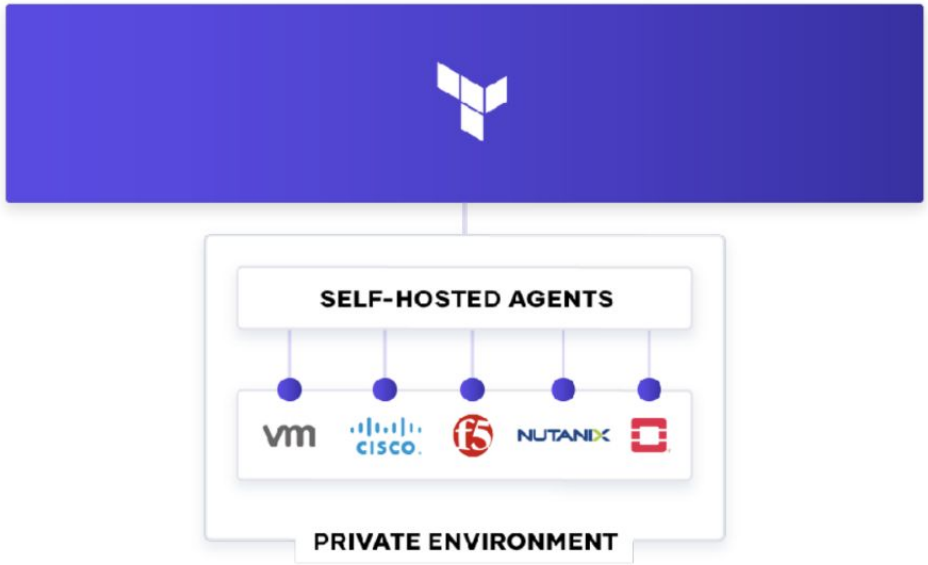
Override ‘soft-mandatory’ policy checks.

02

Cloud Agents

Terraform Cloud Agents

- x86-based Golang binary
- Only outbound connectivity required
- Communicate with isolated, private infrastructure, such as vSphere, Nutanix, OpenStack, or across multiple cloud accounts
- Can be hosted close to target infrastructure
- Deployable on bare metal, a VM, as a Docker container, or in a Kubernetes cluster



Requirements

Supported Platforms

- Baremetal
- Docker
- Kubernetes (K8S)
- Virtual Machine

Hardware Requirements

- x86-based Linux host
- 2 GB of RAM
- 4 GB of disk space

Networking Requirements

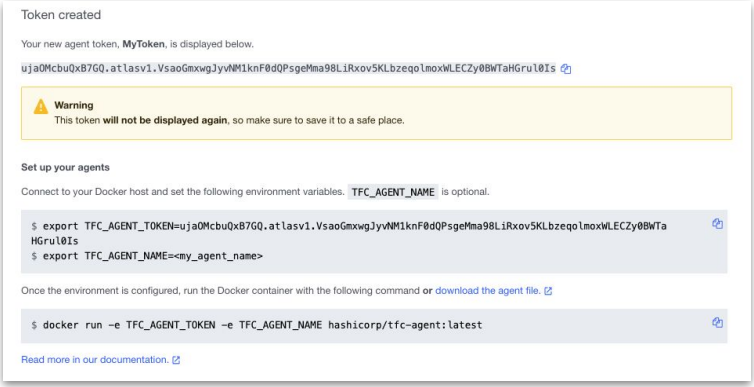
- TFE host via HTTPS (443)
- releases.hashicorp.com
- registry.terraform.io
- (Airgapped) if custom TF CLI binary is used external access is not needed.

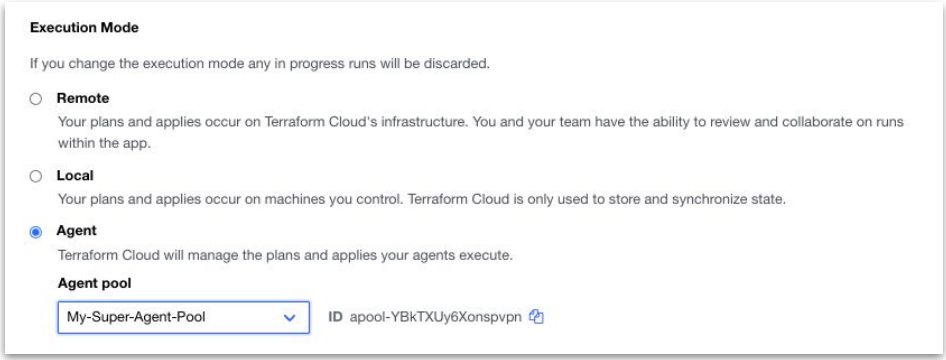
Terraform Cloud Agents

- No restriction on Agent or Agent Pool Count
- Agents must define the TFE hostname via either:
  - -address CLI flag
  - TFC_ADDRESS environment variable
- Agents support custom Terraform bundles
- Must be able to communicate with the TFE instance via **HTTPS**
- There are some restrictions on what versions of Agents can be registered

Terraform Cloud Agents

- Configured as an agent pool with many agents
- A token is generated and applied using a command line or ENV VAR and connects back to TFE
- Once an agent is in a pool, the pool can be assigned to a Workspace





03

Sentinel

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

Sentinel Benefits

- Enforcement
- Speed
- Reproducibility
- Reliability
- Automation
- Version Control
- Auditability

Sentinel

- Has its own language that includes variables, loops, imports, conditionals, and functions
- Modules are useful for creating reusable code and libraries
- Ensures governance is applied automatically rather than relying on manual auditing
- Supports fine-grained policies using conditional logic
- Allows you to write complex logic and even call cost estimation

Sentinel

- Runs **after** a terraform plan and **before** a terraform apply

  terraform plan --> sentinel check --> terraform apply

- Enforcement levels:
  - **Advisory**: 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
  - **Hard mandatory**: guard-rails warning, info warnings in the TF Run

- Includes a CLI tool to allow fast policy tests and runs

- Validates Config and State (Create, Edit, Destroy) of Terraform resources

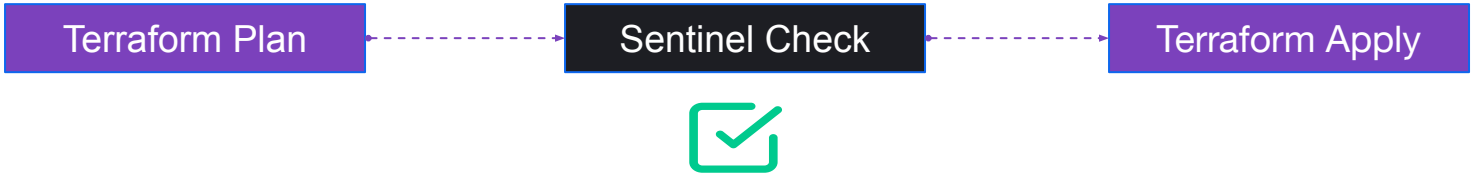
- Foundational Policies Library of premade policies is available

Common Sentinel Use Cases

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

Workflow

1. Create Terraform Workspaces
2. Create Sentinel Policies Git Repo
3. Create Policy Sets in TFC
4. Attach Policy Set to One (or more) Workspaces



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
}
```

Sentinel Rule Git Repo

hashicorp / terraform-sentinel-policies Public

Watch 58 | Fork 20 | Star 18

Code | Issues | Pull requests | Actions | Projects | Wiki | Security | Insights

main | 1 branch | 2 tags | Code

rberlind Give pshamus credit ... 442c23d on 3 Feb 13 commits

aws	add map_key filers and check-ec2-environment-tag.sentinel	last month
azure	add links to aws, azure, and registry functions docs	2 months ago
cloud-agnostic	add links to aws, azure, and registry functions docs	2 months ago
common-functions	Give pshamus credit	last month
gcp	add gcp-functions module	last month
vmware	remove raw data	2 months ago
.gitignore	remove raw data	2 months ago
LICENSE	Initial commit	2 months ago
README.md	add map_key filers and check-ec2-environment-tag.sentinel	last month

About

Example Sentinel Policies for use with Terraform Cloud and Terraform Enterprise

Readme
MPL-2.0 License
Code of conduct
18 stars
58 watching
20 forks

Releases 2

v1.0.1 Latest
on 1 Feb

+ 1 release

Policy Set File Structure

hashicorp / terraform-sentinel-policies Public

Watch 58 | Fork 20 | Star 18

Code | Issues | Pull requests | Actions | Projects | Wiki | Security | Insights

main | terraform-sentinel-policies / gcp / | Go to file | Add file | ···

rberlind add gcp-functions module — b3e3977 on 31 Jan — History

..		
gcp-functions	add gcp-functions module	last month
mocks	remove raw data	2 months ago
test	remove raw data	2 months ago
enforce-mandatory-labels.sentinel	add gcp-functions module	last month
restrict-egress-firewall-destination-ranges.sentinel	remove raw data	2 months ago
restrict-gce-machine-type.sentinel	remove raw data	2 months ago
restrict-gke-clusters.sentinel	remove raw data	2 months ago
restrict-ingress-firewall-source-ranges.sentinel	remove raw data	2 months ago
sentinel.hcl	add gcp-functions module	last month

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

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

04

Terraform & ServiceNow Integration

Integration with ServiceNow

- The Terraform ServiceNow Service Catalog integration enables end-users to provision self-serve infrastructure via ServiceNow
- Connecting ServiceNow to Terraform Enterprise lets users:
  - order Service Items
  - create workspaces
  - perform Terraform runs using prepared Terraform configurations hosted in VCS repositories
- Terraform ServiceNow Service Catalog Integration Setup Instructions
- Terraform ServiceNow Integration Administrator Guide

Integration Workflow

Terraform Admin
Prepare an organization for use with the ServiceNow Catalog
Create a team that can manage workspaces in that organization
Create a Team API so the integration can use that team's permission
Retrieve the oAuth token ID's and repository identifiers for TFC to identify your VCS

ServiceNow Admin
Install the Terraform Integration application from the ServiceNow App Store
Connect the integration application with TFE
Add the Terraform Service Catalog to ServiceNow
Configure the VCS repositories in ServiceNow
Configure the Variable Sets for use with the VCS

05

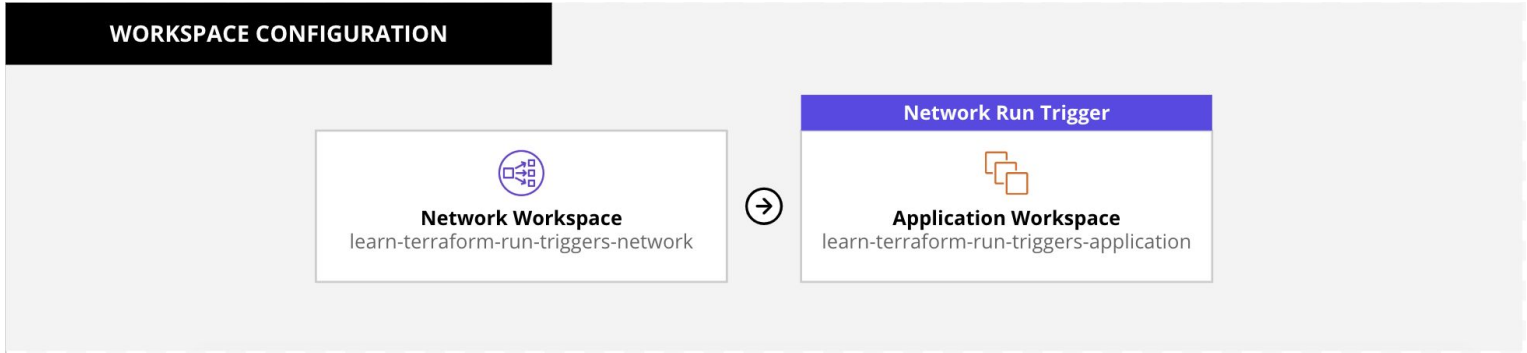
Run Triggers & Run Notifications

Run Triggers

- Create infrastructure pipelines in TFE
- Allow teams to manage complex infrastructure in TFE by creating infrastructure pipelines between multiple workspaces
- When a source workspace is selected, multiple dependent workspaces can be linked
- When a successful apply is executed in the source workspace, the dependent workspaces have runs triggered and can be configured to auto-apply their configurations

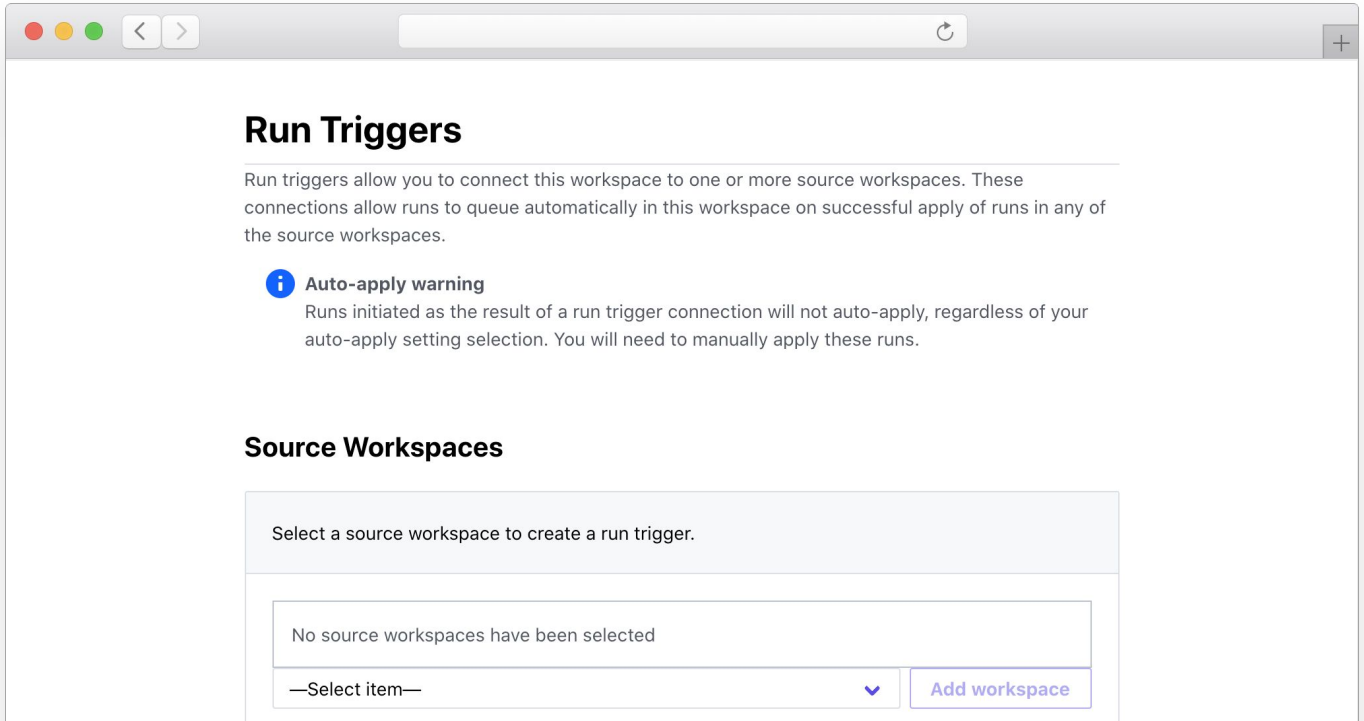
Use Case: Application Configuration Management

Run triggers automatically trigger updates to application configuration to rebalance servers across new subnets once they are successfully provisioned in the network workspace



Create Run Triggers

Workspace Settings → Run Triggers → Select Source Workspace



Run Notifications

- Run Notifications send updates/notifications to external services with details on run progress
- Notifications can be sent to up to 20 destinations
- Each workspace can be configured with it’s own notification settings
- Can send either POST message to any URL via webhook, email message, or sent to Slack & post updates in channels

Notification Triggers

	Trigger	Description
Created	“run:created”	When a run is created and enters the "Pending" state.
Planning	“run:planning”	When a run acquires the lock and starts to execute.
Needs Attention	“run:needs_attention”	Human decision required. When a plan has changes and is not auto-applied, or requires a policy override.
Applying	“run:applying”	When a run begins the apply stage, after a plan is confirmed or auto-applied.
Completed	“run:completed”	When the run has completed on a happy path and can't go any further.
Errored	“run:errored”	When the run has terminated early due to error or cancellation.

Sample Notification Payload

CODE EDITOR


```
{
  "payload_version": 1,
  "notification_configuration_id": "nc-AeUQ2zfKZzW9TiGZ",
  "run_url":
"https://app.terraform.io/app/acme-org/my-workspace/runs/run-FwnENkvDnrpyFC7M",
  "run_id": "run-FwnENkvDnrpyFC7M",
  "run_message": "Add five new queue workers",
  "run_created_at": "2019-01-25T18:34:00.000Z",
  "run_created_by": "sample-user",
  "workspace_id": "ws-XdeUVMWShTesDMME",
  "workspace_name": "my-workspace",
  "organization_name": "acme-org",
  "notifications": [
    {
      "message": "Run Canceled",
      "trigger": "run:errored",
      "run_status": "canceled",
      "run_updated_at": "2019-01-25T18:37:04.000Z",
      "run_updated_by": "sample-user"
    }
  ]
}
```

Create Notification Trigger

Workspace → Settings → Notifications

email-notifications / Workspaces / demo_workspace / Settings / Notifications / New

demo_workspace

Runs | States | Variables | Settings | Queue plan

Create a Notification

Notifications allow you to send messages to other applications based on Run events.

Destination

Webhook
POST messages to any URL

Email
Send messages to users via Email

Slack
Send messages to a Slack Channel

Name

e.g. My Notification

Webhook URL

https://example.com/...

Token

Encrypted - write only

Used to generate the HMAC on the notification request. Read more in the documentation.

Next Steps

Tutorials

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

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

Terraform

Home | Documentation | Tutorials | Install | Registry | Try Cloud

Search ⌘/ctrl K

Terraform Home

Tutorials

Overview

Get Started

AWS

Azure

Docker

GCP

OCI

Terraform Cloud

Fundamentals

CLI

Configuration Language

Modules

Developer / Terraform / Tutorials / Terraform Cloud

Get Started - Terraform Cloud

Collaborate on version-controlled configuration using Terraform Cloud. Follow this track to build, change, and destroy infrastructure using remote runs and state.

Create an account to track your progress.

Start | 10 tutorials

5min

What is Terraform Cloud - Intro and Sign Up

Sign up for Terraform Cloud, which provides free remote state storage, a stable run environment, version control system (VCS) driven plans and applies, a collaborative web GUI, and more. Create your first organization.

3min

Log in to Terraform Cloud from the CLI

Resources

- TFE Permissions
- API Tokens
- Organizing Workspaces with Projects
- Terraform Cloud Agents on TFE
- Manage Private Environments with Agents
- Cloud Agent Releases & Kubernetes Module
- Sentinel Language Reference
- Sentinel Foundational Policies Library
- Run Triggers & Registry: tfe_run_trigger
- Notifications API & Registry: tfe_notifications

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 Enterprise Operations

We take a deep dive into best practices for operating Terraform Enterprise instances including backup & restore operations, upgrade process, and monitoring

Program Closing

We conclude the webinar series with a short recorded session

The session and accompanying materials include an Operational Readiness Checklist for Terraform Enterprise and links to all of the program materials and recordings

Action Items

- Validate TFE architecture and design with appropriate stakeholders for approval (Security Team, Network Team, Developer Leads, etc)
- Start planning RBAC structure for the deployment (Orgs, Teams, Projects, Workspaces, Roles)
- Review Sentinel resources and determine which policy sets will be utilized in your environment(s)

Q & A

Thank You

customer.success@hashicorp.com
www.hashicorp.com