

# Terraform Cloud Governance

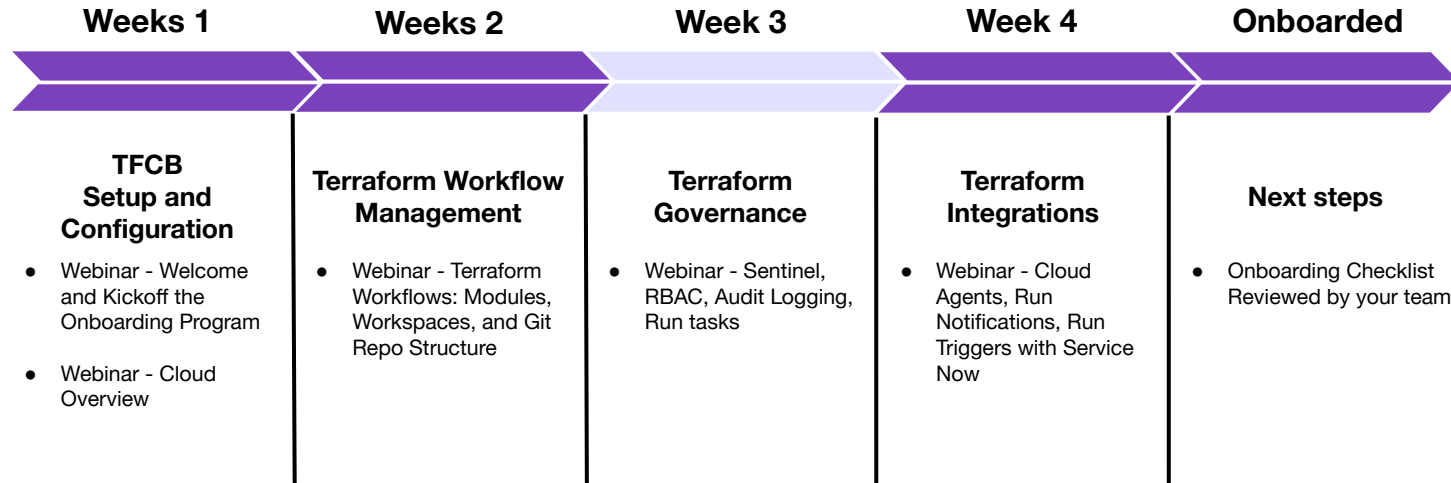


---

# Agenda

1. Role Based Access Controls
2. Sentinel
3. Run Tasks
4. Audit Logs

# TFCB Path to Production



01

# **Role Based Access Controls (RBAC)**

# Terraform Cloud RBAC Model



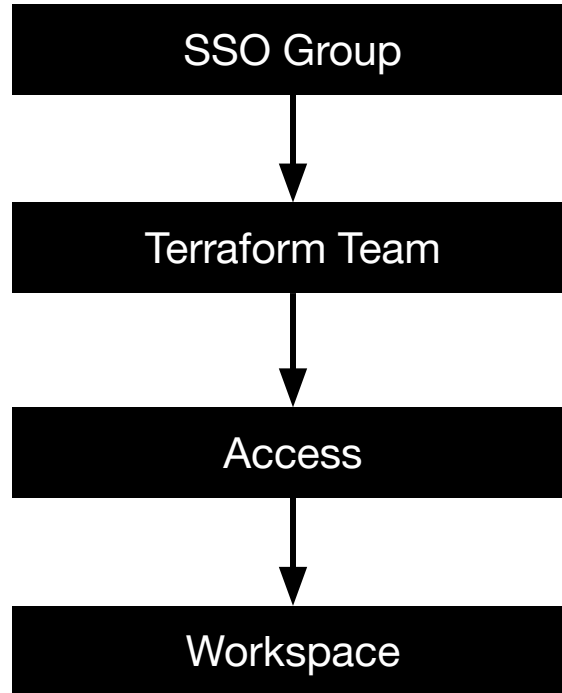
- Terraform Cloud's (TFCB) access model is team-based
  - Permissions are assigned at the team level
  - Users inherit permissions based upon team assignment
- TFCB's permission model is split into organization-level & workspace-level permissions
- Every Org has an “owners” team which have every available 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

## 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, & 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 / 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	
<a href="#">Policy Managers</a>	custom	...
<a href="#">Ops</a>	write	...

Edit permissions

Remove team





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

#### 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

## 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	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

# Benefits



 Enforcement

 Automation

 Speed

 Version Control

 Reproducibility

 Auditability

 Reliability



# 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



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

Terraform Plan

Sentinel Check

Terraform Apply



# 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

# Policy Sets



Pyrocumulus / Settings / Policy Sets

## ORGANIZATION SETTINGS

### Pyrocumulus

- General
- Teams
- VCS Providers
- API Tokens
- Authentication
- SSH Keys
- Cost Estimation
- Policies

Policy Sets

## Policy Sets

Create a new policy set

Policy sets are groups of Sentinel policies which may be enforced on workspaces. Please see the [Sentinel in Terraform Cloud documentation](#).

### pyrocumulus

1 Workspace · hashicorp/pyrocumulus · 1cd6d65

Last updated a month ago

# Create Policy Set



Pyrocmulus / Settings / Policy Sets / pyrocmulus

## ORGANIZATION SETTINGS

### Pyrocmulus

General

Teams

VCS Providers

API Tokens

Authentication

SSH Keys

Cost Estimation

Policies

**Policy Sets**

## Policy Set: pyrocmulus

Last updated September 24th 2019, 2:34:25 pm

### Name

pyrocmulus

You can use letters, numbers, dashes (-) and underscores (\_) in your policy set name.

### Description

### Policy Set Source



Upload via API



hashicorp/pyrocmulus · 1cd6d65 · Last updated 3 days ago

# Attach Policy Set



## Scope of Policies

- ☐ Policies enforced on all workspaces
- ☒ Policies enforced on selected workspaces



## Workspaces

The name of the workspace you wish to add to this policy set.

pyrocumulus



—Select item—



Add workspace

Update policy set

Delete 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)

# Resources: Sentinel Policies



- [Example Sentinel Policies Collection](#)
- [Terraform Foundational Policies Library](#)
- [Sentinel Tutorials](#)

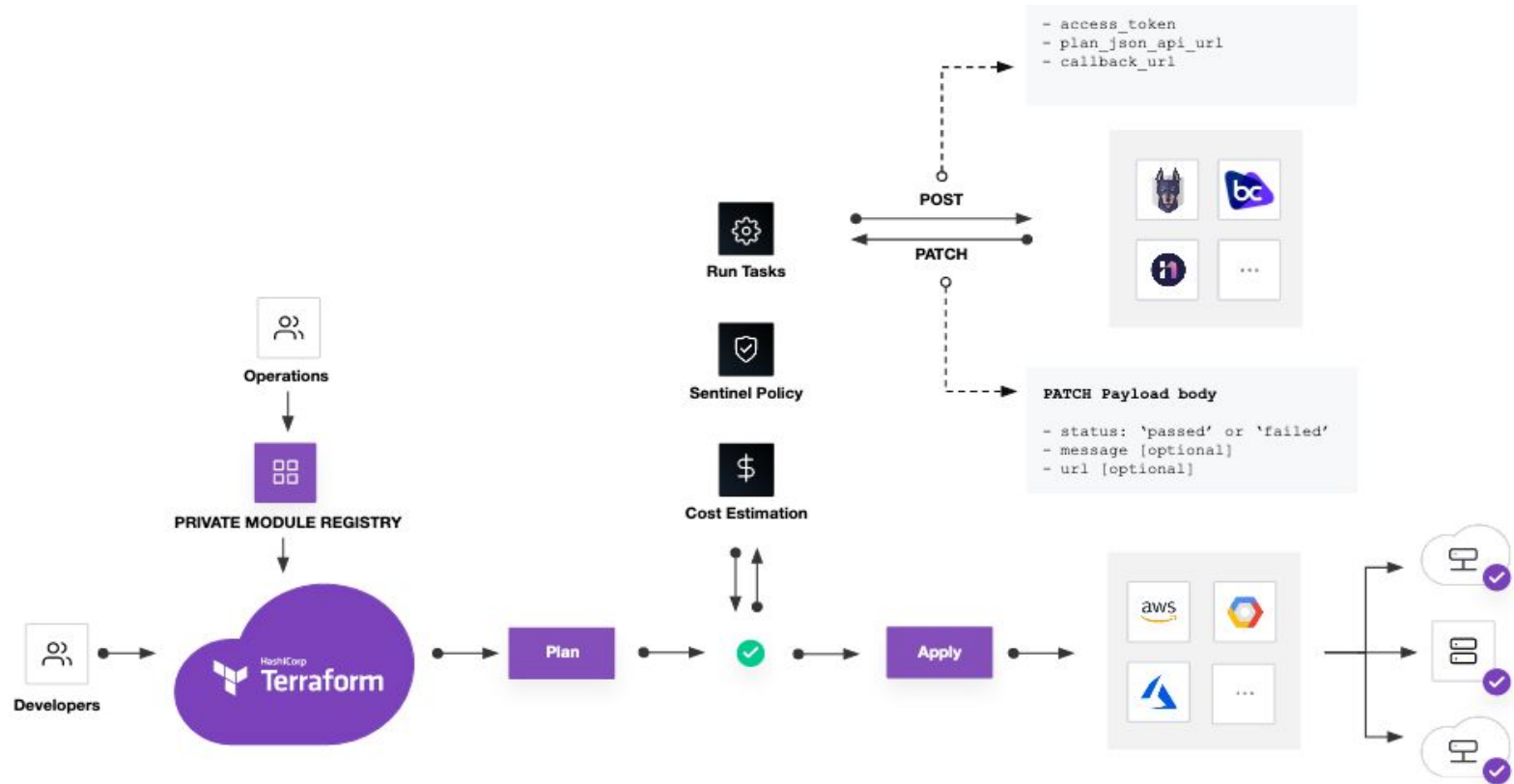
03

# 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](#)



# Payload from Terraform



```
CODE EDITOR

{
  "payload_version": 1,
  "access_token": "4QEuyyxug1f2rw.atlasv1.iDyxqhXGVZ0ykes53YdQyHyYtFOrdAWNbxVUgWvzb64NFHjccquu8gJMEdUwoSLRu4Q",
  "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,
```

# Create Run Tasks



Organization Settings → Run Tasks → Create run tasks

The screenshot shows the HashiCorp Cloud Platform interface. The top navigation bar is purple with the HashiCorp logo, a dropdown menu for 'sandraliu-tam', and links for 'Workspaces', 'Registry', 'Usage', 'Settings' (which is active), and 'HashiCorp Cloud Platform'. A search bar and user profile icon are on the right. Below the navigation bar, the breadcrumb 'sandraliu-tam / Settings / Run Tasks' is visible. The left sidebar contains a list of settings categories: 'Organization settings' (with sub-items: General, Tags, Teams, Users, Variable sets), 'Integrations' (with sub-items: Cost estimation, Policies, Policy sets, Run tasks - which is highlighted), 'Security', 'Agents', 'API tokens', 'Authentication', and 'SSH keys'. The main content area is titled 'Run Tasks' and includes a 'Create run task' button. Below the title, a message states 'No run tasks yet.' with a subtext explaining that Run Tasks allow for integrating third-party tools directly into Terraform runs. A section titled 'Partner Integration Guides' follows, featuring four partner cards: Bridgecrew (Security and compliance visibility streamlined for Terraform), Infracost (Cloud cost estimation and forecasting for Terraform), Lightlytics (Gain unmatched visibility and control across your workflow), and Snyk (Find, prioritize, & fix security vulnerabilities in Terraform). Each card includes the partner's logo, name, description, and an external link icon.

**Run Tasks** [Create run task](#)





Directly integrate third-party tools and services to manage cost, security, compliance and more. Or enhance your workflow with custom logic. [Learn more about run tasks.](#)

**No run tasks yet.**

Run Tasks allow you to integrate third-party tools and services directly in a Terraform run.

**Partner Integration Guides**

Get started with one of our partners' purpose-built run task integrations.

 <b>Bridgecrew</b> Security and compliance visibility streamlined for Terraform. <a href="#">Link</a>	 <b>Infracost</b> Cloud cost estimation and forecasting for Terraform. <a href="#">Link</a>
 <b>Lightlytics</b> Gain unmatched visibility and control across your workflow. <a href="#">Link</a>	 <b>Snyk</b> Find, prioritize, & fix security vulnerabilities in Terraform. <a href="#">Link</a>



# 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

The screenshot shows the HashiCorp Cloud Platform (HCP) interface. The top navigation bar includes 'sandrallu-tam', 'Workspaces', 'Registry', 'Usage', 'Settings', and 'HashiCorp Cloud Platform'. The left sidebar lists various settings categories, with 'Run tasks' highlighted in blue and enclosed in a red box. The main content area is titled 'Run Task: HCP\_Packer' and contains the following fields and options:

- Enabled:** A checkbox that is checked, indicating the task is enabled. Below it, a note states: 'Run task will run across all associated workspaces.'
- Name:** A text input field containing 'HCP\_Packer'. Below the field, a note states: 'Can only contain letters, numbers, dashes and underscores.'
- Endpoint URL:** A text input field containing 'https://api.cloud.hashicorp.com/packer/2021-04-30/terraform-cloud/validation/5424f747-8772-4a10-9014-3a03a4cf608e'. This field is highlighted with a red box. Below the field, a note states: 'Run Tasks will POST to this URL.'
- Description (optional):** A text input field containing 'e.g A description looks like this'.
- HMAC key (optional):** A text input field containing '89a0d40fcd416bc66ef30e983dc94f33277cdb485c34a7e4c485d44ad63ffa9'. This field is highlighted with a red box. Below the field, a note states: 'A secret key that may be required by the service to verify request authenticity.'

At the bottom of the form, there is a blue button labeled 'Save run task'.

# 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.

## **Refactor**

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](#)



# Resources: Run Tasks

- [Run Tasks Documentation](#)
- [Run Tasks Integration](#)
- [Tutorial: Configure Snyk Run Task in Terraform Cloud](#)

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

# Resources: 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](#)

# Next Steps

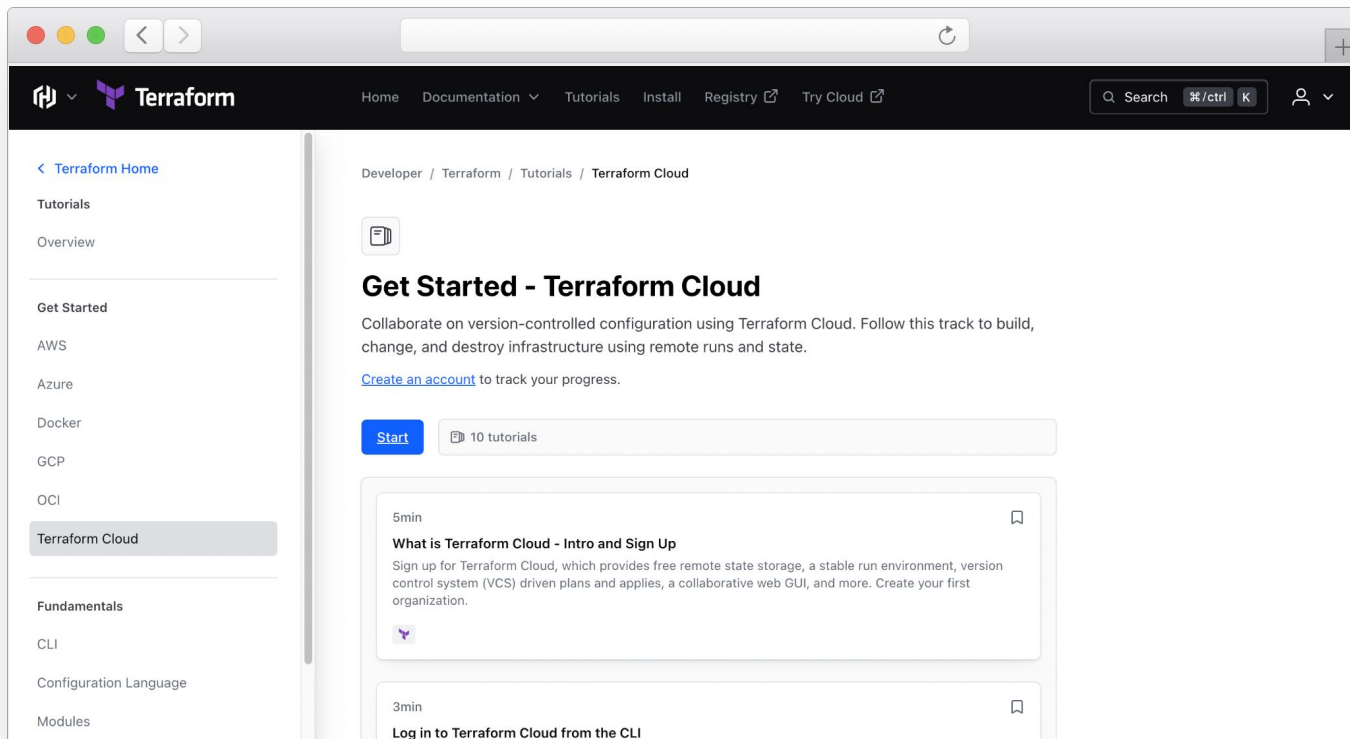


# Tutorials

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



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

A screenshot of a web browser displaying the Terraform Cloud tutorial page. The browser window has a title bar with red, yellow, and green window control buttons, and a search bar. The page header is dark with the Terraform logo and navigation links: Home, Documentation, Tutorials, Install, Registry, and Try Cloud. A search bar is on the right. The left sidebar shows a navigation menu with 'Terraform Home', 'Tutorials', 'Overview', 'Get Started', 'AWS', 'Azure', 'Docker', 'GCP', 'OCI', 'Terraform Cloud' (highlighted), 'Fundamentals', 'CLI', 'Configuration Language', and 'Modules'. The main content area shows the breadcrumb 'Developer / Terraform / Tutorials / Terraform Cloud', a document icon, and the title 'Get Started - Terraform Cloud'. Below the title is a paragraph about collaborating on version-controlled configuration using Terraform Cloud, followed by a link to 'Create an account'. A blue 'Start' button and a box indicating '10 tutorials' are present. The first tutorial card is titled 'What is Terraform Cloud - Intro and Sign Up', estimated at 5 minutes, and describes signing up for Terraform Cloud. The second tutorial card is partially visible, titled 'Log in to Terraform Cloud from the CLI', estimated at 3 minutes.

# 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](mailto: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](https://support.hashicorp.com).

## Discuss

Engage with the HashiCorp Cloud community including HashiCorp Architects and Engineers

[discuss.hashicorp.com](https://discuss.hashicorp.com)

# Up Next



HashiCorp  
Terraform

## **Webinar: Terraform Integrations & Program Closing**

Cloud Agents, Integrations, Run Triggers and Notifications, Production Readiness, and Closing Resources



## **Authorized users for Support**

Please email [customer.success@hashicorp.com](mailto:customer.success@hashicorp.com) with Authorized Support Contacts



## **Q & A**

A Q&A will be held after this session



# Thank You

[customer.success@hashicorp.com](mailto:customer.success@hashicorp.com)  
[www.hashicorp.com/customer-success](http://www.hashicorp.com/customer-success)