HashiCorp Terraform

Governance

Agenda

- Role Based Access Controls
- Sentinel
- Run Tasks
- Audit Logs
- Q & A

TFCB Path to Production

Weeks 1

TFCB Setup and Configuration

- Webinar - Welcome and Kickoff the Onboarding Program
- Webinar - Cloud Overview

Weeks 2

Terraform Workflow Management

- Webinar - Terraform Workflows: Modules, Workspaces, and Git Repo Structure

Week 3

Terraform Governance

- Webinar - Sentinel, RBAC, Audit Logging, Run tasks

Week 4

Terraform Integrations

- Webinar - Cloud Agents, Run Notifications, Run Triggers with Service Now

Onboarded

Next steps

- Exit Ramp & Operational Readiness Workshop

Role Based Access Controls (RBAC)

Common Scenarios

TFC is often used by multiple Teams, including *Developers, QA, Security, Operations, Networking, SQL Admins, Filestore Admins, and Accounting.*

Main Takeaway:
The best approach to managing this is to create Groups within your Single Sign-on (SSO) service for each of these teams, assign them as TFC Teams, decide how your Workspaces should be divided, and assign permissions accordingly.

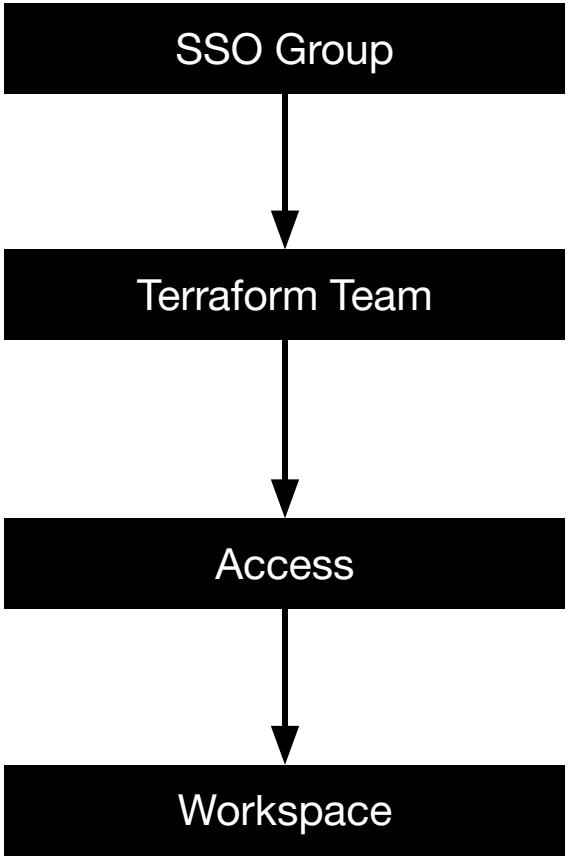
Data can also be dynamically shared between Workspaces as read-only by using the "**terraform_remote_state**" data source.

https://www.terraform.io/docs/language/state/remote-state-data.html

Important to keep in mind

Statefiles may contain secrets, passwords, and API Tokens, and should be handled as sensitive material when applying RBAC permissions.

Main takeaway:
While Statefiles 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.


SSO Group
Terraform Team
Access
Workspace

Workspace Permissions

Read

- Read Runs
- Read Variables
- Read State Versions

Plan

- Create Runs

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 and write workspace settings, general settings, notification configurations, run triggers, and more.

https://www.terraform.io/docs/cloud/workspaces/access.html

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

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.

1. 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

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.

1. 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.

Sentinel

Summary of what we'll cover

- What is Sentinel?
- Use Cases
- Benefits
- Architecture
- Syntax Example
- Workflow
- Limitations
- Questions

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.
  - https://docs.hashicorp.com/sentinel/language/
- 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, but 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 | Workspaces | Modules | Settings | Documentation | Status

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

Pyrocumulus | Workspaces | Modules | Settings | Documentation | Status

Pyrocumulus / Settings / Policy Sets / pyrocumulus

ORGANIZATION SETTINGS

Pyrocumulus

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

Policy Set: pyrocumulus

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

Name

pyrocumulus

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

Description

Policy Set Source

GitHub
HashiCorp Github

Upload via API

+

hashicorp/pyrocumulus · 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 Terraform deployed and managed resources.
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, and does not check costs for usage-based billing (ex: AWS Athena, Azure DataBricks, GCP BigQuery, GCP Pub/Sub).

Sentinel Starter Policies

https://github.com/hashicorp/terraform-sentinel-policies

https://github.com/hashicorp/terraform-foundational-policies-library

Run Tasks

Run Tasks

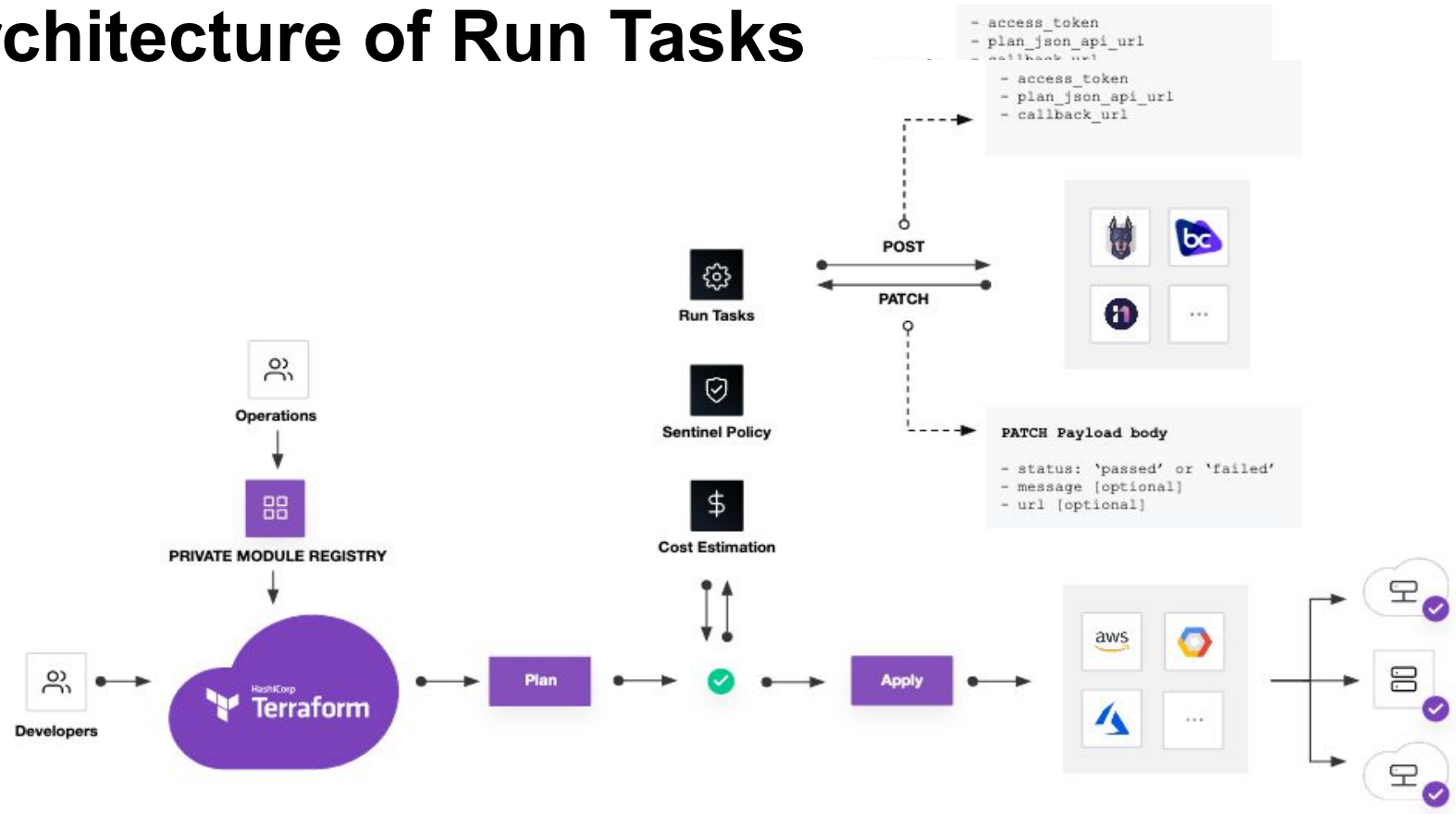
Integrate Third-Party Tools into your Terraform Cloud Workflow

Run Tasks allow you to integrate third-party tools into the pre-apply stage during a Terraform Cloud run. During the pre-apply phase an event hook is triggered and Terraform will send a payload with the details of the run. Terraform will then wait for the service to reply with either passed or failed status.

Integrations we support:

- Snyk, Bridgecrew, Infracost, Lightlytics, Vantage .. and more
- Run integrations with HCP Packer

Architecture of Run Tasks



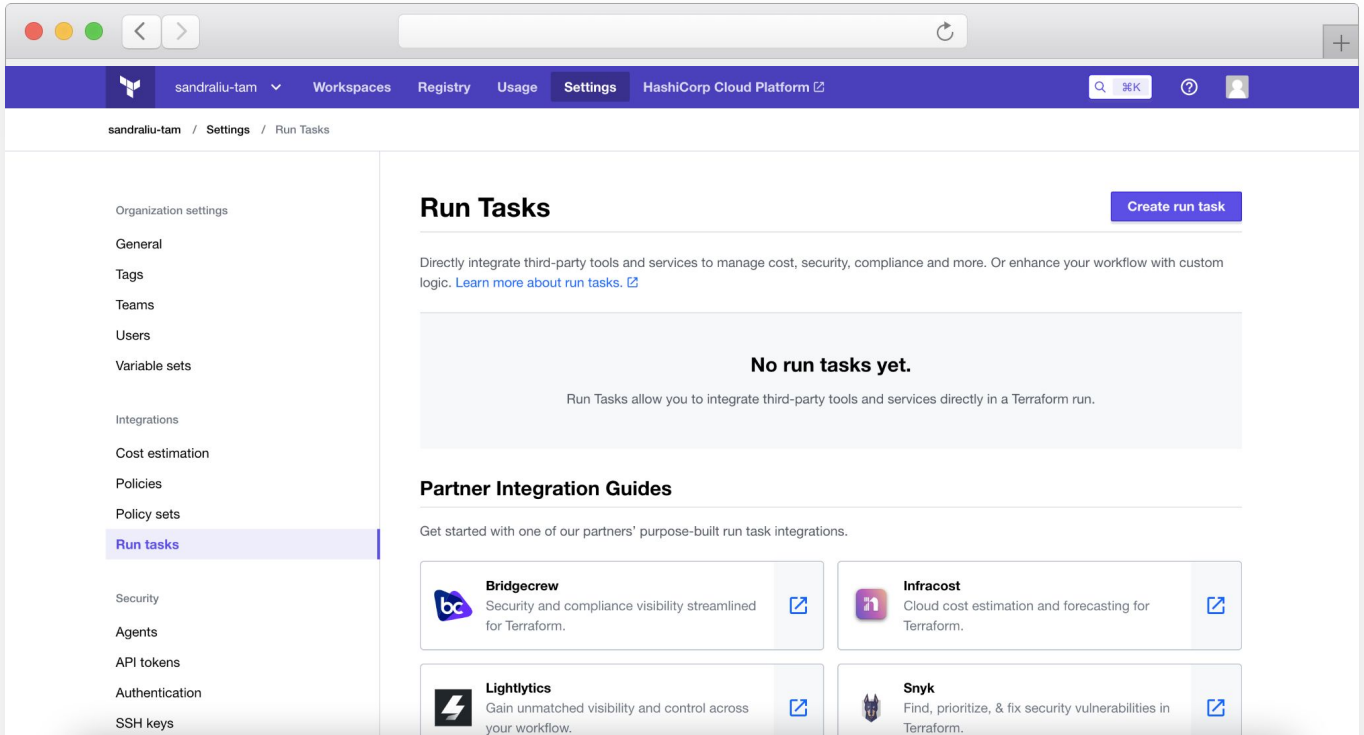
Payload from Terraform

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,
```

Create Run Tasks

Organization Settings → Run Tasks → Create run tasks



Run Task integration with HCP Packer

Run Task will validate that the machine images in your Terraform configuration are not revoked for being insecure or outdated.

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

sandraliu-tam Workspaces Registry Usage Settings HashiCorp Cloud Platform

sandraliu-tam / Settings / Run Tasks / Edit

Organization settings
- General
- Tags
- Teams
- Users
- Variable sets

Integrations
- Cost estimation
- Policies
- Policy sets
- Run tasks

Security
- Agents
- API tokens
- Authentication
- SSH keys
- SSO

Run Task: HCP_Packer

Directly integrate third-party tools and services to manage cost, security, compliance and more. Or enhance your workflow with custom logic.

task-X1zmnFYtjjE32nk2

☑ **Enabled**
Run task will run across all associated workspaces.

Name
HCP_Packer
Can only contain letters, numbers, dashes and underscores.

Endpoint URL
https://api.cloud.hashicorp.com/packer/2021-04-30/terraform-cloud/validation/5424f747-8772-4a10-9014-3a03a4cf608e
Run Tasks will POST to this URL.

Description (optional)
e.g A decription looks like this

HMAC key (optional)
89a0d40fcd416bc66fef30e983dc94f33277cdb485c34a7e4c485d44ad63ffa9
A secret key that may be required by the service to verify request authenticity.

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.

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
An up-to-date list is available **here**.

Audit Logs

Audit Logging

The audit trails API exposes a stream of audit events, which describe changes to the application entities (workspaces, runs, etc.) that belong to a Terraform Cloud organization.

Audit trails are a paid feature, available as part of the Terraform Cloud for Business upgrade package. Terraform Cloud retains 14 days of audit log information. If you need more than 14 days of audit data, it should be ingested into an external solution.

Important takeaway:
This endpoint cannot be accessed with a user token or team token. You must access it with an organization token.

Audit Logging Resources

1. Audit Logs Documentation - here
2. Blogpost on Compliance management - here
3. Log Forwarding Documentation - here
4. Splunk integration - here
5. Medium post for Splunk Integration - here

Need additional help?

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

Discuss

Engage with the HashiCorp Cloud community including HashiCorp Architects and Engineers

discuss.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.

HashiCorp Academy

Consul Enterprise Academy classes are virtual and delivered by a live instructor with in-depth Consul knowledge and implementation expertise.

Academy courses include a sandbox environment for hand-on experience in the 10 labs throughout the 3-day course.

Thank You

customer.success@hashicorp.com
www.hashicorp.com/customer-success