HashiCorp Terraform

# Governance

# Agenda

- Cloud Agents
- Role Based Access Controls
- Sentinel
- Audit Logs
- Splunk
- Q & A

# Cloud Agents

# Terraform Cloud Agents

Terraform Cloud Agents allow TFC to communicate with isolated, private, on-premises infrastructure, such as vSphere, Nutanix, and OpenStack, or across multiple cloud accounts like AWS, Azure, and GCP. The Cloud Agent is an x86-based Golang binary, which can be easily deployed on baremetal, in a VM, as a Docker container, or in a Kubernetes cluster.

The agent architecture is pull-based, so no inbound public internet connectivity is required. The agent will poll Terraform Cloud for work and execute locally. You can optionally include Cloud API Credentials in the run environment for the Cloud Agent to use, allowing for “Terraform Workspaces with Credential Free Provisioning”, allowing you to leverage the cloud-native Identity Services, such as AWS IAM Instance Profiles, Azure VM Managed Identity, or GCP Compute VM Service Account.

https://www.terraform.io/docs/cloud/agents/index.html

# Terraform Cloud Agents

**Supported Platforms**

- Baremetal
- Docker
- Kubernetes (K8S)
- VMware VM
- AWS EC2 VM, EKS, ECS, Fargate EKS, Fargate ECS
- Azure VM, Container Service, AKS
- GCP Compute Engine VM, GKE

**Hardware Requirements**

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

**Networking Requirements**

- Public Egress, outbound network connections to app.terraform.io over HTTPS (443)
- See the "TFC IP Ranges"

- https://releases.hashicorp.com/tfc-agent/
- https://hub.docker.com/r/hashicorp/tfc-agent
- https://registry.terraform.io/modules/redeux/terraform-cloud-agent/kubernetes/latest
- https://www.hashicorp.com/blog/an-introduction-to-terraform-cloud-agents
- https://learn.hashicorp.com/tutorials/terraform/cloud-agents

# Agents

An agent pool represents a group of agents that can be used to allow Terraform Cloud to communicate with isolated, private, or on-premises infrastructure. Each agent pool has its own set of tokens which are not shared across pools. When a workspace is configured to execute runs using agents, any available agent in that workspace's associated agent pool is eligible to complete the run.
Read more in our documentation.

## Create your first agent pool

Agents and agent tokens are organized into agent pools, and cannot be shared among multiple agent pools. Once an agent pool is created, you can generate an agent token to allow your agents to securely communicate with Terraform Cloud.

Create agent pool

Learn more about Terraform Agents

# Create an agent pool

1 Name agent pool

2 Token management

An agent pool represents a group of agents that can be used to allow Terraform Cloud to communicate with isolated, private, or on-premises infrastructure. When a workspace is configured to execute runs using agents, any available agent in that workspace's associated agent pool is eligible to complete the run. Learn more about agents and agent pools

Agent pool names must be unique, and will be used by workspace administrators when linking workspaces to a specific agent pool.

**Agent Pool Name**

Dashes, underscores, and alphanumeric characters are permitted.

Cancel

Continue

# Create an agent pool

Name agent pool

2 Token management

## Token management

Each agent pool has its own set of tokens which are not shared across pools. These tokens allow agents to communicate securely with Terraform Cloud.

Configure your initial tokens for **test** below. Tokens can be created and revoked tokens later, as well.

### Tokens

| Token description | Created | Last used |
|---|---|---|
| No tokens to display | | |

### Add a new token

Choose a description to help you identify this token later.

**Description**

e.g. us-west-01-token

Create token

Cancel

Finish

## Token created

Your new agent token, **test**, is displayed below.

U2VABqmFKk7UOw.atlasv1.4KqCoYqe5AqpDvFOTsDVPfwaOWS3x4ECsvUCkB6oyFy6KgZLW4ZD5txSae3E0mk1S3o

**Warning**
This token **will not be displayed again**, so make sure to save it to a safe place.

### Set up your agents

Connect to your Docker host and set the following environment variables. `TFC_AGENT_NAME` is optional.

```
$ export TFC_AGENT_TOKEN=U2VABqmFKk7UOw.atlasv1.4KqCoYqe5AqpDvFOTsDVPfwaOWS3x4ECsvUCkB6oyF
y6KgZLW4ZD5txSae3E0mk1S3o
$ export TFC_AGENT_NAME=<my_agent_name>
```

Once the environment is configured, run the Docker container with the following command **or** download the agent file.

```
$ docker run -e TFC_AGENT_TOKEN -e TFC_AGENT_NAME hashicorp/tfc-agent:latest
```

Read more in our documentation.

Cancel | Finish

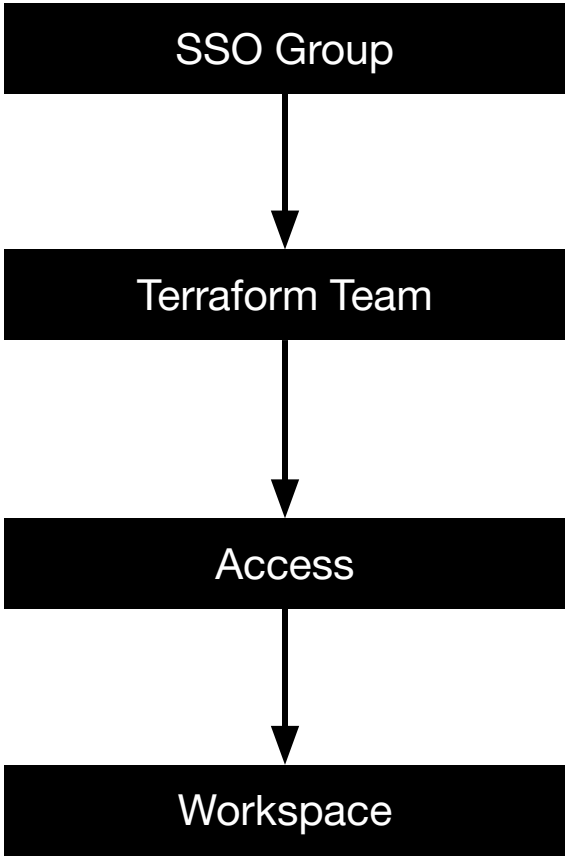
# Role Based Access Controls (RBAC)

# Common Scenarios

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

Statefiles may contain secrets, passwords, and API Tokens, and should be handled as sensitive material. The Statefiles are encrypted at rest using HashiCorp Vault, but 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 workspace information
- ✓ Read variables
- ✓ Read state
- ✓ Read TF config versions

### 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.

# Sentinel

# Summary

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

# Sentinel is “Policy / Governance / Security as Code”

# Use Cases

1. cloud provider
2. cloud account id
3. regions and availability zones
4. cost estimates and limiting
5. resource tagging
6. resource types
7. resource sizes
8. resource configuration
9. resource destruction

# Benefits

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

# 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

- Create Terraform Workspaces
- Create a Sentinel Policies Git Repo
- Create Policy Set in TFC
- Attach Policy Set to one or many 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

- 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).

# Starter Policies

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

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

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

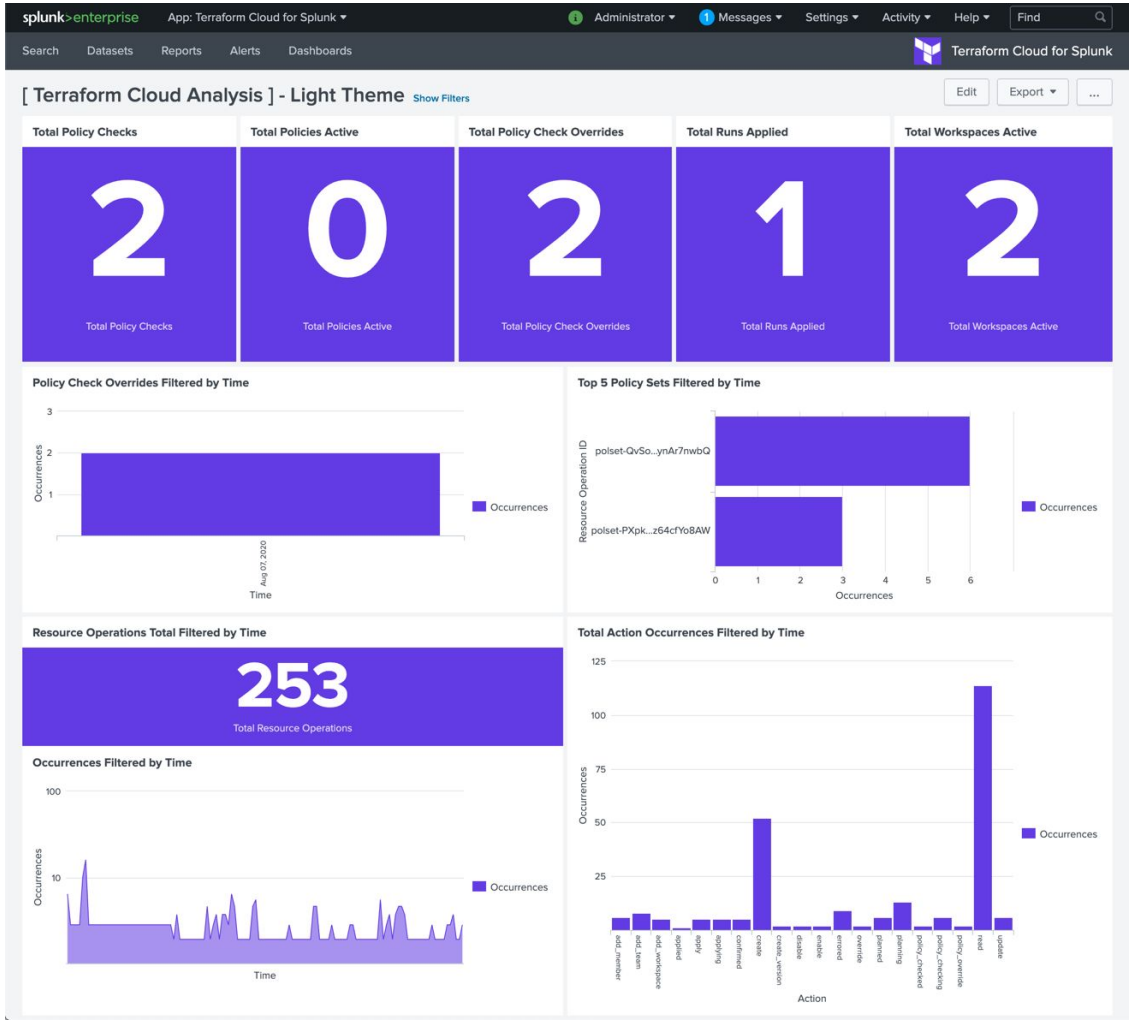
- https://www.terraform.io/docs/cloud/api/audit-trails.html
- https://www.hashicorp.com/resources/cloud-compliance-management-terraform-tracking-infrastructure-audit-logging
- https://www.terraform.io/docs/enterprise/admin/logging.html
- https://www.hashicorp.com/blog/hashicorp-terraform-cloud-audit-logging-with-splunk
- https://medium.com/hashicorp-engineering/audit-logs-for-security-and-compliance-or-how-to-set-up-terraform-cloud-and-splunk-integration-98e4fdd8fda0

# Splunk

# Splunk for Terraform

Announced on 2020-09-10, HashiCorp released a Splunk Dashboard for the TFC Audit Logs, adding that additional level of visibility, as well as accountability for Security Auditing.

- https://splunkbase.splunk.com/app/5141/
- https://www.hashicorp.com/blog/hashicorp-terraform-cloud-audit-logging-with-splunk
- https://www.terraform.io/docs/cloud/integrations/splunk/index.html
- https://www.splunk.com/en_us/blog/partners/manage-your-splunk-infrastructure-as-code-using-terraform.html


splunk>enterprise
App: Terraform Cloud for Splunk
Administrator
Messages
Settings
Activity
Help
Find
Search
Datasets
Reports
Alerts
Dashboards
Terraform Cloud for Splunk
[ Terraform Cloud Analysis ] - Light Theme
Show Filters
Edit
Export
...
Total Policy Checks
2
Total Policies Active
0
Total Policy Check Overrides
2
Total Runs Applied
1
Total Workspaces Active
2
Policy Check Overrides Filtered by Time
Occurrences
Time
Aug 07, 2020
Top 5 Policy Sets Filtered by Time
Resource Operation ID
polset-QvSo...ynAr7nwbQ
polset-PXpk...z64cfYo8AW
Occurrences
Resource Operations Total Filtered by Time
253
Total Resource Operations
Occurrences Filtered by Time
Total Action Occurrences Filtered by Time
Action

# Q & A

# Thank you.


www.hashicorp.com