HashiCorp Terraform

Terraform Cloud Agents, RBAC and Sentinel

Agenda

- Cloud Agents
- Role Based Access Controls
- Sentinel
- Q & A

Terraform Cloud Agents

Terraform Cloud Agents

- Called ‘Cloud Agents’, but run anywhere!
- Enable scaling of TFE
- A small binary the runs on Linux in full OS or container.
- Can be hosted close to target infrastructure.
- Only Outbound connectivity required.
- Can use Cloud identities.

https://www.terraform.io/enterprise/admin/agents-on-tfe

Terraform Cloud Agents

Supported Platforms

- Physical Server
- Virtual Machine
- Container
- Linux only

Minimum Hardware Requirements

- 1 Core
- 2 GB of RAM
- 4 GB of disk space

Networking Requirements

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

- 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

Terraform Cloud Agents

- **No restriction on Agent or Agent Pool Count :**
  TFE does not place a limitation on the number of Agent Pools that can be created per organization, or the number of Agents that may register themselves with a given pool.

- **Hostname Registration:**
  Agents registering with a TFE instance must define the TFE hostname via the -address CLI flag or TFC_ADDRESS environment variable when running tfc-agent.

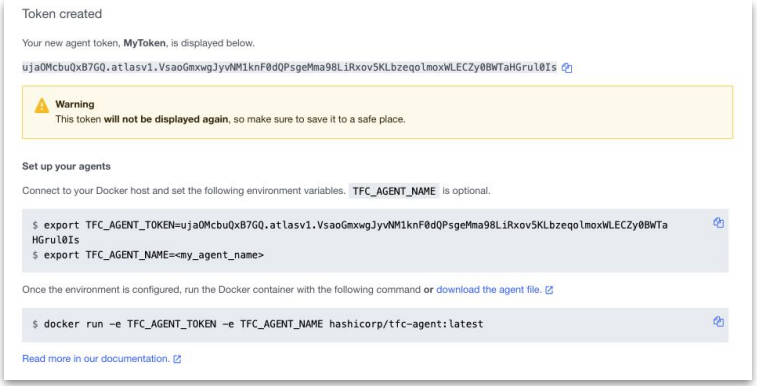
- **Custom Bundle Support:**
  Agents support custom Terraform bundles.

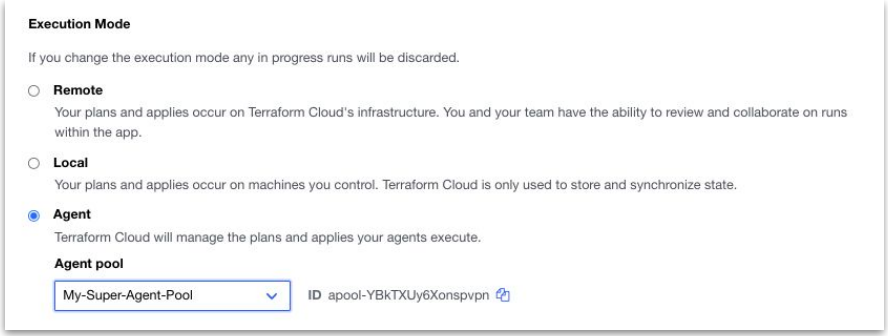
- **Network Access Requirements:**
  Agents must be able to communicate with the TFE instance via HTTPS.

- **Agent Version Compatibility:**
  TFE places restrictions on what versions of Terraform Cloud 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.





Role Based Access Controls

Organizations and Teams

Single Sign On

Standards based Identity Federation

- SAML (supported by all major identity providers)
- A user must be created in Terraform Enterprise (no SCIM provisioning)
- SAML integration allows customization of the Username attribute.
- A custom Team attribute can be specified to map group membership to Team membership. Case sensitive, exact match. Ignores non-matches.
- More details: https://www.terraform.io/enterprise/user-management/saml

Organization

The security boundary for Terraform Enterprise

- An organization is a container for Workspaces, Teams, Module Registry, Policy Sets, etc
- The organization forms part of the url: https://mt_tfe/app/[organization]/*
- An organization can be renamed, but must be unique in the TFE instance
- A user can be granted access to one or more organizations

Teams

Apply roles and permissions via Teams.

- A Team is the equivalent of a group in other identity platforms
- Roles can be applied to a Team
- Workspace permissions can be applied to a Team
- Users and API tokens can be granted roles and permissions via a Team
- A team can have one API token
- A team can be visible or secret
- There is a built in ‘owner’ team.

Teams Use Cases

Three use cases for Teams

Admin Teams

Admin roles are applied to a team and then admin users are added to the team.

Members of this team are your super users, responsible for managing Terraform Enterprise features.

User Teams

Workspace permissions are applied to a team and then users are added to the team.

Members of these teams will operations, development, info sec. The access will be determined by role.

The teams would usually be mapped to SSO groups.

CI / CD Teams

Workspace permissions are applied to the team and an API token is generated and stored in the CI/CD system.

The API token is used to automate Terraform Enterprise plan and apply runs as part of a CI/CD pipeline.

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.

Team API Token

Apply roles and permissions via Teams.

- 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

Team Workspace Permissions

Built In

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

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
- ✓ Lock/unlock workspace
- ✓ Can read and write
- ✓ Approve runs

Admin

Assign permissions

Full control of the workspace

- ✓ All permissions of write
- ✓ VCS configuration
- ✓ Manage team access
- ✓ Execution mode
- ✓ Delete workspace
- ✓ Access to state

Custom

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.

Other controls

- [ ] **Lock/unlock workspace**
  Can manually lock and unlock the workspace. This permission is required when the workspace execution mode is set to "Local".

Sentinel policies

- [ ] **Download Sentinel mocks**
  Can download Sentinel mock data for any of the workspace's runs, generated by Terraform Cloud for convenient testing of policies.

Variables

- (●) **No access**
  No access to the workspace's variables.
- ( ) **Read**
  Can view the workspace's variables.
- ( ) **Read and write**
  Can view and edit the workspace's variables.

State versions

- (●) **No access**
  No access to state versions associated with this workspace.
- ( ) **Read outputs only**
  Can read output values from the workspace's state versions.
- ( ) **Read**
  Can read the workspace's state versions.
- ( ) **Read and write**
  Can view and manually create new state versions. This permission is only required when the workspace execution mode is set to "Loc

Sentinel

Sentinel

- Policy-as-code framework
- Has its own language
- Embedded in all HashiCorp enterprise products
- Extensible using modules
- Runs after a `terraform plan` and before a `terraform apply`
- Enforcement levels: advisory, soft mandatory, hard mandatory
- Ensures governance is applied automatically rather than relying on manual auditing
- Supports fine-grained policies using conditional logic
- Includes a CLI tool to allow fast policy tests and runs
- Foundational Policies Library of premade policies is available
- Use with cost estimation

Example Use Cases

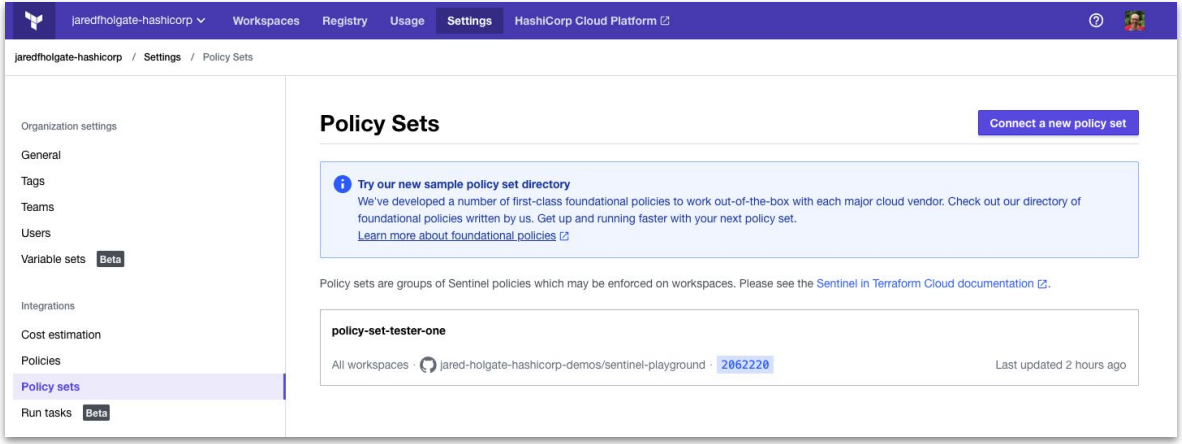
- Cloud providers
- Cloud account id
- Regions and availability zones
- Cost estimates and limiting
- Resource tagging
- Resource types
- Resource sizes
- Resource configuration
- Resource destruction
- Access policy
- Architecture

Sentinel Benefits

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

Sentinel - Policy Sets

- Policies are managed as Policy Sets
- Each set can have one or more policies and sets can share policies
- All sourced from VCS



Sentinel Capabilities

- Variables, conditionals, loops, functions.
  - https://docs.hashicorp.com/sentinel/language/
- Validates Config and State (Create, Edit, Destroy) of Terraform resources.
- Where does it run: 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

Sentinel Setup Steps

- Create a Sentinel Policies Repository in VCS
- Link VCS repository to a Policy Set in TFE
- Attach a Policy Set to one or many 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
}
```

Syntax Example - AWS Tags

CODE EDITOR

```
import "tfplan-functions" as plan
import "aws-functions" as aws

param resource_types default [
 "aws_s3_bucket",
 "aws_instance",
]

param mandatory_tags default ["Name", "ttl", "owner", "se-region", "purpose", "terraform"]

allAWSResourcesWithStandardTags = aws.find_resources_with_standard_tags(resource_types)

violatingAWSResources = plan.filter_attribute_not_contains_list(allAWSResourcesWithStandardTags,
                       "tags", mandatory_tags, true)

main = rule {
 length(violatingAWSResources["messages"]) is 0
}
```

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

Sentinel Starter and Sample Repositories

- https://github.com/hashicorp/terraform-guides/tree/master/governance
- https://github.com/hashicorp/terraform-foundational-policies-library

hashicorp / terraform-foundational-policies-library Public

Watch 23 | Fork 118 | Star 190

Code | Issues 2 | Pull requests 2 | Actions | Security | Insights

master | terraform-foundational-policies-library / cis / azure / compute / | Go to file | Add file

sheeeng feature: hcl configuration ... b41d7c8 on 30 Oct 2020 History

..

azure-cis-7.1-compute-managed-disk-encrypti...	feature: hcl configuration	15 months ago
azure-cis-7.4-compute-only-approved-extensi...	feature: hcl configuration	15 months ago
README.md	Updated source path to incl. root and branch	2 years ago

README.md

CIS Microsoft Azure Foundational Sentinel policies

The following code snippets show the configuration settings that are required to successfully deploy Sentinel policies that follow the security recommendations that are provided in the CIS Microsoft Azure Foundations Benchmark version 1.1.0. We cover policy configuration in more details in the Managing Sentinel Policies section in the Terraform Cloud documentation.

-guides / governance / third-generation / | Go to file | Add file

unctions module to main README.md ... 13 days ago History

	update find_by_provider functions	5 months ago
	add require-free-sec-center-subscription-pricing-for-vms.sentinel	last month
	add use-recent-versions-from-pmr.sentinel	13 days ago
common-functions	fix to_string for config and state	last month
gcp	update sentinel.hcl files to add policies	7 months ago
vmware	update sentinel.hcl files to add policies	7 months ago
README.md	add registry-functions module to main README.md	13 days ago

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

Configure Severity

terraform-guides / governance / second-generation / cloud-agnostic / sentinel.hcl Cancel

Edit file | Preview changes | Spaces | 4 | No wrap

```
policy "blacklist-provisioners" {
    enforcement_level = "advisory"
}

policy "blacklist-resources" {
    enforcement_level = "advisory"
}

policy "limit-cost-by-workspace-type" {
    enforcement_level = "advisory"
}

policy "limit-proposed-monthly-cost" {
    enforcement_level = "advisory"
}

policy "prevent-destruction-of-blacklisted-resources" {
```

Workflow

- Create Terraform Workspaces
- Create a Sentinel Policies Git Repo
- Create Policy Set in TFE
- Attach Policy Set to one or many Workspaces
- terraform plan -> sentinel check -> terraform apply

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

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).

Example Policies

Amazon Web Services

- Restrict owners of the aws_ami data source
- Enforce mandatory tags on taggable AWS resources
- Restrict availability zones used by EC2 instances
- Disallow 0.0.0.0/0 CIDR block in security groups
- Restrict instance types of EC2 instances
- Require S3 buckets to be private and encrypted by KMS keys
- Require VPCs to have DNS hostnames enabled

Microsoft Azure

- Enforce mandatory tags of VMs
- Restrict publishers of VMs
- Restrict VM images
- Restrict the size of Azure VMs
- Enforce limits on AKS clusters
- Restrict CIDR blocks of security groups

Google Cloud Platform

- Enforce mandatory labels on VMs
- Disallow 0.0.0.0/0 CIDR block in network firewalls
- Enforce limits on GKE clusters
- Restrict machine type of VMs

VMware

- Require Storage DRS on datastore clusters
- Restrict size and type of virtual disks
- Restrict CPU count and memory of VMs
- Restrict size of VM disks
- Require NFS 4.1 and Kerberos on NAS datastores

Cloud-Agnostic

- Allowed providers
- Prohibited providers
- Limit proposed monthly costs
- Prevent providers in non-root modules
- Require all modules have version constraints
- Require all resources be created in modules in a private module registry
- Use most recent versions of modules in a private module registry

Additional Policies can be found at https://github.com/hashicorp/terraform-foundational-policies-library

Q & A

Next Steps

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 new ticket for your issue at support.hashicorp.com.

Thank You

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