

HashiCorp Certified Terraform Associate 003

The background features abstract, glowing purple geometric shapes, including a large cube-like structure on the left and various lines and arcs extending across the frame, set against a dark, textured purple background.

9. Understand Terraform Cloud capabilities

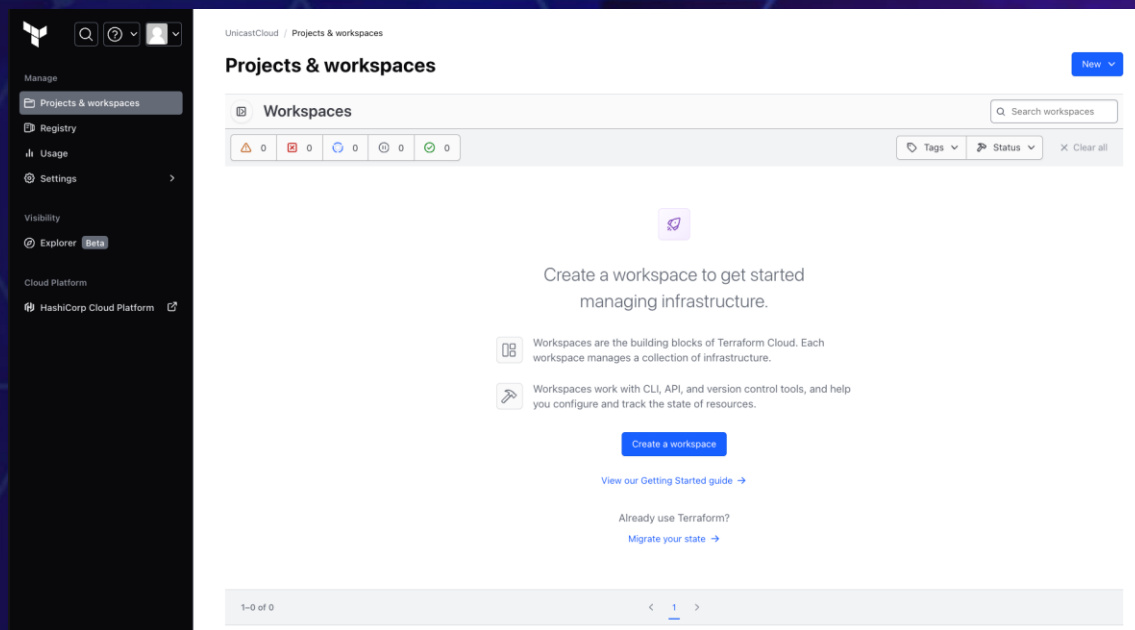
The background features several glowing purple geometric shapes, including a large cube on the left and various lines and arcs extending across the frame, creating a technical or architectural feel.

**Explain how Terraform
Cloud helps to manage
infrastructure**



Terraform Cloud

O Terraform Cloud é uma plataforma hospedada que facilita a colaboração na gestão de infraestrutura usando Terraform. Essa plataforma centraliza configurações, estados e promove a colaboração entre equipes, proporcionando um ambiente seguro e de fácil acesso para desenvolver e implementar infraestrutura como código.



TFTEC CLOUD

Terraform Cloud Terms

- **Workspaces (Espaços de Trabalho):** Ambientes isolados que permitem organizar recursos e configurações relacionadas de forma separada, facilitando a gestão.
- **States (Estados):** Representação atual da infraestrutura gerenciada pelo Terraform, essencial para entender e controlar o estado dos recursos.
- **Runs (Execuções):** Engloba planos de Terraform, como apply, plan e destroy, permitindo o gerenciamento e monitoramento das mudanças na infraestrutura.
- **Variables (Variáveis):** Parâmetros configuráveis que permitem ajustar e personalizar os planos de infraestrutura.
- **Sentinel Policies (Políticas do Sentinel):** Definição de regras e restrições para garantir a conformidade e segurança na configuração da infraestrutura.
- **Cost Estimation (Estimativa de Custos):** Capacidade de calcular estimativas de custos para recursos a serem provisionados, possibilitando a previsão financeira antes da implementação.

Run Workflows

"Run Workflows" dentro do Terraform Cloud envolve a execução, gerenciamento e controle das operações realizadas nos fluxos de trabalho do Terraform.

Version Control Workflow:

Este fluxo de trabalho integra o Terraform Cloud com sistemas de controle de versão (VCS), como Git, SVN, etc. Ele permite que equipes colaborem e controlem as mudanças na infraestrutura por meio de branches, commits e merges. Isso facilita o rastreamento de alterações, o histórico de versões e oferece um ambiente colaborativo para desenvolvimento de infraestrutura.

CLI-Driven Workflow:

Neste workflow, os desenvolvedores gerenciam a infraestrutura usando a linha de comando do Terraform localmente. Eles podem aplicar alterações na infraestrutura usando comandos específicos, como terraform apply, terraform plan, e terraform destroy. Isso oferece controle manual sobre as operações de infraestrutura e é útil para cenários onde a interação direta com a CLI é preferida.

API-Driven Workflow:

Este workflow envolve a interação direta com a API do Terraform Cloud. Ele permite a automação de tarefas e operações de infraestrutura por meio de scripts ou aplicativos que fazem chamadas à API. Isso possibilita a execução automatizada de ações, como a criação de workspaces, aplicação de mudanças na infraestrutura e monitoramento de estados, oferecendo uma abordagem programática para gerenciar a infraestrutura.

Organization Level Permissions

Administração da Organização:

Owner/Administrador: Possui controle total sobre a organização, incluindo a capacidade de gerenciar membros, recursos e permissões. Este papel pode atribuir e alterar funções para outros usuários na organização.

Gerenciamento de Membros:

Member/Membro: Tem permissões para criar e gerenciar workspaces dentro da organização. Pode ser restrito em relação à criação de equipes, convites de membros e outras ações de gerenciamento.

Definição de Papéis e Permissões:

Atribuição de Funções: Os administradores da organização podem atribuir funções específicas a membros ou equipes para definir suas permissões.

Personalização de Permissões: Permite definir permissões personalizadas com base nas necessidades da organização, garantindo um controle granular sobre quem pode acessar e modificar recursos.

Segurança e Controle de Acesso:

Controle de Acesso: Permite restringir o acesso a determinados recursos ou funcionalidades dentro da organização, garantindo a segurança e conformidade com políticas internas.

Integração com Sistemas de Identidade: Permite integrar a autenticação e autorização da organização com sistemas de identidade existentes, como SSO (Single Sign-On), LDAP ou SAML.

Auditoria e Registro de Atividades:

Registro de Atividades: Fornece um registro detalhado das ações realizadas por membros da organização, permitindo auditorias e rastreamento de atividades para garantir a conformidade e segurança.

Private Registry

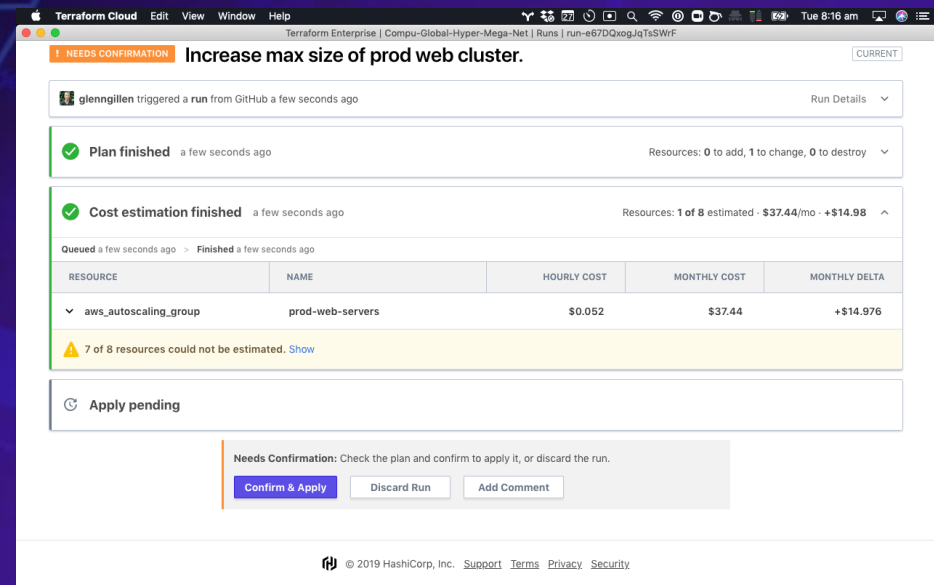
É um recurso seguro que permite armazenar e compartilhar módulos Terraform de forma privada. Oferece controle de acesso, versionamento, e integração com o Terraform Cloud. É útil para organizações que desejam armazenar módulos sensíveis ou específicos internamente, garantindo segurança e reutilização controlada de recursos.

- Armazena módulos Terraform de forma segura e privada.
- Controla quem pode acessar e usar esses módulos.
- Integra-se facilmente com o Terraform Cloud.
- Oferece registro de ações e versionamento de módulos.

Cost Estimation

É uma funcionalidade que permite calcular estimativas dos custos associados à implantação de recursos de infraestrutura. Ajuda na previsão financeira antes da implementação, fornecendo insights sobre os custos que podem ser incorridos com base nas configurações planejadas.

- **Previsão Financeira:** Calcula estimativas de custos para recursos a serem provisionados.
- **Planejamento Orçamentário:** Ajuda na previsão de gastos antes da implementação.
- **Análise de Impacto Financeiro:** Oferece uma visão dos custos potenciais das mudanças na infraestrutura.
- **Suporte à Tomada de Decisão:** Auxilia na escolha de opções de configuração com base em considerações financeiras.



The screenshot displays the Terraform Cloud web interface. At the top, a red banner indicates a 'NEEDS CONFIRMATION' for the plan 'Increase max size of prod web cluster.' Below this, a log entry shows 'glennigillen triggered a run from GitHub a few seconds ago'. The status 'Plan finished' is shown with a green checkmark. The 'Cost estimation finished' section shows a green checkmark and a summary: 'Resources: 1 of 8 estimated - \$37.44/mo - +\$14.98'. A table follows, showing the cost breakdown for the 'aws_autoscaling_group' resource named 'prod-web-servers'. A yellow warning banner states '7 of 8 resources could not be estimated. Show'. At the bottom, there is an 'Apply pending' button and a 'Needs Confirmation' section with 'Confirm & Apply', 'Discard Run', and 'Add Comment' buttons.

RESOURCE	NAME	HOURLY COST	MONTHLY COST	MONTHLY DELTA
aws_autoscaling_group	prod-web-servers	\$0.052	\$37.44	+\$14.976

VCS Integration

Permite configurar ambientes de execução específicos para realizar tarefas ou operações especializadas. O uso de cloud agents facilita a automação e gerenciamento de operações na nuvem de maneira controlada e escalável, adaptando-se às necessidades do projeto.

Create a new Workspace

Terraform Cloud organizes your infrastructure resources by workspaces. A workspace contains infrastructure resources, variables, state data, and run history. [Learn more](#) about workspaces in Terraform Cloud.

1 **Connect to VCS** 2 Choose a repository 3 Configure settings

Connect to a version control provider

Choose the version control provider that hosts the Terraform configuration for this workspace.

 GitHub ▾

 GitLab ▾

 Bitbucket ▾

 Azure DevOps ▾

Terraform Cloud Agents


Os Cloud Agents no Terraform Cloud permitem a comunicação entre o Terraform Cloud e a infraestrutura isolada, privada ou local. Eles são agentes leves implantados em um segmento de rede específico, estabelecendo uma conexão entre o ambiente local e o Terraform Cloud, possibilitando operações de provisionamento e gerenciamento.

- **Conexão com Infraestrutura Isolada:** Os Cloud Agents viabilizam a conexão entre o Terraform Cloud e infraestruturas localizadas em ambientes protegidos, como vSphere, Nutanix, OpenStack, provedores de rede corporativa, entre outros.
- **Arquitetura Pull-Based:** Os agents operam de forma pull-based, não exigindo conectividade de entrada. Cada agent criado consulta periodicamente o Terraform Cloud para receber tarefas de trabalho, realizando a execução dessas tarefas localmente.
- **Suporte ao Terraform Enterprise:** Os Terraform Cloud Agents também são suportados pelo Terraform Enterprise, fornecendo documentação e requisitos específicos para ambientes Enterprise.

Terraform Pricing

<https://www.hashicorp.com/products/terraform/pricing>

Free	Standard	Plus	Enterprise
UP TO 500 resources per month	STARTING AT \$0.00014 per hour per resource	Custom	Custom
Cloud	Cloud	Cloud	Self-managed
Get started with all capabilities needed for infrastructure as code provisioning.	For professional individuals or teams adopting infrastructure as code provisioning.	For enterprises standardizing and managing infrastructure automation and lifecycle, with scalable runs.	For enterprises with special security, compliance, and additional operational requirements.
No credit card required	Enterprise support included	Enterprise support included	Enterprise support included
Get started	Get started	Contact sales	Contact sales
	First 500 resources per month are free Learn more		

The background features several glowing purple geometric shapes, including a large cube on the left and various intersecting lines and arcs, creating a technical or architectural feel. The text is centered in a clean, white, sans-serif font.

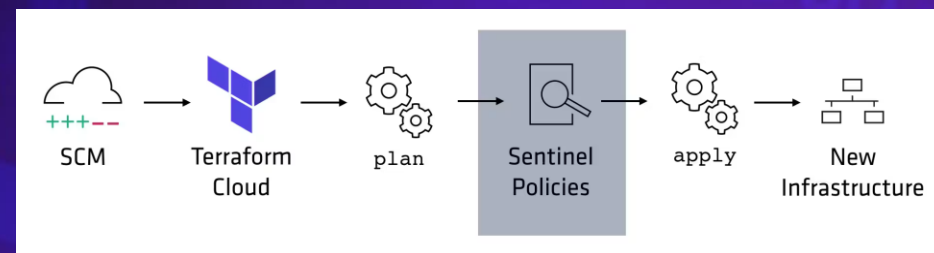
**Describe how Terraform
Cloud enables
collaboration and
governance**



Terraform Sentinel

O Sentinel é uma tecnologia integrada ao Terraform que permite a implementação de políticas de segurança, conformidade e governança em toda a infraestrutura definida por código. Ele atua como um mecanismo de execução de políticas automatizadas e é especialmente útil em ambientes onde a conformidade e a segurança são críticas.

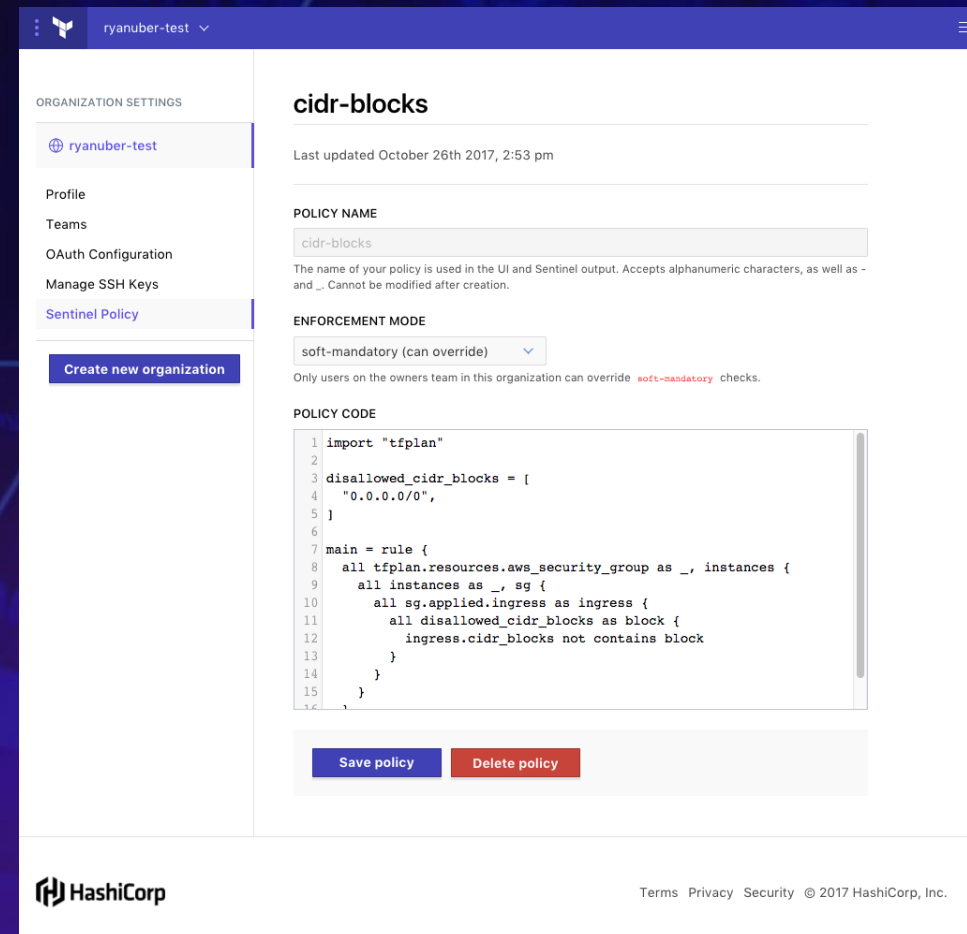
- **Política como Código:** O Sentinel permite que as políticas sejam definidas e codificadas em scripts que podem ser executados automaticamente durante o ciclo de vida do Terraform, desde o planejamento até a aplicação.
- **Integração com o Terraform:** É integrado ao Terraform, garantindo que as políticas sejam aplicadas e verificadas antes da implantação de recursos, ajudando a prevenir configurações inadequadas.
- **Personalização:** Oferece flexibilidade na criação de políticas personalizadas para atender às necessidades específicas da organização.



Policy as Code

A abordagem de "Política como Código" (Policy as Code) refere-se à prática de definir políticas de segurança, conformidade e governança usando código.

Com o Sentinel, as políticas podem ser definidas e implementadas como código, o que permite automação, versionamento e controle sobre essas políticas.



The screenshot displays the HashiCorp Sentinel web interface for an organization named 'ryanuber-test'. The left sidebar contains navigation links for 'ORGANIZATION SETTINGS', 'Profile', 'Teams', 'OAuth Configuration', 'Manage SSH Keys', and 'Sentinel Policy'. A 'Create new organization' button is also present. The main content area is titled 'cidr-blocks' and shows the policy's details. It indicates the policy was last updated on October 26th, 2017, at 2:53 pm. The 'POLICY NAME' field is set to 'cidr-blocks'. The 'ENFORCEMENT MODE' is set to 'soft-mandatory (can override)'. Below this, a note states: 'Only users on the owners team in this organization can override soft-mandatory checks.' The 'POLICY CODE' section contains a Terraform Sentinel rule for restricting AWS security group ingress to specific CIDR blocks. The code is as follows:

```
1 import "tfplan"
2
3 disallowed_cidr_blocks = [
4   "0.0.0.0/0",
5 ]
6
7 main = rule {
8   all tfplan.resources.aws_security_group as _, instances {
9     all instances as _, sg {
10      all sg.applied.ingress as ingress {
11        all disallowed_cidr_blocks as block {
12          ingress.cidr_blocks not contains block
13        }
14      }
15    }
16  }
```

At the bottom of the policy configuration area, there are two buttons: 'Save policy' and 'Delete policy'.

HashiCorp

Terms Privacy Security © 2017 HashiCorp, Inc.

Sentinel Policy Language

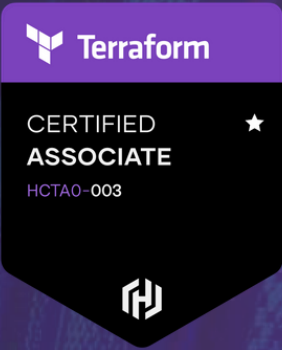
O Sentinel Policy Language é uma linguagem específica para políticas (Policy as Code) usada para definir regras, restrições e políticas de segurança em infraestrutura e código. Ele é integrado ao Terraform e outras ferramentas da HashiCorp para permitir a automação e a aplicação de políticas de segurança em toda a infraestrutura definida por código.

1.Regras (Rules): As regras são a base da linguagem de política do Sentinel. Elas definem as condições que devem ser atendidas para garantir a conformidade.

2.Funções (Functions): As funções são usadas para realizar operações e avaliar condições nas regras. O Sentinel possui funções integradas e também permite a criação de funções personalizadas.

3.Contexto (Context): O contexto fornece informações sobre o ambiente em que a política está sendo aplicada. Isso inclui dados sobre recursos, variáveis, atributos e muito mais.

```
1 # Regra para verificar a região dos recursos.
2 # Esta política garante que todos os recursos sejam
3 # criados em uma região específica.
4 main = rule {
5   all tfplan.resources as _, resources {
6     all resources as _, r {
7       r.region == "us-west-2"
8     }
9   }
10 }
11
12 # Regra para verificar as regras de segurança
13 # Esta política garante que as portas de segurança estejam
14 # restritas apenas aos endereços IP autorizados.
15 main = rule {
16   all tfplan.resources.aws_security_group_rule as _, rules {
17     all rules as _, r {
18       r.from_port < 22 or r.from_port > 22
19     }
20   }
21 }
22
```



Obrigado