Terraform Cloud Integrated GitOps Workflow - Concept

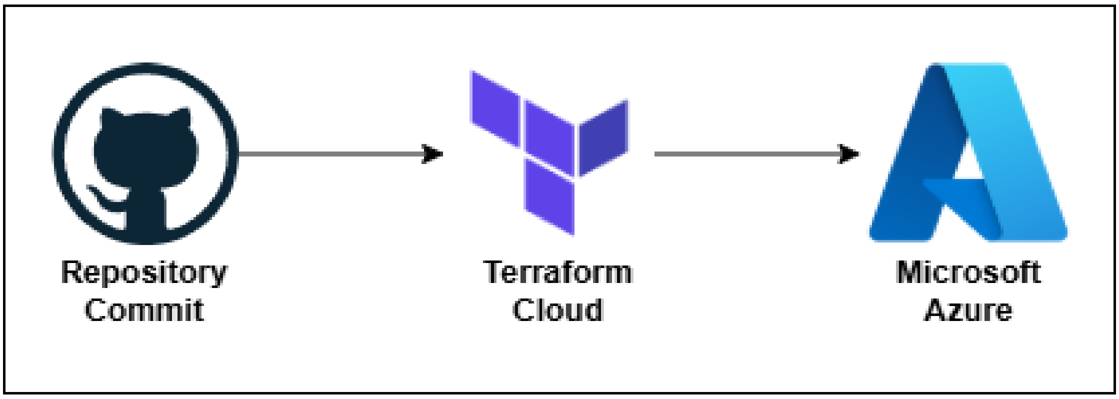
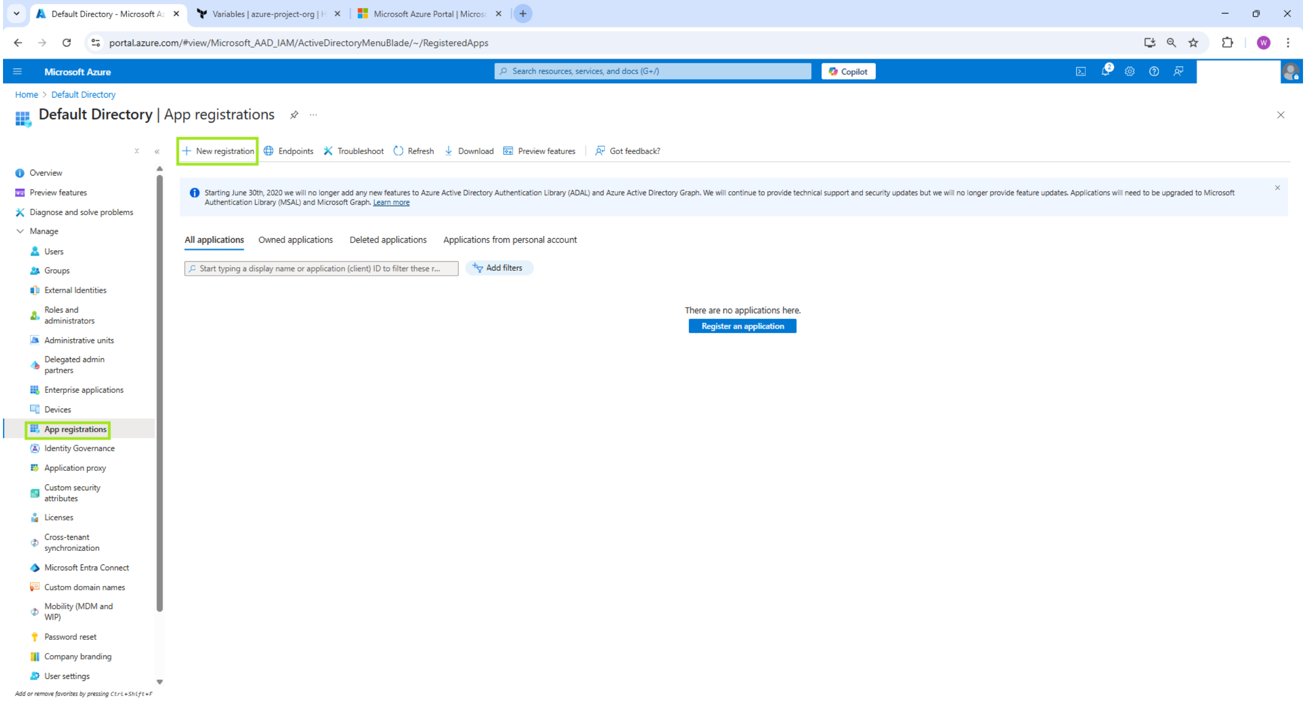


Table of Contents

1. Setting up Azure for Terraform

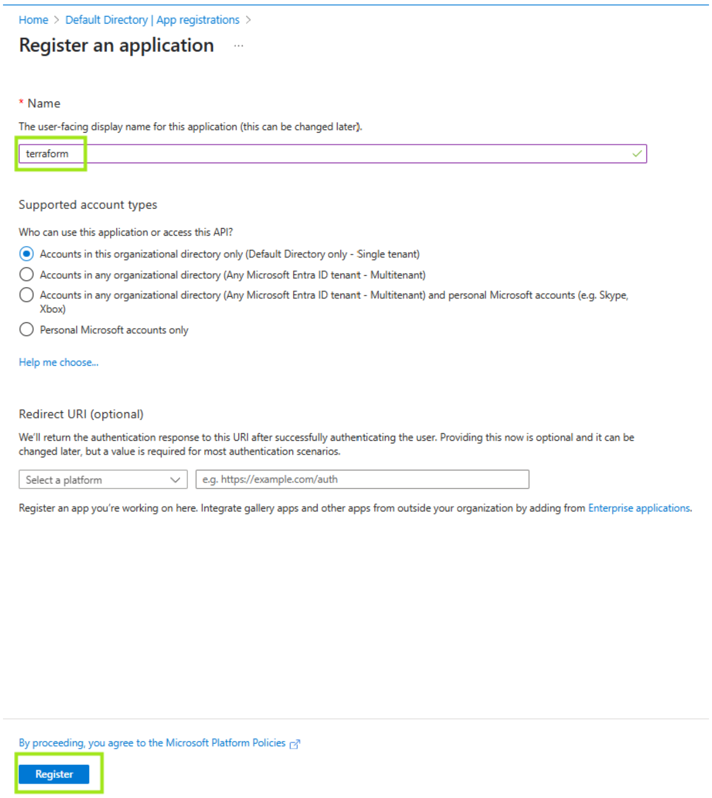
1.1 Create Application in Entra ID



Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure Active Directory Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Learn more

There are no applications here.

1.1.1 Register Application



* Name

The user-facing display name for this application (this can be changed later).

terraform

Supported account types

Who can use this application or access this API?

- ● Accounts in this organizational directory only (Default Directory only - Single tenant)
- ○ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)
- ○ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
- ○ Personal Microsoft accounts only

Help me choose...

Redirect URI (optional)

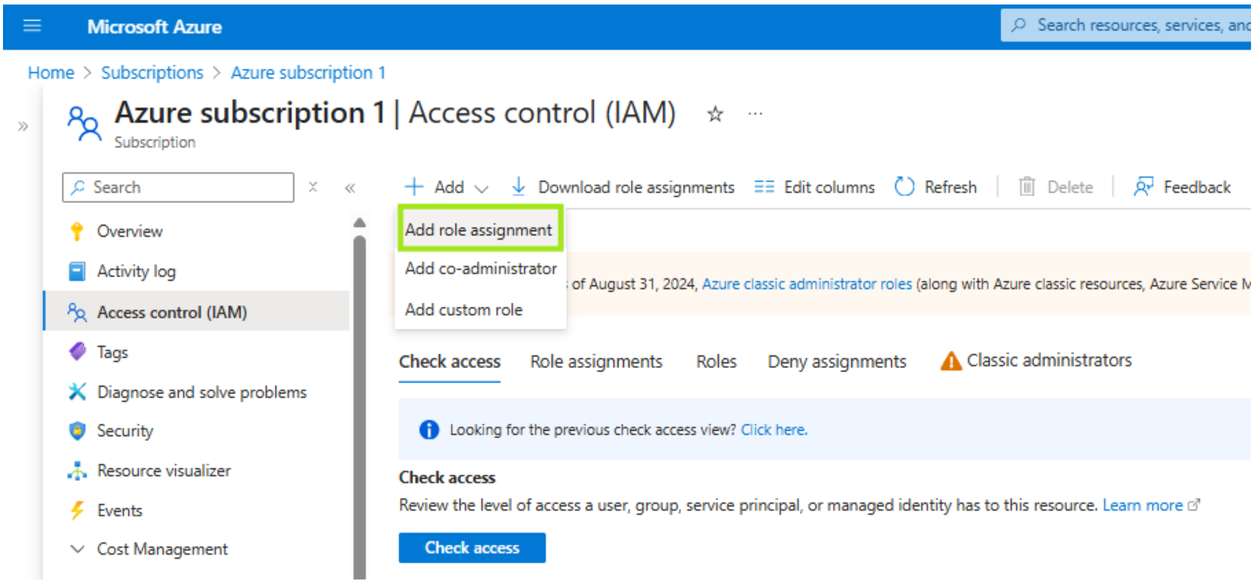
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Select a platform | e.g. https://example.com/auth

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from Enterprise applications.

By proceeding, you agree to the Microsoft Platform Policies

1.2 Allow Application to control Azure Resources through IAM



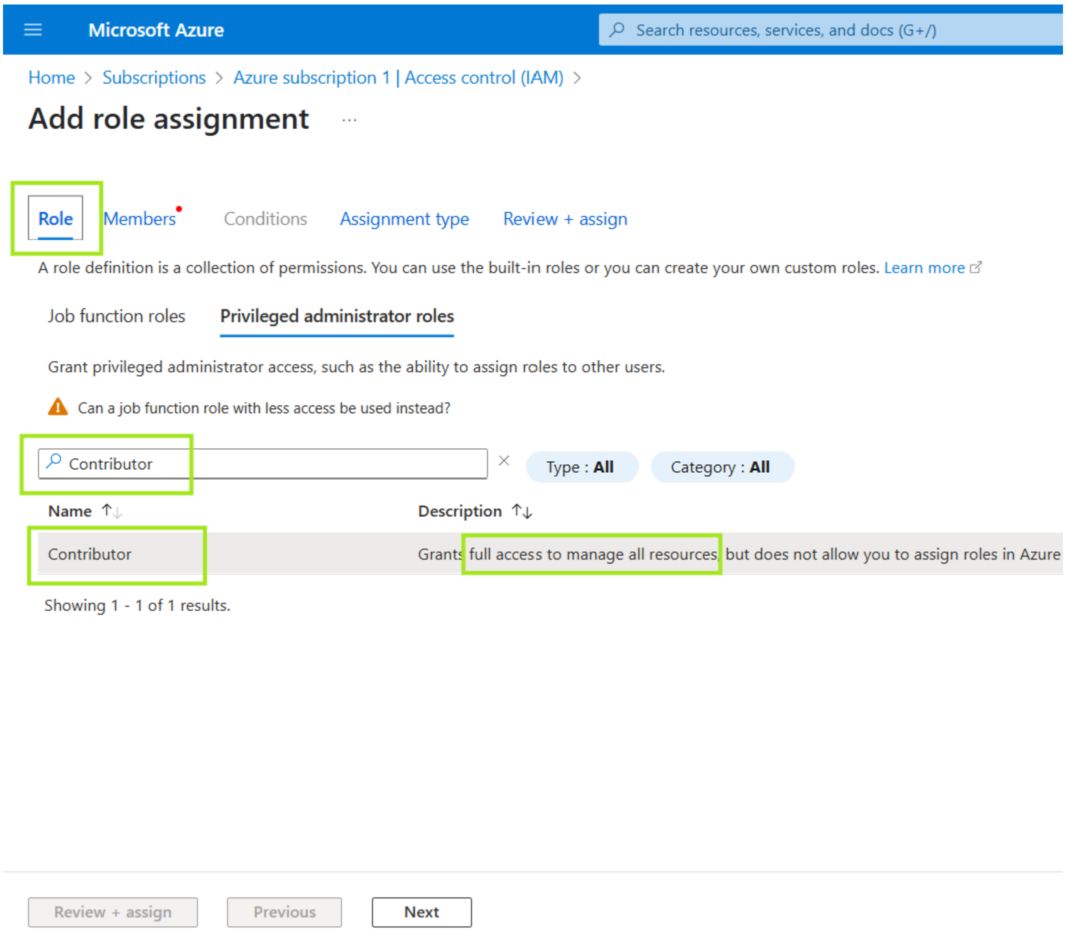
of August 31, 2024, Azure classic administrator roles (along with Azure classic resources, Azure Service M

Looking for the previous check access view? Click here.

Check access

Review the level of access a user, group, service principal, or managed identity has to this resource. Learn more

1.2.1 Creating Role



A role definition is a collection of permissions. You can use the built-in roles or you can create your own custom roles. Learn more

Grant privileged administrator access, such as the ability to assign roles to other users.

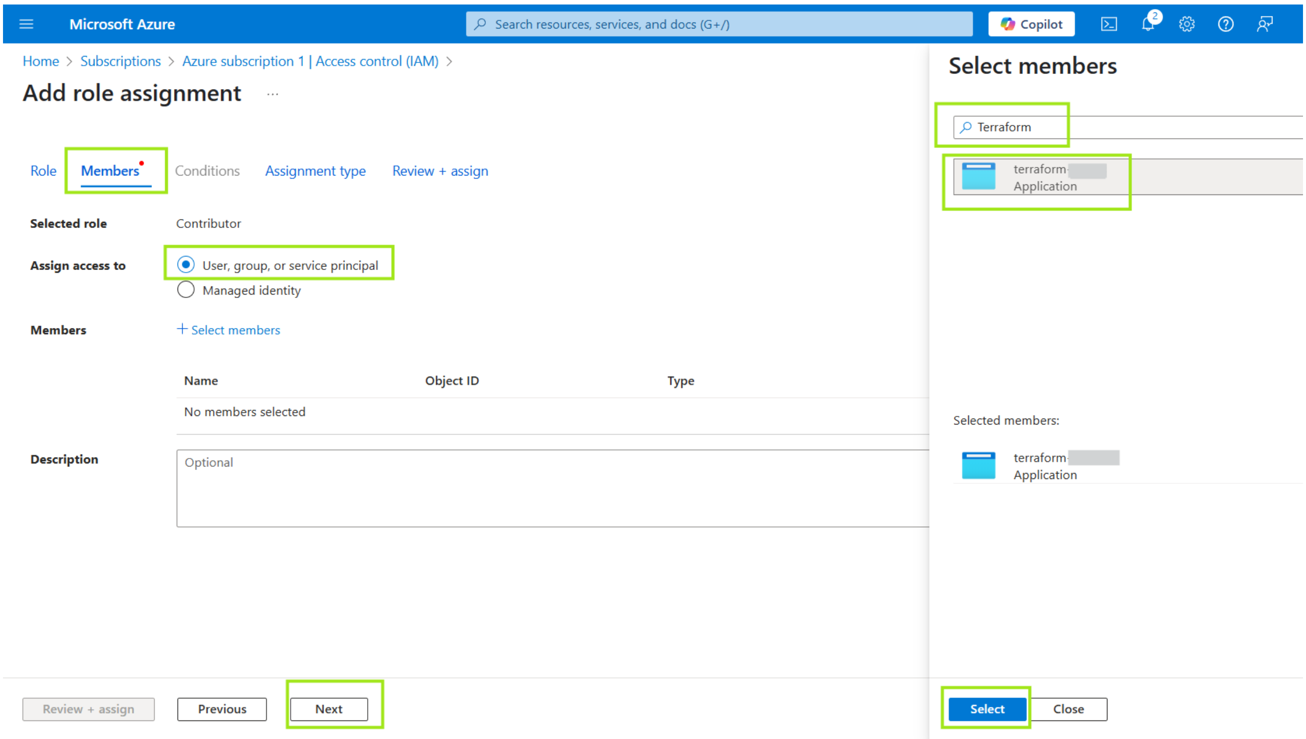
Can a job function role with less access be used instead?

Contributor

Name	Description
Contributor	Grants full access to manage all resources but does not allow you to assign roles in Azure

Showing 1 - 1 of 1 results.

1.2.2 Assigning Role to the Application



Home > Subscriptions > Azure subscription 1 | Access control (IAM) >

Add role assignment ...

Role | Members | Conditions | Assignment type | Review + assign

Selected role: Contributor

Assign access to: ● User, group, or service principal ○ Managed identity

Members: + Select members

Name	Object ID	Type
No members selected		

Description: Optional

Review + assign | Previous | Next

Select members

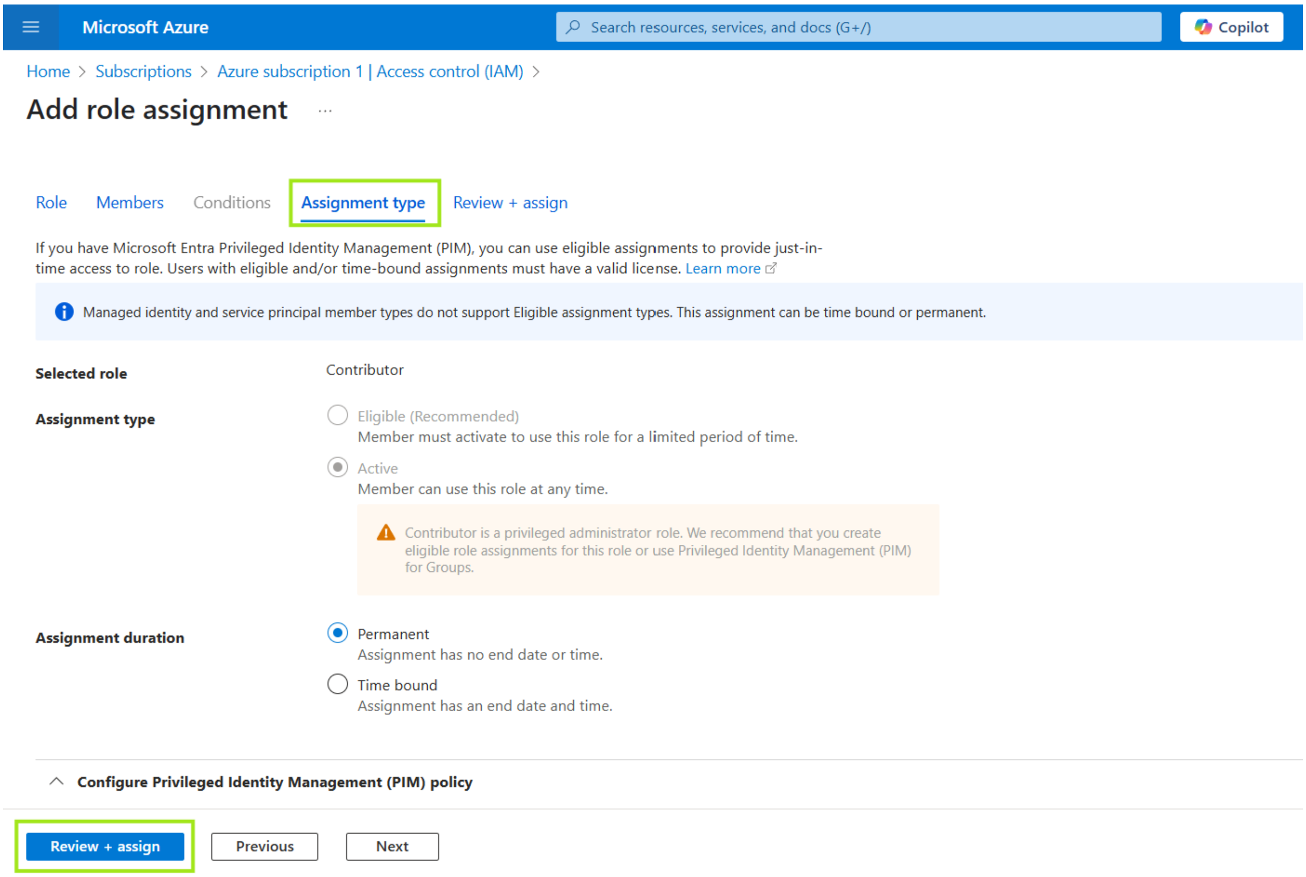
Terraform

terraform[redacted]
Application

Selected members:

terraform[redacted]
Application

Select | Close



Home > Subscriptions > Azure subscription 1 | Access control (IAM) >

Add role assignment ...

Role | Members | Conditions | Assignment type | Review + assign

If you have Microsoft Entra Privileged Identity Management (PIM), you can use eligible assignments to provide just-in-time access to role. Users with eligible and/or time-bound assignments must have a valid license. Learn more

Managed identity and service principal member types do not support Eligible assignment types. This assignment can be time bound or permanent.

Selected role: Contributor

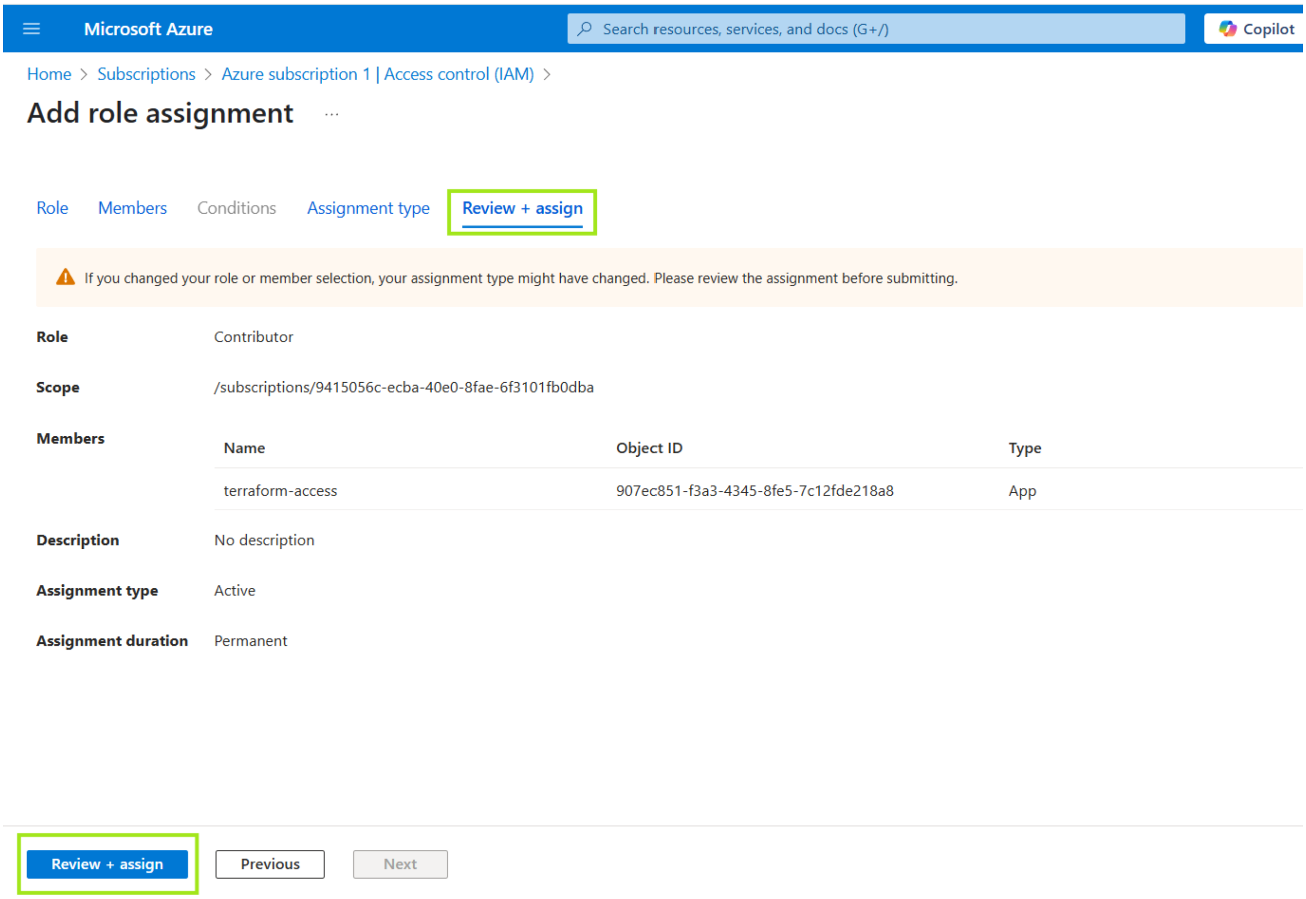
Assignment type:
○ Eligible (Recommended)
Member must activate to use this role for a limited period of time.
● Active
Member can use this role at any time.

Contributor is a privileged administrator role. We recommend that you create eligible role assignments for this role or use Privileged Identity Management (PIM) for Groups.

Assignment duration:
● Permanent
Assignment has no end date or time.
○ Time bound
Assignment has an end date and time.

Configure Privileged Identity Management (PIM) policy

Review + assign | Previous | Next



Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home > Subscriptions > Azure subscription 1 | Access control (IAM) >
Role
Members
Conditions
Assignment type
Review + assign
Review + assign
Previous
Next

Add role assignment ...

⚠ If you changed your role or member selection, your assignment type might have changed. Please review the assignment before submitting.

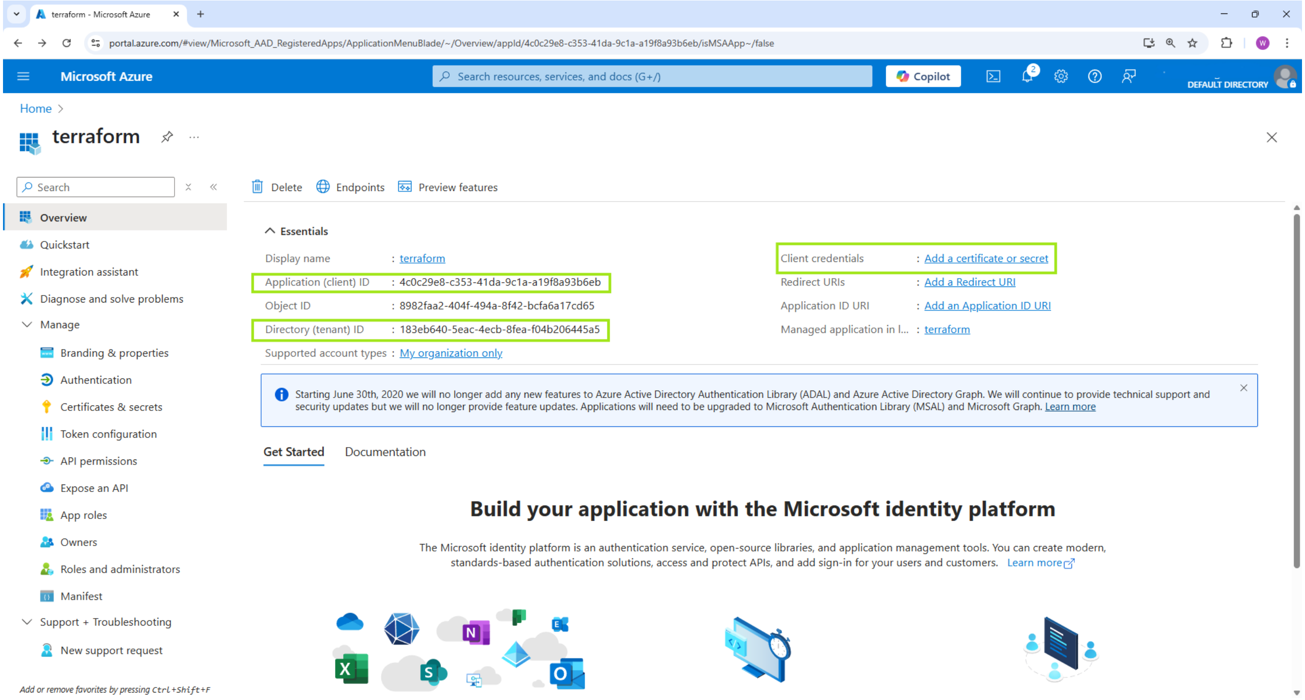
Role	Contributor
Scope	/subscriptions/9415056c-ecba-40e0-8fae-6f3101fb0dba
Members	

Name	Object ID	Type
terraform-access	907ec851-f3a3-4345-8fe5-7c12fde218a8	App

Description	No description
Assignment type	Active
Assignment duration	Permanent

1.3 Retrieving azure env variables for use in terraform cloud

1.3.1 Attain Azure Application Env Variables



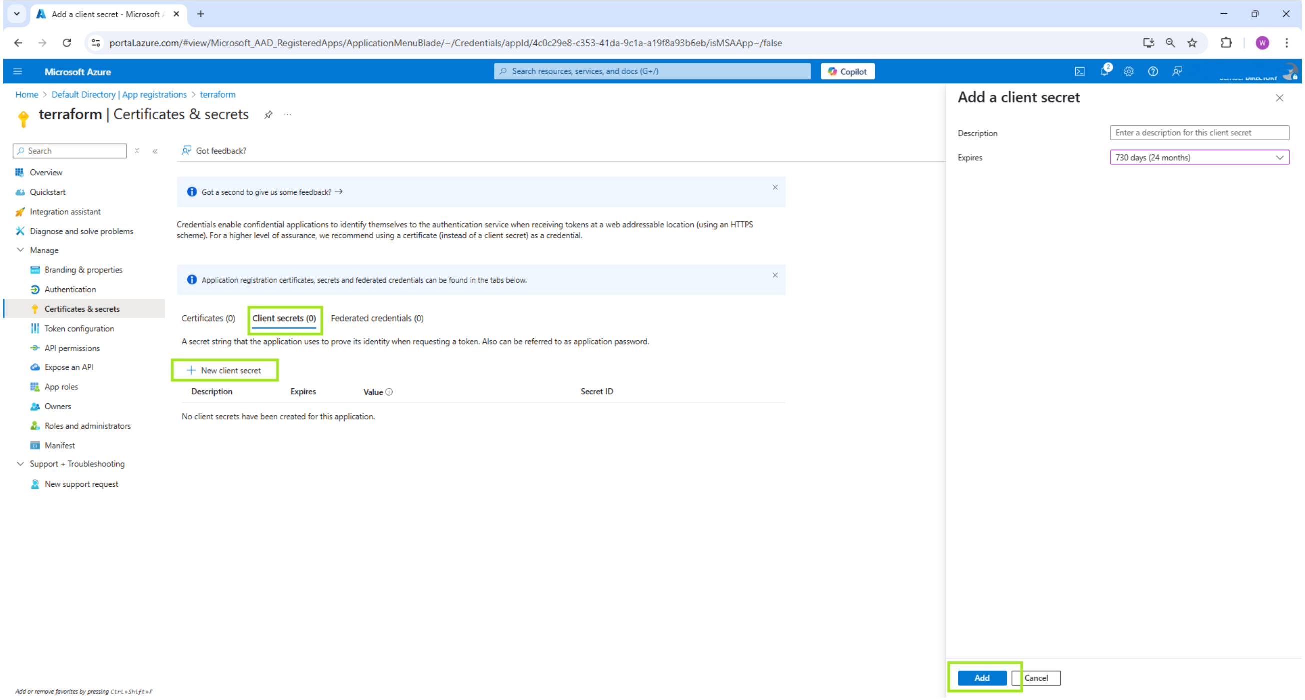
Display name	: terraform	Client credentials	: Add a certificate or secret
Application (client) ID	: 4c0c29e8-c353-41da-9c1a-a19f8a93b6eb	Redirect URIs	: Add a Redirect URI
Object ID	: 8982faa2-404f-494a-8f42-bcfa6a17cd65	Application ID URI	: Add an Application ID URI
Directory (tenant) ID	: 183eb640-5eac-4ecb-8fea-f04b206445a5	Managed application in l...	: terraform
Supported account types	: My organization only		

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure Active Directory Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Learn more

Build your application with the Microsoft identity platform

The Microsoft identity platform is an authentication service, open-source libraries, and application management tools. You can create modern, standards-based authentication solutions, access and protect APIs, and add sign-in for your users and customers. Learn more

1.3.2 Attain Azure Application Env Variables (Client Secret)


Add a client secret - Microsoft A
portal.azure.com/#view/Microsoft_AAD_RegisteredApps/ApplicationMenuBlade/~/Credentials/appId/4c0c29e8-c353-41da-9c1a-a19f8a93b6eb/isMSAApp~/false
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home > Default Directory | App registrations > terraform
terraform | Certificates & secrets
Search
Overview
Quickstart
Integration assistant
Diagnose and solve problems
Manage
Branding & properties
Authentication
Certificates & secrets
Token configuration
API permissions
Expose an API
App roles
Owners
Roles and administrators
Manifest
Support + Troubleshooting
New support request
Add or remove favorites by pressing Ctrl+Shift+F
Got feedback?
Certificates (0)
Client secrets (0)
Federated credentials (0)
+ New client secret
Add
Cancel

Got a second to give us some feedback? →

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

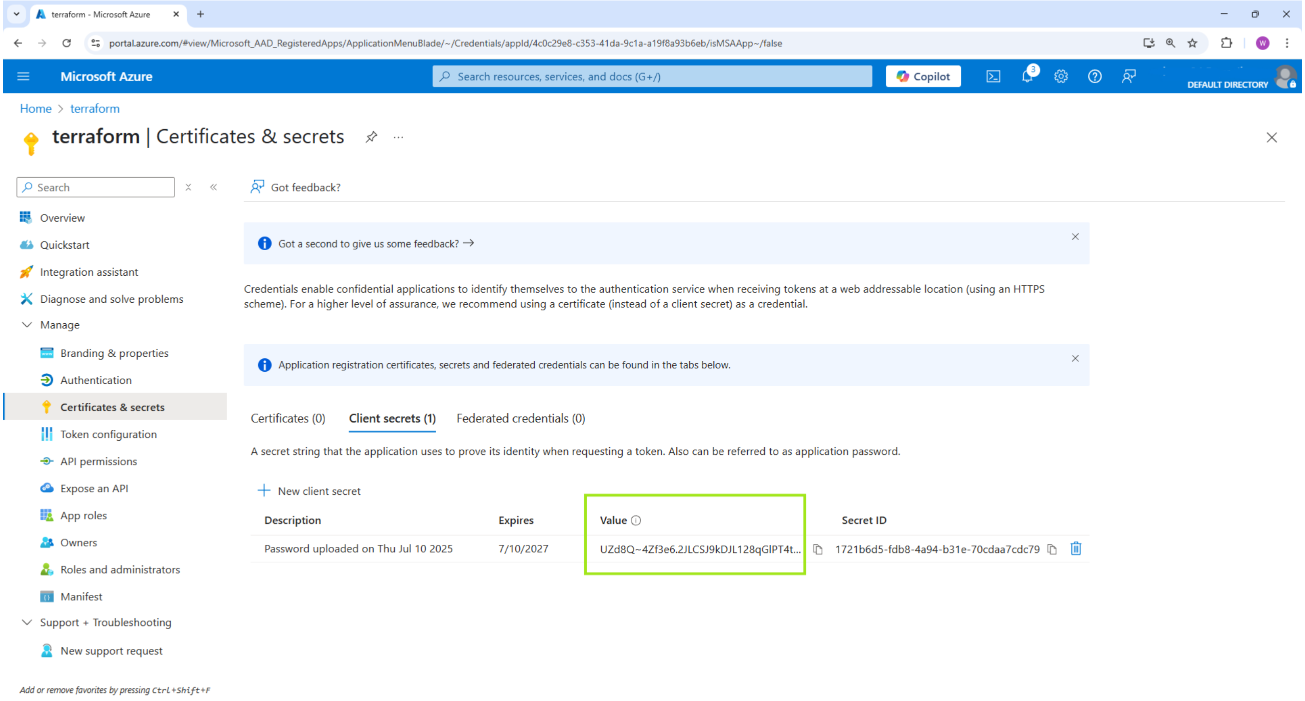
A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

Description	Expires	Value	Secret ID
No client secrets have been created for this application.			

Add a client secret

Description: Enter a description for this client secret

Expires: 730 days (24 months)


terraform - Microsoft Azure
portal.azure.com/#view/Microsoft_AAD_RegisteredApps/ApplicationMenuBlade/~/Credentials/appId/4c0c29e8-c353-41da-9c1a-a19f8a93b6eb/isMSAApp~/false
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
DEFAULT DIRECTORY
Home > terraform
terraform | Certificates & secrets
Search
Overview
Quickstart
Integration assistant
Diagnose and solve problems
Manage
Branding & properties
Authentication
Certificates & secrets
Token configuration
API permissions
Expose an API
App roles
Owners
Roles and administrators
Manifest
Support + Troubleshooting
New support request
Add or remove favorites by pressing Ctrl+Shift+F
Got feedback?
Got a second to give us some feedback? →

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

Certificates (0) | **Client secrets (1)** | Federated credentials (0)

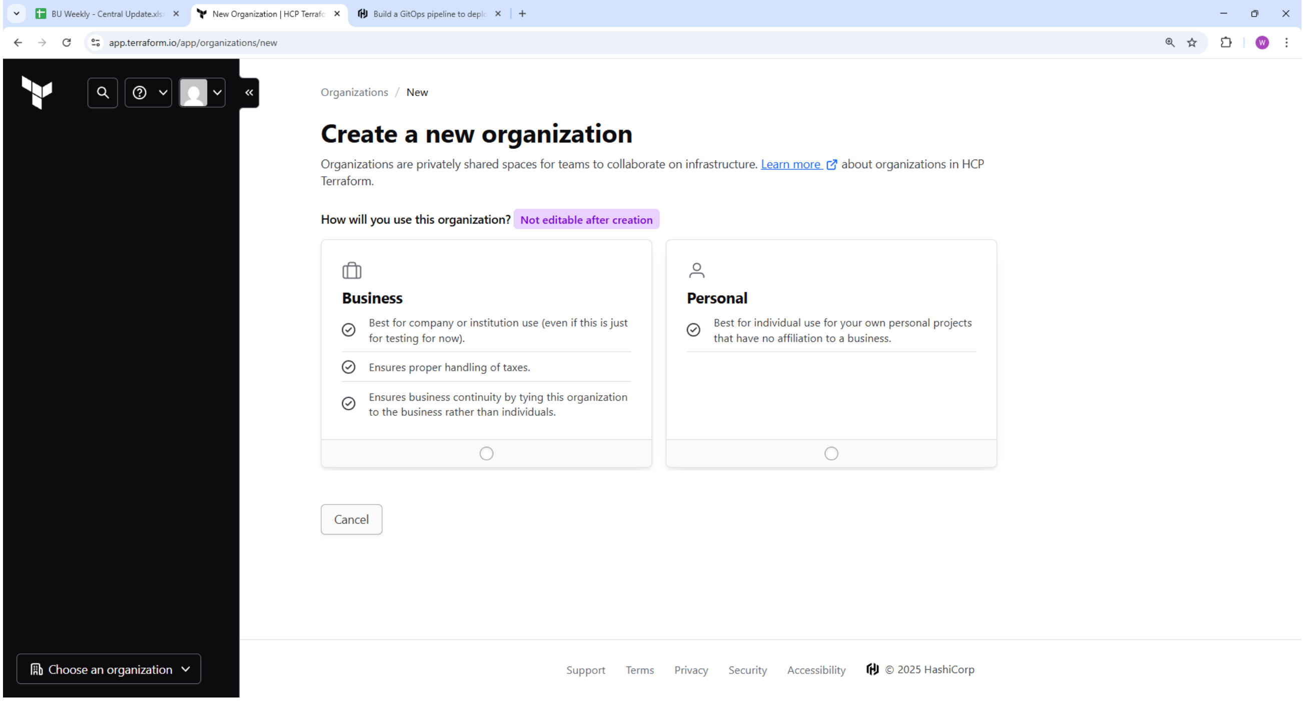
A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value	Secret ID
Password uploaded on Thu Jul 10 2025	7/10/2027	UZd8Q~4Zf3e6.2JLCSJ9kDJL128qGlPT4t...	1721b6d5-fdb8-4a94-b31e-70cdaa7cdc79

2. Creating a Version Control Workflow with Terraform Cloud

2.1 Creating an organization


BU Weekly - Central Update.xls
New Organization | HCP Terraf
Build a GitOps pipeline to depl
app.terraform.io/app/organizations/new
Organizations / New
Choose an organization
Support
Terms
Privacy
Security
Accessibility
© 2025 HashiCorp

Create a new organization

Organizations are privately shared spaces for teams to collaborate on infrastructure. Learn more about organizations in HCP Terraform.

How will you use this organization? Not editable after creation

Business
- Best for company or institution use (even if this is just for testing for now).
- Ensures proper handling of taxes.
- Ensures business continuity by tying this organization to the business rather than individuals.

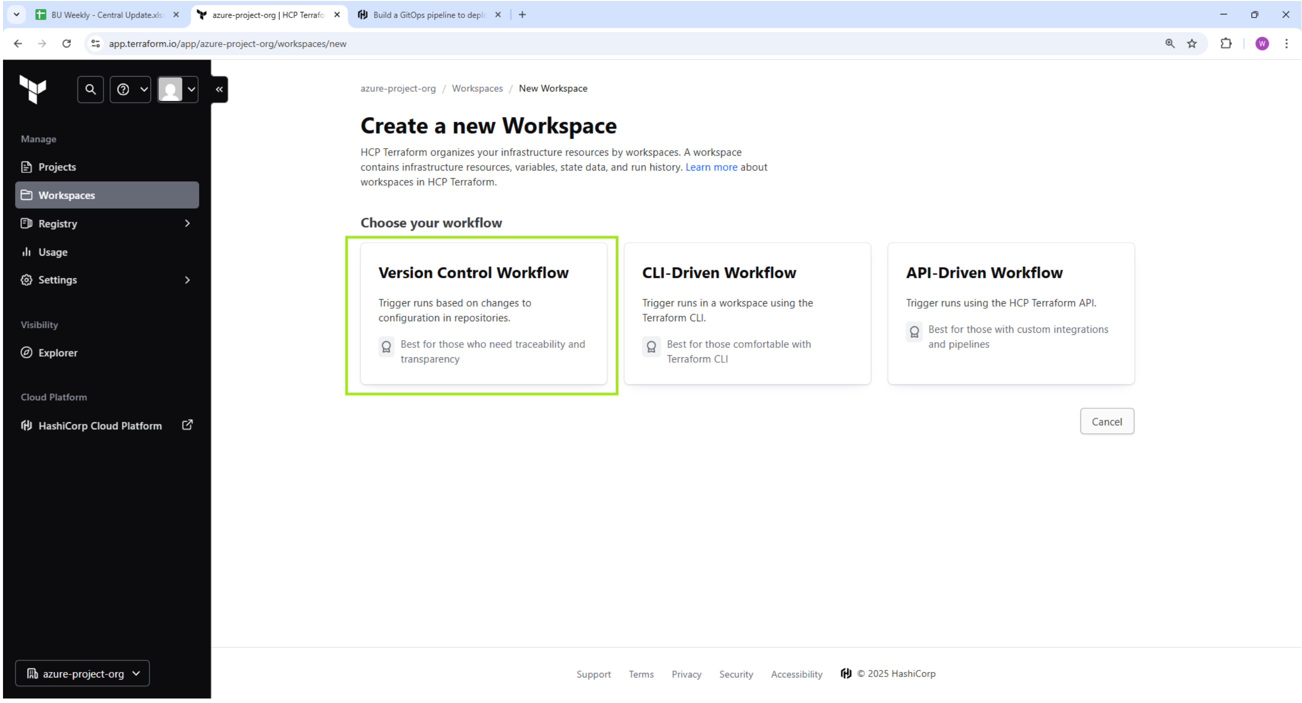
○

Personal
- Best for individual use for your own personal projects that have no affiliation to a business.

○

Cancel

2.2 Creating a Version Control Workflow workspace



azure-project-org / Workspaces / New Workspace

Create a new Workspace

HCP Terraform organizes your infrastructure resources by workspaces. A workspace contains infrastructure resources, variables, state data, and run history. Learn more about workspaces in HCP Terraform.

Choose your workflow

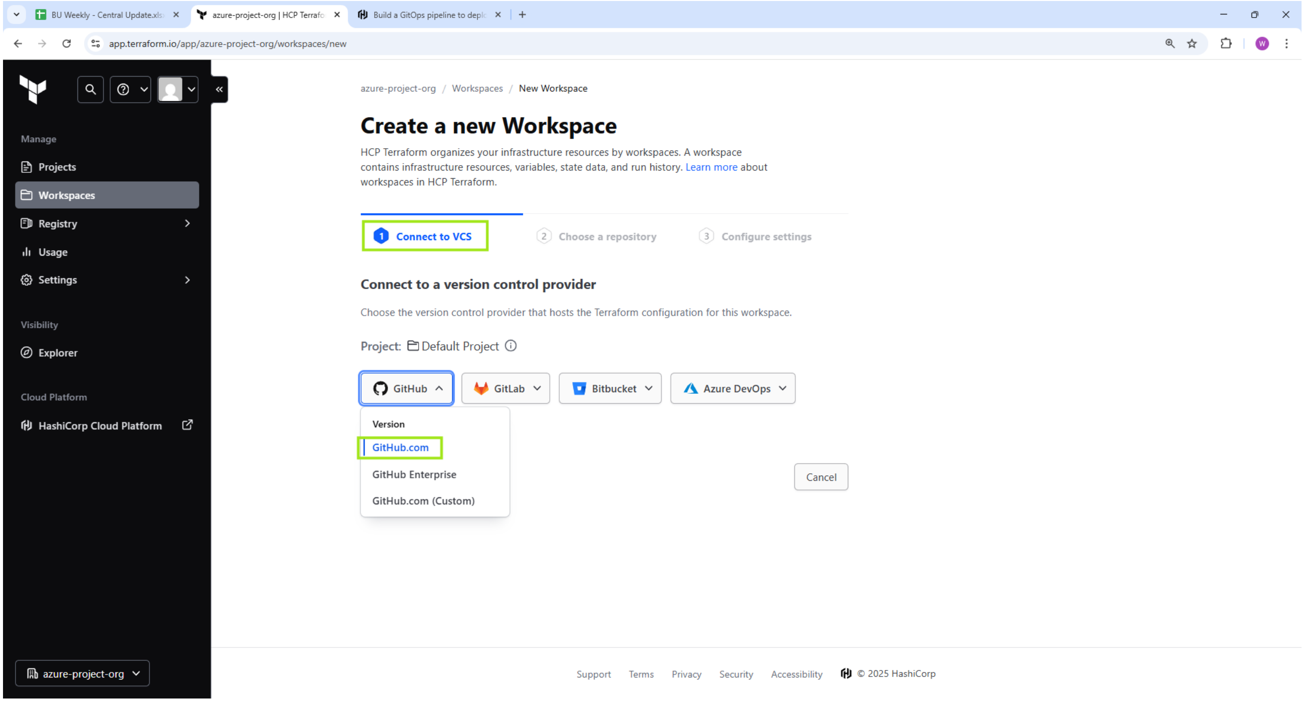
Version Control Workflow
Trigger runs based on changes to configuration in repositories.
Best for those who need traceability and transparency

CLI-Driven Workflow
Trigger runs in a workspace using the Terraform CLI.
Best for those comfortable with Terraform CLI

API-Driven Workflow
Trigger runs using the HCP Terraform API.
Best for those with custom integrations and pipelines

Cancel

2.3 Linking workspace with GitHub (TF Cloud uses GitHub App for Auth)



azure-project-org / Workspaces / New Workspace

Create a new Workspace

HCP Terraform organizes your infrastructure resources by workspaces. A workspace contains infrastructure resources, variables, state data, and run history. Learn more about workspaces in HCP Terraform.

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.

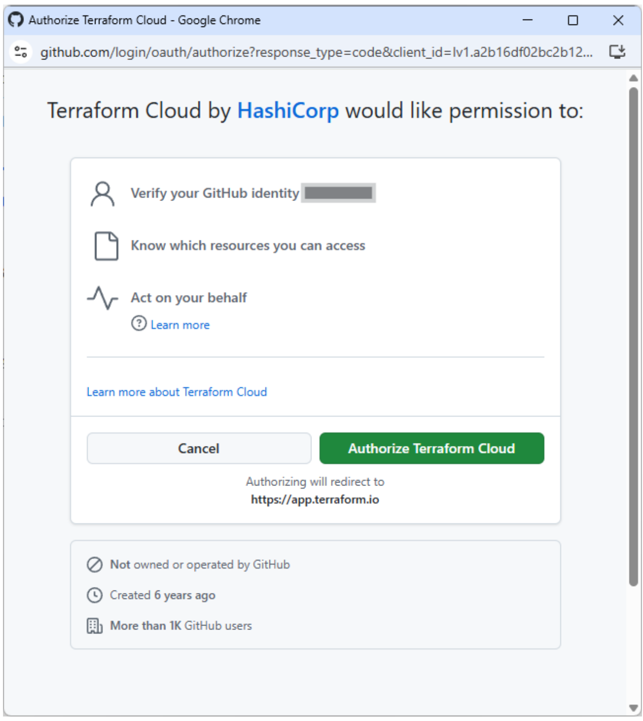
Project: Default Project

GitHub　GitLab　Bitbucket　Azure DevOps

Version
GitHub.com
GitHub Enterprise
GitHub.com (Custom)

Cancel

2.3.1 Authorizing Terraform Cloud to access selected Repository



Authorize Terraform Cloud - Google Chrome

github.com/login/oauth/authorize?response_type=code&client_id=Iv1.a2b16df02bc2b12...

Terraform Cloud by HashiCorp would like permission to:

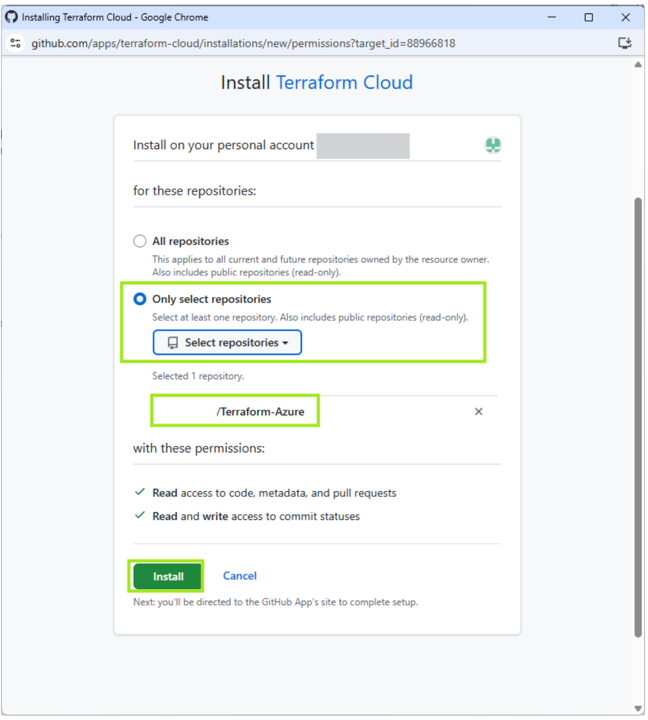
- Verify your GitHub identity [redacted]
- Know which resources you can access
- Act on your behalf
  Learn more

Learn more about Terraform Cloud

Cancel | Authorize Terraform Cloud

Authorizing will redirect to
https://app.terraform.io

- Not owned or operated by GitHub
- Created 6 years ago
- More than 1K GitHub users



Installing Terraform Cloud - Google Chrome

github.com/apps/terraform-cloud/installations/new/permissions?target_id=88966818

Install Terraform Cloud

Install on your personal account [redacted]

for these repositories:

○ All repositories
This applies to all current and future repositories owned by the resource owner. Also includes public repositories (read-only).

● Only select repositories
Select at least one repository. Also includes public repositories (read-only).

Select repositories ▾

Selected 1 repository.

/Terraform-Azure ✕

with these permissions:

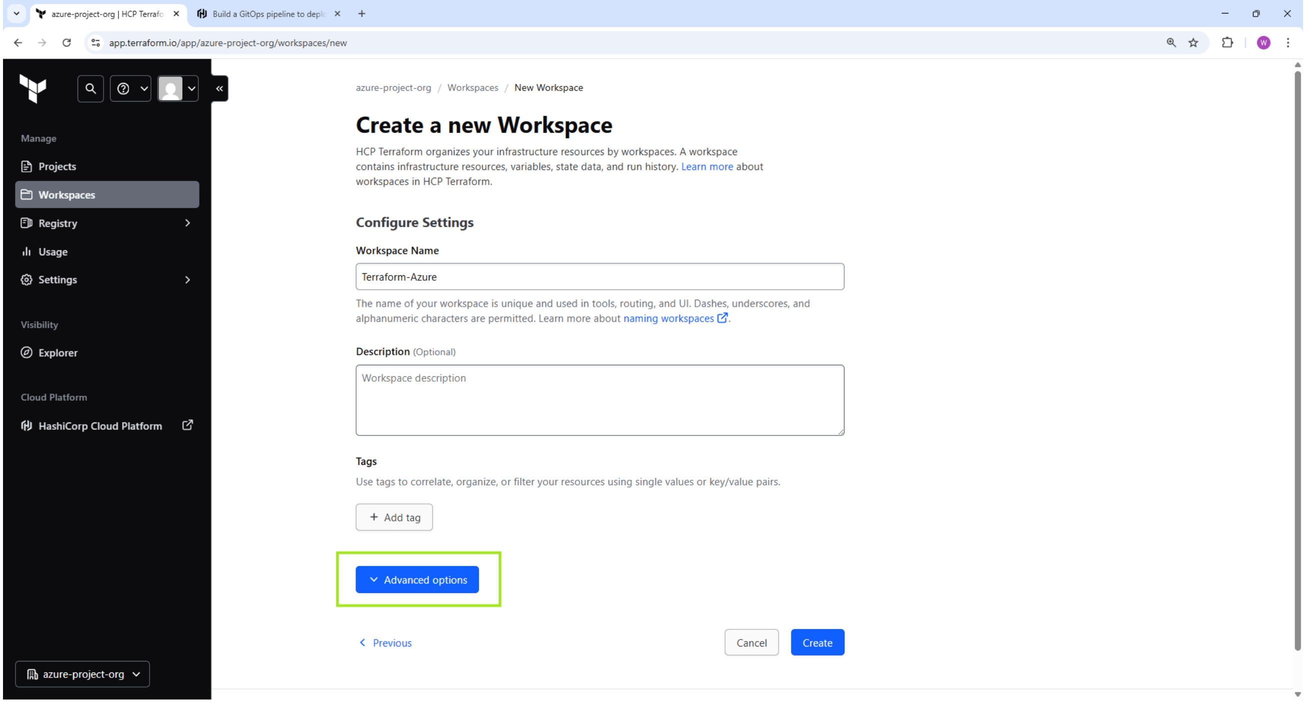
✓ Read access to code, metadata, and pull requests

✓ Read and write access to commit statuses

Install | Cancel

Next: you'll be directed to the GitHub App's site to complete setup.

2.4 Configure workflow settings (advanced options) in workspace



azure-project-org / Workspaces / New Workspace

Create a new Workspace

HCP Terraform organizes your infrastructure resources by workspaces. A workspace contains infrastructure resources, variables, state data, and run history. Learn more about workspaces in HCP Terraform.

Configure Settings

Workspace Name: Terraform-Azure

The name of your workspace is unique and used in tools, routing, and UI. Dashes, underscores, and alphanumeric characters are permitted. Learn more about naming workspaces.

Description (Optional): Workspace description

Tags

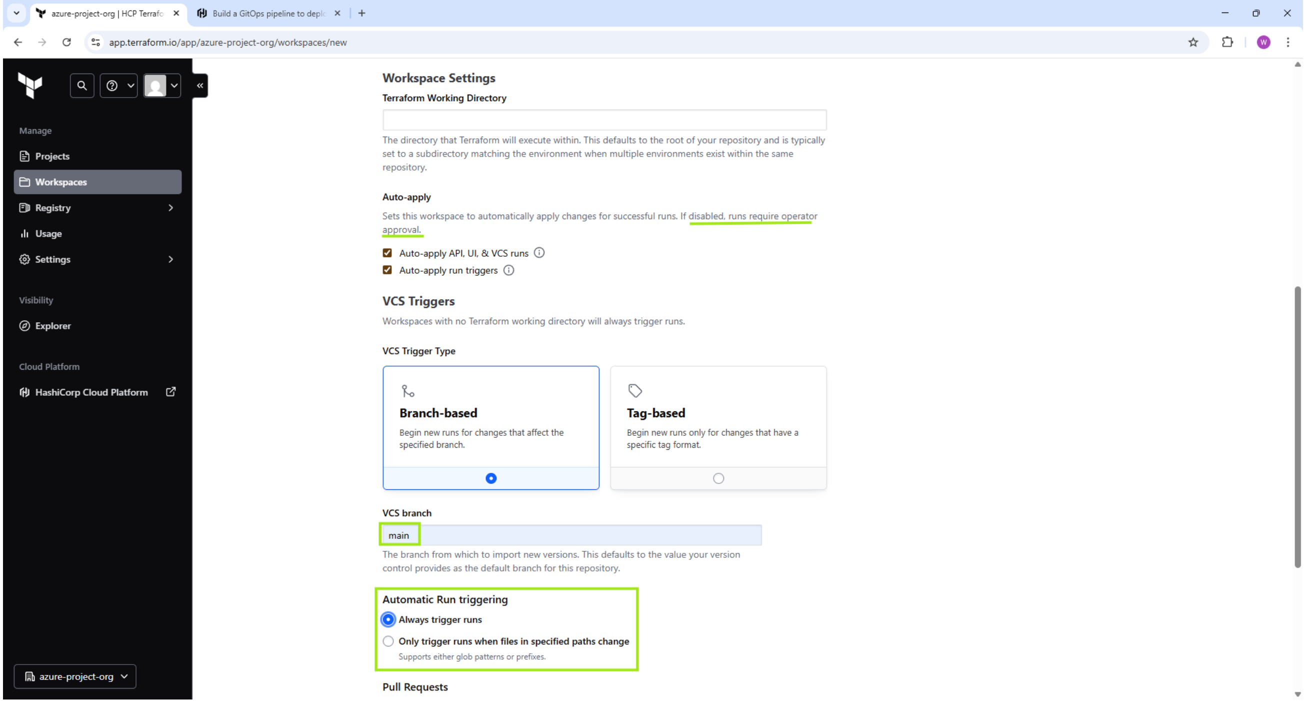
Use tags to correlate, organize, or filter your resources using single values or key/value pairs.

+ Add tag

Advanced options

< Previous | Cancel | Create

2.4.1 Configure Auto-Apply, Repo Branch, Run Triggers, VCS Trigger Type etc.



Workspace Settings

Terraform Working Directory

The directory that Terraform will execute within. This defaults to the root of your repository and is typically set to a subdirectory matching the environment when multiple environments exist within the same repository.

Auto-apply

Sets this workspace to automatically apply changes for successful runs. If disabled, runs require operator approval.

☑ Auto-apply API, UI, & VCS runs

☑ Auto-apply run triggers

VCS Triggers

Workspaces with no Terraform working directory will always trigger runs.

VCS Trigger Type

Branch-based ●
Begin new runs for changes that affect the specified branch.

Tag-based ○
Begin new runs only for changes that have a specific tag format.

VCS branch

main

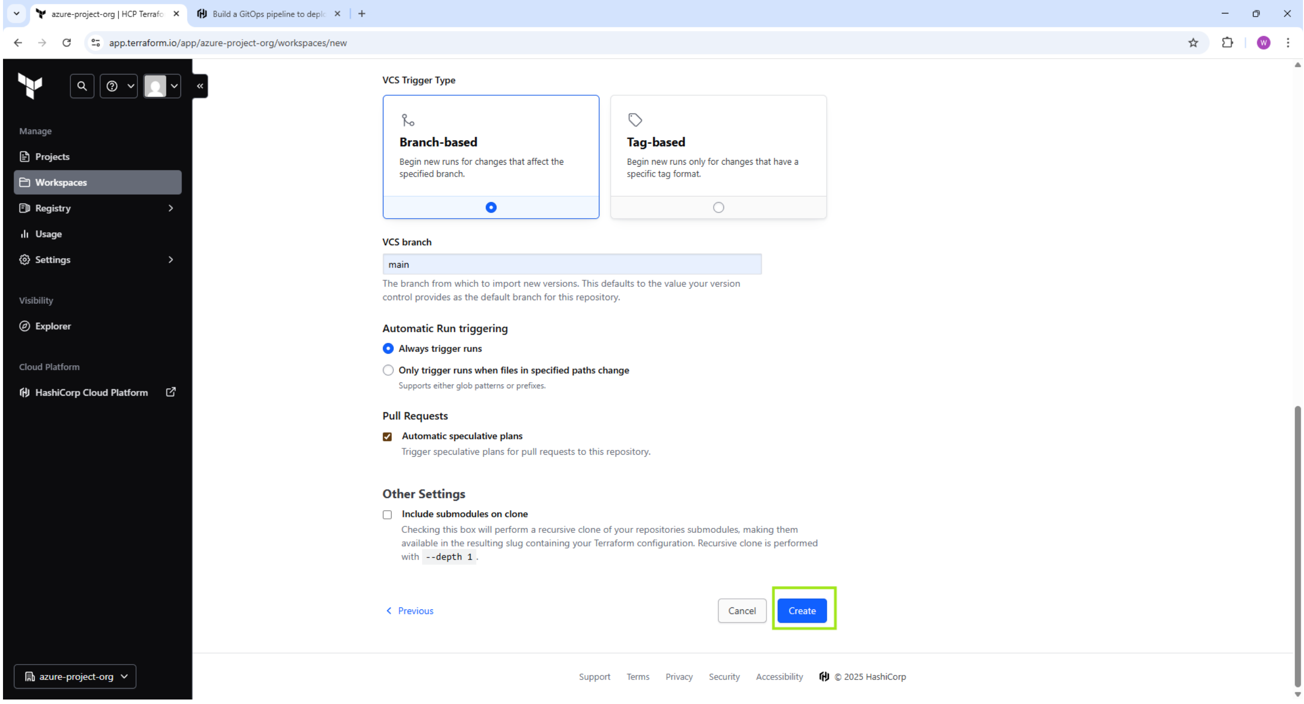
The branch from which to import new versions. This defaults to the value your version control provides as the default branch for this repository.

Automatic Run triggering

● Always trigger runs

○ Only trigger runs when files in specified paths change
Supports either glob patterns or prefixes.

Pull Requests



VCS Trigger Type

Branch-based ●
Begin new runs for changes that affect the specified branch.

Tag-based ○
Begin new runs only for changes that have a specific tag format.

VCS branch

main

The branch from which to import new versions. This defaults to the value your version control provides as the default branch for this repository.

Automatic Run triggering

● Always trigger runs

○ Only trigger runs when files in specified paths change
Supports either glob patterns or prefixes.

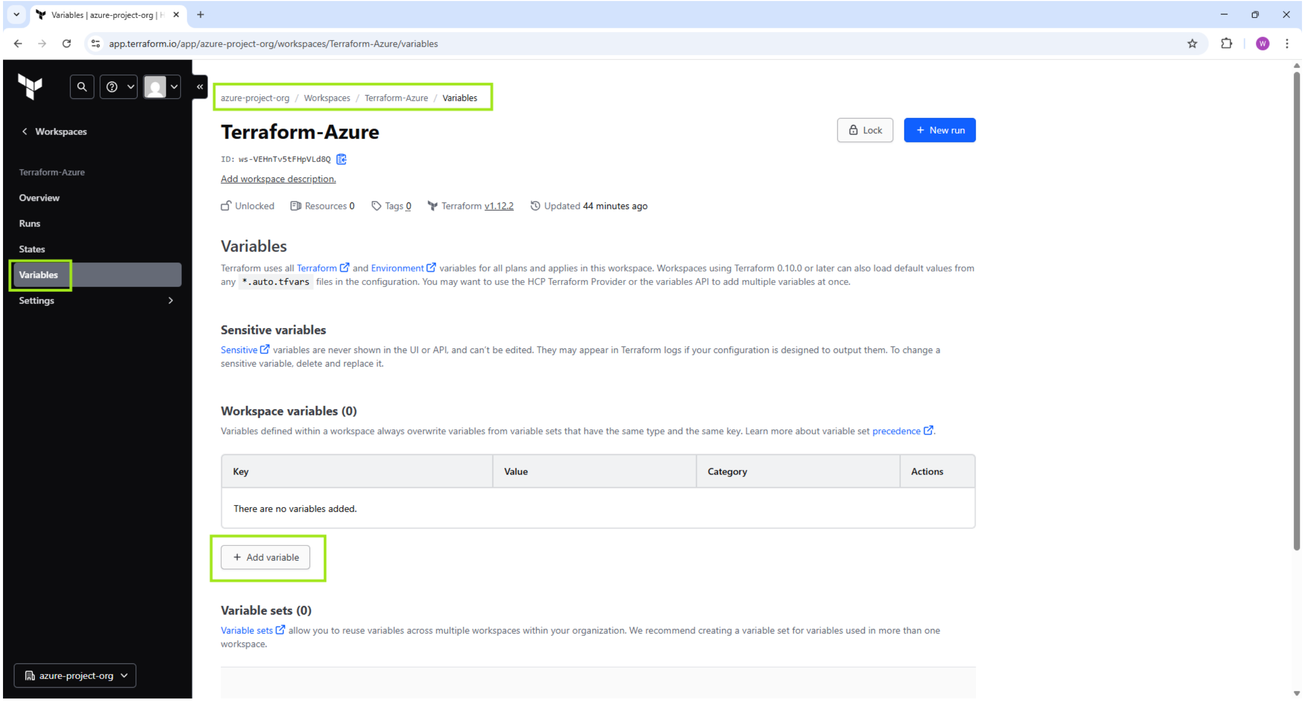
Pull Requests

☑ Automatic speculative plans
Trigger speculative plans for pull requests to this repository.

Other Settings

□ Include submodules on clone
Checking this box will perform a recursive clone of your repositories submodules, making them available in the resulting slug containing your Terraform configuration. Recursive clone is performed with `--depth 1`.

2.5 Adding Terraform Workspace Environment Variables



Variables | azure-project-org | H
app.terraform.io/app/azure-project-org/workspaces/Terraform-Azure/variables
Workspaces
Terraform-Azure
Overview
Runs
States
Variables
Settings
azure-project-org

azure-project-org / Workspaces / Terraform-Azure / Variables

Terraform-Azure

Lock | + New run

ID: ws-VEHnTv5tFHpVLd8Q

Add workspace description.

Unlocked | Resources 0 | Tags 0 | Terraform v1.12.2 | Updated 44 minutes ago

Variables

Terraform uses all Terraform and Environment variables for all plans and applies in this workspace. Workspaces using Terraform 0.10.0 or later can also load default values from any `*.auto.tfvars` files in the configuration. You may want to use the HCP Terraform Provider or the variables API to add multiple variables at once.

Sensitive variables

Sensitive variables are never shown in the UI or API, and can't be edited. They may appear in Terraform logs if your configuration is designed to output them. To change a sensitive variable, delete and replace it.

Workspace variables (0)

Variables defined within a workspace always overwrite variables from variable sets that have the same type and the same key. Learn more about variable set precedence.

Key	Value	Category	Actions
There are no variables added.			

+ Add variable

Variable sets (0)

Variable sets allow you to reuse variables across multiple workspaces within your organization. We recommend creating a variable set for variables used in more than one workspace.

See values in 1.3 Retrieving env variables for use in terraform cloud

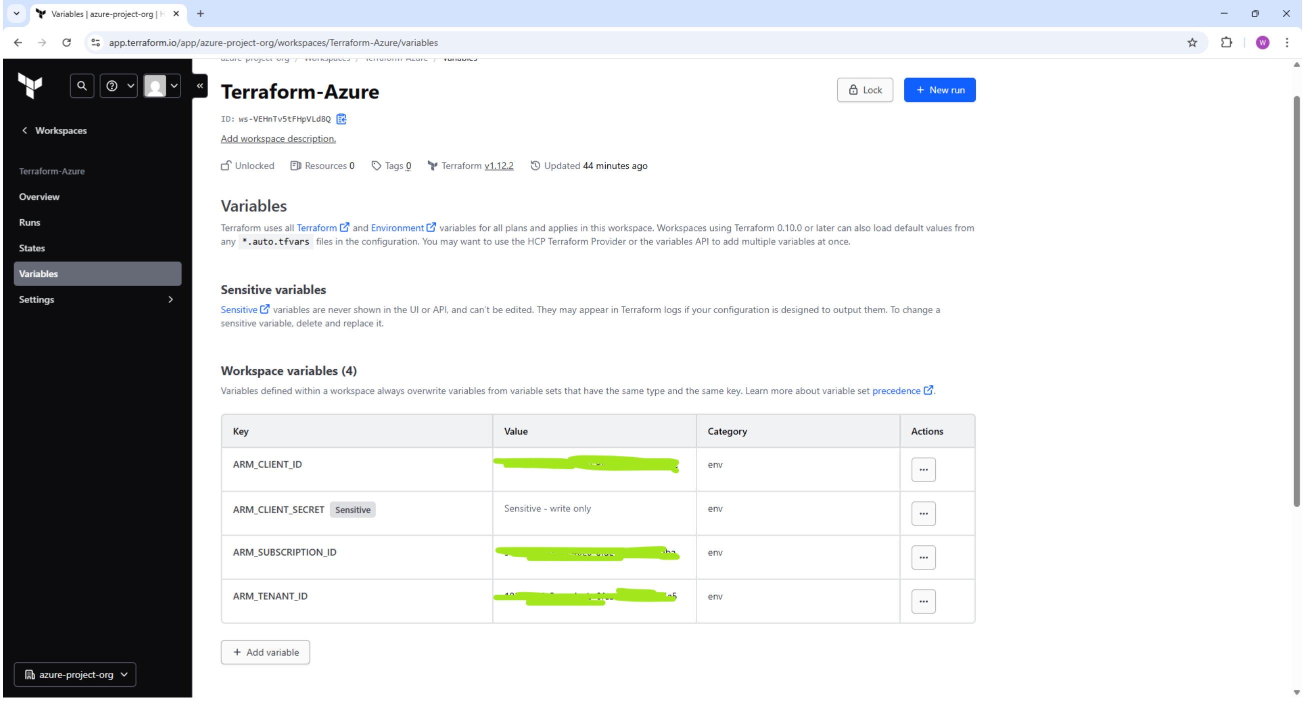
ARM_CLIENT_ID = Application (client) ID

ARM_CLIENT_SECRET = Application Client Secret Value (Mark as Sensitive)

ARM_SUBSCRIPTION_ID = Azure Subscription ID

ARM_TENANT_ID = Directory (tenant) ID

2.5.1 Terraform Workspace Environment Variables



Variables | azure-project-org | H
app.terraform.io/app/azure-project-org/workspaces/Terraform-Azure/variables
Workspaces
Terraform-Azure
Overview
Runs
States
Variables
Settings
azure-project-org

Terraform-Azure

Lock | + New run

ID: ws-VEHnTv5tFHpVLd8Q

Add workspace description.

Unlocked | Resources 0 | Tags 0 | Terraform v1.12.2 | Updated 44 minutes ago

Variables

Terraform uses all Terraform and Environment variables for all plans and applies in this workspace. Workspaces using Terraform 0.10.0 or later can also load default values from any `*.auto.tfvars` files in the configuration. You may want to use the HCP Terraform Provider or the variables API to add multiple variables at once.

Sensitive variables

Sensitive variables are never shown in the UI or API, and can't be edited. They may appear in Terraform logs if your configuration is designed to output them. To change a sensitive variable, delete and replace it.

Workspace variables (4)

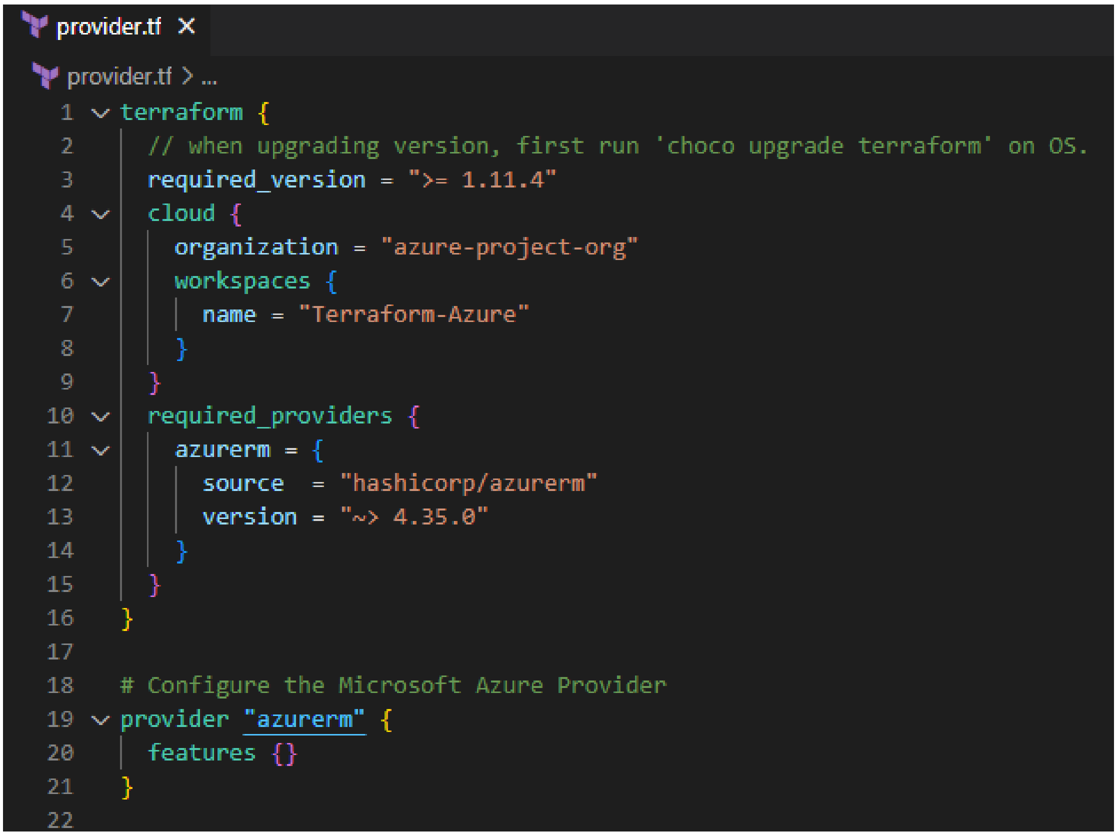
Variables defined within a workspace always overwrite variables from variable sets that have the same type and the same key. Learn more about variable set precedence.

Key	Value	Category	Actions
ARM_CLIENT_ID	[redacted]	env	...
ARM_CLIENT_SECRET Sensitive	Sensitive - write only	env	...
ARM_SUBSCRIPTION_ID	[redacted]	env	...
ARM_TENANT_ID	[redacted]	env	...

+ Add variable

3. Terraform VCS Workflow Illustration

3.1 Terraform Baseline Code Setup

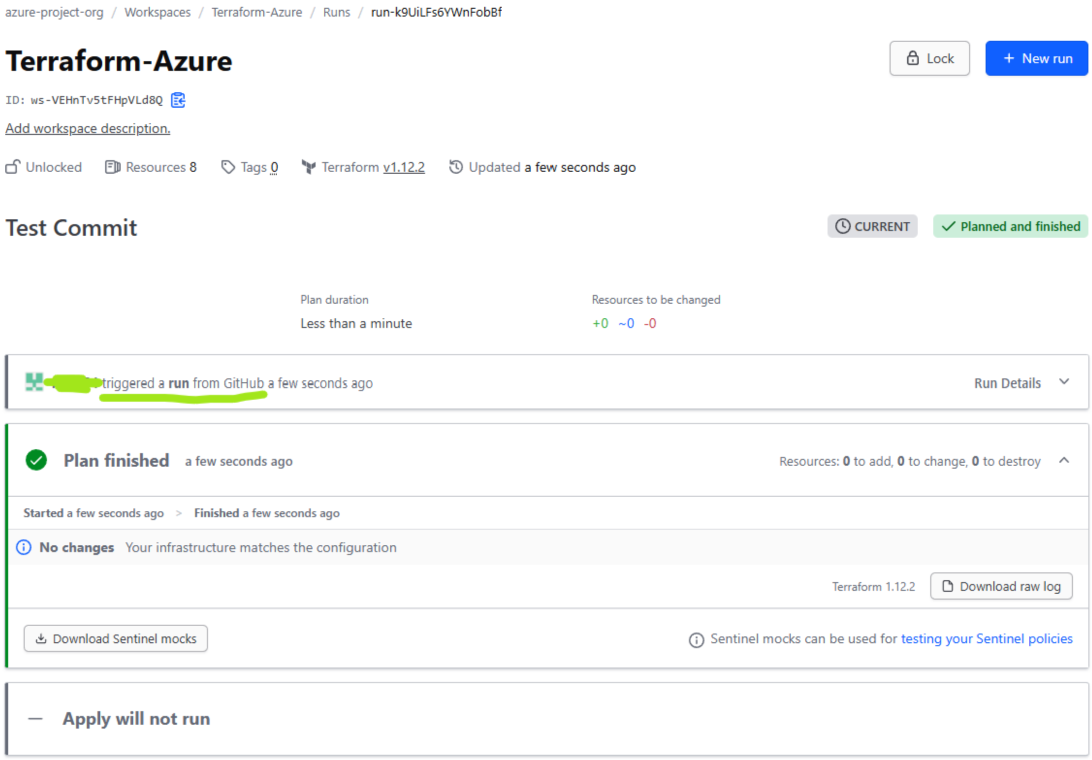


```
terraform {
  // when upgrading version, first run 'choco upgrade terraform' on OS.
  required_version = ">= 1.11.4"
  cloud {
    organization = "azure-project-org"
    workspaces {
      name = "Terraform-Azure"
    }
  }
  required_providers {
    azurerm = {
      source  = "hashicorp/azurerm"
      version = "~> 4.35.0"
    }
  }
}

# Configure the Microsoft Azure Provider
provider "azurerm" {
  features {}
}

```

3.2 Terraform Trigger through TF Cloud upon Commit


azure-project-org / Workspaces / Terraform-Azure / Runs / run-k9UiLFs6YWnFobBf
Lock
+ New run

Terraform-Azure

ID: ws-VEHnTv5tFHpVLd8Q

Add workspace description.

Unlocked · Resources 8 · Tags 0 · Terraform v1.12.2 · Updated a few seconds ago

Test Commit

CURRENT · ✓ Planned and finished

Plan duration: Less than a minute

Resources to be changed: +0 ~0 -0

[redacted] triggered a **run** from GitHub a few seconds ago — Run Details

✓ **Plan finished** a few seconds ago — Resources: **0** to add, **0** to change, **0** to destroy

Started a few seconds ago > Finished a few seconds ago

No changes Your infrastructure matches the configuration

Terraform 1.12.2 · Download raw log

Download Sentinel mocks · Sentinel mocks can be used for testing your Sentinel policies

— **Apply will not run**