Code-centric IaC with Pulumi
GDG Devfest Delhi 2022

2022-12-03
Jasbir Singh

Disclaimer:
The content and the views presented during the talk/session are the author’s own and not of the organizations/companies they are associated with.

Overview

- Pulumi’s main characteristics, comparison and benefits
- Pulumi’s Architecture
- How to use it
- Demonstration

Pulumi

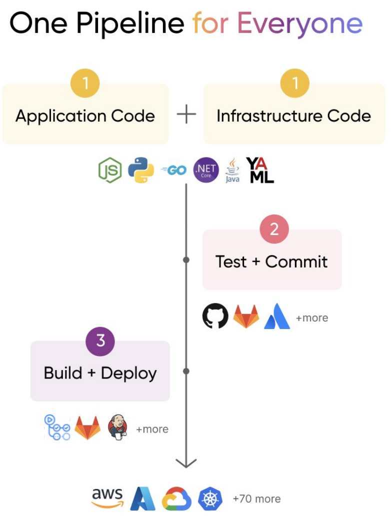
From YAML to code

Pulumi follows the principles of a Developer-First infrastructure.

It allows you to write infrastructure as code in a standard programming language!

Pulumi

CLOUD NATIVE
COMPUTING FOUNDATION



One Pipeline for Everyone

1 Application Code + 1 Infrastructure Code

YAML

2 Test + Commit

+more

3 Build + Deploy

+more

aws +70 more

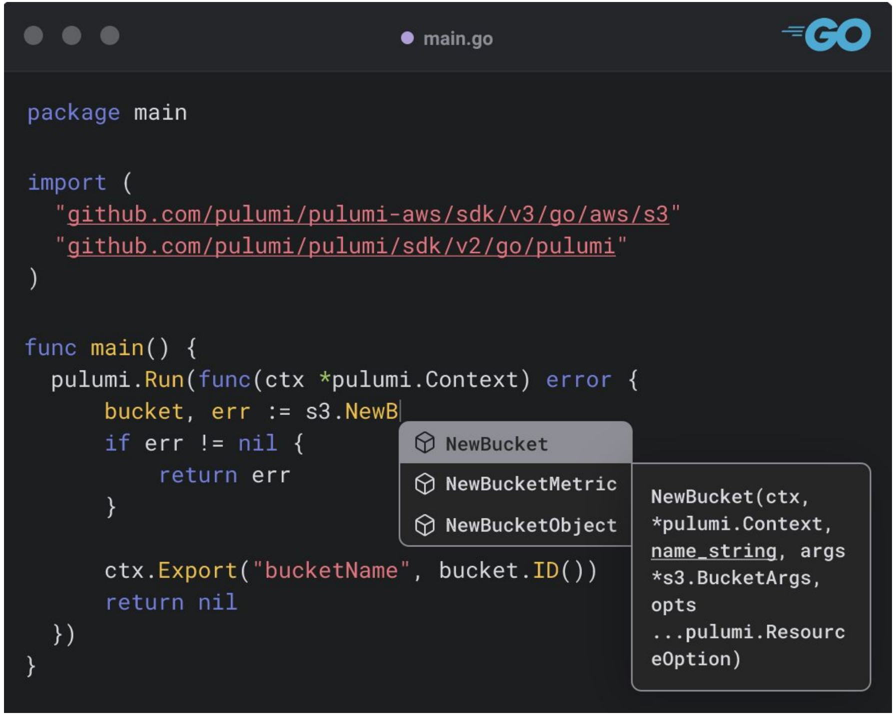
- Founded by Joe Duffy & Eric Rudder in 2017; Seattle; 37.5 Mio Serie B
- Free **Pulumi Open Source** - github.com/pulumi/pulumi
- vs . **Pulumi Service** (Fully-managed cloud engineering platform, expensive)
- **Multi-Cloud** capability & deployments
- **Secret** Management
- **Remote-State** handling
- Multiple-Languages
  - GO TS C# Java
- Stack configurations for handling multiple environments

Pulumi vs Terraform

Feature	Pulumi	Terraform
Language support	Python, TypeScript, JavaScript, Go, C#, F#, Java, YAML	HashiCorp Configuration Language (HCL)
Maturity	Some lack of documentation. Mid-size community.	Very mature. Large community.
Cloud Native support	Richly typed. Includes CRDs & in-cluster operator support for GitOps delivery.	Core API typed. Generic support for CRD.
Reuse, Modularity	Flexible. Reuse functions, classes, packages, and Pulumi components.	Constrained. Can only reuse Terraform modules.
Modes of execution	Run CLI commands or initiate commands programmatically with Automation API.	Run CLI commands or perform remote runs with SaaS offering.
Import code from other IaC	Yes. It allows to convert templates by Terraform HCL, Kubernetes YAML, and Azure ARM into Pulumi programs.	No
State Management	Native support for remote State Handling	Native support for remote State Handling
Secrete Management	Secretes can be managed remotely in Secrete Manager	Difficult to prevent Secretes ending up in StateFiles

Code has a lot of advantages over *static configuration languages*

- Stay with your Application Language
  - Loops, IF, ...
  - Packages/Modules you know
- Rich IDE support
- Type checking
- Create useful abstraction (package managers)
- Run unit and integration tests
- Easy to read - very subjective □



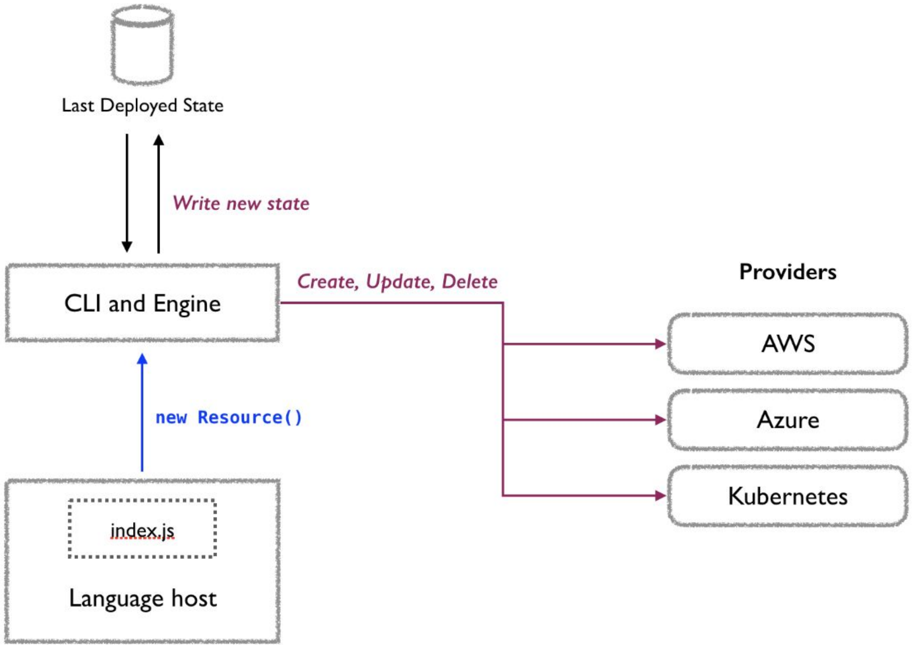
```go
package main

import (
  "github.com/pulumi/pulumi-aws/sdk/v3/go/aws/s3"
  "github.com/pulumi/pulumi/sdk/v2/go/pulumi"
)

func main() {
  pulumi.Run(func(ctx *pulumi.Context) error {
      bucket, err := s3.NewB
      if err != nil {
          return err
      }

      ctx.Export("bucketName", bucket.ID())
      return nil
  })
}
```

Pulumi Architecture

Language host. A language executor, which is a binary, that Pulumi uses to launch the runtime for the language your program is written in

Deployment Engine. It is responsible for computing the set of operations needed to drive the current state of your infrastructure into the desired state expressed by your program.

Resource Provider. A binary used by the deployment engine to manage a resource

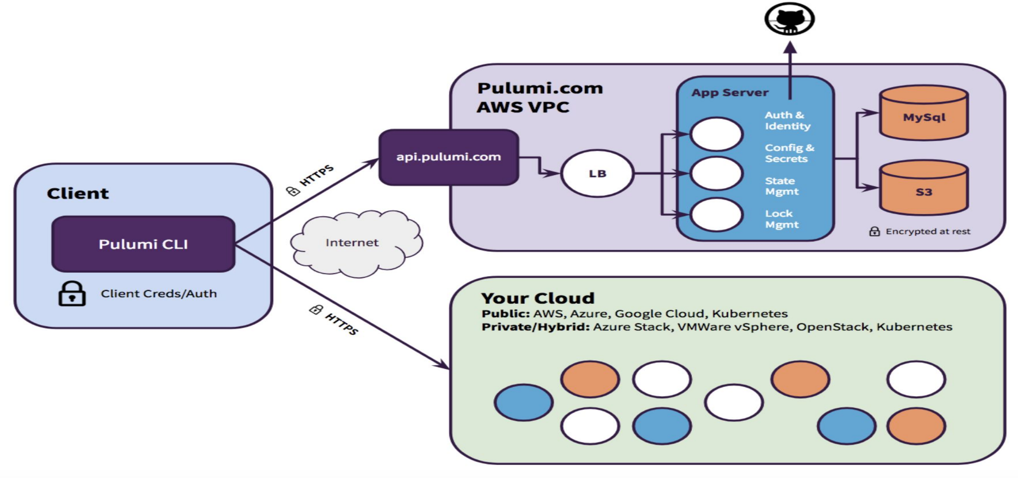


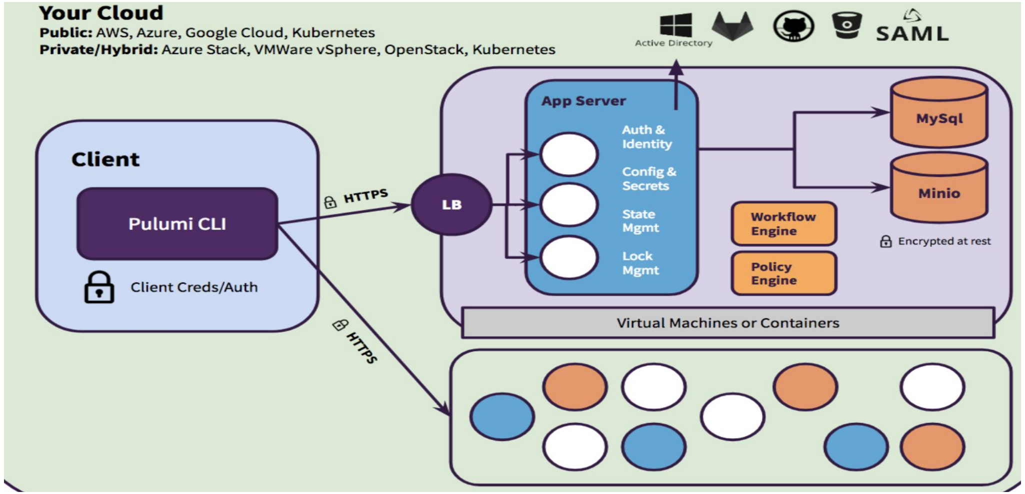
Pulumi Service Architecture

Deciding on State Backend

Pulumi supports two classes of state backends for storing your infrastructure state:

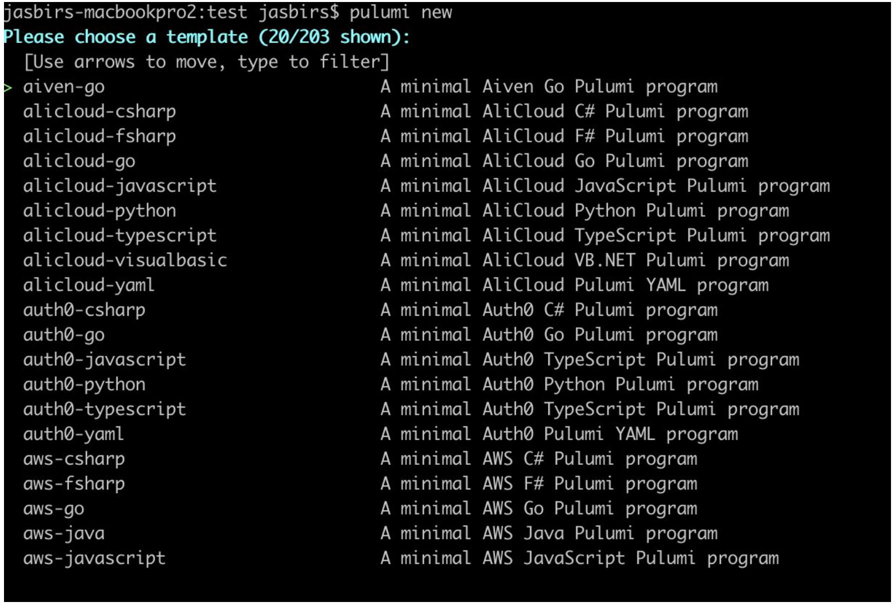
- **Service:** a managed cloud experience using the online or self-hosted Pulumi Service application
- **Self-Managed:** a manually managed object store, including AWS S3, Azure Blob Storage, Google Cloud Storage, any AWS S3 compatible server such as Minio or Ceph, or your local filesystem





Infrastructure as Code

- Starting fast with **templates** ($ pulumi new)

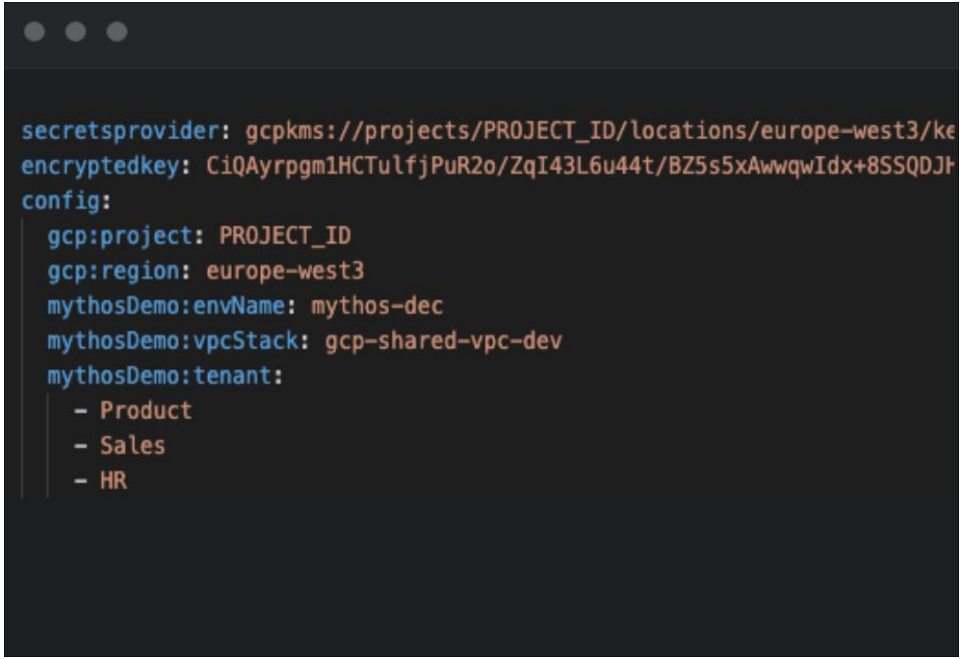


```
jasbirs-macbookpro2:test jasbirs$ pulumi new
Please choose a template (20/203 shown):
  [Use arrows to move, type to filter]
> aiven-go                           A minimal Aiven Go Pulumi program
  alicloud-csharp                    A minimal AliCloud C# Pulumi program
  alicloud-fsharp                    A minimal AliCloud F# Pulumi program
  alicloud-go                        A minimal AliCloud Go Pulumi program
  alicloud-javascript                A minimal AliCloud JavaScript Pulumi program
  alicloud-python                    A minimal AliCloud Python Pulumi program
  alicloud-typescript                A minimal AliCloud TypeScript Pulumi program
  alicloud-visualbasic               A minimal AliCloud VB.NET Pulumi program
  alicloud-yaml                      A minimal AliCloud Pulumi YAML program
  auth0-csharp                       A minimal Auth0 C# Pulumi program
  auth0-go                           A minimal Auth0 Go Pulumi program
  auth0-javascript                   A minimal Auth0 TypeScript Pulumi program
  auth0-python                       A minimal Auth0 Python Pulumi program
  auth0-typescript                   A minimal Auth0 TypeScript Pulumi program
  auth0-yaml                         A minimal Auth0 Pulumi YAML program
  aws-csharp                         A minimal AWS C# Pulumi program
  aws-fsharp                         A minimal AWS F# Pulumi program
  aws-go                             A minimal AWS Go Pulumi program
  aws-java                           A minimal AWS Java Pulumi program
  aws-javascript                     A minimal AWS JavaScript Pulumi program
```

Infrastructure as Code

- Starting fast with **templates** ($ pulumi new)
- **Configurations** for different **stacks**
  - config variables and secrets

    (Remote encryption with GCP KMS)
  - Required or Defaults
  - Reference other stacks - very powerful

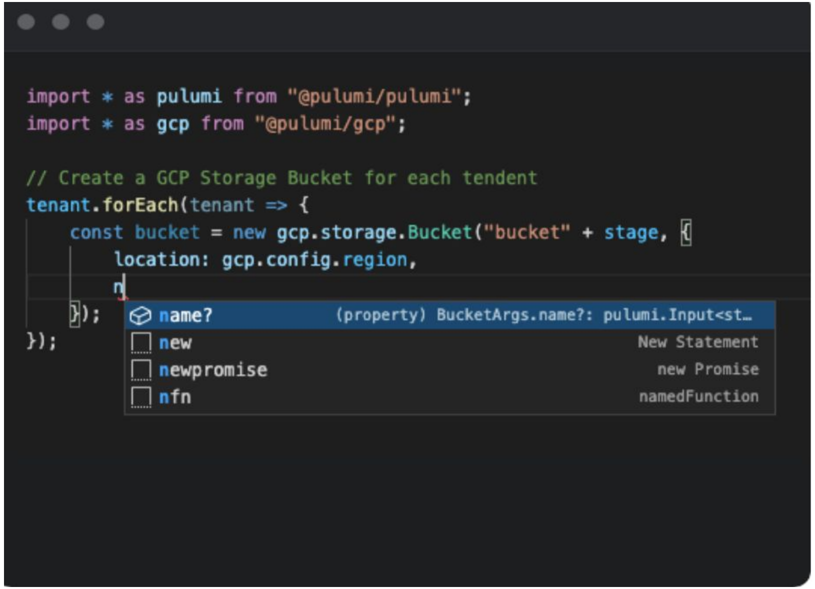


```yaml
secretsprovider: gcpkms://projects/PROJECT_ID/locations/europe-west3/ke
encryptedkey: CiQAyrpgm1HCTulfjPuR2o/ZqI43L6u44t/BZ5s5xAwwqwIdx+8SSQDJ
config:
  gcp:project: PROJECT_ID
  gcp:region: europe-west3
  mythosDemo:envName: mythos-dec
  mythosDemo:vpcStack: gcp-shared-vpc-dev
  mythosDemo:tenant:
    - Product
    - Sales
    - HR
```

Infrastructure as Code

- Starting fast with **templates** ($ pulumi new)
- **Configurations** for different stacks
  - config variables and secrets

    (Remote encryption with GCP KMS)
  - Required or Defaults
  - Reference other stacks - very powerful
- **Code** itself - index.ts, ...
  - create Stack outputs
  - ... and can import other stack's output!



```
import * as pulumi from "@pulumi/pulumi";
import * as gcp from "@pulumi/gcp";

// Create a GCP Storage Bucket for each tendent
tenant.forEach(tenant => {
    const bucket = new gcp.storage.Bucket("bucket" + stage, {
        location: gcp.config.region,
        n
    });
});
```

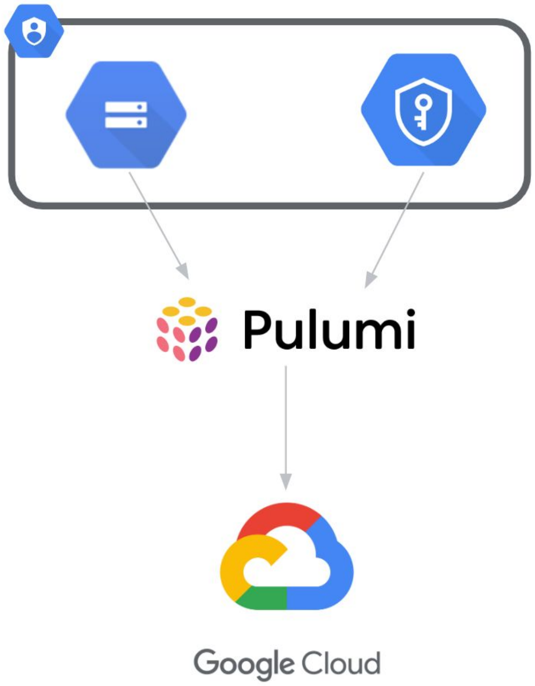
State Management

- free **Pulumi Service** for handling resource state
- **Local State** management possible - similar to TF
- **Remote State** - GCP Storage Bucket

- Select and login via CLI
  - $ **pulumi login** gs://pulumi-statebucket-mythos-dev

GCP - Remote Usage

- Initial local **Pulumi stack** to build the ‘Landing Zone’ for Pulumi
    - Remote State Bucket
    - Cloud KMS as Secret provider
    - Central point for Google Cloud API-Management
- Allows for **central permission handling** via GCP IAM



Demo Time

Q & A