# pûlumi

# Can TypeScript make infrastructure management easy?

Declare cloud infrastructure using real languages. Enable developers and operators to work better together.

Paul Stack (@stack72/paul@pulumi.com) Pulumi Engineer July 2020

### **Cloud Transition**





# What is Infrastructure as Code



- Eliminate manual error-prone provisioning and changes
- Bring software best practices to infrastructure management
- Gain visibility of changes through code reviews and previews

					_	
• • • • iii Create VPC   VPC Management	× +					
$\leftarrow$ $\rightarrow$ $C$ $\triangleq$ https://us-west-2.cons	sole.aws.amazon.com/vpc/home?reg	gion=us-west-2#Cr	eateVpc:VpcId=vpc-0	ea670 😭 🌘	:	
aws Services - Res	source Groups 🗸 🌗 EC2 🐧	cameron	istokes-pulumi 👻 Ori	egon 👻 Support 👻		
VPCs > Create VPC						
Create VPC						
A VPC is an isolated portion of the AWS cl for your VPC. Specify the IPv4 address rar IPv4 CIDR block larger than /16. You can c	oud populated by AWS objects, such nge as a Classless Inter-Domain Routi optionally associate an Amazon-provid	as Amazon EC2 insi ing (CIDR) block; for ded IPv6 CIDR block	tances. You must specif example, 10.0.0.0/16. Y with the VPC.	fy an IPv4 address ran ⁄ou cannot specify an	nge	
Name tag	main		0			
IBv4 CIDP block*	10.0.0.0/16		8			
IFV4 CIDA DICK	10.0.0/18		0			
Te	nort * as aws t	from "@pu	ılımi/aws"			
		epe		,		
V Feedback V English (US	<pre>Preedback @ English(US</pre>					
	tags: {					
	Name: "main", },					
	cidrBlock: "10.0.0.0/16",					
	assignGeneratedIpv6CidrBlock: false,					
	instanceTenancy: "default",					
}	});					
ex	xport const vpc	ra = vpc.	ια;			

# Why Infrastructure as Code

P

- Automated and repeatable deployments
- Decreased time-to-market for new applications and ongoing maintenance
- Safe predictable changes



### Modern Infrastructure as Code

#### CREATE

- Real languages
- Share and reuse abstractions
- Use your favorite tools (IDE, testing, etc)

#### DEPLOY

- Preview changes
- Flexible CLI for Dev and Ops familiarity
- Integrate into CI/CD workflows

#### MANAGE

- Audit all changes
- Managed complex environments
- Implement policies and controls

•••		indicuta — Infra	_	
	TS index.ts			
BANCRER OPENEDTORS (1) BANKRO INFRA I India India (1) India I India (1) India I Ind	Ti index.15 • Contentitude Ti index.15 • Jocontentitude 5 insport + as puter 6 insport + as puter 7 index.15 • Contentitude 7 // Create a buck 13 // Create a buck 13 // Create a buck 14 acti "public" 15 // How 33 · 16 errorbox 19 errorbox 20 } 21 desce	At if on "spolariyolatis"; restory if on 'Auskellientiny'; one; for a configerable location, m point(origi); to store add array of the static conten- et on a store add array to static conten- tion of the store add array to static conten- tion of the store add array to store add and store add array to store add and add and add and add array to store add and add add and add add add and add add add add add add add add and add add add add add add add add add add	t. ", ( te. This lly trans	
	24 // Upload the ent	tire directory contents to the S3 bucker		
🖟 joeduffyjtest_1* 🗢 🙁	2 🗛 0	Ln 21, Col 9 Spaces: 4 UTF-8 LF TypeSci	ript 3.5.2	⊕ ♠
		9 million		
Type           pulled:	ck ketDirectory Nois Pointy Reinfordstander Abinetton Reinfordstander this update? this update?	kan parter backet parter backet content parter backet parter	Plan create create create create create create create	S 🔮 O
o <b>ūlumi</b> "‱,				۹
adulfy / pulumity / pulumit-wafe-	pul-6-merze			
STACK ACTIVITY	RESOURCES FOULY	SETTINGS		
Update 31 persit/spatient 12 hours apr 22 Update Exceeded in a minute				C TXBA
CHANGES TIMELINE	CONFIGURATION			
Type         Non           Type         Non           • Meri (10) Robert         0.00000           • Nondel (10) Robert         0.00000           • Meri (10) Robert         0.00000	Quert200           -bccott         rundi           -placed/p-vol1-plc1-p-wrape rundi         rundi           -place-dplace-ruli         rundi			0

### Infrastructure as Code Software



#### Bring Software Development Practices to Infrastructure

Eliminate slow error-prone manual changes and bring automation and repeatability to infrastructure management.

Enforce best practices using abstractions and reuse -- no more copy and paste.

Use semantic versioning, testing, and code review development practices for all aspects of your cloud software.

•••	C C	Fix location in azure-ts-aks-mu × + GitHub, Inc. [US]   https://github.com/pulun	i/examples/commit/22173d4755cd45a3ef2e01866650887 🛠					
Fix loc	catio r (#197	n in azure-ts-aks-multicluster. (#19	7)					
🞐 clst	okes	committed on Dec 18, 2018 Verified	1 parent dffb7cf commit 22173d4755cd45a3ef2e01					
Showi	ng <mark>2 c</mark>	hanged files with 11 additions and 9 deletions.						
18	az	ure-ts-aks-multicluster/index.ts						
51िड		@@ -4,7 +4,7 @@ import * as azure from "@p	ulumi/azure";					
50	44	clientId: adApp.application	Id,					
51	45	clientSecret: adSpPassword.value,						
52	46	},						
	47	+ // Per-cluster config arguments						
	48	+ location: perClusterConfig.loca	tion,					
	49	+ agentPoolProfile: {						
	50	50 + name: "aksagentpool",						
	51	+ count: perClusterConfig.nodeCount,						
	52	+ vmSize: perClusterConfig.no	deSize,					
	53	+ },						
	54	+ dnsPrefix: `\${pulumi.getStack()	}-kube`,					
53	55	<i>}</i> );						
54	50	return cluster;						
55	27	31;						
283								

## Modern Infrastructure Frameworks

#### **BEST PRACTICES** FRAMEWORKS

Create modern cloud software using best practices.



CLOUDFLARE

### Deploy Code from/to Anywhere



P	•	View changes			
	pulu	mi bot left a	comment		+ 👜 🚥
	🦉 1 Res	The Update (p source Ch	oreview) for stack acmeco nanges	rp/website/production was successful.	
	+~~~	Name nginx gke-cluster	Type kubernetes:core/v1:Pod gcp:container:Cluster	Operation create update	

pûlumi						ø
pulumi / pulumi.io	/ pulumi.io-product	ion				
STACK	ACTIVITY	RESOLACES	WEB-IDOKS	SETTINGS		
Updates on April 8th,	2019					
Unders a	120 - Merge pull request optimet fil hours ago 🖉	#979 from pulumi/masa	r		es 69605 P prototion D 905	DETAILS
Updates on April 5th,	2019					
(polaret ber	119 - Merge pull request updated 4 days ago 🗸	#975 from pulur Amara	y.		o muse P resorter D sec	DETAILS
Updates on April 2nd,	2019					
	118 - Merge pull request	PRIS from outputstands	,		() #2784	

Туре	Name 🕇	Status
pulumi:providers:gcp	default	
<pre>gcp:container:Cluster</pre>	helloworld	S 🔕
pulumi:providers:kubernete	s helloworld	Open in Google Cloud console
kubernetes:core:Namespace	helloworld	
kubernetes:apps:Deployment	helloworld	(B) 2
kubernetes:core:Service	helloworld	🛞 Z

### **Resource Definitions**



# Define the final end state of your resources.

Use a consistent object model for all resource types without needing to know the underlying API operations needed to create and manage the resources.

Pulumi lets you define the final configuration state of your resources and knows the steps to get there.

#### •••

```
// define end state of resource configurations
import * as aws from "@pulumi/aws";
```

```
const size = "t2.micro"; // t2.micro machine type
const ami = "ami-7172b611"; // AMI for Amazon Linux in us-west-2 (Oregon)
```

```
// create a new security group for port 80
const group = new aws.ec2.SecurityGroup("web-secgrp", {
    ingress: [
        { protocol: "tcp", fromPort: 22, toPort: 22, cidrBlocks: ["0.0.0.0/0"] },
        { protocol: "tcp", fromPort: 80, toPort: 80, cidrBlocks: ["0.0.0.0/0"] },
    ],
});
```

```
// create a new security group for port 80
const server = new aws.ec2.Instance("web-server", {
    instanceType: size,
    vpcSecurityGroupIds: [group.id], // reference the group object above
    ami: ami,
    tags: { "Name": "web-server" },
});
```

```
export const publicIp = server.publicIp;
export const publicHostName = server.publicDns;
```

## **Conditionals and Loops**



#### Create Infrastructure Using Real Programming Features

The full functionality of programming languages brought to Infrastructure as Code.

Pulumi lets you program your infrastructure just like the rest of your applications with the expressiveness and flexibility of real programming languages.

In this example, we provision a VPC and public subnets <u>only</u> if we've defined CIDR blocks for them in our configuration.

#### •••

```
// Use real programming language features when defining infrastructure
import * as aws from "@pulumi/aws";
import * as pulumi from "@pulumi/pulumi";
```

```
const config = new pulumi.Config();
const vpcCidr = config.require("vpcCidr");
const publicSubnetCidrs = config.get("publicSubnetCidrs");
```

```
const vpc = new aws.ec2.Vpc("main", {
    cidrBlock: vpcCidr,
});
```

```
// Create Public Subnets _only_ if necessary
if (publicSubnetCidrs != null) {
```

```
// Loop over Public Subnets CIDR blocks
const publicSubnets = publicSubnetCidrs.split(",").map((cidr, i) => {
  return new aws.ec2.Subnet(`public-${i}`, {
    vpcId: vpc.id,
    cidrBlock: cidr,
    mapPublicIpOnLaunch: true,
  });
});
```

## Multi-Provider Workflows



#### Mix Kubernetes, Cloud, and Custom Resources

A consistent programming model, tools, and workflow for deploying and managing IaaS, PaaS, SaaS, and custom resources.

Pulumi makes it possible to declare and manage resources for multiple infrastructure services in a single Pulumi application.

In this example, we provision an AWS S3 bucket and use it with a Kubernetes cluster.

#### •••

});

```
// Use an AWS S3 bucket from Kubernetes
import * as aws from "@pulumi/aws";
import * as k8s from "@pulumi/kubernetes";
```

```
const appName = "nginx";
```

```
// nginx config stored in an S3 bucket.
const bucket = new aws.s3.Bucket(`${appName}-config`);
```

```
// nginx container, replicated 1 time
const appLabels = { app: appName };
const nginx = new k8s.apps.v1.Deployment(appName, {
  spec: {
    selector: { matchLabels: appLabels },
    replicas: 1,
    template: {
      metadata: { labels: appLabels },
      spec: {
         initContainers: [nginxConfigPuller(bucket.bucketDomainName)],
         containers: [{ name: appName, image: "nginx:1.15-alpine" }],
      },
      },
    },
```

# Reusability



#### Build and Share Reusable Components

Compose resources into an architecture that fits your company's requirements and then share that across teams.

Pulumi applications are real software projects that can be re-distributed through typical package managers.

In this example, we provision a Jenkins cluster from a module from our internal software repository.

#### •••

```
// Create a Jenkins cluster from a shared Jenkins module
import * as pulumi from "@pulumi/pulumi";
import * as jenkins from "@internal/jenkins";
```

```
// Load stack configuration
const config = new pulumi.Config("jenkins");
```

```
// Create our Jenkins cluster using our internal jenkins module
const instance = new jenkins.Cluster("jenkins", {
    name: "jenkins",
    credentials: {
        username: config.require("username"),
        password: config.require("password"),
    },
    resources: {
        memory: "512Mi",
        cpu: "100m",
    },
});
```

### **Advanced Orchestration**



#### Enable Advanced DevOps Strategies

Incorporate data from monitoring services into deployment procedures.

#### Pulumi enables previously difficult or impossible deployment scenarios for real-world Kubernetes environments.

In this example, we check Prometheus for healthy metrics before proceeding to deploy to our Production cluster.

#### •••

```
// Canary cluster with 3 replicas of our app.
import * as k8s from "@pulumi/kubernetes";
import * as p8s from "./p8s";
```

```
// Create canary deployment
const canary = new k8s.apps.v1.Deployment("app-canary", {
   spec: {
     selector: { matchLabels: appPodTemplate.metadata.labels },
     replicas: 3,
     template: appPodTemplate
   },
```

```
});
```

});

```
// Check Prometheus app metrics before rolling forward with prod deployment.
const check = p8s.checkAppMetrics(canary);
```

```
// Production cluster with 10 replicas of our app
const prod = new k8s.apps.v1.Deployment("app", {
    metadata: { annotations: { metricsChecked: check } },
    spec: {
        selector: { matchLabels: appPodTemplate.metadata.labels },
        replicas: 10,
        template: appPodTemplate
    },
```

### Test Driven Infrastructure



# Use familiar frameworks and techniques to test infrastructure

No need to master a new set of tools -- reuse what you and your team already knows.

Teams can perform unit, integration, and runtime testing, fully integrated into your development and CI/CD workflows.



#### Secrets Management

Built-in encrypted secrets management and configuration.

\$ pulumi config set --secret dbPassword 2u%^JAEf\*L6.?2}G

**Easy to store and use** deployment-time secrets safely.

**Strong encryption for all state**, ensuring secrets won't leak.

Use built-in Pulumi KMS, or choose seamless integration from leading providers.













# Demo time!

Let's program the cloud!

# In Conclusion

The Easiest Way to Program the Cloud

# Thank You

#### https://www.pulumi.com/

- 🔀 paul@pulumi.com
- 9 @Stack72