ArgoCon

NORTH AMERICA

Bridge the Gap Between Terraform and GitOps

Alexander Matyushentsev & Junze Bao, Akuity

Introductions

November 12, 2024
Salt Lake City

Alexander Matyushentsev
Chief Software Architect
Argo CD Lead
Akuity

Junze Bao
Site Reliability Engineer
Akuity

# Agenda

- Infrastructure beyond Kubernetes
- Terraform/Tofu use cases
- Terraform/Tofu Development Workflow
- Gap between Terraform and GitOps
- Introducing tf-bridge
- Demo!

# Infrastructure beyond Kubernetes

- Kubernetes is a universal orchestrator
- Organizations are still using IaC
- Chicken and Egg problem: what provision K8S cluster
- Some core infrastructure should not be reconciled continuously (like VPC/Database)
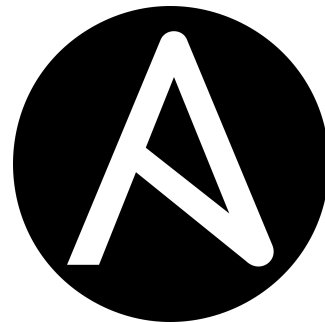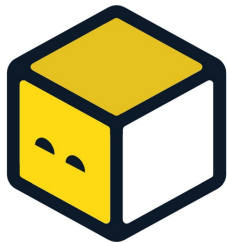
Terraform/Tofu Development Workflow

- Still Infrastructure As Code
- PR Based
- Every change is critical
- Does not need continuous reconciliation loop
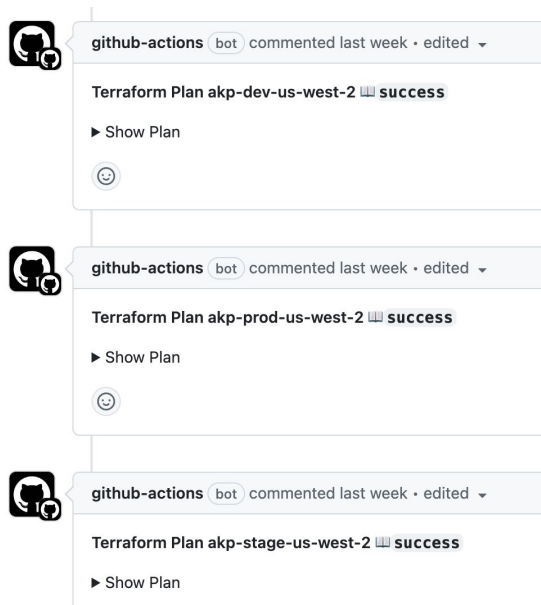
We don't think we should re-invent developers workflow

Gaps between Terraform and GitOps

Terraform outputs are used in K8S manifests

- Generated role ARN
- Database hostnames, availability zones

Orchestrate complex deployment process

https://github.com/argoproj/argo-cd/issues/1786

https://github.com/argoproj/argo-cd/issues/12060

Introducing TF Bridge

https://tf-bridge.akuity.io/

A Kubernetes controller that streamlines Terraform usage along side with GitOps tools.
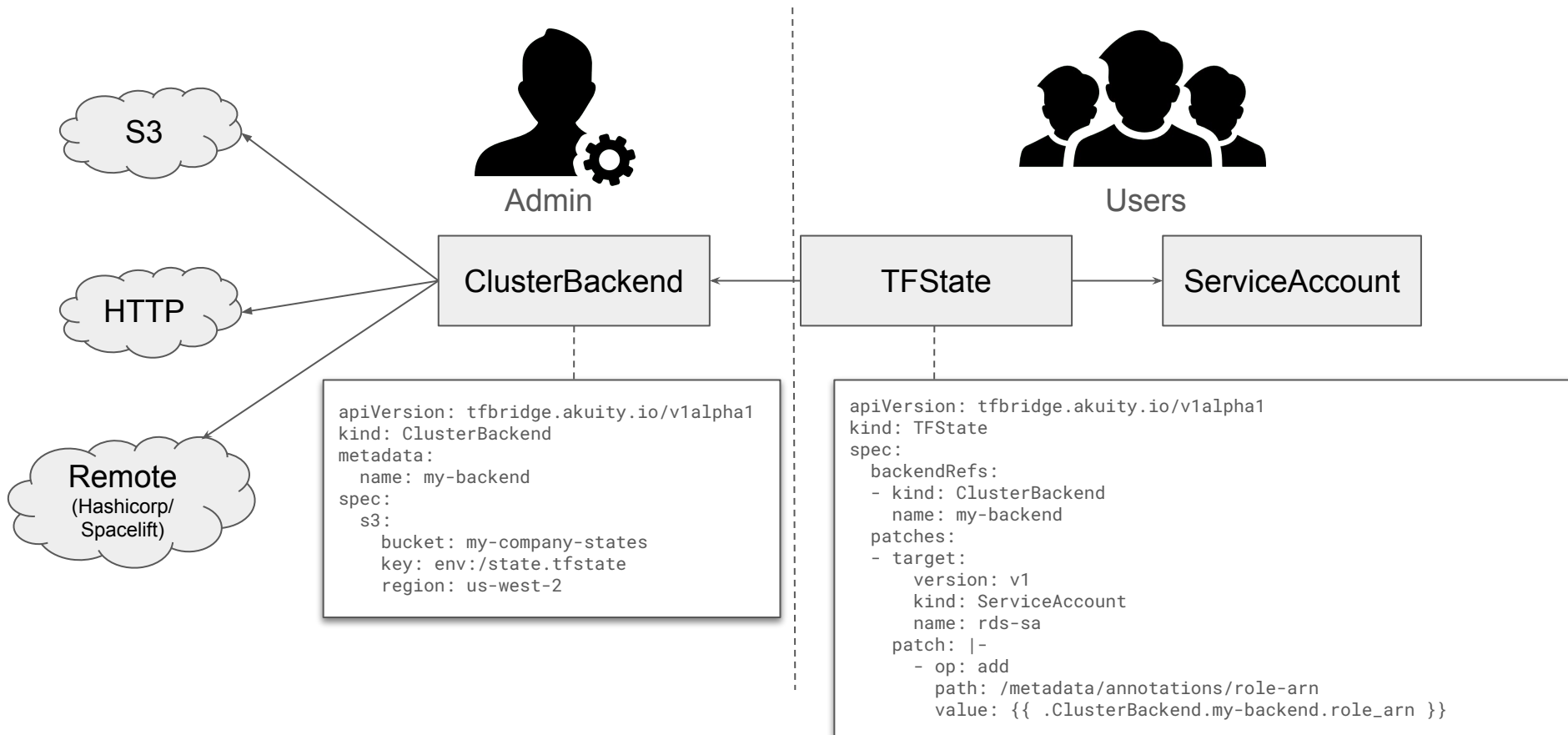
✅ **Goals**

- Continuously monitors state produced by *terraform apply*
- Inject specified terraform outputs into the Kubernetes resources

❌ **Non Goals**

- Does not perform terraform state management
- Does not automate *terraform apply / terraform diff*

TF Bridge Architecture

S3

HTTP

Remote
(Hashicorp/
Spacelift)

Admin

ClusterBackend

Users

TFState → ServiceAccount

```
apiVersion: tfbridge.akuity.io/v1alpha1
kind: ClusterBackend
metadata:
  name: my-backend
spec:
  s3:
    bucket: my-company-states
    key: env:/state.tfstate
    region: us-west-2
```

```
apiVersion: tfbridge.akuity.io/v1alpha1
kind: TFState
spec:
  backendRefs:
  - kind: ClusterBackend
    name: my-backend
  patches:
  - target:
      version: v1
      kind: ServiceAccount
      name: rds-sa
    patch: |-
      - op: add
        path: /metadata/annotations/role-arn
        value: {{ .ClusterBackend.my-backend.role_arn }}
```

Use-Cases

- Ephemeral environment with database
  - Inject auto-generated CName
- Reduce cross availability zone (AZ) traffic
  - Inject DB AZ into deployment spec
- AWS IAM role for service accounts
  - Inject generated IAM role ARN to service account annotations
- Configure list of allowed IPs
  - Inject NAT IPs to ingress configuration

DEMO!

Thank you!

Please give us feedback at https://akuity.community/