KubeCon | CloudNativeCon
North America 2024

Zero Downtime Upgrades at Scale: How Okta Manages Hundreds of Clusters Daily

Jérémy Albuixech & Kahou Lei, Okta

© Okta and/or its affiliates. All rights reserved.

okta

Agenda

- Context and Challenges
- Platform Introduction
- Solutions
- Outcome and Results
- Q&A

© Okta and/or its affiliates. All rights reserved.

CIC Platform’s Global Presence & Data Residency

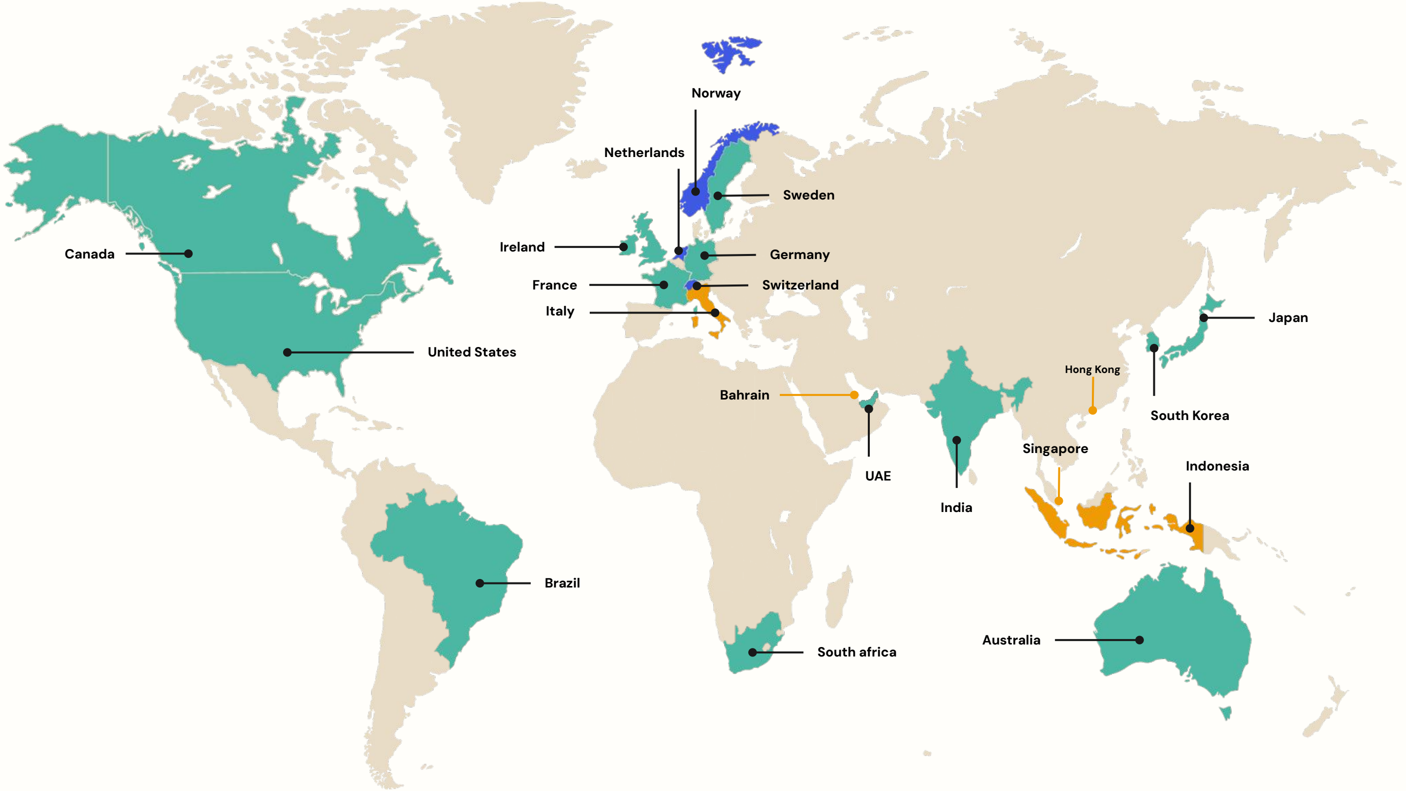
Public cloud:

9 multi-subscriber environments:
US, EU, JP, AUS, UK, CA, UAE

Private cloud:

Hundreds of single-subscriber environments

● AWS & Azure
● Azure only
● AWS only



© Okta and/or its affiliates. All rights reserved.

Management Challenges

- Hundreds of Environments
- Globally Distributed
- Daily Deployment
- Environment Variations (sizing, stacks, etc)
- Multi-cloud (AWS and Azure)
- Constant Security Update

© Okta and/or its affiliates. All rights reserved.

okta

The World's Identity Company

Platform Introduction

© Okta and/or its affiliates. All rights reserved.

Converged Platform

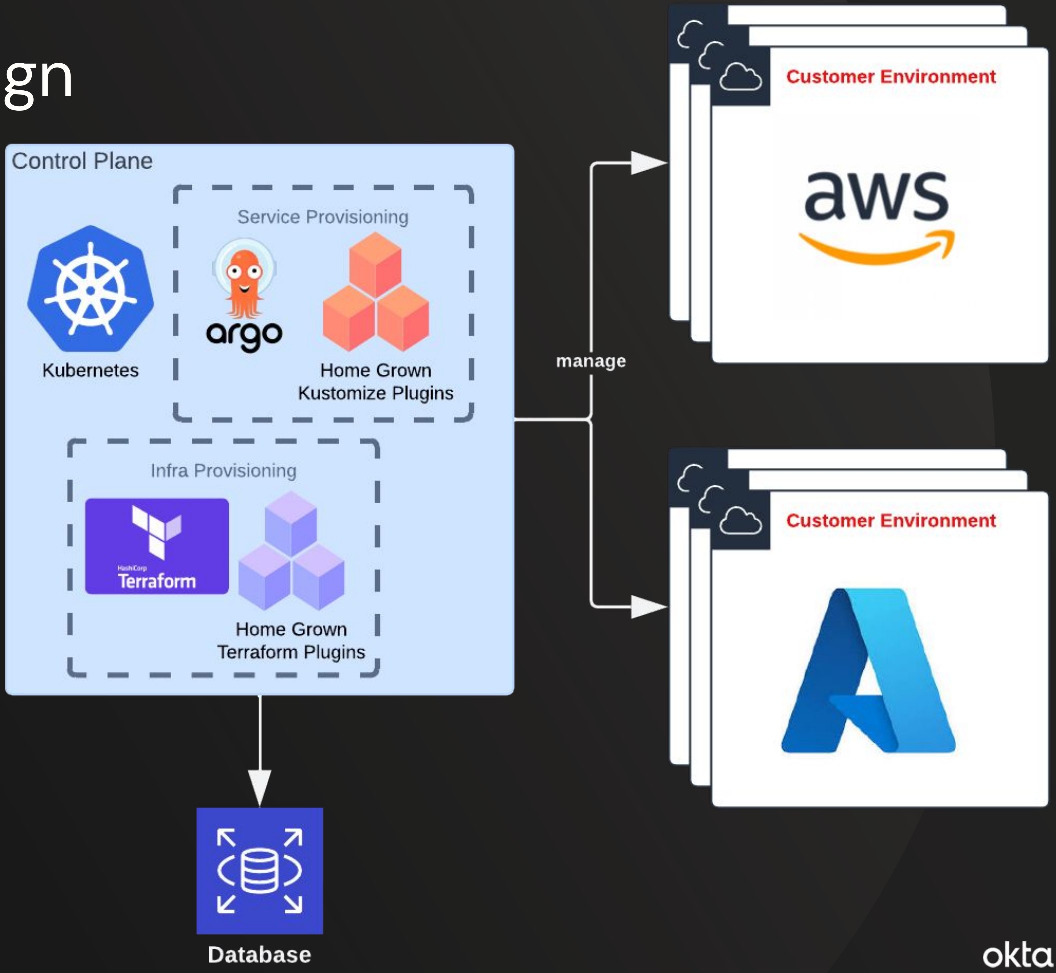
The convergence of multiple disparate customer offerings into a unified, modern, automated, scalable and built-for-the-future platform that runs Auth0 / Okta CIC product and more.

Multi-cloud	**Container Orchestrated**	**Stateless**
Immutable	**Fully Automated**	**Leveraging GitOps**

© Okta and/or its affiliates. All rights reserved.

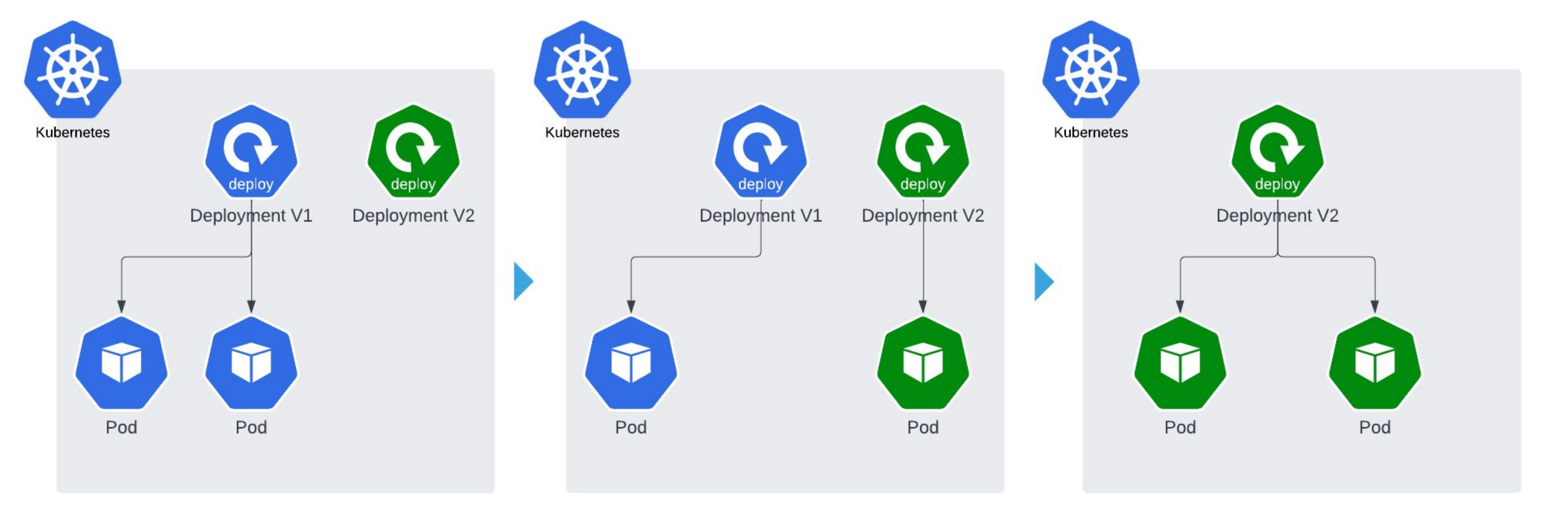
Platform High Level Design

- Customer Infra + Auth0 stack + Custom Config/Secret = **Customer Environment**
- Terraform + Plugins provision Infra
- ArgoCD + Plugins provision Auth0 stack
- Argo Workflow orchestrates deployments



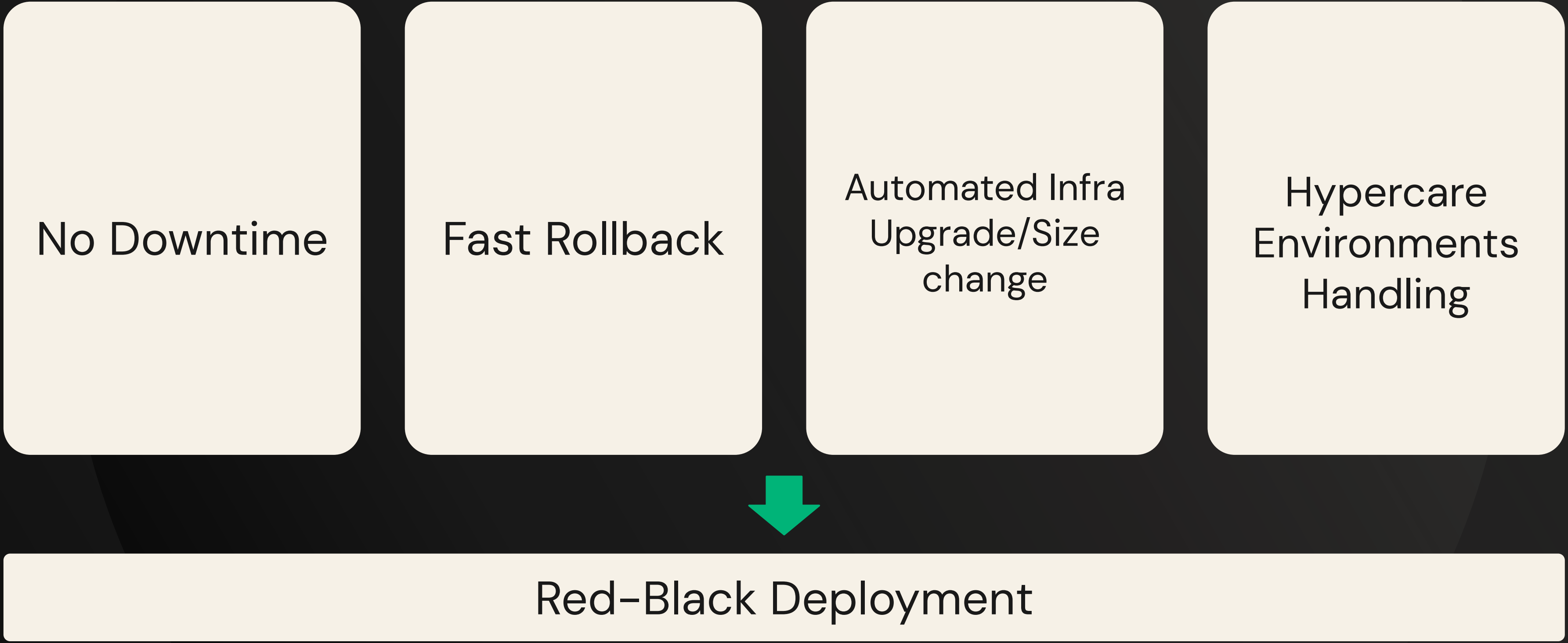
© Okta and/or its affiliates. All rights reserved.

Traditional Deployment (Rolling Deployment)



© Okta and/or its affiliates. All rights reserved.

Deployment requirements



No Downtime

Fast Rollback

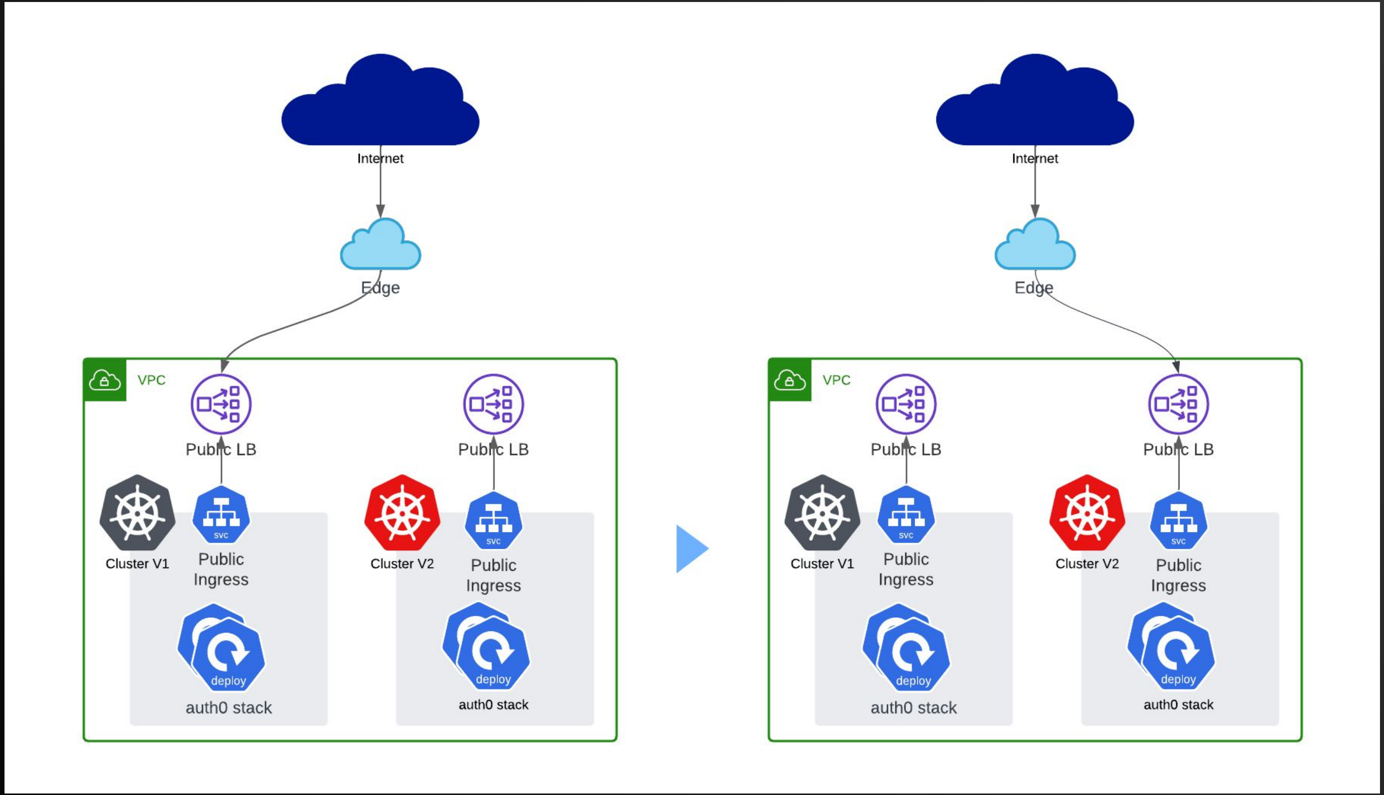
Automated Infra Upgrade/Size change

Hypercare Environments Handling

Red-Black Deployment

© Okta and/or its affiliates. All rights reserved.

What is Red-Black Deployment?



© Okta and/or its affiliates. All rights reserved.

Red-Black Deployment = 100% Automated + No Downtime

Well thought Control Plane Data Model

Consistent Release Pipeline and Definition

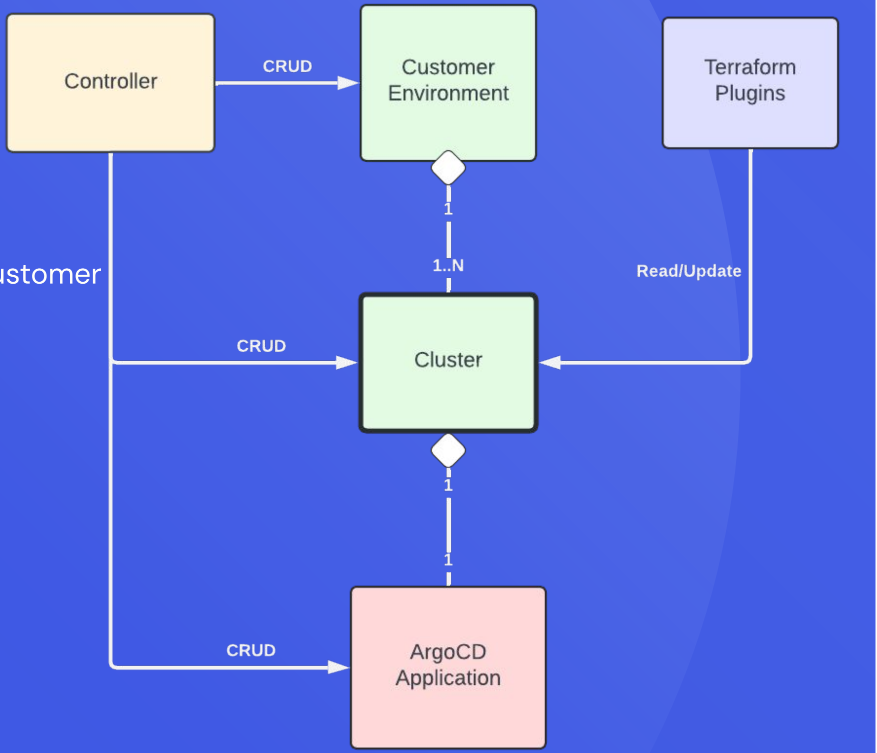
Secret and Config Management

Fine control of workflow orchestration

© Okta and/or its affiliates. All rights reserved.

How do we automate it?

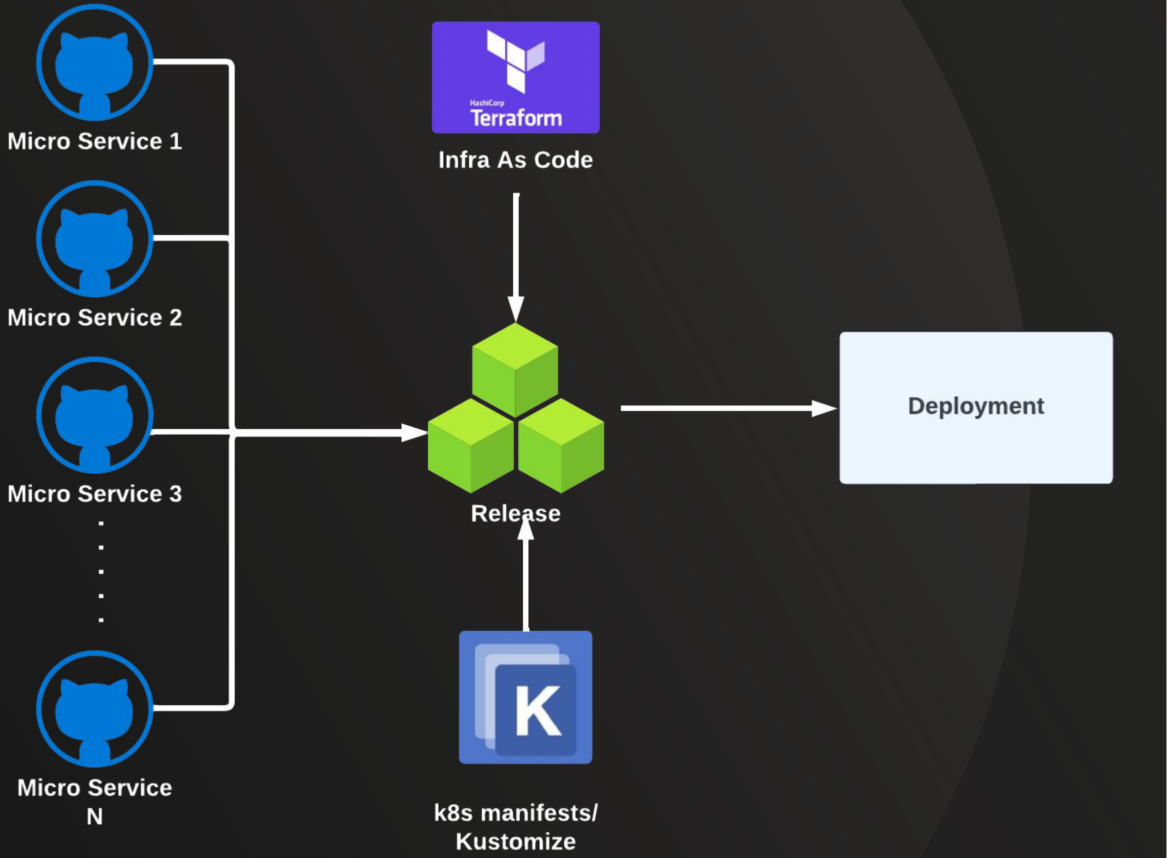
- Abstract the Kubernetes Cluster as a Cluster Object
- Each Cluster Object has an Identification (Cluster ID)
- Control creates the objects on the fly
- Home grown Terraform plugin to manage CRUD operations on all customer environment resources
- One Cluster Object = One ArgoCD application



© Okta and/or its affiliates. All rights reserved.

Release/Release Manifest

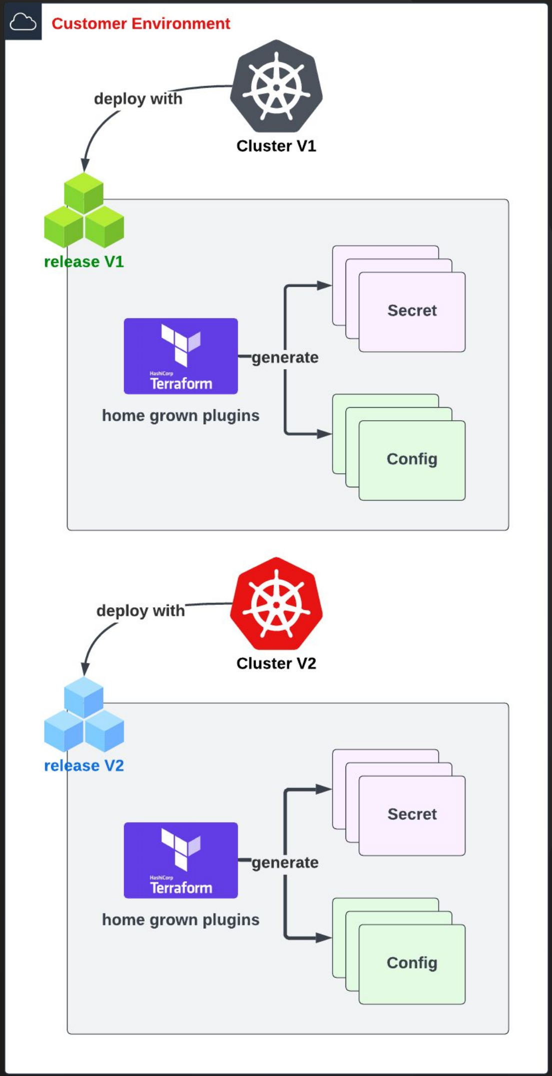
- Complete description of the release:
  - Microservices versions
  - Infrastructure change
  - Resources k8s
    Manifest/Kustomize Change
- Deployment must target one release
- Different environments have different releases



© Okta and/or its affiliates. All rights reserved.

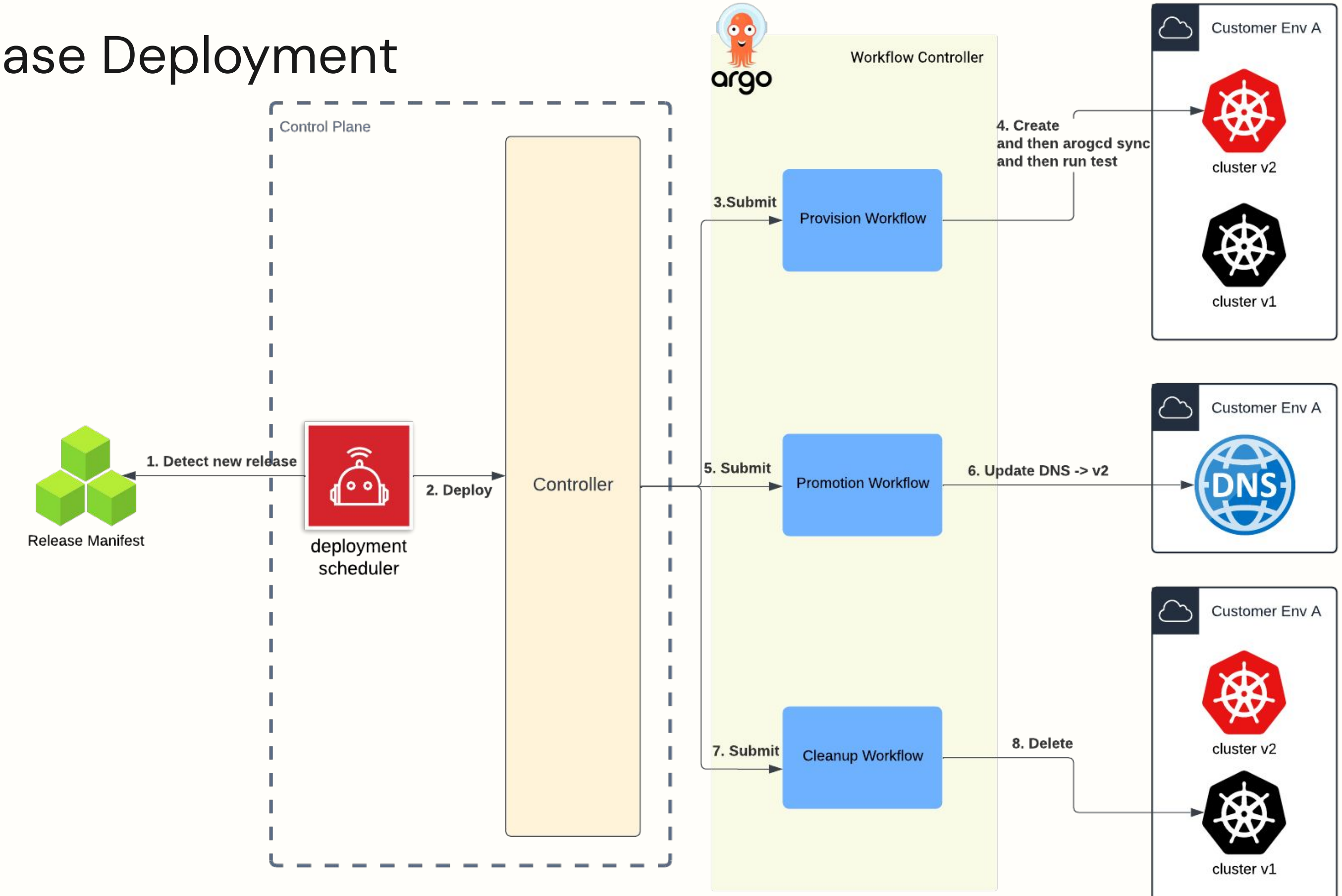
Secrets and Configs Management

- Secrets and Configs are generated by home grown Terraform plugins
- “Snapshot” the secrets and configs per release, per customer
- Old and new clusters own different version of snapshots
- Crucial part of no downtime deployment



© Okta and/or its affiliates. All rights reserved.

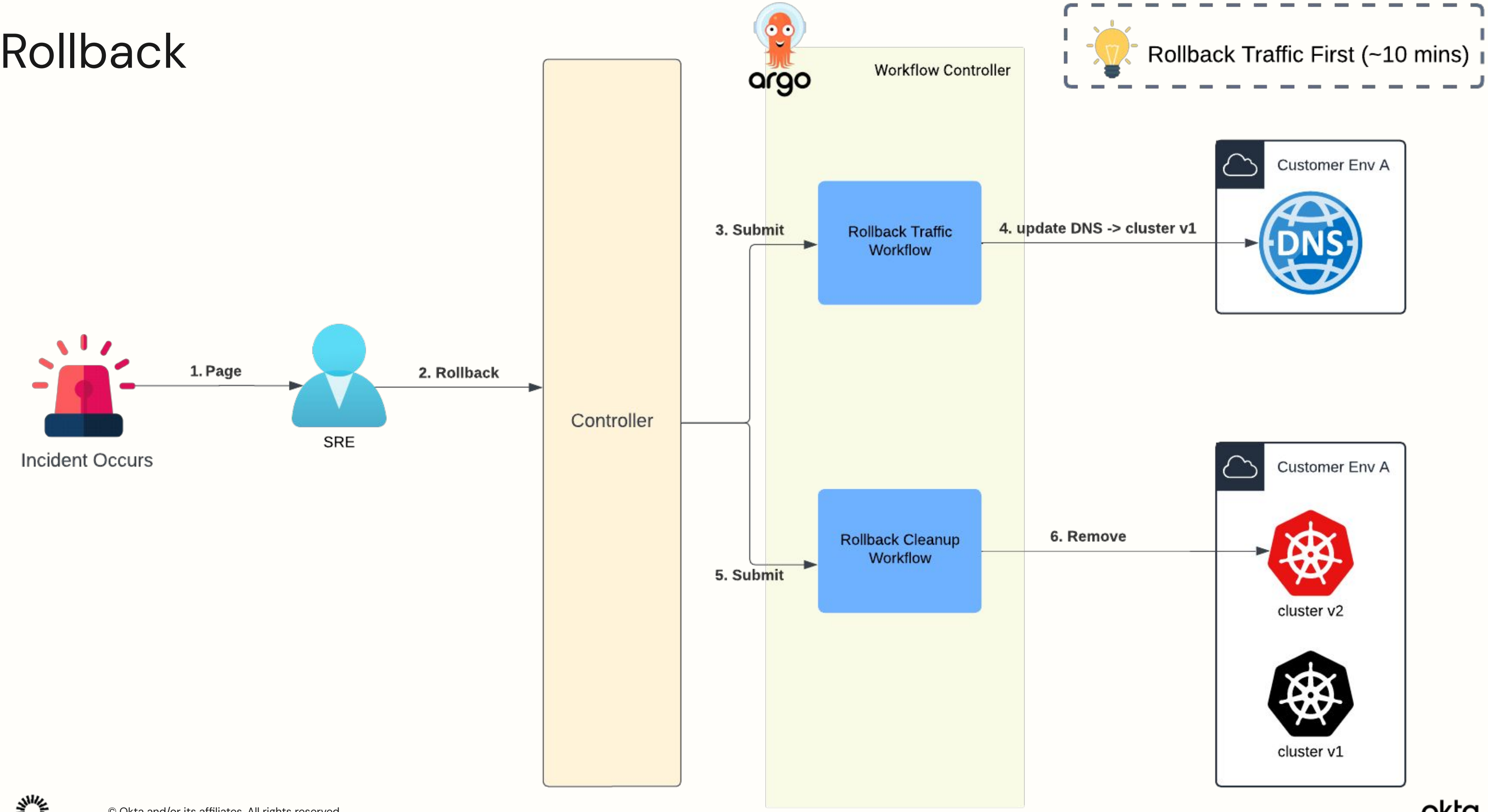
New Release Deployment



Workflows are Idempotent

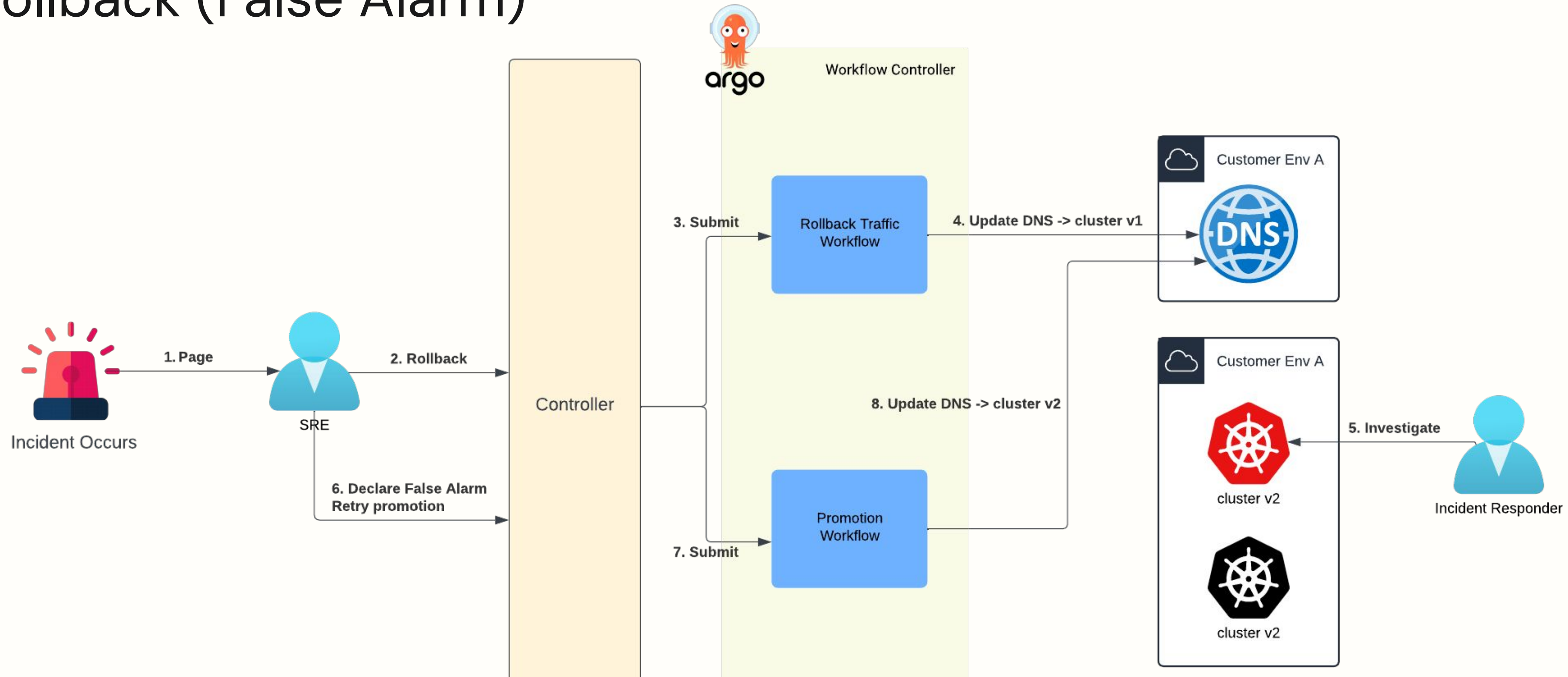
© Okta and/or its affiliates. All rights reserved.

Rollback



© Okta and/or its affiliates. All rights reserved.

Rollback (False Alarm)



Flexibility to re-promote Traffic

© Okta and/or its affiliates. All rights reserved.

Sounds easy? Not Quite…

Need to consider:

- Enough capacity after DNS switch
- No data loss - Poll old cluster idleness
- Singleton services
- Components need to be stateless

Also, there are several extra requirements:

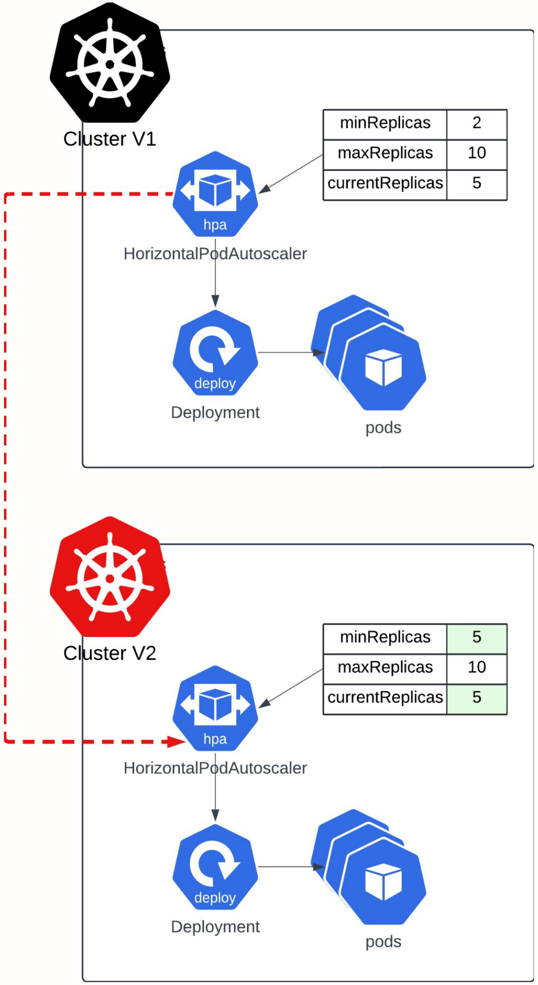
- Canary Traffic Routing (Traffic Segmentation)
- Cluster Overlapping Period
- No downtime secret rotation

© Okta and/or its affiliates. All rights reserved.

Ensure enough capacity in new cluster

Old Cluster is serving live traffic during deployment

1. Old Cluster workloads replicas => New Cluster workloads replicas and min replicas
2. Reset New Cluster workloads replicas when deployment is finished



Cluster V1

minReplicas	2
maxReplicas	10
currentReplicas	5

Cluster V2

minReplicas	5
maxReplicas	10
currentReplicas	5

© Okta and/or its affiliates. All rights reserved.

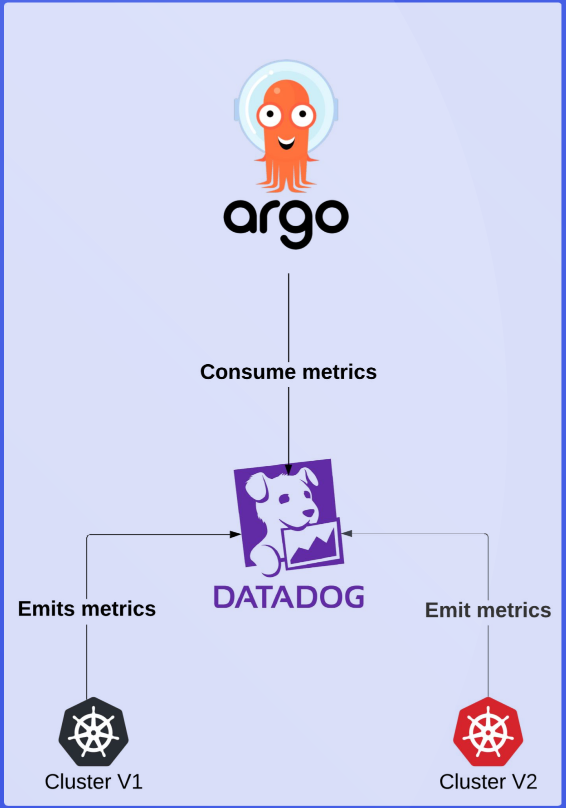
No Data Loss

Before switching the traffic, we need to ensure:

- All tasks are completed on the black cluster.
- New cluster is ready to accept connections.

How?

- Metrics polling step in workflow.
- DNS promotion depends on it.



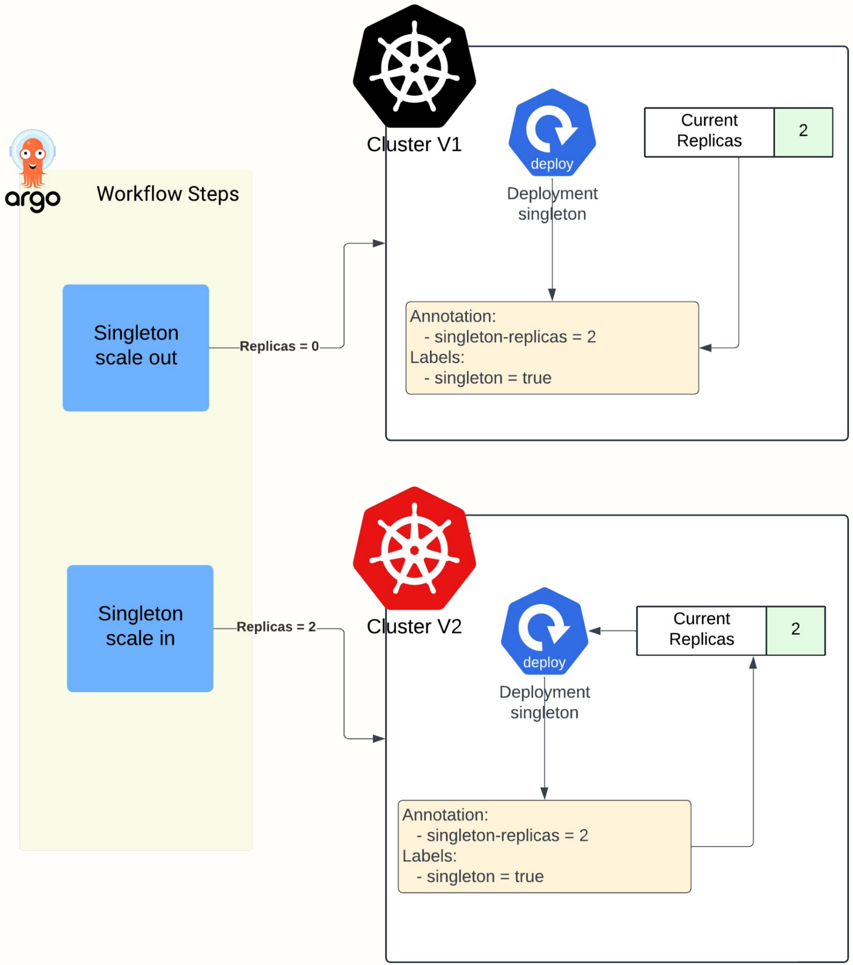
© Okta and/or its affiliates. All rights reserved.

Singleton services

Some legacy services cannot run in two clusters at the same time.

Solution

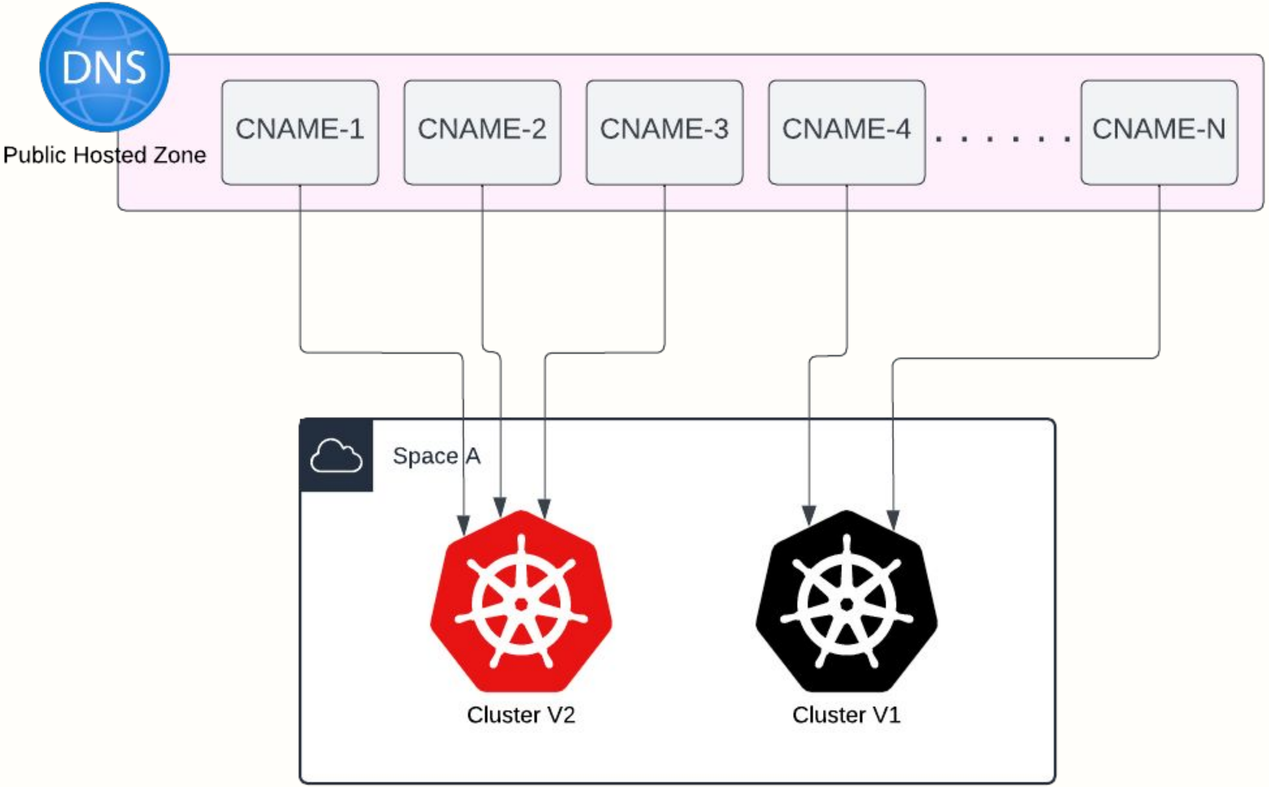
- Kubernetes labels to identify them
- Annotation to keep track of replicas count
- Workflow step to handle scaling



© Okta and/or its affiliates. All rights reserved.

Canary Traffic Routing (Traffic Segmentation)

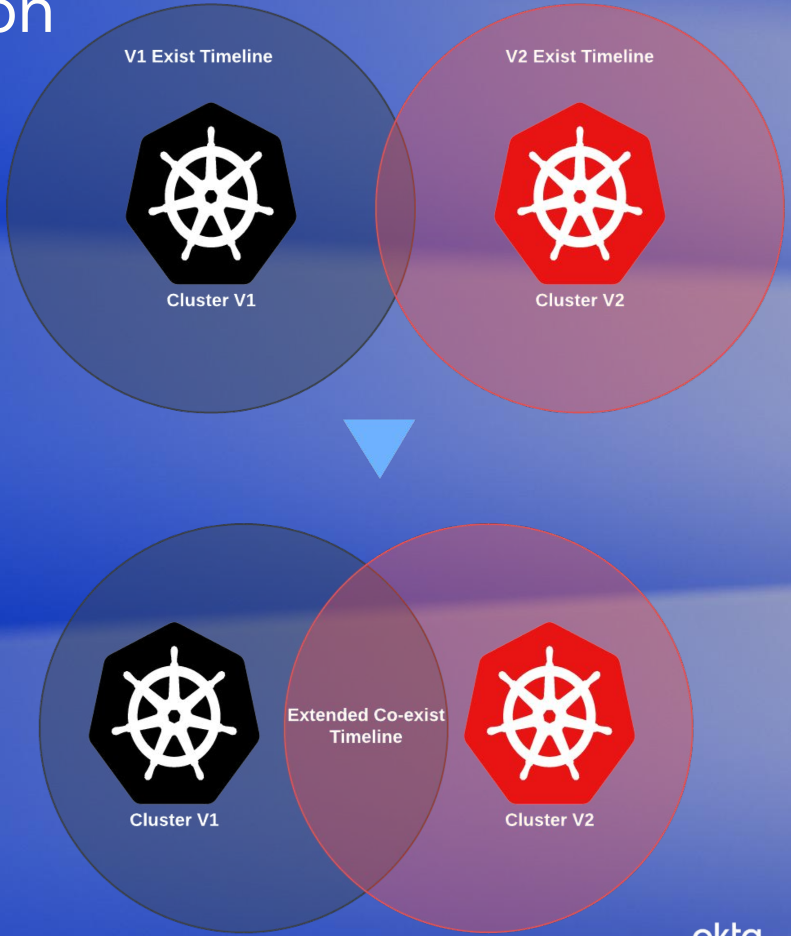
- Switch 1 Record at a time
- Happy Path – ~ 2 Hours
- Incident - Bulk Record Update



© Okta and/or its affiliates. All rights reserved.

Extend Cluster Overlapping Duration

- In normal use case, old cluster is deleted after DNS is switched.
- Delay Old Cluster Deletion to allow us to rollback quickly
- Overlapped for weeks in special occasions
- Less overlapped time -> less cost
- More overlapped time -> faster recovery



© Okta and/or its affiliates. All rights reserved.

Observability & alerting

- Instrumentation of our workflows
- Instrumentation of our control-plane
- Leverage argo workflows built-in metrics.

All these go into dashboards and are used for alerting purposes.

© Okta and/or its affiliates. All rights reserved.

Outcome / Results

© Okta and/or its affiliates. All rights reserved.

Improved security posture

No more friction when:

- Updating nodes images & Kubernetes versions
- Updating cluster components and services

Safety net

Safeguard against global & third party services outages.

One recent example being the Azure central-us/Crowdstrike outage in July 2024.

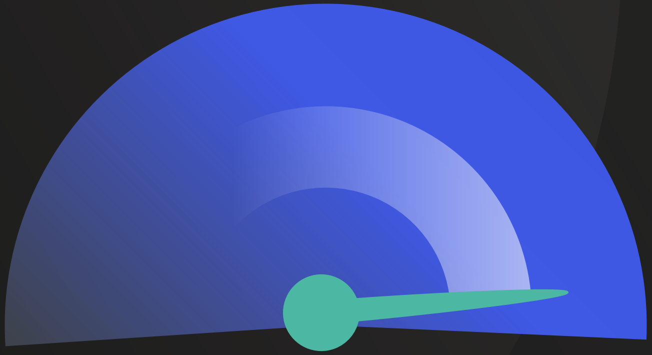
© Okta and/or its affiliates. All rights reserved.

Numbers & more

- Wide range of cluster’s sizes
  - From 2 nodes SPOT instances
  - To more than 250 nodes and 3500 vCPUs
  - ~ 2 Millions Kubernetes resources

High velocity

- >100 releases a day, moving fast with high confidence.
- Peace of mind when troubleshooting issues: no need to hotfix or manually operate on the cluster.



© Okta and/or its affiliates. All rights reserved.

Red-Black vs Rolling deployments

- Default is Red-Black
- Still keep rolling deployment for:
    - Time sensitive hotfixes
    - Minor Microservices patches
    - Bulk deployments patch version during an incident

© Okta and/or its affiliates. All rights reserved.

Q&A

© Okta and/or its affiliates. All rights reserved.

Thank You!

© Okta and/or its affiliates. All rights reserved.