

# Coordinating multiple environments with Flux and Kustomizations

Filip Milichovsky

Software Engineer  
Portworx Data Services, Pure Storage

# Overview

“The Plan”

1. Rolling out changes with Flux
2. Structuring configuration for multiple environments
3. Getting visibility into projected changes





# Intro

# What we do

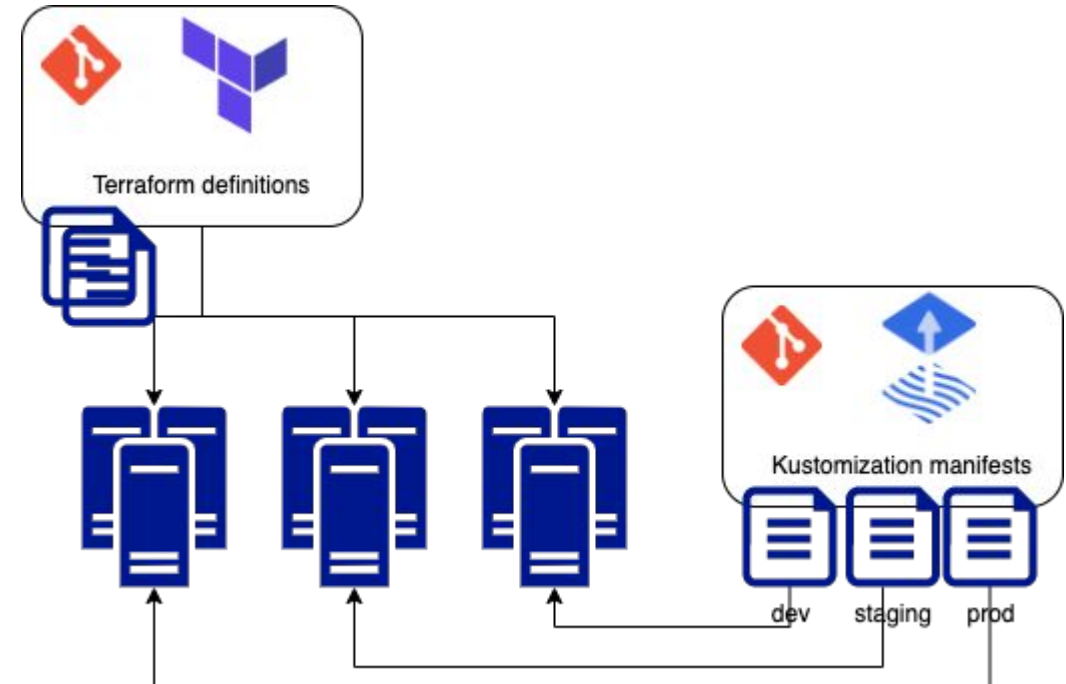
- SaaS platform for stateful application management on Kubernetes
- Users attach their cluster to our control plane fleet
- Self-sufficient team with our own infra
- **20-30** active clusters
- **5-6** cluster subtypes (release stages, development flavors)



# How it runs

Structure of our infrastructure

- Terraform-defined system-level infra
- Flux-defined cluster internals
- Multiple overlay profiles to differentiate stages and cluster types



# Core principles

1. Clusters are cattle
  - Don't get attached
2. Self-contained definitions, repeatability
  - Keep it simple
  - Avoid configuration leaks
3. Everything is codified
  - Avoid manual intervention (outside of incidents)



# Change rollout with Flux

# Letting Git and Flux do the work

- Cluster state determined by root kustomization + branch
- Git operations lead to auto-reconciliation of affected profiles
- Kustomizations - persistent differences between environments
- Branches - Intrinsic time delay in propagation of changes





# Environment separation

Kustomization structure

# Structural concepts

- **Bases** define standalone manifests, main building blocks
- **Components** extract small, focused, reusable aspects - patches focused on a limited subset of fields
- **Overlays** combine base resources, can pick and choose components and apply their own targeted patches (e.g. resource/replica overrides)
- **Profiles** package overlays into Flux-specific semantics (Flux kustomizations)



# Simplified directory tree

```
.
├── apps
│   ├── base
│   │   ├── api-server
│   │   ├── ingress
│   │   └── ui
│   ├── components
│   │   ├── api-profiler
│   │   └── ingress-permissive-cors
│   └── overlays
│       ├── development
│       ├── development-light
│       ├── staging
│       └── production
└── profiles # Flux kustomizations
    ├── development
    ├── development-light
    ├── production
    └── staging
```

```
# overlays/development/kustomization.yaml
apiVersion: kustomize.config.k8s.io/v1beta1
kind: Kustomization
resources:
- ../../base/api-server
- ../../base/api-workers
- ../../base/ingress
- ../../base/ui
- ../../base/teleport
- ../../base/observability

components:
- ../../components/api-profiler
```



# Change transparency


Making sense of the structure

# Environment promotions


Visibility into changes

- Promotions are git operations - fast-forward merges
- Infrastructural changes - local git log
- Changes in component (service) versions - git logs from their respective repos
- ⇒ Collect into PR descriptions

## Promote build-1037 #935

 Merged pdsgithubautom... merged 18 commits into [staging](#) from [release/master-staging-c9474069b5a19108d7183c5fb69dffd21f6](#)

Conversation 12 Commits 18 Checks 20 Files changed 59

 **github-actions** [bot] commented yesterday

@wynxel is promoting `master` to `staging`. Component changelogs:

**portworx/pds-infra:**

- [d1d584b](#) - Bump build number to build-1037 (github-actions)
- [c947406](#) - Promote ci to master ([🔗 Promote ci to master #934](#)) (github-actions[bot])
- [b0f8ecd](#) - [DS-4910](#): pds-system:maas-controller restrictive standard compliance ([🔗 DS-4910: pds-system:maas-controller restrictive standard compliance #878](#)) (Dávid Szakállas)
- [0797b1b](#) - [PWX-30046](#): added env varible for teleport kube proxy in maas deployment specs ([🔗 PWX-30046: added env varible for teleport kube proxy in maas deployment specs #927](#)) (vipin-kumar01)
- [f70454d](#) - [DS-4781](#): Add aws load balancer controller ([🔗 DS-4781: Add aws load balancer controller #909](#)) (Vladimir Aznauryan)
- [74192b9](#) - [DS-4910](#): teleport restrictive standard compliance ([🔗 DS-4910: teleport restrictive standard compliance #887](#)) (Dávid Szakállas)
- [eaf4421](#) - [DS-4918](#): datadog more restrictive security context ([🔗 DS-4918: datadog more restrictive security context #919](#)) (Dávid Szakállas)
- [eff97ea](#) - [DS-5103](#) - Fix For Unprivileged Port Binding ([🔗 DS-5103 - Fix For Unprivileged Port Binding #917](#)) (ismail onur kaya)
- [dbba3a0](#) - [DS-4936](#): Non-root teleport ([🔗 DS-4936: Non-root teleport #926](#)) (Eldar Urmanov)
- [5115139](#) - [DS-5106](#): updated teleport TTL timeout for maas ([🔗 DS-5106: updated teleport TTL timeout for maas #920](#)) (vipin-kumar01)

**portworx/pds-api-workers:**

- [12d5227a](#) - [DS-5094](#): Fix DeleteBackupJob parameters bug ([🔗 DS-5094: Fix DeleteBackupJob parameters bug pds-api-workers#189](#)) (Patrick Everitt)
- [fb28d291](#) - [DS-4825](#): use cache client provider in api-worker ([🔗 DS-4825: use cache client provider in api-worker pds-api-workers#190](#)) (Eldar Urmanov)

**portworx/pds-ui:**


- [d4e3ff4](#) - [DS-4999](#): Fix MSSQL memory metric ([🔗 DS-4999: Fix MSSQL memory metric pds-ui#755](#)) (Esteban Moscoso)



# Regular changes

## Visibility into changes

- How to determine scope of changes? Which profiles will be affected?
- Render all kustomizations for every profile on base+head branches
- Output diffs

 **github-actions** bot commented yesterday • edited ▾

### Generated diffs

---

#### Development

---

##### Apps

0 files changed

##### Infrastructure

unknown | 67 ++++++-----  
1 file changed, 65 insertions(+), 2 deletions(-)

#### Production

---

##### Apps

0 files changed

##### Infrastructure

unknown | 5 +++--  
1 file changed, 3 insertions(+), 2 deletions(-)

[Go to job summary for more details...](#)

production summary

**Found differe**

No differences in |

### Found differences in infrastructure kustomization

```
--- master      2023-03-29 13:37:58.746431720 +0000
+++ iokaya-ds4679 2023-03-29 13:37:58.742431664 +0000
@@ -461,8 +461,9 @@
     "log_checkpoints": true,
     "unix_socket_directories": "/tmp,/crunchyadm",
     "wal_level": "logical",
-    "wal_keep_size": "48MB"
-  },
+    "wal_keep_size": "48MB",
+    "shared_preload_libraries": "pg_stat_statements"
+  },
   "recovery_conf": {
     "restore_command": "source /opt/cpm/bin/pgbackrest/pgbackrest-set-env.sh && pgbackrest archive-get %f \"%p\"",
     "use_slots": false
```

Job summary generated at run-time





# Q&A