

Astro GitOps

Press (x) to start



Operation

A long time ago...

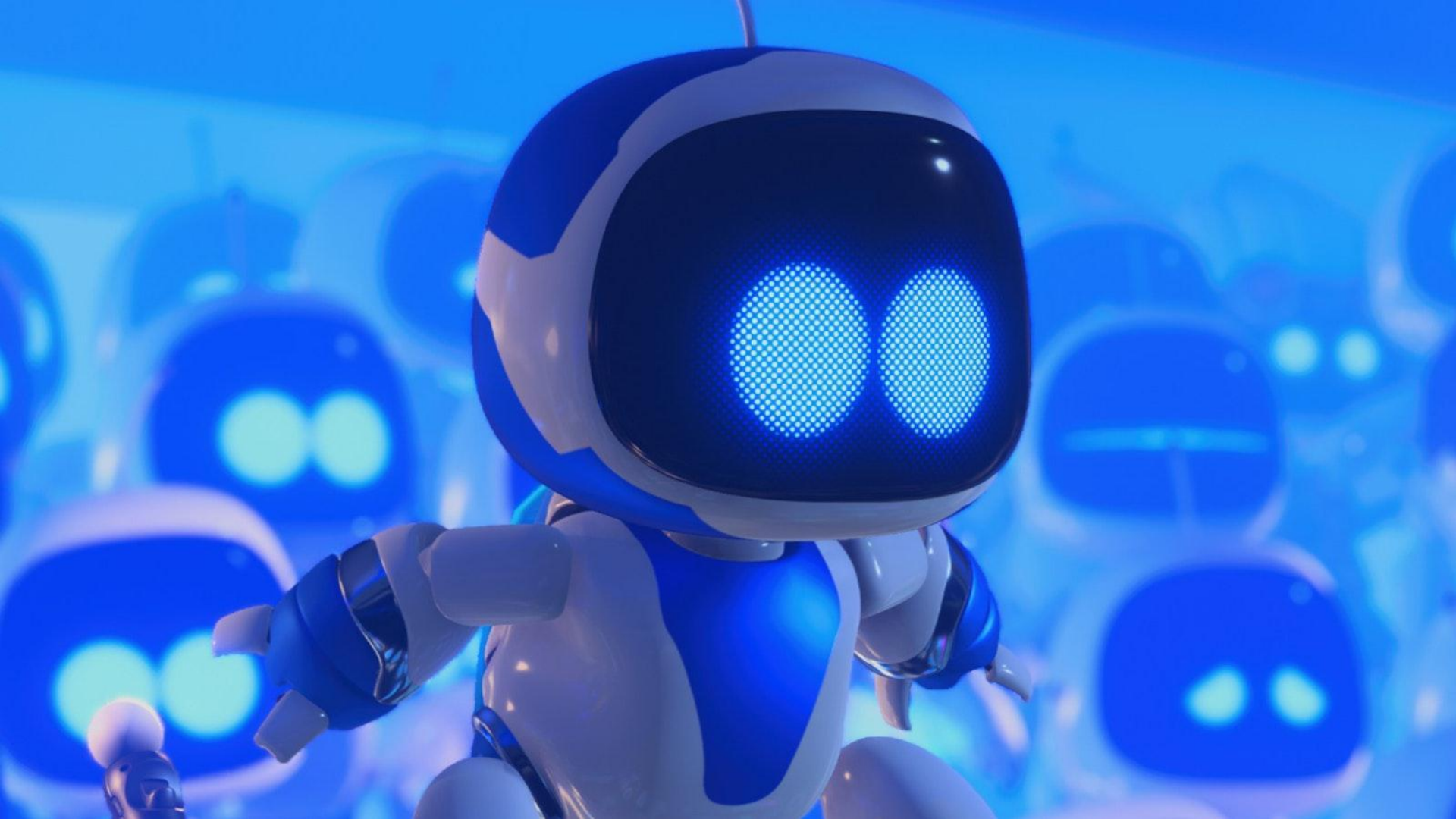


Strange
tools...



Strange
positions





In the meantime
...Devs







Kevin DAVIN

 
@davinkevin@davinkevin.fr




Google Developer Expert
on **Google Cloud & Kotlin**



Gitlab Heroes



Open Source Contributor

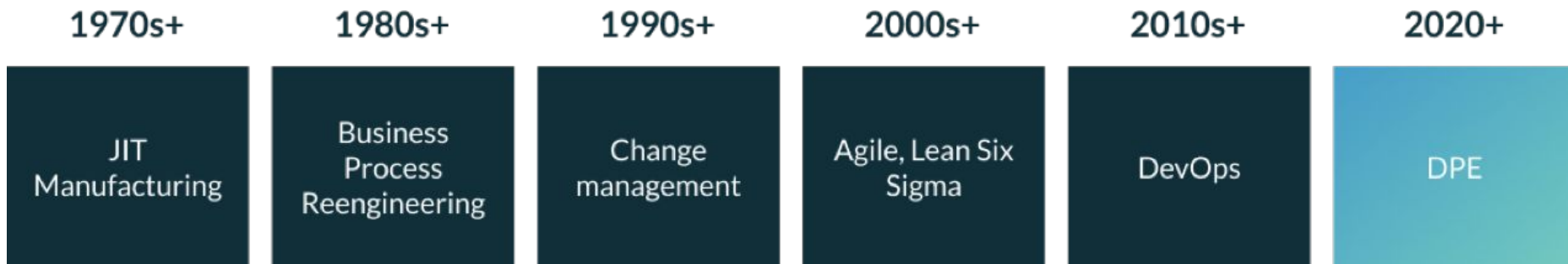




Our mission at **Gradle** is to **accelerate developer productivity** and
make developers happier



What comes after DevOps?



Developer Productivity Engineering



“If you can’t measure it, you can’t improve it!”

by Peter Drucker

Summary

Console log

Failure

Deprecations

Timeline

Performance

Tests

Projects

Dependencies

Build dependencies

Plugins

Custom values

Switches

Infrastructure

See before and after

Compare Build Scan

DEV ELOCITY

Podcast-Server :backend:jib Jan 19 2024 05:06:49 CET

Build Scans | Sign in

29 tasks, 0 transforms executed in 5 projects in 1m 8.206s, with 5 avoided tasks saving 2m 8.748s

Execution

:backend:compileKotlin

:backend:jib

Order: Execution

Ungrouped

Grouped by type

:build-plugin-database:checkKotlinGradlePluginConfigurationErrors	11.376s	0.059s	org.jetbrains.kotlin.gradle.plugin.diagnostics.CheckKotlinGradlePluginConfigurationErrors	T.	
:build-plugin-docker-images:checkKotlinGradlePluginConfigurationErrors	11.376s	0.061s	org.jetbrains.kotlin.gradle.plugin.diagnostics.CheckKotlinGradlePluginConfigurationErrors	T.	
:build-plugin-database:compileKotlin	FROM-CACHE	11.454s	0.568s	org.jetbrains.kotlin.gradle.tasks.KotlinCompile	T.
:build-plugin-docker-images:compileKotlin	FROM-CACHE	11.459s	0.564s	org.jetbrains.kotlin.gradle.tasks.KotlinCompile	T.
:build-plugin-database:compileJava	NO-SOURCE	12.025s	0.012s	org.gradle.api.tasks.compile.JavaCompile	T.
:build-plugin-docker-images:compileJava	NO-SOURCE	12.033s	0.005s	org.gradle.api.tasks.compile.JavaCompile	T.
:build-plugin-database:pluginDescriptors					T.
:build-plugin-docker-images:pluginDescriptors					T.
:build-plugin-database:processResources					T.
:build-plugin-docker-images:processResources					T.
:build-plugin-database:classes					T.
:build-plugin-docker-images:classes					T.
:build-plugin-database:jar					T.
:build-plugin-docker-images:jar					T.
:backend-lib-youtubedl:compileJava	FROM-CACHE				T.
:backend:checkKotlinGradlePluginConfigurationErrors					T.
:backend-lib-database:compileJava	FROM-CACHE				T.
:backend:generateGitProperties					T.
:backend-lib-youtubedl:processResources					T.
:backend-lib-youtubedl:classes	UP-TO-DATE				T.
:backend-lib-youtubedl:jar					T.
:backend-lib-database:processResources	NOT-CACHED				T.
:backend-lib-database:classes	UP-TO-DATE				T.
:backend-lib-database:jar					T.
:backend:compileKotlin	FROM-CACHE				T.
:backend:compileJava	NO-SOURCE				T.

Details

Predecessors

Successors

Kind

Path

Type

TASK

:build-plugin-database:pluginDescriptors

org.gradle.plugin.devel.tasks.GeneratePluginDescriptors

This task is not on the critical path.

Started after

Duration

12.039s

0.012s

This task was not up-to-date because there was no task history available.

Cache key

Not cacheable

0e96cd44a0f07adf9be5f07f1b6301a7

Not worth caching.

View task in console log

Focus on task in timeline

GeneratePluginDescriptors

GeneratePluginDescriptors

processResources

processResources

compile

diagnostics.CheckKotlinGradlePluginConfigurationErrors

compile

tiesTask

processResources

processResources

compile

KotlinCompile

compile

A Dev & Ops Story



Playing Working
Together

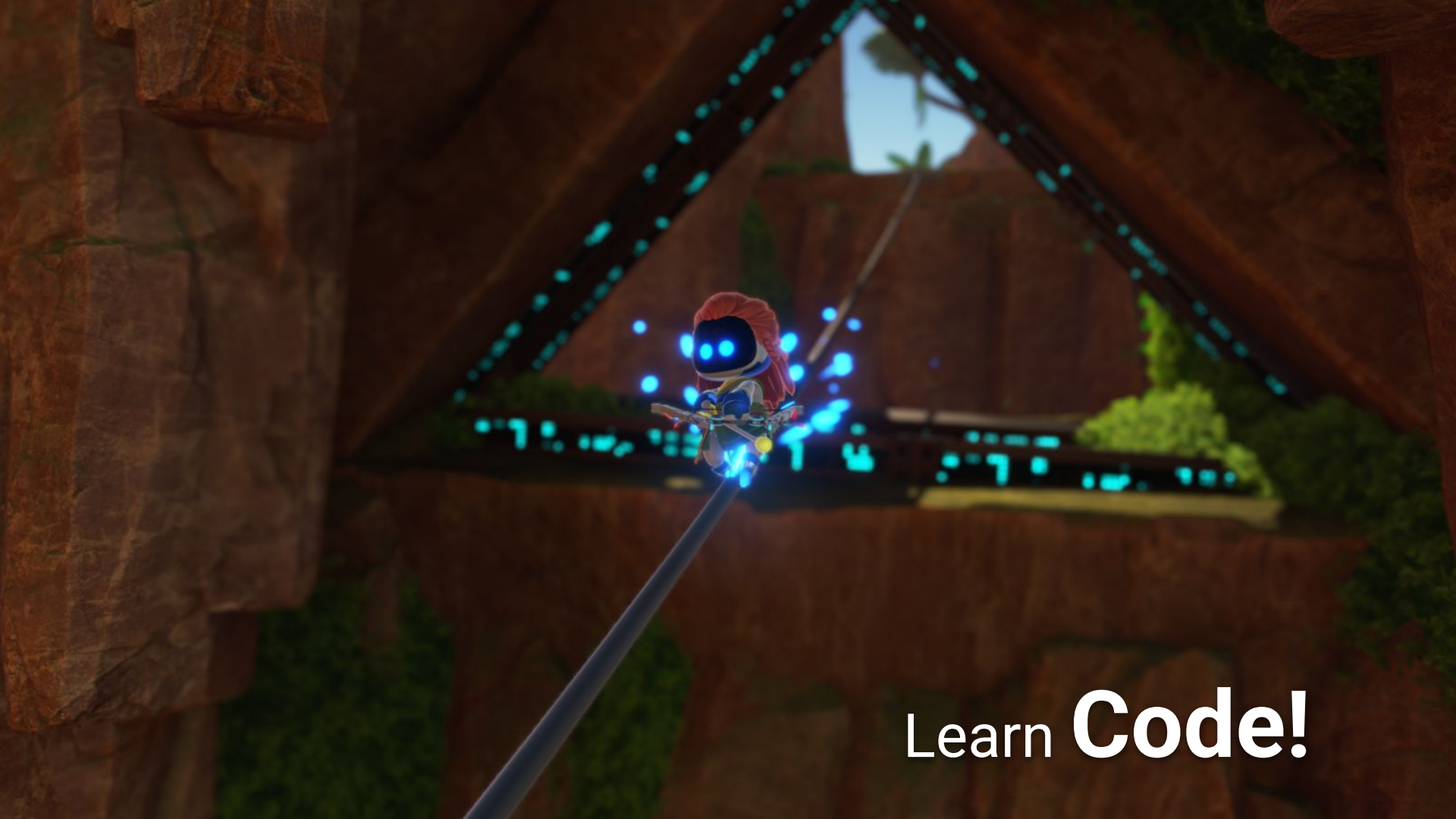




Learn!

Learn³





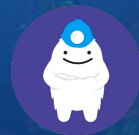
Learn **Code!**

Learn **Tests!**





Learn **Tools!**



test infra

VALIDKUBE

And Git!





Collaboration
around **Git**

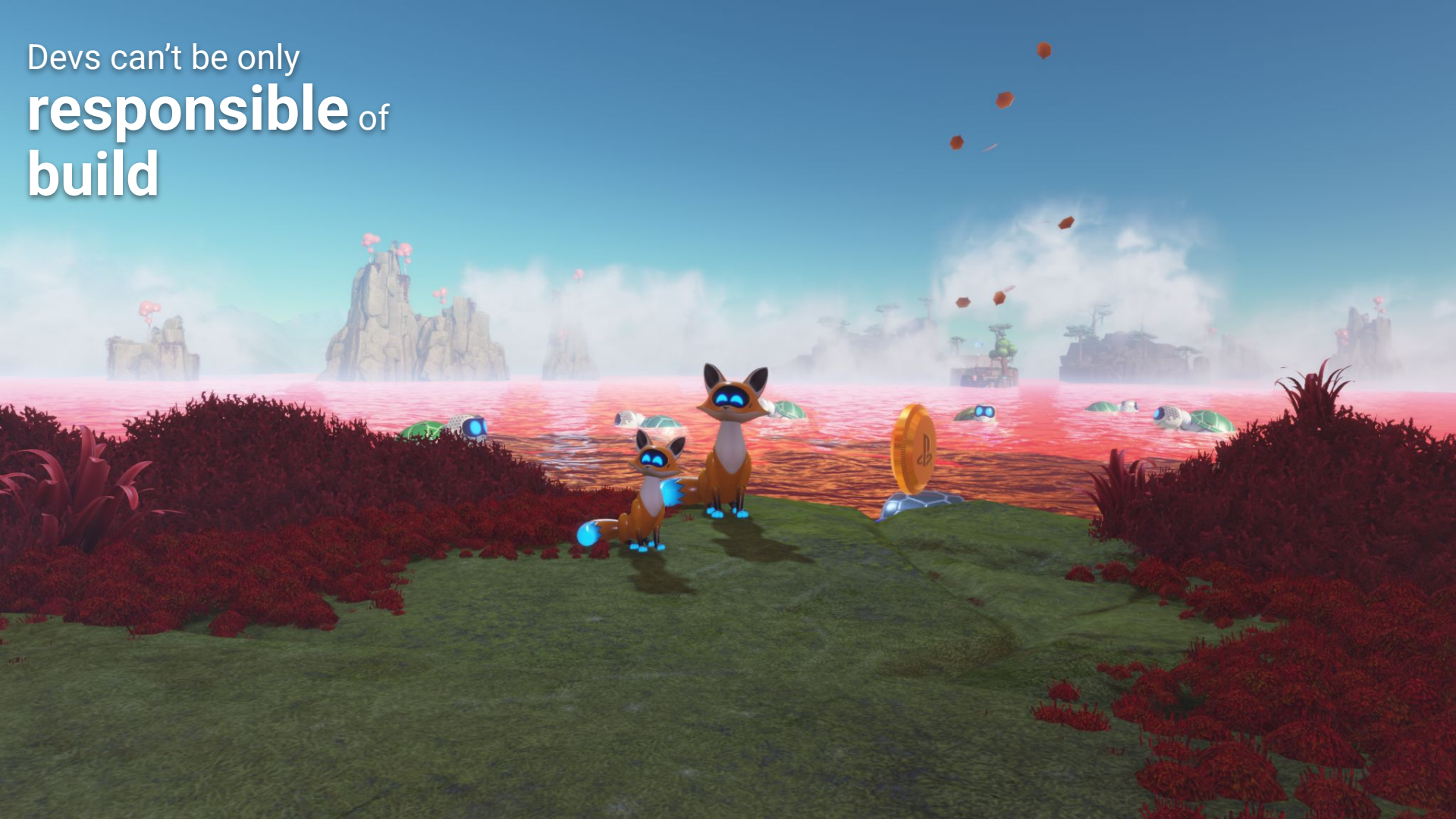


Push **Pull** people to
contribute

Ops **can't** do
everything



Devs can't be only
responsible of
build



You **build** it, you **run** it!







What is Ops job?



Manage a **state** in **prod**

From clusters



To Apps





And monitor!



git as
single source of
truth







CLOUD NATIVE
COMPUTING FOUNDATION

With a
Working Group



Very opinionated
Principles



#1 Declarative





Declarative
is pure gold for **doc!**

I ask what
I want...



... not what to do!



It's not continuous
apply



Demo!




```
#!/usr/bin/env bash
```

```
if ! [[ likeSpyro() ]]; then  
  addLikeTo("Spyro")  
  install("Spyro")  
fi
```



```
f0d763c (HEAD -> main) add install script
```



Shell
is not
declarative

What's the result?



```
#!/usr/bin/env bash
```

```
if ! [[ likeSpyro() ]]; then  
  addLikeTo("Spyro")  
  install("Spyro")  
fi
```



```
f0d763c (HEAD -> main) add install script
```


Not
repeatable



```
#!/usr/bin/env bash
```

```
if ! [[ likeSpyro() ]]; then  
    addLikeTo("Spyro")  
    install("Spyro")  
fi
```

```
if ! [[ likeResidentEvil() ]]; then  
    addLikeTo("ResidentEvil")  
    install("Chris Redfield")  
    install("Jill Valentine")  
fi
```



```
445d9cc (HEAD -> main) add install script v2
```




Not
repeatable²



```
#!/usr/bin/env bash
```

```
if ! [[ likeSpyro() ]]; then  
  addLikeTo("Spyro")  
  install("Spyro")  
fi
```



```
8db734a (HEAD -> main) revert to install v1
```


Tabula Rasa



Even with **Kubernetes** resources




```
apiVersion: kustomize.config.k8s.io/v1beta1
```

```
kind: Kustomization
```

```
namespace: playstation
```

```
resources:
```

- crash.yaml
- lara.yaml
- spyro.yaml



```
$ kubectl apply -k playstation
```




```
> kubectl get pods --namespace playstation
```

NAME	READY	STATUS	RESTARTS	AGE
crash-77ccfb466b-mpt5t	1/1	Running	0	6m44s
lara-b8fd4cc89-w7brd	1/1	Running	0	6m44s
spyro-6c55565cf6-fmngp	1/1	Running	0	6m44s

```
~ 56ms
```

```
> █
```



```
apiVersion: kustomize.config.k8s.io/v1beta1
```

```
kind: Kustomization
```

```
namespace: playstation
```

```
resources:
```

- crash.yaml
- solid-snake.yaml



```
$ kubectl apply -k playstation
```

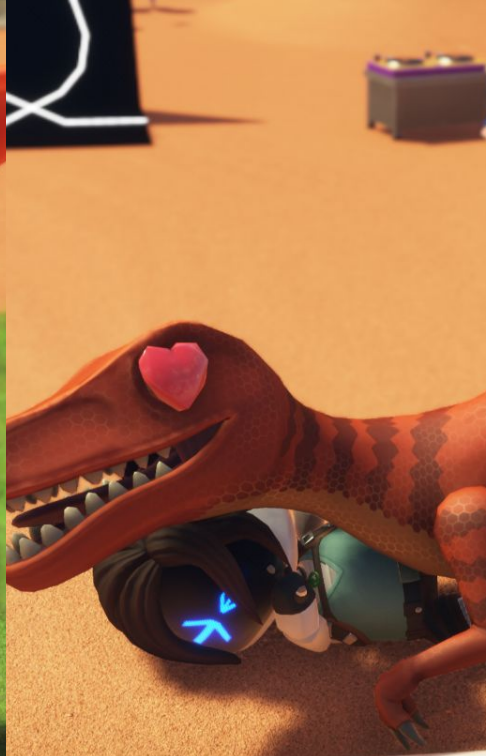



```
> kubectl get pods --namespace playstation
```

NAME	READY	STATUS	RESTARTS	AGE
crash-77ccfb466b-mpt5t	1/1	Running	0	7m55s
lara-b8fd4cc89-w7brd	1/1	Running	0	7m55s
solid-snake-5d464b576f-bwtd7	1/1	Running	0	22s
spyro-6c55565cf6-fmngp	1/1	Running	0	7m55s

```
~ 57ms
```

```
> █
```

kubectl apply
is **imperative** too



Another probl-He1m



HeIm is everywhere...





Declarative?

```
# values.yaml
```

```
global:  
  hostname: myapp.company.com
```

```
componentA:  
  enabled: true  
  features:  
    foo: ENABLED  
    bar: DISABLED
```




Not really...



If/Else

The first control structure we'll look at is for conditionally including blocks of text in a template. This is the `if / else` block.

The basic structure for a conditional looks like this:

```
{{ if PIPELINE }}  
  # Do something  
{{ else if OTHER PIPELINE }}  
  # Do something else  
{{ else }}  
  # Default case  
{{ end }}
```




Using the `lookup` function

The `lookup` function can be used to *look up* resources in a running cluster. The synopsis of the lookup function is `lookup apiVersion, kind, namespace, name -> resource or resource list`.

What do you deploy?
You don't know...




```
kind: NetworkPolicy
apiVersion: networking.k8s.io/v1
metadata:
  name: deny-all
spec:
  podSelector: {}
  ingress: []
```

Not cool...




```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: unwanted-cluster-role
rules:
  - apiGroups: [ "" ]
    resources: [ "secrets" ]
    verbs: [ "get", "watch", "list" ]
```



Unmanageable...

No upgrade path!



```
# values.yaml  
componentA:  
  enabled: true  
  replica: 3
```



```
# values.yaml  
componentA:  
  enabled: true  
  
replicaS: 3
```

(almost) **no** error
management



With an operator?



```
apiVersion: helm.toolkit.fluxcd.io/v2
kind: HelmRelease
metadata:
  name: myapp
spec:
  chart:
    spec: { ... }
  releaseName: podinfo-in-dev
  values:
    global:
      hostname: myapp.company.com

  componentA:
    enabled: true
    features:
      foo: ENABLED
      bar: DISABLED
```




```
apiVersion: argoproj.io/v1alpha1
kind: Application
metadata:
  name: myapp
spec:
  project: default
  destination:
    server: https://kubernetes.default.svc
  source:
    repoURL: oci://ghcr.io/stefanprodan/charts/podinfo
    chart: podinfo-in-dev
  helm:
    values: |
      global:
        hostname: myapp.company.com

    componentA:
      enabled: true
      features:
        foo: ENABLED
        bar: DISABLED
```



```
apiVersion: helm.cattle.io/v1
kind: HelmChart
metadata:
  name: myapp
spec:
  repo: oci://ghcr.io/stefanprodan/charts/podinfo
  chart: podinfo-in-dev
  valuesContent: |-
    global:
      hostname: myapp.company.com

  componentA:
    enabled: true
    features:
      foo: ENABLED
      bar: DISABLED
```



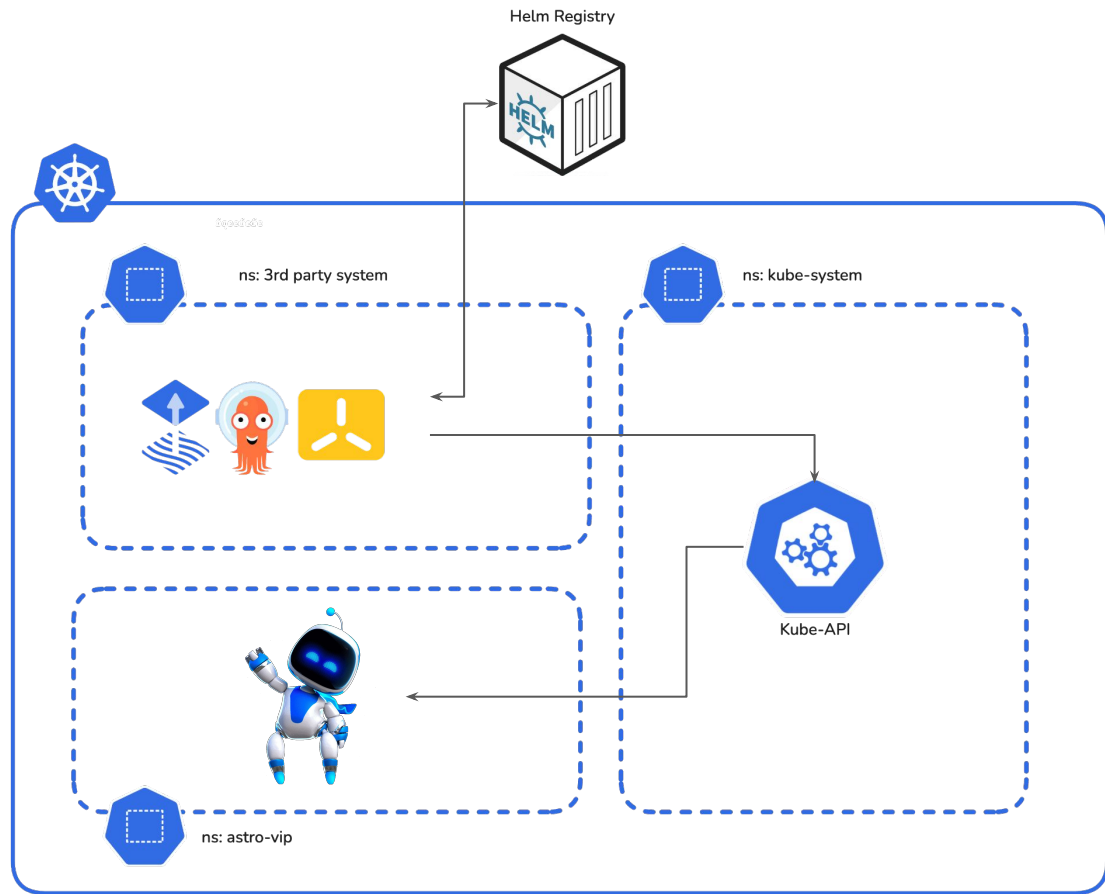




Chart is **remote**

Just the same...





Don't git up 🐵



Commit



CustomResourceDefinition

Fetches by

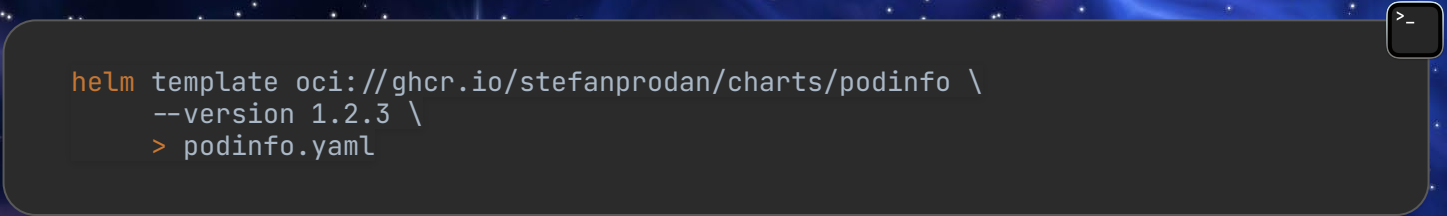


Render & apply



Recommendation
Render!





```
helm template oci://ghcr.io/stefanprodan/charts/podinfo \  
  --version 1.2.3 \  
  > podinfo.yaml
```

✓  podinfo

 podinfo.yaml

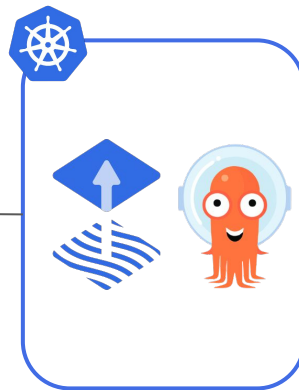

```
> --- release-name-podinfo: v1/Service
> --- release-name-podinfo: apps/v1/Deployment
> --- release-name-podinfo-grpc-test-xiwh7: v1/Pod
> --- release-name-podinfo-jwt-test-9p02s: v1/Pod
> --- release-name-podinfo-service-test-k1k7d: v1/Pod
```



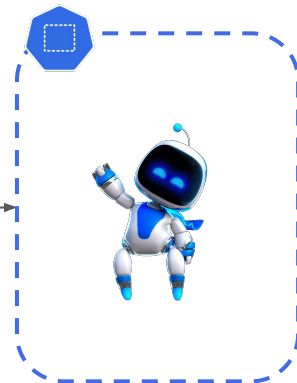
Render & Commit



Fetches by



Apply



Not a problem anymore





Just declarative!



#2 Versioned



...and #2 Immutable

Predictable



feat(backup): add cronjob to backup to the cloud



Pipeline #989878943 passed

1 year ago



Changes 9

Pipelines 2

▼ backup/overlays/k8s-server/cronjob.yaml 0 → 100644

+39 -0



View file @ 8baF98f4

```
1 + apiVersion: batch/v1
2 + kind: CronJob
3 + metadata:
4 +   name: backup-to-bucket
5 + spec:
6 +   concurrencyPolicy: Forbid
7 +   schedule: '0 0 * * 0'
8 +   jobTemplate:
9 +     spec:
10 +       backoffLimit: 2
11 +       template:
12 +         spec:
13 +           restartPolicy: Never
14 +           containers:
15 +             - name: gcloud
16 +               image: google/cloud-sdk:latest
17 +               workingDir: /backup
18 +               env:
19 +                 - name: GOOGLE_APPLICATION_CREDENTIALS
20 +                   value: /credentials
21 +
22 +             - name: backup
23 +               image: gcr.io/kaniko-project/executor:latest
24 +               workingDir: /backup
25 +
26 +           volumeMounts:
27 +             - mountPath: /credentials
28 +               subPath: credentials.json
29 +               name: credentials
30 +             - mountPath: /backup
31 +               name: backup
32 +
33 +           volumes:
34 +             - name: credentials
35 +               secret:
36 +                 secretName: credentials
```




Reproducible

For every system





No matter what!



Tunnel of History

Guides...?



Dec 15, 2024



feat(atuin): configure backup to minio ...

Davin Kevin authored 2 months ago

Verified



163b1d59



feat(atuin): configure & scale-up after PG17 upgrade process ...

Davin Kevin authored 2 months ago

Verified

1e26724a



feat(atuin): create db with PG17 and data migrated from current PG15 ...

Davin Kevin authored 2 months ago

Verified



8ed19ab8



feat(atuin): scale down during PG17 upgrade process ...

Davin Kevin authored 2 months ago

Verified



e3cb5de0



feat(cron): adjust timers to run during night ...

Davin Kevin authored 2 months ago

Verified



6feb81e2





Audit friendly

Mar 14, 2025

 chore(deps): update helm release mastodon to v10.0.11 
Renovate Bot authored 1 day ago and  Davin Kevin committed 1 day ago

Mar 11, 2025

 chore(deps): update helm release mastodon to v10.0.10 Verified 
Renovate Bot authored 4 days ago

Feb 28, 2025

 chore(deps): update helm release mastodon to v10.0.9 Verified 
Renovate Bot authored 2 weeks ago

Jan 17, 2025

 chore(deps): update helm release mastodon to v10.0.8 
Renovate Bot authored 1 month ago and  Davin Kevin committed 1 month ago

Dec 04, 2024

 chore(deps): update helm release mastodon to v10.0.7 Verified 
Renovate Bot authored 3 months ago

Nov 16, 2024

 chore(deps): update helm release mastodon to v10 Verified
Davin Kevin authored 3 months ago

Sep 30, 2024

 chore(deps): update helm release mastodon to v9.2.2
Renovate Bot authored 5 months ago and  Davin Kevin committed 5 months ago

Aug 20, 2024

 chore(deps): update helm release mastodon to v9.2.1 Verified
Renovate Bot authored 6 months ago

Feb 01, 2024

 chore(deps): update helm release mastodon to v9.1.2 Unverified 
Renovate Bot authored 1 year ago

Jan 24, 2024

 chore(deps): update helm release mastodon to v9.1.1 Unverified 
Renovate Bot authored 1 year ago

Jan 14, 2024

 chore(deps): update helm release mastodon to v9.1.0 Unverified 
Renovate Bot authored 1 year ago

Jan 10, 2024

 chore(deps): update helm release mastodon to v9.0.3 Unverified 
Renovate Bot authored 1 year ago

Dec 09, 2023

 chore(deps): update helm release mastodon to v9.0.1 Verified 
Renovate Bot authored 1 year ago

Nov 28, 2023

 chore(deps): update helm release mastodon to v9 Unverified 
Renovate Bot authored 1 year ago

Oct 21, 2023

 chore(mastodon): upgrade mastodon core and chart
Renovate Bot authored 1 year ago and  Davin Kevin committed 1 year ago

Oct 04, 2023

 chore(mastodon): move to helmfile for template generation Verified
Davin Kevin authored 1 year ago

 Failed

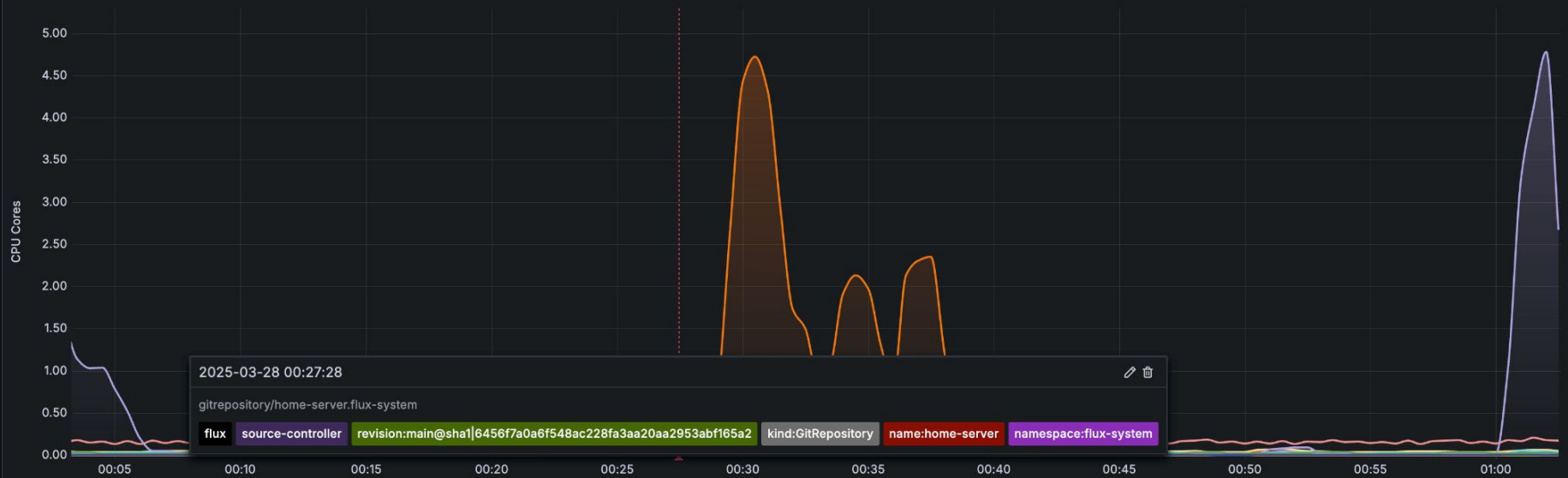
 19 minutes ago

#9557196058: kustomization/kutt/86fd3eb4

 main

 04c2b4bf

CPU Utilization by namespace



A lush, vibrant jungle scene from a video game. In the foreground, a toucan with a black body and a large, colorful beak (red, orange, yellow, green, and blue) is flying towards the left. To its right, a small, silver biplane with a propeller is flying towards the right. The background features a deep canyon with a turquoise river at the bottom, surrounded by steep, rocky cliffs. Large, ancient stone ruins are visible on the left and right sides of the frame. The scene is filled with dense green foliage, including large trees with thick canopies and various tropical plants. A green laser beam is visible on the right side, passing through a stone structure. The overall atmosphere is bright and colorful, typical of a modern action-adventure game.

Author
verification

Feb 28, 2025



chore(deps): update helm release mastodon to v10.0.9

Renovate Bot authored 2 weeks ago

Verified





Secure by
design



#3 Pull only!

Opinionated
again!





Push means
multiple sources

script:

- kustomize build cert-manager/overlays/kserver/ | kubectl apply -f - --dry-run=client
- kustomize build cert-manager/overlays/kserver/ | kubectl apply -f -





Pull from cluster itself



Fight
for security

Disconnected Clusters





A screenshot from a video game showing Sonic the Hedgehog flying through a series of red torii gates. The gates are made of thick red pillars and horizontal beams. The landscape is a misty, orange-hued environment with rocky islands and a small traditional Japanese building in the distance. Sonic is in the center, flying towards the viewer. He is wearing a blue and white hovercraft-like device with blue lights. Two large, dark, cylindrical objects with blue lights are positioned on either side of Sonic, emitting bright blue energy beams. The overall scene is dynamic and action-oriented.

#4 Continuous Reconciliation

Always there for you!





Git → **Cluster**



Cluster → **Kubernetes**

Based on
time




```
apiVersion: kustomize.toolkit.fluxcd.io/v1
kind: Kustomization
metadata:
  name: external
spec:
  interval: 1440m
  path: ./path/to/my/resources
  sourceRef:
    kind: GitRepository
    name: my-repository
```

Doesn't
Scale





Load &
concurrency



Or clever with
WebHooks


```
apiVersion: notification.toolkit.fluxcd.io/v1
kind: Receiver
metadata:
  name: a-cluster
spec:
  type: gitlab
  events:
    - "ping"
    - "Push Hook"
  secretRef:
    name: webhook-token
  resources:
    - kind: GitRepository
      name: my-repository
```

Declarative, of course





WebHook
config

Webhooks 1

Add new webhook

<https://flux.mycomp.com/hook/a-random-string-generated-by-gitlab>

Test ▾

Edit

Delete

Push events

SSL Verification: enabled



Drift
Detection





Keep it **simple** & **stupid**



Too complicated
is **not** an option





Multi-Tech
Repository



Infrastructure



Application

TerraFu™



Kubernetes





One repo!




```
# postgresql.tf
variable "postgres_root_password" {
  type = string
}

resource "google_sql_database_instance" "main" {
  name                = "astrobot"
  database_version    = "POSTGRES_17"
  region              = "astro-world"

  root_password = var.postgres_root_password
  settings {
    tier = "micro"
  }
}
```

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: my-app
spec:
  template:
    spec:
      containers:
        - name: myapp
          image: astrobt.docker.io/my-app
          ports:
            - containerPort: 80
              protocol: TCP
```


feat(app): add myapp to the system! 🚀

🔗 Open Davin Kevin requested to merge myapp into main just now

Overview 0 Commits 1 Changes 2

Files 2

myapp

myapp.yaml +13 -0

postgresql.tf +27 -0

myapp/myapp.yaml 0 → 100644

+13 -0

```
1 + apiVersion: apps/v1
2 + kind: Deployment
3 + metadata:
4 +   name: my-app
5 + spec:
6 +   template:
7 +     spec:
8 +       containers:
9 +       - name: myapp
10 +         image: astrobt.docker.io/my-app
11 +         ports:
12 +         - containerPort: 80
13 +           protocol: TCP
```

myapp/postgresql.tf 0 → 100644

+27 -0

```
1 +
2 + variable "postgres_root_password" {
3 +   type = string
4 + }
5 +
6 + resource "google_sql_database_instance" "main" {
7 +   name             = "astrobot"
8 +   database_version = "POSTGRES_17"
9 +   region           = "astro-world"
10 +
11 +   root_password = var.postgres_root_password
12 +   settings {
13 +     tier = "micro"
14 +   }
15 + }
```

1 source of truth



TerraFu™ managed
in **Kubernetes**





Tofu controller for **FluxCD**



provider-terraform for Crossplane
By Upbound

bridge between
2 worlds!




```
variable "postgres_root_password" {  
  type = string  
}  
  
resource "google_sql_database_instance" "main" {  
  root_password = var.postgres_root_password  
}  
  
resource "kubernetes_secret" "postgres_password" {  
  metadata {  
    name = "postgres-password"  
  }  
  
  type = "Opaque"  
  
  data = {  
    password = base64encode(var.postgres_root_password)  
  }  
}
```

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: my-app
spec:
  template:
    spec:
      containers:
      - name: myapp
        image: astrobt.docker.io/my-app
        envFrom:
        - secretRef:
            name: postgres-password
```


Many
problems



1 system
as a goal





Crossplane

```
apiVersion: sql.gcp.upbound.io/v1beta1
kind: DatabaseInstance
metadata:
  name: myapp
spec:
  forProvider:
    databaseVersion: POSTGRES_17
    region: astro-world
    rootPasswordSecretRef:
      key: password
      name: postgres-password
      namespace: myapp
    settings:
      - tier: micro
  providerConfigRef:
    name: google-cloud-provider
  writeConnectionSecretToRef:
    name: postgres-connection
    namespace: myapp
```



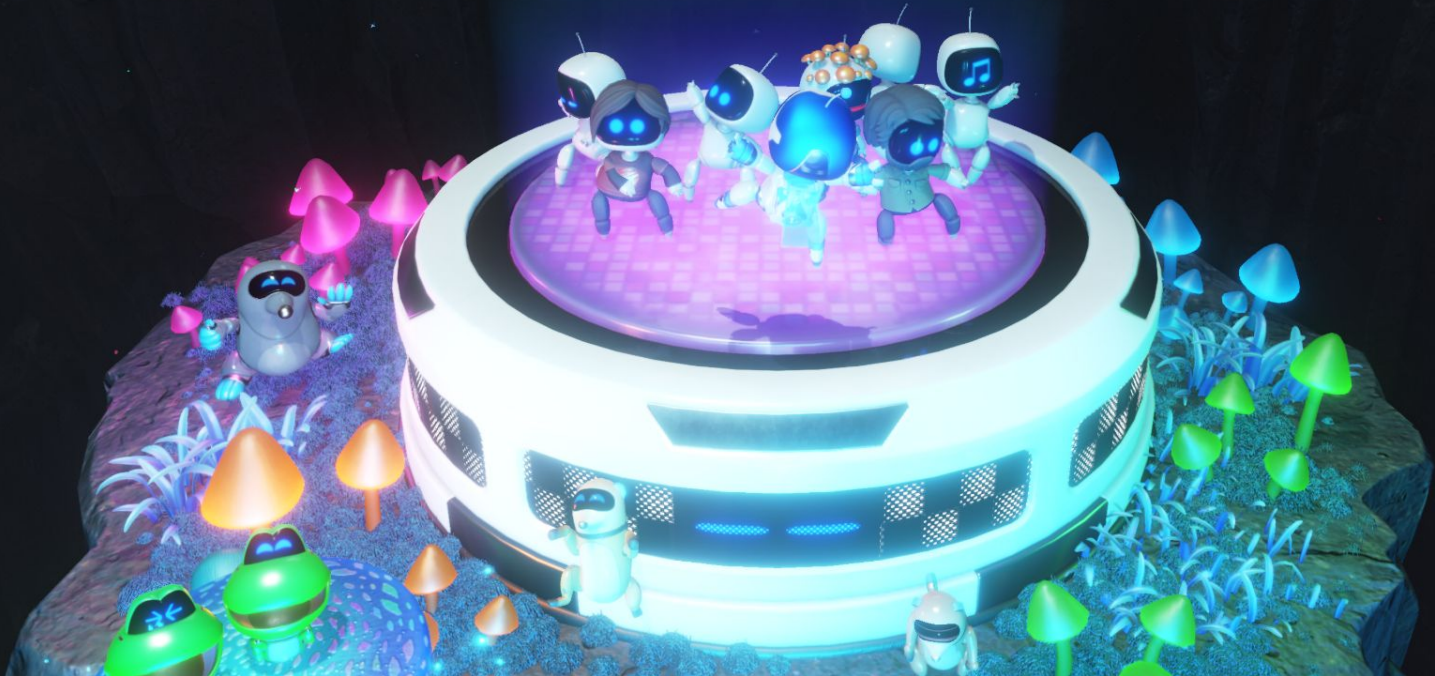

Google Kubernetes Engine
with **ConfigConnector**

```
apiVersion: sql.cnrm.cloud.google.com/v1beta1
kind: SQLInstance
metadata:
  name: myapp
spec:
  databaseVersion: POSTGRES_17
  region: astro-world
  rootPassword:
    valueFrom:
      secretKeyRef:
        key: password
        name: postgres-password
  settings:
    tier: micro
```


Adoption from
Dev to Ops



it's just **Simple**



Another
adventure?



How we
organize the repo?



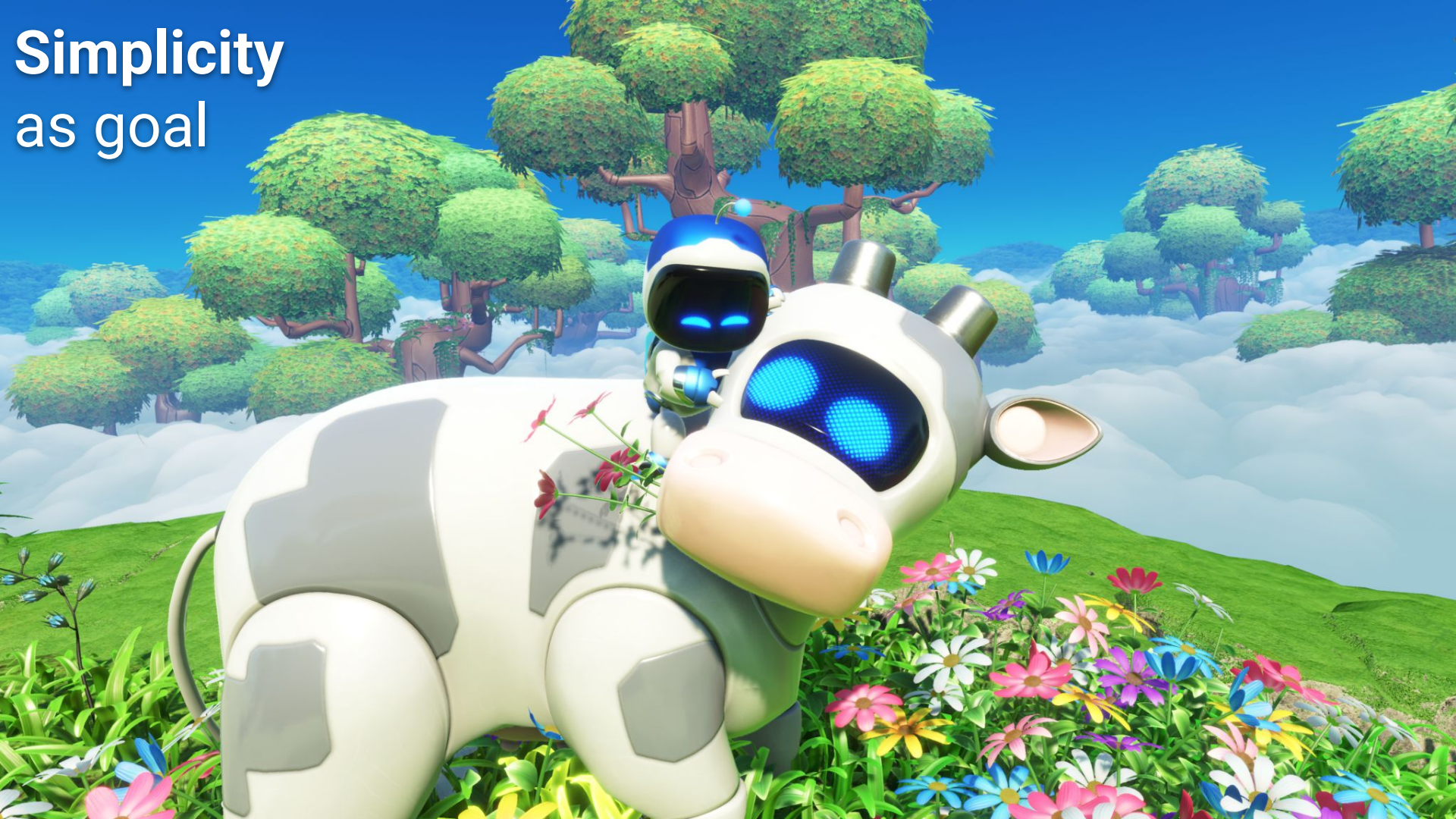
It might **waste** everything



Flat !



Simplicity
as goal



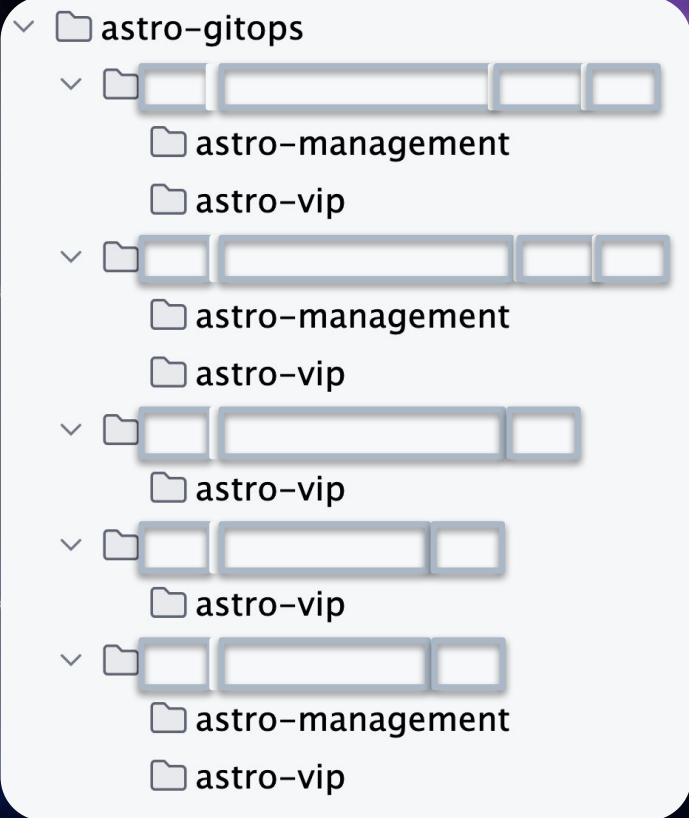
But there is
so many paths...



- ✓  astro-gitops
 - ✓  aks-africa-south1-a-qual-c03
 -  astro-management
 -  astro-vip
 - ✓  eks-europe-north1-b-dev-001
 -  astro-management
 -  astro-vip
 - ✓  gke-europe-west1-c-b02
 -  astro-vip
 - ✓  gke-us-west1-a-a07
 -  astro-vip
 - ✓  gke-us-west1-a-v36
 -  astro-management
 -  astro-vip

Unnecessarily
technical





App as
first-class citizen



- ▼  astro-gitops
 - ▼  astro-management
 -  dev
 -  qual
 -  prod
 - ▼  astro-vip
 -  dev
 -  qual
 -  prod



I want moar!



- ▼  astro-gitops
 - ▼  astro-management
 -  dev.iam.astrobot.com
 -  qual.iam.astrobot.com
 -  iam.astrobot.com
 - ▼  astro-vip
 -  dev.astrobot.com
 -  qual.astrobot.com
 -  astrobot.com

Simplicity!



sometimes
D.R.Y is an
enemy



✓  astro-gitops

✓  astro-vip

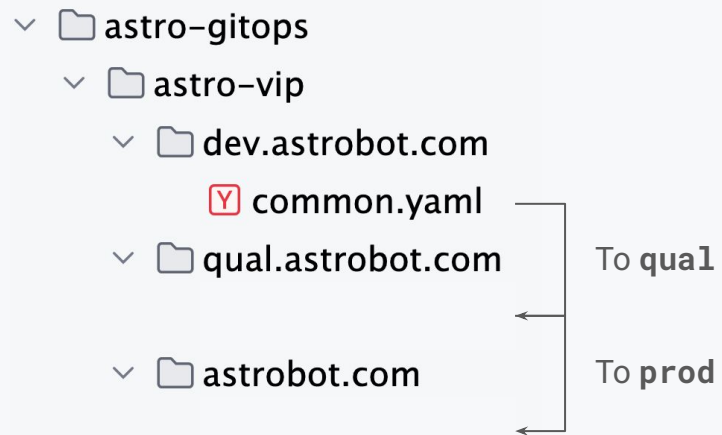




Useless
coupling

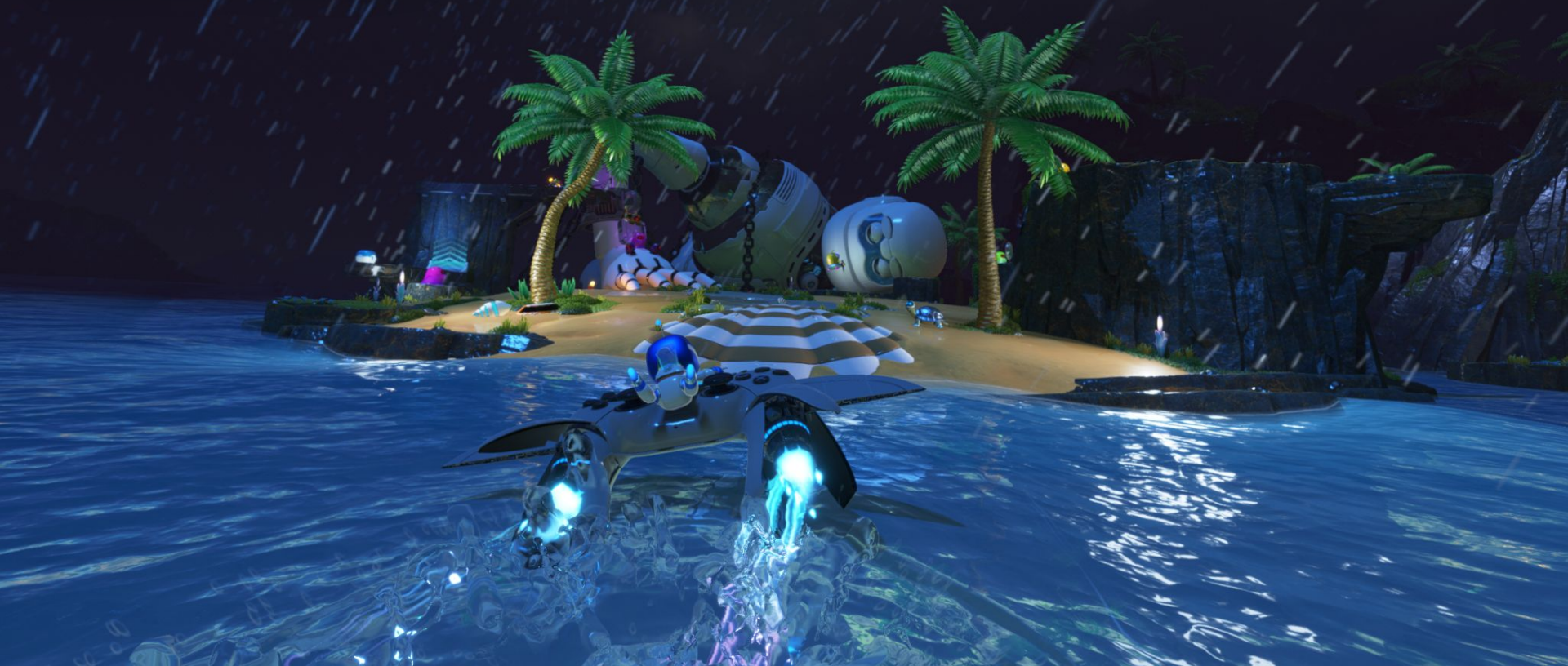
**Automate
promotion**







What about
secrets?

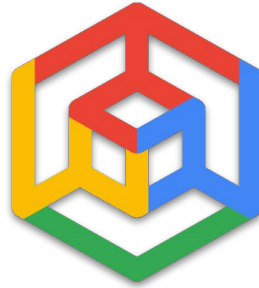


Let's be
secret-less!

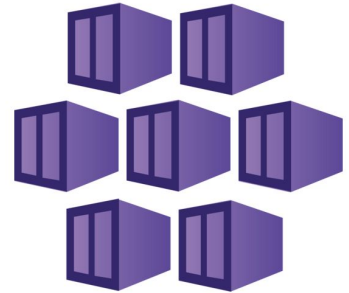




Elastic Kubernetes Service



Google Kubernetes Engine

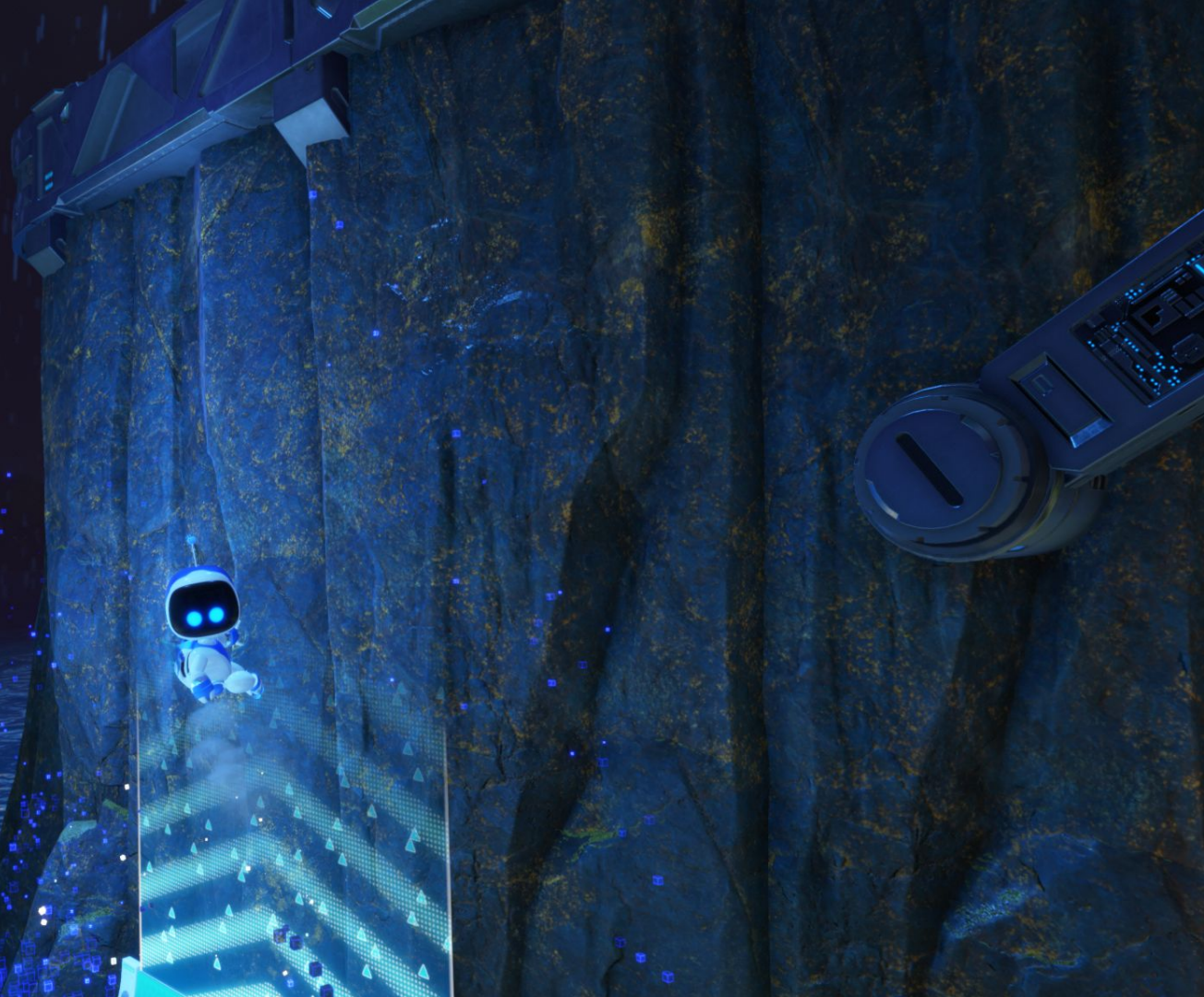


Azure Kubernetes Service

Fallback;
Secrets in Git



Secrets in Git
Really??





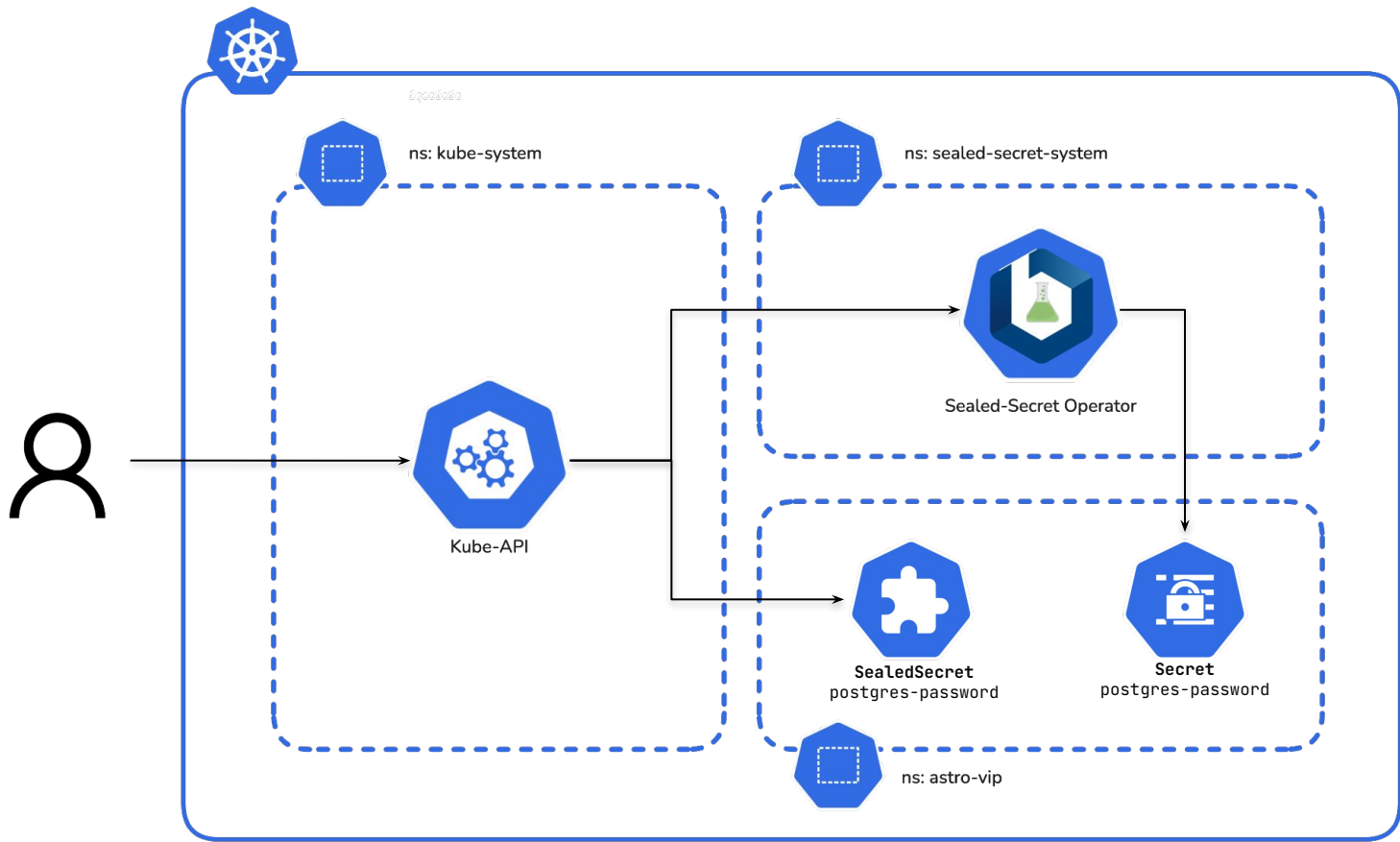
(Mozilla) **SOPS**



Bitnami **Sealed-Secrets**

```
apiVersion: bitnami.com/v1alpha1
kind: SealedSecret
metadata:
  name: postgres-password
spec:
  encryptedData:
    password: AgA8ptqWXbxQMIQARpjQ...KIlgY+37IKvJXT/Uw==
  template:
    metadata:
      name: postgres-password
```





```
login=ENC[AES256_GCM,data:EpBBj8nYFb,iv:l+2rTh8rFDfzIakLMEF6gnsE7fsw3v6NWUyTcZqiEN0=,tag:bqPDRGpGPlz2hLG9VyaLHw==,type:str]
password=ENC[AES256_GCM,data:vKji/bC0kvyWnZFiv2/koTQULz5xx7wVyA=,iv:2MU77Peqj1FfVgsHVMGTF8Ypni/N3UDiBnx6WeQdXss=,tag:PB207H8syjKG+
lYMef+xEw==,type:str]
sops_age__list_0__map_enc=-----BEGIN AGE ENCRYPTED FILE-----\nYWdl-gA==\n-----END AGE ENCRYPTED FILE-----\n
sops_age__list_0__map_recipient=age1wts0su6ae9dy2vrdez630lhac2nae6e4crntavlyrjuglkug6pmqwrtqfr
sops_age__list_1__map_enc=-----BEGIN AGE ENCRYPTED FILE-----\nYWdlL...tA==\n-----END AGE ENCRYPTED FILE-----\n
sops_age__list_1__map_recipient=age1xuv02mpj3pq9y2thaucdx9v97x50jh3z0ud6l2dj5urtjsz9jq8085zz
sops_lastmodified=2025-03-28T23:20:49Z
sops_mac=ENC[AES256_GCM,data:cKZHJBL...THLA==,type:str]
sops_unencrypted_suffix=_unencrypted
sops_version=3.9.2
```

SOPS


```
{
  "type": "ENC[AES256_GCM,data:6goKg10NJOHW7YB1Gf2C,iv:NoH0YBdSq60c/x4up3GnYt2re0+mYB974N9QxHtWJxQ=,tag:T2TUCYsmFWouh9NqoBZ4Gw==,type:str]"
  "project_id": "ENC[AES256_GCM,data:vC702anr7vQ41kPK,iv:X1CjdN08V72VBA4cvXl88qsFZZjexgDJmS1q5WrV2oY=,tag:xTCvxxvSajoC14JnRYUWbnw==,type:str"
  "private_key_id": "ENC[AES256_GCM,data:239uV609Tf8f1dV/yJY=,iv:3RCBu2v60uSEvgLwVeAlDVxsNc1FZhhSmzs9BMCX1hQ=,tag:9+0rzK1pC0dnN7FD1EtTNQ==,
  "private_key": "ENC[AES256_GCM,data:awfEFXEdUe1cHwbdKrs5t68LUEf+mr9pmRn3/uoFzAEPr+wQpfiiwiz4QU6FUtj77CJsBrL2M4xu1bqMGdI9zozBH7kbyWKWemy6Fy
  "client_email": "ENC[AES256_GCM,data:ZiqT4xgqznxw6JsRc28YLXE1Lq0xMFUBKM0n3vJQ0cDLM8/y,iv:8t2A8D/MPVNP6sUeTJc3VH82NNA1GVuv5e2B7hH7Qb8=,tag
  "client_id": "ENC[AES256_GCM,data:G635jqrALVP5,iv:P274LsdhB9/j/TgLcdvjyJhZUCvb0q4QrUQ9Wb9VAsA=,tag:IYVToJ4oPXiISE62H/c25w==,type:str]",
  "auth_uri": "ENC[AES256_GCM,data:CI48bw0Y3xQHDtiC8tceH0VJz0y3IvReYVtUtn2CRvjtlAFW+uhsyGk=,iv:LEom27CgRH8h2Vm9iTDwSW4+rLFVuxLPDCevc+C4UYI=
  "token_uri": "ENC[AES256_GCM,data:qFjBoI/6hg8WhvkUX1xbjx6Z4W+3cvZj6F3UbJD0kwbafZI=,iv:0jS2hjtb2MmgZcmU0drchm3ImzR5J7rwtkJV/Syq7x0=,tag:s1
  "auth_provider_x509_cert_url": "ENC[AES256_GCM,data:TxjAAWo2BwzmSwZXvsrek0prit68DoCaZ9BzNqs0EdrAd14t0u8vZkXX,iv:k8INtdP0tt+wiX9/vD/0/wA/9
  "client_x509_cert_url": "ENC[AES256_GCM,data:7fuT1ChUssBXu2GnHDpa3PsEucvbn9Ame/5YQDCtU5SngFF47KSn9Xi/LCuTgY6ZTdXXCRp9hPKNtsbqibNLXe+XcRqZ
  "universe_domain": "ENC[AES256_GCM,data:Mor3ZICrEmZgoHvxLjk=,iv:Vm78bHZUfR76RJ0fj8RD+PDf3tqn7TKJo+/4vAlEucM=,tag:91E+FPED01TJ3JkAS6LUj2Q==
  "sops": {"kms": null...}
}
```

SOPS

`apiVersion: kustomize.config.k8s.io/v1beta1`

`kind: Kustomization`

`secretGenerator:`

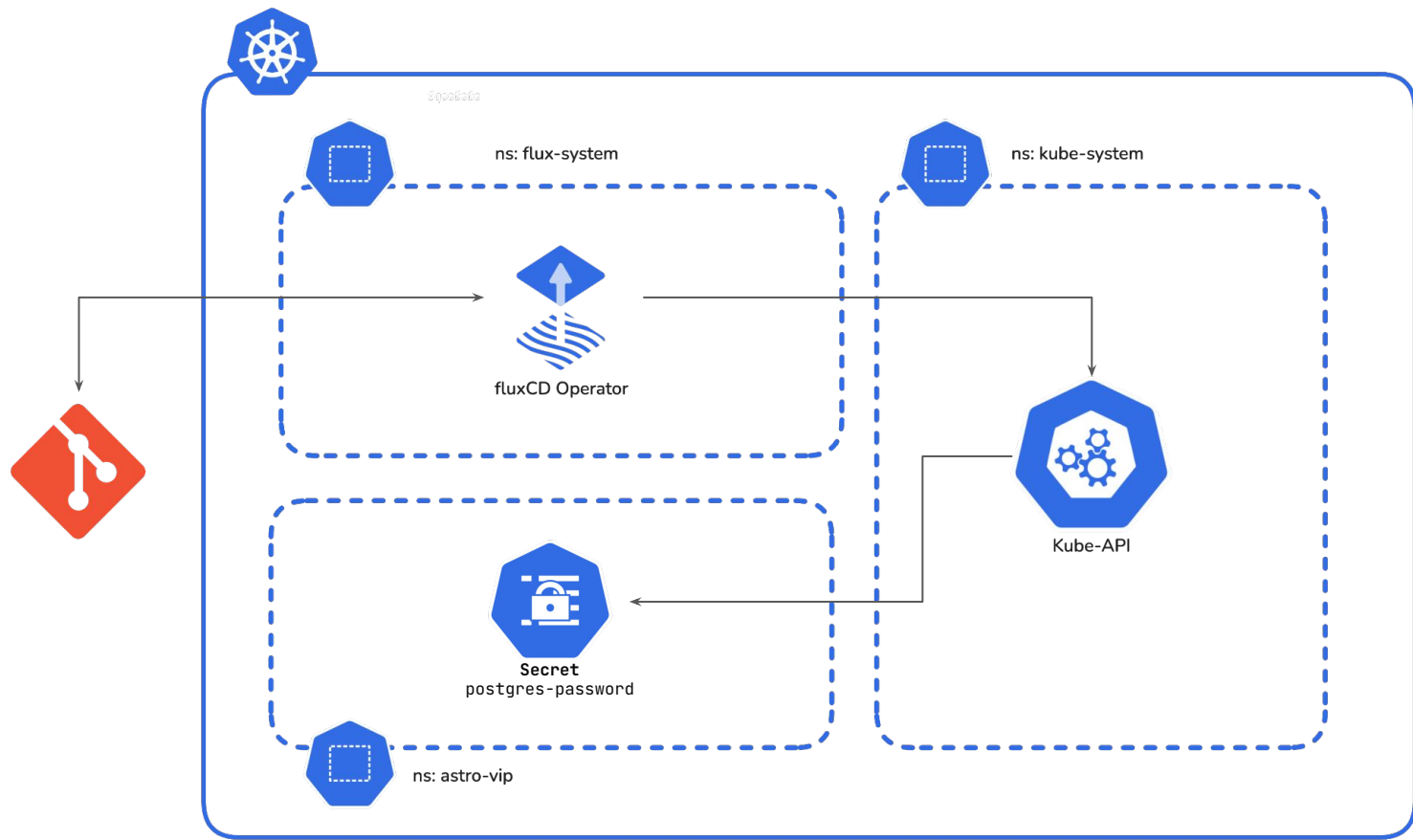
- `name: credentials`

`envs:`

- `astrobot.env`

`files:`

- `serviceAccount.json`



Vault?



Good **Luck!**



1 source of truth!
You remember?



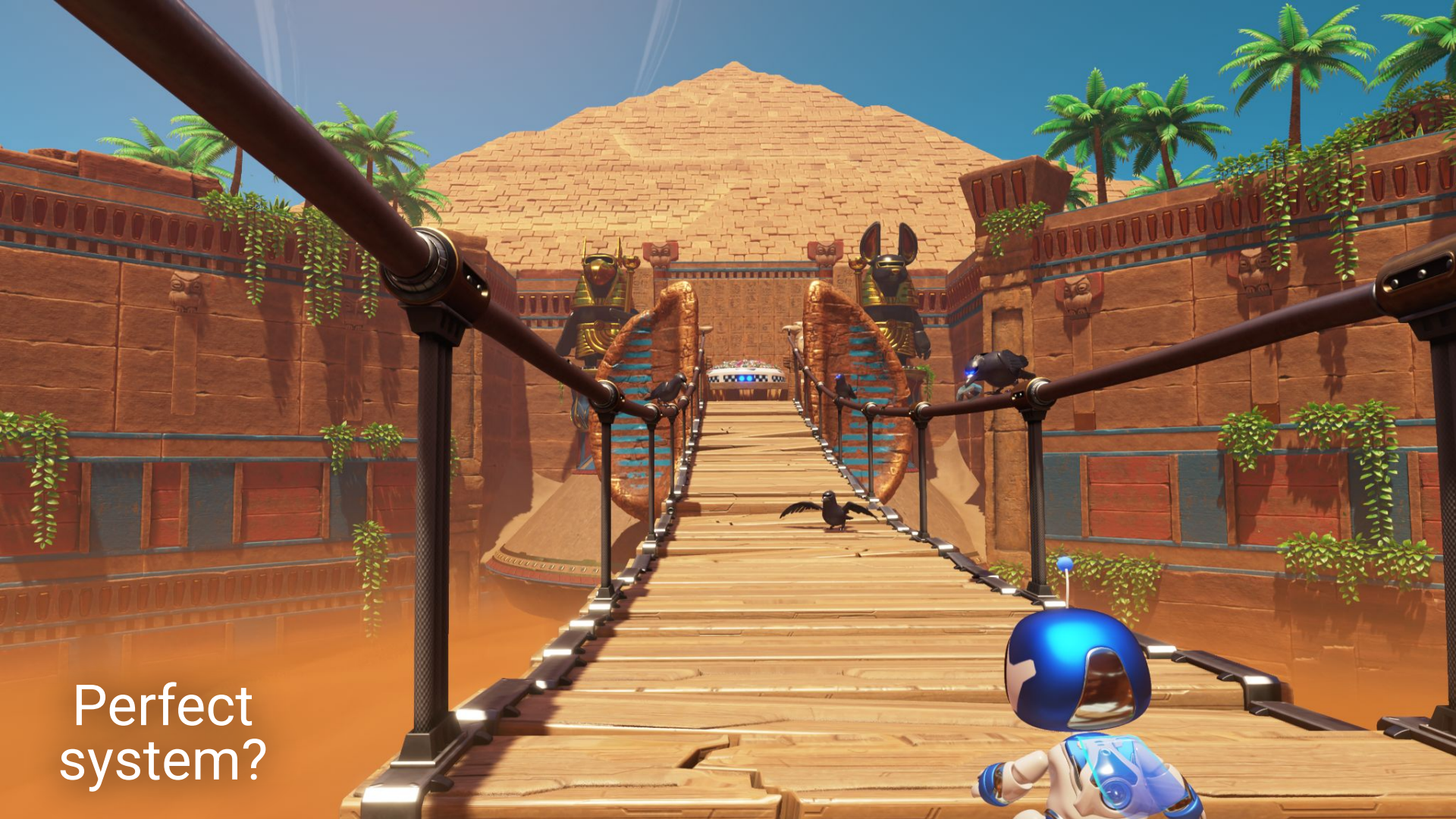
Fully GitOps!

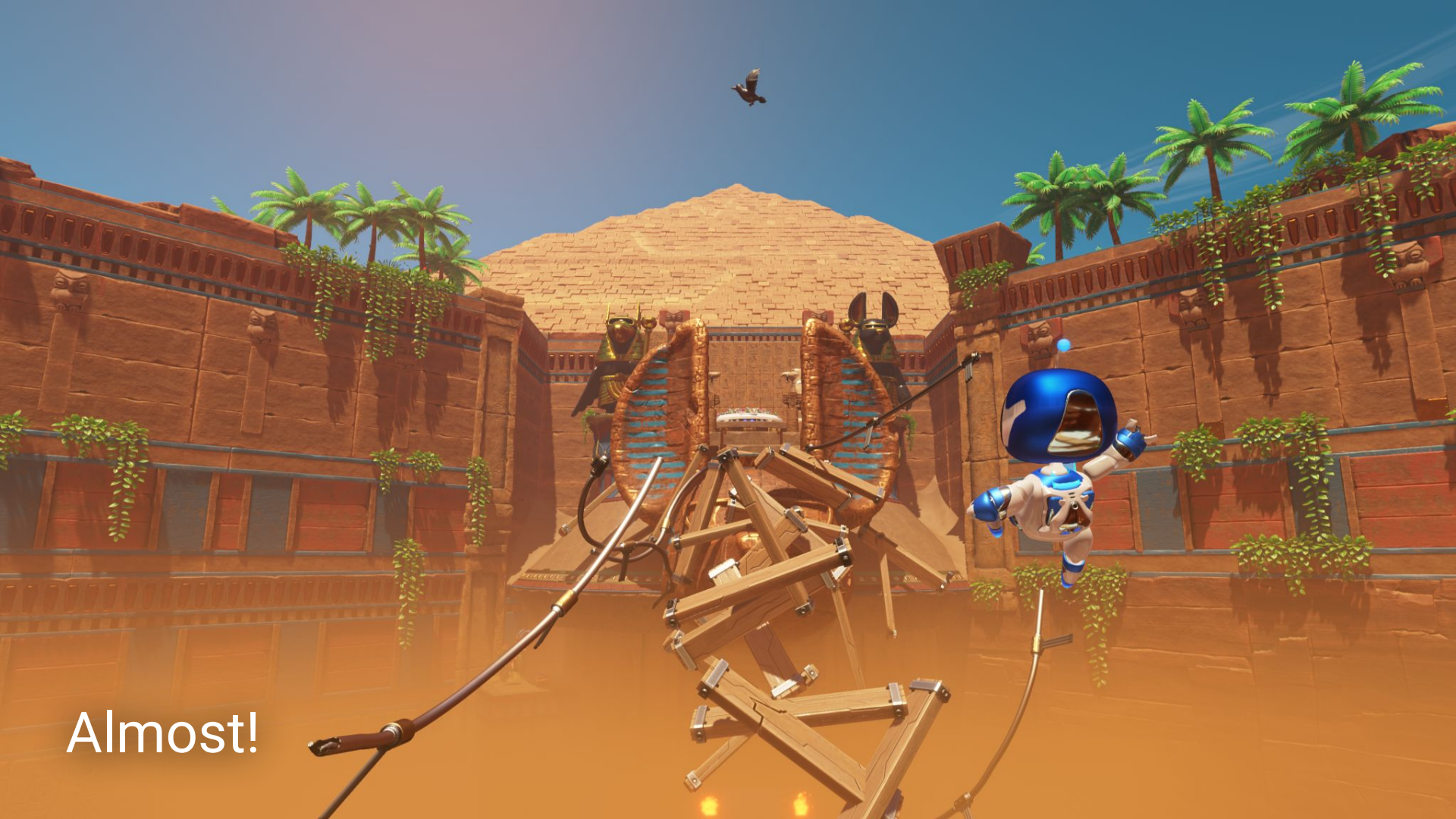




Infra, Apps & Secrets

Perfect
system?





Almost!

Prod is a living
thing



It must be
maintained





Renovate



Alternatives are
copycats

chore(deps): update ghcr.io/home-assistant/home-assistant docker tag to v2025.4.0

Edit

Code ▾

⋮

 Open Renovate Bot requested to merge `renovate/ghcr.io-home-assi...` into `main` 22 hours ago

Mark as done

⏪ Expand

Overview **0** Commits **1** Changes **1**

This MR contains the following updates:

Package	Type	Update	Change
ghcr.io/home-assistant/home-assistant (source)	Kustomization	minor	2025.3.4 -> 2025.4.0

chore(deps): update ghcr.io/home-assistant/home-assistant docker tag to v2025.4.0

Edit

Code ▾

⋮

Open

 Renovate Bot requested to merge `renovate/ghcr.io-home-assi...` into `main` 22 hours ago

Overview 0

Commits 1

Changes 1

Mark as done

Compare `main` ▾ and `latest version` ▾

1 file +1 -1

▾

▾ home-assistant/overlays/k8s-server/kustomization.yaml

+1 -1

☐ Viewed

⋮

@@ -6,7 +6,7 @@ namespace: home-assistant	@@ -6,7 +6,7 @@ namespace: home-assistant
6 images:	6 images:
7 - name: hass	7 - name: hass
8 newName: ghcr.io/home-assistant/home-assistant	8 newName: ghcr.io/home-assistant/home-assistant
9 - newTag: 2025.3.4	9 + newTag: 2025.4.0
10 - name: mosquitto	10 - name: mosquitto
11 newName: eclipse-mosquitto	11 newName: eclipse-mosquitto
12 newTag: 2.0.21	12 newTag: 2.0.21

Yes, it was too
simple





If we
render?

No Problem!



```
{
  $schema: 'https://docs.renovatebot.com/renovate-schema.json',
  extends: [ ],
  ""
  postUpgradeTasks: {
    commands: ['task renovate:update'],
    fileFilters: ['**'],
    executionMode: 'branch',
  },
}
```


chore(deps): update helm release kube-prometheus-stack to v70.4.1 [renovate/kube-prometheus-s...](#) into [main](#)

Overview 0 Commits 1 **Changes 4**

Add a to-do item

▼ monitoring/overlays/k8s-server/prometheus/prometheus.yaml		+52 -20 ☐ Viewed
71088	app.kubernetes.io/instance: prometheus	71088 app.kubernetes.io/instance: prometheus
71089	app.kubernetes.io/name: grafana	71089 app.kubernetes.io/name: grafana
71090 -	app.kubernetes.io/version: 11.5.2	71090 + app.kubernetes.io/version: 11.6.0
71091	spec:	71091 spec:
71092	automountServiceAccountToken: true	71092 automountServiceAccountToken: true
71093	containers:	71093 containers:
⌵	@@ -71197,7 +71197,7 @@ spec:	
⌴		
71197	value: /var/lib/grafana/plugins	71197 value: /var/lib/grafana/plugins
71198	- name: GF_PATHS_PROVISIONING	71198 - name: GF_PATHS_PROVISIONING
71199	value: /etc/grafana/provisioning	71199 value: /etc/grafana/provisioning
71200 -	image: docker.io/grafana/grafana:11.5.2	71200 + image: docker.io/grafana/grafana:11.6.0
71201	imagePullPolicy: IfNotPresent	71201 imagePullPolicy: IfNotPresent
71202	livenessProbe:	71202 livenessProbe:
71203	failureThreshold: 10	71203 failureThreshold: 10
⌵	@@ -71791,9 +71791,9 @@ spec:	
⌴		
71791	summary: An Alertmanager instance failed to send notifications.	71791 summary: An Alertmanager instance failed to send notifications.
71792	expr: -	71792 expr: -
71793	(	71793 (
71794 -	rate(alertmanager_notifications_failed_total{job="prometheus-kube-prometheus-alertmanager",namespace="monitoring"}[5m])	71794 + rate(alertmanager_notifications_failed_total{job="prometheus-kube-prometheus-alertmanager",namespace="monitoring"}[15m])
71795	/	71795 /
71796 -	ignoring (reason) group_left	71796 + ignoring (reason) group_left
	rate(alertmanager_notifications_total{job="prometheus-kube-prometheus-alertmanager",namespace="monitoring"}[5m])	
71797	)	71797)
71798	> 0.01	71798 > 0.01
71799	for: 5m	71799 for: 5m
⌵	@@ -71809,9 +71809,9 @@ spec:	
⌴		



No limit!



Close to
perfection?

chore(deps): update helm release kube-prometheus-stack to v70.4.1

[Edit](#)[Code](#) 

Renovate Bot requested to merge [renovate/kube-prometheus-s...](#) into [main](#) 2 days ago

[Add a to-do item](#)[Expand](#)[Overview](#) **0**[Commits](#) **1**[Changes](#) **4**

This MR contains the following updates:

Package	Update	Change
kube-prometheus-stack (source)	minor	70.3.0 -> 70.4.1

Release Notes

▼ [prometheus-community/helm-charts](#) (kube-prometheus-stack)

[v70.4.1](#)

[Compare Source](#)

kube-prometheus-stack collects Kubernetes manifests, Grafana dashboards, and Prometheus rules combined with documentation and scripts to provide easy to operate end-to-end Kubernetes cluster monitoring with Prometheus using the Prometheus Operator.

What's Changed

- kube-prometheus-stack - Adding imagePullSecret to Admission webhook Jobs by [@arjunbnair97](#) in <https://github.com/prometheus-community/helm-charts/pull/5488>

New Contributors

- [@arjunbnair97](#) made their first contribution in <https://github.com/prometheus-community/helm-charts/pull/5488>

Full Changelog: <https://github.com/prometheus-community/helm-charts/compare/kube-prometheus-stack-70.4.0...kube-prometheus-stack-70.4.1>



Automation FTW!



Disaster management



Recovery

Cluster API



Ready for GitOps!






@davinkevin@davinkevin.fr


Thank you!



@davinkevin@davinkevin.fr



Feedback

Question?





**THANK YOU
FOR
PLAYING**