

THE CUSTOMER

[Tidepool](#) is a 501(c)3 nonprofit organization on a mission to make diabetes data more accessible, actionable, and meaningful for people with diabetes, their care teams, and researchers. Founded in 2013, Tidepool hosts a suite of free software tools for people with diabetes and the clinics that serve them, including Tidepool Web, Tidepool Mobile, Tidepool Uploader, and, pending submission to FDA and associated review, Tidepool Loop.

Their back-end development team is responsible for building and deploying all backend services and managing compute resources associated with operating their services. In 2019, Tidepool [migrated all of their infrastructure to Kubernetes](#).



At Tidepool, we migrated from a non-Kubernetes environment. We had developed these custom deployment tools, but the engineers who wrote those tools are no longer at the company. We were stuck with legacy tools without documentation. ” - Derrick Burns, Backend Engineer

CHALLENGES

Before migrating to Kubernetes, Tidepool’s backend consisted of a distributed system of ~18 microservices written in Node.js and Go that were deployed on Amazon EC2 instances. Through 2018, Tidepool managed their infrastructure using AWS CloudFormation with Lambda and Ansible.

Included among those 18 microservices, were several in-house developed services: an API gateway (styx), a service discovery system (hakken), as well as their own custom load balancing system (shio).

Instead of continuing to invest in their custom tools, Tidepool decided to migrate their services to containers in early 2019, and manage them with Kubernetes using the Amazon Elastic Kubernetes Service (EKS). The team is now running 5 Kubernetes clusters on EKS; the production environment consists of 44 pods that provide for 18 microservices and another 66 pods that provide support services such as their API gateway, telemetry, and logging.

TIDEPOOL

Industry: Software

Location: United States of America

KEY BENEFITS

- GitOps provides a low-risk self-deployment model
- Significant time savings with automated cluster lifecycle management
- Robust and secure platform with built-in auditability

CONTACT US



www.weave.works



sales@weave.works

Lack of support for legacy applications

Prior to their Kubernetes migration, Tidepool developed a number of custom deployment tools in house. The original authors of the tools moved on, leaving the current engineering team without documentation and support. These legacy applications required new features but the team at Tidepool had little time to invest in custom development of infrastructure tooling.

Poor pipeline visibility

Prior to migrating to Kubernetes, the engineering team used a custom tool to deploy software. This tool uses a Git branch per microservice to store configuration data. Git provides a nice audit trail, but the use of so many branches made it difficult to understand the state of the cluster. They sought a similar flow with Kubernetes, without the complexities of multiple git branches.

SOLUTION

Tidepool cites the main reason for adopting Weave Flux and GitOps, was the ability to implement a continuous delivery and a self deployment model for the engineering team without becoming Kubernetes experts.

Tidepool found the adoption of GitOps easy and intuitive. The engineering team trained themselves, using the available documentation and over time, the documentation has further improved with added new features. Another positive was that Weave Flux is a supported tool with strong community engagement so Tidepool were confident that they wouldn't run into the same problems they had before with a lack of resources.

RESULTS

Streamlined workflows

With the migration to Kubernetes and the introduction of Weave Flux, Tidepool was able to replace some of their unsupported tools with a tool that has excellent adoption and community support. Improved stability and higher reliability through automated and proven processes allowed the engineering team to spend more time to accelerate innovation.

Low risk self-deployment model with GitOps

Every member of Tidepool's backend team has direct access to their Kubernetes clusters, but their frontend and QA teams do not. Tidepool wanted to empower the frontend and QA teams to be able to make changes to the images deployed to any kubernetes cluster, but at the same time needed security guardrails in place so services are not impacted.

While the creation of team namespaces could have created a similar separation of concerns, the team did not want to invest time in operating Kubernetes.

In order for developers to deploy a branch without editing YAML configuration files, the Tidepool team wrote a new tool called Tidebot that listens to comments made to a Pull Request (essentially a deployment call via pull request).

When the bot hears a request such as:

```
/deploy qa1
```

it updates the image tag pattern field in a Flux managed resource and commits that change to the configuration repo:

```
fluxcd.io/tag.shoreline: glob:db-jwt-*
```

This instructs Weave Flux to install the latest image whose name is a prefix of db-jwt-.

With this new workflow in place, the team was able to reduce their operational tasks and focus on creating code for innovative new features.



“For Kubernetes, Gitops provides a simple audit trail that is invaluable in figuring out what has broken. Flux (and our Tidebot) give our developers a low-risk self-deployment option. Together, Flux and GitOps accelerate our innovation.” **Derrick Burns, Backend Engineer**

Improved security and auditability

With a GitOps pull pipeline in place, Tidepool's cluster credentials are not exposed outside of their production environment which drastically reduces the attack surface area. The team accesses only one file, and in fact just one line of the file instead of being exposed to all configuration resource files.

The automated GitOps workflow also results in a simple audit trail which provides invaluable insight into determining the root cause of failures or errors that need addressing.

Increased productivity

The newly implemented GitOps workflow in combination with Tidebot allows developers to deploy new branches with a single comment in GitHub. The entire team embraced this new workflow immediately which resulted in a significant increase in the number of deployments and the deployment frequency.