CLOUDFLARE

How Replicated uses Cloudflare Access to develop remotely

REPLICATED

*This story was adapted from an original guest post written by Marc Campbell and Grant Miller, co-founders of **Replicated**. For a more in-depth look at how Campbell and Miller leveraged Cloudflare Access and Argo Tunnel to develop a cloud-based IaaS solution, visit the **Cloudflare Blog.***

There is no doubt that the world is becoming more Internet-connected, and that deployment environments are becoming more complex. It stands to reason that it's only a matter of time before all software development happens through and in concert with the Internet.

Founded in 2014, Replicated is an infrastructure software company with a focus on enabling a new model of enterprise software delivery called Kubernetes Off-The-Shelf (KOTS) Software. Their goal is to make it easy for users to install and operate third party software, so that sending data to multi-tenant SaaS providers isn't the only way to use those providers' services.

"We think that it's possible and easy to bring the applications to your data, securely and without a lot of operational overhead," Campbell and Miller say.

Key Results

- Developers can reach development tools from anywhere in the world without a VPN
- Replicated's development environment now runs entirely on IaaS
- Employees have the same seamless login experience accessing any workplace application

The Challenge

At Replicated, the development environment needs to run on Kubernetes, since KOTS runs in Kubernetes and manages the lifecycle of 3rd-party applications in the Kubernetes cluster. Building and validating the product requires a developer to have access to a cluster.

Since Replicated's engineering team had grown to include dedicated front end engineers and other specialists who shouldn't have to worry about building and maintaining their own cluster, the complexity of managing a local environment became a burden. They needed to simplify in order to maintain developer productivity.

"We'd lose hours every week from engineers troubleshooting their local environments," Campbell and Miller explain. "When a front end engineer (who wasn't expected to be a Kubernetes expert) would have issues, they'd need to pair and get help from a backend engineer; consuming not just one but two people's valuable time. We needed something better."

While searching for a solution that would be simple to implement and maintain, Replicated turned to Cloudflare. Initially, they had used Cloudflare for DNS and DDoS protection, but over time, they started to utilize additional Cloudflare services to help keep their own services available and secure.

Replicated uses Cloudflare to secure their development environment in the cloud

Replicated has designed a solution that uses cloud-based infrastructure components, accessed and secured with Cloudflare Access and Argo Tunnel, to move their development environment to Infrastructure as a Service (IaaS) resources. This means that their entire development environment is in the cloud.

As a result, they've reduced the amount of time that a developer spends troubleshooting their local environment, allowing every engineer on the team to maintain a full stack development environment — even if they are without deep Kubernetes expertise.

"This configuration has several advantages over a traditional deployment," say Campbell and Miller. "For one, the server does not have a public IP and we don't need to have any ports open in the Google Load Balancer, including for SSH. The only way to connect to these servers is through the Argo Tunnel, secured by Cloudflare Access. Access provides a BeyondCorp-style method of authentication, which ensures that the environment can be reached from anywhere in the world without the use of a VPN."

"Cloudflare Access provides a BeyondCorp-style method of authentication, which ensures that the environment can be reached from anywhere in the world without the use of a VPN."

MARC CAMPBELL AND GRANT MILLER
Co-founders

Cloudflare Access puts security fears to rest

Now, Replicated can write a policy that defines which machines a user should have access to and trust that it will be applied everywhere. Instead of managing SSH certificates (which are long-living and hard to revoke), they can allow developers to login with the same Google credentials they use everywhere else. Even if a developer leaves, they can revoke those credentials instantly, so they don't have to worry about any public keys they still might have lying around.

With Cloudflare Access, Replicated's developers can easily set up multiple environments (to try out a new k8s version, for example), and they don't need the biggest and most powerful laptops to do so. They can also choose their local OS and environment (MacOS, Windows, Linux) because every version is supported, as long as SSH is also supported. And, since code does not live on a developer's laptop, it doesn't travel with them to coffee shops or other insecure places. This is a key benefit when it comes to security, since losing a laptop no longer means that the codebase is compromised along with it.

"With the help of Cloudflare Access and Argo Tunnel, every development environment has become a collaborative place," Campbell and Miller say.

“This is great when two engineers aren’t in the same room. Also, we’re less attached to our development environments — if my server isn’t working properly for unknown reasons, instead of troubleshooting it for hours, I can delete it and get a new clean one.”

For an online copy please visit
https://www.cloudflare.com/case-studies/how-replicated-uses-cloudflare-access-to-develop-remotely/