K8s secrets in environment variables

Author: Greg Castle [destijl]
Updated: 2019-03-22
Status: Rough notes for sig-auth

Matt Moore started an internal Google discussion over Knative API plans for secrets I'd like to bring to sig-auth. The question they are grappling with is whether they should allow people to deliver secrets using environment variables as K8s does.

This is generally accepted as a terrible idea for security. I personally wish we hadn't allowed it in Kubernetes, or if we allowed it at all that it requires you to set a --insecure-env-secrets=true flag, so you need to opt-in to bad security. Auditors can put this on their checklists, orgs that care about security will mandate it is false, and use will gradually decline.

The original reasoning was that people will do worse things if we don't support this via secrets because it is difficult to avoid using env vars if you don't have control of the software you're running (examples documented in the issue). While this is absolutely true, we'd be in a stronger position if we defaulted it to off. That ship has sailed and it's easy to say these things in hindsight. So what to do now?

Matt says about half of all helm charts use the env var approach, and there's probably 1000s of howtos and blogs we'll never fix.

Proposals:

- More actively discouraging use of env vars for secrets in K8s official docs (we said we'd do that in the original bug but never did). We're actively setting the wrong example.

- Adding a --insecure-env-secrets flag that defaults to true to maintain current behavior, but as a way for orgs to purge use of environment variables in their stack and then shut the door at the cluster level to stop them creeping back in. Eventually make it a security profile or PSP thing. Eventually some time after that default it to false.