A Story of Vault

How PostFinance adopted HashiCorp Vault for its use cases

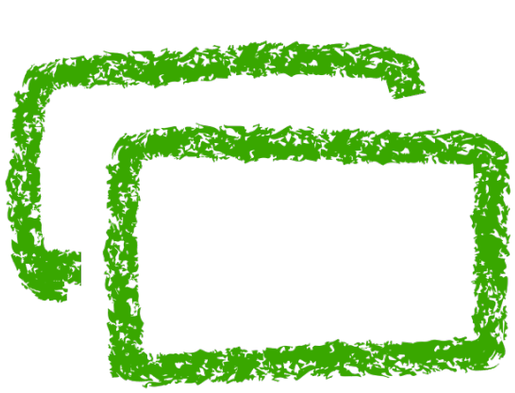
Agenda

- Facts & Figures
- Success Story
- Failure Stories
- Lessons Learned & Next Steps

Facts & Figures

Facts & Figures I

300 applications

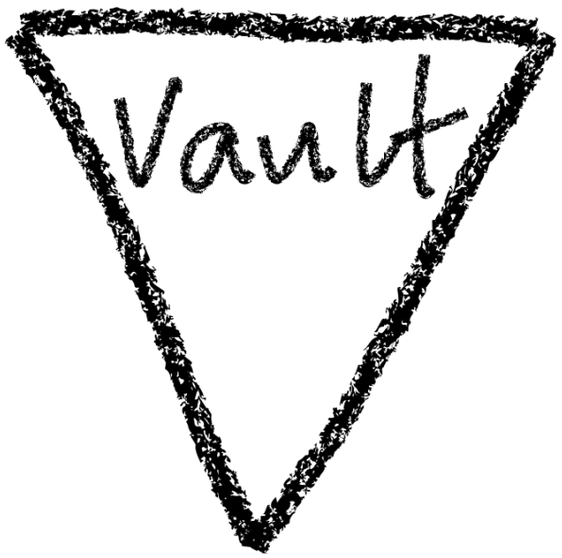


2000 virtual machines

50 application namespaces

14 Kube clusters

Facts & Figures II



800'000 requests/day

100'000 decrypts from Puppet/day

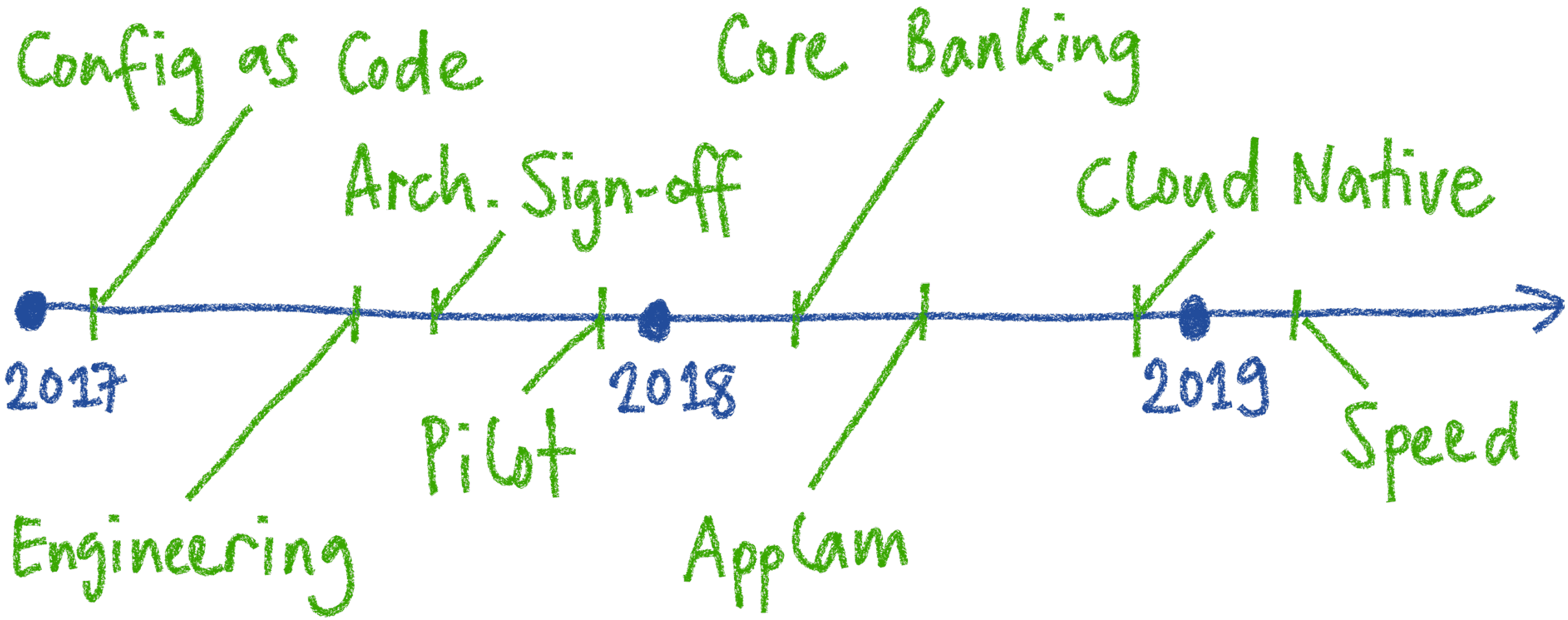
3'000 AppRole logins/day

40 Kube logins/day

30 personal logins/day

Success Story

Timeline


Config as Code
Arch. Sign-off
Core Banking
Cloud Native
2017
2018
2019
Engineering
Pilot
AppCam
Speed

2017-02: Config as Code

central webapp holds application & middleware config

app = foo
port = 7042
cert = my.pem
cert.pass = 1234

git

?

current state → desired state

Use Case #1!

Variants

Develop know-how

Workshops

Prototyping

Calls with HashiCorp

2017-06: Setup & Engineering of Vault

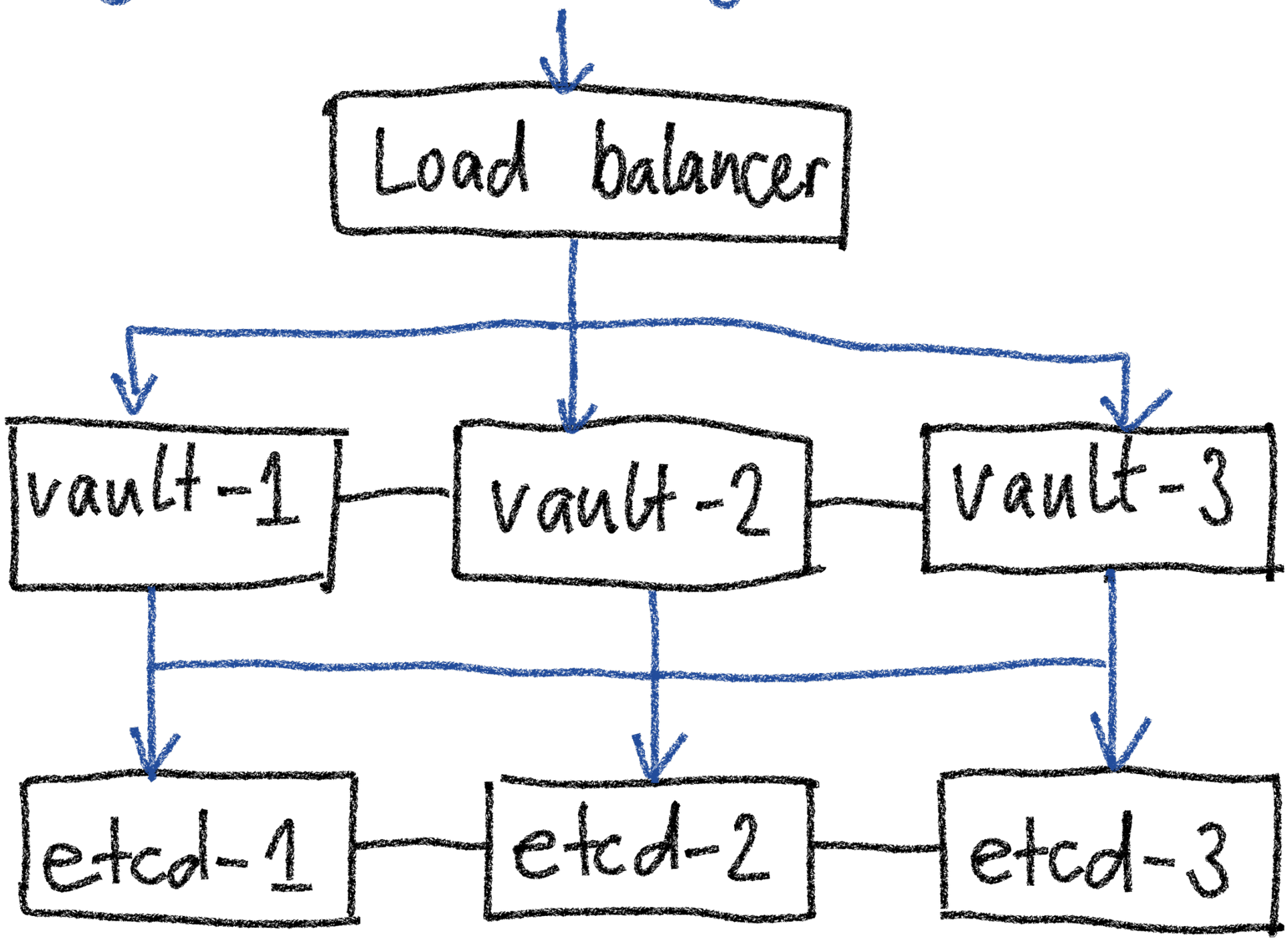
① High availability

② System integration

③ Unsealing

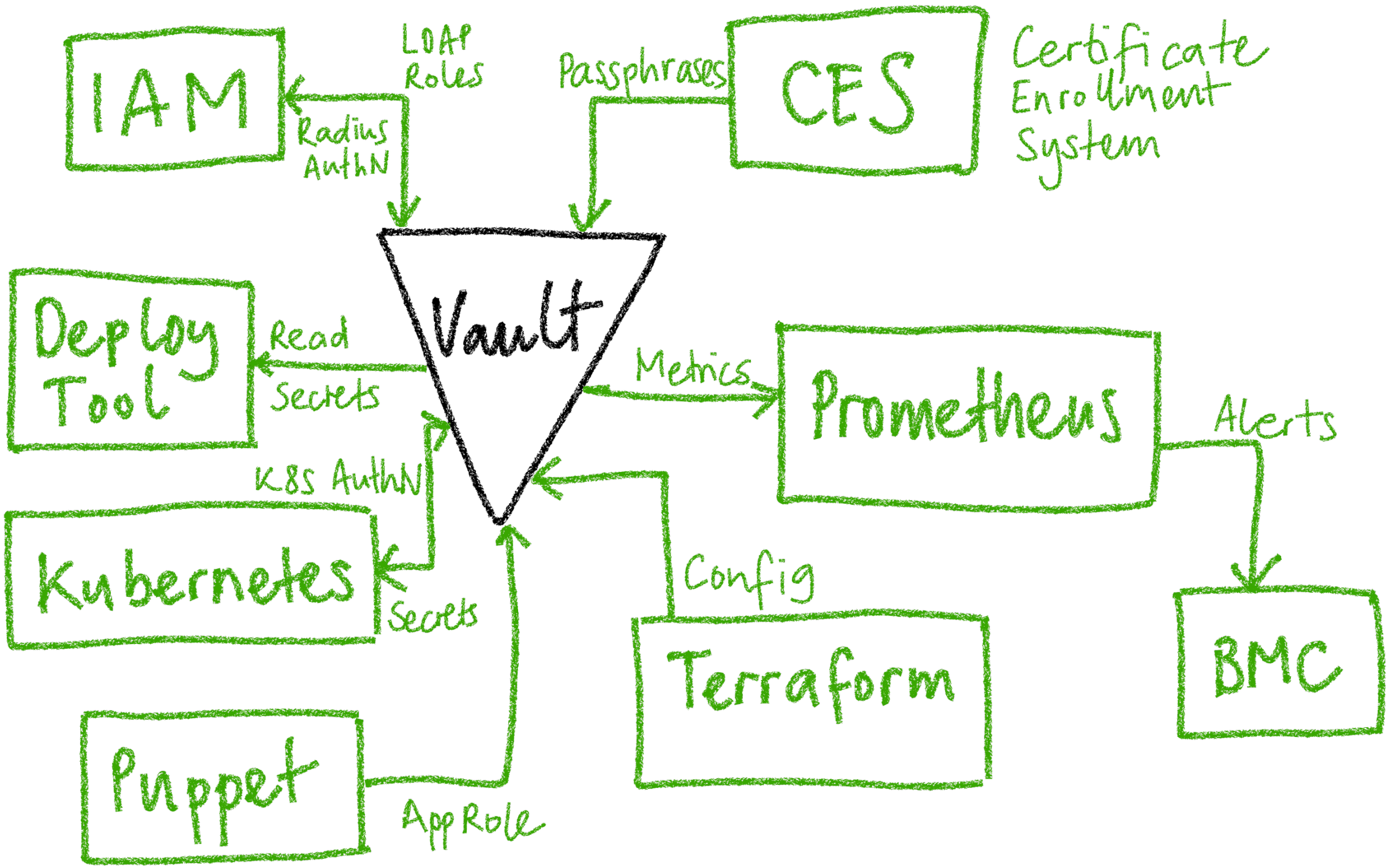
④ Decoupling

① High Availability

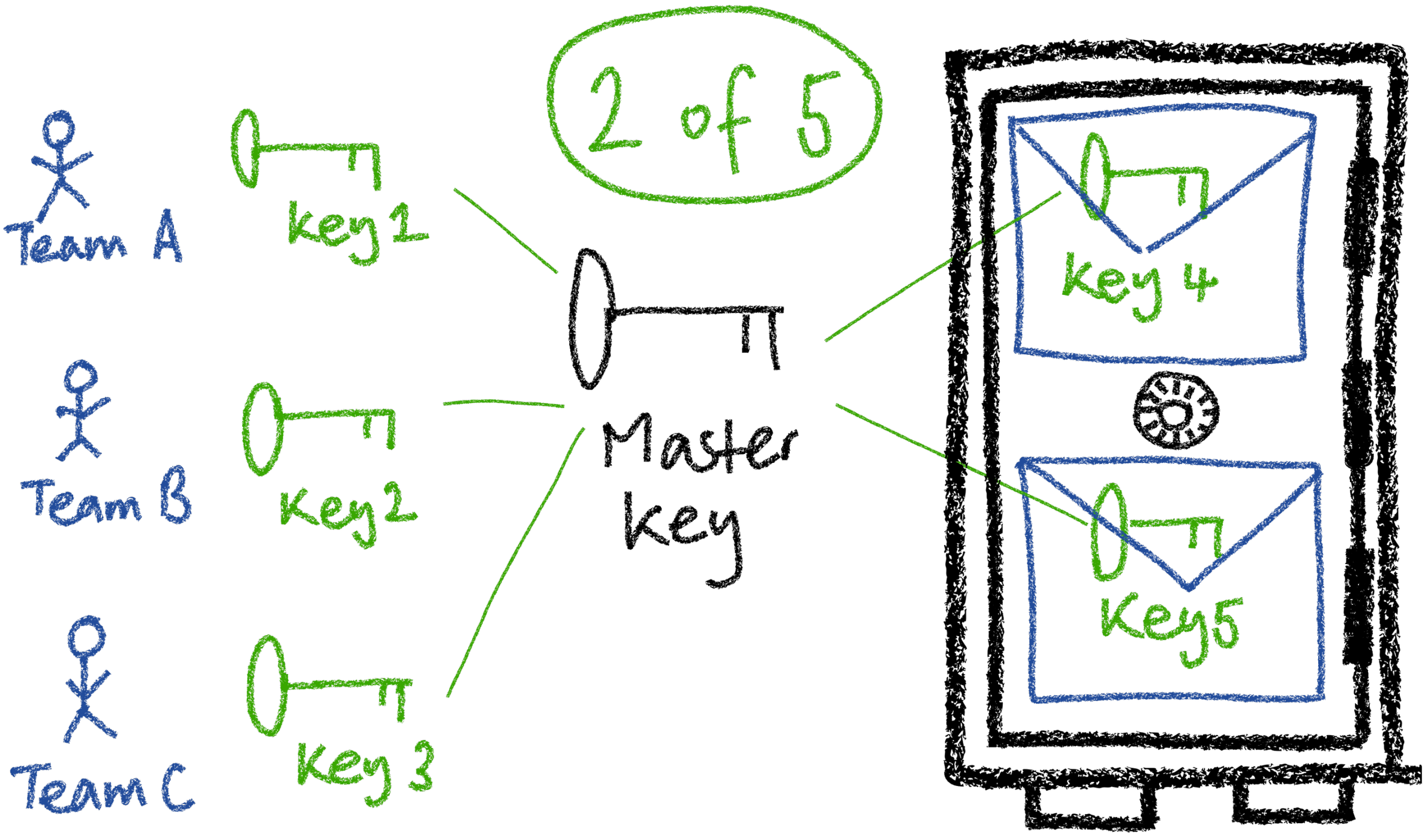


Why etcd ?

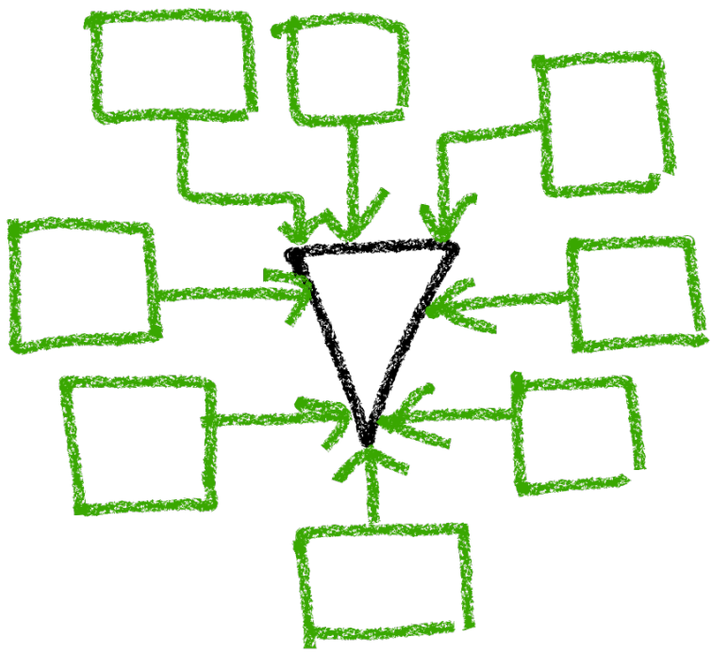
② System Integration



③ Unsealing



④ Decoupling



Vault is a new central component

Downtime could mean bad press!

Applications only have a deploy time dependency, not at runtime.

2017-08 : Architecture Sign-off

Evaluation ?

Nope...

Cost ?

100 man-days

8 VMs

NO Licenses

Licenses ?

We stick with open source

→ Yep, no UI !

→ Yep, no vendor support !

2017-11: Pilot in Production

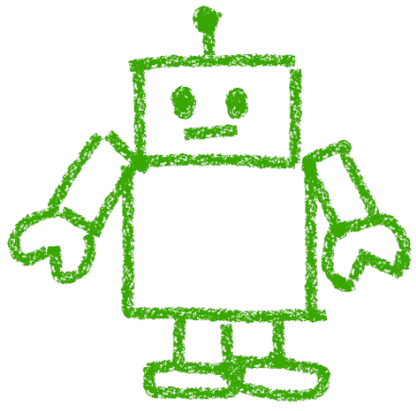
Hand-over to operations

Gain some experience for "big bang" in Spring 2018

Use Case #2

Spaces for teams, i.e. get rid of KeePass

Use Case #3



Robotics

2018-03: Go-live new Core banking

CES writes all 4'2000 cert passphrases to Vault

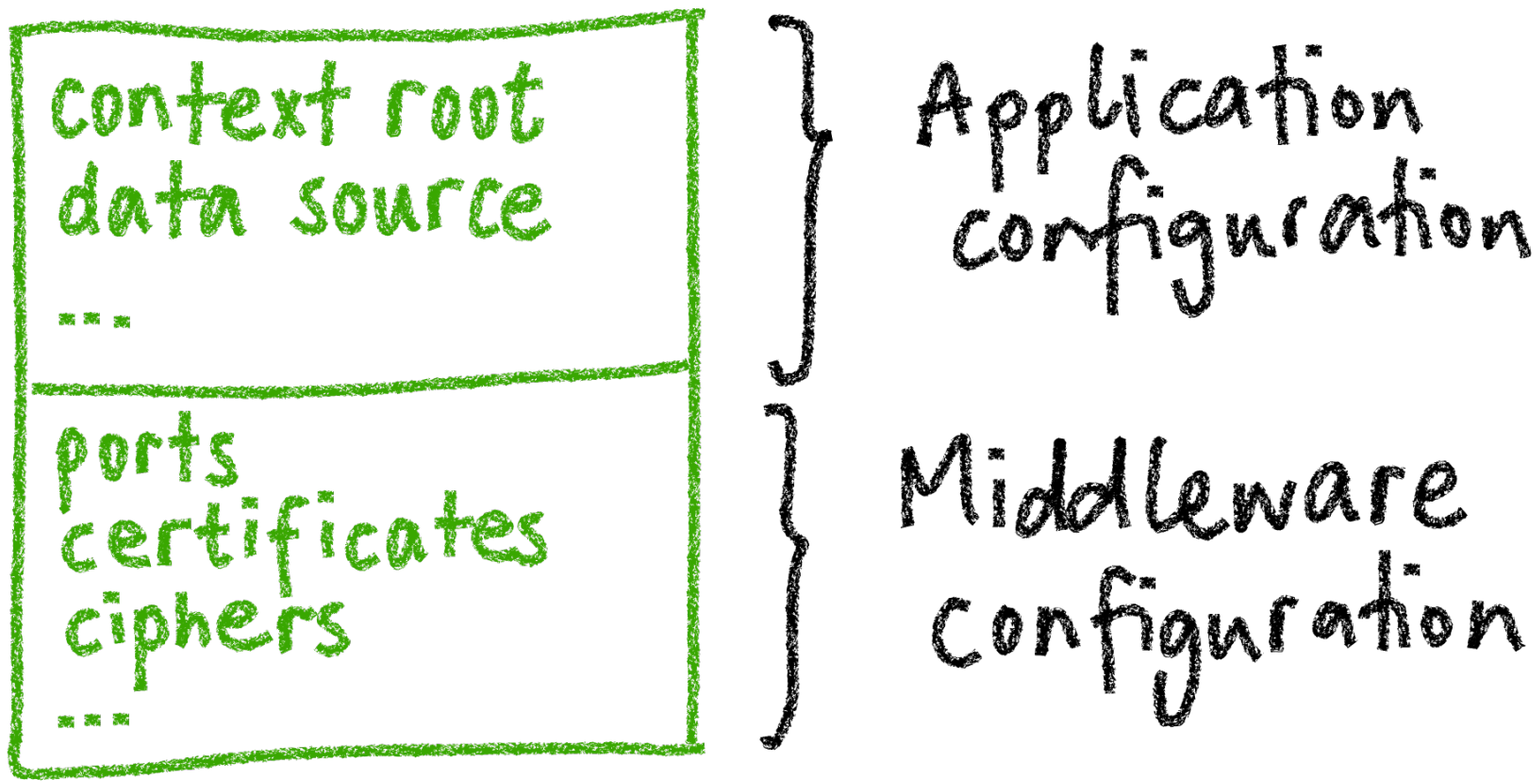
2000 more secrets are migrated to Vault

A LOT of testing and dry-run deployments

During release weekend: Vault is stable, no issues with deployments ☺

2018-06: APPLAM!

= Secrets for APPLication teAMs ☺



Use Case #4

2018-11: Going Cloud Native

Use Case #5

Integration with Terraform

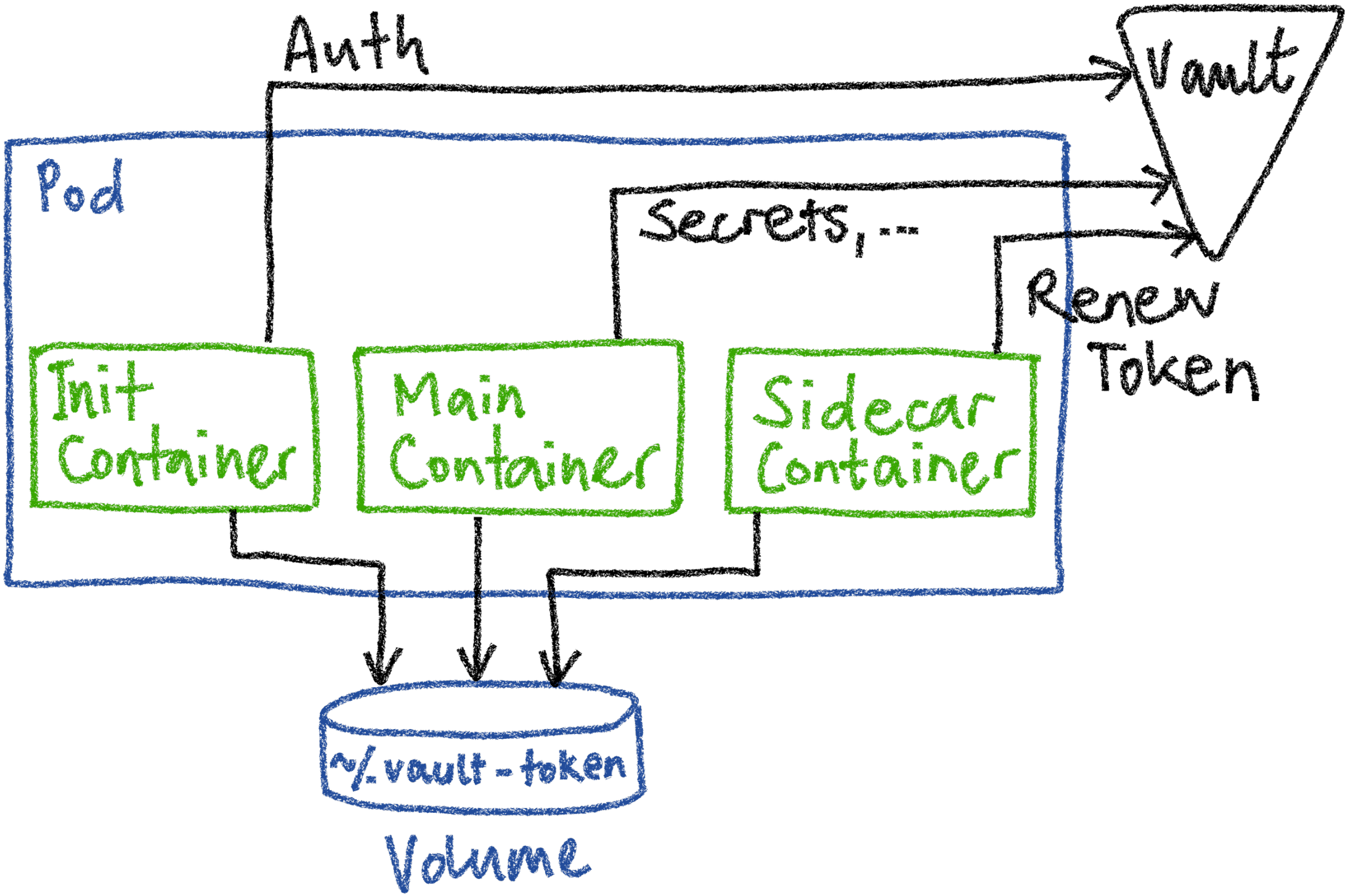
max ttl issues ☹

Use Case #6

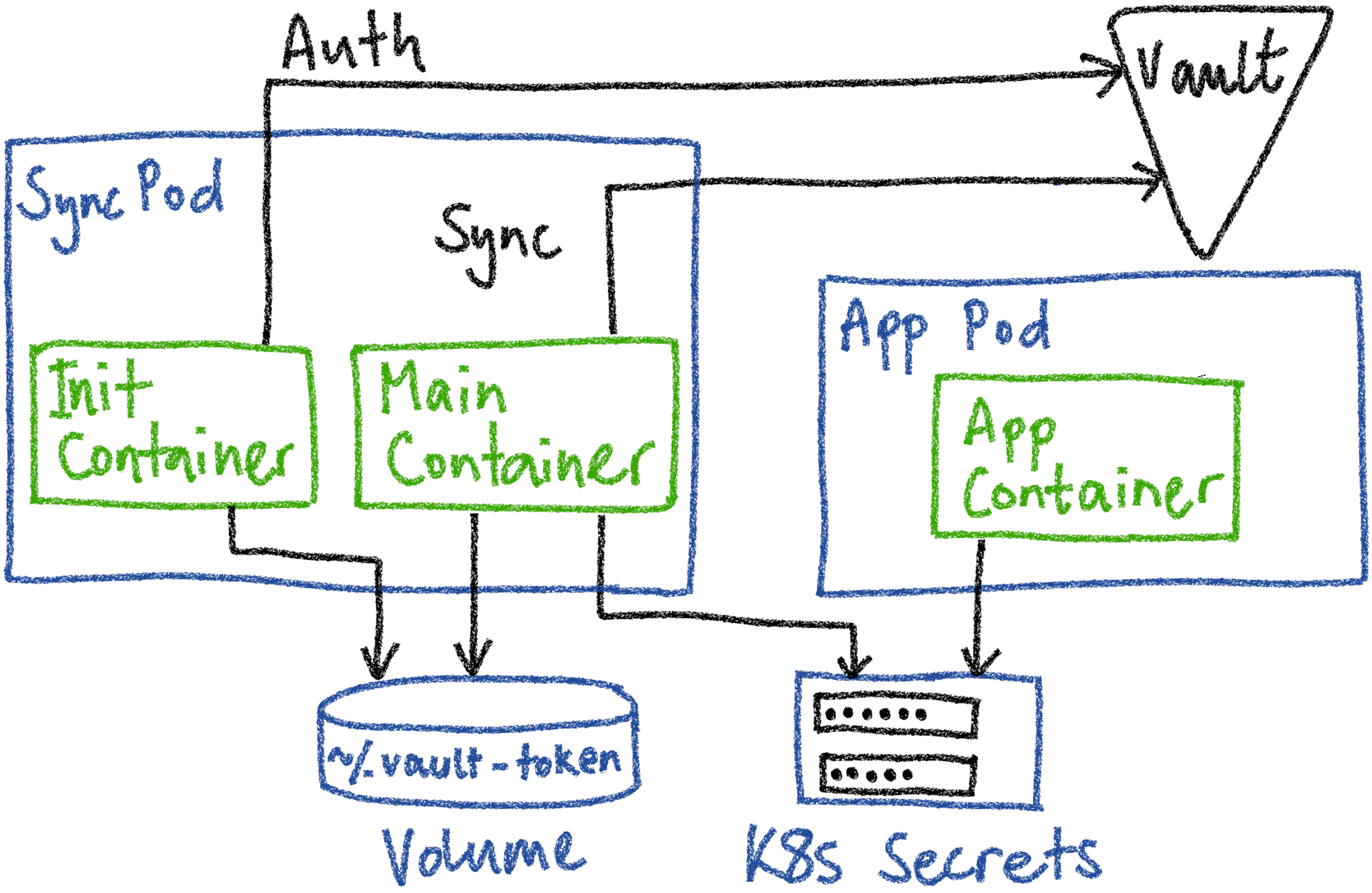
Integration with Kubernetes

Vault vs Kube secrets ?!?

K8s Integration via Token



K8s Integration via Secrets



2019-02 : Need for Speed

Use Case #7

Compliance

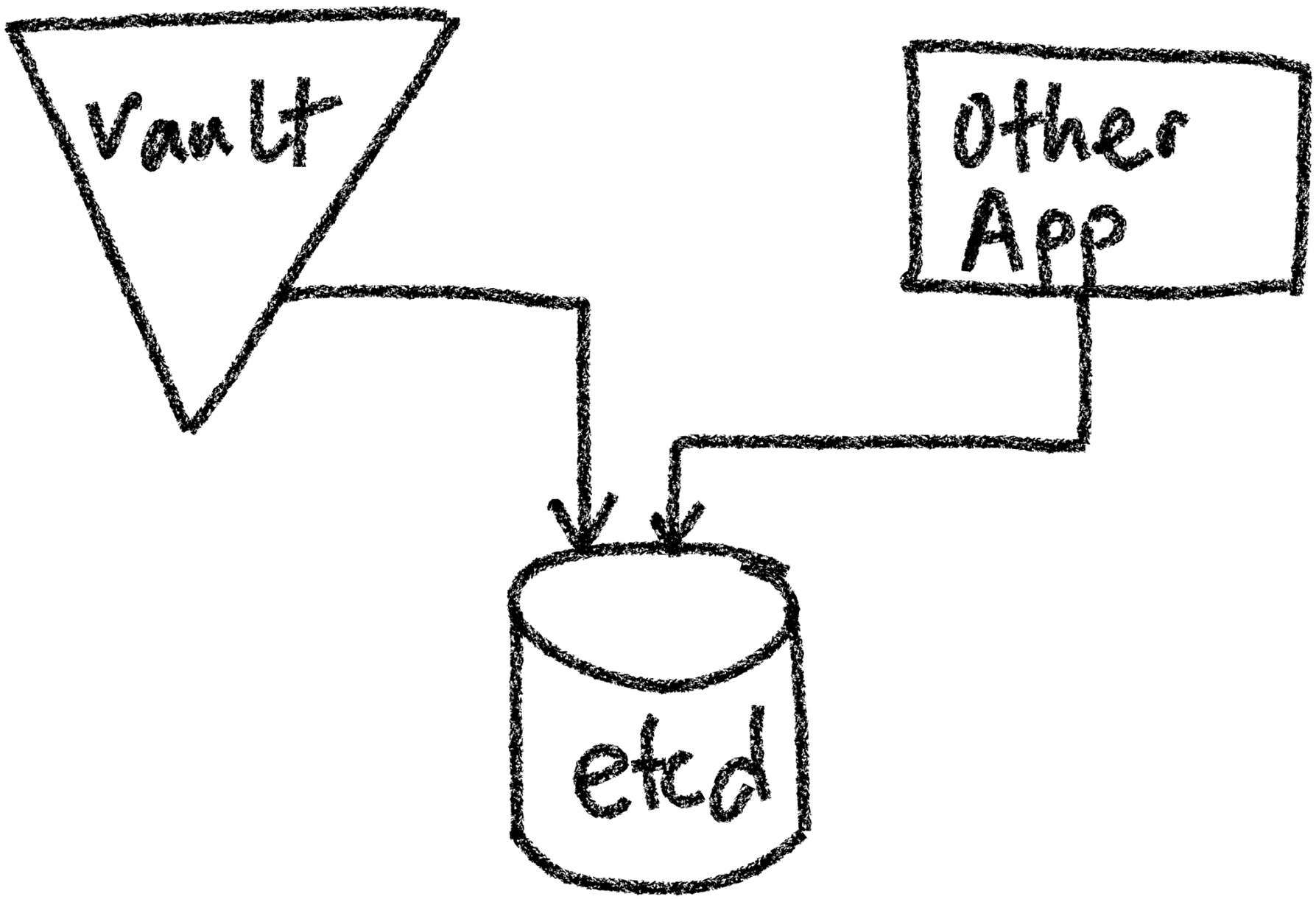
Root passwords must be changed each quarter

Engineers

No problem, we change them every day!

Failure Stories

Failure #1: Shared etcd



Failure #2: Upgrade

Vault 0.10.3 (2018-06-20)
AppRole bug [GH-4981]

↳ Puppet, CES & Deploy Tools fail!

↳ Downgrade!
Setup test instance like prod
Add integration tests

Failure #3 : Upgrade II

Vault 1.2.1 (2019-08-06)

AppRole bug [GH-7270]

↳ Puppet, CES & Deploy Tools fail !

↳ Downgrade !

Add more tests

Choose upgrade time wisely

Lessons Learned & Next Steps

Lessons Learned

- Right people, mindset and skills are key!
- Vault is very stable
- Very good API, easy integration
- Backups & emergency unseal keys are important
- Wrong keystore passphrases are gone
- Simplifies overall configuration
- No passwords in Git anymore
- Iterative approach is good
- Developers are happy ☺
- Security folks are happy, too! ☺☺

Next Steps

Security Audit

Response Wrapping

Auto Unseal

Dynamic Secrets

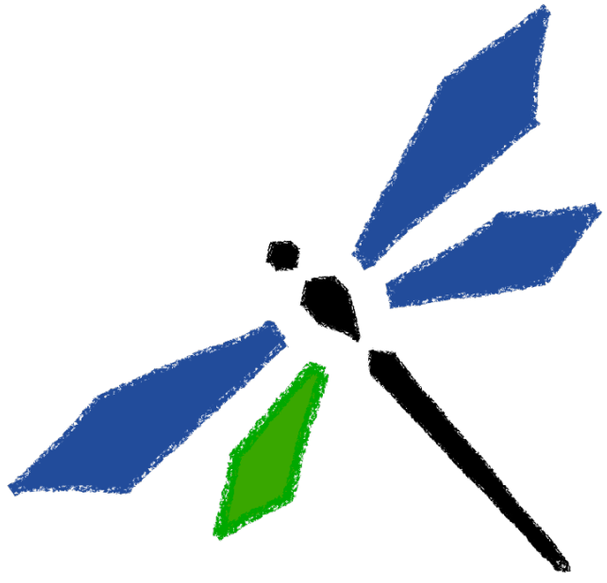
PKI Certificates

... ?

$ whoami

Johann Gyger

@-jogy-



Levingo

Cloud Native
Ambassador

Links

https://github.com/postfinance/vault-kubernetes

https://itnext.io/effective-secrets-with-vault-and-kubernetes-9af5f5c04d06

https://medium.com/@_jogy_/secure-config-as-code-4fd44e277482

https://www.youtube.com/watch?v=Ip8eTPj3Jsk