Exploring HashiCorp Vault and Argo CD: the GitOps Way

GitOps Con EUROPE

17 May 2022 I Valencia, Spain

Tracy P Holmes

Developer Advocate

Codefresh

01

GitOps & Argo CD

What are these things?!

GitOps

https://opengitops.dev

- The system is described in a declarative manner.
- The definition of the system is versioned and audited.
- A software agent automatically pulls the Git state and matches the platform state.
- The state is continuously reconciled.

GitOps

A few benefits…

- Deploying faster and more often,
- Easier and quicker error handling and recovery
- Self-documenting deployments.
- Elimination of configuration drift.

Argo CD

https://argoproj.github.io/cd/

What & Why

Argo CD is a declarative, GitOps continuous delivery tool for Kubernetes.

Application definitions, configurations, and environments should be declarative and version controlled. Application deployment and lifecycle management should be automated, auditable, and easy to understand.

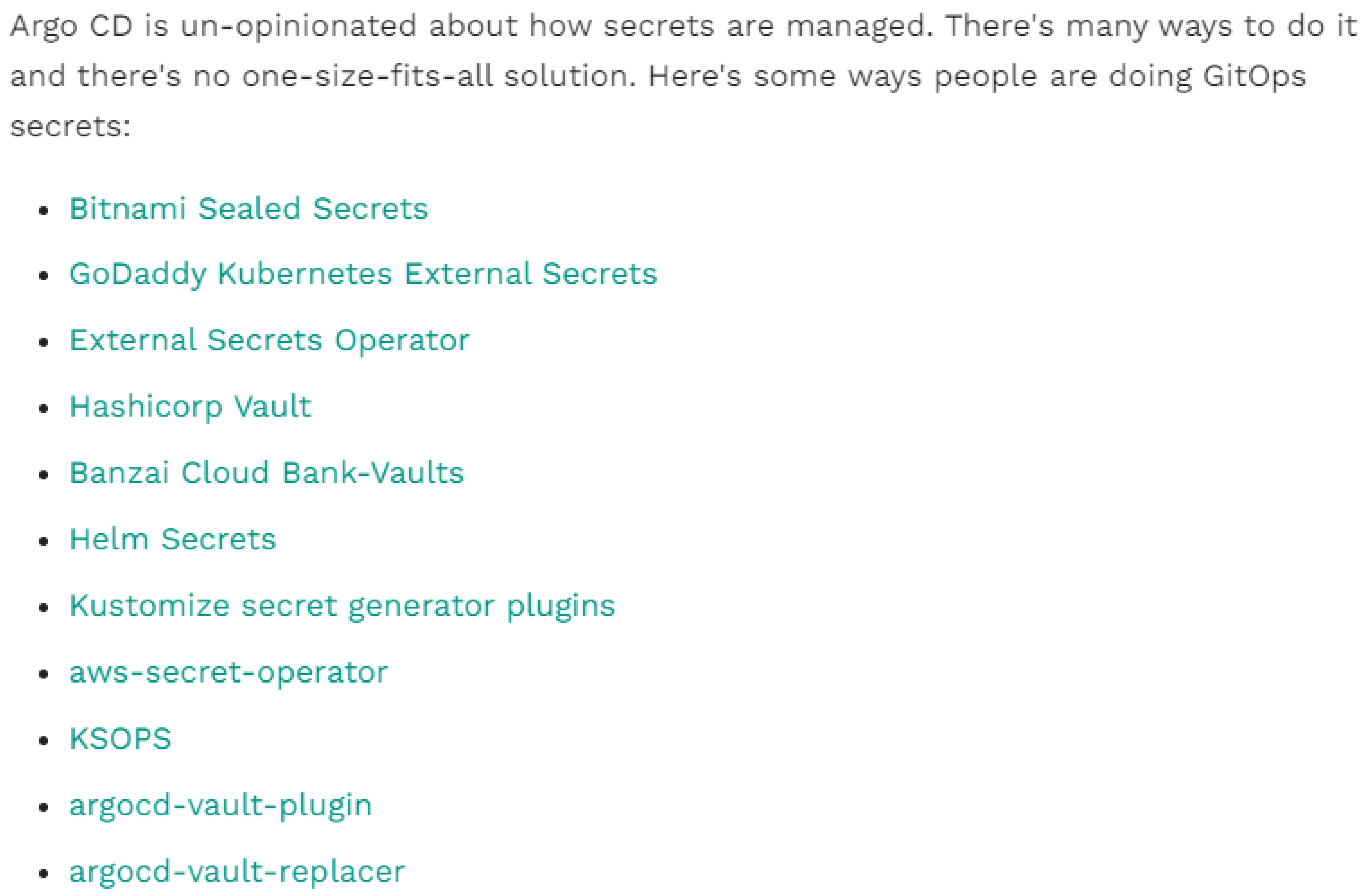
Secrets.

shhhhhhhh...🤫

Why are secrets important?

…and can I use them with GitOps

Argo CD and Secret Management



Argo CD is un-opinionated about how secrets are managed. There's many ways to do it and there's no one-size-fits-all solution. Here's some ways people are doing GitOps secrets:

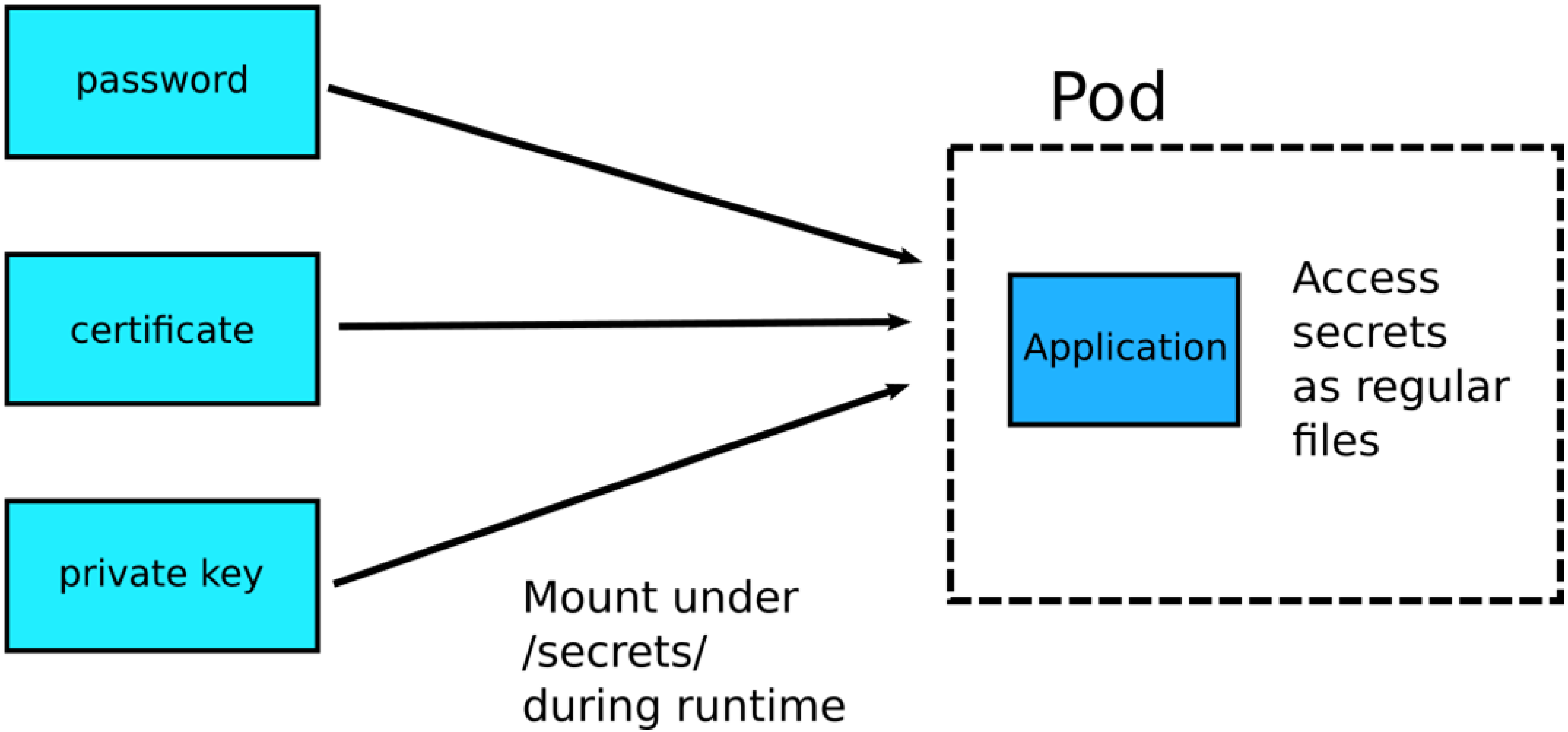
- Bitnami Sealed Secrets
- GoDaddy Kubernetes External Secrets
- External Secrets Operator
- Hashicorp Vault
- Banzai Cloud Bank-Vaults
- Helm Secrets
- Kustomize secret generator plugins
- aws-secret-operator
- KSOPS
- argocd-vault-plugin
- argocd-vault-replacer

https://argo-cd.readthedocs.io/en/stable/operator-manual/secret-management/

Tools I hear about

GitOpsCon EUROPE

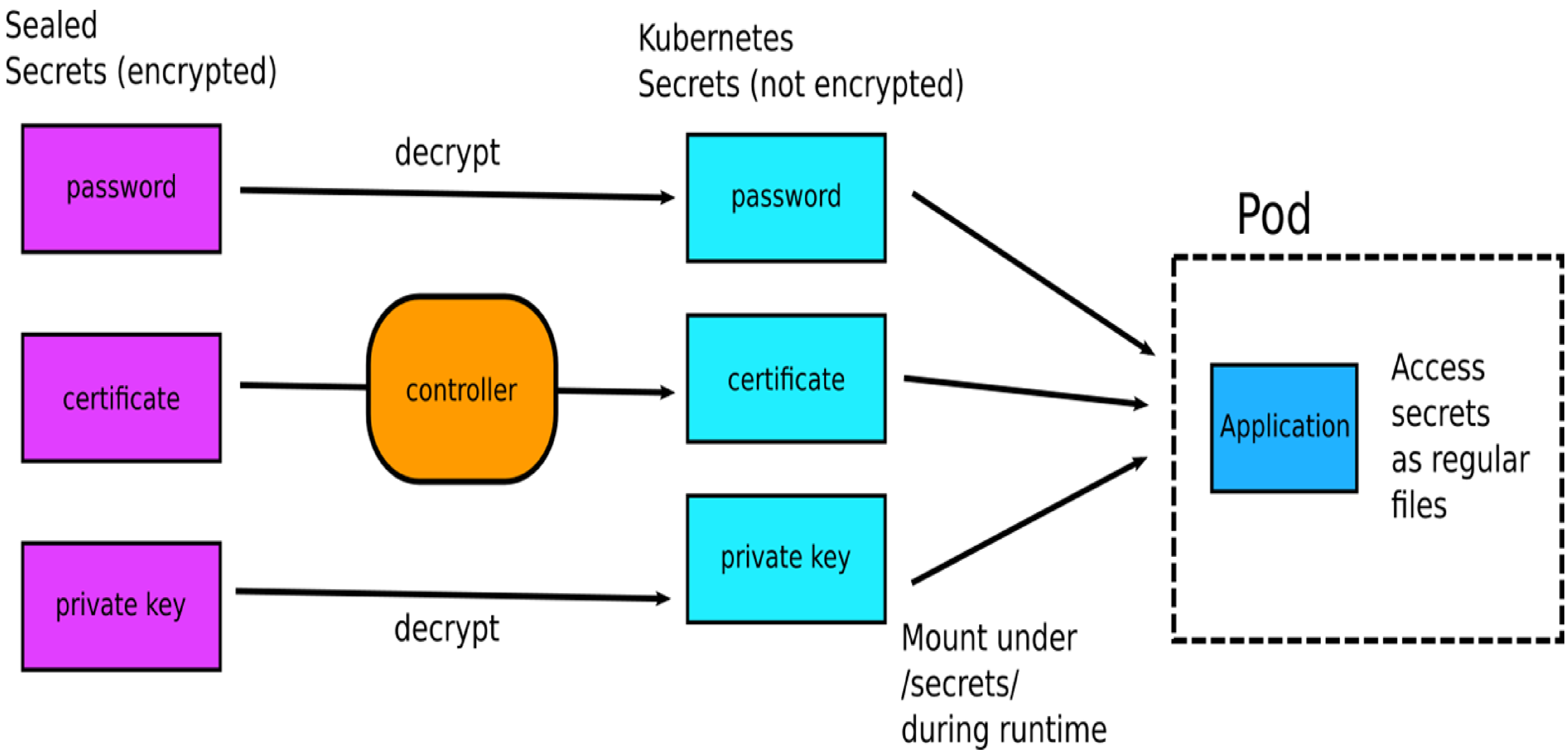
Kubernetes secrets (not encrypted)


password
certificate
private key
Pod
Application
Access secrets as regular files
Mount under /secrets/ during runtime

Tools I hear about

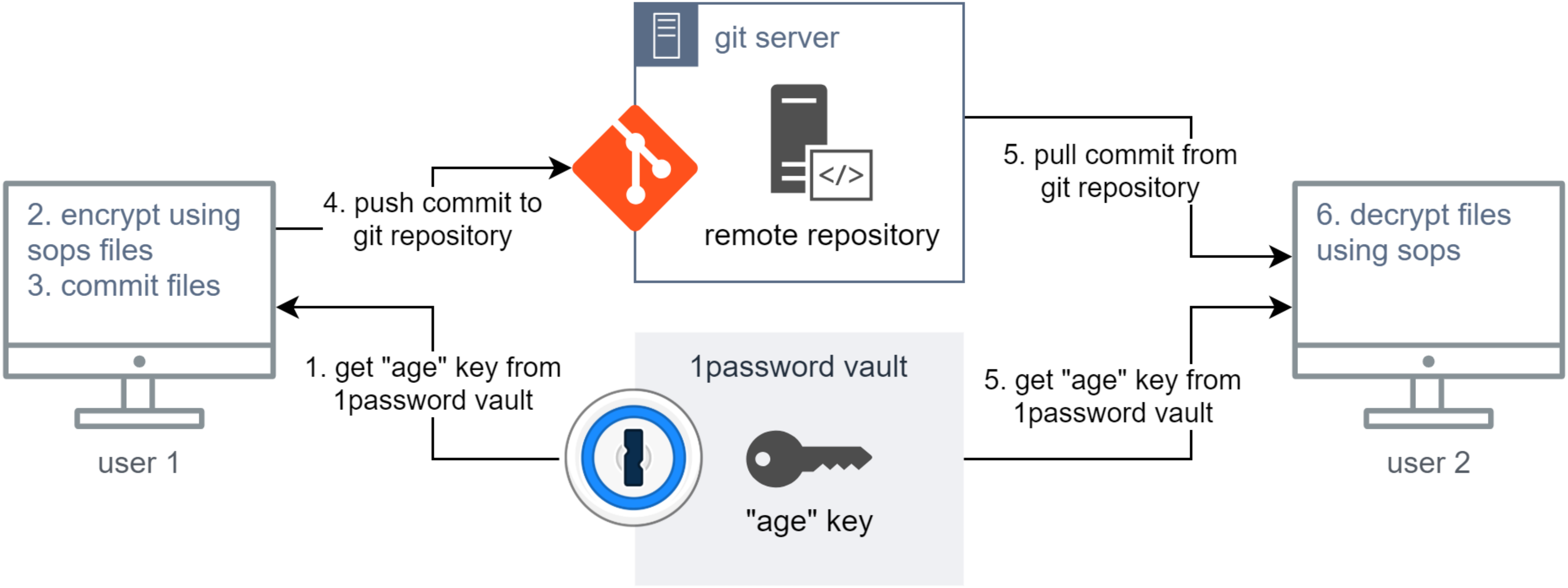
GitOpsCon EUROPE

Bitnami Sealed Secrets



Tools I hear about

Mozilla SOPS: Secrets OPerationS


git server
remote repository
2. encrypt using sops files
3. commit files
user 1
4. push commit to git repository
1. get "age" key from 1password vault
1password vault
"age" key
5. pull commit from git repository
5. get "age" key from 1password vault
6. decrypt files using sops
user 2

SOPS + Git using `age` | h/t to this walkthrough I found

Disadvantages

@tracypholmes

03 @tracypholmes

Vault.

Vault and GitOps.

What makes Vault not GitOps friendly?

Thoughts.

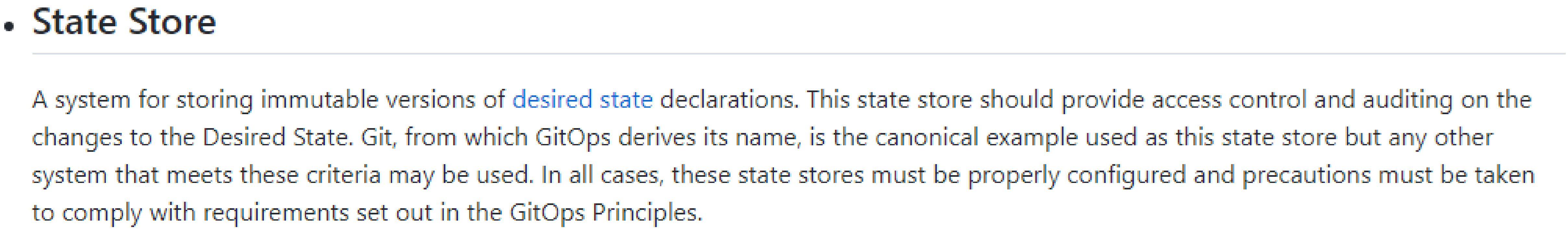
Vault is actually a controller.

All dynamic secrets in Vault are required to have a lease. A lease is required to force the consumer to check in routinely. So, it continuously checks the leases.

And you can configure it declaratively using the CLI.

Vault and Version Control

…and can I use them with GitOps

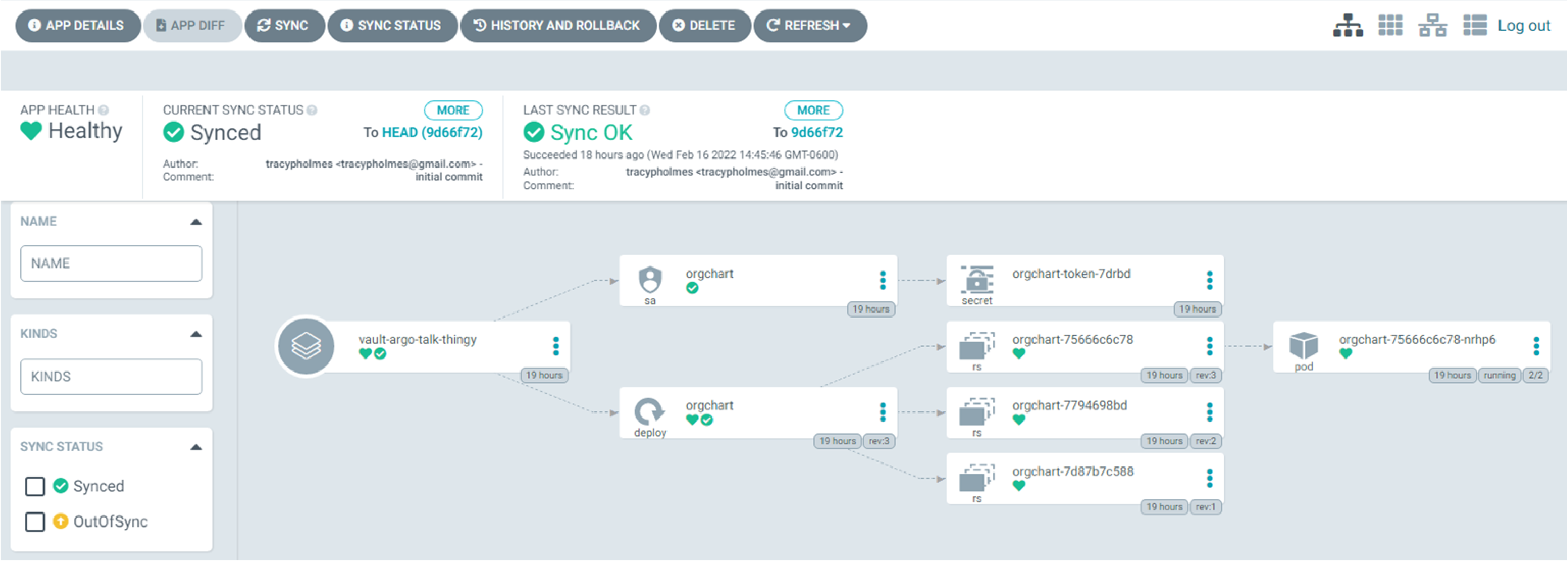


- State Store

A system for storing immutable versions of desired state declarations. This state store should provide access control and auditing on the changes to the Desired State. Git, from which GitOps derives its name, is the canonical example used as this state store but any other system that meets these criteria may be used. In all cases, these state stores must be properly configured and precautions must be taken to comply with requirements set out in the GitOps Principles.

https://github.com/open-gitops/documents/blob/v1.0.0/GLOSSARY.md#state-store

Vault and Kubernetes



APP HEALTH
Healthy

CURRENT SYNC STATUS MORE
Synced
To HEAD (9d66f72)
Author: tracypholmes <tracypholmes@gmail.com> -
Comment: initial commit

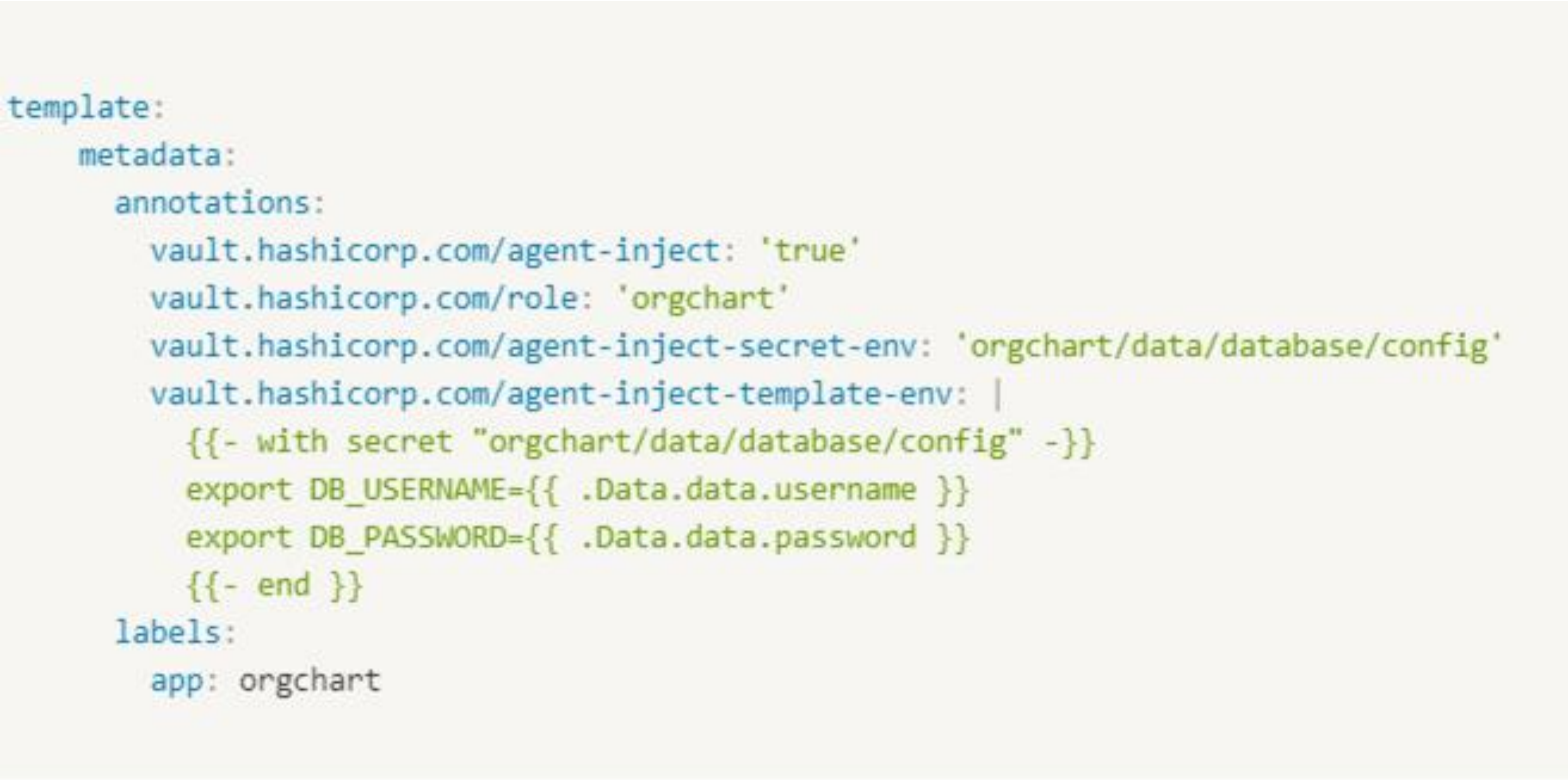
LAST SYNC RESULT MORE
Sync OK
To 9d66f72
Succeeded 18 hours ago (Wed Feb 16 2022 14:45:46 GMT-0600)
Author: tracypholmes <tracypholmes@gmail.com> -
Comment: initial commit

NAME

KINDS

SYNC STATUS
□ Synced
□ OutOfSync

@tracypholmes



```
template:
    metadata:
      annotations:
        vault.hashicorp.com/agent-inject: 'true'
        vault.hashicorp.com/role: 'orgchart'
        vault.hashicorp.com/agent-inject-secret-env: 'orgchart/data/database/config'
        vault.hashicorp.com/agent-inject-template-env: |
          {{- with secret "orgchart/data/database/config" -}}
          export DB_USERNAME={{ .Data.data.username }}
          export DB_PASSWORD={{ .Data.data.password }}
          {{- end }}
      labels:
        app: orgchart
```

Change…is good?

- Argo CD Vault plugin (works with Kubernetes secrets)
- Secrets Store CSI Driver (and the Vault provider for it)
- …something else out there I haven’t had a chance to research

Sidenote

- Part of GitOps says configuration must be declarative. “you can’t configure Vault declaratively”. You can use Terraform for your configurations, OR the Vault Config Operator (which is a community tool)
- If you want to see what Vault Config Operator looks like in practice, check out this repo.
- It ALSO uses Argo Sync Wave to sync things that need to reconcile (seen here)

Why are secrets important?

…and can I use them with GitOps

@tracypholmes

THANKS!

You can find all the resources used for this talk here!