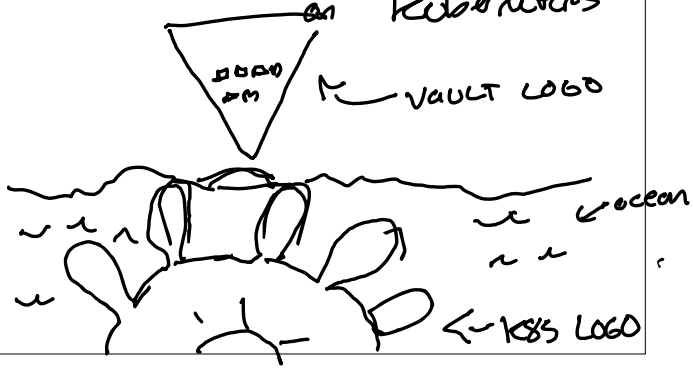
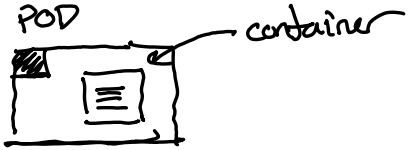
Manage Secrets with Vault on Kubernetes

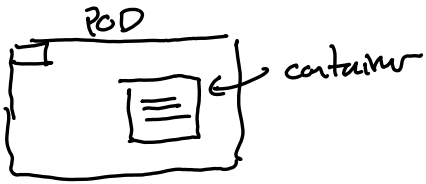


WARM UP EXERCISE



I want to give a few minutes to enable everyone to connect. While doing that I thought it would be a good chance for those of us eager to get started to engage in a thought exercise.

WARM UP EXERCISE

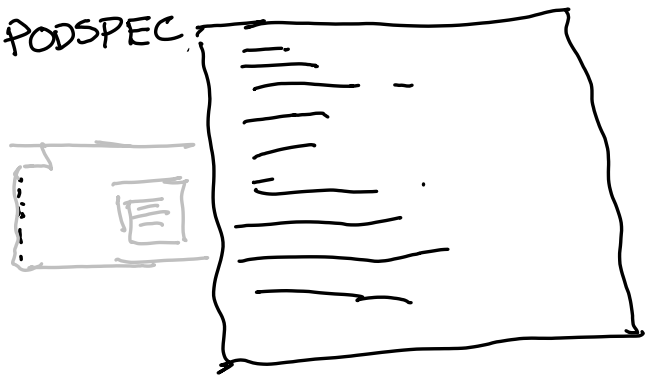


Kubernetes takes the approach of solving the infrastructure mgmt problem with a declaritive approach.

For example this pod that deploys this container can be expressed declaritively in YAML

WARM UP EXERCISE

PODSPEC



(Quickly show the mapping of the spec elements to the visual elements)

Translate the core PODSPEC ITEMS

This is useful to give a quick refresher on the spec and to also familiarize any visual story with the components represented.

WARM UP EXERCISE

How could you manage secrets as this pod?

- Adding them to the PODSPEC makes them visible to the operator

WARM UP EXERCISE

If you were to store these secrets in Vault from the ~~CLI~~

Vault CLI needs to know
the Vault Server
the path to the secret
the credentials

WARM UP

Using the API through
curl commands / HTTP requests

(I thought at this point that leaving more info this being a quick introduction or re-introduction to the ways that Vault might look like for different people)

WARM UP

Using the website through the Web UI

This shows all the ways in which people would interact with Vault. While the demonstration and examples will work through the CLI. This presentation of equivalency ties all these different ways to the CLI and help repeat the concepts

WARM UP EXERCISE

What would your API look like?

First what information do you need to retrieve and where to retrieve it from?

With the secret needing to received in a particular format?

Obviously, I am going to present to you how it is currently implemented but it is important to think about these questions and a potential implementation because this, as all these products are part of the ecosystem. and your use cases may be important in helping shape the features implementation

Display other implementations

(Potentially here is where other implementations are presented for discussion. I assume that this workshop is at the mercy of the platform. If user interaction is not possible present solutions from beta teach)

The benefit would be to convince within the initial minutes that the implementation is important. But the core questions of what data that needs to be expressed is shown in multiple ways.

End with a question and then transition to the introduction

Managing Secrets
with Vault
on Kubernetes

(Rephrase the Title Slide)

Welcome to ...

You are ...

- Have deployed something on Kubernetes
- Have used Vault through the CLI

Let me talk about who I think that you are

[Retrieve the abstract]

(define the audience)

What we are going to cover

Agenda

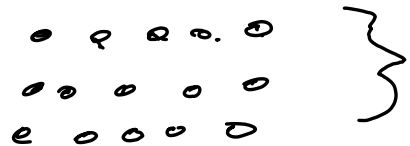
- o
- o
- o
- o
- o
- o
- o
- o

(The bullet points in the proposed topic points seem pretty accurate to add here)

The timeline Agenda

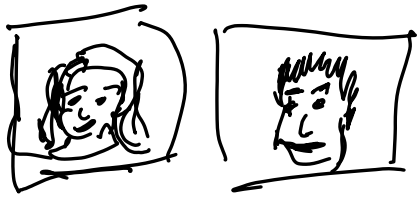
- overview
- Install the helm chart
- Secret with annotations

} objective 1
1600
1630
1645 Activity



(Display how the agenda of events map to the time allotted to the workshop session)

Who we are...



INSERT

It may be useful to outline the platform before people introduction

Presentation platform (FEEDBACK)

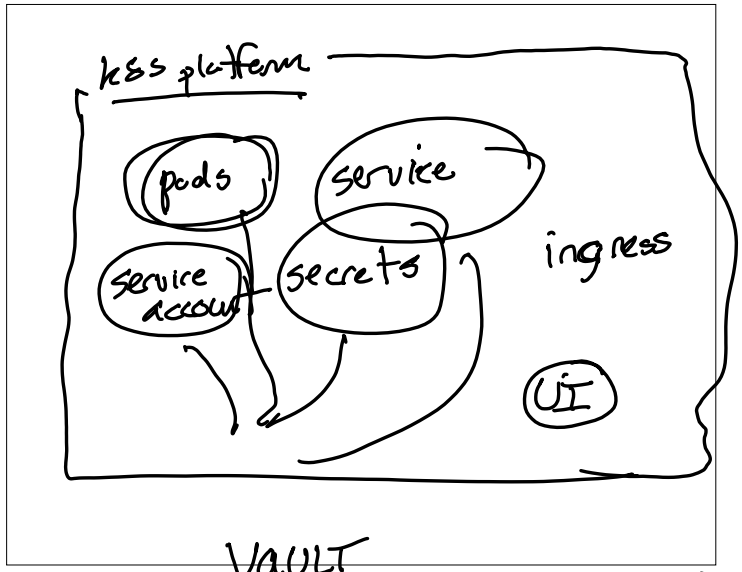
Katacoda

knowing who you are, what you are here to learn, the format on how we are to learn it if is important to introduce those of that are here to help us stay on track with the schedule, meet the objectives, assist during (Labs)

zoom description

Quite possible

Overview of the Helm Chart



To deploy Vault within the k8s platform. It would require a number of resources.