# Hacking Helm

@pczarkowski
@r6by

# HELLO!

Paul Czarkowski
@pczarkowski
pczarkowski@pivotal.io

Scott Rigby
@r6by
scott@r6by.com

# Agenda

- ✘ What is Helm ?
- ✘ Security Concerns
- ✘ Lock down Tiller
- ✘ Secure Values

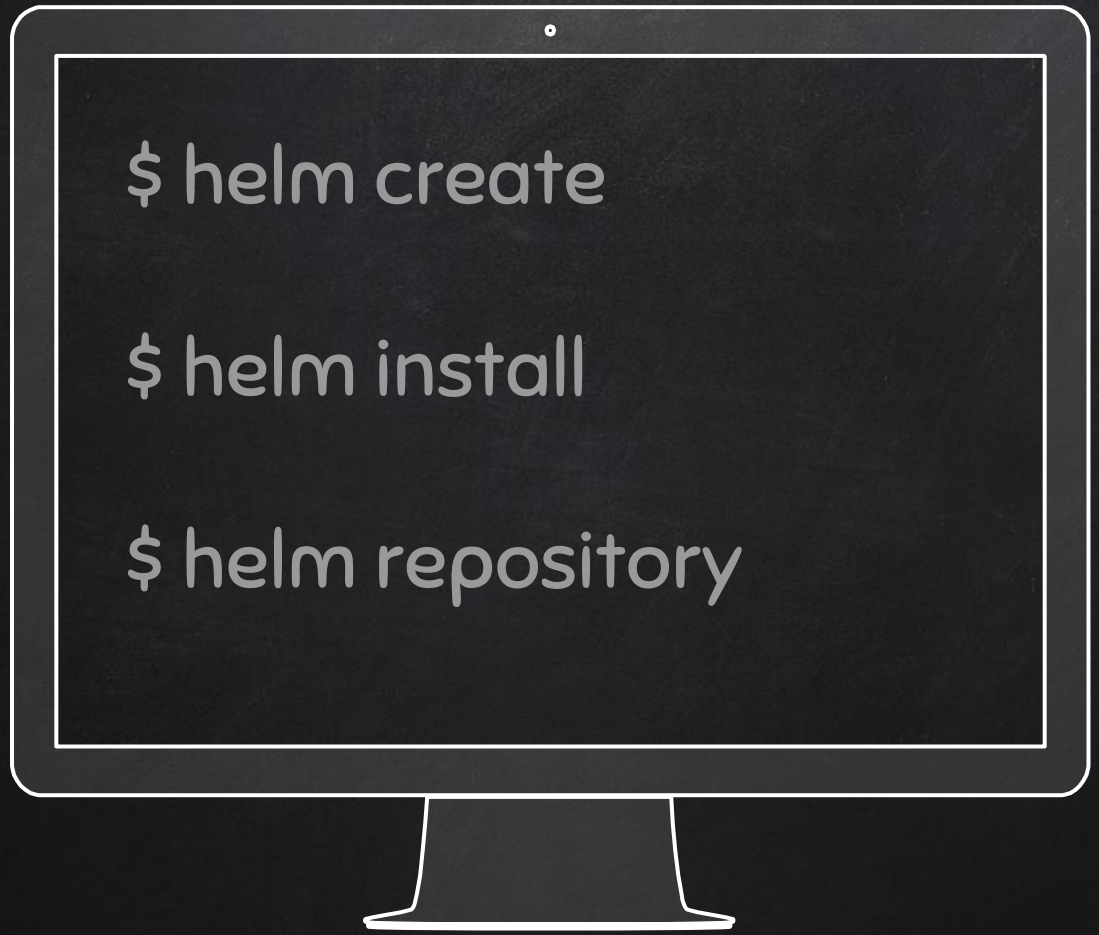

What Is Helm?

Helm is the best way to
find, share, and use
software built for Kubernetes

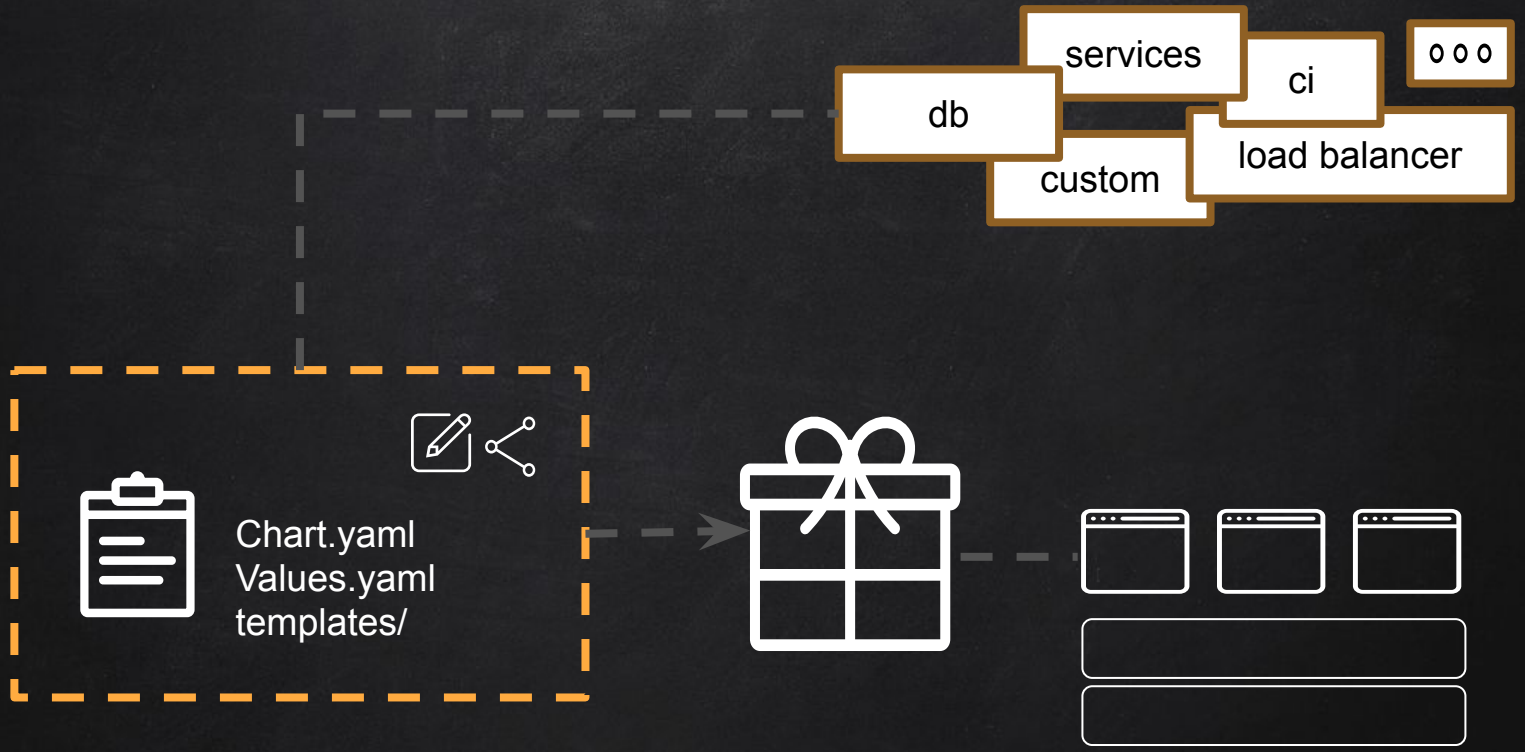
# Components

- ✘ Helm Client
- ✘ Helm Chart [package]
- ✘ Chart Repository
- ✘ Tiller Server


# Helm Client

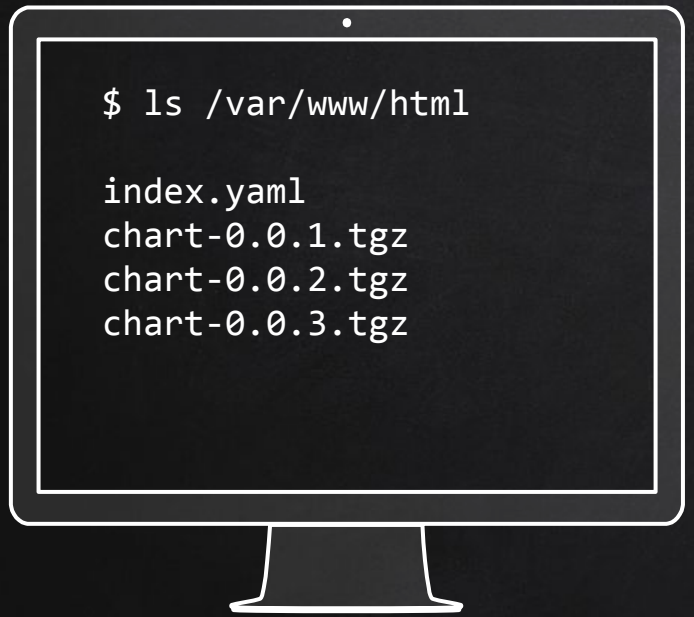

$ helm create
$ helm install
$ helm repository


# Helm Chart [Package]


services
ci
o o o
db
load balancer
custom
Chart.yaml
Values.yaml
templates/


# Helm Repository

# A Helm repository is just a web server.

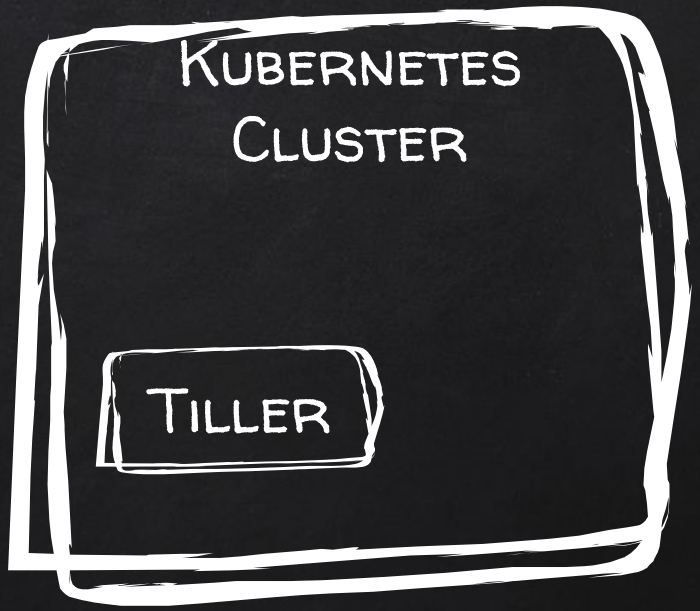



https://github.com/helm/chart-releaser


Secure | https://hub.helm.sh
Kubeapps Hub
Discover & launch great
Kubernetes-ready apps
Search charts
Wordpress, Jenkins, Kubeless...
666 charts ready to deploy


# Tiller Server

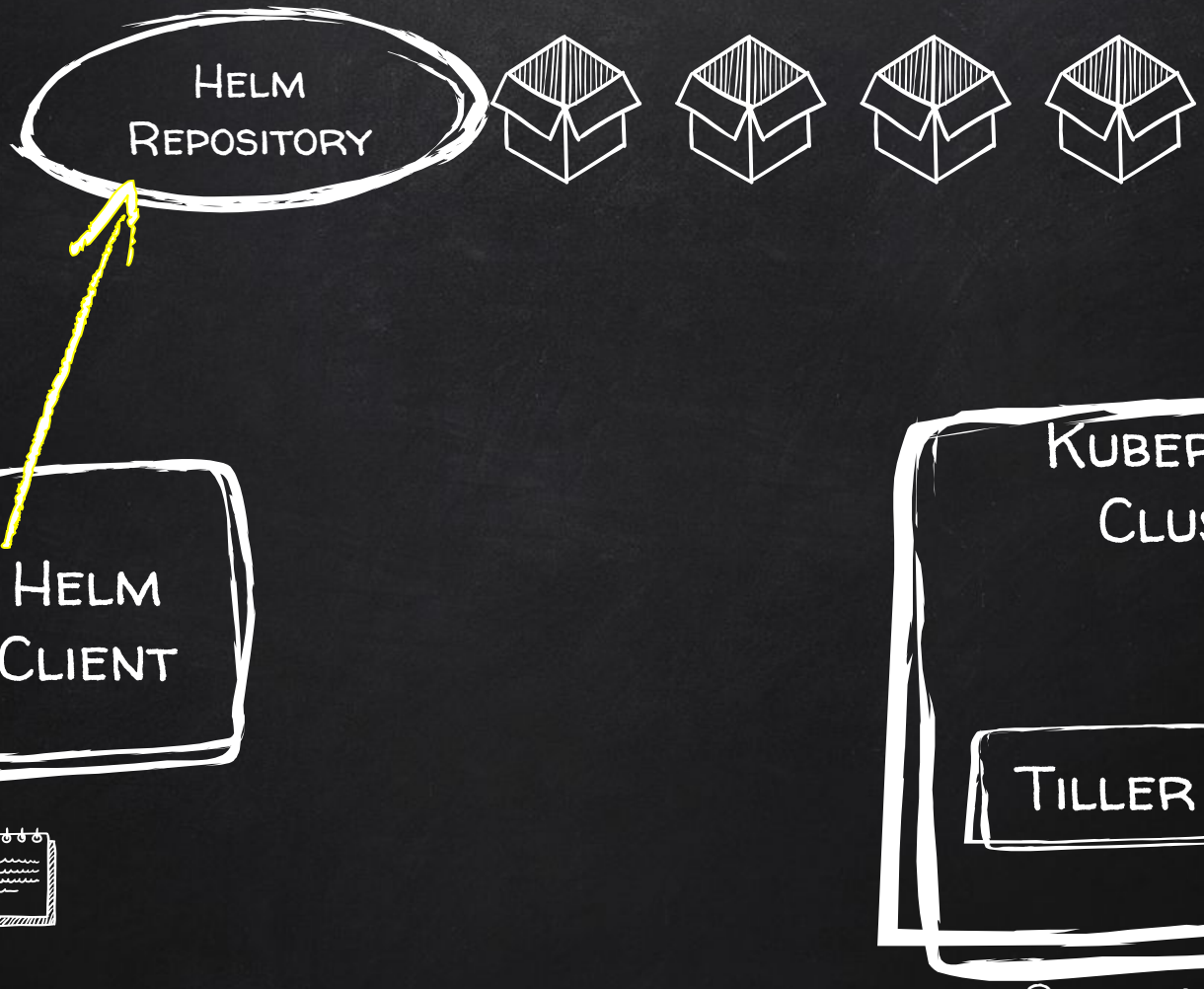
# Tiller server runs in the Kubernetes Cluster



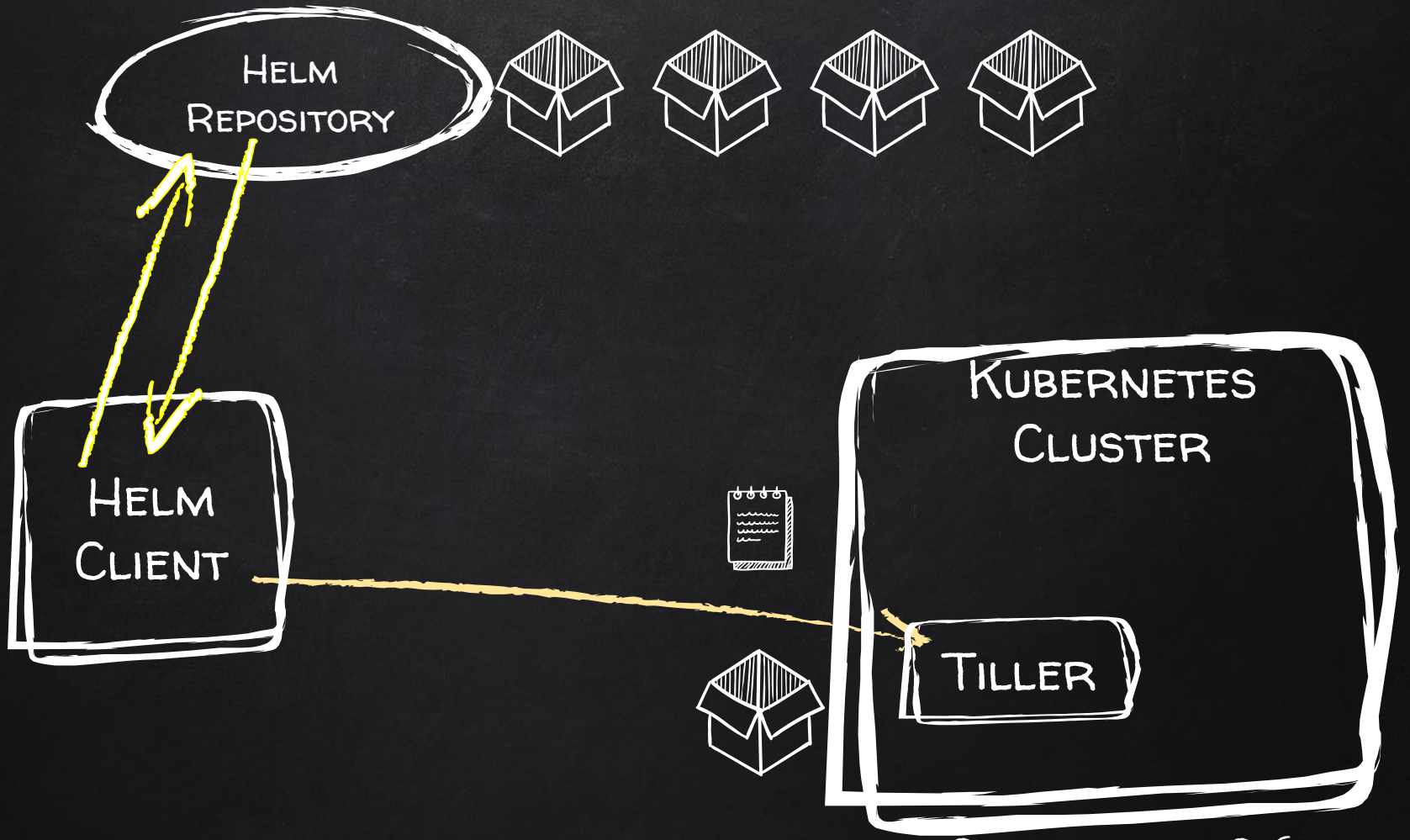

$ helm init
Tiller (the Helm server-side component) has been installed into your Kubernetes Cluster.

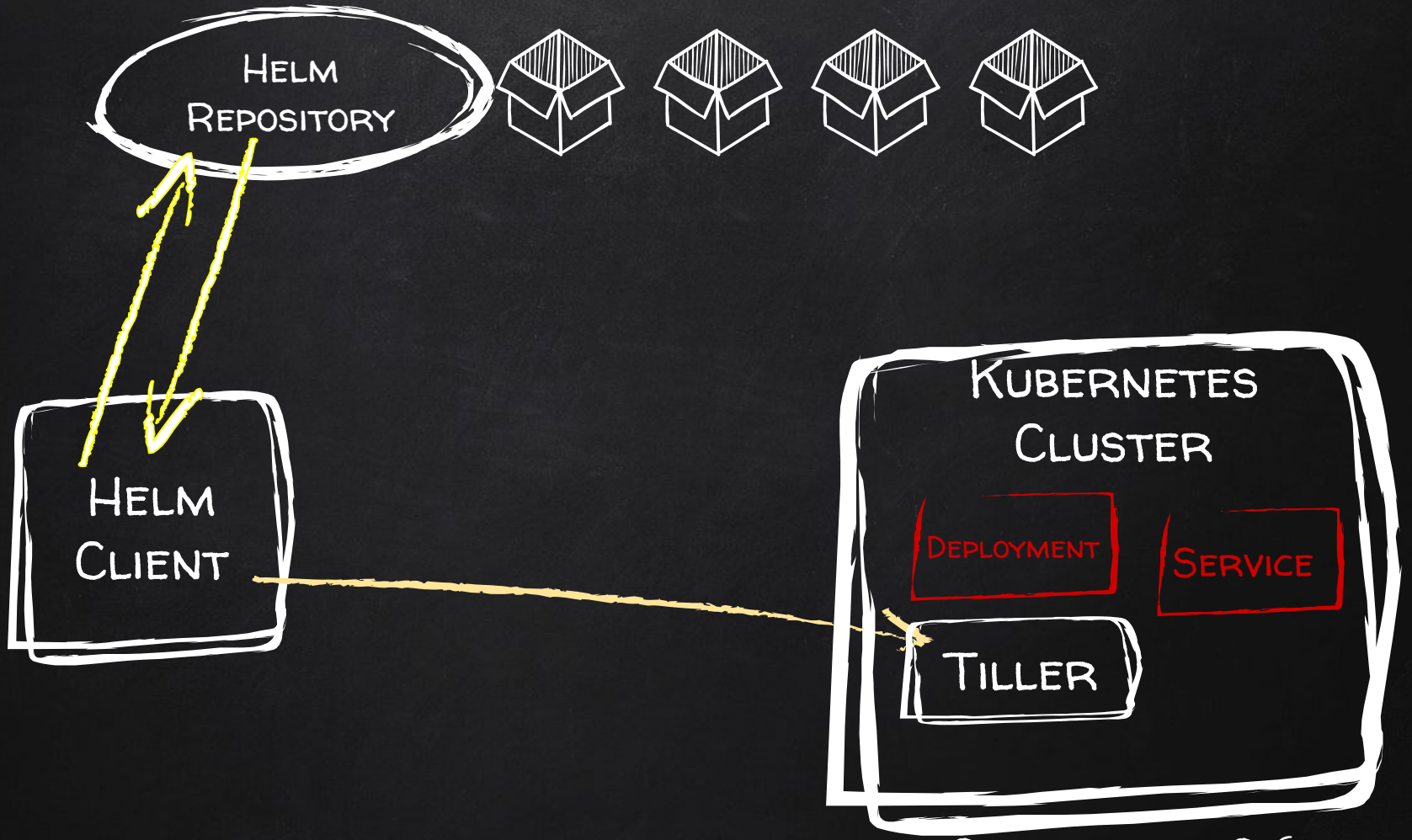

$ k get deployments
NAME READY
UP-TO-DATE AVAILABLE AGE
tiller-deploy 1/1 1
1 63s

# Helm Chart Workflow


Helm
Repository
Helm
Client
Kubernetes
Cluster
Tiller

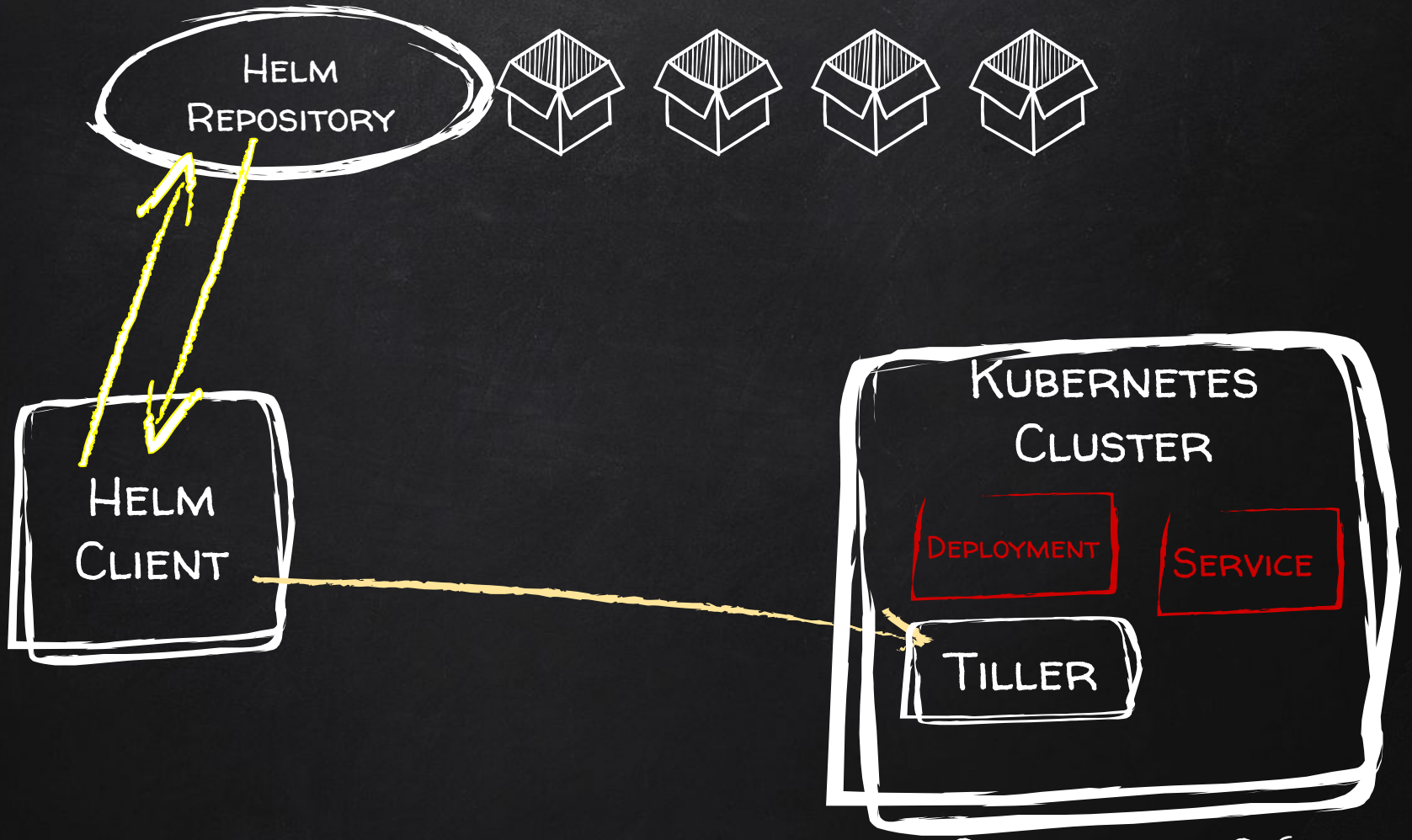

Helm
Repository
Helm
Client
Kubernetes
Cluster
Tiller


Helm
Repository
Helm
Client
Kubernetes
Cluster
Tiller




@pczarkowski @r6by

# Security Concerns


Helm
Repository
Helm
Client
Kubernetes
Cluster
Deployment
Service
Tiller


# Tenancy

# K8s Tenancy Models

| Model | Tenancy |
| --- | --- |
| Everyone is Cluster Admin | none |
| Every User has their own NS | soft |
| Each Team/Project have a shared NS | soft |
| Each Team has their own Cluster | hard |

# K8s Tenancy Models

| Model | Tenancy |
| --- | --- |
| Everyone is Cluster Admin | none |
| Every User has their own NS | soft |
| Each Team/Project have a shared NS | soft |
| Each Team has their own Cluster | hard |

# K8S TENANCY MODELS

| Model | Tenancy |
| --- | --- |
| Everyone is Cluster Admin | none |
| Every User has their own NS | soft |
| Each Team/Project have a shared NS | soft |
| Each Team has their own Cluster | hard |

# K8s Tenancy Models

| Model | Tenancy |
| --- | --- |
| Everyone is Cluster Admin | none |
| Every User has their own NS | soft |
| Each Team/Project have a shared NS | soft |
| Each Team has their own Cluster | hard |


# RBAC vs ABAC


✘ Don't use ABAC


- ✘ Service Accounts – for “robots”
- ✘ User Accounts – for “humans”


- ✘ Service Accounts – for “robots”
- ✘ User Accounts – for “humans”


- ✘ Service Accounts – for “robots”
- ✘ User Accounts – for “humans”


# Lock Down Tiller

# Tiller Attack Vectors

- ✘ Privilege Escalation
- ✘ In Cluster
- ✘ Naughty Chart Author

# Tiller Attack Vectors

- ✘ Privilege Escalation
- ✘ In Cluster
- ✘ Naughty Chart Author

```
$ kubectl -n kube-system create \
    serviceaccount tiller

$ kubectl create clusterrolebinding tiller \
  --clusterrole cluster-admin \
  --serviceaccount=kube-system:tiller

$ helm init --service-account=tiller
```

```
$ kubectl -n paul create \
    serviceaccount tiller

$ kubectl -n paul create role tiller \
    --verb ‘*’ \
    --resources=’services,deployments,...’

$ kubectl -n paul create rolebinding \
    --role tiller --service-account=paul:tiller

$ helm init --service-account=tiller --tiller-namespace=paul
```

# Tiller Attack Vectors

- ✘ Privilege Escalation
- ✘ In Cluster
- ✘ Naughty Chart Author

```
$ kubectl -n kube-system get service tiller-deploy

NAME            TYPE        CLUSTER-IP      EXTERNAL-IP   PORT(S)     AGE
tiller-deploy   ClusterIP   10.110.112.63   <none>        44134/TCP   20h
```

```
$ kubectl run -n default --quiet --rm --restart=Never \
    -ti --image=alpine/helm helm --command -- /bin/sh

helm# helm --host tiller-deploy.kube-system:44134 version
Client: &version.Version{SemVer:"v2.13.1",
GitCommit:"618447cbf203d147601b4b9bd7f8c37a5d39fbb4", GitTreeState:"clean"}
Server: &version.Version{SemVer:"v2.13.1",
GitCommit:"618447cbf203d147601b4b9bd7f8c37a5d39fbb4", GitTreeState:"clean"}

helm# helm --host tiller-deploy.kube-system:44134 install bitcoin
```

```
$ kubectl -n kube-system delete service tiller-deploy
service "tiller-deploy" deleted

helm# helm --host tiller-deploy.kube-system:44134 version
Client: &version.Version{SemVer:"v2.13.1",
GitCommit:"618447cbf203d147601b4b9bd7f8c37a5d39fbb4", GitTreeState:"clean"}
Timed out.

Helm# helm --host 172.17.0.4:44134 version
Client: &version.Version{SemVer:"v2.13.1",
GitCommit:"618447cbf203d147601b4b9bd7f8c37a5d39fbb4", GitTreeState:"clean"}
Server: &version.Version{SemVer:"v2.13.1",
GitCommit:"618447cbf203d147601b4b9bd7f8c37a5d39fbb4", GitTreeState:"clean"}
```

```
$ kubectl -n kube-system patch deployment \
    tiller-deploy --patch '
spec:
  template:
    spec:
      containers:
        - name: tiller
          ports: []
          command: ["/tiller"]
          args: ["--listen=localhost:44134"]
'
```

```
Helm# helm --host 172.17.0.4:44134 version
Client: &version.Version{SemVer:"v2.13.1",
GitCommit:"618447cbf203d147601b4b9bd7f8c37a5d39fbb4", GitTreeState:"clean"}
Timed out.
```


# But how do my Helm commands Still work


# What if I need Helm access from Inside my cluster?

```
$ helm init --tiller-tls --tiller-tls-cert ./tiller.crt \
  --tiller-tls-key ./tiller.key --tiller-tls-verify \
  --tls-ca-cert ca.crt

$ helm --tls --tls-ca-cert ca.crt --tls-cert myclient.crt \
  --tls-key myclient.key version
Client: &version.Version{SemVer:"v2.13.1",
GitCommit:"618447cbf203d147601b4b9bd7f8c37a5d39fbb4", GitTreeState:"clean"}
Server: &version.Version{SemVer:"v2.13.1",
GitCommit:"618447cbf203d147601b4b9bd7f8c37a5d39fbb4", GitTreeState:"clean"}
```

# Tiller Attack Vectors

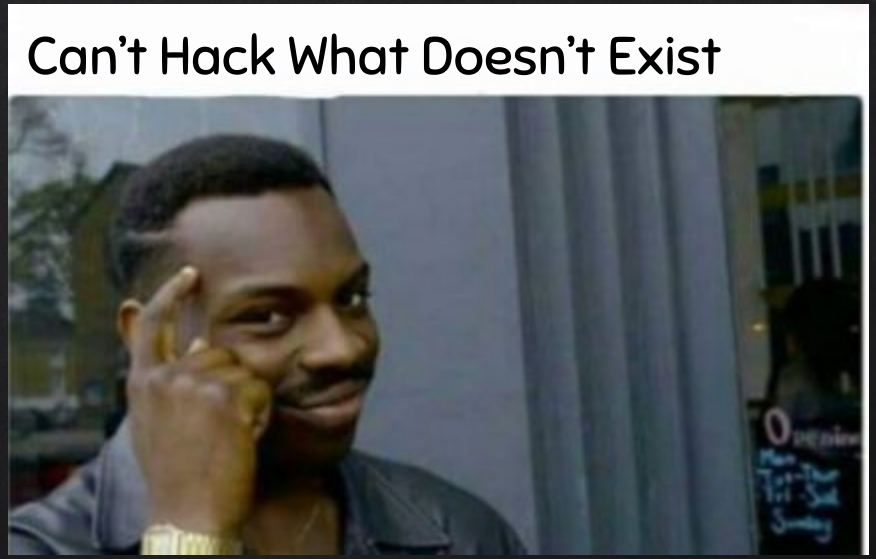
- ✘ Privilege Escalation
- ✘ In Cluster
- ✘ Naughty Chart Author


# Helm Install is the new Curl Bash

# Naughty Chart Authors

- ✘ PodSecurityPolicy
- ✘ AdmissionController Webhooks ( Open Policy Agent! )
- ✘ ConfTest – shift OPA left
  - https://github.com/instrumenta/conftest

# Just Don't Install Tiller!



```
$ helm template -f prod.yaml stable/wordpress > deploy.yaml

$ kubectl apply -f deploy.yaml
```

```
$ helm tiller start my-team-namespace

$ helm install …

$ helm tiller stop
```

https://github.com/rimusz/helm-tiller


# Secrets & Value Leakage

# Leaky Value Syndrome

- ✘ Helm values leak... 😭
- ✘ Version control is forever!
- ✘ Tips for using k8s secrets with Helm

```
$ helm install stable/grafana --name grafana \
    --namespace grafana --set “adminPassword=z3roC00l!”


$ kubectl -n kube-system get configmap grafana.v1 -o yaml
```

```
$ for i in $(helm ls | awk '{print $1}' | tail -n +2)
  do helm get values $i | grep -i pass
done

adminPassword: dsadRGR
    password: flkdjsfdsk3r3r3
harborAdminPassword: sadkljejfewreDDf33
```

```
$ git clone http://github.com/e-corp/infrastructure-as-code

$ cd infrastructure-as-code/envs/production

$ cat values.yaml | grep -i pass
```

# How to Handle Secrets then ?

- ✘ Encrypt them before pushing to github
  - Sealed Secrets ( bitnami tool )
- ✘ Store them in a separate encrypted volume
  - I've even seen a shared keepass/onepass used for this
- ✘ YOLO them into git


BRACE YOURSELVES
HELM 3 IS COMING
imgflip.com

# Forget Everything We Just Told you.

# Summary

- ✘ First know your tenancy model
- ✘ Secure your tiller install based on tenancy
- ✘ Tiller is “insecure” by default
- ✘ We still have a “how to keep secrets secret” problem
- ✘ Helm is awesome, and can used securely!
- ✘ Helm 3 ~~will~~ might be more secure.

# References and Further Reading

- https://hub.helm.sh
- https://engineering.bitnami.com/articles/helm-security.html
- https://github.com/instrumenta/conftest
- https://github.com/helm/chart-releaser
- https://github.com/helm/chart-testing
- https://github.com/rimusz/helm-tiller

# THANKS!

## Any questions?

You can find us at


Paul Czarkowski
@pczarkowski
pczarkowski@pivotal.io

Scott Rigby
@r6by
scott@r6by.com