Argh, yer Kubernetes be now a shark bait!

Ahoy!

I am Alex Ivkin

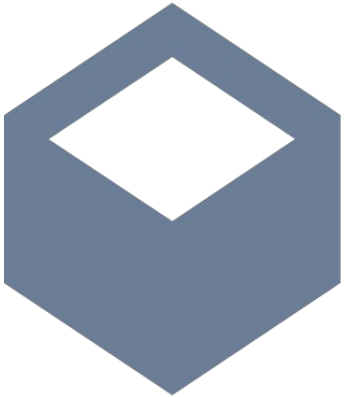
Director of Solutions at Eclypsium, Beaverton, OR

@alexivkinx

Kubernetes

Developers, developers, developers!

@alexivkinx



@alexivkinx

@alexivkinx

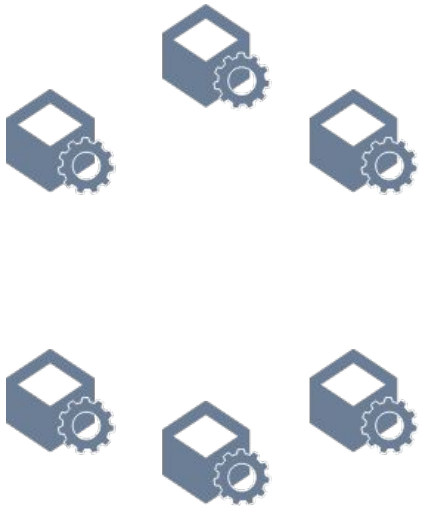
Chef

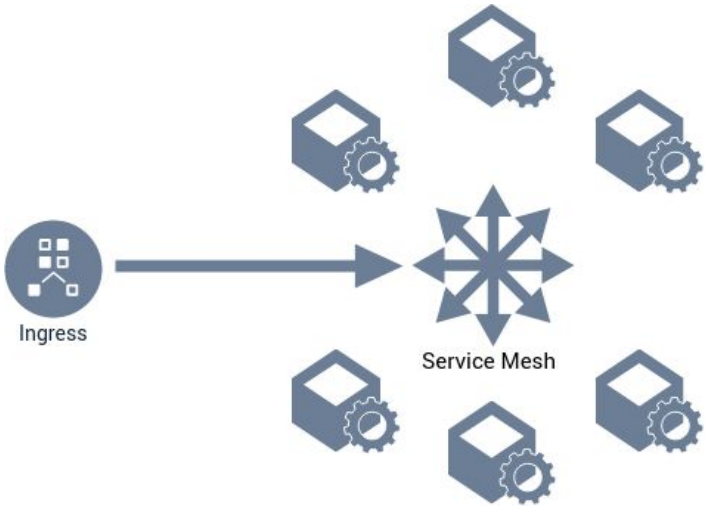
Puppet

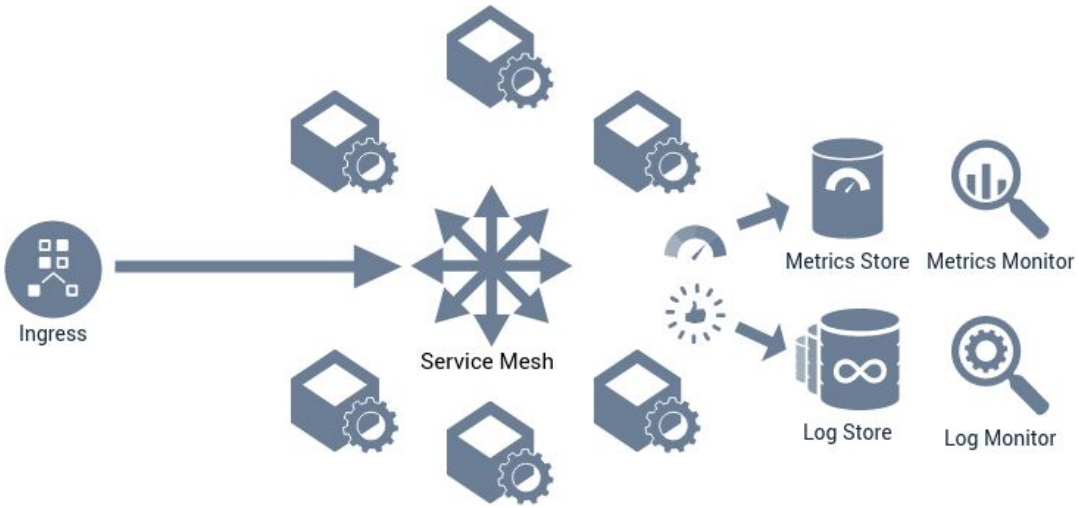
Ahoy!

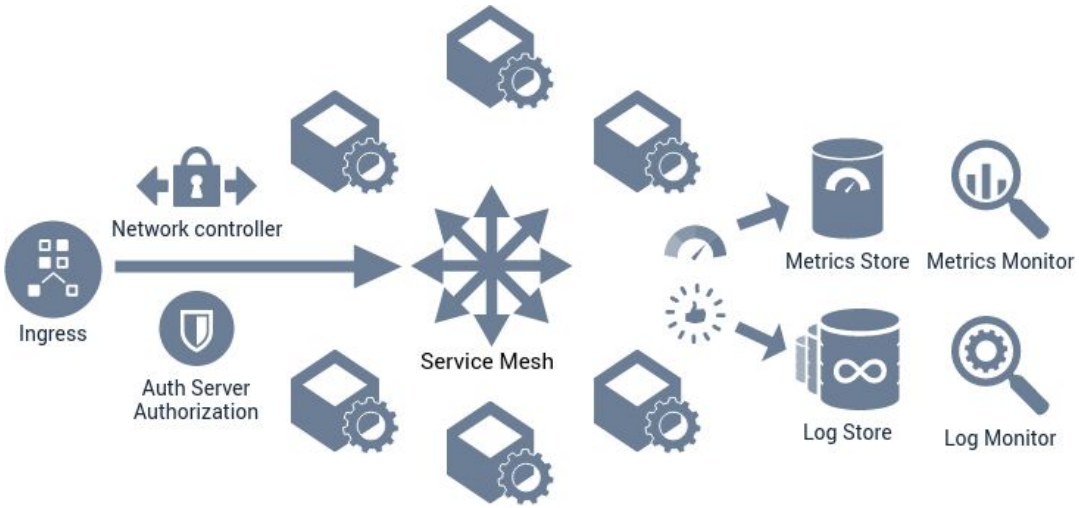
I am Alex Ivkin

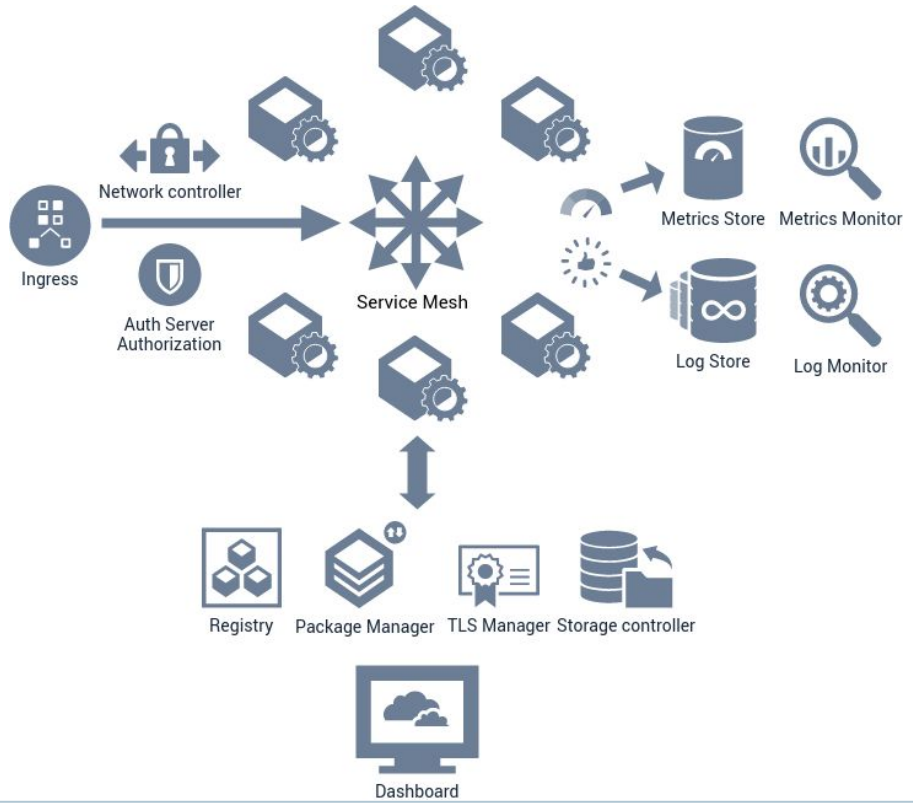
Director of Solutions at Eclypsium, Beaverton, OR






Ingress
Service Mesh
Metrics Store
Metrics Monitor
Log Store
Log Monitor


Network controller
Ingress
Auth Server
Authorization
Service Mesh
Metrics Store
Metrics Monitor
Log Store
Log Monitor


Network controller
Ingress
Auth Server
Authorization
Service Mesh
Metrics Store
Metrics Monitor
Log Store
Log Monitor
Registry
Package Manager
TLS Manager
Storage controller
Dashboard

Ingress - **Istio**, ingress-nginx

Package manager - **Helm/Tiller**, Kustomize

Service meshes - Linkerd, **Envoy**

Data collectors - Fluentd, Loki

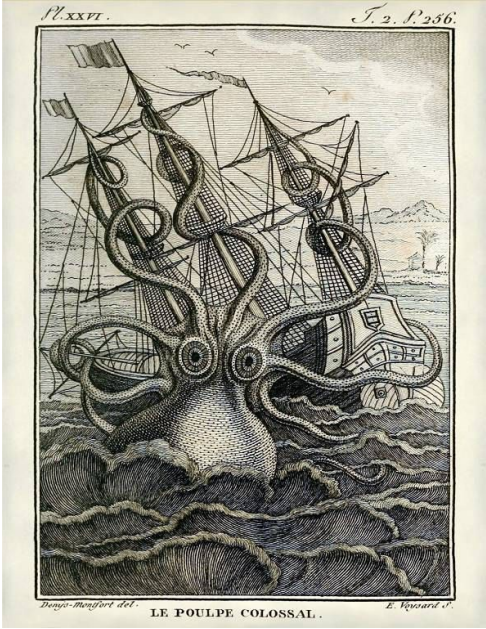
Metrics collectors - **Promethius**, Grafana

Network controller - Flannel, Falco, Calico

TLS manager - **Cert-manager**, Istio SDS

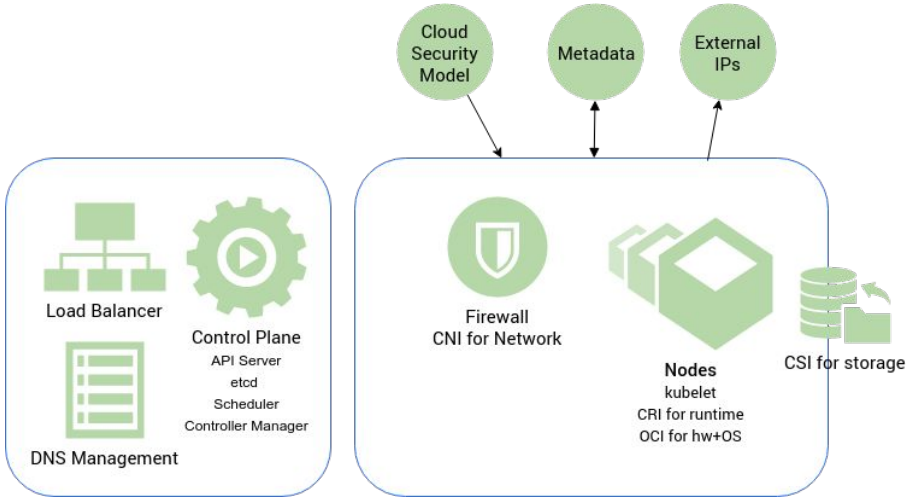
Image store - Docker **registry**, Notary

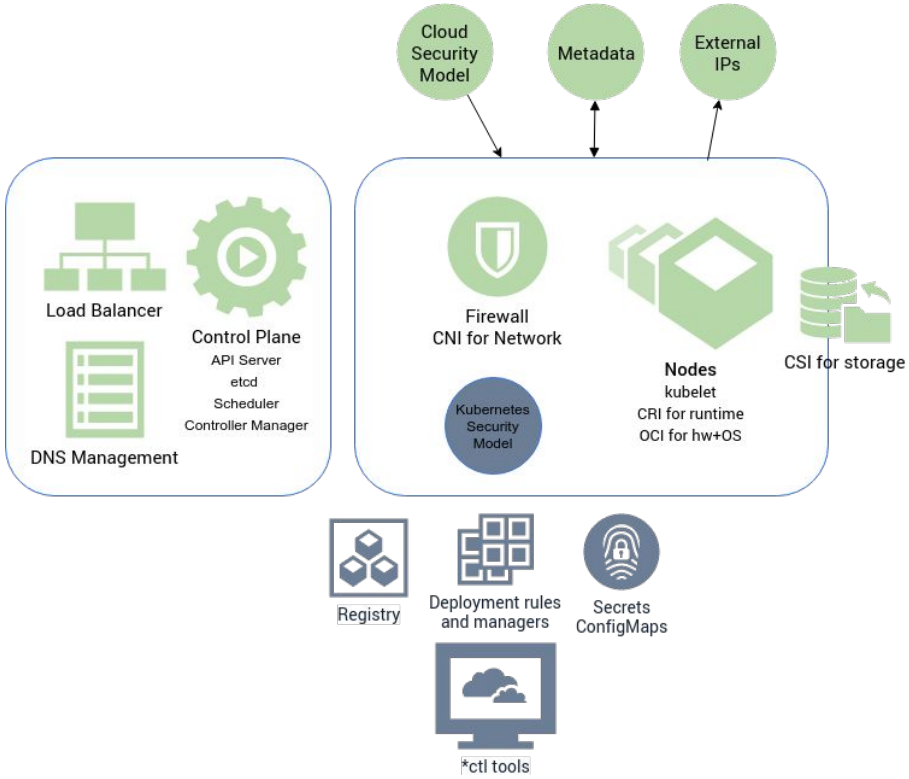
Auth/Azn - Hydra, OPA, SPIRE, RBAC-manager



@alexivkinx


Load Balancer
Control Plane
API Server
etcd
Scheduler
Controller Manager
DNS Management
Firewall
CNI for Network
Nodes
kubelet
CRI for runtime
OCI for hw+OS
CSI for storage

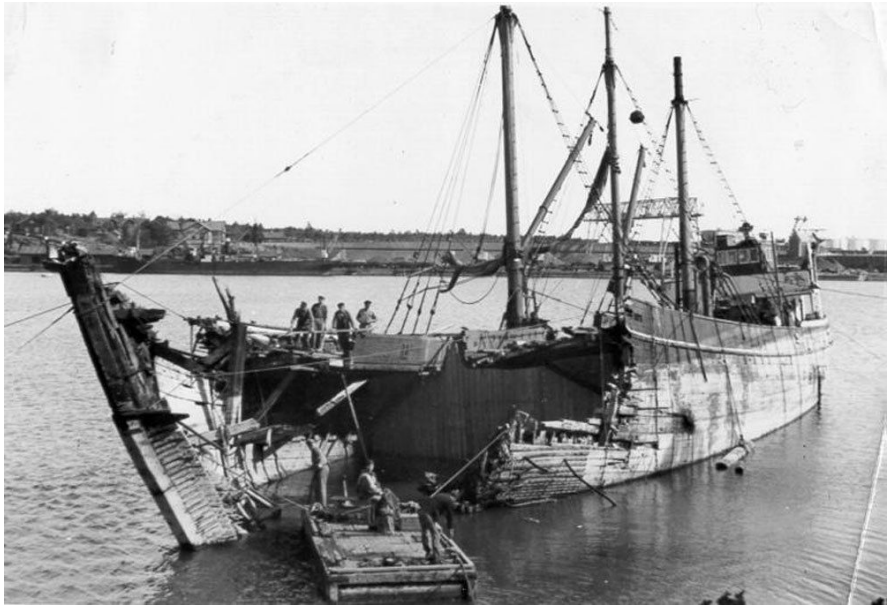

Cloud Security Model
Metadata
External IPs
Load Balancer
Control Plane
API Server
etcd
Scheduler
Controller Manager
DNS Management
Firewall
CNI for Network
Nodes
kubelet
CRI for runtime
OCI for hw+OS
CSI for storage


Cloud Security Model
Metadata
External IPs
Load Balancer
Control Plane
API Server
etcd
Scheduler
Controller Manager
DNS Management
Firewall
CNI for Network
Kubernetes Security Model
Nodes
kubelet
CRI for runtime
OCI for hw+OS
CSI for storage
Registry
Deployment rules and managers
Secrets
ConfigMaps
*ctl tools

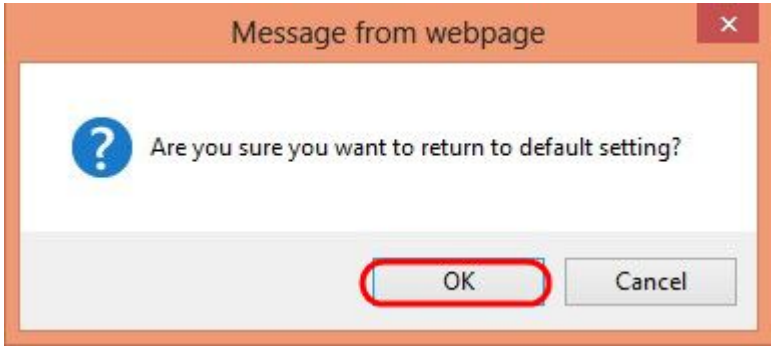
Containment models

	dockerd	minikube	K3s	GCP Kubernetes	DO Kubernetes	AWS AKS
AppArmor	default	unconfined	cri-containerd.apparmor.d	default	unconfined	unconfined
Seccomp	filtering	disabled	disabled	disabled	disabled	disabled
Blocked syscalls	56	19	30	18	21	20

Pillage!

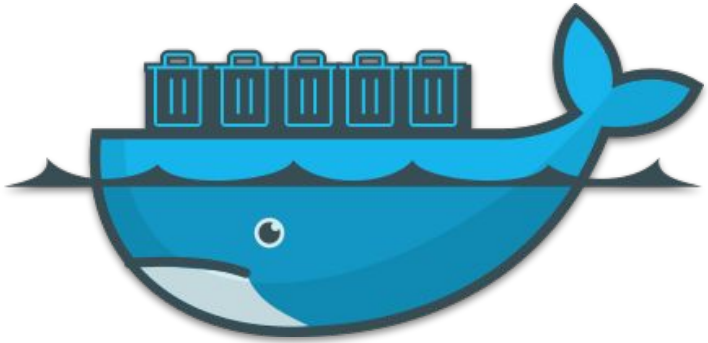


Yer front fell off!



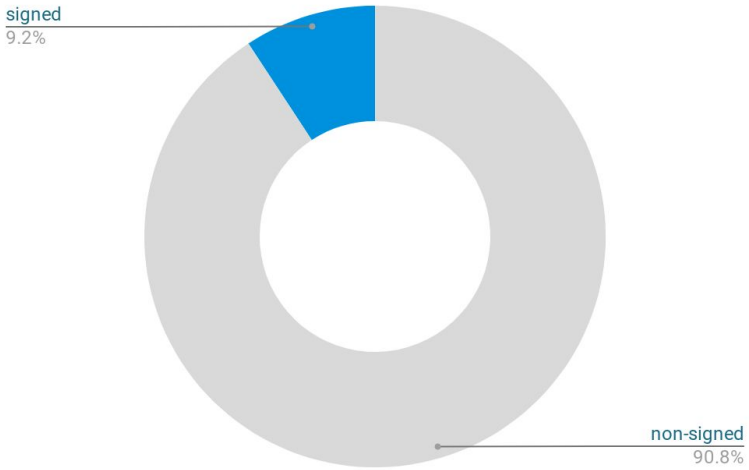
Docker has reasonable defaults
Kubernetes and friends have terrible defaults

Tiller is deployed with an insecure '**allow unauthenticated users**' policy.
Istio installation profile, **policy enforcement is disabled**.
Cert-manager runs with **validation disabled** - it will not reject ‘create’ events when the resources are submitted to the apiserver if they are invalid.
Pods with services and cross namespaces - the port opened on a container is flat



@alexivkinx

@alexivkinx



@alexivkinx

Hide yo' ~~shit~~ meta

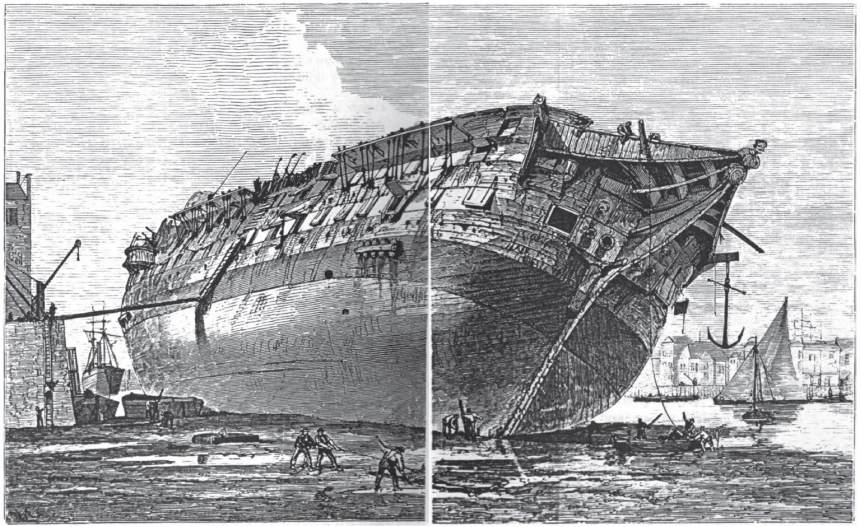
Fail gracefully - losing a container should not mean losing a cluster
Don't use network policies unless you have no other solution.
Errors, not vulnerabilities, lead to a lot of breaches *
Steep learning curve, mistakes will be made

** (Verizon 2019 data breach investigations report)*

THANKS!

Any questions?

You can find me at @alexivkinx & alex@ivkin.net



CREDITS

Special thanks to all the people who made and released these awesome resources for free:

- Presentation template by SlidesCarnival
- Maps in slides 2, 6 and 9 from David Rumsey Map Collection
- Photographs by Unsplash

PRESENTATION DESIGN

This presentation uses the following typographies and colors:

- Titles: Frank Ruhl Libre
- Body copy: Frank Ruhl Libre, Libre Baskerville (Quote)

You can download the fonts on these pages:

https://www.urbanfonts.com/fonts/Frank_Ruhl_Libre.font

https://www.fontsquirrel.com/fonts/libre-baskerville

Dark gray **#6c7a83** · Medium gray **#8a9ba6** · Light gray **#b0c6d3** · Beige **#f2edda**

You don't need to keep this slide in your presentation. It's only here to serve you as a design guide if you need to create new slides or download the fonts to edit the presentation in PowerPoint®

SlidesCarnival icons are editable shapes.

This means that you can:

- Resize them without losing quality.
- Change fill color and opacity.
- Change line color, width and style.

Isn't that nice? :)

Examples: