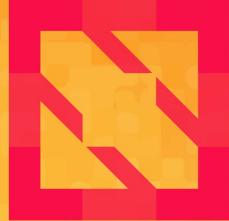




KubeCon



CloudNativeCon

North America 2019



SERVICE MESH: THERE AND BACK AGAIN

CODY VANDERMYN, SOFTWARE ENGINEER

HEMA LEE, SOFTWARE ENGINEER

NOVEMBER 19, 2019

NORDSTROM

TABLE OF CONTENTS

Why Service Mesh?



Investigations and Findings



Service Mesh Rollout

Middle
Earth

Challenges



Open Source Contributions

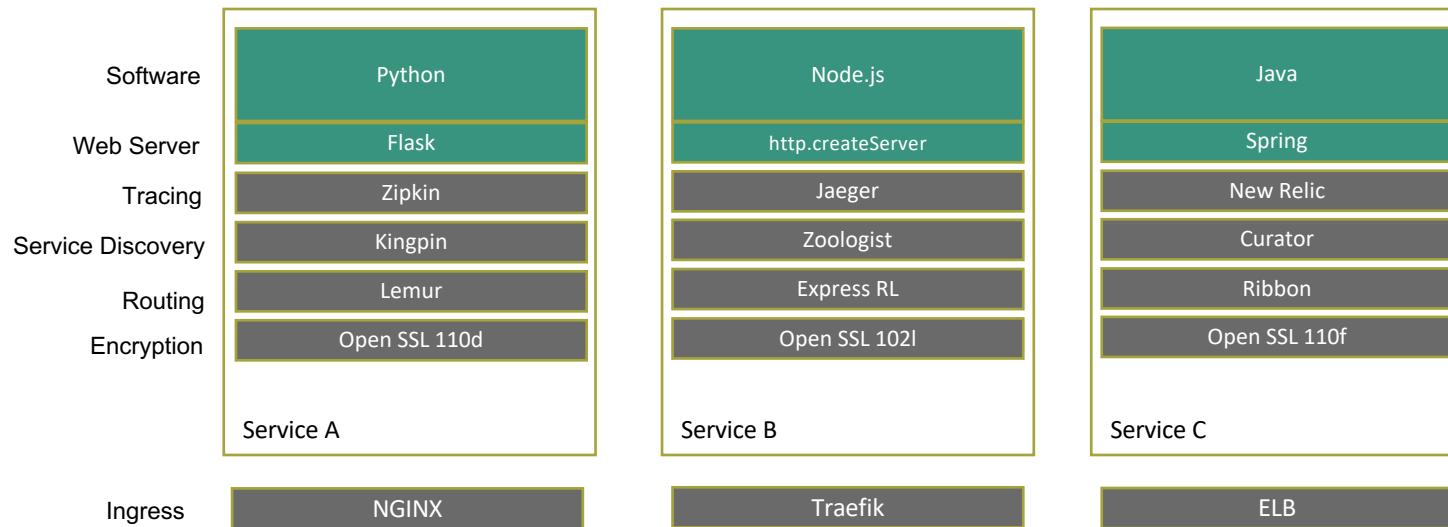


The Last Stage

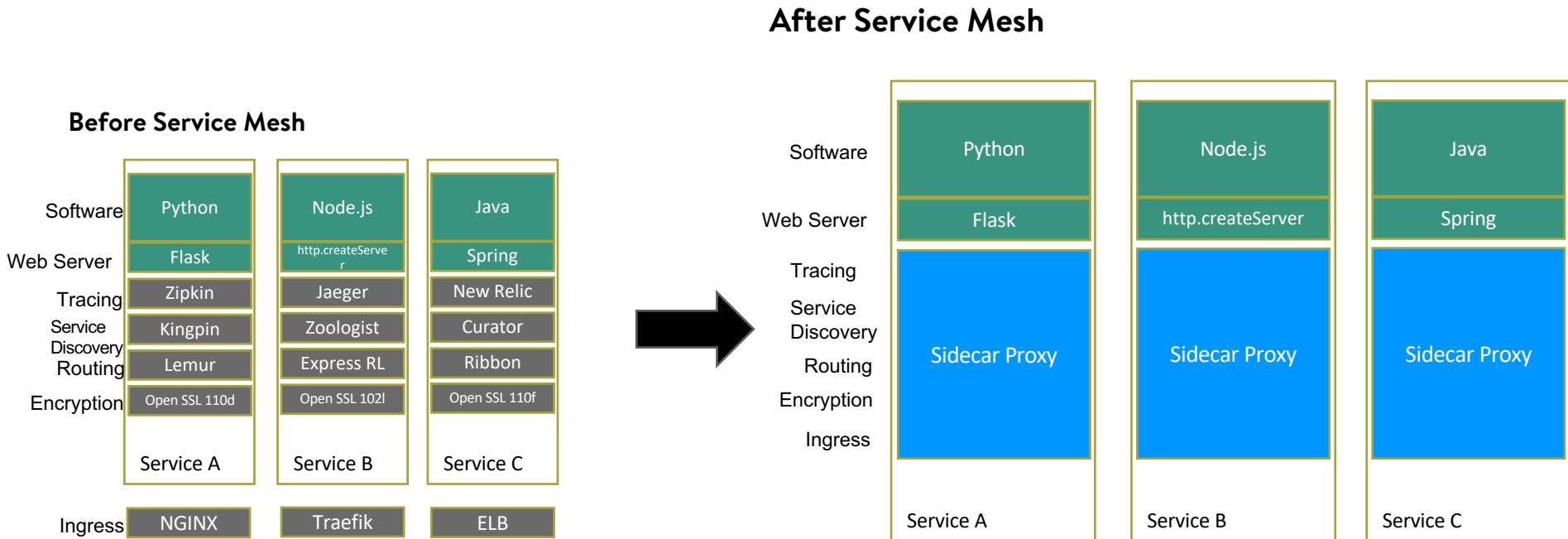
WHY SERVICE MESH?

“...A **SERVICE MESH** IS A DEDICATED INFRASTRUCTURE LAYER FOR FACILITATING SERVICE-TO-SERVICE COMMUNICATIONS BETWEEN MICROSERVICES”¹

Before Service Mesh



WHY SERVICE MESH?



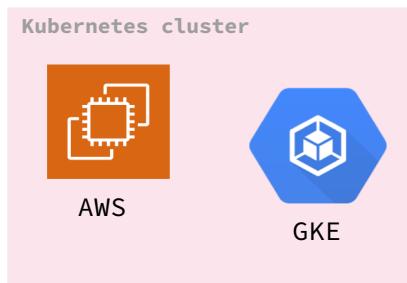
WHY SERVICE MESH?

- Increasing Application Resiliency
- Improving Developer Experience
- Metrics
- Performance
- Securing Communication



INVESTIGATIONS AND FINDINGS

- Where should we focus our priorities?
 - Which environments?



AWS



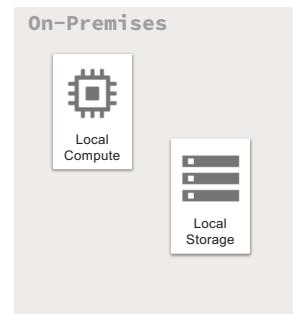
Kubernetes

6000 AWS Prod Pods
680 GKE Prod Pods

Functions
5500 unique Lambdas
3000 Daily Ave



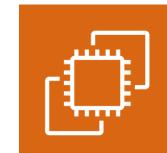
Serverless



On Premises

~7,000 Prod VMs

6,056 Prod EC2s



AWS EC2s

INVESTIGATIONS AND FINDINGS

- Why re-invent the wheel?
- Build or buy? What do we value?



NORDSTROM

INVESTIGATIONS AND FINDINGS

WHAT IS ON THE TABLE?

LINKERD PERFORMANCE TESTING

Load Testing – p90

Latency @ 500 Requests per Second	Latency @ 5,000 Requests per Second
3.70ms	4.23ms

Scalability Testing

Cluster	Number of Pods	Memory per Pod
Baseline	20	10 MB
Large Scale	3,500	10 MB

LINKERD FEATURE SET

- ✓ Lightweight proxy
- ✓ Service discovery
- ✓ Observability: service and route-level metrics include success rate, request volume, latency
- ✓ Diagnostic tools: service dependency maps, live traffic samples
- ✓ Traffic Splitting

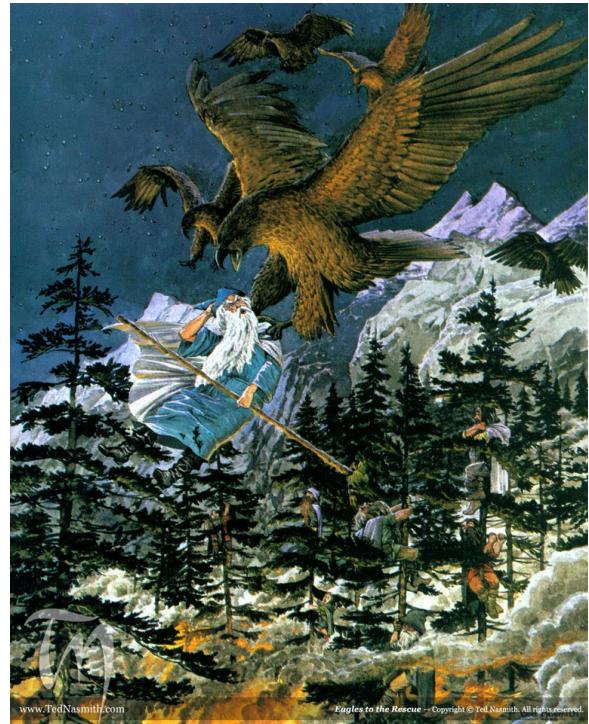
CHALLENGE ACCEPTED

- Secure communication
 - On premises
 - AWS
 - GCP
 - Kubernetes
- Resources
 - # Engineers
 - Time
- Extra complexity



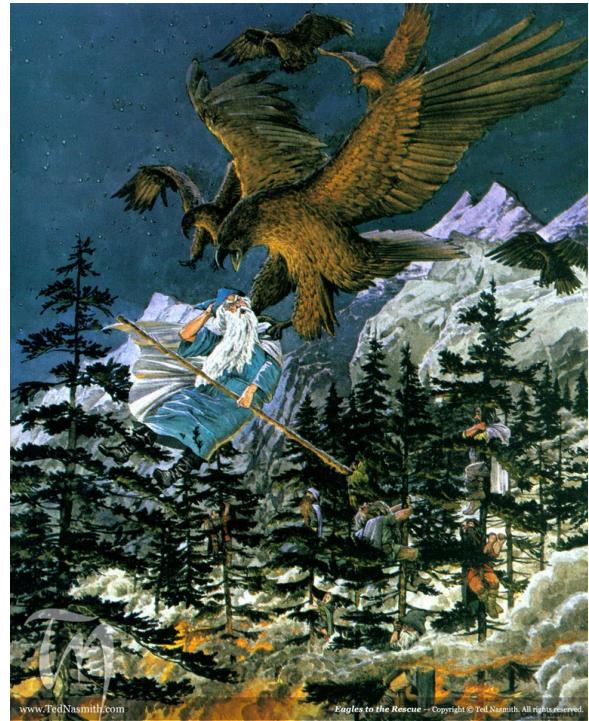
OUT OF THE FRYING PAN INTO THE FIRE

- Kubernetes?...Say what!?
- Installing Linkerd
- Challenges
- Open source community



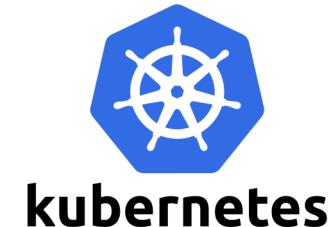
OUT OF THE FRYING PAN INTO THE FIRE

- Kubernetes?...Say what?!
- Installing Linkerd
- Challenges
- Open source community



KUBERNETES?...SAY WHAT?!

“Kubernetes is a **portable, extensible, open-source** platform for **managing containerized** workloads and services, that facilitates both **declarative** configuration and **automation.**”²



KUBERNETES?...SAY WHAT?!

“Kubernetes is a portable, extensible, open-source platform for **managing containerized workloads and services**, that facilitates both declarative configuration and automation.”²

- Monoliths -> microservices
- Desire to increase developer productivity
 - CI/CD automation for deployments
 - Common platform for services
- Desire to reduce costs
 - Many services on an instance

KUBERNETES?...SAY WHAT?!

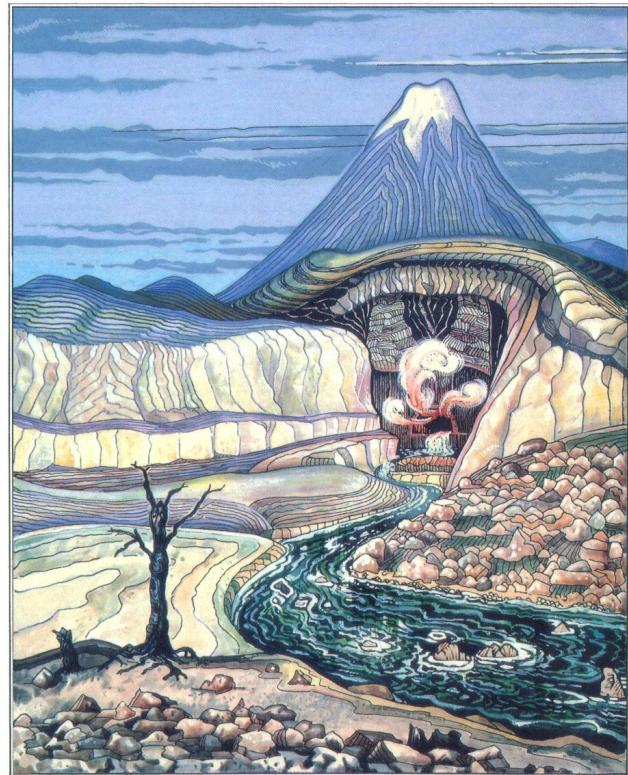
- New terminology
 - Pod, Deployment, ReplicaSet
 - K8s RBAC: ClusterRole, Role
 - Admission Controller, Webhook
- New set of tools to learn
 - kubectl
 - minikube
 - Go
- Development/Test clusters
 - AWS account permissions
 - Cost concerns
 - Custom tooling



bass + rey

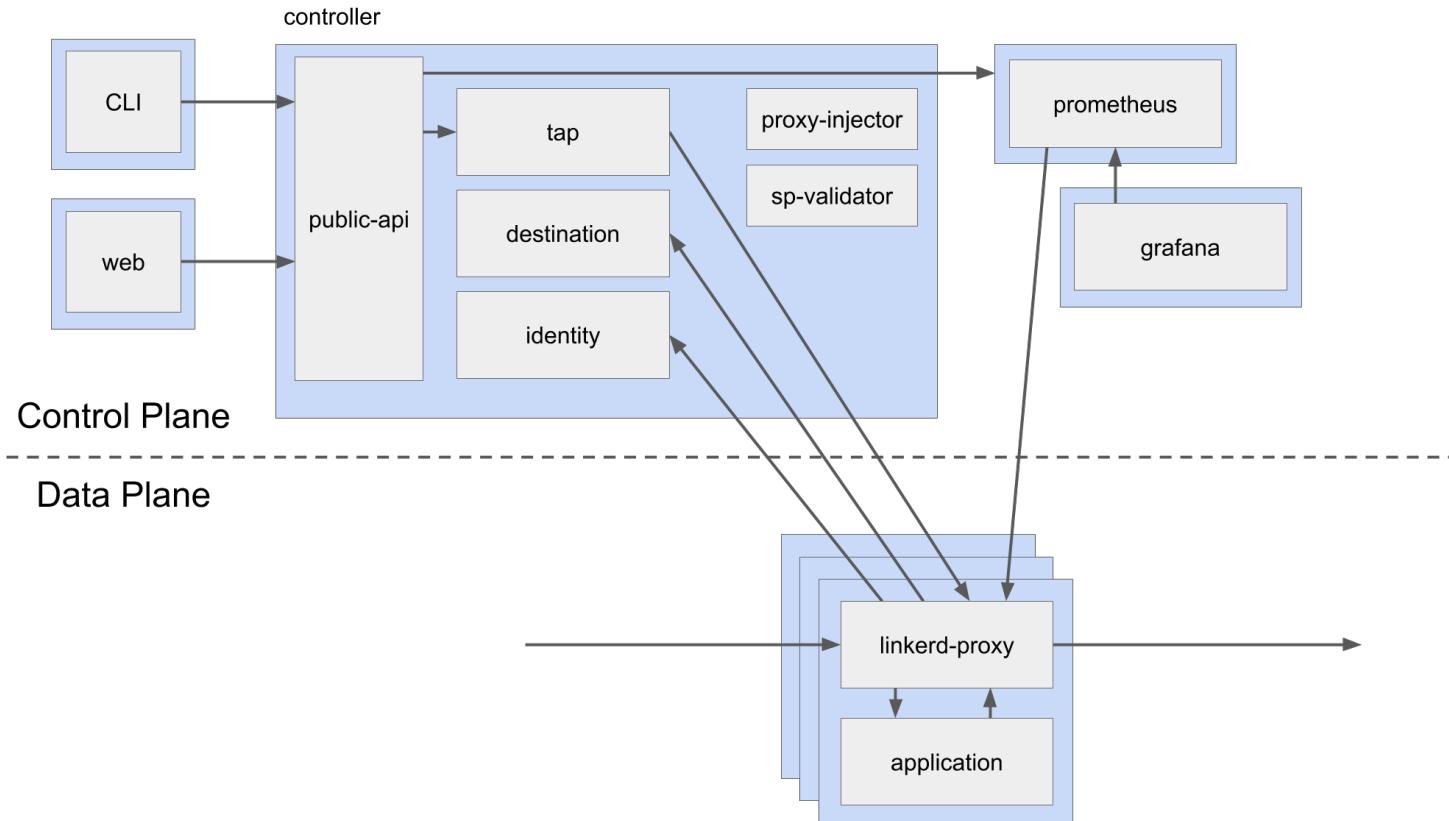
SERVICE MESH ROLLOUT

- Kubernetes?...Say what?!
- **Installing Linkerd**
- Surprises and challenges during rollout
- Open source community



. The Front Gate .

LINKERD



LINKERD INSTALL

The screenshot shows a dark-themed web page for the Linkerd documentation. At the top is a header bar with the Linkerd logo and a navigation menu icon. Below the header, a sidebar on the left lists sections: "Linkerd 2.x" (with a dropdown arrow), "Overview", "Getting Started" (which is highlighted in blue), "Features", "Tasks", and "Reference". The main content area has a large title "Getting Started" and a sub-section "Welcome to Linkerd! 🎉". The text explains the guide's purpose: installing Linkerd into a Kubernetes cluster and deploying a sample application. It also describes the installation process, mentioning the CLI, control plane, and data plane.

LINKERD

Linkerd 2.x

Overview

Getting Started

Features

Tasks

Reference

Getting Started

Welcome to Linkerd! 🎉

In this guide, we'll walk you through how to install Linkerd into your Kubernetes cluster. Then we'll deploy a sample application to show off what Linkerd can do.

Installing Linkerd is easy. First, you will install the CLI (command-line interface) onto your local machine. Using this CLI, you'll then install the *control plane* into your Kubernetes cluster. Finally, you'll “mesh” one or more services by adding the *data plane* proxies. (See the [Architecture](#) page for details.)

LINKERD INSTALL

The screenshot shows the official Linkerd documentation website. At the top is a dark blue header with the Linkerd logo (a teal stylized 'L') and the word "LINKERD". To the right of the logo is a three-line menu icon. Below the header is a light gray sidebar on the left containing navigation links: "Linkerd 2.x" (with a dropdown arrow), "Overview", "Getting Started" (which is bolded and highlighted in a white box), "Features", "Tasks", and "Reference". The main content area has a white background. It features a large, bold title "Getting Started" and a sub-headline "Welcome to Linkerd! 🎉". Below this, there is descriptive text: "In this guide, we'll walk you through how to install Linkerd into your Kubernetes cluster. Then we'll deploy a sample application to show off what Linkerd can do." A yellow callout box highlights the first sentence: "Installing Linkerd is easy. First, you will install the CLI (command-line interface) onto your local machine. Using this CLI, you'll then install the *control plane* into your Kubernetes cluster. Finally, you'll ‘mesh’ one or more services by adding the *data plane* proxies. (See the [Architecture](#) page for details.)"

Getting Started

Welcome to Linkerd! 🎉

In this guide, we'll walk you through how to install Linkerd into your Kubernetes cluster. Then we'll deploy a sample application to show off what Linkerd can do.

Installing Linkerd is easy. First, you will install the CLI (command-line interface) onto your local machine. Using this CLI, you'll then install the *control plane* into your Kubernetes cluster. Finally, you'll “mesh” one or more services by adding the *data plane* proxies. (See the [Architecture](#) page for details.)

LINKERD INSTALL

```
bbaggins@theshire-smial42:~$ linkerd install | kubectl apply -f -
```

LINKERD INSTALL

```
bbaggins@theshire-smial42:~$ linkerd install | kubectl apply -f -
deployment.extensions/linkerd-identity created
```

LINKERD INSTALL

```
bbaggins@theshire-smial42:~$ linkerd install | kubectl apply -f -
deployment.extensions/linkerd-identity created
deployment.extensions/linkerd-controller created
service/linkerd-proxy-injector created
```

LINKERD INSTALL

```
bbaggins@theshire-smial42:~$ linkerd install | kubectl apply -f -
deployment.extensions/linkerd-identity created
deployment.extensions/linkerd-controller created
service/linkerd-proxy-injector created

.
.

.
.

...
... 45 more resource creations later ...
```

```
bbaggins@theshire-smial42:~$
```

LINKERD INSTALL

```
bbaggins@theshire-smial42:~$ kubectl get pods -n linkerd
```

LINKERD INSTALL

```
bbaggins@theshire-smial42:~$ kubectl get pods -n linkerd
```

No resources found in linkerd namespace.

LINKERD INSTALL

```
bbaggins@theshire-smial42:~$ kubectl get deployments -n linkerd
```

NAME	READY	UP-TO-DATE	AVAILABLE	AGE
linkerd-controller	0/1	0	0	96s
linkerd-grafana	0/1	0	0	94s
linkerd-identity	0/1	0	0	97s
linkerd-prometheus	0/1	0	0	95s
linkerd-proxy-injector	0/1	0	0	93s
linkerd-sp-validator	0/1	0	0	91s
linkerd-tap	0/1	0	0	90s
linkerd-web	0/1	0	0	96s

LINKERD INSTALL

```
bbaggins@theshire-smial42:~$ kubectl describe replicaset linkerd-controller-1 -n linkerd
```

Events:

Type	Reason	Message
----	-----	-----
Warning	FailedCreate	Error creating: pods "linkerd-controller-1-" is forbidden: unable to validate against any pod security policy: [spec.initContainers[0].securityContext.runAsNonRoot: Invalid value: false: must be true spec.initContainers[0].securityContext.capabilities.add: Invalid value: "NET_ADMIN": capability may not be added spec.initContainers[0].securityContext.capabilities.add: Invalid value: "NET_RAW": capability may not be added]

LINKERD INSTALL

```
bbaggins@theshire-smial42:~$ kubectl describe replicaset linkerd-controller-1 -n linkerd
```

Events:

Type	Reason	Message
----	-----	-----
Warning	FailedCreate	Error creating: pods "linkerd-controller-1" is forbidden: unable to validate against any pod security policy : [spec.initContainers[0].securityContext. runAsNonRoot : Invalid value: false: must be true spec.initContainers[0].securityContext.capabilities.add: Invalid value: " NET_ADMIN ": capability may not be added spec.initContainers[0].securityContext.capabilities.add: Invalid value: " NET_RAW ": capability may not be added]

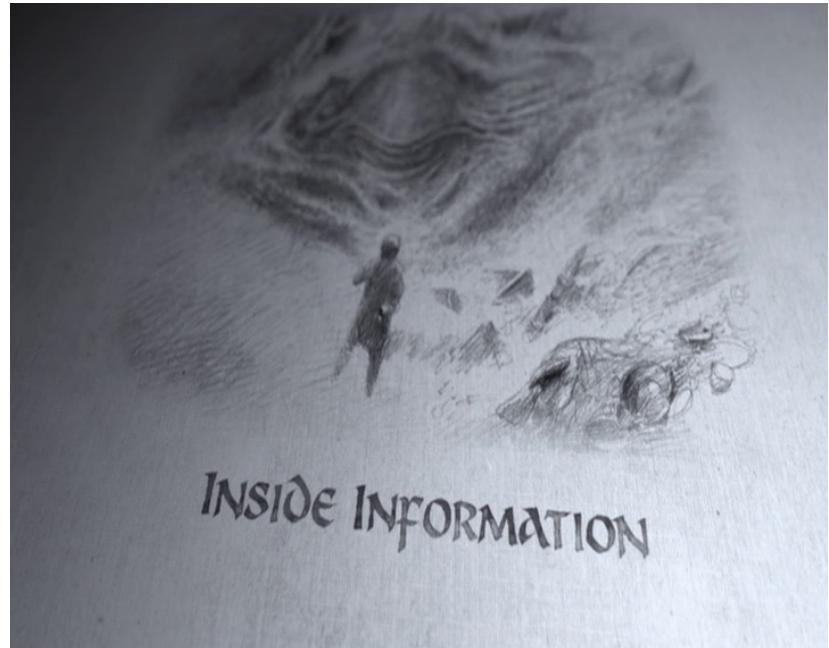
LINKERD INSTALL



NORDSTROM

INSIDE INFORMATION

- Kubernetes?...Say what?!
- Installing Linkerd
- **Challenges**
- Open source community



CHALLENGES



CHALLENGES



NORDSTROM

CHALLENGES

- We are not cluster administrators

```
Error from server (Forbidden): error when creating "linkerd.yaml":  
clusterroles.rbac.authorization.k8s.io is forbidden: User "cody.vandermyn"  
cannot create resource "clusterroles" in API group "rbac.authorization.k8s.io"  
at the cluster scope
```

CHALLENGES

- We are not cluster administrators
- Pod Security Policies (PSP)
 - mustRunAsNonRoot
 - NET_ADMIN, NET_RAW Linux capabilities are prohibited
 - User and Group IDs must be greater than 10000

THE RETURN JOURNEY

- Kubernetes?...Say what!?
- Installing Linkerd
- Challenges
- **Open source community**



OPEN SOURCE COMMUNITY

- Container Networking Interface (CNI) Plugin
 - Provides an interface for a custom executable to perform network related activities whenever a Pod is created or deleted
 - Standard in/out is used as the mechanism to communicate from one plugin to another
 - Istio and Calico already had CNI plugins we could reference



OPEN SOURCE COMMUNITY

- Container Networking Interface (CNI) Plugin
- Deployment of the CNI plugin
 - Typical installation via a Daemonset didn't meet our needs

OPEN SOURCE COMMUNITY

- Container Networking Interface (CNI) Plugin
- Deployment of the CNI plugin
- AWS Certificate Manager Private Certificate Authority (ACM PCA)
 - Linkerd acts as its own CA and the proxies trust the certificates created
 - Fork of Linkerd to add this capability

LINKERD INSTALL

```
bbaggins@theshire-smial42:~$ kubectl get pods -n linkerd
```

NAME	READY	STATUS	RESTARTS	AGE
linkerd-controller-5b95b6f449-2xw26	3/3	Running	2	12d
linkerd-controller-5b95b6f449-7mlh8	3/3	Running	2	12d
linkerd-controller-5b95b6f449-84kwg	3/3	Running	2	12d
linkerd-grafana-5d784ff96b-2z8nx	2/2	Running	0	12d
linkerd-identity-7546c77559-pvdw6	2/2	Running	1	13d
linkerd-identity-7546c77559-qxwt8	2/2	Running	1	12d
linkerd-identity-7546c77559-tdb99	2/2	Running	1	12d
linkerd-prometheus-8448f6d54f-4wdmm	2/2	Running	0	13d
linkerd-proxy-injector-78f5848766-clkjf	2/2	Running	1	13d
linkerd-proxy-injector-78f5848766-sdcch	2/2	Running	1	12d
linkerd-proxy-injector-78f5848766-t7z7j	2/2	Running	1	171m
linkerd-sp-validator-5874c6677-5brvf	2/2	Running	1	12d
linkerd-sp-validator-5874c6677-7qz8z	2/2	Running	1	12d
linkerd-sp-validator-5874c6677-wjpg6	2/2	Running	1	3h8m
linkerd-tap-576f7f8549-k8mfd	2/2	Running	1	12d
linkerd-tap-576f7f8549-pfctb	2/2	Running	1	12d

THE LAST STAGE

- Easy onboarding experience

```
metadata:  
  annotations:  
    linkerd.io/inject: enabled  
  labels:  
    nordstrom.com/uses-linkerd: true  
    app: silmarillion
```

- Cluster impact
- Open Source Contributions
- Long journey ahead



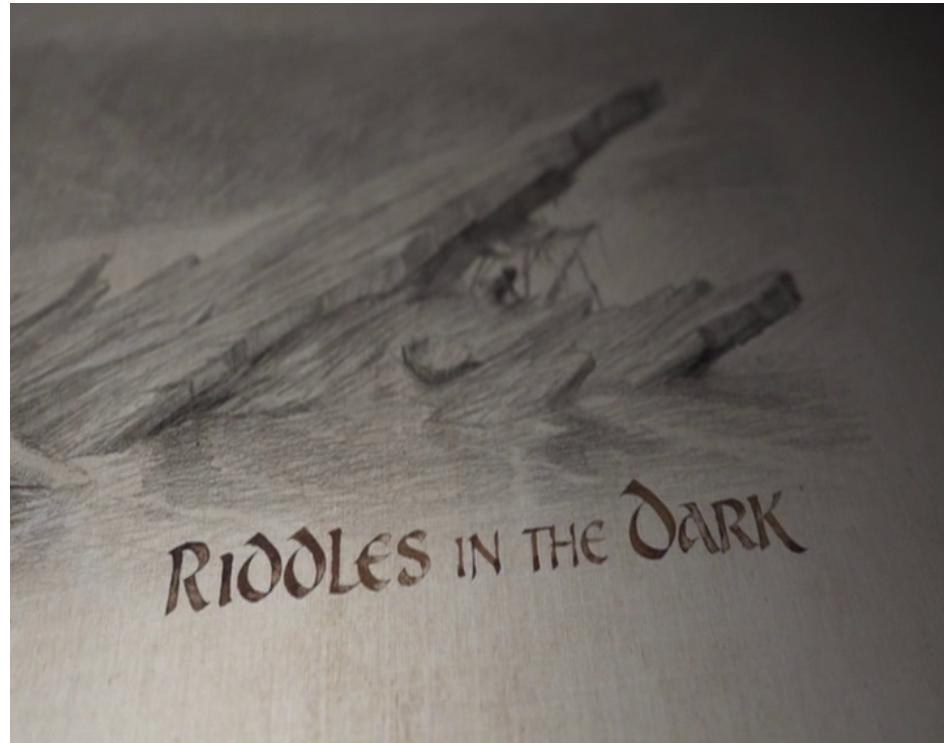
THE END

Q&A

Contact Information

Cody: cody.vandermyn@nordstrom.com

Hema: hemalekha.lee@nordstrom.com



NORDSTROM

REFERENCES AND DISCLAIMERS

¹https://en.wikipedia.org/wiki/Service_mesh

²<https://kubernetes.io/docs/concepts/overview/what-is-kubernetes/>

Images:

<https://www.sutori.com/story/the-evolution-of-bilbo-baggins--M5RRmVV9KCV2erDxBwVyP2v5>

<https://www.tednasmith.com/tolkien/eagles-to-the-rescue/>

<https://scifi.stackexchange.com/questions/96167/why-model-smaug-after-a-cat>

http://tolkiengateway.net/wiki/Front_Gate

https://ouatff.fandom.com/wiki/Bilbo_Baggins

https://lotr.fandom.com/wiki/Inside_Information

<https://www.pinterest.com/pin/488499890818388930/>

[https://lotr.fandom.com/wiki/Riddles_in_the_Dark_\(chapter\)](https://lotr.fandom.com/wiki/Riddles_in_the_Dark_(chapter))

<https://soundcloud.com/bluefax/hobbit19>

EXTRA SLIDES

Extra Slides