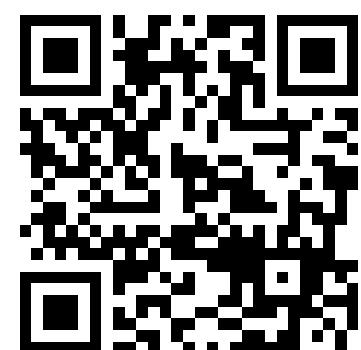


Le Seigneur Des Conteneurs

Un atelier de migration vers Kubernetes et Traefik



<https://containous.github.io/slides/devoxx-fr-2019>

How To Use These Slides?

- **Browse the slides:** Use the arrows
 - Change chapter: Left/Right arrows
 - Next or previous slide: Top and bottom arrows
- **Overview of the slides:** keyboard's shortcut "o"
- **Speaker mode (and notes):** keyboard's shortcut "s"

Whoami 1/2

Nicolas Mengin

- Part Time DevOps & Code Craftsman @ [Containous](#)
- Blacksmith on [Traefik](#)
- [!\[\]\(746d018fdf6ab02bf5fb7681133e8b29_img.jpg\) @nicomengin](#)
- [!\[\]\(5daa6eee1904cb6b9d765700250de764_img.jpg\) nmengin](#)



Whoami 2/2

Damien DUPORTAL

- Traefik's Developer  Advocate @ Containous
-  @DamienDuportal
-  dduortal



Containous

<https://containo.us>

- We Believe in Open Source
- We Deliver Traefik
- Commercial Support for Traefik
- 20 people, 90% tech



Forge Content

- TODO: indicate the checklist
-
-

Once Upon A Time...

An Infrastructure War

- Docker as a standard
- Orchestrators: Docker Swarm, Rancher Caddle, Mesos, Kubernetes...
- The war lasted couple of years...

One Orchestrator To Rule Them All

- **Kubernetes**
- Used by the concurrents
- Standard in industry
- Powerful but not easy to master

Agenda

The Hobbit House: Introduction To Traefik With Docker

Break

Saruman Tower: Migrate Traefik To Kubernetes

Break

The Castle: Migrate The Infrastructure To Kubernetes

The Hobbit House



The Hobbit House

We want a server in AWS:

- to host our own SCM Server,
- and our own Continuous Integration,
- and a static web site,
- and a "web" command line.

Infrastructure Setup

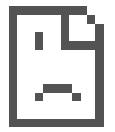
- An AWS VM with a public IP 35.178.178.237 and SSH access
- A domain name lab01.demo.containous.cloud pointing to 35.178.178.237

```
$ dig +short lab01.demo.containous.cloud  
35.178.178.237
```

- Docker and docker-compose for services

Reality Check

<http://lab01.demo.containous.cloud/>



This site can't be reached

refused to connect.

Search Google for

ERR_CONNECTION_REFUSED

Agenda

- Traefik
- Web Server
- CI Server
- SCM: A Gitea Git Server
- Web CLI
- SSL for everyone

Why Traefik?



Why, Mr Anderson?

Evolution Of Software Design



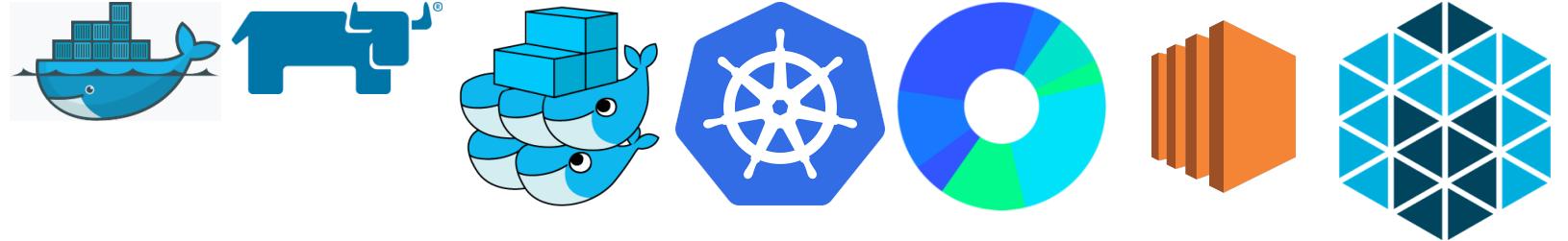
The Premise Of Microservices...



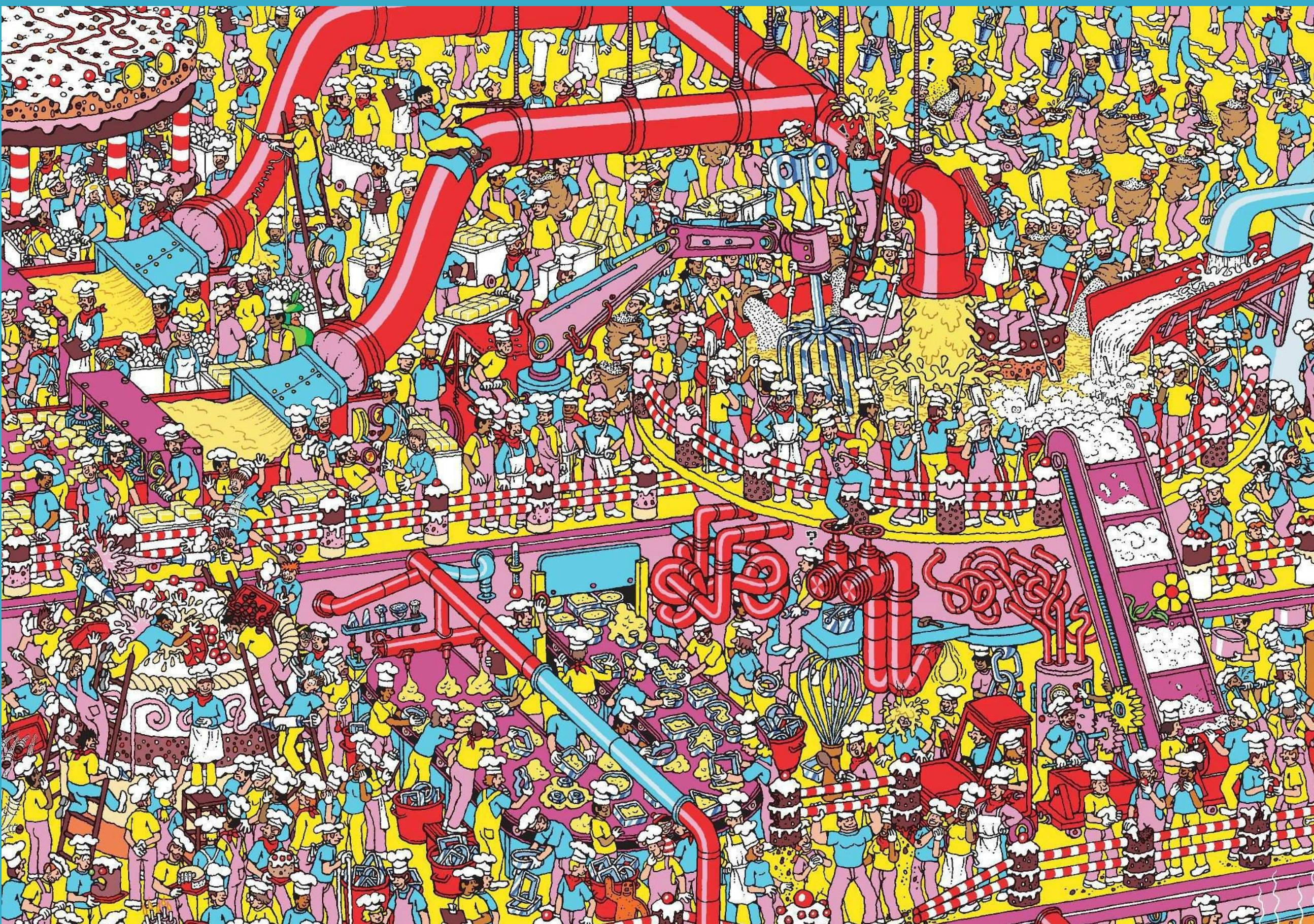
...And What Happens

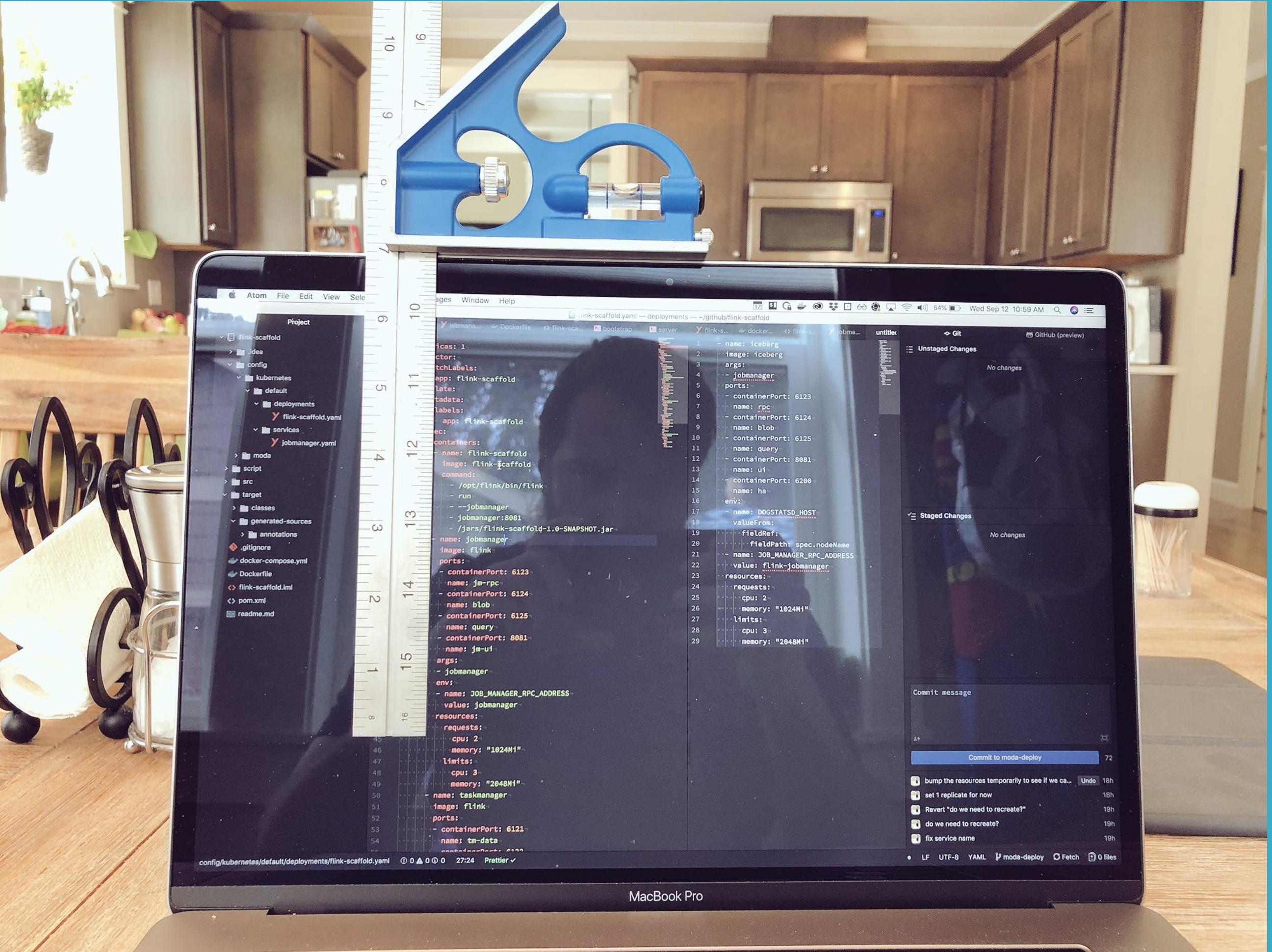


Tools Of The Trade



Where's My Service?





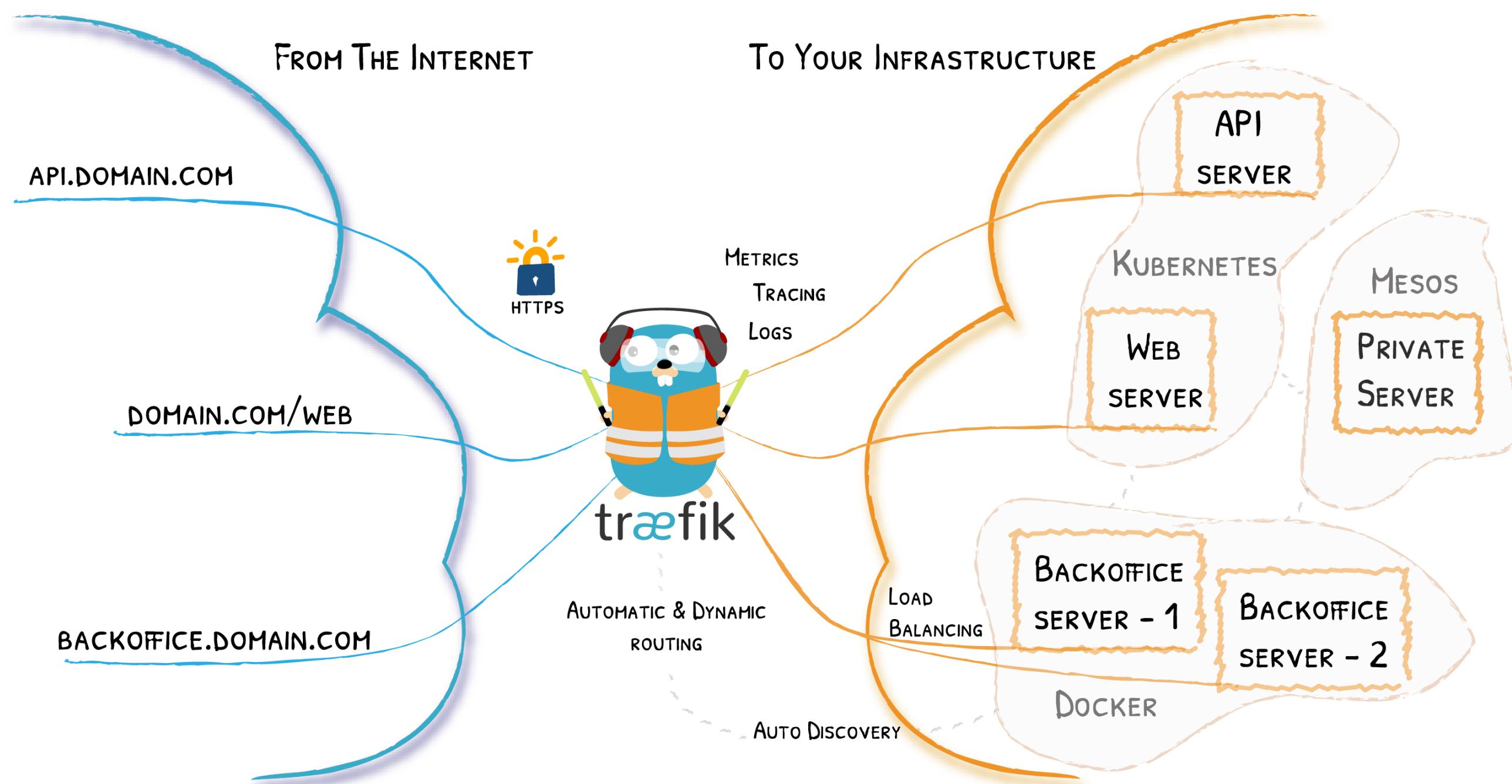
Source: <https://twitter.com/Caged/status/1039937162769096704>

What If I Told You?



That You Don't Have to Write This Configuration File...?

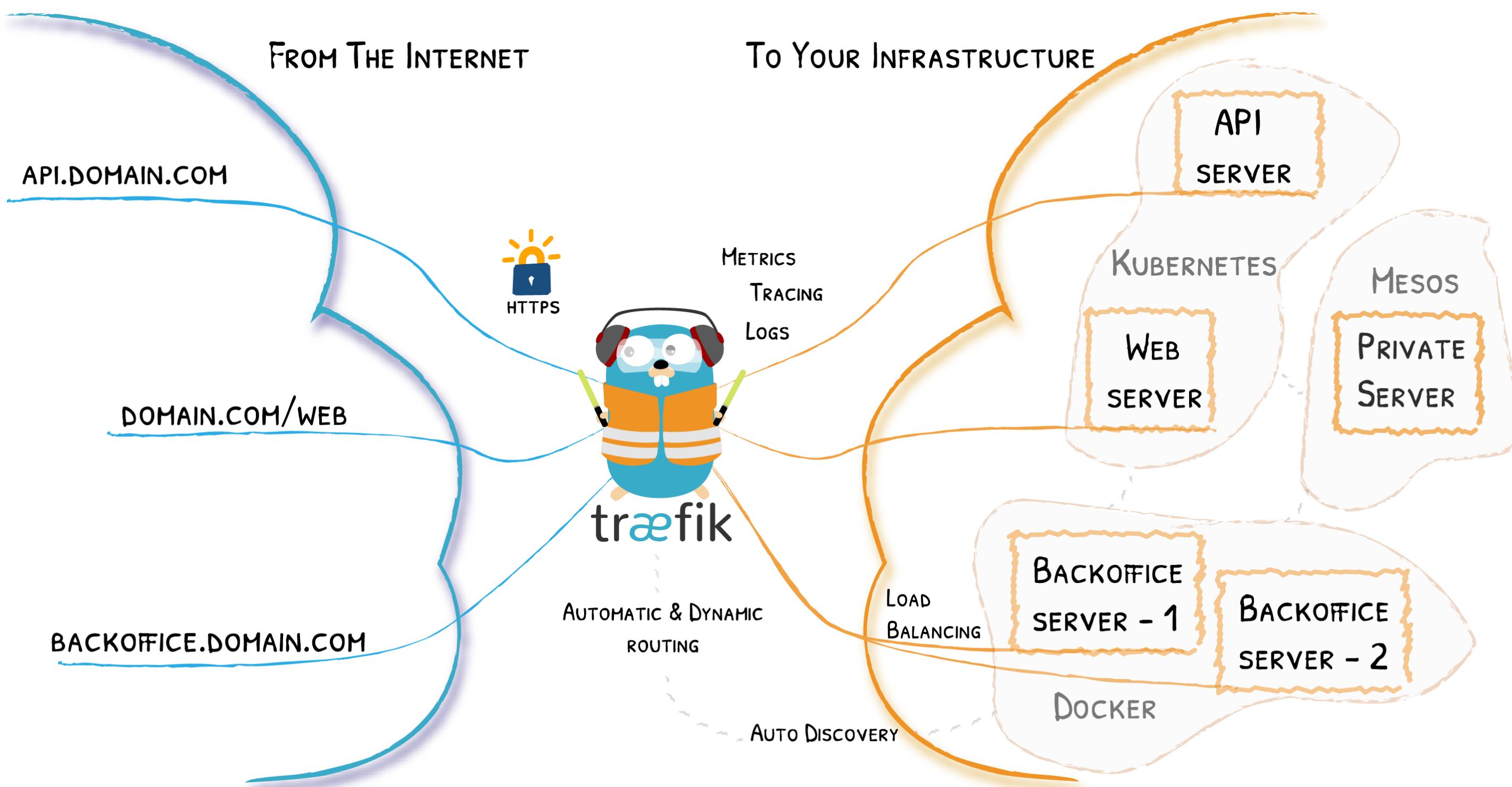
Here Comes Traefik!



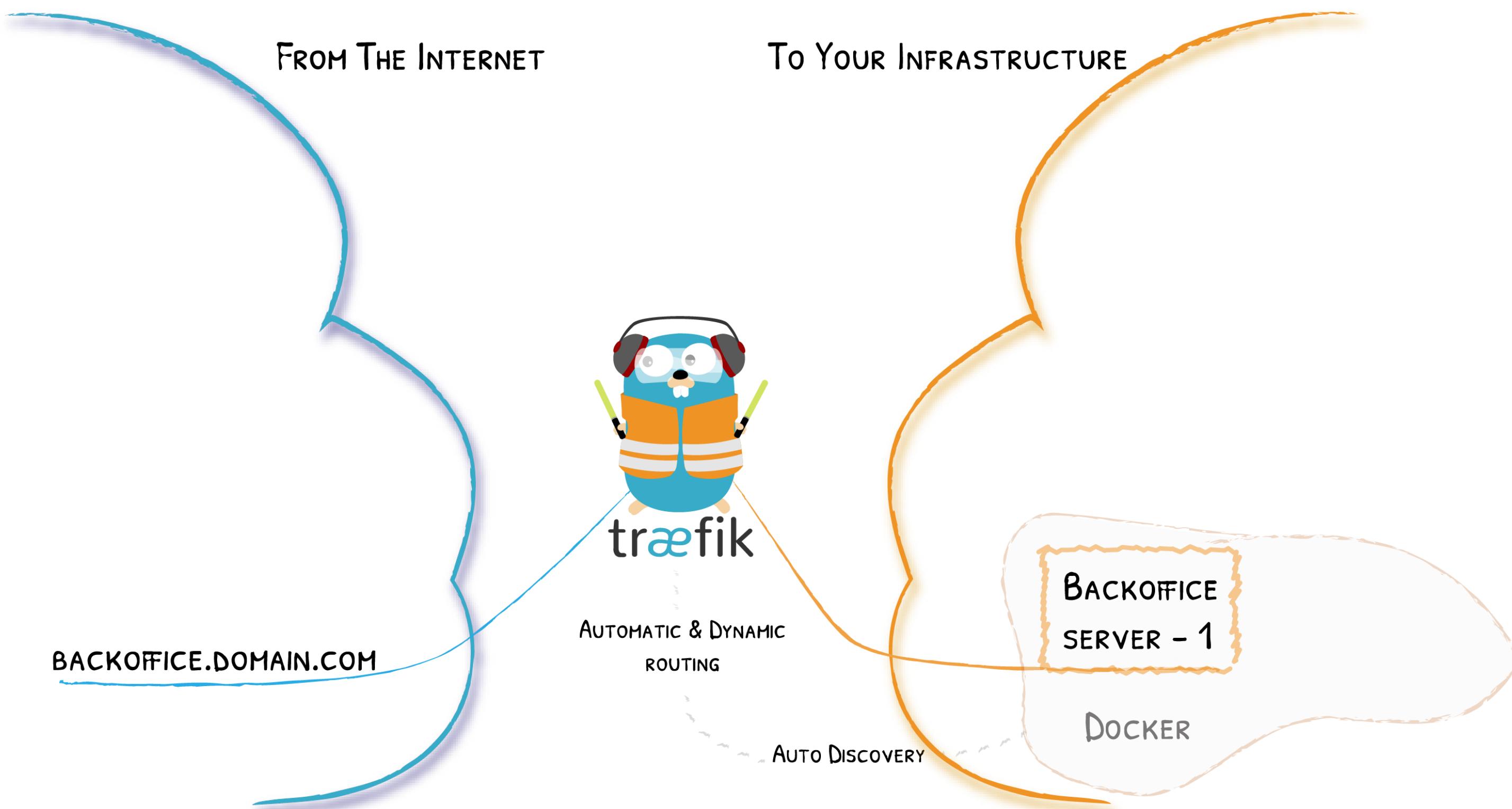
Traefik Project

-  <https://github.com/containous/traefik>
- MIT License
- Written in Go
- 21,000+ 
- 600M+ 
- 350+ 

Remember The Diagram?



Let's Simplify



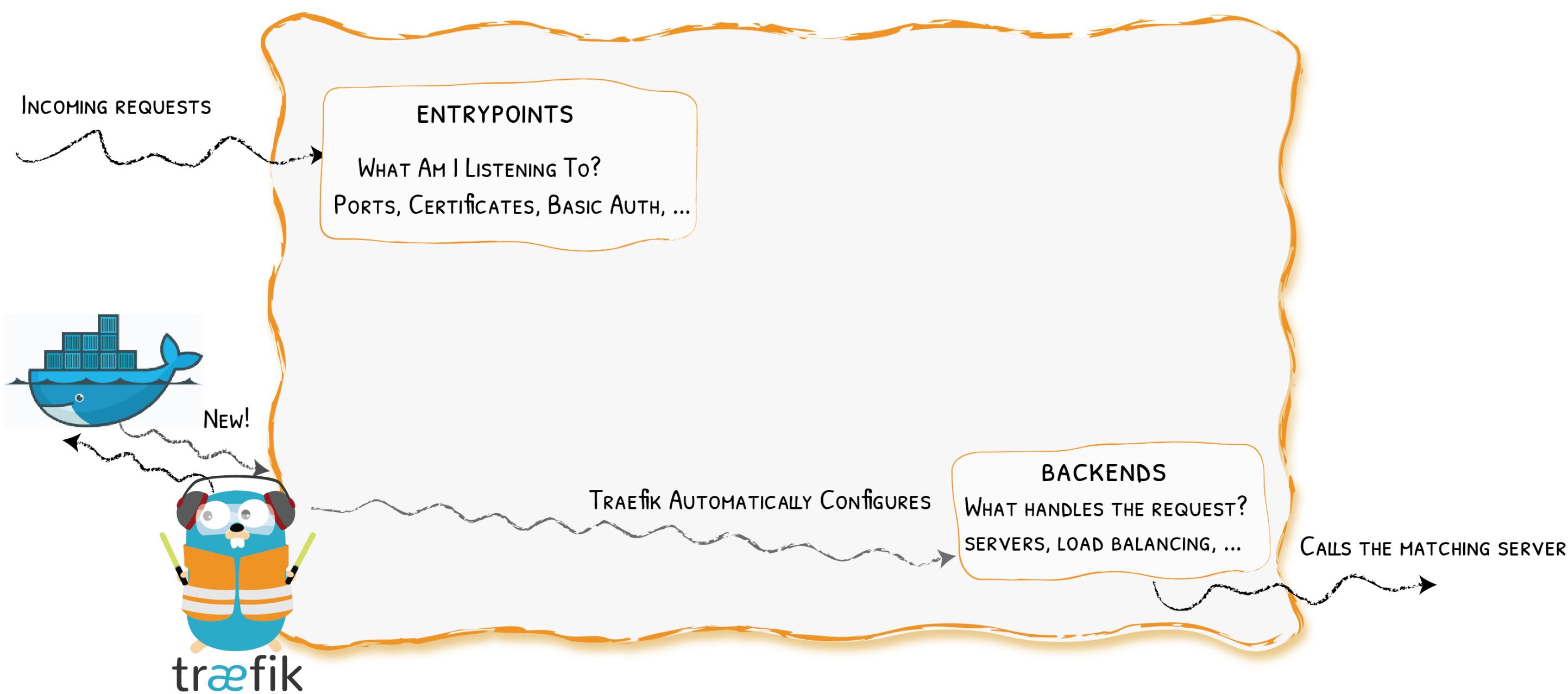
Providers



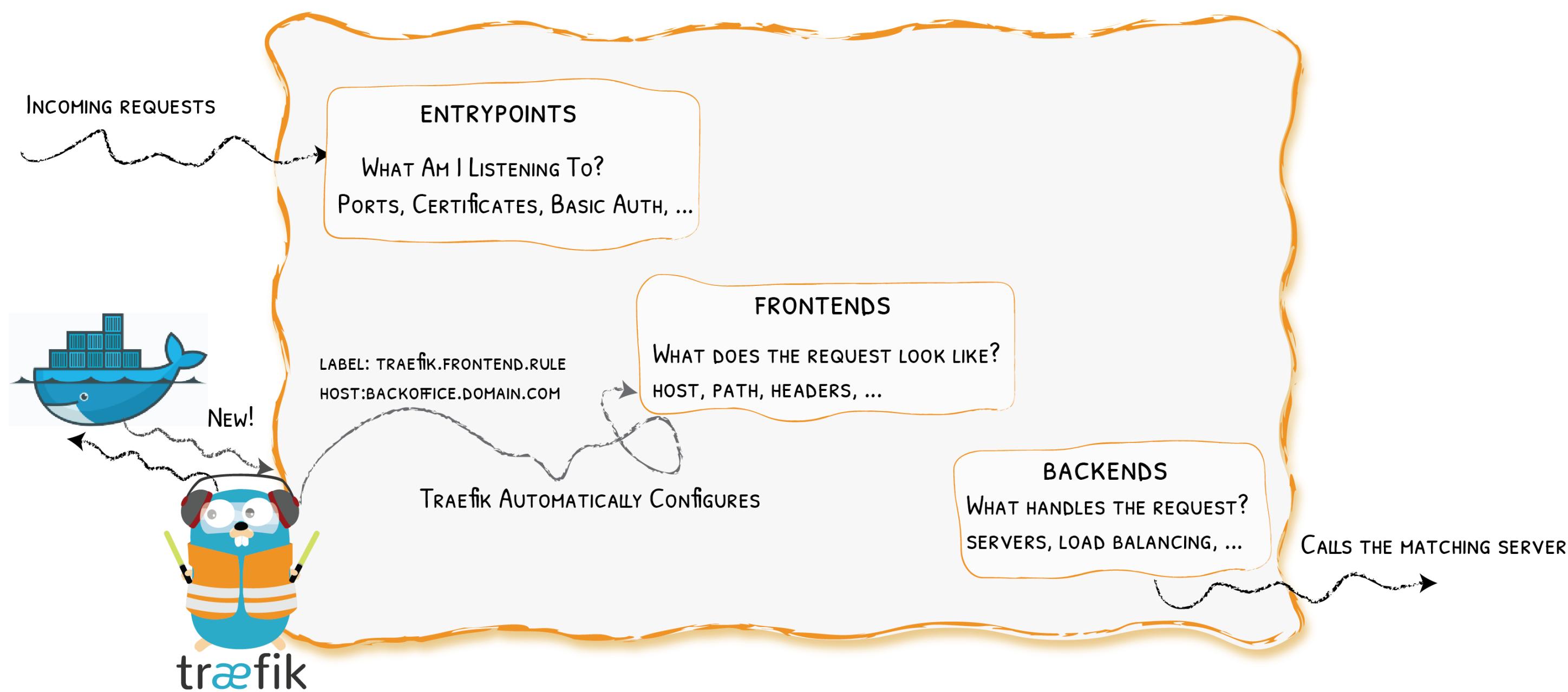
Entrypoints



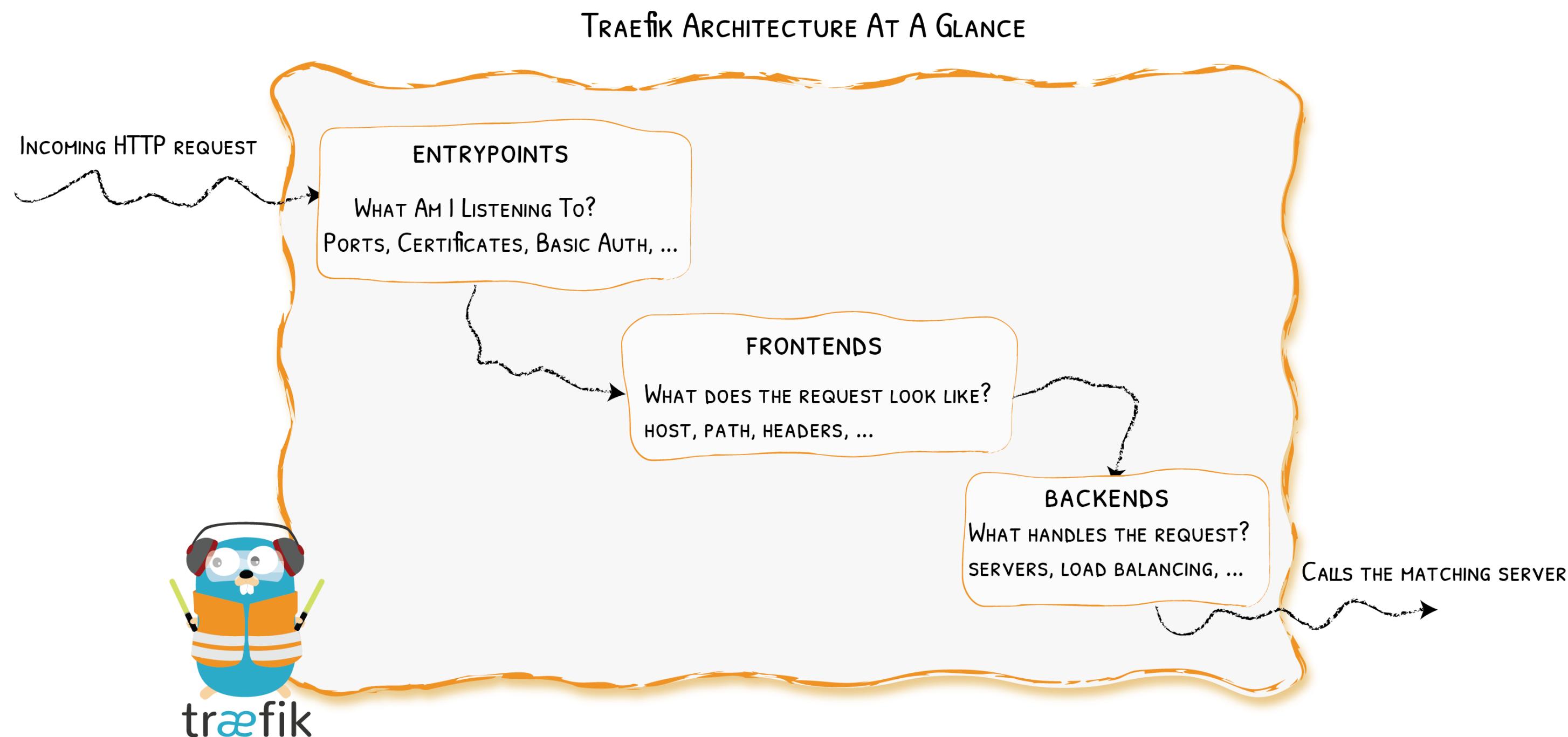
Backends



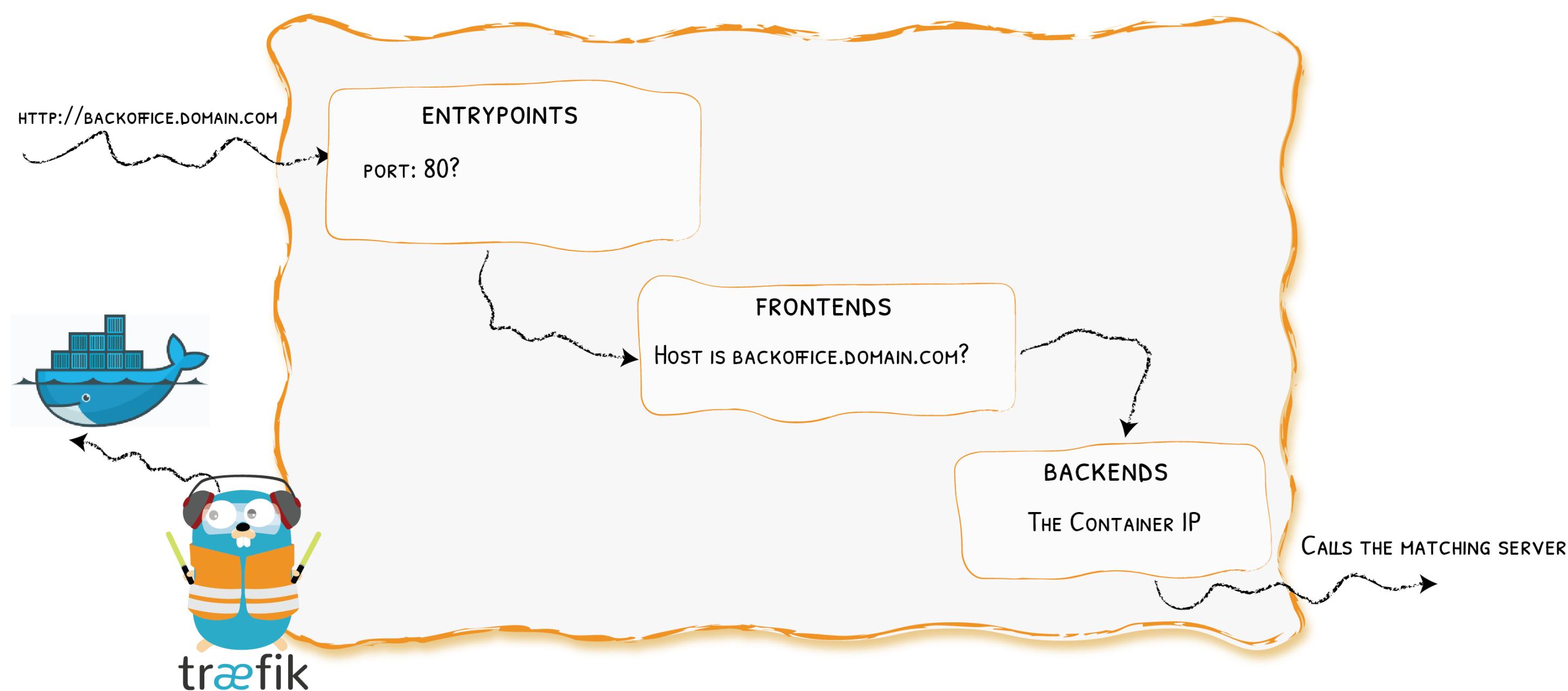
Frontends



At A Glance



In Practice



Let's Go

Traefik Setup

- Step 1: Compose file in /home/ubuntu/lab-docker-k8s/01-docker/docker-compose.yml:

```
version: '2.4'

services:
  edge:
    image: traefik:1.7.10
    command:
      - "--docker.domain=lab01.demo.containous.cloud"
    ports:
      - "80:80"
      - "443:443"
    volumes:
      # To communicate with the Docker Engine
      - /var/run/docker.sock:/var/run/docker.sock
```

- Step 2: Start the stack

```
$ docker-compose up -d
```

Reality Check

<http://lab01.demo.containous.cloud/>



It's good: we have an HTTP answer!

Agenda

- Traefik
- **Web Server**
- CI Server
- SCM: A Gitea Git Server
- Web CLI
- SSL for everyone

Goal

- We want to host a static webserver behind Traefik

Problem

- How to tell Traefik to route requests to the web server?

```
http://lab01.demo.containous.cloud/index.html
  -> Traefik
      -> http://<Webserver Private IP>/index.html
```

The Web Server Setup

- Step 1: web server in Compose. Check the labels:

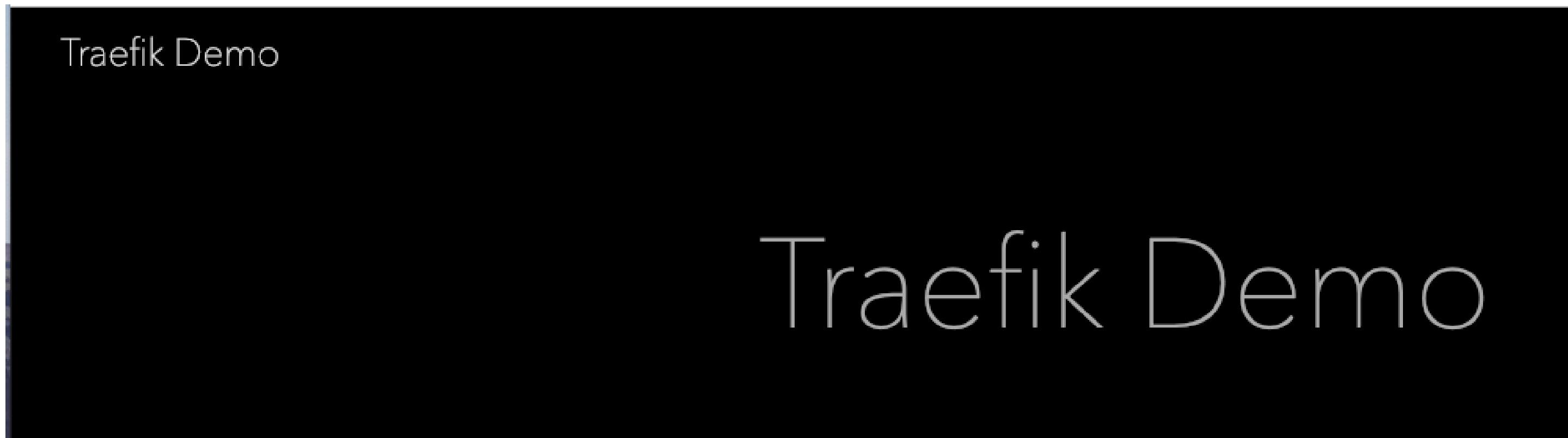
```
web:  
  build: ./web/  
  labels:  
    - "traefik.frontend.rule=Path:/"
```

- Step 2: Start the Web Server:

```
docker-compose up -d web
```

Reality Check

<http://lab01.demo.containous.cloud/>



It's good: we have a web page!

Agenda

- Traefik
- Web Server
- **CI Server**
- SCM: A Gitea Git Server
- Web CLI
- SSL for everyone

Goal

- We want to host our own automation system for Continuous Integration
 - Let's use Jenkins

Challenge 1/3

- Problem:
 - Jenkins exposes 2 ports: 8080 and 50000. How to let Traefik know to only use 8080?
- Solution:
 - Select the port with the label `traefik.port`:

```
- "traefik.port=8080"
```

Challenge 2/3

- Problem:
 - How to let Traefik know when to send requests to the Jenkins backend instead of the webserver?
- Solution:
 - Change the frontend rule to use PathPrefix:

```
- "traefik.frontend.rule=PathPrefix:/jenkins"
```

```
http://lab01.demo.containous.cloud/jenkins/configuration
  -> Traefik
  -> http://<Jenkins Private IP>:8080/jenkins/configuration
```

Challenge 3/3

- **Problem:**
 - How to tell Jenkins to accept requests under /jenkins?
- **Solution:**
 - Use the Jenkins flag --prefix=/jenkins with the variable JENKINS_OPTS:

```
environment:  
  - JENKINS_OPTS=--prefix=/jenkins
```

Jenkins Setup

- Step 1: Edit Compose file:

```
jenkins:  
  image: jenkins/jenkins:2.150.3-alpine  
  expose:  
    - 8080  
    - 50000  
  environment:  
    - JENKINS_OPTS=--prefix=/jenkins  
  labels:  
    - "traefik.port=8080"  
    - "traefik.frontend.rule=PathPrefix:/jenkins"
```

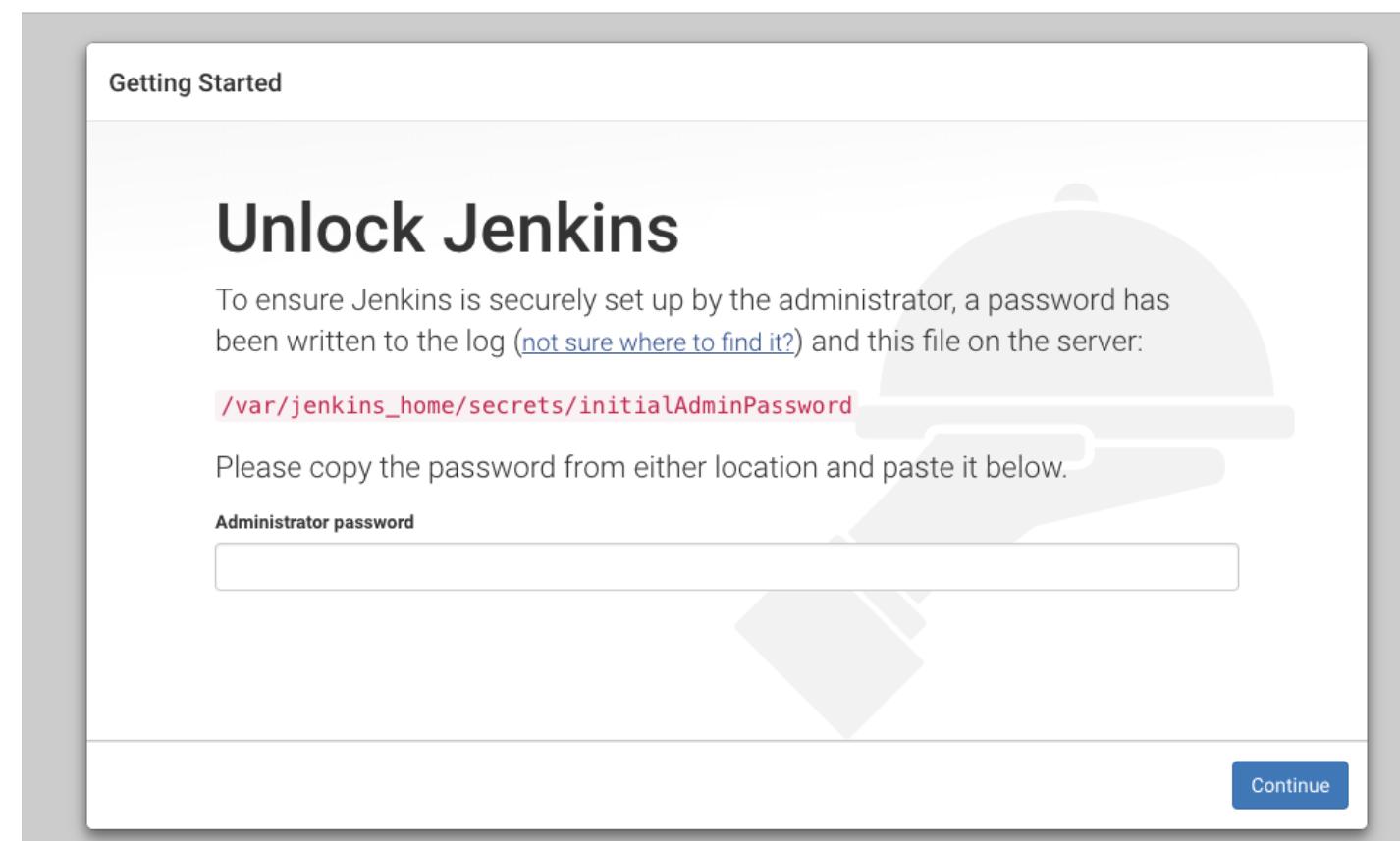
- Step 2: update the service

```
docker-compose up -d jenkins
```

Reality Check

Click on the "Jenkins" link:

<http://lab01.demo.containous.cloud/jenkins>



It's good: we can setup Jenkins!

Agenda

- Traefik
- Web Server
- CI Server
- **SCM: A Gitea Git Server**
- Web CLI
- SSL for everyone

Goal

- We want to host our own git server
 - Let's use Gitea, A painless self-hosted Git service.

Challenge

- Problem:
 - Gitea only serves requests under /: How to remove the prefix /gitserver?

```
http://{{lab-domain}}/gitserver/index.html
  -> Traefik
      -> http://<Gitea private IP>:3000/index.html
```

- Solution:
 - Use the Traefik's Frontend Rule PathPrefixStrip

```
- "traefik.frontend.rule=PathPrefixStrip:/gitserver"
```

Gitea Setup

- Step 1: Edit Compose file:

```
gitserver:  
  image: gitea/gitea:latest  
  expose:  
    - "3000"  
    - "22"  
  environment:  
    - ROOT_URL=/gitserver  
  labels:  
    - "traefik.port=3000"  
    - "traefik.frontend.rule=PathPrefixStrip:/gitserver"
```

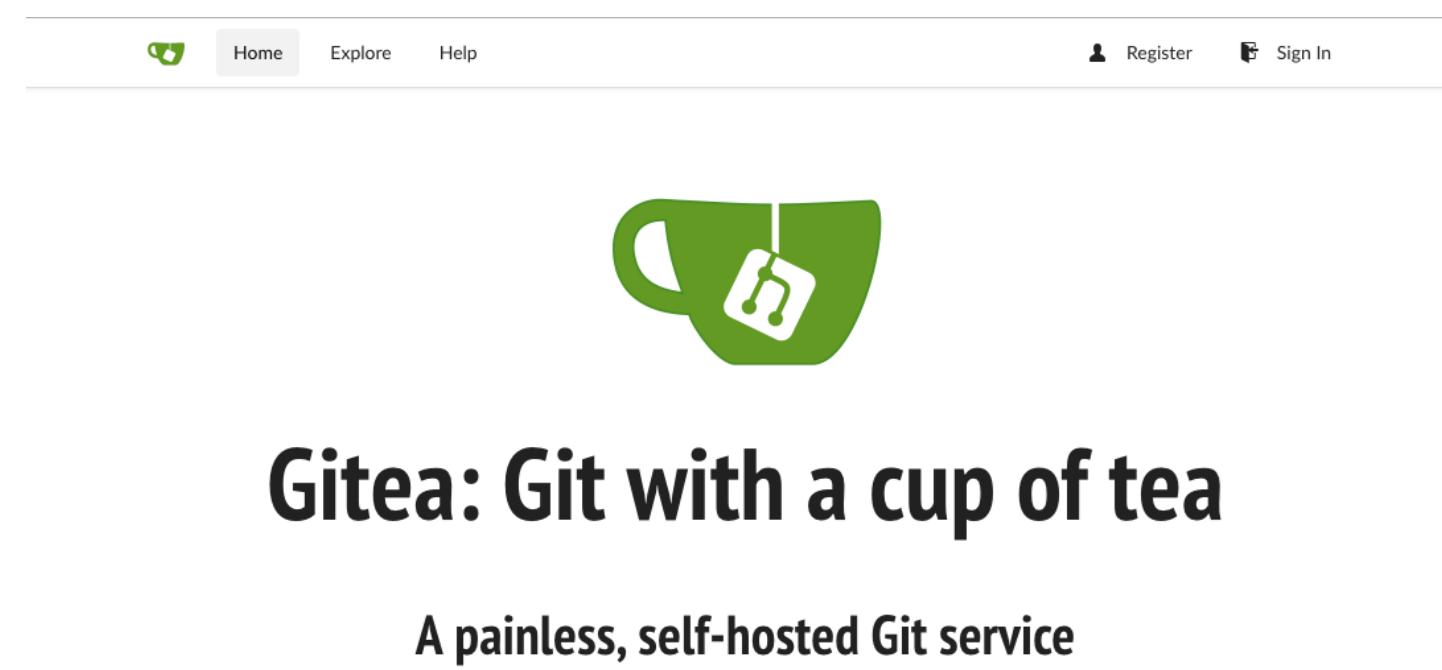
- Step 2: create the service

```
docker-compose up -d gitserver
```

Reality Check

Try the "Gitea Git server" link:

<http://lab01.demo.containous.cloud/gitserver>



It's good: we can setup Gitea!

Agenda

- Traefik
- Web Server
- CI Server
- SCM: A Gitea Git Server
- **Web CLI**
- SSL for everyone

Goal

- We want to host our own Web Command Line
 - Let's use TTYD, Share your terminal over the web.

Challenge

- **Problem:** TTYD requires Websockets
- **Solution:**
 - It's not even a problem with Traefik!

Easy Peasy!

- Step 1: Edit Compose file:

```
ttyd:  
  image: ts10922/ttyd  
  labels:  
    - "traefik.frontend.rule=PathPrefixStrip:/ttyd"
```

- Step 2: create the service

```
docker-compose up -d ttyd
```

Reality Check

Try the "TTYD Web Command Line" link:

<http://lab01.demo.containous.cloud/ttyd>



It's good: we have our own "Dev Box" in a web browser!

Agenda

- Traefik
- Web Server
- CI Server
- SCM: A Gitea Git Server
- Web CLI
- **SSL for everyone**

Goals

- Use HTTPS instead of HTTP
- Do NOT care about certificates and renewal
- Use a TOML configuration file
- Redirect any incoming HTTP request to HTTPS:

```
http://lab01.demo.containous.cloud/  
-> https://lab01.demo.containous.cloud/
```



Let's Encrypt is a free, automated, and open Certificate Authority.

It uses the "ACME" protocol to verify that you control a given domain name and to issue you a certificate.

Problem 1/4

- **Problem:**
 - How to tell Traefik to listen on port 443 for HTTPS requests?
- **Solution:**
 - Create a new entrypoint,
 - Set it as a default entrypoint:

```
defaultEntryPoints = ["http", "https"]

[entryPoints]
  [entryPoints.https]
    address = ":443"
    [entryPoints.https.tls]
```

Problem 2/4

- Problem:
 - How to tell Traefik to redirect request from http to https?
- Solution:
 - Configure the new endpoint http:

```
defaultEntryPoints = ["http", "https"]

[entryPoints]
  [entryPoints.https]
    address = ":443"
      [entryPoints.https.tls]
        [entryPoints.http]
          address = ":80"
            [entryPoints.http.redirect]
              entryPoint = "https"
```

Problem 3/4

- **Problem:**
 - How to tell Traefik to use Let's Encrypt for HTTPS?
- **Solution:**
 - Configure the ACME/Let's Encrypt provider:

```
[acme]
email = "lab01@devoxx.lab"
storage = "/acme.json"
entryPoint = "https"
onHostRule = true
```

- Give the needed rights to the / acme.json file (600)

Problem 4/4

- **Problem:**
 - Traefik detects itself as a docker container with a port, and tries to request a 2nd certificate for edge.lab01.demo.containous.cloud
- **Solution:**
 - Exclude Traefik's container with the label traefik.enable=false

Traefik Setup 1/2

- Step 1: Create the configuration file `traefik.toml`:

```
defaultEntryPoints = ["http", "https"]

[entryPoints]
  [entryPoints.https]
    address = ":443"
    [entryPoints.https.tls]
  [entryPoints.http]
    address = ":80"
    [entryPoints.http.redirect]
      entryPoint = "https"

[acme]
email = "lab01@devoxx.lab"
storage = "/acme.json"
entryPoint = "https"
onHostRule = true

[docker]
domain=lab01.demo.containous.cloud
watch = true
```

Traefik Setup 2/2

- Step 2: Adapt the Compose file:

```
version: '2.4'

services:
  edge:
    image: traefik:1.7.10
    labels:
      - "traefik.enable=false"
    ports:
      - "80:80"      # The HTTP port
      - "443:443"    # The HTTPS port
    volumes:
      # To communicate with the Docker Engine
      - /var/run/docker.sock:/var/run/docker.sock
      # Add the TOML configuration file in the root directory
      - ./traefik.toml:/traefik.toml
      # ACME file (mod: 600)
      - ./acme.json:/acme.json
```

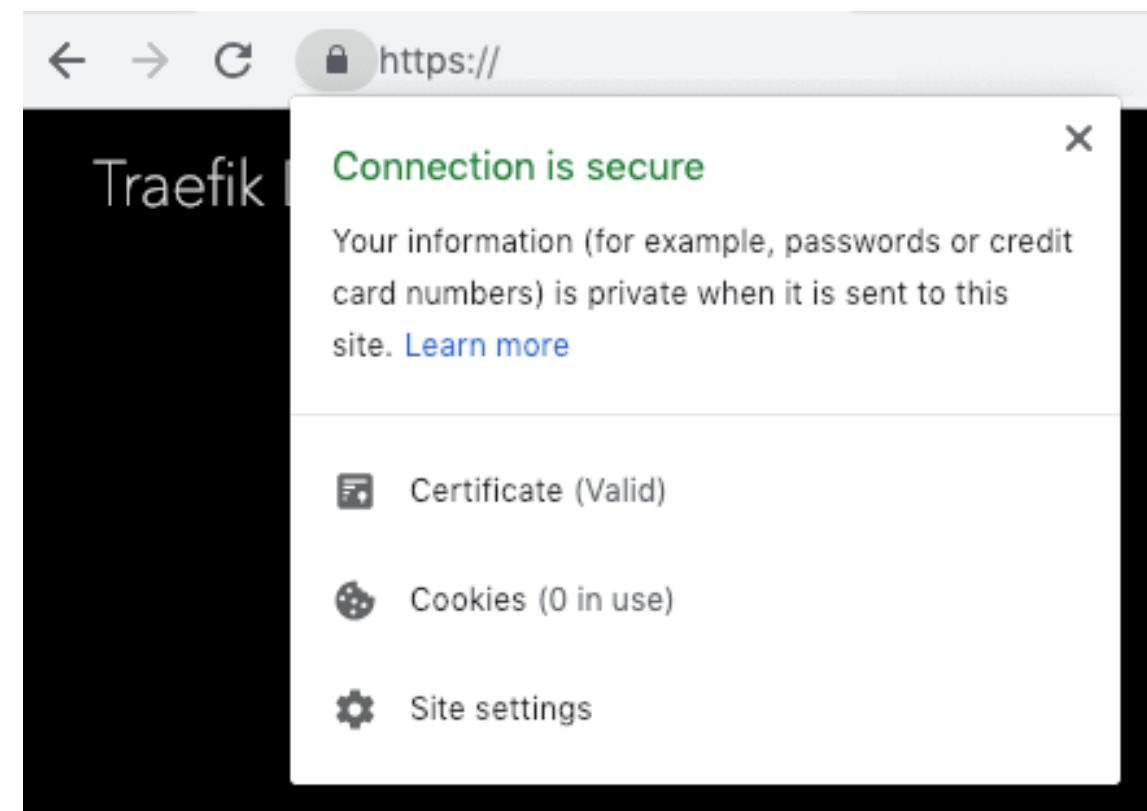
- Step 3: Update the edge service

```
docker-compose up -d edge
```

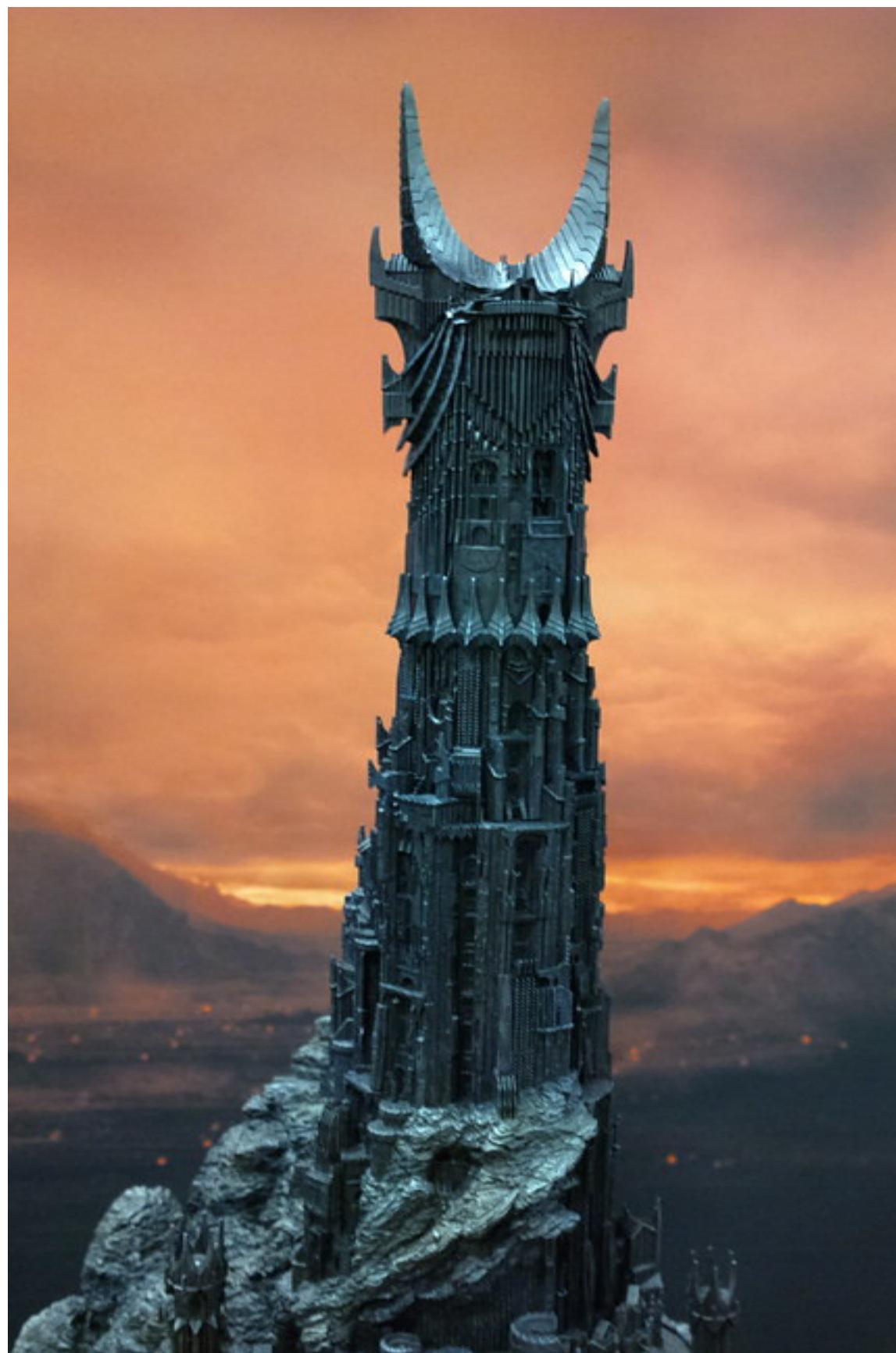
Reality Check

- Wait a few seconds (time to get the certificate from Let's Encrypt) and reload the main page:

<https://lab01.demo.containous.cloud>



Saruman Tower: Migrate Traefik To Kubernetes



Saruman Tower

We want to begin the migration of our services from the AWS VM to a Kubernetes cluster in AWS:

- keep the Docker services
- migrate Traefik to Kubernetes
- migrate the Let's Encrypt certificates
- access to the Docker services through Traefik in Kubernetes

Infrastructure Setup

- An AWS EKS server with a public IP 35.178.178.237 and SSH access
- Kubernetes and Helm to deploy the infrastructure

Agenda

- Let's Encrypt Certificates
- Traefik
- Web Server
- CI Server
- SCM: A Gitea Git Server
- Web CLI

Goal

- We want to use our generated Let's Encrypt certificates
 - We do not want to exceed the ACME Rate Limits.

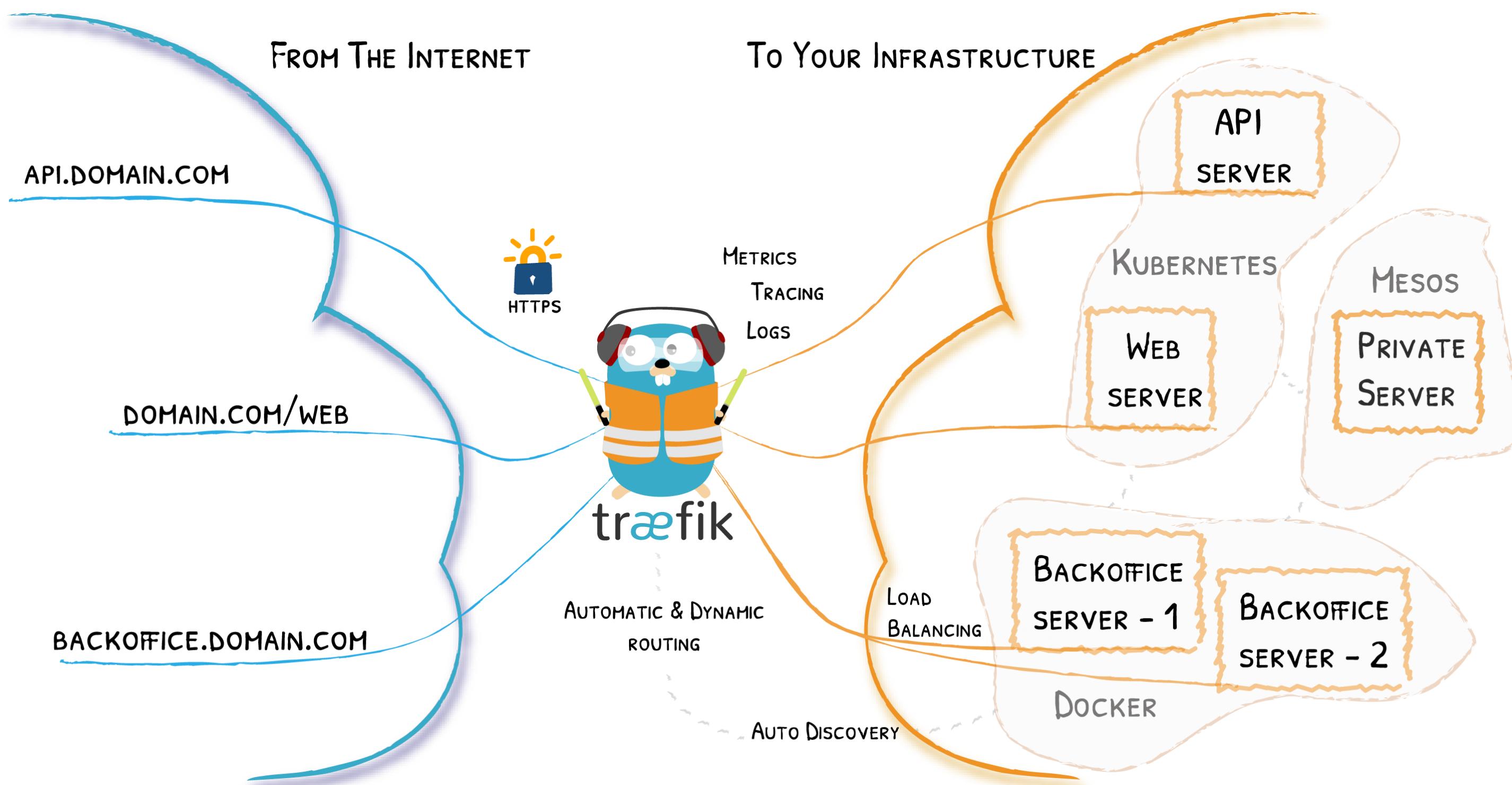
Lab To Define

TODO: dduportal

Agenda

- Let's Encrypt Certificates
- **Traefik**
- Web Server
- CI Server
- SCM: A Gitea Git Server
- Web CLI

Remember The Diagram?



In Kubernetes

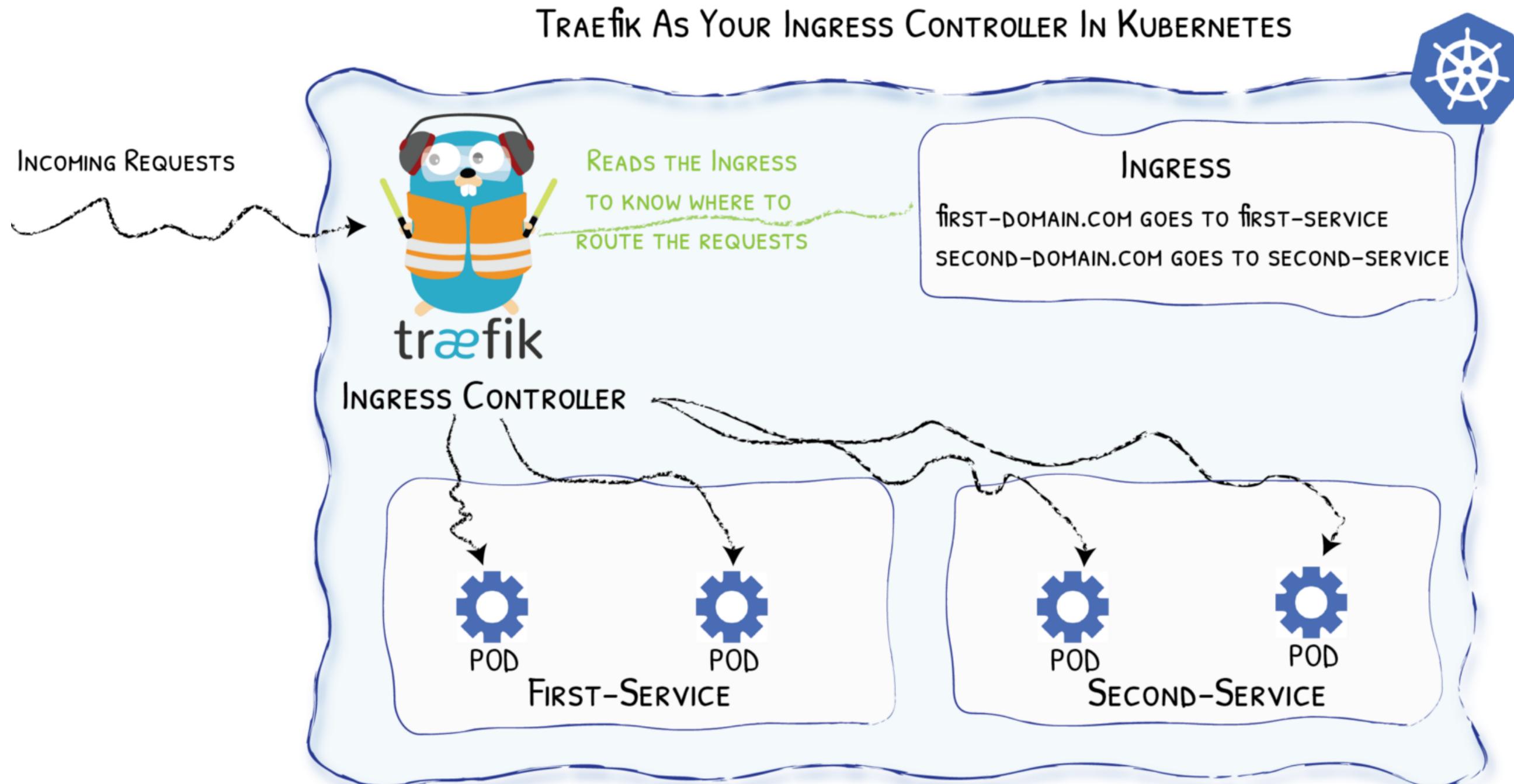


Diagram from <https://medium.com/@geraldcroes>

Let's Go

Initialize Helm

```
curl https://raw.githubusercontent.com/kubernetes/helm/master/scripts/get | bash
# add a service account within a namespace to segregate tiller
kubectl --namespace kube-system create sa tiller
# create a cluster role binding for tiller
kubectl create clusterrolebinding tiller \
    --clusterrole cluster-admin \
    --serviceaccount=kube-system:tiller
# initialized helm within the tiller service account
helm init --service-account tiller
# updates the repos for Helm repo integration
helm repo update
```

Values.Yaml File

- Step 1: Add rights on namespace

```
# Allow creating the needed Role and Service Account
rbac:
  enabled: true
```

- Step 2: Set SSL EntryPoint with redirection

```
ssl:
  enabled: true
  enforced: true
```

- Step 3: Add Let's Encrypt

```
acme:
  enabled: true
  email: devoxxlab@containo.us
  onHostRule: true
  #staging: true
  challengeType: tls-alpn-01
  #  persistence:
  #    existingClaim:
```

Deploy Traefik

```
helm install stable/traefik \  
--name traefik-devoxx \  
--namespace devoxx \  
--set imageTag=1.7.10 \  
--values values.yml  
helm ls
```

Access To Traefik

- Step 1: Run the command:

```
kubectl --namespace=devoxx get services
```

- Step 2: Get the Load Balancer EXTERNAL-IP:

NAME	TYPE	CLUSTER-IP	EXTERNAL-IP	PORT(S)	AGE
traefik-devoxx	LoadBalancer	100.71.101.224	\$EXTERNAL_IP	80:32256/TCP, 443:31489/TCP	12s

- Step 3: Blue-Green on Traefik instances:

```
*TODO: dduportal*
```

Reality Check

<http://lab01.demo.containous.cloud/>



It's good: we have an HTTP answer!

Agenda

- Let's Encrypt Certificates
- Traefik
- **Web Server**
- CI Server
- SCM: A Gitea Git Server
- Web CLI

Goal

- We want access to the webserver hosted in Docker through Traefik in Kubernetes

Challenge 1/2

- **Problem:** How to tell to Traefik to route requests to the web server which is not deployed in Kubernetes?

```
https://lab01.demo.containous.cloud/index.html
-> Traefik Kubernetes
-> Traefik Docker
-> https://<Webserver Private IP>/index.html
```

Headless Service

- **Solution:** Use a service linked to an external address

```
---  
apiVersion: v1  
kind: Service  
metadata:  
  name: web-service  
  namespace: devoxx  
  labels:  
    guilde: web  
spec:  
  ports:  
    # Define the port to contact on the external Host  
    # Here contact Traefik defined in lab1  
    - port: 80  
      name: traefik-http  
    # Indicate to Kubernetes that the service will redirect  
    # to a backend which is not managed in the Kubernets network  
  type: ExternalName  
  # IP of the VM in the lab1  
  externalName: 18.196.121.238
```

Challenge 2/2

- **Problem:** How to detect the HTTPS requests to catch ?

Ingress Rule

- **Solution:** Catch all the incoming requests for the Path: /:

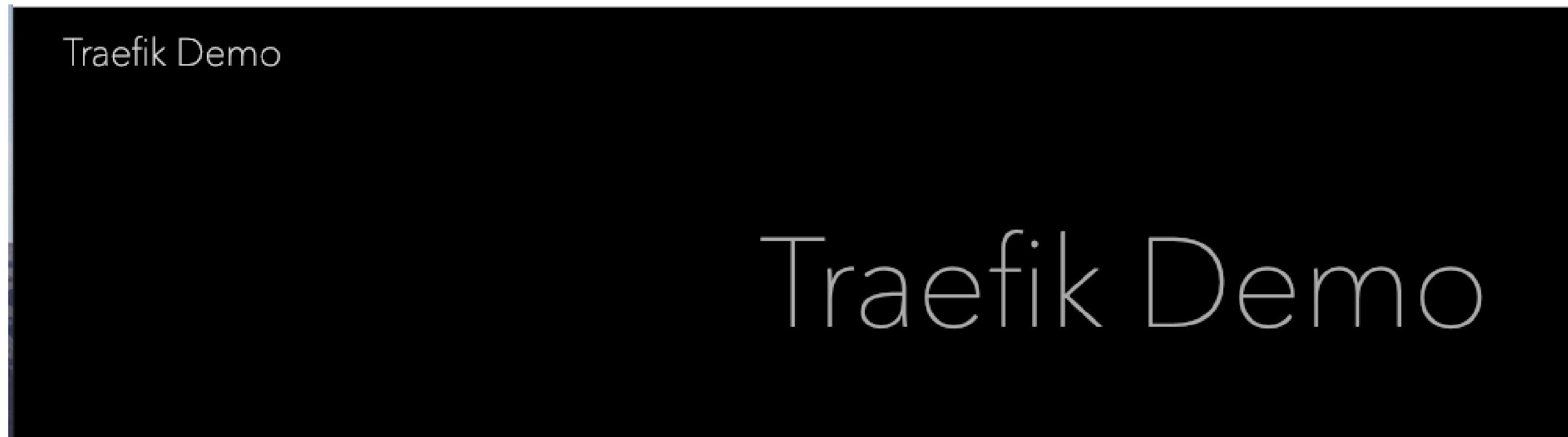
```
---  
apiVersion: extensions/v1beta1  
kind: Ingress  
metadata:  
  name: web-ingress  
  namespace: devoxx  
  labels:  
    guilde: web  
  annotations:  
    kubernetes.io/ingress.class: 'traefik'  
    traefik.frontend.passHostHeader: "false"  
    traefik.frontend.rule.type: PathPrefix  
spec:  
  rules:  
  - host:  
    http:  
      paths:  
      - path: /  
        backend:  
          serviceName: web-service  
          servicePort: traefik-http
```

Apply The Configuration

```
kubectl apply -f ./web/svc-ingress.yml
```

Reality Check

<https://lab01.demo.containous.cloud/>



It's good: we have a web page!

Agenda

- Let's Encrypt Certificates
- Traefik
- Web Server
- **CI Server**
- SCM: A Gitea Git Server
- Web CLI

Goal

- We want access to the CI hosted in Docker through Traefik in Kubernetes

Challenge 1/2

- **Problem:** How to tell to Traefik to route requests to the CI which is not deployed in Kubernetes?

```
https://lab01.demo.containous.cloud/jenkins
  -> Traefik Kubernetes
  -> Traefik Docker
  -> https://<Jenkins Private IP>/jenkins
```

Headless Service

- **Solution:** Use (once again) a service linked to an external address

```
----  
apiVersion: v1  
kind: Service  
metadata:  
  name: jenkins-service  
  namespace: devoxx  
  labels:  
    guilde: ci  
spec:  
  ports:  
  - port: 80  
    name: traefik-http  
  type: ExternalName  
  externalName: 18.196.121.238
```

Challenge 2/2

- **Problem:** How to detect the HTTPS requests to catch ?

Ingress Rule

- **Solution:** Catch the requests for the Path: /jenkins:

```
---  
apiVersion: extensions/v1beta1  
kind: Ingress  
metadata:  
  name: jenkins-ingress  
  namespace: devoxx  
  labels:  
    guilde: ci  
  annotations:  
    kubernetes.io/ingress.class: 'traefik'  
    traefik.frontend.passHostHeader: "false"  
    traefik.frontend.rule.type: PathPrefix  
spec:  
  rules:  
  - host:  
    http:  
      paths:  
      - path: /jenkins  
        backend:  
          serviceName: jenkins-service  
          servicePort: traefik-http
```

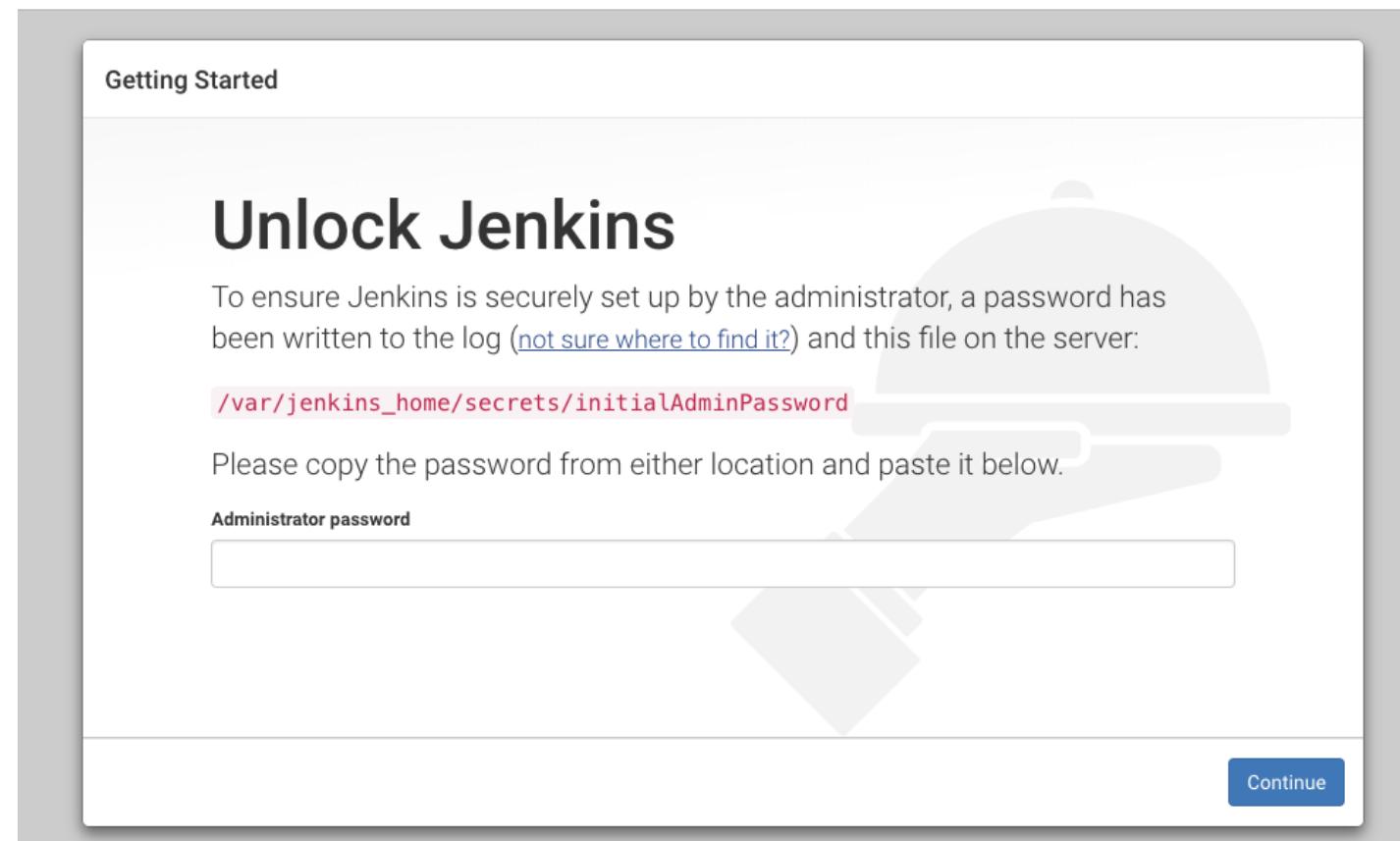
Apply The Configuration

```
kubectl apply -f ./jenkins/svc-ingress.yml
```

Reality Check

Click on the "Jenkins" link:

<https://lab01.demo.containous.cloud/jenkins>



It's good: we still can setup Jenkins!

Agenda

- Let's Encrypt Certificates
- Traefik
- Web Server
- CI Server
- **SCM: A Gitea Git Server**
- Web CLI

Goal

- We want access to the Git server hosted in Docker through Traefik in Kubernetes

Challenge 1/2

- Problem:
 - Gitea only serves requests under /
 - Traefik in Docker already removes the prefix /gitserver

```
http://{{lab-domain}}/gitserver/index.html
  -> Traefik Kubernetes
  -> Traefik Docker
  -> http://<Gitea private IP>:3000/index.html
```

Use A PathPrefix Rule

- **Solution:** Do not remove the prefix (Thank Captain Obvious)

```
---
apiVersion: extensions/v1beta1
kind: Ingress
metadata:
  name: gitea-ingress
  namespace: devoxx
  labels:
    guilde: git
  annotations:
    kubernetes.io/ingress.class: 'traefik'
    traefik.frontend.passHostHeader: "false"
    # Only Path Prefix to let the other Traefik Strip it
    traefik.frontend.rule.type: PathPrefix
spec:
  rules:
  - host: lab.nicolas.containous.cloud
    http:
      paths:
      - path: /gitserver
        backend:
          serviceName: gitea-server
          servicePort: traefik-http
```

Challenge 2/2

- **Problem:** How to tell to Traefik to route requests to the SCM which is not deployed in Kubernetes?

Headless Service

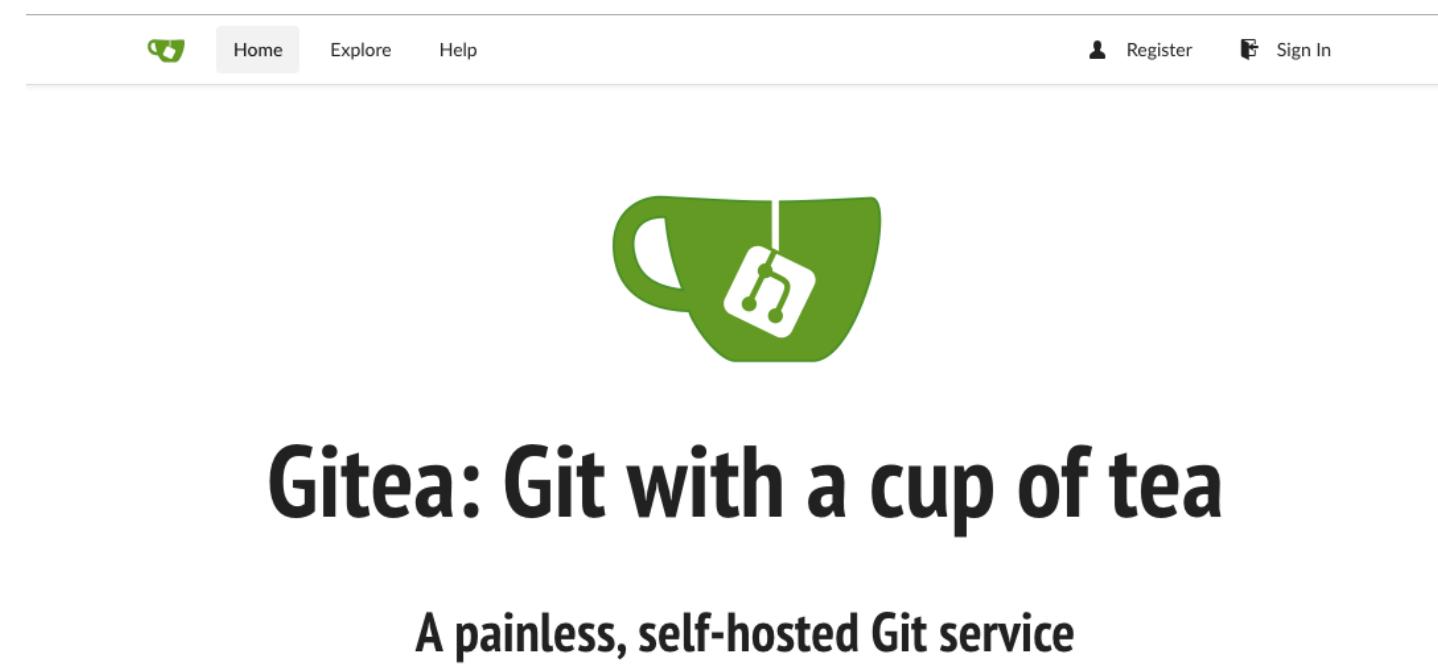
- **Solution:** Use (once again again) a service linked to an external address

```
----  
apiVersion: v1  
kind: Service  
metadata:  
  name: gitea-server  
  namespace: devoxx  
  labels:  
    guilde: git  
spec:  
  ports:  
  - port: 80  
    name: traefik-http  
  type: ExternalName  
  externalName: 18.196.121.238
```

Reality Check

Try the "Gitea Git server" link:

<https://lab01.demo.containous.cloud/gitserver>



It's good: Gitea is still available!

Agenda

- Let's Encrypt Certificates
- Traefik
- Web Server
- CI Server
- SCM: A Gitea Git Server
- **Web CLI**

Goal

- We want to access to TTYD deployed in Docker through Traefik in Kubernetes

Challenges

- **Problem 1:** How to tell to Traefik to route requests to TTYD which is not deployed in Kubernetes?

```
https://lab01.demo.containous.cloud/ttyd
  -> Traefik Kubernetes
  -> Traefik Docker
  -> https://<WebCLI Private IP>/
```

- **Problem 2:** How to detect the HTTPS requests to catch ?

Solution 1

- Use a Headless Service:

```
---  
apiVersion: v1  
kind: Service  
metadata:  
  name: ttyd-service  
  namespace: devoxx  
  labels:  
    guilde: console  
spec:  
  ports:  
  - port: 80  
    name: traefik-http  
  type: ExternalName  
  externalName: 18.196.121.238
```

Solution 2

- Ingress Rule with PathPrefix: /ttyd:

```
---  
apiVersion: extensions/v1beta1  
kind: Ingress  
metadata:  
  name: ttyd-ingress  
  namespace: devoxx  
  annotations:  
    kubernetes.io/ingress.class: 'traefik'  
    traefik.frontend.passHostHeader: "false"  
    traefik.frontend.rule.type: PathPrefix  
spec:  
  rules:  
  - host: lab.nicolas.containous.cloud  
    http:  
      paths:  
      - path: /ttyd  
        backend:  
          serviceName: ttyd-service  
          servicePort: traefik-http
```

Reality Check

Try the "TTYD Web Command Line" link:

<https://lab01.demo.containous.cloud/ttyd>



It's good: we can continue to develop in a web browser!

The Castle



The Castle

We want to terminate the migration of our services from the AWS VM to a Kubernetes cluster in AWS:

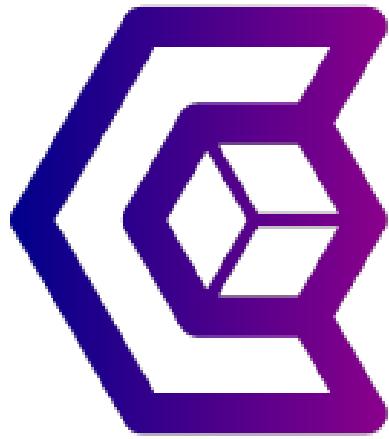
- migrate Stateful applications in Blue Green mode
- migrate Stateless application

Infrastructure Setup

- An AWS EKS server with a public IP 35.178.178.237 and SSH access
- Kubernetes to deploy the infrastructure



We Are Hiring!

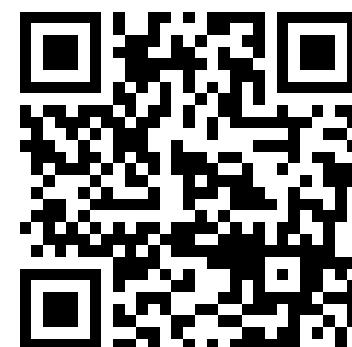


```
docker run -it containous/jobs
```

Thank You!

🐦 @nicomengin 🐕 nmengin

🐦 @DamienDuportal 🐕 dduportal



- Slides (HTML): <https://containous.github.io/slides/devoxx-fr-2019>
- Slides (PDF): <https://containous.github.io/slides/devoxx-fr-2019/slides.pdf>
- Source on 🐕: <https://github.com/containous/slides/tree/devoxx-fr-2019>