# Open Source Kubernetes Stack

Ondřej Šika
Freelance & SikaLabs s.r.o.

ondrej@sika.io
@ondrejsika

Kubernetes Community Days Czech & Slovak 2023
Bratislava SK, 19. 5. 2023



# Ondřej Šika

Jsem DevOps lektor, architekt a konzultant z Prahy.

Navrhnu a implementuji Vám na míru DevOps architekturu od verzování v Gitu po provoz v Cloudu.

Dělám populární školení, kde své znalosti předávám tak, abyste si mohli vše udělat sami a bez zbytečných přešlapů a slepých cest.

@ondrejsika ondrej@sika.io sika.io /in/ondrejsika

# Můj Open Source DevOps Stack

- Git, Gitlab, Github - Versioning & Collaboration
- Gitlab CI, **ArgoCD** - Continuous Integration, Continuous Deployment
- **Docker**, **Kubernetes** - Containers & Orchestration
- **RKE2** & Rancher - Kubernetes Provisioning
- Terraform - Infrastructure management
- Gobble - Configuration management
- **Prometheus**, **Grafana** - Monitoring Stack
- Elastic Stack / **Loki** - Log Management
- DigitalOcean, AWS, VMWare, Proxmox - Public or Private Cloud
- Ceph, **Longhorn** - On Premise Storage
- Tergum - Backups, DR

@ondrejsika ondrej@sika.io sika.io /in/ondrejsika

# Píšu knihu

- Kultura DevOps
- Moderní DevOps Stack
- Jak navrhnout DevOps architekturu
- Kontejnery, Kubernetes, Terraform, ... deep dive
- Automatizace and GitOps
- Spousta ukázek

# kniha.sika.io

@ondrejsika ondrej@sika.io sika.io /in/ondrejsika

# Kubernetes Stack

@ondrejsika ondrej@sika.io sika.io /in/ondrejsika

# Co po stacku požadujeme?

@ondrejsika ondrej@sika.io sika.io /in/ondrejsika

# Co po stacku požadujeme?

- **Plnohodnotně provozovat aplikace v Kubernetes**
  - Ingress - přístup z internetu přes jeden vstupní bod
  - HTTPS - Idelně automatizovaná správa pomocí Let's Encrypt
  - Storage - Podpora PVC (není v Kubernetes by default)
- Monitoring
  - Potřebujeme vědět, v jakém stavu jsou naše aplikace ale i samotná platforma
- Log Management
  - Chceme sbírat logy a případně nad nimi řešit aleting
- GitOps - Správa  platformy z Git repozitáře
- SSO - Správa uživatelů na jednom místě

@ondrejsika ondrej@sika.io sika.io /in/ondrejsika

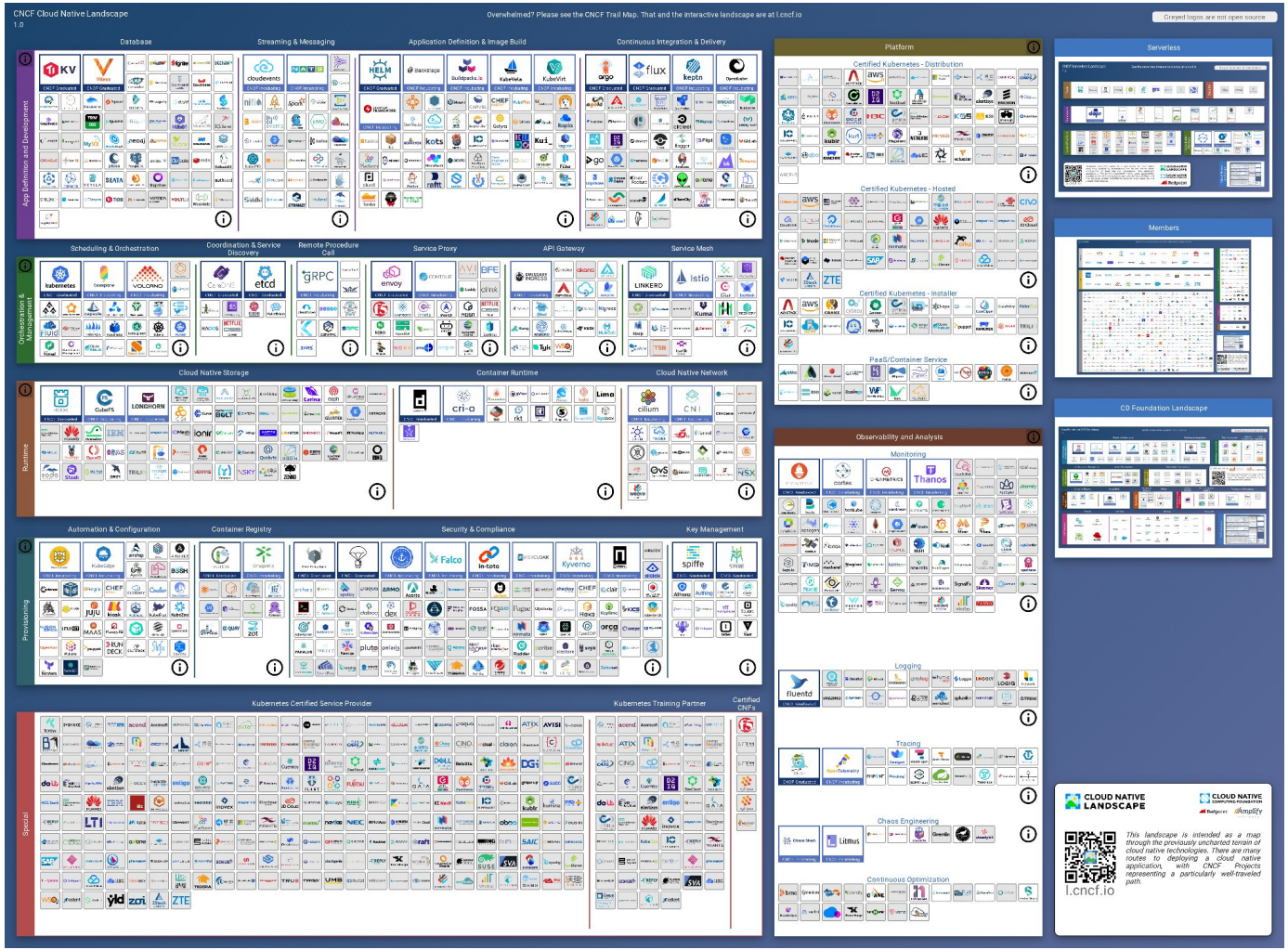
# Kde jej budeme provozovat

- Public Cloud
  - Managed Kubernetes - AKS, EKS, DigitalOcean Kubernetes, ...
  - RKE2 na VMs
- On Premise
  - S přístupem na internet
  - Air-Gap environment



# Můžeme si vybírat ...

@ondrejsika ondrej@sika.io sika.io /in/ondrejsika


CNCF Cloud Native Landscape
1.0
Overwhelmed? Please see the CNCF Trail Map. That and the interactive landscape are at l.cncf.io
Greyed logos are not open source
App Definition and Development
Database
Streaming & Messaging
Application Definition & Image Build
Continuous Integration & Delivery
Orchestration & Management
Scheduling & Orchestration
Coordination & Service Discovery
Remote Procedure Call
Service Proxy
API Gateway
Service Mesh
Runtime
Cloud Native Storage
Container Runtime
Cloud Native Network
Provisioning
Automation & Configuration
Container Registry
Security & Compliance
Key Management
Special
Kubernetes Certified Service Provider
Kubernetes Training Partner
Certified CNFs
Platform
Certified Kubernetes - Distribution
Certified Kubernetes - Hosted
Certified Kubernetes - Installer
PaaS/Container Service
Observability and Analysis
Monitoring
Logging
Tracing
Chaos Engineering
Continuous Optimization
Serverless
Members
CD Foundation Landscape
CLOUD NATIVE LANDSCAPE
CLOUD NATIVE COMPUTING FOUNDATION
Badgerati
Amplify
This landscape is intended as a map through the previously uncharted terrain of cloud native technologies. There are many routes to deploying a cloud native application, with CNCF Projects representing a particularly well-traveled path.
l.cncf.io


@ondrejsika ondrej@sika.io sika.io /in/ondrejsika

# RKE2 - Rancher Kubernetes Engine

- Kubernetes Engine
- Pro svůj běh potřebujeme pouze VMs
- Jednoduchý setup včetně HA řešení
  - Lze použít Cloud Init, Gobble, Ansible
- Vhodné do On-Prem i do Cloudu

@ondrejsika ondrej@sika.io sika.io /in/ondrejsika

# Haproxy

- Proxy zajišťující load balancing a ingress do Kubernetes clusteru
- Nutné v on-premise řešení
- V cloudu může být nahrazena cloudovým load balancerem jako je AWS NLB nebo Azure Load Balancer

# Ingress Nginx Controller

- Umožňuje nám vystavovat aplikace pomocí Ingress objektu (L7 proxy)
- Není potřeba  používat service type LoadBalancer
- Nejrozšířenější Ingress controller - de facto standard
- Přímo od vývojářů Kubernetes

@ondrejsika ondrej@sika.io sika.io /in/ondrejsika

# Cert Manager

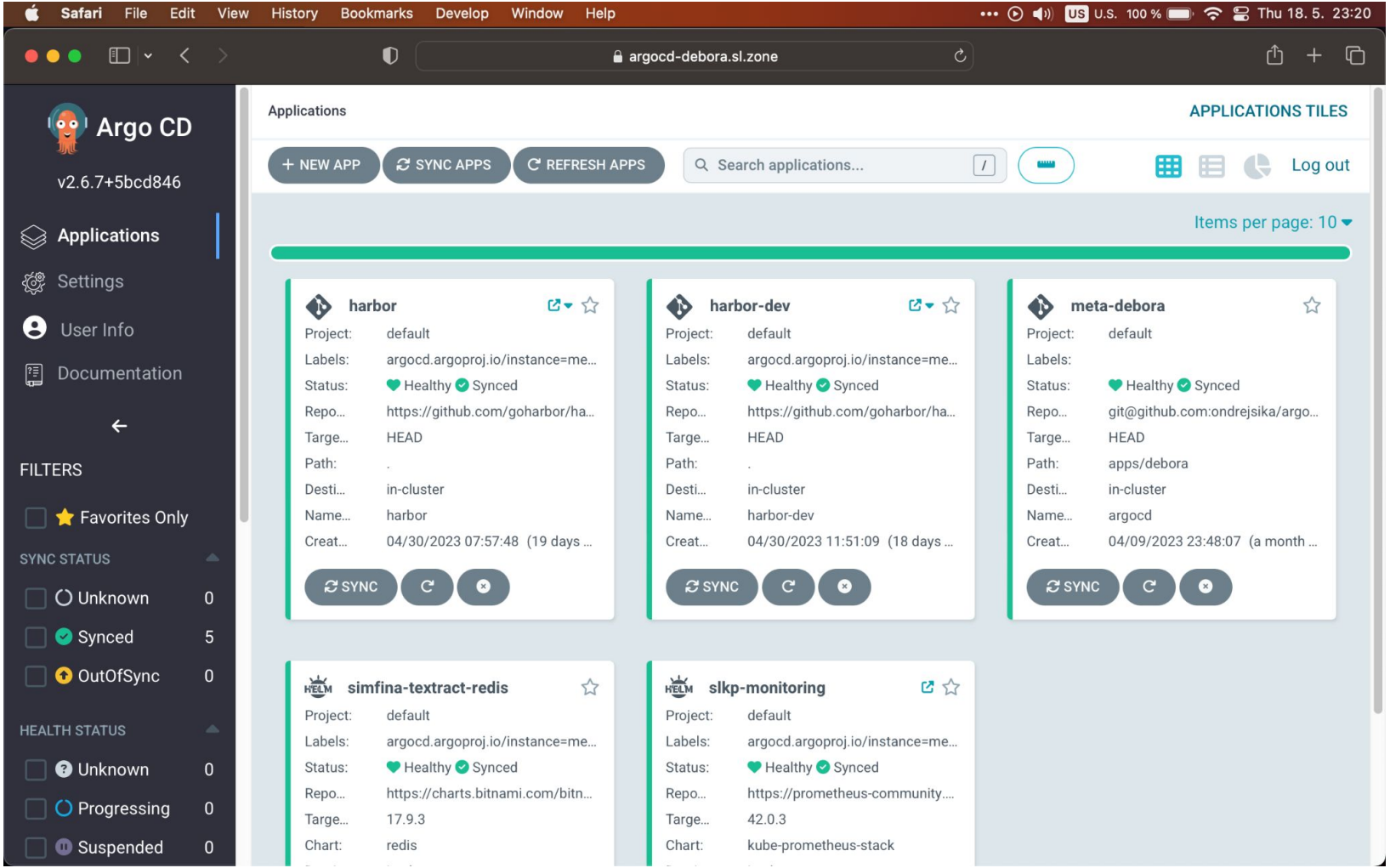
- Umožňuje nám vystavovat TLS certifikáty
  - Primárně pro Ingress
- Podpora Let's Encrypt
- HTTP i DNS Challenge
- Funguje i za VPN


@ondrejsika ondrej@sika.io sika.io /in/ondrejsika

# ArgoCD

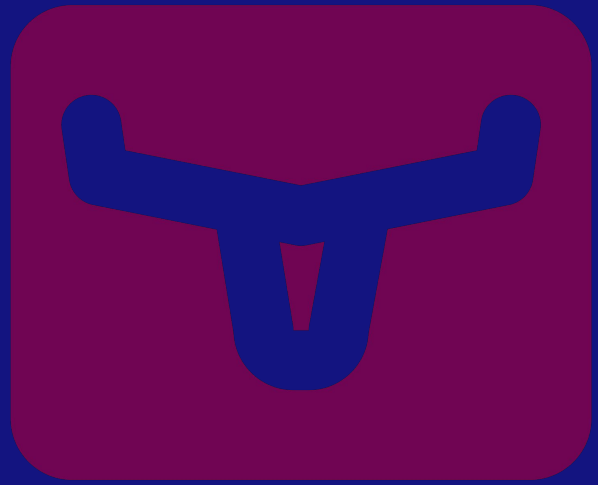
- Populární CD pro Kubernetes
- GitOps přístup - vše, co je nasazené, je nasazené z Gitu
- Podpora SSO pomocí Keycloaku
- Pull metoda - není potřeba žádné CI na straně Gitlabu / Githubu
- Není potřeba konfigurovat connection ke clusteru na Githubu / Gitlabu

@ondrejsika ondrej@sika.io sika.io /in/ondrejsika

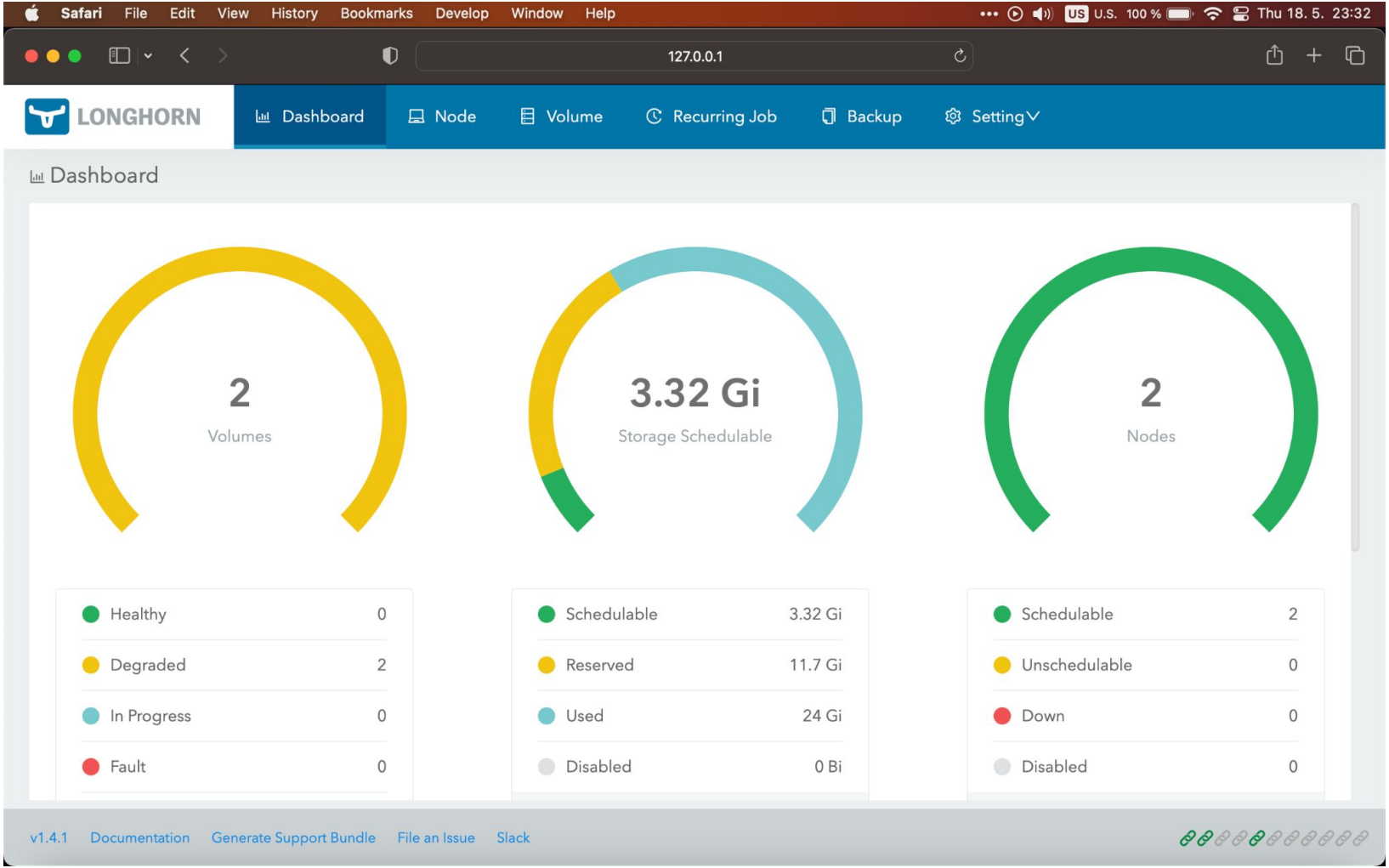

Safari File Edit View History Bookmarks Develop Window Help
US U.S. 100 % Thu 18. 5. 23:20
argocd-debora.sl.zone
Argo CD
v2.6.7+5bcd846
Applications
Settings
User Info
Documentation
FILTERS
Favorites Only
SYNC STATUS
Unknown 0
Synced 5
OutOfSync 0
HEALTH STATUS
Unknown 0
Progressing 0
Suspended 0
Applications
APPLICATIONS TILES
+ NEW APP
SYNC APPS
REFRESH APPS
Search applications...
Log out
Items per page: 10
harbor
Project: default
Labels: argocd.argoproj.io/instance=me...
Status: Healthy Synced
Repo... https://github.com/goharbor/ha...
Targe... HEAD
Path: .
Desti... in-cluster
Name... harbor
Creat... 04/30/2023 07:57:48 (19 days ...
SYNC
harbor-dev
Project: default
Labels: argocd.argoproj.io/instance=me...
Status: Healthy Synced
Repo... https://github.com/goharbor/ha...
Targe... HEAD
Path: .
Desti... in-cluster
Name... harbor-dev
Creat... 04/30/2023 11:51:09 (18 days ...
SYNC
meta-debora
Project: default
Labels:
Status: Healthy Synced
Repo... git@github.com:ondrejsika/argo...
Targe... HEAD
Path: apps/debora
Desti... in-cluster
Name... argocd
Creat... 04/09/2023 23:48:07 (a month ...
SYNC
simfina-textract-redis
Project: default
Labels: argocd.argoproj.io/instance=me...
Status: Healthy Synced
Repo... https://charts.bitnami.com/bitn...
Targe... 17.9.3
Chart: redis
slkp-monitoring
Project: default
Labels: argocd.argoproj.io/instance=me...
Status: Healthy Synced
Repo... https://prometheus-community....
Targe... 42.0.3
Chart: kube-prometheus-stack

# Longhorn

- Storage pro Kubernetes
- Čistě Kubernetes (RKE2) nemá by default žádnou storage
- HA & Distribuovaná storage (jako Ceph)
- Jednoduchý setup, aktualizace a provoz
- Umožňuje vytvářet PVC
  - ReadWriteOnce - Vhodné pro DB, Minio, ...
  - ReadWriteMany - Vhodné pro soubory aplikací
- Podpora automatického zálohování do S3 a NFS



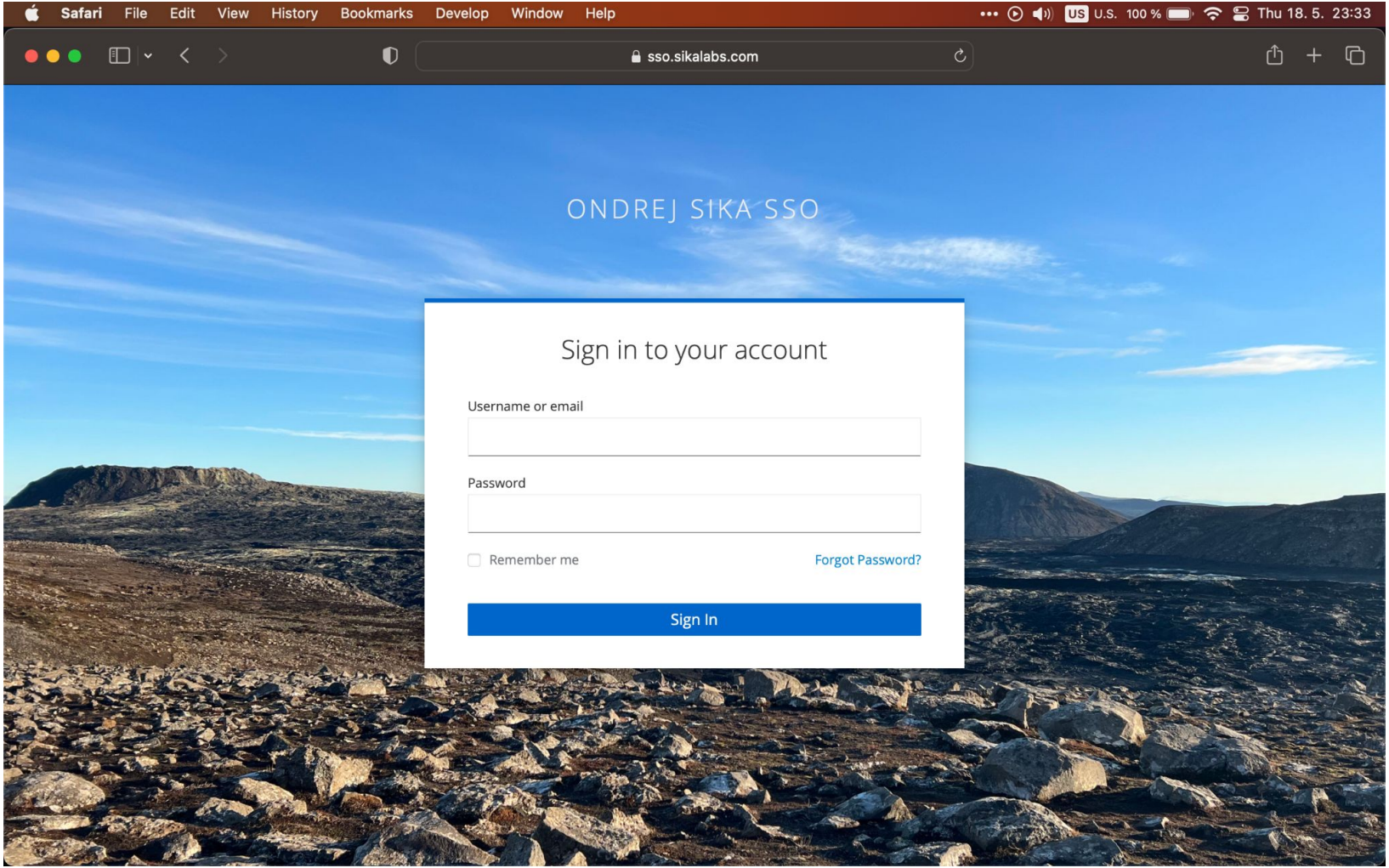
@ondrejsika ondrej@sika.io sika.io /in/ondrejsika


Safari File Edit View History Bookmarks Develop Window Help
US U.S. 100 % Thu 18. 5. 23:32
127.0.0.1
LONGHORN
Dashboard
Node
Volume
Recurring Job
Backup
Setting
Dashboard
2
Volumes
3.32 Gi
Storage Schedulable
2
Nodes
Healthy 0
Degraded 2
In Progress 0
Fault 0
Schedulable 3.32 Gi
Reserved 11.7 Gi
Used 24 Gi
Disabled 0 Bi
Schedulable 2
Unschedulable 0
Down 0
Disabled 0
v1.4.1
Documentation
Generate Support Bundle
File an Issue
Slack

# Keycloak SSO

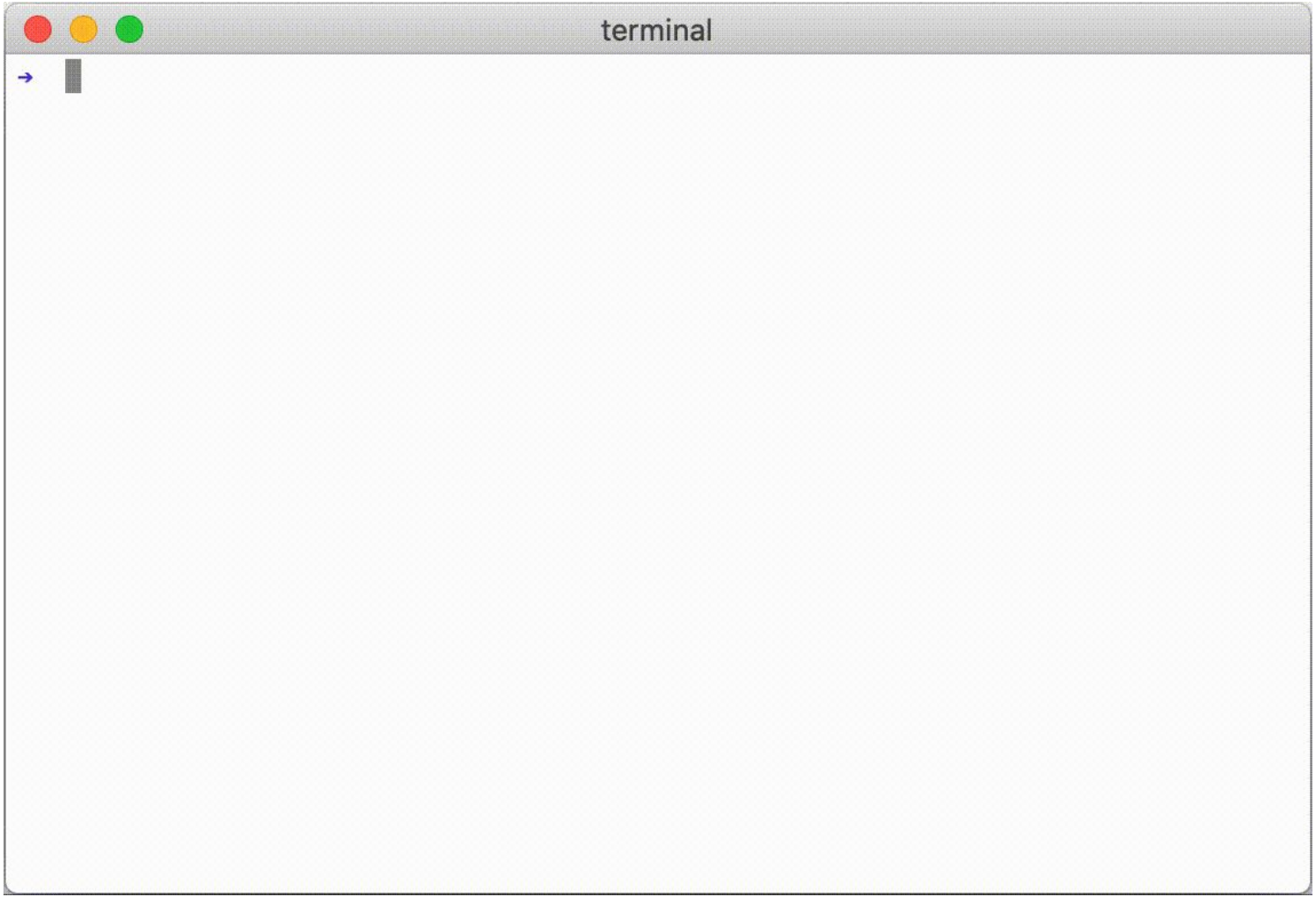
- Vlastní SSO (single sign on)
- Podpora v Kubernetes - kubectl za SSO
- SSO do celého stacku
  - ArgoCD
  - Grafana
  - Prometheus (za Oauth2 Proxy)
- Možnost správy pomocí Terraformu

@ondrejsika ondrej@sika.io sika.io /in/ondrejsika


Safari File Edit View History Bookmarks Develop Window Help
US U.S. 100 % Thu 18. 5. 23:33
sso.sikalabs.com
ONDREJ SIKA SSO
Sign in to your account
Username or email
Password
Remember me
Forgot Password?
Sign In

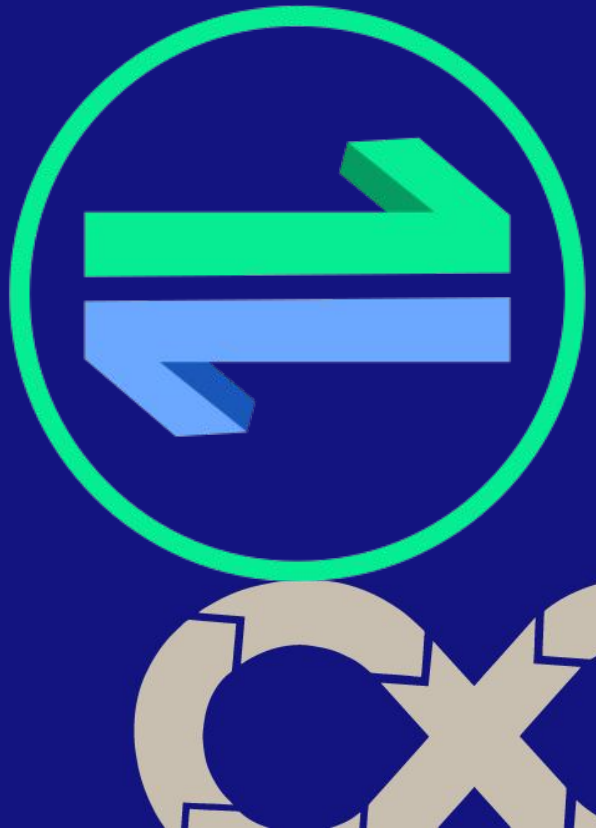
# Kubectl OIDC Login

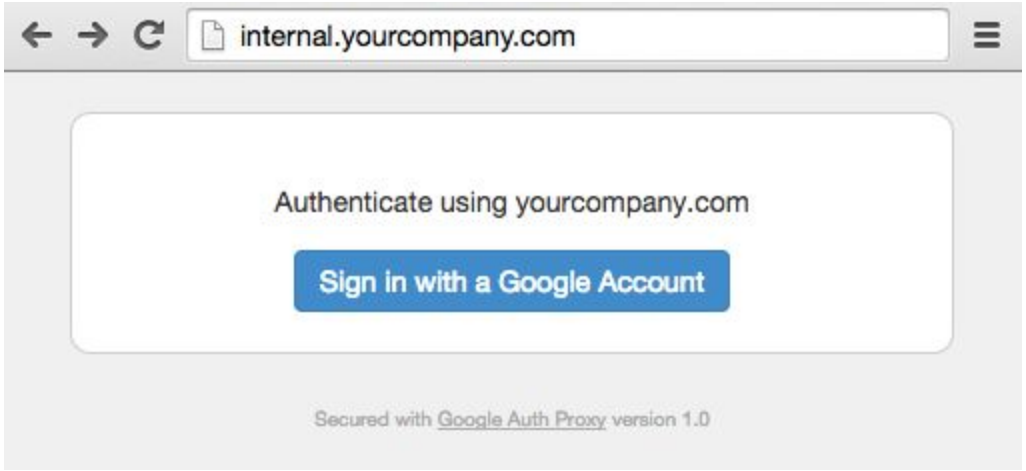
- Plugin do kubectl ktery umožňuje přihlášení pomocí OIDC (Keycloak SSO)
- Správa uživatelů možná na úrovni Keycloaku
- **https://github.com/int128/kubelogin**


terminal

# Oauth2 Proxy

- Umožní nám schovat konkrétní služby / endpointy za SSO
- Kromě Keycloaku (vlastního OIDC) umí i Google, Github, ...
- **https://github.com/oauth2-proxy/oauth2-proxy**




internal.yourcompany.com
Authenticate using yourcompany.com
Sign in with a Google Account
Secured with Google Auth Proxy version 1.0

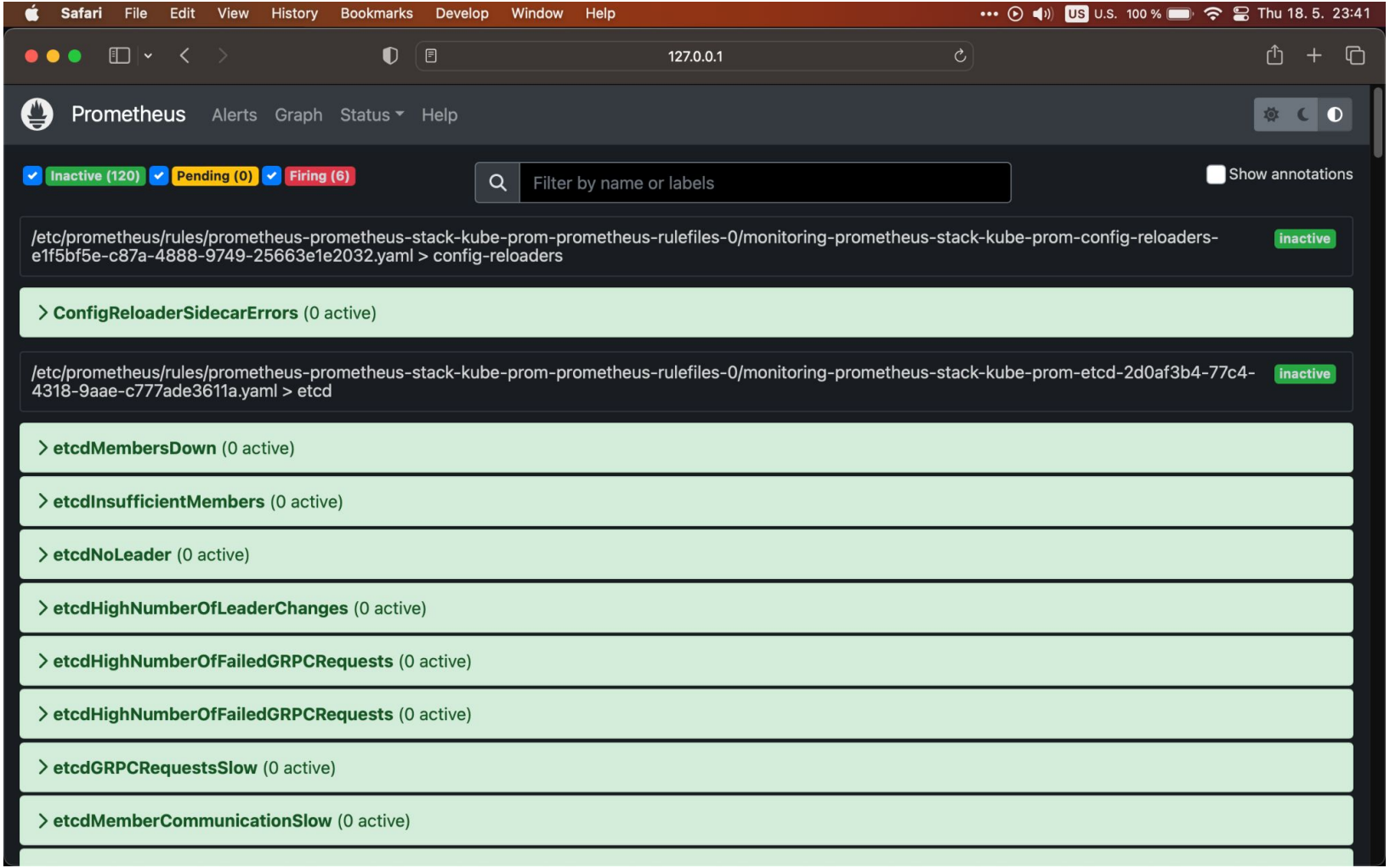
# Kube Prometheus Stack

- Skládá se z
  - Prometheus
  - Alert Manager
  - Grafana
- Obsahuje defaultní konfiguraci

# Prometheus

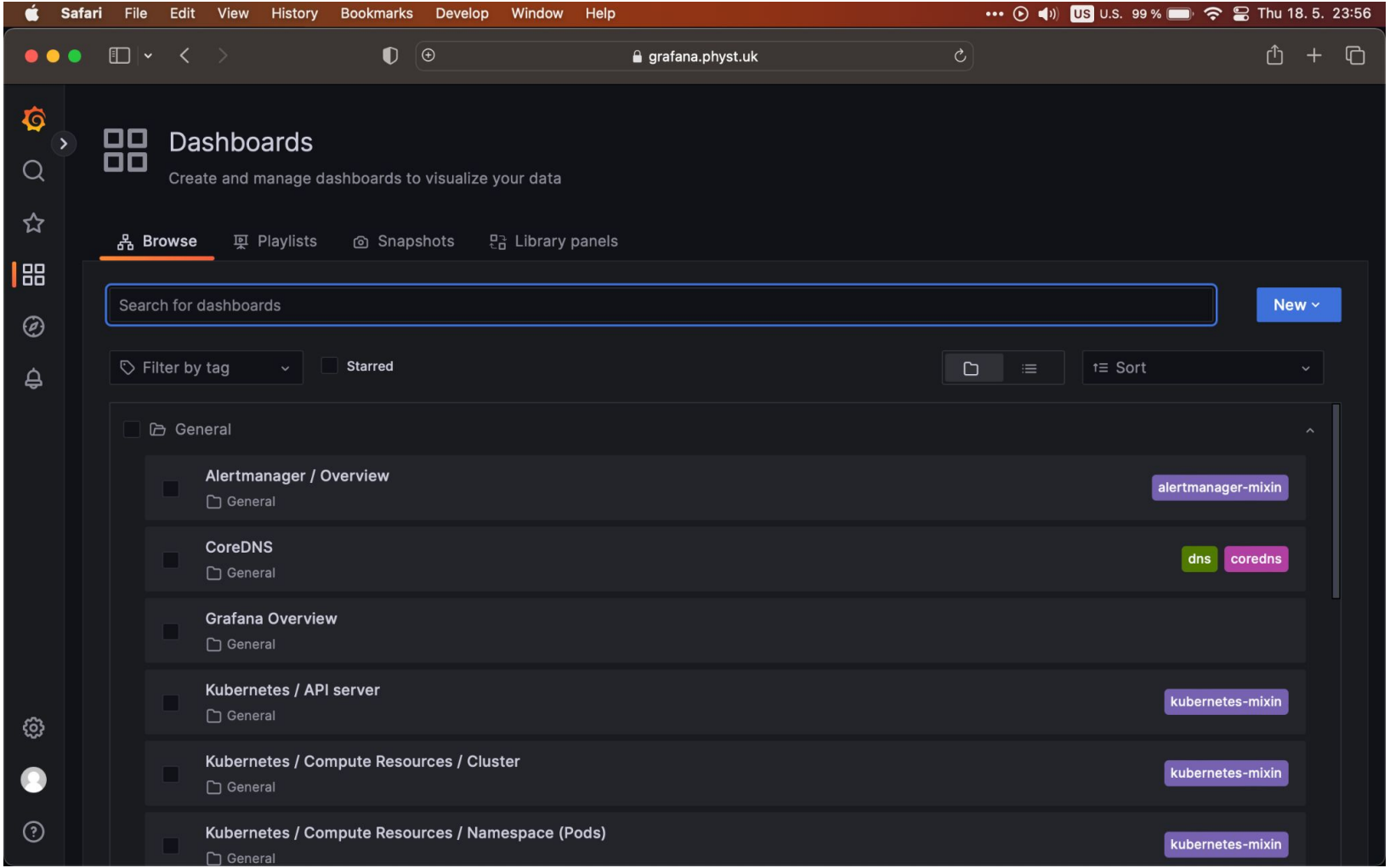
- Sběr metrických dat z clusteru
- White box monitoring

@ondrejsika ondrej@sika.io sika.io /in/ondrejsika


Safari File Edit View History Bookmarks Develop Window Help
US U.S. 100 % Thu 18. 5. 23:41
127.0.0.1
Prometheus Alerts Graph Status Help
Inactive (120) Pending (0) Firing (6)
Filter by name or labels
Show annotations
/etc/prometheus/rules/prometheus-prometheus-stack-kube-prom-prometheus-rulefiles-0/monitoring-prometheus-stack-kube-prom-config-reloaders-e1f5bf5e-c87a-4888-9749-25663e1e2032.yaml > config-reloaders
inactive
> ConfigReloaderSidecarErrors (0 active)
/etc/prometheus/rules/prometheus-prometheus-stack-kube-prom-prometheus-rulefiles-0/monitoring-prometheus-stack-kube-prom-etcd-2d0af3b4-77c4-4318-9aae-c777ade3611a.yaml > etcd
inactive
> etcdMembersDown (0 active)
> etcdInsufficientMembers (0 active)
> etcdNoLeader (0 active)
> etcdHighNumberOfLeaderChanges (0 active)
> etcdHighNumberOfFailedGRPCRequests (0 active)
> etcdHighNumberOfFailedGRPCRequests (0 active)
> etcdGRPCRequestsSlow (0 active)
> etcdMemberCommunicationSlow (0 active)

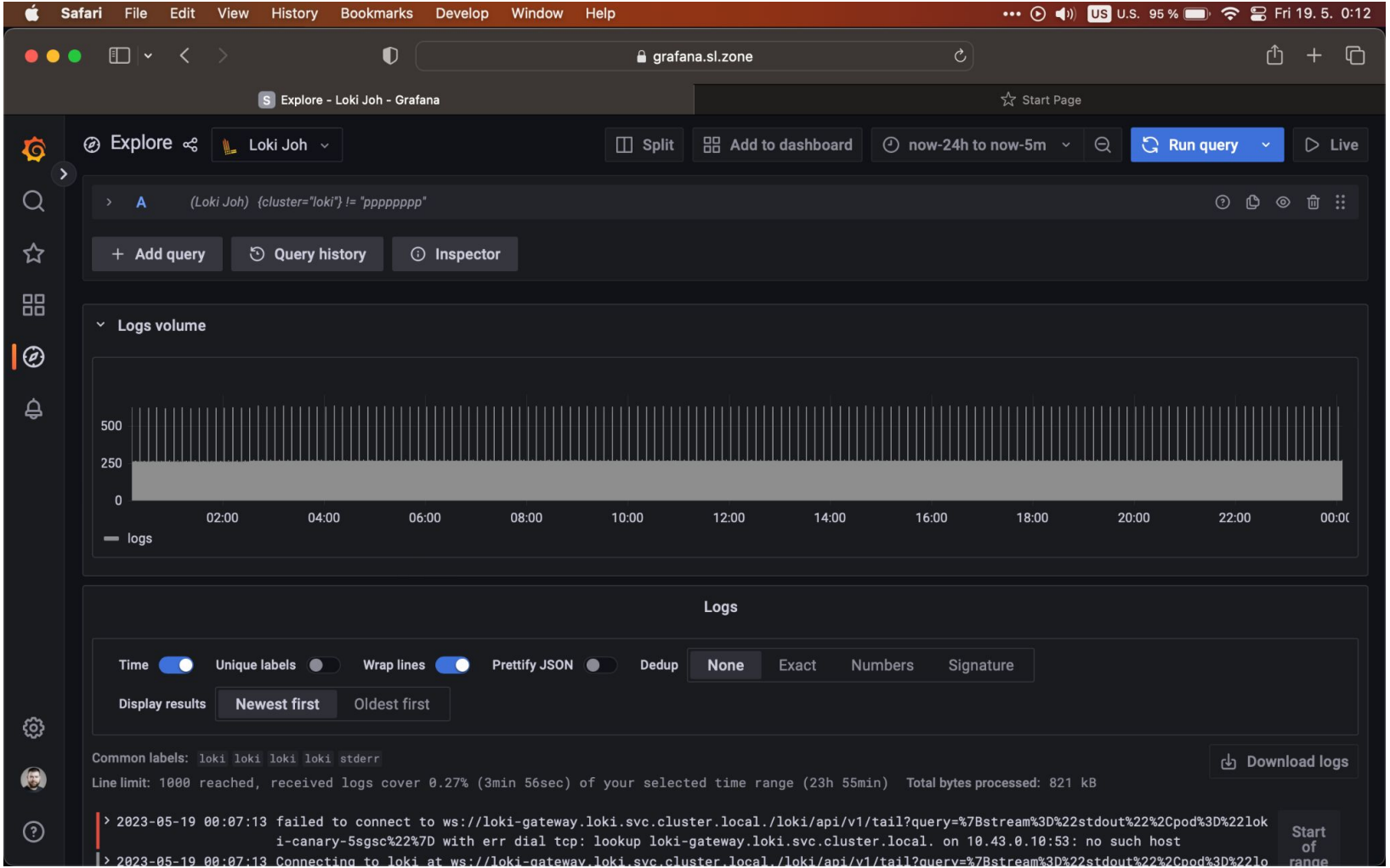
# Grafana

- Vizualizace metických dat
- Přístup k logům - z Lokiho
- Podporuje SSO (z Keycloaku)
- Umožňuje řízení přístupu
- Správa pomocí Terraformu


Safari File Edit View History Bookmarks Develop Window Help
US U.S. 99 % Thu 18. 5. 23:56
grafana.physt.uk
Dashboards
Create and manage dashboards to visualize your data
Browse
Playlists
Snapshots
Library panels
Search for dashboards
New
Filter by tag
Starred
Sort
General
Alertmanager / Overview
General
alertmanager-mixin
CoreDNS
General
dns
coredns
Grafana Overview
General
Kubernetes / API server
General
kubernetes-mixin
Kubernetes / Compute Resources / Cluster
General
kubernetes-mixin
Kubernetes / Compute Resources / Namespace (Pods)
General
kubernetes-mixin

# Loki

- Platforma na ukládání logů (od Grafany)
- Lightweight (oproti Elastic Stacku)
- Umožňuje mít data v S3
- Integrace / UI v Grafane


Safari File Edit View History Bookmarks Develop Window Help
US U.S. 95 % Fri 19. 5. 0:12
grafana.sl.zone
Explore - Loki Joh - Grafana
Start Page
Explore
Loki Joh
Split
Add to dashboard
now-24h to now-5m
Run query
Live
A
(Loki Joh) {cluster="loki"} != "ppppppp"
Add query
Query history
Inspector
Logs volume
500
250
0
02:00
04:00
06:00
08:00
10:00
12:00
14:00
16:00
18:00
20:00
22:00
logs
Logs
Time
Unique labels
Wrap lines
Prettify JSON
Dedup
None
Exact
Numbers
Signature
Display results
Newest first
Oldest first
Common labels: loki loki loki loki stderr
Download logs
Line limit: 1000 reached, received logs cover 0.27% (3min 56sec) of your selected time range (23h 55min)
Total bytes processed: 821 kB
2023-05-19 00:07:13 failed to connect to ws://loki-gateway.loki.svc.cluster.local./loki/api/v1/tail?query=%7Bstream%3D%22stdout%22%2Cpod%3D%22loki-canary-5sgsc%22%7D with err dial tcp: lookup loki-gateway.loki.svc.cluster.local. on 10.43.0.10:53: no such host
Start of range

# A mohli bychom pokračovat ...

@ondrejsika ondrej@sika.io sika.io /in/ondrejsika

# Demo time 🎉🎉

@ondrejsika ondrej@sika.io sika.io /in/ondrejsika

# Závěr

@ondrejsika ondrej@sika.io sika.io /in/ondrejsika

# Open Source Kubernetes Stack

- Z open source nástrojů se dá poskládat robustní Kubernetes stack
- Platforma je nezávislá na prostředí, kde ji provozujeme
  - Bare metal
  - Privatni Cloud - VMWare, OpenStack, ...
  - Public Cloud - AWS, Azure, DigitalOcean, ...
- Obsahuje vše, co potřebujete pro day-to-day Kubernetes operation
- Vhodné pro produkční nasazení - technologie jsou prověřené
- Vše se dá spravovat z kódu (GitOps) - ArgoCD + Terraform

@ondrejsika ondrej@sika.io sika.io /in/ondrejsika

# Díky za pozornost

@ondrejsika ondrej@sika.io sika.io /in/ondrejsika

# Otázky?

@ondrejsika ondrej@sika.io sika.io /in/ondrejsika

Email

**ondrej@sika.io**

Twitter

**@ondrejsika**

LinkedIn

**/in/ondrejsika**

Slides

**sika.link/slides**