

Orquestração de Containers

Arquitetura do cluster
Kubernetes e
tópicos avançados

Tópicos abordados

- Cases de instalação
- Arquitetura, instalação e tipos de cluster
- Soluções customizadas de kubernetes
- Ferramentas de *deployment*
- Considerações sobre armazenamento e *nodes*
- Soluções *on-premise* e *cloud-based*
- Aspectos avançados em *clusters* de produção
- Tópicos sobre segurança

Cases de instalação: engenharia reversa

Iremos agora fazer a “engenharia reversa” do processo de criação do *cluster* utilizado no curso. Vamos lá?

Cases de instalação: *Kubernetes the Hard Way*

<https://github.com/kelseyhightower/kubernetes-the-hard-way>

Arquitetura e instalação do *cluster* Kubernetes

Antes de planejar e instalar um *cluster* Kubernetes, é fundamental responder algumas perguntas

Qual o objetivo do *cluster*?

Ele será executado *on-premises* ou em *clouds* pública/híbrida?

Qual a carga de trabalho esperada para as aplicações?

Objetivos do *cluster*

Educativo

Teste e desenvolvimento

Aplicações de produção

Pode-se utilizar o *Minikube*, *play-with-k8s* ou *single-node clusters* locais ou em *cloud*



<https://labs.play-with-k8s.com/>

[illegible]

play-with-k8s

copy → ctrl + insert

paste → shift + insert



<https://dockerlabs.collabnix.com/kubernetes/beginners/getting-started-on-pwk.html>

Clusters de teste e desenvolvimento

Pode-se utilizar um *multi-node cluster* com apenas um *master* e diversos *workers*

Ferramentas como o *kubeadm* são ideais

Métodos de *quick provisioning* em *clouds* como GCP, EKS e AKS

Permissionamento flexibilizado para maior agilidade no trabalho

Clusters de teste e desenvolvimento

Um exemplo simples
Usando o eksctl:

```
eksctl create cluster \  
--name my-cluster \  
--region us-west-2 \  
--with-oidc \  
--ssh-access \  
--ssh-public-key <your-key> \  
--managed
```

Creating and managing clusters - eksctl

Clusters de produção

Deve-se levar em
consideração aspectos de:

Alta disponibilidade

Escalabilidade

Manutenibilidade

Distribuição geográfica

Ferramentas de *deployment*

<https://www.altoros.com/blog/a-multitude-of-kubernetes-deployment-tools-kubespri-kops-and-kubeadm>

Kops

kubeadm

Kubespray

Kubo

On-premises ou cloud?

A escolha do ambiente de *deployment* raramente é técnica

Considerações como parque instalado, objetivos da organização e outros são fatores

Custo também é relevante: considere o custo total: prédio, refrigeração, gerador, etc

Expertise da equipe e flexibilidade de contratação/consultoria também são importantes

Soluções kubernetes on-premises

Vanilla K8S

Rancher

Red Hat OpenShift

Mirantis Kubernetes Engine

VMWare PKS

Soluções kubernetes

Google Kubernetes Engine

Cloud Foundry
(Korifi)

Azure Kubernetes Service

Oracle OKE

AWS EKS

IBM Cloud Kubernetes Service

<https://www.notion.so/MATERIAL-COMPLEMENTAR-cec8924a535c4bdfa15df1696f6736d6?pvs=4>

Considerações no armazenamento

Obviamente é necessário ter *storage* disponível via rede em ambientes de produção

Leve em conta ainda necessidades em termos de velocidade de acesso, a depender da aplicação/uso

Considere o uso de SAN e NAS quando aplicável

Utilize *labels* e seletores para assinalar aplicações de acordo com o uso de *storage*

Considerações para os *nodes*

Pode-se utilizar máquinas físicas ou virtuais (provisionamento automático)

Ao menos 3 (três) master *nodes* para operar o *control plane*

Tantos *workers* quanto necessários para atender a demanda objetivada

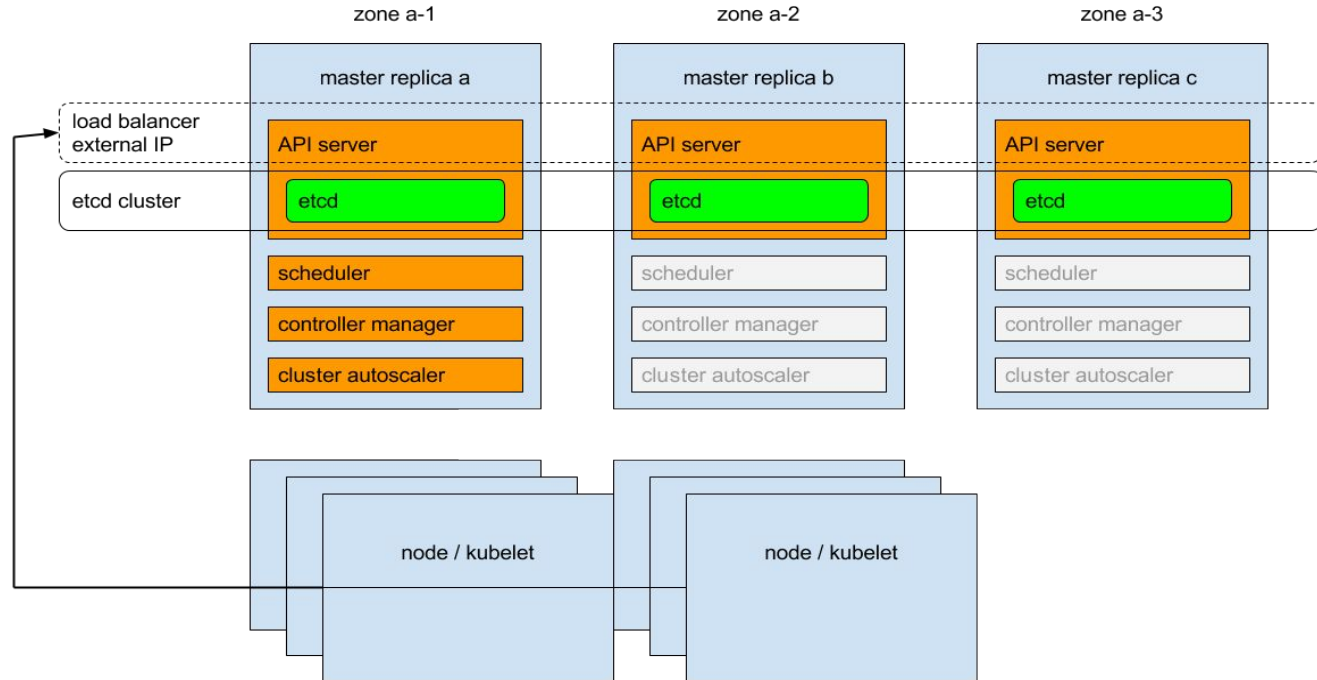
Como melhor prática, não executar *workloads* em *master nodes*

Criando clusters de alta disponibilidade com kubeadm ou kubespray

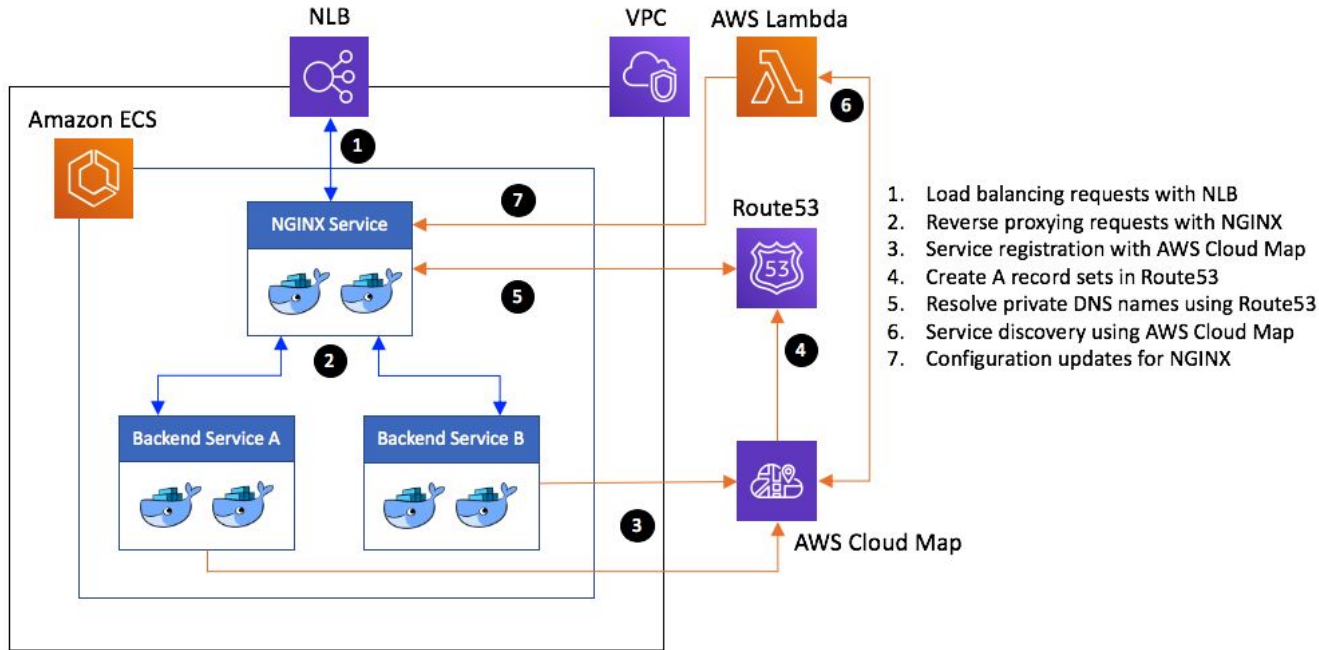
<https://kubernetes.io/docs/setup/production-environment/tools/kubeadm/high-availability/>

<https://kubernetes.io/docs/setup/production-environment/tools/kubespray/>

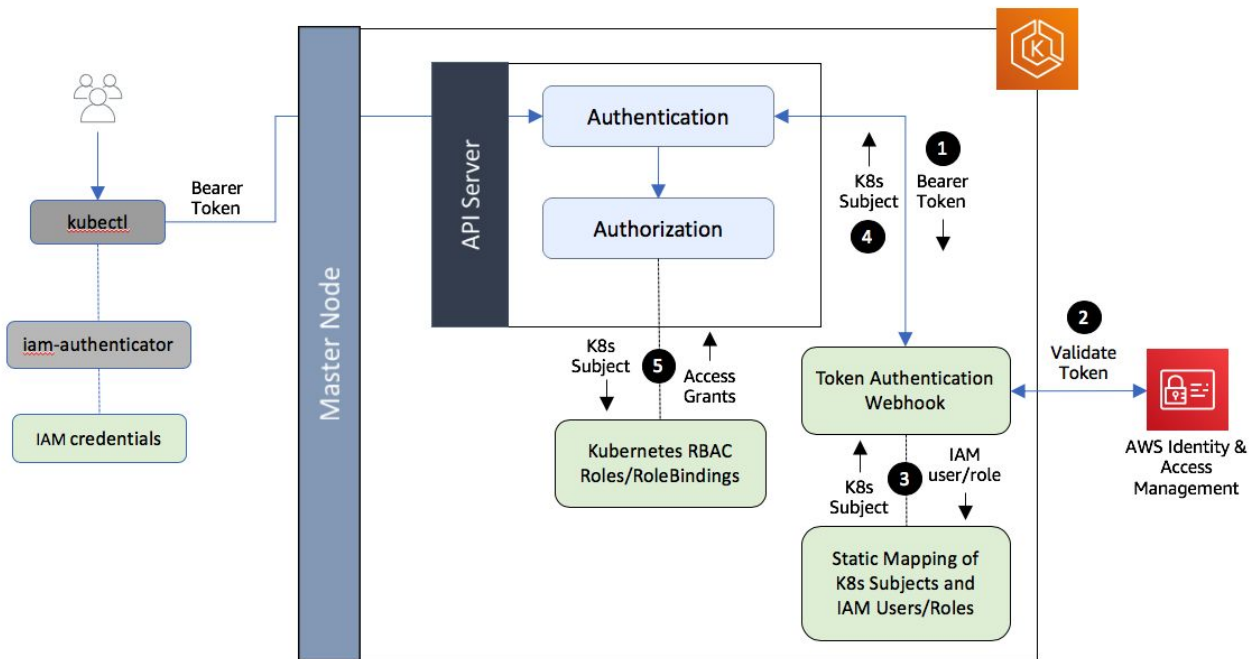
Arquitetura-exemplo



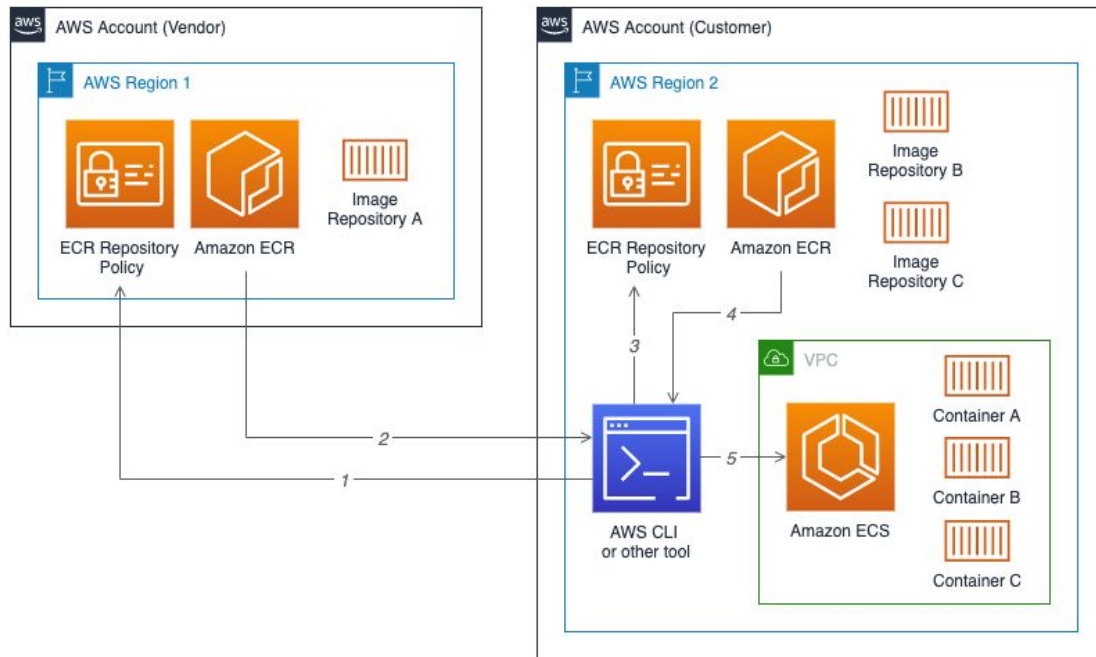
Considerações avançadas: *Load Balancing* e DNS



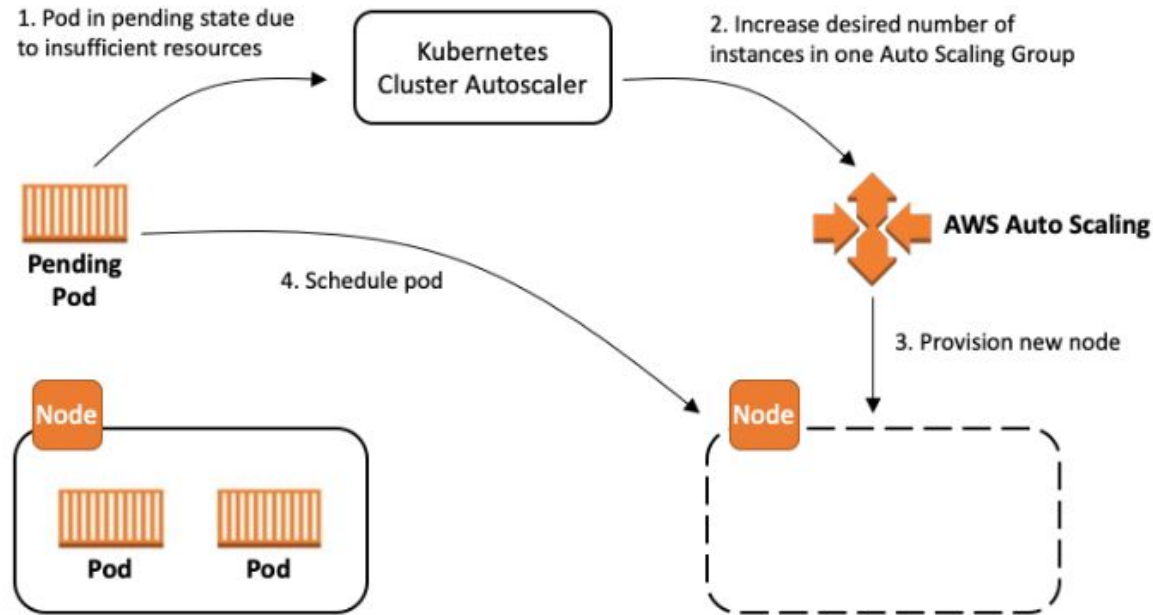
Considerações avançadas: gestão de acesso



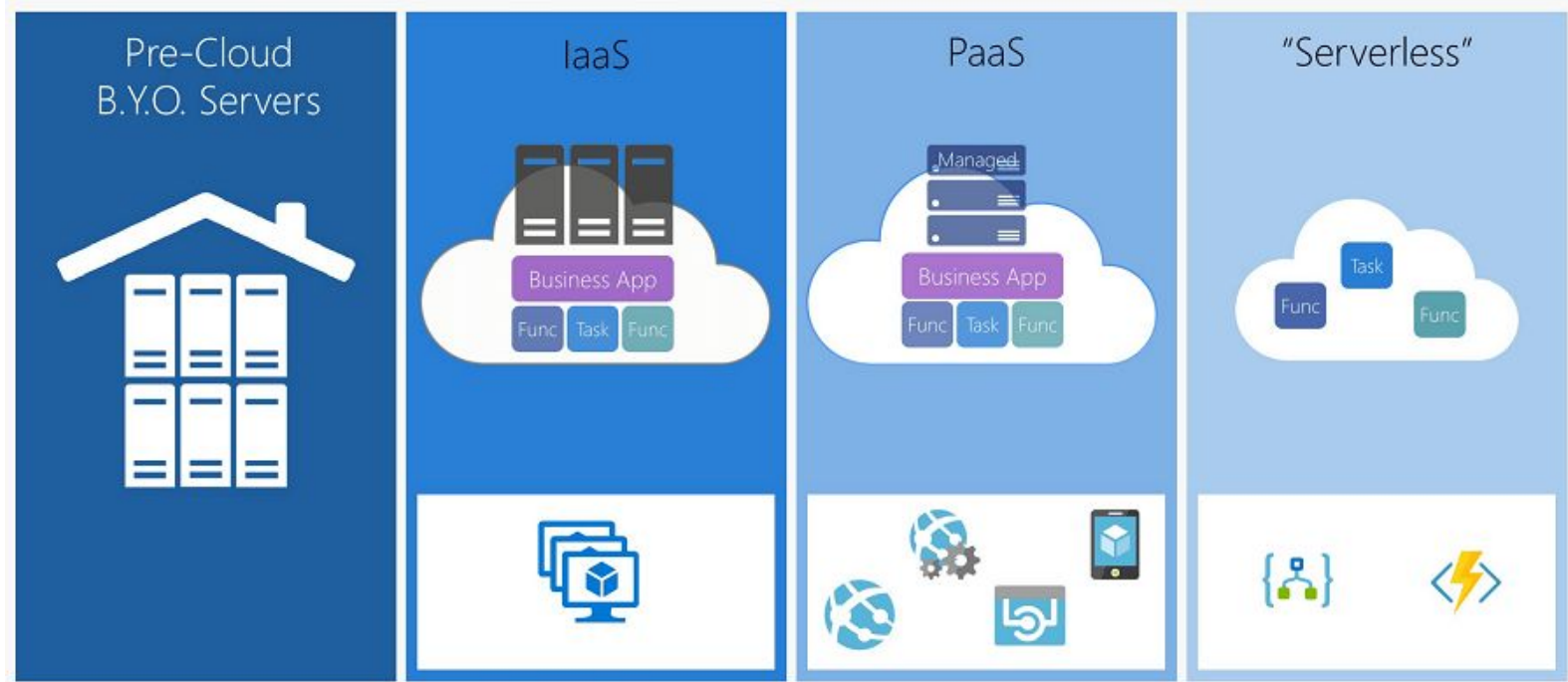
Considerações avançadas: *registry* privado



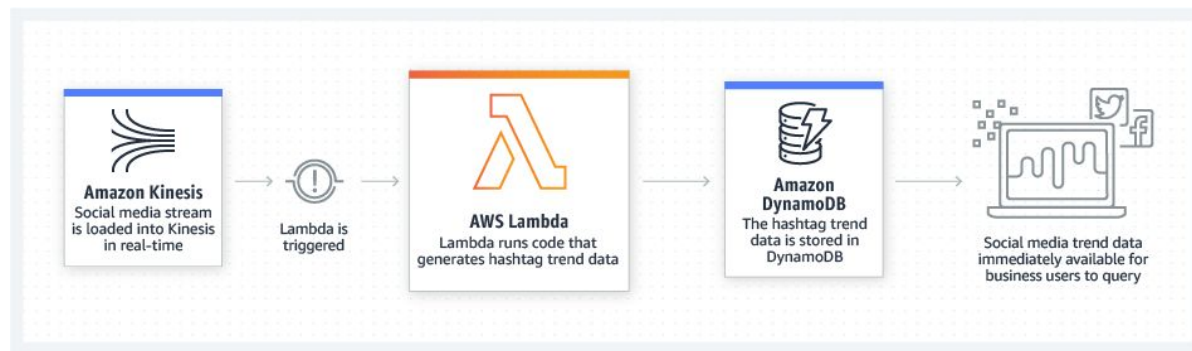
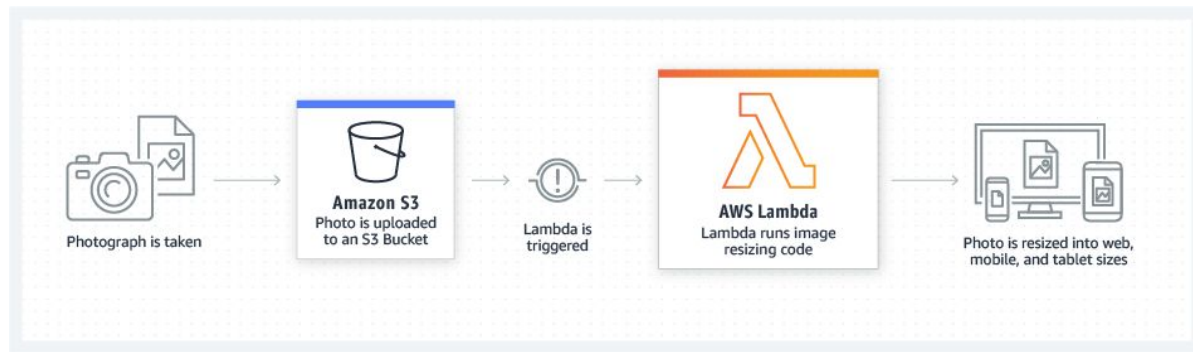
Considerações avançadas: *cluster autoscaling*



Considerações avançadas: *serverless*



Considerações avançadas: *serverless*



Considerações avançadas: *serverless*

AWS Lambda

Kubeless

Knative

Fission

OpenFaas

IronFunctions

OpenWhisk

Oracle Fn



Tópicos sobre segurança

Pergunta

Quem é o responsável pelas VMs em um ambiente de produção? E o *cluster* k8s? E as aplicações?

Segmentação de responsabilidades

Desenvolvimento
Dev

Infraestrutura
Ops

Segurança
Sec

VMs

Rede

Storage

Loadbalancer

DNS

Kubernetes

Configuração

Deployments

Aplicações

Teste

Integração

Imagens

Pentesting

WAF

Políticas

Considerações adicionais

Permissividade em ambientes
dev x produção

Compartilhamento de
responsabilidade

Realização de *sprints* com
participação conjunta

Abordagem cooperativa

Desafios com relação à segurança

Comunicação de rede em
larga escala pod-to-pod
(movimentação lateral)

Gerência de configuração: do
cluster às imagens de
containers

Visibilidade

Segurança no K8S

<https://kubernetes.io/docs/concepts/security/overview/>

<https://kubernetes.io/docs/tasks/administer-cluster/securing-a-cluster>

<https://www.stackrox.com/post/2020/05/kubernetes-security-101/>










































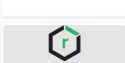






Segurança no K8S

<https://www.aquasec.com/cloud-native-academy/kubernetes-in-production/kubernetes-security-best-practices-10-steps-to-securing-k8s/>

[https://cheatsheetseries.owasp.org/cheatsheets/Kubernetes Security Cheat Sheet.html](https://cheatsheetseries.owasp.org/cheatsheets/Kubernetes_Security_Cheat_Sheet.html)

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-190.pdf>

Projetos em segurança

 alcide Alcide Funding: \$12.3M	 anchore Anchore ★ 1,285 Funding: \$23M	 apolicy Apolicy Funding: \$3.5M	 aqua Aqua Funding: \$205M	 ARMO ARMO Funding: \$205M	 BLACKDUCK Black Duck MCap: \$44.5B	 BLOOMBASE Bloomberg Funding: \$30M	 CAPSULE8 Capsule8 Funding: \$30M
 cert-manager Cloud Native Computing Foundation (CNCF) ★ 7,634 Funding: \$3M	 Check Point Check Point Software Technologies MCap: \$16.4B	 CHEF INSPEC Chef Software ★ 2,362 Funding: \$105M	 clair Red Hat ★ 8,059 MCap: \$126.6B	 Curiefense Cloud Native Computing Foundation (CNCF) ★ 243 Funding: \$3M	 Datica Datica Funding: \$14.8M	 dex Cloud Native Computing Foundation (CNCF) ★ 6,164 Funding: \$3M	 DOSEC Dosec ★ 6,164 Funding: \$3M
 Fairwinds Insights Fairwinds Funding: \$3M	 falco Cloud Native Computing Foundation (CNCF) ★ 3,343 Funding: \$3M	 FOSSA FOSSA ★ 910 Funding: \$33.9M	 FOSSID FOSSID ★ 910 Funding: \$33.9M	 Goldilocks Fairwinds ★ 865	 Grafeas Google ★ 1,242 MCap: \$1.8T	 in-toto Cloud Native Computing Foundation (CNCF) ★ 267 Funding: \$3M	 Keylime Cloud Native Computing Foundation (CNCF) ★ 267 Funding: \$3M
 kube-bench Aqua Security ★ 3,333 Funding: \$28M	 kube-hunter Aqua Security ★ 3,123 Funding: \$28M	 kyverno Cloud Native Computing Foundation (CNCF) ★ 1,293 Funding: \$3M	 NeuVector NeuVector Funding: \$10M	 vulntray Cloud Native Computing Foundation (CNCF) ★ 2,849 Funding: \$3M	 Open Policy Agent Cloud Native Computing Foundation (CNCF) ★ 1,272 Funding: \$3M	 OpenSCAP Red Hat ★ 814 MCap: \$126.6B	 orca security Orca Security ★ 814 Funding: \$40M
 PARSEC Cloud Native Computing Foundation (CNCF) ★ 216 Funding: \$3M	 pluto Fairwinds ★ 608	 polaris Fairwinds ★ 2,234	 portshift Portshift Funding: \$3.3M	 paloalto networks Palo Alto Networks MCap: \$57.8B	 青藤云安全 QINGTENG, CH Funding: \$179.8M	 RBAC LOOKUP Fairwinds ★ 527	 rbac manager Fairwinds ★ 527
 snyk Snyk Funding: \$72M	 nexus repository Sonatype Funding: \$154.7M	 SONOBUOY Sonobuoy ★ 2,322 MCap: \$63.9B	 STACKHAWK Stackhawk Funding: \$14.6M	 StackRox StackRox Funding: \$65.5M	 Synchron Security Tower Synchron Group Funding: \$279.5M	 sysdig SECURE Sysdig Funding: \$279.5M	 探真科技 TensorSecurity Funding: \$279.5M

Tarefa 10

As atividades práticas desta sessão podem ser obtidas em formato HTML via:

<https://bit.ly/ads19-tarefas-s10>



ESCOLA
SUPERIOR
DE REDES

Arquitetura do cluster Kubernetes