CLOUD NATIVE

THE NEW STACK IN A TORTILLA

slides: https://berkus.org

Josh Berkus
Red Hat OSPO
FOSSY 2023
@fuzzychef@m6n.io

ME

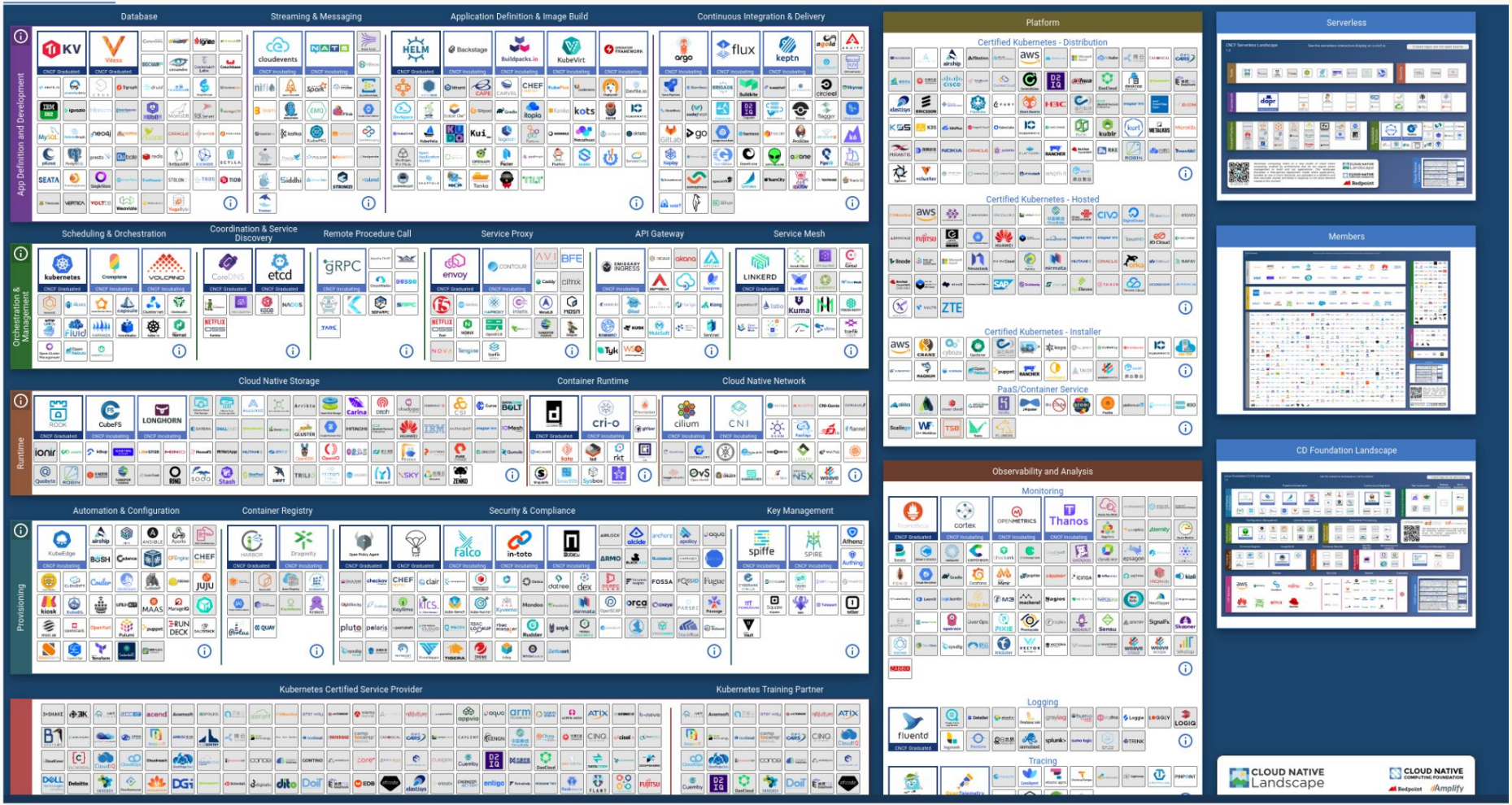
- CNCF Ambassador
- TAG Contributors
- Kubernetes SIG Chair
- RedHat Kubernetes

@fuzzychef@m6n.io
slides: https://berkus.org

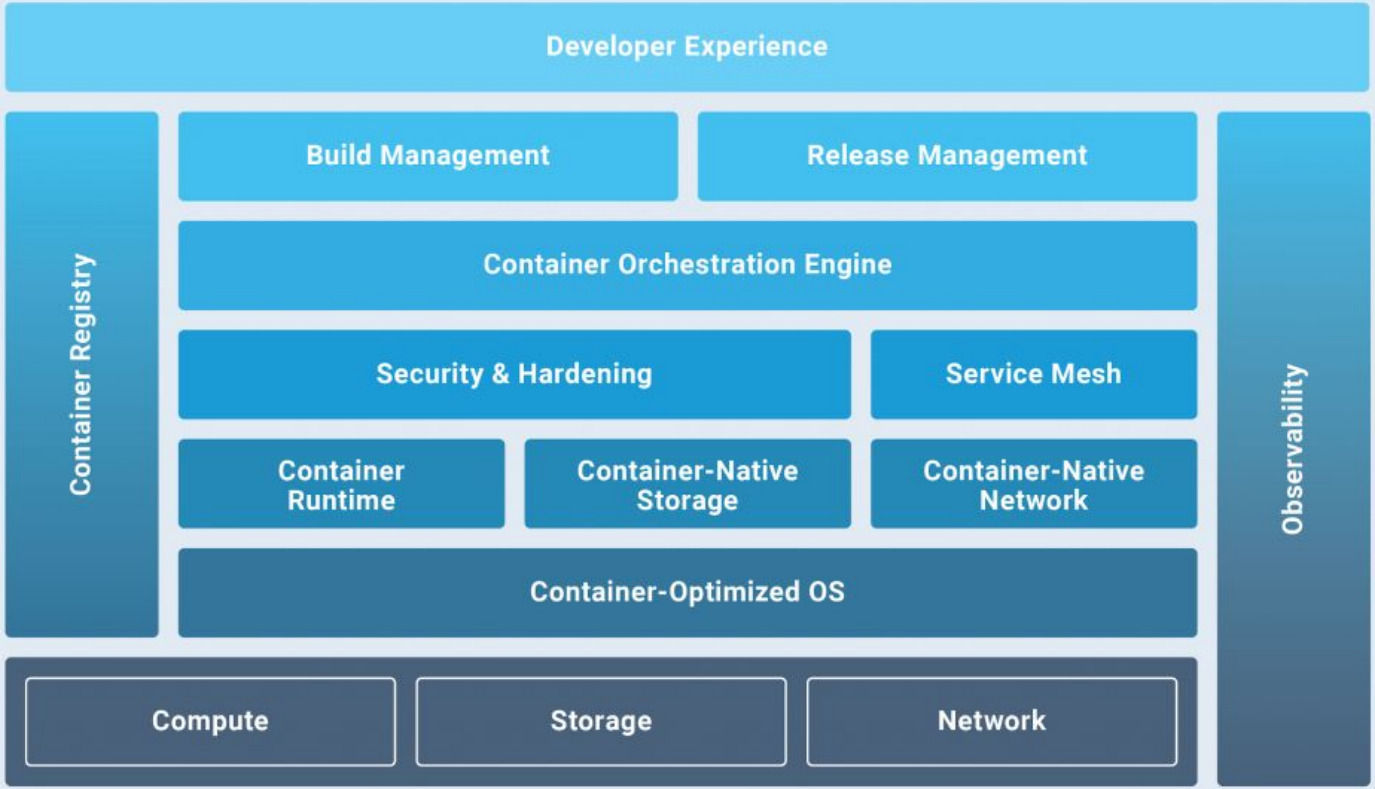
WHAT'S CLOUD NATIVE?

“Cloud native technologies empower organizations to build and run scalable applications in modern, dynamic environments such as public, private, and hybrid clouds. Containers, service meshes, microservices, immutable infrastructure, and declarative APIs exemplify this approach.

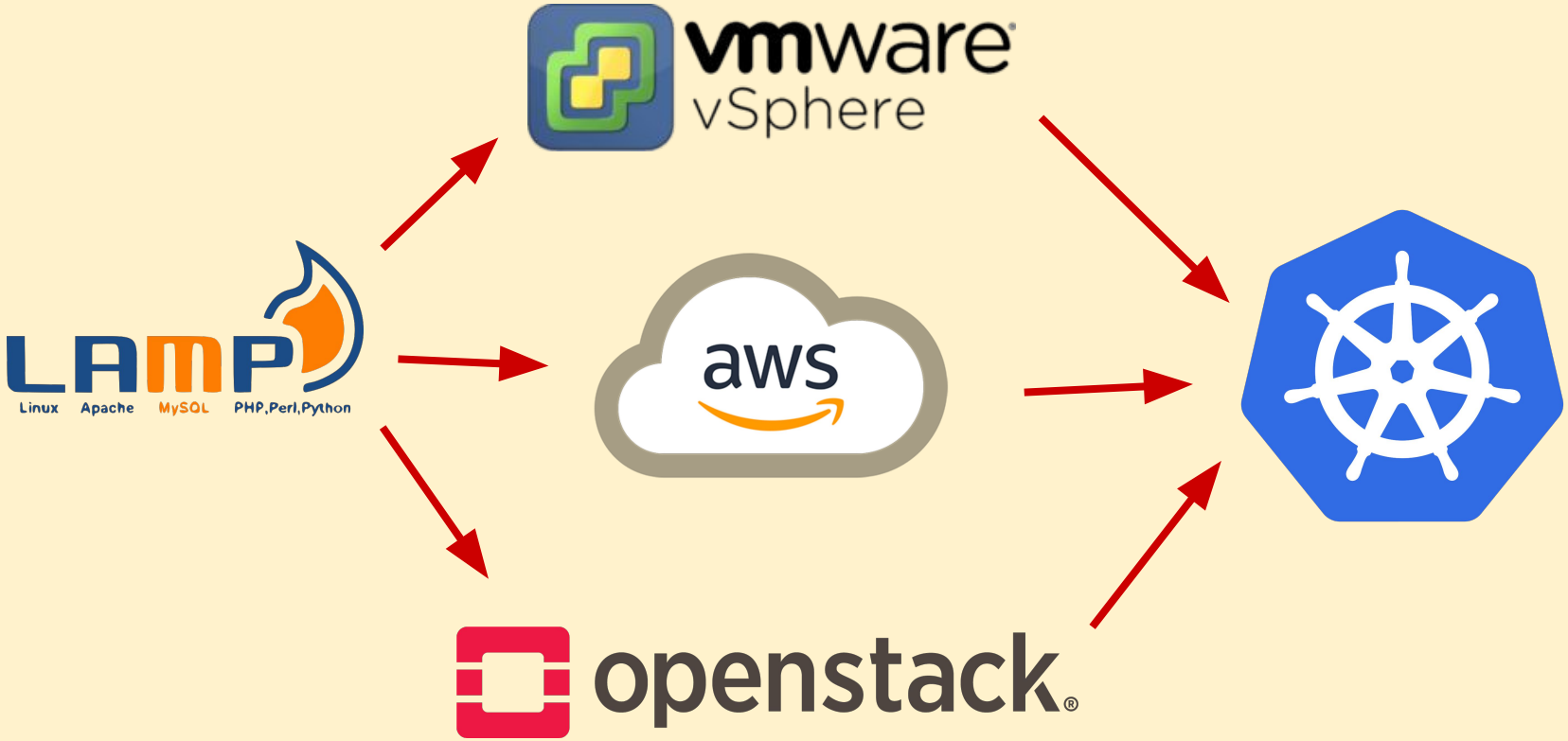
These techniques enable loosely coupled systems that are resilient, manageable, and observable. Combined with robust automation, they allow engineers to make high-impact changes frequently and predictably with minimal toil.”

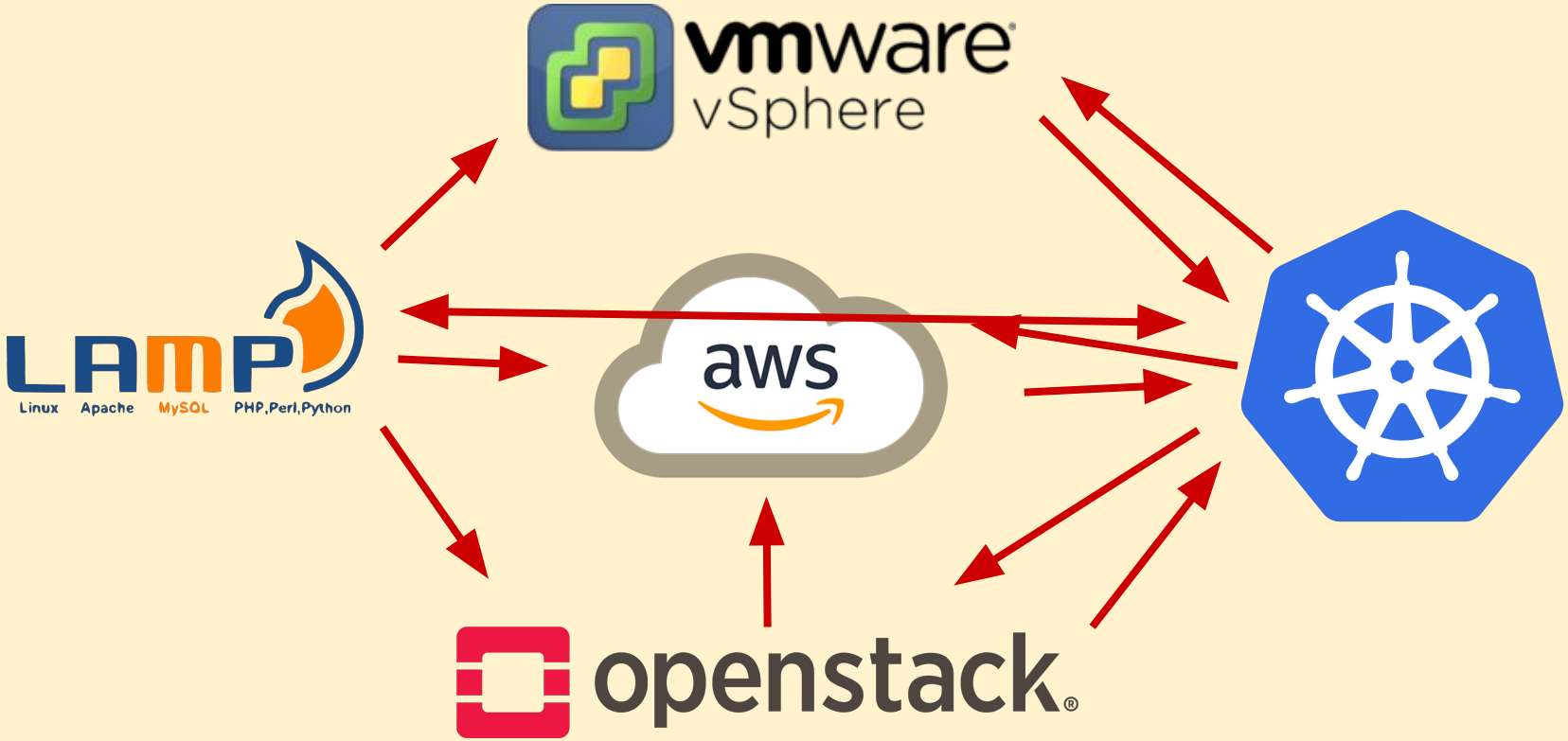

App Definition and Development
Database
Streaming & Messaging
Application Definition & Image Build
Continuous Integration & Delivery
Orchestration & Management
Scheduling & Orchestration
Coordination & Service Discovery
Remote Procedure Call
Service Proxy
API Gateway
Service Mesh
Runtime
Cloud Native Storage
Container Runtime
Cloud Native Network
Provisioning
Automation & Configuration
Container Registry
Security & Compliance
Key Management
Kubernetes Certified Service Provider
Kubernetes Training Partner
Platform
Certified Kubernetes - Distribution
Certified Kubernetes - Hosted
Certified Kubernetes - Installer
PaaS/Container Service
Observability and Analysis
Monitoring
Logging
Tracing
Serverless
Members
CD Foundation Landscape
CLOUD NATIVE Landscape
CLOUD NATIVE COMPUTING FOUNDATION

The Cloud Native Stack



Source: Janakiram MSV


vmware
vSphere
LAMP
Linux Apache MySQL PHP,Perl,Python
aws
openstack®


vmware
vSphere
LAMP
Linux Apache MySQL PHP,Perl,Python
aws
openstack®

FILLINGS

- CHICKEN
- CARNITAS
- BARBACOA
- STEAK
- SOFRITAS
- VEGGIE

RICE AND BEANS

- WHITE RICE
- BROWN RICE
- BLACK BEANS
- PINTO BEANS
- FAJITA VEGGIES

TOPPINGS

- CHEESE
- FRESH TOMATO SALSA
- CHILI-CORN SALSA
- RED-CHILI SALSA
- GREEN-CHILI SALSA
- SOUR CREAM
- LETTUCE
- QUESO
- GUACAMOLE

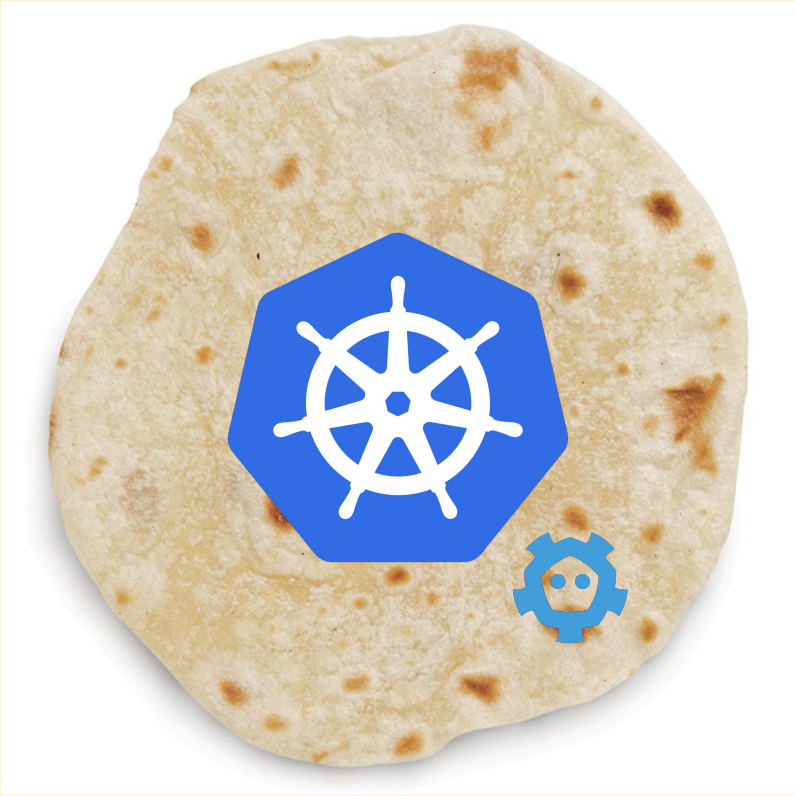
SIDES

- CHIPS
- CHIPS & GUACAMOLE
- CHIPS & QUESO
- CHIPS & SALSA

build your own burrito

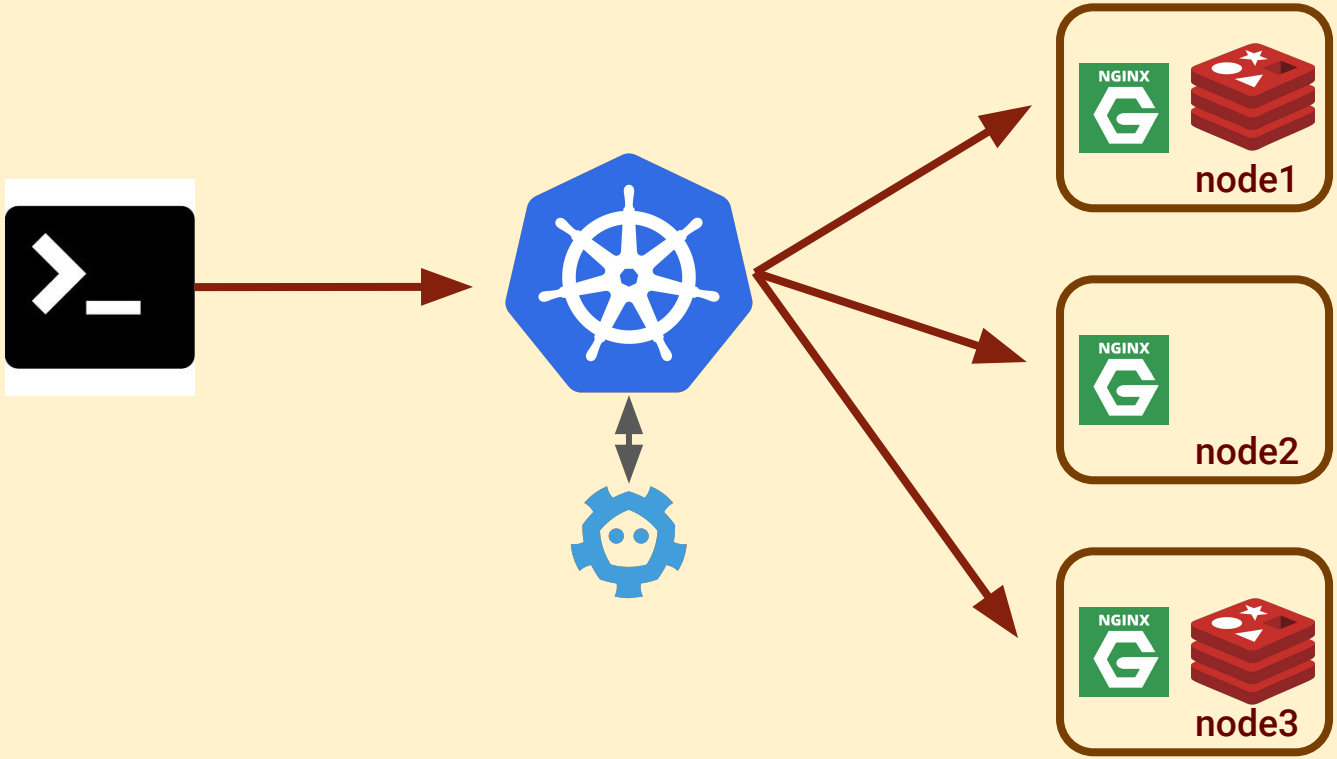
- some things are required
  - even those have options
- many things are optional
- combinations are infinite


320 Calories
9g Fat
50g Carbs
8g Protein
FLOUR TORTILLA (BURRITO)
200 Calories
9g Fat
29g Carbs
3g Protein
TACO SHELLS (3 TACOS)
250 Calories
8g Fat
40g Carbs
7g Protein
FLOUR TORTILLAS (3 TACOS)
210 Calories
4-6g Fat
36-40g Carbs
4g Protein
WHITE/BROWN RICE
40 Calories
1g Fat
7g Carbs
3g Protein
CAULIFLOWER RICE
320 Calories
9g Fat
50g Carbs
8g Protein
FLOUR TORTILLA (BURRITO)
200 Calories
9g Fat
29g Carbs
3g Protein
TACO SHELLS (3 TACOS)
180 Calories
7g Fat
0g Carbs
32g Protein
CHICKEN
150 Calories
6g Fat
1g Carbs
21g Protein
STEAK
210 Calories
12g Fat
0g Carbs
23g Protein
170 Calories
7g Fat
2g Carbs
24g Protein
150 Calories
10g Fat
9g Carbs
8g Protein
180 Calories
7g Fat
0g Carbs
32g Protein
150 Calories
6g Fat
1g Carbs
21g Protein
STEAK
130 Calories
1.5g Fat
22g Carbs
8g Protein
PINTO & BLACK BEANS
20 Calories
0g Fat
5g Carbs
1g Protein
FAJITA VEGETABLES
80 Calories
1.5g Fat
16g Carbs
3g Protein
ROASTED CORN SALSA
18g Carbs
1g Protein
CHIPOTLE HONEY VINAIGRETTE
4g Carbs
5g Protein
QUESO BLANCO
4g Carbs
0g Protein
TOMATILLO GREEN SALSA
3g Carbs
1g Protein
SUPERGREENS LETTUCE
1.5g Fat
16g Carbs
3g Protein
ROASTED CORN SALSA
220 Calories
16g Fat
18g Carbs
1g Protein
CHIPOTLE HONEY VINAIGRETTE
110 Calories
8g Fat
1g Carbs
6g Protein
MONTERY JACK CHEESE
540 Calories
25g Fat
73g Carbs
7g Protein
SIDE OF CHIPS
810 Calories
38g Fat
110g Carbs
11g Protein
LARGE CHIPS
230 Calories
22g Fat
8g Carbs
2g Protein
GUACAMOLE
460 Calories
44g Fat
16g Carbs
4g Protein
LARGE GUACAMOLE
110 Calories
8g Fat
1g Carbs
6g Protein
MONTERY JACK CHEESE
540 Calories
25g Fat
73g Carbs
7g Protein
SIDE OF CHIPS
CLOUD NATIVE
INGREDIENTS

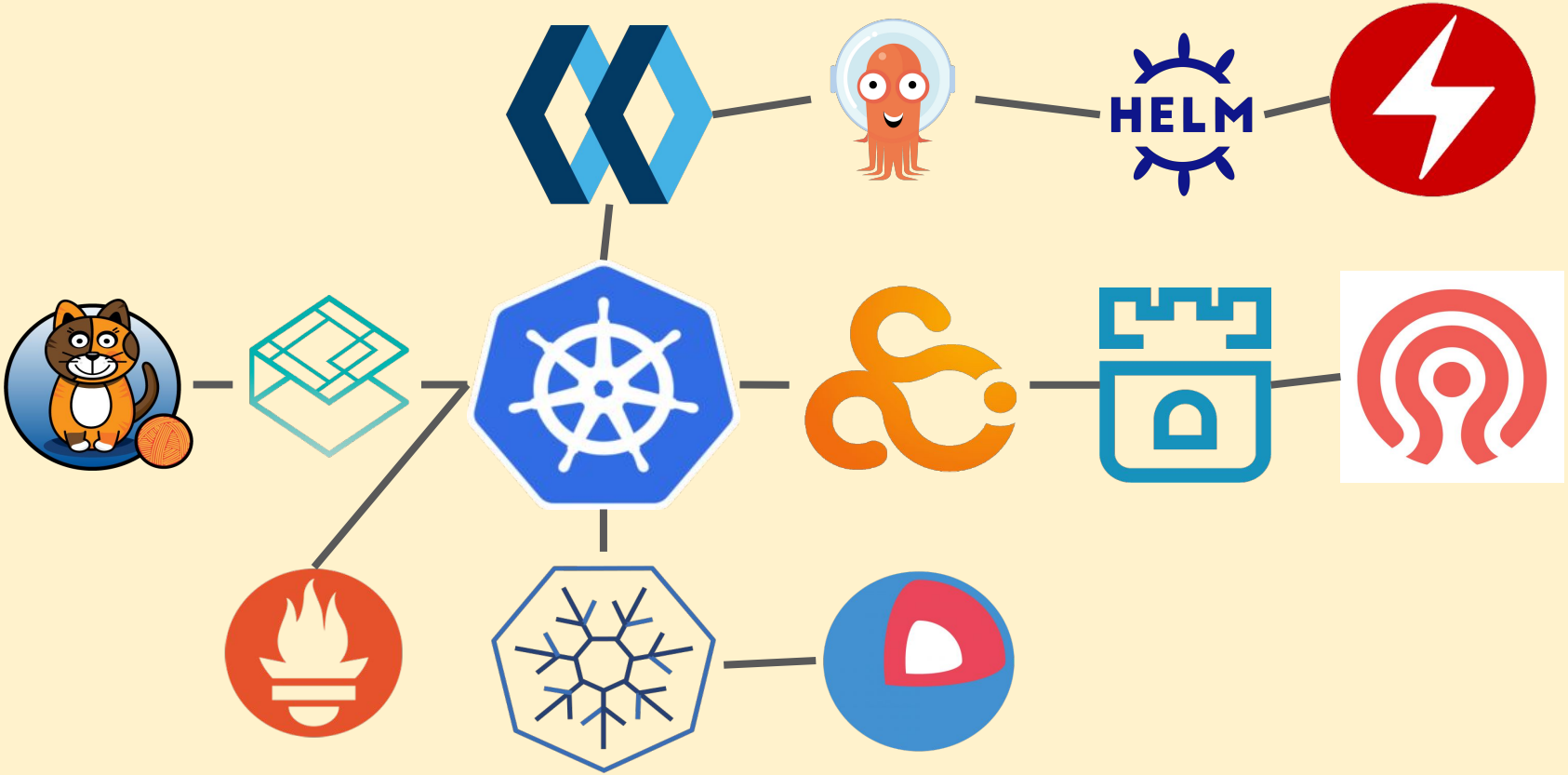


Kubernetes (and etcd)

kubernetes orchestrator



API for Cloud Native



still swappable!

lightweight mini-kubernetes

K3S

μ

rice & beans

staple components

choice of flavors, but required

(most of the time)

@fuzzychef@m6n.io

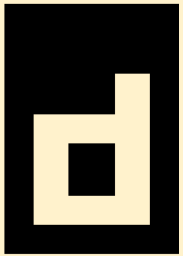
rice & beans

- container runtime
- virtual network
- storage
- cloud provider

@fuzzychef@m6n.io

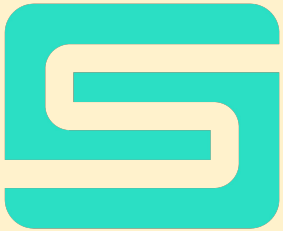
container runtimes

- why: something needs to launch the containers on each node
- options: CRI-O, containerd
  - (not Docker)
- alternates: KubeVirt, KataContainers, WASM



virtual networks

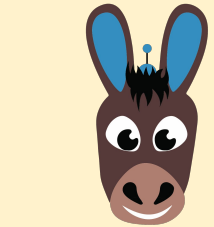
- why: containers need to have network interfaces and route connections
- CNI is the foundation
- networks: Calico, Cillium, OVN
- discovery: CoreDNS, K3GB
- routing: ingress, Contour
- WAN: Submariner, Antrea

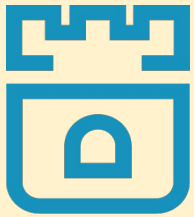


@fuzzychef@m6n.io

storage

- why: need to allocate shared storage to containers
- CSI is the foundation
- built-in: ephemeral volumes
- options: Rook, OpenEBS, Longhorn





cloud provider

- why: every Kubernetes runs somewhere
- public cloud: AWS, Azure, GCE plugin
- private cloud: OpenStack plugin
- bare metal: MetalLB, Metal^3

protein

App Deployment

because … you want to run apps on this, right?

simple apps: Helm

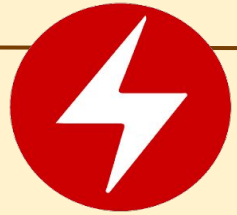
- what: a tool for scripting app deployments on Kubernetes
- who: people who have relatively simple/small clusters
- or: combine with the other app tools

dev infra: CI/CD tools

- why: build a pipeline for the whole company to deploy to Kubernetes
- what: many tools, several of which can be used together
  - ArgoCD
  - Flux
  - JenkinsX
  - Tekton & Shipwright

@fuzzychef@m6n.io

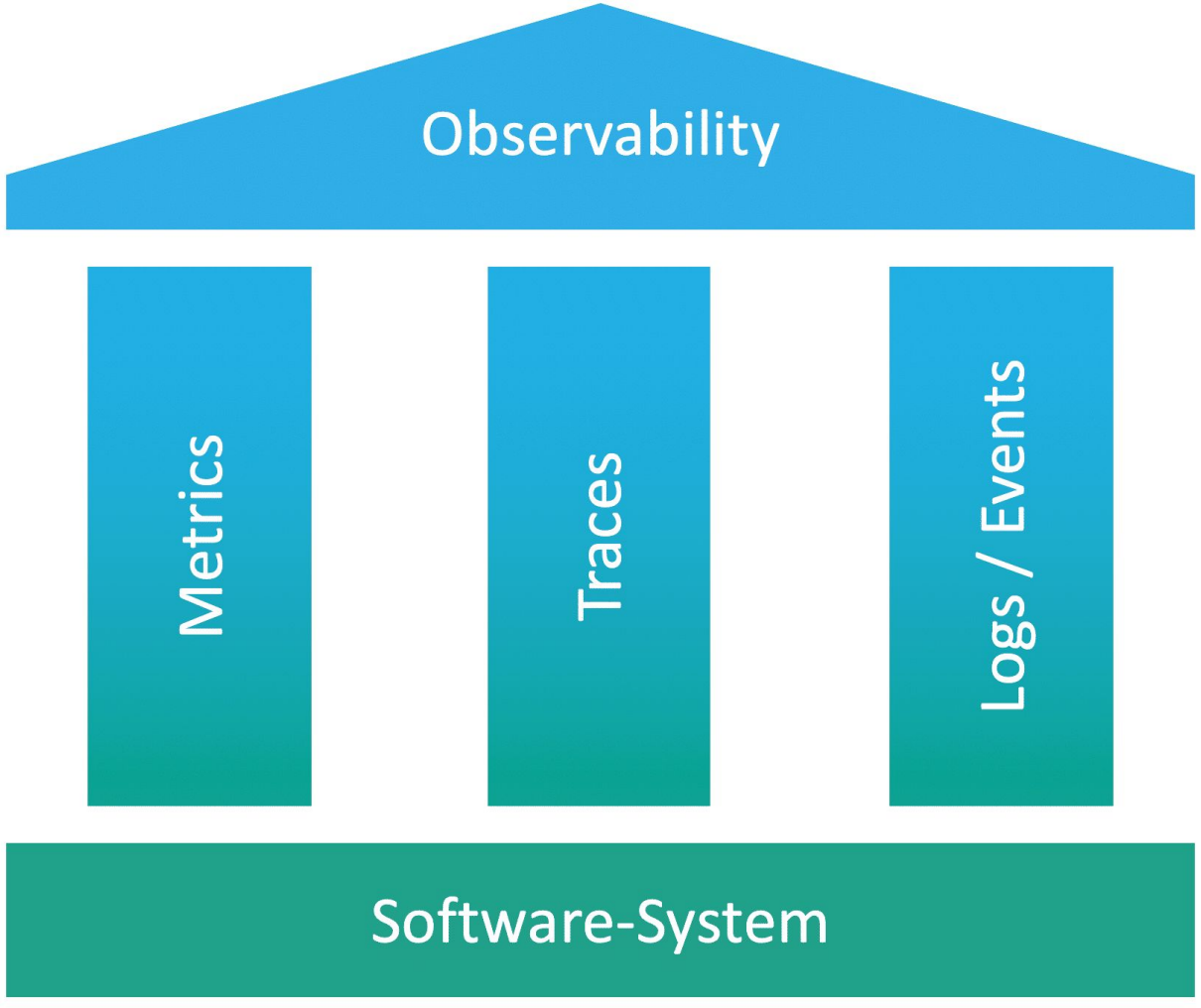
self-driving apps: Operators



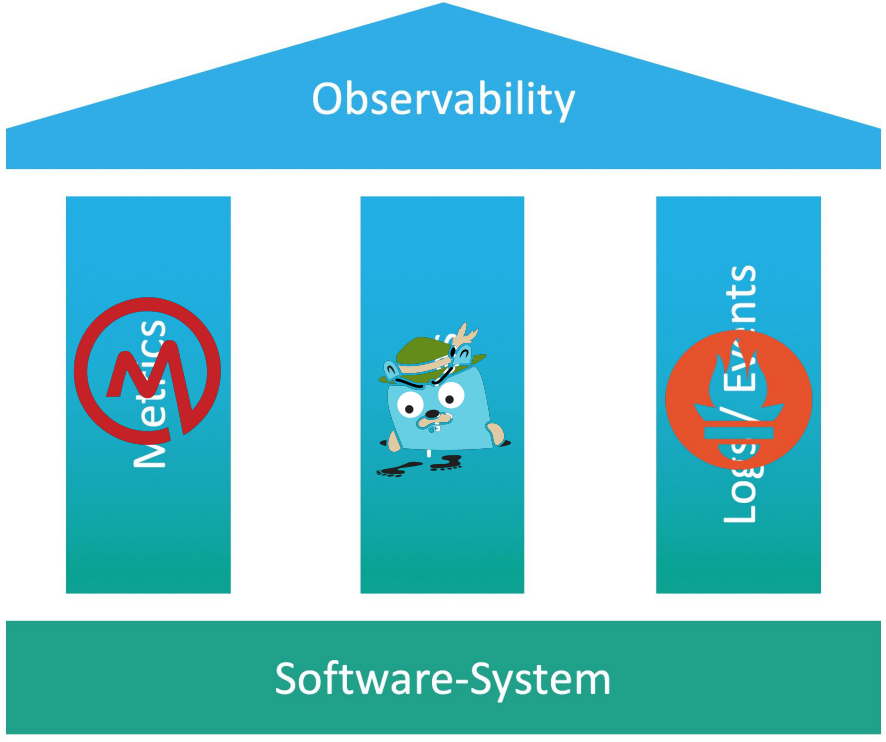
- what: Kubernetes programming for apps
- who: folks who need maximum repeatable automation
- how: write your own Kubernetes “object” (CRD) or get one from the Operator Hub

@fuzzychef@m6n.io


The Cheese:
Observability


Observability
Metrics
Traces
Logs / Events
Software-System

3 pillars in Cloud Native



ie

metry

Sysdig)

@fuzzychef@m6n.io


Toppings Time

many “optional” components

- security tools
- service mesh
- serverless
- container registry
- image building
- management
- alternate runtimes

security

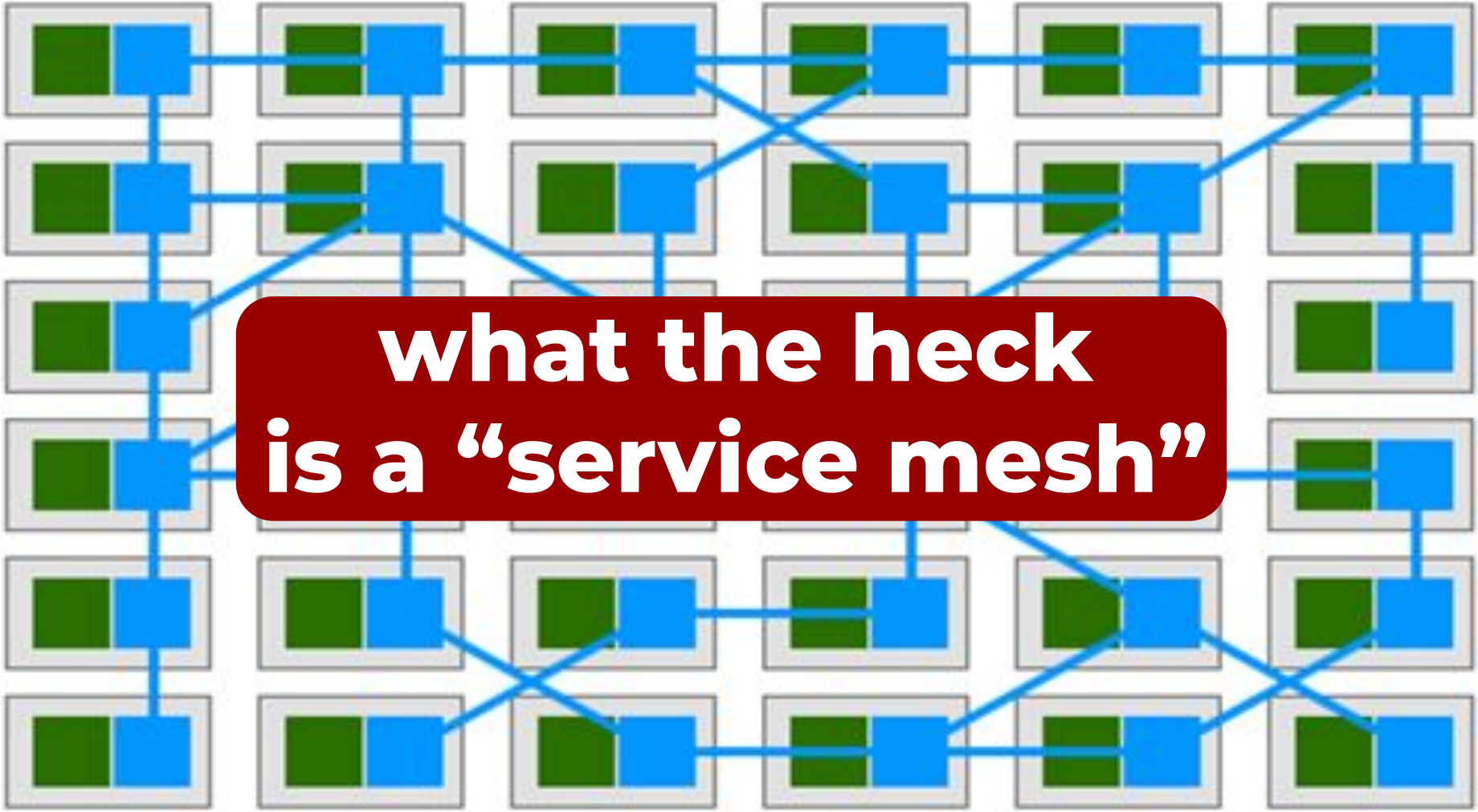
security: many + interrelated

- policy: Open Policy Agent, OCM-Policy, Kyverno
- identity/secrets: Keylime, Keycloak, Vault, Cert-Manager, SPIFFE
- network: Calico, Cillium
- runtime: confidential containers
- devops: kubelinter
- threats: Falco
- framework: Stackrox






ychef@mon.io


what the heck
is a “service mesh”

service mesh

Collapse multiple network layers (4-7) into a single tool in order to centrally control and monitor network traffic on a granular level.

Discovery, routing, sessions, and identity are controlled through configurable proxies.

Why? A/B testing, traffic status, bridging, live migration, security.

many meshes

- Istio + Envoy
- Contour + Envoy
- ~~OSM + Envoy~~
- Kuma + Envoy
- Linkerd





serverless tools

- knative: events & functions
- cloud events: event spec
- OpenFaaS: functions
- Dapr: events
- Strimzi: streaming support

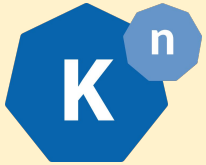
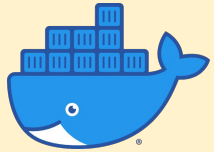
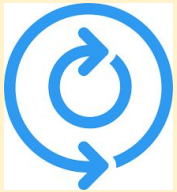
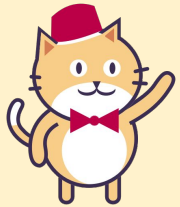


image building

- why: you need better ways to create containers from code than BASH
- what: tools that integrate into CI/CD
- tools: Docker, BuildPacks, S2I, Backstage, DevFile, Porter







@fuzzychef@m6n.io

image registry

- why: you need a private/secure place to host your own images (instead of docker/google/GH)
- what: server applications that store & distribute
- tools: Harbor, Quay, Dragonfly

alternate runtimes

- why: you need to run nonstandard containers, or you need Kubernetes to run somewhere special
- alternate containers: KubeVirt, KataContainers, WASMEdgeRuntime
- alternate kubelets: krustlet, Virtual Kubelet, KubeEdge

@fuzzychef@m6n.io

managing it all

- why: you need a console/API that lets you manage everything (inc. multiple clusters)
- tools: Open Cluster Management, CrossPlane, Keptn, Argo, Backstage

combos & specials

Cloud Native distributions & platforms

most people pick a distro

- why: too many options & tools, easier to pick an opinionated stack
  - also, integration is hard
- options: public cloud, on-prem or “hybrid”

public cloud distros

- why: you don’t want to think about install at all, and you’re OK with being on one cloud
- what: fully hosted Kubernetes + CN, you just get a kubectl interface
- tools: Google GKE, Azure AKS, Amazon EKS
  - plus most other cloud hosts

hybrid cloud distros

- why: you want to run your distro on-prem, across multiple clouds, or both
- what: full Kubernetes stack install including lots of options
- tools: Red Hat OpenShift, VMware Tanzu, SuSE Rancher

wrapping it up

burrito conclusions

- Cloud Native is an entire application runtime stack
- Like burritos, there are many alternate ingredients offering millions of possible combinations
  - a few are essential, but most are optional
  - you can start simple and build up
  - or use someone else's recipe

¿preguntas?

- josh@redhat.com
  - slack: @jberkus
  - mastodon: @fuzzychef@m6n.io
- CNCF Slack: slack.cncf.io
- Slides: https://berkus.org