Beyond the Pod: IaC with OpenShift

Mark Hinnen
System Architect
SBB CFF FFS

Martin Seman
Senior EMEA Black Belt
Red Hat

Red Hat

What we'll discuss today

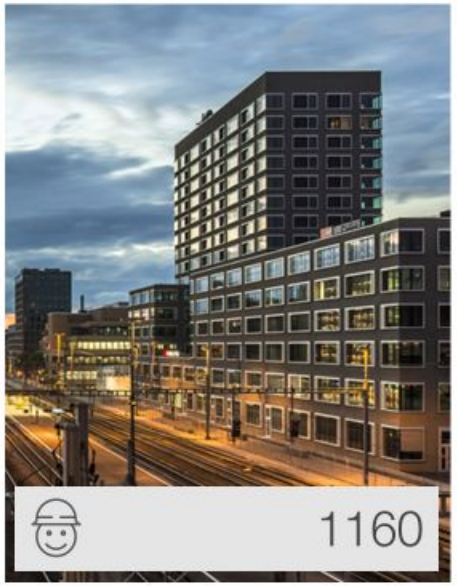
- Business Case
- Platform setup
- OpenShift
- Operators

Red Hat

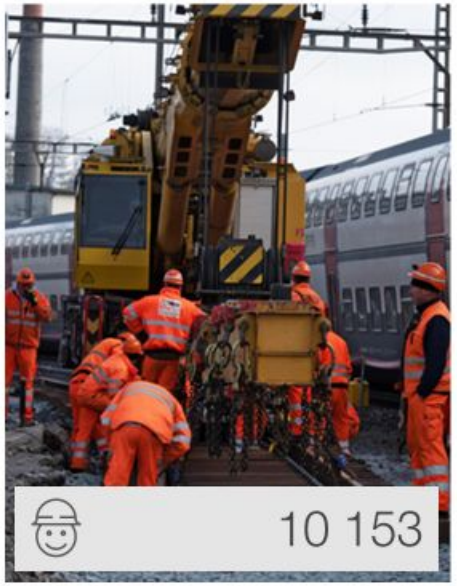
As an integrated railway, we get Switzerland moving – every single day.

Passenger Services Production
7947 trains/day

Passenger Services Markets
1,39 m. passengers/day



Real Estate
3500 buildings



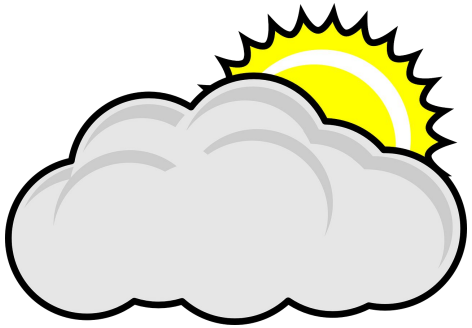
Infrastructure
3266km of network

Freight Services
170 000 tonnes of freight per day

Group-Level Units: Subsidiaries (2230 FTE), Information Technology (1444 FTE), Human Resources (812 FTE), ohter group-level units (703 FTE)

5189

Domain example of digitalization



Prediction

Realtime recommendations

Auto decisions

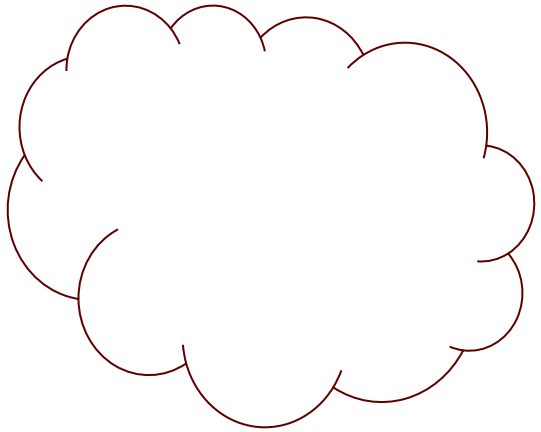
Bridge to signal boxes

Auto shunting

Red Hat

Resilience – Multi Productions

2x PROD



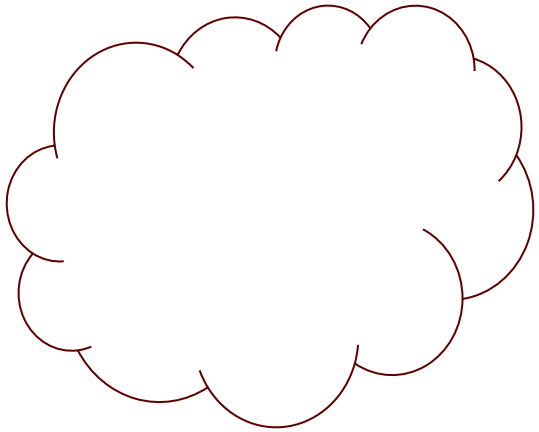
DC

Location

Config

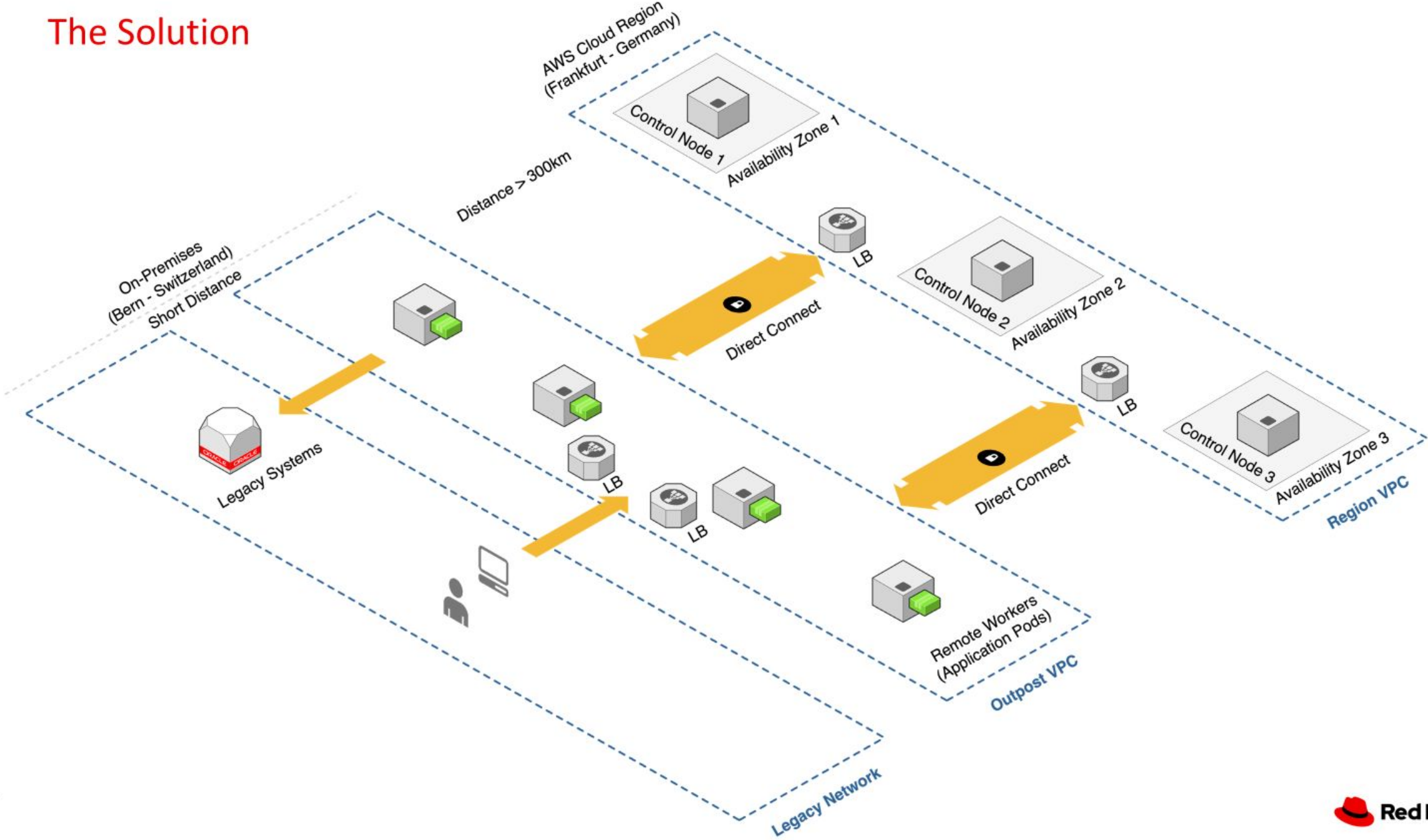
Accounts

Maintenance windows



Red Hat

The Solution



Red Hat

What is OpenShift?

Red Hat

CNCF Cloud Native Landscape

2019-07-12T03:51:02Z 024e93b

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

CNCF Incubating: KV, Vitess

Streaming & Messaging

CNCF Incubating: NATS

Application Definition & Image Build

CNCF Incubating: Helm

Continuous Integration & Delivery

CNCF Incubating: Argo, Buildkite, CircleCI, Draft, GitLab, Jenkins, Jenkins X, Spinnaker, Tekton, Weave Flux, Zuul

Orchestration & Management

Scheduling & Orchestration

CNCF Graduated: Kubernetes

Coordination & Service Discovery

CNCF Graduated: CoreDNS
CNCF Incubating: etcd

Remote Procedure Call

CNCF Incubating: gRPC

Service Proxy

CNCF Graduated: Envoy
CNCF Incubating: Linkerd

API Gateway

CNCF Incubating: Ambassador, Kong, Tyk

Service Mesh

CNCF Incubating: Linkerd, Istio, Envoy, Consul, NGINX, Traefik, Tyk, Vamp

Runtime

Container Runtime

CNCF Graduated: containerd
CNCF Incubating: cri-o, rkt, Firecracker, gVisor, kata, Pouch

Cloud-Native Network

CNCF Incubating: CNI, Cilium, Flannel, Contiv, Multus, OVN, Weave Net

Storage

CNCF Incubating: Rook

Provisioning

Automation & Configuration

CNCF Incubating: Helm, Brigade, Cloud Foundry Eirini, Cloud Foundry Korifi, Dragonfly, Harbor, Kraken, Notary, Open Policy Agent, TUF

Security & Compliance

CNCF Incubating: Falco, kube-bench, kube-hunter, Twistlock, Anchore, Aqua, Clair, OpenSCAP, SPIFFE, SPIRE

Key Management

CNCF Incubating: Vault

Platform

Certified Kubernetes - Distribution

CNCF Graduated: Prometheus

Certified Kubernetes - Hosted

Certified Kubernetes - Installer

PaaS/Container Service

Observability and Analysis

Monitoring

CNCF Graduated: Prometheus
CNCF Incubating: Thanos

Logging

CNCF Graduated: fluentd

Tracing

CNCF Incubating: Jaeger, OpenTracing

Chaos Engineering

Serverless

Public

Cloud

Kubernetes Certified Service Provider

Kubernetes Training Partner

Special

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

CLOUD NATIVE COMPUTING FOUNDATION

CLOUD NATIVE Landscape

Redpoint Amplify

CNCF Cloud Native Landscape

2019-07-12T03:51:02Z 024e93b

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

- KV — CNCF Incubating
- Vitess — CNCF Incubating
- CockroachDB, Ignite, ArangoDB, BigchainDB, Cassandra, Couchbase, Crate.io, Dgraph, druid, FoundationDB, Hasura, IBM DB2, Iguazio, Infinispan, JanusGraph, MariaDB, MemSQL, SQL Server, MongoDB, MySQL, Neo4j, nuoDB, Oracle, OrientDB, Percona, pitosa, PostgreSQL, presto, Pivotal Cloud Foundry, redis, RethinkDB, Riak KV, SEATA, ShardingSphere, Splice Machine, STOLON, TiDB, Vertica, YugaByte DB

Streaming & Messaging

- NATS — CNCF Incubating
- nifi, Apache Pulsar, RabbitMQ, Spark, Storm, Beam, cloudevents, Flink, Kafka, Pravega, RocketMQ, Siddhi, STRIMZI, +talend

Application Definition & Image Build

- HELM — CNCF Incubating
- apache brooklyn, Buildpacks.io, Buildpacks.io, Dockerfile, DRAFT, Habitat, Kaniko, Kubernetes, MIRANTIS Mirantis, OPENAPI, Packer, podman, Ship, Singularity, Snap, sqe_bh, Telepresence, TMI

Continuous Integration & Delivery

- argo, Apache Flagger, Azure Functions, Bamboo, BRIGADE, Buildkite, CircleCI, Skycap, cloudbees, codefresh, Concourse, Drone, Gitea, GitHub Actions, GitLab, go, Harness, Jenkins, Jenkins X, OpenFaaS, Rancher, shippable, Spinnaker, TeamCity, Travis CI, Weave Flux, wercker, ZUUL

Orchestration & Management

Scheduling & Orchestration

- kubernetes — CNCF Graduated
- Amazon EKS, Apache Mesos, Azure Service Fabric, Cloud Foundry Diego, Crossplane, Hashicorp Nomad

Coordination & Service Discovery

- CoreDNS — CNCF Graduated
- etcd — CNCF Incubating
- Consul, NACOS, NETFLIX OSS Eureka

Remote Procedure Call

- gRPC — CNCF Incubating
- Apache Thrift, Finagle, JSON-RPC, SOFARPC

Service Proxy

- envoy — CNCF Graduated
- AVI Networks, Citrix, F5 Networks, HAProxy, Linkerd, NGINX, Skipper, SOFAMosn, Tengine, Traefik, Vulcand

API Gateway

- 3scale, Ambassador, APISIX, Gloo, Kong, krakend, Mulesoft, Orbiter, Sentinel, Skipper, Tyk

Service Mesh

- LINKERD — CNCF Incubating
- Grey Matter, Istio, NETFLIX OSS Zuul, SuperGloo, vamp

Runtime

Cloud-Native Storage

- ROOK — CNCF Incubating
- Arrikto, ceph, Ceph CSI, CSI, DATERA, Dell EMC, elastifile, GLUSTER, HEDVIG, Hitachi Vantara, INFINIDAT, kasten, LeoFS, Longhorn, MINIO, MooseFS, NetApp, OpenEBS, OpenIO, OpenSDS, portworx, PURE Storage, Quobyte, redundant, ROBIN, RING, SWIFT, TRITON Object Storage, Weka IO, ZENKO

Container Runtime

- containerd — CNCF Graduated
- cri-o — CNCF Incubating
- rkt — CNCF Incubating
- Firecracker, gVisor, kata, lxd, Pouch, Singularity, SmartOS, unik

Cloud-Native Network

- CNI — CNCF Incubating
- alcide, Apoteo, cilium, Contiv, CUMULUS, DANM, flannel, Kube-OVN, LIBATO, Midokura, NSX, OvS, Plumgrid, Romana, Tungsten Fabric, VMware NSX, weave net, ZTE

Provisioning

Automation & Configuration

- airship, Ansible, Apollo, Bosh, CFEngine, Chef, Cloudify, Cloudsoft, Foreman, Itamae, juju, KubeOps, Landscape, Limit IT, MAAS, ManageIQ, openstack, Pallet, pulumi, puppet, Rundeck, SaltStack, StackStorm, Terraform, vmware

Container Registry

- HARBOR — CNCF Incubating
- Artifactory, Docker Registry, Dragonfly, Kraken, Portus, QUAY

Security & Compliance

- Notary — CNCF Incubating
- Open Policy Agent — CNCF Incubating
- TUF — CNCF Incubating
- anchore, aqua, Black Duck, Clair, Datica, Falco, FOSSA, Grafeas, kube-bench, kube-hunter, OpenSCAP, Oracle Container Automation, Shift Left Security, snyk, StackRox, TIGERA, Twistlock, Weave Scope

Key Management

- CyberArk Conjur, Knox, Spiffe, SPIRE, Square Keywhiz, SSO, Teleport, Vault

Platform

Certified Kubernetes - Distribution

- Canonical, Cisco Mantaro, Cloud Foundry Container Runtime, Cloudcalc, DaoCloud, docker, docker EE, EasyStack, ENC, Ericsson, Gravity, Huawei, IBM Cloud, Inspur, JD.COM, Joyent, KDS, Kontena, kubeedge, Kubermatic, Kubernetes, kublr, Messosphere, Metal K8s, Mirantis, NetApp, Netease Cloud, Oracle, Pivotal, Platform9, QingCloud, Rancher, Red Hat OpenShift, Robin, SUSE, Symphony, Tencent, vmware, VMware Pivotal

Certified Kubernetes - Hosted

- Alibaba Cloud, Amazon EKS, Azure, DigitalOcean, eBaoCloud, ELASTX, Google Kubernetes Engine, Huawei, Inspur, intellect SEEC, JD Cloud, Linode, Nirmata, Nutanix, Oracle, Platform9, Samsung SDS, SAP, Scaleway, Tencent Cloud, UCloud, vmware, ZTE

Certified Kubernetes - Installer

- Cobra.cloud, Ruby, Canonical, Google Cloud, Kops, kubeadm, KubeOne, kubespray, Linode, MicroK8s, Puppet, Rancher, Talos, vmware

PaaS/Container Service

- Flynn, Hasura, Platform9, Scalingo, Stackpoint, Tectonic, Yunify

Observability and Analysis

Monitoring

- Prometheus — CNCF Graduated
- Cortex, Grafana, kiali, Sysdig, Thanos, Sensu, SignalFx, Weave Cloud, Weave Scope, ZABBIX

Logging

- fluentd — CNCF Graduated
- elastic, graylog, Logdna, LOGGLY, Logs.io, Loom, SCALYR, sematext, splunk, sumo logic

Tracing

- JAEGER — CNCF Incubating
- OPENTRACING — CNCF Incubating
- Appdash, Datadog, Instana, LightStep, SOFATracer, Zipkin

Chaos Engineering

- Chaos Mesh, Gremlin, LitmusChaos, PowerfulSeal

Serverless

Cloud

- aws, Alibaba Cloud, DigitalOcean, Exoscale, Fujitsu, Google Cloud, Huawei, IBM Cloud, Joyent, linode, Oracle, packet, Scaleway, Tencent Cloud

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

CLOUD NATIVE COMPUTING FOUNDATION

CLOUD NATIVE Landscape

Redpoint Amplify

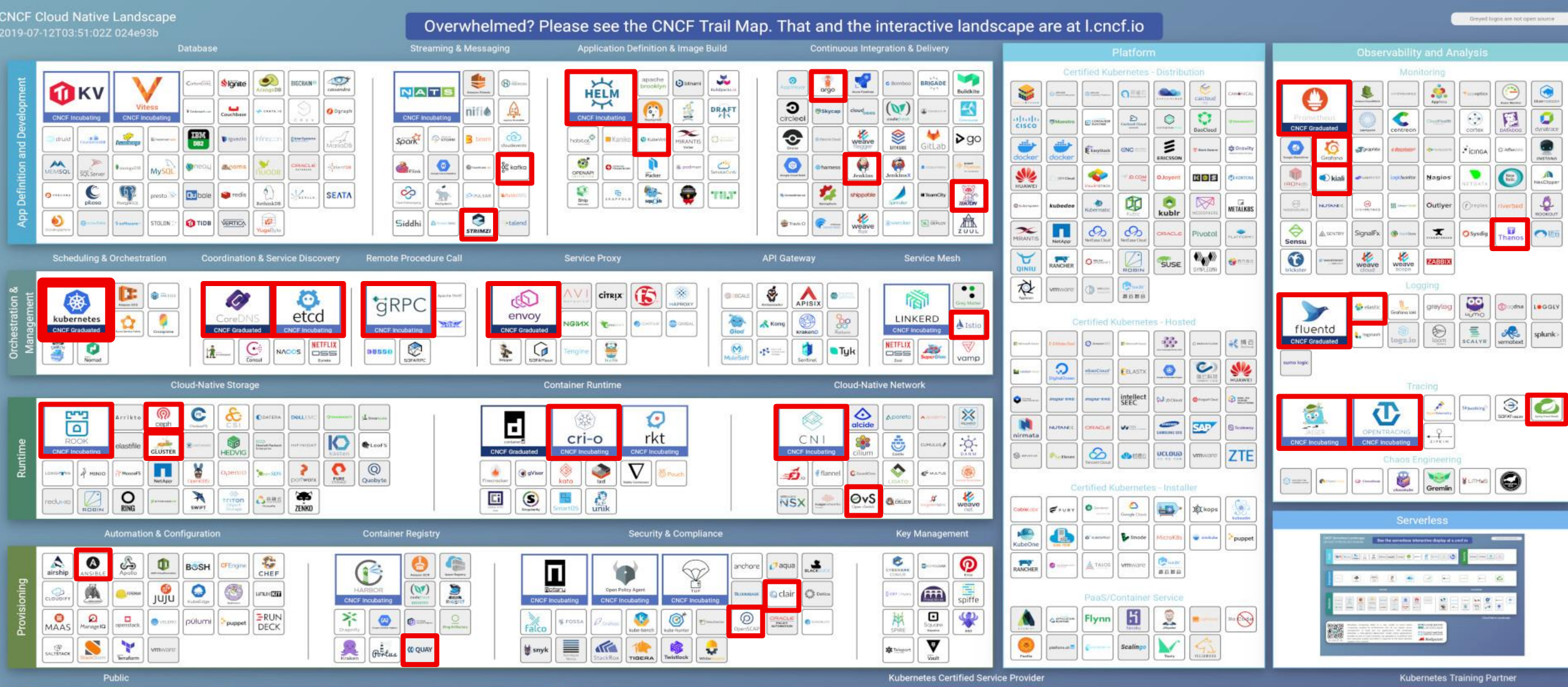
Special

- accenture, Acorn soft, BEFOLKS, Canonical, Cisco, Container Solutions, Coreos, Cuemby, DaoCloud, Container Solutions, Deloitte, Dell Technologies, Doit, EasyStack, elastisys, ELASTX, FLANT, grape up, Heptio, Huawei, IBM Cloud, Inovex, Isotoma, JFrog, kublr, kumina, loodse, Mirantis, mobilise, navilas, Nirmata, NTT Data, OCTO, Origins, Platform9, portworx, Pragma, Rancher, Reactive Ops, Rx-M, Samsung SDS, SAP, Sighup, Southbridge, SUSE, Tectonic, Treasure Data, VMware, ZTE

Public

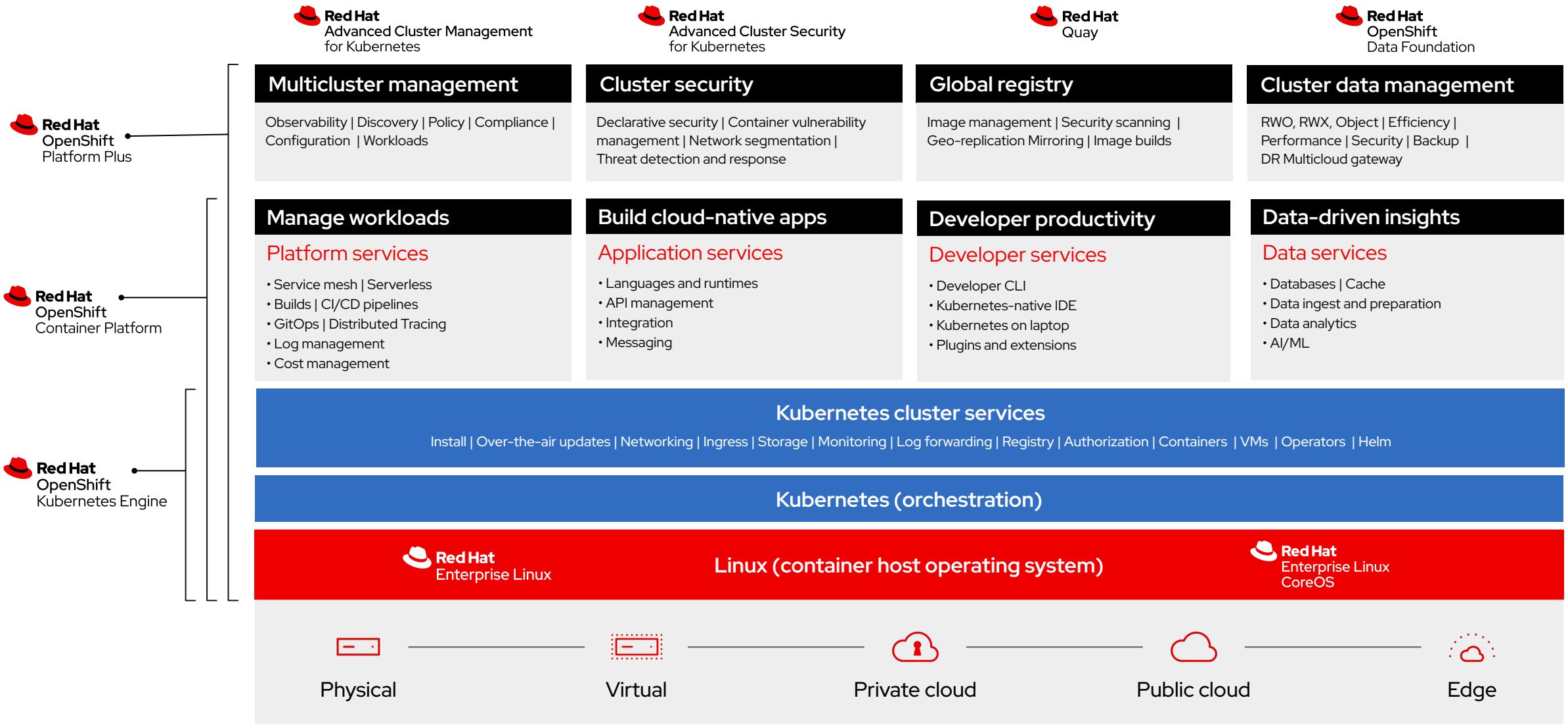
Kubernetes Certified Service Provider

Kubernetes Training Partner



Red Hat manages and MAINTAINS this complexity for its customers

Red Hat OpenShift

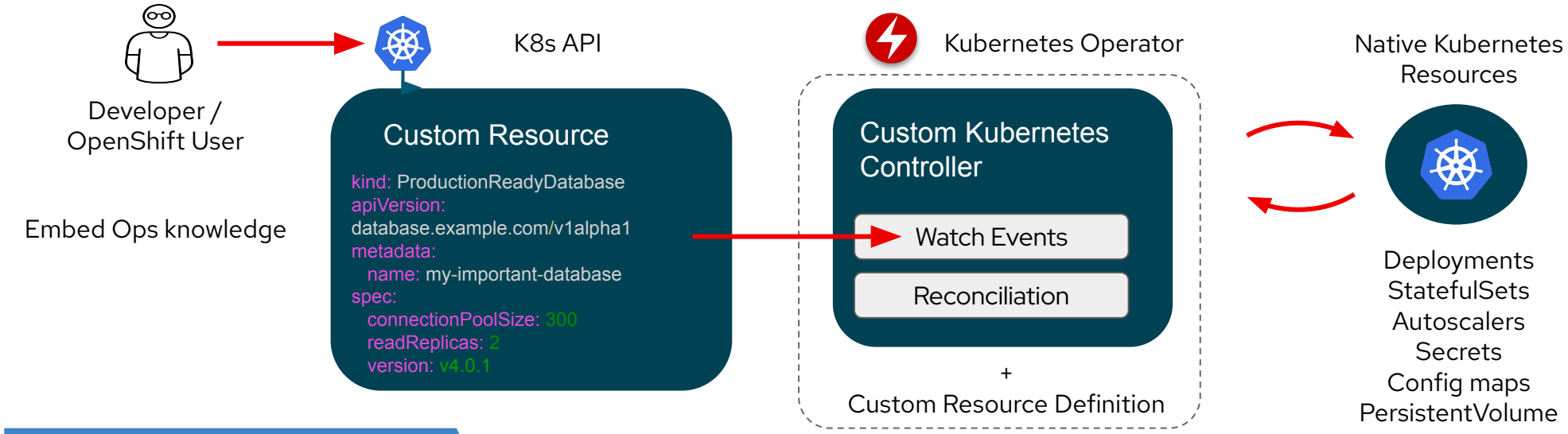


Red Hat

OpenShift Operators

Red Hat

Managing deployments



Helm
Package and Basic Install

Operator
Automated Day-2 Operations

Phase I	Phase II	Phase III	Phase IV	Phase V
Basic Install	Seamless Upgrades	Full Lifecycle	Deep Insights	Auto Pilot
Automated application provisioning and configuration management	Patch and minor version upgrades supported	App lifecycle, storage lifecycle (backup, failure recovery)	Metrics, alerts, log processing and workload analysis	Horizontal/vertical scaling, auto config tuning, abnormal detection, scheduling tuning

Red Hat

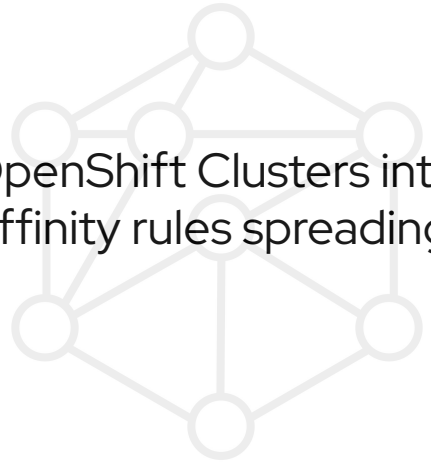
Custom Resource Definitions (CRDs) from the SBB perspective

Life of Devs

Config Errors

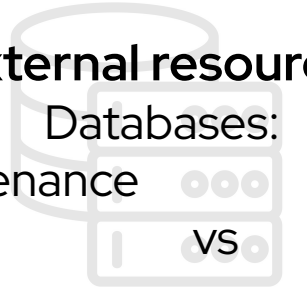
Red Hat

Default usage: Internal kubernetes setup



Solve OpenShift Clusters internal like anti-affinity rules spreading pods

Pod Autoscaler



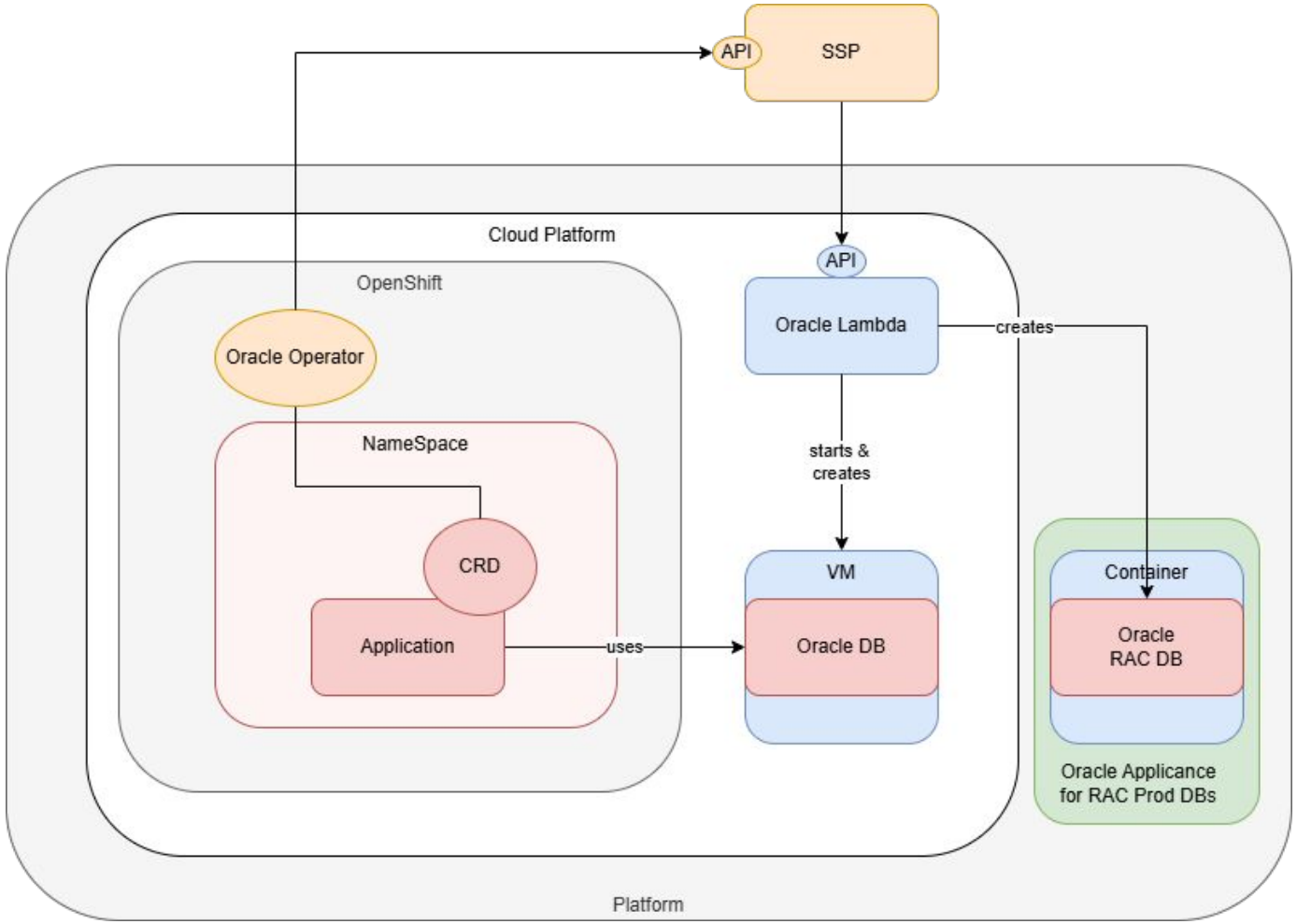
External resources

Databases:

Maintenance vs Setup

Red Hat

Database Example



CR defines:

Database name

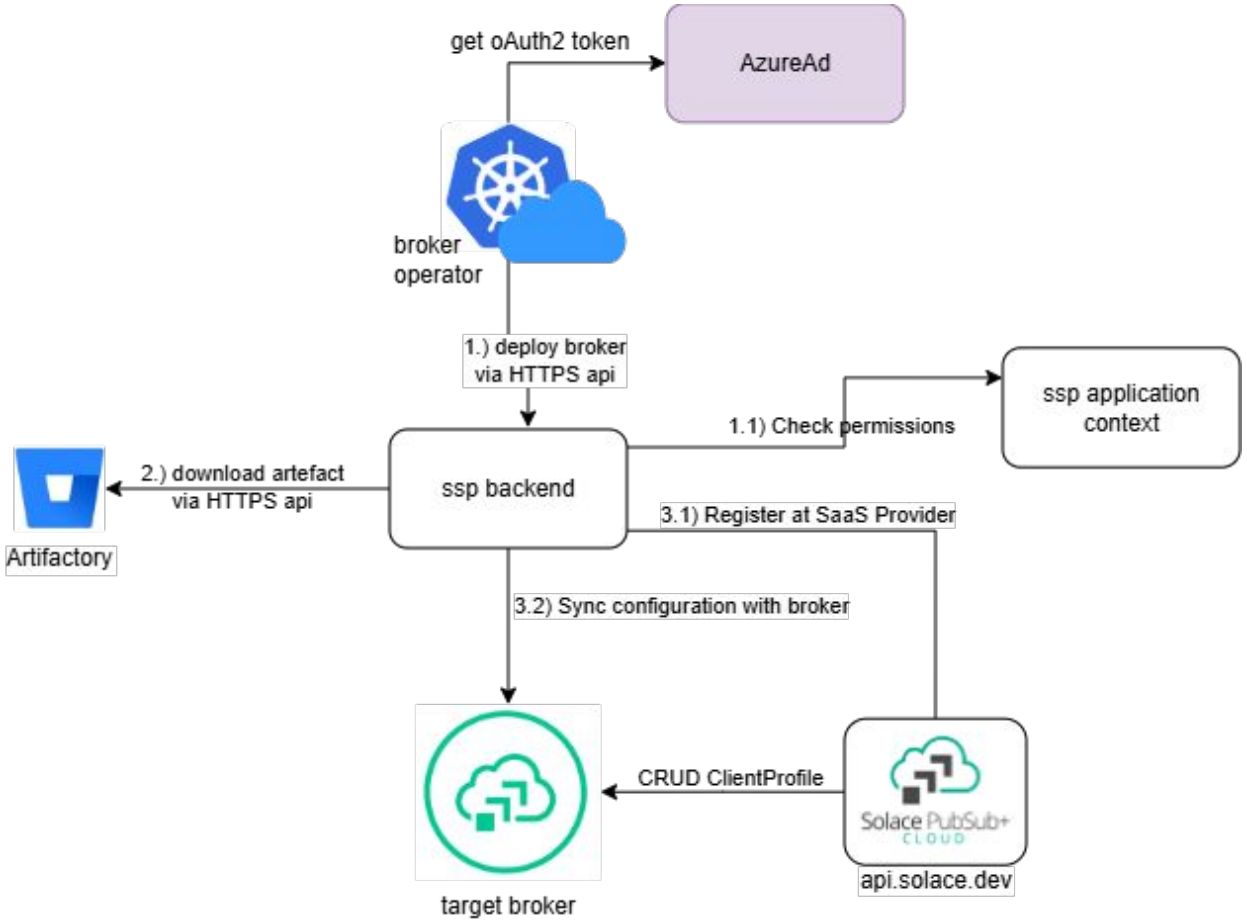
Database user/pw

Sizing/Parameter

Red Hat

The magic behind the operator

a message broker setup



Other examples:

Monitoring

AzureAD Registration

Vault Credentials

Postgres Database

Red Hat

Takeaways

Go full IaC

CRD is good abstraction for any kind of resources

Openshift & Operators

Operators are flexible and easy made

Red Hat

Thank you

Red Hat is the world's leading provider of enterprise open source software solutions. Award-winning support, training, and consulting services make Red Hat a trusted adviser to the Fortune 500.

linkedin.com/company/red-hat

youtube.com/user/RedHatVideos

facebook.com/redhatinc

twitter.com/RedHat