Repel Boarders!

How to find a Kubernetes database operator that protects your data

Robert Hodges

Altinity

v0.0.1

Altinity

A brief message from our sponsor...

Robert Hodges

Database geek with 30+ years on DBMS. Kubernaut since 2018. Day job: Altinity CEO

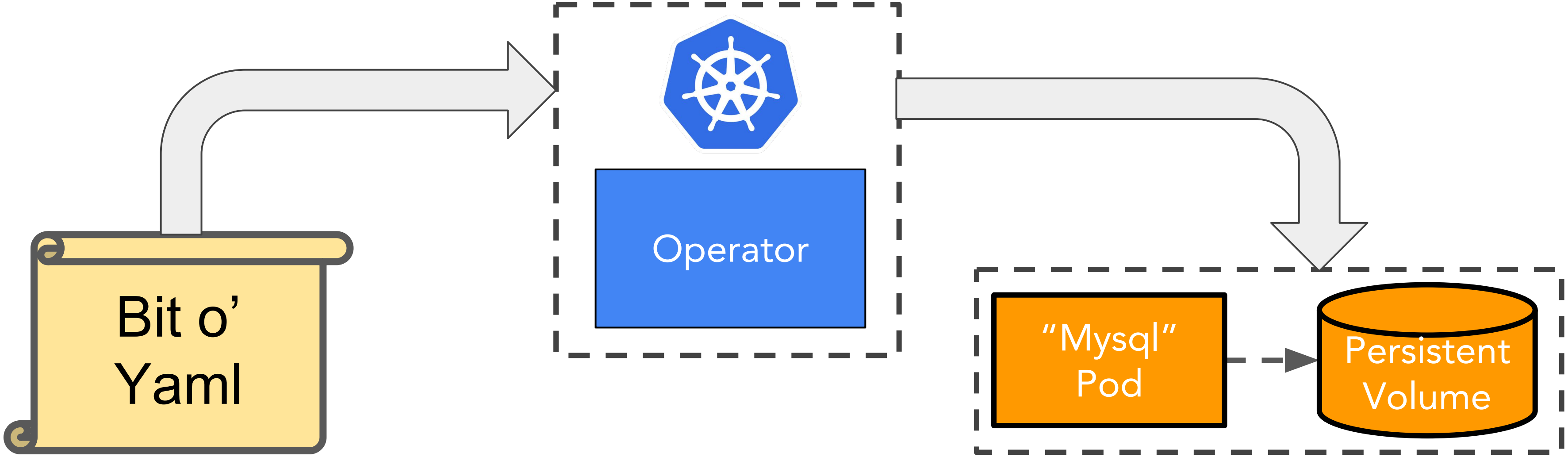
Altinity Engineering

Database geeks with centuries of experience in DBMS and applications

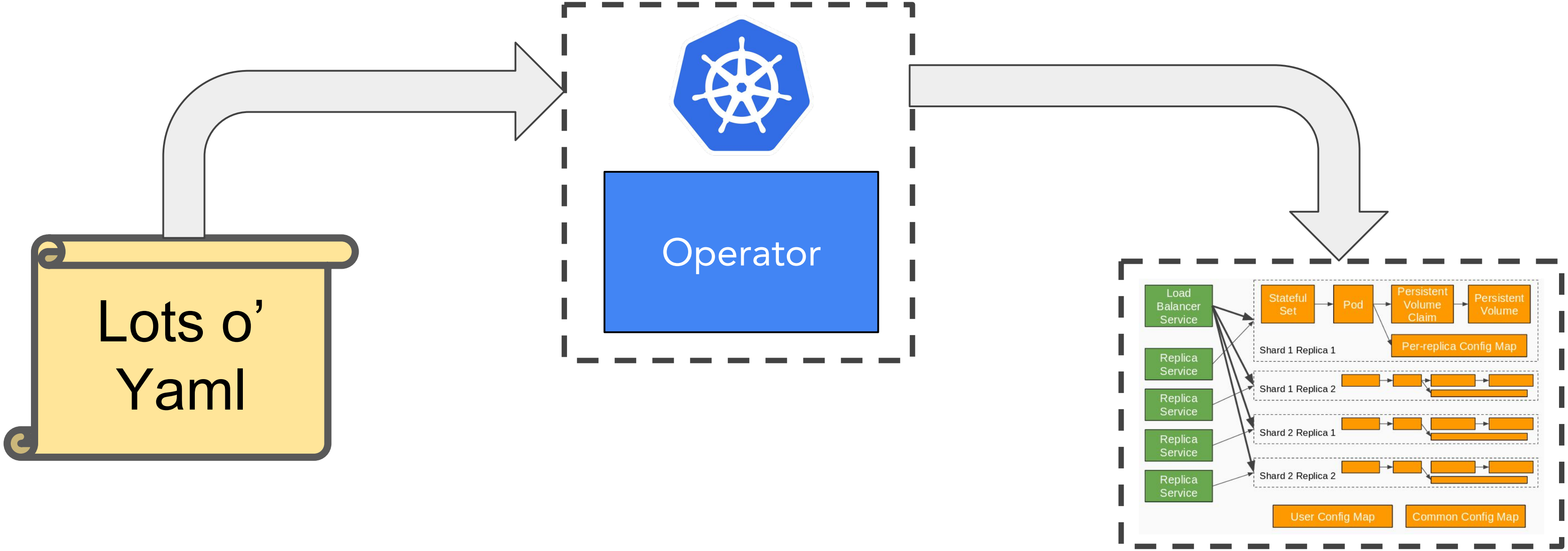
Altinity

ClickHouse support and services including Altinity.Cloud
Authors of Altinity Kubernetes Operator for ClickHouse
and other open source projects

Kubernetes operators make the world a better place



Especially when the world is complicated



Lots o’ Yaml

Operator

Load Balancer Service

Stateful Set

Pod

Persistent Volume Claim

Persistent Volume

Per-replica Config Map

Shard 1 Replica 1

Replica Service

Shard 1 Replica 2

Replica Service

Shard 2 Replica 1

Replica Service

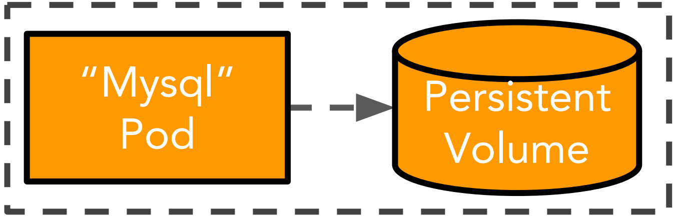
Shard 2 Replica 2

Replica Service

User Config Map

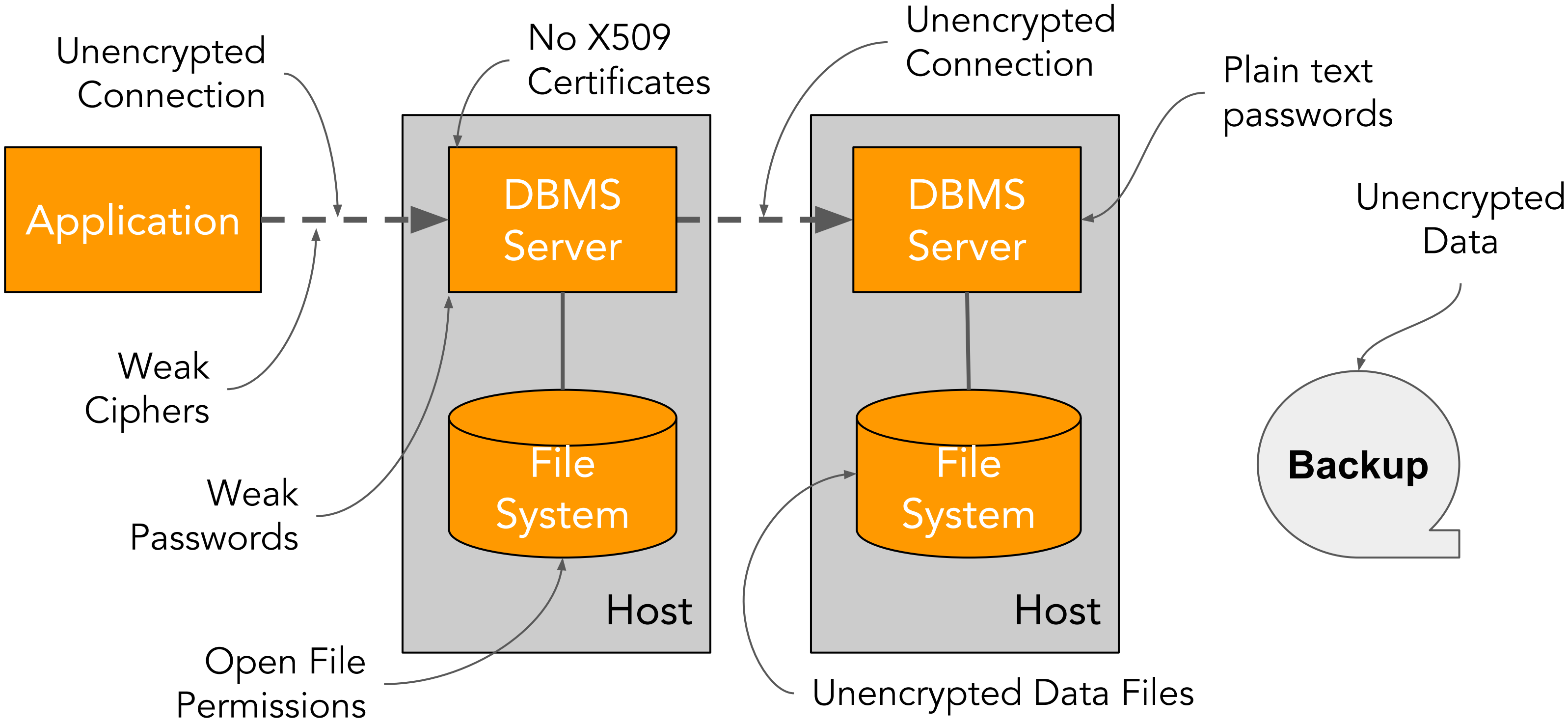
Common Config Map

As they say, every silver lining has a cloud...

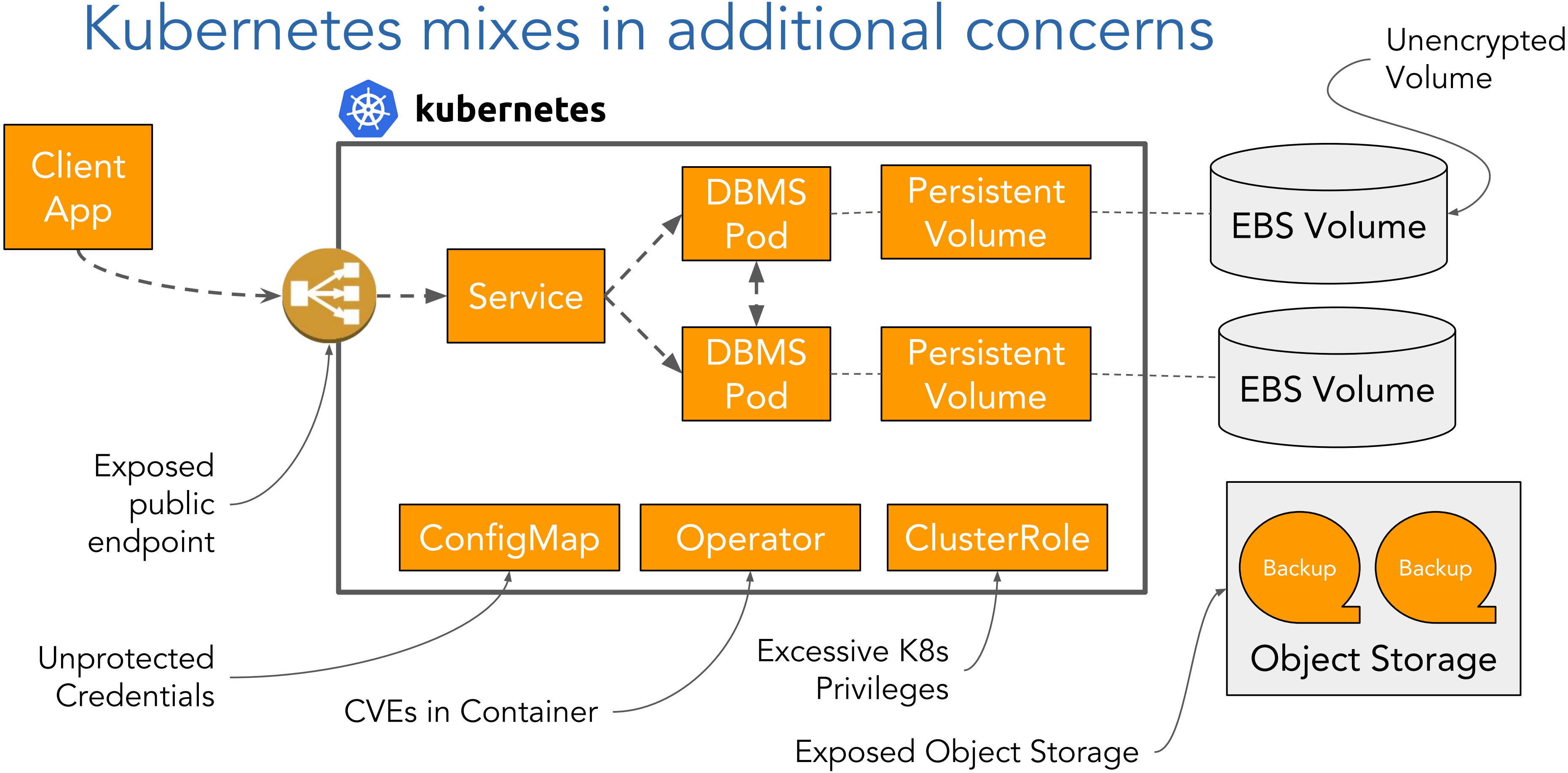


Somebody, somewhere, is trying to steal your data!

A traditional database threat model



Kubernetes mixes in additional concerns



Unencrypted Volume

Exposed public endpoint

Unprotected Credentials

CVEs in Container

Excessive K8s Privileges

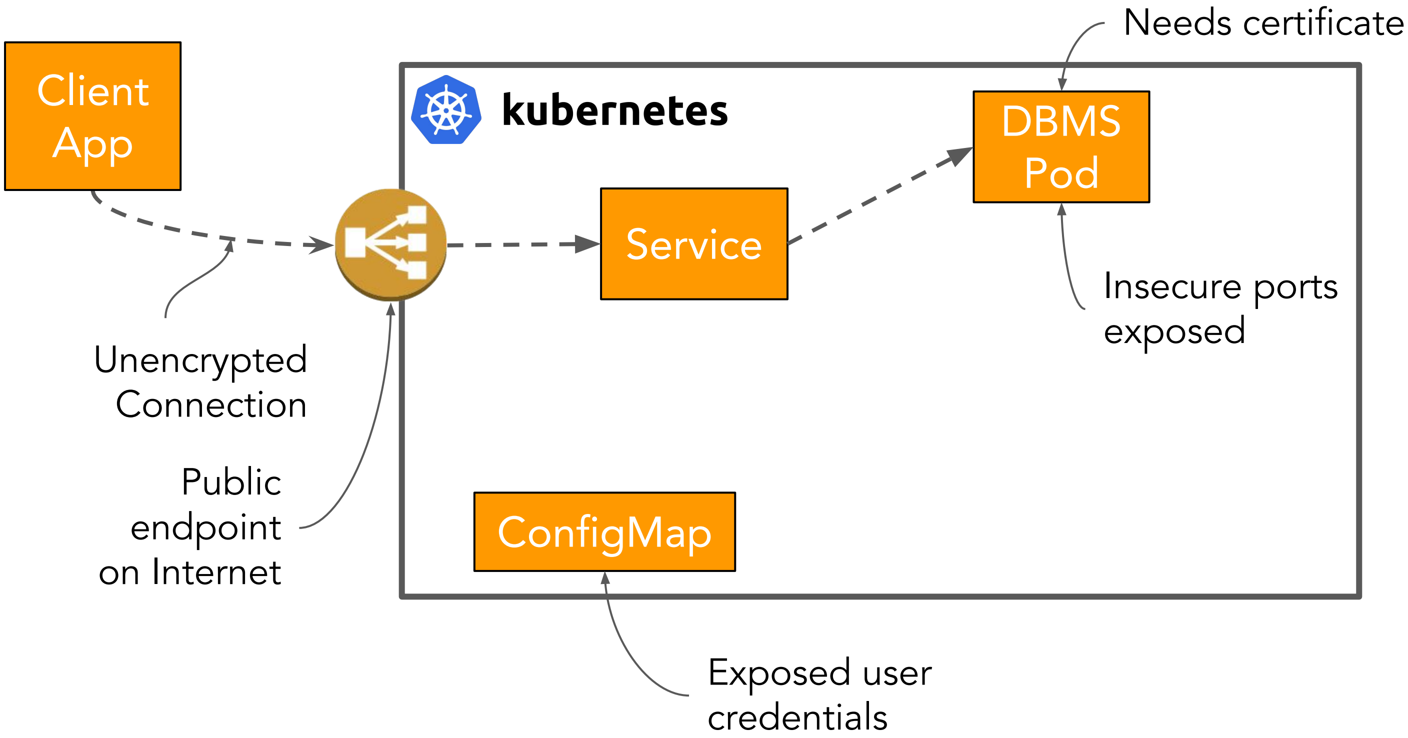
Exposed Object Storage

v0.0.1

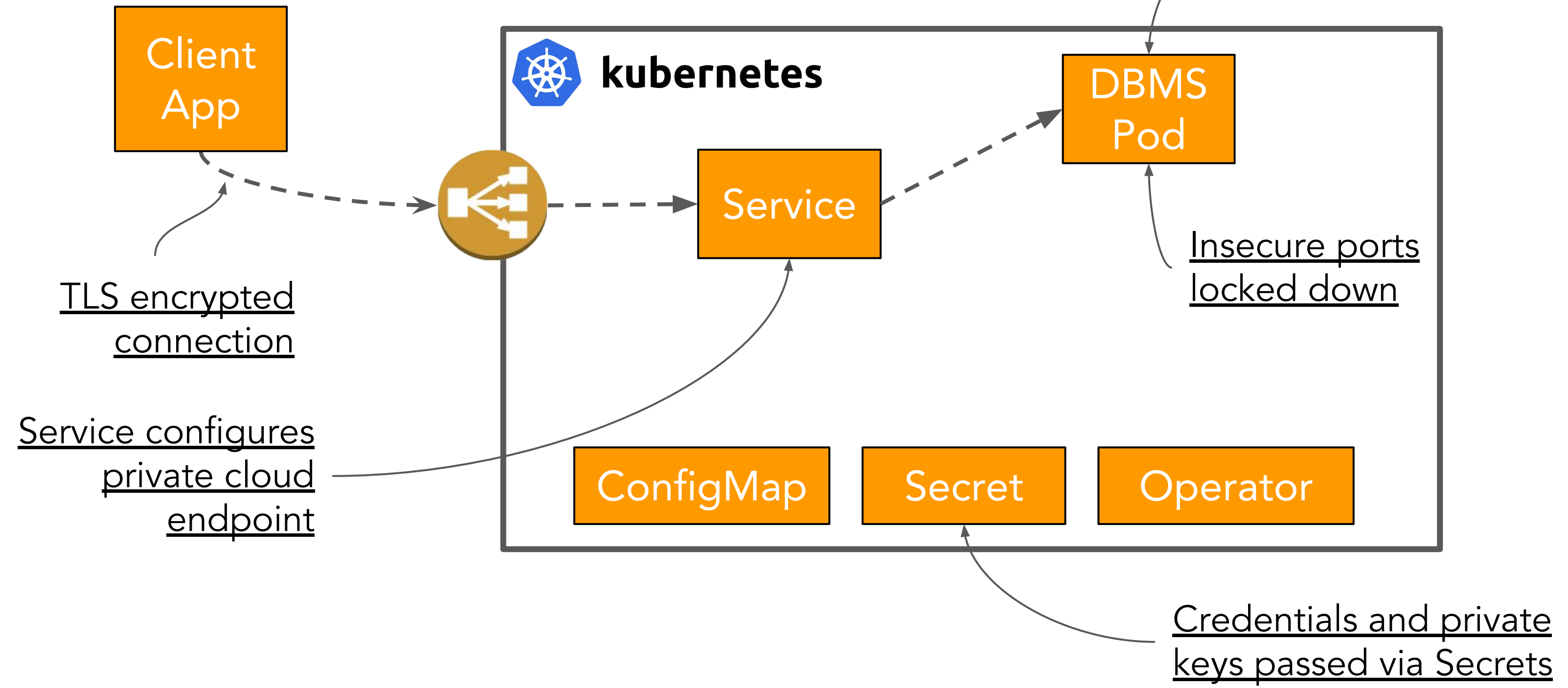
Which leads to a question…

Can operators fix this mess?

Cancerous connectivity



Operator cure for cancerous connectivity



X509 / private key inserted and TLS configured

TLS encrypted connection

Insecure ports locked down

Service configures private cloud endpoint

Credentials and private keys passed via Secrets

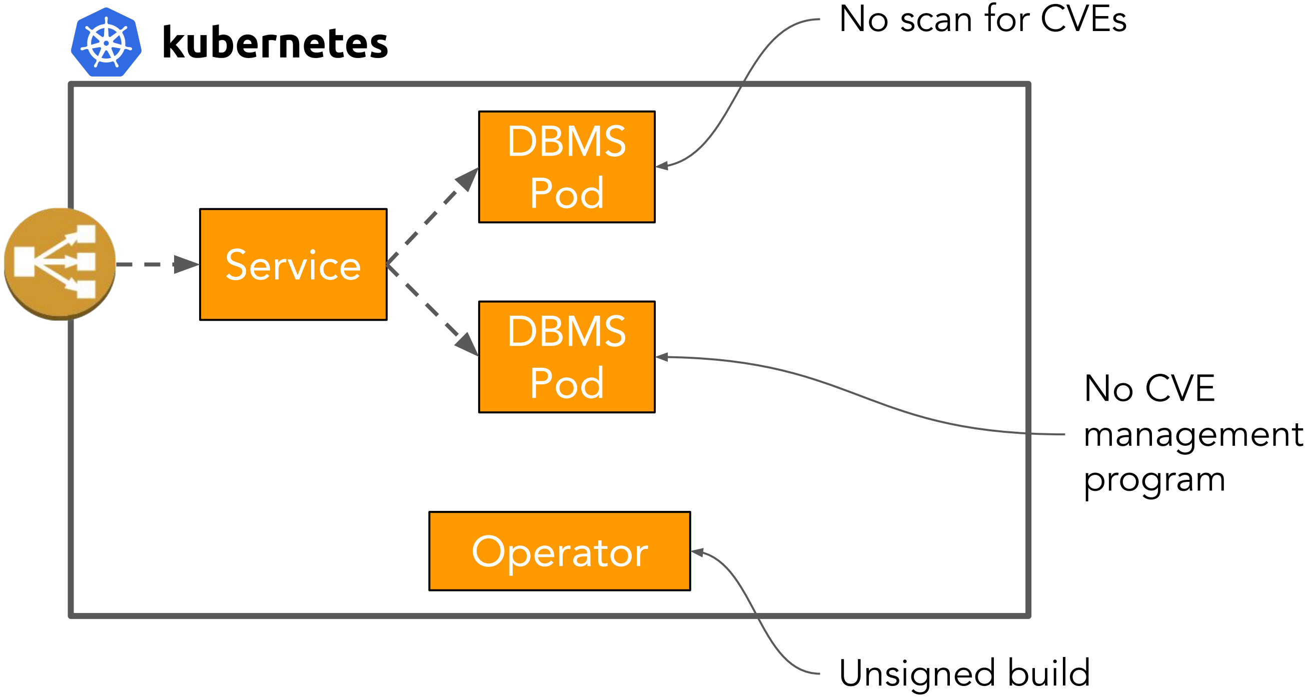
Example of operator networking configuration

```
apiVersion: "clickhouse.altinity.com/v1"
kind: "ClickHouseInstallation"metadata:
  name: "prod"
spec:
  templates:
    serviceTemplates:
      - generateName: clickhouse-{chi}
        metadata:
          annotations:
            service.beta.kubernetes.io/aws-load-balancer-internal: "true"
        name: default-service-template
        spec:
          ports:
            - name: https
              port: 8443
            - name: secureclient
              port: 9440
          type: LoadBalancer
```

Vendor specific config for internal load balancer without public IP address

Only permit secure protocols

Container supply chain chaos

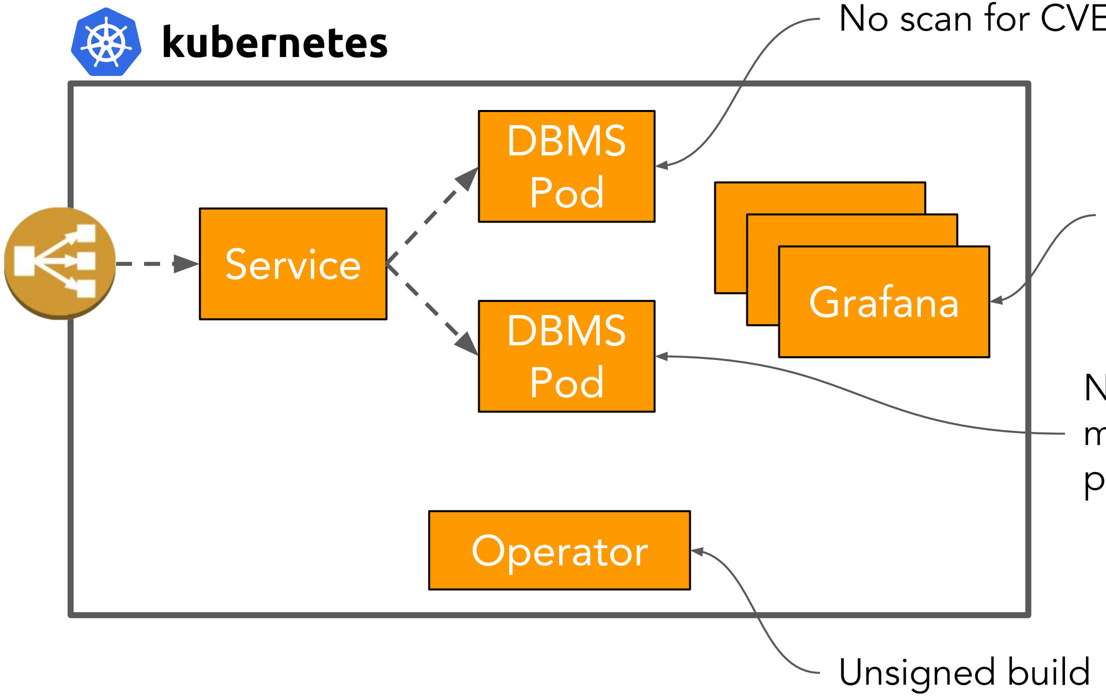


No scan for CVEs

No CVE management program

Unsigned build

More containers equals more chaos…



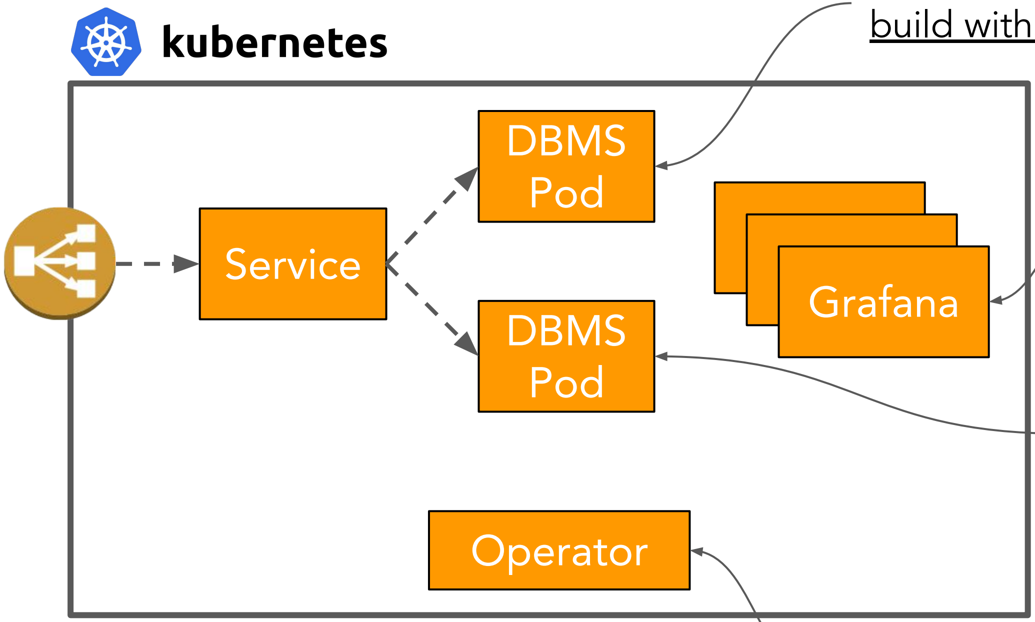
No scan for CVEs

More rando containers for required services

No CVE management program

Unsigned build

Operators can help with supply chain chaos, too



Containers scanned during build with public report

Dependencies also scanned and updated when CVEs appear

CVEs managed and fixed in new releases

Signed builds

Security features to look for in database operators

User Management
Secure `default` accounts
Strong password configuration
Use secrets to pass credentials
Network access restrictions

Data
At-rest volume encryption
File system permissions
Secure logs / event data
Backup encryption

Kubernetes
Minimal ClusterRole privileges
Integration with cluster monitoring

Networking
X509 certificate management
Application TLS configuration
Intra-cluster TLS configuration
Disable insecure ports

Public Cloud Integration
Private network load balancing
Encrypted object / block storage
Cloud IAM account integration

Software Supply Chain
Signed, scanned containers
CVE reporting and fixes
Dependency management

Good documentation == good security

Announcing a new Data on Kubernetes project

DoK Operator Security and Hardening Guide

Goal: Define guidelines for operator security

Audience: Operator producers and consumers

Interested in helping? Get involved!

Join the #sig-operator channel in DoK Slack Workspace

https://github.com/dokc/sig-operator/tree/main/operator-security-hardening

Background information

- Altinity Kubernetes Operator for ClickHouse on GitHub
  - https://github.com/Altinity/clickhouse-operator
  - Operator Hardening Guide
- OWASP Security Guidelines
- Kubernetes docs (https://kubernetes.io/docs/home/)

Thank you!

Any Questions?

Robert Hodges
rhodges at altinity dot com