Automate Kubernetes Workloads with Ansible

Michael Hrivnak

Principal Software Engineer

January, 2019

@michael_hrivnak

redhat.

1. What is Kubernetes

```yaml
apiVersion: v1
kind: Pod
metadata:
  name: example-app
  labels:
    app: example-app
spec:
  containers:
  - name: example
    image: companyname/example:v1.2.0
    ports:
    - containerPort: 8000
```

```yaml
apiVersion: v1
kind: Service
metadata:
  name: example-service
spec:
  selector:
    app: example-app
  ports:
  - protocol: TCP
    port: 80
    targetPort: 8000
```

2. Ansible k8s module

K8s YAML

```
apiVersion: v1
kind: ConfigMap
metadata:
  name: foo
  namespace: default
data:
  color: red
```

Ansible Task

```
---
- name: create foo configmap
  k8s:
    definition:
      apiVersion: v1
      kind: ConfigMap
      metadata:
        name: foo
        namespace: default
      data:
        color: “{{ color }}”
```

Ansible Template

```
---
- name: create foo configmap
  k8s:
    definition: "{{ lookup('template', '/foo.yml') | from_yaml }}"
```

Ansible Role

- Packages related Ansible code for **re-use**
- Create a Role that deploys and manages your application
- Ansible Galaxy: central location to share Roles with the world

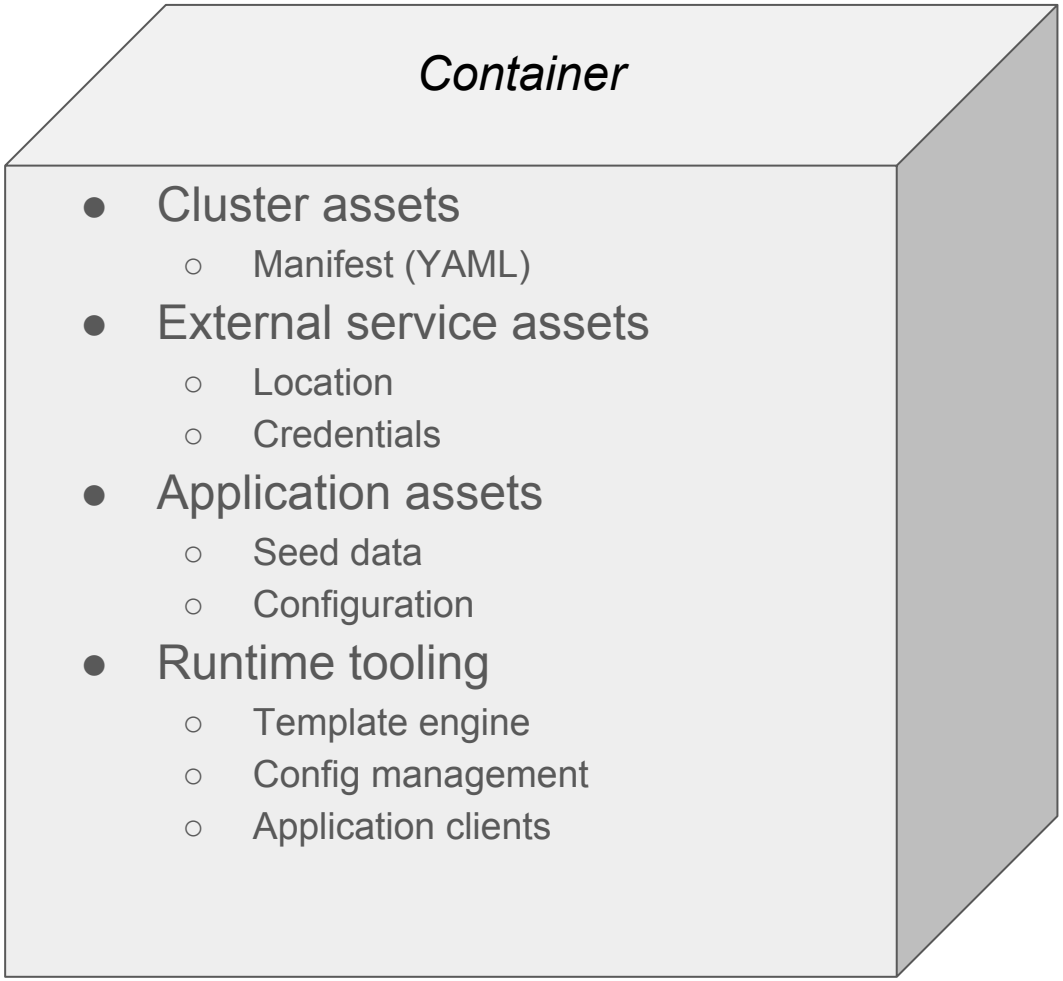
```
memcached/
├── defaults
│   └── main.yml
├── files
├── handlers
│   └── main.yml
├── meta
│   └── main.yml
├── README.md
├── tasks
│   └── main.yml
├── templates
├── tests
│   ├── inventory
│   └── test.yml
└── vars
    └── main.yml
```

3. Ansible Playbook Bundle (APB)

Provisioning

- Create a full stack of cluster resources
  - DB
  - API Service
  - Frontend
- Integrate with external services
  - Legacy applications
  - Traditional DB cluster
  - Appliances
- Post-install bootstrapping
  - Initialize a DB
  - Restore from backup
  - Create resources in the application

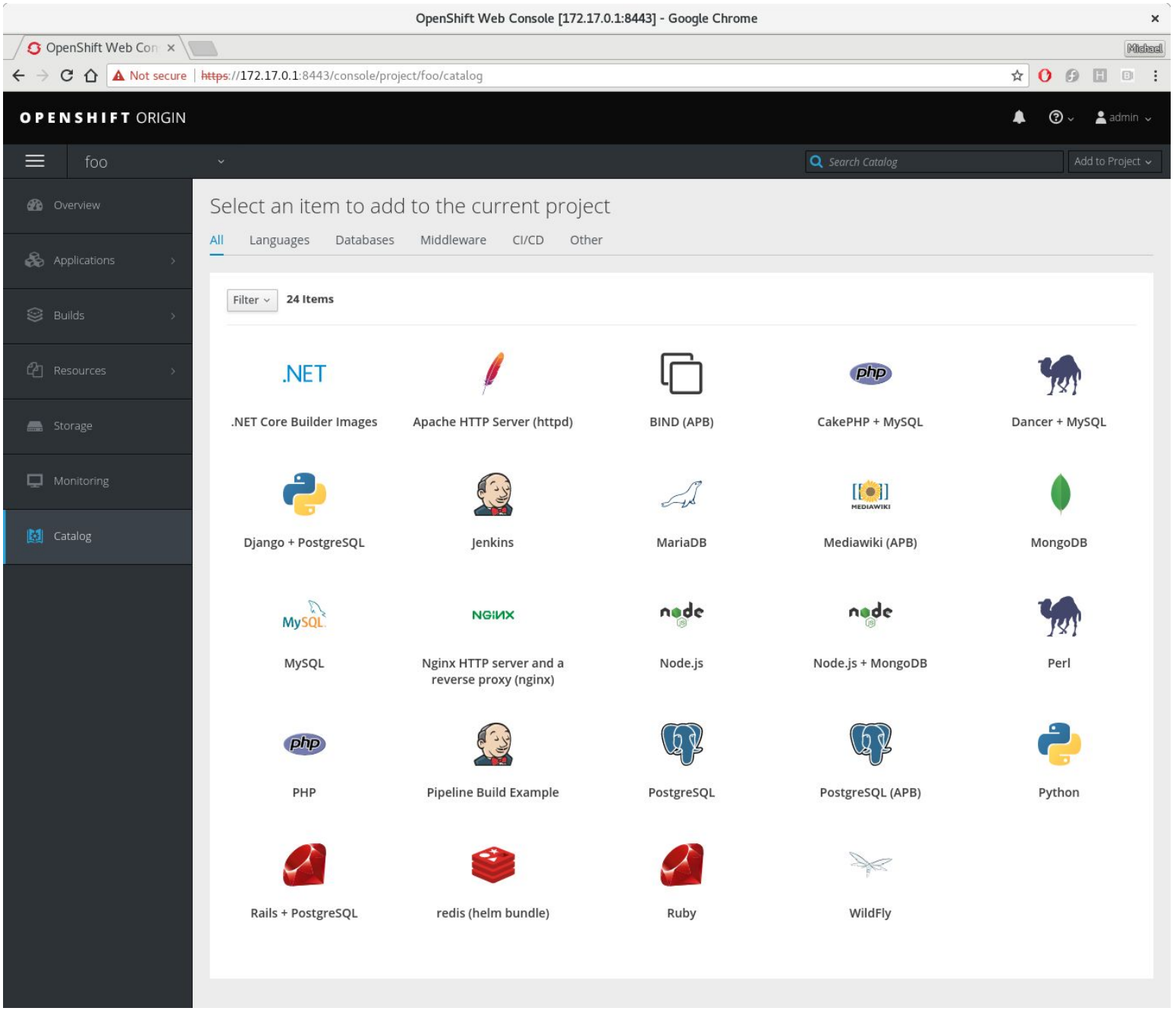
Requirements for Provisioning



Ansible Playbook Bundle

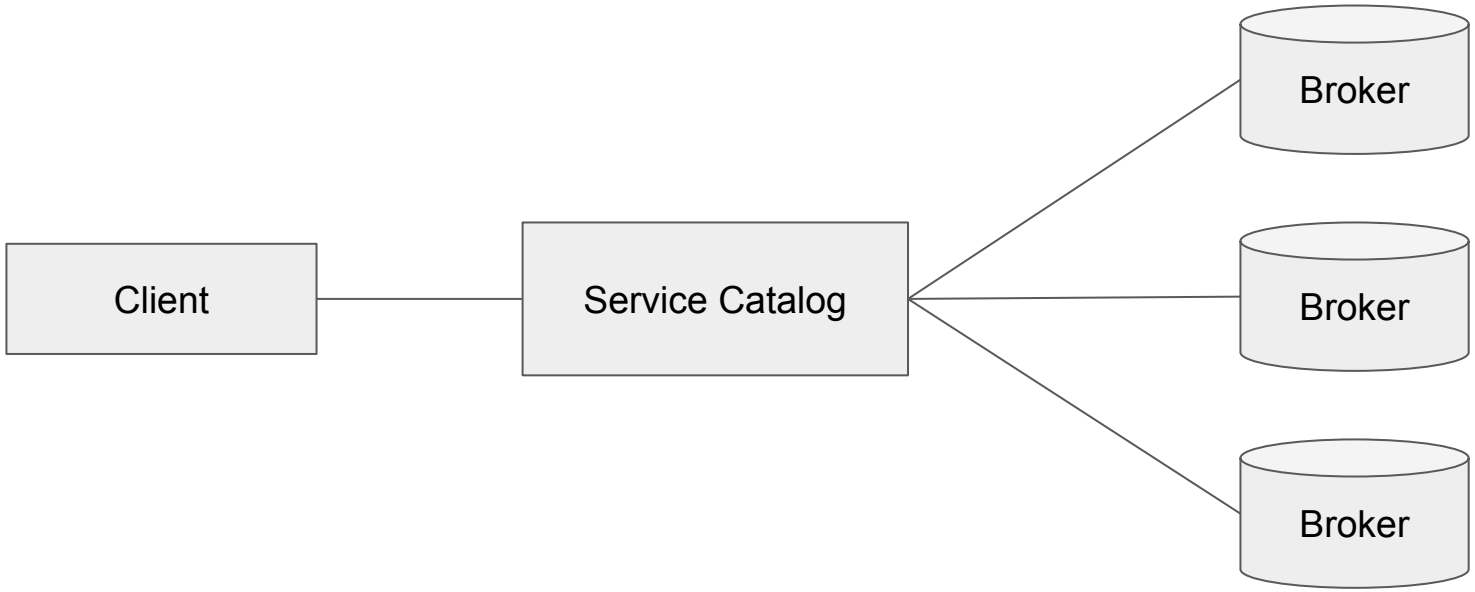
- Bundles everything you need at provision time
- Runs to completion as a pod in your cluster
- Testable and reproducible
  - Suitable for a full CI lifecycle

4. Service Catalog

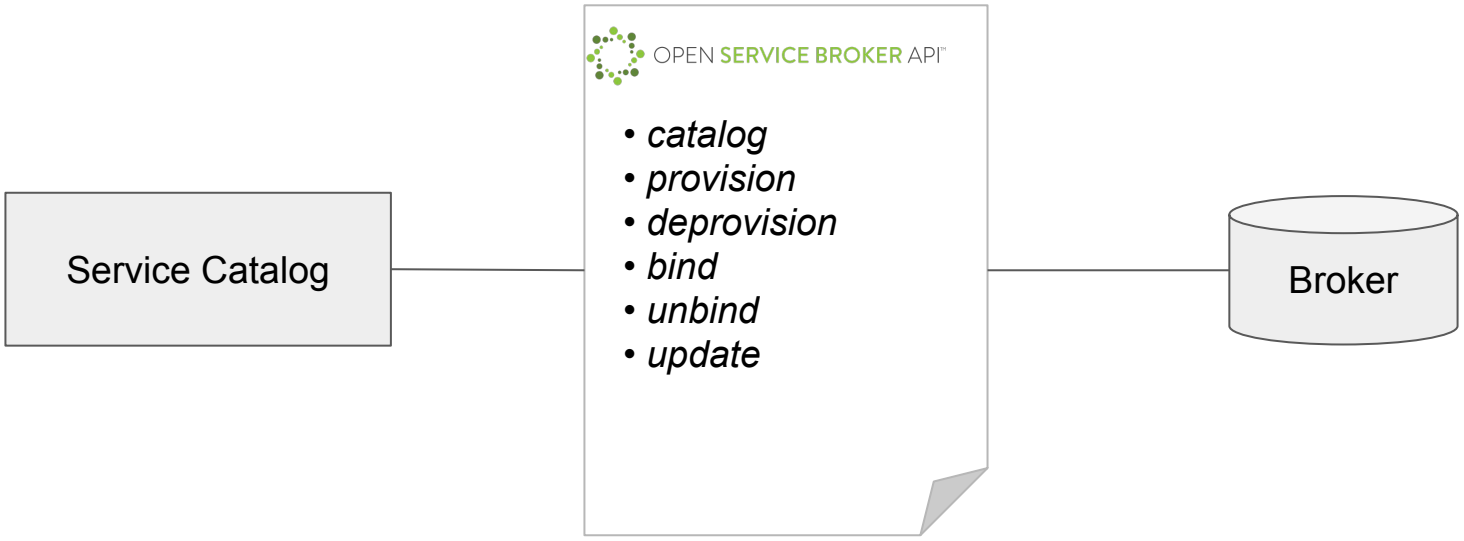

OpenShift Web Console [172.17.0.1:8443] - Google Chrome
OpenShift Web Con
Michael
Not secure | https://172.17.0.1:8443/console/project/foo/catalog
OPENSHIFT ORIGIN
admin
foo
Search Catalog
Add to Project
Overview
Applications
Builds
Resources
Storage
Monitoring
Catalog
Select an item to add to the current project
All
Languages
Databases
Middleware
CI/CD
Other
Filter
24 Items
.NET Core Builder Images
Apache HTTP Server (httpd)
BIND (APB)
CakePHP + MySQL
Dancer + MySQL
Django + PostgreSQL
Jenkins
MariaDB
Mediawiki (APB)
MongoDB
MySQL
Nginx HTTP server and a reverse proxy (nginx)
Node.js
Node.js + MongoDB
Perl
PHP
Pipeline Build Example
PostgreSQL
PostgreSQL (APB)
Python
Rails + PostgreSQL
redis (helm bundle)
Ruby
WildFly

Service Catalog

- Provides composable services to applications
- Actions
  - Provision / Deprovision
  - Bind / Unbind
- Self-service provisioning



OPEN SERVICE BROKER API™





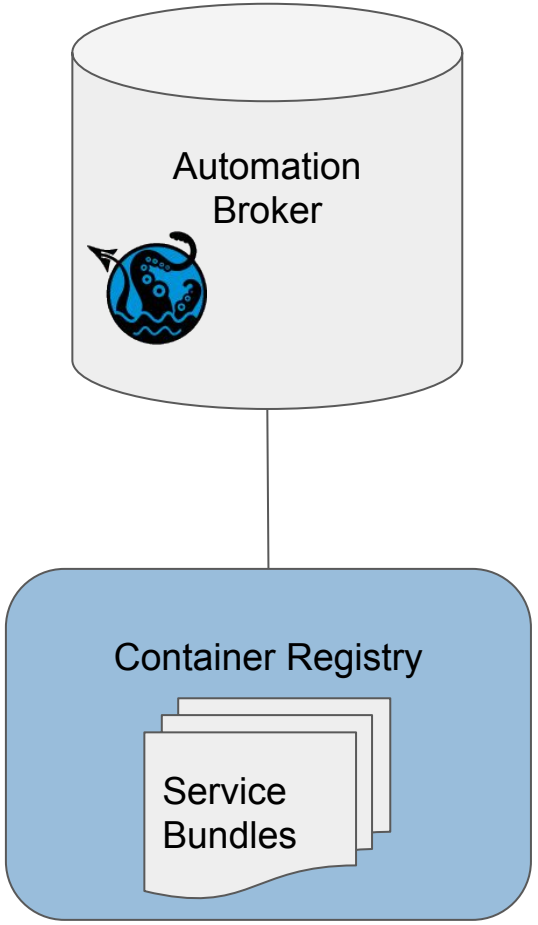



5. Automation Broker

Automation Broker

Service Bundles (APBs)

- Are Catalog entries
- Run to completion for each operation
- Run in a secure sandbox
- Remove need to make your own broker



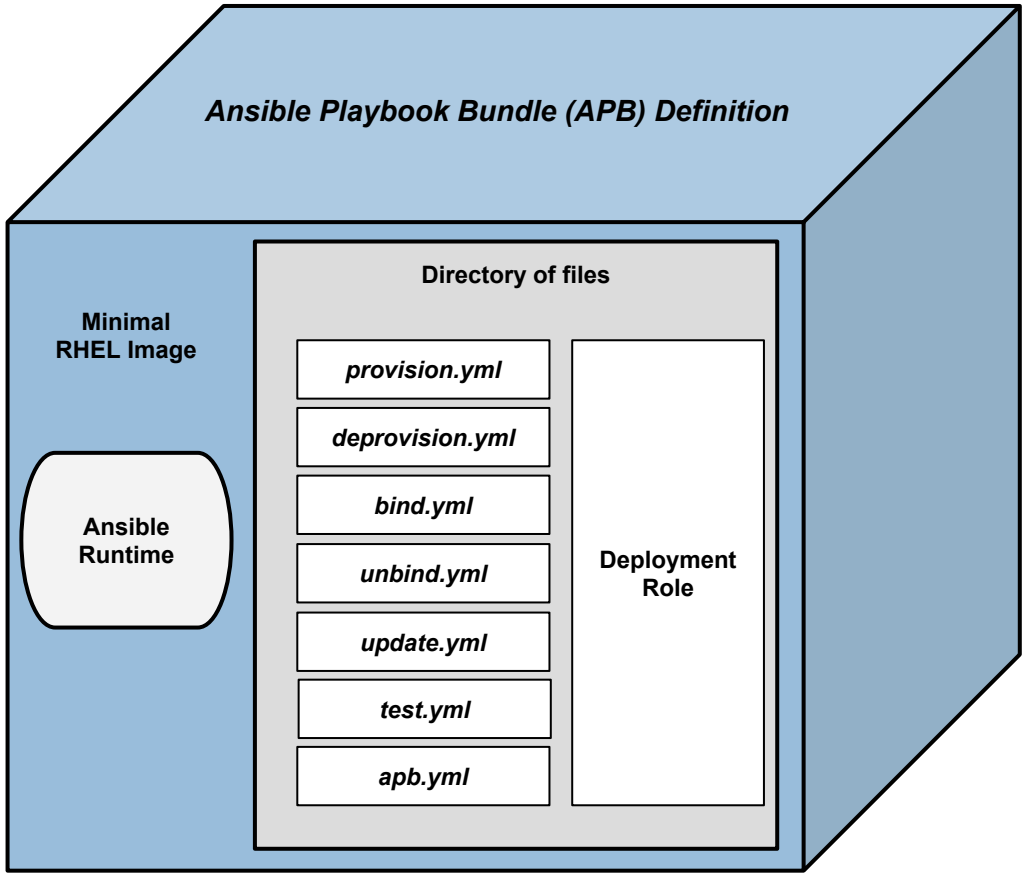
$ apb init lisa

apb.yml

```
version: 1.0
name: lisa
description: This is a sample application generated by apb init
bindable: False
async: optional
metadata:
  displayName: lisa
plans:
  - name: default
    description: This default plan deploys lisa
    free: True
    metadata: {}
    parameters: []
```

Ansible Playbook Bundle (APB) Definition

- Is a Service Bundle
- Ansible runtime
- Playbook per action
- Developer tooling available for simple, guided approach to APB creation
- Easily modified or extended
- Several example APB's available for popular RHSCL services

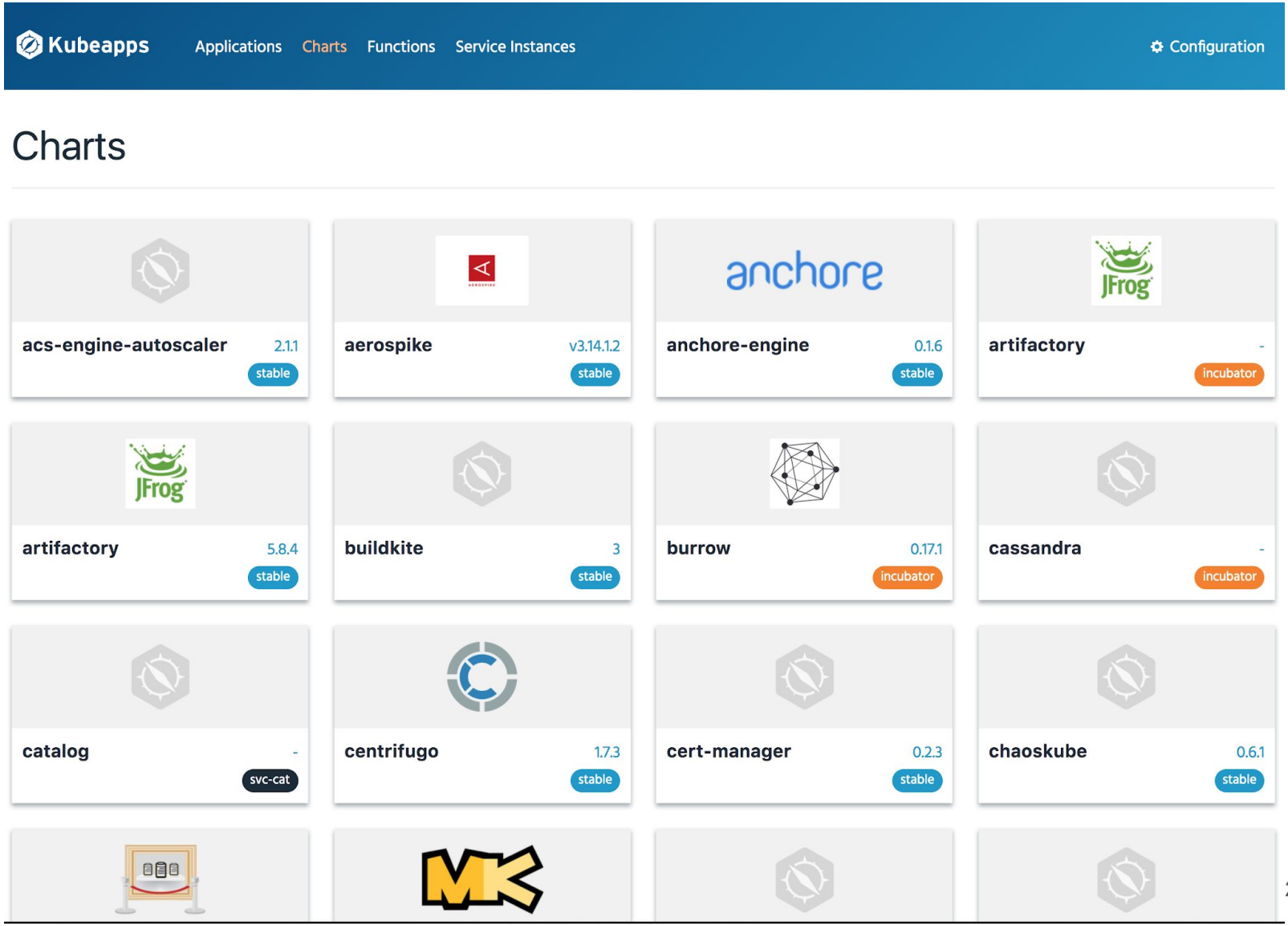


Kubernetes UX

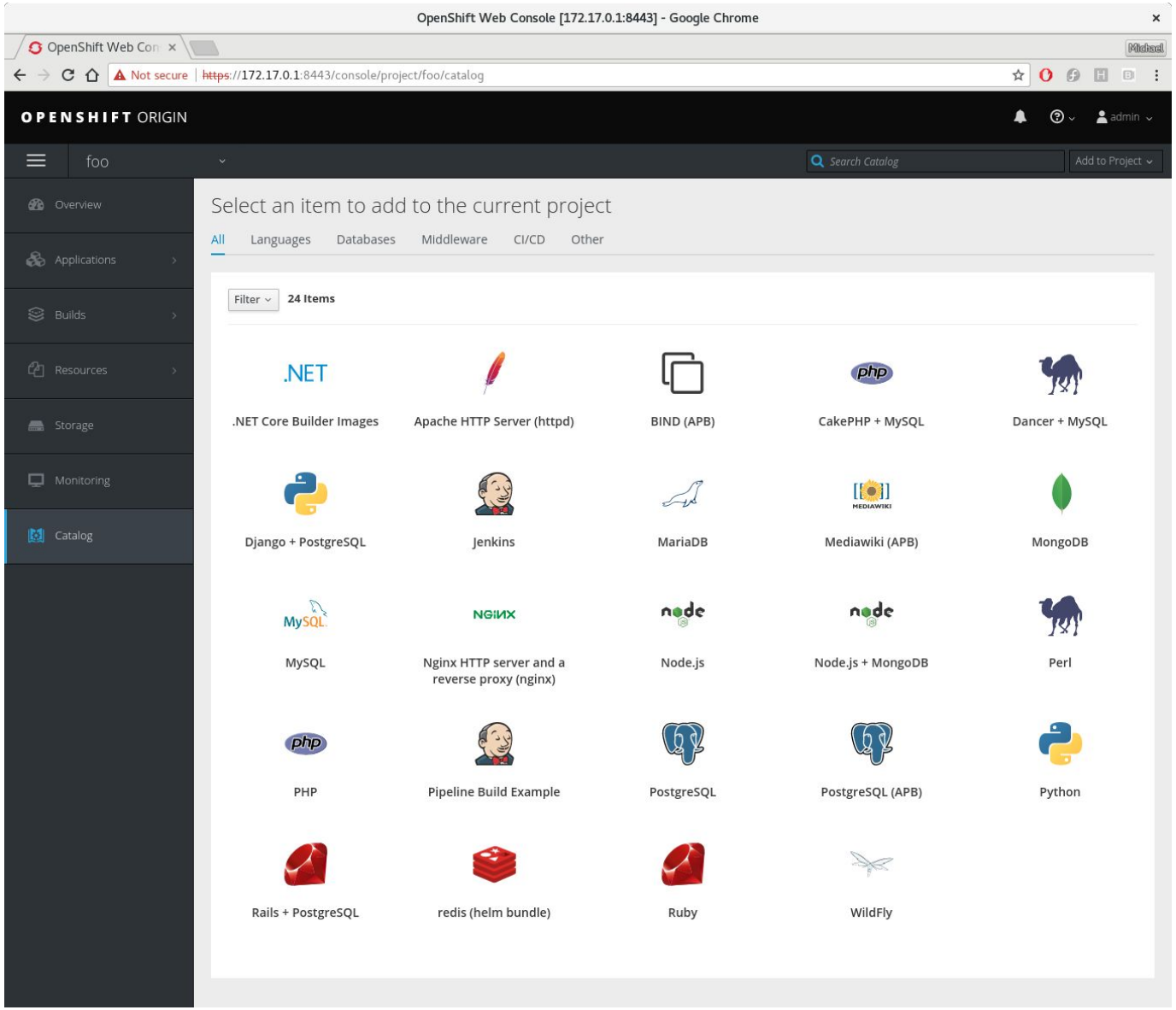
```
$ svcat get classes
```

```
+-------------------------+-----------------------------------------------------------------------------------------------------------+--------------------------------------+
  mysql-persistent          MySQL database service, with persistent storage. For more information                                       f1a201f3-2365-11e8-aa33-68f72877eaca
                            about using this template, including OpenShift considerations, see
                            https://github.com/sclorg/mysql-container/blob/master/5.7/root/usr/share/container-scripts/mysql/README.md.
                             NOTE: Scaling to more than one replica is not supported. You must have persistent volumes available in
                            your cluster to use this template.
  django-psql-persistent    An example Django application with a PostgreSQL database. For more information about using this template,  f1a7745e-2365-11e8-aa33-68f72877eaca
                            including OpenShift considerations, see https://github.com/openshift/django-ex/blob/master/README.md.
  nodejs-mongo-persistent   An example Node.js application with a MongoDB database. For more information about using this template,    f1ab7d00-2365-11e8-aa33-68f72877eaca
                            including OpenShift considerations, see https://github.com/openshift/nodejs-ex/blob/master/README.md.
  jenkins-pipeline-example  This example showcases the new Jenkins Pipeline integration in OpenShift, which performs continuous        f1ae9a44-2365-11e8-aa33-68f72877eaca
                            integration and deployment right on the platform. The template contains a Jenkinsfile - a definition of
                            a multi-stage CI/CD process - that leverages the underlying OpenShift platform for dynamic and scalable
```

Kubeapps


Kubeapps
Applications
Charts
Functions
Service Instances
Configuration
Charts
acs-engine-autoscaler 2.1.1 stable
aerospike v3.14.1.2 stable
anchore-engine 0.1.6 stable
artifactory - incubator
artifactory 5.8.4 stable
buildkite 3 stable
burrow 0.17.1 incubator
cassandra - incubator
catalog - svc-cat
centrifugo 1.7.3 stable
cert-manager 0.2.3 stable
chaoskube 0.6.1 stable

OpenShift UX



Status

- Great path for automated and self-service provisioning that works today.
- Off-cluster integration is the best use case.
- Lacks Day-2 management.
- Operators will take over as the preferred solution.
- Service Catalog will remain part of Kubernetes, and of course OpenShift, for the long term.

6. Operators

What is an Operator?

- Kubernetes Controller
- Deploys and manages an application
- Human operation knowledge in code

Extending the Kubernetes API

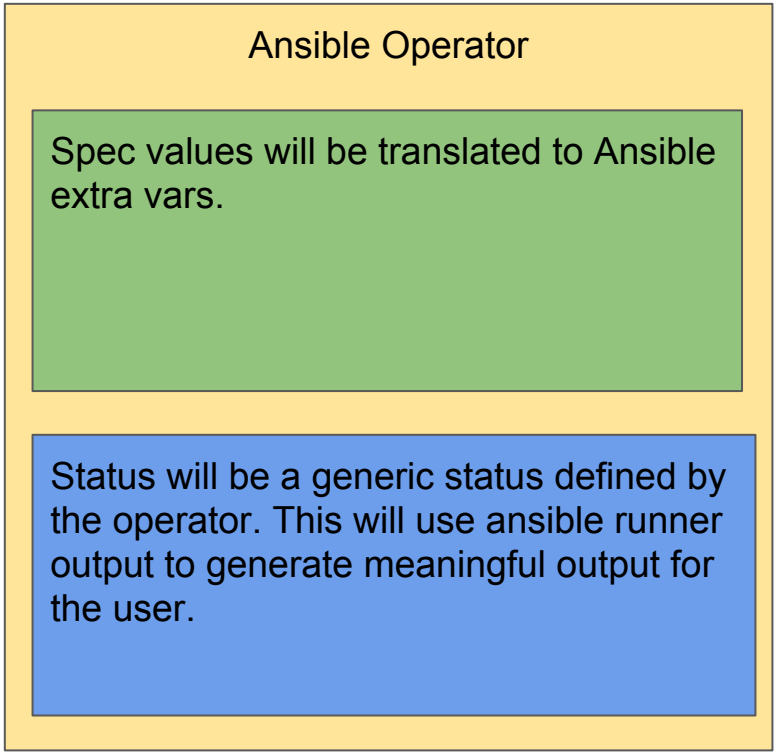
- You can define Custom Resources
- Choose what fields a user can “specify”

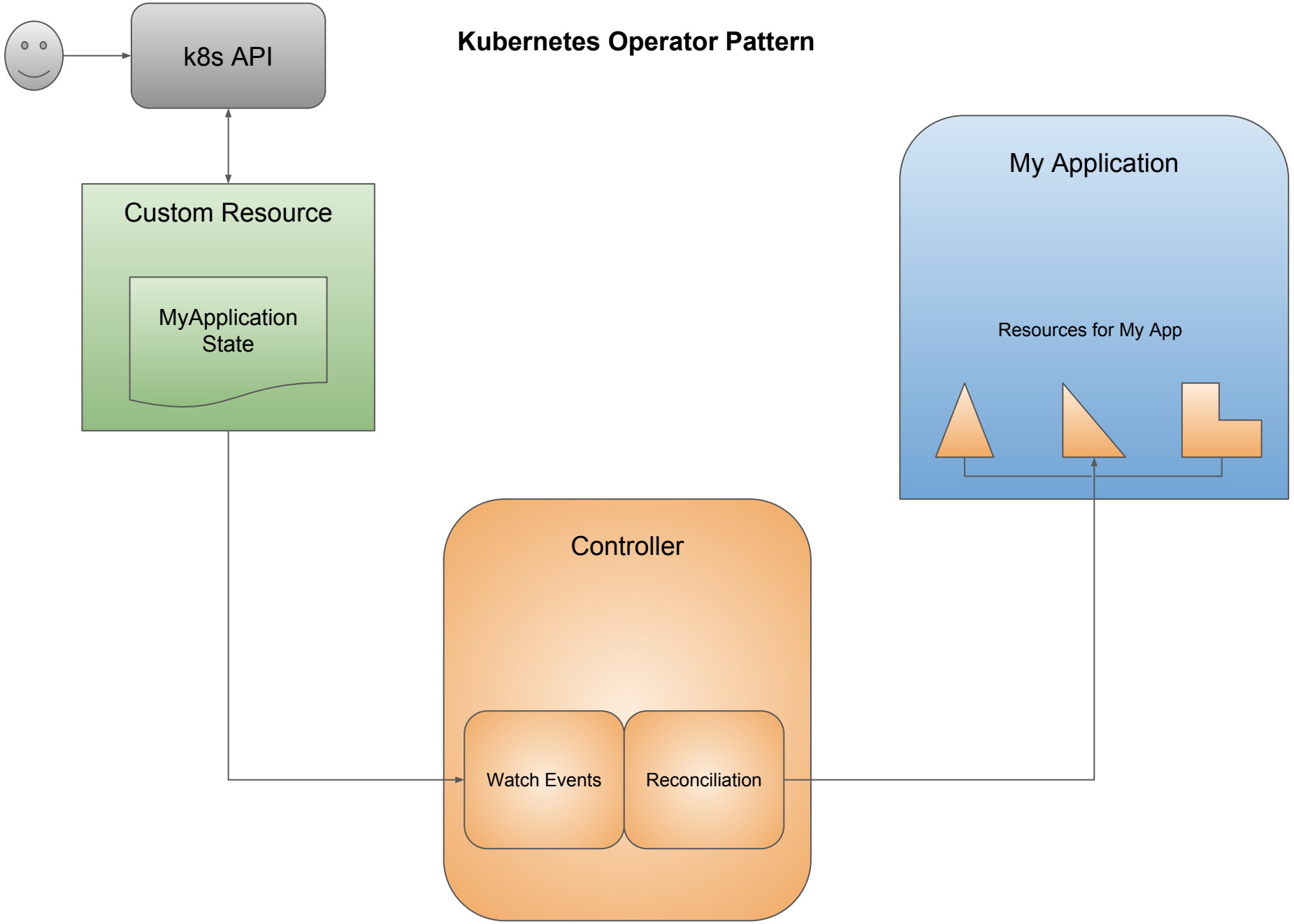
```
apiVersion: cache.example.com/v1alpha1
kind: Memcached
metadata:
  name: example-memcached
spec:
  size: 3
```

Spec To Parameters

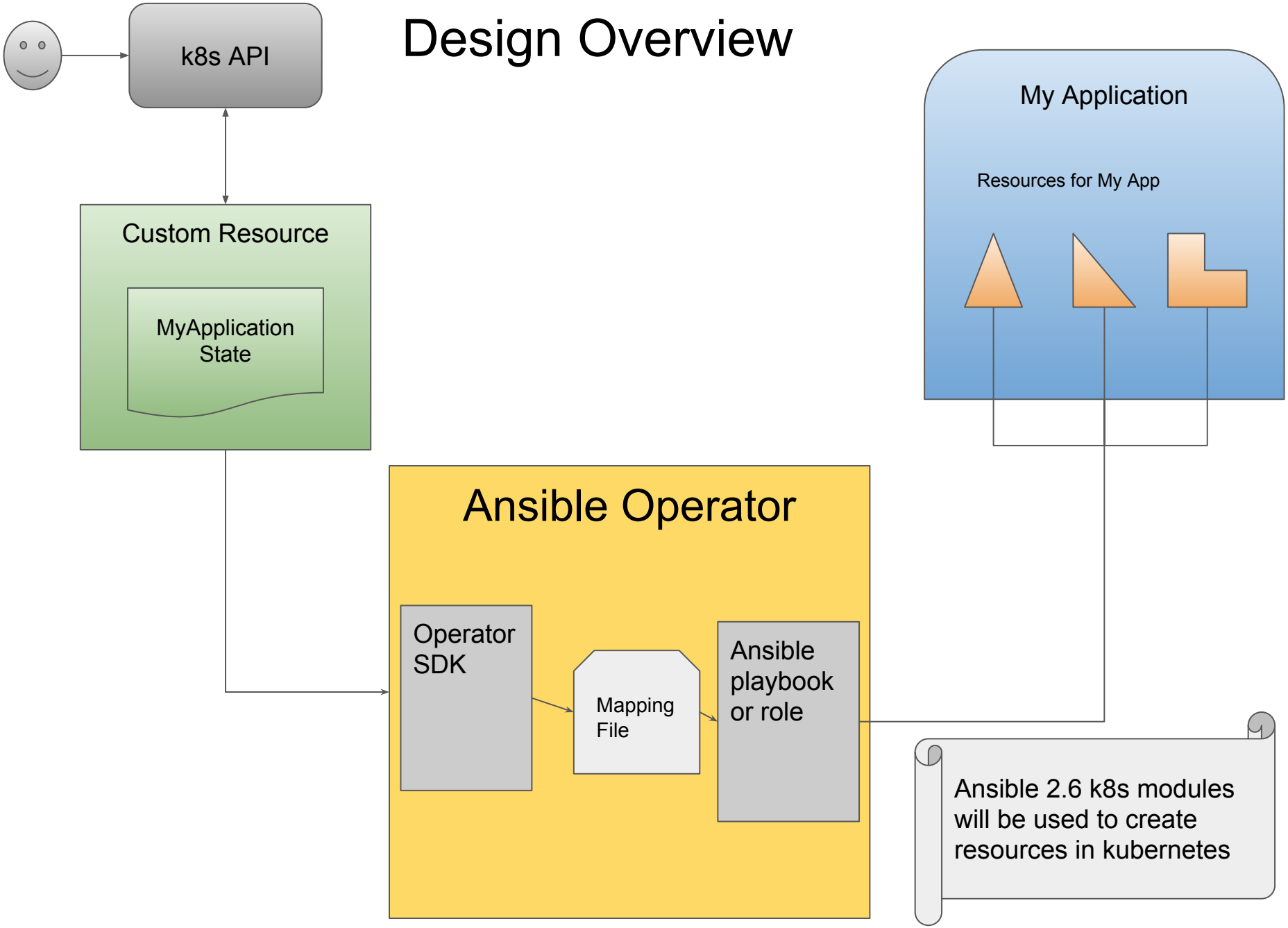
Properly formatted custom resource

```
apiVersion: <Group/Version>
kind: <kind>
metadata:
  name: <name>
spec:
   <key>: <value>
   ….
status:
  <key>: <value>
  ….
```




Kubernetes Operator Pattern
k8s API
Custom Resource
MyApplication State
My Application
Resources for My App
Controller
Watch Events
Reconciliation

Design Overview



watches.yaml

- Maps a Group Version Kind (GVK) to a role or playbook.

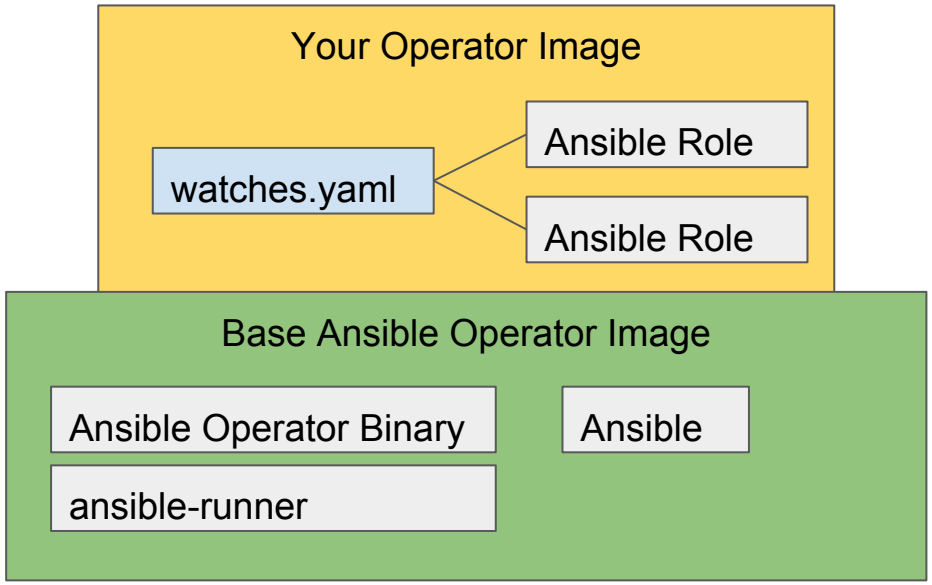
```
# watches.yaml
---
 -  version: v1alpha1
    group: cache.example.com
    kind: Memcached
    playbook: /path/to/playbook
```

- Helps you create an operator
- Write using Go, Ansible, or Helm
- https://github.com/operator-framework/operator-sdk/

Anatomy of Operator Image

From a base Ansible Operator image:

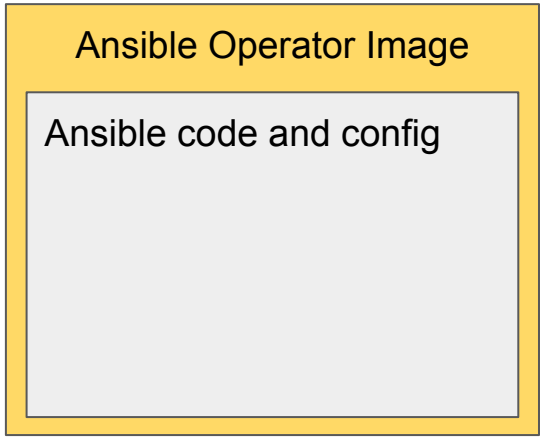
- Add **watches.yaml**, which is a mapping of Group-Version-Kinds to a playbook or role.
- Add one or more **Ansible roles**.

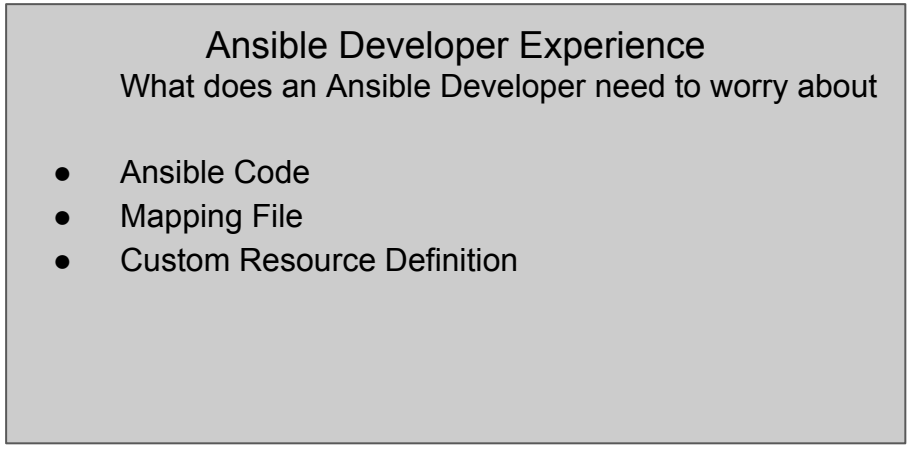


Using Ansible Operator

Use a base Ansible Operator image

- A user will need to add a config file, which is a mapping of Group-Version-Kinds to a playbook or role.
- Ansible operator will manage the watching and reconciliation of the resources by calling roles or playbooks.





https://learn.openshift.com/operatorframework/

Questions?

http://automationbroker.io/
@autom8broker
https://learn.openshift.com/operatorframework/

Michael Hrivnak

@michael_hrivnak