


# Compliant PostgreSQL access management with Kubernetes operators

Cloud Native Aarhus 2020



# Me

Bjørn Hald Sørensen

 @Bjorn\_Sorensen

Web Architect at Lunar since 2017



# Agenda

**Who are we?**

**What and why compliance?**

**The challenge**

**Implementation**

**Who is Lunar?**



**Faster  
Better  
Stronger**

# Facts

**100+**

Employees

**150k**

Users

**~100**

μ services

**25%**

Engineers

**1M+**

Tx pr month

**3**

K8S clusters

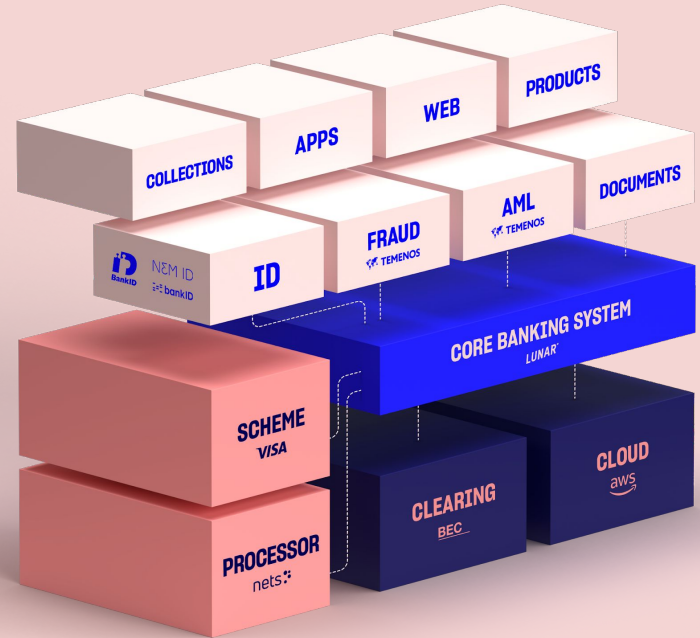
# What and why compliance?

**License to build a  
bank.**

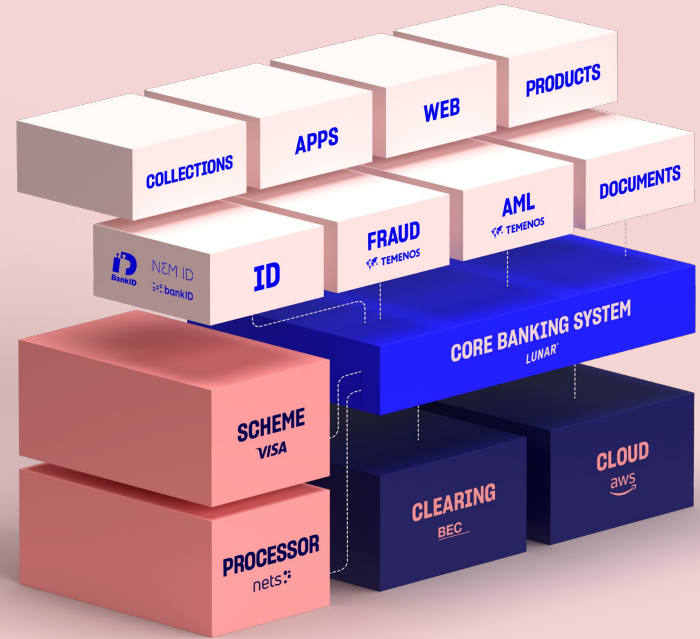




# Building a bank from scratch



# Building a bank from scratch IS HARD





**Compliance is about trust**



**... and technology**





**Looking back**



# The challenge





**Stay safe**





**Be compliant**



**No manual tasks**

**CREATE**

The word 'CREATE' is written in a bold, hand-drawn, sketchy font. Each letter is filled with fine, parallel lines, giving it a textured, three-dimensional appearance. The word is slanted upwards from left to right. At the bottom right, the tip of a pencil is visible, having just finished drawing the final letter 'E'.

**Stay productive**  
**Keep moving**



# Functional requirements

- Create databases
- Create roles for application access
- Create roles for developer access
- Granular access to individual databases
- AWS IAM authentication

# Implementation

CHANGE  
CHANGE  
CHANGE  
CHANGE  
CHANGE  
CHANGE LUNAR®





“Operators are software extensions to Kubernetes that make use of custom resources to manage applications and their components.”

<https://kubernetes.io/docs/concepts/extend-kubernetes/operator/>



## Explore

Topics

Trending

Collections

Events

GitHub Sponsors

#

# operator

★ Star

Here are 381 public repositories matching this topic...

Language: All ▼

Sort: Best match ▼

# Controllers

- **Reconciles state**
- **Interacts with k8s API**

# Operators

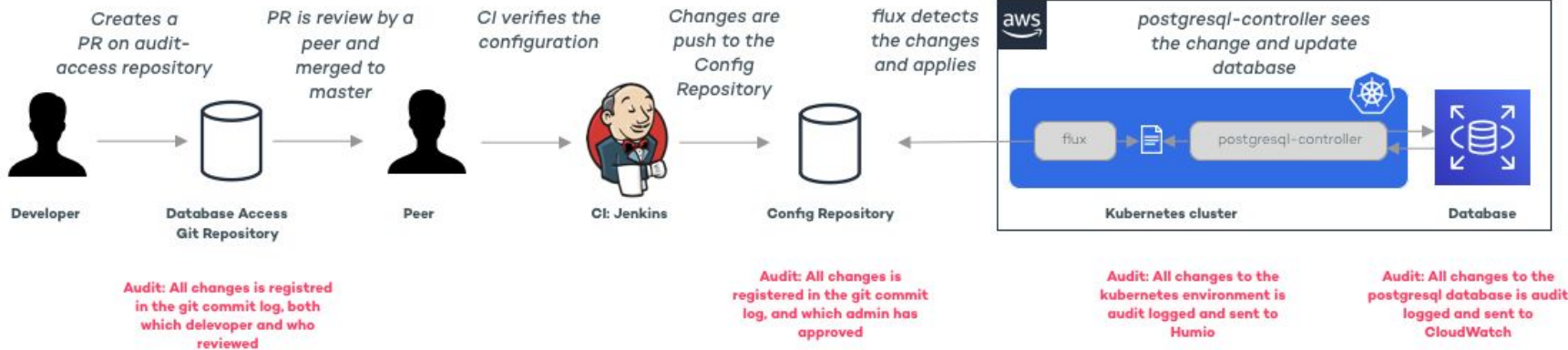
- **Reconciles state**
- **Interacts with k8s API**
- **API extension (CRD)**
- **More domain logic (?)**

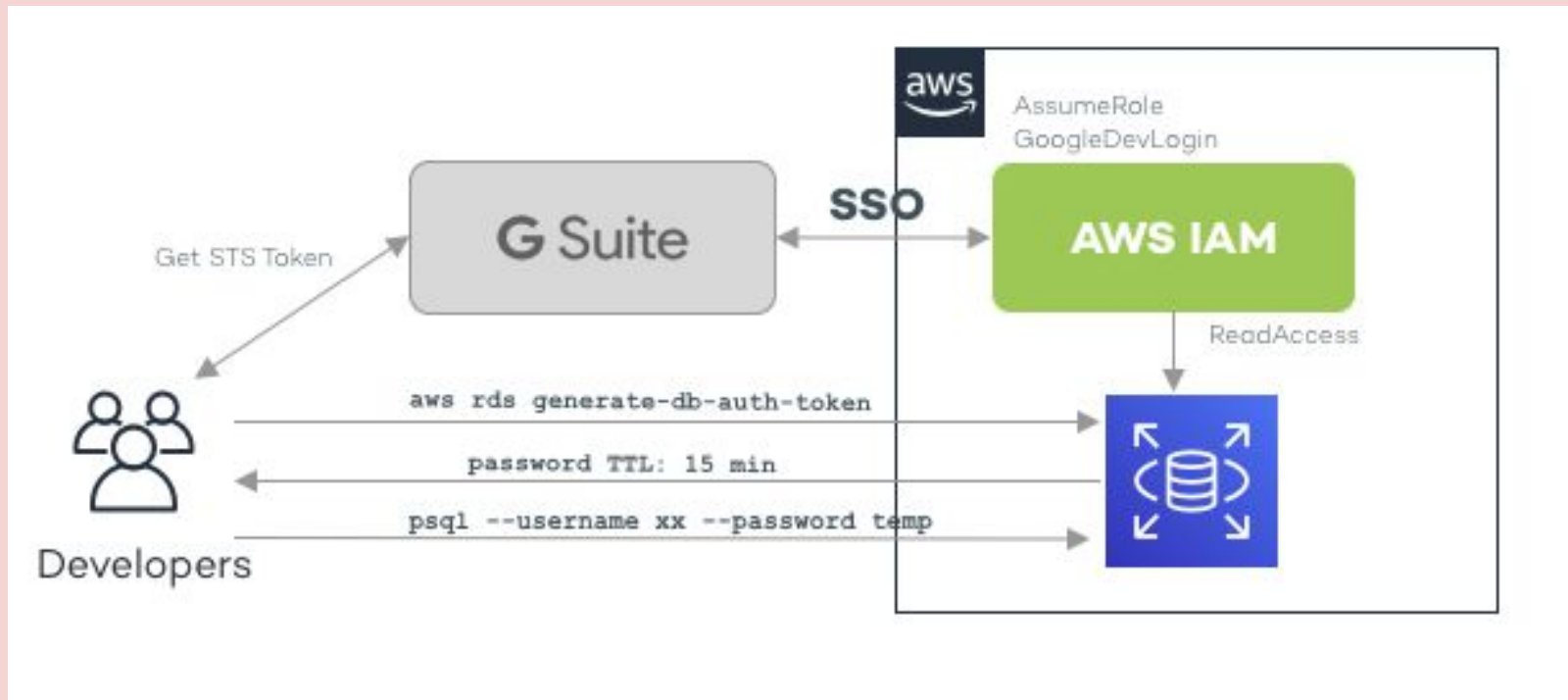


# Reconciliation









# TODO: implement



<https://github.com/operator-framework/operator-sdk>

Developed by CoreOS

- High level APIs and abstractions
- Tools for scaffolding and code generation to bootstrap
- Uses kubernetes-sigs/controller-runtime
- Supports Go, Ansible and Helm implementations



## kubernetes-sigs / kubebuilder

<https://github.com/kubernetes-sigs/kubebuilder>

Developed by Kubernetes' sig-apimachinery

- Tools for scaffolding and code generation to bootstrap
- Implement reconcile loops in controllers and watch additional resources
- Uses kubernetes-sigs/controller-runtime
- Admission and CRD conversion webhooks



## kubernetes / sample-controller

<https://github.com/kubernetes/sample-controller>  
Developed by Kubernetes' sig-apimachinery

- Sample project for copying
- Used as a baseline for kubernetes controllers





```
1 apiVersion: lunarway.com/v1alpha1
2 kind: PostgreSQLDatabase
3 metadata:
4   name: cloud-native-nordics
5 spec:
6   name: cloudbativenordics
7   host:
8     value: postgres.cloudbativenordics.com
9   password:
10    valueFrom:
11     secretKeyRef:
12     key: db.password
13     name: cloud-native-nordics
```

```
1 apiVersion: lunarway.com/v1alpha1
2 kind: PostgreSQLUser
3 metadata:
4   name: developer-bso
5 spec:
6   name: bso
7   read:
8     - allDatabases: true
9     host:
10       value: postgres.cloudnativenordics.com
11     reason: I got a good reason, trust me!
```

```
1 // PostgreSQLUserSpec defines the desired state of PostgreSQLUser
2 // +k8s:openapi-gen=true
3 type PostgreSQLUserSpec struct {
4     Name string `json:"name"`
5     // +listType=set
6     // +optional
7     Read []AccessSpec `json:"read"`
8     // +listType=set
9     // +optional
10    Write []AccessSpec `json:"write"`
11 }
12
13 type AccessSpec struct {
14     Host ResourceVar `json:"host"`
15     // +optional
16     AllDatabases bool `json:"allDatabases"`
17     // +optional
18     Database ResourceVar `json:"database"`
19     // +optional
20     Schema ResourceVar `json:"schema"`
21     Reason string `json:"reason"`
22     // +optional
23     Start metav1.Time `json:"start"`
24     // +optional
25     Stop metav1.Time `json:"stop"`
26 }
```

```
1 func (r *ReconcilePostgreSQLUser) Reconcile(request reconcile.Request)
  (reconcile.Result, error) {
2   var user lunarwayv1alpha1.PostgreSQLUser
3   err := r.client.Get(context.TODO(), request.NamespacedName, &user)
4   if err != nil {
5     if errors.IsNotFound(err) {
6       // Could have been deleted after reconcile request.
7       // Owned objects are automatically garbage collected.
8       reqLogger.Info("Object not found")
9       return reconcile.Result{}, nil
10    }
11    // Error reading the object - requeue the request.
12    return reconcile.Result{}, err
13  }
14
15  // details omitted
16
17  err = r.ensurePostgreSQLRoles(reqLogger, user.Spec.Name, accesses, hosts)
18  if err != nil {
19    return reconcile.Result{}, fmt.Errorf("ensure postgresql roles: %w", err)
20  }
21
22  return reconcile.Result{}, nil
23 }
```



```
lunarway (watch) lunarway (watch) zsh
Every 2.0s: kubectl get po,postgresqldatabase,postgresqluser Bjrns-MBP-3: Wed Feb 19 20:49:06 2020
error: the server doesn't have a resource type "postgresqldatabase"
```

Every 2.0s: kubectl get po,postgreslatabase,postgresluser Bjrns-MBP-3: Wed Feb 19 20:49:53 2020

NAME	READY	STATUS	RESTARTS	AGE
pod/postgresql-68bc6c8fc8-f4xfl	0/1	ContainerCreating	0	8s



```
lunarway (watch) zsh #1 zsh #2 zsh #3 kubectl #4 +
20:56:48 postgresql-controller
cat demo/database.yaml
apiVersion: lunarway.com/v1alpha1
kind: PostgreSQLDatabase
metadata:
  name: cloud-native-aarhus
spec:
  name: cloudnative
  host:
    value: 'postgresql:5432'
  password:
    value: 'password'
20:56:50 postgresql-controller
kubectl apply -f demo/database.yaml
postgresqldatabase.lunarway.com/cloud-native-aarhus created
20:56:57 postgresql-controller
```

Every 2.0s: kubectl get po,postgreslatabase,postgresluser Bjrns-MBP-3: Wed Feb 19 20:51:09 2020

NAME	READY	STATUS	RESTARTS	AGE
pod/postgresql-68bc6c8fc8-f4xfl	1/1	Running	0	84s

NAME	DATABASE	STATUS	UPDATED	HOST
postgreslatabase.lunarway.com/cloud-native-aarhus	cloudnative			

```
lunarway (watch) zsh #1 zsh #2 zsh #3
20:54:36 postgresql-controller
OPERATOR_NAME=postgresql-controller WATCH_NAMESPACE=default go run cmd/manager/main.go \
  --user-roles= \
  --user-role-prefix= \
  --host-credentials-user=postgresql:5432=iam_creator: \
  --host-credentials-database=postgresql:5432=iam_creator: \
  --zap-level \
  --all-databases-enabled-read=true
```

Every 2.0s: kubectl get po,postgreslatabase,postgresluser Bjrn-MBP-3: Wed Feb 19 20:55:20 2020

NAME	READY	STATUS	RESTARTS	AGE
pod/postgresql-68bc6c8fc8-f4xfl	1/1	Running	0	5m35s

NAME	DATABASE	STATUS	UPDATED	HOST
postgreslatabase.lunarway.com/cloud-native-aarhus	cloudnative	Running	11s	postgresql:5432

```
spec:  
  name: bso  
  read:  
    - host:  
      value: postgresql:5432  
      allDatabases: true  
      reason: Cloud Native Aarhus should see this  
  write:  
    - host:  
      value: postgresql:5432  
      database:  
        value: cloudnative  
      schema:  
        value: cloudnative  
      reason: I got the best of reasons
```

```
✓ 20:57:24 postgresql-controller  
kubectl apply -f demo/user.yaml  
postgresqluser.lunarway.com/bso created  
✓ 20:57:28 postgresql-controller
```

Every 2.0s: kubectl get po,postgreslatabase,postgresluser Bjrn-MBP-3: Wed Feb 19 20:57:50 2020

NAME	READY	STATUS	RESTARTS	AGE
pod/postgresql-68bc6c8fc8-f4xfl	1/1	Running	0	8m6s

NAME	DATABASE	STATUS	UPDATED	HOST
postgreslatabase.lunarway.com/cloud-native-aarhus	cloudnative			

NAME	AGE
postgresluser.lunarway.com/bsl	23s

20:58:27 postgresql-controller

psql -hlocalhost cloudnative bso

Pager usage is off.
psql (12.1, server 9.6.5)
Type "help" for help.

cloudnative=> \du

Role name	Attributes	Member of
bso		{cloudnative_read,cloudna
cloudnative	Password valid until infinity	{}
cloudnative_read	Cannot login	{}
cloudnative_readwrite	Cannot login	{}
iam_creator	Superuser	{}
postgres	Superuser, Create role, Create DB, Replication, Bypass RLS	{}

cloudnative=> █

# Thank You!

<https://tech.lunarway.com/blog/>

<https://tech.lunarway.com/talks/>

<https://tech.lunarway.com/opensource/>

<https://go.lunarway.com/postgresql-controller>



**LUNAR<sup>®</sup>**

We are hiring!  
[jobs.lunarway.com](https://jobs.lunarway.com)