

Red Hat

A Case-study On The value of Operators

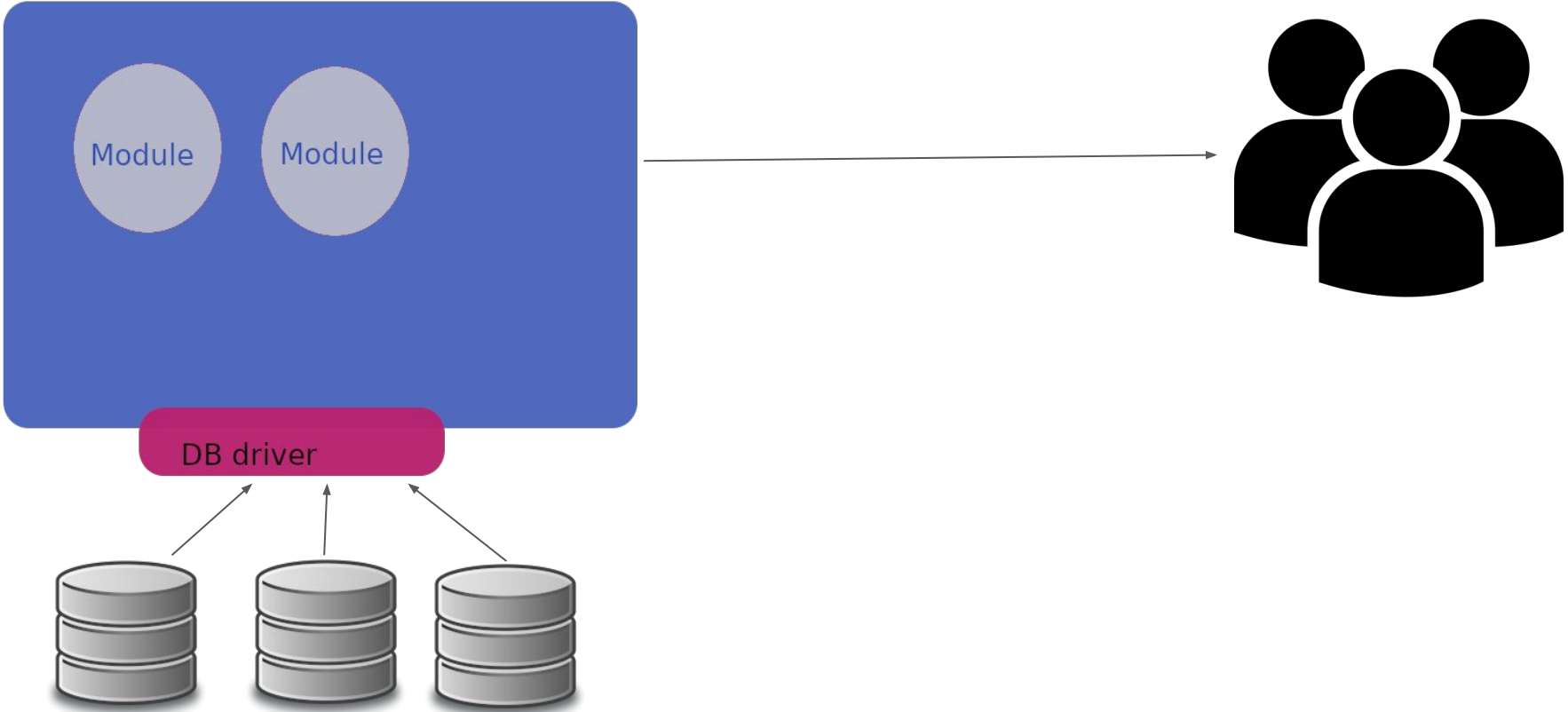
What are Operators?

- Operators provide a way of packaging, deploying and managing Kubernetes applications using software
- Comprises of CRD, a custom controller and operational business logic

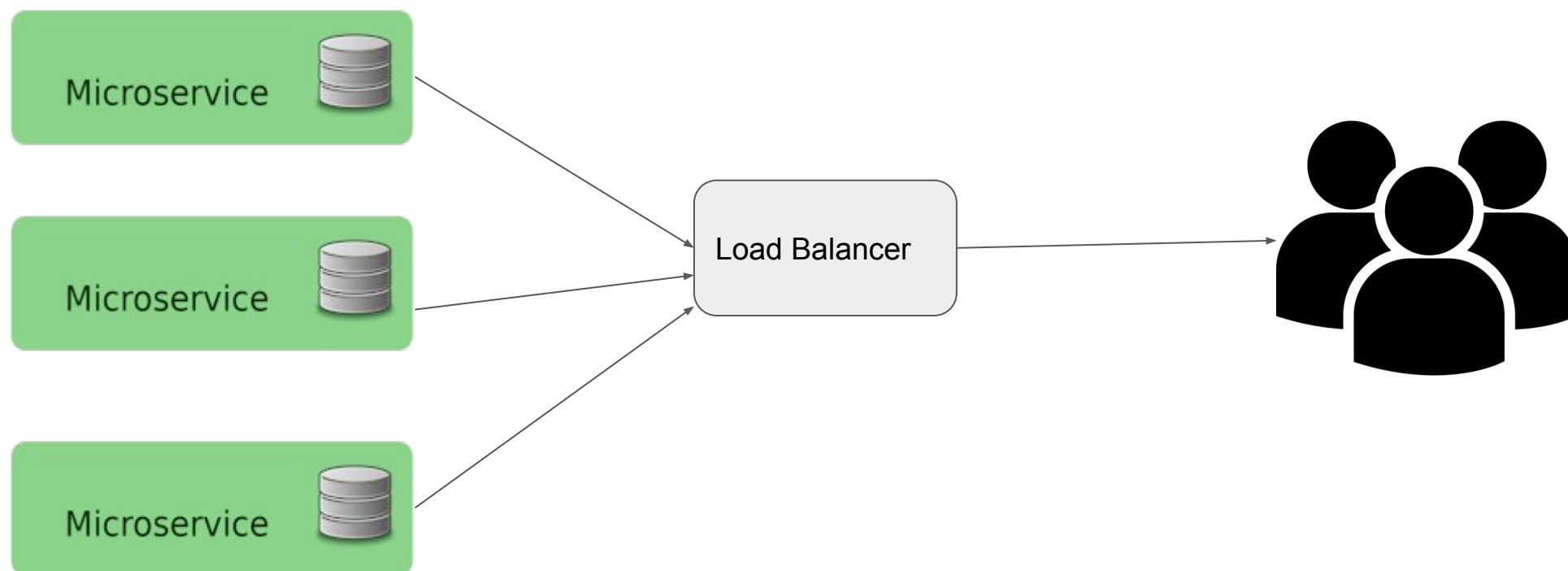


Evolution of Application Architectures

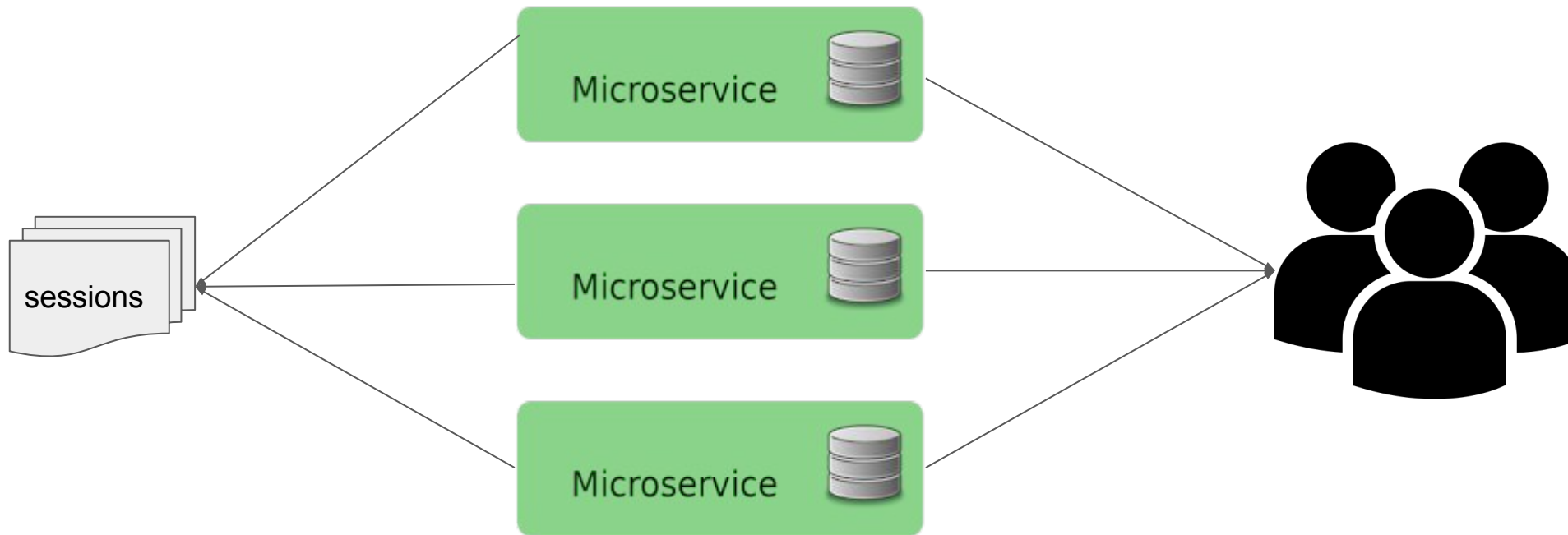
The Monolith



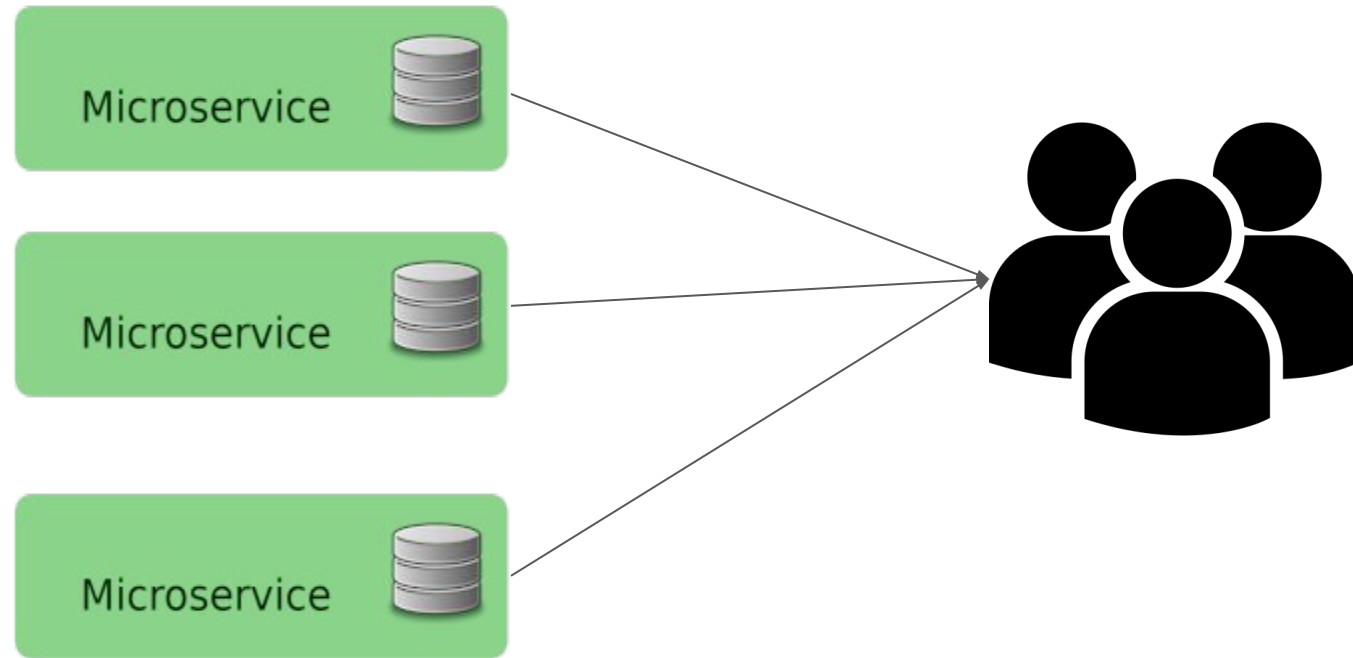
Distributed Session Management



Shared Session Store



Stateless Tokens





A Peek into Doorman (An Auth Microservice)

Scenario

- Picture a company established in the early 2000s is attempting to transform their monolithic application into a set of microservices
- The first phase will involve creating an authentication microservice named, doorman
- The application will be hosted in a Container platform such as Openshift or Kubernetes

Doorman Feature List

- Manage users
- Creating and signing tokens
- Validating tokens

JSON Web Tokens(JWT)

- Pronounced as the English word “jot”
- Is compact and URL safe way to represent claims
- Have three sections - header, claims and signature verification
- Some supported algorithms are:
 - None
 - HMAC (HS256)
 - RSA (RS256)

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWI
iOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG91
IiwiaWF0IjoxNTE2MzE1MDIyfQ.SflKxwRJSMeKK
F2QT4fwpMeJf36POk6yJV_adQssw5c

JWT Header

```
{  
  "alg": "RS256",  
  "typ": "JWT"  
}
```

JWT Claims

```
{  
  "exp": 1571715259,  
  "iat": 1571693659,  
  "id": "cb13924f-e5da-4e5c-b5d3-566ed32faad7",  
  "sub": "Edmund"  
}
```

JWT Signature

- This portion of the JWT is used to determine if the contents of the JWT have been tampered with

HMAC

- Uses a symmetrical algorithm
- Designed to be fast
- Should only be used within the same microservice
- Also susceptible to brute force attacks

RS256 (RSA Key pair)

- Uses an asymmetrical algorithm
- Slower than HMAC
- Secure and can be used across microservices
- Disable HMAC if using RS256 to sign JWT tokens

```
verifyKey, err := jwt.ParseWithClaims(jwtString, &MyClaims{},
    func(token *jwt.Token) (interface{}, error) {
    if token.Method.Alg() != "RS256" {
        return nil, errors.New("Unsupported signing key")
    }
    ...
})
```

200 OK

138.99 ms

DETAILS ^

POST http://localhost:5000/user/login

Response headers **3**

Request headers **1**

Redirects **0**

Timings

```
content-type: application/json
date: Fri, 25 Oct 2019 14:52:57 GMT
content-length: 860
```



```
{
  "token": "eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJleHAiOiJlNzIwMjIzZmFhZDciLCJzdWIiOiJFZG11bmQifQ.PWHG5IUC
FDJZ-vH0ujxJ-jdKlaEXVquk050Qf-_steTeNTVrQ0KHZfEGgtyrg0kk0EzGd50k-
UURpx9ANcjF8prfegI_TxpIgdWfylnāM1cVmUEIjJDi1SZFN0t7M97q05_d1P8t0uleZDdZJGkvaR8R4nFH1Dkgse-
Rdb782WpMYE4t6-sIj089ZFevM5REAIWmor0hhf0KuP3ExokS8kYTDS9qYSRv20Q-
UKbFD0dRHMSmSR78WjPRFwaKrV5rj-XXj0cp865-
6MFQzQtkmK_m86rLQkrNuoWJyBfShMLTBppsZBdfIT7FssZeiKLRyfkxxvKY6FBed_KnYW3bM3JjVNzj7lgXwRv6WTa
dFvDCJ5gavMi7i5_9qPPiDWMhozeqbuBKFBq-fLpiL_pnC93G0JckvMPUrsRKnBIhxl_m6t-T8s4txo8Vfzg6AUXjv-
a0xpmLqpkHMq29L98499IVoThgvJfp5CFd5uRh0AvVou-UjYBoK97JcRF0cZ0P5b0qqiE20119rU-
kLYFoX93gg5hyKNVbfUP9amRkJUg4pYvB_-
fWX4CYqF673Lzg4xr2Nrd3BTI7S7NE7bJvPp7oMYXPawd0wjH1pPbsz8IKrbi5Fv0w552PgHydkBe70GGhb4HKTW0gA
7ar2gd0eCX4mXkbR491JSaNri2PM"
}
```

200 OK 6.33 ms

DETAILS ^

GET http://localhost:5000/users/list

Response headers 3

Request headers 2

Redirects 0

Timings

```
content-type: application/json
date: Fri, 25 Oct 2019 14:58:17 GMT
content-length: 287
```



```
[Array[2]]
  -0: {
    "id": "2019-09-14 21:09:54",
    "created_at": "cb13924f-e5da-4e5c-b5d3-566ed32faad7",
    "firstname": "Edmund",
    "lastname": "Ochieng",
    "username": "eochieng"
  },
  -1: {
    "id": "2019-10-24T04:29:42Z",
    "created_at": "64dac74c-4aa6-4b59-a16b-4e128bff0fa9",
    "firstname": "Jane",
    "lastname": "Doe",
    "username": "jane.doe"
  }
}
```



Database Design

- Data security
- Scalability
- Client library support
- Performance
- Data replication
- High-availability
- Resilience

Persistent Volumes

- This volume would be required to store persistent data from the micro-service
- Data that should be retained long-term should not be installed within a container

Technical resources involved

- Database Administrators to review database design and tuning
- Network engineers/Security engineers to ensure application is secure
- Cloud Operations/Engineering team
- Backup team



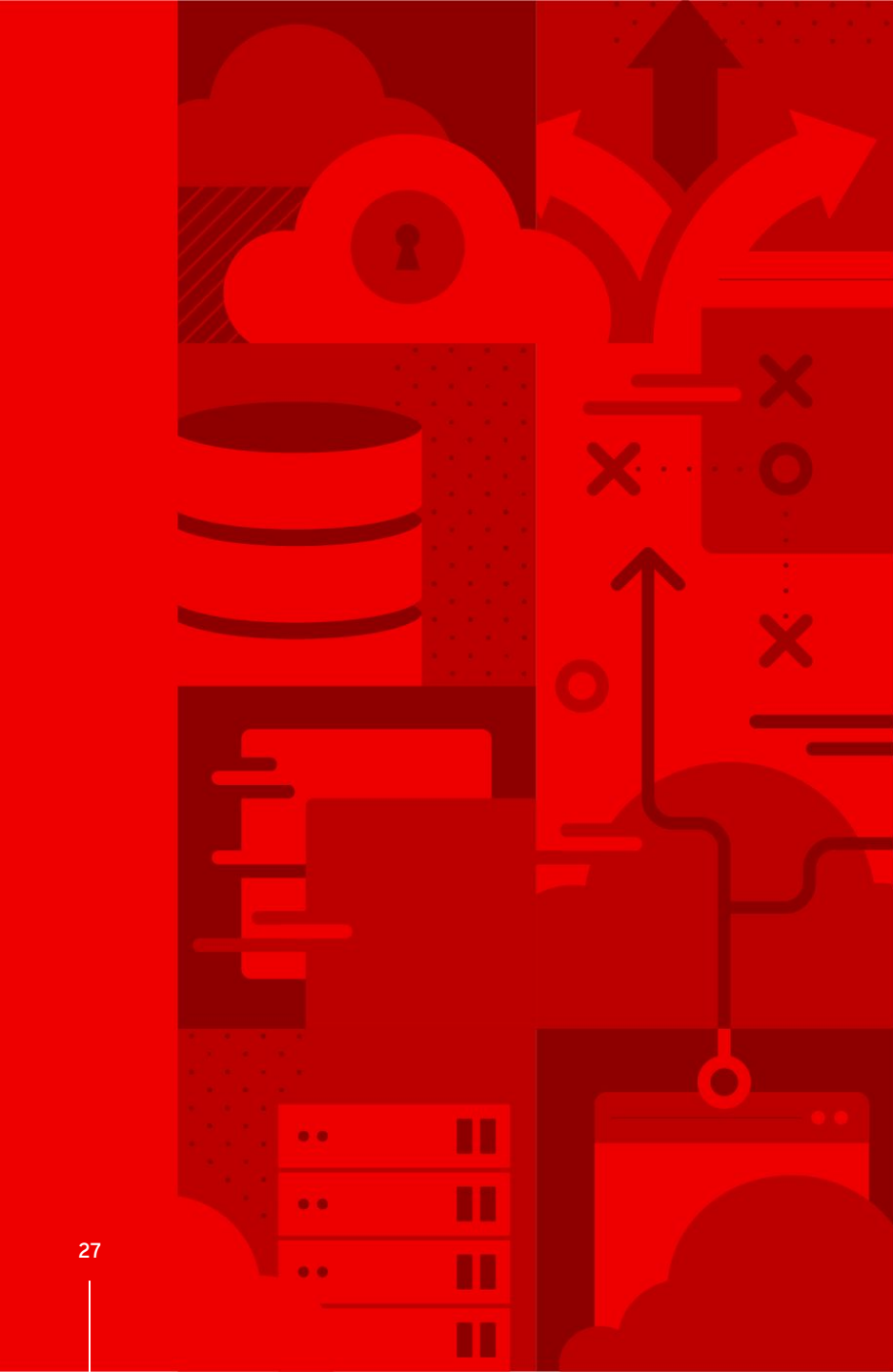
Comparison of Install Processes

Install via Kubernetes Manifests

- Create Database credential secret
- Create tls secret to store RSA SSL certificate and private key
- Create Persistent volume used to hold the microservice data
- Install the Database statefulset
- Create database credentials
- Define the application database and tables
- Deploy the application

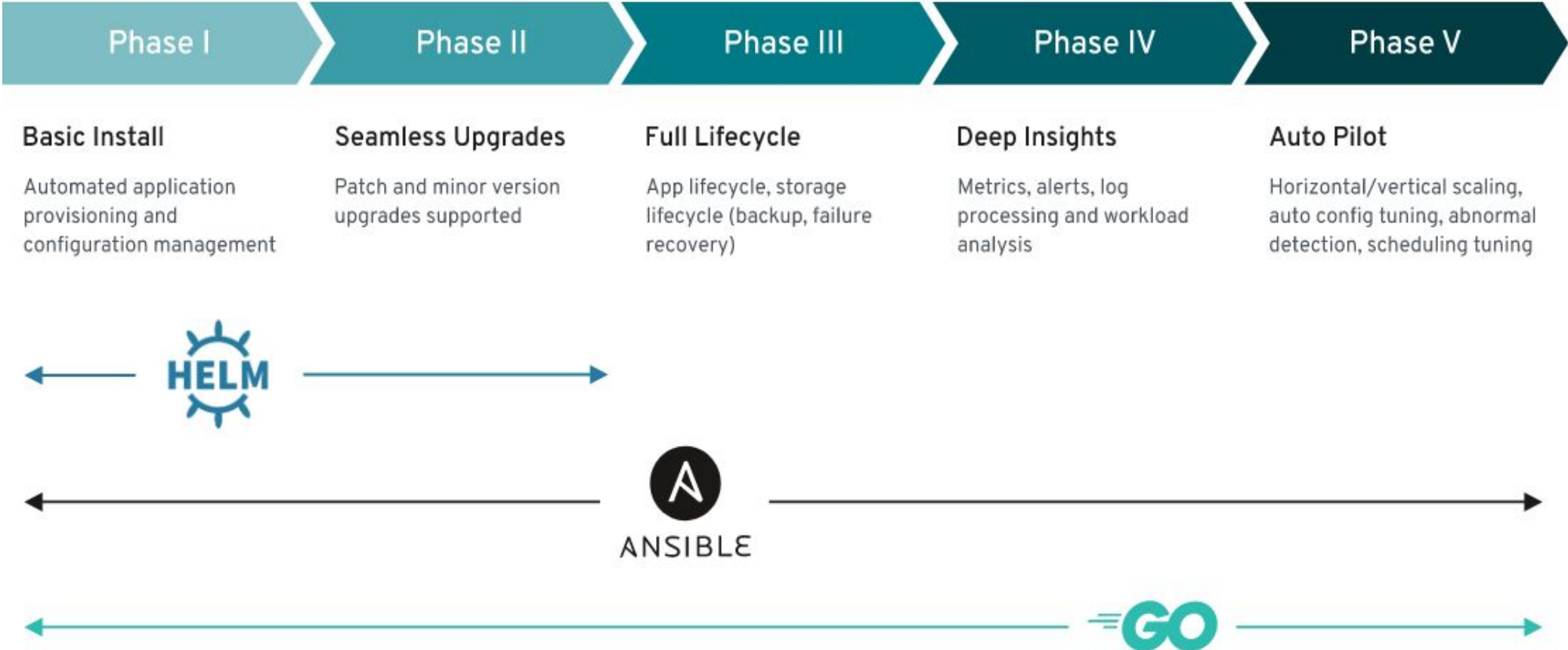
Installation using Operators

- Deploy the operator
- Deploy the application via a custom resource



Doorman Operator Design

Operator Maturity



Level 1 - Basic Install

- Generate/Acquire RSA SSL certificate for signing JWT tokens
- Create Database for storing user identities
- Create credentials for connecting to the database
- Deploy the authentication microservice

Level 2 - Seamless Upgrade

- Upgrade to the latest version of the application
- Rollback to previous version when deemed necessary

Level 3 - Full Lifecycle

- Create backups of the database
- Check integrity of backups
- Test functionality of the microservice

Level 4 - Deep Insights

- Expose custom metrics for the microservice
- Show graphs based on the metrics
- Setup alerting for only scenarios that need human intervention


```
shell$ curl -s http://localhost:5000/metrics | egrep '^doorman'
doorman_login_rate_seconds_bucket{total_logins="200",le="0.1"} 0
doorman_login_rate_seconds_bucket{total_logins="200",le="0.5"} 1
doorman_login_rate_seconds_bucket{total_logins="200",le="1"} 1
doorman_login_rate_seconds_bucket{total_logins="200",le="5"} 1
doorman_login_rate_seconds_bucket{total_logins="200",le="+Inf"} 1
doorman_login_rate_seconds_sum{total_logins="200"} 0.134216975
doorman_login_rate_seconds_count{total_logins="200"} 1
doorman_login_rate_seconds_bucket{total_logins="401",le="0.1"} 7
doorman_login_rate_seconds_bucket{total_logins="401",le="0.5"} 7
doorman_login_rate_seconds_bucket{total_logins="401",le="1"} 7
doorman_login_rate_seconds_bucket{total_logins="401",le="5"} 7
doorman_login_rate_seconds_bucket{total_logins="401",le="+Inf"} 7
doorman_login_rate_seconds_sum{total_logins="401"} 0.642076606
doorman_login_rate_seconds_count{total_logins="401"} 7
doorman_total_failed_logins 7
shell$
```

Level 5 - Auto Pilot

- Scale the auth service up/down based on traffic
- Ensure that the SSL certificates in use are valid

Conclusion

Conclusion


- Operators can save time for your skilled human assets and allow them to focus on enhancing the agenda of your organizations
- You also get consistency within each operator version

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](https://www.linkedin.com/company/red-hat)

 [facebook.com/redhatinc](https://www.facebook.com/redhatinc)

 [youtube.com/user/RedHatVideos](https://www.youtube.com/user/RedHatVideos)

 twitter.com/RedHat

