

Modern Technology Adventure with OpenShift and Microservices

Tayyip Osmanoglu
DevOps Team Lead at Payten
28.11.2023

ASEE ve Payten Asseco Grup Şirketleri

1991'de kuruldu



Tescilli **yazılım** ve hizmete odaklanmış



Varşova Borsası'nda
işlem görüyor

32.400
çalışan



60 ülkede hizmet veriyor

2022'de **3.7 milyar EUR** gelir



Avrupa'daki 6. en büyük IT şirketi



2022'de **387 milyon EUR** faaliyet kârı



+ 20% Gelir

ASEE ve Payten

3 kıtada Operasyon



- 23 ülke, 3800+ çalışan
- 2022 satışları 333.9 m EUR
- 2022 FAVÖK 65.9 m EUR
- Tescilli yazılım ve çözümler
- Yılda 1 milyarın üzerinde e-ticaret işlemi
- Ayda 5.5 milyon üzerinde Tokenization işlemi
- 10,000+ ATM
- 1,000,000 POS

ASEE ve Payten, 60 ülkede operasyonu olan Avrupa'nın 6. büyük yazılım firması Asseco Grup'a bağlıdır.

Payten Türkiye Ürün Portföyü

Payten
Nestpay

Payten
Payment Gateway

Payten
Fintech Suite


paratika

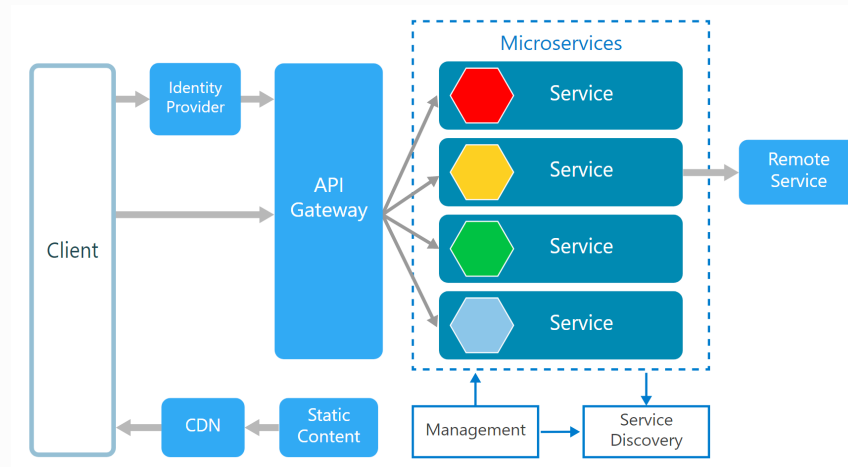
 LexisNexis®
RISK SOLUTIONS

 InACT
by CLUSTRO

 ThreatMetrix®
A LexisNexis® Risk Solutions Company

Application and Infrastructure Modernization

- Application and infrastructure modernization project.
- Using Java programming language and Spring framework.
- Ability to process 1+ billion transactions annually.
- The non-production and production environments are running on Red Hat OpenShift Container Platform.



Payten Tech Stack

Bitbucket, Jenkins, SonarQube, Argo CD, Nexus, Ansible

OpenShift Container Platform, Red Hat Advanced Cluster Security, OpenShift Data Foundation, Rancher Kubernetes

Kafka, Redis, Cassandra, Oracle, HashiCorp Vault

Graylog, Opensearch, Prometheus, Grafana, Dynatrace, Opsgenie



DevOps Pipelines

- All pipelines were written with Jenkins Shared Libraries
- Running unit tests
- Code quality analysis with SonarQube
- Build and push images to image registry
- Image scanning with cli tool of Red Hat Advanced Cluster Security
- Image signing with cosign
- Continuous deployment with Argo CD

OpenShift Container Platform

- Installed on vSphere with IPI method.
- 3 master nodes, 3 infra nodes and n worker nodes are members of OCP Cluster.
- OpenShift components are running on infra nodes such as Logging, Monitoring, Ingress, Image Registry, GitOps and ACS.
- User management configurations.
- AlertManager integration with Opsgenie.

OpenShift GitOps & Argo CD

- Installed on OpenShift with OpenShift GitOps Operator.
- All resources were created with declarative methods and yaml files are stored in git repositories.

The screenshot displays the OpenShift GitOps console interface for an application named 'argocd-dev'. The top navigation bar includes 'Applications / Q argocd-dev' and an 'APPLICATION DETAILS TREE' link. Below this, there are several action buttons: 'APP DETAILS', 'APP DIFF', 'SYNC', 'SYNC STATUS', 'HISTORY AND ROLLBACK', 'DELETE', and 'REFRESH'. The main content area is divided into three sections: 'APP HEALTH' (Missing), 'CURRENT SYNC STATUS' (OutOfSync From 3.33.2 (3.33.2)), and 'LAST SYNC RESULT' (Sync OK To 3.33.2, Succeeded a minute ago). The central part of the screen shows a dependency graph for the application, with nodes representing various Kubernetes resources like 'argocd-dex-server', 'argocd-server', 'argocd-dev-application-controller', 'argocd-dev-repo-server', and 'argocd-dev-server'. Each node is connected to its dependencies and includes a status icon (heart for OK, yellow triangle for warning, red triangle for error) and a refresh button. A search bar at the top left of the graph shows '90%'.

OpenShift GitOps & Argo CD

- Installed on OpenShift with OpenShift GitOps Operator.
- All resources were created with declarative methods and yaml files are stored in git repositories.

```
1  apiVersion: argoproj.io/v1alpha1
2  kind: Application
3  metadata:
4    labels:
5      env: dev
6      type: backend
7    name: service-a-dev
8    namespace: openshift-gitops
9  spec:
10 destination:
11   namespace: app-develop
12   server: https://kubernetes.default.svc
13   project: app-develop
14   source:
15     chart: generic-chart
16     helm:
17       parameters:
18         - name: image.tag
19           value: 1.0.1
20         - name: image.repository
21           value: nexus.local/service-a
22       valueFiles:
23         - helm-values/service-a/values-dev.yaml
24     repoURL: https://nexus.local/repository/helmrepo/
25     targetRevision: 1.0.1
```

```
1  apiVersion: argoproj.io/v1alpha1
2  kind: AppProject
3  metadata:
4    name: app-develop
5    namespace: openshift-gitops
6  spec:
7    destinations:
8      - name: in-cluster
9        namespace: app-develop
10       server: https://kubernetes.default.svc
11    sourceRepos:
12      - https://nexus.local/repository/helmrepo/
```

Helm Charts

- Generic helm chart for all microservices.
- Contains all the necessary Kubernetes objects for application.
- Contains values files for each environment.

templates

- _helpers.tpl
- configmap-js.yaml
- configmap-nginx.yaml
- configmap.yaml
- deployment.yaml
- externalSecret.yaml
- hpa.yaml
- ingress.yaml
- pdb.yaml
- routes.yaml
- secret.yaml
- secretStore.yaml
- service.yaml
- serviceaccount.yaml

```

1 apiVersion: apps/v1
2 kind: Deployment
3 metadata:
4   name: {{ .Values.application }}-{{ .Values.env }}
5   namespace: {{ .Release.Namespace }}
6   {{- with .Values.labels }}
7   labels:
8     {{- toYaml . | nindent 4 }}
9   {{- end }}
10 spec:
11   {{- if not .Values.autoscaling.enabled }}
12   replicas: {{ .Values.replicaCount }}
13   {{- end }}
14   {{- with .Values.labels }}
15   selector:
16     matchLabels:
17       {{- toYaml . | nindent 6 }}
18   {{- end }}
19   template:
20     metadata:
21       {{- with .Values.podAnnotations }}
22       annotations:
23         {{- toYaml . | nindent 4 }}
24       {{- end }}
25       {{- with .Values.labels }}
26       labels:
27         {{- toYaml . | nindent 4 }}
28       {{- end }}

```

```

1 # Deployment
2 application: service-a
3 env: dev
4 labels:
5   app: service-a
6   env: dev
7 replicaCount: 3
8 terminationGracePeriodSeconds: 90
9
10 image:
11   repository: nexus.local/service-a
12   tag: 1.0.1
13   pullPolicy: Always
14
15 imagePullSecrets:
16   - name: image-registry-secret
17
18 containerPorts:
19   - name: http
20     containerPort: 8080
21
22
23 serviceAccount:
24   name: service-a
25   create: true
26   annotations: {}

```

```

1 # Configuration
2 configMap:
3   create: true
4   variables:
5     SPRING_DATA_CASSANDRA_CONTACT_POINTS: ''
6     SPRING_DATA_CASSANDRA_PORT: 9042
7   additionalConfigMaps:
8     - common-config
9
10 secret:
11   create: false
12   variables: {}
13   additionalSecrets:
14     - common-secret
15
16 externalSecret:
17   create: true
18
19 secretStore:
20   create: false

```

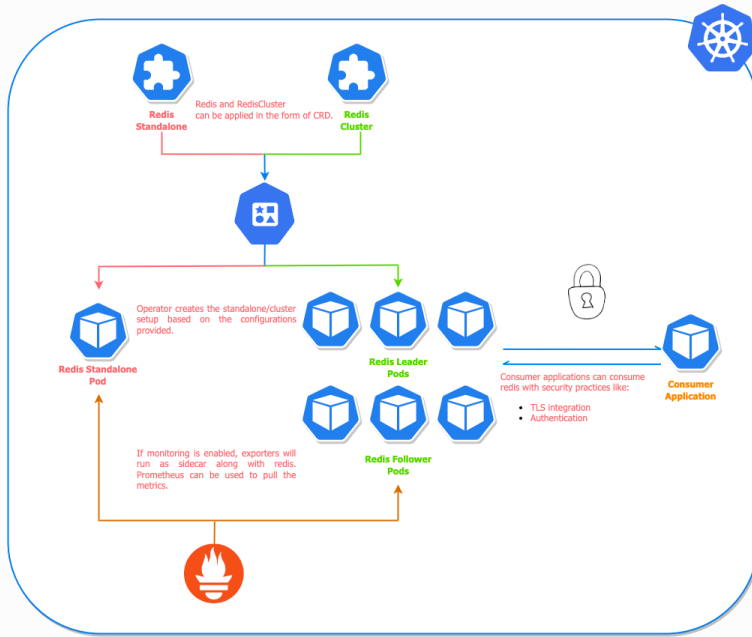
```

1 {{- if .Values.configMap.create -}}
2 apiVersion: v1
3 data:
4   {{- range $key, $value := .Values.configMap.variables }}
5     {{ $key }}: {{ $value | quote }}
6   {{- end }}
7 kind: ConfigMap
8 metadata:
9   name: {{ .Values.application }}-{{ .Values.env }}
10  namespace: {{ .Release.Namespace }}
11  {{- else -}}
12 apiVersion: v1
13 data:
14   {{- range $key, $value := .Values.configMap.variables }}
15     {{ $key }}: {{ $value | quote }}
16   {{- end }}
17 kind: ConfigMap
18 metadata:
19   name: {{ .Values.application }}
20   namespace: {{ .Release.Namespace }}
21 {{- end }}

```

Redis Clusters

- Installed on OpenShift Container Platform with community operator.
- One cluster for each environment.



```
1  apiVersion: v1
2  kind: Secret
3  metadata:
4    name: redis-dev-secret
5  namespace: ops
6  type: Opaque
7  stringData:
8    password: ''
9
10 ---
11
12 apiVersion: v1
13 kind: ConfigMap
14 metadata:
15   name: redis-dev-additional-config
16   namespace: ops
17 data:
18   redis-additional.conf: |
19     appendonly no
20     save ""
21
22 ---
23
24 apiVersion: redis.redis.opstree labs.in/v1beta1
25 kind: RedisCluster
26 metadata:
27   name: redis-dev
28   namespace: ops
29 spec:
30   clusterSize: 3
31   clusterVersion: v7
32   persistenceEnabled: true
33   securityContext:
34     runAsUser: 1000
35     fsGroup: 1000
36   serviceAccountName: redis-sa
37   kubernetesConfig:
38     image: quay.io/opstree/redis:v7.0.5
39     imagePullPolicy: IfNotPresent
40     resources:
41       requests:
42         cpu: 50m
43         memory: 300Mi
44       limits:
45         cpu: 50m
46         memory: 300Mi
47     redisSecret:
48       name: redis-dev-secret
49       key: password
50     redisExporter:
51       enabled: true
52       image: quay.io/opstree/redis-exporter:v1.44.0
53       imagePullPolicy: Always
54     resources:
55       requests:
56         cpu: 50m
57         memory: 120Mi
58       limits:
59         cpu: 100m
60         memory: 120Mi
61     env:
62       - name: REDIS_EXPORTER_INCL_SYSTEM_METRICS
63         value: "true"
64     redisLeader:
65     additionalRedisConfig: redis-dev-additional-config
66     redisFollower:
67     redisConfig:
68     additionalRedisConfig: redis-dev-additional-config
69     storage:
70     volumeClassNameTemplate:
71     spec:
72     storageClassName: ocs-storagecluster-ceph-rbd
73     accessModes:
74     - ReadWriteOnce
75     resources:
76     requests:
77     storage: "100Mi"
78
79
```

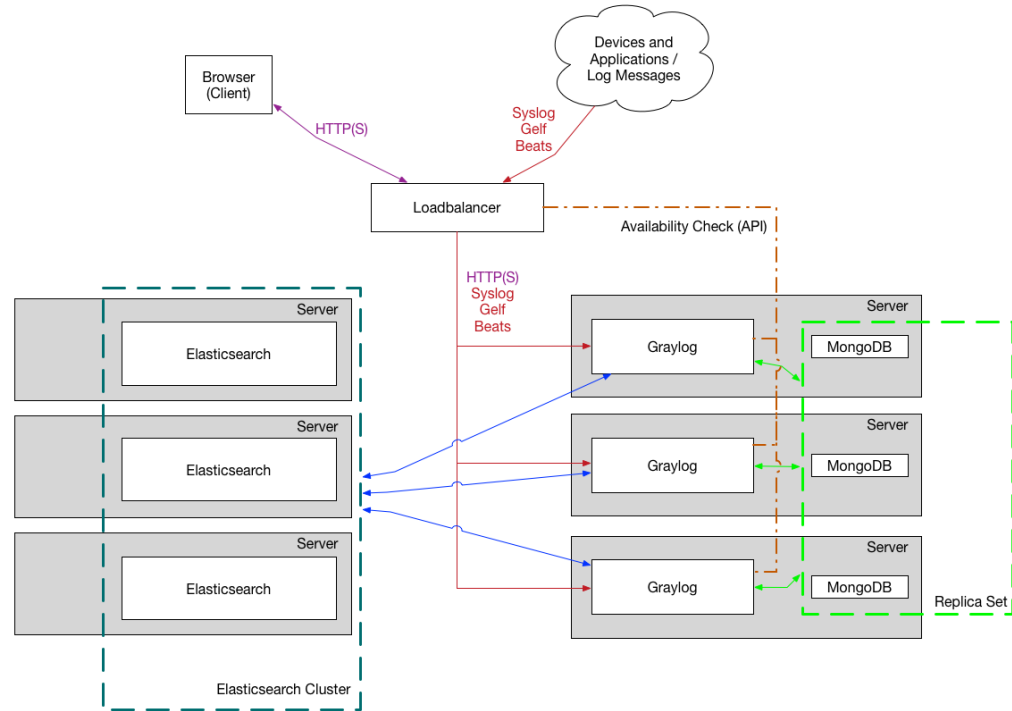
Kafka Clusters

- Installed on VMs with Ansible playbooks.
- Created topics for all environments.
- Default topic configurations about retention, partition and replication factor.

```
1 - name: Update Cache
2   apt:
3     update_cache: yes
4
5 - name: Installing java
6   apt:
7     name: openjdk-11-jdk
8     state: present
9
10 - name: Creating kafka user
11   user:
12     name: kafka
13     shell: /bin/sh
14     create_home: no
15
16 - name: Creating /opt/kafka-{{ kafka_version }}
17   file:
18     path: /opt/kafka-{{ kafka_version }}
19     state: directory
20     owner: kafka
21     group: kafka
22   tags:
23     - upgrade
24
25 - name: Downloading and extracting kafka
26   unarchive:
27     src: "{{ kafka_source }}"
28     dest: /opt/kafka-{{ kafka_version }}
29     remote_src: yes
30     extra_opts: [--strip-components=1]
31     owner: kafka
32     group: kafka
33   tags:
34     - upgrade
```

Graylog and Opensearch Clusters

- Installed on VMs with Ansible playbooks.
- There are 3 Graylog and MongoDB servers and 6 Opensearch server
- Created indices, streams for each environment.
- Event and notification definitions for several case and Opsgenie integration.



Graylog and Opensearch Clusters

Ansible Playbook for Opensearch

```

- README.md
- files
  - internal_users.yml
  - roles.yml
  - roles_mapping.yml
  - tenants.yml
- inventories
  - opensearch
    - drc-hosts
    - group_vars
      - all
        - all.yml
    - prod-hosts
    - test-hosts
- opensearch-drc.yml
- opensearch-prod.yml
- opensearch-test.yml
- roles
  - linux
    - dashboards
      - defaults
        - main.yml
      - handlers
        - main.yml
      - tasks
        - dashboards.yml
        - etchosts.yml
        - main.yml
        - tune.yml
      - templates
        - dashboards.service
        - opensearch_dashboards.yml
      - vars
        - main.yml
    - opensearch
      - defaults
        - main.yml
      - handlers
        - main.yml
      - secrets
        - drc.yml
        - prod.yml
        - test.yml
      - tasks
        - etchosts.yml
        - main.yml
        - opensearch.yml
        - security.yml
        - tune.yml
      - templates
        - internal_users.yml
        - jvm.options
        - opensearch-multi-node.yml
        - opensearch-single-node.yml
        - opensearch.service
        - security_conf.yml
        - security_plugin_conf.yml
        - tlsconfig.yml
      - vars
        - main.yml
  
```

21 directories, 40 files

```

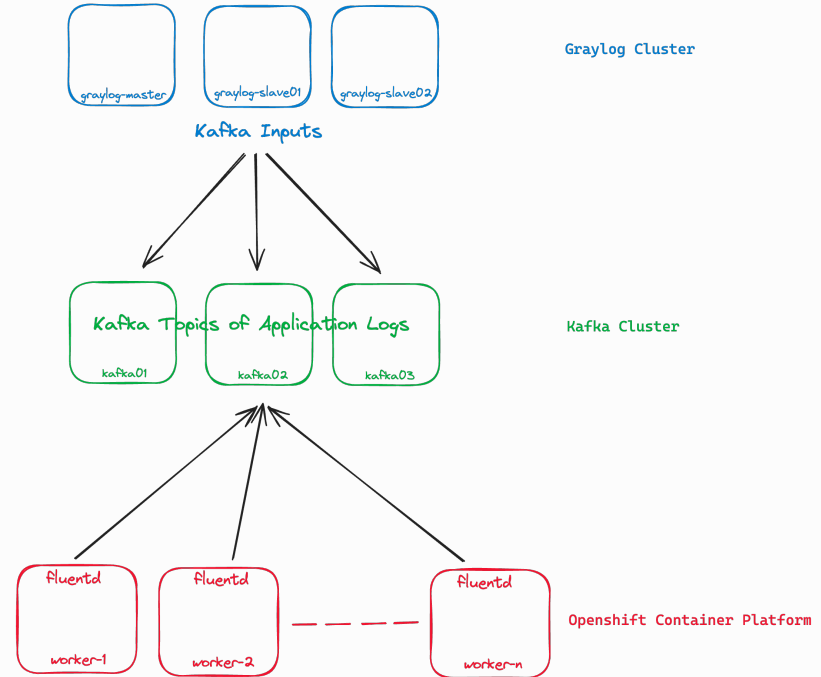
- README.md
- graylog
  - defaults
    - main.yml
  - handlers
    - main.yml
  - secrets
    - drc.yml
    - prod.yml
    - test.yml
  - tasks
    - etchosts.yml
    - main.yml
    - mongodb-Debian.yml
    - mongodb-RedHat.yml
    - mongodb-conf.yml
    - security.yml
    - server.yml
    - setup-Debian.yml
    - setup-RedHat.yml
  - templates
    - apt_preferences.d
      - debian_elasticsearch.j2
    - graylog.server.conf.j2
    - graylog.server.default.j2
    - mongo-admin-conf.sh
    - mongo-log-conf.sh
    - mongo-rs-conf.sh
    - mongodb-init.conf.j2
    - mongodb-latest.conf.j2
    - mongodb.service-Debian.j2
    - mongodb.service-RedHat.j2
  - vars
    - Debian.yml
    - RedHat.yml
    - main.yml
- graylog-drc.yml
- graylog-prod.yml
- graylog-test.yml
- inventory-drc
- inventory-prod
- inventory-test
  
```

9 directories, 34 files

Ansible Playbook for Graylog and MongoDB

Graylog and Opensearch Clusters

- OpenShift Logging component has collector pods to gather logs from application containers and it writes logs to target Kafka Topics.
- Graylog has input types that read messages from Kafka Topics.
- Indices and streams are created for each environment.



Red Hat Advanced Cluster Security

- Vulnerability management
- Compliance
- Network segmentation
- Verify images with trusted signature before deployment



Red Hat
Advanced Cluster
Security
for Kubernetes

Prometheus&Grafana and Dynatrace

- Installed on VMs with docker containers.
- Gathering metrics from multiple targets such as OpenShift, Kafka, Redis, etc.
- Dashboards for JVM, Kafka Clusters, Redis Clusters and OpenShift Infrastructure monitoring.
- OpenShift monitoring component collects metrics from specified endpoints of microservices and sends to OpenShift Prometheus for user workloads.
- Application performance monitoring (APM) with Dynatrace.

Thank you!

Tayyip Osmanođlu

DevOps Team Lead at Payten

tr.marcom@payten.com

www.payten.com/tr

Payten

Yasal Sorumluluk

Bu sunumda sunulan içerik telif hakkı korumasına tabidir. Metinler, grafikler, fotoğraflar, sesler, animasyonlar ve videolar ile bunların sunumda dağıtımı, Telif Hakları ve ilgili haklar Kanunu kapsamında korunmaktadır. Bu belgede yer alan herhangi bir materyalin izinsiz kullanımı, telif hakkı, ticari marka veya diğer yasaların ihlali anlamına gelebilir. Bu sunumdaki materyaller, Payten yazılı olarak onay vermediği sürece, kamuya açıklanamaz, kamuya açıklanamaz, icra edilemez, dağıtılamaz veya başka herhangi bir kamusal veya ticari amaçla kullanılamaz. Bu sunumun içeriğinin üçüncü şahıslar tarafından ticari kullanımı, dağıtımı, değiştirilmesi veya içeriğinin alınması dahil olmak üzere herhangi bir amaç için kopyalanması yasaktır. Ayrıca, bu sunum üçüncü taraflara sunulan tekliflere ve hizmetlere referans içerebilir. Bu teklifler ve hizmetler için kullanım şartları bu kuruluşlar tarafından tanımlanır.

Payten, bu kuruluşların teklif ve hizmetlerinin kullanım koşullarına, içeriklerine ve etkilerine ilişkin hiçbir sorumluluk kabul etmez. Bu sunumda yer alan bilgi ve bilgiler sadece bilgi amaçlıdır. Sunum Inscale şirket ürünlerinin kullanımı ile hazırlanmıştır. Payten'in adı ve logosu tescilli ticari markalardır. Bu işaretlerin kullanılması, Payten'in önceden açık bir şekilde anlaşılmasını gerektirir.