

# Install SSO

## اب SSO ب ص ن د ن ت س م Keycloak

ن ژرو Keycloak زا هدف ت س ا اب Single Sign-On (SSO) س ی و ر س کی ر ا ر ق ت س ا و د ا ج ی ا ل ح ا ر م د ن ت س م ن ی ا و ، Docker Registry ه ب ش و پ و د ل ی ب ، Docker Image ت خ ا س ل م ا ش ل ح ا ر م . د ه د ی م ح ی ص و ت ا ر 23 ت س ا Kuberentes ی و ر ی و ل پ ی د

## ل ح ا ر م

### 1. Docker Image ت خ ا س

د و ش ی م ه د ا ف ت س ا ر ی ز `Dockerfile` ل ی ا ف ، Docker Image د ا ج ی ا ی ا ر ب

```
FROM quay.io/keycloak/keycloak:23.0.3 as builder

# Enable health and metrics support
ENV KC_HEALTH_ENABLED=true
ENV KC_METRICS_ENABLED=true

# Configure a database vendor
ENV KC_DB=postgres

WORKDIR /opt/keycloak
# for demonstration purposes only, please make sure to use proper certificates in production
instead
RUN keytool -genkeypair -storepass password -storetype PKCS12 -keyalg RSA -keysize 2048 -
  dname "CN=server" -alias server -ext "SAN: c=DNS: localhost, IP: 127.0.0.1" -keystore
  conf/server.keystore
```

```
ADD --chown=keycloak:keycloak ./com.mavaratech.login-natcode-jar-with-dependencies.jar
/opt/keycloak/providers/com.mavaratech.login-natcode-jar-with-dependencies.jar

RUN /opt/keycloak/bin/kc.sh build

FROM quay.io/keycloak/keycloak: 23.0.3

COPY --from=builder /opt/keycloak/ /opt/keycloak/

# change these values to point to a running postgres instance
ENV KC_DB=postgres
#ENV KC_DB_URL=<DBURL>
#ENV KC_DB_USERNAME=<DBUSERNAME>
#ENV KC_DB_PASSWORD=<DBPASSWORD>
ENV KC_HOSTNAME=localhost
ENV KC_HOSTNAME_STRICT_HTTPS=false
ENV TZ=Asia/Tehran
ENTRYPOINT ["/opt/keycloak/bin/kc.sh", "start", "--debug", "--spi-theme-static-max-age=1", "--spi-theme-cache-themes=false", "--spi-theme-cache-templates=false"]
```

دش ه فاضا `/opt/keycloak/providers/` ی روت کرایاد هب هدش لی اپماک اواج نی گالپ ، لیاف نی اردت سا

**دلیب روت سرد**

```
docker build -t keycloak-custom: 23 .
```

ش فیرعت ی اوتحم زا `23` هخسن و `keycloak-custom` مان اب ار Docker Image روت سرد نی **حیضوت** دزاسیم `Dockerfile` رد

## Docker Registry هب Docker Image شوپ 2.

مینکیم شوپ `192.168.30.26:5000` رورس یور Docker یرتسیجر هب ار هدشهتخاس Docker Image

**تاروت سرد**

```
docker tag keycloak-custom: 23 192.168.30.26: 5000/keycloak-custom: 23
```

شوپ یارب ات دنکیم داچیا هدشهتخاس Docker Image یارب دیج گت کی روتسد نیا **حیضوت**  
دوش هدامآ یرتسیجر هب ندرک

```
docker push 192.168.30.26: 5000/keycloak-custom: 23
```

اسرا (|192.168.30.26: 5000|) هدشخصشم یرتسیجر هب ار Docker Image روتسد نیا **حیضوت**  
دنکیم

## Kubernetes یوریولپی د 3.

دوشیم هدافتسا ریز |keycloak-deploy. yaml| لیاف زا Keycloak، رارقتسا یارب

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: keycloak-deployment
  namespace: nioc
  labels:
    app: keycloak
spec:
  replicas: 1
  selector:
    matchLabels:
      app: keycloak
  template:
    metadata:
      labels:
        app: keycloak
    spec:
      containers:
        - name: keycloak
          image: image
          volumeMounts:
            - mountPath: /opt/keycloak/themes
              name: files-vol
              subPath: keycloak/themes
```

env:

- name: KC\_DB\_URL  
valueFrom:  
configMapKeyRef:  
name: integration-configs  
key: keycloak-db-url
- name: KC\_DB\_USERNAME  
valueFrom:  
configMapKeyRef:  
name: integration-configs  
key: keycloak-db-username
- name: KC\_DB\_PASSWORD  
valueFrom:  
configMapKeyRef:  
name: integration-configs  
key: keycloak-db-password
- name: KC\_HOSTNAME  
valueFrom:  
configMapKeyRef:  
name: integration-configs  
key: keycloak-db-hostname
- name: KEYCLOAK\_ADMIN  
valueFrom:  
configMapKeyRef:  
name: integration-configs  
key: keycloak-admin-user
- name: KEYCLOAK\_ADMIN\_PASSWORD  
valueFrom:  
configMapKeyRef:  
name: integration-configs  
key: keycloak-admin-password
- name: KC\_HOSTNAME\_STRICT\_HTTPS  
value: "false"
- name: KC\_HOSTNAME\_STRICT  
value: "false"
- name: DEBUG\_PORT  
value: " \*:8787"

volumes:

- name: files-vol  
persistentVolumeClaim:

```
claimName: pvc-files
```

```
---
```

```
apiVersion: v1
```

```
kind: Service
```

```
metadata:
```

```
  name: keycloak-service
```

```
  namespace: nioc
```

```
spec:
```

```
  selector:
```

```
    app: keycloak
```

```
  ports:
```

```
    - name: app
```

```
      protocol: TCP
```

```
      port: 8443
```

```
      targetPort: 8443
```

```
    - name: debug
```

```
      protocol: TCP
```

```
      port: 8787
```

```
      targetPort: 8787
```

یولپی د روتسد:

```
kubectl apply -f keycloak-deploy.yaml
```

هدرک لامغا Kubernetes رتسالك یور ار `keycloak-deploy.yaml` لیاف روتسد نی **حیضوت** دنکیم زاغآ ار Keycloak یولپید.

## 4. هئارا یارب Ingress میظنت

دوشیم هئارا نیمادباس یور SSO سیورس، ریز `ingress.yaml` لیاف زا هدافتسا اب

```
apiVersion: networking.k8s.io/v1
```

```
kind: Ingress
```

```
metadata:
```

```
  annotations:
```

```
    kubernetes.io/ingress.class: nginx
```

```

nginx.ingress.kubernetes.io/backend-protocol: HTTPS
nginx.ingress.kubernetes.io/keep-alive-requests: "10000"
nginx.ingress.kubernetes.io/large-client-header-buffers: 8 512k
nginx.ingress.kubernetes.io/max-worker-connections: "100000"
nginx.ingress.kubernetes.io/proxy-body-size: 8m
nginx.ingress.kubernetes.io/proxy-buffer-size: 256k
nginx.ingress.kubernetes.io/proxy-buffering: "on"
nginx.ingress.kubernetes.io/proxy-buffers: 4 512k
nginx.ingress.kubernetes.io/rewrite-target: /
nginx.ingress.kubernetes.io/ssl-redirect: "false"
nginx.ingress.kubernetes.io/upstream-keepalive-connections: "2000"
nginx.ingress.kubernetes.io/use-forwarded-headers: "true"
nginx.ingress.kubernetes.io/use-proxy-protocol: "true"
nginx.org/server-snippets: |
    listen 80 443 backlog=4096;
name: integration-ingress-ssl
namespace: nioc
spec:
  rules:
  - host: myso.nioc.ir
    http:
      paths:
      - backend:
          service:
            name: keycloak-service
            port:
              number: 8443
          path: /
          pathType: Prefix

```

ل‌ام‌عا روت‌سد:

```
kubectl apply -f ingress.yaml
```

ام‌ی‌ظ‌ن‌ت و ه‌د‌ر‌ک ل‌ام‌عا Kubernetes ر‌ت‌س‌ال‌ک ی‌ور ار `ingress.yaml` ل‌ی‌اف ر‌وت‌سد ن‌ی‌ا **ح‌ی‌ض‌وت** دن‌ک‌ی‌م د‌ا‌ج‌ی‌ا ار SSO س‌ی‌ور‌س ه‌ب ی‌س‌ر‌ت‌سد ی‌ار‌ب Ingress

## ه‌ج‌ی‌ت‌ن

گا. دوب دهاوخ سرتسد رد |myssso.nioc.ir| نیمادباس یور SSO سیورس، الاب لحارم یارجا زا سپ  
دینک هدافتسا یبایبیع یارب طبترم یاهگال زا، دمآشیپ هلحرم ره رد یلکش

## ی:سررب یارب دیفم تاروتسد

اهدآپ تیعضو یسررب

```
kubectl get pods -n nioc
```

دهدیم شیامن ار |nioc| namespace رد هدرقتسم یاهدآپ تیعضو روتسد نیا: **حیضوت**

دآپ یاهگال یسررب

```
kubectl logs [POD_NAME] -n nioc
```

شیامن تالکشم ای اطخ یسررب یارب ار صخش دآپ کی یاهگال روتسد نیا: **حیضوت**  
دهدیم

Revision #1

Created 8 January 2025 12:38:19 by sh.alavian

Updated 8 January 2025 12:49:18 by sh.alavian