

Kubernetes Authentication with Dex and OpenLDAP



X



<https://tinyurl.com/kubedexauth>



X



Challenge

Despite being the most widely used open source container orchestration platform today, Kubernetes does not have the means to create and manage users -at least not natively.

Far from being a disadvantage, however, this allows administrators to integrate the most appropriate identity service provider for their organization.

Why we need Dex ? (Cont.)

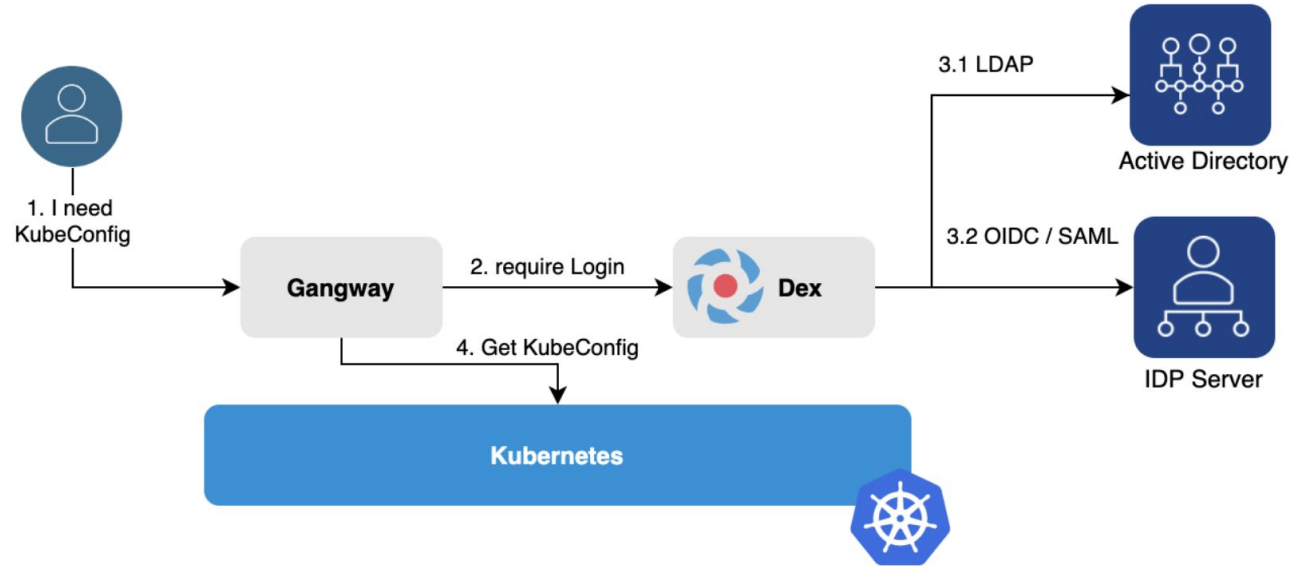
Dex comes with many different connectors for Authentication such as Okta, GitHub, Google, Microsoft, Linkedin, and LDAP. You can see all the supported connectors from [here](#).

But LDAP is a crucial tool here for big organizations, and this is why we will be focusing on LDAP connectors.

Dex solves Following problems

- Kubeconfig distribution
- Fine-grained control over the RBAC rules. (LDAP group + Role mapping)
- User Audit Logs

Dex Architecture



Let's config together



X



Configuration - LDAP (LDIFS)

```
dn: cn=oamooo,ou=users,dc=kubeops,dc=guru
```

```
cn: oamooo
```

```
sn: Doeooo
```

```
objectClass: inetOrgPerson
```

```
objectClass: shadowAccount
```

```
userPassword: password02
```

```
uid: oamooo
```

```
mail: oamooo@kubeops.guru
```

```
dn: cn=clusterusers,ou=users,dc=kubeops,dc=guru
```

```
cn: clusterusers
```

```
objectClass: groupOfNames
```

```
member: cn=oatooo,ou=users,dc=kubeops,dc=guru
```

```
member: cn=oamooo,ou=users,dc=kubeops,dc=guru
```


Configuration - LDAP (Deployment)

```
containers:  
- name: openldap  
  image: docker.io/bitnami/openldap:latest  
  imagePullPolicy: "IfNotPresent"  
  env:  
    - name: LDAP_ROOT  
      value: "dc=kubeops,dc=guru"  
    - name: BITNAMI_DEBUG  
      value: "true"  
    - name: LDAP_PORT_NUMBER  
      value: "3389"
```

Configuration - DEX (OIDC)

```
config:
  ""
  host: openldap:3389
  usernamePrompt: Email Address
  userSearch:
    baseDN: ou=users,dc=kubeops,dc=guru
    filter: "(objectClass=inetOrgPerson)"
    username: mail
    idAttr: DN
    emailAttr: mail
    nameAttr: cn
  groupSearch:
    baseDN: ou=users,dc=kubeops,dc=guru
    filter: "(objectClass=groupOfNames)"
    userMatchers:
      - userAttr: DN
        groupAttr: member
    nameAttr: cn
```

Configuration - DEX (OIDC Cont.)

```
staticClients:  
- id: loginapp  
  redirectURIs:  
  - 'http://20.24.21.143:32002/callback'  
  name: 'loginapp'  
  secret: OI DCAPPSECRET123
```

Configuration - DEX (Deployment)

```
containers:  
- image: ghcr.io/dexidp/dex:v2.30.0  
  name: dex  
  command:  
  ["/usr/local/bin/dex","serve","/etc/dex/cfg/config.yaml"]  
  ports:  
  - name: http  
    containerPort: 5556
```

Configuration – Loginapp or Gangway (Callback)

oidc:

client:

id: "loginapp"

secret: OI DCAPPSECRET123

redirectURL: "http://20.24.21.143:32002/callback"

issuer:

rootCA: "/etc/kubernetes/ssl/ca.pem"

url: "https://20.24.21.143:32000"

insecureSkipVerify: true

Configuration – Loginapp or Gangway (Deployment)

containers:

- image: quay.io/fydrah/loginapp:v3.2.1

command: ["/loginapp","serve","-c","/app/config.yaml"]

name: loginapp

ports:

- name: http

containerPort: 5555

volumeMounts:

- name: ca

mountPath: /etc/kubernetes/ssl/

- name: config

mountPath: /app/

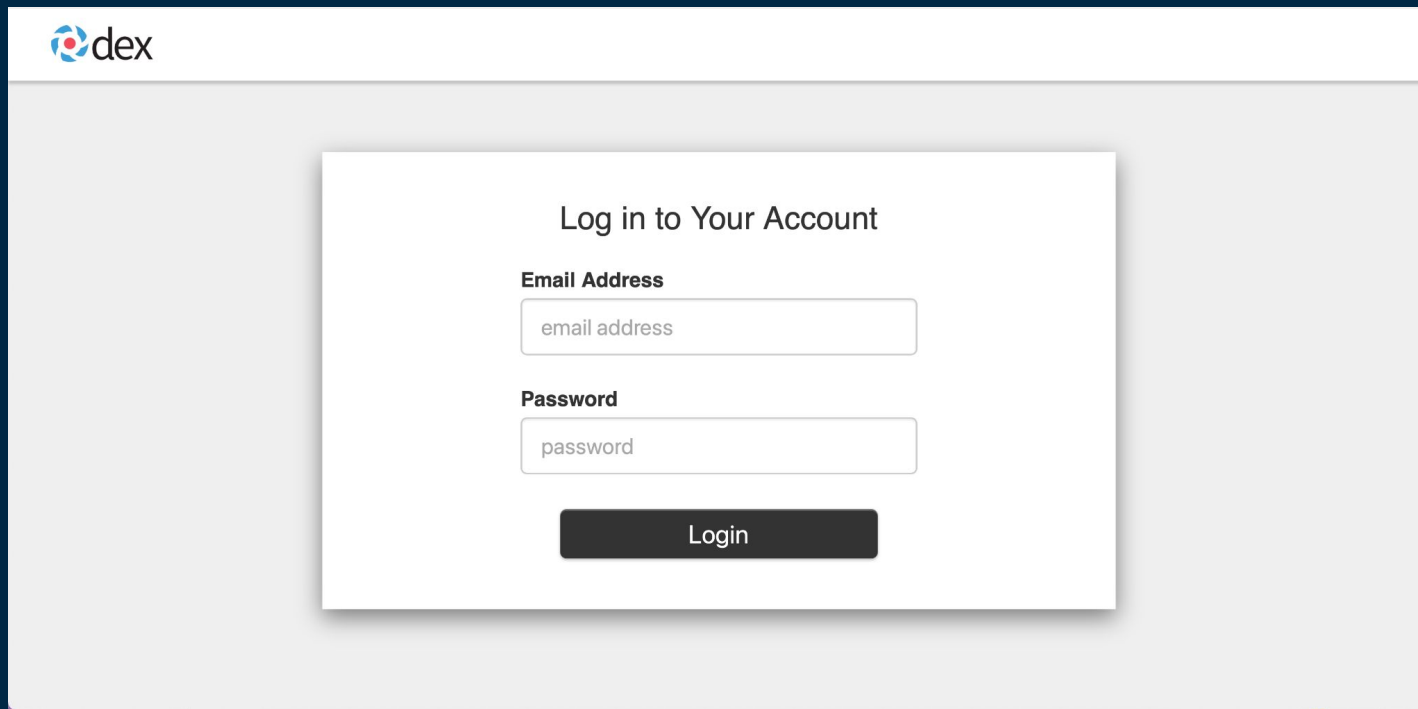
Dex and LDAP – Real Action




X



Loginapp (Client) <-> Dex (OIDC) <-> LDAP (IDP)



The image shows a web browser window displaying the Dex login page. The page has a white header with the Dex logo (a blue and red circular icon) and the word "dex" in black. Below the header is a light gray background. In the center, there is a white rectangular box with a subtle shadow. Inside this box, the text "Log in to Your Account" is centered at the top. Below this text, there are two input fields. The first is labeled "Email Address" in bold black text, and the second is labeled "Password" in bold black text. Both input fields have placeholder text: "email address" and "password" respectively. Below the input fields is a dark gray button with the word "Login" in white text.

 dex

Log in to Your Account

Email Address

email address

Password

password

Login

[Home](#)

Loginapp <-> Copy Kubeconfig to ~/.kube/config

loginapp

Kubectl

Credential

Kubeconfig

Full Kubeconfig

Clusters

Copy/paste this in your shell

```
kubectl config set-credentials 0atooo \  
  --auth-provider oidc \  
  --auth-provider-arg idp-issuer-url=https://20.24.21.143:32000 \  
  --auth-provider-arg client-id=loginapp \  
  --auth-provider-arg id-token=eyJhbGciOiJSUzI1NiIsImtpZCI6IjJmZTMxOWMzYTRhMTU0NDY5NmUxZGY3NDQzNTY0ZWVhMDY1YWRlMmEifQ.eyJpc3MiOiJodHRwczovLzIwLjI0LjIxLjE0MzozMjAwMCIsInN1YiI6IkpNpVmpiajF2WVhSdmIyOHNiM1U5ZFh0bG9uTXNaR005YTlnWVpXOXdjeXhrwXoxbmRYSjFFZ1JzWkdGdyIsImF1ZCI6ImxvZ2luYXBwIiwiaXhwIjojNjQ3NzkwOTg2LjE0MzozMzQ1ODY5ImF0X2hhc2giOiJVa2FXSGxuUmFOWGpwaFo2WkNwdGpRIiwiaY19oYXNoIjoib2F0b29vQGt1YmVvcHMuz3VydSIsImVtYWlsX3ZlcmIuZWVhIj0pbnVLLCJncm91cHM0IiwiaY2x1c3RlcjVzZXJzIl0sIm5hbWUiOiJwYXRvb28ifQ.tmcB0uPzS0RHR1kR6FSUDzEBjWfcTyyDCEe00pQkNTfyF_PkUGmZ2wYf3TH-E01U1oFRqwt-80dv_LkW3mJZxtInvw8vbKaed8339tM9I936zfsXzATq5krD7y7x134HXxsQBInPYInZmI I7S8ofRiBzaS4T_j_32u_su3uLC1JuhGTie-0M9PN9KG06nkB0ctyYAadsWxvuKnynakRUMI5II5RrtJWhLi2eFijEQ0Jb34EqWrRqH6KC1UVdprnFR i7BoSEN-7nrHIwnw6MsBzHjzaXmHHutuZdLpsT4qNtJr95vlnDahbaf7V5oyuVgzI-FdMeJJ30E3-HT6gYQ
```

Home

Kubernetes Authenticated

```
sirinatpaphatsirinatti — sirinatpaphatsirinatti@Sirinats-MacBook-Pro — ~ — zsh — 118x24
Last login: Sat Mar 19 22:29:30 on ttys000
→ ~ kubectl get pods
```

NAME	READY	STATUS	RESTARTS	AGE
hello-kubernetes-74544fff4f-97zq4	1/1	Running	0	21h
hello-kubernetes-74544fff4f-xkrbz	1/1	Running	0	21h
nfs-subdir-external-provisioner-7c8b4d4fcb-csvsg	1/1	Running	0	21h
nfs-subdir-external-provisioner-7c8b4d4fcb-p8lxm	1/1	Running	0	21h
nfs-subdir-external-provisioner-7c8b4d4fcb-qxfcx	1/1	Running	0	21h
node-problem-detector-2zkn	1/1	Running	0	21h
node-problem-detector-jlz4b	1/1	Running	0	21h
sample-app-57c486dd58-vs88j	1/1	Running	0	9h

```
→ ~
```

Q & A

The background is a solid dark blue. It features several decorative elements: a horizontal bar at the bottom composed of a teal segment on the left and a light pink segment on the right; a vertical line on the left with a teal square at its base; a vertical line on the right with a teal square at its base; a small teal square in the upper left; a small pink square in the upper right; a small orange square in the middle right; and several small white squares and lines scattered in the upper portion of the image.



- **100% Work Remotely**
- **Board Game Party**
- **Flexible Hours**
- **Learning Environment**
- **Mood Management**



Apply Here

<https://tinyurl.com/kubeopsap>



Contact Us



KubeOps Skills



@kubeops_skills



support@kubeops.guru



063-245-2168 (JoJo)

092-336-8882 (Oam)





**Thank you for your
Attention**



X

