KASTEN by Veeam

K8s and Active Directory Can Be Friends! How to Use Dex to Bridge the Gap

Onkar Bhat

Engineering Manager

Kasten by Veeam

www.linkedin.com/in/onkarbhat/

@onkarbhat

Start setting up the lab pre-requisites for this workshop now!

`https://k10.fyi/DexLab`

Agenda

1. Why attend this tutorial?
2. What are Active Directory and LDAP?
3. The Application
4. OpenLDAP
5. Dex
6. OAuth2 Proxy
7. Prerequisites
8. Setup OpenLDAP, Dex, OAuth2 Proxy and the App
9. Demo
10. Q&A
11. Thank you

Why Attend This Tutorial?

- Do you want to migrate an application to a Kubernetes cluster and secure access to it?
- Do you want to secure access to this application using your existing Active Directory server deployed outside a Kubernetes cluster?
- Do you want to secure access to new apps using the same Active Directory server?
- You are in the right tutorial!

Start setting up the lab pre-requisites for this workshop now!

`https://k10.fyi/DexLab`

KASTEN by Veeam

What is Active Directory?

- **Active Directory** (**AD**) is a directory service developed by Microsoft for Windows domain networks.

- Active Directory uses Lightweight Directory Access Protocol (LDAP) as well as other services (Kerberos & DNS) that won't be covered in this talk

KASTEN by Veeam

What is LDAP?

- The **Lightweight Directory Access Protocol** (**LDAP**) is an open, vendor-neutral, industry standard protocol for accessing and maintaining distributed directory information services

- A common use of LDAP is to provide a central place to store usernames and passwords. This allows many different applications and services to connect to the LDAP server to validate users

KASTEN by Veeam

What is OpenLDAP?

- OpenLDAP Software is an open-source implementation of the **L**ightweight **D**irectory **A**ccess **P**rotocol.

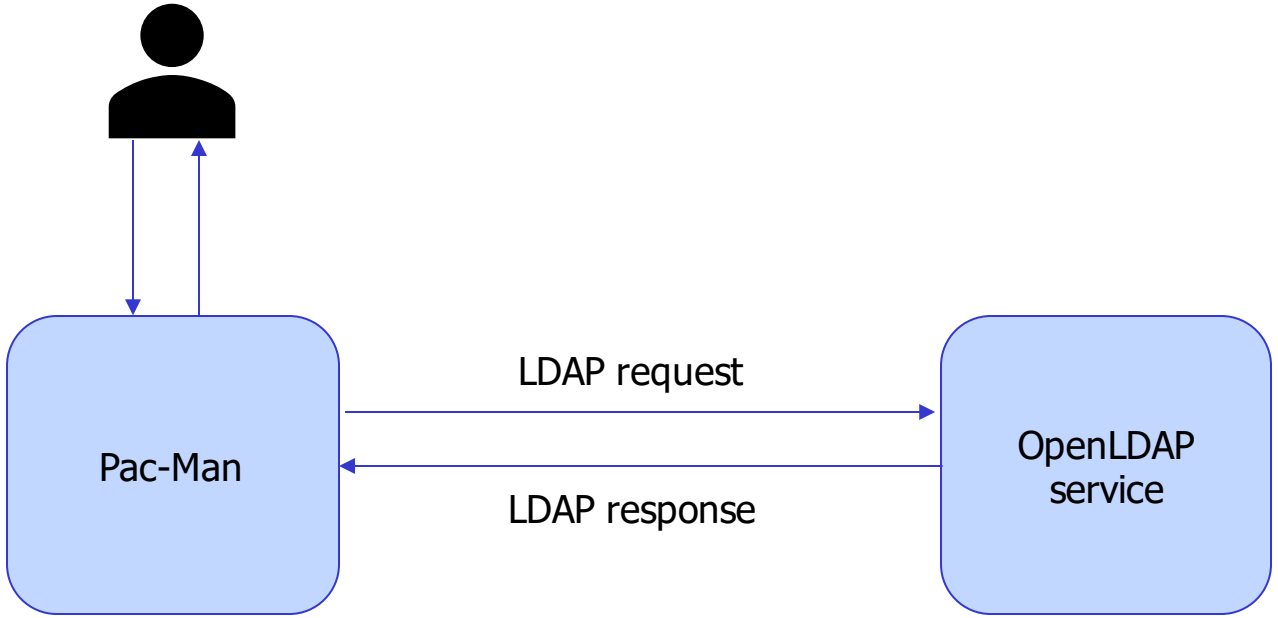
KASTEN by Veeam

The Application

- Deploy Pac-Man in a Kubernetes cluster
- Secure access to the application using the information stored in an OpenLDAP service

KASTEN by Veeam

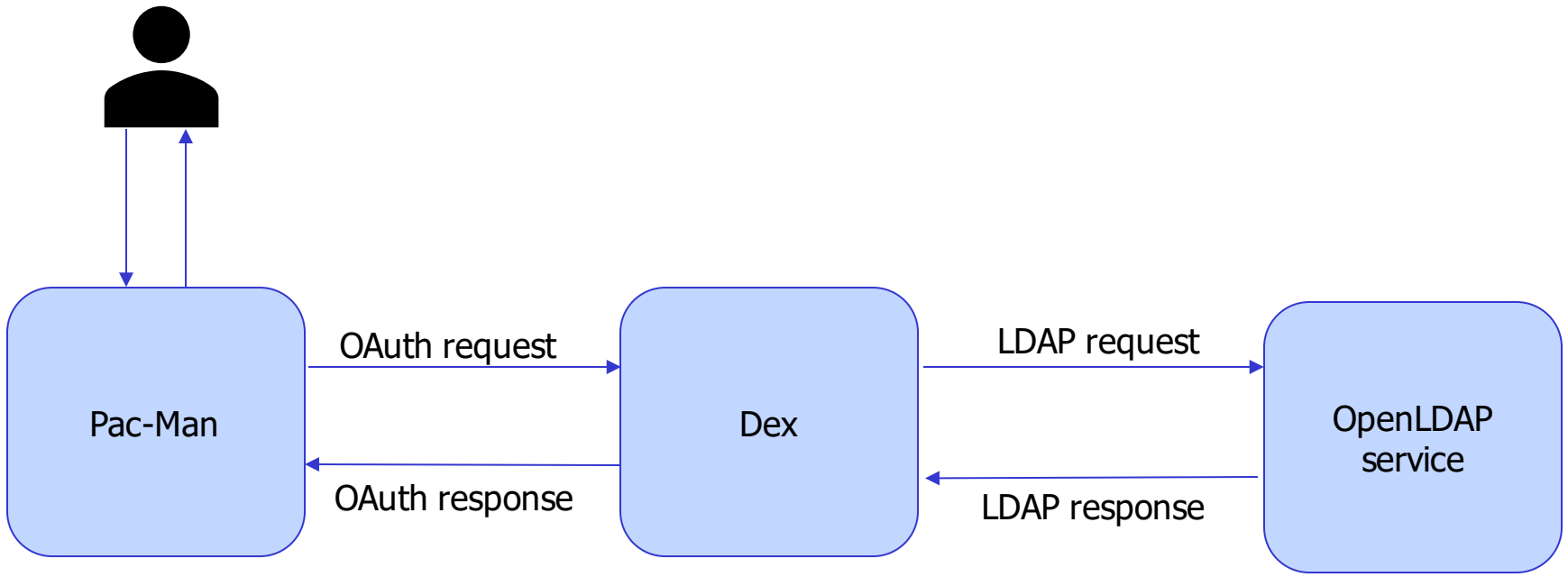
Pac-Man ⟷ OpenLDAP



Pac-Man ⟷ OpenLDAP

- Pro: OpenLDAP service is available for the app's authentication requirements.
- Con: To use the OpenLDAP service, you have to rewrite Pac-Man so that it authenticates against the OpenLDAP service each time someone accesses the Pac-Man app.

Pac-Man ⟷ Dex ⟷ OpenLDAP



Pac-Man ⟷ Dex ⟷ OpenLDAP

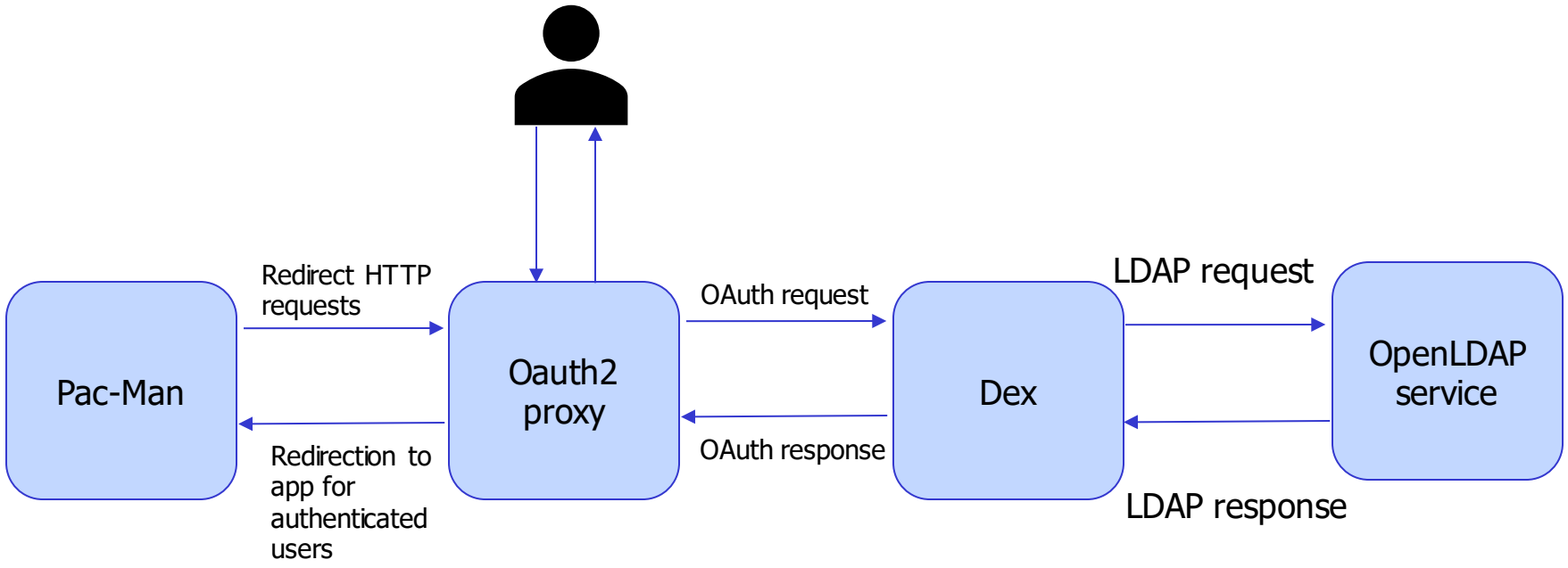
- Pro:
  - Dex knows how to interact with the OpenLDAP service
  - It serves as a proxy to the OpenLDAP service. Pac-Man can redirect requests to Dex. Dex will present a login screen.
  - After the user enters creds, Dex will initiate authN against the OpenLDAP service.
  - On successful authN, Dex will redirect back to the app.
- Con:
  - You still have to rewrite the application, so that it can play the role of an OAuth client.

What is OAuth?

- OAuth 2.0 is the industry standard (RFC6749) protocol for authorization

KASTEN by Veeam

Pac-Man ⟷ OAuth2-proxy ⟷ Dex ⟷ OpenLDAP



Pac-Man ⟷ OAuth2-proxy ⟷ Dex ⟷ OpenLDAP

- Pro: No modifications to the app! (well, almost)
- A Kubernetes service redirects HTTP traffic to the OAuth2 proxy.
- OAuth2 proxy is the OAuth client
- Dex is the OAuth server
- Dex can speak LDAP with the OpenLDAP service.
- On successful authN, the user is redirected from Dex to OAuth2 proxy, which in turn proxy the Pac-Man app to the user.

KASTEN by Veeam

Prerequisites

- x86_64 or amd64 based machine
- **ARM** is unfortunately not supported by the app in this lab
- Packages - Install guidance provided in tutorial instructions
  - Git
  - Docker
  - Kind
  - Kubectl
  - Helm
  - OpenLDAP Utils

Instructions

`https://k10.fyi/DexLab`

KASTEN by Veeam

Download Kind

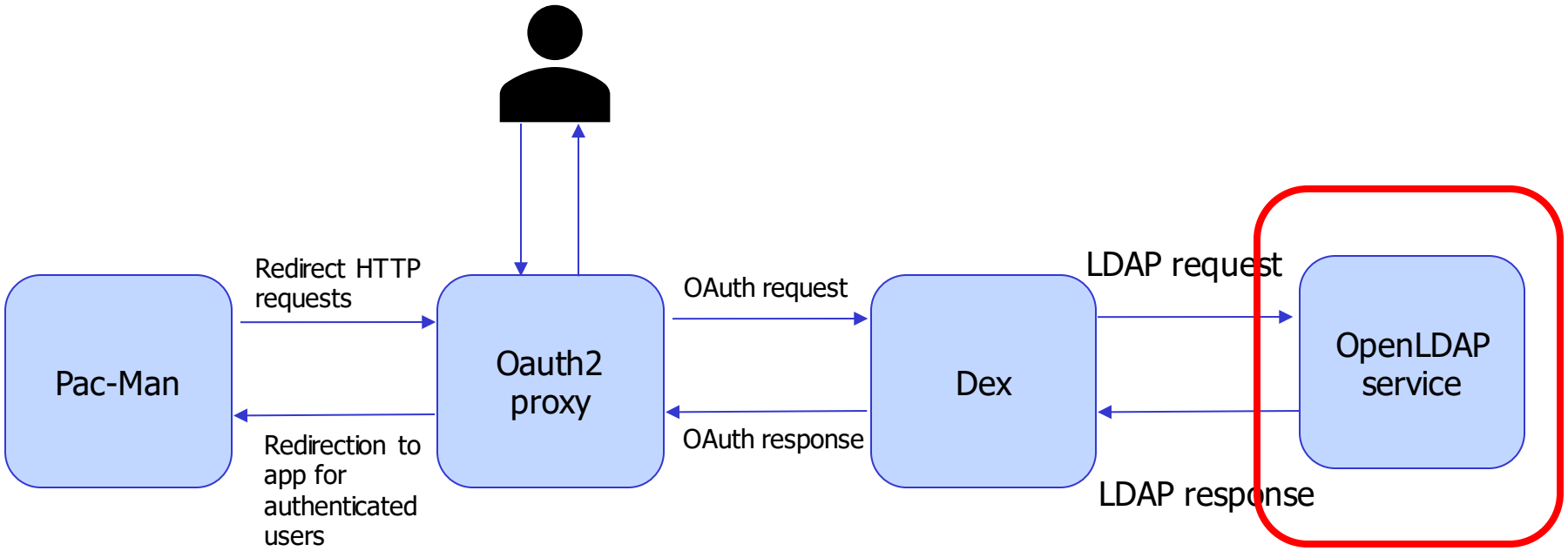
- Kind = Kubernetes in Docker
- Easy, fast & free way of running a Kubernetes cluster inside a set of docker containers
- macOS: `$ brew install kind`
- Windows: `$ choco install kind`
- Linux: use your distribution's package manager

KASTEN by Veeam

KASTEN by Veeam

Demo!

OpenLDAP



OpenLDAP

- Deploy OpenLDAP in our K8s cluster
- Add users and groups to this deployment
- Use LDAP utilities for querying the objects in the OpenLDAP directory

KASTEN by Veeam

OpenLDAP Group

- $ cat pacman-admin-group.ldif

```
dn: cn=pacmanAdmins,ou=users,dc=example,dc=org
cn: pacmanAdmins
objectClass: groupOfNames
member: cn=productionadmin,ou=users,dc=example,dc=org
member: cn=productionbasic,ou=users,dc=example,dc=org
```

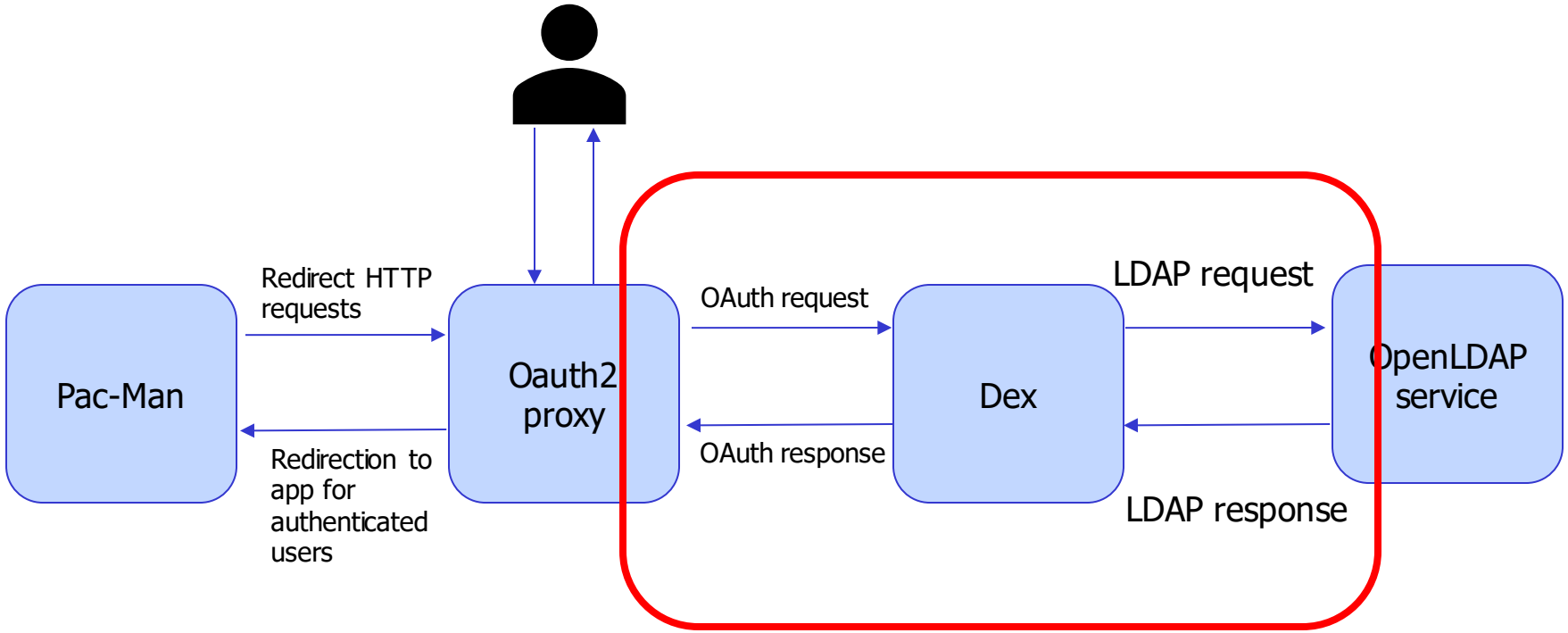
What is LDIF ?

- LDAP Data Interchange Format
- Plain text format
- Directory content and update requests

LDAP Fields in a Record

- `dn: cn=pacmanAdmins,ou=users,dc=example,dc=org`
- dn : This refers to the name that uniquely identifies an entry in the directory.
- cn : This refers to the individual object (person's name; group's name; meeting room; job title; etc.) for whom/which you are querying.
- ou : This refers to the organizational unit that the user is part of. If the user is part of more than one group, you may specify as such, e.g., OU= Lawyer,OU= Judge.
- dc : This refers to each component of the domain. For example, www.example.org would be written as dc=www,dc=example,dc=org

Dex



Dex Values File

- LDAP connector config
- Dex OIDC issuer config
- OAuth Client config

```yaml
config:
  connectors:
  - config:
      bindDN: cn=admin,dc=example,dc=org
      bindPW: <Enter the bind password here>
      groupSearch:
        baseDN: dc=example,dc=org
        filter: (objectClass=groupOfNames)
        nameAttr: cn
        userMatchers:
        - groupAttr: member
          userAttr: DN
      host: openldap.openldap:1389
      insecureNoSSL: true
      insecureSkipVerify: true
      startTLS: false
      userSearch:
        baseDN: ou=users,dc=example,dc=org
        emailAttr: uid
        filter: (objectClass=inetOrgPerson)
        idAttr: uid
        nameAttr: uid
        preferredUsernameAttr: uid
        username: uid
    id: ldap
    name: LDAP
    type: ldap
  issuer: http://dex.dex:5556/dex
  logger:
    format: text
    level: info
  oauth2:
    skipApprovalScreen: true
  storage:
    type: memory
  web:
    http: 0.0.0.0:8080
  staticClients:
  - id: kasten
    name: OAuth2Proxy
    redirectURIs:
    - http://oauth2-proxy.pacman:4180/oauth2/callback
    secret: kastensecret
```


KASTEN by Veeam

Dex – LDAP Connector Config

```yaml
config:
  connectors:
  - config:
      bindDN: cn=admin,dc=example,dc=org
      bindPW: adminpassword
      groupSearch:
        baseDN: dc=example,dc=org
        filter: (objectClass=groupOfNames)
        nameAttr: cn
        userMatchers:
        - groupAttr: member
          userAttr: DN
      host: openldap.openldap:1389
      insecureNoSSL: true
      insecureSkipVerify: true
      startTLS: false
      userSearch:
        baseDN: ou=users,dc=example,dc=org
        emailAttr: uid
        filter: (objectClass=inetOrgPerson)
        idAttr: uid
        nameAttr: uid
        preferredUsernameAttr: uid
        username: uid
    id: ldap
    name: LDAP
    type: ldap
```

Dex – OIDC Issuer Config

```
issuer: http://dex.dex:5556/dex
logger:
  format: text
  level: info
oauth2:
  skipApprovalScreen: true
storage:
  type: memory
web:
  http: 0.0.0.0:8080
```

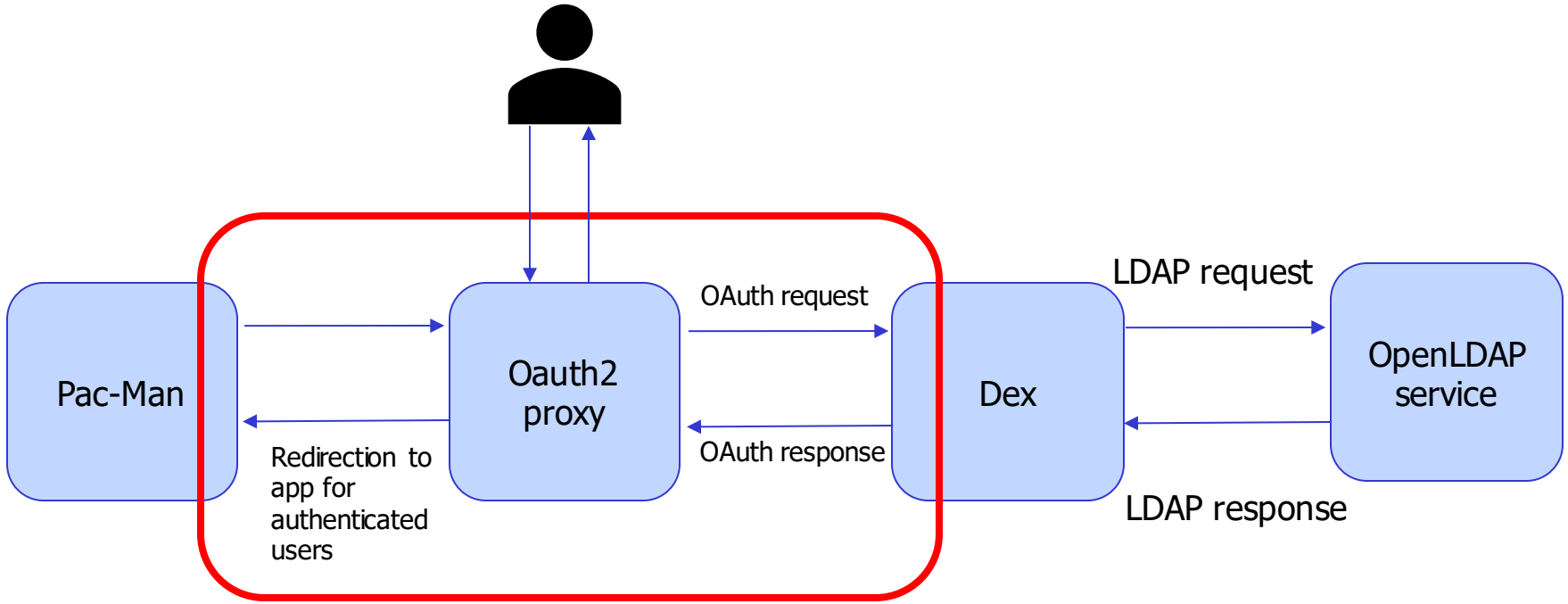

KASTEN by Veeam

Dex - OAuth Client Config

```yaml
staticClients:
- id: kasten
  name: OAuth2Proxy
  redirectURIs:
  - http://oauth2-proxy.pacman:4180/oauth2/callback
  secret: kastensecret
```


KASTEN by Veeam

OAuth2 Proxy



Edit the system's hosts file

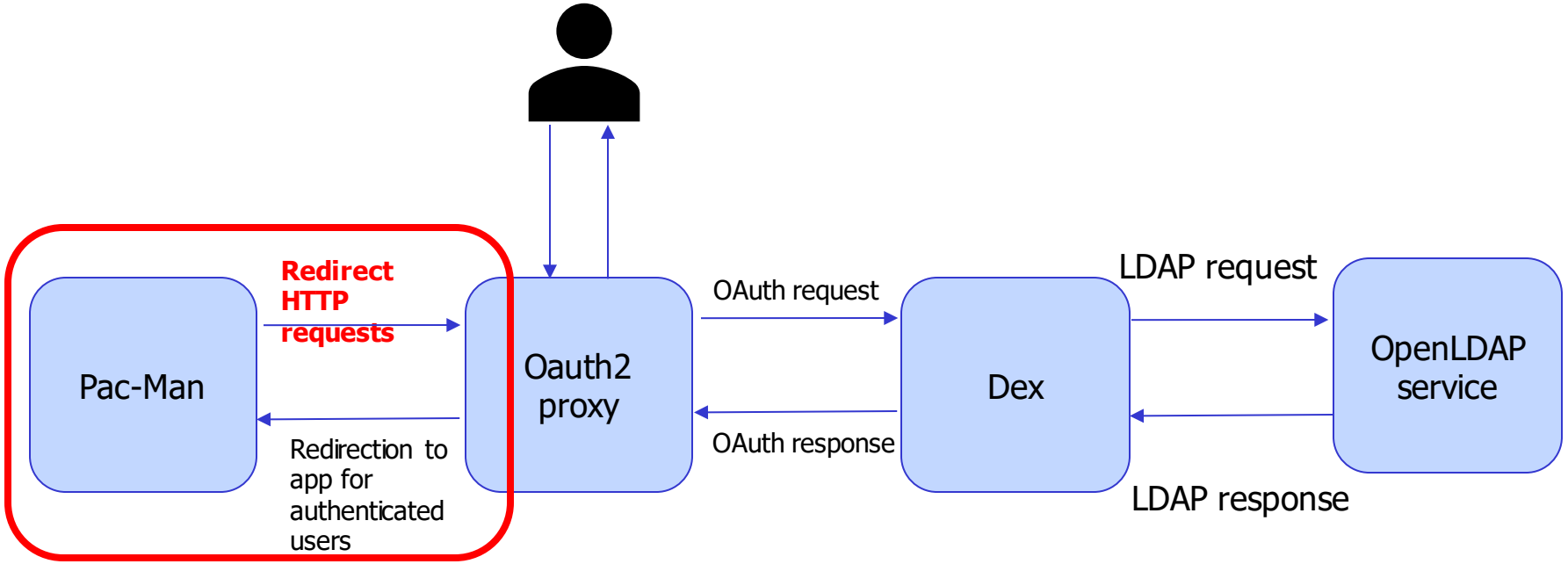
- macOS & Linux: sudo vi /etc/hosts
- Windows: c:\windows\system32\drivers\etc\hosts
- Add those lines:

```
127.0.0.1 dex.dex

127.0.0.1 oauth2-proxy.pacman
```


KASTEN by Veeam

Pac-Man



Deploy Pac-Man

- `$ helm repo add pacman` https://shuguet.github.io/pacman/
- `$ helm repo update pacman`
- `$ helm install pacman pacman/pacman -n pacman`

KASTEN by Veeam

Verify Pac-Man is Installed

- `$ helm status pacman -n pacman`
- `$ watch kubectl get pod -n pacman`

KASTEN by Veeam

Check Default Pac-Man Service Config

- `$ kubectl get svc pacman -n pacman -o yaml`

Pac-Man - Port-Forward

- `$ kubectl port-forward service/pacman -n pacman 9090:80`
- Open your web browser to http://127.0.0.1:**9090**

Update the pacman service

- ```
  $ kubectl patch svc pacman -n pacman --type='json' -p='[{"op": "replace", "path": "/spec/ports/0/targetPort", "value":4180}]'
  ```
- ```
  $ kubectl patch svc pacman -n pacman --type='json' -p='[{"op": "replace", "path": "/spec/selector", "value":{"k8s-app": "oauth2-proxy"}}]'
  ```


KASTEN by Veeam

Redirect Traffic to OAuth2 Proxy

Result of the patches:

```
kubectl get svc pacman -n pacman -o yaml
```

```yaml
spec:
  clusterIP: 10.96.42.18
  clusterIPs:
  - 10.96.42.18
  internalTrafficPolicy: Cluster
  ipFamilies:
  - IPv4
  ipFamilyPolicy: SingleStack
  ports:
  - name: http
    port: 80
    protocol: TCP
    targetPort: 8080
  selector:
    app.kubernetes.io/instance: pacman
    app.kubernetes.io/name: pacman
  sessionAffinity: None
  type: ClusterIP
status:
  loadBalancer: {}
```

```yaml
spec:
  clusterIP: 10.96.42.18
  clusterIPs:
  - 10.96.42.18
  internalTrafficPolicy: Cluster
  ipFamilies:
  - IPv4
  ipFamilyPolicy: SingleStack
  ports:
  - name: http
    port: 80
    protocol: TCP
    targetPort: 4180
  selector:
    k8s-app: oauth2-proxy
  sessionAffinity: None
  type: ClusterIP
status:
  loadBalancer: {}
```

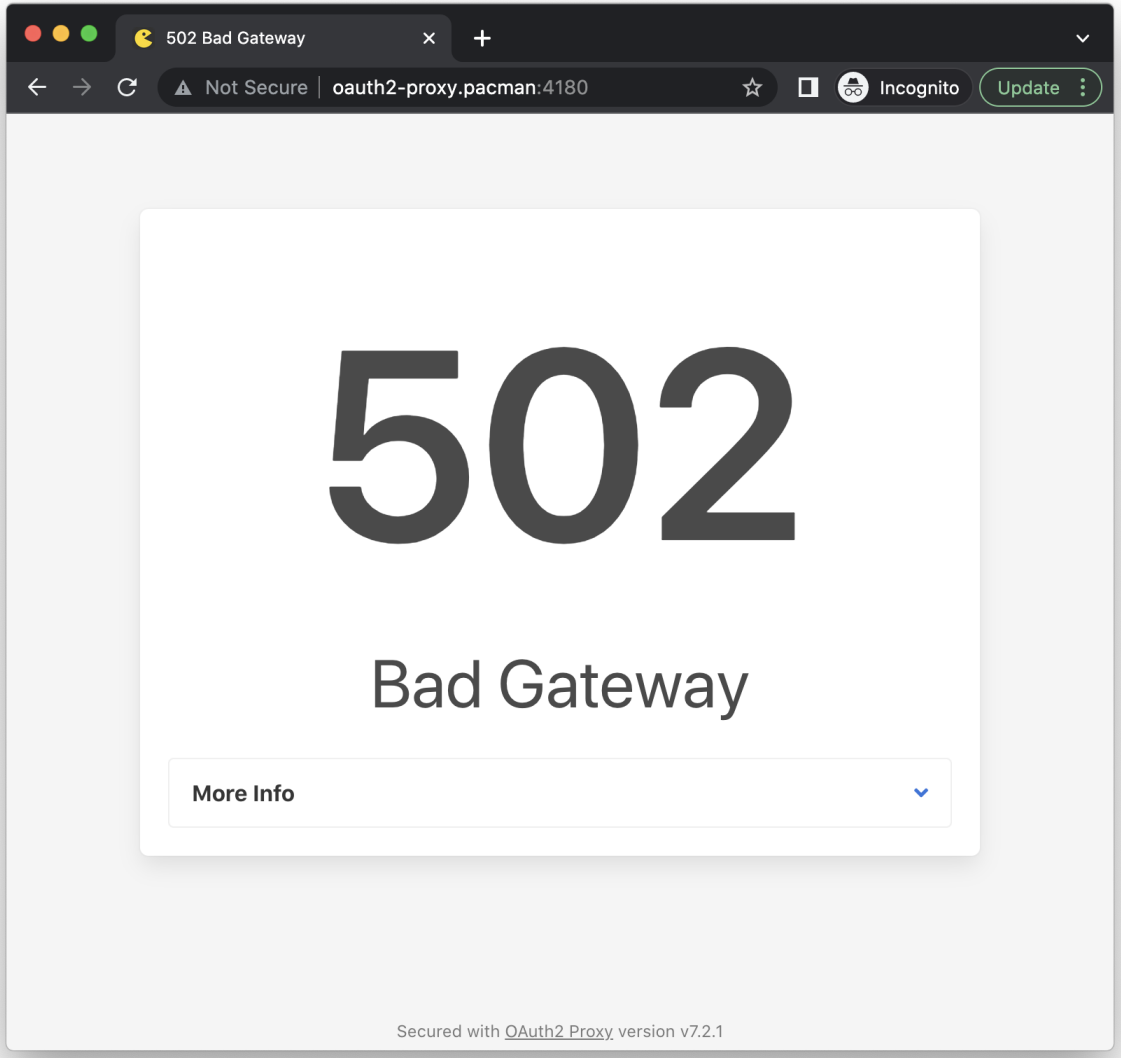

KASTEN by Veeam

Pac-Man – Look at the End Result

- `$ kubectl port-forward service/pacman -n pacman 9090:80`
- Open your web browser to http://127.0.0.1:**9090**

KASTEN by Veeam

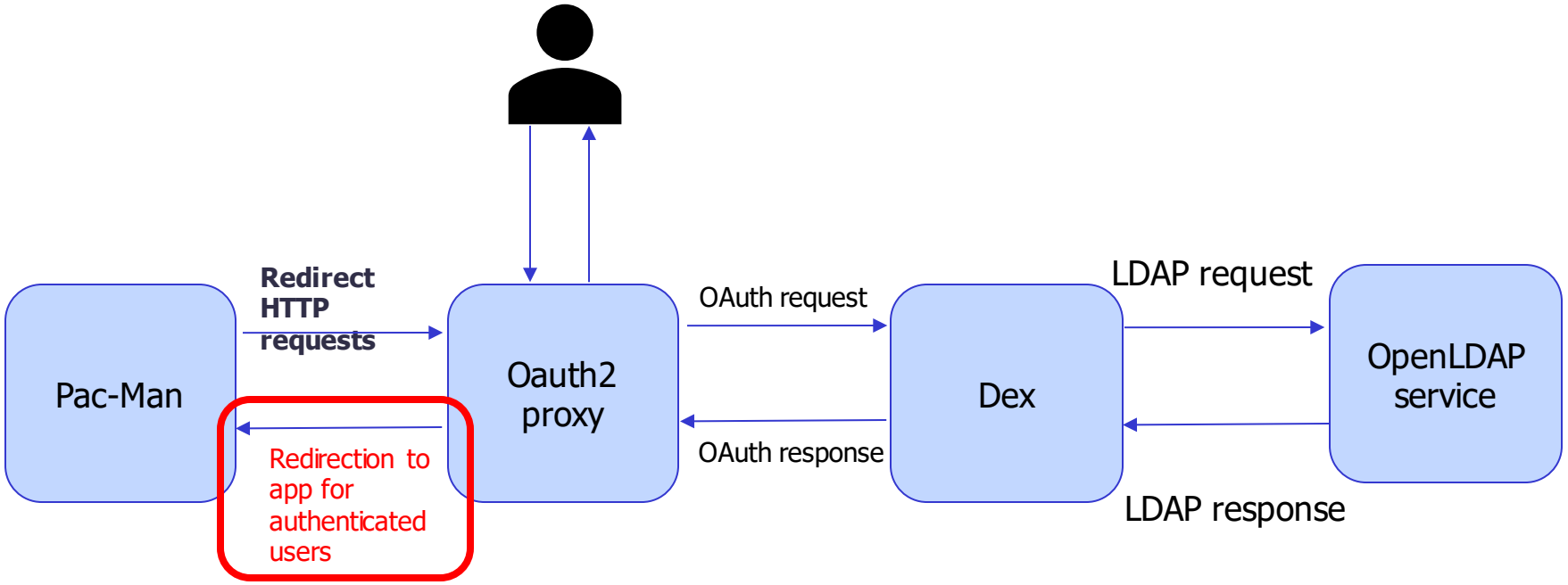
Demo



Oops...

KASTEN by Veeam

Pac-Man



Pac-Man – Deploy pacman-actual Service

- `$ cd pacman`
- `$ kubectl create -f pacman-actual-service.yaml -n pacman`

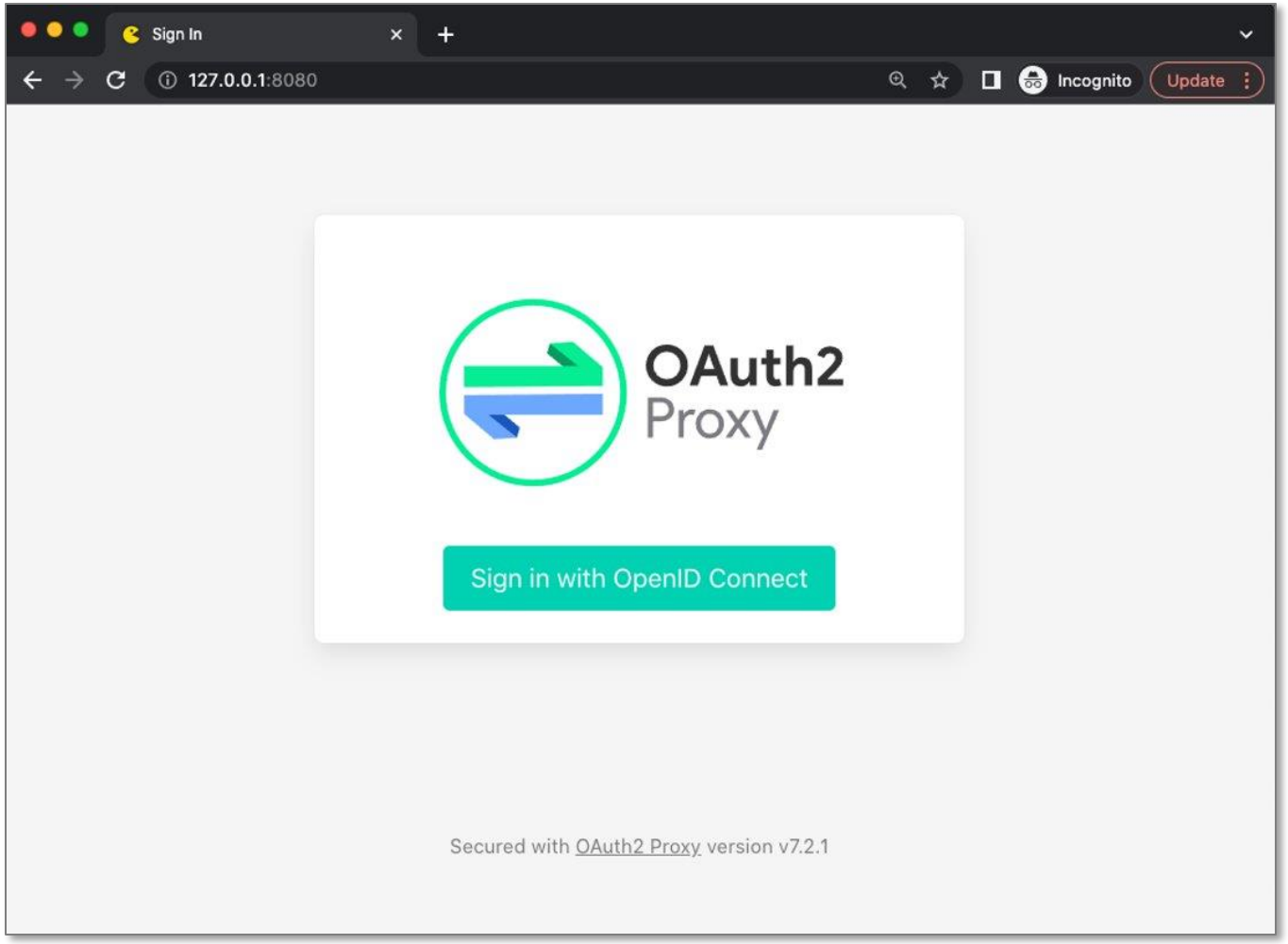
KASTEN by Veeam

Pac-Man – Look at the End Result

- `$ kubectl port-forward service/pacman -n pacman 9090:80`
- Open your web browser to http://127.0.0.1:**9090**

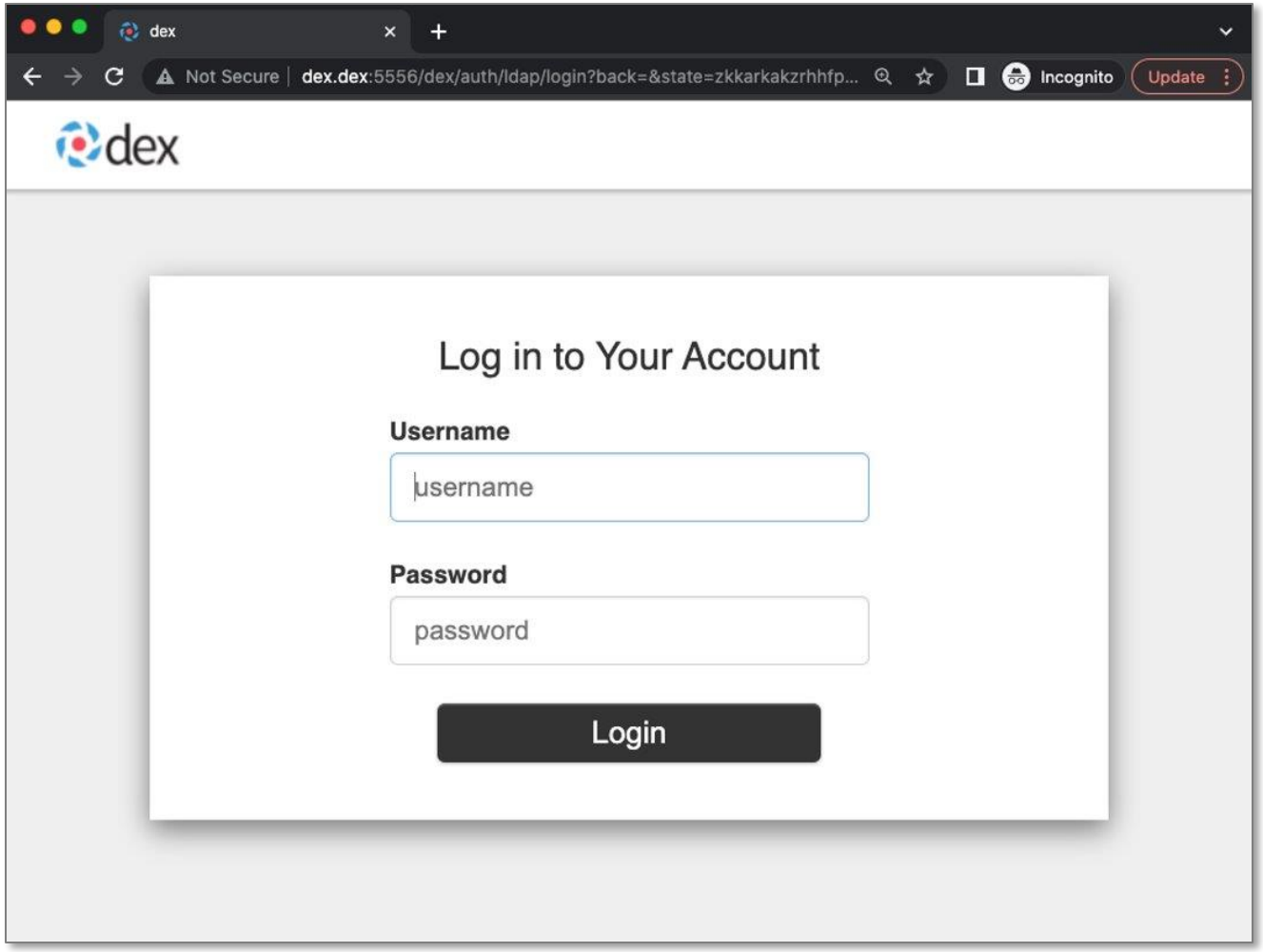
KASTEN by Veeam

Demo



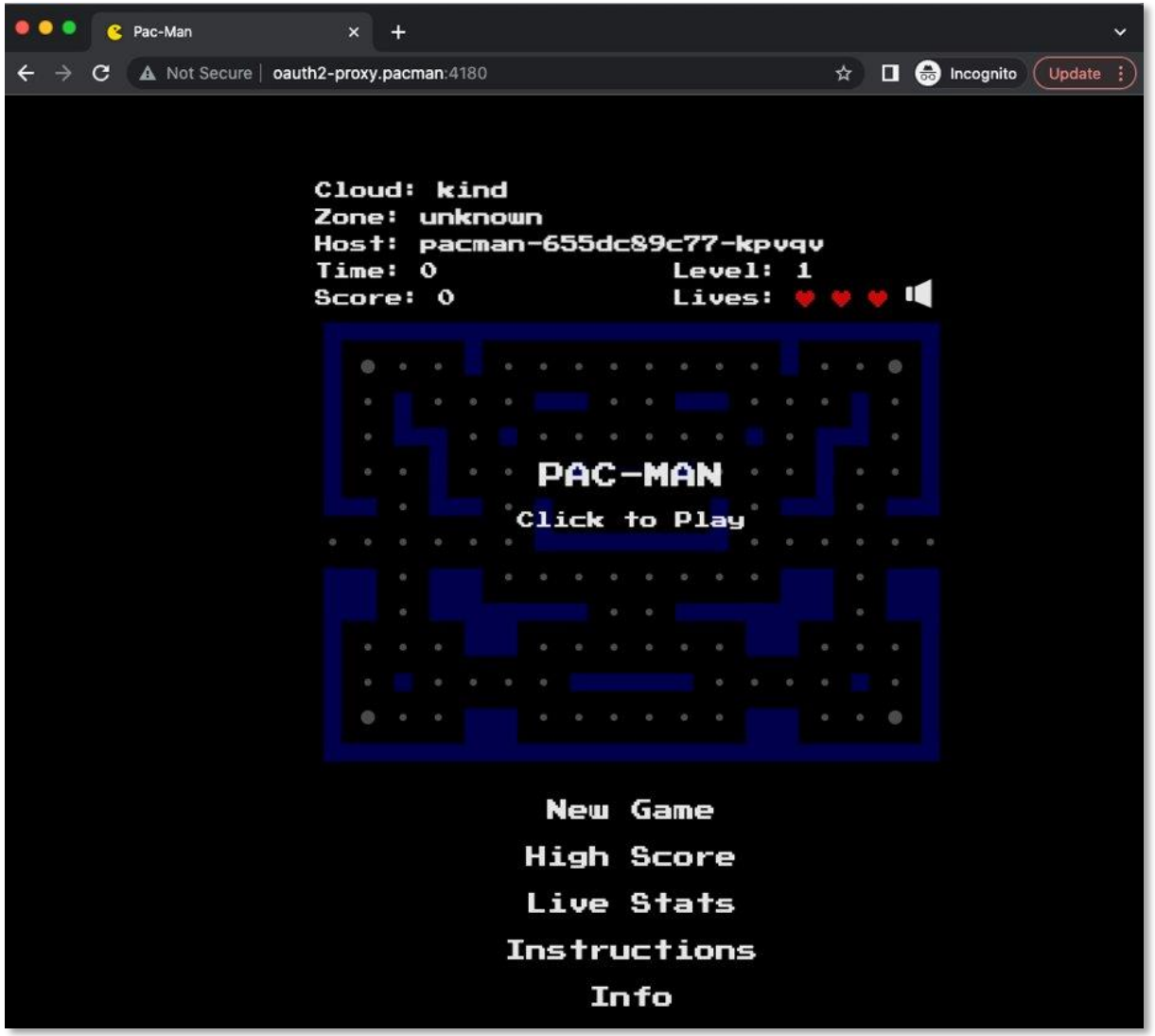
KASTEN by Veeam

Demo



KASTEN by Veeam

Demo



Hurray!

KASTEN by Veeam

Demo – Dex Logs

```
time="2022-05-05T22:36:16Z" level=info msg="performing ldap search
  ou=users,dc=example,dc=org sub
  (&(objectClass=inetOrgPerson)(uid=productionadmin))"

time="2022-05-05T22:36:16Z" level=info msg="username \"productionadmin\" mapped
  to entry cn=productionadmin,ou=users,dc=example,dc=org"

time="2022-05-05T22:36:16Z" level=info msg="performing ldap search
  dc=example,dc=org sub
  (&(objectClass=groupOfNames)(member=cn=productionadmin,ou=users,dc=example,
  dc=org))"

time="2022-05-05T22:36:16Z" level=info msg="login successful: connector \"ldap\",
  username=\"productionadmin\", preferred_username=\"productionadmin\",
  email=\"productionadmin\", groups=[\"readers\" \"pacmanAdmins\"]"
```


KASTEN by Veeam

Demo – Dex Logs

```
time="2022-05-05T22:36:35Z"  level=info msg="performing ldap search
ou=users,dc=example,dc=org sub
(&(objectClass=inetOrgPerson)(uid=productionconfig))"

time="2022-05-05T22:36:35Z"  level=info msg="username \"productionconfig\" mapped
to entry cn=productionconfig,ou=users,dc=example,dc=org"

time="2022-05-05T22:36:35Z"  level=info msg="performing ldap search
dc=example,dc=org sub
(&(objectClass=groupOfNames)(member=cn=productionconfig,ou=users,dc=example,dc
=org))"

time="2022-05-05T22:36:35Z"  level=info msg="login successful: connector \"ldap\",
username=\"productionconfig\", preferred_username=\"productionconfig\",
email=\"productionconfig\", groups=[\"readers\"]"
```


KASTEN by Veeam

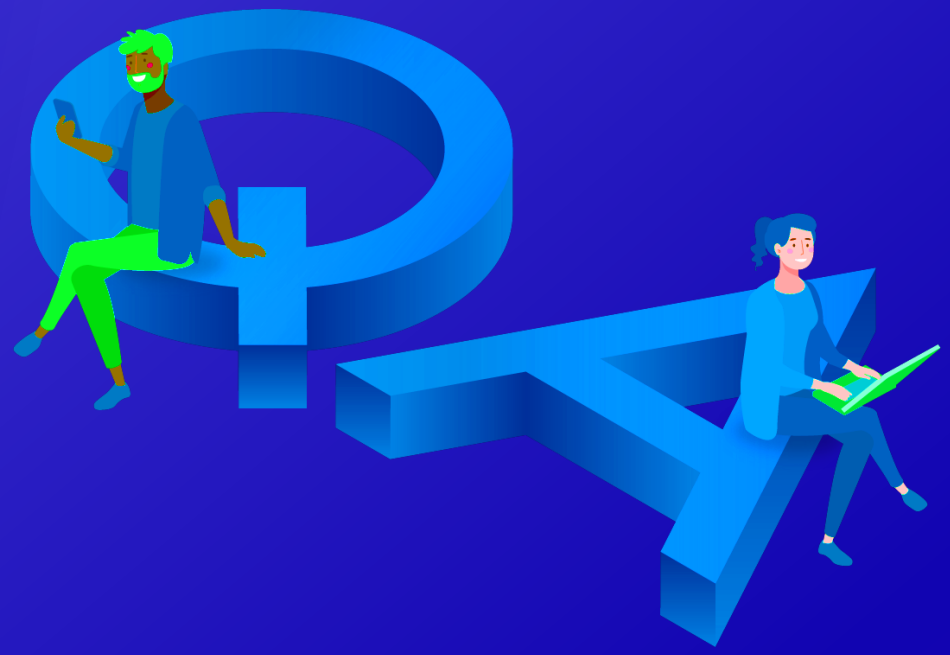
Switch to Production Active Directory Server

```
config:
  connectors:
  - config:
      bindDN: cn=admin,dc=example,dc=org
      bindPW: adminpassword
      groupSearch:
        baseDN: dc=example,dc=org
        filter: (objectClass=groupOfNames)
        nameAttr: cn
        userMatchers:
        - groupAttr: member
          userAttr: DN
      host: openldap.openldap:1389
      insecureNoSSL: true
      insecureSkipVerify: true
      startTLS: false
      userSearch:
        baseDN: ou=users,dc=example,dc=org
        emailAttr: uid
        filter: (objectClass=inetOrgPerson)
        idAttr: uid
        nameAttr: uid
        preferredUsernameAttr: uid
        username: uid
    id: ldap
    name: LDAP
    type: ldap
```

Further Reading

- Dex:
  - https://dexidp.io/
  - Slack: #dexidp at http://cloud-native.slack.com/
- OAuth2 proxy:
  - https://oauth2-proxy.github.io/oauth2-proxy/
- OpenLDAP:
  - https://www.openldap.org/
- Secure Pac-Man:
  - https://github.com/onkarbhat/secure-pacman

KASTEN by Veeam



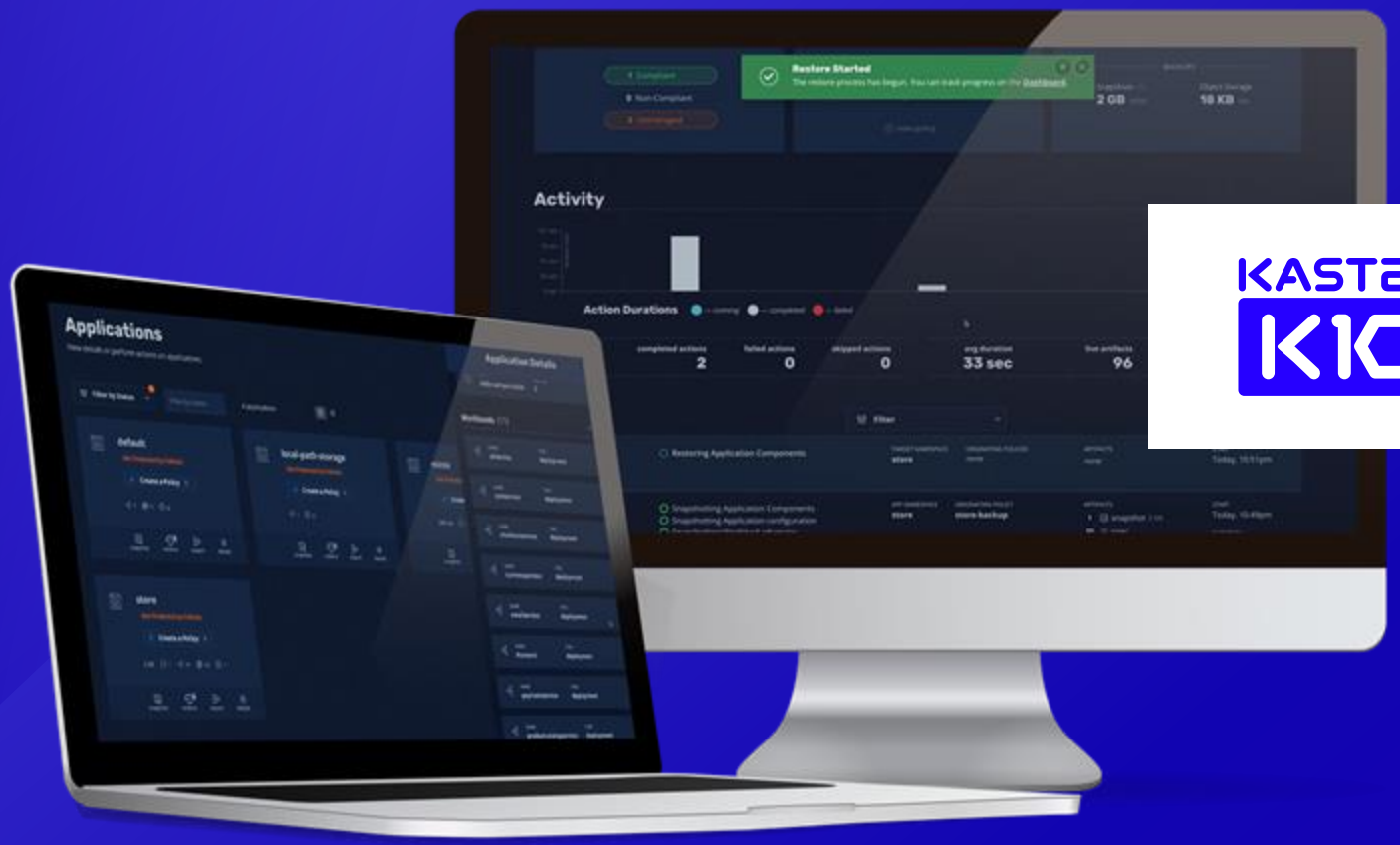
KASTEN
by Veeam

Thank You

We're hiring!

kasten.io/careers/

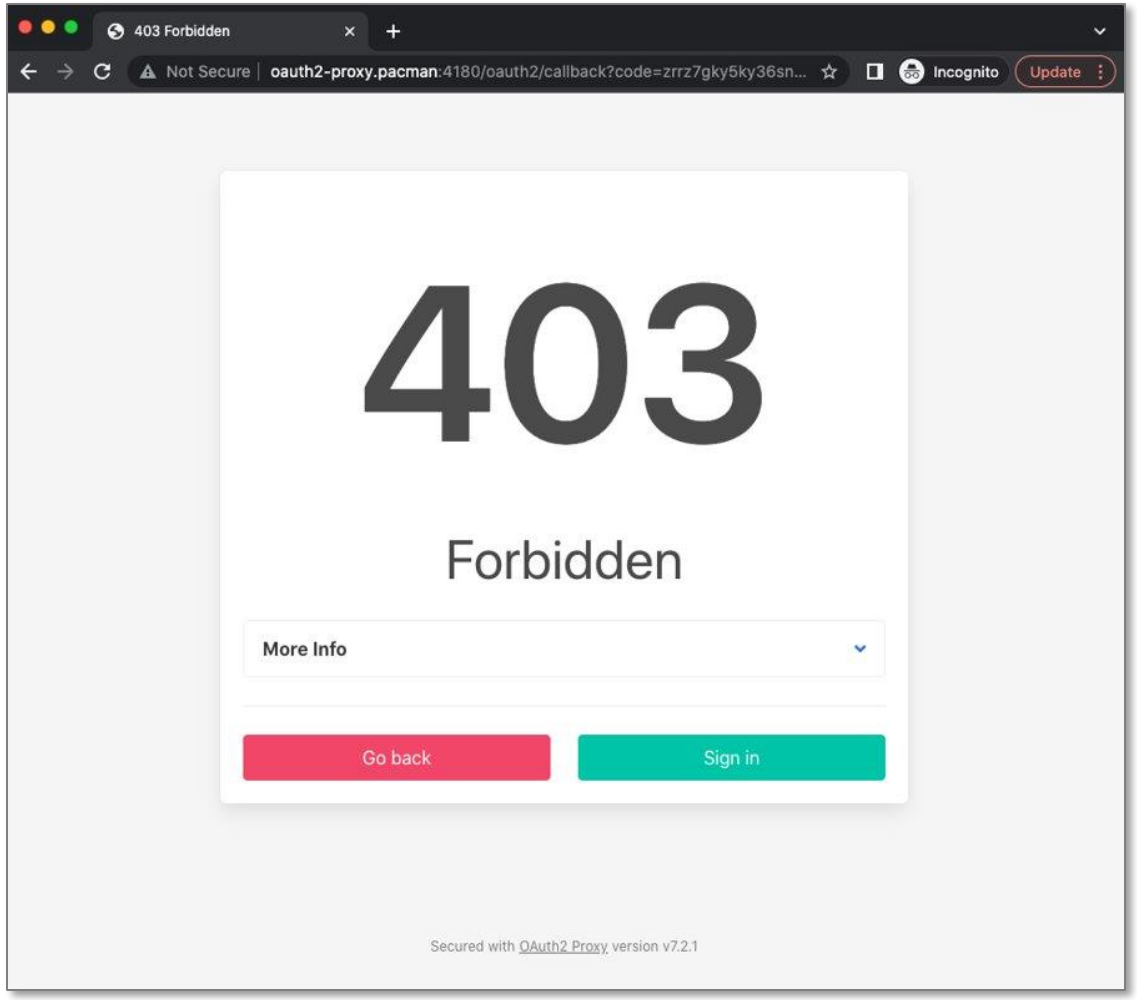
KASTEN
by Veeam



KASTEN K10

KASTEN by Veeam

Extra Slide



Extra Slide

Common Errors:

- The bindPW field in the dex-values.yaml file should be updated before installing Dex using helm. If you skip this, you will see an error about invalid credentials after logging in using the Dex login page.

- Did you update the /etc/hosts file with an entry for dex.dex ? If you skip this, you will get an error after clicking on the "Sign in with OpenID connect" button on the OAuth2 proxy login screen.

- Did you update the /etc/hosts file with an entry for oauth2-proxy.pacman ? If you skip this, you will get an error when Dex tries to redirect back to OAuth2 proxy after you enter the username and password on the Dex login screen.

KASTEN by Veeam