**LDAP Integration**

Installs OpenLDAP and phpLDAPadmin with a few initial users for the purposes of showing LDAP integration capabilities with Cloud Pak for Integration.

Connect to the bastian node and perform following operations.

**Installation:**

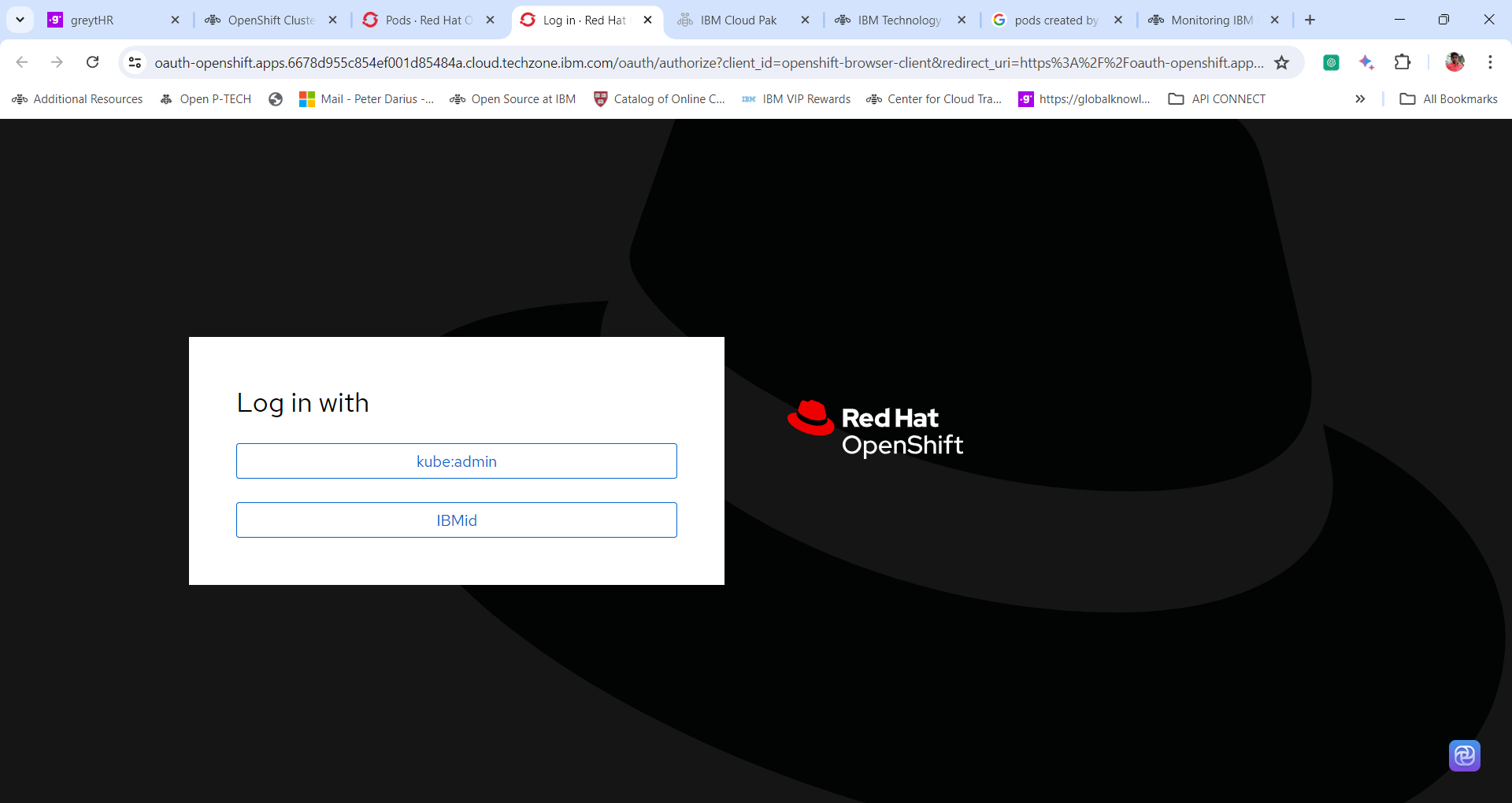
**OpenShift CLI Login Token**

1. Login into the Red Hat OpenShift Console with the provided user id and password.

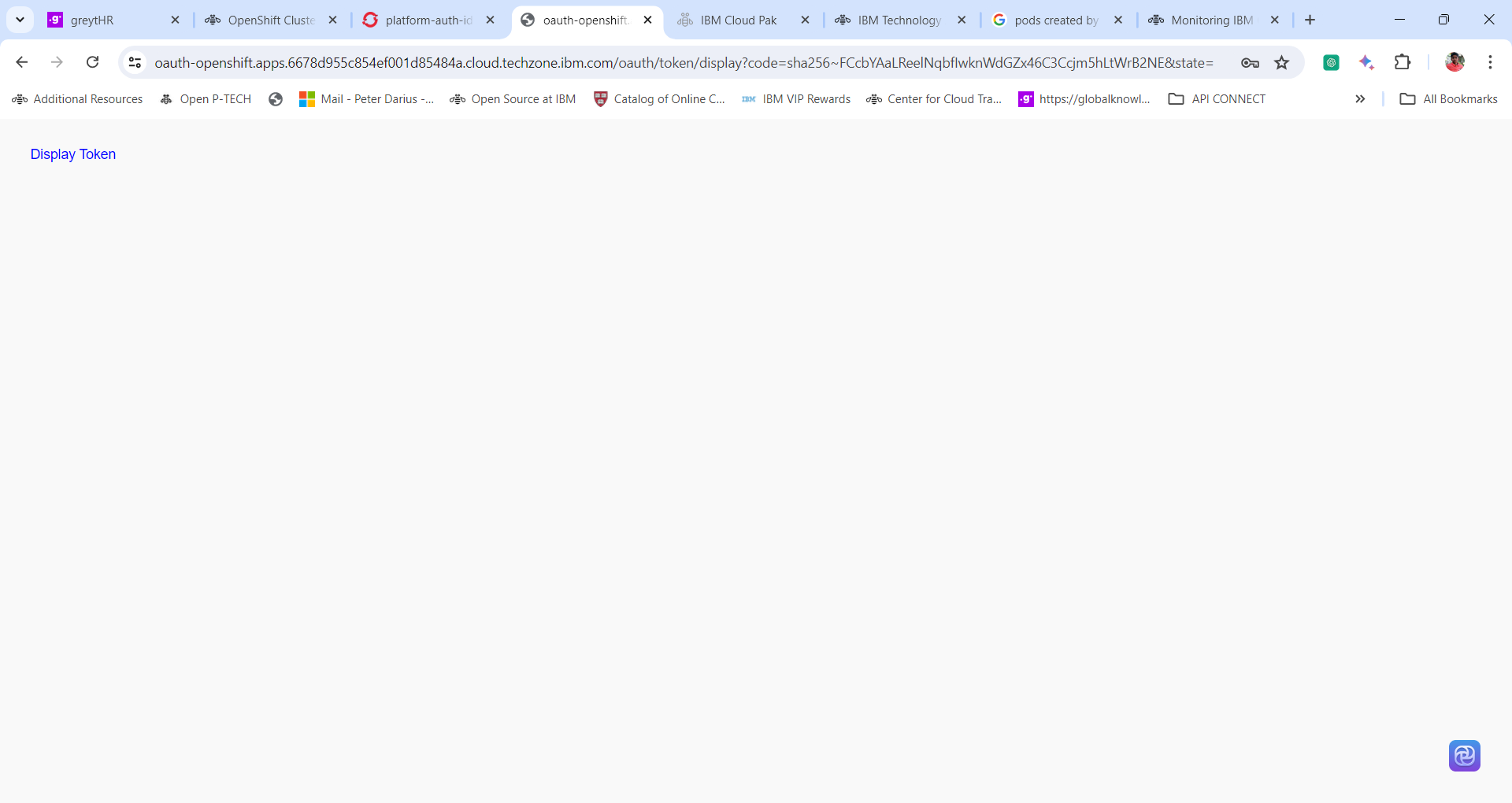
2. Go to the top right corner of the console and expand **kube:admin** and click on **Copy login command**.



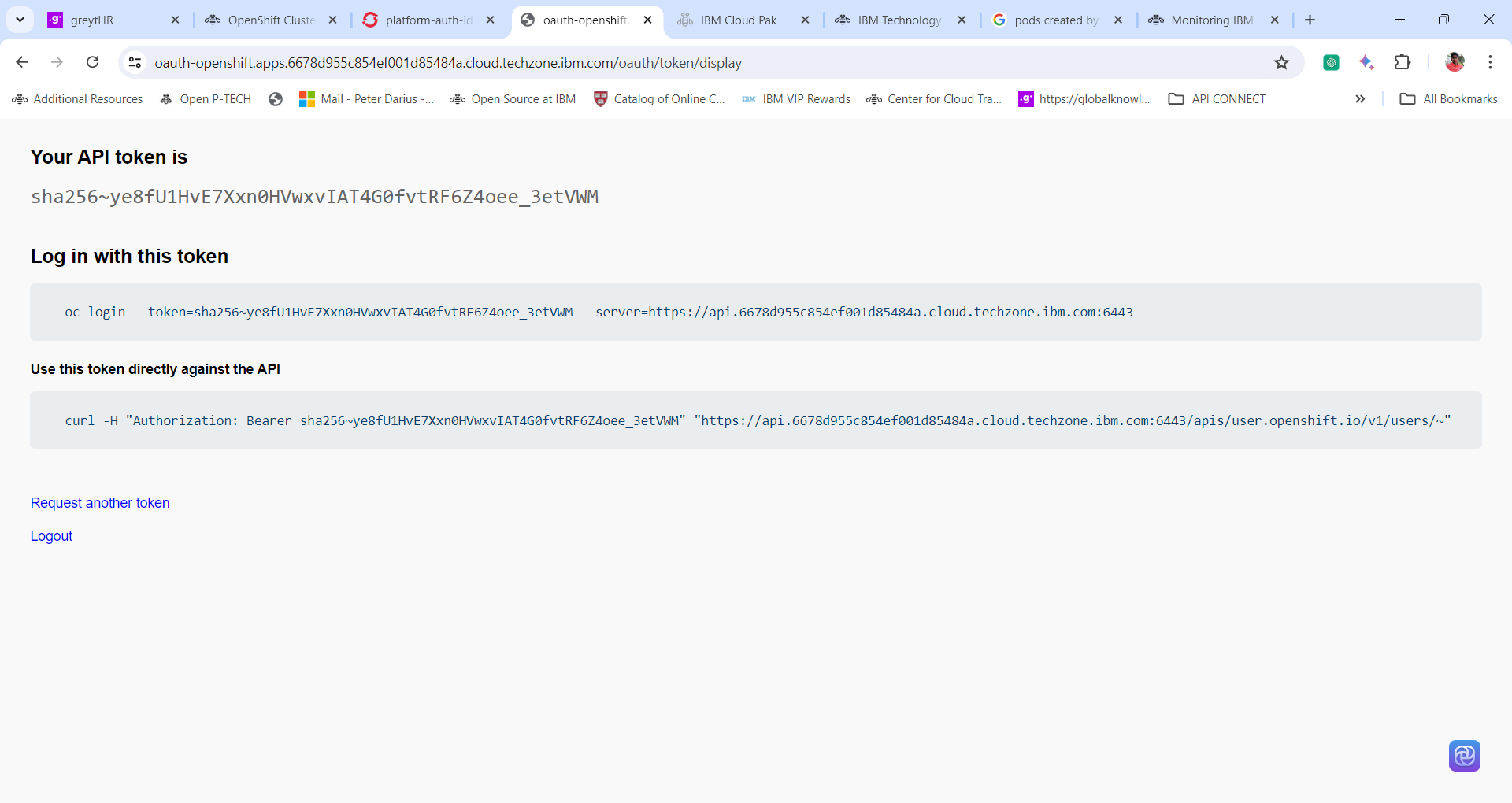
3. In a new tab once again login into the Red Hat OpenShift Console if prompted, else follow the next step.



4. Once logged in, click on **Display Token**.



5. Copy the token under **Log in with this token**.



**Login to the OpenShift Cluster from CLI**

1. Use the above Token and paste it in the terminal to login to the OpenShift Cluster from the Command Line.

**oc login --token=sha256~jZGpi6\_NtqvqwHMjoGieACMQybG5-de-Hq6XE3d9gx0 --server=https://api.daffy-3ajt4xen.cloud.techzone.ibm.com:6443**

**Note:** The above token changes as per the cluster, so copy the login token for your cluster.

2. **RELEASE\_NAME=cp4i-openldap**

**$ NAMESPACE=cp4i-ldap**

**$ oc new-project $NAMESPACE**

**$ oc adm policy add-scc-to-user anyuid -z default -n $NAMESPACE**

3. Install the Helm binary **(If you get an authentication error try to use sudo with below commands. Ex. Sudo curl ….., sudo chmod…. Sudo helm install …… etc)**

**$ curl -L https://mirror.openshift.com/pub/openshift-v4/clients/helm/latest/helm-linux-amd64 -o /usr/local/bin/helm**

4. Make the binary file executable

**chmod +x /usr/local/bin/helm**

5. Check the installed version:

**helm version**

**Sample Output:**

**version.BuildInfo{Version:"v3.0", GitCommit:"b31719aab7963acf4887a1c1e6d5e53378e34d93", GitTreeState:"clean", GoVersion:"go1.13.4"}**

6. Run the command to install the openldap

**helm install $RELEASE\_NAME https://github.com/ccavazos/cp4i-openldap/releases/download/0.1.7/cp4i-openldap-0.1.7.tgz --namespace $NAMESPACE**

Output:

**NAME: cp4i-openldap**

**LAST DEPLOYED: Thu Aug 27 18:20:27 2020**

**NAMESPACE: cp4i-ldap**

**STATUS: deployed**

**REVISION: 1**

**TEST SUITE: None**

### 7. Manage users via OpenShift

To get the information of the users created check the config map

**~ oc describe configmap cp4i-openldap-seedusers -n $NAMESPACE**

------------------------------------------------------------------------------------------------------------------------------------------------------------

**Optional:**

If you need to edit the configmap then provide the following command to edit and then save.

**oc edit configmap cp4i-openldap-seedusers**

If the edit is successful, meaning there are no syntax errors, something like this should be returned.

**configmap/cp4i-openldap-seedusers edited**

If you do changes to the users (add, edit, remove) make sure you delete the pod

**$ oc get pods**

**NAME READY STATUS RESTARTS AGE**

**cp4i-openldap-67676b9c5b-tft6x 1/1 Running 0 2m**

**cp4i-openldap-admin-5c98969977-rt2np 1/1 Running 0 2m**

**$ oc delete pod cp4i-openldap-67676b9c5b-tft6x -n $NAMESPACE pod "cp4i-openldap-67676b9c5b-tft6x" deleted**

The deployment will recreate the pod automatically and the changes will be loaded.

**Read the following and Jump to LDAP integration with CP4I section**

**Assets:**

**Configmap: cp4i-openldap-seedusers.yaml file**

kind: ConfigMap

apiVersion: v1

metadata:

  name: cp4i-openldap-seedusers

  namespace: cp4i-openldap

  uid: 7d61de7b-f4d3-437b-a276-19da4db9bd00

  resourceVersion: '5434855'

  creationTimestamp: '2023-10-11T01:43:47Z'

  labels:

    app.kubernetes.io/managed-by: Helm

  annotations:

    meta.helm.sh/release-name: cp4i-openldap

    meta.helm.sh/release-namespace: cp4i-openldap

  managedFields:

    - manager: helm

      operation: Update

      apiVersion: v1

      time: '2023-10-11T01:43:47Z'

      fieldsType: FieldsV1

      fieldsV1:

        'f:data':

          .: {}

          'f:seedusers.ldif': {}

        'f:metadata':

          'f:annotations':

            .: {}

            'f:meta.helm.sh/release-name': {}

            'f:meta.helm.sh/release-namespace': {}

          'f:labels':

            .: {}

            'f:app.kubernetes.io/managed-by': {}

data:

  seedusers.ldif: |

    dn: ou=Groups,dc=ibm,dc=com

    changetype: add

    objectclass: organizationalUnit

    ou: Groups

    # Add People OU

    dn: ou=People,dc=ibm,dc=com

    changetype: add

    objectclass: organizationalUnit

    ou: People

    # Add users

    dn: uid=user1,ou=People,dc=ibm,dc=com

    changetype: add

    objectclass: inetOrgPerson

    objectclass: organizationalPerson

    objectclass: person

    objectclass: top

    uid: user1

    displayname: user1

    sn: user1

    cn: user1

    userpassword: cp4iForAll

    dn: uid=user2,ou=People,dc=ibm,dc=com

    changetype: add

    objectclass: inetOrgPerson

    objectclass: organizationalPerson

    objectclass: person

    objectclass: top

    uid: user2

    displayname: user2

    sn: user2

    cn: user2

    userpassword: cp4iForAll

    dn: uid=user3,ou=People,dc=ibm,dc=com

    changetype: add

    objectclass: inetOrgPerson

    objectclass: organizationalPerson

    objectclass: person

    objectclass: top

    uid: user3

    displayname: user3

    sn: user3

    cn: user3

    userpassword: cp4iForAll

    dn: uid=user4,ou=People,dc=ibm,dc=com

    changetype: add

    objectclass: inetOrgPerson

    objectclass: organizationalPerson

    objectclass: person

    objectclass: top

    uid: user4

    displayname: user4

    sn: user4

    cn: user4

    userpassword: cp4iForAll

    # Create ICP user group

    dn: cn=cp4iusers,ou=Groups,dc=ibm,dc=com

    changetype: add

    cn: cp4iusers

    objectclass: groupOfUniqueNames

    objectclass: top

    owner: cn=admin,dc=ibm,dc=com

    uniquemember: uid=user1,ou=People,dc=ibm,dc=com

    uniquemember: uid=user2,ou=People,dc=ibm,dc=com

    uniquemember: uid=user3,ou=People,dc=ibm,dc=com

    uniquemember: uid=user4,ou=People,dc=ibm,dc=com

**All the users are available in this configmap if needed we can edit this yaml file.**

### OpenLDAP

OpenLdap:

OpenLdap:

Image: "docker.io/osixia/openldap"

ImageTag: "1.4.0"

ImagePullPolicy: "Always"

Component: "openldap"

Replicas: 1

Cpu: "512m"

Memory: "200Mi"

Organisation: "Example Inc."

Domain: "ibm.com"

AdminPassword: "Passw0rd!"

SeedUsers:

usergroup: "cp4iusers"

userlist: "user1,user2,user3,user4"

initialPassword: "cp4iForAll"

### phpLDAPadmin

Default values:

PhpLdapAdmin:

Component: "phpadmin"

Image: "docker.io/osixia/phpldapadmin"

ImageTag: "0.9.0"

ImagePullPolicy: "Always"

Replicas: 1

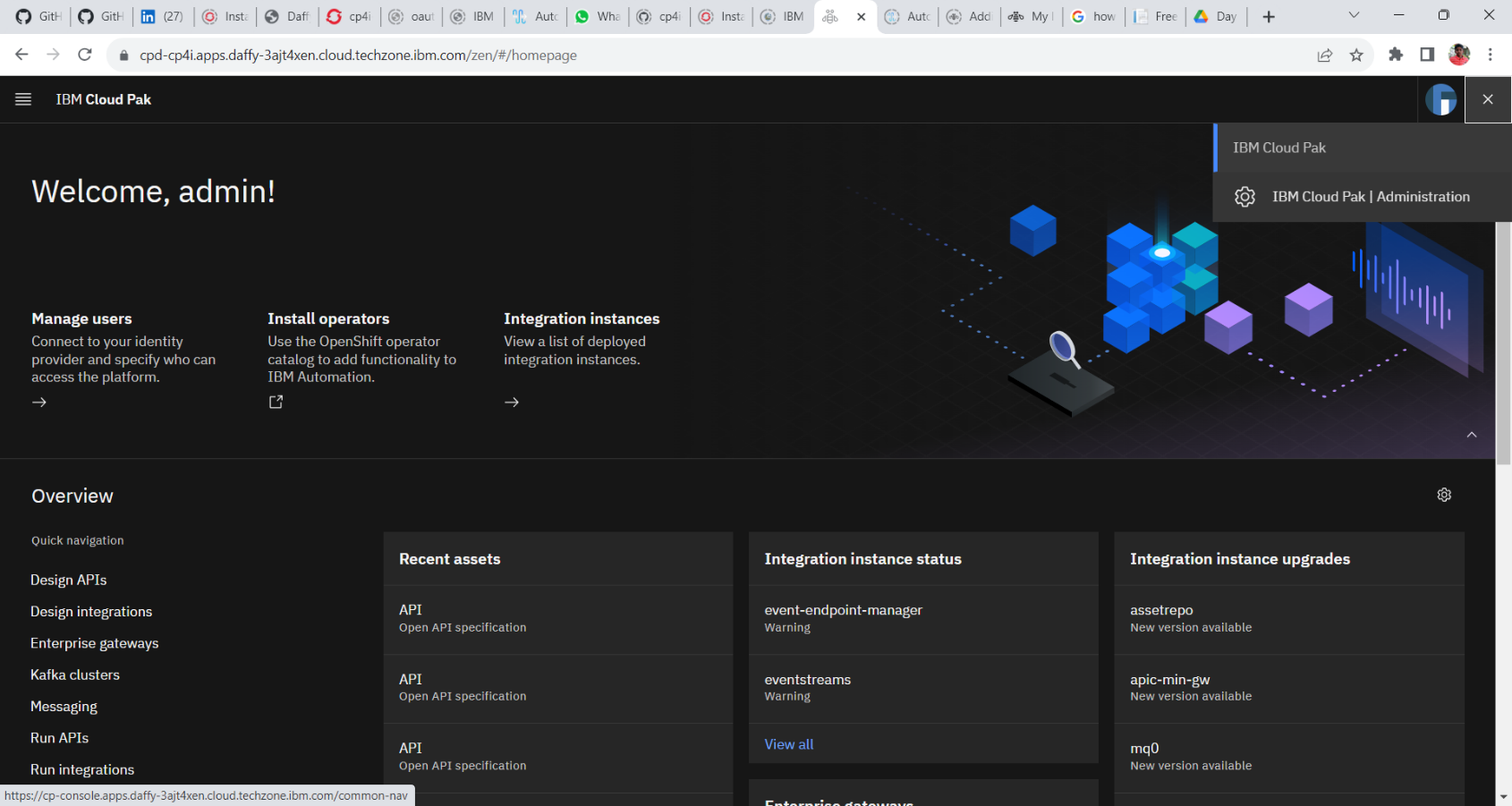
Cpu: "512m"

Memory: "200Mi"

Https: "false"

**LDAP Integration with CP4I**

1. Open the IBM Cloud Pak for Integration **Platform Navigator**. After login switch location to **IBM Cloud Pak Administration**. Click **IBM Cloud Pak Administration**.

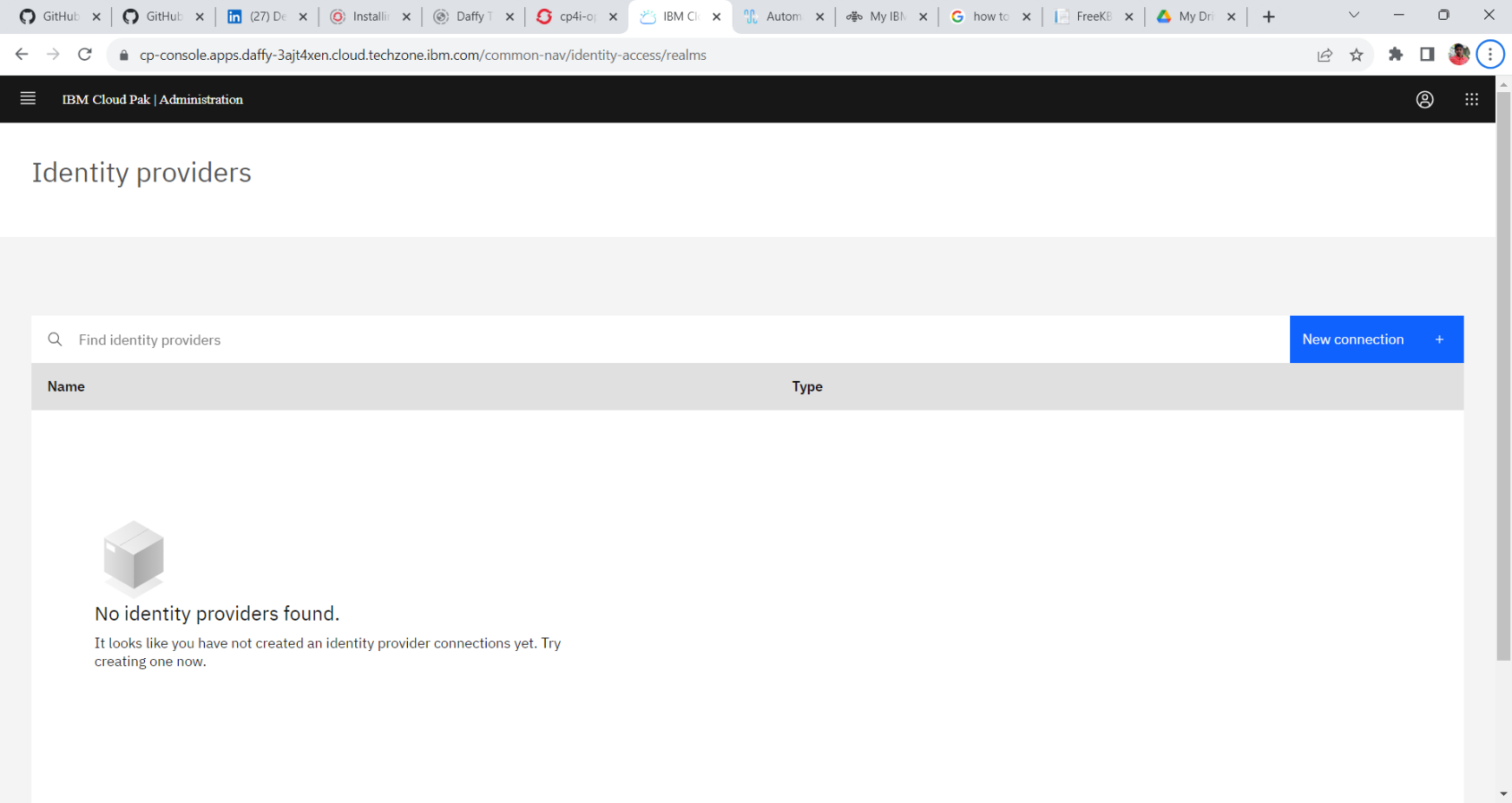


2. Expand the menu **Identity and access** and click **Identity Providers**.

A computer screen with a black screen

Description automatically generated

3. In the Identity providers windows Click **New Connections**.



5. Select the Identity provider has **LDAP** and click **Next**.

A screenshot of a computer

Description automatically generated

4. In the New Connection window provide the following configuration to configure the connection to the openldap configured with the cluster.

**Connection Details**

**Name: newconnection**

**Server Type: custom**

**Base DN: dc=ibm,dc=com**

**Bind DN: cn=admin,dc=ibm,dc=com**

**Bind DN Password: Passw0rd!**

A screenshot of a computer

Description automatically generated**LDAP Server URL: ldap://cp4i-openldap.cp4i-openldap.svc.cluster.local:389**

A screenshot of a computer

Description automatically generated

5. Enter the Server URL and click on Test Connection.

A screenshot of a computer

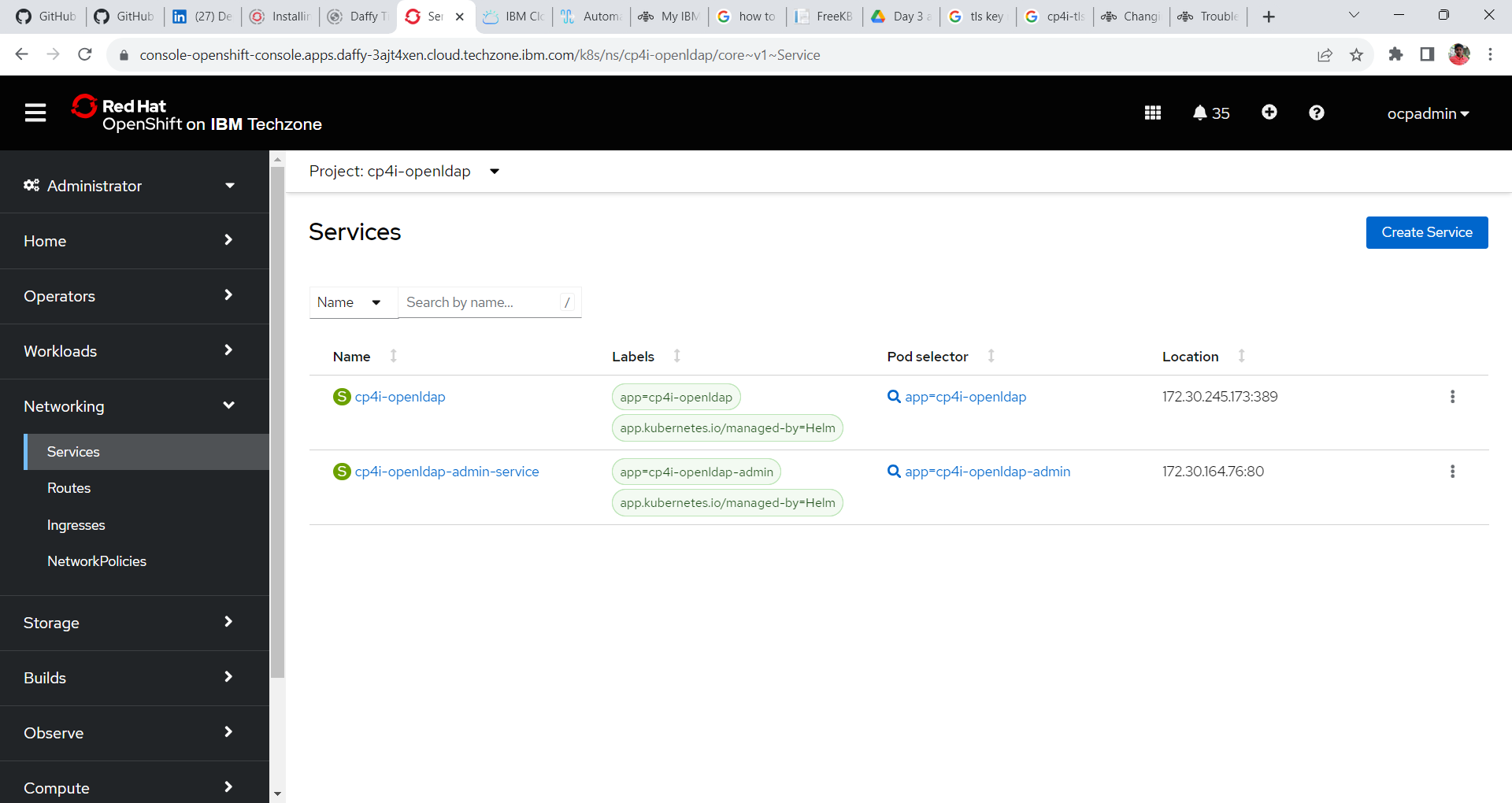
Description automatically generated

---------------------------------------------------------------------------------------------------------------------------------------------------------

**To get the Server URL follow the procedure given below:**

1. Go to **OpenShift Web Console**.

2. Navigate to **Networking** and click **Services**.



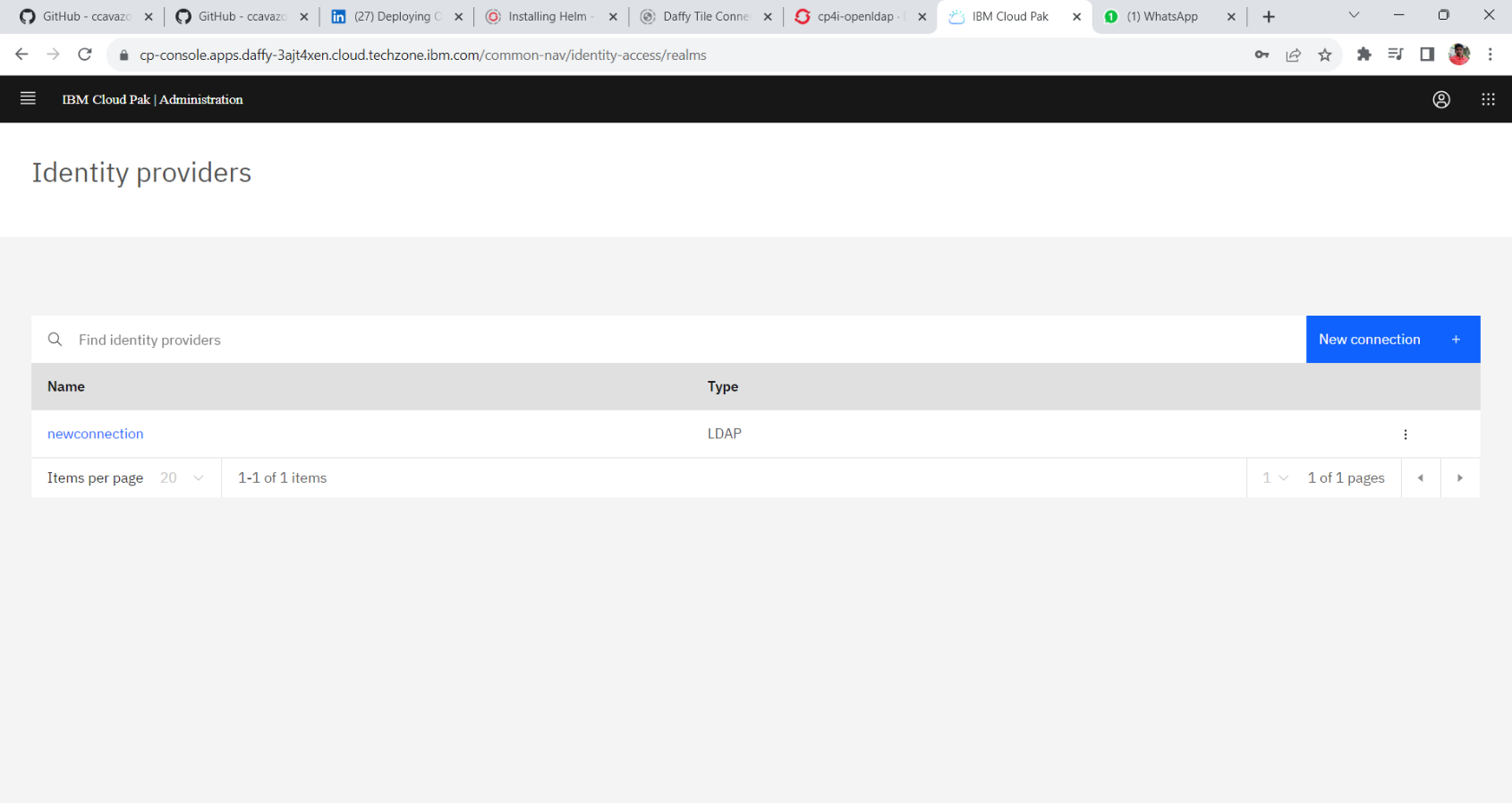
3. Change the **project name** to **cp4i-openldap** (Project under which you have installed the open ldap). Click on the services **cp4i-openldap** and locate **hostname and the port number**.



A screenshot of a computer

Description automatically generated6. Update the **filter values**:

Change the user filter value from (&(uid=%v)(objectclass-**ePerson**)) to (&(uid=%v)(objectclass-**Person**))

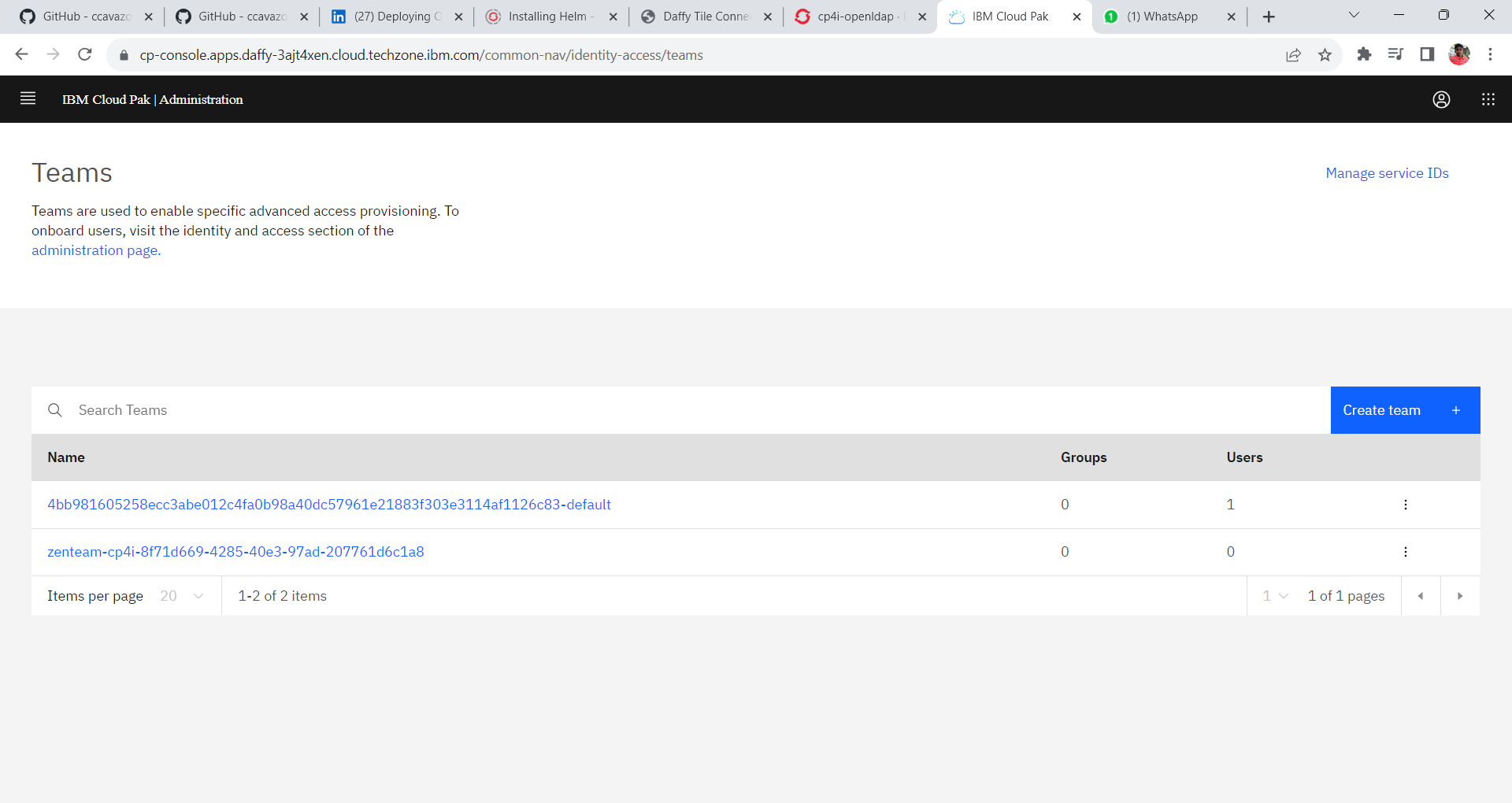
7. Click **Create**.

8. from the Menu navigate to **Identity and access** and click **Teams and Service IDs**.

A screenshot of a computer

Description automatically generated

9. In the Teams window the group id is listed with 1 user. Now let’s create a team or a group of users. Click **Create team**.

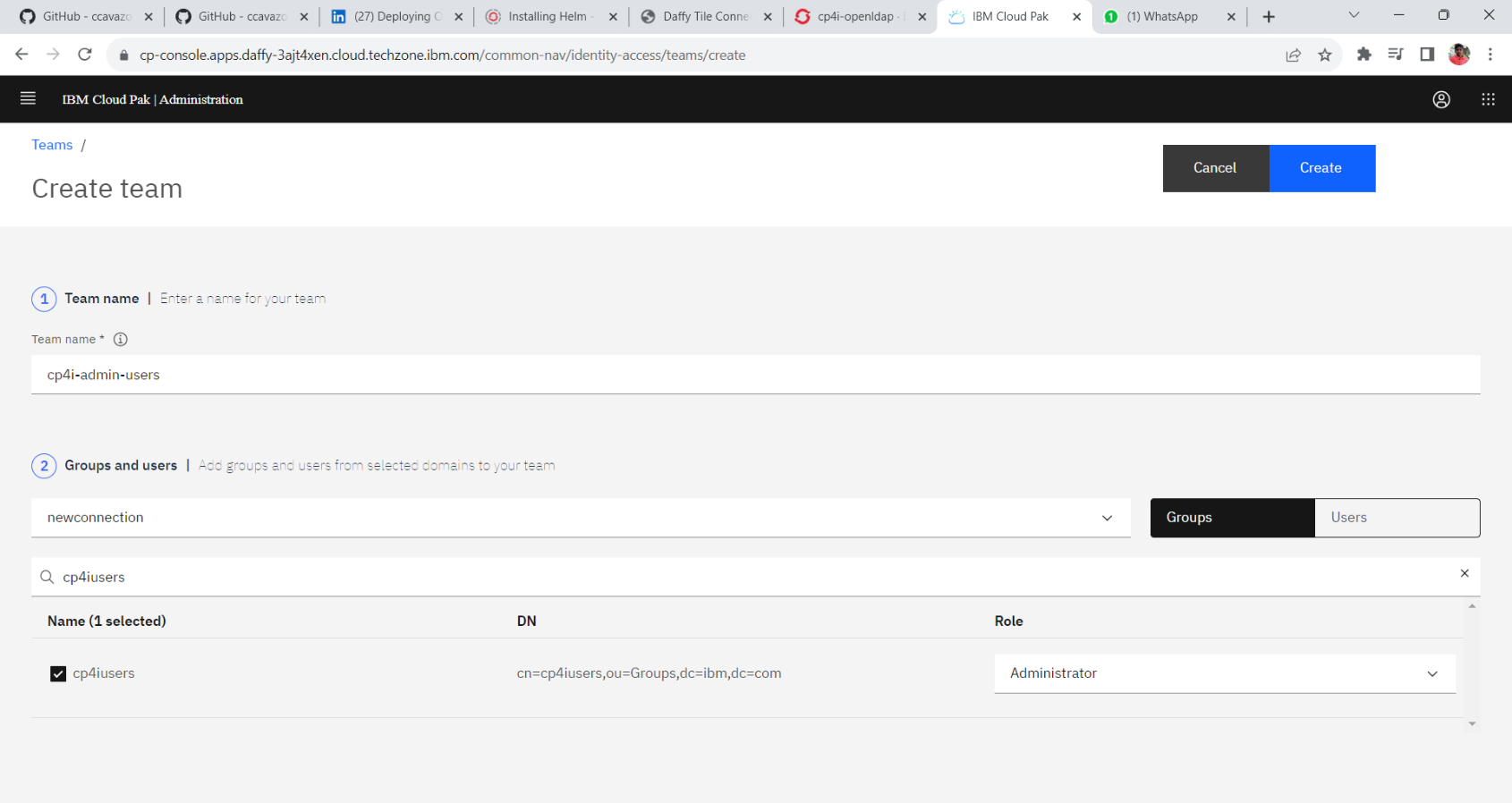


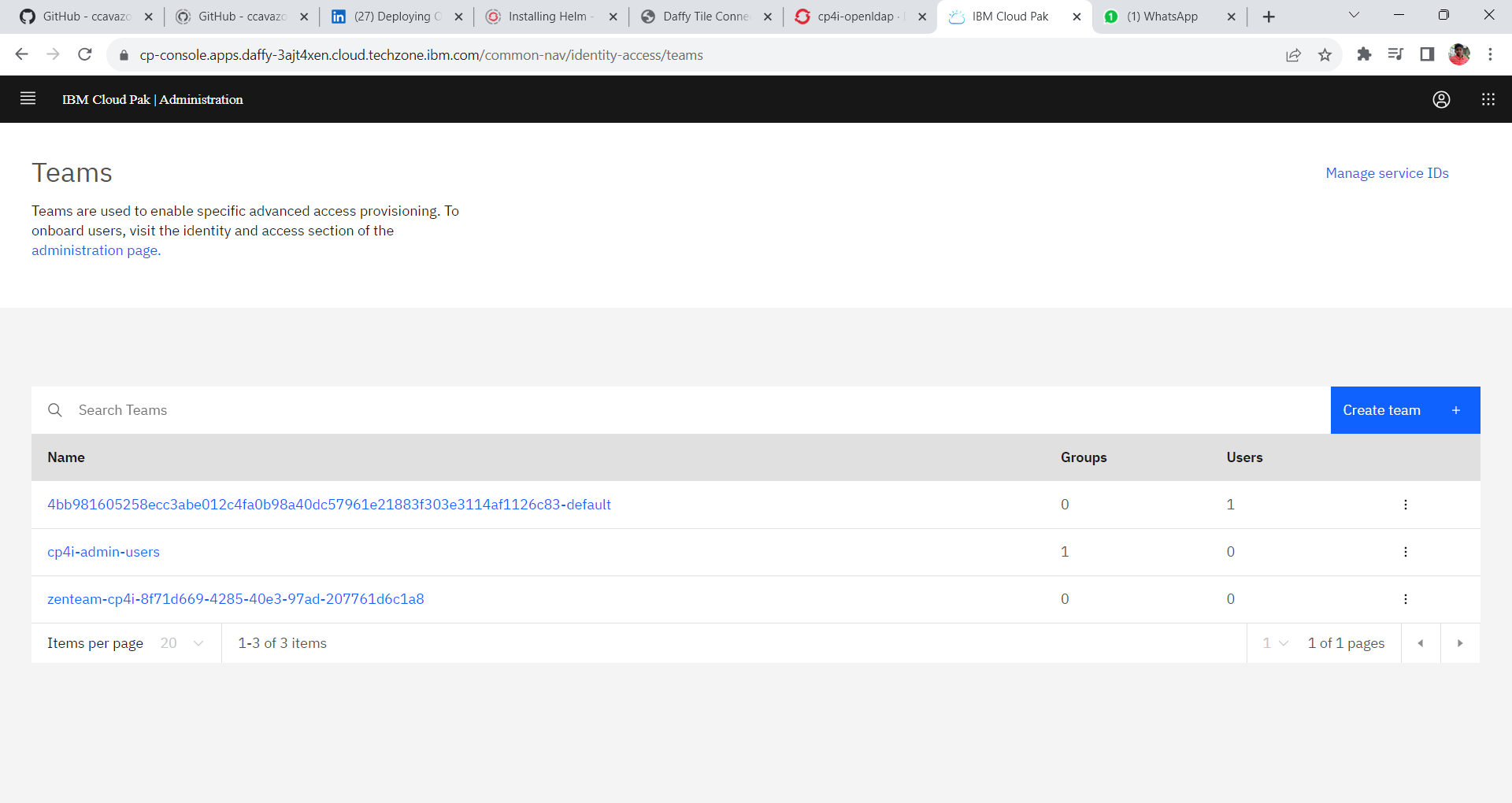
10. In the Create Teams window create a teams by providing the following details

**Team Name: cp4i-admin-users**

**Groups and Users: newconnection (Select the connection created)**

In the search bar search for the following group **cp4iusers**. Once the group cp4iusers is listed select the group and provide the role as Administrator and click create to create a team.



11. In the teams windows find the created teams.

A screenshot of a computer

Description automatically generated12. Let’s create a team with a user who has a cluster administrator role. Click **Create Team**.

13. In the create team window provide the following values.

**Team Name: cp4i-cluster-admin**

**Groups and Users: newconnection and select the Users button**

**In the search box search for user1 and select user1 and change the role to clusteradministrator.**

**Click Create a team with one user.**



14. In the teams window the newly created team is listed.

15. In order to the users logout of the Platform Navigator and login again the user available in the ldap. Open an incognito window and open the platform navigator. Select Enterprise LDAP.

A screenshot of a computer

Description automatically generated

16. Provide the following **credentials and login**

**Username: user1**

**Password: cp4iForAll**

After verifying logout from the Platform Navigator.