

### Lab3. Аутентификация и авторизация.

Чтобы пользователи могли взаимодействовать с OpenShift Container Platform, они должны сначала пройти аутентификацию в кластере. Уровень аутентификации идентифицирует пользователя, связанного с запросами к API OpenShift Container Platform. Затем уровень авторизации использует информацию о запрашивающем пользователе, чтобы определить, разрешен ли запрос.

Пользователь в OpenShift Container Platform — это сущность, которая может делать запросы к API OpenShift Container Platform. Объект OpenShift Container Platform User представляет субъекта, которому могут быть предоставлены разрешения в системе путем добавления ролей к ним или к их группам.

#### Группы

Пользователь может быть отнесен к одной или нескольким группам, каждая из которых представляет определенный набор пользователей. Группы полезны для одновременного предоставления разрешений нескольким пользователям, например, предоставления доступа к объектам в рамках проекта вместо предоставления их пользователям по отдельности.

#### OAuth-сервер

Мастер нод OpenShift Container Platform включает встроенный сервер OAuth.

Пользователи получают от него токены доступа для аутентификации в API.

Когда субъект запрашивает новый токен OAuth, сервер OAuth использует настроенного поставщика удостоверений, чтобы определить identity, делающего запрос.

Затем он определяет, с каким пользователем сопоставляется это удостоверение (identity) и создает маркер доступа для этого пользователя.

#### Упражнение 1. Настройка аутентификации

Если вы хотите, чтобы дополнительные пользователи могли аутентифицироваться и использовать кластер, вы должны настроить поставщика аутентификации.

Поставщик OAuth HTPasswd

Этот провайдер проверяет пользователей по секрету, который содержит имена пользователей и пароли, сгенерированные с помощью команды **htpasswd** из проекта HTTP-сервера Apache.

#### Задание 1. Предварительные требования.

Поскольку мы будем использовать метод аутентификации kubeconfig для добавления провайдера HTPasswd в OpenShift. Для этой операции требуется клиент oc

Если хостовая машина Linux:

## OpenShift Administration: Operating a Production Kubernetes Cluster

wget [https://mirror.openshift.com/pub/openshift-v4/x86\\_64/clients/ocp/stable/openshift-client-linux.tar.gz](https://mirror.openshift.com/pub/openshift-v4/x86_64/clients/ocp/stable/openshift-client-linux.tar.gz)

```
tar -xvf openshift-client-linux.tar.gz
```

```
sudo mv oc kubectrl /usr/local/bin
```

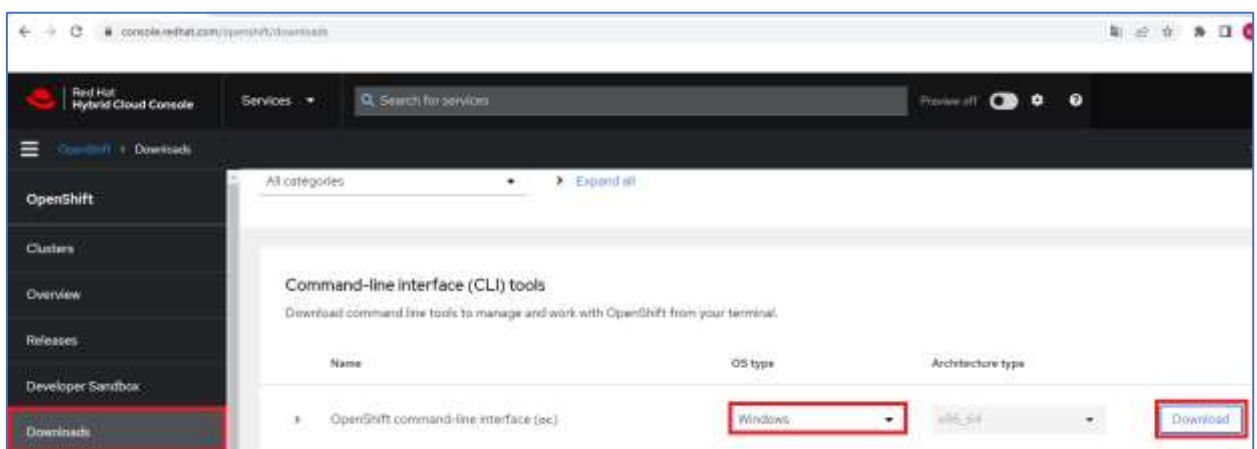
```
mkdir .kube
```

```
mv kubeconfig .kube/config
```

```
oc login --username=kubeadmin
```

Если хостовая машина Windows 10:

<https://console.redhat.com/openshift/downloads>



Скачать и сохранить под именем oc.exe в C:\Windows

### Задание 2. Настройка поставщика удостоверений HTTPasswd

Мы начнем с создания необходимого файла htpasswd, в котором будут храниться учетные данные пользователя.

#### Шаг 1. Установите htpasswd:

В случае ОС CentOS / RHEL / Fedora:

```
sudo yum -y install httpd-tools
```

В случае ОС Ubuntu / Debian:

```
sudo apt install apache2-utils
```

#### Шаг 2. Создание файла HTTPasswd

Создайте файл htpasswd:

```
htpasswd -c -B -b ocp_users.htpasswd user1 password1
```

**Прим.** Чтобы добавить или обновить учетные данные, используйте:

## OpenShift Administration: Operating a Production Kubernetes Cluster

```
htpasswd -Bb ocp_users.htpasswd user2 password2
```

```
htpasswd -Bb ocp_users.htpasswd user3 password3
```

Проверьте, что файл создан:

```
$ cat ocp_users.htpasswd
```

**Прим.** Чтобы удалить пользователя из htpasswd, можно выполнить следующую команду:

```
$ htpasswd -D ocp_users.htpasswd user3
```

### Задание 3. Создать секрет HTTPasswd

Нам нужно определить секрет, содержащий пользовательский файл HTTPasswd, прежде чем мы сможем использовать поставщика удостоверений HTTPasswd. Секрет, это объект в OpenShift для хранения записей из внешнего ресурса (файла htpasswd).

```
oc create secret generic htpass-secret --from-file=htpasswd=./ocp_users.htpasswd -n openshift-config
```

#### Или можно в консоли:

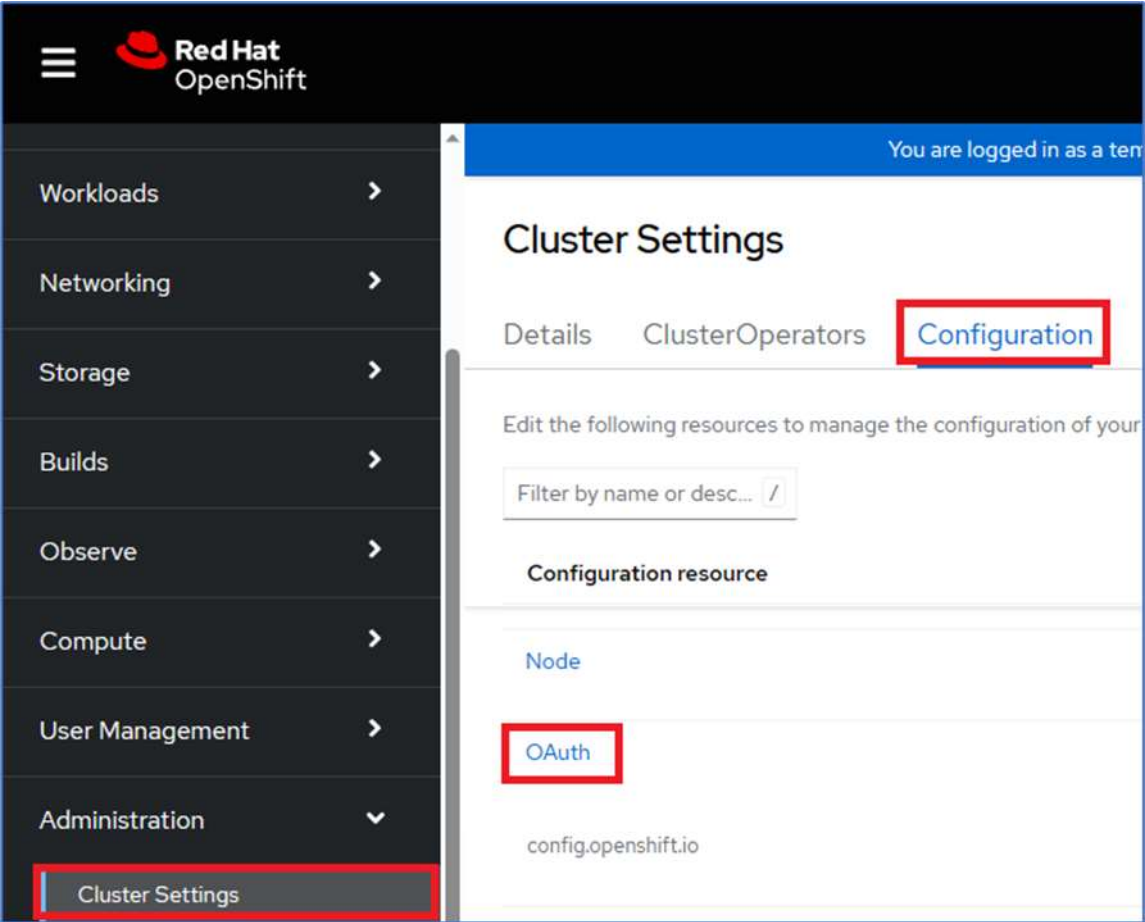
Тогда файл нужно скопировать в директорию доступную с хоста, на котором открыта консоль.

Например: `scp michael@192.168.0.2:ocp_users.htpasswd .`

Зайдите в консоль ->Administration ->Cluster Settings:

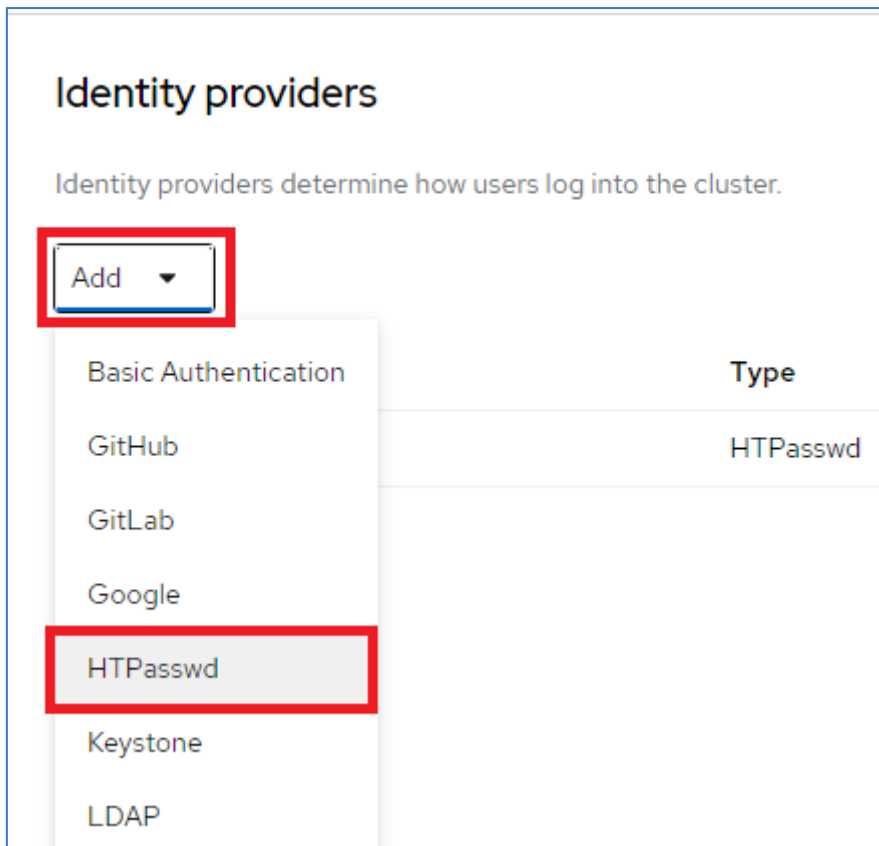
Откройте вкладку Configuration

Найдите и кликните по OAuth



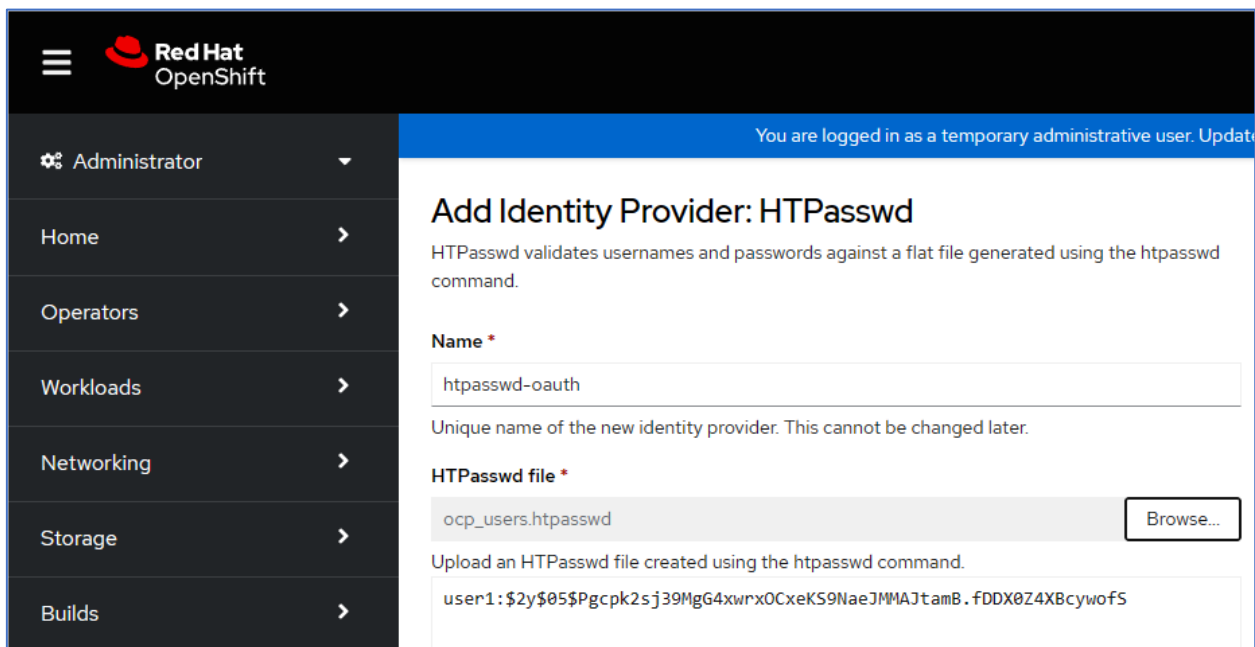
## OpenShift Administration: Operating a Production Kubernetes Cluster

В разделе Identity providers нажмите Add и из выпадающего списка выберите HTPasswd:



Введите произвольное имя, например httpasswd-secret

И нажав Browse укажите путь к файлу httpasswd

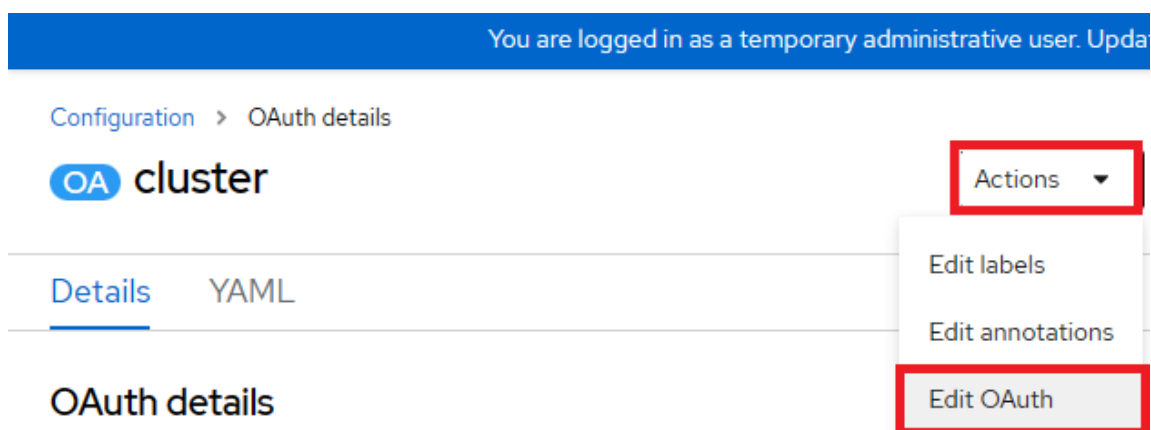
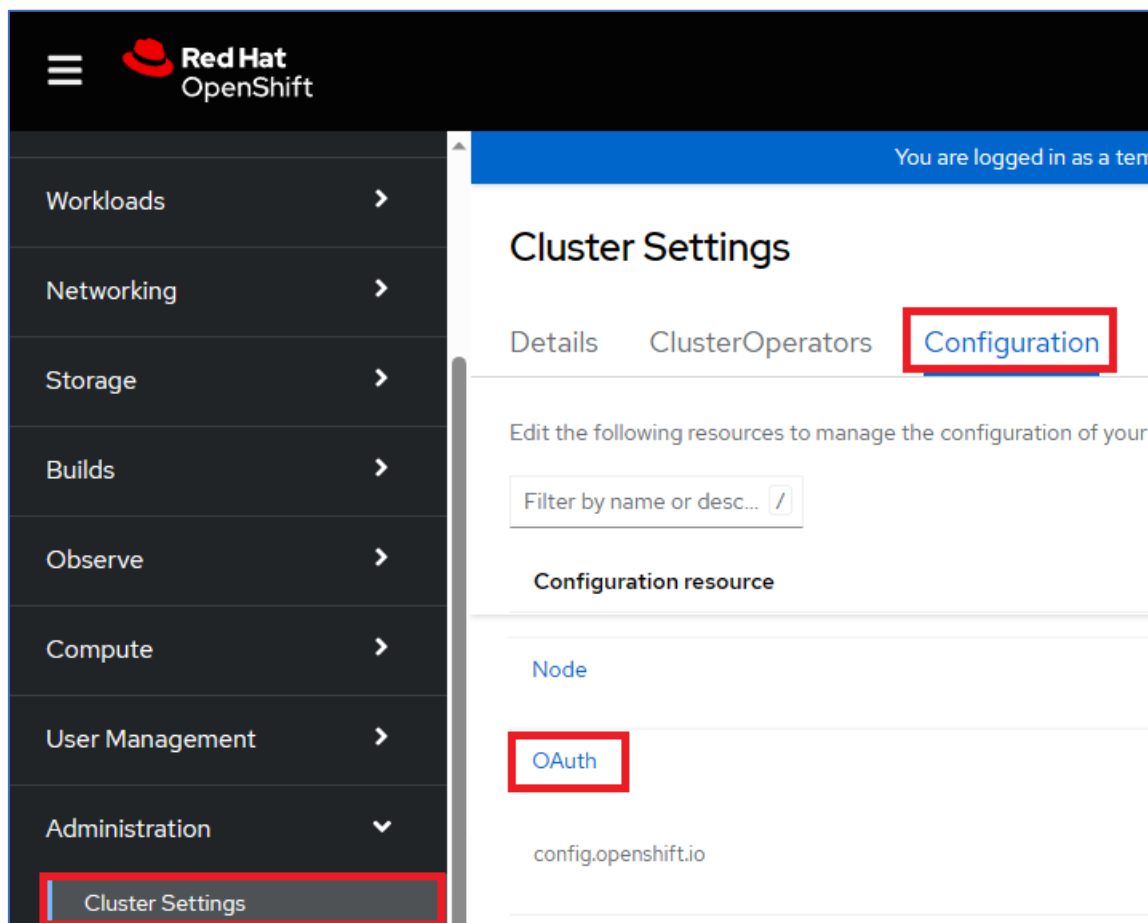


Внизу нажмите Add

### Задание 4. Настройка пользовательского ресурса OAuth

Чтобы использовать поставщика удостоверений HTTPasswd, необходимо изменить пользовательский ресурс OAuth и добавить запись в массив spec: identityProviders.

Можно в веб консоли:



Выглядит это следующим образом:

Details
YAML

View sidebar

```

11 creationTimestamp: 2023-03-10T11:00:27Z
12 generation: 23
13 > managedFields: ...
48 name: cluster
49 ownerReferences:
50   - apiVersion: config.openshift.io/v1
51     kind: ClusterVersion
52     name: version
53     uid: b7a6660e-99d5-4b30-8b02-0d0f95046753
54 resourceVersion: '269225'
55 uid: 0edbc6db-4cf4-4266-a37c-76aab4562216
56 spec:
57   identityProviders:
58     - httpswd:
59       fileName:
60         name: httpswd-7q42h
61       mappingMethod: claim
62       name: httpswd-secret
63       type: HTTPswd
64

```

Save
Reload
Cancel
Download

Можно его выгрузить и сохранить как файл соответствующей кнопкой. Например:

httpswd-oauth.yaml

```

apiVersion: config.openshift.io/v1
kind: OAuth
metadata:
  name: cluster
spec:
  identityProviders:
    - httpswd:
      fileName:
        name: httpswd-7q42h
      mappingMethod: claim
      name: httpswd-secret
      type: HTTPswd

```

Где:

httpswd-secret — это имя провайдера. Это имя добавляется к имени пользователя провайдера для формирования имени удостоверения.

httpswd-7q42h — это имя существующего секрета, содержащего файл, сгенерированный с помощью httpswd.

## OpenShift Administration: Operating a Production Kubernetes Cluster

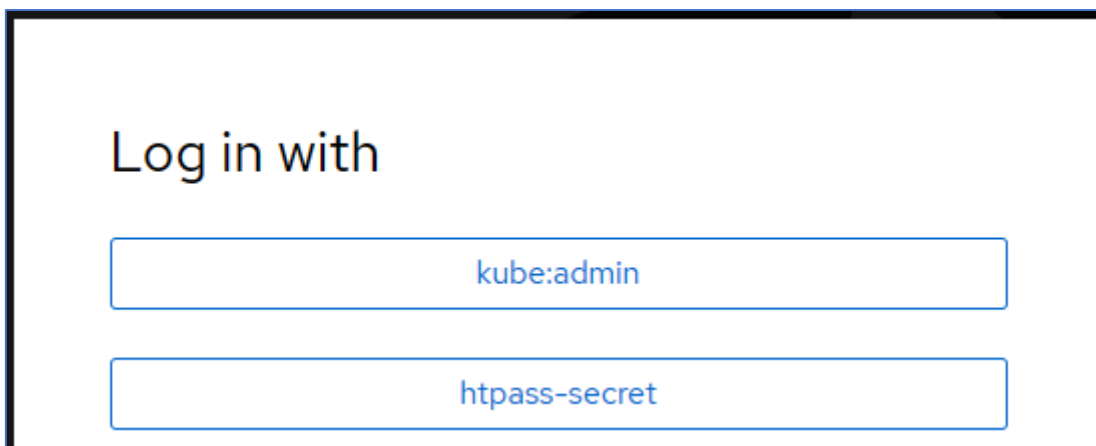
Применить отредактированный пользовательский ресурс (CR) можно в консоли кнопками Save - Reload:

После чего можно увидеть, что поды в пространстве имен openshift-authentication перезапускаются:

```
oc get pods -n openshift-authentication
```

NAME	READY	STATUS	RESTARTS	AGE
oauth-openshift-5469bb6b97-k5wht	1/1	Running	0	91s

Теперь вы можете выбрать «htpasswd-secret» на экране входа в OpenShift для аутентификации с помощью поставщика HTTPasswd, используя соответствующие учетные данные.



The image shows a web-based login interface for OpenShift. At the top, it says "Log in with". Below this, there are two input fields. The first field contains the text "kube:admin" and the second field contains the text "htpasswd-secret".

Также можно с командной строки

```
C:\Users\Michael>oc login --username=user1
Authentication required for https://api.sno.test.local:6443 (openshift)
Console URL: https://api.sno.test.local:6443/console
Username: user1
Password:
Login successful.

You don't have any projects. You can try to create a new project, by running

  oc new-project <projectname>
```

Пользователь создается автоматически при первом входе

**Внимание!** Для входа в веб консоль надо открыть либо другой браузер, отличный от того, где зашли под kubeadmin'ом, либо открыть страницу режиме инкогнито.

Иначе получите следующий эффект:

При входе в вебконсоль отобразился токен и url



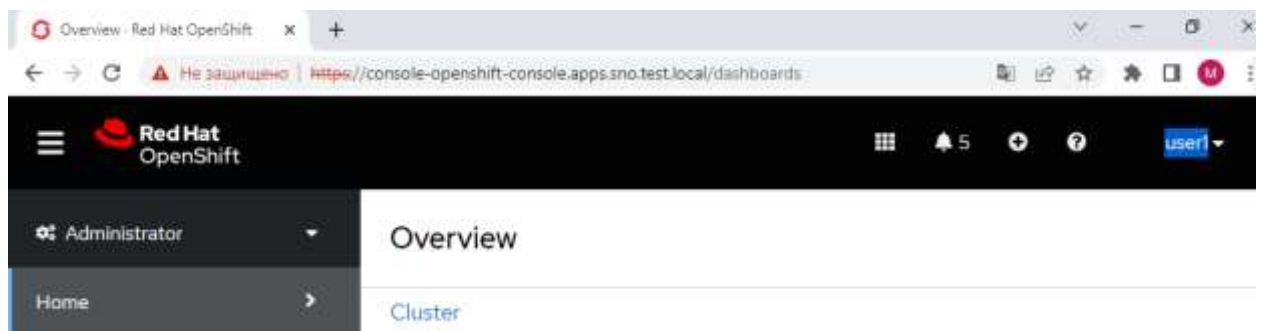
## OpenShift Administration: Operating a Production Kubernetes Cluster



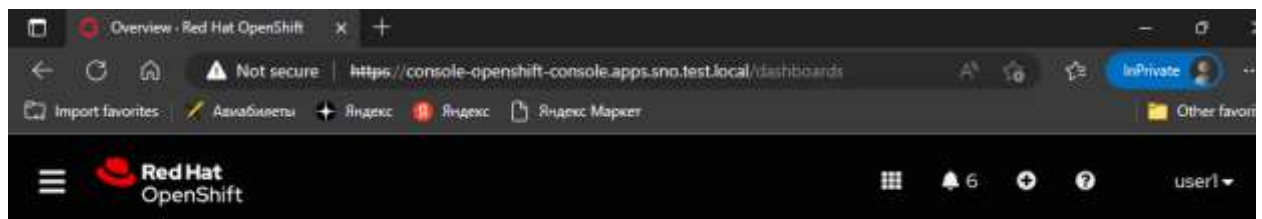
Вводим url, получаем

<https://api.sno.test.local:6443/apis/user.openshift.io/v1/users/~>

```
{
  "kind": "Status",
  "apiVersion": "v1",
  "metadata": {},
  "status": "Failure",
  "message": "users.user.openshift.io \"~\" is forbidden: User\n\"system:anonymous\" cannot get resource\n\"users\" in API group\n\"user.openshift.io\" at the cluster scope",
  "reason": "Forbidden",
  "details": {
    "name": "~",
    "group": "user.openshift.io",
    "kind": "users"
  },
  "code": 403
}
```



Либо так:



### Упражнение 2. Работа с группами и ролями.

#### Задание 1. Добавление пользователю привилегий:

Шаг 1. Создать группу

```
oc adm groups new mylocaladmins
```

Шаг 2. Добавить пользователя

```
oc adm groups add-users localadmins user1
```

Шаг 3. Назначить группе роль

```
oc adm policy add-cluster-role-to-group cluster-admin localadmins
```

Шаг 4. Получить информацию для входа в веб консоль:

```
C:\Users\Michael>oc whoami --show-console
```

Вывод:

<https://console-openshift-console.apps.sno.test.local>

Прим. Управлять созданием групп и назначением ролей можно также их веб консоли.

#### Задание 2. Управление доступом к проекту

Вывести всех пользователей кластера можно командой:

```
oc get users
```

Вывести все удостоверения кластера:

```
oc get identity
```

```
oc describe identity htpass-secret:user1
```

```
Select Command Prompt
C:\Users\Michael>oc get identity
NAME                                IDP NAME      IDP USER NAME  USER NAME  USER UID
htpass-secret:user1                htpass-secret user1           user1      d50ad0f1-ba0d-4a7c-98f9-883ec30af71d
htpasswd-7q42h:user1               htpasswd-7q42h user1           user1      d50ad0f1-ba0d-4a7c-98f9-883ec30af71d
htpasswd-oauth:user1               htpasswd-oauth user1           user1      462f27f7-ea11-4e03-aa61-d344d6f659e3
htpasswd-secret:user1              htpasswd-secret user1           user1      462f27f7-ea11-4e03-aa61-d344d6f659e3
htpasswd-secret:user2              htpasswd-secret user2           user2      a0122955-7b2c-4dab-9a23-3abedbf9e9f8
htpasswd-secret:user3              htpasswd-secret user3           user3      e7fcb147-4386-403c-ba08-9c33935c00b2
htpasswd:michael                   htpasswd       michael         michael    64845233-198e-492a-8e83-b8c568be346f
htpasswd:user1                     htpasswd       user1           user1      f984d6f9-4a2c-4972-ad46-d7556f1bf176
htpasswd:user2                     htpasswd       user2           user2      d80a0ae6-fb34-4983-99ca-73d1ec423077
htpasswd:user3                     htpasswd       user3           user3      390b9148-47e5-43fd-8fea-c01dea86561b

C:\Users\Michael>oc describe identity htpass-secret:user1
Name:                                htpass-secret:user1
Created:                             3 weeks ago
Labels:                              <none>
Annotations:                         <none>
User Name:                           user1 (Error: User identities do not include htpass-secret:user1)
User UID:                             d50ad0f1-ba0d-4a7c-98f9-883ec30af71d (Error: Actual user UID is f984d6f9-4a2c-4972-ad46-d7556f1bf176)

C:\Users\Michael>oc describe identity htpasswd-secret:user1
Name:                                htpasswd-secret:user1
Created:                             3 weeks ago
Labels:                              <none>
Annotations:                         <none>
User Name:                           user1 (Error: User identities do not include htpasswd-secret:user1)
User UID:                             462f27f7-ea11-4e03-aa61-d344d6f659e3 (Error: Actual user UID is f984d6f9-4a2c-4972-ad46-d7556f1bf176)

C:\Users\Michael>
```

Создайте проект и предоставьте пользователям доступ к проекту.

oc new-project test

Один из пользователей будет иметь доступ только для просмотра в кластере, а другой пользователь будет иметь возможность редактировать все ресурсы в пространстве имен / проекте.

Вывести все проекты можно командой:

oc get projects

Задать текущий командой:

oc project test

Назначте роль edit пользователю user1

Синтаксис команды имеет вид:

oc adm policy add-role-to-user <role> <user> -n <projectname>

oc adm policy add-role-to-user edit user1 -n test

Для того, чтобы удалить роль пользователя, используется синтаксис:

oc adm policy remove-role-from-user <role> <user> -n <projectname>

oc adm policy remove-cluster-role-from-user <role> <user> -n <projectname>

Можно вывести список пользователей, имеющих доступ к проекту следующей командой:

## OpenShift Administration: Operating a Production Kubernetes Cluster

```
oc get rolebindings -n <projectname>
```

```
oc get rolebindings <rolename> -n <projectname>
```