作者：李晓辉

联系方式：

1. 微信：Lxh_Chat

2. 邮箱：939958092@qq.com

OpenShift 用户和组

用户

- **简单说**：用户就是能和 OpenShift 里的 API 服务器打交道的家伙。
- **权限咋整**：想给用户权限，就直接把角色加到用户或者用户所在的组里。

身份

- **啥玩意儿**：身份资源就是记录用户从身份提供程序那儿成功登录的信息。
- **存啥数据**：身份验证来源的所有数据都存在身份里。

服务帐户

- **有啥用**：当应用没法拿到用户凭据，但又得和 API 通信时，服务帐户就派上用场了。
- **好处**：用服务帐户能控制 API 访问，不用借普通用户的证。

组

- **定义**：组就是把一些用户凑一块儿。
- **为啥用**：授权策略用组来一次性给多个用户分配权限，方便得很。
- **系统组**：OpenShift 还有系统自动弄好的系统组或者虚拟组。

角色

- **定义**：角色就是定义用户在特定资源上能干啥。
- **权限分配**：把角色分配给用户、组或者服务帐户，就能给权限。

资源创建

- **自动搞定**：一般情况下，用户和身份资源不会提前准备好，OpenShift 会在用户通过 OAuth 成功登录后自动创建。

对 API 请求进行身份验证

身份验证和授权

- **身份验证层**：就是验证用户是不是真的。
- **授权层**：用基于角色的访问控制（RBAC）策略来决定用户能不能干啥，接受或者拒绝请求。

身份验证方法

- **OAuth 访问令牌**：一种验证方法。
- **X.509 客户端证书**：另一种验证方法。
- **匿名用户**：要是请求啥令牌或者证书都没有，身份验证层就会把它当成匿名用户，分配到未认证的虚拟组里，也就是会为其分配 `system:anonymous` 虚拟用户，以及 `system:unauthenticated` 虚拟组。

身份验证 Operator

作用

- **OAuth 服务器**：由身份验证 Operator 运行，给用户提供 OAuth 访问令牌。
- **身份提供程序**：必须配置好身份提供程序，交给 OAuth 服务器，用来验证请求者的身份。

身份提供程序类型

- **HTPasswd**：通过机密文件验证用户名和密码。
- **Keystone**：用 OpenStack Keystone v3 服务器进行身份验证。
- **LDAP**：配置 LDAP 身份提供程序，用简单的绑定身份验证对 LDAPv3 服务器验证用户名和密码。
- **GitHub 或 GitHub Enterprise**：根据 GitHub 或 GitHub Enterprise 的 OAuth 身份验证服务器来验证用户名和密码。
- **OpenID Connect**：用授权代码流和 OpenID Connect 身份提供程序集成。

集群管理员

新安装的 OpenShift 集群提供了两种方法来通过集群管理员特权来验证 API 请求。一种方法是使用 `kubeconfig` 文件，其中嵌入了永不过期的 X.509 客户端证书。另一种方法是作为 `kubeadmin` 虚拟用户进行身份验证。成功的身份验证会授予 OAuth 访问令牌。

1. 在课堂环境中， `utility` 计算机将 `kubeconfig` 文件存储在 `/home/lab/ocp4/auth/kubeconfig` 中。
2. 在课堂环境中， `utility` 计算机将 `kubeadmin` 用户的密码存储在 `/home/lab/ocp4/auth/kubeadmin-password` 文件中。

```
[root@utility ~]# export KUBECONFIG=/home/lab/ocp4/auth/kubeconfig
[root@utility ~]# oc get nodes
NAME       STATUS   ROLES                          AGE    VERSION
master01   Ready    control-plane,master,worker    447d   v1.25.4+77bec7a
```

```
[root@utility ~]# oc login -u kubeadmin -p 8UgkW-u7pMu-223kK-PmNZH https://api.ocp4.example
The server uses a certificate signed by an unknown authority.
You can bypass the certificate check, but any data you send to the server could be intercep
Use insecure connections? (y/n): y

WARNING: Using insecure TLS client config. Setting this option is not supported!

Login successful.

You have access to 72 projects, the list has been suppressed. You can list all projects wit

Using project "default".
Welcome! See 'oc help' to get started.

[root@utility ~]# oc get nodes
NAME       STATUS   ROLES                          AGE    VERSION
master01   Ready    control-plane,master,worker    447d   v1.25.4+77bec7a
```

这里要注意kubeadmin这个用户，这个是临时的超级管理员，在我们至少提供了一种身份认证提供程序后，这个用户最好删除，避免风险，不过在课程中，**切勿** 删除 `kubeadmin` 用户。 `kubeadmin` 用户对于课程实验架构至关重要。删除 `kubeadmin` 用户会损坏实验环境

配置 HTPasswd 身份提供程序

在我们的课程中，我们用的是HTPasswd类型，HTPasswd 身份提供程序依照机密对用户进行验证，该机密中包含通过 Apache HTTP Server 项目中的 `htpasswd` 命令生成的用户名和密码。只有集群管理员可以更改 HTPasswd 机密内的数据。普通用户不能更改自己的密码。

我们需要创建一些HTPasswd用户，然后给用户授予权限，并更新oauth服务器以便于使用HTPasswd类型

新建htpasswd用户

```
[student@workstation ~]$ htpasswd --help
 -c  Create a new file.
 -b  Use the password from the command line rather than prompting for it.
 -B  Force bcrypt encryption of the password (very secure).
```

这里创建了一个new-htpasswd.txt的文件，里面包含两个用户

```
[student@workstation ~]$ htpasswd -c -B -b new-htpasswd.txt lxh-admin lxhpass
Adding password for user lxh-admin
[student@workstation ~]$ htpasswd -B -b new-htpasswd.txt zhangsan zhangsanpass
Adding password for user zhangsan
[student@workstation ~]$ cat new-htpasswd.txt
lxh-admin:$2y$05$hGcuccbY8BGrmq5G58f3zOP2hz2w1/WqNPepJZ1oXsL9pUHoPOKzK
zhangsan:$2y$05$JFwYSQdeZmU1p1vv8vKweO9g2pApGcH8E7UHC7PwH5eZ6joLG4aua
```

分配集群超级管理员

分配权限之前，我们用创建机密的方式，先把这两个用户建出来

```
[student@workstation ~]$ oc login -u admin -p redhatocp https://api.ocp4.example.com:6443
[student@workstation ~]$ oc create secret generic my-htpass --from-file htpasswd=new-htpass
secret/my-htpass created
```

分配超级管理员

由于我们还没有将身份提供程序改为htpasswd，所以提示没有用户很正常，忽略即可

```
[student@workstation ~]$ oc adm policy add-cluster-role-to-user cluster-admin lxh-admin
Warning: User 'lxh-admin' not found
clusterrole.rbac.authorization.k8s.io/cluster-admin added: "lxh-admin"
```

添加HTPasswd认证方式

我们先导出服务器上正在生效的配置，稍微改改就行

```
[student@workstation ~]$ oc get oauth cluster -o yaml > my-oauth.yml
[student@workstation ~]$ cat my-oauth.yml
apiVersion: config.openshift.io/v1
kind: OAuth
metadata:
  annotations:
    include.release.openshift.io/ibm-cloud-managed: "true"
    include.release.openshift.io/self-managed-high-availability: "true"
    include.release.openshift.io/single-node-developer: "true"
    kubectl.kubernetes.io/last-applied-configuration: |
      {"apiVersion":"config.openshift.io/v1","kind":"OAuth","metadata":{"annotations":{},"r
    release.openshift.io/create-only: "true"
  creationTimestamp: "2023-09-28T14:08:46Z"
  generation: 3
  name: cluster
  ownerReferences:
  - apiVersion: config.openshift.io/v1
    kind: ClusterVersion
    name: version
    uid: 72d0e456-95f1-4410-926d-04980c8ba544
  resourceVersion: "332963"
  uid: c8ba3aad-8360-4c1b-9049-00410bc5d2eb
spec:
  identityProviders:
  - ldap:
      attributes:
        email:
        - mail
        id:
        - dn
        name:
        - cn
        preferredUsername:
        - uid
      bindDN: uid=admin,cn=users,cn=accounts,dc=ocp4,dc=example,dc=com
      bindPassword:
        name: ldap-secret
      ca:
        name: ca-config-map
      insecure: false
      url: ldap://idm.ocp4.example.com/cn=users,cn=accounts,dc=ocp4,dc=example,dc=com?uid
    mappingMethod: claim
    name: Red Hat Identity Management
    type: LDAP
```

在spec下的identityProviders中，添加新的类型

```
[student@workstation ~]$ cat my-oauth.yml
apiVersion: config.openshift.io/v1
kind: OAuth
metadata:
  annotations:
    include.release.openshift.io/ibm-cloud-managed: "true"
    include.release.openshift.io/self-managed-high-availability: "true"
    include.release.openshift.io/single-node-developer: "true"
    kubectl.kubernetes.io/last-applied-configuration: |
      {"apiVersion":"config.openshift.io/v1","kind":"OAuth","metadata":{"annotations":{},"r
    release.openshift.io/create-only: "true"
  creationTimestamp: "2023-09-28T14:08:46Z"
  generation: 3
  name: cluster
  ownerReferences:
  - apiVersion: config.openshift.io/v1
    kind: ClusterVersion
    name: version
    uid: 72d0e456-95f1-4410-926d-04980c8ba544
  resourceVersion: "332963"
  uid: c8ba3aad-8360-4c1b-9049-00410bc5d2eb
spec:
  identityProviders: # 下面的htpasswd是新加的，一直到ldap
  - htpasswd:
      fileData:
        name: my-htpass
    mappingMethod: claim
    name: Lxh-Users
    type: HTPasswd
  - ldap:
      attributes:
        email:
        - mail
        id:
        - dn
        name:
        - cn
        preferredUsername:
        - uid
      bindDN: uid=admin,cn=users,cn=accounts,dc=ocp4,dc=example,dc=com
      bindPassword:
        name: ldap-secret
      ca:
        name: ca-config-map
      insecure: false
      url: ldap://idm.ocp4.example.com/cn=users,cn=accounts,dc=ocp4,dc=example,dc=com?uid
    mappingMethod: claim
    name: Red Hat Identity Management
    type: LDAP
```

这个会触发operator的更新，不会那么快，观察一下内容，确认更新过程已经完成

```
[student@workstation ~]$ oc get co
NAME                                       VERSION   AVAILABLE   PROGRESSING   DEGRADED   S
authentication                             4.12.0    True        True          False      2
```

验证权限分配

经过验证，发现lxh-admin有权限获取节点，而zhangsan没有权限

```
[student@workstation ~]$ oc login -u lxh-admin -p lxhpass https://api.ocp4.example.com:6443
Login successful.

You have access to 72 projects, the list has been suppressed. You can list all projects wit

Using project "default".
[student@workstation ~]$ oc get nodes
NAME       STATUS   ROLES                          AGE    VERSION
master01   Ready    control-plane,master,worker    447d   v1.25.4+77bec7a

[student@workstation ~]$ oc get users
NAME         UID                                    FULL NAME       IDENTITIES
admin        bc98d46a-dd9f-4917-8246-089f10f95e75   Administrator   Red Hat Identity Managem
developer    12724778-65ba-411a-aa80-a9634228e116   . developer     Red Hat Identity Managem
lxh-admin    693dfbd1-5721-4ffe-b569-fa346675cf61                   Lxh-Users:lxh-admin
zhangsan     6563b503-367e-47fe-8a40-62dcb37e344a                   Lxh-Users:zhangsan
[student@workstation ~]$ oc get identities.user.openshift.io
NAME
Lxh-Users:lxh-admin

[student@workstation ~]$ oc login -u zhangsan -p zhangsanpass https://api.ocp4.example.com:
Login successful.

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

    oc new-project <projectname>

[student@workstation ~]$ oc get nodes
Error from server (Forbidden): nodes is forbidden: User "zhangsan" cannot list resource "nc

[student@workstation ~]$ oc get nodes
Error from server (Forbidden): nodes is forbidden: User "zhangsan" cannot list resource "nc
[student@workstation ~]$ oc get users
Error from server (Forbidden): users.user.openshift.io is forbidden: User "zhangsan" cannot
[student@workstation ~]$ oc get identities.user.openshift.io
Error from server (Forbidden): identities.user.openshift.io is forbidden: User "zhangsan" c
```

添加新用户到HTPasswd用户列表

添加用户，需要先把线上现有的用户导出来，然后新增，我们是模拟本地没有txt文件的情况下如何新增

这个--to可以不用加，默认是当前路径，--confirm如果不加，而当前路径存在有htpasswd文件时，会失败

```
[student@workstation ~]$ oc extract secret/my-htpass -n openshift-config --to=/home/student
/home/student/htpasswd
[student@workstation ~]$ cat /home/student/htpasswd
lxh-admin:$2y$05$hGcuccbY8BGrmq5G58f3zOP2hz2w1/WqNPepJZ1oXsL9pUHoPOKzK
zhangsan:$2y$05$JFwYSQdeZmU1p1vv8vKweO9g2pApGcH8E7UHC7PwH5eZ6joLG4aua
```

添加一个wangwu用户

```
[student@workstation ~]$ htpasswd -b -B htpasswd wangwu wangwupass
Adding password for user wangwu
[student@workstation ~]$ cat htpasswd
lxh-admin:$2y$05$hGcuccbY8BGrmq5G58f3zOP2hz2w1/WqNPepJZ1oXsL9pUHoPOKzK
zhangsan:$2y$05$JFwYSQdeZmU1p1vv8vKweO9g2pApGcH8E7UHC7PwH5eZ6joLG4aua
wangwu:$2y$05$AJorPPbJ1Z3cVci8IAV5zuQln4XBrwPrS5qQqfXpk3IGmd3w1CxOm
```

触发一次secret数据更新

供 HTPasswd 身份提供程序使用的机密需要在指定文件的路径之前添加 htpasswd= 前缀

--from-file后面的htpasswd是secret的key，后面的一个是文件名

```
[student@workstation ~]$ oc set data secret/my-htpass --from-file htpasswd=htpasswd -n oper
```

确认wangwu用户登录成功

```
[student@workstation ~]$ oc login -u wangwu -p wangwupass https://api.ocp4.example.com:6443
Login successful.
```

更新用户密码

更新wangwu用户的密码

```
[student@workstation ~]$ oc extract secret/my-htpass -n openshift-config --to=/home/student
/home/student/htpasswd
```

```
[student@workstation ~]$ cat htpasswd
lxh-admin:$2y$05$hGcuccbY8BGrmq5G58f3zOP2hz2w1/WqNPepJZ1oXsL9pUHoPOKzK
zhangsan:$2y$05$JFwYSQdeZmU1p1vv8vKwe09g2pApGcH8E7UHC7PwH5eZ6joLG4aua
wangwu:$2y$05$AJorPPbJ1Z3cVci8IAV5zuQln4XBrwPrS5qQqfXpk3IGmd3w1CxOm

[student@workstation ~]$ htpasswd -b -B htpasswd wangwu lixiaohuipass
Updating password for user wangwu

[student@workstation ~]$ cat htpasswd
lxh-admin:$2y$05$hGcuccbY8BGrmq5G58f3zOP2hz2w1/WqNPepJZ1oXsL9pUHoPOKzK
zhangsan:$2y$05$JFwYSQdeZmU1p1vv8vKwe09g2pApGcH8E7UHC7PwH5eZ6joLG4aua
wangwu:$2y$05$HoT.vyizHJotzDCQ1qjDLuJc7K3noHVyEej9UgFADcRrBc4VPOOf.
```

```
[student@workstation ~]$ oc set data secret/my-htpass --from-file htpasswd=htpasswd -n oper
```

别忘了观察oc get co

删除用户

```
[student@workstation ~]$ oc extract secret/my-htpass -n openshift-config --to=/home/student
/home/student/htpasswd
```

删除用户可以手工vim删除这一条，或者用

```
[student@workstation ~]$ cat htpasswd
lxh-admin:$2y$05$hGcuccbY8BGrmq5G58f3zOP2hz2w1/WqNPepJZ1oXsL9pUHoPOKzK
zhangsan:$2y$05$JFwYSQdeZmU1p1vv8vKwe09g2pApGcH8E7UHC7PwH5eZ6joLG4aua
wangwu:$2y$05$HoT.vyizHJotzDCQ1qjDLuJc7K3noHVyEej9UgFADcRrBc4VPOOf.

[student@workstation ~]$ htpasswd -D htpasswd wangwu
Deleting password for user wangwu

[student@workstation ~]$ cat htpasswd
lxh-admin:$2y$05$hGcuccbY8BGrmq5G58f3zOP2hz2w1/WqNPepJZ1oXsL9pUHoPOKzK
zhangsan:$2y$05$JFwYSQdeZmU1p1vv8vKwe09g2pApGcH8E7UHC7PwH5eZ6joLG4aua
```

```
[student@workstation ~]$ oc set data secret/my-htpass --from-file htpasswd=htpasswd -n oper
```

当出现需要删除用户的情形时，仅从身份提供程序中删除该用户是不够的。还必须删除用户和身份资源

```
[student@workstation ~]$ oc delete identities.user.openshift.io Lxh-Users:
lxh-admin  wangwu     zhangsan
[student@workstation ~]$ oc delete identities.user.openshift.io Lxh-Users:wangwu
identity.user.openshift.io "Lxh-Users:wangwu" deleted
[student@workstation ~]$ oc delete user wangwu
user.user.openshift.io "wangwu" deleted
```

别忘了观察oc get co

新建组

```
[student@workstation ~]$ oc adm groups new lxh-group
group.user.openshift.io/lxh-group created
```

添加用户到组

```
[student@workstation ~]$ oc adm groups add-users lxh-group lxh-admin
group.user.openshift.io/lxh-group added: "lxh-admin"
```

查一下大家在哪个组

```
[student@workstation ~]$ oc get group
NAME                USERS
Default SMB Group
admins              Administrator
developer
editors
lxh-group           lxh-admin
ocpadmins           Administrator
ocpdevs             . developer
```

本文档在线版本：https://www.linuxcenter.cn