作者：李晓辉

联系方式：

1. 微信：Lxh_Chat

2. 邮箱：939958092@qq.com

最近在研究红帽OpenShift里的RBAC（基于角色的访问控制），觉得这东西还挺有意思的。简单来说，RBAC就是用来决定用户能不能在集群或者项目里干某些事儿的。你可以根据用户的职责，从两种角色类型里选：集群角色和本地角色。

- **集群角色**：这角色的权限范围挺大的，能跨多个项目管事儿。
- **本地角色**：这个就比较“专一”了，只针对某个特定的项目。

授权过程

授权这事儿，主要是靠规则、角色和绑定来搞定的，听起来是不是有点像游戏里的设定呀。

RBAC对象	描述
规则	就是说允许某个对象或者对象组能干啥操作，相当于给权限“划个范围”。
角色	把一堆规则打包成一个集合，用户或者用户组可以和多个角色关联起来， 有点像给权限“打个包”。
绑定	把用户或者用户组分配到某个角色里，这一步就是“分配权限”的关键环节啦。

RBAC范围

说到RBAC的范围，OpenShift分了两组角色和绑定，一个是集群角色，有这角色的用户或者用户组能管整个OpenShift集群；另一个是本地角色，只能管项目里的事儿。

角色级别	描述
集群角色	具有此角色级别的用户或组可以管理OpenShift集群，相当于“大管家”。
本地角色	具有此角色级别的用户或组只能管理项目级别的元素，就是“小管家”，只管自己那一摊。

而且，集群角色绑定的优先级比本地角色绑定高，这就好比“大管家”的指令优先级更高一样。

默认角色

OpenShift自带了一堆默认的集群角色，这些角色既可以分配到本地项目，也可以分配到整个集群，挺灵活的。

默认角色	描述
`admin`	具有此角色的用户可以管理所有项目资源， 包括向其他用户授予访问权限来访问项目，简直就是“项目老板”。
`basic-user`	具有此角色的用户具有项目的读取访问权限，能看看，但不能乱动， 相当于“项目游客”。
`cluster-admin`	具有此角色的用户拥有对集群资源的超级用户访问权限， 这些用户可以在集群上执行任何操作，并且拥有所有项目的完全控制权限， 妥妥的“超级大老板”。
`cluster-status`	具有此角色的用户可以获取集群状态信息，就像是“集群情报员”。
`edit`	具有此角色的用户可以创建、更改和删除项目中的通用应用资源， 如服务和部署。不过，这些用户无法操作管理资源，如限值范围和配额， 也不能管理项目的访问权限，就是“项目施工队”，能干活但不能管人。
`self-provisioner`	具有此角色的用户可以创建项目，这是集群角色，而非项目角色， 相当于有“项目创建许可证”。
`view`	具有此角色的用户可以查看项目资源，但不能修改项目资源， 就是“项目观察员”。

用户类型

在OpenShift容器平台里，用户可不止一种呢，每种用户都有自己的特点和用途，就像不同的角色在舞台上扮演不同的角色一样。

普通用户

大多数和OpenShift容器平台打交道的用户，都是普通用户，用`User`对象来表示。这就好比是那些有权限进入游乐场的游客，他们有权访问平台，能干不少事儿呢。

系统用户

系统用户就有点厉害了，很多都是在搭建基础架构的时候自动创建的，主要任务是让基础架构和API能安全地互动。你可以把他们想象成游乐场里的工作人员，他们负责各种重要的任务，比如管理整个游乐场的集群管理员、各个游乐设施（节点）的管理员、负责门票（路由器）和纪念品（注册表）的工作人员，还有好多其他角色呢。要是有人没带票（未经身份验证的请求），就会用到一个默认的匿名系统用户。

系统用户的用户名都有个特别的标志，以`system:`开头，比如`system:admin`（游乐场的大老板）、`system:openshift-registry`（纪念品仓库管理员）和`system:node:node1.example.com`（某个游乐设施的管理员）。

服务账户

服务账户也很有意思，它们是和项目关联的系统用户。你可以把它们想象成游乐场里那些专门负责特定任务的工作人员，比如负责搭建游乐设施（工作负载）的工人，他们可以用服务账户来调用Kubernetes API，完成自己的任务。

服务账户用`ServiceAccount`对象来表示，它们的用户名也有个特别的前缀，以`system:serviceaccount:*namespace*:`开头，比如`system:serviceaccount:default:deployer`（默认项目里的搭建工人）和`system:serviceaccount:accounting:builder`（财务项目里的建设者）。

授权案例

分配超级管理员

```
[student@workstation ~]$ oc adm policy add-cluster-role-to-user cluster-admin lxh-admin
clusterrole.rbac.authorization.k8s.io/cluster-admin added: "lxh-admin"
```

同理，只需要把to-user改成to-group即可授权给组

从用户身上回收集群权限

```
[student@workstation ~]$ oc adm policy remove-cluster-role-from-user cluster-admin zhangsan
```

同理，只需要把from-user改成from-group即可从组回收

分配本地角色

在default的project中，给lxh-admin分配edit角色

```
oc policy add-role-to-user edit lxh-admin -n default
```

确认谁有哪种权限

```
[student@workstation ~]$ oc adm policy who-can create deployment
resourceaccessreviewresponse.authorization.openshift.io/<unknown>

Namespace: default
Verb:      create
Resource:  deployments.apps

Users:  admin
        lxh-admin
        system:admin
        system:serviceaccount:metallb-system:manager-account
        system:serviceaccount:openshift-apiserver-operator:openshift-apiserver-operator
        system:serviceaccount:openshift-apiserver:openshift-apiserver-sa
        system:serviceaccount:openshift-authentication-operator:authentication-operator
        system:serviceaccount:openshift-authentication:oauth-openshift
        system:serviceaccount:openshift-cluster-storage-operator:cluster-storage-operator
        system:serviceaccount:openshift-cluster-version:default
        system:serviceaccount:openshift-config-operator:openshift-config-operator
        system:serviceaccount:openshift-controller-manager-operator:openshift-controller-ma
        system:serviceaccount:openshift-etcd-operator:etcd-operator
        system:serviceaccount:openshift-etcd:installer-sa
        system:serviceaccount:openshift-infra:template-instance-controller
        system:serviceaccount:openshift-infra:template-instance-finalizer-controller
        system:serviceaccount:openshift-ingress-operator:ingress-operator
        system:serviceaccount:openshift-kube-apiserver-operator:kube-apiserver-operator
        system:serviceaccount:openshift-kube-apiserver:installer-sa
        system:serviceaccount:openshift-kube-apiserver:localhost-recovery-client
        system:serviceaccount:openshift-kube-controller-manager-operator:kube-controller-ma
        system:serviceaccount:openshift-kube-controller-manager:installer-sa
        system:serviceaccount:openshift-kube-controller-manager:localhost-recovery-client
        system:serviceaccount:openshift-kube-scheduler-operator:openshift-kube-scheduler-op
        system:serviceaccount:openshift-kube-scheduler:installer-sa
        system:serviceaccount:openshift-kube-scheduler:localhost-recovery-client
        system:serviceaccount:openshift-kube-storage-version-migrator-operator:kube-storage
        system:serviceaccount:openshift-kube-storage-version-migrator:kube-storage-version-
        system:serviceaccount:openshift-machine-api:cluster-baremetal-operator
        system:serviceaccount:openshift-machine-config-operator:default
        system:serviceaccount:openshift-network-operator:default
        system:serviceaccount:openshift-oauth-apiserver:oauth-apiserver-sa
        system:serviceaccount:openshift-operator-lifecycle-manager:olm-operator-serviceacco
        system:serviceaccount:openshift-service-ca-operator:service-ca-operator
        system:serviceaccount:openshift-storage:lvms-operator
Groups: ocpadmins
```

```
        system:cluster-admins
        system:masters
```

本文档在线版本：https://www.linuxcenter.cn