作者：李晓辉

联系方式：

1. 微信：Lxh_Chat

2. 邮箱：939958092@qq.com

要是你想成为那种超级厉害的 OpenShift 集群管理员，这课就是你的菜。简单来说，就是让你能搞定一个超级复杂的集群，里面既有自己团队的应用，也有外面供应商的应用，你要负责日常的管理，还得让不同角色的用户能自己搞定一些事儿，比如部署一些需要特殊权限的应用，像 CI/CD 工具、性能监控和安全扫描程序之类的。

DO280 这课重点讲的是怎么把 OpenShift 配置成多租户的，同时保证安全性，还教你用 operator 来搞定那些附加组件。这课是基于红帽 OpenShift 容器平台 4.12 搭建的。

课程目标

- 让你搞定 OpenShift 集群的配置和管理，不管多少应用和开发团队，都能保证安全性和可靠性。
- 教你配置身份验证、授权和资源配额。
- 通过网络政策和 TLS 安全性（HTTPS）来保护网络流量。
- 用 HTTP 和 TLS 以外的协议公开应用，还能把应用附加到多宿主网络。
- 管理 OpenShift 集群更新和 Kubernetes operator 更新。
- 这课和红帽 OpenShift 一：容器和 Kubernetes（DO180）一起，能帮你备考红帽认证 OpenShift 管理专家考试（EX280）。

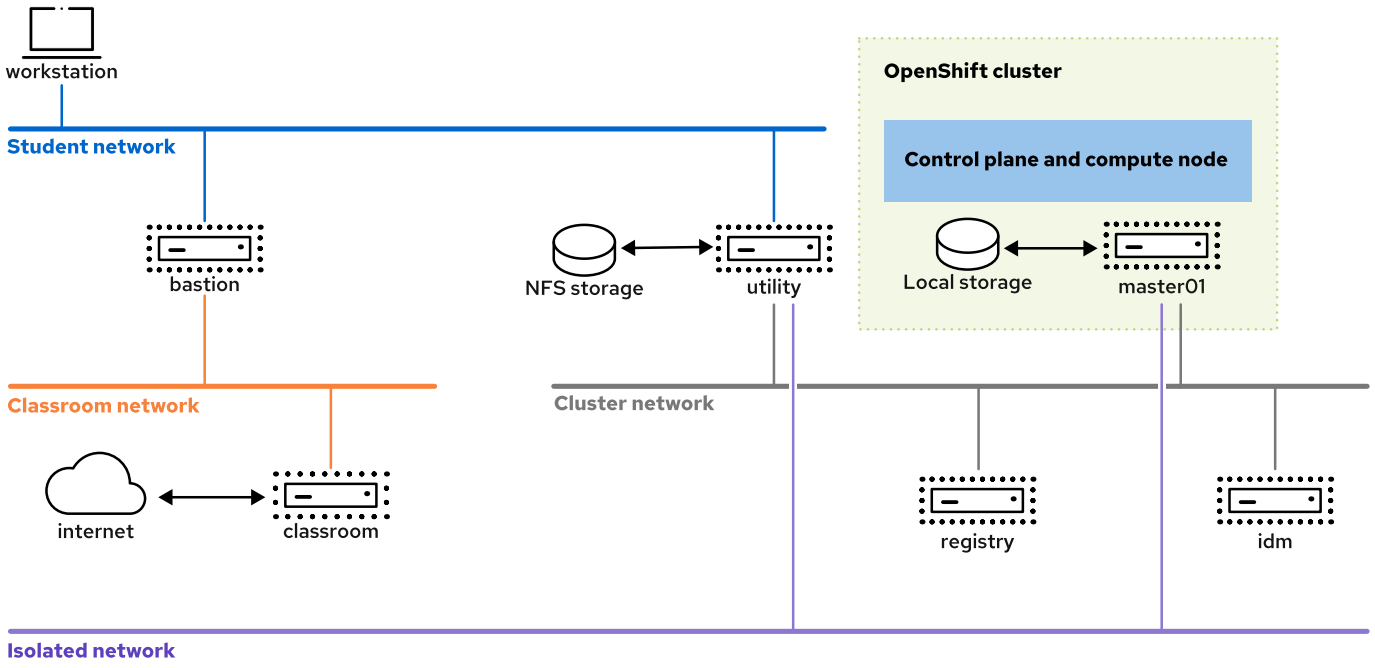
培训对象

- 那些喜欢折腾 OpenShift 集群、应用、用户和附加组件的系统管理员。
- 对 Kubernetes 集群持续维护和故障排除感兴趣的站点可靠性工程师。
- 想了解 OpenShift 集群安全性的系统和软件架构师。

先决条件

- 你得上过红帽系统管理一（RH124），或者会从 Bash shell 管理 Linux 系统和服务器。
- 上过红帽 OpenShift 一：容器和 Kubernetes（DO180 v4.12），或者会用 OpenShift Web 控制台和命令行界面来部署和管理 Kubernetes 应用。

课堂环境介绍



workstation 虚拟机 (VM)是唯一装有图形桌面的虚拟机

咱这课里，主要用来动手操作的计算机系统是 workstation 哦。为了保证实验环境能正常用，一定要让 bastion 和 classroom 这俩系统一直开着。

这三个系统都在 lab.example.com 的 DNS 域里。

咱们课堂用的是红帽 OpenShift 容器平台（RHOCP）4.12 单节点（SNO）裸机 UPI 安装。RHOCP 集群的那些基础架构系统都在 ocp4.example.com 的 DNS 域里。

所有学员的计算机系统都有一个标准用户账户，叫 student，密码就是 student。要是需要管理员权限，所有学员系统的 root 密码都是 redhat。

课堂计算机

计算机名称	IP 地址	角色
bastion.lab.example.com	172.25.250.254	将虚拟机链接到中央服务器的路由器
classroom.lab.example.com	172.25.252.254	托管所需课堂资料的服务器
idm.ocp4.example.com	192.168.50.40	用于集群身份验证和授权支持的身份管理服务器
master01.ocp4.example.com	192.168.50.10	RHOCP 单节点（SNO）集群
registry.ocp4.example.com	192.168.50.50	注册表服务器，用于为集群提供私有注册表和 GitLab 服务

计算机名称	IP 地址	角色
utility.lab.example.com	192.168.50.254	用于提供 RHOCP 集群所需支持服务的服务器，包括 DHCP、NFS 以及通向集群网络的路由
workstation.lab.example.com	172.25.250.9	学员使用的图形工作站

bastion 就像一座桥，连接着学员计算机的网络和课堂网络。要是 **bastion** 关了，其他学员的计算机就可能出问题，甚至启动都启动不了。

utility 系统也很关键，它连接着 RHOCP 集群计算机的网络和学员的网络。要是 **utility** 关了，RHOCP 集群也会出问题，甚至启动都启动不了。

有些练习里，课堂会有一个独立的小网络，只有 **utility** 系统和集群能连上这个网络。

课堂里还有几个系统是来帮忙的。**classroom** 服务器存着咱们动手实践要用的软件和实验材料。**registry** 服务器是个私有的红帽 Quay 容器注册表，专门存动手实践要用的容器镜像。怎么用这些服务器，到时候实验说明里会有详细讲。

master01 系统是 RHOCP 集群的大脑和肌肉，既是控制平面，也是计算节点。集群用 **registry** 系统来存自己的私有容器镜像，还用它当 GitLab 服务器。**idm** 系统给 RHOCP 集群提供 LDAP 服务，搞定身份验证和授权这些事儿。

学员们用 **workstation** 计算机来访问专用的 RHOCP 集群，而且学员们在集群里有管理员的权限，能干不少事儿。

课堂中有几个系统提供支持服务。`classroom` 服务器托管动手实践活动中使用的软件和实验材料。`registry` 服务器是私有的红 帽 Quay 容器注册表，用于托管用于动手实践活动的容器镜像。有关如何使用这些服务器的信息将在这些活动的说明中提供。

`master01` 系统充当 RHOCP 集群的控制平面和计算节点。集群使用 `registry` 系统作为自己的私有容器镜像注册表和 GitLab 服务器。`idm` 系统为 RHOCP 集群提供 LDAP 服务，以提供身份验证和授权支持。

学员使用 `workstation` 计算机访问专用 RHOCP 集群，学员具有集群管理员特权。

RHOCP 访问方式

访问方式	端点
Web 控制台	https://console-openshift-console.apps.ocp4.example.com
API	https://api.ocp4.example.com:6443
registry 服务器	https://registry.ocp4.example.com:8443

RHOCP 集群有一个标准用户帐户 `developer`，其密码为 `developer`。管理帐户 `admin` 的密码为 `redhatocp`。

注册表配置有用户帐户 `developer` ， 密码为 `developer`

本文档在线版本：https://www.linuxcenter.cn