Openshift部署手册

# Plan

## 安装之前需要确定的几个方面

### Installation Type

openshift支持rpm 和container,使用rpm会更好一点。

### pods 数量

<https://docs.openshift.com/container-platform/3.9/scaling_performance/cluster_limits.html#scaling-performance-cluster-limits>

一个node上最大支持跑250个pods

一个core 最大支持跑10个pods

### Master HA

这一点要先考虑好。

Moving from a single master cluster to multiple masters after installation is not supported.

### Host的角色和Layout

<https://docs.openshift.com/container-platform/3.9/install_config/install/planning.html#environment-scenarios>

#### 规划结果

使用8个虚拟机来构建Openshift集群

|  |  |  |
| --- | --- | --- |
| Role | 数量 | Hostname |
| Master | 3 | ose0 ose1 ose2 |
| LB | 1 | ose5 |
| Etcd | 3 | ose0 ose1 ose2 |
| Node | 2 | ose3 ose4 |
| Infra | 2 | ose6 ose7 |

这个Infra是什么的？ 用来跑一些Openshift Infrastruture的 Pods , Infra节点专门用于这类pods, 跟user pods 区别开来。

还有一个DNS服务器； 问题：

一般公司已经有一个公共的DNS服务器，Openshift平台的DNS服务器如何和公共服务器和谐共处？

### Installation Method

quick 这种交互式cli的方式，不能对很多细节进行配置，因此比较适合生产的是advanced installation method。 这种方法就是跑ansible脚本。

### 独立的docker registry Server

Openshift里面包含有 Openshift container registry (OCR)， 但可以单独进行部署。

<https://docs.openshift.com/container-platform/3.9/install_config/install/stand_alone_registry.html#install-config-installing-stand-alone-registry>

要求“

/var/ 至少15G

docker storage back end最少15G

### docker storage

目前推荐overlay2 ,好处是在同一个host node上的多个使用同一个image的container可以利用 page cache sharing ，减少了IO , 降低了容器start的时间。

To use overlay2 with RHEL or CentOS you need version 3.10.0-693 or higher of the kernel

而Device Mapper 就不可能具有page cache sharing特性。

overlay2 相对overlay，对使用layer的命令如docker build 提供了更好的performance ,而且使用的inode会更少。

### Storage

从

<https://docs.openshift.com/container-platform/3.9/scaling_performance/optimizing_storage.html#_footnotedef_4>

可以看到需要用存储的几个地方：

1. registry
2. metrics
3. logs
4. application

其中registry 适合用对象存储去做， 其他的都适合用block /file

总体上来讲， 选用Netapp存储是可以满足所有需求的，  NetApp NFS supports dynamic PV provisioning when using the Trident plugin.

Redhat 推荐使用 Glusterfs ，宣称是cloud native storage , 值得了解一下。

### 其他在安装时可以一并考虑的点

如软件版本，docker版本以及storage driver (是Device mapper还是Overlay2 )

Openshift 3.9自带的k8s版本是1.9.1 ,在已安装部署的环境上如何查询？

详见

<https://access.redhat.com/articles/2176281>

# Prepare

## 安装os

1. disable swap 为何不要swap分区？
2. selinux=enforcing ,为何啊？
3. ntp on

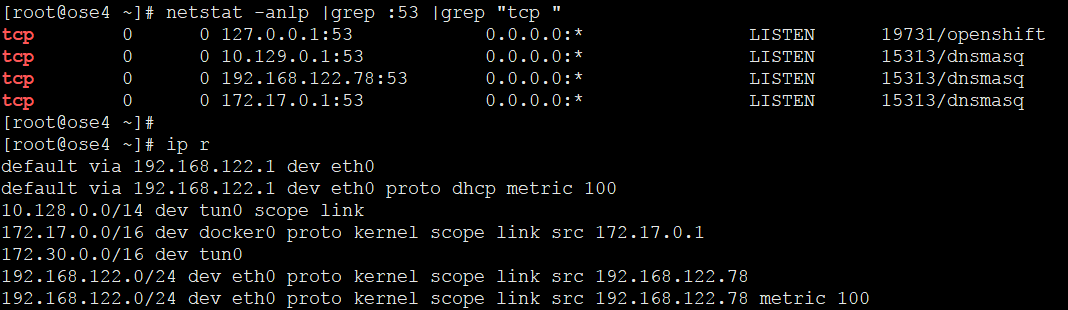
## 配置DNS

目的是：

1. 集群扩容缩容的时候不用去维护/etc/hosts

master和node上面都使用dnsmasq ，node上面的pods 使用该node上的dnsmasq来解析DNS

Dnsmasq is still responsible for dispatching queries inside pods to the right nameserver



为了利用dnsmasq来解析DNS-》ip地址， 要求node上面运行NetworkManager

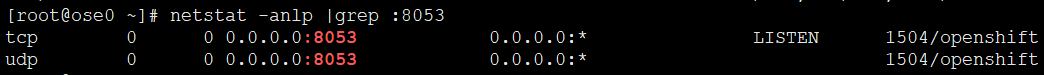
ifcfg-XXX 文件要求：

**NM\_CONTROLLED=yes**

PEERDNS=yes

这两个参数的值也是默认的。

master节点上面skyDNS，监听在8053 端口上



SkyDNS是内含在Openshift进程中的。

参见

<https://www.redhat.com/en/blog/red-hat-openshift-container-platform-dns-deep-dive-dns-changes-red-hat-openshift-container-platform-36>



In your ***/etc/resolv.conf*** file on each node host, ensure that the DNS server that has the wildcard entry is not listed as a nameserver or that the wildcard domain is not listed in the search list. Otherwise, containers managed by OpenShift may fail to resolve host names properly.

CentOS-OpenShift-Origin

参见：

<http://zhubingbing.cn/2017/07/17/openshift/openshift-env-reday/>

### 配置hosts使用dns

确保您的环境中的每个主机都配置为从DNS服务器解析主机名。主机DNS解析的配置取决于是否启用DHCP。

* 如果dhcp服务器是禁用的， 应该将您的网络接口配置为静态，并将DNS名称服务器添加到NetworkManager。
* 如果dhcp服务器是启用的，NetworkManager调度脚本将根据DHCP配置自动配置DNS。或者，您可以在node-config.yaml文件中的dnsIP中添加一个值，以将pod的resolv.conf文件添加到前面。然后，第二个名称服务器由主机的第一个名称服务器定义。默认情况下，这将是节点主机的IP地址。

对于大多数配置，请勿在OpenShift Origin（使用Ansible）高级安装期间设置openshift\_dns\_ip选项，因为此选项将覆盖由dnsIP设置的默认IP地址。

相反，允许安装程序配置每个节点使用dnsmasq并将请求转发给SkyDNS或外部DNS提供程序。如果您设置了openshift\_dns\_ip选项，则应该使用首先查询SkyDNS的DNS IP或SkyDNS服务或端点IP（Kubernetes服务IP）进行设置。

# Post-Install

## 1.创建user

## 2.修改docker-registry

注意，openshift 安装时会在openshift cluster上默认部署docker registry, 在安装时并不支持外部已经存在的docker registry

所以安装完之后oc get pods 可以发现docker-registry , 而且docker-registry的存储backend configuration 可能需要修改， 方法见：

<https://docs.openshift.com/container-platform/3.3/install_config/registry/deploy_registry_existing_clusters.html#install-config-deploy-registry-existing-clusters>

### 实践

在ose5上添加disk, 配置nfs server

oc volume deploymentconfigs/docker-registry --add --name=registry-storage -t pvc \

--claim-name=<pvc\_name> --overwrite

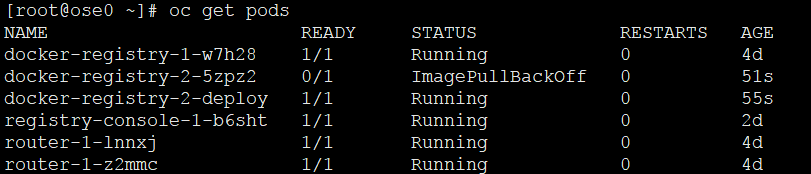
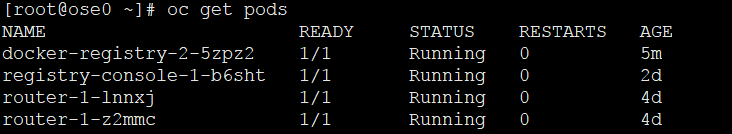


image pull成功之后，发现docker-registry-1-w7h28已经不见了。



### 访问registry

参见  
<https://docs.openshift.com/container-platform/3.3/install_config/registry/accessing_registry.html>

## 3.如何从cluster外部访问registry

<https://docs.openshift.com/container-platform/3.3/install_config/registry/securing_and_exposing_registry.html#exposing-the-registry>

## 4.访问registry-console

<https://docs.openshift.com/container-platform/3.3/install_config/registry/deploy_registry_existing_clusters.html#registry-console>

# Authentication

openshift 自带有built-in的Oauth Server , 最好是在安装时配置 ,但也可以在安装完了之后再配置。

Todo：默认安装用的htpasswd, 在安装完之后修改为Oauth

<https://docs.openshift.com/container-platform/3.9/install_config/configuring_authentication.html>