融合容器平台云环境部署指南

[1.文档说明 2](#_Toc534812022)

[2.环境准备 2](#_Toc534812023)

[2.1 服务购买 2](#_Toc534812024)

[2.2 内网负载均衡监控端口设置 3](#_Toc534812025)

[2.2 外网负载均衡监控端口设置 3](#_Toc534812026)

[3 安装原理 3](#_Toc534812027)

[4.安装步骤 4](#_Toc534812028)

[4.1 安装机设置 4](#_Toc534812029)

[4.1.1 拷贝安装介质 4](#_Toc534812030)

[4.1.2 安装docker 4](#_Toc534812031)

[4.2 安装机器上启动local repo 5](#_Toc534812032)

[4.3 安装容器中配置ssh免密登陆 5](#_Toc534812033)

[4.4 计算参数 5](#_Toc534812034)

[4.5 定制集群配置参数 6](#_Toc534812035)

[4.6 启动安装脚本 12](#_Toc534812036)

# 1.文档说明

本手册是给实施人员或者用户的系统安装人员提供新智认知新氦云平台公有云（如阿里云、腾讯云）的安装和配置指导，帮助实施人员或用户能够快速安装配置新氦云平台。

# 2.环境准备

## 2.1 服务购买

* 至少3台以上的云服务器作为集群节点；建议5台以上。

云服务器配置要求如下

|  |  |  |
| --- | --- | --- |
| **硬件** | | |
| CPU（总核数） | | ≥60 |
| 内存（总数） | | ≥ 160G |
| 存储（单机） | 系统盘（根目录） | ≥ 100GB |
| 数据盘两块（每块） | 数据盘A：Docker数据盘，300G以上  数据盘B：本地存储数据盘，500G以上 |

|  |  |
| --- | --- |
| **软件** | |
| 操作系统 | CentOS7.4 |
| 操作系统内核 | = kernel3.10.0-693 |

* 安装机器1台，安装机器和集群节点机器在一个局域网内

|  |  |
| --- | --- |
| **软件** | |
| 操作系统 | CentOS7.4 |
| 操作系统内核 | = kernel3.10.0-693 |
| **网络：** 有外网访问能力，能ssh远程登陆 | |

* 内网负载均衡
* 外网负载均衡
* 支持NFS协议的文件存储，500G以上
* 支持S3协议的对象存储

## 2.2 内网负载均衡监控端口设置

|  |  |  |  |
| --- | --- | --- | --- |
| 端口 | 绑定主机 | 映射端口 | 用途 |
| 29001 | 所有集群节点机器 | 29001 | Console gateway |
| 29003 | 所有集群节点机器 | 29003 | Console web socket |
| 29006 | 所有集群节点机器 | 29006 | Harbor |
| 6442 | 所有集群节点机器 | 6443 | API |

## 2.3 外网负载均衡监控端口设置

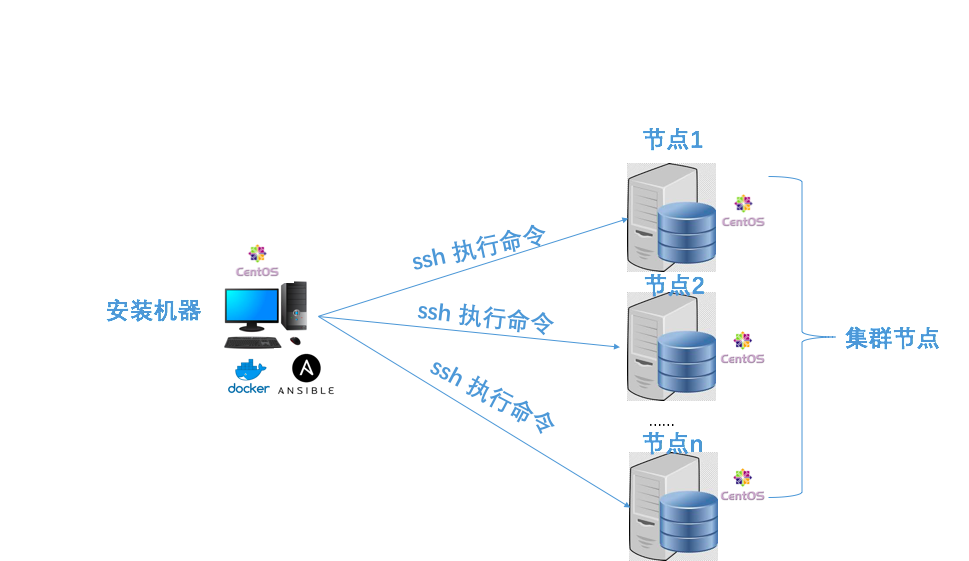
外网负载均衡

|  |  |  |  |
| --- | --- | --- | --- |
| 端口 | 绑定主机 | 映射端口 | 用途 |
| 29000 | 所有集群节点机器 | 29000 | Console UI |
| 29003 | 所有集群节点机器 | 29003 | Console web socket |
| 29002 | 所有集群节点机器 | 29002 | Console gateway http port |
| 29270 | 所有集群节点机器 | 29270 | Keycloak Port |
| 29008 | 所有集群节点机器 | 29008 | Granfana port |
| 29001 | 所有集群节点机器 | 29001 | Console gateway https port |
| 29021 | 所有集群节点机器 | 29021 | AutoScale web |
| 29004 | 所有集群节点机器 | 29004 | User guide |
| 29005 | 所有集群节点机器 | 29005 | 一体化监控 web |
| 29006 | 所有集群节点机器 | 29006 | Harbor web |
| 29312 | 所有集群节点机器 | 29312 | 大屏配置web |

# 3 安装原理

新智云平台的安装部署是基于Ansible脚本，原理如图所示。安装人员在安装机器上运行预先安装好ansible的docker容器，在容器中执行ansible命令完成产品的安装。

有关ansible的原理和介绍，请参见：https://ansible-tran.readthedocs.io/en/latest/docs/intro.html



# 4.安装步骤

## 4.1 安装机设置

### 4.1.1 拷贝安装介质

将安装包拷贝到安装机上，安装包的目录结构如图所示：

|  |
| --- |
| helium-1.4.0-release# tree -L 1  .  *├── centosrepo7.4 ---------- local repository，用于安装各种软件*  *├── k8s-ansible-script ---------ansible脚本* |

### 4.1.2 在安装机器上安装docker

|  |
| --- |
| cd centosrepo7.4/Packagse  yum install docker-common-1.13.1-53.git774336d.el7.centos.x86\_64.rpm -y  yum install -y docker-client-1.13.1-53.git774336d.el7.centos.x86\_64.rpm -y  yum install docker-1.13.1-53.git774336d.el7.centos.x86\_64.rpm -y  systemctl status docker  systemctl start docker  systemctl status docker  systemctl enable docker |

## 4.2 安装机器上启动local repo

在安装机器上启动local repo，打开terminal，执行以下命令：

|  |
| --- |
| cd centosrepo7.4  bash start\_localrepo.sh |

## 4.3 安装容器中配置ssh免密登陆

1. 进入wizard:latest容器

|  |
| --- |
| cd *k8s-ansible-script*  sudo bash scripts/start.sh |

2. 在容器中生成ssh key

|  |
| --- |
| ssh-keygen -t rsa |

一路回车即可。

2、在将生成的公钥复制到 所有集群节点机器上，使用如下命令：

|  |
| --- |
| ssh-copy-id -i /root/.ssh/id\_rsa.pub root@<node ip> |

3、测试免密码登录,

|  |
| --- |
| ssh root@<node ip> |

## 4.4 计算参数

环境： 安装容器

集群中有些参数需要根据集群的规模来决定，如大数据中一些POD的内存、CPU取值。

|  |
| --- |
| cd /opt  bash monitor/cal\_bigdata\_resource.sh *<cpu> <mem>* |

注释：

* *cpu是集群机器总CPU 单位：核*
* *mem是集群机器总内存 单位：G*

## 4.5 定制集群配置参数

1. 创建安装的配置文件

k8s-cluster/cluster/cloud/cloud.yml是配置模版文件，安装人员可以拷贝配置模版生成一份客户配置文件，操作方法如下

|  |
| --- |
| *# 在terminal中输入：*  cd k8s-ansible-script  cp –r k8s-cluster/cluster/cloud k8s-cluster/cluster/*<customername>* -r |

2、修改下列配置（红色为必须修改的配置）

k8s-cluster/cluster/*<customername>*/cloud.yml

|  |
| --- |
| ---  all:  vars:  ###### 云环境部署 #######  cloud\_name: "ali"  #####服务器时间同步##############  ## ntp\_orphan\_parents: required, recommendate use two of master node as ntp\_orphan\_parents  ntp\_orphan\_parents: [172.17.0.3, 172.17.0.10]  ## ntp\_server, optional, if not provided, cluster use ntp\_orphan\_paraents to sync  ## ntp\_server: ""  ###########集群信息############  ## master\_list three master node IP  ## required  master\_list: [172.17.0.3, 172.17.0.10,172.17.0.15]    ## etcd\_init\_servers: etcd cluster IP  ##required  ##recommmendate reuse master node ips  etcd\_init\_servers: [172.17.0.3, 172.17.0.10,172.17.0.15]  ##hanode\_list: HA node ip for KeepAlive node  ##required  ##  ##for cloud installation, keep HA as empty  ##for on premise installation, use two of master node, like master0, master1  hanode\_list: []  ##host\_path\_list: hostpath nodes list  ## required  host\_path\_list: [172.17.0.3, 172.17.0.10,172.17.0.15]  ## cluster\_name:  ## required  cluster\_name: "enc-cluster"    ## 集群中服务（service）IP  ## required  cluster\_ip\_range: "192.168.0.0/16"    ##domain: 集群DNS域名  ##required  domain: "cluster.local"    ## kl\_interface  ##comment kl\_interface or set this to "", ansible will check the default using interface.  ##or you can set this manually  kl\_interface: eth0  ### host search in /etc/resolv.conf, if exist  searchdomains: []    ### host nameserver in /etc/resolv.conf, if exist  nameservers: [183.60.83.19,183.60.82.98]    ## max\_pods: 一个节点上可以起的最大POD数  #max\_pods: 100  ## cpu\_reserved 预留的CPU  # cpu\_reserved: 0    ##memory\_reserved  #memory\_reserved: 0    ##kubelet\_dir: Kubelet的地址  #kubelet\_dir: "/data/kubelet"    ##sample\_rate: 监控数据收集频率，单位：秒／次  #sample\_rate: 30  ##flannel用的etcd节点  #required  flannel\_etcd\_list: [172.17.0.3, 172.17.0.10,172.17.0.15]    ##backend\_type： Flannel backend type： vxlan ||vxlan-over-hostgw  #backend\_type: "vxlan"  ##flanneld\_subnet： 集群中pod IP  flanneld\_subnet: "10.0.0.0/8"    ## local\_repo: local repo地址，一般是安装机器的ip:8009  local\_repo: "172.17.0.6:8009"  ##ca\_vip: 虚IP地址  ca\_vip: "172.17.0.8"  public\_vip: "212.64.45.181"    ##集群密码  admin\_password: admin    ##集群用户名  admin\_username: admin    #storage：集群默认存储类型，可选，默认是ceph，可以是ceph或者nfs或者ebs  #对于私有云：CEPH  #阿里云，华为云，腾讯云：nfs  #亚马逊：ebs  storage\_type: nfs  ##nfs地址，如果没有nfs，可以忽略  nfs\_enabled: "true"  nfs\_host: 10.66.158.232  nfs\_path: /    #ingress：Ingress dns域名  ingress\_dns\_domain: enn.ingress.cn    ##########CEPH##################  ceph\_enabled: false  # mon\_list: [10.19.140.6, 10.19.140.10, 10.19.140.14]  # osd\_list: [10.19.140.6, 10.19.140.10, 10.19.140.14]  # ceph\_public\_network: 10.19.140.0/24  # ceph\_cluster\_network: 10.19.140.0/24  # rgw\_dns\_name: enncloud.ceph.s3  # rbd\_dev\_list: [sdc]    ##############HARBOR ################  ##local\_registry\_port：无须改动  local\_registry\_port: 5000  ## harbor登陆密码  harbor\_admin\_password: admin    ########## CONSOLE##############  ## console image的版本，无须改动  console\_version: release-1.5.0  ## 公司名称；主要用于用户注册  company\_name: 新智认知  ## branding  title\_cn: 新智认知新氦云平台  title\_en: ENC Cloud Platform +  ## CONSOLE 默认登陆密码  keystone\_admin\_password: admin  ## CONSOLE LICENSE，  is\_trial\_version: 2 # 1: 试用版 2：正式版  months: 0 #使用月数 （正式版请输入0）  days: 0 #使用天数 （正式版请输入0）  # will be override by script for ceph s3 case  # 对于私有安装：无须填写  # 对于云安装，请填写 s3\_host s3\_access\_key s3\_secret\_key  s3\_host: cos.ap-shanghai.myqcloud.com  s3\_access\_key: rSounUvBG7i38zd1A4j9JDuOhofGfohS  s3\_secret\_key: AKIDwFLCnFQZNkvqWwA3lDPP9drpY1D9mMZW  #bigdata image vesion; 无须改动  release\_version: helium-1.4.0  children:  centos:  vars:  #机器域名默认前缀  hostname\_prefix: enn  ansible\_ssh\_user: root  ansible\_ssh\_pass: Test1234  ansible\_ssh\_port: 22  bin\_dir: "/usr/bin"  cgroup\_driver: "systemd"  ###对于物理盘进行分区：通常对HOSTPATH和DOCKER盘需要分区  special\_mounts:  /dev/vdc:  path: /xfs/disk1  opt: prjquota  /dev/vdb:  path: /data  opt: defaults  hosts:  172.17.0.3:  172.17.0.10:  172.17.0.15: |

**注：配置时需要保证cluster\_ip\_range、flanneld\_subnet与三台master集群IP不在同一个网段。**

## 4.6 启动安装脚本

1、进入opt

|  |
| --- |
| cd /opt |

2、启动安装脚本

|  |
| --- |
| ansible-playbook -i k8s-cluster/cluster/*<customername>*/cloud.yml playbook/cloud.yml |