# 阿里云

阿里云最佳实践 企业软件上云

文档版本: 20210527

(一) 阿里云

阿里云最佳实践 企业软件上云·法律声明

### 法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。 如果您阅读或使用本文档,您的阅读或使用行为将被视为对本声明全部内容的认可。

- 1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档,且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息,您应当严格遵守保密义务;未经阿里云事先书面同意,您不得向任何第三方披露本手册内容或提供给任何第三方使用。
- 2. 未经阿里云事先书面许可,任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部,不得以任何方式或途径进行传播和宣传。
- 3. 由于产品版本升级、调整或其他原因,本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利,并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。
- 4. 本文档仅作为用户使用阿里云产品及服务的参考性指引,阿里云以产品及服务的"现状"、"有缺陷"和"当前功能"的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引,但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的,阿里云不承担任何法律责任。在任何情况下,阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害,包括用户使用或信赖本文档而遭受的利润损失,承担责任(即使阿里云已被告知该等损失的可能性)。
- 5. 阿里云网站上所有内容,包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计,均由阿里云和/或其关联公司依法拥有其知识产权,包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意,任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外,未经阿里云事先书面同意,任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称(包括但不限于单独为或以组合形式包含"阿里云"、"Aliyun"、"万网"等阿里云和/或其关联公司品牌,上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司)。
- 6. 如若发现本文档存在任何错误,请与阿里云取得直接联系。

# 通用约定

格式	说明	样例
⚠ 危险	该类警示信息将导致系统重大变更甚至故 障,或者导致人身伤害等结果。	⚠ 危险 重置操作将丢失用户配置数据。
☆ 警告	该类警示信息可能会导致系统重大变更甚至故障,或者导致人身伤害等结果。	
☆注意	用于警示信息、补充说明等,是用户必须 了解的内容。	(大) 注意 权重设置为0,该服务器不会再接受新 请求。
② 说明	用于补充说明、最佳实践、窍门等 <i>,</i> 不是用户必须了解的内容。	② 说明 您也可以通过按Ctrl+A选中全部文 件。
>	多级菜单递进。	单击设置> 网络> 设置网络类型。
粗体	表示按键、菜单、页面名称等UI元素。	在 <b>结果确认</b> 页面,单击 <b>确定</b> 。
Courier字体	命令或代码。	执行 cd /d C:/window 命令,进入 Windows系统文件夹。
斜体	表示参数、变量。	bae log listinstanceid  Instance_ID
[] 或者 [a b]	表示可选项,至多选择一个。	ipconfig [-all -t]
{} 或者 {a b}	表示必选项,至多选择一个。	switch {active stand}

企业软件上云·<mark>目录</mark>

# 目录

阿里云最佳实践

1.SAP HANA同可用区高可用部署	05
2.Mendix部署阿里云容器服务最佳实践	23
3.金蝶云星空企业版配置阿里云RDS	24
4.红帽OpenShift安装部署	26

### 1.SAP HANA同可用区高可用部署

本文档介绍了如何在公共云环境同可用区部署SAP HANA的高可用环境。

#### 背景信息

镜像版本支持SLES for SAP 11/12/15。

#### 名词解释

#### VPC

专有网络VPC(Virtual Private Cloud)是基于阿里云构建的一个隔离的网络环境,专有网络之间逻辑上彻底隔离。专有网络是您自己独有的的云上私有网络。

#### ECS

云服务器ECS(Elastic Compute Service)是阿里云提供的性能卓越、稳定可靠、 弹性扩展的 laaS(Infrastructure as a Service)级别云计算服务。

#### ENI

弹性网卡ENI(Elastic Network Interface)是一种可以附加到专有网络VPC类型 ECS实例上的虚拟网卡,通过弹性网卡,您可以实现高可用集群搭建、低成本故障 转移和精细化的网络管理。

#### HAVIP

高可用虚拟IP HAVIP(Private High-Availability Virtual IP Address),是一种可以 独立创建和释放的私网IP资源。这种私网IP的特殊之处在于,用户可以在ECS上 使用ARP协议进行该IP的宣告。

#### ● 共享块存储

共享块存储是一种支持多台ECS实例并发读写访问的数据块级存储设备,具备多并发、高性能、高可靠等特性。常用于高可用架构数据库集群Oracle RAC(Real Application Cluster)以及高可用架构服务器集群(High-availability cluster)的场景。

#### ● 地域

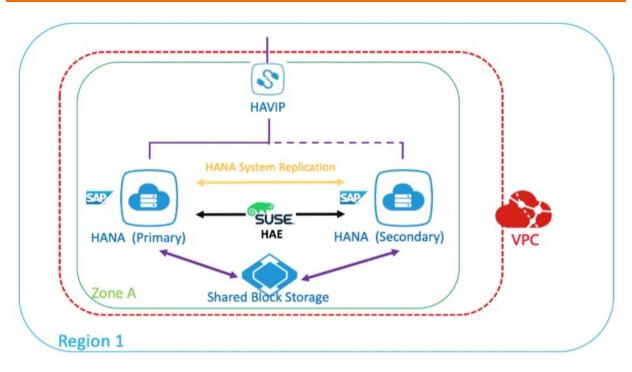
地域(Region)是指物理的数据中心。资源创建成功后不能更换地域。

#### • 可用区

可用区(Zone)是指在同一地域内,电力和网络互相独立的物理区域。同一可用区内实例之间的网络延时更小。

#### 架构介绍

阿里公共云支持SAP HANA在同可用区的高可用部署,通过配置SAP HANA的System Replication功能,结合 Suse HAE实现自动切换。



### 准备工作

#### ● SAP安装介质准备

工具	访问方式	备注
Windows跳板机	在跳板机上安装SAP Download Manager下载介质上传到OSS或直 接挂载到ECS	跳板机需使用EIP或NAT具备公网访 问能力
OSS工具	将本机介质通过OSS工具(如 ossutil)上传到客户的 oss bucket	无

#### ● 网络规划

网络	地域	用途	子网
业务网	华东2 可用区F	For Business/SR	192.168.10.0/24
心跳网	华东2 可用区F	For HA	192.168.20.0/24

#### • 主机规划

主机名	角色	心跳地址	业务地址	高可用虚拟 IP(HAVIP)
saphana-01	HANA主节点	192.168.20.19	192.168.10.168	192.168.10.12
saphana-02	HANA备节点	192.168.20.20	192.168.10.169	192.100.10.12

#### • 文件系统规划

类型	大小	文件系统	VG	LVM条带	挂载点
数据盘	800G	XFS	datavg	是	/hana/data
数据盘	400G	XFS	datavg	是	/hana/log
数据盘	300G	XFS	datavg	是	/hana/shared
数据盘	50G	XFS	sapvg	是	/usr/sap

#### 云资源配置

#### 创建VPC和ECS

使用ECS之前,您需要先创建VPC和Vswitch。请根据实际情况创建所需的VPC和 Vswitch。

- 1. 登录阿里云控制台https://vpc.console.aliyun.com/。
- 2. 按规划在上海可用区F, 创建 192.168.0.0/16的网段和192.168.10.0/24(业务)、192.168.20.0/24(心跳)这两个子网。
- 3. 登录阿里云控制台https://ecs.console.aliyun.com/。
- 4. 按规划创建两台HANA ECS。

#### 创建其他云资源

在部署SAP同可用区高可用环境前,您需要先创建共享块存储和高可用虚拟IP。

共享块存储作为高可用集群的STNOITH设备,用来fence故障节点。

高可用虚拟IP作为集群中的虚拟IP挂载到集群中的活动主节点,本示例作为HANA实例对 外提供服务的虚拟IP地址。

- 1. 登录阿里云控制台,**云服务器>存储与快照>共享块存储**,创建共享块存储;在 ECS同地域同可用区下,创建一个20G SSD共享块存储。
- 2. 创建完后分别挂载到集群中两台ECS实例。
- 3. 登录阿里云控制台, **云服务器>网络与安全>专有网络VPC>高可用虚拟IP**, 创建高可用虚拟IP; 按规划这里创建192.168.10.12, 并挂载到刚才新建的两台HANA ECS。

#### HANA ECS配置

#### ● 主机名及DNS解析

分别在HA 集群两台HANA 服务器上,实现两台HANA ECS之间的主机名称解析。

本示例的/etc/hosts:

127.0.0.1 localhost 192.168.10.168 saphana-01 saphana-01 192.168.10.169 saphana-02 saphana-02 192.168.20.19 hana-ha01 hana-ha01 192.168.20.20 hana-ha02 hana-ha02

#### • ECS SSH互信

HA集群的两台HANA ECS的需要配置SSH互信。

○ 配置认证公钥

#### 在HANA主节点执行如下命令:

```
saphana-01:~ # ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa): 直接回车
Enter passphrase (empty for no passphrase): 直接回车
Enter same passphrase again: 直接回车
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:6lX54zFixfUF7Ni+yEn8+lzBjj4XSF4QoVjznKNx15M root@saphana-01
The key's randomart image is:
+---[RSA 2048]----+
     0 ++ |
    0.0.0
    . o XoEo
    0=0*00
   S 00=.00.
  ..000+..
  .. 00== 00
| ...o=*oo|
| . o+= |
+----[SHA256]-----+
saphana-01:~ # ssh-copy-id -i /root/.ssh/id_rsa.pub root@192.168.10.169
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/root/.ssh/id_rsa.pub"
The authenticity of host '192.168.10.169 (192.168.10.169)' can't be established.
ECDSA key fingerprint is
SHA256:iD5aepnspZcREGbGJpExnMd3YGXPM8FcmSq66KLCgsk.
Are you sure you want to continue connecting (yes/no)? yes
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are
already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to
install the new keys
Password: 输入备节点root密码
Number of key(s) added: 1
Now try logging into the machine, with: "ssh 'root@192.168.10.169'"
and check to make sure that only the key(s) you wanted were added.
saphana-01:~#
```

#### 在hana备节点上执行如下命令:

```
saphana-02:~ # ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:116JLe/MTR494dejsZkgrtvfFdL6+WwGnmcc9QD38Zcroot@saphana-02
The key's randomart image is:
+---[RSA 2048]----+
     . .. |
     0.+
     .ooE=
   S.+.+=+|
    ..+=.*|
    ...+.X*
    0.0+@=%
   000.. *+B*
+----[SHA256]-----+
saphana-02:~ # ssh-copy-id -i /root/.ssh/id_rsa.pub root@192.168.10.169
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/root/.ssh/id_rsa.pub"
The authenticity of host '192.168.10.169 (192.168.10.169)' can't be established.
ECDSA key fingerprint is
SHA256:iD5aepnspZcREGbGJpExnMd3YGXPM8FcmSq66KLCgsk.
Are you sure you want to continue connecting (yes/no)? yes
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are
already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to
install the new keys
Password:
Number of key(s) added: 1
Now try logging into the machine, with: "ssh 'root@192.168.10.169'"
and check to make sure that only the key(s) you wanted were added.
```

#### ○ 配置验证结果

分别在两个节点上,使用 SSH 登录另外一个节点,如果不需要密码登录,则说明互信已经建立。

```
saphana-01:~ # ssh saphana-02
Last login: Mon Apr 22 23:36:01 2019 from 192.168.10.168
Welcome to Alibaba Cloud Elastic Compute Service!
saphana-02:~ #
```

在hana备节点,进行验证:

在hana主节点,进行验证:

```
saphana-02:~ # ssh saphana-01
Last login: Mon Apr 22 23:36:21 2019 from 192.168.10.169
Welcome to Alibaba Cloud Elastic Compute Service!
saphana-01:~ #
```

#### ● 部署ECS Metrics Collector for SAP监控代理

ECS Metrics Collector监控代理程序,用于云平台上SAP系统收集需要的虚拟机配置信息和 底层物理资源使用相关的信息,供日后做性能统计和问题分析使用。 每台SAP应用和数据库都需要安装Metrics Collector,监控代理的部署请参考ECS Metrics Collector for SAP部署指南。

#### • 文件系统划分

按前面的文件系统规划,用LVM来管理和配置云盘(集群两个节点)。

有关LVM分区的介绍,请参考LVM HOWTO。

#### ○ 创建PV和VG

# pvcreate /dev/vdb /dev/vdc /dev/vdd /dev/vdg
Physical volume "/dev/vdb" successfully created
Physical volume "/dev/vdc" successfully created
Physical volume "/dev/vdd" successfully created
Physical volume "/dev/vdg" successfully created
# vgcreate hanavg /dev/vdb /dev/vdc /dev/vdd
Volume group "hanavg" successfully created
# vgcreate sapvg /dev/vdg
Volume group "sapvg" successfully created

#### 。 创建LV

# lvcreate -l 100%FREE -n usrsaplv sapvg
Logical volume "usrsaplv" created.
将三块500G的SSD云盘配置条带化
# lvcreate -L 800G -n datalv -i 3 -l 64 hanavg
Rounding size (204800 extents) up to stripe boundary size (204801 extents).
Logical volume "datalv" created.
# lvcreate -L 400G -n loglv -i 3 -l 64 hanavg
Rounding size (102400 extents) up to stripe boundary size (102402 extents).
Logical volume "loglv" created.
# lvcreate -l 100%FREE -n sharedlv -i 3 -l 64 hanavg
Rounding size (38395 extents) down to stripe boundary size (38394 extents)
Logical volume "sharedlv" created.

#### ○ 创建挂载点并格式化文件系统

# mkdir-p /usr/sap /hana/data /hana/log /hana/shared # mkfs.xfs /dev/sapvg/usrsaplv # mkfs.xfs /dev/hanavg/datalv # mkfs.xfs /dev/hanavg/loglv # mkfs.xfs /dev/hanavg/sharedlv

#### ○ 挂载文件系统并加到开机自启动项

# vim /etc/fstab 添加下列项: /dev/mapper/hanavg-dataly /hana/data xfs defaults 0 0 /dev/mapper/hanavg-loglv /hana/log xfs defaults 0 0 /dev/mapper/hanavg-sharedly /hana/shared xfs defaults 0 0 /dev/mapper/sapvg-usrsaplv/usr/sap xfs defaults 0 0 /dev/vdf swap swap defaults 0 0 # mount -a #df-h Filesystem Size Used Avail Use% Mounted on devtmpfs 32G 0 32G 0%/dev 48G 55M 48G 1%/dev/shm tmpfs tmpfs 32G 768K 32G 1%/run /dev/vda1 99G 30G 64G 32%/ 6.3G 16K 6.3G 1%/run/user/0 tmpfs /dev/mapper/hanavg-datalv 800G 34M 800G 1%/hana/data /dev/mapper/sapvg-usrsaplv 50G 33M 50G 1%/usr/sap /dev/mapper/hanavg-loglv 400G 33M 400G 1%/hana/log /dev/mapper/hanavg-sharedly 300G 33M 300G 1% /hana/shared

#### 安装SAP HANA并配置HANA System replication

● 安装SAP HANA

HANA的主节点和备节点的System ID和Instance ID要相同。本示例的HANA的System ID为H01,Instance ID为00。

有关SAP HANA的安装请参考SAP HANA Platform。

配置HANA System Replication

有关SAP HANA System Replication的配置请参考How To Perform System Replication for SAP HANA。

#### SLES HAE安装与配置

● 安装SLES HAE软件

有关SLES HAE的文档请参考SUSE Linux Enterprise High Availability Extension 12。

在主、备节点,检查是否已经安装HAE组件和SAPHanaSR组件。

文 注意 本示例使用的是SLES for SAP 12 SP3 CSP(Cloud Service Provider)镜像,此镜像已经预置了阿里云SUSE SMT Server配置,可直接进行组件检查和安装。如果您使用的是自定义镜像,请先购买SUSE授权以获得并注册到SUSE官方的SMT Server或者手工配置zypper repository源,才能进行后面的操作。

#### 配置SLES HAE和安装管理SAP HANA资源,需要以下组件:

- o patterns-ha-ha\_sles
- SAPHanaSR
- sap\_suse\_cluster\_connector
- o patterns-sle-gnome-basic

用以下命令安装需要的组件:

zypper in patterns-ha-ha\_sles SAPHanaSR sap\_suse\_cluster\_connector

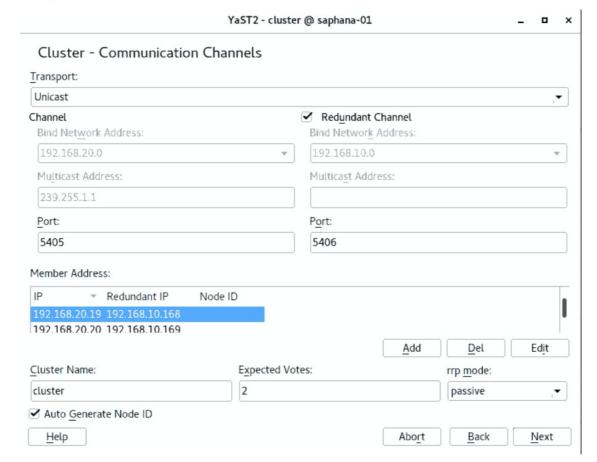
#### ● 配置集群

本示例使用VNC打开图形界面,在HANA主节点上配置Corosync。

#### yast2 cluster

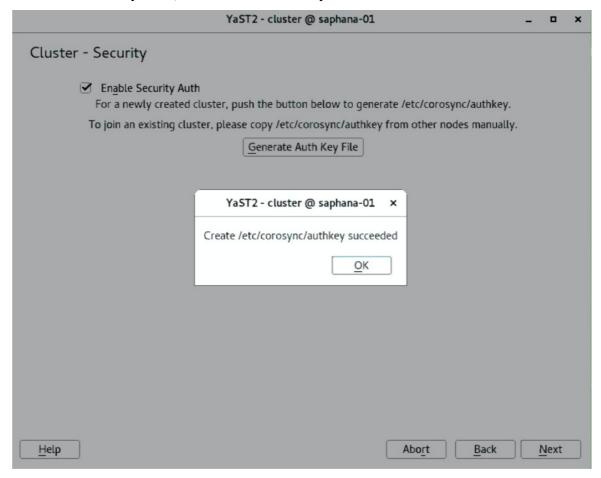
#### ○ 配置communication channels

- Channel选择心跳网段, Redundant Channel选择业务网段。
- 按正确的顺序依次添加Member address(前心跳地址,后业务地址)。
- Excepted Votes: 2。
- Transport: Unicast。



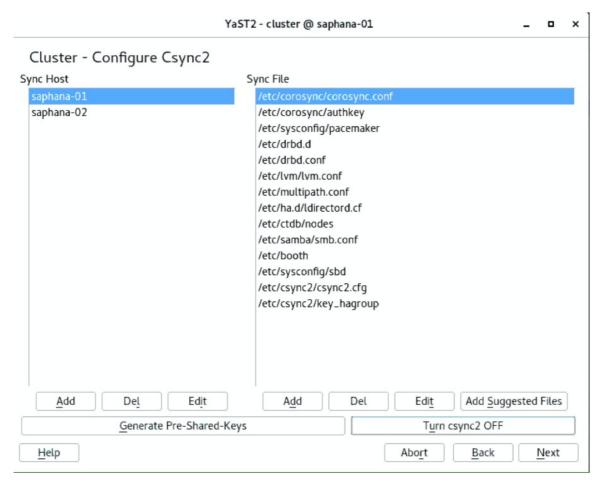
#### ○ 配置Security

选中Enable Security Auth,单击Generate Auth Key File。

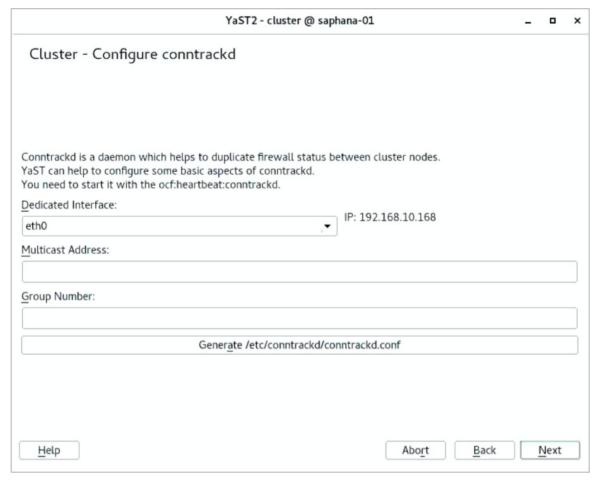


#### ○ 配置Csync2

- 添加Sync host
- 点击Add Suggested Files
- 点击Generate Pre-Shared-Keys
- 点击Turn csync2 ON

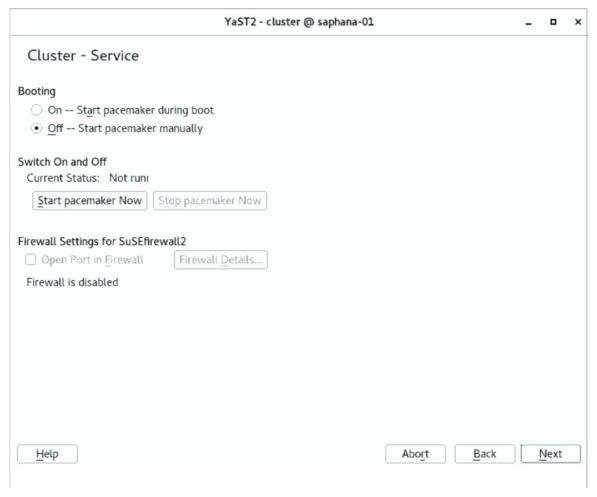


Configure conntrackd这一步使用默认,直接下一步。



#### ○ 配置Service

确认Cluster服务不要设成开机自启动。



配置完成后保存退出,将Corosync配置文件复制到hana备节点,在主节点执行以下命令:

#sudo scp -pr /etc/corosync/authkey /etc/corosync/corosync.conf root@saphana-02:/etc/corosync/

#### ● 验证集群状态

在两个节点中分别执行如下命令,启动pacemaker服务。

#### # systemctl start pacemaker

确认集群中两个节点的状态为online。

# crm\_mon -r Stack: corosync

Current DC: saphana-02 (version 1.1.16-4.8-77ea74d) - partition with quorum

Last updated: Tue Apr 23 11:22:38 2019

Last change: Tue Apr 23 11:22:36 2019 by hacluster via crmd on saphana-02

2 nodes configured 0 resources configured

Online: [ saphana-01 saphana-02 ]

No resources

激活hawk2的web服务。

```
# passwd hacluster

New password:
Retype new password:
passwd: password updated successfully
# systemctl restart hawk.service
```

设置hawk2服务开机自启动。

# systemctl enable hawk.service

#### 配置SBD (仲裁盘)

请确认已经按规划将20G的共享块存储正确挂载到了两台ECS上,本示例仲裁盘为 /dev/def。

```
saphana-01:~# lsblk
NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
vda 253:0 0 100G 0 disk
└─vda1 253:1 0 100G 0 part /
vdb 253:16 0 500G 0 disk
vdc 253:32 0 500G 0 disk
vdd 253:48 0 500G 0 disk
vde 253:64 0 64G 0 disk
vdf 253:80 0 20G 0 disk
saphana-02:~# lsblk
NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
vda 253:0 0 100G 0 disk
└─vda1 253:1 0 100G 0 part /
vdb 253:16 0 500G 0 disk
vdc 253:32 0 500G 0 disk
vdd 253:48 0 500G 0 disk
vde 253:64 0 64G 0 disk
vdf 253:80 0 20G 0 disk
```

#### • 配置 watchdog (集群两个节点)

```
# echo "modprobe softdog" > /etc/init.d/boot.local
# echo "softdog" > /etc/modules-load.d/watchdog.conf
# modprobe softdog
**watchdog配置检查**
saphana-01:~ # ls -l /dev/watchdog
crw------ 1 root root 10, 130 Apr 23 12:09 /dev/watchdog
saphana-01:~ # lsmod | grep -e wdt -e dog
softdog 16384 0
saphana-01:~ # grep -e wdt -e dog /etc/modules-load.d/watchdog.conf
softdog
```

#### ● 配置SBD (集群两个节点)

```
可用部署
```

```
# sbd -d /dev/vdf create
Initializing device /dev/vdf
Creating version 2.1 header on device 4 (uuid: e3874a81-47ae-4578-b7a2-4b32bd139e07)
Initializing 255 slots on device 4
Device /dev/vdf is initialized.
# sbd -d /dev/vdf dump
==Dumping header on disk /dev/vdf
Header version : 2.1
UUID
          : e3874a81-47ae-4578-b7a2-4b32bd139e07
Number of slots : 255
Sector size : 512
Timeout (watchdog): 5
Timeout (allocate): 2
Timeout (loop) :1
Timeout (msgwait):10
==Header on disk /dev/vdf is dumped
配置SBD参数:
# vim /etc/sysconfig/sbd
修改以下参数:
SBD_DEVICE="/dev/vdf" - 修改成SBD的云盘设备ID
SBD_STARTMODE="clean"
```

#### ● 验证SBD服务

两个节点分别启动sbd:

SBD\_OPTS="-W"

```
#/usr/share/sbd/sbd.sh start
```

#### 验证SBD进程:

```
# ps -ef | grep sbd
root 16148 1 0 14:02 pts/0 00:00:00 sbd: inquisitor
root 16150 16148 0 14:02 pts/0 00:00:00 sbd: watcher: /dev/vdf - slot: 1 - uuid:
9b620112-1031-48b8-9510-8e1b77032472
root 16151 16148 0 14:02 pts/0 00:00:00 sbd: watcher: Pacemaker
root 16152 16148 0 14:02 pts/0 00:00:00 sbd: watcher: Cluster
root 16162 15254 0 14:05 pts/0 00:00:00 grep --color=auto sbd
检查SBD状态
#sbd -d /dev/vdf list
```

#### 确保两个节点的状态为clear:

```
#/usr/bin # sbd -d /dev/vdf list
0 saphana-01 clear
1 saphana-02 clear
```

#### SBD fence验证:

⑦ 说明 请确保被fence的节点重要的服务进程已关闭。

本示例,登录主节点saphana01,准备fence掉备节点saphana02:

saphana-01 # sbd -d /dev/vdf message saphana-02 reset

如果备节点saphana-02正常重启,表示SBD盘配置成功。

### SAP HANA与SLES HAE集成

● 使用SAPHanaSR配置SAP HANA资源

在任意集群节点,新建脚本文件,替换脚本中的HANA SID、Instance Number和HAVIP三个参数。本示例中,HANA SID: *H01*,Instance Number: *00*,HAVIP: *192.168.10.12*,脚本文件名*HANA\_HA\_script.sh*。

```
###SAP HANA Topology is a resource agent that monitors and analyze the HANA
landscape and communicate the status between two nodes##
primitive rsc_SAPHanaTopology_HDB ocf:suse:SAPHanaTopology \
   operations $id=rsc_SAPHanaTopology_HDB-operations \
   op monitor interval=10 timeout=600 \
   op start interval=0 timeout=600 \
   op stop interval=0 timeout=300 \
   params SID=H01 InstanceNumber=00
###This file defines the resources in the cluster together with the Virtual IP###
primitive rsc_SAPHana_HDB ocf:suse:SAPHana \
   operations $id=rsc_SAPHana_HDB-operations \
   op start interval=0 timeout=3600 \
   op stop interval=0 timeout=3600 \
   op promote interval=0 timeout=3600 \
   op monitor interval=60 role=Master timeout=700 \
   op monitor interval=61 role=Slave timeout=700 \
   params SID=H01 InstanceNumber=00 PREFER_SITE_TAKEOVER=true
DUPLICATE_PRIMARY_TIMEOUT=7200 AUTOMATED_REGISTER=false
#This is for sbd setting##
primitive rsc_sbd stonith:external/sbd \
   op monitor interval=20 timeout=15 \
   meta target-role=Started maintenance=false
#This is for VIP resource setting##
primitive rsc_vip IPaddr2 \
   operations $id=rsc_vip-operations \
   op monitor interval=10s timeout=20s \
   params ip=192.168.10.12
ms msl_SAPHana_HDB rsc_SAPHana_HDB \
   meta is-managed=true notify=true clone-max=2 clone-node-max=1 target-
role=Started interleave=true maintenance=false
clone cln_SAPHanaTopology_HDB rsc_SAPHanaTopology_HDB \
   meta is-managed=true clone-node-max=1 target-role=Started interleave=true
maintenance=false
colocation col_saphana_ip_HDB 2000: rsc_vip:Started msl_SAPHana_HDB:Master
order ord_SAPHana_HDB 2000: cln_SAPHanaTopology_HDB msl_SAPHana_HDB
property cib-bootstrap-options: \
   have-watchdog=true \
   cluster-infrastructure=corosync \
  cluster-name=cluster \
   no-quorum-policy=ignore \
   stonith-enabled=true \
   stonith-action=reboot \
   stonith-timeout=150s
op_defaults op-options: \
   timeout=600 \
   record-pending=true
```

运行以下命令使HAE接管SAP HANA:

```
crm configure load update HANA_HA_script.sh
```

#### ● 验证集群状态

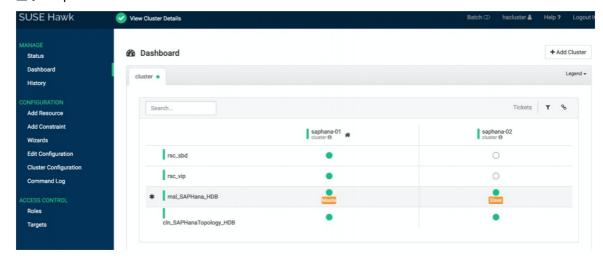
正常的集群资源状态:

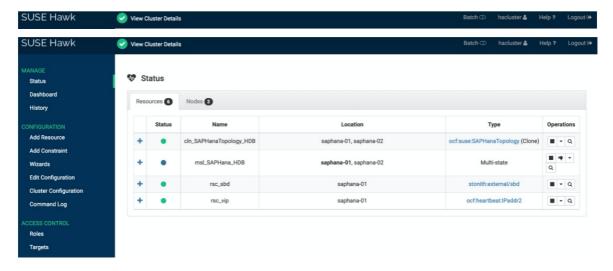
- sbd和vip资源在当前的主节点。
- SAPHana\_HDB资源,在mast er和slave节点分别为绿色。
- SAPHanaTopolopy资源,在master和slave节点同时为绿色。

可以通过crmsh或hawk图形化界面来管理和配置HAE资源。

○ 通过Hawk web管理

登录 https://<ECS IP address>:7630





#### ○ 通过crmsh管理

# crm\_mon -r Stack: corosync

Current DC: saphana-01 (version 1.1.16-4.8-77ea74d) - partition with quorum

Last updated: Wed Apr 24 11:48:38 2019

Last change: Wed Apr 24 11:48:35 2019 by root via crm\_attribute on saphana-01

2 nodes configured 6 resources configured

Online: [saphana-01 saphana-02]

Full list of resources:

rsc\_sbd (stonith:external/sbd): Started saphana-01
rsc\_vip (ocf::heartbeat:IPaddr2): Started saphana-01
Master/Slave Set: msl\_SAPHana\_HDB [rsc\_SAPHana\_HDB]

Masters: [saphana-01] Slaves: [saphana-02]

Clone Set: cln\_SAPHanaTopology\_HDB [rsc\_SAPHanaTopology\_HDB]

Started: [saphana-01 saphana-02]

#### 关联文档

● 有关SAP系统高可用测试和维护请参考SAP高可用测试最佳实践。

● 有关SAP系统高可用环境维护请参考SAP高可用环境维护指南SAP高可用环境维。

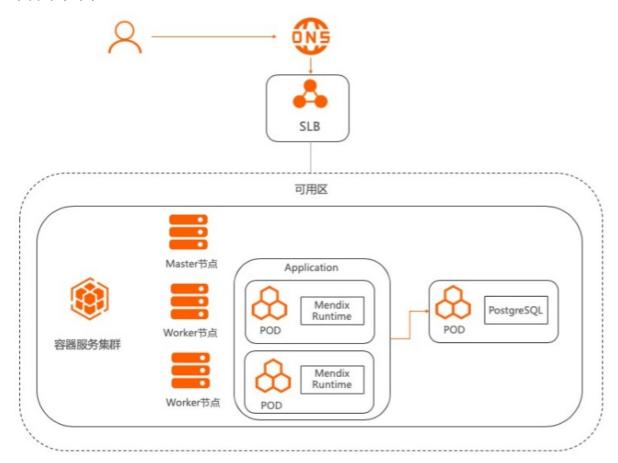
# 2.Mendix部署阿里云容器服务最佳实践

介绍西门子低代码应用开发平台Mendix应用如何快速托管到阿里云容器服务。

#### 方案优势

- 快速部署。自建集群手工配置繁琐,需要专业人员数天到数周的时间,托管部署只需要数分钟。
- 成本低廉。不需要部署常规的本地服务器, 只需较少的启动成本。
- 随用随取。根据业务灵活创建和释放资源, 满足测试验证需求。

#### 部署架构图



#### 详细信息

点击查看最佳实践详情。

#### 更多最佳实践

点击查看更多阿里云最佳实践。

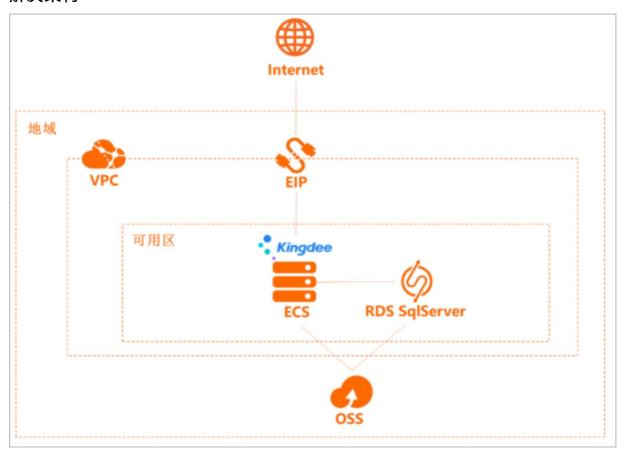
## 3.金蝶云星空企业版配置阿里云RDS

在阿里云上部署金蝶云星空企业版,并使用阿里云RDS SQL Server数据库。

#### 背景描述

金蝶云星空是金蝶公司主打产品,已获得工信部"中国云服务联盟百万企业上云推进大会主委会"的授权合作伙伴资格,成为"百万企业上云行动战略合作伙伴"。现在有很多客户在阿里云上部署金蝶云星空。阿里云RDS SQL Server最高管理员权限是"阉割版"的。金蝶云星空无法正常部署,所有在金蝶与星空客户都遇到过这个问题,然后自行搭建SqlServer数据库。为了解决这个权限问题,提供了本最佳实践,可以让客户在阿里云使用金蝶云星空+阿里云RDS SQL Server。

#### 解决架构



#### 方案优势

- 快速开通资源。不需要部署常规的本地服务器,云上快速开通云服务器ECS等资源。
- 节省成本。阿里云RDS自带微软SQL Server的软件许可,无需购置数据库服务器硬件或软件,节省大量成本。
- 按需变配。在业务初期,可以购买小规格的RDS实例来应对业务压力。随着数据库压力和数据存储量的增加,可以降低实例规格,节省费用。

#### 详细信息

点击查看最佳实践详情。

### 更多最佳实践

点击查看更多阿里云最佳实践。

# 4.红帽OpenShift安装部署

本最佳实践在红帽OpenShift的英文官方安装指南的基础上,提供了在阿里云上安装部署红帽OpenShift软件的中文详细指导。

#### 前提条件

在进行本实践前,您需要完成以下准备工作:

- 1. 注册阿里云账号,并完成实名认证。您可以登录阿里云控制台,并前往<mark>实名认证页面</mark>查看是否已经完成 实名认证。
- 2. 阿里云账户余额大于100元。您可以登录阿里云控制台,并前往账户总览页面查看账户余额。
- 3. 使用阿里云账号开通以下阿里云产品:
  - 专有网络VPC,点击查看产品详情。
  - 云服务器ECS,点击查看产品详情。
  - 对象存储,点击查看产品详情。
  - 云解析DNS,点击查看产品详情。

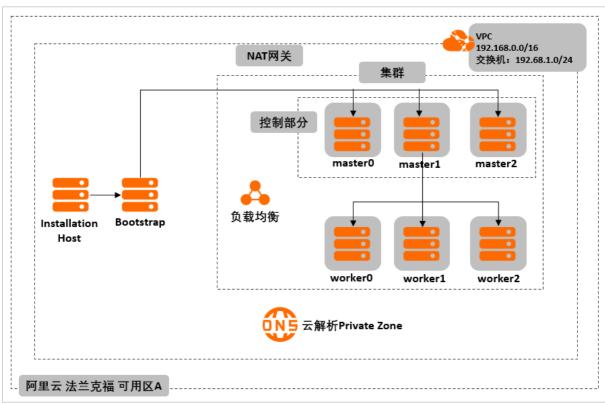
#### 背景信息

红帽OpenShift容器平台将开发人员和IT运维团队统一到了一个平台上,从而可以跨混合云和多云基础架构方便地构建、部署和管理应用。红帽OpenShift能够使企业在交付现代和传统应用的过程中,缩短开发周期,降低运营成本,从而取得更大收益。红帽OpenShift构建于开源创新和行业标准的基础上,包括Kubernetes和红帽企业Linux®(世界领先的企业级Linux发行版)。

红帽OpenShift提供两种安装部署方式,Installer-provisioned infrastructure (IPI) 以及User-provisioned infrastructure (UPI) 。本最佳实践用于指导您在阿里云上使用UPI模式bare metal方式安装部署红帽OpenShift。

#### 署

#### 本最佳实践系统架构图如下:



产品或服务	本文示例	备注
专有云VPC	名称: osVPC IPv4: 192.168.0.0/16 资源组: 默认资源组	法兰克福,可用区A 交换机: osVSW lpV4: 192.168.1.0/24
	名称: oslnstaller ecs.sn2ne.large(2vCP, 8GiB) 系统盘: 100GiB, 按量付费	操作系统: CentOS 8.1 64-bit 地域信息: 法兰克福,可用区A 私网地址: 192.168.1.53 目录设置:  OpenShift安装文件: /mnt <installation_directory>: /Install_Dir <storage_directory>: /osStorage/alicloud <sim_directory>: /simRoot</sim_directory></storage_directory></installation_directory>
	名称: bootstrap ecs.sn2ne.xlarge(4vcpu, 16GiB) 系统盘: 100GiB, 按量付费	红帽coreOS 地域信息:法兰克福,可用区A 私网地址:192.168.1.59

产品或服务	本文示例	备注
	名称: master0 ecs.sn2ne.xlarge(4vcpu, 16GiB) 系统盘: 100GiB, 按量付费	操作系统:红帽coreOS 地域信息:法兰克福,可用区A 私网地址:192.168.1.61
弹性计算ECS	名称: master1 ecs.sn2ne.xlarge(4vcpu, 16GiB) 系统盘: 100GiB, 按量付费	操作系统:红帽coreOS 地域信息:法兰克福,可用区A 私网地址:192.168.1.62
	名称: master2 ecs.sn2ne.xlarge(4vcpu, 16GiB) 系统盘: 100GiB, 按量付费	操作系统:红帽coreOS 地域信息:法兰克福,可用区A 私网地址:192.168.1.63
	名称: worker0 ecs.sn2ne.xlarge(4vcpu, 16GiB) 系统盘: 100GiB, 按量付费	操作系统:红帽coreOS 地域信息:法兰克福,可用区A 私网地址:192.168.1.64
	名称: worker1 ecs.sn2ne.xlarge(4vcpu, 16GiB) 系统盘: 100GiB, 按量付费	操作系统:红帽coreOS 地域信息:法兰克福,可用区A 私网地址:192.168.1.65
	名称: worker2 ecs.sn2ne.xlarge(4vcpu, 16GiB) 系统盘: 100GiB, 按量付费	操作系统:红帽coreOS 地域信息:法兰克福,可用区A 私网地址:192.168.1.66
负载均衡SLB	名称:osSLB 私网类型,slb.s1.small,按流量付费	地域信息:法兰克福,可用区A 服务地址(私网):192.168.1.54
对象存储OSS	Bucket名称:ostestfrankfurt 标准存储, 私有	地域信息:法兰克福,可用区A
云解析Private Zone	Private Zone名称:testos.com	地域信息:法兰克福,可用区A 名称:testos.com 关联osVPC

### 阿里云环境部署

署

首先,您需要完成阿里云上的一系列环境部署,包括专有网络VPC的创建,Installation Host的创建以及负载均衡SLB的创建。这些是您开启后续红帽OpenShift安装的必要条件。

- 1. 创建VPC和vSwitch。
  - i. 登录阿里云管理控制台。
  - ii. 通过产品与服务导航,定位到专有网络VPC,单击进入专有网络VPC管理控制台。



iii. 在页面上方,选择地域为**法兰克福**。



iv. 在专有网络页面,单击下方的创建专有网络。



v. 在创建专有网络页面,进行专有网络和交换机相关参数配置,具体配置描述见下表。



类别	配置项	说明
	名称	osVPC
专有网络	IPv4网段	推荐网段 192.168.0.0/16
	名称	osVSW
	可用区	法兰克福,可用区A
交换机		

类别	配置项	说明
	IPv4网段	192.168.1.0/24

- vi. 参数配置完成,单击**确定**。
- vii. 等待专有网络和交换机创建成功,单击完成。
- 2. 创建Inst allation Host。在您完成专有网络VPC的创建后,请继续Inst allation Host的创建。该服务器主要用于红帽OpenShift集群的安装,集群的登陆。
  - i. 登录阿里云控制台。
  - ii. 通过产品与服务导航,定位到云服务器ECS,单击进入云服务器ECS控制台。



iii. 在左侧导航栏选择实例, 地域选择为法兰克福, 并单击创建实例。



iv. 在自定义购买模式下,配置相关参数。



#### 在网络和安全组页面,参考下表,配置相关参数。

存储

镜像

类别	配置项	说明
	网络	专有网络 选择在第1章中创建的VPC(osVPC)和交换机(osVSW)

的Linux操作系统。

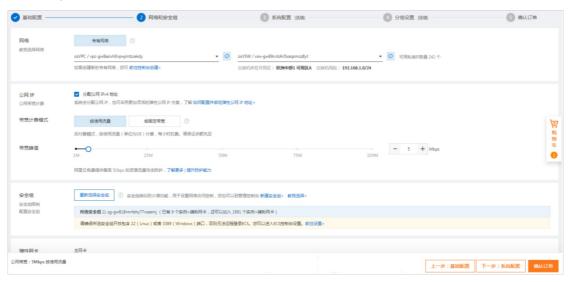
**注意** 此处对操作系统类型无强制要求,可选用任何

32 > 文档版本: 20210527

系统盘

SSD100GiB

#### 配置完成,单击下一步:系统配置。

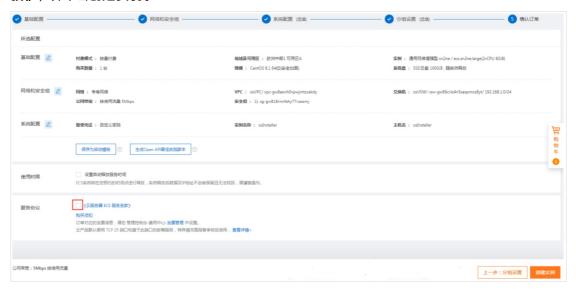


#### v. 在系统配置页面, 配置相关参数。



vi. 单击确认订单。

vii. 在确认订单页面,确认各项参数信息。确认无误,阅读、同意并勾选《云服务器ECS 服务条款》,并单击创建实例。



viii. 创建任务提交成功后,单击管理控制台前往服务器实例列表页面查看详情。



- 3. 创建负载均衡SLB。
  - i. 登录阿里云控制台。

糧

ii. 通过产品与服务导航,定位到负载均衡SLB,单击进入负载均衡SLB控制台。



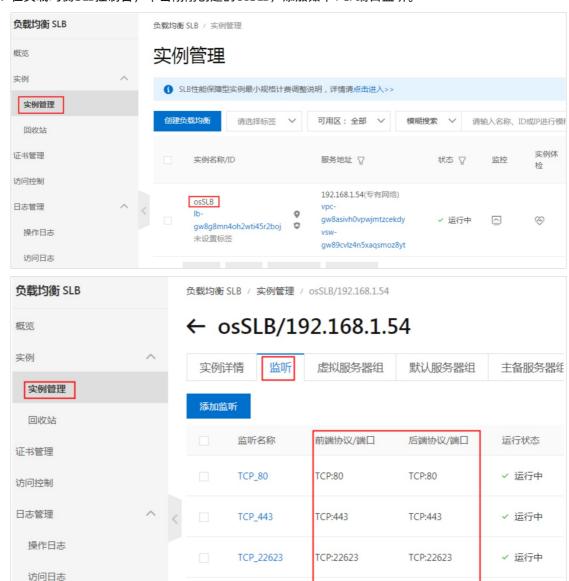
iii. 在左侧导航栏选择实例 > 实例管理,单击创建负载均衡。



#### iv. 在负载均衡SLB(按量购买)页面,配置相关参数,并单击立即购买。

类别	配置项	说明
	付费方式	按量付费
	地域	欧洲与美洲,法兰克福,可用区A
购买配置	实例	■ 规格: 简约型 ■ 实例规格: slb.s1.small
	实例类型	私网
	专有网络	osVPC





v. 在负载均衡SLB控制台,单击刚刚创建的osSLB,添加如下TCP端口监听。

# 红帽OpenShift集群安装准备

健康检查日志

- 1. 在Installation Host上创建SSH私有key并添加到代理。
  - i. 使用Putty等工具,以root账号用户名密码,通过公网IP,登陆Installation Host osInstaller。

TCP\_6443

ii. 运行以下命令:

```
$ cd ~/.ssh
$ ssh-keygen -t rsa -b 4096 -N '' -f id_rsa
$ eval "$(ssh-agent -s)"
```

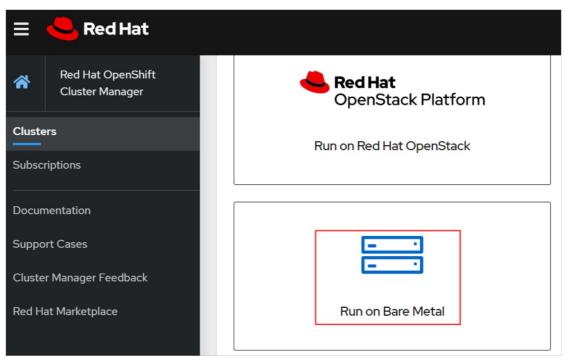
TCP:6443

TCP:6443

✓ 运行中

2. 在Installation Host上获取红帽 OpenShift安装程序。

i. 使用您的红帽账号登录Infrastructure Provider页面,选择Run on Bare Metal。



- ii. 根据您的操作系统(Linux, MaxOS)选择download Installer。本最佳实践中选择Linux。
- iii. 将上一步骤中下载好的安装包上传到InstallationHostosInstaller,并进行解压缩。
  - ☐ 注意 建议您将所有的OpenShift相关安装程序放到统一目录方便管理,本最佳实践中我们都放在/mnt目录中。

#### \$ tar xvf <installation\_program>.tar.gz

- iv. 在Infrastructure Provider页面,选择copy pull secret并保存。
- 3. 在Installation Host上安装cli客户端。
  - i. 在Infrastructure Provider页面,选择Download command-line tools。
  - ii. 将步骤1下载好的安装包上传到InstallationHostosInstaller, 并进行解压缩。
    - ☐ 注意 本最佳实践中,我们将该其解压缩到 /mnt 目录。
  - iii. 将该oc执行文件所在的目录设置成系统环境变量,从而方便之后运行oc命令。您可以通过修改您当前用户的profile文件来达到此效果。
  - iv. 完成上述操作后,您可以在Installation Host上执行如下oc命令来检查安装是否成功:

#### \$.oc <command>

- 4. 在Installation Host上创建安装配置文件install-config.yaml。
  - i. 使用Putty等工具,以root账号用户名密码,通过公网IP,登陆Installation Host osInstaller。

ii. 在/mnt创建install-config.yaml文件,文件内容如下:

```
apiVersion: v1
baseDomain: testos.com1
compute:
-hyperthreading: Enabled
name: worker
replicas: 0
controlPlane:
hyperthreading: Enabled
name: master
replicas: 32
metadata:
name: alicloud3
networking:
clusterNetwork:
-cidr: 10.128.0.0/14
hostPrefix: 23
networkType: OpenShiftSDN
serviceNetwork:
-172.30.0.0/16
platform:
none: {}
fips: false
pullSecret: '{"auths": ...}' 4
sshKey: 'ssh-ed25519 AAAA...'5
```

#### 点击查看安装配置文件详情。

- 5. 在Installation Host上创建Kubernetes manifest以及Ignition文件。
  - i. 使用Putty等工具,以root账号用户名密码,通过公网IP,登陆Installation Host osInstaller。
  - ii. 运行以下命令:

```
$ mkdir <installation_directory>
$ cd /mnt
$ cp install-config.yaml <installation_directory>
$ ./openshift-install create manifests --dir=<installation_directory>
INFO Consuming Install Config from target directory
WARNING Making control-plane schedulable by setting MastersSchedulable to true for Scheduler cl
uster settings
```

- → 注意 本最佳实践中, <installation\_directory> 为/Installation\_Dir。
- iii. 修改/Install\_Dir/manifests/cluster-scheduler-02-config.yml文件中的参数mastersSchedulable为False来防止Pods在控制部分被启动。

iv. 运行以下命令来生成ignit ion配置文件:

./openshift-install create ignition-configs --dir=<installation\_directory>

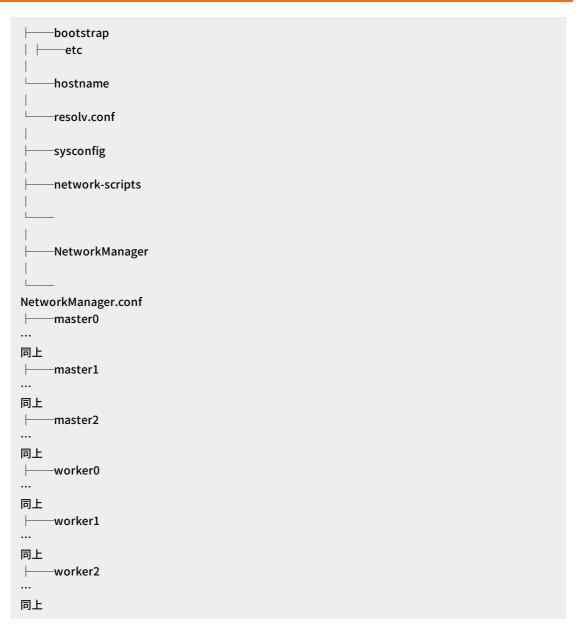
□ 注意 本最佳实践中, <installation\_directory> 为/Installation\_Dir。

您会发现下述文件在/Install\_Dir目录中被生成:

├auth		
kubeadmin-password		
bootstrap.ign		
——master.ign		
——metadata.json		
└──worker.ign		

□ 注意 创建完ignition文件后,必须在24小时内完成OpenShift集群的创建,否则证书会过期失效。

- 6. 在Inst allation Host上创建各节点配置文件目录。
  - i. 使用Putty等工具,以root账号用户名密码,通过公网IP,登陆Installation Host osInstaller。
  - ii. 通过mkdir命令手动创建目录<sim\_directory>, 并新创建各个节点的配置文件放置在相应的目录中。本最佳实践中, 我们使用/simRoot目录, 并创建如下文件体系:



此处,我们以bootstrap节点为例,各文件内容如下。其他节点的文件内容与之一致。

[root@osInstaller etc]# pwd

/simRoot/bootstrap/etc

[root@osInstaller etc]# cat hostname

bootstrap

[root@osInstaller etc]# cat resolv.conf

domain alicloud.testos.com

nameserver 100.100.2.136

nameserver 100.100.2.138

[root@osInstaller etc]# cat NetworkManager/NetworkManager.conf

红帽OpenShift 安装部署最佳实践

[main]

dns=none

[root@osInstaller etc]# cat sysconfig/network-scripts/ifcfg-ens3

BOOTPROTO=dhcp

DEVICE=ens3

PEERDNS=ves

ONBOOT=yes

STARTMODE=auto

TYPE=Ethernet

USERCTL=no

#### 制作coreOS镜像

红帽OpenShift集群的节点只支持coreOS操作系统,目前阿里云上还没有该系统的镜像,请使用如下方法来制作您的阿里云自定义镜像。本方法需要在您的一台物理机上使用KVM虚拟机,用于制作镜像。请确保本物理机能够访问公网。

- 1. 在index of coreOS页面,选择下载*rhcos-4.3.8-x86\_64-installer.x86\_64.iso*。以及rhcos-4.3.8-x86\_64-metal.x86\_64.raw.gz,并将rhcos-4.3.8-x86\_64-metal.x86\_64.raw.gz上传到阿里云OSS bucket ostestfrankfurt,将rhcos-4.3.8-x86\_64-installer.x86\_64.iso文件上传到您本地的物理机上。
- 2. 为了使用KVM虚拟机,您的物理机需要libvirt等相关组件,可以通过运行如下命令在该物理机上进行安装:

\$ yum -y install qemu-img qemu-kvm libvirt

\$ systemctl start libvirtd

3. 在该物理机上运行如下命令来生成需要制作的qcow2格式的镜像。本最佳实践中,我们选定/disk1/openshift/目录来存放和生成所有镜像相关的文件。

\$ cd /disk1/openshift/

\$ qemu-img create -f qcow2 openshift.qcow2 <image\_size>

## ☐ 注意 您可以依据实际情况来配置<image\_size>的大小,本最佳实践中使用20G。

4. 在该物理机的/disk1/openshift/目录中创建openshift.xml, 用于启动虚拟机。请注意qcow2类型及iso文件的路径。

<domain type='kvm' id='2'>

<name>openshift</name>

<memory unit='KiB'>8388608</memory>

<currentMemory unit='KiB'>8388608</currentMemory>

<vcpu placement='static' cpuset='4-31' current='4'>4</vcpu>

<cpu mode='host-passthrough'>

-tanalaguaadkota-111 caraa-141 thraada-111/2

```
<topology sockets= 1 cores= 4 threads= 1/>
</cpu>
<os>
 <type arch='x86_64' machine='pc'>hvm</type>
 <boot dev='hd'/>
 <book dev='cdrom' />
</os>
<features>
 <acpi/>
 <apic/>
 <pae/>
 <hap/>
</features>
<clock offset='localtime'>
 <timer name='hpet' present='no'/>
</clock>
<on_poweroff>destroy</on_poweroff>
<on_reboot>restart</on_reboot>
<on_crash>restart</on_crash>
<devices>
 <emulator>/usr/bin/qemu-kvm</emulator>
 <disk type='file' device='disk'>
  <driver name='qemu' type='qcow2'/>
 <source file='/disk1/openshift/openshift.gcow2'/>
  <target dev='vda' bus='virtio'/>
</disk>
<disk type='file' device='cdrom'>
 <driver name='qemu' type='raw'/>
  <source file='/disk1/openshift/rhcos-4.3.8-x86_64-</pre>
installer.x86_64.iso'/>
 <target dev='hdc' bus='ide'/>
 <readonly/>
 <address type='drive' controller='0' bus='1' target='0' unit='0'/>
</disk>
<interface type='bridge'>
 <source bridge='virbr0'/>
 <target dev='vnet0'/>
 <model type='virtio'/>
</interface>
<input type='tablet' bus='usb'>
 <alias name='input0'/>
</input>
<graphics type='vnc' port='5900' autoport='yes' listen='0.0.0.0' keymap='en-</pre>
us'>
  ten type='address' address='0.0.0.0'/>
 </graphics>
</devices>
</domain>
```

5. 创建shadow.ign文件,内容如下,并将其上传到阿里云OSS bucket ostestfrankfurt。

"passwd": {},
"storage": {},
"systemd": {}

```
{
  "ignition": {
    "config": {
      "append": [{
        "source": "<shadow_static.ignURL>",
        "verification": {}
    }]
    },
    "timeouts": {},
    "version": "2.1.0"
    },
    "networkd": {},
```

- □ 注意 < shadow\_static.ign URL>为您OSSbucket下shadow\_static.ign文件的URL,本最佳实践中为https://ostestfrankfurt.oss- eu-central-1.aliyuncs.com/shadow\_static.ign
- 6. 在该物理机上执行命令 *virsh create openshift.xml*来启动虚拟机。使用vnc连接虚拟机,当出现如下的安装界面时,按Tab键。



#### 输入如下启动参数:

ip=dhcp coreos.inst.install\_dev=sda coreos.inst.image\_url=<raw gz file URL> coreos.inst.ignition\_url=< shadow ign file URL>

□ 注意 在本最佳实践中,<raw gz file URL>为https://ostestfrankfurt.oss-eu-central-1.aliyuncs.com/rhcos-4.3.8-x86\_64-metal.x86\_64.raw.gz,<shadow ign file URL>为https://ostestfrankfurt.oss-eu-central-1.aliyuncs.com/shadow.ign。

请务必确保安装过程中,您的OSS bucket里没有*shadow\_static.ign*文件。安装过程会使用*shadown.ign*初始化系统,因shadow.ign指向的*source*文件不存在,故而安装到最后会卡住,此时执行 virsh destroy openshift ,销毁虚拟机。这时*openshift .qcow2*的制作就完成了。

- 7. 将上述创建好的 openshift.gcow2 文件上传到阿里云OSS bucket ostest frankfurt。
- 8. 导入镜像。
  - i. 登录阿里云控制台。
  - ii. 通过产品与服务导航,定位到**云服务器ECS**,单击进入云服务器ECS控制台。



iii. 在左侧导航栏选择实例与镜像 > 镜像 / 并单击手动导入镜像。



iv. 在镜像导入页面,配置相关参数,并单击确定。

类别	配置项	说明		
	ossobject 地址 镜像名称	您制作好的qcow2镜像在oss URL		
C		□ 注意 本最佳实践中地址为 https://ostestfrankfurt.oss-eu-central- 1.aliyuncs.com/openshift.qcow2		
		openshiftImage		
镜像导入	操作系统	Linux		
	系统架构	X86_64		
	系统平台	RedHat		
	镜像格式	QCOW2		
	许可证类型	自动		



# 创建和配置红帽 OpenShift集群

- 1. 在Installation Host上创建bootstrap定制ignition配置文件。
  - i. 使用Putty等工具,以root账号用户名密码,通过公网IP,登陆Installation Host osInstaller。
  - ii. 从Git Hub下载工具filet ranspiler, 并解压缩到目录/mnt。
  - iii. 从阿里云官网下载ossutil, 并解压缩到目录/mnt。

#### iv. 运行如下命令:

- \$ cd /mnt
- \$ .filetranspile -I <installation\_directory> /bootstrap.ign -f \
- <sim\_directory>/bootstrap -o <installation\_directory>/shadow\_static.ign
- \$./ossutil64 config
- \$./ossutil64 cp <installation\_directory> /shadow\_static.ign oss://ostestfrankfurt
- → 注意 本最佳实践中,<inst allat ion\_direct ory> 为/Inst allat ion\_Dir,<sim\_direct ory> 为/simRoot。
- 2. 创建bootstrap节点。
  - i. 登录阿里云控制台。
  - ii. 通过产品与服务导航,定位到云服务器ECS,单击进入云服务器ECS控制台。



iii. 在左侧导航栏选择实例,地域选择为法兰克福,并单击创建实例。



iv. 在自定义购买模式下,配置相关参数。





#### 在网络和安全组页面,参考下表,配置相关参数。

类别	配置项	说明
网络和安全组	网络	专有网络
	安全组	选择默认安全组

#### 配置完成,单击下一步:系统配置。



#### v. 在系统配置页面, 配置相关参数。

□ 注意 尽管此处选择了密码登陆,但是coreOS强制要求密钥登陆。SSH的private key信息已经保存到步骤的install\_config.yaml 文件中。

✓ 基础配置 ———	✓ 网络和安	2全组 ————————————————————————————————————	3 系統配置 (透填)	4 分组设置 (选填)	5 确认订单
登录凭证	○ 密钥対 ○ 使用機像預设密码 ● 自定义	寄码 创建后设置			
登录名	root				
登录密码		•			
	8 - 30 个字符,必须同时包含三项(大写字母、小写	字母、数字、()"~!@#\$%^&*+= [][];"<>,:?/中部	的特殊符号),其中 Windows 实例不能以斜线号(	/) 为首字符	
确认密码		•			
	请牢记您所设置的密码,如違忘可登录ECS控制台重复	图密码,若不填选 密钥对 / 自定义密码,则默认》	为创建后再设置。		
实例名称	bootstrap	如何自定义有序实例名称③			
	2-128个字符,以大小写字母或中文开头,可包含数针	K. Tr. Tr. Yeller			
描述	輸入網送				
	长度为2-256个字符,不能以http://或https://开头				
主机名 ②	bootstrap	如何自定义有序主机名 ⑦			
1000	Linux 等其他操作系统: 长度为 2-64 个字符,允许任		字母、数字式连字符(-),但不能连续使用点号()或近	至字符(-)。不能以点号()或连字符(-)开头或填尾。	
有序后缀	为实例名称和主机名添加有序后摄 ③				
13.3.3.00	- Same a Table treatment of				

#### vi. 单击确认订单。

vii. 在确认订单页面,确认各项参数信息。确认无误,阅读、同意并勾选《云服务器ECS 服务条款》复选框,并单击创建实例。



viii. 创建任务提交成功后,单击管理控制台前往服务器实例列表页面查看详情。



3. 创建master和worker节点。

在您完成bootstrap机器创建后,请务必为每一个master和worker节点(本最佳实践中共6个,3个master,3个worker)按照顺序重复步骤及的操作来创建定制ignition文件和ECS。

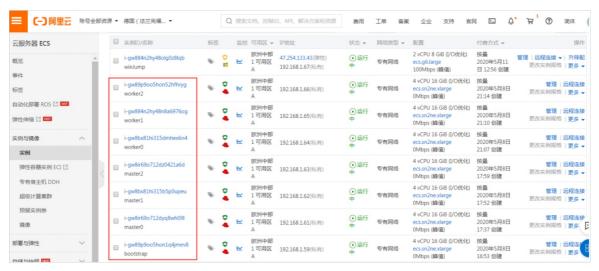
□ 注意 务必要在为一个节点生成shadow\_static.ign文件,上传到OSS,并创建完ECS后再进行下一个节点的重复操作,否则会导致后续集群安装失败。

在Inst allationHost osInst aller上生成定制ignition配置文件的命令分别为:

- \$.filetranspile -I <installation\_directory> /master.ign -f \
- <sim\_directory>/master0-o <installation\_directory>/shadow\_static.ign
- \$.filetranspile -I < installation\_directory > /master.ign -f \
- \$.filetranspile -I < installation\_directory > /master.ign -f \
- <sim\_directory>/master2-o <installation\_directory>/shadow\_static.ign
- \$.filetranspile -I < installation\_directory > /worker.ign -f \
- <sim\_directory>/worker0-o <installation\_directory>/shadow\_static.ign
- \$.filetranspile -I < installation\_directory > /worker.ign -f \
- <sim\_directory>/worker1 -o <installation\_directory>/shadow\_static.ign
- \$.filetranspile -I < installation\_directory > /worker.ign -f \
- <sim\_directory>/worker2 -o <installation\_directory>/shadow\_static.ign

□ 注意 本最佳实践中,<inst allation\_direct ory> 为/Inst allation\_Dir,<sim\_direct ory> 为/simRoot。

当您完成上述所有操作后,您可以在ECS控制台看到1台bootstrap,3台master以及3台workerECS创建成功。



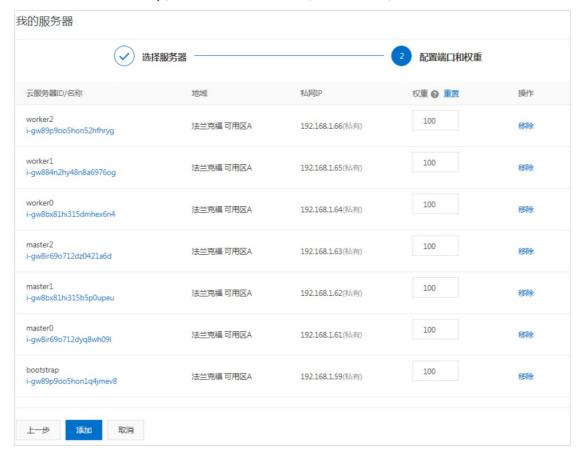
- 4. 添加负载均衡默认服务器组。
  - i. 登录阿里云控制台。
  - ii. 通过产品与服务导航,定位到负载均衡SLB,单击进入负载均衡SLB控制台。

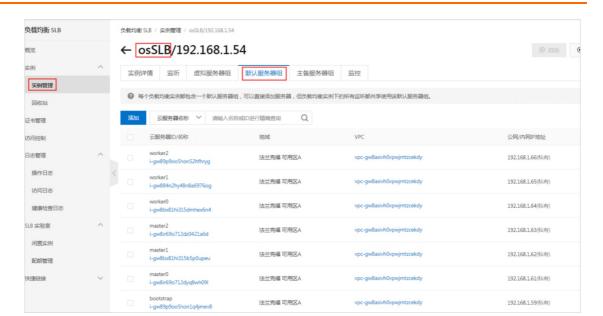


iii. 在左侧导航栏选择实例 > 实例管理,选择此前创建的osSLB实例,并单击添加后端服务器。



iv. 勾选此前创建的bootstrap, master以及worker节点, 单击下一步, 并单击添加。



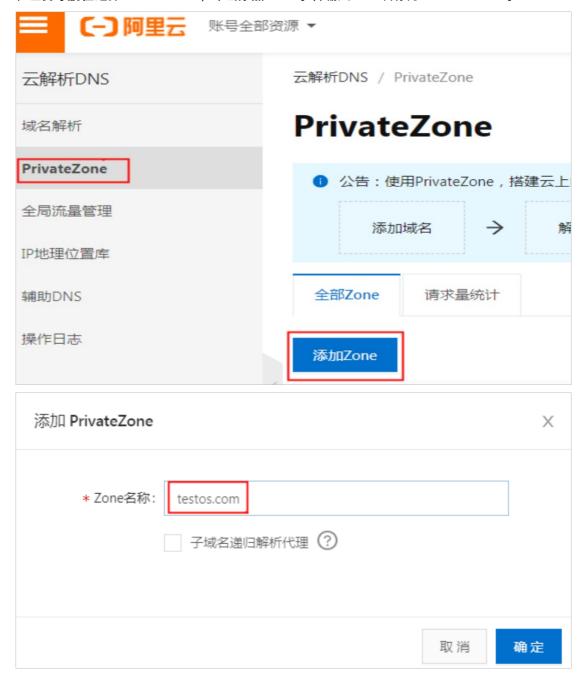


- 5. 配置云解析Private Zone。
  - i. 登录阿里云管理控制台。
  - ii. 通过产品与服务导航,定位到云解析DNS,单击进入云解析DNS管理控制台。

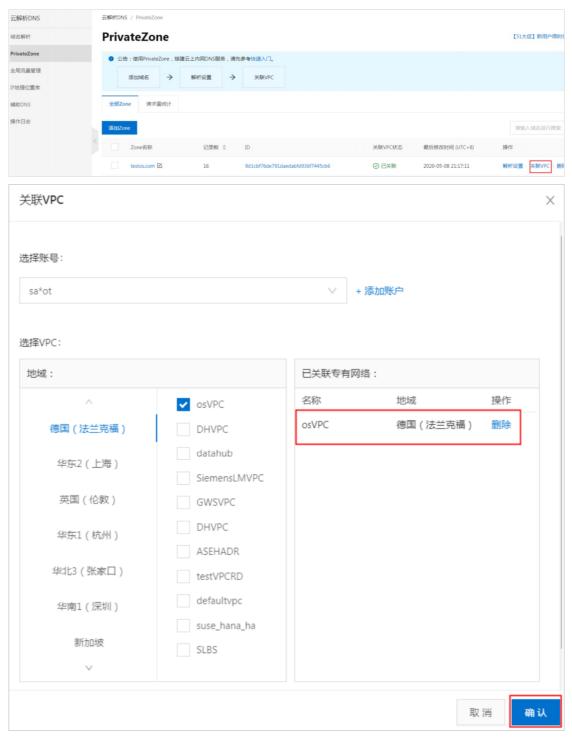


糧

iii. 在左侧导航栏选择PrivateZone,单击添加Zone。并输入Zone名称为: testos.com。



iv. 选择上述创建的Private Zone,并单击**关联VPC**。选择关联osVPC。

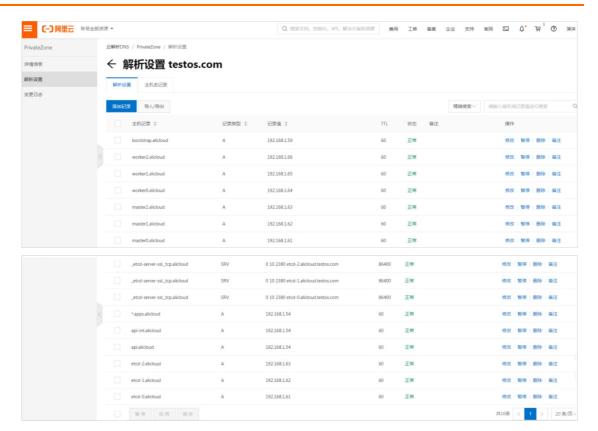


v. 单击创建的testos.com进入设置页面,并单击添加记录。



### vi. 按照如下配置来添加记录。

记录类型	主机记录	记录值	TTL值(秒)
А	bootstrap.alicloud	192.168.1.59	60
А	worker2.alicloud	192.168.1.66	60
А	worker1.alicloud	192.168.1.65	60
А	worker0.alicloud	192.168.1.64	60
А	master0.alicloud	192.168.1.61	60
А	master1.alicloud	192.168.1.62	60
А	master2.alicloud	192.168.1.63	60
А	*.apps.alicloud	192.168.1.54	60
А	api-int.alicloud	192.168.1.54	60
А	api.alicloud	192.168.1.54	60
А	etcd-2.alicloud	192.168.1.63	60
А	etcd-1.alicloud	192.168.1.62	60
А	et cd-0.alicloud	192.168.1.61	60
SRV	_etcd-server- ssltcp.alicloud	0 10 2380 etcd- 2.alicloud.testos.com	86400
SRV	_etcd-server- ssltcp.alicloud	0 10 2380 etcd- 1.alicloud.testos.com	86400
SRV	_etcd-server- ssltcp.alicloud	0 10 2380 etcd- 0.alicloud.testos.com	86400



- 6. 登陆集群检查安装结果。
  - i. 使用Putty等工具,以root账号用户名密码,通过公网IP,登陆Installation Host osInstaller。
  - ii. 运行以下命令来检查bootstrap进展:
    - \$ ./openshift-install --dir=<installation\_directory> wait-for\bootstrap-complet e --log-level=info
    - INFO Waiting up to 30m0s for the Kubernetes API at https://api.alicloud.testos.com...

INFO API v1.16.2 up

INFO Waiting up to 30m0s for bootstrapping to complete...

INFO It is now safe to remove the bootstrap resources

- ② 说明 本最佳实践中, <inst allation\_directory> 为/Inst allation\_Dir。
- iii. bootstrap过程结束后,您可以从负载均衡SLB中移除bootstrap。
- iv. bootstrap过程结束后,您可以通过设置KUBECONFIG环境变量来登陆红帽OpenShift集群。 Kubeconfig文件是在红帽OpenShift安装过程中创建的。用于通过CLI来登陆集群和API server。

\$ export KUBECONFIG=<installation\_directory>/auth/kubeconfig

v. 运行以下命令来检查oc命令可以成功执行:

\$ oc whoami system:admin

vi. 运行以下命令来确认集群识别出所有节点。

```
$ oc get nodes

NAME STATUS ROLES AGE VERSION

master0 Ready master 4d v1.16.2

master1 Ready master 4d v1.16.2

master2 Ready master 4d v1.16.2

worker0 Ready worker 4d v1.16.2

worker1 Ready worker 4d v1.16.2

worker2 Ready worker 4d v1.16.2
```

vii. 运行以下命令来检查集群的所有组件可用:

```
$ watch -n5 oc get clusteroperators
```

- 7. Image Registry配置。最新的红帽OpenShiftImage Registry Operator默认设置为Removed,以保证在所有平台上安装成功。故而在集群安装完成后,需要修改Image Registry配置。
  - i. 登录阿里云控制台。

ii. 通过产品与服务导航,定位到云服务器ECS,单击进入云服务器ECS控制台。



iii. 在左侧导航栏选择存储与快照 > 云盘,单击创建云盘。



耄

iv. 在云盘购买页面,配置相关参数,并单击**购买**。

类别	配置项	说明
云盘	是否挂载	挂在到ECS实例
	地域	法兰克福osInstaller
	云盘付费方式	按量付费
	存储	SSD云盘200GiB



- v. 使用Putty等工具,以root账号用户名密码,通过公网IP,登陆Installation Host osInstaller。
- vi. 执行以下命令:

```
署
```

```
$ fdisk /dev/vdb
$ mkfs.xfs /dev/vdb1
$ mkdir <storage_directory>
$ echo /dev/vdb1 <storage_directory> xfs defaults 0 0 >> /etc/fstab
$ echo /dev/vdb1 /osStorage xfs defaults 0 0 >> /etc/exports
$ systemctl start nfs-server.service
$ systemctl start rpcbind
$ mkdir <storage_directory>/alicloud
$ chmod 777 <storage_directory>/alicloud
$ exportfs -rv
$ systemctl reload nfs-server.service
$ oc create -f -<<EOF
apiVersion: v1
kind: PersistentVolume
metadata:
name: registry
spec:
capacity:
 storage: 100Gi
 accessModes:
 -ReadWriteMany
 path: <storage_directory>/alicloud
 server: <IP address of Installation Host>
persistentVolumeReclaimPolicy: Retain
EOF
$ oc get pv
NAME CAPACITY ACCESS MODES RECLAIM POLICY STATUS CLAIM
  STORAGECLASS REASON AGE
registry 100Gi RWX
                          Retain
                                    Bound openshift-image-re
gistry/image-registry-storage
```

注意 本最佳实践中,<storage\_directory> 为/osStorage. 如果您的系统里没有安装nfs-server请使用yum in nfs-util\*命令来安装。<IP address of Installation Host> 为192.168.1.53。

vii. 运行以下命令来修改registry配置,请确保claim值为空。

```
$ oc edit configs.imageregistry.operator.openshift.io
storage:
pvc:
claim:
```

viii. 运行以下命令来检查ImageRegistry配置:

- 8. 完成红帽OpenShift集群的安装和配置。
  - i. 使用Putty等工具,以root账号用户名密码,通过公网IP,登陆Installation Host osInstaller。

#### ii. 运行以下命令:

\$./openshift-install --dir=<installation\_directory> wait-for install-complete

INFO Waiting up to 30m0s for the cluster at https://api.alicloud.testos.com:6443 to initialize...

INFO Waiting up to 10m0s for the openshift-console route to be created...

**INFOInstall complete!** 

INFO To access the cluster as the system:admin user when using 'oc', run 'export KUBECONFIG=/Ins tall\_Dir/auth/kubeconfig'

INFO Access the OpenShift web-console here: https://console-openshift-console.apps.alicloud.tes tos.com

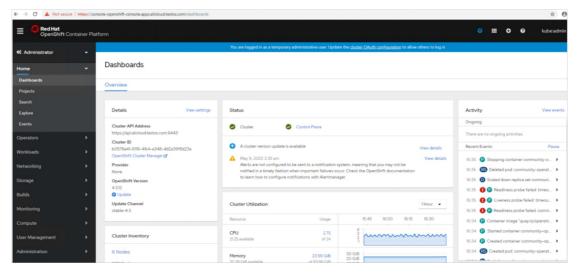
INFO Login to the console with user: kubeadmin,

☐ 注意 请妥善保存您的OpenShift集群web console地址及用户名密码,我们在后续章节中会用到。

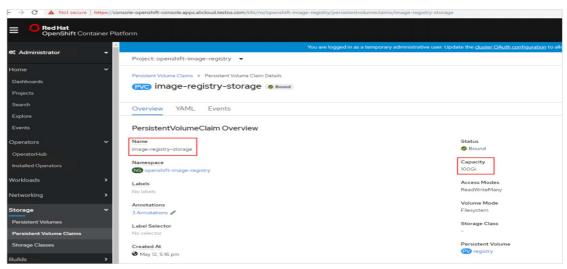
## 校验红帽 OpenShift集群安装结果

红帽OpenShift安装完成后,我们得到了其web console的地址,在本章节中我们将在其web console上进行安装的校验以及应用的创建。您需要在Installation Host上安装网页浏览器应用,或者在本vpcosVPC内创建一个windows跳转机。

- 1. 在Installation Host上检查集群运行状态。
  - i. 使用Putty等工具,以root账号用户名密码,通过公网IP,登陆Installation Host osInstaller。
  - ii. 打开网页并输入此前得到的web console地址https://console-openshift-console.apps.alicloud.testos.com。
  - iii. 使用此前得到的用户名密码登陆。登录成功后,您将看到如下集群信息:



iv. 您可以在administrator视图查看集群的各项属性,我们以此前创建的storage为例:

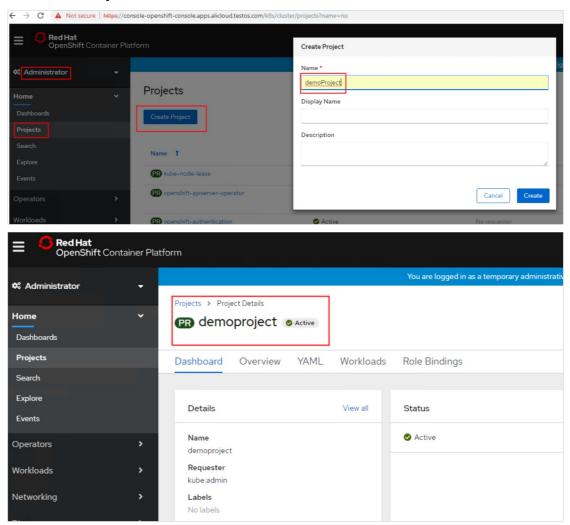


### 2. 创建应用。

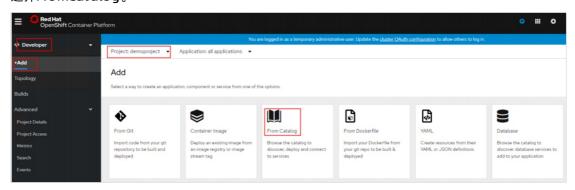
- i. 使用Putty等工具,以root账号用户名密码,通过公网IP,登陆Installation Host osInstaller。
- ii. 打开网页并输入此前得到的web console地址https://console-openshift-console.apps.alicloud.testos.com。
- iii. 使用此前得到的用户名密码登陆。

署

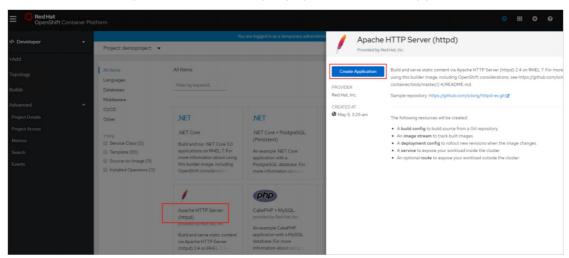
iv. 在administrator视图,在左侧**导航栏**选择**home > project**,并单击创建**Create Project**。输入Name为demoProject。



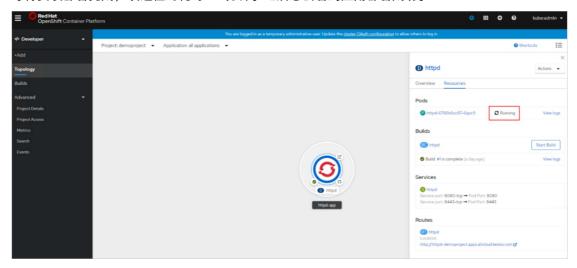
v. 切换视图为Developer, 在左侧**导航栏**选择**+add**, 切换project为我们刚刚创建的demoproject, 选择**FromCatalog**。



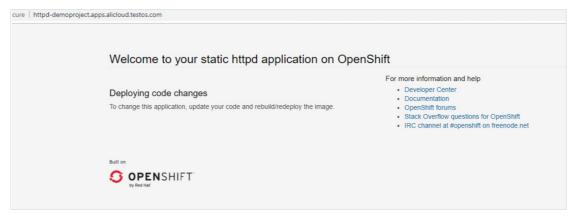
vi. 在应用列表中,选择Apache HTTP Server (httpd),并单击Create Application。



vii. 等待安装部署完成,该过程约耗时1~3分钟。之后您会看到应用部署成功。



viii. 打开该应用的网址。



# 名词解释

● 云服务器

云服务器ECS(Elastic Compute Service)是一种简单高效、处理能力可弹性伸缩的计算服务。ECS帮助您构建更稳定、安全的应用,提升运维效率,降低IT成本,使您更专注于核心业务创新。

### ● 专有网络

专有网络VPC(Virtual Private Cloud)是用户基于阿里云创建的自定义私有网络,不同的专有网络之间二层逻辑隔离,用户可以在自己创建的专有网络内创建和管理云产品实例,比如ECS、负载均衡、RDS等。

#### ● 负载均衡

负载均衡SLB是多台云服务器进行流量分发的负载均衡服务,可以通过流量分发扩展应用系统对外的服务能力,通过消除单点故障提升应用系统的可用性。

#### ● 云解析Private Zone

云解析PrivateZone,是基于阿里云专有网络VPC (Virtual Private Cloud)环境的私有域名解析和管理服务。可以在自定义的一个或多个专有网络中快速构建DNS系统,实现私有域名映射到IP资源地址。

#### ● 对象存储OSS

海量、安全、低成本、高可靠的云RESTful API可以在互联网任何位置存储和访问,容量和处理能力弹性扩展,多种存储类型供选择全面优化存储成本。

#### • 红帽OpenShift

红帽®OpenShift®是一个企业就绪型Kubernetes容器平台,可以实现全堆栈自动化运维,以管理混合云和多云部署。红帽OpenShift已进行过优化,可以提高开发人员的生产力并推动创新。

## 更多最佳实践

点击查看更多阿里云最佳实践。