解决方案实践

华为云芯片 EDA 云服务解决方案实践

文档版本 1.0

发布日期 2023-12-07

华为技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

安全声明

漏洞处理流程

华为公司对产品漏洞管理的规定以“漏洞处理流程”为准，该流程的详细内容请参见如下网址：
https://www.huawei.com/cn/psirt/vul-response-process
如企业客户须获取漏洞信息，请参见如下网址：
https://securitybulletin.huawei.com/enterprise/cn/security-advisory

目 录

1 方案概述 1
2 资源和成本规划 4
3 实施步骤 7
3.1 搭建北鲲云平台运行环境 7
3.1.1 配置云上网络环境 7
3.1.2 购买云资源 12
3.1.3 部署北鲲云平台服务 15
3.2 配置 LDAP 服务 17
3.2.1 部署 ldap 服务端 17
3.2.2 配置 ldap 主从 17
3.2.3 配置 ldap 客户端 18
4 修订记录 19

1 方案概述

应用场景

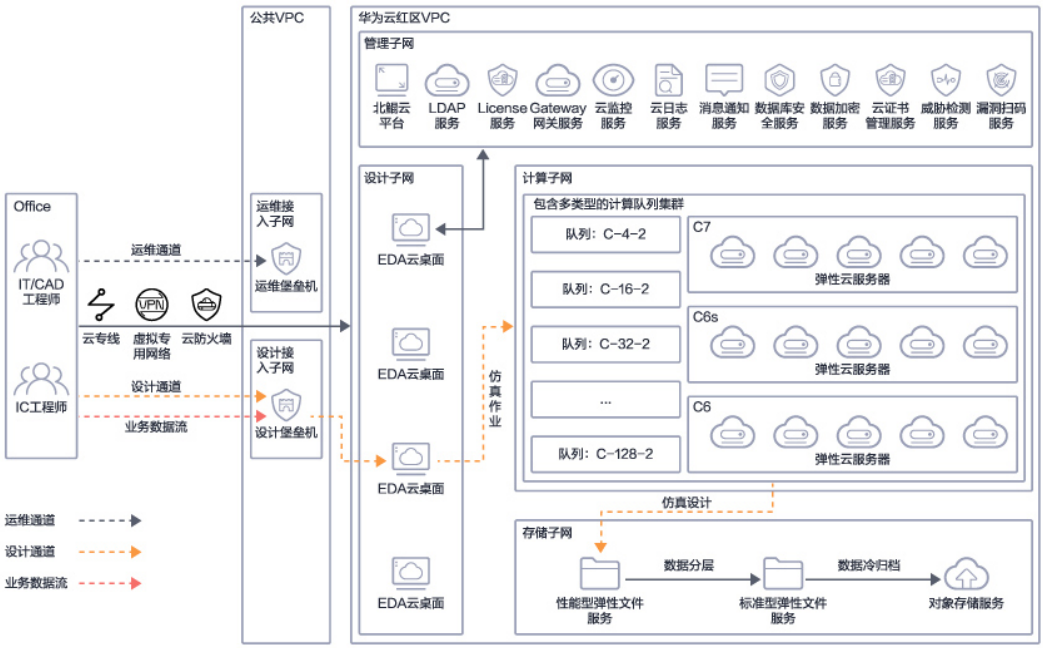
- 芯片设计企业弹性上云：整合本地资源和华为云资源，构建混合云集群，弹性按需上云，解决业务高峰期算力存力不足的问题；
- 芯片设计企业轻资产运营：企业IT全面上云，云上构建设计仿真一体化环境，通过多维度多层次的安全服务，在弹性使用云上算力资源的同时，保证芯片设计各阶段的数据安全；
- 多地域协同办公的芯片设计企业：结合专线、VPN等技术搭建国内外多团队协同多地域高可用的EDA设计仿真云平台。

业务痛点及挑战

- 芯片研发全流程对于IT资源的诉求是波动，资源高峰期，本地静态资源无法满足动态需求，资源低谷期，本地资源只能闲置，整体IT资源利用率低，影响项目进度；
- 芯片研发随着工艺节点发展，对于IT资源的诉求是翻倍，企业IT部门无法快速做到无限制扩机房、扩容操作。
- 公有云资源丰富多样，一旦云上资源调度策略不合适，会导致云山仿真任务挂住，无法发挥云上弹性按需的效果，还影响仿真工作稳定性；
- 以传统方式将芯片研发环境迁移云上的解决方案严重改变了芯片设计工程师线下操作方式，增加了学习成本，降低了工作效率；
- 多地域的研发中心协同能力不足，计算资源调度差；
- 作业、资源监控不直观，作业状态通知不全面、不及时，导致作业运行失败频发，资源有效利用率不高。

方案架构

图 1-1 华为云芯片设计仿真一体化解决方案架构



1. 运维人员和设计人员双通道接入，保护数据网络的互相隔离访问，子网隔离，防护项目数据安全；
2. 静态云上工作站，完善的IC设计仿真环境，仿真作业弹性调度云上集群；

方案优势

- 安全高效的云上EDA设计桌面：设立多个安全分区，使用 ACL和安全组访问控制技术保障核心数据的安全；
- 不改变原有操作习惯：云上和线下保持一致的EDA软件环境，混合云模式支持本地设计云上仿真，结合调度系统命令的转译适配，为芯片设计工程师提供无感化上云的操作体验；
- 无需运维 资源最新：管理无压力：无需运维管理线下计算机，线上的硬件资源持续更新，您可以一直使用到最新的配置；
- 联合运营 服务稳定：服务全方位：华为云与北鲲云联合运营，市场合作深度绑定，北鲲云为客户解决云上资源调度、软件工艺库安装、案例脚本调试全方位服务，为客户减负，服务稳定有保障；
- 按需使用 弹性计费：成本更可控：云上计算机资源闲置关闭不计费，按照工作有效时间弹性计费，成本更加可控。

约束与限制

管理平台部署限制

- 硬件限制：北鲲云管理平台运行环境推荐配置CPU4核、内存16G、系统盘200GB，最少需要三个节点做高可用部署。

- 软件系统限制：北鲲云管理平台运行在CentOS7下，其他Linux发行版本可能出现兼容问题。

2 资源和成本规划

基于北鲲云平台+华为云搭建芯片设计仿真一体化环境

表 2-1 资源和成本规划

云资源	规格	数量	每月费用（元）
VPC	公共VPC 红区VPC	2	00.00
子网	设计堡垒机子网 运维堡垒机子网 设计子网 计算子网 存储子网 公共子网	6	00.00
安全组	设计安全组 计算安全组 存储安全组 公共安全组	4	00.00
对等连接	打通公共VPC和红区VPC	1	00.00
云服务器(包月)	北鲲云平台运行服务器 4核16G(高IO 200G存储)	3	1,709
云服务器(按需)	包括设计桌面，如果干台计算节点 配置不固定	弹性	弹性
LICENSE服务器	LDAP服务 主从 EDA软件LICENSE服务 主从 2核4G(高IO 200G存储)	2	439

云资源	规格	数量	每月费用（元）
主机安全服务(包月)	企业版 10台 以实际数量为准	弹性	900
云审计服务	基础功能免费 可查看7天内数据	1	00.00
云日志服务	500M以内免费	1	00.00
云堡垒机(包月)	华为云堡垒机标准版100资产	1	3,780
弹性文件服(包月)	SFS turbo 标准型增强版10TB，增加的容量按需购买	1	4,096
文件系统备份	SFS Turbo备份存储库 20TB	1	7168
VPN网关	IPsec 10M	1	775
北鲲云平台 LICENSE	以商务合同为准，以调用核数进行收费	1	弹性
正式阶段：	该价格仅为参考，实际需要以控制台显示为准, 且仅包含固定费用，不包含弹性资源费用	合计	**81931.4**

表 2-2 网络规划

云资源	名称	网段	说明
VPC	公共VPC	172.16.0.0/20	和本地建立VPN连接
	芯片研发VPC	172.17.0.0/20	EDA黑盒环境
子网	设计堡垒机子网	172.16.0.0/24	/
	运维堡垒机子网	172.16.1.0/24	/
	设计子网	172.17.0.0/24	VDI设计桌面
	计算子网	172.17.0.1/24	弹性计算资源
	存储子网	172.17.0.2/24	SFS存储
	公共子网	172.17.0.3/24	北鲲云平台服务器
安全组	设计安全组	/	通过堡垒机子网进行跳转
	计算安全组	/	仅运维堡垒机子网可跳转
	存储安全组	/	仅运维堡垒机子网可跳转
	公共安全组	/	仅运维堡垒机子网可跳转

云资源	名称	网段	说明
对等连接	公共VPC-红区VPC	/	/
路由表	rtb-公共	/	设计堡垒机子网路由至设计子网 运维堡垒机子网路由至红区所有子网
	rtb-红区	/	设计子网路由至设计堡垒机子网
网络ACL	设计子网ACL	/	仅可访问红区内部子网和 设计堡垒机子网
	设计堡垒机子网ACL	/	可访问红区设计子网

表 2-3 数据规划

数据类型	目录	读取频率	备份频率
用户数据	/home	较高速IOPS读取	备份频率高
项目数据	/data/project	较高速IOPS读取	备份频率高
设计工具	/opt/modulefiles	普通高速读取	备份频率低
IP和工艺库数据	/public/foundry	普通高速读取	备份频率低
仿真数据	/data/project/user/sim	较高速IOPS读写	较少备份或不备份
推荐与本地目录保持一致减少调试成本			

3 实施步骤

3.1 搭建北鲲云平台运行环境
3.2 配置LDAP服务

3.1 搭建北鲲云平台运行环境

3.1.1 配置云上网络环境

说明

以下操作均在虚拟私有云VPC控制台完成

1. 创建VPC

   分别创建架构中的公共VPC和红区VPC，创建VPC时注意网段划分。

图 3-1 创建 VPC1

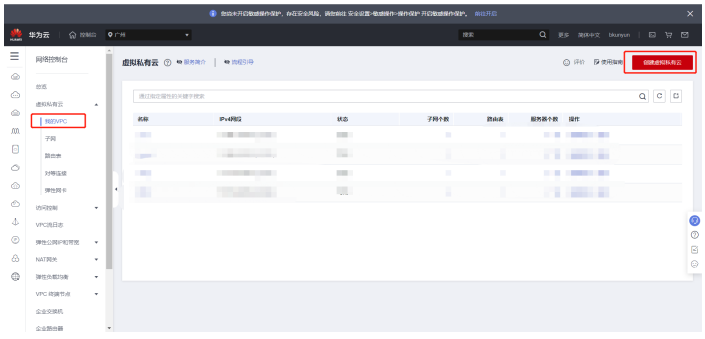
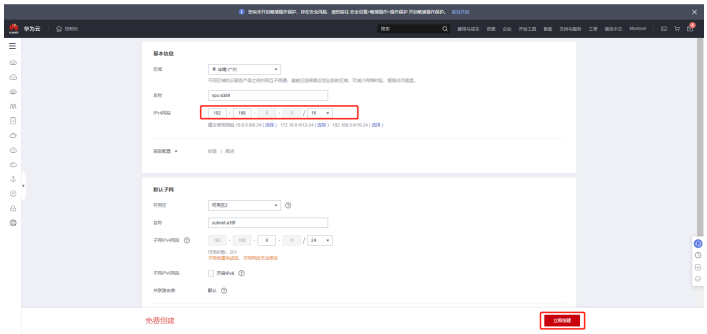


图 3-2 创建 VPC2



2. 创建子网

在公共VPC和红区VPC中分别创建以下子网，操作演示见截图。

表 3-1 创建子网

云资源	名称	网段	说明
子网	设计堡垒机子网	172.16.0.0/24	跳转
	运维堡垒机子网	172.16.1.0/24	运维
	设计子网	172.17.0.0/24	VDI设计桌面
	计算子网	172.17.0.1/24	弹性计算资源
	存储子网	172.17.0.2/24	SFS存储
	公共子网	172.17.0.3/24	北鲲云平台服务器

图 3-3 创建子网 1

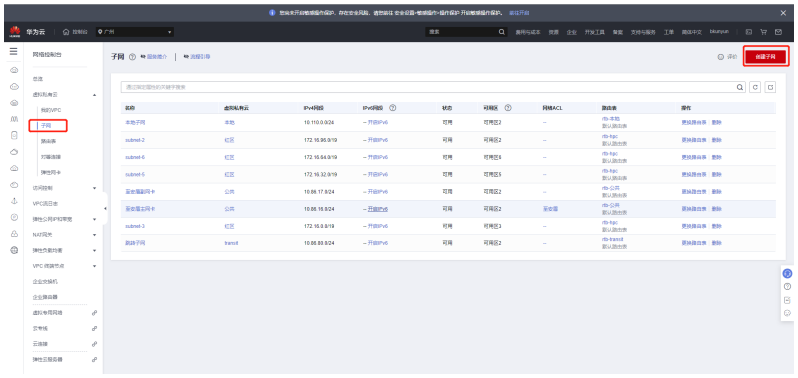
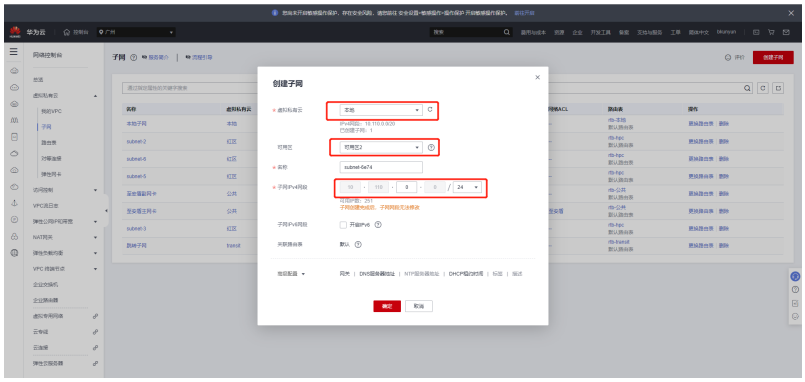


图 3-4 创建子网 2



3. 创建对等连接

   打通红区VPC和公共VPC的对等连接，使得公共VPC可以跳转至红区VPC。

图 3-5 创建对等连接 1

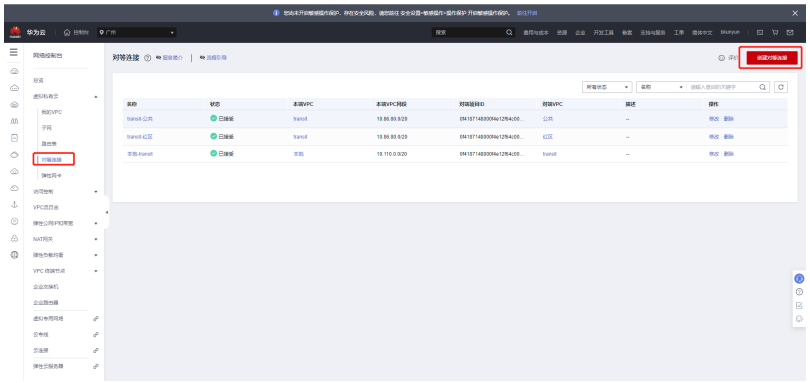
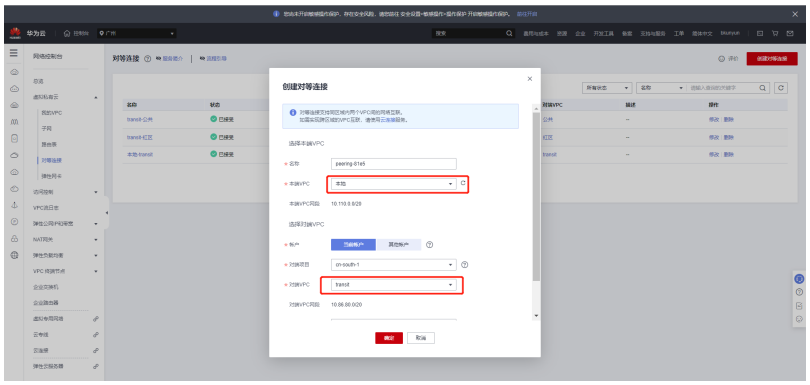


图 3-6 创建对等连接 2



4. 配置网络ACL规则

   配置红区VPC和公共VPC内部子网之间的网络控制策略，公共VPC的运维接入子网和设计接入子网是唯一开放office访问的网络。

图 3-7 配置网络 ACL 规则 1

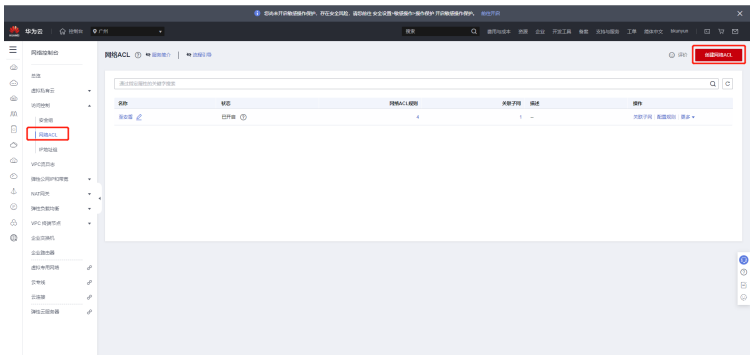


图 3-8 配置网络 ACL 规则 2

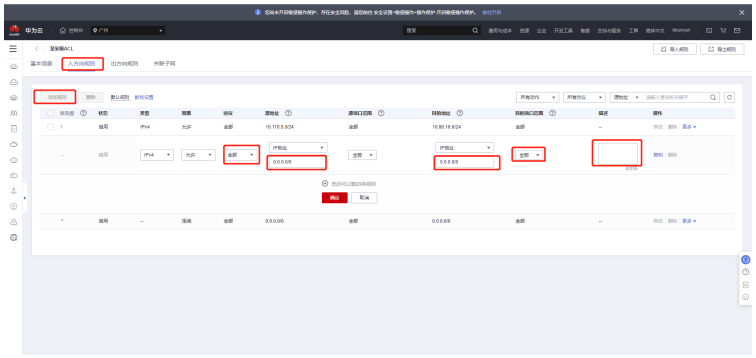


图 3-9 配置网络 ACL 规则 3

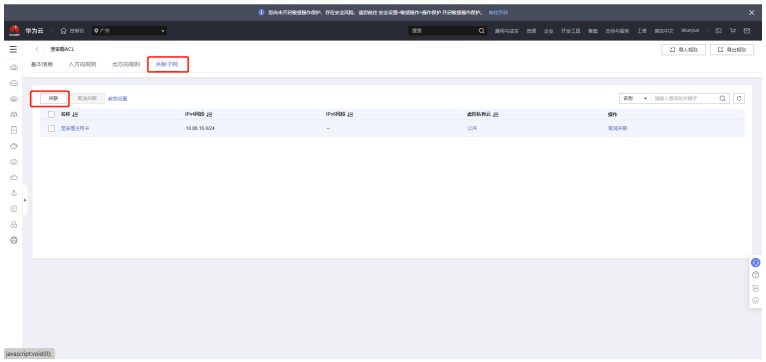
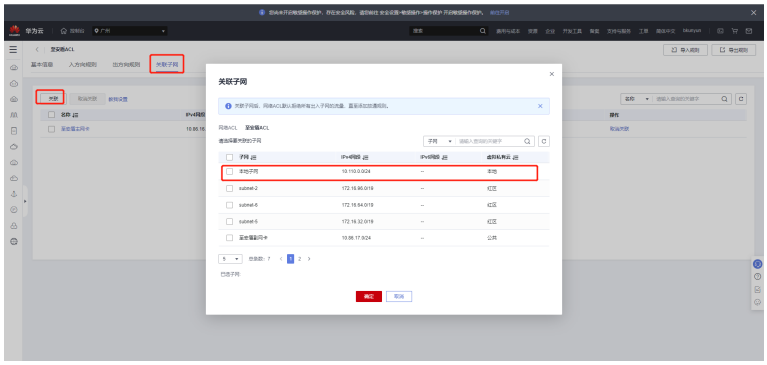


图 3-10 配置网络 ACL 规则 4



5. 配置路由表

路由表由一系列路由规则组成，用于控制虚拟私有云内子网的出流量走向。创建虚拟私有云时，系统会自动为生成一个默认路由表，同时可以为子网自定义路由表。

图 3-11 配置路由表 1

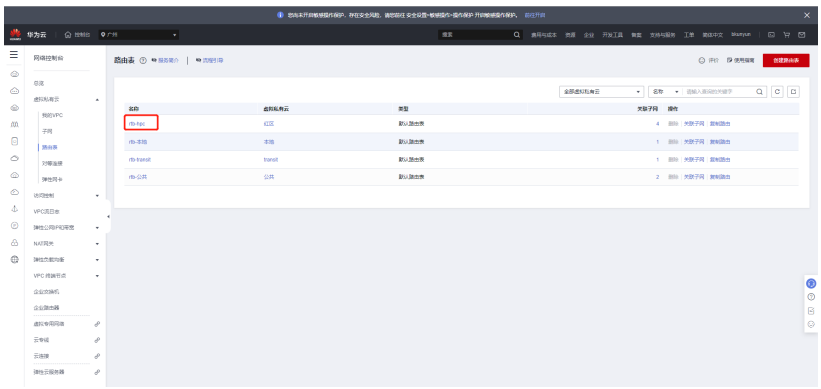
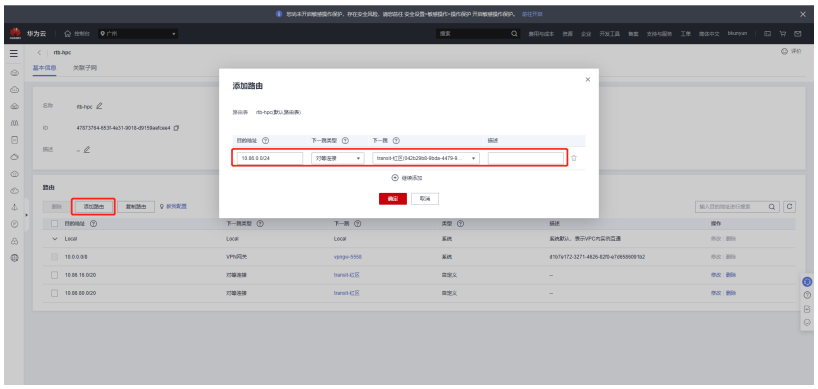


图 3-12 配置路由表 2



6. 配置安全组规则

通过安全组规则对弹性云服务器进行防护。

图 3-13 配置安全组规则 1

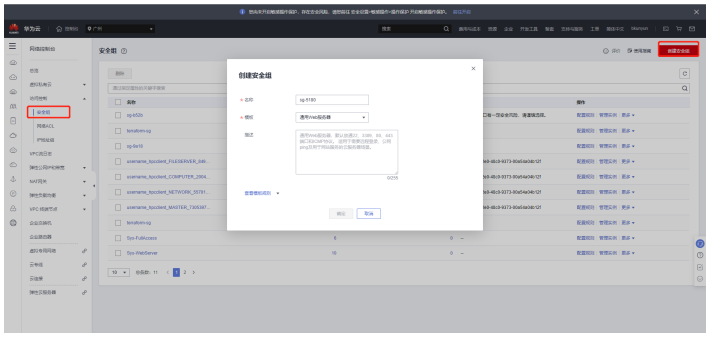
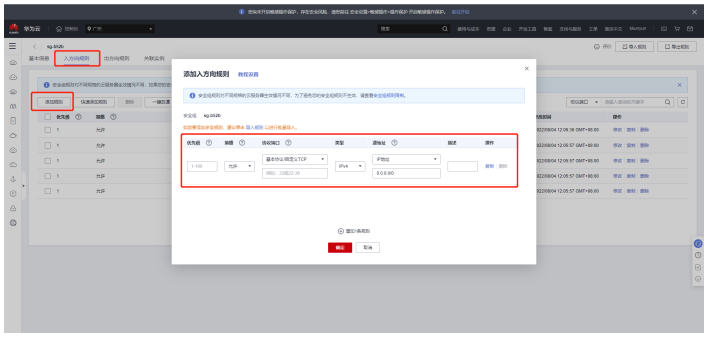


图 3-14 配置安全组规则 2



3.1.2 购买云资源

1. 购买云服务器
   用于部署北鲲云管理平台和堡垒机，配置见上面章节。

图 3-15 购买云服务器 1

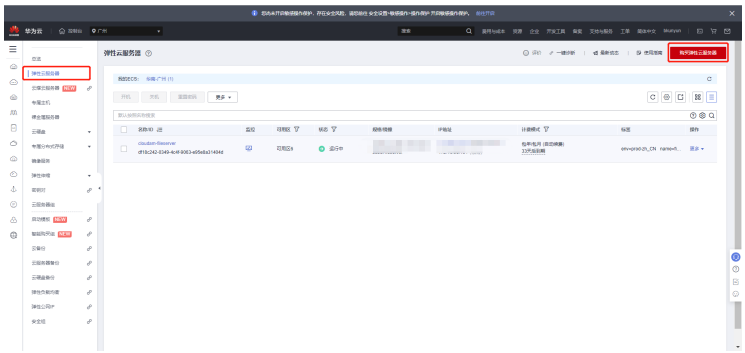


图 3-16 购买云服务器 2

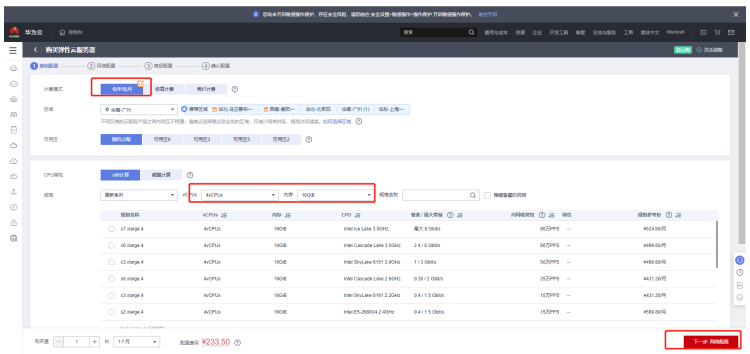


图 3-17 购买云服务器 3

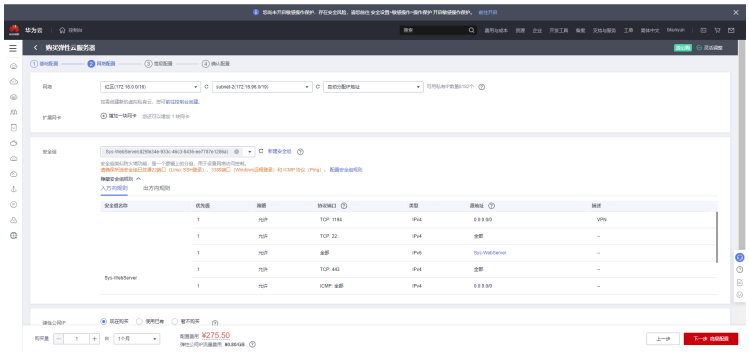
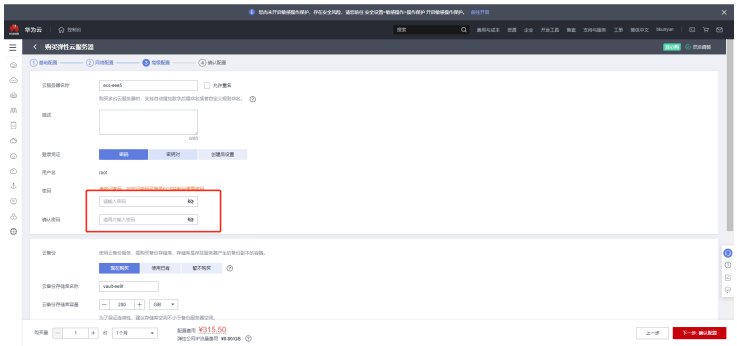


图 3-18 购买云服务器 4



2. 购买SFS Turbo存储

   用于搭建文件系统，服务于芯片设计环节的仿真业务、软件安装、工艺库、IP库等数据存储。

图 3-19 购买 SFS Turbo 存储 1

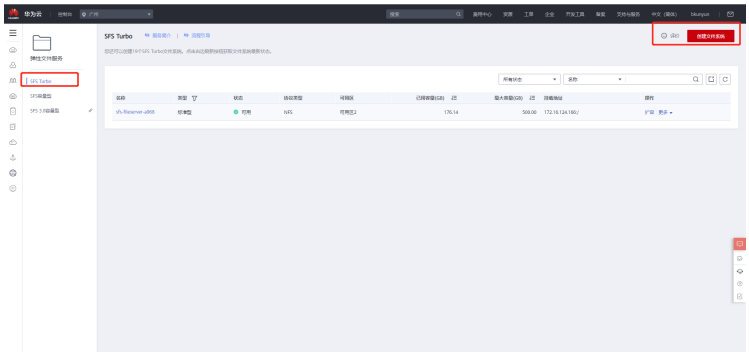
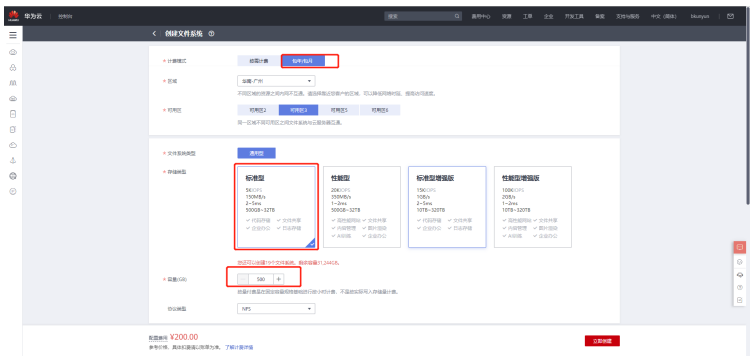


图 3-20 购买 SFS Turbo 存储 2



3. 购买云堡垒机

   云堡垒机提供云计算安全管控的系统和组件，包含部门、用户、资源、策略、运维、审计等功能模块，集单点登录、统一资产管理、多终端访问协议、文件传输、会话协同等功能于一体。通过统一运维登录入口，基于协议正向代理技术和远程访问隔离技术，实现对服务器、云主机、数据库、应用系统等云上资源的集中管理和运维审计。

图 3-21 购买云堡垒机 1

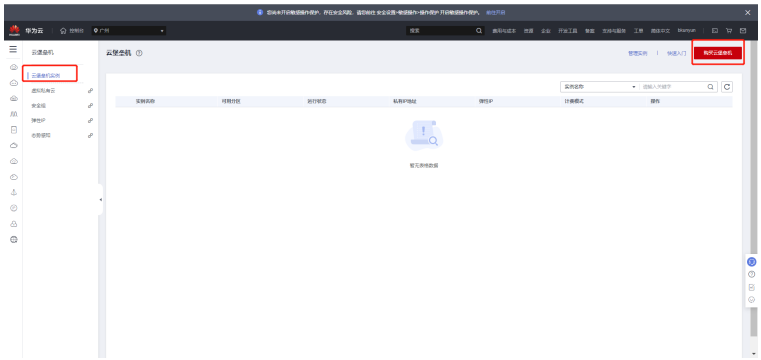
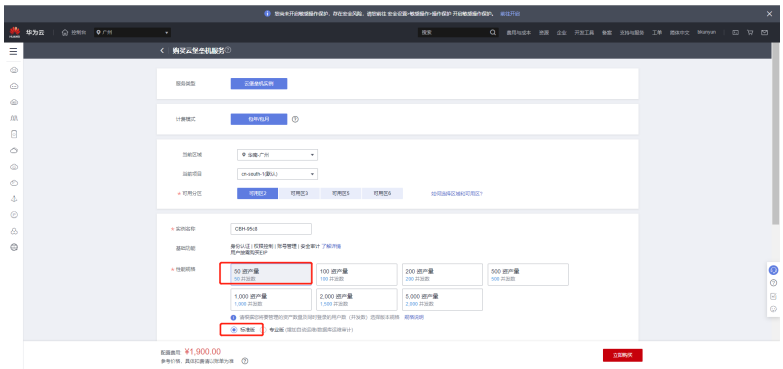


图 3-22 购买云堡垒机 2

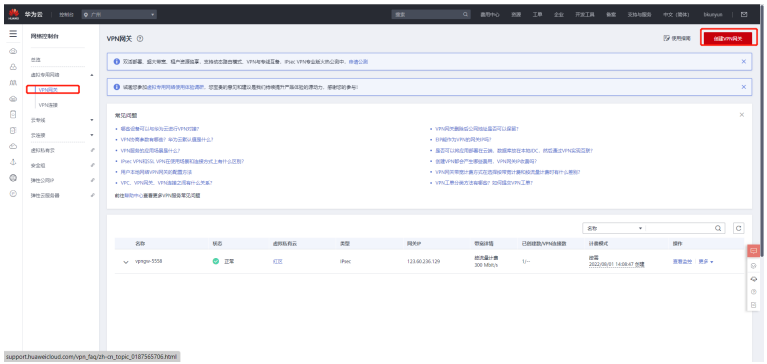


4. 购买VPN网关

   VPN网关是虚拟私有云中建立的出口网关设备，通过VPN网关可建立虚拟私有云和企业数据中心或其它区域VPC之间的安全可靠的加密通信。

   VPN网关需要与用户本地数据中心的对端网关配合使用，一个本地数据中心绑定一个对端网关，一个虚拟私有云绑定一个VPN网关。VPN支持点到点或点到多点连接，所以，VPN网关与对端网关为一对一或一对多的关系。

图 3-23 购买 VPN 网关



3.1.3 部署北鲲云平台服务

步骤1 配置北鲲云平台部署服务器

1. 配置节点域名解析 3台服务器都需要

```
vi /etc/hosts
172.17.3.11 deploy
172.17.3.12 accountslave
172.17.3.13 authslave
```

2. 配置部署服务器间免密登录

```
ssh-keygen -f ~/.ssh/id_rsa -t rsa -N ''
cat /root/.ssh/id_rsa.pub >> /root/.ssh/authorized_keys
cd ~/.ssh
ssh-copy-id accountslave
scp ~/.ssh/id_rsa accountslave:/root/.ssh
```

3. 关闭防火墙和selinux

```
#关闭防火墙 需要注意要在安装docker之前就关闭好 否则关闭后要重启docker
systemctl disable firewalld --now
#禁用selinux  需要重启才能生效
sed -i "s/SELINUX=enforcing/SELINUX=disabled/g" /etc/sysconfig/selinux
sed -i "s/SELINUX=enforcing/SELINUX=disabled/g" /etc/selinux/config
```

4. 安装必备软件例如docker

```
yum install -y docker-ce-19.03.9-3.el7.x86_64 docker-ce-cli-19.03.9-3.el7.x86_64
containerd.io-1.2.6-3.3.el7.x86_64
systemctl enable docker --now
curl -o /usr/local/bin/docker-compose -L https://get.daocloud.io/docker/compose/releases/download/
1.27.4/docker-compose-`uname -s`-`uname -m`
chmod +x /usr/local/bin/docker-compose
```

5. 部署节点安装gnome桌面和VNC服务方便堡垒机可视化连接

```
yum install -y tigervnc-server xorg-x11-fonts-Type1 xrdp
yum groupinstall -y "GNOME Desktop" "Graphical Administration Tools"
yum install -y mesa-libGL
yum install -y fwupdate
systemctl enable gdm --now
```

步骤2 创建docker swarm集群

1. 初始化docker swarm集群

```
deploy节点执行 初始化swarm集群 deploy
docker swarm init
```

2. 添加节点到docker swarm集群并建立必须目录

以下accountslave节点执行

```
docker swarm join --token
SWMTKN-1-1rmkhkehf6ciu45803kg2ixu48jvbl7rzbdsbyqe3lc4dqxd6d-14d7kfs2ei4lzit4h3hgczuu3
172.17.3.11:2377
mkdir -p /data/db/account /data/logs/nginx /data/zk/zoo/data /data/zk/zoo/datalog /data/logs/zoo /
data/logs/kafka
```

```
chmod -R 777 /data/logs/nginx
以下authslave节点执行
docker swarm join --token
SWMTKN-1-1rmkhkehf6ciu45803kg2ixu48jvbl7rzbdsbyqe3lc4dqxd6d-14d7kfs2ei4lzit4h3hgczuu3
172.17.3.11:2377
mkdir -p /data/db/auth /data/logs/nginx /data/logs/openresty /etc/openldap/cacerts
chmod -R 777 /data/logs/nginx
```

3. 给docker node打上标签

   在主节点打标签

```
docker node ls
docker node update --label-add master=true deploy
docker node update --label-add account=true accountslave
docker node update --label-add auth=true authslave
```

步骤3 搭建本地docker镜像仓库

1. 创建本地仓库目录

```
部署本地docker registry 并上传cloudam镜像
cd /etc/cloudam
docker pull docker.io/library/registry:latest
docker tag docker.io/library/registry:latest docker-registry
```

2. 使用yml文件启动docker服务

```
mkdir -p /etc/cloudam/registry
cp ./config/deploy/registry.yml ./
docker-compose -f registry.yml up -d
```

步骤4 启动docker集群

1. 解压docker镜像压缩文件并推送至本地docker镜像仓库

```
tar -zxvf image_cloud.tar.gz
ls ./image/local/*.tar | xargs -n1 docker load -i
docker images | grep latest | grep -v deploy | awk '{print "docker tag " $1 ":latest deploy:5000/" $1
":latest;docker push deploy:5000/" $1 ":latest"}' | xargs  -i  sh -c '{}'
```

2. 按说明配置.env文件内容

```
vi  /etc/cloudam/.env
```

3. 使用yml文件启动docker服务

```
env $(cat /etc/cloudam/.env | grep ^[A-Z] | xargs) docker stack deploy --with-registry-auth --compose-
file $cluster_file cloudam
```

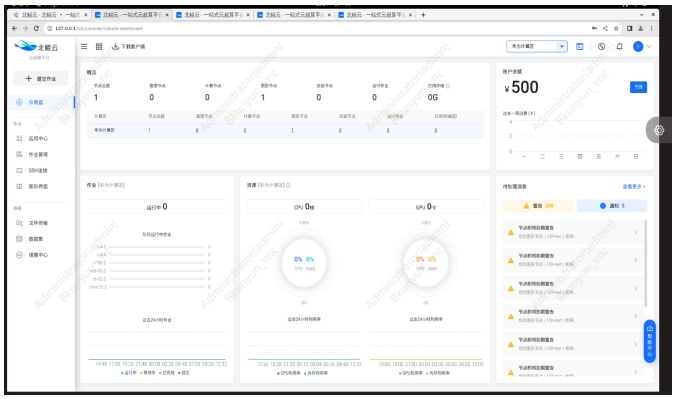
步骤5 验证服务是否正常运行

1. 部署后检查是否成功

```
cd /etc/cloudam
cp ./config/deploy/step4_check_post.sh ./
bash step4_check_post.sh
```

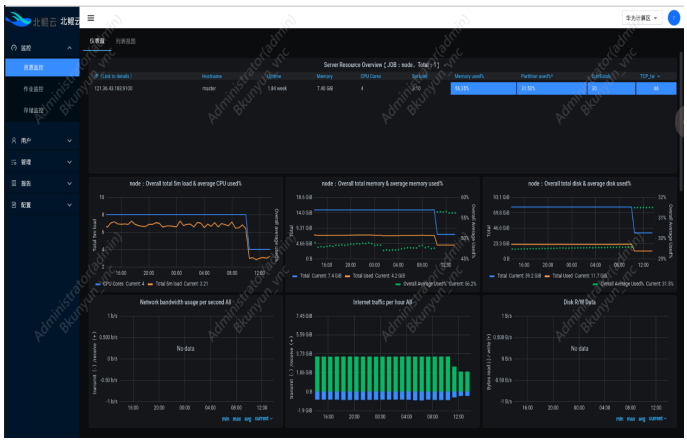
2. 登录北鲲云控制台

图 3-24 登录北鲲云控制台



3. 登录北鲲云管理后台

图 3-25 登录北鲲云管理后台



----结束

3.2 配置 LDAP 服务

3.2.1 部署 ldap 服务端

1. 配置yml文件ldap用户密码等信息
```
vi ldap.yml
```
2. 使用yml文件启动ldap docker服务
```
docker-compose -f ldap.yml up -d
```

3.2.2 配置 ldap 主从

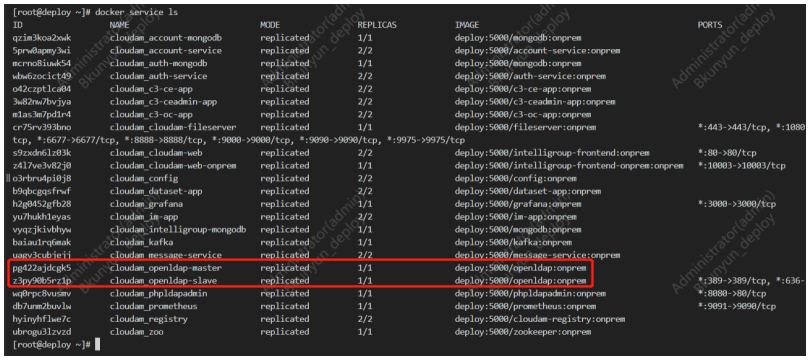
1. 开启syncprov模块
```
cat << EOF > mod_syncprov.ldif
dn: cn=module{0},cn=config
changetype: modify
add: olcModuleLoad
olcModuleload: syncprov.la
EOF
DOCKER_LDAP_ID=`docker ps |grep openldap |awk '{print $1}'`
docker cp mod_syncprov.ldif ${DOCKER_LDAP_ID}:/
docker exec ${DOCKER_LDAP_ID} ldapadd -Y EXTERNAL -H ldapi:/// -f /mod_syncprov.ldif
```
2. 生成 syncprov 配置
```
cat << EOF > syncprov.ldif
dn: olcOverlay=syncprov,olcDatabase={1}mdb,cn=config
objectClass: olcOverlayConfig
objectClass: olcSyncProvConfig
olcOverlay: syncprov
olcSpCheckpoint: 100 10
olcSpSessionLog: 100
EOF
docker cp syncprov.ldif ${DOCKER_LDAP_ID}:/
docker exec ${DOCKER_LDAP_ID} ldapadd -Y EXTERNAL -H ldapi:/// -f /syncprov.ldif
```
3. 开启同步
```
cat << EOF > syncrepl.ldif
dn: olcDatabase={1}mdb,cn=config
changetype: modify
add: olcSyncRepl
```

```
olcSyncRepl: rid=002
provider=ldap://openldap-master
bindmethod=simple
binddn="cn=admin,dc=xxx,dc=xxx"
credentials=xxxx
searchbase="dc=xxx,dc=xxx"
scope=sub
schemachecking=on
type=refreshAndPersist
retry="5 5 600 +"
attrs="*,+"
EOF
DOCKER_LDAP_ID=`docker ps |grep openldap |awk '{print $1}'`
docker cp syncrepl.ldif ${DOCKER_LDAP_ID}:/
docker exec ${DOCKER_LDAP_ID} ldapadd -Y EXTERNAL -H ldapi:/// -f /syncrepl.ldif
```

3.2.3 配置 ldap 客户端

1. 在目标主机安装ldap客户端
   ```
   yum install -y nss-pam-ldapd openldap-clients
   ```
2. 配置系统文件
   ```
   /bin/cp -f /tmp/packer/config/ldap/centos/nslcd.conf /etc/nslcd.conf
   /bin/cp -f /tmp/packer/config/ldap/centos/nsswitch.conf /etc/nsswitch.conf
   /bin/cp -f /tmp/packer/config/ldap/centos/authconfig /etc/sysconfig/authconfig
   /bin/cp -f /tmp/packer/config/ldap/centos/password-auth /etc/pam.d/password-auth
   /bin/cp -f /tmp/packer/config/ldap/centos/system-auth /etc/pam.d/system-auth
   ```
3. 配置客户端连接配置nslcd.conf
   ```
   vi /etc/nslcd.conf
   ```
4. 启动客户端服务
   ```
   sudo chmod 600 /etc/nslcd.conf
   sudo systemctl disable nslcd
   ```
5. 查看部署状态
   ```
   docker service ls
   ```

图 3-26 查看部署状态



4 修订记录

表 4-1 修订记录

发布日期	修订记录
2023-03-03	第一次正式发布。