UniCloud OS 云操作系统

部署指导

紫光云技术有限公司
www.unicloud.com

资料版本：5W100-20230515
产品版本：UniCloud OS-E7108

前 言

UniCloud OS 云操作系统部署指导介绍了 UniCloud OS 的组成和服务器类型、安装前的准备工作、网络及存储规划、安装的具体步骤、安装完成后服务器系统时间的设置方法及访问方法。

前言部分包含如下内容：

读者对象

本手册主要适用于如下工程师：

- 网络规划人员
- 现场技术支持与维护人员
- 负责网络配置和维护的网络管理员

本书约定

1. 图形界面格式约定

格　式	意　义
< >	带尖括号“< >”表示按钮名，如“单击<确定>按钮”。
[ ]	带方括号“[ ]”表示窗口名、菜单名和数据表，如“弹出[新建用户]窗口”。
/	多级菜单用“/”隔开。如[文件/新建/文件夹]多级菜单表示[文件]菜单下的[新建]子菜单下的[文件夹]菜单项。

2. 各类标志

本书还采用各种醒目标志来表示在操作过程中应该特别注意的地方，这些标志的意义如下：

 警告	该标志后的注释需给予格外关注，不当的操作可能会对人身造成伤害。
 注意	提醒操作中应注意的事项，不当的操作可能会导致数据丢失或者设备损坏。
 提示	为确保设备配置成功或者正常工作而需要特别关注的操作或信息。
 说明	对操作内容的描述进行必要的补充和说明。
 窍门	配置、操作、或使用设备的技巧、小窍门。

3. 端口编号示例约定

本手册中出现的端口编号仅作示例，并不代表设备上实际具有此编号的端口，实际使用中请以设备上存在的端口编号为准。

资料意见反馈

如果您在使用过程中发现产品资料的任何问题，可以通过以下方式反馈：

E-mail：unicloud-ts@unicloud.com

感谢您的反馈，让我们做得更好！

目 录

1 概述

1.1 CloudOS7.0大云解决方案简介

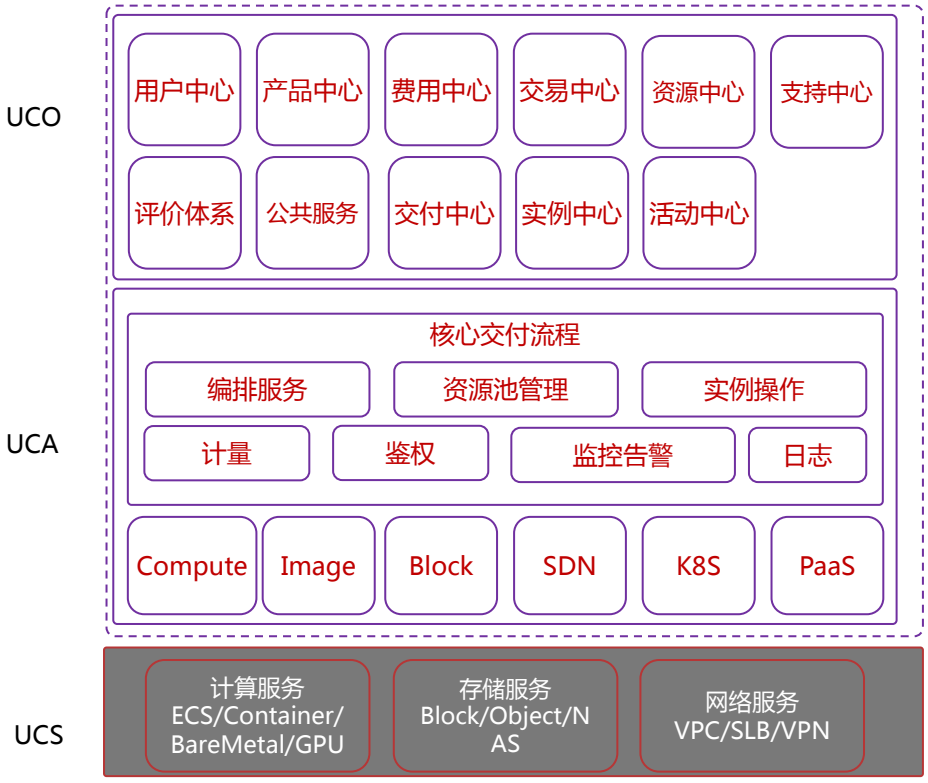
CloudOS 7.0 作为全新的云操作系统，纳管传统 IT 资源，并融合容器、DevOps、大数据等新兴技术，在保障云安全的同时，实现了 IaaS、PaaS、SaaS 的自动化交付。

1.2 部署架构介绍

1.2.1 整体架构介绍

CloudOS7.0 整体架构设计分为三大部分：产品服务层（UniCloud system，以下简称 UCS）、产品运营层（UniCloud orchestration，以下简称 UCO）和产品管理层（UniCloud administration，以下简称 UCA）。UCS 提供独立、可配置的云产品服务，即云服务产品的配置管理平台；UCA 提供实例配置、操作、资源池的管理，作为云服务产品的运维平台，可部署在各个节点。UCO 提供云产品的定义、资源实例售卖、交易，作为云服务产品的运营平台部署在管理节点。

图1-1 CloudOS 7.0 整体架构



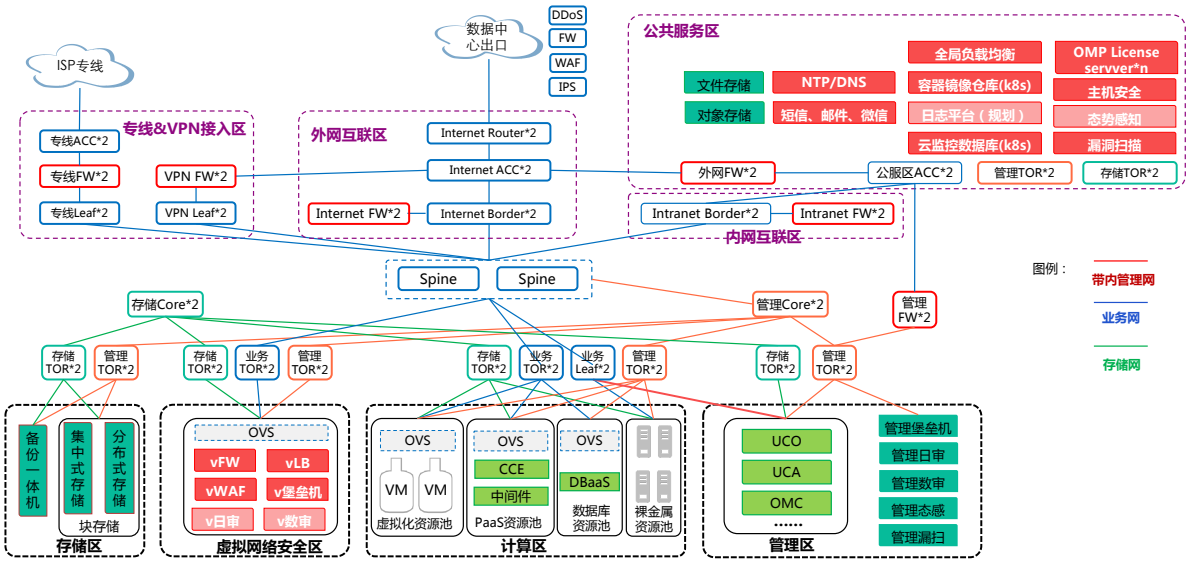
1.2.2 网络架构介绍

私有云场景下当前主推单 AZ 标准部署、单 AZ 轻量化部署、多 AZ 标准部署和边缘云 LZ 部署四种网络部署方式。

1. 单 AZ 标准部署网络架构

标准部署模式提供全栈云服务及必要的网络接入分区配置。内网互联区负责租户访问、对象存储及公共安全的 NAT 转换，为防止网络规划冲突，内网互联区为必配。

图1-2 单 AZ 标准部署模式网络拓扑

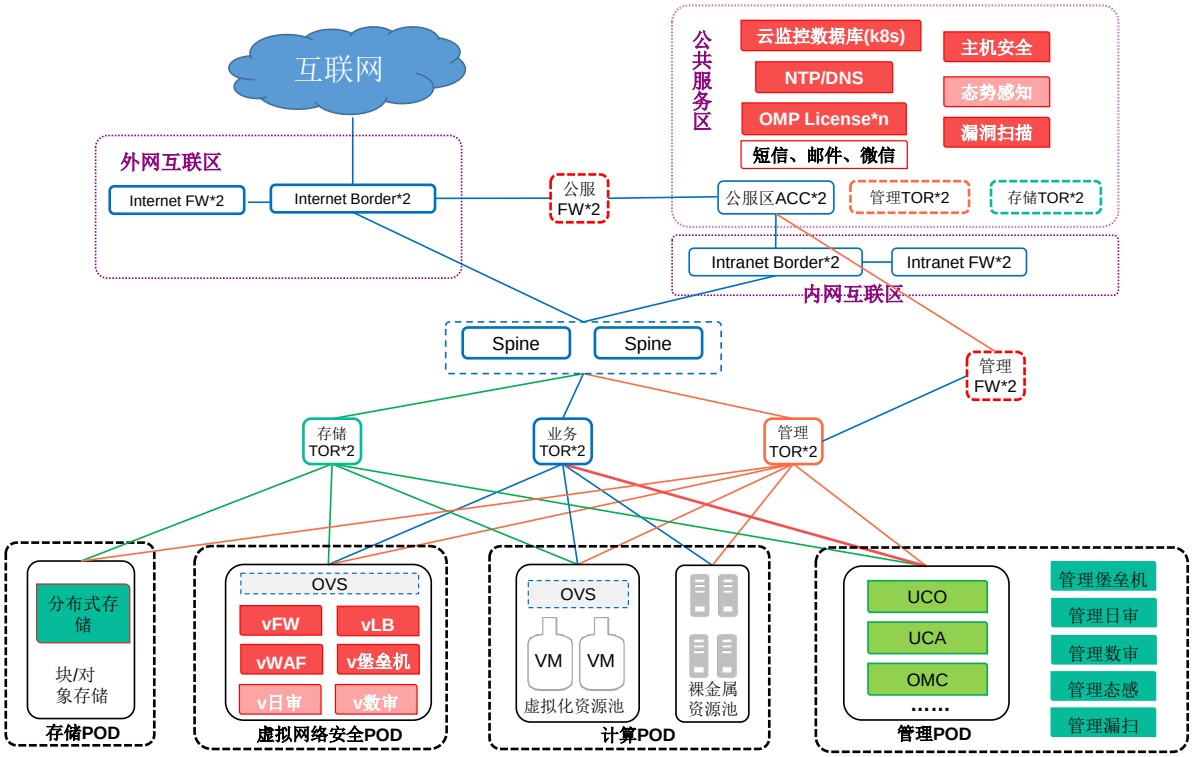


- 服务器到业务/存储 TOR 连接可支持选择万兆/25G；服务器到管理 TOR 为万兆连接。
- 服务器带外管理连接网络为千兆板载网络，未在图中体现。
- 图中，公共安全区 Intranet FW 可以用 vFW 方案代替，即在公共安全区资源池内起虚机部署防火墙镜像。
- NAS 存储与块存储同时存在时，需为 NAS 存储单独规划存储前端及存储后端 TOR 交换机。
- 租户业务区流量经网络安全服务器解封装及 NAT 后去往外网及对象存储、主机安全。
- 交换机及防火墙带外管理连接网络未体现，为千兆板载网络。

2. 单 AZ 轻量化部署模式

单 AZ 轻量化部署模式可满足基础的 IAAS、PAAS 服务需求。无专线/VPN 接入和对象存储服务需求，交换机可根据端口数量评估是否复用。DMZ（公共安全区）与管理区合并。

图1-3 单 AZ 轻量化部署模式网络拓扑

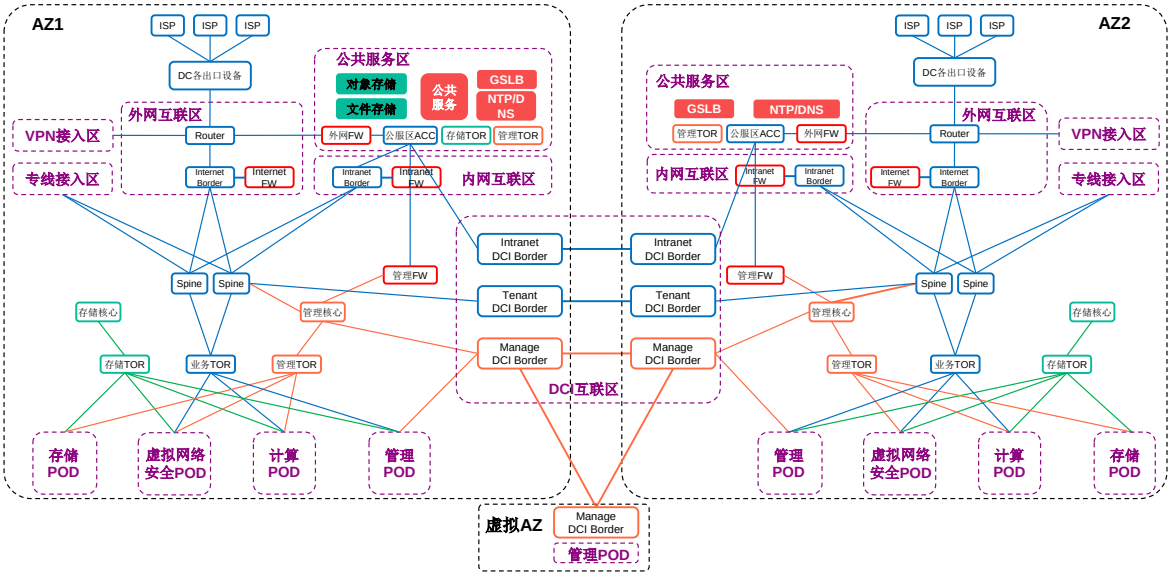


- 轻量化云逻辑组网与标准云方案完全一致；
- 轻量化方案主要在物理部署上做网络和服务器使用做融合，用虚拟交换机、服务器双网卡实现安全隔离；
- 建议轻量化云建设项目规模小于 50 节点，否则优先采用标准云方案。

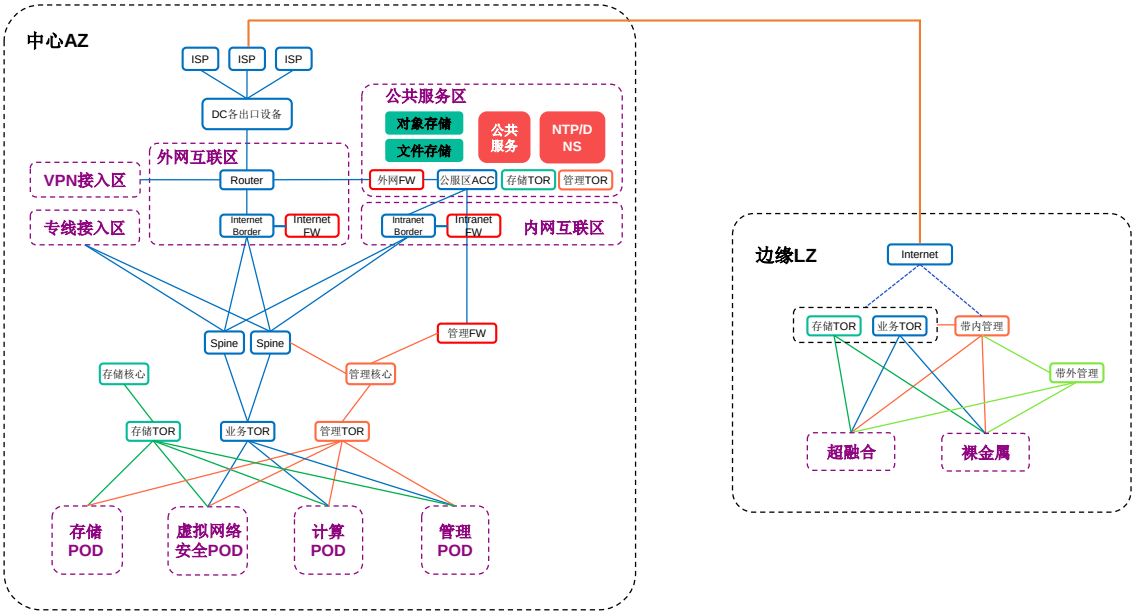
3. 多 AZ 标准部署模式

多区域部署模式采用双中心设计，且两个数据中心网络系统的总体设计基本保持一致。两个数据中心之间通过专线连接进行数据级交互。网络架构采用 spine-leaf 结构，结合 VxLAN+SDN 技术，对整个网络进行管理和配置。当用户业务扩展时，通过集中管理，用户可以方便快速的部署网络设备，便于网络的扩展和管理。

图1-4 多区域部署模式网络拓扑



4. 边缘云 LZ 部署模式



2 部署流程介绍

CloudOS7.0 的部署整体可分为管理区部署和业务区部署。管理区整体采用容器化部署，保障业务的高可用集群化部署，以及横向扩展的能力，并保障管理区的稳健运行。业务区资源池的部署，依托现有各产品部署方案，对资源池的纳管需要可以通过 UI 进行，无需任何命令行模式的操作。云服务可以独立部署。部署某云服务后，将安装此云服务的控制台、A 层服务等，并且可根据需要对云服务进行独立升级。

CloudOS 7.0 的整体部署流程如下。

2.1 项目规划

您需要准备如下清单：

- 产品规格清单
- 平台拓扑图
- 机柜图和连线表
- IP 地址规划表
- 设备登录管理表

2.2 部署前的准备

开始部署前，您需要准备如下信息。

1. 部署前需确认的信息

需要参照产品同步发布的《CloudOS 7.0 软硬件兼容性列表》来确认平台的每个分区中所使用的配套设备的类型、设备型号、硬件配置及软件版本等信息。

2. 部署场景及资源规划

提供了不同的业务规模、不同场景下，建议部署的服务器数量。您可以根据实际业务情况进行规划部署。

3. 网络准备

包括网络及安全设备配置要求、网络地址规划建议、网络设备基础配置。

4. 存储准备

包括存储设备硬件配置要求、存储基本配置。

5. 管理区准备

包括服务器硬件配置要求、服务器安装配置。

6. 业务区准备

包括服务器硬件配置要求、服务器安装配置。

7. 网络安全区准备

提供了网络安全区服务器硬件配置要求及推荐选型，您可以根据需要进行选择。

8. 安装文件准备

需要参照产品同步发布的《CloudOS 7.0 软硬件兼容性列表》来准备 Usphere VMS/VKS 安装包、分布式存储安装包。

9. NTP 服务器准备

当用户指定 NTP 服务器的 IP 地址时，可以进行准备。

2.3 云平台软件部署

通过 Rebirth 工具，依次完成云平台软件的部署和健康检查。

2.3.1 部署前准备

在使用 Rebirth 工具前，您需要先准备安装文件、准备部署工具的虚拟机运行环境、基础组件运行的虚拟机环境，并准备版本交付件清单。

2.3.2 部署阶段

准备阶段完成后，登录 Rebirth 工具，依次完成基础组件部署、云模块部署、VKS 初始化和裸金属初始化等操作。

2.3.3 健康检查

组件部署完成后，您需要对每个组件的部署情况进行健康检查，确保组件部署成功。包括基础组件集群状态巡检、云模块运行状态巡检、设备初始化结果检查。

2.4 资源纳管

- 纳管网络设备
- 纳管存储设备
- 纳管镜像服务器
- 纳管计算设备

2.5 平台初始化配置

2.5.1 运营平台数据初始化

您需要查看已上架产品是否符合环境需求，对缺失产品进行配置并上架、对多余产品进行下架。

2.5.2 运维平台 OMC 初始化

包括容量平台、CMDB、作业平台及监控平台、日志平台等的初始化操作。

2.5.3 云监控初始化

包括对云监控内置探针进行升级等操作。

2.5.4 对象存储初始化

通过 SDS 创建对象存储时，需要进行初始化操作，以便完成与云平台对接。

2.5.5 中间件初始化

您需配置用户目录、产品上架、售卖项价格上架以及镜像上传和注册等。

2.5.6 公共服务区 PaaS 底座部署

在对镜像仓库 CCR 等进行初始化前，需要先对公共服务区 PaaS 底座进行部署。

2.5.7 公共服务区 CCR Harbor 初始化

您需要新建存储桶、配置环境变量、执行部署脚本等。

2.5.8 云容器引擎 CCE 初始化

您需上传系统镜像、修改云模块参数、安装并配置云容器引擎等。

2.5.9 数据库初始化

包括 DBAAS MONITOR 初始化、DBAAS RDS UCA 初始化和 DBAAS RDS/NOSQL UCO 初始化。

2.5.10 PaaS 平台数据库初始化

包括应用管理组件、微服务引擎和服务网关组件以及持续交付组件的初始化。

3 部署前的规划

3.1 服务规格清单规划

在部署前需规划整体解决方案的详细规格。举例如下。

表3-1 服务规格清单规划

类别	服务	类型	核数（vCPU）	内存（GB）
计算	云主机（ECS）	通用型	1	4
			2	8
			4	16
			8	32
			12	48
			16	64
			24	96
		计算型	1	2
			2	4
			4	8
			8	16
			12	24
			16	32
			24	48
		内存型	1	8
			2	16
			4	32
			8	64
			12	96
			16	128
			24	192
存储	云硬盘（EBS）	类型	步长规格	
		高性能HDD	1GB	
网络	弹性公网IP（EIP）	类型	规格	
		单线	1Mbps	
			2Mbps	
			3Mbps	

			4Mbps	
			5Mbps	
			>=6Mbps	
		IP 地址费用	规格	
		IP地址费用 （仅在共享带宽和按流量计费时收取）	单线	个
	共享带宽	类型	步长规格	
		单线	1Mbps	
	负载均衡	报价项	规格	
		报价项1：实例费	基础型I	
			标准型I	
			增强型I	
			增强型II	
		报价项2：带宽费	Mbps	
	NAT网关	报价项1：实例费	个	
		报价项2：带宽费	Mbps	

3.2 网络拓扑图

请参考附录 A、附录 B。

3.3 机柜图和连线表

根据实际机房情况，设计云平台各设备的摆放位置，并设计设备之间的连线关系。机柜图举例如下：

图3-1 机柜连线图示例

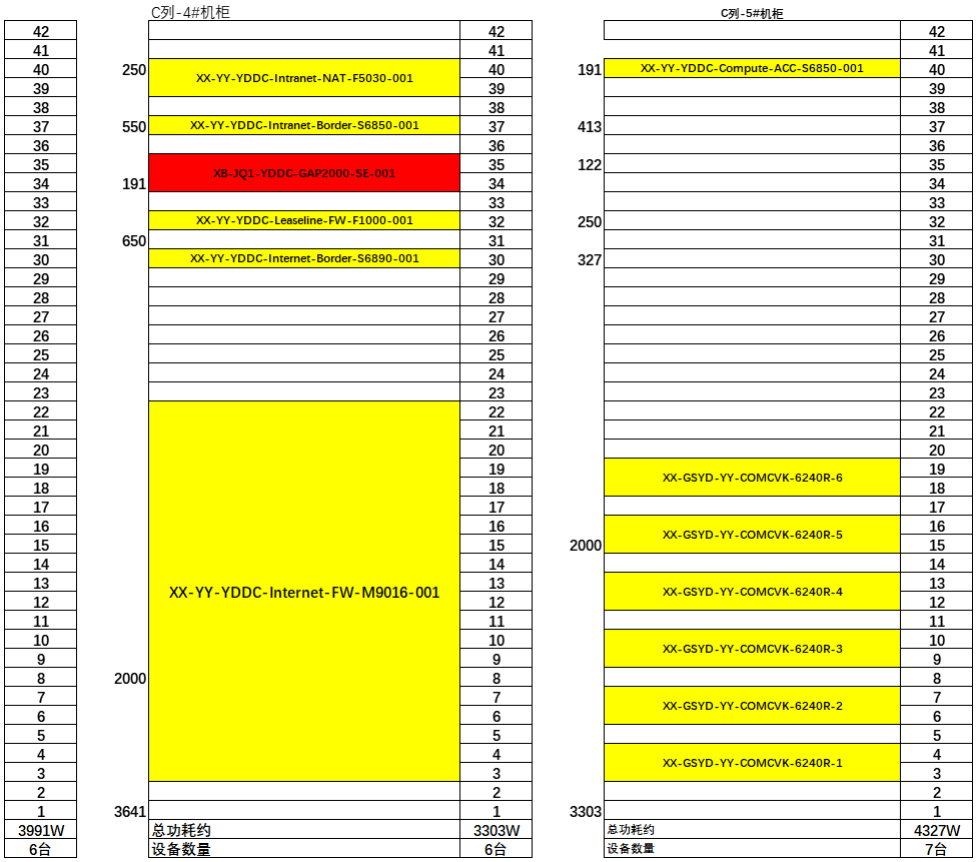

C列-4#机柜
XX-YY-YDDC-Intranet-NAT-F5030-001
XX-YY-YDDC-Intranet-Border-S6850-001
XB-JQ1-YDDC-GAP2000-SE-001
XX-YY-YDDC-Leaseline-FW-F1000-001
XX-YY-YDDC-Internet-Border-S6890-001
XX-YY-YDDC-Internet-FW-M9016-001
总功耗约
设备数量
3991W
6台
3303W
6台
C列-5#机柜
XX-YY-YDDC-Compute-ACC-S6850-001
XX-GSYD-YY-COMCVK-6240R-6
XX-GSYD-YY-COMCVK-6240R-5
XX-GSYD-YY-COMCVK-6240R-4
XX-GSYD-YY-COMCVK-6240R-3
XX-GSYD-YY-COMCVK-6240R-2
XX-GSYD-YY-COMCVK-6240R-1
总功耗约
设备数量
4327W
7台

表3-2 设备连线对应表示例

设备类型	本端设备名	本端机柜	本地端口	接口类型	本端vlan	本端IP	对端设备名	对端机柜	对端接口	接口类型	对端vlan	对端IP	线缆类型
VPN Router	YDDC-MSR3610-001	G05	GE0/0	Route	untagged	10.106.46.1/30	G04-YDDC-Console-SW-001	G04	Eth1	Route	untagged	10.106.46.2/30	RJ45
			GE0/1	Route	untagged	10.106.46.5/30	G05-YDDC-Console-SW-002	G05	Eth1	Route	untagged	10.106.46.6/30	RJ45
			GE0/2	RAGG2	untagged	10.106.46.9/30	YDDC-MGT-AGG-S6800-001	G04	XGE1/0/1	RAGG1	untagged	10.106.46.10/30	LC-LC
			GE0/3	RAGG3	untagged	10.106.46.13/30	YDDC-MGT-AGG-S6800-002	G05	XGE1/0/1	RAGG1	untagged	10.106.46.14/30	LC-LC
			GE0/4	Route	untagged	[redacted]	BRAS08(4层)		G6/0/1.1				LC-FC
Console Server-1	YDDC-Console-SW-001	G04	Port1				YDDC-Internet-RT-SR8803-001	G02	Console				RJ45
			Port2				YDDC-MGT-AGG-S6800-001	G04	Console				RJ45
			Port3				YDDC-MGT-FW-F1010-001	G04	Console				RJ45
			Port4				YDDC-Intranet-ACC-S6800-001	G02	Console				RJ45
			Port5				YDDC-Intranet-NAT-F5030D-001	G02	Console				
			Port6				YDDC-Intranet-Border-S6800-001	G02	Console				RJ45
			Port7				YDDC-Corenet-Spine-9804-001	G04	Console				RJ45
			Port8				YDDC-Net-MGT-ACC-S5560X-001	G02	Console				RJ45
			Port9				YDDC-oneStor-ACC-S6800-001	G06	Console				RJ45
			Port10				YDDC-oneStor-Backend-S6800-001	G06	Console				RJ45
			Port11				YDDC-DMZ-ACC-S6800-001	G04	Console				RJ45
			Port12				YDDC-Server-MGT-ACC-S6800-001	G06	Console				RJ45
			Port13				YDDC-DANOS-ACC-S6800-001	G02	Console				RJ45
			Port14				YDDC-Compute-ACC-S6800-001	G06	Console				RJ45
			Port15				YDDC-Leaseline-AGG-S6800-001	G04	Console				RJ45
			Port16				YDDC-Leaseline-FW-F5020-001	G04	Console				RJ45
			Port17				YDDC-Leaseline-ACC-S6800-001	G04	Console				RJ45
			Port18				YDDC-VPN-FW-5030D-001	G04	Console				RJ45
			Port19				YDDC-IPS-T5030-001	G02	Console				RJ45
			Port20				YDDC-Internet-FW-F5020-001	G02	Console				RJ45
			Port21				YDDC-log-SecCenter CSAP	G02	Console				RJ45
			Port22				YDDC-Internet-ACC-S6800-001	G02	Console				RJ45
			Port23				YDDC-DB-D2030-001	G02	Console				RJ45
			Eth1	Route	untagged	10.106.46.2/30	YDDC-MSR3610-001	G05	GE0/0	Route	untagged	10.106.46.1/30	RJ45
Console Server-2	YDDC-Console-SW-002	G05	Port1				YDDC-Internet-RT-SR8803-002	G03	Console				RJ45
			Port2				YDDC-MGT-AGG-S6800-002	G05	Console				RJ45
			Port3				YDDC-MGT-FW-F1010-002	G05	Console				RJ45
			Port4				YDDC-Intranet-ACC-S6800-002	G03	Console				RJ45
			Port5				YDDC-Intranet-NAT-F5030D-002	G03	Console				RJ45
			Port6				YDDC-Intranet-Border-S6800-002	G03	Console				RJ45
			Port7				YDDC-Corenet-Spine-9804-002	G05	Console				RJ45
			Port8				YDDC-Net-MGT-ACC-S5560X-002	G03	Console				RJ45
			Port9				YDDC-oneStor-ACC-S6800-002	G07	Console				RJ45
			Port10				YDDC-oneStor-Backend-S6800-002	G07	Console				RJ45
			Port11				YDDC-DMZ-ACC-S6800-002	G05	Console				RJ45
			Port12				YDDC-Server-MGT-ACC-S6800-002	G07	Console				RJ45
			Port13				YDDC-DANOS-ACC-S6800-002	G03	Console				RJ45
			Port14				YDDC-Compute-ACC-S6800-002	G07	Console				RJ45
			Port15				YDDC-Leaseline-AGG-S6800-002	G05	Console				RJ45
			Port16				YDDC-Leaseline-FW-F5020-002	G05	Console				RJ45
			Port17				YDDC-Leaseline-ACC-S6800-002	G05	Console				RJ45
			Port18				YDDC-VPN-FW-F5030D-002	G05	Console				RJ45
			Port19				YDDC-NTA-SecCenter CSAP	G03	Console				RJ45
			Port20				YDDC-Internet-FW-F5020-002	G03	Console				RJ45
			Port21				YDDC-ILO-MGT-ACC-S5560X-001	G04	Console				RJ45
			Port22				YDDC-Internet-ACC-S6800-002	G03	Console				RJ45
			Port23				YDDC-SecCenter CSAP-X	G03	Console				RJ45
			Eth1	Route	untagged	10.106.46.6/30	YDDC-MSR3610-001	G05	GE0/1	Route	untagged	10.106.46.5/30	RJ45
MGT FW-1	YDDC-MGT-FW-F1010-001	G04	GE1/0/0	RBM-RAGG1	untagged	10.106.45.46/30	YDDC-Intranet-ACC-S6800-001	G02	XGE1/0/5	RAGG5	untagged	10.106.45.45/30	LC-LC
MGT FW-1			GE1/0/1	RBM-RAGG2	untagged	10.106.46.18/30	YDDC-MGT-AGG-S6800-001	G04	XGE1/0/2	RAGG2	untagged	10.106.46.17/30	LC-LC
			GE1/0/8	RBM-RAGG8	untagged		YDDC-Net-MGT-ACC-S5560X-001	G02	GE1/0/3				RJ45
MGT FW-1			.....										
MGT FW-1			GE1/0/10	RBM-Group	None	1.1.1.1/30	YDDC-MGT-FW-F1010-002	G05	GE1/0/10	RBM-Group	None	1.1.1.2/30	RJ45
MGT FW-1			GE1/0/11	RBM-Group	None	1.1.1.1/30	YDDC-MGT-FW-F1010-002	G05	GE1/0/11	RBM-Group	None	1.1.1.2/30	RJ45
MGT FW-2	YDDC-MGT-FW-F1010-002	G05	GE1/0/0	RBM-RAGG1	untagged	10.106.45.58/30	YDDC-Intranet-ACC-S6800-002	G03	XGE1/0/5	RAGG5	untagged	10.106.45.57/30	LC-LC
MGT FW-2			GE1/0/1	RBM-RAGG2	untagged	10.106.46.22/30	YDDC-MGT-AGG-S6800-002	G05	XGE1/0/2	RAGG2	untagged	10.106.46.21/30	LC-LC
			GE1/0/8	RBM-RAGG8	untagged		YDDC-Net-MGT-ACC-S5560X-002	G03	GE2/0/4				RJ45
MGT FW-2			.....										
MGT FW-2			GE1/0/10	RBM-Group	None	1.1.1.2/30	YDDC-MGT-FW-F1010-001	G04	GE1/0/10	RBM-Group	None	1.1.1.1/30	RJ45
MGT FW-2			GE1/0/11	RBM-Group	None	1.1.1.2/30	YDDC-MGT-FW-F1010-001	G04	GE1/0/11	RBM-Group	None	1.1.1.1/30	RJ45
MGT AGG-1	YDDC-MGT-AGG-S6800-001	G04	XGE1/0/1	RAGG1	untagged	10.106.46.10/30	YDDC-MSR3610-001	G05	GE0/2	RAGG2	untagged	10.106.46.9/30	LC-LC
MGT AGG-1			XGE1/0/2	RAGG2	untagged	10.106.46.17/30	YDDC-MGT-FW-F1010-001	G04	GE1/0/8	RBM-RAGG8	untagged	10.106.46.18/30	LC-LC
MGT AGG-1			XGE1/0/3	RAGG3	untagged	10.106.46.25/30	YDDC-MGT-AGG-S6800-002	G05	XGE1/0/3	RAGG3	untagged	10.106.46.26/30	LC-LC
MGT AGG-1			XGE1/0/4	RAGG4	untagged	10.106.46.29/30	YDDC-Server-MGT-ACC-S6800-001	G06	XGE1/0/47	RAGG47	untagged	10.106.46.30/30	LC-LC
MGT AGG-1			XGE1/0/5	RAGG5	untagged	10.106.46.33/30	YDDC-Net-MGT-ACC-S5560X-001	G02	XGE1/0/49	RAGG49	untagged	10.106.46.34/30	LC-LC
MGT AGG-1			XGE1/0/6	RAGG6	untagged	10.106.46.37/30	YDDC-ILO-MGT-ACC-S5560X-001	G04	XGE1/0/49	RAGG49	untagged	10.106.46.38/30	LC-LC

3.4 IP地址规划表

请参考附录 A、附录 B 对应的组网方案。

说明

IP 网段 10.96.0.0/12、10.244.0.0/16 和 172.17.0.0/16 为系统所占用，在进行 IP 地址规划时请避开这三个网段。

3.5 计算设备登录管理表

请参考附录 A、附录 B 对应的组网方案。

3.6 网络设备登录管理表

请参考附录 A、附录 B 对应的组网方案。

4 部署前的准备

4.1 部署前需确认的信息

针对不同的部署模式，在部署前需要确认以下信息。以下信息仅供参考，请参考产品同步发布的《CloudOS 7.0 软硬件兼容性列表》进行确认。

图4-1 资源分配及配置说明

	规划分区	组成模块	配套设备	关键点说明	支持型号	必配/选配	备注
精简方案必配分区	互联网接入区	网络	出口路由器	接入设备	SR6604/8803	必配	
			外网ACC	万兆网卡	S6800	选配	
			Internet Border	交换机，南北向流量VTEP，负责VxLAN流量加解封装	S6800	必配	
		安全	互联网接入IPS	出口流量安全防护	Secpath T5030	选配	可通过一组防火墙复用
			互联网接入FW	出口流量安全防护	F5080/M9000	选配	
			Internet FW	提供租户南北向流量安全防护及NAT转换功能	F5030D/M9000	必配	
	核心交换区	网络	管理核心、业务核心、存储核心	Spine（RR），RR与leaf 及Border建立iBGP邻居，用于反射EVPN发布的路由。	S9850/S12500	必配	三个核心交换区可合并复用
	存储资源区	网络	存储前端TOR	存储前端网，供业务访问；	S6800	必配	
			存储后端TOR	存储后端网，存储设备互连；	S6800	必配	
		分布式存储	块存储	四节点起配，多副本机制；推荐SAS 8T盘，单盘容量确定后后续集群扩容不可变	UniCloud SDS	必配	3.0和5.0版本的RBD-client不支持同时安装到同一个业务VKS和镜像服务器
			文件存储	四节点起配，无特殊要求	UniCloud SDS	选配	
		集中式存	集中式存	提供SSD和高性能	Primera	选配	

	规划分区	组成模块	配套设备	关键点说明	支持型号	必配/选配	备注
		储	储	HDD，每种类型硬盘8块起配，RAID6			
	业务资源区	网络	虚拟化业务TOR	无特殊要求	S6800	必配	
			裸金属业务TOR	需要支持VxLAN功能	S6800	必配	
		服务器	x86/ARM	数据库服务器需本地NVME SSD盘承载存储； 配置文件需要对象存储；	R4900	必配	
	网络安全区	服务器	x86/ARM	租户安全服务及网络服务由NFV网元提供，提供VPC、vLB、EIP、NAT网关、vFW、云堡垒机、vWAF、数审、日审等服务； 4张网卡起配，有对象存储需求按照5张网卡配置；服务器主备模式，2台起配，按租户数量评估	R4900	必配	
		网络	网络安全接入TOR		S6800	必配	
	管理区	网络	管理TOR	万兆网卡	S6800	必配	
			带外管理交换机	千兆网卡即可	S5560	必配	
		安全	防火墙	管理区安全防护，可与DMZ复用	F5030D或vFW	必配	可与公共安全区（DMZ）复用
		服务器	x86/ARM	标准方案4台起配	R4900	必配	
标准方案增加分区	内网互联区	网络	Border交换机	租户访问对象存储或公共安全服务时的VTEP设备	S6800	推荐必配	若租户网络规划不存在内网IP冲突，可不使用，一般必配
		安全	防火墙	租户访问对象存储或公共安全服务做SNAT	F5030		
	公共安全区（DMZ）	网络	交换机	与外网接入ACC、内网互联区Border等设备互联	S6800	必配	
		安全	外网防火墙	外网流量防护	F5030	必配	

	规划分区	组成模块	配套设备	关键点说明	支持型号	必配/选配	备注
		服务器	x86/ARM	2台起配，无特殊要求；负责云平台及管理区安全防护；提供主机安全、态势感知、漏洞扫描、NTP、DNS等服务	R4900	必配	公共安全区可与管理区合并，复用交换机及安全设备
	对象存储区	存储	分布式存储	四节点起配，按照2N节点扩容；可直接通过外网访问使用服务	UniCloud SDS	必配	
	VPN接入区	网络	VPN TOR		S6800	选配	专线和VPN区tor可复用
		安全	防火墙		F5030D/M9000	选配	
	专线接入区	网络	专线Border		S6800	选配	
		安全	防火墙		F5030D/M9000	选配	

4.2 部署场景及资源规划

针对不同的业务规模，在不同场景下部署 CloudOS 7.0 管理平台建议使用的服务器数量如下所示。

图4-2 各核心区域硬件资源配置比例

业务规模（物理节点）	管理 POD（纯 IaaS 精简架构）	管理 POD（IAAS+PAAS 全量服务）	网络安全 POD（与租户数量相关）	分布式存储	DMZ 区
≤50台	精简配置3台	标准配置4台	2台起，主备HA	块存储、文件存储各4台起（不支持混合部署）；对象存储4台起	精简方案2台起，标准方案3台起配
50-100台	4台	7台	每增加20台，加一组（2台）		根据实际运行需求
100台以上	每增加50台业务节点，扩容1台	9台	每增加20台，加一组（2台）		
300台以上		每增加50台业务节点，扩容1台	每增加20台，加一组（2台）		

4.3 设备上架和综合布线

按照机柜图和连线表，将物理设备部署到机柜，并进行连线。

4.4 网络准备

请参考附录 A、附录 B。

4.5 存储准备

4.5.1 存储设备硬件配置要求

存储设备的硬件配置要求及建议选型如下表所示。

图4-3 存储设备硬件配置及选型

部署区域	存储类型	单台规格	推荐型号	功能用途	是否必配	说明
存储资源区	分布式存储-块存储	2路服务器，单颗CPU主频≥2.2GHz，核数≥24；内存≥256G；系统盘≥2块480G SSD盘，数据盘≥5块8T SATA HDD盘，缓存盘≥1块3.2T NVME SSD盘；3块10GE或25GE网卡。	R4900 G3/R4900 G5	提供分布式块存储服务	是	1. 计算服务器 10 台以下，默认配置 4 节点起配，每加 5 台计算服务器，扩容 2 台存储节点； 2. 单台配置不低于 5 块硬盘（IOPS 为 3000 左右），满配的情况下 IOPS 可达 6000-7000； 3. 推荐 8T SATA 盘，对容量要求较大时，可采用 14T/16T 硬盘，限制条件：单盘容量一旦确定后续集群扩容不可再变。
	集中式存储-块存储	按需选择2控或4控设备，硬盘容量按需配置	Primera CF22000	提供集中式块存储服务	视项目需求	1. SSD块存储需求采用集中存储（Primera）根据项目需求出配置； 2. 当明确同时存在 SSD 需求和 HDD 需求且 HDD 需求小于 116T 时，可采用 Primera 同时提供 SSD 和高性能 HDD 服务，要求每种类型硬盘起配数量为 8 块，硬盘通过 raid6(10+2+1spare）做数据保护。其中，SSD 建议配置 3.84T 硬盘，HDD 建议配置 2.4T SAS 盘；
	分布式存储-文件存储	2路服务器，单颗CPU主频≥2.2GHz，核数≥24；内存≥256G；系统盘≥2块480G SSD盘，数据盘≥5块8T SATA HDD盘，缓存盘≥1块1T	R4900 G3/R4900 G5	提供分布式文件存储服务	视项目需求	1. 单台配置不低于 5 块硬盘（IOPS 为 3000 左右），满配的情况下 IOPS 可达 6000-7000； 2. 推荐 8T SATA 盘，对容量要求较大时，可采用 14T/16T 硬盘，但限制条件是单盘容量一旦确定,后续集群扩容不可

部署区域	存储类型	单台规格	推荐型号	功能用途	是否必配	说明
		NVME SSD盘+1块4T NVME SSD盘；3块10GE或25GE网卡。				再变； **3.** NAS基线推荐配置采用容量型，采用分布式存储（SDS），默认配置4 节点起配，对于 NAS 文件存储性能型配置焱融存储 IOPS 为 30000 左右、容量型配置 SDS 存储，IOPS 为 5000 左右。
对象存储区	分布式存储-对象存储	2路服务器，单颗CPU主频≥2.4GHz，核数≥10；内存≥256G；系统盘≥2块480G SSD盘，数据盘≥5块8T SATA HDD盘，缓存盘≥1块1T NVME SSD盘+1块4T NVME SSD盘；3块10GE或25GE网卡。	R4900 G3/R4900 G5	提供分布式对象存储服务	否	对象存储采用分布式存储，默认配置4节点起配，按照2N节点扩容，采用3副本存储容量需求确定。

4.5.2 共享存储卷要求

CloudOS7.0 管理区和公服区需要外联块存储设备提供共享存储卷，当前版本共享存储卷需求如下。

名称	推荐大小	说明
单机部署模式的管理虚机	2T	为管理区单机部署的云平台虚机（如harbor、PMS）提供共享存储，通过UIS/Usphere HA来保证虚机的高可用。同时预留一部分空间作为虚机模板存储使用
管理区备份	1T	为管理区云平台备份提供存储空间
公服区安全服务	根据部署的安全服务按需配置	部署在公共服务区的安全服务虚机（如服务器安全监测服务端、漏扫、各种安全服务License Server）均使用共享存储

4.5.3 存储基本配置

请分别参考 3PAR、Primera 和 SDS 存储产品的开局指导书，进行基本配置。

4.6 管理区准备

4.6.1 服务器硬件配置要求

云管理区的服务器的硬件配置要求及推荐选型如下表所示。

图4-4 云管理区服务器硬件配置要求及选型

服务器	单台规格配置	推荐型号	功能用途	说明	是否必选
管理服务器	2路服务器，单颗CPU主频≥2.2GHz，核数≥32；内存≥768G；系统盘≥2块480G SSD盘，数据盘≥4块1.92T SSD盘；3块10GE或25GE网卡。	R4900 G3/R4900 G5	提供云平台部署环境，云资源运营管理，客户自服务控制台等功能	标准架构下推荐：4台服务器起配，每加50台计算服务器，扩容1台管理服务器； 精简架构下推荐：推荐3台服务器起配。	是
DMZ（公共安全区）服务器	2路服务器，单颗CPU主频≥2.2GHz，核数≥10；内存≥512G；系统盘≥2块480G SSD盘，数据盘≥2块3.84T SSD盘；3块10GE或25GE网卡。	R4900 G3/R4900 G5	平台及管理区安全防护，提供如主机安全、漏洞扫描、DNS、NTP等多安全防护服务。多租户共享一套服务	标准架构下推荐3台服务器起配，精简架构下最低配置2台，此部分扩容按实际运行需求。	否

4.6.2 服务器安装配置

每台管理服务器配置 2 个 10G 网口作为管理网、2 个 10G 网口作为业务网络、2 个 10G 网口作为存储网络。管理网、业务网、存储网的 2 个网口分别连接到管理接入、业务接入、存储接入交换机，并且管理网、业务网、存储网的 2 个网口分别做网卡聚合。

管理虚拟化集群中需要分别创建管理、业务、存储虚拟交换机用于转发 VKS 或者管理虚拟机不同网络平面的数据。所有 VKS 上虚拟交换机命名规则如下表所示。

图4-5 虚拟交换机命名规则

用途	名称
管理虚拟交换机	vswitch0
业务虚拟交换机	vsw-yw
存储虚拟交换机	vsw-stor

云管理区的所有服务器中，选择 2 台服务器安装 VMS 系统搭建双机热备环境，其余均安装 VKS 系统，并由管理区 VMS 统一纳管。

4.7 业务区和网络安全区准备

4.7.1 服务器硬件配置要求

1. 业务区服务器硬件配置要求

计算资源区的服务器硬件配置要求及推荐选型如下表所示。

图4-6 计算资源区服务器硬件配置要求及推荐选型

服务器	单台规格配置	推荐型号	功能用途	说明	是否必选
计算虚拟化服务器（虚拟机）	2路服务器，单颗CPU主频≥2.2GHz，核数≥24；内存≥256G；系统盘≥2块480G SSD盘；3块10GE或25GE网卡。	R4900 G3/R4900 G5	提供虚拟机服务	1. 超分比：1:4 以内 2. 网卡需要 DPDK	是
PaaS资源服务器（容器）	2路服务器，单颗CPU主频≥2.2GHz，核数≥24；内存≥256G；系统盘≥2块480G SSD盘；3块10GE或25GE网卡。	R4900 G3/R4900 G5	提供虚拟机服务	1. 超分比：1:4 以内 2. 网卡需要 DPDK	否
裸金属服务器	参考兼容性列表进行配置	R4900 G3/R4900 G5	提供裸金属服务	-	否
PaaS资源服务器（数据库）	2路服务器，单颗CPU主频≥2.2GHz，核数≥24；内存≥768G；系统盘≥2块480G SSD盘，数据盘≥4块4T NVME SSD盘；3块10GE或25GE网卡。	R4900 G3/R4900 G5	提供本地盘数据库服务	1. 对IO性能要求高的选用本地盘 2. 网卡需要支持DPDK 3. 高可用，4台起配（3+1） 4. 需要配置本地盘	否
大数据资源池&绿洲资源池	参考绿洲、大数据平台规格配置	R4900 G3/R4900 G5	提供大数据、数据中台服务	-	否

说明

- 服务器网卡数量及端口用途：虚拟化服务器、裸金属服务器、PaaS 服务器 3 张网卡，跨网卡做 BOND。
- 同一个集群中的服务器建议采用同一 CPU 厂商、同一代 CPU 型号。

2. 网络安全区服务器硬件配置要求

网络安全区服务器硬件配置要求及推荐选型如下表所示。

图4-7 网络安全区服务器硬件配置要求及推荐选型

服务器	单台规格配置	推荐型号	功能用途	说明	是否必选
网络安全服务器	2路服务器，单颗CPU主频≥2.2GHz，核数≥24；内存≥768；系统盘≥2块480G SSD盘，数据盘≥4块3.84T SSD盘；≥4块10GE或25GE网卡。	R4900 G3/R4900 G5	提供租户的网络安全服务，如vSLB、vNAT网关、vWAF、v堡垒机、v日志审计、v数据库审计、CFW	计算服务器20台以下网络安全服务器2台起配，每增加50计算节点扩容2台，需保证CPU选型不低于5220R。	是

说明

服务器网卡数量及端口用途：网络安全服务区推荐的网卡张数有如下三种情况，存储网和业务网需要跨网卡做 BOND。

- 2 张：例如网络 VKS 方案使用本地存储。
- 3 张：例如安全 VKS 方案使用共享存储。
- 4 张：使用 VSR 和 Danos。

4.7.2 服务器安装配置

1. 规格说明

如果该 VKS 需要存储网，VKS 主机配置 2 个 10G 网口作为管理网、2 个 10G 网口作为业务网、2 个 25G 网口作为存储网。管理网、业务网、存储网的 2 个网口分别连接到管理接入、业务接入、存储接入交换机，并且管理网、业务网、存储网的 2 个网口分别做网卡聚合。

如果该 VKS 不需要存储网，VKS 主机配置 2 个 10G 网口作为管理网、2 个 10G 网口作为业务网。管理网、业务网的 2 个网口分别连接到管理接入、业务接入交换机，并且管理网、业务网的 2 个网口分别做网卡聚合。

2. 安装前服务器配置

在安装 Usphere 系统前，需要根据规划对服务器的本地磁盘进行 RAID 配置，配置方法请参考相应服务器的配置手册。建议 VKS 服务器配置 2 块 600G SAS 盘，配置 RAID 1 作为系统盘。若服务器已安装过系统，再次安装系统前请对服务器的磁盘进行格式化操作。

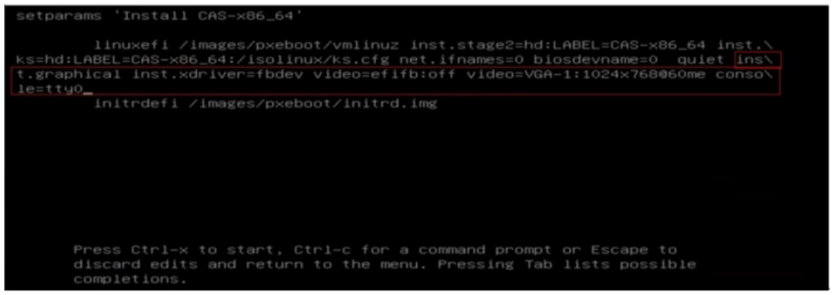
3. 安装步骤

计算资源区的所有服务器，除裸金属服务器无需安装系统外，其余均安装 VKS 系统。安装配置过程如下：

(1) 访问 HDM 界面的远程控制台，挂载 iso 安装包（安装包格式为 UniCloud_USphere-Exxxx-xxx.iso，版本号请从 CloudOS7.0 对应版本的版本说明书文档获取），重启选择启动选择光驱启动，即会进入系统安装界面。

需注意，对于华为服务器（如 RH5885 V3、2288H V5），在安装 Usphere 时可能会遇到黑屏或者其他类似问题，无法进入系统安装界面。

- 为避免该问题的出现，需要在进入 grub 界面时（出现该问题之前），按[e]键进入编辑模式，在 linuxefi 或者 linux 的行末尾增加参数：inst.graphical inst.xdriver=fbdev video=efifb:off video=VGA-1:1024x768-32@60me ro console=tty0，如下图所示，参数添加无误后，按[ctrl+x]，启动安装。

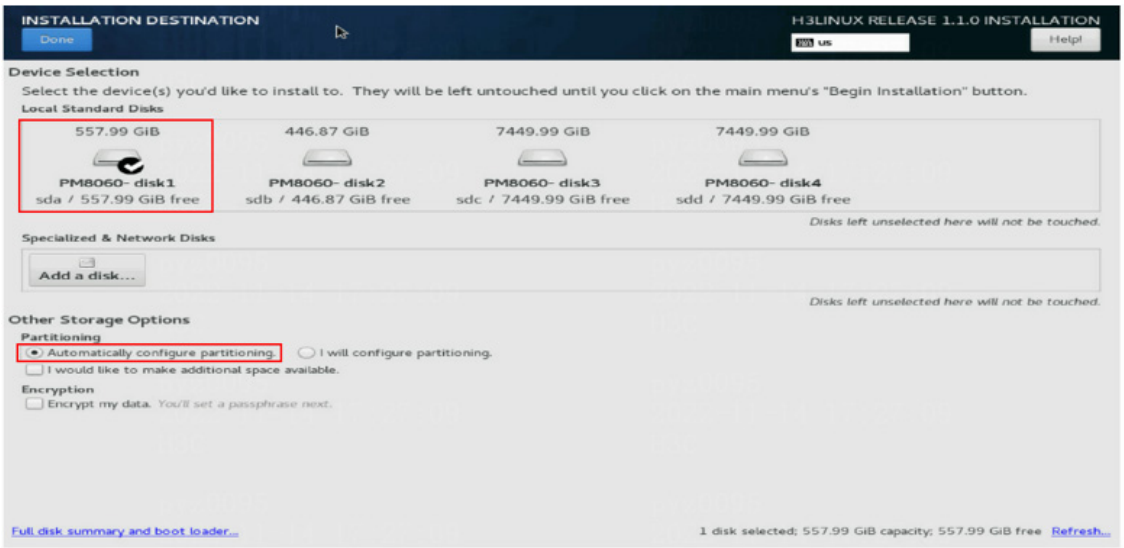


- 若上述问题已出现，只能重启再执行。

(2) 进入 INSTALLATION SUMMARY 页面，请选择系统安装目的地<INSTALLATION DESTINATION>。

a. 请在 Local Standard Disks 区域勾选系统盘，并去勾选不需要安装系统的磁盘。系统盘请选用 sda，即做完 RAID 后的第一块盘。

b. 设置分区配置策略。系统盘支持自动分区<automatically configure partition>和手动分区<I will configure partitioning>两种分区方式，若服务器从未安装过系统或已执行过格式化操作，推荐采用自动分区方式，注意若在 Local Standard Disks 区域未去勾选数据盘，则/vms 分区会自动落在数据盘上。



(3) 请配置 root 密码，root 密码缺省未设置。

(4) 安装完成后，进入系统内，做如下预配置。

a. 挂载 ISO 镜像（cvk-preinit.iso 在 Rebirth 虚机的如下路径：\root\cvk-init\file）。

```
mount /dev/sr0 /mnt
sh /mnt/cvk-preinit.sh
depmod -a
dracut -f
reboot
```

需要注意的是，重启后网卡名可能会发生变化。需先找到正确的网卡，再执行下一步操作。

b. 对管理网卡配置 bond，其中 exxx、ipaddr、netmask 和 gateway 请替换为 VKS 实际管理网卡名、管理 IP、掩码和网关。

```
sh /opt/config-bond-network.sh add bond0 --bond-mode=802.3ad --iface=exxx
--iface=exxx --ipaddr=x.x.x.x --netmask=x.x.x.x --gateway=x.x.x.x
ifup bond0
```

SSH 可以连接为正常。

4.7.3 配置 VNC 服务

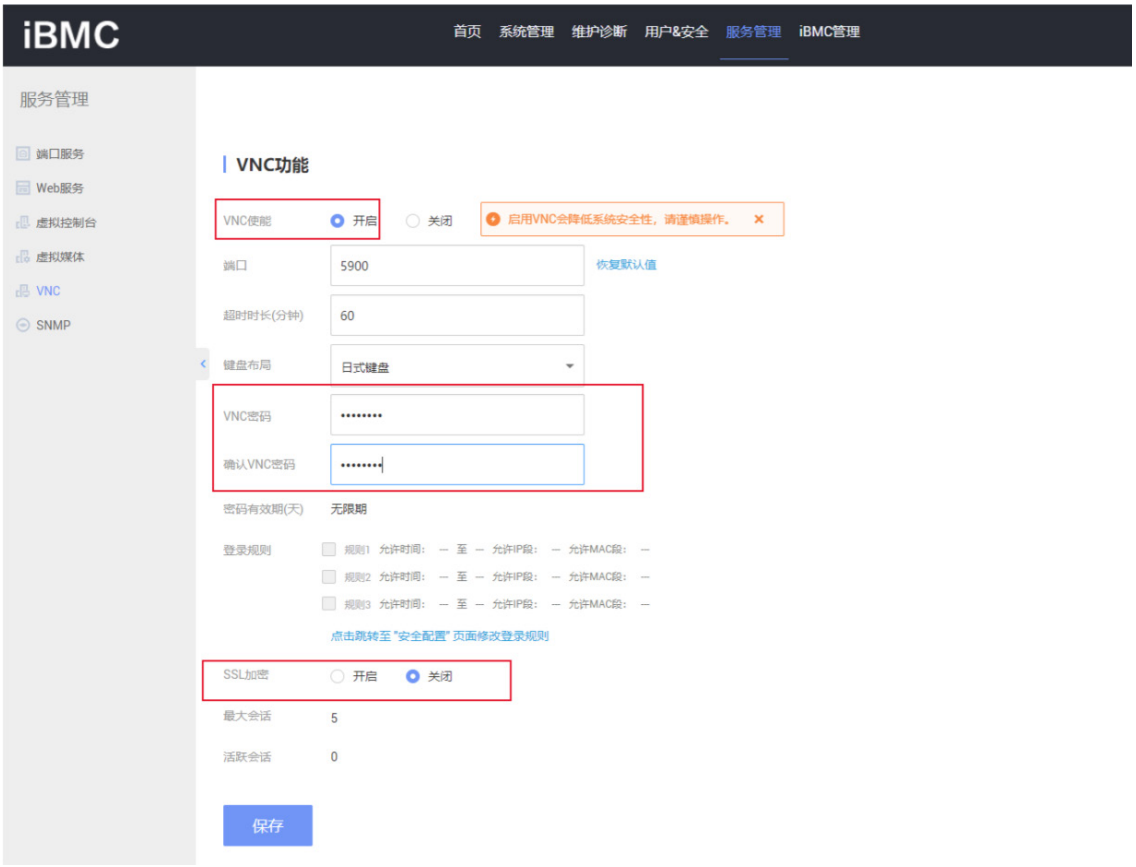
目前支持通过 VNC 方式对业务区服务器进行远程控制。您需要先开启服务器的 VNC 服务，并修改 VNC 登录密码。

如果使用清华同方的 Chaoqiang K620 服务器，由于其密码要求与默认密码不一致，目前暂时不支持通过 VNC 登录。

(1) 登录服务器 Web 页面，选择[远程服务/服务设置]。

(2) 启用 VNC：在服务设置页面，点击 VNC 服务后的<修改>按钮，将 VNC 服务状态修改为“开启”，点击<确定>按钮。

另外需注意，对于华为 2288H V5 服务器，在带外管理页面开启 VNC 使能时要关闭 SSL 加密。



(3) 配置 VNC 密码：选择[远程服务/远程控制台/VNC]，不启用密码复杂度检查，并将密码设置为 cds-chin，点击<保存>按钮。

4.8 安装文件准备

请参考产品同步发布的《CloudOS 7.0 软硬件兼容性列表》进行准备。

4.8.1 Usphere VMS/VKS 安装包

在安装部署 CloudOS 7.0 管理平台前，管理区需安装 Usphere 的 VMS 和 VKS，业务区服务器需安装 VKS。

管理区 Usphere 的安装方式，请参考《UniCloud Usphere 安装指导》。

业务区 VKS 版本请使用正式发布版本，安装包格式为 UniCloud_USphere-Exxxx-xxx.iso，版本号请从 CloudOS 7.0 对应版本的版本说明书文档获取。

4.8.2 分布式存储安装包

存储区需安装 SDS，具体安装方法请参考 SDS 安装指导。

5 云平台软件部署

Rebirth 工具是 CloudOS 7.0 平台的部署工具。通过 Rebirth 工具平台可以实现包括 CloudOS 7.0 基础组件、云模块、主机以及裸金属等的自动化部署。通过该工具平台，还可以完成已部署组件或服务健康状态的巡检。

5.1 部署前准备

5.1.1 安装文件准备

CloudOS 7.0 的部署需要准备如下文件：

- Rebirth 工具（部署工具虚拟机镜像）

  版本号_时间_MD5 值.qcow2

  获取路径：全量包/镜像
- 其他组件主机镜像（基础组件运行虚拟机镜像）

  *时间*_MGT-IMAGE_*用户名_密码_MD5 值*.qcow2

  获取路径：全量包/镜像
- 交付件

  pulled_images.tar（微服务容器镜像文件）、adapter.tar.gz（微服务适配环境变量配置文件）、images_details.list（微服务镜像列表）、codes.tar.gz（配置文件）、md5.txt（交付件校验文件）、productDetails.json（云模块清单）

  获取路径：全量包/XXXX-rebirth

5.1.2 Rebirth 工具虚拟机运行环境准备

在 Usphere 上使用“*版本号_时间_MD5 值*.qcow2”镜像创建虚拟机作为 Rebirth 工具主机，配置管理网络，启动虚拟机。

Rebirth 工具虚拟机后台缺省登录用户名和密码为：

- 缺省用户名：root
- 缺省密码：unicloud

建议在准备 Rebirth 虚机时，参考“10.1 备份准备”章节，完成数据盘挂载。若不进行目录挂载，会导致数据备份时备份失败。

5.1.3 基础组件运行虚拟机环境准备

创建运行基础组件的虚拟机的方法有两种，一种是手工创建，另一种是通过 Rebirth 工具自动创建。

- 若使用手工创建，请根据“虚拟机资源规划表”中的虚拟机规划信息，在 Usphere 管理平台上使用“*时间_用户名_密码_MD5 值*.qcow2”镜像创建虚拟机，配置对应的网络，执行对应的挂盘操作（请参考 5.2.2.1 中挂载硬盘的命令进行操作），启动虚拟机。

- 若使用自动创建可跳过这步，通过 Rebirth 工具创建虚拟机的方法请参见 5.2.3 自动创建虚拟机。

有关“虚拟机资源规划表”的详细介绍，请参见 5.2.2 2. 配置虚拟机资源规划表。

基础组件虚拟机后台缺省登录用户名和密码为：

- 缺省用户名：root
- 缺省密码：unicloud

说明

手工创建时，建议将集群中的虚拟机分别部署在不同的物理服务器上，以确保高可用性。

5.1.4 交付件拷贝

进入 Rebirth 工具虚拟机，将 pulled_images.tar、adapter.tar.gz、images_details.list、codes.tar.gz、md5.txt、productDetails.json 交付件复制到虚拟机的/root/published 路径下。

5.2 基础组件部署

5.2.1 登录 Rebirth 工具平台

(1) 启动浏览器，输入 URL 地址跳转到 Rebirth 工具登录页面（URL 地址：http://*Rebirth 工具主机 IP 地址*:8080/www）

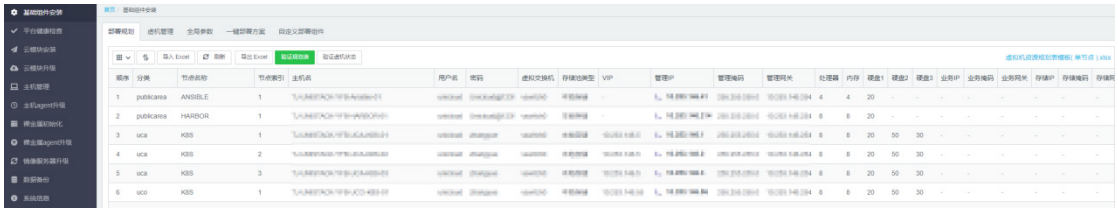
说明

当前支持的浏览器类型有 360 极速和 Chrome 浏览器。不支持使用 IE 浏览器。

---

(2) 在 Rebirth 工具登录页面输入用户名和密码（缺省账号：admin；缺省密码：unicloud），登录 Rebirth 工具平台。

图5-1 登录 Rebirth 工具平台



5.2.2 基础组件部署规划

1. 基础组件部署要求

基础组件部署有如下要求：

- 基础组件部署前后禁止修改各组件的主机名称。
- 管理区 Usphere 上创建的所有虚拟机中，单台虚拟机的 CPU 核数必须小于其所在物理 VKS 的超线程核数。
- 由于 DMZ 区位于公共服务区，当云平台中存在 DMZ 区域时，需要将管理区虚拟机和 DMZ 区的虚拟机分开创建，分别进行两次主机规划和自动创建虚拟机的操作。

各组件虚拟机的要求如下：

节点名称	CPU/内存	数据盘/文件系统	存储类型（推荐）
ANSIBLE	无特殊要求，参考规划表	无特殊要求，参考规划表	硬盘1：共享存储
HARBOR	无特殊要求，参考规划表	数据盘：创建1个数据盘，盘号为vdb，精简模式下数据盘大小为200G；创建/data目录，将vdb盘挂载到/data目录，并将配置添加到/etc/fstab中。 文件系统：ext4。	硬盘1：共享存储 硬盘2：共享存储
UCA K8S	64核	每台虚机均需要创建2块数据盘： • vdb：精简模式下至少 500G；挂载到/var/lib/docker，并将配置添加到/etc/fstab中。 • vdc：精简模式下至少 300G；挂载到/var/log，并将配置添加到/etc/fstab 中。	硬盘1：本地SSD存储 硬盘2：本地SSD存储 硬盘3：本地SSD存储
UCO K8S	64核		硬盘1：本地SSD存储 硬盘2：本地SSD存储 硬盘3：本地SSD存储
TAAG K8S	无特殊要求，参考规划表		硬盘1：本地SSD存储 硬盘2：本地HDD存储 硬盘3：本地HDD存储
DMZ K8S	无特殊要求，参考规划表		硬盘1：本地SSD存储 硬盘2：本地HDD存储 硬盘3：本地HDD存储
OMC K8S	无特殊要求，参考规划表		硬盘1：本地SSD存储 硬盘2：本地SSD存储 硬盘3：本地HDD存储
MYSQL	无特殊要求，参考规划表	数据盘：MYSQL-01、MYSQL-02、MYSQL-03节点需要创建数据盘，盘号为vdb，精简模式下数据盘大小为500G；创建/data目录，将vdb盘挂载到/data目录，删除/data目录下的lost+found，并将配置添加到/etc/fstab中。 文件系统：ext4。	MYSQL-01、MYSQL-02、MYSQL-03节点： 硬盘1：本地SSD存储 硬盘2：本地SSD存储 MYSQLREPM节点： 硬盘1：共享存储
RABBITMQ	无特殊要求，参考规划表	无特殊要求，参考规划表	硬盘1：本地HDD存储
REDIS	无特殊要求，参考规划表	无特殊要求，参考规划表	硬盘1：本地SSD存储

ZOOKEEPER	无特殊要求，参考规划表	无特殊要求，参考规划表	硬盘1：本地HDD存储
KAFKA	无特殊要求，参考规划表	无特殊要求，参考规划表	硬盘1：本地HDD存储
PROMETHEUS	无特殊要求，参考规划表	数据盘：创建1个数据盘，盘号为vdb，精简模式下数据盘大小为300G；创建/var/lib/influxdb目录，将vdb盘挂载到/var/lib/influxdb目录，并将配置添加到/etc/fstab中。 文件系统：ext4。	硬盘1：共享存储 硬盘2：共享存储
PGSQL	无特殊要求，参考规划表	无特殊要求，参考规划表	硬盘1：本地HDD存储
NGINX	无特殊要求，参考规划表	无特殊要求，参考规划表	硬盘1：本地HDD存储
IMAGESERVER	无特殊要求，参考规划表	数据盘：3台虚机均需要创建数据盘，盘号为vdb，精简模式下数据盘大小为500G；创建/image-dir目录，将vdb盘挂载到/image-dir目录，并将挂载配置添加到/etc/fstab中。 文件系统：ext4。	硬盘1：本地SSD存储 硬盘2：本地SSD存储
TFTP	无特殊要求，参考规划表	无特殊要求，参考规划表	硬盘1：共享存储
ELASTICSEARCH	16C32G	4台虚机均需要创建数据盘，盘号为vdb，大小为500G。不需要对数据盘进行任何操作。	硬盘1：本地HDD存储 硬盘2：本地HDD存储
CASSANDRA	16C16G	4台虚机均需要创建数据盘，盘号为vdb，大小为200G。不需要对数据盘进行任何操作。	硬盘1：本地HDD存储 硬盘2：本地HDD存储
GITLAB	4C8G	创建1块数据盘，盘号为vdb，大小为300G。创建/var/opt/gitlab目录，将vdb盘挂载到/var/opt/gitlab目录，并将配置添加到/etc/fstab中。 文件系统：ext4。	硬盘1：共享存储 硬盘2：共享存储

挂载硬盘的命令操作如下（仅手动创建虚拟机的场景下需要执行，自动创建虚拟机场景下不需要执行）。

- 创建文件夹，以/var/lib/docker 为例。

  ```
  mkdir /var/lib/docker
  ```

- 初始化为 ext4 格式。

  ```
  mkfs.ext4 /dev/vdb
  mkfs.ext4 /dev/vdc
  ```

- 查询磁盘 uuid。

  ```
  [root@moban-beifen ~]# blkid
  /dev/vda1: UUID="5f22d8be-50f7-4e78-a432-d6cdf7372a6b" TYPE="xfs"
  /dev/vdb: UUID="6fa68703-2c53-43c5-8b29-d07b839f3fd5" TYPE="ext4"
  /dev/vdc: UUID="fd19f203-8b76-4bfd-b359-25a166efbc61" TYPE="ext4"
  ```

- 添加配置。

```
[root@moban-beifen ~]# cat /etc/fstab

#
# /etc/fstab
# Created by anaconda on Wed May 13 13:45:41 2020
#
# Accessible filesystems, by reference, are maintained under '/dev/disk'
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info
#
UUID=5f22d8be-50f7-4e78-a432-d6cdf7372a6b /                       xfs     defaults        0 0
UUID=6fa68703-2c53-43c5-8b29-d07b839f3fd5 /var/lib/docker     ext4 defaults 0 0
UUID=fd19f203-8b76-4bfd-b359-25a166efbc61 /var/log ext4 defaults 0 0
```

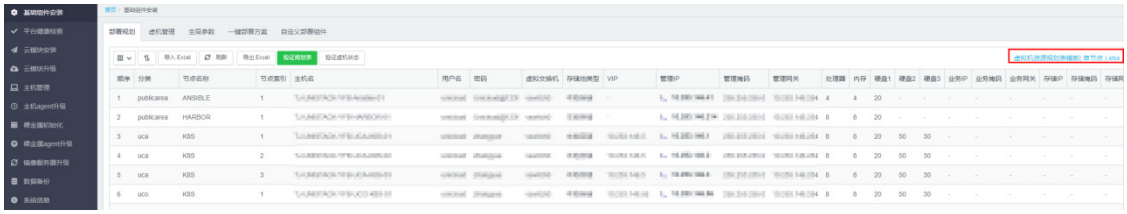
- 挂载文件系统。

  ```
  mount -a
  ```

2. 配置虚拟机资源规划表

(1) 选择[基础组件安装/部署规划]菜单项，点击“虚拟机资源规划表模板.xlsx”，下载到本地。

图5-2 下载虚拟机资源规划表模板



(2) 根据《虚拟机资源规划表模板》各列对基础组件进行规划，并将实际的虚拟机规划信息填写到规划表中。

注意

修改虚拟机资源规划表时:

- “顺序编号、分类、节点名称、节点索引”这几列为系统字段，禁止修改其中的内容。对应图 5-4 中的“区域 1”。
- “处理器、内存、硬盘 1、硬盘 2、硬盘 3”这几列的值为推荐配置，在生产环境中必须保证能满足系统配置的要求。对应图 5-4 中的“区域 4”。特殊配置要求请参考“1. 基础组件部署要求”。
- 区域 1 和区域 4 中的字段值会影响到部署成功与否，以及其他系统调用部署工具的 API 的结果，请务必关注。
- 请根据实际情况修改主机名、存储池类型、VIP、管理 IP、管理掩码和管理网关。对应图 5-4 中的“区域 2”和“区域 3”。存储的配置要求请参考“1. 基础组件部署要求”。

图5-3 填写虚拟机规划信息

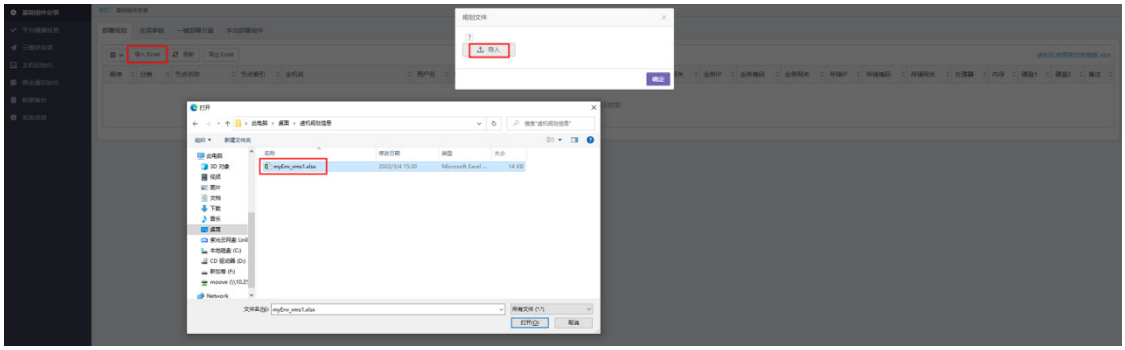
顺序编号	分类	节点名称	节点索引	主机名	用户名	密码	虚拟交换机	存储池类型	VIP	管理IP	管理掩码	管理网关	处理器	内存	硬盘1	硬盘2	硬盘3
1	publicarea	ANSIBLE	1	AUTOPS-ANSIBLE-01	root	unicloud	vswitch0	本地存储		192.168.10.102	255.255.255.0	192.168.10.254	4	4	100		
2	publicarea	HARBOR	1	AUTOPS-HARBOR-01	root	unicloud	vswitch0	本地存储		192.168.10.10	255.255.255.0	192.168.10.254	8	16	100	200	
3	uca	K8S	1	AUTOPS-UCA-K8S-01	root	unicloud	vswitch0	本地存储	192.168.10.81	192.168.10.11	255.255.255.0	192.168.10.254	64	100	100	500	300
4	uca	K8S	2	AUTOPS-UCA-K8S-02	root	unicloud	vswitch0	本地存储	192.168.10.81	192.168.10.12	255.255.255.0	192.168.10.254	64	100	100	500	300
5	uca	K8S	3	AUTOPS-UCA-K8S-03	root	unicloud	vswitch0	本地存储	192.168.10.81	192.168.10.13	255.255.255.0	192.168.10.254	64	100	100	500	300
6	uco	K8S	1	AUTOPS-UCO-K8S-01	root	unicloud	vswitch0	本地存储	192.168.10.82	192.168.10.14	255.255.255.0	192.168.10.254	64	128	100	500	300
7	uco	K8S	2	AUTOPS-UCO-K8S-02	root	unicloud	vswitch0	本地存储	192.168.10.82	192.168.10.15	255.255.255.0	192.168.10.254	64	128	100	500	300
8	uco	K8S	3	AUTOPS-UCO-K8S-03	root	unicloud	vswitch0	本地存储	192.168.10.82	192.168.10.16	255.255.255.0	192.168.10.254	64	128	100	500	300
9	taag	K8S	1	AUTOPS-TAAG-K8S-01	root	unicloud	vswitch0	本地存储	192.168.10.83	192.168.10.17	255.255.255.0	192.168.10.254	8	16	100	500	300
10	taag	K8S	2	AUTOPS-TAAG-K8S-02	root	unicloud	vswitch0	本地存储	192.168.10.83	192.168.10.18	255.255.255.0	192.168.10.254	8	16	100	500	300
11	taag	K8S	3	AUTOPS-TAAG-K8S-03	root	unicloud	vswitch0	本地存储	192.168.10.83	192.168.10.19	255.255.255.0	192.168.10.254	8	16	100	500	300
12	dmz	K8S	1	AUTOPS-DMZ-K8S-01	root	unicloud	vswitch0	本地存储	192.168.10.84	192.168.10.20	255.255.255.0	192.168.1.254	8	8	100	500	300
13	dmz	K8S	2	AUTOPS-DMZ-K8S-02	root	unicloud	vswitch0	本地存储	192.168.10.84	192.168.10.21	255.255.255.0	192.168.1.254	8	8	100	500	300
14	dmz	K8S	3	AUTOPS-DMZ-K8S-03	root	unicloud	vswitch0	本地存储	192.168.10.84	192.168.10.22	255.255.255.0	192.168.1.254	8	8	100	500	300
15	omc	K8S	1	AUTOPS-OMC-K8S-01	root	unicloud	vswitch0	本地存储	192.168.10.85	192.168.10.23	255.255.255.0	192.168.10.254	16	64	100	500	300
16	omc	K8S	2	AUTOPS-OMC-K8S-02	root	unicloud	vswitch0	本地存储	192.168.10.85	192.168.10.24	255.255.255.0	192.168.10.254	16	64	100	500	300
17	omc	K8S	3	AUTOPS-OMC-K8S-03	root	unicloud	vswitch0	本地存储	192.168.10.85	192.168.10.25	255.255.255.0	192.168.10.254	16	64	100	500	300
18	publicarea	MYSQL	1	AUTOPS-UCA-MYSQL-01	root	unicloud	vswitch0	本地存储	192.168.10.86	192.168.10.26	255.255.255.0	192.168.10.254	16	32	100	500	
19	publicarea	MYSQL	2	AUTOPS-UCA-MYSQL-02	root	unicloud	vswitch0	本地存储	192.168.10.86	192.168.10.27	255.255.255.0	192.168.10.254	16	32	100	500	
20	publicarea	MYSQL	3	AUTOPS-UCA-MYSQL-03	root	unicloud	vswitch0	本地存储	192.168.10.86	192.168.10.28	255.255.255.0	192.168.10.254	16	32	100	500	
21	publicarea	MYSQLREPM	1	AUTOPS-UCA-MYSQL-REPM-MANAGER	root	unicloud	vswitch0	本地存储		192.168.10.29	255.255.255.0	192.168.10.254	4	8	100		
22	publicarea	RABBITMQ	1	AUTOPS-RABBITMQ-01	root	unicloud	vswitch0	本地存储		192.168.10.30	255.255.255.0	192.168.10.254	8	16	100		
23	publicarea	RABBITMQ	2	AUTOPS-RABBITMQ-02	root	unicloud	vswitch0	本地存储		192.168.10.31	255.255.255.0	192.168.10.254	8	16	100		
24	publicarea	RABBITMQ	3	AUTOPS-RABBITMQ-03	root	unicloud	vswitch0	本地存储		192.168.10.32	255.255.255.0	192.168.10.254	8	16	100		
25	publicarea	REDIS	1	AUTOPS-REDIS-01	root	unicloud	vswitch0	本地存储	192.168.10.87	192.168.10.33	255.255.255.0	192.168.10.254	8	32	100		
26	publicarea	REDIS	2	AUTOPS-REDIS-02	root	unicloud	vswitch0	本地存储	192.168.10.87	192.168.10.34	255.255.255.0	192.168.10.254	8	32	100		
27	publicarea	REDIS	3	AUTOPS-REDIS-03	root	unicloud	vswitch0	本地存储	192.168.10.87	192.168.10.35	255.255.255.0	192.168.10.254	8	32	100		
28	publicarea	ZOOKEEPER	1	AUTOPS-UCA-ZOOKEEPER-01	root	unicloud	vswitch0	本地存储		192.168.10.36	255.255.255.0	192.168.10.254	16	32	100		
29	publicarea	ZOOKEEPER	2	AUTOPS-UCA-ZOOKEEPER-02	root	unicloud	vswitch0	本地存储		192.168.10.37	255.255.255.0	192.168.10.254	16	32	100		
30	publicarea	ZOOKEEPER	3	AUTOPS-UCA-ZOOKEEPER-03	root	unicloud	vswitch0	本地存储		192.168.10.38	255.255.255.0	192.168.10.254	16	32	100		
31	publicarea	KAFKA	1	AUTOPS-UCA-KAFKA-01	root	unicloud	vswitch0	本地存储		192.168.10.39	255.255.255.0	192.168.10.254	16	32	100		
32	publicarea	KAFKA	2	AUTOPS-UCA-KAFKA-02	root	unicloud	vswitch0	本地存储		192.168.10.40	255.255.255.0	192.168.10.254	16	32	100		
33	publicarea	KAFKA	3	AUTOPS-UCA-KAFKA-03	root	unicloud	vswitch0	本地存储		192.168.10.41	255.255.255.0	192.168.10.254	16	32	100		
34	publicarea	PROMETHEUS	1	AUTOPS-OP-PMS-01	root	unicloud	vswitch0	本地存储		192.168.10.42	255.255.255.0	192.168.10.254	16	32	100	300	
35	publicarea	PGSQL	1	AUTOPS-PGSQL-01	root	unicloud	vswitch0	本地存储	192.168.10.88	192.168.10.43	255.255.255.0	192.168.10.254	4	8	100		
36	publicarea	PGSQL	2	AUTOPS-PGSQL-02	root	unicloud	vswitch0	本地存储	192.168.10.88	192.168.10.44	255.255.255.0	192.168.10.254	4	8	100		
37	publicarea	PGSQL	3	AUTOPS-PGSQL-03	root	unicloud	vswitch0	本地存储	192.168.10.88	192.168.10.45	255.255.255.0	192.168.10.254	4	8	100		
38	publicarea	NGINX	1	AUTOPS-NGINX-01	root	unicloud	vswitch0	本地存储	192.168.10.89	192.168.10.46	255.255.255.0	192.168.10.254	4	8	100		
39	publicarea	NGINX	2	AUTOPS-NGINX-02	root	unicloud	vswitch0	本地存储	192.168.10.89	192.168.10.47	255.255.255.0	192.168.10.254	4	8	100		
40	publicarea	IMAGESERVER	1	AUTOPS-IMAGE-SERVER-01	root	unicloud	vswitch0	本地存储		192.168.10.48	255.255.255.0	192.168.10.254	8	16	100	500	
41	publicarea	IMAGESERVER	2	AUTOPS-IMAGE-SERVER-02	root	unicloud	vswitch0	本地存储		192.168.10.49	255.255.255.0	192.168.10.254	8	16	100	500	
42	publicarea	IMAGESERVER	3	AUTOPS-IMAGE-SERVER-03	root	unicloud	vswitch0	本地存储		192.168.10.50	255.255.255.0	192.168.10.254	8	16	100	500	
43	publicarea	TFTP	1	AUTOPS-TFTPSERVER-01	root	unicloud	vswitch0	本地存储		192.168.10.51	255.255.255.0	192.168.10.254	4	4	100		
44	publicarea	ELASTICSEARCH1	1	AUTOPS-OMCBASE-ES-01	root	unicloud	vswitch0	本地存储		192.168.10.52	255.255.255.0	192.168.10.254	16	32	100	500	
45	publicarea	ELASTICSEARCH1	2	AUTOPS-OMCBASE-ES-02	root	unicloud	vswitch0	本地存储		192.168.10.53	255.255.255.0	192.168.10.254	16	32	100	500	
46	publicarea	ELASTICSEARCH2	1	AUTOPS-OMCBASE-ES-03	root	unicloud	vswitch0	本地存储		192.168.10.54	255.255.255.0	192.168.10.254	16	32	100	500	
47	publicarea	ELASTICSEARCH2	2	AUTOPS-OMCBASE-ES-04	root	unicloud	vswitch0	本地存储		192.168.10.55	255.255.255.0	192.168.10.254	16	32	100	500	
48	publicarea	CASSANDRA1	1	AUTOPS-OMCBASE-CASS-01	root	unicloud	vswitch0	本地存储		192.168.10.56	255.255.255.0	192.168.10.254	16	16	100	200	
49	publicarea	CASSANDRA1	2	AUTOPS-OMCBASE-CASS-02	root	unicloud	vswitch0	本地存储		192.168.10.57	255.255.255.0	192.168.10.254	16	16	100	200	
50	publicarea	CASSANDRA2	1	AUTOPS-OMCBASE-CASS-03	root	unicloud	vswitch0	本地存储		192.168.10.58	255.255.255.0	192.168.10.254	16	16	100	200	
51	publicarea	CASSANDRA2	2	AUTOPS-OMCBASE-CASS-04	root	unicloud	vswitch0	本地存储		192.168.10.59	255.255.255.0	192.168.10.254	16	16	100	200	
52	publicarea	GITLAB	1	AUTOPS-OMCBASE-GITLAB-01	root	unicloud	vswitch0	本地存储		192.168.10.60	255.255.255.0	192.168.10.254	4	8	100	300	

区域1　区域2　区域3　区域4

(3) 填写完成后修改规划表的名称，本节以“myEnv_vms1.xlsx”为例。

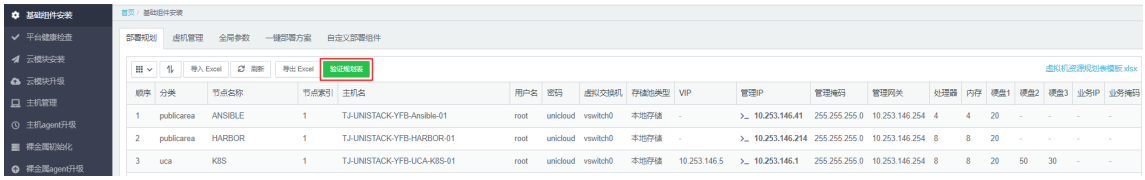
(4) 点击<导入>按钮，将填写好的“myEnv_vms1.xlsx”文件导入 Rebirth 工具。

图5-4 导入“myEnv_vms1.xlsx”



(5) 实际的虚拟机信息即呈现在 Rebirh 工具平台上。

(6) 点击<验证规划表>按钮，对规划表进行验证，包括填写是否正确、IP 地址是否被占用等。请务必在验证通过后，再进行后续操作。



5.2.3 自动创建虚拟机

通过自动创建虚拟机功能，可以实现在 Usphere 管理平台中自动创建管理区的虚拟机。如不使用该功能，则需要在 Usphere 管理平台中手工创建。

在界面输入对应信息后，部署工具会连接到 Usphere 管理平台，并按照“2. 配置虚拟机资源规划表”中设置的虚拟机规格，完成创建虚拟机、分配硬盘容量空间以及挂载硬盘的操作。

1. Usphere 中配置 VKS 和虚拟机

(1) 登录 Usphere 管理平台，将 VKS 放置到同一个主机池中。

(2) 创建虚拟机模板

a. 登录 Usphere 管理平台，选择任何一台 VKS，按照如下规格创建一台虚拟机。

- CPU 个数为 1，核数为 1
- 内存为 1GB
- 存储卷镜像：

  vda：使用标准镜像文件_基础组件运行虚拟机镜像，例如 0801_TEMPL0506STD.qcow2，容量为 100GB

  vdb：新建存储卷，容量为 10GB

  vdc：新建存储卷，容量为 10GB

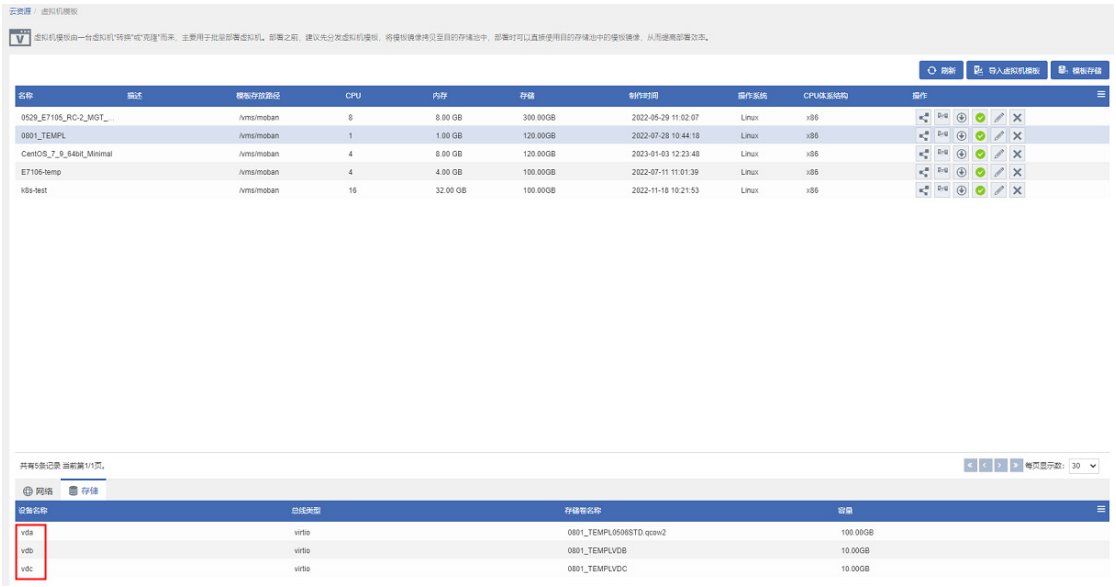
b. 将虚拟机安全关闭。

c. 在导航栏中，右键单击该虚机，选择<转换为模板>，将虚拟机配置保存为模板。

d. 在导航栏中选择[云资源/虚拟机模板]，查看虚拟机模板。

查看虚拟机模板如下。

确认虚机模板的磁盘顺序，确保顺序为 vda、vdb、vdc。



(3) 创建 VKS 存储池：进入 VKS 管理页面，创建对应的本地存储和共享存储的存储池。

主机池下的所有 VKS 都需要创建本地存储池和共享存储池。

(4) 指定虚拟交换机：进入 VKS 管理页面，指定虚拟交换机。

主机池下的所有 VKS 都需要指定虚拟交换机。

2. 部署工具中自动创建虚拟机

(1) 在部署工具中，选择[基础组件安装/虚机管理]菜单项，填写虚机管理参数。

参数说明如下。

参数	说明
CAS主机地址	输入Usphere管理平台的登录IP地址。
CAS主机端口	输入Usphere管理平台的登录端口号。
CAS登录账号	输入登录Usphere管理平台的账号。
CAS登录密码	输入登录Usphere管理平台的密码。
CAS主机池名称	输入Usphere管理平台中创建的主机池的名称。参见“1. Usphere中配置VKS和虚拟机”中的配置。
CAS集群名称	输入Usphere管理平台中VKS所在集群名称。参见“1. Usphere中配置VKS和虚拟机”中的配置。
虚机模板名称	输入Usphere管理平台中创建的虚机模板名称，参见“1. (2)创建虚拟机模板”中的配置。
本地存储名称	输入Usphere管理平台中创建的本地存储名称，参见“1. (3)创建VKS存储池”中的配置。
共享存储池名称	输入Usphere管理平台中创建的本地存储名称，参见“1. (3)创建VKS存储池”中的配置。
虚拟交换机	输入Usphere管理平台中虚拟交换机名称，参见“1. (4)指定虚拟交换机”中的配置。

(2) 填写完成后，点击<保存设置>按钮，并点击<创建虚机>按钮，开始创建虚拟机。虚机创建过程中，不能关闭弹框。

虚机创建完成后，请单击<验证虚机状态>按钮，校验虚机状态。

请在虚拟机创建完成后，再进行后续操作。

3. DMZ 区自动创建虚拟机说明

由于 DMZ 区位于公共服务区，当云平台中存在 DMZ 区域时，需要将管理区虚拟机和 DMZ 区的虚拟机分开创建，分别进行两次主机规划和自动创建虚拟机的操作。具体步骤如下：

(1) 在部署规划页面，导入除 DMZ 区之外的其它虚拟机信息。

(2) 按照上述步骤创建除 DMZ 区之外的其它虚拟机。

(3) 在部署规划页面，导入 Ansible 和 DMZ 区虚拟机信息。

(4) 按照上述步骤创建 DMZ 区的虚拟机。

(5) 创建完成后根据需要修改虚拟机的网络策略模板。

(6) 虚拟机都创建完成后，在部署规划页面，重新导入所有虚拟机信息。

DMZ 区虚拟机创建完成后，如果管理网不可达，导致后续虚拟机磁盘配置会失败，请根据需要手动修改虚拟机的网络策略模板和虚拟机磁盘配置。

5.2.4 设置基础组件全局参数

(1) 选择[基础组件安装/全局参数]菜单项，根据实际情况配置基础组件全局参数。标*为必填信息，未标*为非必填信息，灰色填充为不可修改信息。

图5-5 基础组件全局参数设置页面

参数说明：

参数	说明
ansible主机IP	即Rebirth工具虚拟机的IP地址，系统自动填写。
ansible账号/ansible密码	即登录Rebirth工具虚拟机的账号和密码，系统自动填写。
节点信息	填写节点名称。
region值	填写Region的英文名称。
az值	填写AZ的英文名称。
授时服务器类型	时钟同步服务器的类型，系统自动填写。
授时服务器地址	时钟同步服务器的IP地址。如果有自己的授时服务器，则可按照实际信息填写，如果没有，则填写Rebirth工具主机IP地址。

(2) 填写完成后，点击<保存>按钮。

5.2.5 一键部署方案

基础组件部署可以选择一键部署方案和自定义部署组件两种方式。一键部署方案会将所有组件一次部署完毕，通常用于首次全量部署，而不适用于缺少某些组件的环境。

说明

一键部署方案目前仅支持单 Region 单 AZ 环境。

(1) 选择[基础组件安装/一键部署方案]菜单项，进入一键部署方案页面。

图5-6 一键部署页面

(2) 点击<开始部署>按钮，即可对所有组件进行安装。

5.2.6 （可选）自定义部署组件

基础组件部署可以选择一键部署方案和自定义部署组件两种方式。自定义部署通常用于选择性部署某些组件（例如有些 AZ 中不需要部署全量组件）；或者当某个组件部署失败后，后续组件使用自定义部署等情况。请根据实际情况进行部署。

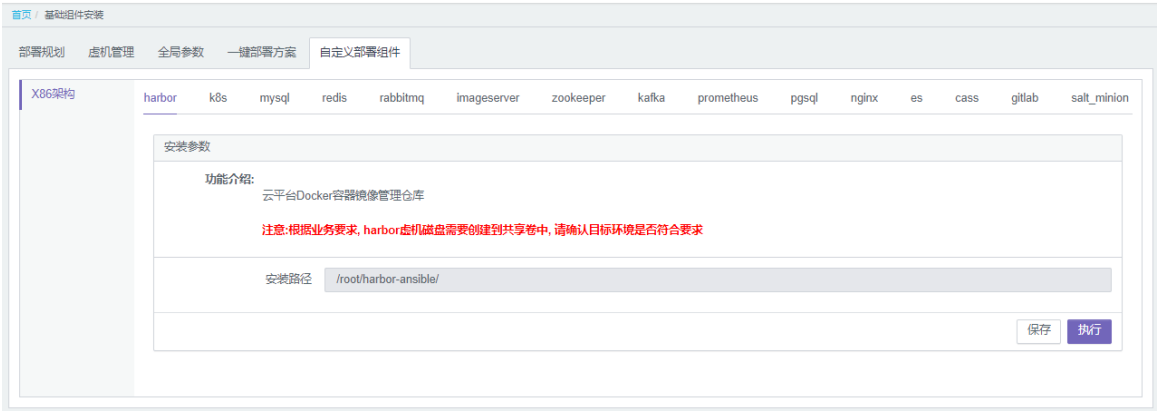
说明

- 组件安装部署过程中，弹框不可关闭，PC 不可以断网。
- 部署集群时，K8S 组件 uca、uco、taag、omc、dmz 不允许并行部署，Kafka 需要在 Zookeeper 后部署，其他组件的部署没有前后顺序要求，可以并行部署。
- 若部署过程中，部署页面出现 failed=1，说明部署失败，请查看并解决部署失败原因后，重新部署。
- **自定义部署组件前，请参考“10.1 备份准备”章节，完成目录挂载。若不进行目录挂载，会导致数据备份时备份失败。**

1. Harbor 组件

(1) 选择[基础组件安装/手动部署组件/harbor]菜单项，进入 Harbor 组件安装页面。

图5-7 Harbor 组件安装页面



(2) 单击<执行>按钮，执行自动化部署流程。

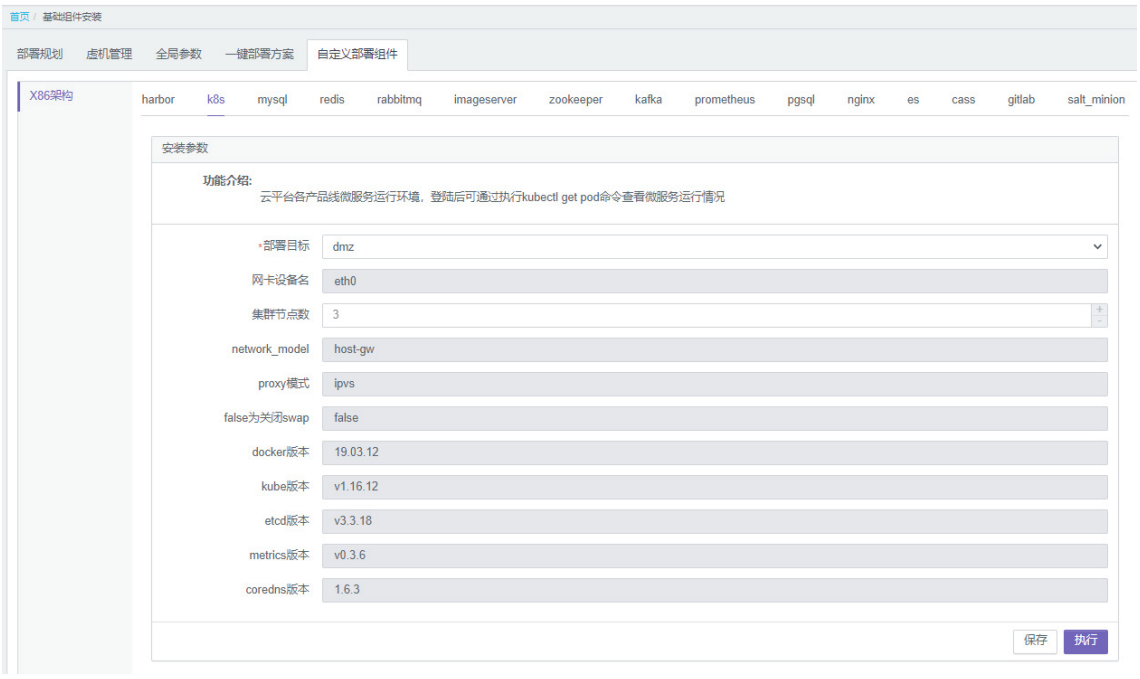
(3) 自动化部署完成后，单击<关闭>按钮。

2. K8S 组件安装

在 uca、uco、taag（租管互通）、omc 和 dmz 上都需要安装 K8S 组件，请按照 uca、uco、taag、omc、dmz 的顺序依次安装。如下步骤以 uca 为例，其余模块的安装方法与 uca 相同。

(1) 选择[基础组件安装/手动部署组件/k8s]菜单项，进入 K8S 组件安装页面，并按照页面提示配置参数。

图5-8 K8S 组件安装页面



参数说明：

参数	说明
部署目标	可选择uca、uco、taag、omc、dmz，请按照uca、uco、taag、omc、dmz的顺

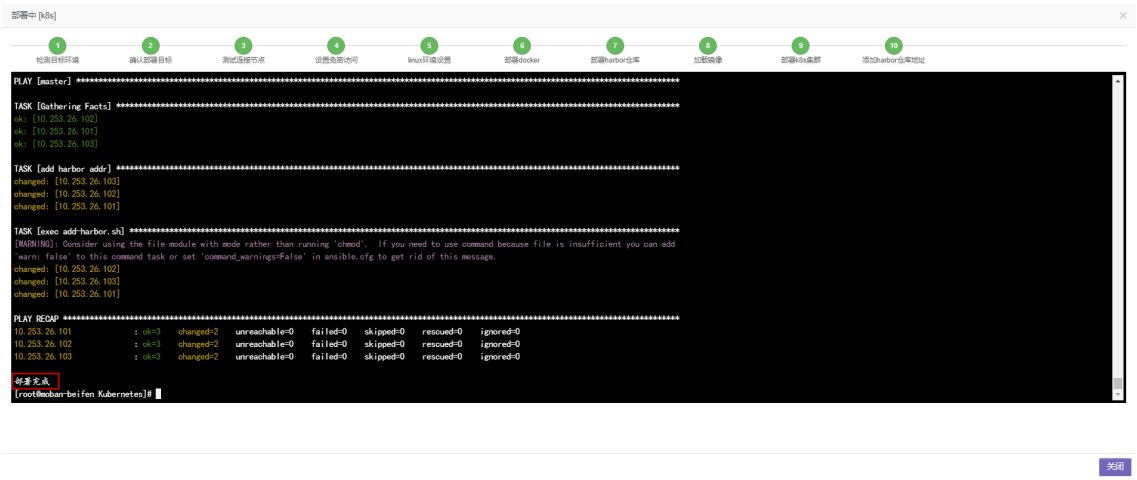
	序依次完成部署。
网卡设备名	配置网卡信息，一般默认eth0。
集群节点数	集群的节点数量。
network_model	网络模式。
proxy模式	代理模式。
false为关闭swap	关闭SWAP内存。

(2) 填写完成后，单击<保存>按钮。

(3) 单击<执行>按钮，执行自动化部署流程。

(4) 自动化部署流程执行完成后，将出现如下图所示界面，单击<关闭>按钮。

图5-9 K8S 组件安装完成界面

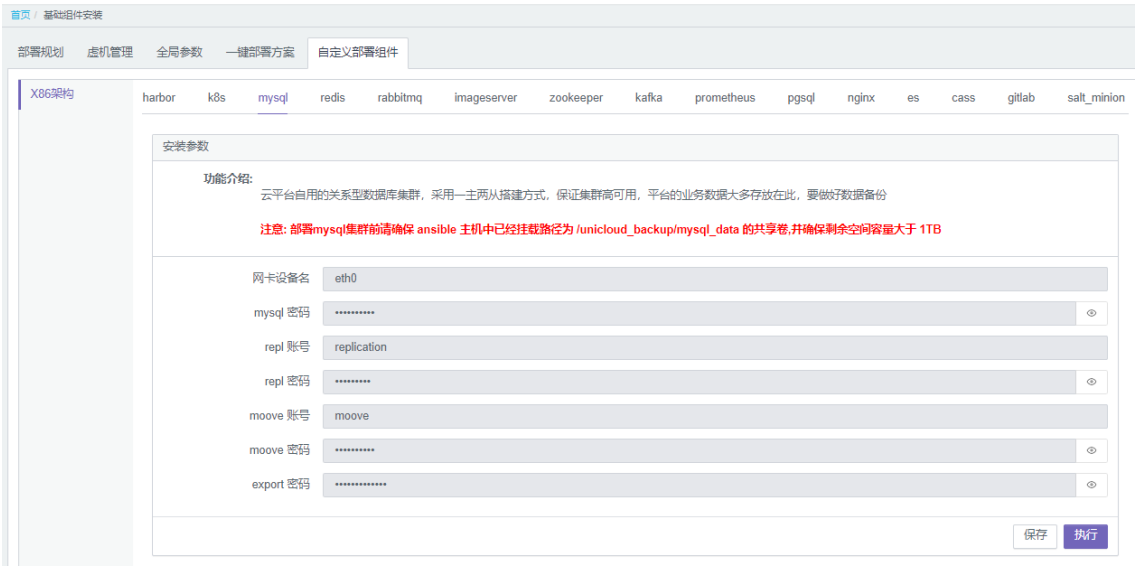


(5) 重复以上步骤，依次完成 uca、uco、taag、omc、dmz 的 K8S 组件安装。

3. MySQL 组件安装

(1) 选择[基础组件安装/手动部署组件/mysql]菜单项，进入 MySQL 组件安装页面。

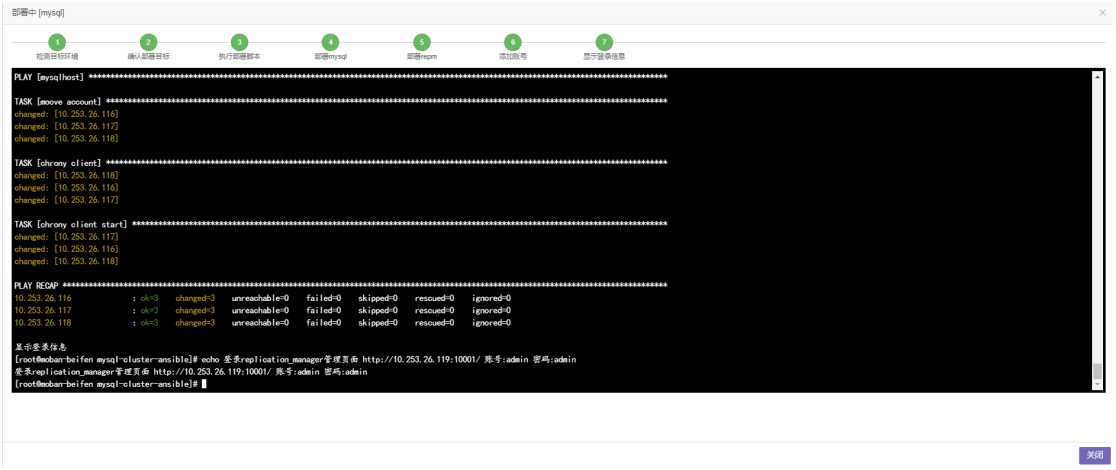
图5-10 MySQL 组件安装页面



(2) 单击<执行>按钮，执行自动化部署流程。

(3) 部署流程执行完成后将出现如图 5-12 所示页面，单击<关闭>按钮。

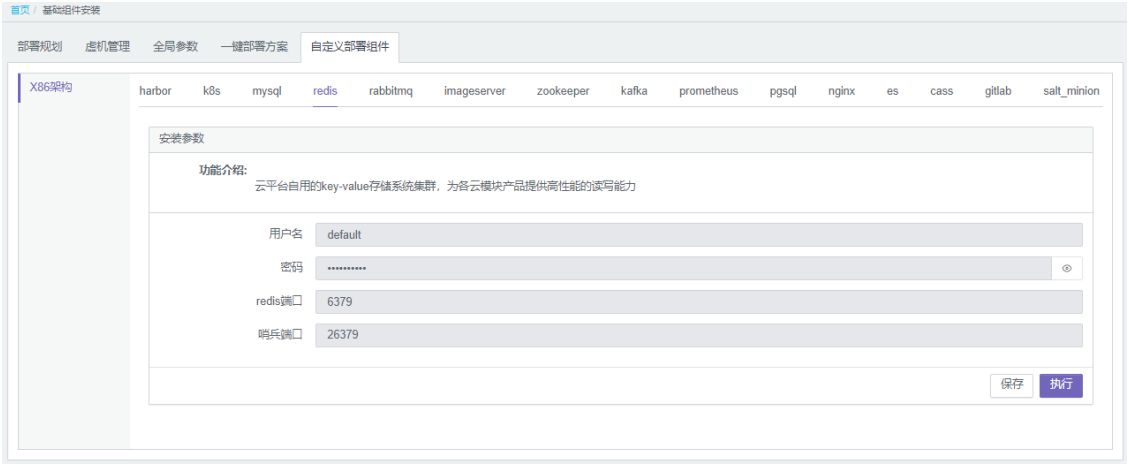
图5-11 MySQL 组件安装完成界面



4. Redis 组件安装

(1) 选择[基础组件安装/手动部署组件/redis]菜单项，进入 Redis 组件安装页面。

图5-12 Redis 组件安装页面



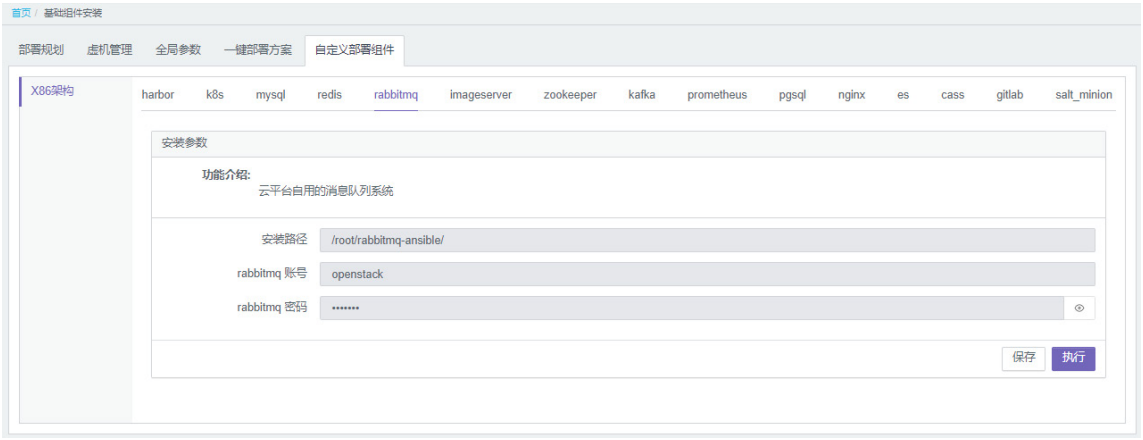
(2) 单击<执行>按钮，执行自动化部署流程。

(3) 自动化部署完成后，单击<关闭>按钮。

5. RabbitMQ 组件安装

(1) 选择[基础组件安装/手动部署组件/rabbitmq]菜单项，进入 RabbitMQ 组件安装页面。

图5-13 RabbitMQ 组件安装页面



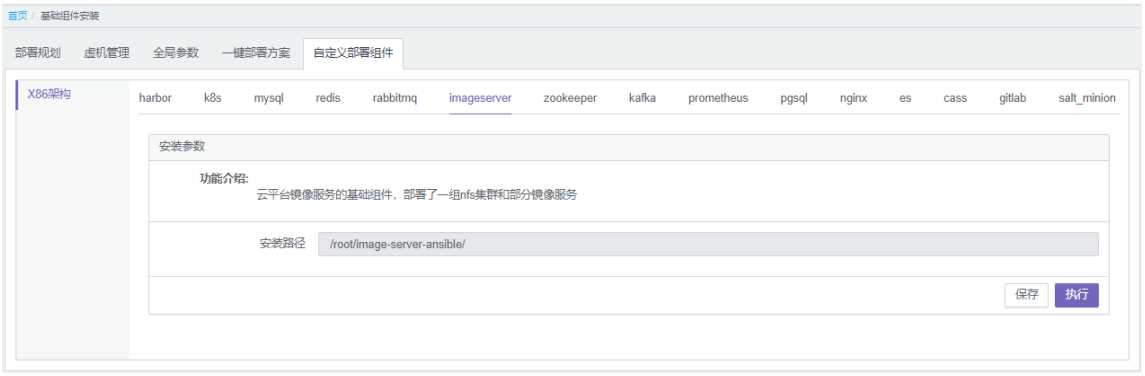
(2) 单击<执行>按钮，执行自动化部署流程。

(3) 自动化部署完成后，单击<关闭>按钮。

6. imageserver 组件安装

(1) 选择[基础组件安装/手动部署组件/imageserver]，进入 imageserver 组件安装页面。

图5-14 imageserver 组件安装页面



(2) 单击<执行>按钮，执行自动化部署流程。

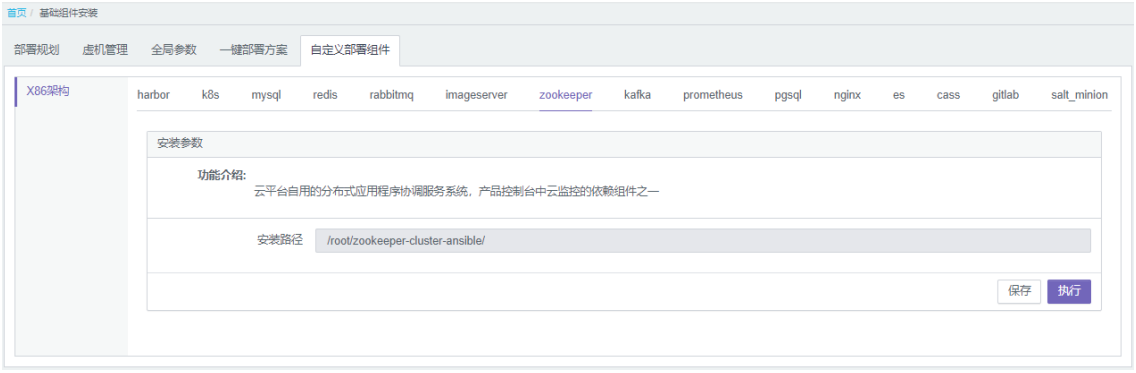
(3) 自动化部署完成后，单击<关闭>按钮。

7. Zookeeper、Kafka、Prometheus 组件安装

Zookeeper、Kafka 和 Prometheus 组件的安装方式完全相同，本节将以 Zookeeper 组件为例介绍。

(1) 选择[基础组件安装/手动部署组件/zookeeper]，进入 Zookeeper 组件安装页面。

图5-15 Zookeeper 组件安装页面



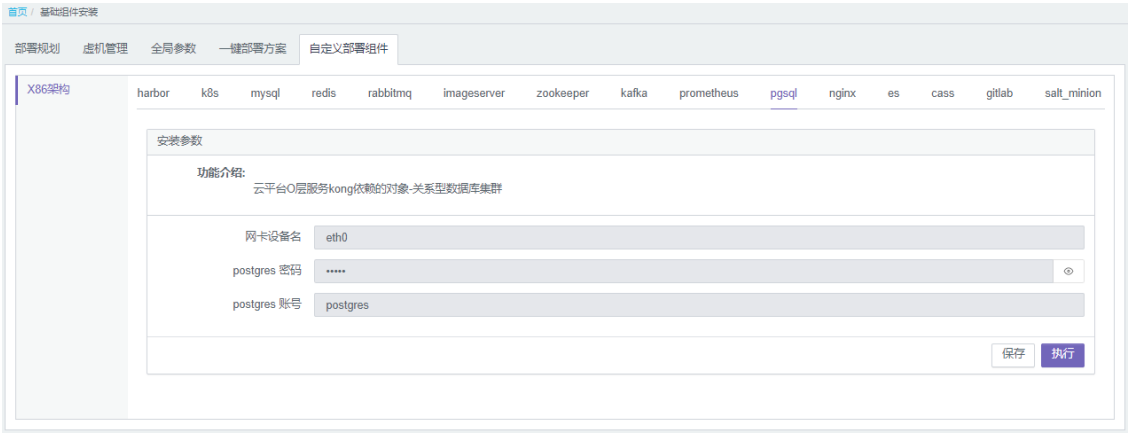
(2) 单击<执行>按钮，执行自动化部署流程。

(3) 自动化部署完成后，单击<关闭>按钮。

8. PostgreSQL 组件安装

(1) 选择[基础组件安装/手动部署组件/pgsql]菜单项，进入 PostgreSQL 组件安装页面。

图5-16 PostgreSQL 组件安装页面



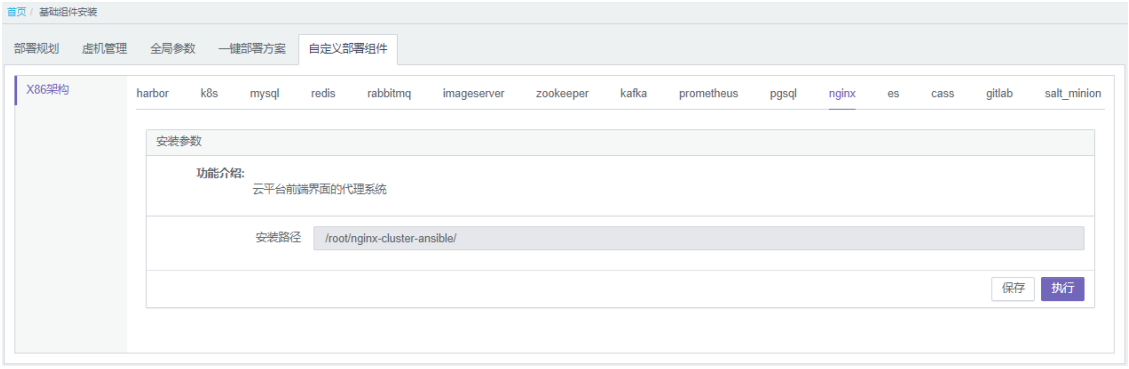
(2) 单击<执行>按钮，执行自动化部署流程。

(3) 自动化部署完成后，单击<关闭>按钮。

9. Nginx 组件安装

(1) 选择[基础组件安装/手动部署组件/nginx]菜单项，进入 Nginx 组件安装页面。

图5-17 Nginx 组件安装页面



(2) 单击<执行>按钮，执行自动化部署流程。

(3) 自动化部署完成后，单击<关闭>按钮。

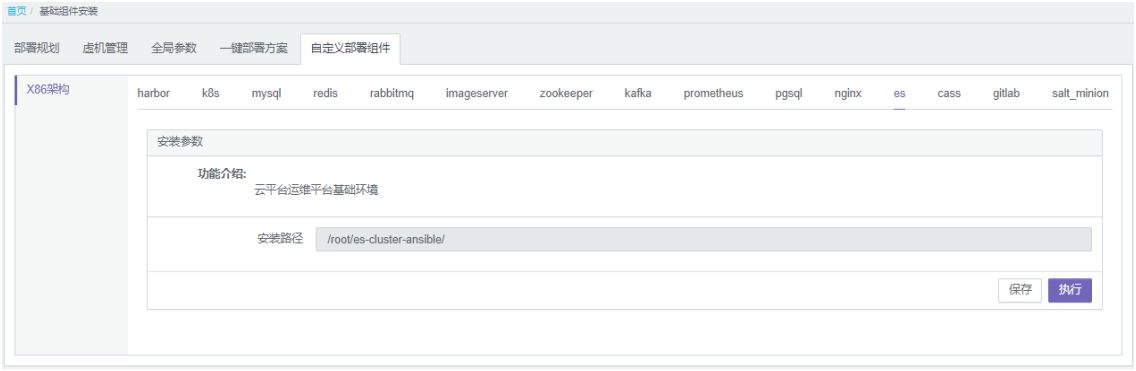
10. OMC_base 组件安装

OMC_base 组件包括 ElasticSearch、Cassandra 和 Gitlab 组件。组件安装顺序不分先后，请分别进行安装。

安装前，请参考“1. 基础组件部署要求”中要求的规格信息进行检查，确保虚拟机规格无误。

(1) 分别选择[基础组件安装/手动部署组件/es]、[基础组件安装/手动部署组件/cass]、[基础组件安装/手动部署组件/gitlab]菜单项，进入组件安装页面。下图以 es 页面为例。

图5-18 OMC_base 组件安装页面



(2) 单击<执行>按钮，执行自动化部署流程。

(3) 自动化部署完成后，单击<关闭>按钮。

5.2.7 公共手动操作

基础组件一键部署或自定义部署后，需要执行如下手动操作。

1. 为镜像服务器安装 SDS 客户端

目前有两个 SDS 版本，请参考 CloudOS7.0 的版本说明书获取对应版本的 client 安装包，安装当前 AZ 部署的 SDS 集群对应的 client 版本。以 SDS 3xxxx 版本进行举例。

(1) 在 Usphere 上对 3 台 imagesever 主机添加第二块网卡，IP 地址设置为相对应规划表中的存储地址。注意添加时不填写网关，只填写 IP 地址和掩码。

(2) 登录 3 台 imagesever 主机，ping 通存储网关，确保可以 ping 通。

(3) 将 SDS 软件包拷贝到每台 imagesever 主机的/opt/目录下。

(4) 解压 SDS 软件包。

```
tar -zxvf SDS 软件包名称
```

(5) 安装 SDS 客户端。

```
cd ceph_client_rpm/
sh install_ceph_client.sh
```

(6) 拷贝 SDS 的配置文件到所有 imagesever 主机上。

a. 登录 SDS 服务器，确认 ceph.conf 和 ceph.client.admin.keyring 文件存在。

b. 拷贝配置文件。

```
#fsid=$(grep fsid /etc/ceph/ceph.conf | awk -F'= ' '{print $NF}')
#cp /etc/ceph/ceph.conf /tmp/$fsid.conf
#cp /etc/ceph/ceph.client.admin.keyring /tmp/$fsid.keyring
#ll /tmp/$fsid.*
-rw-r--r-- 1 SDS_Admin root 2218 Dec 24 15:35
/tmp/eea733ef-98b2-404c-807b-a16149e2487e.conf
-rw-r--r-- 1 SDS_Admin root   63 Dec 24 15:35
/tmp/eea733ef-98b2-404c-807b-a16149e2487e.keyring
#scp /tmp/$fsid.* root@10.254.7.3:/etc/onestor_client  //镜像服务器 IP 和密码请按照实际情况输入
```

c. 查看镜像服务器 SDS 集群配置类似如下：

```
# ll /etc/onestor_client
total 16
-rw-r--r-- 1 root root 1932 Dec 24 15:29 a338d222-9fd5-4530-9087-4c1cc272702a.conf
-rw-r--r-- 1 root root  63 Dec 24 15:29 a338d222-9fd5-4530-9087-4c1cc272702a.keyring
-rw-r--r-- 1 root root 2218 Dec 24 15:56 eea733ef-98b2-404c-807b-a16149e2487e.conf
-rw-r--r-- 1 root root  63 Dec 24 15:56 eea733ef-98b2-404c-807b-a16149e2487e.keyring
```

(7) 检查是否与 SDS 建立通信。

```
ceph -s
```

如发生配置文件无法找到等类似的问题，则使用如下命令：

```
ceph -c <conf 文件位置> -k <keyring 文件位置> -s
```

例如，当只有一套集群时，执行命令如下：

```
ceph -c /etc/onestor_client/ceph.conf -k
/etc/onestor_client/ceph.client.admin.keyring –s
```

2. 镜像服务器对接 SDS 集群

镜像服务器对接 SDS 集群时，需要在镜像服务器上配置 SDS 集群配置文件，为适配多套 SDS 集群，需要将不同的 SDS 集群配置文件以集群 fsid 作为标志，文件名称如下：fsid.conf、fsid.keyring。该配置适用于镜像服务器初始化场景、新增加 SDS 集群。

说明

- 多套 SDS 集群版本必须一致，不支持跨版本。
- 跨 AZ 迁移时，需要把 2 套 AZ 的存储配置文件（fsid.conf 和 fsid.keyring）都添加到镜像服务器中。

---

(1) SDS 集群创建 Fsid 配置文件

a. 登录 SDS 集群的 node 节点。

b. 拷贝 fsid.conf、fsid.keyring 配置文件。

```
fsid=$(grep fsid /etc/ceph/ceph.conf | awk -F'= ' '{print $NF}')
cp /etc/ceph/ceph.conf /tmp/$fsid.conf
cp /etc/ceph/ceph.client.admin.keyring /tmp/$fsid.keyring
ll /tmp/$fsid.*
-rw-r--r-- 1 SDS_Admin root 2218 Dec 24 15:35
/tmp/eea733ef-98b2-404c-807b-a16149e2487e.conf
-rw-r--r-- 1 SDS_Admin root   63 Dec 24 15:35
/tmp/eea733ef-98b2-404c-807b-a16149e2487e.keyring
```

(2) 镜像服务器配置 SDS 集群配置文件

a. 在 SDS 集群里执行如下命令，将 fsid.conf,fsid.keyring 复制到/etc/onestor_client 目录。

```
scp /tmp/$fsid.* root@10.254.7.3:/etc/onestor_client  //镜像服务器的 IP 地址、登录密码请按照实际情况输入
```

b. 查看多套 SDS 集群配置，例如如下回显为正常：

```
ll /etc/onestor_client
total 16
-rw-r--r-- 1 root root 1932 Dec 24 15:29 a338d222-9fd5-4530-9087-4c1cc272702a.conf
```

```
-rw-r--r-- 1 root root  63 Dec 24 15:29 a338d222-9fd5-4530-9087-4c1cc272702a.keyring
-rw-r--r-- 1 root root 2218 Dec 24 15:56 eea733ef-98b2-404c-807b-a16149e2487e.conf
-rw-r--r-- 1 root root  63 Dec 24 15:56 eea733ef-98b2-404c-807b-a16149e2487e.keyring
```

3. 添加 TAAG 集群业务网卡

(1) 租管互通 IP 网段配置

地址规划：

- 租管互通 IP 网段：100.100.0.0/18
- 地址池：100.100.1.0-100.100.15.254
- 网关：100.100.63.254
- 租管互通地址段（TAAG 集群节点业务网卡用）：100.100.0.0-100.100.0.254，掩码 18 位

示例参考如下，请在 Leaf 交换机上进行配置。

```
#

ip vpn-instance moove-manager
 route-distinguisher 5:901
 description PRE_confige_moove-manager
 #
 address-family ipv4
  vpn-target 0:901 5:901 import-extcommunity
  vpn-target 5:901 export-extcommunity
 #
 address-family evpn
  vpn-target 0:901 5:901 import-extcommunity
  vpn-target 5:901 export-extcommunity

interface Vsi-interface900
 description PRE_confige_VSI_Interface_900
 ip binding vpn-instance moove-manager
 ip address 100.100.63.254 255.255.192.0 sub
 mac-address fe54-00f6-cf41
 distributed-gateway local


interface Vsi-interface901
 description PRE_confige_901
 ip binding vpn-instance moove-manager
 l3-vni 901


# 其中 BGP 号请根据实际环境来填写。
  ip vpn-instance moove-manager
  #
  address-family ipv4 unicast
   balance 4
   network 100.100.0.0 255.255.192.0
   network 100.100.63.254 255.255.255.255
```

```
vsi CORE_AGENT_VSI_900
 gateway vsi-interface 900
 statistics enable
 arp suppression enable
 flooding disable all
 vxlan 900
 evpn encapsulation vxlan
  route-distinguisher auto
  vpn-target auto export-extcommunity
  vpn-target auto import-extcommunity
```

(2) 在 Usphere 上对管理物理主机配置添加虚拟交换机、增加网络策略模板 vlan id 为 900

(3) 在 Usphere 上对 TAAG 层 3 台 K8S 主机添加第二块网卡，选用租管互通地址段中的地址。例如：100.100.0.17~19/18

(4) 登录 3 台 K8S 主机，ping 租管互通网关 100.100.63.254，检查是否可以 ping 通。

(5) 配置 TAAG 层段主机 VIP，选用租管互通地址段中的地址。例如：100.100.0.20/18

(6) 在三台 TAAG 主机均进行如下操作：

a. 修改/etc/keepalived/keepalived.conf ，新增以下内容。

```
vrrp_instance nginx-vip {
state BACKUP
priority 101
interface eth1
virtual_router_id 48
advert_int 3
unicast_src_ip 100.100.0.18              //当前主机的 ip 地址
unicast_peer {
100.100.0.17                            //其他主机的 ip 地址
100.100.0.19                            //其他主机的 ip 地址
}
virtual_ipaddress {
100.100.0.20/18                        //虚 ip 地址，CloudOS 平台对接使用
}
track_script {
nginx-check
}
}
```

b. 重启 keepalived 服务。

```
systemctl restart keepalived
```

4. 设置开机启动 Nginx 服务

登录 Rebirth 虚机，执行如下命令，设置开机启动 nginx 服务。

```
cd /root/nginx-cluster-ansible && ansible -i inventory/hosts.ini all -m shell -a "systemctl enable nginx;systemctl enable nginx_exporter.service;systemctl enable nginx_vts_exporter;"
```

5.2.8 基础组件状态巡检

基础组件部署完毕后，需保证所有已部署的基础组件均为正常状态，才能进行云模块的部署。

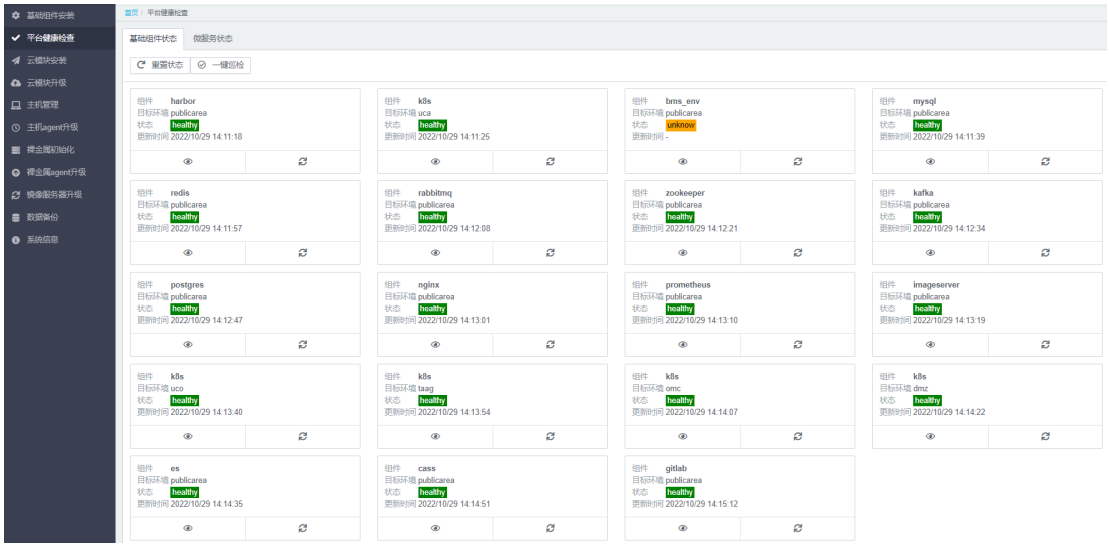
1. 巡检步骤

说明

基础组件巡检时，bms_env 还未部署，因此暂时不必关注其健康状态。

(1) 选择[平台健康检查/基础组件状态]菜单项，进入基础组件状态巡检页面。

图5-19 基础组件状态巡检页面



参数说明：

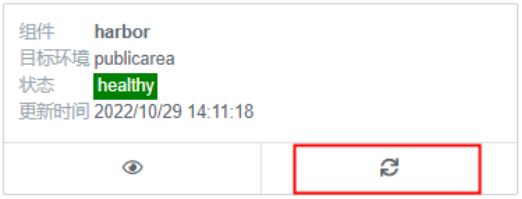
- Healthy 状态：组件已部署且状态正常。
- Unhealthy 状态：组件已部署但状态异常。
- Unknow 状态：组件未部署且状态未知。

(2) 在基础组件状态巡检页面单击<重置状态>按钮，可将基础组件状态重置为 Unknow。

图5-20 重置组件状态

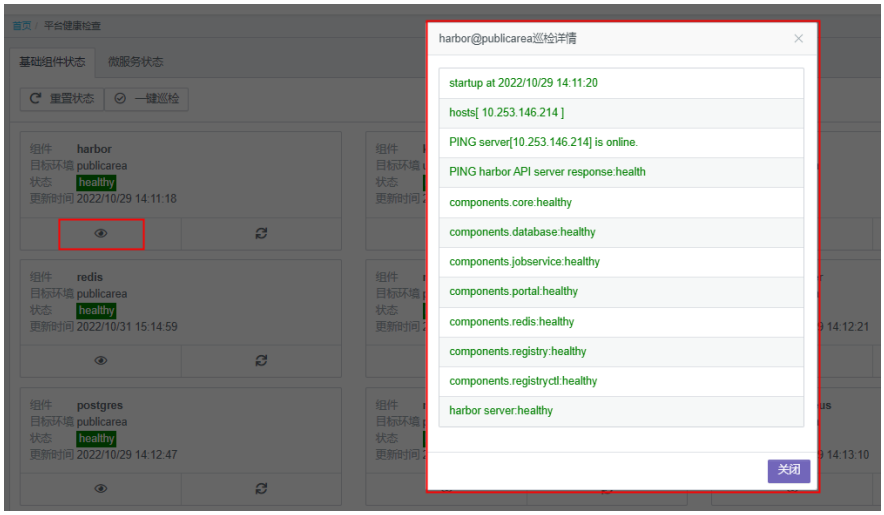
(3) 在基础组件状态巡检页面，单击组件右下角的<刷新>按钮，可刷新某个基础组件的状态。

图5-21 刷新组件状态



(4) 在基础组件状态巡检页面单击<查看>按钮，可查看当前组件状态的详细信息。组件详情包括组件启动的时间、组件所属主机的 IP 地址，组件所使用的 VIP 以及组件节点的状态是否正常。

图5-22 查看组件状态详细信息



2. 问题处理

如果巡检过程中，postgres 出现异常，提示如下：

```
[root@HZ-AZ1-PGSQL-02 ~]# systemctl status repmgr11.service -l
● repmgr11.service - A replication manager, and failover management tool for PostgreSQL
   Loaded: loaded (/usr/lib/systemd/system/repmgr11.service; enabled; vendor preset: disabled)
   Active: failed (Result: exit-code) since Fri 2022-12-09 21:57:23 CST; 11h ago

Dec 09 21:57:23 HZ-AZ1-PGSQL-02 systemd[1]: Starting A replication manager, and failover management tool for PostgreSQL...
Dec 09 21:57:23 HZ-AZ1-PGSQL-02 repmgrd[1137]: [2022-12-09 21:57:23] [NOTICE] using provided configuration file "/etc/repmgr/11/repmgr.conf"
Dec 09 21:57:23 HZ-AZ1-PGSQL-02 repmgrd[1137]: [2022-12-09 21:57:23] [NOTICE] redirecting logging output to "/var/log/repmgr/repmgrd.log"
Dec 09 21:57:23 HZ-AZ1-PGSQL-02 systemd[1]: Can't open PID file /run/repmgr/repmgrd-11.pid (yet?) after start: No such file or directory
Dec 09 21:57:23 HZ-AZ1-PGSQL-02 systemd[1]: Started A replication manager, and failover management tool for PostgreSQL.
Dec 09 21:57:23 HZ-AZ1-PGSQL-02 systemd[1]: repmgr11.service: control process exited, code=exited status=1
Dec 09 21:57:23 HZ-AZ1-PGSQL-02 systemd[1]: Unit repmgr11.service entered failed state.
Dec 09 21:57:23 HZ-AZ1-PGSQL-02 systemd[1]: repmgr11.service failed.
[root@HZ-AZ1-PGSQL-02 ~]#
```

请通过如下方法进行规避处理：

从另外两个节点拷贝/run/repmgr/repmgrd-11.pid 进程，注意使用 postgres 用户拷贝，拷贝完成后重启 systemctl restart repmgr11 服务，重启后重新进行巡检。

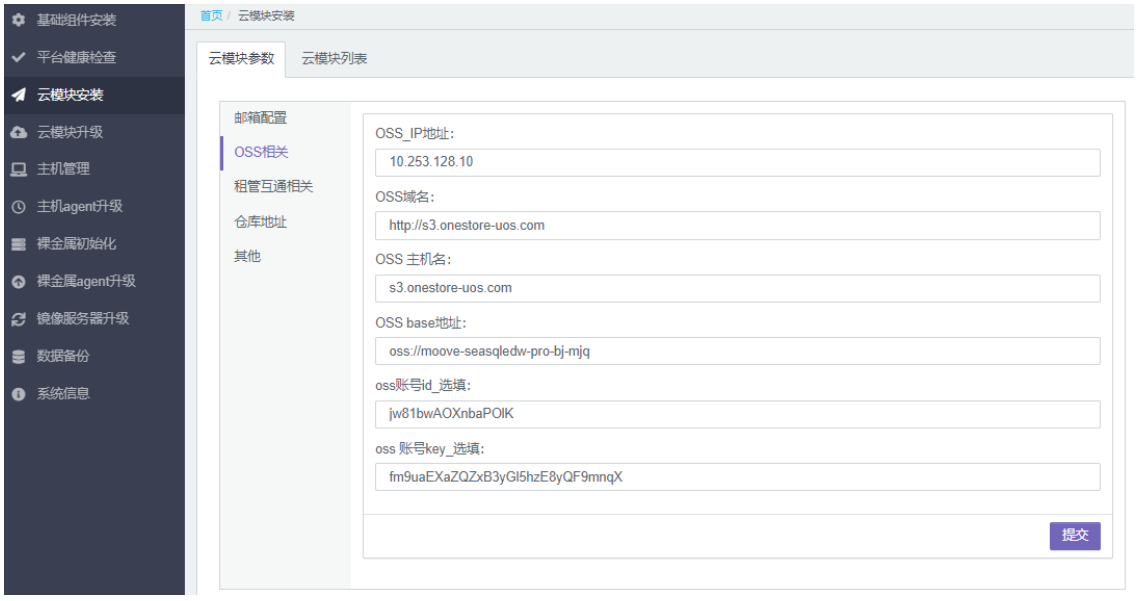
5.3 云模块部署

CloudOS 7.0 的管理平台部署可以通过自动化部署工具快速部署 UCA、UCO、TAAG、DMZ 和 OMC，本节将详细介绍其部署方式。

5.3.1 云模块参数设置

1. 操作步骤

(1) 选择“云模块安装”菜单项，在“云模块参数”页签，修改云模块参数。若无特别规划信息，则无需修改云模块参数。



(2) 点击<提交>按钮，即可完成云模块参数设置。

2. 参数说明

云模块参数说明如下。

说明

邮箱配置和仓库地址菜单无需填写。

表5-1 OSS 相关参数说明

参数名称	含义	常见值或示例
OSS_IP地址	部署节点的OSS的IP	节点实际建设情况
OSS域名	部署节点的OSS EndPoint配置	节点实际建设情况
OSS主机名	部署节点的OSS EndPoint配置	节点实际建设情况
OSSbase地址	数据库NOSQL在OSS上存放脚本的桶	oss://dbaas-nosql-service
oss账号id	部署节点的OSS Key Id配置	选填，请根据节点实际建设情况填写。 变量未填写会导致如下组件部署失败： uca-dbaas-rds.git uca-dbaas-dms.git uca-dbaas-nosql.git uca-ccr-core.git
oss账号key	部署节点的OSS Secret Key配置	选填，请根据节点实际建设情况填写。 变量未填写会导致如下组件部署失败： uca-dbaas-rds.git uca-dbaas-dms.git uca-dbaas-nosql.git uca-ccr-core.git

表5-2 租管互通相关参数说明

参数名称	含义	常见值或示例
租管互通业务网关地址(必填)	租管互通业务网关地址	节点实际建设情况
租管互通管理VIP(必填)	租管互通K8S集群管理VIP	节点实际建设情况
租管互通业务VIP(必填)	租管互通K8S集群业务VIP	节点实际建设情况

表5-3 其他云模块参数说明

参数名称	含义	常见值或示例
CMDB ELASTICSEARCH 节点1	OMC_BASE ES的地址	-
CMDB ELASTICSEARCH 节点	OMC_BASE ES的地址	-

参数名称	含义	常见值或示例
2		
CMDB ELASTICSEARCH 节点3	OMC_BASE ES的地址	-
CMDB ELASTICSEARCH 节点4	OMC_BASE ES的地址	-
cce服务文件仓库、yum仓库、harbor仓库IP地址	cce服务文件仓库、yum仓库、harbor仓库IP地址	平台初始化前无需变更 请在云容器引擎CCE初始化完成后，根据7.10.1 安装前装备中所搭建的cce_repo_server服务器的真实业务ip进行填写，填写完后重新部署uca-cce-core服务。
公服区HARBOR管理网地址(必填)	CCR HARBOR 管理网地址，UCA-CCR-CORE使用	节点实际建设情况 (公服区k8s集群管理网ip:30002，样例：10.253.146.225:30002)
公服区HARBOR业务网地址(必填)	CCR HARBOR 业务网地址，CCE集群使用	节点实际建设情况 (公服区k8s集群业务网ip:30002，样例：100.100.63.120:30002)
公服区 OPENAPI的业务地址(必填)	公服区OPENAPI的业务地址	节点实际建设情况 (公服区k8s集群业务网ip:30990，样例：http://100.100.63.120:30990)
内网oss域名	对象存储的内网域名(暂时未支持)	内网oss域名和OSS 主机名保持一致
ossprometheus地址	对象存储的prometheus的地址ip:port(暂时未支持)	请保持默认值，无需修改
必填_版本环境配套OSS的通用AK	该字段为应用管理所依赖的对象存储的AK（暂时未支持）	请保持默认值，无需修改
必填_版本环境配套OSS的通用SK	该字段为应用管理所依赖的对象存储的SK（暂时未支持）	请保持默认值，无需修改
必填_版本环境配套OSS的地址(需要指明协议与端口，协议与平台前端协议一致)	该字段为应用管理所依赖的DMZ区对象存储的地址，需要与DMZ区的镜像仓库harbor使用同一对象存储服务器。该对象存储服务器由环境建设而定。 一般可从环境地址记录表中获取。 需要根据环境情况携带协议前缀，例如平台访问若是https，则需要https://xxx	http://s3.test.com
必填_配套OSS的管理集群内部使用的地址(需要指明协议与端口,若使用域名与前者一致)	该字段为应用管理所依赖的DMZ区对象存储的地址，需要与DMZ区的镜像仓库harbor使用同一对象存储服务器。该对象存储服务器由环境建设而定。 该地址供管理区A层使用，需要保证A层服务可以通该域名或ip；一般若是域名地址，则与上方变量相同，若是ip，需要采取oss可以在管区通的管区ip。协议一般内部使用http。	http://s3.test.com

参数名称	含义	常见值或示例
	一般可从环境地址记录表中获取。	
必填_配套OSS的DMZ集群地址(需要指明协议与端口,需业务区可通,若使用域名与前者一致)	该字段为应用管理所依赖的DMZ区对象存储的地址，需要与DMZ区的镜像仓库harbor使用同一对象存储服务器。该对象存储服务器由环境建设而定。 该地址供业务层S层虚拟机下载文件使用，需要保证S层可以通该域名或ip；一般若是域名地址，则与上方变量相同，若是ip，需要采取oss可以在S层通的DMZ区ip。 一般可从环境地址记录表中获取。	http://s3.test.com
用户控制台入口	Cloudos7.0 用户控制台登录入口常为 http(s)://{入口nginxVip}+12011	http://10.253.146.70:12011 https://10.253.146.70:12011
云监控服务地址	云监控服务地址 需要配置内网域名解析，域名解析的服务IP地址是DMZ区的K8S的VIP 如果租区访问不到该地址时，需要配置公网	uca.reception.unicloudsrv.com
云监控服务的端口	云监控服务的端口，默认40702	40702
创建实例默认出口放行的ip	创建实例默认出口放行的ip DMZ区的网段信息，参考DMZ区K8S的VIP网段 若访问云监控服务地址时需要添加安全组策略，请在此配置	100.67.100.1/24
事件上报服务地址	事件上报服务地址	http://taag-monitor-reception-service:40702
云监控服务的IP(云监控服务所在节点的业务IP)	云监控服务的IP(云监控服务所在节点的业务IP) 一般填写DMZ区的K8S的VIP	
必填_DMZ区所搭建的redis的vip地址	该字段为DMZ区所搭建的一套轻量化K8S集群中的供DMZ区服务使用的REDIS的访问VIP。 一般可从环境地址记录表中获取。	100.66.1.169
必填_DMZ区所搭建的REDIS的端口	该字段为DMZ区所搭建的一套轻量化K8S集群中的供DMZ区服务使用的REDIS的端口 一般可从环境地址记录表中获取。	6379
必填_DMZ区所搭建的RABBITMQ的vip地址	该字段为DMZ区所搭建的一套轻量化K8S集群中的供DMZ区服务使用的RABBITMQ的VIP 一般可从环境地址记录表中获取。	100.66.1.175
必填_DMZ区所搭建的	该字段为DMZ区所搭建的一套轻量化K8S集群中的供DMZ区服务使用	5672

参数名称	含义	常见值或示例
RABBITMQ的端口	的RABBITMQ的端口 一般可从环境地址记录表中获取。	
必填_DMZ区所搭建的RABBITMQ的user用户名	该字段为DMZ区所搭建的一套轻量化K8S集群中的供DMZ区服务使用的RABBITMQ的用户 一般可从环境地址记录表中获取。	openstack
必填_DMZ区所搭建的数据库的用户	该字段为DMZ区所搭建的一套轻量化K8S集群中的供DMZ区服务使用的数据库的用户 一般可从环境地址记录表中获取。	moove
必填_DMZ区所搭建的数据库的端口	该字段为DMZ区所搭建的一套轻量化K8S集群中的供DMZ区服务使用的数据库的端口 一般可从环境地址记录表中获取。	3306
服务魔方传输VPC的ID	服务魔方传输VPC的ID	平台初始化前无需变更。 请参考7.3.1 登录OMC运维平台，完成OMC平台初始化后，参考“3. 获取服务魔方的VPC相关参数”的步骤来获取。三个变量均获取完成后，填写到变量参数中，并重新部署uca-csc云服务。
服务魔方传输VPC创建者的用户ID	服务魔方传输VPC创建者的用户ID	
服务魔方传输VPC的子网的ID	服务魔方传输VPC的子网的ID	

3. 获取服务魔方的 VPC 相关参数

服务魔方中 AUTOPS_TRANSFER_VPC_ID 、 AUTOPS_TRANSFER_VPC_USER_ID 和 AUTOPS_TRANSFER_VPC_SUB_NET_ID 三个云模块变量的取值，需要在 OMC 中创建对应参数后，再从 OMC 中获取。在 OMC 中创建 VPC 相关参数的步骤如下。

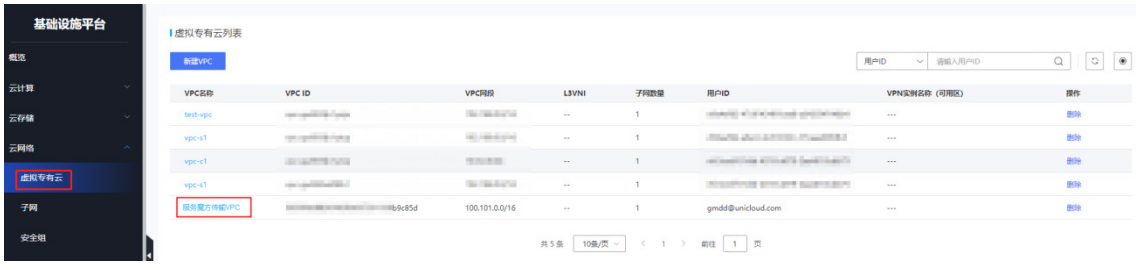
(1) 使用管理员账号登录 OMC 系统，点击页面左上方的，选择[IAAS/基础设施平台]。

(2) 在基础设施平台导航栏中，选择[云网络/虚拟专有云]，点击<新建 VPC>按钮。

(3) 按照如下参数值填写 VPC 信息，填写完成后点击<确定>按钮。

参数	取值
VPC名称	服务魔方传输VPC
VPC网段	100.101.0.0/16
是否跨可用区	是
子网名称	服务魔方传输VPC子网
子网网段	100.101.0.0/17

(4) 返回虚拟专有云列表页面，点击创建的 VPC 名称，查看 VPC 基本信息。



(5) 在 VPC 基本信息页面，可以获取到 AUTOPS_TRANSFER_VPC_ID、AUTOPS_TRANSFER_VPC_USER_ID 的变量取值。

- AUTOPS_TRANSFER_VPC_ID：对应 VPC ID 参数值。
- AUTOPS_TRANSFER_VPC_USER_ID：对应用户 ID 参数值。

(6) 点击<子网列表>页签。子网 ID 即为 AUTOPS_TRANSFER_VPC_SUB_NET_ID 变量取值。

5.3.2 部署项目

部署项目可以选择所有组件全量部署、单项部署和按所在层批量部署三种方式，且需按照 UCA、UCO、TAAG、OMC、DMZ 的顺序执行，下面将分别进行介绍三种部署方式。

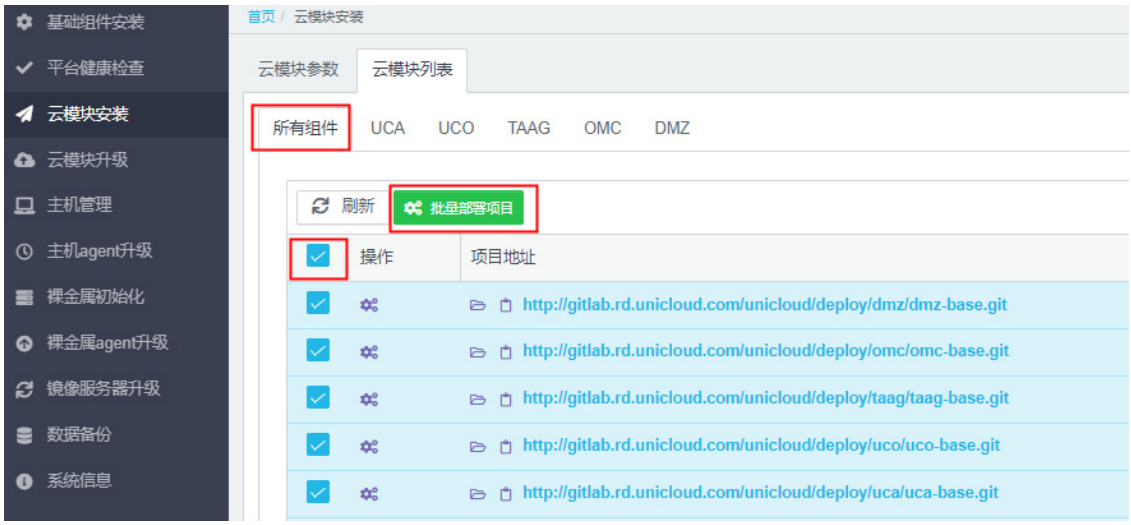
说明

- 云模块安装部署过程中，弹框不可关闭，PC 不可以断网。
- 部署各层云模块时，均需要部署对应的 base 项目。当使用单项部署方式时，请优先部署各层云模块 base 项目，且对于 UCO 云模块，紧接着还需要部署 uco-op-config; 对于 OMC 云模块，紧接着需要部署 omc-nacos。首次全新部署建议使用批量部署，系统会自动规划所有服务的安装顺序。

1. 全量部署

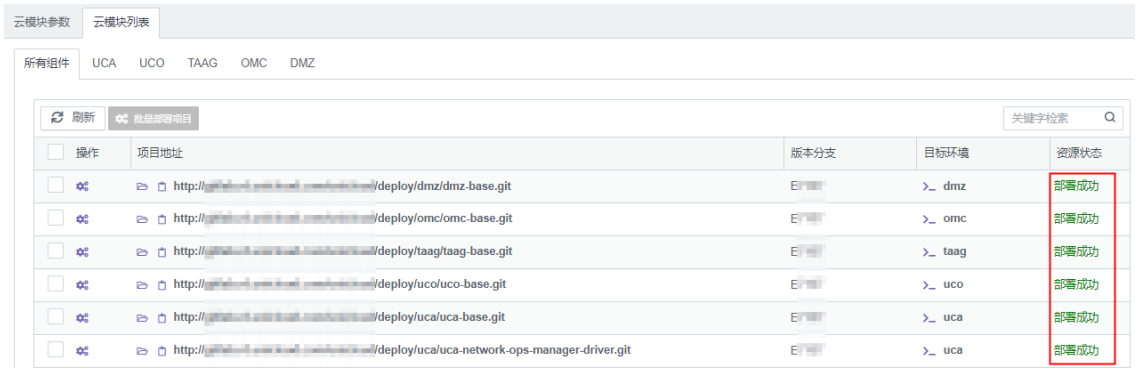
(1) 在导航栏选择[云模块安装]，并选择[云模块列表/所有组件]。勾选全部组件，点击<批量部署项目>按钮，开始对所有层级的项目按顺序依次进行部署。

图5-23 全量部署项目



(2) 当项目部署成功后，资源状态列表显示“部署成功”，说明资源部署正常。若资源状态为空或者部署失败，则说明部署异常，请查看日志，日志路径：/root/myDeployer/outputs.log。

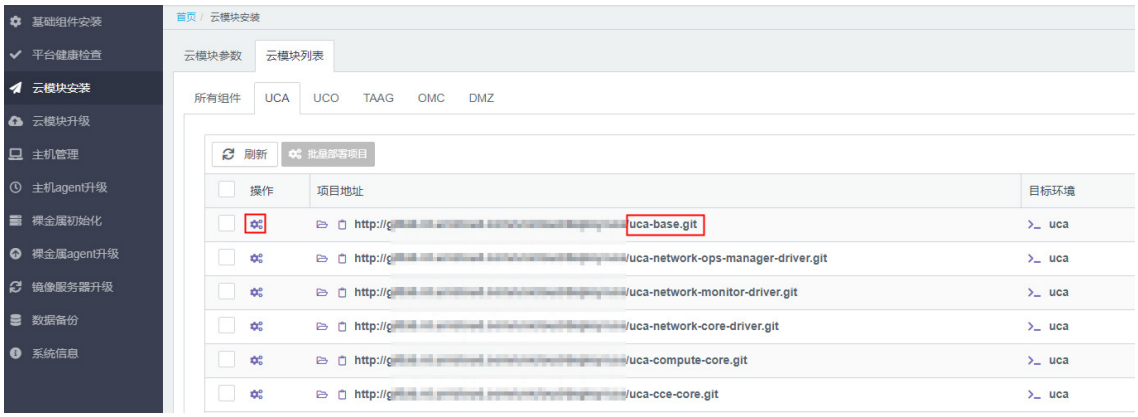
图5-24 查看项目资源



2. 单项部署项目

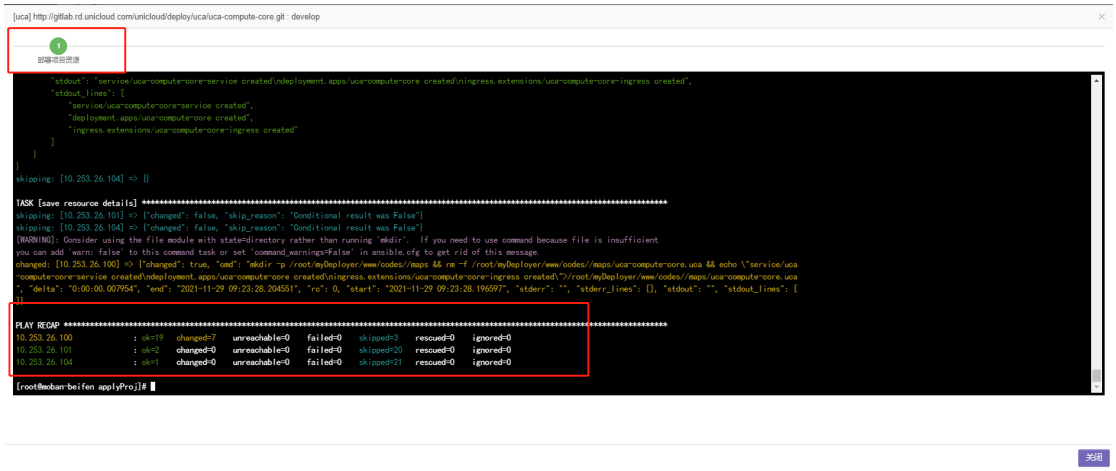
(1) 在导航栏选择[云模块安装]，根据需要选择对应页签和项目，单击 图标完成对应项目代码的部署。

图5-25 单项部署项目



(2) 出现以下界面即代表项目部署成功，若 failed=1，说明项目部署失败，请查看日志，日志路径：/root/myDeployer/outputs.log。

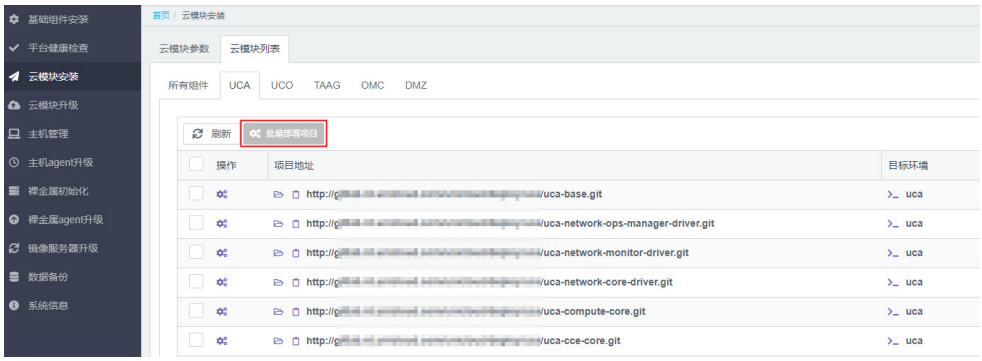
图5-26 项目部署成功



3. 批量部署项目

(1) 在导航栏选择[云模块安装]，根据需要选择对应页签，勾选该项目对应的所有项目代码，并单击<批量部署项目>按钮，可一次性完成该项目对应的所有代码。

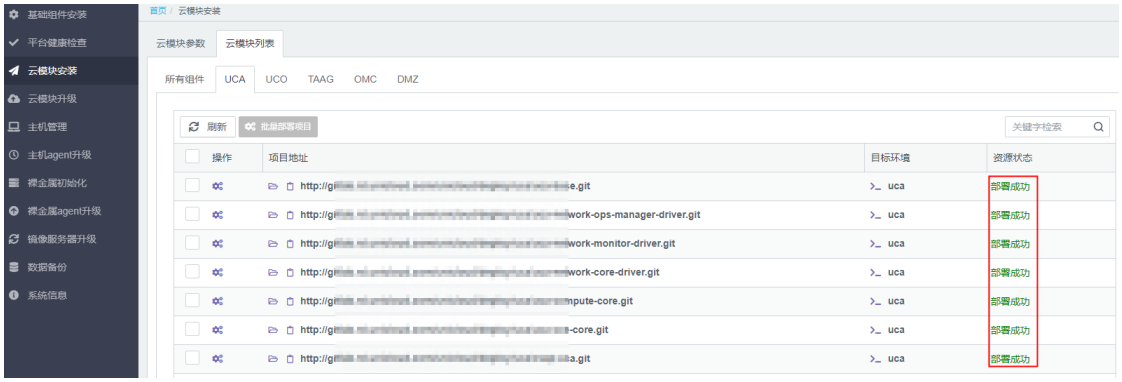
图5-27 批量部署项目



(2) 当项目部署成功后，资源状态列表显示“部署成功”，说明资源部署正常。若资源状态为空或部署失败，则说明部署异常，请查看日志，日志路径：/root/myDeployer/outputs.log。

组件 uco-monitor-portal 在 rebirth 页面上的部署结果可能显示为空，显示为空时请确认后台对应 pod 状态，如果 pod 状态正常，则无需关注，否则请联系研发支持。

图5-28 查看项目资源



(3) 如果某个项目部署失败，请单击该项目前面的 图标，重新部署该项目的代码。

4. 手动增加裸金属探针安装文件

(1) 登录 DMZ K8S 区，编辑增加 Linux 裸金属探针安装文件的 json 文件。

```
vim /etc/bms-server/linux-config-agent/linux-agent.json
```

增加文本内容如下，之后保存退出。

```
{
    "Version": "v4.1.1.2"
}
```

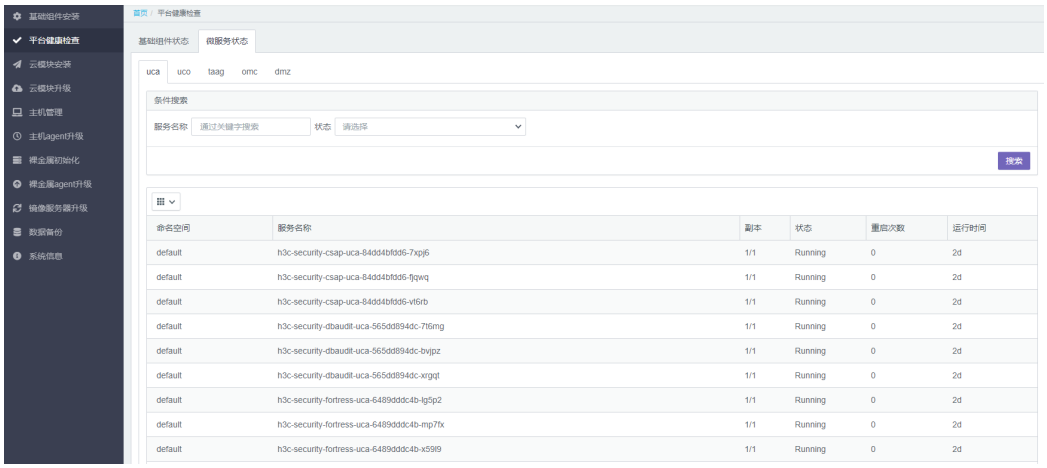
(2) 再复制该文件到 window 裸金属探针目录下。

```
cp /etc/bms-server/linux-config-agent/linux-agent.json
/etc/bms-server/win-config-agent/linux-agent.json
```

5.3.3 微服务状态巡检

(1) 选择[平台健康检查/微服务状态]菜单项，进入微服务状态巡检页面。

图5-29 微服务状态巡检



(2) 在微服务状态巡检页面，选择 uca、uco、taag、omc 或 dmz，在“条件搜索”框中，通过指定服务名称或状态，单击<搜索>按钮，可以查看对应功能模块下指定微服务的状态信息。

5.3.4 执行 CURL 命令（计算和块存储定时任务）

云模块部署完成后，需在 UCA K8S 任意节点执行计算和块存储定时任务初始化 CURL 脚本。执行以下操作：

(1) 从 Rebirth 主机中获取 CURL 脚本，脚本存放路径为：

/root/myDeployer/www/codesource/uca-center/overlays/tempnode/tempregion/9_init_schedule_job_compute_storage.sh

(2) 执行脚本中的命令，在 UCA 的 K8S 集群中的任一主机执行即可。

示例如下，请将脚本中的“AUTOPS_UCA_K8S_VIP”变量替换为真实环境中的 UCA K8S 的 VIP。

```
echo "计算、块存储定时任务初始化脚本($0)，A是VIP AUTOPS_UCA_K8S_VIP"
curl -x POST "http://AUTOPS_UCA_K8S_VIP:40444/uca/iaas/scheduler/v1.0/schedule/create" -H "accept: */*" -H "Content-Type: application/json" -d '{"schedule_task_info":[
{"description":"创建定时快照","schedule_cron":"0 0 0/1 * * ? *","service_name":"storage","task_name":"CreateAutoSnapshot","trigger_url":"http://uca-center-service:40298/uca/storage/v2.0
/snapshot/autoCreate","type":"SYSTEM"},
{"description":"定时释放本地快照","schedule_cron":"0 0 0 1/1 * ? *","service_name":"storage","task_name":"SnapshotLocalReleaseJob","trigger_url":"http://uca-center-service:40298/uca/sto
rage/v2.0/snapshot/local/autoDelete","type":"SYSTEM"},
{"description":"创建全局定时快照","schedule_cron":"0 0 0/1 * * ? *","service_name":"storage","task_name":"CreateGlobalAutoSnapshot","trigger_url":"http://uca-center-service:40298/uca/st
orage/v2.0/snapshot/globalAutoCreate","type":"SYSTEM"},
{"description":"定时清理预占资源","schedule_cron":"0 0 0,12 * * ? *","service_name":"compute","task_name":"SyncHostResourceJob","trigger_url":"http://uca-center-service:40298/uca/comput
e/v3.0/host/syncResource","type":"SYSTEM"},
{"description":"定时释放存储设备快照","schedule_cron":"0 40 0/1 * * ? *","service_name":"storage","task_name":"SnapshotStorageReleaseJob","trigger_url":"http://uca-center-service:40298/
uca/storage/v2.0/snapshot/storage/autoDelete","type":"SYSTEM"},
{"description":"工作流巡检重试定时任务","schedule_cron":"0 */5 * * * ? *","service_name":"compute","task_name":"WorkFlowAutoFixJob","trigger_url":"http://uca-center-service:40298/uca/ce
nter/v2.0/workflow/autofix","type":"SYSTEM"},
{"description":"工作流巡检告警定时任务","schedule_cron":"0 0 9,14,18 * * ? *","service_name":"compute","task_name":"WorkFlowMonitorJob","trigger_url":"http://uca-center-service:40298/uc
a/center/v2.0/workflow/monitor","type":"SYSTEM"},
{"description":"定时刷新缓存队列","schedule_cron":"0/10 * * * * ? *","service_name":"storage","task_name":"QueueRefresh","trigger_url":"http://uca-center-service:40298/uca/storage/v2.0/
system/trigger","type":"SYSTEM"},
{"description":"Ha Keeper定时任务执行","schedule_cron":"0 */5 * * * ? *","service_name":"compute","task_name":"HAKeeperExecuteJob","trigger_url":"http://uca-center-service:40298/uca/com
pute/v3.0/ha/keeper/job/execute","type":"SYSTEM"},
{"description":"Ha Keeper定时任务通知","schedule_cron":"0 0 9,14,18 * * ? *","service_name":"compute","task_name":"HAKeeperNoticeJob","trigger_url":"http://uca-center-service:40298/uca/
compute/v3.0/ha/keeper/job/notice","type":"SYSTEM"},
{"description":"计算数据检查定时任务执行","schedule_cron":"0 0/5 * * * ?","service_name":"compute","task_name":"ComputeDataCheckExecuteJob","trigger_url":"http://uca-center-service:4029
8/uca/compute/v2.0/data/check","type":"SYSTEM"},
{"description":"Ha组件状态同步","schedule_cron":"0 0/30 * * * ? ","service_name":"compute","task_name":"HaStateCheckJob","trigger_url":"http://uca-center-service:40298/uca/compute/v3.0/
ha/map/job/checkHastate","type":"SYSTEM"},
{"description": "定时检测双活设备信息", "schedule_cron": "* 0/5 * * * ? *", "service_name": "storage", "task_name": "storage_rc_monitor", "trigger_url": "http://uca-storage-service:4000
2/uca/storage/v2.0/remotecopy/monitor", "type": "SYSTEM"}
]}'
```

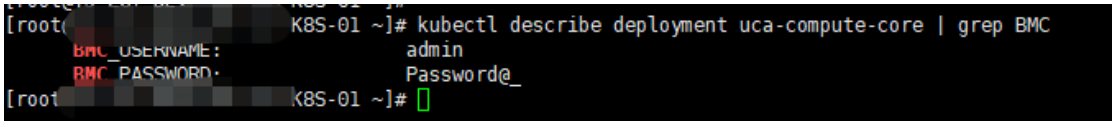
5.3.5 更新主机带外账号密码

目前环境中所有主机的带外账号密码必须保持一致，默认是：admin/Password@_

环境默认正确时，可忽略本章节操作。如果需要修改，则必须同步修改所有的主机，然后更新 uca-compute-core 服务环境变量，具体操作如下：

(1) 在 UCA K8S 节点执行如下命令，查看当前环境配置。

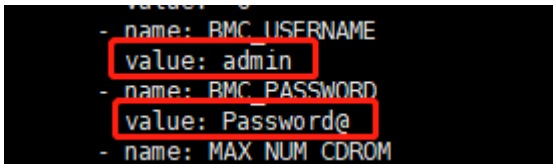
```
kubectl describe deployment uca-compute-core | grep BMC
```



(2) 更新环境变量。

a. 执行命令修改 yaml：kubectl edit deployment uca-compute-core

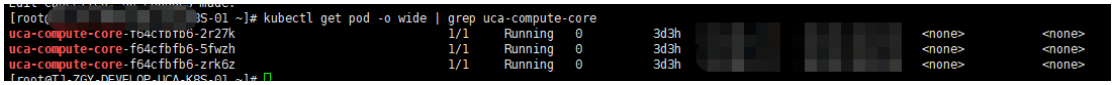
b. 更新变量：BMC_USERNAME 、 BMC_PASSWORD



c. 输入命令【:wq】，保存更改。

(3) 执行如下命令，检查 Pod 启动状态。

```
kubectl get pod -o wide | grep uca-compute-core
```



5.4 VKS主机初始化

VKS 主机初始化包括自动初始化和自定义初始化两种方式：

- 自动初始化：由系统依次执行所有模块的初始化。初始化步骤为：设备列表导入、自动化部署、VKS 主机状态巡检。
- 自定义初始化：由用户按需选择模块进行初始化。初始化步骤为：设备列表导入、设置初始化参数、执行自定义初始化、VKS 主机状态巡检。

5.4.1 前提条件

- 进行 VKS 主机初始化前，请确保 VKS 的 BIOS 程序中 NUMA 为开启状态。
- 若 VKS 需使用本地盘且数据盘已经使用过，建议初始化前务必对本地数据盘进行格式化。确保对数据盘执行 blkid 命令，无任何回显，若有回显可使用 wipefs 命令擦除。
- 执行初始化前请检查，若部署工具中预装的 SDS Client 版本与项目环境实际需求的 Client 版本不一致，请在初始化 VKS 前，将预装环境中的 SDS Client 版本替换为需要的 Client 版本，具体操作步骤请参见“5.4.2 自动初始化 SDS 客户端版本替换”章节。若替换不成功，请联系研发处理。
- 当服务器使用 NVME 盘作为本地盘时，请手工对本地盘进行初始化，具体操作步骤请联系研发处理。

5.4.2 自动初始化 SDS 客户端版本替换

(1) 获取 SDS 客户端软件包（请从 SDS 产品获取），并上传软件包到 Rebirth 虚机的如下路径：/root/cvk_auto_init/cvk-init

(2) 修改软件包脚本。

`vi /root/cvk_auto_init/cvk-init/install-ONEStor-Client.yml`

将新包名替换到红色框中

```
---
- hosts: all
  gather_facts: no
  remote_user: root

  tasks:
    - name: copy ONEStor-Client
      copy: src=ONEStor-E3338-x86_64-ceph_client_rpm.tar.gz dest=/opt
            owner=root group=root mode=0644

    - name: "ceph client info"
      ignore_errors: True
      raw: ceph --version | grep 12.2.1
      register: returnmsg

    - name: "install ceph client"
      raw: cd /opt/; tar -xvf ONEStor-E3338-x86_64-ceph_client_rpm.tar.gz; cd ceph_client_rpm/;
           chmod +x  install_ceph_client.sh; ./install_ceph_client.sh
      when: returnmsg.rc != 0

    - name: "dir info"
      ignore_errors: True
      raw: ls /var/run/ceph
      register: returnmsg2

    - name: "install ceph client"
      raw: chmod 777 /var/run/ceph
      when: returnmsg2.rc == 0
~
~
```

5.4.3 设备列表导入

当前支持如下几种设备类型：

- COM：计算类 VKS
- SEC：安全类 VKS
- SLB：负载均衡类 VKS
- RDS：关系型数据库类 VKS

使用共享存储的 VKS，设备类型可统一使用 COM；使用本地存储的 VKS，设备类型可统一选为 SLB 或 RDS；同时使用共享存储和本地盘的 VKS，设备类型可统一选择 COM_LOCAL。

(1) 选择[主机管理/设备列表]菜单项，单击<清单模板>按钮，即可进行下载查看。

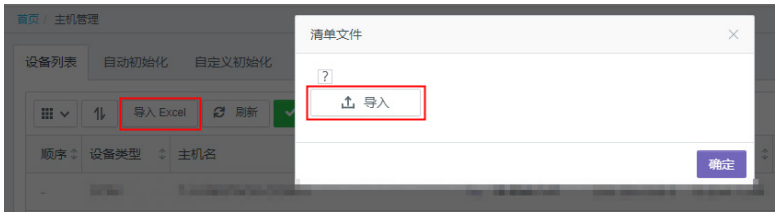
图5-30 下载清单模板

(2) 按照清单模板修改实际的设备信息，修改完毕后保存文件。

其中，ONESTOR 掩码、PRIMERA 控制器 IP 列表掩码、PRIMERA 控制器 IP 列表 2 掩码，请填写为“#”。其余不需要使用的信息也可以填写为“#”。

(3) 单击设备列表页面的<导入 Excel>按钮，将修改后的设备列表导入至 Rebirth 工具平台。

图5-31 导入设备列表



(4) 单击<刷新>按钮，实际的列表信息即呈现在 Rebirth 工具平台上。

(5) 单击页面上方的<预配置检查>按钮进，检查大页内存是否生效，mlx 网卡驱动是否安装等。

(6) （可选）单击<导出 Excel>按钮，导出列表到本地进行查看。

5.4.4 自动初始化

(1) 登录 Rebirth 主机，执行如下命令。

```
cd /root/cvk_auto_init/
sed -i  "s/item_nicid.trim().startsWith(bus_info)/-1 !=
item_nicid.trim().indexOf(bus_info)/" 01-cvkPreFilterCkecl.js
sed -i  "s/item_nicid.trim().startsWith(bus_info)/-1 !=
item_nicid.trim().indexOf(bus_info)/" 03-cvkChecker.js
sed -i  "s/item.startsWith('bus-info: ')/-1 != item.indexOf('bus-info: ')/g"
03-cvkChecker.js
sed -i "s/item.startsWith(businfo)/-1 != item.indexOf(businfo)/g" 03-cvkChecker.js
```

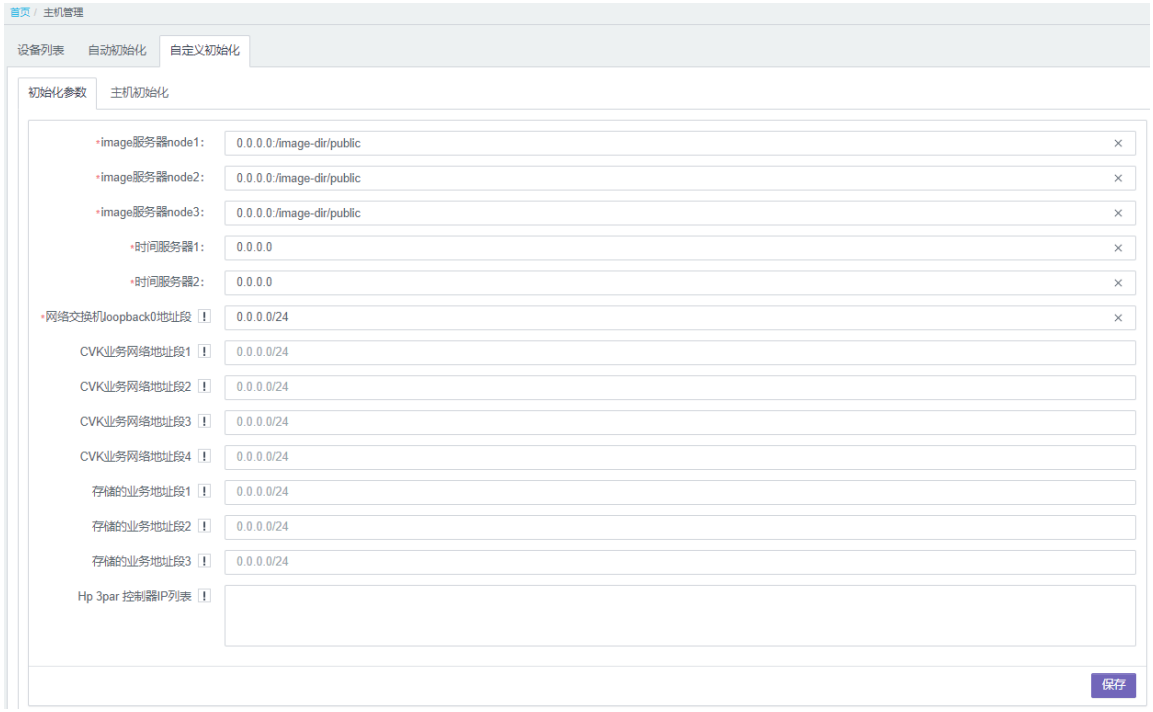
(2) 选择[主机管理/自动初始化]菜单项，单击[自动化部署]按钮，系统开始依次执行自动化部署。

初始化过程中，界面会显示正在执行任务的日志。其中显示“ignoring”的日志为可忽略的错误日志，无需处理；显示“failed=1”的日志表示任务执行失败，请查找失败原因并重新执行任务。

5.4.5 自定义初始化

1. 初始化参数设置

(1) 选择[主机管理/自定义初始化/初始化参数]菜单项，配置主机初始化参数。



参数说明：

参数	说明
Image服务器	镜像服务器的虚机IP地址和镜像路径，格式为：server-ip:/image-patch。 server-ip为虚机IP地址，image-patch为镜像路径，请按照实际信息填写。
时间服务器	即授时服务器，如果没有单独的时间服务器，请填写Rebirth工具的IP地址。这里的填写要与[基础组件安装/全局参数]中填写的授时服务器

	地址保持一致。
网络交换机loopback0地址段	用于主机Overlay建立BGP，填写交换机、路由器、防火墙等设备的Loopback 0接口地址段。
业务网络、存储网络、Hp 3PAR控制器IP	请按照实际信息填写，如果没有，需要保持为空。

(2) 点击<保存>按钮，完成初始化参数设置。

2. 主机初始化操作

选择[主机管理/自定义初始化/主机初始化]菜单项。请按照步骤顺序依次单击<执行>按钮，即可完成操作。

图5-32 主机初始化

初始化过程中，界面会显示正在执行任务的日志。其中显示“ignoring”的日志为可忽略的错误日志，无需处理；显示“failed=1”的日志表示任务执行失败，请查找失败原因并重新执行任务。

5.4.6 （可选）调整大页内存

OVS 默认占用 32G 大页内存，新部署时，建议参照 11.3 如何调整业务区 VKS 大页内存章节，调整 OVS 内存占用，为系统预留更多的运行内容。

5.4.7 VKS 主机对接 SDS 集群

VKS 对接 SDS 集群时，需要在 VKS 上配置 SDS 集群配置文件。为适配多套 SDS 集群，需要将不同的 SDS 集群配置文件以集群 fsid 作为标志，文件名称如下：fsid.conf、fsid.keyring。

1. 适用场景

- VKS 初始化。
- 新增加 SDS 集群。

2. 使用限制

多套 SDS 集群版本必须一致，不支持跨版本。

跨 AZ 迁移时，需要把 2 套 AZ 的存储配置文件（fsid.conf 和 fsid.keyring）都添加到 VKS 中。

3. SDS 集群创建 Fsid 配置文件

(1) 登录到 SDS 集群的 node 节点。

(2) 拷贝 fsid.conf、fsid.keyring 配置文件。

```
fsid=$(grep fsid /etc/ceph/ceph.conf | awk -F'= ' '{print $NF}')
```

```
cp /etc/ceph/ceph.conf /tmp/$fsid.conf
cp /etc/ceph/ceph.client.admin.keyring /tmp/$fsid.keyring
ll /tmp/$fsid.*
-rw-r--r-- 1 SDS_Admin root 2218 Dec 24 15:35
/tmp/eea733ef-98b2-404c-807b-a16149e2487e.conf
-rw-r--r-- 1 SDS_Admin root   63 Dec 24 15:35
/tmp/eea733ef-98b2-404c-807b-a16149e2487e.keyring
```

4. VKS 配置 SDS 集群配置文件

(1) 在 SDS 上执行如下命令，将 fsid.conf、fsid.keyring 文件复制到/etc/onestor_client 目录。

```
scp /tmp/$fsid.* root@10.254.7.3:/etc/onestor_client  //VKS 的 IP 地址、登录密码请按照实际情况输入
```

(2) 查看多套 SDS 集群配置，例如如下回显为正常：

```
ll /etc/onestor_client
total 16
-rw-r--r-- 1 root root 1932 Dec 24 15:29 a338d222-9fd5-4530-9087-4c1cc272702a.conf
-rw-r--r-- 1 root root   63 Dec 24 15:29 a338d222-9fd5-4530-9087-4c1cc272702a.keyring
-rw-r--r-- 1 root root 2218 Dec 24 15:56 eea733ef-98b2-404c-807b-a16149e2487e.conf
-rw-r--r-- 1 root root   63 Dec 24 15:56 eea733ef-98b2-404c-807b-a16149e2487e.keyring
```

(3) 重启 cvk-agent 服务。

```
systemctl restart cvk-agent
```

(4) 查看 SDS 对应秘钥是否创建。

```
virsh secret-list
eea733ef-98b2-404c-807b-a16149e2487e  ceph eea733ef-98b2-404c-807b-a16149e2487e
```

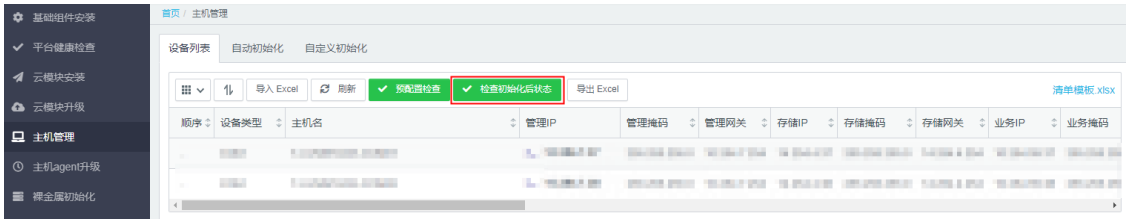
5.4.8 设置 enable_unsafe_noiommu_mode 为开机自启动

在所有计算 VKS 服务器上执行。

```
echo  "/usr/bin/echo 1 >
/sys/module/vfio/parameters/enable_unsafe_noiommu_mode" >>/etc/rc.local;
echo  "/usr/bin/echo 1 >
/sys/module/vfio/parameters/enable_unsafe_noiommu_mode" >>/etc/rc.d/rc.local;
```

5.4.9 VKS 主机状态巡检

(1) 选择[主机管理/设备列表]菜单项，单击<检查初始化后状态>按钮，系统自动开始进行 VKS 主机状态检查。



(2) 如果检查时报错，根据检查结果进行定位排查。

5.4.10 升级 VKS 补丁

若业务区 VKS 使用的是 E0730P06 版本，需要安装 E0730P06H03、E0730P06H06 两个补丁。

1. 版本配套表

请准备如下补丁包。

表5-4 版本配套表

补丁版本号	补丁文件名	补丁适用的软件版本	发布日期	备注
CAS-E0730P06H03	CAS-E0730P06H03-Patch.tar.gz	CAS-E0730P06	2022-08-09	热补丁
CAS-E0730P06H06	CAS-E0730P06H06-Patch.tar.gz	CAS-E0730P06	2022-10-26	冷补丁

2. 使用限制和注意事项

- 打上冷补丁后需要重启主机生效。
- 若涉及同时升级多个补丁版本，则必须遵循从低版本到高版本的升级顺序。

3. 升级前准备

(1) 检查 Usphere 版本：登录 VKS，查看 Usphere 版本与补丁包适配软件版本是否一致。

```
cat /etc/cas_cvk-version
```

4. 升级步骤

注意

补丁版本必须与服务器的软件版本相匹配。如果不匹配，则会造成补丁操作失败。

请勿修改补丁包的任何信息，例如补丁名称、内容、后缀等，否则可能导致补丁安装失败。

升级日志及升级相关信息统一存放在/var/log/patch/目录下面，补丁日志文件名为：补丁版本.log。每一个补丁对应一个日志文件，记录了补丁升级相关的日志信息。

(1) 创建配置文件/etc/cvk/net_manage.conf，配置文件内容如下。

```
openvswitch_uninstall=True
```

(2) 单独的主机补丁升级通过后台 hotpatch-manage.sh 脚本来进行，命令如下，需要注意的是，如果是冷补丁，需要 reboot 重启 VKS。

```
hotpatch-manage.sh  install +补丁压缩包名称
```

(3) 升级完成后，退出维护模式，迁回或开启业务虚机。

5.5 GPU环境初始化

5.5.1 操作说明

一张 GPU 卡有三种使用方式：GPU 直通，时分 vGPU，MIG vGPU（某些型号支持），不同的使用方式进行不同的初始化步骤。

初始化步骤如下：

(1) 配置 BIOS 基础环境

(2) 配置 GPU 基础环境

(3) 根据使用方式执行相应的初始化：

- 初始化直通型 GPU
- 初始化时分 vGPU
- 初始化 MIG vGPU

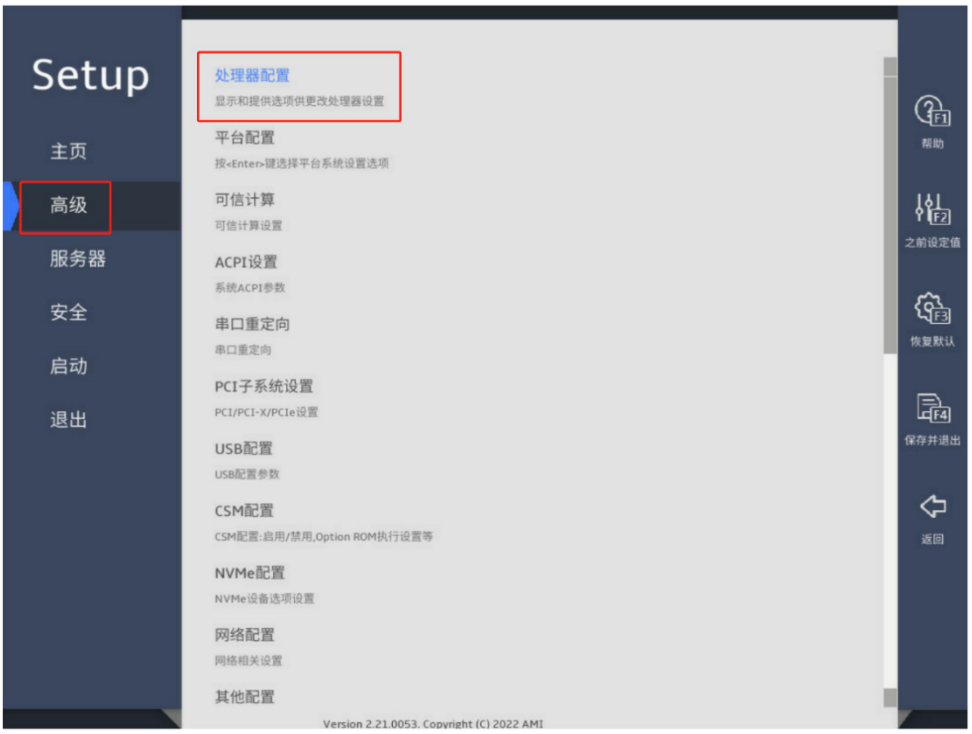
5.5.2 配置 BIOS 基础环境

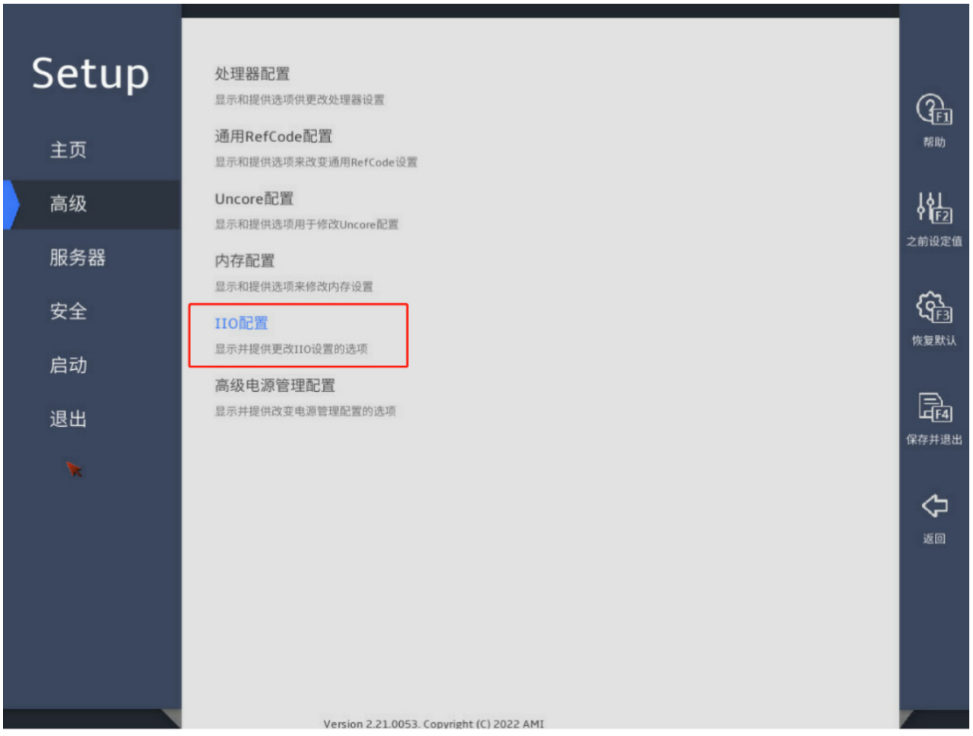
(1) 插上 GPU 卡，启动服务器进入 BIOS 界面。

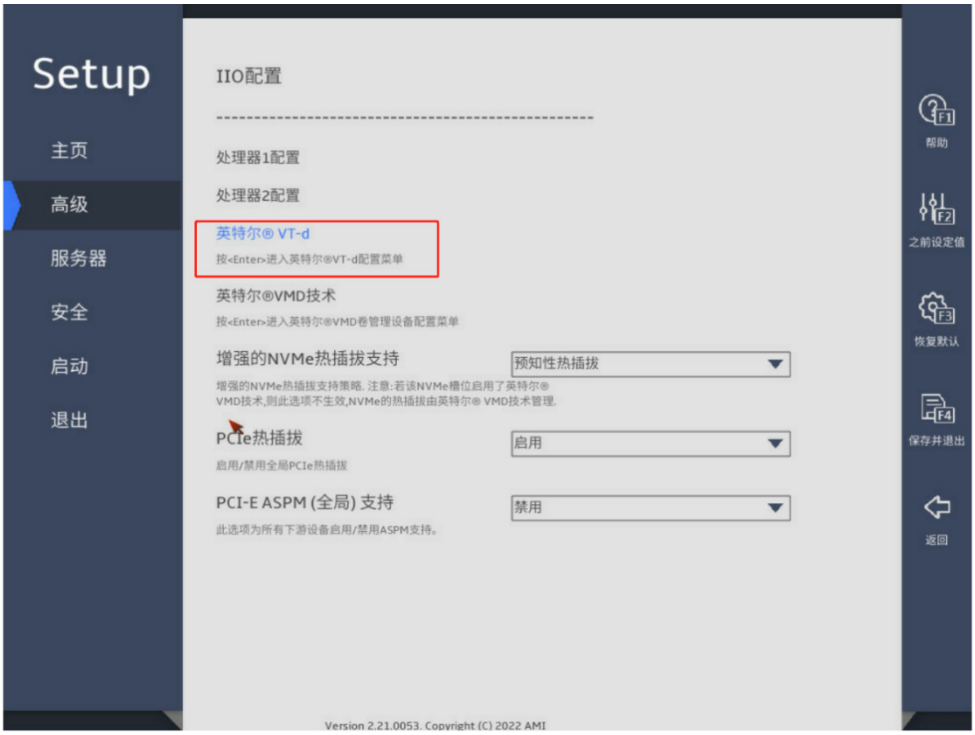
(2) 开启 IOMMU。

对于 inter 处理器，使用的技术为 VT-d，对于 AMD 处理器，使用的技术为 IOMMU。这里以 H3C 5300G5 服务器开启 IOMMU 举例。

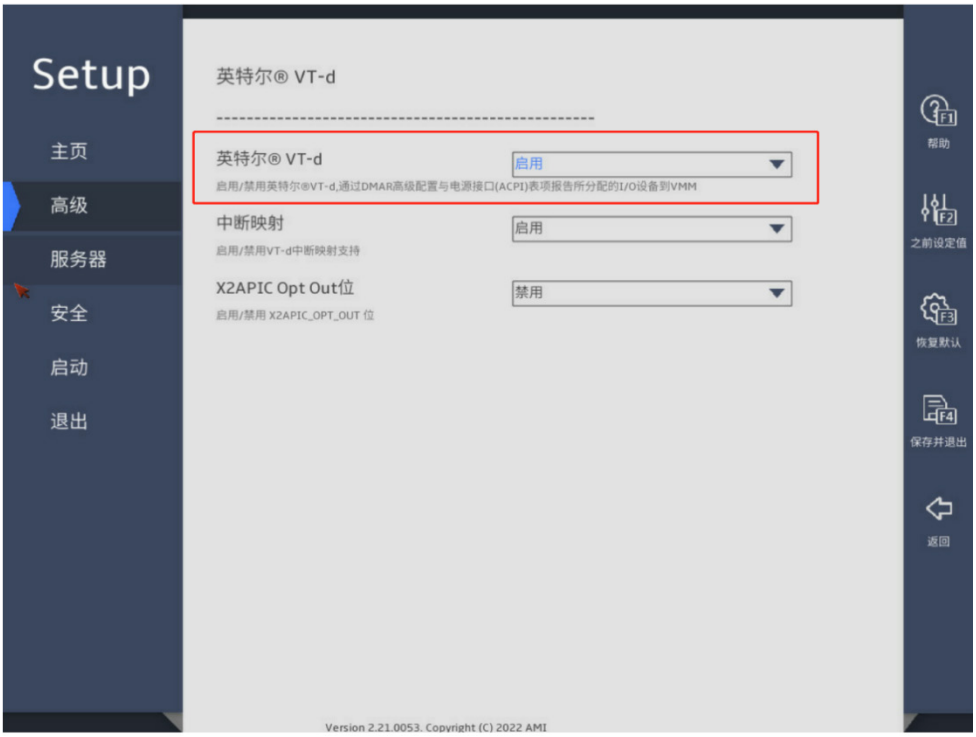
a. 在 BIOS 中，依次选择[高级/处理器配置/IIO 配置/英特尔 VT-d]。


Setup
主页
高级
服务器
安全
启动
退出
处理器配置
显示和提供选项供更改处理器设置
平台配置
按<Enter>键选择平台系统设置选项
可信计算
可信计算设置
ACPI设置
系统ACPI参数
串口重定向
串口重定向
PCI子系统设置
PCI/PCI-X/PCIe设置
USB配置
USB配置参数
CSM配置
CSM配置:启用/禁用,Option ROM执行设置等
NVMe配置
NVMe设备选项设置
网络配置
网络相关设置
其他配置
Version 2.21.0053. Copyright (C) 2022 AMI
帮助
之前设定值
恢复默认
保存并退出
返回


Setup
主页
高级
服务器
安全
启动
退出
处理器配置
显示和提供选项供更改处理器设置
通用RefCode配置
显示和提供选项来改变通用RefCode设置
Uncore配置
显示和提供选项用于修改Uncore配置
内存配置
显示和提供选项来修改内存设置
IIO配置
显示并提供更改IIO设置的选项
高级电源管理配置
显示并提供改变电源管理配置的选项
Version 2.21.0053. Copyright (C) 2022 AMI
帮助
之前设定值
恢复默认
保存并退出
返回

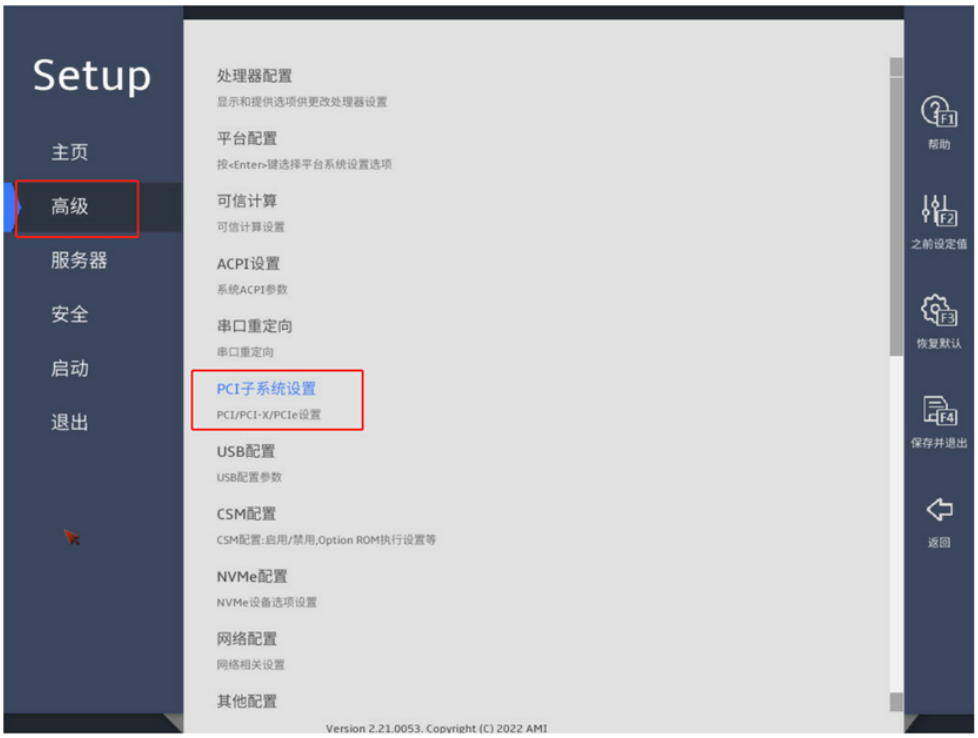


b. 在[英特尔 VT-d]后的下拉框中，选择<启用>。

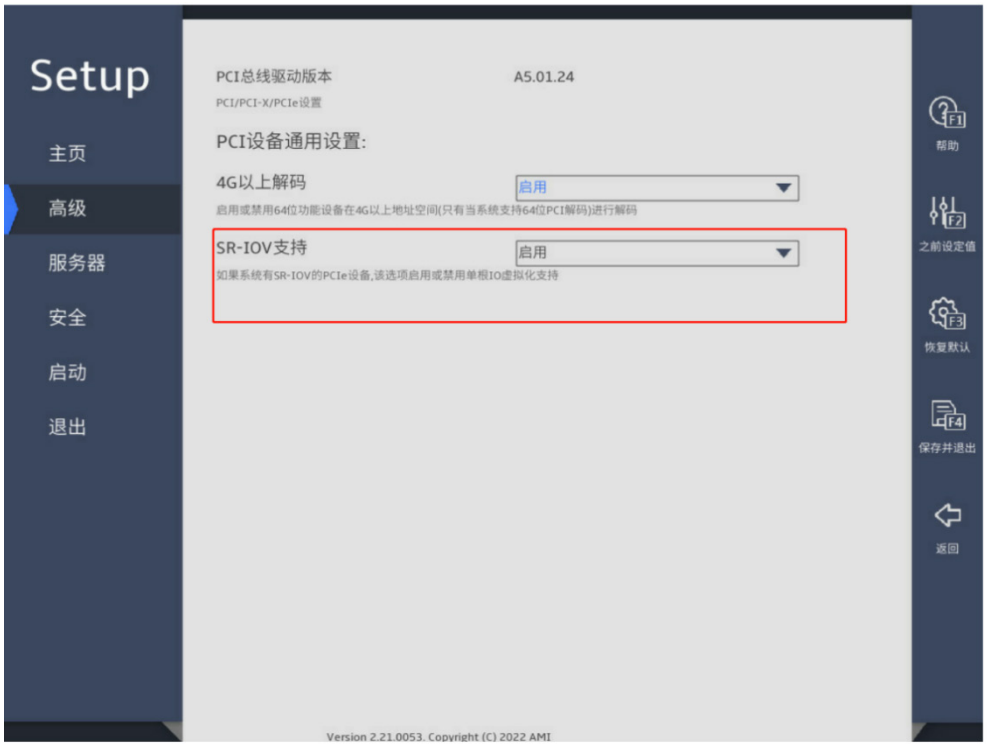


(3) 开启 SR-IOV：

a. 在 BIOS 中，依次选择[高级/PCI 子系统设置]。



b. 在[SR-IOV 支持]后的下拉框中，选择<启用>。



5.5.3 配置 GPU 基础环境

进入系统后，需要再对 IOMMU（VT-d）进行以下配置。

1. 判断服务器启动方式

执行如下命令：

```
[ -d /sys/firmware/efi ] && echo UEFI || echo BIOS
```

若为 Legacy，则执行 2. Legacy 启动模式，若为 UEFI 启动，则执行 3. UEFI 启动模式。

2. Legacy 启动模式

(1) 确认 grub 文件内容是否包含以下内容：执行如下命令，编辑 grub 文件。

对于 Intel CPU(VT-d)，在 GRUB_CMDLINE_LINUX 行应包含：intel_iommu=on iommu=pt

对于 AMD CPU(AMD-Vi)，在 GRUB_CMDLINE_LINUX 行应包含：amd_iommu=on iommu=pt

若包含，跳过步骤(1)，若不包含，则编辑 grub 文件添加以上配置，并更新 grub 文件。

```
vi /etc/default/grub
```


```
grub2-mkconfig -o /boot/grub2/grub.cfg
```

(2) 执行如下命令，检查 iommu 是否开启成功。回显中包含 intel_iommu=on 或者 amd_iommu=on 代表开启成功。

```
# dmesg |grep DMAR |grep IOMMU |grep enable
 [ 0.000000] DMAR: IOMMU enabled
# cat /proc/cmdline
BOOT_IMAGE=/boot/vmlinuz-4.14.0-generic
root=UUID=8c0c9362-be45-46dc-92d5-f82abd5d04c1 ro ramdisk_size=2048000 nomodeset
elevator=deadline transparent_hugepage=always crashkernel=512M intel_iommu=on
iommu=pt quiet
```

3. UEFI 启动模式

(1) 确认 grub 文件内容是否包含以下内容：执行如下命令，编辑 grub 文件。

对于 Intel CPU(VT-d)，在 GRUB_CMDLINE_LINUX 行应包含：intel_iommu=on iommu=pt

对于 AMD CPU(AMD-Vi)，在 GRUB_CMDLINE_LINUX 行应包含：amd_iommu=on iommu=pt

若包含，则执行步骤（2）即可；若不包含，则编辑 grub 文件添加以上配置，并更新 grub 文件，之后重启服务器。

```
vi /etc/default/grub
grub2-mkconfig -o /boot/efi/EFI/centos/grub.cfg
```

(2) 执行如下命令，检查 iommu 是否开启成功。

```
# dmesg |grep DMAR |grep IOMMU |grep enable
[ 0.000000] DMAR: IOMMU enabled
# cat /proc/cmdline
intel_iommu=on 或者 amd_iommu=on
```

5.5.4 初始化直通型 GPU

完成基础环境配置后，直通型的 GPU 在 OMC 平台纳管服务器后即可使用。

5.5.5 初始化 vGPU（包括时分 vGPU 和 MIG vGPU）

1. vGPU 划分规则

vGPU 的 VKS 在环境初始化时进行 vGPU 的划分，划分规则如下：

- 按照显存大小进行一个切分，每个 vGPU 的显存大小是固定的。
- 每一个物理 GPU 同时只能划分出一种类型的 vGPU，不能再创建其他类型的 vGPU。
- 同一显卡的不同物理 GPU 可以同时划分不同类型的 vGPU。
- 每个虚拟机只能挂载一个 vGPU。
- 划分 vGPU 后的 GPU 卡，不能再用于直通设备。

2. 划分 vGPU 的接口说明

计算代理提供了初始化 vGPU 的接口，并会将 vGPU 的划分信息持久化到/etc/cvk-agent/vgpu.conf。

接口描述如下：

接口	method	URL	同步/异步
vgpu划分接口	POST	http://<hostip>:33333/compute/v1/gpu/divide	同步

请求 body 参数：

参数	类型	位置	是否必传	说明
BusList	Array	Body	否	要用作vGPU的物理GPU pci 号地址列表。默认不传，表示将VKS上的所有GPU都划分Type类型的 vgpu
MdevType	string	Body	是	vgpu 规格 分时模式：16Q/8Q/4Q/2Q2/2B/1B/16C等（常见于 V100） MIG模式：2g.10gb-2g.10gb-2g.10gb-1g.5gb 3g.20gb-3g.20gb等（常见于 A100 MIG-backed）
Model	string	Body	否	vgpu模式：timesliced/mig，默认是 timesliced

3. 删除 vGPU 的接口说明

删除 vGPU 是将对应 GPU 设备中的 vGPU 设备全部清理，该接口在用于环境清理或者虚拟机想使用直通型 GPU 设备时使用。

接口描述如下：

接口	method	URL	同步/异步
删除 vGPU 接口	POST	http://<hostip>:33333/compute/v1/gpu/clean	同步

请求 header 参数：参考默认请求参数。

请求 body 参数：

参数	类型	位置	是否必传	说明
BusList	Array	Body	否	要清理的物理GPU PCI号地址。默认不传，表示将VKS上所有GPU

				中的vGPU都做清理。

响应参数：参考默认响应体。

请求示例：

```
curl -X POST "http://10.254.7.4:33333/compute/v1/gpu/clean" -H "accept: application/json"
-H "Content-Type: application/json" -d "{ }"
```

其中，10.254.7.4 为 VKS 管理网的 IP 地址。

4. 初始化时分 vGPU

(1) 完成基础环境配置后，在 OMC 平台纳管服务器。

(2) 安装使用 cvk-agent 接口进行 vGPU 的划分：

vGPU 划分时，请遵守 vGPU 划分规则。

执行 vGPU 划分命令，接口说明请参考“划分 vGPU 的接口说明”。请求示例如下：

```
curl -X POST "http://10.254.7.8:33333/compute/v1/gpu/divide" -H "accept: applicatio
n/json" -H "Content-Type: application/json" -d "{ \"BusList\": [ \"0000:0e:00.0\" ]
, \"MdevType\": \"6Q\", \"Model\": \"timesliced\"}"
```

回显说明：

10.254.7.4 为 VKS 管理网 IP 地址。

BusList 的值 0000:0e:00.0，是通过在 VKS 中执行如下命令来获取的：

```
nvidia-smi --query-gpu=name,index,pci.bus_id  --format=csv
```

示例如下：

```
[root@A100-MIG-CVK02 0000:0e:00.4]# nvidia-smi --query-gpu=name,index,pci.bus_id  --format=csv
name, index, pci.bus_id
NVIDIA A100-PCIE-80GB, 0, 00000000:0E:00.0
NVIDIA A40, 1, 00000000:17:00.0
NVIDIA A10, 2, 00000000:1B:00.0
```

(3) （可选）删除 vGPU

当需要删除时，可以参考“删除 vGPU 的接口说明”操作。

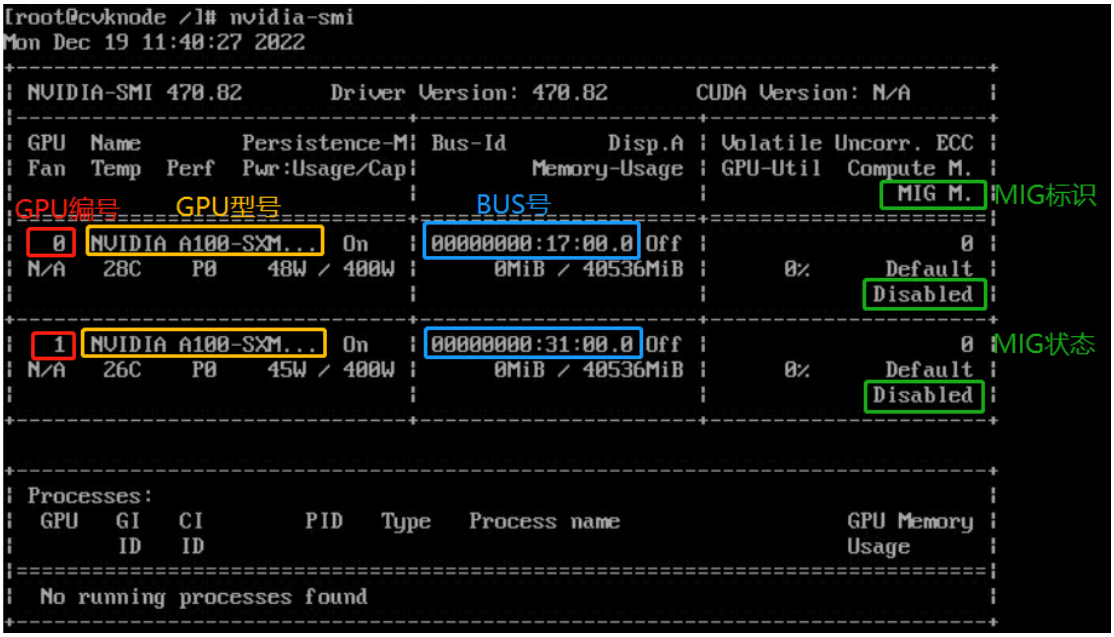
5. 初始化 MIG vGPU

使用前请注意，MIG vGPU 支持的 Usphere 版本为 E0760P01。

(1) 完成基础环境配置后，在 OMC 平台纳管服务器。

(2) 执行如下命令，查看 GPU 信息，具有 MIG 标识的为具有 MIG 功能的 GPU。

```
nvidia-smi
```



(3) 执行如下命令之一，开启 MIG 模式。

为所有支持 MIG 的 GPU 开启 MIG：

```
nvidia-smi -mig 1
```

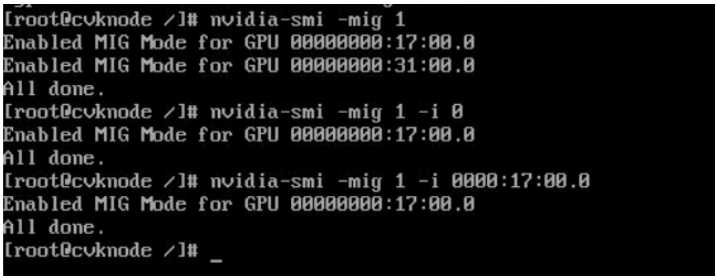
为指定的 GPU 开启 MIG：

```
nvidia-smi –mig 1 -i [bus-id]
```

或

```
nvidia-smi -mig 1 -i [gpu-id]
```

以下图为例，nvidia-smi -mig 1 -i 0 或 nvidia-smi -mig 1 -i 0000:17:00.0



(4) 执行如下命令，查看 MIG 划分支持的规格。

```
# nvidia-smi mig -lgip
```

```
[root@A100-MIG-CVK02 ~]# nvidia-smi mig -lgip
+-----------------------------------------------------------------------------+
| GPU instance profiles:                                                      |
| GPU   Name             ID    Instances   Memory     P2P    SM    DEC   ENC  |
|                              Free/Total   GiB              CE    JPEG  OFA  |
|=============================================================================|
|   0  MIG 1g.10gb       19     2/7         9.50       No     14     0     0   |
|                                                              1     0     0   |
+-----------------------------------------------------------------------------+
|   0  MIG 1g.10gb+me    20     1/1         9.50       No     14     1     0   |
|                                                              1     1     1   |
+-----------------------------------------------------------------------------+
|   0  MIG 2g.20gb       14     1/3         19.50      No     28     1     0   |
|                                                              2     0     0   |
+-----------------------------------------------------------------------------+
|   0  MIG 3g.40gb        9     0/2         39.50      No     42     2     0   |
|                                                              3     0     0   |
+-----------------------------------------------------------------------------+
|   0  MIG 4g.40gb        5     0/1         39.50      No     56     2     0   |
|                                                              4     0     0   |
+-----------------------------------------------------------------------------+
|   0  MIG 7g.80gb        0     0/1         79.25      No     98     5     0   |
|                                                              7     1     1   |
+-----------------------------------------------------------------------------+
```

回显信息中，Name 列为支持的 MIG vGPU 规格，Instances Free/Total 为实例的可用量和总量。在创建 MIG vGPU 时，可对以上规格进行组合。例如，对于 A100 40G 的 GPU 卡，在 Instances Free/Total 列中，Free 值为 7 时，可选择组合 1g.5gb-1g.5gb-1g.5gb-1g.5gb-1g.5gb-1g.5gb-1g.5gb(共 7 个)，同样对于 A100 80G 的 GPU 卡，在 Instances Free/Total 列中，Free 值为 7 时，可选择组合 1g.10gb-1g.10gb-1g.10gb-1g.10gb-1g.10gb-1g.10gb-1g.10gb(共 7 个)。

(5) 安装使用 cvk-agent 接口进行 vGPU 的划分：

vGPU 划分时，请遵守 vGPU 划分规则。

执行 vGPU 划分命令，接口说明请参考“划分 vGPU 的接口”。请求示例如下：

```
curl -X POST "http://10.254.7.8:33333/compute/v1/gpu/divide" -H "accept: applicatio
n/json" -H "Content-Type: application/json" -d "{ \"BusList\": [ \"0000:0e:00.0\" ]
, \"MdevType\": \"3g.40gb-3g.50gb\", \"Model\": \"mig\"}"
```

回显说明：

10.254.7.4 为 VKS 管理网 IP 地址。

BusList 的值 0000:0e:00.0，是通过在 VKS 中执行如下命令来获取的：

```
nvidia-smi --query-gpu=name,index,pci.bus_id  --format=csv
```

示例如下：

```
[root@A100-MIG-CVK02 0000:0e:00.4]# nvidia-smi --query-gpu=name,index,pci.bus_id  --format=csv
name, index, pci.bus_id
NVIDIA A100-PCIE-80GB, 0, 00000000:0E:00.0
NVIDIA A40, 1, 00000000:17:00.0
NVIDIA A10, 2, 00000000:1B:00.0
```

(6) （可选）删除 vGPU

当需要删除时，可以参考“删除 vGPU 的接口说明”操作。

5.6 （可选）边缘自治服务部署

边缘自治服务（uca-center-edge）仅部署在边缘 LZ 的 UCA K8S 服务器中。由于未集成到自动部署组件中，需要使用下列部署文件手动部署。

另外边缘自治服务需与边缘 LZ 的 VKS 上的 cvk-agent 和 cvk-ha 服务配合使用，需更新边缘 LZ VKS 的 cvk-agent 和 cvk-ha 配置文件。

5.6.1 获取部署文件

部署文件请从版本发布路径下获取：全量包\云服务组件包\IAAS\uca-center-edge.tar.gz。

解压缩后，包括如下文件：

- 镜像文件：

  ARM 镜像文件：uca-center-edge-vxxxx.tar.gz

  X86 镜像文件：uca-center-edge-vxxxx.tar.gz

  其中 vxxx 代表镜像文件的版本号。

- SQL 脚本文件：

  1_uca_center_edge_init_tables.sql

  2_uca_center_edge_time_jobs.sql

- yaml 文件：

  uca-center-edge-deploy.yaml

  uca-center-edge-ingress.yaml

  uca-center-edge-service.yaml

5.6.2 uca-center-edge 服务部署步骤

(1) 将版本发布路径中的 uca-center-edge 文件夹上传到需要安装或升级边缘自治服务的边缘 LZ 的 K8S 集群上的/root 目录下。

(2) 在 K8S 集群所有节点上，分别执行如下命令，上传镜像。

```
# x86 环境
cd /root/uca-center-edge/image/x86
docker load -i uca-center-edge-vxxxx.tar.gz
# arm 环境
cd /root/uca-center-edge/image/arm
docker load -i uca-center-edge-vxxxx.tar.gz
```

(3) 按文件名顺序，依次执行/root/uca-center-edge/sql 目录下的 SQL 脚本。

(4) 更改 uca-center-edge-ingress.yaml 文件，替换<当前 AZ ID>、<当前 Region ID>为实际环境的值。

```
apiVersion: extensions/v1beta1
kind: Ingress
metadata:
  name: uca-center-edge-ingress
  namespace: default
  annotations:
```

```
    nginx.ingress.kubernetes.io/rewrite-target: /
    nginx.ingress.kubernetes.io/ssl-redirect: "false"
    nginx.ingress.kubernetes.io/server-alias: ~^uca-center-edge-service\.<当前 AZ ID>\.[A-Za-z0-9-]+\.unicloud\.space$
spec:
  rules:
    - host: uca-center-edge-service. <当前 AZ ID>.<当前 Region ID>.unicloud.space
      http:
        paths:
          - path: /
            backend:
              serviceName: uca-center-edge-service
              servicePort: 40268
```

(5) 在 K8S 集群任意节点上，执行如下命令。

```
cd /root/uca-center-edge/yaml
kubectl apply -f uca-center-edge-deploy.yaml
kubectl apply -f uca-center-edge-service.yaml
kubectl apply -f uca-center-edge-ingress.yaml
```

5.6.3 更新 VKS Agent 配置文件

(1) 使用 root 用户登录到边缘 LZ 的 VKS。

(2) 执行如下命令，增加边缘自治服务地址到 cvk-agent.yaml 文件中。

```
sed -i "/UCAURL/a\EDGEUCAURL: <az-k8s-vip>:40268" /etc/cvk-agent/cvk-agent.yaml
```

其中<az-k8s-vip>为边缘 LZ 的 K8S VIP 地址。示例如下：

```
sed -i "/UCAURL/a\EDGEUCAURL: 10.254.7.229:40268" /etc/cvk-agent/cvk-agent.yaml
```

5.6.4 更新 VKS HA 配置文件

(1) 使用 root 用户登录到边缘 LZ 的 VKS。

(2) 执行如下命令，增加边缘自治服务地址到 cvk-ha.yaml 文件中。

```
sed -i "/ReportCenterUrl/a\ComputeEdgeUrl: <az-k8s-vip>:40268"
/etc/cvk-ha/cvk-ha.yaml
```

其中<az-k8s-vip>为边缘 LZ 的 K8S VIP 地址。示例如下：

```
sed -i "/ReportCenterUrl/a\ComputeEdgeUrl: 10.254.7.229:40268"
/etc/cvk-ha/cvk-ha.yaml
```

5.7 裸金属初始化

X86 架构的裸金属和 ARM 架构的裸金属在 PXE 启动中使用不同的引导固件和部署镜像，需规划不同的 DHCP 网段和 VLAN，但两者共用一套 TFTP Server。

目前 X86 架构的裸金属通过部署工具进行初始化，ARM 架构的裸金属需手动初始化。两种架构初始化步骤分别如下。

- X86 架构：配置 HDM（X86/ARM）> 配置 TFTP（X86/ARM）> 配置 DHCP（X86）>（可选）配置域名解析。

- ARM 架构：配置 HDM（X86/ARM） > 配置 TFTP（X86/ARM） > 配置 DHCP(ARM) > 安装引导固件（ARM） > 安装部署镜像（ARM） > （可选）配置域名解析。

说明

本章节仅针对常见的裸金属服务器型号进行介绍，对于特殊型号裸金属服务器，初始化方法请参考部署指导的“附录 D”。

5.7.1 配置 HDM（X86/ARM）

本节主要升级裸金属 HDM 和 BIOS 固件版本，每台裸金属都需执行。

(1) 登录 Rebirth 虚机，执行如下命令，赋予 Builder 可执行权限。

```
chmod +x /root/myDeployer/www/proj/bms/Builder
```

(2) 选择[裸金属初始化/HDM]菜单项，配置 HDM 的带外管理 IP 地址。HDM 和 BIOS 的固件版本需要大于等于如下版本：

- HDM 固件版本：1.30.21 HDM V100R001B03D021
- BIOS 固件版本：2.00.39 V100R001B02D039

图5-33 HDM 设置

(3) 填写完成后，单击<保存>按钮。

(4) 单击<执行>按钮，工具会将 VNC 设置、BIOS 设置、PXE 引导设置等信息下发到裸金属服务器。

5.7.2 配置 TFTP（X86/ARM）

如果 TFTP 服务器在之前部署时已内置，请跳过该步骤，反之请按照如下步骤操作。

(1) 在部署工具中选择[裸金属初始化/TFTP]菜单项，配置裸金属主机 PXE 引导镜像。

图5-34 裸金属主机 PXE 引导镜像

参数说明：

参数	说明
启动镜像路径	默认为/home/tftpboot，不可修改。

(2) 填写完成后，点击<保存>按钮。

(3) 点击<执行>按钮，将 PXE 引导镜像拷贝到 TFTP 服务器。

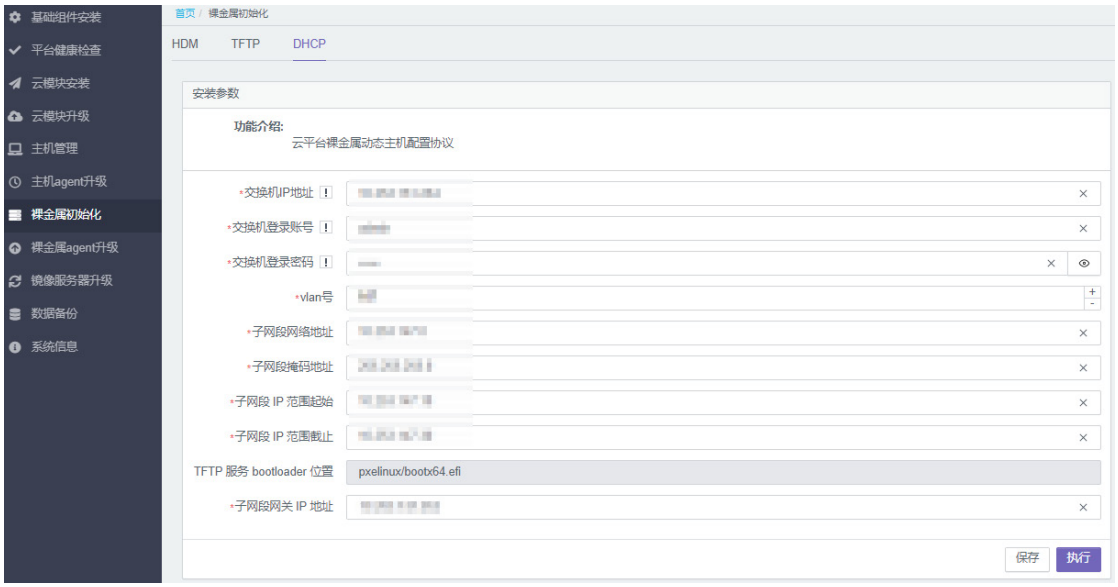
(4) 登录到 TFTP 服务器上，执行以下命令创建目录。

```
mkdir -p /home/tftpboot
```

5.7.3 配置 DHCP（X86）

(1) 选择[裸金属初始化/DHCP]菜单项，根据 3.4 IP 地址规划表中裸金属设备规划实际管理地址。

图5-35 裸金属设备地址规划



(2) 填写完成后，点击<保存>按钮。

(3) 点击<执行>按钮，配置裸金属 DHCP 网段和交换机。

5.7.4 配置 DHCP(ARM)

在管理交换机上配置 DHCP 服务，为 ARM 架构裸金属的部署网提供 IP 地址。

ARM 引导固件服务位于 Rebirth 虚机的/root/tftp-ansible/file-arm 路径下，名称为 pxelinux/aarch_64/bootaa64.efi。DHCP 的 IP 网段、ARM 架构裸金属部署网 VLAN 和 TFTP Server 的 IP 地址请按照实际环境规划来填写。

注：交换机应事先添加好 DHCP 网段相应的路由，确保配置完成后，tftp 可 ping 通 dhcp gateway-list。

(1) 创建并配置 DHCP Pool。注意 DHCP Pool 的编号不能为 1，与 X86 架构使用的 DHCP Pool 编号区分开。

```
[Region2-MGT-S6800-001]dhcp server ip-pool 3
[Region2-MGT-S6800-001-dhcp-pool-3]display this
#
dhcp server ip-pool 3
#
return
[Region2-MGT-S6800-001-dhcp-pool-3]gateway-list 10.254.12.254
[Region2-MGT-S6800-001-dhcp-pool-3]network 10.254.12.0 mask 255.255.255.0
[Region2-MGT-S6800-001-dhcp-pool-3]address range 10.254.12.100 10.254.12.200
[Region2-MGT-S6800-001-dhcp-pool-3]bootfile-name pxelinux/aarch_64/bootaa64.efi
[Region2-MGT-S6800-001-dhcp-pool-3]next-server 10.254.4.230  //需配置为 TFTP Server 的 IP 地址
[Region2-MGT-S6800-001-dhcp-pool-3]tftp-server ip-address 10.254.4.230
[Region2-MGT-S6800-001-dhcp-pool-3]display this
#
dhcp server ip-pool 3
 gateway-list 10.254.12.254
 network 10.254.12.0 mask 255.255.255.0
 address range 10.254.12.100 10.254.12.200
 bootfile-name pxelinux/aarch_64/bootaa64.efi
 next-server 10.254.4.230
 tftp-server ip-address 10.254.4.230
#
return
[Region2-MGT-S6800-001-dhcp-pool-3]quit
```

(2) 创建并配置 VLAN。

```
[Region2-MGT-S6800-001]interface Vlan 120
[Region2-MGT-S6800-001-Vlan-interface120]ip address 10.254.12.254 255.255.255.0  //需与 DHCP Pool 的网关 gateway-list 配置一致
[Region2-MGT-S6800-001-Vlan-interface120]display this
#
interface Vlan-interface120
ip address 10.254.12.254 255.255.255.0
#
return
[Region2-MGT-S6800-001-Vlan-interface120]quit
```

(3) 手动添加 nfs-ganesha 中 ARM 裸金属部署网网段。

此时的/etc/ganesha/ganesha.conf 配置文件中的所有 Clients 应包含云平台的管理网段（VKS 自动初始化之后会添加）、X86 裸金属 PXE 部署网段（X86 裸金属下发 DHCP 的时候会下发裸金属的网段），如果为空或者缺失，根据实际组网配置进行补充，然后手动加入 ARM 裸金属 PXE 部署网段。

注意要修改三个 NFS Server，以及 ganesha.conf 配置文件中多个目录的 Clients 范围都要修改，修改完重启 nfs-ganesha.service 服务（systemctl restart nfs-ganesha）。

```
EXPORT {
  Path = /image-dir/public;
  Export_Id = 1;
  Pseudo = /image;
  FSAL {
    Name = VFS;
  }
  CLIENT {
    Clients = 192.168.6.0/24,192.168.7.0/24,192.168.37.0/24;
    Squash = none;
    Access_Type = RW;
  }
}
LOG {
  Default_Log_Level = WARN;
  Facility {
    enable = active;
    destination = /var/log/ganesha/ganesha.log;
    name = FILE;
  }
}

NFS_CORE_PARAM {
  Bind_Addr = 0.0.0.0;
  MNT_Port = 2050;
  Enable_NLM = true;
  NLM_POrt = 2051;
  NFS_Port = 2049;
  mount_path_pseudo = true;
  Protocols = 3,4;
  Rquota_Port = 2052;
}

EXPORT {
  Path = /image-dir/public;
  Export_Id = 11;
  Pseudo = /image-dir/public;
  FSAL {
    Name = VFS;
  }
  CLIENT {
    Clients = 192.168.6.0/24,192.168.7.0/24,192.168.37.0/24;
    Squash = none;
    Access_Type = RW;
```

5.7.5 安装引导固件（ARM）

ARM 架构的裸金属 PXE 启动需要使用 ARM 架构的引导固件。

1. 文档准备

本次部署的组件为 PXE BootLoader 提供以下代码包：

UNI_UCA_Compute_BMS_v3.3.2_0001_.BootLoader_arm.tar

2. 部署步骤

(1) 拷贝 UNI_UCA_Compute_BMS_v3.3.2_0001_.BootLoader_arm.tar 到 TFTP Server 服务器。

(2) 创建目录。

```
#mkdir -p /home/tftpboot/pxelinux/aarch_64
```

(3) 解压 tar 包到目录下。

```
#tar -xvf UNI_UCA_Compute_BMS_v3.3.2_0001_.BootLoader_arm.tar -C
/home/tftpboot/pxelinux/aarch_64
#mv /home/tftpboot/pxelinux/aarch_64/pxelinux/* /home/tftpboot/pxelinux/aarch_64
#rm -rf /home/tftpboot/pxelinux/aarch_64/pxelinux
```

(4) 配置 grub.cfg。

grub.cfg 为 PXE BIOS 的引导文件，手动配置。配置文件中的 scheduler-callback 和 logDirPath 请结合实际情况配置。

```
#vim  /home/tftpboot/pxelinux/aarch_64/grub.cfg
 set default="0"
 set timeout=3
 set hidden_timeout_quiet=false

 menuentry "deploy" {
    linux deploy_image_aarch_64/uni-deploy.vmlinuz rw selinux=0
scheduler-callback=http://10.252.146.111:40201/uca/compute/v2.0/callback/baremetal/
weekup logDirPath=10.252.146.200:/var/log/pxe-agent

   initrd deploy_image_aarch_64/uni-deploy.initramfs
 }
```

(5) 配置权限。

```
#chmod -R 777 /home/tftpboot/pxelinux
```

(6) 最终回显如下。

```
#ll /home/tftpboot/pxelinux/aarch_64
 total 2036
 -rwxr-xr-x 1 root root 1034000 Jul 22 18:00 bootaa64.efi
 -rwxr-xr-x 1 root root 1041440 Jul 22 18:00 grubaa64.efi
 -rwxr-xr-x 1 root root     328 Oct 20 16:33 grub.cfg
```

5.7.6 安装部署镜像（ARM）

1. 文件准备

部署镜像压缩包 deploy_image.UNI_UCA_Compute_BMS_V3.3.6_0001_arm.tar.gz，其中压缩包内关键文件的 MD5 值如下，部署完成后请进行验证。

```
#md5sum uni-deploy.initramfs
 912cbbe1cf2236ff68f80b79cdee7dd1  uni-deploy.initra
```

2. 部署步骤

将最新的部署镜像压缩包拷贝到 TFTP Server 的“/home/tftpboot/”目录下。

```
#cd /home/tftpboot/
#mkdir -p deploy_image_aarch_64
#tar -zxvf deploy_image.UNI_UCA_Compute_BMS_V3.3.6_0002_arm.tar.gz -C
/home/tftpboot/deploy_image_aarch_64
#mv /home/tftpboot/deploy_image_aarch_64/deploy_image/*
/home/tftpboot/deploy_image_aarch_64
#chmod -R 777 deploy_image_aarch_64
```

最终 deploy_image 文件目录如下：

```
#ll /home/tftpboot/deploy_image_aarch_64
```

```
total 839136
-rwxrwxrwx 1 root root        0 Oct 19 18:37 deploy_image.UNI_UCA_Compute_BMS_V3.3.6_0002
-rwxrwxrwx 1 root root 850748836 Oct 19 18:37 uni-deploy.initramfs
-rwxrwxrwx 1 root root   8523650 Oct 19 18:37 uni-deploy.vmlinuz
```

5.7.7 （可选）配置 DMZ 区域名解析

当 DMZ 区存在内网 DNS 服务器时，也需要在 DNS 中增加域名解析。具体步骤如下。

(1) 登录到内网 DNS 域名服务器。

(2) 在 unicloud.com 的域中添加以下内容：

```
echo “ucm.agent IN  A  <dmz-k8s-假公网 vip>” >> /var/named/unicloud.com.zone
```

其中，<dmz-k8s-假公网 vip>需修改为 bms-server 所在 DMZ 区 K8S 的假公网 VIP 地址。

例如，当<dmz-k8s-假公网 vip>取值为 100.67.100.248 时，命令如下：

```
echo “ucm.agent IN  A  100.67.100.248” >> /var/named/unicloud.com.zone
```

(3) 执行如下命令，检测文件配置是否正常。

```
named-checkconf -z /etc/named.conf
```

(4) 执行如下命令，重启 named 服务。

```
systemctl restart named
```

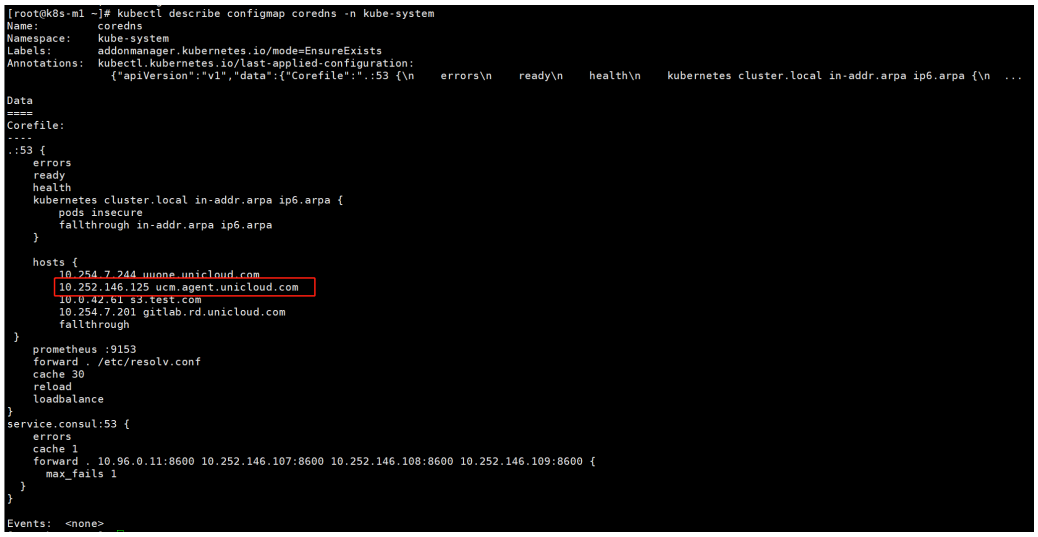
5.7.8 （可选）配置管区 K8S DNS 域名解析规则

管区的 compute-core 服务，通过域名访问 bms-server 服务，为使用裸金属 Config-agent，需要在管区 K8S 的 configmap 中配置 bms-server 的域名解析规则。具体配置步骤如下：

(1) 在 UCA K8S 集群任一节点，执行如下命令。

```
kubectl edit  configmap coredns -n kube-system
```

将 10.252.146.125 ucm.agent.unicloud.com 添加到 configmap 的 Corefile 的 hosts 中，其中 10.252.146.128 为 DMZ 区的 K8S 管理 VIP。



(2) 保存并退出。

6 资源纳管

6.1 前提条件

资源纳管前，请先完成 OMC 运维管理平台的管理员注册，具体方法请参考 7.3.1 登录 OMC 运维平台。

6.2 管理License授权

6.2.1 License Server 部署指导

如果当前项目环境中需要进行 License 授权，则需要安装 License Server。License Server 的安装指导、License 授权指导等文档，请从 CloudOS7.0 的版本说明书中获取。

6.3 纳管网络设备

6.3.1 网络设备基础配置检查

- 检查所有网络设备是否开启 Netconf、SSH 和 LLDP，链路聚合需要配置动态 LACP。
- 确认 Underlay 配置已完成。
- 网络 Overlay 的 Leaf 交换机需要检查 Loop0 地址、OSPF 和 BGP 协议状态；主机 Overlay 的 Leaf 交换机需要检查 Loop0 地址和计算区业务网络网关地址联通性。
- Spine 交换机检查 Loop0 地址和 OSPF，配置 BGP 发布 EVPN 路由，配置 Spine 为路由反射器。
- Border 交换机检查安全外网网关地址、OSPF 和 BGP 协议状态。

6.3.2 纳管网络设备

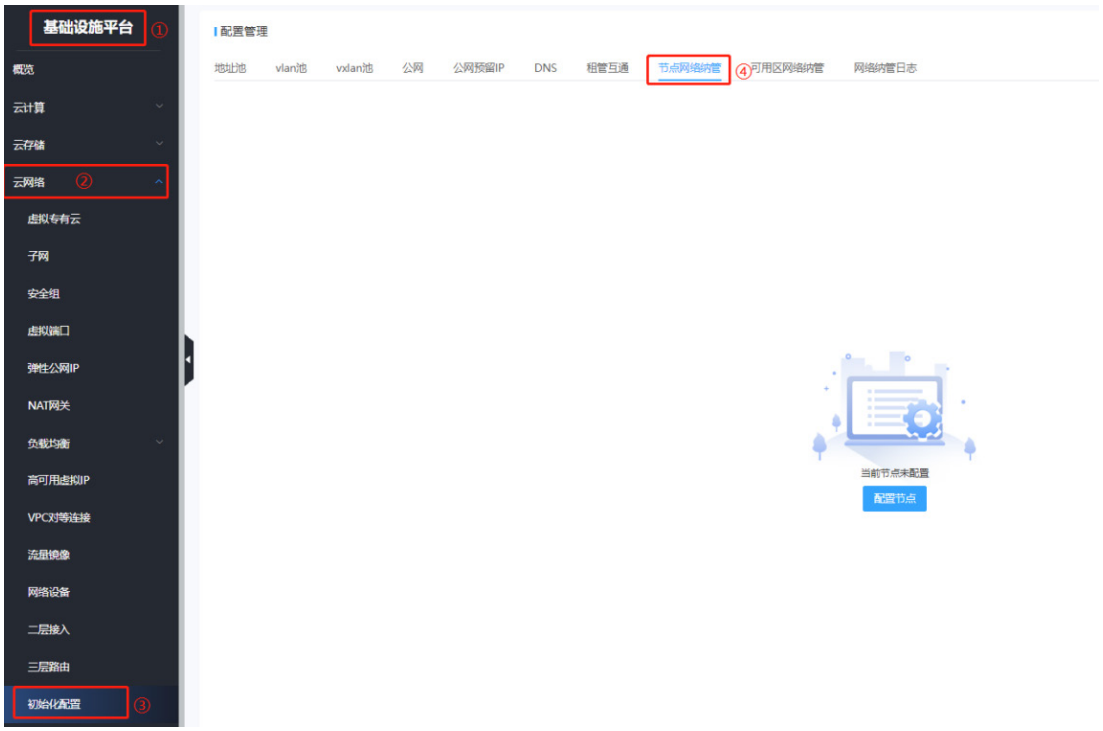
纳管 AZ 需要填写的参数较多，且没有保存配置功能，请规划好 OMC 账户超时登出时长，以免配置过程中账户登录超时自动登出。且 OMC 的用户不支持多人同时使用，请避免账户被挤登出。

1. 节点网络纳管

(1) 登录 OMC 运维管理系统，选择[IAAS/基础设施平台]。

(2) 在基础设施平台导航中，选择[云网络/初始化配置/节点网络纳管]。

图6-1 节点网络纳管



节点纳管包括两页，请参考下述步骤分别配置。

(3) 第一页主要需要填写的包括两部分，Redis 配置和和租管互通配置。

Redis 配置如下。

参数说明如下。

- 配置 Redis

参数	说明
Redis管理VIP	若Redis单独部署，写Redis实际管理VIP；若部署在管区，则填写UCA K8S集群的VIP地址
管理VIP	UCA K8S集群的VIP地址
密码	根据实际情况填写，一般为unic-moove
模式	如无特殊要求，选择sentinel-哨兵模式
端口	根据所选模式自动填充
哨兵集群地址	哨兵集群实服务地址，多个以英文半角逗号隔开。标准部署模式时，Redis集群三节点都是哨兵，端口都是26379，需要输入三节点信息。根据哨兵集群地址的

	实际情况填写，例如100.100.0.1:26379,100.100.0.2:26379

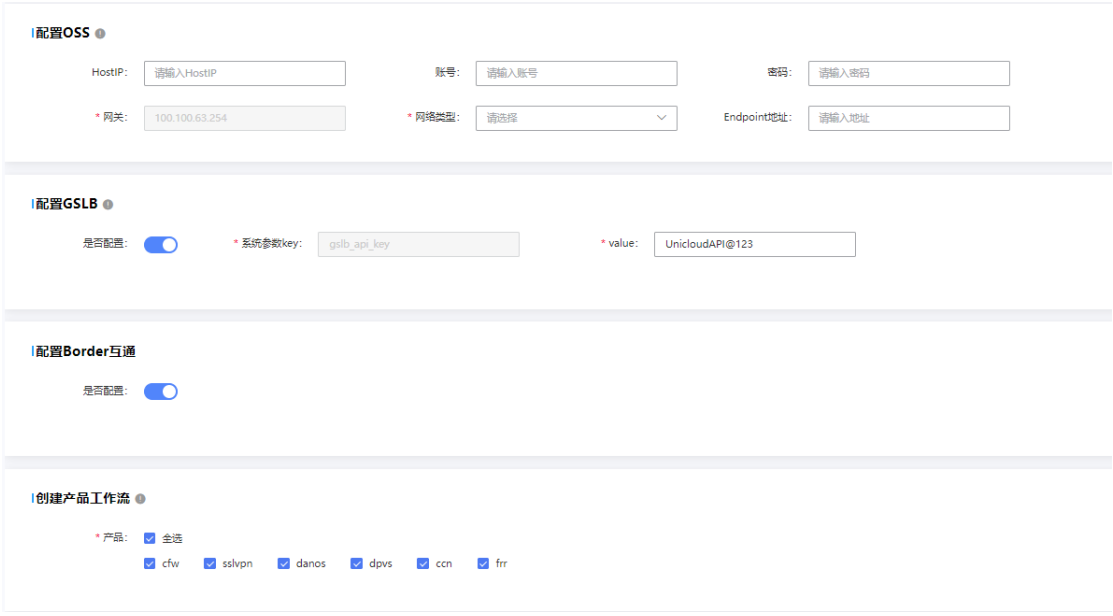
租管互通配置如下。

参数说明如下。

- ①管理网配置，默认已填充数据。
- ②为 PaaS 服务相关的地址和端口，默认地址为 uca-dbaas-nginx-service，默认端口为 40621。若无特殊情况，无需修改
- ③默认为 100.100.0.0/24，作用是承载网络业务的虚拟机的管理网安全组规则。

(4) 第二页主要涉及 4 部分改动。

PaaS 类服务镜像一般从 OSS 下载，OSS 位于公共服务区。



参数说明如下。

- 配置 OSS

参数	说明
Endpoint地址	OSS的访问域名（注意确定是内网访问还是外网访问）
HostIP	公共服务区OSS服务的IP地址
网关	租管互通网段设置的网关，自动填充

网络类型	public：公网访问 private：内网访问（若内网访问，HostIp需填入一个ping不通的ip地址）
账号	OSS对象存储的accessKey
密码	OSS对象存储的secretKey

OSS 相关配置可参考 7.4 对象存储初始化部分所述配置。

- 配置 GSLB：默认打开，使用默认值即可。
- 配置 Border 互通：若当前环境规划无防火墙设备，需要打开此开关。
- 创建产品工作流：保存对应产品创建工作流模板，默认全选。

(5) 配置网络类型：保持默认数据。

(6) 确认填写无误后，点击<完成>即发起创建节点任务流。

如需查看任务流进度，请参考“6. 纳管日志”。

2. 主 AZ 纳管

注意

纳管 AZ 需要填写的参数较多，且没有保存配置功能，请规划好 OMC 账户超时登出时长，以免配置过程中账户登录超时自动登出。且 OMC 的用户不支持多人同时使用，请提示用户避免账户被挤登出。

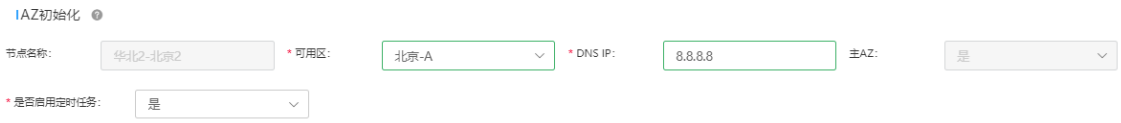
主 AZ 纳管前，请确保运营平台配置了对应 azid，且对应节点纳管完毕。

(1) 登录 OMC 运维管理系统，选择[基础设施平台/云网络]，进入云网络页面。

(2) 在基础设施平台导航中，选择[云网络/初始化配置/可用区网络纳管]。

(3) 点击<配置可用区>进入配置页面。

(4) 配置 AZ 初始化参数。



参数说明如下。

参数	说明
节点名称	自动填充，不可修改。
可用区	可用区已经预配置，从下拉列表中选择即可。
DNS IP	若当前环境有dns服务器，填写对应服务器业务IP，多个Ip以英文半角逗号分隔； 若没有dns服务器，可以填写8.8.8.8,114.114.114.114。
主az	第一个纳管的AZ默认是主AZ，自动填充。
定时任务	slb、dpvs、eip等的监控定时任务启动开关。

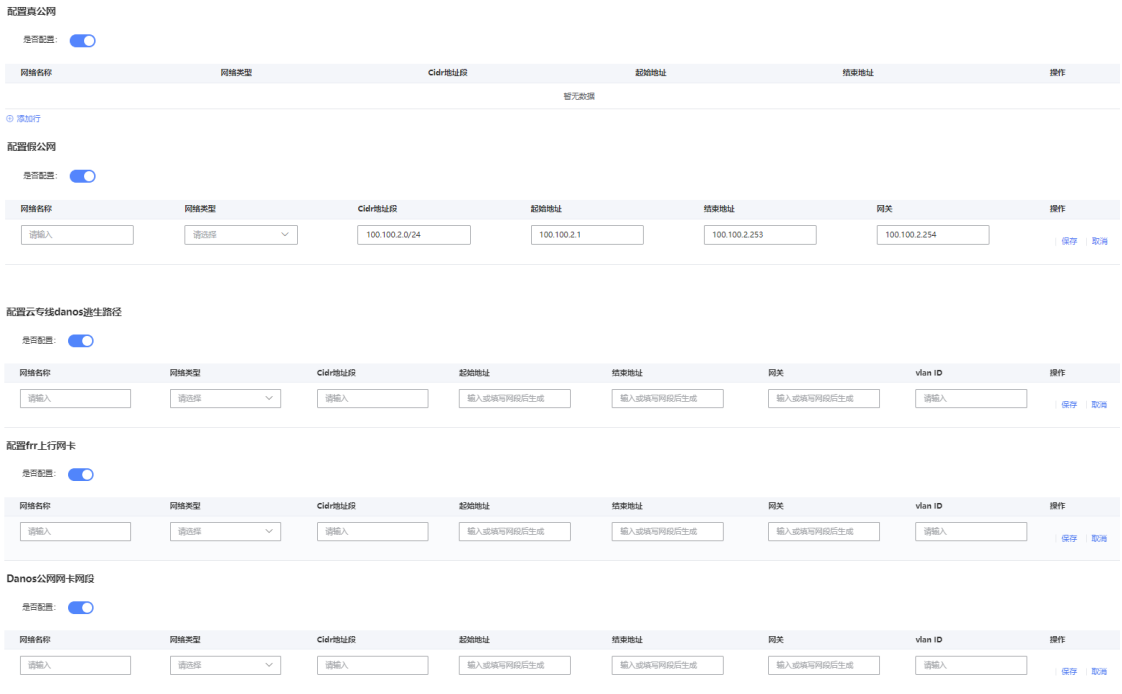
说明

第一个纳管的 AZ 默认为主 AZ，需选择对应可用区名称。

(5) 配置 IPV4 地址池初始化。

如果不需要配置某项，则点击<是否配置>开关，关闭配置项。

如果需要配置某项，点击<是否配置>开关，开启配置项，并点击<添加行>，输入对应参数，点击<保存>，即配置完毕。

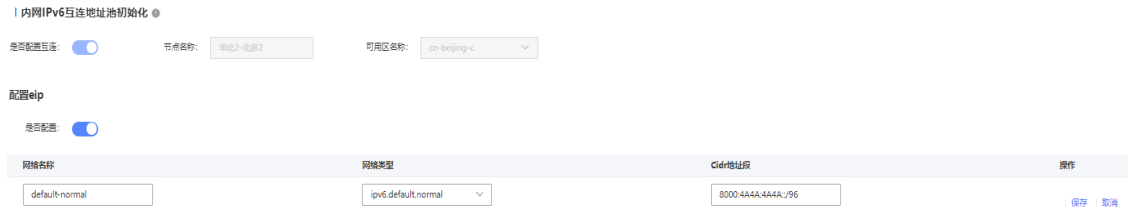


参数说明如下。

参数	说明
真公网	租户EIP、NAT网关的公网IP地址
假公网	租户内网NAT网关IP地址
云专线danos逃生路径	配置云专线danos逃生路径，danos网关环境中需要配置
Frr上行网卡	配置Frr上行网卡，danos网关环境中需要配置
Danos公网网卡	Danos软网关网卡上行公网网段，danos网关环境中需要配置
网络名称	名称命名无特殊要求，默认为类型。例： bgp-static
网络类型	下拉选，真公网需要与o层确定具体类型； 其他为单选
子网信息	填写CIDR地址段后，起止地址及网关自动填充，若与实际规划不一致，可自行修正。 真公网不设置网关；

	VLAN ID 需要按照实际配置填写。

(6) 配置 IPv6 互连地址池初始化。



若当前环境有规划 IPv6 的 EIP，需要在此处纳管：

打开<配置开关>，点击<添加行>,如示例填写规划 IPv6 地址段，点击<保存>；

请注意，IPv6 地址段的掩码位数必须**不大于 96**。

若无规划，关闭配置开关即可。

(7) 配置设备。

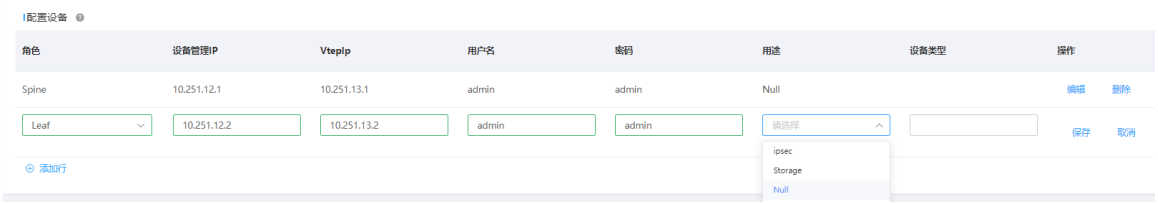
需要同步的设备：Leaf、Border、Spine、FW、管理交换机，Ipsec Leaf，存储 Leaf 等。

点击<添加行>，填写设备信息。

点击<保存>，保存该条设备信息，若填写错误，点击<编辑>进行修改，修改完毕，点击<保存>。

注意

此处设备纳管情况将直接影响后续纳管环节，请仔细确认。



参数说明如下。

参数	说明
角色	设备角色(Spine/Leaf/Firewall/Border/Manage)
设备管理IP	设备IP
VtepIp	loopback IP
用户名	登录设备的用户名
密码	登录设备的密码
用途	internet/intranet/ipsec/Storage/Manage/business (备注：

	Firewall:internet/intranet/ipsec/l3route **Border**:internet/intranet/l3route **Leaf**:ipsec/Storage/Manage/business **spine**:business)
设备类型	设备标识，默认为空。若 FW 类型为 M9K 系列或者 F5080D 或者 F5030D，device_type 填为 M9006；其他设备保持默认，不需要修改

(8) 同步 AZ-RT 信息

无需填写，根据纳管可用区个数自增。

(9) IPSec Leaf 逻辑口集合

当前环境规划专线区，且纳管 ipsec leaf ， 需要打开此配置。

(10) 存储 Leaf-公网网络

点击<添加存储 Leaf-公网网络配置>，展开交换机和后端信息填写页面，示例如下。

图6-2 存储 Leaf 纳管示例图

图6-3 存储 Leaf 绑定公网网络示例图

如果存在多组存储设备，可以点击<添加存储 Leaf-公网网络配置>继续添加。

参数说明如下。

参数	说明
存储交换机管理Ip	存储交换机管理IP
公网网络类型	需要纳管的网络类型
序号	当存在多个相同的公网网络类型时，需要增加序号做区分。默认从0开始，公网类型序号不能重复
存储网网段	存储网网段的cidr、起止地址和网关配置
存储后端信息	存储后端服务器地址、端口号、网段和角色，存在多个服务器点击<添加行>增加

(11) 配置 VLAN 池

与设备纳管关联，数值固定。

(12) 同步 Border-Fw

与设备纳管关联，存在 border 和 fw 设备即默认打开，无法修改。

(13) Border 内网信息

配置 Border 的内网信息(Internet Border、Intranet Border 及 l3route Border 分别配置)。图例只配置了 internet 的。

说明

如果当前环境有规划并纳管 IPSec VPN，则需要增加配置 IPSec 的虚拟设备管理网。

当环境有规划 IPv6 EIP 时，需要给 internet-border 配置 IPv6 的安全外网和租户承载网。

IPv6 的安全外网和租户承载网的网段子网掩码位数必须不大于 96。

参数说明如下。

参数	说明
设备用途	internet、intranet、ipsec或l3route
内网网段cidr	租户承载网、安全外网、虚墙管理网网段
起始IP	租户承载网、安全外网、虚墙管理网分配的起始IP
结束IP	租户承载网、安全外网、虚墙管理网分配的结束IP
网关	租户承载网、安全外网、虚墙管理网的网关
内网类型	TENANT_SUPPORT：租户承载网 SEC_EXTERNAL：安全外网 NGFW_MANAGE_EXTERNAL：带外方式 虚拟设备管理网 NGFW_MANAGE：带内方式 虚拟设备管理网 SEC_EXTERNAL_IPV6：IPV6安全外网 TENANT_SUPPORT_IPV6：IPV6租户承载网

(14) 出口路由器信息

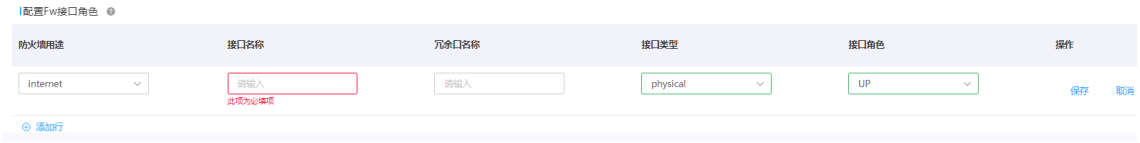
点击<添加行>增加一条数据，填写并检查完毕，点击<保存>。

参数说明如下。

参数	说明
路由器设备管理IP	路由器设备管理IP
路由器用户名	登录路由器设备的用户名
路由器密码	登录路由器设备的密码
下行口名称	路由器下行口
上行口名称	路由器上行口，物理口或者RAGG口 不能是BAGG口
是否支持流量统计	是否支持统计功能(目前SR66型号不支持)

(15) 配置 Fw 接口角色

为纳管设备时纳管的实墙配置上行口、下行口和管理口，点击<添加行>添加数据。

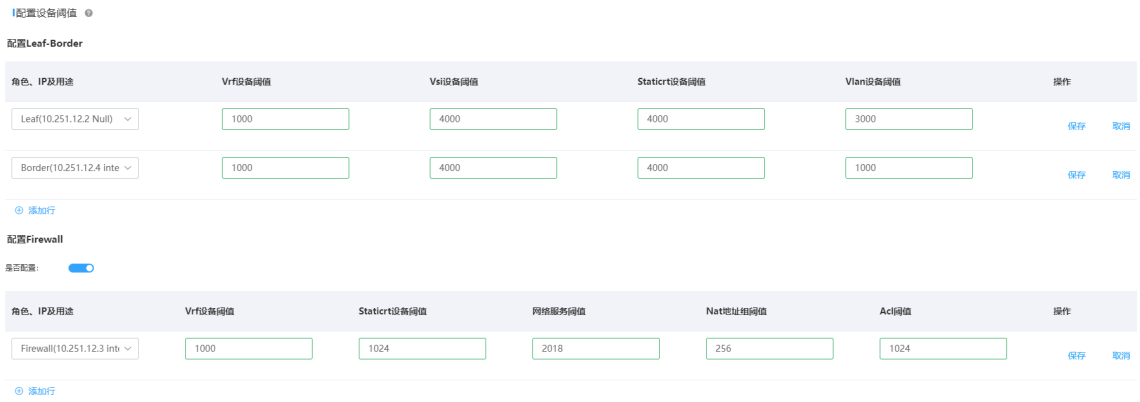


参数说明如下。

参数	说明
防火墙用途	internet、intranet或ipsec
接口名称	设备对应的上下行和管理口的接口名称（若为冗余口，需写其成员口中的一个）
冗余口名称	无冗余口置空
接口类型	物理口或者逻辑口
接口角色	上行口、下行口、管理口

(16) 配置设备阈值

配置设备纳管的 Leaf、Border 和 Firewall 需要在这里配置阈值。



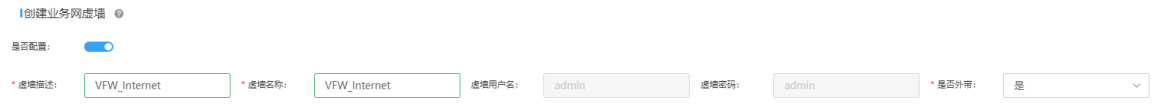
参数说明如下。

参数	说明
角色、IP及用途	分别为配置设备时对应角色的设备信息。
Vrf设备阈值	默认1000
Vsi设备阈值	默认4000
Staticrt设备阈值	Leaf设备和Border设备默认4000， Firewall设备默认1024
Vlan设备阈值	Leaf设备默认3000， Border设备默认1000
网络服务阈值	默认2048
Nat地址组阈值	默认256
Acl阈值	默认1024

(17) 创建虚墙

包括业务网虚墙、假公网虚墙、ipsec 虚墙和三层路由（l3route）虚墙，只有在配置设备时，纳管对应用途的防火墙和 Border（ipsec 为 Leaf）时，才会出现创建对应虚墙的页签。

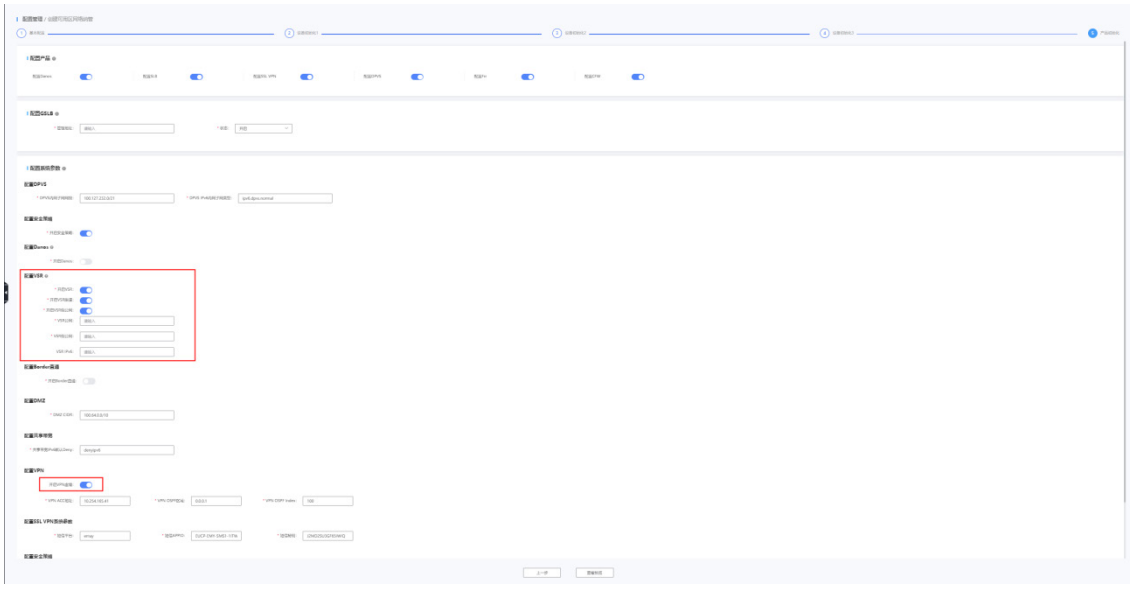
以业务网虚墙为例：

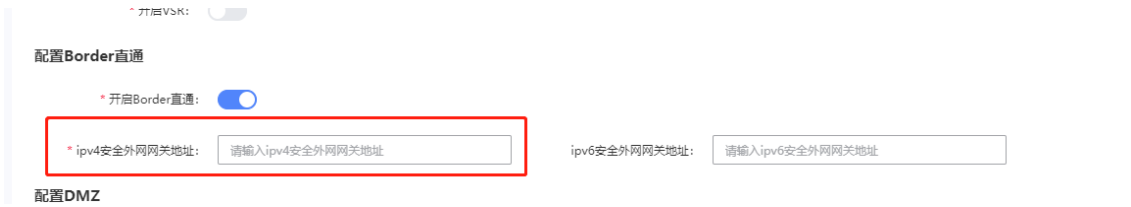


参数说明如下。

参数	说明
虚墙描述	虚墙的描述，建议携带对应角色
虚墙名称	虚墙的名称，建议携带对应角色
虚墙用户名和密码	该实墙设备的用户名和密码，不可修改
是否带外	需与该墙配置虚拟设备管理网时的设置保持一致

(18) 系统参数配置页





参数说明如下。

参数	说明
配置产品	默认全部勾选，需保持默认
配置GSLB	GSLB配置，若无此功能，管理地址写http://www.baidu1.com，开关打开
配置dpvs	推荐默认填充配置
配置安全策略	控制vpc、bfw、三层路由安全策略等向虚墙下的配置。开启即下发安全策略配置。
配置danos	若为danos软网关环境，danos开关需要打开，其他开关视环境规划配置
配置VSR	• 开启 VSR：若为 VSR 软网关环境，VSR 开关需要打开，与 danos 开关互斥，VSR 环境下必须打开此开关。 • 开启 VSR 限速：需要打开。 • 开启 VSR 假公网：根据需求打开。 • VSR 公网：VSR Internet 接口上联 TOR 接口的 IPV4 VRRP 虚地址。 • VSR 假公网：VSR Intranet 接口上联 TOR 接口的 IPV4 VRRP 虚地址。 • VSR IPv6：VSR Internet 接口上联 TOR 接口的 IPV6 VRRP 虚地址。
配置Border直通	若节点纳管Border互通开关打开，此处需要打开开关并填写如下参数： • ipv4 安全外网网关地址：按照建设规划填写。 • Ipv6 安全外网网关地址：按照建设规划填写。

配置DMZ	DMZ区业务网段
配置三层路由网段	新三层路由需要配置的外网大段，支持多个，英文半角逗号分隔
配置共享带宽	推荐默认填充配置
配置VPN	推荐开关打开，默认配置
配置SSL VPN系统参数	推荐默认填充配置
配置BFW系统参数	推荐默认填充配置

(19) 点击<查看预览>弹出窗口，检查所填数据是否正确。

若有填写错误，点击对应模块<编辑>按钮，跳转到修改页面进行修改。

(20) 确认填写无误后点击<确认提交>，发起可用区纳管任务工作流。

如需查看任务流进度，请参考“6. 纳管日志”。

3. 从 AZ 纳管

配置从 AZ 纳管前，请确保当前环境已经纳管过一个或者多个可用区。

(1) 登录 OMC 运维管理系统，选择[基础设施平台/云网络]，进入云网络页面。

(2) 在基础设施平台导航中，选择[云网络/初始化配置/可用区网络纳管]。

(3) 点击<配置可用区>进入配置页面。

(4) 配置 AZ 初始化

参数说明如下。

参数	说明
节点名称	RegionId 默认填充，不可修改。
可用区	可用区已经预配置，从下拉列表中选择即可。
DNS IP	若当前环境有dns服务器，填写对应服务器业务IP，多个Ip以英文半角逗号分隔； 若没有dns服务器，可以填写8.8.8.8,114.114.114.114
主AZ	否
K8sVip	从az的uca-k8s-vip
是否启用定时任务	是

(5) 其他部分可参考主 AZ 纳管，若从 AZ 组网与主 AZ 有差异，请以实际情况为准。

4. 从 AZ 相关改造

自动化部署工具暂时不支持多 AZ 部署，所以 UCA-Network 未进行适配。使用自动部署工具部署的从 AZ，需要进行手动改造。通过 OMC 运维管理平台提交网络初始化任务之后，如果查看纳管任务日志时，流程 singleAzInitialize 中任务 SyncDevice 失败，需要参考如下步骤进行改造。

部署脚本请从版本发布路径下获取：全量包\云服务组件包\IAAS\uca-network\从 AZ 部署指导.zip。请将压缩包下载到本地，解压缩后获取各部署脚本。

说明

实际环境中的 Region ID 和 AZ ID 可能为大写字母，或者小写字母。但是在从 AZ K8S 网络服务的 ingress 文件中，使用的统一是小写字母。

假设环境中 Region ID 和 AZ ID 如下。

- Region ID：hz-hzid-region
- AZ1 ID：hz-region-az1
- AZ2 ID：hz-region-az2

(1) 数据库初始化改造

执行 sql 文件对初始化网络服务需要的数据库，文件路径：sql/init

按照顺序，依次执行此目录下的 sql 文件。

目标数据库：从 AZ 的 mysql 数据库。

(2) 服务改造

从 AZ UCA K8S 集群上，网络服务需要部署的共计 6 个，需要注意的是，uca_base 也需要部署：

- uca-network-core-agent
- uca-network-extension-agent
- uca-network-ops-agent
- uca-network-core-driver
- uca-network-monitor-driver
- uca-network-ops-manager-driver

其他产品服务，不在本指导手册范围内。

a. 如果以下服务也存在于从 AZ 的 UCA K8S 上，可以将其删除，包括 deployment、service、和 ingress。

- uca-iaas-scheduler
- uca-network-api
- uca-network-common-ecs
- uca-network-core-basic
- uca-network-meter
- uca-network-ops-manager-basic

- uca-network-resource-inspection
- uca-network-slb

b. 三个 driver 服务的 deployment 文件需要重新部署。

文件路径：deployment

uca-network-core-driver-deploy.yaml

uca-network-monitor-driver-deploy.yaml

uca-network-ops-manager-driver-deploy.yaml

请注意：如果 region id 不是 hz-hzid-region，请将三个文件中的 hz-hzid-region 替换为正确的 region id

uca-network-core-driver-deploy.yaml 文件中，请将 v4.1.3_E7108_RC2-0002 替换为 v4.1.3_E7108_RC2-1003

uca-network-monitor-driver-deploy.yaml 文件中，请将 v4.1.3_E7108_RC2-0001 替换为 v4.1.3_E7108_RC2-1002

uca-network-ops-manager-driver-deploy.yaml 文件中，请将 v4.1.3_E7108_RC2-0002 替换为 v4.1.3_E7108_RC2-1002

c. 六个网络服务的 ingress 文件需要重新部署

文件路径：ingress

uca-network-core-agent-ingress.yaml

uca-network-extension-agent-ingress.yaml

uca-network-ops-agent-ingress.yaml

uca-network-core-driver-ingress.yaml

uca-network-monitor-driver-ingress.yaml

uca-network-ops-manager-driver-ingress.yaml

请注意：如果 region id 和 az id 与本指导示例不同，请将三个文件中的 hz-hzid-region 和 hz-hzid-az1 分别替换为正确的 region id 和 az id，优先替换 az id。

(3) 数据库改造 tbl_az_driver_ip_port

uni_network_basic 库 tbl_az_driver_ip_port 表

该表中，关于 hz-region-az2 的 driver_ip_port 列数据需要修改。

纳管后，hz-region-az2 的 driver_ip_port 都是 ip+端口形式，需要根据实际情况改成 ingress 域名访问。

a. 访问 driver 服务和 Agent 服务

执行 SQL 文件进行修改，请按照实际的环境信息修改变量。文件路径：sql/update

请注意：如果 region id 和 az id 与本指导示例不同，请将 sql 文件中的变量 region_id 和 az_id 分别替换为正确的 region id 和 az id，优先替换 az id。

目标数据库：主 AZ 的 MySQL 数据库。

b. 租管互通访问

用于租管互通的端口为 40621 的租管互通服务，需要根据实际情况进行修改

请根据以下情况，选择要执行的 SQL，三选一。

目标数据库：主 AZ 的 MySQL 数据库。

- 从 AZ 使用与主 AZ 相同的租管互通集群

  ```
  UPDATE `uni_network_basic`.`tbl_az_driver_ip_port` SET `driver_ip_port`=
  'http://uca-dbaas-nginx-service:40621' WHERE (az_id = @az_id AND driver_type = 3 AND
  is_deleted = 0);
  ```

- 从 AZ 使用单独的租管互通集群，且 nginx service 为 ClusterIP 类型

  在租管互通集群中，获取 nginx service 对应的 ingress 域名（kubectl get ingress | grep nginx-service）。

  ```
  UPDATE `uni_network_basic`.`tbl_az_driver_ip_port` SET `driver_ip_port`=
  'http://nginx-service' WHERE (az_id = @az_id AND driver_type = 3 AND is_deleted = 0);
  ```

  其中，*http://nginx-service* 为实际环境中的 ingress 域名。

- 从 AZ 使用单独的租管互通集群，且 service 为 NodePort 类型

  ```
  UPDATE `uni_network_basic`.`tbl_az_driver_ip_port` SET `driver_ip_port`=
  'http://172.40.150.60:40621' WHERE (az_id = @az_id AND driver_type = 3 AND is_deleted
  = 0);
  ```

  其中，172.40.150.60 为租管互通集群 K8S VIP，请替换为实际环境中的值。

c. 边缘 AZ

  如果本从 AZ 是边缘 AZ，需要执行以下 SQL：

  ```
  UPDATE `uni_network_basic`.`tbl_az_driver_ip_port` SET `driver_ip_port`=
  'http://uca-center-edge-service.uca.region.unicloud.space' WHERE (az_id = @az_id
  AND driver_type = 5 AND is_deleted = 0);
  ```

(4) 定时任务

请根据环境信息，替换加粗内容，在主 AZ 的 UCA K8S 中依次执行下面三个 CURL 命令。

```
curl -X POST "http://{主 AZ UCA K8S VIP}:40444/uca/iaas/scheduler/v1.0/schedule/delete"
-H "accept: */*" -H "Content-Type: application/json" -d '{"Force": true, "service_name":
"network", "task_names":
[ "save_device_config_schedule_hz-region-az2","floatingip_monitor_schedule-hz-region-az
2" ]}'
```

```
curl -X POST "http://{主 AZ UCA K8S VIP}:40444/uca/iaas/scheduler/v1.0/schedule/create"
-H "accept: */*" -H "Content-Type: application/json" -d
'{"schedule_task_info":[{"description":"定时保存设备配置信息","schedule_cron":"0 0 1 *
* ?","service_name":"network","task_name":"save_device_config_schedule_hz-region-az2"
,"trigger_url":"http://uca-network-ops-manager-driver.hz-region-az2.hz-hzid-region.unicl
oud.space/uca/network/v1.0/audit/configure/save/schedule","type":"SYSTEM"}]}'
```

```
curl -X POST "http://{主 AZ UCA K8S VIP}:40444/uca/iaas/scheduler/v1.0/schedule/create"
-H "accept: */*" -H "Content-Type: application/json" -d
'{"schedule_task_info":[{"description":"弹性公网 IP 的流量定时监控","schedule_cron":"0
0/5 * *
* ?","service_name":"network","task_name":"floatingip_monitor_schedule-hz-region-az2"
,"trigger_url":"http://uca-network-monitor-driver.hz-region-az2.hz-hzid-region.unicloud.
space/uca/network/monitor/v1.0/schedule","type":"SYSTEM"}]}'
```

5. 修改 coredns

(1) 若当前节点有多个 AZ，需要修改主从 UCA 集群的 coredns，分别在主从节点上追加域名，主追加从，从追加主，若有错误，请注意修改。域名规则为：*.[az_id].[region_id].unicloud.space.

```
apiVersion: v1
data:
  Corefile: |
    .:53 {
        errors
        ready
        health
        kubernetes cluster.local in-addr.arpa ip6.arpa {
            pods insecure
            fallthrough in-addr.arpa ip6.arpa
        }
        file /etc/coredns/unicloud.db unicloud.space
        prometheus :9153
        forward . /etc/resolv.conf
        cache 30
        reload
        loadbalance
        hosts {
          172.40.150.50 w-3306-mysql.service.consul
          100.66.1.110 ucm.agent.unicloud.com
          100.66.1.185 1.hzoss.unicloud.com
          fallthrough
        }
    }
  unicloud.db: |
    ; example.org test file
    unicloud.space.            IN      SOA     sns.dns.icann.org. noc.dns.icann.org. 2015082541 7200 3600 1209600 3600
    *.uco.unicloud.space.            IN      A       172.40.150.70
    *.taag.unicloud.space.            IN      A       172.40.150.60
    *.omc.unicloud.space.            IN      A       172.40.150.120
    *.uca.hz-hzid-region.unicloud.space.        IN      A       172.40.150.40
    *.hz-region-az1.hz-hzid-region.unicloud.space.        IN      A       172.40.150.40
    *.hz-region-az2.hz-hzid-region.unicloud.space.        IN      A       172.40.151.40
kind: ConfigMap
metadata:
  annotations:
```

```
[root@HZ-AZ2-TO2-UCA-K8S-01 ~]# kubectl edit cm coredns -n kube-system -o yaml
apiVersion: v1
data:
  Corefile: |
    .:53 {
        errors
        ready
        health
        kubernetes cluster.local in-addr.arpa ip6.arpa {
            pods insecure
            fallthrough in-addr.arpa ip6.arpa
        }
        file /etc/coredns/unicloud.db unicloud.space
        prometheus :9153
        forward . /etc/resolv.conf
        cache 30
        reload
        loadbalance
        hosts {
          172.40.151.50 w-3306-mysql.service.consul
          100.66.1.110 ucm.agent.unicloud.com
          100.66.1.184 1.hzoss.unicloud.com
          fallthrough
        }
    }
  unicloud.db: |
    ; example.org test file
    unicloud.space.            IN      SOA     sns.dns.icann.org. noc.dns.icann.org. 2015082541 7200 3600 1209600 3600
    *.uco.unicloud.space.            IN      A       172.40.150.70
    *.taag.unicloud.space.            IN      A       172.40.150.60
    *.omc.unicloud.space.            IN      A       172.40.150.120
    *.uca.hz-hzid-region.unicloud.space.        IN      A       172.40.150.40
    *.hz-region-az2.hz-hzid-region.unicloud.space.        IN      A       172.40.151.40
    *.hz-region-az1.hz-hzid-region.unicloud.space.        IN      A       172.40.150.40
kind: ConfigMap
```

(2) 执行如下命令，重启 coredns 和 deploy 控制器使配置生效。

```
kubectl rollout restart deploy coredns –n kube-system
```

6. 纳管日志

(1) 登录 OMC 运维管理系统，选择[基础设施平台/云网络]，进入云网络页面。

(2) 在基础设施平台导航中，选择[云网络/初始化配置/网络纳管日志]。

图6-4 纳管日志页面

(3) 点击流程 ID 链接，进入对应流程具体步骤运行状态。

任务状态全部显示成功，则表示网络设备纳管完毕。

若出现失败步骤，需要进行定位修正，修正完毕后，点击图 6-5 中对应流程后边的重试按钮，进行流程重试。

图6-5 纳管日志任务流程详情页

6.3.3 纳管 IPv6 网络

若纳管流程中未进行 IPv6 网络相关的配置，需要进行如下操作，进行单独纳管；若已经对 IPv6 网络相关配置进行纳管，则只需执行“4. OMC 页面打开 IPv6 开关”步骤。

进入 UCA-K8S，查询 uca-network-ops-manager-basic-service 的 ip（下面称 ops-basic-svc-ip）以及 uca-network-ops-manager-driver-service 的 IP（下面称 ops-driver-svc-ip）

执行如下命令：

```
kubectl get svc | grep ops-manager-basic
kubectl get svc | grep  ops-manager-driver
```

1. IPv6 EIP 纳管

规划好 IPv6 EIP 网段后，需执行如下 CURL 命令，在 UCA 任意节点执行即可。

```
curl -X POST "http://{ops-basic-svc-ip}:40496/uca/network/v1.0/ipv6/networks/create" -H "accept: */*" -H "Content-Type: application/json" -d '{"Networks":[{"AzId":"AZ 值
```

```
","NetworkName":"ipv6-network","NetworkPrefix":"IPv6 地址前缀
","NetworkType":"ipv6.default.normal","PrefixDigits":掩码位数,"RegionId":"Region 值"}]}'
```

其中，ops-basic-svc-ip、AZ 值、IPv6 地址前缀、掩码位数、Region 值请替换为实际环境中的值；且掩码位数必须**不大于 96**。例如：

```
curl -X POST "http://172.16.150.30:40496/uca/network/v1.0/ipv6/networks/create" -H "accept:
*/*" -H "Content-Type: application/json" -d
'{"Networks":[{"AzId":"H3C-HZ-AZ1","NetworkName":"ipv6-network","NetworkPrefix":"2408:80
e0:4100:51","NetworkType":"ipv6.default.normal","PrefixDigits":65,"RegionId":"H3C-HZ"}]}
'
```

2. Border 内网纳管

(1) 登入当前环境数据库，uni_network_driver 库,执行如下 sql，查询 internet border 的 device_id，并记录查询到的 device_id 值。

```
USE uni_network_driver;
select device_id from tbl_devices where device_use= 'internet' and role = 'Border';
```

(2) 在 UCA K8S 中执行如下 CURL 命令：

```
curl -X POST
"http://{ops-driver-svc-ip}:40486/uca/network/v1.0/basic_device_info/border_interna
l_ip_pool/create" -H "accept: */*" -H "Content-Type: application/json" -d
'{"ip_pools":[{"border_device_id":"查询到的 device_id 值","cidr":"租户承载网地址
","end_ip":"","gateway_ip":"2408:80e0:4000:51::1","name":"TENANT_SUPPORT_IPV6","sta
rt_ip":"","type":"TENANT_SUPPORT_IPV6"},{"border_device_id":"查询到的 device_id 值
","cidr":"安全外网地址
","end_ip":"","gateway_ip":"2408:80e0:4000:51:0:1::1","name":"SEC_EXTERNAL_IPV6","s
tart_ip":"","type":"SEC_EXTERNAL_IPV6"}]}'
```

其中，ops-driver-svc-ip、查询到的 device_id 值、租户承载网地址、安全外网地址，需分别替换为实际环境中的值。例如：

```
curl -X POST
"http://172.16.150.40:40486/uca/network/v1.0/basic_device_info/border_internal_ip_p
ool/create" -H "accept: */*" -H "Content-Type: application/json" -d
'{"ip_pools":[{"border_device_id":"8cea1c50b4e5461fbe5a15d344adab07","cidr":"2408:8
0e0:4000:51::/96","end_ip":"","gateway_ip":"2408:80e0:4000:51::1","name":"TENANT_SU
PPORT_IPV6","start_ip":"","type":"TENANT_SUPPORT_IPV6"},{"border_device_id":"8cea1c
50b4e5461fbe5a15d344adab07","cidr":"2408:80e0:4000:51:0:1::/96","end_ip":"","gatewa
y_ip":"2408:80e0:4000:51:0:1::1","name":"SEC_EXTERNAL_IPV6","start_ip":"","type":"S
EC_EXTERNAL_IPV6"}]}'
```

3. 修改数据库系统表数据

打开当前环境数据库 uni_network_basic 库，修改 azid 为当前纳管可用区 azid，执行如下 sql：

```
USE uni_network_basic;
SET @azid = 'cn-beijing-c';
INSERT INTO `uni_network_basic`.`tbl_system_parameter`(`zone_id`, `parameter_key`,
`parameter_value`, `is_deleted`) VALUES ( @azid, 'ipv6_subnet_prefix', '96', 0);
INSERT INTO `uni_network_basic`.`tbl_system_parameter`(`zone_id`, `parameter_key`,
`parameter_value`, `is_deleted`) VALUES ( @azid, 'ipv6_default_type', 'ipv6.default.normal',
0);
```

上述命令中，cn-beijing-c 请修改为实际环境的 azid。

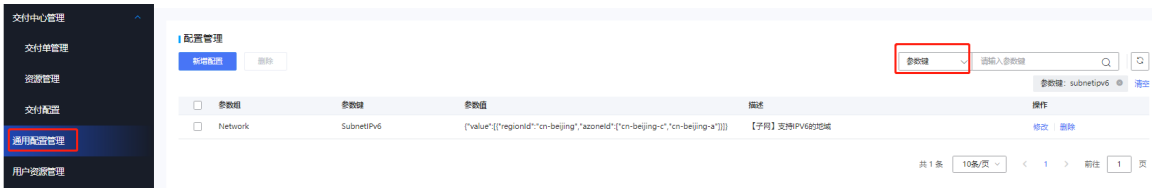
当 IPv6 EIP 地址段子网掩码为 96 时，上述 sql 中的 96 需要改为 112。即需要保证 IPv6 公网网段能正常分配子网，且对应子网能正常分配 IPv6 地址。

4. OMC 页面打开 IPv6 开关

(1) 登录 OMC 运维管理平台，选择[用户控制台/产品控制台/通用配置管理]。

(2) 在页面右上方下拉选项中进行筛选，筛选出参数键为 SubnetIPv6 的选项。

(3) 查出<支持 IPV6 的地域>，点击修改，增加对应可用区 id，点击提交即可。详情如图：



6.4 纳管镜像服务器

6.4.1 纳管镜像服务器

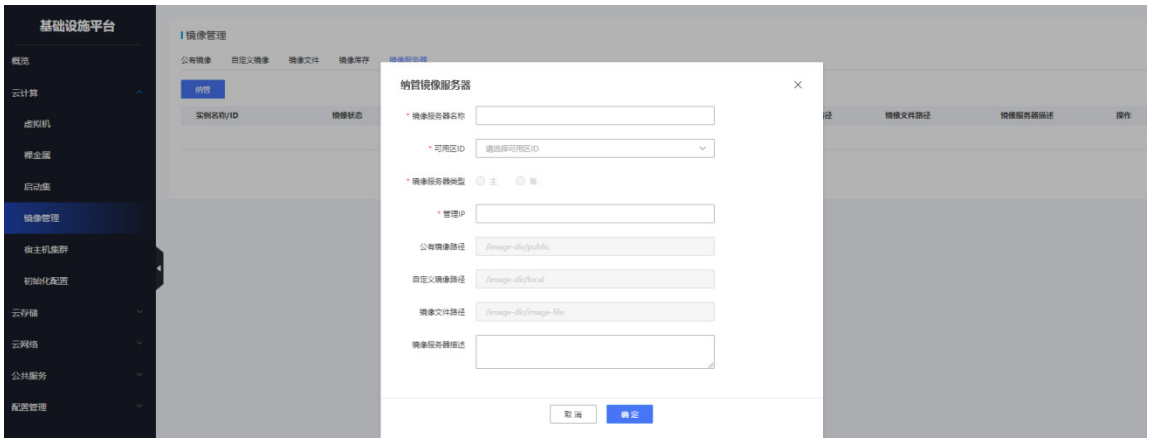
(1) 登录 OMC 运维管理平台，点击页面左上方的  ，选择[IAAS/基础设施平台]。

(2) 在基础设施平台导航栏中，选择[云计算/镜像管理]。

(3) 选择[镜像服务器]页签，进入镜像服务器纳管页面。

(4) 单击<纳管>按钮，在纳管镜像服务器对话框中，填写镜像服务器名称、镜像服务器 IP 和镜像服务器描述，并选择可用区和主/备镜像服务器，需要注意同一可用区只能纳管一个主镜像服务器。

图6-6 纳管镜像服务器



(5) 单击<确定>完成镜像服务器纳管。

6.4.2 检查服务器目录

检查镜像服务器上是否存在如下目录：

- /image-dir/public
- /image-dir/local

- /image-dir/cache
- /image-dir/image-file

如有缺失需要补全。

6.5 纳管存储设备

6.5.1 3PAR 和 Primera 初始化配置

3PAR 和 Primera 的初始化配置相同，区别为 Primera 存储不支持 HTTP 协议。

下列将以 3PAR 的初始化配置为例进行说明。

1. 开启 WSAPI 服务

登录 3PAR 控制台，依次点击[系统/服务/编辑/WSAPI 服务器]，分别将“服务”、“HTTP”和“HTTPS”设置为“已启用”。

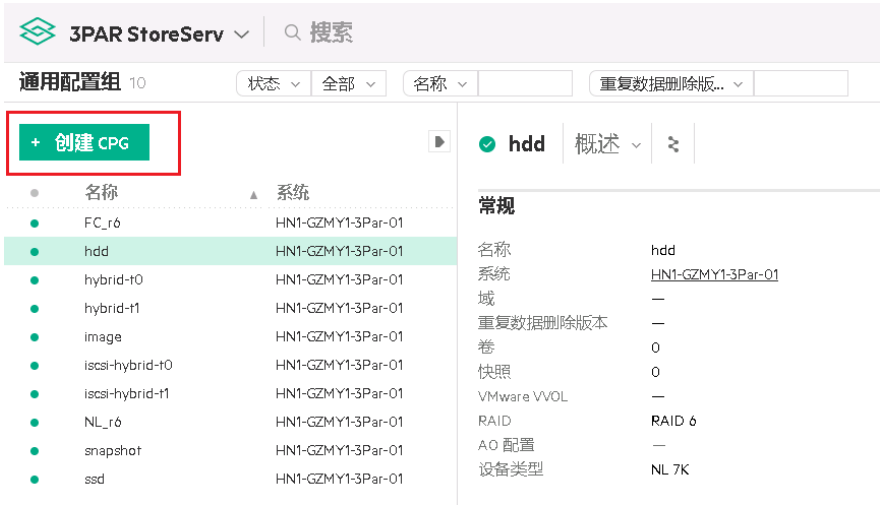
需要注意的是 Primera 存储不支持 HTTP 协议，所以只需将“HTTPS”和“服务”调整为“已启用”，“HTTPS”的状态保持关闭即可。

2. 配置存储池

如果使用的磁盘规格编码是定制规格，非系统默认规格，请参考执行 4.（可选）3PAR 和 Primera 使用定制新规格，否则按以下步骤执行。

(1) 登录 3PAR 控制台，点击“通用配置组”进入通用配置组页面。

(2) 在通用配置组页面，点击<创建 CPG>按钮。（除了 image 和 snapshot，其他的存储池名称都是按磁盘规格名称创建）



(3) 创建 SSD 类型的存储池

如果存储设备配置了 SSD 类型磁盘，创建名称为“ebs.highIO.ssd”、“ebs.iscsi.ssd”和“ebs.share_fc.ssd”的 CPG，参数如下，设备类型和 RAID 类型需要根据 3PAR 实际磁盘配置情况进行调整。

- 当云硬盘类型为 High IO 时

图6-7 配置 High IO 类型云硬盘的 CPG 参数

参数说明：

参数	说明
名称	CPG名称为ebs.highIO.ssd
系统	选择该环境使用存储设备名称
设备类型	根据设备实际配置选择“SSD”、SSD 100K”或“SSD 150K”
RAID类型	根据设备实际配置选择“RAID 6”
可用性	默认选择Cage
其他参数	使用默认值

- 当云硬盘类型为 ISCSI 类型时

图6-8 配置 ISCSI 型云硬盘的 CPG 参数

参数说明：

参数	说明
名称	CPG名称为ebs.iscsi.ssd
系统	选择该环境使用存储设备名称
设备类型	根据设备实际配置选择“SSD”、SSD 100K”或“SSD 150K”
RAID类型	根据设备实际配置选择“RAID 6”
可用性	默认选择Cage
其他参数	使用默认值

- 当云硬盘类型为 share_fc 类型时

创建步骤参数同 ISCSI 类型一样，只需 CPG 名称改为 ebs.share_fc.ssd。

(4) 创建镜像所属 CPG

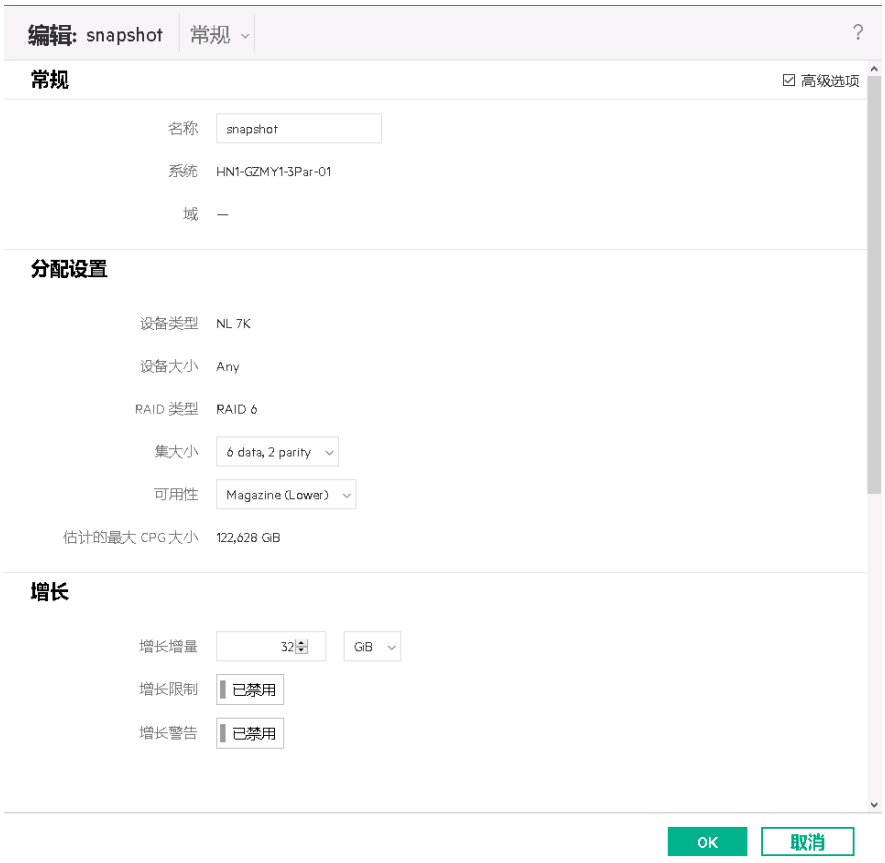
点击<创建 CPG>按钮创建名称为“image”的 CPG，如果配置有 SSD 磁盘，选设备类型为 SSD，如果没有配置 SSD 磁盘，则选择现在有的 FC 或 NL 类型磁盘。

参数说明：

参数	说明
名称	image
系统	选择该环境使用存储设备名称
设备类型	根据设备实际配置选择“SSD”、“FC 10K”、“FC”或“NL”
RAID类型	根据设备实际配置选择“RAID 6”
可用性	默认选择Cage
其他参数	使用默认值

(5) 创建快照所属 CPG

点击<创建 CPG>按钮创建名称为“snapshot”的 CPG，设备类型可选 FC 或 NL 类型磁盘，如果没有慢盘，可以使用 SSD 类型磁盘。



参数说明：

参数	说明
名称	snapshot
系统	选择该环境使用存储设备名称
设备类型	根据设备实际配置选择“SSD”、“FC 10K”、“FC”或“NL”
RAID类型	根据设备实际配置选择“RAID 6”
可用性	默认选择Cage
其他参数	使用默认值

(6) 创建 hybrid 类型存储池

- 如果存储设备上只配置了一种 HDD 类型磁盘（FC 或者 NL），则只需要创建名称为“ebs.hybrid.hdd”、“ebs.iscsi.hdd”和“ebs.share_fc.hdd”的 CPG，根据存储设备磁盘配置情况选择磁盘类型（FC 或 NL）；

参数说明：

参数	说明
名称	ebs.hybrid.hdd、ebs.iscsi.hdd、ebs.share_fc.hdd
系统	选择该环境使用存储设备名称
设备类型	根据设备实际配置选择转速较高的磁盘类型（SSD或FC）
RAID类型	根据设备实际配置选择“RAID 6”
可用性	默认选择Cage
其他参数	使用默认值

- 如果存储设备上既配置了两种以上的磁盘类型，则需要创建名称为“ebs.hybrid.hdd”、“ebs.hybrid.hdd-t1”、“ebs.iscsi.hdd”、“ebs.iscsi.hdd-t1”、“ebs.share_fc.hdd”和“ebs.share_fc.hdd-t1”的 CPG，ebs.hybrid.hdd、ebs.iscsi.hdd、ebs.share_fc.hdd 可根据存储设备磁盘的配置情况选择转速较高的磁盘类型（SSD 或 FC），ebs.hybrid.hdd-t1、ebs.iscsi.hdd-t1、ebs.share_fc.hdd-t1 选择转速较低的磁盘类型（FC 或 NL）。

参数说明：

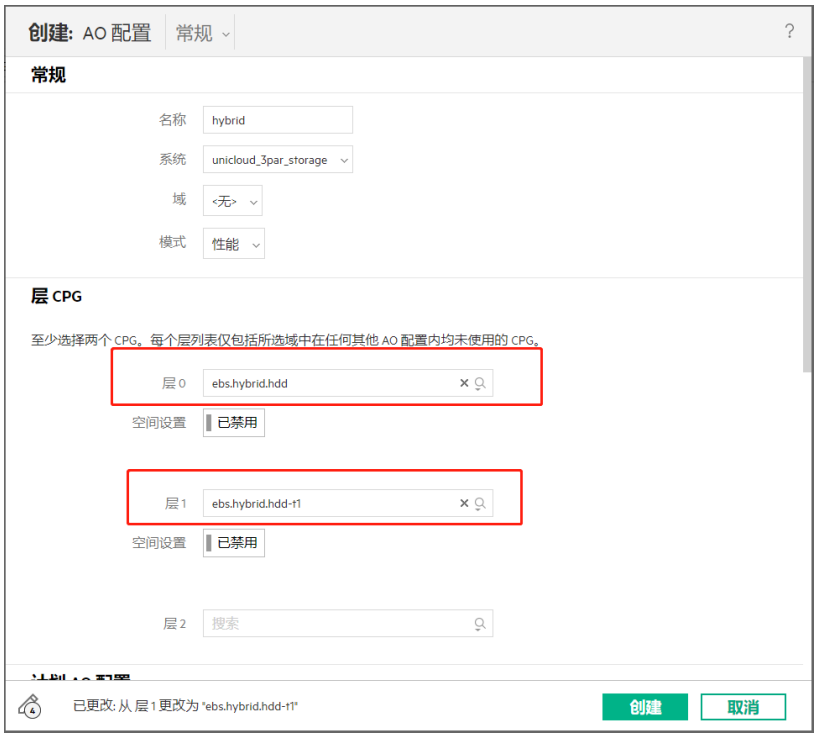
参数	说明
名称	ebs.hybrid.hdd-t1、ebs.iscsi.hdd-t1、ebs.share_fc.hdd-t1
系统	选择该环境使用存储设备名称
设备类型	根据设备实际配置选择转速较低的磁盘类型（FC或NL）
RAID类型	根据设备实际配置选择“RAID 6”
可用性	默认选择Cage
其他参数	使用默认值

(7) 创建“自适应优化”

a. 点击“自适应优化”进入自适应优化配置页面。（存储设备只有一种磁盘类型时不需要创建自适应优化）。

b. 创建名称为“hybrid”、“iscsi-hybrid”和“share_fc-hybrid”的自适应优化，参数如下。

– hybrid



参数说明：

参数	说明
名称	hybrid
系统	选择该环境使用存储设备名称
模式	默认使用“已平衡”选项
层0	选择前面创建好的ebs.hybrid.hdd
层1	选择前面创建好的ebs.hybrid.hdd-t1
层2	不用选择
计划AO配置计划	已启用
计划名称	填写可以识别的ao计划名称，例如ao-for-hybrid
计划模式	每日
开始时间	23：00
其他参数	默认缺省值

– iscsi-hybrid


创建: AO 配置
常规
常规
名称
iscsi-hybrid
系统
unicloud_3par_storage
域
<无>
模式
已平衡
层 CPG
至少选择两个 CPG。每个层列表仅包括所选域中在任何其他 AO 配置内均未使用的 CPG。
层 0
ebs.iscsi.hdd
空间设置
已禁用
层 1
ebs.iscsi.hdd-t1
空间设置
已禁用
层 2
搜索
已更改: 从 层 1 更改为 "ebs.iscsi.hdd-t1"
创建
取消


创建: AO 配置
层 CPG
层 CPG
计划 AO 配置
计划
已启用
设置
最长运行时间
6
小时
无损压缩模式
自动
最小 IOPS
50
分析
分析并优化
数据分析间隔
开始分析
12
小时
优化计划之前
持续时间
12
小时
优化计划
计划名称
ao-for-iscsi-hybrid
警报
任务失败时生成
计划模式
每日
开始时间
23:00
已更改: 从 计划名称 更改为 "ao-for-iscsi-hybrid"
创建
取消

参数说明：

参数	说明
名称	选择iscsi-hybrid
系统	选择该环境使用存储设备名称
模式	默认使用“已平衡”选项
层0	选择前面创建好的ebs.iscsi.hdd
层1	选择前面创建好的ebs.iscsi.hdd-t1
层2	不用选择
计划AO配置计划	已启用
计划名称	填写可以识别的ao计划名称，例如ao-for-hybrid
计划模式	每日
开始时间	23：00
其他参数	默认缺省值

– share_fc-hybrid

操作步骤和参数同 iscsi-hybrid，名称改为 share_fc-hybrid，层 0 和层 1 选择之前创建好的 ebs.share_fc.hdd 和 ebs.share_fc.hdd-t1，其他参数同上。

3. OMC 界面纳管设备

(1) 登录 OMC 运维管理界面，选择[IAAS/基础设施平台]。

(2) 在基础设施平台导航栏中，选择[计算集群管理/存储集群]。

(3) 单击<纳管>按钮，在弹出的纳管存储设备对话框中，配置各项参数。

图6-9 纳管设备

参数说明：

参数	说明
集群名称	输入集群名称
集群类型	包括3PAR、SDS、Primera。这里选择3PAR或Primera
管理接口地址	Primera、曙光存储、宏杉存储、华为分布式存储选择https,其他类型选择http，然后填写存储设备管理IP和端口，3par的端口是8008，Primera是443，曙光存储是8443，宏杉存储是8443，华为分布式存储是8088
通信协议	3PAR、Primera和Nimble选择iscsi或者fc-scsi（需要存储设备和VKS都支持FC协议），SDS选择rbd，其他存储目前都选择iscsi
可用区	选择该设备属于哪个AZ
用户名和密码	登录该存储设备的账号密码

(4) 单击<确定>按钮完成 OMC 界面纳管配置。

4.（可选）3PAR 和 Primera 使用定制新规格

只有新设备使用了定制新磁盘规格编码，才需要按照以下步骤进行操作，如果使用的是常规磁盘规格编码，不需要执行以下步骤。

(1) 在数据库添加新规格

在 A 层存储服务数据库 uni_uca_storage 中的 tbl_disk_spec 中添加新规格数据。

如果新加规格的介质是 SSD 的，则使用以下 sql 脚本，替换**<规格族>**和**<新规格编码(ssd 介质)>**相应值：

```
USE uni_uca_storage;
DROP PROCEDURE IF EXISTS uni_uca_storage.`insertNewDiskSpec`;
delimiter //
CREATE PROCEDURE uni_uca_storage.`insertNewDiskSpec`()
BEGIN

IF NOT EXISTS(SELECT id FROM `uni_uca_storage`.`tbl_disk_spec` WHERE is_deleted = 0 AND `code`='<新规格编码(ssd 介质)>') THEN
INSERT INTO uni_uca_storage.tbl_disk_spec(capacity_min, capacity_max, iops_base, iops_factor, iops_max, bw_base, bw_factor, bw_max, family, code, `usage`, medium, tag, format, feature, is_deleted)VALUES(20, 65536, 1600, 40, 30000, 100, 0.50, 512, '<规格族>', '<新规格编码(ssd 介质)>', 'elastic', 'ssd', NULL, '', '', 0);
END IF;

END//
delimiter ;
CALL uni_uca_storage.`insertNewDiskSpec`();
DROP PROCEDURE IF EXISTS uni_uca_storage.`insertNewDiskSpec`;
```

如果新加规格的介质是 HDD 的，则使用以下 sql 脚本，替换**<规格族>**和**<新规格编码(ssd 介质)>**相应值：

```
USE uni_uca_storage;
DROP PROCEDURE IF EXISTS uni_uca_storage.`insertNewDiskSpec`;
delimiter //
CREATE PROCEDURE uni_uca_storage.`insertNewDiskSpec`()
BEGIN

IF NOT EXISTS(SELECT id FROM `uni_uca_storage`.`tbl_disk_spec` WHERE is_deleted = 0 AND `code`='<新规格编码(hdd 介质)>') THEN
INSERT INTO uni_uca_storage.tbl_disk_spec(capacity_min, capacity_max, iops_base, iops_factor, iops_max, bw_base, bw_factor, bw_max, family, code, `usage`, medium, tag, format, feature, is_deleted)VALUES(20, 65536, 1000, 6, 5000, 50, 0.15, 160, '<规格族>', '<新规格编码(hdd 介质)>', 'elastic', 'hdd', NULL, '', '', 0);
END IF;

END//
delimiter ;
CALL uni_uca_storage.`insertNewDiskSpec`();
DROP PROCEDURE IF EXISTS uni_uca_storage.`insertNewDiskSpec`;
```

(2) 在数据库添加新限速规则

添加完新规格后，在 A 层存储服务数据库 uni_uca_storage 中的 tbl_qos_level 中添加新的限速规则，sql 脚本如下，替换<新规格编码（ssd 介质）>和<新规格编码（hdd 介质）>两个值，添加的规格是哪种介质就替换那种介质的规格编码，如果添加两种，则可以同时替换；

```
 USE uni_uca_storage;
DROP PROCEDURE IF EXISTS uni_uca_storage.`insertQosLevel`;
delimiter //
```

```
CREATE PROCEDURE uni_uca_storage.`insertQosLevel`()
BEGIN
set @ssd_spec:=0;
set @hdd_spec:=0;
SELECT id INTO @ssd_spec FROM tbl_disk_spec WHERE is_deleted = 0 AND `code`= '<新规格编码（ssd 介质）>';
SELECT id INTO @hdd_spec FROM tbl_disk_spec WHERE is_deleted = 0 AND `code`= '<新规格编码（hdd 介质）>';
if (@ssd_spec != 0 AND NOT EXISTS(SELECT id FROM `uni_uca_storage`.`tbl_qos_level` WHERE disk_spec_id = @ssd_spec)) then
INSERT INTO
`tbl_qos_level`(`id`, `disk_spec_id`, `cap_min`, `cap_max`, `iops`, `bw`, `count_max`)
values
(CONCAT(@ssd_spec,'-1'), @ssd_spec, 20, 50, 3600, 128000, 3),
(CONCAT(@ssd_spec,'-10'), @ssd_spec, 290, 320, 14400, 266240, 3),
(CONCAT(@ssd_spec,'-11'), @ssd_spec, 320, 350, 15600, 281600, 3),
(CONCAT(@ssd_spec,'-12'), @ssd_spec, 350, 380, 16800, 296960, 3),
(CONCAT(@ssd_spec,'-13'), @ssd_spec, 380, 410, 18000, 312320, 3),
(CONCAT(@ssd_spec,'-14'), @ssd_spec, 410, 440, 19200, 327680, 3),
(CONCAT(@ssd_spec,'-15'), @ssd_spec, 440, 470, 20400, 343040, 3),
(CONCAT(@ssd_spec,'-16'), @ssd_spec, 470, 500, 21600, 358400, 3),
(CONCAT(@ssd_spec,'-17'), @ssd_spec, 500, 530, 22800, 373760, 3),
(CONCAT(@ssd_spec,'-18'), @ssd_spec, 530, 560, 24000, 389120, 3),
(CONCAT(@ssd_spec,'-19'), @ssd_spec, 560, 590, 25200, 404480, 3),
(CONCAT(@ssd_spec,'-2'), @ssd_spec, 50, 80, 4800, 143360, 3),
(CONCAT(@ssd_spec,'-20'), @ssd_spec, 590, 620, 26400, 419840, 3),
(CONCAT(@ssd_spec,'-21'), @ssd_spec, 620, 650, 27600, 435200, 3),
(CONCAT(@ssd_spec,'-22'), @ssd_spec, 650, 680, 28800, 450560, 3),
(CONCAT(@ssd_spec,'-23'), @ssd_spec, 680, 710, 30000, 465920, 3),
(CONCAT(@ssd_spec,'-24'), @ssd_spec, 710, 740, 30000, 481280, 3),
(CONCAT(@ssd_spec,'-25'), @ssd_spec, 740, 770, 30000, 496640, 3),
(CONCAT(@ssd_spec,'-26'), @ssd_spec, 770, 800, 30000, 512000, 3),
(CONCAT(@ssd_spec,'-27'), @ssd_spec, 800, 65537, 30000, 524288, 3),
(CONCAT(@ssd_spec,'-3'), @ssd_spec, 80, 110, 6000, 158720, 3),
(CONCAT(@ssd_spec,'-4'), @ssd_spec, 110, 140, 7200, 174080, 3),
(CONCAT(@ssd_spec,'-5'), @ssd_spec, 140, 170, 8400, 189440, 3),
(CONCAT(@ssd_spec,'-6'), @ssd_spec, 170, 200, 9600, 204800, 3),
(CONCAT(@ssd_spec,'-7'), @ssd_spec, 200, 230, 10800, 220160, 3),
(CONCAT(@ssd_spec,'-8'), @ssd_spec, 230, 260, 12000, 235520, 3),
(CONCAT(@ssd_spec,'-9'), @ssd_spec, 260, 290, 13200, 250880, 3);
end if;
if (@hdd_spec != 0 AND NOT EXISTS(SELECT id FROM `uni_uca_storage`.`tbl_qos_level` WHERE disk_spec_id = @hdd_spec)) then
INSERT INTO
`tbl_qos_level`(`id`, `disk_spec_id`, `cap_min`, `cap_max`, `iops`, `bw`, `count_max`)
values
(CONCAT(@hdd_spec,'-1'), @hdd_spec, 20, 50, 1300, 58880, 5),
(CONCAT(@hdd_spec,'-10'), @hdd_spec, 290, 320, 2920, 100352, 5),
(CONCAT(@hdd_spec,'-11'), @hdd_spec, 320, 350, 3100, 104960, 5),
```

```
(CONCAT(@hdd_spec,'-12'), @hdd_spec, 350, 380, 3280, 109568, 5),
(CONCAT(@hdd_spec,'-13'), @hdd_spec, 380, 410, 3460, 114176, 5),
(CONCAT(@hdd_spec,'-14'), @hdd_spec, 410, 440, 3640, 118784, 5),
(CONCAT(@hdd_spec,'-15'), @hdd_spec, 440, 470, 3820, 123392, 5),
(CONCAT(@hdd_spec,'-16'), @hdd_spec, 470, 500, 4000, 128000, 5),
(CONCAT(@hdd_spec,'-17'), @hdd_spec, 500, 530, 4180, 132608, 5),
(CONCAT(@hdd_spec,'-18'), @hdd_spec, 530, 560, 4360, 137216, 5),
(CONCAT(@hdd_spec,'-19'), @hdd_spec, 560, 590, 4540, 141824, 5),
(CONCAT(@hdd_spec,'-2'), @hdd_spec, 50, 80, 1480, 63488, 5),
(CONCAT(@hdd_spec,'-20'), @hdd_spec, 590, 620, 4720, 146432, 5),
(CONCAT(@hdd_spec,'-21'), @hdd_spec, 620, 650, 4900, 151040, 5),
(CONCAT(@hdd_spec,'-22'), @hdd_spec, 650, 680, 5000, 155648, 5),
(CONCAT(@hdd_spec,'-23'), @hdd_spec, 680, 710, 5000, 160256, 5),
(CONCAT(@hdd_spec,'-24'), @hdd_spec, 710, 65537, 5000, 163840, 5),
(CONCAT(@hdd_spec,'-3'), @hdd_spec, 80, 110, 1660, 68096, 5),
(CONCAT(@hdd_spec,'-4'), @hdd_spec, 110, 140, 1840, 72704, 5),
(CONCAT(@hdd_spec,'-5'), @hdd_spec, 140, 170, 2020, 77312, 5),
(CONCAT(@hdd_spec,'-6'), @hdd_spec, 170, 200, 2200, 81920, 5),
(CONCAT(@hdd_spec,'-7'), @hdd_spec, 200, 230, 2380, 86528, 5),
(CONCAT(@hdd_spec,'-8'), @hdd_spec, 230, 260, 2560, 91136, 5),
(CONCAT(@hdd_spec,'-9'), @hdd_spec, 260, 290, 2740, 95744, 5);
end if;
END//
delimiter ;
CALL uni_uca_storage.`insertQosLevel`();
DROP PROCEDURE IF EXISTS uni_uca_storage.`insertQosLevel`;
```

(3) 在存储设备上创建相应存储池

在新 3PAR/Primera 上创建相应 CPG，除了 snapshot 和 image CPG 外，其他 CPG 名称用新加规格编码，具体添加方式以及参数细节请参考 2. 配置存储池。

(4) 在 OMC 上纳管存储设备

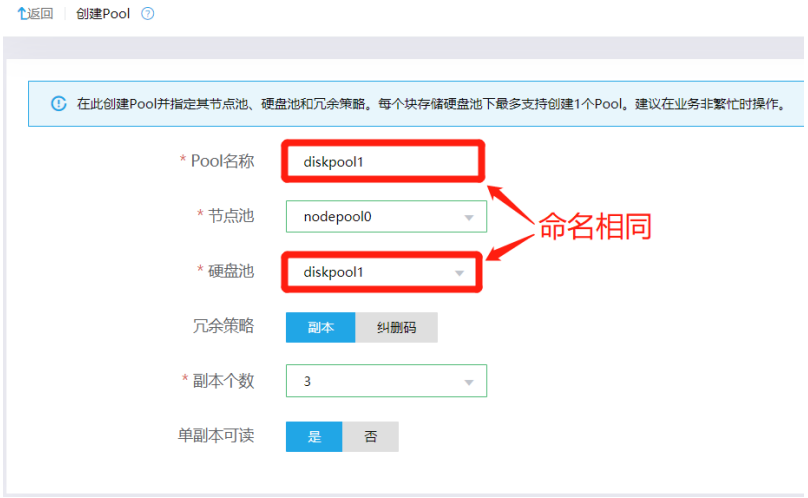
执行完以上 3 步后，在 OMC 上对新加 3PAR/Primera 设备进行纳管，纳管方式和参数请参考 3. OMC 界面纳管设备。

6.5.2 SDS 初始化配置

1. 创建存储池

在 SDS 页面需创建与硬盘池名称相同的存储池。

图6-10 创建存储池



2. OMC 界面纳管设备

(1) 登录 OMC 运维管理平台，点击页面左上方的，选择[IAAS/基础设施平台]。

(2) 在基础设施平台导航栏中，选择[计算集群管理/存储集群]。

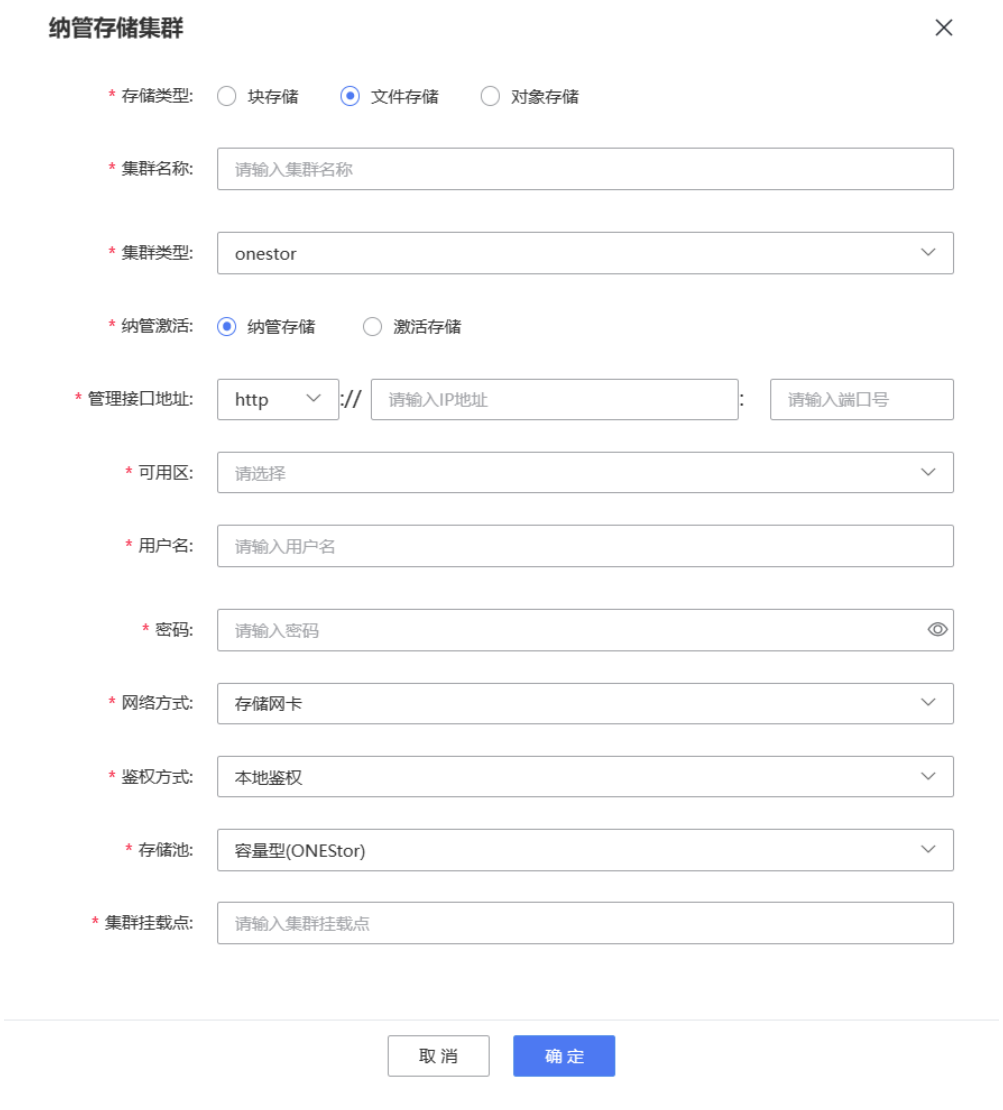
(3) 单击<纳管>按钮，在弹出的纳管存储设备对话框中，配置各项参数。

图6-11 纳管设备

参数说明：

参数	说明
集群名称	输入集群名称
集群类型	包括3PAR、SDS、Primera。这里选择SDS
纳管激活	选择纳管存储还是激活存储。 如果选择“激活存储”，需要上传激活文件，License授权在SDS来控制，平台不再管理（在License管理模块不会看到容量型License的授权信息）。 如果选择的是“纳管存储”，需要首先取得纳管型的License授权，导入到License服务器，平台在进行纳管的时候会进行相应的扣除。
管理接口地址	Primera、曙光存储、宏杉存储、华为分布式存储选择https,其他类型选择http，然后填写存储设备管理IP和端口，3par的端口是8008，Primera是443，曙光存储是8443，宏杉存储是8443，华为分布式存储是8088
通信协议	3PAR、Primera和Nimble选择iscsi或者fc-scsi（需要存储设备和VKS都支持FC协议），SDS选择rbd，其他存储目前都选择iscsi
可用区	选择该设备属于哪个AZ
用户名和密码	登录该存储设备的账号密码

图6-12 纳管文件存储设备



参数说明：

参数	说明
集群名称	输入集群名称
集群类型	包括SDS、X10000。这里选择SDS
纳管激活	选择纳管存储还是激活存储。 如果选择“激活存储”，需要上传激活文件，License授权在SDS来控制，平台不再管理（在License管理模块不会看到容量型License的授权信息）。 如果选择的是“纳管存储”，需要首先取得纳管型的License授权，导入到License服务器，平台在进行纳管的时候会进行相应的扣除。
管理接口地址	SDS和X10000均选择http，然后填写存储设备管理IP和端口，SDS和X10000的端口都是80
可用区	选择该设备属于哪个AZ

用户名和密码	登录该存储设备前台管理页面的用户名和密码。
网络方式	用户通过哪种网络访问创建的文件存储。可以选择假公网和第二存储网卡，与部署环境时文件存储的组网规划有关。对于第二存储网卡方式纳管的集群，用户需要创建NAS专用网卡或者第二存储网卡才能访问。
鉴权方式	cifs文件协议的鉴权方式，需要与SDS中配置的鉴权方式相一致，有本地鉴权、AD域、匿名访问三种。 • 如果选择本地鉴权，需要用户自己配置用户、用户组权限。 • 如果选择 AD 域则通过 AD 域服务器对访问共享目录的用户进行身份验证。 • 如果选择匿名访问，则用户创建文件系统时会自动添加 everyone 权限。
存储池	存储集群的存储池类型，请根据实际情况选择。 SDS有性能型（SSD盘）和容量型（HDD盘）。X10000固定为容量II型
集群挂载点	SDS的挂载点。通常为SDS中的NAS组的动态业务IP或者SDS文件存储负载均衡中配置的域名

(4) 单击<确定>按钮完成配置。

6.5.3 其他类型存储初始化配置

1. 创建存储池

在其他类型存储的 Web 管理页面上创建名称与对应磁盘规格编码相同的存储池。

- 曙光存储：ebs.sugon.ssd、ebs.sugon.hdd
- 宏杉存储：ebs.macrosan.ssd、ebs.macrosan.hdd
- 华为分布式存储：ebs.fusion.ssd、ebs.fusion.hdd
- Nimble 存储：ebs.nimble.ssd

2. OMC 界面纳管设备

(1) 登录 OMC 运维管理平台，点击页面左上方的  ，选择[IAAS/基础设施平台]。

(2) 在基础设施平台导航栏中，选择[计算集群管理/存储集群]。

(3) 单击<纳管>按钮，在弹出的纳管存储设备对话框中，配置各项参数。

图6-13 纳管设备

参数说明：

参数	说明
集群名称	输入集群名称
集群类型	包括3PAR、SDS、Primera。这里选择SDS
管理接口地址	Primera、曙光存储、宏杉存储、华为分布式存储选择https,其他类型选择http，然后填写存储设备管理IP和端口，3par的端口是8008，Primera是443，曙光存储是8443，宏杉存储是8443，华为分布式存储是8088；
通信协议	3PAR、Primera和Nimble选择iscsi或者fc-scsi（需要存储设备和VKS都支持FC协议），SDS选择rbd，其他存储目前都选择iscsi；
可用区	选择该设备属于哪个AZ
用户名和密码	登录该存储设备的前台账号密码

(4) 单击<确定>按钮完成配置。

6.6 上传镜像

6.6.1 （推荐）自动上传弹性云主机镜像/其他公共镜像

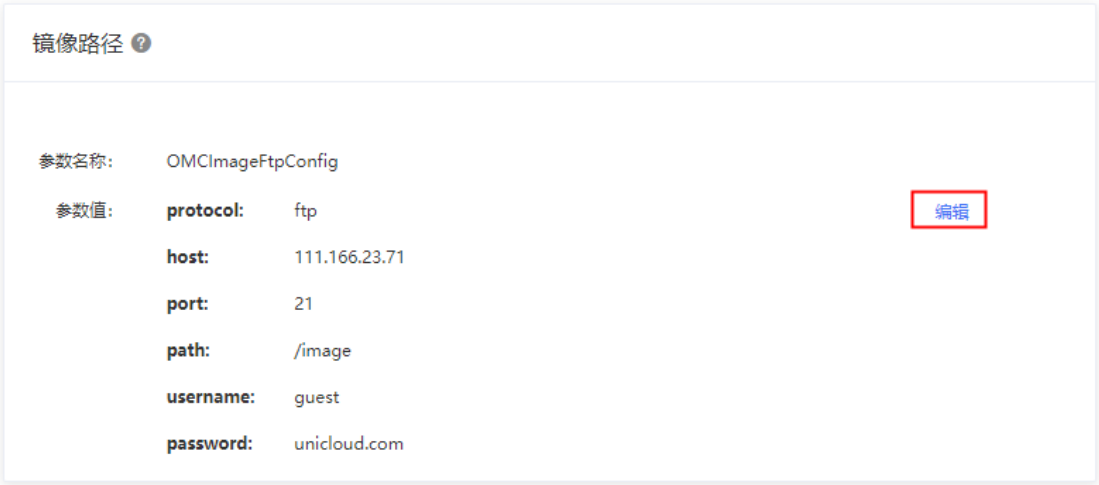
说明

通过 OMC 平台上传云主机镜像时，需要关注管区第一台 image-server 虚机（image-server01）的存储空间，避免根目录占满造成虚机异常。

(1) 登录 OMC 运维管理平台，点击页面左上方的，选择[IAAS/基础设施平台]。

(2) 在基础设施平台导航栏中，选择[配置管理/参数配置]，修改配置项 OMCImageFtpConfig 的值。将 host 修改为 imageserver01 虚机的 IP、username 修改为 ftpadmin，password 修改为 unic-moove，path 修改为"/"。例如：

{"hostname": "10.253.146.15", "port": 21, "path": "/", "username": "ftpadmin", "password": "unic-moove"}



(3) 使用 FTP 工具连接步骤(1)中填写的 FTP 地址，上传镜像文件。仅支持 qcow2 格式的镜像文件。

(4) 在基础设施平台导航栏选择[云计算/镜像管理]，进入镜像管理页面。

(5) 点击<上传公有镜像>按钮，进入公有镜像上传页面，按要求填写或者选择参数，点击<确定>按钮进行镜像上传。如果上传的是弹性云主机镜像，分发位置需选择存储设备。上传其他公共镜像，分发位置选择 NFS。

参数说明：

参数	说明
镜像ID	镜像的唯一标识，不可重复，如镜像有在运营平台上架的需要（例如，云主机镜像和裸金属镜像）则必须保证和运营平台镜像规格详情中的imageId是一致的。 常用镜像ID格式如下： • debian_1002 • ubuntu_1404 • ubuntu_1604 • ubuntu_1804 • ubuntu_2004 • WServer_2008R2_Standard • WServer_2012R2_Standard • WServer_2016_DataCenter • WServer_2008R2_DataCenter • WServer_2012R2_DataCenter • WServer_2012_Standard • WServer_2016_Standard • WServer_2019_Standard • WServer_2019_Essential • WServer_2012_DataCenter • WServer_2019_DataCenter • CentOS_6_5_64bit_minimal_std

参数	说明
	• CentOS_6_6_64bit_minimal_std • CentOS_6_7_64bit_minimal_std • CentOS_6_8_64bit_minimal_std • CentOS_6_9_64bit_minimal_std • CentOS_6_10_64bit_Minimal_std • CentOS_7_2_64bit_Minimal_std • CentOS_7_3_64bit_Minimal_std • CentOS_7_4_64bit_Minimal_std • CentOS_7_5_64bit_Minimal_std • CentOS_7_6_64bit_Minimal_std • CentOS_7_7_64bit_Minimal_std • CentOS_7_8_64bit_Minimal_std • CentOS_7_9_64bit_Minimal_std • CentOS_8_0_64bit_Minimal_std • CentOS_7_6_UNI_SLB_HOST_IMG_V4.0.6 PAAS网络产品镜像ID（image_id）是固定的，每次上传更新镜像时必须保证镜像文件名（file_name）不同，如果相同时需要上VKS清除镜像的缓存，否则可能会用到旧镜像。 PAAS网络产品使用的固定image_id如下： • UNI_DANOS_Debian_IMG • UNI_FRR_CentOS_7_9_IMG • UNI_SSLVPN_Comware_IMG • UNI_DPVS_CentOS_7_6_IMG • UNI_SLB_CentOS_7_6_HOST_IMG • UNI_SLB_CentOS_7_6_NET_IMG • UNI_CFW_Comware_IMG
镜像名称	输入镜像名称，一般和镜像ID一致。
镜像架构	选择该镜像可以被用在哪种架构的服务器上。
启动方式	选择虚机系统启动方式。
分发位置	选择该镜像是要被放在NFS上，还是存储设备上。 一般弹性云主机的镜像放在存储设备上，PAAS类主机的镜像放在NFS上。但是对于确定有云盘需求的镜像应选择存储设备作为分发位置，具体情况以各产品说明为准。
操作系统类型	选择Linux或Windows。
操作系统	选择操作系统运行的版本。
适用主机类型	选择镜像给云主机还是给裸金属使用。除了给裸金属使用的，其它都是云主机。
磁盘容量	该镜像上传时所需磁盘容量，一般跟该镜像虚拟大小一样。
上传镜像	该列表是从镜像所在FTP上获取需要上传的镜像文件。

6.6.2 （不推荐）手动上传弹性云主机镜像

说明

通过 OMC 平台上传云主机镜像时，需要关注管区第一台 image-server 虚机（image-server01）的存储空间，避免根目录占满造成虚机异常。

1. 导入 3PAR 镜像

(1) 使用 qemu-img info 命令查看镜像信息，查看并记录镜像的 virtual size：

```
[root@hb1-bjmy1-image-server01 2020-05-28]# qemu-img info Temp_Centos_6_5_05130940
image: Temp_Centos_6_5_05130940
file format: qcow2
virtual size: 40G (42949672960 bytes)
disk size: 1.7G
cluster_size: 262144
Format specific information:
    compat: 1.1
    lazy refcounts: false
[root@hb1-bjmy1-image-server01 2020-05-28]#
```

(2) 登录 3PAR 控制台，点击[块角色/虚拟卷]进入 3PAR 配置页面，点击<创建虚拟卷>，在 3PAR 中创建一个不小于镜像 virtual size 的空卷，并导出到镜像所在的服务器。命名规则参考镜像 ID 命名（运营平台已经预置镜像 ID）；如果是更新镜像，为了方便回溯，使用<原镜像名称.n>作为新镜像的名称（例如：CentOS_6_5_64bit_Minimal_std.n）。

图6-14 进入 3PAR 配置页面

图6-15 创建虚拟卷

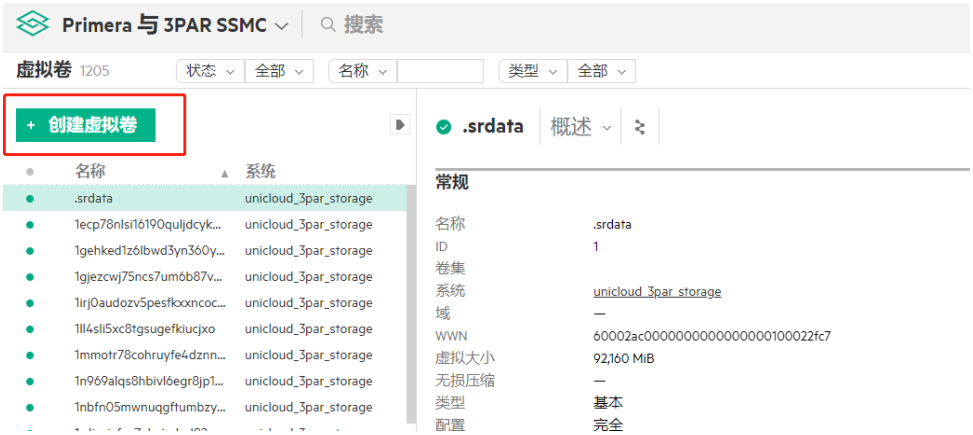


图6-16 配置虚拟卷

参数说明：

参数	说明
名称	从运营平台获取的镜像ID，后面会配置到数据库

系统	该环境适用的存储设备
配置	精简配置
CPG	选择image
大小	填写不小于镜像virtual size的大小
副本CPG	也选择image
注释	可以注明一下原始镜像文件名以及md5值
其他参数	默认

(3) 创建完以后在虚拟卷页面点击右侧的[操作/导出]，将该卷导出到镜像所在服务器主机上。

图6-17 导出虚拟卷

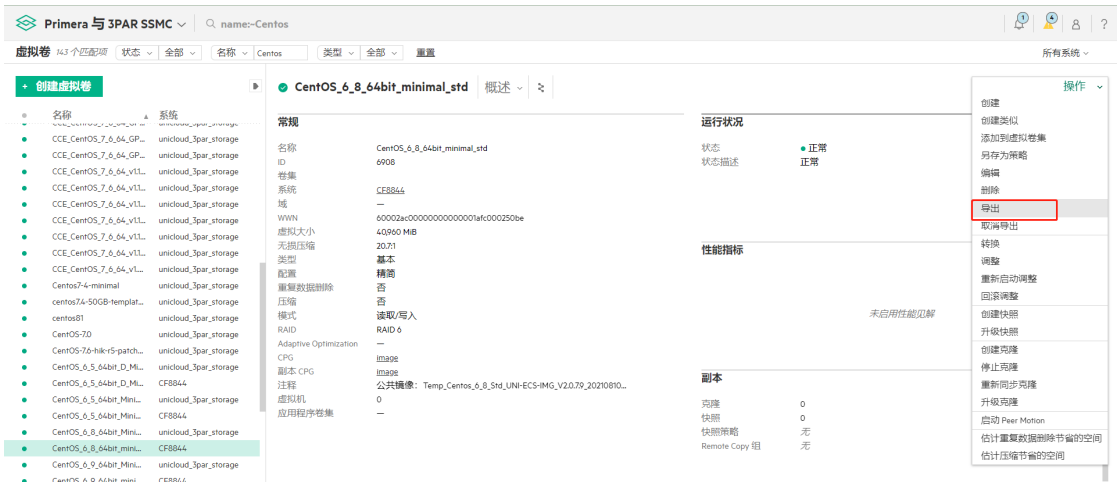


图6-18 配置导出方式

参数说明：

参数	说明
添加	添加镜像所在服务器主机
Lun号	勾选自动

(4) 设置完成后记录卷的 WWN（注意将字母转换为小写后再使用）。

图6-19 记录 WWN

(5) 执行下列命令件并写入到 3PAR 卷中。

```
#iscsiadm --mode discovery --type st --portal <3PAR 控制器 ip 地址> //发现 3PAR 设备
#iscsiadm -m node -l // 登录 3PAR
#ll /dev/disk/by-id | grep <WWN> // 查看卷是否正确导出
#qemu-img convert -p -f qcow2 -O raw <镜像文件> <卷路径> // 其中，-p 显示进度，-f 指定源镜像格式，-O 指定转换后格式（必须为 raw），卷路径为/dev/disk/by-id/scsi-3<WWN>；
#md5sum /dev/disk/by-id/scsi-3<WWN> // 可用于验证卷是否写入完整
#iscsiadm -m node -u // 登出 3PAR
```

(6) 在 3PAR 中取消卷的导出。

登录控制台，点击[块角色/虚拟卷]进入 3PAR 配置页面，点击[操作/取消导出]取消卷的导出。

图6-20 进入 3PAR 配置页面

图6-21 取消导出卷

(7) 如果是更新镜像，先将原镜像名称修改为<原镜像名称.递增数字>的形式（例如：CentOS_6_5_64bit_Minimal_std.1），然后去掉新镜像名称中的<.n>部分。

2. 导入 SDS 镜像

(1) 客户机安装 SDS client。

(2) 通过 SDS client 提供的 rbd 命令将镜像导入 SDS。

```
$ qemu-img convert -f qcow2 -O raw -p /path/to/qcow2/image /path/to/raw/image
# 首先需要将镜像格式转成 raw
$ rbd import --dest <镜像 id> /path/to/raw/image --dest-pool .<硬盘池名称>.rbd --data-pool <存储池名称>    # 导入镜像
```

(3) 批量上传镜像到 SDS 时可以使用 onestor-image-upload.sh 脚本文件，需要注意的是每次运行脚本前需要将脚本文件中的镜像 id 和镜像文件名改为本次上传镜像的 id 和文件名，镜像 id 保证与数据库的 image 表中的 image_id 字段一致，并且将所有镜像文件放在脚本文件所在目录后执行脚本文件。

```
onestor-image-upload.sh
#!/bin/bash

declare -a images

images=(
    "<镜像 1 的 id>|<镜像 1 的镜像文件名>"
    "<镜像 2 的 id>|<镜像 2 的镜像文件名>"
    ……
)

for item in "${images[@]}"; do
    id=${item%|*}
    image=${item#*|}
    raw=$image.raw

    echo "id: ${id} image: ${image}"

    if [ -f $image ]; then
```

```
            echo "convert image: ${image}, id: ${id}"
            qemu-img convert -f qcow2 -O raw -p $image $raw

            echo "import image: ${image}, id: ${id}"
            rbd import --dest $id $raw --dest-pool .<硬盘池名称>.rbd --data-pool <存储池名
    称>

            rm -f $raw
            echo "image done: ${image}, id: ${id}"
        fi
    done
```

3. 数据库添加记录

镜像表在 A 层 uni_uca_image 数据库中，此处需要更新的表名为 tbl_image、tbl_image_storage，如果是新加镜像，使用以下 sql 语句添加一条记录，其中`image_id`为存储设备中卷名称，`name`和`os`目前和`image_id`一致，`distros_name`、`distros_version`、`channel_type`请根据下方的参数说明填写。

```
INSERT INTO `uni_uca_image`.`tbl_image`(`image_id`, `status`, `name`, `arch`,
`distros_name`, `distros_version`, `os`, `os_type`,  `tag`, `channel_type`, `min_cpu`,
`min_disk`, `min_ram`, `boot_mode`, `user_id`, `virtual_size`, `description`, `version`)
VALUES ('<镜像 ID，和 3PAR 中卷名一致>', 'available', '<镜像名称>', 'amd64', '<镜像发行版名称>', '<
镜像发行版版本>', '<镜像系统>', '<操作系统类型，1.Linux 2.Windows>', '<镜像标签，1、ecs 2、bms>',
'<qga 通信 channel 类型，1、serial 2、virtio>', 0, 0, 0, '<镜像启动方式：legacy 、uefi >', '<镜
像所属 user id，公共镜像为 public>', <镜像未压缩容量，Byte>, '', '');
INSERT INTO `uni_uca_image`.`tbl_image_storage`(`image_id`, `volume_id`, `status`,
`storage_id`, `internal_id`, `wwn`, `format`, `hash_algo`, `hash`, `size`) VALUES ('<镜像
ID，和 3PAR 中卷名一致>', '<镜像 ID，和 3PAR 中卷名一致>', 'available', '<存储集群 id，可查看表
tbl_storage_server 中字段 server_id>', '', '', '<镜像格式，qcow2，raw>', '', '', <镜像未压缩容
量，Byte>);
```

例如：

```
INSERT INTO `uni_uca_image`.`tbl_image`(`image_id`, `status`, `name`, `arch`,
`distros_name`, `distros_version`, `os`, `os_type`, `tag`, `channel_type`, `min_cpu`,
`min_disk`, `min_ram`, `boot_mode`, `user_id`, `virtual_size`, `description`, `version`)
VALUES ('CentOS_7_3_64bit_Minimal_std', 'available', 'CentOS_7_3_64bit_Minimal_std',
'amd64', 'CentOS', '7.3 64bit', 'CentOS_7_3_64bit_Minimal_std', 'linux', 'ecs', 'virtio',
0, 0, 0, 'legacy', 'public', 42949672960, '公共镜像', '');
INSERT INTO `uni_uca_image`.`tbl_image_storage`(`image_id`, `volume_id`, `status`,
`storage_id`, `internal_id`, `wwn`, `format`, `hash_algo`, `hash`, `size`) VALUES
('CentOS_7_3_64bit_Minimal_std', 'CentOS_7_3_64bit_Minimal_std', 'available',
'CN7948097W', '', '', 'raw', '', '', 42949672960);
```

如果是更新镜像，则需要同步更新表中`updated_at`字段。

```
UPDATE `uni_uca_image`.`tbl_image` SET `updated_at`='2020-04-27 20:30:00' WHERE
`image_id`='CentOS_7_3_64bit_Minimal_std';
UPDATE `uni_uca_image`.`tbl_image_storage` SET `updated_at`='2020-04-27 20:30:00' WHERE
`image_id`='CentOS_7_3_64bit_Minimal_std';
```

参数说明：

参数	说明
distros_name	镜像的发行版名称。 可选的发行版名称如下：

参数	说明
	• CentOS • Ubuntu • Debian • Windows Server • FreeBSD 如镜像系统发行版并未列出，请根据系统类型从以下选项中选择： • Other Linux • Other Windows • Other Unix
distros_version	镜像的发行版版本。 发行版名称为CentOS时可选的发行版版本如下： • 6.5 64bit • 6.8 64bit • 6.9 64bit • 6.10 64bit • 7.2 64bit • 7.3 64bit • 7.4 64bit • 7.5 64bit • 7.6 64bit • 7.7 64bit • 7.8 64bit • 7.9 64bit • 8.0 64bit 发行版名称为Ubuntu时可选的发行版版本如下： • 14.04 64bit • 16.04 64bit • 18.04 64bit • 20.04 64bit 发行版名称为Debian时可选的发行版版本如下： • 10.02 64bit 发行版名称为Windows Server时可选的发行版版本如下： • 2008 Standard • 2008 DataCenter • 2008R2 Standard • 2008R2 DataCenter • 2012 Standard • 2012 DataCenter • 2012R2 Standard • 2012R2 DataCenter • 2016 Standard

参数	说明
	• 2016 DataCenter • 2019 Standard • 2019 Essentials • 2019 DataCenter 如镜像版本未列出，请根据系统类型选择对应的发行版名称，发行版版本统一为： • 64bit
channel_type	qga通信channel类型。 当镜像系统是FreeBSD时，使用serial，否则均使用virtio。

6.6.3 （不推荐）手动上传其他公共镜像

此类镜像通过挂载 nfs 的方式使用，将镜像文件放置到 **3** 台镜像服务器的 nfs 共享目录里，这个目录在镜像数据库 tbl_image_server 表中有的 dir_public 字段内有标识，然后使用以下 sql 语句添加镜像，`distros_name`、`distros_version`、`channel_type`请根据上一小节的参数说明填写（更新已有镜像只需更新 tbl_image_local 表中数据，注意同步更新<记录更新时间>，PAAS 网络产品镜像 ID（image_id）是固定的，每次上传更新镜像时需要更新`hash`，否则可能会使用 VKS 上镜像的缓存用到旧镜像）：

```
INSERT INTO `uni_uca_image`.`tbl_image`(`image_id`, `status`, `name`, `arch`, `distros_name`, `distros_version`, `os`, `os_type`, `tag`, `channel_type`, `min_cpu`, `min_disk`, `min_ram`, `boot_mode`, `user_id`, `virtual_size`, `description`, `version`) VALUES ('<镜像 ID>', 'available', '<镜像名称>', 'amd64', '<镜像发行版名称>', '<镜像发行版版本>', '<镜像系统>', '<操作系统类型，1.Linux 2.Windows>', '<镜像标签，1、ecs 2、bms>', '<qga 通信 channel 类型，1、serial 2、virtio>', 0, 0, 0, '<镜像启动方式：legacy 、uefi >', '<镜像所属 user id，公共镜像为 public>', @<镜像未压缩容量，Byte>, '', '');
INSERT INTO `uni_uca_image`.`tbl_image_local`(`image_id`, `status`, `image_server_id`, `path`, `file_name`, `format`, `hash_algo`, `hash`, `size`) VALUES ('<镜像 ID>', 'available', '<镜像服务器 ID，在镜像数据库 tbl_image_server 表中有，上传到几个镜像服务器上就添加几条>', '', '<镜像文件名>', '<镜像格式，qcow2 为 1，raw 为 2，3PAR 中通常为 raw 格式，其它为 qcow2 >', '<加密镜像文件算法，md5, sha1, sha256, sha512, etag>', '<镜像文件哈希值>', <镜像压缩后容量，Byte>);
```

例如：

```
INSERT INTO `uni_uca_image`.`tbl_image`(`image_id`, `status`, `name`, `arch`, `distros_name`, `distros_version`, `os`, `os_type`, `tag`, `channel_type`, `min_cpu`, `min_disk`, `min_ram`, `boot_mode`, `user_id`, `virtual_size`, `description`, `version`) VALUES ('Commware_CFW_IMG_V1.0.1', 'available', 'Commware_CFW_IMG_V1.0.1', 'amd64', 'Other Linux', '64bit', 'Other Linux', 'linux', 'ecs', 'virtio', 0, 0, 0, 'legacy', 'public', 8589934592, '', '');
INSERT INTO `uni_uca_image`.`tbl_image_local`(`image_id`, `status`, `image_server_id`, `path`, `file_name`, `format`, `hash_algo`, `hash`, `size`) VALUES ('Commware_CFW_IMG_V1.0.1', 'available', 'image-server-a', '', 'vFW1000_H3C-CMW710-E1185P12-X64.qco', 'qcow2', 'md5', 'ff2da59025be32dff7272d4972dde692', 406847488);
```

6.6.4 更新本地镜像（手动上传）

由于 OMC 界面上无法更新镜像文件，并且公共镜像也不能通过界面删除，因此如果需要更新镜像服务器上的镜像文件，只能手动进行替换。替换步骤如下：

(1) 替换 3 台镜像服务器的 nfs 共享目录里的镜像文件。

nfs 共享目录在镜像数据库 tbl_image_server 表中有的 dir_public 字段内有标识。

(2) 更新数据库表 tbl_image_local 中`file_name`、`hash_algo`、`hash`、`size`四个字段的值。

其中`file_name`必须手动更新，`hash_algo`、`hash`、`size`可调用以下接口自动更新。

```
curl -X POST "http://<k8s vip>:40004/uca/image/v2.0/image/local/update" -H "accept: */*" -H "X-Instance-Id:<镜像 ID>" -H "X-Request-Id:<请求 ID>" -d ""
```

6.7 （可选）配置存储双活和备份功能

如果项目环境中需要添加存储双活或者备份功能，请参考如下步骤进行配置。如果项目环境中不需要此功能请忽略。

6.7.1 存储设备 RC 配置

1. 双活和备份设备需具备的条件

双活和备份设备需要同时具备如下条件：

- 双活设备必须是 primera 或者 3par；
- 双活设备已经配置了 RCIP 端口，并且 RC 网络已经打通。

所需安装包如下，请向存储开发人员获取：

qwserv-3.0.014-1.el7.centos.x86_64.rpm

qwserv.7z

2. Remote Copy 链路配置（通过 SSMC 客户端进行配置）

存储双活和存储备份都需要配置 RC 链路。可通过 SSMC 客户端和通过 CLI 命令行进行配置，选择其中一种即可。本节内容为通过 SSMC 客户端进行配置。

(1) 创建配置，选择需要配置的系统（点“创建配置”时右上角的系统选择请选择“所有系统”，否则会显示没有权限）；

(2) 添加系统后，选择需要链接的端口，分别链接；

(3) 确认保存。

配置完成以后如下图：

3. Remote Copy 链路配置（通过 CLI 命令行进行配置）

存储双活和存储备份都需要配置 RC 链路。可通过 SSMC 客户端和通过 CLI 命令行进行配置，选择其中一种即可。本节内容为通过 CLI 命令行进行配置。

(1) 在两个系统上分别执行以下命令查看可用 RCIP 端口信息：

```
cli% showrctransport -rcip
```

显示结果如下：

```
CF22055 cli% showrctransport -rcip
N:S:P State HwAddr       IPAddress     PeerIPAddress Netmask       Gateway        MTU   Rate Duplex
0:1:1 new   040973BA0ADD 10.253.17.13  -             255.255.255.0 10.253.17.254 1500 10Gbps Full
0:2:1 new   040973BA0ADE 192.168.1.11  -             255.255.255.0 192.168.1.254 1500 10Gbps Full
1:1:1 new   040973BA0B71 10.253.17.14  -             255.255.255.0 10.253.17.254 1500 10Gbps Full
1:2:1 new   040973BA0B72 192.168.1.12  -             255.255.255.0 192.168.1.254 1500 10Gbps Full
```

```
CF22000 cli%
CF22000 cli% showrctransport -rcip
N:S:P State HwAddr       IPAddress     PeerIPAddress Netmask       Gateway        MTU   Rate Duplex
0:1:1 new   040973BAC689 192.168.1.13  -             255.255.255.0 192.168.1.254 1500 10Gbps Full
1:1:1 new   040973BAC7A1 192.168.1.14  -             255.255.255.0 192.168.1.254 1500 10Gbps Full
CF22000 cli%
```

(2) 要在存储系统 (System1) 上启动 HPE 3PAR Remote Copy，请执行以下命令：

```
cli% startrcopy
```

(3) 要在存储系统 (System1) 上定义目标，请执行以下命令：

```
cli% creatercopytarget <target_name> IP <N:S:P>:<link_IP_addr> <N:S:P>:<link_IP_addr>
```

其中：

- <target_name> - 辅助系统的名称 (System2，跟System1配对的设备系统名称，这个名称默认使用配对存储设备名称，也可以自定义)。
- IP - 将链路定义为 IP 链路。
- <N:S:P> - 当前系统 (System1) 上与辅助系统建立 IP 连接的端口位置，表示为 node:slot:port。
- <link_IP_addr> - 辅助系统上相应端口的链路 IP 地址（例如， XXX.XX.2.10 或 XXX.XX.2.11）。

(4) 要在存储系统 (System2) 上启动 HPE 3PAR Remote Copy，请发出以下命令：

```
cli% startrcopy
```

(5) 要在存储系统 (System2) 上定义目标，请执行以下命令：

```
cli% creatercopytarget <target_name> IP <N:S:P>:<link_IP_addr> <N:S:P>:<link_IP_addr>
```

其中：

- <target_name> - 辅助系统的名称 (System1，跟System2配对的设备系统名称，这个名称默认使用配对存储设备名称，也可以自定义)。
- IP - 将链路定义为 IP 链路。
- <N:S:P> - 当前系统 (System2) 上与辅助系统建立 IP 连接的端口位置，表示为 node:slot:port。
- <link_IP_addr> - 辅助系统上相应端口的链路 IP 地址（例如， XXX.XX.2.10 或 XXX.XX.2.11）。

(6) 配置后通过以下命令可以查看：

```
cli% showrcopy -qw
```

确认：

- Target Information 区域的 Status 显示为 ready；
- Link Information 区域所有链接的 Status 均显示为 Up。

在其中一个系统命令输出如下（在另一个系统进行同样的操作，显示结果与此相似）：

```
CF22055 cli%
CF22055 cli% showrcopy -qw

Remote Copy System Information
Status: Started, Normal

Target Information

Name    ID Type Status Policy        QW-Server QW-Ver Q-Status Q-Status-Qual ATF-Timeout
CF22000  9 IP   ready  mirror_config NA        NA     NA       NA                      NA

Link Information

Target  Node  Address      Status Options
CF22000 0:2:1 192.168.1.13 Up     -
CF22000 1:2:1 192.168.1.14 Up     -
receive 0:2:1 receive      Up     -
receive 1:2:1 receive      Up     -
CF22055 cli%
```

4. 配置存储双活仲裁机

只有后期要使用存储双活盘的配对设备才需要配置仲裁机，要用作备份的配对设备不需要配置仲裁机。

(1) 在镜像服务器安装仲裁机

a. 获取仲裁机 rpm 包，目前使用版本为 3.0.014。

包名称：qwserv-3.0.014-1.el7.centos.x86_64.rpm

b. 安装 rpm 包。

```
rpm -vi qwserv-3.0.014-1.el7.centos.x86_64.rpm
```

c. 检查仲裁机状态。

```
systemctl list-units | grep qwserv
```

返回结果：

```
[root@localhost ~]#
[root@localhost ~]# systemctl list-units | grep qwserv
  qwserv.service                                                    loaded active running   Quorum Witness ser
ver daemon
[root@localhost ~]#
```

(2) 在存储设备上配置仲裁机

a. 在两个存储设备上分别确认是否可以连接仲裁机。

```
cli% setrcopytarget witness check <new_witness_ip>
```

其中，<new_witness_ip>为安装仲裁机的服务器管理 IP 地址。

返回结果：

```
CF22055 cli%
CF22055 cli%  setrcopytarget witness check 10.254.4.149
Connectivity check passed
CF22055 cli%
```

```
CF22000 cli%
CF22000 cli% setrcopytarget witness check 10.254.4.149
Connectivity check passed
CF22000 cli%
```

b. 在 System1 创建仲裁机 client（后续步骤都只在一个设备操作即可）。

```
cli% setrcopytarget witness create <new_witness_ip> <target_name>
```

其中：

- <new_witness_ip>：仲裁机服务器 IP 地址。
- <target_name>：在 System1 上的目标名称。

c. 在 System1 上给 System2 创建仲裁机 client。

```
cli% setrcopytarget witness create -remote <new_witness_ip> <target_name>
```

其中：

- -remote：发送命令到备份系统上执行。
- <new_witness_ip>：仲裁机服务器 IP 地址。
- <target_name>：在 System1 上的目标名称。

d. 确认仲裁机 client 创建成功。

```
cli% showrcopy -qw targets
```

示例如下：

```
CF22000 cli%
CF22000 cli% showrcopy -qw targets

Remote Copy System Information
Status: Started, Normal

Target Information

Name    ID Type Status Policy        QW-Server    QW-Ver  Q-Status     Q-Status-Qual ATF-Timeout
CF22055  6 IP   ready  mirror_config 10.254.4.149 3.0.014 Initializing -                      10
CF22000 cli%
CF22000 cli%
CF22000 cli% showrcopy -qw targets

Remote Copy System Information
Status: Started, Normal

Target Information

Name    ID Type Status Policy        QW-Server    QW-Ver  Q-Status    Q-Status-Qual ATF-Timeout
CF22055  6 IP   ready  mirror_config 10.254.4.149 3.0.014 Not-started                       10
```

e. 等 Client 初始化完，在 System1 上启动仲裁机 Client:

`cli% setrcopytarget witness start <target_name>`

其中，<target_name>为在 System1 上的目标名称。

f. 在 System1 上启动 System2 的仲裁机 Client:

`cli% setrcopytarget witness start  -remote <target_name>`

其中：

– -remote 表示发送命令到备份系统上执行。

– <target_name>为在 System1 上的目标名称。

g. 在两台设备上都确认仲裁机 Client 都已经启动。

`cli% showrcopy -qw targets`

示例如下：

```
CF22055 cli%
CF22055 cli% showrcopy -qw targets

Remote Copy System Information
Status: Started, Normal

Target Information

Name    ID Type Status Policy        QW-Server    QW-Ver  Q-Status Q-Status-Qual ATF-Timeout
CF22000  9 IP   ready  mirror_config 10.254.4.149 3.0.014 Started                      10
CF22055 cli%
```

```
CF22000 cli% showrcopy -qw targets

Remote Copy System Information
Status: Started, Normal

Target Information

Name    ID Type Status Policy        QW-Server    QW-Ver  Q-Status Q-Status-Qual ATF-Timeout
CF22055  6 IP   ready  mirror_config 10.254.4.149 3.0.014 Started                      10
CF22000 cli%
```

5. 仲裁机监控配置

(1) 服务部署

需要准备安装包：qwserv.7z

a. 在安装了存储双活仲裁机的镜像服务器上解压文件。

b. 新建文件夹。

```
mkdir /opt/process_exporter
```

c. 将三个文件拷贝到新建的文件夹下。

```
chmod 755 process_exporter_x86_64
mv process_exporter_x86_64 process_exporter
mv process_exporter.service /usr/lib/systemd/system/
systemctl daemon-reload
systemctl enable --now process_exporter
```

d. 检查机器防火墙是否放通 9256 端口。

(2) 数据获取配置

修改 qwserv.yml 中预制的变量，将 server_ip（仲裁机部署机器 IP），server_name（仲裁机服务器名称），zone_code（可用区编码），替换为真实值，保存文件，放到租管互通 K8S 服务器的如下路径（3 台服务器都要有这个文件）：/opt/omc/prometheus/targets/process。

(3) 规则添加

手动添加一条规则以确保能够产生对应的告警。

a. 在 OMC 运维管理平台，点击页面左上方的  ，选择[监控告警/监控平台]，进入监控平台。

b. 在导航栏选择[告警规则]，进入告警规则页面。

c. 点击<新建>按钮，并在新建告警规则页面，按照下表添加规则。

规则项	填写值
规则名称	3par仲裁机进程异常
规则编码	qwserv_process_state_error
PromQL表达式	sum without(state)(namedprocess_namegroup_states{state=~"Sleeping|Running",groupname="qwserv"}) == 0
持续时间	0
告警类型	存储
告警主题	3par仲裁机进程异常
告警详情	节点: {{region}}; 可用区: {{zone}}; 实例: {{instance}}; 仲裁机进程qwserv状态为Sleeping或Running的进程总数为0
告警级别	严重
告警对象	admin（崇明应该只有admin）

(4) 填写完成后，点击[确定]按钮进行提交。

6. 双活和备份存储池创建

(1) 在存储设备上创建双活和备份存储池

a. 在配置 RC 链路的存储设备上分别创建双活存储池（ebs.highio.ssd_aa、ebs.hybrid.hdd_aa）和备份存储池（ebs.highio.ssd_ab、ebs.hybrid.hdd_ab）。

b. 创建方式跟 3par/primera 设备初始化时操作一致，根据磁盘类型分别创建 ssd 和 hdd 的存储池（存储池名称如上所述，如果只有一种磁盘类型则只创建名称符合的存储池）。

(2) 在数据库中纳管新创建存储池

a. 确认双活磁盘规格（ebs.highio.ssd_aa、ebs.hybrid.hdd_aa）和备份磁盘规格（ebs.highio.ssd_ab、ebs.hybrid.hdd_ab）已经在存储服务数据库的 tbl_disk_spec 表中添加，如果没有则需要先添加。

b. 对新增了存储池的存储设备通过存储服务纳管接口进行再次纳管，将新的存储池纳管到数据库，在存储服务数据库的 tbl_storage_pool 表中确认新增存储池已经纳管进来。

6.7.2 数据库存储 RC 配置

双活主主、双活主备和备份模式配置信息统一提取到 tbl_storage_rc_config 表中进行设置，目前配置信息粒度是存储池级别的，所以如果一对设备上双活或者备份既有 ssd 又有 hdd，则需要分别为 ssd 和 hdd 进行配置，示例如下：

id	source_server_id	source_server_name	source_pool_name	target_server_id	target_server_name	target_pool_name	ha_type	rc_group_mode	sync_perio	created_at	updated_at	deleted_at	is_deleted
1	CN7948097W	CF8844	ebs.highio.ssd_ab	CN71080VLL	CF22055	ebs.highio.ssd_ab	active-backup	3	300	2022-06-13 14:	2022-06-13 14:4	(Null)	0
2	CN7948097W	CF8844	ebs.hybrid.hdd_ab	CN71080VLL	CF22055	ebs.hybrid.hdd_ab	active-backup	3	300	2022-06-20 09:	2022-06-22 10:4	(Null)	0
3	CN71080VLL	CF22055	ebs.highio.ssd_aa	CNX123045H	CF22000	ebs.highio.ssd_aa	active-active	1	0	2022-06-13 15:	2022-06-20 20:5	(Null)	0
4	CNX123045H	CF22000	ebs.highio.ssd_aa	CN71080VLL	CF22055	ebs.highio.ssd_aa	active-active	1	0	2022-06-13 15:	2022-06-22 10:4	(Null)	0

1. 配置 RC 信息

配置方式有如下两种。

- 执行脚本对设备的 RC 信息进行配置（每次配置需要重新设置参数）

  RC 信息配置脚本 ：

```
#!/bin/bash

#K8s 的 vip
Ip="10.0.9.33"

#参数设置，每次执行前需要重新按要求设置！！！！！！
SourceServerId="CN71080VLL"
SourceInstanceCode="ebs.highio.ssd_ab"
TargetServerId="CNX123045H"
TargetInstanceCode="ebs.highio.ssd_ab"
#active-active/active-backup
HaType="active-backup"
#sync/periodic
RcGroupMode="periodic"
SyncPeriod=300
```

```
#设置 RC 配置信息
echo "设置 RC 配置信息:"
url="http://$Ip:40002/uca/storage/v2.0/storage/server/rcconfig/add"
echo "请求 URL：$url"
echo "请求结果："
curl -X POST "$url" -H "accept: */*" -H "Content-Type: application/json" -d
"{\"SourceServerId\":\"$SourceServerId\",\"SourceInstanceCode\":\"$SourceInstanceCo
de\",\"TargetServerId\":\"$TargetServerId\",\"TargetInstanceCode\":\"$TargetInstanc
eCode\",\"HaType\":\"$HaType\",\"RcGroupMode\":\"$RcGroupMode\",\"SyncPeriod\":$Syn
cPeriod}"
echo
```

- 通过 Postman 调用接口配置（每次配置需要重新设置参数）：

  添加存储设备 RC 信息配置

```
POST http://{{uca-center}}:40298/uca/storage/v2.0/storage/server/rcconfig/add
HTTP/1.1


{
  "HaType": "active-backup",                          //必输项，高可用类型（active-active：
双活类型，active-backup：备份卷类型）
  "RcGroupMode": "SYNC",                              //必输项，RC 组模式：1、SYNC ，3、
PERIODIC
  "SourceInstanceCode": "ebs.hybrid.hdd_ab",          //必输项，主存储设备磁盘规格
  "SourceServerId": "CN7948097W",                     //必输项，主存储设备 ID
  "SyncPeriod": 0,                                    //必输项，异步 RC 组同步周期，单位：s
（rc_group_mode 设置为 PERIODIC 时才有用，默认 0，Range is 300－31622400 seconds (1 year).）
  "TargetInstanceCode": "ebs.hybrid.hdd_ab",          //必输项，目标设备磁盘规格
  "TargetServerId": "CN71080VLL"                      //必输项，目标设备 ID
}


--------------------------------------------------------------------------------
---------------------------------
{
  "RequestId": "",
  "Status": "Success",
  "Message": "操作成功",
  "WaitCallback": null,
  "Detail": {
    "SourceServerId": "CN7948097W",
    "SourceServerName": "CF8844",
    "SourcePoolName": "ebs.hybrid.hdd_ab",
    "TargetServerId": "CN71080VLL",
    "TargetServerName": "CF22055",
    "TargetPoolName": "ebs.hybrid.hdd_ab",
    "HaType": "active-backup",
    "RcGroupMode": "SYNC",
    "SyncPeriod": 0,
    "CreatedAt": null,
    "UpdatedAt": null,
    "DeletedAt": null,
```

```
        "IsDeleted": false
      }
    }
```

配置参数说明如下。

参数	说明
SourceServerId	需要配置的源设备ID。
SourceInstanceCode	需要配置的源设备的磁盘规格。
TargetServerId	需要配置的目标设备ID。
TargetInstanceCode	需要配置的目标设备的磁盘规格。
HaType	这次配置的高可用类型（active-active/active-backup）。
RcGroupMode	这次配置的RC组模式（SYNC/PERIODIC）。
SyncPeriod	如果是异步RC组模式，需要配置该同步周期值（不能小于300s），单位为秒（s）。

2. 配置说明

目前配置信息粒度是存储池级别的，所以如果一对设备上双活或者备份既有 ssd 又有 hdd，则需要分别为 ssd 和 hdd 进行配置。

各种模式的配置说明如下。

- 双活主备模式

  配置双活主备时，HaType 必须为 active-active，RcGroupMode 必须为 SYNC，源设备 A 和目标设备 B 的 ID 确定后，只需要配置一个方向即可（A → B）。

- 双活主主模式

  配置双活主主时，HaType 必须为 active-active，RcGroupMode 必须为 SYNC，设备 A 和设备 B 两者都可为源，都可为备，所以在配置时需要配置两个方向的数据信息（A → B 和 B → A）。

- 备份模式

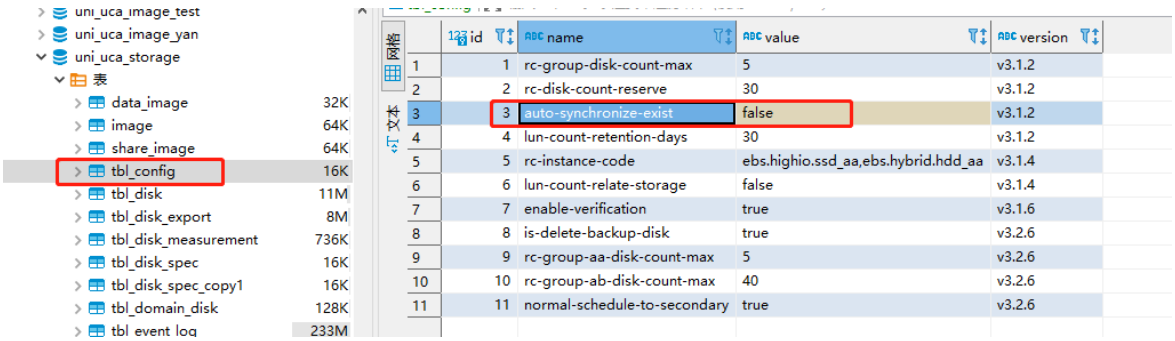
  配置备份模式时，HaType 必须为 active-backup，RcGroupMode 可以为 SYNC 也可以为 PERIODIC，如果 RcGroupMode 选 PERIODIC，则 SyncPeriod 值必须大于等于 300， 源设备 A 和目标设备 B 的 ID 确定后，给不同存储池配置即可。

配置 RC 信息时，有如下限制：

- 备份模式一对设备只能配置一个备份方向，例如配了 A → B，就不能再配 B → A；
- 双活模式一对设备的一条配置中使用的源磁盘规格和目标磁盘规格必须一致；
- 同一设备同一磁盘规格以及相同的 HaType，只能和一台设备配置，不能一对多；
- 一对设备只能配置双活或者备份的一种，不能同时配置双活和备份；
- 双活磁盘规格为（ebs.highio.ssd_aa、ebs.hybrid.hdd_aa），备份磁盘规格为（ebs.highio.ssd_ab、ebs.hybrid.hdd_ab）。

3. 注意事项

如果配置了双活并且双活设备类型是 3Par，则需要将存储服务数据库 uni_uca_storage 的表 tbl_config 中的 auto-synchronize-exist 参数值设置为 false，否则不需要处理。



6.7.3 双活卷设备故障后恢复说明

1. 故障处理

当其中一台主设备出现故障，发生自动故障转移后可能会出现如下场景：

- 场景 A：其中一台设备出现故障时，此时没有正在下发的双活业务，所有 RC 组都处在已启动状态；

  这种情况下所有主卷在故障设备上的 RC 组都会进行自动故障转移，切换为备卷供主机访问，并且在设备上 RC 组显示为停止状态；这时所有 RC 组内的卷都不能进行其他业务操作，存储服务的定时 RC 设备监控任务（下称定时任务）在 5m 内会检测到其中一台设备故障，然后将涉及到的 RC 组在数据库中的状态置为 error 状态；之后如果有对该设备的双活盘的业务操作，编排在进行资源准备时判断到该磁盘所属 RC 组状态是 error 时，会阻断流程下发，防止产生脏数据；

  等故障设备恢复后，会出现两种情况：

  第一种：由于部分设备系统版本问题，RC 组无法设置自动同步策略，所以故障设备恢复后 RC 组不能自动恢复，一直处于 failsafe 状态，需要人为介入手动修复，这个时候定时任务还是会将 RC 组状态置为 error；

  第二种：RC 组设置了自动同步策略，底层设备上所有 RC 组会自动恢复启动，原来的备卷角色为主卷，原来的主卷现在为备卷；此时数据面和底层设备主备对应关系不符，在定时任务一个周期后，定时任务会检测到故障设备恢复，将切换了主备的 RC 组再次按照数据库中方向切换回原状，并且更新 RC 组状态为 started，上层编排可以正常下发流程；

  出现第一种情况手动介入处理：

  1、此时 RC 组在原来主设备上处于 failsafe 状态，角色还是 Primary，在备设备上 RC 组处于 stopped 状态，角色是 Primary-Rev；

  2、在角色是 Primary-Rev 的备设备的 CLI 上执行如下 2 个命令，且顺序不能有误；

  1）setrcopygroup recover <RC 组在此设备上的名称>（该命令可将故障转移后转换卷组中的数据复制到已恢复系统上的相应卷组中），执行完以后 RC 组在原来主设备上处于 started 状态，角色是 Secondary-Rev，备设备上 RC 组处于 started 状态，角色是 Primary-Rev，等 RC 组中所有卷的状态为 Synced；

  2）setrcopygroup restore <RC 组在此设备上的名称>（还原 Remote Copy 对中数据流的自然方向），执行完以后 RC 组在原来主设备上处于 started 状态，角色是 Primary，备设备上 RC 组处于 started 状态，角色是 Secondary；

3、等 RC 组状态恢复后，在一个定时任务周期后，数据库中会自定更新 RC 组状态为正常状态，上层编排可以正常下发流程。

- 场景 B：其中一台设备出现故障时，此时有正在下发的双活业务，此时有一个 RC 组 M 处于停止状态；

这种情况下所有主卷在故障设备上的 RC 组也会进行自动故障转移，切换为备卷供主机访问，并且在设备上 RC 组显示为停止状态，但是那个下发业务有同步数据任务的 RC 组 M 不会切换；这时所有 RC 组内的卷都不能进行其他业务操作，并且未切换的 RC 组 M 因为没有自动故障转移，所以此时主机是无法访问 RC 组 M 中的所有卷的，会中断虚机的业务；定时在 5m 内会检测到其中一台设备故障，然后将涉及到的 RC 组在数据库中的状态置为 error 状态。

未切换 RC 组 M 的处理方式如下。

RC 组 M 中卷的业务如果不是很着急，或者故障设备很快能修复，则可以不用处理，等故障设备恢复后再恢复业务，统一处理，这样不存在数据丢失问题，建议不进行操作等故障设备恢复；如果可接受数据丢失，想快速恢复 RC 组 M 中的卷的访问，需要做如下操作：

1、在现在 RC 组的备设备上调用接口对 RC 组 M 进行故障转移（此动作要谨慎再谨慎，此操作会将这个 RC 组从停止到设备故障这个时间段内写的数据丢失，需要跟客户确认）；

表6-1 对 RC 组进行故障转移

HTTP 请求	请求内容
URL	POST http://<此RC组备设备IP>:443/api/v1/remotecopygroups/<RC组名称> HTTP/1.1
响应	同步
Header	"X-Hp3Par-Wsapi-Sessionkey": "", //3par或者primera设备请求sessionKey

Body	{
	"action": 7
	}

2、在磁盘挂载的 VKS 上，将虚机关机，并且将磁盘的多路径删除；

3、重新原来的备盘进行 map，将盘符和多路径刷回来；

4、此时可以重启虚机恢复业务；

5、等故障设备恢复后，再次将原来的主盘进行 map，也将盘符和多路径刷回来；

6、故障设备恢复后，如果 RC 组 M 未自动恢复 started，则需要按照场景 A 中的第一种情况来处理。

等故障设备恢复后，底层设备上除 RC 组 M 外，其他 RC 组会出现两种情况：

第一种：由于部分设备系统版本问题，RC 组无法设置自动同步策略，所以故障设备恢复后 RC 组不能自动恢复，一直处于 failsafe 状态，需要人为介入手动修复，这个时候定时任务还是会将 RC 组状态置为 error；

第二种：RC 组设置了自动同步策略，底层设备上所有 RC 组会自动恢复启动，原来的备卷角色为主卷，原来的主卷现在为备卷；此时数据面和底层设备主备对应关系不符，在定时任务一个周期后，定时任务会检测到故障设备恢复，将切换了主备的 RC 组再次按照数据库中方向切换回原状，并且更新 RC 组状态为 started，上层编排可以正常下发流程；

出现第一种情况手动介入处理：

1、此时 RC 组在原来主设备上处于 failsafe 状态，角色还是 Primary，在备设备上 RC 组处于 stopped 状态，角色是 Primary-Rev；

2、在角色是 Primary-Rev 的备设备的 CLI 上执行如下 2 个命令，且顺序不能有误；

1）setrcopygroup recover <RC 组在此设备上的名称>（该命令可将故障转移后转换卷组中的数据复制到已恢复系统上的相应卷组中），执行完以后 RC 组在原来主设备上处于 started 状态，角色是 Secondary-Rev，备设备上 RC 组处于 started 状态，角色是 Primary-Rev，等 RC 组中所有卷的状态为 Synced；

2）setrcopygroup restore <RC 组在此设备上的名称>（还原 Remote Copy 对中数据流的自然方向），执行完以后 RC 组在原来主设备上处于 started 状态，角色是 Primary，备设备上 RC 组处于 started 状态，角色是 Secondary。

3、等 RC 组状态恢复后，在一个定时任务周期后，数据库中会自定更新 RC 组状态为正常状态，上层编排可以正常下发流程。

- 场景 C：当存储设备发生故障转移，VKS 上的双活盘多路径概率性切换不成功，该盘不可用，导致 libvirt 死锁，virsh 命令卡死；

这种场景下需要人为介入修复该磁盘多路径，删除原来的多路径，重新扫描刷新多路径，修复好后 libvirt 死锁会自动解除；

操作步骤如下：

1、过滤出多路径有问题链路：使用命令 multipath -l |grep -10 failed ；

2、删除多路径：将步骤 1 中过滤出的磁盘多路径用命令 multipath -f 36xxxxxxxxxxx 进行删除；

3、过滤该多路径下的块设备：使用命令 lsscsi -git *:0:0:lun 号（主备磁盘的 lun 号可能不一致，需过滤两次）；

4、删除块设备：使用命令 echo 1 > /sys/block/sdxx/device/delete 将步骤 3 过滤出的块设备都删除了；

5、确认块设备都删除：再次使用命令 lsscsi -git *:0:0:lun 号 验证确认所有该多路径下的块设备是否都删除掉；

6、重新扫描块设备：先刷主磁盘，后刷备磁盘，使用命令 echo "0 0 lun 号" > /sys/class/scsi_host/hostxx/scan 进行扫描，存储设备有几条链路就需要扫描几次，host 序号在/sys/class/scsi_host/目录下；

7、确认多路径是否刷新：使用命令 lsscsi -git *:0:0:lun 号 进行过滤，确认块设备是否已经刷出来，并且组出多路径。

2. 故障恢复后可能出现问题清单及建议解决方式

序号	触发场景	问题现象	解决或规避措施
1	主主模式，主3par断开时	对双活虚拟机重装系统（重装流程会失败卡住，为正常现象），此时再到OMC对该虚拟机执行克隆，克隆流程会跳过关键步骤直接报成功。克隆出的虚拟机由于没有系统盘，产生脏数据，无法删除掉，也无法回滚掉	A层使用编排流程中删除接口删除残留虚拟机
2	主主模式，主	主3par断开时构造双活盘自定义镜像，概	1、第一种处理方式：OMC跳过流程,直至该

序号	触发场景	问题现象	解决或规避措施
	3par断开后恢复	率性出现流程无法成功。原因是因为创建镜像的过程中底层存储主备切换，流程中使用的数据与底层数据存在差异。	镜像状态为可用，然后从页面删除该镜像。后期可以再次重新新建自定义镜像； 2、第二种处理方式：等故障设备修复后，定时任务将底层3par的主备模式切换回原来的角色，重试失败流程修复； 3、第三种处理方式：等故障设备修复后，在数据面上切换主备，跟底层设备主备角色一致，此时需要人为介入修改编排流程参数，切换资源中的主备，然后使流程继续走下去；
3	主主模式，主3par断开时	主3par断开时，删除带双活盘的虚拟机，用户控制台删除成功，实际残留	1、第一种处理方式：等故障设备修复后，定时任务将底层3par的主备模式切换回原来的角色，重试失败流程修复； 2、第二种处理方式：等故障设备修复后，在数据面上切换主备，跟底层设备主备角色一致，此时需要人为介入修改编排流程参数，切换资源中的主备，然后使流程继续走下去；
4	主主模式，主3par断开时	对于两个用户来说，扩容系统盘均失败	1、第一种处理方式：等故障设备修复后，定时任务将底层3par的主备模式切换回原来的角色，重试失败流程修复； 2、第二种处理方式：等故障设备修复后，在数据面上切换主备，跟底层设备主备角色一致，此时需要人为介入修改编排流程参数，切换资源中的主备，然后使流程继续走下去；
5	主主模式，主3par断开时	其中一台3par故障后发生主备切换，此时主盘在故障设备上的虚机进行迁移时会报错，流程失败	1、第一种处理方式：等故障设备修复后，定时任务将底层3par的主备模式切换回原来的角色，重试失败流程修复； 2、第二种处理方式：等故障设备修复后，在数据面上切换主备，跟底层设备主备角色一致，此时需要人为介入修改编排流程参数，切换资源中的主备，然后使流程继续走下去。或者回滚原来的流程，然后重新进行迁移；
6	主备或者主主模式下，主3par断开	在底层3par自动进行了主备切换，此时主盘在故障设备上的磁盘进行挂载相关操作时会失败	1、第一种处理方式：等故障设备修复后，定时任务将底层3par的主备模式切换回原来的角色，重试失败流程修复； 2、第二种处理方式：等故障设备修复后，在数据面上切换主备，跟底层设备主备角色一致，此时需要人为介入修改编排流程参数，切换资源中的主备，然后使流程继续走下去；

6.8 纳管计算设备

6.8.1 纳管裸金属前提条件

在 OMC 平台上纳管裸金属服务器前，需要完成如下操作：

(1) 确认服务器物理连线都正常后，通过 PXE 启动裸金属服务器，并开启 LLDP 功能。

(2) 需要在 OMC 的网络设备页面，进行裸金属连接 Leaf 设备的同步。在[基础设施平台/云网络/网络设备]，对裸金属连接的三台网络设备（管理、业务、存储交换机）点击同步。

6.8.2 创建调度组

(1) 登录 OMC 运维管理平台，点击页面左上方的，选择[IAAS/基础设施平台]。

(2) 在基础设施平台导航栏中，选择[云计算/初始化配置/调度组]，进入调度组管理列表页面。

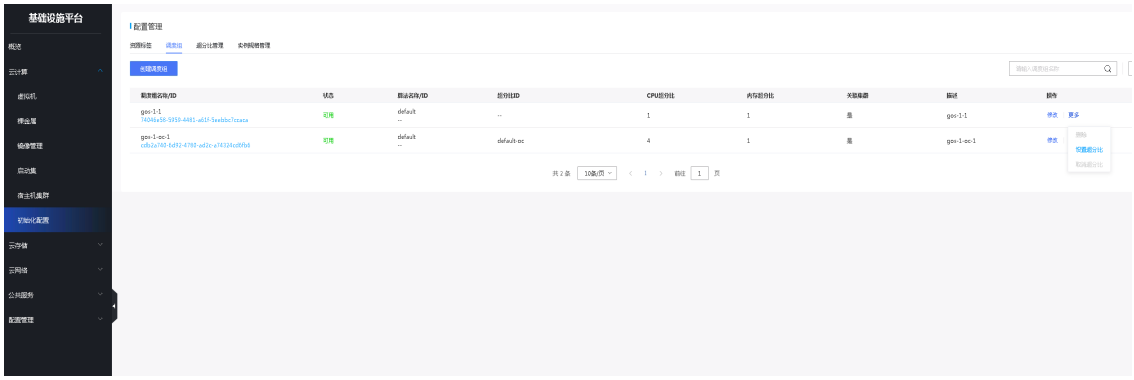
(3) 单击<创建调度组>，在创建调度组对话框中，填写调度组名称和调度组描述。

(4) 单击<确定>完成调度组创建。

图6-22 创建调度组

(5) 在调度组管理列表页面，单击指定调度组列表右侧的<更多>，选择“设置超分比”，选择默认 1:4 即可。

图6-23 设置超分比



6.8.3 资源标签

(1) 在基础设施平台导航栏中，选择[云计算/初始化配置]，进入配置管理页面，首先展现的就是资源标签。

(2) 资源标签是产品规格和集群的纽带，这里定义的资源标签将会应用到规格管理和集群管理。资源标签支持新建和编辑，可以定义资源标签、资源标签别名以及描述；而编辑仅允许修改别名和描述。

(3) 标签的状态表示引用情况。未使用：表示还没有应用到任何集群；已使用表示已经有集群使用了该标签。

(4) 平台会预置基础的资源标签，也给出基本的标签定义格式。

资源标签	产品
ecs	云主机
ecs-xxx	云主机衍生产品 ARM云主机：ecs-arm 本地盘云主机：ecs-ld 内存快照云主机：ecs-qcow2
ld	数据库、中间件、大数据等
ld-net	SLB、HSLB
ld-danos	Danos、CFW/CCN（如果CFW/CCN与SLB共用资源池，请手动修改CFW/CCN产品规格的资源标签）
ld-xxx	本地盘资源衍生产品 ld-drbd：基于DRBD存储的数据库 ld-nvme：基于NVME SSD存储的数据库
gpu-xxx	GPU产品 GPU-v100：基于v100的N卡云主机 GPU-t4：基于t4的N卡云主机 GPU-vRay-v8g：vGPU云主机，基于vRay卡，按8g划分 gpu-v100-v4g：vGPU云主机，基于v100卡，按4g划分 gpu-rtx6000：虚拟化渲染rtx6000型
bms-xxx	裸金属 bms-xxx 后缀会按节点裸金属配置或者型号定义
sec	安全产品，堡垒机、waf（请新建此资源标签）
cce	云容器引擎

图6-24 资源标签

参数说明：

参数	说明
资源标签	必须全局唯一
资源标签别名	可以重复

图6-25 资源标签

资源标签	资源标签别名
ecs	通用型
ecs-ld	本地盘型弹性云主机
ld	DB型
ld-net	SLB型
ld-file	文件存储型
gpu-v100	GPU-V100型
gpu	GPU
gpu-t4	gpu-t4
gpu-m60	GPU-M60型
bms	裸金属

6.8.4 新建集群

(1) 在基础设施平台导航栏中，选择[云计算/宿主机集群]，进入集群管理页面。

(2) 单击<新建集群>按钮，在弹出的新建集群对话框中，配置集群可用区、集群名称、资源标签、调度组名称、集群描述以及是否具备 HA 功能。

图6-26 新建集群

参数说明：

参数	说明
可用区	选择该集群的可用区
资源标签	选择该集群的资源标签标识，参见“6.5.3 资源标签”
调度组	为该集群分配已有的调度组
是否具备HA功能	为该集群选择是否具备HA，只有具备HA功能的集群，其内VKS才可执行开启配置HA、关闭配置HA、开启自动HA、关闭自动HA功能

6.8.5 同步主机

(1) 在基础设施平台导航栏中，选择[云计算/宿主机集群]，在页面中选择[主机]页签，进入主机管理页面。

(2) 纳管弹性云主机：点击<纳管主机>按钮，在弹出的[纳管主机]对话框中，配置集群类型为<弹性云服务器>、主机位置、是否超分、纳管方式、主机 IP 和网络类型。

(3) 纳管裸金属：点击<纳管主机>按钮，在弹出的[纳管主机]对话框中，配置集群类型为<裸金属服务器>、主机位置、纳管方式、带外管理 IP、网络类型、主机名称、网络连接。其中，网络连接中选择的三个设备分别为业务网、管理网和存储网设备，需提前在 OMC 中对三个网络设备进行同步。

(4) 点击<确定>完成同步主机配置。

6.8.6 （可选）非 root 用户迁移

出于安全考虑，环境中可以配置 Migrate 用户以及 TLS 协议来支持虚拟机的迁移操作。该章节中涉及的脚本从 init_migrate_user.tar 包中获取。

1. 创建 Migrate 用户

```
# useradd migrate
# echo migrate:migrate | chpasswd     #密码可以设置自定义
```

2. Migrate 用户设置 dd 权限

(1) 给/etc/sudoers 写权限。

```
#chmod +w /etc/sudoers
```

(2) 打开/etc/sudoers，在“root ALL=(ALL) ALL”行下添加 Migrate 用户 dd 权限。

```
#vim /etc/sudoers
root    ALL=(ALL)       ALL
migrate    ALL=(ALL)       /bin/dd
```

3. Migrate 用户互信

通过在 Ansible 服务器上生成 Migrate 用户 SSH Key 并批量拷贝到每台 VKS，登录到环境中的 Ansible 服务器，并将要初始化的 VKS 信息提前录入到 Ansible 的 hosts 中。

(1) 切换至 Migrate 用户。

```
# su  -  migrate
```

(2) 创建 SSH Key。

```
$ ssh-keygen -t rsa
```

一直点确认直到完成。

(3) 拷贝 ssh_pub 到自身 authorized_keys。

```
$ ssh-copy-id migrate@localhost
```

默认密码为 migrate，如在步骤一中设置密码未使用默认密码，此处使用指定的密码。

(4) 回到 root 用户。

```
$ exit
```

(5) 从 Ansible 服务器中拷贝 id_rsa 和 authorized_keys 到目的 VKS。

```
#ansible  <hosts> -f 10 -m copy -a "src=/home/migrate/.ssh/authorized_keys
dest=/home/migrate/.ssh/ "  //hosts 为要做互信的 VKS 集
#ansible  <hosts> -f 10 -m copy -a "src=/home/migrate/.ssh/id_rsa
dest=/home/migrate/.ssh/ " //hosts 为要做互信的 VKS 集
```

(6) 设置权限。

```
#ansible <hosts> -f 10  -m shell -a "chmod 700 /home/migrate/.ssh;chmod 755
/home/migrate/.ssh/authorized_keys"
```

4. 创建 CA 文件

在环境中选择一台服务器注册成为 CA 签发机构，并创建 CA 证书。

(1) 拷贝 init_migrate_user.tar 到服务器的 root 目录。

(2) 解压 init_migrate_user.tar 文件。

```
#tar -xvf init_migrate_user.tar
```

(3) 创建 CA 证书。

```
#cd init_migrate_user
#./CreateCA.sh
```

说明

一套环境中只允许生成一次 CA 证数的公钥和私钥，使用该私钥和公钥签发其他 VKS 的证书，因此建议将生成的 CA 证书文件进行备份，以防止误删。

---

5. 准备 VKS 初始化文件信息

需要在 CA 签发机构的服务器上需要进行 TLS 互信的一系列 VKS 进行 CA 证书分发，首先需要在签发机构服务器上创建/root/pki/cvkinfo 文件并写入准备好目的 VKS 的信息。

文件格式为：

com-001 M00ve 10.254.7.3 14.254.7.3

com-003 M00ve 10.254.4.7 14.254.4.7

com-002 M00ve 10.254.7.4 14.254.4.4

其中每一行对应一个 VKS 的信息，分别为 VKS 的 hostname、密码、VKS 的管理网 IP、VKS 的存储网 IP。

6. 签发 VKS TLS 证书

准备好文件后，就可直接执行分发证书脚本 IssueCert.sh。

```
#cd init_migrate_user
# ./IssueCert.sh -x        #该命令会根据/root/pki/cvkinfos 中的信息，对其中配置的 VKS 进行分发 ca 证书
```

执行脚本后需要通过/var/log/issue-cert.log 日志看签发是否有问题。

6.9 （可选）配置边缘可用区

请在中心可用区和边缘可用区都部署完毕后，再进行此章节的操作。

配置边缘可用区的步骤包括：

(1) 新建边缘可用区，并配置边缘自治服务。

(2) 纳管边缘资源，包括网络资源、计算资源和存储资源。

6.9.1 新建边缘可用区

(1) 登录 OMC 运维管理系统，点击页面左上方的，选择[基础平台/节点管理]，进入节点管理页面。

(2) 通过如下两种方法之一，进入可用区管理页面。

- 方法一：点击节点名称，进入节点信息页面；选择[可用区列表]页签。

- 方法二：在页面右上方选择地域，然后在导航栏中选择[可用区管理]，进入可用区列表页面。

(3) 配置边缘可用区：在可用区列表页面，点击<新建可用区>按钮，新建可用区。

参数说明如下。

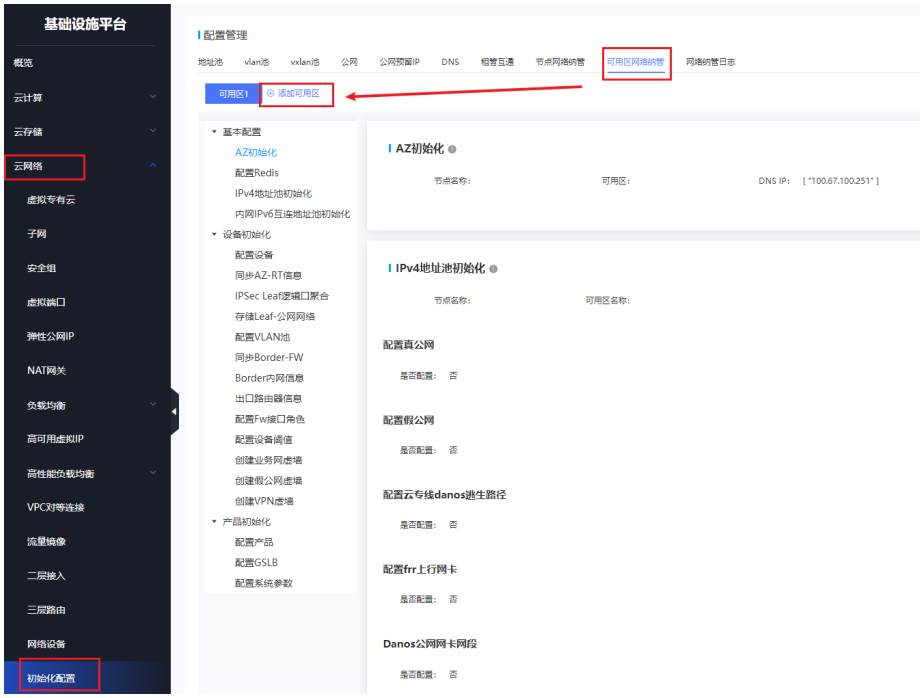
参数	说明
可用区	输入边缘可用区的名称和ID。
类型	选择<边缘站点>。
所属中心站点	每个边缘可用区必须选择一个中心可用区，一般中心可用区就是集团或者行政单位的中心节点。
终端管理地址	为边缘AZ的UCA K8S的VIP地址。
自治服务	即边缘高可用自治，当与中心的管理网中断时边缘发生的HA会由边缘AZ处理。如果不开启，边缘可用区HA的处理方式与一般可用区的处理方式相同。

(4) 填写完成后，点击<确定>按钮。

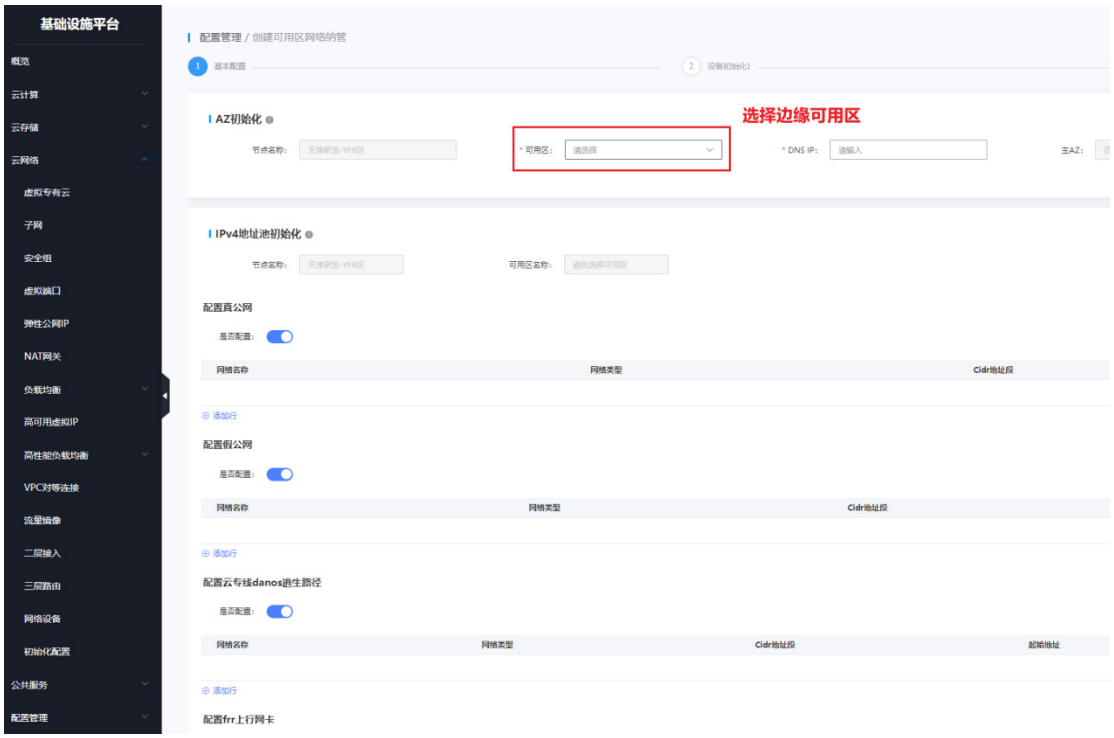
6.9.2 配置边缘可用区网络纳管

(1) 登录 OMC 运维管理系统，点击页面左上方的，选择[IAAS/基础设施平台]。

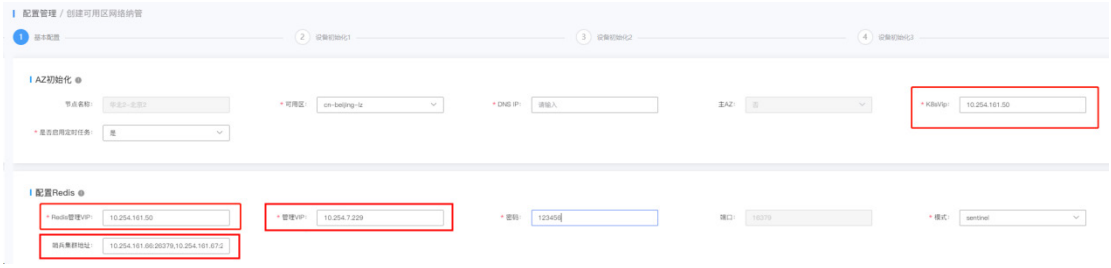
(2) 在基础设施平台导航栏，选择[云网络/初始化配置/可用区网络纳管]，点击<添加可用区>。



(3) 在创建可用区网络纳管页面，选择运营平台创建的边缘可用区，<AZ 初始化>页签下会弹出<边缘可用区 Redis 配置>页签。



(4) 填写边缘可用区 Redis 信息。



部分参数填写说明如下。

参数	说明
Redis管理VIP	需填写边缘AZ的UCA K8S的VIP地址，与AZ初始化中的K8sVip填写一致。
管理VIP	不能使用系统自填充的IP，需要改为主AZ的UCA K8S的VIP地址。
哨兵集群地址	必填项。填写边缘AZ的Redis哨兵集群IP地址段，中间用英文逗号分隔。根据哨兵集群地址的实际情况填写。（例如10.254.161.66:26379,10.254.161.67:26379,10.254.161.68:26379）。

(5) 如果环境是 Rebirth 部署工具部署，则网络初始化成功之后，以确保主 AZ 到从 AZ 之间的服务可达，需要修改部分数据库配置。修改方法可以联系研发人员进行支持。

(6) Rebirth 部署工具不支持从 AZ 部署。如果环境已经使用 Rebirth 部署工具部署，则网络初始化参数提交之后，要确保主 AZ 到从 AZ 之间的服务可达，需要修改数据库配置、服务配置文件和定时任务。修改方法可参考“6.2.2 纳管网络设备”中的“5. 从 AZ 相关改造”。

(7) 其余信息填写参考“6.2.2 纳管网络设备”中的“2. 主 AZ 纳管”。

6.9.3 配置边缘可用区计算纳管（非超融合）

适用于非超融合环境。

示例配置如下。

ONEStor集群	lz-cvk-11	UniServer R4900 G3	ONESTOR-ZZ-1		192.167.100.11
	lz-cvk-12	UniServer R4900 G3	ONESTOR-ZZ-2		192.167.100.12
	lz-cvk-12	UniServer R4900 G3	ONESTOR-ZZ-3		192.167.100.13

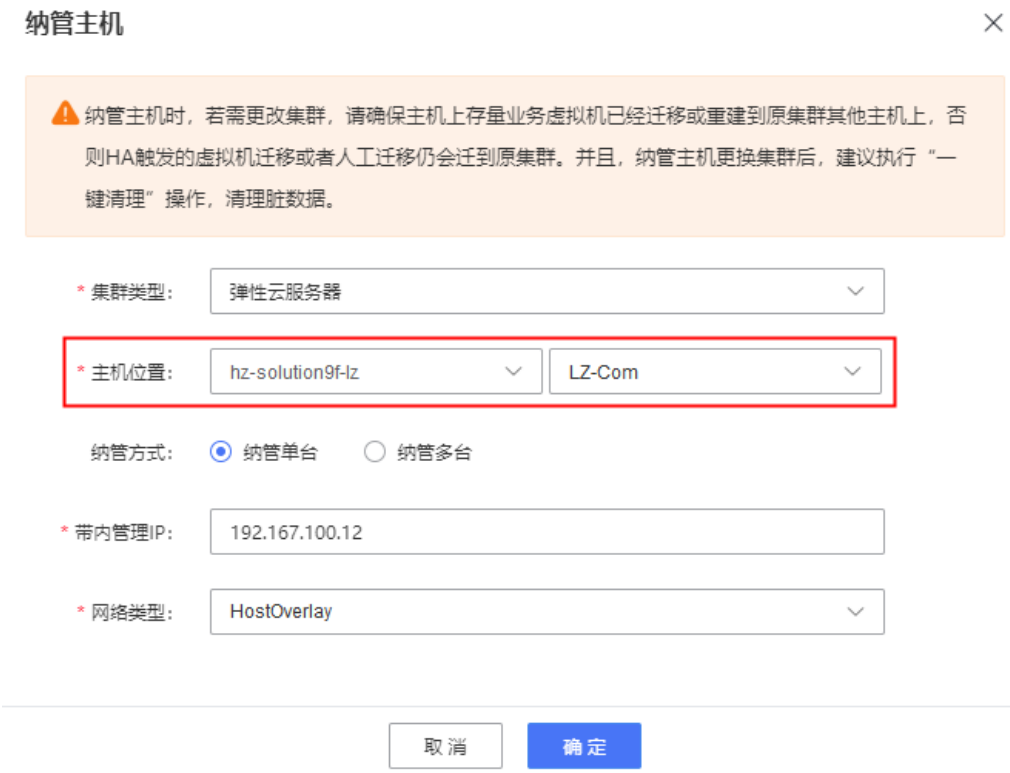
1. 纳管计算云资源

(1) 登录 OMC 运维管理系统，点击页面左上方的，选择[IAAS/基础设施平台]。

(2) 在基础设施平台导航栏，选择[云计算/宿主机集群/主机]。

(3) 点击<纳管主机>按钮，填写纳管参数。

lz-cvk-11、lz-cvk-12 和 lz-cvk-13 纳管到通用型集群。



2. 高可用数据同步

(1) 登录 OMC 运维管理系统，点击页面左上方的，选择[基础平台/节点管理]，进入节点管理页面。

(2) 点击节点名称，选择[可用区列表]页签。

(3) 点击边缘可用区后的<修改>按钮。

(4) 在修改页面，关闭自治服务开启，点击<确定>按钮；然后重新进入修改页面，开启自治服务，点击<确定>按钮。

先关闭自治服务后再启用自治服务，是为了触发主动刷新高可用数据到边缘服务。

主要是同步克隆机数据，因为克隆机数据是从母机复制过来的，而不是通过纳管，所以不能同步到边缘可用区的的边缘服务。

6.9.4 配置边缘可用区计算纳管（超融合）

边缘融合环境需要支持一机多用，也就是一个主机上可以创建不同类型的虚拟机。

本版本计算实现了调度 3.0，引入混合集群概念，从架构上支持一个主机创建多种类型虚拟机的场景，提高计算调度的灵活性。

1. 混合集群

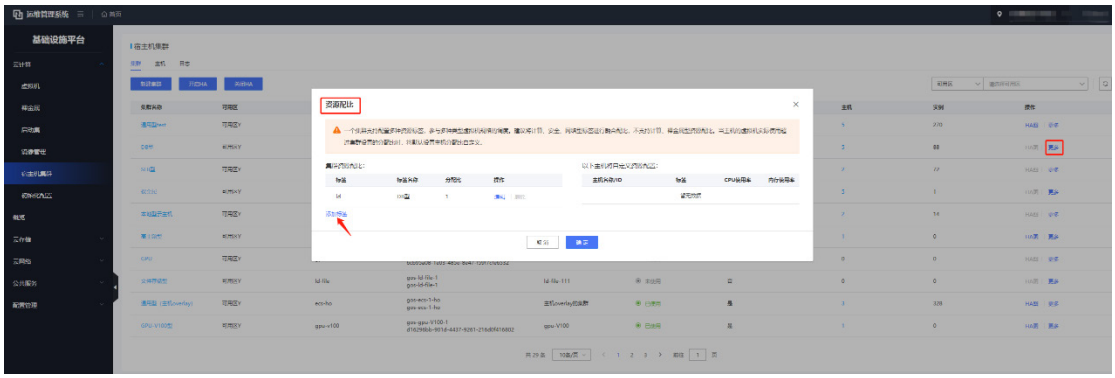
一个集群支持多种资源标签，可以创建多种类型的虚机。该集群下的主机也可以支持创建多种类型虚拟机，实现融合环境一机多用的目的。

2. 资源配置步骤

(1) 配置主机所在集群资源标签

a. 集群调整资源配比

主机当前支持 ld 类型资源：

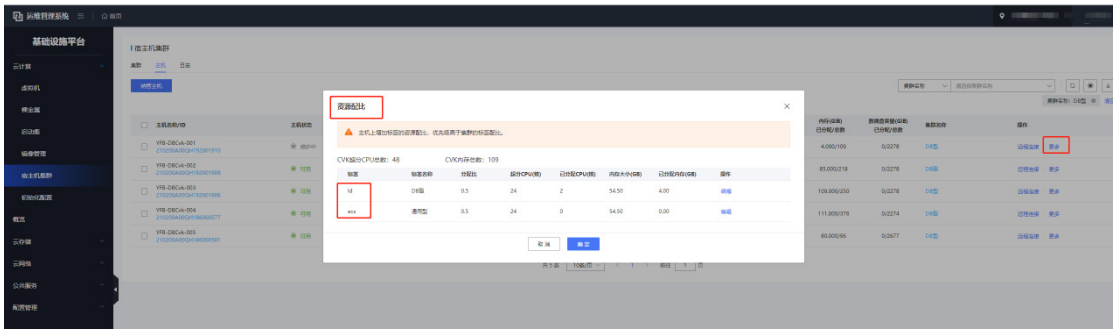


融合部署环境下，如果需要再支持 ld-net 类型，则点击[添加标签]新建，需要调整分配比，保证所有标签的分配比总和是 1，最后点击[确定]。

以上操作后，该集群就支持创建 ld、ld-net 两种类型的资源。

b. 集群内主机调整资源配比

检查主机的资源配置，支持针对主机进行配置资源分配比例。如果将某一个资源标签的[分配比]调整为 0，则主机不支持该标签类型的虚拟机创建。

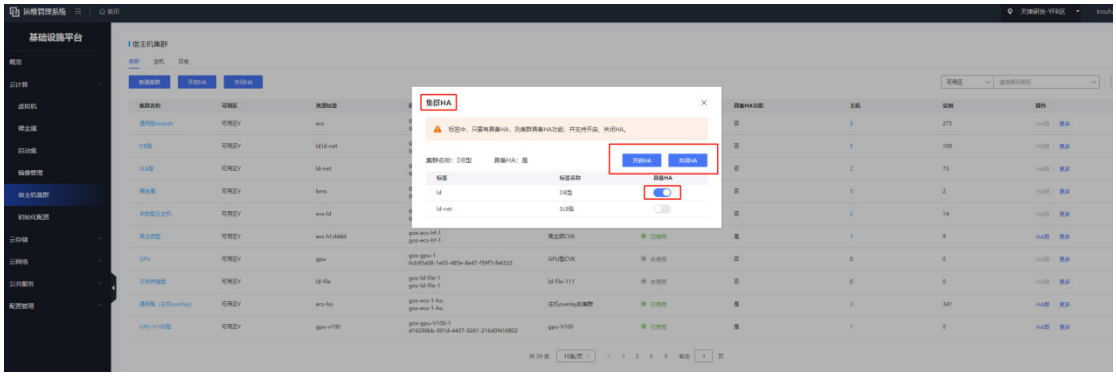


(2) HA 配置

原主机所在集群配置完集群标签后，该集群下主机支持创建多种类型的虚拟机。比如一个集群配置了标签 ecs 和 ld-net，ecs 类型的虚拟机需要开启 HA，ld-net 类型的虚拟机不开启 ha，则可以在集群列表进行配置，步骤如下。

a. 集群列表页面，选择[更多/集群 HA]。

b. 选择需要支持 HA 的标签，打开[具备 HA]按钮，然后点击[开启 HA]，则该集群已下发配置 HA。当发生异常时，主机上对应标签类型的虚拟机触发 HA。



c. 关闭 HA 时，在[集群 HA]中点击[关闭 HA]。

3. 其他

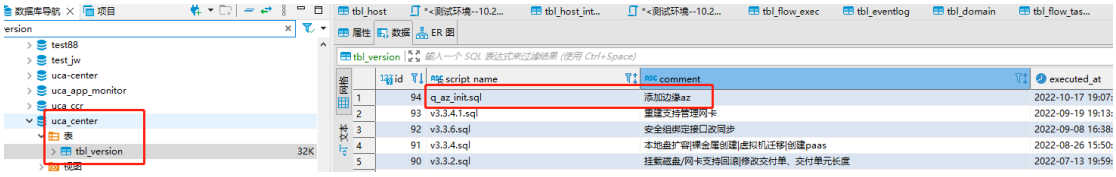
(1) 编排新增 AZ 数据

a. 请从发版路径下获取 SQL 脚本：全量包\云服务组件包\IAAS\uca-center-edge\资源超融合配置脚本\q_az_init.sql

b. 设置脚本参数，然后执行脚本。

```
use uca_center;
drop procedure if exists updateUniCompute;
delimiter //
create procedure updateUniCompute()
begin

set @regionId:='';
set @zoneId:='';

if not exists (select * from tbl_site_zone where zone_uuid = @zoneId) then
select id into @id from tbl_site_region where region_uuid = @regionId;
insert into tbl_site_zone (zone_uuid, zone_name, zone_desc, zone_state, region_id) value (@zoneId,
end if;


if not exists(select id from tbl_version where script_name ='q_az_init.sql')
then insert into tbl_version (script_name,comment) values('q_az_init.sql','添加边缘az');
end if;

end

//
delimiter ;
call updateUniCompute();
drop procedure if exists updateUniCompute;
```

c. 查看执行结果：



(2) 编排新增 az 网关脚本

请从发版路径下获取 SQL 脚本：全量包\云服务组件包\IAAS\uca-center-edge\资源超融合配置脚本\uca_center_route_gateway_add_az.sql

修改脚本参数，变量@zoneId 为新可用域的 id，修改后执行脚本。

```
use `uca_center`;

drop procedure if exists initRouteGateway;
delimiter //
create procedure initRouteGateway()
begin

-- 从az
set @zoneId:='AUTOPS_AZ_2';

-- network-api
if not exists (select * from tbl_router_gateway where service_type='uca' and service_name='api' and service_group='
and service_version='v1.0' and service_state='up' and zone_id=@zoneId and service_visible='outer')
then
INSERT INTO `tbl_router_gateway`(`service_type`, `service_name`, `service_uri`, `service_version`, `service_group`,
VALUES ('uca', 'api', 'http://uca-network-api-service:40406', 'v1.0', 'network', 'up', @zoneId, 'outer');
else update tbl_router_gateway set service_uri='http://uca-network-api-service:40406' where service_type='uca' and
and service_version='v1.0' and service_state='up' and zone_id=@zoneId and service_visible='outer';
end if;

-- network-meter
if not exists (select * from tbl_router_gateway where service_type='uca' and service_version='v1.0' and service_nam
```

4. 常见问题

(1) 边缘环境主机是否支持一键清理，是否会删除管区虚机。

本版本支持边缘环境主机执行一键清理，清理操作排除非“ecs-”开头的虚机。也就是要求管区的虚机的实例 id 不是“ecs-”开头。

(2) 边缘环境主机是否支持重新纳管、刷新操作。

支持。

(3) 边缘环境是否支持开启定时清理主机预占脏数据。

支持。另外主机 overlay dpdk 环境，主机资源使用量不会统计管区虚机。

(4) 集群标签支持最大数量

目前页面支持 3 个，A 层计算改参数是配置项，可更新数据库配置。

(5) 集群下主机的 cpu、ram 的分配比是否支持不一样配置

目前不支持。

(6) 集群、主机的资源配比，标签分配比总和是否可以小于 1

目前页面限制必须等于 1，A 层计算没有限制。

6.9.5 配置边缘可用区块存储纳管

与中心可用区纳管块存储相同，请参见“6.4 纳管存储设备”。

7 数据初始化

7.1 云平台页面登录

云平台部署完成后，即可登录产品控制台、运营控制台和运维控制台，具体登录信息及方式如下。

7.1.1 控制台登录信息

各控制台登录信息如下：

控制台	缺省登录信息
产品控制台	• URL 地址：http://nginx_vip:12011 • 用户名/密码：SPgmdd/Deve10p! 产品控制台缺省提供1个登录用户。
运营控制台	• URL 地址：http://nginx_vip:12008 • 用户名/密码：supergmdd/Deve10p!（超管账号） 运营控制台登录背景图默认通过nginx_vip获取。若已通过网络配置进行了IP映射，需在运营控制台的[系统管理/外观配置]中，单击“编辑”，修改访问地址为映射地址或映射地址对应的域名。
运维控制台	• URL 地址：https://nginx_vip:40299/#/register • 用户名/密码：无缺省用户

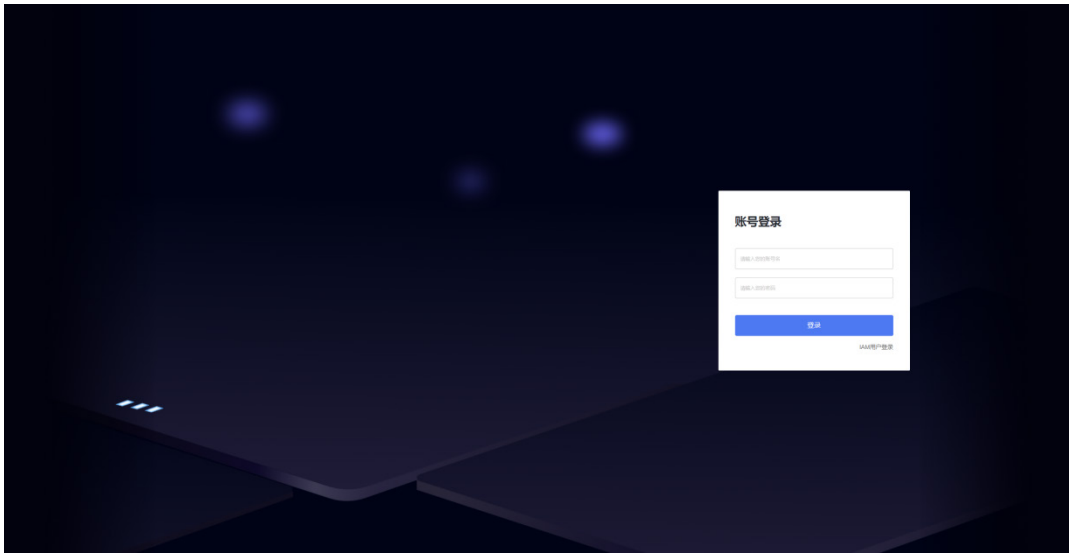
7.1.2 登录产品控制台

说明

产品控制台、运营控制台和运维控制台的登录方式相同，本文以登录产品控制台为例。

(1) 在 PC 上启动浏览器，在地址栏中输入产品控制台地址，即可进入产品控制台登录页面。

图7-1 产品控制台登录页面



(2) 输入用户名和密码，单击<登录>，即可登录产品控制台。

7.2 运营平台数据初始化

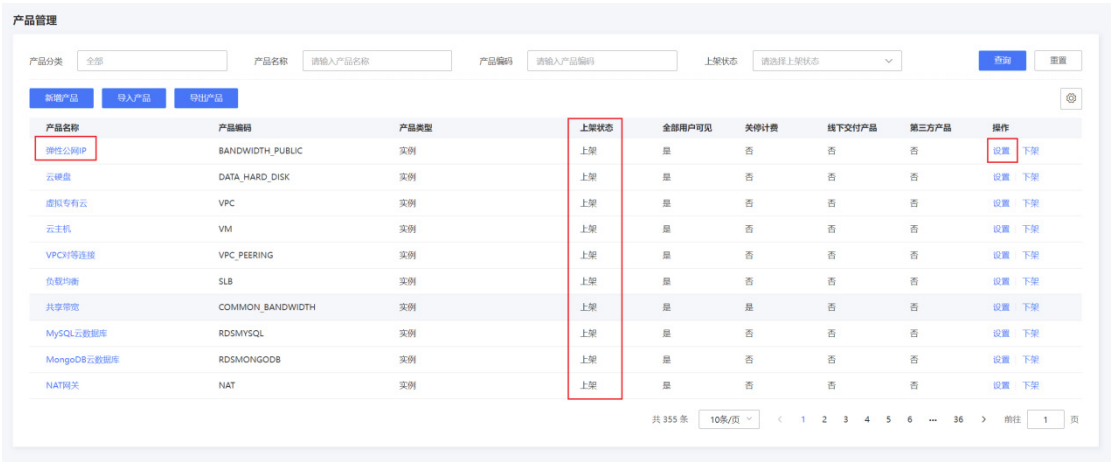
7.2.1 运营平台预置产品及配额清单

运营平台中已经内置了大部分产品规格、价格以及配额，具体可以参考运营平台中的产品列表，或向运营平台开发人员获取。

7.2.2 （可选）配置产品及可售卖项价格信息

1. 配置产品信息

(1) 登录运营控制台，在左侧导航栏选择[产品中心/产品管理]，此页面可以查看已配置的产品，以及上架状态。如果需要修改上架状态，可以在操作列进行上架或下架。

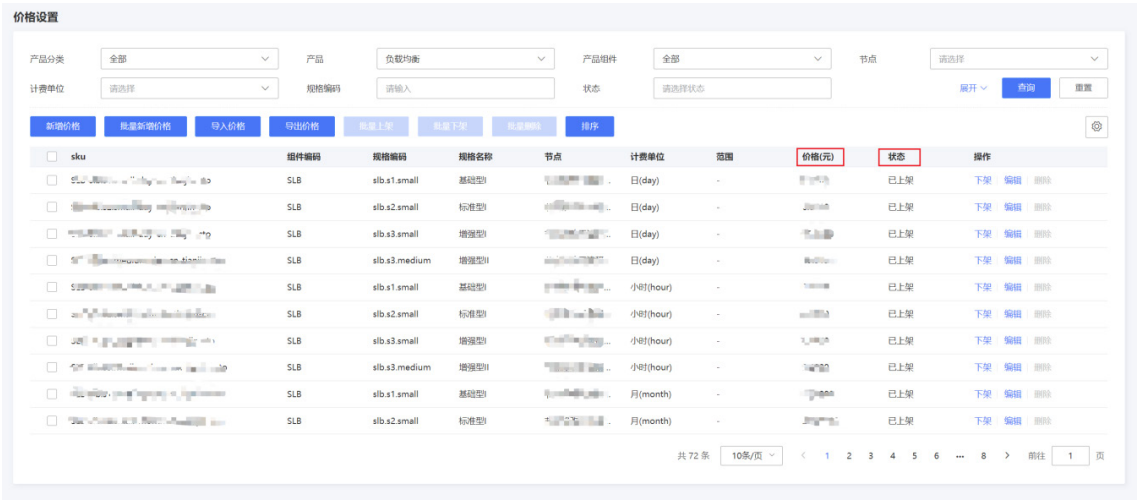


(2) 如需修改产品信息，或者新增产品，可以点击[产品名称]或[设置]，进入产品页面。针对产品节点、售卖时长、计费方式、规格族等信息，根据实际环境进行修改。

2. 配置产品价格

平台部署后，产品价格已预置，默认已上架。

(1) 登录运营控制台，在左侧导航栏选择[产品中心/价格设置]，可以查看产品价格的配置信息，以及上架状态。



(2) 如果预置价格不适用于当前环境，请根据实际情况进行修改。

- 如果云平台中尚未部署某个产品或规格，请在价格配置页面，将其手动下架，等部署完毕后再上架。例如，下图为云主机镜像规格，由于当前环境后端没有上传此镜像，因此将价格进行下架。

- 如需修改价格信息，可以点击[编辑]按钮进行修改；如需新增产品价格，可以搜索产品名称后，进入编辑页面进行修改。

7.2.3 （可选）配置邮件服务器

1. SMTP 邮件发送协议

QQ 邮箱

(1) 开启 SMTP 服务

(2) 获取 SMTP 服务器地址。

QQ邮箱的POP3与SMTP服务器是什么?

QQ邮箱 POP3 和 SMTP 服务器地址设置如下:

邮箱	POP3服务器（端口995）	SMTP服务器（端口465或587）
qq.com	pop.qq.com	smtp.qq.com

SMTP服务器需要身份验证。

163 邮箱

(3) 开启 SMTP 服务。

(4) 获取 SMTP 服务器地址。

自建邮件服务器

2. SMTP 发件人配置

常见邮件服务提供商，一般需使用发件人邮箱和授权码进行邮件的发送。

- QQ 邮箱

- 163 邮箱

- 自建邮件服务器

一般直接使用邮箱和登录密码即可。

3. Exchange 协议

一般为：{域名}/EWS/exchange.asmx。具体配置请联系 IT 获取。

7.2.4 （可选）运营平台消息中心模块

1. 发件配置说明

(1) message_core 数据库 params 表有一条“email_setting”记录，该记录中保存了发送邮件时使用到的配置，配置中包括：邮件发送协议、邮箱服务器相关配置、发件人相关配置、邮件发件人显示名称和签名。

(2) 若该数据库表中不存在此记录，可执行如下 sql 脚本增加该记录。

```
INSERT INTO `params` (`code`, `value`, `memo`) VALUES
('email_setting', '{\r\n        \"email\": \"发件人邮箱\",\r\n        \"host\": \"邮箱服务器地址
\",\r\n        \"name\": \"public_default_channel\",\r\n        \"password\": \"发件人密码或授权码\",\r\n        \"protocol\": \"邮件协议\",\r\n        \"senderName\": \"发件人显示名称\",\r\n        \"signature\": \"邮件配置
\",\r\n        \"ssl\": false\r\n}', '邮件发送配置');
```

由上边的脚本可知，配置内容是一串 json 格式的字符串，对 json 中的字段做如下说明：

- protocol -- 邮件协议：smtp 或 exchange
- host -- smtp 或 exchange 服务器名称

- port -- smtp 服务器端口（exchange 协议时不需要），一般不开启 ssl 时时 25，开启 ssl 时是 465
- ssl -- 是否开启 ssl
- email -- 发件人邮箱
- password -- 发件人密码或授权码，需加密，请联系研发进行加密处理
- senderName -- 发件人名称
- signature -- 邮件签名

(3) 配置模板

- exchange 协议

```
{
 "email": "*******",
 "host": "*******",
 "name": "public_default_channel",
 "password": "*******",
 "protocol": "exchange",
 "senderName": "*******",
 "signature": "*******"
}
```

- smtp 协议

```
{
 "email": "**********",
 "host": "*******",
 "name": "public_default_channel",
 "password": "***********",
 "protocol": "smtp",
 "senderName": "*******",
 "signature": "*******",
 "ssl": false,
 "port": 25
}
```

2. 验证

```
curl -X POST "http://10.254.7.226:31109/uco/v1/instance/remind" -H "accept: */*" -H "Content-Type: application/json" -d "[ \"7\",\"3\",\"1\",\"0\"]"
```

如果有预付费实例，可以将到期时间先改成当天时间，然后将上面的 **10.254.7.226** 改成 instance-core 服务的 SVC 的 IP，然后执行该 curl 命令，查看是否能收到邮件。验证后再把到期时间恢复成原来的。

3. 邮件发送记录

(1) message_core 数据库 message_log 表记录了所有消息的发送记录，其中 msgType 字段等于“email”的记录，表示邮件的发送记录。

(2) 记录中若 sendStatus 等于 1，则表示邮件发送成功，否则表示失败。

(3) 可按照 sendTime 字段进行倒序排列，排在最前边的即为最近发送的记录。

4. 常见问题说明

(1) 邮件发送失败原因，需通过查看 message-core 服务的日志进行定位，具体操作步骤如下：

a. 使用 ssh 工具远程连接到 UCO 的 K8S 集群

b. 查找到 message-core 服务的 pod

```
kubectl get pod | grep message-core
```

c. 查看 pod 的日志（若是多副本的情况，可逐个 pod 进行查看）

```
kubectl logs -f --tail=100 {pod 名称}
```

(2) 邮件发送失败的原因大致有如下几类情况：

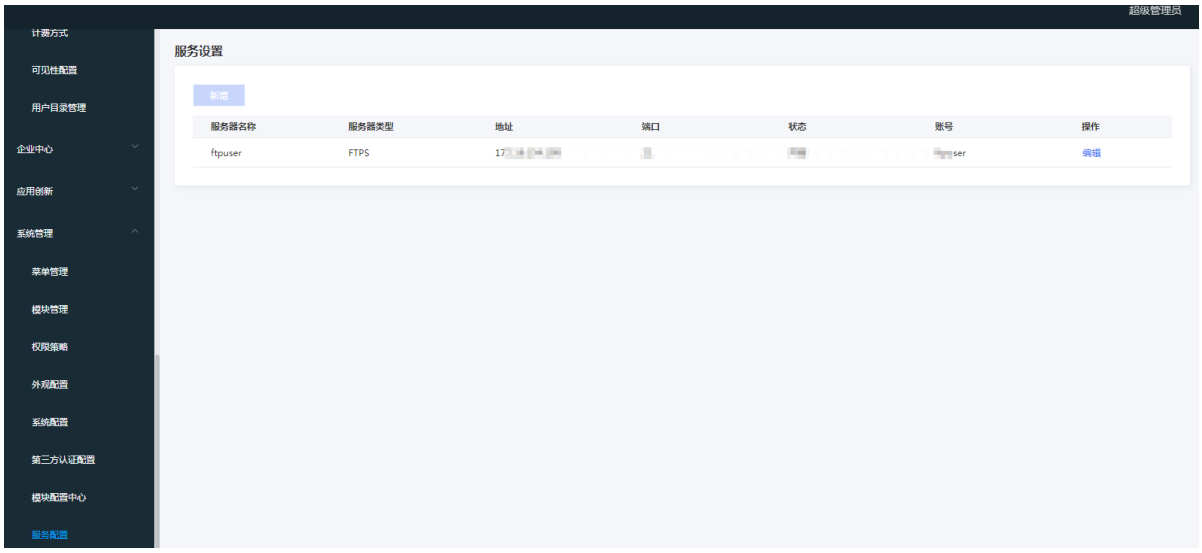
a. 连接服务器超时：请检查邮件服务器相关配置是否正确、UCO 的 K8S 集群到邮件服务器的网络是否联通正常。

b. 认证失败：请检查发件人信息配置是否正确。

c. 程序和数据库记录显示邮件发送成功，但收件人并未收取到邮件：需确保发件人的邮件服务器和收件人的邮件服务器的联通正常，如 QQ 邮箱可向 163 邮箱发送邮件，但一般情况下 QQ 邮箱不可向我们自建的邮件服务器发送邮件。

7.2.5 （可选）配置 FTP 服务器

当需要使用工单上传附件时，请先访问“运营平台 > 系统管理 > 服务配置”，配置 FTP 服务器。



7.3 运维平台数据初始化

7.3.1 登录 OMC 运维平台

(1) 登录 OMC 运维平台，地址 https://nginx_vip:40299/#/register。

(2) 在打开的页面中进行超管账号注册。填写用户名、昵称、密码、确认密码、手机、邮箱等信息。点击注册，完成超级管理员注册，超级管理员默认开启。

说明

建议使用最新版的谷歌浏览器或者火狐浏览器进行访问，以避免出现安全及浏览器兼容性问题。超级管理员且仅可注册一次，无法重复注册。

7.3.2 配置平台会话策略

(1) 超级管理员或者系统管理员登录 OMC 运维管理平台。

(2) 点击页面左上方的，选择[系统管理]。

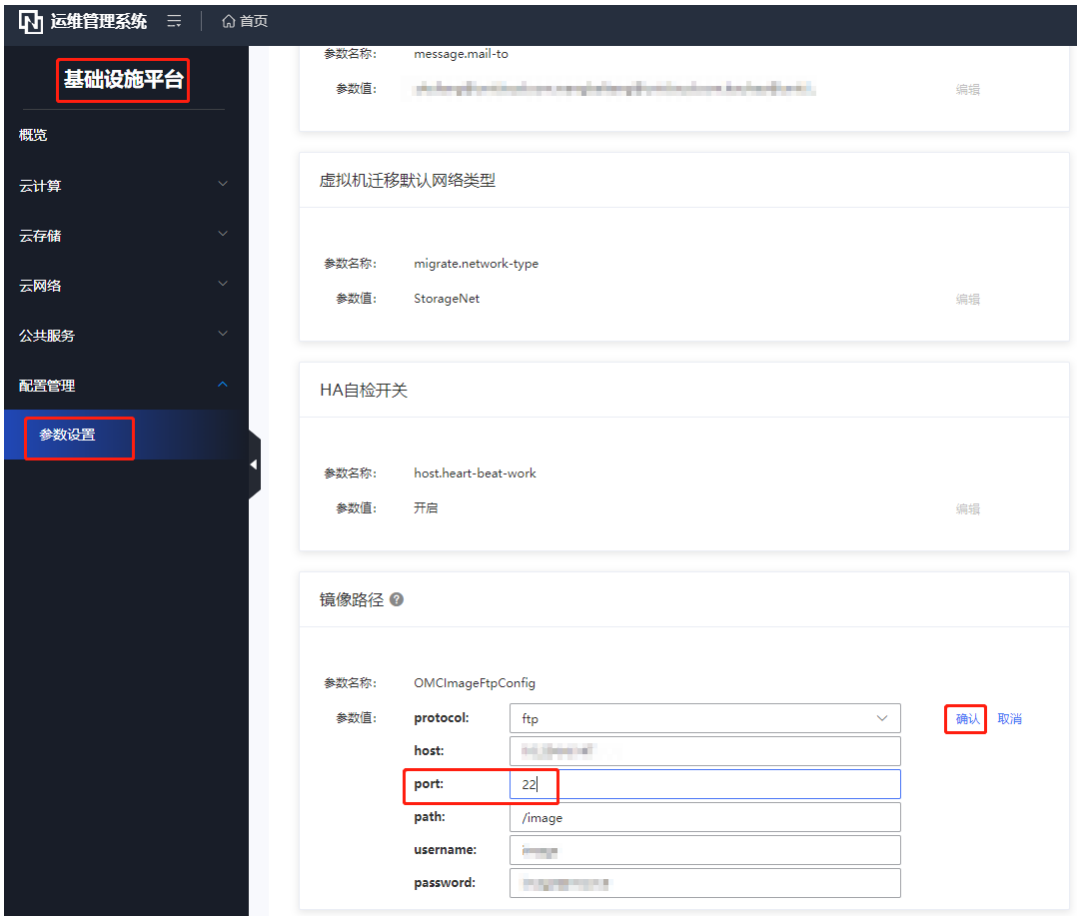
(3) 在导航栏选择[系统设置-会话策略]，按需配置会话超时策略、账号锁定策略、登录方式等。

7.3.3 基础设施平台

(1) 在数据库中执行如下 sql。

```
UPDATE `uco_omc`.`omc_system_param`
SET param_value='{"path": "/image", "port": "21", "hostname": "10.254.4.147",
"password": "image@moove", "protocol": "ftp", "username": "image"}', description=NULL,
param_type='Public'
WHERE param_key='OMCImageFtpConfig';
```

(2) 在页面选择协议并编辑端口号值触发更新 Redis，比如将端口号修改为 22 即可触发更新 Redis，然后再将该端口号修改为正确的值即可。



7.3.4 容量平台

(1) 在 OMC 运维管理平台，点击页面左上方的，选择[数据平台/容量平台]，进入容量平台。

(2) 平台初始化过程中会对部分节点及该节点对应的计算资源、块存储、文件存储、EIP 资源、SLB 资源、VPC 资源、网络设备、防火墙资源八个资源类别的调度任务进行初始化。

a. 选择[基础配置]，检查以上 8 个资源类别下的调度任务是否覆盖了全部节点，选择[任务调度]，查看调度状态是否正常。

图7-2 检查 8 个资源类别下的调度任务覆盖的节点

图7-3 检查 8 个资源类别下的调度任务状态

b. 未做配置的资源类别（对象存储，对象存储的统计服务地址为 UCO VIP），如节点内包含此服务，需要在页面上手动添加。

图7-4 添加其他资源类别

(3) 如初始化过程中添加的节点未覆盖环境内的全部节点，需要到后台数据库中手动增加数据。

a. 登录到环境中容量平台使用的 MySQL 数据库实例，根据环境实际情况替换 sql 中的变量并执行 SQL：

```
INSERT INTO `uni_cmdb_volacct`.`region_zone`(`id`, `region_id`, `region_name`, `zone_id`, `zone_name`, `region_type`, `deleted`)
VALUES (replace(uuid(),"-",""), '节点编码', '节点名称', '可用区编码', '可用区名称', 1, b'0');
```

b. SQL 执行完之后，选择[基础配置]，参照初始化的节点的任务，进行任务添加，待任务生效之后，到[任务调度]检查任务调度状态。

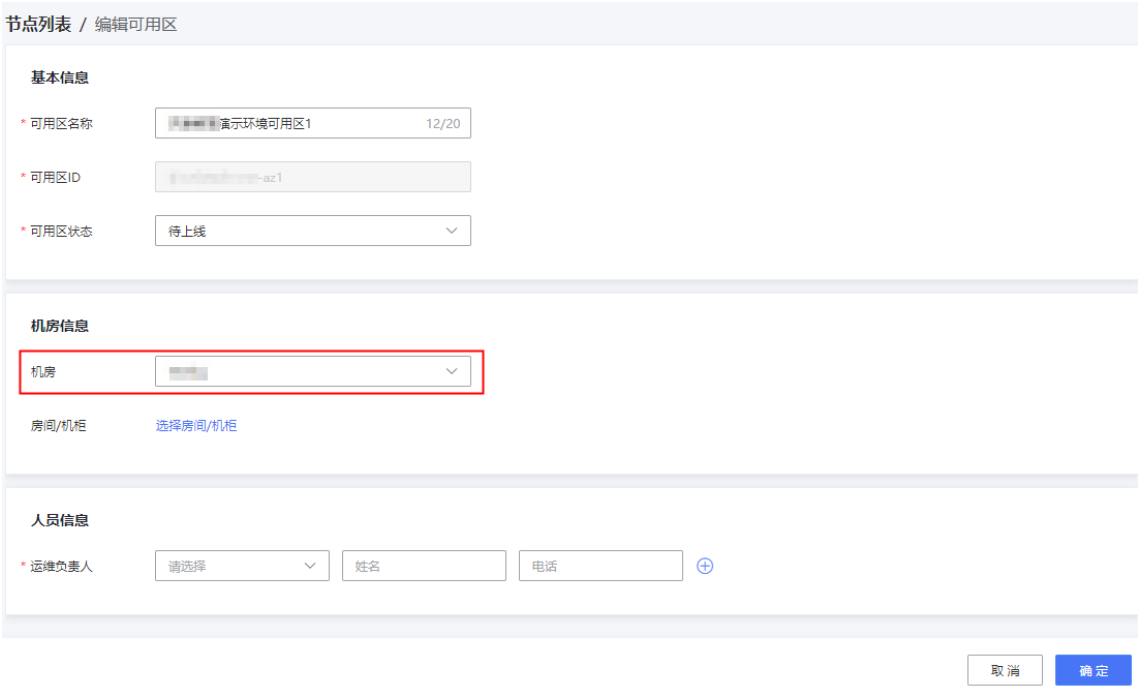
7.3.5 CMDB

1. 配置节点和可用区

(1) 在 OMC 运维管理平台，点击页面左上方的，选择[基础平台/CMDB]。

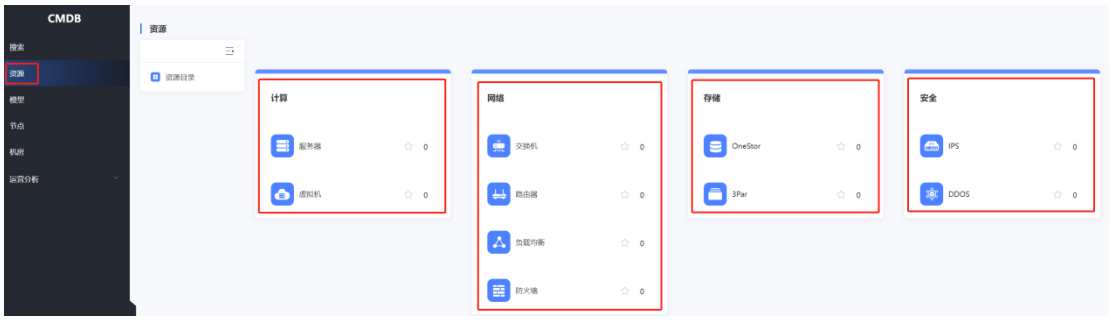
(2) 在 CMDB 导航栏，选择[节点]，查看初始化的节点、可用区信息和环境内实际情况是否一致（点击节点名称可查看可用区信息），如不一致，按照实际情况添加或修改节点、可用区。

(3) 如果可用区未绑定机房，则处于“未上线”状态。请点击可用区后的编辑按钮，将机房信息绑定到可用区，可用区才能上线。



2. 配置资源

(1) 在 CMDB 导航栏选择[资源]，依据节点内设备的实际情况，依次对服务器、虚拟机、交换机、路由器、负载均衡、防火墙（含虚拟防火墙），SDS、3Par（含 Primera），IPS、DDOS 类别的资源进行添加，各个类别需独立下载模板填充数据并进行导入，业务类型和应用标签可参考业务类型与应用标签对照表（请从版本发布路径获取：全量包\云服务组件包\OMC\omc-监控配置.zip，解压缩后得到《业务类型-应用标签.xlsx》）。如一个资源实例具有多个应用标签，用英文逗号隔开。



(2) 完成导入后，确保全部的资源实例处于“运行中”状态。

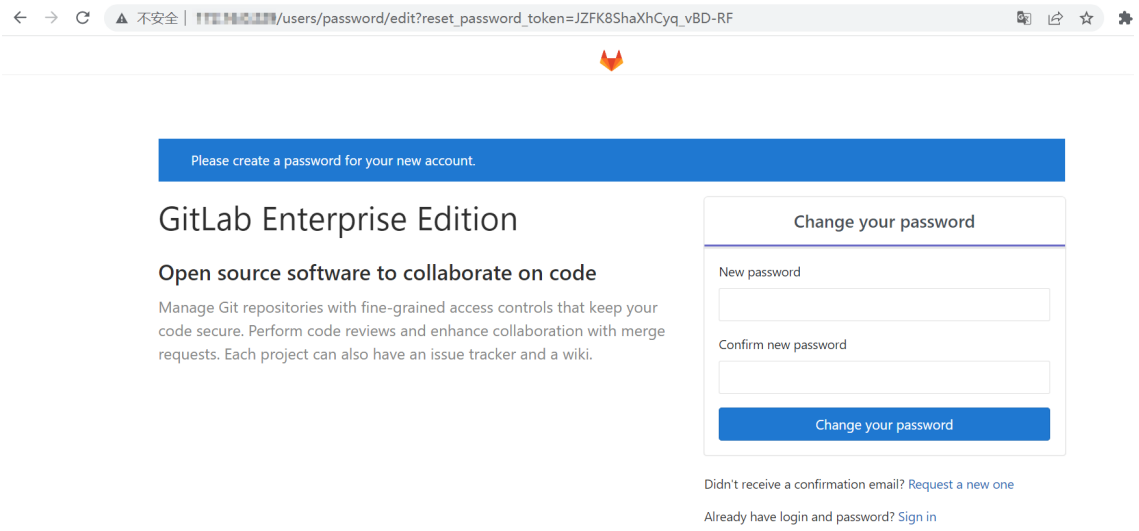
注意

需特别注意的是，当前版本的 Redis 高可用方案为一主一从一哨兵模式，对应的三个 Redis 节点的业务类型应为 redis，主从节点的应用标签应为 redis，哨兵节点的应用标签应为 default，务必配置正确。

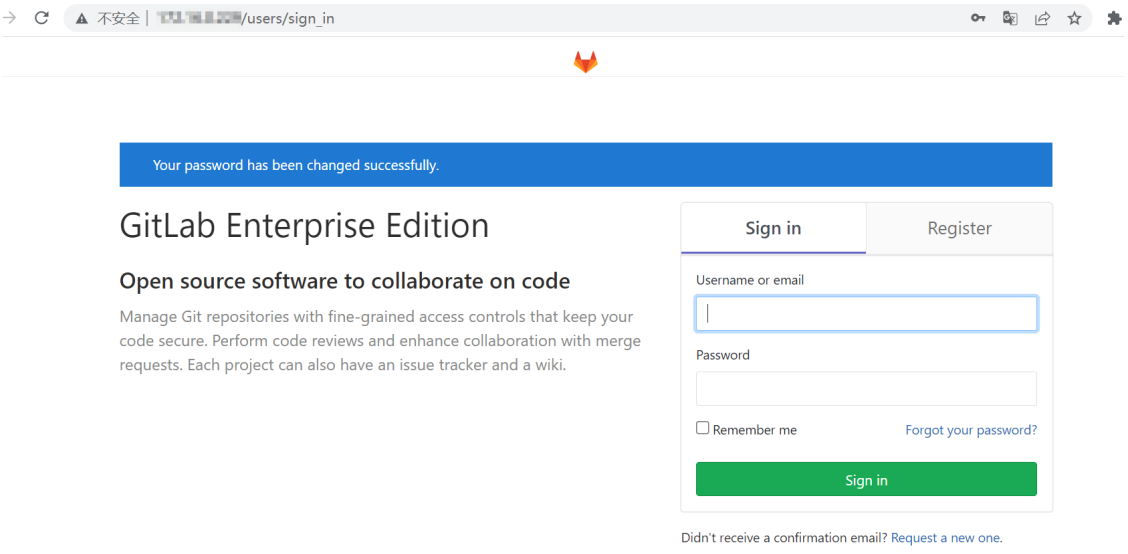
7.3.6 作业平台

1. 配置 GitLab 服务器

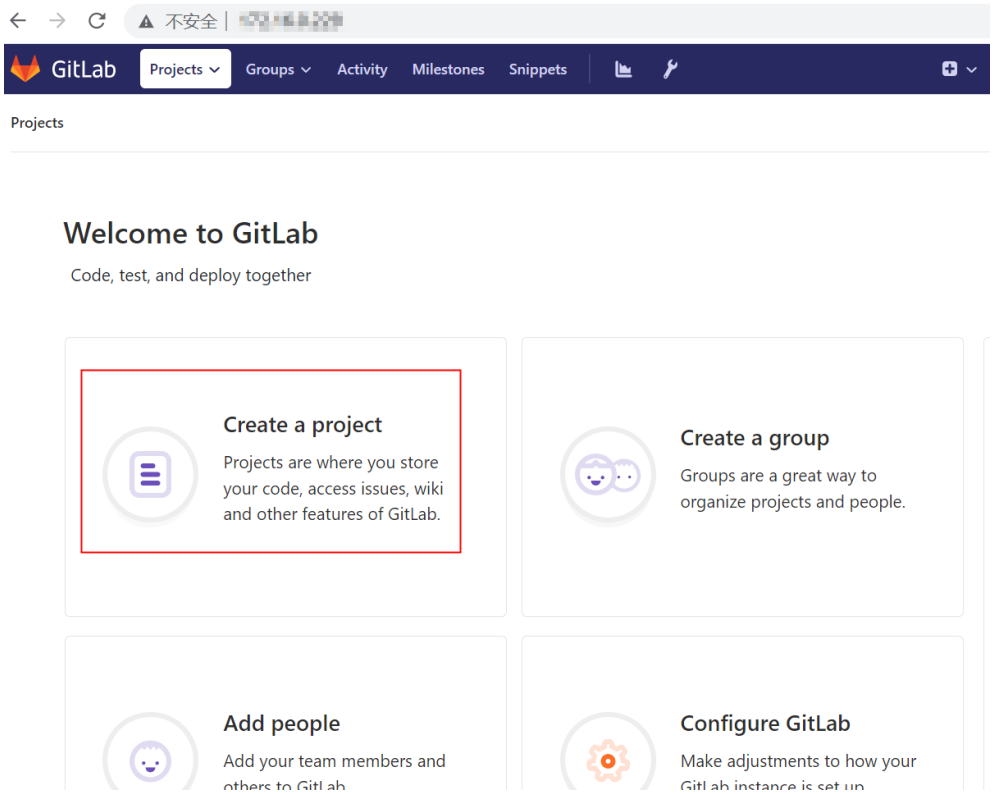
(1) 登录到 GitLab 服务器，设置 root 用户的密码为 Tstyllr123，地址为 http://gitlab_vm_ip，两次键入密码后点击<change your password>按钮，更新密码。



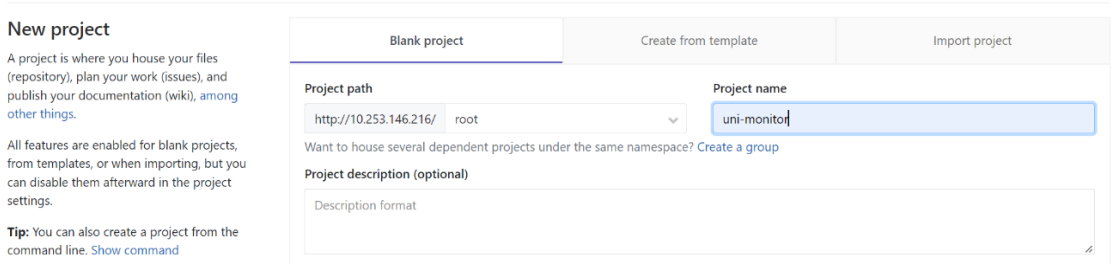
(2) 使用创建的用户名密码登录到平台上。



(3) 点击 Create a project。

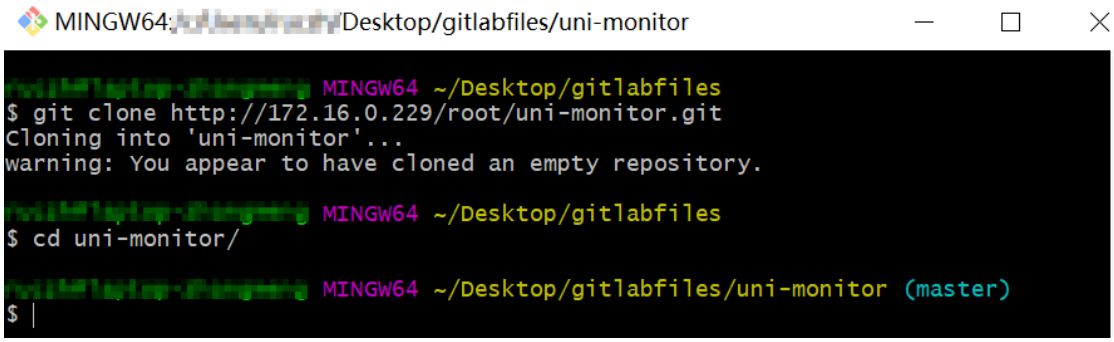


(4) 新建一个名为 uni-monitor 的项目。IP 地址请修改为实际环境的地址。

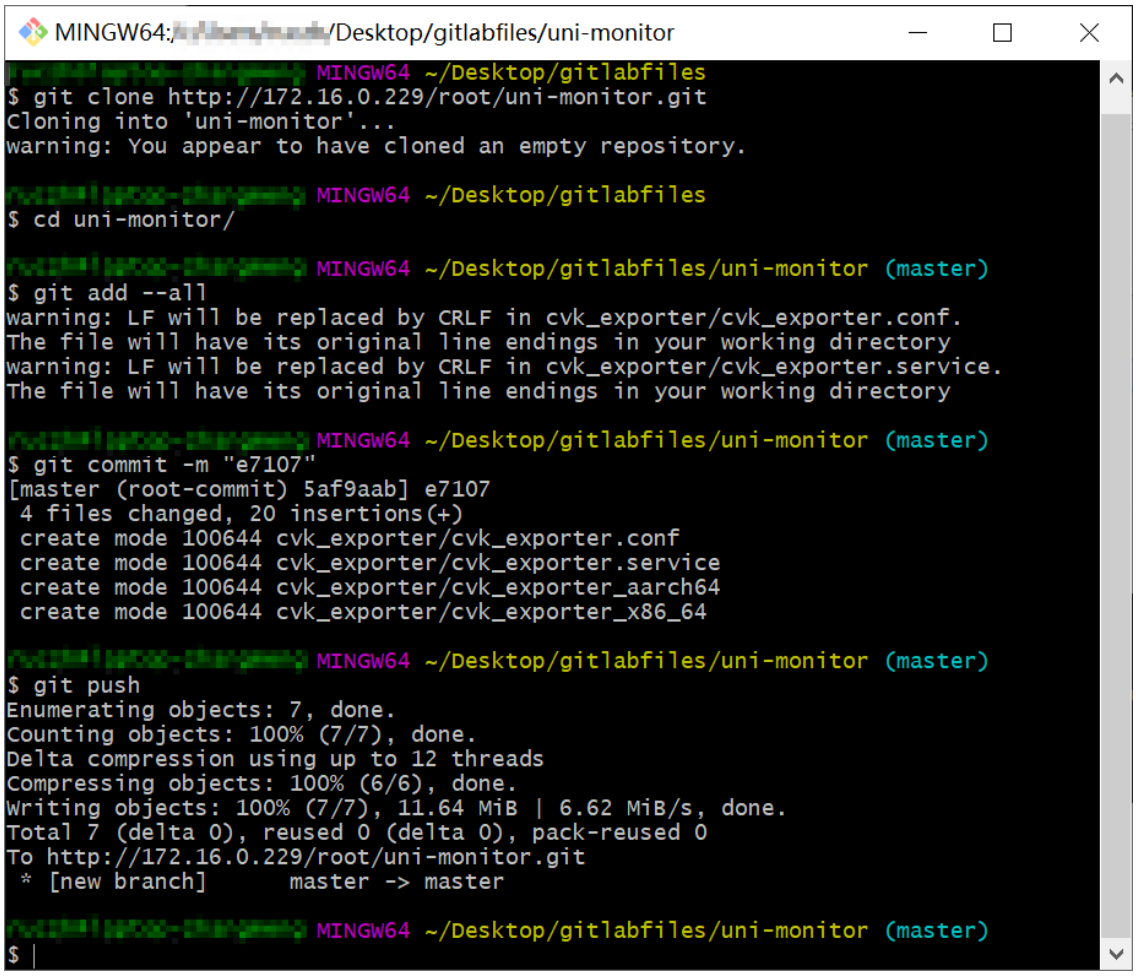


(5) 在安装了 Git 客户端的本地电脑上，新建一个临时文件夹。进入文件夹中，在空白处右键选择<Git Bash Here>。如果本地电脑上没有 Git 客户端，请到官网下载，地址为 https://git-scm.com/downloads。

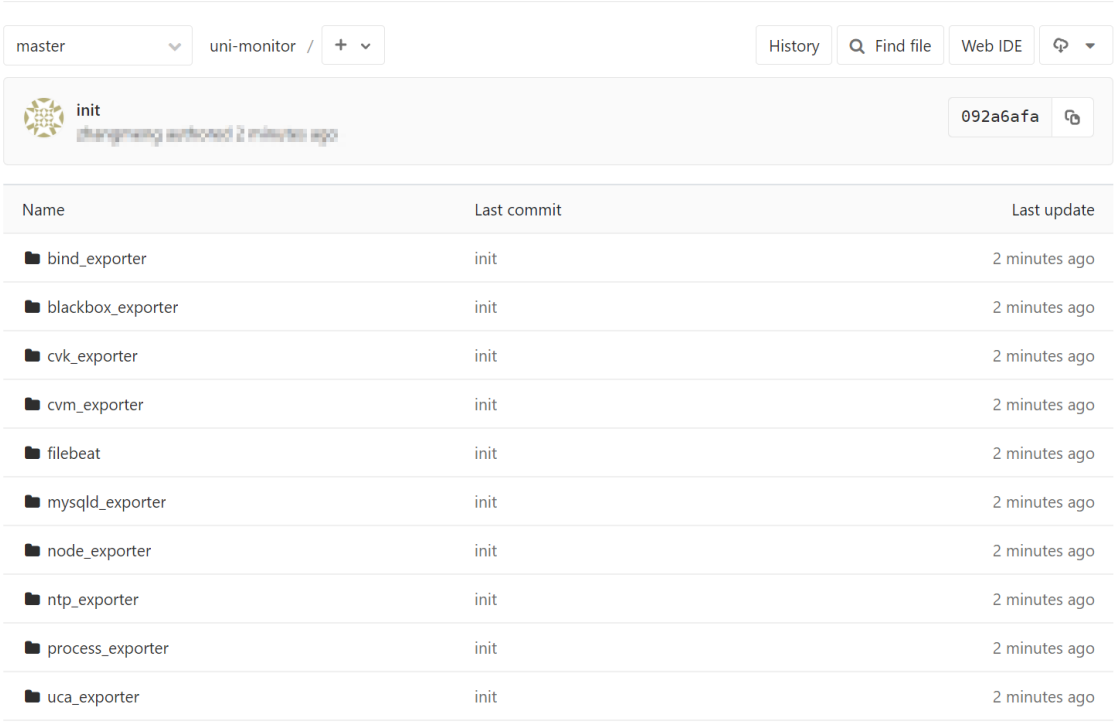
(6) Clone 刚刚新建的项目 uni-monitor，并进入项目文件夹，输入 GitLab 页面设置的用户名和密码。如下图所示。



(7) 在版本发布路径下，找到“omc-监控配置”文件夹，将 EXXXX-basefiles 中的归档文件提交到 GitLab 上，提交时注意分支需为 Master 分支。过程如下，此处仅作命令示例，不代表实际提交文件列表。



(8) 完成提交之后可到页面确认提交状态，如下图所示。



2. 配置 K8S 节点

(1) 登录到 UCA K8S 节点，进入“omc namespace”下的“pod omc-saltstack-0”内，执行 salt-run fileserver.update 命令触发 SaltStack gitfs 更新并查看更新状态，如无错误，执行 salt-run fileserver.file_list 命令查看 gitfs 中的文件列表。

```
[root@[redacted]-UCA-Node1 ~]# kubectl -n omc exec -ti omc-saltstack-0 sh
/ # salt-run fileserver.update
True
/ # salt-run fileserver.file_list
- basefiles/bind_exporter/bind_exporter
- basefiles/bind_exporter/bind_exporter.service
- basefiles/blackbox_exporter/blackbox.service
- basefiles/blackbox_exporter/blackbox.yml
- basefiles/blackbox_exporter/blackbox_exporter
- basefiles/cvk_exporter/cvk_exporter
- basefiles/cvk_exporter/cvk_exporter.service
```

如更新后无文件列表显示，重启 pod 并重新更新 gitfs，再次查看。

(2) 执行命令 salt-key -A 接受 pod 内 salt-minion，然后执行命令 salt-key -L 查看已所有状态的 key。

```
/ # salt-key -A
The following keys are going to be accepted:
Unaccepted Keys:
master
Proceed? [n/Y] y
Key for minion master accepted.
/ # salt-key -L
Accepted Keys:
master
Denied Keys:
Unaccepted Keys:
Rejected Keys:
/ #
```

3. 配置 OMC 运维平台

(1) 在 OMC 运维管理平台，点击页面左上方的，选择[告警监控/作业平台]，进入作业平台。

(2) 选择[工具管理]，点击[新建]添加 SaltStack 实例，按照节点内的 IP 规划实际情况，进行添加。

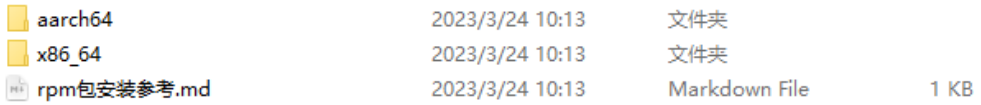
(3) EndPoint 栏填写 A 层 VIP，端口为 10106（Salt-API 的缺省用户名及密码为：salt/devops2020@Salt）。选择对应节点，状态为启用，完成添加。

(4) 客户端管理。

a. 除业务 VKS 以外的其他设备。

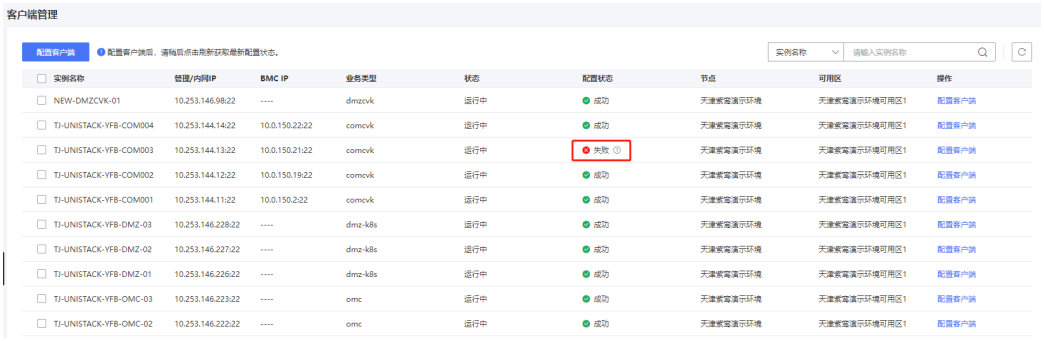
除业务区 VKS 外，其他设备均需要完成 salt-minion 服务安装及其依赖的 Python3 环境安装。其中管区虚拟机 salt-minion 系统里已经装好，只需要安装 Python3 的安装包即可。

a) 从解压缩后的 saltstack-rpms 中，根据当前实例的 CPU 架构类型，获取里面的 rpm 包。安装包请从版本发布路径获取：全量包\云服务组件包\OMC\omc-监控配置.zip。具体安装步骤见（saltstack-rpms\rpm 包安装参考.md）。



b) 选择[客户端管理]，优先配置“资源类型”为“uca”的服务器，待此类型的服务器安装成功后，再批量选择剩余服务器，单击“配置客户端”。

c) 对于配置状态为“失败”的实例，需要进入实例内部执行 systemctl status salt-minion 查看是否状态异常。



b. 业务区 VKS。

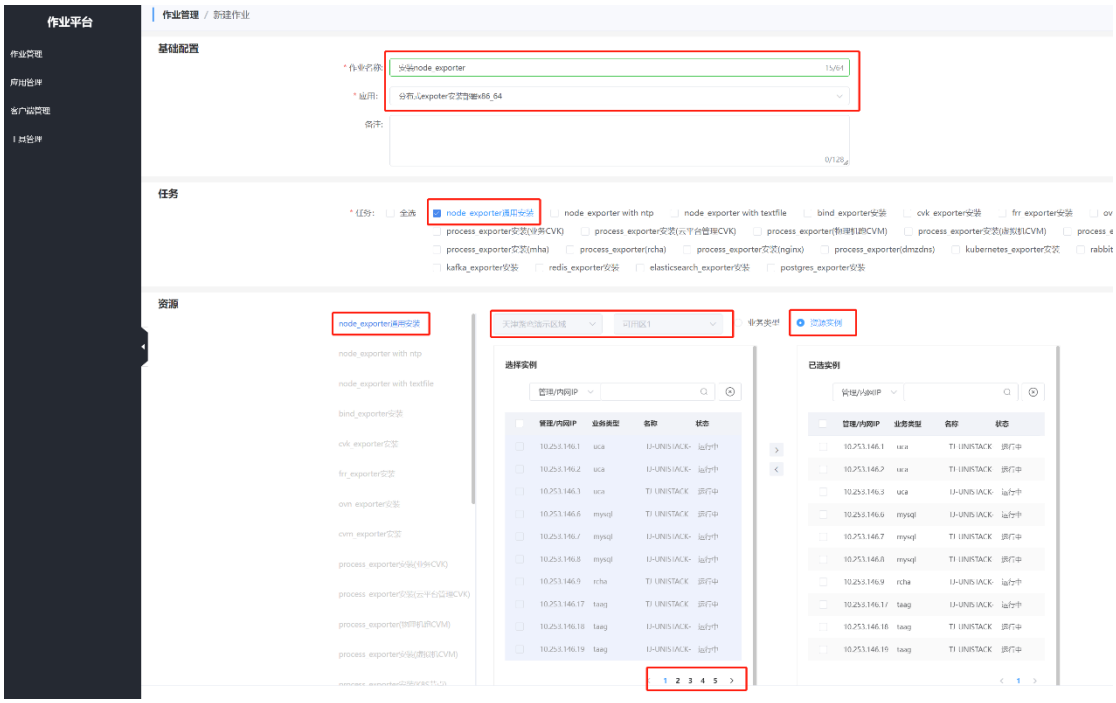
自动初始化的 VKS 已经自动安装过 salt-minion 服务及其依赖的 Python3 环境。直接配置客户端即可。

选择[客户端管理]，对业务区 VKS 实例进行“配置客户端”操作。

(5) 所有服务器资源的客户端配置成功后，选择[应用管理]，这里预制有安装 exporter 所需的应用，并已绑定好各 exporter 适用的业务类型。依次新建作业，进行分布式 exporter 的安装。

(6) 点击[创建作业]，填入作业名称，选择正确应用（默认为创建作业按钮对应的应用，可切换），选择需要执行的任务。

由于任务较多，建议每个任务单独创建一个作业，选择需要执行的节点、可用区，勾选资源时，建议以“资源实例”维度进行选择，注意左侧待选实例列表下方的分页标志，需分页多次全选，资源实例选择完成后点击确定完成作业创建。



(7) 作业创建完成后，点击[立即执行]执行作业。所有 exporter 安装完成后进入[监控平台]进行后续配置。

7.3.7 监控平台初始化

1. 配置网络设备侧 SNMP

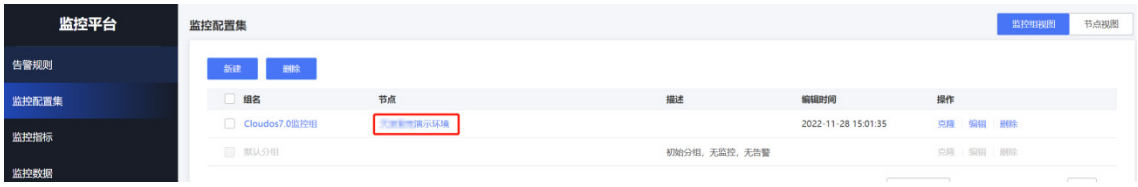
若要对网络设备进行监控，需要在网络设备中开启 SNMP 功能。当前平台支持 v1、v2c 版本，推荐使用 v2c 版本。若要使用 Trap 管理功能，请将接收 Trap 告警信息的目的主机（target-host）配置为 UCA 集群的 VIP。

2. 配置监控平台

(1) 在 OMC 运维管理平台，点击页面左上方的  ，选择[告警监控/监控平台]，进入监控平台。

(2) 选择[监控配置集]，编辑名为“Cloudos7.0 监控组”的监控配置集，将环境内的节点全部关联到此配置集。

关联后：



(3) 点击节点列种对应节点的名称，如上图中的[*XXXX* 演示环境]，进入该节点的监控配置集页面。

(4) 请检查监控配置集是否下发成功。

(5) 等待一至两分钟后，打开 Prometheus 管理页面（http://UCA_VIP:19090、http://UCA_VIP:29090），监控平台页面点击“节点名称”（如：*XXXX* 演示环境）切换到节点视图。

(6) 依次点击 Targets 列表中的条目，查看关联的实例信息，与 Prometheus 管理页面的实例信息进行对比，确保数据一致，如不一致请勾选该条目并点击[立即下发]进行刷新。

(7) prometheus 管理页面上的所有 target 应处于 up 状态，如有 down 状态的，需依次排查该 target 对应机器上的 exporter 是否完成安装，服务状态是否正常，prometheus 到 exporter 的网络是否可达。

(8) 规则下发完成后，检查 prometheus 上有无告警产生，与前台页面上显示的是否一致，确认告警发送链路无异常后，需依次解决已触发的告警，确保问题在节点彻底初始化完前解决。

7.3.8 （可选）扩容监控平台

监控平台 Prometheus 组件需要根据纳管的 VKS 设备数量来灵活配置资源规模。当资源不足时，监控数据采集和告警规则的计算过程中会出现脏数据。平台中有可能会出现以下问题：基础设施平台的概览页面中的 CPU 利用率有可能为负。此时需要对监控平台进行扩容。

1. 步骤说明

扩容步骤为：

(1) 评估 Prometheus 需要的资源规模

(2) 修改 Prometheus 配置

(3) 验证扩容是否成功

1. 评估 Prometheus 需要的资源规模

根据节点纳管的 VKS 设备数量来评估 Prometheus 需要的资源规模，对应关系如下：

- 100 台 VKS：limit8C8G
- 200 台 VKS：limit8C16G
- 300 台 VKS：limit8C24G

2. 修改 Prometheus 配置

由于监控平台的 Prometheus 组件是部署在 UCA 集群内中，需要在 UCA 的 K8S 集群中进行对应修改。

(1) 在 UCA 的 K8S 集群中，执行如下命令，编辑 omc-prometheus 文件：

```
kubectl edit -n omc statefulset.apps/omc-prometheus
```

(2) 执行后需要将 resources.limit.cpu、resources.limit.memory 的值替换为评估的资源数量。

(3) 替换后保存退出。

```
      containers:
      - args:
        - --config.file=/etc/prometheus-config/$(HOSTNAME).yaml
        - --storage.tsdb.path=/prometheus
        - --storage.tsdb.retention.time=3d
        - --web.enable-lifecycle
        - --web.console.libraries=/usr/share/prometheus/console_libraries
        - --web.console.templates=/usr/share/prometheus/consoles
        env:
        - name: HOSTNAME
          valueFrom:
            fieldRef:
              apiVersion: v1
              fieldPath: metadata.name
        image: harbor-local.unicloudsrv.com/library/prometheus:v2.24.0
        imagePullPolicy: IfNotPresent
        name: omc-prometheus
        ports:
        - containerPort: 9090
          protocol: TCP
        resources:
          limits:
            cpu: "8"
            memory: 8Gi
          requests:
            cpu: "4"
            memory: 4Gi
        terminationMessagePath: /dev/termination-log
        terminationMessagePolicy: File
        volumeMounts:
        - mountPath: /etc/prometheus-config
          name: config
        - mountPath: /etc/prometheus-rules
          name: rules
:wq
```

(4) 执行如下命令，重启 Pod。

```
kubectl delete pod -n omc -l app=omc-prometheus
```

```
[root@TJ-UNISTACK-YFB-UCA-K8S-01 ~]# kubectl delete pod -n omc -l app=omc-prometheus
pod "omc-prometheus-0" deleted
pod "omc-prometheus-1" deleted
```

(5) 待服务重启完成后即扩容成功。

3. 验证扩容是否成功

(1) 在 UCA 的 K8S 集群中，执行命令：

```
kubectl describe -n omc pod omc-prometheus-0
kubectl describe -n omc pod omc-prometheus-1
```

```
[root@TJ-UNISTACK-YFB-UCA-K8S-01 ~]# kubectl describe -n omc pod omc-prometheus-0
Name:         omc-prometheus-0
Namespace:    omc
Priority:     0
Node:         10.253.146.1/10.253.146.1
Start Time:   Tue, 14 Mar 2023 07:19:27 +0000
Labels:       app=omc-prometheus
              controller-revision-hash=omc-prometheus-65f6d54f94
              statefulset.kubernetes.io/pod-name=omc-prometheus-0
Annotations:  <none>
Status:       Running
IP:           10.244.2.61
IPs:
  IP:           10.244.2.61
Controlled By:  StatefulSet/omc-prometheus
Containers:
  omc-prometheus:
    Container ID:  docker://fcc86b77df9fe589ea7d23dc23c1041a0d5cb15276cf529531dc941d2bdb3037
    Image:         harbor-local.unicloudsrv.com/library/prometheus:v2.24.0
    Image ID:      docker-pullable://harbor-local.unicloudsrv.com/library/prometheus@sha256:114cc056795b021473c1195cd2ed4a258f8da6c0d006a755ef1fccabd5d216ed
    Port:          9090/TCP
    Host Port:     0/TCP
    Args:
      --config.file=/etc/prometheus-config/$(HOSTNAME).yaml
      --storage.tsdb.path=/prometheus
      --storage.tsdb.retention.time=3d
      --web.enable-lifecycle
      --web.console.libraries=/usr/share/prometheus/console_libraries
      --web.console.templates=/usr/share/prometheus/consoles
    State:          Running
      Started:      Tue, 14 Mar 2023 07:19:28 +0000
    Ready:          True
    Restart Count:  0
    Limits:
      cpu:     4
      memory:  8Gi
    Requests:
      cpu:     2
      memory:  4Gi
```

(2) 查看回显中 Limits 字段的扩容结果，确认是否扩容成功。

```
    State:          Running
      Started:      Tue, 14 Mar 2023 07:19:28 +0000
    Ready:          True
    Restart Count:  0
    Limits:
      cpu:     4
      memory:  8Gi
    Requests:
      cpu:     2
      memory:  4Gi
```

7.3.9 日志平台

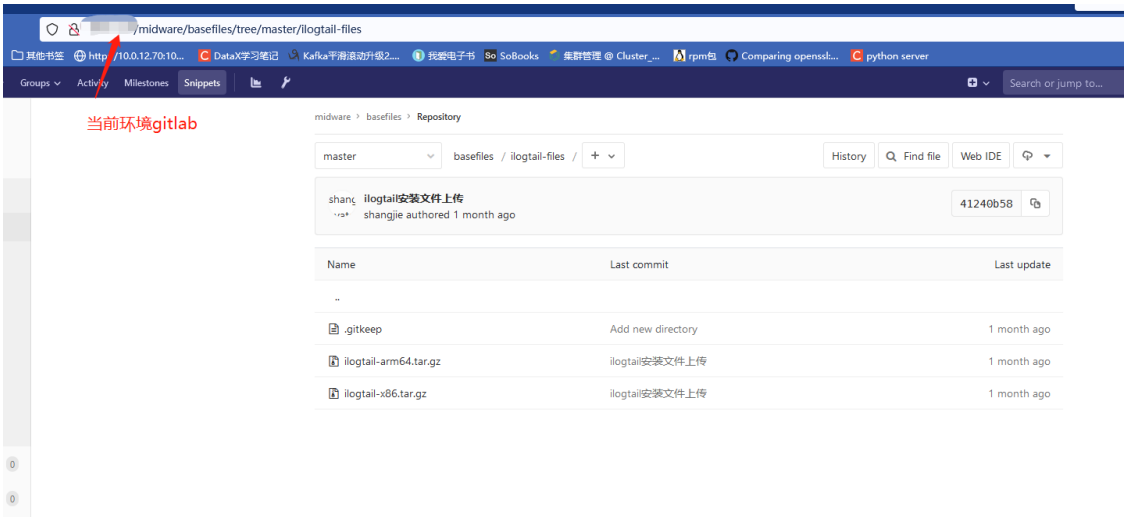
1. 链路日志

链路日志平台在服务启动后，无后续的组件部署、配置、调整等工作，可直接到页面上查看链路日志收集情况，如出现数据为空的情况，重点检查 ElasticSearch 集群状态，Kafka 地址配置，ElasticSearch 地址配置是否正确。

2. 上传 Ilogtail 安装包到 gitlab

(1) 在当前环境 gitlab 的 uni-monitor 目录下新建 ilogtail-files 目录。

(2) 将 ilogtail 安装包 ilogtail-arm64.tar.gz/ilogtail-x86.tar.gz 上传到 uni-monitor/ilogtail-files 目录下。ilogtail 安装包获取路径为：全量包\云服务组件包\OMC\日志平台。



3. 服务异常处理建议

如启动服务后运行日志功能报错，建议在 OMC K8S 集群中执行以下命令重启 omc-peafowl-smart 服务。

```
kubectl delete pod -l app=omc-peafowl-smart -n omc
```

7.4 对象存储初始化

通过 SDS 创建对象存储时，需要执行如下操作，完成与云平台的对接。

7.4.1 前提条件

- 对象存储使用的 SDS 搭建完成，并且建立好存储池、高可用组、DNS 等，使用 SDS 自身的 AK 和 SK 可以访问对象存储。
- 使用自动部署工具部署时，变量中的域名和解析的地址填写正确，域名使用 SDS 高可用组的全局域名，解析地址使用高可用组的地址中的一个。
- 已完成运营平台的部署，且工作正常。
- 已完成运维平台 OMC 的部署，且工作正常。
- 确保云平台可以正常生成 AK 和 SK。
- 完成了对象存储 UCO 层的部署(oss-core-deployment 能正常生成 POD)。

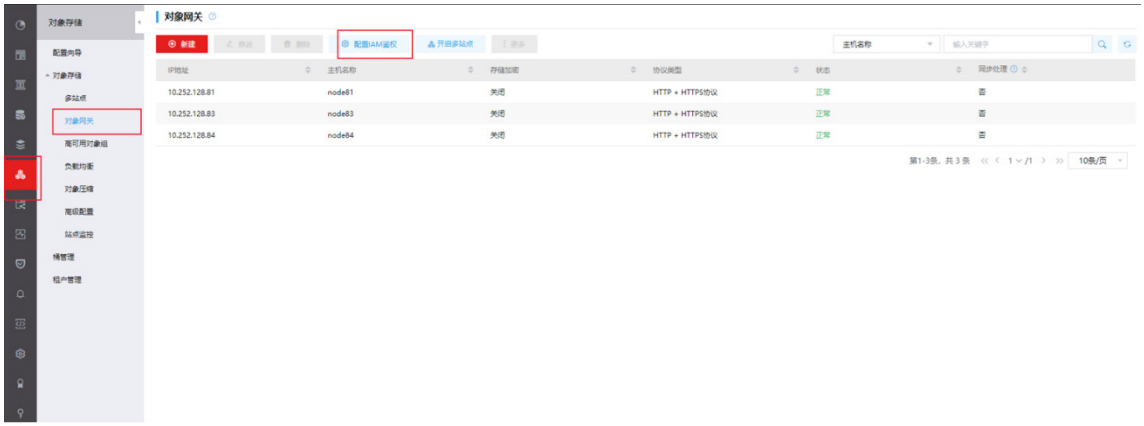
7.4.2 准备工作

- 登录产品控制台，使用主账号或者单独账号生成 AK 和 SK。
- 获取对象存储 handy 的登录方式。
- 运营平台上，将已完成部署的对象存储相关产品上架。

7.4.3 SDS3 对接步骤

(1) 登录 SDS3 的 handy 页面(缺省的账号和密码为 admin、Admin@123)。

(2) 依次选择[对象存储/对象网关/配置 IAM 鉴权]。



(3) 配置 IAM 鉴权

IAM 鉴权中心 URL 请填写: http://<UCO 的 VIP>:30990

IAM 鉴权中心路径请填写: oss/IamBlackUser/access/info。请注意这里 Iam 中的 I 必须使用大写字母。

管理用户 AK 和 SK 请根据准备工作中，通过产品控制台获取到的 AK 和 SK 进行填写。

(4) 等待 IAM 鉴权建立完成。

(5) 使用浏览器访问 https://<endpoint 地址>，勾选信任 HTTPS 证书。

(6) 修改本地机器的 Host，可以正确解析出对象存储的 Endpoint 域名地址。

(7) 使用浏览器登录云平台，访问对象页面。

如果是第一次访问，点击页面上的<开通对象存储>按钮即可，依次点击<确定>，最后重新在主菜单上点击<对象存储>，即可访问对象存储。

7.4.4 SDS5 对接步骤

(1) 登录 SDS5 的 handy 页面(缺省的账号和密码为 admin、Admin@123)。

(2) 依次选择[对象存储/高级配置/配置 IAM 鉴权]。

(3) 配置 IAM 鉴权

IAM 鉴权中心 URL 请填写：http://<UCO 的 VIP>:30990

IAM 鉴权中心路径请填写: oss/IamBlackUser/access/info。请注意这里 Iam 中的 I 必须使用大写字母。

管理用户 AK 和 SK 请根据准备工作中，通过产品控制台获取到的 AK 和 SK 进行填写。

(4) 等待 IAM 鉴权建立完成。

(5) 使用浏览器访问 https://<endpoint 地址>，勾选信任 HTTPS 证书。

(6) 修改本地机器的 Host，可以正确解析出对象存储的 Endpoint 域名地址。

(7) 使用浏览器登录云平台，访问对象页面。

如果是第一次访问，点击页面上的<开通对象存储>按钮即可，依次点击<确定>，最后重新在主菜单上点击<对象存储>，即可访问对象存储。

7.5 文件存储初始化

UCA 的文件系统业务涉及批量删除，使用了批量删除接口，因此需要对 SDS 集群进行设置，开启批量删除功能。

7.5.1 打开批量删除开关

批量删除功能默认关闭，如需使用，需要修改 mds 配置及配置文件。

需要对部署 SDS 存储的所有节点均进行配置。

1. 操作步骤

(1) 在集群监控节点执行如下命令。

```
ceph tell mds.* injectargs --mds_rm_switch=true
```

(2) 修改所有节点的配置文件/etc/ceph/ceph.conf，[mds]下增加批量删除开关配置信息。

```
vim /etc/ceph/ceph.conf
[mds]
mds_rm_switch = true
```

另外如果有新增节点，请按照此步骤来修改新增节点的配置文件。

7.5.2 （可选）修改最大可同时删除的目录数

默认可同时删除的目录数为 8192，如需修改，请按照如下步骤配置属性参数。

1. 操作步骤

(1) 在集群监控节点执行如下命令。

```
ceph tell mds.* injectargs --mds_rm_max_subdirs=NUMS
```

(2) 修改所有节点的配置文件/etc/ceph/ceph.conf，[mds]下增加可同时删除目录数的最大值配置信息。

```
vim /etc/ceph/ceph.conf
[mds]
mds_rm_max_subdirs = NUMS
```

另外如果有新增节点，请按照此步骤来修改新增节点的配置文件。

7.6 云监控初始化

7.6.1 重启云监控 A 层 prometheus 服务

重启 Pod 服务：uca-monitor-prometheus-readonly、uca-monitor-prometheus-writeonly。

1. 升级步骤

(1) 登录管区 UCA K8S VIP 地址。

(2) 执行如下命令，查看待重启的 Pod。

```
kubectl get pod | grep prometheus
```

```
[root@k8s-m1 ~]# kubectl get pod | grep monitor-prometheus
uca-dbaas-monitor-prometheus-read-df9c7                  1/1     Running            3          242d
uca-dbaas-monitor-prometheus-read-gn4w9                  1/1     Running            0          28d
uca-dbaas-monitor-prometheus-read-k4s86                  1/1     Running            0          42d
uca-dbaas-monitor-prometheus-write-db6ln                 1/1     Running            2          170d
uca-dbaas-monitor-prometheus-write-wzwls                 1/1     Running            0          28d
uca-dbaas-monitor-prometheus-write-zpjh6                 1/1     Running            3          242d
uca-monitor-prometheus-readonly-79bb989899-jzj2g         1/1     Running            0          3h8m
uca-monitor-prometheus-readonly-79bb989899-p9mt9         1/1     Running            0          3h8m
uca-monitor-prometheus-readonly-79bb989899-wxg44         1/1     Running            0          3h8m
uca-monitor-prometheus-writeonly-88dfd8d54-rdnm7         1/1     Running            0          3h7m
uca-monitor-prometheus-writeonly-88dfd8d54-stfkg         1/1     Running            0          3h7m
uca-monitor-prometheus-writeonly-88dfd8d54-vwg7p         1/1     Running            0          3h7m
```

(3) 执行如下命令，重启 Pod。

```
kubectl delete pod -l app=uca-monitor-prometheus-readonly
kubectl delete pod -l app=uca-monitor-prometheus-writeonly
```

```
[root@k8s-m1 ~]# kubectl delete pod -l app=uca-monitor-prometheus-readonly
pod "uca-monitor-prometheus-readonly-79bb989899-jzj2g" deleted
pod "uca-monitor-prometheus-readonly-79bb989899-p9mt9" deleted
pod "uca-monitor-prometheus-readonly-79bb989899-wxg44" deleted
^C
[root@k8s-m1 ~]# kubectl delete pod -l app=uca-monitor-prometheus-writeonly
pod "uca-monitor-prometheus-writeonly-88dfd8d54-rdnm7" deleted
pod "uca-monitor-prometheus-writeonly-88dfd8d54-stfkg" deleted
pod "uca-monitor-prometheus-writeonly-88dfd8d54-vwg7p" deleted
^C
```

(4) 执行如下命令，查看 Pod 的运行时间是否重新计时。重新计时说明重启成功。

```
kubectl get pod | grep prometheus
```

```
[root@k8s-m1 ~]# kubectl get pod | grep monitor-prometheus
uca-dbaas-monitor-prometheus-read-df9c7                  1/1     Running   3          242d
uca-dbaas-monitor-prometheus-read-gn4w9                  1/1     Running   0          28d
uca-dbaas-monitor-prometheus-read-k4s86                  1/1     Running   0          42d
uca-dbaas-monitor-prometheus-write-db6ln                 1/1     Running   2          170d
uca-dbaas-monitor-prometheus-write-wzwls                 1/1     Running   0          28d
uca-dbaas-monitor-prometheus-write-zpjh6                 1/1     Running   3          242d
uca-monitor-prometheus-readonly-79bb989899-5v7jg         1/1     Running   0          2m1s
uca-monitor-prometheus-readonly-79bb989899-g4wg6         1/1     Running   0          2m1s
uca-monitor-prometheus-readonly-79bb989899-qmh2f         1/1     Running   0          2m1s
uca-monitor-prometheus-writeonly-88dfd8d54-9llcf         1/1     Running   0          39s
uca-monitor-prometheus-writeonly-88dfd8d54-n8fbs         1/1     Running   0          39s
uca-monitor-prometheus-writeonly-88dfd8d54-qpf8b         1/1     Running   0          39s
```

7.6.2 （可选）云监控内置探针升级

云监控内置探针分为 Linux 和 Windows 两个版本，适用于弹性云主机和裸金属产品，其他资源类型探针内置，无需上传。

探针版本通过 OMC 平台上传到对象存储，之后客户从对象存储下载安装包到客户系统。探针管理功能依赖于对象存储服务，若环境不支持对象存储服务，则探针管理不可提供内置探针管理服务。

由于 OMC 中的探针信息是自动部署的，因此探针升级只是升级探针的版本，并不改动探针管理中的探针信息。

1. 步骤说明

升级步骤为：

(1) 文件准备与 MD5 值校验

(2) 通过 OMC 上传探针

(3) 通过 OMC 绑定探针

(4) 检测探针

2. 文件准备

升级包请从版本发布路径下获取（全量包\云服务组件包\OMC\）。将升级包放在本地，并校验安装包的 MD5 值。

此版本的升级信息如下：

表7-1 探针说明

探针名称	探针版本	升级包名称	MD5 值
wmi-monitor-agent	v1.0.0	wmi-monitor-agent-v3.3.6_0004.tar.gz	01e25f0c20155fb839aabf37327bc1c5
linux-monitor-agent	v1.0.0	linux-monitor-agent-v3.4.2_0004.tar.gz	225b0ece351bb3aad8ac827f3a41af9f

3. OMC 上传探针

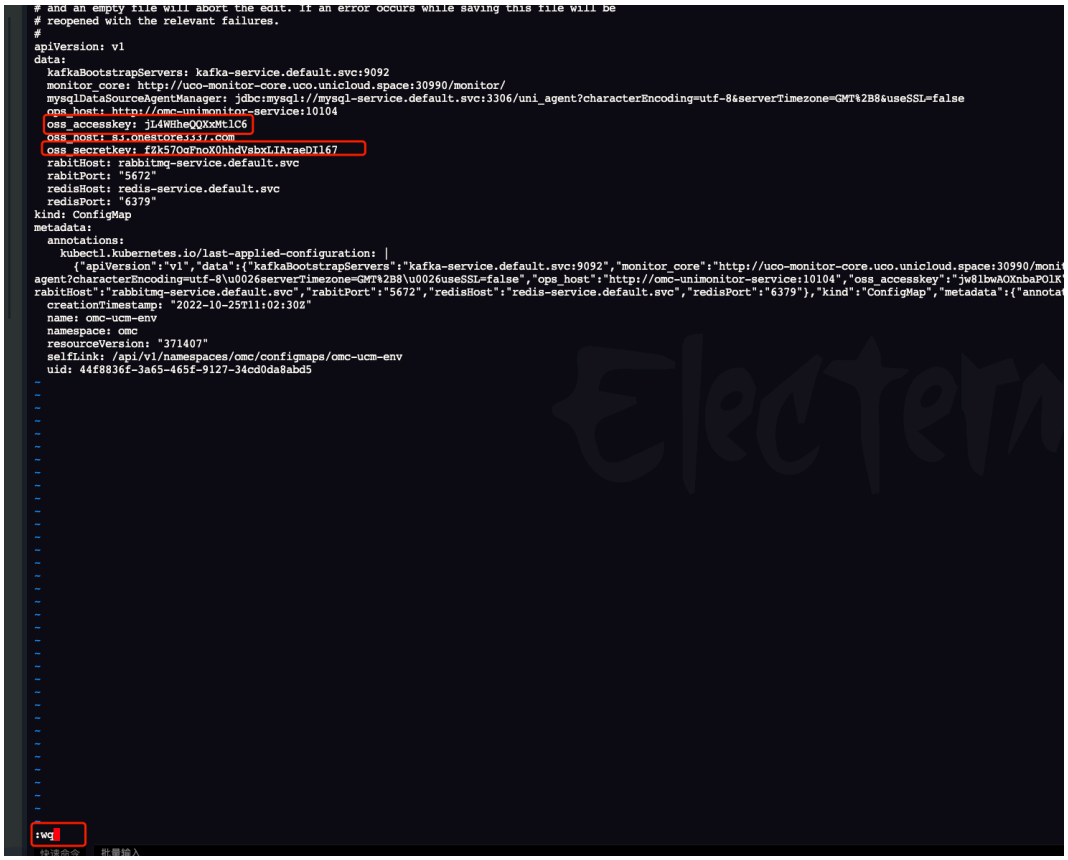
由于 OMC 上探针是分产品的，因此裸金属和弹性云主机都需上传 Linux 和 Windows 版本的探针。

(1) 在 OMC K8S 集群中，执行如下命令。

```
kubectl edit cm -n omc omc-ucm-env
```

```
^[[AEdit cancelled, no changes made.
[root@[redacted]-OMC-K8S-01 ~]# kubectl edit cm -n omc omc-ucm-env
```

(2) 将 oss_accesskey、oss_secretkey 的值替换为对象存储侧提供的 AK 和 SK，AK/SK 请从 7.4 对象存储初始化章节获取，替换后保存退出。



(3) 再执行命令 kubectl delete pod -n omc -l app=omc-agent-manager。

```
[root@[redacted]-OMC-K8S-01 ~]# kubectl delete pod -n omc -l app=omc-agent-manager
pod "omc-agent-manager-deployment-57844df7f-7gp7q" deleted
pod "omc-agent-manager-deployment-57844df7f-vsq5w" deleted
pod "omc-agent-manager-deployment-57844df7f-x225s" deleted
```

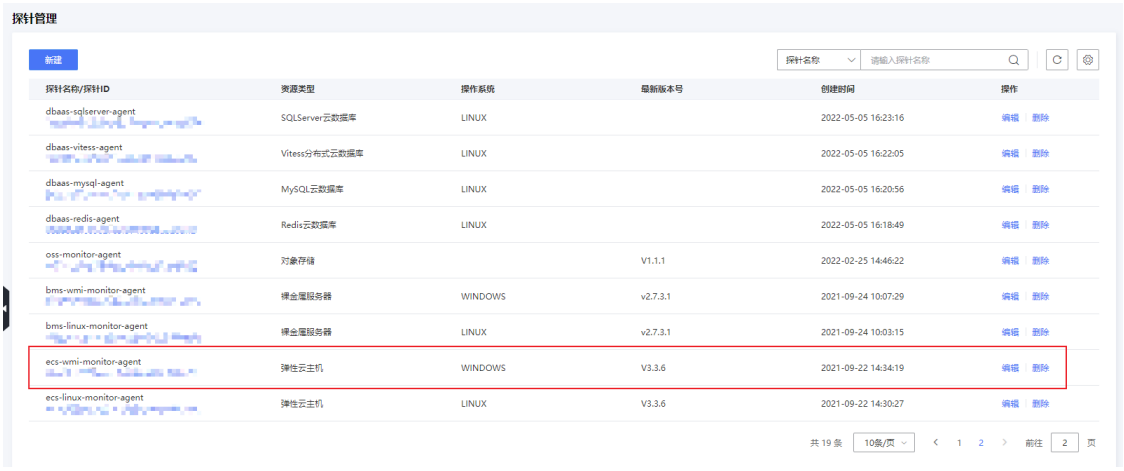
(4) 待服务重启完成后可上传探针。

(5) 执行如下命令，解压探针 tar 包到本地。

```
tar -zxvf   wmi-monitor-agent-v3.3.6_0004.tar.gz
tar -zxvf   linux-monitor-agent-v3.3.6_0004.tar.gz
```

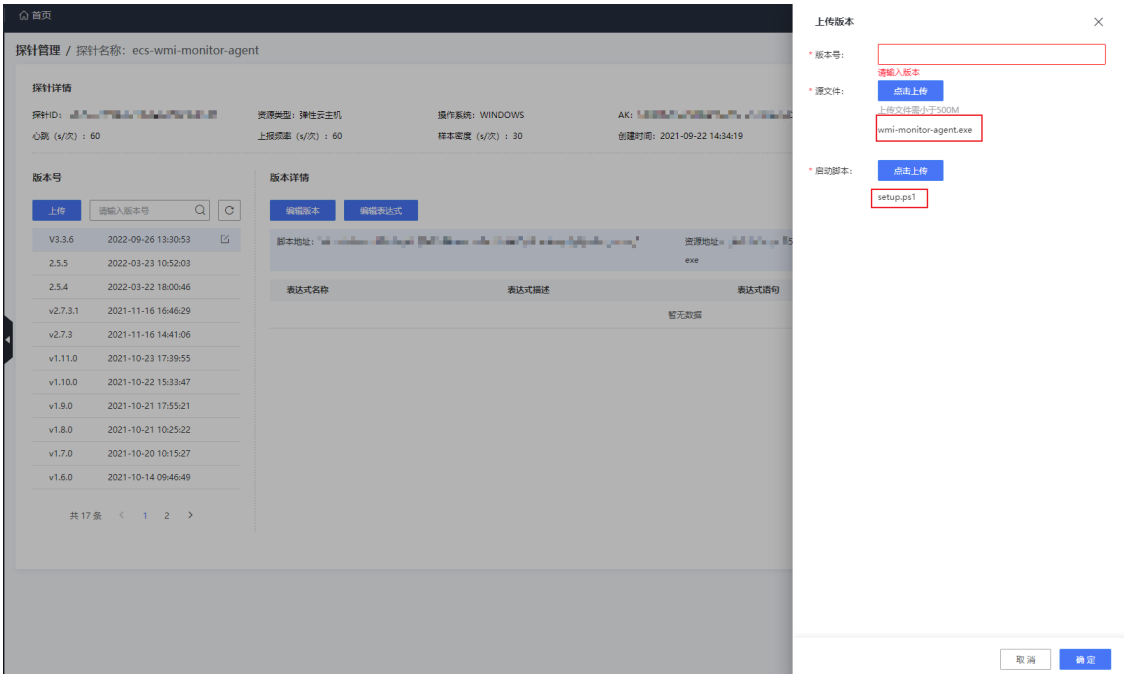
(6) 登录 OMC 平台，在云监控管理的探针管理中找到对应探针，进入详情页面。下图以操作系统为 Windows 的弹性云主机为例，需上传 wmi-monitor-agent 探针：

请注意检查 OMC K8S 集群或 omc-agent-manager 与 oss 集群的互通性，不通就会导致探针上传失败。

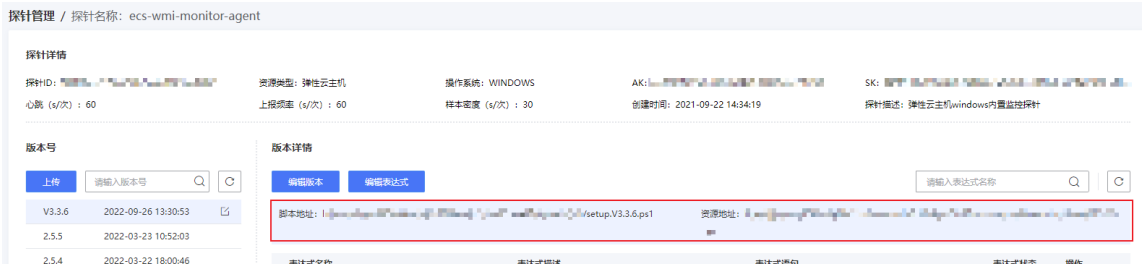


(7) 点击探针版本下的<上传>按钮。

(8) 输入版本号，上传源文件以及启动脚本，点击<确定>按钮。



(9) 上传成后，该界面会显示上传到对象存储的探针信息。

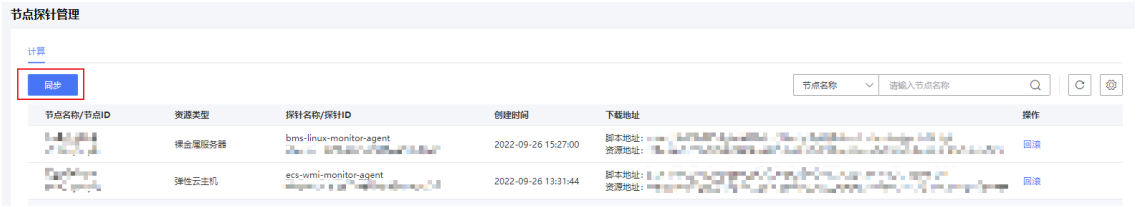


4. 节点同步探针

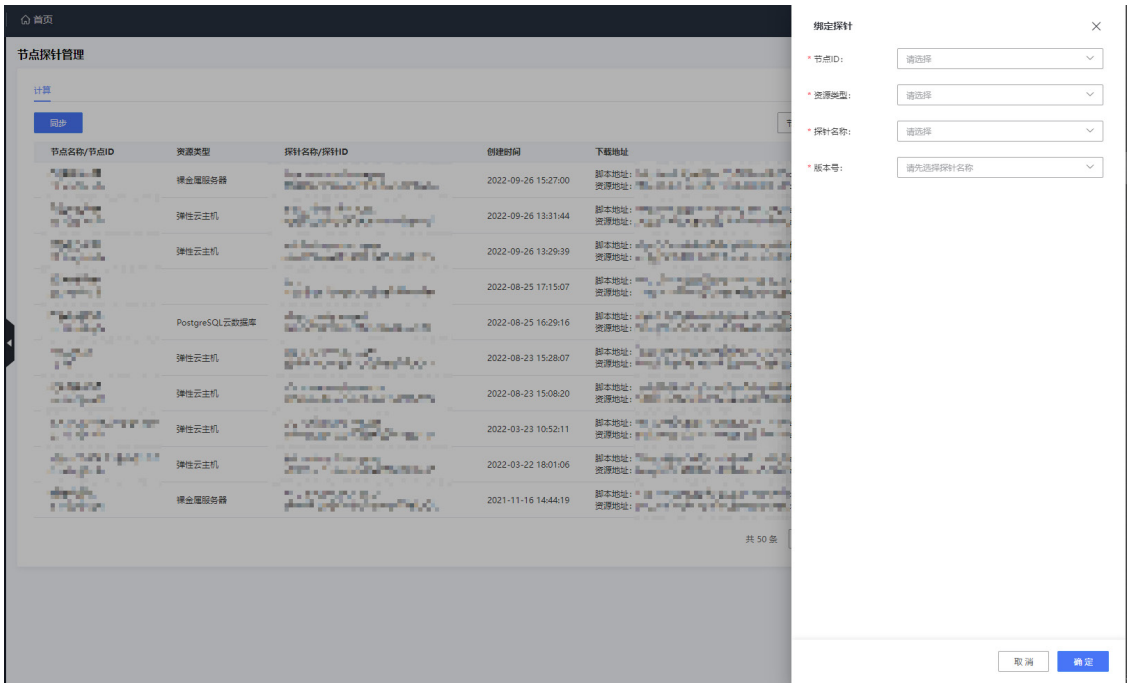
在上述流程中上传探针版本后，在节点探针管理页面将探针同步到某一节点。

根据节点实际情况，如需升级请务必将弹性云主机和裸金属对应的探针版本都进行升级。

(1) 点击<同步>按钮。



(2) 选择待同步的节点 ID、资源类型、探针名称，以及上述流程中上传的探针版本号，点击<确定>按钮。



5. 校验探针

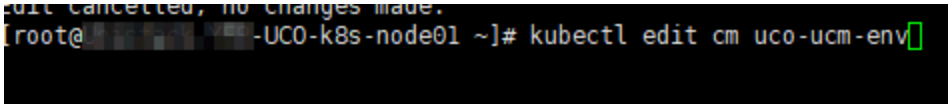
检测部署脚本中的 URL 是否为该节点探针保存在对象存储的地址。

7.6.3 （可选）云监控数据中心对象存储配置

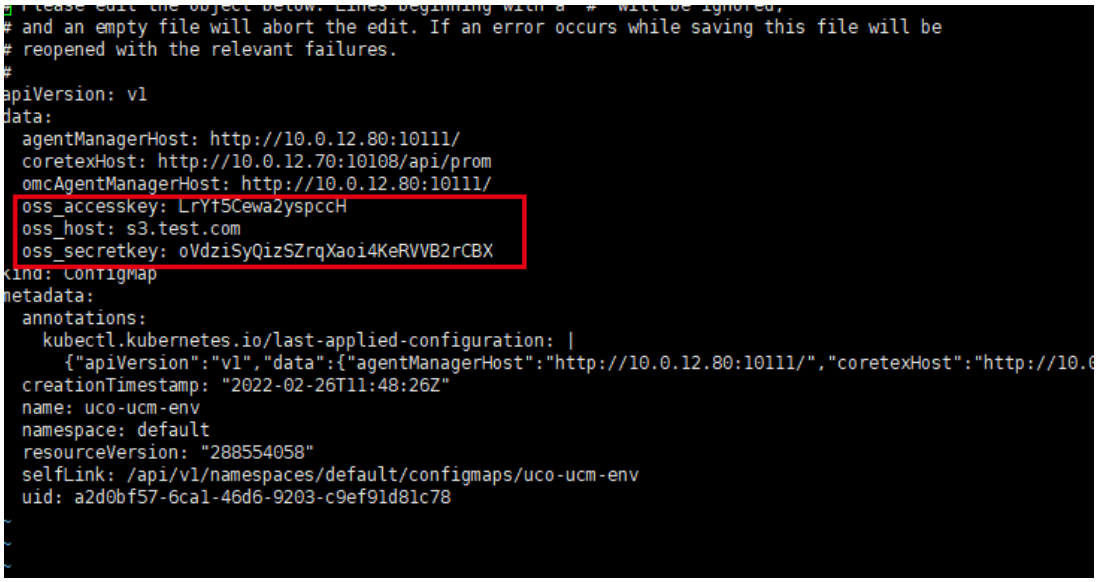
客户使用云监控/数据中心下载导出任务文件，任务文件的存储依赖于对象存储服务，若环境不支持对象存储服务，则产品控制台/云监控不可提供数据中心服务。

(1) 在 UCO 集群中执行如下命令。

```
kubectl edit cm uco-ucm-env
```



(2) 将 oss_accesskey、oss_secretkey 的值替换为对象存储侧提供的 AK、SK，AK/SK 请从 7.4 对象存储初始化章节获取，然后保存退出。



(3) 重启对应的服务。

```
kubectl rollout restart deploy uco-data-center-deployment
```

7.7 中间件初始化

7.7.1 镜像上传和注册

(1) 从版本发布交付件（路径：全量包\云服务组件包\中间件\MQS_IMAGES.tar.gz）中解压后获取消息队列 Kafka、消息队列 ActiveMQ、消息队列 RabbitMQ、消息队列 RocketMQ、数据同步 Kafka-Connector、日志服务和应用协调服务 ZooKeeper 产品的镜像文件。

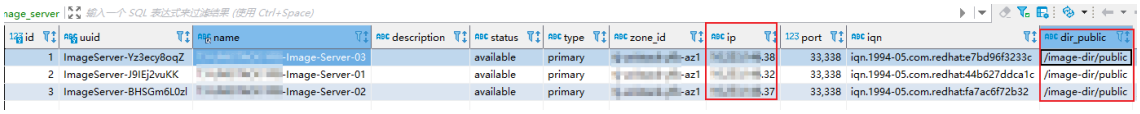
(2) 检查各镜像 MD5 值是否准确。

(3) 将镜像文件上传至镜像服务器的对应目录。镜像服务器及对应目录可根据数据库“uni_uca_image.tbl_image_server”表查询。

说明

如果存储类型需要支持 SSD 云盘，需要将上面所有镜像文件同时上传到镜像服务器 /image-dir/local 目录下，如果不需要支持云盘，该目录下则不需要上传消息队列各产品的镜像。如果存储类型需要支持 FC 云盘，需要将上述的镜像文件通过 OMC 平台上传至存储服务器，同时需确保中间件 A 层数据库 uni_bigdata.tb_config_node 的 image_uuid 和 OMC 中的镜像名称保持一致。

图7-5 查询镜像服务器及镜像存储路径



id	uuid	name	description	status	type	zone_id	ip	port	iqn	dir_public
1	ImageServer-Yz3ecy8oqZ	-Image-Server-03		available	primary	-az1	.38	33,338	iqn.1994-05.com.redhat:e7bd96f3233c	/image-dir/public
2	ImageServer-J9IEj2vuKK	-Image-Server-01		available	primary	-az1	.32	33,338	iqn.1994-05.com.redhat:44b627ddca1c	/image-dir/public
3	ImageServer-BHSGm6L0zl	-Image-Server-02		available	primary	-az1	.37	33,338	iqn.1994-05.com.redhat:fa7ac6f72b32	/image-dir/public

(4) 执行版本发布交付件中的 uca.sql 文件，执行完成后检查“uni_uca_image.tbl_image”和“uni_uca_image.tbl_image_local”表，分别有以下内容则表示注册成功。

说明

请将表 tbl_image_local 中的 image_id 和 file_name 替换成对应的镜像名称，把 image_server_id 替换成表 tbl_image_server 中的 uuid。

请将表 tbl_image 中的 image_id 和 name 替换成对应的镜像名称。

图7-6 在 uni_uca_image.tbl_image 表中检查是否注册成功

22	activemq_08_5.15_h	available	activemq_08_5.15_h	amd64	Other Linux	linux
23	rabbitmq_08_3.8_h	available	rabbitmq_08_3.8_h	amd64	Other Linux	linux
24	kafka_08_2.7_h	available	kafka_08_2.7_h	amd64	Other Linux	linux
25	kafka-connector_08_2.7_h	available	kafka-connector_08_2.7_h	amd64	Other Linux	linux
26	zookeeper_08_3.7_h	available	zookeeper_08_3.7_h	amd64	Other Linux	linux
27	rocketmq_08_4.8.0_h	available	rocketmq_08_4.8.0_h	amd64	Other Linux	linux
28	logservice_08_7.10_h	available	logservice_08_7.10_h	amd64	Other Linux	linux

图7-7 在 uni_uca_image.tbl_image_local 表中检查是否注册成功

58	activemq_08_5.15_h	available	ImageServer-bVmwgmFjso	activemq_08_5.15_h	qcow2
59	activemq_08_5.15_h	available	ImageServer-t6GM3kpR6f	activemq_08_5.15_h	qcow2
60	activemq_08_5.15_h	available	ImageServer-p3Ghy0n1dP	activemq_08_5.15_h	qcow2
61	rabbitmq_08_3.8_h	available	ImageServer-bVmwgmFjso	rabbitmq_08_3.8_h	qcow2
62	rabbitmq_08_3.8_h	available	ImageServer-t6GM3kpR6f	rabbitmq_08_3.8_h	qcow2
63	rabbitmq_08_3.8_h	available	ImageServer-p3Ghy0n1dP	rabbitmq_08_3.8_h	qcow2
64	kafka_08_2.7_h	available	ImageServer-bVmwgmFjso	kafka_08_2.7_h	qcow2
65	kafka_08_2.7_h	available	ImageServer-t6GM3kpR6f	kafka_08_2.7_h	qcow2
66	kafka_08_2.7_h	available	ImageServer-p3Ghy0n1dP	kafka_08_2.7_h	qcow2
67	kafka-connector_08_2.7_h	available	ImageServer-bVmwgmFjso	kafka-connector_08_2.7_h	qcow2
68	kafka-connector_08_2.7_h	available	ImageServer-t6GM3kpR6f	kafka-connector_08_2.7_h	qcow2
69	kafka-connector_08_2.7_h	available	ImageServer-p3Ghy0n1dP	kafka-connector_08_2.7_h	qcow2
70	zookeeper_08_3.7_h	available	ImageServer-bVmwgmFjso	zookeeper_08_3.7_h	qcow2
71	zookeeper_08_3.7_h	available	ImageServer-t6GM3kpR6f	zookeeper_08_3.7_h	qcow2
72	zookeeper_08_3.7_h	available	ImageServer-p3Ghy0n1dP	zookeeper_08_3.7_h	qcow2
73	rocketmq_08_4.8.0_h	available	ImageServer-bVmwgmFjso	rocketmq_08_4.8.0_h	qcow2
74	rocketmq_08_4.8.0_h	available	ImageServer-t6GM3kpR6f	rocketmq_08_4.8.0_h	qcow2
75	rocketmq_08_4.8.0_h	available	ImageServer-p3Ghy0n1dP	rocketmq_08_4.8.0_h	qcow2
76	logservice_08_7.10_h	available	ImageServer-bVmwgmFjso	logservice_08_7.10_h	qcow2
77	logservice_08_7.10_h	available	ImageServer-t6GM3kpR6f	logservice_08_7.10_h	qcow2
78	logservice_08_7.10_h	available	ImageServer-p3Ghy0n1dP	logservice_08_7.10_h	qcow2

(5) 完成以上所有配置，即可在用户产品控制台进入对应的产品管理页面执行实例创建操作。

7.7.2 设置 Kafka 参数配置功能

在 O 层数据库执行如下命令：

```
UPDATE  `uco_bigdata`.`db_available_features` SET `feature` =
'kafka_base,kafka_user,kafka_role,kafka_consumer_group,kafka_params,kafka_whitelist,kafk
a_nodeinfo,kafka_topic,kafka_message_query' WHERE `engine`='kafka' and
`feature_type`='router';
```

7.7.3 检查 A 层数据库云监控配置

(1) 查询数据库 uni_bigdata.tb_config 表中的云监控配置项。

图7-8 云监控配置项

事件上报服务地址	MONITOR_UCM_HOST	http://uca-monitor-reception-service:40702	
云监控服务的端口	AGENT_UCM_HOST_PORT	40702	
云监控服务地址	AGENT_UCM_HOST	100.100.63.11	
创建实例默认出口放行的ip	DEFAULT_DMZ_IPS		若访问云监控服务地址时需要添加安全组策略，请在此配置。

(2) 检查配置项是否正确。

配置项说明如下：

参数名称	含义	常见值或示例
云监控服务地址	云监控服务地址 域名解析的服务IP地址是DMZ区的K8S的VIP 如果租区访问不到该地址时，需要配置公网	-
云监控服务的端口	云监控服务的端口，默认40702	40702
创建实例默认出口放行的ip	创建实例默认出口放行的ip DMZ区的网段信息，参考DMZ区K8S的VIP网段	100.67.100.1/24

参数名称	含义	常见值或示例
	若访问云监控服务地址时需要添加安全组策略，请在此配置	
事件上报服务地址	事件上报服务地址 域名解析的服务IP地址是DMZ区的K8S的VIP http://{云监控服务的地址，如果租区访问不到该地址时，需要配置公网}:40702	-

7.7.4 SSD 云盘支持（选配）

1. 配置须知

如果存储类型需要支持 SSD 云盘，该章节的操作需要在运营平台进行配置，同时确保消息队列各产品的镜像已上传到镜像仓库指定目录（可参考 7.8.1 镜像上传和注册）。如果不需要支持 SSD 云盘，该章节不需要配置。

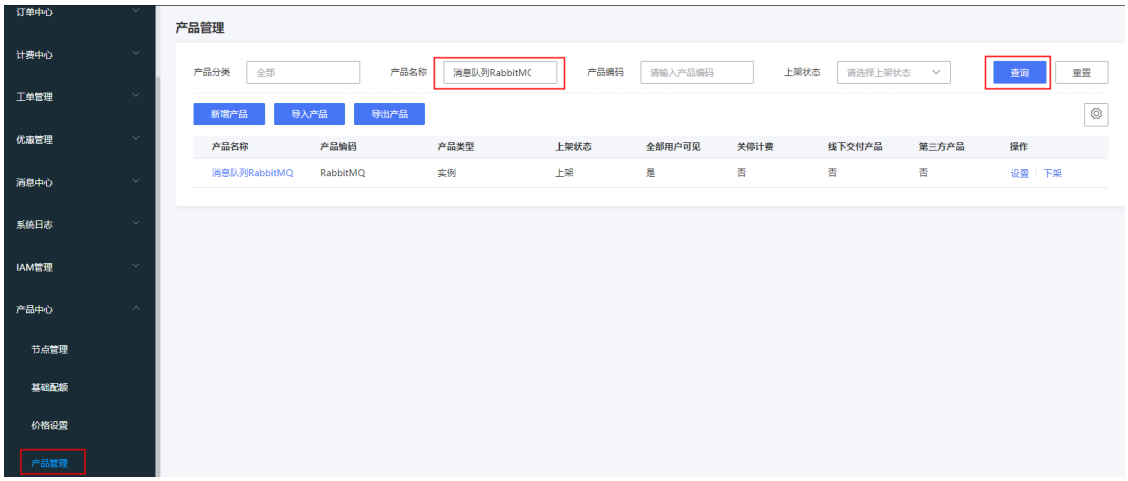
配置前需和负责编排的相关人员确认当前环境支持的存储类型(如 3Par、SDS)，避免出现配置后环境不支持问题。

以下配置以消息队列 RabbitMQ 为例。

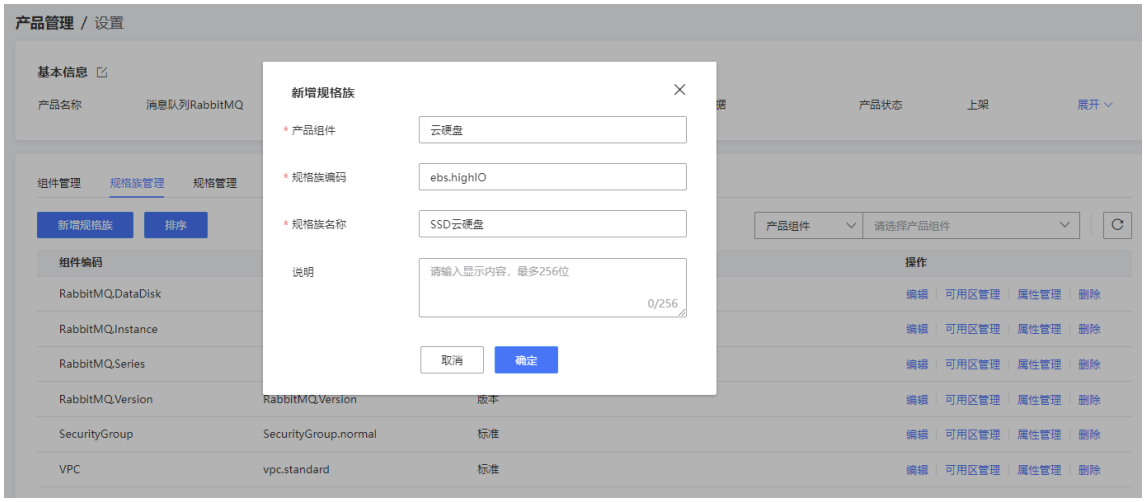
2. 运营平台配置产品

(1) 登录运营平台，在导航栏选择[产品中心/产品管理]，进入产品详情页面。

(2) 在产品管理页面查询对应产品，点击产品名称链接进入设置页面。



(3) 选择[规格族管理]页签，点击<新建规格族>按钮，新建规格族。编码和规格族名称可参考下图。



(4) 在规格族管理页面，点击操作列的<属性管理>按钮，新增属性。

注意

请严格按照下图为规格族配置属性，尤其是属性编码，否则可能出现编排失败场景。

(5) 在规格族管理页面，单击操作列的<可用区管理>，为规格族设置可用区，请根据现场环境确定，配置后开启可用区。

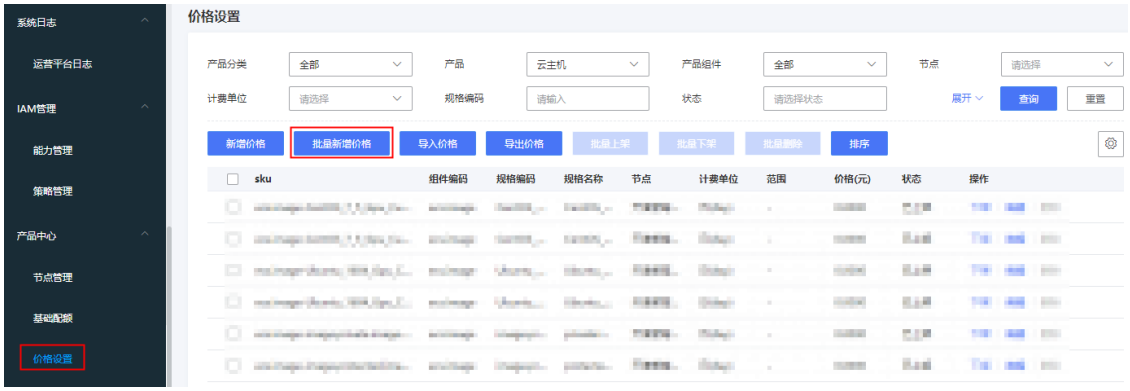
(6) 在产品设置页面，选择[规格管理]页签，点击<新建规格>按钮，在规格族中创建规格，并配置相关属性。

根据实际项目环境，可选择配置以下规格：

规格编码	规格族名称	规格名称	存储类型
ebs.hybrid.hdd	高性能HDD云硬盘	高性能HDD云硬盘	根据现场环境确定，3par\SDS
ebs.highIO.ssd	SSD云硬盘	SSD云硬盘	根据现场环境确定，3par\SDS

容量、步长请根据实际需求确定。需注意，最小容量、最大容量均需为步长的倍数，否则创建页面会报错 productConfigError。

(7) 在导航栏选择[产品中心/价格设置]，进入价格设置页面。

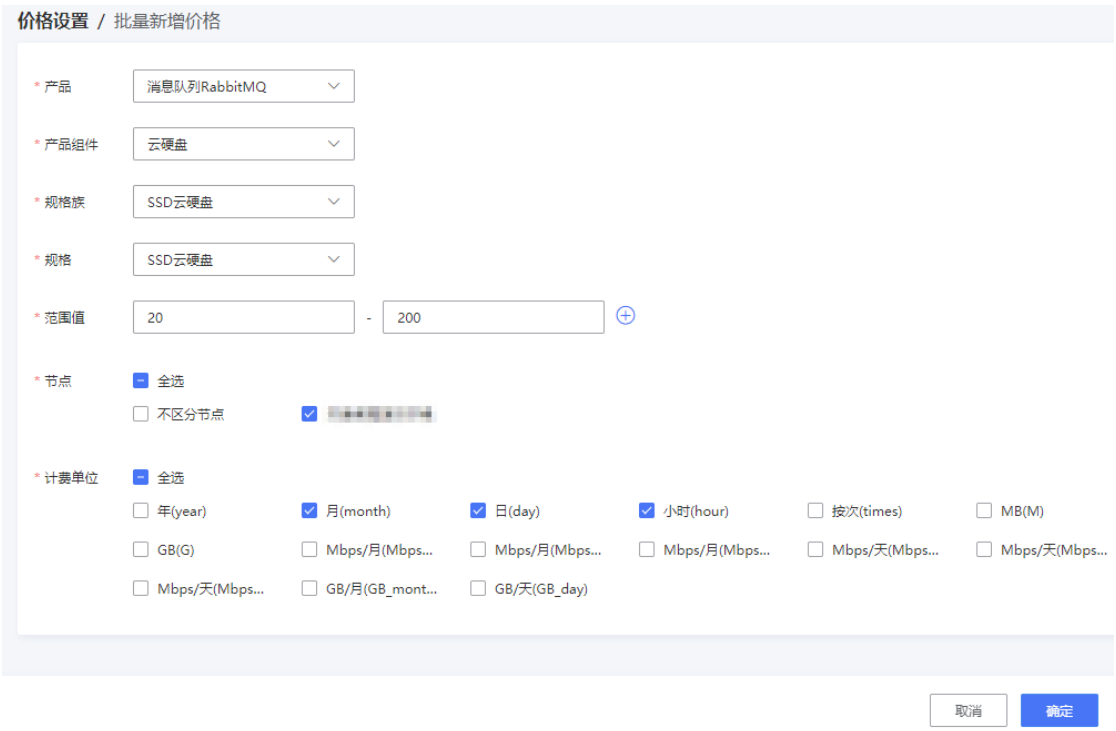


(8) 点击<批量新增价格>按钮，批量新增价格。

需注意，配置的计费单位和创建页面上的计费方式有对应关系，比如若不配置计费单位为小时的售卖项，则前段页面选择按小时付费时，存储类型中是没有云硬盘选项的。

图7-9 计费单位和计费方式的对应关系

计费单位	对应的计费方式
日	按日月结
月	包年包月
小时	按小时付费



(9) 为售卖项设置价格及单位。

X 表示绝对价，AX 表示单价。例如：

公式	价格	购买容量	购买价格
X	1元	50G	1元
AX	1元	50G	50元

(10) 设置完成后，将价格上架。

3. 产品控制台进行检查

此时刷新组件的创建页面，存储类型处即可看到云硬盘选项。

7.7.5 FC 云盘支持（选配）

1. 配置须知

如果存储类型需要支持 FC 云盘，该章节的操作需要在运营平台进行配置。如果不需要支持，该章节不需要配置。

配置前需和负责编排的相关人员确认当前环境支持的存储类型(primera)，避免出现配置后环境不支持问题。

以下配置以消息队列 Kafka 为例。

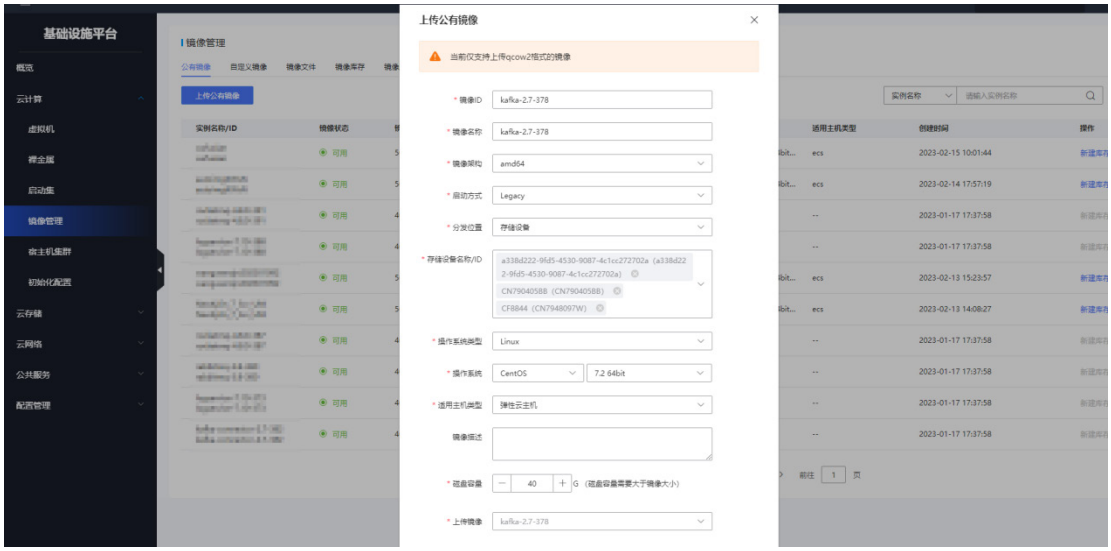
2. 运维控制台上传镜像

(1) 通过 OMC 上传中间件镜像。

先将中间件的三个镜像通过 FTP 上传至指定的镜像仓库，镜像 FTP 地址和路径获取方式可登录 OMC 平台查询，可参考下图。

(2) 登录 OMC 平台，点击页面左上方的  ，选择[基础设施平台/云计算/镜像管理]。

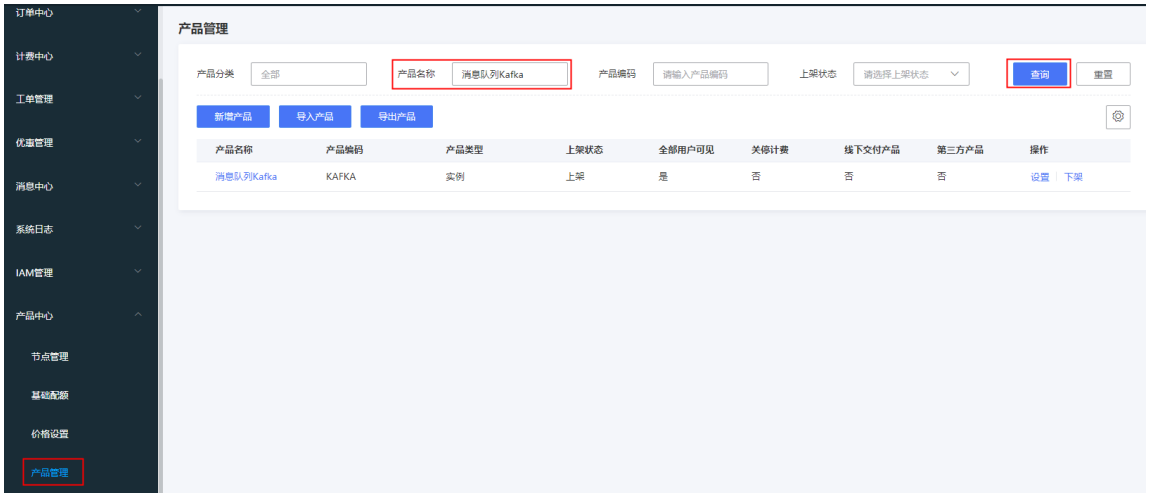
(3) 点击<上传公有镜像>按钮，上传中间件的镜像，可参考下图。



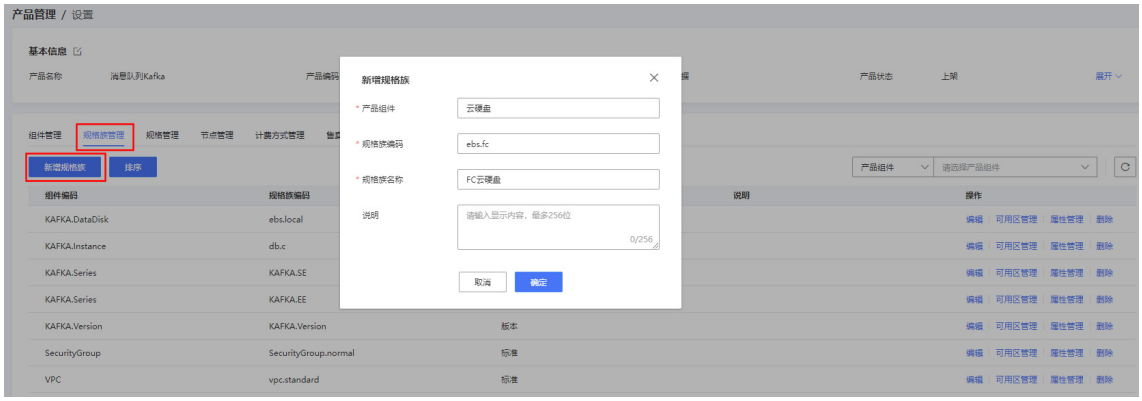
3. 运营平台配置产品

(1) 登录运营平台，在导航栏选择[产品中心/产品管理]，进入产品详情页面。

(2) 在产品管理页面查询对应产品，点击产品名称链接进入设置页面。



(3) 选择[规格族管理]页签，点击<新建规格族>按钮，新建规格族。编码和规格族名称可参考下图。



(4) 在规格族管理页面，点击操作列的<属性管理>按钮，新增属性。

新增属性如下。

注意

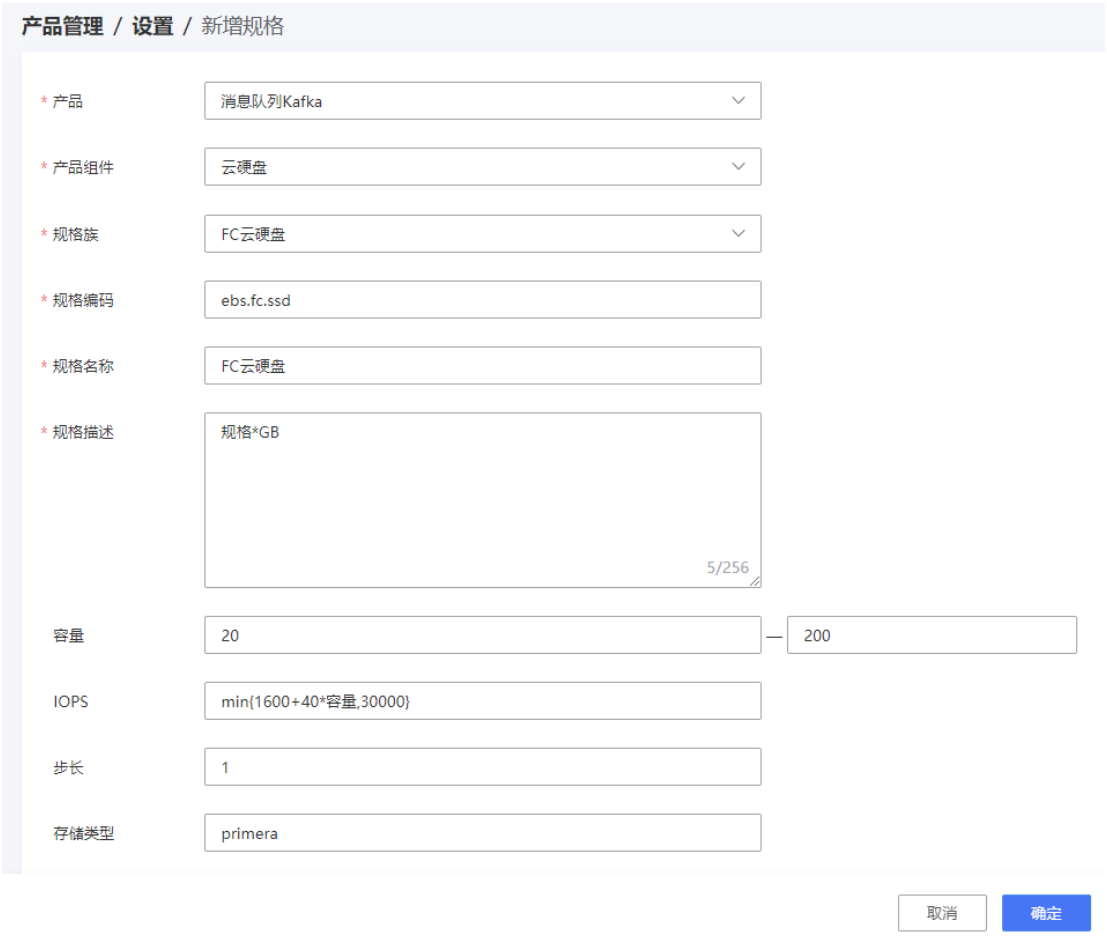
请严格按照下图为规格族配置属性，尤其是属性编码，否则可能出现编排失败场景。

(5) 在规格族管理页面，单击操作列的<可用区管理>，为规格族设置可用区，请根据现场环境确定，配置后开启可用区。

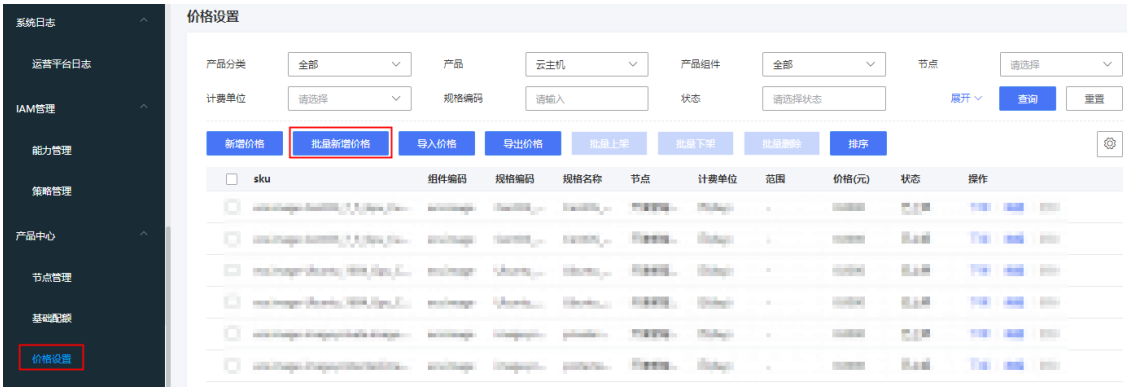
(6) 在产品设置页面，选择[规格管理]页签，点击<新建规格>按钮，在规格族中创建规格，并配置相关属性。

规格编码	规格名称	存储类型
ebs.fc.ssd	FC云硬盘	primera

容量、步长请根据实际需求确定。需注意，最小容量、最大容量均需为步长的倍数，否则创建页面会报错 productConfigError。



(7) 在导航栏选择[产品中心/价格设置]，进入价格设置页面。



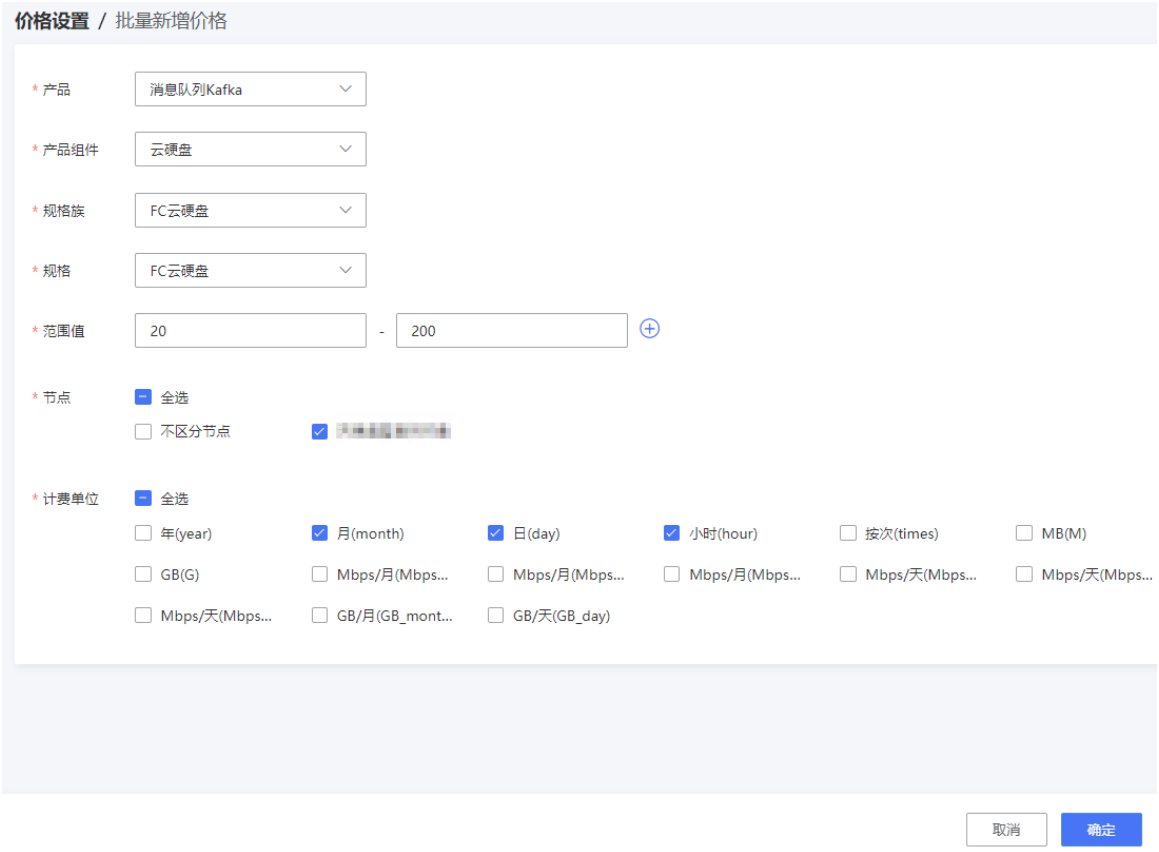
(8) 点击<批量新增价格>按钮，批量新增价格。

需注意，配置的计费单位和创建页面上的计费方式有对应关系，比如若不配置计费单位为小时的售卖项，则前段页面选择按小时付费时，存储类型中是没有云硬盘选项的。

图7-10 计费单位和计费方式的对应关系

计费单位	对应的计费方式

日	按日月结
月	包年包月
小时	按小时付费



(9) 为售卖项设置价格及单位。

X 表示绝对价，AX 表示单价。例如：

公式	价格	购买容量	购买价格
X	1元	50G	1元
AX	1元	50G	50元

(10) 设置完成后，将价格上架。

4. 产品控制台进行检查

登录产品控制台，在导航栏选择[大数据/消息队列 Kakfa]，点击<创建>按钮。

此时刷新组件的创建页面，存储类型处即可看到 FC 云硬盘选项。

7.7.6 采集器镜像上传（选配）

1. 配置限制

该步骤仅适用于日志服务，其他产品安装部署时跳过此章节。

请从版本发布路径下获取压缩包（路径：全量包\云服务组件包\中间件\MQS_IMAGES.tar.gz），解压后获取容器日志采集器镜像。

2. 配置步骤

(1) 确认 CCR 的镜像仓库地址。

确认方式可联系 CCR 研发人员。

(2) 访问上面的 harbor 地址，并成功登陆后，新建项目：logservice，并设置访问级别为公开。

(3) 将 log-collect.tar 和 logserviceImagePush.sh 上传到 ccr 部署的 harbor 所在的主机上的任意目录。

(4) 执行如下脚本，上传镜像。

```
chmod +x logserviceImagePush.sh
./logserviceImagePush.sh {仓库地址}
```

需要注意的是，脚本执行时的输入参数要去掉“http://”。

(5) 检查采集器镜像是否上传成功。

脚本打印出以下内容，标识上传镜像成功。

```
3dc45127907f: Layer already exists
10f243b7644c: Layer already exists
2753bbe4d833: Layer already exists
2e53ff372aca: Layer already exists
3547f858003f: Layer already exists
fce3586aa288: Layer already exists
89ae5c4ee501: Layer already exists
1.0.1: digest: sha256:2db4be73b8fc0195c217cd515860dcb98cbb902ab559bd49ace873ca9c5ec332 size: 1795
docker push success!
[root@cd-dev-dmz-03 wps]#
```

或可登陆到 harbor 仓库，查看 logservice 项目下是否存在 log-collect 镜像。

7.7.7 修改 A 层配置（选配）

1. 配置须知

该步骤仅适用于日志服务部署的环境，如果当前局点需要部署日志服务，该步骤需要操作。

2. 配置步骤

(1) 登录 A 层 K8S 控制节点。

(2) 备份 configmap。

```
kubectl get cm uca-dbaas-bigdata-configmap -o yaml >
/home/uca-dbaas-bigdata-configmap.yaml
```

(3) 修改 configmap。

在 configmap 中，新增如下值对。

Key	Value	含义
TAAG_VIP	例如：10.51.80.120	租管互通vip，联系环境运维人员获取
LOG_COLLECT_REPOSITORY	例如：{仓库地址}/logservice/log-collect:1.0.0	采集器仓库地址，获取方式参考 7.8.5 采集器镜像上传（选配）

操作步骤如下：

执行 kubectl edit cm uca-dbaas-bigdata-configmap 命令，新增上面两组值，保存。

```
COMPUTE_HOST: http://uca-compute-core-service:40201
DELIVERY_HOST: http://uca-center-service:40298
ENV_MODE: production
LOG_COLLECT_REPOSITORY: 100.100.63.138:30002/logservice/log-collect:1.0.0
MQ_EXCHANGE: oc-database
MQ_HOST: rabbitmq-service:5672
MQ_ROUTINGKEY: notifications.*
MYSQL_DB_NAME: uni_bigdata
MYSQL_HOST: uca-mysql
MYSQL_PORT: "3306"
NETWORK_HOST: http://uca-network-core-service:40416
NETWORK_HOST_20: http://uca-center-service:40298/core
NGINX_HOST: http://uca-dbaas-nginx-service:40621/default/
OSS_ACCESS_KEY_ID: admin
OSS_ACL: private
OSS_BASE: oss://moove-uni-bigdata
OSS_ENDPOINT: http://s3.cddev.com
OSS_ENV_AUTH: "false"
OSS_HOST: s3.cddev.com
OSS_IP: 10.51.80.115
OSS_PROVIDER: Ceph
OSS_SECRET_ACCESS_KEY: Passw0rd@_
OSS_TYPE: s3
SLB_HOST: http://uca-network-slb-service:40456
TAAG_VIP: 10.51.80.120
```

(4) 重启 UCA 层 Pod。

```
kubectl get pod |grep uca-dbaas-bigdata | awk '{print $1}' | xargs -I {} kubectl delete
pod {}
```

7.8 公共服务区PaaS底座部署

7.8.1 准备集群虚拟机

(1) 将 PaaS-Plat-template.ori 复制成 3 份后，分别作为磁盘文件创建 3 台虚拟机。请从版本发布路径下获取：全量包\云服务组件包\容器\PaaS-Plat-template.ori

(2) 分别登录 3 台虚拟机。虚拟机后台默认账号为 root，密码为 Passw0rd@_。每台虚拟机需要设置自己的主机名，且主机名中的字母需为小写，例如 paas-plat-{1,2,3}。

(3) 配置虚拟机资源。每台虚拟机资源要求如下。

CPU 核数	内存	系统盘	Etcd 盘	存储盘
8	16G	500G	60G	200G

(4) 在 3 台虚拟机上分别配置公共服务区规划的业务网卡。例如：

```
root@node:~# cat /etc/netplan/00-installer-config.yaml
# This is the network config written by 'subiquity'
network:
  ethernets:
    ens3:
      addresses: [10.125.30.255/22]
      gateway4: 10.125.28.1
    ens12:
      addresses: [192.168.1.10/24]
  version: 2
```

(5) 执行如下命令，使得网卡配置生效。

```
netplan apply
```

7.8.2 登录部署界面

(1) 启动浏览器，在地址栏中输入 https://<某一节点的管理 IP>:9091，打开“GoMatrix”安装部署页面，如下图所示。

(2) 输入缺省的用户名和密码：admin/Passw0rd@_，单击“登录”按钮进入 GoMatrix 首页，即部署页面。

7.8.3 部署节点

(1) 单击<部署>按钮，进入集群的基础配置页面，如图 7-21 所示。配置“集群网虚 IP”、“管理网虚 IP”和 NTP 服务地址，且可在当前页的高级配置（如图 7-22）中修改配置“pod 网段”和“service 网段”。

- 集群网虚 IP：平台业务网络的虚服务地址，此处填写业务网的虚 IP。
- 管理网虚 IP：平台管理网络的虚服务地址，此处填写业务网的虚 IP。
- NTP 服务地址：缺省为主节点的管理 IP 地址，不需要填写。
- 系统默认配置了 10.240.0.0/12（缺省容器网段）、10.100.0.0/16（缺省 K8S 服务网段）。无需变动。
- 平台页面端口：允许用户在部署时修改业务平台页面的登录端口，以下拉选择的形式进行，不支持自定义。

图7-11 基础配置页面

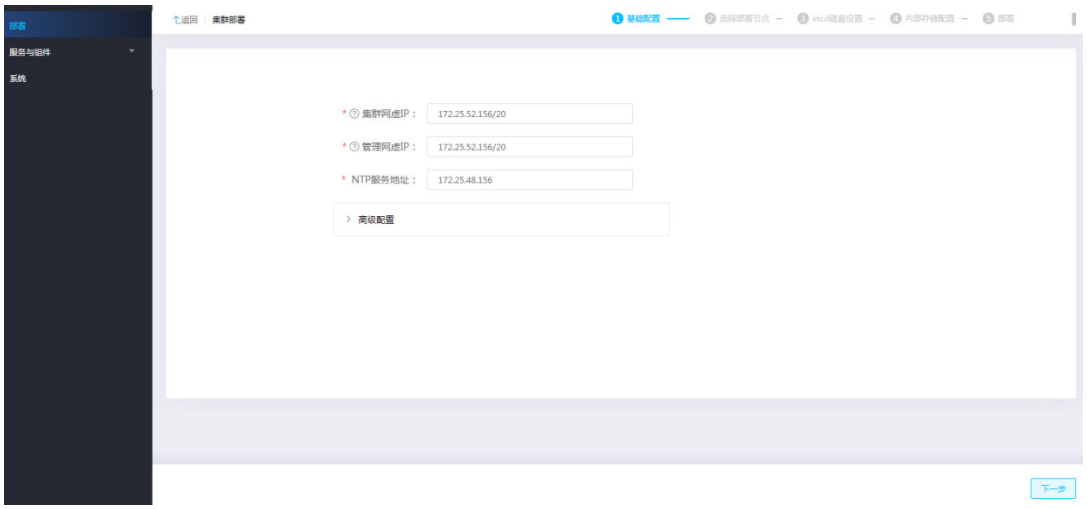
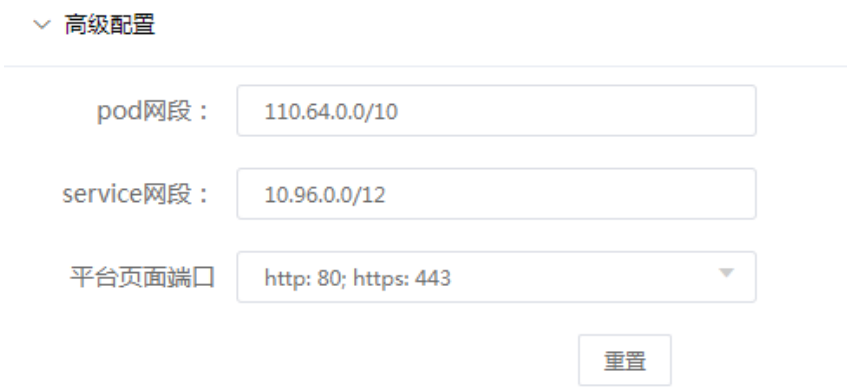
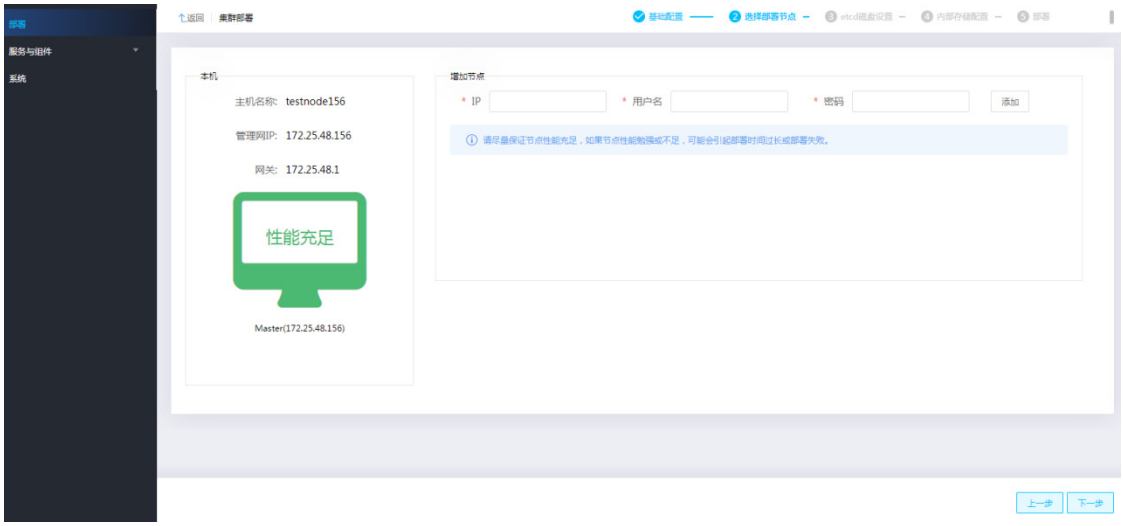


图7-12 高级配置



(2) 配置完成后，单击<下一步>按钮。

(3) 在[选择部署节点]区域中，选择主节点的集群 IP，然后填写其他两个节点的管理网 IP、集群网 IP、用户名与密码，单击“添加”按钮，将节点加入集群。添加节点后的数量为 3。



性能判断：系统会自动判断安装环境的性能，有性能充足、性能普通、性能勉强、性能不足四种情况，每种情况可能会影响安装的结果。例如：性能充足和性能普通时，可以正常安装部署；性能勉强或性能不足时，可能导致部署时间延长或者部署失败，此时不建议继续部署，需要确认服务器硬件配置是否满足要求。

⚠ 注意

必须保证集群节点间的管理网络 IP 可达且在同一网段内。

---

(4) etcd 磁盘设置。

etcd 是平台集群核心组件的底层分布式数据库，保存和实时更新了平台集群的诸多状态信息。

⚠ 注意

平台每个控制节点都需要准备一块单独的硬盘供 etcd 使用，推荐使用 SSD，切勿使用与其他设备在物理层面共享的磁盘设备或将一块磁盘分区给多个 etcd 使用，因为 IO 被挤占会导致 ETCD 节点之间数据不同步，容易引发集群故障。

安装部署开始前，请用户正确设置服务器的磁盘 RAID 配置，安装时必须使用完成 RAID 配置后的第一块盘作为系统盘。通常为系统盘配置成 RAID1，两块数据盘分别配置 RAID0。

etcd 硬盘容量需不小于 60G。

---

a. 选择主机。

b. 选择磁盘。

生产环境 etcd 必须使用独立磁盘；非生产环境建议使用独立磁盘，如果使用系统盘则需要保障系统盘的高性能。

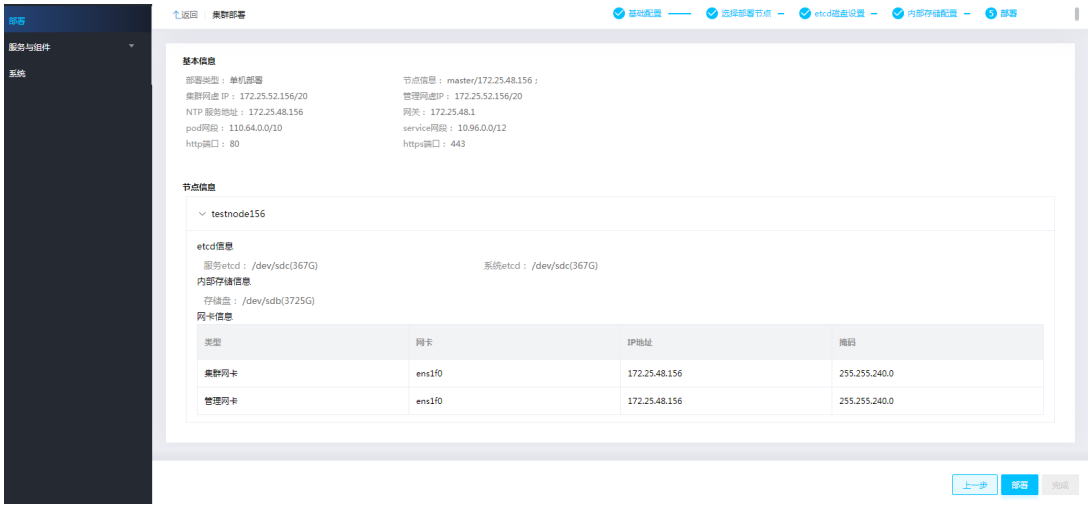
c. 分别对三台节点勾选并选择磁盘后，单击“下一步”。

如果不选择磁盘，etcd 将使用系统盘。

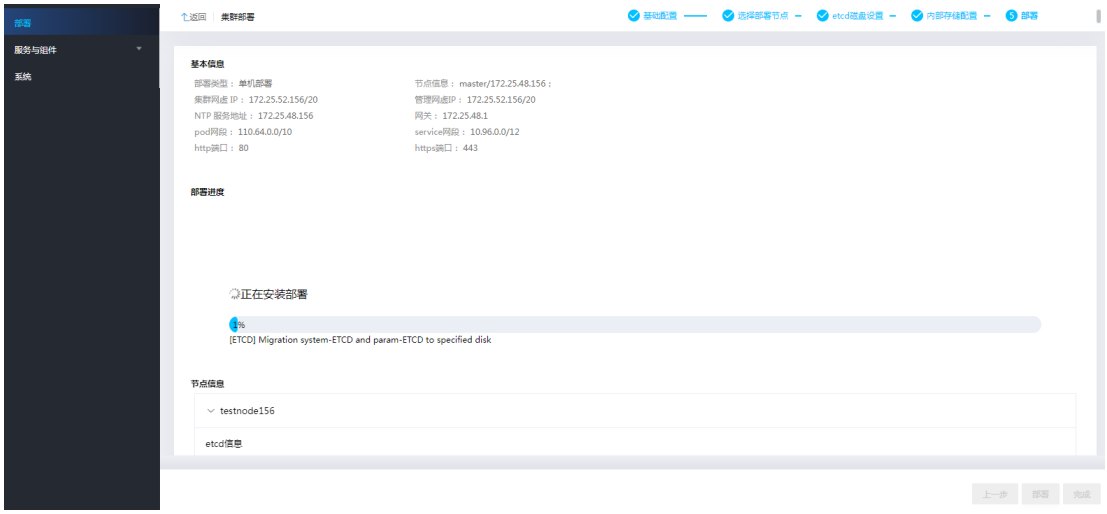
请注意，如果在操作过程中由于操作失误，选择了错误的磁盘，需要重新配置。

(5) 内部存储所选盘将会作为集群存储空间，提供给集群上的容器使用。请注意，所选盘的原有数据会被清除。

(6) 进入配置信息确认页面，如下图所示。分别核对基础信息、节点配置信息和 etcd 配置信息，确认无误后单击“部署”按钮。如果有配错的地方可返回上一步重新配置。



(7) 开始 PaaS 底座集群，如下图所示。



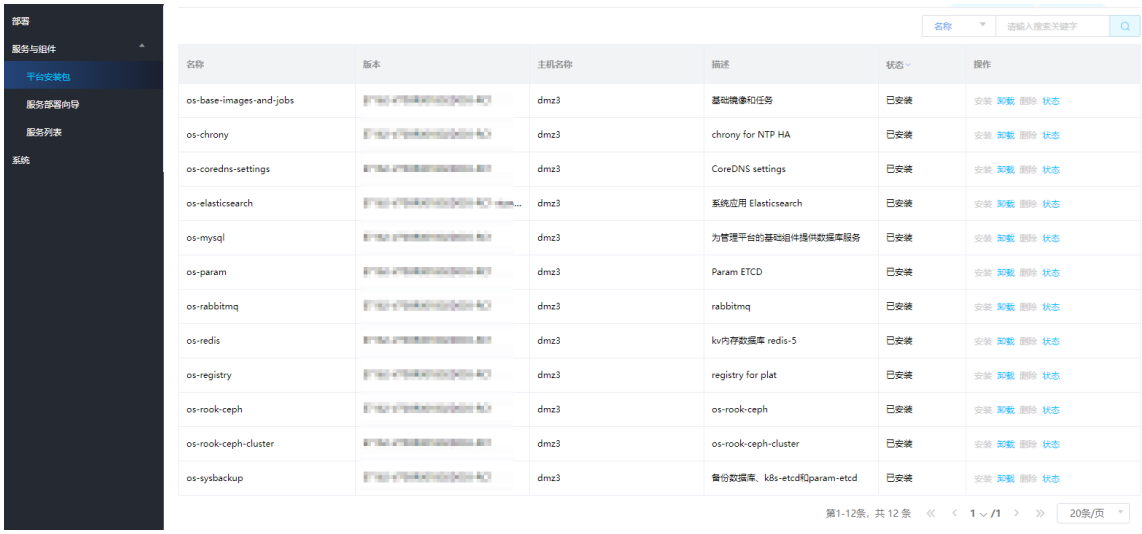
注意

点击部署后，部署完成耗时正常为 1 个小时左右，但在某些性能较差的环境下，安装部署耗时会相对长一些，部署进度条会停留在 66%较长时间，此时请耐心等待。如果 Gomatrix 页面超时退出登录，可重新打开浏览器并登录 Gomatrix，即可看到部署进度和结果。

(8) 等待部署完成。可在节点信息页面查看部署详细信息。

图7-13 查看部署信息

图7-14 检查组件安装情况



(9) 查看组件执行情况：进入部署页面，单击右上角“预装组件状态”按钮，查看各组件是否正常。若存在执行失败的脚本，请联系技术支持。

(10) 若所有组件部署成功且不存在执行失败的脚本，则表示安装部署成功。

7.9 公共服务区CCR Harbor初始化

7.9.1 部署说明

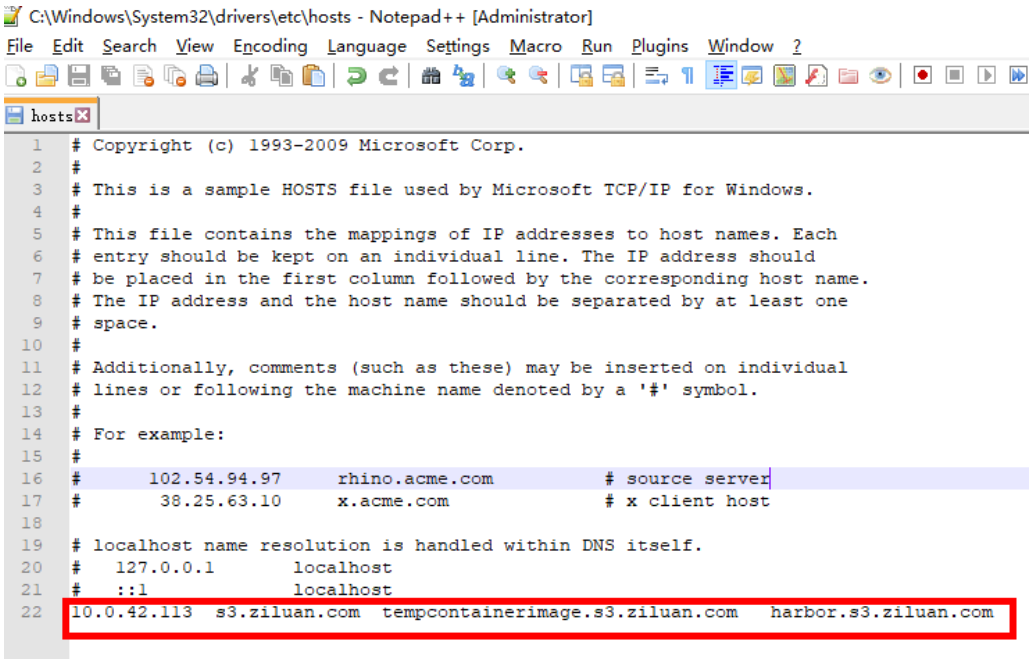
在私有云环境中：

- Harbor 使用公共服务区 PaaS 底座上的 mysql/redis。
- Harbor 使用 SDS 或者 yig 对象存储。

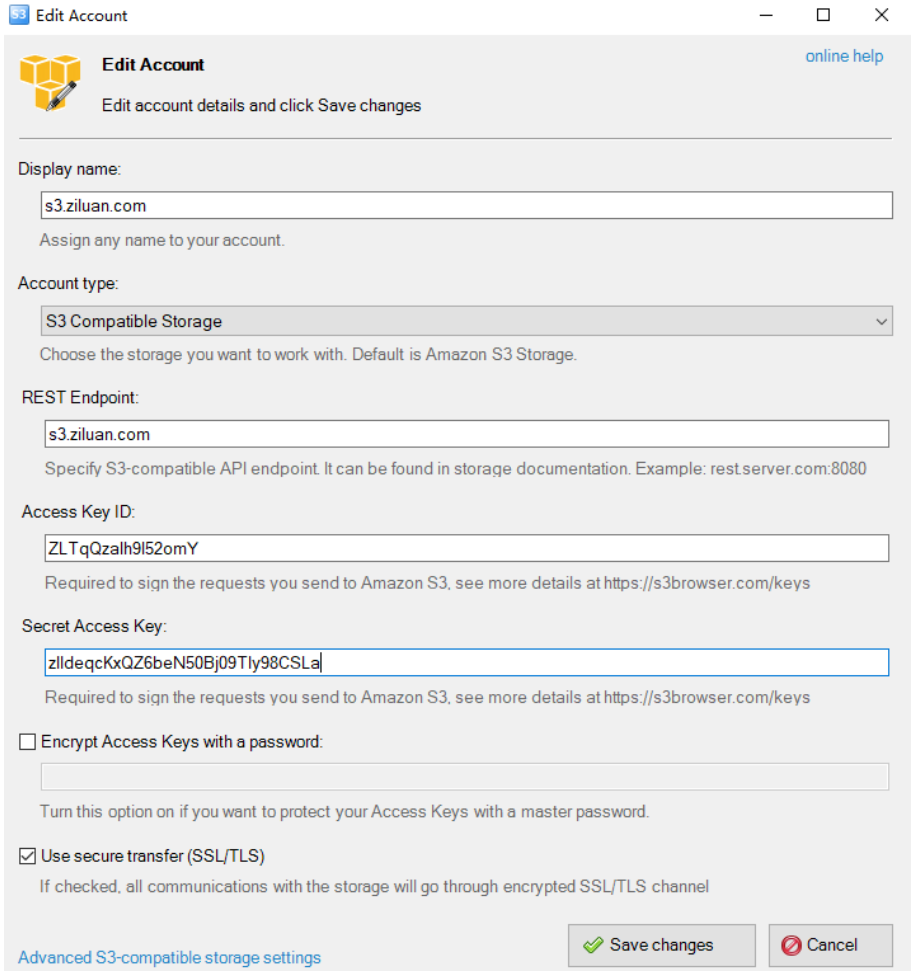
部署文件请从版本发布路径下获取：全量包\云服务组件包\容器\CCR.zip。下载到本地后解压缩。

7.9.2 创建对象存储桶

(1) 配置本地 Windows 主机 hosts 文件，增加对象存储的域名解析，如下图示例：

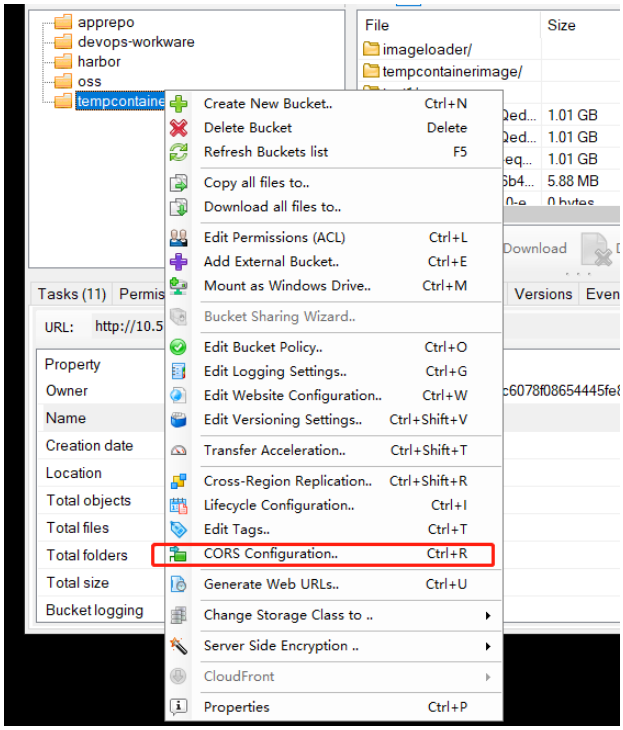


(2) 打开对象存储工具（例如 S3Browser），登录对应的对象存储，如下图示例：

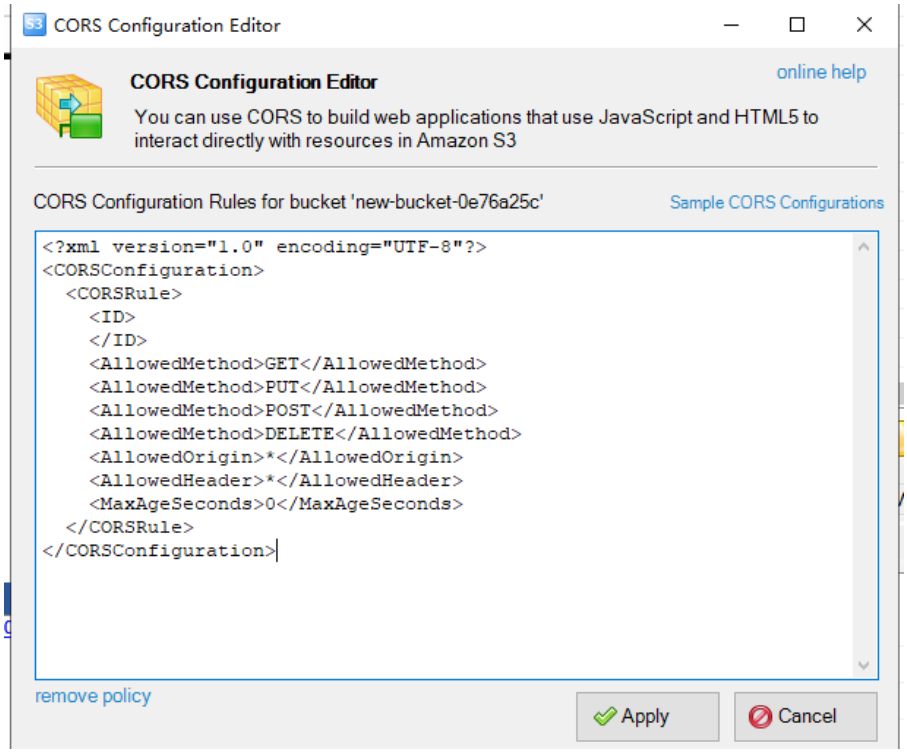


(3) 新建两个桶：harbor 和 tempcontainerimage

(4) 为 tempcontainerimage 桶配置跨域



(5) 配置跨域信息



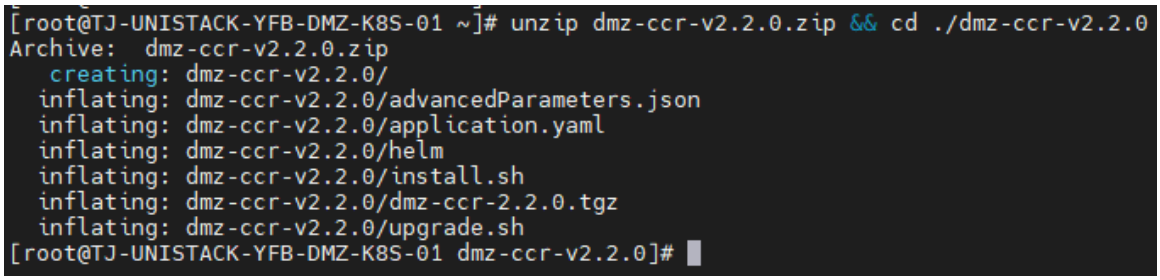
```
<?xml version="1.0" encoding="UTF-8"?>
<CORSConfiguration>
  <CORSRule>
    <ID>
    </ID>
    <AllowedMethod>GET</AllowedMethod>
    <AllowedMethod>PUT</AllowedMethod>
    <AllowedMethod>POST</AllowedMethod>
    <AllowedMethod>DELETE</AllowedMethod>
    <AllowedOrigin>*</AllowedOrigin>
    <AllowedHeader>*</AllowedHeader>
    <MaxAgeSeconds>0</MaxAgeSeconds>
  </CORSRule>
</CORSConfiguration>
```

7.9.3 安装 Harbor 服务

将归档版本包 dmz-ccr-v2.2.0.zip（解压 CCR.zip 获得）上传到公服区 K8S 集群任一个节点，然后执行如下操作：

(1) 解压 Harbor 服务包:

```
unzip dmz-ccr-v2.2.0.zip && cd ./dmz-ccr-v2.2.0
```



(2) 编辑 vi install.sh 脚本如下部分参数值。

```
#####################以下变量的值需要配置成当前环境的#################################

#公服区k8s集群的业务网vip
vip=100.100.0.17

#公服区k8s集群的管理网vip,若是单网卡，则和业务网vip一样
managerVip=10.51.80.135

#对象存储ak
accessKey=ScoQ2xTWguyfMPYL

#对象存储sk
secretKey=hHCSNQC165AfGnBElDfPRbX9xVnuFX

#对象存储访问域名 ENDPOINT
s3Endpoint=s3.onestore-uos.com

#对象存储 访问ip
s3Ip=100.100.0.18

#harbor 的管理员密码。密码长度在8到20之间且需包含至少一个大写字母，一个小写字母和一个数字,特殊字符用\转义。
harborAdminPassword=Harbor12345

#公服区PaaS底座mysql地址
mysqlHost=100.100.0.100

#公服区PaaS底座redis地址+端口号
redisAddr=100.100.0.100:26380


####################变量配置完毕################################
```

(3) 编辑完成后，执行如下命令进行安装。

```
sh install.sh
```

```
[root@ -DMZ-01 dmz-ccr]# sh install.sh
本脚本第一部分是部署Harbor服务需要的环境变量，是否确认已完成参数配置(y/n)，默认为n：y
```

(4) 安装完成后，修改 imageloader 的 configmap，删除定时清理时间配置。

```
kubectl edit cm  dmz-ccr-harbor-imageloader  -n dmz-ccr
```

删除如下内容“CRON_CLEAN_LOG_FILE: 0 1 * * *”。

```
# Please edit the object below. Lines beginning with a '#' will be ignored,
# and an empty file will abort the edit. If an error occurs while saving thi
# reopened with the relevant failures.
#
apiVersion: v1
data:
  CRON_CLEAN_LOG_FILE: 0 1 * * *
  OSS_ACCESS_KEY: ScoQ2xTWguyfMPYL
  OSS_ENDPOINT: http://s3.test.com
  OSS_SECRET_KEY: hHCSNQC165AfGnBElDfPRbX9xVnuFX
  OSS_TEMP_IMAGE_BUCKET: tempcontainerimage
  PRIVATE_REGISTRY: 100.67.0.16:30002
  config.json: |
    {"auths":{"10.252.146.116:30002":{"auth": "YWRtaW46RD0jJkwxI0soOSE4RDVxN
kind: ConfigMap
metadata:
  annotations:
```

(5) 重启 pod。

```
kubectl rollout restart deployment.apps/dmz-ccr-harbor-imageloader -n dmz-ccr
```

```
[root@k8s-m1 cert_manager]# kubectl rollout restart deployment.apps/dmz-ccr-harbor-imageloader -n dmz-ccr
deployment.apps/dmz-ccr-harbor-imageloader restarted
[root@k8s-m1 cert_manager]#
```

7.9.4 验证

安装完成后，查看当前 Harbor 服务是否可以正常使用。方法如下。

(1) 执行如下命令，查看 Harbor 相关 POD 是否正常启动。

```
kubectl get pod -n dmz-ccr
```

```
[root@[redacted]-DMZ-01 ~]# kubectl get pod -n dmz-ccr
NAME                                          READY   STATUS      RESTARTS   AGE
dmz-ccr-harbor-chartmuseum-c4df8fd79-4wnq9    1/1     Running     0          45m
dmz-ccr-harbor-core-756c8b4798-7tnkf          1/1     Running     0          45m
dmz-ccr-harbor-harbor-mysql-init-4hcmz        0/1     Completed   0          49m
dmz-ccr-harbor-imageloader-b954bb496-kpnwh    1/1     Running     0          49m
dmz-ccr-harbor-jobservice-6fd776dc4f-4574g    1/1     Running     0          45m
dmz-ccr-harbor-nginx-6c44684fb5-f7krv         1/1     Running     0          45m
dmz-ccr-harbor-portal-7fb8bff85f-gbcqx        1/1     Running     0          34m
dmz-ccr-harbor-registry-d47df7ccc-spjcl       2/2     Running     0          34m
dmz-ccr-harbor-trivy-0                        1/1     Running     0          45m
```

(2) 在公服务 K8S 集群各个节点执行如下命令，检查是否将 harbor 认证信息加入 docker。

```
cat /root/.docker/config.json
```

```
[root@                -DMZ-K8S-01 ~]# cat /root/.docker/config.json
{
        "auths": {
                "10.253.146.226:30002": {
                        "auth": "YWRtaW46SGFyYm9yNTQzMjE="
                },
                "harbor-local.unicloudsrv.com": {
                        "auth": "YWRtaW46SGFyYm9yMTIzNDU="
                }
        },
        "HttpHeaders": {
                "User-Agent": "Docker-Client/19.03.12 (linux)"
        }
}[root@               -DMZ-K8S-01 ~]#
```

7.9.5 修改 A 层配置

1. 修改 configmap

(1) 在 UCA 集群控制节点执行：kubectl edit cm uca-ccr-cm，编辑如下参数值：

```
# Please edit the object below. Lines beginning with a '#' will be ignored,
# and an empty file will abort the edit. If an error occurs while saving this file will be
# reopened with the relevant failures.
#
apiVersion: v1
data:
  harbor_endpoint: http://10.253.146.225:30002
  harbor_internal_endpoint: http://100.100.63.120:30002
  oss_access_key: jw81bwAOXnbaPOlK
  oss_endpoint_env: http://s3.onestore-uos.com
  oss_secret_key: fm9uaEXaZQZxB3yGl5hzE8yQF9mnqX
kind: ConfigMap
metadata:
```

回显字段说明如下。

- harbor_endpoint：公共服务区 CCR harbor 的管理网访问地址。
- harbor_internal_endpoint：公共服务区 CCR harbor 的业务网访问地址。
- oss_endpoint_env：对象存储的访问地址，注意看云平台控制台是 http 还是 https，需要与云平台的协议保持一致。
- oss_access_key：对象存储的 AK。
- oss_secret_key：对象存储的 SK。

(2) 修改完成后，保存退出。

2. 修改 secret

(1) 在 UCA 集群控制节点执行：

```
kubectl edit  secret dmz-harbor-secret,
```

(2) 编辑如下参数值：

harbor_pass：公共服务区 CCR Harbor 的管理员密码，需要用 base64 加密，比如密码为 Harbor54321，用 base64 加密： echo -n Harbor54321|base64 后为 SGFyYm9yNTQzMjE=。

```
[root@ [redacted] -UCA-K8S-02 ~]# echo  -n  Harbor54321|base64
SGFyYm9yNTQzMjE=
```

```
# Please edit the object below. Lines beginning with a '#' will be ignored,
# and an empty file will abort the edit. If an error occurs while saving this file will be
# reopened with the relevant failures.
#
apiVersion: v1
data:
  harbor_pass: SGFyYm9yMTIzNDU=
  harbor_user: YWRtaW4=
kind: Secret
metadata:
  annotations:
    kubectl.kubernetes.io/last-applied-configuration: |
      {"apiVersion":"v1","data":{"harbor_pass":"SGFyYm9yMTIzNDU=","harbor_user":"YWRtaW4="},"
"type":"Opaque"}
  creationTimestamp: "2023-02-15T06:57:09Z"
  name: dmz-harbor-secret
  namespace: default
  resourceVersion: "8575"
  selfLink: /api/v1/namespaces/default/secrets/dmz-harbor-secret
  uid: 23477347-2c8b-4dd3-b22c-3c0f4179be57
type: Opaque
```

3. 重启 pod

在 UCA 集群控制节点执行命令加载重启 pod：

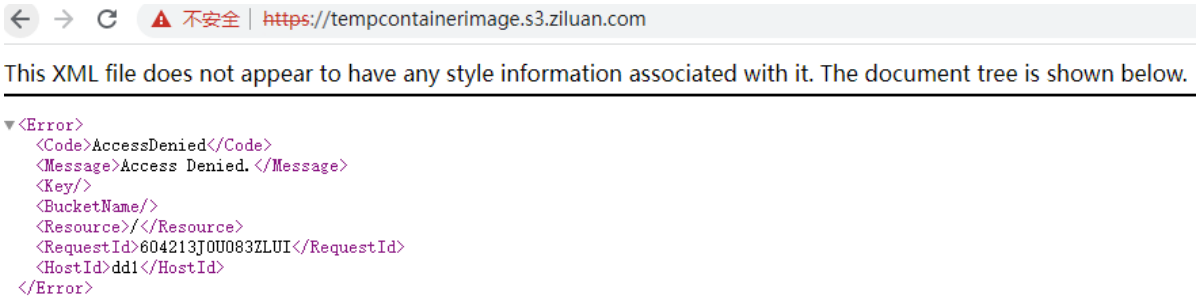
```
kubectl rollout restart deployment.apps/uca-ccr-core
```

```
[root@ [redacted] -UCA-K8S-02 ~]# kubectl rollout restart deployment.apps/uca-ccr-core
deployment.apps/uca-ccr-core restarted
[root@ [redacted] -UCA-K8S-02 ~]#
```

4. 检查控制台操作

在云平台“镜像仓库”控制台上传、下载、构建镜像，查看是否正常。

上传镜像前需要先在浏览器访问对象存储域名地址，如：https://tempcontainerimage.s3.ziluan.com/，用于下载对象存储的相关证书。



如果上传过程中出现 blocked:mixed-contet，https mixed http 等相关报错，是平台使用的协议和对象存储的协议不相同导致（一个为 https，一个为 http）。需要修改 UCA 集群 ccr 的 configmap：uca-ccr-cm，在 UCA 集群任一节点执行命令 kubectl edit configmap uca-ccr-cm，修改 oss_endpoint_env 属性为对应 http 或者 https。修改完毕执行 kubectl rollout restart deployment.apps/uca-ccr-core 重启 uca-ccr-core。

7.9.6 修改 O 层配置

修改 uco-ccr 数据库中的表 ccr_region，新增如下记录。截图中的取值仅为示例，请以实际环境为准。

uco_ccr.ccr_region: 1 总记录数 (大约)

id	region_id	endpoint	internal_endpoint
1	[redacted]	10[redacted]:30002	10[redacted]:30002

其中，region_id 为当前 region 的 id；endpoint 为公服务 CCR Harbor 的管理网地址，internal_endpoint 为公服务 CCR Harbor 的业务网地址，注意地址不加 http，如果公服区 k8s 为单网卡，管理网地址和业务网地址填一样。

7.10 云容器引擎CCE初始化

7.10.1 安装前装备

1. 文件仓库、yum 仓库、镜像仓库服务搭建

在公共服务区域搭建一个仓库服务，用于提供创建 CCE 集群所需要的文件仓库服务、yum 仓库服务、镜像仓库服务。要求如下：

- 通过虚拟机镜像模板 cce_repo_server 进行创建。默认 root 密码：Passw0rd@_。请从版本发布路径下获取：全量包\云服务组件包\容器\cce_repo_server
- 硬件要求：至少 4 核 CPU、8G 内存，硬盘 50G。
- 配置业务 IP，确保 CCE 集群能访问该 IP。安装完成后进行验证，保证各个服务能正常运行。

2. 验证文件仓库和 yum 仓库

打开浏览器，在地址栏中输入地址: http://{虚拟机 IP}:8081，初始账号为:admin / Passw0rd@_，检查服务是否正常。

如果不能正常访问，尝试使用 systemctl restart artifactory 命令重启服务。

如果仍然无法访问，执行 ps -ef |grep artifactory 命令，然后用 kill 命令停掉所有的 artifactory 进程，再执行 systemctl start artifactory。

3. 验证镜像仓库

打开浏览器，在地址栏中输入地址: http://{虚拟机 IP}:30002，初始账号/密码为:admin/Harbor12345，检查服务是否正常。

如果不能正常访问，执行 systemctl restart docker 命令重启 Docker，待 Docker 重启后，执行 systemctl restart harbor 命令重启 harbor。

4. 系统镜像和上传方法说明

x86 架构系统镜像包括 CentOS 和 Kylin 系统镜像，镜像包分别为：centos-7.6-x86_64.tar、kylin-v10-x86_64.tar（请从版本发布路径获取：全量包\云服务组件包\容器），解压后得到镜像文件名称以及一个 MD5 文件，请确保镜像文件的 MD5 值与文件中的 md5 值相同。

- CentOS 系统镜像

镜像文件名称	IMAGE_ID
CCE_CentOS_7_6_64_ECS	CCE_CentOS_7_6_64_ECS
CCE_CentOS_7_6_64_BMS	CCE_CentOS_7_6_64_BMS
CCE_CentOS_7_6_64_GPU	CCE_CentOS_7_6_64_GPU

- Kylin 系统镜像

镜像文件名称	IMAGE_ID
CCE_Kylin_V10_X86_64_ECS	CCE_Kylin_V10_X86_64_ECS
CCE_Kylin_V10_X86_64_BMS	CCE_Kylin_V10_X86_64_BMS

上传方式说明：通过 OMC 自动上传。参见 5. 通过 OMC 运维管理平台上传。

5. 通过 OMC 运维管理平台上传

在 OMC 界面上传之前必须将镜像上传至指定的 FTP 服务器上，保证 OMC 能连接上 FTP 服务器。

(1) 登录运维 OMC 界面，点击页面左上方的  ，选择[IAAS/基础设施平台]。

(2) 在基础设施平台导航栏中，选择[云计算/镜像管理]，进入镜像管理界面。

(3) 选择[公共镜像]页签，点击<上传共有镜像>按钮，按要求填写或者选择参数，分发位置选存储设备，然后上传；下面以 cce-ecs 为例。

其中，[存储设备]参数请仅选中存储类型为块存储的设备。存储类型在[云存储/存储集群]中查看。

6. 确保容器 VKS 纳管

确保容器 VKS 已经纳管完成。如果已纳管，则忽略。

(1) 登录运维 OMC 界面，点击页面左上方的  ，选择[IAAS/基础设施平台]。

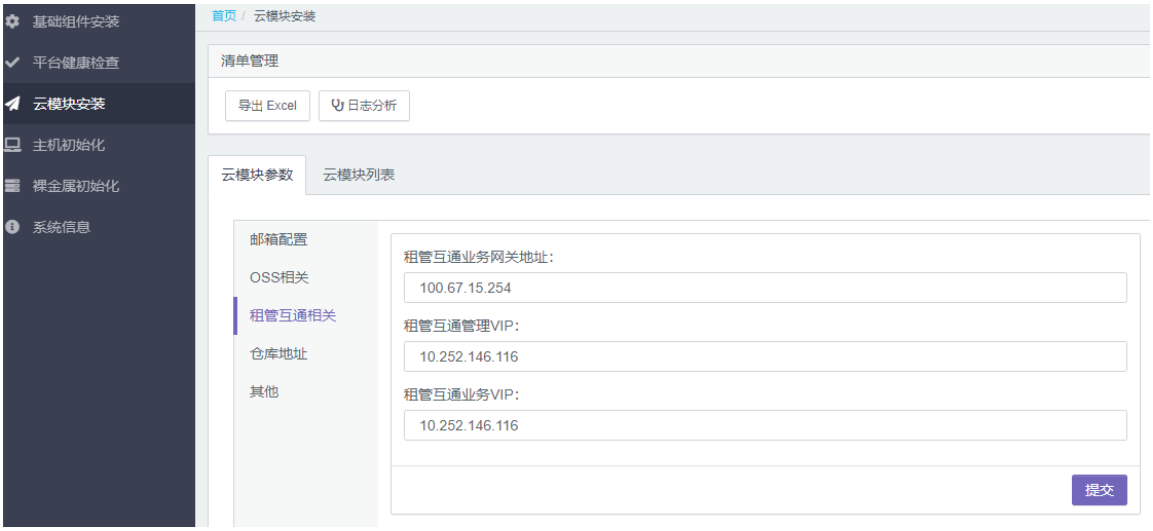
(2) 在基础设施平台导航栏中，选择[云计算/宿主机集群]，查看“资源标签”是否存在“cce”，如果没有，则新建集群。

(3) 在宿主机集群页面，选择[主机]页签，点击<纳管主机>按钮，请根据实际情况进行纳管，集群类型如果是 bms，则选择“裸金属服务器”，网络类型根据实际规划选择“HostOverlay”或者“NetworkOverlay”。

(4) 纳管后，此时的主机处于维护模式，需要在“操作”一栏的“更多”选择“退出维护模式”。

7. 修改云模块参数

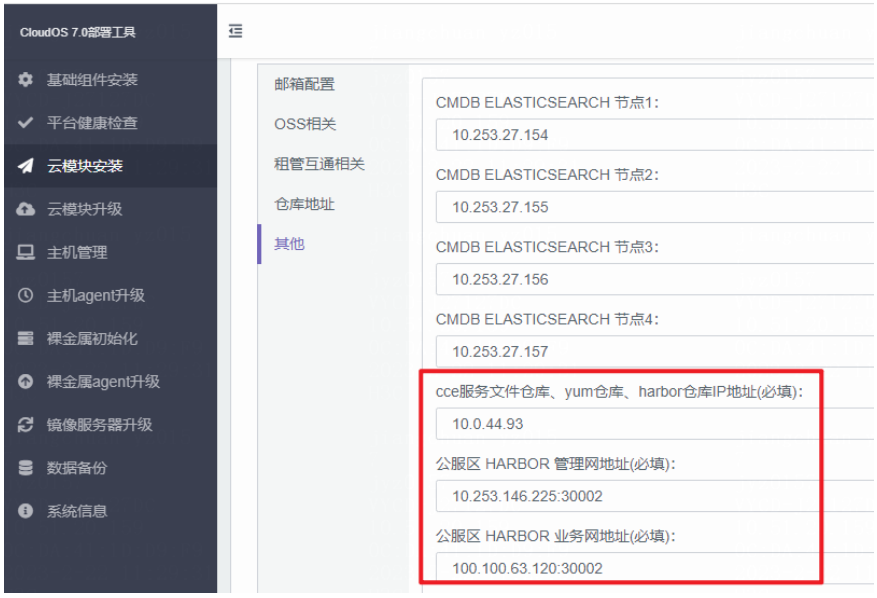
使用云平台部署工具安装部署云容器前，需要修改云模块参数。在浏览器中打开部署工具地址，点击[云模块安装/云模块参数]，选择<租管互通相关>页签，根据组网要求，填写相关参数，填写完成后，点击提交。如果无 VIP，则填写租管互通某台具体服务器的管理 IP、业务 IP。



点击“其他”选项，修改参数：

- cce 服务文件仓库、yum 仓库、harbor 仓库 IP 地址：将参数值修改为第 1 步过程中创建的虚拟机的业务 IP 地址。
- 公服区 HARBOR 管理网地址：公共服务区 Harbor 的管理地址。
- 公服区 HARBOR 业务网地址：公共服务区 Harbor 的业务地址。

示例如下：



8. A 层服务部署

使用云平台部署工具安装部署。在浏览器中打开部署工具地址，点击[云模块安装/云模块列表]，点击<uca>按钮，找到 uca-cce-core 服务，点击左侧<部署项目>按钮进项部署。

9. O 层服务部署

使用云平台部署工具安装部署。在浏览器中打开部署工具地址，点击[云模块安装/云模块列表]，点击<uca>按钮，找到 uco-cce-core 服务，点击左侧<部署项目>按钮进项部署。

7.10.2 数据库配置

1. 配置 A 层数据库虚机模板

如果**云容器引擎的 VKS 主机数>=3 台**，则忽略。

如果**云容器引擎的 VKS 主机数< 3 台**，请修改 cce.dictionary 表，找到 name 为“创建集群模板”和“创建虚拟机裸金属混合集群模板”：

id	dictionary_type	name	value	description
64	21	创建集群模板	{"ServiceType": "...	(NULL)
67	24	创建虚拟机裸金属混合集群模板	{"ServiceType": "...	(NULL)

修改其中的 master 节点的 Level 为“non-force”(worker 的 Level 不变)。

```
[
    "ServiceType": "[redacted]::PaaS",
    "ServiceTag": "[redacted]::k8s::Instance",
    "UserId": "{{userId}}",
    "Region": "{{regionId}}",
    "AvailableZones": [{
        "AvailableZone": "{{zoneId}}",
        "Count": 1,
        "Replica": [{
            "Count": {{masterCount}},
            "Type": "master",
            "NonAffinity": "server",
            "Level": "non-force",
            "Env": {
                "Path": "/local/bin"
            },
            "ConfigId": "{{masterConfigId}}"
        },{
```

7.10.3 修改 UCA 的配置

1. 修改配置 configmap cce-cm

执行命令：

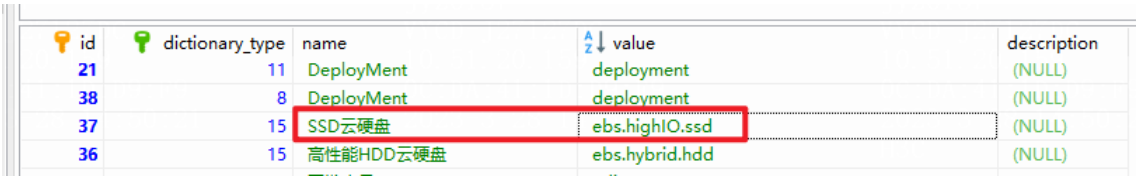
```
kubectl edit cm cce-cm
```

修改如下字段。

- regionendpoint，OSS 对象存储的域名(需要在 node_hosts 中加上，ip 使用业务 ip)
- node_hosts，表示“IP 域名”解析列表，在创建集群时会添加到 CCE 节点的/etc/hosts 中。当存在多个时，使用逗号进行分隔。比如 regionendpoint 中的对象存储，就需要加上业务 IP，例如：

```
node_hosts: 100.100.63.121  cce-harbor.unicloudsrv.com,100.100.0.1 s3.test.com
node_routes: |
  []
pluginharts: http://100.100.63.121:30002/chartrepo/pluginchart
publicharts: http://100.100.63.136:30002/chartrepo/public_charts
region: cd-l2-dev
regionendpoint: s3.test.com
```

- pvEbsType，默认配置”ebs.highIO,ebs.hybrid,ebs.fc”这三类云硬盘，根据实际情况进行配置，多个配置用英文逗号分隔，如果使用全部类型，请用”*”代替所有，如果 configMap 中没有该字段，请添加。
- storageclassEbsType，storageClass 使用的云硬盘类型，{"storageclassEbsType":[{"name":"SSD 云硬盘","value":"ebs.ones_ssd.ssd"},{"name":"高性能云硬盘","value":"ebs.ones_hybrid.hdd"}]}，请确保 name 和 value 与 A 层数据库表 cce.dictionary 中的配置保持一致。



id	dictionary_type	name	value	description
21	11	DeployMent	deployment	(NULL)
38	8	DeployMent	deployment	(NULL)
37	15	SSD云硬盘	ebs.highIO.ssd	(NULL)
36	15	高性能HDD云硬盘	ebs.hybrid.hdd	(NULL)

2. 重启

修改完 configmap 后，需要重启 uca-cce 的 pod。

```
kubectl get pod | grep uca-cce- | grep -v uca-cce-manager | awk '{print $1}' |xargs kubectl delete pod
```

7.11 数据库初始化

7.11.1 DBAAS RDS UCA 初始化

镜像文件位于版本发布路径：全量包\云服务组件包\数据库\05UNICLOUD-DBAAS.tar.gz，将压缩包下载到本地，解压缩后获取镜像文件。

1. 上传 RDS 镜像

上传镜像的方式有两种，您可以选择其中一种：

第一种为参考“6.5 上传镜像”中对应的导入镜像章节，手动导入镜像。

第二种为在 OMC 平台中进行上传。上传方法如下。

(1) 在 OMC 运维管理平台选择[IAAS/基础设施平台]菜单项，进入基础设施平台页面。

(2) 单击左侧导航树[云计算/镜像管理]菜单项，进入镜像管理页面。

(3) 在公有镜像页签中，单击<上传公有镜像>按钮，进入上传公有镜像页面。

(4) 输入各项属性值，单击<确定>按钮完成操作。

镜像路径、镜像 ID 说明如下。

- sqlserver-2016(2019)-enterprise-HA-witness (samba)镜像：
  UCA-RDS\images\sqlserver_samba_41016_*XXXX*.qcow2
  “镜像 ID”字段与数据库表 uni_rds.image_versions 中 sqlserver-2016(2019)-enterprise-HA-witness 对应的 image_id 保持一致。
- sqlserver-2016-enterprise-HA & SE 镜像：
  UCA-RDS\images\Win2k19_MSSQL2k16_IMG_*XXXX*.qcow2
  “镜像 ID”字段与数据库表 uni_rds.image_versions 中 sqlserver-2016-enterprise-HA & SE 对应的 image_id 保持一致。
- sqlserver-2019-enterprise-HA & SE 镜像：
  UCA-RDS\images\Win2k19_MSSQL2k19_IMG_*XXXX*.qcow2
  “镜像 ID”字段与数据库表 uni_rds.image_versions 中 sqlserver-2019-enterprise-HA & SE 对应的 image_id 保持一致。
- Postgresql-11.6-SE & HA 镜像：
  UCA-RDS\images\rds-postgresql-11.6-v3.4.3-*XXXX*.qcow2
  “镜像 ID”字段与数据库表 uni_rds.image_versions 中 postgresql-11.6-SE & HA 对应的 image_id 保持一致。

- Postgresql-13.4-SE & HA 镜像：

  UCA-RDS\images\rds-postgresql-13.4-v3.4.3-*XXXX*.qcow2

  “镜像 ID”字段与数据库表 uni_rds.image_versions 中 postgresql-13.4-SE & HA 对应的 image_id 保持一致。
- Mysql-5.7-SE & HA 镜像：

  UCA-NOSQL\images\rds-mysql-5.7-v3.4.4-*XXXX*.qcow2

  “镜像 ID”字段与数据库表 uni_rds.image_versions 中 mysql-5.7-SE & HA 对应的 image_id 保持一致。
- Mysql-8.0-SE & HA & EE 镜像：

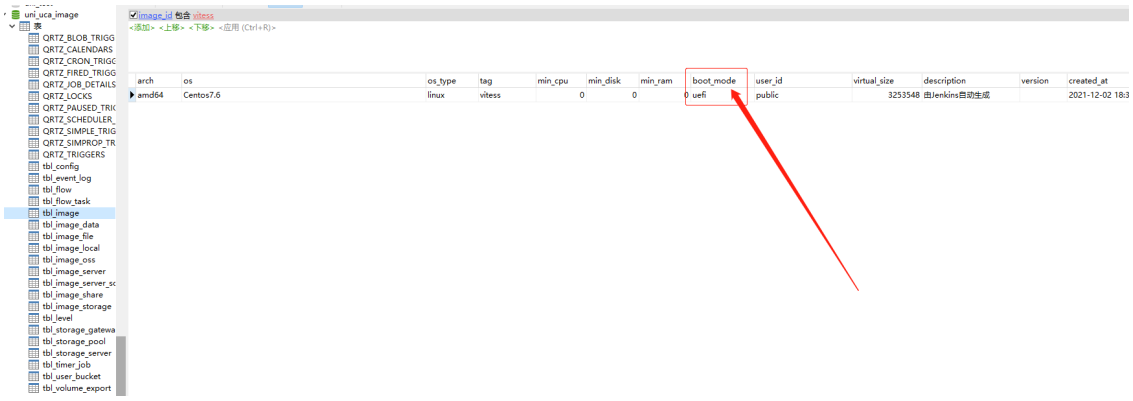
  UCA-NOSQL\images\rds-mysql-8.0.28-v3.4.4-*XXXX*.qcow2

  “镜像 ID”字段与数据库表 uni_rds.image_versions 中 mysql-8.0-SE & HA & EE 对应的 image_id 保持一致。
- Vitess 镜像：

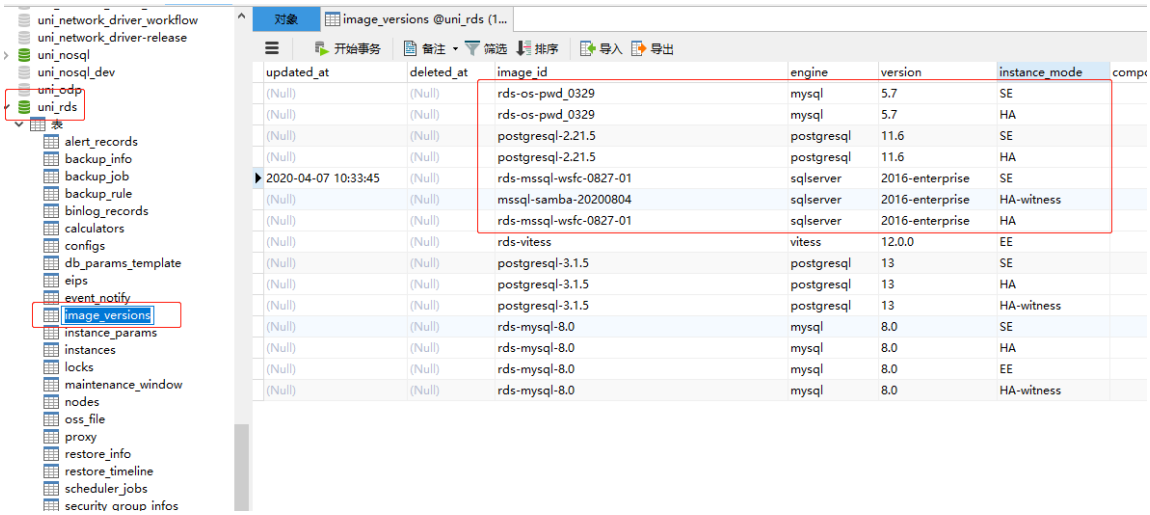
  UCA-NOSQL\images\rds-vitess-12.0.0-v3.1.2-*XXXX*.qcow2

  “镜像 ID”字段与数据库表 uni_rds.image_versions 中 Vitess 对应的 image_id 保持一致。

  注意：vitess 镜像的 boot_mode 是 uefi



RDS 镜像配置示例如下：



2. 上传 RDS 的 OSS 文件

在 OSS 上创建 4 个桶，桶名称可以自定义，但需要和 uni_rds 库中的 configs 表的参数字段对应：参数字段如下：

id	created_at	updated_at	deleted_at	key	value
25	(Null)	(Null)	(Null)	board_url	10.252.146.115:18080
32	(Null)	2022-01-21 20:3	(Null)	ALERT_RECEIVER_USER_ID	37b2bbe4-ed23-4a25-ad30-8c398bbd3639,8cc52fa3-c113-4857-b33b-bf0c9469e8e4
33	(Null)	(Null)	(Null)	ALERT_LEVEL	1
34	(Null)	2021-12-02 16:3	(Null)	ADMIN_ACCOUNT	admin
35	(Null)	2021-12-02 16:3	(Null)	ADMIN_PASSWORD	Bjzw2020!
36	(Null)	2021-12-02 16:3	(Null)	ALERT_HOST	http://uca-dbaas-oc-alert-service:40611
37	(Null)	2022-08-22 16:2	(Null)	BACKUP_AGENT_TIMEOUT	100
38	(Null)	2022-04-12 16:0	(Null)	BACKUP_BUCKET_NAME	uni-backup-rds-yfb1
39	(Null)	2021-12-02 16:3	(Null)	BINLOG_RESERVE_HOUR	6
40	(Null)	2022-04-11 18:0	(Null)	BINLOG_RETAIN_DAYS	2
41	(Null)	2022-12-14 13:1	(Null)	BINLOG_UPLOAD_INTERVAL	10
42	(Null)	2022-01-27 14:1	(Null)	FUNCTION_VERSION	3.1.2
43	(Null)	2021-12-02 16:3	(Null)	LOG_BACKUP_INTERVAL	15
44	(Null)	2021-12-02 16:3	(Null)	MAX_READ_ONLY_COUNT	5
45	(Null)	2021-12-02 16:3	(Null)	MSSQL_MAX_MEMORY_MB	2: 1024, 4: 3072,6:4608,8: 6144, 12:9216,16: 12288, 24: 19456, 32: 26624,48: 40496, 6
46	(Null)	2022-04-12 16:0	(Null)	MYSQL_BINLOG_BUCKET_NAME	moove-mysqlbinlogs-yfb1
47	(Null)	2021-12-02 16:3	(Null)	NETWORK_OS_BASE	http://uni-uca-center-service:40298/core
48	(Null)	2021-12-02 16:3	(Null)	NGINX_HOST	http://uca-dbaas-nginx-service:40621/rds/
49	(Null)	2022-12-14 13:3	(Null)	NON_AFFINITY	false
50	(Null)	2022-12-14 13:1	(Null)	OSS_ACCESS_KEY	ZL69KjBaS24HimJnS4ibypwpymfkyE
51	(Null)	2021-12-02 16:3	(Null)	OSS_CONFIG_RETRY_TIMES	10
52	(Null)	2022-12-14 13:1	(Null)	OSS_ENDPOINT	http://s3.test.com
53	(Null)	2022-12-14 13:1	(Null)	OSS_HOSTNAME	s3.test.com
54	(Null)	2022-12-14 14:0	(Null)	OSS_IP	10.0.42.61
55	(Null)	2022-12-14 13:1	(Null)	OSS_KEY_ID	NsDV1JQdZZA1jKtJ
56	(Null)	2021-12-02 16:3	(Null)	OSS_NETMASK	255.255.255.255
57	(Null)	2022-12-14 16:2	(Null)	OSS_RDS_BUCKET	uni-rds-yfb344
58	(Null)	2022-04-12 16:0	(Null)	OSS_RDS_LOG_BUCKET	moove-rds-log-pre1
59	(Null)	2022-08-10 11:3	(Null)	OSS_TIME_DELAY	800
60	(Null)	2021-12-02 16:3	(Null)	RABBIT_HOST	rabbitmq-service:5672
61	(Null)	2021-12-02 16:3	(Null)	RABBIT_PWD	cloudos
62	(Null)	2021-12-02 16:3	(Null)	RABBIT_USER	openstack
63	(Null)	2021-12-02 16:3	(Null)	REDIS_HOST	redis-service:6379
64	(Null)	2021-12-02 16:3	(Null)	REDIS_PWD	unic-moove
65	(Null)	2022-08-10 11:3	(Null)	RESTORE_AGENT_TIMEOUT	800

- BACKUP_BUCKET_NAME：RDS 实例备份桶
- MYSQL_BINLOG_BUCKET_NAME：mysqlbinlog 桶
- OSS_RDS_BUCKET：RDS 依赖文件桶

- OSS_RDS_LOG_BUCKET：RDS 日志桶

将 RDS 的依赖文件（位于 UCA-RDS\oss）上传到 RDS 的依赖文件桶中，依赖文件桶的桶名可以从 configs 表中 OSS_RDS_BUCKET 字段获取。可以使用 S3 客户端上传，也可以在云控制台使用与 configs 表中的 AK、SK 对应的账号登录，在控制台上传。

3. 配置参数

RDS 在数据库中（uni_rds 库中的 config 表）进行配置，请根据根据具体环境配置参数，修改后需要重启 pod。

id	created_at	updated_at	deleted_at	key	value
38	(Null)	2022-04-12 16:0	(Null)	BACKUP_BUCKET_NAME	uni-backup-rds-yfb1
39	(Null)	2021-12-02 16:3	(Null)	BINLOG_RESERVE_HOUR	6
40	(Null)	2022-04-11 18:0	(Null)	BINLOG_RETAIN_DAYS	2
41	(Null)	2022-12-14 13:1	(Null)	BINLOG_UPLOAD_INTERVAL	10
42	(Null)	2022-01-27 14:1	(Null)	FUNCTION_VERSION	3.1.2
43	(Null)	2021-12-02 16:3	(Null)	LOG_BACKUP_INTERVAL	15
44	(Null)	2021-12-02 16:3	(Null)	MAX_READ_ONLY_COUNT	5
45	(Null)	2021-12-02 16:3	(Null)	MSSQL_MAX_MEMORY_MB	2: 1024, 4: 3072,6:4608,8: 6144, 12:9216,16: 12288, 24: 19456, 32: 26624,48: 40496, 6
46	(Null)	2022-04-12 16:0	(Null)	MYSQL_BINLOG_BUCKET_NAME	moove-mysqlbinlogs-yfb1
47	(Null)	2021-12-02 16:3	(Null)	NETWORK_OS_BASE	http://uni-uca-center-service:40298/core
48	(Null)	2021-12-02 16:3	(Null)	NGINX_HOST	http://uca-dbaas-nginx-service:40621/rds/
49	(Null)	2022-12-14 13:3	(Null)	NON_AFFINITY	false
50	(Null)	2022-12-14 13:1	(Null)	OSS_ACCESS_KEY	ZL69KjBaS24HimJnS4ibypwpymfkyE
51	(Null)	2021-12-02 16:3	(Null)	OSS_CONFIG_RETRY_TIMES	10
52	(Null)	2022-12-14 13:1	(Null)	OSS_ENDPOINT	http://s3.test.com
53	(Null)	2022-12-14 13:1	(Null)	OSS_HOSTNAME	s3.test.com
54	(Null)	2022-12-14 14:0	(Null)	OSS_IP	10.0.42.61
55	(Null)	2022-12-14 13:1	(Null)	OSS_KEY_ID	NsDV1JQdZZA1jKtJ
56	(Null)	2021-12-02 16:3	(Null)	OSS_NETMASK	255.255.255.255
57	(Null)	2022-12-14 16:2	(Null)	OSS_RDS_BUCKET	uni-rds-yfb344
58	(Null)	2022-04-12 16:0	(Null)	OSS_RDS_LOG_BUCKET	moove-rds-log-pre1
59	(Null)	2022-08-10 11:3	(Null)	OSS_TIME_DELAY	800
60	(Null)	2021-12-02 16:3	(Null)	RABBIT_HOST	rabbitmq-service:5672
61	(Null)	2021-12-02 16:3	(Null)	RABBIT_PWD	cloudos
62	(Null)	2021-12-02 16:3	(Null)	RABBIT_USER	openstack
63	(Null)	2021-12-02 16:3	(Null)	REDIS_HOST	redis-service:6379
64	(Null)	2021-12-02 16:3	(Null)	REDIS_PWD	unic-moove
65	(Null)	2022-08-10 11:3	(Null)	RESTORE_AGENT_TIMEOUT	800
66	(Null)	2022-09-19 11:4	(Null)	RETAIN_DAYS	7
67	(Null)	2021-12-02 16:3	(Null)	UCO_DELIVERY_PORT	31112
68	(Null)	2021-12-02 16:3	(Null)	UCO_OS_BASE	uco-delivery-core
69	(Null)	2021-12-02 16:3	(Null)	UCO_RDS_PORT	31125
70	(Null)	2022-06-20 16:5	(Null)	UCM_GROUP_IPS	100.67.100.1/24
71	(Null)	2021-12-02 16:3	(Null)	RELOAD_FLAG	false
72	(Null)	2022-01-24 13:4	(Null)	DEFAULT_SYSTEM_DISK_SIZE	60
73	(Null)	2022-01-24 13:4	(Null)	DEFAULT_SYSTEM_DISK_SIZE	60
74	(Null)	2022-01-24 13:4	(Null)	DEFAULT_SYSTEM_DISK_SIZE	60
75	(Null)	(Null)	(Null)	ALERT_REGION_ID	cn-tianjin-yfb
76	(Null)	2022-04-08 14:5	(Null)	MANUAL_UPGRADE	false
77	(Null)	(Null)	(Null)	UCM_HOST_NAME	uca.reception.unicloudsrv.com
78	(Null)	2022-06-20 16:2	(Null)	UCM_HOST_IP	100.67.100.225
79	(Null)	(Null)	(Null)	UCM_HOST_PORT	40702
80	(Null)	(Null)	(Null)	UCM_PUSH_WAY	ip
81	(Null)	(Null)	(Null)	UCM_PUSH_INTERVAL	30
82	(Null)	(Null)	(Null)	UCM_HEARTBEAT_INTERVAL	30
83	(Null)	(Null)	(Null)	UCM_AK_MYSQL	849A65BAB85E0D72BB350A67B33AA53D
84	(Null)	(Null)	(Null)	UCM_SK_MYSQL	1A58673DB26542F6AE99BD15994AEE35E836F7A7A2CB405CA88164CB0DDC9F69
85	(Null)	(Null)	(Null)	UCM_AGENT_ID_MYSQL	0e25e272d4eb576c1074cddf9b837f36
86	(Null)	(Null)	(Null)	UCM_AK_POSTGRESQL	A53A8AF85AC2EA2E577D1A6371E3F761

参数说明：

- OSS_ACCESS_KEY：OSS SK
- OSS_KEY_ID：OSS AK

- OSS_ENDPOINT：OSS 地址，注意私有云部署无 https 证书时，配置为 http://域名
- OSS_HOSTNAME：OSS 域名
- OSS_IP：OSS IP 地址
- BACKUP_BUCKET_NAME：RDS 备份桶
- MYSQL_BINLOG_BUCKET_NAME：mysqlbinlog 桶
- OSS_RDS_BUCKET：RDS 依赖文件桶
- OSS_RDS_LOG_BUCKET：RDS 日志桶
- UCM_HOST_IP：云监控地址
- UCM_GROUP_IPS：云监控 DMZ 地址段，逗号分割

4. 执行 sql 文件

由于该版本使用 Rebirth 工具自动部署时，有 sql 文件顺序问题导致 sql 文件：12.UNI_DBAAS_UCA_RDS_V4.1.1.sql 无法完全执行，需要在自动化部署后，手动执行 sql 文件：12.UNI_DBAAS_UCA_RDS_V4.1.1.sql 完成部署。文件位于发版路径：全量包/云服务组件包/数据库/05UNICLOUD-DBAAS.tar.gz，解压缩后获取。

7.11.2 DBAAS NOSQL UCA 初始化

1. 上传 NOSQL 镜像

上传镜像的方式有两种，您可以选择其中一种：

第一种为参考“6.5 上传镜像”中对应的导入镜像章节，手动导入镜像。

第二种为在 OMC 平台中进行上传。上传方法如下：

(1) 在 OMC 运维管理平台选择[IAAS/基础设施平台]菜单项，进入基础设施平台页面。

(2) 单击左侧导航树[云计算/镜像管理]菜单项，进入镜像管理页面。

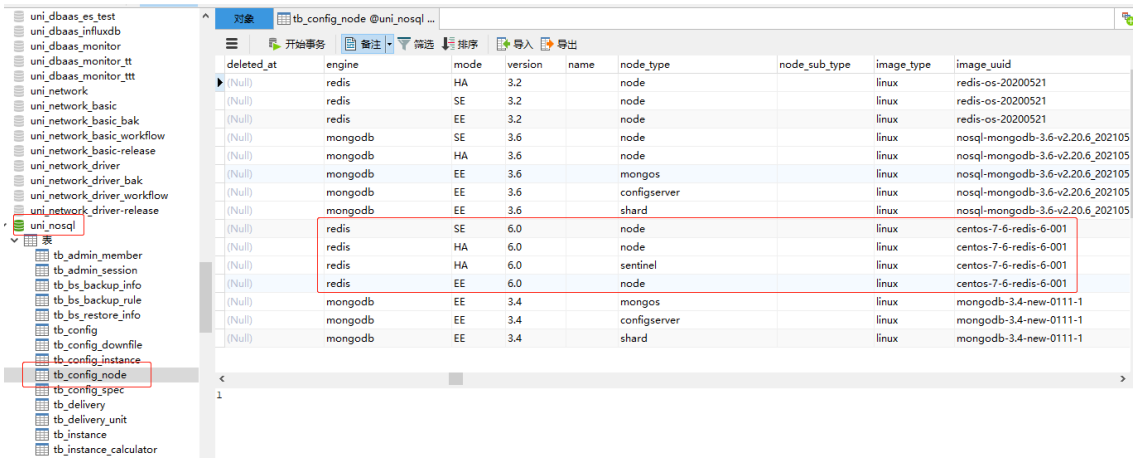
(3) 在公有镜像页签中，单击<上传公有镜像>按钮，进入上传公有镜像页面。

(4) 输入各项属性值，单击<确定>按钮完成操作。

镜像路径、镜像 ID 说明如下。截图仅供参考，请以实际项目为准。

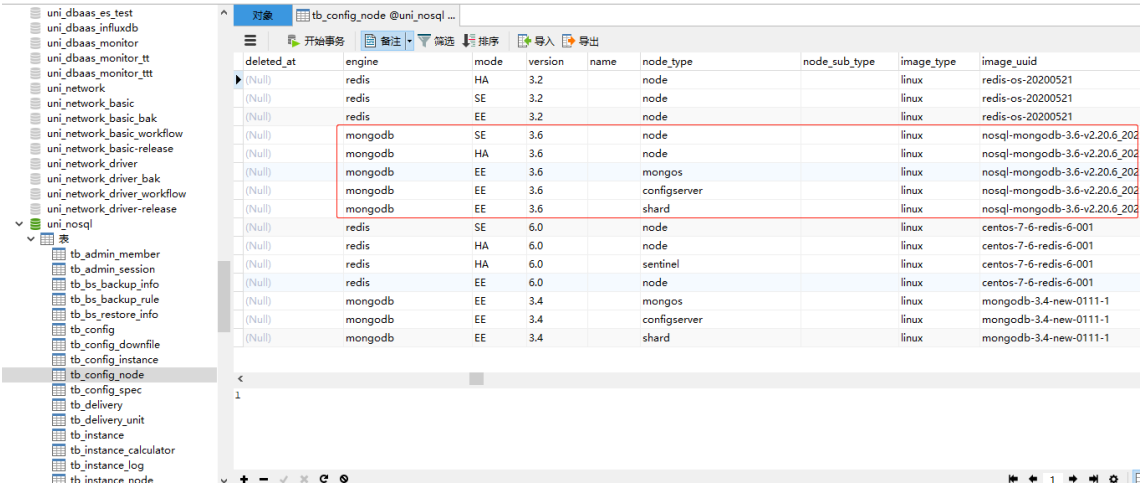
- **Redis6.0 镜像：**UCA-NOSQL\images\nosql-redis-6.0-*XXXX*

  “镜像 ID”字段需要与数据库表 uni_nosql.tb_config_node 中 redis 6.0 对应的 image_uuid 保持一致。



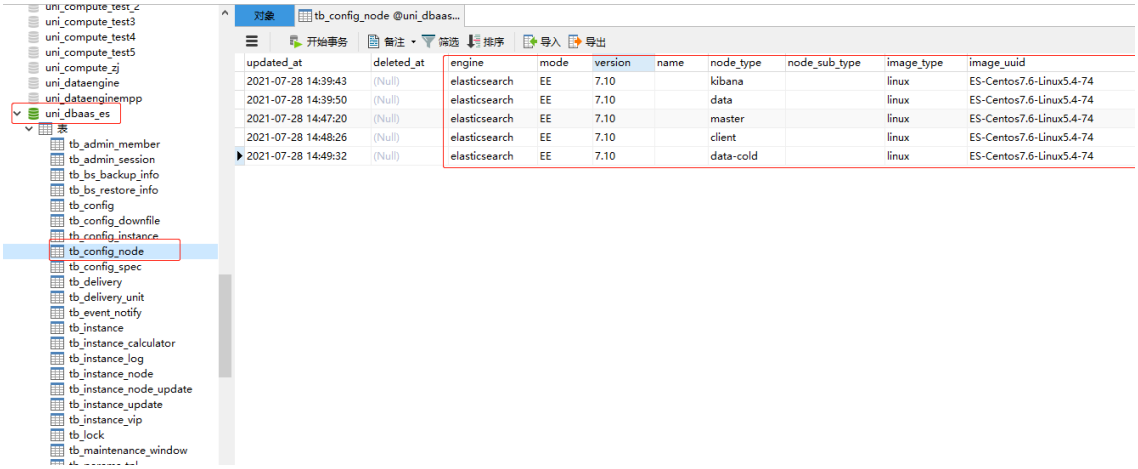
- **Mongodb3.6 镜像：**UCA-NOSQL\images\nosql-mongodb-3.6-*XXXX*

  “镜像 ID”字段需要与数据库表 uni_nosql.tb_config_node 中 mongodb3.6 对应的 image_uuid 保持一致。



- **Elasticsearch 镜像：**UCA-NOSQL\images\ES-Centos7.6-Linux5.4-88.qcow2

  “镜像 ID”字段需要与数据库表 uni_dbaas_es.tb_config_node 中 elasticsearch7.10 对应的 image_uuid 保持一致。



- **InfluxDB 镜像：**UCA-NOSQL\images\InfluxDB-Centos7.6-Linux5.4-86.qcow2

  “镜像 ID”字段需要与数据库表 uni_dbaas_influxdb.tb_config_node 中 influxdb2.1 对应的 image_uuid 保持一致。

2. 修改云监控相关配置

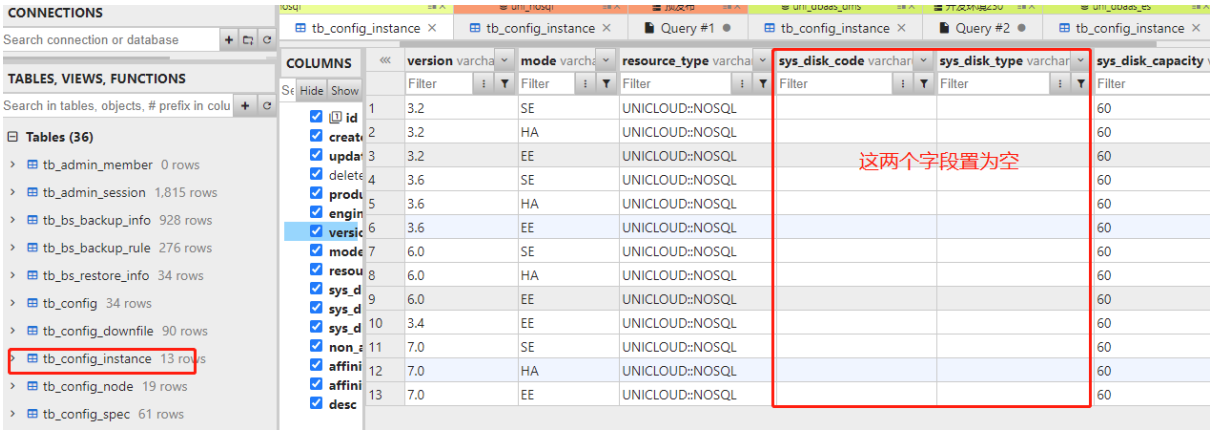
请根据真实环境信息，修改云监控相关的配置。修改【uni_nosql.tb_config，uni_dbaas_es. tb_config，uni_dbaas_influxdb.tb_config】表中的如下信息。

Key 名字	说明
DEFAULT_EGRESS_IPS	安全组出口放行的IP，一般为DMZ区的IP段（因为云监控在DMZ区，实例需要通过业务网向DMZ区的云监控服务推送数据），举例：100.100.12.0/24。
AGENT_UCM_DOMAIN_NAME	云监控服务的域名（IP也支持，参数）

3. 存储双活相关配置

如果项目环境中需要添加存储双活功能，请参考如下步骤进行修改。

Redis 和 MongoDB 产品需要将 uni_nosql.tb_config_instance 的[sys_disk_code]和[sys_disk_type]两个字段的值置为空。如下图所示：



4. 上传 NOSQL 的 OSS 文件

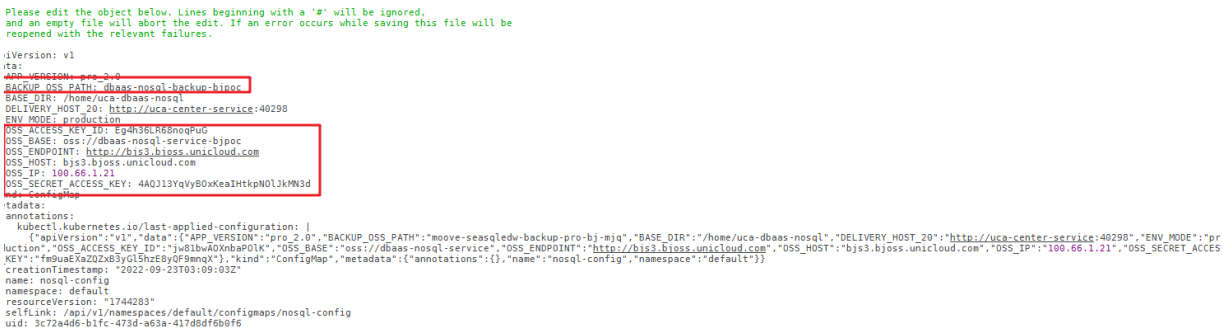
在 OSS 上创建两个桶，NOSQL 备份桶和 NOSQL 依赖文件桶。桶命名如下：

- NOSQL 备份桶：dbaas-nosql-backup-【自定义字段】
- NOSQL 依赖文件桶：dbaas-nosql-service-【自定义字】

其中，自定义字段建议使用 Region 的简写，能区分出 Region 即可。

OSS 上创建的桶要与 configmap 中的配置相对应：

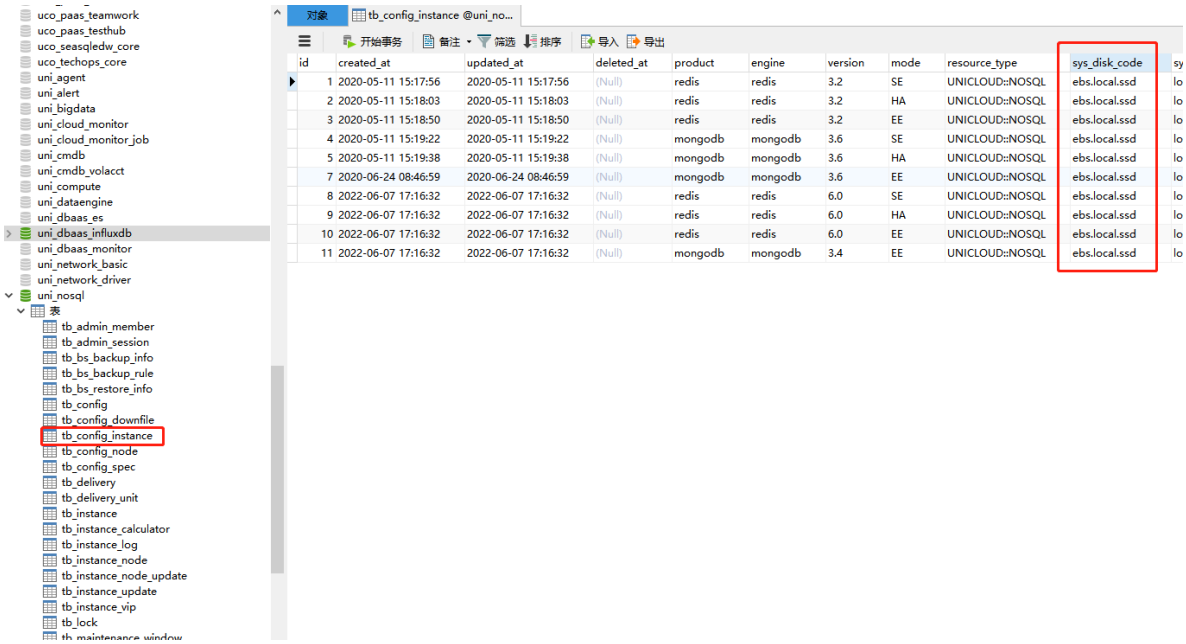
- BACKUP_OSS_PATH 为 NOSQL 的备份桶
- OSS_BASE 为 NOSQL 的依赖文件桶



将 NOSQL 的依赖文件（位于 UCA-RDS\oss）上传到 NOSQL 的依赖文件桶中，依赖文件桶的桶名可以从 configmap 中的 OSS_BASE 字段获取。可以使用 S3 客户端上传，也可以在云控制台使用与 configmap 中 AK、SK 对应的账号登录，在控制台上传。

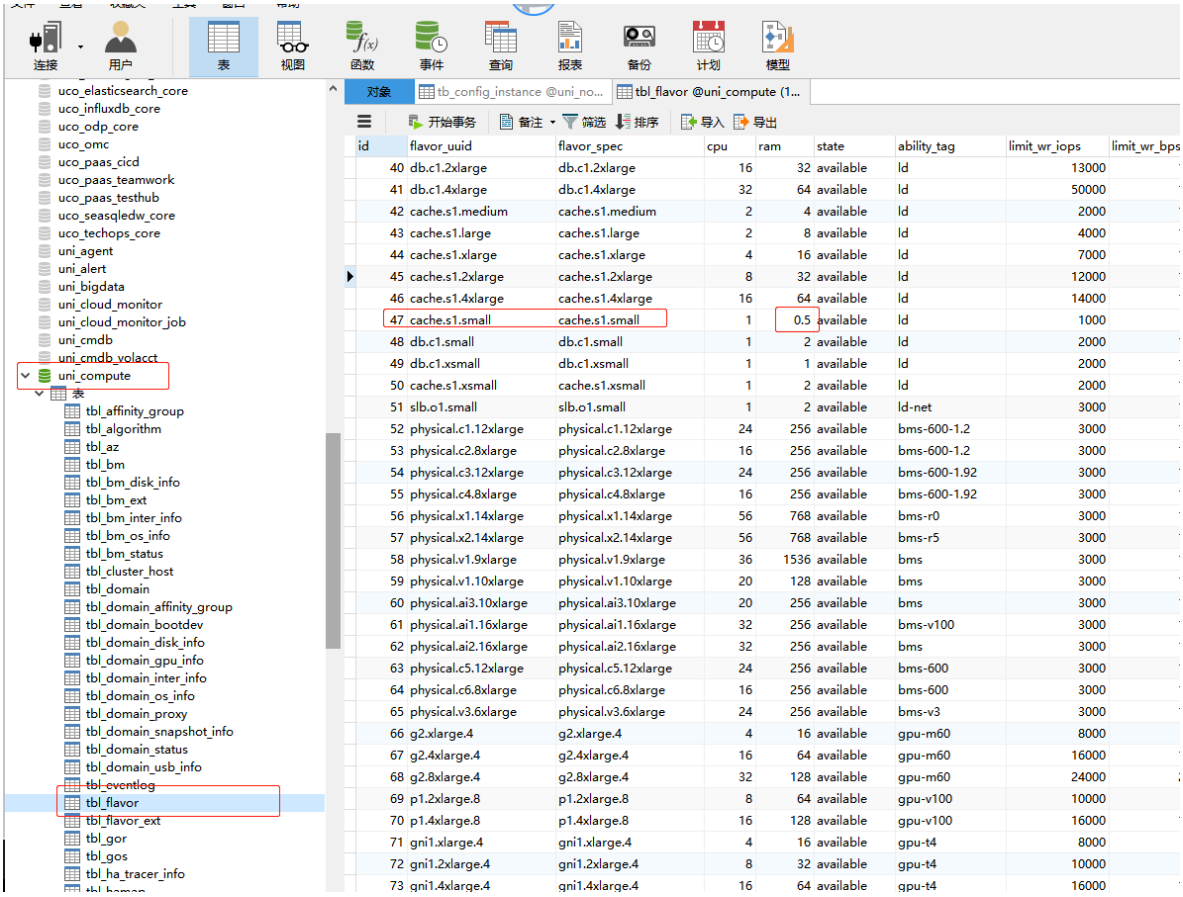
5. 确认系统盘对应的规格编码

本地盘一般使用 ebs.local.ssd，云盘看对应环境的配置。



6. 确认主机 Overlay 下虚拟机内存

cache.s1.small 是 Redis6.0 HA 哨兵节点使用的规格，网络 Overlay 下是 0.5GB，在主机 Overlay 下请改为 1GB。



7.11.3 DBAAS DMS UCA 初始化

1. 上传镜像

上传镜像的方式有两种，您可以选择其中一种：

第一种为参考“6.5 上传镜像”中对应的导入镜像章节，手动导入镜像。

第二种为在 OMC 平台中进行上传。上传方法如下。

(1) 在 OMC 运维管理平台选择[IAAS/基础设施平台]菜单项，进入基础设施平台页面。

(2) 单击左侧导航树[云计算/镜像管理]菜单项，进入镜像管理页面。

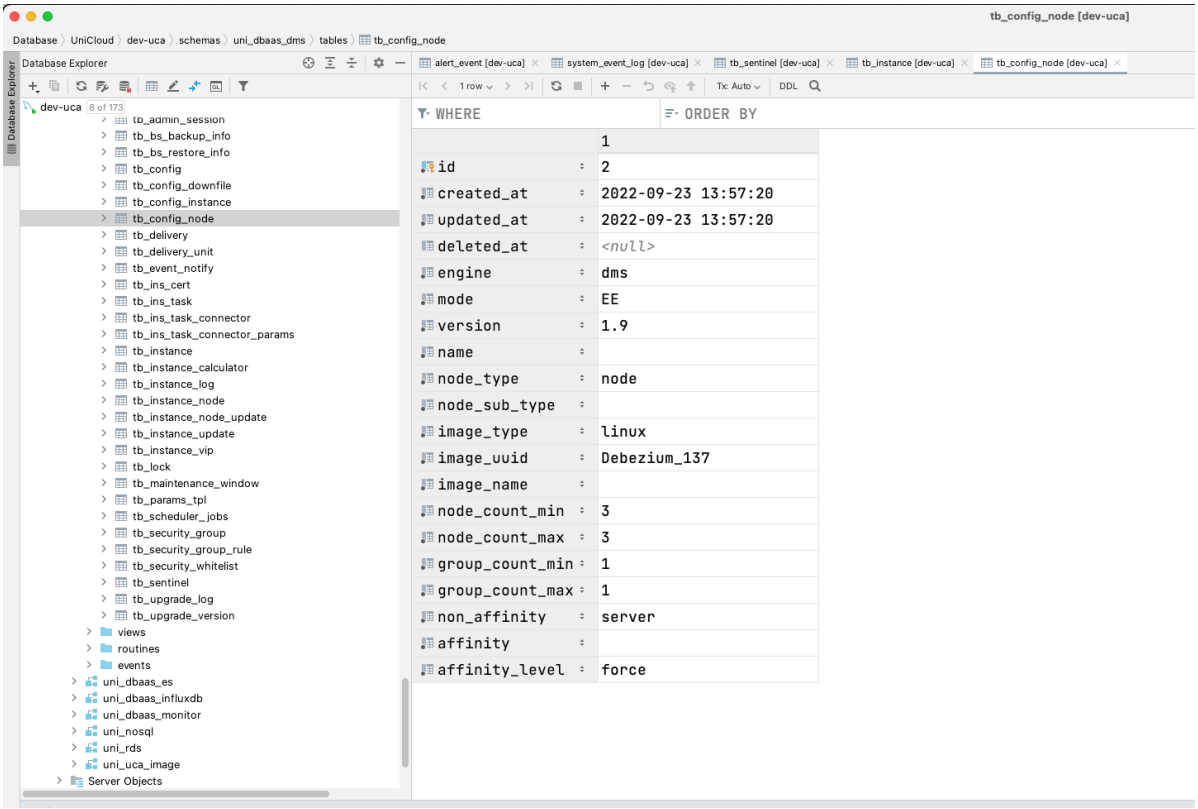
(3) 在公有镜像页签中，单击<上传公有镜像>按钮，进入上传公有镜像页面。

(4) 输入各项属性值，单击<确定>按钮完成操作。

镜像路径、镜像 ID 说明如下。

DMS 镜像：Debezium_161.qcow2

“镜像 ID”字段需要与数据库表 uni_dbaas_dms.tb_config_node 中 dms 对应的 image_uuid 保持一致。



2. 修改云监控相关配置

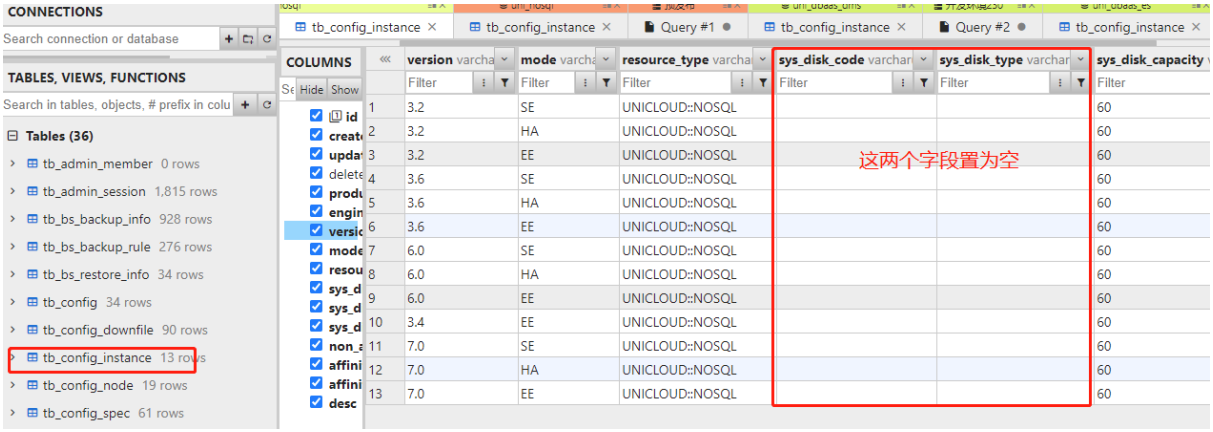
请根据真实环境信息，修改云监控相关的配置。修改【uni_nosql.tb_config，uni_dbaas_es. tb_config，uni_dbaas_influxdb.tb_config】表中的如下信息。

Key 名字	说明
DEFAULT_EGRESS_IPS	安全组出口放行的IP，一般为DMZ区的IP段（因为云监控在DMZ区，实例需要通过业务网向DMZ区的云监控服务推送数据），举例：100.100.12.0/24。
AGENT_UCM_DOMAIN_NAME	云监控服务的域名（IP也支持，参数）

3. 存储双活相关配置

如果项目环境中需要添加存储双活功能，请参考如下步骤进行修改。

Redis 和 MongoDB 产品需要将 uni_nosql.tb_config_instance 的[sys_disk_code]和[sys_disk_type]两个字段的值置为空。如下图所示：



4. 上传 DMS 的 OSS 文件

在 OSS 上创建 NOSQL 依赖文件桶。桶命名为：dbaas-nosql-service-【自定义字】

其中，自定义字段建议使用 Region 的简写，能区分出 Region 即可。

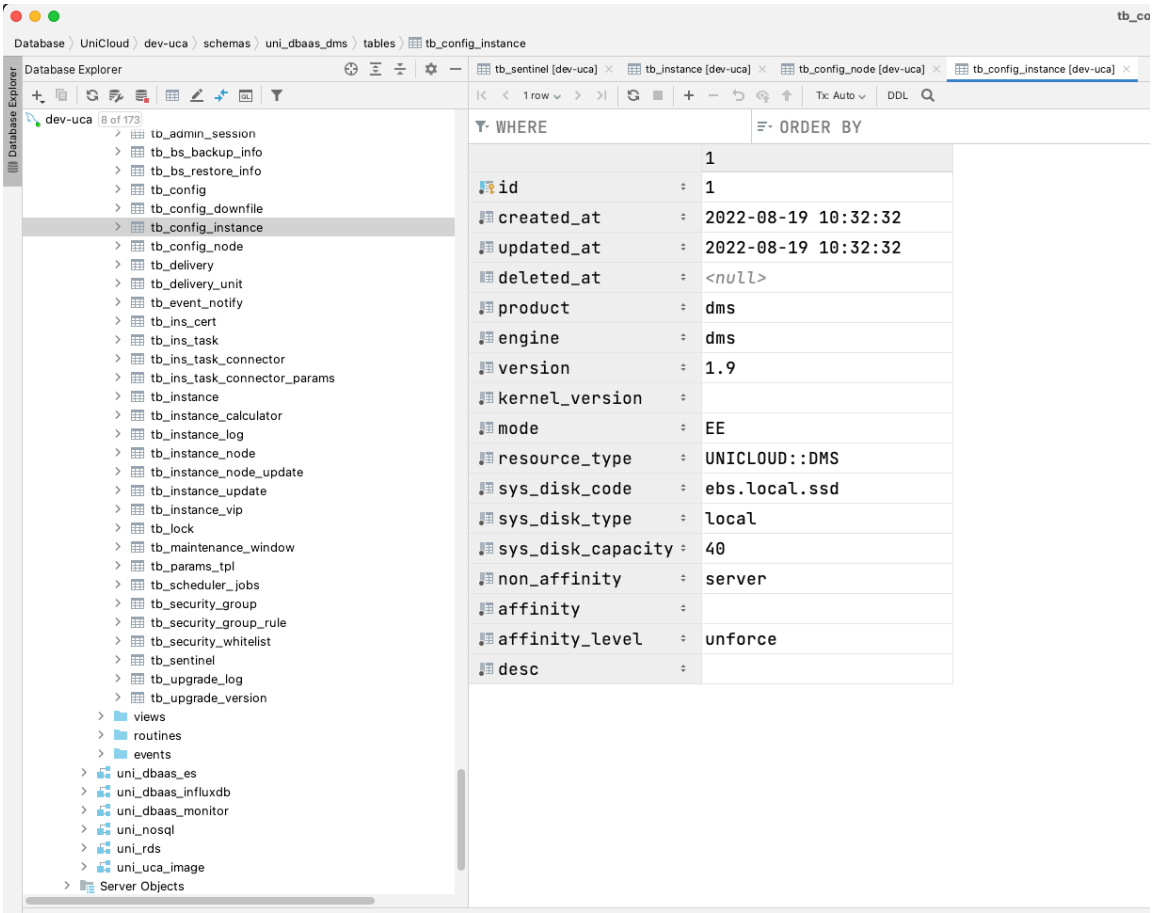
OSS 上创建的桶要与 configmap 中的配置相对应：

- BACKUP_OSS_PATH 为 DMS 的备份桶（保留, 暂时没有用到）
- OSS_BASE 为 DMS 的依赖文件桶（暂时用做日志存储）

将 DMS 的依赖文件（位于 UCA-RDS\oss）上传到 DMS 的依赖文件桶中，依赖文件桶的桶名可以从 configmap 中的 OSS_BASE 字段获取。可以使用 S3 客户端上传，也可以在云控制台使用与 configmap 中 AK、SK 对应的账号登录，在控制台上传。

5. 确认系统盘对应的规格编码

本地盘一般使用 ebs.local.ssd，云盘请查看 A 层数据库 tb_uni_dbaas_dms.tb_config_instance 的配置。

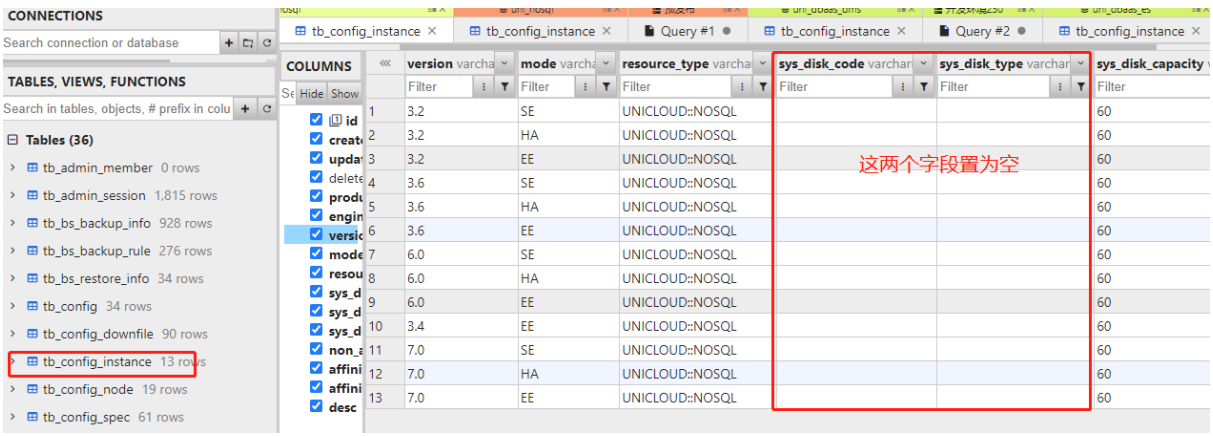


7.11.4 DBAAS ElasticSearch UCA 初始化

1. 存储双活相关配置

如果项目中需要添加存储双活功能，请参考如下步骤进行修改。

ElasticSearch 产品需要将 uni_dbaas_es.tb_config_instance 的[sys_disk_code]和[sys_disk_type]两个字段的值置为空。如下图所示：

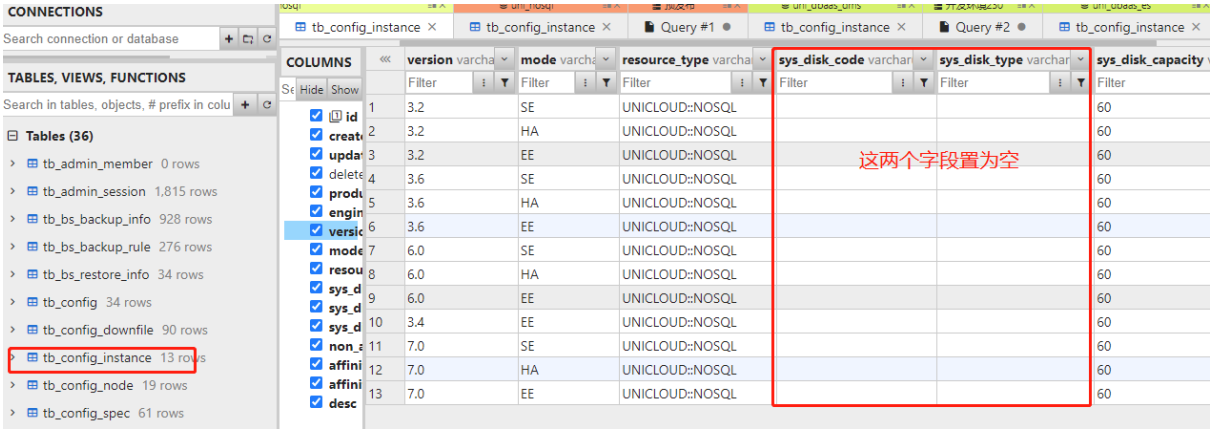


7.11.5 DBAAS InfluxDB UCA 初始化

1. 存储双活相关配置

如果项目中需要添加存储双活功能，请参考如下步骤进行修改。

InfluxDB 产品需要将 uni_dbaas_influxdb.tb_config_instance 的[sys_disk_code]和[sys_disk_type]两个字段的值置为空。如下图所示：



7.12 PaaS平台数据初始化

7.12.1 预置应用管理组件对象存储文件

1. 前置条件

CCR 服务部署完毕。

2. 上传预置文件至 OSS 对象存储

⚠ 注意

应用仓库与 CCR 所使用的对象存储为同一个。

---

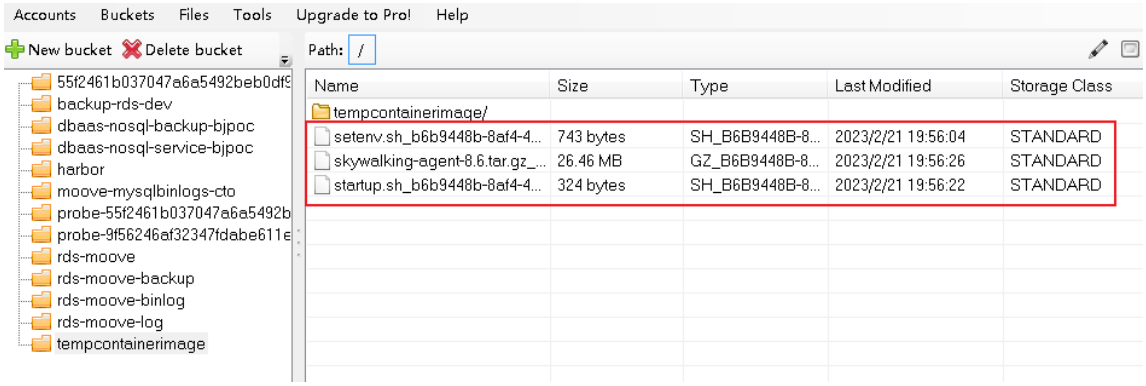
(1) 请从版本发布下获取 PaaS 配套包，路径为：全量包\云服务组件包\PaaS\PaaS-DMZ.zip。压缩文件中包括 EAMS.zip 文件，EAMS.zip 文件中包括后续需要用到的需要预置的数据。

(2) 使用对象存储客户端工具连接至 CCR 所对接的对象存储上。

(3) 连接至对象存储后，可以看到已经存在 tempcontainerimage 桶，将 setenv.sh_b6b9448b-8af4-48a7-a6eb-80598869834c_1614996005730、skywalking-agent-8.6.tar.gz_b6b9448b-8af4-48a7-a6eb-80598869834c_1614996005730、startup.sh_b6b9448b-8af4-48a7-a6eb-80598869834c_1614996005730 文件上传到该桶。这些文件可从[EAMS.zip\需上传至公共对象存储中的文件]中获取。

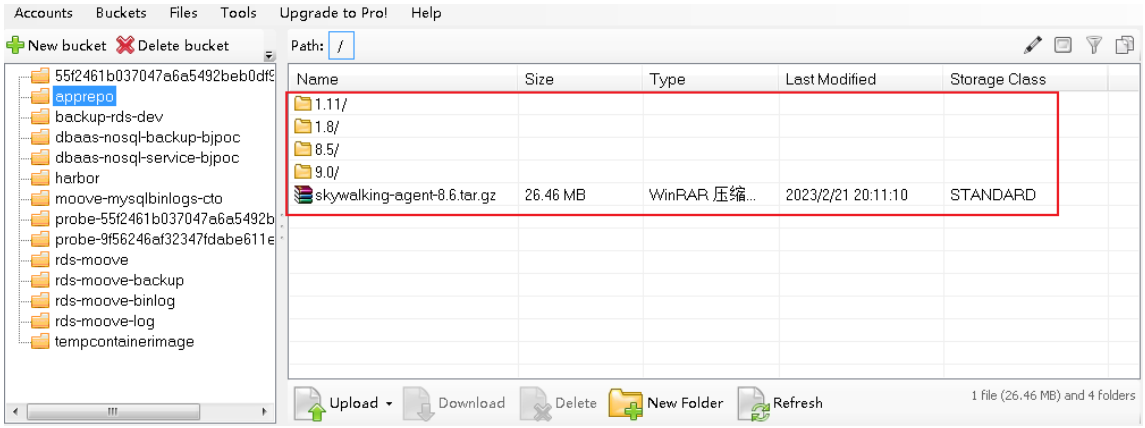
(4) 上传完成后桶内文件如下图所示。注意是 tempcontainerimage 桶，而非 tempcontainerimage 桶内的 tempcontainerimage 目录。

图7-15 tempcontainerimage 桶内文件



(5) 新创建名称为 apprepo 的桶，将 jdk 下的目录和 tomcat 下的目录上传至该桶，然后将 skywalking-agent-8.6.tar.gz 上传至该桶根目录，上传完成后桶内文件如下：

图7-16 apprepo 桶文件

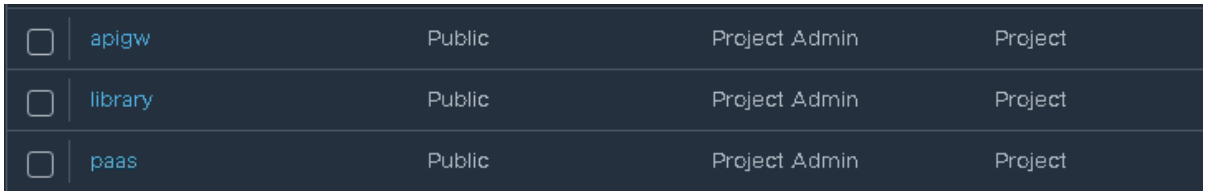


7.12.2 预置 DMZ 区基础镜像

1. 前置条件

CCR 已部署完毕，并且 Harbor 中存在公开项目 library、apigw 和 paas。如图 7-22 所示。

图7-17 Harbor 内项目信息



方法如下。

(1) 登录 Harbor，查看是否存在公开项目。

Harbor 默认地址：http://{DMZ_VIP}:30002，默认用户名 admin，密码 Harbor12345

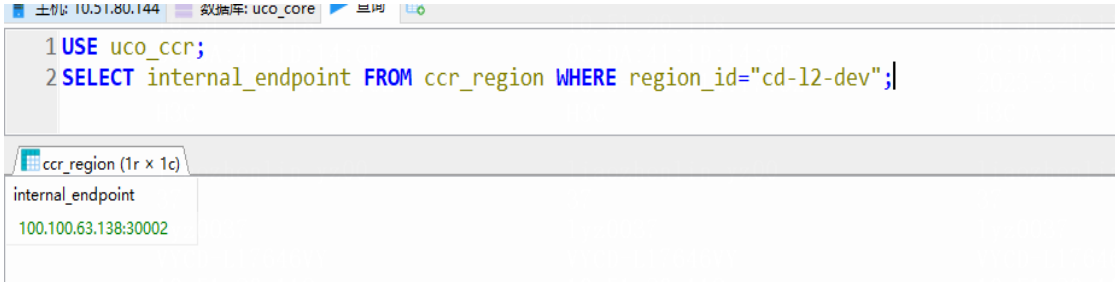
(2) 若不存在公开项目，需新建项目。新建项目时，统一配置为：“访问级别”为公开，其余配置默认值。

2. 上传基础镜像至 CCR 所对应的 Harbor 仓库

(1) 基础镜像包括：应用管理、微服务引擎、服务网关、分布式事务和分布式任务等组件用到的配套基础镜像；配套包一般位于版本发布路径：全量包\云服务组件包\PaaS\PaaS-DMZ.zip 文件，该文件中包含 PaaS-DMZ-BaseIMG.zip 文件，即所需要预置的镜像。

(2) 确定 CCE 租区上拉取 CCR 镜像地址 IP，比如 100.100.63.138（以下步骤(3)用此地址举例）。该地址可从数据库中根据 region_id 值获取：

```
USE uco_ccr;
SELECT internal_endpoint FROM ccr_region WHERE region_id="cd-l2-dev";
```



(3) 确定 A 层相关服务拉取镜像地址参数正确（参考步骤(2)获取的值），若环境变量不正确，则需要手动修改。相关服务、环境变量及示例值如下：

命名空间	组件	环境变量	举例
uca-paas-mse	uca-mse-microservice	IMAGE_REPO	100.100.63.138:30002
default	uca-apigw-engine	DOCKER_REGISTRY	100.100.63.138:30002
default	uca-dts-engine	DOCKER_REGISTRY	100.100.63.138:30002
default	uca-seata-engine	DOCKER_REGISTRY	100.100.63.138:30002

手动修改及验证环境变量步骤：

a. uca-mse-microservice 组件的 IMAGE_REPO：

```
kubectl edit -n uca-paas-mse deployment.apps/uca-mse-microservice
```

```
        successThreshold: 1
        tcpSocket:
          port: 53
        timeoutSeconds: 1
      name: dnsmasq
      ports:
      - containerPort: 53
        name: dns-udp
        protocol: UDP
      - containerPort: 53
        name: dns-tcp
        protocol: TCP
      readinessProbe:
        failureThreshold: 3
        initialDelaySeconds: 30
        periodSeconds: 10
        successThreshold: 1
        tcpSocket:
          port: 53
        timeoutSeconds: 1
      resources: {}
      securityContext:
        capabilities:
          add:
          - NET_ADMIN
      terminationMessagePath: /dev/termination-log
      terminationMessagePolicy: File
      volumeMounts:
      - mountPath: /etc/dnsmasq.d/
        name: config-volume
    - env:
      - name: BUILD_VERSION
        value: 20220715.RC1
      - name: IMAGE_REPO
        value: 100.100.63.138:30002
      - name: LOG_LEVEL
        value: debug
      - name: DELIVERY_ADDR
        value: http://uco-delivery-core.uco.unicloud.space:30990
      - name: CCE_ADDR
        value: http://uca-cce-service.default:40300
      - name: MYSQL_USER
        valueFrom:
          secretKeyRef:
            key: username
            name: mysql-secret
      - name: MYSQL_HOST
        value: 10.51.80.144
      - name: MYSQL_PASSWORD
        valueFrom:
```

步骤（2）中CCR镜像仓库地址

验证生效：

```
[root@cd-dev-uca-k8s-02 ~]# kubectl get pod -n uca-paas-mse | grep uca-mse-microservice
uca-mse-microservice-866bc68455-mrnjk       2/2     Running   0          29m
[root@cd-dev-uca-k8s-02 ~]# kubectl exec -itn uca-paas-mse uca-mse-microservice-866bc68455-mrnjk sh -c uca-mse-microservice
# set | grep IMAGE_REPO
IMAGE_REPO='100.100.63.138:30002'
#
```

b. uca-apigw-engine 组件的 DOCKER_REGISTRY：

```
kubectl edit deployment.apps/uca-apigw-engine
```

```
        - name: DATABASE_HOST
          value: 10.51.80.144
        - name: DATABASE_USER
          valueFrom:
            secretKeyRef:
              key: username
              name: mysql-secret
        - name: DATABASE_PWD
          valueFrom:
            secretKeyRef:
              key: password
              name: mysql-secret
        - name: MOOVE_NETWORK_SLB_URL
          value: http://uca-network-slb-service:40456
        - name: MOOVE_NETWORK_SECURITY_GROUP_URL
          value: http://uca-network-core-basic-service:40466
        - name: CCE_URL
          value: http://uca-cce-service:40300
        - name: UCO_DELIVERY_CENTER_URL
          value: http://uco-delivery-core.uco.unicloud.space:30990
        - name: UCO_TENANT_CORE_URL
          value: http://unicloud-tenant-core.uco.unicloud.space:30990
        - name: KUBERNETES_AUTH_TRYSERVICEACCOUNT
          value: "false"
        - name: DIAG_LOG_LEVEL
          value: info
        - name: SYS_LOG_LEVEL
          value: info
        - name: BUILD_VERSION
          value: E7106-RC2
        - name: DOCKER_REGISTRY
          value: 100.100.63.138:30002
        - name: CHEAT_USE_EMPTYDIR
          value: "true"
```

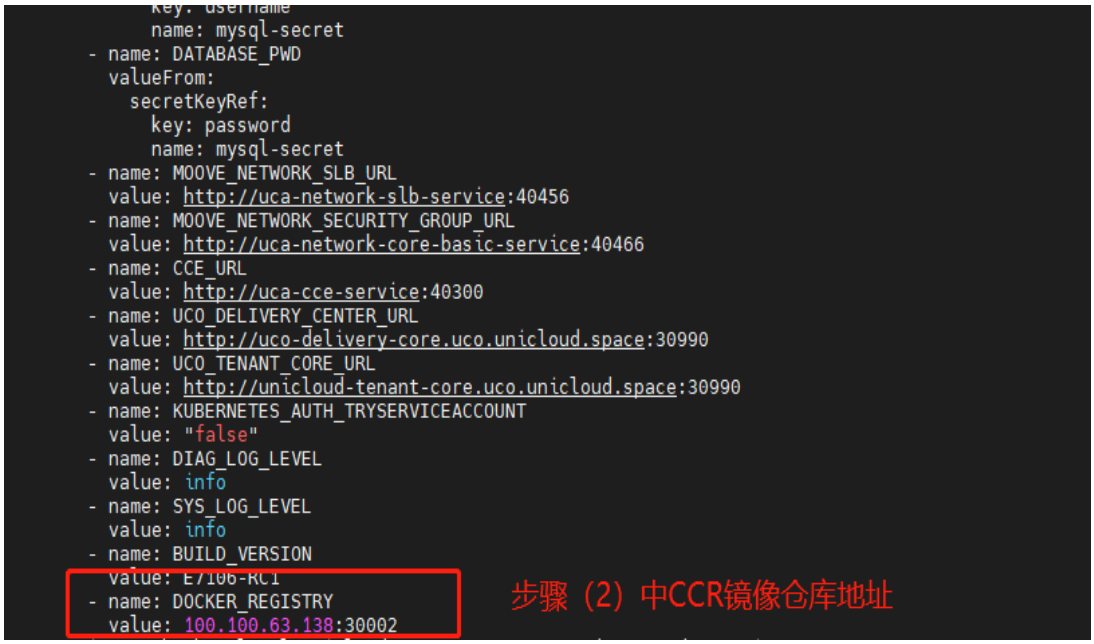
步骤（2）中镜像仓库地址

验证生效：

```
[root@cd-dev-uca-k8s-02 ~]#
[root@cd-dev-uca-k8s-02 ~]# kubectl get pod -A | grep apigw
default          uca-apigw-engine-577459755b-wsq6w                 3/3     Running           0          28h
paas-job-ns      unicloud-harbor-images-apigw-move-k24cq           0/1     Completed         0          28h
paas-job-ns      unicloud-harbor-images-apigw-move-seata-mgx46     0/1     Completed         0          101d
[root@cd-dev-uca-k8s-02 ~]#
[root@cd-dev-uca-k8s-02 ~]# kubectl exec -itn default         uca-apigw-engine-577459755b-wsq6w sh -c engine
# set | grep DOCKER_REGISTRY
DOCKER_REGISTRY='100.100.63.138:30002'
#
```

c. uca-dts-engine 组件的 DOCKER_REGISTRY：

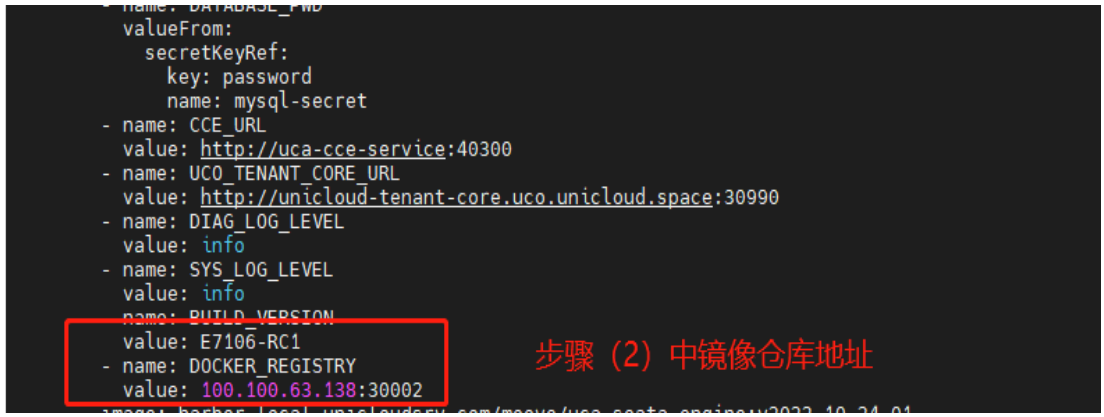
```
kubectl edit deployment.apps/uca-dts-engine
```



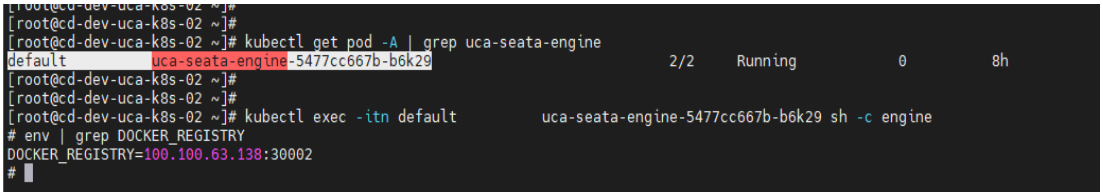
验证生效：

d. uca-seata-engine 组件的 DOCKER_REGISTRY：

```
kubectl edit deploy/uca-seata-engine
```



验证生效：



(4) 参考配套包中 README.txt 描述执行脚本将基础镜像上传到 Harbor 仓库。

将 PaaS-DMZ-BaseIMG.zip 上传到安装 DMZ 区 docker 的主机上并解压，该主机需到上述的 harbor 仓库网络可达，可以使用 DMZ K8S 集群的节点上传。脚本参数为 CCR Harbor 地址。

执行前，请为执行脚本 ccr-images-tools.sh 添加执行权限。

```
[root@AUTOPS-DMZ-K8S-01 ~]# cd PaaS-DMZ-BaseIMG/
[root@AUTOPS-DMZ-K8S-01 PaaS-DMZ-BaseIMG]# ll
total 16
drwxr-xr-x 2 root root  146 Oct 10 11:08 apigw
-rw-r--r-- 1 root root 9360 Oct 10 11:09 ccr-images-tools.sh
drwxr-xr-x 2 root root   47 Oct 10 11:09 dts
drwxr-xr-x 2 root root  209 Oct 10 11:12 eams
drwxr-xr-x 2 root root  258 Oct 10 11:19 mse
-rw-r--r-- 1 root root  430 Oct 10 11:22 README.txt
drwxr-xr-x 2 root root   49 Oct 10 11:22 seata
drwxr-xr-x 2 root root   83 Oct 10 11:24 techops
[root@AUTOPS-DMZ-K8S-01 PaaS-DMZ-BaseIMG]# chmod 755 ccr-images-tools.sh
[root@AUTOPS-DMZ-K8S-01 PaaS-DMZ-BaseIMG]# ./ccr-images-tools.sh 100.66.1.110:30002
+ echo 'CCR Harbor: 100.66.1.110:30002'
CCR Harbor: 100.66.1.110:30002
+ docker login 100.66.1.110:30002 -u admin -p Harbor12345
WARNING! Using --password via the CLI is insecure. Use --password-stdin.
WARNING! Your password will be stored unencrypted in /root/.docker/config.json.
Configure a credential helper to remove this warning. See
https://docs.docker.com/engine/reference/commandline/login/#credentials-store

Login Succeeded
+ echo '****************** starting to process apigw docker images ******************'
****************** starting to process apigw docker images ******************
+ docker load -i ./apigw/apimgt-E7106-RC2.tar
51a4bedddf27: Loading layer [==================================================>]  2.048kB/2.048kB
97836976d878: Loading layer [==================================================>]  71.62MB/71.62MB
731864c0424e: Loading layer [==================================================>]  4.608kB/4.608kB
0c073816828c: Loading layer [==================================================>]  3.072kB/3.072kB
cb9c9c392045: Loading layer [==================================================>]  3.072kB/3.072kB
Loaded image: harbor-local.unicloudsrv.com/moove/apigw/apimgt:E7106-RC2
+ docker load -i ./apigw/initpostgres-E7106-RC2.tar
```

7.12.3 项目协作组件

1. 前置条件

由于 DevOps 项目协作采用服务魔方架构，部署在 S 层的 CCE 集群中，享有独有的虚拟专有云 VPC 网络。此外，DevOps 项目协作还依赖 MySQL、Redis、RabbitMQ、Elasticsearch、弹性公网 IP、负载均衡等服务，且都需要在同一个 VPC 和地域下面开通。由于 DevOps 中交付业务还依赖于应用仓库、应用管理、镜像仓库服务，因此这三个云服务也需要保证在该地域下可用。

2. 创建虚拟专有云 VPC

(1) 登录产品控制台，在左侧导航栏选中选择[网络/虚拟专有云]，进入虚拟专有云页面。

(2) 点击<申请虚拟专有云>按钮，输入所需参数，创建虚拟专有云。

注意网段和子网的分配和地域的选择与实际环境一致。

(3) 申请成功后，查看子网信息是否正确。

3. 开通云容器引擎 CCE

(1) 登录产品控制台，在左侧导航栏选择[计算/云容器引擎]，进入云容器引擎页面。

(2) 点击<创建>按钮进行创建。

注意地域需要与 VPC 的地域相同，并且需要选择 VPC 中创建的专有网络及子网。

(3) 创建完成后，进入集群详情页面，选择[使用 Kubectl 连接集群]页签，打开访问方式中的内网。

4. 开通 MySQL

(1) 登录产品控制台，在左侧导航栏选择[数据库/MySQL 云数据库]，进入 RDS 云数据库页面，点击<新建>按钮进行新建。

注意地域需要与 VPC 的地域相同，并且需要选择 VPC 中创建的专有网络及子网，MySQL 版本只能选择 5.7。

(2) 进入创建成功的 MySQL 实例，选择白名单页面，给选择的子网配置白名单。

(3) 进入创建成功的 MySQL 实例，进入参数设置页面，检查 MySQL 的参数 sql_mode,如果有 only_full_group_by，请移除此设置，移除后点击提交参数。

5. 开通 Redis

(1) 登录产品控制台，在左侧导航栏选择[数据库/Redis 云数据库]，进入 Redis 云数据库页面，点击<新建>按钮进行新建。

注意地域需要与 VPC 的地域相同，并且需要选择 VPC 中创建的专有网络及子网。

(2) 进入创建成功的 Redis 实例，选择白名单页面，给选择的子网配置白名单。

6. 开通 RabbitMQ

(1) 登录产品控制台，在左侧导航栏选择[中间件/RabbitMQ]，进入消息队列 RabbitMQ 页面，点击<新建>按钮进行新建。

注意地域需要与 VPC 的地域相同，并且需要选择 VPC 中创建的专有网络及子网。

(2) 进入创建成功的 RabbitMQ 实例，选择白名单页面，给选择的子网配置白名单。

(3) 在 RabbitMQ 实例下，创建一个/devops 的 vhost。

7. 开通 ElasticSearch

(1) 登录产品控制台,在左侧导航栏选择[中间件/ElasticSearch],进入云搜索 ElasticSearch 页面，点击<新建>按钮进行新建。

注意地域需要与 VPC 的地域相同，并且需要选择 VPC 中创建的专有网络及子网。

(2) 进入创建成功的 ES 实例，选择白名单页面，给选择的子网配置白名单。

8. 开通弹性公网 IP

(1) 登录产品控制台，在左侧导航栏选择[网络/弹性公网 IP]，进入弹性公网 IP 列表页面，点击<新建>按钮进行新建，生成公网 EIP。

注意地域需要与 VPC 的地域相同。

9. 配置服务魔方

(1) 登录产品控制台，在左侧导航栏选择[服务魔方控制台]，进入扩展服务页面，点击<创建扩展服务>按钮进行新建。

服务名称和服务编码可以都填写 devops。创建 devops 扩展服务成功之后，点击进入 devops 扩展服务。

(2) 点击<服务授权>按钮，选择配置权限。配置完成后点击<确定>按钮，并在列表页面点击<启用>按钮。

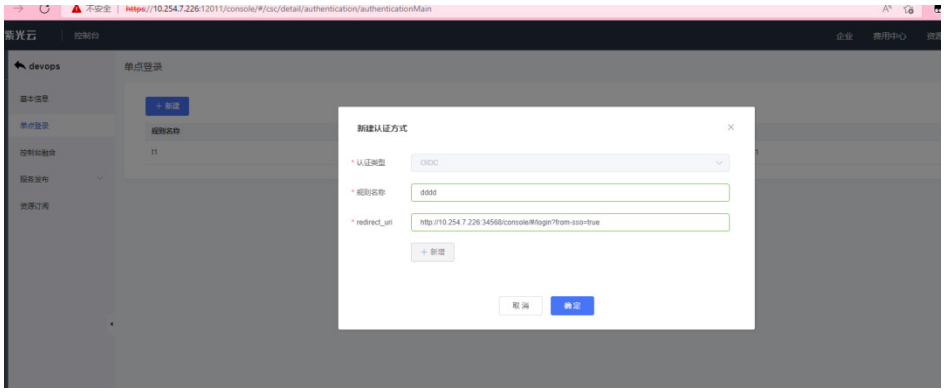
名称根据需要填写即可，比如 devops-oidc。

选择“OAuth 2.0 服务 OpenID 身份认证权限”。

(3) 在 devops 导航栏选择[单点登录]，进入单点登录页面，点击<新建>按钮进行新建。

规则名称根据需要填写即可，比如 devops。

redirect_uri 填写格式如下：http://{ip}:31160/console/#/ssoLogin 其中 IP 地址填写申请的弹性公网 IP。



(4) 在 devops 导航栏选择[控制台融合]，选择[新建接入方式/独立控制台]，进行配置。

- 产品分类：可以选择企业应用；
- 产品名称：填写项目协作；
- 产品 URL：填写 http://{ip}:31160/api/v1.0/login?from-sso=true。其中 IP 地址填写申请的弹性公网 IP。

(5) 在 devops 导航栏选择[资源订阅]，点击<新建>按钮进行新建。

勾选详情如图所示，回调地址填写 http://{ip}:{{port}}/api/v1.0/mate?Action=WebhookZiLuanUserInfo 其中 IP 地址填写服务魔方 Nginx 的 IP，port 是代理 devops 31160 的端口。（也可以直接填申请的弹性公网 EIP：31160）

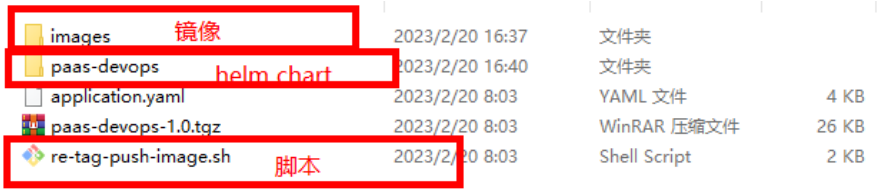
(6) 登录运营控制台（12008 端口），在[应用创新->服务魔方->控制台注册审核]，审批申请的控制台。

(7) 登录运营控制台（12008 端口），在[应用创新->服务魔方->资源订阅审核]，审批申请的资源订阅。

(8) 登录运营控制台（12008 端口），在[应用创新->服务魔方->扩展服务汇总->devops 服务->配置 License]，选中 DEVOPS 后缀结尾的授权编码填 CloudDEVOPS，选中 DEVOPS-PER-10 后缀结尾的授权编码填 CloudDEVOPS-PER-Count，再点击确定。之后将会在[用户控制台->服务魔方->扩展服务管理->devops->服务审计]下会生成一个 License 授权的菜单栏。

10. 上传配套镜像至 Harbor 仓库

(1) 解压提供的 DevOps 整包（请从版本发布路径下获取：全量包\云服务组件包\PaaS\paas-devops-V*XXXX*.zip），并再次解压 paas-devops-1.0 包到当前文件包，解压之后目录如下。



(2) 登录用户控制台，在左侧导航栏选择[容器镜像仓库]，进入镜像仓库页面，新建 devops 项目。

(3) 点击容器镜像仓库中的访问凭证页面，登录镜像仓库实例的 endpoint 即为镜像要上传的 Harbor 仓库地址。

(4) 登录到 DMZ 区任一节点之上，拷贝 images 镜像目录和 re-tag-push-image.sh 脚本到服务器上；并在该节点上登录上一步的 harbor 仓库地址。

(5) 运行 re-tag-push-image.sh 脚本，传递三个参数，分别为镜像目录的路径、镜像的 tag、不带 http://的 harbor 仓库地址。样例：./re-tag-push-image.sh ./images xxx xxx

(6) 登录 CCE 集群，分别在每个 Node 节点上登录上述的 harbor 仓库。

11. 部署 DevOps 项目协作

(1) 登录到租管互通 TAAG 区任意节点，新建一个 devops 目录，并将“10. 上传配套镜像至 Harbor 仓库”中解压的 paas-devops 目录拷贝到 devops 目录下，并在 devops 目录下新建一个 devops-cce-kubeconfig 文件。

(2) 登录产品控制台，进入“3. 开通云容器引擎 CCE”中创建的 CCE 集群，进入[使用 Kubectl 连接集群]页面，拷贝 Kubeconfig 的内容到上述新建的 devops-cce-kubeconfig 文件中。

(3) 在节点的/etc/hosts 文件里面加上 CCE 集群域名和 VIP 的映射关系，在文本最后添加一行“$CCE_IP 域名”。（其中 CCE 集群的 IP 填 100 开始的 IP）

(4) 登录产品控制台，在左侧导航栏中选择[服务魔方控制台]，进入[扩展服务]页面，找到 devops 的扩展服务实例，点击进入详情，选择[单点登录]，再选择[详情]。

(5) 打开 devops/paas-devops/values.yaml 文件，并依次修改下述的值。

除下列字段外的其他字段值可以不修改。

a. config.cronjobVersion：若 cce 集群的 k8s 版本大于 1.21 填 batch/v1，否则填 batch/v1beta1。

b. config.release：忽略。

c. config.dockerRegistry：其中 value 填写“容器镜像仓库--->访问凭证-→登录实例中的 endpoint，不带 http:// ”；username 和 password 分别填写镜像仓库的用户名和密码，admin 和 Harbor12345 是部署时默认的超管用户名和密码。

d. config.EAMS_APPMGMT_ENDPOINT：忽略，不用修改。

e. config.EAMS_APPSTORE_ENDPOINT：忽略，不用修改。

f. config.CCR_ENDPOINT：忽略，不用修改。

g. config.REGISTRY_ENDPOINT：同 config.dockerRegistry。

h. config.REGISTRY_EXTERNALENDPOINT：填写 config.dockerRegistry 的外部地址。

i. config.enterpriseApp：填 true。

j. config.version：填 csc。

k. config.userSourcePlat：填 csc。

l. config.regionId：填创建 VPC 等资源选择地域对应的 id。

m. config.CLUSTER_EXTERNAL_ENDPOINT：填写申请的弹性公网 EIP。

n. moduleConf.inputs.s3：填写同 CCR 使用的公用的对象存储信息，当 enpoin 本身就是 ip 时，ip 值则不填。

o. moduleConf.inputs.mysql*：根据创建的 mysql 实例填写。

p. moduleConf.inputs.redis*：根据创建的 redis 实例填写。

q. moduleConf.inputs.mq*：根据创建的 mq 实例填写。其中 mqManagePort 是 MQ 的管理端口默认就是 15672，注意和 mqPort 默认是 5672 区分开来。

r. moduleConf.inputs.elasticsearch：根据创建的 es 实例填写。其中 endpoint 填写 ip 和端口，用户名和密码分别对应 username 和 password，当有用户名和密码时，auth 填”true”（注意是引号引起来的字符串”true”）。

s. moduleConf.inputs.checkLicense：填 true。

t. moduleConf.inputs.openAPI：https://云平台 Nginx 的 VIP:30990

u. moduleConf.inputs.cscSecretID：用户的 ak。（登录用户控制台，右上角用户，访问密钥）

v. moduleConf.inputs.cscSecretKey：用户的 sk。

w. moduleConf.inputs.ziLuanAuthURI：复制单点登录详情基本信息中的 auth_url，若云平台入口为 https，并将 http 修改为 https，将 IP 替换成云平台 Nginx 的 EIP。

x. moduleConf.inputs.ziLuanRedirectURI：复制单点登录详情基本信息中的 redirect_uri，并将#替换成%23。

y. moduleConf.inputs.ziLuanClientID：复制单点登录详情基本信息中的 client_id。

z. moduleConf.inputs.ziLuanClientSecret：复制单点登录详情基本信息中的 client_secret。

aa. moduleConf.inputs.ziLuanResponseType：忽略，不用修改。

bb. moduleConf.inputs.ziLuanUserInfoURL：复制单点登录详情基本信息中的 user_info_url，若云平台入口为 https，并将 http 修改为 https，将 IP 替换成云平台 Nginx 的 VIP。

cc. moduleConf.inputs.ziLuanState：忽略，不用修改。

dd. moduleConf.inputs.ziLuanScope：忽略，不用修改。

ee. moduleConf.inputs.ziLuanAccessTokenURI：复制单点登录详情基本信息中的 access_token_url，若云平台入口为 https，并将 http 修改为 https，将 IP 替换成云平台 Nginx 的 VIP。

ff. moduleConf.inputs.ziLuanDefaultPassword：忽略，不用修改。

(6) 在 devops/paas-devops 目录执行 helm template . > devops-deploy.yaml

(7) 部署服务 kubectl apply –f devops-deploy.yaml --kubeconfig ../devops-cce-kubeconfig。若为升级时，执行报错为 cicd-initdatabase 这个 Job 执行失败，并不影响升级的实际的成功与否，可以忽略这个错误。

(8) 查看 pod 的用户状态 kubectl pod --all-namespaces --kubeconfig ../devops-cce-kubeconfig |grep devops

(9) 查看 CCE 集群的节点信息 kubectl get node --kubeconfig ../devops-cce-kubeconfig

(10) 分别给给个节点打标签 kubectl label node xxx build-worker=kubernetes --kubeconfig ../devops-cce-kubeconfig。

12. 绑定负载均衡

(1) 登录产品控制台，在左侧导航栏中选择[计算/云容器引擎]，进入集群列表页面。

(2) 进入上述创建的 CCE 集群，选择“服务管理”中的 Service，在“命令空间”的下拉选框中选择包含 devops 的命名空间，编辑包含 devops-ui-nginx-service 的服务名：

- 将“访问类型”由 NodePort 修改为 LoadBalancer；
- 负载均衡类型选择普通；
- 高级设置 externalTrafficPolicy 选择 Cluster。

(3) 点击<确定>按钮，等待对应的生成负载均衡生成成功。

(4) 登录产品控制台，在左侧导航栏中选择[网络/负载均衡]，进入负载均衡列表页面。

(5) 在负载均衡列表页面，选中生成的包含 devops-ui-nginx-service-cce 的负载均衡实例，并绑定上述开通生成的弹性公网 IP。

13. 离线导入用户数据

登录云平台 mysql, tenant_core 数据库，导出用户信息。

将用户的 uuid、name、fullname 插入到上述创建的 MySQL 云服务实例的 teamwork_mate database 的 csc_user_info 表中，其中 is_occupied 字段默认都填 0，created_at 填当前时间。

7.12.4 补丁包部署

如果当前版本存在补丁包，请按照如下步骤进行部署；若不存在补丁包，则不需要执行该章节中的步骤。

1. 前置条件

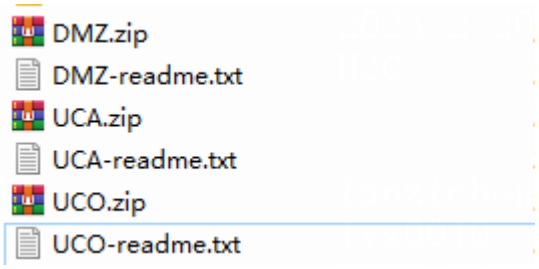
PaaS 云服务已正常安装成功。

2. 补丁包部署

(1) 获取 PaaS 配套云服务补丁包，一般位于：云服务组件包\PaaS\PaaS-Patch.zip 文件。

(2) 参考该 Patch 文件中不同 Region 的 Readme 文件，执行对应操作。

例如：解压补丁包后，解压后的文件夹包括 UCA、UCO 和 DMZ 补丁（实际补丁个数以具体版本补丁包为准）；



以 A 层为例，将 UCA.zip 包上传至 UCA 集群中的任一控制节点（其它文件同理，例如 UCO.zip 即上传至 UCO 层），解压此文件，然后进入 UCA 目录，运行命令"sh PaaS-UCA-PATCH.sh"等待脚本执行完成。

需要注意，执行的脚本若没有执行权限，则需要添加执行权限。

7.12.5 配置校验

当利用部署工具进行部署或升级时，若环境变量填写有误，可能导致业务功能有问题。此时可对比此章节进行检查必要的变量是否正确。

1. 环境变量

通用查看服务环境变量的步骤及方式：

(1) 连接对应的环境，例如 UCO 层:ssh root@ip;

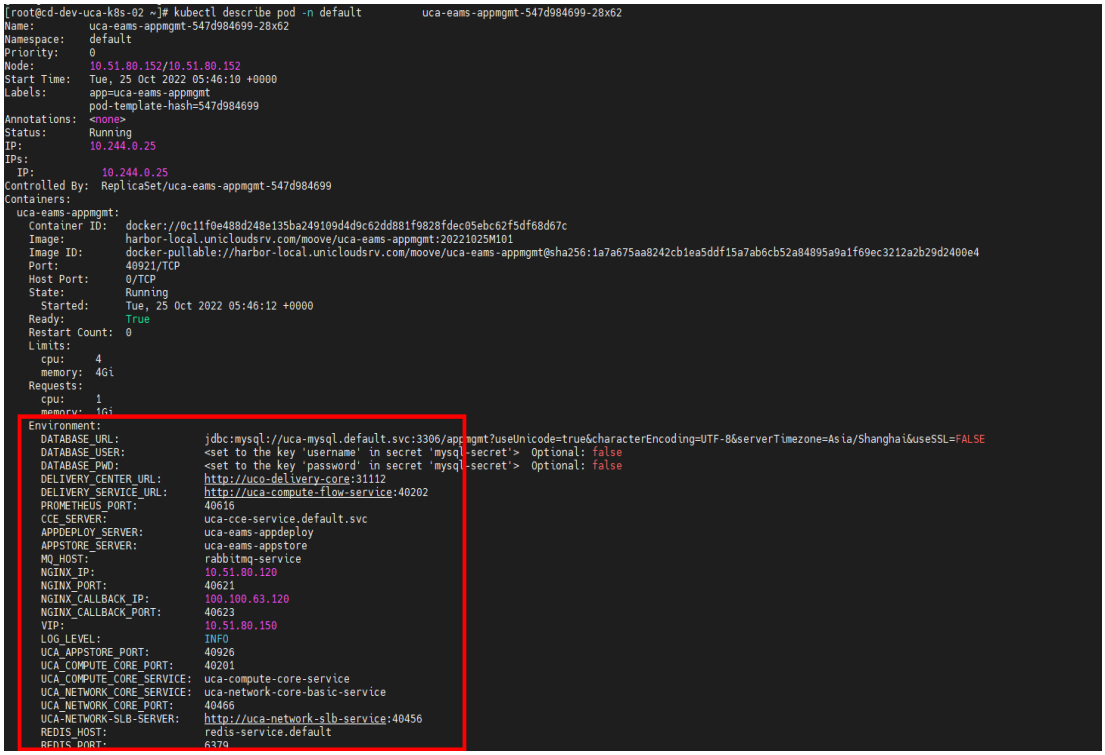
(2) 根据表格中的“服务”列的名称获取对应的服务，例如：

```
kubectl get pod -A |grep uco-eams-appmgmt
```

```
[root@cd-dev-uca-k8s-02 ~]# kubectl get pod -A |grep uca-eams-appmgmt
default          uca-eams-appmgmt-547d984699-28x62                        2/2     Running          0          26h
[root@cd-dev-uca-k8s-02 ~]#
```

(3) 根据上一步返回结果，填充变量：

```
kubectl describe pod -n xxx xxx
```



(4) 根据表格信息，检查对应环境变量是否正确。

UCO 层环境变量表格信息：

服务	环境变量 Key	环境变量 Value 示例	含义	获取方式
uco-eams-appmgmt	DMZ_BODHI_ADDR	10.51.80.135:40925	DMZ区bodhi服务的访问方式	由DMZ地址+端口拼接而成。DMZ地址一般由环境规划文档获取。
uco-eams-orch-core	UCO_VIP	10.51.80.5	uco层的VIP	由环境规划文档获取。关键词“UCO”。

UCA 层环境变量表格信息：

服务	环境变量 Key	环境变量 Value 示例	含义	获取方式
uca-eams-appalert	VM_PROMETHEUS_URL	http://10.51.80.124:9090	获取虚拟机的Prometheus的地址信息	由协议+平台Prometheus地址+端口拼接而成。 平台Prometheus地址由环境规划文档获取。
uca-apigw-engine	NGINX_URL	http://10.253.146.20:40621	租管互通区，组件的nginx service访问地址	由协议+租管互通的管理VIP+端口拼接而成。 租管互通的管理VIP，由环境规划文档获取TAAG层的管理VIP。关键词“租管互通”或“TAAG”。

服务	环境变量 Key	环境变量 Value 示例	含义	获取方式
uca-dts-engine	NGINX_URL	http://10.253.146.20:40621	租管互通区，组件的nginx service访问地址	由协议+租管互通的管理VIP+端口拼接而成。 租管互通的管理VIP，由环境规划文档获取TAAG层的管理VIP。 关键词“租管互通”或“TAAG”。
uca-eams-appdeploy	NGINX_IP	10.51.80.120	租管互通的管理VIP	由环境规划文档获取TAAG层的管理VIP。 关键词“租管互通”或“TAAG”。
	NGINX_CALLBACK_IP	100.100.63.120	租管互通的业务VIP	由环境规划文档获取TAAG层的业务VIP。 关键词“租管互通”或“TAAG”。
	VIP	10.51.80.150	UCA层VIP地址	由环境规划文档获取。关键词“UCA”。
	OSS_SERVER	http://10.51.80.200:9000 或http://s3.test.com	该字段为应用管理所依赖的DMZ区对象存储的地址，需要与DMZ区的镜像仓库harbor使用同一对象存储服务器。 该地址供管理区A层使用，需要保证A层服务可以通该域名或ip。若是IP，一般需要采取oss可以在管区通的**管区IP**。	由协议+域名（或IP）+端口组成。 对象存储的管理IP。 均由环境规划文档获取。关键词“OSS”或“对象存储”。
	OSS_SERVER_DMZ	http://100.100.63.115:9000 或http://s3.test.com	该字段为应用管理所依赖的DMZ区对象存储的地址，需要与DMZ区的镜像仓库harbor使用同一对象存储服务器。 该地址供业务层S层虚拟机下载文件使用，需要保证S层可以通该域名或ip；若是IP，需要采取oss可以在S层连通的**DMZ区IP**。	由协议+域名（或IP）+端口组成。 对象存储的DMZ层IP。 均由环境规划文档获取。关键词“OSS”或“对象存储”。
	OSS_PROXY_ENDPOINT	10.51.80.160:8082	常规情况下不使用。某些特殊情况下O层搭建的Proxy地址。	由O层地址+端口拼接而成。O层地址由环境规划文档获取。
	OSS_AK	5W3ZGC5C1AI48ZDF8KFB	版本环境配套OSS	由环境规划文档获取。关键词

服务	环境变量 Key	环境变量 Value 示例	含义	获取方式
			的通用AK	“AK”。
	OSS_SK	ZlzXXWTyQBfXe4q7NTkedBWokNt3QtKQZTGUmHXh	版本环境配套OSS的通用SK	由环境规划文档获取。关键词“SK”。
	IMAGE_LOADER_SERVER	10.51.80.135	DMZ区image-loader服务的访问地址，一般填写dmz区地址即可	由环境规划文档获取DMZ区的VIP地址信息。关键词“DMZ”。
	HARBOR_SERVER	10.51.80.135	DMZ区Harbor服务的访问地址，一般填写dmz区地址即可	由环境规划文档获取DMZ区的VIP地址信息。关键词“DMZ”。
	DMZ_EAMS_BODHI_SERVICE	10.51.80.135	DMZ区Bodhi服务的访问地址，一般填写dmz区地址即可	由环境规划文档获取DMZ区的VIP地址信息。关键词“DMZ”。
uca-eams-appmgmt	NGINX_IP	10.51.80.120	租管互通的管理VIP	由环境规划文档获取TAAG层的管理VIP。 关键词“租管互通”或“TAAG”。
	NGINX_CALLBACK_IP	100.100.63.120	租管互通的业务VIP	由环境规划文档获取TAAG层的业务VIP。 关键词“租管互通”或“TAAG”。
	VIP	10.51.80.150	UCA层VIP地址	由环境规划文档获取UCA层的业务VIP。 关键词“UCA”。
	DMZ_EAMS_BODHI_SERVICE	10.51.80.135	DMZ区Bodhi服务的访问地址，一般填写dmz区地址即可	由环境规划文档获取DMZ区的VIP地址信息。关键词“DMZ”。
uca-eams-appstore	VIP	10.51.80.150	UCA层VIP地址	由环境规划文档获取UCA层的业务VIP。 关键词“UCA”。
	OSS_ENDPOINT	https://10.51.80.200:9000	该字段为应用管理所依赖的DMZ区对象存储的地址，需要与DMZ区的镜像仓库harbor使用同一对象存储服务器。 该地址供用户控制台上传文件使用，故需要根据环境情况携带协议前缀，与**用户控制台协议相同**。 例如平台12011界面端口访问若是采取https，则需要https://xxx。若是IP，一般需要采取oss可以在管区通的**管区**	由协议+域名（或IP）+端口组成。 **协议需要与用户控制台协议相同。** 其它均由环境规划文档获取。 关键词“OSS”或“对象存储”。

服务	环境变量 Key	环境变量 Value 示例	含义	获取方式
			IP。	
	OSS_PROXY_ENDPOINT	10.51.80.160:8082	常规情况下不使用。某些特殊情况下O层搭建的Proxy地址。	由O层地址+端口拼接而成。O层地址由环境规划文档获取。
	OSS_AK	5W3ZGC5C1AI48ZDF8KFB	版本环境配套OSS的通用AK	由环境规划文档获取。关键词“AK”。
	OSS_SK	ZlzXXWTyQBfXe4q7NTkedBWokNt3QtKQZTGUmHXh	版本环境配套OSS的通用SK	由环境规划文档获取。关键词“SK”。
	OSS_SERVER	http://10.51.80.200:9000	该字段为应用管理所依赖的DMZ区对象存储的地址，需要与DMZ区的镜像仓库harbor使用同一对象存储服务器。 该地址供管理区A层使用，需要保证A层服务可以通该域名或ip。若是IP，一般需要采取oss可以在管区通的**管区IP**。	由协议+域名（或IP）+端口组成。 对象存储的管理IP。 均由环境规划文档获取。关键词“OSS”或“对象存储”。
uca-eams-appsync	NGINX_ENDPOINT	10.51.80.120:40621	租管互通区Dbaas的nginx的Service访问地址	由环境规划文档获取TAAG层的管理VIP+端口拼接组成。 关键词“租管互通”或“TAAG”。
	BODHI_ENDPOINT	10.51.80.135:40925	DMZ区Bodhi服务的访问地址，需要携带端口信息	由环境规划文档获取DMZ区的VIP地址+端口拼接组成。 关键词“DMZ”。

DMZ 区环境变量表格信息：

服务	环境变量 Key	环境变量 Value 示例	含义	获取方式

服务	环境变量 Key	环境变量 Value 示例	含义	获取方式
dmz-eams-bodhi	BODHI_DB_URL	**root**:**unic-moove**@tcp(**10.51.93.15**:**3306**)/bodhi?charset=utf8&parseTime=True&loc=Local	DMZ区搭建的PaaS底座所提供的mysql连接地址，主要关心其中用户名/密码/服务地址/端口四项。如示例中加粗地方所示。	由环境规划文档获取用户名/密码/服务地址/端口四项。 关键词“PaaS底座”。
	BODHI_REDIS_HOST	10.51.93.15	DMZ区搭建的PaaS底座所提供的Redis地址，一般填写集群VIP即可。	由环境规划文档获取PaaS底座的VIP。 关键词“PaaS底座”。
	BODHI_REDIS_PORT	6379	DMZ区搭建的PaaS底座所提供的Redis端口	由环境规划文档获取PaaS底座的Redis的端口。 关键词“PaaS底座”。
	BODHI_RABBIT_HOST	10.51.93.15	DMZ区搭建的PaaS底座所提供的RabbitMQ地址，一般填写集群VIP即可。	由环境规划文档获取PaaS底座的VIP。 关键词“PaaS底座”。
	BODHI_RABBIT_USER	openstack	DMZ区搭建的PaaS底座所提供的RabbitMQ的用户信息	由环境规划文档获取PaaS底座的RabbitMQ的用户。 关键词“PaaS底座”。
	BODHI_RABBIT_PORT	5672	DMZ区搭建的PaaS底座所提供的RabbitMQ的端口信息	由环境规划文档获取PaaS底座的RabbitMQ的端口。 关键词“PaaS底座”。
	BODHI_DMZ_HOST	10.51.93.15	DMZ区搭建的PaaS底座所提供的RabbitMQ的主机地址信息，供agent渲染使用，需要与BODHI_RABBIT_HOST是同一个mq	由环境规划文档获取PaaS底座的VIP。 关键词“PaaS底座”。
	BODHI_DMZ_PORT	5672	DMZ区搭建的PaaS底座所提供的RabbitMQ的端口信息，供agent渲染使用，需要与BODHI_RABBIT_HOST是同一个mq	由环境规划文档获取PaaS底座的MQ的端口。 关键词“PaaS底座”。

(5) 若环境变量检查之后存在错误，需要手动修改，修改步骤如下。

a. 连接对应环境后台任一节点，例如 UCO 层任一节点：ssh root@ip。

b. 根据表格中的“服务”列的名称，填入命令中标红部分，输入以下命令，例如：

```
kubectl get deploy -A |grep uco-eams-appmgmt
```

```
[root@cd-dev-uco-k8s-02 ~]#  kubectl get deploy -A |grep uco-eams-appmgmt
default          uco-eams-appmgmt                          1/1     1            1           153d
[root@cd-dev-uco-k8s-02 ~]#
```

c. 复制上图中的两个信息，按照顺序填至以下命令中标红的部分。

```
kubectl edit deploy -n default uco-eams-appmgmt
```

d. 找到与表格中环境变量对应的 Key 值，修改对应的值为正确的值，例如：

```
        - name: LOG_LEVEL
          value: INFO
        - name: TENANTSERVERADDR
          value: unicloud-tenant-core-service.default.svc:30210
        - name: PRODUCTSERVERADDR
          value: uco-product-core-service.default.svc:30212
        - name: TRANSACTIONSERVERADDR
          value: unicloudpco-transaction-core-service.default.svc:31002
        - name: IDGENERATORADDR
          value: uco-instance-id-generator-service.default.svc:31146
        - name: DMZ_BODHI_ADDR
          value: 10.51.80.135:40925
```

e. 修改后进行保存退出（vi 的操作方式，输入冒号与 wq）。

f. 查看对应的 pod 是否重启成功（kubectl get pod -A |grep uco-eams-appmgmt），若图中标红部分对应 pod 的存活时间已更新，则重启成功。

```
[root@cd-dev-uco-k8s-02 ~]#  kubectl get pod -A |grep uco-eams-appmgmt
default          uco-eams-appmgmt-65c675db46-mp4fl                 1/1     Running            0          7d4h
[root@cd-dev-uco-k8s-02 ~]#
```

g. 重启成功后，则可参考查看环境变量步骤再次检查变量修改是否生效。

2. 底层配置

检查适配 CCE 租管互通相关配置。

(1) 连接 A 层后台地址；通过如下命令查询 configmap 配置信息

```
[root@cd-dev-uca-k8s-02 ~]# kubectl get cm -n uca-paas-mse cce-cm -o yaml
apiVersion: v1
data:
  dnsmasq.conf: |
    address=/.cce.unicloudsrv.com/10.51.80.120
kind: ConfigMap
metadata:
  annotations:
    kubectl.kubernetes.io/last-applied-configuration: |
      {"apiVersion":"v1","data":{"dnsmasq.conf":"address=/.cce.unicloudsrv.com/10.51.80.120\n"},"kind":"Con
  creationTimestamp: "2022-05-30T21:01:11Z"
  name: cce-cm
  namespace: uca-paas-mse
  resourceVersion: "19124609"
  selfLink: /api/v1/namespaces/uca-paas-mse/configmaps/cce-cm
```

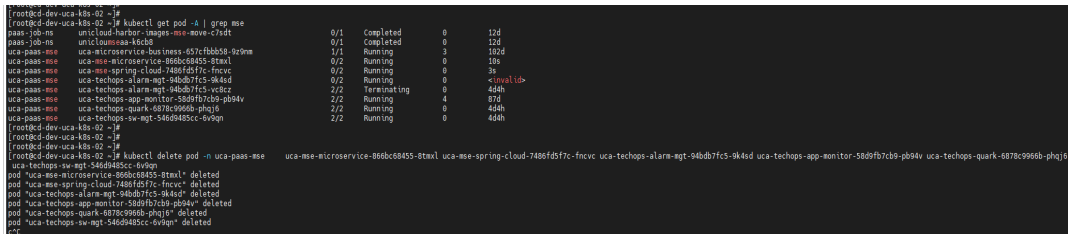
若此处IP地址不为租管互通地址，则需要修正

(2) 若上述地址 10.51.80.120 不是租管互通地址，需要将地址修正后重启相关服务：

修正命令：kubectl edit cm -n uca-paas-mse cce-cm

租管互通地址从环境规划文档获取。

修正后重启 pod 命令：



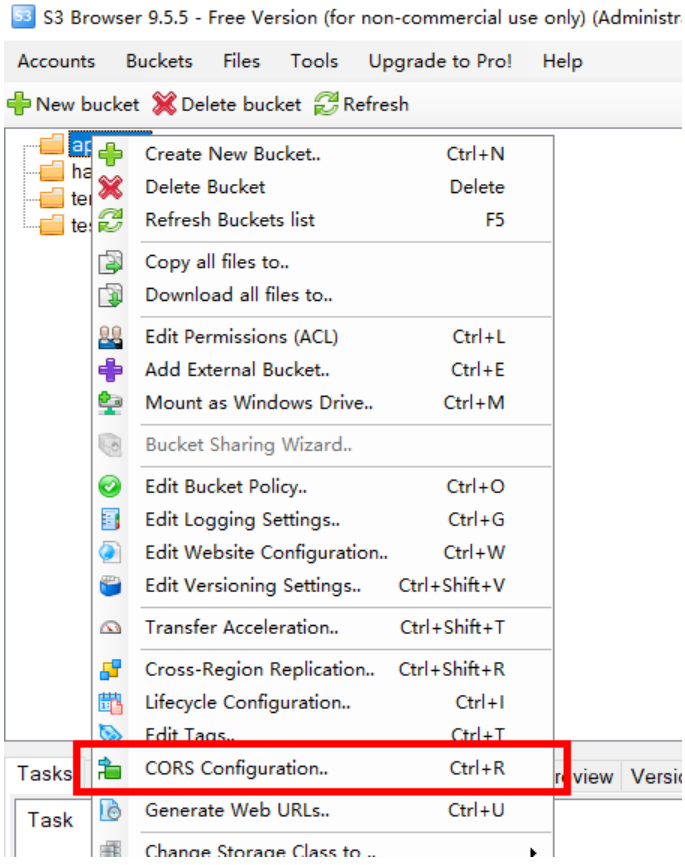
(3) uca-paas-mse 命名空间内相关服务均需要重启；

(4) 若上述地址 10.51.80.120 是租管互通地址，则不需要任何改动。

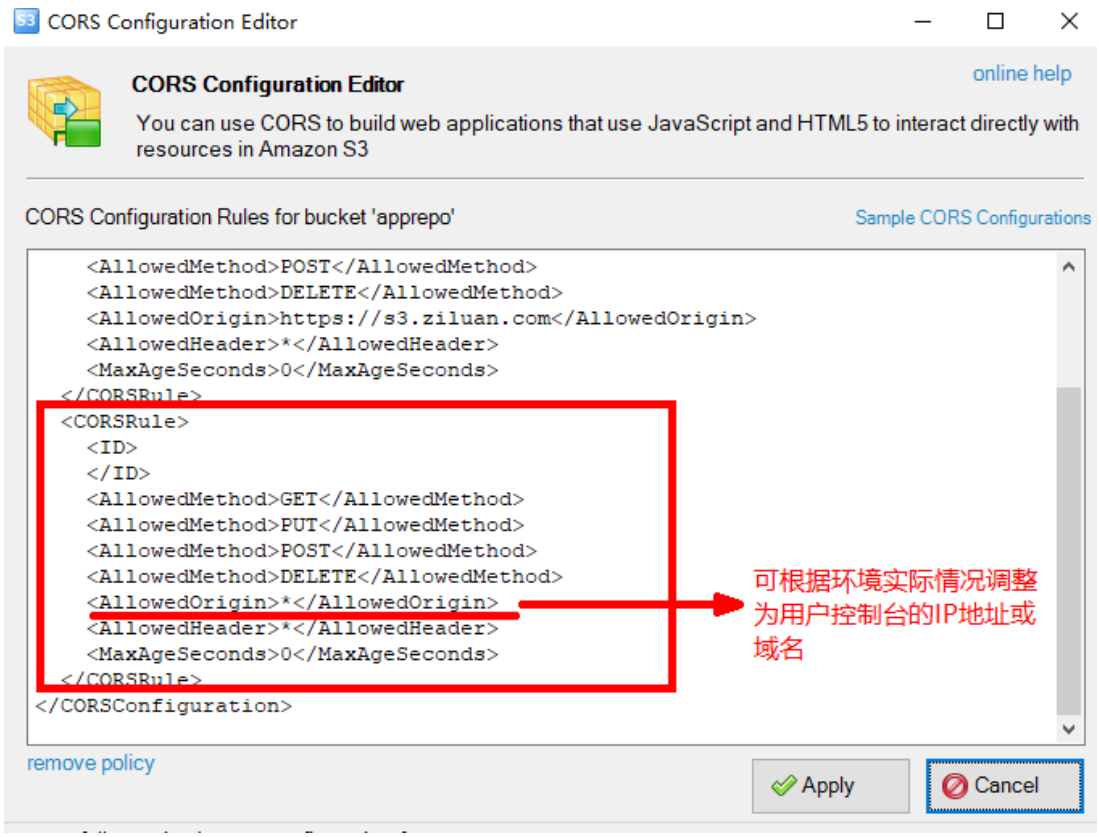
3. 对象存储配置

(1) 企业应用上传应用包功能会将应用包直接上传至对象存储，若对象存储服务端没有配置时，可能会产生跨域的错误（此时将浏览器的 F12 开发者工具打开，切换到 Network 页签，会看到请求产生 CORS 的错误）；

(2) 需要配置对象存储的跨域，首先通过 S3 Browser 连接对象存储，选择 apprepo 桶，右键进行配置，点击 CORS Configuration：



(3) 将其中内容进行设置，源地址可以设置为用户控制台的 IP 或域名；参考如下配置：



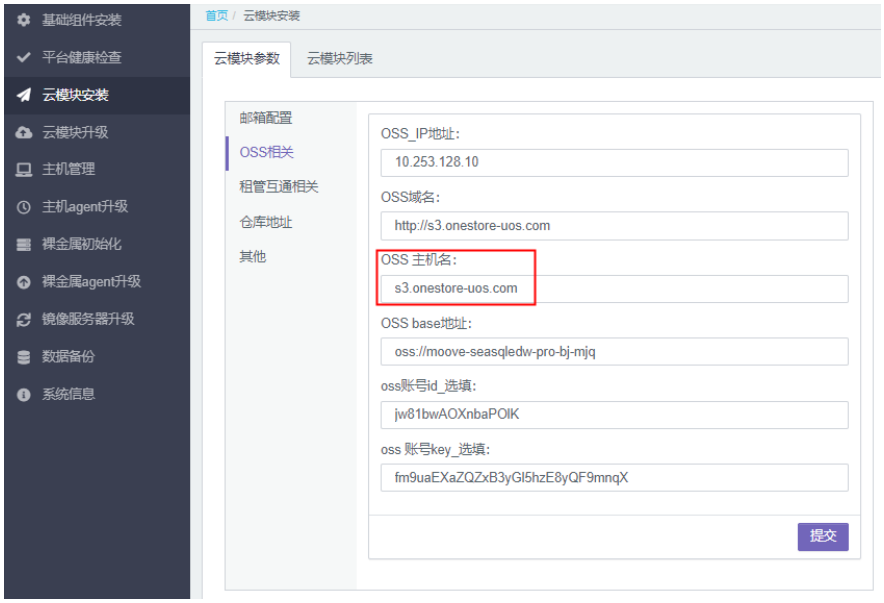
示例（仅供参考）：

```
<?xml version="1.0" encoding="UTF-8"?>
<CORSConfiguration>
  <CORSRule>
    <ID>
    </ID>
    <AllowedMethod>GET</AllowedMethod>
    <AllowedMethod>PUT</AllowedMethod>
    <AllowedMethod>POST</AllowedMethod>
    <AllowedMethod>DELETE</AllowedMethod>
    <AllowedOrigin>*</AllowedOrigin>
    <AllowedHeader>*</AllowedHeader>
    <MaxAgeSeconds>0</MaxAgeSeconds>
  </CORSRule>
</CORSConfiguration>
```

(4) 校验 UCO/UCA 层是否能够正确解析到对象存储的域名地址，校验方式如下。

a. 首先获取 OSS 节点的域名地址，一般可从环境部署规划表中获取，例如：1.hzoss.unicloud.com

b. 若环境部署规划表中未获取该值，可从 rebirth 部署工具中获取，打开环境的 rebirth 部署工具，进入如下界面，获取其中填写的值（该方法前提为 rebirth 部署工具中安装时填写正确，若后期经过变更修改，请以实际值为准）：



c. 连接到 UCO/UCA 集群中任一节点，输入：kubectl get pod –A|grep eams;

```
[root@HZ-AZ1-UCA-K8S-02 ~]# kubectl get pod -A|grep eams
default          uca-eams-appalert-595549c744-xjxmg
default          uca-eams-appconfig-5b88dd9d96-44g6j
default          uca-eams-appdeploy-c9c7969d8-c7t4j
default          uca-eams-appmgmt-8564dfbc57-4xr2r
default          uca-eams-appstore-659cbfd96-l74w4
default          uca-eams-appsync-5bc8cb5698-jfp69
[root@HZ-AZ1-UCA-K8S-02 ~]#
```

d. 复制上图中的任一 pod 的标红部分的两个信息，按照顺序填至以下命令中标红的部分，进入其中任一 pod：kubectl exec -it -n default uca-eams-appmgmt-8564dfbc57-4xr2r bash

```
[root@HZ-AZ1-UCA-K8S-02 ~]# kubectl exec -it -n default        uca-eams-appmgmt-8564dfbc57-4xr2r bash
Defaulting container name to uca-eams-appmgmt.
Use 'kubectl describe pod/uca-eams-appmgmt-8564dfbc57-4xr2r -n default' to see all of the containers in this pod.
root@uca-eams-appmgmt-8564dfbc57-4xr2r:/opt/uca-eams-appmgmt#
root@uca-eams-appmgmt-8564dfbc57-4xr2r:/opt/uca-eams-appmgmt#
```

e. 输入 ping oss 域名地址，若能够解析出正确的 ip 并且能够访问通，即证明 oss 域名地址解析正确，如图即是正确情况：

```
root@uca-eams-appmgmt-8564dfbc57-4xr2r:/opt/uca-eams-appmgmt# ping 1.hzoss.unicloud.com
PING 1.hzoss.unicloud.com (100.66.1.184): 56 data bytes
64 bytes from 100.66.1.184: icmp_seq=0 ttl=58 time=0.286 ms
64 bytes from 100.66.1.184: icmp_seq=1 ttl=58 time=0.242 ms
^C--- 1.hzoss.unicloud.com ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.242/0.264/0.286/0.000 ms
root@uca-eams-appmgmt-8564dfbc57-4xr2r:/opt/uca-eams-appmgmt#
```

(5) 若解析不正确或访问不通，请检查集群的 dns 配置情况。

7.13 计算规格初始化

在 uni_compute 数据库中执行如下命令。

```
use uni_compute;
drop procedure if exists updateUniCompute;
delimiter //
create procedure updateUniCompute()
begin

declare v_flavor_id varchar(36) default '';
declare v_ext_key varchar(255) default '';
declare v_ext_value varchar(255) default '';

declare flag int default 0;

declare bms cursor for
select f.flavor_spec as flavor_id, 'multiQueues' as ext_key, (case
       when cpu =1 then 0
       when cpu<8 then cpu
       when cpu>=8 and cpu<24 then 8
       when cpu>=24 then floor(cpu/2) end) as ext_value
       from tbl_flavor f where (f.flavor_spec like 'c1%.qcow2' or flavor_spec like
's1%.qcow2' or flavor_spec like 'm1%.qcow2') and f.cpu>1;

declare continue handler for not found set flag=1;
-- ecs
if not exists (select id from tbl_flavor where flavor_uuid='s1.medium.4.qcow2') then insert
into
tbl_flavor(flavor_uuid,flavor_spec,cpu,ram,state,ability_tag,limit_wr_iops,limit_wr_bps,
limit_io_qos,flavor_version)
values('s1.medium.4.qcow2','s1.medium.4.qcow2','1','4','available','ecs-qcow2','4000','4
09.6','204.8','1'); end if;
if not exists (select id from tbl_flavor where flavor_uuid='s1.large.4.qcow2') then insert
into
tbl_flavor(flavor_uuid,flavor_spec,cpu,ram,state,ability_tag,limit_wr_iops,limit_wr_bps,
limit_io_qos,flavor_version)
values('s1.large.4.qcow2','s1.large.4.qcow2','2','8','available','ecs-qcow2','4000','409
.6','409.6','1'); end if;
if not exists (select id from tbl_flavor where flavor_uuid='s1.xlarge.4.qcow2') then insert
into
tbl_flavor(flavor_uuid,flavor_spec,cpu,ram,state,ability_tag,limit_wr_iops,limit_wr_bps,
limit_io_qos,flavor_version)
values('s1.xlarge.4.qcow2','s1.xlarge.4.qcow2','4','16','available','ecs-qcow2','8000','
614.4','614.4','1'); end if;
if not exists (select id from tbl_flavor where flavor_uuid='s1.2xlarge.4.qcow2') then insert
into
tbl_flavor(flavor_uuid,flavor_spec,cpu,ram,state,ability_tag,limit_wr_iops,limit_wr_bps,
limit_io_qos,flavor_version)
values('s1.2xlarge.4.qcow2','s1.2xlarge.4.qcow2','8','32','available','ecs-qcow2','10000
','819.2','1024','1'); end if;
```

```
if not exists (select id from tbl_flavor where flavor_uuid='s1.3xlarge.4.qcow2') then insert
into
tbl_flavor(flavor_uuid,flavor_spec,cpu,ram,state,ability_tag,limit_wr_iops,limit_wr_bps,
limit_io_qos,flavor_version)
values('s1.3xlarge.4.qcow2','s1.3xlarge.4.qcow2','12','48','available','ecs-qcow2','1200
0','1024','1638.4','1'); end if;
if not exists (select id from tbl_flavor where flavor_uuid='s1.4xlarge.4.qcow2') then insert
into
tbl_flavor(flavor_uuid,flavor_spec,cpu,ram,state,ability_tag,limit_wr_iops,limit_wr_bps,
limit_io_qos,flavor_version)
values('s1.4xlarge.4.qcow2','s1.4xlarge.4.qcow2','16','64','available','ecs-qcow2','1600
0','1228.8','2048','1'); end if;
if not exists (select id from tbl_flavor where flavor_uuid='s1.6xlarge.4.qcow2') then insert
into
tbl_flavor(flavor_uuid,flavor_spec,cpu,ram,state,ability_tag,limit_wr_iops,limit_wr_bps,
limit_io_qos,flavor_version)
values('s1.6xlarge.4.qcow2','s1.6xlarge.4.qcow2','24','96','available','ecs-qcow2','2000
0','1638.4','3072','1'); end if;
if not exists (select id from tbl_flavor where flavor_uuid='s1.8xlarge.4.qcow2') then INSERT
INTO  `tbl_flavor` (`flavor_uuid`, `flavor_spec`, `cpu`, `ram`, `state`, `ability_tag`,
`limit_wr_iops`, `limit_wr_bps`, `limit_io_qos`, `flavor_version`) VALUES
('s1.8xlarge.4.qcow2', 's1.8xlarge.4.qcow2', '32', '128', 'available', 'ecs-qcow2', '24000',
'2048', '4096', '1'); end if;
if not exists (select id from tbl_flavor where flavor_uuid='c1.medium.2.qcow2') then insert
into
tbl_flavor(flavor_uuid,flavor_spec,cpu,ram,state,ability_tag,limit_wr_iops,limit_wr_bps,
limit_io_qos,flavor_version)
values('c1.medium.2.qcow2','c1.medium.2.qcow2','1','2','available','ecs-qcow2','4000','4
09.6','204.8','1'); end if;
if not exists (select id from tbl_flavor where flavor_uuid='c1.large.2.qcow2') then insert
into
tbl_flavor(flavor_uuid,flavor_spec,cpu,ram,state,ability_tag,limit_wr_iops,limit_wr_bps,
limit_io_qos,flavor_version)
values('c1.large.2.qcow2','c1.large.2.qcow2','2','4','available','ecs-qcow2','4000','409
.6','409.6','1'); end if;
if not exists (select id from tbl_flavor where flavor_uuid='c1.xlarge.2.qcow2') then insert
into
tbl_flavor(flavor_uuid,flavor_spec,cpu,ram,state,ability_tag,limit_wr_iops,limit_wr_bps,
limit_io_qos,flavor_version)
values('c1.xlarge.2.qcow2','c1.xlarge.2.qcow2','4','8','available','ecs-qcow2','8000','6
14.4','614.4','1'); end if;
if not exists (select id from tbl_flavor where flavor_uuid='c1.2xlarge.2.qcow2') then insert
into
tbl_flavor(flavor_uuid,flavor_spec,cpu,ram,state,ability_tag,limit_wr_iops,limit_wr_bps,
limit_io_qos,flavor_version)
values('c1.2xlarge.2.qcow2','c1.2xlarge.2.qcow2','8','16','available','ecs-qcow2','10000
','819.2','1024','1'); end if;
if not exists (select id from tbl_flavor where flavor_uuid='c1.3xlarge.2.qcow2') then insert
into
tbl_flavor(flavor_uuid,flavor_spec,cpu,ram,state,ability_tag,limit_wr_iops,limit_wr_bps,
limit_io_qos,flavor_version)
values('c1.3xlarge.2.qcow2','c1.3xlarge.2.qcow2','12','24','available','ecs-qcow2','1200
0','1024','1638.4','1'); end if;
if not exists (select id from tbl_flavor where flavor_uuid='c1.4xlarge.2.qcow2') then insert
into
```

```
tbl_flavor(flavor_uuid,flavor_spec,cpu,ram,state,ability_tag,limit_wr_iops,limit_wr_bps,
limit_io_qos,flavor_version)
values('c1.4xlarge.2.qcow2','c1.4xlarge.2.qcow2','16','32','available','ecs-qcow2','1600
0','1228.8','2048','1'); end if;
if not exists (select id from tbl_flavor where flavor_uuid='c1.6xlarge.2.qcow2') then insert
into
tbl_flavor(flavor_uuid,flavor_spec,cpu,ram,state,ability_tag,limit_wr_iops,limit_wr_bps,
limit_io_qos,flavor_version)
values('c1.6xlarge.2.qcow2','c1.6xlarge.2.qcow2','24','48','available','ecs-qcow2','2000
0','1638.4','3072','1'); end if;
if not exists (select id from tbl_flavor where flavor_uuid='c1.8xlarge.2.qcow2') then INSERT
INTO  `tbl_flavor` (`flavor_uuid`, `flavor_spec`, `cpu`, `ram`, `state`, `ability_tag`,
`limit_wr_iops`, `limit_wr_bps`, `limit_io_qos`, `flavor_version`) VALUES
('c1.8xlarge.2.qcow2', 'c1.8xlarge.2.qcow2', '32', '64', 'available', 'ecs-qcow2', '24000',
'2048', '4096', '1'); end if;
if not exists (select id from tbl_flavor where flavor_uuid='m1.medium.8.qcow2') then insert
into
tbl_flavor(flavor_uuid,flavor_spec,cpu,ram,state,ability_tag,limit_wr_iops,limit_wr_bps,
limit_io_qos,flavor_version)
values('m1.medium.8.qcow2','m1.medium.8.qcow2','1','8','available','ecs-qcow2','4000','4
09.6','204.8','1'); end if;
if not exists (select id from tbl_flavor where flavor_uuid='m1.large.8.qcow2') then insert
into
tbl_flavor(flavor_uuid,flavor_spec,cpu,ram,state,ability_tag,limit_wr_iops,limit_wr_bps,
limit_io_qos,flavor_version)
values('m1.large.8.qcow2','m1.large.8.qcow2','2','16','available','ecs-qcow2','4000','40
9.6','409.6','1'); end if;
if not exists (select id from tbl_flavor where flavor_uuid='m1.xlarge.8.qcow2') then insert
into
tbl_flavor(flavor_uuid,flavor_spec,cpu,ram,state,ability_tag,limit_wr_iops,limit_wr_bps,
limit_io_qos,flavor_version)
values('m1.xlarge.8.qcow2','m1.xlarge.8.qcow2','4','32','available','ecs-qcow2','8000','
614.4','614.4','1'); end if;
if not exists (select id from tbl_flavor where flavor_uuid='m1.2xlarge.8.qcow2') then insert
into
tbl_flavor(flavor_uuid,flavor_spec,cpu,ram,state,ability_tag,limit_wr_iops,limit_wr_bps,
limit_io_qos,flavor_version)
values('m1.2xlarge.8.qcow2','m1.2xlarge.8.qcow2','8','64','available','ecs-qcow2','10000
','819.2','1024','1'); end if;
if not exists (select id from tbl_flavor where flavor_uuid='m1.3xlarge.8.qcow2') then insert
into
tbl_flavor(flavor_uuid,flavor_spec,cpu,ram,state,ability_tag,limit_wr_iops,limit_wr_bps,
limit_io_qos,flavor_version)
values('m1.3xlarge.8.qcow2','m1.3xlarge.8.qcow2','12','96','available','ecs-qcow2','1200
0','1024','1638.4','1'); end if;
if not exists (select id from tbl_flavor where flavor_uuid='m1.4xlarge.8.qcow2') then insert
into
tbl_flavor(flavor_uuid,flavor_spec,cpu,ram,state,ability_tag,limit_wr_iops,limit_wr_bps,
limit_io_qos,flavor_version)
values('m1.4xlarge.8.qcow2','m1.4xlarge.8.qcow2','16','128','available','ecs-qcow2','160
00','1228.8','2048','1'); end if;
if not exists (select id from tbl_flavor where flavor_uuid='m1.6xlarge.8.qcow2') then insert
into
tbl_flavor(flavor_uuid,flavor_spec,cpu,ram,state,ability_tag,limit_wr_iops,limit_wr_bps,
limit_io_qos,flavor_version)
```

```
values('m1.6xlarge.8.qcow2','m1.6xlarge.8.qcow2','24','192','available','ecs-qcow2','200
00','1638.4','3072','1'); end if;

open bms;
  fetch bms into v_flavor_id, v_ext_key, v_ext_value;
  while flag <> 1 do
       if not exists (select * from tbl_flavor_ext where flavor_id=v_flavor_id and
ext_key=v_ext_key and ext_value=v_ext_value)
       then insert into tbl_flavor_ext (flavor_id,ext_key,ext_value)
values( v_flavor_id,v_ext_key,v_ext_value);
       else update tbl_flavor_ext set flavor_id=v_flavor_id, ext_key=v_ext_key,
ext_value=v_ext_value
       where flavor_id=v_flavor_id and ext_key=v_ext_key and ext_value=v_ext_value;
       end if;
  fetch bms into v_flavor_id, v_ext_key, v_ext_value;
  end while;
close bms;

if not exists (select * from tbl_tag where tag='ecs-qcow2')
then INSERT INTO `tbl_tag` (tag,tag_name) VALUES ('ecs-qcow2', '通用(本地)型'); end if;


end

//
delimiter ;
call updateUniCompute();
drop procedure if exists updateUniCompute;
```

7.14 （可选）配置云平台密码评估服务

当前云平台加密方式支持硬件加密（加密机）和软件加密两种加密方式。两种方式可以通过配置 UCO K8S 集群中任意节点的 configmap 进行切换。当云平台需要通过密码安全性评估（密评）时，需要使用硬件加密方式。

7.14.1 注意事项

如果部署环境变迁，例如新增密评需求时，请提前联系技术支持人员，在技术人员指导下完成操作。

请务必在完成修改配置文件后，再进行各服务开启加密方法的操作。

开启加密后请不要随意关闭。

7.14.2 修改配置文件

1. 查看配置文件

执行命令 kubectl get cm |grep pasa，查看待修改的配置文件。

```
[root@ [redacted]-UCO-K8S-01 sec]# kubectl get cm |grep pasa
pasa-croptconfig                1      25d
pasa-fmdevice                   1      25d
pasa-fmjceconf                  1      25d
pasa-swxaconfig                 1      25d
uco-pasa-configmap              4      25d
[root@ [redacted]-UCO-K8S-01 sec]#
```

配置文件说明如下：

- pasa-croptconfig：启用密评相关配置。
- pasa-fmdevice：加密机 IP 相关配置。
- pasa-fmjceconf：加密机密码配置。
- uco-pasa-configmap：CA 系统配置。

2. 配置 pasa-croptconfig

(1) 执行命令 kubectl edit cm pasa-croptconfig。

(2) 修改 mode 字段。

mode 字段用来设置当前使用的加密方式。默认取值是 BC，即软件加密。如果需要切换为硬件加密方式，则修改为对应的值即可。

如果使用渔翁加密机，请修改 mode 字段为 FishermanJCE。另外请将 kmsProvider 回显中，FishermanJCE 前的#号删除。

(3) 根据项目实际环境，修改 slot 号。Slot 号要和加密机的配置一致。

```
#------configmap---------------
apiVersion: v1
kind: ConfigMap
metadata:
  name: pasa-croptconfig
data:
  crypto.yaml: |+
    pasa:
      crypto:
        mode: BC # 取值范围FishermanJCE（渔翁） ，BC （软件）
        kmsProvider:
          - BC
          #- FishermanJCE
        kmsRSAKeyPub: MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDQWG0ao255rUQIleIhXyCkPlGuWlK5XO19pCY6rWUwSK
        kmsSymKeyEnc: kXfRZly7C5CpspYhyuOndl0uoayVU/3Xqhw+kxugg3apaVjsnc1dxvSWoUG76PNYJLWgnubzRdEYJSoYP8
        kmsSymKeyAlg: AES
        kmsHSMKeySlot: 1
        fmSM3Slot: 11
        fmSM2Slot: 2
        kmsSymKeyVerifyText:
          - nk+3ekfOawvsYYYaWle0Eg==
          - LV4J8ah1F9p+VR6Xa+zwWQ==
        swxaConfig:
          swsds.ini
        sm2:
          slot: 2
          sm3:
            slot: 11
```

另外，如为软件加密，后面的 pasa-fmdevice，pasa-fmjceconf 不需要进行修改；如果项目选用渔翁加密设备，则需要对设备信息进行配置。

3. 配置 pasa-fmdevice

执行命令 kubectl edit cm pasa-fmdevice。

使用该 configmap 对渔翁设备进行配置，主要包括加密机服务 IP、连接数、日志路径等。

其中，加密机服务 IP 字段需修改为实际环境中加密机服务平台的 IP 地址；如果并发数不够时，需要修改连接数。

```
#------configmap---------------
apiVersion: v1
kind: ConfigMap
metadata:
  name: pasa-fmdevice
data:
  FMDevice.conf: |+
    [Server]
    deviceCount=1
    ServerIP1=10.0.150.144
    ConnectCount=50
    [LOG]
    level=3
    path=/var/log/uco-pasa/fmapiv100.log
```

4. 配置 pasa-fmjceconf

执行命令 kubectl edit cm pasa-fmjceconf。

此 configmap 是渔翁加密机初始化连接的相关配置，需要根据实际项目修改 passWord 的值。

```
#------configmap---------------
apiVersion: v1
kind: ConfigMap
metadata:
  name: pasa-fmjceconf
data:
  FMJCECONF.conf: |+
    [LOGCONFIG]
    LEVEL=3
    LOGPATH=/var/log/uco-pasa/fmlog.log
    [Keystore]
    storageType=0
    flashSize=20
    [BasicConf]
    passWord=12345678
    keyRSASize=768
    keySM2Size=1024
    keySM1Size=128
    rsaModLen=2048
    sm2SignFormat=3
    sm2CipherFormat=2
    sm2CipherLength=160
    hashHard=1
    padingType=0
    deviceType=57600
```

5. 配置 uco-pasa-configmap

执行命令 kubectl edit cm uco-pasa-configmap。

需根据项目实际情况，修改 CERT_CA 字段的值为 CA 认证系统的 IP 地址。

```
---
apiVersion: v1
data:
  BATCH_MAX_SIZE: "1000"
  CONFIGDIR_FM: "/opt/pasa/fm/"
  CONFIGDIR_SW: "/opt/pasa/sw"
  CERT_CA: http://10.253.27.131:8080
kind: ConfigMap
metadata:
  name: uco-pasa-configmap
```

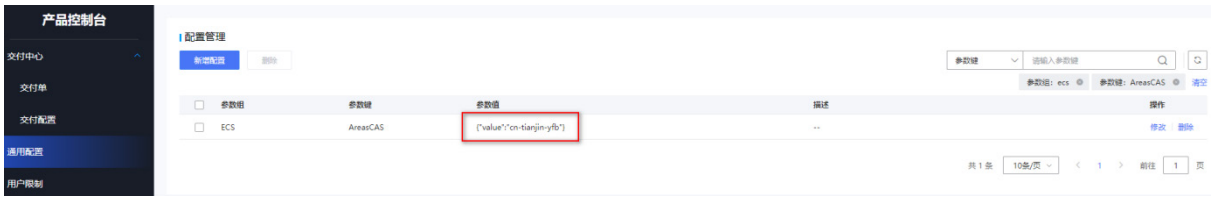
6. 重启 uco-pasa 的 Pod

所有修改都完成后，请重启 uco-pasa 所在的 Pod。

7.14.3 开启计算服务加密方法

1. 开启 O 层开关方法

登录运维控制台，选择[用户控制台/产品控制台/通用配置]，修改参数如下。参数组和参数键参见下图，参数值为节点 ID。

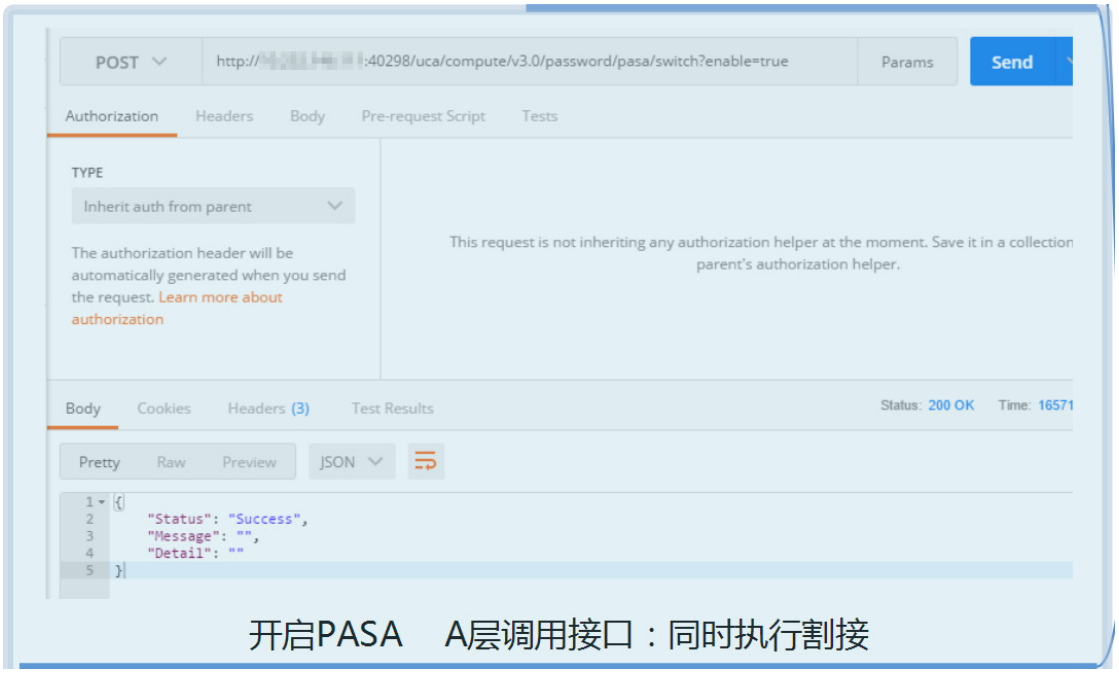


2. 开启 A 层开关方法

使用 postman 工具调用接口:

http://<IP>40298/uca/compute/v3.0/password/pasa/switch?enable=true

其中，IP 为 UCA 的 VIP，ture 改为 false 为关闭。



3. 重启 UCA 层 compute-core 服务

```
Kubectl get pod|grep compute-core
Kubectl delete pod <podname>
```

7.14.4 开启网络服务加密方法

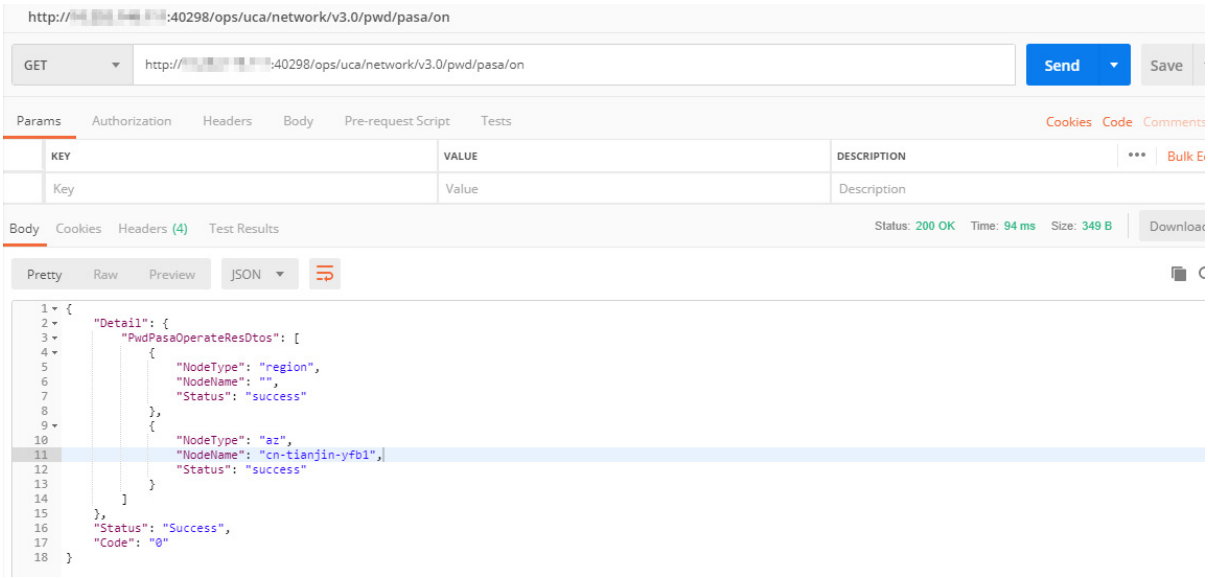
1. 开启 A 层开关方法

使用 postman 工具调用接口:

GET

http://{k8svip}:40298/ops/uca/network/v3.0/pwd/pasa/on

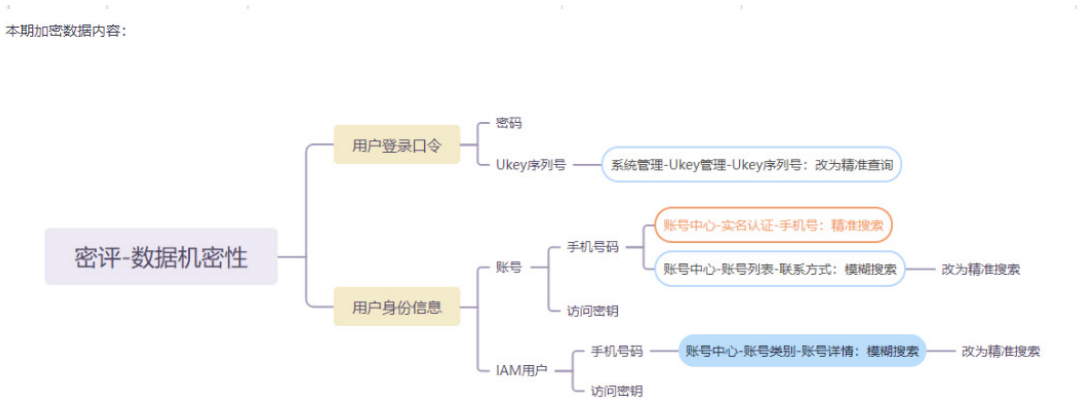
其中，K8S 的 VIP 为 UCA 的 VIP。



响应体 Region 和 AZ 的状态都为 success，说明开启成功，数据割接完成。

7.14.5 运营服务加解密操作方法

1. 数据加密的范围



2. 数据库表

涉及的数据库表如下。

表7-2 运营加密涉及的数据库表

库	表	字段	字段含义	是否加密	加密算法	检索需求
tenant-core	access	access_key	AK	否	-	-
tenant-core	access	access_secret	SK	否	-	-
tenant-core	admin	phone	手机号	否	-	-
tenant-core	ukey_certificate	certificate_key_no	key序列号	否	-	精确检索

tenant-core	user	phone	手机号	否	-	模糊检索 -> 精确检索
tenant-core	user_password_history	password	历史登录密码	是	h3（即原PCO中的加密工具类）	-
tenant-core	login_config	password	登录密码	是	h3（即原PCO中的加密工具类）	

3. 加密场景

场景定义如下：

- 将公有云场景定义为未加密状态（null）。
- 将调用密评服务加密场景定义为 pasa 加密。
- 将使用原 PCO 中的加密工具类定义为 h3 加密。

加密场景包括：

(1) 当前环境由未加密状态变成 pasa 加密状态。

(2) 当前环境由 pasa 加密状态变成 h3 加密状态。

(3) 当前环境由 h3 加密状态变成 pasa 加密状态。

(4) 当前环境由 pasa 或 h3 加密状态变为未加密状态。

4. 操作方法

注意

- 操作前，请务必备份表 7-2 中的 6 个表的数据。
- 第一次操作时，需要保证这两个表没有数据：encrypt_value、encrypt_value_error。操作前请进行检查。
- 请严格按照下面的操作顺序从前往后操作，不能乱序，否则会出现错误。

(1) 从未加密状态到 pasa 状态

a. 如下方式调用 tenant-core 工程清洗数据 URL（由于需调用 pasa 服务接口进行加密，清洗数据用时会比较长，且数据量越大，清洗时间越长）：执行下面的命令即可。

```
curl -X GET "http://10.103.248.80:30210/v1/encrypt/inner/data/clean/null_to_pasa" -H "accept: */*"
```

其中，10.103.248.80 需要替换为具体的 tenant-core 服务的 SVC 的 IP 值。

b. 进行业务验证。

(2) 从 pasa 状态到 h3 状态

a. 如下方式调用 tenant-core 工程清洗数据 URL：

```
curl -X GET "http://10.103.248.80:30210/v1/encrypt/inner/data/clean/pasa_to_h3" -H "accept: */*"
```

其中，10.103.248.80 需要替换为具体的 tenant-core 服务的 SVC 的 IP 值。

b. 进行业务验证。

(3) 从 h3 状态到 pasa 状态

a. 如下方式调用 tenant-core 工程清洗数据 URL：

```
curl -X GET "http://10.103.248.80:30210/v1/encrypt/inner/data/clean/h3_to_pasa" -H "accept: */*"
```

其中，10.103.248.80 需要替换为具体的 tenant-core 服务的 SVC 的 IP 值。

b. 进行业务验证。

(4) 从 pasa/h3 状态到未加密状态

a. 如下方式调用 tenant-core 工程清洗数据 URL：

```
curl -X GET "http://10.103.248.80:30210/v1/encrypt/inner/data/clean/to_null " -H "accept: */*"
```

其中，10.103.248.80 需要替换为具体的 tenant-core 服务的 SVC 的 IP 值。

b. 进行业务验证。

5. 密文临时表

加密后的数据可以查看表 encrypt_value 和 encrypt_value_error。

存储的加密数据，表 7-2 中的 6 个表的字段数据加密后，正常时会存储在 encrypt_value 表中，异常时的数据会存储在 encrypt_value_error 中，两个表的并集数据为所有的加密数据。

6. 异常处理

在调用清洗数据接口后，程序会自动对相关库表进行备份操作，备份表的命名规则为“被备份表名_bk_操作时间_清洗方式”，如“user_bk_20230307123000_null2pasa”。

若在调用清洗数据接口后，发现接口响应异常，或 encrypt_value_error 表存在异常数据，可手动将备份的数据覆盖回业务表，并联系技术人员解决异常。解决异常后重新调用接口清洗数据即可。

8 安全云服务组件部署

CloudOS 7.0 提供多个安全云服务，维护云上业务安全。当前云平台上可提供漏洞扫描、堡垒机、WAF、服务器安全监测、网页防篡改、日志审计、数据库审计、态势感知等八个安全云服务。

本章将介绍如何在 CloudOS 7.0 云平台上安装和部署安全云服务。

说明

创建 NFV（堡垒机、数据库审计、日志审计、网页防篡改和 WAF）使用的 VKS 存储建议使用共享存储，否则无法保证虚机的高可用。

8.1 手动操作部分处理

8.1.1 执行 exportSql 文件

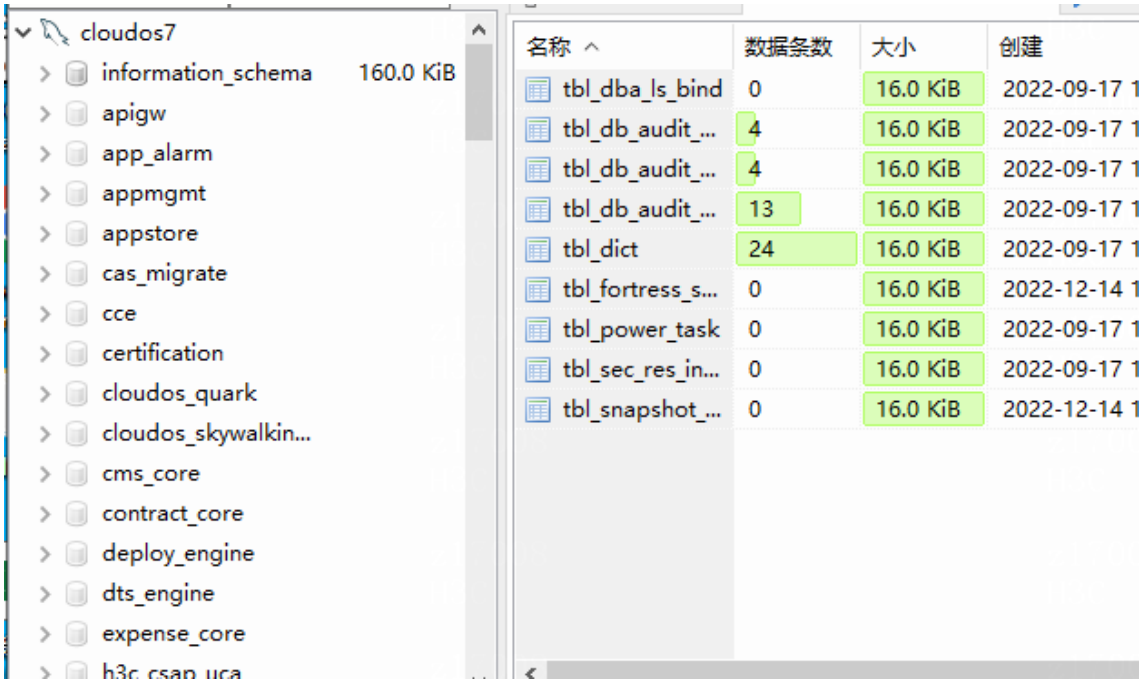
进入 TAAG 集群任一节点后台，执行 exportSql.sh 脚本。exportSql.sh 脚本获取路径为：升级包/手动操作部分及使用说明/安全/

执行完后，当前目录会生成一个名为 logaudit_dict_svc.sql 文件。

在数据库执行 logaudit_dict_svc.sql 脚本。

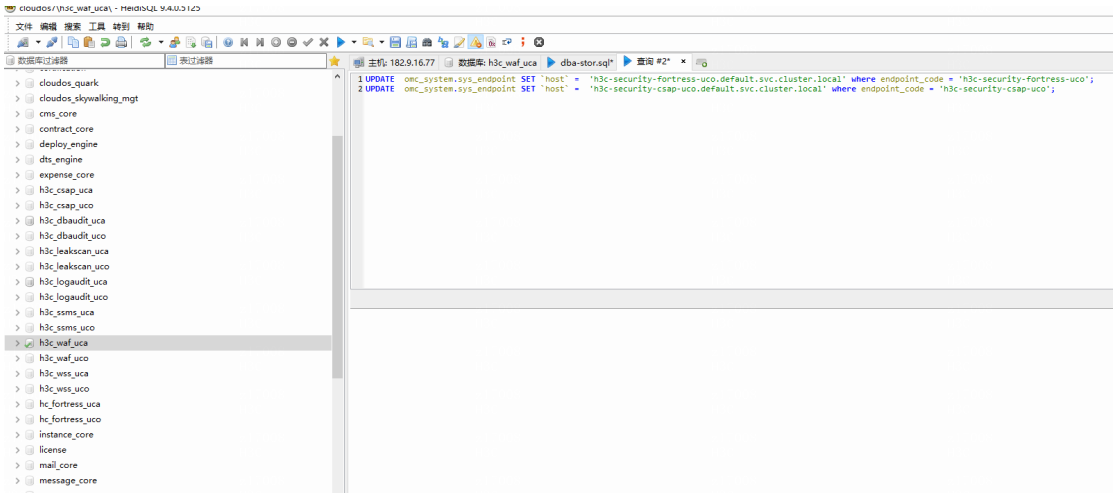
8.1.2 更新 OMC 配置

(1) 使用数据库客户端工具连接云平台数据库。

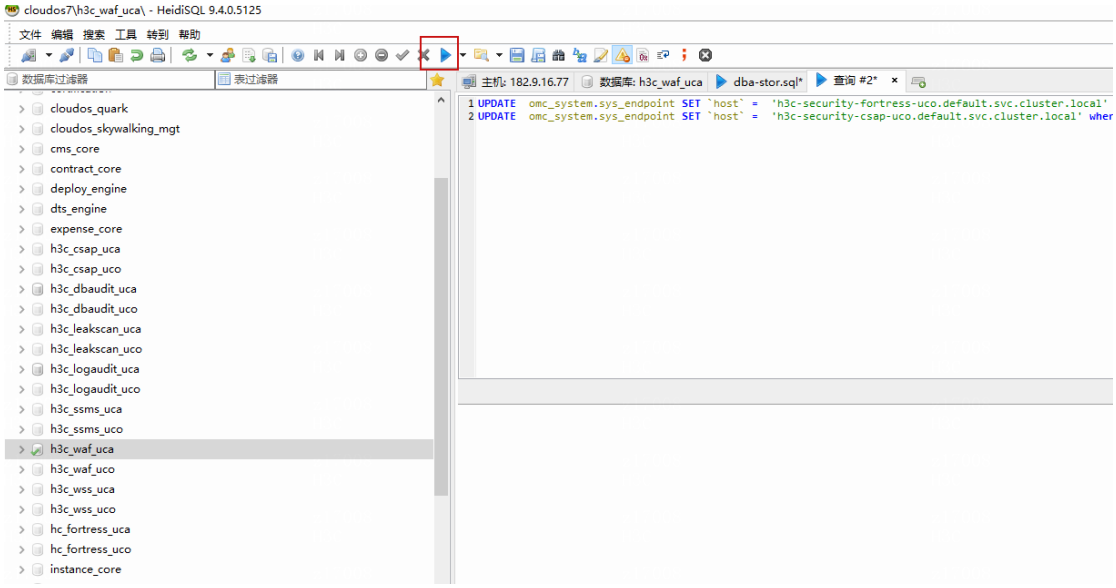


(2) 将以下两行脚本拷贝到数据库客户端工具。

```
UPDATE  omc_system.sys_endpoint SET `host` =
'h3c-security-fortress-uco.default.svc.cluster.local' where endpoint_code =
'h3c-security-fortress-uco';
UPDATE  omc_system.sys_endpoint SET `host` =
'h3c-security-csap-uco.default.svc.cluster.local' where endpoint_code =
'h3c-security-csap-uco';
```



(3) 点击执行按钮。



(4) 完成执行。

8.2 配置指导

在云平台部署成功之后，需要进行一系列配置操作，成功配置之后才能在云平台正常使用相应的安全服务。

8.2.1 授权服务器部署

1. 部署前必读

WAF、堡垒机、漏洞扫描、数据库审计、日志审计、网页防篡改等六个云安全云服务需要部署授权服务器（当前仅支持手动部署），并导入授权文件；服务器安全监测和态势感知不需要部署授权服务器。

部署授权服务器注意事项如下：

- 每个云服务需要单独部署授权服务器，并导入授权文件。
- 所有授权服务器都必须部署在 DMZ 区，且使用单网卡；此网卡要与云平台 A 层互通，也要保证云平台所有 VPC 与此网卡互通；建议使用 100.64.0.0/24 网段地址，请提前规划地址信息。
- WAF 和网页防篡改可以共用一个授权服务器。
- 授权服务器安装完成后，建议使用 Google 访问 Web 页面，导入授权文件。
- 要求授权服务器时间与云平台时间差不超过 3 分钟。

各安全云服务是否需要部署授权服务器，以及在部署授权服务器时，是否需要部署额外服务以支持云服务使用，相关说明见下表。

表8-1 安全云服务授权服务器部署情况说明

服务名称	手动部署授权服务器	部署额外服务	备注
WAF	√	×	
堡垒机	√	应用发布服务	应用发布服务根据现场需求

			确认是否安装
服务器安全监测	×	×	支持共享模式
漏洞扫描	√	×	支持共享模式
数据库审计	√	cas-agent	
日志审计	√	×	
网页防篡改	√	×	
态势感知	×	×	支持共享模式

2. WAF

授权服务器部署

相关安装包在 CloudOS 7.0 版本发布包中“全量包/云服务组件包/安全/VWAF/”目录下获取，授权服务器部署请参考“附录 E.1 WAF 授权服务器部署”。

授权资源导入

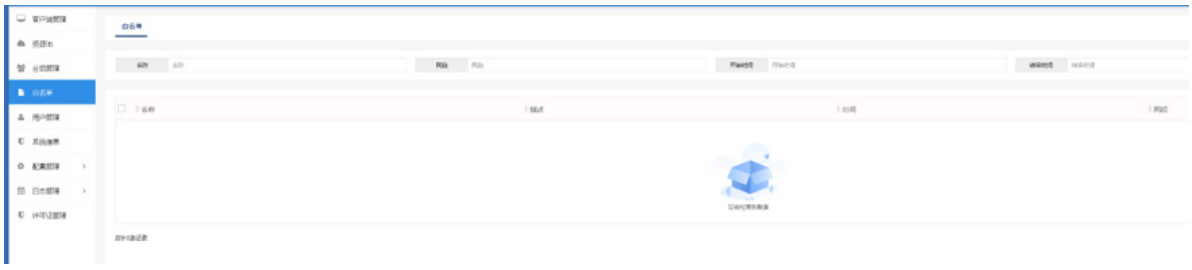
搭建好授权服务器后，请导入相关规格的授权资源。运营平台和控制台上支持配置的 WAF 规格为 vwaf-v100、vwaf-v300、vwaf-v500，对应 WAF 设备规格分别为 v100、v200、v300。如下表。

云规格	WAF 规格
vwaf-v100	v100
vwaf-v300	v200
vwaf-v500	v300

白名单配置

配置方式：登录授权管理系统，在左侧导航树选择[白名单]菜单项，单击<新增>，添加网段。需要注意：

- 请提前与运维人员确认租户业务网和 DMZ 区之间是否设置防火墙，如果有，就添加业务网 NAT 之后的地址，如果没有，就添加租户业务网地址。
- 目前只能添加 24 位掩码长度的网段；如果所添加的网段掩码超过 24 位，需要拆分成多个子网网段（必须覆盖要添加的网段）添加进去。



3. 堡垒机

授权服务器部署

相关安装包在 CloudOS 7.0 版本发布包中“全量包/云服务组件包/安全/堡垒机/”目录下获取，授权服务器部署请参考“附录 E.2 堡垒机授权服务器部署”。

说明

堡垒机临时授权和永久授权不能共存，如果使用临时授权，需要手动修改数据库 h3c_fortress_uca 的表 tbl_dict_name 为 fortress 记录的值 value 修改为 T（永久授权），默认临时授权为 P。

授权资源导入

搭建好授权服务器后，要成功导入相关规格的授权资源。

4. 日志审计

授权服务器部署

相关安装包在 CloudOS 7.0 版本发布包中“全量包/云服务组件包/安全/日志审计/”目录下获取。授权服务器部署请参考“附录 E.3 日志审计授权服务器部署”。

授权资源导入

搭建好授权服务器后，要成功导入相关规格的授权资源。

注意

日志审计支持 CSAP-SA-V，不支持–VLAPSTD 授权。

配置客户端

需要在 Web 页面配置客户端用于授权通信，新建一个客户端即可。

(1) 选择[客户端配置]菜单项，单击<增加>，弹出增加客户端窗口。

(2) 配置参数：自定义客户端名称、客户端密码。

注意

请记录此处的客户端名称及密码，配置日志审计授权服务器时会用到。

5. 数据库审计

说明

数据库审计安装包的获取，请到 Cloudos 7.0 版本发布包中“全量包/云服务组件包/安全/数据库审计/”目录下获取。

Agent-casserver 部署

agent-casserver 主要用于数据库审计所部署的虚拟机和授权服务器的接口被调用时 token 的验证，agent-casserver 和授权服务器部署一样**部署在 DMZ 区**，部署前需要找环境负责人确认平台 A 层和 DMZ 区是互通的。agent-casserver 部署请参考“附录 E.4.1 Agent-casserver 部署”。

授权服务器部署

授权服务器部署请参考“附录 E.4.2 授权服务器部署”和“E.4.3 Casagent 安装”。

注意

- 在数据库审计授权服务器中正确配置 agent-casserver 信息，确保数据库审计授权服务器、agent-casserver、管区 UCA 虚拟机三方各自操作系统时钟一致，误差允许在 3 分钟以内。
- 一个 VKS 只能部署一台授权服务器。

授权资源导入

搭建好授权服务器后，要成功导入相关规格的授权资源。

6. 网页防篡改

授权服务器部署

相关安装包在 CloudOS 7.0 版本发布包中“全量包/云服务组件包/安全/网页防篡改/”目录下获取，授权服务器部署请参考“附录 E.5 网页防篡改授权服务器部署”。

授权资源导入

搭建好授权服务器，然后导入相关规格的授权资源。

注意

云平台网页防篡改使用的授权区分 Linux 和 Windows 类型授权，请根据类型申请相应授权。

白名单配置

配置方式：登录授权管理系统，在左侧导航树选择[白名单]菜单项，单击<新增>，添加网段。需要注意：

- 请提前和运维人员确认租户业务网和 DMZ 区之间有没有设置防火墙，如果有，添加业务网 NAT 之后的地址，如果没有，添加租户业务网地址。
- 目前只能添加 24 位掩码长度的网段，如果所添加的网段掩码超过 24 位，需要拆分成多个子网网段（必须覆盖要添加的网段）添加进去。

8.2.2 共享模式的云服务部署

漏洞扫描、态势感知、服务器安全监测等三个服务支持租户共享模式，需要手动将这三个云服务**部署在 DMZ 区域**。

1. 漏洞扫描

授权服务器和漏洞扫描部署

目前使用的是三代漏扫，三代漏扫需要部署授权服务器和漏扫虚拟机，**均需要部署在 DMZ 区**。

(1) 三代漏扫授权服务器部署，相关安装包在 CloudOS 7.0 版本发布包中“全量包/云服务组件包/安全/漏洞扫描/”目录下获取，授权服务器部署具体操作步骤请参考“E.6.1 授权服务器安装”。

(2) 三代漏扫虚拟机部署，使用的版本是 E6202P03，虚拟机部署具体操作步骤请参考“E6.2 漏扫虚拟机安装”。

授权资源导入

搭建好授权服务器后需导入相应的授权，以及对部署完成的漏扫虚拟机授权。

白名单配置

配置方式：登录授权管理系统，在左侧导航树中选择[白名单]菜单项，单击<新增>，添加 NAT 网段。需要注意：

- 请提前和运维人员确认租户业务网和 DMZ 区之间有没有设置防火墙，如果有，就添加业务网 NAT 之后的地址，如果没有，就添加租户业务网地址。
- 目前只能添加 24 位掩码长度的网段，如果所添加的网段掩码超过 24 位，需要拆分成多个子网段（必须覆盖要添加的网段）添加进去。

说明

建议将特征库升级到最新版本。

2. 态势感知

态势感知安装

态势感知需要部署在 DMZ 区，相关安装包在 CloudOS 7.0 版本发布包中“全量包/云服务组件包/安全/态势感知/”目录下获取，单机版参考“附录 E.7 态势感知部署”，集群版请联系研发支持。

授权资源导入

部署完成后，需要手动导入授权资源。

3. 服务器安全监测

一代服务器安全监测部署

当前使用服务器安全监测版本为 E6404，服务器安全监测需要部署在 DMZ 区，具体配置步骤请参考“E.8 一代服务器安全检测部署。

注意

修改服务器安全监测操作系统时间，使其与 A 层管理平台系统时间一致，否则开通会失败。修改指令为：date　s “2022-xx-xx xx:xx:xx”部署时，建议开启防护墙，暴露必要的端口。

1、授权资源导入

服务器安全监测服务不涉及授权服务器部署。在服务器安全监测部署完成后，需要导入相应的授权。

2、域名访问配置

如果不需要支持域名访问，请跳过该步骤。

(1) 使用 root 用户进入服务器安全监测的后台。

执行命令 cd /data/app/titan-config

执行命令 jps

执行命令 vi java.json

```
[root@ssms titan-config]# pwd
/data/app/titan-config
[root@ssms titan-config]# vi java.json
```

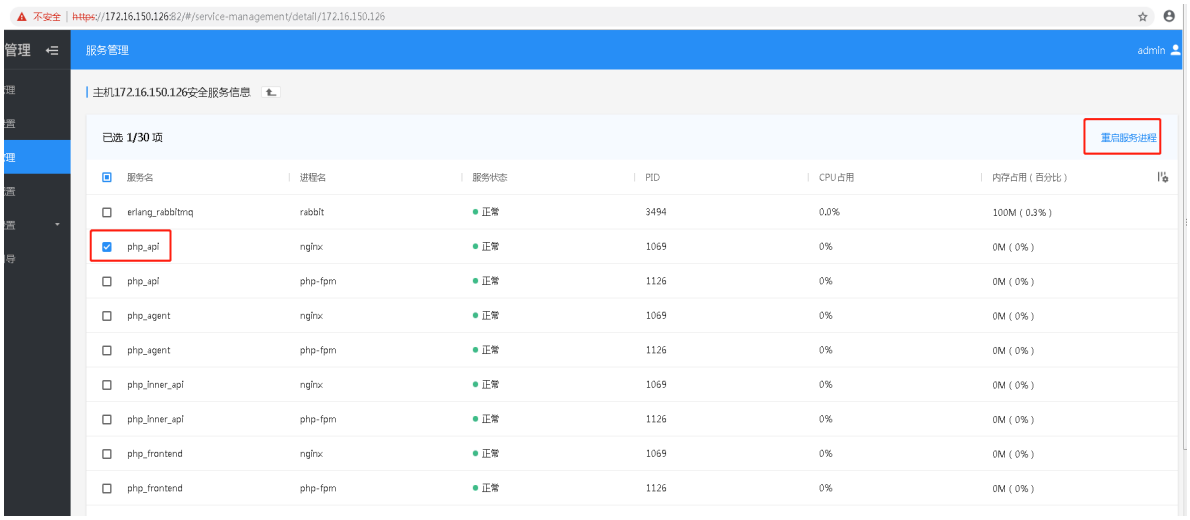
(2) 把域名加入 refer_domains 对应的值中。举例：通过域名为 ssm.unicloud.com 的方式访问服务器安全监测，修改方式如下：

```
  "gateway" : {
    "api_sign_key_keep_days" : 10,
    "ext_api_flow_control_enable" : false,
    "ext_api_max_concurrency" : 20,
    "login_rsa_private_key" : "MIICdQIBADANBgkqhkiG9w0BAQEFAASCAl8wggJbAgEAAoGBAJK93rLGFugZlERgyExqxFIL4
AwlPmrDr/4FZ7AzLi1VgRHVfniZ7zOQS4Bh7GuSY2O0GddFjeho7eWuIPWpxIV1AgMBAAECgYAIJnOQCmCLU6Bgi9+UHvn4dKBl9BZ+zP
VII+IhAJve8DoH36AKgpgSvFO6EUgTr4Sa+B7l4SUKXJ5jnFYc49rnoQJBANHibCo64vRHeK5rtVTmUEbggnDbnfzGVD9rguMw2QkRIyV
3jS62PjXs88hvZ0s8JUIf6hCJ/aOHzu7eq/GPQmMFLQGfAkBnvInJtaFHK6wySXoupEc5QO436dSEg2JQlkrzD8m1+Yptj6po8eZ4Mm5x
lDIAK0S9upoDqXqLBOiuvYf7w/FlOh7vAkB+mrT6c82FeaNvt0dR45g+r9vdfiCzHVF7hi+oJOltjb5p54P1wbwsTeEZJqHrcCOQ/NfwP
    "login_rsa_public_key" : "MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCSvd6yxhboGZREYMhMasRSC+Accoc8cnqvkA
ewMy4tVYER1X54me8zkEuAYexrkmNjtBnXRY3oaO3lriD1qcSFdQIDAQAB",
    "refer_check" : true,
    "refer_domains" : "http://172.16.150.126,https://172.16.150.126,http://ssms.unicloud.com",
    "session_inactive_interval" : 30,
    "upload" : {
      "maxFileSize" : "500MB",
      "maxRequestSize" : "1000MB"
    }
  },
  "scan" : {
```

3、检查组件是否正常

登录 web 页面，url 为 https://{ip}:82，进入服务管理页面，点击<安全服务信息>。

如果服务进程有异常（查看服务状态列），选择该异常进程，点击<重启服务进程>。如果重启后仍然异常，请联系相关技术人员。



二代服务器安全监测部署

当前使用服务器安全监测版本为 E6901P03，服务器安全监测需要部署在 DMZ 区，具体配置步骤请参考“E.9 二代服务器安全检测部署”。

注意

修改服务器安全监测操作系统时间，使其与 A 层管理平台系统时间一致，否则开通会失败。修改指令为：date　s “2022-xx-xx xx:xx:xx”部署时，建议开启防护墙，暴露必要的端口；

授权资源导入

服务器安全监测服务不涉及授权服务器部署。在服务器安全监测部署完成后，需要导入相应的授权。

8.2.3 镜像制作

说明

只有涉及虚拟机的安全云服务，即 WAF、堡垒机、日志审计、数据库审计、网页防篡改需要进行本操作，如果配置漏洞扫描、服务器安全监测、态势感知服务，可忽略该步骤。严格按照文档要求添加镜像 id 和大小。

安全产品的基础镜像请在 CloudOS 7.0 版本发布包中获取（获取路径：全量包/云服务组件包/安全），具体制作、上传镜像方式请参考如下操作步骤。目前云平台支持 3par、SDS、本地三种存储类型，不同的存储类型对应镜像制作过程存在差异，请谨慎操作。

表8-2 安全云服务镜像系统盘大小参考值列表

服务	镜像 id	大小
WAF	h3c-security-waf-v100-v1	100G

WAF	h3c-security-waf-v300-v1	100G
WAF	h3c-security-waf-v500-v1	100G
堡垒机	h3c-security-fortress-v10-v1	500G
堡垒机	h3c-security-fortress-v20-v1	500G
堡垒机	h3c-security-fortress-v200-v1	500G
堡垒机	h3c-security-fortress-v50-v1	500G
堡垒机	h3c-security-fortress-v100-v1	500G
堡垒机	h3c-security-fortress-v500-v1	500G
日志审计	img-logaudit-cloud	50G
数据库审计	h3c-security-db-audit-num3-v1	80G
数据库审计	h3c-security-db-audit-num5-v1	80G
数据库审计	h3c-security-db-audit-num10-v1	80G
数据库审计	h3c-security-db-audit-num25-v1	80G
网页防篡改	h3c-security-wss	500G

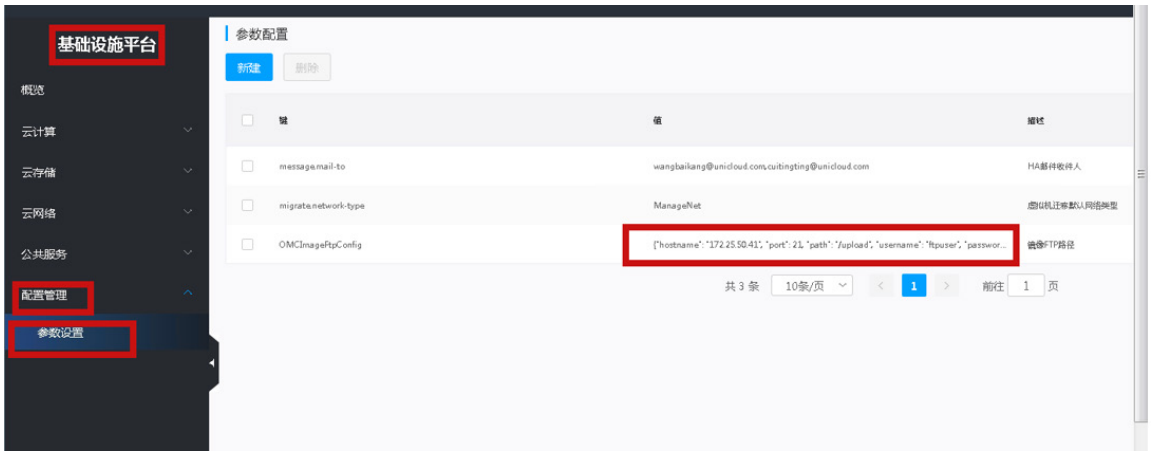
说明：没有特殊要求，请按照表格中大小配置；若有修改后面涉及到磁盘容量的值需要同步修改；否则创建服务异常。

1. 自动上传

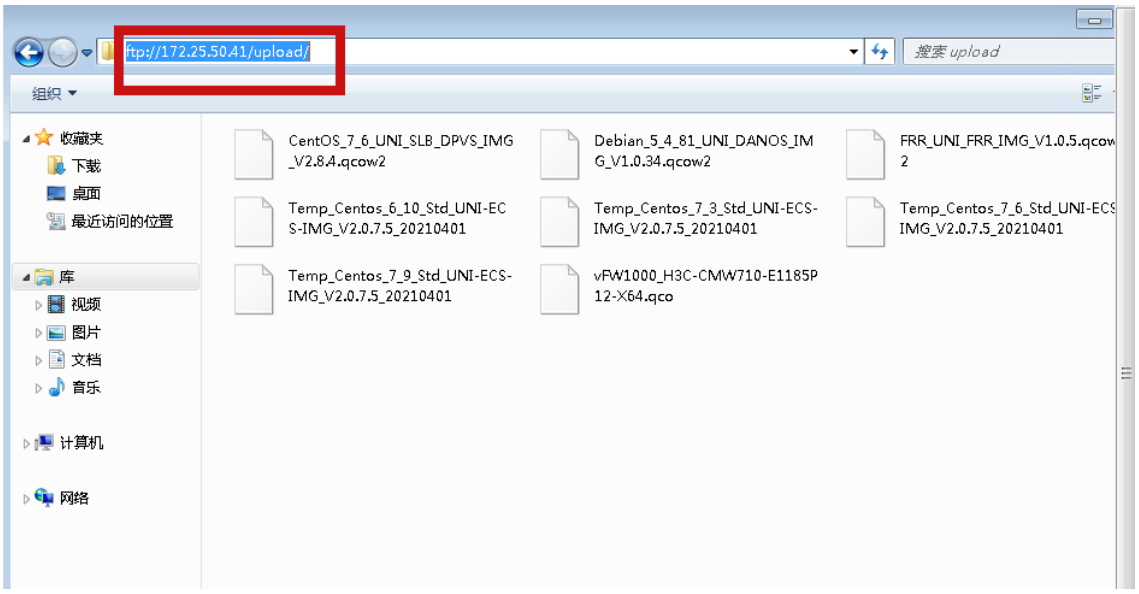
(1) 上传镜像到指定目录

镜像目录可找运维人员确定或者登录 OMC 平台，进入基础设施平台-》配置管理-》参数设置，定位到键为 OMCImageFtpConfig 的记录，其中：

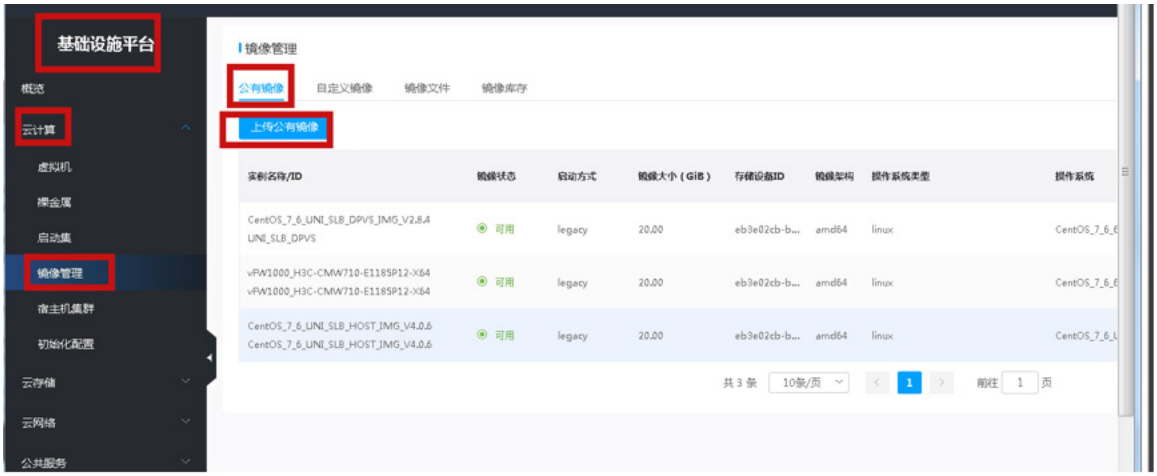
Host 为 ftp 服务器地址，path 为要上传的目录，username 为登录 ftp 服务器的用户名，password 为登录密码。



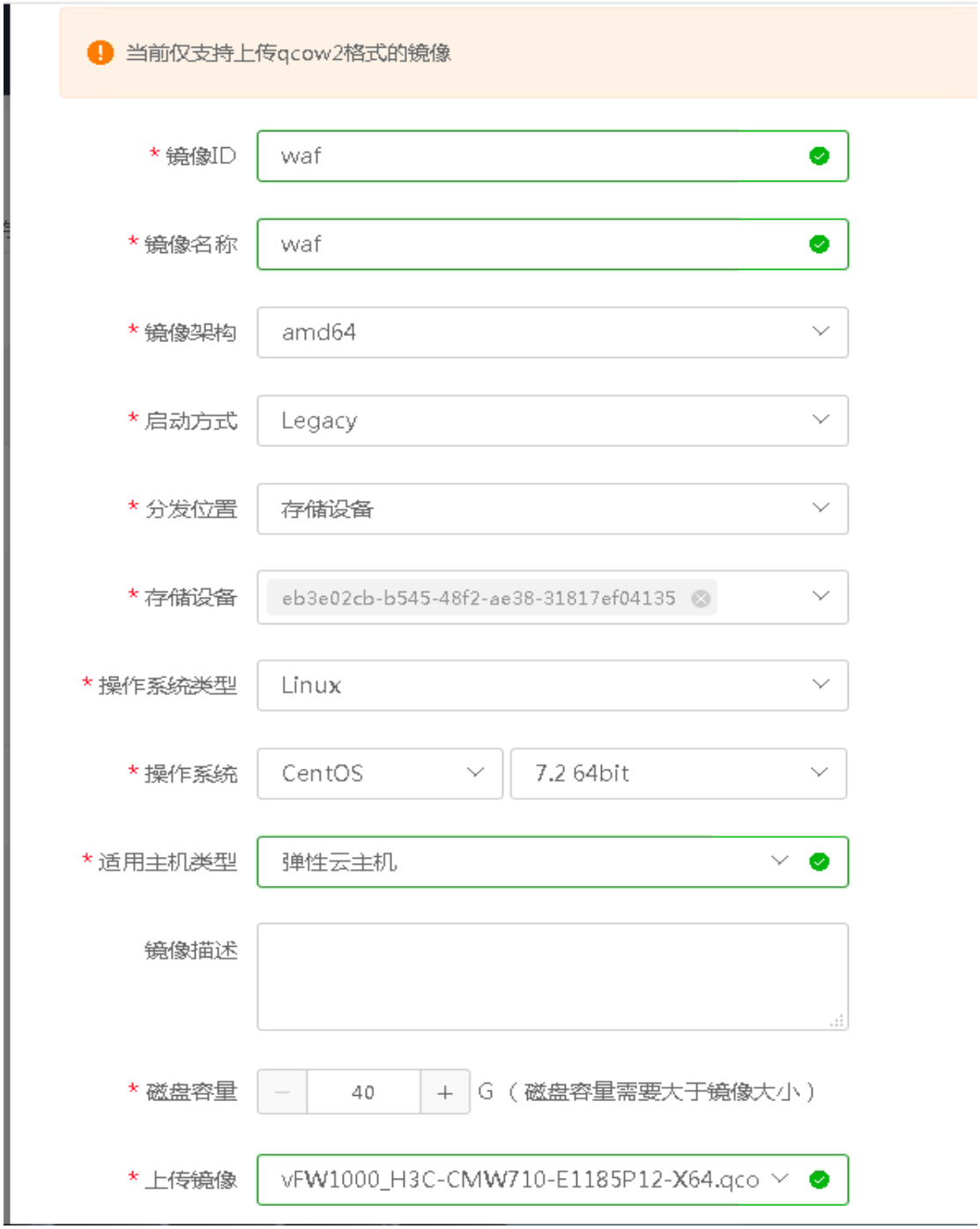
登录后，把镜像文件传入该目录下。



(2) 进入上传界面，点击“上传公有云镜像”。



(3) 配置参数



参数说明如下：

- 镜像 ID：参考文档中第三部分，输入服务的镜像 id，注意要保持一致。
- 镜像名称：和镜像 id 一样。
- 镜像架构：amd64/arm64，根据情况确定 arm 版本选择 arm64，x86 选择 amd64。
- 启动方式：Legacy。
- 分发位置：存储设备。
- 存储设备：下拉显示的是存储池的 id，不确认选哪个的话找该模块负责人确认。
- 操作系统：Linux（目前都是），7.2 64bit（暂时都选择这个，不影响功能）。
- 适用主机类型：选择弹性云主机。

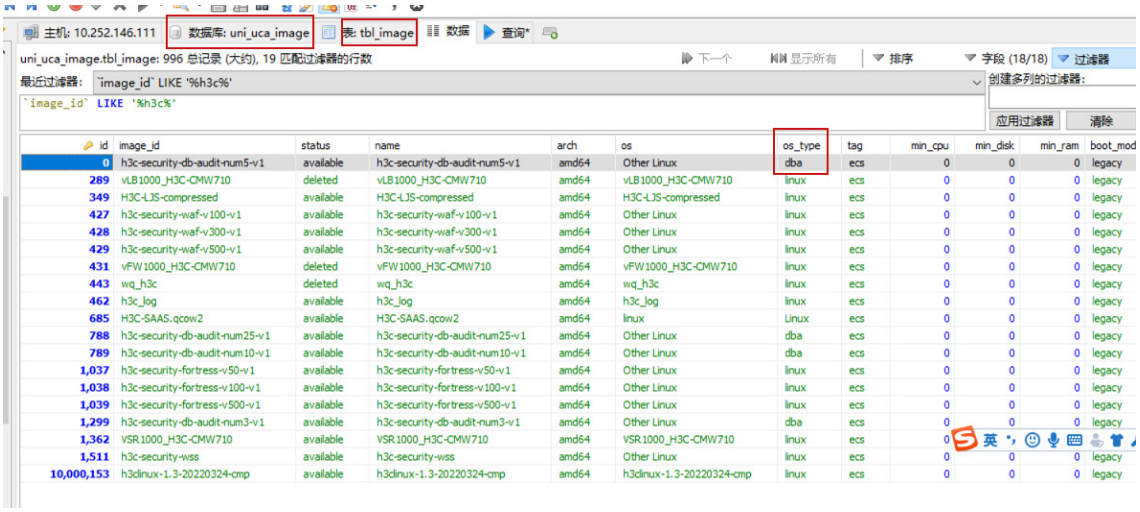
- 磁盘容量：不小于镜像的 virtual size。

```
[root@hb1-bjmy1-image-server01 2020-05-28]# qemu-img info Temp_Centos_6_5_05130940
image: Temp_Centos_6_5_05130940
file format: qcow2
virtual size: 40G (42949672960 bytes)
disk size: 1.7G
cluster_size: 262144
Format specific information:
    compat: 1.1
    lazy refcounts: false
[root@hb1-bjmy1-image-server01 2020-05-28]#
```

- 上传镜像：选择步骤 1 中的镜像。

(4) 修改 os_type

如果是数据库审计，需要把A层的uni-uca-image数据库，tbl_image表的os_type修改为dba。其他的服务镜像无需该操作。



id	image_id	status	name	arch	os	os_type	tag	min_cpu	min_disk	min_ram	boot_mod
0	h3c-security-db-audit-num5-v1	available	h3c-security-db-audit-num5-v1	amd64	Other Linux	dba	ecs	0	0	0	legacy
289	vLB1000_H3C-CMW710	deleted	vLB1000_H3C-CMW710	amd64	vLB1000_H3C-CMW710	linux	ecs	0	0	0	legacy
349	H3C-LJS-compressed	available	H3C-LJS-compressed	amd64	H3C-LJS-compressed	linux	ecs	0	0	0	legacy
427	h3c-security-waf-v100-v1	available	h3c-security-waf-v100-v1	amd64	Other Linux	linux	ecs	0	0	0	legacy
428	h3c-security-waf-v300-v1	available	h3c-security-waf-v300-v1	amd64	Other Linux	linux	ecs	0	0	0	legacy
429	h3c-security-waf-v500-v1	available	h3c-security-waf-v500-v1	amd64	Other Linux	linux	ecs	0	0	0	legacy
431	vFW1000_H3C-CMW710	deleted	vFW1000_H3C-CMW710	amd64	vFW1000_H3C-CMW710	linux	ecs	0	0	0	legacy
443	wq_h3c	deleted	wq_h3c	amd64	wq_h3c	linux	ecs	0	0	0	legacy
462	h3c_log	available	h3c_log	amd64	h3c_log	linux	ecs	0	0	0	legacy
685	H3C-SAAS.qcow2	available	H3C-SAAS.qcow2	amd64	linux	Linux	ecs	0	0	0	legacy
788	h3c-security-db-audit-num25-v1	available	h3c-security-db-audit-num25-v1	amd64	Other Linux	dba	ecs	0	0	0	legacy
789	h3c-security-db-audit-num10-v1	available	h3c-security-db-audit-num10-v1	amd64	Other Linux	dba	ecs	0	0	0	legacy
1,037	h3c-security-fortress-v50-v1	available	h3c-security-fortress-v50-v1	amd64	Other Linux	linux	ecs	0	0	0	legacy
1,038	h3c-security-fortress-v100-v1	available	h3c-security-fortress-v100-v1	amd64	Other Linux	linux	ecs	0	0	0	legacy
1,039	h3c-security-fortress-v500-v1	available	h3c-security-fortress-v500-v1	amd64	Other Linux	linux	ecs	0	0	0	legacy
1,299	h3c-security-db-audit-num3-v1	available	h3c-security-db-audit-num3-v1	amd64	Other Linux	dba	ecs	0	0	0	legacy
1,362	VSR1000_H3C-CMW710	available	VSR1000_H3C-CMW710	amd64	VSR1000_H3C-CMW710	linux	ecs	0	0	0	legacy
1,511	h3c-security-wss	available	h3c-security-wss	amd64	Other Linux	linux	ecs	0	0	0	legacy
10,000,153	h3clinux-1.3-20220324-cmp	available	h3clinux-1.3-20220324-cmp	amd64	h3clinux-1.3-20220324-cmp	linux	ecs	0	0	0	legacy

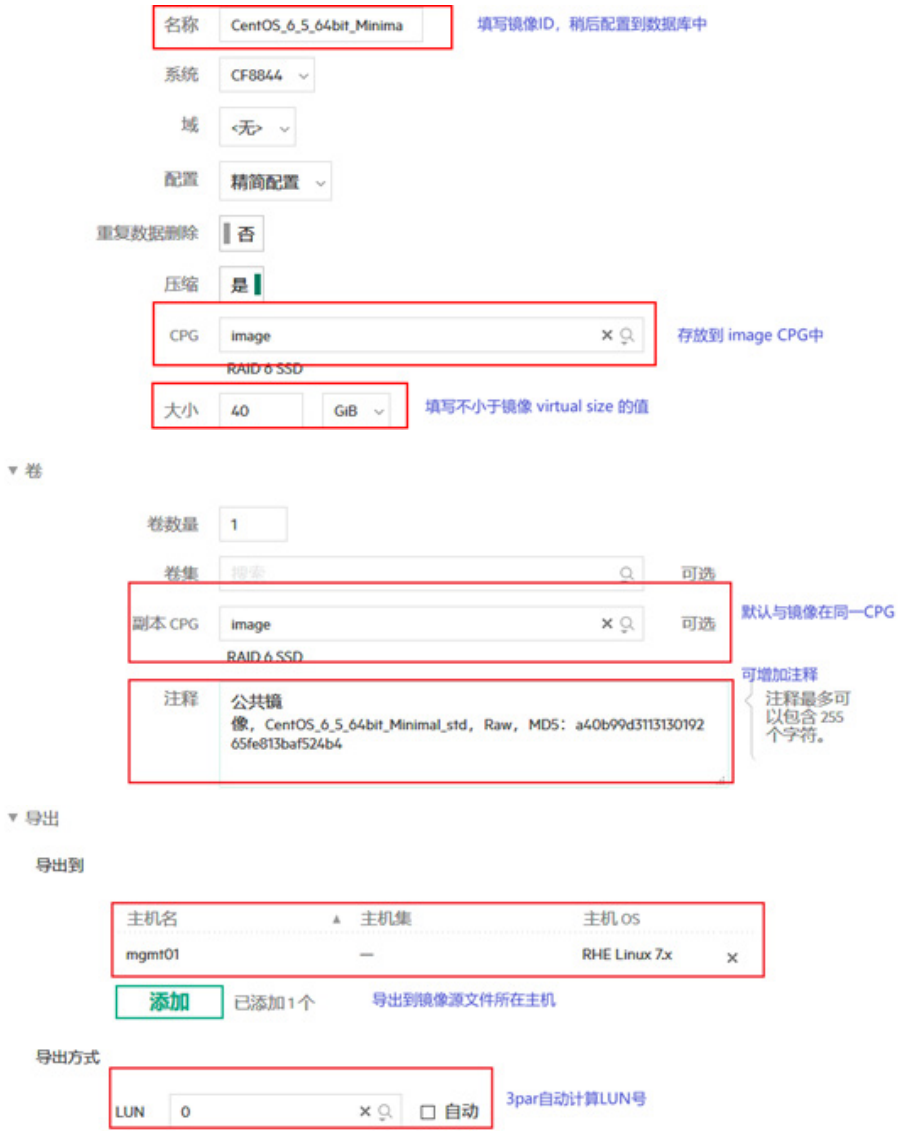
2. 手动上传

3par：

(1) 使用 qemu-img info 命令查看镜像信息，注意镜像的 virtual size。

```
[root@hb1-bjmy1-image-server01 2020-05-28]# qemu-img info Temp_Centos_6_5_05130940
image: Temp_Centos_6_5_05130940
file format: qcow2
virtual size: 40G (42949672960 bytes)
disk size: 1.7G
cluster_size: 262144
Format specific information:
    compat: 1.1
    lazy refcounts: false
[root@hb1-bjmy1-image-server01 2020-05-28]#
```

(2) 在 3par 中创建一个不小于镜像 virtual size 的空卷，并导出到镜像所在的服务器（如果 3par 中找不到服务器，请参考 3Par/Primera 创建主机）。命名规则参考镜像 ID 命名；如果是更新镜像，为了方便回溯，先将原镜像重命名为<原镜像名称.n>（例如：CentOS_6_5_64bit_Minimal_std.1）。



(3) 设置完成后记录卷的 WWN（3par 默认字母大写，兆维和上海已设置为显示小写，和 Linux 中统一）。

(4) 转换源镜像文件并写入到 3par 卷中。

在上传服务器上映射创建的镜像卷（操作步骤参考连接/断开连接卷）。

a. 通过 wwn 查看卷信息。

```
[root@i-9Ugzds6NaA ~]# ll /dev/mapper | grep -E '60002ac00000000001b11000250be'
lrwxrwxrwx 1 root root      7 Apr 22 09:07 360002ac00000000001b11000250be -> ../dm-3
```

b. 写入镜像。

```
[root@i-9Ugzds6NaA ~]# qemu-img convert -p -O raw /path/to/image/file
/dev/mapper/360002ac00000000001b11000250be
```

写入完成后断开镜像卷（操作步骤参考连接/断开连接卷）。

SDS：

找到一个已安装 SDS client 的虚机，其中使用的 SDS client 与 SDS 版本应当一致。使用 qemu-img 写入镜像。

(1) 使用 qemu-img 导入镜像，使用默认的 SDS 配置文件。

```
[root@i-9Ugzds6NaA ~]# qemu-img convert -p -O raw /path/to/qcow2/file rbd:.<存储池名称>.rbd/<镜像 id>
```

(2) 多套 SDS 时，指定 SDS 配置文件。

```
[root@i-9Ugzds6NaA ~]# qemu-img convert -p -O raw /path/to/qcow2/file rbd:.<存储池名称>.rbd/<镜像 id>:conf=/etc/onestor_client/<ceph conf 文件>:keyring=/etc/onestor_client/<ceph keyring 文件>
```

(3) SDS 已创建卷，使用 qemu-img 更新镜像。

```
[root@i-9Ugzds6NaA ~]# qemu-img convert -p -n -O raw /path/to/qcow2/file rbd:.<存储池名称>.rbd/<镜像 id>
```

添加记录：

镜像表在 A 层 uni_uca_image 数据库中，此处需要更新的表名为 tbl_image、tbl_image_storage，如果是新加镜像，使用以下 sql 语句添加一条记录，其中`image_id`为存储设备中卷名称，`name`和`os`目前和`image_id`一致：

INSERT INTO `uni_uca_image`.`tbl_image`(`image_id`, `status`, `name`, `arch`, `os`, `os_type`, `tag`, `min_cpu`, `min_disk`, `min_ram`, `boot_mode`, `user_id`, `virtual_size`, `description`, `version`) VALUES ('<镜像 ID，和 3par 中卷名一致>', 'available', '<镜像名称>', 'amd64', '<镜像系统>', '<操作系统类型，1.Linux 2.Windows>', '<镜像标签，1、ecs 2、bms>', 0, 0, 0, '<镜像启动方式：legacy 、uefi >', '<镜像所属 user id，公共镜像为 public>', <镜像未压缩容量，Byte>, '', '');

-- 公共镜像上传到几台存储设备，此数据就需要添加几条，只是 storage_id 不同，比如 3par 和 SDS 都传了，需要写入两条；

INSERT INTO `uni_uca_image`.`tbl_image_storage`(`image_id`, `volume_id`, `status`, `storage_id`, `internal_id`, `wwn`, `format`, `hash_algo`, `hash`, `size`) VALUES ('<镜像 ID，和 3par 中卷名一致>', '<镜像 ID，和 3par 中卷名一致>', 'available', '<存储集群 id，可查看表 tbl_storage_server 中字段 server_id>', '', '', '<镜像格式，qcow2，raw>', '', '', <镜像未压缩容量，Byte>);

注：如果是数据库审计的镜像，os_type 的值必须为 dba

例：

INSERT INTO `uni_uca_image`.`tbl_image`(`image_id`, `status`, `name`, `arch`, `os`, `os_type`, `tag`, `min_cpu`, `min_disk`, `min_ram`, `boot_mode`, `user_id`, `virtual_size`, `description`, `version`) VALUES ('CentOS_7_3_64bit_Minimal_std', 'available', 'CentOS_7_3_64bit_Minimal_std', 'amd64', 'CentOS_7_3_64bit_Minimal_std', 'linux', 'ecs', 0, 0, 0, 'legacy', 'public', 42949672960, '公共镜像', '');

INSERT INTO `uni_uca_image`.`tbl_image_storage`(`image_id`, `volume_id`, `status`, `storage_id`, `internal_id`, `wwn`, `format`, `hash_algo`, `hash`, `size`) VALUES ('CentOS_7_3_64bit_Minimal_std', 'CentOS_7_3_64bit_Minimal_std', 'available', 'CN7948097W', '', '', 'raw', '', '', 42949672960);

如果是更新镜像，同步更新表中`updated_at`字段：

UPDATE `uni_uca_image`.`tbl_image` SET `updated_at`='2020-04-27 20:30:00' WHERE `image_id`='CentOS_7_3_64bit_Minimal_std';

UPDATE `uni_uca_image`.`tbl_image_storage` SET `updated_at`='2020-04-27 20:30:00' WHERE `image_id`='CentOS_7_3_64bit_Minimal_std';

3. 安全服务的镜像 id

(1) 堡垒机

- 迷你版：h3c-security-fortress-v10-v1
- 基础版：h3c-security-fortress-v20-v1
- 企业增强版：h3c-security-fortress-v200-v1
- 标准版：h3c-security-fortress-v50-v1
- 企业版：h3c-security-fortress-v100-v1

- 旗舰版：h3c-security-fortress-v500-v1

(2) 日志审计

img-logaudit-cloud

(3) WAF

- V100: h3c-security-waf-v100-v1
- V300: h3c-security-waf-v300-v1
- V500: h3c-security-waf-v500-v1

(4) 数据库审计

- 标准版：h3c-security-db-audit-num3-v1
- 企业版：h3c-security-db-audit-num5-v1
- 企业增强版：h3c-security-db-audit-num10-v1
- 旗舰版：h3c-security-db-audit-num25-v1

(5) 网页防篡改

h3c-security-wss

8.3 安全服务配置

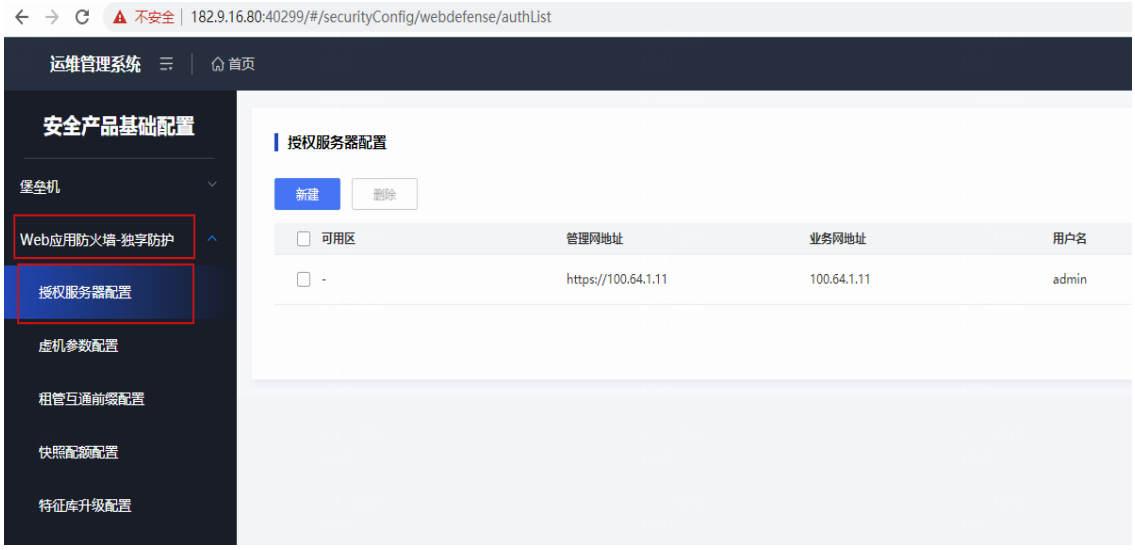
(1) 登录运维管理平台。

(2) 通过“运维管理平台 > 安全产品基础配置”页面，进行各云服务的授权服务器配置、虚机磁盘参数配置、资源池配置等操作，用来保障服务正常创建。

8.3.1 WAF

1. 授权服务器配置

(1) 访问“安全产品基础配置 > Web 应用防火墙-独享防护 > 授权服务器配置”页面。



(2) 单击<新建>按钮，弹出新建输入框。

参数说明如下：

- 可用区：从当前区域下可用区列表中选择。
- 管理网地址：授权服务器管理网地址。
- 业务网地址：授权服务器业务网地址，标准方案中授权服务器只有一个地址，此时可填写该地址。
- 用户名：授权服务器管理页面的用户名。
- 密码：授权服务器管理页面的密码。

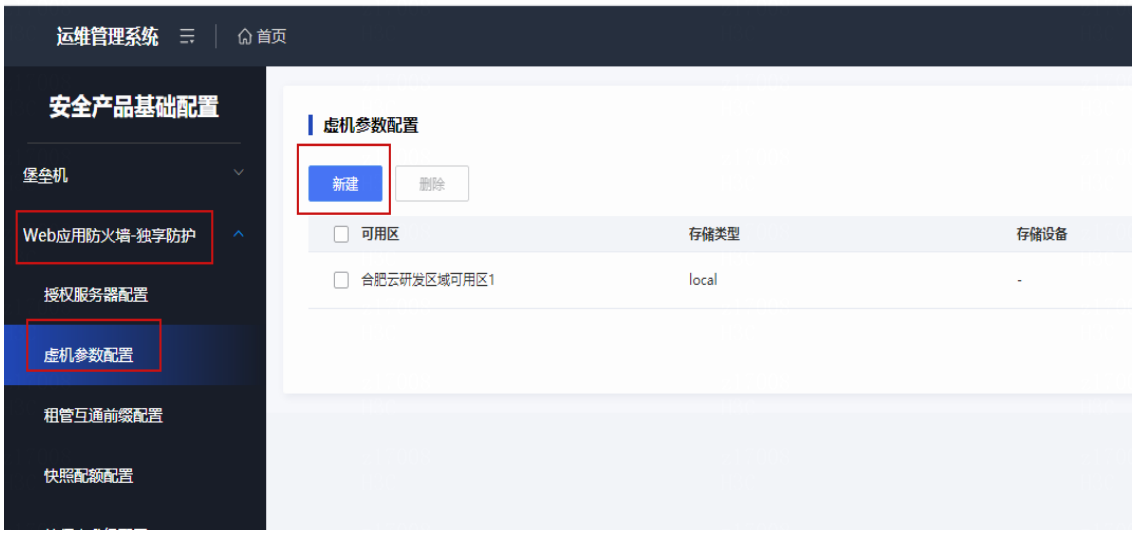
(3) 单击<提交>按钮，完成配置。

2. 虚机磁盘参数配置

默认使用从云存储中读取到的磁盘参数。如果要求使用指定的磁盘参数，或者指定使用 Local 存储类型，需要进行此参数配置。

按照如下步骤配置虚机磁盘相关参数。

(1) 访问安全产品基础配置>>Web 应用防火墙-独享防护>>虚机参数配置页面。



(2) 单击<新建>按钮，弹出新建窗口。

参数说明如下：

- 可用区：从当前区域下可用区列表中选择。
- 存储方式：区分本地模式与共享存储模式。
- 存储类型：当前云平台支持共享存储类型为（SDS、3par）。
- 存储设备：根据存储类型过滤出存储设备。
- 磁盘规格：选择存储设备所支持的磁盘规格。

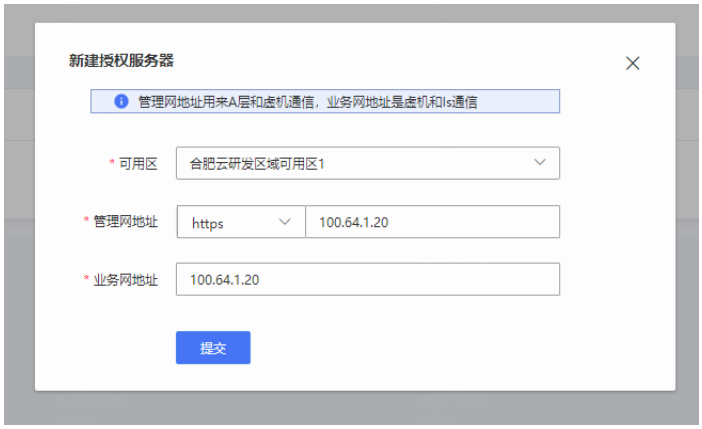
(3) 单击<提交>按钮，完成配置。

8.3.2 堡垒机

1. 授权服务器配置

(1) 访问“安全产品基础配置 > 堡垒机 > 授权服务器配置”页面。

(2) 单击<新建>，进入新建页面。



参数说明如下：

- 可以区：从当前区域下可用区列表中选择。
- 管理网地址：授权服务器管理网地址。
- 业务网地址：授权服务器业务网地址，标准方案中授权服务器只有一个地址，此时可填写该地址。

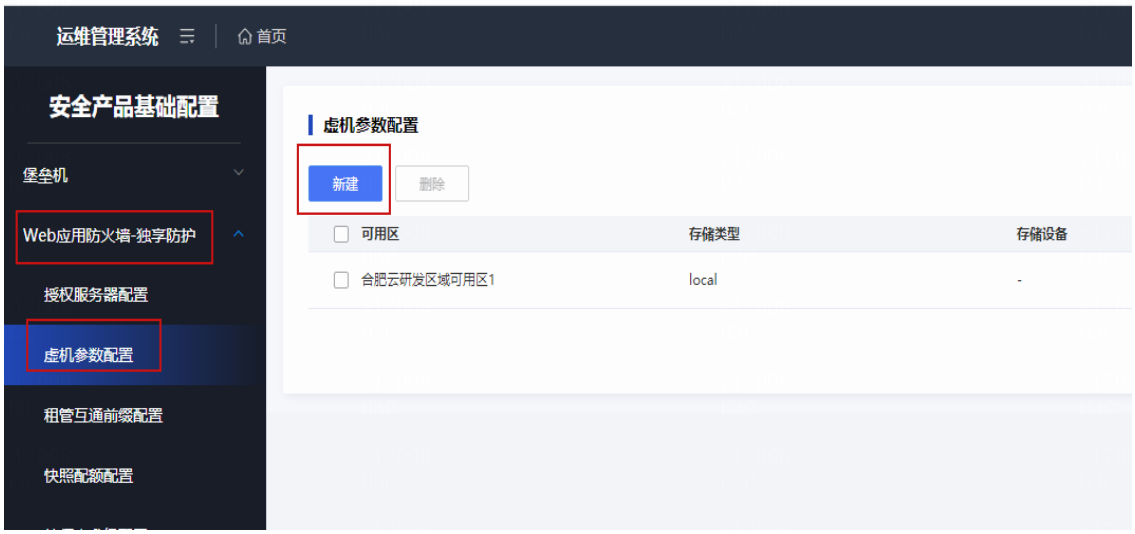
(3) 单击<提交>按钮，完成配置。

2. 虚机磁盘参数配置

默认使用从云存储中读取到的磁盘参数。如果要求使用指定的磁盘参数，或者指定使用 Local 存储类型，需要进行此参数配置

按照如下步骤配置虚机磁盘相关参数。

(1) 访问“安全产品基础配置 > Web 应用防火墙-独享防护 > 虚机参数配置”页面。



(2) 单击<新建>按钮，弹出新建窗口。

参数说明如下：

- 可用区：从当前区域下可用区列表中选择。
- 存储方式：区分本地模式与共享存储模式。
- 存储类型：当前云平台支持共享存储类型为（SDS、3par）。
- 存储设备：根据存储类型过滤出存储设备。
- 磁盘规格：选择存储设备所支持的磁盘规格。

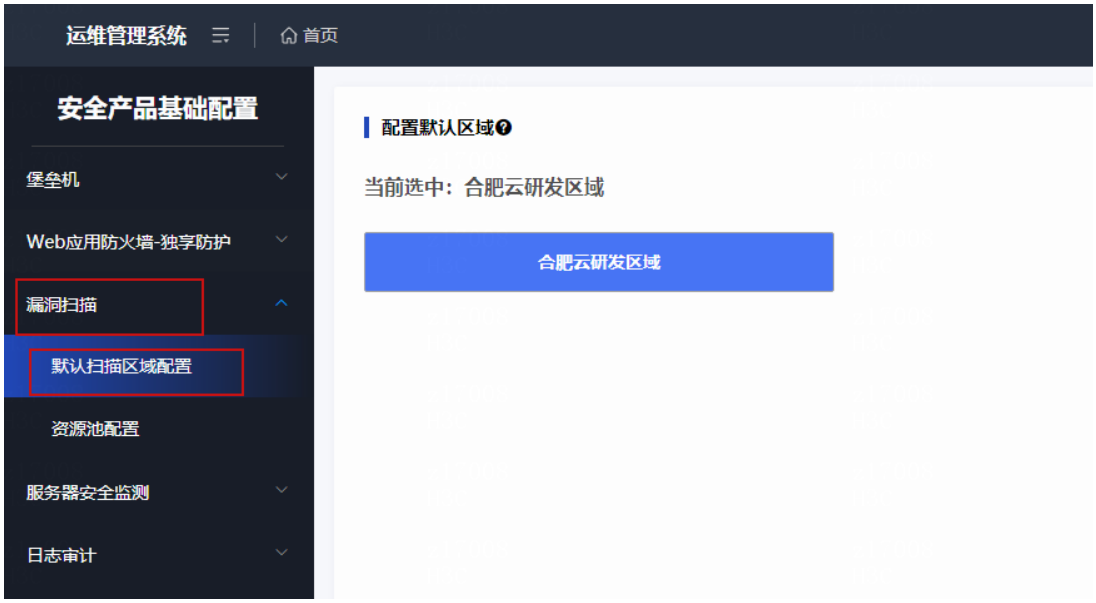
(3) 单击<提交>按钮，完成配置。

8.3.3 漏洞扫描

1. 配置默认地域

当前漏洞扫描产品购买时不区分区域，但漏扫服务器部署时会选择一个默认区域进行部署。且在使用漏洞扫描服务前，需配置漏洞扫描的默认地域，否则订单无法交付成功。

(1) 访问“安全产品基础配置 > 漏洞扫描 > 默认扫描区域配置”页面。



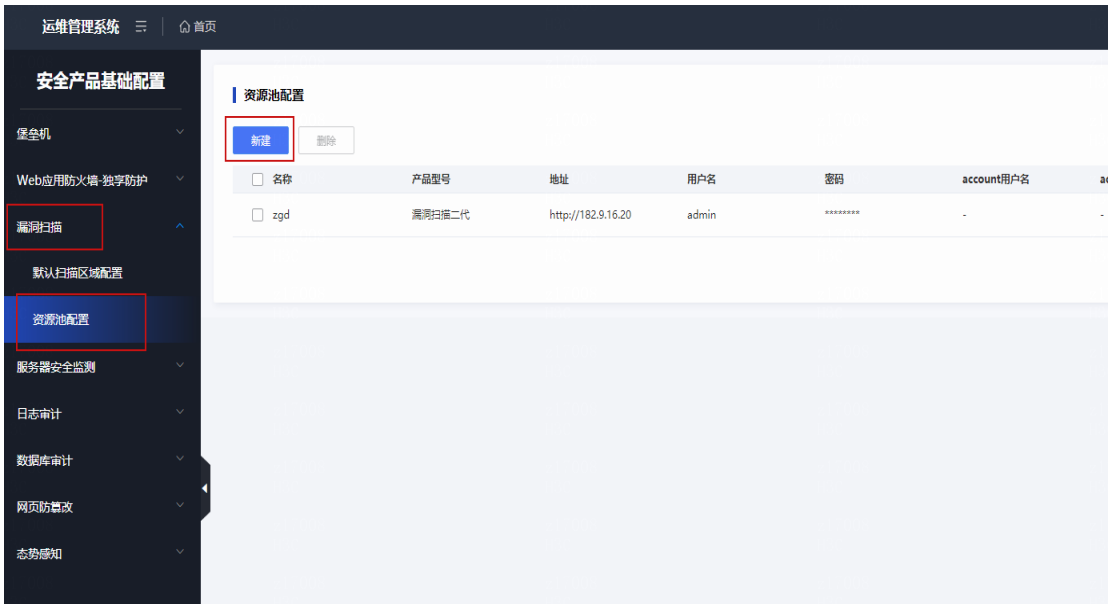
(2) 选择地区，完成配置。

2. 配置资源池

在使用漏扫服务前，需将部署在默认地域的漏扫服务器信息添加到漏扫资源池中，否则无法使用漏洞扫描服务。

具体资源池的配置步骤如下：

(1) 访问“漏洞扫描 > 资源池配置”页面。



(2) 添加三代漏扫服务器，单击<新建>，弹出新建窗口。

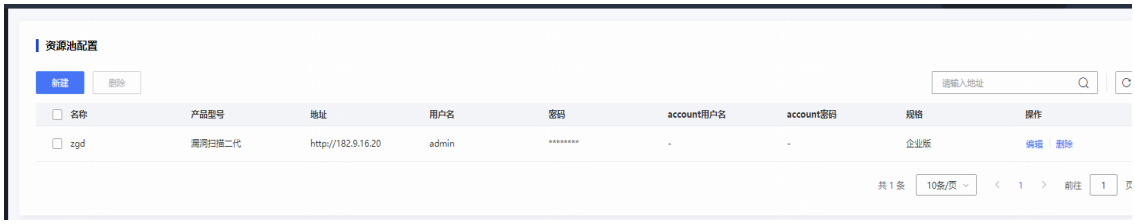
参数说明如下：

- 协议默认 https，不建议修改。
- 地址：ip 必填，为漏扫服务器 IP 地址。
- 用户名：固定为“admin”，必填。
- 密码：admin 账号对应的密码，必填。
- account 用户名：固定为“account”，必填。**查询授权相关信息时需要使用该账号**。
- account 密码：必填。
- 规格：默认为企业版，必填。
- 产品型号：漏洞扫描三代。

注意

请确保填写的参数正确。当用户正常使用各安全服务时，请勿随意对安全服务中资源池配置进行改动，以免出现异常情况。

(3) 如果添加多台，请重复上述新建操作。



8.3.4 服务器安全监测

1. 配置资源池

在使用服务前，需将服务器安全监测设备添加到资源池中。

(1) 访问“服务器安全监测 > 资源池配置”页面。

(2) 添加服务器安全设备，单击<新建>，弹出新建窗口。

参数说明如下：

- 资源名称：同一平台名称不能重复
- 规格：对应产品配置中的规格。
- 产品型号：一代，二代
- apiKey：一代自动填充，二代值获取方式如下：

a. 进入 SSMS-CLOUD 后台。

b. 执行命令 cat /home/bss/conf/hosteye.conf，API_KEY 对应的值就是需要的值。

- URL：调用接口管理设备（下图中是二代的配置，一代的协议选 http，端口改成 6000）。
- WEB URL：跳转登录设备的链接（下图中是二代的配置，一代的协议选 http，端口改成 80）。
- 管理员用户名：默认 admin。
- 终端数量：设备上授权的中的数量。

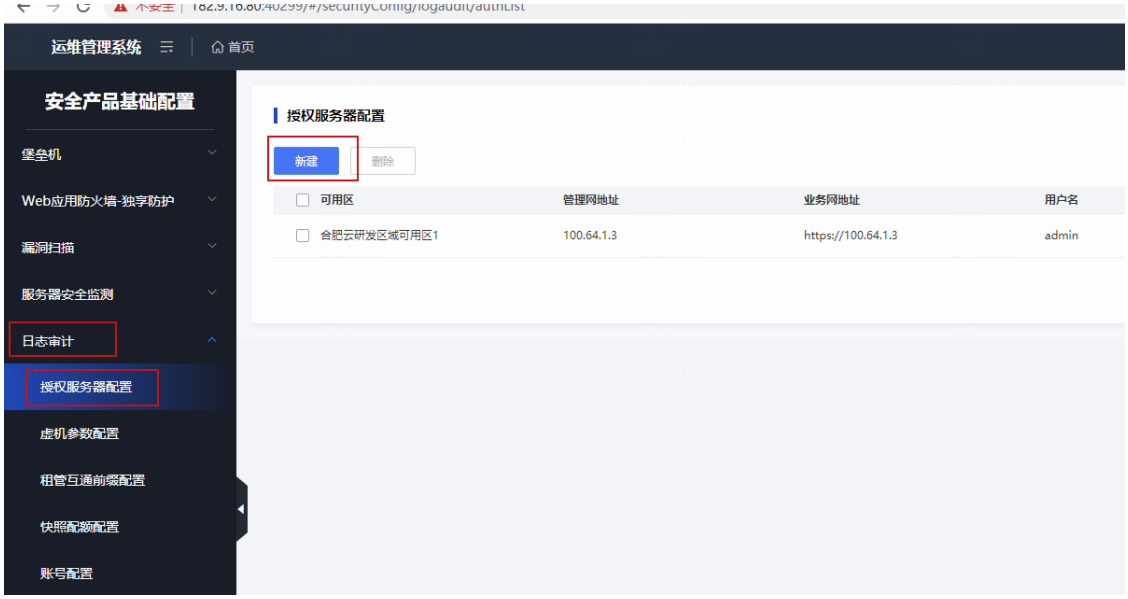
(3) 单击<确定>，完成配置。

8.3.5 日志审计

1. 授权服务器配置

在使用服务前，将部署在 DMZ 区域的授权服务器添加到资源池中，否则无法使用日志审计服务。具体配置步骤如下：

(1) 访问“日志审计 > 授权服务器配置”页面。



(2) 添加授权服务器，单击<新建>，弹出新建窗口。

参数说明如下：

- 可用区：选择授权服务器所在 az。
- 管理网地址：授权服务器与管理交互的管理 IP，单网卡下和业务网地址的 ip 相同。
- 业务网地址：
  - 协议默认 http、https 均可，无特殊要求，必填。
  - 地址：ip+端口，必填。Ip 为授权服务器与业务区交互的 IP；端口为部署授权服务器时指定的 client 和 server 的通信端口，默认是 5555。**注意：非 web 页面登录 port**。
- 用户名：管理员登录授权服务器页面的用户名。
- 密码：管理员登录授权服务器页面的密码。

(3) 点击<提交>，完成配置。

注意

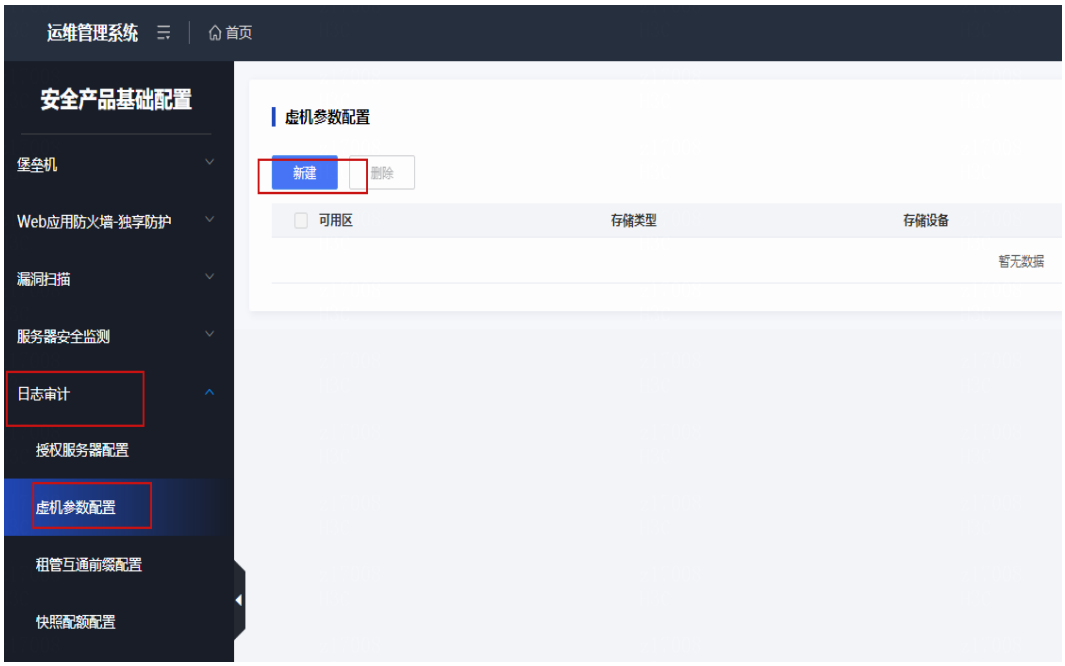
- 确保填写参数正确，当用户正常使用各安全服务时，请勿随意对各安全服务中资源池配置进行改动，以免出现异常情况。
- 授权服务器配置区分区域，不同区域的授权服务器需要单独配置。

2. 虚机磁盘参数配置

默认使用从云存储中读取到的磁盘参数。如果要求使用指定的磁盘参数，或者指定使用 Local 存储类型，需要进行此参数配置

按照如下步骤配置虚机磁盘相关参数。

(1) 访问“安全产品基础配置 > 日志审计 > 虚机参数配置”页面.



(2) 单击<新建>按钮，弹出新建窗口。

参数说明如下：

- 可用区：从当前区域下可用区列表中选择。
- 存储方式：区分本地模式与共享存储模式。
- 存储类型：当前云平台支持共享存储类型为（SDS、3par）。
- 存储设备：根据存储类型过滤出存储设备。
- 磁盘规格：选择存储设备所支持的磁盘规格。

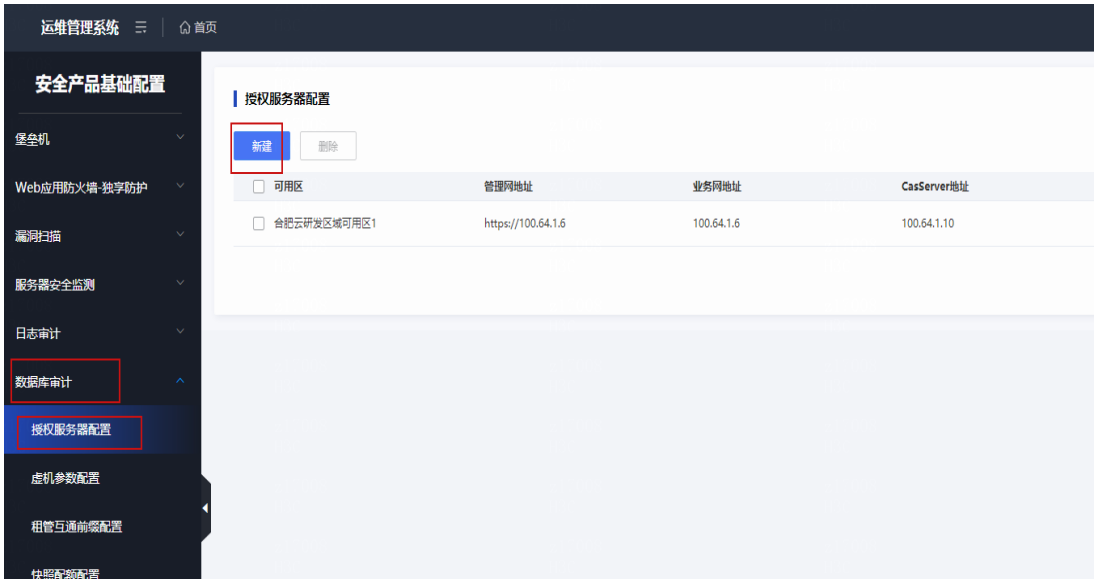
(3) 单击<提交>按钮，完成配置。

8.3.6 数据库审计

1. 授权服务器配置

在使用服务前，需在页面上配置部署在 DMZ 区的授权服务器，否则无法使用数据库审计服务。具体配置步骤如下：

(1) 访问“数据库审计 > 授权服务器配置”页面。



(2) 单击<新建>按钮，弹出新建窗口。

参数说明如下：

- 可用区：选择授权服务器所在 AZ。
- 管理网地址：默认 https,授权服务器管理网地址。
- 业务网地址：授权服务器业务网地址，标准方案中授权服务器只有一个地址，此时可填写该地址。
- CasServer 地址：DMZ 区 CasServer 虚拟机地址。
- CasServer 端口：DMZ 区 CasServer 服务端口，默认 9999。

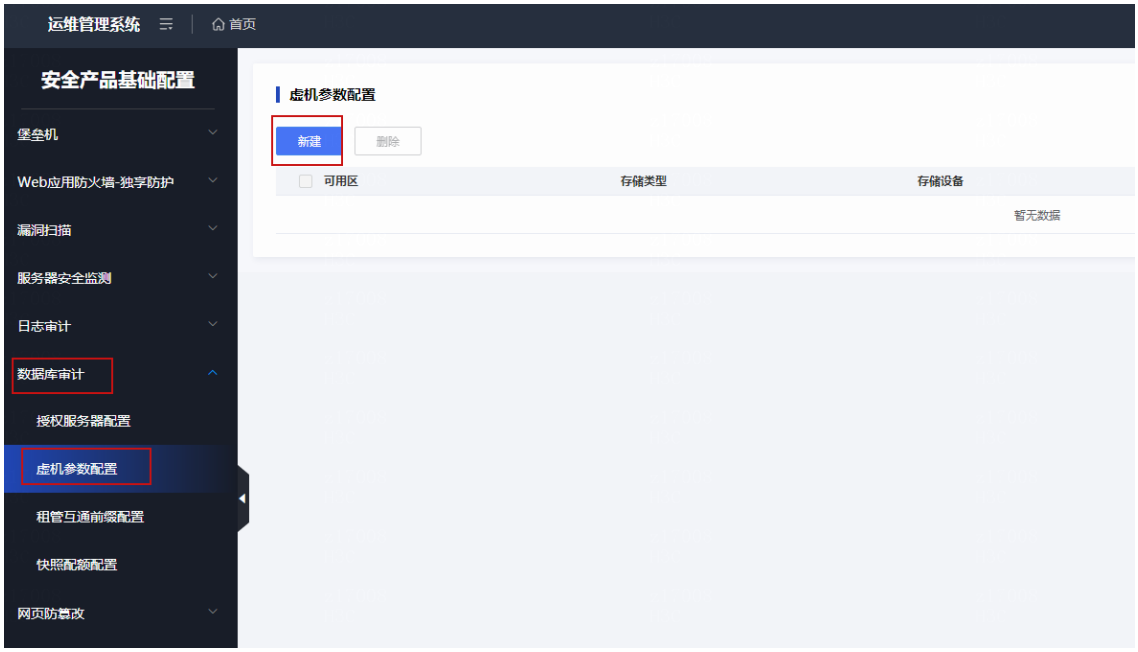
(3) 单击<提交>，完成配置。

2. 虚机磁盘参数配置

默认使用从云存储中读取到的磁盘参数。如果要求使用指定的磁盘参数，或者指定使用 Local 存储类型，需要进行此参数配置

按照如下步骤配置虚机磁盘相关参数。

(1) 访问“安全产品基础配置 > 数据库审计 > 虚机参数配置”页面.



(2) 单击<新建>按钮，弹出新建窗口。

参数说明如下：

- 可用区：从当前区域下可用区列表中选择。
- 存储方式：区分本地模式与共享存储模式。
- 存储类型：当前云平台支持共享存储类型为（SDS、3par）。
- 存储设备：根据存储类型过滤出存储设备。
- 磁盘规格：选择存储设备所支持的磁盘规格。

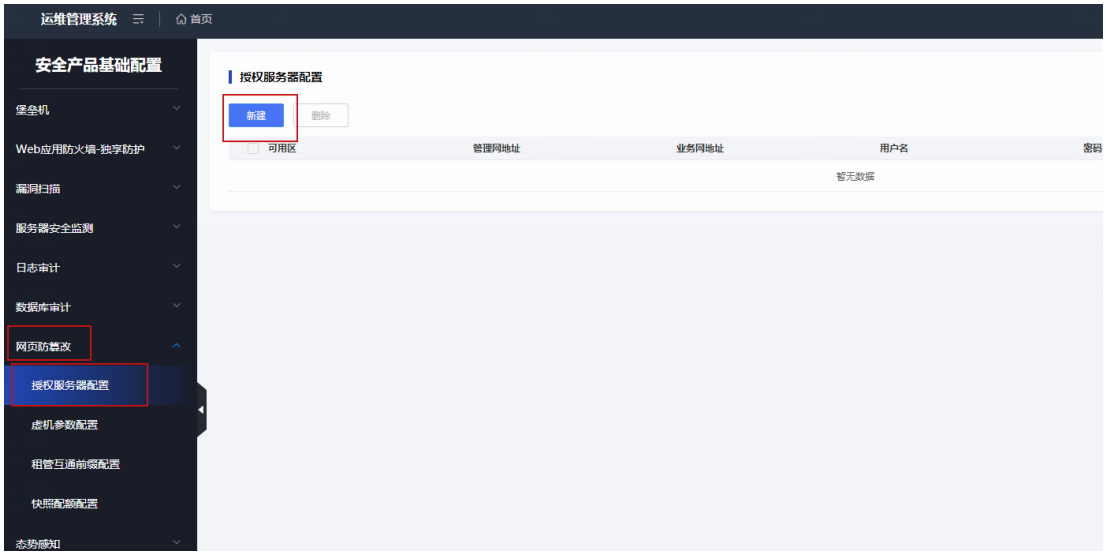
(3) 单击<提交>按钮，完成配置。

8.3.7 网页防篡改

1. 授权服务器配置

按照如下步骤配置授权服务器。

(1) 访问“安全产品基础配置 > 网页防篡改 > 授权服务器配置”页面。



(2) 单击<新建>按钮,弹出新建输入框

参数说明如下：

- 可用区：从当前区域下可用区列表中选择。
- 管理网地址：授权服务器管理网地址。
- 业务网地址：授权服务器业务网地址，标准方案中授权服务器只有一个地址，此时可填写该地址。
- 用户名：授权服务器管理页面的用户名。
- 密码：授权服务器管理页面的密码。

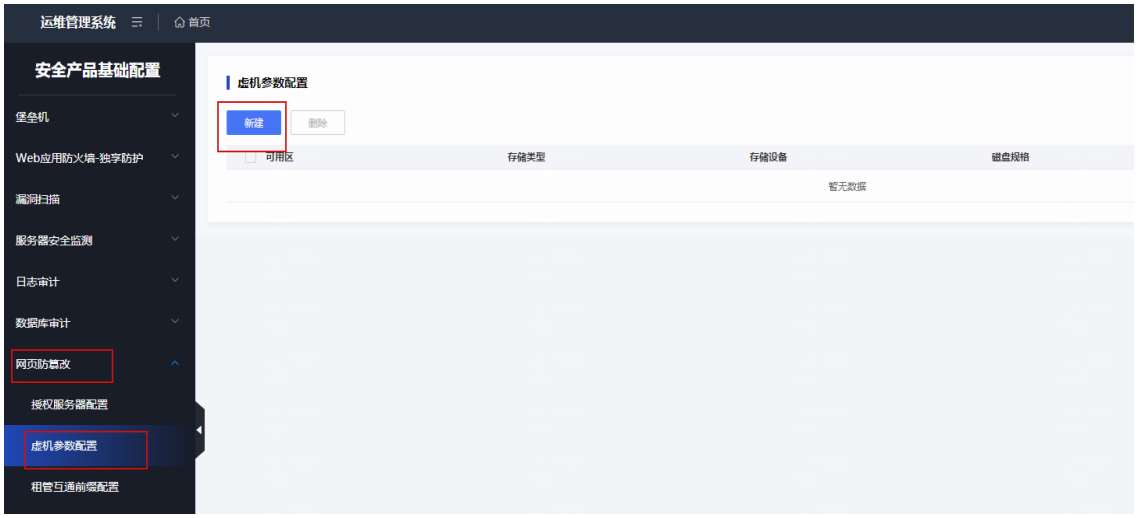
(3) 单击<提交>按钮，完成配置。

2. 虚机磁盘参数配置

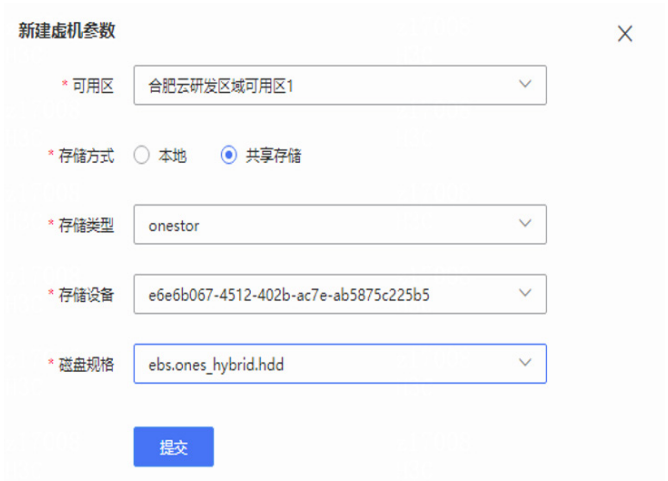
默认使用从云存储中读取到的磁盘参数。如果要求使用指定的磁盘参数，或者指定使用 Local 存储类型，需要进行此参数配置

按照如下步骤配置虚机磁盘相关参数。

(1) 访问“安全产品基础配置 > 网页防篡改 > 虚机参数配置”页面。



(2) 单击<新建>按钮，弹出新建窗口。



参数说明如下：

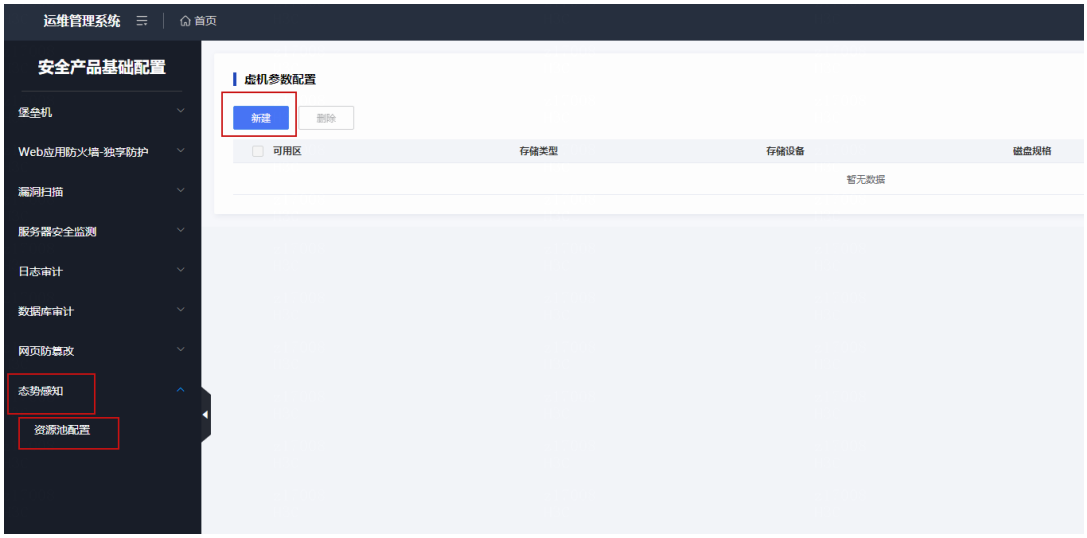
- 可用区：从当前区域下可用区列表中选择。
- 存储方式：区分本地模式与共享存储模式。
- 存储类型：当前云平台支持共享存储类型为（SDS、3par）。
- 存储设备：根据存储类型过滤出存储设备。
- 磁盘规格：选择存储设备所支持的磁盘规格。

(3) 单击<提交>按钮，完成配置。

8.3.8 态势感知

1. 配置资源池

(1) 访问“态势感知 > 资源池配置”页面。



(2) 添加态势感知设备，单击<新建>，弹出新建窗口。

参数说明如下：

- 地址：协议 https，地址是态势感知的地址。
- 名称：态势感知
- 用户名：admin
- 密码：admin
- 服务上限：最大能开通的态势感知数量。
- 同步租户地址：态势感知的地址。
- 同步资产地址：如果是集群版，则地址为 syber4 的地址；如果是单机版，则是态势感知的地址。端口默认 9999
- 同步系统地址：态势感知的地址。
- 域名地址：态势感知系统配置的域名。

(3) 单击<确定>。

9 管区服务一键开关机

组件及服务部署完毕后，可使用管区服务一键开关机轻松实现虚拟机开关机操作。脚本支持重复执行，开关机集群前都会检测集群是否已经开启或关闭，重复执行不会导致集群异常。

一键开关机工具主要针对管区 UCA、UCO、OMC、TAAG、DMZ 的 K8S 集群虚机、MySQL 集群虚机和 Replication Manager 节点虚机、Redis 集群虚机、PostgreSQL 集群虚机进行统一的开关机管理，确保使用此脚本对管区各个服务集群进行开关机重启后均能正常提供服务，不出现集群 VIP 不可用或者个别服务无法访问的情况。

9.1 注意事项

- 不支持直接使用此脚本开机

  脚本执行集群关机过程中会记录必要的集群关机前的必要信息，如：主从节点的 IP、vmid 信息等到本地，若未使用本工具关机或因其他意外断电集群关机，直接使用本工具开机可能会出现无法开机的情况。
- 不支持穿插其他手动操作

  此脚本工具只负责管理使用本脚本开关机各集群后服务正常访问使用，其他途径手动开关虚机导致服务异常不在此脚本工具处理范围。

9.2 工具构成

此脚本工具主要包括 3 个文件：dominator-v3.3.3、dominator.yml 和 dominator.db。请从 Rebirth 虚机的如下目录获取：/root/tools/dominator。

文件说明如下。

文件	说明
dominator-v3.3.3	可执行文件，需要赋予可执行权限。
dominator.yml	配置管区Usphere服务器的地址及中间件登录信息等，需要根据项目实际环境进行修改。 ⚠ 注意 具体项目中，务必要根据实际情况修改 dominator.yml 配置文件中的底座 IP 和虚拟机所在 Usphere 地址以及账号信息（参见图 5-24）。 若 DMZ 和其他 K8S 集群不在同一套 Usphere，需分别维护，单独处理。
deployDetails.json（可选）	服务虚机的规划信息，与基座共用。可配置资源地址（http://xxx/deployDetails.json）。
dominator.db	本地数据文件，用于记录节点虚机相关信息，自动生成，使用过程中无需过多关注。

图9-1 修改 dominator.yml 文件信息

9.3 执行脚本

(1) 在 Rebirth 虚拟机中执行如下命令，赋予可执行权限。

```
chmod a+x dominator-v3.3.3
```

(2) 调整配置（dominator.yml）：

- deploy.setting.path：服务虚机的规划信息，与基座共用。可配置资源地址（http://xxx/deployDetails.json），需要根据现场环境调整。
- cas.*：Usphere 平台 admin 账号配置，用于操作虚拟机，需要根据现场环境调整。

(3) 执行一键开关机脚本：

```
./dominator-v3.3.3
```

请根据提示选择对应的集群类型和操作类型（可使用数字代替），按<Enter>键确认，脚本工具会自动执行对应操作。具体运行日志会同步输出在控制台以及同目录下“dominator_xx.log”文件。

示例如下：

```
[root@Ansible dominator]# ./dominator-v3.3.3
********** 一键开关机脚本 **********
请输入服务类型：all(0)/redis(1)/mysql(2)/pgsql(3)/k8s(4)/dmz(5)/exit(-1)
k8s
请输入K8S服务类型：all(0)/uco(1)/uca(2)/omc(3)/taag(4)/exit(-1)
uco
请输入操作类型：shutdown(1)/startup(2)/restart(3)/exit(-1)
shutdown
```

10 数据备份

10.1 备份准备

在执行数据备份前，请确保数据备份相关路径为正常状态，否则可能导致备份失败。

在 Rebirth 虚机进行如下操作：

(1) 使用共享卷保证数据备份的可靠性，空间大小 1T，挂载点为/unicloud_backup。

(2) 创建数据备份相关路径。

系统默认已创建数据备份相关路径，但在挂载共享存储后，需要重新创建。

```
/unicloud_backup/{mysql_data,pgsql_data,redis_data,etcd_data/{uca,uco,omc,taag,dmz}
}
```

(3) 查看并确认已存在/unicloud_backup 目录。

```
/unicloud_backup
├── etcd_data
│   ├── dmz
│   ├── omc
│   ├── taag
│   ├── uca
│   └── uco
├── mysql_data
└── pgsql_data
└── redis_data
```

10.2 自动备份策略

选择自动备份后，系统将在指定的时间对 MySQL 和 etcd 进行自动备份。周日进行全量备份，周一至周六进行增量备份。建议启用自动备份策略。

(1) 选择[数据备份/自动备份策略]菜单项，设置备份服务状态为开启，并填写备份时间点。

图10-1 自动备份设置

(2) 填写完成后，单击<执行>按钮即可。

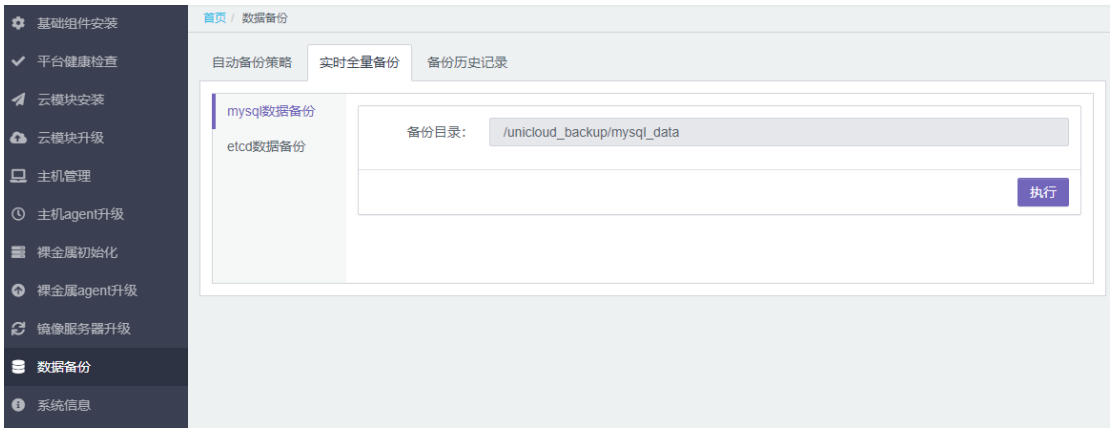
10.3 实时全量备份

实时全量备份，即点击执行按钮后，系统立即对 MySQL 或 etcd 进行全量备份操作。

10.3.1 MySQL 数据备份

(1) 选择[数据备份/实时全量备份/mysql 数据备份]菜单项，进入 MySQL 数据备份页面。

图10-2 实时全量备份设置

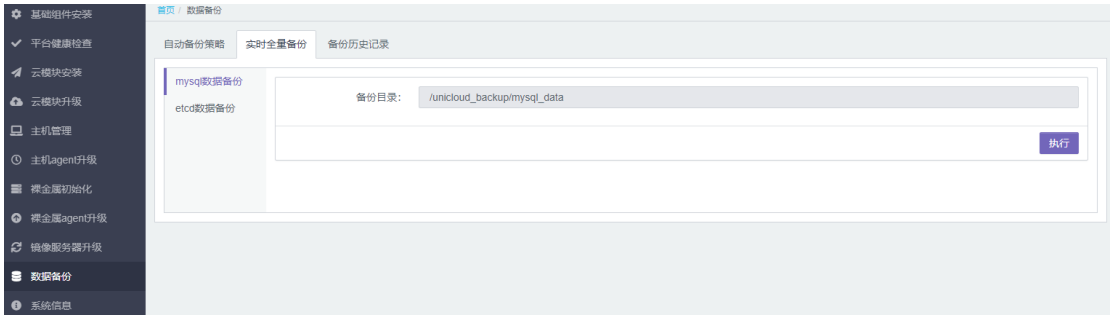


(2) 确认无误后，单击<执行>按钮。

10.3.2 etcd 全量备份

(1) 选择[数据备份/实时全量备份/etcd 数据备份]菜单项，进入 etcd 数据备份页面。

图10-3 实时全量备份设置



(2) 确认无误后，单击<执行>按钮。

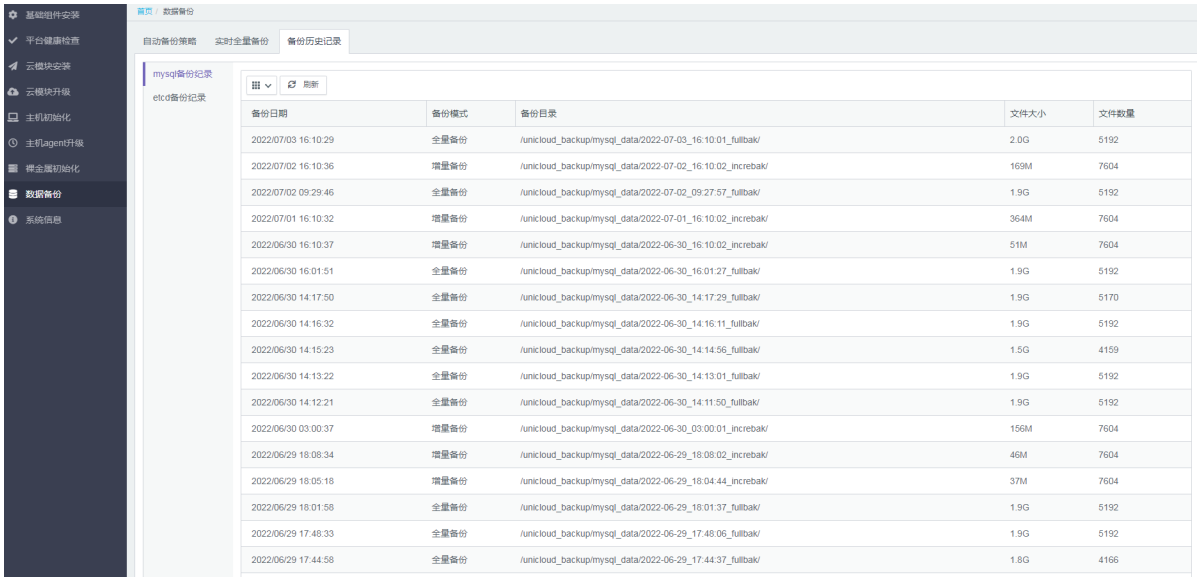
10.4 备份历史记录

备份历史记录页面可以查看到历史备份的日期、备份模式、备份目录、文件大小和文件数量信息。

1. MySQL 备份记录

选择[数据备份/备份历史记录/mysql 备份记录]菜单项，进入 MySQL 数据备份记录页面。

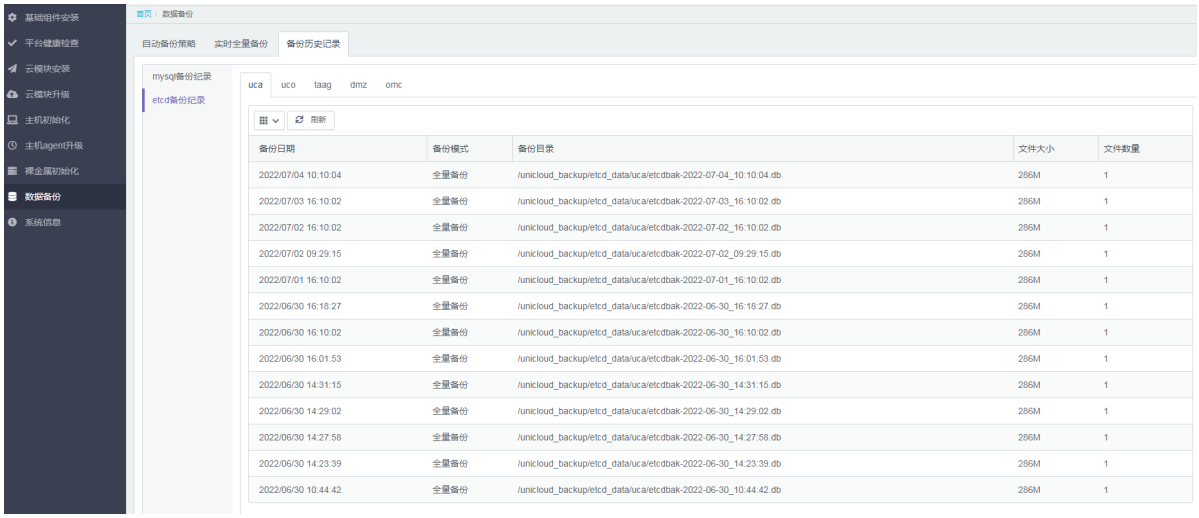
图10-4 MySQL 备份历史记录



2. etcd 备份记录

选择[数据备份/备份历史记录/etcd 备份记录]菜单项，进入 etcd 数据备份记录页面。

图10-5 etcd 备份历史记录

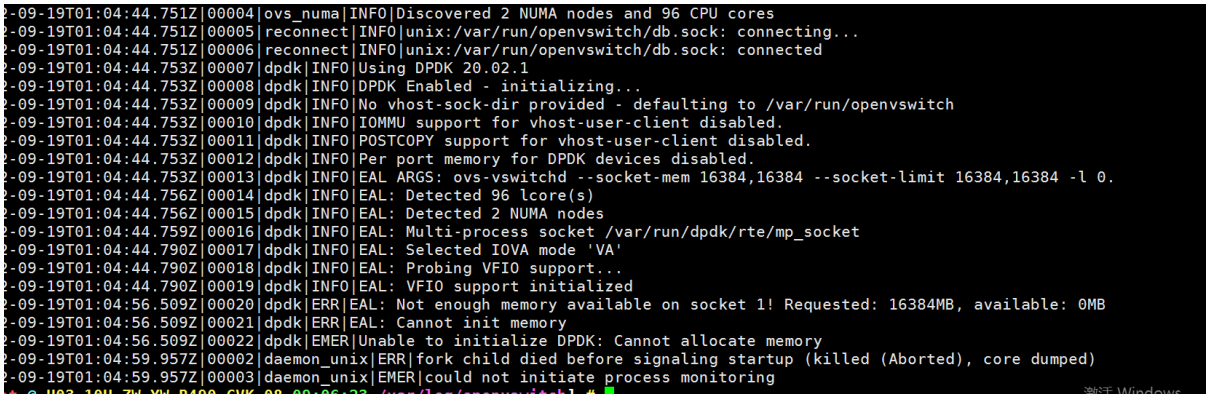


11 常见问题

11.1 如何查看业务区VKS中虚拟机网卡DPDK绑定失败原因？

进入虚拟机日志文件，查看日志：/var/log/openvswitch/ovs-vswitchd.log

通过日志可以查看具体的失败原因，例如 CPU1 未分配到大页内存等。



11.2 如何调整业务区VKS大页内存？

缩减 OVS 占用大页内存操作步骤：

(1) 查看系统空闲大页内存，如下显示 24GB。

```
cat /proc/meminfo | grep HugePages_Free
HugePages_Free:       24
```

(2) 修改 OVS 数据库，降低内存占用，将原先 16+16=32GB 改为 8+8=16GB。

```
ovs-vsctl --no-wait set Open_vSwitch . other_config:dpdk-socket-mem="8192,8192"
```

(3) 修改 OVS 的服务配置文件，降低内存占用，将原先 16+16=32GB 改为 8+8=16GB。

```
sed -i  "s/16384/8192/g" /etc/rc.d/init.d/openvswitch
```

(4) 重载 OVS 的服务配置文件。

```
systemctl daemon-reload
```

(5) 重启 OVS，以使缩减内存的配置生效，命令大约执行 30 秒左右，此时可以会导致业务断流，建议在 VKS 初始化时调整。

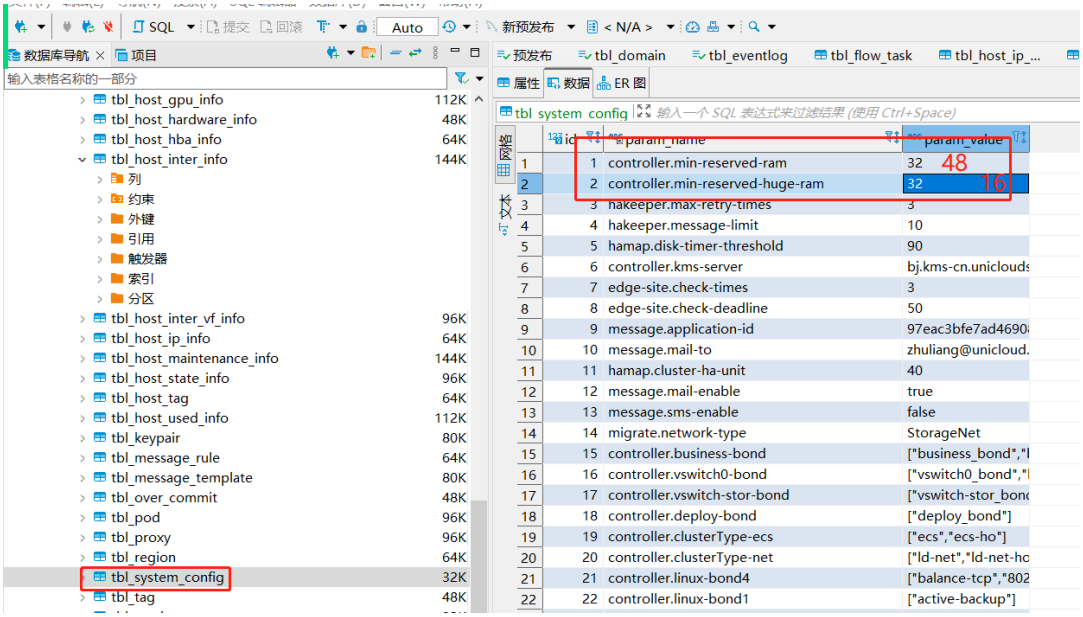
```
systemctl restart openvswitch
```

(6) 查看系统空闲大页内存，如下显示 40GB，多出了 16GB。

```
# cat /proc/meminfo | grep HugePages_Free
HugePages_Free:       40
```

(7) 在 uni-compute 数据库中，按照如下图，对 tbl_system_config 表中的如下参数进行调整：

- controller.min-reserved-ram：调整为 48。
- controller.min-reserved-huge-ram：调整为 16。

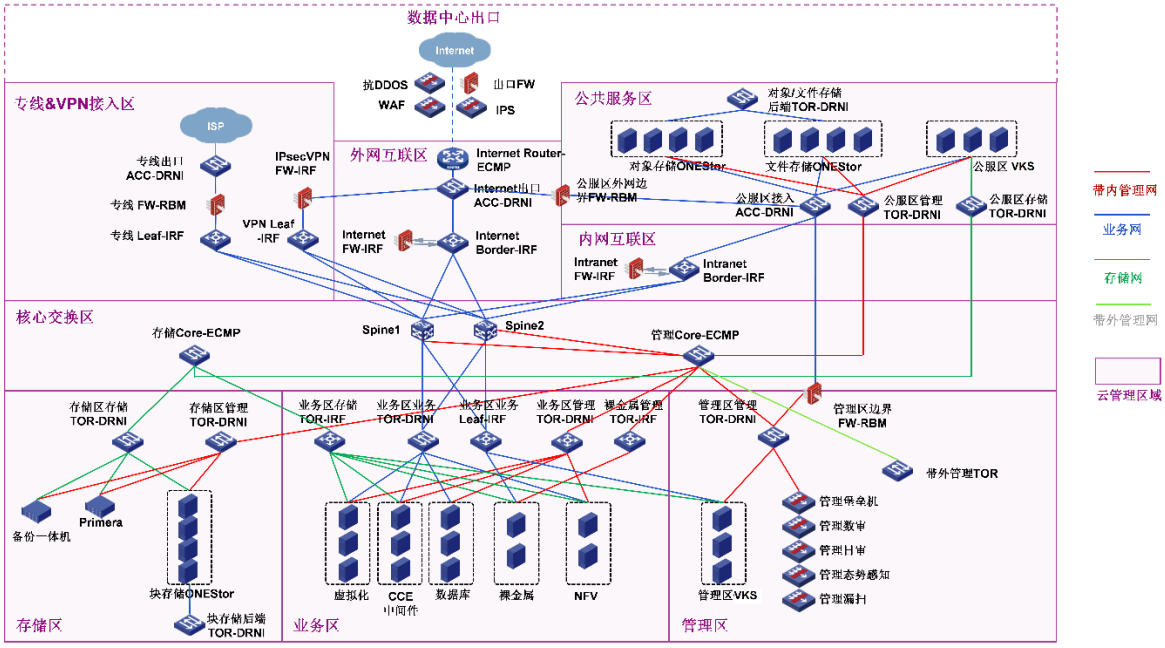

tbl_host_gpu_info 112K
tbl_host_hardware_info 48K
tbl_host_hba_info 64K
tbl_host_inter_info 144K
列
约束
外键
引用
触发器
索引
分区
tbl_host_inter_vf_info 96K
tbl_host_ip_info 64K
tbl_host_maintenance_info 144K
tbl_host_state_info 96K
tbl_host_tag 64K
tbl_host_used_info 112K
tbl_keypair 80K
tbl_message_rule 64K
tbl_message_template 80K
tbl_over_commit 48K
tbl_pod 96K
tbl_proxy 96K
tbl_region 64K
tbl_system_config 32K
tbl_tag 48K
tbl_system_config
id
param_name
param_value
1 controller.min-reserved-ram 32
2 controller.min-reserved-huge-ram 32
3 hakeeper.max-retry-times 3
4 hakeeper.message-limit 10
5 hamap.disk-timer-threshold 90
6 controller.kms-server bj.kms-cn.unicloud
7 edge-site.check-times 3
8 edge-site.check-deadline 50
9 message.application-id 97eac3bfe7ad4690
10 message.mail-to zhuliang@unicloud.
11 hamap.cluster-ha-unit 40
12 message.mail-enable true
13 message.sms-enable false
14 migrate.network-type StorageNet
15 controller.business-bond ["business_bond","
16 controller.vswitch0-bond ["vswitch0_bond","
17 controller.vswitch-stor-bond ["vswitch-stor_bon
18 controller.deploy-bond ["deploy_bond"]
19 controller.clusterType-ecs ["ecs","ecs-ho"]
20 controller.clusterType-net ["ld-net","ld-net-ho
21 controller.linux-bond4 ["balance-tcp","802
22 controller.linux-bond1 ["active-backup"]
48
16

目 录

附录A 单 AZ 标准部署模式

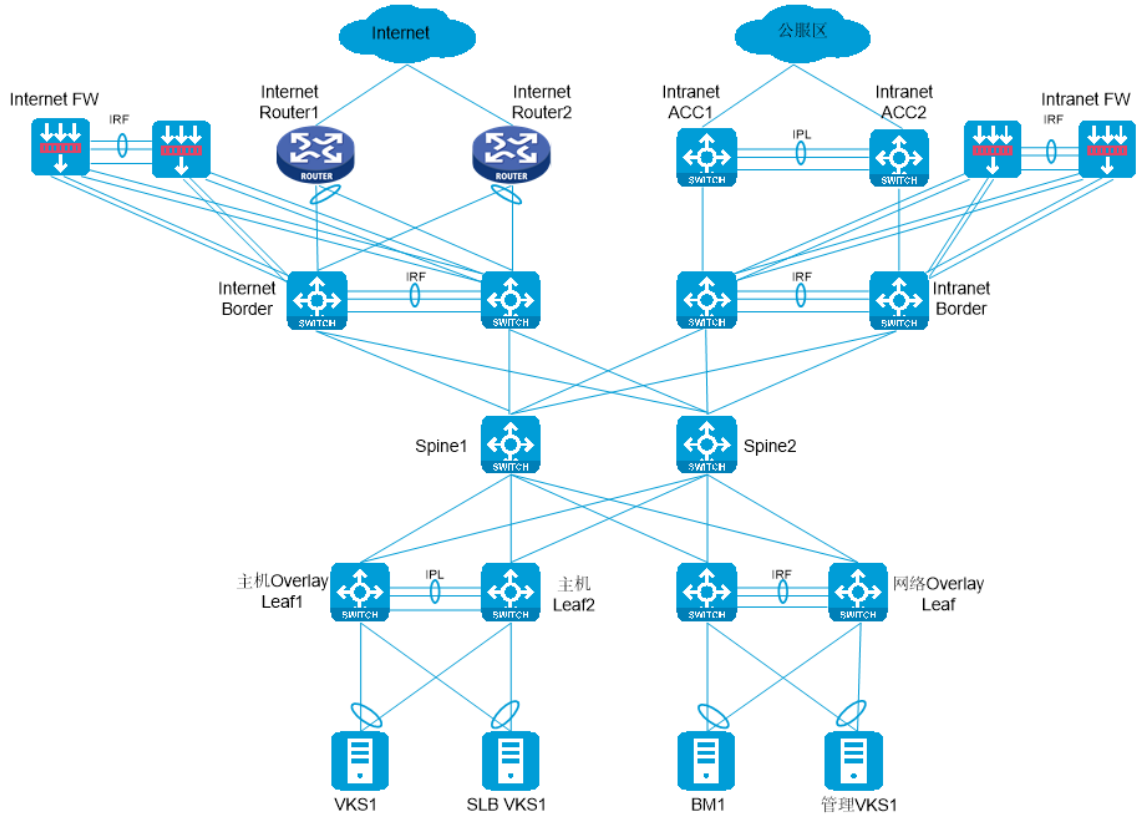
A.1 组网图

图A-1 单 AZ 标准部署模式组网图



A.2 设备接口连线图

图A-2 单 AZ 标准部署设备连线图



A.3 地址规划

A.3.1 网络 IP 地址池规划

表A-1 网络 IP 地址池规划

网络名称	IP 地址段	描述
网络设备带外管理地址	192.166.0.0/16	网络设备MGE口管理 IP地址
网络设备带内管理地址 loopback 1	10.92.54.0/24	【可选项】不配置时使用MGE口地址进行网络设备纳管；配置网络设备loopback1口与云平台管理区打通时，可用该地址进行网络设备的纳管（本文档未配置该地址）
虚拟防火墙管理地址1	10.92.30.0/24	Internet FW硬件防火墙设备context虚拟防火墙管理地址，用于对接SDN下发配置
虚拟防火墙管理地址2	10.92.31.0/24	Intranet FW硬件防火墙设备context虚拟防火墙管理地址，用于对接SDN下发配置
租户承载网1	10.92.32.0/21	Internet Border与Internet FW下行口之间租户VRF互联IP地址段，用于Internet Border解封装VXLAN报文后发送到Internet FW
租户承载网2	10.92.40.0/21	Intranet Border与Intranet FW下行口之间租户VRF互联IP地址段，用于Intranet Border解封装VXLAN报文后发送到

网络名称	IP 地址段	描述
		Intranet FW
安全外网1	10.92.56.0/24	Internet Border与Internet FW上行口之间互联IP地址段，Internet FW去往Internet业务underlay下一跳地址
安全外网2	10.92.57.0/24	Intranet Border与Intranet FW上行口之间互联IP地址段，Intranet FW去往公服区业务underlay下一跳地址
loopback 0（VTEP）	10.92.50.0/24	交换机、路由器、防火墙等设备上的loopback 0，兼做VTEP地址。被纳管网络设备均需要配置该地址
VKS vlan30（VTEP）	10.92.52.0/24	虚拟化VKS和主机overlay leaf互联的VTEP地址。每增加一组主机overlay leaf就需要增加一个网段
VKS vlan30（VTEP）	10.92.54.0/24	虚拟化VKS和主机overlay leaf互联的VTEP地址。每增加一组主机overlay leaf就需要增加一个网段
业务网互联IP地址	10.92.51.0/24	交换机、路由器、防火墙等设备的互联IP地址，每条点对点链路使用30位掩码
管理网互联IP地址	10.92.53.0/24	交换机、路由器、防火墙等设备的互联IP地址，每条点对点链路使用30位掩码

A.3.2 假公网地址规划

表A-2 假公网地址池规划

使用范围	IP 地址段	描述
公服区业务地址	100.66.1.0/24	公服区服务器业务网卡IP，如对象存储网关地址。该网段的网关需要和Intranet NAT网段的网关打通
租管互通地址	100.100.0.0/18 （一般不建议修改）	vLB、RDS虚机第二块虚拟管理网卡、Nginx业务IP（管理服务器业务网卡）。用于租管互通云平台给PAAS类虚拟机下发配置
Intranet NAT地址	100.66.4.0/22	租户假公网NAT网关IP地址，用于租户访问公服区业务做SNAT
预留	100.66.3.0/24	预留IP地址

A.3.3 网络设备地址规划

表A-3 网络设备地址规划

设备名称	带外管理地址	VTEP 地址
Internet Border	192.166.0.1	10.92.50.1
Intranet Border	192.166.0.2	10.92.50.2
Internet FW	192.166.0.81	10.92.50.81
Intranet FW	192.166.0.82	10.92.50.82
Spine1	192.166.0.77	10.92.50.77

设备名称	带外管理地址	VTEP 地址
Spine2	192.166.0.78	10.92.50.78
主机overlay Leaf1-1	192.166.0.11	10.92.50.11
主机overlay Leaf1-2	192.166.0.12	10.92.50.12
网络overlay Leaf	192.166.0.13	10.92.50.13
专线Leaf	192.166.0.101	10.92.50.101
Router1	192.166.0.73	10.92.50.73
Router2	192.166.0.74	10.92.50.74

A.4 网络设备及用途介绍

设备角色	是否必选	设备用途	支持型号	可靠性方式
Internet Border	必选	Internet出口边界网关，Internet业务VXLAN终结	S6800	IRF
Internet FW	必选	Internet业务公网地址NAT，防火墙安全过滤	M9000 F50X0 D	IRF
Spine	必选	核心汇聚设备，EVPN路由反射器	S125X S9800	ECMP
网络overlay Leaf	必选	1. 租管互通 VTEP 节点 2. 网络 Overlay 业务（如裸金属）VTEP 接入和分布式网关，VXLAN 封装	S6800	IRF
主机overlay Leaf	必选	主机Overlay VXLAN业务下一跳设备，转发到Spine	S6800	DRNI
Router	必选	Internet出口业务限速和流量统计	SR88	ECMP
			SR66	ECMP
Intranet Border	公共服务业务必选	公共服务&DMZ区边界网关，公共服务业务VXLAN终结	S6800	IRF
Intranet FW	公共服务业务必选	公共服务业务假公网地址映射，防火墙安全过滤	M9000	IRF
			F50X0	IRF
专线Leaf	专线业务必选	专线业务VTEP接入接入和分布式网关，VXLAN封装	S6800	IRF
专线FW	按需配置	专线业务安全防护	不限制	
出口FW、抗ddos等互联网出口设备	按需配置	Internet业务出口安全防护	不限制	

设备角色	是否必选	设备用途	支持型号	可靠性方式
存储交换机	必选	存储业务转发	S6800	
管理交换机	必选	管理业务转发	S6800	

A.5 网络设备基础配置模板

A.5.1 堆叠设备配置模板

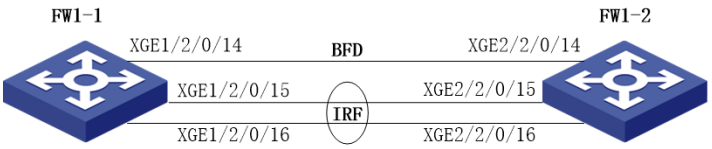
1. 组网图

此处以 M9K FW 作为介绍。

FW1-1 和 FW1-2 组成 IRF，名称为 FW1。FW1-1 与 FW1-2 之间两条直连链路聚合（XGE1/2/0/15、XGE2/2/0/15、XGE1/2/0/16、XGE2/2/0/16）作为 IRF 堆叠链路，FW1-1 与 FW1-2 之间一条直连链路（XGE1/2/0/14、XGE2/2/0/14）作为 MAD 检测链路。

登录 FW1-1 和 FW1-2 的 console 口，先配置堆叠，再配置管理口等。

图A-3 堆叠设备组网



2. 设备配置

(1) FW 1-1 IRF 配置

- FW1-1 设备切换为 IRF 模式。（不需要切换模式的设备不用此步）

```
[H3C] chassis convert mode irf
The device will switch to IRF mode and reboot.
You are recommended to save the current running configuration and specify the configuration file for the next startup. Continue? [Y/N]:Y
Do you want to convert the content of the next startup configuration file flash:/startup.cfg to make it available in IRF mode? [Y/N]:Y
Now rebooting, please wait...
```

设备启动成功后，查看 IRF 的初始配置命令如下：

```
irf mac-address persistent always
 irf auto-update enable
 irf auto-merge enable
 undo irf link-delay
 irf member 1 priority 1
```

- FW1-1 设备配置 IRF 成员优先级。由于 IRF 成员优先级缺省是 1，需要修改。

```
[H3C] irf member 1 priority 32
```

- FW1-1 设备配置 IRF domain

```
[H3C] irf domain 1
```

- FW1-1 设备配置 IRF-port

```
[H3C] interface Ten-GigabitEthernet1/2/0/15
[H3C-Ten-GigabitEthernet1/2/0/15] shutdown
[H3C-Ten-GigabitEthernet1/2/0/15]interface Ten-GigabitEthernet1/2/0/16
[H3C-Ten-GigabitEthernet1/2/0/16] shutdown
[H3C-Ten-GigabitEthernet1/2/0/16] quit
[H3C] irf-port 1/1
[H3C-irf-port1/1] port group interface Ten-GigabitEthernet 1/2/0/15
[H3C-irf-port1/1] port group interface Ten-GigabitEthernet 1/2/0/16
[H3C irf-port1/1] quit
[H3C] interface Ten-GigabitEthernet1/2/0/15
[H3C-Ten-GigabitEthernet1/2/0/15] undo shutdown
[H3C-Ten-GigabitEthernet1/2/0/15] interface Ten-GigabitEthernet1/2/0/16
[H3C-Ten-GigabitEthernet1/2/0/16] undo shutdown
[H3C] save
The current configuration will be written to the device. Are you sure? [Y/N]:Y
Please input the file name(*.cfg)[flash:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
Validating file. Please wait...
The current configuration adds 56 commands and deletes 2 commands.
The flash:/startup.cfg file already exists. The save operation will overwrite the file.
Are you sure you want to continue the save operation? [Y/N]:Y

Saving the current configuration to the file.
```

- FW1-1 设备 IRF port 配置激活。

```
[H3C] irf-port-configuration active
```

(2) FW 1-2 IRF 配置

- FW1-2 设备切换为 IRF 模式。

```
[H3C] chassis convert mode irf
The device will switch to IRF mode and reboot.
You are recommended to save the current running configuration and specify the configuration
file for the next startup. Continue? [Y/N]:Y
Do you want to convert the content of the next startup configuration file flash:/startup.cfg
to make it available in IRF mode? [Y/N]:Y
Now rebooting, please wait...
```

设备启动成功后，查看 IRF 的初始配置命令如下：

```
irf mac-address persistent always
 irf auto-update enable
 irf auto-merge enable
 undo irf link-delay
 irf member 1 priority 1
```

- FW1-2 设备配置 IRF 成员号

FW1-2 设备 IRF 成员号改为 2

```
[H3C] irf member 1 renumber 2
[H3C] save
The current configuration will be written to the device. Are you sure? [Y/N]:Y
Please input the file name(*.cfg)[flash:/startup.cfg]
```

```
(To leave the existing filename unchanged, press the enter key):
Validating file. Please wait...
The current configuration adds 56 commands and deletes 2 commands.
The flash:/startup.cfg file already exists. The save operation will overwrite the file.
Are you sure you want to continue the save operation? [Y/N]:Y
Saving the current configuration to the file.
[H3C] quit
<H3C> reboot force
A forced reboot might cause the storage medium to be corrupted. Continue? [Y/N]:Y
Now rebooting, please wait...
```

- FW1-2 设备配置 IRF 成员优先级。

```
[H3C] irf member 2 priority 31
```

- FW1-2 设备配置 IRF domain。

```
[H3C] irf domain 1
```

- FW1-2 设备配置 IRF-port。

```
[H3C] interface Ten-GigabitEthernet2/2/0/15
[H3C-Ten-GigabitEthernet2/2/0/15] shutdown
[H3C-Ten-GigabitEthernet2/2/0/15] interface Ten-GigabitEtherne 2/2/0/16
[H3C-Ten-GigabitEthernet2/2/0/16] shutdown
[H3C-Ten-GigabitEthernet2/2/0/16] quit
[H3C] irf-port 2/2
[H3C-irf-port2/2] port group interface Ten-GigabitEthernet 2/2/0/15
[H3C-irf-port2/2] port group interface Ten-GigabitEthernet 2/2/0/16
[H3C] interface Ten-GigabitEthernet2/2/0/15
[H3C-Ten-GigabitEthernet2/2/0/15] undo shutdown
[H3C-Ten-GigabitEthernet2/2/0/15] interface Ten-GigabitEthernet2/2/0/16
[H3C-Ten-GigabitEthernet2/2/0/16] undo shutdown
[H3C] save
The current configuration will be written to the device. Are you sure? [Y/N]:Y
Please input the file name(*.cfg)[flash:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
Validating file. Please wait...
The current configuration adds 56 commands and deletes 2 commands.
The flash:/startup.cfg file already exists. The save operation will overwrite the file.
Are you sure you want to continue the save operation? [Y/N]:Y
Saving the current configuration to the file.
[H3C] quit
```

- FW1-2 设备 IRF port 配置激活。

```
[H3C] irf-port-configuration active
```

(3) IRF 堆叠完成

- 在 IRF port 激活期间，在 FW1-1 和 FW1-2 这两台设备中有一台设备自动重启，重启完毕后，IRF 堆叠建立好。可用 display irf 命令查看 IRF 状态。
- 修改堆叠体的名称

```
[H3C] sysname FW1
```

```
[FW1]
```

- 管理口地址配置。

```
[FW1]interface M-GigabitEthernet1/0/0/0
[FW1-M-GigabitEthernet1/0/0/0] ip address 192.168.11.101 255.255.255.0
[FW1-M-GigabitEthernet1/0/0/0] quit
```

(4) IRF MAD 检测端口配置。

```
[FW1] interface Route-Aggregation64
[FW1-Route-Aggregation64] mad bfd enable
[FW1-Route-Aggregation64] mad ip address 192.168.2.1 24 member 1
[FW1-Route-Aggregation64] mad ip address 192.168.2.2 24 member 2
[FW1-Route-Aggregation64] interface Ten-GigabitEthernet1/2/0/14
[FW1-Ten-GigabitEthernet1/2/0/14] port link-aggregation group 64
[FW1-Ten-GigabitEthernet1/2/0/14] interface Ten-GigabitEthernet2/2/0/14
[FW1-Ten-GigabitEthernet2/2/0/14] port link-aggregation group 64
[FW1-Ten-GigabitEthernet2/2/0/14] quit
```

A.5.2 通用基础配置模板

- 设备命名，需要根据实际命名修改

```
sysname Border1
```

- 配置设备带外管理 IP，IP 地址根据规划进行配置

```
interface M-GigabitEthernet0/0/0
 ip binding vpn-instance mgmt
 ip address 192.166.0.1 255.255.0.0
```

- 设置管理用户，同时作为 netconf 配置下发的帐号，用户名、密码根据规划进行配置

```
local-user admin
 password simpel unicloud123
service-type ssh
 authorization-attribute user-role network-admin
authorization-attribute user-role network-operator
```

- 配置远程访问

```
line vty 0 63
 authentication-mode scheme
 user-role network-admin
 user-role network-operator
 idle-timeout 20 0
```

- 使能 SSH 服务

```
ssh server enable
```

- 使能 netconf ssh 服务

```
netconf ssh server enable
```

- 使能 lldp 及 stp 协议

```
lldp global enable
stp global enable
```

- 配置带内管理地址（可选配置，配置后可用该 IP 进行 SDN 设备纳管，不配置则使用 MGE 带外管理 IP 进行纳管）

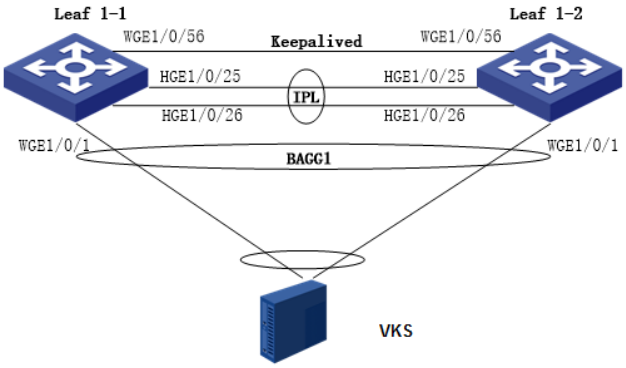
```
interface LoopBack1
 ip address 10.92.54.1 255.255.255.255
```

A.5.3 DRNI 基础配置模板

以下组网图以 Leaf 为例介绍。DRNI（Distributed Resilient Network Interconnect，分布式弹性网络互联）是一种跨设备链路聚合技术，将两台物理设备在聚合层面虚拟成一台设备来实现跨设备链路聚合，从而提供设备级冗余保护和流量负载分担。如图所示，Leaf1-和 Leaf1-2 设备形成负载分担，共同进行流量转发，当其中一台设备发生故障时，流量可以快速切换到另一台设备，保证业务的正常运行。

1. 组网图

图A-4 DRNI 基础配置组网



- DR 接口（Distributed Relay interface，分布式聚合接口）：与外部设备互联的二层聚合接口。与外部设备相连的 DR 接口属于同一 DR 组。如 Leaf1-1 和 Leaf1-2 设备与外部设备（VKS）连接的 DR 接口（WGE1/0/1）加入聚合接口 BAAG1，BAAG1 加入同一个 DR 组。
- IPP（Intra-Potal Port，内部控制链路端口）：连接对端 DR 邻居设备用于内部控制的接口，每台 DR 设备只有一个 IPP 口，IPP 之间通过 IPL 在 DR 设备间传输 DRNI 协议报文，一个 DR 系统只有一条 IPL。Leaf1-1 与 Leaf1-2 的 HGE1/0/25、HGE1/0/26 组成 BAAG100，作为 IPP 口。
- DR 设备间通过 Keepalive 链路检测邻居状态。

2. 设备配置

(1) Leaf 1-1 DRNI 系统参数配置

- DR 系统中所有 DR 设备的 system-mac 必须相同，且保证全网唯一

```
drni system-mac 0001-0001-0001
```

- 两台 DR 设备的 system-number 必须不同。可以配置第一台 DR 设备为 1，第二台为 2

```
drni system-number 1
```

- 配置 DR 设备的 system-priority 必须相同

```
drni system-priority 123
```

(2) Leaf 1-1 IPP 口配置

- 创建 IPP 聚合口

```
interface Bridge-Aggregation100
link-aggregation mode dynamic
```

- IPP 物理口添加到聚合口中

```
interface HundredGigE1/0/25
 port link-aggregation group 100
#
interface HundredGigE1/0/26
 port link-aggregation group 100
```

- IPP 聚合口配置

```
interface Bridge-Aggregation100
 port link-type trunk
 port trunk permit vlan all
 link-aggregation mode dynamic
 port drni intra-portal-port 1
 undo mac-address static source-check enable
```

(3) Leaf 1-1 DRNI MAD 配置

- 配置 DRNI MAD 恢复延迟。当 IPL 链路恢复以后，需要延迟指定时间后，链路才 MAD UP。

```
drni restore-delay 180
```

- 配置 Keepalive 报文的目的 IP 地址和源 IP 地址

```
drni keepalive ip destination 10.250.27.74 source 10.250.27.73
```

- 配置 MAD 接口为 3 层接口，并配置 IP 地址为 Keepalive 报文的源 IP 地址

```
interface Twenty-FiveGigE1/0/56
 port link-mode route
 speed 10000
ip address 10.250.27.73 255.255.255.252
```

- 配置 MAD 链路接口为保留接口

```
drni mad exclude interface Twenty-FiveGigE1/0/56
```

(4) Leaf 1-1 DRNI 业务聚合口配置

- 创建二层聚合口，加入 DRNI Group

```
interface Bridge-Aggregation1
 link-aggregation mode dynamic
 port drni group
```

- 物理接口添加到聚合口

```
interface Twenty-FiveGigE1/0/1
 port link-mode bridge
port link-aggregation group 1
```

(5) Leaf 1-2 DRNI 系统参数配置

- DR 系统中所有 DR 设备的 system-mac 必须相同，且保证全网唯一

```
drni system-mac 0001-0001-0001
```

- 两台 DR 设备的 system-number 必须不同。可以配置第一台 DR 设备为 1，第二台为 2

```
drni system-number 2
```

- 配置 DR 设备的 system-priority 必须相同

```
drni system-priority 123
```

(6) Leaf 1-2 IPP 口配置

- 创建 IPP 聚合口

```
interface Bridge-Aggregation100
link-aggregation mode dynamic
```

- IPP 物理口添加到聚合口中

```
interface HundredGigE1/0/25
 port link-aggregation group 100
#
interface HundredGigE1/0/26
 port link-aggregation group 100
```

- IPP 聚合口配置

```
interface Bridge-Aggregation100
 port link-type trunk
 port trunk permit vlan all
 link-aggregation mode dynamic
 port drni intra-portal-port 1
 undo mac-address static source-check enable
```

(7) Leaf 1-2 DRNI MAD 配置

- 配置 DRNI MAD 恢复延迟。当 IPL 链路恢复以后，需要延迟指定时间后，链路才 MAD UP。

```
drni restore-delay 180
```

- 配置 Keepalive 报文的目的 IP 地址和源 IP 地址

```
drni keepalive ip destination 10.250.27.73 source 10.250.27.74
```

- 配置 MAD 接口为 3 层接口，并配置 IP 地址为 Keepalive 报文的源 IP 地址

```
interface Twenty-FiveGigE1/0/56
 port link-mode route
 speed 10000
ip address 10.250.27.74 255.255.255.252
```

- 配置 MAD 链路接口为保留接口

```
drni mad exclude interface Twenty-FiveGigE1/0/56
```

(8) Leaf 1-2 DRNI 业务聚合口配置

- 创建二层聚合口，加入 DRNI Group

```
interface Bridge-Aggregation1
 link-aggregation mode dynamic
 port drni group
```

- 物理接口添加到聚合口

```
interface Twenty-FiveGigE1/0/1
 port link-mode bridge
port link-aggregation group 1
```

A.5.4 交换机硬件参数配置

交换机设备作为网络 overlay Leaf、Border 角色时需要修改硬件参数。各型号交换机硬件参数配置如下，配置完成后需要重启设备生效。

1. S12500X-AF

S12500X-AF 无论做 spine、leaf 或 border，其硬件资源参数，推荐使用缺省配置。

```
hardware-resource tcam routing
hardware-resource vxlan normal
hardware-resource mcast normal
hardware-resource monitor normal
hardware-resource scale-rt-prefix none
hardware-resource mpls normal
hardware-resource parser normal
```

2. S12500G

S12500G 的硬件资源参数如下：

```
<addc-net3-leaf1>dis hardware-resource
Tcam resource(tcam), all supported modes:
  NORMAL             The normal mode
  MAC                The mac mode
  ROUTING            The routing mode
  ARP                The arp mode
  DUAL-STACK         The dual-stack mode
  MIX                The mix bridging routing mode
  ENHANCE-IPV6       The enhance ipv6 mode
  ENHANCE-ARPND      The enhance arpnd mode
  ACL                The acl mode
  NAT                The nat mode
  ------------------------------------------------
  Default          Current          Next
  NORMAL           NORMAL           NORMAL

Routing-mode resource(routing-mode), all supported modes:
  ipv6-64            IPv6-64 supported
  ipv6-128           IPv6-128 supported
  ------------------------------------------------
  Default          Current          Next
  ipv6-64          ipv6-64          ipv6-64

VXLAN resource(vxlan), all supported modes:
  L2GW               The Layer 2 gateway mode
  L3GW               The Layer 3 gateway mode
  ------------------------------------------------
  Default          Current          Next
  L3GW             L3GW             L3GW
```

S12500G 做 leaf，border 或 spine 等角色时，推荐硬件参数配置如下：

```
hardware-resource tcam normal
hardware-resource routing-mode ipv6-128
hardware-resource vxlan l3gw
```

3. S6800

S6800 的硬件参数如下：

```
[S6800]hardware-resource switch-mode ?
  0  MAC table is 288K, L3 host table is 16K, LPM Table is 16K
  1  MAC table is 224K, L3 host table is 80K, LPM Table is 16K
  2  MAC table is 160K, L3 host table is 144K, LPM Table is 16K
  3  MAC table is 96K, L3 host table is 208K, LPM Table is 16K
  4  MAC table is 32K, L3 host table is 16K, LPM Table is 250K
[S6800]hardware-resource routing-mode ?
  ipv6-64   ipv6-64 supported
  ipv6-128  ipv6-128 supported
[S6800]hardware-resource vxlan ?
  l2gw       L2 gateway--underlay/overlay 48K/0K
  l3gw8k     L3 gateway--underlay/overlay 40K/8K
  l3gw16k    L3 gateway--underlay/overlay 32K/16K
  l3gw24k    L3 gateway--underlay/overlay 24K/24K
  l3gw32k    L3 gateway--underlay/overlay 16K/32K
  l3gw40k    L3 gateway--underlay/overlay 8K/40K
  border8k   Border--underlay/overlay 40K/8K
  border16k  Border--underlay/overlay 32K/16K
  border24k  Border--underlay/overlay 24K/24K
  border32k  Border--underlay/overlay 16K/32K
  border40k  Border--underlay/overlay 8K/40K
```

Leaf 角色推荐配置：

```
 hardware-resource switch-mode 4
 hardware-resource routing-mode ipv6-128
 hardware-resource vxlan l3gw40k
```

border 角色推荐配置：

```
hardware-resource switch-mode 4
 hardware-resource routing-mode ipv6-128
 hardware-resource vxlan border40k
```

4. S6805

S6805 的硬件参数如下：

```
<S6805>dis hardware-resource
Switch-mode resource(switch-mode), all supported modes:
  NORMAL            MAC table:96K,  ARP and ND tables:80K,  routing table:160K
  MAC               MAC table:288K, ARP and ND tables:16K,  routing table:32K
  ROUTING           MAC table:32K,  ARP and ND tables:16K,  routing table:324K
  ARP               MAC table:32K,  ARP and ND tables:272K, routing table:32K
  DUAL-STACK        MAC table:32K,  ARP and ND tables:16K,  routing:v4-87K,v6-86K
  EM                MAC table:32K,  ARP and ND tables:16K,  routing table:32K
  ---------------------------------------------
  Default         Current         Next
  NORMAL          ROUTING             ROUTING
Routing-mode resource(routing-mode), all supported modes:
  ipv6-64           ipv6-64 supported
  ipv6-128          ipv6-128 supported
  ---------------------------------------------
  Default         Current         Next
```

```
  ipv6-64         ipv6-64         ipv6-64
Vxlan resource(vxlan), all supported modes:
  l2gw              L2 gateway--underlay/overlay 64K/0K
  l3gw              L3 gateway--underlay/overlay 24K/40K
  ------------------------------------------------
  Default         Current         Next
  l2gw            l3gw            l3gw
```

S6805 做 leaf，border 或 spine 等角色时，推荐硬件参数配置如下：

```
 hardware-resource switch-mode ROUTING
 hardware-resource routing-mode ipv6-128
 hardware-resource vxlan l3gw
```

5. S6850/S9850

```
<addc-net3-leaf2-1>dis hardware-resource
Switch-mode resource(switch-mode), all supported modes:
  NORMAL            MAC table:96K,  ARP and ND tables:80K,  routing table:160K
  MAC               MAC table:288K, ARP and ND tables:16K,  routing table:32K
  ROUTING           MAC table:32K,  ARP and ND tables:16K,  routing table:324K
  ARP               MAC table:32K,  ARP and ND tables:272K, routing table:32K
  DUAL-STACK        MAC table:32K,  ARP and ND tables:16K,  routing:v4-87K,v6-86K
  EM                MAC table:32K,  ARP and ND tables:16K,  routing table:32K
  ------------------------------------------------
  Default         Current         Next
  NORMAL          ROUTING         ROUTING
Routing-mode resource(routing-mode), all supported modes:
  ipv6-64           ipv6-64 supported
  ipv6-128          ipv6-128 supported
  ------------------------------------------------
  Default         Current         Next
  ipv6-64         ipv6-128        ipv6-128
Vxlan resource(vxlan), all supported modes:
  l2gw              L2 gateway--underlay/overlay 64K/0K
  l3gw              L3 gateway--underlay/overlay 24K/40K
  ------------------------------------------------
  Default         Current         Next
  l2gw            l3gw            l3gw
```

S6850 做 leaf，border 或 spine 等角色时，推荐硬件参数配置如下：

```
 hardware-resource switch-mode ROUTING
 hardware-resource routing-mode ipv6-128
 hardware-resource vxlan l3gw
```

6. S6860

- S686 的硬件资源参数如下：

```
[leaf1-1]hardware-resource switch-mode ?
  0  MAC table is 272K, L3 host table is 4K, LPM Table is 16K
  1  MAC table is 208K, L3 host table is 68K, LPM Table is 16K
  2  MAC table is 80K, L3 host table is 196K, LPM Table is 16K
```

```
 3  MAC table is 16K, L3 host table is 260K, LPM Table is 16K
 4  MAC table is 80K, L3 host table is 68K, LPM Table is 128K
 5  MAC table is 16K, L3 host table is 4K, LPM Table is 256K
[leaf1-1]hardware-resource routing-mode ?
 ipv6-64   ipv6-64 supported
 ipv6-128  ipv6-128 supported
[leaf1-1]hardware-resource vxlan ?
 l2gw       L2 gateway--underlay/overlay 32K/0K
 l3gw8k     L3 gateway--underlay/overlay 24K/8K
 l3gw16k    L3 gateway--underlay/overlay 16K/16K
 l3gw24k    L3 gateway--underlay/overlay 8K/24K
 border24k  Border--underlay/overlay 8K/24K
 border28k  Border--underlay/overlay 4K/28K
```

- Leaf 角色推荐配置：

```
hardware-resource switch-mode 4
hardware-resource routing-mode ipv6-128
hardware-resource vxlan l3gw24k
```

- border 角色推荐配置：

```
hardware-resource switch-mode 4
hardware-resource routing-mode ipv6-128
hardware-resource vxlan border24k
```

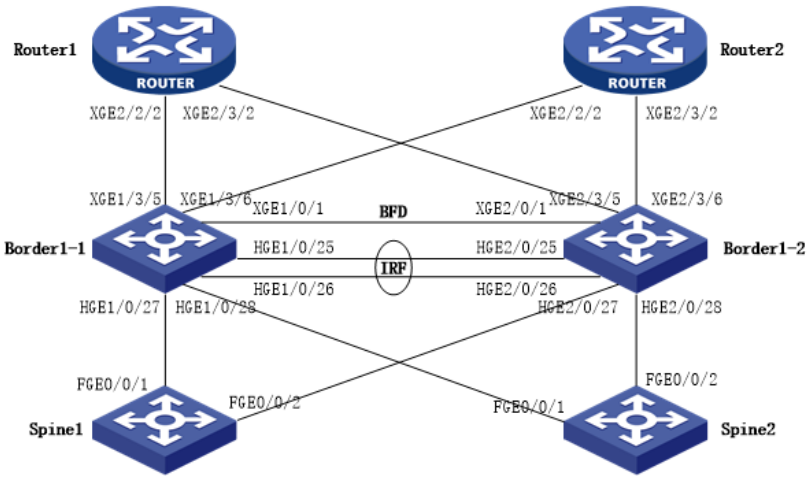
A.6 网络设备overlay配置

A.6.1 Internet Border 配置

1. 组网说明

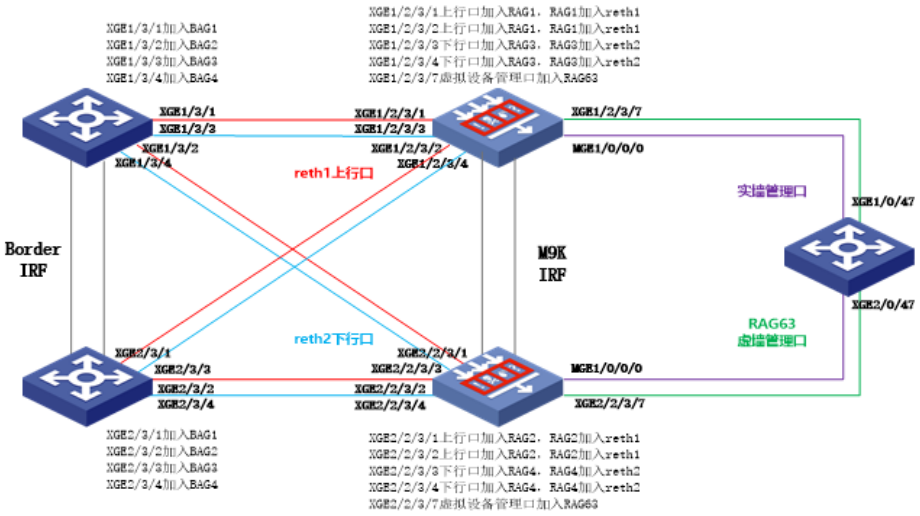
(1) Internet Border 与 Spine/Router 组网图

图A-5 Internet Border 组网图



(2) Internet Border 与旁挂 Internet FW 组网图

图A-6 Internet Border 与旁挂 Internet FW 组网图



2. 接口互联表

本端接口	VLAN	IP	对端设备	对端接口	VLAN	IP
BAGG1（上行） XGE1/3/1 XGE2/3/1	201	10.92.56.254/24	Internet FW	Reth1-RAGG1 XGE1/2/3/1 XGE1/2/3/2	/	/
BAGG2（上行） XGE1/3/2 XGE2/3/2	201	10.92.56.254/24		Reth1-RAGG2 XGE2/2/3/1 XGE2/2/3/2	/	/
BAGG3（下行） XGE1/3/3 XGE2/3/3	1000-3999	/		Reth2-RAGG3 XGE1/2/3/3 XGE1/2/3/4	/	/
BAGG4（下行） XGE1/3/4 XGE2/3/4	1000-3999	/		Reth2-RAGG4 XGE2/2/3/3 XGE2/2/3/4	/	/
RAGG135 XGE1/3/5 XGE2/3/5	/	10.92.51.6/30	Router1	RAGG2 XGE2/2/2 XGE2/2/3	/	10.92.51.5/30
RAGG136 XGE1/3/6 XGE2/3/6	/	10.92.51.10/30	Router2	RAGG2 XGE2/2/2 XGE2/2/3	/	10.92.51.9/30
HGE1/0/27	/	10.92.51.42/30	Spine1	FGE0/0/1	/	10.92.51.41/30
HGE1/0/28	/	10.92.51.58/30	Spine2	FGE0/0/1	/	10.92.51.57/30
HGE2/0/27	/	10.92.51.46/30	Spine1	FGE0/0/2	/	10.92.51.45/30
HGE2/0/28	/	10.92.51.62/30	Spine2	FGE0/0/2	/	10.92.51.61/30

本端接口	VLAN	IP	对端设备	对端接口	VLAN	IP
Loopback0		10.92.50.1				

3. 网络配置

(1) 交换机硬件资源参数配置

参考 3. 交换机硬件参数配置，根据实际交换机型号进行配置，此处以 S6805 为例，配置完成后需要重启设备生效）

```
hardware-resource switch-mode ROUTING
 hardware-resource routing-mode ipv6-128
 hardware-resource vxlan l3gw
```

(2) 配置两台交换机设备做 IRF 堆叠

具体参考 1.6.1 堆叠设备配置模板

(3) 堆叠 Border 基础配置

参考 1.6.2 通用基础配置模板进行配置

- 设备命名，需要根据实际命名修改

```
sysname Internet_border
```

- 配置设备带外管理 IP，IP 地址根据规划进行配置

```
interface M-GigabitEthernet0/0/0
 ip binding vpn-instance mgmt
 ip address 192.166.0.1 255.255.0.0
```

- 设置管理用户，同时作为 netconf 配置下发的帐号，用户名、密码根据规划进行配置

```
local-user admin
 password simpel unicloud123
service-type ssh
 authorization-attribute user-role network-admin
authorization-attribute user-role network-operator
```

- 配置远程访问

```
line vty 0 63
 authentication-mode scheme
 user-role network-admin
 user-role network-operator
 idle-timeout 20 0
```

- 使能 SSH 服务

```
ssh server enable
```

- 使能 netconf ssh 服务

```
netconf ssh server enable
```

- 使能 lldp 及 stp 协议

```
lldp global enable
stp global enable
```

- 使能 L2VPN，配置禁止通过 vxlan 隧道学习 mac 和 arp

```
l2vpn enable
vxlan tunnel mac-learning disable
vxlan tunnel arp-learning disable
```

(4) Underlay 路由协议配置

- 创建 Border 上行外部网络 VPN 实例

```
ip vpn-instance external_vpn
```

- 创建 Border 上行外部网络 OSPF

```
ospf 100 vpn-instance external_vpn router-id 10.92.50.1
non-stop-routing
vpn-instance-capability simple
area 0.0.0.0
```

- 使能 OSPF 协议，实现 spine 和内部 leaf/border 的三层互通

```
ospf 1 router-id 10.92.50.1
non-stop-routing
area 0.0.0.0
```

(5) 接口配置

- 配置环回口地址并使能内部网络 OSPF

```
interface LoopBack0
ip address 10.92.50.1 32
ospf 1 area 0.0.0.0
```

- 配置安全外网 1 网关地址，作为防火墙上行口的网关，加入外部网络 VPN 实例，使能外部网络 OSPF

```
vlan 201
#
interface Vlan-interface 201
ip binding vpn-instance external_vpn
ip address 10.92.56.254 24
ip mtu 2000
ospf 100 area 0.0.0.0
ospf network-type p2p
#
interface BAGG1
link-aggregation mode dynamic
#
interface BAGG2
link-aggregation mode dynamic
#
interface Ten-GigabitEthernet 1/3/1
 port link-aggregation group 1
#
interface Ten-GigabitEthernet 2/3/1
 port link-aggregation group 1
#
interface Ten-GigabitEthernet 1/3/2
 port link-aggregation group 2
#
```

```
interface Ten-GigabitEthernet 2/3/2
 port link-aggregation group 2
#
interface BAGG1
link-aggregation mode dynamic
port access vlan 201
#
interface BAGG2
link-aggregation mode dynamic
port access vlan 201
#
```

- 配置 border 与防火墙下行口互联接口允许租户承载网 vlan 通过

```
vlan 1000 to 3999
#
interface BAGG3
link-aggregation mode dynamic
#
interface BAGG4
link-aggregation mode dynamic
#
interface Ten-GigabitEthernet 1/3/3
 port link-aggregation group 3
#
interface Ten-GigabitEthernet 2/3/3
 port link-aggregation group 3
#
interface Ten-GigabitEthernet 1/3/4
 port link-aggregation group 4
#
interface Ten-GigabitEthernet 2/3/4
 port link-aggregation group 4
#
interface BAGG3
link-aggregation mode dynamic
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 1000 to 3999
#
interface BAGG4
link-aggregation mode dynamic
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 1000 to 3999
#
```

- 配置 border 与出口路由器互联接口地址，加入外部网络 VPN 实例，并使能外部网络 OSPF

```
interface RAGG135
link-aggregation mode dynamic
#
```

```
interface RAGG136
link-aggregation mode dynamic
#
interface Ten-GigabitEthernet 1/3/5
port link-mode route
 port link-aggregation group 135
#
interface Ten-GigabitEthernet 2/3/5
port link-mode route
 port link-aggregation group 135
#
interface Ten-GigabitEthernet 1/3/6
port link-mode route
 port link-aggregation group 136
#
interface Ten-GigabitEthernet 2/3/6
port link-mode route
 port link-aggregation group 136
#

interface RAGG135
link-aggregation mode dynamic
ip binding vpn-instance external_vpn
ip address 10.92.51.6 30
ospf 100 area 0.0.0.0
ip mtu 2000
ospf network-type p2p
#
interface RAGG136
link-aggregation mode dynamic
ip binding vpn-instance external_vpn
ip address 10.92.51.10 30
ospf 100 area 0.0.0.0
ip mtu 2000
ospf network-type p2p
#
```

- 配置 Border 与 Spine 互联接口地址并使能内部网络 OSPF

```
interface HGE1/0/27
port link-mode route
ip address 10.92.51.42 30
ip mtu 2000
ospf 1 area 0.0.0.0
ospf network-type p2p
#
interface HGE1/0/28
port link-mode route
ip address 10.92.51.58 30
ip mtu 2000
```

```
ospf 1 area 0.0.0.0
ospf network-type p2p
#
interface HGE2/0/27
port link-mode route
ip address 10.92.51.46 30
ip mtu 2000
ospf 1 area 0.0.0.0
ospf network-type p2p
#
interface HGE2/0/28
port link-mode route
ip address 10.92.51.62 30
ip mtu 2000
ospf 1 area 0.0.0.0
ospf network-type p2p
#
```

(6) BGP 配置

- 配置 BGP 进程，配置 spine 为对等体

```
bgp 65027
non-stop-routing
router-id 10.92.50.1
peer 10.92.50.77 as-number 65027
peer 10.92.50.77 connect-interface LoopBack0
peer 10.92.50.78 as-number 65027
peer 10.92.50.78 connect-interface LoopBack0
#
address-family l2vpn evpn
peer 10.92.50.77 enable
peer 10.92.50.78 enable
```

A.6.2 Spine 配置

1. 接口互联表

(1) Spine1

本端接口	IP	对端设备	对端接口	IP
FGE0/0/1	10.92.51.41/30	Internet Border1-1	HGE1/0/27	10.92.51.42/30
FGE0/0/2	10.92.51.45/30	Internet Border1-2	HGE2/0/27	10.92.51.46/30
FGE0/0/3	10.92.51.49/30	Intranet Border1-1	HGE1/0/27	10.92.51.50/30
FGE0/0/4	10.92.51.53/30	Intranet Border1-2	HGE2/0/27	10.92.51.54/30
FGE0/0/5	10.92.51.73/30	主机overlay Leaf1-1	HGE1/0/27	10.92.51.74/30
FGE0/0/6	10.92.51.77/30	主机overlay Leaf1-2	HGE1/0/27	10.92.51.78/30

FGE0/0/7	10.92.51.89/30	网络overlay Leaf1-1	HGE1/0/27	10.92.51.90/30
FGE0/0/8	10.92.51.93/30	网络overlay Leaf1-2	HGE2/0/27	10.92.51.94/30
FGE0/0/13	10.92.51.137/30	专线Leaf1-1	HGE1/0/27	10.92.51.138/30
FGE0/0/14	10.92.51.141/30	专线Leaf1-2	HGE2/0/27	10.92.51.142/30
Loopback0	10.92.50.77			

(2) Spine2

本端接口	IP	对端设备	对端接口	IP
FGE0/0/1	10.92.51.57/30	Internet Border1-1	HGE1/0/28	10.92.51.58/30
FGE0/0/2	10.92.51.61/30	Internet Border1-2	HGE2/0/28	10.92.51.62/30
FGE0/0/3	10.92.51.65/30	Intranet Border1-1	HGE1/0/28	10.92.51.66/30
FGE0/0/4	10.92.51.69/30	Intranet Border1-2	HGE2/0/28	10.92.51.70/30
FGE0/0/5	10.92.51.81/30	主机overlay Leaf1-1	HGE1/0/28	10.92.51.82/30
FGE0/0/6	10.92.51.85/30	主机overlay Leaf1-2	HGE1/0/28	10.92.51.86/30
FGE0/0/7	10.92.51.97/30	网络overlay Leaf1-1	HGE1/0/28	10.92.51.98/30
FGE0/0/8	10.92.51.101/30	网络overlay Leaf1-2	HGE2/0/28	10.92.51.102/30
FGE0/0/13	10.92.51.145/30	专线Leaf1-1	HGE1/0/28	10.92.51.146/30
FGE0/0/14	10.92.51.149/30	专线Leaf1-2	HGE2/0/28	10.92.51.150/30
Loopback0	10.92.50.78			

2. 网络配置

(1) Spine1 基础配置

参考 1.6.2 通用基础配置模板进行配置。

- 设备命名，需要根据实际命名修改

```
sysname Spine1
```

- 配置设备带外管理 IP，IP 地址根据规划进行配置

```
interface M-GigabitEthernet0/0/0
 ip binding vpn-instance mgmt
 ip address 192.166.0.77 255.255.0.0
```

- 设置管理用户，同时作为 netconf 配置下发的帐号，用户名、密码根据规划进行配置

```
local-user admin
 password simpel unicloud123
service-type ssh
 authorization-attribute user-role network-admin
authorization-attribute user-role network-operator
```

- 配置远程访问

```
line vty 0 63
 authentication-mode scheme
 user-role network-admin
 user-role network-operator
 idle-timeout 20 0
```

- 使能 SSH 服务

```
ssh server enable
```

- 使能 netconf ssh 服务

```
netconf ssh server enable
```

- 使能 lldp 及 stp 协议

```
lldp global enable
stp global enable
```

(2) Spine1 网络配置

- 使能 L2vpn

```
l2vpn enable
```

- 使能 OSPF 协议，实现 spine 和 leaf/border 的三层互通

```
ospf 1 router-id 10.92.50.77
non-stop-routing
area 0.0.0.0
```

- 配置环回口地址并使能 OSPF

```
interface LoopBack0
ip address 10.92.50.77 32
ospf 1 area 0.0.0.0
```

- 配置 BGP 进程，配置 Leaf、Border、VKS vtep 为对等体

```
bgp 65027
non-stop-routing
router-id 10.92.50.77
peer 10.92.50.1 as-number 65027                --Internet border vtep
peer 10.92.50.1 connect-interface LoopBack0
peer 10.92.50.2 as-number 65027                --Intranet border vtep
peer 10.92.50.2 connect-interface LoopBack0
peer 10.92.50.13 as-number 65027             --网络 overlay Leaf vtep
peer 10.92.50.13 connect-interface LoopBack0
peer 10.92.50.101 as-number 65027            --专线 Leaf vtep
peer 10.92.50.101 connect-interface LoopBack0
peer 10.92.52.11 as-number 65027             --主机 overlay VKS1 vtep
peer 10.92.52.11 connect-interface LoopBack0
peer 10.92.52.12 as-number 65027             --主机 overlay VKS2 vtep
peer 10.92.52.12 connect-interface LoopBack0
peer 10.92.52.128 as-number 65027            --SLB VKS1 vtep
peer 10.92.52.128 connect-interface LoopBack0
peer 10.92.52.129 as-number 65027            --SLB VKS2 vtep
peer 10.92.52.129 connect-interface LoopBack0

#
```

```
address-family l2vpn evpn   //主机 overlay VKS 不用配置 rc
undo policy vpn-target
peer 10.92.50.1 enable
peer 10.92.50.1 reflect-client
peer 10.92.50.2 enable
peer 10.92.50.2 reflect-client
peer 10.92.50.13 enable
peer 10.92.50.13  reflect-client
peer 10.92.50.101 enable
peer 10.92.50.101 reflect-client
peer 10.92.52.11 enable
peer 10.92.52.12 enable
peer 10.92.52.128 enable
peer 10.92.50.128 reflect-client
peer 10.92.52.129 enable
peer 10.92.50.129 reflect-client
#
address-family ipv4 unicast
peer 10.92.50.1 enable
peer 10.92.50.2 enable
peer 10.92.50.13 enable
peer 10.92.50.101 enable
peer 10.92.52.11 enable
peer 10.92.52.12 enable
peer 10.92.52.128 enable
peer 10.92.52.129 enable
```

- 配置 Spine 与 Boder、Leaf 互联接口地址并使能 OSPF

```
interface FGE0/0/1
port link-mode route
ip address 10.92.51.41 30
ip mtu 2000
ospf 1 area 0.0.0.0
ospf network-type p2p
#
interface FGE0/0/2
port link-mode route
ip address 10.92.51.45 30
ip mtu 2000
ospf 1 area 0.0.0.0
ospf network-type p2p
#
interface FGE0/0/3
port link-mode route
ip address 10.92.51.49 30
ip mtu 2000
ospf 1 area 0.0.0.0
ospf network-type p2p
```

```
#
interface FGE0/0/4
port link-mode route
ip address 10.92.51.53 30
ip mtu 2000
ospf 1 area 0.0.0.0
ospf network-type p2p
#
interface FGE0/0/5
port link-mode route
ip address 10.92.51.73 30
ip mtu 2000
ospf 1 area 0.0.0.0
ospf network-type p2p
#
interface FGE0/0/6
port link-mode route
ip address 10.92.51.77 30
ip mtu 2000
ospf 1 area 0.0.0.0
ospf network-type p2p
#
interface FGE0/0/7
port link-mode route
ip address 10.92.51.89 30
ip mtu 2000
ospf 1 area 0.0.0.0
ospf network-type p2p
#
interface FGE0/0/8
port link-mode route
ip address 10.92.51.93 30
ip mtu 2000
ospf 1 area 0.0.0.0
ospf network-type p2p
#
interface FGE0/0/13
port link-mode route
ip address 10.92.51.137 30
ip mtu 2000
ospf 1 area 0.0.0.0
ospf network-type p2p
#
interface FGE0/0/14
port link-mode route
ip address 10.92.51.141 30
ip mtu 2000
ospf 1 area 0.0.0.0
```

```
ospf network-type p2p
#
```

(3) Spine2 基础配置

参考 1.6.2 通用基础配置模板进行配置。

- 设备命名，需要根据实际命名修改

```
sysname Spine2
```

- 配置设备带外管理 IP，IP 地址根据规划进行配置

```
interface M-GigabitEthernet0/0/0
 ip binding vpn-instance mgmt
 ip address 192.166.0.78 255.255.0.0
```

- 设置管理用户，同时作为 netconf 配置下发的帐号，用户名、密码根据规划进行配置

```
local-user admin
 password simpel unicloud123
service-type ssh
 authorization-attribute user-role network-admin
authorization-attribute user-role network-operator
```

- 配置远程访问

```
line vty 0 63
 authentication-mode scheme
 user-role network-admin
 user-role network-operator
 idle-timeout 20 0
```

- 使能 SSH 服务

```
ssh server enable
```

- 使能 netconf ssh 服务

```
netconf ssh server enable
```

- 使能 lldp 及 stp 协议

```
lldp global enable
stp global enable
```

(4) Spine2 网络配置

- 使能 L2vpn

```
l2vpn enable
```

- 使能 OSPF 协议，实现 spine 和 leaf/border 的三层互通

```
ospf 1 router-id 10.92.50.78
non-stop-routing
area 0.0.0.0
```

- 配置环回口地址并使能 OSPF

```
interface LoopBack0
ip address 10.92.50.78 32
ospf 1 area 0.0.0.0
```

- 配置 BGP 进程，配置 Leaf、Border、VKS vtep 为对等体

```
bgp 65027
non-stop-routing
router-id 10.92.50.78
```

```
peer 10.92.50.1 as-number 65027                --Internet border vtep
peer 10.92.50.1 connect-interface LoopBack0
peer 10.92.50.2 as-number 65027                --Intranet border vtep
peer 10.92.50.2 connect-interface LoopBack0
peer 10.92.50.13 as-number 65027             --网络 overlay Leaf vtep
peer 10.92.50.13 connect-interface LoopBack0
peer 10.92.50.101 as-number 65027            --专线 Leaf vtep
peer 10.92.50.101 connect-interface LoopBack0
peer 10.92.52.11 as-number 65027             --主机 overlay VKS1 vtep
peer 10.92.52.11 connect-interface LoopBack0
peer 10.92.52.12 as-number 65027             --主机 overlay VKS2 vtep
peer 10.92.52.12 connect-interface LoopBack0
peer 10.92.52.128 as-number 65027            --SLB VKS1 vtep
peer 10.92.52.128 connect-interface LoopBack0
peer 10.92.52.129 as-number 65027            --SLB VKS2 vtep
peer 10.92.52.129 connect-interface LoopBack0

#
address-family l2vpn evpn   //主机 overlay VKS 不用配置 rc
undo policy vpn-target
peer 10.92.50.1 enable
peer 10.92.50.1 reflect-client
peer 10.92.50.2 enable
peer 10.92.50.2 reflect-client
peer 10.92.50.13 enable
peer 10.92.50.13  reflect-client
peer 10.92.50.101 enable
peer 10.92.50.101 reflect-client
peer 10.92.52.11 enable
peer 10.92.52.12 enable
peer 10.92.52.128 enable
peer 10.92.50.128 reflect-client
peer 10.92.52.129 enable
peer 10.92.50.129 reflect-client
#
address-family ipv4 unicast
peer 10.92.50.1 enable
peer 10.92.50.2 enable
peer 10.92.50.13 enable
peer 10.92.50.101 enable
peer 10.92.52.11 enable
peer 10.92.52.12 enable
peer 10.92.52.128 enable
peer 10.92.52.129 enable
```

- 配置 Spine 与 Boder、Leaf 互联接口地址并使能 OSPF

```
interface FGE0/0/1
port link-mode route
ip address 10.92.51.57 30
```

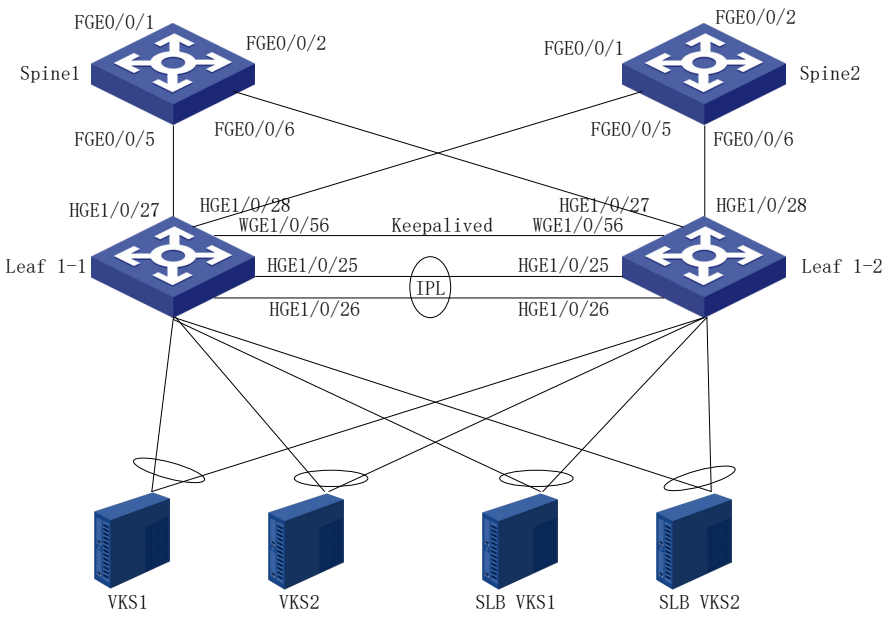
```
ip mtu 2000
ospf 1 area 0.0.0.0
ospf network-type p2p
#
interface FGE0/0/2
port link-mode route
ip address 10.92.51.61 30
ip mtu 2000
ospf 1 area 0.0.0.0
ospf network-type p2p
#
interface FGE0/0/3
port link-mode route
ip address 10.92.51.65 30
ip mtu 2000
ospf 1 area 0.0.0.0
ospf network-type p2p
#
interface FGE0/0/4
port link-mode route
ip address 10.92.51.69 30
ip mtu 2000
ospf 1 area 0.0.0.0
ospf network-type p2p
#
interface FGE0/0/5
port link-mode route
ip address 10.92.51.81 30
ip mtu 2000
ospf 1 area 0.0.0.0
ospf network-type p2p
#
interface FGE0/0/6
port link-mode route
ip address 10.92.51.85 30
ip mtu 2000
ospf 1 area 0.0.0.0
ospf network-type p2p
#
interface FGE0/0/7
port link-mode route
ip address 10.92.51.97 30
ip mtu 2000
ospf 1 area 0.0.0.0
ospf network-type p2p
#
interface FGE0/0/8
port link-mode route
```

```
ip address 10.92.51.101 30
ip mtu 2000
ospf 1 area 0.0.0.0
ospf network-type p2p
#
interface FGE0/0/13
port link-mode route
ip address 10.92.51.145 30
ip mtu 2000
ospf 1 area 0.0.0.0
ospf network-type p2p
#
interface FGE0/0/14
port link-mode route
ip address 10.92.51.149 30
ip mtu 2000
ospf 1 area 0.0.0.0
ospf network-type p2p
#
```

A.6.3 主机 Overlay Leaf 配置

1. 组网图

图A-7 主机 Overlay Leaf 组网图



2. 接口互联表

(1) Leaf1-1

本端接口	VLAN	IP	对端设备	对端接口	IP

BAGG1 WGE1/0/1	30	10.92.52.254/24	VKS1	br-tun	10.92.52.11/24
BAGG2 WGE1/0/2	30	10.92.52.254/24	VKS2	br-tun	10.92.52.12/24
BAGG11 WGE2/0/1	30	10.92.52.254/24	SLB VKS1	br-tun	10.92.52.128/24
BAGG12 WGE2/0/2	30	10.92.52.254/24	SLB VKS2	br-tun	10.92.52.129/24
HGE1/0/27	/	10.92.51.74/30	Spine1	FGE0/0/5	10.92.51.73/30
HGE1/0/28	/	10.92.51.82/30	Spine2	FGE0/0/5	10.92.51.81/30
Loopback0		10.92.50.11			

(2) Leaf1-2

本端接口	VLAN	IP	对端设备	对端接口	IP
BAGG1	30	10.92.52.254/24	VKS1	br-tun	10.92.52.11/24
BAGG2	30	10.92.52.254/24	VKS2	br-tun	10.92.52.12/24
BAGG11	30	10.92.52.254/24	SLB VKS1	br-tun	10.92.52.128/24
BAGG12	30	10.92.52.254/24	SLB VKS2	br-tun	10.92.52.129/24
HGE1/0/27	/	10.92.51.78/30	Spine1	FGE0/0/6	10.92.51.77/30
HGE1/0/28	/	10.92.51.86/30	Spine2	FGE0/0/6	10.92.51.85/30
Loopback0		10.92.50.12			

3. 设备配置

(1) 主机 overlay Leaf1-1 基础配置

参考 1.6.2 通用基础配置模板进行配置。

- 设备命名，需要根据实际命名修改

```
sysname Host_leaf1-1
```

- 配置设备带外管理 IP，IP 地址根据规划进行配置

```
interface M-GigabitEthernet0/0/0
 ip binding vpn-instance mgmt
 ip address 192.166.0.11 255.255.0.0
```

- 设置管理用户，同时作为 netconf 配置下发的帐号，用户名、密码根据规划进行配置

```
local-user admin
 password simpel unicloud123
service-type ssh
 authorization-attribute user-role network-admin
authorization-attribute user-role network-operator
```

- 配置远程访问

```
line vty 0 63
 authentication-mode scheme
 user-role network-admin
 user-role network-operator
 idle-timeout 20 0
```

- 使能 SSH 服务

```
ssh server enable
```

- 使能 netconf ssh 服务

```
netconf ssh server enable
```

- 使能 lldp 及 stp 协议

```
lldp global enable
stp global enable
```

(2) 主机 overlay Leaf1-2 基础配置

参考 1.6.2 通用基础配置模板进行配置。

- 设备命名，需要根据实际命名修改

```
sysname Host_leaf1-2
```

- 配置设备带外管理 IP，IP 地址根据规划进行配置

```
interface M-GigabitEthernet0/0/0
 ip binding vpn-instance mgmt
 ip address 192.166.0.12 255.255.0.0
```

- 设置管理用户，同时作为 netconf 配置下发的帐号，用户名、密码根据规划进行配置

```
local-user admin
 password simpel unicloud123
service-type ssh
 authorization-attribute user-role network-admin
authorization-attribute user-role network-operator
```

- 配置远程访问

```
line vty 0 63
 authentication-mode scheme
 user-role network-admin
 user-role network-operator
 idle-timeout 20 0
```

- 使能 SSH 服务

```
ssh server enable
```

- 使能 netconf ssh 服务

```
netconf ssh server enable
```

- 使能 lldp 及 stp 协议

```
lldp global enable
stp global enable
```

(3) 主机 overlay Leaf1-1 DRNI 配置

- DR 系统中所有 DR 设备的 system-mac 必须相同，且保证全网唯一

```
drni system-mac 0001-0001-0001
```

- 两台 DR 设备的 system-number 必须不同。可以配置第一台 DR 设备为 1，第二台为 2

```
drni system-number 1
```

- 配置 DR 设备的 system-priority 必须相同

```
drni system-priority 123
```

- 创建 IPP 聚合口

```
interface Bridge-Aggregation100
link-aggregation mode dynamic
```

- IPP 物理口添加到聚合口中

```
interface HundredGigE1/0/25
 port link-aggregation group 100
#
interface HundredGigE1/0/26
 port link-aggregation group 100
```

- IPP 聚合口配置

```
interface Bridge-Aggregation100
 port link-type trunk
 port trunk permit vlan all
 link-aggregation mode dynamic
 port drni intra-portal-port 1
 undo mac-address static source-check enable
```

- 配置 DRNI MAD 恢复延迟。当 IPL 链路恢复以后，需要延迟指定时间后，链路才 MAD UP

```
drni restore-delay 180
```

- 配置 Keepalive 报文的目的 IP 地址和源 IP 地址

```
drni keepalive ip destination 10.250.27.74 source 10.250.27.73
```

- 配置 MAD 接口为 3 层接口，并配置 IP 地址为 Keepalive 报文的源 IP 地址

```
interface Twenty-FiveGigE1/0/56
 port link-mode route
 speed 10000
ip address 10.250.27.73 255.255.255.252
```

- 配置 MAD 链路接口为保留接口

```
drni mad exclude interface Twenty-FiveGigE1/0/56
```

(4) 主机 overlay Leaf1-2 DRNI 配置

- DR 系统中所有 DR 设备的 system-mac 必须相同，且保证全网唯一

```
drni system-mac 0001-0001-0001
```

- 两台 DR 设备的 system-number 必须不同。可以配置第一台 DR 设备为 1，第二台为 2

```
drni system-number 2
```

- 配置 DR 设备的 system-priority 必须相同

```
drni system-priority 123
```

- 创建 IPP 聚合口

```
interface Bridge-Aggregation100
link-aggregation mode dynamic
```

- IPP 物理口添加到聚合口中

```
interface HundredGigE1/0/25
 port link-aggregation group 100
#
interface HundredGigE1/0/26
 port link-aggregation group 100
```

- IPP 聚合口配置

```
interface Bridge-Aggregation100
 port link-type trunk
 port trunk permit vlan all
 link-aggregation mode dynamic
 port drni intra-portal-port 1
 undo mac-address static source-check enable
```

- 配置 DRNI MAD 恢复延迟。当 IPL 链路恢复以后，需要延迟指定时间后，链路才 MAD UP

```
drni restore-delay 180
```

- 配置 Keepalive 报文的目的 IP 地址和源 IP 地址

```
drni keepalive ip destination 10.250.27.73 source 10.250.27.74
```

- 配置 MAD 接口为 3 层接口，并配置 IP 地址为 Keepalive 报文的源 IP 地址

```
interface Twenty-FiveGigE1/0/56
 port link-mode route
 speed 10000
ip address 10.250.27.74 255.255.255.252
```

- 配置 MAD 链路接口为保留接口

```
drni mad exclude interface Twenty-FiveGigE1/0/56
```

(5) 主机 overlay Leaf1-1 网络配置

- 使能 OSPF 协议，实现 spine 和 leaf/border 的三层互通

```
ospf 1 router-id 10.92.50.11
non-stop-routing
area 0.0.0.0
```

- 配置环回口地址并使能 OSPF

```
interface LoopBack0
ip address 10.92.50.11 32
ospf 1 area 0.0.0.0
```

- 配置主机 overlay VKS underlay 网关地址并使能 OSPF 协议，VKS 业务网 VTEP 地址的网关为 vrrp vip

```
vlan 30
#
interface vlan-interface30
ip address 10.92.52.252 24
ip mtu 2000
ospf network-type p2p
ospf 1 area 0.0.0.0
vrrp vrid 1 virtual-ip 10.92.52.254
vrrp vrid 1 priority 200
```

- 配置主机 overlay Leaf 与 VKS 互联接口，配置两个设备的物理接口跨设备聚合加入聚合口，并配置聚合口加入 drni group

```
interface BAGG1
link-aggregation mode dynamic
interface WGE1/0/1
port link-aggregation group 1
interface BAGG1
link-aggregation mode dynamic
```

```
port access vlan 30
port drni group 1
stp edged-port
#
interface BAGG2
link-aggregation mode dynamic
interface WGE1/0/2
port link-aggregation group 2
interface BAGG2
link-aggregation mode dynamic
port access vlan 30
port drni group 2
stp edged-port
#
interface BAGG11
link-aggregation mode dynamic
interface WGE2/0/1
port link-aggregation group 11
interface BAGG11
link-aggregation mode dynamic
port access vlan 30
port drni group 11
stp edged-port
#
interface BAGG12
link-aggregation mode dynamic
interface WGE2/0/2
port link-aggregation group 12
interface BAGG12
link-aggregation mode dynamic
port access vlan 30
port drni group 12
stp edged-port
#
```

- 配置 Leaf 与 Spine 互联接口地址并使能 OSPF

```
interface HGE1/0/27
port link-mode route
ip address 10.92.51.74 30
ospf 1 area 0.0.0.0
ospf network-type p2p
ip mtu 2000
#
interface HGE1/0/28
port link-mode route
ip address 10.92.51.82 30
ospf 1 area 0.0.0.0
ospf network-type p2p
ip mtu 2000
```

```
#
```

(6) 主机 overlay Leaf1-2 网络配置

- 使能 OSPF 协议，实现 spine 和 leaf/border 的三层互通

```
ospf 1 router-id 10.92.50.12
non-stop-routing
area 0.0.0.0
```

- 配置环回口地址并使能 OSPF

```
interface LoopBack0
ip address 10.92.50.12 32
ospf 1 area 0.0.0.0
```

- 配置主机 overlay VKS underlay 网关地址并使能 OSPF 协议，VKS 业务网 VTEP 地址的网关为 vrrp vip

```
vlan 30
#
interface vlan-interface30
ip address 10.92.52.253 24
ip mtu 2000
ospf network-type p2p
ospf 1 area 0.0.0.0
vrrp vrid 1 virtual-ip 10.92.52.254
vrrp vrid 1 priority 200
```

- 配置主机 overlay Leaf 与 VKS 互联接口，配置两个设备的物理接口跨设备聚合加入聚合口，并配置聚合口加入 drni group

```
interface BAGG1
link-aggregation mode dynamic
interface WGE1/0/1
port link-aggregation group 1
interface BAGG1
link-aggregation mode dynamic
port access vlan 30
port drni group 1
stp edged-port
#
interface BAGG2
link-aggregation mode dynamic
interface WGE1/0/2
port link-aggregation group 2
interface BAGG2
link-aggregation mode dynamic
port access vlan 30
port drni group 2
stp edged-port
#
interface BAGG11
link-aggregation mode dynamic
interface WGE2/0/1
port link-aggregation group 11
```

```
interface BAGG11
link-aggregation mode dynamic
port access vlan 30
port drni group 11
stp edged-port
#
interface BAGG12
link-aggregation mode dynamic
interface WGE2/0/2
port link-aggregation group 12
interface BAGG12
link-aggregation mode dynamic
port access vlan 30
port drni group 12
stp edged-port
#
```

- 配置 Leaf 与 Spine 互联接口地址并使能 OSPF

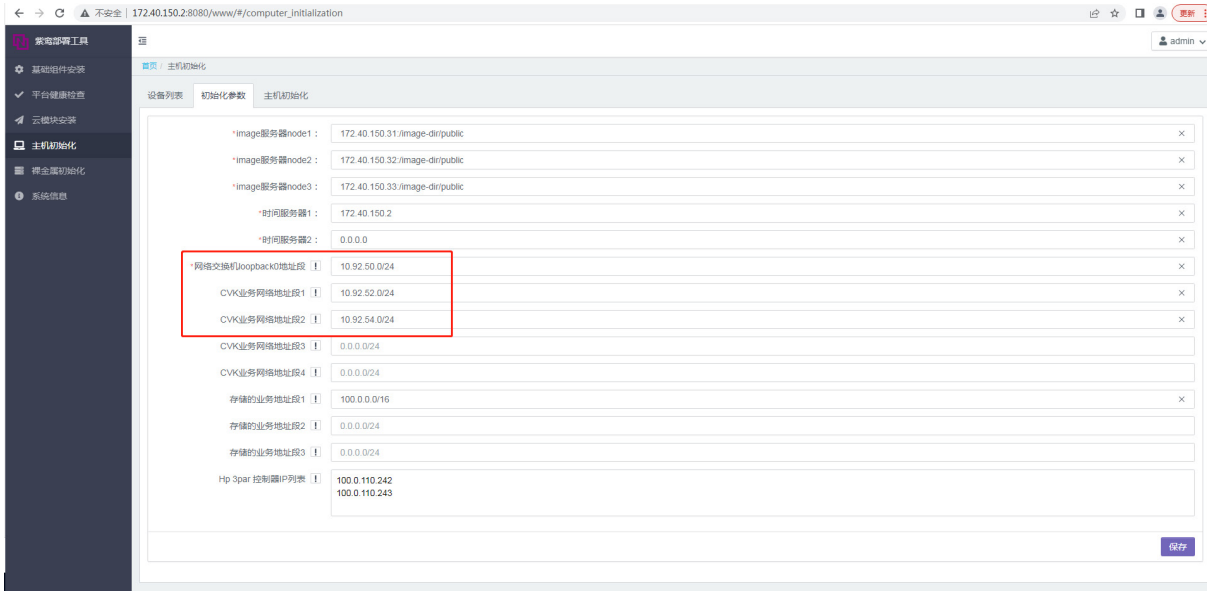
```
interface HGE1/0/27
port link-mode route
ip address 10.92.51.78 30
ospf 1 area 0.0.0.0
ospf network-type p2p
ip mtu 2000
#
interface HGE1/0/28
port link-mode route
ip address 10.92.51.86 30
ospf 1 area 0.0.0.0
ospf network-type p2p
ip mtu 2000
#
```

(7) VKS 初始化配置

- 使用部署工具配置 VKS 业务网卡聚合，配置业务网地址，配置完成如下

```
[root@H3C-HZ-VKS11 ~]# ifconfig
br-tun: flags=4419<UP,BROADCAST,RUNNING,PROMISC,MULTICAST>  mtu 2000
        inet 10.92.52.11  netmask 255.255.255.0  broadcast 10.92.52.255
        inet6 fe80::5ec9:99ff:fede:e764  prefixlen 64  scopeid 0x20<link>
        ether 5c:c9:99:de:e7:64  txqueuelen 1000  (Ethernet)
        RX packets 29962881  bytes 2955417777 (2.7 GiB)
        RX errors 0  dropped 2  overruns 0  frame 0
        TX packets 192019  bytes 14421317 (13.7 MiB)
        TX errors 0  dropped 2 overruns 0  carrier 0  collisions 0
```

- 使用部署工具配置 VKS 业务网路由，添加网络交换机 loopback0 地址段和所有 VKS 业务网络地址段



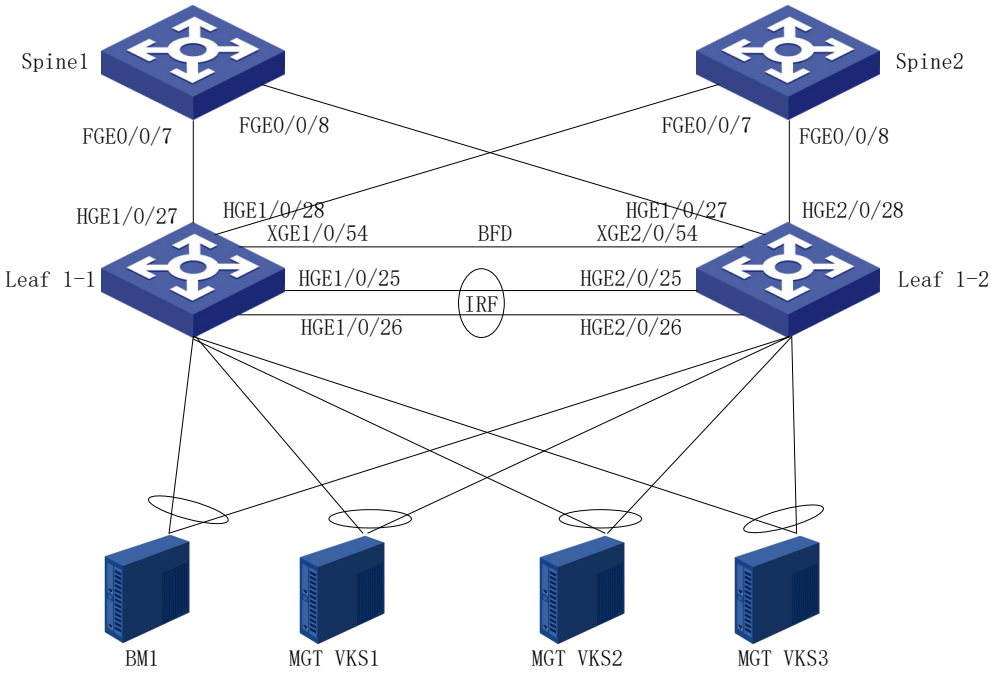
- 查看路由信息如下

```
[root@H3C-HZ-CVK239 ~]# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         172.16.202.254  0.0.0.0         UG    0      0        0 enp6
10.92.50.0      10.92.52.254    255.255.255.0   UG    0      0        0 br-tun
10.92.52.0      10.92.52.254    255.255.255.0   UG    0      0        0 br-tun
10.92.52.0      0.0.0.0         255.255.255.0   U     0      0        0 br-tun
10.92.54.0      10.92.52.254    255.255.255.0   UG    0      0        0 br-tun
100.0.0.0       100.0.206.3     255.255.0.0     UG    0      0        0 vswitch-stor
100.0.0.0       0.0.0.0         255.255.0.0     U     0      0        0 vswitch-stor
169.254.0.0     0.0.0.0         255.255.0.0     U     1012   0        0 br-tun
169.254.0.0     0.0.0.0         255.255.0.0     U     1014   0        0 vswitch-stor
172.16.0.0      0.0.0.0         255.255.0.0     U     0      0        0 enp6
```

A.6.4 网络 Overlay Leaf 配置

1. 组网图

图A-8 网络 Overlay Leaf 组网图



2. 接口互联表

本端接口	VLAN	IP	对端设备	对端接口	IP
BAGG1 XGE1/0/1 XGE2/0/1	900		MGT VKS1	Vswitch1 Eth3 Eth4	100.100.0.61
BAGG2 XGE1/0/2 XGE2/0/2	900		MGT VKS2	Vswitch1 Eth3 Eth4	100.100.0.62
BAGG3 XGE1/0/3 XGE2/0/3	900		MGT VKS3	Vswitch1 Eth3 Eth4	100.100.0.63
BAGG21 XGE1/0/21 XGE2/0/21	1000-3999		BM1	Eth1	
HGE1/0/27	/	10.92.51.90/30	Spine1	FGE0/0/7	10.92.51.89/30
HGE1/0/28	/	10.92.51.98/30	Spine2	FGE0/0/7	10.92.51.97/30
HGE2/0/27	/	10.92.51.94/30	Spine1	FGE0/0/8	10.92.51.93/30
HGE2/0/28	/	10.92.51.102/30	Spine2	FGE0/0/8	10.92.51.101/30

Loopback0		10.92.50.13			

3. 网络配置

(1) 交换机硬件资源参数配置

参考 1.6.4 交换机硬件参数配置，根据实际交换机型号进行配置，此处以 S6805 为例，配置完成后需要重启设备生效。

```
hardware-resource switch-mode ROUTING
 hardware-resource routing-mode ipv6-128
 hardware-resource vxlan l3gw
```

(2) 配置两台交换机设备做 IRF 堆叠

具体参考 1.6.1 堆叠设备配置模板

(3) 堆叠 Leaf 基础配置

参考 1.6.2 通用基础配置模板进行配置

- 设备命名，需要根据实际命名修改

```
sysname Network_leaf
```

- 配置设备带外管理 IP，IP 地址根据规划进行配置

```
interface M-GigabitEthernet0/0/0
 ip binding vpn-instance mgmt
 ip address 192.166.0.13 255.255.0.0
```

- 设置管理用户，同时作为 netconf 配置下发的帐号，用户名、密码根据规划进行配置

```
local-user admin
 password simpel unicloud123
service-type ssh
 authorization-attribute user-role network-admin
authorization-attribute user-role network-operator
```

- 配置远程访问

```
line vty 0 63
 authentication-mode scheme
 user-role network-admin
 user-role network-operator
 idle-timeout 20 0
```

- 使能 SSH 服务

```
ssh server enable
```

- 使能 netconf ssh 服务

```
netconf ssh server enable
```

- 使能 lldp 及 stp 协议

```
lldp global enable
stp global enable
```

(4) 使能 L2VPN

使能 L2vpn,配置禁止通过 vxlan 隧道学习 mac 和 arp

```
l2vpn enable
vxlan tunnel mac-learning disable
vxlan tunnel arp-learning disable
```

(5) Underlay 路由协议配置

使能 OSPF 协议，实现 leaf 与 spine 的三层互通

```
ospf 1 router-id 10.92.50.13
non-stop-routing
area 0.0.0.0
```

(6) 接口配置

- 配置环回口地址并使能内部网络 OSPF

```
interface LoopBack0
ip address 10.92.50.13 32
ospf 1 area 0.0.0.0
```

- 配置网络 overlay Leaf 与裸金属的互联接口为 vtep access 接口

```
vlan 1000 to 3999
#
interface BAGG21
link-aggregation mode dynamic
#
interface Ten-GigabitEthernet 1/0/21
 port link-aggregation group 21
#
interface Ten-GigabitEthernet 2/0/21
 port link-aggregation group 21
#
interface BAGG21
link-aggregation mode dynamic
port link-type trunk
undo port trunk permit vlan 1
stp edged-port
vtep access port
#
```

- 配置网络 overlay Leaf 上租管互通 VPC 的 nginx 接入接口为 vtep access 接口，其他具体配置请参考 1.8 租管互通网络配置

```
vlan 1000 to 3999
#
interface BAGG1
link-aggregation mode dynamic
#
interface BAGG2
link-aggregation mode dynamic
#
interface BAGG3
link-aggregation mode dynamic
#
interface Ten-GigabitEthernet 1/0/1
 port link-aggregation group 1
#
interface Ten-GigabitEthernet 2/0/1
 port link-aggregation group 1
```

```
#
interface Ten-GigabitEthernet 1/0/2
 port link-aggregation group 2
#
interface Ten-GigabitEthernet 2/0/2
 port link-aggregation group 2
#
interface Ten-GigabitEthernet 1/0/3
 port link-aggregation group 3
#
interface Ten-GigabitEthernet 2/0/3
 port link-aggregation group 3
#
interface BAGG1
link-aggregation mode dynamic
port link-type trunk
undo port trunk permit vlan 1
stp edged-port
vtep access port
#
interface BAGG2
link-aggregation mode dynamic
port link-type trunk
undo port trunk permit vlan 1
stp edged-port
vtep access port
#
interface BAGG3
link-aggregation mode dynamic
port link-type trunk
undo port trunk permit vlan 1
stp edged-port
vtep access port
#
```

- 配置 Leaf 与 Spine 互联接口地址并使能 OSPF

```
interface HGE1/0/27
port link-mode route
ip address 10.92.51.90 30
ospf 1 area 0.0.0.0
ospf network-type p2p
#
interface HGE1/0/28
port link-mode route
ip address 10.92.51.98 30
ospf 1 area 0.0.0.0
ospf network-type p2p
#
interface HGE2/0/17
```

```
port link-mode route
ip address 10.92.51.94 30
ospf 1 area 0.0.0.0
ospf network-type p2p
#
interface HGE2/0/28
port link-mode route
ip address 10.92.51.102 30
ospf 1 area 0.0.0.0
ospf network-type p2p
#
```

(7) BGP 配置

- 配置 BGP 进程，配置 spine 为对等体

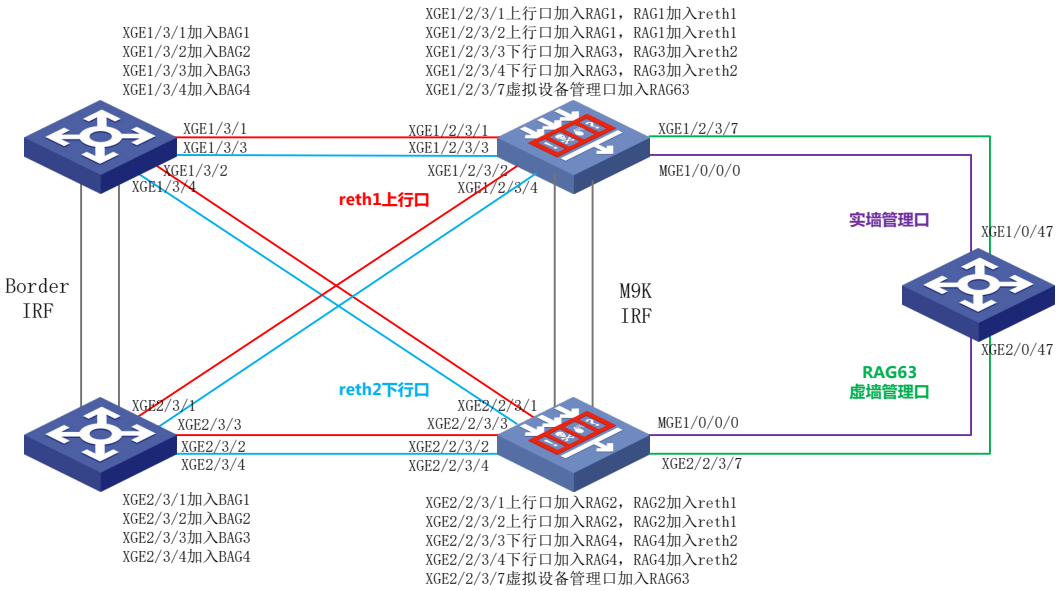
```
bgp 65027
non-stop-routing
router-id 10.92.50.13
peer 10.92.50.77 as-number 65027
peer 10.92.50.77 connect-interface LoopBack0
peer 10.92.50.78 as-number 65027
peer 10.92.50.78 connect-interface LoopBack0
#
address-family l2vpn evpn
peer 10.92.50.77 enable
peer 10.92.50.78 enable
```

A.6.5 Internet FW 配置

此处以 M9K 类型防火墙设备作为介绍，F5K 类型防火墙设备配置可以参考 Intranet FW 配置

1. 组网图

防火墙框内两个接口做聚合，跨框聚合口做冗余口。对端交换机接口跨框做聚合。



2. 接口互联表

本端接口	VLAN	IP	对端设备	对端接口	VLAN	IP
Reth1-RAGG1	/	/	Internet Border	BAGG1	201	10.92.56.254/24
Reth1-RAGG2	/	/		BAGG2	201	10.92.56.254/24
Reth2-RAGG3	/	/		BAGG3	1000-3999	/
Reth2-RAGG4	/	/		BAGG4	1000-3999	/
RAG63	/	/	管理ACC	BAG47	107	10.92.30.254/24
Loopback0		10.92.50.81				

3. 网络配置

(1)　配置两台防火墙设备做 IRF 堆叠，

具体参考 1.6.1 堆叠设备配置模板

(2)　配置堆叠防火墙基础配置

参考 1.6.2 通用基础配置模板进行配置

- 设备命名，需要根据实际命名修改

```
sysname Internet-FW
```

- 配置设备带外管理 IP，IP 地址根据规划进行配置

```
interface M-GigabitEthernet1/0/0/0
 ip binding vpn-instance mgmt
 ip address 192.166.0.81 255.255.0.0
```

- 设置管理用户，同时作为 netconf 配置下发的帐号，用户名、密码根据规划进行配置

```
local-user sdn
 password simpel unicloud123
service-type ssh
 authorization-attribute user-role network-admin
authorization-attribute user-role network-operator
```

- 配置远程访问

```
line vty 0 63
 authentication-mode scheme
 user-role network-admin
 user-role network-operator
 idle-timeout 20 0
```

- 使能 SSH 服务

```
ssh server enable
```

- 使能 netconf ssh 服务

```
netconf ssh server enable
```

- 使能 lldp 及 stp 协议

```
lldp global enable
stp global enable
```

- 配置会话同步

```
session synchronization enable asymmetric
```

(3) 防火墙接口配置

- 配置防火墙与 Border 上行口 Reth1，4 个物理接口配置成 2 个聚合口，2 个聚合口配置成冗余口

```
interface Route-Aggregation1
 link-aggregation mode dynamic
interface Ten-GigabitEthernet1/2/3/1
 port link-mode route
 port link-aggregation group 1
interface Ten-GigabitEthernet1/2/3/2
 port link-mode route
 port link-aggregation group 1
#
interface Route-Aggregation2
 link-aggregation mode dynamic
interface Ten-GigabitEthernet2/2/3/1
 port link-mode route
 port link-aggregation group 2
interface Ten-GigabitEthernet2/2/3/2
 port link-mode route
 port link-aggregation group 2
#
interface Reth1
member interface RAGG1 priority 255
member interface RAGG2 priority 100
#
```

配置防火墙与 Border 下行口 Reth2，4 个物理接口配置成 2 个聚合口，2 个聚合口配置成冗余口

```
interface Route-Aggregation3
 link-aggregation mode dynamic
interface Ten-GigabitEthernet1/2/3/3
 port link-mode route
 port link-aggregation group 3
interface Ten-GigabitEthernet1/2/3/4
 port link-mode route
 port link-aggregation group 3
#
interface Route-Aggregation4
 link-aggregation mode dynamic
interface Ten-GigabitEthernet2/2/3/3
 port link-mode route
 port link-aggregation group 4
interface Ten-GigabitEthernet2/2/3/4
 port link-mode route
 port link-aggregation group 4
#
interface Reth2
member interface RAGG3 priority 255
member interface RAGG4 priority 100
```

- 配置环回口地址，用于纳管时填入

```
interface LoopBack0
ip address 10.92.50.81 32
```

- 配置防火墙虚墙接口，该接口会下发“防火墙虚拟设备管理网”网段地址，云平台需要和该地址通信进行防火墙配置下发

```
interface Route-Aggregation63
link-aggregation mode dynamic
interface Ten-GigabitEthernet1/2/3/7
 port link-mode route
 port link-aggregation group 63
interface Ten-GigabitEthernet2/2/3/7
 port link-mode route
 port link-aggregation group 63
#
```

(4) 冗余组配置

所有 FW blade 卡都默认加入安全引擎组 1。推荐使用共享 Context+单安全引擎组方式。

- 安全引擎组 1 的聚合接口配置

```
interface Blade-Aggregation1
link-aggregation blade Blade4fw
```

- 故障恢复组 1 配置

```
failover group backup1
bind chassis 1 slot 2 cpu 1 primary
bind chassis 2 slot 2 cpu 1 secondary
```

- 故障恢复组 2 配置

```
failover group backup2
bind chassis 1 slot 3 cpu 1 primary
bind chassis 2 slot 3 cpu 1 secondary
```

- Track 配置

```
track 1 interface Route-Aggregation1 physical
track 2 interface Route-Aggregation3 physical
track 3 interface Blade1/2/0/1 physical
track 4 interface Blade1/2/0/2 physical
track 5 interface Blade1/3/0/1 physical
track 6 interface Blade1/3/0/2 physical
track 11 interface Route-Aggregation2 physical
track 12 interface Route-Aggregation4 physical
track 13 interface Blade2/2/0/1 physical
track 14 interface Blade2/2/0/2 physical
track 15 interface Blade2/3/0/1 physical
track 16 interface Blade2/3/0/2 physical
```

- 冗余组配置。RAGG1、3 为堆叠框 1 的聚合口，配置在 node1 里，RAGG2、4 为堆叠框 2 的聚合口，配置在 node2 里

```
redundancy group 1
 member interface Reth1
 member interface Reth2
 member failover group 1
 member failover group 2
 node 1
  bind chassis 1
  priority 150
track 1 interface Route-Aggregation1 physical
track 2 interface Route-Aggregation3 physical
track 3 interface Blade1/2/0/1 physical
track 4 interface Blade1/2/0/2 physical
track 5 interface Blade1/3/0/1 physical
track 6 interface Blade1/3/0/2 physical

node 2
  bind chassis 2
  priority 100
track 11 interface Route-Aggregation2 physical
track 12 interface Route-Aggregation4 physical
track 13 interface Blade2/2/0/1 physical
track 14 interface Blade2/2/0/2 physical
track 15 interface Blade2/3/0/1 physical
track 16 interface Blade2/3/0/2 physical
```

(5) 防火墙安全策略配置

```
security-policy ip
rule 10 name local-any
action pass
source-zone local
rule 20 name any-local
```

```
action pass
destination-zone local
#
security-zone intra-zone default permit
#
security-zone name Trust
import interface Reth2
import interface Route-Aggregation63
#
security-zone name Untrust
import interface Reth1
#
security-zone name Management
 import interface M-GigabitEthernet1/0/0/0
```

(6) 防火墙虚墙接口对端设备配置参考

配置防火墙虚墙接口对端设备上配置“防火墙虚拟设备管理网”的网关地址，本指导中为10.92.30.254/24，确保云平台可以和该地址通信。

```
interface Bridge-Aggregation47
 port access vlan 107
 link-aggregation mode dynamic
interface Ten-GigabitEthernet1/0/47
 port access vlan 107
 port link-aggregation group 47
interface Ten-GigabitEthernet2/0/47
 port access vlan 107
 port link-aggregation group 47
#
interface Vlan-interface107
 ip address 10.93.30.254 255.255.255.0
```

A.6.6 Internet Router 配置

1. 接口互联表

(1) Router1

本端接口	IP	对端设备	对端接口	IP
RAGG1 XGE2/2/1 XGE2/3/1	/	上行出口设备		
RAGG2 XGE2/2/2 XGE2/3/2	10.92.51.5/30	Internet Border	RAGG135 XGE1/3/5 XGE2/3/5	10.92.51.6/30
Loopback0	10.92.50.73			

(2) Router2

本端接口	IP	对端设备	对端接口	IP

RAGG1 XGE2/2/1 XGE2/3/1	/	上行出口设备		
RAGG2 XGE2/2/2 XGE2/3/2	10.92.51.9/30	Internet Border	RAGG135 XGE1/3/5 XGE2/3/5	10.92.51.10/30
Loopback0	10.92.50.74			

2. 网络配置

(1) Router1 基础配置

参考 1.6.2 通用基础配置模板进行配置。

- 设备命名，需要根据实际命名修改

```
sysname Router1
```

- 配置设备带外管理 IP，IP 地址根据规划进行配置

```
interface M-GigabitEthernet0/0/0
 ip binding vpn-instance mgmt
 ip address 192.166.0.73 255.255.0.0
```

- 设置管理用户，同时作为 netconf 配置下发的帐号，用户名、密码根据规划进行配置

```
local-user admin
 password simpel unicloud123
service-type ssh
 authorization-attribute user-role network-admin
authorization-attribute user-role network-operator
```

- 配置远程访问

```
line vty 0 63
 authentication-mode scheme
 user-role network-admin
 user-role network-operator
 idle-timeout 20 0
```

- 使能 SSH 服务

```
ssh server enable
```

- 使能 netconf ssh 服务

```
netconf ssh server enable
```

- 使能 lldp 及 stp 协议

```
lldp global enable
stp global enable
```

(2) Router1 网络配置

- 使能 OSPF 协议

```
ospf 100 router-id 10.92.50.73
non-stop-routing
area 0.0.0.0
```

- 配置环回口地址并使能 OSPF

```
interface LoopBack0
ip address 10.92.50.73 32
```

```
ospf 100 area 0.0.0.0
```

- 配置与 Internet Border 互联接口地址并使能 OSPF

```
interface RAGG2
link-aggregation mode dynamic
ip address 10.92.51.5 30
ip mtu 2000
ospf 100 area 0.0.0.0
ospf network-type p2p
#
interface XGE2/2/2
port link-mode route
port link-aggregation group 2
#
interface XGE2/3/2
port link-mode route
port link-aggregation group 2
#
```

- 配置与互联网互联接口配置，按实际情况配置，此处不再介绍

(3) Router2 基础配置

参考 1.6.2 通用基础配置模板进行配置。

- 设备命名，需要根据实际命名修改

```
sysname Router2
```

- 配置设备带外管理 IP，IP 地址根据规划进行配置

```
interface M-GigabitEthernet0/0/0
 ip binding vpn-instance mgmt
 ip address 192.166.0.74 255.255.0.0
```

- 设置管理用户，同时作为 netconf 配置下发的帐号，用户名、密码根据规划进行配置

```
local-user admin
 password simpel unicloud123
service-type ssh
 authorization-attribute user-role network-admin
authorization-attribute user-role network-operator
```

- 配置远程访问

```
line vty 0 63
 authentication-mode scheme
 user-role network-admin
 user-role network-operator
 idle-timeout 20 0
```

- 使能 SSH 服务

```
ssh server enable
```

- 使能 netconf ssh 服务

```
netconf ssh server enable
```

- 使能 lldp 及 stp 协议

```
lldp global enable
stp global enable
```

(4) Router2 网络配置

- 使能 OSPF 协议

```
ospf 100 router-id 10.92.50.74
non-stop-routing
area 0.0.0.0
```

- 配置环回口地址并使能 OSPF

```
interface LoopBack0
ip address 10.92.50.74 32
ospf 100 area 0.0.0.0
```

- 配置与 Internet Border 互联接口地址并使能 OSPF

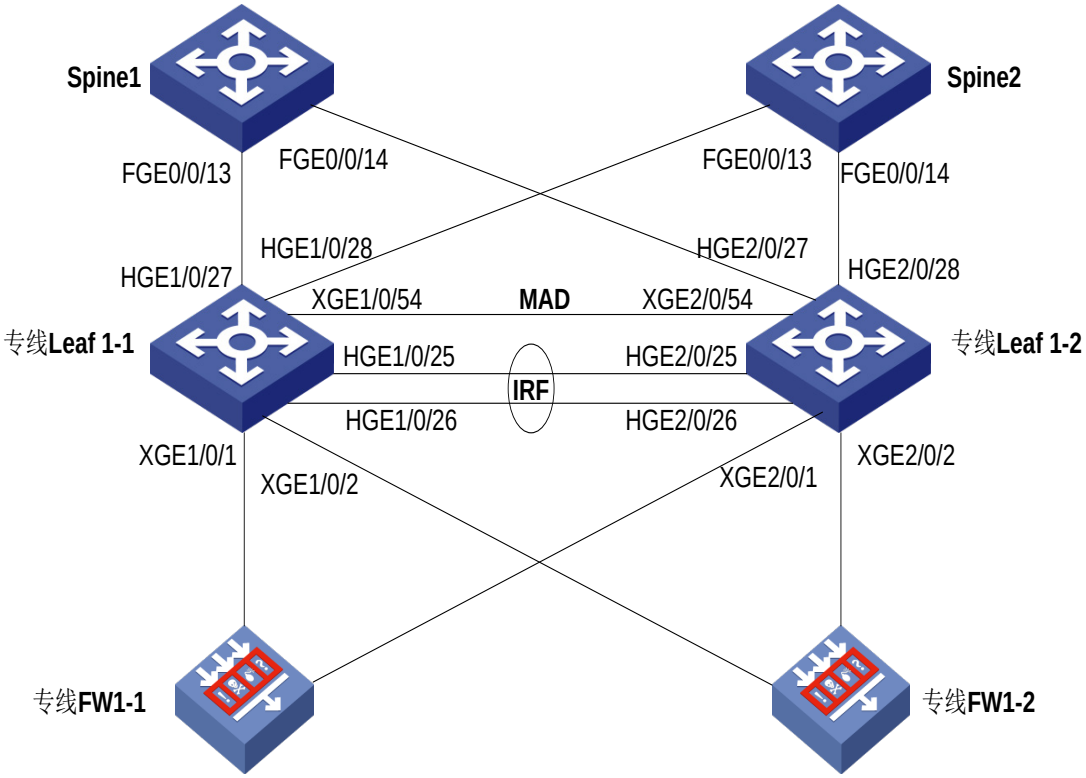
```
interface RAGG2
link-aggregation mode dynamic
ip address 10.92.51.9 30
ip mtu 2000
ospf 100 area 0.0.0.0
ospf network-type p2p
#
interface XGE2/2/2
port link-mode route
port link-aggregation group 2
#
interface XGE2/3/2
port link-mode route
port link-aggregation group 2
#
```

- 配置与互联网互联接口配置，按实际情况配置，此处不再介绍

A.6.7 专线 Leaf 配置（有专线业务时配置）

1. 组网图

图A-9 专线 Leaf 组网图



2. 接口互联表

本端接口	VLAN	IP	对端设备	对端接口	VLAN	IP
BAGG1 XGE1/0/1 XGE2/0/1	998		专线FW1-1	BAG14	Trunk	
BAGG2 XGE1/0/2 XGE2/0/2	998		专线FW1-2	BAG15	Trunk	
HGE1/0/27	/	10.92.51.138/30	Spine1	FGE0/0/13	/	10.92.51.137/30
HGE1/0/28	/	10.92.51.146/30	Spine2	FGE0/0/13	/	10.92.51.145/30
HGE2/0/27	/	10.92.51.142/30	Spine1	FGE0/0/14	/	10.92.51.141/30
HGE2/0/28	/	10.92.51.150/30	Spine2	FGE0/0/14	/	10.92.51.149/30
Loopback0		10.92.30.101				

3. 网络配置

(1) 交换机硬件资源参数配置

参考 1.6.4 交换机硬件参数配置，根据实际交换机型号进行配置，此处以 S6805 为例，配置完成后需要重启设备生效

```
hardware-resource switch-mode ROUTING
 hardware-resource routing-mode ipv6-128
 hardware-resource vxlan l3gw
```

(2) 配置两台交换机设备做 IRF 堆叠

具体参考 1.6.1 堆叠设备配置模板

(3) 堆叠 Leaf 基础配置

参考 1.6.2 通用基础配置模板进行配置

- 设备命名，需要根据实际命名修改

```
sysname LeasedLine_leaf
```

- 配置设备带外管理 IP，IP 地址根据规划进行配置

```
interface M-GigabitEthernet0/0/0
 ip binding vpn-instance mgmt
 ip address 192.166.0.101 255.255.0.0
```

- 设置管理用户，同时作为 netconf 配置下发的帐号，用户名、密码根据规划进行配置

```
local-user admin
 password simpel unicloud123
service-type ssh
 authorization-attribute user-role network-admin
authorization-attribute user-role network-operator
```

- 配置远程访问

```
line vty 0 63
 authentication-mode scheme
 user-role network-admin
 user-role network-operator
 idle-timeout 20 0
```

- 使能 SSH 服务

```
ssh server enable
```

- 使能 netconf ssh 服务

```
netconf ssh server enable
```

- 使能 lldp 及 stp 协议

```
lldp global enable
stp global enable
```

(4) 使能 L2VPN

使能 L2vpn,配置禁止通过 vxlan 隧道学习 mac 和 arp

```
l2vpn enable
vxlan tunnel mac-learning disable
vxlan tunnel arp-learning disable
```

(5) Underlay 路由协议配置

使能 OSPF 协议，实现 leaf 与 spine 的三层互通

```
ospf 1 router-id 10.92.50.101
non-stop-routing
area 0.0.0.0
```

(6) 接口配置

- 配置环回口地址并使能内部网络 OSPF

```
interface LoopBack0
ip address 10.92.50.101 32
ospf 1 area 0.0.0.0
```

- 配置专线 Leaf 上与专线 FW 互联的接入接口为 vtep access 接口 vlan 1000 to 3999

```
#
interface BAGG1
link-aggregation mode dynamic
#
interface BAGG2
link-aggregation mode dynamic
#
interface Ten-GigabitEthernet 1/0/1
 port link-aggregation group 1
#
interface Ten-GigabitEthernet 2/0/1
 port link-aggregation group 1
#
interface Ten-GigabitEthernet 1/0/2
 port link-aggregation group 2
#
interface Ten-GigabitEthernet 2/0/2
 port link-aggregation group 2
#
interface BAGG1
link-aggregation mode dynamic
port link-type trunk
undo port trunk permit vlan 1
stp edged-port
vtep access port
#
interface BAGG2
link-aggregation mode dynamic
port link-type trunk
undo port trunk permit vlan 1
stp edged-port
vtep access port
#
```

- 配置 Leaf 与 Spine 互联接口地址并使能 OSPF

```
interface HGE1/0/27
port link-mode route
ip address 10.92.51.138 30
ospf 1 area 0.0.0.0
ospf network-type p2p
#
interface HGE1/0/28
```

```
port link-mode route
ip address 10.92.51.146 30
ospf 1 area 0.0.0.0
ospf network-type p2p
#
interface HGE2/0/17
port link-mode route
ip address 10.92.51.142 30
ospf 1 area 0.0.0.0
ospf network-type p2p
#
interface HGE2/0/28
port link-mode route
ip address 10.92.51.150 30
ospf 1 area 0.0.0.0
ospf network-type p2p
#
```

(7) BGP 配置

- 配置 BGP 进程，配置 spine 为对等体

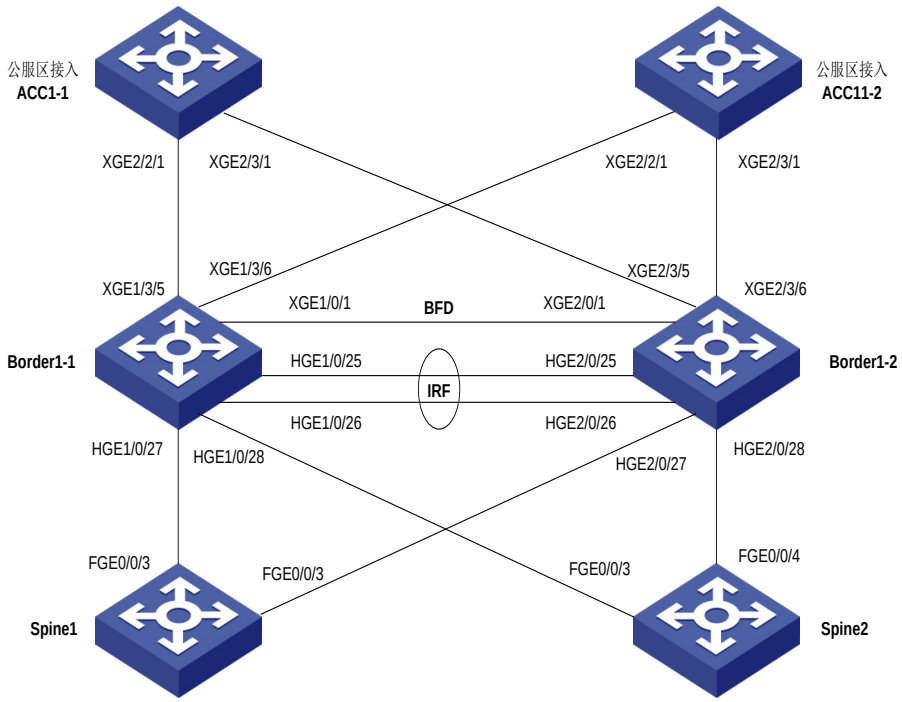
```
bgp 65027
non-stop-routing
router-id 10.92.50.101
peer 10.92.50.77 as-number 65027
peer 10.92.50.77 connect-interface LoopBack0
peer 10.92.50.78 as-number 65027
peer 10.92.50.78 connect-interface LoopBack0
#
address-family l2vpn evpn
peer 10.92.50.77 enable
peer 10.92.50.78 enable
```

A.6.8 Intranet Border 配置

1. 组网说明

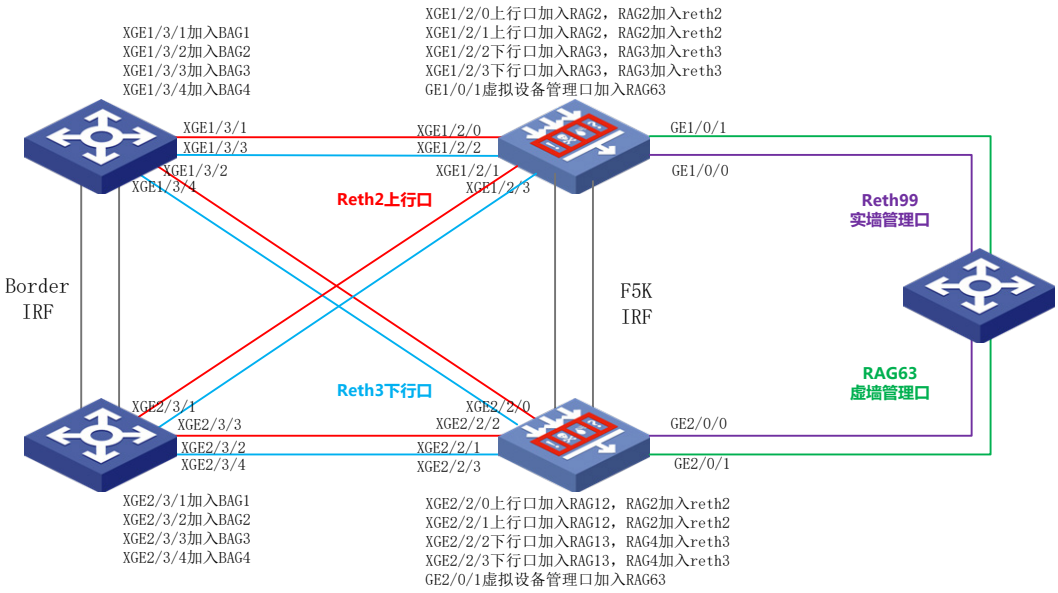
(1) Intranet Border 与 Spine 组网图

图A-10 Intranet Border 与 Spine 组网图



(2) Intranet Border 与旁挂 Intranet FW 组网图

图A-11 Intranet Border 与旁挂 Intranet FW 组网图



2. 接口互联表

本端接口	VLAN	IP	对端设备	对端接口	IP

BAGG1（上行） XGE1/3/1 XGE2/3/1	201	10.92.56.254/24	Intranet FW	Reth1-RAGG1 XGE1/2/3/1 XGE1/2/3/2	/
BAGG2（上行） XGE1/3/2 XGE2/3/2	201	10.92.56.254/24		Reth1-RAGG2 XGE2/2/3/1 XGE2/2/3/2	/
BAGG3（下行） XGE1/3/3 XGE2/3/3	1000-3999	/		Reth2-RAGG3 XGE1/2/3/3 XGE1/2/3/4	/
BAGG4（下行） XGE1/3/4 XGE2/3/4	1000-3999	/		Reth2-RAGG4 XGE2/2/3/3 XGE2/2/3/4	/
RAGG135 XGE1/3/5 XGE2/3/5	/	10.92.51.14/30	公服区接入 ACC	RAGG2	10.92.51.13/30
RAGG136 XGE1/3/6 XGE2/3/6	/	10.92.51.18/30		RAGG3	10.92.51.17/30
HGE1/0/27	/	10.92.51.50/30	Spine1	FGE0/0/3	10.92.51.49/30
HGE1/0/28	/	10.92.51.66/30	Spine2	FGE0/0/3	10.92.51.65/30
HGE2/0/27	/	10.92.51.54/30	Spine1	FGE0/0/4	10.92.51.53/30
HGE2/0/28	/	10.92.51.70/30	Spine2	FGE0/0/4	10.92.51.69/30
Loopback0		10.92.50.2			

3. 网络配置

(1) 交换机硬件资源参数配置

参考 1.6.4 交换机硬件参数配置，根据实际交换机型号进行配置，此处以 S6805 为例，配置完成后需要重启设备生效。

```
hardware-resource switch-mode ROUTING
 hardware-resource routing-mode ipv6-128
 hardware-resource vxlan l3gw
```

(2) 配置两台交换机设备做 IRF 堆叠

具体参考 1.6.1 堆叠设备配置模板

(3) 堆叠 Border 基础配置

参考 1.6.2 通用基础配置模板进行配置

- 设备命名，需要根据实际命名修改

```
sysname Intranet_border
```

- 配置设备带外管理 IP，IP 地址根据规划进行配置

```
interface M-GigabitEthernet0/0/0
 ip binding vpn-instance mgmt
 ip address 192.166.0.2 255.255.0.0
```

- 设置管理用户，同时作为 netconf 配置下发的帐号，用户名、密码根据规划进行配置

```
local-user admin
 password simpel unicloud123
service-type ssh
 authorization-attribute user-role network-admin
authorization-attribute user-role network-operator
```

- 配置远程访问

```
line vty 0 63
 authentication-mode scheme
 user-role network-admin
 user-role network-operator
 idle-timeout 20 0
```

- 使能 SSH 服务

```
ssh server enable
```

- 使能 netconf ssh 服务

```
netconf ssh server enable
```

- 使能 lldp 及 stp 协议

```
lldp global enable
stp global enable
```

(4) 使能 L2VPN

使能 L2vpn,配置禁止通过 vxlan 隧道学习 mac 和 arp

```
l2vpn enable
vxlan tunnel mac-learning disable
vxlan tunnel arp-learning disable
```

(5) Underlay 路由协议配置

- 创建 Border 上行外部网络 VPN 实例

```
ip vpn-instance external_vpn
```

- 创建 Border 上行外部网络 OSPF

```
ospf 100 vpn-instance external_vpn router-id 10.92.50.2
non-stop-routing
vpn-instance-capability simple
area 0.0.0.0
```

- 使能 OSPF 协议，实现 spine 和内部 leaf/border 的三层互通

```
ospf 1 router-id 10.92.50.2
non-stop-routing
area 0.0.0.0
```

(6) 接口配置

- 配置环回口地址并使能内部网络 OSPF

```
interface LoopBack0
ip address 10.92.50.2 32
ospf 1 area 0.0.0.0
```

- 配置安全外网 2 网关地址，作为防火墙上行口的网关，加入外部网络 VPN 实例，使能外部网络 OSPF

```
vlan 201
#
```

```
interface Vlan-interface 201
ip binding vpn-instance external_vpn
ip address 10.92.57.254 24
ip mtu 2000
ospf 100 area 0.0.0.0
ospf network-type p2p
#
interface BAGG1
link-aggregation mode dynamic
#
interface BAGG2
link-aggregation mode dynamic
#
interface Ten-GigabitEthernet 1/3/1
 port link-aggregation group 1
#
interface Ten-GigabitEthernet 2/3/1
 port link-aggregation group 1
#
interface Ten-GigabitEthernet 1/3/2
 port link-aggregation group 2
#
interface Ten-GigabitEthernet 2/3/2
 port link-aggregation group 2
#
interface BAGG1
link-aggregation mode dynamic
port access vlan 201
#
interface BAGG2
link-aggregation mode dynamic
port access vlan 201
#
```

- 配置 border 与防火墙下行口互联接口允许租户承载网 vlan 通过

```
vlan 1000 to 3999
#
interface BAGG3
link-aggregation mode dynamic
#
interface BAGG4
link-aggregation mode dynamic
#
interface Ten-GigabitEthernet 1/3/3
 port link-aggregation group 3
#
interface Ten-GigabitEthernet 2/3/3
 port link-aggregation group 3
#
```

```
interface Ten-GigabitEthernet 1/3/4
 port link-aggregation group 4
#
interface Ten-GigabitEthernet 2/3/4
 port link-aggregation group 4
#
interface BAGG3
link-aggregation mode dynamic
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 1000 to 3999
#
interface BAGG4
link-aggregation mode dynamic
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 1000 to 3999
#
```

- 配置 border 与公服区接入 ACC 互联接口地址，加入外部网络 VPN 实例，并使能外部网络 OSPF

```
interface RAGG135
link-aggregation mode dynamic
#
interface RAGG136
link-aggregation mode dynamic
#
interface Ten-GigabitEthernet 1/3/5
port link-mode route
 port link-aggregation group 135
#
interface Ten-GigabitEthernet 2/3/5
port link-mode route
 port link-aggregation group 135
#
interface Ten-GigabitEthernet 1/3/6
port link-mode route
 port link-aggregation group 136
#
interface Ten-GigabitEthernet 2/3/6
port link-mode route
 port link-aggregation group 136
#

interface RAGG135
link-aggregation mode dynamic
ip binding vpn-instance external_vpn
ip address 10.92.51.14 30
ospf 100 area 0.0.0.0
```

```
ip mtu 2000
ospf network-type p2p
#
interface RAGG136
link-aggregation mode dynamic
ip binding vpn-instance external_vpn
ip address 10.92.51.18 30
ospf 100 area 0.0.0.0
ip mtu 2000
ospf network-type p2p
#
```

- 配置 Border 与 Spine 互联接口地址并使能内部网络 OSPF

```
interface HGE1/0/27
port link-mode route
ip address 10.92.51.50 30
ip mtu 2000
ospf 1 area 0.0.0.0
ospf network-type p2p
#
interface HGE1/0/28
port link-mode route
ip address 10.92.51.66 30
ip mtu 2000
ospf 1 area 0.0.0.0
ospf network-type p2p
#
interface HGE2/0/27
port link-mode route
ip address 10.92.51.54 30
ip mtu 2000
ospf 1 area 0.0.0.0
ospf network-type p2p
#
interface HGE2/0/28
port link-mode route
ip address 10.92.51.70 30
ip mtu 2000
ospf 1 area 0.0.0.0
ospf network-type p2p
#
```

(7) BGP 配置

- 配置 BGP 进程，配置 spine 为对等体

```
bgp 65027
non-stop-routing
router-id 10.92.50.2
peer 10.92.50.77 as-number 65027
peer 10.92.50.77 connect-interface LoopBack0
peer 10.92.50.78 as-number 65027
```

```
peer 10.92.50.78 connect-interface LoopBack0
#
address-family l2vpn evpn
peer 10.92.50.77 enable
peer 10.92.50.78 enable
```

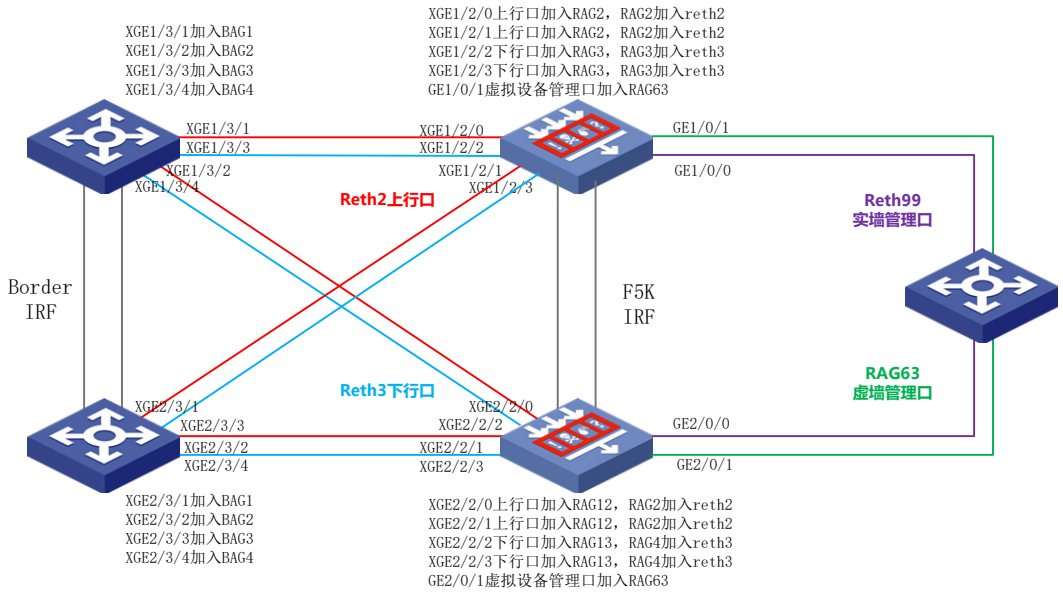
A.6.9 Intranet FW 配置

此处以 F5K 类型防火墙设备作为介绍，M9K 类型防火墙设备配置可以参考 Internet FW 配置

1. 组网图

此处是以 F50X0 系列防火墙为例，其他系列防火墙如果涉及到接口连线或配置有所区别，请以使用的防火墙配置为准。

图A-12 Intranet FW 组网图



2. 接口互联表

本端接口	VLAN	IP	对端设备	对端接口	VLAN	IP
Reth2-RAGG2	/	/	Internet Border	BAGG1	201	10.92.57.254/24
Reth2-RAGG12	/	/		BAGG2	201	10.92.57.254/24
Reth3-RAGG3	/	/		BAGG3	1000-3999	/
Reth3-RAGG13	/	/		BAGG4	1000-3999	/
RAGG63	/	/	管理ACC	BAGG48	106	10.92.31.254/24
Loopback0		10.92.50.82				

3. 网络配置

(1) 配置两台防火墙设备做 IRF 堆叠，

具体参考 1.6.1 堆叠设备配置模板

(2) 配置堆叠防火墙基础配置

参考 1.6.2 通用基础配置模板进行配置

- 设备命名，需要根据实际命名修改

```
sysname Intranet-FW
```

- 配置设备带外管理 IP，IP 地址根据规划进行配置

```
interface Reth99
member interface GigabitEthernet1/0/0 priority 32
member interface GigabitEthernet2/0/0 priority 31
ip address 192.166.0.82 255.255.0.0
```

- 设置管理用户，同时作为 netconf 配置下发的帐号，用户名、密码根据规划进行配置

```
local-user sdn
 password simpel unicloud123
service-type ssh
 authorization-attribute user-role network-admin
authorization-attribute user-role network-operator
```

- 配置远程访问

```
line vty 0 63
 authentication-mode scheme
 user-role network-admin
 user-role network-operator
 idle-timeout 20 0
```

- 使能 SSH 服务

```
ssh server enable
```

- 使能 netconf ssh 服务

```
netconf ssh server enable
```

- 使能 lldp 及 stp 协议

```
lldp global enable
stp global enable
```

- 配置会话同步

```
session synchronization enable asymmetric
```

(3) 防火墙接口配置

配置防火墙与 Border 上行口 Reth2，4 个物理接口配置成 2 个聚合口，2 个聚合口配置成冗余口

```
interface Route-Aggregation2
 link-aggregation mode dynamic
interface Ten-GigabitEthernet1/2/0
 port link-mode route
 port link-aggregation group 2
interface Ten-GigabitEthernet1/2/1
 port link-mode route
 port link-aggregation group 2
```

```
#
interface Route-Aggregation12
 link-aggregation mode dynamic
interface Ten-GigabitEthernet2/2/0
 port link-mode route
 port link-aggregation group 12
interface Ten-GigabitEthernet2/2/1
 port link-mode route
 port link-aggregation group 12
#
interface Reth2
member interface RAGG2 priority 255
member interface RAGG12 priority 100
#
```

- 配置防火墙与 Border 下行口 Reth3，4 个物理接口配置成 2 个聚合口，2 个聚合口配置成冗余口

```
interface Route-Aggregation3
 link-aggregation mode dynamic
interface Ten-GigabitEthernet1/2/2
 port link-mode route
 port link-aggregation group 3
interface Ten-GigabitEthernet1/2/3
 port link-mode route
 port link-aggregation group 3
#
interface Route-Aggregation13
 link-aggregation mode dynamic
interface Ten-GigabitEthernet2/2/2
 port link-mode route
 port link-aggregation group 13
interface Ten-GigabitEthernet2/2/3
 port link-mode route
 port link-aggregation group 13
#
interface Reth3
member interface RAGG3 priority 255
member interface RAGG13 priority 100
```

- 配置环回口地址，用于纳管时填入

```
interface LoopBack0
ip address 10.92.50.82 32
```

- 配置防火墙虚墙接口，该接口会下发“防火墙虚拟设备管理网”网段地址，云平台需要和该地址通信进行防火墙配置下发

```
interface Route-Aggregation63
link-aggregation mode dynamic
interface GigabitEthernet1/0/1
 port link-mode route
 port link-aggregation group 63
```

```
interface GigabitEthernet2/0/1
 port link-mode route
 port link-aggregation group 63
#
```

(4) 冗余组配置

- Track 配置

```
track 2 interface Route-Aggregation2 physical
track 3 interface Route-Aggregation3 physical
track 12 interface Route-Aggregation12 physical
track 13 interface Route-Aggregation13 physical
```

- 冗余组配置。RAGG2、3 为堆叠框 1 的聚合口，配置在 node1 里，RAGG12、13 为堆叠框 2 的聚合口，配置在 node2 里

```
redundancy group 1
 member interface Reth2
 member interface Reth3
node 1
  bind chassis 1
  priority 150
track 2 interface Route-Aggregation2 physical
track 3 interface Route-Aggregation3 physical
node 2
  bind chassis 2
  priority 100
track 12 interface Route-Aggregation12 physical
track 13 interface Route-Aggregation13 physical
```

(5) 防火墙安全策略配置

```
security-policy ip
rule 10 name local-any
action pass
source-zone local
rule 20 name any-local
action pass
destination-zone local
#
security-zone intra-zone default permit
#
security-zone name Trust
import interface Reth2
import interface Route-Aggregation63
#
security-zone name Untrust
import interface Reth1
#
security-zone name Management
 import interface Reth99
```

(6) 防火墙虚墙接口对端设备配置参考

配置防火墙虚墙接口对端设备上配置“防火墙虚拟设备管理网”的网关地址，本指导中为10.92.31.254/24，确保云平台可以和该地址通信。

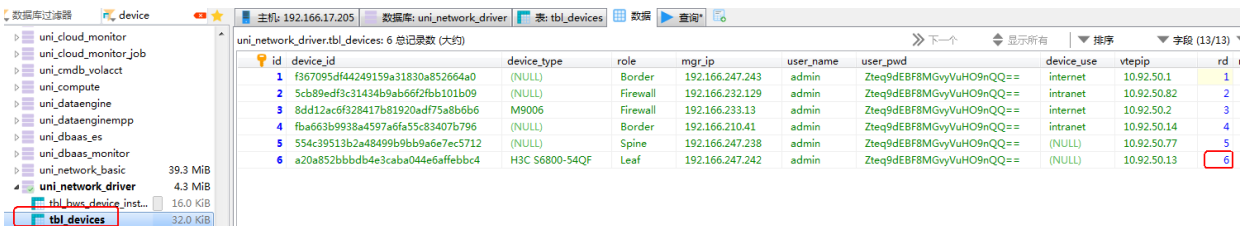
```
interface Bridge-Aggregation48
 port access vlan 106
 link-aggregation mode dynamic
interface Ten-GigabitEthernet1/0/48
 port access vlan 106
 port link-aggregation group 48
interface Ten-GigabitEthernet2/0/48
 port access vlan 106
 port link-aggregation group 48
#
interface Vlan-interface106
 ip address 10.93.31.254 255.255.255.0
```

A.7 租管互通网络配置

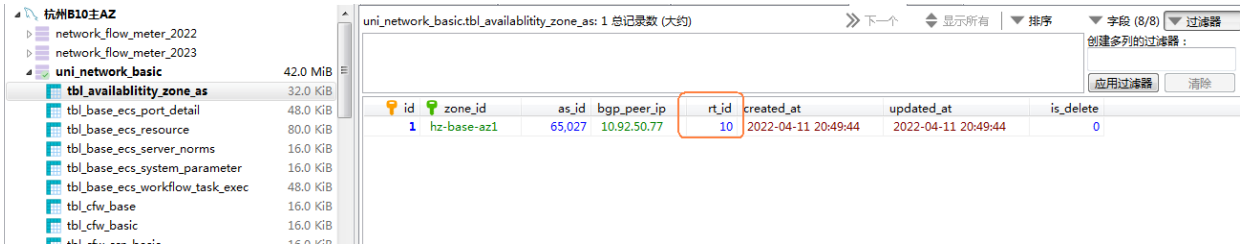
说明

- 租户互通需要在网络 overlay Leaf 上进行配置，实验室环境复用了裸金属的网络 overlay Leaf 设备。
- 配置指导中的 900、901 为模板配置，非特别情况下建议不修改。

(1) 查找数据库，找到需要配置的网络 overlay Leaf 设备的 RD 值。



(2) 查找数据库，找到对应 AZ 的租管互通的的 RT 值。



(3) 创建租管互通 VPC 的 vpn 实例，rd、rt 值与数据库中保持一致。

```
ip vpn-instance moove-manager
 route-distinguisher 6:901
 description PRE_confige_moove-manager
 #
```

```
 address-family ipv4
  vpn-target 0:901 10:901 import-extcommunity
  vpn-target 10:901 export-extcommunity
 #
 address-family evpn
  vpn-target 0:901 10:901 import-extcommunity
  vpn-target 10:901 export-extcommunity
#创建租管互通 VPC 的 vsi 接口
interface Vsi-interface900
 description PRE_confige_VSI_Interface_900
 ip binding vpn-instance moove-manager
 ip address 100.100.63.254 255.255.192.0 sub
 mac-address fe54-00f6-cf41
 distributed-gateway local
#
interface Vsi-interface901
 description PRE_confige_901
 ip binding vpn-instance moove-manager
 l3-vni 901
```

(4) 创建租管互通 VPC 的 vsi

```
vsi CORE_AGENT_VSI_900
 gateway vsi-interface 900
 statistics enable
 arp suppression enable
 flooding disable all
 vxlan 900
 evpn encapsulation vxlan
  route-distinguisher auto
  vpn-target auto export-extcommunity
  vpn-target auto import-extcommunity
```

(5) 配置租管互通 VPC 的 nginx 接入接口

```
vlan900
#
interface BAGG1
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 900
 stp edged-port
 vtep access port
 #
 service-instance 900
  encapsulation s-vid 900
  xconnect vsi CORE_AGENT_VSI_900
#
interface BAGG2
port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 900
```

```
 stp edged-port
 vtep access port
 #
 service-instance 900
  encapsulation s-vid 900
  xconnect vsi CORE_AGENT_VSI_900
#
interface BAGG3
port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 900
 stp edged-port
 vtep access port
 #
 service-instance 900
  encapsulation s-vid 900
  xconnect vsi CORE_AGENT_VSI_900
```

(6) 配置租管互通 VPC 的 BGP 网络

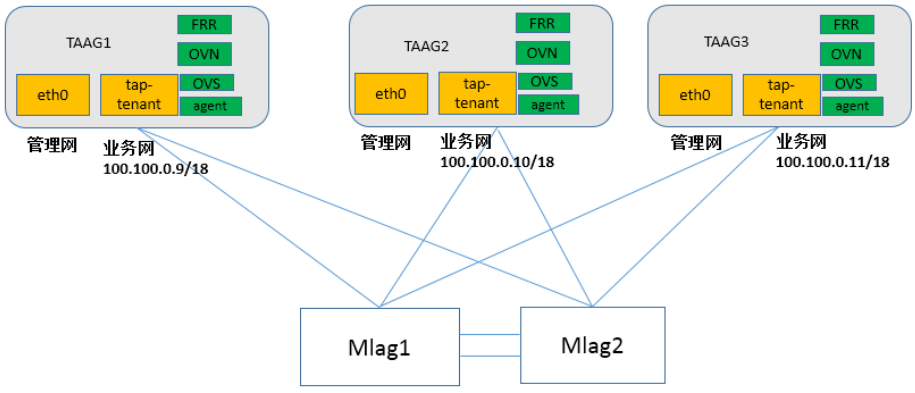
```
bgp 65027
#
 ip vpn-instance moove-manager
  #
  address-family ipv4 unicast
   balance 4
   network 100.100.0.0 255.255.192.0
   network 100.100.63.254 255.255.255.255
#
```

A.8 租管互通主机Overlay方式对接Mlag配置

A.8.1 组网及地址规划

1. 组网图

TAAG 三台虚机业务口分别连 Mlag 交换机，在虚机里创建 Business 网桥，并创建 tap-tenant 端口，作为租管互通端口。



2. IP 地址规划

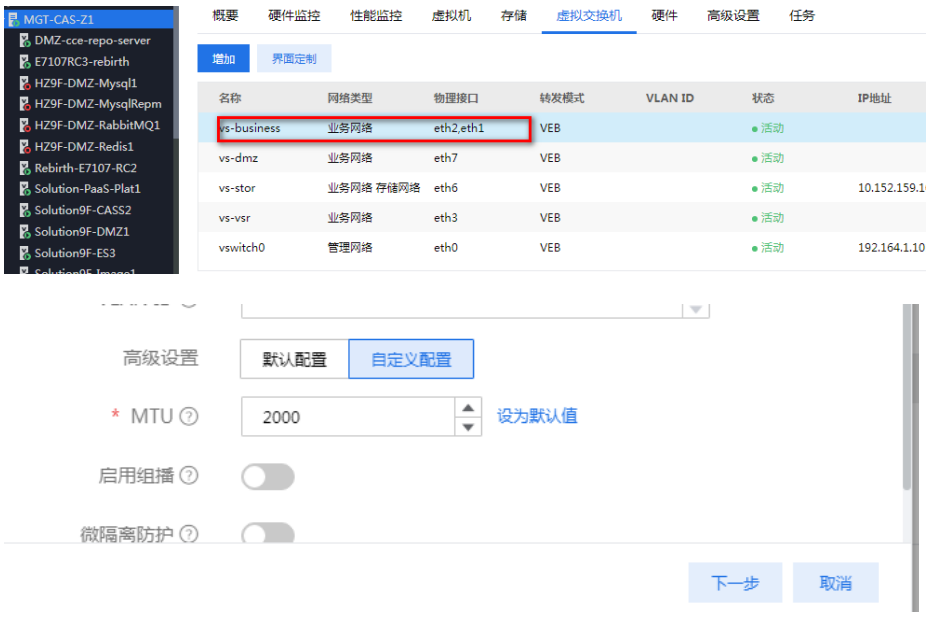
网络名称	IP 地址段	描述
管理网	192.164.1.0/24	TAAG虚机管理地址和云平台管理网同一网段。同时配置VIP
Vtep地址	10.92.55.0/24	TAAG虚机业务网卡地址，vlan为30，网关vlanif 30在Mlag交换机上。Vxlan的Vtep地址，用此地址和Spine建立EVPN邻居。
租管互通地址	100.100.0.0/24	TAAG虚机上tap-tenant地址，配置100.100.0.0/24网段地址，掩码配置为18位。同时配置VIP

A.8.2 TAAG 虚机及对端 Mlag 设备配置

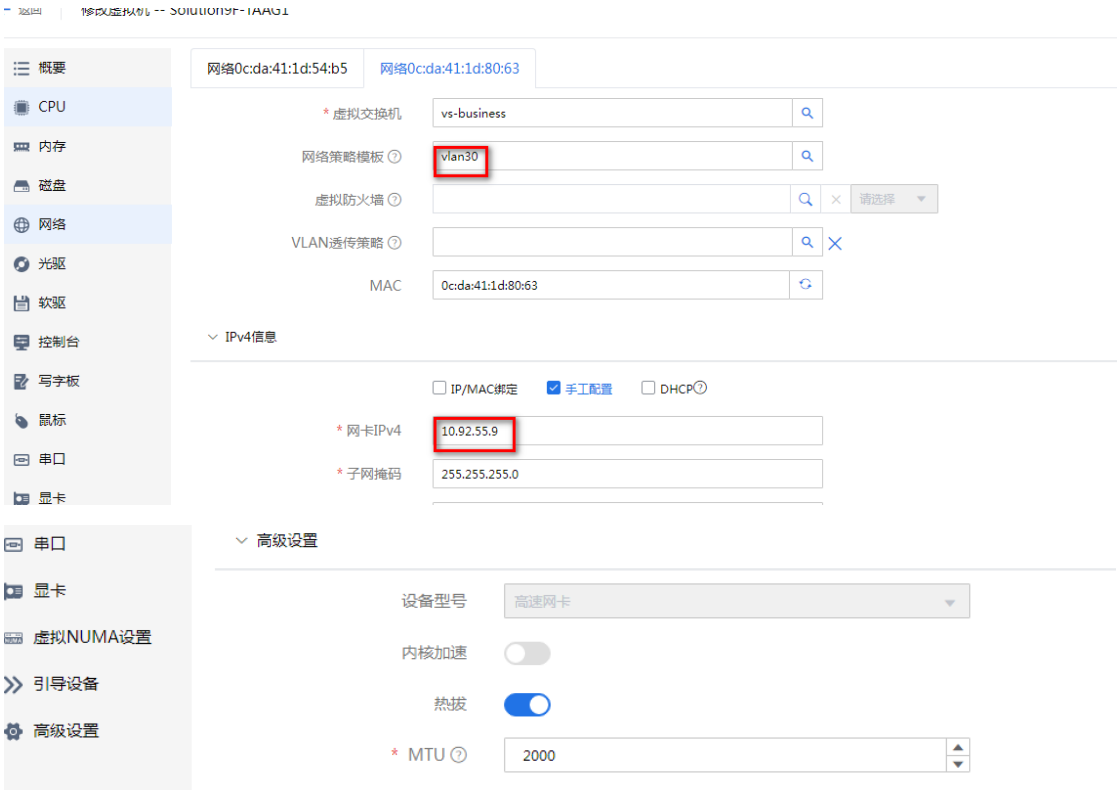
1. TAAG 虚机配置

(1) 管区 VKS 业务口 eth1 和 eth2 连接 Mlag 配置的 leaf。

(2) 创建 vs-business 虚机交换机做聚合，成员口为 eth1 和 eth2，并设置 mtu 为 2000。



(3) 配置 taag 上 vtep 的地址，vlan 配置为 30，MTU 配置为 2000，由于要转发 vxlan 报文，为了避免分片，需要配置全链路上的三层口的 MTU 为 2000（包括交换机上 vlanif 30、Spine 和 Mlag 交换机互联的三层物理口等）



(4) 配置到 Spine 及其他 VKS 的 vtep 路由，保证 taag 到 Spine 和其他 VKS 的 vtep 全部网络可达。

(5) Spine loopback0 地址网段 10.92.50.0。

(6) 业务 VKS 1 210.10.12.0/24。

```
[root@Solution9F-TAAG1 ~]# more /etc/sysconfig/static-routes
any net 10.92.52.0/24 gw 10.92.55.254
any net 10.92.50.0/24 gw 10.92.55.254
```

```
[root@Solution9F-TAAG1 ~]# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.164.1.254   0.0.0.0         UG    0      0        0 eth0
10.92.50.0      10.92.55.254    255.255.255.0   UG    0      0        0 eth1
10.92.52.0      10.92.55.254    255.255.255.0   UG    0      0        0 eth1
10.92.55.0      0.0.0.0         255.255.255.0   U     0      0        0 eth1
10.244.0.0      192.164.1.10    255.255.255.0   UG    0      0        0 eth0
10.244.2.0      192.164.1.11    255.255.255.0   UG    0      0        0 eth0
100.100.0.0     0.0.0.0         255.255.192.0   U     0      0        0 tap-tenant
172.17.0.0      0.0.0.0         255.255.0.0     U     0      0        0 docker0
192.164.1.0     0.0.0.0         255.255.255.0   U     0      0        0 eth0
```

2. Mlag/DRNI 交换机创建 vtep 的网关

聚合口配置：

```
#
interface Bridge-Aggregation3
 port link-type trunk
```

```
 undo port trunk permit vlan 1
 port trunk permit vlan 30
port drni group 3 allow-single-member(只连了一台 leaf)
 link-aggregation mode dynamic
 port drni group 3（标准配置）
#
网关接口配置，下面配置是 vrrp 主
interface Vlan-interface30
 ip address 10.92.55.1 255.255.255.0
 vrrp vrid 4 virtual-ip 10.92.55.254
 vrrp vrid 4 priority 200（取值范围 1-254，数值越大优先级越高）
 ip mtu 2000

网关接口配置，下面配置是 vrrp 从
interface Vlan-interface30
 ip address 10.92.55.2 255.255.255.0
 vrrp vrid 4 virtual-ip 10.92.55.254
 vrrp vrid 4 priority 100
 ip mtu 2000

#
查看 vrrp 状态
```

```
[VSR-switch1]dis vrrp
IPv4 Virtual Router Information:
 Running mode : Standard
 Total number of virtual routers : 4
 Interface          VRID  State        Running Adver   Auth      Virtual
                                        Pri     Timer   Type        IP
 ------------------------------------------------------------------------
 Vlan30             4     Master       200     100     None      10.92.55.254
 Vlan1001           1     Master       200     100     None      11.92.51.9
 Vlan1002           2     Master       200     100     None      11.92.52.254
 Vlan1003           3     Master       200     100     None      11.92.53.254
```

3. 配置 VIP

管理口的 VIP。

```
[root@Solution9F-TAAG1 ~]# more /etc/keepalived/keepalived.conf
global_defs {
    enable_script_security
}

vrrp_script haproxy-check {
    user root
    script "/bin/bash /etc/keepalived/check_haproxy.sh"
    interval 3
    weight -2
    fall 10
    rise 2
}

vrrp_instance haproxy-vip {
    state BACKUP
    priority 101
    interface eth0
    virtual_router_id 47
    advert_int 3
    unicast_src_ip 192.164.1.9
    unicast_peer {
        192.164.1.10
        192.164.1.11
    }

    virtual_ipaddress {
        192.164.1.203/24
    }

    track_script {
        haproxy-check
    }
}
```

TAAG 网卡的 VIP，注意需要把 Interface 写成 tap-tenant。

```
vrrp_instance nginx-vip {
state BACKUP
priority 101
interface tap-tenant
virtual_router_id 48
advert_int 3
unicast_src_ip 100.100.0.9
unicast_peer {
100.100.0.10
100.100.0.11
}
virtual_ipaddress {
100.100.0.8/18
}
track_script {
nginx-check
}
}
```

A.8.3 主机 overlay 环境搭建

1. 城市安装依赖包

(1) 需要配置 yum 源，配置本地 yum 源或者能连上互联网 yum 源（配置代理）。

```
yum install libunwind  unbound-libs  libibverbs python3  c-areroute-nroutes c-ares -y
```

```
[root@Solution9F-TAAG1 yum.repos.d]# yum install libunwind  unbound-libs  libibverbs python3  c-areroute-nroutes c-ares -y
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
Package matching python3-3.6.8-17.el7.x86_64 already installed. Checking for update.
No package c-areroute-nroutes available.
Resolving Dependencies
--> Running transaction check
---> Package c-ares.x86_64 0:1.10.0-3.el7 will be installed
---> Package libibverbs.x86_64 0:22.4-5.el7 will be installed
--> Processing Dependency: rdma-core(x86-64) = 22.4-5.el7 for package: libibverbs-22.4-5.el7.x86_64
---> Package libunwind.x86_64 2:1.2-2.el7 will be installed
---> Package unbound-libs.x86_64 0:1.6.6-5.el7_8 will be installed
--> Processing Dependency: libevent-2.0.so.5()(64bit) for package: unbound-libs-1.6.6-5.el7_8.x86_64
--> Running transaction check
---> Package libevent.x86_64 0:2.0.21-4.el7 will be installed
---> Package rdma-core.x86_64 0:22.4-5.el7 will be installed
--> Finished Dependency Resolution
```

(2) 执行 rpm -ivh libyang-0.16.111-0.x86_64.rpm，安装 libyang-0.16.111-0.x86_64.rpm。

rpm 包可以从如下路径获取：

https://unidrive.unicloud.com:443/link/A831FF81932122944F3B5C93CD9411CC

```
[root@Solution9F-TAAG1 taag]# rpm -ivh libyang-0.16.111-0.x86_64.rpm
Preparing...                          ################################# [100%]
Updating / installing...
   1:libyang-0.16.111-0               ################################# [100%]
[root@Solution9F-TAAG1 taag]#
```

2. 安装 OVS

在主机 overlay 的组件包中（可以在 ansible 的虚机中找到）安装 ovs，首先解压，然后执行。

```
tar -zxvf UNI_NETWORK_UCS_V3.4.3_Build0028.tar.gz
cd UNI_NETWORK_UCS_V3.4.3_Build0028/ovs/kernel
chmod 777 run_ovs_kernel.sh
```

```
./run_ovs_kernel.sh
```

使用 systemctl status openvswitch 检查服务状态。

```
[root@Solution9F-TAAG1 kernel]# ./run_ovs_kernel.sh
Preparing...                          ################################# [100%]
Updating / installing...
   1:openvswitch-2.13.1-uni.network.uc################################# [100%]
[root@Solution9F-TAAG1 kernel]# systemctl status openvswitch
● openvswitch.service - LSB: Open vSwitch switch
   Loaded: loaded (/etc/rc.d/init.d/openvswitch; bad; vendor preset: disabled)
   Active: active (running) since Tue 2023-01-31 16:37:13 CST; 11s ago
     Docs: man:systemd-sysv-generator(8)
  Process: 43625 ExecStart=/etc/rc.d/init.d/openvswitch start (code=exited, status=0/SUCCESS)
    Tasks: 4
   Memory: 6.0M
   CGroup: /system.slice/openvswitch.service
           ├─43653 ovsdb-server: monitoring pid 43654 (healthy)
           ├─43654 ovsdb-server /etc/openvswitch/conf.db -vconsole:emer -vsyslog:err -vfile:info --remote=punix:/var/run/openvswitch/db.sock --private-k..
           ├─43671 ovs-vswitchd: monitoring pid 43672 (healthy)
           └─43672 ovs-vswitchd unix:/var/run/openvswitch/db.sock -vconsole:emer -vsyslog:err -vfile:info --mlockall --no-chdir --log-file=/var/log/open..
```

3. 安装 OVN

在 overlay 的组件包中安装 ovn，依次执行如下命令。

```
cd UNI_NETWORK_UCS_V3.3.6_Build0030/ovn/
chmod 777 run_ovn.sh
./run_ovn.sh
```

使用 systemctl status ovn-controller 检查服务状态。

```
[root@Solution9F-TAAG1 ovn]# systemctl status ovn-controller
● ovn-controller.service - OVN controller daemon
   Loaded: loaded (/usr/lib/systemd/system/ovn-controller.service; enabled; vendor preset: disabled)
   Active: active (running) since Tue 2023-01-31 16:41:32 CST; 56s ago
 Main PID: 46733 (ovn-controller)
   CGroup: /system.slice/ovn-controller.service
           └─46733 ovn-controller unix:/var/run/openvswitch/db.sock -vconsole:emer -vsyslog:err -vfile:info --

Jan 31 16:41:32 Solution9F-TAAG1 systemd[1]: Starting OVN controller daemon...
Jan 31 16:41:32 Solution9F-TAAG1 ovn-ctl[46718]: Starting ovn-controller [  OK  ]
Jan 31 16:41:32 Solution9F-TAAG1 systemd[1]: Started OVN controller daemon.
```

4. 安装 FRR

在 overlay 的组件包中安装 FRR。

```
cd UNI_NETWORK_UCS_V3.3.6_Build0030/frr
chmod 777 frr_install.sh
./frr_install.sh
```

查询 FRR 服务状态。

```
[root@Solution9F-TAAG1 frr]# systemctl status frr
● frr.service - FRRouting
   Loaded: loaded (/etc/systemd/system/frr.service; enabled; vendor preset: disabled)
   Active: active (running) since Tue 2023-01-31 16:54:32 CST; 5s ago
     Docs: https://frrouting.readthedocs.io/en/latest/setup.html
  Process: 56140 ExecStop=/usr/lib/frr/frrinit.sh stop (code=exited, status=0/SUCCESS)
  Process: 56164 ExecStart=/usr/lib/frr/frrinit.sh start (code=exited, status=0/SUCCESS)
   Status: "FRR Operational"
    Tasks: 13
   Memory: 13.0M
   CGroup: /system.slice/frr.service
           ├─56169 /usr/lib/frr/watchfrr -d -F traditional zebra bgpd ospfd staticd
           ├─56187 /usr/lib/frr/zebra -d -F traditional -A 127.0.0.1 -s 90000000 --log file:/var/log/frr/zebra.log
           ├─56191 /usr/lib/frr/bgpd -d -F traditional -A 127.0.0.1 --log file:/var/log/frr/bgpd.log
           ├─56197 /usr/lib/frr/ospfd -d -F traditional -A 127.0.0.1 --log file:/var/log/frr/ospfd.log
           └─56200 /usr/lib/frr/staticd -d -F traditional -A 127.0.0.1
```

5. 安装 network-cvk-agent

在 overlay 的组件包中安装 network-cvk-agent。

```
rpm -ivh network-cvk-agent-release-v3.3.6_E7107_RC2.x86_64.rpm
```

使用 systemctl status network-cvk-agent。

```
[root@Solution9F-TAAG1 taag]# systemctl status network-cvk-agent
● network-cvk-agent.service - UNI NETWORK CVK Agent Daemon
   Loaded: loaded (/usr/lib/systemd/system/network-cvk-agent.service; enabled; vendor preset: disabled)
   Active: active (running) since Tue 2023-01-31 16:58:16 CST; 10s ago
 Main PID: 58713 (network-cvk-age)
   CGroup: /system.slice/network-cvk-agent.service
           └─58713 /usr/local/bin/network-cvk-agent
```

6. 创建 tap-tenant 网卡

装完主机 overlay 的组件会创建一个 bsiness 的网桥。

```
[root@Solution9F-TAAG1 taag]# ovs-vsctl show
0f0b9df4-bb05-4239-b85e-a1949b9a5086
    Bridge business
        fail_mode: secure
        Port business
            Interface business
                type: internal
    ovs_version: "2.13.1"
```

执行下面命令创建网卡。

```
ovs-vsctl add-port business tap-tenant -- set interface tap-tenant type=internal
ifconfig tap-tenant 100.100.0.9/18 （租管互通网段分配的 IP 地址，这个地址必须是 100.100.0.网段） up
ifconfig tap-tenant mtu 1500
```

```
[root@Solution9F-TAAG1 taag]# ovs-vsctl add-port business tap-tenant -- set interface tap-tenant type=internal
[root@Solution9F-TAAG1 taag]# ifconfig tap-tenant 100.100.63.81/18 up
[root@Solution9F-TAAG1 taag]# ifconfig tap-tenant mtu 1500
```

添加完之后，在/etc/sysconfig/network-scripts 下创建 ifcfg-tap-tenant 配置文件持久化，mac 地址、IP、掩码都需要填写，格式样例如下：

```
[root@Solution9F-TAAG1 ~]# more /etc/sysconfig/network-scripts/ifcfg-tap-tenant
DEVICE=tap-tenant
ONBOOT=yes
MTU=1500
MACADDR=de:64:da:7b:8b:6f
BOOTPROTO=none
TYPE=Ethernet
IPADDR=100.100.0.9
NETMASK=255.255.192.0
[root@Solution9F-TAAG1 ~]#
```

7. 配置 BGP 配置

Spine 上配置 taag 的 BGP 信息，不需要配置成反射器。

```
#
bgp 65027
 non-stop-routing
 router-id 10.92.50.77
 peer 10.92.50.1 as-number 65027
```

```
peer 10.92.50.1 connect-interface LoopBack0
peer 10.92.50.13 as-number 65027
peer 10.92.50.13 connect-interface LoopBack0
peer 10.92.50.23 as-number 65027
peer 10.92.50.23 description ED
peer 10.92.50.23 connect-interface LoopBack0
peer 10.92.50.101 as-number 65027
peer 10.92.50.101 connect-interface LoopBack0
peer 10.92.52.1 as-number 65027
peer 10.92.52.1 connect-interface LoopBack0
peer 10.92.52.2 as-number 65027
peer 10.92.52.2 connect-interface LoopBack0
peer 10.92.52.6 as-number 65027
peer 10.92.52.6 connect-interface LoopBack0
peer 10.92.52.7 as-number 65027
peer 10.92.52.7 connect-interface LoopBack0
peer 10.92.52.11 as-number 65027
peer 10.92.52.11 connect-interface LoopBack0
peer 10.92.52.12 as-number 65027
peer 10.92.52.12 connect-interface LoopBack0
peer 10.92.52.13 as-number 65027
peer 10.92.52.13 connect-interface LoopBack0
peer 10.92.52.14 as-number 65027
peer 10.92.52.14 connect-interface LoopBack0
peer 10.92.52.90 as-number 65027
peer 10.92.52.90 connect-interface LoopBack0
peer 10.92.52.91 as-number 65027
peer 10.92.52.91 connect-interface LoopBack0
peer 10.92.55.9 as-number 65027
peer 10.92.55.9 connect-interface LoopBack0
peer 10.92.55.10 as-number 65027
peer 10.92.55.10 connect-interface LoopBack0
peer 10.92.55.11 as-number 65027
peer 10.92.55.11 connect-interface LoopBack0
peer 11.92.50.10 as-number 65027
peer 11.92.50.10 connect-interface LoopBack0
#
address-family ipv4 unicast
 peer 10.92.50.1 enable
 peer 10.92.50.13 enable
 peer 10.92.50.101 enable
 peer 10.92.52.1 enable
 peer 10.92.52.2 enable
 peer 10.92.52.6 enable
 peer 10.92.52.7 enable
 peer 10.92.52.11 enable
 peer 10.92.52.12 enable
 peer 10.92.52.13 enable
```

```
  peer 10.92.52.14 enable
  peer 10.92.52.90 enable
  peer 10.92.52.91 enable
  peer 10.92.55.9 enable
  peer 10.92.55.10 enable
  peer 10.92.55.11 enable
 #
 address-family l2vpn evpn
  undo policy vpn-target
  peer 10.92.50.1 enable
  peer 10.92.50.1 reflect-client
  peer 10.92.50.13 enable
  peer 10.92.50.13 reflect-client
  peer 10.92.50.23 enable
  peer 10.92.50.23 reflect-client
  peer 10.92.50.101 enable
  peer 10.92.50.101 reflect-client
  peer 10.92.52.1 enable
  peer 10.92.52.2 enable
  peer 10.92.52.6 enable
  peer 10.92.52.6 reflect-client
  peer 10.92.52.7 enable
  peer 10.92.52.7 reflect-client
  peer 10.92.52.11 enable
  peer 10.92.52.12 enable
  peer 10.92.52.13 enable
  peer 10.92.52.14 enable
  peer 10.92.52.90 enable
  peer 10.92.52.91 enable
  peer 10.92.55.9 enable
  peer 10.92.55.10 enable
  peer 10.92.55.11 enable
  peer 11.92.50.10 enable
  peer 11.92.50.10 reflect-client
#
```

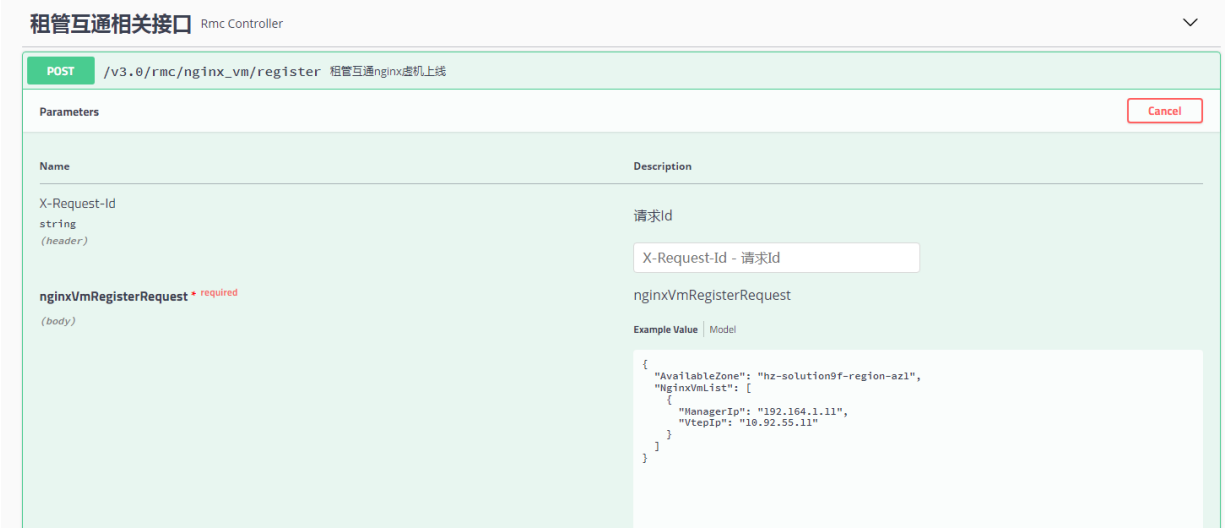
TAAG 虚机配置，使用 UCA K8S 的 VIP 访问 swagger。

http://192.164.1.201:40465/uca/network/swagger-ui.html

AvailableZone：可用区 ID

ManagerIp：TAAG 虚机的管理地址

VtepIp：TAAG 虚机的 VTEP 地址



配置完成后检查 BGP 建立信息，邻居建立起来。

```
[root@Solution9F-TAAG1 ~]# vtysh -c "show bgp summary"

IPv4 Unicast Summary:
BGP router identifier 10.92.55.9, local AS number 65027 vrf-id 0
BGP table version 0
RIB entries 0, using 0 bytes of memory
Peers 2, using 41 KiB of memory

Neighbor        V         AS MsgRcvd MsgSent   TblVer  InQ OutQ  Up/Down State/PfxRcd
10.92.50.77     4      65027   10358    7720        0    0    0 06:29:15            0
10.92.50.78     4      65027       0       0        0    0    0    never       Connect

Total number of neighbors 2

L2VPN EVPN Summary:
BGP router identifier 10.92.55.9, local AS number 65027 vrf-id 0
BGP table version 0
RIB entries 459, using 82 KiB of memory
Peers 2, using 41 KiB of memory

Neighbor        V         AS MsgRcvd MsgSent   TblVer  InQ OutQ  Up/Down State/PfxRcd
10.92.50.77     4      65027   10358    7720        0    0    0 06:29:15          682
10.92.50.78     4      65027       0       0        0    0    0    never       Connect

Total number of neighbors 2
```

8. 验证租管互通联通性

Ping 租管互通的网关 100.100.63.254 和 SLB 的地址 100.100.6.134 都可以通。

ping –s 1500 100.100.6.134 通过指定包大小来验证。

```
[root@Solution9F-TAAG1 ~]# ping 100.100.63.254
PING 100.100.63.254 (100.100.63.254) 56(84) bytes of data.
64 bytes from 100.100.63.254: icmp_seq=1 ttl=254 time=0.729 ms
^C
--- 100.100.63.254 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.729/0.729/0.729/0.000 ms
[root@Solution9F-TAAG1 ~]# ping 100.100.6.134
PING 100.100.6.134 (100.100.6.134) 56(84) bytes of data.
64 bytes from 100.100.6.134: icmp_seq=1 ttl=64 time=1.68 ms
^C
```

A.9 数据库服务访问对象存储配置

A.9.1 Intranet border 配置

(1) 创建租管互通 VPC 的 vpn 实例，rd、rt 值与数据库中保持一致，参考 1.8 租管互通网络配置

```
ip vpn-instance moove-manager
 route-distinguisher 6:901
 description PRE_confige_moove-manager
 #
 address-family ipv4
  vpn-target 0:901 10:901 import-extcommunity
  vpn-target 10:901 export-extcommunity
 #
 address-family evpn
  vpn-target 0:901 10:901 import-extcommunity
  vpn-target 10:901 export-extcommunity
```

(2) 创建租管互通 VPC 的 L3 vsi 接口

```
interface Vsi-interface901
 description PRE_confige_901
 ip binding vpn-instance moove-manager
 l3-vni 901
```

(3) 配置租管互通 VPC 的 BGP 网络，引入静态路由

```
bgp 65027
#
 ip vpn-instance moove-manager
  #
  address-family ipv4 unicast
   default-route imported
   balance 4
   import-route static
```

(4) 手动配置租管互通 VPC，Intranet Border 和 Intranet FW 之间的租户承载网地址

```
vlan 999
interface Vlan-interface999
 ip binding vpn-instance moove-manager
 ip address 10.92.47.251 255.255.248.0 sub
```

```
ip route-static vpn-instance  moove-manager 100.64.0.0 10 10.92.47.252 description
CORE_AGENT_ROUT

interface Bridge-Aggregation 3
 port trunk permit  vlan 999
```

A.9.2 Intranet FW 配置

(1) 进入 VFW_Intranet 的 context

```
switchto context VFW_Intranet
```

(2) 创建租户互通 VPC 的 vpn 实例

```
 ip vpn-instance moove-manager
```

(3) 从 Intranet NAT 地址池中取一个地址，作为租管互通 VPC 的 SNAT 地址，创建 nat address-group

```
nat address-group 10999 name INTERNAL_SNAT_GROUP_moove_manager_10999
 address 100.66.7.252 100.66.7.252
```

(4) 在 Intranet FW 上行口配置 nat outbond

```
interface Reth1
nat outbound name INTERNAL_SNAT_ACL_moove_manager_10999 address-group 10999 vpn-instance
external_vpn
```

(5) 在 Intranet FW 下行口配置租管互通 VPC 和 Intranet Border 互联的租户承载网地址

```
interface Reth2.999
 description moove_manager_Reth2.999
 ip binding vpn-instance moove-manager
 ip address 10.92.47.252 255.255.248.0
 vlan-type dot1q vid 999
```

(6) 在安全域中添加租管互通 VPC 对应的接口

```
security-zone name Trust
 import interface Reth2.999

security-zone name moovemanager
 import ip 100.100.0.0 18 vpn-instance moove-manager
```

(7) 创建租管互通 VPC 各安全域之间的安全策略

```
security-policy ip
  rule 994 name moovemanager-moovemanager
    action pass
    counting enable
    vrf moove-manager
    source-zone moovemanager
    destination-zone moovemanager
  rule 995 name moovemanager-EXTERNAL
    action pass
    counting enable
    vrf moove-manager
    source-zone moovemanager
    destination-zone EXTERNAL
```

```
 rule 996 name moovemanager-Local
  action pass
  counting enable
  vrf moove-manager
  source-zone moovemanager
  destination-zone Local
 rule 997 name EXTERNAL-moovemanager
  action pass
  counting enable
  vrf moove-manager
  source-zone EXTERNAL
  destination-zone moovemanager
 rule 998 name EXTERNAL-Local
  action pass
  counting enable
  vrf moove-manager
  source-zone EXTERNAL
  destination-zone Local
 rule 999 name Local-moovemanager
  action pass
  counting enable
  vrf moove-manager
  source-zone Local
  destination-zone moovemanager
```

(8) 配置静态路由，去往公服区业务网段 100.66.1.0/24 的下一跳地址为安全外网 2 的网段地址 10.92.57.254；去往租管互通 VPC 网段 100.100.0.0/18 的下一跳地址为 Intranet Border 上的租户承载网地址

```
ip route-static vpn-instance moove-manager 100.66.1.0 24 vpn-instance external_vpn 10.92.57.254 description CORE_AGENT_ROUTE
 ip route-static vpn-instance moove-manager 100.100.0.0 18 10.92.47.251 description CORE_AGENT_ROUTE
```

(9) 配置 ACL

```
acl advanced name INTERNAL_SNAT_ACL_moove_manager_10999
 rule 40000 permit ip vpn-instance moove-manager
```

A.10 裸金属PXE管理交换机配置

裸金属 PXE 管理交换机设备配置 IRF 堆叠且需要被纳管。

A.10.1 接口互联表

本端接口	VLAN	IP	对端设备	对端接口	IP
RAGG15	/	10.92.53.5/30	管理ACC	RAGG15	10.92.53.6/30
FGE1/0/15	115	10.250.2.62	BM	eth0	
Loopback0		10.92.50.27			

A.10.2 网络配置

(1) 使能 OSPF 协议，实现 spine 和 leaf/border 的三层互通

```
ospf 10 router-id 10.92.50.27
non-stop-routing
area 0.0.0.0
```

(2) 配置环回口地址并使能 OSPF

```
interface LoopBack0
ip address 10.92.50.27 32
ospf 1 area 0.0.0.0
```

(3) 使能 DHCP

```
 dhcp enable
```

(4) 配置 DHCP server 地址池，next-server 地址为 tftp server 地址，tftp server 可以直接部署在 Image server 上

```
dhcp server ip-pool 1
 gateway-list 10.250.2.62
 network 10.250.2.0 mask 255.255.255.192
 address range 10.250.2.1 10.250.2.61
 bootfile-name pxelinux/bootx64.efi
 next-server 192.167.100.38
 tftp-server ip-address 192.167.100.38
```

(5) 配置 DHCP 网关接口地址，配置连接裸金属 PXE 接口

```
vlan 115
#
interface Vlan-interface115
 description Bare-Metal-Server-Mgmt
 ip address 10.250.2.62 255.255.255.192
 ospf 10 area 0.0.0.0
#
interface Ten-GigabitEthernet1/0/15
 port link-mode bridge
 description to bm server mg
 port access vlan 115
#
```

(6) 配置裸金属 PXE 管理交换机与管理核心交换机互联接口地址并使能 OSPF，打通裸金属 DHCP 网络和云平台管理网

```
interface RAGG15
link-aggregation mode dynamic
ip address 10.92.53.5 30
ospf 10 area 0.0.0.0
ospf network-type p2p
#
```

(7) 配置远程访问

```
line vty 0 63
```

```
 authentication-mode scheme
 user-role network-admin
 user-role network-operator
 idle-timeout 20 0
```

(8) 使能全局 LLDP

```
lldp global enable
```

(9) 使能 SSH 服务

```
ssh server enable
```

(10) 使能 netcong ssh 服务

```
netconf ssh server enable
```

(11) 新建 local-user 并使能 ssh 服务

```
local-user admin class manage
 password simple Passw0rd@_
 service-type ssh
 authorization-attribute user-role network-admin
 authorization-attribute user-role network-operator
```

A.11 IPV6配置

A.11.1 VFW_Internet 配置

1. 配置 ovpfv3，引入 IPV6 静态路由

(1) 进入虚墙 context

```
switchto context VFW_Internet
```

(2) 创建 IPV6 的 ospfv3 进程，引入 IPV6 静态路由

```
ospfv3 10 vpn-instance external_vpn
router-id 10.92.50.81
non-stop-routing
 import-route direct
 import-route static
 area 0.0.0.0
```

(3) 与 Border 互通的上行接口下添加 ipv6 互联地址并应用 ospfv3

```
interface Reth1
 description PRE_external
 ip binding vpn-instance external_vpn
 ip address 10.92.56.1 255.255.255.0
 ospf network-type p2p
 ospf 1 area 0.0.0.0
 ospfv3 10 area 0.0.0.0
 ipv6 address 2408:80E0:4000:51:0:1:0:2/96
 nat static enable
```

A.11.2 Internet Border 配置

(1) 创建 ospfv3 进程

```
ospfv3 10 vpn-instance external_vpn
```

```
 router-id 10.92.50.1
 non-stop-routing
 import-route direct
 import-route static
 area 0.0.0.0
#
```

(2) 与 FW 互通的上行接口下添加 ipv6 互联地址并应用 ospfv3

```
interface Vlan-interface201
 ip binding vpn-instance external_vpn
 ip address 10.92.56.254 255.255.255.0
 ospf network-type p2p
 ospf 100 area 0.0.0.0
 ospfv3 10 area 0.0.0.0
 ipv6 address 2408:80E0:4000:51:0:1:0:1/96
#
```

A.11.3 Internet Router 配置

1. 把路由器与交换机互联地址的网段默认放通

(1) 创建 permit acl。

```
acl ipv6 advanced name acl_ipv6permit
rule 0 permit ipv6 source 2408:80E0:4000:51:0:6::/96
rule 10 permit ipv6 source 2408:80E0:4000:51:0:5::/96
rule 20 permit ipv6 destination 2408:80E0:4000:51:0:6::/96
rule 30 permit ipv6 destination 2408:80E0:4000:51:0:5::/96
```

说明：2408:80E0:4000:51:0:6::/96 和 2408:80E0:4000:51:0:5::/96 是路由器和 Internet ACC 互联的地址段，需要根据各节点实际情况更改。

(2) 创建 permit classifier。

```
traffic classifier permitipv6 operator and
if-match acl ipv6 name acl_ipv6permit
```

(3) 创建 permit behavior

```
traffic behavior permitipv6
filter permit
```

(4) 路由器出入口应用。

进入入口：qos policy inratelimit

执行命令：classifier permitipv6 behavior permitipv6

进入出口：qos policy outratelimit

执行命令：classifier permitipv6 behavior permitipv6

2. 禁止掉所有过路由器的 IPv6 地址，deny 优先级保证最低，放最后面。

(1) 创建 acl。

```
acl ipv6 advanced name acl_ipv6deny
rule 60000 permit ipv6
```

(2) 创建 classifier。

```
traffic classifier denyipv6 operator and
if-match acl ipv6 name acl_ipv6deny
```

(3) 创建 bahavior。

```
traffic behavior denyipv6
filter deny
```

(4) 路由器出入口应用。

```
进入入口：qos policy inratelimit
    执行命令：classifier denyipv6 behavior denyipv6
进入出口：qos policy outratelimit
    执行命令：classifier denyipv6 behavior denyipv6
进入 qos policy flowstatistic
```

说明：

(1) 请按照上面顺序执行。

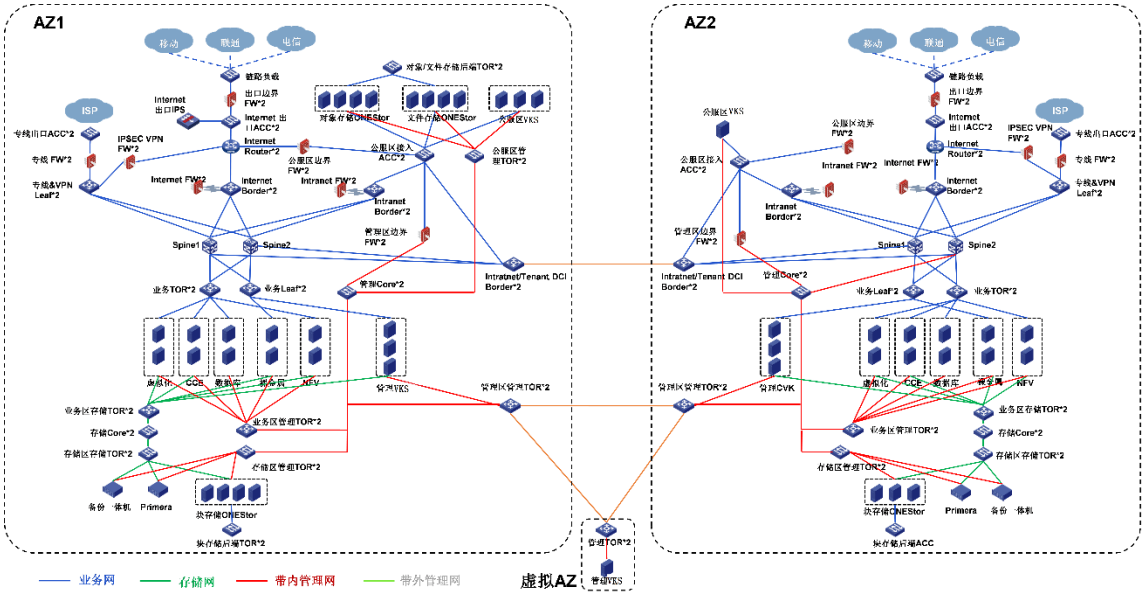
(2) 下完配置以后 permitipv6 一定要保证在 denyipv6 前面，permitipv6 比 denyipv6 优先级高。

(3) 如果没按顺序执行，先配置的是 denyipv6，在 qos policy 下应用 permitipv6 时，执行 classifier permitipv6 behavior permitipv6 insert-before denyipv6。

附录B 多 AZ 标准部署模式

B.1 组网图

图B-1 多 AZ 标准部署模式组网图



B.2 IP地址规划

B.2.1 管理网 IP 地址池

序号	网络名称	IP 地址段	描述
1	跨AZ部署云平台管理网	172.40.0.0/16	当云平台跨AZ分布式时部署，配置云平台虚机管理网为独立网段，在多AZ之间二层互通
2	AZ1设备管理网	172.16.0.0/16	AZ1 VKS、网络设备等管理网段
3	AZ2设备管理网	172.41.0.0/16	AZ2 VKS、网络设备等管理网段

B.2.2 网络区 IP 地址池

租户承载网、安全外网、VTEP 网络等，AZ1 和 AZ2 独立配置一套网络地址，互不关联。

B.2.3 假公网地址池（100.64.0.0/10）

假公网 IP 地址池需要被云平台纳管，建议不修改。如下各网络网段范围可根据实际需要做调整，只要在假公网 IP 地址池范围内即可。

表B-1 假公网地址池

序号	网络名称	IP 地址段	描述
31	AZ1公服区业务地址	100.66.1.0/24	AZ1公服区业务网卡地址，包含对象存储业务网、DMZ K8S业务网、公服区安全类虚机网络等
32	AZ1 Intranet SNAT	100.66.4.0/22	AZ1租户云主机访问公服区服务，经过AZ1 Intranet FW后做假公网Intranet SNAT地址
33	AZ2公服区业务地址	100.66.12.0/24	AZ2公服区业务网卡地址，主要为GSLB等需要跨AZ公服区部署的服务虚机地址
34	AZ2 Intranet SNAT	100.66.8.0/22	AZ2租户云主机访问公服区服务，经过AZ2 Intranet FW后做假公网Intranet SNAT地址

B.2.4 租管互通 IP 地址池（100.100.0.0/18）

租管互通 IP 地址池需要被云平台纳管，建议不修改。当云平台跨 AZ 部署时，管理区租管互通业务网分别连接两个 AZ 的 Leaf 设备，通过 Tenant DCI Border 实现二层互通。

表B-2 租管互通 IP 地址池

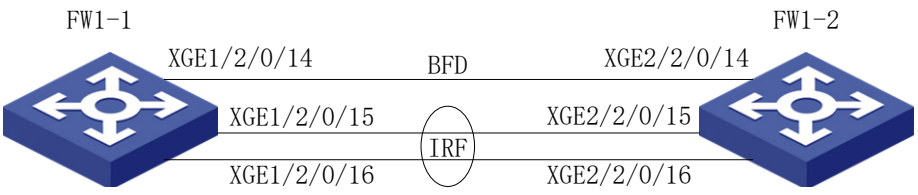
序号	网络名称	地址范围	描述
41	业务区虚机管理网	100.100.1.0-100.100.15.253	业务区应用类虚机（SLB、DB、中间件等）的管理网卡地址，与管理区租管互通K8S业务网在租管互通VPC中进行通信
42	管理区租管互通业务网	100.100.0.0-100.100.0.254	管理区租管互通TAAG K8S业务网地址，通过租管互通VPC给应用类虚机（SLB、DB、中间件等）下发配置

B.3 网络设备基础配置模板

B.3.1 堆叠设备配置模板

1. 组网图

图B-2 堆叠设备配置模板组网图



本节以 M9000 防火墙为例进行介绍。FW1-1 和 FW1-2 组成 IRF，名称为 FW1。FW1-1 与 FW1-2 之间两条直连链路聚合（XGE1/2/0/15、XGE2/2/0/15、XGE1/2/0/16、XGE2/2/0/16）作为 IRF 堆叠链路，FW1-1 与 FW1-2 之间一条直连链路（XGE1/2/0/14、XGE2/2/0/14）作为 MAD 检测链路。登录 FW1-1 和 FW1-2 的 console 口，先配置堆叠，再配置管理口等。

2. 设备配置

(1) FW 1-1 IRF 配置

- FW1-1 设备切换为 IRF 模式。（不需要切换模式的设备不用此步）

  对于 M9000 防火墙，不论是堆叠模式还是单台模式，都需要切换为 IRF 模式。

```
[H3C] chassis convert mode irf
The device will switch to IRF mode and reboot.
You are recommended to save the current running configuration and specify the configuration file for the next startup. Continue? [Y/N]:Y
Do you want to convert the content of the next startup configuration file flash:/startup.cfg to make it available in IRF mode? [Y/N]:Y
Now rebooting, please wait...
```

设备启动成功后，查看 IRF 的初始配置命令如下：

```
irf mac-address persistent always
 irf auto-update enable
 irf auto-merge enable
 undo irf link-delay
 irf member 1 priority 1
```

- FW1-1 设备配置 IRF 成员优先级。由于 IRF 成员优先级缺省是 1，需要修改。

```
[H3C] irf member 1 priority 32
```

- FW1-1 设备配置 IRF domain

```
[H3C] irf domain 1
```

- FW1-1 设备配置 IRF-port

```
[H3C] interface Ten-GigabitEthernet1/2/0/15
[H3C-Ten-GigabitEthernet1/2/0/15] shutdown
[H3C-Ten-GigabitEthernet1/2/0/15]interface Ten-GigabitEthernet1/2/0/16
[H3C-Ten-GigabitEthernet1/2/0/16] shutdown
[H3C-Ten-GigabitEthernet1/2/0/16] quit
[H3C] irf-port 1/1
[H3C-irf-port1/1] port group interface Ten-GigabitEthernet 1/2/0/15
[H3C-irf-port1/1] port group interface Ten-GigabitEthernet 1/2/0/16
[H3C irf-port1/1] quit
[H3C] interface Ten-GigabitEthernet1/2/0/15
[H3C-Ten-GigabitEthernet1/2/0/15] undo shutdown
[H3C-Ten-GigabitEthernet1/2/0/15] interface Ten-GigabitEthernet1/2/0/16
[H3C-Ten-GigabitEthernet1/2/0/16] undo shutdown
[H3C] save
The current configuration will be written to the device. Are you sure? [Y/N]:Y
Please input the file name(*.cfg)[flash:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
Validating file. Please wait...
The current configuration adds 56 commands and deletes 2 commands.
The flash:/startup.cfg file already exists. The save operation will overwrite the file.
Are you sure you want to continue the save operation? [Y/N]:Y

Saving the current configuration to the file.
```

- FW1-1 设备 IRF port 配置激活。

```
[H3C] irf-port-configuration active
```

(2) FW 1-2 IRF 配置

- FW1-2 设备切换为 IRF 模式

```
[H3C] chassis convert mode irf
The device will switch to IRF mode and reboot.
You are recommended to save the current running configuration and specify the configuration file for the next startup. Continue? [Y/N]:Y
Do you want to convert the content of the next startup configuration file flash:/startup.cfg to make it available in IRF mode? [Y/N]:Y
Now rebooting, please wait...
```

设备启动成功后，查看 IRF 的初始配置命令如下：

```
irf mac-address persistent always
 irf auto-update enable
 irf auto-merge enable
 undo irf link-delay
 irf member 1 priority 1
```

- FW1-2 设备配置 IRF 成员号

FW1-2 设备 IRF 成员号改为 2

```
[H3C] irf member 1 renumber 2
[H3C] save
The current configuration will be written to the device. Are you sure? [Y/N]:Y
Please input the file name(*.cfg)[flash:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
Validating file. Please wait...
The current configuration adds 56 commands and deletes 2 commands.
The flash:/startup.cfg file already exists. The save operation will overwrite the file.
Are you sure you want to continue the save operation? [Y/N]:Y
Saving the current configuration to the file.
[H3C] quit
<H3C> reboot force
A forced reboot might cause the storage medium to be corrupted. Continue? [Y/N]:Y
Now rebooting, please wait...
```

- FW1-2 设备配置 IRF 成员优先级

```
[H3C] irf member 2 priority 31
```

- FW1-2 设备配置 IRF domain

```
[H3C] irf domain 1
```

- FW1-2 设备配置 IRF-port

```
[H3C] interface Ten-GigabitEthernet2/2/0/15
[H3C-Ten-GigabitEthernet2/2/0/15] shutdown
[H3C-Ten-GigabitEthernet2/2/0/15] interface Ten-GigabitEtherne 2/2/0/16
[H3C-Ten-GigabitEthernet2/2/0/16] shutdown
[H3C-Ten-GigabitEthernet2/2/0/16] quit
[H3C] irf-port 2/2
[H3C-irf-port2/2] port group interface Ten-GigabitEthernet 2/2/0/15
[H3C-irf-port2/2] port group interface Ten-GigabitEthernet 2/2/0/16
[H3C] interface Ten-GigabitEthernet2/2/0/15
[H3C-Ten-GigabitEthernet2/2/0/15] undo shutdown
```

```
[H3C-Ten-GigabitEthernet2/2/0/15] interface Ten-GigabitEthernet2/2/0/16
[H3C-Ten-GigabitEthernet2/2/0/16] undo shutdown
[H3C] save
The current configuration will be written to the device. Are you sure? [Y/N]:Y
Please input the file name(*.cfg)[flash:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
Validating file. Please wait...
The current configuration adds 56 commands and deletes 2 commands.
The flash:/startup.cfg file already exists. The save operation will overwrite the file.
Are you sure you want to continue the save operation? [Y/N]:Y
Saving the current configuration to the file.
[H3C] quit
```

- FW1-2 设备 IRF port 配置激活

```
[H3C] irf-port-configuration active
```

(3) IRF 堆叠完成

在 IRF port 激活期间，在 FW1-1 和 FW1-2 这两台设备中有一台设备自动重启，重启完毕后，IRF 堆叠建立好。可用 display irf 命令查看 IRF 状态。

- 修改堆叠体的名称

```
[H3C] sysname FW1
[FW1]
```

- 管理口地址配置

```
[FW1]interface M-GigabitEthernet1/0/0/0
[FW1-M-GigabitEthernet1/0/0/0] ip address 192.168.11.101 255.255.255.0
[FW1-M-GigabitEthernet1/0/0/0] quit
```

(4) IRF MAD 检测端口配置。

```
[FW1] interface Route-Aggregation64
[FW1-Route-Aggregation64] mad bfd enable
[FW1-Route-Aggregation64] mad ip address 192.168.2.1 24 member 1
[FW1-Route-Aggregation64] mad ip address 192.168.2.2 24 member 2
[FW1-Route-Aggregation64] interface Ten-GigabitEthernet1/2/0/14
[FW1-Ten-GigabitEthernet1/2/0/14] port link-aggregation group 64
[FW1-Ten-GigabitEthernet1/2/0/14] interface Ten-GigabitEthernet2/2/0/14
[FW1-Ten-GigabitEthernet2/2/0/14] port link-aggregation group 64
[FW1-Ten-GigabitEthernet2/2/0/14] quit
```

3. 通用基础配置模板

(1) 设备命名，需要根据实际命名修改

```
sysname Border1
```

(2) 配置设备带外管理 IP，IP 地址根据规划进行配置

```
interface M-GigabitEthernet0/0/0
 ip binding vpn-instance mgmt
 ip address 192.164.4.1 255.255.0.0
```

(3) 设置管理用户，同时作为 netconf 配置下发的帐号，用户名、密码根据规划进行配置

```
local-user admin
 password simpel unicloud123
service-type ssh
```

```
 authorization-attribute user-role network-admin
authorization-attribute user-role network-operator
```

(4) 配置远程访问

```
line vty 0 63
 authentication-mode scheme
 user-role network-admin
 user-role network-operator
 idle-timeout 20 0
```

(5) 使能 SSH 服务

```
ssh server enable
```

(6) 使能 netconf ssh 服务

```
netconf ssh server enable
```

(7) 使能 lldp 及 stp 协议

```
lldp global enable
stp global enable
```

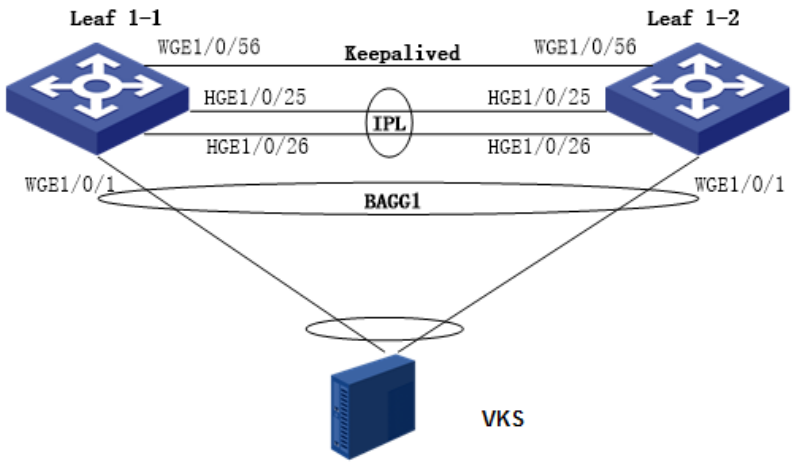
(8) 配置带内管理地址【可选配置，配置后可用该 IP 进行 SDN 设备纳管，不配置则使用 MGE 带外管理 IP 进行纳管】

```
interface LoopBack1
 ip address 10.92.54.1 255.255.255.255
```

B.3.2 DRNI 基础配置模板

1. 组网图

图B-3 DRNI 基础配置模板组网图



本节以 Leaf 为例进行介绍。DRNI（Distributed Resilient Network Interconnect，分布式弹性网络互联）是一种跨设备链路聚合技术，将两台物理设备在聚合层面虚拟成一台设备来实现跨设备链路聚合，从而提供设备级冗余保护和流量负载分担。如图所示，Leaf1-和 Leaf1-2 设备形成负载分担，共同进行流量转发，当其中一台设备发生故障时，流量可以快速切换到另一台设备，保证业务的正常运行。

- DR 接口（Distributed Relay interface，分布式聚合接口）：与外部设备互联的二层聚合接口。与外部设备相连的 DR 接口属于同一 DR 组。如 Leaf1-1 和 Leaf1-2 设备与外部设备（VKS）连接的 DR 接口（WGE1/0/1）加入聚合接口 BAAG1，BAAG1 加入同一个 DR 组。
- IPP（Intra-Potal Port，内部控制链路端口）：连接对端 DR 邻居设备用于内部控制的接口，每台 DR 设备只有一个 IPP 口，IPP 之间通过 IPL 在 DR 设备间传输 DRNI 协议报文，一个 DR 系统只有一条 IPL。Leaf1-1 与 Leaf1-2 的 HGE1/0/25、HGE1/0/26 组成 BAAG100，作为 IPP 口。
- DR 设备间通过 Keepalive 链路检测邻居状态。

2. 设备配置

(1) Leaf 1-1 DRNI 系统参数配置

- DR 系统中所有 DR 设备的 system-mac 必须相同，且保证全网唯一

```
drni system-mac 0001-0001-0001
```

- 两台 DR 设备的 system-number 必须不同。可以配置第一台 DR 设备为 1，第二台为 2

```
drni system-number 1
```

- 配置 DR 设备的 system-priority 必须相同

```
drni system-priority 123
```

(2) Leaf 1-1 IPP 口配置

- 创建 IPP 聚合口

```
interface Bridge-Aggregation100
link-aggregation mode dynamic
```

- IPP 物理口添加到聚合口中

```
interface HundredGigE1/0/25
 port link-aggregation group 100
#
interface HundredGigE1/0/26
 port link-aggregation group 100
```

- IPP 聚合口配置

```
interface Bridge-Aggregation100
 port link-type trunk
 port trunk permit vlan all
 link-aggregation mode dynamic
 port drni intra-portal-port 1
 undo mac-address static source-check enable
```

(3) Leaf 1-1 DRNI MAD 配置

- 配置 DRNI MAD 恢复延迟。当 IPL 链路恢复以后，需要延迟指定时间后，链路才 MAD UP

```
drni restore-delay 180
```

- 配置 Keepalive 报文的目的 IP 地址和源 IP 地址

```
drni keepalive ip destination 10.250.27.74 source 10.250.27.73
```

- 配置 MAD 接口为 3 层接口，并配置 IP 地址为 Keepalive 报文的源 IP 地址

```
interface Twenty-FiveGigE1/0/56
 port link-mode route
 speed 10000
ip address 10.250.27.73 255.255.255.252
```

- 配置 MAD 链路接口为保留接口

```
drni mad exclude interface Twenty-FiveGigE1/0/56
```

(4) Leaf 1-1 DRNI 业务聚合口配置

- 创建二层聚合口，加入 DRNI Group

```
interface Bridge-Aggregation1
 link-aggregation mode dynamic
 port drni group
```

- 物理接口添加到聚合口

```
interface Twenty-FiveGigE1/0/1
 port link-mode bridge
port link-aggregation group 1
```

(5) Leaf 1-2 DRNI 系统参数配置

- DR 系统中所有 DR 设备的 system-mac 必须相同，且保证全网唯一

```
drni system-mac 0001-0001-0001
```

- 两台 DR 设备的 system-number 必须不同。可以配置第一台 DR 设备为 1，第二台为 2

```
drni system-number 2
```

- 配置 DR 设备的 system-priority 必须相同

```
drni system-priority 123
```

(6) Leaf 1-2 IPP 口配置

- 创建 IPP 聚合口

```
interface Bridge-Aggregation100
link-aggregation mode dynamic
```

- IPP 物理口添加到聚合口中

```
interface HundredGigE1/0/25
 port link-aggregation group 100
#
interface HundredGigE1/0/26
 port link-aggregation group 100
```

- IPP 聚合口配置

```
interface Bridge-Aggregation100
 port link-type trunk
 port trunk permit vlan all
 link-aggregation mode dynamic
 port drni intra-portal-port 1
 undo mac-address static source-check enable
```

(7) Leaf 1-2 DRNI MAD 配置

- 配置 DRNI MAD 恢复延迟。当 IPL 链路恢复以后，需要延迟指定时间后，链路才 MAD UP

```
drni restore-delay 180
```

- 配置 Keepalive 报文的目的 IP 地址和源 IP 地址

```
drni keepalive ip destination 10.250.27.73 source 10.250.27.74
```

- 配置 MAD 接口为 3 层接口，并配置 IP 地址为 Keepalive 报文的源 IP 地址

```
interface Twenty-FiveGigE1/0/56
 port link-mode route
 speed 10000
```

```
ip address 10.250.27.74 255.255.255.252
```

- 配置 MAD 链路接口为保留接口

```
drni mad exclude interface Twenty-FiveGigE1/0/56
```

(8) Leaf 1-2 DRNI 业务聚合口配置

- 创建二层聚合口，加入 DRNI Group

```
interface Bridge-Aggregation1
 link-aggregation mode dynamic
 port drni group
```

- 物理接口添加到聚合口

```
interface Twenty-FiveGigE1/0/1
 port link-mode bridge
port link-aggregation group 1
```

B.3.3 交换机硬件参数配置

交换机设备作为网络 overlay Leaf、Border 角色时需要修改硬件参数。各型号交换机硬件参数配置如下。（配置完成后需要重启设备生效）

1. S12500X-AF

S12500X-AF 无论做 spine、leaf 或 border，其硬件资源参数，推荐使用缺省配置。

```
hardware-resource tcam routing
hardware-resource vxlan normal
hardware-resource mcast normal
hardware-resource monitor normal
hardware-resource scale-rt-prefix none
hardware-resource mpls normal
hardware-resource parser normal
```

2. S12500G

S12500G 的硬件资源参数如下：

```
<addc-net3-leaf1>dis hardware-resource
Tcam resource(tcam), all supported modes:
  NORMAL            The normal mode
  MAC               The mac mode
  ROUTING           The routing mode
  ARP               The arp mode
  DUAL-STACK        The dual-stack mode
  MIX               The mix bridging routing mode
  ENHANCE-IPV6      The enhance ipv6 mode
  ENHANCE-ARPND     The enhance arpnd mode
  ACL               The acl mode
  NAT               The nat mode
  ------------------------------------------------
  Default         Current         Next
  NORMAL          NORMAL          NORMAL

Routing-mode resource(routing-mode), all supported modes:
  ipv6-64           IPv6-64 supported
```

```
  ipv6-128          IPv6-128 supported
  ---------------------------------------------
  Default         Current         Next
  ipv6-64         ipv6-64         ipv6-64

VXLAN resource(vxlan), all supported modes:
  L2GW              The Layer 2 gateway mode
  L3GW              The Layer 3 gateway mode
  ---------------------------------------------
  Default         Current         Next
  L3GW            L3GW            L3GW
```

S12500G 做 leaf，border 或 spine 等角色时，推荐硬件参数配置如下：

```
hardware-resource tcam normal
hardware-resource routing-mode ipv6-128
hardware-resource vxlan l3gw
```

3. S6800

(1) S6800 的硬件参数如下：

```
[S6800]hardware-resource switch-mode ?
  0  MAC table is 288K, L3 host table is 16K, LPM Table is 16K
  1  MAC table is 224K, L3 host table is 80K, LPM Table is 16K
  2  MAC table is 160K, L3 host table is 144K, LPM Table is 16K
  3  MAC table is 96K, L3 host table is 208K, LPM Table is 16K
  4  MAC table is 32K, L3 host table is 16K, LPM Table is 250K
[S6800]hardware-resource routing-mode ?
  ipv6-64   ipv6-64 supported
  ipv6-128  ipv6-128 supported
[S6800]hardware-resource vxlan ?
  l2gw       L2 gateway--underlay/overlay 48K/0K
  l3gw8k     L3 gateway--underlay/overlay 40K/8K
  l3gw16k    L3 gateway--underlay/overlay 32K/16K
  l3gw24k    L3 gateway--underlay/overlay 24K/24K
  l3gw32k    L3 gateway--underlay/overlay 16K/32K
  l3gw40k    L3 gateway--underlay/overlay 8K/40K
  border8k   Border--underlay/overlay 40K/8K
  border16k  Border--underlay/overlay 32K/16K
  border24k  Border--underlay/overlay 24K/24K
  border32k  Border--underlay/overlay 16K/32K
  border40k  Border--underlay/overlay 8K/40K
```

(2) Leaf 角色推荐配置：

```
 hardware-resource switch-mode 4
 hardware-resource routing-mode ipv6-128
 hardware-resource vxlan l3gw40k
```

(3) border 角色推荐配置：

```
hardware-resource switch-mode 4
 hardware-resource routing-mode ipv6-128
 hardware-resource vxlan border40k
```

4. S6805

S6805 的硬件参数如下：

```
<S6805>dis hardware-resource
Switch-mode resource(switch-mode), all supported modes:
  NORMAL            MAC table:96K,  ARP and ND tables:80K,  routing table:160K
  MAC               MAC table:288K, ARP and ND tables:16K,  routing table:32K
  ROUTING           MAC table:32K,  ARP and ND tables:16K,  routing table:324K
  ARP               MAC table:32K,  ARP and ND tables:272K, routing table:32K
  DUAL-STACK        MAC table:32K,  ARP and ND tables:16K,  routing:v4-87K,v6-86K
  EM                MAC table:32K,  ARP and ND tables:16K,  routing table:32K
  ---------------------------------------------
  Default         Current         Next
  NORMAL          ROUTING             ROUTING
Routing-mode resource(routing-mode), all supported modes:
  ipv6-64           ipv6-64 supported
  ipv6-128          ipv6-128 supported
  ---------------------------------------------
  Default         Current         Next
  ipv6-64         ipv6-64         ipv6-64
Vxlan resource(vxlan), all supported modes:
  l2gw              L2 gateway--underlay/overlay 64K/0K
  l3gw              L3 gateway--underlay/overlay 24K/40K
  ---------------------------------------------
  Default         Current         Next
  l2gw            l3gw            l3gw
```

S6805 做 leaf，border 或 spine 等角色时，推荐硬件参数配置如下：

```
 hardware-resource switch-mode ROUTING
 hardware-resource routing-mode ipv6-128
 hardware-resource vxlan l3gw
```

5. S6850/S9850

```
<addc-net3-leaf2-1>dis hardware-resource
Switch-mode resource(switch-mode), all supported modes:
  NORMAL            MAC table:96K,  ARP and ND tables:80K,  routing table:160K
  MAC               MAC table:288K, ARP and ND tables:16K,  routing table:32K
  ROUTING           MAC table:32K,  ARP and ND tables:16K,  routing table:324K
  ARP               MAC table:32K,  ARP and ND tables:272K, routing table:32K
  DUAL-STACK        MAC table:32K,  ARP and ND tables:16K,  routing:v4-87K,v6-86K
  EM                MAC table:32K,  ARP and ND tables:16K,  routing table:32K
  ---------------------------------------------
  Default         Current         Next
  NORMAL          ROUTING         ROUTING
Routing-mode resource(routing-mode), all supported modes:
  ipv6-64           ipv6-64 supported
  ipv6-128          ipv6-128 supported
  ---------------------------------------------
  Default         Current         Next
  ipv6-64         ipv6-128        ipv6-128
```

```
Vxlan resource(vxlan), all supported modes:
  l2gw              L2 gateway--underlay/overlay 64K/0K
  l3gw              L3 gateway--underlay/overlay 24K/40K
  ------------------------------------------------
  Default         Current         Next
  l2gw            l3gw            l3gw
```

S6850 做 leaf，border 或 spine 等角色时，推荐硬件参数配置如下：

```
 hardware-resource switch-mode ROUTING
 hardware-resource routing-mode ipv6-128
 hardware-resource vxlan l3gw
```

6. S6860

S686 的硬件资源参数如下：

```
[leaf1-1]hardware-resource switch-mode ?
  0  MAC table is 272K, L3 host table is 4K, LPM Table is 16K
  1  MAC table is 208K, L3 host table is 68K, LPM Table is 16K
  2  MAC table is 80K, L3 host table is 196K, LPM Table is 16K
  3  MAC table is 16K, L3 host table is 260K, LPM Table is 16K
  4  MAC table is 80K, L3 host table is 68K, LPM Table is 128K
  5  MAC table is 16K, L3 host table is 4K, LPM Table is 256K
 [leaf1-1]hardware-resource routing-mode ?
  ipv6-64   ipv6-64 supported
  ipv6-128  ipv6-128 supported
 [leaf1-1]hardware-resource vxlan ?
  l2gw       L2 gateway--underlay/overlay 32K/0K
  l3gw8k     L3 gateway--underlay/overlay 24K/8K
  l3gw16k    L3 gateway--underlay/overlay 16K/16K
  l3gw24k    L3 gateway--underlay/overlay 8K/24K
  border24k  Border--underlay/overlay 8K/24K
  border28k  Border--underlay/overlay 4K/28K
```

(1) Leaf 角色推荐配置：

```
 hardware-resource switch-mode 4
 hardware-resource routing-mode ipv6-128
 hardware-resource vxlan l3gw24k
```

(2) border 角色推荐配置：

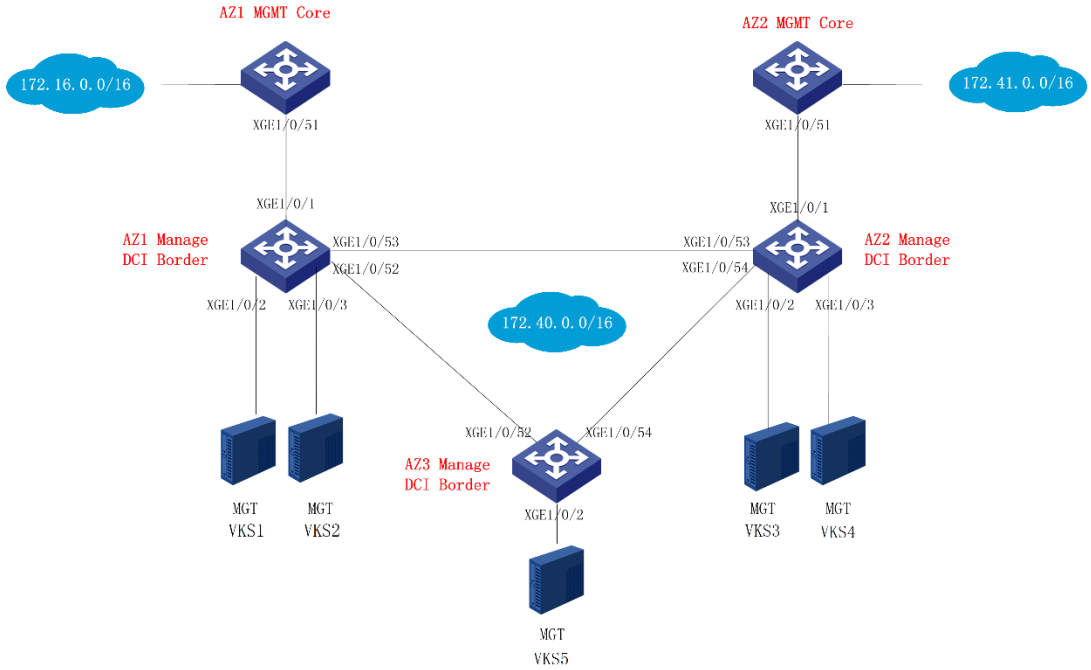
```
hardware-resource switch-mode 4
hardware-resource routing-mode ipv6-128
hardware-resource vxlan border24k
```

B.4 管理区部署指导

B.4.1 Manage DCI Border 配置（管区跨 AZ 部署时配置）

1. 组网图

图B-4 Manage DCI Border 组网图



2. 设备通用基础配置

参考 2.4.1 3. 通用基础配置模板 ，根据规划配置堆叠后的防火墙设备名称、带外 IP 地址、远程登录方式，使能 LLDP 和 STP，使能 netconf。

3. 设备高可靠性配置

参考 2.4.2 DRNI 基础配置模板，配置 AZ 内两台管理 DCI Border 做 DRNI。

4. 设备 EVPN 基础配置

测试环境未配置 DRNI，所以本指导按单机进行配置，现场请根据实际情况进行配置。

5. AZ1 Manage Border 配置

(1) 硬件资源参数：这里以 S6805 为例（配置完成后需要重启设备生效）

```
hardware-resource switch-mode ROUTING
hardware-resource routing-mode ipv6-128
hardware-resource vxlan l3gw
```

(2) 使能 L2vpn,配置禁止通过 vxlan 隧道学习 mac 和 arp

```
l2vpn enable
vxlan tunnel mac-learning disable
vxlan tunnel arp-learning disable
```

(3) 使能 OSPF 协议，实现和 AZ1、 AZ2 和 AZ3 的 Manage DCI Border 的三层互通

```
ospf 1 router-id 10.92.50.81
 non-stop-routing
```

```
 area 0.0.0.0
```

(4) 配置环回口地址并使能 OSPF

```
interface LoopBack0
 ip address 10.92.50.81 255.255.255.255
 ospf 1 area 0.0.0.0
```

(5) 配置 BGP 进程，配置 AZ2 和 AZ3 的 Manage DCI Border 为对等体

```
bgp 65028
 non-stop-routing
 router-id 10.92.50.81
 peer 10.92.50.82 as-number 65028
 peer 10.92.50.82 connect-interface LoopBack0
 peer 10.92.50.83 as-number 65028
 peer 10.92.50.83 connect-interface LoopBack0
 #
 address-family l2vpn evpn
  peer 10.92.50.82 enable
  peer 10.92.50.83 enable
 #
```

(6) 配置 AZ1 Manage DCI Border 与 AZ2 Manage DCI Border 互联接口地址并使能 OSPF

```
interface Ten-GigabitEthernet1/0/53
 port link-mode route
ip address 10.92.53.81 255.255.255.252
 ospf network-type p2p
 ospf 1 area 0.0.0.0
```

(7) 配置 AZ1 Manage DCI Border 与 AZ3 Manage DCI Border 互联接口地址并使能 OSPF

```
interface Ten-GigabitEthernet1/0/52
 port link-mode route
 ip address 10.92.53.85 255.255.255.252
 ospf network-type p2p
 ospf 1 area 0.0.0.0
```

6. AZ2 Manage Border 配置

(1) 硬件资源参数，这里以 S6805 为例（配置完成后需要重启设备生效）

```
hardware-resource switch-mode ROUTING
hardware-resource routing-mode ipv6-128
hardware-resource vxlan l3gw
```

(2) 使能 L2vpn,配置禁止通过 vxlan 隧道学习 mac 和 arp

```
l2vpn enable
vxlan tunnel mac-learning disable
vxlan tunnel arp-learning disable
```

(3) 使能 OSPF 协议，实现和 AZ1、 AZ2 和 AZ3 的 Manage DCI Border 的三层互通

```
ospf 1 router-id 10.92.50.82
 non-stop-routing
 area 0.0.0.0
```

(4) 配置环回口地址并使能 OSPF

```
interface LoopBack0
 ip address 10.92.50.82 255.255.255.255
```

```
 ospf 1 area 0.0.0.0
```

(5) 配置 BGP 进程，配置 AZ1 和 AZ3 的 Manage DCI Border 为对等体

```
bgp 65028
 non-stop-routing
 router-id 10.92.50.82
 peer 10.92.50.81 as-number 65028
 peer 10.92.50.81 connect-interface LoopBack0
 peer 10.92.50.83 as-number 65028
 peer 10.92.50.83 connect-interface LoopBack0
 #
 address-family l2vpn evpn
  peer 10.92.50.81 enable
  peer 10.92.50.83 enable
 #
```

(6) 配置 AZ2 Manage DCI Border 与 AZ1 Manage DCI Border 互联接口地址并使能 OSPF

```
interface Ten-GigabitEthernet1/0/53
 port link-mode route
ip address 10.92.53.82 255.255.255.252
 ospf network-type p2p
 ospf 1 area 0.0.0.0
```

(7) 配置 AZ2 Manage DCI Border 与 AZ3 Manage DCI Border 互联接口地址并使能 OSPF

```
interface Ten-GigabitEthernet1/0/52
 port link-mode route
 ip address 10.92.53.89 255.255.255.252
 ospf network-type p2p
 ospf 1 area 0.0.0.0
```

7. AZ3 Manage Border 配置

(1) 硬件资源参数，这里以 S6805 为例（配置完成后需要重启设备生效）

```
hardware-resource switch-mode ROUTING
hardware-resource routing-mode ipv6-128
hardware-resource vxlan l3gw
```

(2) 使能 L2vpn,配置禁止通过 vxlan 隧道学习 mac 和 arp

```
l2vpn enable
vxlan tunnel mac-learning disable
vxlan tunnel arp-learning disable
```

(3) 使能 OSPF 协议，实现和 AZ1、 AZ2 和 AZ3 的 Manage DCI Border 的三层互通

```
ospf 1 router-id 10.92.50.83
 non-stop-routing
 area 0.0.0.0
```

(4) 配置环回口地址并使能 OSPF

```
interface LoopBack0
 ip address 10.92.50.83 255.255.255.255
 ospf 1 area 0.0.0.0
```

(5) 配置 BGP 进程，配置 AZ1 和 AZ2 的 Manage DCI Border 为对等体

```
bgp 65028
 non-stop-routing
```

```
 router-id 10.92.50.83
 peer 10.92.50.81 as-number 65028
 peer 10.92.50.81 connect-interface LoopBack0
 peer 10.92.50.82 as-number 65028
 peer 10.92.50.82 connect-interface LoopBack0
 #
 address-family l2vpn evpn
  peer 10.92.50.81 enable
  peer 10.92.50.82 enable
 #
```

(6) 配置 AZ3 Manage DCI Border 与 AZ1 Manage DCI Border 互联接口地址并使能 OSPF

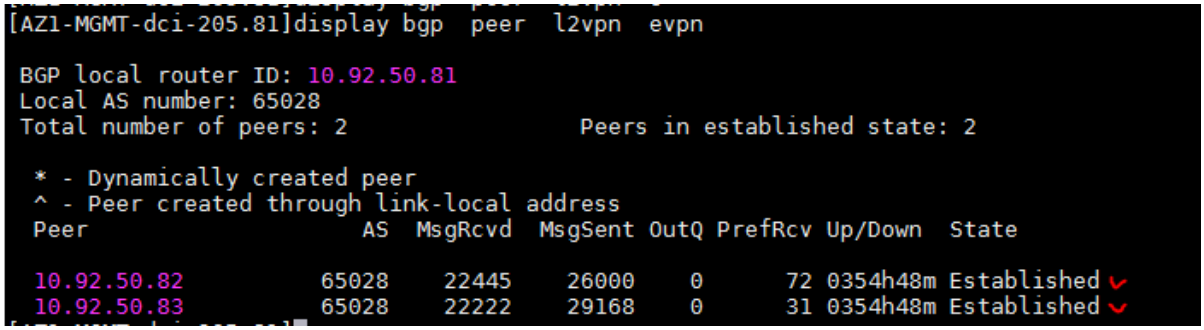
```
interface Ten-GigabitEthernet1/0/52
 port link-mode route
ip address 10.92.53.86 255.255.255.252
 ospf network-type p2p
 ospf 1 area 0.0.0.0
```

(7) 配置 AZ3 Manage DCI Border 与 AZ2 Manage DCI Border 互联接口地址并使能 OSPF

```
interface Ten-GigabitEthernet1/0/54
 port link-mode route
 ip address 10.92.53.90 255.255.255.252
 ospf network-type p2p
 ospf 1 area 0.0.0.0
```

8. 验证配置

(1) AZ1 Manage DCI Border 上查看 BGP peer，正常与 AZ2、AZ3 的 Manage DCI Border 建立了 peer



(2) AZ2 Manage DCI Border 上查看 BGP peer，正常与 AZ1、AZ3 的 Manage DCI Border 建立了 peer

```
[AZ2-MGMT-dci-205.82]display bgp  peer l2vpn evpn

 BGP local router ID: 10.92.50.82
 Local AS number: 65028
 Total number of peers: 2                 Peers in established state: 2

  * - Dynamically created peer
  ^ - Peer created through link-local address
  Peer                    AS  MsgRcvd  MsgSent OutQ PrefRcv Up/Down  State

  10.92.50.81          65028    26008    22452    0      83 0354h55m Established
  10.92.50.83          65028    21562    23126    0      31 0354h55m Established
```

(3) AZ3 Manage DCI Border 上查看 BGP peer，正常与 AZ1、AZ2 的 Manage DCI Border 建立了 peer

```
[AZ3-MGMT-dci-205.83]display bgp  peer  l2vpn evpn

 BGP local router ID: 10.92.50.83
 Local AS number: 65028
 Total number of peers: 2                 Peers in established state: 2

  * - Dynamically created peer
  ^ - Peer created through link-local address
  Peer                    AS  MsgRcvd  MsgSent OutQ PrefRcv Up/Down  State

  10.92.50.81          65028    29181    22233    0      83 0354h58m Established
  10.92.50.82          65028    23130    21566    0      72 0354h58m Established
```

B.4.2 云平台管理互联 EVPN 业务配置

1. AZ1 Manage Border 配置

(1) 创建管理互联的 vpn 实例，RD、RT 值可以根据规划配置

```
ip vpn-instance vpn-mgmtdci
 route-distinguisher 81:60100
 description mutil AZ_ vpn_mgmtdci
 #
 address-family ipv4
  vpn-target 0:60100 1:60100 import-extcommunity
  vpn-target 1:60100 export-extcommunity
 #
 address-family evpn
  vpn-target 0:60100 1:60100 import-extcommunity
  vpn-target 1:60100 export-extcommunity
```

(2) 创建租管互通 VPC 的 L2 VNI vsi-interface 和 L3 VNI vsi-interface，端口号和网关地址根据规划配置

```
interface Vsi-interface100
 description PRE_confige_VSI_Interface_100
 ip binding vpn-instance vpn-mgmtdci
 ip address 172.40.255.254 255.255.0.0 sub
 mac-address fe54-00f6-cf41
 distributed-gateway local
```

```
#
interface Vsi-interface101
 description PRE_confige_101
 ip binding vpn-instance vpn-mgmtdci
 l3-vni 101
```

(3) 创建租管互通 VPC 的 vsi，vsi 值和 VXLAN 值可以根据规划配置

```
vsi 100
 gateway vsi-interface 100
 statistics enable
 vxlan 100
 evpn encapsulation vxlan
  route-distinguisher auto
  vpn-target auto export-extcommunity
  vpn-target auto import-extcommunity
```

(4) 配置管理 VKS 的接入接口为 VTEP AC 口，并与 vsi 做关联。VLAN 与 VXLAN 的映射根据规划进行配置

```
interface Ten-GigabitEthernet1/0/2
 port link-mode bridge
 description MGT-VKS-1
 port access vlan 100
 vtep access port
 #
 service-instance 100
  encapsulation untagged
  xconnect vsi 100
#
interface Ten-GigabitEthernet1/0/3
 port link-mode bridge
 description MGT-VKS-2
 port access vlan 100
 vtep access port
 #
 service-instance 100
  encapsulation untagged
  xconnect vsi 100
```

(5) 配置管区互联 的 BGP 网络，引入直连路由、静态路由

```
bgp 65028
 ip vpn-instance vpn-mgmtdci
  #
  address-family ipv4 unicast
   balance 4
   import-route direct
   import-route static
#
```

2. AZ2 Manage Border 配置

(1) 创建管理互联的 vpn 实例，RD、RT 值可以根据规划配置

```
ip vpn-instance vpn-mgmtdci
```

```
 route-distinguisher 82:60100
 description mutil AZ_ vpn_mgmtdci
 #
 address-family ipv4
  vpn-target 0:60100 1:60100 import-extcommunity
  vpn-target 1:60100 export-extcommunity
 #
 address-family evpn
  vpn-target 0:60100 1:60100 import-extcommunity
  vpn-target 1:60100 export-extcommunity
```

(2) 创建租管互通 VPC 的 L2 VNI vsi-interface 和 L3 VNI vsi-interface，端口号和网关地址根据规划配置

```
interface Vsi-interface100
 description PRE_confige_VSI_Interface_100
 ip binding vpn-instance vpn-mgmtdci
 ip address 172.40.255.254 255.255.0.0 sub
 mac-address fe54-00f6-cf41
 distributed-gateway local
#
interface Vsi-interface101
 description PRE_confige_101
 ip binding vpn-instance vpn-mgmtdci
 l3-vni 101
```

(3) 创建租管互通 VPC 的 vsi，vsi 值和 VXLAN 值可以根据规划配置

```
vsi 100
 gateway vsi-interface 100
 statistics enable
 vxlan 100
 evpn encapsulation vxlan
  route-distinguisher auto
  vpn-target auto export-extcommunity
  vpn-target auto import-extcommunity
```

(4) 配置管理 VKS 的接入接口为 VTEP AC 口，并与 vsi 做关联。VLAN 与 VXLAN 的映射根据规划进行配置

```
interface Ten-GigabitEthernet1/0/2
 port link-mode bridge
 description MGT-VKS-1
 port access vlan 100
 vtep access port
 #
 service-instance 100
  encapsulation untagged
  xconnect vsi 100
#
interface Ten-GigabitEthernet1/0/3
 port link-mode bridge
 description MGT-VKS-2
```

```
 port access vlan 100
 vtep access port
 #
 service-instance 100
  encapsulation untagged
  xconnect vsi 100
```

(5) 配置管区互联 的 BGP 网络，引入直连路由、静态路由

```
bgp 65028
 ip vpn-instance vpn-mgmtdci
  #
  address-family ipv4 unicast
   balance 4
   import-route direct
   import-route static
```

3. AZ3 Manage Border 配置

(1) 创建管理互联的 vpn 实例，RD、RT 值可以根据规划配置

```
ip vpn-instance vpn-mgmtdci
 route-distinguisher 83:60100
 description mutil AZ_ vpn_mgmtdci
 #
 address-family ipv4
  vpn-target 0:60100 1:60100 import-extcommunity
  vpn-target 1:60100 export-extcommunity
 #
 address-family evpn
  vpn-target 0:60100 1:60100 import-extcommunity
  vpn-target 1:60100 export-extcommunity
```

(2) 创建租管互通 VPC 的 L2 VNI vsi-interface 和 L3 VNI vsi-interface，端口号和网关地址根据规划配置

```
interface Vsi-interface100
 description PRE_confige_VSI_Interface_100
 ip binding vpn-instance vpn-mgmtdci
 ip address 172.40.255.254 255.255.0.0 sub
 mac-address fe54-00f6-cf41
 distributed-gateway local
#
interface Vsi-interface101
 description PRE_confige_101
 ip binding vpn-instance vpn-mgmtdci
 l3-vni 101
```

(3) 创建租管互通 VPC 的 vsi，vsi 值和 VXLAN 值可以根据规划配置

```
vsi 100
 gateway vsi-interface 100
 statistics enable
 vxlan 100
 evpn encapsulation vxlan
  route-distinguisher auto
```

```
  vpn-target auto export-extcommunity
  vpn-target auto import-extcommunity
```

(4) 配置管理 VKS 的接入接口为 VTEP AC 口，并与 vsi 做关联。VLAN 与 VXLAN 的映射根据规划进行配置

```
interface Ten-GigabitEthernet1/0/2
 port link-mode bridge
 description MGT-VKS-1
 port access vlan 100
 vtep access port
 #
 service-instance 100
  encapsulation untagged
  xconnect vsi 100
#
```

(5) 配置管区互联 的 BGP 网络，引入直连路由、静态路由

```
bgp 65028
 ip vpn-instance vpn-mgmtdci
  #
  address-family ipv4 unicast
   balance 4
   import-route direct
   import-route static
```

4. 验证配置

(1) AZ1 Manage DCI Border 上查看路由信息，有直连的 AZ1 的云平台虚机路由和通过 BGP 学习到的其他 AZ 的云平台虚机路由

```
[AZ1-MGMT-dci-205.81]display ip routing-table vpn-instance  vpn-mgmtdci
```

172.40.0.0/16	Direct	0	0	172.40.255.254	Vsi100
172.40.0.0/32	Direct	0	0	172.40.255.254	Vsi100
172.40.150.11/32	BGP	255	0	10.92.50.82	Vsi101
172.40.150.12/32	BGP	255	0	10.92.50.83	Vsi101
172.40.150.22/32	BGP	255	0	10.92.50.82	Vsi101
172.40.150.31/32	BGP	255	0	10.92.50.83	Vsi101
172.40.150.40/32	BGP	255	0	10.92.50.83	Vsi101
172.40.150.42/32	BGP	255	0	10.92.50.82	Vsi101
172.40.150.43/32	BGP	255	0	10.92.50.83	Vsi101
172.40.150.52/32	BGP	255	0	10.92.50.82	Vsi101
172.40.150.53/32	BGP	255	0	10.92.50.83	Vsi101

(2) AZ2 Manage DCI Border 上查看路由信息，有直连的 AZ2 的云平台虚机路由和通过 BGP 学习到的其他 AZ 的云平台虚机路由

```
[AZ2-MGMT-dci-205.82]display ip routing-table vpn-instance  vpn-mgmtdci
```

```
172.40.0.0/16       Direct  0    0           172.40.255.254  Vsi100
172.40.0.0/32       Direct  0    0           172.40.255.254  Vsi100
172.40.150.2/32     BGP     255  0           10.92.50.81     Vsi101
172.40.150.3/32     BGP     255  0           10.92.50.81     Vsi101
172.40.150.4/32     BGP     255  0           10.92.50.81     Vsi101
172.40.150.12/32    BGP     255  0           10.92.50.83     Vsi101
172.40.150.13/32    BGP     255  0           10.92.50.81     Vsi101
172.40.150.21/32    BGP     255  0           10.92.50.81     Vsi101
172.40.150.23/32    BGP     255  0           10.92.50.81     Vsi101
172.40.150.31/32    BGP     255  0           10.92.50.83     Vsi101
172.40.150.32/32    BGP     255  0           10.92.50.81     Vsi101
172.40.150.33/32    BGP     255  0           10.92.50.81     Vsi101
172.40.150.40/32    BGP     255  0           10.92.50.83     Vsi101
172.40.150.41/32    BGP     255  0           10.92.50.81     Vsi101
172.40.150.43/32    BGP     255  0           10.92.50.83     Vsi101
```

(3) AZ3 Manage DCI Border 上查看路由信息，有直连的 AZ3 的云平台虚机路由和通过 BGP 学习到的其他 AZ 的云平台虚机路由

```
[AZ3-MGMT-dci-205.83]display ip routing-table vpn-instance  vpn-mgmtdci
```

```
172.40.0.0/16       Direct  0    0           172.40.255.254  Vsi100
172.40.0.0/32       Direct  0    0           172.40.255.254  Vsi100
172.40.150.2/32     BGP     255  0           10.92.50.81     Vsi101
172.40.150.3/32     BGP     255  0           10.92.50.81     Vsi101
172.40.150.4/32     BGP     255  0           10.92.50.81     Vsi101
172.40.150.11/32    BGP     255  0           10.92.50.82     Vsi101
172.40.150.13/32    BGP     255  0           10.92.50.81     Vsi101
172.40.150.21/32    BGP     255  0           10.92.50.81     Vsi101
172.40.150.22/32    BGP     255  0           10.92.50.82     Vsi101
172.40.150.23/32    BGP     255  0           10.92.50.81     Vsi101
172.40.150.32/32    BGP     255  0           10.92.50.81     Vsi101
172.40.150.33/32    BGP     255  0           10.92.50.81     Vsi101
172.40.150.41/32    BGP     255  0           10.92.50.81     Vsi101
172.40.150.42/32    BGP     255  0           10.92.50.82     Vsi101
```

(4) 3 个 AZ 之间的云平台虚机可以正常通信

```
[root@HZ-AZ1-UCA-Node1 ~]# ping 172.40.150.42
PING 172.40.150.42 (172.40.150.42) 56(84) bytes of data.
64 bytes from 172.40.150.42: icmp_seq=1 ttl=64 time=0.496 ms
64 bytes from 172.40.150.42: icmp_seq=2 ttl=64 time=0.112 ms
64 bytes from 172.40.150.42: icmp_seq=3 ttl=64 time=0.121 ms
64 bytes from 172.40.150.42: icmp_seq=4 ttl=64 time=0.166 ms

--- 172.40.150.42 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3000ms
rtt min/avg/max/mdev = 0.112/0.223/0.496/0.159 ms
[root@HZ-AZ1-UCA-Node1 ~]# ping 172.40.150.43
PING 172.40.150.43 (172.40.150.43) 56(84) bytes of data.
64 bytes from 172.40.150.43: icmp_seq=1 ttl=64 time=0.475 ms
64 bytes from 172.40.150.43: icmp_seq=2 ttl=64 time=0.131 ms
64 bytes from 172.40.150.43: icmp_seq=3 ttl=64 time=0.121 ms
64 bytes from 172.40.150.43: icmp_seq=4 ttl=64 time=0.110 ms

--- 172.40.150.43 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3000ms
rtt min/avg/max/mdev = 0.110/0.209/0.475/0.153 ms
```

B.4.3 云平台管理网与其他网络互联配置

本配置基于实验室情况做的配置参考，非固定配置，实际可以根据现场情况进行配置。

1. AZ1 Manage Border 配置

(1) 创建 OSPF，与对端 AZ1 MGMT core 实现路由互通。引入 direct、static、bgp 路由

```
ospf 100 vpn-instance vpn-mgmtdci
 import-route direct
 import-route static
 import-route bgp
 area 0.0.0.0
```

(2) 配置 AZ1 Manage DCI Border 与 AZ1 MGMT Core 互联接口地址并使能 OSPF

```
interface Ten-GigabitEthernet1/0/1
 port link-mode route
 description AZ1-MGT-GW
 ip binding vpn-instance vpn-mgmtdci
 ip address 10.92.53.2 255.255.255.252
 ospf cost 10
 ospf network-type p2p
 ospf 100 area 0.0.0.0
```

(3) 配置管区互联 的 BGP 网络，引入学习到的 AZ1 MGMT core 的 ospf 路由

```
bgp 65028
 ip vpn-instance vpn-mgmtdci
  #
  address-family ipv4 unicast
   balance 4
   import-route direct
   import-route static
   import-route ospf 100
```

2. AZ1 MGMT Core 配置

(1) 创建 OSPF，与对端 AZ1 Manage DCI Border 实现路由互通。引入 direct、static 路由

```
ospf 100
 import-route direct
 import-route static
 area 0.0.0.0
```

(2) 配置 AZ1 MGMT Core 与 AZ1 Manage DCI Borde 互联接口地址并使能 OSPF

```
interface Ten-GigabitEthernet1/0/51
 port access vlan 40
#
interface Vlan-interface40
 ip address 10.92.53.1 255.255.255.252
 ospf network-type p2p
 ospf 100 area 0.0.0.0
```

(3) 配置 AZ1 MGMT Core 与其他区域的网络互联，此处以静态路由举例。现场需要根据实际组网情况和网络放行规定进行配置。

```
ip route-static 10.92.30.0 24 10.92.53.6 --虚墙管理网段
ip route-static 10.92.31.0 24 10.92.53.6 --虚墙管理网段
ip route-static 100.66.1.0 24 10.92.53.6 --公服区业务网段
ip route-static 150.66.0.0 24 10.92.53.6 --公网 IP 网段
ip route-static 172.16.0.0 16 10.92.53.6 --AZ1 其他管理网段
ip route-static 172.29.29.0 24 10.92.53.6 --裸金属 DHCP 网段
ip route-static 192.167.0.0 16 10.92.53.6 --外网接入访问网段
```

3. AZ2 Manage Border 配置

(1) 创建 OSPF，与对端 AZ2 MGMT core 实现路由互通。引入 direct、static、bgp 路由

```
ospf 100 vpn-instance vpn-mgmtdci
 import-route direct
 import-route static
 import-route bgp
 area 0.0.0.0
```

(2) 配置 AZ2 Manage DCI Border 与 AZ2 MGMT Core 互联接口地址并使能 OSPF

```
interface Ten-GigabitEthernet1/0/1
 port link-mode route
 description AZ2-MGT-GW
 ip binding vpn-instance vpn-mgmtdci
 ip address 10.93.53.2 255.255.255.252
 ospf cost 50
 ospf network-type p2p
 ospf 100 area 0.0.0.0
```

(3) 配置管区互联 的 BGP 网络，引入学习到的 AZ2 MGMT core 的 ospf 路由

```
bgp 65028
 ip vpn-instance vpn-mgmtdci
  #
  address-family ipv4 unicast
   balance 4
   import-route direct
```

```
 import-route static
 import-route ospf 100
```

4. AZ2 MGMT Core 配置

- 创建 OSPF，与对端 AZ2 Manage DCI Border 实现路由互通。引入 direct、static 路由

```
ospf 100
 import-route direct
 import-route static
 area 0.0.0.0
```

- 配置 AZ1 MGMT Core 与 AZ1 Manage DCI Borde 互联接口地址并使能 OSPF

```
interface Ten-GigabitEthernet1/0/51
 port access vlan 40
#
interface Vlan-interface40
 ip address 10.93.53.1 255.255.255.252
 ospf network-type p2p
 ospf 100 area 0.0.0.0
```

- 配置 AZ2 MGMT Core 与其他区域的网络互联，此处以静态路由举例。现场需要根据实际组网情况和网络放行规定进行配置。

```
ip route-static 192.167.0.0 16 10.92.53.6 --外网接入访问网段
ip route-static 172.16.0.0 16 10.92.53.6 --AZ1 其他管理网段
```

5. 验证配置

(1) AZ1 Manage DCI Border 上查看路由信息，有通过 AZ1 MGMT Core 学习到的路由信息，有通过 AZ2 Manage DCI Border BGP 学习到 AZ2 的路由信息

```
[AZ1-MGMT-dci-205.81]display ip routing-table vpn-instance  vpn-mgmtdci
```

```
150.66.0.0/24      O_ASE2  150 1          10.92.53.1      XGE1/0/1
172.16.0.0/16      O_ASE2  150 1          10.92.53.1      XGE1/0/1
172.20.0.0/16      O_ASE2  150 1          10.92.53.1      XGE1/0/1
172.25.0.0/16      O_ASE2  150 1          10.92.53.1      XGE1/0/1
172.29.29.0/24     O_ASE2  150 1          10.92.53.1      XGE1/0/1
172.40.0.0/16      Direct  0   0          172.40.255.254  Vsi100
172.40.0.0/32      Direct  0   0          172.40.255.254  Vsi100
```

```
172.41.0.0/16      BGP     255 52         10.92.50.82     Vsi101
```

(2) AZ2 Manage DCI Border 上查看路由信息，有通过 AZ2 MGMT Core 学习到的路由信息，有通过 AZ1 Manage DCI Border BGP 学习到 AZ2 的路由信息

```
[AZ2-MGMT-dci-205.82]display ip routing-table vpn-instance  vpn-mgmtdci
```

```
172.41.0.0/16      O_INTRA 10  51         10.93.53.1      XGE1/0/1
172.50.0.0/16      BGP     255 2          10.92.50.81     Vsi101
172.99.0.0/16      BGP     255 2          10.92.50.81     Vsi101
192.165.0.0/16     BGP     255 2          10.92.50.81     Vsi101
192.167.0.0/16     O_ASE2  150 1          10.93.53.1      XGE1/0/1
```

(3) AZ3 Manage DCI Border 上查看路由信息，有通过 AZ1 MGMT Core 和 AZ2 Manage DCI Border BGP 学习到的路由信息

```
[AZ3-MGMT-dci-205.83]display ip routing-table vpn-instance  vpn-mgmtdci
```

```
150.66.0.0/24       BGP      255 2          10.92.50.81     Vsi101
172.16.0.0/16       BGP      255 2          10.92.50.81     Vsi101
                                            10.92.50.82     Vsi101
172.20.0.0/16       BGP      255 2          10.92.50.81     Vsi101
172.25.0.0/16       BGP      255 2          10.92.50.81     Vsi101
                                            10.92.50.82     Vsi101
172.29.29.0/24      BGP      255 2          10.92.50.81     Vsi101
```

(4) AZ1 的云平台管理虚机可以访问 AZ1 的其他管理网网段，可以访问 AZ2 的其他管理网段

```
[root@HZ-AZ1-UCA-Node1 ~]# ping 172.16.205.41
PING 172.16.205.41 (172.16.205.41) 56(84) bytes of data.
64 bytes from 172.16.205.41: icmp_seq=1 ttl=252 time=0.363 ms
64 bytes from 172.16.205.41: icmp_seq=2 ttl=252 time=0.252 ms
64 bytes from 172.16.205.41: icmp_seq=3 ttl=252 time=0.260 ms
64 bytes from 172.16.205.41: icmp_seq=4 ttl=252 time=0.247 ms
64 bytes from 172.16.205.41: icmp_seq=5 ttl=252 time=0.245 ms

--- 172.16.205.41 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3999ms
rtt min/avg/max/mdev = 0.245/0.273/0.363/0.047 ms
```

```
[root@HZ-AZ1-UCA-Node1 ~]# ping 172.41.205.101
PING 172.41.205.101 (172.41.205.101) 56(84) bytes of data.
64 bytes from 172.41.205.101: icmp_seq=1 ttl=252 time=0.241 ms
64 bytes from 172.41.205.101: icmp_seq=2 ttl=252 time=0.197 ms
64 bytes from 172.41.205.101: icmp_seq=3 ttl=252 time=0.167 ms
64 bytes from 172.41.205.101: icmp_seq=4 ttl=252 time=1.55 ms

--- 172.41.205.101 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2999ms
rtt min/avg/max/mdev = 0.167/0.539/1.553/0.586 ms
```

(5) AZ2 的云平台管理虚机可以访问 AZ2 的其他管理网网段，可以访问 AZ1 的其他管理网段

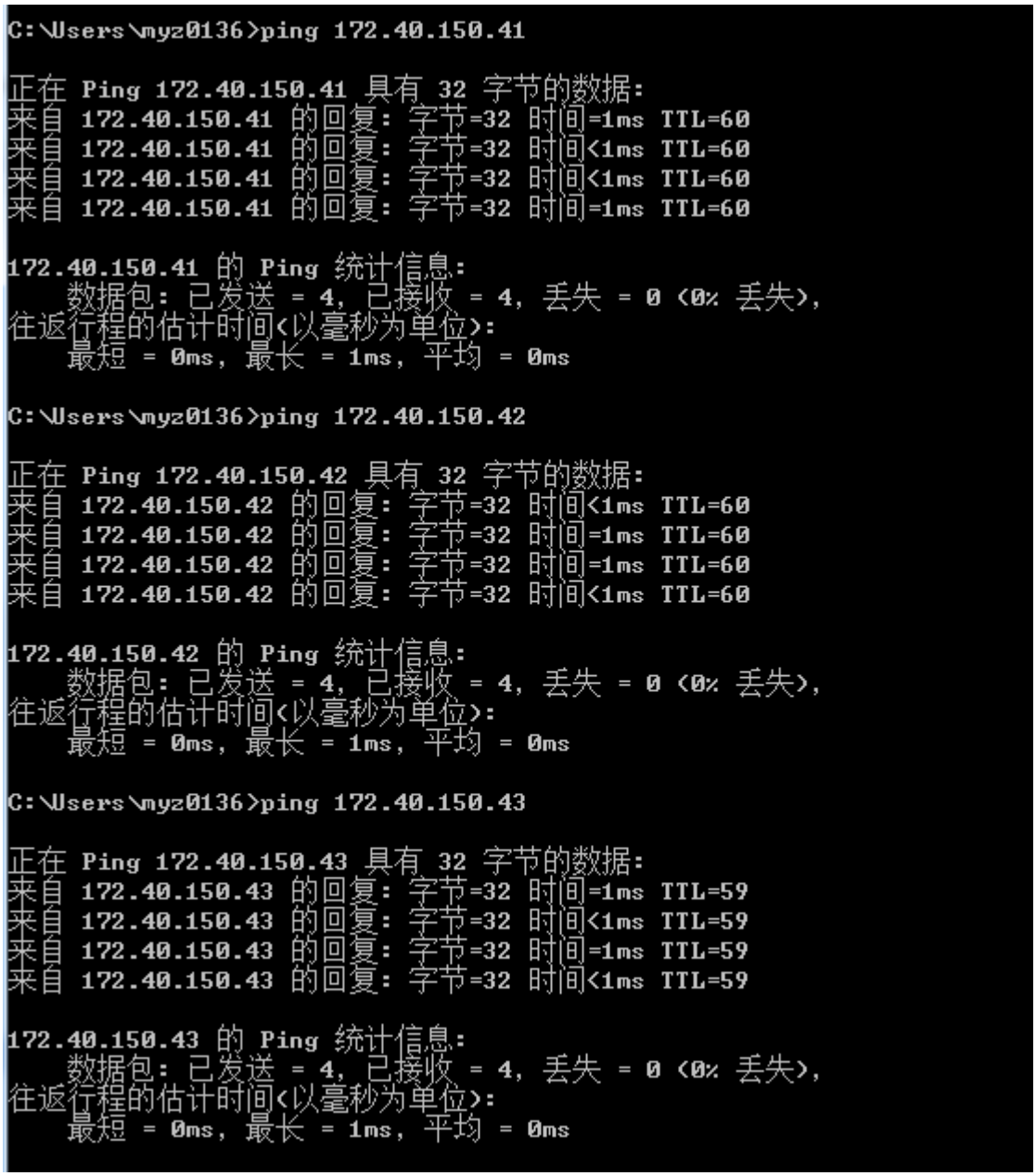
```
[root@HZ-AZ1-UCA-Node2 ~]# ping 172.41.205.101
PING 172.41.205.101 (172.41.205.101) 56(84) bytes of data.
64 bytes from 172.41.205.101: icmp_seq=1 ttl=253 time=0.244 ms
64 bytes from 172.41.205.101: icmp_seq=2 ttl=253 time=2.03 ms
64 bytes from 172.41.205.101: icmp_seq=3 ttl=253 time=0.209 ms
64 bytes from 172.41.205.101: icmp_seq=4 ttl=253 time=0.187 ms

--- 172.41.205.101 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3000ms
rtt min/avg/max/mdev = 0.187/0.669/2.037/0.790 ms
```

```
[root@HZ-AZ1-UCA-Node2 ~]# ping 172.16.205.41
PING 172.16.205.41 (172.16.205.41) 56(84) bytes of data.
64 bytes from 172.16.205.41: icmp_seq=1 ttl=251 time=0.364 ms
64 bytes from 172.16.205.41: icmp_seq=2 ttl=251 time=0.226 ms
64 bytes from 172.16.205.41: icmp_seq=3 ttl=251 time=0.274 ms
64 bytes from 172.16.205.41: icmp_seq=4 ttl=251 time=0.845 ms

--- 172.16.205.41 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3000ms
rtt min/avg/max/mdev = 0.226/0.427/0.845/0.246 ms
```

(6) AZ3 的云平台管理虚机可以访问 AZ1 和 AZ2 的其他管理网段

```
[root@HZ-AZ1-UCA-Node3 ~]# ping 172.16.205.41
PING 172.16.205.41 (172.16.205.41) 56(84) bytes of data.
64 bytes from 172.16.205.41: icmp_seq=1 ttl=251 time=0.528 ms
64 bytes from 172.16.205.41: icmp_seq=2 ttl=251 time=0.328 ms
64 bytes from 172.16.205.41: icmp_seq=3 ttl=251 time=0.337 ms
64 bytes from 172.16.205.41: icmp_seq=4 ttl=251 time=0.269 ms

--- 172.16.205.41 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2999ms
rtt min/avg/max/mdev = 0.269/0.365/0.528/0.099 ms
[root@HZ-AZ1-UCA-Node3 ~]# ping 172.41.205.101
PING 172.41.205.101 (172.41.205.101) 56(84) bytes of data.
64 bytes from 172.41.205.101: icmp_seq=1 ttl=252 time=0.457 ms
64 bytes from 172.41.205.101: icmp_seq=2 ttl=252 time=0.198 ms
64 bytes from 172.41.205.101: icmp_seq=3 ttl=252 time=0.203 ms
64 bytes from 172.41.205.101: icmp_seq=4 ttl=252 time=1.90 ms

--- 172.41.205.101 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3000ms
rtt min/avg/max/mdev = 0.198/0.689/1.900/0.707 ms
```

(7) 外网可以访问 3 个 AZ 的云平台虚机



B.5 网络设备区部署指导

B.5.1 AZ 内网络设备业务配置

参考 1 单 AZ 标准部署模式文档分别对两个 AZ 内的网络设备进行配置。

B.5.2 Tenant DCI Border 配置

1. 组网图

图B-5 Tenant DCI Border 组网图

2. AZ1 Tenant DCI Border 配置

交换机硬件资源参数配置

参考 2.4.3 交换机硬件参数配置根据实际交换机型号进行配置，以 S6805 为例（配置完成后需要重启设备生效）

```
hardware-resource switch-mode ROUTING
 hardware-resource routing-mode ipv6-128
 hardware-resource vxlan l3gw
```

3. 配置 AZ1 两台 DCI Border 交换机设备做 IRF 堆叠

参考 2.4.1 堆叠设备配置模板进行配置。

4. 堆叠 DCI Border 基础配置

参考 3. 通用基础配置模板进行配置。

5. 网络业务配置

(1) 使能 L2vpn,配置禁止通过 vxlan 隧道学习 mac 和 arp

```
l2vpn enable
vxlan tunnel mac-learning disable
vxlan tunnel arp-learning disable
```

(2) 使能 OSPF 协议，实现和 AZ1 的 spine 和 AZ1 的 Tenant DCI Border 的三层互通

```
ospf 1 router-id 10.92.50.84
non-stop-routing
area 0.0.0.0
import-route static
```

(3) 配置环回口地址并使能 OSPF

```
interface LoopBack0
ip address 10.92.50.84 32
ospf 1 area 0.0.0.0
```

(4) 配置 DCI Border 与 Spine 互联接口地址并使能 OSPF

```
interface XGE1/0/54
port link-mode route
ip address 10.92.51.122 30
ip mtu 2000
ospf 1 area 0.0.0.0
ospf network-type p2p
#
```

(5) 配置 AZ1 Tenant DCI Border 与 AZ2 Tenant DCI Border 互联接口地址并使能 OSPF

```
interface HGE1/0/25
port link-mode route
ip address 10.92.51.141 30
ip mtu 2000
ospf 1 area 0.0.0.0
ospf network-type p2p
dci enable
```

(6) 配置 BGP 进程，与 AZ1 Spine（10.92.50.84）建立 ibgp peer，与 AZ2 Tenant DCI Border（10.93.50.85）建立 ebgp peer

```
bgp 65027
 non-stop-routing
 router-id 10.92.50.84
 peer 10.92.50.77 as-number 65027
 peer 10.92.50.77 connect-interface LoopBack0
 peer 10.93.50.85 as-number 65028
 peer 10.93.50.85 connect-interface LoopBack0
 peer 10.93.50.85 ebgp-max-hop 10
 #
 address-family l2vpn evpn
  peer 10.92.50.77 enable
  peer 10.92.50.77 next-hop-local
  peer 10.93.50.85 enable
       peer 10.93.50.85 router-mac-local
```

6. AZ1 Spine 配置

(1) BGP 中增加 Tenant DCI Border peer 信息

```
bgp 65027
peer 10.92.50.84 as-number 65027                --Tenant DCI Border vtep
peer 10.92.50.84 connect-interface LoopBack0
#
address-family l2vpn evpn
peer 10.92.50.84 enable
peer 10.92.50.84 reflect-client
#
address-family ipv4 unicast
peer 10.92.50.84 enable
```

(2) 配置 Spine 与 DCI Boder 互联接口地址并使能 OSPF

```
interface WGE1/0/54
port link-mode route
```

```
ip address 10.92.51.121 30
ip mtu 2000
ospf 1 area 0.0.0.0
ospf network-type p2p
#
```

7. AZ2 Tenant DCI Border 配置

交换机硬件资源参数配置，参考 2.4.3 交换机硬件参数配置，根据实际交换机型号进行配置，以 S6805 为例（配置完成后需要重启设备生效）

```
hardware-resource switch-mode ROUTING
 hardware-resource routing-mode ipv6-128
 hardware-resource vxlan l3gw
```

8. 配置 AZ1 两台 DCI Border 交换机设备做 IRF 堆叠

参考 2.4.1 堆叠设备配置模板进行配置。

9. 堆叠 DCI Border 基础配置

参考 3. 通用基础配置模板进行配置。

10. 网络业务配置

(1) 使能 L2vpn,配置禁止通过 vxlan 隧道学习 mac 和 arp

```
l2vpn enable
vxlan tunnel mac-learning disable
vxlan tunnel arp-learning disable
```

(2) 使能 OSPF 协议，实现和 AZ2 的 spine 和 AZ2 的 Tenant DCI Border 的三层互通

```
ospf 1 router-id 10.93.50.85
non-stop-routing
area 0.0.0.0
import-route static
```

(3) 配置环回口地址并使能 OSPF

```
interface LoopBack0
ip address 10.93.50.85 32
ospf 1 area 0.0.0.0
```

(4) 配置 DCI Border 与 Spine 互联接口地址并使能 OSPF

```
interface XGE1/0/54
port link-mode route
ip address 10.93.51.122 30
ip mtu 2000
ospf 1 area 0.0.0.0
ospf network-type p2p
#
```

(5) 配置 AZ2 Tenant DCI Border 与 AZ1 Tenant DCI Border 互联接口地址并使能 OSPF

```
interface HGE1/0/25
port link-mode route
ip address 10.92.51.142 30
ip mtu 2000
ospf 1 area 0.0.0.0
ospf network-type p2p
```

```
dci enable
```

(6) 配置 BGP 进程，与 AZ2 Spine（10.93.50.104）建立 ibgp peer，与 AZ1 Tenant DCI Border（10.92.50.84）建立 ebgp peer

```
bgp 65028
non-stop-routing
router-id 10.93.50.85
peer 10.93.50.104 as-number 65028
peer 10.93.50.104 connect-interface LoopBack0
peer 10.92.50.84 as-number 65027
peer 10.92.50.84 connect-interface LoopBack0
peer 10.92.50.84 ebgp-max-hop 10
#
address-family l2vpn evpn
peer 10.93.50.104 enable
peer 10.93.50.104 next-hop-local
peer 10.92.50.84 enable
peer 10.92.50.84 router-mac-local
```

B.5.3 AZ2 Spine 配置

(1) BGP 中增加 Tenant DCI Border peer 信息

```
bgp 65028
peer 10.93.50.85 as-number 65028                --Tenant DCI Border vtep
peer 10.93.50.85 connect-interface LoopBack0
#
address-family l2vpn evpn
peer 10.93.50.85 enable
peer 10.93.50.85 reflect-client
#
address-family ipv4 unicast
peer 10.93.50.85 enable
```

(2) 配置 Spine 与 DCI Boder 互联接口地址并使能 OSPF

```
interface WGE1/0/54
port link-mode route
ip address 10.93.51.121 30
ip mtu 2000
ospf 1 area 0.0.0.0
ospf network-type p2p
#
```

B.6 云平台纳管网络设备

当前版本暂不支持云平台界面纳管 AZ 内网络设备和 AZ 间 Tenant DCI Boder 设备，需要联系研发进行操作。

B.7 租管互通VPC跨AZ部署指导

租管互通 TAAG K8S 的 3 个虚机部署在 3 个 AZ 内。AZ1 和 AZ2 的 TAAG K8S 虚机租管互通业务网卡分别连接各自 AZ 的网络 overlay Leaf 上，通过配置实现跨 AZ 的租管互通 VPC 二层互通。即 AZ1 的 TAAG K8S 中 Pod 可以户通过 Tenant DCI Border 访问到 AZ2 的应用类虚机管理网络。

由于虚拟 AZ 无网络 overlay Leaf 设备，不用连接租管互通业务网卡，通过配置限制租管互通的 K8S POD 不调度到虚拟 AZ 的 node 上。

B.7.1 租管互通 VPC 跨 AZ 二层互访配置（管区跨 AZ 部署时配置）

请确保 AZ1、AZ2 各自的租管互通 VPC 已经配置完成，AZ1 和 AZ2 的 Tenant DCI Border 基础 EVPN 配置已完成。AZ1 和 AZ2 的租管互通 VPC vxlan 为 900，映射到 VXLAN 902；AZ1 的 RT 为 10，AZ2 的 RT 为 11。

1. AZ1 Tenant Border 配置

(1) 创建租管互通 vsi，配置 vxlan mapping

```
 vsi CORE_AGENT_VSI_900                ---AZ1 租管互通 vxlan
 statistics enable
 arp suppression enable
 flooding disable all
 vxlan 900
 evpn encapsulation vxlan
  route-distinguisher auto
  vpn-target auto export-extcommunity
  vpn-target auto import-extcommunity
  mapping vni 902
#
```

(2) 创建租管互通 mapping vsi

```
vsi CORE_vsimap_VSI_902
 vxlan 902
 evpn encapsulation vxlan
  route-distinguisher 2:902
  vpn-target 10:902 export-extcommunity
  vpn-target 10:902 import-extcommunity
#
```

2. AZ2 Tenant Border 配置

(1) 创建租管互通 vsi，配置 vxlan mapping

```
vsi CORE_AGENT_VSI_900
 statistics enable
 arp suppression enable
 flooding disable all
 vxlan 900
 evpn encapsulation vxlan
  route-distinguisher auto
  vpn-target auto export-extcommunity
  vpn-target auto import-extcommunity
```

```
  mapping vni 902
#
```

(2) 创建租管互通 mapping vsi

```
vsi CORE_vsimap_VSI_902
 vxlan 902
 evpn encapsulation vxlan
  route-distinguisher 3:902
  vpn-target 10:902 export-extcommunity
  vpn-target 10:902 import-extcommunity
#
```

B.7.2 AZ2 租管互通 Leaf 配置

在租管互通 vpc 所属的 vpn 实例中，增加 vpn-target 10:901 引入引出（红色字体）

```
ip vpn-instance moove-manager
 route-distinguisher 6:901
 description PRE_confige_moove-manager
 #
 address-family ipv4
  vpn-target 0:901 11:901 10:901 import-extcommunity
  vpn-target 11:901 10:901 export-extcommunity
 #
 address-family evpn
  vpn-target 0:901 11:901 10:901 import-extcommunity
  vpn-target 11:901 10:901 export-extcommunity
#
```

B.7.3 配置 租管互通 Pod 不调度到虚拟 AZ 的 TAAG K8S 上

(1) SSH 登录虚拟 AZ TAAG 虚机，查询虚拟 AZ TAAG 虚机的 node 名

```
[root@HZ-AZ1-TAAG_003 ~]# kubectl get node
NAME            STATUS   ROLES    AGE   VERSION
172.40.150.61   Ready    <none>   64d   v1.16.12
172.40.150.62   Ready    <none>   64d   v1.16.12
172.40.150.63   Ready    <none>   64d   v1.16.12
[root@HZ-AZ1-TAAG_003 ~]#
```

(2) 执行 kubectl taint node [*虚拟 AZ TAAG 的 nod 名*] node-role.kubernetes.io/master=:NoSchedule

```
[root@HZ-AZ1-TAAG_003 ~]# kubectl taint node 172.40.150.63 node-role.kubernetes.io/master=:NoSchedule
node/172.40.150.63 tainted
[root@HZ-AZ1-TAAG_003 ~]#
```

(3) 将虚拟 AZ TAAG 虚机上的 pod 删除

```
[root@HZ-AZ1-TAAG_003 ~]# kubectl get pod -o wide
NAME                                  READY   STATUS    RESTARTS   AGE   IP             NODE             NOMINATED NODE   READINESS GATES
taag-dbaas-db-exporter-585b6c5f7d-8t4rr   1/1     Running   42         64d   10.244.2.17    172.40.150.63    <none>           <none>
taag-dbaas-db-exporter-585b6c5f7d-lhsln   1/1     Running   42         64d   10.244.1.15    172.40.150.62    <none>           <none>
taag-dbaas-db-exporter-585b6c5f7d-wvtzv   1/1     Running   41         64d   10.244.0.7     172.40.150.61    <none>           <none>
taag-dbaas-nginx-5f8f78cc55-x92tk         1/1     Running   1          64d   10.244.0.11    172.40.150.61    <none>           <none>
taag-dbaas-vm-exporter-677c7f6979-9spm9   1/1     Running   4          64d   10.244.2.14    172.40.150.63    <none>           <none>
taag-dbaas-vm-exporter-677c7f6979-qrbkk   1/1     Running   2          64d   10.244.0.9     172.40.150.61    <none>           <none>
taag-dbaas-vm-exporter-677c7f6979-s5sbp   1/1     Running   3          64d   10.244.1.12    172.40.150.62    <none>           <none>
taag-monitor-reception-7f8f96cc65-945zf   1/1     Running   0          40d   10.244.0.12    172.40.150.61    <none>           <none>
taag-monitor-reception-7f8f96cc65-brg8k   1/1     Running   0          40d   10.244.2.18    172.40.150.63    <none>           <none>
taag-monitor-reception-7f8f96cc65-tw7zl   1/1     Running   0          40d   10.244.1.17    172.40.150.62    <none>           <none>
uca-paas-nginx-777c6686db-7dn5s           1/1     Running   2          64d   10.244.1.14    172.40.150.62    <none>           <none>
[root@HZ-AZ1-TAAG_003 ~]# kubectl delete pod taag-dbaas-db-exporter-585b6c5f7d-8t4rr
pod "taag-dbaas-db-exporter-585b6c5f7d-8t4rr" deleted
[root@HZ-AZ1-TAAG_003 ~]# kubectl delete pod taag-dbaas-vm-exporter-677c7f6979-9spm9
pod "taag-dbaas-vm-exporter-677c7f6979-9spm9" deleted
[root@HZ-AZ1-TAAG_003 ~]# kubectl delete pod taag-monitor-reception-7f8f96cc65-brg8k
pod "taag-monitor-reception-7f8f96cc65-brg8k" deleted
[root@HZ-AZ1-TAAG_003 ~]#
```

(4) Pod 已不会再调度到虚拟 AZ TAAG 虚机上

```
[root@HZ-AZ1-TAAG_003 ~]# kubectl get pod -o wide
NAME                                  READY   STATUS    RESTARTS   AGE   IP             NODE             NOMINATED NODE   READINESS GATES
taag-dbaas-db-exporter-585b6c5f7d-lhsln   1/1     Running   42         64d   10.244.1.15    172.40.150.62    <none>           <none>
taag-dbaas-db-exporter-585b6c5f7d-vvvcm   1/1     Running   0          63s   10.244.1.18    172.40.150.62    <none>           <none>
taag-dbaas-db-exporter-585b6c5f7d-wvtzv   1/1     Running   41         64d   10.244.0.7     172.40.150.61    <none>           <none>
taag-dbaas-nginx-5f8f78cc55-x92tk         1/1     Running   1          64d   10.244.0.11    172.40.150.61    <none>           <none>
taag-dbaas-vm-exporter-677c7f6979-qrbkk   1/1     Running   2          64d   10.244.0.9     172.40.150.61    <none>           <none>
taag-dbaas-vm-exporter-677c7f6979-s5sbp   1/1     Running   3          64d   10.244.1.12    172.40.150.62    <none>           <none>
taag-dbaas-vm-exporter-677c7f6979-zh7xv   1/1     Running   0          47s   10.244.1.19    172.40.150.62    <none>           <none>
taag-monitor-reception-7f8f96cc65-945zf   1/1     Running   0          40d   10.244.0.12    172.40.150.61    <none>           <none>
taag-monitor-reception-7f8f96cc65-r4gg8   1/1     Running   0          29s   10.244.0.13    172.40.150.61    <none>           <none>
taag-monitor-reception-7f8f96cc65-tw7zl   1/1     Running   0          40d   10.244.1.17    172.40.150.62    <none>           <none>
uca-paas-nginx-777c6686db-7dn5s           1/1     Running   2          64d   10.244.1.14    172.40.150.62    <none>           <none>
[root@HZ-AZ1-TAAG_003 ~]#
[root@HZ-AZ1-TAAG_003 ~]#
```

B.8 公服区互通配置指导

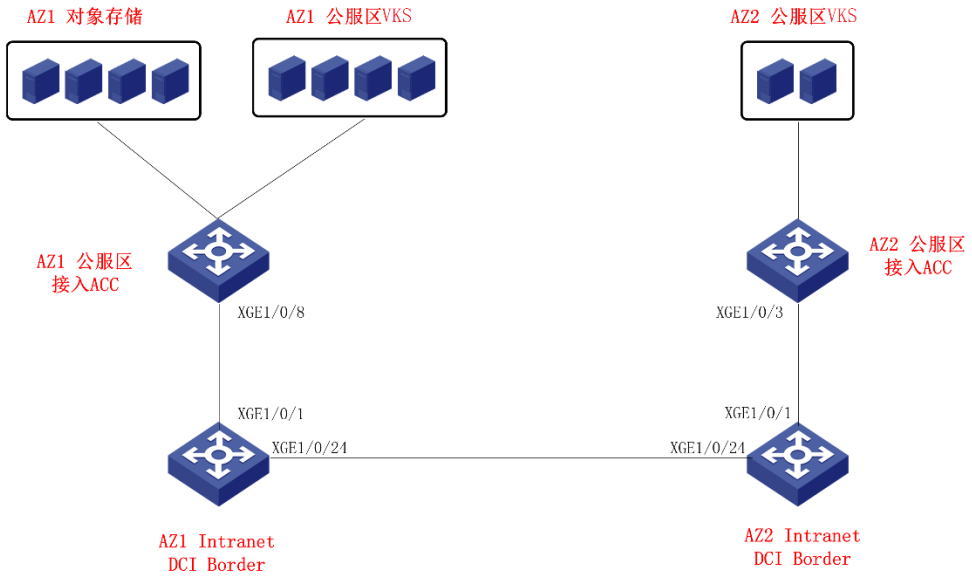
当前版本多 AZ 组网中，对象存储、公服区安全设备等只部署一套在主 AZ 的公服区。需要跨 AZ 部署的虚机（如 GSLB）分别部署在两个 AZ 的公服区 VKS 上。

两个 AZ 的公服区通过手动配置 Intranet DCI Border 路由来实现互通。AZ2 的租户云主机通过 AZ2 的内网互联区 Intranet SNAT 以后经过 Intranet DCI Border 访问 AZ1 的公服区业务网。AZ2 的公服区业务网经过 Intranet DCI Border 访问 AZ1 的公服区业务网。

Intranet DCI Border 可以复用 Tenant DCI Border 设备。

B.8.1 组网图

图B-6 公服区互通组网图



B.8.2 AZ1 公服区接入 ACC 配置

(1) 配置与 AZ1 Intranet DCI Border 的互联接口

```
#
interface Ten-GigabitEthernet1/0/8
 port link-mode route
 ip binding vpn-instance external_vpn
 ip address 10.92.51.161 255.255.255.252
#
```

(2) 配置访问 AZ2 公服区的静态路由

在 AZ1 公服区接入 ACC 配置静态路由，访问 AZ2 公服区业务网、Intranet SNAT 网段，下一跳地址为 AZ1 Intranet DCI Border 的接口地址。

```
#
 ip route-static 100.66.12.0 24 10.92.51.162
 ip route-static 100.64.8.0 22 10.92.51.162
#
```

B.8.3 AZ1 Inranet DCI Border 配置

(1) 创建 Intanet 互联 VPN 实例

```
ip vpn-instance intanet_vpn
```

(2) 配置与 AZ1 公服区接入 ACC 的互联接口

```
#
interface Ten-GigabitEthernet1/0/1
 port link-mode route
```

```
 ip binding vpn-instance intranet_vpn
 ip address 10.92.51.162 255.255.255.252
#
```

(3) 配置访问 AZ1 公服区的静态路由

在 AZ1 Intranet DCI Border 配置静态路由，访问 AZ1 公服区业务网段，下一跳地址为 AZ1 公服区接入 ACC 的接口地址

```
ip route-static vpn-instance intranet_vpn 100.66.1.0 24 10.92.51.161
```

(4) 创建 OSPF 实例并引入静态路由

```
#
ospf 100 router-id 10.92.50.84 vpn-instance intranet_vpn
 import-route static
 area 0.0.0.0
#

配置与 AZ2 Intranet DCI Border 互联接口并使能 OSPF
#
interface Ten-GigabitEthernet1/0/24
 port link-mode route
 ip binding vpn-instance intranet_vpn
 ip address 10.93.51.141 255.255.255.252
 ospf network-type p2p
 ospf 100 area 0.0.0.0
#
```

B.8.4 AZ2 公服区接入 ACC 配置

(1) 配置与 AZ2 Intranet DCI Border 的互联接口

```
#
interface Ten-GigabitEthernet1/0/3
 port link-mode route
 ip binding vpn-instance external_vpn
 ip address 10.93.51.41 255.255.255.252
#
```

(2) 配置访问 AZ1 公服区的静态路由

在 AZ2 公服区接入 ACC 配置静态路由，访问 AZ1 公服区业务网段，下一跳地址为 AZ2 Intranet DCI Border 的接口地址

```
#
 ip route-static 100.66.1.0 24 10.93.51.42
#
```

B.8.5 AZ2 Inranet DCI Border 配置

(1) 创建 Intanet 互联 VPN 实例

```
ip vpn-instance intanet_vpn
```

(2) 配置与 AZ2 公服区接入 ACC 的互联接口

```
#
```

```
interface Ten-GigabitEthernet1/0/1
 port link-mode route
 ip binding vpn-instance intranet_vpn
 ip address 10.93.51.42 255.255.255.252
#
```

(3) 配置访问 AZ2 公服区的静态路由

在 AZ2 Intranet DCI Border 配置静态路由，访问 AZ2 公服区业务、Intranet 网段，下一跳地址为 AZ2 公服区接入 ACC 的接口地址

```
#
ip route-static vpn-instance intranet_vpn 100.66.8.0 22 10.93.51.41
ip route-static vpn-instance intranet_vpn 100.66.12.0 24 10.93.51.41
#
```

(4) 创建 OSPF 实例并引入静态路由

```
#
ospf 100 router-id 10.92.50.85 vpn-instance intranet_vpn
 import-route static
 area 0.0.0.0
#
```

(5) 配置与 AZ1 Intranet DCI Border 互联接口并使能 OSPF

```
#
interface Ten-GigabitEthernet1/0/24
 port link-mode route
 ip binding vpn-instance intranet_vpn
 ip address 10.93.51.142 255.255.255.252
 ospf network-type p2p
 ospf 100 area 0.0.0.0
#
```

B.8.6 验证配置

(1) 查看 AZ1 Intranet DCI Border 的路由，可以学习到 AZ2 公服区业务网、Intranet SNAT 网段路由

```
[AZ1-TenantDCIborder-172.16.205.84]display  ip routing-table vpn-instance intranet_vpn

Destinations : 19       Routes : 19

Destination/Mask    Proto   Pre Cost        NextHop         Interface
0.0.0.0/32          Direct  0   0           127.0.0.1       InLoop0
10.92.51.160/30     Direct  0   0           10.92.51.162    XGE1/0/1
10.92.51.160/32     Direct  0   0           10.92.51.162    XGE1/0/1
10.92.51.162/32     Direct  0   0           127.0.0.1       InLoop0
10.92.51.163/32     Direct  0   0           10.92.51.162    XGE1/0/1
10.93.51.140/30     Direct  0   0           10.93.51.141    XGE1/0/24
10.93.51.140/32     Direct  0   0           10.93.51.141    XGE1/0/24
10.93.51.141/32     Direct  0   0           127.0.0.1       InLoop0
10.93.51.143/32     Direct  0   0           10.93.51.141    XGE1/0/24
100.66.1.0/24       Static  60  0           10.92.51.161    XGE1/0/1
100.66.8.0/22       O_ASE2  150 1           10.93.51.142    XGE1/0/24
100.66.12.0/24      O_ASE2  150 1           10.93.51.142    XGE1/0/24
127.0.0.0/8         Direct  0   0           127.0.0.1       InLoop0
127.0.0.0/32        Direct  0   0           127.0.0.1       InLoop0
127.0.0.1/32        Direct  0   0           127.0.0.1       InLoop0
127.255.255.255/32  Direct  0   0           127.0.0.1       InLoop0
224.0.0.0/4         Direct  0   0           0.0.0.0         NULL0
224.0.0.0/24        Direct  0   0           0.0.0.0         NULL0
255.255.255.255/32  Direct  0   0           127.0.0.1       InLoop0
```

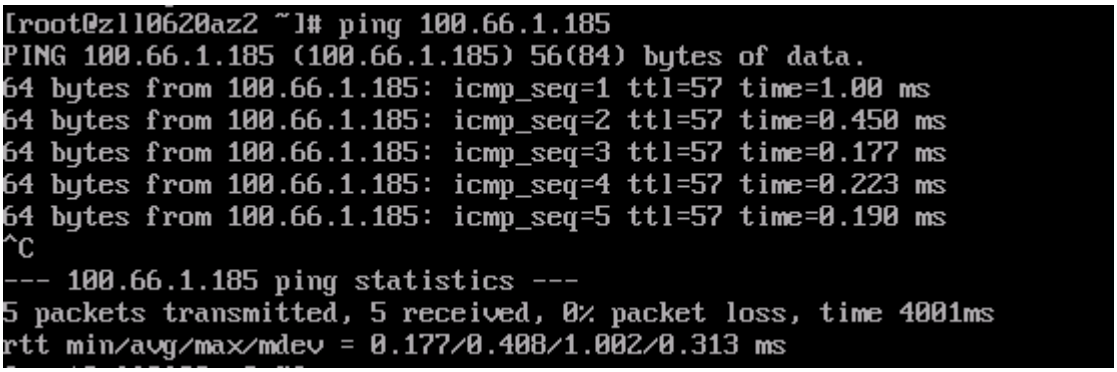
(2) 查看 AZ2 Intranet DCI Border 的路由，可以学习到 AZ1 公服区业务网路由

```
[AZ2-TenantDCIborder-172.41.205.85]display ip routing-table vpn-instance intranet_vpn

Destinations : 19       Routes : 19

Destination/Mask    Proto   Pre Cost        NextHop         Interface
0.0.0.0/32          Direct  0   0           127.0.0.1       InLoop0
10.93.51.40/30      Direct  0   0           10.93.51.42     XGE1/0/1
10.93.51.40/32      Direct  0   0           10.93.51.42     XGE1/0/1
10.93.51.42/32      Direct  0   0           127.0.0.1       InLoop0
10.93.51.43/32      Direct  0   0           10.93.51.42     XGE1/0/1
10.93.51.140/30     Direct  0   0           10.93.51.142    XGE1/0/24
10.93.51.140/32     Direct  0   0           10.93.51.142    XGE1/0/24
10.93.51.142/32     Direct  0   0           127.0.0.1       InLoop0
10.93.51.143/32     Direct  0   0           10.93.51.142    XGE1/0/24
100.66.1.0/24       O_ASE2  150 1           10.93.51.141    XGE1/0/24
100.66.8.0/22       Static  60  0           10.93.51.41     XGE1/0/1
100.66.12.0/24      Static  60  0           10.93.51.41     XGE1/0/1
127.0.0.0/8         Direct  0   0           127.0.0.1       InLoop0
127.0.0.0/32        Direct  0   0           127.0.0.1       InLoop0
127.0.0.1/32        Direct  0   0           127.0.0.1       InLoop0
127.255.255.255/32  Direct  0   0           127.0.0.1       InLoop0
224.0.0.0/4         Direct  0   0           0.0.0.0         NULL0
224.0.0.0/24        Direct  0   0           0.0.0.0         NULL0
255.255.255.255/32  Direct  0   0           127.0.0.1       InLoop0
```

(3) AZ2 公服区业务网可以 ping 通 AZ1 公服区业务网

```
[AZ2-intraborder-205.105]ping -a 100.66.12.254 -vpn-instance external_vpn 100.66.1.254
Ping 100.66.1.254 (100.66.1.254) from 100.66.12.254: 56 data bytes, press CTRL+C to break
56 bytes from 100.66.1.254: icmp_seq=0 ttl=253 time=1.473 ms
56 bytes from 100.66.1.254: icmp_seq=1 ttl=253 time=1.272 ms
56 bytes from 100.66.1.254: icmp_seq=2 ttl=253 time=1.084 ms
56 bytes from 100.66.1.254: icmp_seq=3 ttl=253 time=1.140 ms
56 bytes from 100.66.1.254: icmp_seq=4 ttl=253 time=1.204 ms

--- Ping statistics for 100.66.1.254 in VPN instance external_vpn ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.084/1.235/1.473/0.135 ms
```

(4)　AZ2 虚拟机可以 ping 通 AZ1 公服区业务网



附录C 管理区虚拟机开关机顺序

如果在项目部署时有特殊情况需要关闭管理区的虚拟机，请严格按照如下顺序进行关机和开机操作。

C.1 关机顺序

C.1.1 集群关机顺序

管理区虚拟机集群的关机顺序依次为：

(1) K8S 集群
(2) MySQL 集群
(3) PostgreSQL 集群
(4) Redis 集群
(5) RabbitMQ 集群
(6) Zookeeper 集群
(7) Kafka 集群
(8) PMS 集群
(9) Image-server 集群
(10) Cassandra 集群
(11) 公共虚拟机

在虚拟机集群中，也需要按照顺序依次关机，请严格执行。

C.1.2 K8S 集群

K8S 集群虚拟机之间没有特定的关机顺序，全部安全关闭即可。包括如下虚拟机：

⚠ 注意

请根据现场实际环境关闭 K8S 集群，例如多 AZ 情况下，关闭从 AZ 的虚拟机时，切勿关闭主 AZ 的虚拟机。

下列为全量 K8S 集群，现场环境中如果没有部署某个 K8S 集群，请忽略。

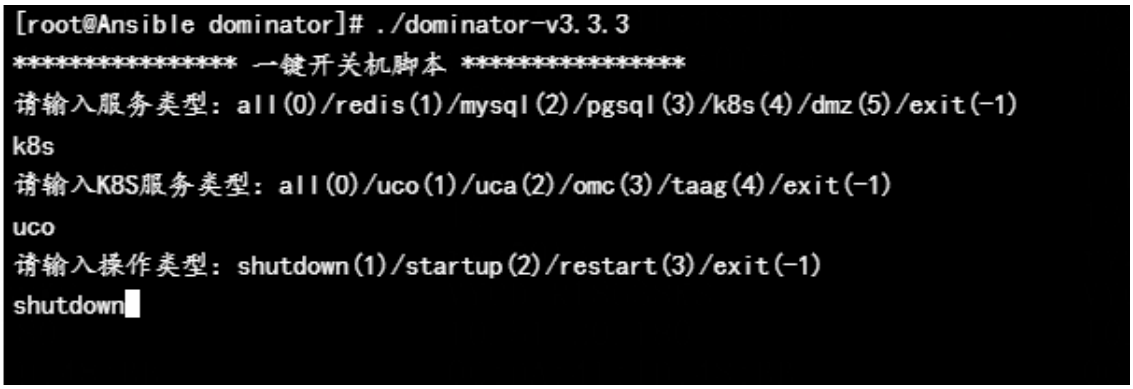
- AUTOPS-UCA-K8S-01
- XXXX-UCA-K8S-02
- XXXX-UCA-K8S-03
- XXXX-UCO-K8S-01
- XXXX-UCO-K8S-02
- XXXX-UCO-K8S-03
- XXXX-TAAG-K8S-01

- XXXX-TAAG-K8S-02
- XXXX-TAAG-K8S-03
- XXXX-DMZ-K8S-01
- XXXX-DMZ-K8S-02
- XXXX-DMZ-K8S-03
- XXXX-OMC-K8S-01
- XXXX-OMC-K8S-02
- XXXX-OMC-K8S-03

您可以手动关闭集群虚机，也可以使用一键开关机脚本来自动关闭集群虚机。通过一键开关机脚本关闭虚拟机方法如下：

(1) 对脚本进行初始化配置，具体请参见“C.3 一键开关机脚本基础配置”。

(2) 执行./dominator-v3.3.3 命令，根据提示进行选择对应的集群类型和操作类型（可使用数字代替），按<Enter>键确认，脚本工具会自动执行对应操作。



C.1.3 MySQL 集群

MySQL 集群的虚拟机包括：

- XXXX-UCA-MYSQL-01
- XXXX-UCA-MYSQL-02
- XXXX-UCA-MYSQL-03
- XXXX-UCA-MYSQL-REPM-MANAGER

按照如下顺序依次关闭虚拟机：

⚠ 注意

关机前，请确认 MySQL 集群状态正常。

---

(1) 关闭 XXXX-UCA-MYSQL-REPM-MANAGER。

(2) 关闭 XXXX-UCA-MYSQL-03。

(3) 关闭 MySQL 集群的 Slave 节点（从节点：虚机内部 ip a 显示没有 vip 的）。

(4) 关闭 MySQL 集群的 Master 节点（主节点：虚机内部 ip a 显示有 vip 的）。

请记录主从节点所在虚拟机信息，后面开机时会用到。

您可以手动关闭集群虚机，也可以使用一键开关机脚本来自动关闭集群虚机。通过一键开关机脚本关闭虚拟机方法如下：

(1) 对脚本进行初始化配置，具体请参见“C.3 一键开关机脚本基础配置”。

(2) 执行./dominator-v3.3.3 命令，根据提示进行选择对应的集群类型和操作类型（可使用数字代替），按<Enter>键确认，脚本工具会自动执行对应操作。

```
[root@Ansible dominator]# ./dominator-v3.3.3
**************** 一键开关机脚本 ****************
请输入服务类型：all(0)/redis(1)/mysql(2)/pgsql(3)/k8s(4)/dmz(5)/exit(-1)
mysql
请输入操作类型：shutdown(1)/startup(2)/restart(3)/exit(-1)
shutdown
```

C.1.4 PostgreSQL 集群

PostgreSQL 集群的虚拟机包括：

- XXXX-PGSQL-01
- XXXX-PGSQL-02
- XXXX-PGSQL-03

按照从如下顺序依次关闭虚拟机：

⚠ 注意

关机前，请确认 PostgreSQL 集群状态正常。

---

(1) 关闭 Standby (没有 vip 存在的)。

(2) 关闭 Primary (有 vip 存在的)。

(3) 关闭 XXXX-PGSQL-03。

请记录主从节点所在虚拟机信息，后面开机时会用到。

您可以手动关闭集群虚机，也可以使用一键开关机脚本来自动关闭集群虚机。通过一键开关机脚本关闭虚拟机方法如下：

(1) 对脚本进行初始化配置，具体请参见“C.3 一键开关机脚本基础配置”。

(2) 执行./dominator-v3.3.3 命令，根据提示进行选择对应的集群类型和操作类型（可使用数字代替），按<Enter>键确认，脚本工具会自动执行对应操作。

C.1.5 Redis 集群

Redis 集群的虚拟机包括：

- XXXX-REDIS-01
- XXXX-REDIS-02
- XXXX-REDIS-03

按照如下顺序依次关闭虚拟机：

⚠ 注意

关机前，请确认 Redis 集群状态正常。

---

(1) 先登录虚机内部，关闭服务。

a. 三台都执行关闭哨兵，命令如下：

```
systemctl stop redis-sentinel
```

若没有 `redis-sentinel` 服务，请执行`/etc/init.d/server-sentinel stop`

b. 关闭 Redis 集群 Slave 节点的 Redis 服务（从节点：虚机内部 ip a 显示没有 vip 的）

```
systemctl stop redis
```

若没有 `redis-sentinel` 服务，请执行`/etc/init.d/server-redis stop`

c. 关闭 Redis 集群 Master 节点的 Redis 服务（主节点：虚机内部 ip a 显示有 vip 的）

```
systemctl stop redis
```

(2) 关闭虚拟机（记录主从所在虚机信息）。

a. 关闭 ZJ-AN-uca-REDIS03。

b. 关闭 Redis 集群 Slave 节点虚机。

c. 关闭 Redis 集群 Master 节点虚机。

您可以手动关闭集群虚机，也可以使用一键开关机脚本来自动关闭集群虚机。通过一键开关机脚本关闭虚拟机方法如下：

(1) 对脚本进行初始化配置，具体请参见“C.3 一键开关机脚本基础配置”。

(2) 执行./dominator-v3.3.3 命令，根据提示进行选择对应的集群类型和操作类型（可使用数字代替），按<Enter>键确认，脚本工具会自动执行对应操作。

```
[root@Ansible dominator]# ./dominator-v3.3.3
**************** 一键开关机脚本 ****************
请输入服务类型: all(0)/redis(1)/mysql(2)/pgsql(3)/k8s(4)/dmz(5)/exit(-1)
redis
请输入操作类型: shutdown(1)/startup(2)/restart(3)/exit(-1)
shutdown
```

C.1.6 RabbitMQ 集群

RabbitMQ 集群虚拟机之间没有特定的关机顺序，直接进行安全关闭即可。包括如下虚拟机：

- XXXX-RABBITMQ-01
- XXXX-RABBITMQ-02
- XXXX-RABBITMQ-03

C.1.7 Zookeeper 集群

Zookeeper 集群虚拟机之间没有特定的关机顺序，直接进行安全关闭即可。包括如下虚拟机：

- XXXX-UCA-ZOOKEEPER-01
- XXXX-UCA-ZOOKEEPER-02
- XXXX-UCA-ZOOKEEPER-03

C.1.8 Kafka 集群

Kafka 集群虚拟机之间没有特定的关机顺序，直接进行安全关闭即可。包括如下虚拟机：

- XXXX-UCA-KAFKA-01
- XXXX-UCA-KAFKA-02
- XXXX-UCA-KAFKA-03

C.1.9 PMS 集群

XXXX-OP-PMS-01

C.1.10 Image-server 集群

Image-serve 集群虚拟机之间没有特定的关机顺序，直接进行安全关闭即可。包括如下虚拟机：

- XXXX-IMAGE-SERVER-01
- XXXX-IMAGE-SERVER-02
- XXXX-IMAGE-SERVER-03

C.1.11 OMC 基础组件

OMC 基础组件虚拟机之间没有特定的关机顺序，直接进行安全关闭即可。包括如下虚拟机：

- XXXX-OMCBASE-ES-01

- XXXX-OMCBASE-ES-02
- XXXX-OMCBASE-ES-03
- XXXX-OMCBASE-ES-04
- XXXX-OMCBASE-CASS-01
- XXXX-OMCBASE-CASS-02
- XXXX-OMCBASE-CASS-03
- XXXX-OMCBASE-CASS-04
- XXXX-OMCBASE-GITLAB-01

C.1.12 公共虚拟机

公共虚拟机没有特定的关机顺序，全部安全关闭即可。包括：

- XXXX-ANSIBLE-01
- XXXX-HARBOR-01
- XXXX-NGINX-01
- XXXX-NGINX-02
- XXXX-TFTPSERVER-01

C.2 开机顺序

C.2.1 集群开机顺序

管理区虚拟机集群的开机顺序依次为：

(1) RabbitMQ 集群
(2) Zookeeper 集群
(3) Kafka 集群
(4) PMS 集群
(5) Image-server 集群
(6) Cassandra 集群
(7) 公共虚拟机
(8) Redis 集群
(9) PostgreSQL 集群
(10) MySQL 集群
(11) K8S 集群

在虚拟机集群中，也需要按照顺序依次开机，请严格执行。

C.2.2 RabbitMQ 集群

RabbitMQ 集群虚拟机之间没有特定的开机顺序，全部安全开启即可。包括如下虚拟机：

- XXXX-RABBITMQ-01
- XXXX-RABBITMQ-02

- XXXX-RABBITMQ-03

C.2.3 Zookeeper 集群

Zookeeper 集群虚拟机之间没有特定的开机顺序，全部安全开启即可。包括如下虚拟机：

- XXXX-UCA-ZOOKEEPER-01
- XXXX-UCA-ZOOKEEPER-02
- XXXX-UCA-ZOOKEEPER-03

C.2.4 Kafka 集群

Kafka 集群虚拟机之间没有特定的开机顺序，全部安全开启即可。包括如下虚拟机：

- XXXX-UCA-KAFKA-01
- XXXX-UCA-KAFKA-02
- XXXX-UCA-KAFKA-03

C.2.5 PMS 集群

XXXX-OP-PMS-01

C.2.6 Image-server 集群

Image-serve 集群虚拟机之间没有特定的开机顺序，全部安全开启即可。包括如下虚拟机：

- XXXX-IMAGE-SERVER-01
- XXXX-IMAGE-SERVER-02
- XXXX-IMAGE-SERVER-03

C.2.7 OMC 基础组件

OMC 基础组件虚拟机之间没有特定的开机顺序，全部安全开启即可。包括如下虚拟机：

- XXXX-OMCBASE-ES-01
- XXXX-OMCBASE-ES-02
- XXXX-OMCBASE-ES-03
- XXXX-OMCBASE-ES-04
- XXXX-OMCBASE-CASS-01
- XXXX-OMCBASE-CASS-02
- XXXX-OMCBASE-CASS-03
- XXXX-OMCBASE-CASS-04
- XXXX-OMCBASE-GITLAB-01

开启后，需手动恢复状态并进行检查。

(1) Cassandra 集群检查

a. 以 root 身份登录到 Cassandra 虚拟机上，执行如下命令：

```
systemctl status Cassandra
```

确认状态为 running。

b. 执行如下命令：

```
nodetool status
```

确认 Cassandra 的四个节点都处于 UN 状态，各个节点为 UP。

c. 执行如下命令，查看集群的 Schema。

```
nodetool describecluster
```

确认节点个数为 4，同时 4 个节点在同一个 Schema。

(2) ES 集群检查

a. 以 root 身份登录到 ES 虚拟机上，四台机器依次执行命令：

```
systemctl status elasticsearch
```

确认 4 台 ES 机器 elasticsearch.service 为 running 状态。

b. 启动完成之后，执行 CURL 命令测试 ES 集群状态。首先查看 ES 版本。

```
cat /usr/lib/systemd/system/elasticsearch.service | grep Environment=ES_HOME | grep -Po '(?<=-).*'
```

c. 根据不同版本执行对应命令，查看集群节点数，节点数为 4 时正常。

```
curl http://127.0.0.1:9200/_cat/nodes          # 7.3.0 版本命令
curl -k -u 'elastic:devops2020@es' https://127.0.0.1:9200/_cat/nodes        # 7.10.2 版本，增加 basicauth 和 SSL，检查时增加认证并忽略证书校验
```

d. 根据不同版本执行对应命令，检查健康状态，status 字段为 green 时正常。

```
curl http://127.0.0.1:9200/_cluster/health     # 7.3.0 版本命令
curl -k -u 'elastic:devops2020@es' https://127.0.0.1:9200/_cluster/health    # 7.10.2 版本，增加 basicauth 和 SSL，检查时增加认证并忽略证书校验
```

如果 status 字段为 yellow，其中一个原因是关机之前部分存在本地缓存里的分片没有写到硬盘就掉电了，上电之后这部分就是未分片状态，此种情况下会自动恢复为 green 状态。回显中的 unassigned_shards 字段为未分片数。多次查询可以发现未分片数在不断减小（例如第二次回显为"unassigned_shards":376），等待未分片数减小到 0 时，status 字段会变为 green。

示例如下。

```
[root@OMCBASE-ES-01 ~]# curl -k -u 'elastic:devops2020@es' https://127.0.0.1:9200/_cluster/health
{"cluster_name":"XX 节点_ELASTICSEARCH","status":"yellow","timed_out":false,"number_of_nodes":4,"number_of_data_nodes":4,"active_primary_shards":1517,"active_shards":1855,"relocating_shards":0,"initializing_shards":7,"unassigned_shards":1663,"delayed_unassigned_shards":0,"number_of_pending_tasks":2,"number_of_in_flight_fetch":0,"task_max_waiting_in_queue_millis":29,"active_shards_percent_as_number":52.6241134751773}

[root@OMCBASE-ES-01 ~]# curl -k -u 'elastic:devops2020@es' https://127.0.0.1:9200/_cluster/health
{"cluster_name":"XX 节点_ELASTICSEARCH","status":"yellow","timed_out":false,"number_of_nodes":4,"number_of_data_nodes":4,"active_primary_shards":1533,"active_shards":3180,"relocating_shards":0,"initializing_shards":7,"unassigned_shards":376,"delayed_unassigned_shards":0,"number_of_pending_tasks":0,"number_of_in_flight_fetch":0,"task_max_waiting_in_queue_millis":0,"active_shards_percent_as_number":89.25063149031715}
```

C.2.8 公共虚拟机

公共虚拟机没有特定的开机顺序，全部安全开启即可。包括：

- XXXX-ANSIBLE-01
- XXXX-HARBOR-01
- XXXX-NGINX-01
- XXXX-NGINX-02
- XXXX-TFTPSERVER-01

C.2.9 Redis 集群

Redis 集群的虚拟机包括：

- XXXX-REDIS-01
- XXXX-REDIS-02
- XXXX-REDIS-03

根据关机时记录的主从节点所在虚机信息，按照如下顺序依次开启虚拟机：

(1) 开启 Redis 集群 Master 节点虚机。

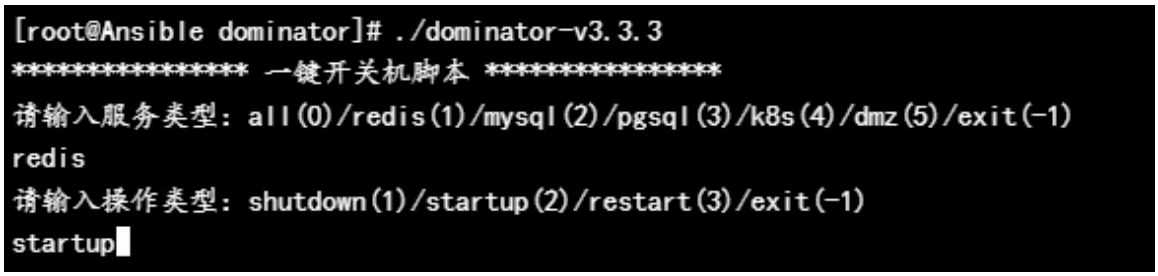
(2) 开启 Redis 集群 Slave 节点虚机。

(3) 开启 XXXX-REDIS-03。

您可以手动开启集群虚机，也可以使用一键开关机脚本开启集群虚机（前提是使用了本脚本进行关机）。通过一键开关机脚本开启虚拟机的方法如下：

(1) 对脚本进行初始化配置，具体请参见“C.3 一键开关机脚本基础配置”。

(2) 执行./dominator-v3.3.3，根据提示进行选择对应的集群类型和操作类型（可使用数字代替），按<Enter>键确认，脚本工具会自动执行对应操作。具体运行日志会同步输出在控制台以及同目录下“dominator_xx.log”文件。



C.2.10 PostgreSQL 集群

PostgreSQL 集群的虚拟机包括：

- XXXX-PGSQL-01
- XXXX-PGSQL-02
- XXXX-PGSQL-03

(1) 根据关机时记录的主从节点所在虚机信息，按照如下顺序依次开启虚拟机：

a. 开启 Witness（XXXX-PGSQL-03）。

b. 开启 Primary（有 VIP 存在的）。

c. 开启 Standby（没有 VIP 存在的）。

(2) 检查集群状态。

a. 登录到 Witness（XXXX-PGSQL-03）节点，输入如下命令：

```
su - postgres -c “repmgr cluster show”
```

若回显中 Role 分别为三个角色且唯一则正确。

否则，登录到 Status 为“!running”的节点，依次执行以下命令：

```
su - postgres
pg_ctl -D /var/lib/pgsql/11/data stop
/usr/pgsql-11/bin/repmgr -h 10.253.146.77 -U repmgr -d repmgr -f
/etc/repmgr/11/repmgr.conf standby clone --upstream-node-id=2 --force
sudo systemctl restart postgresql-11
repmgr standby register –-force
```

上述命令中，请修改如下字段为实际环境的值：10.253.146.77 为 Status 为“*running”的节点 IP 地址(除了 witeness 节点)；upstream-node-id=2 中的 2 是 Status 为“*running”的节点的 ID。

b. 循环执行步骤 a，直至正确。

(3) 检查 VIP 是否存在。

a. 集群状态正确之后，登陆到 Role 为 primary 的节点执行以下命令，查看 VIP：

```
VIP=`cat /pgscript/failover.sh  | grep VIRTUALIP= | awk -F "=" '{print $2}'`
echo $VIP
```

b. 执行以下命令，查看本机是否存在 VIP：

```
hostname –I
```

若 VIP 存在，则正确。

否则，执行以下命令添加 VIP：

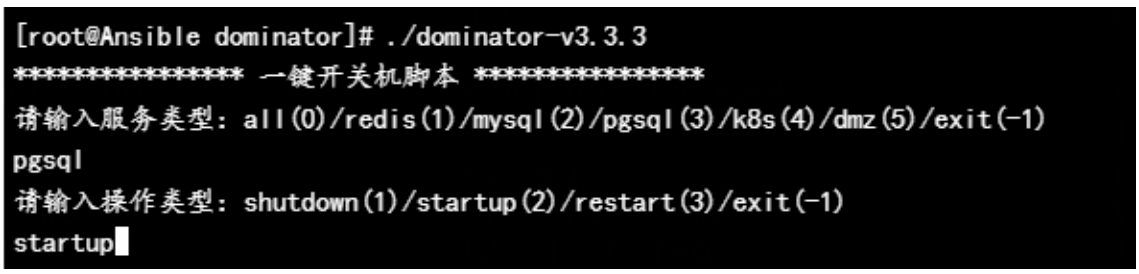
```
ip addr add $VIP/24 dev eth0
```

c. 循环执行步骤 b，直至正确。

您可以手动开启集群虚机，也可以使用一键开关机脚本开启集群虚机（前提是使用了本脚本进行关机）。通过一键开关机脚本开启虚拟机的方法如下：

(1) 对脚本进行初始化配置，具体请参见“C.3 一键开关机脚本基础配置”。

(2) 执行./dominator-v3.3.3，根据提示进行选择对应的集群类型和操作类型（可使用数字代替），按<Enter>键确认，脚本工具会自动执行对应操作。具体运行日志会同步输出在控制台以及同目录下“dominator_xx.log”文件。



C.2.11 MySQL 集群

MySQL 集群的虚拟机包括：

- XXXX-UCA-MYSQL-01
- XXXX-UCA-MYSQL-02
- XXXX-UCA-MYSQL-03
- XXXX-UCA-MYSQL-REPM-MANAGER

根据关机时记录的主从节点所在虚机信息，按照如下顺序依次开启虚拟机：

(1) 开启 MySQL 集群的 Master 节点（主节点：虚机内部 ip a 显示有 vip 的）。

(2) 开启 MySQL 集群的 2 个 Slave 节点（从节点：虚机内部 ip a 显示没有 vip 的）。

(3) 开启 XXXX-UCA-MYSQL-REPM-MANAGER。

您可以手动开启集群虚机，也可以使用一键开关机脚本开启集群虚机（前提是使用了本脚本进行关机）。通过一键开关机脚本开启虚拟机的方法如下：

(4) 对脚本进行初始化配置，具体请参见“C.3 一键开关机脚本基础配置”。

(5) 执行./dominator-v3.3.3，根据提示进行选择对应的集群类型和操作类型（可使用数字代替），按<Enter>键确认，脚本工具会自动执行对应操作。具体运行日志会同步输出在控制台以及同目录下“dominator_xx.log”文件。

```
[root@Ansible dominator]# ./dominator-v3.3.3
**************** 一键开关机脚本 ****************
请输入服务类型：all(0)/redis(1)/mysql(2)/pgsql(3)/k8s(4)/dmz(5)/exit(-1)
mysql
请输入操作类型：shutdown(1)/startup(2)/restart(3)/exit(-1)
startup
```

C.2.12 K8S 集群

K8S 集群虚拟机之间没有特定的开机顺序，全部安全开启即可。包括如下虚拟机：

- AUTOPS-UCA-K8S-01
- XXXX-UCA-K8S-02
- XXXX-UCA-K8S-03
- XXXX-UCO-K8S-01
- XXXX-UCO-K8S-02
- XXXX-UCO-K8S-03
- XXXX-TAAG-K8S-01
- XXXX-TAAG-K8S-02
- XXXX-TAAG-K8S-03
- XXXX-DMZ-K8S-01
- XXXX-DMZ-K8S-02

- XXXX-DMZ-K8S-03
- XXXX-OMC-K8S-01
- XXXX-OMC-K8S-02
- XXXX-OMC-K8S-03

您可以手动开启集群虚机，也可以使用一键开关机脚本开启集群虚机（前提是使用了本脚本进行关机）。通过一键开关机脚本开启虚拟机的方法如下：

(1) 对脚本进行初始化配置，具体请参见“C.3 一键开关机脚本基础配置”。

(2) 执行./dominator-v3.3.3，根据提示进行选择对应的集群类型和操作类型（可使用数字代替），按<Enter>键确认，脚本工具会自动执行对应操作。具体运行日志会同步输出在控制台以及同目录下“dominator_xx.log”文件。

C.3 一键开关机脚本基础配置

C.3.1 注意事项

- 不支持直接使用此脚本开机

  脚本执行集群关机过程中会记录必要的集群关机前的必要信息，如：主从节点的 IP、vmid 信息等到本地，若未使用本工具关机或因其他意外断电集群关机，直接使用本工具开机可能会出现无法开机的情况。

- 不支持穿插其他手动操作

  此脚本工具只负责管理使用本脚本开关机各集群后服务正常访问使用，其他途径手动开关虚机导致服务异常不在此脚本工具处理范围。

C.3.2 脚本构成

此脚本工具主要包括 3 个文件：dominator-v3.3.3、dominator.yml 和 dominator.db。具体项目中，务必要根据实际情况修改 dominator.yml 配置文件中的底座 IP 和虚拟机所在 CAS 地址以及账号信息。若 DMZ 和其他 K8S 集群不在同一套 CAS，需分别维护，单独处理。

```yaml
# 基座中节点配置清单
deploy:
  setting:
    # path支持本地路径及网络资源路径（http://IP:8080/www/tasks/deployDetails.json）
    path: http://IP:8080/www/tasks/deployDetails.json

# cas相关配置
cas:
  schema: http # cas的API协议
  port: 8080 # cas的API端口
  ip: 192.168.3.9 # cas服务地址
  username: admin # cas管理员账号
  password: admin # cas管理员账号密码
```

C.3.3 执行步骤

(1) 将 dominator-v3.3.3 脚本存放于底座服务器的任意目录，默认位置在 rebirth 平台虚机的 /root/tools/dominator 目录下，赋予可执行权限即可直接执行。

(2) 调整配置（dominator.yml）

- deploy.setting.path：服务虚机的规划信息，与基座共用。可配置资源地址（http://xxx/deployDetails.json），需要根据现场环境调整。
- cas.*：cas 平台 admin 账号配置，用于操作虚拟机，需要根据现场环境调整。

(3) 执行一键开关机脚本：

```
./dominator-v3.3.3
```

根据提示进行选择对应的集群类型和操作类型（可使用数字代替），按<Enter>键确认，脚本工具会自动执行对应操作。具体运行日志会同步输出在控制台以及同目录下“dominator_xx.log”文件。

示例如下：

```
[root@Ansible dominator]# ./dominator-v3.3.3
**************** 一键开关机脚本 ****************
请输入服务类型：all(0)/redis(1)/mysql(2)/pgsql(3)/k8s(4)/dmz(5)/exit(-1)
k8s
请输入K8S服务类型：all(0)/uco(1)/uca(2)/omc(3)/taag(4)/exit(-1)
uco
请输入操作类型：shutdown(1)/startup(2)/restart(3)/exit(-1)
shutdown
```

附录D 特殊型号裸金属初始化

对于某些特殊型号的裸金属服务器，请参考如下方法进行初始化操作。

D.1 前提条件

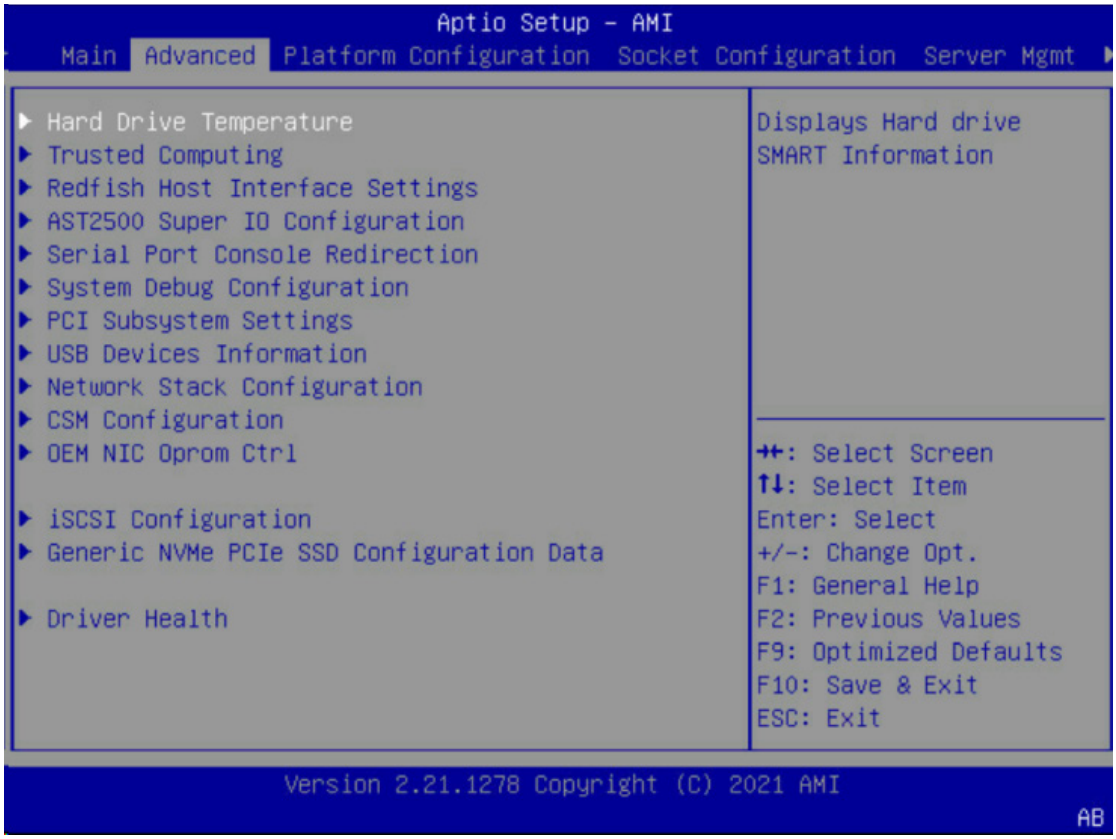
进行初始化操作前，请先搭建好 DHCP 和 TFTP 环境。

D.2 NF5280M6型号

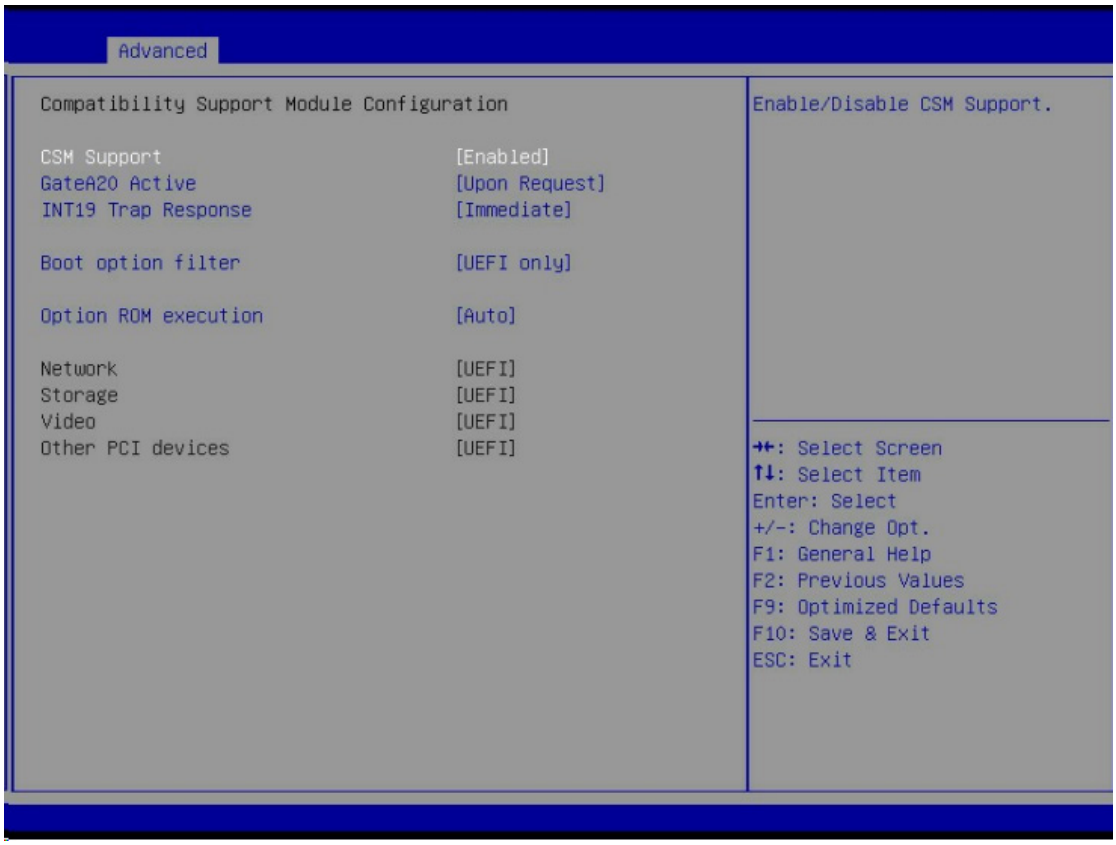
1. 设置 UEFI

(1) 进入 BIOS Setup 界面。

(2) 选择 Advanced 界面，如下图所示。



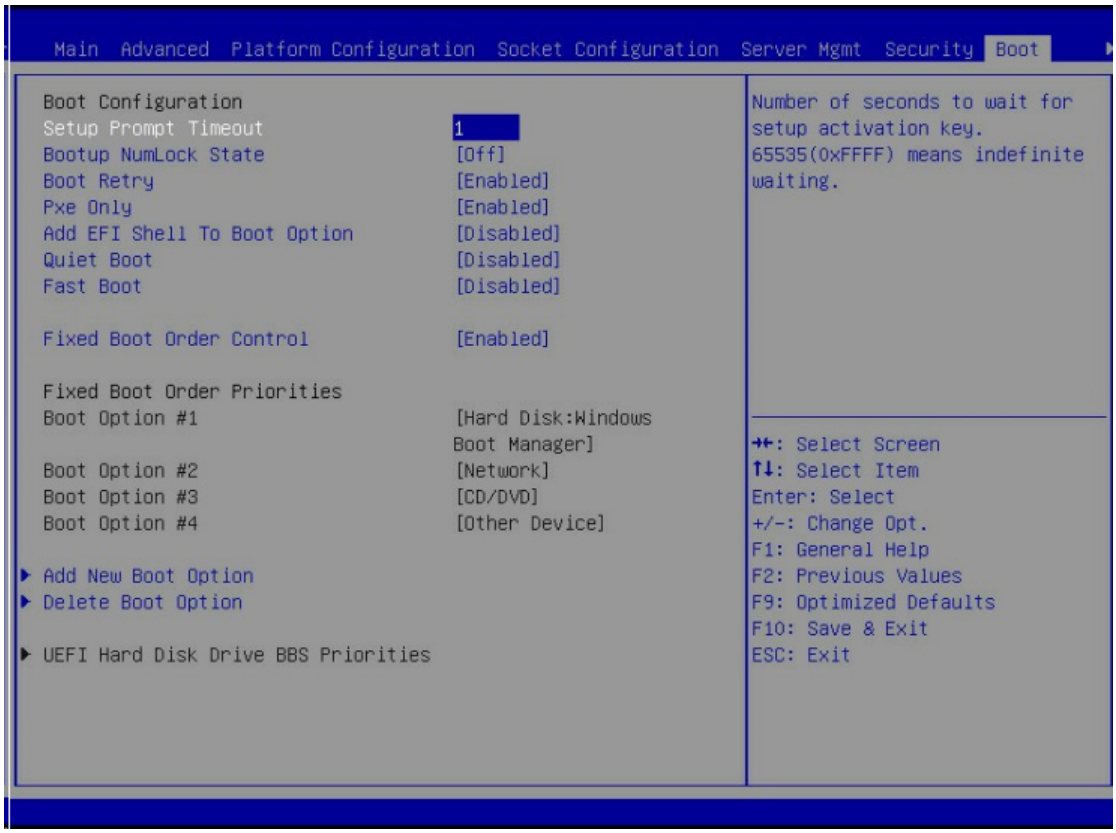
(3) 选择“CSM Configuration”，按“Enter”进入，如下图所示。



(4) 选择“Boot option filter”，按“Enter 选择 UEFI only。

2. 设置服务器启动顺序

(1) 选择 Boot 界面。



(2) 选择“Fixed Boot Order Control”，按“Enter”，在弹出的选项对话框中选择 “Disabled”，按”Enter”。

(3) “Boot Option #1”变为可选状态，选择“Boot Option #1”，按“Enter”, 根据需要在弹出的选项对话框中选择“Hard Disk”或“Network”或“CD/DVD”或 “Other Device”为第一启动项。 “Boot Option #2”与“Boot Option #1”设置相同。

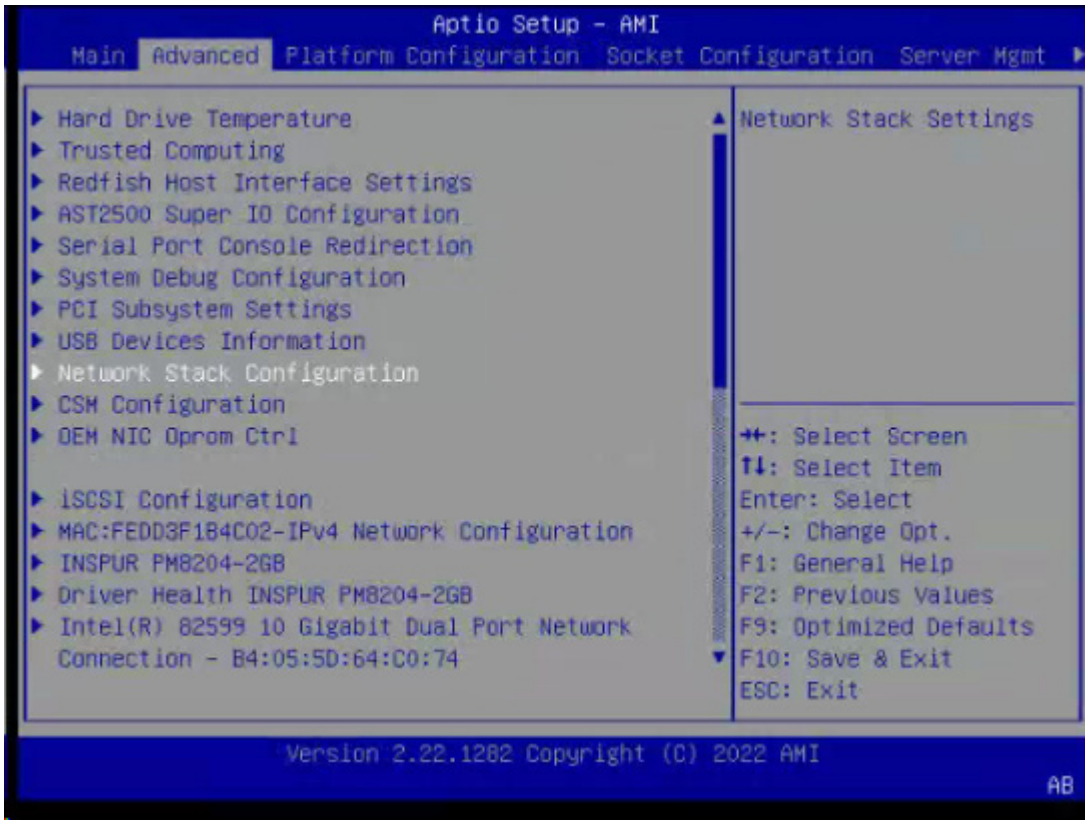
最终设置为：

BootOption#1: Hard Disk

BootOption#2: Network

3. 设置 PXE 启动项

Network Stack Configuration 界面是 Network UEFI PXE 相关选项设置。



(1) 选择 Network Stack，Enter 设置为 Enabled。

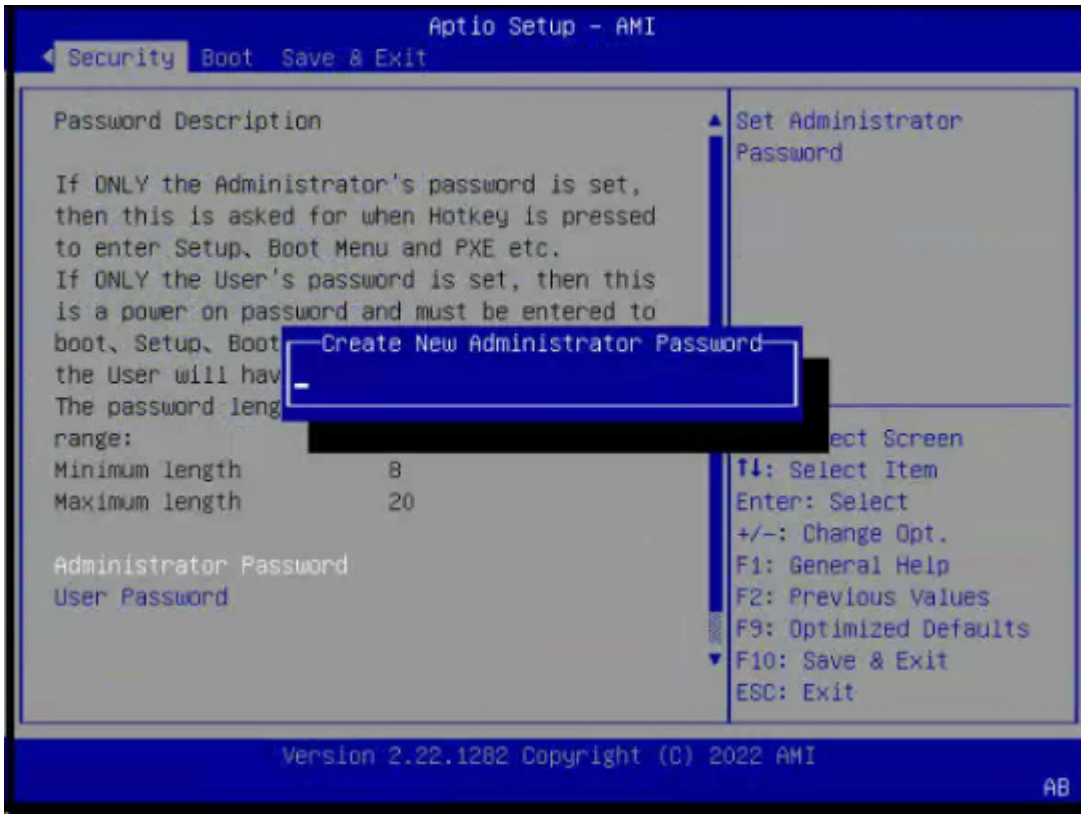
(2) 将 Ipv4 PXE Support 设置为 Enabled。

(3) Ipv6 PXE Support 设置为 Disabled。

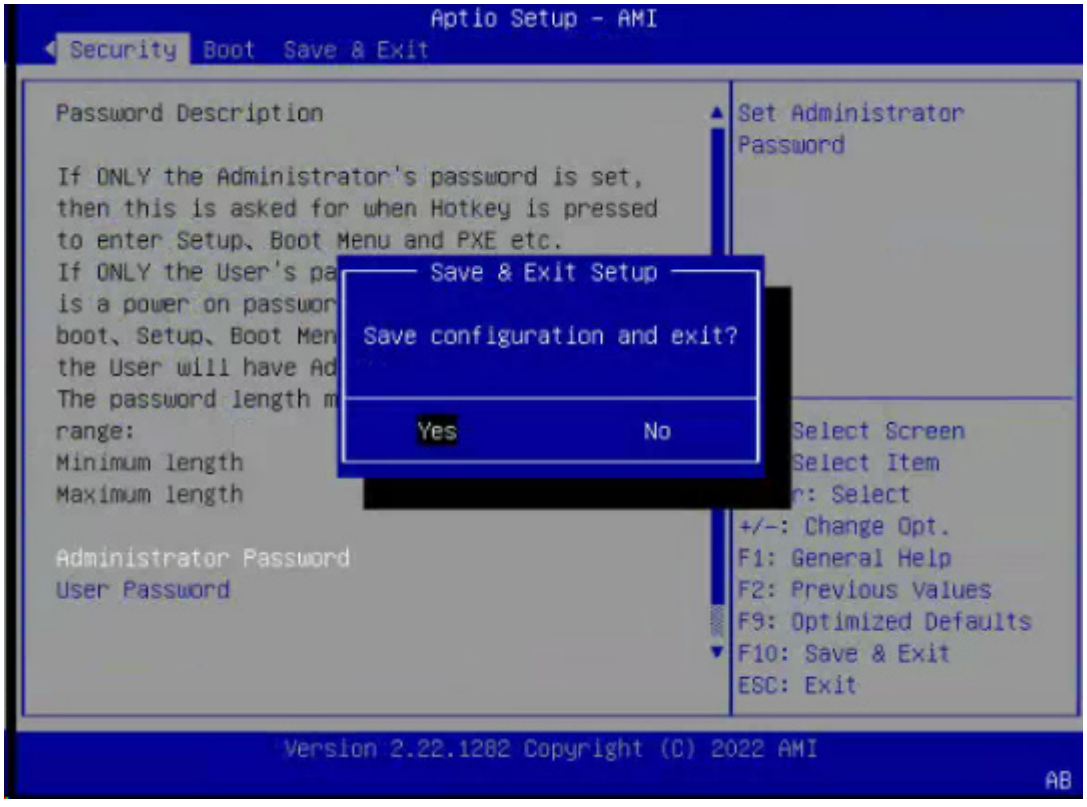
4. 设置 BIOS ADMIN 密码

(1) 进入 security 界面。

(2) 设置 administrator password 为：U1cloud@M00ve



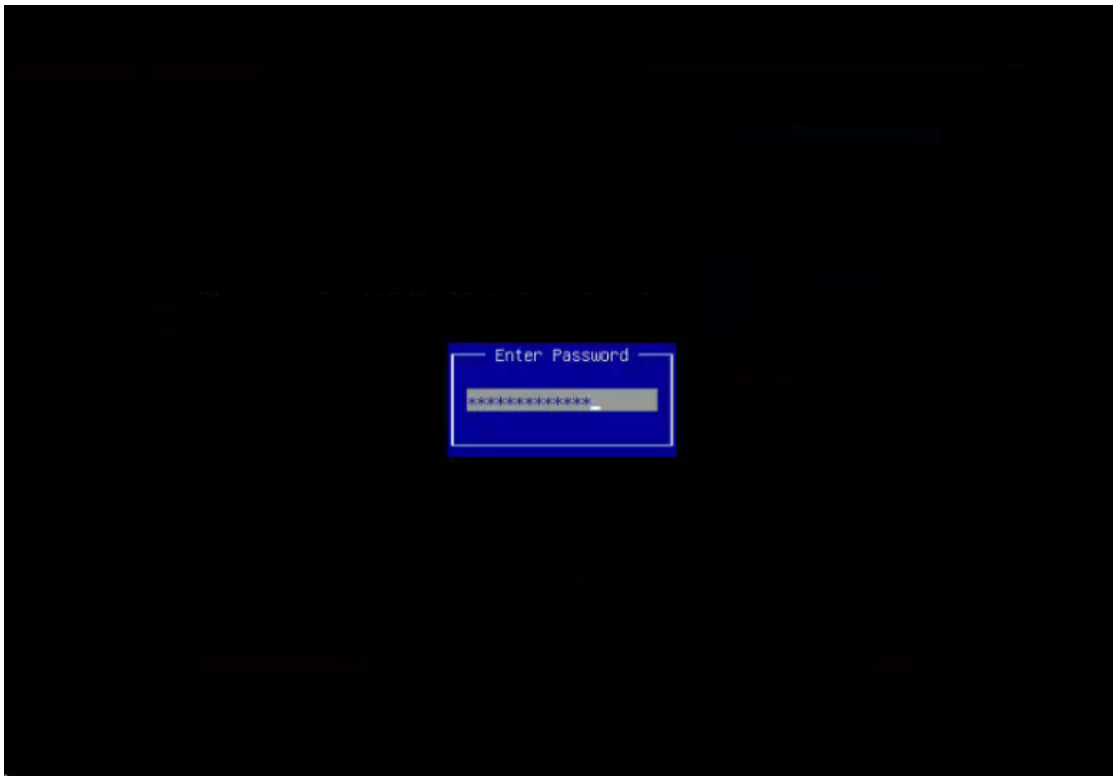
(3) 按 F10 保存设置。



5. 加载 PXE 小镜像

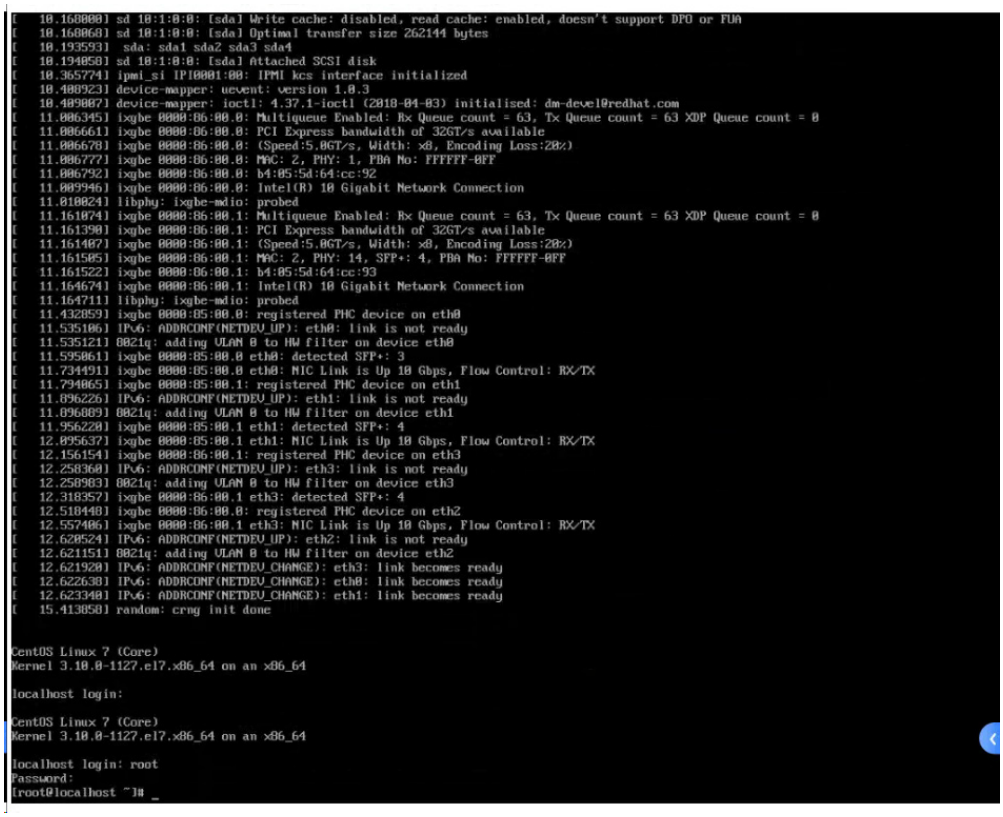
(1) 按 F12 进入 PXE，获取小镜像。

(2) 输入密码 U1cloud@M00ve。



(3) 等待至以下界面，即为 load 小镜像成功。

(4) 等待系统加载完毕 root/unicloud 进入系统即完成。



6. 设置 VNC 密码为 cds-ch1n

(1) 执行命令 hostname -I，获取小镜像 IP。

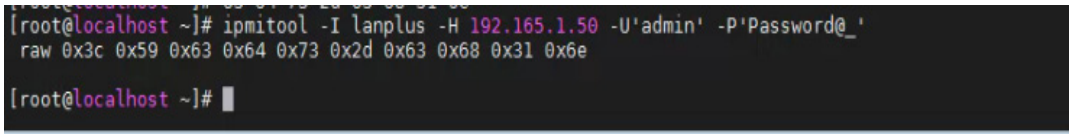
(2) MobaXterm 登陆小镜像 IP（上图中小镜像 IP 为 10.250.2.3），账号密码为：root/unicloud。

(3) 执行以下命令：

```
ipmitool -I lanplus -H 192.165.1.50 -U'admin' -P'Password@_' raw 0x3c 0x59 0x63 0x64
0x73 0x2d 0x63 0x68 0x31 0x6e
```

命令中以下 3 处需要修改为环境中的带外管理信息：

- 带外管理地址（IPMI）192.165.1.50
- 带外管理账号 admin
- 带外管理密码 Password@_



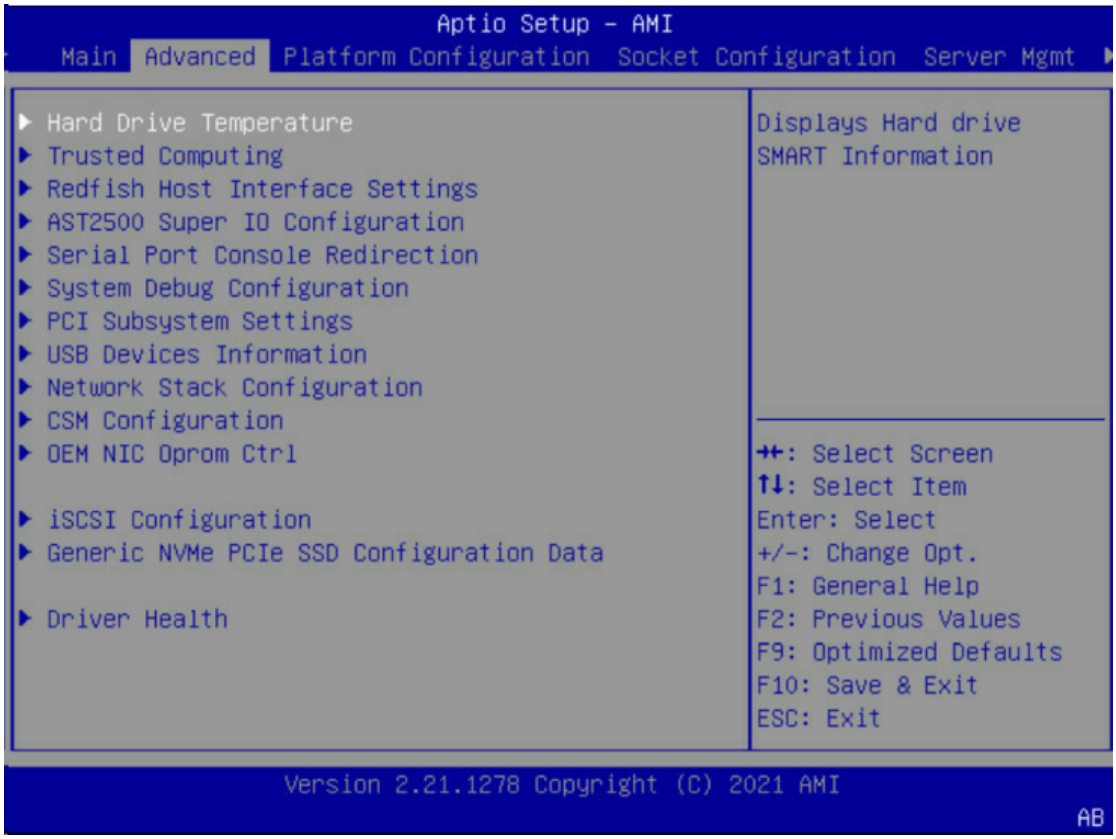
D.3 NF8260M6型号

请在 BIOS 操作页面进行以下操作。

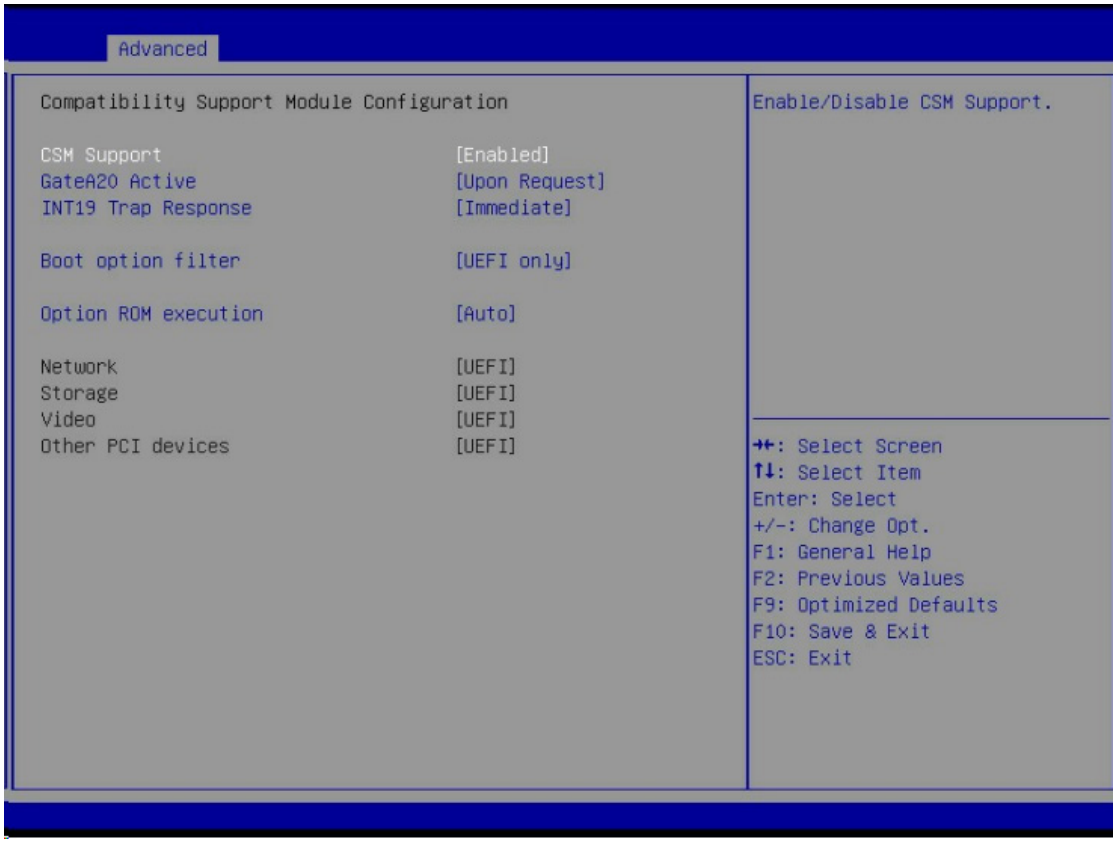
1. 设置 UEFI

(1) 进入 BIOS Setup 界面。

(2) 选择 Advanced 界面，如下图所示。



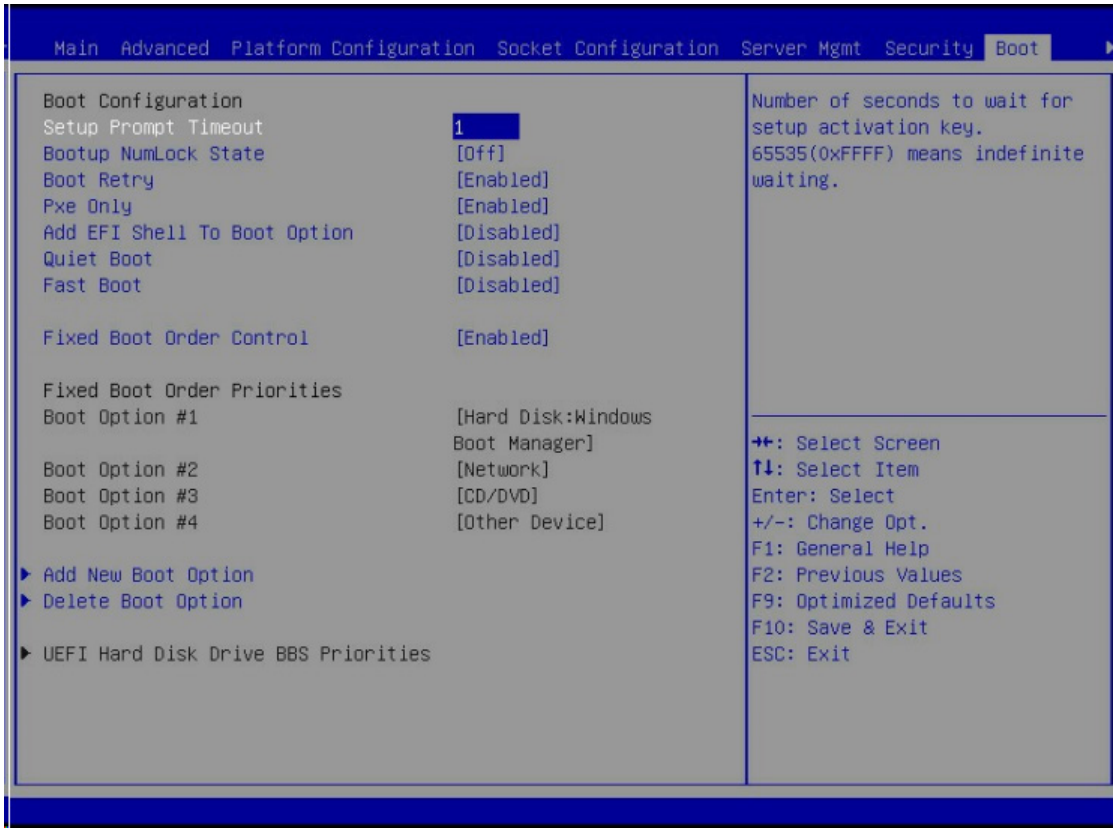
(3) 选择“CSM Configuration”，按“Enter”进入，如下图所示。



(4) 选择“Boot option filter”，按“Enter 选择 UEFI only。

2. 设置服务器启动顺序

(1) 选择 Boot 界面。



(2) 选择“Fixed Boot Order Control”，按“Enter”，在弹出的选项对话框中选择 “Disabled”，按”Enter”。

(3) “Boot Option #1”变为可选状态，选择“Boot Option #1”，按“Enter”, 根据需要在弹出的选项对话框中选择“Hard Disk”或“Network”或“CD/DVD”或 “Other Device”为第一启动项。 “Boot Option #2”与“Boot Option #1”设置相同。

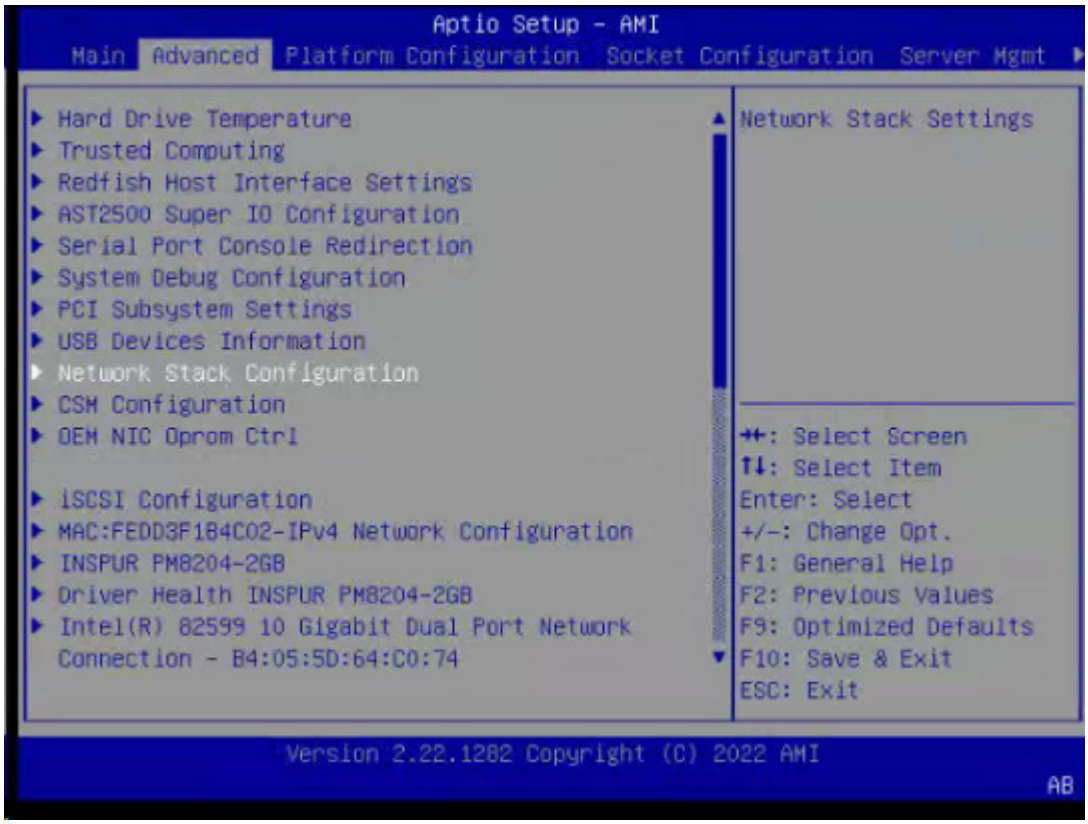
最终设置为：

BootOption#1: Hard Disk

BootOption#2: Network

3. 设置 PXE 启动

(1) Network Stack Configuration 界面是 Network UEFI PXE 相关选项设置。



(2) 选择 Network Stack，Enter 设置为 Enabled。

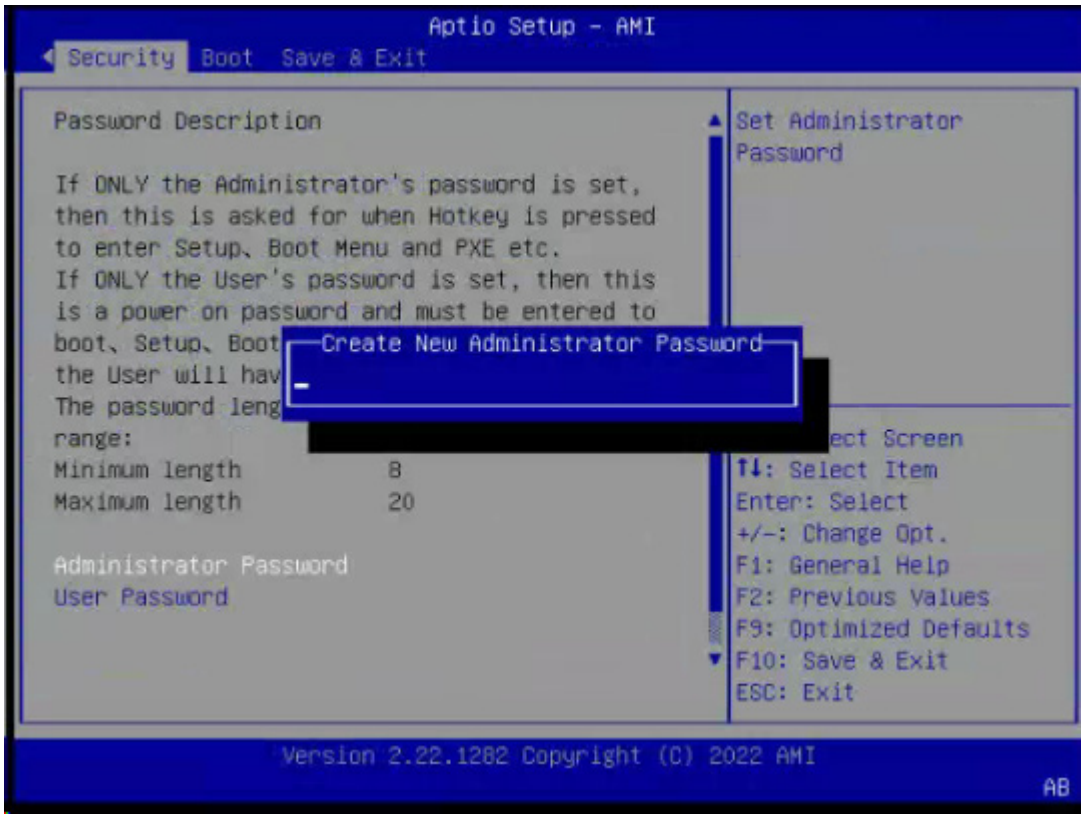
(3) 将 Ipv4 PXE Support 设置为 Enabled。

(4) Ipv6 PXE Support 设置为 Disabled。

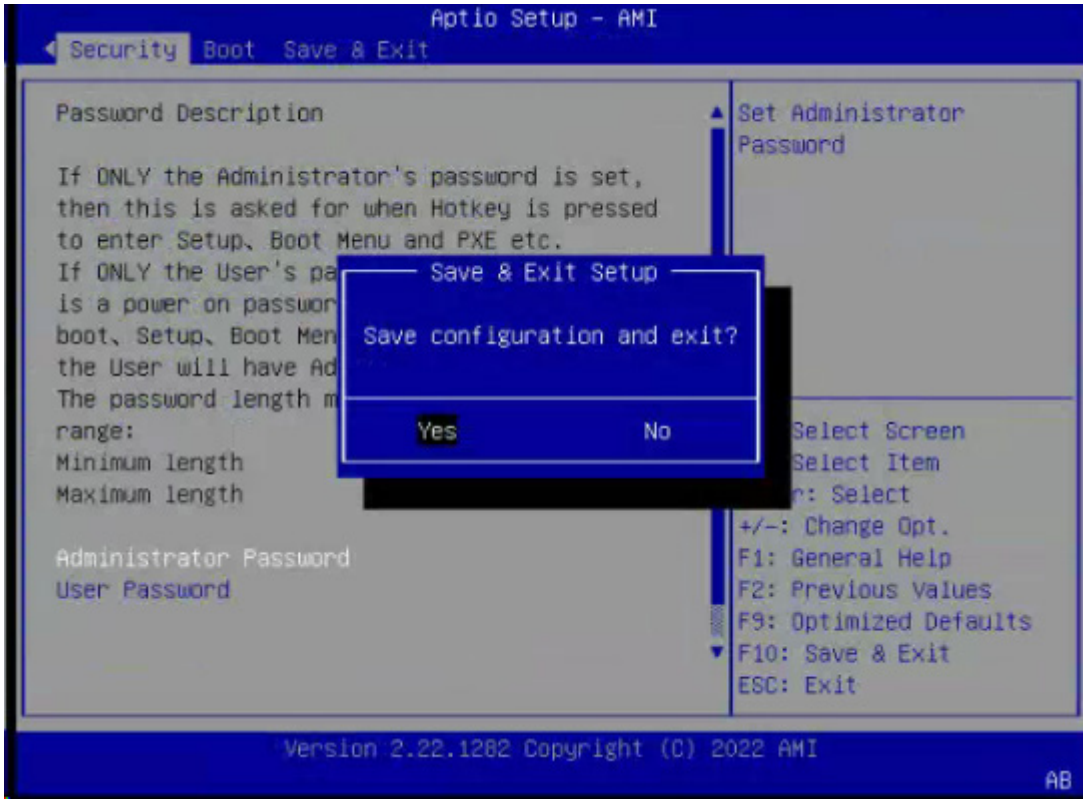
4. 设置 BIOS ADMIN 密码

(1) 进入 security 界面。

(2) 设置 administrator password 为：U1cloud@M00ve



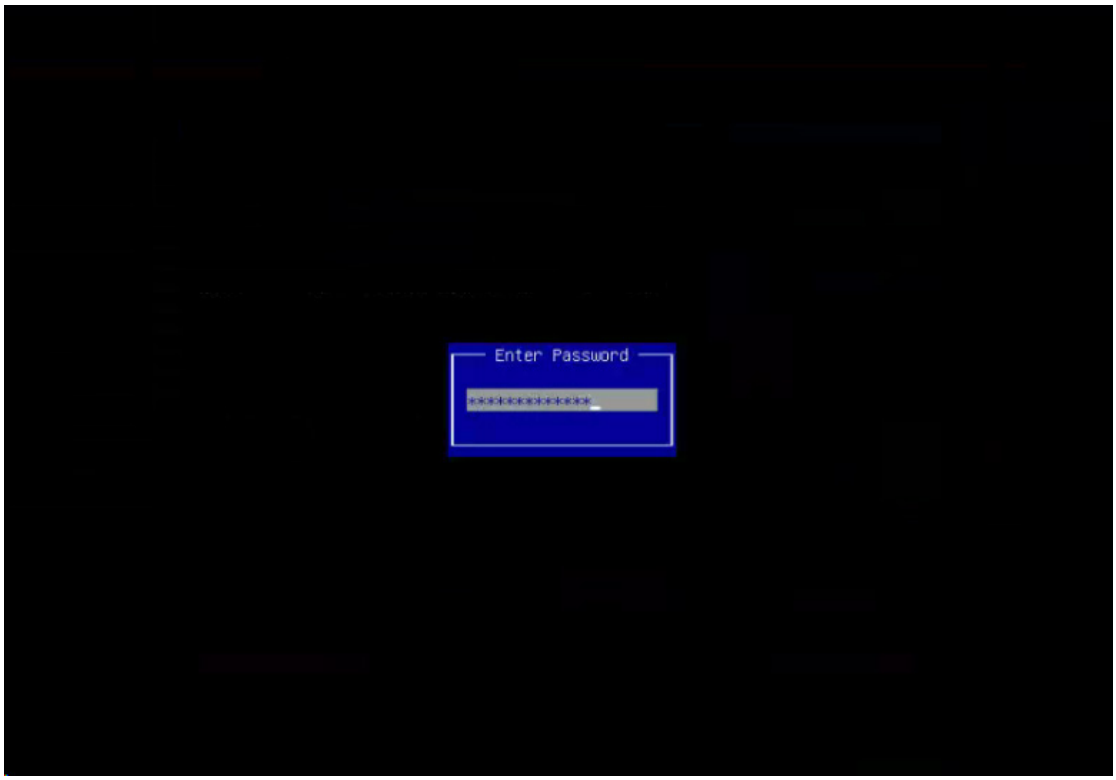
(3) 按 F10 保存设置。



5. 加载 PXE 小镜像

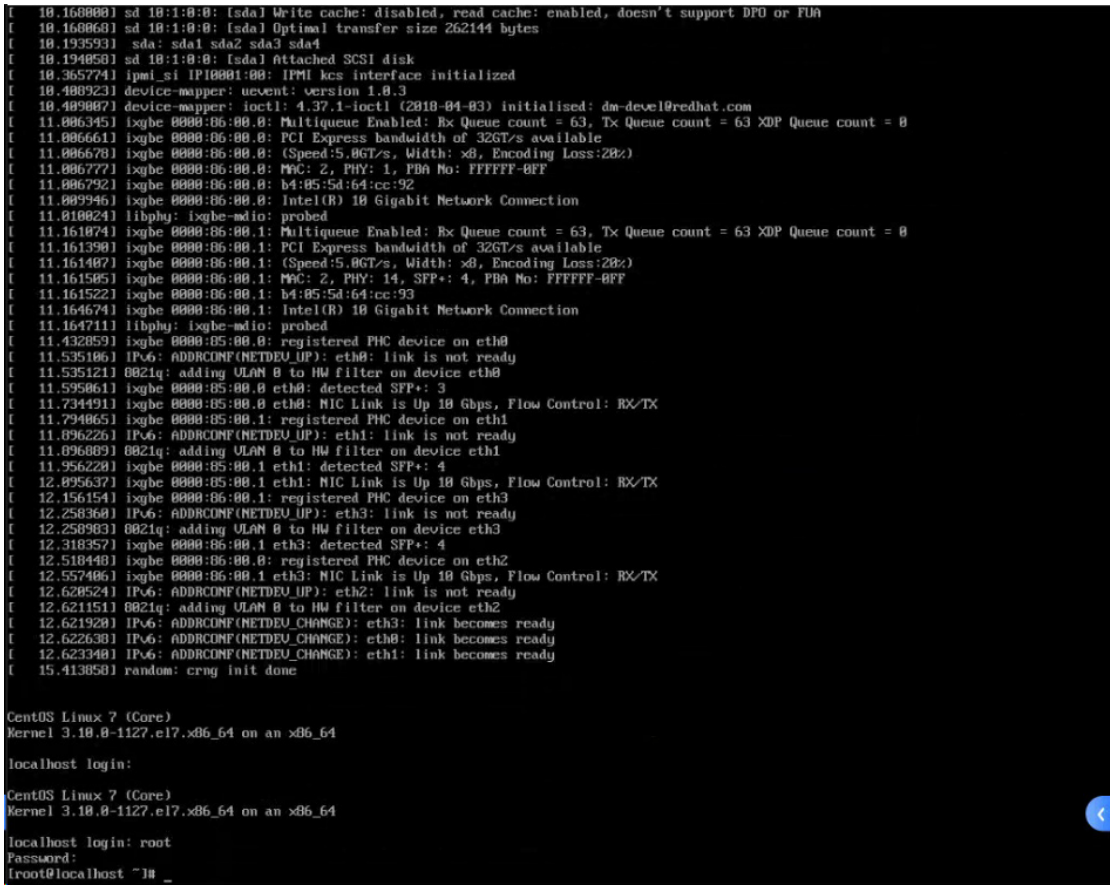
(1) 按 F12 进入 PXE 获取小镜像。

(2) 输入密码 U1cloud@M00ve



(3) 等待至以下界面，即为 load 小镜像成功。

(4) 等待系统加载完毕 root/unicloud 进入系统即完成。



6. 设置 VNC 密码为 cds-ch1n

(1) 执行命令 hostname -I，获取小镜像 IP。

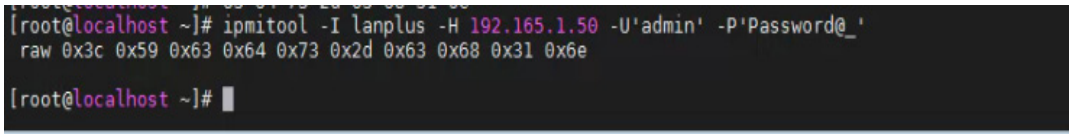
(2) MobaXterm 登陆小镜像 IP（上图中小镜像 IP 为 10.250.2.3），账号密码为：root/unicloud。

(3) 执行以下命令：

```
ipmitool -I lanplus -H 192.165.1.50 -U'admin' -P'Password@_' raw 0x3c 0x59 0x63 0x64
0x73 0x2d 0x63 0x68 0x31 0x6e
```

命令中以下 3 处需要修改为环境中的带外管理信息：

- 带外管理地址（IPMI）192.165.1.50
- 带外管理账号 admin
- 带外管理密码 Password@_

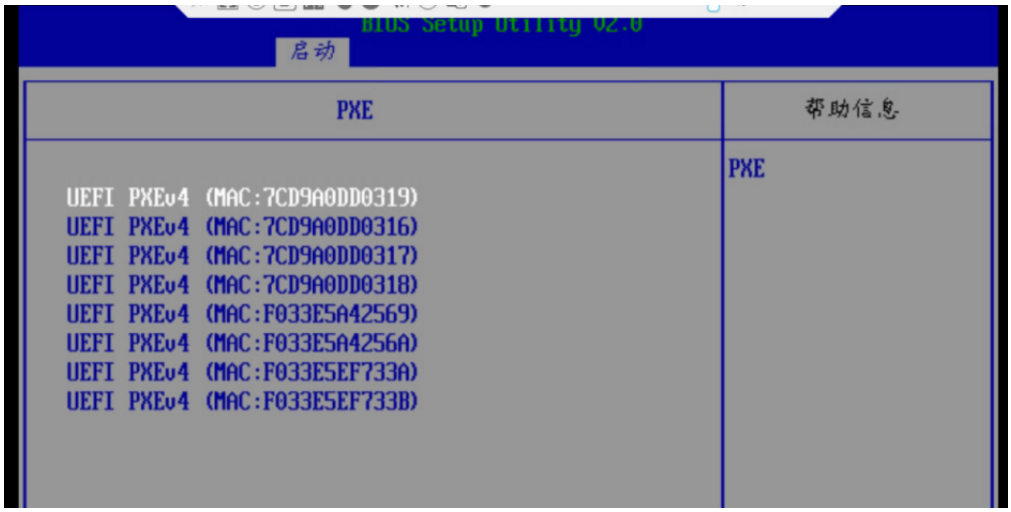


D.4 鲲鹏R3820 G3

鲲鹏 R3820 G3 ARM 架构的裸金属服务器暂不支持云平台对 BIOS 进行自动化设置，需手动配置，服务器默认为 UEFI 启动模式。

D.4.1 设置服务器启动顺序

进入 BIOS 启动页面，在启动分类调整中，设置启动顺序为第一优先级为硬盘设备，第二优先级为 PXE，同时可以在 PXE 网卡启动顺序中，将第一设备设置为管理网卡，可加速 PXE 引导过程。



D.4.2 设置 PXE 启动

(1) 登陆需配置的裸金属服务器 BMC 页面，在系统管理中—BIOS 配置中，引导介质有效期选择单次有效，引导介质选择 PXE，点击保存，重启后生效。

(2) 设置 BIOS ADMIN 密码

进入 BIOS 安全界面，设置管理员密码（administrator password）为 U1cloud@M00ve。

(3) 设置 VNC 密码

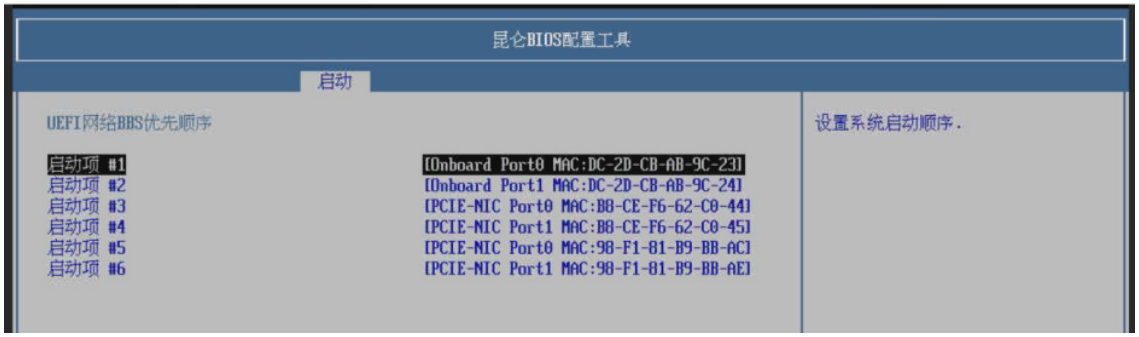
登陆 BMC，在远程设置中，开启 VNC 服务，并设置 VNC 密码为 cds-ch1n。

D.5 飞腾R3810 G5

飞腾 R3810 G5 ARM 架构的裸金属服务器暂不支持云平台对 BIOS 进行自动化设置，需手动配置，服务器默认为 UEFI 启动模式。

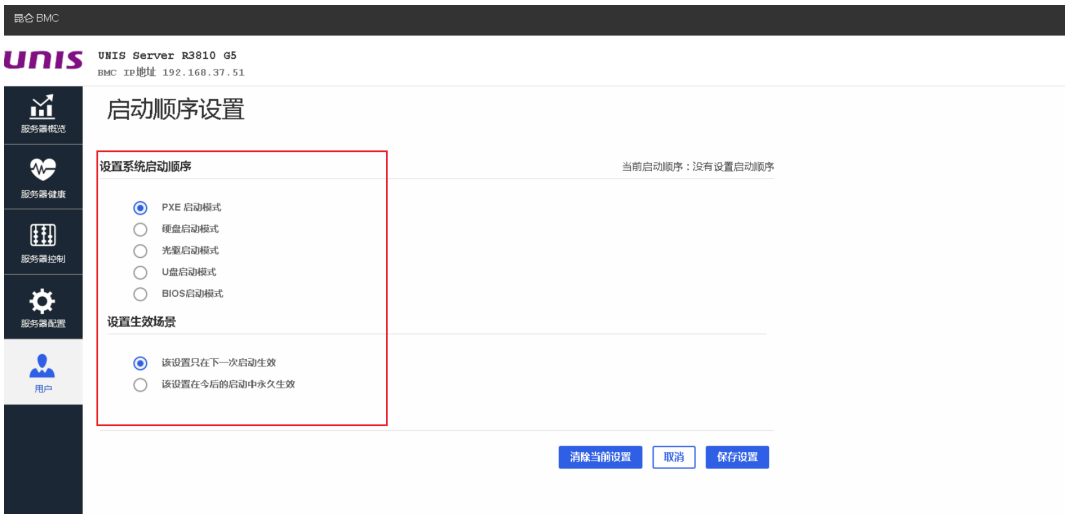
D.5.1 设置服务器启动顺序

进入 BIOS 启动页面，在默认启动顺序设置中，设置启动顺序为第一优先级为硬盘，第二优先级为网络，同时可以在 UEFI 网络 BBS 优先顺序中，将启动项#1 为管理网卡，可加速 PXE 引导过程。



D.5.2 设置 PXE 启动设置

(1) 登录需配置的裸金属服务器 BMC 页面，在[服务器配置/启动顺序设置]中，设置系统启动顺序为 PXE 启动模式，设置生效场景，点击<保存设置>按钮，重启后生效。



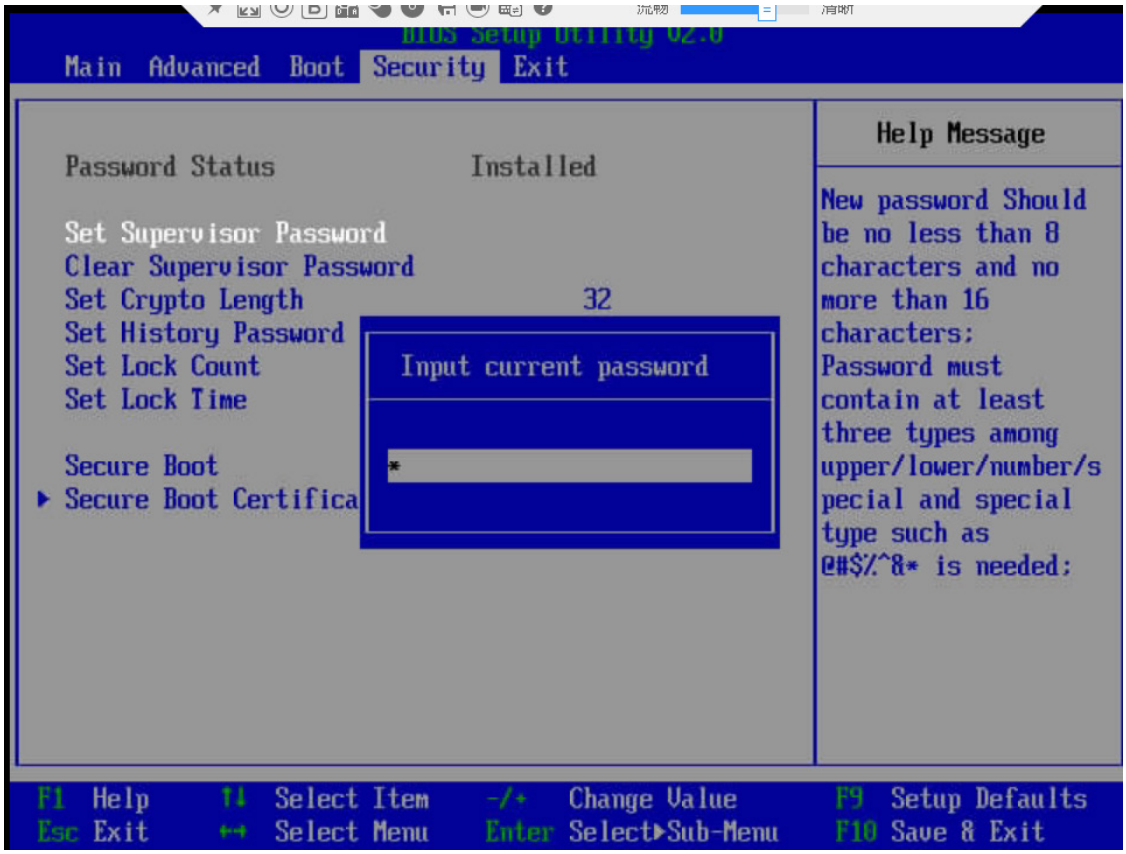
(2) 设置 BIOS ADMIN 密码

进入 BIOS 安全维护界面，设置管理员密码（administrator password）为 U1cloud@M00ve。

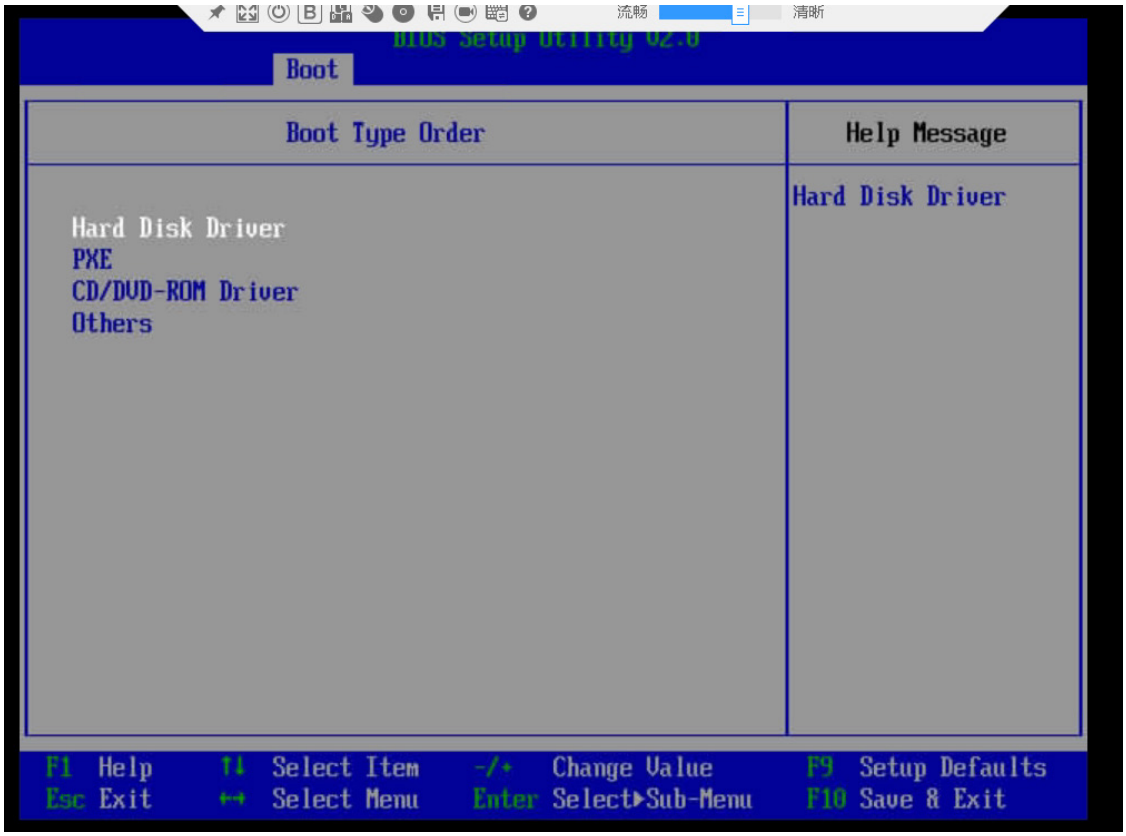
D.6 UniServer R4960 G3

D.6.1 设置服务器启动顺序

(1) 将 BIOS 管理员密码修改为 U1cloud@M00ve

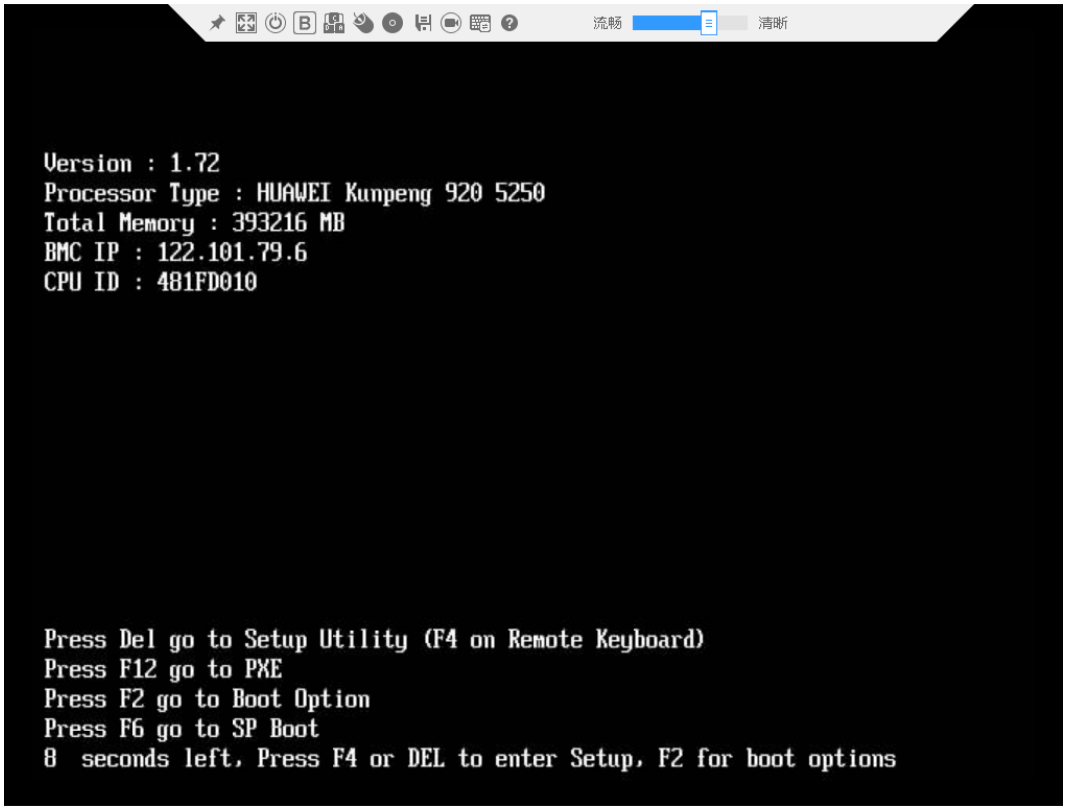


(2) 进入 BIOS 启动页面，在默认启动顺序设置中，设置启动顺序为第一优先级为硬盘，第二优先级为 PXE，F10 保存并退出。



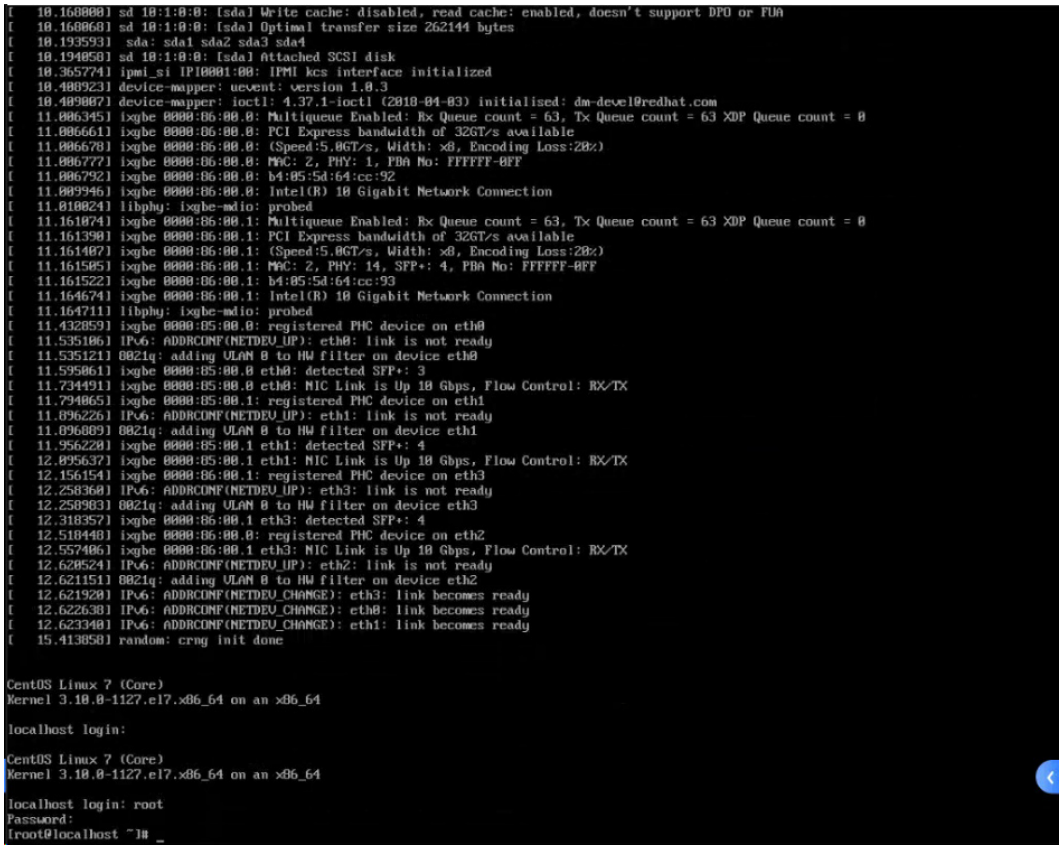
D.6.2 PXE 启动

(1) 按 F12，输入 BIOS 管理员密码。


流畅
清晰
Version : 1.72
Processor Type : HUAWEI Kunpeng 920 5250
Total Memory : 393216 MB
BMC IP : 122.101.79.6
CPU ID : 481FD010
Press Del go to Setup Utility (F4 on Remote Keyboard)
Press F12 go to PXE
Press F2 go to Boot Option
Press F6 go to SP Boot
8 seconds left, Press F4 or DEL to enter Setup, F2 for boot options

(2) 获取小镜像进入即可。


deploy
Use the ▲ and ▼ keys to change the selection.
Press 'e' to edit the selected item, or 'c' for a command prompt.
The selected entry will be started automatically in 1s.


[10.160808] sd 10:1:0:0: [sda] Write cache: disabled, read cache: enabled, doesn't support DPO or FUA
[10.160868] sd 10:1:0:0: [sda] Optimal transfer size 262144 bytes
[10.193593] sda: sda1 sda2 sda3 sda4
[10.194058] sd 10:1:0:0: [sda] Attached SCSI disk
[10.365774] ipmi_si IPI0001:00: IPMI kcs interface initialized
[10.480923] device-mapper: uevent: version 1.0.3
[10.489087] device-mapper: ioctl: 4.37.1-ioctl (2018-04-03) initialised: dm-devel@redhat.com
[11.006345] ixgbe 0000:86:00.0: Multiqueue Enabled: Rx Queue count = 63, Tx Queue count = 63 XDP Queue count = 0
[11.006661] ixgbe 0000:86:00.0: PCI Express bandwidth of 32GT/s available
[11.006678] ixgbe 0000:86:00.0: (Speed:5.0GT/s, Width: x8, Encoding Loss:20%)
[11.006777] ixgbe 0000:86:00.0: MAC: 2, PHY: 1, PBA No: FFFFFF-0FF
[11.006792] ixgbe 0000:86:00.0: b4:05:5d:64:cc:92
[11.009946] ixgbe 0000:86:00.0: Intel(R) 10 Gigabit Network Connection
[11.010024] libphy: ixgbe-mdio: probed
[11.161074] ixgbe 0000:86:00.1: Multiqueue Enabled: Rx Queue count = 63, Tx Queue count = 63 XDP Queue count = 0
[11.161390] ixgbe 0000:86:00.1: PCI Express bandwidth of 32GT/s available
[11.161407] ixgbe 0000:86:00.1: (Speed:5.0GT/s, Width: x8, Encoding Loss:20%)
[11.161505] ixgbe 0000:86:00.1: MAC: 2, PHY: 14, SFP+: 4, PBA No: FFFFFF-0FF
[11.161522] ixgbe 0000:86:00.1: b4:05:5d:64:cc:93
[11.164674] ixgbe 0000:86:00.1: Intel(R) 10 Gigabit Network Connection
[11.164711] libphy: ixgbe-mdio: probed
[11.432859] ixgbe 0000:05:00.0: registered PHC device on eth0
[11.535106] IPv6: ADDRCONF(NETDEV_UP): eth0: link is not ready
[11.535121] 8021q: adding VLAN 0 to HW filter on device eth0
[11.595061] ixgbe 0000:05:00.0 eth0: detected SFP+: 3
[11.734491] ixgbe 0000:05:00.0 eth0: NIC Link is Up 10 Gbps, Flow Control: RX/TX
[11.794065] ixgbe 0000:05:00.1: registered PHC device on eth1
[11.896226] IPv6: ADDRCONF(NETDEV_UP): eth1: link is not ready
[11.896089] 8021q: adding VLAN 0 to HW filter on device eth1
[11.956220] ixgbe 0000:05:00.1 eth1: detected SFP+: 4
[12.095637] ixgbe 0000:05:00.1 eth1: NIC Link is Up 10 Gbps, Flow Control: RX/TX
[12.156154] ixgbe 0000:86:00.1: registered PHC device on eth3
[12.258360] IPv6: ADDRCONF(NETDEV_UP): eth3: link is not ready
[12.258983] 8021q: adding VLAN 0 to HW filter on device eth3
[12.318357] ixgbe 0000:86:00.1 eth3: detected SFP+: 4
[12.518448] ixgbe 0000:86:00.0: registered PHC device on eth2
[12.557406] ixgbe 0000:86:00.1 eth3: NIC Link is Up 10 Gbps, Flow Control: RX/TX
[12.620524] IPv6: ADDRCONF(NETDEV_UP): eth2: link is not ready
[12.621151] 8021q: adding VLAN 0 to HW filter on device eth2
[12.621920] IPv6: ADDRCONF(NETDEV_CHANGE): eth3: link becomes ready
[12.622638] IPv6: ADDRCONF(NETDEV_CHANGE): eth0: link becomes ready
[12.623340] IPv6: ADDRCONF(NETDEV_CHANGE): eth1: link becomes ready
[15.413858] random: crng init done
CentOS Linux 7 (Core)
Kernel 3.10.0-1127.el7.x86_64 on an x86_64
localhost login:
CentOS Linux 7 (Core)
Kernel 3.10.0-1127.el7.x86_64 on an x86_64
localhost login: root
Password:
[root@localhost ~]# _

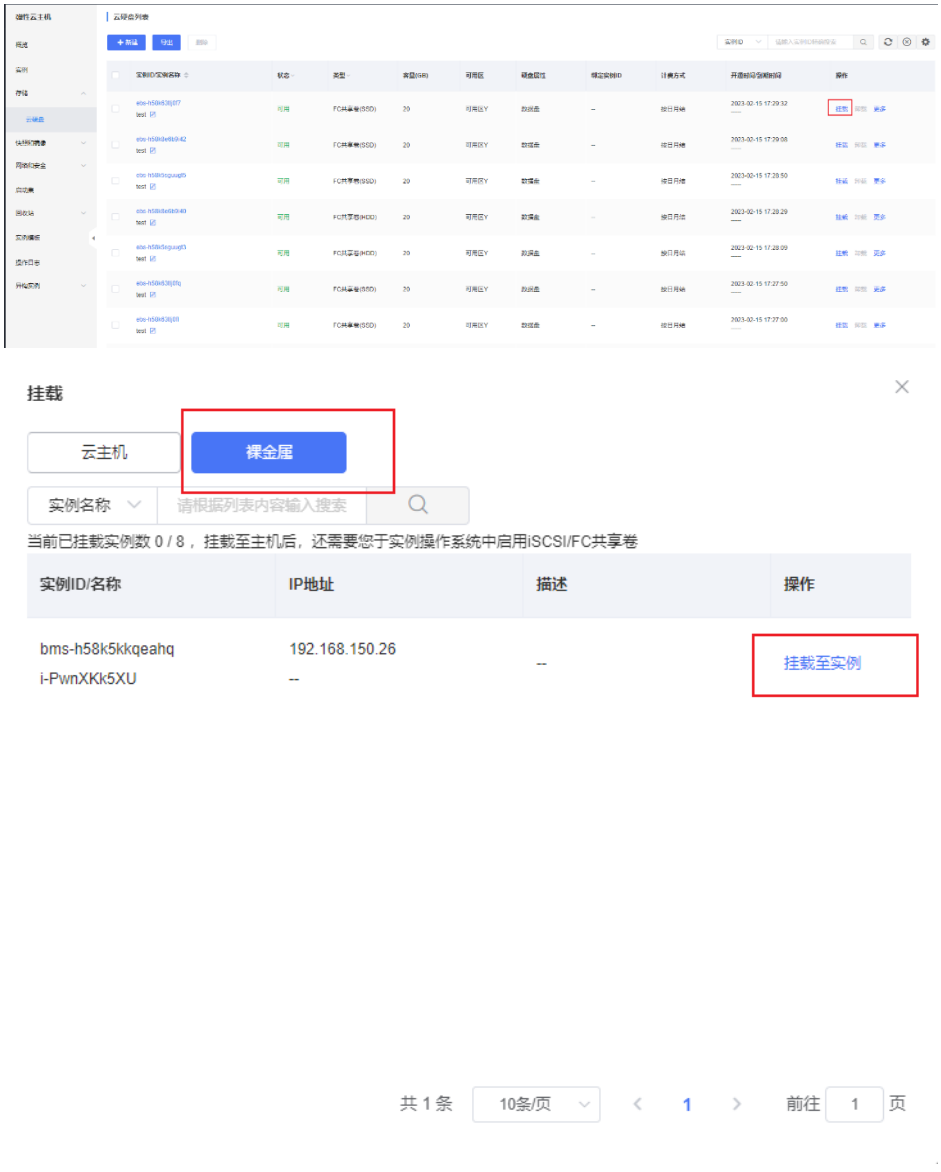
D.7 裸金属挂载FC共享卷

D.7.1 Linux 连接 FC 共享卷

(1) 登录用户控制台，给裸金属挂载共享卷。

- 从裸金属列表挂载共享卷。

- 或者从硬盘列表挂载共享卷。



(2) 安装共享卷访问需要的应用程序。

- RHEL / CentOS

```
yum install device-mapper-multipath -y
```

- Ubuntu

```
apt-get update
apt-get install multipath-tools -y
apt-get install open-iscsi -y
```

(3) 配置 multipath。Ubuntu 不需要执行该步骤。

- RHEL/CentOS：添加/etc/multipath.conf 文件。

```
defaults {
        polling_interval 10
        max_fds 8192
        user_friendly_names no
}
```

```
devices {
        device {
                vendor "3PARdata"
                product "VV"
                path_grouping_policy "group_by_prio"
                path_selector "round-robin 0"
                path_checker tur
                features "0"
                hardware_handler "1 alua"
                prio "alua"
                failback immediate
                rr_weight "uniform"
                no_path_retry 18
                rr_min_io_rq 1
                detect_prio yes
                fast_io_fail_tmo 10
                dev_loss_tmo "infinity"
        }
}

blacklist {
}
```

- Debian：添加/etc/multipath.conf 文件。

```
defaults {
        polling_interval 10
        max_fds 8192
        user_friendly_names no
        find_multipaths yes   # 需要添加这行配置
}


devices {
        device {
                vendor "3PARdata"
                product "VV"
                path_grouping_policy "group_by_prio"
                path_selector "round-robin 0"
                path_checker tur
                features "0"
                hardware_handler "1 alua"
                prio "alua"
                failback immediate
                rr_weight "uniform"
                no_path_retry 18
                rr_min_io_rq 1
                detect_prio yes
                fast_io_fail_tmo 10
                dev_loss_tmo "infinity"
```

```
        }
    }
```

(4) 启动相关服务。

- CentOS6

```
chkconfig multipathd on
# service multipathd start
```

- CentOS7/OpenSUSE

```
systemctl enable multipathd
systemctl start multipathd
```

- Ubuntu 14/16

```
# service multipath-tools start
```

(5) 在裸金属系统内查看 FC port 信息。ls /sys/class/fc*。获取目录中 target H:B:T

```
[root@BJ-COM-VKS-011 ~]# ls /sys/class/fc*
/sys/class/fc_host:
host25  host26

/sys/class/fc_remote_ports:
rport-25:0-0  rport-25:0-2  rport-26:0-2  rport-26:0-4  rport-26:0-56  rport-26:0-7
rport-25:0-1  rport-26:0-0  rport-26:0-3  rport-26:0-5  rport-26:0-6

/sys/class/fc_transport:
target25:0:0  target25:0:1  target26:0:0  target26:0:1

/sys/class/fc_vports:
```

(6) 查看 port 状态。Online：正常使用，Linkdown：未使用。确保所有 HBA 端口和存储端口在 VKS 上的链路至少一条状态正常。

```
[root@BJ-COM-VKS-011 ~]#  cat /sys/class/fc_host/host25/port_state
Online
[root@BJ-COM-VKS-011 ~]# cat /sys/class/fc_remote_ports/rport-25\:0-0/port_state
Online
```

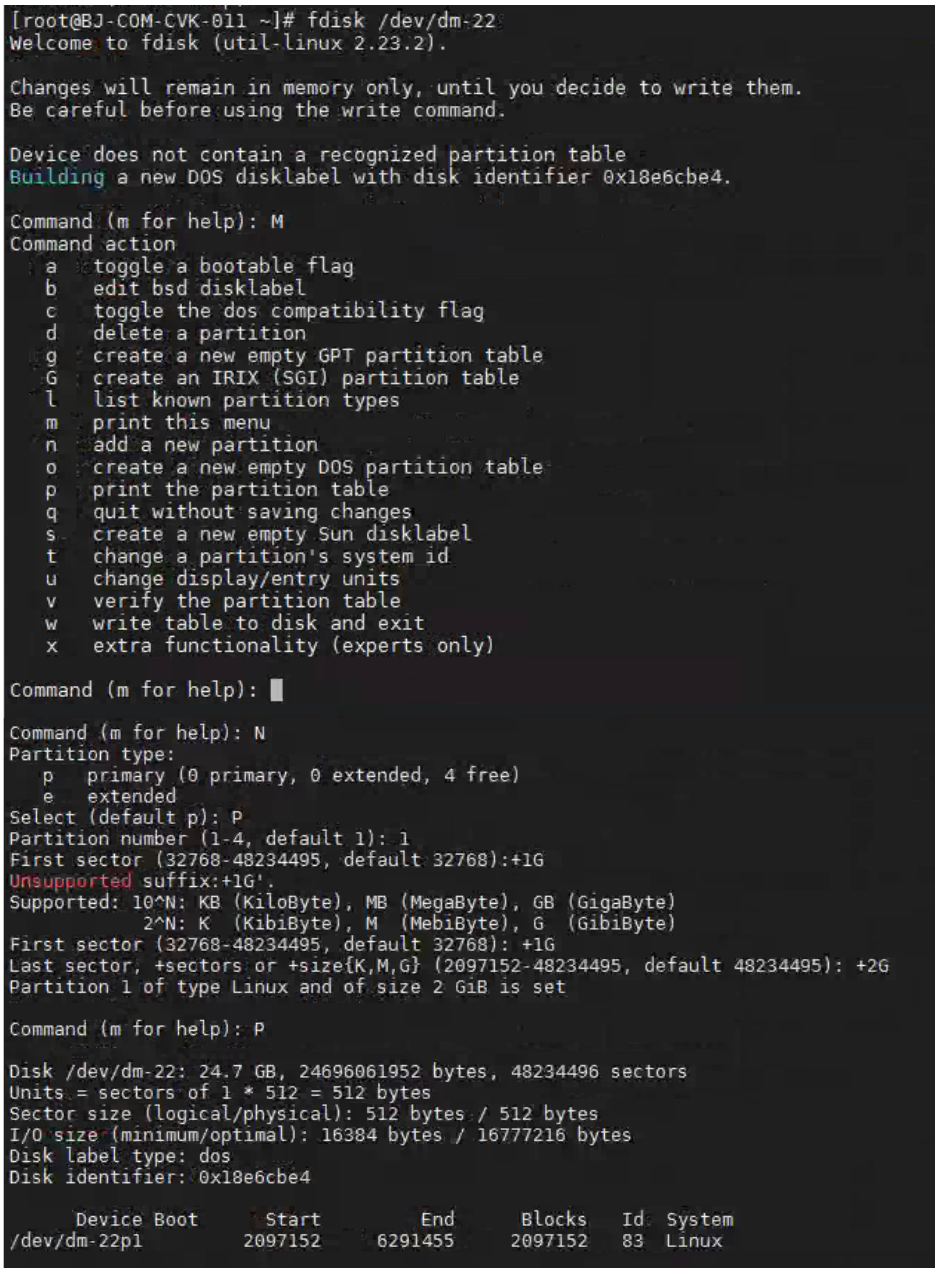
(7) 映射 lun 卷。根据当前裸金属已经分配的存储 target 信息，完成映射 lun 卷。echo "- - -" > /sys/class/scsi_host/host<H>/scan 查询到该 lun 卷的所有链路，组成一个多路径。

```
[root@BJ-COM-VKS-011 ~]#  echo "- - -" > /sys/class/scsi_host/host25/scan
[root@BJ-COM-VKS-011 ~]#  echo "- - -" > /sys/class/scsi_host/host26/scan
[root@BJ-COM-VKS-011 ~]# lsblk
```

(8) 查询 lun 的设备映射 dm。通过 3par FC 共享卷的 wwn，查询 dm。multipath -ll |grep "<wwn>"

```
# multipath -ll | grep "60002ac0000000000000149240001e39e"
360002ac0000000000000149240001e39e dm-22 3PARdata,VV
```

(9) 对共享卷进行分区，查询分区信息。分区后，新分区生成新的设备映射 dm-N，示例如下。



输入命令:partprobe,让系统读取分区信息

fdisk /dev/dm-22

[root@BJ-COM-VKS-011 ~]# ls /dev/mapper/360002ac0000000000000149240001e39e* -l

lrwxrwxrwx 1 root root 8 Feb 14 14:56 /dev/mapper/360002ac0000000000000149240001e39e -> ../dm-22

lrwxrwxrwx 1 root root 8 Feb 14 14:56 /dev/mapper/360002ac0000000000000149240001e39e-part1 -> ../dm-30

lrwxrwxrwx 1 root root 8 Feb 14 14:56 /dev/mapper/360002ac0000000000000149240001e39e-part2 -> ../dm-31

(10) 使用共享卷，通过格式化 multipath 多路径设备，实现对共享卷的使用。分区后不要格式化整个磁盘。格式化分区磁盘，并挂载给目录使用。# mount /dev/<dm-N>/挂载目录

mkfs.xfs /dev/dm-30

mount /dev/dm-30 /mnt

D.7.2 Linux 卸载 FC 共享卷

(1) 卸载共享卷。如果共享卷被挂载到本地文件目录，则先从系统内取消对共享卷的使用。

```
fuser -mv /mnt/
Kill -g pid
umount /dev/mapper/360002ac0000000000000149240001e39e-part1
```

(2) 删除多路径。

```
multipath -f /dev/dm-22
```

(3) 删除磁盘设备。echo 1 > /sys/class/scsi_device/<路径>/device/delete，示例如下：

```
echo 1 >  /sys/class/scsi_device/25:0:1:1234/device/delete
```

注:(路径查询:multipath -ll)

(4) 登录用户控制台卸载共享卷。

D.7.3 Linux 扩容 FC 共享卷

(1) 登录用户控制台，在控制台的硬盘列表中，扩容共享卷到指定大小。

(2) 在裸金属系统内扩容 FC 共享卷。

示例如下，扩展共享卷 360002ac0000000000000149240001e39e 到 40G。

```
[root@BJ-COM-VKS-011 ~]# lsblk |grep "60002ac0000000000000149240001e39e"
└─360002ac0000000000000149240001e39e          253:22   0    23G  0 mpath
  ├─360002ac0000000000000149240001e39e-part2 253:31   0     3G  0 part
  └─360002ac0000000000000149240001e39e-part1 253:30   0     2G  0 part  /mnt1
└─360002ac0000000000000149240001e39e          253:22   0    23G  0 mpath
  ├─360002ac0000000000000149240001e39e-part2 253:31   0     3G  0 part
  └─360002ac0000000000000149240001e39e-part1 253:30   0     2G  0 part  /mnt1
```

a. 选择共享卷的盘符设备。查询多路径对应盘符为 sdap/sdaq。

```
[root@BJ-COM-VKS-011 ~]#lsblk
```

b. 刷新盘符以及多路径设备到最新的容量

```
[root@BJ-COM-VKS-011 ~]# echo 1 >  /sys/block/sdap/device/rescan
[root@BJ-COM-VKS-011 ~]# echo 1 >  /sys/block/sdaq/device/rescan
[root@BJ-COM-VKS-011 ~]# multipathd resize map /dev/dm-22
ok
```

c. 完成该步骤后，FC 共享卷扩容成功。

```
[root@BJ-COM-VKS-011 ~]# lsblk |grep "60002ac0000000000000149240001e39e"
└─360002ac0000000000000149240001e39e         253:22   0    40G  0 mpath
  ├─360002ac0000000000000149240001e39e-part2 253:31   0     3G  0 part
  └─360002ac0000000000000149240001e39e-part1 253:30   0     2G  0 part  /mnt1
└─360002ac0000000000000149240001e39e         253:22   0    40G  0 mpath
  ├─360002ac0000000000000149240001e39e-part2 253:31   0     3G  0 part
  └─360002ac0000000000000149240001e39e-part1 253:30   0     2G  0 part  /mnt1
```

如 ext4 文件使用 resize2fs，xfs 文件系统使用 xfs_growfs，另外可指定扩展的具体大小，具体用法这里不对细节描述。

如下示例为将扩展的部分完全分配给多路径设备。

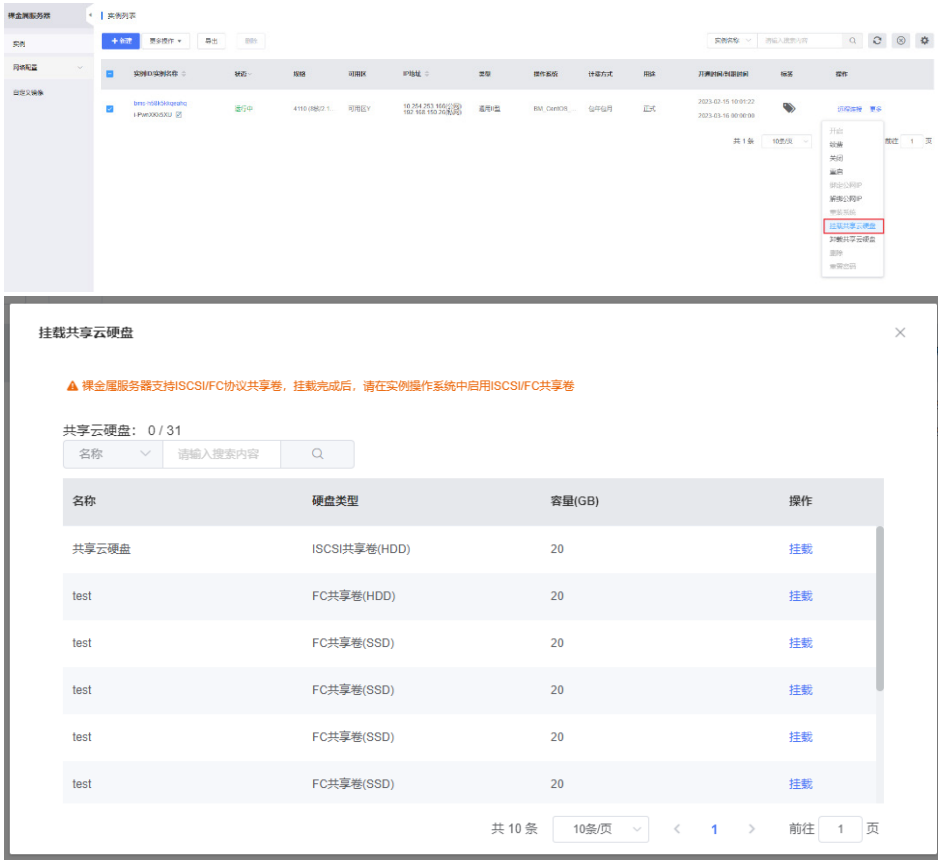
```
root@i-CBO9ePVtHP:~# resize2fs /dev/mapper/360002ac0000000000000154400022fc7
resize2fs 1.42.13 (17-May-2015)
Filesystem at /dev/mapper/360002ac0000000000000154400022fc7 is mounted on /mnt;
on-line resizing required
old_desc_blocks = 2, new_desc_blocks = 3
The filesystem on /dev/mapper/360002ac0000000000000154400022fc7 is now 10485760 (4k)
blocks long.
```

D.7.4 Windows 连接 FC 共享卷

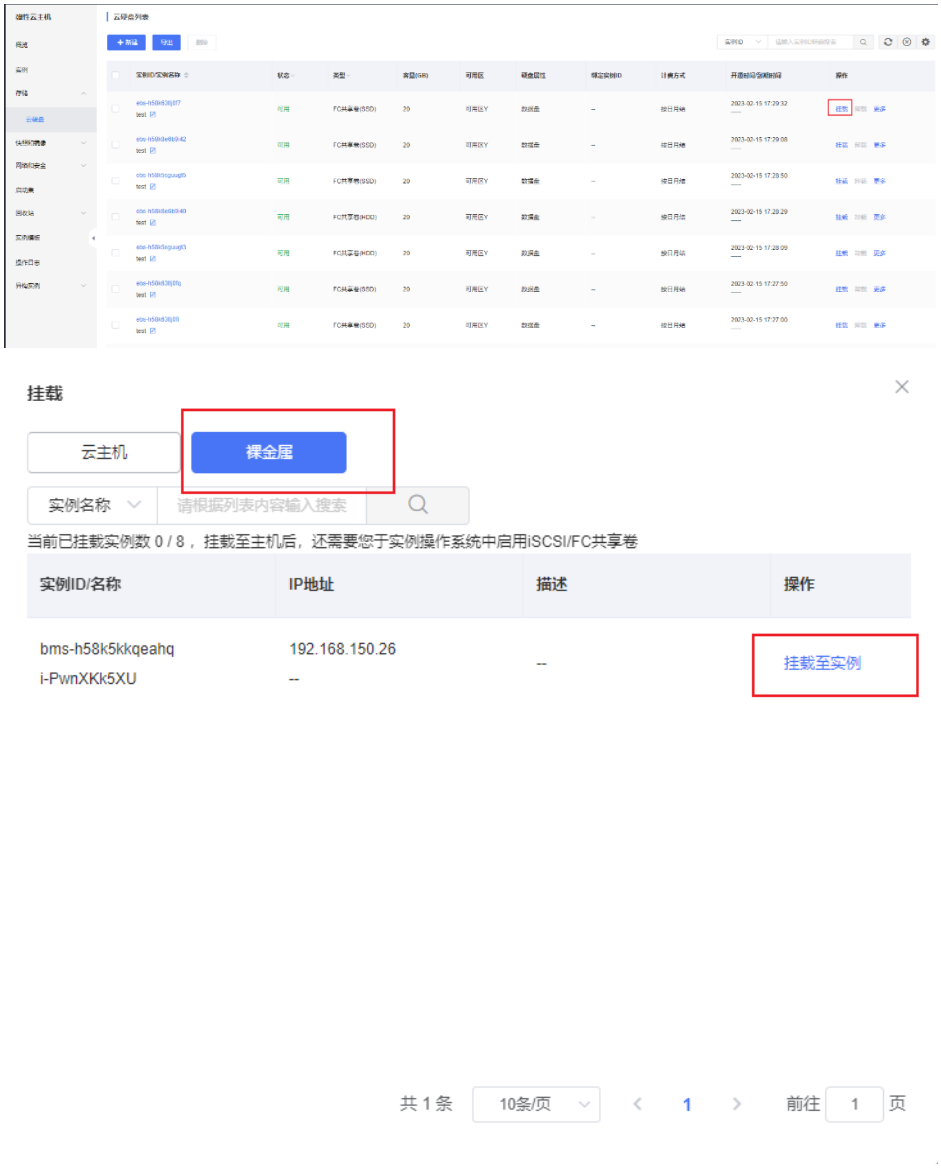
示例中使用的是 Windows Server 2018 Standard 操作系统。

(1) 登录用户控制台，给裸金属挂载共享卷。

- 从裸金属列表挂载共享卷。

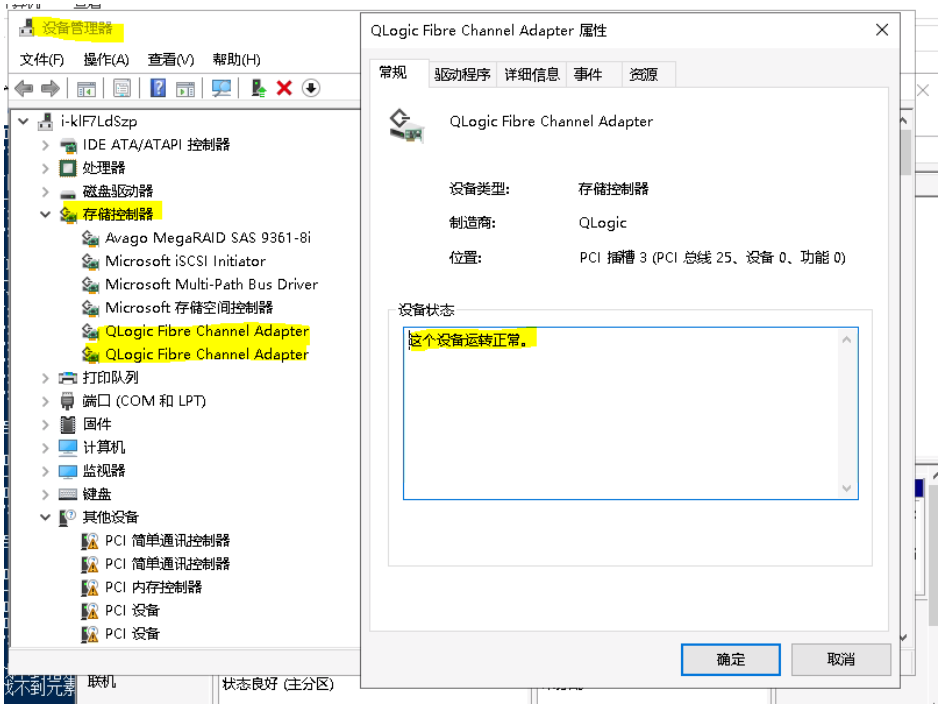


- 或者从硬盘列表挂载共享卷。



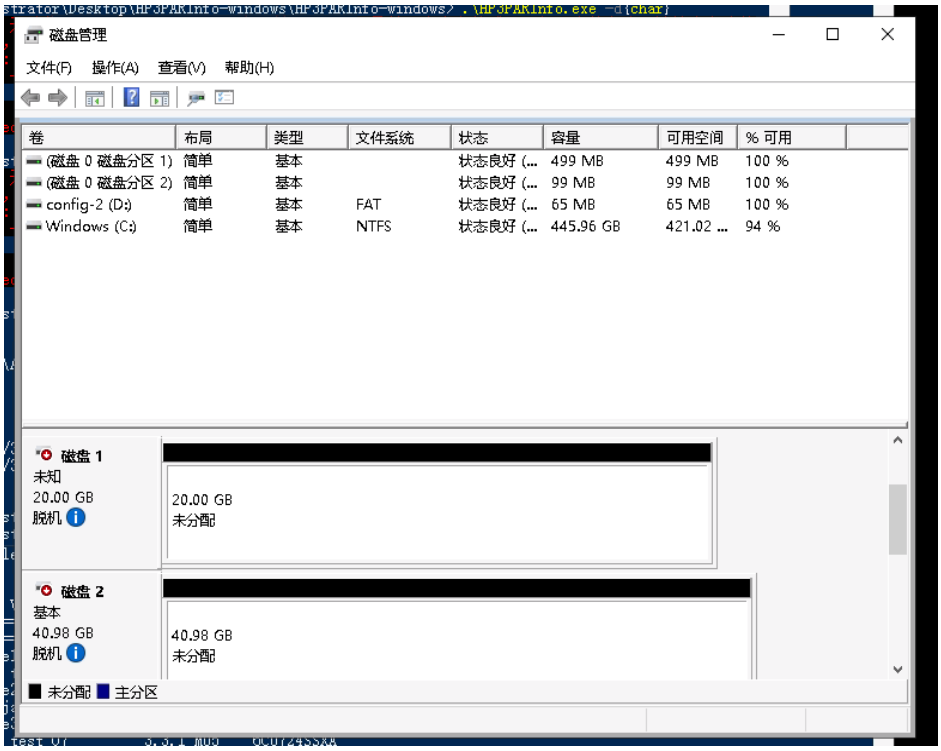
(2) 确认 HBA 卡状态。

windows 在【设备管理器】--->【存储控制器】，找到 FC 设备，确保设备运转正常。

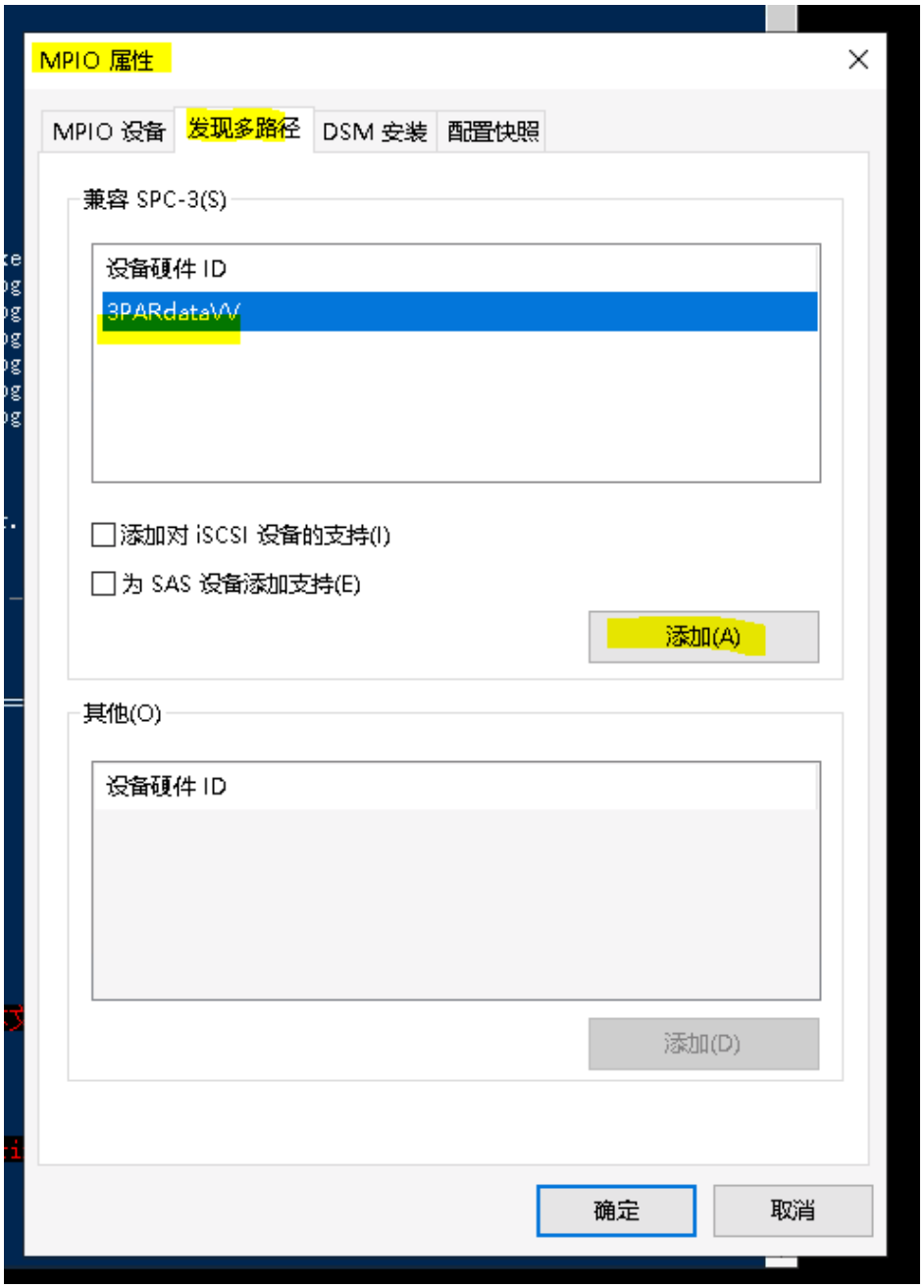


(3) 安装多路径 I/O。打开【服务器管理器】--->【仪表板】--->【添加角色和功能】，下一步到【功能】中找到【多路径 I/O】点击安装。重启服务器。

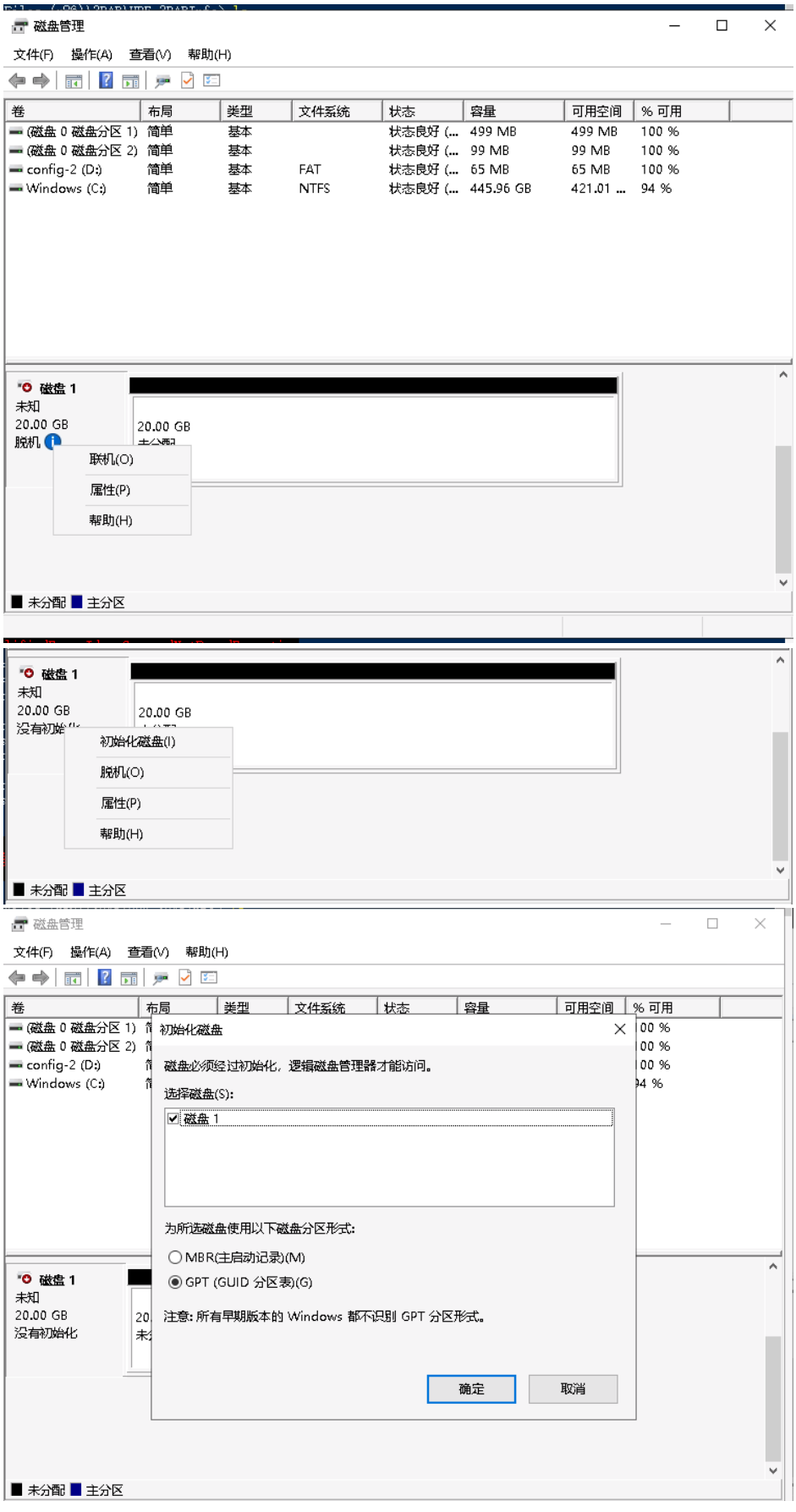
完成后，在磁盘管理中【操作】--->【重新扫描】，出现脱机的磁盘。注:进入磁盘管理 1、 win+r 2、 diskmgmt.msc

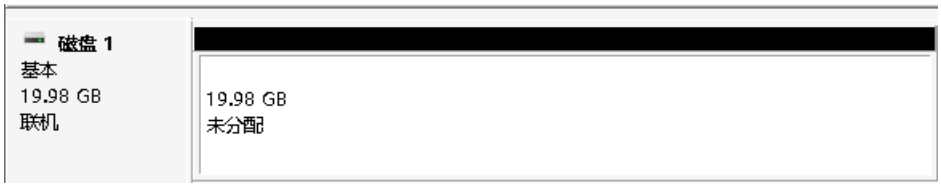


(4) 配置 MPIO 程序。启动【服务器管理器】，选择右上角【工具】--->【MPIO】-→【发现多路径】-→【3PARdataVV】,点击添加。

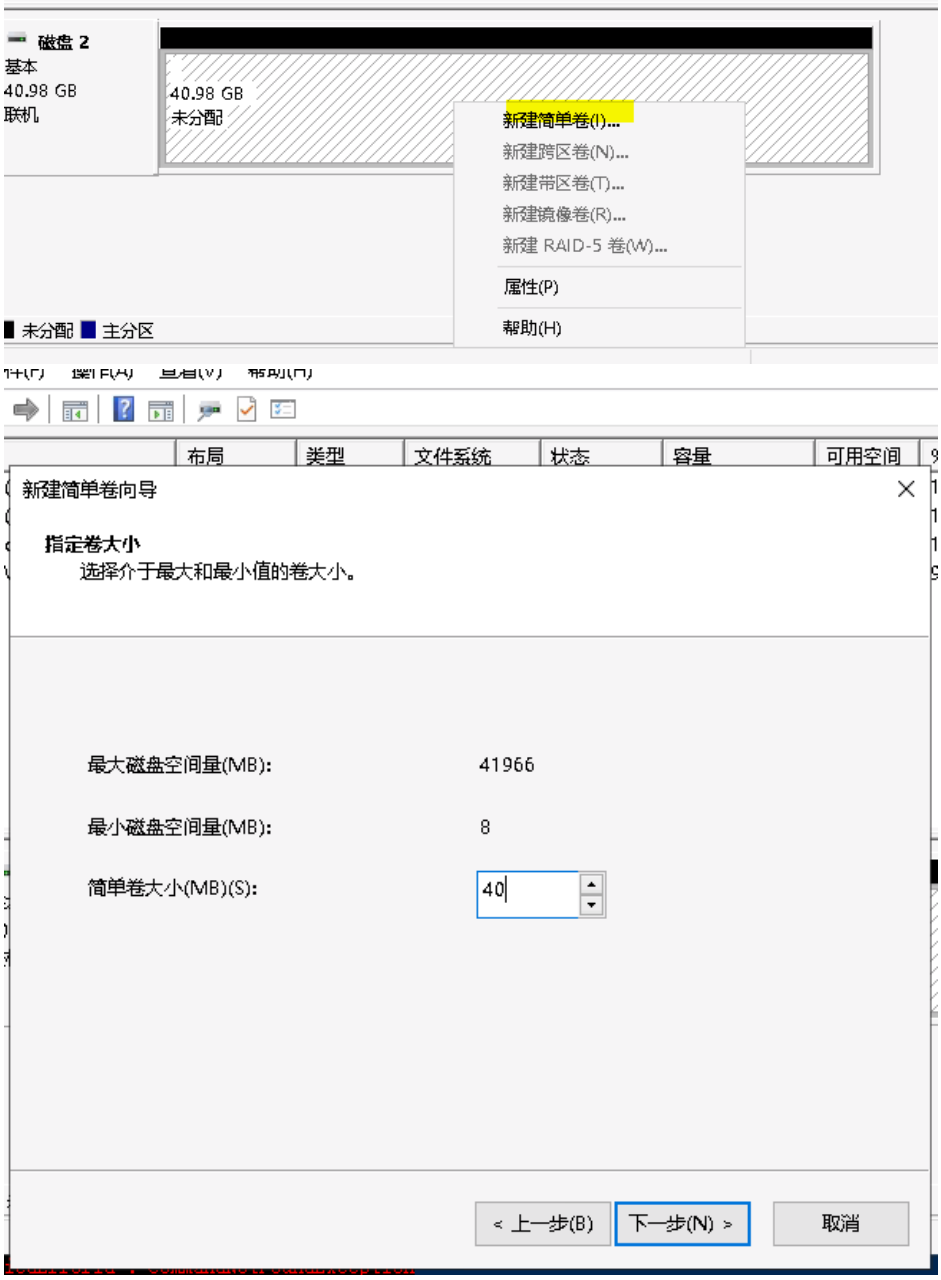


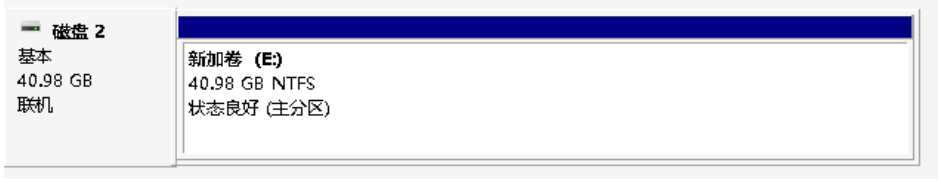
(5) 初始化磁盘。在磁盘管理中，右键点击脱机旁蓝色圆圈，选择【联机】，磁盘状态变为没有初始化。右击，选择【初始化磁盘】，弹窗点击【确认】，磁盘状态变为联机，初始化完成。


磁盘管理
文件(F) 操作(A) 查看(V) 帮助(H)
卷 布局 类型 文件系统 状态 容量 可用空间 % 可用
(磁盘 0 磁盘分区 1) 简单 基本 状态良好 (... 499 MB 499 MB 100 %
(磁盘 0 磁盘分区 2) 简单 基本 状态良好 (... 99 MB 99 MB 100 %
config-2 (D:) 简单 基本 FAT 状态良好 (... 65 MB 65 MB 100 %
Windows (C:) 简单 基本 NTFS 状态良好 (... 445.96 GB 421.01 ... 94 %
磁盘 1
未知
20.00 GB
脱机
20.00 GB
联机(O)
属性(P)
帮助(H)
未分配 主分区
磁盘 1
未知
20.00 GB
没有初始化
20.00 GB
初始化磁盘(I)
脱机(O)
属性(P)
帮助(H)
未分配 主分区
磁盘管理
文件(F) 操作(A) 查看(V) 帮助(H)
初始化磁盘
磁盘必须经过初始化，逻辑磁盘管理器才能访问。
选择磁盘(S):
磁盘 1
为所选磁盘使用以下磁盘分区形式:
MBR(主启动记录)(M)
GPT (GUID 分区表)(G)
注意: 所有早期版本的 Windows 都不识别 GPT 分区形式。
确定
取消
磁盘 1
未知
20.00 GB
没有初始化
未分配 主分区



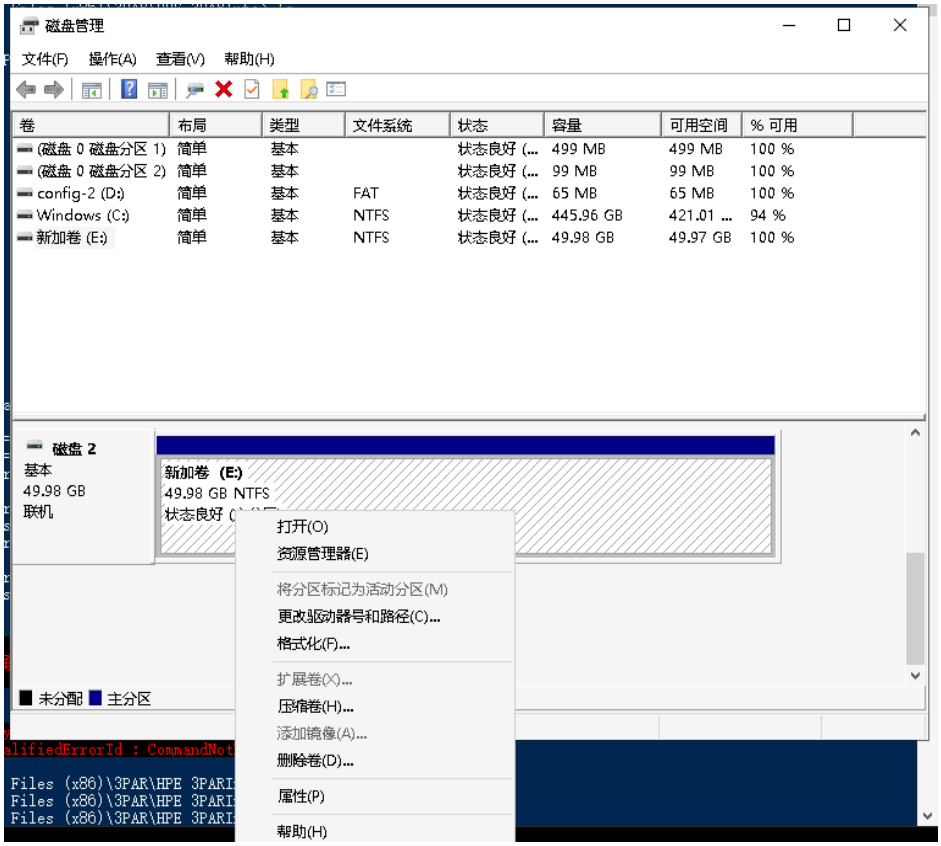
(6) 在磁盘内存区域右键，选择【新建简单卷】。弹窗中点击下一步，选择分配给新卷的内存，创建。





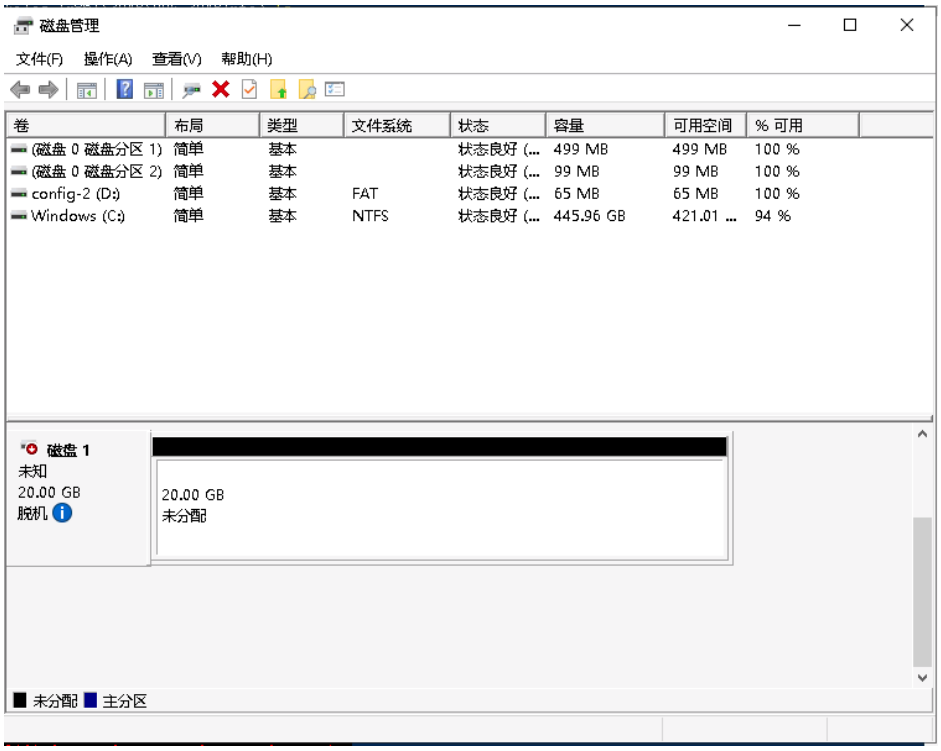
D.7.5 Windows 卸载 FC 共享卷

(1) 在磁盘管理中删除新加卷。在新加卷（E）中，右击。选择删除卷。



(2) 在控制台卸载共享卷；

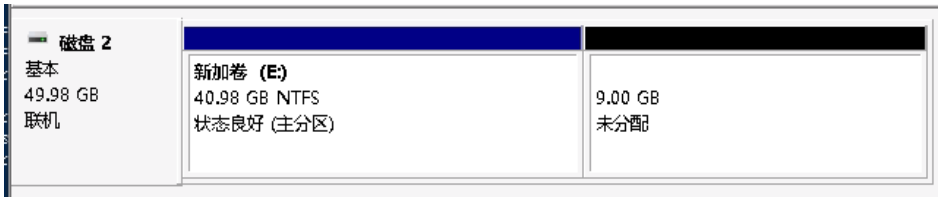
(3) 在磁盘管理中【操作】--->【重新扫描】，磁盘 2 已经被卸载。



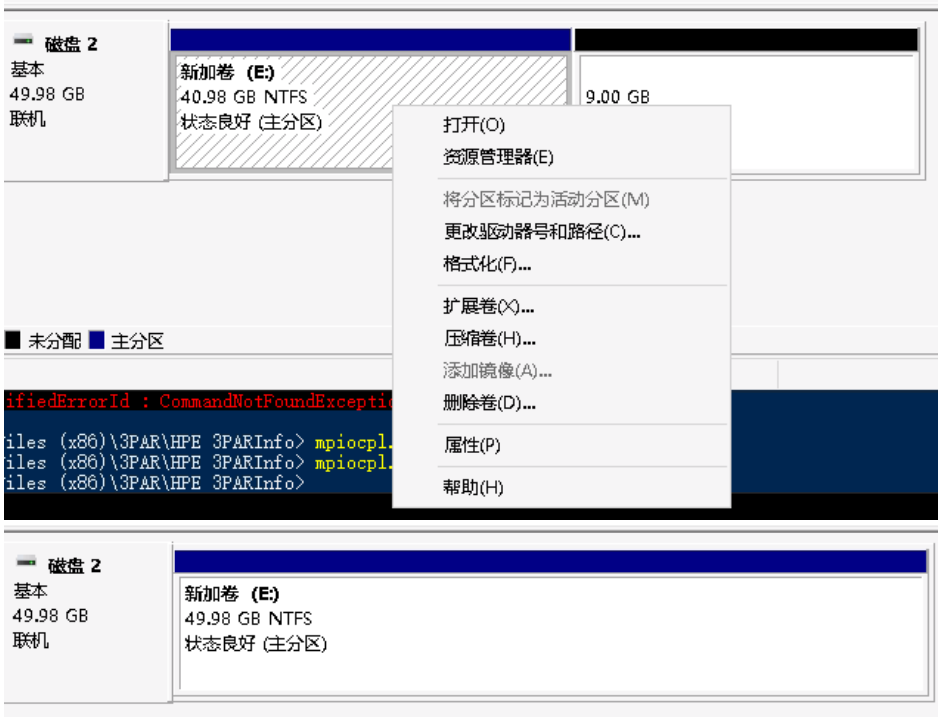
D.7.6 Windows 扩容 FC 共享卷

(1) 在控制台的硬盘列表中，扩容共享卷到指定大小。

(2) 在磁盘管理中【操作】--->【重新扫描】，磁盘容量增大，出现未分配区域。



(3) 在新加卷（E）中，右击。选择扩展卷，将未分配内存，按需求分配给新加卷（E）。



附录E 授权服务器部署

E.1 WAF授权服务器部署

E.1.1 硬件规格

WAF 授权管理系统的硬件服务器规格如表 E-1 所示。

表E-1 虚拟 web 应用防火墙授权管理系统硬件规格（仅支持在 CAS 平台下安装）

客户端个数	CPU	内存	硬盘
0-50	CPU类型：不限制cpu类型，确保分配4核	至少1G	至少25G
50-100		至少2G	至少 40G
100-150		至少2G	至少50G
150-200		至少4G	至少64G
大于200	暂不支持超过200个客户端		
安装包	SecPath W2000-VG2&SysScan&WG-LicenseServer-E6202-x86.iso		

E.1.2 CAS 平台安装虚拟 web 应用防火墙授权管理系统

(1) 上传镜像包。点击存储，选择目录，点击上传文件。

图E-1 上传镜像包

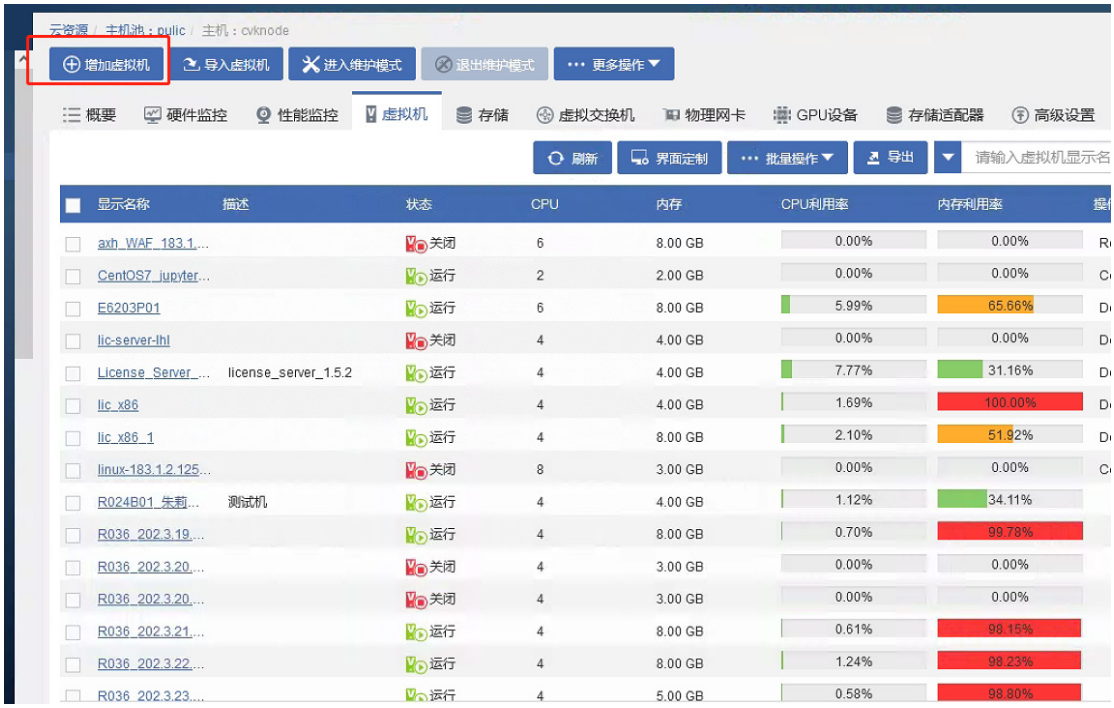
(2) 选择镜像包后，点击开始上传。

图E-2 选择镜像包

图E-3 查看上传的镜像包

(3) 点击增加虚拟机。

图E-4 增加虚拟机



(4) 设置虚拟机的显示名称，操作系统选择 Linux，版本选择 DebianGUN/Linux9(64 位)，CAStools 自动升级选择否。

图E-5 虚拟机基本配置

(5) 选择磁盘的总线类型为 IDE 硬盘，也可选择默认的高速磁盘。

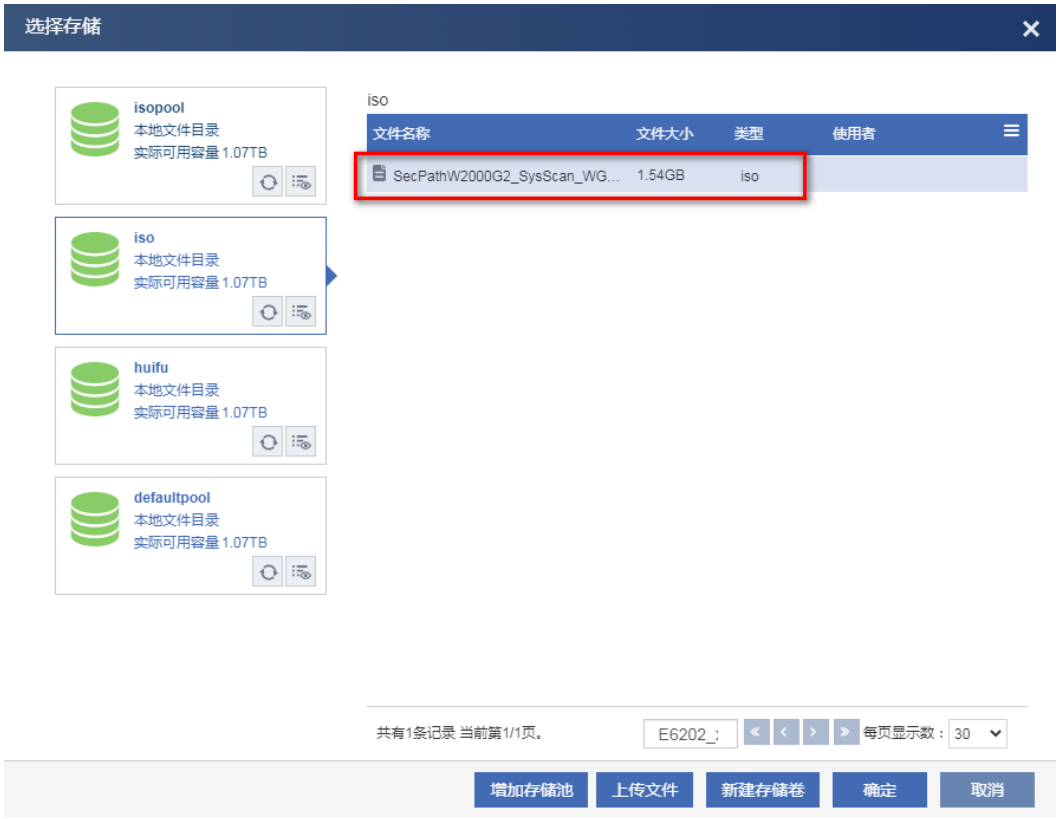
图E-6 设置磁盘的总线类型

(6) 选择光驱，点击光驱右侧的搜索。

图E-7 设置光驱

(7) 在文件目录中，选择镜像包，点击确定。

图E-8 选择镜像包



(8) 配置完成后，确认无误，点击完成。

图E-9 配置完成

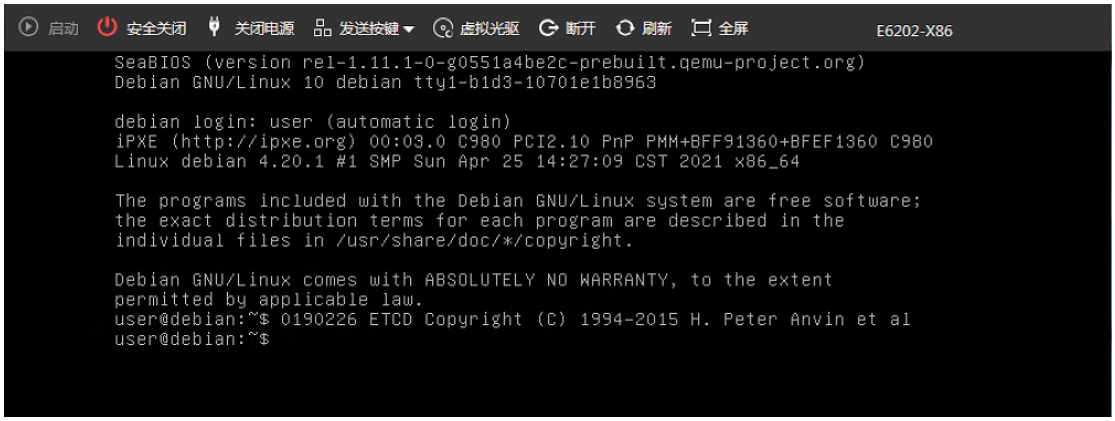
(9) 选择创建的虚拟机，点击启动。

图E-10 启动虚拟机

(10) 点击控制台，进行安装。

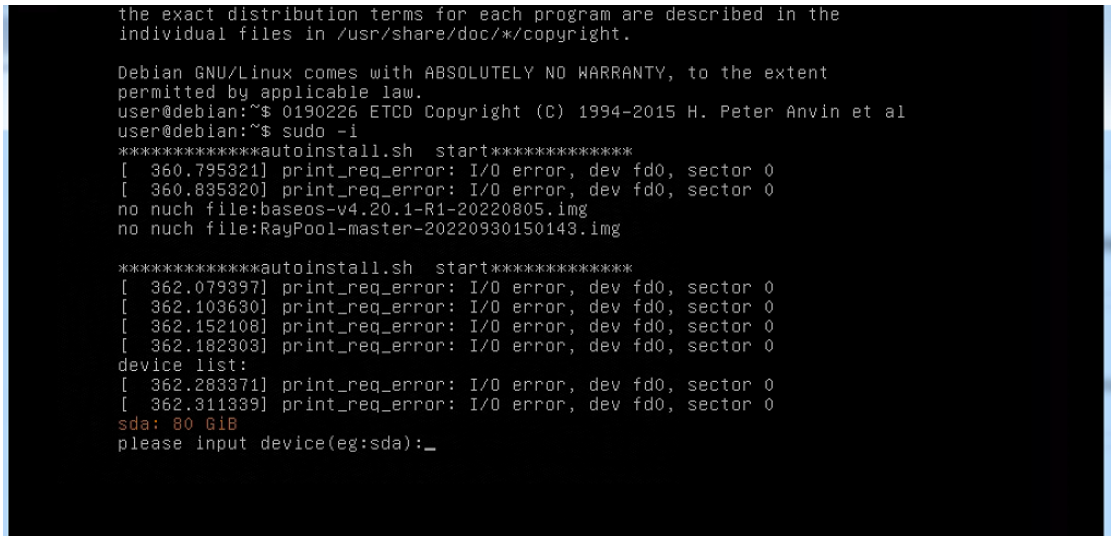
图E-11 打开控制台

(11) 系统会自动登录 user，手动输入 sudo su 即可调起 autoinstall.sh 安装程序。



注意：

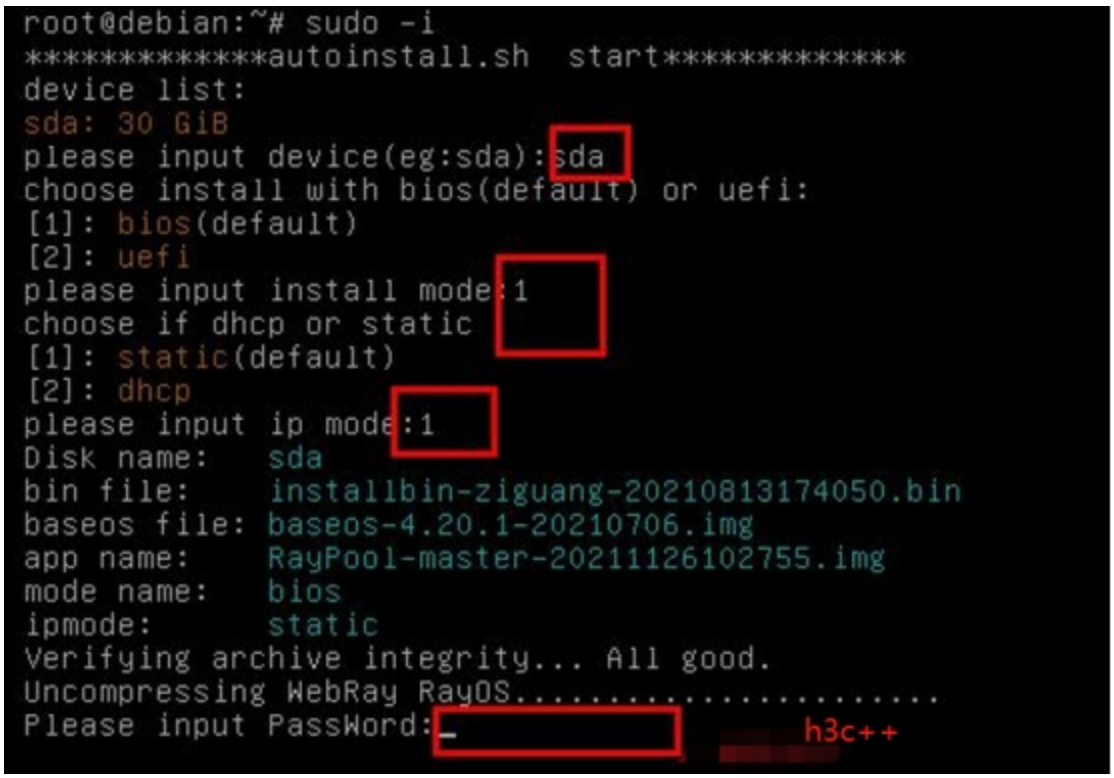
由于磁盘名为 vda 的情况较多，故自动化安装默认选择 vda，若 Disk name 是 sda 而非 vda 时，系统会提示



此时需要手动安装，即需要手动输入下述内容：

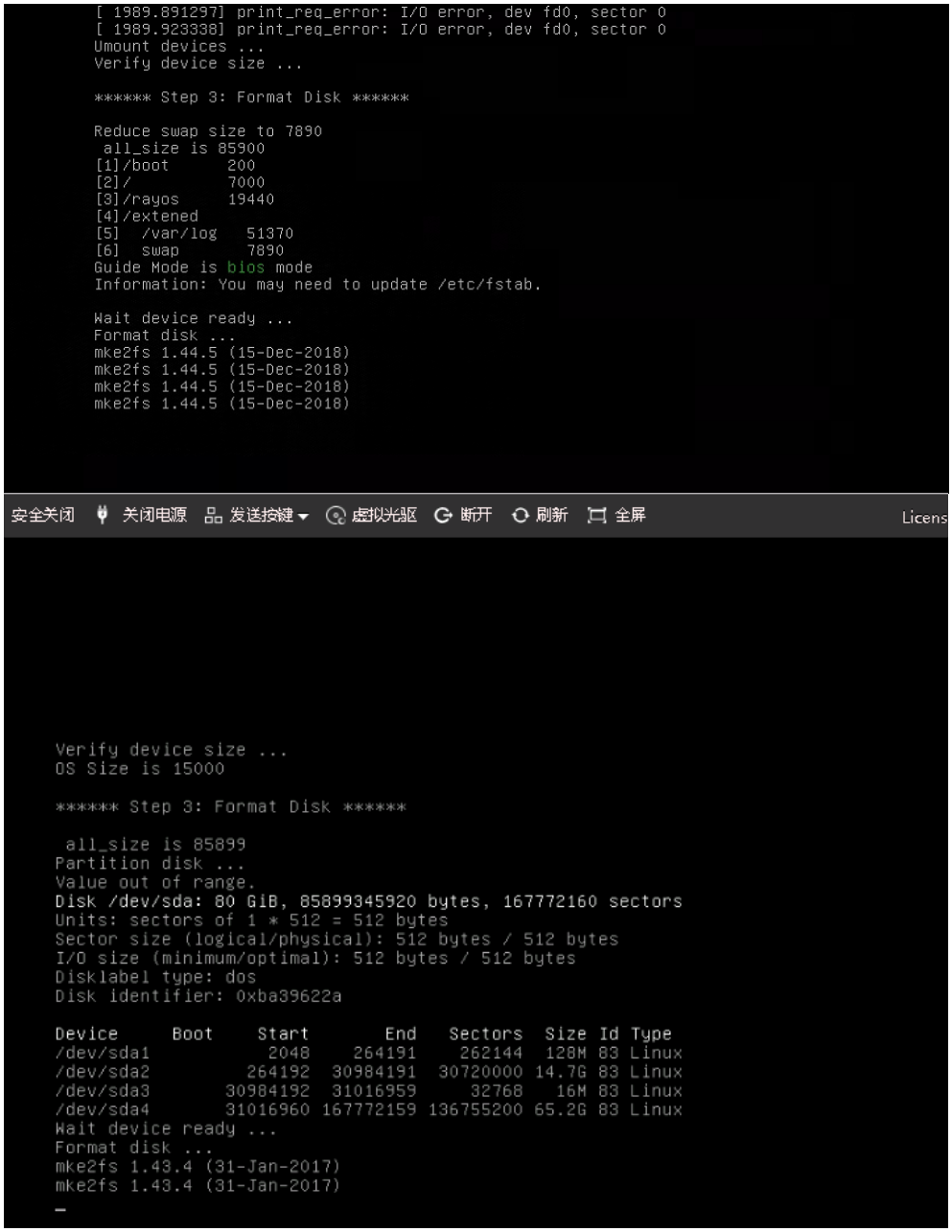
输入 sda，输入 1 选择 bios 模式，输入 1 选择 static 模式，输入刻盘密码：h3c++ 输入 y 继续。

图E-12 输入刻盘密码



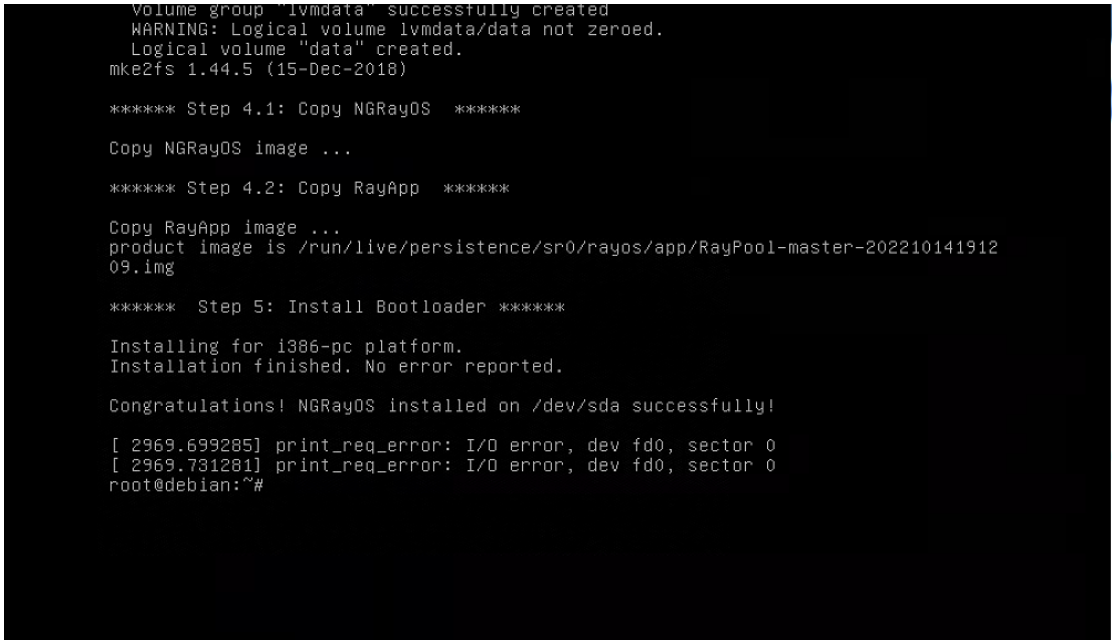
(12) 系统开始安装，一共五步，不需要手动参与，大概需要三到五分钟。

图E-13 开始安装



(13) 安装完成之后，出现提示“Congratulations! NGRayOS installed on /dev/sda successfully!”，按回车键，系统将自动重启。

图E-14 安装完成



(14) 输入 reboot 重启后进行刻盘。

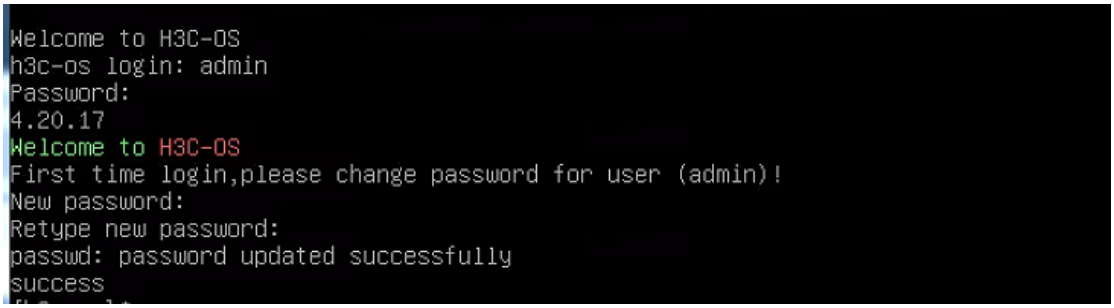
图E-15 重启系统

(15) 请耐心等待，刻盘结束后，会自动关闭机器，需要在 CAS 平台手动启动。此过程大约 10 分钟，请耐心等待。

图E-16 手动启动授权管理系统

(16) 在控制台下使用账号密码 admin/admin 登录系统，登陆成功后需要修改密码。

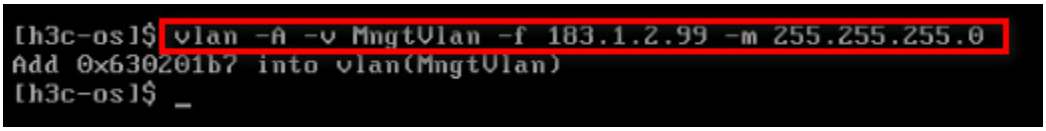
图E-17 登录成功



(17) 根据 CAS 平台的实际网络配置，来配置授权管理系统的管理 IP 地址。命令如下：

```
vlan –A –v MngtVlan –f 183.1.2.99 –m 255.255.255.0
## 请根据实际组网情况合理配置管理地址
```

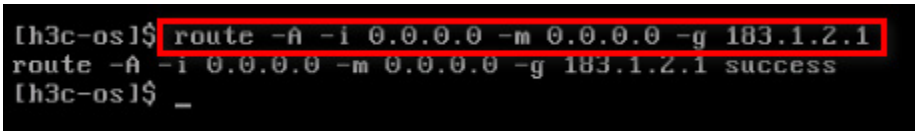
图E-18 配置 ip 地址



(18) 配置默认路由，命令如下：

```
route –A –i 0.0.0.0 –m 0.0.0.0 –g 183.1.2.1
## 请根据实际组网情况合理配置路由
```

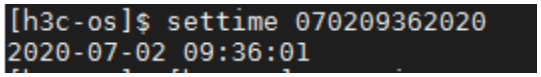
图E-19 添加默认路由



(19) 配置系统时间，命令如下：

```
settime 070209362020
##说明 settime 格式，settime 月日时分年
```

图E-20 添加系统时间



(20) 如果命令输入错误，导致 IP 或者路由配置错误，可以通过命令修改，查询 vlan 和 route 的命令格式，只需要输入 vlan 或者 route 即可。

图E-21 vlan 命令帮助

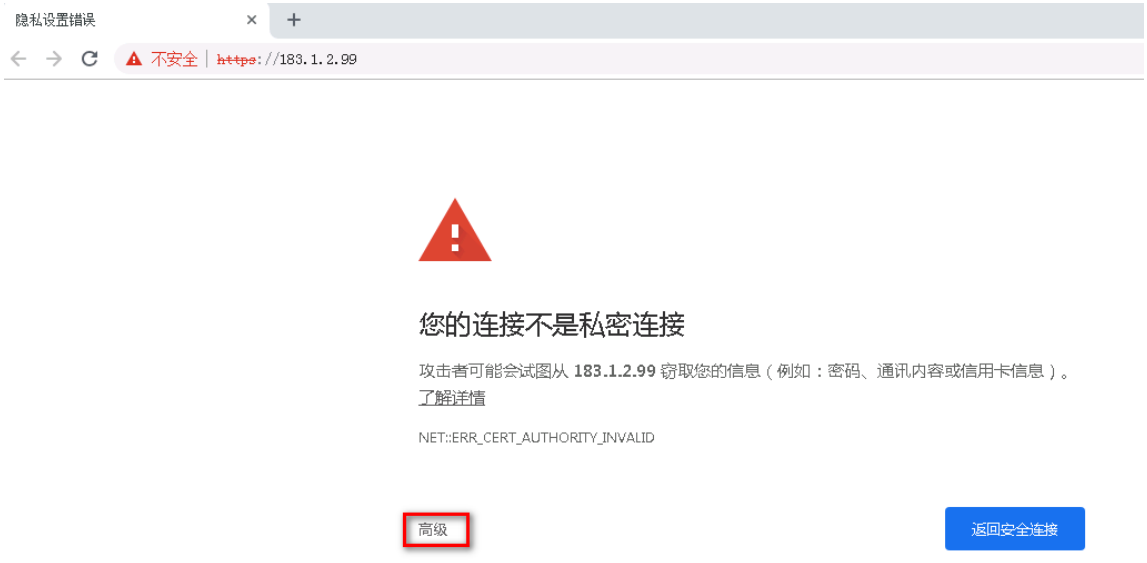
```
[h3c-os]$ vlan
none cmd is set!
vlan usage:
        vlan -C/--create -i/--vid <vlanid>(2-4094) [-v/--vname <vlanname>(def na
me: vlan$vid)] -d/--mode <0-traditional|1-transparent|2-passthrough>
        vlan -D/--delete -v/--vname <vlanname>
        vlan -E/--enable -v/--vname <vlanname>
        vlan -N/--disable -v/--vname <vlanname>
        vlan -A/--add -v/--vname <vlanname> -f/--ip <ipv4> -m/--mask <mask>
        vlan -R/--remove -v/--vname <vlanname> -f/--ip <ipv4>
        vlan -L/--link -v/--vname <channelname> -g/--group <portname/channelname
>
        vlan -U/--unlink -v/--vname <vlanname> -g/--group <portname/channelname>
        vlan -M/--modify -v/--vname <vlanname>  <-t/--mtu <mtu>>
        vlan -S/--show
[h3c-os]$ _
```

图E-22 route 命令帮助

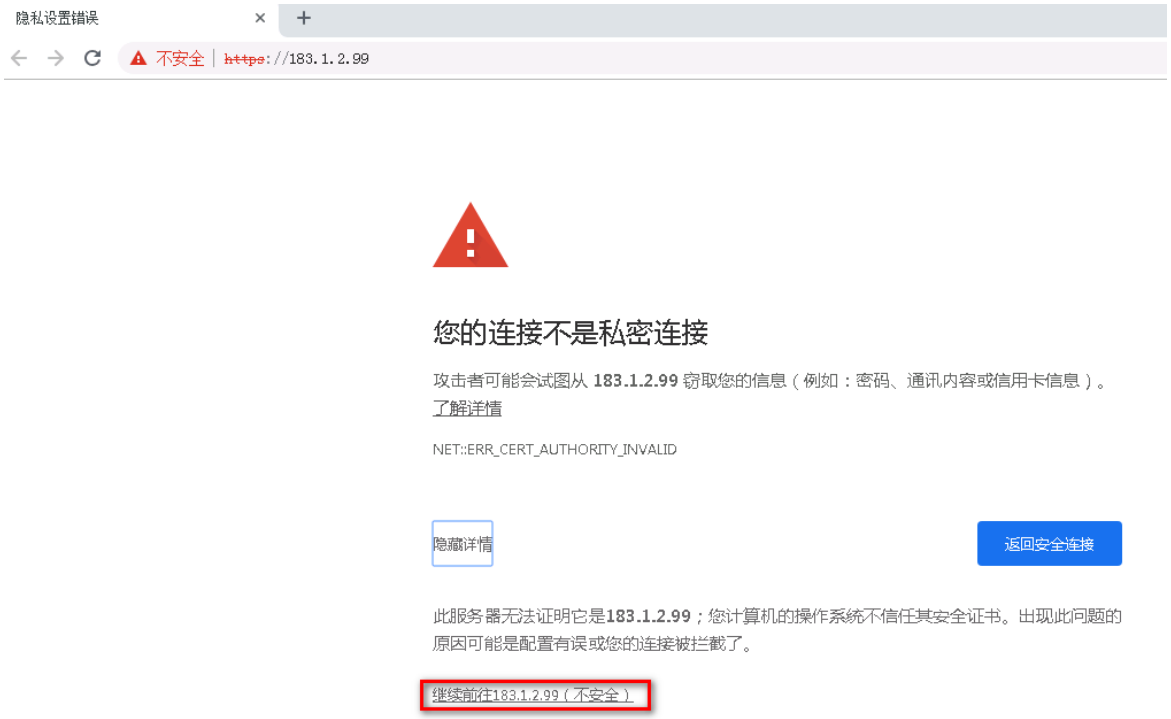
```
[h3c-os]$ route
none cmd is set!
route usage:
        route -A/--add -i/--ip {ip} -m/--mask {mask} <[-g/--gateway {gateway}] [
-n/--interface {interface}]> [-t {metric}]
        route -D/--del -i/--ip {ip} -m/--mask {mask} [-g/--gateway {gateway}] [-
n/--interface {interface}] [-t {metric}]
        route -S/--show
[h3c-os]$
```

(21) 使用浏览器（以 Chrome 为例）访问虚拟 WAF 授权管理系统，管理地址为 https://183.1.2.99，点击高级，选择继续前往。

图E-23 访问登录页面



图E-24 访问登录页面



(22) 输入账号密码 admin/admin 登录授权管理系统。

图E-25 登录页面

(23) 进入授权管理系统之后，需要导入授权方可使用。

E.2 堡垒机授权服务器部署

E.2.1 版本配置要求

运行环境要求

CPU	内存	硬盘
至少单颗2核	至少4G	至少300G

E.2.2 安装步骤

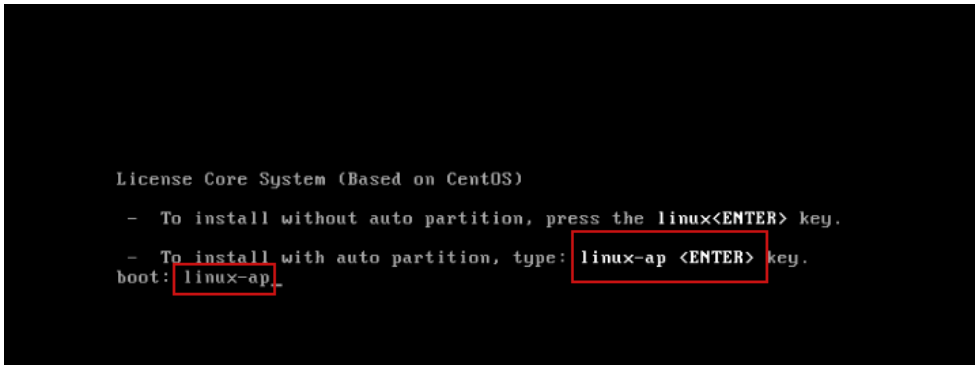
授权服务器是一个 Linux 安装包，安装包大约 900M，可以直接安装虚拟机上，一般默认的虚拟机配置都可以满足性能要求。

安装过程如下：

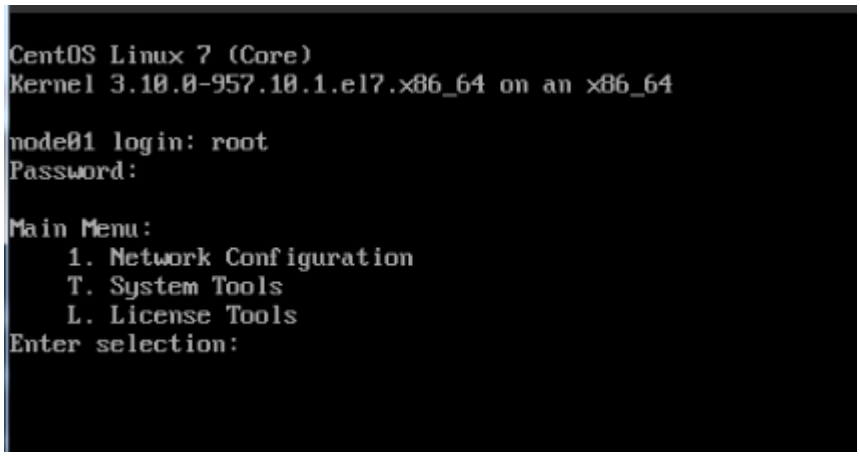
(1) 新建虚机。

(2) 一直“下一步”，直到创建虚拟机结束。

(3) 打开虚拟机电源，打开虚拟机控制台进行系统安装，根据提示一直安装下去。

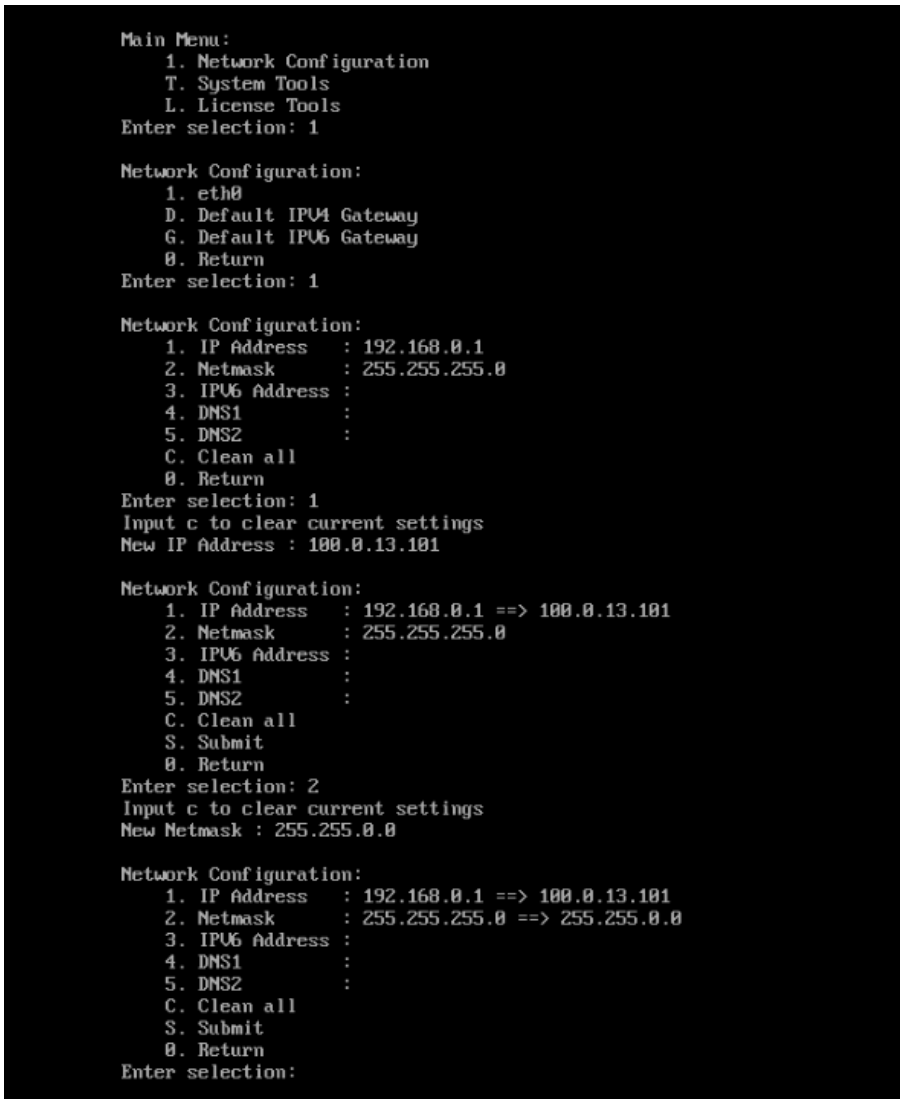


(4) 安装成功后界面如下：登录名和密码默认：root/admin

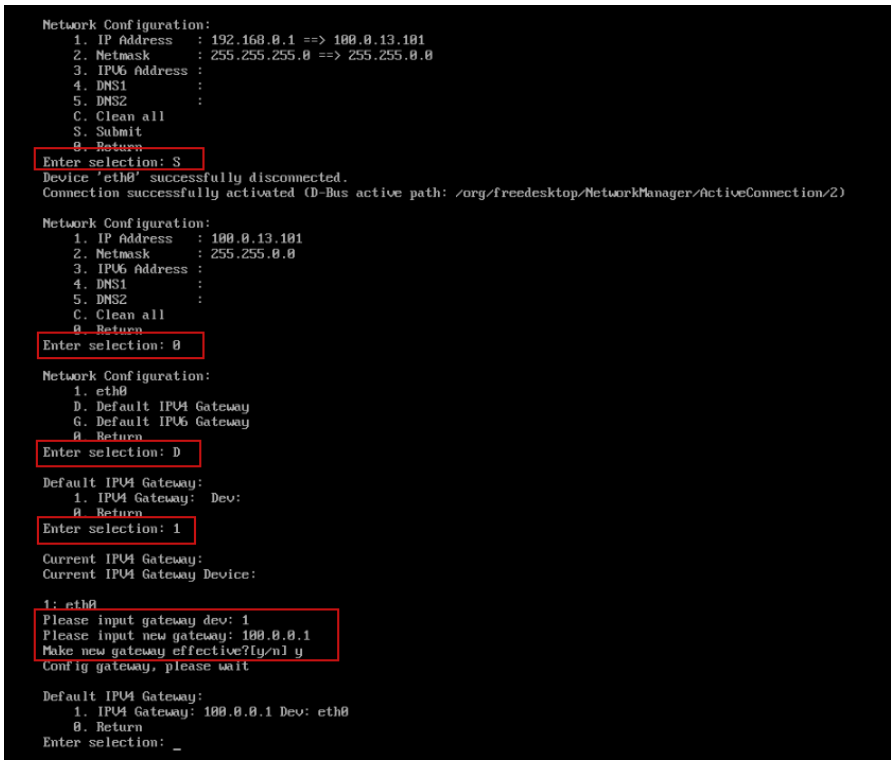


(5) 配置 IP 地址，掩码和网关地址。

输入 1 修改 IP 配置,输入 2 修改掩码。



输入 D 修改网关信息，输入 S 提交，输入 0 返回，具体可按照提示信息。



(6) 配置 IP 成功，安装完毕。

检查是否配置成功: 登录界面 https://100.0.13.101/upload

E.2.3 获取授权文件和使用说明

(1) 获取软件序列号。

（2）获取授权文件，授权文件是 tar.gz 包。

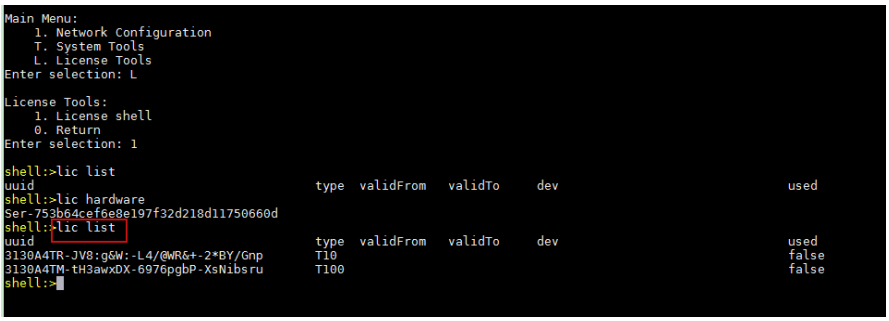
a. 申请授权码。在官网申请堡垒机授权码，授权类型如下

b. 激活 license。结合授权服务器软件序列号，获取授权文件 Ser-XXXX;

c. 导入授权文件，请使用上传授权文件。

d. 查看导入文件，查看授权资产。

查看命令：lic list



E.2.4 注意事项

在创建虚机前，先导入授权文件，同时授权与创建规格对应，避免创建虚机成功，但是服务状态为授权失败。服务不可以使用。

E.3 日志审计授权服务器部署

E.3.1 安装前的准备工作

1. 网络配置需求

在安装 License Server 之前，建议您根据具体需求先规划好基础网络，使得 License Server 所在的 服务器的 IP 地址在网络中可达。

2. 服务器配置需求

硬件配置需求

License Server 所需服务器的硬件配置如下表所示。

表 2-1 硬件配置需求

CPU 架构	CPU 内核	内存	所需磁盘空间	网卡	备注
x86_64(Intel64/AMD64)或ARM64	16核、2.6Ghz主 频及以上	64GB及以上	64GB及以上(根目录 所在的系统分区)	支持1-10Gbps带宽	推荐配置 基于该配置可支持满 规格的客户端数量
x86_64(Intel64/AMD64) 或ARM64	4核及以上 2.0Ghz主 频及以上	16GB及以上	64GB及以上(根目录 所在的系统分区)	支持1-10Gbps带宽	最简配置 基于该配置仅支持20个以内的客户端数量

说明：为保证 License Server 正常运行，请将 License Server 安装在物理服务器而非虚拟机上。

软件配置需求

License Server 所需服务器的操作系统为：

- CentOS 7.6 x86_64
- H3Linux Release 1.1.2 x86_64
- H3Linux 1.1.2 ARM64
- Kylin Linux Advanced Server release V10 x86_64
- Kylin Linux Advanced Server release V10 ARM64
- BC-Linux V7.7 x86_64
- BC-Linux V7.7 aarch64

License Server 安装需要依赖软件包如下表所示：

表 2-2 依赖包版本号

依赖包名称	版本号
unzip	6.0

3. 浏览器需求

用户使用浏览器即可访问 License Server。支持的浏览器类型及版本为：

- Google Chrome 55 及以上；
- Internet Explorer 11 及以上。

4. 运行环境配置

1. 禁用 SELinux

(1) 禁用 SELinux 需要修改 SELinux 配置文件。

```
vi/etc/selinux/config
```

(2) 将 SELINUX 参数值设置为 disabled，以禁用 SELINUX。

```
SELINUX=disabled
```

(3) 保存退出后重启系统即可生效。

2. 配置 DNS

Linux 操作系统下的/etc/resolv.conf 是 DNS 客户机的配置文件，可用于设置 DNS 服务器的 IP 地址。License Server 的授权文件在线自动安装功能需要配置 DNS 服务器的 IP 地址，以对“License 管 理平台域名”进行域名解析。配置文件的内容举例说明：

```
[root@localhost opt]# cat /etc/resolv.conf
search localdomain
nameserver 192.168.1.1
```

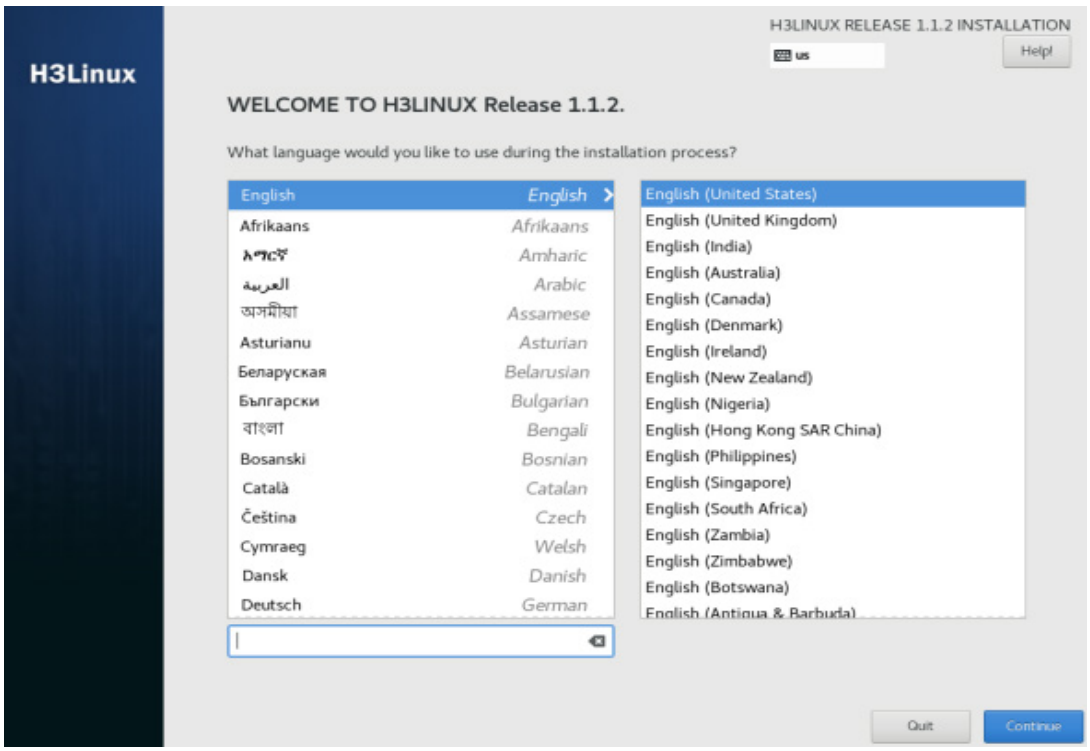
其中，nameserver 表明 DNS 服务器的 IP 地址。可以配置很多行的 nameserver，每一个带一个 IP 地址。在查询时就按 nameserver 在本文件中的顺序进行， 且只有当第一个 nameserver 没有反应时才查询下面的 nameserver。

E.3.2 安装操作系统和 License Server

(1) 使用服务器的远程控制台通过虚拟光驱加载安装软件包的 ISO 文件。

(2) 重新启动服务器，重启后进入系统加载过程，加载完成后，进入 WELCOME TO H3LINUX 界面。

图E-26 图 3-1 WELCOME TO H3LINUX 界面



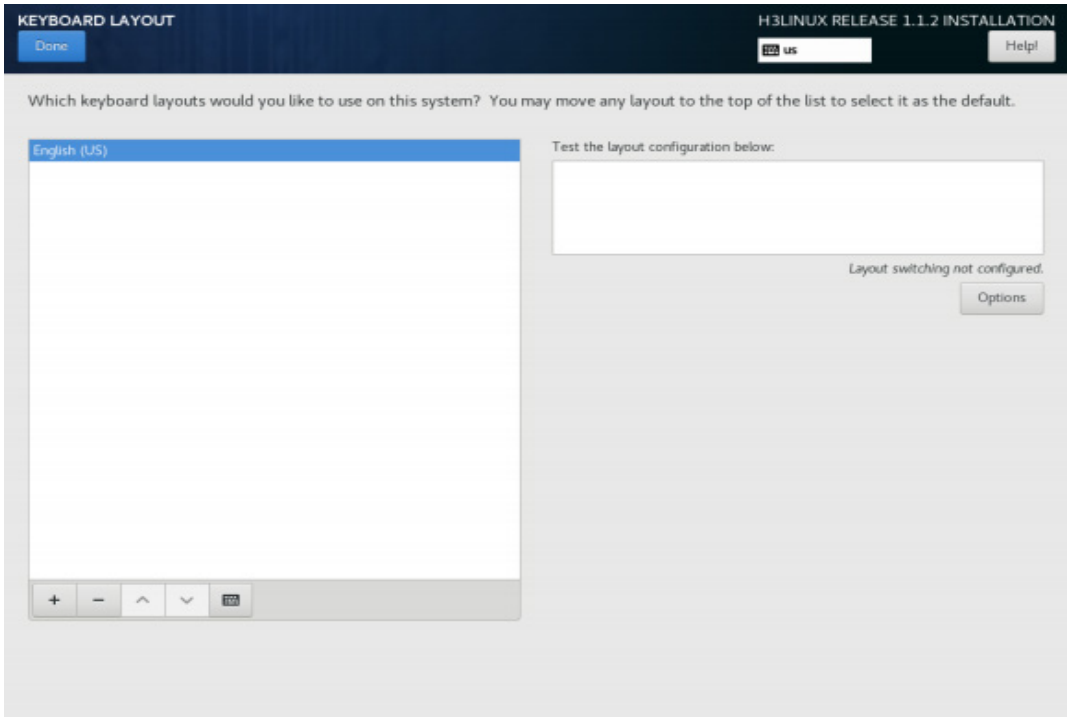
(3) 选择语言，以 English 为例，单击<Continue>按钮进入 INSTALLATION SUMMARY 界面。

图E-27 图 3-2 INSTALLATION SUMMARY 界面

(4) 单击“LOCALIZATION”栏目下的“DATE & TIME”链接进入时间和时区设置页面，选择当前地区的时区，例如，中国地区请选择 Asia/Shanghai 时区。时区和时间设置完成后，单击<Done>按钮返回 INSTALLATION SUMMARY 界面。

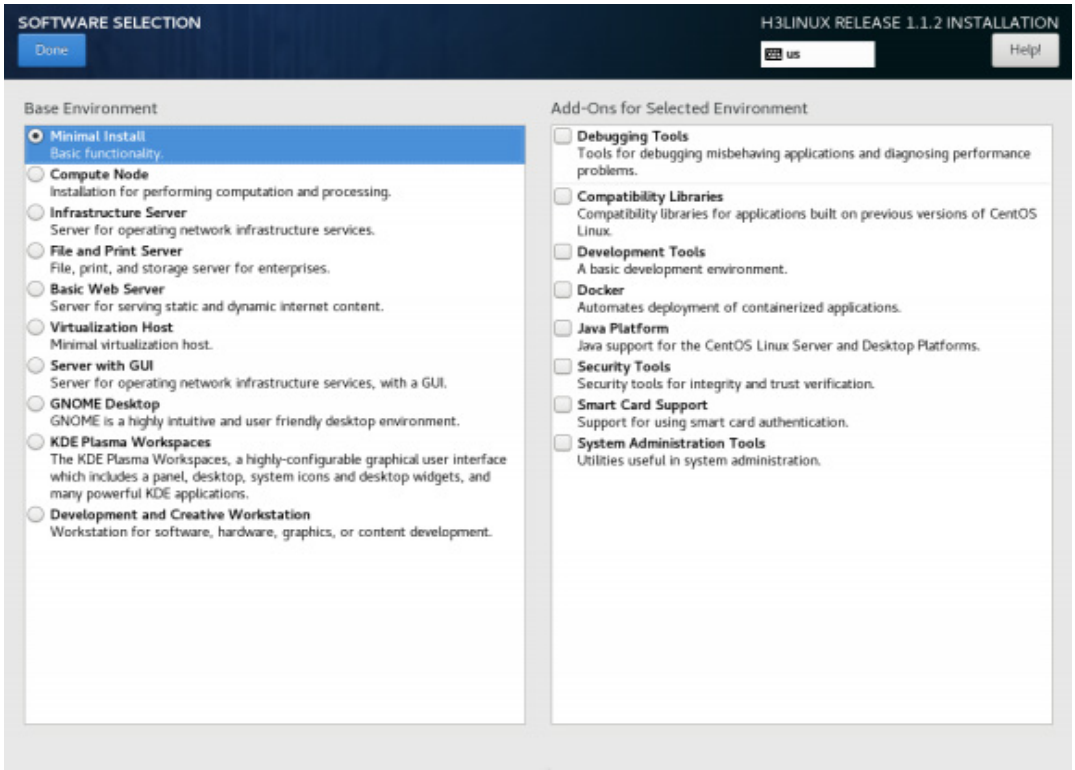
(5) 单击“LOCALIZATION”栏目下的“KEYBOARD”链接进入键盘布局配置页面，选择English(US)。单击<Done>按钮返回 INSTALLATION SUMMARY 界面。

图E-28 图 3-3 键盘布局配置页面



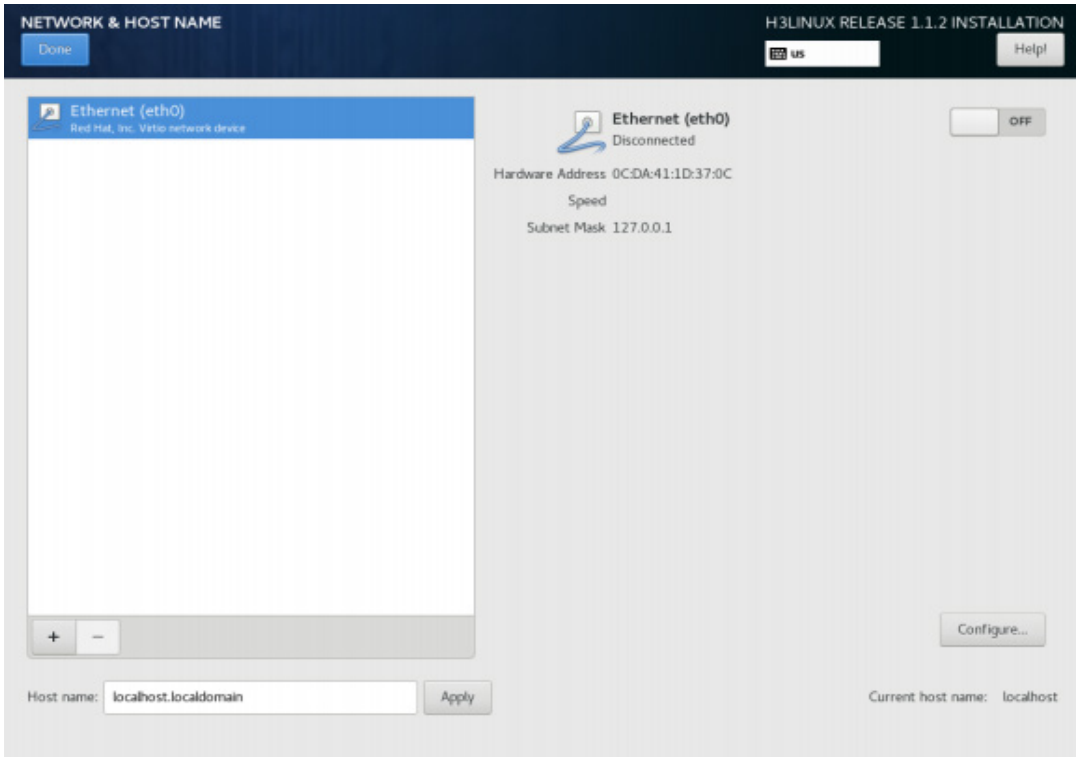
(6) 单击“SOFTWARE”栏目下的“SOFTWARE SELECTION”链接进入软件选择页面，选择 Minimal Install。单击<Done>按钮返回 INSTALLATION SUMMARY 界面。

图E-29 图 3-4 软件选择页面



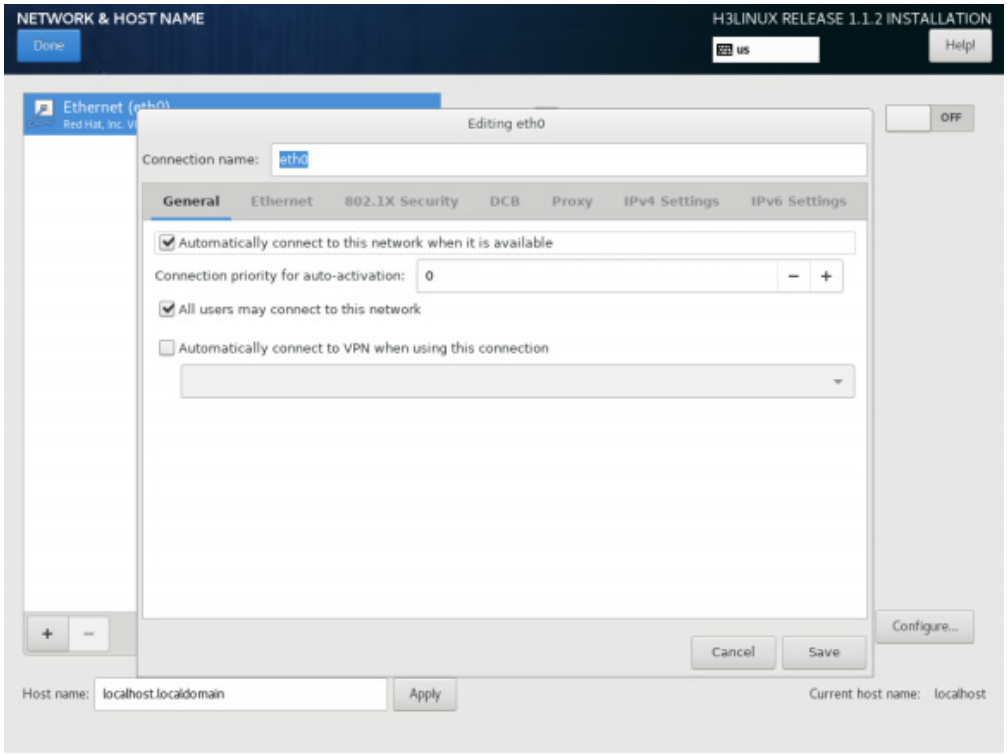
(7) 单击“SYSTEM”栏目下的“NETWORK& HOST NAME”链接进入网络和主机名配置页面，如需修改主机名，可在 Host name 输入框中输入新的主机名， 单击<Apply>按钮完成修改。

图E-30 图 3-5 网络和主机名配置页面

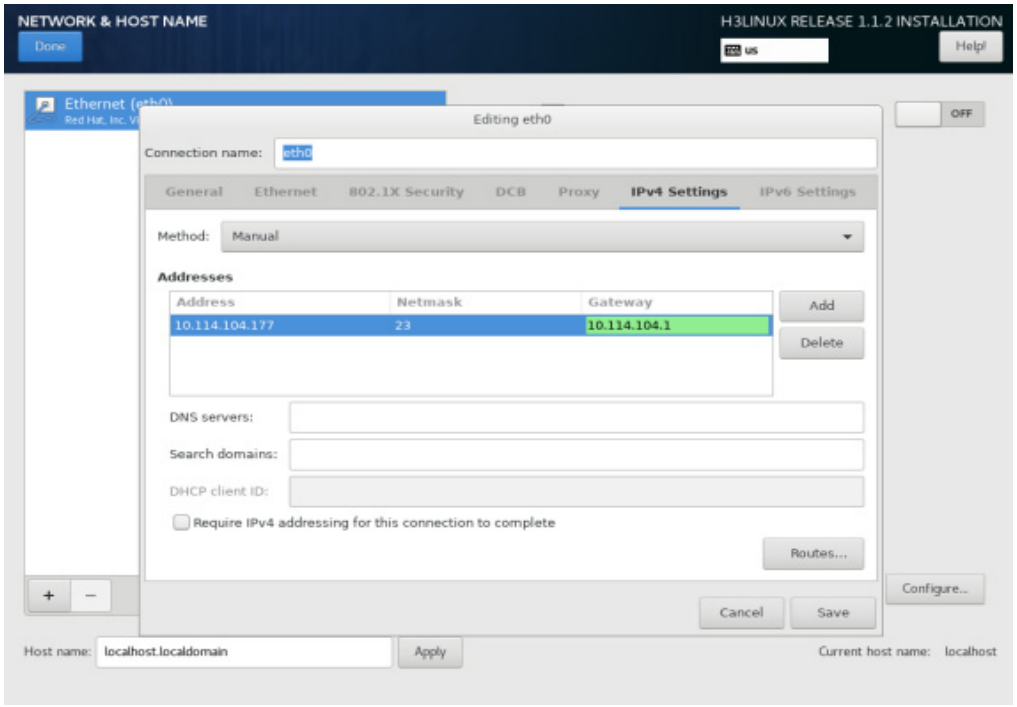


(8) 在网络和主机名配置页面单击<Configure>按钮进入网络配置界面， 单击<General>，勾选<Automatically connect to this network when it is available>复选框， 如图 E-31 所示； 然后单击<IPv4 Settings>配置 IPv4 地址，如图 E-32 所示。配置完成后单击<Save>按钮保存配置， 再单击<Done>按钮返回 INSTALLATION SUMMAY 界面。

图E-31 General 配置

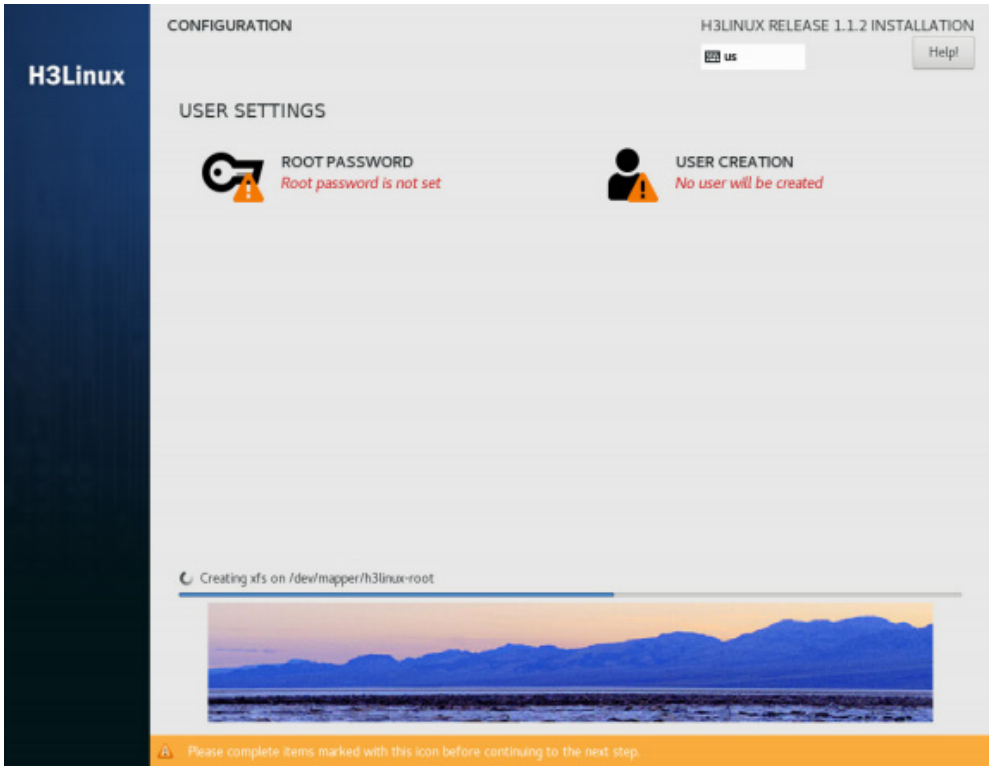


图E-32 配置 IPv4 地址



(9) 完成上述操作后，单击<Begin Installation>按钮开始安装。在安装过程中会弹出用户配置选项，在该页面可创建 Root 用户和密码。

图E-33 设置用户及密码



(10) 安装完成后会自动重启， 完成操作系统和 License Server 的安装。

E.3.3 登录 License Server

(1) 在浏览器中输入 License Server 的 GUI 登录地址(格式为：https://lics_ipv4_address:port/licsmgr 或 https://[lics_ipv6_address]:port/licsmgr，如 https://172.16.0.227:28443/licsmgr)， 回车后会弹出如图 4-1 所示登录界面。

- lics_ip4_address/lics_ipv6_address 为 License Server 软件安装所在服务器的 IPv4 或 IPv6 地址，如果已配置 HA 功能， 则该地址可以为虚拟 IP 地址或主 License Server 的 IP 地址；
- port 为端口号， 缺省为 28443。

图E-34 图 4-1 License Server GUI 登录界面

(2) 输入管理员的用户名和密码(缺省用户名为 admin，密码为 admin@123)后，单击<登录>按钮进入 License Server GUI 首页。

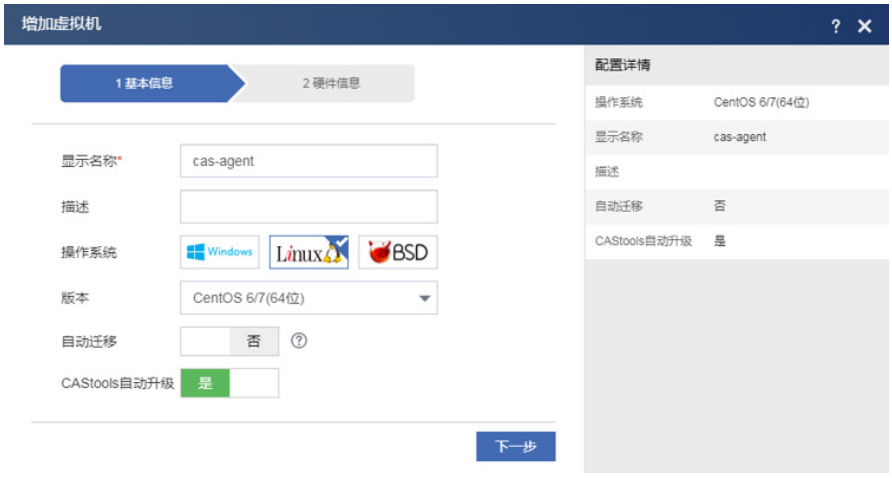
E.4 数据库审计授权服务器部署

E.4.1 Agent-casserver 部署

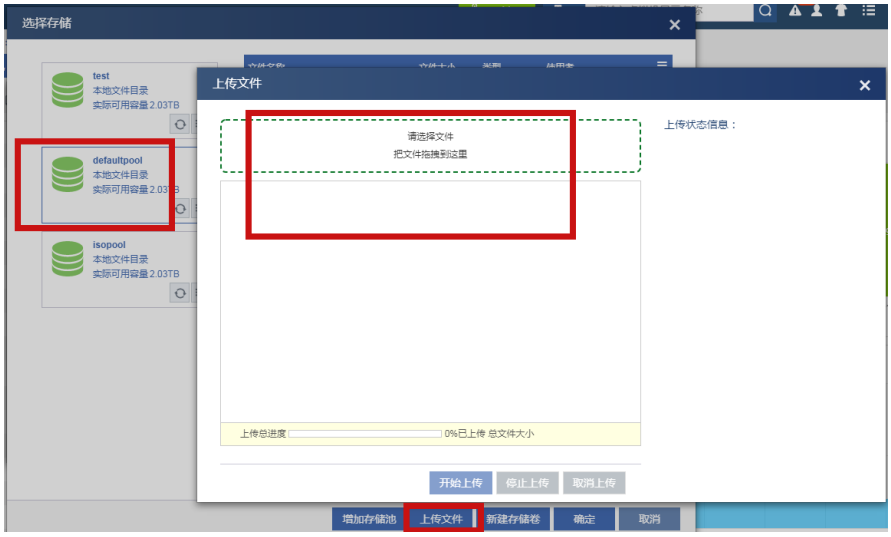
运行环境要求：

CPU	内存	硬盘
至少单颗4核	至少8G	至少200G

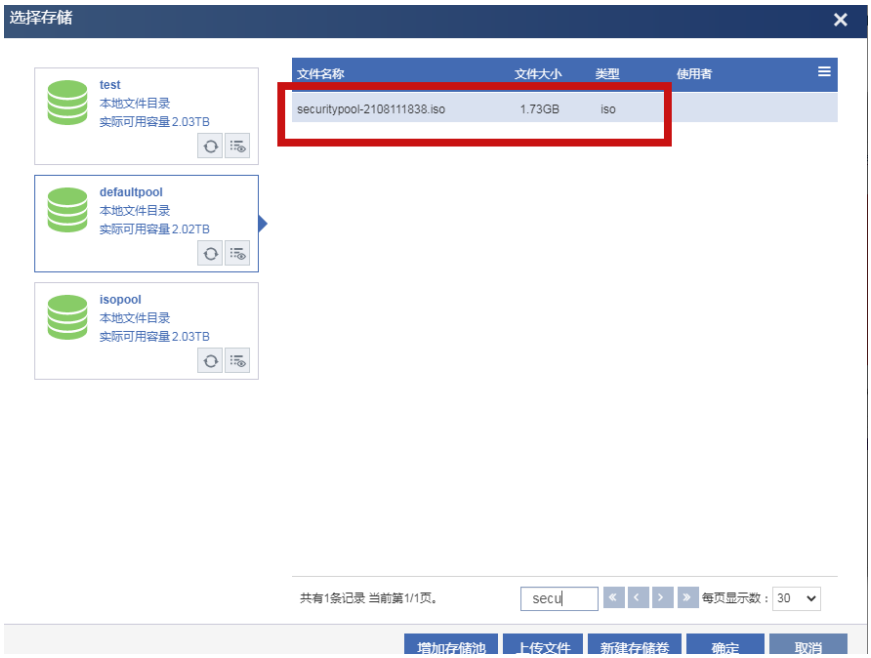
(1) 在 CAS 上创建虚拟机。



a. 选择一个资源池上传镜像。

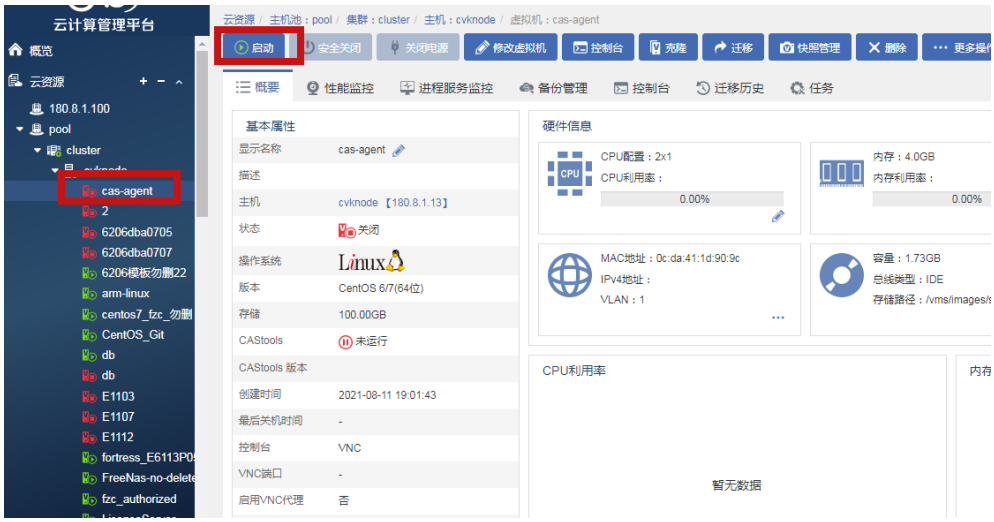


b. 光驱中选择上一步骤中上传的文件。

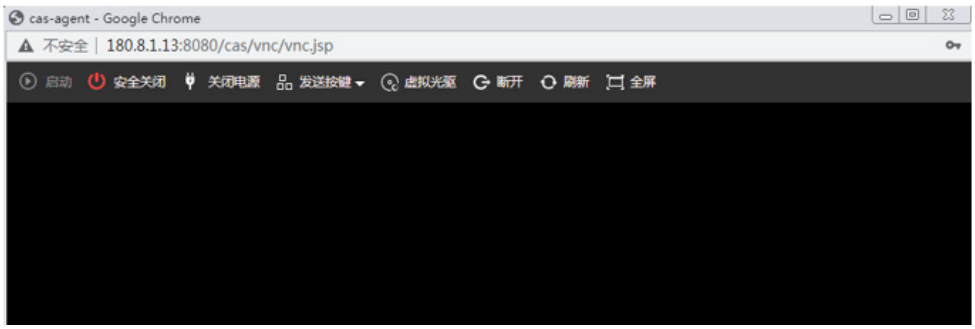


c. 完成虚拟机创建。

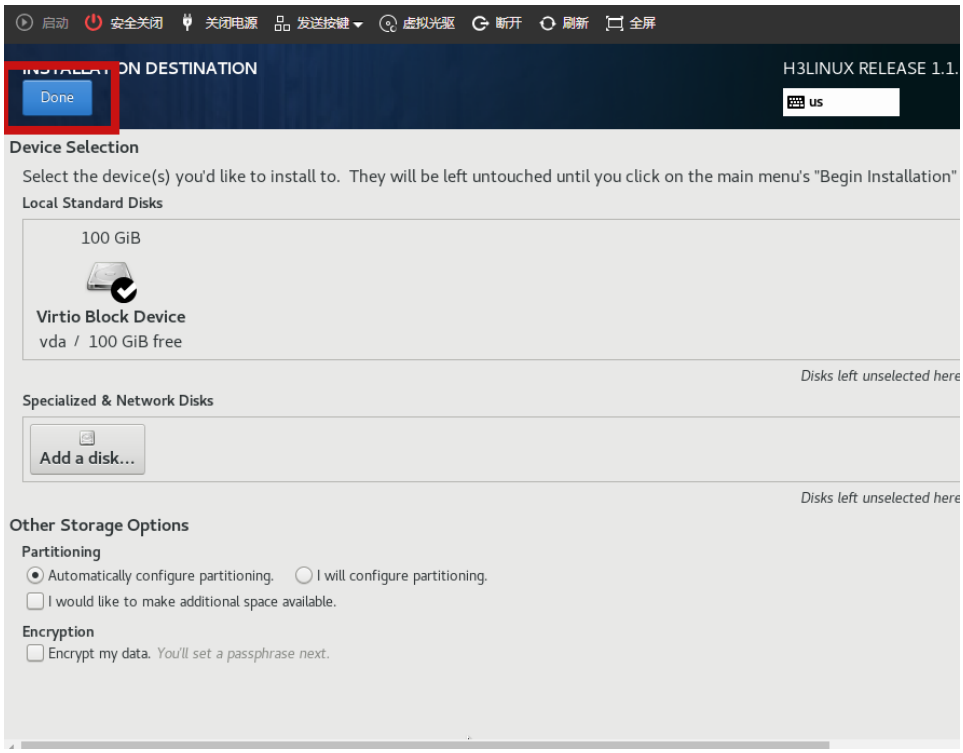
(2) 启动虚拟机，进行虚拟机安装。

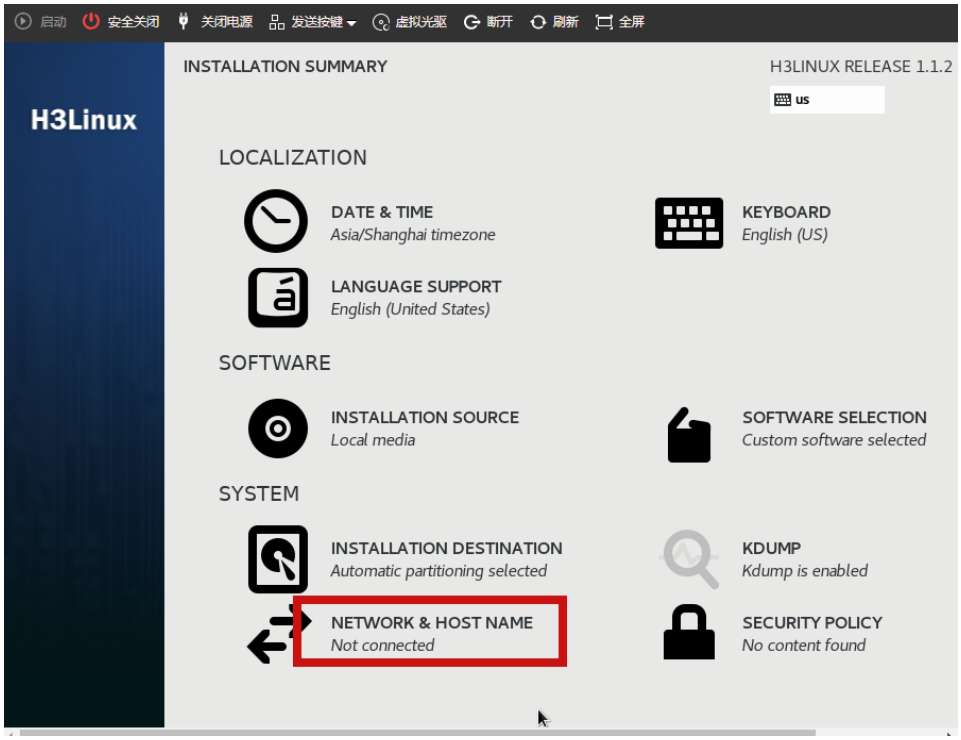


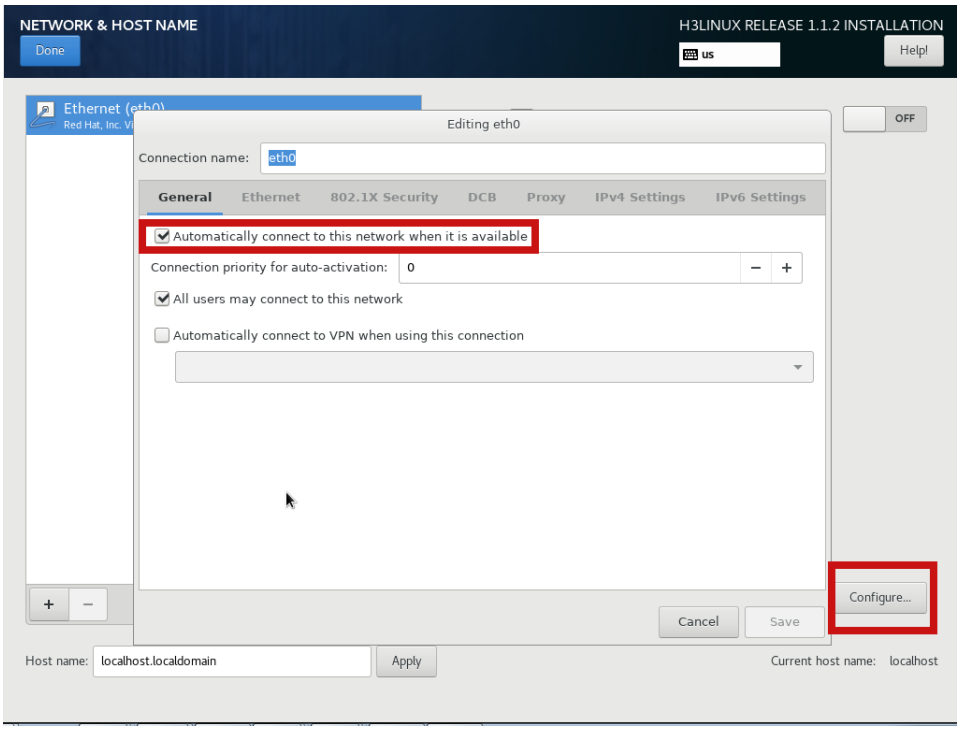
a. 打开控制台。

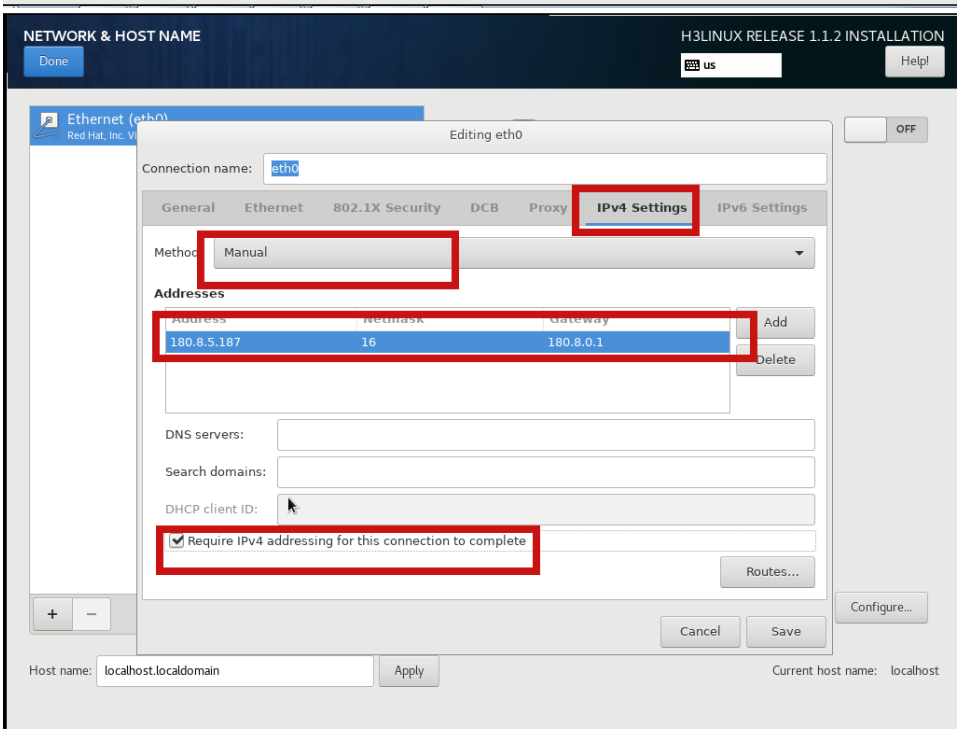


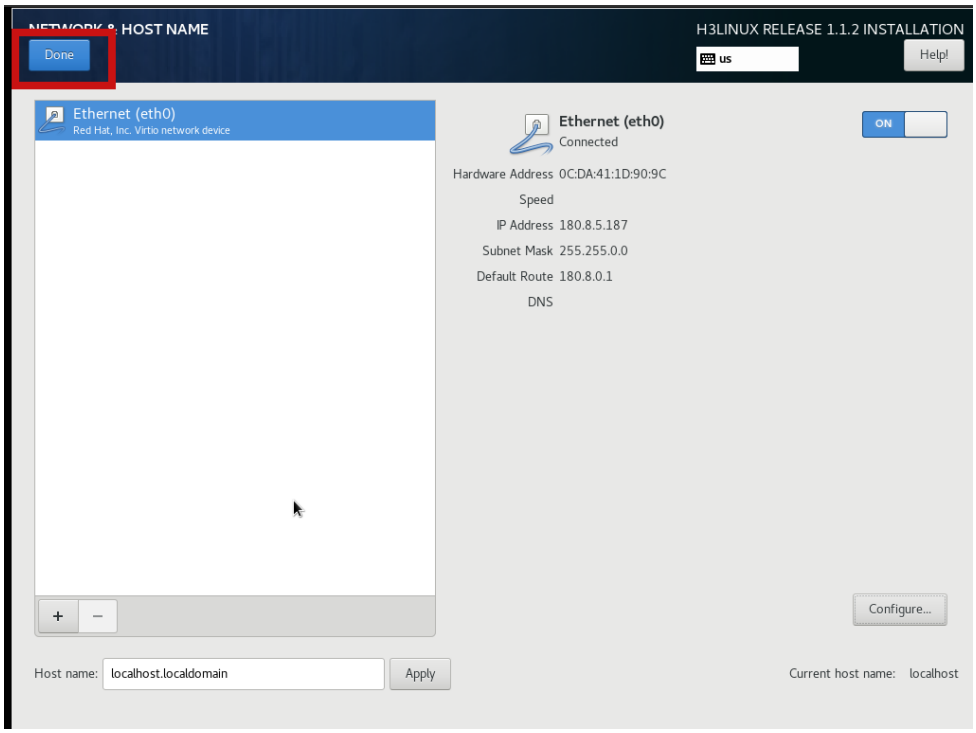
b. 配置磁盘和网络。


启动
安全关闭
关闭电源
发送按键
虚拟光驱
断开
刷新
全屏
ON DESTINATION
Done
H3LINUX RELEASE 1.1.
us
Device Selection
Select the device(s) you'd like to install to. They will be left untouched until you click on the main menu's "Begin Installation"
Local Standard Disks
100 GiB
Virtio Block Device
vda / 100 GiB free
Disks left unselected here
Specialized & Network Disks
Add a disk...
Disks left unselected here
Other Storage Options
Partitioning
Automatically configure partitioning.
I will configure partitioning.
I would like to make additional space available.
Encryption
Encrypt my data. You'll set a passphrase next.

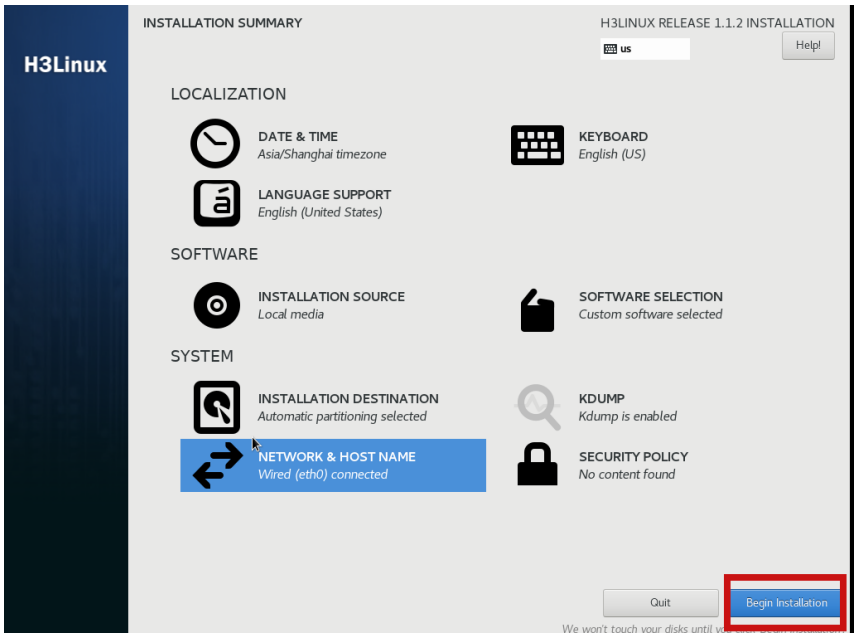

启动
安全关闭
关闭电源
发送按键
虚拟光驱
断开
刷新
全屏
H3Linux
INSTALLATION SUMMARY
H3LINUX RELEASE 1.1.2
us
LOCALIZATION
DATE & TIME
Asia/Shanghai timezone
KEYBOARD
English (US)
LANGUAGE SUPPORT
English (United States)
SOFTWARE
INSTALLATION SOURCE
Local media
SOFTWARE SELECTION
Custom software selected
SYSTEM
INSTALLATION DESTINATION
Automatic partitioning selected
KDUMP
Kdump is enabled
NETWORK & HOST NAME
Not connected
SECURITY POLICY
No content found

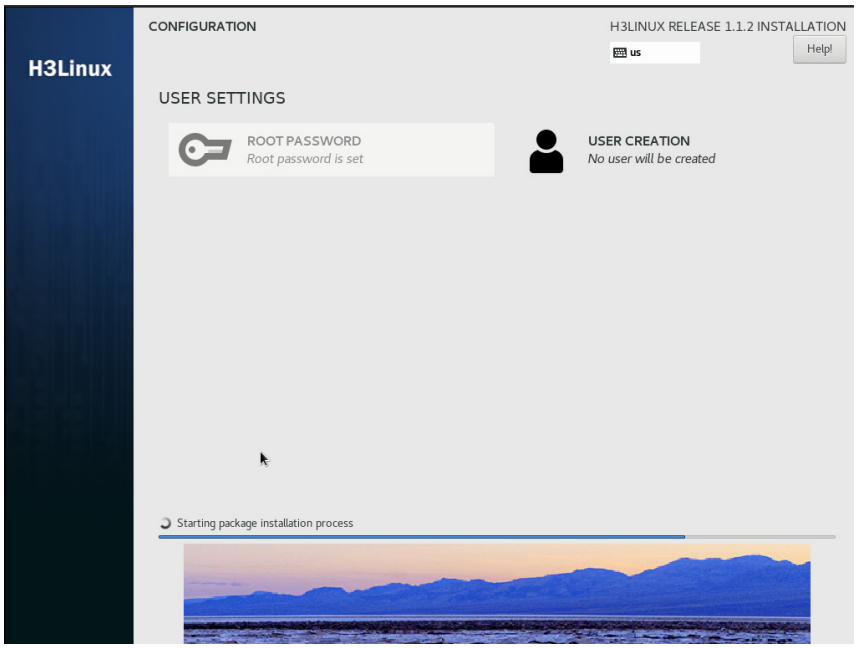

NETWORK & HOST NAME
Done
H3LINUX RELEASE 1.1.2 INSTALLATION
us
Help!
Ethernet (eth0)
Red Hat, Inc. Vi
OFF
Editing eth0
Connection name: eth0
General
Ethernet
802.1X Security
DCB
Proxy
IPv4 Settings
IPv6 Settings
Automatically connect to this network when it is available
Connection priority for auto-activation: 0
All users may connect to this network
Automatically connect to VPN when using this connection
Configure...
Cancel
Save
Host name: localhost.localdomain
Apply
Current host name: localhost


NETWORK & HOST NAME
Done
H3LINUX RELEASE 1.1.2 INSTALLATION
us
Help!
Ethernet (eth0)
Red Hat, Inc. Vi
OFF
Editing eth0
Connection name: eth0
General
Ethernet
802.1X Security
DCB
Proxy
IPv4 Settings
IPv6 Settings
Method: Manual
Addresses
Address
Netmask
Gateway
180.8.5.187
16
180.8.0.1
Add
Delete
DNS servers:
Search domains:
DHCP client ID:
Require IPv4 addressing for this connection to complete
Routes...
Configure...
Cancel
Save
Host name: localhost.localdomain
Apply
Current host name: localhost


HOST NAME
Done
H3LINUX RELEASE 1.1.2 INSTALLATION
us
Help!
Ethernet (eth0)
Red Hat, Inc. Virtio network device
Ethernet (eth0)
Connected
ON
Hardware Address 0C:DA:41:1D:90:9C
Speed
IP Address 180.8.5.187
Subnet Mask 255.255.0.0
Default Route 180.8.0.1
DNS
Configure...
Host name: localhost.localdomain
Apply
Current host name: localhost

c. 开始安装系统。


H3Linux
INSTALLATION SUMMARY
H3LINUX RELEASE 1.1.2 INSTALLATION
us
Help!
LOCALIZATION
DATE & TIME
Asia/Shanghai timezone
KEYBOARD
English (US)
LANGUAGE SUPPORT
English (United States)
SOFTWARE
INSTALLATION SOURCE
Local media
SOFTWARE SELECTION
Custom software selected
SYSTEM
INSTALLATION DESTINATION
Automatic partitioning selected
KDUMP
Kdump is enabled
NETWORK & HOST NAME
Wired (eth0) connected
SECURITY POLICY
No content found
Quit
Begin Installation

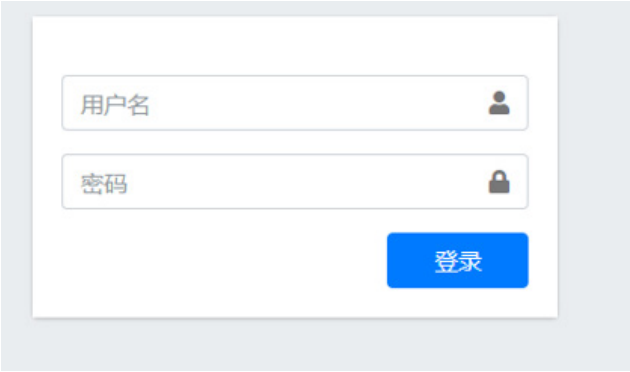


d. 完成操作系统安装。

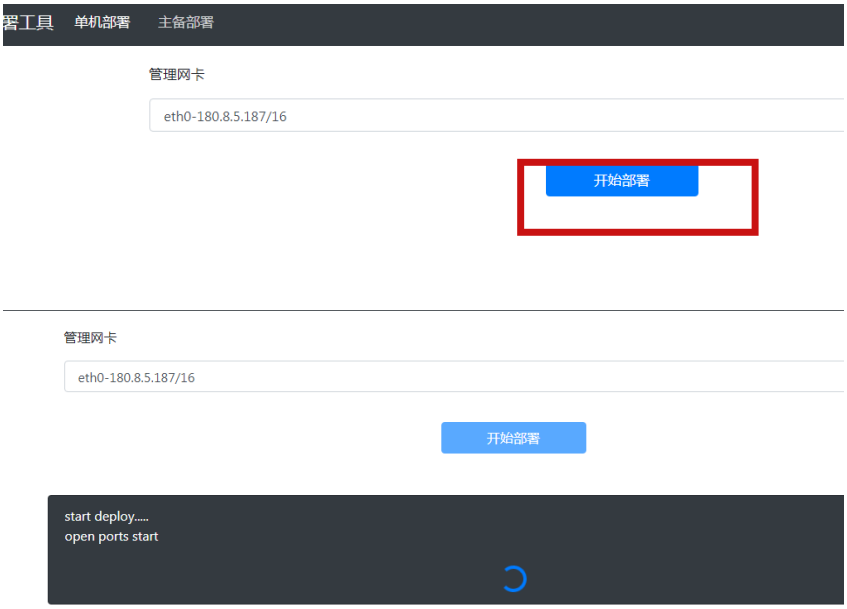
默认后台账号：root/securitypool

(3) 服务安装。

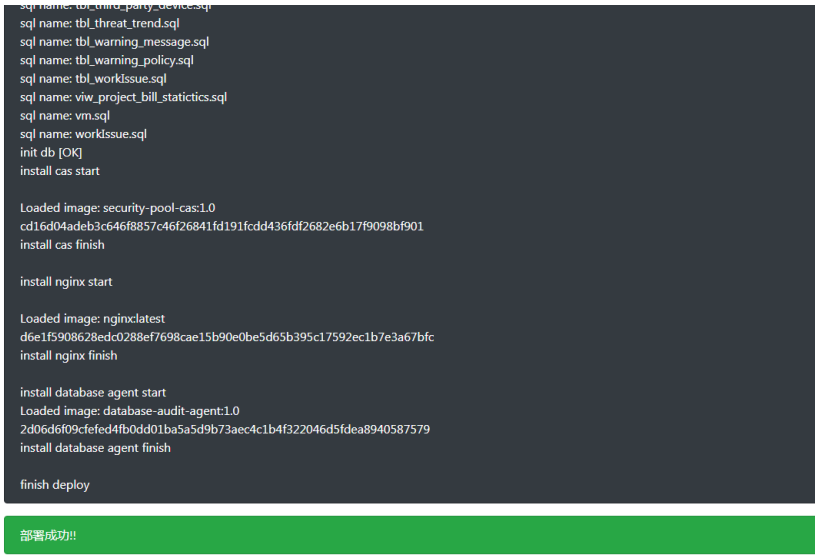
a. 在浏览器输入设置的 ip:9090，输入账号：admin/admin。



b. 点击开始部署。



c. 完成部署。



E.4.2 授权服务器部署

(1) 在“云资源”-“主机池”-“主机”目录，点击“增加虚拟机”，弹出“基本信息”页面，填写“显示名称”、描述等信息，操作系统选择“Linux”，版本可选“CentOS 6/7（64 位）”或者“Other linux（64 位）”，点击“下一步”。

(2) 在硬件信息配置页面后，需增加的配置为：

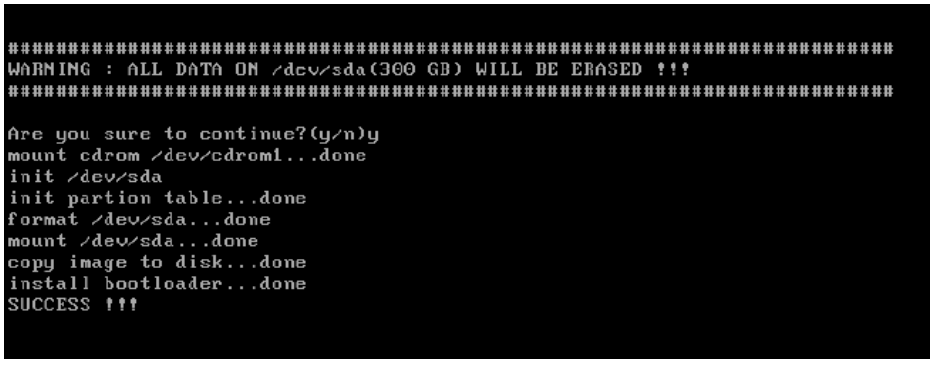
- 建议安装内存不小于 4G。
- 硬盘大小应不小于 200G，且仅支持单硬盘模式。
- 硬盘选项中的设备对象需设置为“SCSI 硬盘或高速 SCSI 硬盘”。
- Castools 类型为：Virtio 串口。

(3) 点击光驱处按钮，选择 license server 镜像包，CPU 最低单个 2 核。

(4) 配置信息填写无误后，点击完成，右键点击修改虚拟机，在”概要“可查看 castools 类型。

(5) 至此，虚拟机已成功添加至“主机”下，点击“启动”即可。

(6) 通过硬盘模式检测后，安装系统弹出提示，询问是否格式化硬盘，在提示界面，输入 y，则系统将格式化硬盘，格式化完后自动开始安装系统。如输入 n，则系统将不会格式化硬盘，安装中止，系统退出并关机。



(7) 格式化硬盘过程完成后，系统会自动关机，右键点击修改虚拟机，选择光驱，点击断开连接，再次启动虚拟机，等待系统安装完成。

(8) 安装完成后，默认管理口 IP 地址为 192.168.0.1/24，可通过点击修改虚拟机，点击网络，IPv4 信息处勾选“手工配置”，根据实际环境配置管理口 IP，点击应用，如下图所示。

说明：若使用的 License Server 安装包为 SecPathD2000V-LicenseServer-201911141731611.iso，在系统安装完成后，不支持在 CAS 界面通过手工配置管理口 IP 地址，可在 CAS 中可以使用与 license server 相同 vswitch 的一台 windows 虚拟机，配置与默认管理口（192.168.0.1）相同网段的 IP 地址，如：192.168.0.2，使用火狐浏览器，在地址栏中输入管理口 IP 地址（https://192.168.0.1），即

可打开 License Server 登录页面。可使用系统默认管理员账号 admin/admin，登录 License Server。

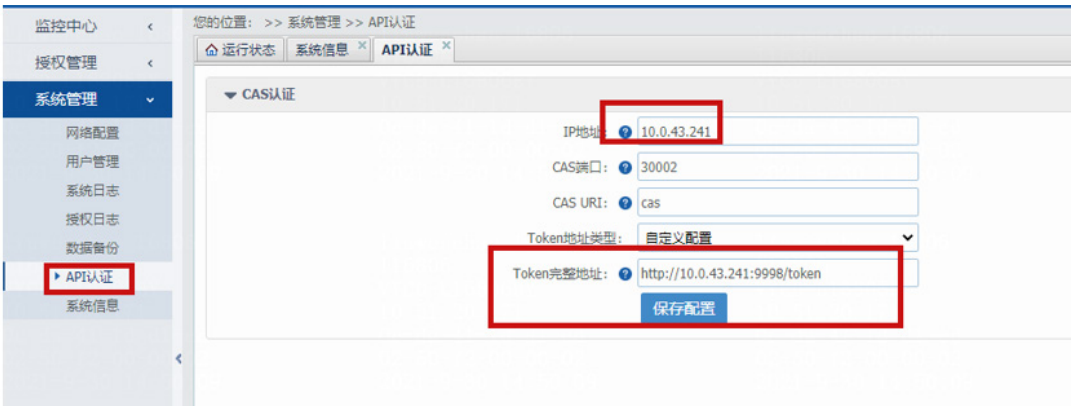
(9) 使用火狐浏览器访问登录地址 https://ip/（如 https://183.1.4.32），如下图所示。

注：出现上述登录提示后，需进入 CAS 后台安装并配置硬件信息采集探针 casagent，安装过程请参考下文“Casagent 安装”，Casagent 安装完成后，刷新浏览器界面，即可登录系统。

(10) License Server 部署完成，使用默认账号密码 admin/admin 即可登录系统。

(11) 配置 API 认证。

进入系统管理 > API 认证，使用给 agent-casserver 分配的地址替换下图中的地址。



E.4.3 Casagent 安装

1. 硬件信息采集探针安装

(1) 使用远程工具，如 Xshell 工具，设置连接参数，输入用户名、密码，连接 CAS 后台。

(2) 连接设备后，将下载好的硬件信息采集探针 casagent.tar.gz 文件通过文件传输工具 Xftp 上传到固定目录/mnt/test 文件夹下，使用命令（cd /路径名，如“cd /mnt/test”）进入 该文件夹后，通过解压命令“tar -zxvf casagent.tar.gz”，解压 casagent.tar.gz 文件。

在当前文件夹，使用命令（cd /路径名，如“cd /mnt/test/cassetup”）进入该文件夹后输入安装命令“sh setup.sh”，回车后完成安装。

```
➤ SSH session to root@100.0.13.20
  ? SSH compression : ✔
  ? SSH-browser     : ✔
  ? X11-forwarding  : ✘  (disabled or not supported by server)
  ? DISPLAY         : 182.9.11.211:0.0

➤ For more info, ctrl+click on help or visit our website

Authorized users only. All activity may be monitored and reported
Last login: Thu Nov 26 20:36:04 2020 from 182.9.11.139
root@cvknode:~# cd /mnt/test
root@cvknode:/mnt/test# ll
total 352
drwxr-xr-x 2 root root   4096 Jan 14 14:20 ./
drwxr-xr-x 3 root root   4096 Jan 14 14:19 ../
-rw-r--r-- 1 root root 348733 Jan 14 14:20 casagent-1.1.tar.gz
root@cvknode:/mnt/test# tar -zxvf casagent-1.1.tar.gz
./cassetup/
./cassetup/简要说明.txt
./cassetup/setup.sh
./cassetup/casagent/
./cassetup/casagent/cas_hd_info_run.log
./cassetup/casagent/cas_get_host_info
./cassetup/casagent/cas_vmlist.ini
./cassetup/casagent/casag_system.sh
./cassetup/casagent/casag_agentd.sh
./cassetup/readme.txt
root@cvknode:/mnt/test# cd cassetup/
root@cvknode:/mnt/test/cassetup# ll
total 24
drwxr-xr-x 3 root root 4096 Aug 21 17:46 ./
drwxr-xr-x 3 root root 4096 Jan 14 14:20 ../
drwxr-xr-x 2 root root 4096 Nov 25 08:58 casagent/
-rw-r--r-- 1 root root  294 Aug 21 11:39 readme.txt
-rw-r--r-- 1 root root  284 Aug 21 16:00 setup.sh
-rw-r--r-- 1 root root  580 Aug 21 11:36 简要说明.txt
root@cvknode:/mnt/test/cassetup# sh setup.sh
-e END
```

(3) 安装完成后探针程序自动运行， 并在/etc/rc.local 文件中增加监控服务脚本的调用（/mnt/casagent/casag_system.sh &）。

使用命令 vi /etc/rc.local 查看，按 Esc 并输入:q 退出当前界面。

注意：如发现/etc/rc.local 文件中存在 exit 0 的结束命令，基于系统安全性和不同平台差异性考虑，请手动将监控服务脚本的调用命令移至该结束命令上方，如下图：

```
#!/bin/sh -e
#
# rc.local
#
# This script is executed at the end of each multiuser runlevel.
# Make sure that the script will "" on success or any other
# value on error.
#
# In order to enable or disable this script just change the execution
# bits.
#
# By default this script does nothing.


touch /var/run/cas_cvk
/opt/bin/util_cvk_reserved_mem.sh
/usr/bin/set-printk-console 2
/opt/bin/open-iscsi_check.sh
/opt/bin/util_remove_audio.sh
/opt/bin/util_setup_new_interfaces.sh
/usr/bin/python /opt/bin/set_irq_affinity.pyc execute
/usr/bin/python /opt/bin/inspection_mem_cpufreq_init.pyc
iptables-restore < /etc/cvm/iptables.roles
/mnt/casagent/casag_system.sh &
exit 0
```

2. 硬件信息采集探针配置

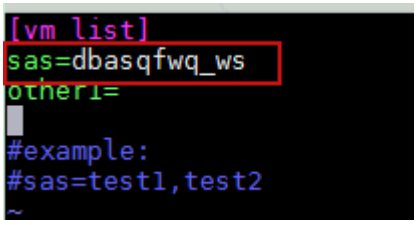
配置探针通讯文件，使用命令“virsh list”列出平台上所有虚拟机名称，如下图：

运行命令执行成功后界面

```
Authorized users only. All activity may be monitored and reported
Last login: Thu Jan 14 15:24:27 2021 from 182.9.11.211
root@cvknode:~# virsh list
 Id    Name                           State
----------------------------------------------------
 2     LicenseServer                  running
 3     WAFsqfwq_E6203P01              running
 4     WAFsqfwq_E6203P01_zs           running
 10    yyjk                           running
 13    FW                             running
 37    DNS                            running
 52    rzsjE1706bb                    running
 54    SSMS6403bb_ws                  running
 57    wafsqfwq-zs                    running
 59    WAF-sqfwq-zs                   running
 60    lsP04                          running
 67    dbasqfwq_ws                    running

root@cvknode:~# vi /mnt/casagent/cas_vmlist.ini
root@cvknode:~#
```

修改通讯配置文件，输入命令“vi /mnt/casagent/cas_vmlist.ini”，回车后，进入参数配置页，修改默认参数为“virsh list”查出的虚拟数据库审计的名称，如下图，保存后无需重启服务；

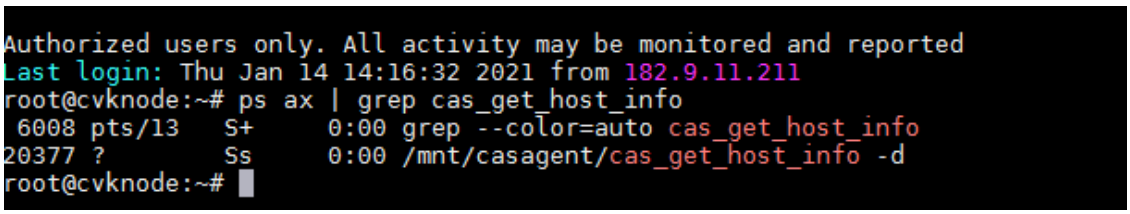
备注：该配置仅支持填写一个虚拟机名称。



3. 硬件信息采集探针运行

探针安装完毕后，通过“ps ax|grep cas_get_host_info”命令查看进程是否在运行。

查看运行状态



E.5 网页防篡改授权服务器部署

E.5.1 硬件规格

网页防篡改授权管理系统的硬件服务器规格如表 E-1 所示。

表E-2 网页防篡改授权管理系统硬件规格（仅支持在 CAS 平台下安装）

客户端个数	CPU	内存	硬盘
0-50	CPU类型：不限制cpu类型，确保分配4核	至少1G	至少25G
50-100		至少2G	至少 40G
100-150		至少2G	至少50G
150-200		至少4G	至少64G
大于200	暂不支持超过200个客户端		
安装包	SecPath W2000-VG2&SysScan&WG-LicenseServer-E6202-x86.iso		

E.5.2 CAS 平台安装虚拟 web 应用防火墙授权管理系统

(1) 上传镜像包。点击存储，选择目录，点击上传文件。

图E-35 上传镜像包

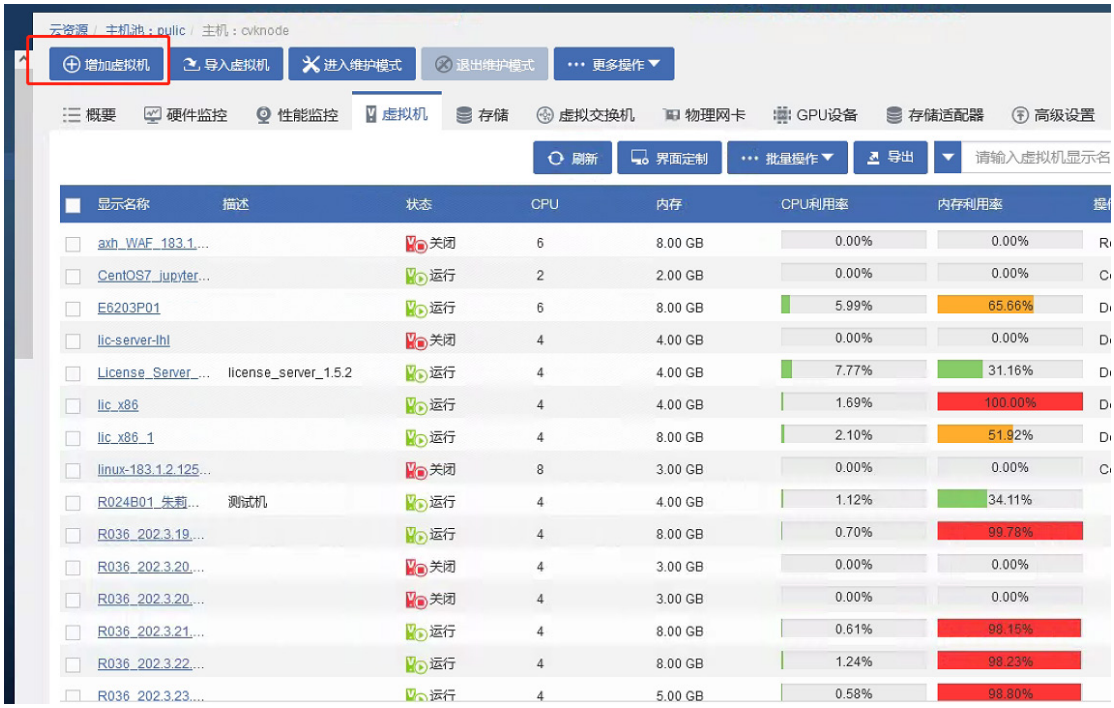
(2) 选择镜像包后，点击开始上传。

图E-36 选择镜像包

图E-37 查看上传的镜像包

(3) 点击增加虚拟机。

图E-38 增加虚拟机



(4) 设置虚拟机的显示名称，操作系统选择 Linux，版本选择 DebianGUN/Linux9(64 位)，CAStools 自动升级选择否。

图E-39 虚拟机基本配置

(5) 选择磁盘的总线类型为 IDE 硬盘，也可选择默认的高速磁盘。

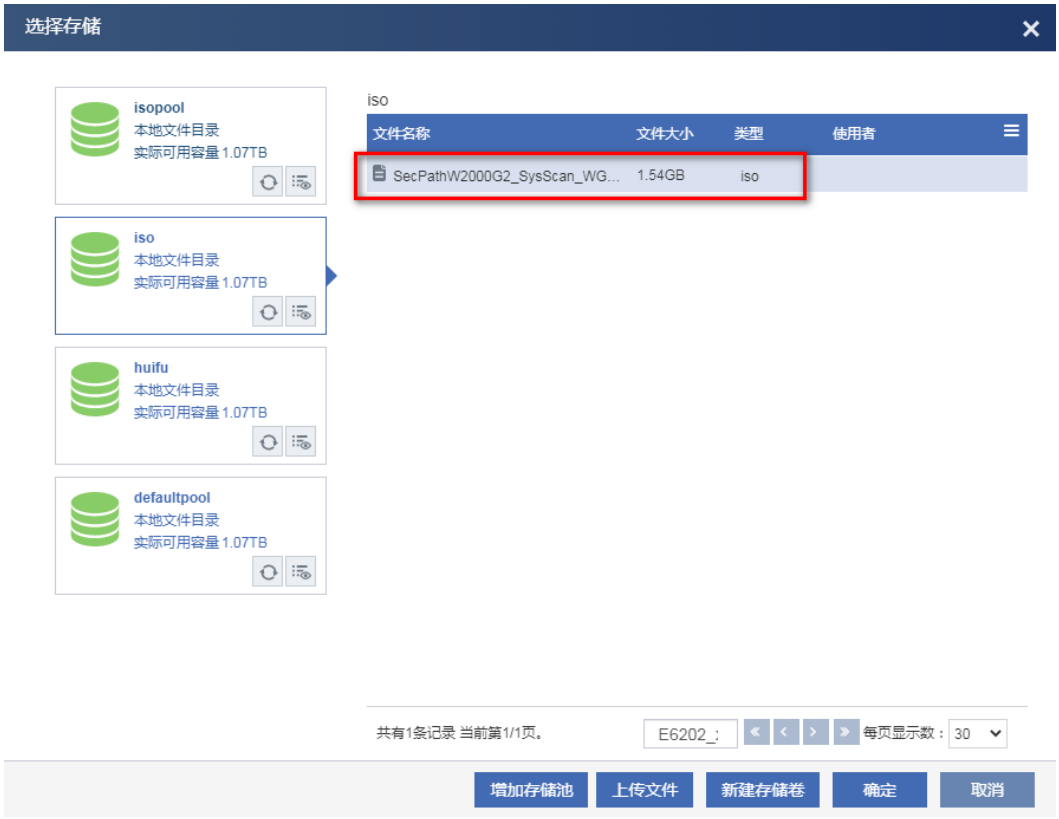
图E-40 设置磁盘的总线类型

(6) 选择光驱，点击光驱右侧的搜索。

图E-41 设置光驱

(7) 在文件目录中，选择镜像包，点击确定。

图E-42 选择镜像包



(8) 配置完成后，确认无误，点击完成。

图E-43 配置完成

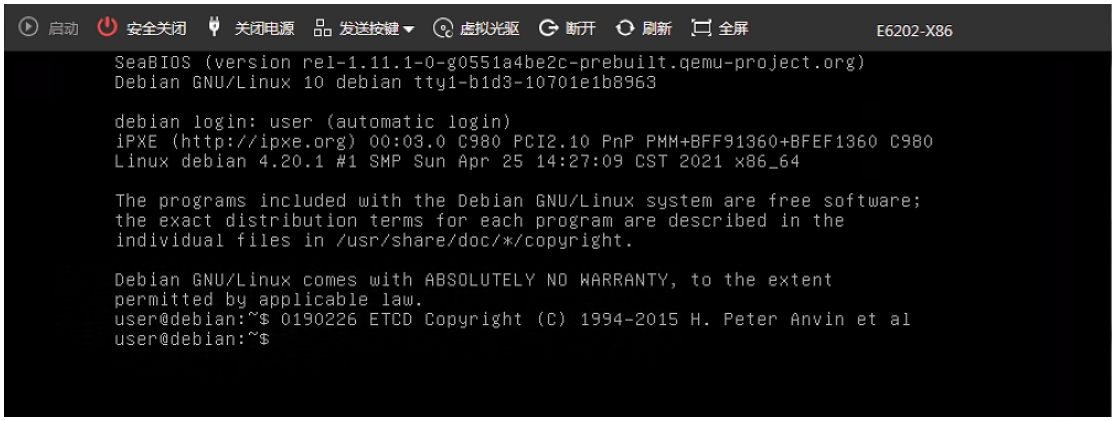
(9) 选择创建的虚拟机，点击启动。

图E-44 启动虚拟机

(10) 点击控制台，进行安装。

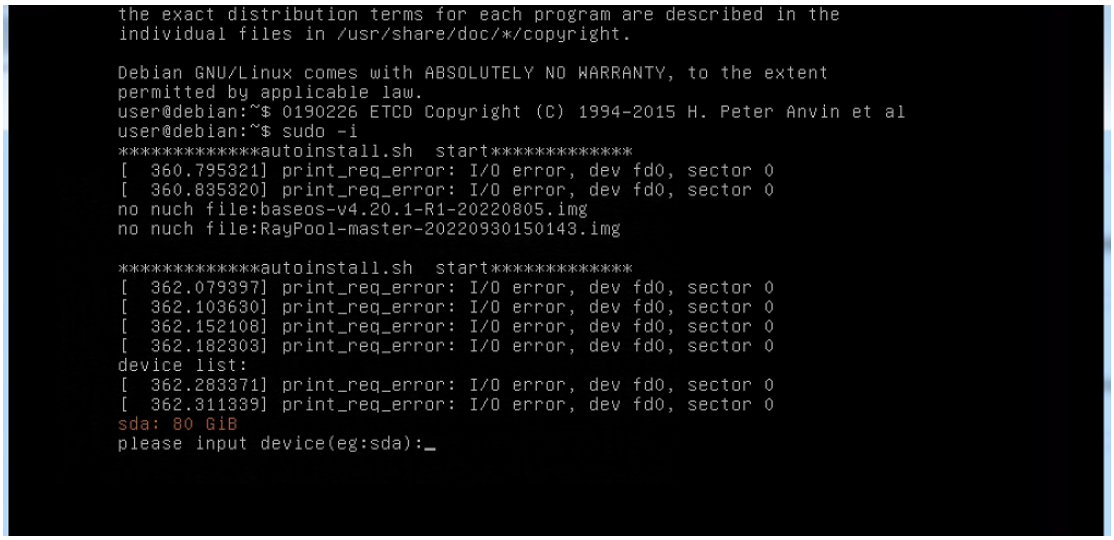
图E-45 打开控制台

(11) 系统会自动登录 user，手动输入 sudo su 即可调起 autoinstall.sh 安装程序。



注意：

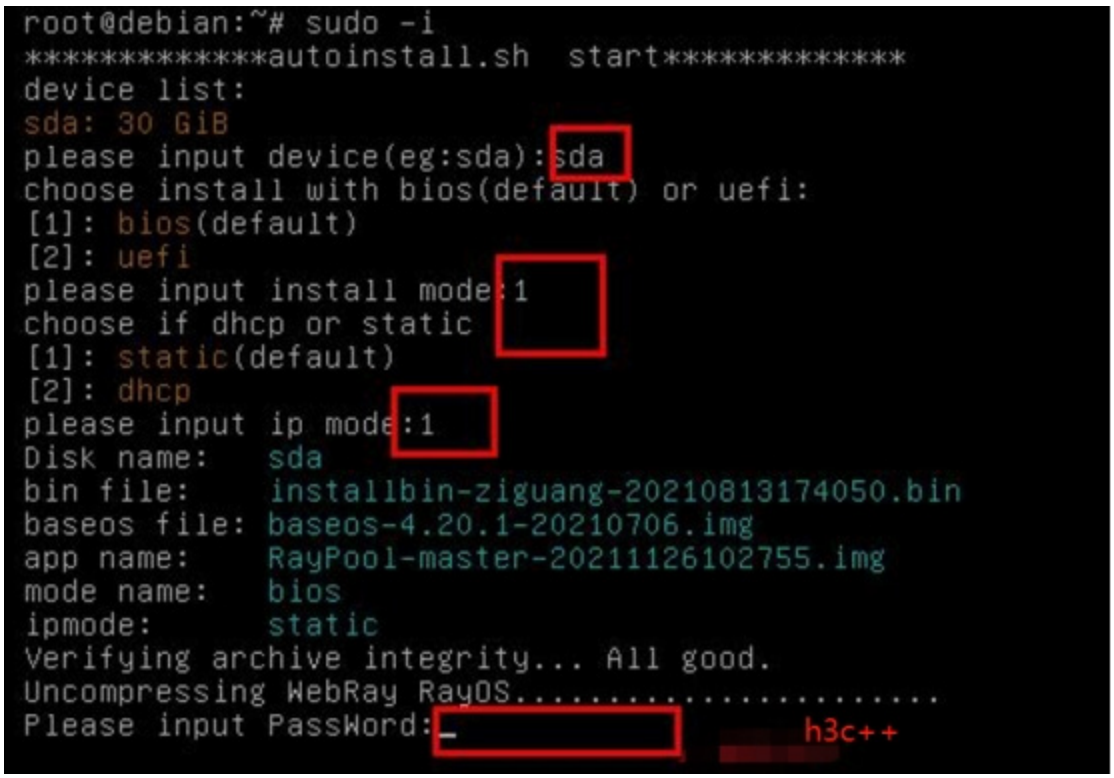
由于磁盘名为 vda 的情况较多，故自动化安装默认选择 vda，若 Disk name 是 sda 而非 vda 时，系统会提示



此时需要手动安装，即需要手动输入下述内容：

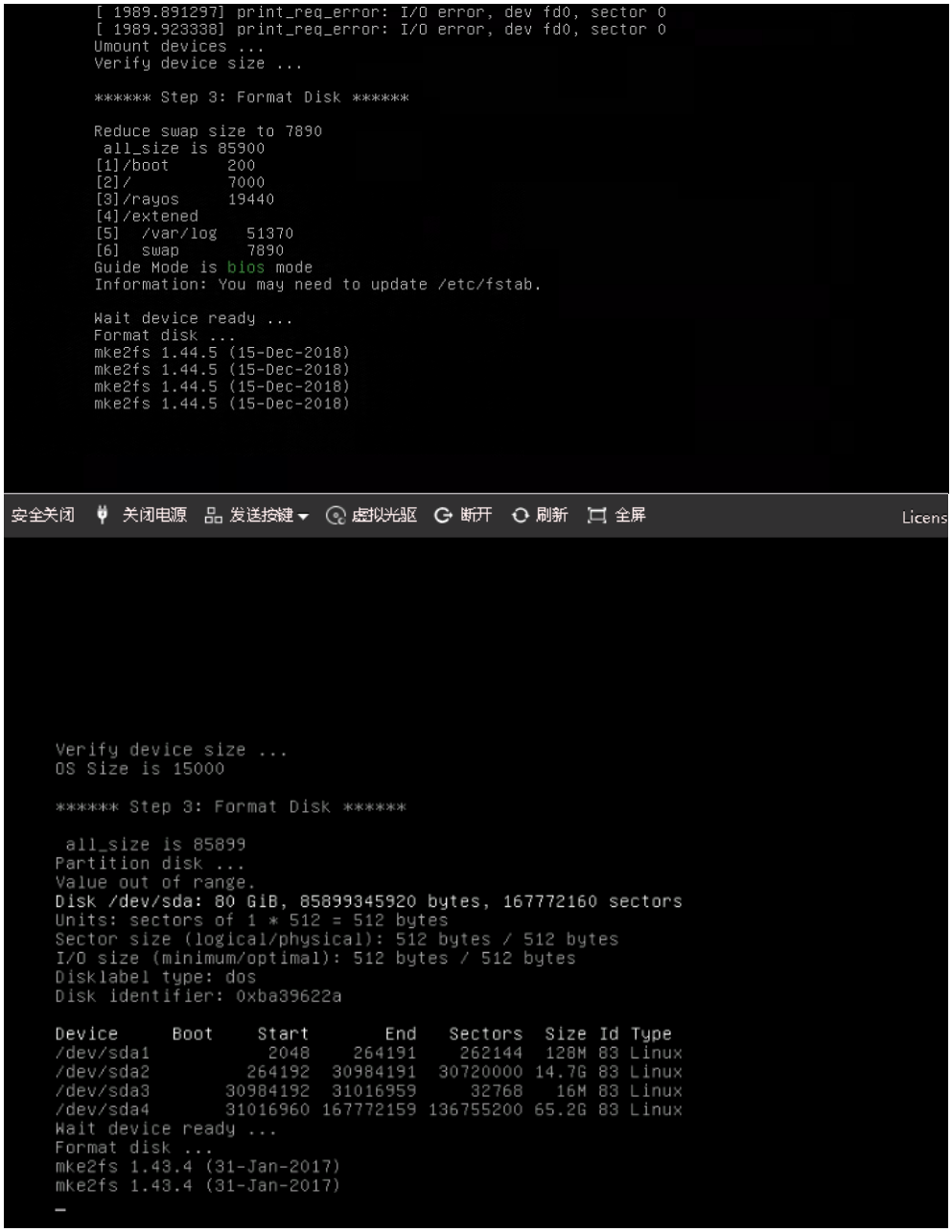
输入 sda，输入 1 选择 bios 模式，输入 1 选择 static 模式，输入刻盘密码：h3c++ 输入 y 继续。

图E-46 输入刻盘密码



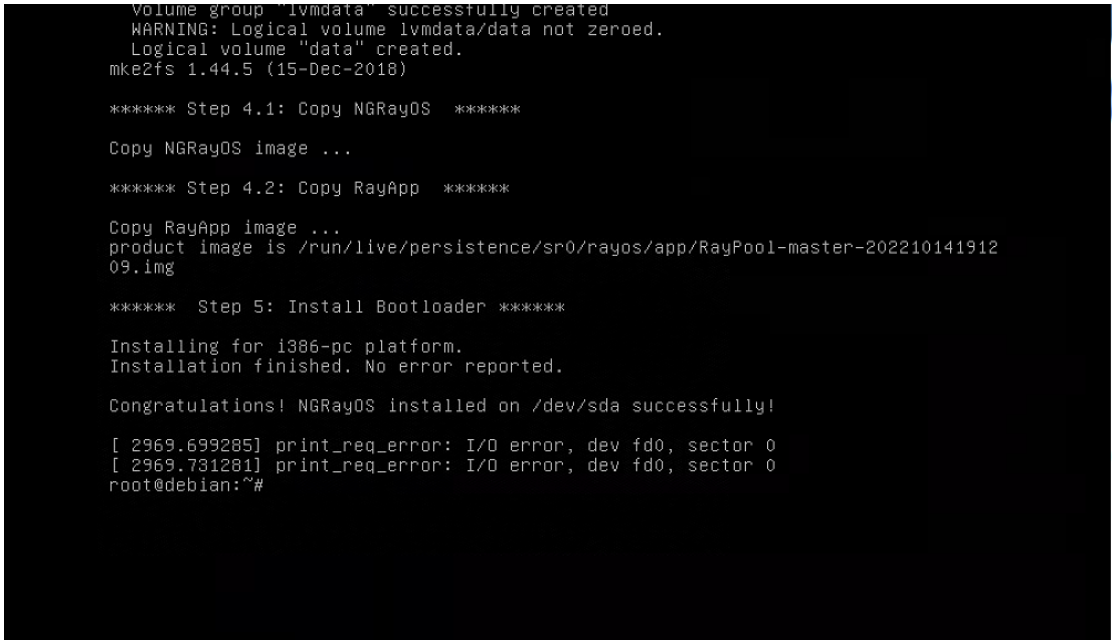
(12) 系统开始安装，一共五步，不需要手动参与，大概需要三到五分钟。

图E-47 开始安装



(13) 安装完成之后，出现提示“Congratulations! NGRayOS installed on /dev/sda successfully!”，按回车键，系统将自动重启。

图E-48 安装完成



(14) 输入 reboot 重启后进行刻盘。

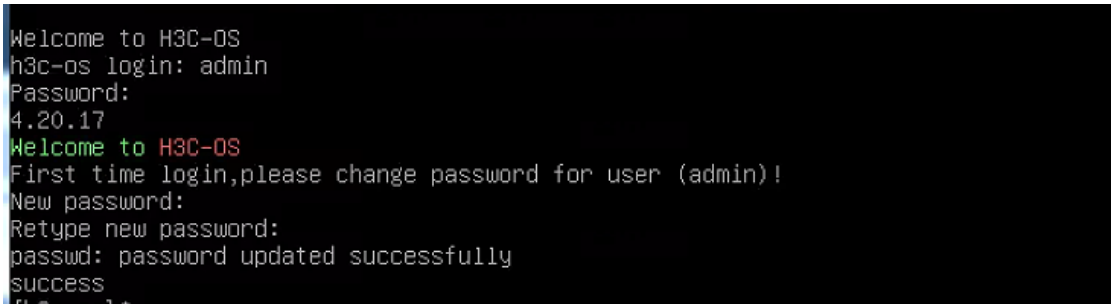
图E-49 重启系统

(15) 请耐心等待，刻盘结束后，会自动关闭机器，需要在 CAS 平台手动启动。此过程大约 10 分钟，请耐心等待。

图E-50 手动启动授权管理系统

(16) 在控制台下使用账号密码 admin/admin 登录系统，登陆成功后需要修改密码。

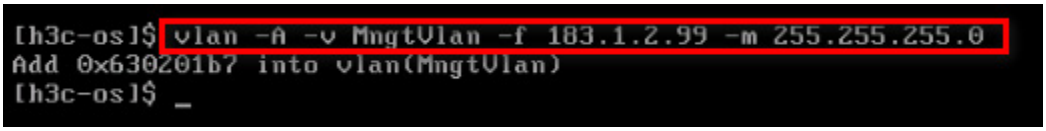
图E-51 登录成功



(17) 根据 CAS 平台的实际网络配置，来配置授权管理系统的管理 IP 地址。命令如下：

```
vlan –A –v MngtVlan –f 183.1.2.99 –m 255.255.255.0
## 请根据实际组网情况合理配置管理地址
```

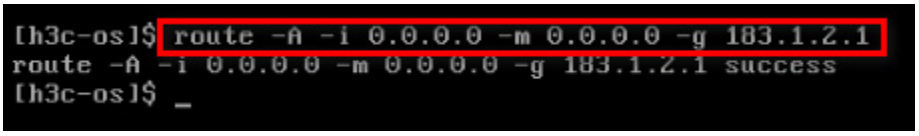
图E-52 配置 ip 地址



(18) 配置默认路由，命令如下：

```
route –A –i 0.0.0.0 –m 0.0.0.0 –g 183.1.2.1
## 请根据实际组网情况合理配置路由
```

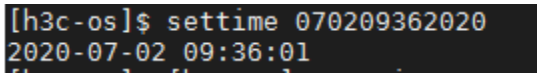
图E-53 添加默认路由



(19) 配置系统时间，命令如下：

```
settime 070209362020
##说明 settime 格式，settime 月日时分年
```

图E-54 添加系统时间



(20) 如果命令输入错误，导致 IP 或者路由配置错误，可以通过命令修改，查询 vlan 和 route 的命令格式，只需要输入 vlan 或者 route 即可。

图E-55 vlan 命令帮助

```
[h3c-os]$ vlan
none cmd is set!
vlan usage:
        vlan -C/--create -i/--vid <vlanid>(2-4094) [-v/--vname <vlanname>(def na
me: vlan$vid)] -d/--mode <0-traditional|1-transparent|2-passthrough>
        vlan -D/--delete -v/--vname <vlanname>
        vlan -E/--enable -v/--vname <vlanname>
        vlan -N/--disable -v/--vname <vlanname>
        vlan -A/--add -v/--vname <vlanname> -f/--ip <ipv4> -m/--mask <mask>
        vlan -R/--remove -v/--vname <vlanname> -f/--ip <ipv4>
        vlan -L/--link -v/--vname <channelname> -g/--group <portname/channelname
>
        vlan -U/--unlink -v/--vname <vlanname> -g/--group <portname/channelname>
        vlan -M/--modify -v/--vname <vlanname>  <-t/--mtu <mtu>>
        vlan -S/--show
[h3c-os]$ _
```

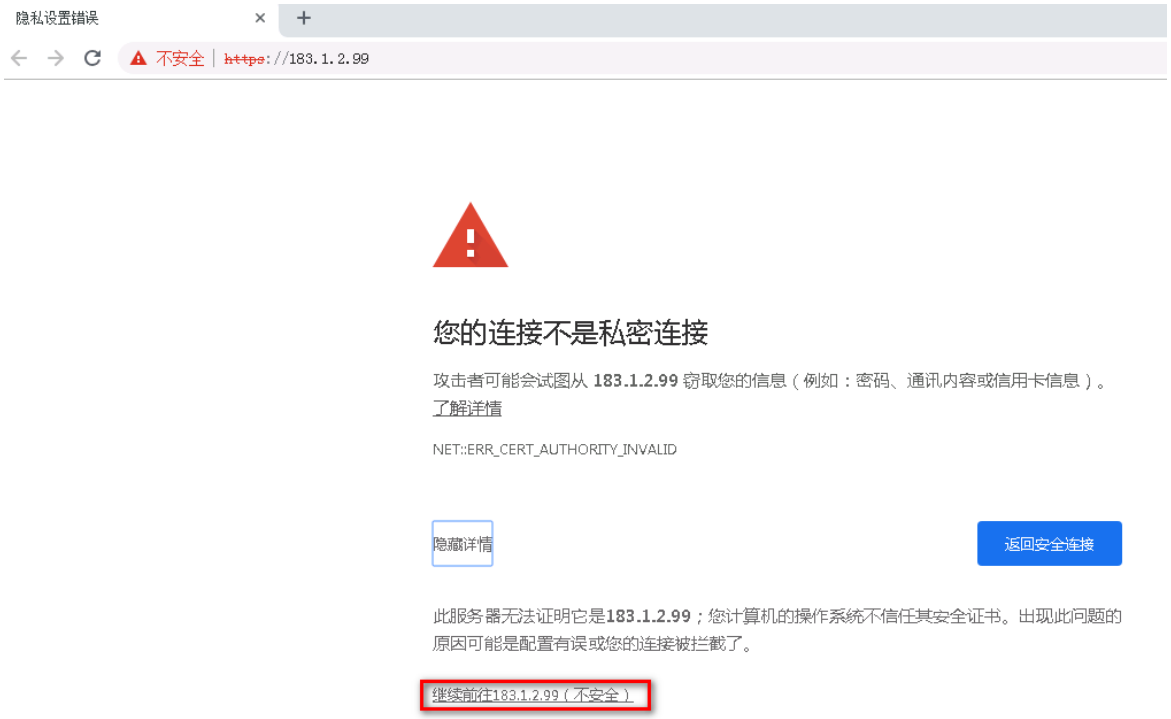
图E-56 route 命令帮助

```
[h3c-os]$ route
none cmd is set!
route usage:
        route -A/--add -i/--ip {ip} -m/--mask {mask} <[-g/--gateway {gateway}] [
-n/--interface {interface}]> [-t {metric}]
        route -D/--del -i/--ip {ip} -m/--mask {mask} [-g/--gateway {gateway}] [-
n/--interface {interface}] [-t {metric}]
        route -S/--show
[h3c-os]$
```

(21) 使用浏览器（以 Chrome 为例）访问虚拟 WAF 授权管理系统，管理地址为 https://183.1.2.99，点击高级，选择继续前往。

图E-57 访问登录页面

图E-58 访问登录页面



(22) 输入账号密码 admin/admin 登录授权管理系统。

图E-59 登录页面

(23) 进入授权管理系统之后，需要导入授权方可使用。

E.6 漏洞扫描授权服务器部署

E.6.1 授权服务器部署

1. 硬件规格

虚拟授权管理系统的硬件服务器规格如下表所示。

表E-3 虚拟授权管理系统硬件规格(仅支持在 CAS 5.0/7.0 平台下安装)

客户端个数	CPU	内存	硬盘
0-50	CPU 类型：不限制cpu 类型，确保分配 4 核	至少 2G	至少 25G
50-100		至少 4G	至少 40G
100-150		至少 4G	至少 50G
150-200		至少 8G	至少 64G
大于 200	暂不支持超过 200 个客户端		

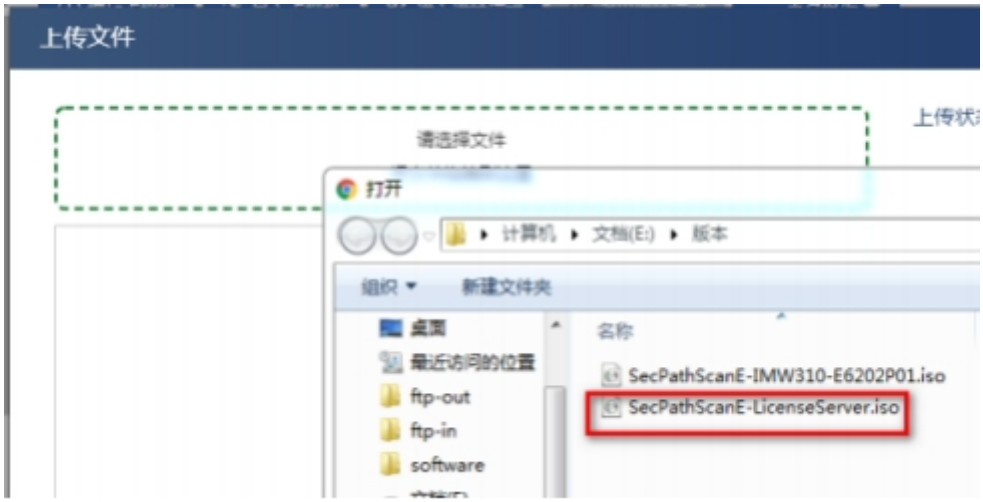
2. CAS 5.0/7.0 平台安装虚拟授权管理系统

(1) 上传镜像包。点击存储，选择目录，点击上传文件。

图E-60 图 3-1 上传镜像包

(2) 选择镜像包后，点击开始上传。

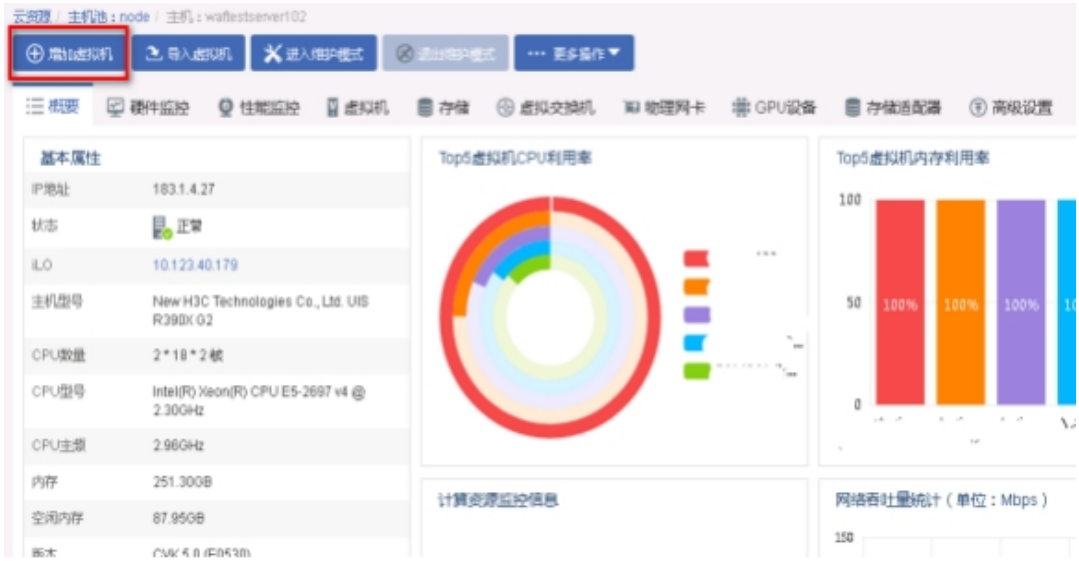
图E-61 选择镜像包



图E-62 查看上传的镜像包

(3) 点击增加虚拟机。

图E-63 增加虚拟机



(4) 设置虚拟机的显示名称，操作系统选择 Linux，版本选择 DebianGUN/Linux9(64 位)，CAStools 自动升级选择否。

图E-64 虚拟机基本配置

(5) 选择磁盘的总线类型为 IDE 硬盘，也可选择默认的高速磁盘。

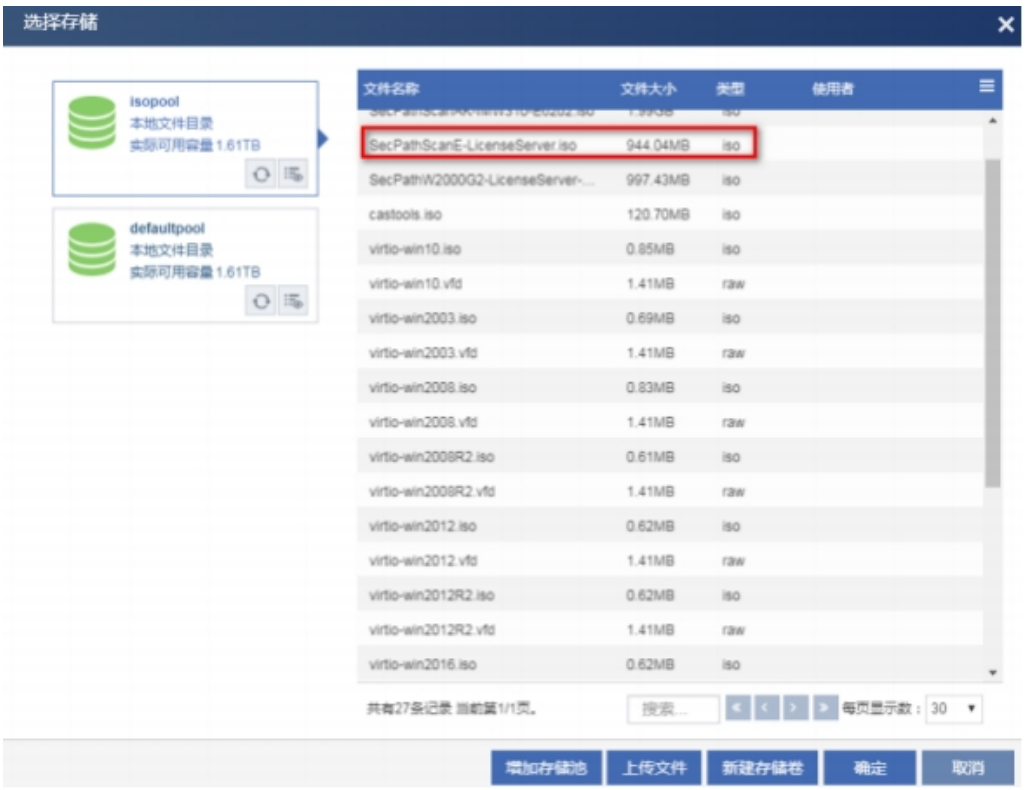
图E-65 设置磁盘的总线类型

(6) 选择光驱，点击光驱右侧的搜索。

图E-66 设置光驱

(7) 在文件目录中，选择镜像包，点击确定。

图E-67 选择镜像包



(8) 配置完成后，确认无误，点击完成。

图E-68 配置完成

(9) 修改虚拟机系统时间为本地时间，点击修改虚拟机，概要>高级设置>时钟设置，选择本地时钟，点击应用。

图E-69 修改虚拟机

图E-70 本地时钟

(10) 选择创建的虚拟机，点击启动。

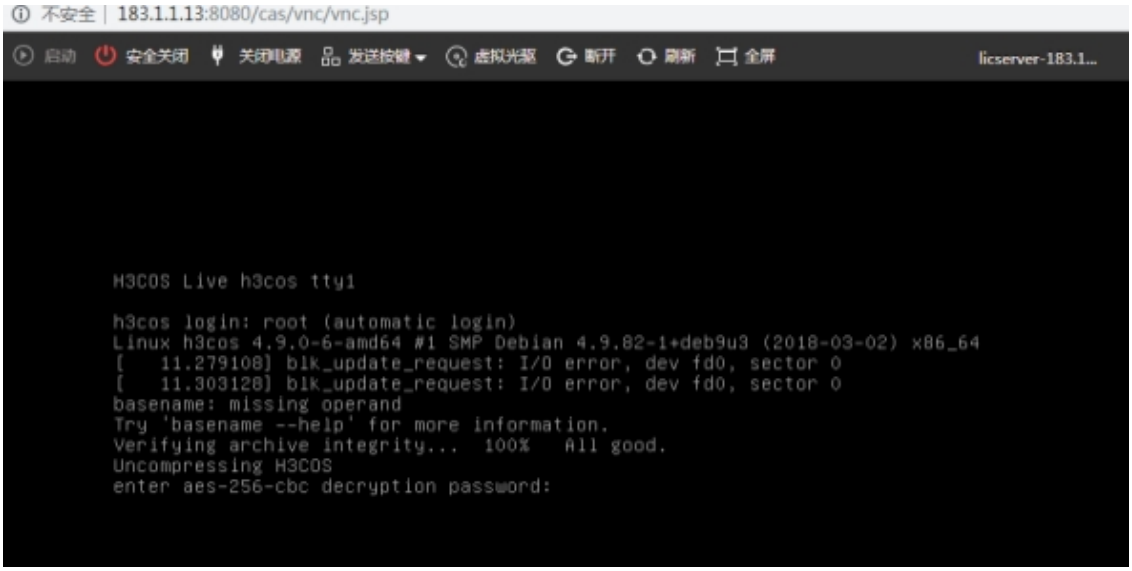
图E-71 启动虚拟机

(11) 点击控制台，进行安装。

图E-72 打开控制台

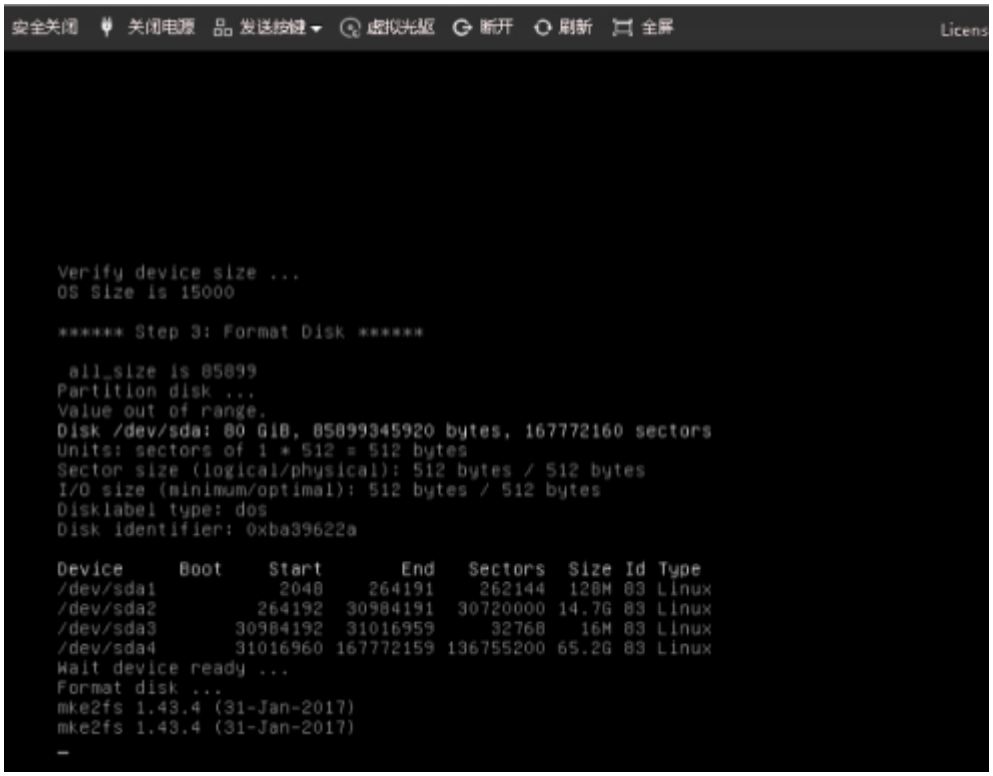
(12) 提示输入密码，输入刻盘密码 h3c++。

图E-73 输入刻盘密码



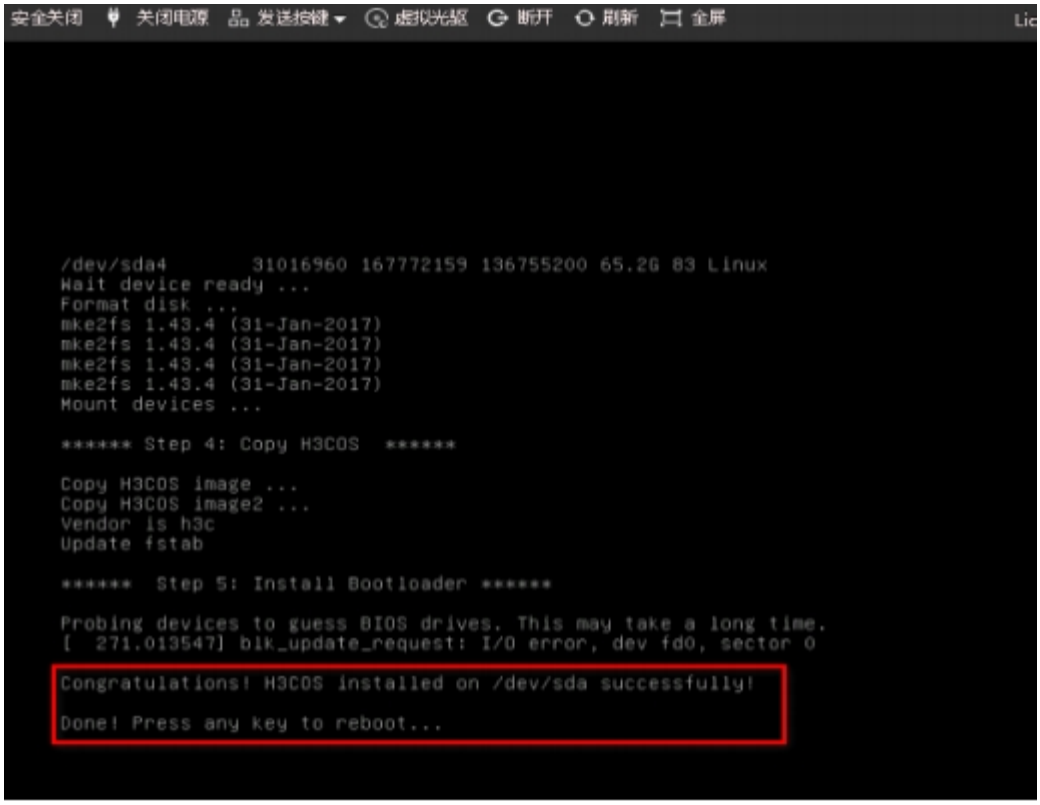
(13) 系统开始安装，一共五步，不需要手动参与，大概需要三到五分钟。

图E-74 开始安装



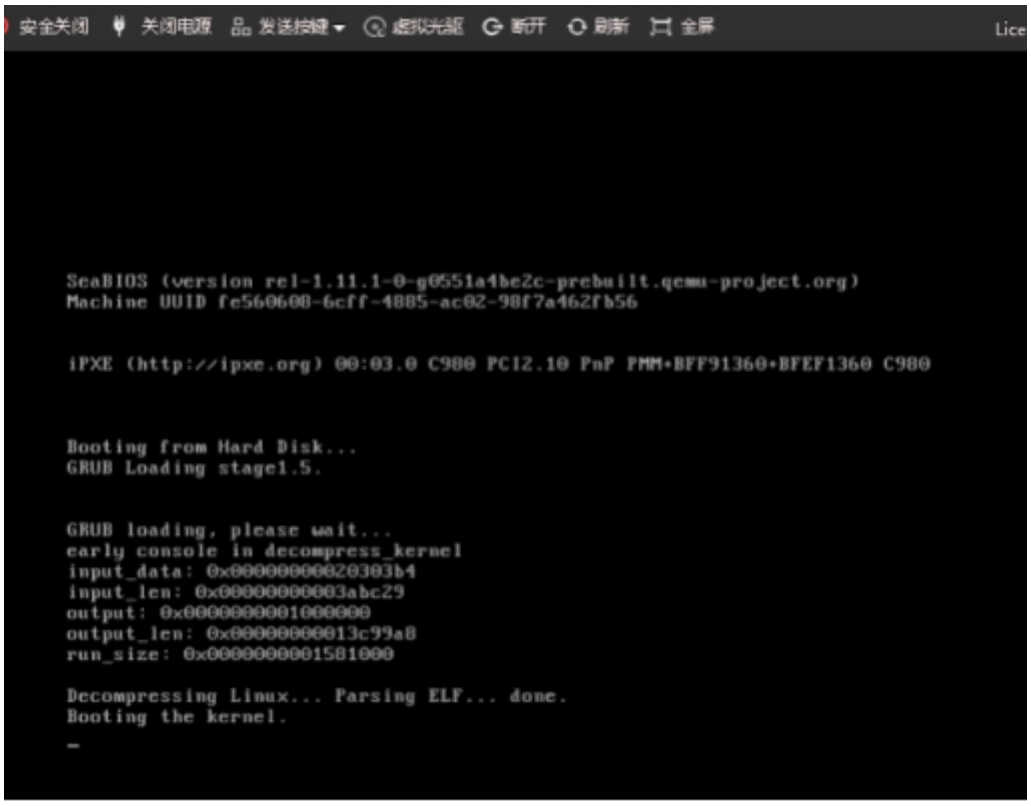
(14) 安装完成之后，出现提示“Congratulations! H3COS installed on /dev/sda successfully!”，按回车键，系统将自动重启。

图E-75 安装完成



(15) 重启后进行刻盘。

图E-76 重启系统

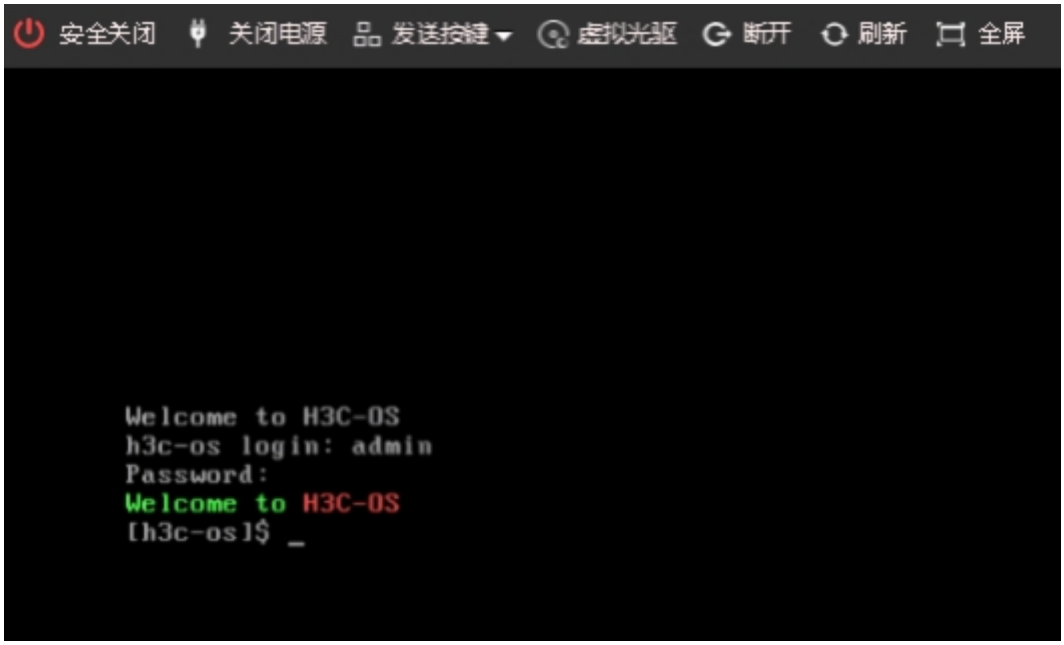


(16) 请耐心等待，刻盘结束后，会自动关闭机器，需要在 CAS 平台手动启动。此过程大约 40 分钟，请耐心等待。

图E-77 手动启动授权管理系统

(17) 在控制台下使用账号密码 admin/admin 登录系统。

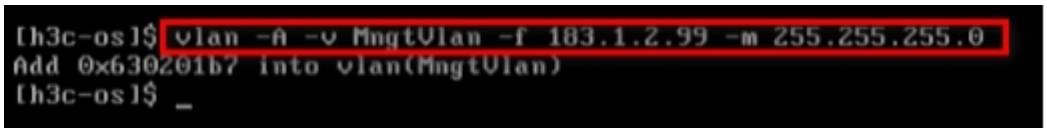
图E-78 登录成功



(18) 根据 CAS 平台的实际网络配置， 来配置授权管理系统的管理 IP 地址。命令如下：

```
vlan –A –v MngtVlan –f 183.1.2.99 –m 255.255.255.0
## 请根据实际组网情况合理配置管理地址
```

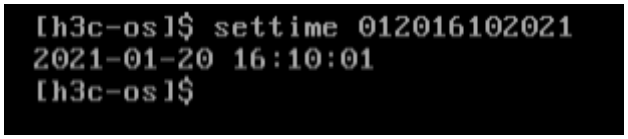
图E-79 配置 ip 地址



(19) 配置默认路由，命令如下：

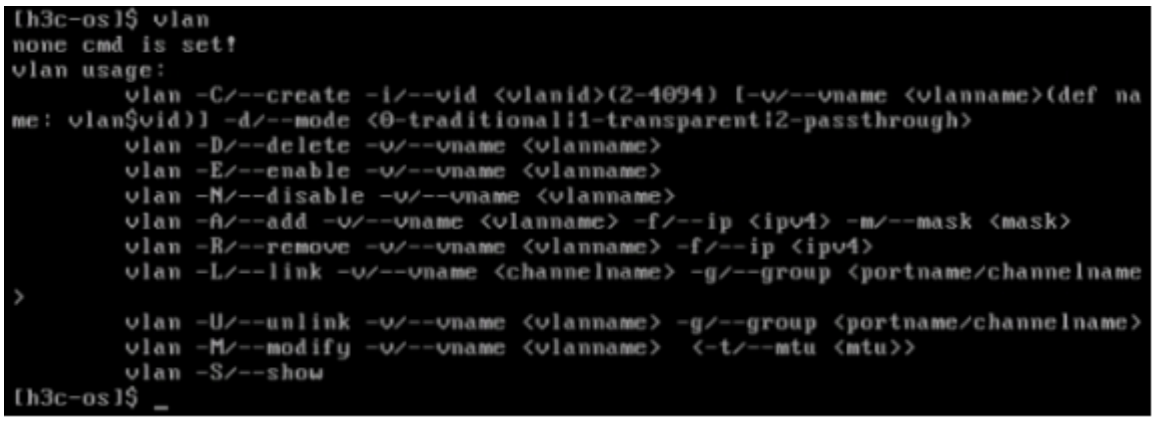
```
route –A – i 0.0.0.0 –m 0.0.0.0 –g 183.1.2.1
## 请根据实际组网情况合理配置路由
```

图E-80 添加系统时间

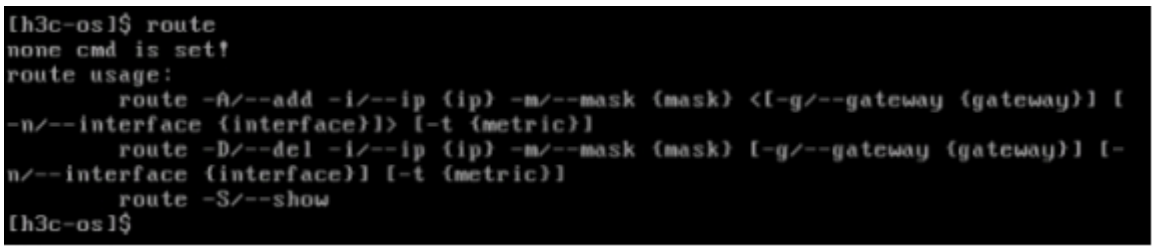


(20) 如果命令输入错误，导致 IP 或者路由配置错误，可以通过命令修改，查询 vlan 和 route 的命令格式，只需要输入 vlan 或者 route 即可。

图E-81 vlan 命令帮助

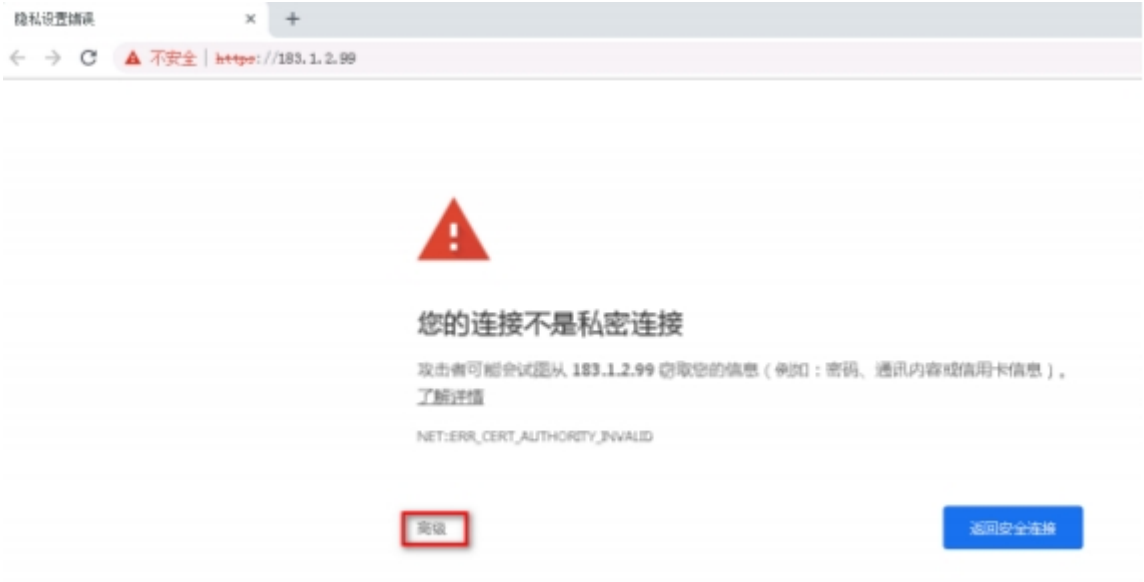


图E-82 route 命令帮助

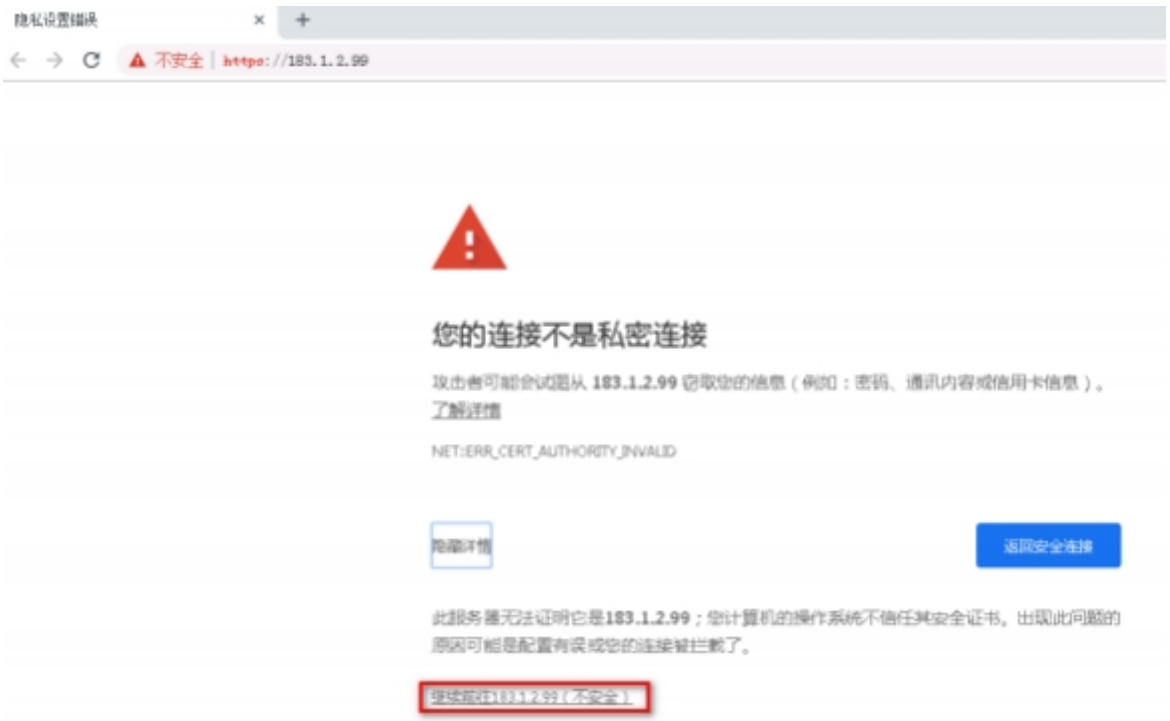


(21) 使用浏览器(以 Chrome 为例)访问虚拟授权管理系统，管理地址为 https://183.1.2.99，点击高级，选择继续前往。

图E-83 访问登录页面



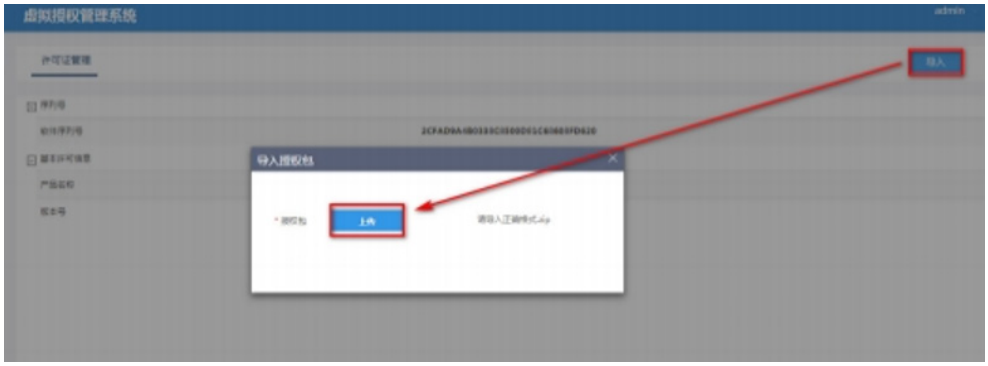
图E-84 访问登录页面



(22) 输入账号密码 admin/admin 登录授权管理系统。

图E-85 登录页面

(23) 进入授权管理系统之后， 需要导入授权方可使用。



E.6.2 漏扫虚拟机安装

1. 安装准备

本章节以 Cloud 漏扫的 ESS6202P01 版本镜像文件安装为例，支持在 CAS 5.0/7.0 版本上安装。

(1) E6202P01 版本建议适配 CAS 5.0/7.0 平台默认的磁盘类型(高速硬盘)；

(2) 下表为不同授权型号的 Cloud 漏扫对应的标配 CPU、内存、存储，可按照客户实际需要选择安装对应 Cloud 漏扫，确定安装授权型号后，需要确保所安装在的虚拟化系统上对应资源 足够使用。

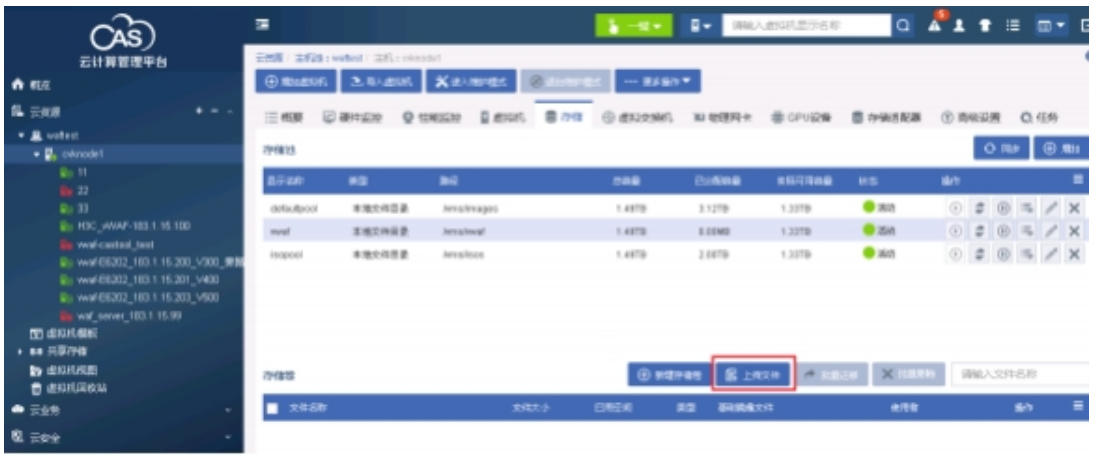
表E-4 Cloud 漏扫硬件配置要求

SysScan-Cloud 漏扫硬件配置要求表				
授权型号	标配CPU	标配内存	标配存储	适配的虚拟化系统
SysScan-Cloud-64	4核	8G	500GB	CAS 5.0/7.0
SysScan-Cloud-128	4核	16G	500GB	CAS 5.0/7.0
SysScan-Cloud-512	8核	24G	500GB	CAS 5.0/7.0
SysScan-Cloud-UL	8核	32G	500GB	CAS 5.0/7.0
注意：授权规格叠加上限	16核	64G	500GB	CAS 5.0/7.0

2. CAS 5.0/7.0 平台软件安装指导

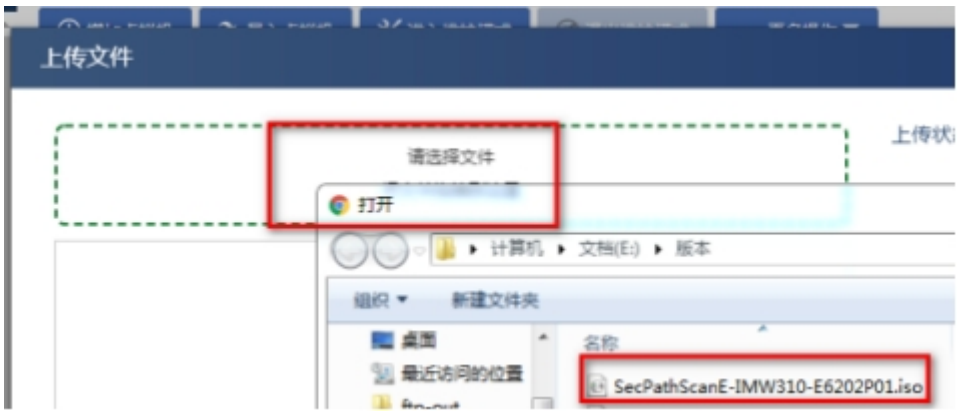
(1)　登录到 CAS 平台，上传 ISO 镜像文件，选择存储，点击上传文件。如下图所示：

图E-86 存储池



(2)　从本地选择需要上传的 ISO 文件，并开始上传，以 6202P01 版本镜像文件为例。如下图所示：

图E-87 ISO 文件信息



将文件拖放到虚线框内，显示文件名。 点击开始上传。如下图所示：

图E-88 上传文件

上传完成后，关闭上传页面，在该存储池中可以查看到文件信息。如下图所示：

图E-89 上传的 ISO 信息

(3) 镜像文件上传完成后，点击新增虚拟机。如下图所示：

图E-90 新增虚拟机

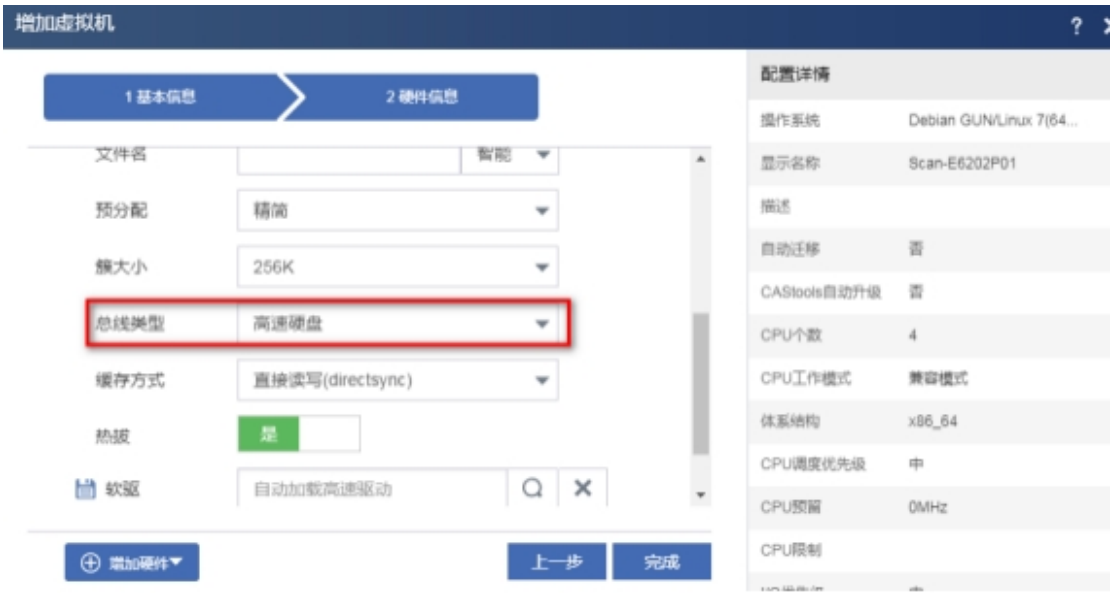
(4) 填写虚拟机名称 Scan-E6202P01，操作系统选择 Linux，版本选择 Debian GUN/Linux 7(64 位)，CAStools 自动升级选择为否，点击下一步。如下图所示。

图E-91 虚拟机基本配置

(5) 本文档以安装 SysScan-Cloud-64 授权型号的虚拟漏扫为例，因此，根据“表 E-3 Cloud 漏扫硬件配置要求”，配置 CPU 为4核， 内存为8G，网络配置根据 CAS 的实际情况进行配，磁盘为 500G(建议适配 CAS 平台默认的磁盘类型(高速硬盘))。如下图所示：

图E-92 虚拟漏扫基本配置

图E-93 虚拟漏扫硬盘配置



(6) 配置完成 CPU、内存、网络、磁盘、光驱后，点击完成。如下图所示：

图E-94 虚拟机配置

(7) 修改虚拟机系统时间为本地时间，点击修改虚拟机，概要>高级设置>时钟设置，选择本地时钟，点击应用。

图E-95 修改虚拟机

图E-96 本地时钟

(8) 启动虚拟机，选中新建的虚拟机，点击启动。如下图所示：

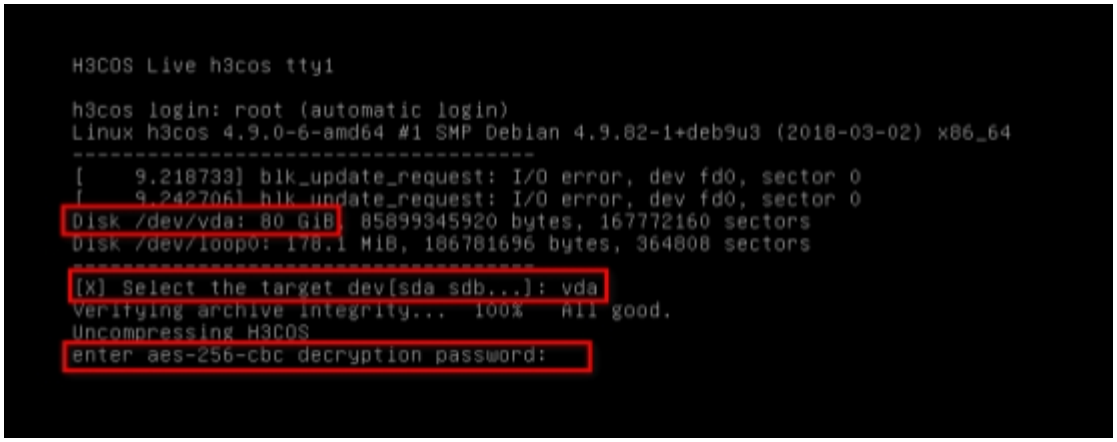
图E-97 启动虚拟机

(9) 点击控制台。如下图所示：

图E-98 打开控制台

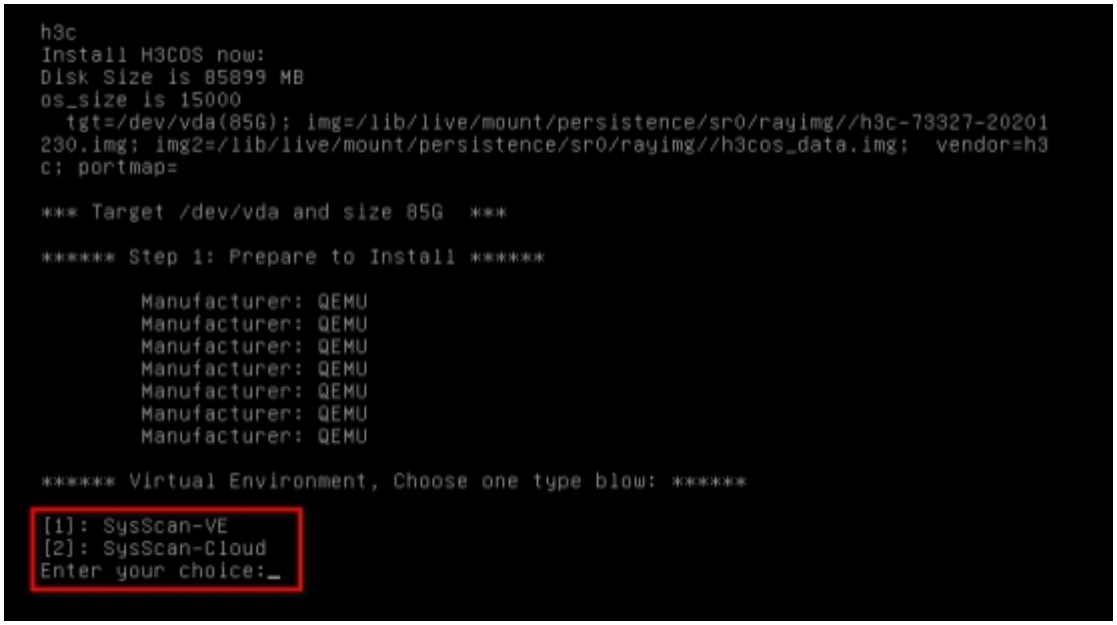
(10) 进入到虚拟机控制台，出现安装界面， 选择安装目标盘类型为 vda(高速硬盘对应为 vda)，回车后再输入安装密码 h3c++ ，如下图所示：

图E-99 安装盘类型选择与输入安装密码



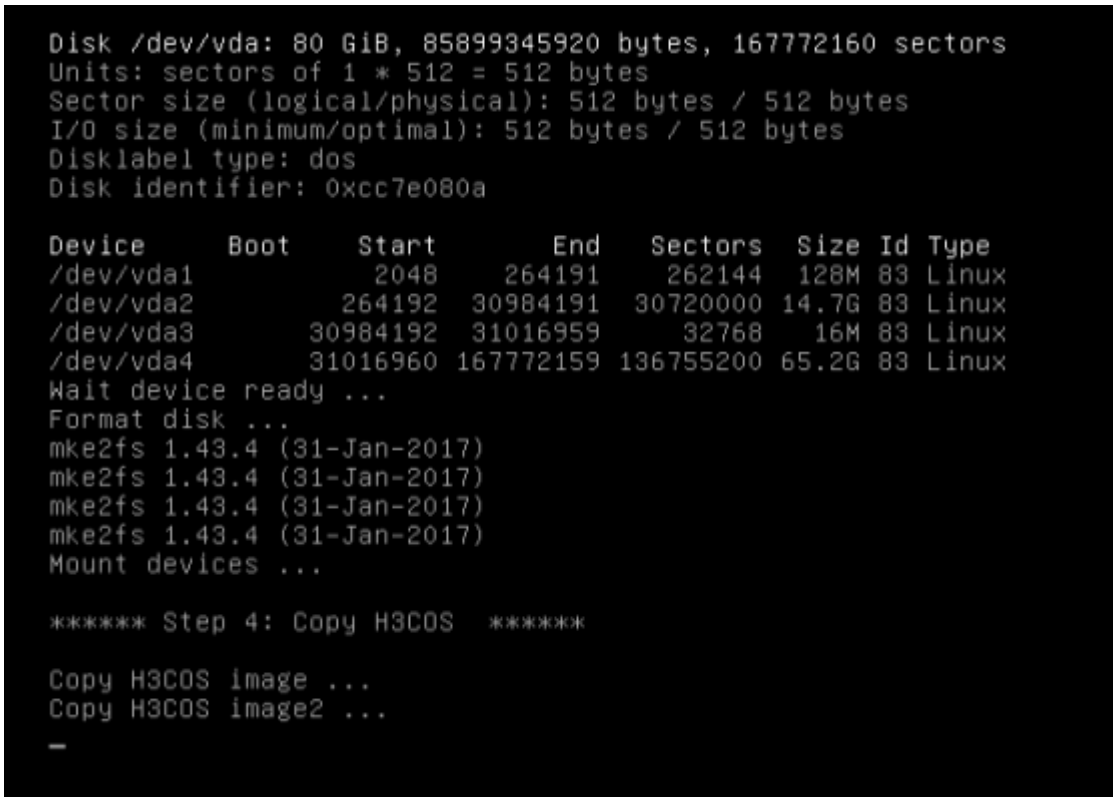
(11) 选择安装方式， 有两种安装安装方式，VE 生产方式 选择 1 ；cloud 生产方式选择 2 ，本此安装选择 2，按回车键进入安装页面。如下图所示：

图E-100 选择安装方式 SysScan-Cloud



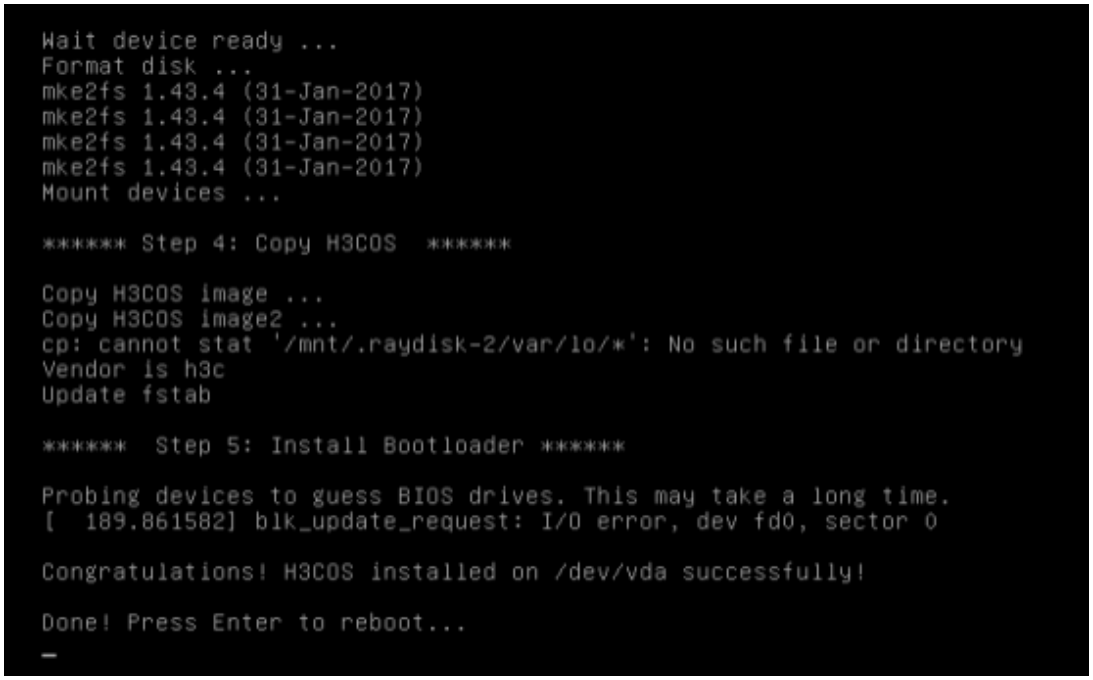
(12) 系统开始安装，一共五步，不需要手动参与， 大概需要五分钟左右。如下图所示：

图E-101 安装界面



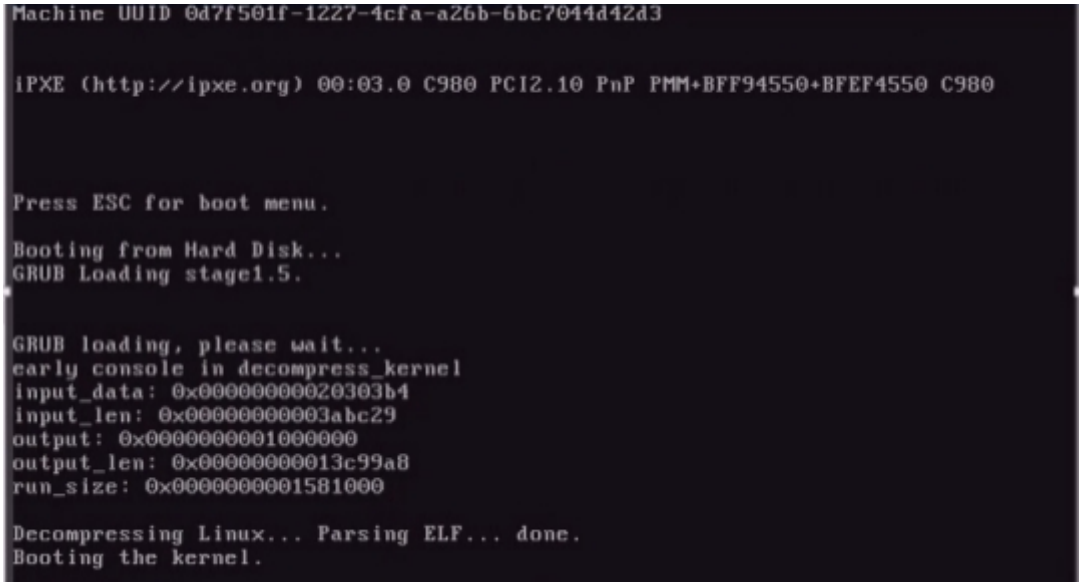
(13) 安装完成之后，出现提示“Congratulations! H3COS installed on /dev/sda successfully!”，提示按 enter 键重启。如下图所示：

图E-102 系统安装完成提示



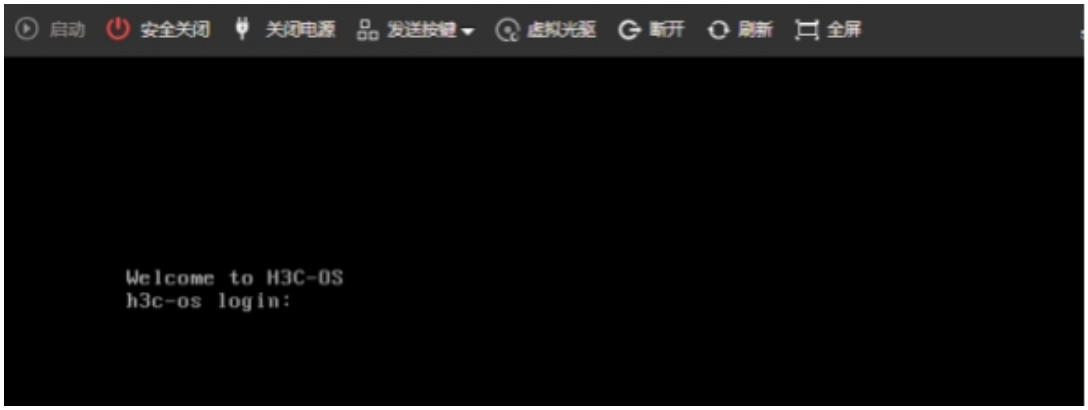
(14) 虚拟漏扫重启系统，进入“Bootingthe kernel”阶段，不需要手动参与， 与 CAS 硬件资源有关，时间约 40 分钟左右，若 CAS 性能较好，安装时间较快，此处时间仅供参考，请耐心等 待。如下图所示。

图E-103 重启虚拟漏扫



(15) “Bootingthe kernel”之后的一段时间， 控制台将没有输出， 结束之后系统会自动关机，重启设备，当出现 H3C login 时，表明系统安装完成。 如下图所示：

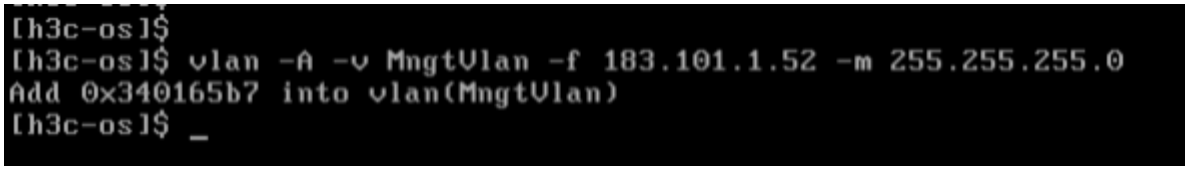
图E-104 系统关机界面



(16) 使用账号密码 admin/admin 登录漏扫，根据 CAS 平台的实际网络配置，来配置虚拟漏扫的管理 IP 地址。命令如下：

```
vlan –A –v MngtVlan –f 183.101.1.52 –m 255.255.255.0
```

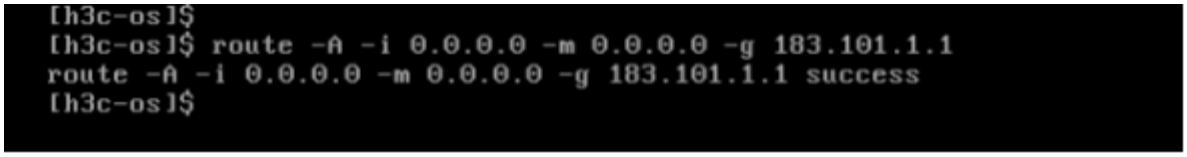
图E-105 配置管理 IP



配置默认路由，命令如下：

```
route –A – i 0.0.0.0 –m 0.0.0.0 –g 183.101.1.1
```

图E-106 配置默认路由



(17) 配置好磁盘类型后， 配置光驱，点击光驱右侧的搜索按钮，选择上传的 ISO 镜像文件，并点击确定。如下图所示：

图E-107 点击光驱的搜索按钮

图E-108 选择 ISO 镜像文件

(18) 如果命令输入错误，导致 IP 或者路由配置错误，可以通过命令修改，查询 vlan 和 route 的命令格式， 只需要输入 vlan 或者 route 回车即可。 如下图所示：

图E-109 vlan 命令帮助

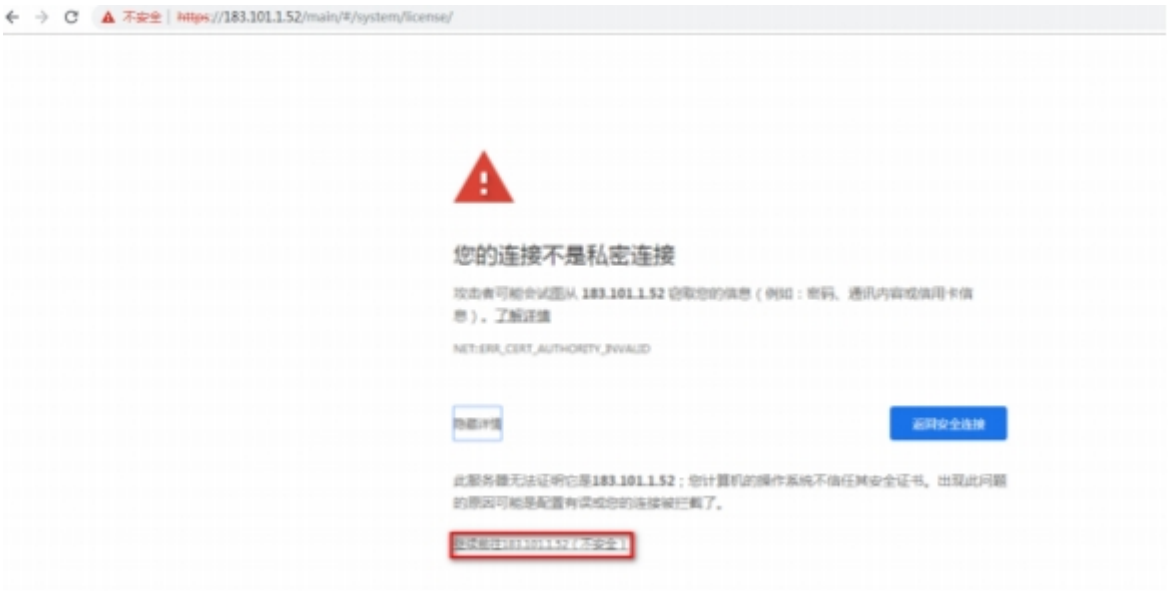
```
[h3c-os]$ vlan
none cmd is set!
vlan usage:
        vlan -C/--create -i/--vid <vlanid>(2-4094) [-v/--vname <vlanname>(def na
me: vlan$vid)] -d/--mode <0-traditional>
        vlan -D/--delete -v/--vname <vlanname>
        vlan -E/--enable -v/--vname <vlanname>
        vlan -N/--disable -v/--vname <vlanname>
        vlan -A/--add -v/--vname <vlanname> -f/--ip <ipv4> -m/--mask <mask>
        vlan -R/--remove -v/--vname <vlanname> -f/--ip <ipv4>
        vlan -L/--link -v/--vname <channelname> -g/--group <portname/channelname
>
        vlan -U/--unlink -v/--vname <vlanname> -g/--group <portname/channelname>
        vlan -M/--modify -v/--vname <vlanname>  <-t/--mtu <mtu>>
        vlan -S/--display
[h3c-os]$
```

图E-110 route 命令帮助

```
[h3c-os]$ route
none cmd is set!
route usage:
        route -A/--add -i/--ip {ip} -m/--mask {mask} <[-g/--gateway {gateway}] [
-n/--interface {interface}]> [-t {metric}]
        route -D/--del -i/--ip {ip} -m/--mask {mask} [-g/--gateway {gateway}] [-
n/--interface {interface}] [-t {metric}]
        route -S/--display
[h3c-os]$
```

(19) 使用浏览器 (推荐使用谷歌浏览器) 访问漏扫的 Web 管理页面，管理地址为 https://183.101.1.52，点击继续前往。如下图所示：

图E-111 访问 Web 管理页面



(20) 使用账号密码 account/account 登录系统。 如下图所示：

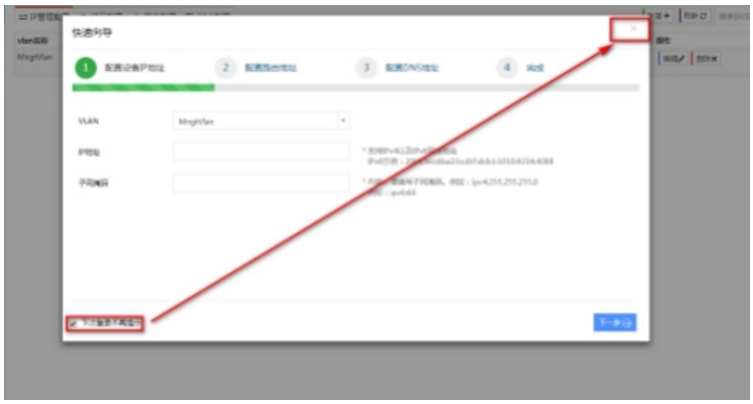
图E-112 登录虚拟漏扫

说明

首次使用 account/account 登录需要强制修改默认密码,后续涉及的登录操作，需使用更改后的密码进行登录。

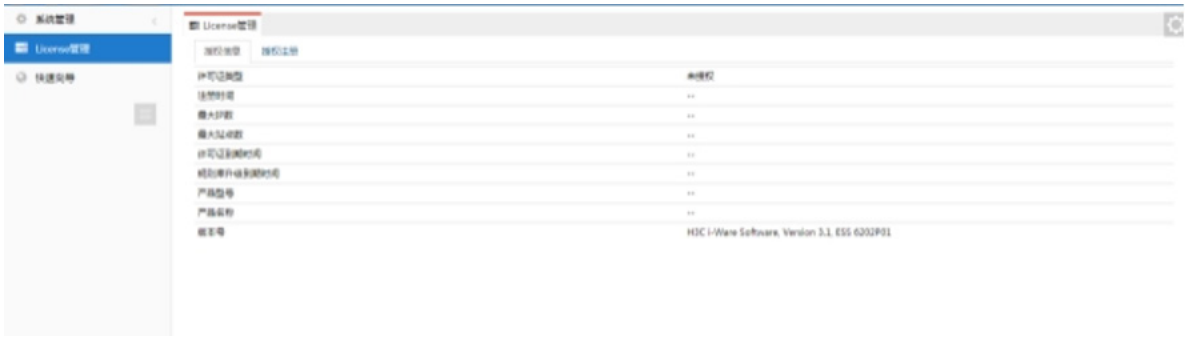
(21) 登录系统后，进入快速向导，由于已在命令行界面配置完成，故选择下次登录不再提示， 点击关闭。如下图所示：

图E-113 关闭快速向导



(22) 进入 License 管理界面后，查看版本号。如下图所示：

图E-114 查看漏洞扫描系统信息



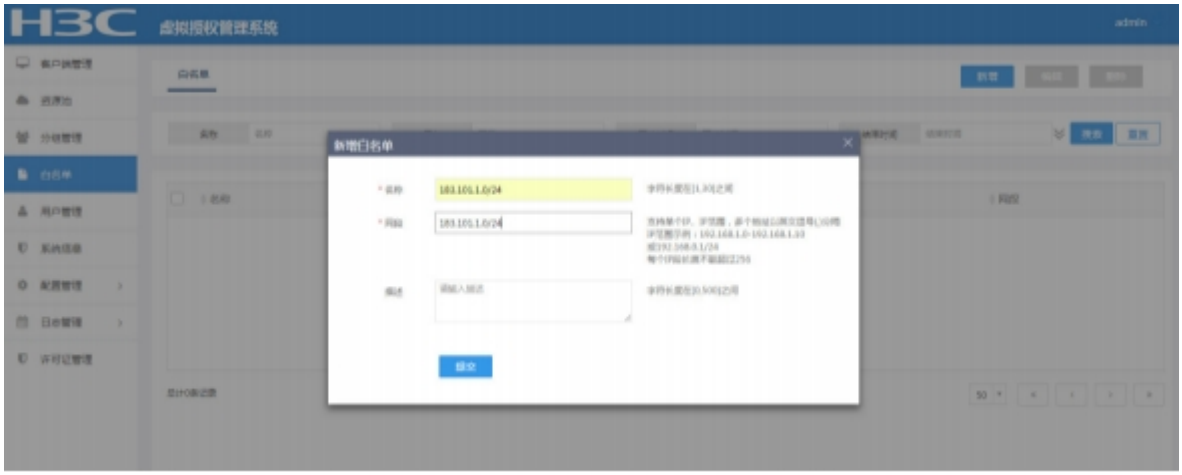
说明

Cloud 漏扫默认不含有授权，需要先在 License Server 上注册授权，才能显示产品型号以及其它功能选项。

3. 漏扫在 License Server 上注册授权

(1) License server 已导入授权，登录 License server，默认用户名密码为： admin/admin，配置漏扫所在网段白名单。

图E-115 注册授权服务器

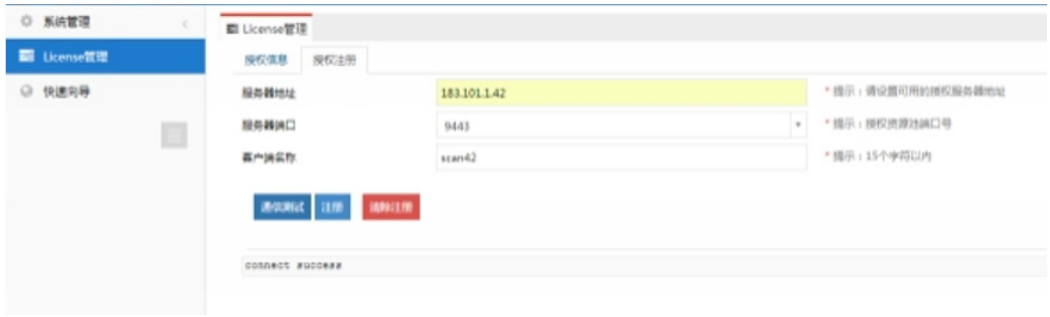


(2) 登录漏扫，进入 License 管理>授权注册界面，配置服务器地址、服务器端口、客户端名称。如下图所示：

图E-116 注册授权服务器

点击通信测试，显示“connect success”表示连接正常。

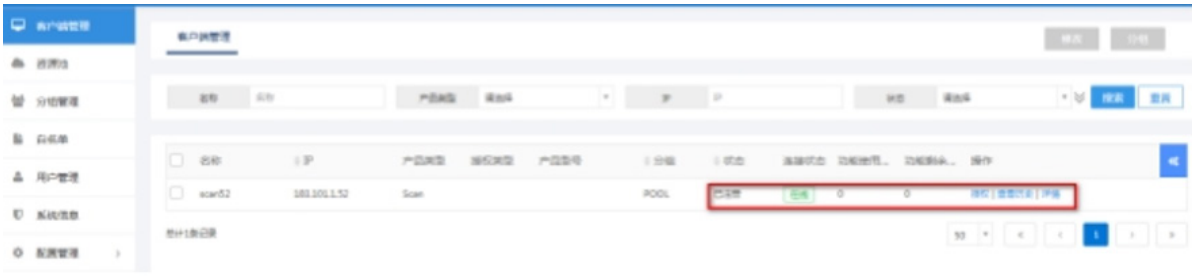
图E-117 通信测试



图E-118 注册

(3) License server 资源池界面显示已注册漏扫，具体可参考授权管理系统 Web 配置指导。

图E-119 漏扫在授权服务器上注册成功



点击授权，可对漏扫进行授权。

(4) 授权成功后， 漏扫 License 管理>授权信息界面，显示授权信息。

图E-120 漏扫授权成功

E.7 态势感知部署

E.7.1 系统安装

1. 资源信息

设备描述	资源要求	网络要求	部署位置
态势感知	32核CPU、128G内存、600G+2*4T磁盘、1张网卡	1、UCA访问虚拟机同步租户和资产、漏扫报告，访问端口443,9999	DMZ
Casagent	4核CPU、8G内存、300G磁盘、1张网卡	1、 uca访问casagent同步租户信息，获取token，分别使用端口10000 2 、态势虚拟机访问casagent进行token验证登录，使用443/8443	DMZ

2. 态势感知安装

新建虚拟机

(1) 上传镜像至 VKS 存储。

说明

H3Linux_k310_V111_Patch1.iso 是用来部署态势感知所需要的虚机操作系统;

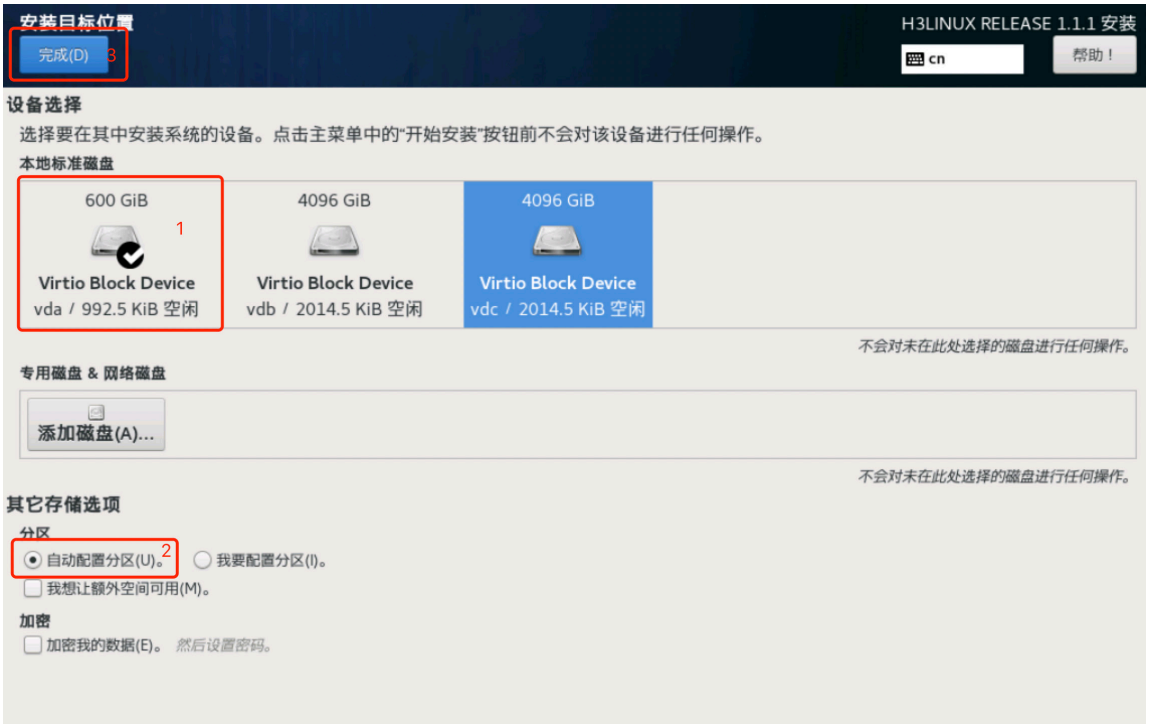
SecCloudOMP-E1115.iso 是用来部署应用于态势感进行单点登录的 CAS Server 虚机。

(2) 创建部署态势感知所需要的虚拟机

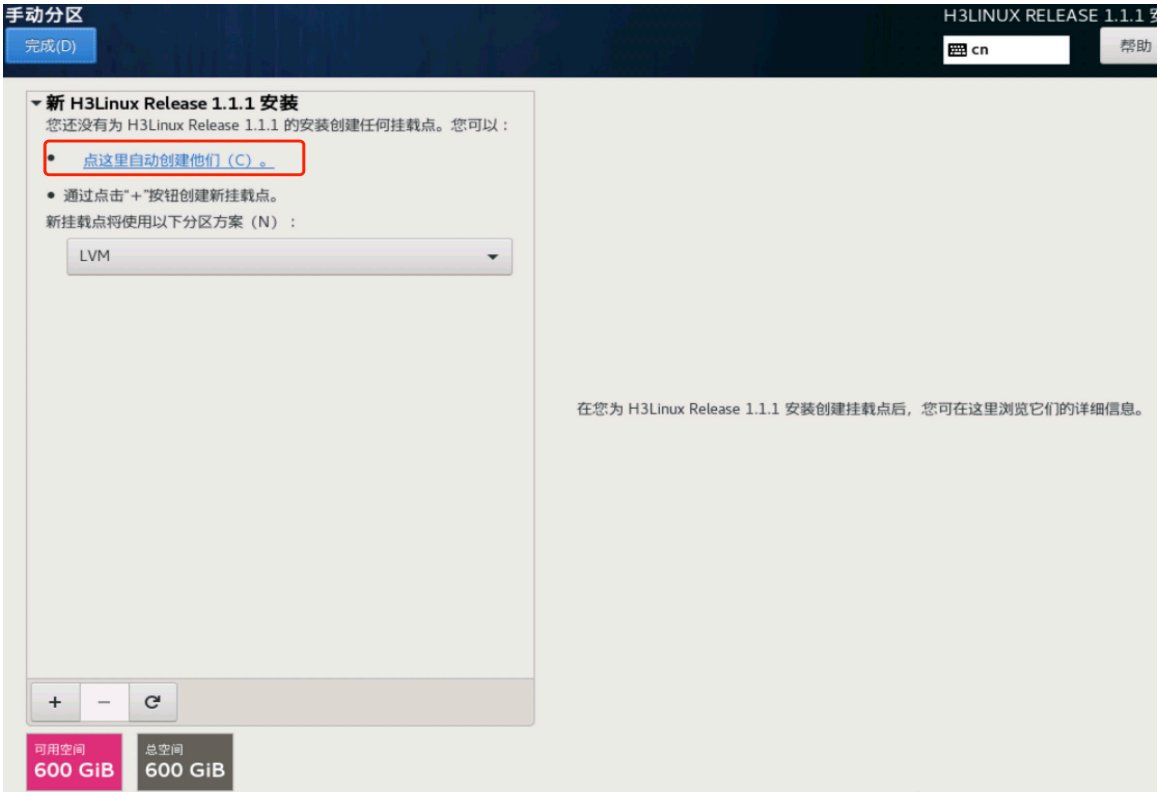
根据虚拟机要求创建态势感知安全虚机。

(3)　系统安装

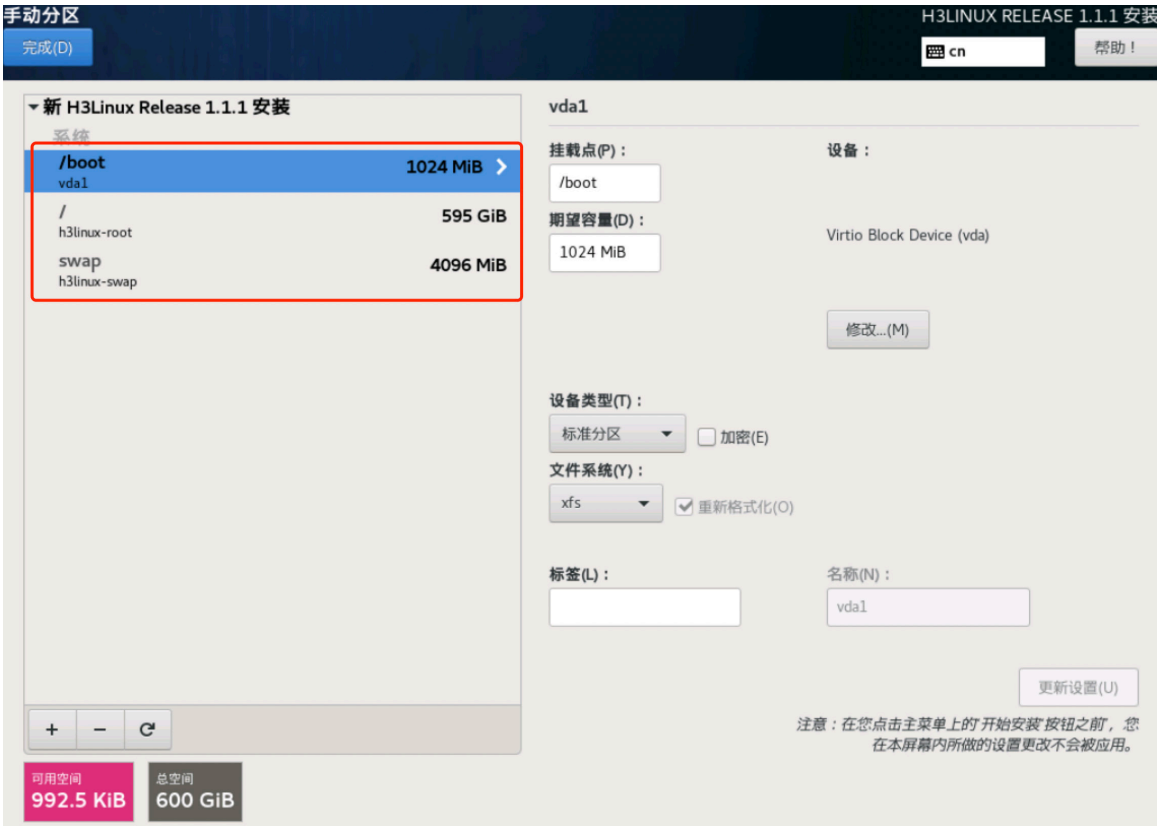
本地标准磁盘只勾选 600G 磁盘，选择自动配置分区后，点击完成。



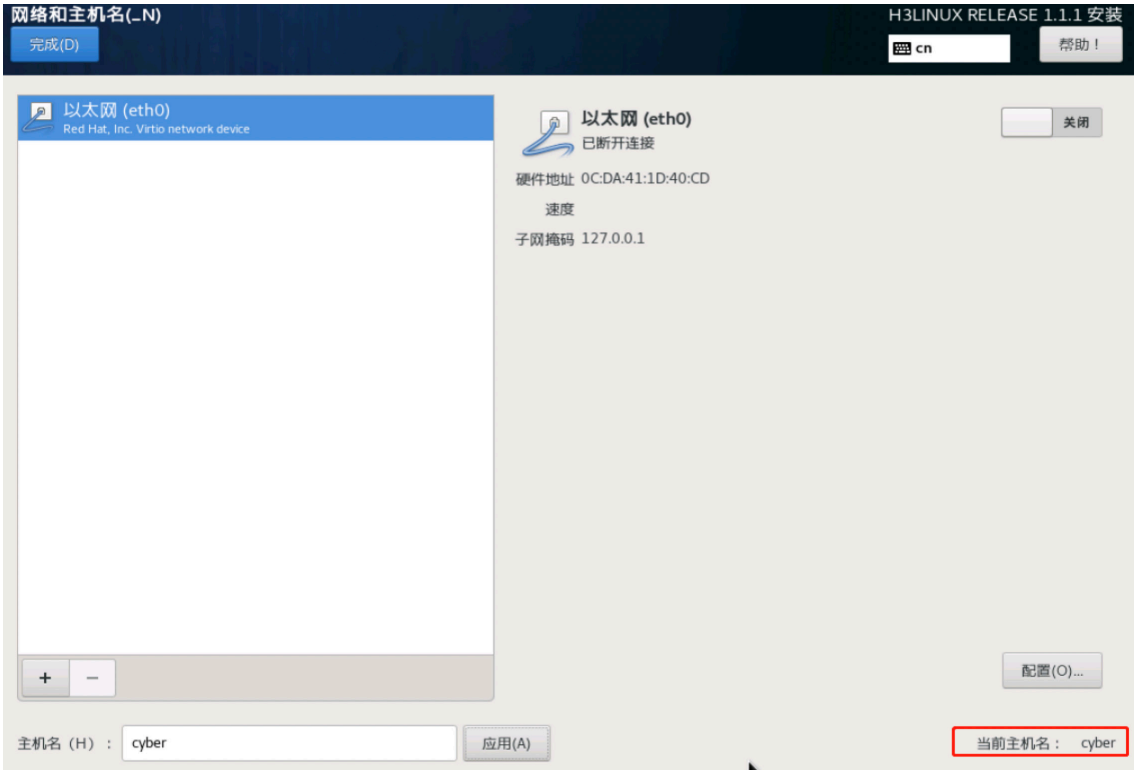
点击“点这里自动创建他们（C）。”



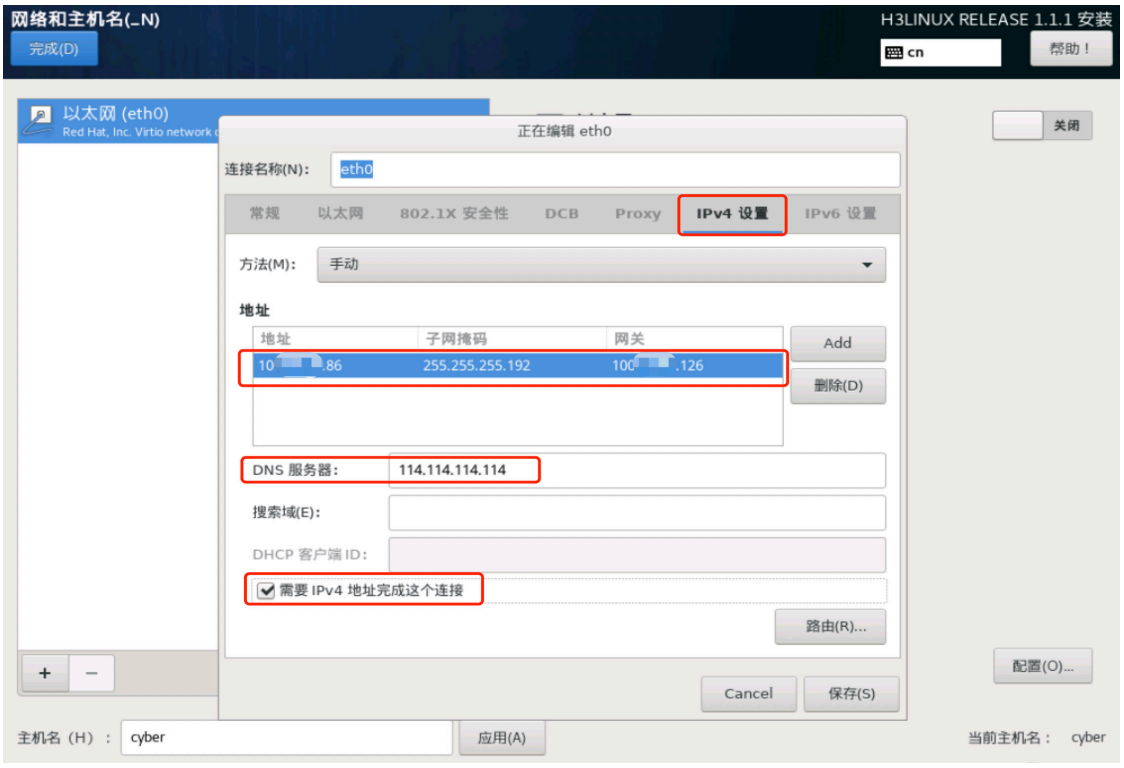
分区要求：/boot 1G、/ 595G、swap 4G

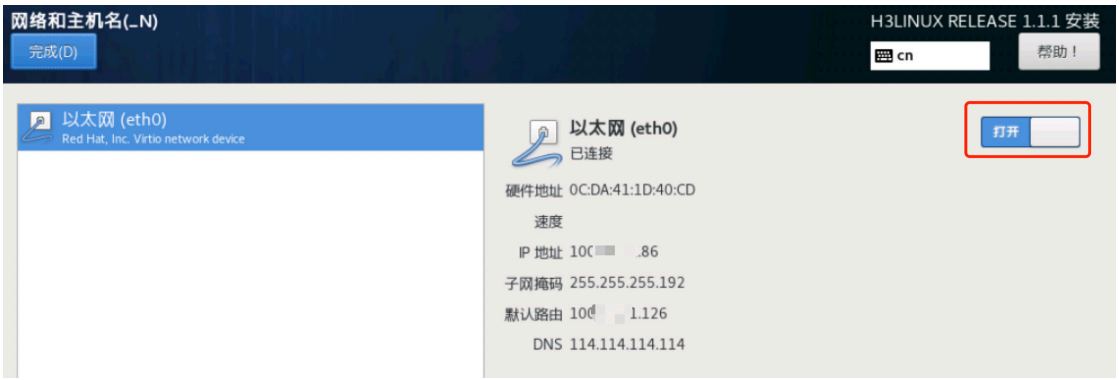


更改主机名为 cyber（主机名为必须更改项，且必须为 cyber）

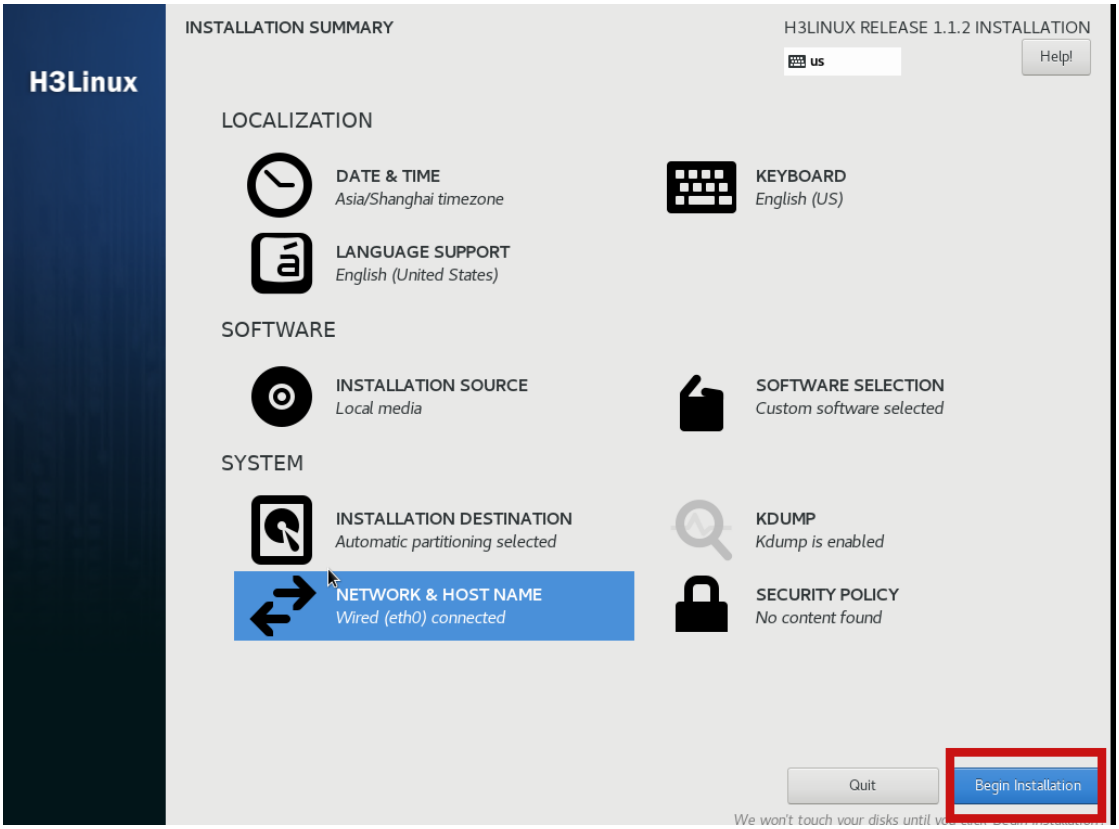

网络和主机名(_N)
完成(D)
H3LINUX RELEASE 1.1.1 安装
cn
帮助！
以太网 (eth0)
Red Hat, Inc. Virtio network device
以太网 (eth0)
已断开连接
关闭
硬件地址 0C:DA:41:1D:40:CD
速度
子网掩码 127.0.0.1
配置(O)...
主机名（H）：
cyber
应用(A)
当前主机名： cyber

更改网络配置


网络和主机名(_N)
完成(D)
H3LINUX RELEASE 1.1.1 安装
cn
帮助！
以太网 (eth0)
正在编辑 eth0
关闭
连接名称(N):
eth0
常规
以太网
802.1X 安全性
DCB
Proxy
IPv4 设置
IPv6 设置
方法(M):
手动
地址
地址
子网掩码
网关
Add
255.255.255.192
删除(D)
DNS 服务器:
114.114.114.114
搜索域(E):
DHCP 客户端 ID:
需要 IPv4 地址完成这个连接
路由(R)...
Cancel
保存(S)
配置(O)...
主机名（H）：
cyber
应用(A)
当前主机名： cyber



点击“完成”后开始安装系统。（密码必须设置为 csap_H3C@yunzhi）

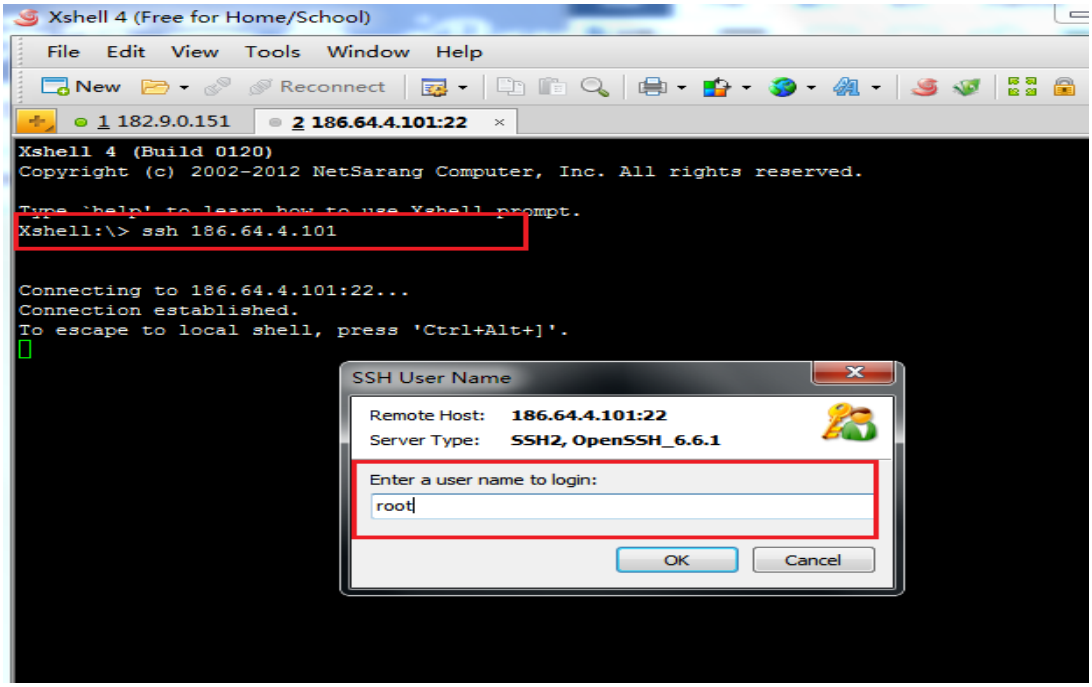


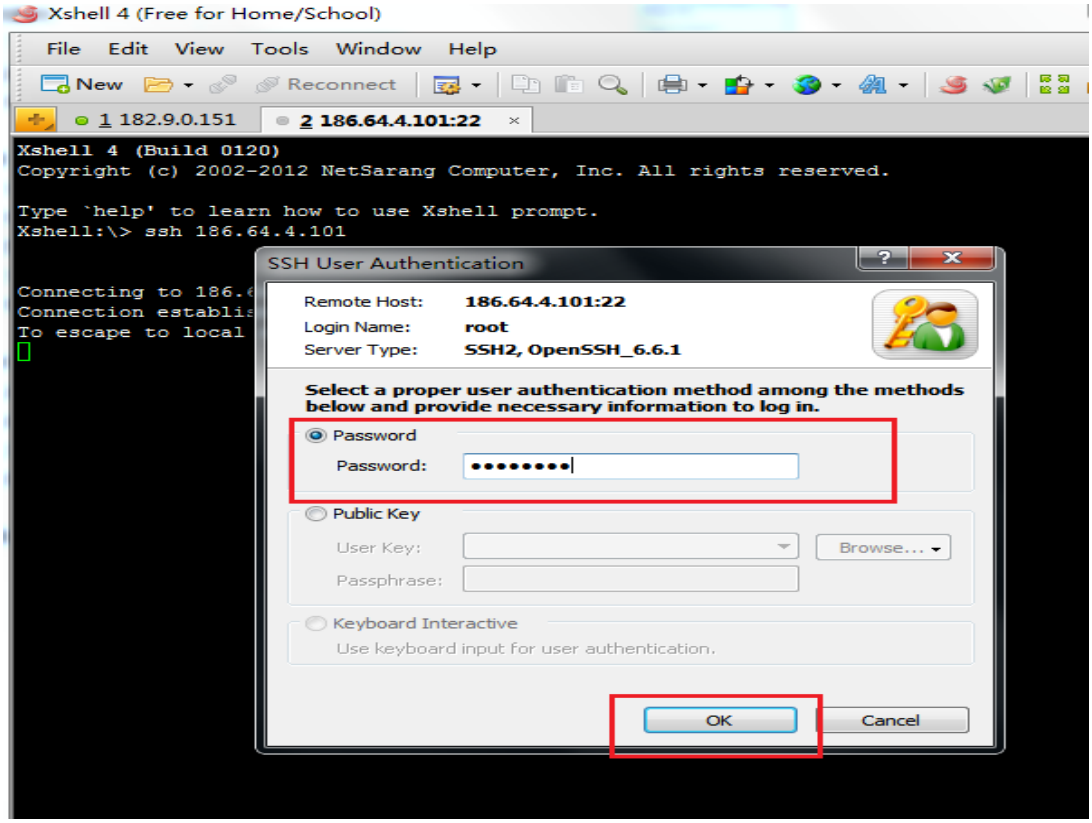
挂载磁盘

态势感知单机版，需要对两块 4T 硬盘进行挂载操作。可以通过 VNC 或 ssh 登录操作。

(4)　ssh 连接服务器

在 ssh 工具中直接输入：ssh 服务器 IP(如 ssh 186.64.4.101)，然后根据提示输入用户名（root）和密码（csap_H3C@yunzhi），如下图所示。





(5) 查看磁盘信息

通过命令 fdisk –l 当前服务器硬盘和分区情况，正常情况下会出现如下信息,确认 /dev/vdb ,/dev/vdc 这两块硬盘是否正常。

```
[root@cyber ~]# fdisk -l
```

```
磁盘 /dev/vdb：4398.0 GB, 4398046511104 字节，8589934592 个扇区
Units = 扇区 of 1 * 512 = 512 bytes
扇区大小(逻辑/物理)：512 字节 / 512 字节
I/O 大小(最小/最佳)：512 字节 / 512 字节

磁盘 /dev/vdc：4398.0 GB, 4398046511104 字节，8589934592 个扇区
Units = 扇区 of 1 * 512 = 512 bytes
扇区大小(逻辑/物理)：512 字节 / 512 字节
I/O 大小(最小/最佳)：512 字节 / 512 字节
```

(6) 创建物理卷

使用命令:pvcreate 将磁盘/dev/sdb，/dev/sdc 创建成物理卷，然后使用命令 pvs 或 pvdisplay 查看创建的物理卷。

```
[root@cyber ~]# pvcreate /dev/ vdb
Physical volume "/dev/vdb successfully created
[root@cyber ~]# pvcreate /dev/vdc
Physical volume "/dev/vdc successfully created
[root@cyber ~]# pvdisplay
```

```
  --- Physical volume ---
  PV Name               /dev/vdb
  VG Name               es_file
  PV Size               4.00 TiB / not usable 4.00 MiB
  Allocatable           yes (but full)
  PE Size               4.00 MiB
  Total PE              1048575
  Free PE               0
  Allocated PE          1048575
  PV UUID               1H8pJI-nyrQ-Hd6F-wHgi-Kbb8-v5Ss-oBoVbK

  --- Physical volume ---
  PV Name               /dev/vdc
  VG Name               es_file
  PV Size               4.00 TiB / not usable 4.00 MiB
  Allocatable           yes
  PE Size               4.00 MiB
  Total PE              1048575
  Free PE               131070
  Allocated PE          917505
  PV UUID               fDMHXB-epto-Ye1r-cQyP-p5rj-OSWt-c7xdtd
```

(7) 创建卷组

物理卷创建好之后，使用命令 vgcreate 创建卷组 es_file，并将物理卷/dev/vdb /dev/vdc 加入到卷组中，若将多个物理卷加入卷组中，只需将物理卷路径以空格分隔添加在后面即可。创建完成后使用命令 vgdisplay 查看卷组信息。

```
[root@cyber ~]# vgcreate es_file /dev/vdb /dev/vdc
Volume group es_file" successfully created
```

```
[root@cyber ~]# vgdisplay
```

```
  --- Volume group ---
  VG Name               es_file
  System ID
  Format                lvm2
  Metadata Areas        2
  Metadata Sequence No  2
  VG Access             read/write
  VG Status             resizable
  MAX LV                0
  Cur LV                1
  Open LV               1
  Max PV                0
  Cur PV                2
  Act PV                2
  VG Size               <8.00 TiB
  PE Size               4.00 MiB
  Total PE              2097150
  Alloc PE / Size       1966080 / 7.50 TiB
  Free  PE / Size       131070 / 511.99 GiB
  VG UUID               LBbDHo-GJxb-KQ9j-XmZ5-6hzw-RBDZ-fkoP74
```

(8) 创建逻辑卷

使用命令 lvcreate 创建逻辑卷，创建逻辑卷时需要使用-L 制定逻辑卷大小，使用-n 指定逻辑卷名字并指定卷组的名称。创建完成之后使用 lvdisplay 查看逻辑卷信息。

```
[root@cyber ~] lvcreate -L 7.5T -n data es_file
WARNING: xfs signature detected on /dev/es_file/data at offset 0. Wipe it? [y/n]: y

Wiping xfs signature on /dev/es_file/data
Logical volume "data" created
[root@cyber /]# lvdisplay
```

```
  --- Logical volume ---
  LV Path                /dev/es_file/data
  LV Name                data
  VG Name                es_file
  LV UUID                wnxKyn-ehUU-fRMA-OFJZ-Ymk4-raFX-gDgezs
  LV Write Access        read/write
  LV Creation host, time cyber, 2021-12-30 15:30:00 +0800
  LV Status              available
  # open                 1
  LV Size                7.50 TiB
  Current LE             1966080
  Segments               2
  Allocation             inherit
  Read ahead sectors     auto
  - currently set to     8192
  Block device           253:2
```

(9) 创建文件系统

逻辑卷 data 创建好之后，创建文件系统。

```
[root@cyber ~]# mkfs.xfs /dev/es_file/data
meta-data=/dev/es_file/data      isize=512    agcount=8, agsize=268435455 blks
         =                       sectsz=512   attr=2, projid32bit=1
         =                       crc=1        finobt=0, sparse=0
data     =                       bsize=4096   blocks=2013265920, imaxpct=5
         =                       sunit=0      swidth=0 blks
naming   =version 2              bsize=4096   ascii-ci=0 ftype=1
log      =internal log           bsize=4096   blocks=521728, version=2
         =                       sectsz=512   sunit=0 blks, lazy-count=1
realtime =none                   extsz=4096   blocks=0, rtextents=0
```

(10) 挂载

将逻辑卷挂载到/home 下,挂载完成后使用命令 df –h 查看是否挂载成功。

```
[root@cyber ~]# mount /dev/es_file/data /home/
[root@cyber ~]# df -h
文件系统                  容量  已用  可用 已用% 挂载点
/dev/mapper/h3linux-root  595G 1023M  594G    1% /
devtmpfs                   63G     0   63G    0% /dev
tmpfs                      63G     0   63G    0% /dev/shm
tmpfs                      63G  9.3M   63G    1% /run
tmpfs                      63G     0   63G    0% /sys/fs/cgroup
/dev/vda1                1014M  163M  852M   17% /boot
/dev/mapper/es_file-data  7.5T   33M  7.5T    1% /home
tmpfs                      13G     0   13G    0% /run/user/0
```

8、配置自动挂载

挂载之后需要配置/etc/fstab 使得硬盘在系统重启后可以自动挂。

```
[root@cyber ~]# cat /etc/fstab

#
# /etc/fstab
# Created by anaconda on Thu Dec 30 15:17:25 2021
#
# Accessible filesystems, by reference, are maintained under '/dev/disk'
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info
#
/dev/mapper/h3linux-root /                       xfs     defaults        0 0
UUID=da77409b-2f61-4bb2-a4cb-2fe47c0dfa20 /boot                   xfs     defaults
       0 0
/dev/mapper/h3linux-swap swap                    swap    defaults        0 0
/dev/es_file/data    /home xfs defaults        0 0
```

(11) 重启服务器生效

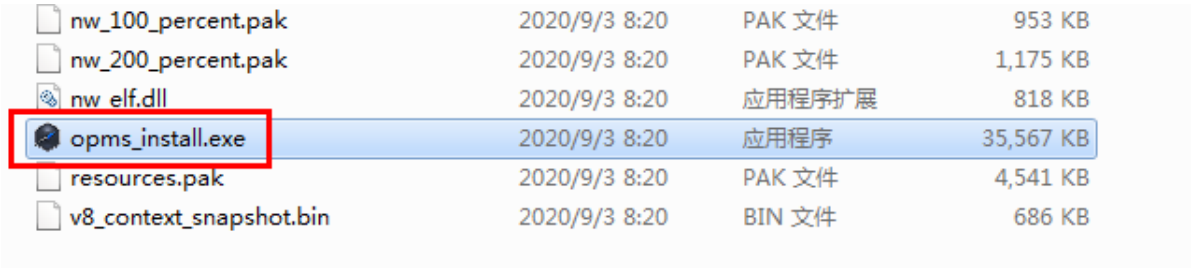
重启服务器后通过 XSHELL 工具连上该服务器后通过 fdisk –l 确认/home 后面对应的硬盘信息是否正确。

注意

至此完成整个操作系统的安装。操作系统的安装一定要注意 IP 和主机名还有磁盘挂载问题，其中如果有一步出错都会导致态势感知软件无法安装

3. 统一运维管理系统安装

上传 opms 压缩包至跳板机（或者是管理服务器），解压安装工具，进入解压后文件目录。双击 opms_install.exe 进行安装

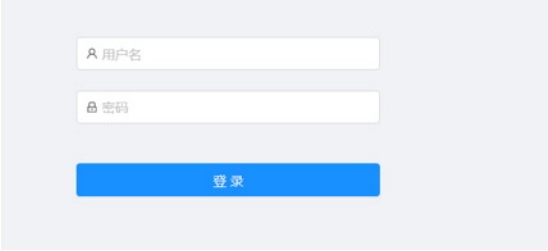


在输入框中输入要部署统一运维管理系统的主机 IP 和密码（即态势感知 IP 和后台密码 csap_H3C@yunzhi），单击空白处后，单击开始安装，如下图

安装完成见下图

4. 平台部署

使用 Chrome 浏览器最新版本（78.0.3904.97 及以后版本）访问，在地址栏输入态势感知 IP,http://主机 IP:2080，默认登录用户名/密码：admin/o9p1M0s2。登录后可以在 admin>修改密码中修改用户密码。目前暂不提供找回密码功能，请妥善保管。



环境校验通过后，点击开始部署，上传安装包 single_plat_CSAPV100R012E1145.tar.gz 即可进行平台部署（此过程不可刷新页面）

此过程可通过后台查看部署日志

```
[root@cyber ~]# tail -f /opt/install/plat_install.log
.....
*******Deploy web_service success*******
========== 2021-12-30 17:54:10 完成部署可视化相关组件 ==========
========== 2021-12-30 17:54:10 开始部署 SNMP、升级 Openssh、systemd-219 等依赖组
件 ==========
*******Begin to set crontab*******
*******Set crontab success*******
*******Begin to deploy SNMP*******
success
success
*******Deploy SNMP success*******
mkdir: 已创建目录 "/home/ips"
mkdir: 已创建目录 "/home/ips/pcap"
mkdir: 已创建目录 "/home/ips/download"
success
success
========== 2021-12-30 17:54:22 完成部署 SNMP、升级 Openssh 等依赖组件 ==========
*******Wait a moment, start checking the CSAP system.*******
 ===== 开始检查 Spark 状态 =====
 Spark 服务正常
 ===== 开始检查 Kafka 状态 =====
 Kafka 服务正常
 ===== 开始检查 Redis 状态 =====
 Redis 服务正常
 ===== 开始检查 MySQL 状态 =====
 MySQL 服务正常
 MySQL 服务 cybersa_db 数据库存在
 MySQL 服务 csap_monitor 数据库存在
 MySQL 服务 cybersasim_db 数据库存在
 MySQL 服务 logcollector 数据库存在
 MySQL 服务 proxy_db 数据库存在
 MySQL 服务 tip_db 数据库存在
 MySQL 服务 flow_db 数据库存在
 MySQL 服务 csap_nacos 数据库存在
 MySQL 服务 auth 数据库存在
 ===== 开始检查 Elasticsearch 状态 =====
 ElasticSearch 服务正常
```

```
===== 开始检查 Clickhouse 状态 =====
Clickhouse 服务正常
===== 开始检查态势感知应用服务状态 =====
csap-minio 文件管理服务正常
csap-asso-event 关联分析服务正常
csap-log-rich 数据丰富服务正常
csap-monitor 系统监控服务正常
Bootstrap 可视化服务正常
tip 情报接入服务正常
cloudops 资产配置服务正常
nativeproxy 资产采集服务正常
sis 响应编排服务正常
probe 资产探针服务正常
cloudagent 专家会诊服务正常
nacos-server 微服务注册中心正常
nginx 反向代理服务正常
csap-gateway 接口网关服务正常
csap-rules-config 规则配置服务正常
csap-nat 通报溯源服务正常
csap-aggregation 风险分析服务正常
csap-scene 场景化分析服务正常
csap-vulnerability 脆弱性分析服务正常
csap-sis-vulnerability 响应编排脆弱性服务正常
csap-base-screen 基础大屏服务正常
csap-base-search 风险分析查询服务正常
csap-logsearch-ck 日志检索服务正常
csap-base-report 通用报表服务正常
csap-auth 接口认证服务正常
csap-app APP 后台服务正常
csap-license License 管理服务正常
csap-user-manager 用户管理服务正常
csap-permission 用户权限服务正常
csap-notification-disposal 通报处置服务正常
csap-nta-abnormal 异常流量分析服务正常
csap-dataclean 数据清理服务正常
vulner-opms 漏扫联动服务正常
csap-lca-manager 数据接入服务正常
CollectorServer 被动采集器服务正常
AliveCollectorServer 主动采集器服务正常
csap-lca-adapter 日志适配服务正常
*******The installation is complete*******
========== 2021-12-30 17:56:56 开始注册部署记录 ==========
1<script language='javascript'>let url = window.location.href;let str = 'security/de
vice/web';let index = url.indexOf(str);if (index > -1) {   let nextSlashIndex = url
.indexOf('/', index + str.length + 1);   let num = url.slice(index + str.length + 1
, nextSlashIndex);   top.location.href = `${top.location.protocol}//${top.location.
hostname}/${str}/${num}/toLogin?forceLogout=1`;} else {   top.location.href = '/toLog
in?forceLogout=1';}</script>Chassis Part Number is
*****WEB service has started*****
```

```
*******No need to deal with it*******
========== 2021-12-30 17:56:57 完成注册部署记录 ==========
```

5. 插件部署

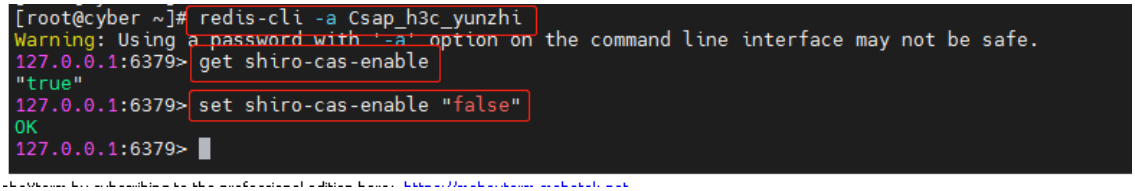
(1) 解压 cloudos-csap-plugin1.zip 补丁包，获取 jar 包（补丁包为 zip 包，使用 unzip 命令解压，或者在 Windows 桌面使用工具解压）。

(2) 将全部 jar 包替换到以下目录。

/opt/web-service/webapps/skynet/WEB-INF/lib

(3) 执行 addUrl.sh 脚本。

(4) 执行如下图中的命令，修改 redis 中的值。



(5) 重启前端 WEB 服务，先杀掉 WEB 进程，例如：ps –ef | grep tomcat 获取进程号后 kill 该进程。然后启动服务，启动脚本位于/opt/web-service/bin/startup.sh。

注意：态势感知的监控服务会定期巡检并拉起失效的 WEB 服务，所以杀掉 WEB 进程后请尽快启动 WEB，否则可能会造成启动两个 WEB 服务进而 WEB 失效的问题。

E.7.2 授权激活

浏览器访问 https://ip，显示基础平台软件授权 license 未激活。

点击“产品注册”，下载主机信息文件，然后进行激活（激活方式找产品经理协调）

选择 license 文件上传，激活成功后，登录态势感知，确认激活成功。（用户名/密码：admin/secCsap@12345）

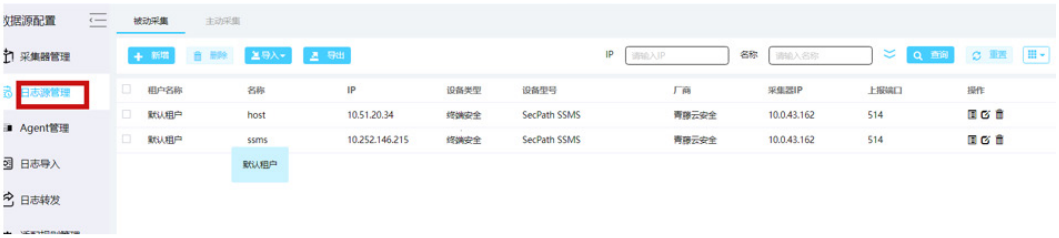
E.7.3 态势感知 Logo 定制

(1) 将下图另存为.png 格式的图片。

(2) 使用 admin 用户登录后进入“系统配置 > 个性化定制页面”修改即可。

E.7.4 日志源的配置

如果需要与主机安全联动，需要配置主机安全的日志源（主机安全侧也需配置日志发送的目的地址为态势感知的地址），其他的根据局点需求配置日志源（目前主要收集 IPS/NTA 的日志）。日志源配置方式：admin 用户进入配置中心-》日志源管理，按需添加即可。



E.7.5 端口限源和关闭

如果考虑部署区域的安全性问题需要限源和关闭态势和 casagent 的端口，请参考下面配置实施，关闭和限源通过 firewall-cmd 命令实现。

1. 态势感知端口

端口	协议	描述	备注
161	udp	访问SNMP节点	可以关闭
69	udp	tftp	端口抓包取证使用，不使用可以关闭
6379	tcp	访问数据缓存	可以关闭
8988/8998/9002	tcp	agent服务端口	可以关闭
443	tcp	WEB访问接口https端口	
80	tcp	WEB访问接口http端口	无对接UC场景可以关闭
22	tcp	SSH连接端口	运维网需开放
9990	tcp	手机app服务端口	可关闭
8999/9090/9091/9092	tcp	nginx开放端口	9090/9092端口为对接知识图谱，不使用可关闭 9091端口对接SMP，不使用可关闭
2080/2081	tcp	opms工具的服务端口	系统安装完成后，可以关闭
9001	tcp	采集器rest接口	可以关闭
9995	tcp	威胁情报服务端口	安全云情报读取使用，表中无标明，可以关闭
9999	tcp	运维组件服务端口	没有外部系统对接可以关闭
10002	tcp	资产探针服务端口	资产主动探测表中无标明，可以关闭
3443	tcp		可以关闭
514	udp	日志采集端口	不可关闭
端口	协议	描述	备注
161	udp	访问SNMP节点	可以关闭
69	udp	tftp	端口抓包取证使用，不使用可以关闭

6379	tcp	访问数据缓存	可以关闭
8988/8998/9002	tcp	agent服务端口	可以关闭
443	tcp	WEB访问接口https端口	
80	tcp	WEB访问接口http端口	无对接UC场景可以关闭
22	tcp	SSH连接端口	运维网需开放
9990	tcp	手机app服务端口	可关闭
8999/9090/9091/9092	tcp	nginx开放端口	9090/9092端口为对接知识图谱，不使用可关闭 9091端口对接SMP，不使用可关闭
2080/2081	tcp	opms工具的服务端口	系统安装完成后，可以关闭
9001	tcp	采集器rest接口	可以关闭
9995	tcp	威胁情报服务端口	安全云情报读取使用，表中无标明，可以关闭
9999	tcp	运维组件服务端口	没有外部系统对接可以关闭
10002	tcp	资产探针服务端口	资产主动探测表中无标明，可以关闭
3443	tcp		可以关闭
514	udp	日志采集端口	不可关闭

E.8 一代服务器安全监测部署

E.8.1 安装说明

(1) 目标服务器推荐安装配置要求

类型	CPU（核）	内存（GB）	硬盘（GB）	安装应用
A	8	32	1024	SSMS主服务
B	8	16	512	事件采集服务

(2) **由于 E6404 版本事件采集功能变更，目前提供单台部署和两台部署两种方案进行安装，强烈建议使用两台部署方案，将事件采集服务器单独安装在一台机器上。若是无事件采集功能需求可以使用单台部署方案，注意单台部署不支持使用事件采集功能。**

(3) 单台部署时仅需安装 A 类主机；双台部署时需分别安装 A，B 类主机，对应安装服务。**两台主机部署安装时，除配置要求不同外，两台主机都需要执行：E8.4 安装系统。**

(4) 目标服务器预先安装好 CentOS 7.x 系统。

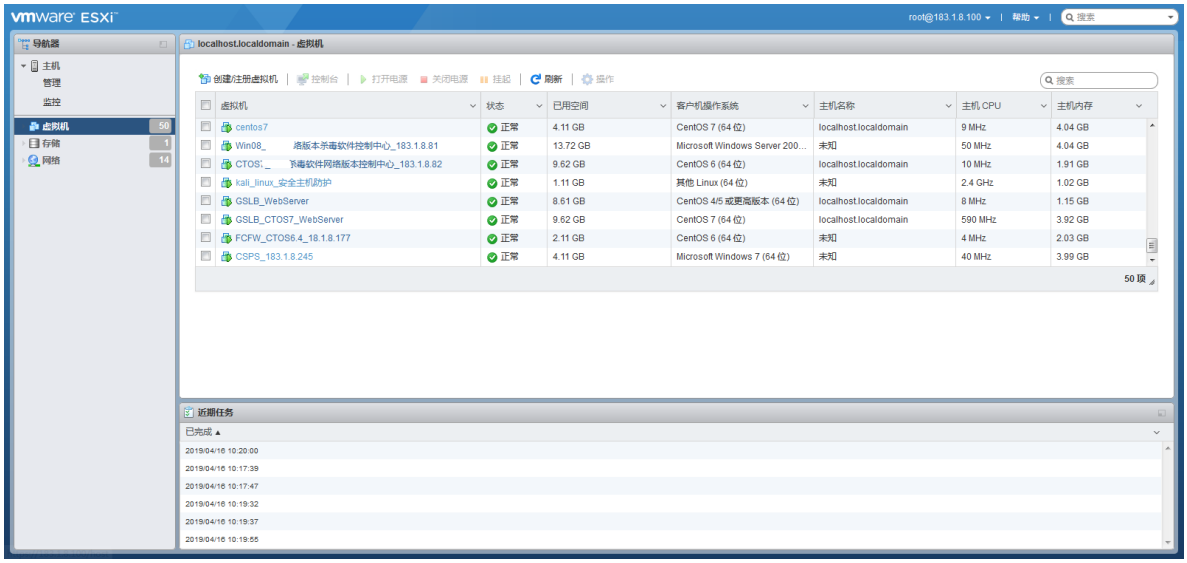
(5) 安装包为 H3C SecPath 服务器安全监测系统程序。

E.8.2 VMware ESXi 6.5 环境安装举例

1. Centos7.X 安装举例（安装包需客户准备）

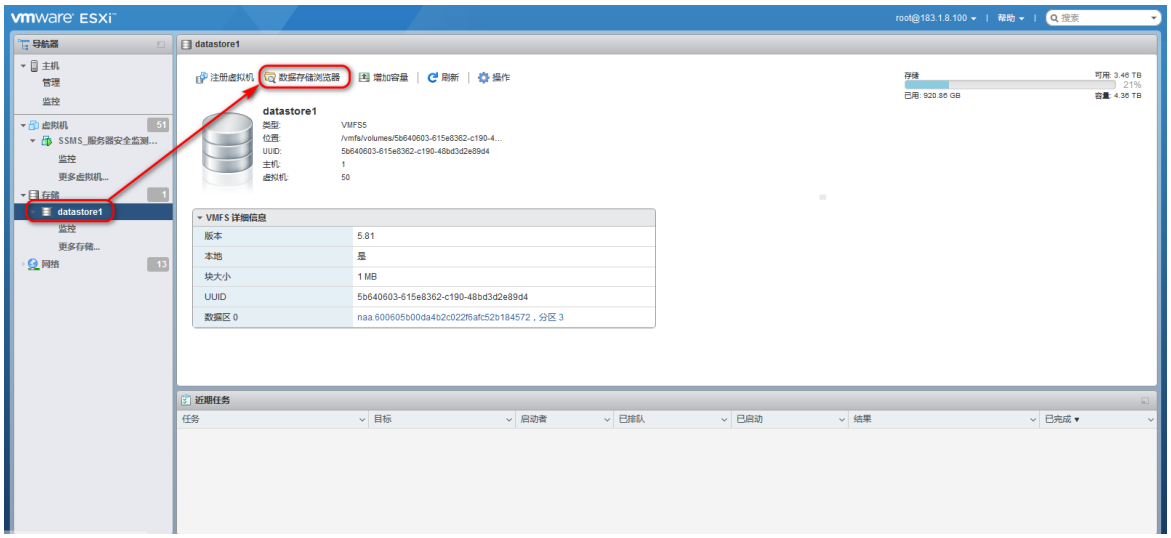
(1) 使用火狐浏览器登录到 VMware ESXi 6.5 管理平台。

图E-121 登录 VMware ESXi 6.5 管理平台



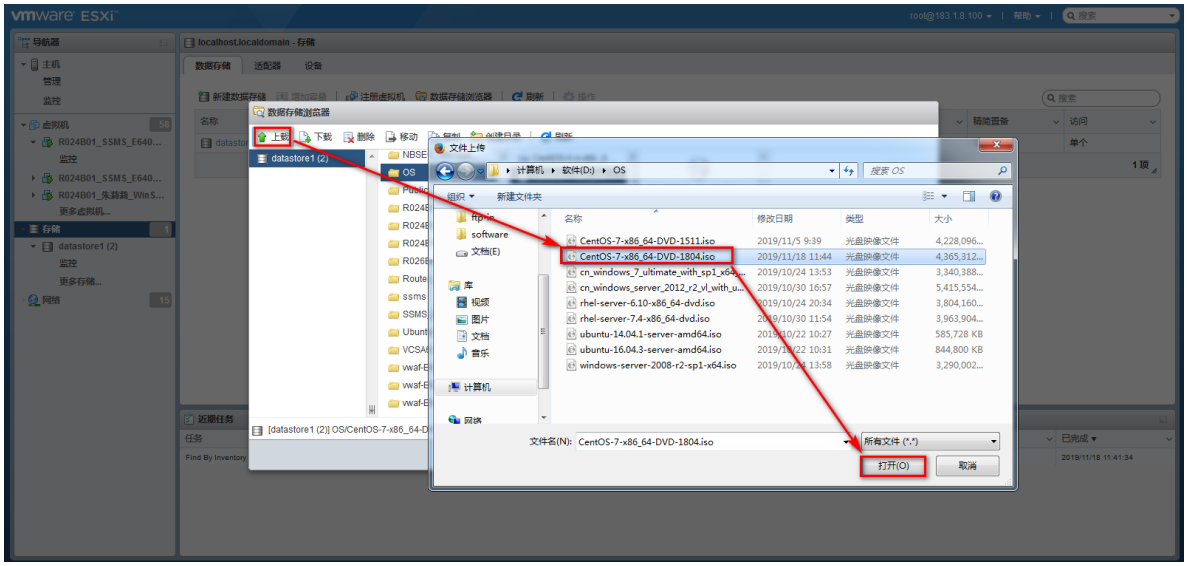
(2) 进入[主页/存储/databases1]，单击页面上的<数据存储浏览器>，并点击“浏览数据存储”。

图E-122 配置存储器



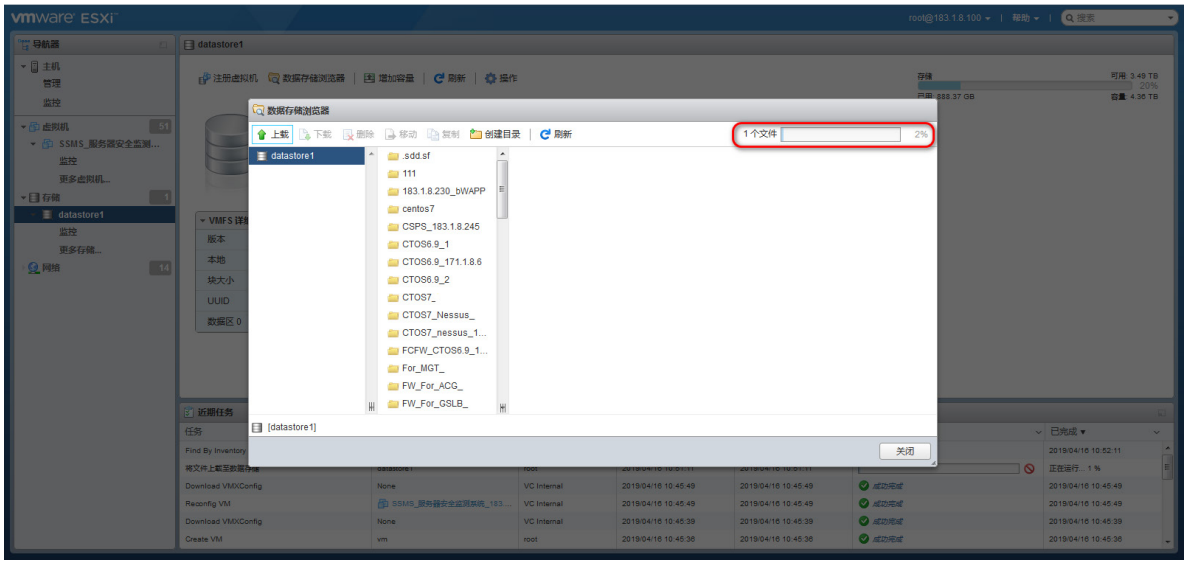
(3) 点击“上传”并选择 Centos7.X 镜像文件（CentOS-7-x86_64-DVD-1804.iso）上传到 databases1 上。

图E-123 上传镜像



右上角显示上传时进度条，可查看上传进度。

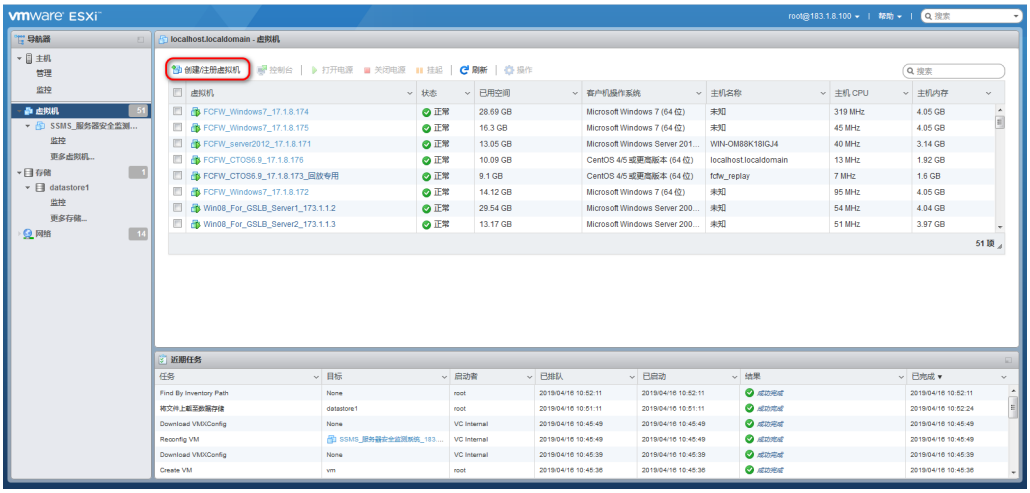
图E-124 上传镜像进度条



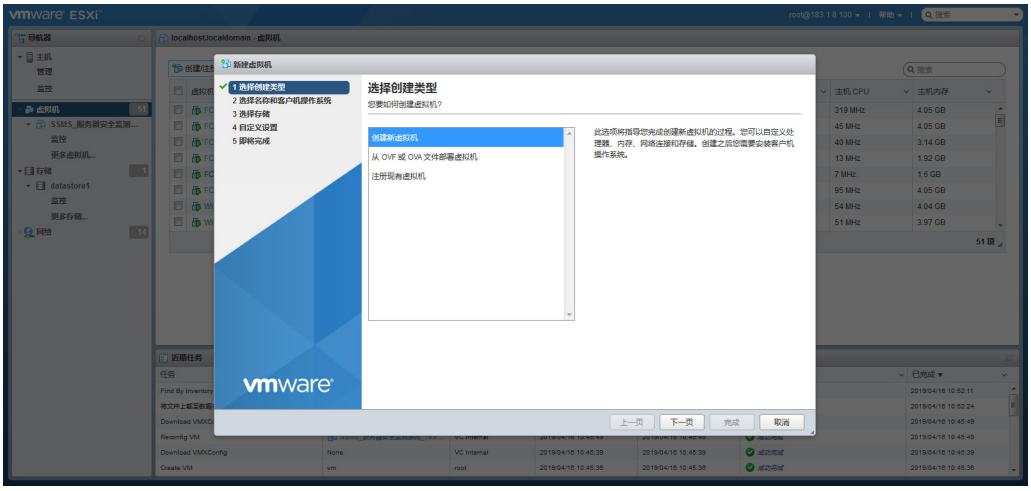
2. 部署虚拟机

(1) 在 VMware ESXi 6.5 主页上，单击<创建/注册虚拟机>按钮，自定义选择创建类型、选择名称和客户操作系统、选择存储和自定义设置。如下图所示。

图E-125 创建/注册虚拟机

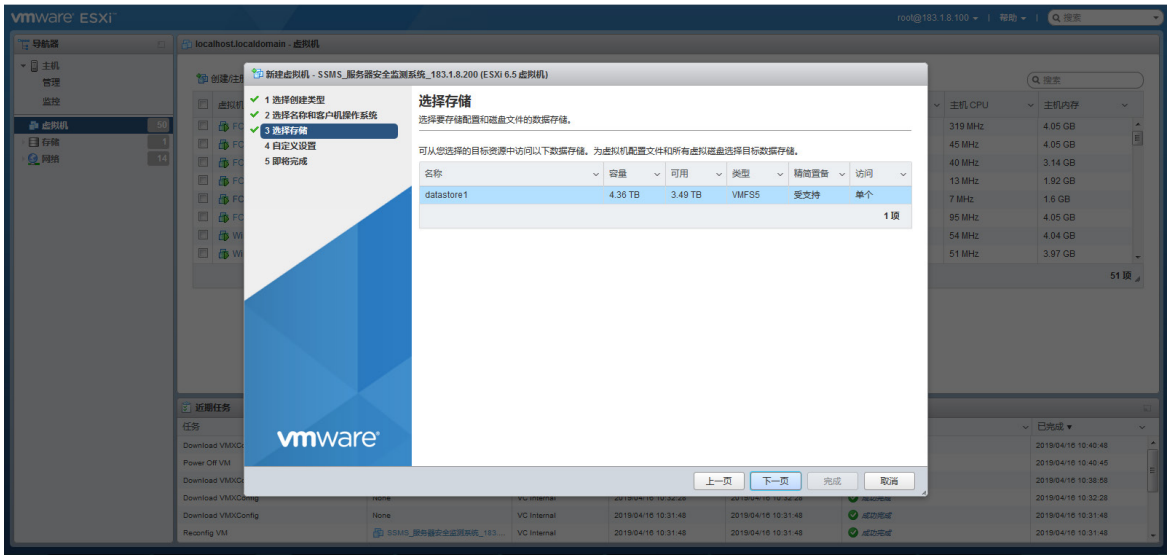


图E-126 选择创建类型



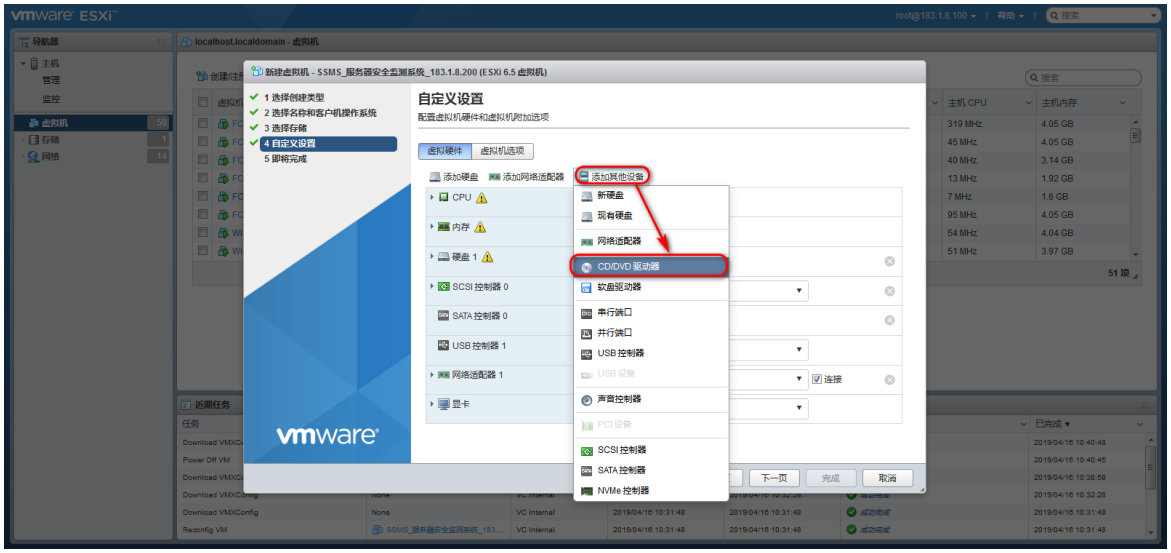
图E-127 选择名称和客户端操作系统

图E-128 选择存储

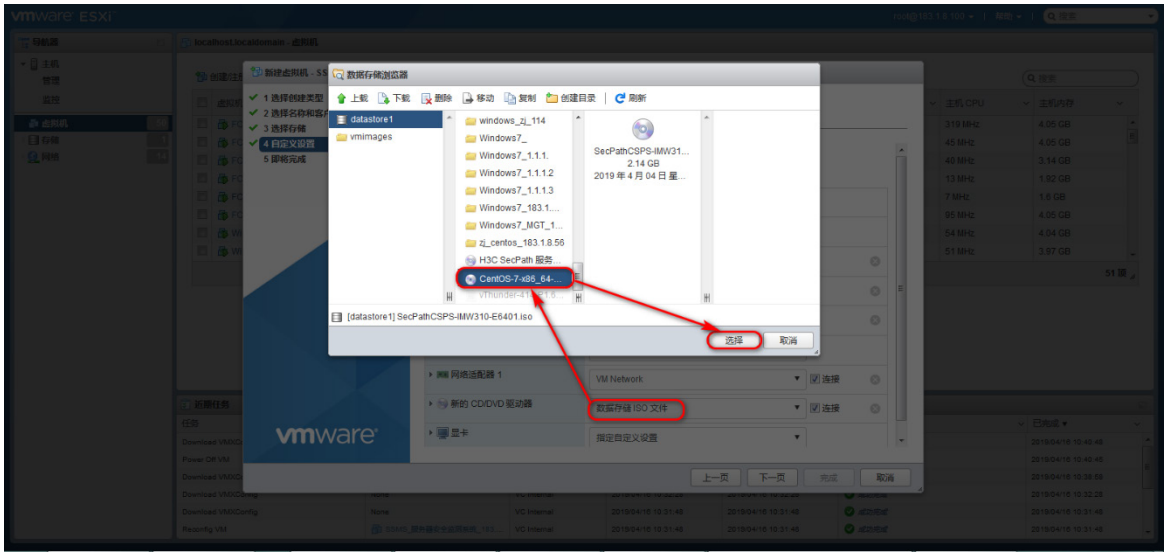


(2) 自定义设置配置，点击“添加其他设备”选择“CD/DVD 驱动器”，并通过点击“数据存储 ISO 文件”选择之前导入 databases1 中的服务器安全系统 ISO 文件（CentOS-7-x86_64-DVD-1804.iso）。

图E-129 添加 CD/DVD 驱动器

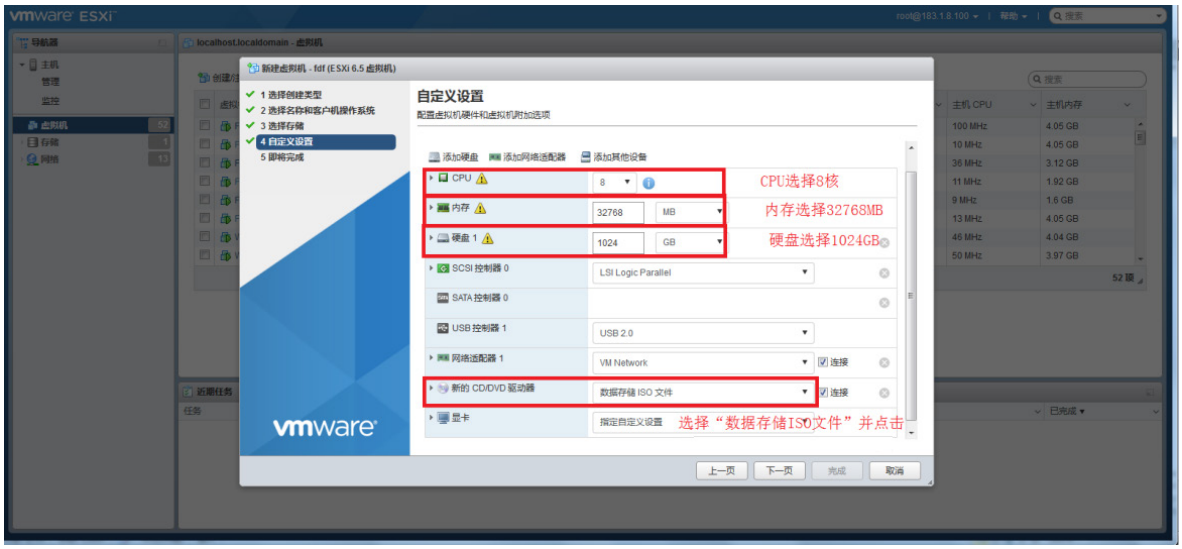


图E-130 选择镜像文件



(3) 根据服务器安全系统配置要求，设置如下图所示：

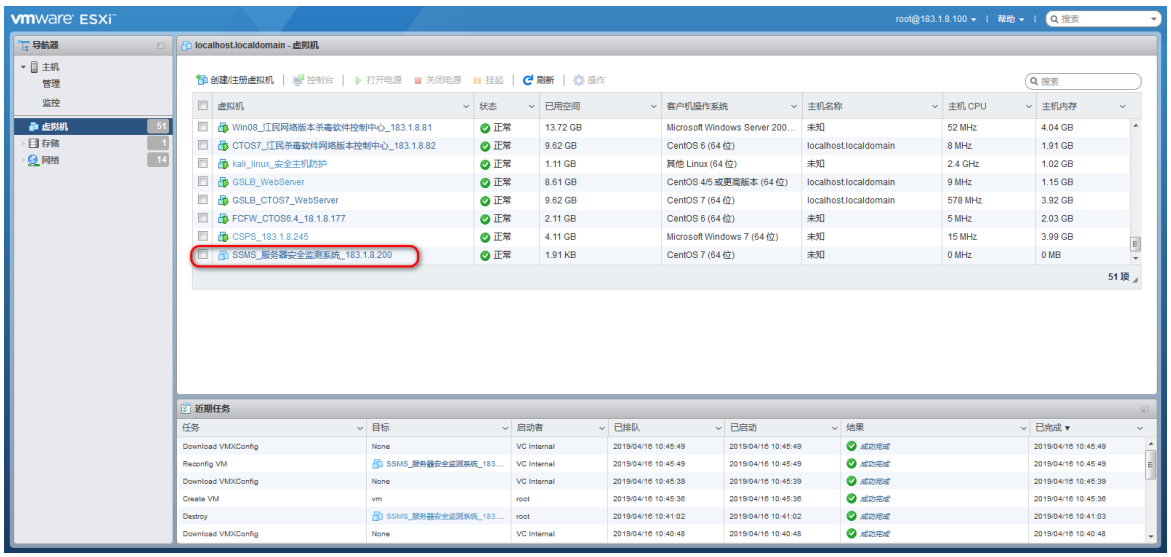
图E-131 自定义设置硬件配置



(4) 单击<完成>之后，虚拟机配置完毕。

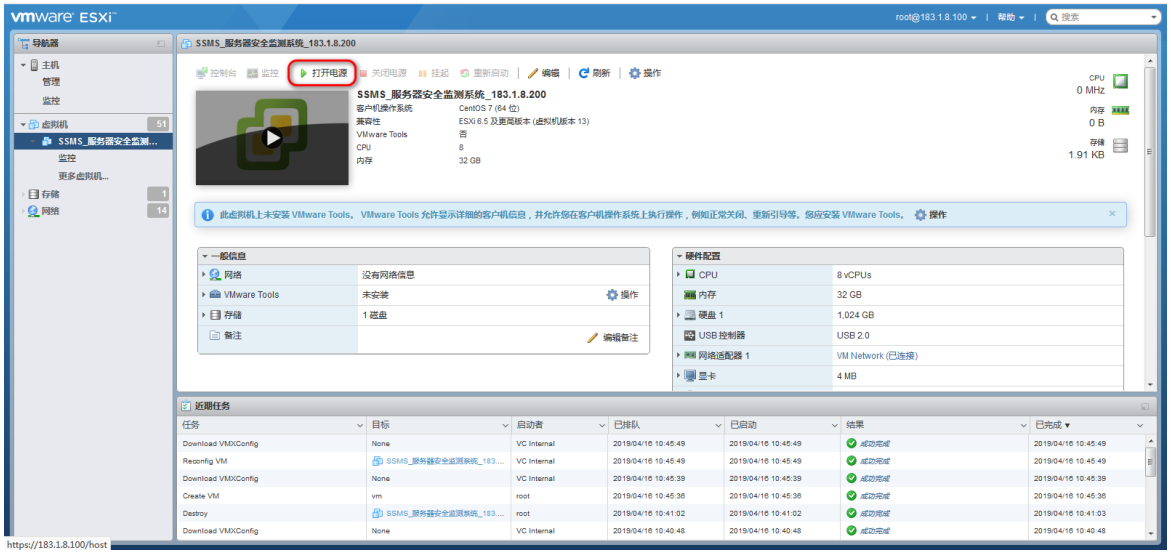
图E-132 完成向导

图E-133 完成虚拟机创建



(5) 单击<打开电源>按钮，进入安装系统界面。

图E-134 启动虚拟机



虚拟机设置完成后即可进行下一步系统安装配置，请继续查看“E.8.4 安装系统”。

E.8.3 CAS 7.0 环境安装举例

1. Centos7.X 安装举例（安装包需客户准备）

(1) 登录虚拟化管理平台。

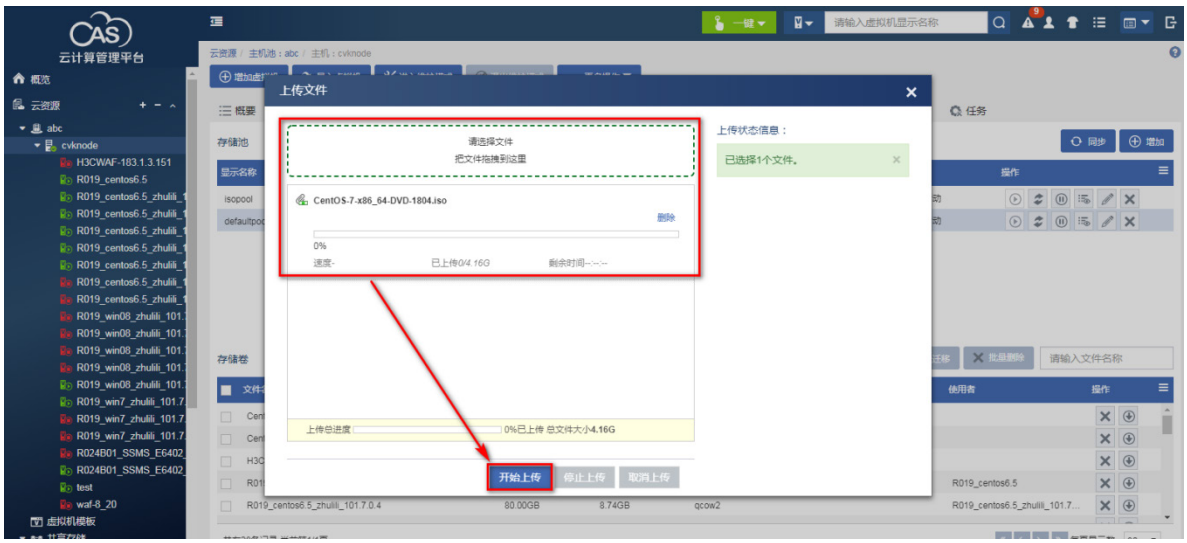
图E-135 登录 CAS 管理平台

(2) 进入[云资源/cvknode/cvknode]，单击页面上方的<存储>。

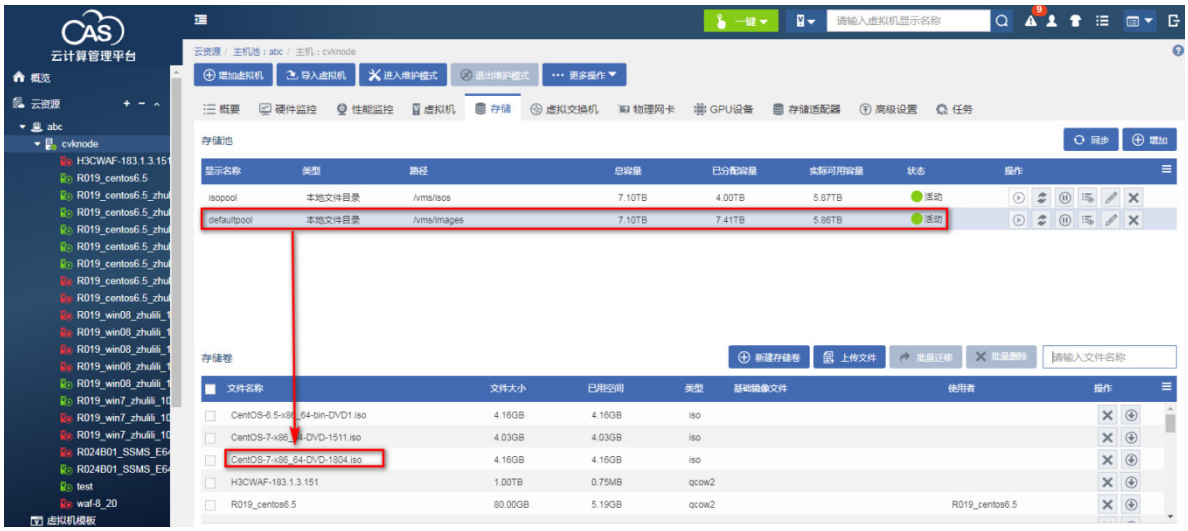
图E-136 配置存储

(3) 把操作系统 ISO 镜像文件上传到 defaultpool。

图E-137 上传镜像



图E-138 查看镜像



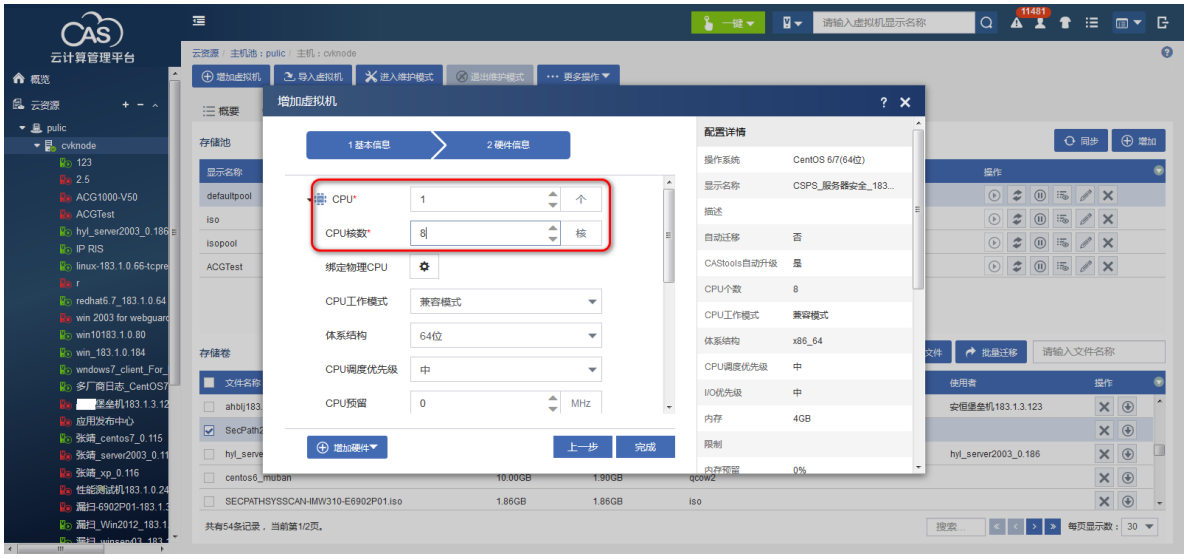
2. 部署虚拟机

(1) 单击<增加虚拟机>按钮，<基本信息>页面设置如下图所示。

图E-139 增加虚拟机

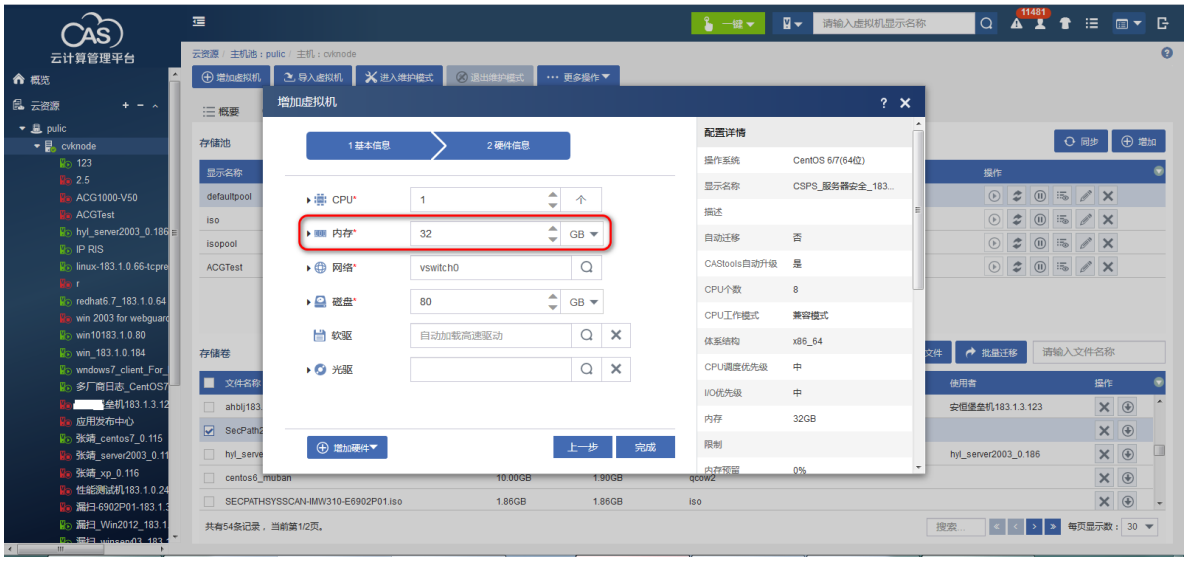
(2) <硬件信息>的推荐最低配置要求，如下图所示。CPU 需要 8 核以上。

图E-140 配置 CPU



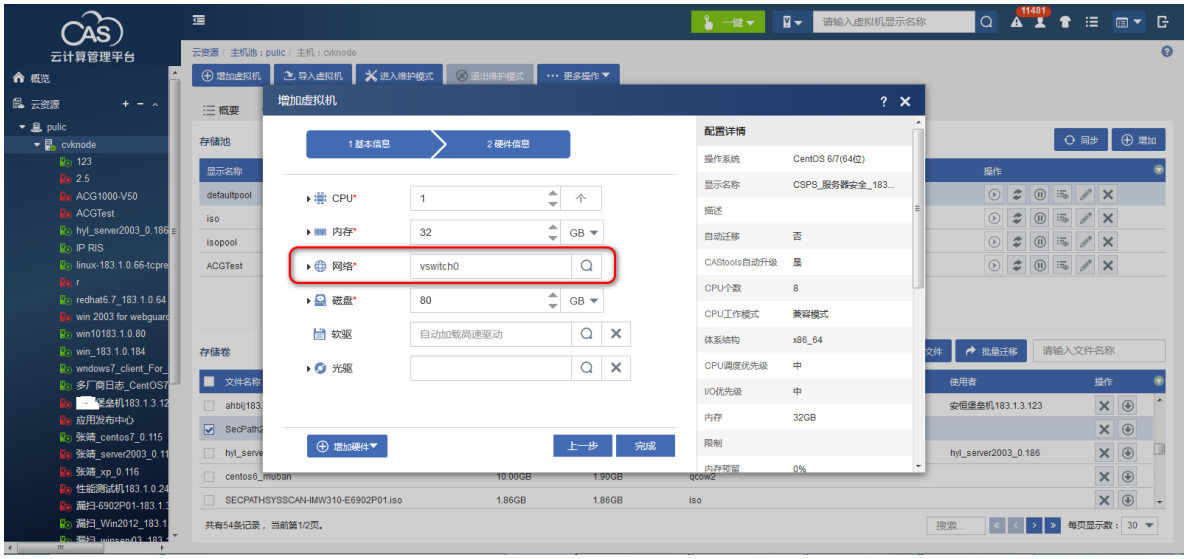
(3) 内存大小需要 32G 以上。

图E-141 配置内存



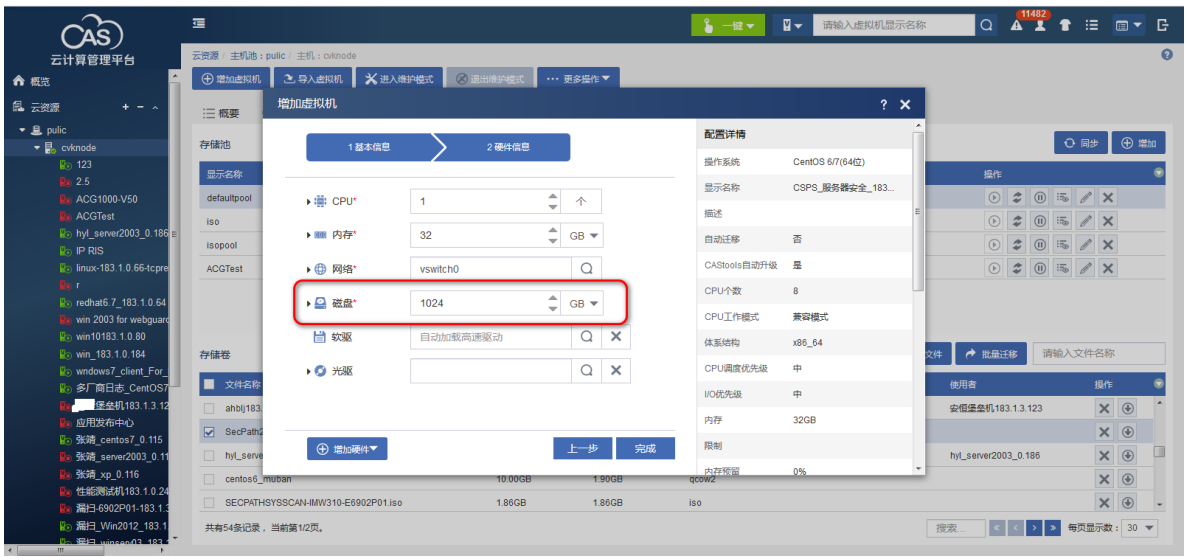
(4) 网卡选择一块

图E-142 配置网卡



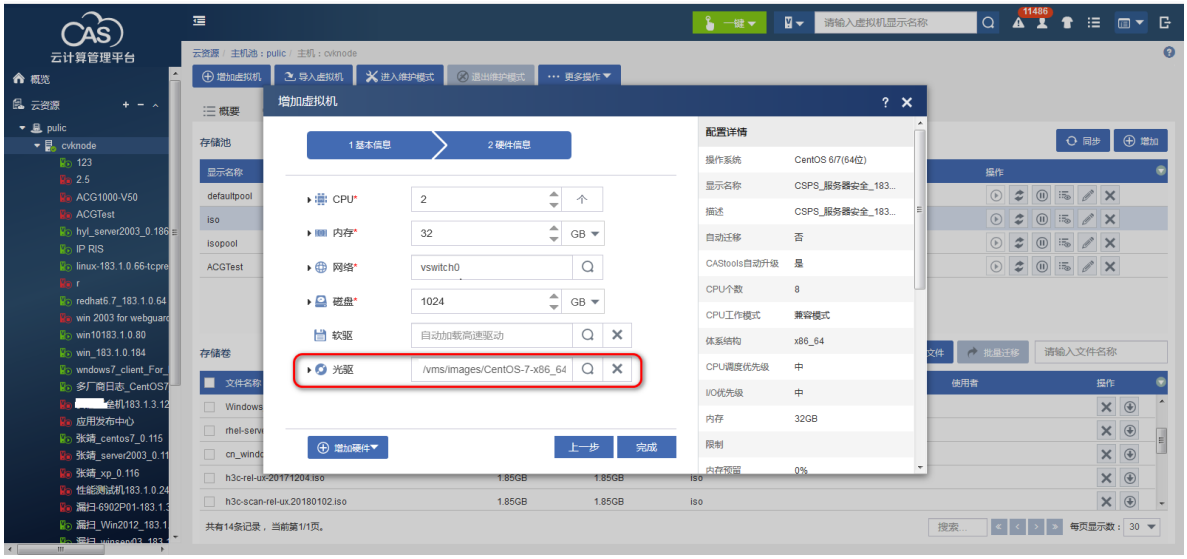
(5) 单块硬盘大小不低于 1024G。

图E-143 配置硬盘



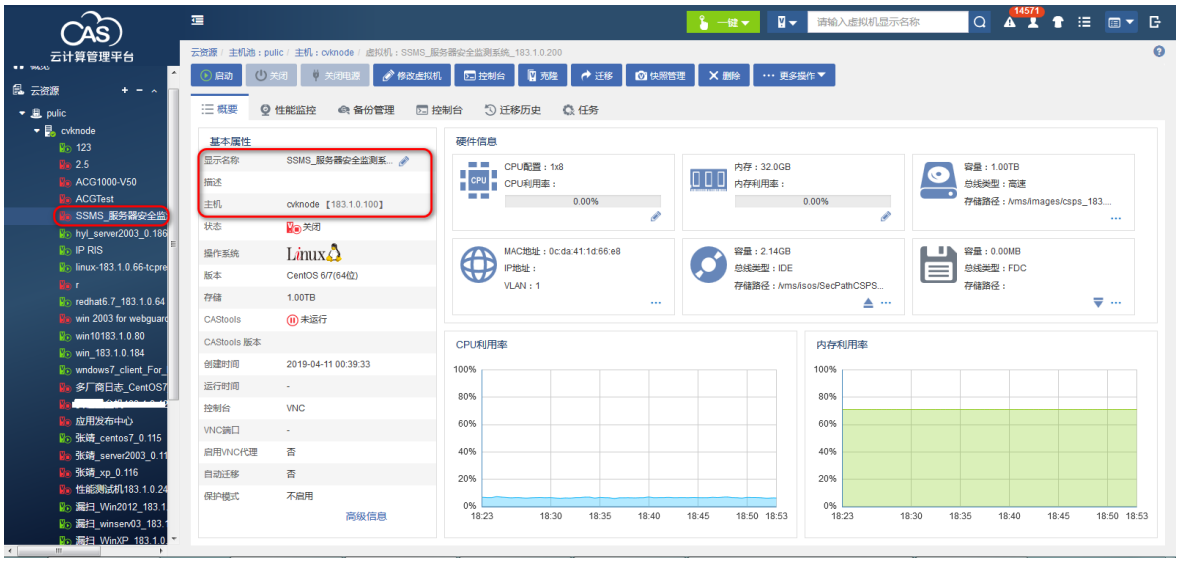
(6) 点击<光驱>选择镜像文件

图E-144 选择光驱



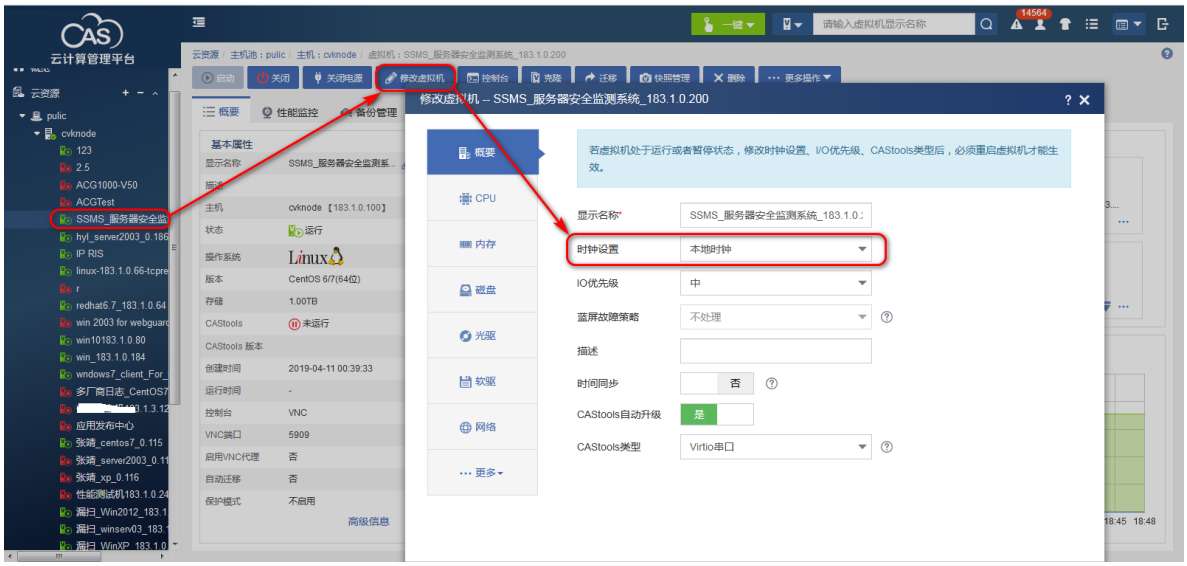
(7) 单击<完成>之后，虚拟机配置完毕。

图E-145 完成虚拟机配置



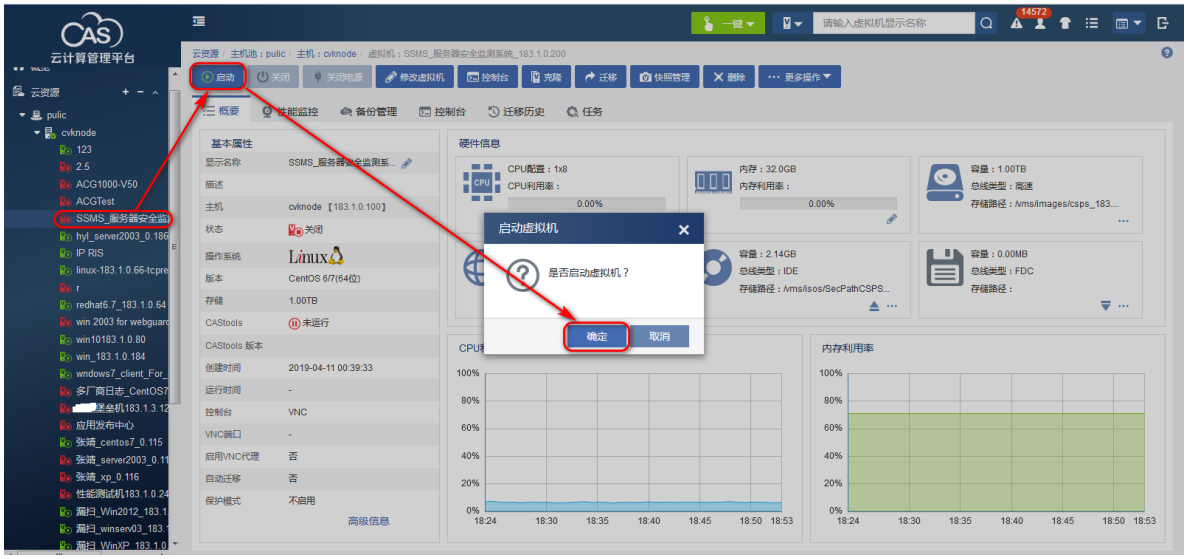
(8) 选择服务器安全，单击修改虚拟机，在概要/高级设置中将系统时钟修改为本地时钟。

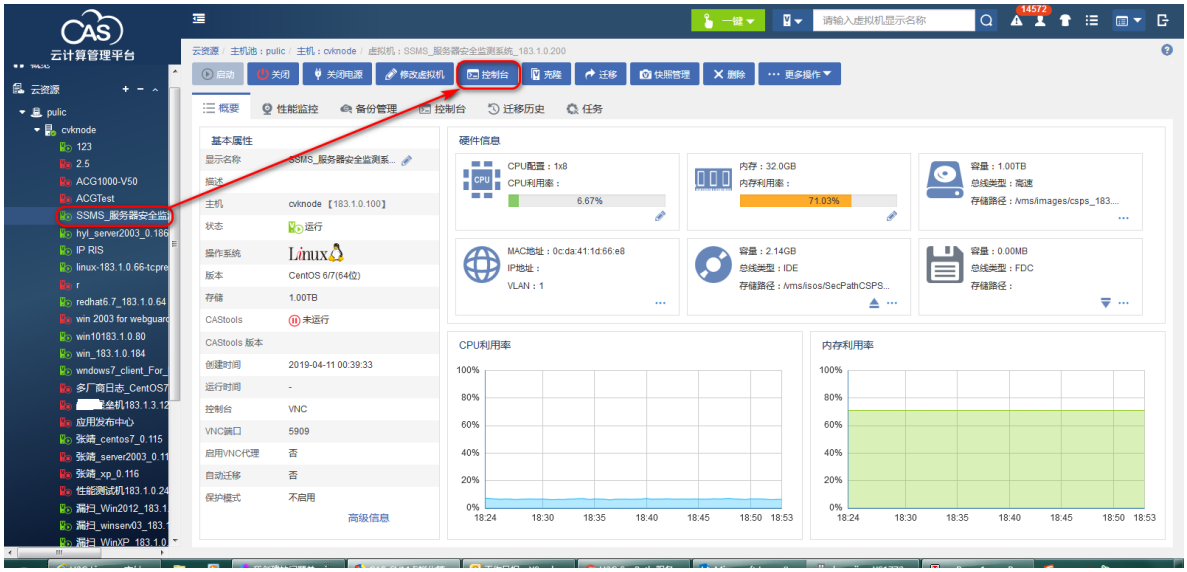
图E-146 修改系统时钟



(9) 单击<启动>按钮，进入控制台界面。

图E-147 启动系统





虚拟机设置完成后即可进行下一步系统安装配置，请继续查看“E.8.4 安装系统”。

(10) 两台部署请重复上述步骤，配置请参考 安装说明 B 机器 内存 16G 硬盘 512G。

E.8.4 安装系统

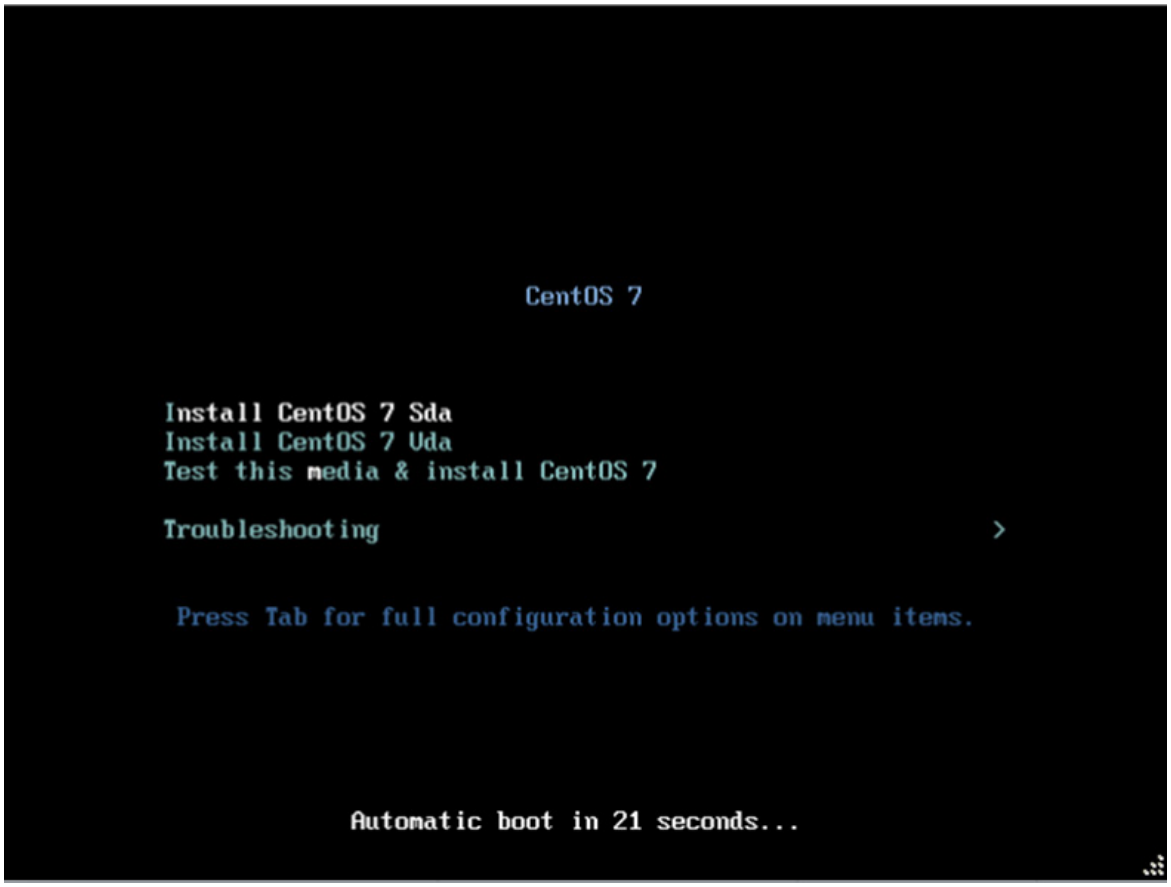
说明

两台主机部署安装时，除配置不同外，其余均相同。

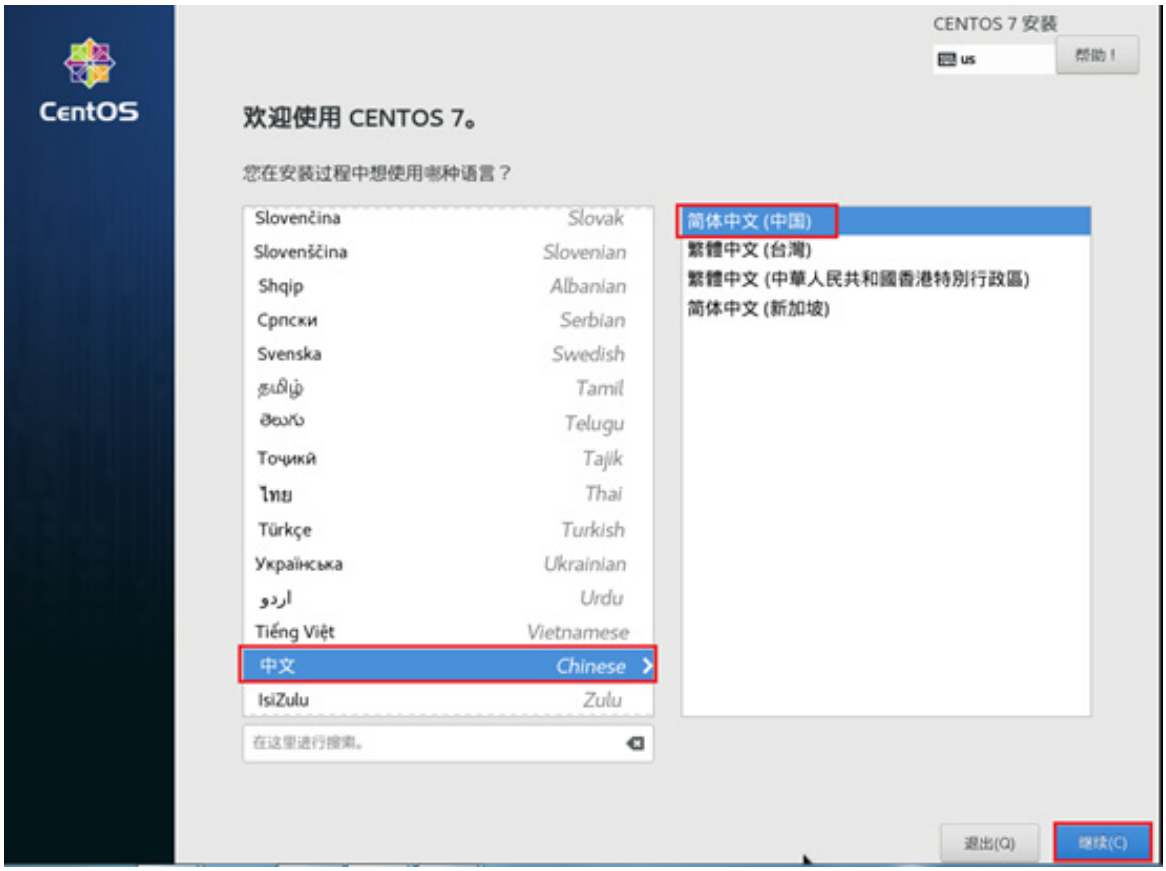
1. 安装系统

(1) 在安装系统界面下，按硬盘类型选择需要安装的系统类型，一般情况下，选择“Install CentOS 7 Sda”；如果硬盘是 Virtio I/O，选择“Install CentOS 7 Vda”。选择会自动安装系统，直到可登录系统。

图E-148 安装系统



图E-149 选择语言

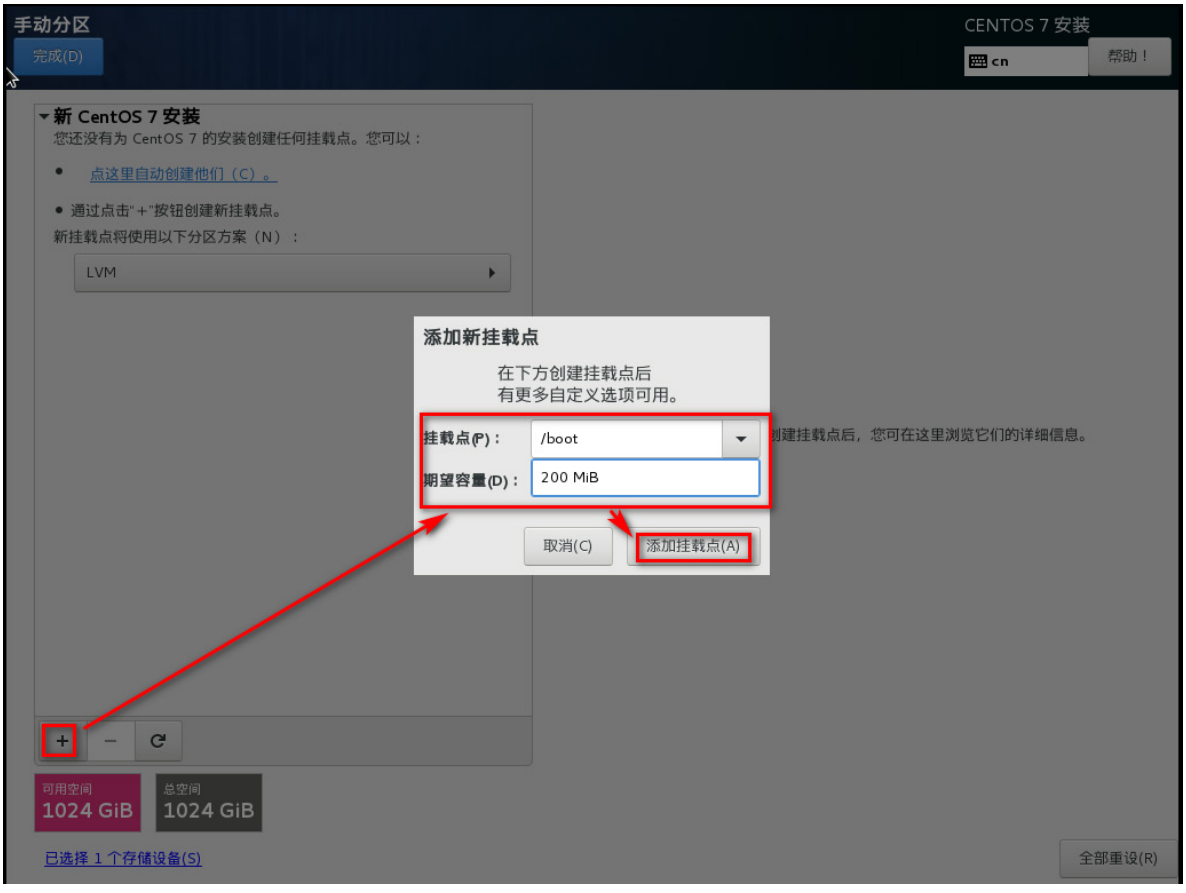


(2) 在安装信息摘要界面下，系统>安装位置，默认使用自动分区，此时需要手动划分磁盘空间。建议给/boot 目录分配 200M、swap 目录分配 8192M，剩余空间分配给/目录。

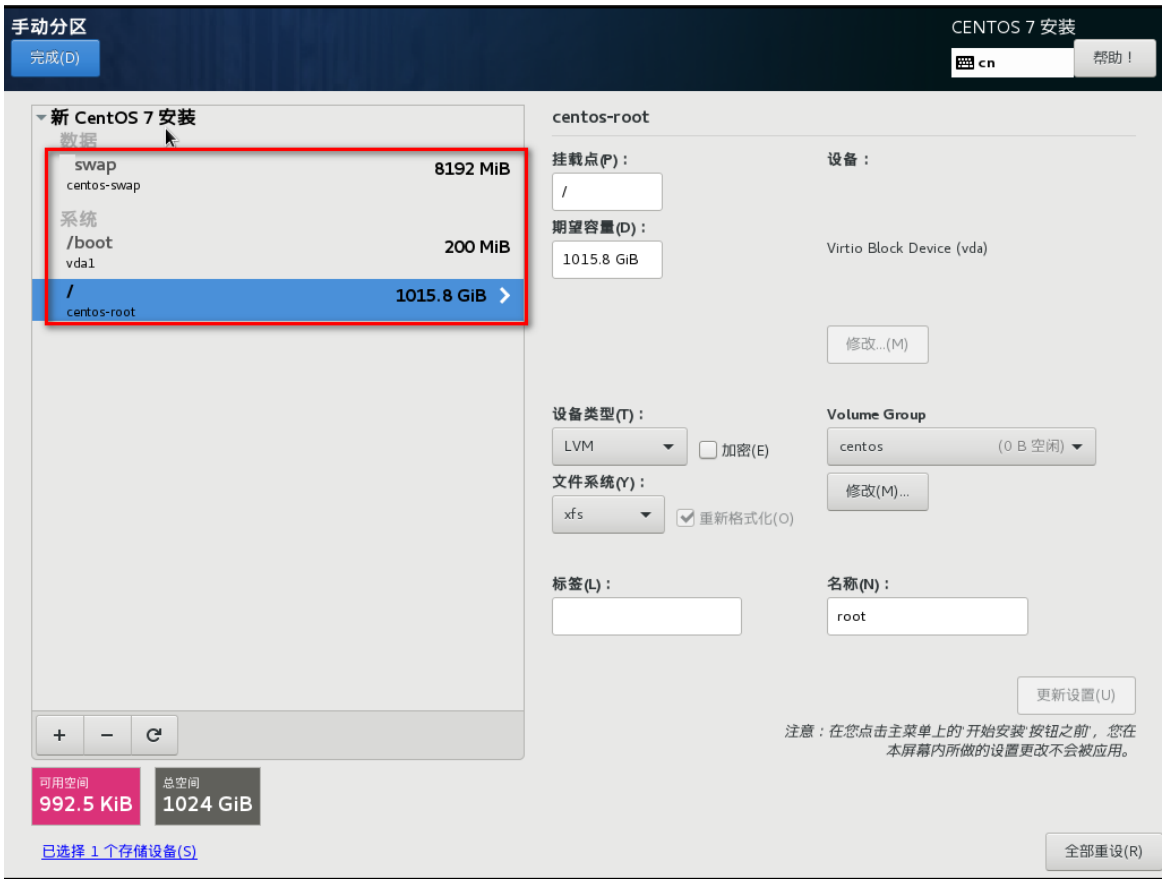
图E-150 磁盘划分

图E-151 选择我要配置分区后点击完成

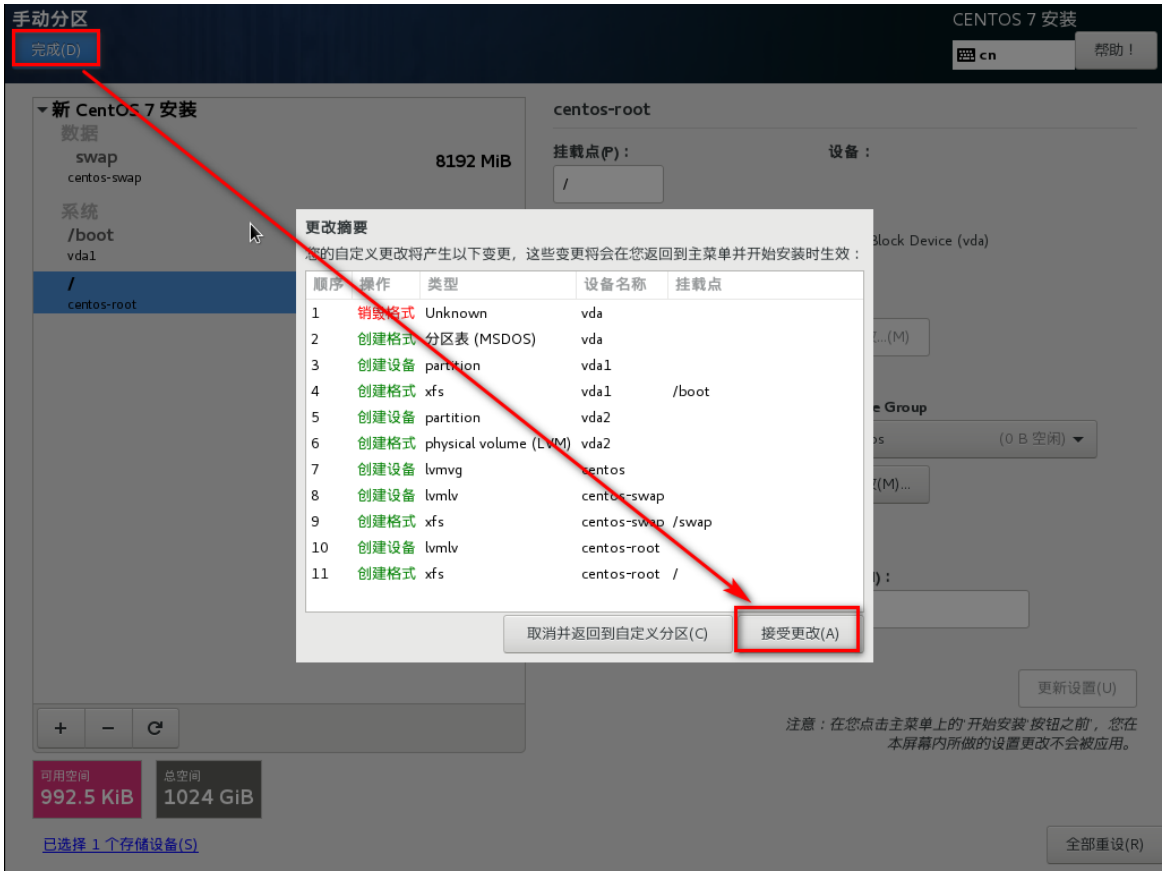
图E-152 添加/boot 挂载点（swap 与/目录分配类似）



图E-153 添加/挂载点

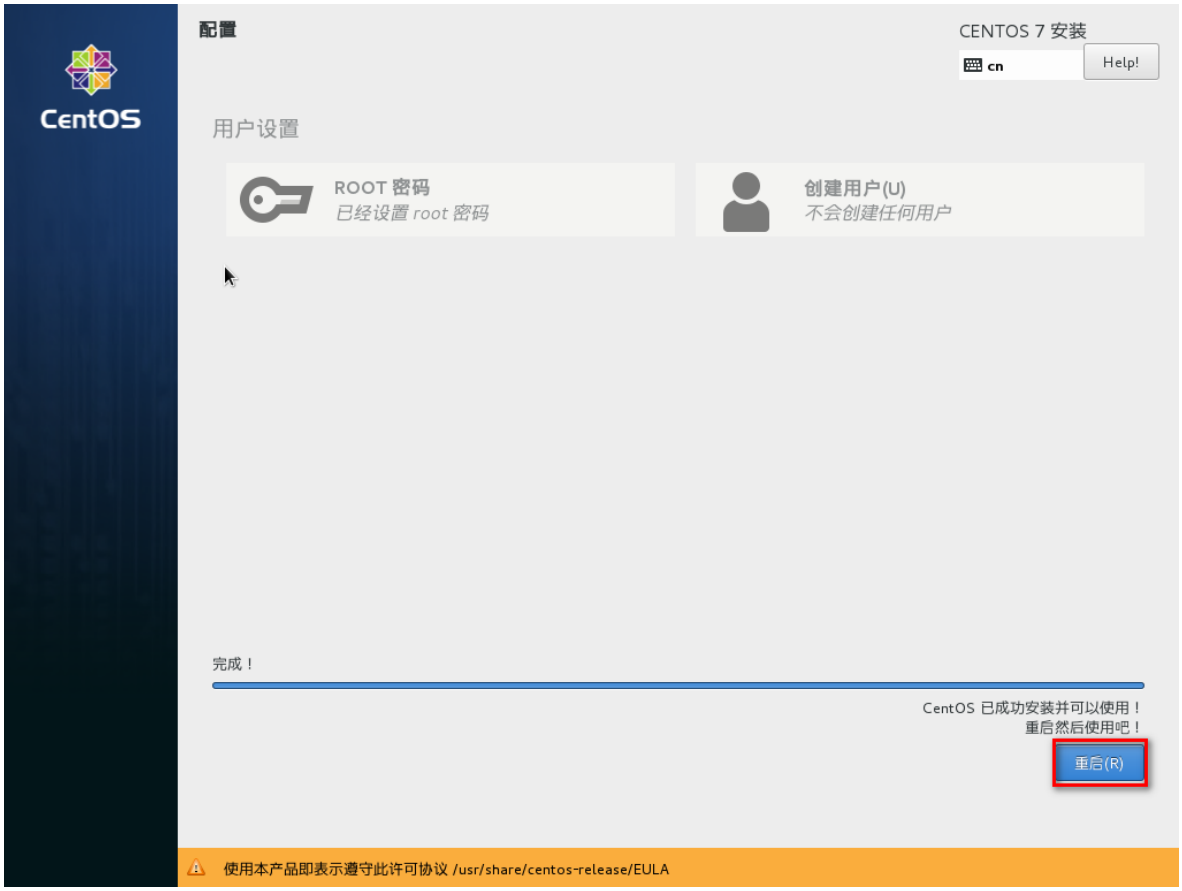


图E-154 点击完成


手动分区
完成(D)
CENTOS 7 安装
cn
帮助！
新 CentOS 7 安装
数据
swap
centos-swap
8192 MiB
系统
/boot
vda1
/
centos-root
centos-root
挂载点(P)：
/
设备：
更改摘要
您的自定义更改将产生以下变更，这些变更将会在您返回到主菜单并开始安装时生效：
顺序 操作 类型 设备名称 挂载点
1 销毁格式 Unknown vda
2 创建格式 分区表 (MSDOS) vda
3 创建设备 partition vda1
4 创建格式 xfs vda1 /boot
5 创建设备 partition vda2
6 创建格式 physical volume (LVM) vda2
7 创建设备 lvmvg centos
8 创建设备 lvmlv centos-swap
9 创建格式 xfs centos-swap /swap
10 创建设备 lvmlv centos-root
11 创建格式 xfs centos-root /
取消并返回到自定义分区(C)
接受更改(A)
更新设置(U)
注意：在您点击主菜单上的'开始安装'按钮之前，您在本屏幕内所做的设置更改不会被应用。
可用空间
992.5 KiB
总空间
1024 GiB
已选择 1 个存储设备(S)
全部重设(R)

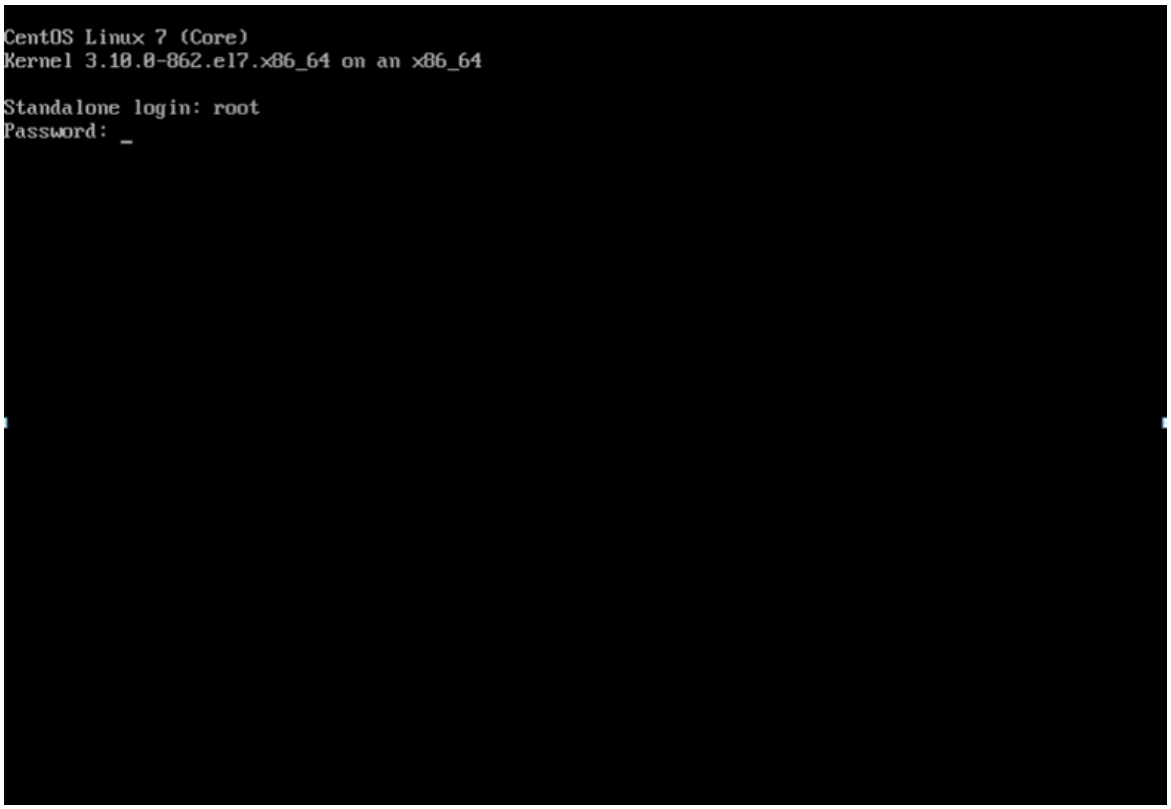

CentOS
安装信息摘要
CENTOS 7 安装
cn
帮助！
本地化
日期和时间(T)
亚洲/上海 时区
键盘(K)
汉语
语言支持(L)
简体中文 (中国)
软件
安装源(I)
本地介质
软件选择(S)
最小安装
系统
安装位置(D)
警告，正在检查存储配置
KDUMP
已启用 Kdump
网络和主机名(N)
未连接
SECURITY POLICY
No profile selected
退出(Q)
开始安装(B)
在点击'开始安装'按钮前我们并不会操作您的磁盘。

图E-155 配置 root 密码



(3) 等候安装完毕后 reboot 系统，输入账号、密码，登录系统。

图E-156 安装完成



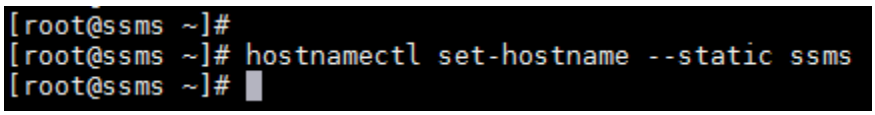
2. 配置静态主机名

(1) 登录系统后，设置静态主机名。

hostnamectl set-hostname --static staticName

eg：hostnamectl set-hostname --static ssms

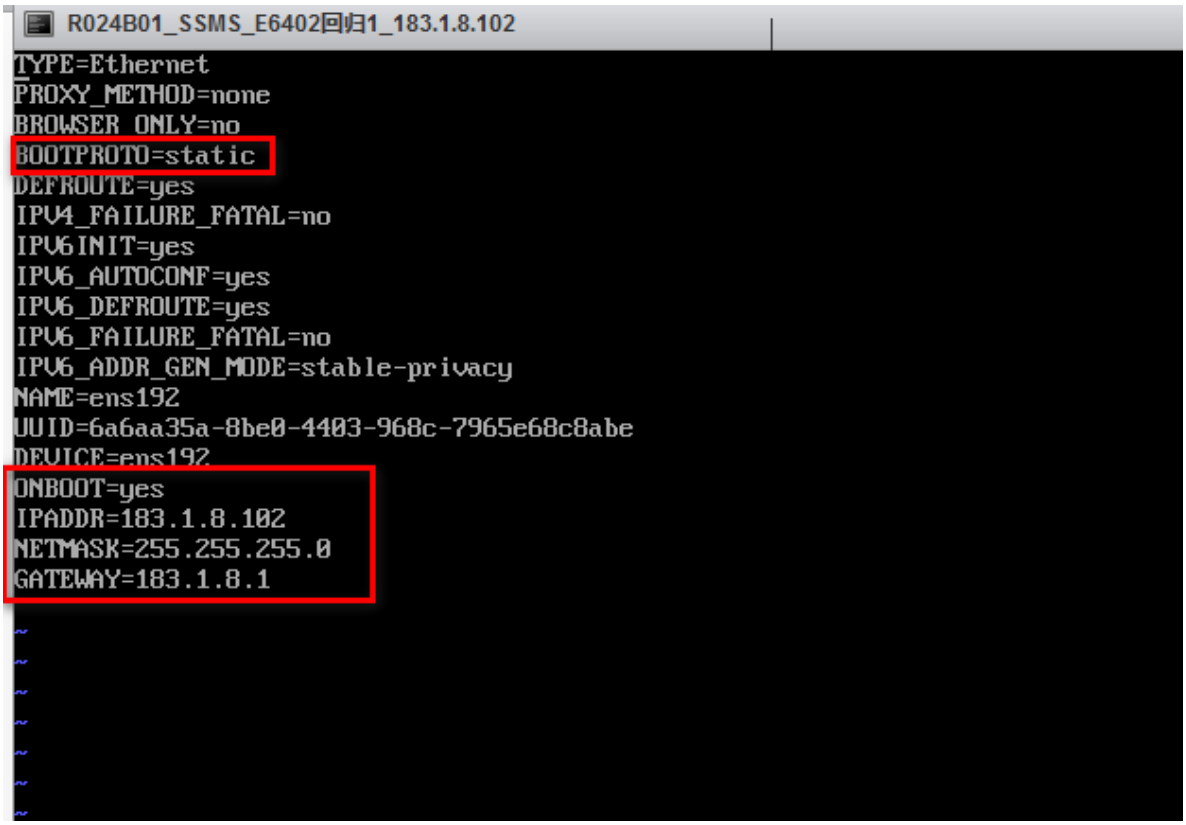
图E-157 配置静态主机名



3. 配置网络

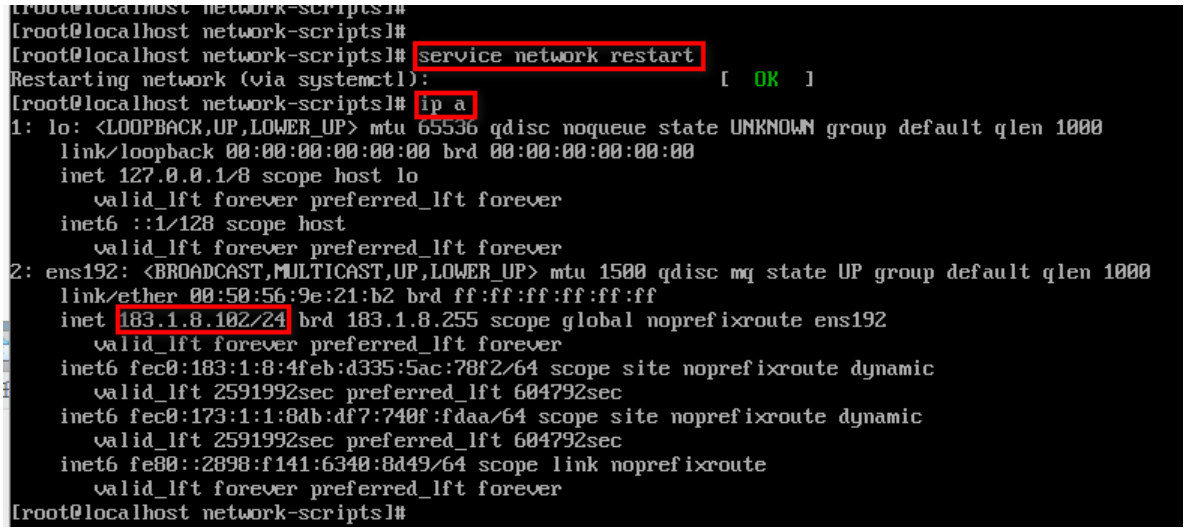
(1) 登录系统后，设置服务端网络参数。输入命令 vi /etc/sysconfig/network-scripts/ifcfg-eth0。（eth0 为该 CAS 虚拟机的网卡名称，VMware 虚拟机的网卡名可能为 ensXXX，请确认自己网卡名称之后修改配置文件）

图E-158 配置静态 IP



退出编辑页面后，输入命令 service network restart 重启网卡。

图E-159 重启网卡

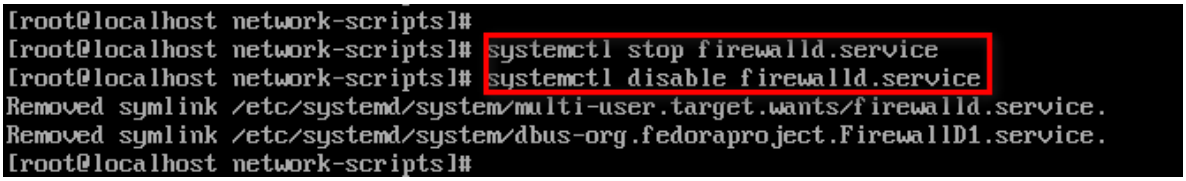


4. 关闭防火墙

systemctl stop firewalld.service　#停止防火墙

systemctl disable firewalld.service　#禁止防火墙开机启动

图E-160 关闭防火墙



5. 系统环境检查

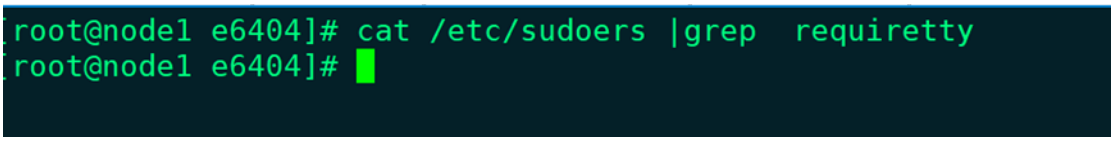
（1）sudoer 文件校验

对/etc/sudoers 文件进行检查，需要注释 Defaults requiretty 选项。

执行：cat /etc/sudoers |grep requiretty

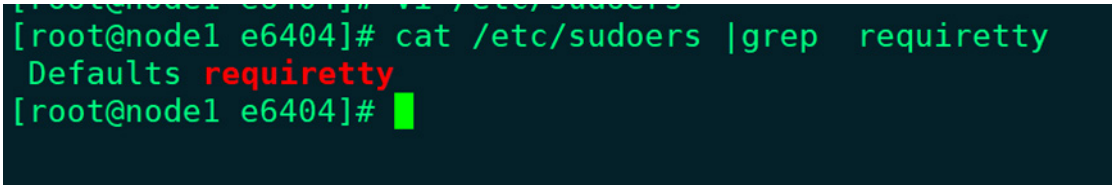
如图显示则可以忽略：

图E-161 sudoer 文件校验-1



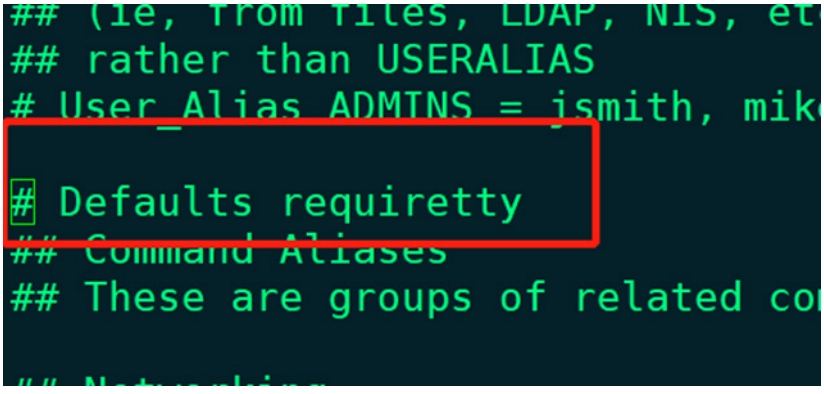
如图显示则需要手动注释：

图E-162 sudoer 文件校验-2



则需要执行: chmod 755 /etc/sudoers && vi /etc/sudoers，注释然后保存退出。如下图：

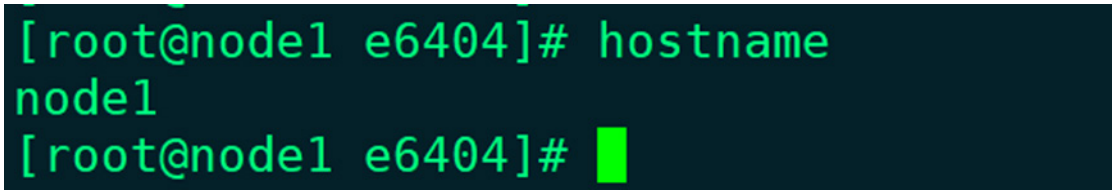
图E-163 sudoer 文件校验-3



（2）检查 hostname 不可以是纯数字或 localhost

执行：hostname

图E-164 hostname 检查



如果显示 localhost 或者纯数字，则执行: hostnamectl set-hostname master

（3）检查/etc/ssh/sshd_config 文件中'RSAAuthentication yes' 'PubkeyAuthentication yes' 两个参数项保证可以使用密钥登陆。若无该参数或者参数值为 yes，无需修改。否则需修改完成后重启 sshd 服务。

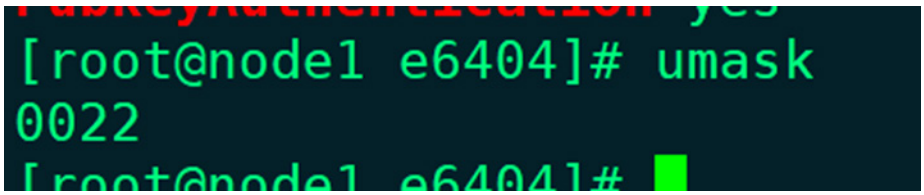
（4）执行 cat /etc/selinux/config 命令查看是否是 SELINUX=disabled 配置

执行: sed -i 's/SELINUX=.*/SELINUX=disabled/g' /etc/selinux/config && setenforce 0

图E-165 SELINUX 参数校验

（5）umask 校验 执 umask 看是否是 0022，不是请执行 umask 0022

图E-166 umask 校验



（6）通过 ssh-copy-id 命令对相关的机器，手动进行免密，保证存在安装包的服务器能免密登录到每一台服务器上（包括自己），免密后请确认是否可以登录（执行 ssh root@IP 无需输入密码即为免密配置成功）。

【双台部署时免密举例】

SSMS 服务端（假设为 A 机器）需要对事件采集服务器（假设为 B 机器）免密登录配置

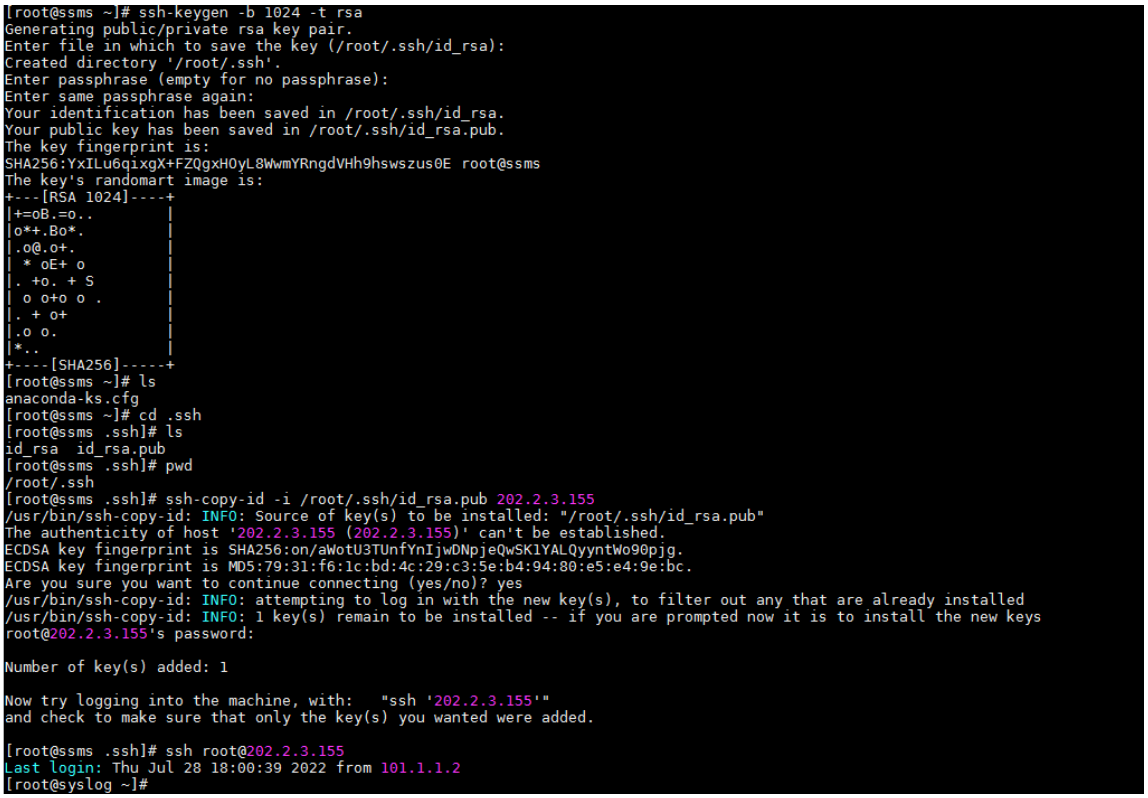
（SSMS 服务器配置）命令举例：

ssh-keygen -b 1024 -t rsa

ssh-copy-id -i /root/.ssh/id_rsa.pub B 机器 IP

ssh root@ B 机器 IP

图E-167 免密登录-1



（事件采集服务器配置）事件采集器上需要对 SSMS 服务端免密配置

命令举例：

ssh-keygen -b 1024 -t rsa

ssh-copy-id -i /root/.ssh/id_rsa.pub A 机器 IP

ssh root@ A 机器 IP

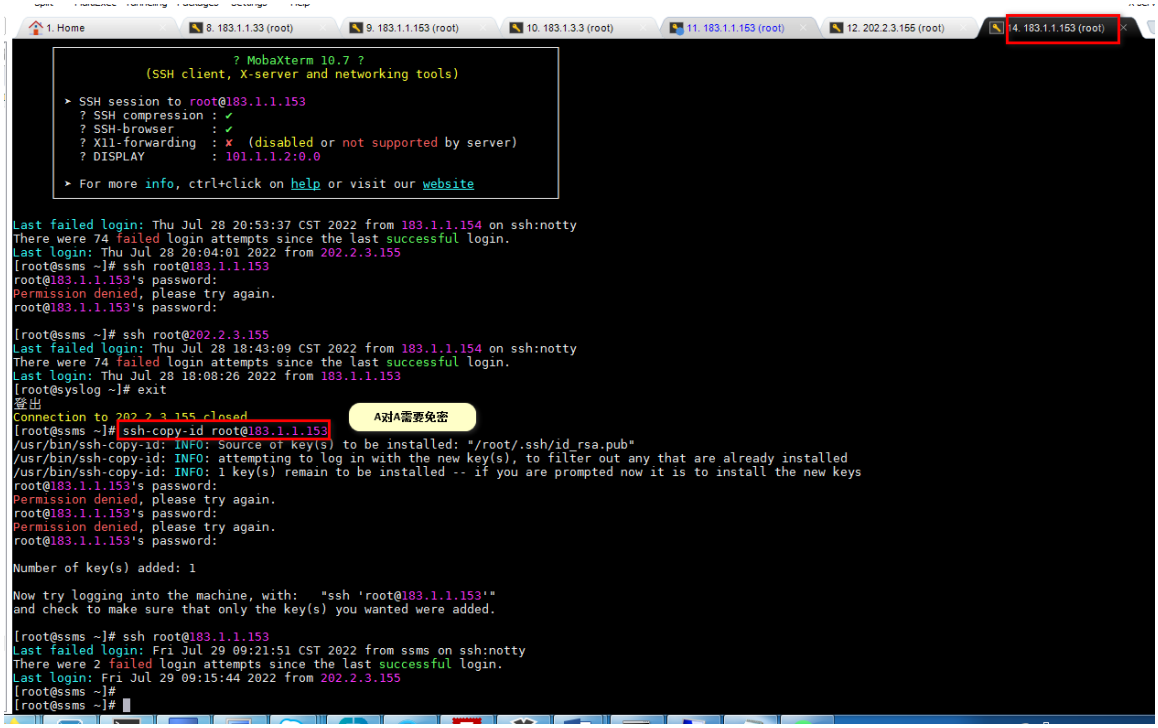
图E-168 免密登录-2

```
[root@syslog ~]# ssh-keygen -b 1024 -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:yGaffaH3H7tJlyM0LtCTnK2m6dspaPOL65u1P+mtFfA root@syslog
The key's randomart image is:
+---[RSA 1024]----+
|                 |
|                 |
|           .     |
|     . .  o *    |
|      = S. *.E   |
|     o . o..=.o .|
|        +.o+++ =.|
|       ++.*==.o *|
|      o**O**o..=o|
+----[SHA256]-----+
[root@syslog ~]#
[root@syslog ~]#
[root@syslog ~]# cd .ssh
[root@syslog .ssh]# ls
authorized_keys  id_rsa  id_rsa.pub
[root@syslog .ssh]# pwd
/root/.ssh
[root@syslog .ssh]# ssh-copy-id  -i /root/.ssh/id_rsa.pub 183.1.1.153
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/root/.ssh/id_rsa.pub"
The authenticity of host '183.1.1.153 (183.1.1.153)' can't be established.
ECDSA key fingerprint is SHA256:KCUO2YbHoReNi3Oh28mQ4/jQg/u2rktvWEi0/yJ7x2k.
ECDSA key fingerprint is MD5:20:c4:e4:40:09:52:28:6e:2f:0e:7b:02:5c:24:b3:7a.
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
root@183.1.1.153's password:

Number of key(s) added: 1

Now try logging into the machine, with:   "ssh '183.1.1.153'"
and check to make sure that only the key(s) you wanted were added.

[root@syslog .ssh]# ssh root@183.1.1.153
Last login: Thu Jul 28 19:47:43 2022 from 101.1.1.2
[root@ssms ~]# exit
登出
Connection to 183.1.1.153 closed.
[root@syslog .ssh]#
```

（SSMS 服务器配置）SSMS 服务端需要对自身进行免密配置

ssh-copy-id root@A 机器 IP

图E-169 免密登录-3

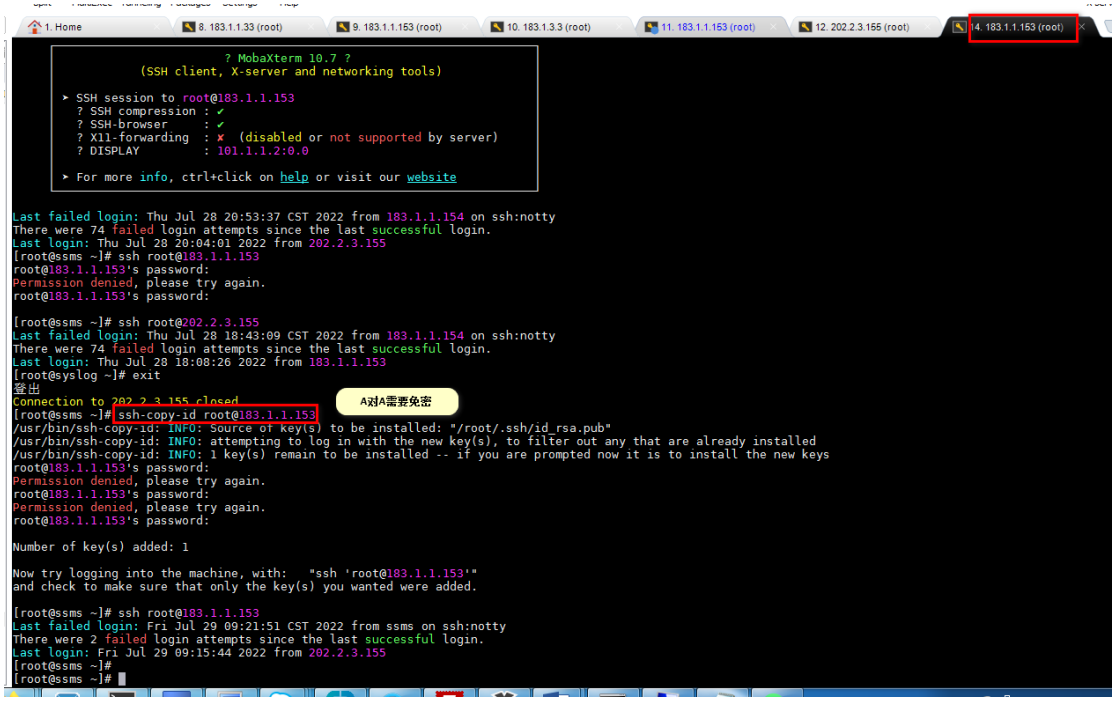


【单台部署时免密举例】

SSMS 服务端需要对自身进行免密配置

ssh-copy-id root@A 机器 IP

图E-170 免密登录-4



（7）请检查对应服务器的时间，若不正确需要自行校准。

E.8.5 x86 服务器安装步骤

1. 准备安装包

- 登录 A 类服务器，以下操作均在 A 类服务器上操作。
- 上传 SecPathSSMS-IMW310-E6404_x86.tar.gz 安装到/opt 目录下
- 上传 auto_install 文件到/opt 目录下
- 进入/opt 目录下执行 tar -zxvf SecPathSSMS-IMW310-E6404_x86.tar.gz 命令进行解压缩

图E-171 安装包解压

```
[root@ssms .ssh]# cd /opt
[root@ssms opt]# ls
auto_install  SecPathSSMS-IMW310-E6404_x86.tar.gz
[root@ssms opt]#
[root@ssms opt]# tar -zxvf SecPathSSMS-IMW310-E6404_x86.tar.gz
temp.tar.gz
sign
patch_h3c.sh
install
sysinfo_common_v3.4.0.10
[root@ssms opt]#
```

- 对 auto_install 文件赋予可执行权限 chmod +x auto_install

图E-172 对 auto_install 文件赋权

```
[root@ssms opt]# chmod +x auto_install
```

- 对 sysinfo_common_v3.4.0.10 文件赋予可执行权限 chmod +x sysinfo_common*

图E-173 对 sysinfo_common*文件赋权

```
[root@ssms opt]# ls
auto_install  install  patch_h3c.sh  SecPathSSMS-IMW310-E6404_x86.tar.gz  sign  sysinfo_common_v3.4.0.10  temp.tar.gz
[root@ssms opt]# chmod +x sysinfo_common_v3.4.0.10
[root@ssms opt]#
```

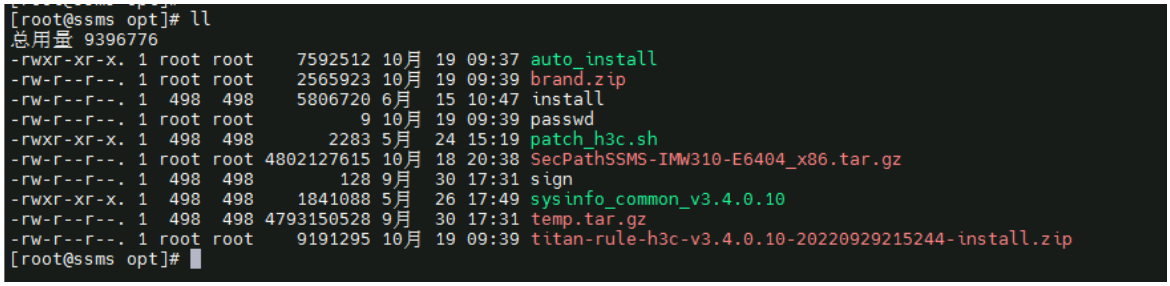
- 准备规则包 titan-rule-h3c-v3.4.0.10-*-install.zip 上传至/opt 目录下

图E-174 规则包上传/opt 目录

```
[root@ssms opt]# ll
总用量 9398044
-rwxr-xr-x. 1 root root    7592440 10月 10 19:59 auto_install
-rw-r--r--. 1 root root    2565703 10月 10 20:13 brand.zip
-rw-r--r--. 1  498  498    5806720 6月  15 10:47 install
drwxr-xr-x. 2 root root         37 10月 10 20:15 install_tmp
-rw-r--r--. 1 root root          9 10月 10 20:13 passwd
-rwxr-xr-x. 1  498  498       2283 5月  24 15:19 patch_h3c.sh
-rw-r--r--. 1 root root 4802127615 10月 10 19:59 SecPathSSMS-IMW310-E6404_x86.tar.gz
-rw-r--r--. 1  498  498        128 9月  30 17:31 sign
-rwxr-xr-x. 1  498  498    1841088 5月  26 17:49 sysinfo_common_v3.4.0.10
-rw-r--r--. 1  498  498 4793150528 9月  30 17:31 temp.tar.gz
-rw-r--r--. 1 root root    1296626 10月 10 20:18 titan-license-h3c344_571-20221109-020221010201708468848.zip
-rw-r--r--. 1 root root    9191295 10月 10 20:12 titan-rule-h3c-v3.4.0.10-20220929215244-install.zip
[root@ssms opt]#
```

- 上传 passwd 文件至/opt 目录下
- 上传 brand.zip 文件至/opt 目录下

图E-175 安装包信息



2. Step 1 获取授权码

- 执行./auto_install license 命令进行授权码获取

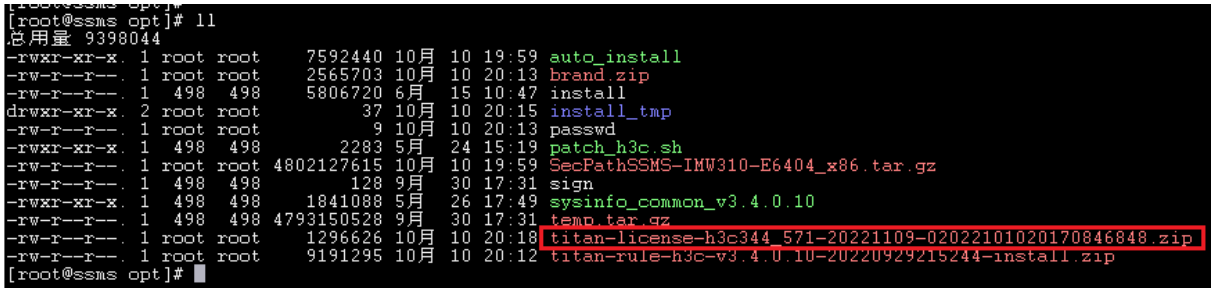
图E-176 授权码获取

- 根据主机的硬件信息，获得唯一的标识号即设备信息，请复制上图授权码，粘贴进 txt 文档中保存，用于申请授权时设备信息文件的导入。

图E-177 设备信息文件

- 申请得到 license 激活文件后，将授权文件上传至/opt 目录下(与 auto_install 文件同级目录)

图E-178 授权文件上传/opt 目录



3. Step 2 执行安装程序

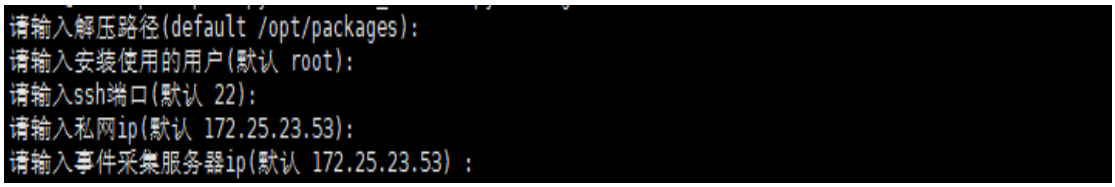
【单台部署】(事件采集 APP 和其它程序全部安装在一台机器上)

- 执行./auto_install install 命令执行安装命令
- 配置解压路径，若不修改，直接回车即可
- 安装用户默认为 root 一般不做修改，ssh 端口默认为 22 根据实际情况修改
- 私网 IP 必须配置，一般为目标服务器 IP，即机器 A 的 IP
- 域名根据实际情况配置，默认不配置
- 公网 IP 根据实际情况配置，默认不配置
- 事件采集服务器 IP 必须配置，单台部署时为目标服务器 IP，即机器 A 的服务器 IP
- 配置完毕后，程序会自动进行剩余安装步骤，并输出相关安装信息，如有报错根据实际情况处理

【两台部署】(事件采集服务器单独部署在一台机器上)

- 检查两台机器的配置，配置信息请看本手册的安装说明
- 对两台机器都进行系统环境检查，相关操作请看本手册 4.5
- 请进行相关检查保证两台机器可以相互免密登录，在机器 A 上可以免密登录到 B，在机器 B 上可以免密登录到 A，且机器 A 可对自身免密
- 在机器 A 上执行./auto_install install 命令执行安装命令
- 配置解压路径
- 安装包解压后进行相关配置
- 安装用户默认为 root 一般不做修改，ssh 端口默认为 22 根据实际情况修改
- 私网 IP 必须配置，配置机器 A 的服务器 IP
- 域名根据实际情况配置，默认不配置
- 公网 IP 根据实际情况配置，默认不配置
- 事件采集服务器 IP 必须配置，双台部署时事件采集服务器 IP，即机器 B 的服务器 IP
- 配置完毕后，程序会自动进行剩余安装步骤，并输出相关安装信息，如有报错根据实际情况处理

图E-179 双台部署时安装举例



安装过程中可实时查看控制台信息，了解安装详细信息。若安装时出现异常，可在控制台中查看错误、异常信息。

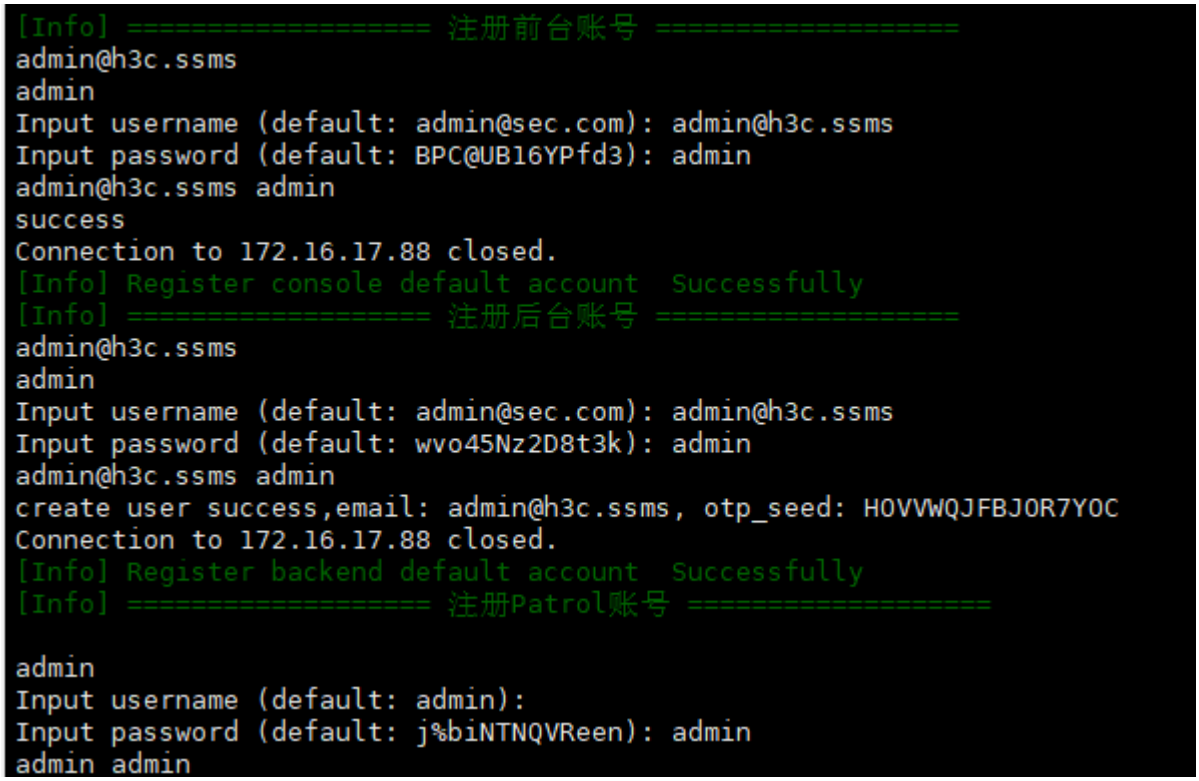
图E-180 实时输出

图E-181 安装日志输出

4. Step 3 安装完成

安装完毕后，最后会输出默认帐号和密码

图E-182 账号输出

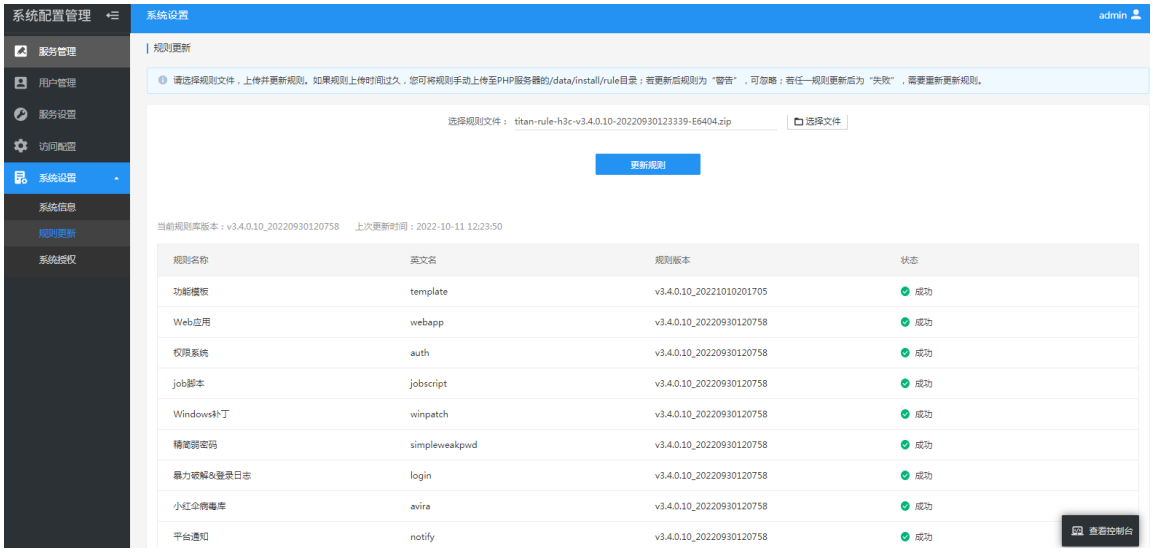


- 在浏览器的网址栏输 http://ServerIP:80 进入 H3C SecPath 服务器安全监测系统登录页。
- 在浏览器的网址栏输 http://ServerIP:81 进入用户管理后台界面。
- 在浏览器的网址栏输 http://ServerIP:6110 进入 patrol 管理界面，即系统配置管理界面。

5. Step 4 导入规则

- 在浏览器的网址栏输 http://ServerIP:6110 进入 patrol 管理界面
- 选择“系统设置>规则更新”下的规则导入，点击选择文件上传规则包 titan-rule-h3c-v3.4.0.10-20220930123339-E6404.zip

图E-183 规则更新



- 点击更新规则进行规则更新，规则更新完成后，表示 SSMS 已部署完成。

E.9 二代服务器安装监测部署

SSMS-Cloud 的管理端可以安装在 Ubuntu16、18，centos7、8 操作系统上。

E.9.1 SSMS-Cloud 管理端安装

此处以 SSMS-Cloud 在 centos7 的安装举例说明，部署包名称举例：SecPathSSMSC-IMW310-E6901.tar。

1. 部署环境要求

硬件要求

- CPU 核数：>=4 核
- 内存：>=16G
- 硬盘：>=512G(建议)

操作系统要求

- 支持 Linux 发行版本列表
  - Ubuntu：16、18
  - Centos：7、8
- Linux 内核要求 >= 3.10
- GLIBC >= 2.17
- GLIBCXX >= 3.4.19
- Python 2.7

端口占用

服务部署占用比较多端口，建议单独机器部署，不要与其它业务混用。

表E-5 端口占用表

源设备	目的设备	目的端口	特性名称	是否可关闭
web客户端	SSMS-Cloud管理中心	443 8303 8304 8305	nginx	否
OPEN API	SSMS-Cloud管理中心	8306	OPEN API	否
secAgent客户端	SSMS-Cloud管理中心	1812 1813 1814 8090	secAgent通讯	否
SSMS-Cloud管理中心	SSMS-Cloud管理中心自带mysql服务	3306	SSMS-Cloud内部通讯端口	否
SSMS-Cloud管理中心	SSMS-Cloud管理中心自带redis服务	6379	SSMS-Cloud内部通讯端口	否
SSMS-Cloud管理中心	SSMS-Cloud管理中心自带elastic服务	9200 9300	SSMS-Cloud内部通讯端口	否
SSMS-Cloud管理中心	SSMS-Cloud管理中心	8100 8102 8098 8586 8587 8588 8580 35357 8302 8143 8988 8989 8000 9105 12345	SSMS-Cloud内部通讯端口	否

2. 部署包说明

获取部署包：SecPathSSMSC-IMW310-E6901.tar.gz。

解压部署包：tar -zxvf SecPathSSMSC-IMW310-E6901.tar.gz，生成 README、deploy_script.tar.gz、images.tar.gz 三个文件。文件说明如下：

- deploy_script.tar.gz：部署安装包。
- images.tar.gz：部署镜像。
- README：记录 deploy_script.tar.gz 和 images.tar.gz 的 md5 信息。

3. 环境检测

(1) 将安装包 SecPathSSMSC-IMW310-E6901.tar.gz 传入 Centos7 主机中。

(2) 解压安装包：tar -zxvf SecPathSSMSC-IMW310-E6901.tar.gz，生成 README、deploy_script.tar.gz、images.tar.gz 三个文件。文件说明如下：

- deploy_script.tar.gz：部署安装包。
- images.tar.gz：部署镜像。
- README：记录 deploy_script.tar.gz 和 images.tar.gz 的 md5 信息。

(3) 解压部署安装包：tar –zxvf deploy_script.tar.gz, 进入解压的[output/deploy]目录：cd output/deploy。

(4) 执行环境检测命令： bash deploy.sh envcheck。

提示

环境检查的结论会在最后以 The conclusion of environment checking is :fail/pass 打印出来，fail 表示环境检查未通过，pass 表示环境检查通过;

未通过的检查项会以表格形式打印出来，检查结果示例如图。

图E-184 命令示意图

```
--------------------------------------------------------------------------------
[sec-server-eplite] environment checking start >>>>>>>>>>>>>
>>>>>>>>>>>>>nic checking: ... pass( Find physics network interface card: /bin/sh: netstat: command not found  )
>>>>>>>>>>>>>machine checking: ... fail( You are running on a virtual machine. )
>>>>>>>>>>>>>memory checking: ... pass( claim is >=15 GB, real is 15 GB )
>>>>>>>>>>>>>port checking: ...
            pass
[default] environment checking start >>>>>>>>>>>>>
>>>>>>>>>>>>>cpu_digit checking: ... pass( claim is .*x86_64.*, real is x86_64 )
>>>>>>>>>>>>>glibc_version checking: ... pass( claim is 2.14, real is 2.17 )
>>>>>>>>>>>>>python_version checking: ... pass( claim is 2.7, real is 2.7.5 )
>>>>>>>>>>>>>kernel_version checking: ... pass( claim is 3.10, real is 3.10.0 )
>>>>>>>>>>>>>glibcxx_version checking: ... pass( claim is 3.4.19, real is 3.4.19 )
>>>>>>>>>>>>>disk_home checking: ... pass( claim is >=512 GB, real is 541 GB )
>>>>>>>>>>>>>cpu_model checking: ... fail( claim is .*(Intel|AMD).*, real is 2  Hygon C86 7265 24-core Processor )
>>>>>>>>>>>>>release_version checking: ... pass( centos 7.7.1908 )
>>>>>>>>>>>>>root checking: ... pass
>>>>>>>>>>>>>network checking: ... pass( Get IP informations: ens3:183.1.3.223/24  )
The conclusion of environment checking is :fail
未通过的检查项详情如下:
You can use 'pip install prettytable' to use PrettyTable.
        模块          检查项        指标要求                实际参数或报错信息
 sec-server-eplite  * machine                    You are running on a virtual machine.
      default       cpu_model  .*(Intel|AMD).*   2  Hygon C86 7265 24-core Processor
* means this is just a suggested standard, the installation may fail due to it.
/root/output/deploy
```

注意

未通过的检查项表格列出了未通过检查项所属的模块、检查项名称、检查项含义、检查项应满足的要求、检查项实际结果或报错信息。检查项名称前带*的表示此检查项非强制要求。

(5) 检查环境检测命令执行结果。

注意

若环境检查通过，可进行部署。

若环境检查未通过，可根据未通过项表格的提示自行排查，或将日志提供给 H3C 支持人员，日志位于 output/tools/environment_check/scripts/envcheck.log。

4. 部署环境初始化

(1) 服务器时间同步。

a. 检查服务器时间是否为北京标准时间，使用下面的命令查看是否为东 8 区

date –R。

如果展示结果中有+0800，则表示当前为东 8 区时间。

b. 如果时区不正确，按照如下方法配置。

- 执行 tzselect
- 选择 Asia，输入 5 回车
- 选择 China，输入 9 回车
- 选择 Beijing Time，输入 1 回车
- 选择 Yes，输入 1 回车
- 执行 echo "TZ='Asia/Shanghai'; export TZ" >> /etc/profile
- source /etc/profile 使配置生效。
- ln -sf /usr/share/zoneinfo/Asia/Shanghai /etc/localtime

(2) 执行环境初始化命令：bash deploy.sh init。

图E-185 命令示意图

```
[root@localhost deploy]# sh deploy.sh init
start deploy docker.
注意docker将部署到/home/docker目录,确认目录下有足够磁盘空间。是否继续部署[Y/N]y
ok
Created symlink from /etc/systemd/system/multi-user.target.wants/docker.service to /etc/systemd/system/docker.service.
deploy docker success.
start collect finger..
0/root/output/deploy
[root@localhost deploy]#
```

5. 服务部署

(1) 执行下面的命令，导入服务器安全监测服务器安全监测服务镜像，此过程花费的时间会较长。

执行命令：bash deploy.sh load 镜像路径

例如： bash deploy.sh load /root/images.tar.gz

图E-186 命令示意图

```
[root@localhost deploy]# sh deploy.sh load /root/images.tar.gz
loading images...
tar /root/images.tar.gz Successful
174f56854903: Loading layer [==================================================>]  211.7MB/211.7MB
2eb116c16f24: Loading layer [==================================================>]  231.5MB/231.5MB
b2a99c0ad2d2: Loading layer [==================================================>]  380.9kB/380.9kB
3511a9b5f79b: Loading layer [==================================================>]  13.52MB/13.52MB
ff94f5b7babe: Loading layer [==================================================>]  22.43MB/22.43MB
85a03bdb2472: Loading layer [==================================================>]  3.072kB/3.072kB
06dbe4627a09: Loading layer [==================================================>]   12.8kB/12.8kB
94fa71eb1554: Loading layer [==================================================>]  8.192kB/8.192kB
0b22f81e8ea1: Loading layer [==================================================>]  13.82kB/13.82kB
2f3f3ce6d2c3: Loading layer [==================================================>]  3.072kB/3.072kB
4100617077db: Loading layer [==================================================>]  133.5MB/133.5MB
```

(2) 一键部署服务器安全监测服务器安全监测服务。

执行命令：bash deploy.sh install

如果执行 bash deploy.sh install

报[ERROR]无效的厂商名。 后面加 h3c 再执行

即 bash deploy.sh install h3c

图E-187 命令示意图

```
[root@localhost deploy]# sh deploy.sh install
create directory: /home/bss/deploy
current vm.max_map_count: 65530,increase to at least [262144]
vm.max_map_count = 262144
crontab:docker exec -u 1004 Hosteye-Iam /bin/bash -c 'sh /home/abcsecurity/iam/opbin/log/logMgr.sh' is not exist
crontab:docker exec -u 1004 Hosteye-Iam /bin/bash -c 'sh /home/abcsecurity/iam/opbin/tools/clean_expired_tokens.sh > /home/abcsecurity/iam/opbin/token_clean.log' is not exist
crontab:docker exec -u 1004 Hosteye-Server /bin/bash -c 'bash /home/abcsecurity/meta/meta/backuplog.sh -T D -P /home/abcsecurity/meta/log -F BSS_SERVICE,BSS_SERVICE.wf,bss_service.log,bss_se
ce.log.wf -S 15 -B /home/abcsecurity/meta/log' is not exist
crontab:docker exec -u 1004 Hosteye-Server /bin/bash -c 'bash /home/abcsecurity/hosteye/op/log_mange.sh -T D -P /home/abcsecurity/hosteye/log -F auth_server.log,auth_server.log.wf,command_se
r.log,command_server.log.wf,communication_server.log,communication_server.log.wf -S 7' is not exist
3306
6379
9200
9300
8100
8102
8098
8587
8586
8588
8580
35357
8302
8143
8988
8989
8000
8083
license server exit success [grace].
/root/output/deploy
请输入本机内网IP地址(通讯网卡IP):
183.1.3.223
请输入外网访问IP地址(无外网地址，配置内网IP地址),用户通过此IP访问主机安全管理界面:
183.1.3.223
是否已登录主机安全docker镜像仓库？[y/n],(镜像已经下载到本地情况,不用登录选[y])y
ok
Creating Hosteye-Redis   ... done
Creating Hosteye-Elastic ... done
Creating Hosteye-Mysql   ... done
Creating Hosteye-Fe      ... done
Creating Hosteye-Nginx   ... done
Creating Hosteye-Iam     ... done
Creating Hosteye-Consolehub ... done
Creating Hosteye-Server     ... done
Start running autoMonitor.
start read config ../conf/autoMonitor.xml
No child node of monitor_config/golbal/redis_item/pwd!
```

⚠ 注意

“请输入本机内网 IP 地址（通讯网卡 IP）”

此 IP 用于各服务之间的通讯，可以与“外网访问 IP”相同

“请输入外网访问 IP 地址”:

此 IP 作为服务器安全监测系统的管理 IP 与外界通讯。

---

(3) 检查服务是否启动完成。

服务端启动完成大约 5 分钟左右，可通过以下命令检测服务启动情况：

执行命令： bash deploy.sh status

图E-188 命令示意图

```
[root@localhost deploy]# sh deploy.sh status
which: no netstat in (/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/root/bin)
Service started successfully!
[root@localhost deploy]#
```

提示

回执 "xxx is not bind, Service is starting, Please wait a minute..." 信息说明服务还在启动中，稍后可再执行一遍确认是否已启动完成。

回执 "Service started successfully!" 信息说明服务已启动完成，可执行步骤 4

(4) 导入漏洞库。

执行命令： bash deploy.sh vul &

注意

漏洞库导入时间比较长，一般需要 30 分钟左右才能导入完毕。

(5) 部署完成，登录 web 控制台验证，登录不上，关闭防火墙解决。

a. 浏览器访问 https://管理端 IP。

b. 输入用户名、密码、验证码，默认用户名、密码 admin/admin。

图E-189 登录示意图

注意

- 部署人员注意以下几个端口的防火墙策略:
- 服务管理界面通讯端口：443、8303、8304、8305。
- 客户端与服务端通讯端口：1812、1813、1814、8090。

E.9.2 Agent 安装

1. Linux Agent 安装

前提条件

(1) 目前已适配下列 Linux 操作系统。

表E-6 Agent 的 Linux 操作系统适配表

系统名称	版本信息
Linux操作系统	CentOS 6.4 X86_64 (64bit) CentOS 6.5 X86_64 (64bit) CentOS 6.8 X86_64 (64bit) CentOS 7.1 X86_64 (64bit) CentOS 7.2 X86_64 (64bit) CentOS 7.3 X86_64 (64bit) CentOS 7.4 X86_64 (64bit) CentOS 7.5 X86_64 (64bit) CentOS 7.6 X86_64 (64bit) openSUSE 42.3 (64bit) debian 7.5.0 amd64 (64bit) debian 8.1.0 amd64 (64bit) debian 9.1.0 amd64 (64bit) Ubuntu 14.04.1 LTS amd (64bit) Ubuntu 16.04.1 LTS amd (64bit) Ubuntu 18.04.1 LTS amd (64bit)

(2) 需要提前安装 curl 或 wget 工具。

(3) 需要提前启动 Cron 定时任务服务（系统默认自动开启）。

安装步骤

需要以 root 权限在 shell 中执行安装命令。

(4) 在您的 Linux 云服务器系统中执行下面两条命令中的其中一条，安装服务器安全监测服务器安全监测客户端。

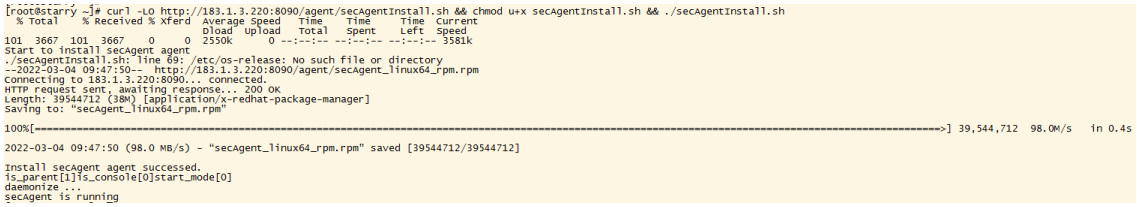
- wget -c http:// X.X.X.X:8090/agent/secAgentInstall.sh -O secAgentInstall.sh && chmod u+x secAgentInstall.sh && ./secAgentInstall.sh
- curl -LO http://X.X.X.X:8090/agent/secAgentInstall.sh && chmod u+x secAgentInstall.sh && ./secAgentInstall.sh

注：X.X.X.X 为 SSMS-Cloud 管理端主机 IP

(5) 安装过程如下图所示，如果提示 secAgent is running，表明已经正常启动，安装结束。

- Centos (64 位)

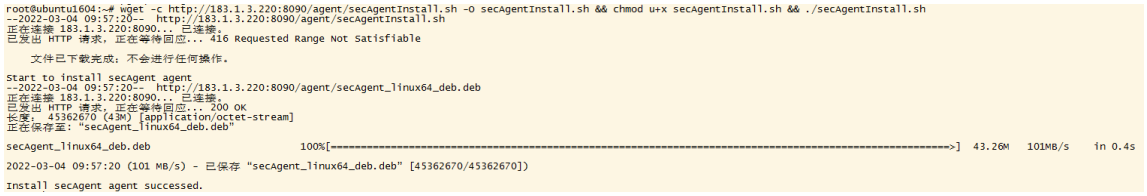
图E-190 命令示意图



如果提示 rpm 未安装，则先安装 rpm，再执行上一步。

- Ubuntu/Debian（64 位）

图E-191 命令示意图

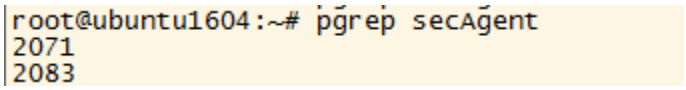


如果提示 dpkg 未安装，则先安装 dpkg，再执行上一步。

(6) 执行命令 pgrep secAgent 检查服务器安全监测服务器安全监测客户端是否正常启动。

(7) 如果命令结果返回两个进程号，表明已经正常启动。

图E-192 命令示意图



其它相关命令

- 重启 agent 服务： service secAgent restart 。如果没有任何异常输出，表明已经正常启动。
- 停止 agent 服务： service secAgent stop 。如果没有任何异常输出，表明正常关闭。
- agent 运行状态： service secAgent status。如果提示 secAgent is running ，表明已经正常启动。

2. Windows Agent 安装

前提条件

目前已适配下列 Windows Server 操作系统。

图E-193 Agent 的 Windows Server 操作系统适配表

系统名称	版本信息
Windows操作系统	Windows server 2008 R2 X86_64 (64bit) 英文版 Windows server 2008 R2 X86_64 (64bit) 中文版 Windows server 2012 R2 X86_64 (64bit) 英文版 Windows server 2012 R2 X86_64 (64bit) 中文版 Windows server 2016 X86_64 (64bit) 英文版 Windows server 2016 X86_64 (64bit) 中文版 Windows server 2019 X86_64 (64bit) 英文版 Windows server 2019 X86_64 (64bit) 中文版

安装步骤

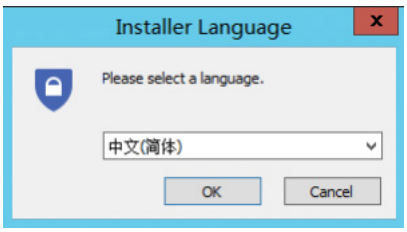
需要以管理员权限运行安装程序。

(2) 下载 Windows 平台服务器安全监测服务器安全监测客户端安装程序。

http://183.1.3.220:8090/agent/secAgent_windows_setup.exe

(3) 运行安装程序，点击“OK”。

图E-194 安装示意图

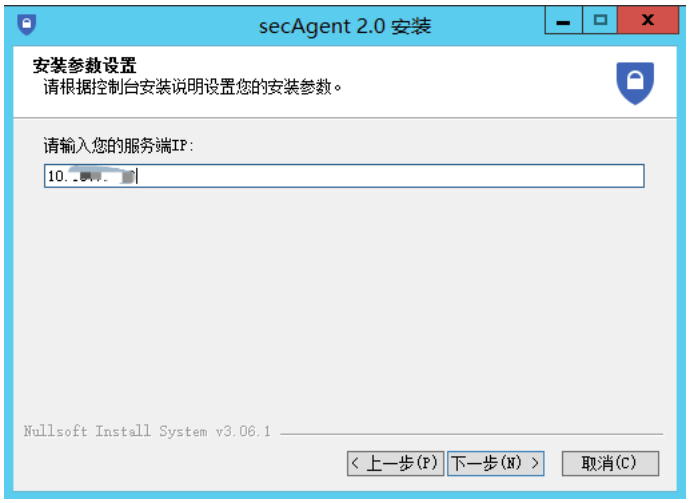


(4) 点击“下一步”。

图E-195 安装示意图

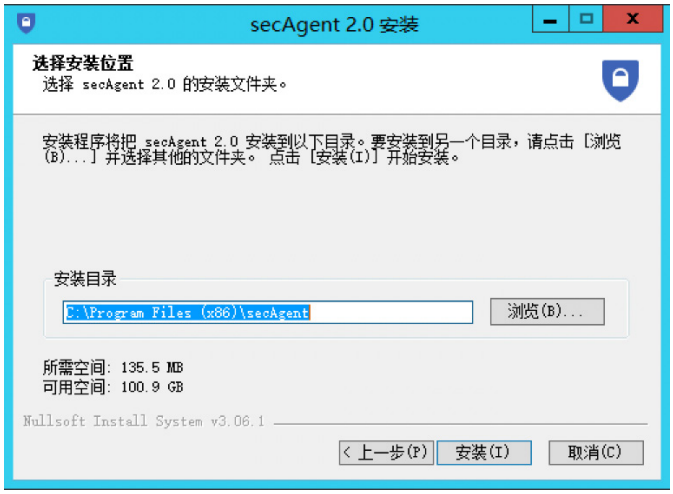
(5) 填入管理端的 IP 地址，然后点击下一步。

图E-196 安装示意图



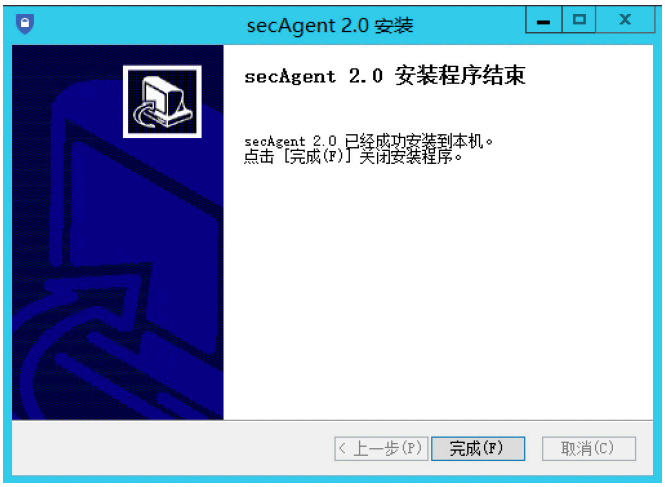
(6) 选择需要安装的位置，默认即可，点击“安装”。

图E-197 安装示意图



(7) 安装完成，点击“完成”按钮。

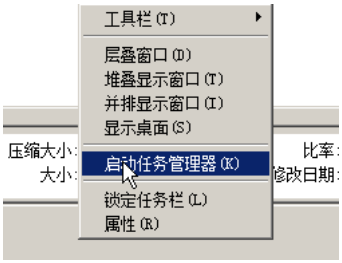
图E-198 安装示意图



(8) 检查状态

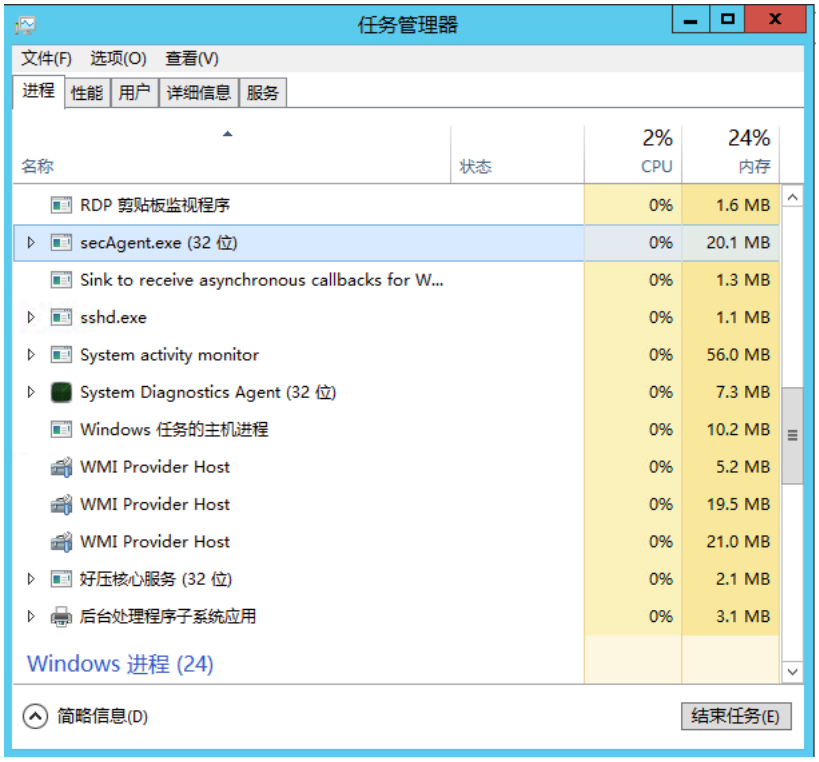
a. 在任务栏上点击鼠标右键，选择“启动任务管理器”，在弹出的任务管理器中点击“进程”。

图E-199 检测状态示意图



b. 在“进程”中查看是否存在 secAgent.exe 这个进程。

图E-200 检测状态示意图



c. 如果无存在该进程，表明未在工作，请重新安装或启动。