UniCloud Workspace 云桌面

安全网关安装部署指导(办公场景)

紫光云技术有限公司
www.unicloud.com

资料版本：5W100-20230605
产品版本：UniCloud_Workspace-E1015P02

目 录

1 概述

安全网关是 Workspace 云桌面提供的广域网接入组件，用于为用户提供访问 VDI 云桌面资源的统一入口。用户通过安全网关从公网环境访问单位内部云桌面，实现远程办公，同时能保障 VDI 云桌面资源的安全。

2 安装前准备

2.1 配置要求

安全网关可以部署在一台物理服务器或者虚拟机上，虚拟机安全网关的最低配置要求如下表所示：

表2-1 虚拟机安全网关配置要求

网关配置	网关数量	支持点数	服务器数量	千兆网口数量	万兆网口数量	配置方式
CPU：4 vCPU 主频 ≥ 2.3GHz 内存：4 GB 硬盘 ≥50 GB SSD 操作系统：H3Linux	1	50	1	1	-	单网卡
	2	100	2	2	-	网关HA
	2	150	3	4	2	网关HA
	2	200	4	4	2	网关HA
CPU：8 vCPU 主频 ≥ 2.3GHz 内存：8 GB 硬盘 ≥50 GB SSD 操作系统：H3Linux	2	250	5	6	2	网关HA
	2	300	6	6	2	网关HA
	2	350	7	8	2	网关HA
	2	400	8	-	2	网关HA
CPU：4 vCPU 主频 ≥ 2.3GHz 内存：4 GB 硬盘 ≥50 GB SSD 操作系统：H3Linux	3	450	9	6	3	软负载均衡
	3	500	10	6	3	软负载均衡
	3	550	11	6	3	软负载均衡
	3	600	12	6	3	软负载均衡
CPU：8 vCPU 主频 ≥ 2.3GHz 内存：8 GB 硬盘 ≥50 GB SSD 操作系统：H3Linux	2	450	9	8	2	软负载均衡
	2	500	10	-	2	软负载均衡
	2	550	11	-	2	软负载均衡
	2	600	12	-	2	软负载均衡
	2	650	13	-	2	软负载均衡
	2	700	14	-	2	软负载均衡
	2	750	15	-	2	软负载均衡
	2	800	16	-	2	软负载均衡

网关配置	网关数量	支持点数	服务器数量	千兆网口数量	万兆网口数量	配置方式
	2	850	16	-	2	软负载均衡
CPU：4 vCPU 主频 ≥ 2.3GHz 内存：8 GB 硬盘 ≥50 GB SSD 操作系统：H3Linux	2	800	16	-	4	软负载均衡+DPDK
	3	850	17	-	6	软负载均衡+DPDK
	3	900	18	-	6	软负载均衡+DPDK
	3	950	19	-	6	软负载均衡+DPDK

说明

- 表中的“千兆网口”与“万兆网口”配置为二选一，并非同时配置。
- 表中的网口均为外网网口，其中千兆网口推荐做聚合。
- 如果要开启 SR-IOV+安全网关 DPDK 功能，目前仅支持使用 Intel 82599 系列网卡，且宿主机的 CPU 最低配置为 Intel Haswell(2013 年发布)，ARM 架构主机不支持 DPDK 功能。
- 如果要启用网关支持 IDV/VOI 功能，则网关配置需满足: 16 vCPU、内存 16 GB、硬盘 100 GB、内外网口均为万兆网口。

2.2 安装软件准备

在开始部署安全网关之前，请从 UniCloud 官方渠道获取正式发布的最新版本安装软件，安装软件清单如下表所示。

表2-2 安装文件清单

软件包名称	说明
UniCloud_Workspace_Gateway_Solution-*version-x86_64*.tar.gz	X86架构安全网关安装包，包含安全网关和软件LB两种功能
UniCloud_Workspace_Gateway_Solution-*version*-aarch64.tar.gz	ARM架构安全网关安装包，包含安全网关和软件LB两种功能
H3Linux_K414_V112_BBR.iso	X86架构网关底层操作系统
H3Linux_K414_V112_ARM.iso	ARM架构网关底层操作系统

3 注意事项

安全网关解决方案部署中的注意事项如下：

- 请保障网关虚拟机不被手动或自动迁移。

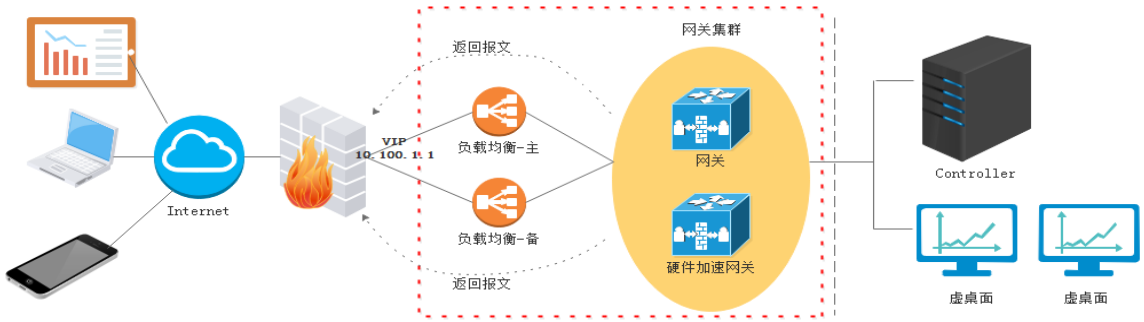
- 启用 SR-IOV+安全网关 DPDK 功能的组网环境不支持 HA 特性。
- 所有命令请以 root 用户权限执行。
- E1009 及之后版本，网关默认端口为 8860。
- 当命令行提示输入[Y/n]以确认执行命令时，直接按下 Enter 键的效果与输入 Y 键后按下 Enter 键相同，即确认执行此操作。

4 部署方案

安全网关提供两种部署场景：非负载均衡部署和负载均衡部署。

- 非负载均衡部署：适用于小规模部署环境，环境中无 LB 设备。
- 负载均衡部署：使用 LB 设备为多个网关提供负载均衡，LB 设备分为硬件 LB 设备与软件 LB，硬件 LB 设备需要用户自行准备，安全网关自带软件 LB，启用软件 LB 的方法请见软件 LB。

图4-1 安全网关部署示意图



说明

- Controller 即 Workspace 云桌面中负责与客户端通信的服务器端组件，部署管理平台时会自动部署 Controller。
- Controller 通常与管理平台部署在同一服务器上，且 IP 地址相同。

本文以部署在虚拟机中为例，部署在物理服务器上的方案类似。

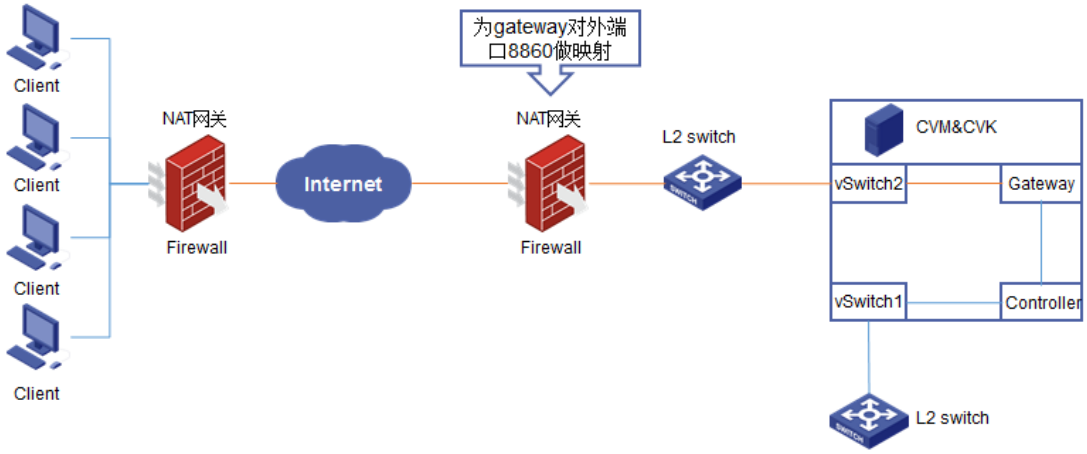
4.1 非负载均衡部署

4.1.1 单台服务器

单台服务器的部署方式要求如下：

- 网关虚拟机配置请参考配置要求。
- 网关的一个网口 vSwitch2 用于外网访问云桌面资源，一个网口 vSwitch1 用于内网的管理网和业务网访问。

图4-2 单台服务器部署网关组网图

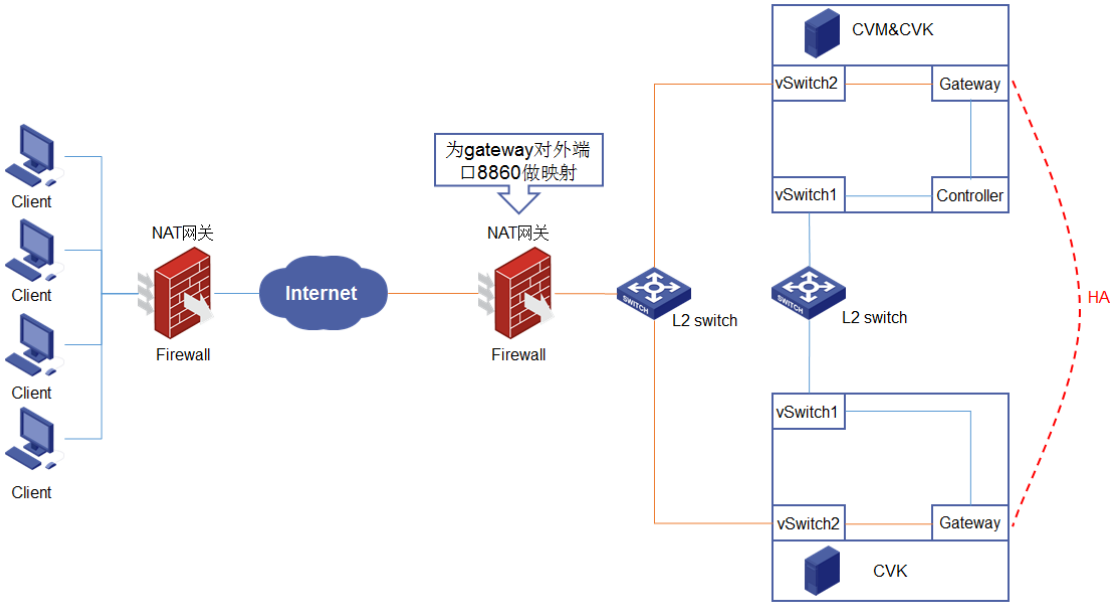


4.1.2 两台服务器单集群

两台服务器单集群的部署方式要求如下：

- 网关虚拟机配置请参考配置要求。
- 网关虚拟机分别部署到两台服务器上组成 HA。
- 每台服务器上各提供一个外网网口给网关用于外网访问，两个网关虚拟机分别关联到各自所在服务器的外网网口。

图4-3 两台服务器单集群网关组网图

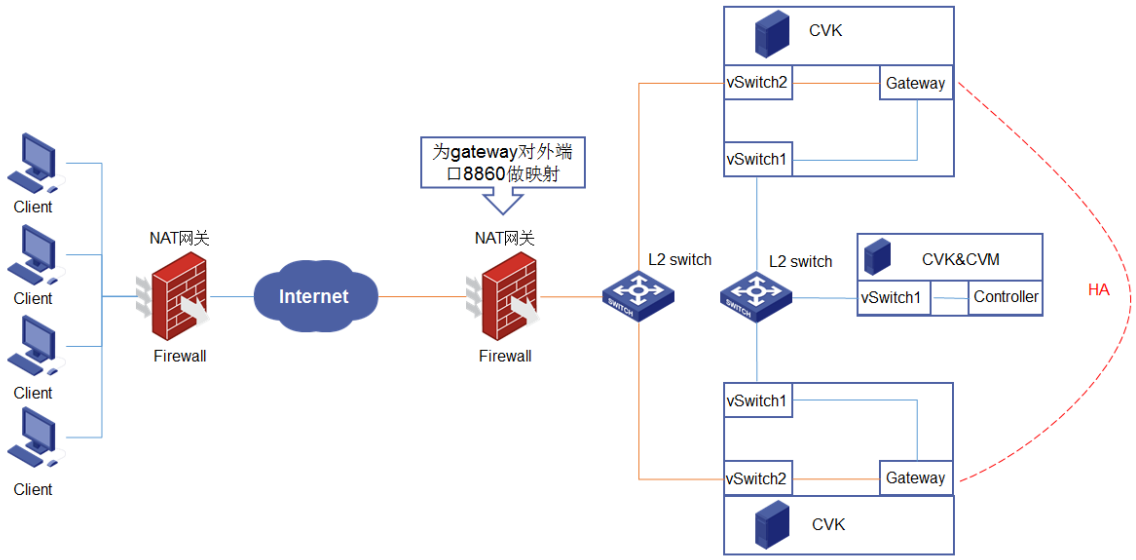


4.1.3 三台及以上服务器单集群

三台及以上服务器部署要求如下：

- 网关虚拟机配置请参考配置要求。
- 网关虚拟机分别部署在两台服务器上组成 HA，推荐将网关和 Controller 部署在不同服务器上，以避免带宽抢占和服务器故障同时影响网关与 Controller 的风险。
- 服务器上各提供一个网口给网关用于外网访问，两个网关虚拟机分别关联到各自所在服务器的外网网口。

图4-4 三台及以上服务器单集群网关组网图

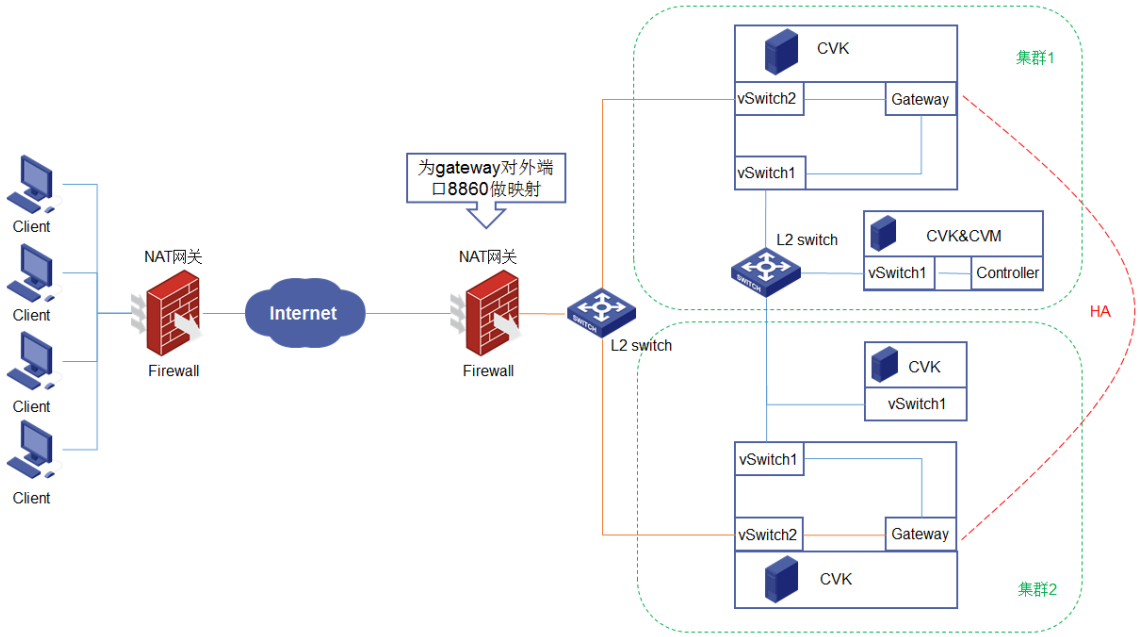


4.1.4 多集群

多集群的部署方式要求如下：

- 网关虚拟机配置请参考配置要求。
- 网关虚拟机分别部署在不同集群的服务器上，推荐将网关和 Controller 部署在不同服务器上，以避免带宽抢占和服务器故障同时影响网关与 Controller 的风险。
- 服务器上各提供一个网口给网关用于外网访问，两个网关虚拟机分别关联到各自所在服务器的外网网口。

图4-5 多集群网关组网图



4.2 负载均衡部署

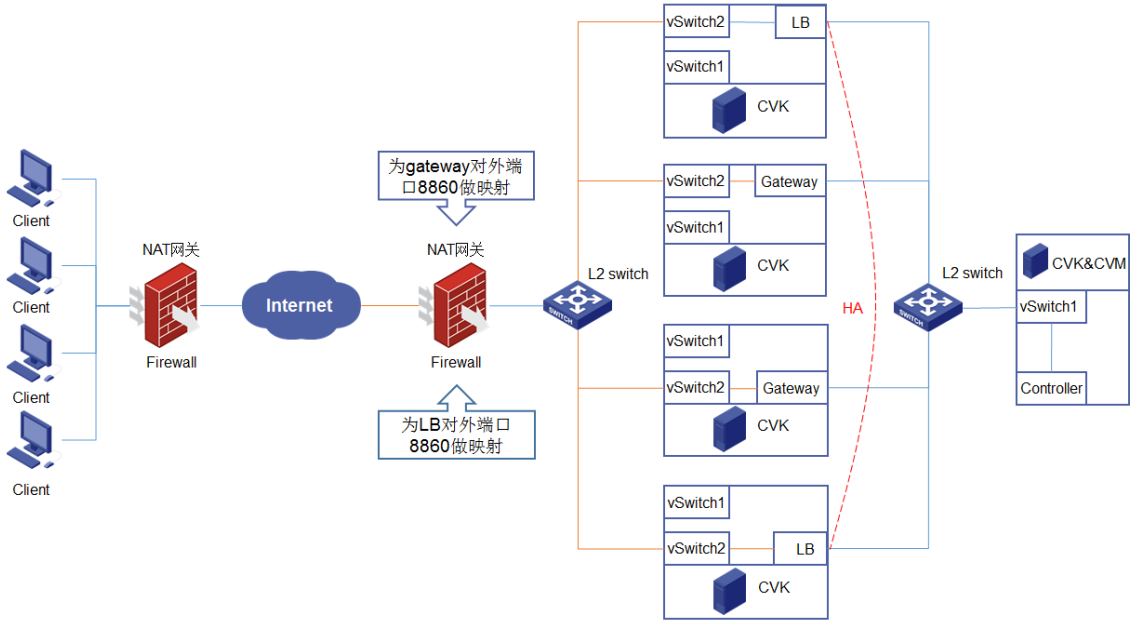
安全网关解决方案提供软件负载均衡模式，负载均衡模式采用高效率转发策略，能提升数据转发性能。450 点云桌面以上规模的局点建议启用负载均衡部署。负载均衡用软件 LB 方案或者 LB 物理设备实现，参与负载均衡的多个网关只能对应同一个 Controller 或 Controller 集群。

4.2.1 单集群

部署要求如下：

- 软件 LB 虚拟机配置、网关虚拟机配置请参考配置要求。
- 两台主备 LB 设备做 HA，分别部署到两台服务器上，网关虚拟机分别部署在不同服务器上。
- 服务器上各提供一个网口给网关用于外网访问，网关虚拟机与软件 LB 虚拟机分别关联到各自所在服务器的外网网口。

图4-6 单集群负载均衡网关组网图

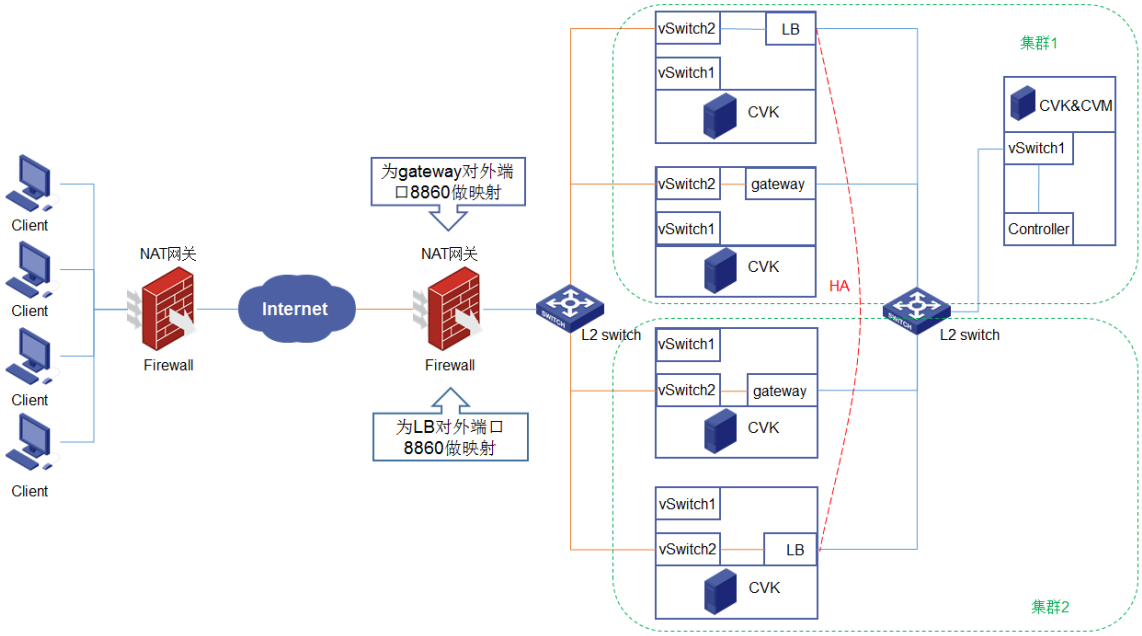


4.2.2 多集群

部署要求如下：

- 软件 LB 虚拟机配置、网关虚拟机配置请参考配置要求。
- 两台主备 LB 设备做 HA，分别部署到不同集群的服务器上，网关虚拟机分别部署在各集群不同服务器上。
- 服务器上各提供一个网口给网关用于外网访问，只有网关虚拟机与软件 LB 虚拟机分别关联到各自所在服务器的外网网口。

图4-7 多集群负载均衡网关组网图



5 网关部署

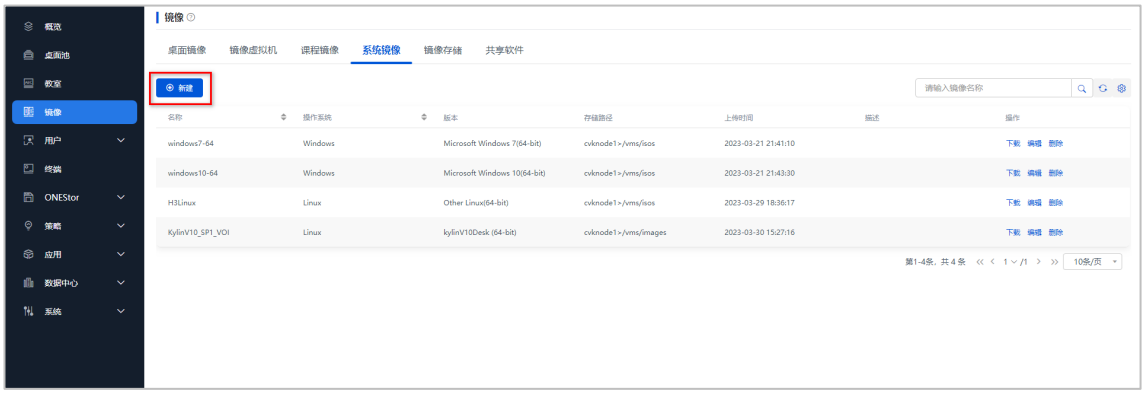
本文中网关部署环境为云下 UniCloud Workspace 环境，云上 UniCloud Workspace 环境的网关请在对应的云下环境中进行部署。

5.1 制作网关虚拟机镜像

X86 架构与 ARM 架构主机制作网关虚拟机镜像的操作步骤(1)-步骤(15)基本相同，ARM 架构主机需额外进行操作步骤(16)-步骤(20)。

(1) 单击左侧导航树[镜像]菜单项，进入镜像页面。在“系统镜像”页签下单击<新建>按钮，弹出“新建系统镜像”对话框。

图1-1 系统镜像页面

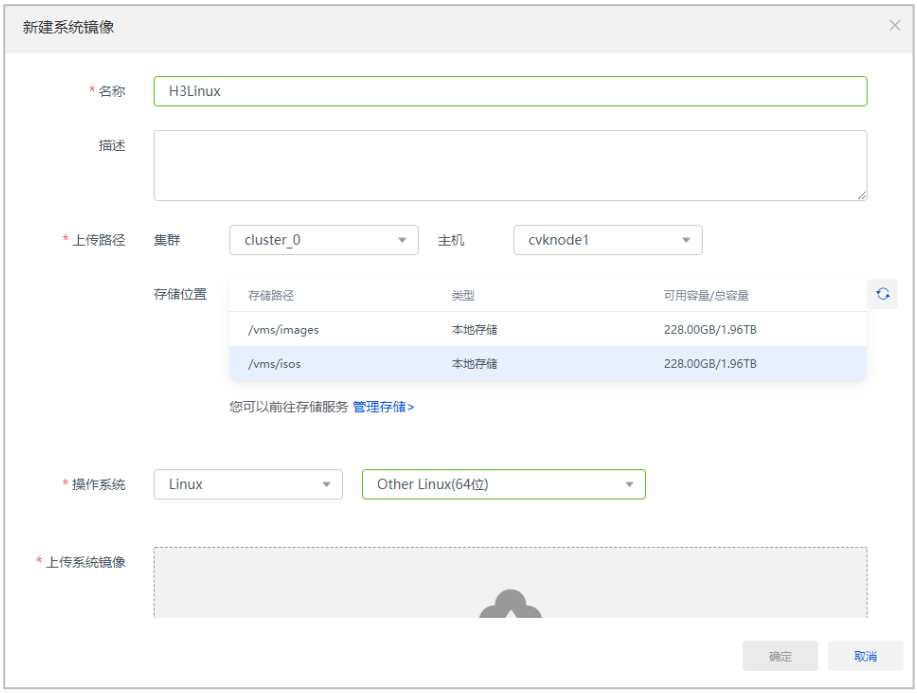


(2) 设置镜像名称，根据上传系统镜像选择操作系统类型及版本，设置系统镜像上传路径，并将镜像文件拖拽到虚线框中，或单击<点击上传>，在弹出的对话框中选择待上传的镜像文件，单击<打开>按钮开始上传镜像。

注意

- 若系统镜像的上传路径为主机本地目录，则只有该主机能使用该系统镜像。
- 若系统镜像的上传路径为共享存储路径，则所有主机均可使用该系统镜像。
- 请确保系统镜像的上传路径有足够的磁盘空间，否则上传系统镜像将失败，建议上传路径选择/vms/isos。

图1-2 新建系统镜像对话框

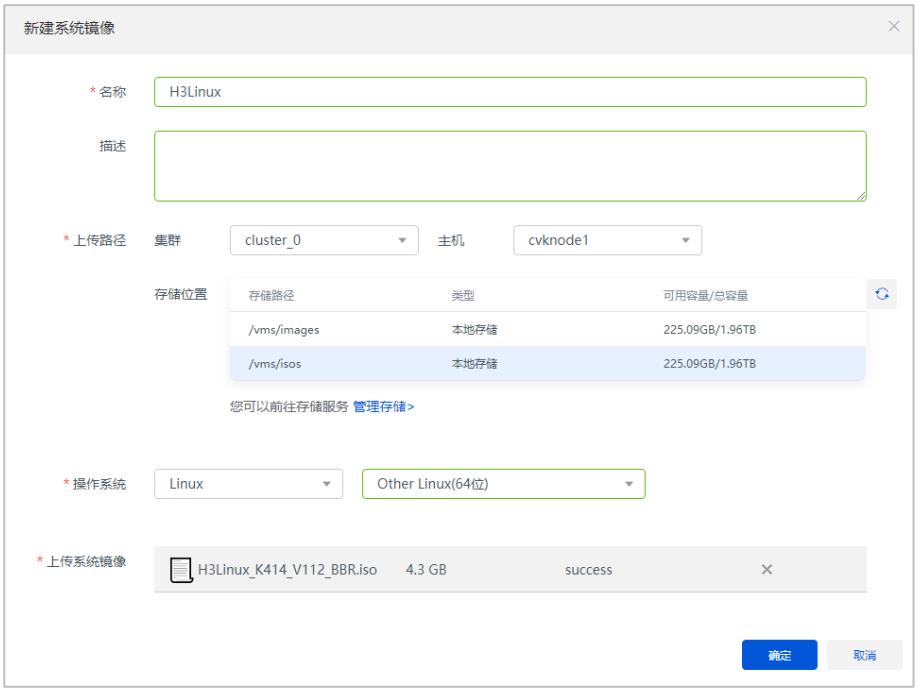


注意

上图中，“操作系统”和“版本”的配置需与实际上传的 ISO 系统镜像保持一致。

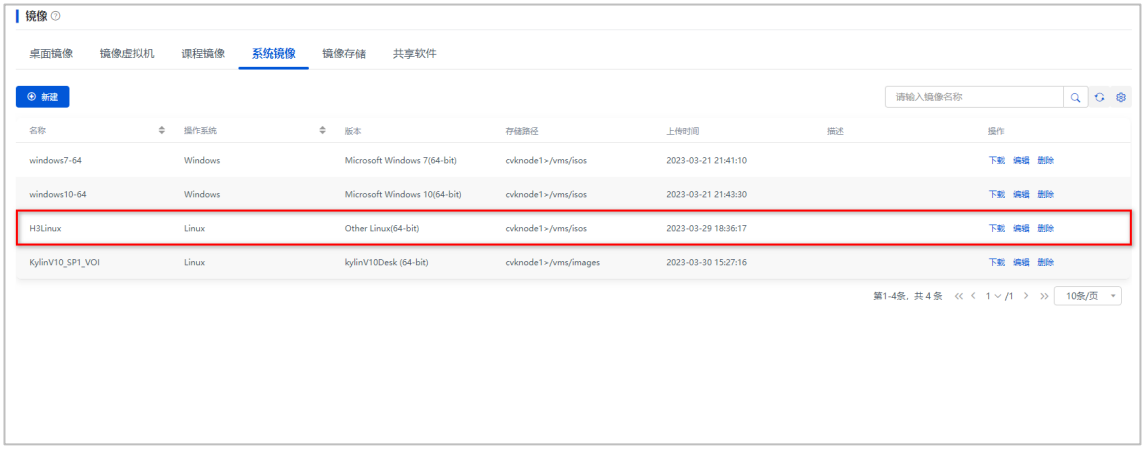
(3) 上传完成后，右上角弹出提示框“上传文件成功”，单击<确定>按钮完成新建系统镜像操作。

图1-3 新建系统镜像完成



(4) 系统镜像上传完成后，在系统镜像列表页面可以看到新建的系统镜像。

图1-4 已上传的系统镜像



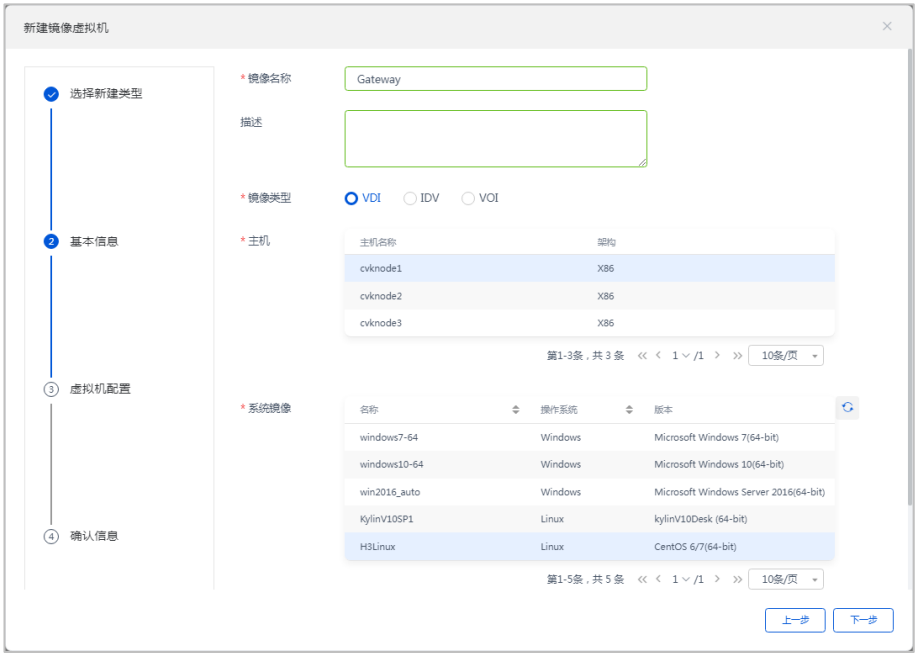
(5) 在 “镜像虚拟机”页签下，单击<新建>按钮弹出新建镜像虚拟机对话框。

图5-1 桌面镜像页面

(6) 在新建镜像虚拟机对话框中，新建类型选择“ 新建镜像虚拟机”，单击<下一步>按钮，配置镜像虚拟机基础信息，系统镜像选择上传的 H3Linux 系统镜像。

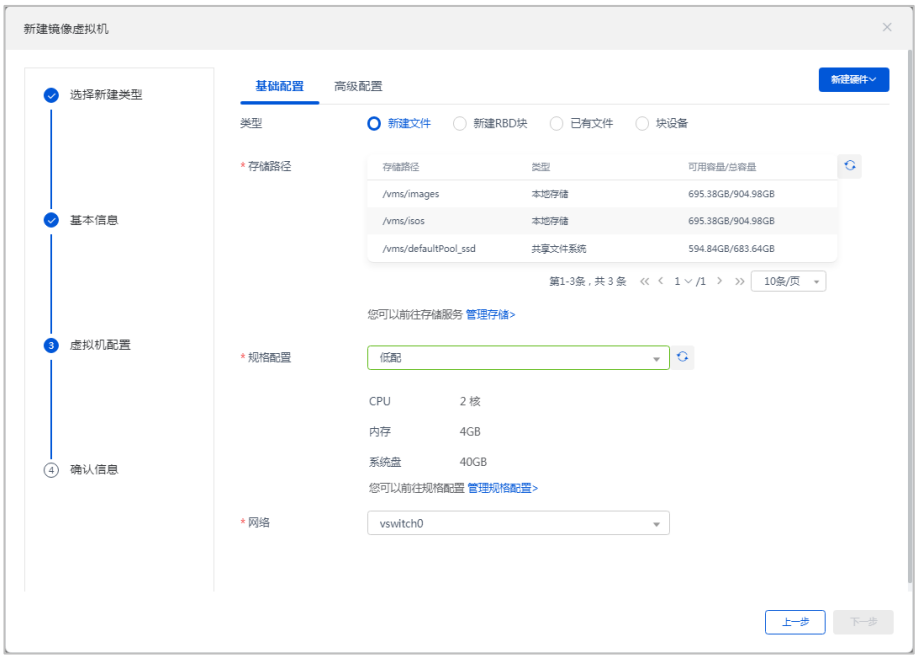
图5-2 新建镜像虚拟机

图5-3 配置基本信息



(7) 基础信息配置完成后，继续完成虚拟机配置。

图5-4 虚拟机配置



(8) 虚拟机配置完成后，确认配置信息，单击<确定>按钮完成新建镜像虚拟机。

图5-5 确认信息

表5-1 新建桌面镜像参数说明

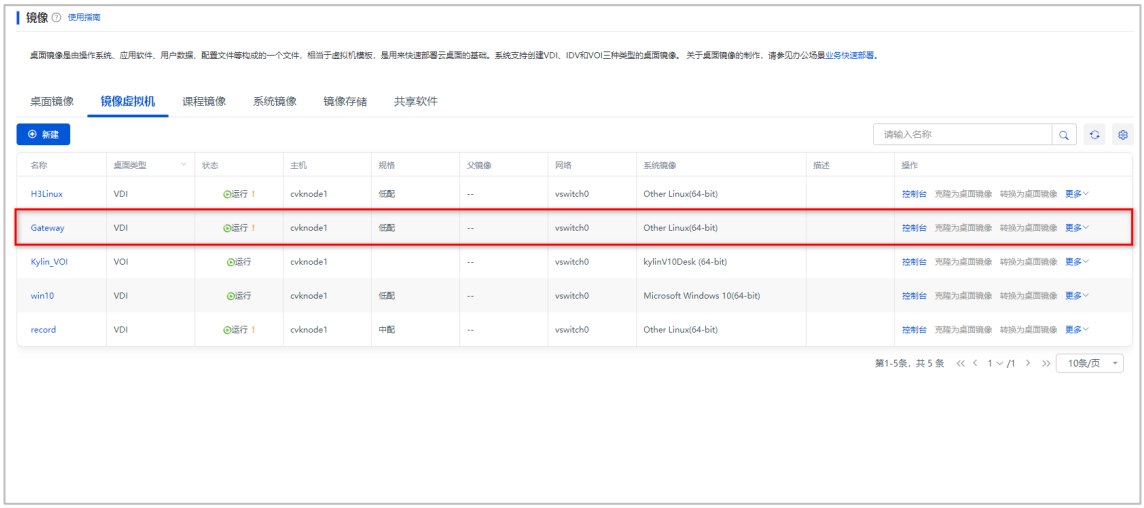
参数名称	参数说明
主机	选择镜像虚拟机所在的主机。
镜像类型	新建镜像虚拟机的类型，网关虚拟机使用VDI类型。
系统镜像	镜像虚拟机使用的操作系统的纯净ISO镜像。
类型	设置镜像虚拟机的磁盘类型，包括文件、新建RBD块和块设备，其中文件分为新建文件和已有文件。当主机上存在活动的RBD网络存储池时，默认为新建RBD块；反之，默认为新建文件。 • 新建文件：文件是构建在文件系统之上的磁盘文件，虚拟机看到的是一个实际的磁盘，实际使用的是一个虚拟磁盘文件所表示的一个磁盘。文件方式的磁盘挂接方式更便于管理。新建文件是新建一个空的存储文件作为虚拟机的磁盘。 • 新建 RBD 块：在 RBD 网络存储池中新建一个 RBD 块作为虚拟机的磁盘。 • 已有文件：选择一个已经存在且未被其他虚拟机使用的存储文件作为虚拟机的磁盘。可选项包括本地文件目录、共享文件系统、NFS 网络文件系统类型的存储池中的存储卷。 • 块设备：块设备也称作裸设备，即磁盘上没有文件系统，如 IP SAN 或 FC SAN 上的存储 LUN。块设备一般应用于性能要求较高的虚拟化环境，如数据库、高性能 I/O 计算等。该选项用于选择一个已经存在且未被其他虚拟机使用的存储卷作为虚拟机的磁盘。可选项包括 RBD 网络存储、iSCSI 网络存储、FC 网络存储和 LVM 逻辑存储卷类型的存储池中的存储卷。
存储路径	作为镜像虚拟机文件的存储路径，不作为桌面镜像的最后存储路径。其中，/vms/images和/vms/isos为本地文件目录，建议选择其他路径防止本地目录空间不足。
规格配置	镜像虚拟机适配的VDI终端的配置，可选系统默认的VDI终端或在规格配置中自定义的VDI终端配置。
网络	选择镜像虚拟机网络通信使用的虚拟交换机。
高级配置	可进行CPU工作模式、文件名、预分配、簇大小、总线类型、缓存方式、显卡型号和大页配置相关配置。

说明

新建的镜像虚拟机的本质是一台未安装操作系统和必要驱动的虚拟机，因此部署安全网关软件的虚拟机时，需进行新建镜像虚拟机操作，并在镜像虚拟机中安装网关软件，最终将网关镜像虚拟机发布为网关桌面镜像。

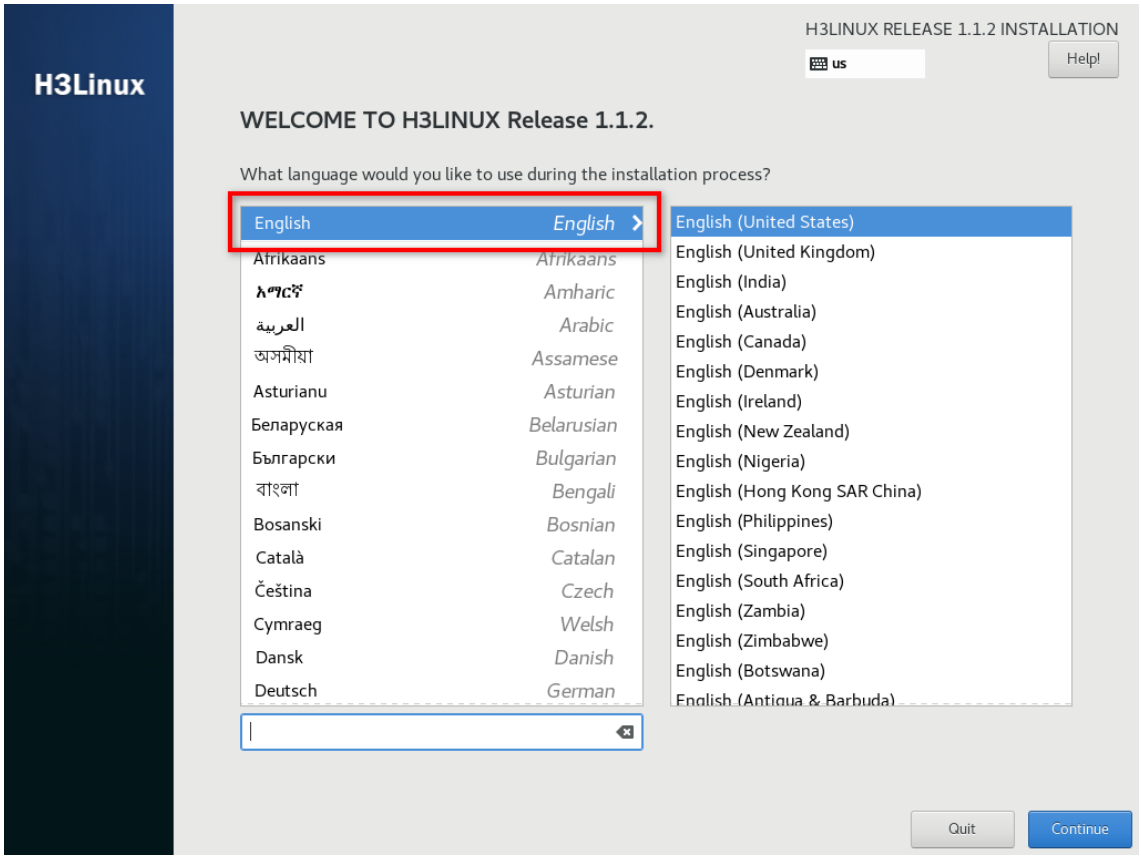
(9) 新建的未完成制作的镜像虚拟机将会显示在镜像虚拟机列表中，单击新建的镜像虚拟机操作列的<控制台>按钮，进入镜像虚拟机的控制台。

图5-6 新建的镜像虚拟机



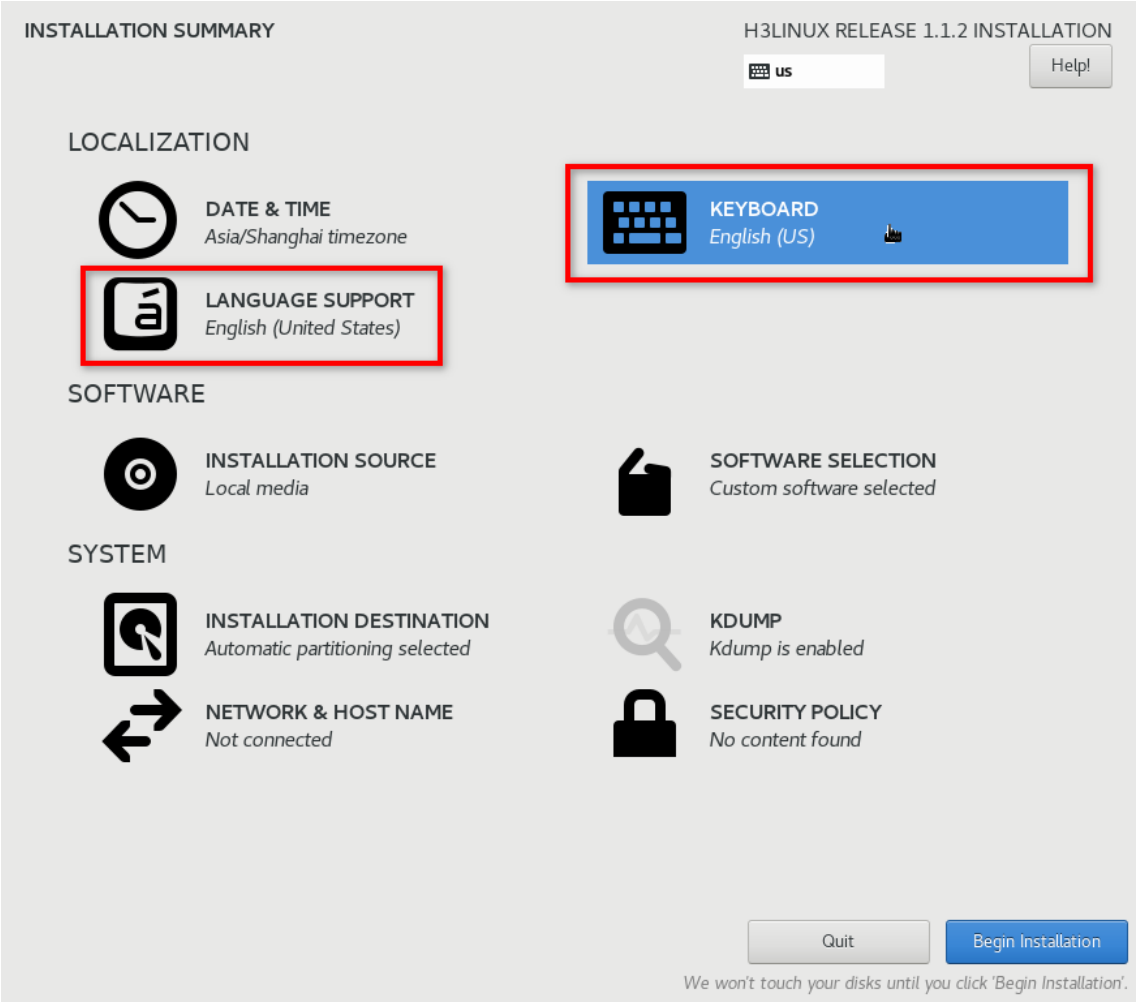
(10) 在虚拟机控制台中安装 H3Linux 操作系统，在安装开始界面语言请选择 English，单击<Continue>按钮进入“INSTALLATION SUMMARY”界面。

图5-7 安装开始界面



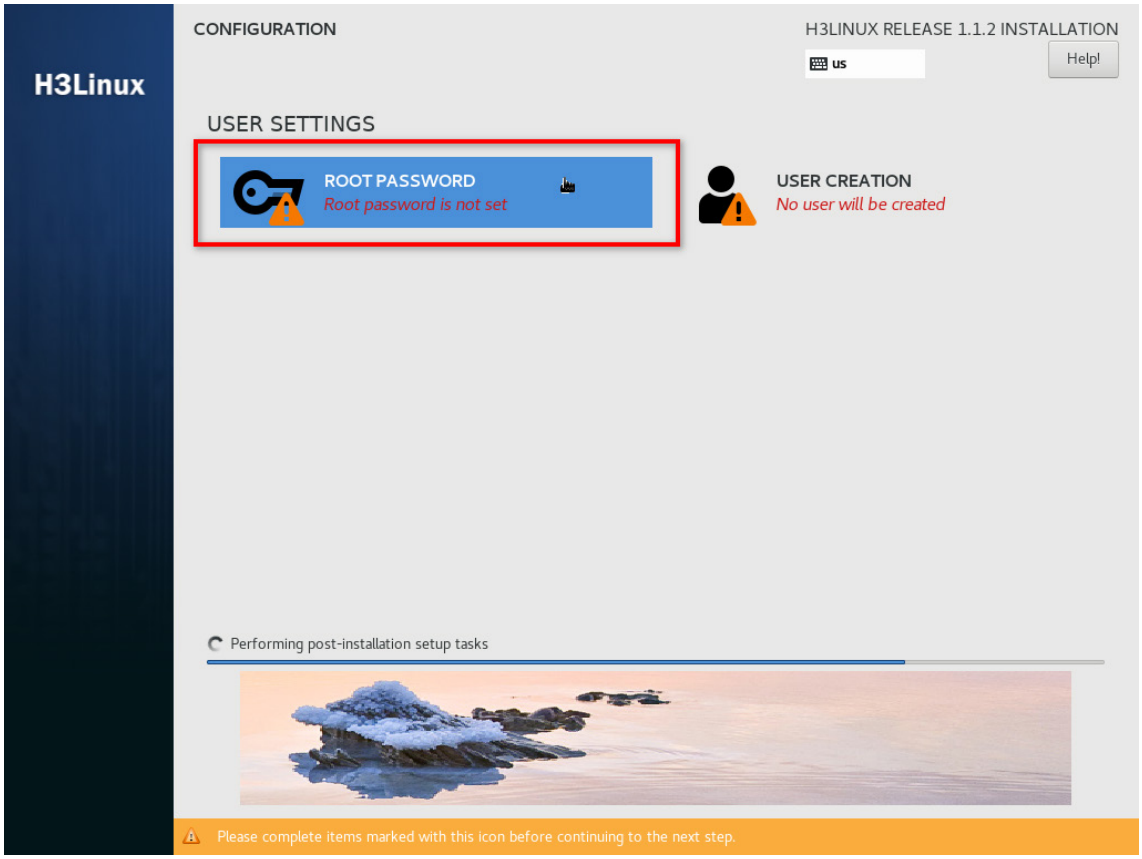
(11) 在“INSTALLATION SUMMARY”界面中确保“KEYBOARD”与“LANGUAGE SUPPORT”项均设置为“English”，其余配置项会自动完成配置，单击<Begin Installation>按钮开始安装。

图5-8 INSTALLATION SUMMARY 界面



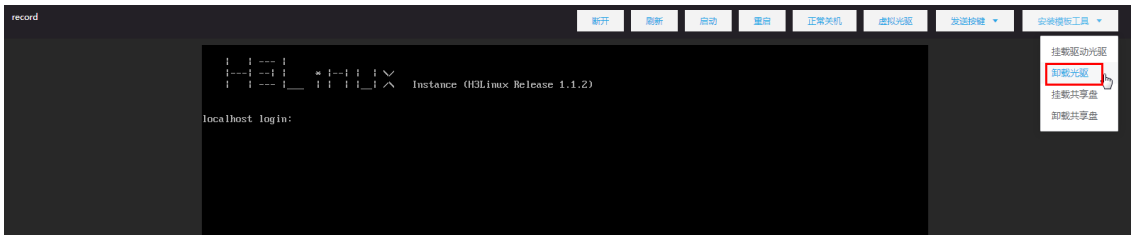
(12) 单击安装界面上方的“ROOT PASSWORD”项，进入 ROOT PASSWORD 页面，设置 ROOT 密码，完成后等待安装完成。

图5-9 设置 ROOT 密码



(13) 安装完成后单击<安装模板工具>按钮，在下拉菜单中选择[卸载光驱]菜单项，卸载光驱。

图5-10 卸载光驱



(14) 在管理平台中单击左侧导航树[数据中心/虚拟化/]菜单项，进入虚拟化页面，单击主机页面下的“虚拟机”页签，找到对应的虚拟机，单击操作列的<修改>按钮进入修改虚拟机页面。在“光驱”页签下单击<连接>按钮选择 castools.iso 文件，为虚拟机挂载 castools.iso。

图5-11 修改虚拟机

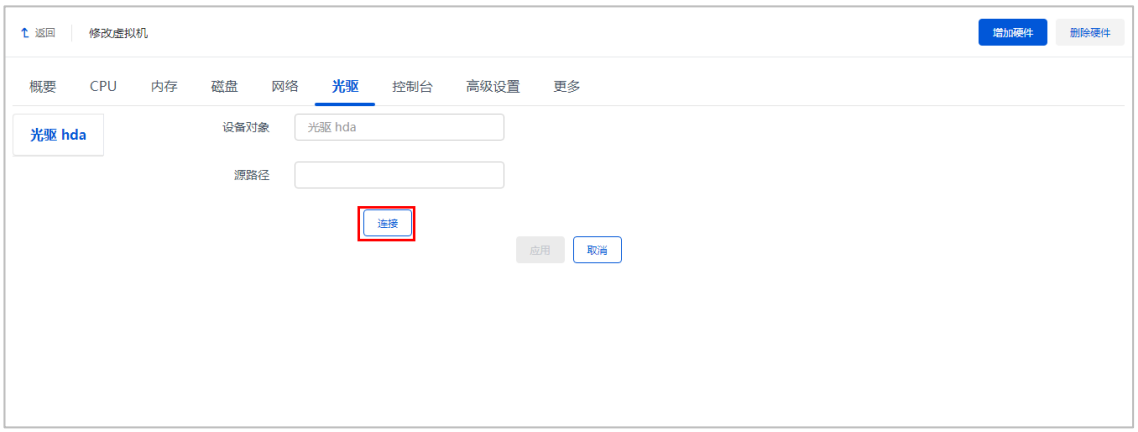


图5-12 选择文件

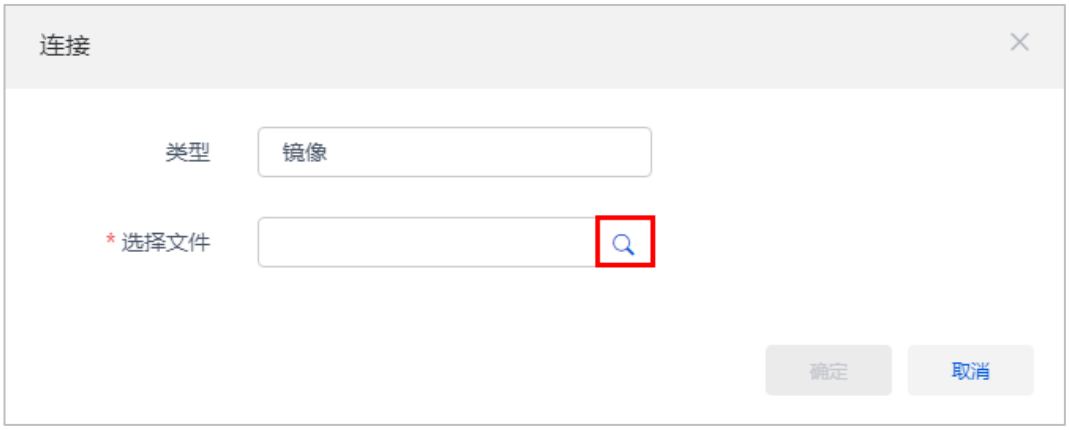


图5-13 选择 castools.iso 文件

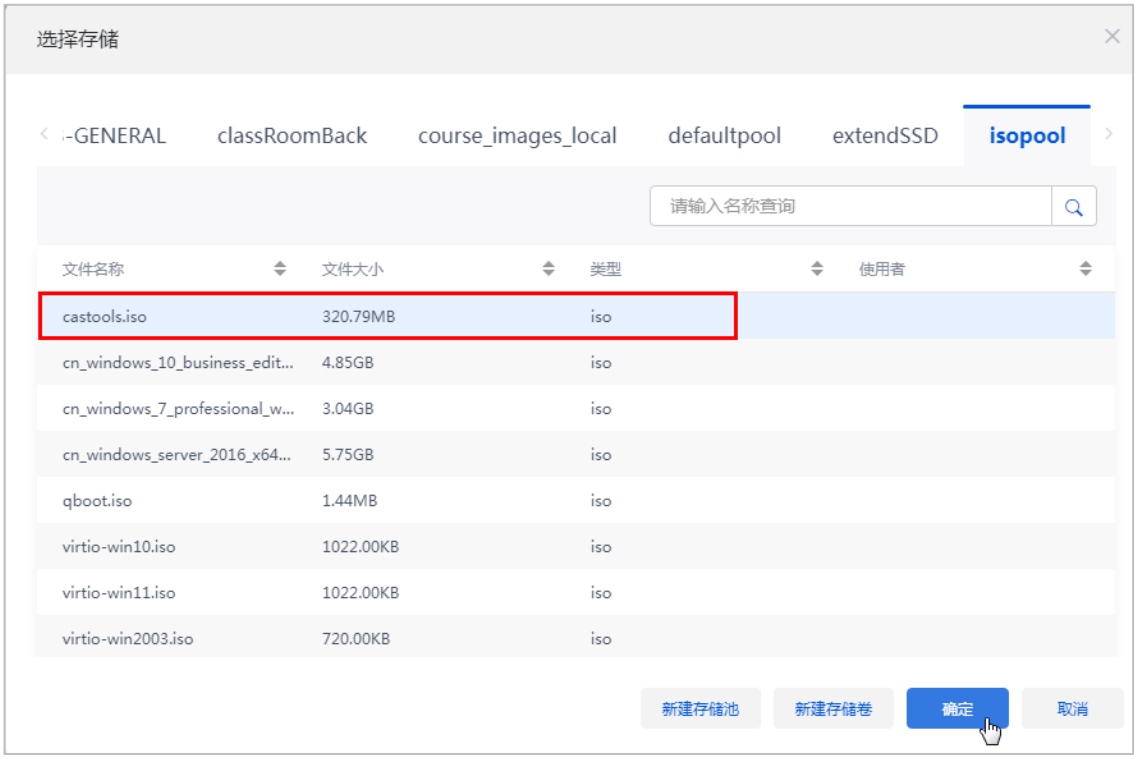


图5-14 挂载 catstools.ios 成功

(15) 挂载完成后，登录操作系统，执行如下命令安装 CAStools。

a. 查看光驱路径。

```
[root@localhost ~]# ll /dev/ | grep -i cdrom
```

图5-15 查看光驱路径

```
[root@localhost ~]# ll /dev/ | grep -i cdrom
lrwxrwxrwx. 1 root root           3 Jul 26 16:10 cdrom -> sr0
crw-rw----. 1 root cdrom    21,   0 Jul 26 16:06 sg0
brw-rw----. 1 root cdrom    11,   0 Jul 26 16:10 sr0
[root@localhost ~]# _
```

b. 挂载光驱到指定路径。

```
[root@localhost ~]# mount /dev/sr0 /media/
```

图5-16 挂载光驱到指定路径

```
[root@localhost ~]# mount /dev/sr0 /media/
mount: /dev/sr0 is write-protected, mounting read-only
[root@localhost ~]#
```

c. 进入 CAStools 安装脚本路径，不同版本 Workspace 的 CAStools 安装脚本路径可能不同，进入到/media/linux 目录中，在此目录中找到 CAS_tools_install.sh，并执行该安装脚本。

```
./CAS_tools_install.sh
```

图5-17 安装 castools

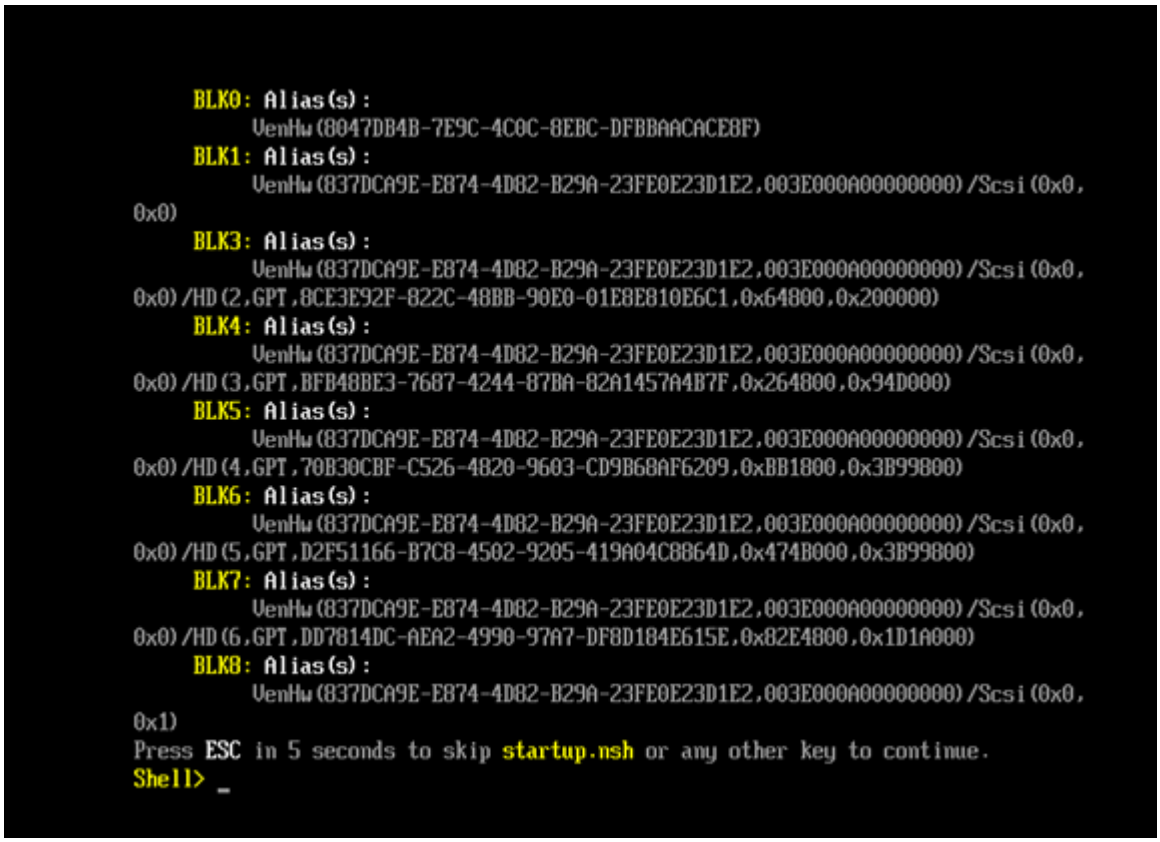
```
[root@localhost media]# ls
CAS_tools_install.sh                    qemu-ga-10.1.5.0-1.el7.i686.rpm      qemu-ga-7.1.1.99-1.x86_64.rpm
ds_filefilter                           qemu-ga-10.1.5.0-1-i686.pkg.tar.gz   qianxin
old-release                             qemu-ga-10.1.5.0-1-x86_64.pkg.tar.gz util_ds_filefilter_arm_manage.sh
qemu-ga-10.1.5.0-0ubuntu13_amd64.deb    qemu-ga-10.1.5.0-amd64.txz           util_ds_filefilter_patch_manage.sh
qemu-ga-10.1.5.0-0ubuntu13_i386.deb     qemu-ga-10.1.5.0-i386.txz
qemu-ga-10.1.5.0-1.el7.centos.x86_64.rpm qemu-ga-7.1.1.99-1.i386.rpm
[root@localhost media]# ./CAS_tools_install.sh
Preparing...                          ################################# [100%]
Updating / installing...
   1:qemu-ga-10.1.5.0-1.el7.centos    ################################# [100%]
non-SUSE
Created symlink from /etc/systemd/system/multi-user.target.wants/qemu-ga.service to /usr/lib/systemd/system/qemu-ga.service.
[root@localhost media]# _
```

(16) 将/boot/efi/EFI/centos 路径下的 grubaa64.efi 文件拷贝并重命名覆盖/boot/efi/EFI/BOOT 下的 BOOTAA64.efi，该操作是为了解决重启虚拟机后停留在图 5-18 界面无法进入系统的问题。以 root 用户执行如下命令：

```
[root@localhost ~]# mount -o rw,remount /boot/efi
[root@localhost ~]# cp /boot/efi/EFI/centos/grubaa64.efi /boot/efi/EFI/BOOT/BOOTAA64.EFI
```

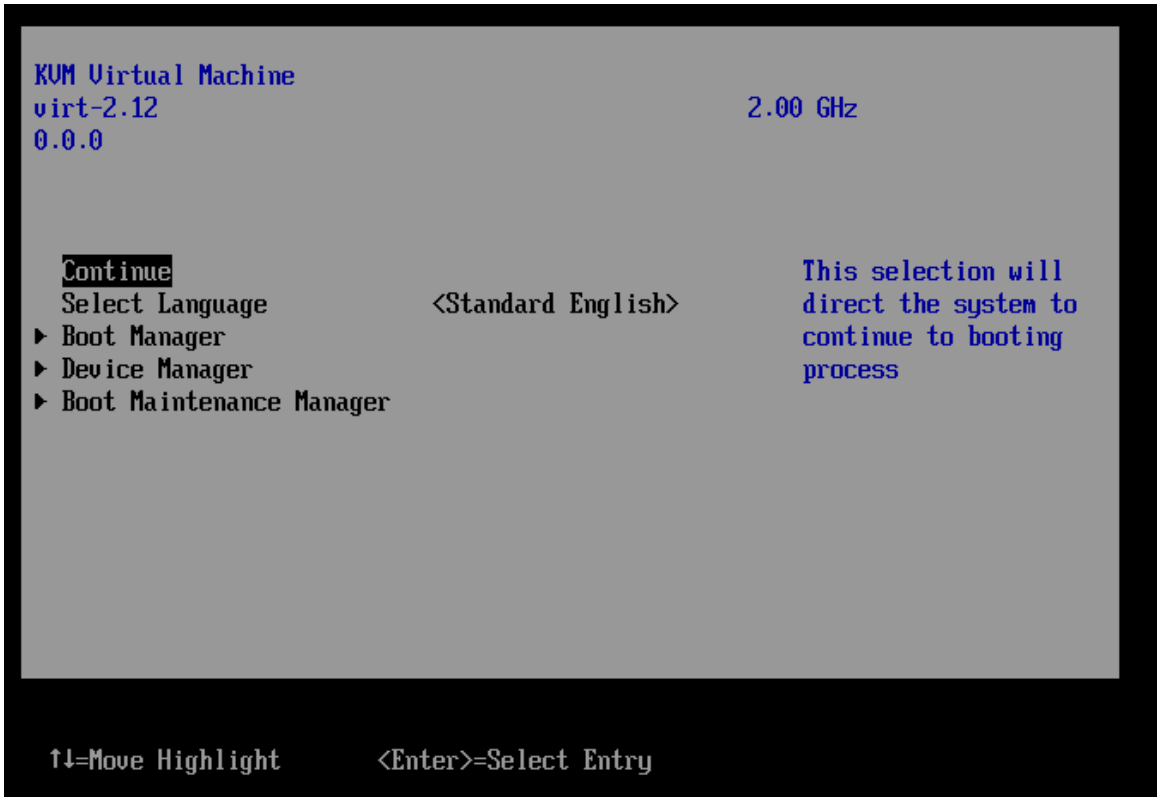
(17) 重启虚拟机验证是否修改成功。如果能正常启动进入系统，则表示修改成功。如果启动过程中停留在如下界面，则继续下一步。

图5-18 重启后停留界面



(18) 在上图停留界面中，输入 exit 进入虚拟机 BIOS 界面，或在虚拟机开机过程中按下 ESC 键进入 BIOS 界面。

图5-19 BIOS 界面



(19) 依次选择 Boot Maintenance Manager→Boot From File→No Volume Label,xxxx[第一项]—>EFI→centos→grubaa64.efi 启动。

(20) 虚拟机将正常进入系统，继续执行步骤(16)替换文件，完成后重启虚拟机，如果能正常启动进入系统，则表示修改成功。

说明

请严格按照步骤(16)-(20)进行操作，若虚拟机重启后仍然停留在图 5-18 的界面，请联系技术支持工程师获取帮助。

5.2 安装网关

说明

- 网关安装完成后，默认只有 8860 端口放通，其余端口被关闭。
- 登录虚拟机后台可采用以下任意一种方式：1、通过虚拟机控制台进入后台；2、通过 SSH 登录，登录前需开启指定端口，详细步骤可参考 7.5 章节；3、开启所有端口，详细步骤可参考 7.4 章节。

(1) 登录虚拟机后台，并上传网关安装包（安装包名称为UniCloud_Workspace_Gateway_Solution-*version*.tar.gz）到虚拟机后台。

(2) 执行如下命令解压安装包并切换至解压后的目录。此处，*version* 表示版本号。

```
[root@localhost ~]# tar -xvf UniCloud_Workspace_Gateway_Solution-version.tar.gz
[root@localhost ~]# cd UniCloud_Workspace_Gateway_Solution-version
```

(3) 执行安装脚本安装网关。

```
[root@localhost ~]# ./install.sh
```

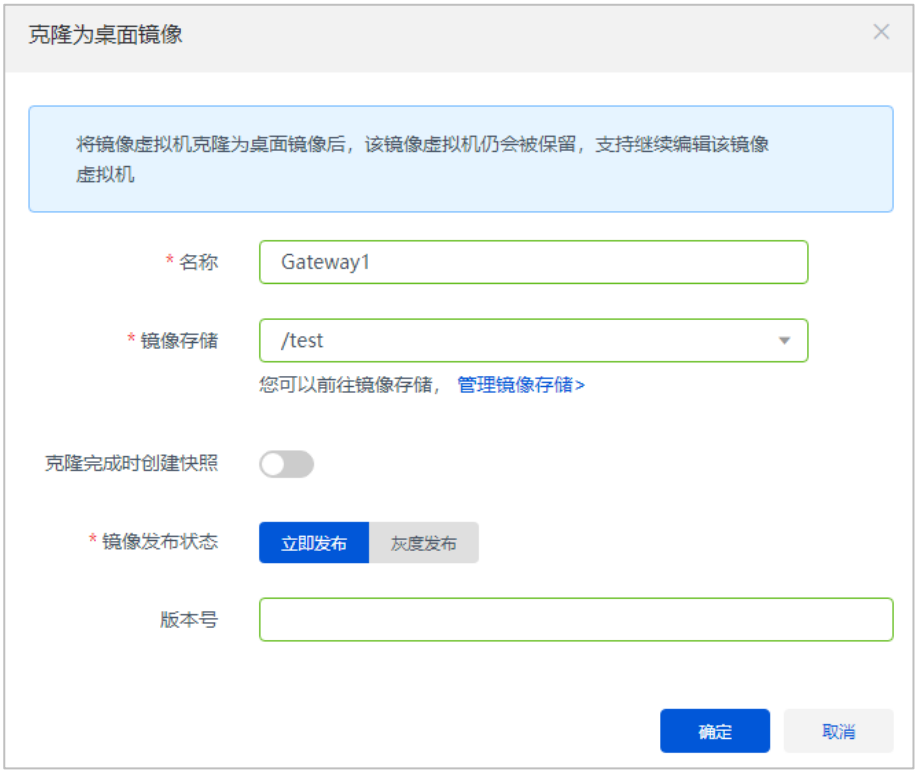
5.3 部署网关虚拟机

(1) 在管理平台中单击左侧导航树[镜像]菜单项，进入镜像页面，单击“镜像虚拟机”页签，将网关镜像虚拟机正常关机后，发布为网关桌面镜像，本文以转换为桌面镜像为例，单击网关镜像虚拟机操作列的<转换为桌面镜像>按钮将网关镜像虚拟机转换为网关桌面镜像，弹出“转换为桌面镜像”对话框。

图5-20 桌面镜像页面

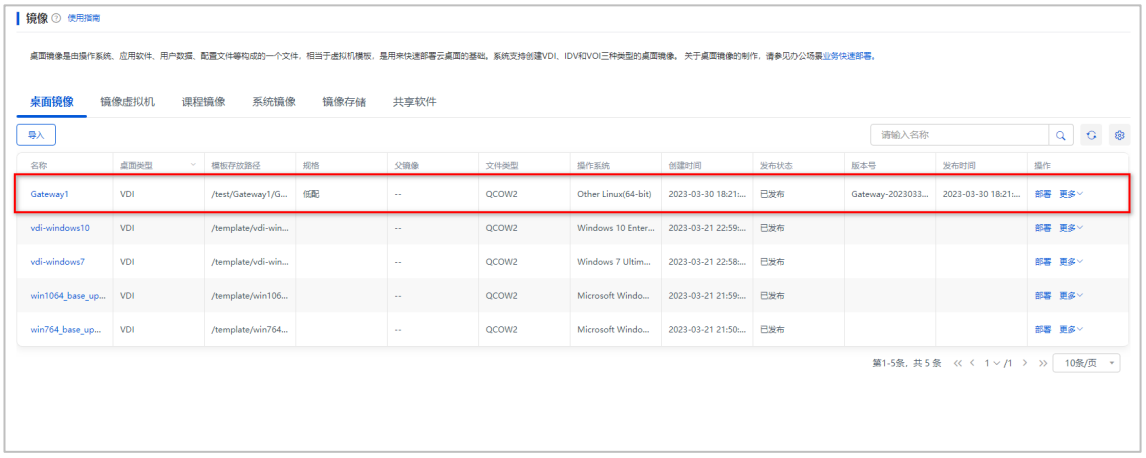
(2) 在“转换为桌面镜像”对话框中选择镜像存储路径，单击<确定>按钮将网关镜像虚拟机转化为桌面镜像。

图5-21 完成制作对话框



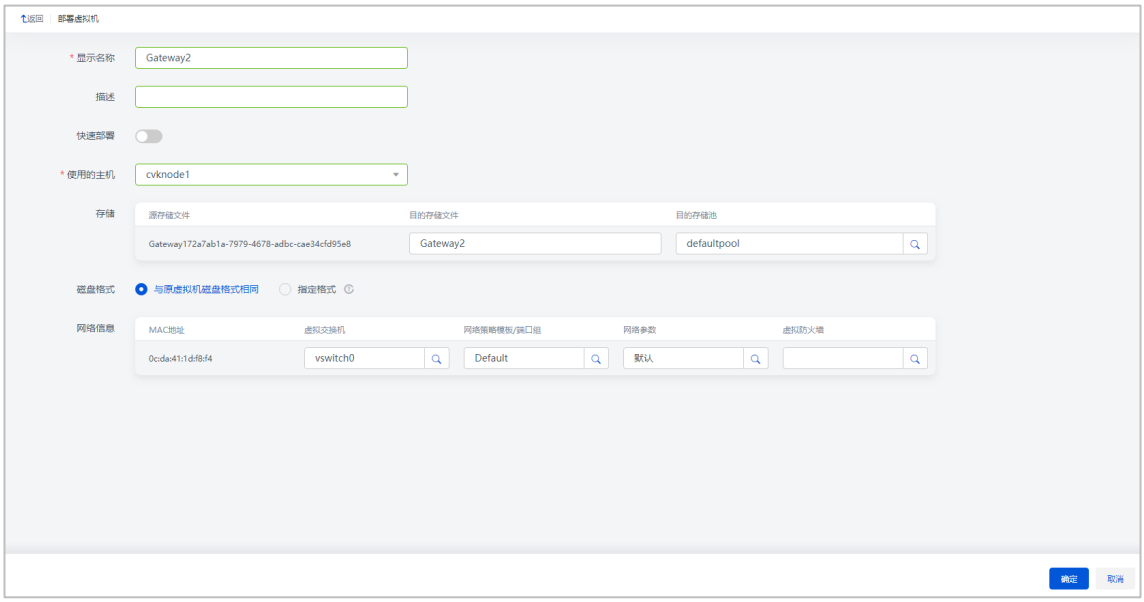
(3) 转换为桌面镜像完成之后，在桌面镜像页面的“桌面镜像”页签下，单击网关桌面镜像操作列的<部署>按钮，进入部署虚拟机页面，根据使用需求，在指定主机上部署相应的网关虚拟机。

图5-22 部署网关虚拟机



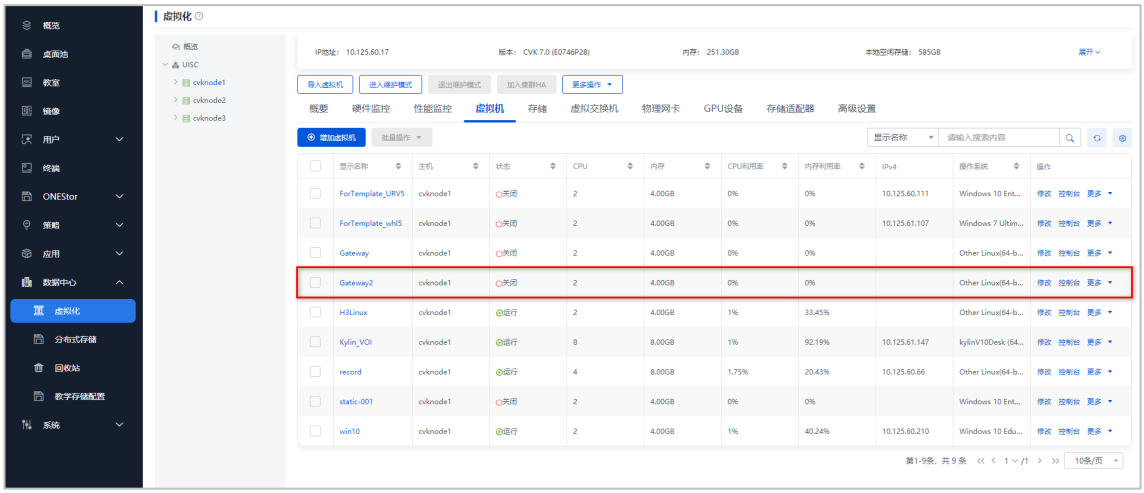
(4) 在部署虚拟机页面，根据使用需求，在指定主机上部署相应的网关虚拟机。

图5-23 部署网关虚拟机



(5) 部署后的网关虚拟机可以在[数据中心/虚拟化]页面中的对应主机的“虚拟机”页签下看到。

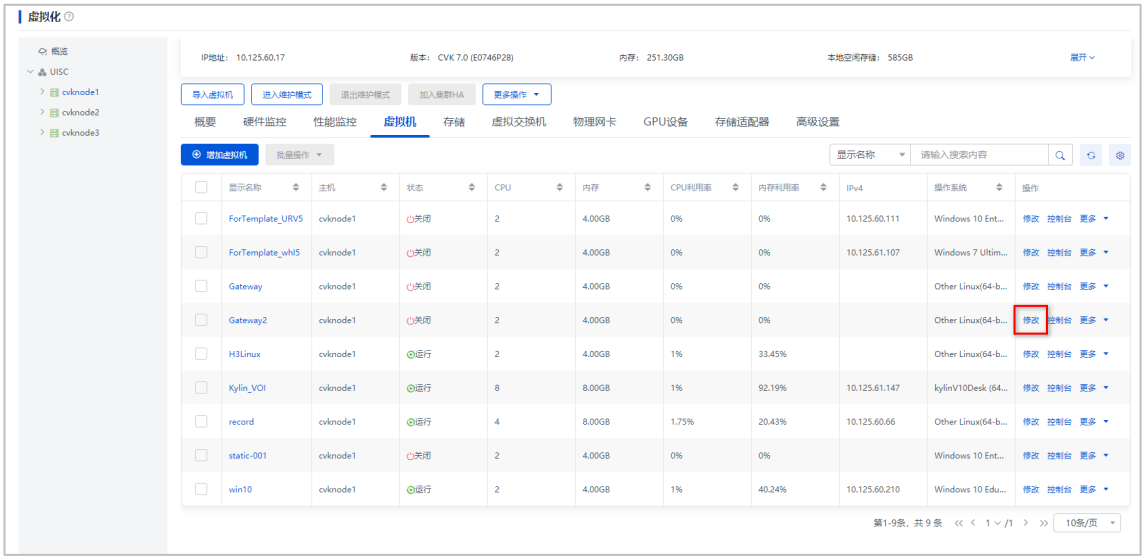
图5-24 网关虚拟机



5.4 添加网卡

(1) 在[数据中心/虚拟化]页面中单击虚拟机列表中的网关虚拟机操作列下的<修改>按钮，进入修改虚拟机页面。

图5-25 桌面镜像页面



(2) 单击修改虚拟机页面右上方的<增加硬件>按钮，弹出“增加硬件”对话框。

图5-26 修改虚拟机

(3) 在“增加硬件”对话框中，硬件类型选择“网络”，配置网卡相关信息，完成后单击<确定>按钮完成新建网卡。

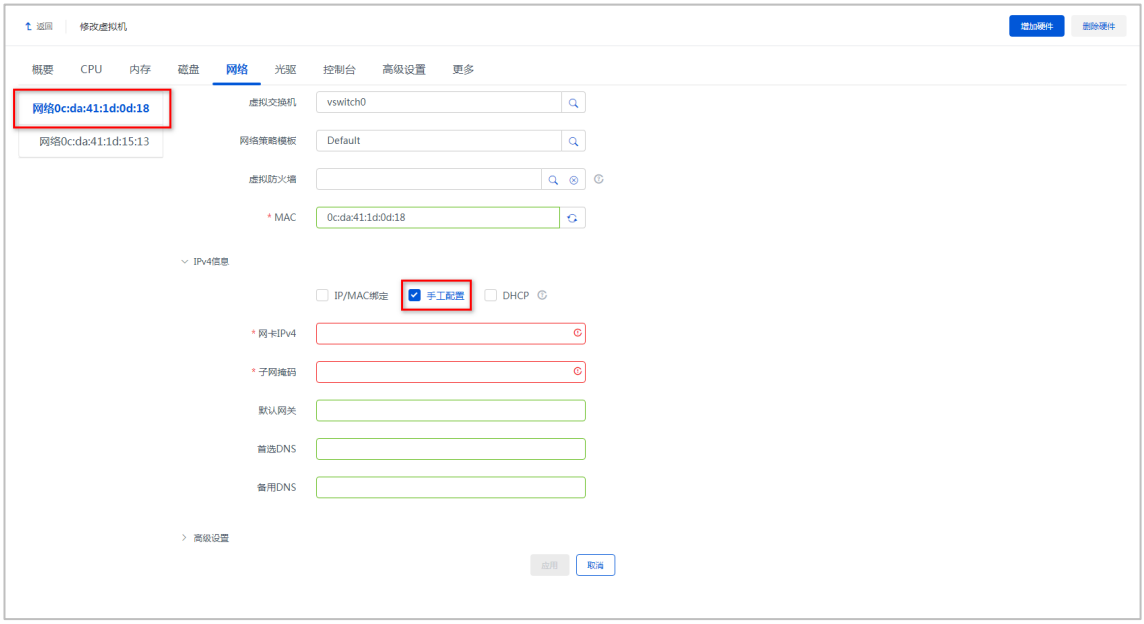
图5-27 新建网卡

说明

此时的桌面镜像一共有两张网卡，一张用于对外提供访问，一张用于对内访问 Controller 和 CVK。

(4) 增加网卡完成后，在修改虚拟机页面中的网络页签下为两张网卡配置 IP，在 IPv4 信息项中选择“手工配置”，为虚拟机配置网卡 IP 地址，也可通过命令行形式配置网卡 IP 地址，具体操作步骤请参见配置网关网卡 IP。

图5-28 配置网卡



5.5 配置网关代理地址

说明

- Controller IP 一般默认为管理平台 IP，管理平台如果有业务网和管理网，则根据实际组网情况选择。
- 登录虚拟机后台可采用以下任意一种方式：1、通过虚拟机控制台进入后台；2、通过 SSH 登录，登录前需开启指定端口，详细步骤可参考 7.5 章节；3、开启所有端口，详细步骤可参考 7.4 章节。

---

(1) 登录虚拟机后台，根据实际网关代理的 Controller 地址，执行 `gateway proxy -c controller_ip` 命令为网关配置代理的 Controller IP（如下以 10.125.11.112 为例）。

```
[root@localhost ~]# gateway proxy -c 10.125.11.112
Do you want to change the Controller IP for gateway? [Y/n]: y
The controller IP set successfully
```

(2) 执行命令 `gateway config proxy` 确认 Controller IP 是否配置正确。

```
[root@localhost ~]# gateway config proxy
controller:10.125.11.112
```

(3) Controller 地址配置成功后，便可以使用客户端登录和访问云桌面。

5.6 连通性检测

网关虚拟机部署完成后，禁止回应 icmp 报文，ping 命令无法 ping 通网关，因此需在客户端使用 tcping.exe 工具检测客户端与网关的连通性。tcp.exe 为网上开源工具，请根据需求从官网下载获取 32 位或 64 位工具。使用方法如下：

(1) 将下载的 tcping.exe 工具放在 C:\WINDOWS\system32 目录下。若下载的工具是 64 位，请将名称改为 tcping.exe。

(2) 在 Windows 命令提示符里可以直接使用该命令，输入 tcping 若出现帮助文档说明工具安装成功。

(3) 使用命令“tcping *网关 IP 网关端口号*”检测与网关虚拟机的连通性。

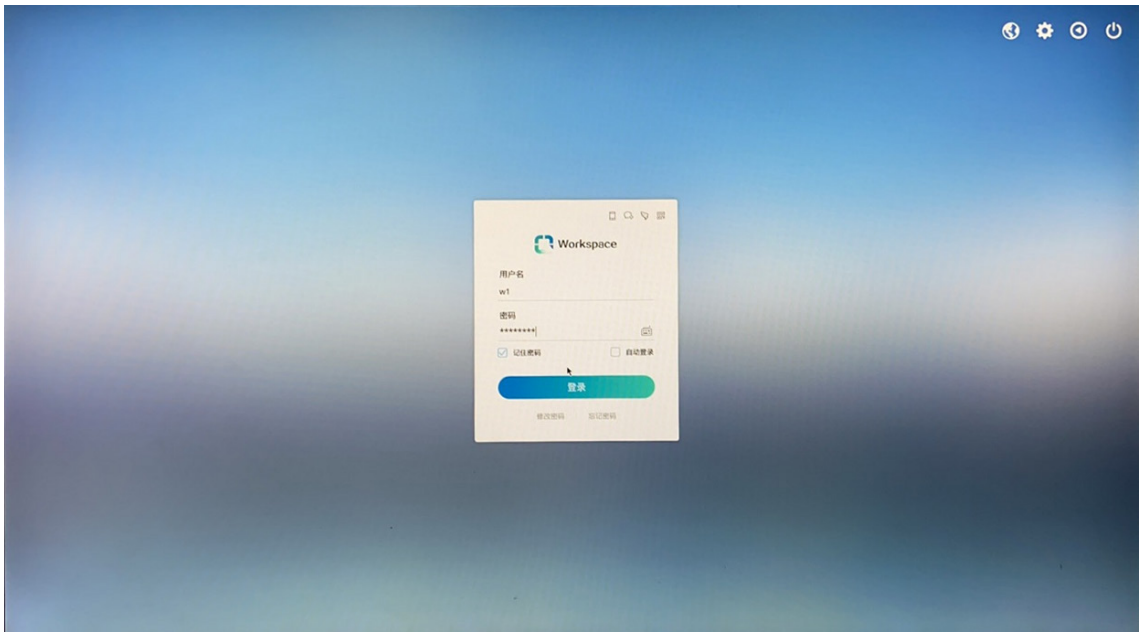
5.7 客户端登录网关

如使用 IDV 和 VOI 客户端登录网关，需开启代理，配置方法请参考启用网关支持 IDV/VOI 章节。此处以 VDI 客户端登录网关为例，登录过程如下：

(1) 用户在终端上启动 Workspace App 客户端，进入登录界面，单击图 5-29右上角⚙图标或单击图 5-30右上角图标，选择[服务器配置]菜单项。

图5-29 客户端登录界面（客户端窗口模式）

图5-30 客户端登录界面（客户端全屏模式）



(2) 在“服务器配置”对话窗中单击<添加服务器>按钮，弹出“添加服务器信息”对话框。在对话框中，服务器地址填写网关服务器地址，端口填写网关服务器对外的端口，单击<确定>按钮完成添加。

说明

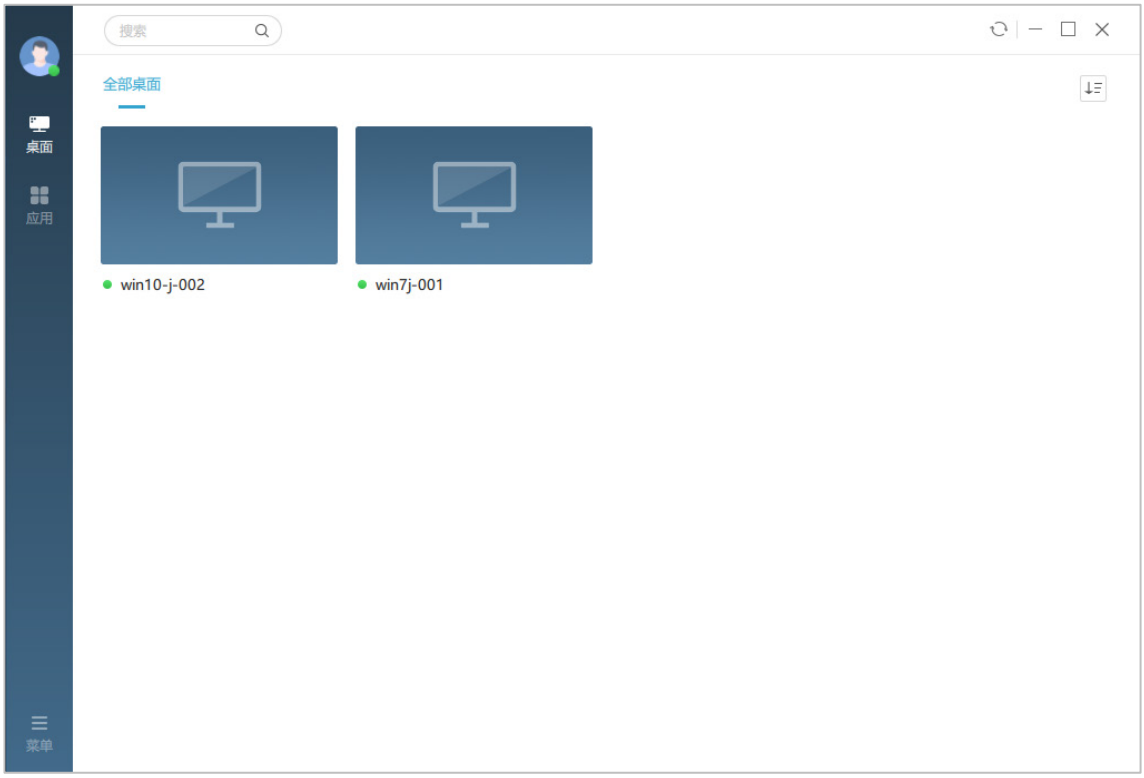
- 若网关公网 IP 和端口经过映射（如映射到企业内部出方向防火墙），请输入映射后的 IP 地址和端口号。映射后的网络信息，请联系网络管理员获取。
- 若网关公网 IP 和端口未经过映射，则保持默认端口号 8860。
- 服务器地址也支持输入域名与端口号。

图5-31 服务器配置

图5-32 添加服务器信息

(3) 添加网关服务器信息完成后，在“服务器配置”对话窗中勾选添加的网关服务器，单击<关闭>按钮，回到登录界面。在登录界面输入用户名与密码，进入桌面列表界面，双击桌面图标，连接进入到对应的云桌面中。

图5-33 桌面列表界面



6 高级配置

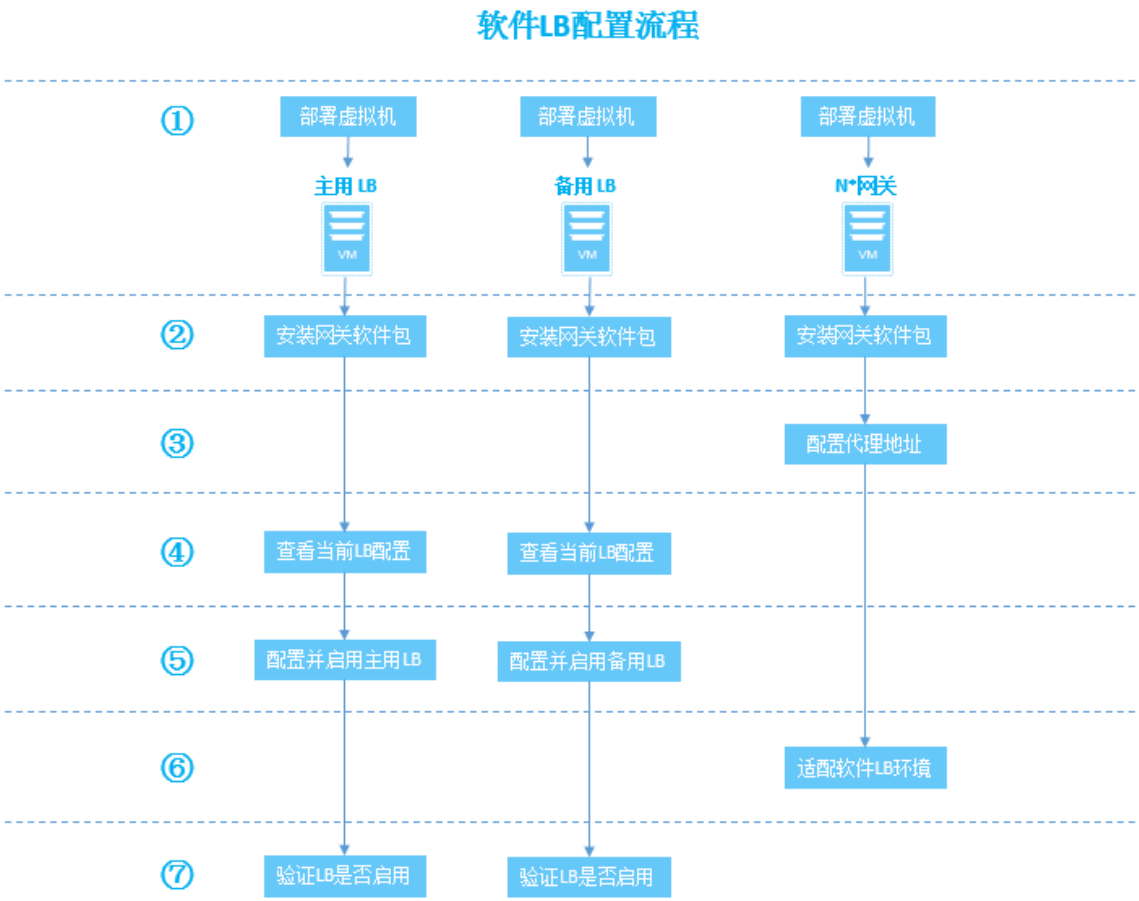
6.1 软件LB

负载均衡方案支持启用软件 LB 功能，软件负载均衡采用 LVS DR 模式提高转发性能。负载均衡方案的部署要求和组网图请参考负载均衡部署。

6.1.1 配置流程

软件 LB 配置流程如下图所示。

图6-1 软件 LB 配置流程



6.1.2 命令行参数说明

功能配置命令行帮助如下所示，请参考命令行帮助进行 LB 配置：

```
[root@localhost ~]# gateway lb --help
Usage: gateway lb [OPTIONS] ACTION
  LB service control, action: enable, disable, status
Options:
  -v, --lb-vip VIP              Set virtual IP for LB.
  -m, --lb-mask NETMASK         Set virtual IP network mask for LB.
  -t, --lb-port PORT            Set Port for LB.
  -o, --lb-role ROLE            Set default role for this LB.
  -a, --lb-master-ip MASTER_IP  Set master IP for LB.
  -b, --lb-backup-ip BACKUP_IP  Set backup IP for LB.
  -e, --lb-expose-iface IFACE   Set expose interface for LB.
  -i, --lb-inner-iface IFACE    Set inner interface for LB.
  -d, --lb-vroute-dst IP        Set virtual route destination for LB.
  -s, --lb-vroute-mask NETMASK  Set virtual route destination mask for LB.
  -n, --lb-vroute-nexthop IP    Set virtual route nexthop for LB.
  -r, --real-servers IPs        Set real servers for LB to proxy.
```

```
-p, --real-server-port PORT   Set real servers port for LB to proxy.
-u, --lb-virtual-router-id ID   Set virtual route id. value range from 1 to 255
--help                        Show this message and exit.
```

表6-1 参数说明

参数	说明
-v或--lb-vip	高可用虚拟IP地址，对外提供服务的IP
-m或--lb-mask	虚拟IP地址的掩码
-t或—lb-port	本LB设备上提供VDP协议服务的端口
-r或--lb-role	本LB设备在HA中的默认角色，取值为master或backup
-a或--lb-master-ip	默认主用LB的实IP地址，对应主用LB上的lb-expose-iface参数配置的网卡的IP地址
-b或--lb-backup-ip	默认备用LB的实IP地址，对应备用LB上的lb-expose-iface参数配置的网卡的IP地址
-e或--lb-expose-iface	本LB上对外暴露的IP所在网卡的名称，用于客户端访问LB
-i或--lb-inner-iface	本LB上对内访问的IP所在网卡的名称，用于管理平台纳管LB设备用，并且会交互HA的协议报文，不负责转发业务流量
-d或--lb-vroute-dst	虚拟路由的目的网段地址，如果要设置默认路由，则输入0.0.0.0
-s或--lb-vroute-mask	虚拟路由的目的网段的掩码，如果要设置默认路由，则输入0.0.0.0
-n或--lb-vroute-nexthop	虚拟路由的下一跳地址
-r或--real-servers	LB设备代理的网关地址列表，多个IP地址用逗号分隔，如192.168.3.5,192.168.3.6,192.168.3.7
-p或--real-server-port	LB设备代理的网关VDP端口
-u或--lb-virtual-router-id	设置虚拟路由器的ID，取值范围为1-255

6.1.3 配置场景

目前 LB 仅支持主备模式，配置命令需要分别在主备 LB 上配置。LB 设备使用的虚拟 IP 地址可以是私网地址或公网地址。无论私网地址或公网地址，推荐将虚拟 IP 地址配置在对外网卡的子接口上，同时对外网卡的 IP 地址和网关二层互通。虚拟 IP 地址可以跟实 IP 地址同一网段，也可以不同网段，若不同网段，则需要在交换机等网络设备上给虚拟 IP 地址配置好路由。下面将介绍虚拟 IP 是私网地址和公网地址两种场景的部署步骤。

1. 虚拟 IP 地址是私网 IP 地址场景

该场景下，虚拟路由为可选字段，未配置时，虚拟 IP 地址的路由使用的是实 IP 地址相关的路由配置，如实 IP 地址配置有网关地址，则虚拟 IP 也可以通过该网关访问到外网。若实 IP 地址上没有配置网关地址，也没有配置相关路由，则需要配置虚拟路由，使得虚拟 IP 地址可以访问外网。

以下表网络规划为例：

图6-2 LB 网络规划举例-虚拟 IP 地址是私网 IP

LB 类型	对外网卡/IP	对外网关	对内网卡	说明
主用LB	eth0/10.99.207.10	10.99.207.1	eth1	• 虚拟 IP 地址：10.99.207.2

LB 类型	对外网卡/IP	对外网关	对内网卡	说明
备用LB	eth0/10.99.207.11	10.99.207.1	eth1	• 两个 LB 的对内网卡 eth1 上配置有同网段的 IP 地址，对内网卡和对外网卡也可以是同一个网卡 • LB 设备代理的安全网关对外网卡地址列表为 10.99.207.20，10.99.207.21，10.99.207.22，安全网关地址要求和虚拟 IP 和实 IP 都属于同一网段

配置步骤如下：

(1) 完成部署方案中的 LB 虚拟机与网关虚拟机的安装部署。

说明

启用软件 LB 的 LB 虚拟机的部署方法与网关虚拟机相同，但是 LB 虚拟机安装无需进行“配置网关代理地址”步骤。

(2) 在 LB 虚拟机上执行 `gateway config lb` 命令查看当前 LB 配置信息，出厂有默认配置，默认 LB 模式处于关闭状态。

```
[root@localhost ~]# gateway config lb
lb:disable
lb_gateway:false
```

说明

- lb 参数显示 enable 表示当前设备是一台 LB 设备，disable 表示当前设备未启用 LB 模式。
- lb_gateway 参数显示 false 表示当前设备不是配合软件 LB 使用的网关设备，显示 true 则表示当前设备是配合环境中的软件 LB 使用的网关设备。
- 需要注意的是，硬件 LB 设备跟此处的两个参数无关。

(3) 在主用 LB 上执行如下命令。

```
gateway lb -v 10.99.207.2 -a 10.99.207.10 -b 10.99.207.11 -e eth0 -i eth1 -r
10.99.207.20,10.99.207.21,10.99.207.22 enable。
```

(4) 在备用 LB 上执行如下命令

```
gateway lb -v 10.99.207.2 -a 10.99.207.10 -b 10.99.207.11 -e eth0 -i eth1 -r
10.99.207.20,10.99.207.21,10.99.207.22 enable。
```

(5) 在每台网关设备上配置好代理的 Controller 地址后，执行如下命令将网关适配软件 LB 环境。

```
gateway lb-gateway -v 10.99.207.2 enable
```

(6) 通过如下命令 gateway lb status 查看本 LB 设备上 LB 服务是否开启，显示 active 表示已开启。

```
[root@localhost ~]# gateway lb status
LB service status:  active
```

2. 虚拟 IP 地址是公网 IP 地址场景

虚拟 IP 配置在子接口上，在对外的接口上配置实 IP，但是不要求实 IP 和虚拟 IP 在同一网段。虚拟 IP 地址是公网 IP，则需要在交换机上配置路由使得数据包可以送到虚拟 IP 地址上。

以下表网络规划为例：

图6-3 LB 网络规划举例-虚拟 IP 地址是公网 IP

LB 类型	对外网卡/IP	对外网关	对内网卡	说明
主用LB	eth0/192.168.5.10	不配置	eth1	• 虚拟 IP 地址：122.99.207.2，掩码为 255.255.255.0，需要配置虚拟的缺省路由的下一跳为 122.99.207.10。 • 两个 LB 的对内网卡 eth1 上配置有同网段的 IP 地址，可跟 Controller 和其他 CVK 互通，主要是用于后续纳管使用。 • LB 设备代理的安全网关对外地址列表为 192.168.5.20，192.168.5.21，192.168.5.22，安全网关对外地址要求和 LB 对外网卡的实 IP 地址在同一个二层网络，并且配置有网络网关地址，网络网关地址是交换机上的 vlan 接口地址。 • 交换机上两台 LB 和三台网关的对外接口的网口需允许通过 122.99.207.10 和 192.168.5.20 两个网段的 VLAN。
备用LB	eth0/192.168.5.11	不配置	eth1	

(1) 在主用 LB 上执行如下命令。

```
gateway lb -v 122.99.207.2 -m 255.255.255.0 -a 192.168.5.10 -b 192.168.5.11 -e eth0 -i eth1 -r 192.168.5.20,192.168.5.21,192.168.5.22 -d 0.0.0.0 -s 0.0.0.0 -n 122.99.207.10 enable。
```

(2) 在备用 LB 上执行如下命令。

```
gateway lb -v 122.99.207.2 -m 255.255.255.0 -a 192.168.5.10 -b 192.168.5.11 -e eth0 -i eth1 -r 192.168.5.20,192.168.5.21,192.168.5.22 -d 0.0.0.0 -s 0.0.0.0 -n 122.99.207.10 enable。
```

(3) 在每台网关设备上配置好代理的 Controller 地址后，执行如下命令将网关适配软件 LB 环境。

```
gateway lb-gateway -v 122.99.207.2 enable
```

(4) 通过如下命令 gateway lb status 查看本 LB 设备上 LB 服务是否开启，显示 active 表示已开启。

```
[root@localhost ~]# gateway lb status
LB service status:  active
```

6.1.4 关闭软件 LB 功能

输入以下命令关闭软件 LB 功能：

```
[root@localhost ~]# gateway lb disable
```

6.1.5 修改软件 LB 配置

修改软件 LB 配置需先关闭软件 LB 功能，再配置参数并启用软件 LB 功能，以使修改的配置生效。

6.2 HA

安全网关解决方案支持双网关 HA 部署，主网关失效时，将自动切换到备网关，可以有效防止单点故障，提高可靠性。

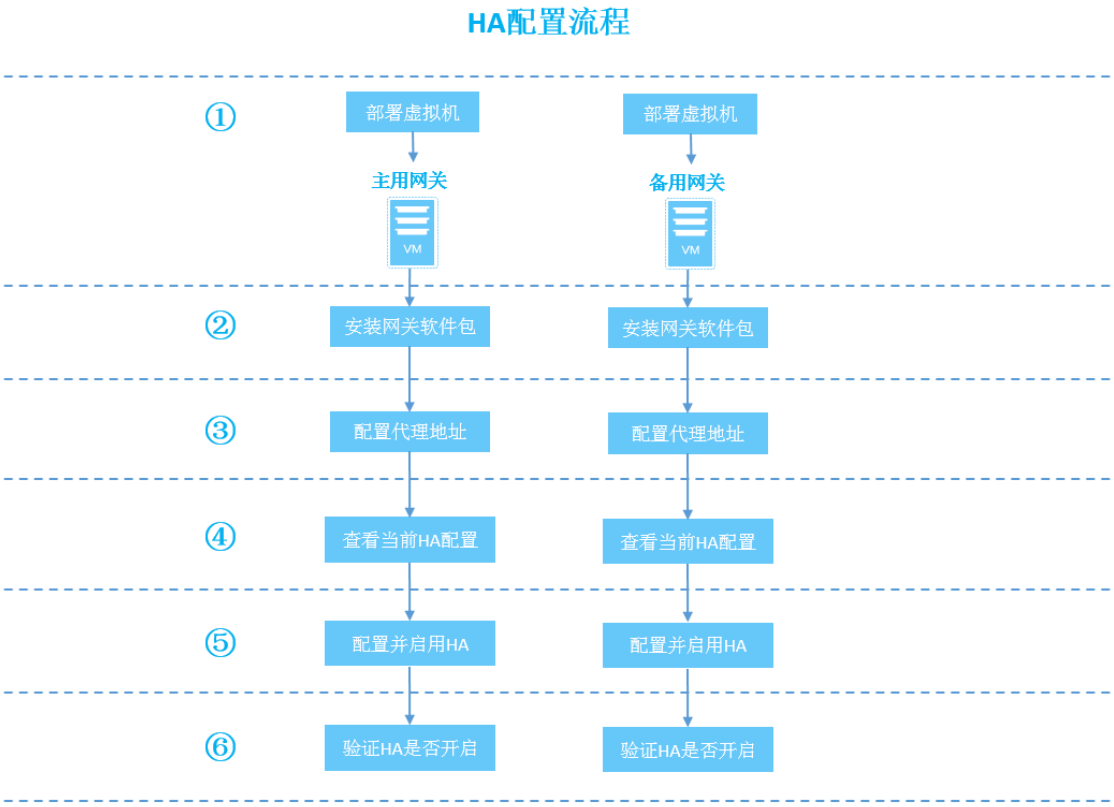
说明

启用 SR-IOV+安全网关 DPDK 功能的组网环境不支持 HA 特性，未启用 SR-IOV+安全网关 DPDK 功能的组网环境可以启用 HA 功能。

6.2.1 配置流程

HA 配置流程如下图所示。

图6-4 HA 配置流程



6.2.2 命令行参数说明

功能配置命令行帮助如下所示，请参考命令行帮助进行 HA 配置：

```
[root@localhost ~]# gateway ha --help
Usage: gateway ha [OPTIONS] ACTION
```

```
  HA service control, action: enable,disable,status
Options:
  -v, --vip VIP              Set virtual IP for Gateway HA.
  -m, --mask NETMASK         Set virtual IP network mask for Gateway HA.
  -r, --role ROLE            Set default role for this Gateway for HA.
  -a, --master-ip MASTER_IP  Set master IP for Gateway HA.
  -b, --backup-ip BACKUP_IP  Set backup IP for Gateway HA.
  -e, --expose-iface IFACE   Set expose interface for Gateway HA.
  -i, --inner-iface IFACE    Set inner interface for Gateway HA.
  -d, --vroute-dst IP        Set virtual route destination.
  -s, --vroute-mask NETMASK  Set virtual route destination mask.
  -n, --vroute-nexthop IP    Set virtual route nexthop.
  -u, --virtual-router-id ID  Set virtual route id. value range from 1 to 255
  --help                     Show this message and exit.
```

表6-2 参数说明

参数	说明
-v或--vip	高可用虚拟IP地址，对外提供服务的IP
-m或--mask	虚拟IP地址的掩码
-r或--role	本网关设备在HA中的默认角色，取值为master或backup
-a或--master-ip	默认主用网关的实IP地址，对应主用网关上的expose_iface参数配置的网卡的IP地址
-b或--backup-ip	默认备用网关的实IP地址，对应备用网关上的expose_iface参数配置的网卡的IP地址
-e或--expose-iface	对外暴露的IP所在网卡的名称，用于客户端访问网关
-i或--inner-iface	对内访问的IP所在网卡的名称，用于网关访问Controller和虚拟机
-d或--vroute-dst	虚拟路由的目的网段地址，如果要设置默认路由，则输入0.0.0.0
-s或--vroute-mask	虚拟路由的目的网段的掩码，如果要设置默认路由，则输入0.0.0.0
-n或--vroute-nexthop	虚拟路由的下一跳地址
-u或—virtual-router-id	设置虚拟路由器的ID，取值范围从1到255

6.2.3 配置场景

目前 HA 仅支持主备网关，配置命令需要分别在主备网关上配置。高可用虚拟 IP 地址可以配置在对外网卡的主接口上，也可以配置在对外网卡的子接口上。配置在主接口上一般适用于虚拟 IP 地址是一个公网 IP 地址的场景，配置在子接口上一般适用于虚拟 IP 地址是一个私网 IP 地址的场景。下面将分别介绍两种场景的 HA 配置方案。

1. 虚拟 IP 地址为私网 IP 地址场景

该场景对于 IP 地址使用数量不敏感，推荐为对外网卡配置实 IP 地址，虚拟 IP 地址与实 IP 地址在同一网段。该场景下，虚拟路由为可选字段，未配置时虚拟 IP 地址的路由使用的是实 IP 地址相关的路由配置，如果实 IP 地址配置有网关地址，则虚拟 IP 也可以通过该网关访问到外网。如果实 IP 地址上没有配置网关地址，也没有配置相关路由，则需要配置虚拟路由，使得虚拟 IP 地址可以访问外网。

以下表网络规划为例：

表6-3 启用 HA 网络规划举例-虚拟 IP 地址为私网 IP

网关类型	对外网卡/IP	对外网卡网关	对内网卡	说明
主用网关	eth0/10.99.207.10	10.99.207.1	eth1	• 虚拟 IP 地址：10.99.207.2 • 两个网关的对内网卡 eth1 上配置有同网段的 IP 地址
备用网关	eth0/10.99.207.11	10.99.207.1	eth1	

配置步骤如下：

(1) 执行 gateway config ha 命令查看当前 HA 配置信息，出厂有默认配置，默认 HA 处于关闭状态。HA 参数为 enable 则表示 HA 服务已开启，disable 则表示 HA 服务已关闭。

```
[root@localhost ~]# gateway config ha
ha:disable
```

(2) 在主用网关上执行如下命令。

```
gateway ha -v 10.99.207.2 -a 10.99.207.10 -b 10.99.207.11 -e eth0 -i eth1 enable
```

(3) 在备用网关上执行如下命令。

```
gateway ha -v 10.99.207.2 -a 10.99.207.10 -b 10.99.207.11 -e eth0 -i eth1 enable。
```

(4) 通过命令 gateway ha status 查看本机上 HA 服务是否开启，显示 active 则表示已开启。

```
[root@localhost ~]# gateway ha status
gateway HA service status:  active
```

2. 虚拟 IP 地址为公网 IP 地址场景

该场景一般对于公网 IP 地址使用数量较为敏感，所以我们推荐不给对外网卡配置实 IP 地址，虚拟 IP 地址直接通过 HA 功能下发到网卡主接口上。

以下表网络规划为例：

表6-4 启用 HA 网络规划举例-虚拟 IP 地址为公网 IP

网关类型	对外网卡	对外网卡 IP	下一跳地址	对内网卡	说明
主用网关	eth0	未配置	10.99.207.1	eth1	• 虚拟 IP 地址：10.99.207.2 • 两个网关的对内网卡 eth1 上配置有同网段的 IP 地址，请勿在 eth1 上配置网关地址
备用网关	eth0	未配置	10.99.207.1	eth1	

配置步骤如下：

(1) 执行 gateway config ha 命令查看当前 HA 配置信息，出厂有默认配置，默认 HA 处于关闭状态。HA 参数为 enable 则表示 HA 服务已开启，disable 则表示 HA 服务已关闭。

```
[root@localhost ~]# gateway config ha
ha:disable
```

(2) 在主用网关上执行如下命令。

```
gateway ha -v 10.99.207.2 -m 255.255.255.0 -r master -e eth0 -i eth1 -d 0.0.0.0 -s 0.0.0.0
-n 10.99.207.1 enable
```

(3) 在备用网关上执行如下命令。

```
gateway ha -v 10.99.207.2 -m 255.255.255.0 -r backup -e eth0 -i eth1 -d 0.0.0.0 -s 0.0.0.0
-n 10.99.207.1 enable
```

(4) 通过命令 gateway ha status 查看本机上 HA 服务是否开启，显示 active 则表示已开启。

```
[root@localhost ~]# gateway ha status
gateway HA service status:  active
```

6.2.4 关闭 HA 功能

输入以下命令即可关闭 HA 功能：

```
gateway ha disable
```

6.2.5 修改 HA 配置

修改 HA 配置需先关闭 HA 功能，再配置参数并启用 HA 功能，以使修改的配置生效。

6.3 网关性能加速

当安全网关部署于虚拟机上时，可通过网关性能加速功能，提升安全网关性能。网关性能加速功能提供 3 种提升性能的方法，三种方法只能采用其中一种，请用户根据实际情况选择对应方法：

- 虚拟化 DPDK：若服务器网卡为 Workspace 管理平台 DPDK 功能支持的网卡，则可采用此方法。
- SR-IOV+安全网关 DPDK：若服务器网卡为 Intel 82599 系列网卡，则可采用此方法。
- 内核加速：若前两种方法条件都不满足，则可采用此方法。

说明

若安全网关部署于物理服务器，则无需配置网关性能加速功能。

6.3.1 虚拟化 DPDK

UniCloud Workspace 支持启用管理平台自带虚拟化 DPDK 功能，启用虚拟化 DPDK 功能步骤如下：

1. 主机启用 DPDK 功能

主机启动项配置

主机启用 DPDK 功能需要完成如下启动项配置：

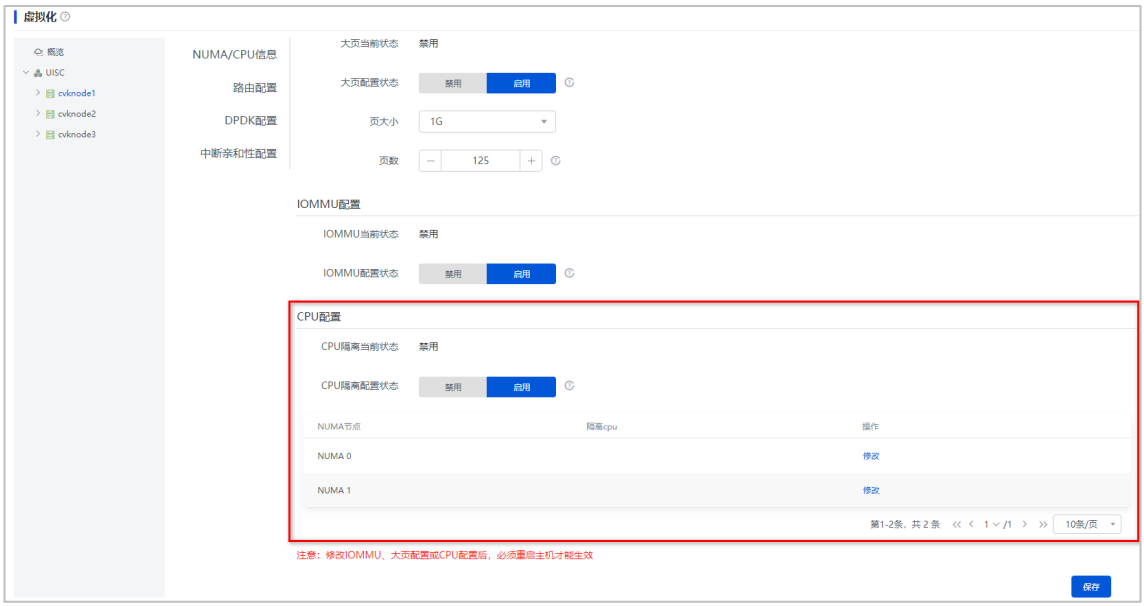
- 主机开启大页配置：该功能是将内存分页从默认的 4K 改为 2M 或 1G，减少在运行 DPDK 时出现从寄存器获取页表失败的情况，提高使用内存时的查表速率，默认将主机一半的内存设为大页内存。
- 主机开启 IOMMU 配置：该功能是将网卡分为不同的 IOMMU 组，将物理内存映射为虚拟内存，提升 IO 设备访问内存的性能。
- CPU 隔离：为了能达到最好的性能效果，需要将物理主机的 CPU 进行隔离，在每个 NUMA 节点中中选择若干 CPU 隔离给 DPDK 使用。如果开启了超线程，也需要将对应的 CPU 进行隔离，同时预留部分 CPU 给系统处理使用，不推荐 CPU0 给 DPDK 使用。

(1) 在管理平台中单击左侧导航树[数据中心/虚拟化]菜单项，在虚拟化页面左侧单击欲修改的主机，然后单击右侧的“高级设置”页签，将该服务器的大页配置状态和 IOMMU 状态设置为启用，页大小选择 2MB，页数会根据页大小设置带出。

图6-5 启用大页配置与 IOMMU

(2) 启用 CPU 隔离，在 CPU 隔离配置状态选择框中选择启用 CPU 隔离。分别选择每个 NUMA 节点，单击 NUMA 节点对应操作列的图标，弹出隔离 CPU 对话框，根据需要选择几个 CPU 隔离给 DPDK 使用，不推荐 CPU0 给 DPDK 使用，设置完成后单击<保存>按钮。

图6-6 启用 CPU 隔离



(3) （选配）启用中断亲和性配置，在主机的“高级选项”页签，选择[中断亲和性配置]菜单项，进入主机的中断亲和性配置页面。启用中断亲和性状态。分别选择每个 NUMA 节点，单击 NUMA 对应操作列的图标，弹出中断亲和性绑定页面，选择在主机启动项配置步骤(2)中未配置隔离的 CPU，单击<确定>按钮，设置完成后单击<保存>按钮。

说明

中断亲和性配置是将中断程序运行到非隔离的 CPU 上，避免对 DPDK 或其他实时性程序的影响。

图6-7 中断亲和性配置

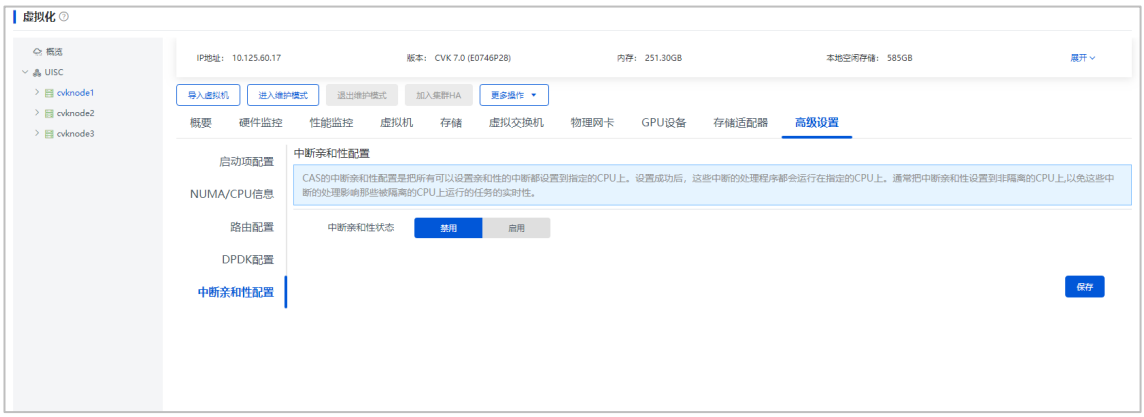


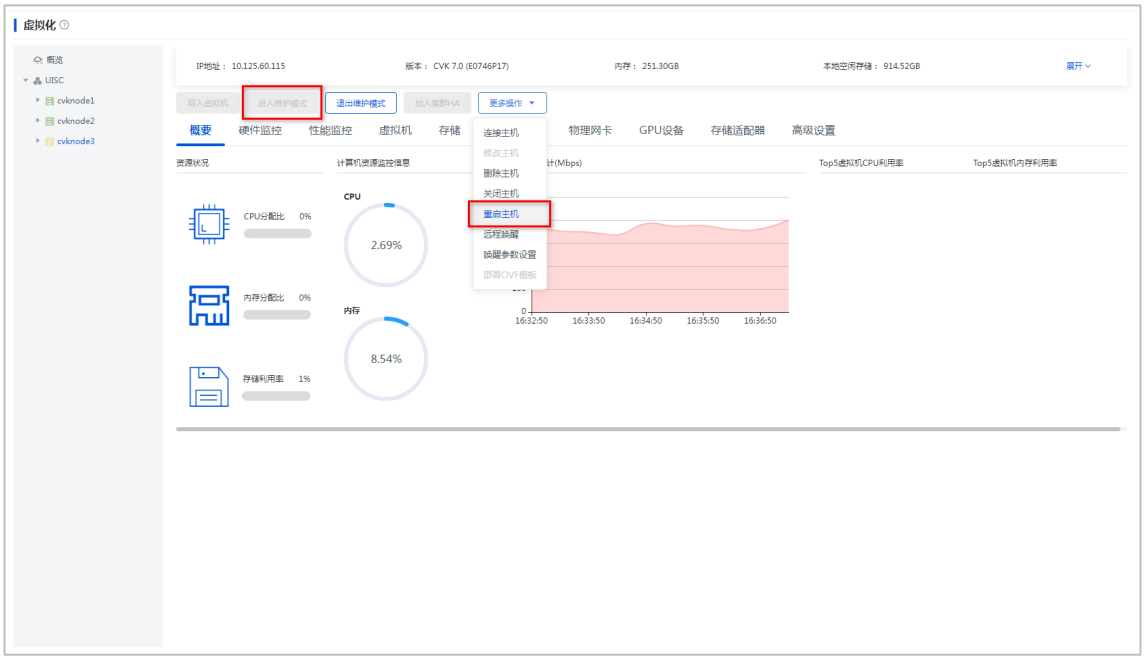
图6-8 启用中断亲和性状态

(4) 完成上述配置后，重启主机使得配置生效。在主机概要信息页面单击<进入维护模式>按钮，使主机进入维护模式，单击<更多操作>按钮，选择[重启主机]菜单项重启主机。重启主机完成后退出维护模式。

说明

重启主机时，主机上的业务将中断，请提前完成应对措施。

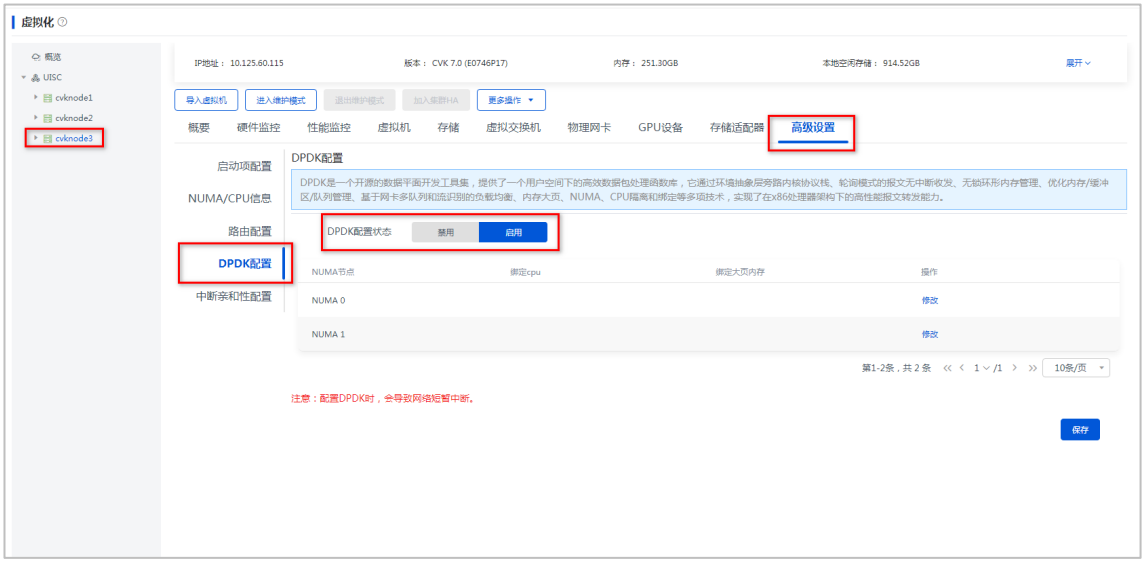
图6-9 重启主机



开启主机 **DPDK** 功能

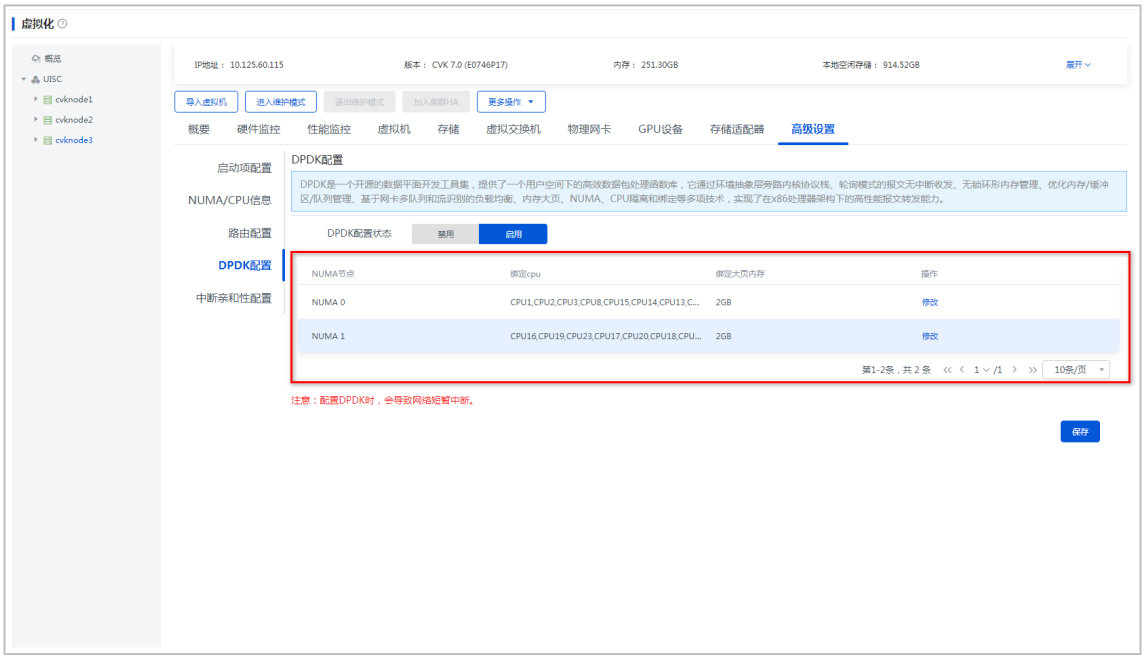
(1) 在主机的“高级设置”页签，选择[DPDK 配置]菜单项，进入主机的 DPDK 配置页面，启用 DPDK。

图6-10 启用主机 DPDK 功能



(2) 分别选择两个 NUMA 节点，单击 NUMA 对应操作列的图标，弹出“隔离 cpu”对话框，输入大页内存容量为 2GB，选择在主机启动项配置步骤(2)中设置的隔离的 CPU，单击<确定>按钮。

图6-11 配置隔离 CPU



2. 修改网卡为 VFIO 驱动

(1) 在管理平台中单击左侧导航树[数据中心/虚拟化]菜单项，在虚拟化页面左侧单击欲修改的主机，单击右侧的“物理网卡”页签，选择规划的网卡，单击操作列下的<修改>按钮，弹出“修改物理网卡”对话框，将驱动修改为“VFIO 驱动”，单击<确定>按钮，保存修改。

图6-12 修改主机物理网卡驱动-1

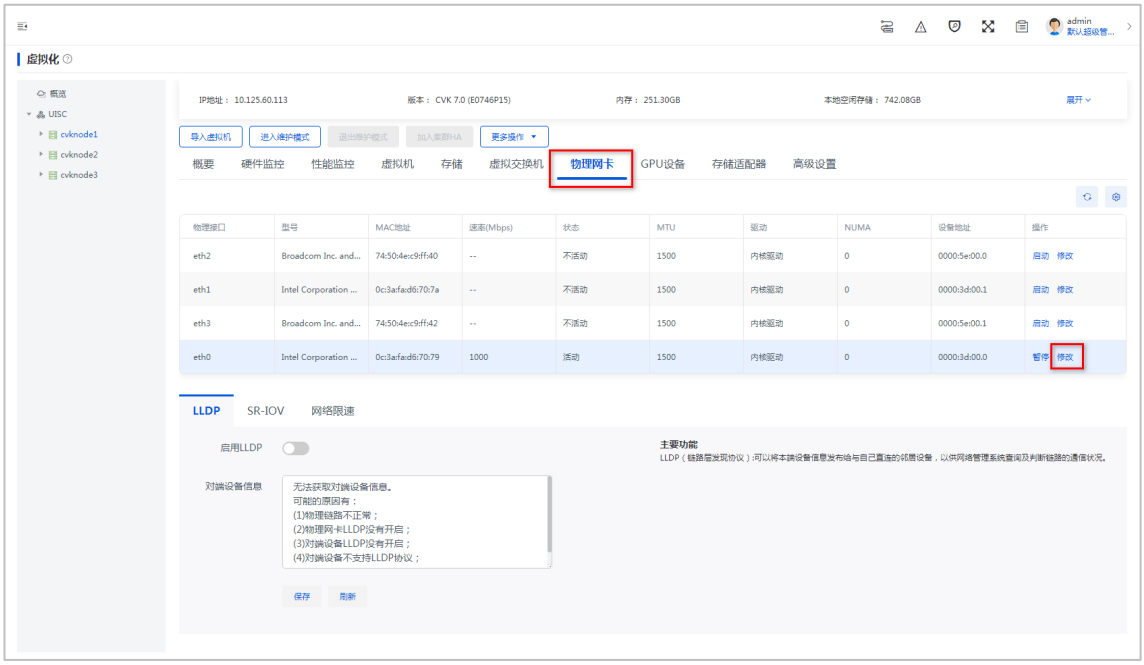
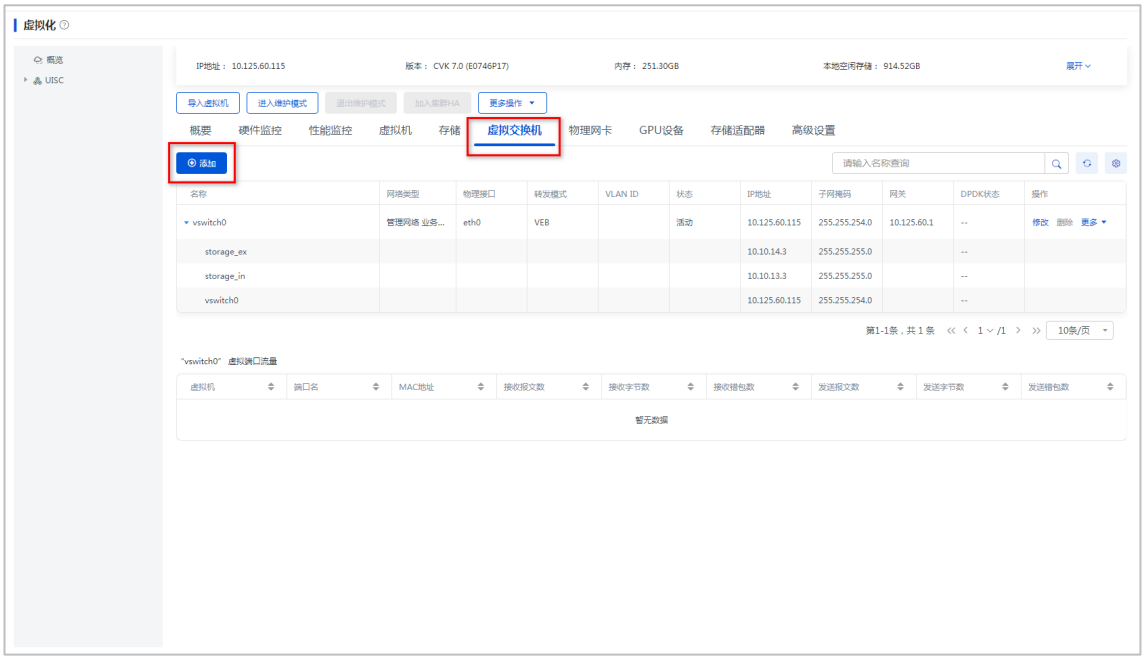


图6-13 修改主机物理网卡驱动-2

3. 增加 DPDK 虚拟交换机

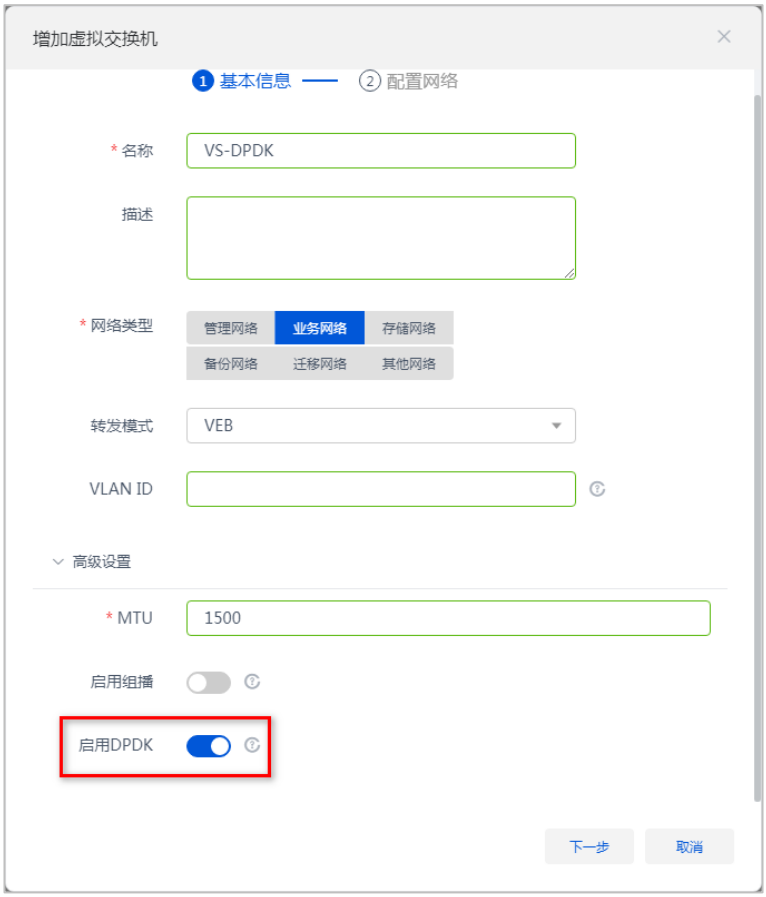
(1) 在管理平台中单击左侧导航树[数据中心/虚拟化]菜单项，在虚拟化页面左侧单击欲修改的主机，单击右侧的“虚拟交换机”页签，单击<添加>按钮，弹出“增加虚拟交换机”对话框。

图6-14 “虚拟交换机”页签



(2) 在对话框中，网络类型选择“业务网络”，根据需要设置虚拟交换机的 VLAN ID，在高级设置中选择启用 DPDK，单击<下一步>按钮。

图6-15 增加 DPDK 虚拟交换机-基本信息



(3) 选择在修改网卡驱动为 VFIO 步骤中修改了驱动的网卡，根据需要设置 IP 地址和掩码，单击<完成>按钮完成操作。

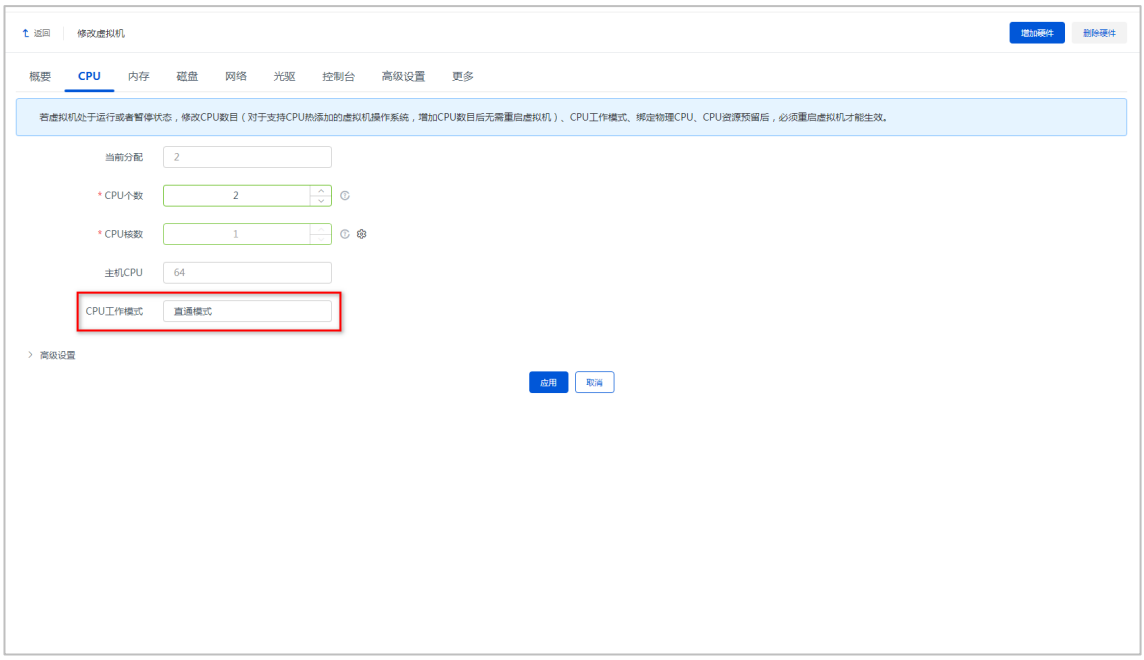
图6-16 增加 DPDK 虚拟交换机-配置网络

4. 虚拟机 DPDK 设置

(1) 选择顶部“虚拟机”页签，在虚拟机列表中选择网关虚拟机，进入虚拟机概要页面。

(2) 单击<修改>按钮，修改虚拟机 CPU 工作模式为直通模式。

图6-17 修改 CPU 工作模式

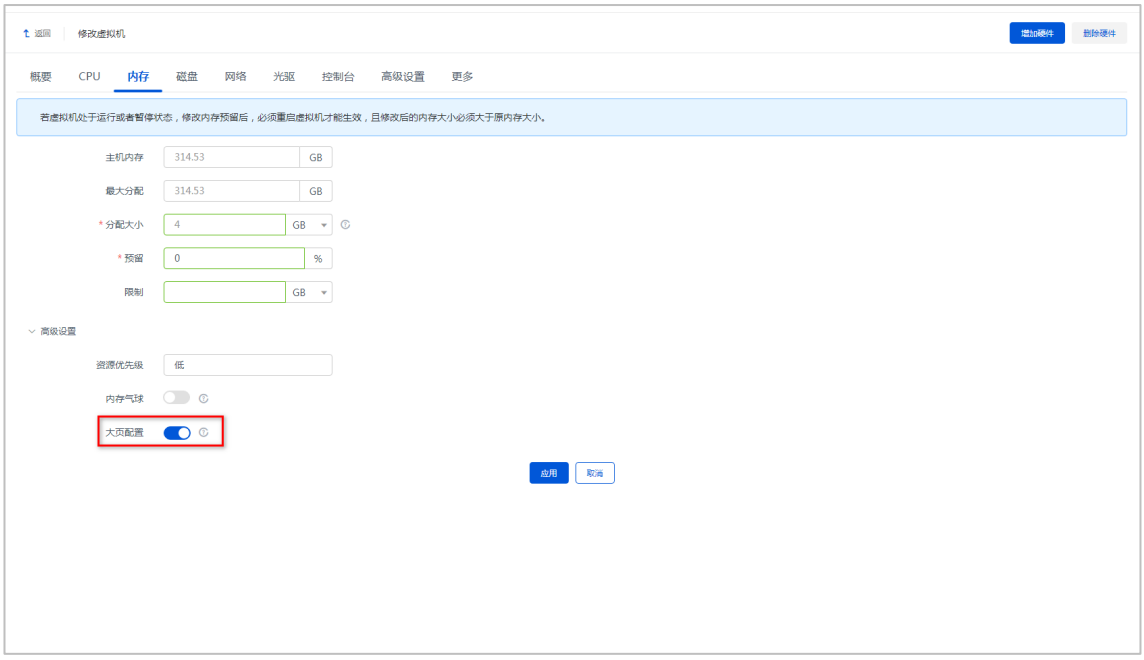


(3) 虚拟机 CPU 与物理 CPU 绑定：单击 CPU 核数右边的 图标，选择虚拟 CPU 需要绑定的物理 CPU，可以一个虚拟 CPU 绑定多个物理 CPU，但同一虚拟机所有的虚拟 CPU 绑定的物理 CPU 需要在同一个 NUMA 里。单击<确定>按钮。

图6-18 绑定物理 CPU

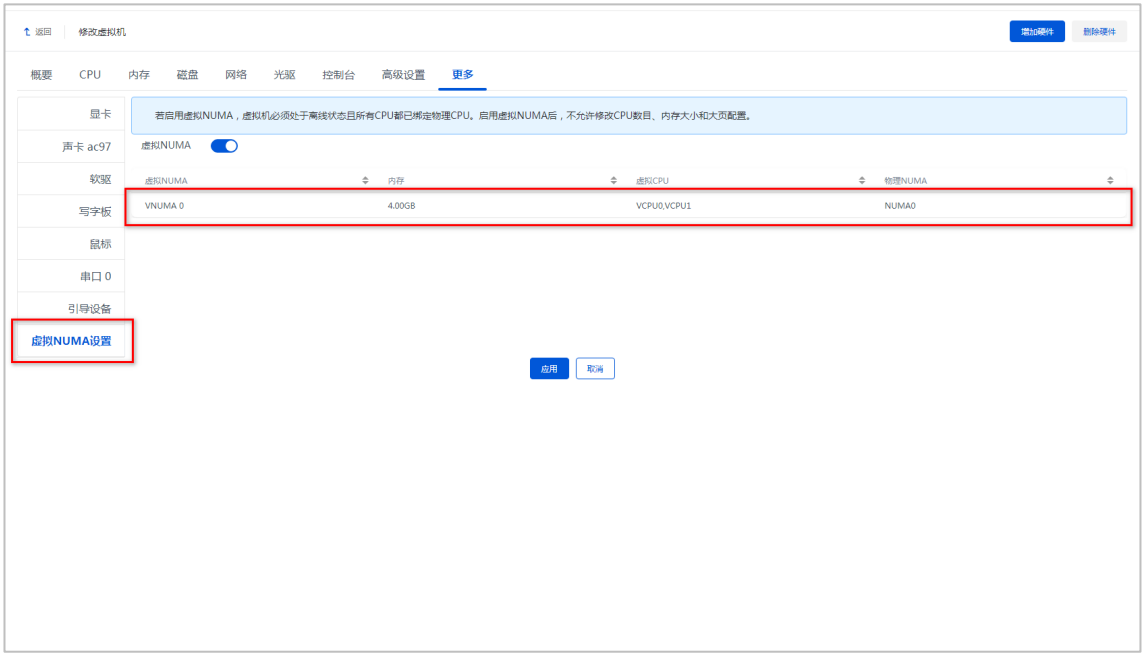
(4) 开启内存大页功能，该功能需要在虚拟机关闭状态才能开启，且开启内存大页功能后内存预留，内存限制，内存优先级和内存气球功能都不可以再配置。

图6-19 开启虚拟机大页功能



(5) 开启虚拟 NUMA 功能。

图6-20 开启虚拟 NUMA



(6) 为虚拟机增加 DPDK 网卡。在修改虚拟机页面单击<增加硬件>按钮，硬件类型选择“网络”，单击<下一步>按钮。设置型号选择“高速网卡”，虚拟交换机选择开启了 DPDK 功能的虚拟交换机，其余选项根据实际需要进行设置，单击<完成>按钮完成配置。

图6-21 增加 DPDK 网卡

(7)　至此网关虚拟机 DPDK 功能配置完成。

6.3.2 SR-IOV+安全网关 DPDK

安全网关解决方案目前仅支持使用 Intel 82599 系列网卡，且启用了 SR-IOV 的情况下启用安全网关自带的 DPDK 功能，ARM 架构主机不支持本功能。建议欲启用本功能的网关虚拟机配置三个网口，一个网口用于管理，使用普通的 virtio 网卡，另外两个网口使用支持 SR-IOV 的 82599 网卡。一张 82599 网卡上通常有两个网口，可以分别作为出入网关流量的网口。

⚠ 注意

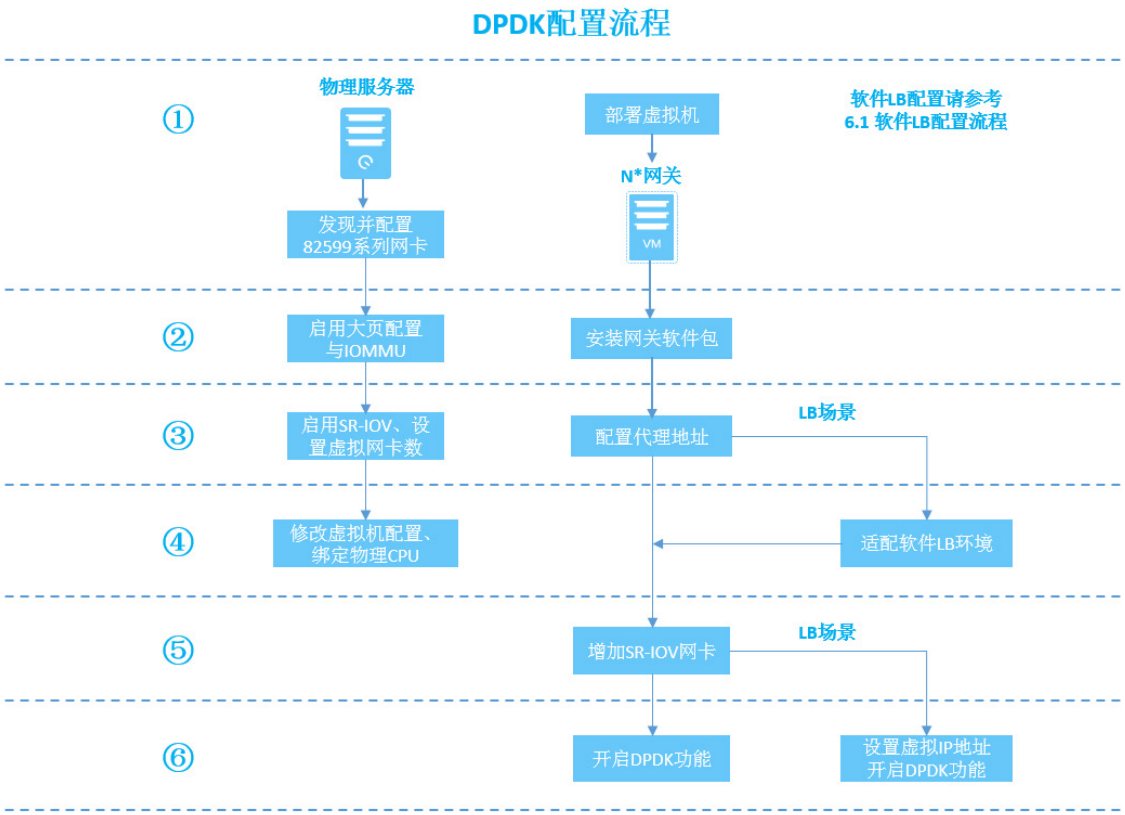
物理服务器开启 SR-IOV 功能中启用大页配置和 IOMMU 操作需重启物理服务器以生效，在启用 SR-IOV+安全网关 DPDK 功能之前，请做好应对举措，避免服务器重启导致服务器上运行虚拟机受到影响。

---

1. 配置流程

DPDK 配置流程如下图所示，软件 LB 配置请参考软件 LB。

图6-22 DPDK 配置流程



2. 在物理服务器上开启 SR-IOV 功能

(1) 进入物理服务器后台，通过 lspci | grep 82599 命令确认服务器上是否有支持 SR-IOV 的 82599 系列网卡。

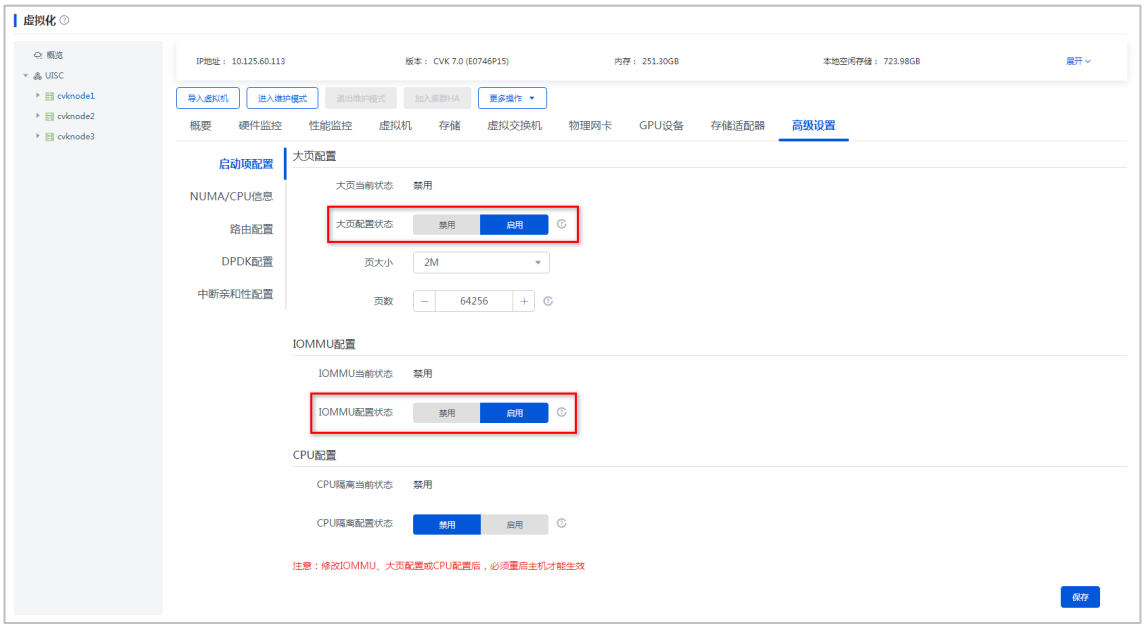
```
root@cvknode124:~# lspci | grep 82599
86:00.0 Ethernet controller: Intel Corporation 82599ES 10-Gigabit SFI/SFP+ Network Connection (rev 01)
86:00.1 Ethernet controller: Intel Corporation 82599ES 10-Gigabit SFI/SFP+ Network Connection (rev 01)
```

(2) 在服务器上分别为 82599 系列网卡的两个网口执行如下命令（命令中以 eth5，eth6 为例，请根据实际网卡名称进行配置），并且将命令写入启动项脚本中。

```
[root@cvknode ~]# ethtool -X eth5 hkey
d1:81:c6:2c:f7:f4:db:5b:19:83:a2:fc:94:3e:1a:db:d9:38:9e:6b:d1:03:9c:2c:a7:44:99:ad
:59:3d:56:d9:f3:25:3c:06:2a:dc:1f:fc
[root@cvknode ~]# ethtool -X eth6 hkey
d1:81:c6:2c:f7:f4:db:5b:19:83:a2:fc:94:3e:1a:db:d9:38:9e:6b:d1:03:9c:2c:a7:44:99:ad
:59:3d:56:d9:f3:25:3c:06:2a:dc:1f:fc
[root@cvknode ~]# echo "ethtool -X eth5 hkey            //将命令加入启动项
d1:81:c6:2c:f7:f4:db:5b:19:83:a2:fc:94:3e:1a:db:d9:38:9e:6b:d1:03:9c:2c:a7:44:99:ad
:59:3d:56:d9:f3:25:3c:06:2a:dc:1f:fc" >> /etc/rc.d/rc.local
[root@cvknode ~]# echo "ethtool -X eth6 hkey          //将命令加入启动项
d1:81:c6:2c:f7:f4:db:5b:19:83:a2:fc:94:3e:1a:db:d9:38:9e:6b:d1:03:9c:2c:a7:44:99:ad
:59:3d:56:d9:f3:25:3c:06:2a:dc:1f:fc" >> /etc/rc.d/rc.local
[root@cvknode ~]# chmod +x /etc/rc.d/rc.local
```

(3) 如果服务器上存在符合条件的网卡，则在管理平台中单击左侧导航树[数据中心/虚拟化]菜单项，在虚拟化页面左侧单击欲修改的主机，然后单击右侧的“高级设置”页签，将该服务器的大页配置状态和 IOMMU 状态设置为启用，页大小选择 2MB，页数会根据页大小设置带出。设置完成后单击<保存>按钮，并重启主机使得配置生效。

图6-23 启用大页配置与 IOMMU

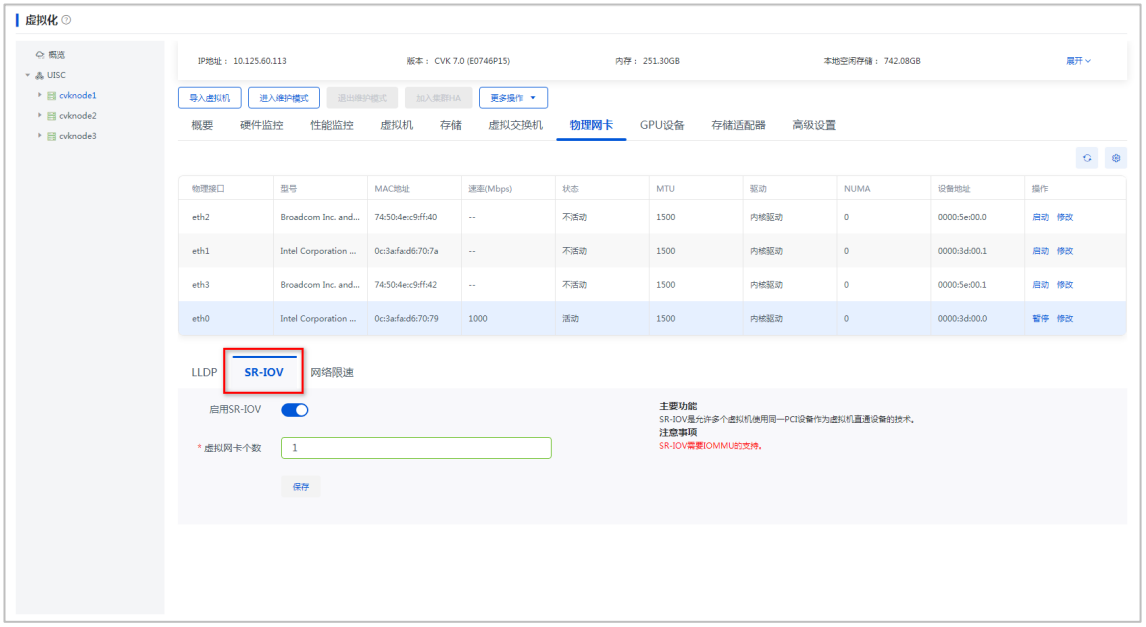


(4) 服务器启动完成后，单击主机操作页面上的“物理网卡”页签，在页签下选择对应的处于活动状态的 82599 系列网卡，然后在下方的[SR-IOV]页签中启用 SR-IOV，并根据网关虚拟机数量配置虚拟网卡个数，一个网关虚拟机需要一个虚拟网卡。

说明

配置 SR-IOV 之前请做好规划，当网关虚拟机使用 SR-IOV 切分的虚拟网卡之后，无法再次对 SR-IOV 进行虚拟网卡数设置。

图6-24 配置 SR-IOV



(5) 在管理平台左侧导航栏中单击[数据中心/虚拟化]菜单项，进入虚拟化页面，在页面中单击“虚拟机”页签，单击下方显示的虚拟机列表中的网关虚拟机操作列下的<修改>按钮，进入修改虚拟机页面。参考表 2-1 修改虚拟机的配置，将 CPU 个数修改为 1 个，CPU 核数修改为大于等于 4 核，CPU 工作模式改为直通模式。单击 CP 核数旁的⚙按钮，弹出“绑定物理 CPU”对话框，单击虚拟 CPU 操作列的<编辑>按钮，在弹出的对话框中选择欲绑定的物理 CPU，将 4 个虚拟 CPU 绑定在同一个物理 CPU 的不同核上。

图6-25 修改虚拟机 CPU 配置

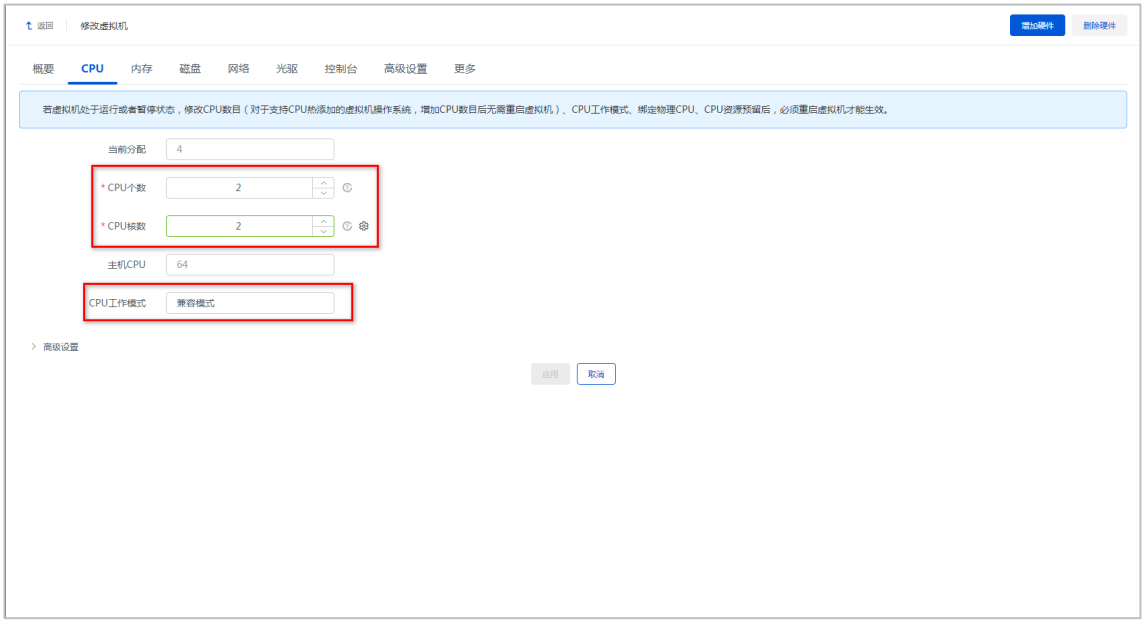


图6-26 绑定物理 CPU

(6) 单击<增加硬件>按钮，为虚拟机增加两块 SR-IOV 直通网卡。在“增加硬件”对话框中，硬件类型选择网络，设备类型选择 SR-IOV 网卡，记录下 MAC 地址，便于后续通过 MAC 地址分辨对应网卡和物理端口。重复同样的操作，完成两块 SR-IOV 网卡的增加，完成后在虚拟化页面中先关闭虚拟机，再启动虚拟机使配置生效。

说明

- 两块 SR-IOV 直通网卡分别用于外网和内网访问，需要分布在不同的物理网口上，一块 82599 网卡上有两个万兆口，可以分别给出入方向使用。
- 增加网卡完成后，请务必在虚拟化界面先关闭虚拟机，再启动虚拟机使配置生效。在 shell 中通过 reboot 命令重启将会不生效。
- 新增的 SR-IOV 网卡无需配置 IP 等信息，在启用 DPDK 功能时会通过命令行配置。

图6-27 增加 SR-IOV 网卡

(7) 打开虚拟机控制台，通过 ifconfig 命令查看网卡是否添加成功，并分别记录网卡编号。如下命令行显示 ens10，ens11 两个网卡是添加的 SR-IOV 直通网卡。

```
[root@localhost ~]# ifconfig
ens10: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        ether 0c:da:41:1d:4c:a3  txqueuelen 1000  (Ethernet)
        RX packets 35450  bytes 2331379 (2.2 MiB)
        RX errors 0  dropped 37  overruns 0  frame 0
        TX packets 203  bytes 35762 (34.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

ens11: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        ether 0c:da:41:1d:7b:9c  txqueuelen 1000  (Ethernet)
        RX packets 35450  bytes 2331379 (2.2 MiB)
        RX errors 0  dropped 37  overruns 0  frame 0
```

```
        TX packets 203  bytes 35762 (34.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

3. 启用 DPDK 功能

(1) DPDK 功能配置命令行帮助如下所示，参考命令行帮助配置网卡 IP 并启用 DPDK 功能。

```
[root@localhost ~]# gateway dpdk --help
  DPDK control, action: enable or disable.
Options:
  -e, --ex-iface IFACE         Set DPDK exter interface.
  -a, --ex-addr IP             Set DPDK exter interface IP address.
  -m, --ex-mask NETMASK        Set DPDK exter interface netmask.
  -l, --ex-addr-alias IP       Set DPDK exter interface IP address alias for
                               LB.
  -d, --ex-route-dst IP        Set DPDK exter interface route destination.
  -k, --ex-route-mask NETMASK  Set DPDK exter interface route destination
                               mask.
  -n, --ex-route-nexthop IP    Set DPDK exter interface route nexthop.
  -i, --in-iface IFACE         Set DPDK inner interface.
  -r, --in-addr IP             Set DPDK inner interface IP address.
  -s, --in-mask NETMASK        Set DPDK inner interface netmask.
  -o, --in-route-dst IP        Set DPDK inner interface route destination.
  -u, --in-route-mask NETMASK  Set DPDK inner interface route destination
                               mask.
  -x, --in-route-nexthop IP    Set DPDK inner interface route nexthop.
  --help                       Show this message and exit.
```

表6-5 参数解释

参数	说明
ACTION	enable或disable，enable表示启用dpdk，disable表示关闭dpdk
-e或--ex-iface	DPDK对外提供访问的网口
-a或--ex-addr	对外提供访问的网口的IP地址
-m或--ex-mask	对外提供访问的网口的掩码
-l或--ex-addr-alias	配合软件LB使用的VIP地址。用于实际提供外网访问，可选参数
-d或--ex-route-dst	外网路由的目的网段地址，0.0.0.0表示默认路由
-k或--ex-route-mask	外网路由的目的网段掩码，0.0.0.0表示默认路由
-n或 --ex-route-nexthop	外网路由的目的下一跳地址
-i或--in-iface	DPDK对内访问Controller和CVK的网口
-r或--in-addr	对内访问Controller和CVK的网口的IP地址
-s或--in-mask	对内访问Controller和CVK的网口的掩码
-o或--in-route-dst	对内路由的目的网段地址，可选，若未填写，默认内网走二层转发
-u或--in-route-mask	对内路由的目的网段掩码，可选，若未填写，默认内网走二层转发
-x或	对内路由的目的下一跳地址，可选，若未填写，默认内网走二层转发

--in-route-nexthop	

说明

为了排除网络中杂包的干扰，提升转发性能，要求网关虚拟机的内部网络和 CVK 不在同一个二层网络（需要路由器三层转发）。

(2) 以下表网络规划为例，输入以下命令即可开启 DPDK 功能。

```
gateway dpdk -e ens11 -a 10.125.35.222 -m 255.255.252.0 -d 0.0.0.0 -k 0.0.0.0 -n 10.125.32.1 -i ens12 -r 192.168.3.222 -s 255.255.255.0 -o 192.168.5.23 -u 255.255.255.0 -x 192.168.3.1 enable
```

表6-6 启用 DPDK-网络规划举例

网口类型	名称	网口 IP	掩码	下一跳地址	目的网段/掩码
对外网口	eth11	10.125.35.222	255.255.252.0	10.125.32.1	无
对内网口	eth12	192.168.3.222	255.255.255.0	192.168.3.1	192.168.5.23/24（Controller与CVK在该网段下）

(3) 对于 DPDK 支持 LB 的场景，需要在 DPDK 网关上启用-l 或--ex-addr-alias 参数，设置软件 LB 使用的虚拟 IP 地址。该虚拟 IP 地址和软件 LB 设备上使用的虚拟 IP 地址一致。在上述同样环境下，假设虚拟 IP 地址是 10.125.35.224，在其他网关设备上启用软件 LB 后，该网关上需要执行的命令如下。

```
gateway dpdk -e ens11 -a 10.125.35.222 -m 255.255.252.0 -l 10.125.35.224 -d 0.0.0.0 -k 0.0.0.0 -n 10.125.32.1 -i ens12 -r 192.168.3.222 -s 255.255.255.0 -o 192.168.5.23 -u 255.255.255.0 -x 192.168.3.1 enable
```

4. 关闭 DPDK 功能

输入以下命令即可关闭 DPDK 功能：

```
Gataway dpdk disable
```

5. 修改 DPDK 配置

修改 DPDK 配置需先关闭 DPDK 功能，再配置参数并启用 DPDK 功能，以使修改的配置生效。

6.3.3 内核加速

开启内核加速功能后，高速类型网卡将以一个单独线程的形式在 CVK 内核中进行模拟，可以提升虚拟机网络性能，配置方法如下：

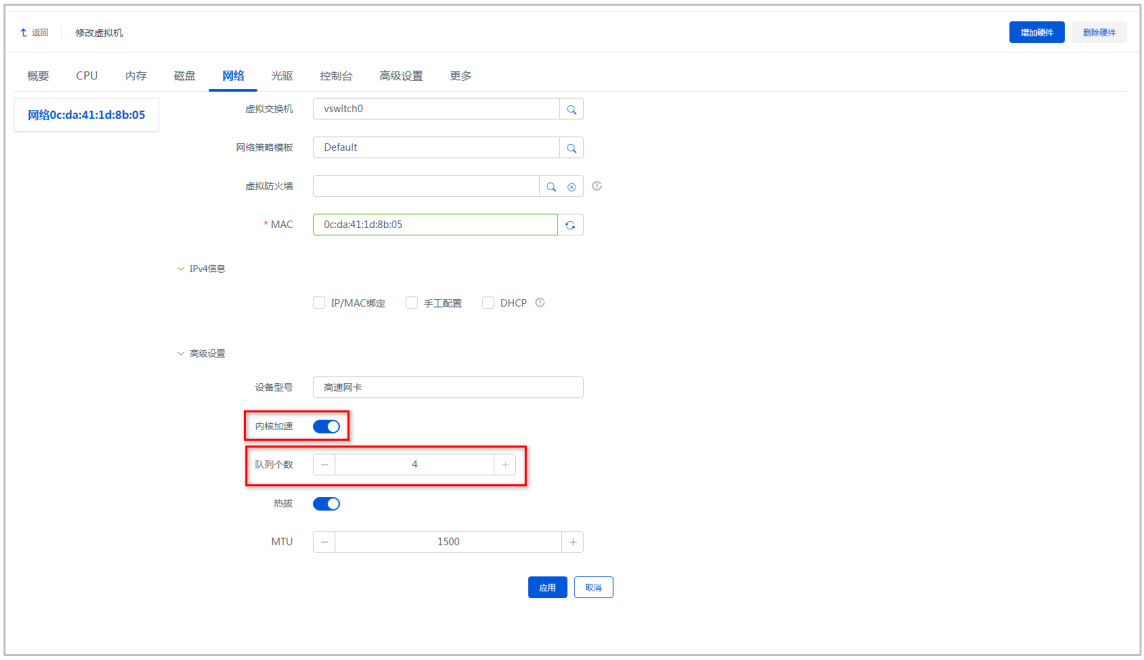
(1) 选择顶部“虚拟机”页签，在虚拟机列表中选择网关虚拟机，进入虚拟机概要页面。

(2) 单击<修改>按钮，单击“网络”页签，在类型为高速网卡的网卡“高级设置”中，启用“内核加速”功能，并设置队列个数与 CPU 个数*CPU 核数相同，单击<应用>按钮，完成内核加速配置。

说明

虚拟机处于关闭状态才可配置内核加速功能。

图6-28 启用内核加速功能



7 辅助功能

7.1 修改网关默认端口

安全网关默认端口为 8860，支持修改网关端口，修改网关端口命令帮助如下：

```
[root@localhost ~]# gateway server --help
Usage: gateway server [OPTIONS]

  Config server attribute

Options:
  -p, --server-port PORT  Set Server Port.
  --help                  Show this message and exit.
```

7.2 启用网关支持SSV

SSV 是 UniCloud Workspace 的用户自助系统，网关默认未开启代理 SSV。

执行 gateway proxy –help 可查看支持的命令，命令帮助如下：

```
[root@localhost ~]# gateway proxy --help
```

```
Usage: gateway proxy [OPTIONS]

  Config proxy service attribute

Options:
  -c, --controller IP             Set controller IP for Gateway to proxy.
  -p, --controller-port PORT      Set controller port for Gateway to proxy.
  -w, --platform-server IP       Set platform-server IP for Gateway to
                                  proxy.
  -s, --platform-server-port PORT
                                  Set platform-server port for Gateway to
                                  proxy.
  -t, --platform-server-http-type TYPE
                                  Set platform-server http-type[http/https]
                                  for Gateway to proxy.
  -i, --idvvoi STATE              Enable IDV/VOI[enable/disable] for Gateway
                                  to proxy.
  -n, --nextcloud STATE           Enable nextcloud[enable/disable] for
                                  Gateway to proxy.
  -y, --nextcloud-http-type TYPE  Set nextcloud http-type[http/https] for
                                  Gateway to proxy.
  -e, --nextcloud-ip IP           Set nextcloud IP for Gateway to proxy.
  -x, --nextcloud-port PORT       Set nextcloud port for Gateway to proxy.
  -v, --ssv STATE                 Enable SSV[enable/disable] for Gateway to
                                  proxy.
  -o, --ssv-port PORT             Set SSV port for Gateway to proxy.
  --help                          Show this message and exit.
```

其中，如下几个参数涉及到 SSV 功能：

- -c, --controller IP ：默认反向代理的 SSV 功能访问的 IP 使用 controller IP，如果设置了 platform-server IP 参数，则以 platform-server IP 为反向代理的 SSV IP。
- -v, --ssv STATE：开启或关闭 SSV 功能。
- -o, --ssv-port PORT：设置 SSV 的端口号，用于对接云上版本。云下版本的 SSV 的端口号默认为 8083，无需修改。云上版本的 SSV 端口号与云下不同，云上版本使用 SSV 时需将端口号修改为 8099。
- -w, --platform-server IP：设置管理平台访问路径，若未设置则默认使用 controller IP，也可根据实际部署环境进行设置。

说明

- 正常情况下，云下管理平台环境开启 ssv 功能只需执行 gateway proxy -v enable 即可。
- 开启后，即可通过 https://网关对外 IP 地址:网关对外端口号/ssv/，访问 ssv 门户网站下载客户端，其中/ssv/最后的/不能省略，需要完整输入。

7.3 配置网关网卡IP

除了在管理平台中的虚拟化页面中配置网关网卡 IP，还支持通过命令行配置网关网卡 IP 地址，命令行帮助如下：

```
[root@localhost nginx]# gateway network --help
Usage: gateway network [OPTIONS] IFACE
  system network control, iface: eth0, eth1
Options:
  -o, --onboot ONBOOT    Set ONBOOT[yes/no] for Interface config file.
  -b, --bootproto PROTO  Set BOOTPROTO[static/dhcp/none] for Interface config
                         file.
  -i, --ipaddr IP        Set IPADDR for Interface config file.
  -n, --netmask NETMASK  Set NETMASK for Interface config file.
  -g, --gateway GATEWAY  Set GATEWAY for Interface config file.
  -d, --dns DNS          Set DNS for Interface config file.
  --help                 Show this message and exit.
```

7.4 开启或关闭系统端口

网关支持通过命令行开启或关闭系统端口，默认网关系统仅开放 8860 端口供访问使用，当需要进行网络故障排查时，可执行如下命令开启系统端口：

```
[root@localhost nginx]# gateway sys-port open     //开启系统端口
```

当完成系统排查后，建议执行如下命令关闭系统端口：

```
[root@localhost nginx]# gateway sys-port close    //关闭系统端口
```

7.5 配置维护用于SSH访问的端口和网卡

网关支持配置用于平时维护用的 ssh 端口和访问网卡，网卡建议指定为内网访问网卡。命令帮助如下：

```
[root@localhost nginx]# gateway ssh-access --help
Usage: gateway ssh-access [OPTIONS] ACTION
  ssh access control, action: open, close
Options:
  -i, --interface INTERFACE  Set interface for ssh access.
  -p, --port PORT            Set port for ssh access.
  --help                     Show this message and exit.
```

如果要配置通过网卡 eth0，端口 12345 以 SSH 方式访问网关，则命令为：

```
[root@localhost nginx]# gateway ssh-access -i eth0 -p 12345 open
```

输入以下命令禁用以 SSH 方式访问网关：

```
[root@localhost nginx]# gateway ssh-access close
```

7.6 启用网关支持IDV/VOI

网关默认未开启代理 IDV/VOI 客户端，开启之后 IDV/VOI 终端可通过网关连接管理平台。

注意

IDV/VOI 终端无法自动发现网关地址，需在 IDV/VOI 终端手动设置网关对外 IP 地址、端口号。

执行 gateway proxy –help 查看支持的命令，命令的帮助如下：

```
[root@localhost ~]# gateway proxy --help
Usage: gateway proxy [OPTIONS]

  Config proxy service attribute

Options:
  -c, --controller IP             Set controller IP for Gateway to proxy.
  -p, --controller-port PORT      Set controller port for Gateway to proxy.
  -w, --platform-server IP       Set platform-server IP for Gateway to
                                  proxy.
  -s, --platform-server-port PORT
                                  Set platform-server port for Gateway to
                                  proxy.
  -t, --platform-server-http-type TYPE
                                  Set platform-server http-type[http/https]
                                  for Gateway to proxy.
  -i, --idvvoi STATE              Enable IDV/VOI[enable/disable] for Gateway
                                  to proxy.
  -n, --nextcloud STATE           Enable nextcloud[enable/disable] for
                                  Gateway to proxy.
  -y, --nextcloud-http-type TYPE  Set nextcloud http-type[http/https] for
                                  Gateway to proxy.
  -e, --nextcloud-ip IP           Set nextcloud IP for Gateway to proxy.
  -x, --nextcloud-port PORT       Set nextcloud port for Gateway to proxy.
  -v, --ssv STATE                 Enable SSV[enable/disable] for Gateway to
                                  proxy.
  -o, --ssv-port PORT             Set SSV port for Gateway to proxy.
  --help                          Show this message and exit.
```

其中，如下参数涉及到网关代理 IDV/VOI 功能：

- -i, --idvvoi STATE：表示是否开启或关闭网关代理 IDV/VOI 功能。默认为关闭。

说明

正常情况下，执行 gateway proxy -i enable 即可开启网关代理 IDV/VOI 功能。

7.7 启用网关云盘代理

网关默认未开启云盘代理，但是可以通过命令开启代理功能。

执行 gateway proxy --help 查看支持的命令，命令的帮助如下：

```
[root@localhost ~]# gateway proxy --help
Usage: gateway proxy [OPTIONS]

  Config proxy service attribute

Options:
  -c, --controller IP             Set controller IP for Gateway to proxy.
  -p, --controller-port PORT      Set controller port for Gateway to proxy.
  -w, --platform-server IP       Set platform-server IP for Gateway to
                                  proxy.
  -s, --platform-server-port PORT
                                  Set platform-server port for Gateway to
                                  proxy.
  -t, --platform-server-http-type TYPE
                                  Set platform-server http-type[http/https]
                                  for Gateway to proxy.
  -i, --idvvoi STATE              Enable IDV/VOI[enable/disable] for Gateway
                                  to proxy.
  -n, --nextcloud STATE           Enable nextcloud[enable/disable] for
                                  Gateway to proxy.
  -y, --nextcloud-http-type TYPE  Set nextcloud http-type[http/https] for
                                  Gateway to proxy.
  -e, --nextcloud-ip IP           Set nextcloud IP for Gateway to proxy.
  -x, --nextcloud-port PORT       Set nextcloud port for Gateway to proxy.
  -v, --ssv STATE                 Enable SSV[enable/disable] for Gateway to
                                  proxy.
  -o, --ssv-port PORT             Set SSV port for Gateway to proxy.
  --help                          Show this message and exit.
```

其中，如下参数涉及到网关云盘代理功能：

- -n, --nextcloud STATE：该参数用于开启或关闭云盘代理功能。
- -y, --nextcloud-http-type TYPE：该参数用于修改反向代理的云盘服务器的访问协议，默认是 http。
- -e, --nextcloud-ip IP：:该参数可以修改反向代理的云盘服务器的 IP，默认使用 controller IP 地址。
- -x, --nextcloud-port PORT：该参数用于修改反向代理的云盘服务器的端口号，默认使用 8888。

说明

- 正常情况下，执行 gateway proxy -n enable 即可开启网关代理云盘功能。
- 开启云盘代理之前要保证已经在相应的管理平台上启用云盘功能，否则开启代理由于后台服务本身未启动也会无法正常使用。

7.8 启用网关VNC代理

配置完成后，管理平台支持对通过网关接入的 IDV、VOI 终端进行远程协助。

执行 gateway proxy –-help 查看支持的命令，命令的帮助如下：

```
[root@localhost ~]# gateway vnc --help
Usage: gateway vnc [OPTIONS] ACTION

  Config vnc proxy service attribute, action:enable,disable or status

Options:
  -p, --vnc-port PORT             Set Port for VNC proxy service.
  -a, --vnc-access-ip IP          Set IP for browser to access.
  --help                          Show this message and exit.
```

其中，如下参数涉及到开启 VNC 代理功能：

- --vnc-port PORT：网关上提供 VNC 代理服务的端口，若存在 NAT 设置，则需要将其通过 NAT 设备映射到公网。
- -a, --vnc-access-ip IP：网关上能够与管理平台互通的 IP 地址，用于在管理平台使用远程协助功能访问 IDV、VOI 终端。

7.9 配置网关代理协议

网关默认代理协议为 http，但是可以通过命令切换为 https。

执行 gateway proxy --help 查看支持的命令，命令的帮助如下：

```
[root@localhost ~]# gateway proxy --help
Usage: gateway proxy [OPTIONS]

  Config proxy service attribute

Options:
  -c, --controller IP             Set controller IP for Gateway to proxy.
  -p, --controller-port PORT      Set controller port for Gateway to proxy.
  -w, --platform-server IP       Set platform-server IP for Gateway to
                                  proxy.
  -s, --platform-server-port PORT
                                  Set platform-server port for Gateway to
                                  proxy.
  -t, --platform-server-http-type TYPE
                                  Set platform-server http-type[http/https]
                                  for Gateway to proxy.
  -i, --idvvoi STATE              Enable IDV/VOI[enable/disable] for Gateway
                                  to proxy.
  -n, --nextcloud STATE           Enable nextcloud[enable/disable] for
                                  Gateway to proxy.
  -y, --nextcloud-http-type TYPE  Set nextcloud http-type[http/https] for
                                  Gateway to proxy.
  -e, --nextcloud-ip IP           Set nextcloud IP for Gateway to proxy.
```

```
  -x, --nextcloud-port PORT       Set nextcloud port for Gateway to proxy.
  -v, --ssv STATE                 Enable SSV[enable/disable] for Gateway to
                                  proxy.
  -o, --ssv-port PORT             Set SSV port for Gateway to proxy.
  --help                          Show this message and exit.
```

其中，如下参数涉及到网关代理协议 http 功能：

- -s, --platform-server-port PORT：该参数用于设置网关代理到管理平台的端口，管理平台协议为 http 时，端口为 8083；管理平台协议为 https 时，端口为 8480。
- -t, --platform-server-http-type TYPE：设置网关代理到管平台的访问协议，可设置为 http 或 https，默认为 http。

 注意

当管理平台的访问协议切换为 https，安全网关代理协议也需同步切换为 https。

输入以下命令设置网关代理协议为 https：

```
[root@localhost ~]# gateway proxy –t https –s 8480
```

7.10 启用UDP协议

安全网关支持启用 UDP 协议，通过 UDP 协议可以提升广域网或者弱网环境下的用户体验。启用 UDP 命令帮助如下：

```
[root@localhost udplib]# gateway udp --help
Usage: gateway udp [OPTIONS] ACTION

  UDP control, action: enable or disable.

Options:
  --help  Show this message and exit.
```

即执行 gateway udp enable 即可启用 UDP 协议，UDP 端口跟 TCP 端口相同，默认也是 8860,TCP 端口修改后 UDP 端口也会同步修改，修改端口命令为 gateway server -p 命令。

7.11 启用VDP服务代理

如果需要安全网关代理虚拟应用和共享桌面，则需要在安全网关上启用 VDP 服务代理。启用 VDP 服务代理命令帮助如下：

```
[root@localhost ~]# gateway vdp-service --help
Usage: gateway vdp-service [OPTIONS] ACTION

  Config VDP service gateway attribute, action: enable, disable or status
```

```
Options:
  -p, --vdp-service-port PORT     Set Port for VDP service Gateway.
  -h, --vdp-service_hosts IP:PORT
                                  Set Hosts for VDP service Gateway to proxy.
                                  The setting form is IP1:Port1,IP2:Port2 or
                                  any, any will allowed to connect to any
                                  hosts(insecure)
  --help                          Show this message and exit.
```

- -p, --vdp-service-port PORT：(可选)如果公网仅支持映射安全网关上的一个端口出去，则本参数可以不配置，不配置情况下跟安全网关连接云桌面的端口复用，即虚拟应用和共享桌面默认也走 8860 端口。如果手动配置该端口，则即可以通过配置的独立端口访问虚拟应用和共享桌面，也可以跟连接云桌面的端口复用。端口复用的优点是对公网仅需要暴露一个端口，缺点是同样连接数量，CPU 占用会更高。
- -h, --vdp-service_hosts IP:PORT：(必选)配置安全网关代理的虚拟应用和共享桌面服务器的 IP 和端口。格式为 IP1:Port1,IP2:Port2,如 192.168.1.2:3389,192.168.1.3:3389，表示 192.168.1.2 和 192.168.1.4 两台是提供虚拟应用或者共享桌面的服务器，也可以设置为 any，此时表示安全网关可以代理任意的虚拟应用或者共享桌面服务器。

7.12 启用网关报表服务代理

网关默认未开启报表服务代理，可以通过命令开启并自定义服务端口。

执行 gateway log-monitor --help 命令以查看支持的命令：

```
[root@localhost ~]# gateway log-monitor --help
Usage: gateway log-monitor [OPTIONS] ACTION

  Config log monitor proxy attribute, action: enable or disable

Options:
  -p, --log-monitor-port PORT     Set Port for log monitor service.
  -r, --log-monitor-server IP     Set log monitor server for VDI Gateway to proxy.
  -s, --log-monitor-server-port PORT   Set log monitor server Port for VDI Gateway to proxy.
  --help                          Show this message and exit.
```

- -p,--log-monitor-port PORT：网关上提供报表服务的端口，若存在 NAT 设置，则需要将其通过 NAT 设备映射到公网。
- -r,--log-monitor-server IP：报表服务器的 IP 地址。
- -s,--log-monitor-server-port PORT：报表服务器提供服务的端口。

若报表服务器 IP 为 1.1.1.1，网关与报表服务器提供服务端口均为 8702，则开启配置网关报表服务命令示例为：

```
gateway log-monitor -p 8702 -r 1.1.1.1 -s 8702 enable
```

8 网关升级

当管理平台完成升级之后，必须将安全网关也升级到对应的版本。

注意

- 进行网关升级操作之前，请确保升级网关上没有承载云桌面连接，网关升级过程中会重启相关服务，可能会导致网关上的云桌面连接中断。
- 如果是从 E1011L06 之前版本升级到新版本，升级成功后，需要重启安全网关所在的虚拟机或服务器。

安全网关升级操作步骤如下：

(1) 登录网关虚拟机后台，并上传网关安装包（安装包名称为 UniCloud_Workspace_Gateway_Solution-version.tar.gz）到虚拟机后台。

(2) 执行如下命令解压安装包并切换至解压后的目录。此处，*version* 表示版本号。

```
[root@localhost ~]# tar -xvf UniCloud_Workspace_Gateway_Solution-version.tar.gz
[root@localhost ~]# cd UniCloud_Workspace_Gateway_Solution-version
```

(3) 执行升级脚本升级网关。

```
[root@localhost ~]# ./install.sh –u
```

(4) 查看网关版本，确认升级结果。

```
[root@localhost ~]# gateway --version
```

说明

- 网关升级完成后，原有的网关功能配置不会发生变化，如需启用新功能或变更网关配置，请按需执行配置命令。
- 登录虚拟机后台可采用以下任意一种方式：1、通过虚拟机控制台进入后台；2、通过 SSH 登录，登录前需开启指定端口，详细步骤可参考 7.5 章节；3、开启所有端口，详细步骤可参考 7.4 章节。

9 网关卸载

如需卸载网关虚拟机上安装的网关，请通过以下方法卸载：

(1) 在解压后的安装包路径 UniCloud_Workspace_Gateway_Solution-*version* 中，执行./install.sh –r 命令完成网关卸载。

(2) 也可在路径/var/lib/vdigateway/中，执行./install.sh –r 命令完成网关卸载。