CentOS 7系统 模板封装教程

产品版本：ZStack 3.10.0

文档版本：V3.10.0

ZStack

版权声明

商标说明

ZStack商标和其他云轴科技商标均为上海云轴信息科技有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

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

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

目录

1 环境准备

1.1 准备软件工具

准备软件工具：

- **可用的ZStack云平台**：

  请在官网获取最新版本

- **CentOS镜像**：

  请在CentOS官网自行获取CentOS 7镜像，并遵守相关授权许可。本文档参考版本为：*CentOS-7-x86_64-DVD-1804.iso*

2 准备安装镜像

2.1 添加安装镜像

背景信息

将CentOS 7添加到ZStack的镜像列表，为安装操作系统使用。

操作步骤

1. 在ZStack私有云主菜单，点击**云资源池** > **镜像**按钮。
2. 在**镜像**页面，点击**添加镜像**按钮。
3. 在弹出的**添加镜像**界面，可参考以下示例输入相应内容：

    - **名称**：设置镜像名称
    - **简介**：可选项，可留空不填
    - **镜像类型**：选择系统镜像
    - **镜像格式**：选择ISO
    - **平台**：选择Linux平台
    - **镜像服务器**：选择已创建的镜像服务器
    - **镜像路径**：选择并填写添加镜像的URL路径或本地文件路径

        注:

        - URL路径支持**HTTP/HTTPS** 、**ftp**、**sftp**和**file:///**格式，其中*file:///*格式目前仅支持Sftp镜像服务器和镜像仓库。
        - 本地文件，表示选择当前浏览器可访问的镜像直接上传，支持镜像仓库。
    - **BIOS模式**：选择BIOS模式，默认为Legacy。包括：Legacy和UEFI

        注: 模式不匹配可能导致云主机无法正常工作，请谨慎选择。

        - 使用该镜像创建的云主机将使用所选的BIOS模式启动。
        - 镜像详情页和云主机详情页支持修改BIOS模式。
        - 对于使用UEFI引导模式的CentOS 7.4及以上版本Linux类型镜像，创建的云主机重启可能进入UEFI Shell，请参考以下方法，成功启动并进入操作系统：
            - 方法一：添加脚本自动跳过UEFI Shell，直接进入操作系统。

在安装好的操作系统中，执行vim /boot/efi/startup.nsh命令，创建脚本并保存以下内容，后续重启云主机将跳过UEFI Shell，直接进入操作系统：

```
FS0:
CD EFI
CD centos
shimx64-centos.efi
```

- 方法二：手动退出UEFI Shell。

  若已经进入UEFI Shell，可手动执行以下命令，退出UEFI Shell：

```
Shell> fs0:
FS0:\> cd EFI
FS0:\EFI\> cd centos
FS0:\EFI\centos\> shimx64-centos.efi
```

- **已安装Qemu guest agent**：

  注:

  - 请务必确保被导入的镜像已安装Qemu guest agent，并已设置为自启动。
  - 满足以上条件后，勾选**Qemu guest agent**选项，则由添加的镜像创建出来的云主机，以及该云主机克隆生成的云主机或创建的镜像，可在运行状态下从外部修改云主机密码。

如图 *1:* 添加镜像所示，点击**确定**，完成Linux镜像添加。

图 1: 添加镜像


确定
取消
添加镜像
名称 *
CentOS 7
简介
镜像类型 *
系统镜像
云盘镜像
镜像格式 *
iso
平台 *
Linux
镜像服务器 *
BS-1
镜像路径 *
URL
本地文件
https://mirrors.aliyun.com/centos/7/isos/x86_64/Cen
BIOS模式 *
Legacy
请谨慎选择，模式不匹配可能导致云主机无法正常工作
已安装 Qemu guest agent

2.2 新建云盘规格

背景信息

根据需求创建合适的云盘规格大小，用于CentOS 7云主机系统硬盘。

- 若安装CentOS 7命令行界面，推荐设定40GB的云盘规格；
- 若安装CentOS 7图形界面（GNOME），推荐设定60GB的云盘规格。

操作步骤

1. 在ZStack私有云主菜单，点击**云资源池** > **云盘规格**按钮。
2. 在**云盘规格**页面，点击**创建云盘规格**按钮。
3. 在弹出的**创建云盘规格**界面，可参考以下示例输入相应内容：
   - **名称**：填写云盘规格的名称
   - **简介**：可选项，可留空不填
   - **容量**：选择或填写云盘容量，例如：40G
   - **磁盘带宽**：可选项，可留空不填

   如图 *2:* 创建云盘规格所示：

   图 2: 创建云盘规格

4. 点击**确定**，完成云盘规格创建。

3 安装操作系统

3.1 安装云主机镜像-CentOS 7

操作步骤

1. 新建云主机

   在ZStack私有云主菜单，点击**云资源池** > **云主机**，进入**云主机**界面，点击**创建云主机**，在弹出的**创建云主机**页面中，可参考以下示例输入相应内容：

   - **添加方式**：选择添加云主机的方式
   - **名称**：设置云主机的名称
   - **简介**：可选项，可留空不填
   - **计算规格**：选择适合的计算规格
   - **根云盘规格**：选择合适的根云盘规格
   - **镜像**：选择云主机的镜像
   - **网络**：选择创建云主机的三层网络

   如图 *3: 新建CentOS 7云主机*所示，点击**确定**按钮，完成CentOS 7云主机创建，系统会自动进入安装引导模式。

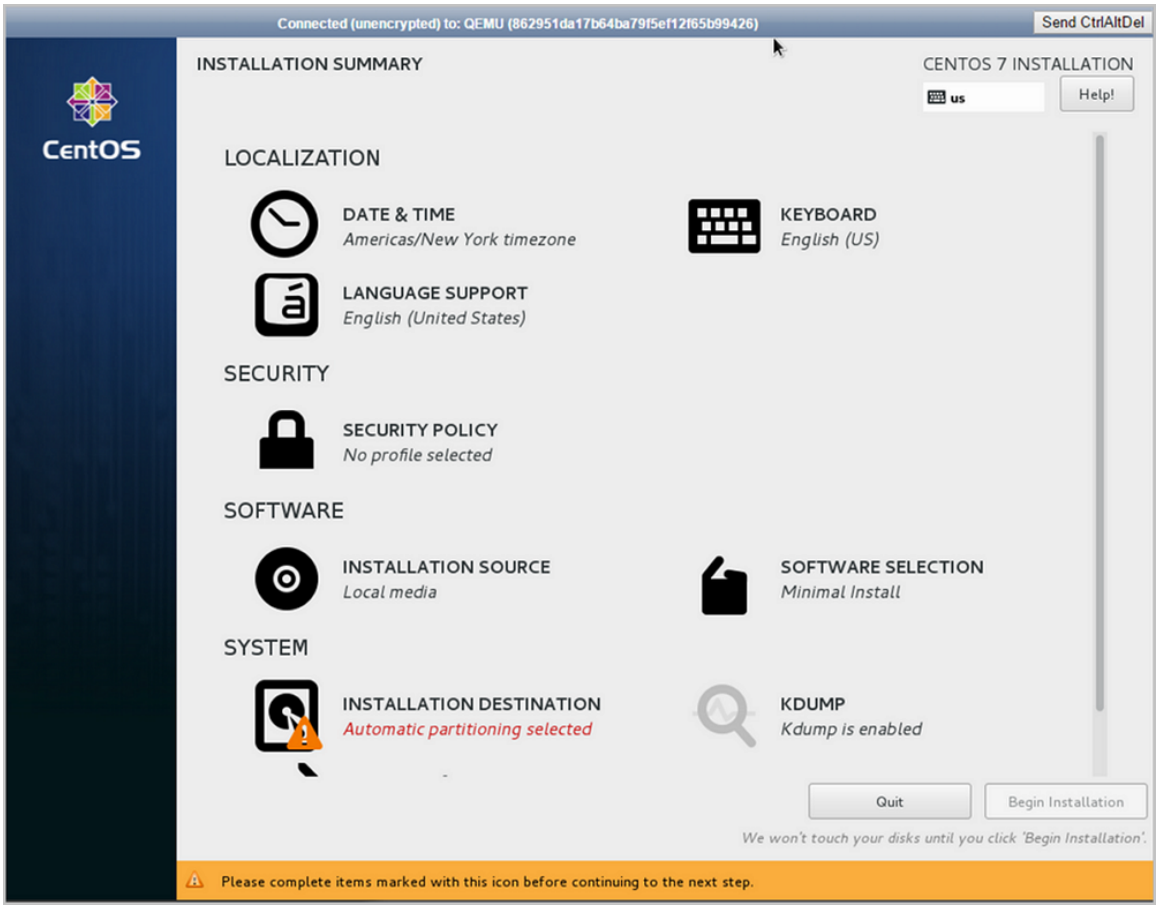
   图 3: 新建CentOS 7云主机

2. 安装CentOS 7镜像

a) 进入控制台

在**云主机**界面选中云主机名称，点击**更多操作** > **打开控制台**按钮，进入控制台系统会进行初始化，完成后显示云主机镜像安装界面，如图 *4:* 安装界面所示：

图 4: 安装界面



注:

- 除磁盘分区有叹号标志外，此页面所有配置已做默认设置，可根据自己使用习惯进行设置。
- 对于使用UEFI引导模式的CentOS 7.4及以上版本Linux类型镜像，创建的云主机重启可能进入UEFI Shell，请参考以下方法，成功启动并进入操作系统：
  - 方法一：添加脚本自动跳过UEFI Shell，直接进入操作系统。

    在安装好的操作系统中，执行vim /boot/efi/startup.nsh命令，创建脚本并保存以下内容，后续重启云主机将跳过UEFI Shell，直接进入操作系统：

    ```
    FS0:
    CD EFI
    CD centos
    ```

```
shimx64-centos.efi
```

- 方法二：手动退出UEFI Shell。

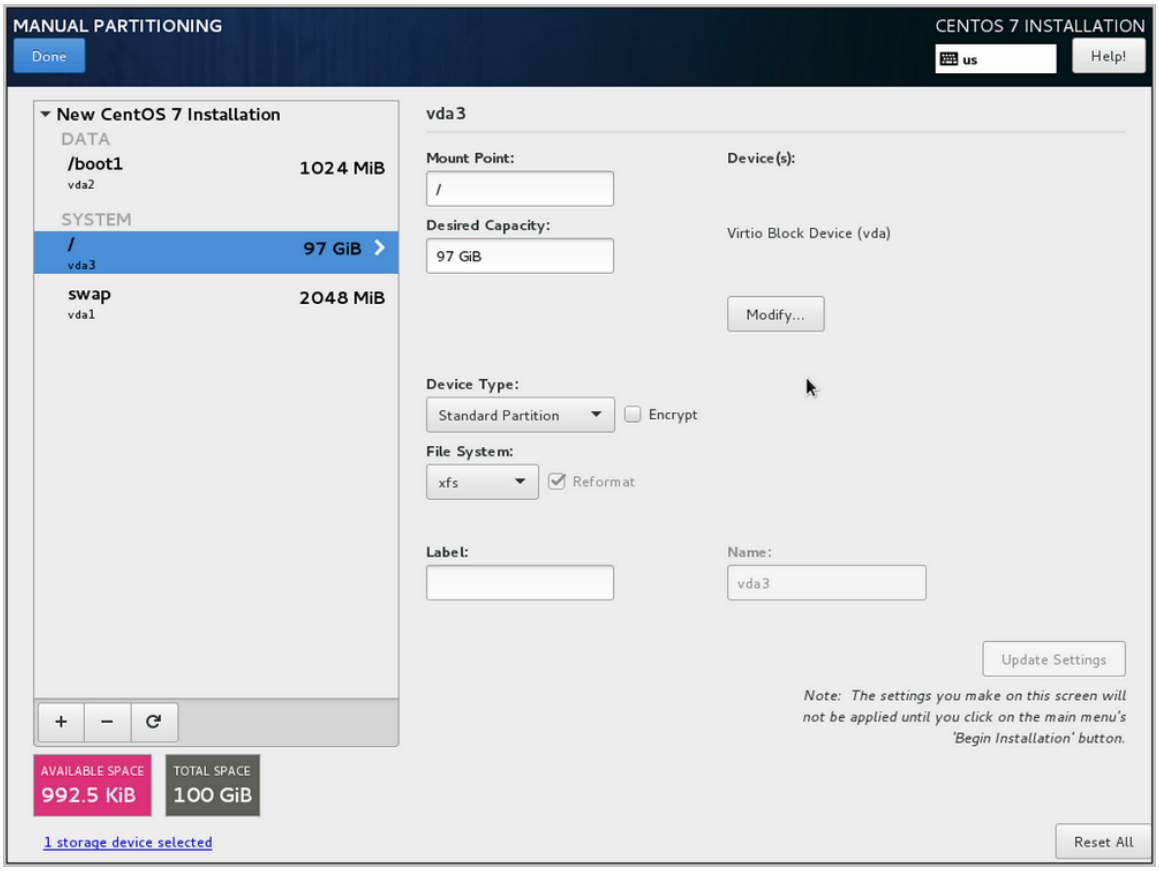
  若已经进入UEFI Shell，可手动执行以下命令，退出UEFI Shell：

```
Shell> fs0:
FS0:\> cd EFI
FS0:\EFI\> cd centos
FS0:\EFI\centos\> shimx64-centos.efi
```

b) （可选）磁盘分区环节

点击**INSTALLATION DESTINATION**按钮进入**磁盘分区**页面，默认磁盘不进行分区，如果用户需要根据自己的使用习惯对磁盘进行分区，建议*/boot1*分配1G，*swap*分配2GB，剩下可以分配给根分区，如图 *5:* 分区界面所示：

图 5: 分区界面

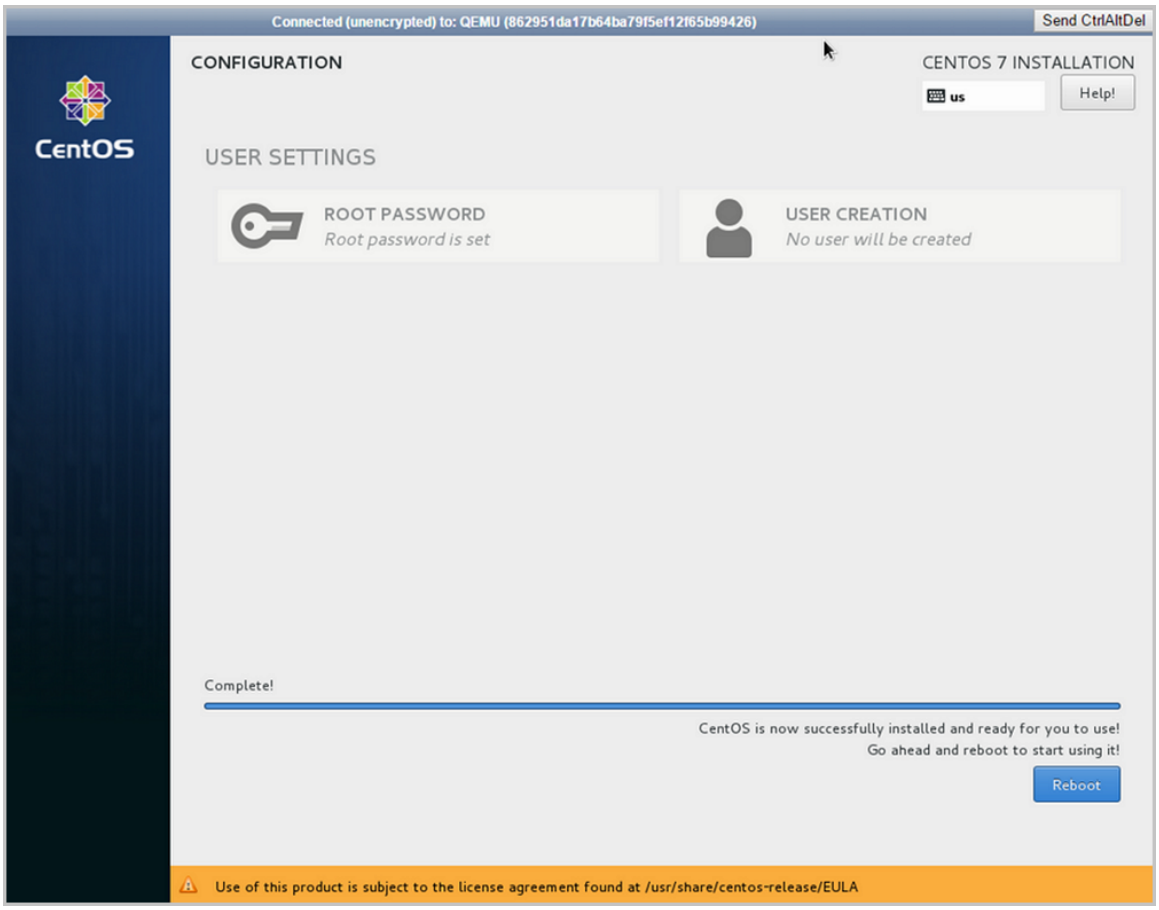


c) 安装系统

设置完成后，点击右下角**Begin Installation**按钮，进入安装图形界面。如图 *6:* 安装界面所示：

注: 在安装界面中，用户可以设置root用户密码和创建用户。

图 6: 安装界面



安装完成后，点击右下角**Reboot**按钮重启，完成系统安装。

3.2 系统模板配置

操作步骤

1. 指定hostname

   在CentOS 7中，执行命令hostnamectl set-hostname localhost.domain.com，指定hostname名称为**localhost**，立即生效。

2. （可选）安装cloud-init

   为了保证使用封装镜像新创建云主机时支持User Data或SSH公钥等自定义配置功能，需要在封装镜像前安装cloud-init。推荐cloud-init版本为：0.7.9、17.1、19.4及以后版本，请按需选择并自行安装。

注: 安装cloud-init需注意以下情况：

- 请安装推荐版本cloud-init，否则可能导致User Data或SSH公钥功能不可用。
- 安装cloud-init前，需重启云主机。
- 安装cloud-init后，ssh密码认证默认关闭，若需要开启，需将配置文件*/etc/cloud/cloud.cfg*中参数**ssh_pwauth**的值设置为1。

3. 配置网络

   参考以下配置修改相应文件，以避免云主机开机后，无法自动获取IP地址。

   将*/etc/sysconfig/network-scripts/ifcfg-eth0*文件修改为以下内容。删除相关UUID的指定信息。

```
[root@localhost ~]# cat /etc/sysconfig/network-scripts/ifcfg-eth0
DEVICE=eth0
TYPE=Ethernet
ONBOOT=yes
BOOTPROTO=dhcp
NAME=eth0
```

4. 安装Qemu Guest Agent

   a) 使用命令yum install qemu-guest-agent -y安装qga。

   b) 使用命令systemctl enable qemu-guest-agent设置开机启动。

   c) 使用*getenforce*命令检查SELINUX状态，如果返回**Enforcing**，则执行vi /etc/selinux/config命令修改SELINUX状态为**disabled**，保存并退出。

5. （可选）安装agent

   1. 在云主机详情页安装性能优化工具。
   2. 进入云主机控制台，输入以下命令执行安装，具体可参考用户手册*agent安装*章节。

```
/bin/bash -c "$(curl -s -S http://169.254.169.254/vm-tools.sh)"
```

6. （可选）关闭漏洞补丁

   针对CentOS 7.5或CentOS 7.6版本，关闭幽灵漏洞补丁和熔断漏洞补丁，能有效提升云主机性能。可参考以下步骤进行操作：

   1. 查看漏洞补丁是否打开

      执行grep . /sys/devices/system/cpu/vulnerabilities/*命令，通过查看/sys的方法检测漏洞补丁是否打开，例如：

```
# grep . /sys/devices/system/cpu/vulnerabilities/*
/sys/devices/system/cpu/vulnerabilities/l1tf:Not affected
/sys/devices/system/cpu/vulnerabilities/meltdown:Not affected
```

```
/sys/devices/system/cpu/vulnerabilities/spec_store_bypass:Mitigation: Speculative
 Store Bypass disabled via prctl and seccomp
/sys/devices/system/cpu/vulnerabilities/spectre_v1:Mitigation: Load fences, __user
 pointer sanitization
/sys/devices/system/cpu/vulnerabilities/spectre_v2:Mitigation: Enhanced IBRS
```

根据最后一条返回结果进行判断，状态显示为**Mitigation**表示漏洞补丁已开启，显示为**vulnerable**表示漏洞补丁已关闭。

2. 查看漏洞修复方式

   若漏洞补丁已开启，再根据上步骤最后一条返回结果进行判断，修复方式包括Retpoline without IBPB和Enhanced IBRS两种。

   - Retpoline without IBPB：此修复方式对系统性能影响较小，关闭或不关闭漏洞补丁均可，请按需选择。
   - Enhanced IBRS：此修复方式对系统性能影响较大，推荐关闭幽灵补丁漏洞，可有效提升云主机性能（实测可提升30%左右）。

3. 关闭漏洞补丁

   可参考以下步骤关闭漏洞补丁：

   1. 在*/etc/default/grub*文件为**GRUB_CMDLINE_LINUX**参数添加值*noibrs noibpb nopti spectre_v2=off nospectre_v1 l1tf=off nospec_store_bypass_disable no_stf_barrier mds=off mitigations=off*。
   2. 执行 grub2-mkconfig > /boot/grub2/grub.cfg命令应用配置。
   3. 重启云主机，配置生效。

   参考示例如下：

```
[root@10-0-5-87 ~]# cat /etc/default/grub      #查看/etc/default/grub文件配置，实际请按要求添加配置
GRUB_TIMEOUT=5
GRUB_DISTRIBUTOR="$(sed 's, release .*$,,g' /etc/system-release)"
GRUB_DEFAULT=saved
GRUB_DISABLE_SUBMENU=true
GRUB_TERMINAL_OUTPUT="console"
GRUB_CMDLINE_LINUX="crashkernel=auto rd.lvm.lv=zstack/root rd.lvm.lv=zstack
/swap rhgb quiet noibrs noibpb nopti spectre_v2=off nospectre_v1 l1tf=off nospec_
store_bypass_disable
       no_stf_barrier mds=off mitigations=off"
GRUB_DISABLE_RECOVERY="true"
[root@10-0-5-87 ~]# grub2-mkconfig > /boot/grub2/grub.cfg     #应用配置
```

```
[root@10-0-5-87 ~]# reboot    #重启云主机，配置生效
```

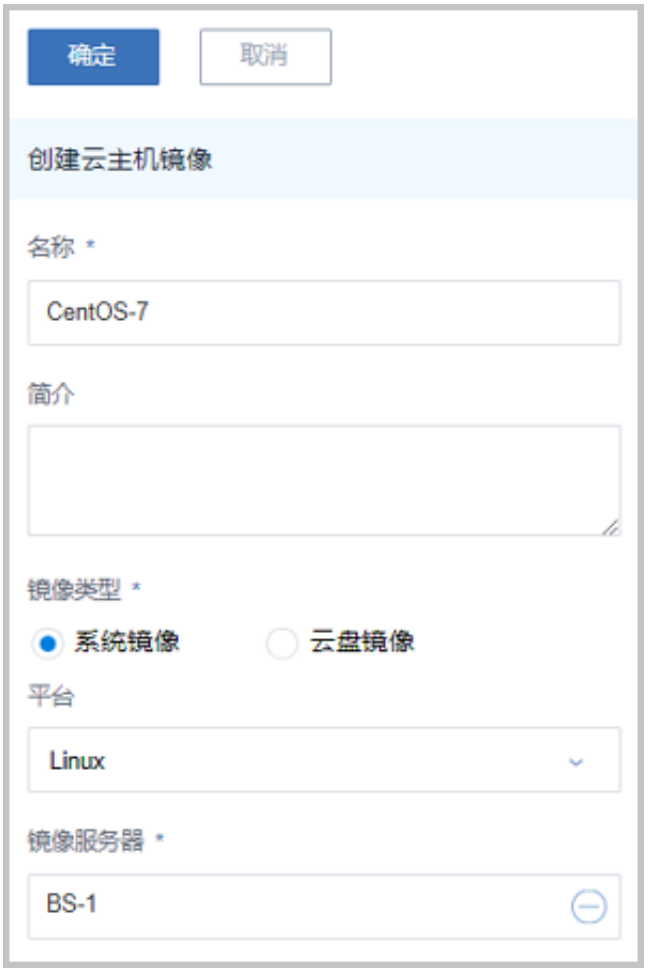
3.3 创建系统模板

操作步骤

1. 在**云主机**界面，点击**更多操作** > **创建云主机镜像**按钮。
2. 在**创建云主机镜像**界面，参考以下示例输入相应内容：
   - **名称**：填写创建镜像的名称
   - **简介**：可选项，可留空不填
   - **平台**：安装镜像的平台，选择Linux
   - **镜像服务器**：选择已创建的镜像服务器

   如图 7: 创建云主机镜像界面所示：

图 7: 创建云主机镜像界面



注:

- 在线创建云主机镜像：使用ImageStore或Ceph类型的镜像服务器，支持在线创建云主机镜像。
- 关机创建云主机镜像：使用ImageStore、Sftp或Ceph类型的镜像服务器，支持关机创建云主机镜像。
- 使用Linux操作系统的云主机创建云主机镜像时，请勿在*/etc/fstab*文件中写入数据云盘信息，否则使用该镜像创建的云主机无法启动。

3. 点击**确定**按钮，完成镜像创建。
4. 导出镜像

创建镜像完成后，可以拷贝云主机镜像进行再次定制，不同类型镜像服务器的导出方法不同，如下所示：

- 镜像服务器采用ImageStore类型

在**镜像**页面点击**更多操作** > **导出**按钮，可导出需要的镜像，如图 *8:* 镜像导出所示：

图 8: 镜像导出

镜像生成后，可以在**基本属性**页面复制已导出的镜像URL下载镜像。如图 *9:* 拷贝镜像路径界面所示：

图 9: 拷贝镜像路径界面

- 镜像服务器采用Ceph块存储类型

  在**基本属性**页面复制**镜像服务器路径**会显示Ceph中对应的pool和image信息，拷贝此镜像路径后，需要在Ceph服务器上执行*rbd*命令将Ceph镜像导出。

  假设镜像存储路径为*ceph#//bak-t-c9923f982/61ece0adc72*操作如下：

```
[root@ceph-node1 ~]#rbd export bak-t-c9923f982/61ece0adc72 /root/export-test.image
#bak-t-c9923f982表示镜像所在的pool的名字
#61ece0adc72表示镜像的名字
#/root/export-test.image表示导出的目标文件名字
```

至此，基于CentOS系统模板封装操作全部完成。用户可以使用此镜像创建更多的CentOS云主机。

后续操作

云主机在线创建镜像时需注意：

如果加载数据云盘后修改云主机的*/etc/fstab*文件，对该云主机在线创建镜像，使用该镜像创建其它云主机时，由于fstab文件没有相应的挂载信息，再创建的云主机会hang住无法启动。

- Linux云主机加载云盘后不建议通过修改*/etc/fstab*文件方式挂载。
- 推荐的做法：

  进入*/etc/rc.d/rc.local*执行*mount*命令来挂载云盘：

```
# chmod +x /etc/rc.d/rc.local
```

```
# mount -U 文件系统UUID 目标挂载路径
```

注: 建议使用云盘的ID来挂载而非*/dev/vdb*类似的盘符来挂载。

术语表

区域（Zone）

ZStack中最大的一个资源定义，包括集群、二层网络、主存储等资源。

集群（Cluster）

一个集群是类似物理主机（Host）组成的逻辑组。在同一个集群中的物理主机必须安装相同的操作系统（虚拟机管理程序，Hypervisor），拥有相同的二层网络连接，可以访问相同的主存储。在实际的数据中心，一个集群通常对应一个机架（Rack）。

管理节点（Management Node）

安装系统的物理主机，提供UI管理、云平台部署功能。

计算节点（Compute Node）

也称之为物理主机（或物理机），为云主机实例提供计算、网络、存储等资源的物理主机。

主存储（Primary Storage）

用于存储云主机磁盘文件的存储服务器。支持本地存储、NFS、 Ceph、Shared Mount Point、Shared Block类型。

镜像服务器（Backup Storage）

也称之为备份存储服务器，主要用于保存镜像模板文件。建议单独部署镜像服务器。支持ImageStore、Sftp（社区版）、Ceph类型。

镜像仓库（Image Store）

镜像服务器的一种类型，可以为正在运行的云主机快速创建镜像，高效管理云主机镜像的版本变迁以及发布，实现快速上传、下载镜像，镜像快照，以及导出镜像的操作。

云主机（VM Instance）

运行在物理机上的虚拟机实例，具有独立的IP地址，可以访问公共网络，运行应用服务。

镜像（Image）

云主机或云盘使用的镜像模板文件，镜像模板包括系统云盘镜像和数据云盘镜像。

云盘（Volume）

云主机的数据盘，给云主机提供额外的存储空间，共享云盘可挂载到一个或多个云主机共同使用。

计算规格（Instance Offering）

启动云主机涉及到的CPU数量、内存、网络设置等规格定义。

云盘规格（Disk Offering）

创建云盘容量大小的规格定义。

二层网络（L2 Network）

二层网络对应于一个二层广播域，进行二层相关的隔离。一般用物理网络的设备名称标识。

三层网络（L3 Network）

云主机使用的网络配置，包括IP地址范围、网关、DNS等。

公有网络（Public Network）

由因特网信息中心分配的公有IP地址或者可以连接到外部互联网的IP地址。

私有网络（Private Network）

云主机连接和使用的内部网络。

L2NoVlanNetwork

物理主机的网络连接不采用Vlan设置。

L2VlanNetwork

物理主机节点的网络连接采用Vlan设置，Vlan需要在交换机端提前进行设置。

VXLAN网络池（VXLAN Network Pool）

VXLAN网络中的 Underlay 网络，一个 VXLAN 网络池可以创建多个 VXLAN Overlay 网络（即 VXLAN 网络），这些 Overlay 网络运行在同一组 Underlay 网络设施上。

VXLAN网络（VXLAN）

使用 VXLAN 协议封装的二层网络，单个 VXLAN 网络需从属于一个大的 VXLAN 网络池，不同 VXLAN 网络间相互二层隔离。

云路由（vRouter）

云路由通过定制的Linux云主机来实现的多种网络服务。

安全组（Security Group）

针对云主机进行第三层网络的防火墙控制，对IP地址、网络包类型或网络包流向等可以设置不同的安全规则。

弹性IP（EIP）

公有网络接入到私有网络的IP地址。

快照（Snapshot）

某一时间点某一磁盘的数据状态文件。包括手动快照和自动快照两种类型。