ZStack 技术白皮书精选

ZStack 云平台应用堡垒机教程

扫一扫二维码，获取更多技术干货吧

版权声明

摘要

大道至简·极速部署，ZStack 致力于产品化私有云和混合云。

ZStack 是新一代创新开源的云计算 IaaS 软件，由英特尔、微软、CloudStack 等世界上最早一批虚拟化工程师创建，拥有 KVM、Xen、Hyper-V 等成熟的技术背景。

ZStack 创新提出了云计算 4S 理念，即 Simple (简单)、Strong (健壮)、Smart (智能)、Scalable (弹性)，通过全异步架构，无状态服务架构，无锁架构等核心技术，完美解决云计算执行效率低，系统不稳定，不能支撑高并发等问题，实现 HA 和轻量化管理。

ZStack 发起并维护着国内最大的自主开源 IaaS 社区——zstack.io，吸引了 6000 多名社区用户，对外公开的 API 超过 1000 个。基于这 1000 多个 API，用户可以自由组装出自己的私有云、混合云，甚至利用 ZStack 搭建公有云对外提供服务。

ZStack 拥有充足的知识产权储备，积极申报多项软著和专利，参与业内标准、白皮书的撰写，入选云计算行业方案目录，还通过了工信部云服务能力认证和信通院可信云认证。ZStack 面向企业用户提供基于 IaaS 的私有云和混合云，是业内唯一一家实现产品化，并领先业内首家推出同时打通数据面和控制面无缝混合云的云服务商。选择 ZStack，用户可以官网直接下载、1 台 PC 也可上云、30 分钟完成从裸机的安装部署。

目前已有 1000 多家企业用户选择了 ZStack 云平台。

主题：ZSTACK 云平台应用堡垒机教程

1. 目的

1.1 堡垒机支持统一账户管理策略，能够实现对所有远程服务器等账号进行集中管理，完成对账号整个生命周期的监控；还支持对不同用户进行不同策略的制定，细粒度的访问控制能够严防非法、越权访问事件的发生，最大限度保护用户资源的安全。

1.2 同时堡垒机也能解决一些安全上的不稳定因素，堡垒机执行的任务对于整个网络安全系统至关重要。由于堡垒机完全暴露在外网安全威胁之下，需要做许多工作来设计和配置堡垒机，使它遭到外网攻击成功的可能性减至最低。甚至，一些网络管理员会用堡垒机做牺牲品来换取网络的安全。这些堡垒机吸引入侵者的注意力，消耗攻击真正网络主机的时间并且使追踪入侵企图变得更加容易。

1.3 堡垒机在企业网络管理中充当着门卫的重要职责，所有内外部对网络设备及服务器的请求，都要通过堡垒机。因此，堡垒机能够拦截非法访问和恶意攻击，对不合法命令进行阻断、过滤掉所有对目标设备的非法访问行为。总之，堡垒机能够最大的保护企业内部网络设备及服务器资源的安全性，使得企业内部网络管理合理化和专业化。

1.4 本文档旨在提供 ZStack 云平台很多用户通过堡垒机对部署在 ZStack 平台的应用系统进行日常维护，并进行集中式的管理，从而无需管理运维人员逐一进行相关运维，只需通过一台或者多台堡垒机即可运营整个服务架构中的主机，同时也为管理私有网络的服务器提供便利，最小化应用系统的安全风险，从而有利于提升整体架构的安全，并结合这些场景和安全因素考虑，写下关于 ZStack 云平台应用部署 Linux 堡垒机的教程。

2. ZStack 云平台方案

2.1 准备软件

1. 进行部署之前，需提前下载云平台所需的系统 ISO、部署安装包。

2. 以 ZStack 3.7.1 版本为例，可在官网下载相关资源。

http://cdn.zstack.io/product_downloads/iso/ZStack/3.7.1/7948o1y5rx/ZStack-x86_64-DVD-3.7.1-c74.iso

注意：下载 ISO 请下载与当前云平台适配的 ISO 版本，例如，当前云平台采用 C74 版本，请下载 C74 版本的 ISO。

注：下载完毕，请在管理节点检查 md5 值与网站标识的是否一致，如不一致，请重新下载。

校验 md5 的检测方法参考：

```
#md5sum ZStack-x86_64-DVD-3.7.1-c74.iso
```

2.2 总体规划

2.2.1 网络规划介绍

对于网络规划通常需要划分为若干个子网，分为公有网络和私有网络。公有网络中的云主机可以直接从 Internet 中接收入站数据流，也可以直接向 Internet 发送出站数据流，而私有网络中的云主机则不可。但是私有网络中的云主机可以使用位于公有网络中的网络地址转换（NAT）网关访问 Internet。

根据以上描述不同子网的特点，我们需要把堡垒机放置在公有子网中，也就是绑定弹性公网 IP，以便接受管理人员通过 Internet 的访问，受管理的服务器根据其在业务系统中充当的角色选择放置在公有网络或着私有网络中。在实际生产环境中根据需要可为堡垒机设置一个独立的公有地址。

2.2.2 实验环境介绍

1. PC 为本机，能连通 Internet，本机 IP 为 192.168.167.38/24

2. Jumpserver 为 centos7 虚拟机，安装一块网卡，IP 地址为 10.0.149.157/16,并绑定一个弹性公网 IP，IP

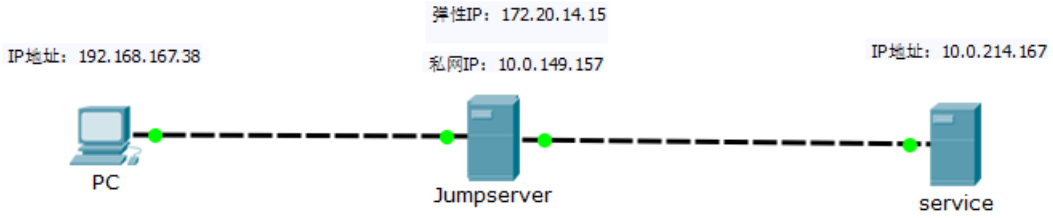
地址为 172.20.14.15/16，能连通 Internet，堡垒机能够 ping 通 PC 和 Service

3. service 为 Centos7 虚拟机，安装一块网卡，IP 地址为 10.0.214.167/16

4. 目前 PC 端无法连接 10.0.0.0/16 网段的所有 IP

5. 两个 Centos 均安装 openssh-client 和 openssh-service，并能正常使用 sshd 服务

6. PC 通过弹性公网 IP 远程连接到 jumpserver，再利用 jumpserver 的私网 IP 来远程连接管理 service，达到 PC 控制远端 service 的效果，具体网络构架规划示意图，如下图所示：



3. Linux 堡垒机部署

3.1 创建堡垒机

在 ZStack 私有云主菜单，点击云资源池 > 云主机按钮，进入云主机界面，点击创建云主机按钮，在弹出的创建云主机页面，可参考以下示例输入相应内容，这里所使用的镜像是 CentOS-7-x86_64-DVD-1804，三层网络选择私有网络，具体如图 1 所示：

图 1 创建云主机

3.2 安装系统

3.2.1 打开控制台

打开当前云主机的控制台，可以登录云主机系统，进入 ISO 引导安装界面，默认选择 Install ZStack 开始安装操作系统；当服务器引导模式选择为 Legacy 模式时 U 盘引导，如图 2 所示：

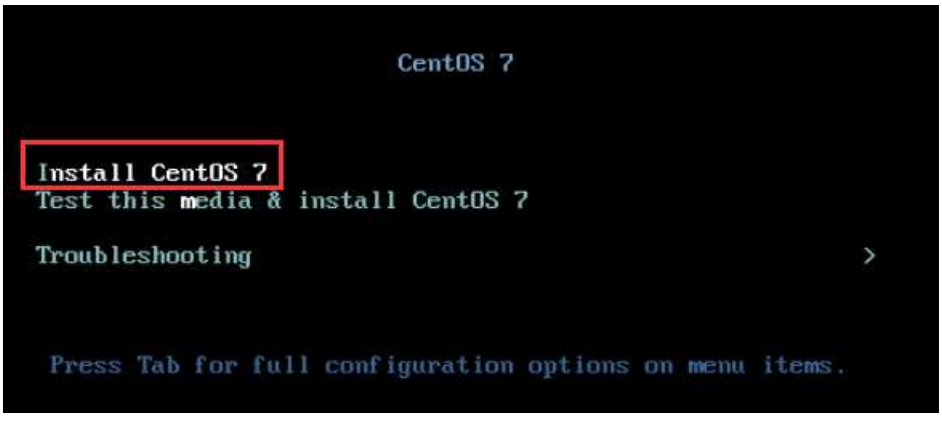


图 2 选择安装方式

3.2.2 选择语言

根据个人喜好选择语言，这里选择 English(United States)，如图 3 所示：

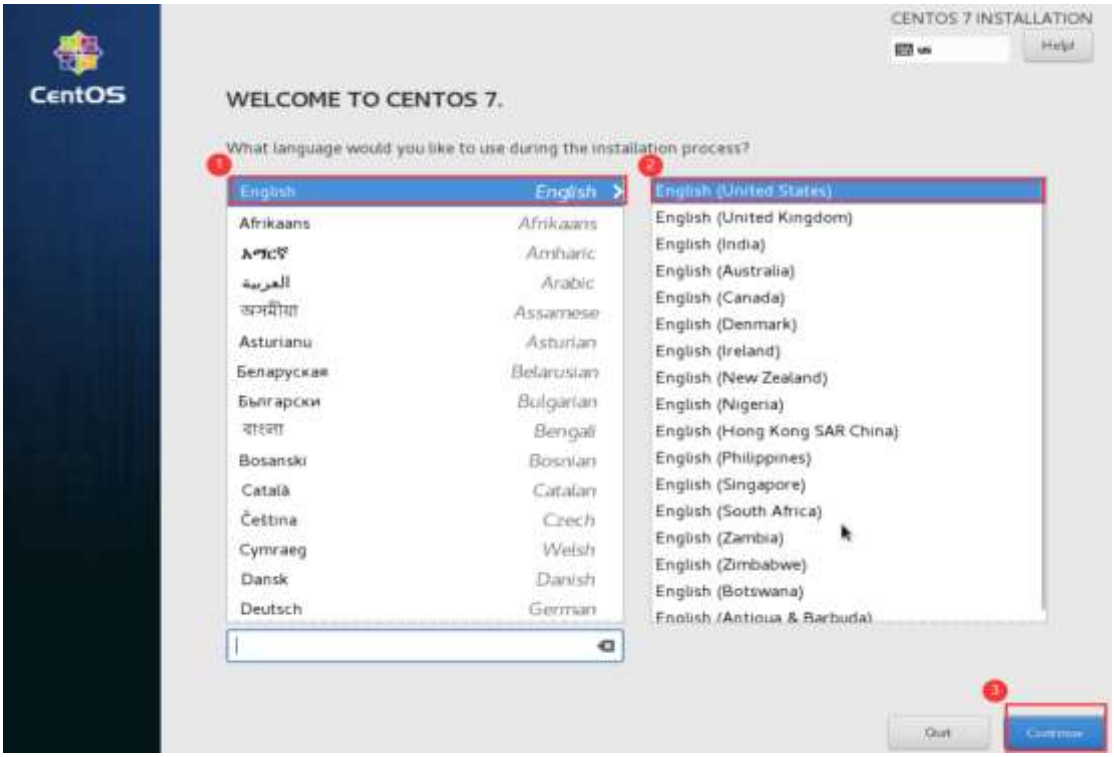


图 3 语言选择

3.2.3 进入系统安装界面

进入系统安装界面后，已经预先配置如下默认选项，一般情况下管理员无需更改配置。

- DATE&TIME：Americas/New York timezone
- LANGUAGE：English(United States)
- KEYBOARD：English(US)

系统安装界面如下图 4 所示：

图 4 系统安装界面

3.2.4 选择安装模式

在系统安装界面，点击 SOFTWARE SELECTION 进入服务器安装模式候选，根据个人喜好选择服务器安装模式，这里选择 Minimal Install，然后点击 Done，如图 5 所示：

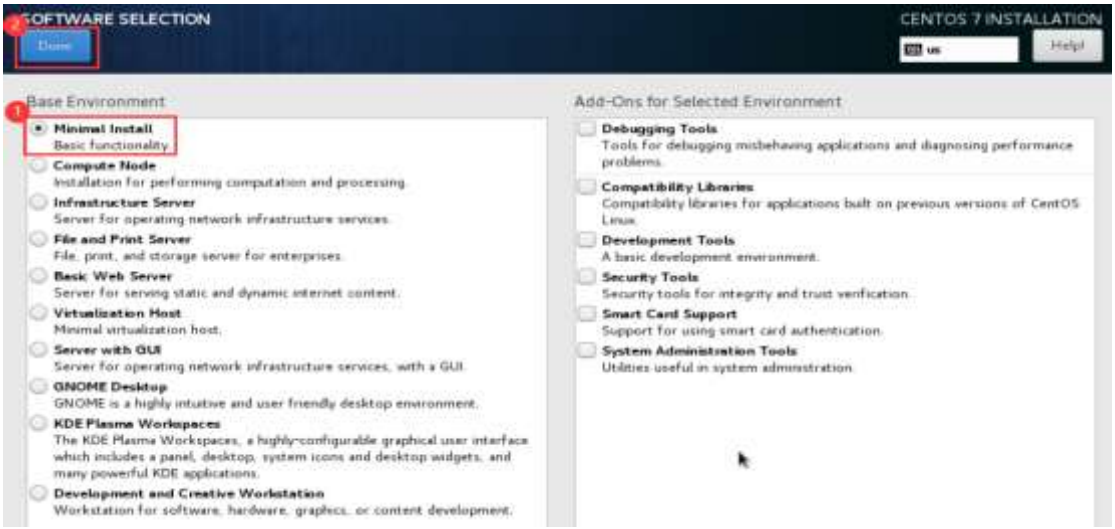


图 5 服务器安装模式候选

3.2.5 配置硬盘分区

1. 在系统安装界面，点击 INSTALLATION DESTINATION 进入硬盘分区配置界面，选择要做的系统盘，点击 I will configure partitioning 进行手动分区，然后点击 Done 开始分区配置，如图 6 所示：

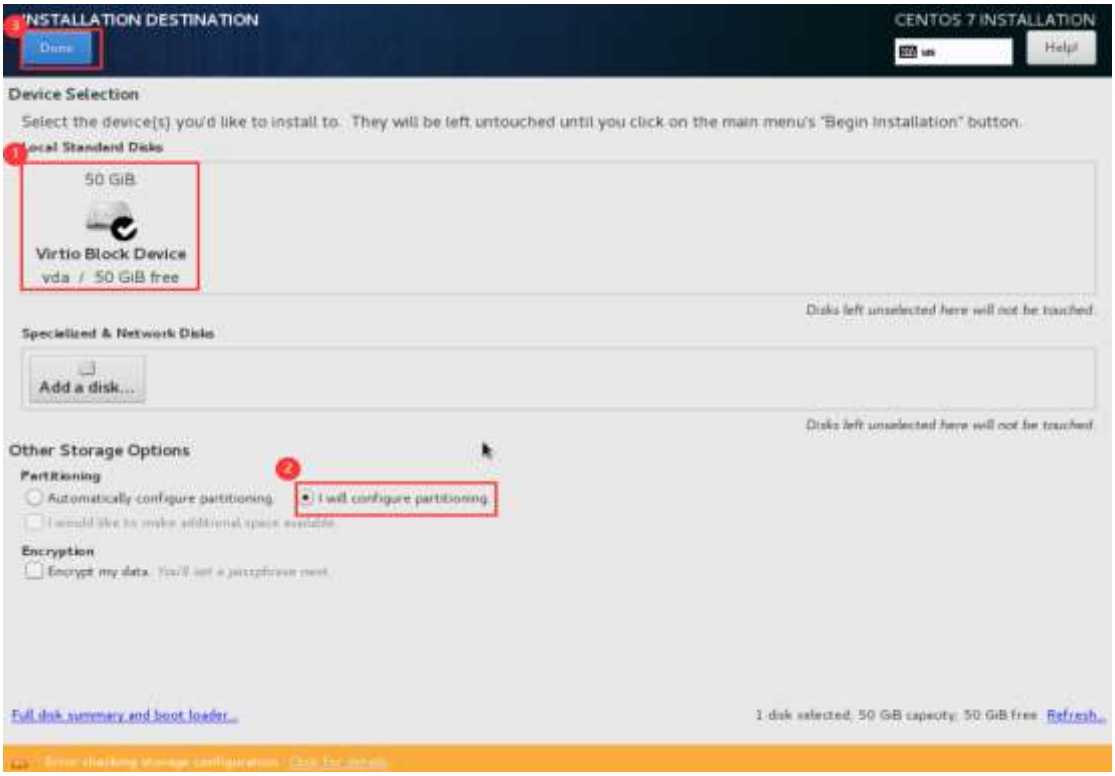


图 6 配置硬盘分区

2. 手动选择分区类型 Standard Partition、Btrfs、LVM、LVM Thin Provisioning，这里选择 Standard Partition，然后点击"+"进行分区，创建好分区后点击 Done 完成分区创建 ，如图 7 所示：

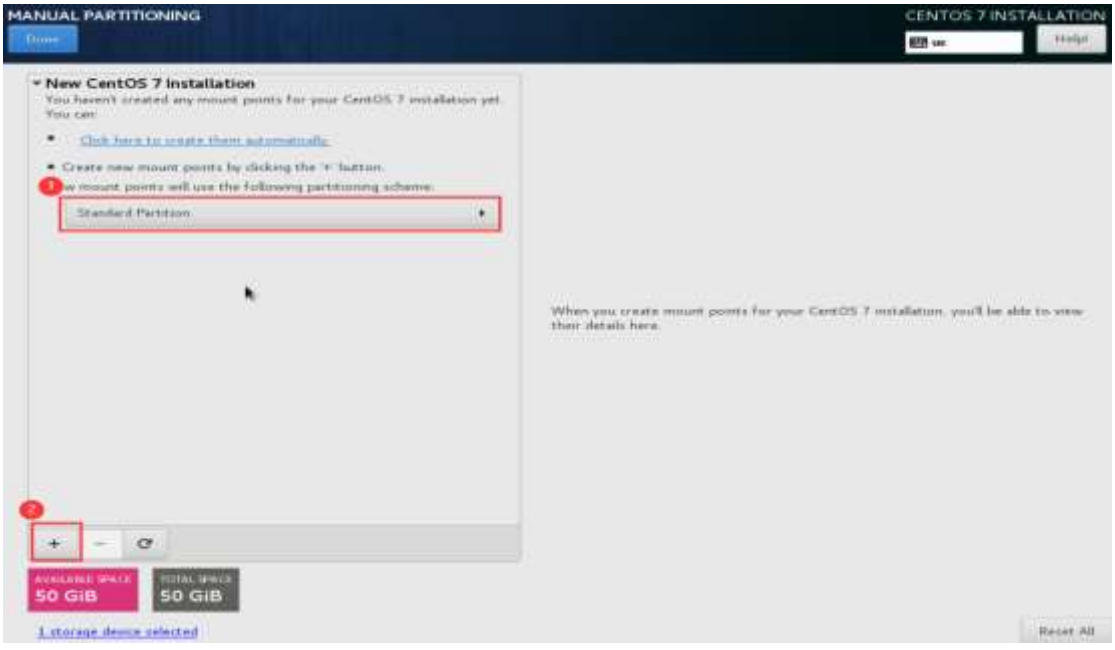


图 7 选择分区格式

3. 创建引导分区，如图 8 所示：

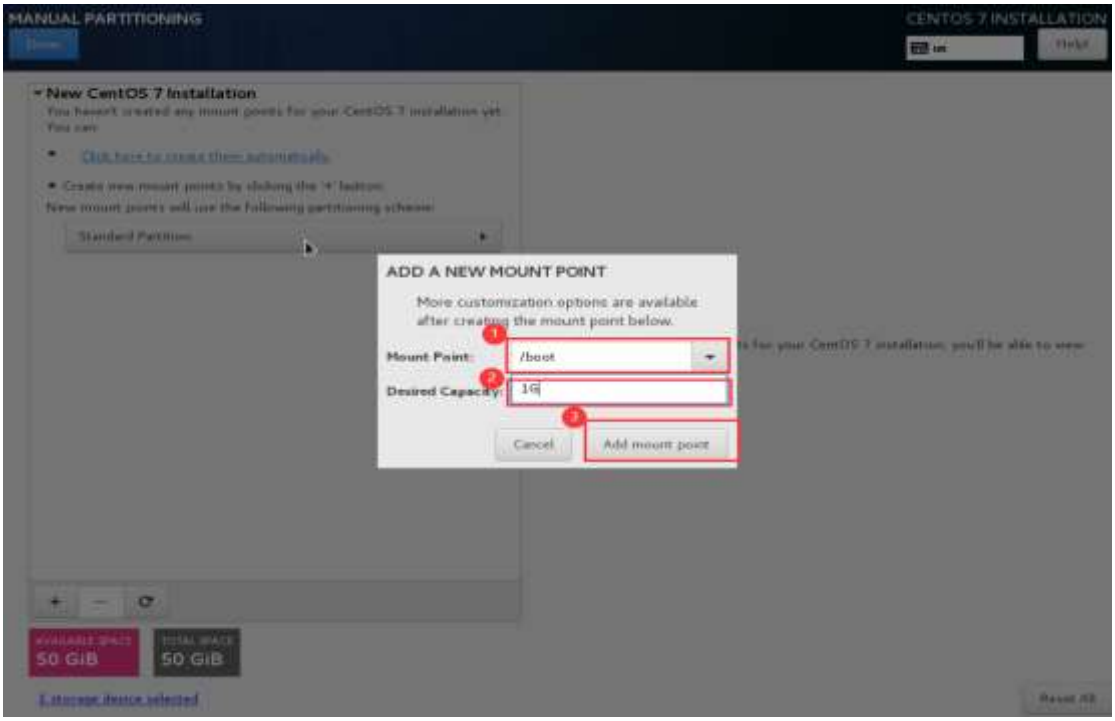


图 8 创建引导分区

4. 创建 swap 分区，如图 9 所示：

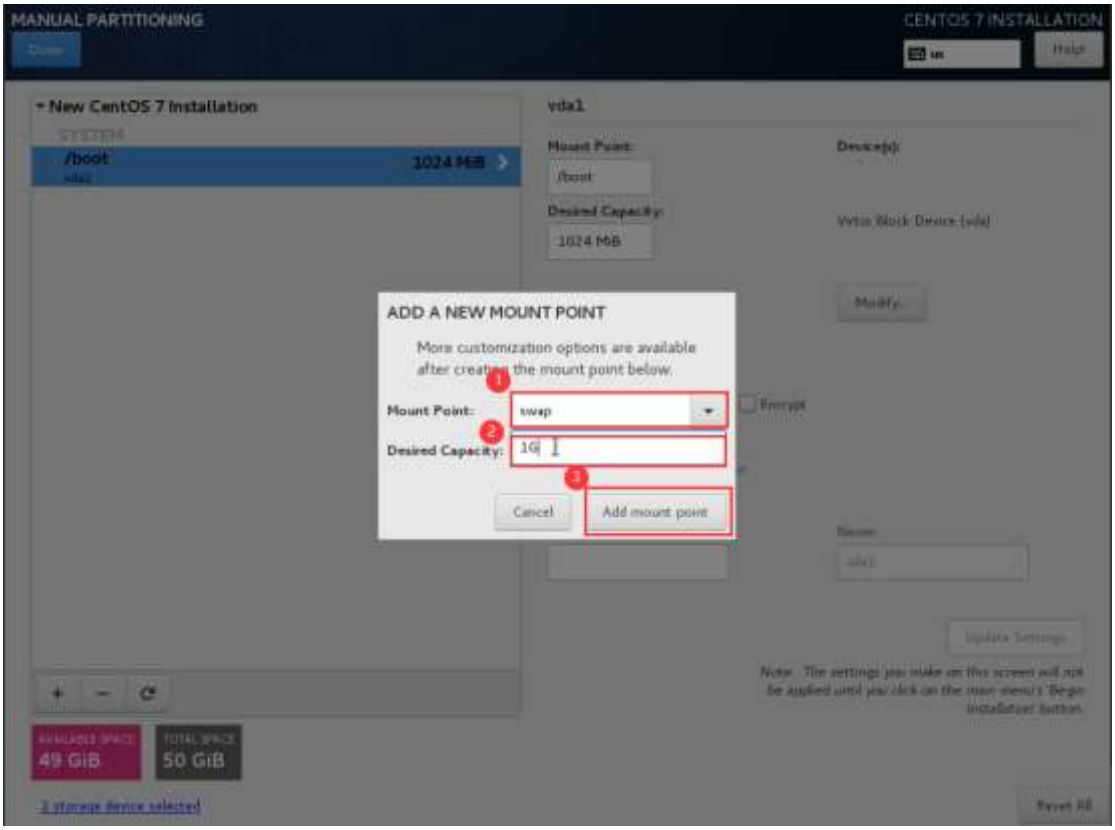


图 9 创建 swap 分区

5. 创建根分区，在配置根目录时，在 Desired Capacity 不输入数据，表示将所有空间都划分给/目录，

如图 10 所示。

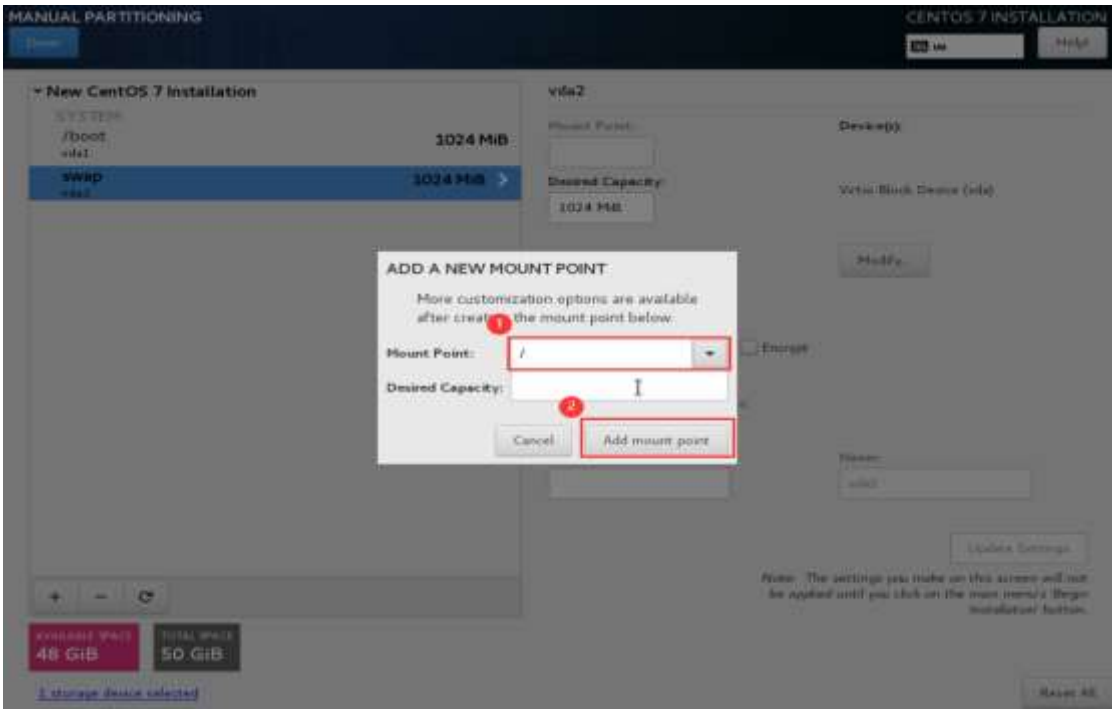


图 10 创建根分区

6. 确认无误后，点击 Done 按钮完成磁盘分区操作，如图 11 所示：

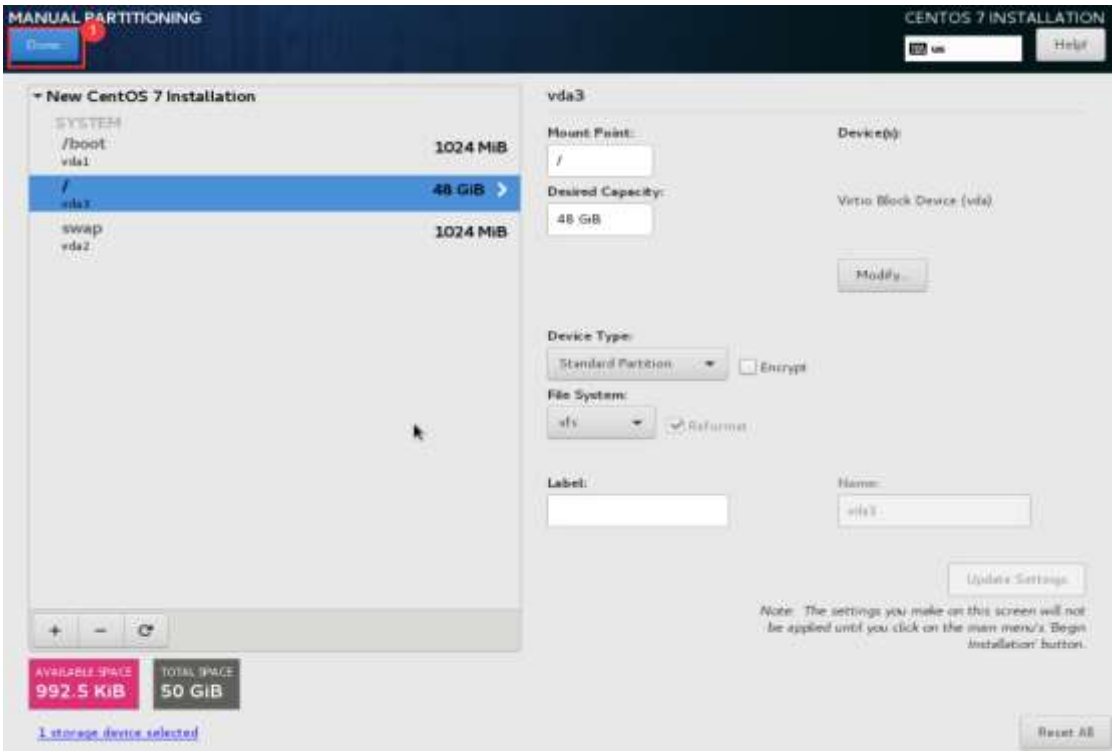


图 11 完成磁盘分区

7. 点击 Done 按钮后会弹出确认框;点击 Accept Changes 应用分区配置，如图 12 所示：

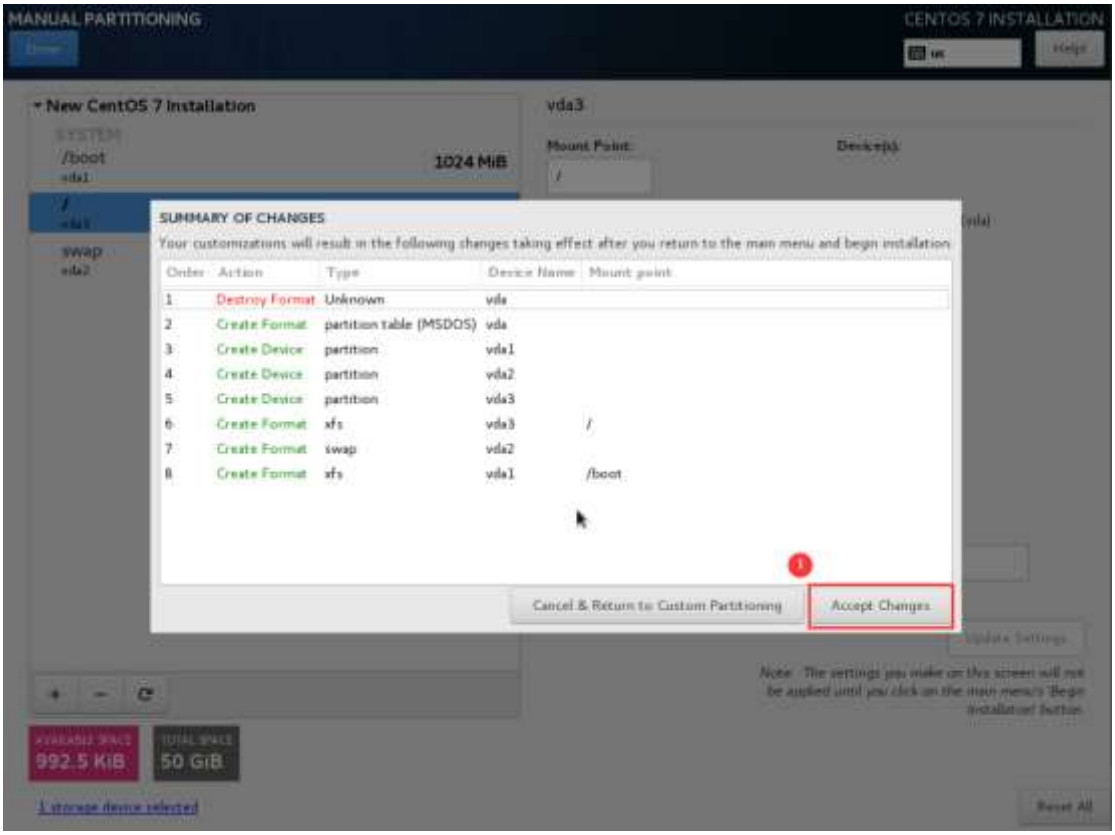


图 12 应用分区配置

3.2.6 配置网络

1. 在系统安装界面，点击 NETWORK & HOST NAME 进入网卡配置主界面，选择需要修改的网卡，点击 Configure 按钮进行配置，如图 13 所示：

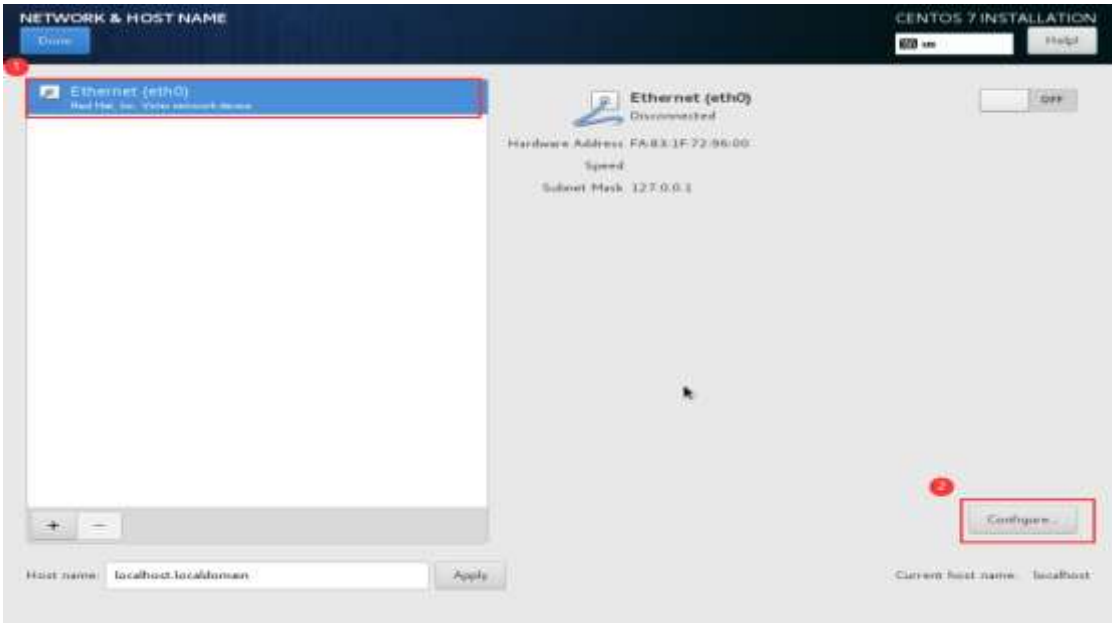


图 13 配置网卡

2. 在 General 选项中，默认不会勾选 Automatically connect to this network when it is available，因此需要检查该网卡是否勾选开机自动启动网卡，如果未勾选请手动勾选，如图 14 所示：

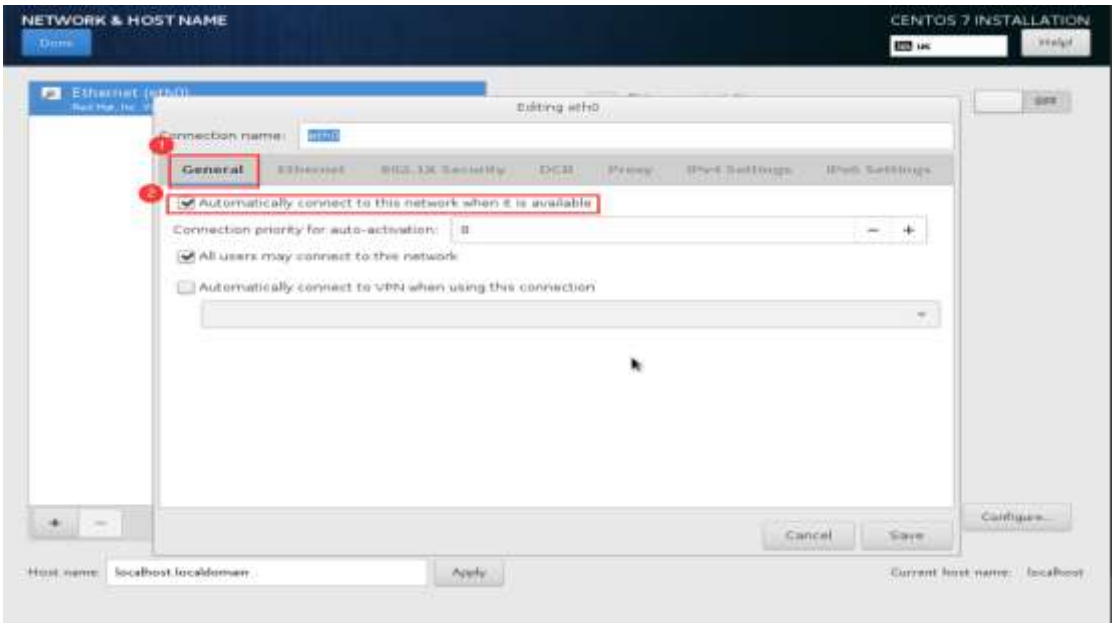


图 14 自动启动网卡

3. 在 Ipv4 Settings 选项中，根据个人环境选择 DHCP 还是 Manual，Manual 需要手动设置 IP 地址、掩码、网关、DNS，这里选择 DHCP，设置好后点击 Save 按钮进行保存，如图 15 所示：

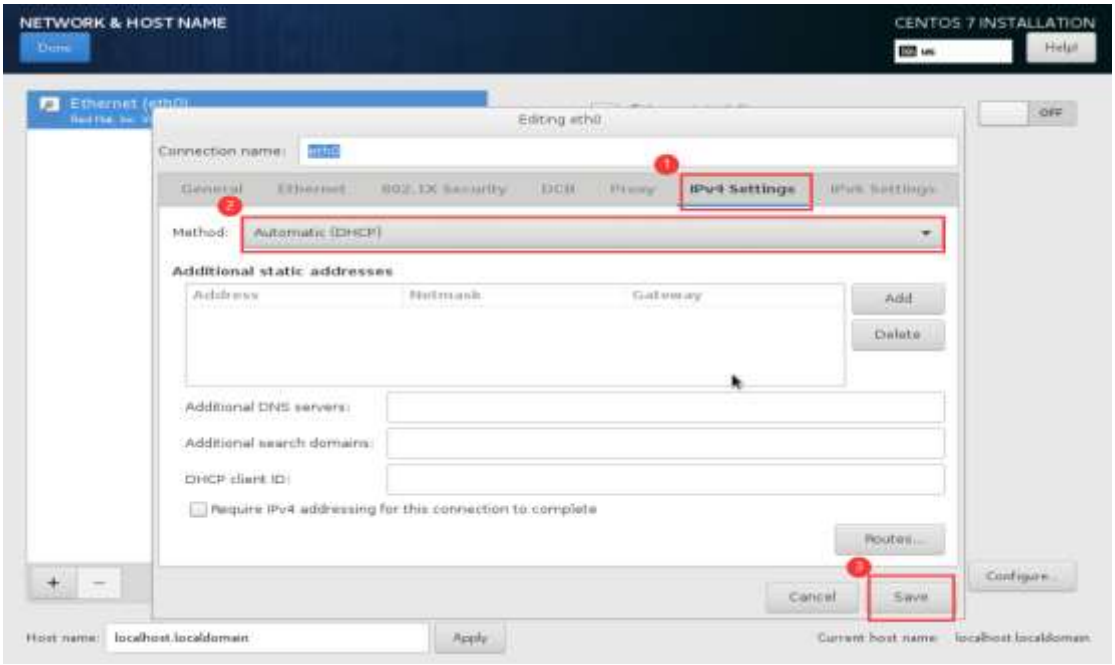


图 15 配置网卡

3.2.7 开始安装

网络配置完后，回到系统安装主界面，点击 Begin Installation 开始安装，如图 16 所示：

图 16 开始安装

3.2.8 设置 root 用户密码

1. 安装过程自动进行，安装过程中请设置 ROOT PASSWORD，如图 17 所示：

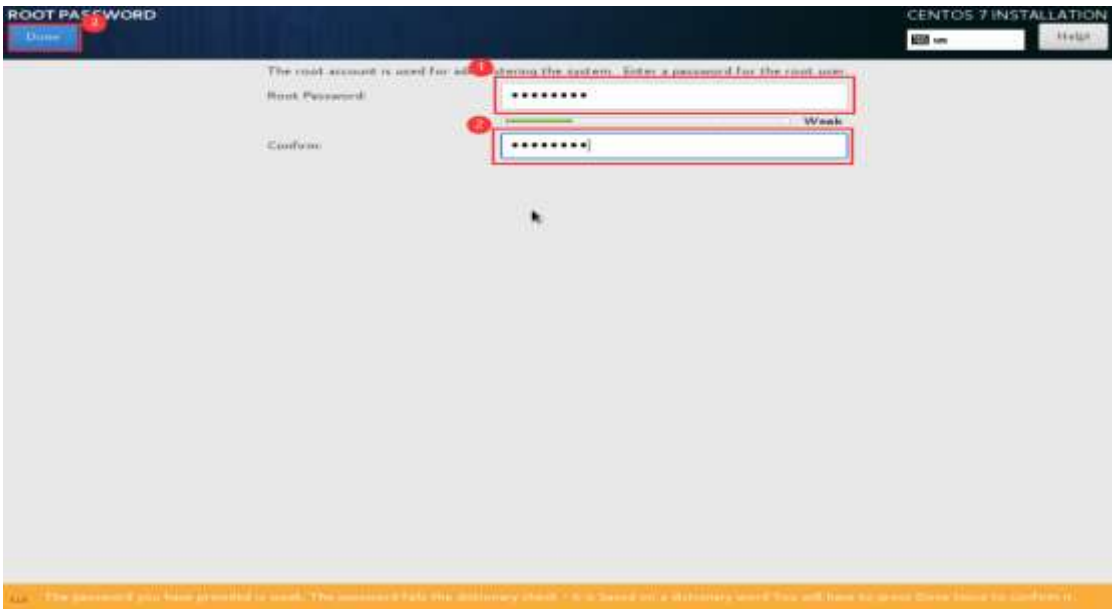


图 17 设置 root 用户密码

2. 基础系统安装完毕后需要手动点击 Reboot 进行重启，重启完成后会自动进入 Linux 系统中，如图 18、

图 19 所示：

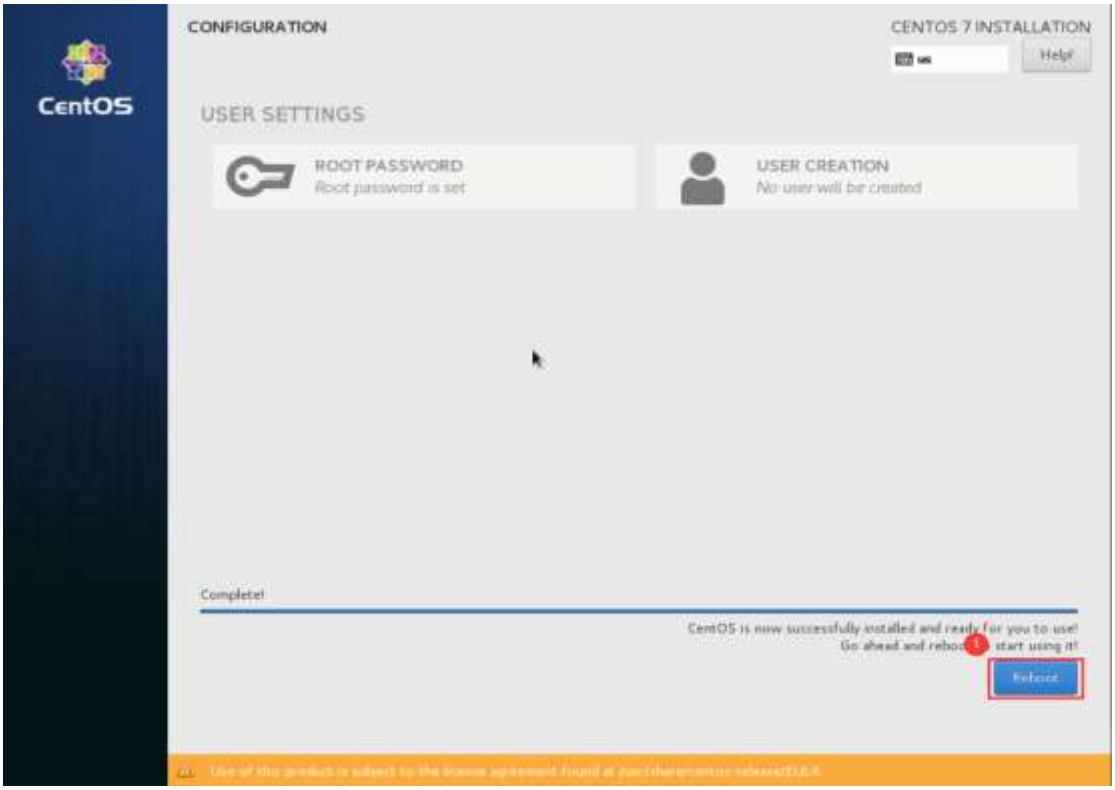


图 18 重启

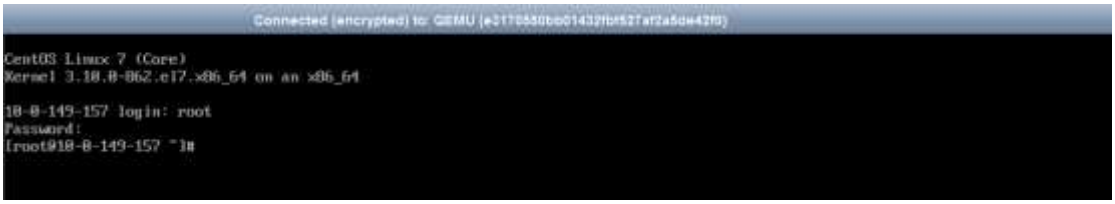


图 19 进入系统

3.3 添加公网弹性 IP

1. 在 ZStack 私有云主菜单，点击网络服务 > 弹性 IP，进入弹性 IP 界面，点击创建弹性 IP，在弹出的创建弹性 IP 界面，可参考以下示例输入相应内容，如图 20 所示：

图 20 创建弹性 IP

2. 绑定云主机网卡，选择要绑定的云主机并选择该云主机所需要绑定的网卡，然后点击确定，完成创建，如图 21、图 22、图 23 所示：

图 21 绑定云主机

图 22 绑定云主机网卡

图 23 弹性 IP 详情界面

3. 弹性 IP 绑定成功，到云主机界面 ping www.baidu.com，测试网络的连通性，如图 24 所示：

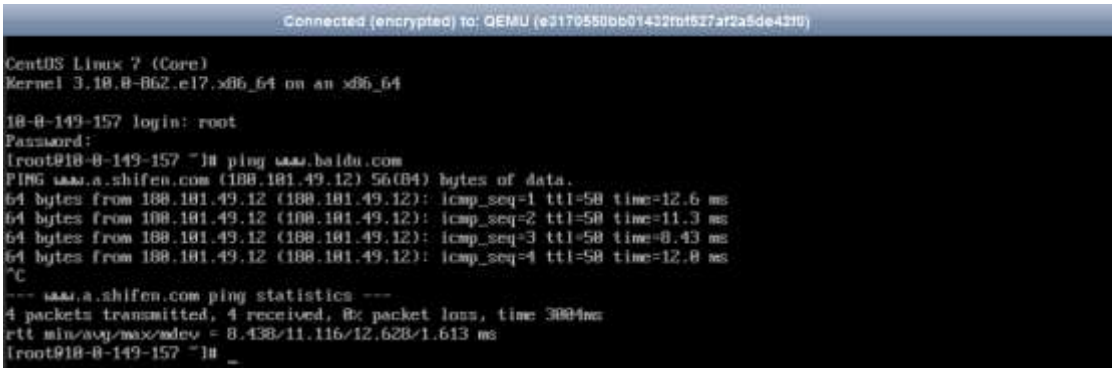


图 24 测试网络连通性

3.4 应用部署

3.4.1 安装 yum 源

Yum(全称为 Yellow dog Updater, Modified)是一个在 Fedora 和 RedHat 以及 CentOS 中的 Shell 前端软件包管理器。基于 RPM 包管理，能够从指定的服务器自动下载 RPM 包并且安装，可以自动处理依赖性关系，并且一次安装所有依赖的软件包，无须繁琐地一次次下载、安装。Yum 源就是一个软件集合地，你只需要搜索并安装你想要的软件，它会帮你解决大部分软件的依赖问题。

```
#mkdir /etc/yum.repos.d/back

#mv /etc/yum.repos.d/* /etc/yum.repos.d/back

#curl –o /etc/yum.repos.d/CentOS-Base.repo http://mirrors.aliyun.com/repo/Centos-7.repo
```

```
#yum clean all && yum makecache

#yum install wget -y

#wget -O /etc/yum.repos.d/epel.repo http://mirrors.aliyun.com/repo/epel-7.repo
```

3.4.2 安装 python 包

Python 是一种跨平台的计算机程序设计语言。是一种面向对象的动态类型语言，最初被设计用于编写自动化脚本(shell)，随着版本的不断更新和语言新功能的添加，越来越多地被用于独立的、大型项目的开发，目前最稳定的版本也是 Python3.0 以上。

```
#yum -y install wget sqlite-devel xz gcc automake zlib-devel openssl-devel

#mkdir -p /opt/server/tools

#cd /opt/server/tools/

#tar xvf Python-3.6.1.tar.xz && cd Python-3.6.1

#./configure --prefix=/usr/local/python3 && make && make install
```

3.4.3 安装 git

Git 是目前流行的非常好用的版本控制工具，这里介绍其中一种安装方式：使用 yum 安装。

```
#yum -y install git
```

3.4.4 安装 mysql 和创建数据库

数据库是"按照数据结构来组织、存储和管理数据的仓库"。是一个长期存储在计算机内、有组织、有共享、统一管理的数据集合。数据库是以一定方式储存在一起、能与多个用户共享、具有尽可能小的冗余度、与应用程序彼此独立的数据集合，可视为电子化的文件柜——存储电子文件的处所，用户可以对文件中的数据进行新增、查询、更新、删除等操作。

```
#yum -y install mariadb mariadb-devel mariadb-server

#systemctl enable mariadb
```

```
#systemctl start mariadb

#DB_PASSWORD=`cat /dev/urandom | tr -dc A-Za-z0-9 | head -c 24`

#echo -e "\033[31m 数据库密码是 $DB_PASSWORD \033[0m"

#mysql -uroot -e "create database jumpserver default charset 'utf8'; grant all on jumpserver.* to

'jumpserver'@'127.0.0.1' identified by '$DB_PASSWORD'; flush privileges;"
```

3.4.5 建立加速 pip

在使用 Python 的时候，需要下载各种各样的库，于是就需要一个下载库的管理工具，所以就需要在我们的 Linux 上下载 pip 帮助我们管理库。

```
#cd

#mkdir .pip

#vi ~/.pip/pip.conf

[global]

index-url = http://mirrors.aliyun.com/pypi/simple/



[install]

trusted-host=mirrors.aliyun.com
```

3.4.6 安装 jumpserver

1. JumpServer 是全球首款完全开源的堡垒机，使用 GNU GPL v2.0 开源协议，是符合 4A 的专业运维审计系统。
2. JumpServer 使用 Python / Django 进行开发，遵循 Web 2.0 规范，配备了业界领先的 Web Terminal 解决方案，交互界面美观、用户体验好。
3. JumpServer 采纳分布式架构，支持多机房跨区域部署，中心节点提供 API，各机房部署登录节点，可

横向扩展、无并发访问限制。

4. JumpServer 现已支持管理 SSH、 Telnet、 RDP、 VNC 协议资产。

5. Jumpserver 安装包地址：https://pan.baidu.com/s/1HlNOxnd3jxstw5cMMLU--g

```
#cd /opt/server/tools/

#yum install unzip -y

#unzip jumpserver-rpm.zip

#cd jumpserver-rpm/jumpserver

#git checkout master

#cd install/

#python install.py
```

3.4.7 配置

配置安装 jumpserver 所需要的数据库、管理员账号密码、163 邮箱、QQ 邮箱等，完成 jumpserver 的配置部署。

```
请输入您服务器的 IP 地址，用户浏览器可以访问 [10.0.0.31]: 172.20.14.15

是否安装新的 MySQL 服务器? (y/n) [y]: n

请输入数据库服务器 IP [127.0.0.1]: 127.0.0.1

请输入数据库服务器端口 [3306]: 3306

请输入数据库服务器用户 [jumpserver]: jumpserver

请输入数据库服务器密码: M0ynoMmM6p3Egz3qtQhjS07I

请输入使用的数据库 [jumpserver]: jumpserver

连接数据库成功

……
```

请输入管理员用户名 [admin]: admin

请输入管理员密码: [5Lov@wife]: password

请再次输入管理员密码: [5Lov@wife]: password

Starting jumpserver service: [确定]

安装成功，Web 登录请访问 http://ip:8000，祝你使用愉快。

请访问 https://github.com/jumpserver/jumpserver/wiki 查看文档

3.4.8 登陆

打开浏览器，输入 http://IP:8000，就能看到 jumpserver 登陆界面，并进行登陆，如图 25、26 所示：

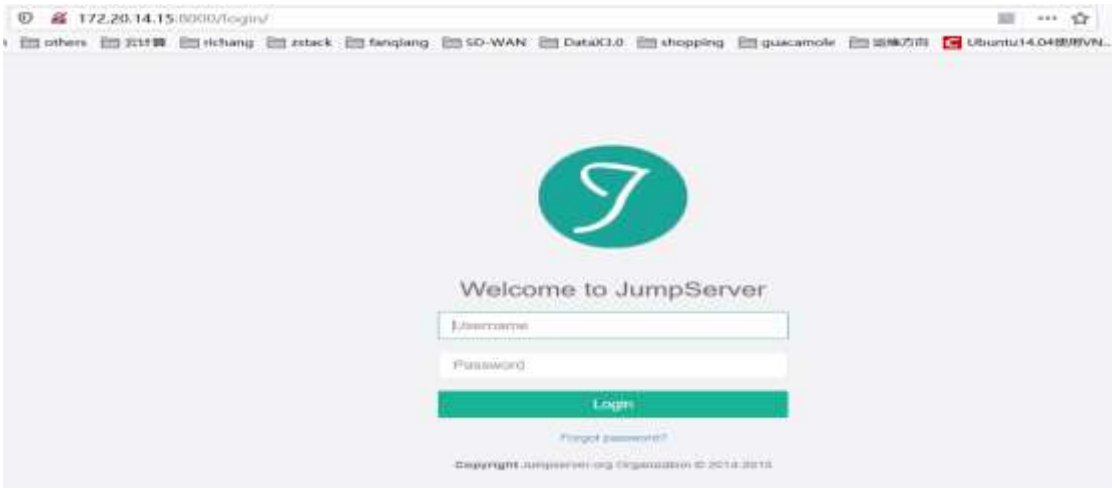


图 25 登陆

图 26 用户界面

3.4.9 添加远程主机

远程主机是所需要远程管理的主机，方便用户远程进行操作，点击资产管理 —> 查看资产，输入相关内容，如图 27 所示：

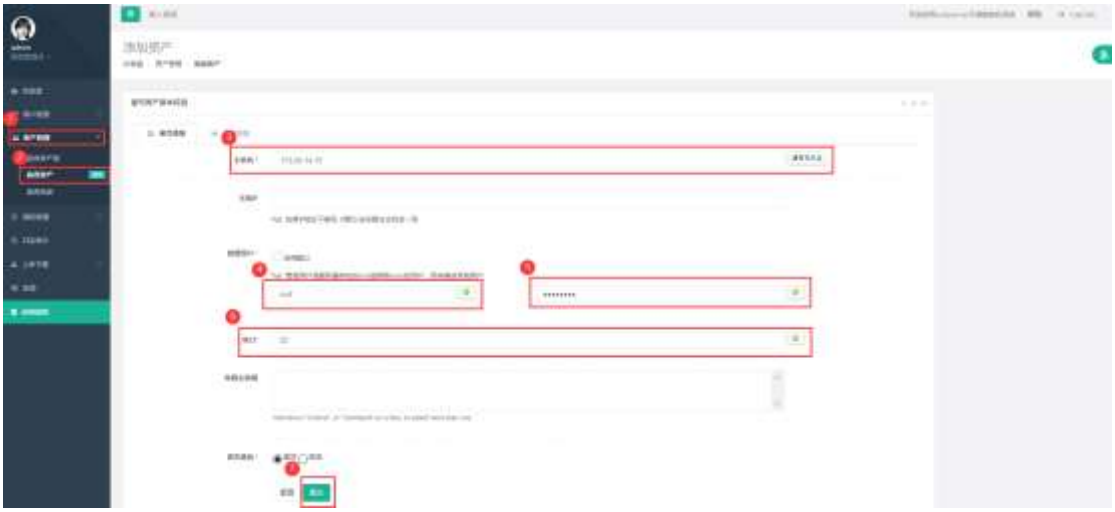


图 27 添加主机

3.4.10 添加 Sudo 命令

Sudo 命令是系统用户登陆远程主机时该用户所能执行那些命令操作，点击授权管理 —> Sudo，输入相关内容，如图 28 所示：

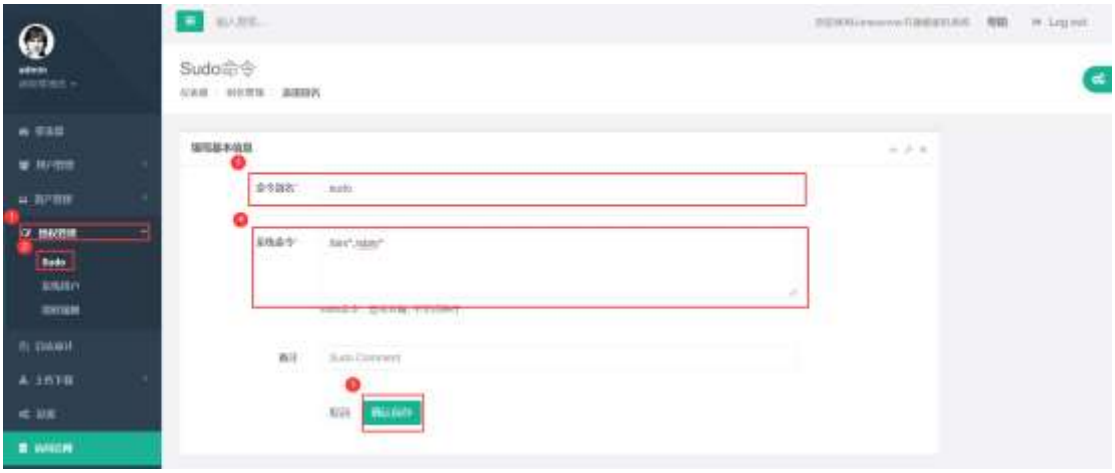


图 28 添加 Sudo

3.4.11 添加系统用户

1. 系统用户是 Linux 远程主机中用来远程进行登录的用户，其中要注意该系统用户在所需要远程操控的

主机中是真实存在的，点击授权管理 —> 系统用户，输入相关内容，如图 29 所示：

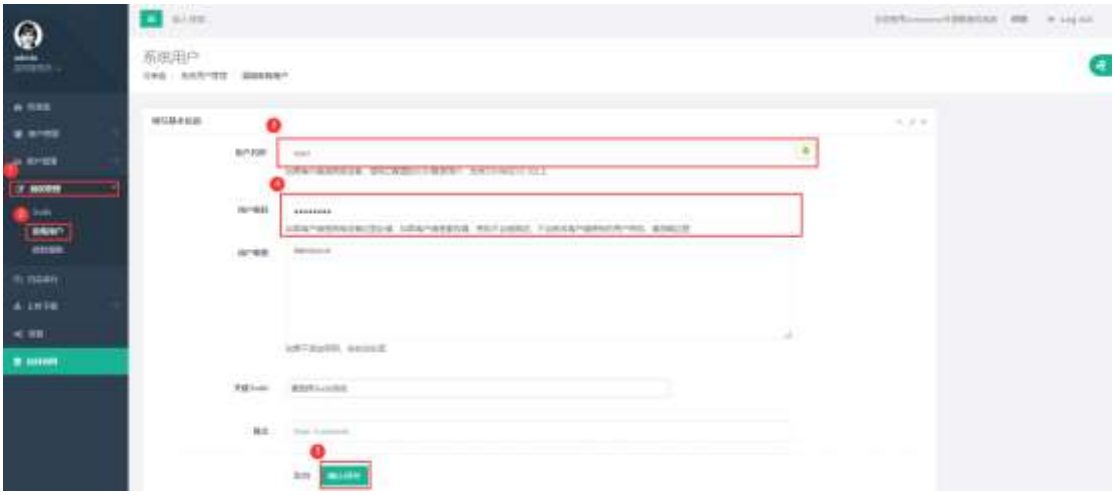


图 29 添加系统用户

2. 创建完系统用户后，点击推送，输入相关内容，绑定主机，如图 30、31 所示：

图 30 点击推送

图 31 绑定主机

3.4.12 添加授权规则

授权规则是可以指定哪些系统用户、用户组可以进行登录哪些远程主机，同时也方便分类进行管理，点击授权管理 —> 授权规则，输入相关内容，如图 32 所示：

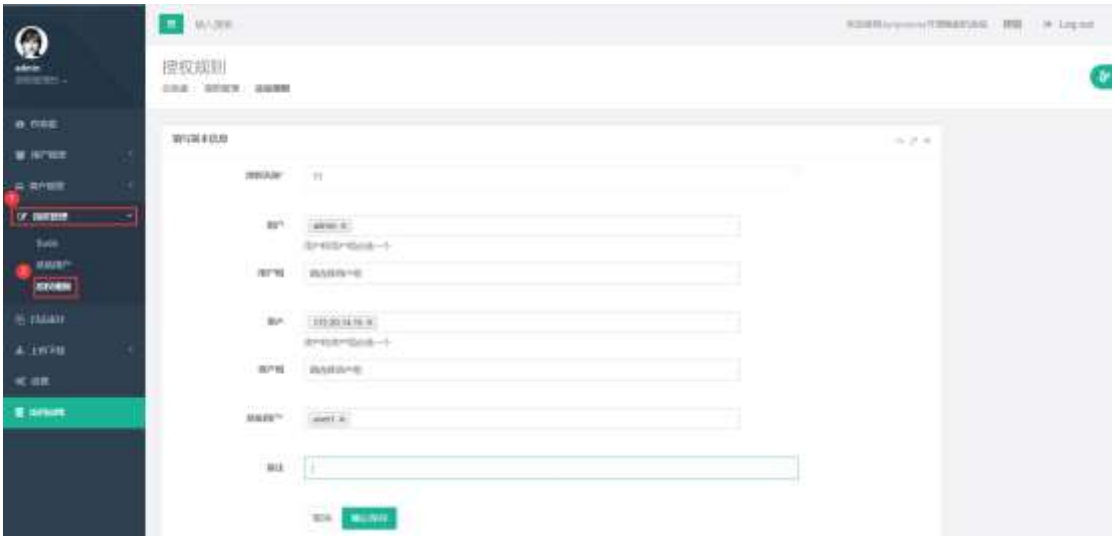


图 32 添加授权规则

3.4.13 连接

最后点击资产管理 —> 查看资产，点击主机的连接按钮，完成连接，如图 33、34 所示：

图 33 点击连接

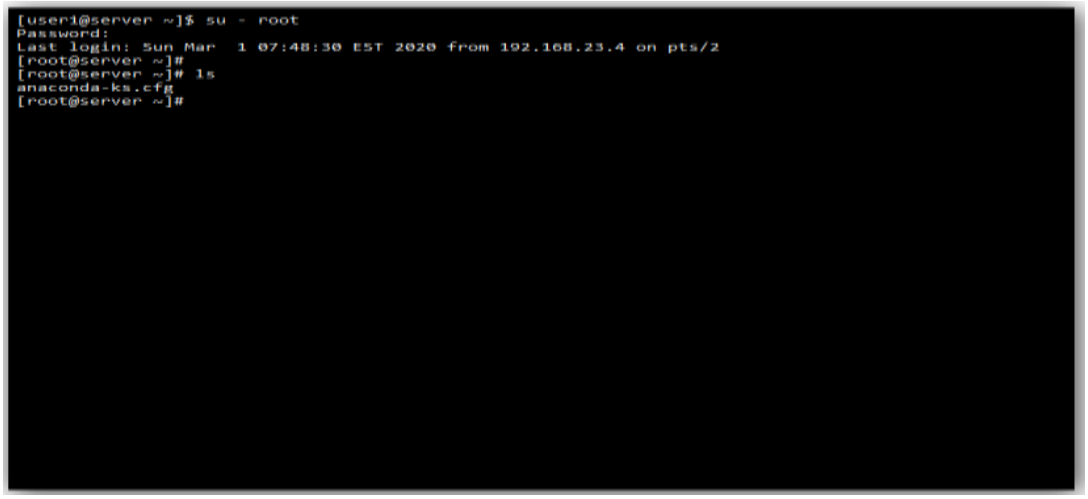


图 34 完成连接

4. 测试

4.1 从 PC 端直接连接 service，无法进行连接，如图 35 所示：

```
[C:\~]$ ssh 10.0.214.167


Connecting to 10.0.214.167:22...
Could not connect to '10.0.214.167' (port 22): Connection failed.

Type `help' to learn how to use Xshell prompt.
```

图 35 连接失败

1.5 从 PC 端通过 Xhell 连接 Jumpserver 主机远程 service 或者直接通过 jumpserver 管理界面连接到 service，都能能成功连接，如图 36、37 所示：

```
[C:\~]$ ssh user1@172.20.14.15


Connecting to 172.20.14.15:22...
Connection established.
To escape to local shell, press 'Ctrl+Alt+]'.

WARNING! The remote SSH server rejected X11 forwarding request.
Last login: Sun Mar  1 07:55:19 2020 from 172.20.15.194
[user1@server ~]$ su - root
Password:
Last login: Mon Mar  2 07:17:10 EST 2020 from 192.168.23.4 on pts/0
[root@server ~]# ssh 10.0.214.167
root@10.0.214.167's password:
Last login: Mon Mar  2 12:17:56 2020 from 10.0.149.157
[root@10-0-214-167 ~]#
```

图 36 连接成功

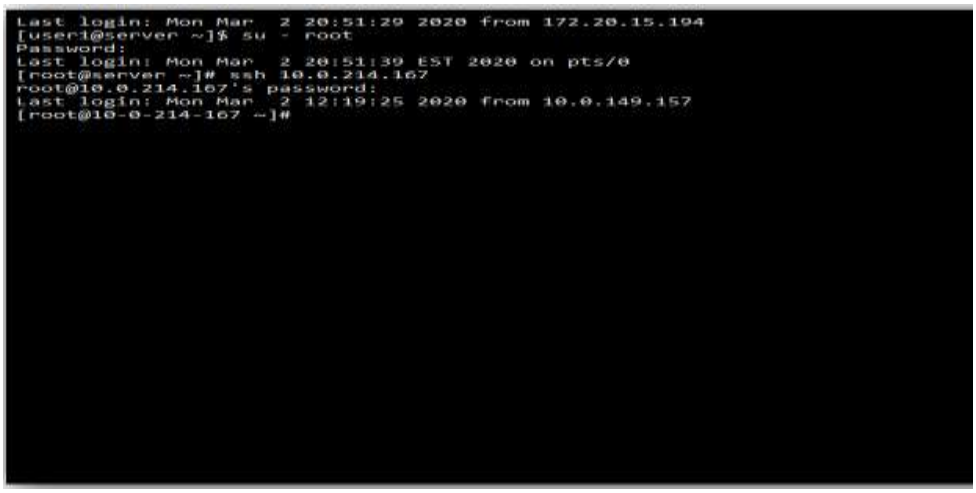


图 37 连接成功

5. 总结

堡垒机往往是作为系统管理员或运维人员常用的操作平台之一、可以被理解为一类可作为跳板批量操作远程设备的网络设备。同时，堡垒机是网络中容易受到侵害的主机，所以堡垒机也必须是自身保护完善的主机。

堡垒机通常至少配备两块网卡设备，分别具备不同的网络连接。但在 ZStack 平台中，我们可以做到：只绑定弹性 IP 就能实现两块网卡设备所具有的效果，并且弹性 IP 定义了通过公有网络访问内部私有网络的方法，内部私有网络是隔离的网络空间，不能直接被外部网络访问，这也就一定程度上控制堡垒机在网络上受到侵害，同时弹性 IP 基于网络地址转换（NAT），将一个网络（通常是公有网络）的 IP 地址转换成另一个网络（通常是私有网络）的 IP 地址；通过弹性 IP，可对公网的访问直接关联到内部私网的云主机 IP。

但堡垒机并没有实现对运维人员操作行为的控制和审计，所以在使用堡垒机过程中还是会有误操作、违规操作导致的操作事故，一旦出现操作事故也很难快速定位原因和责任人。