

## 重要配置信息

[系统信息](#)

[帐户信息](#)

[其他信息](#)

[虚拟系统管理](#)

[重要评测信息](#)

## 练习要求

1. 配置 IPV6 地址
2. 配置 dhcp 服务器
3. 配置防火墙
4. 完成主 DNS 配置
5. 准备 samba 共享
6. 使用多用户访问 samba 共享目录
7. 配置 NFS 服务
8. 挂载一个 NFS 共享
9. 配置 iSCSI 服务端
10. 配置 iSCSI 的客户端
11. 搭建 MariaDB
12. 数据查询填空1
13. 数据查询填空2
14. 实现一个 web 服务器
15. 配置安全 web 服务
16. 配置虚拟主机
17. 配置web内容的访问
18. 通过 ansible 部署 Nginx
19. 通过 ansible 配置 firewall
20. 通过 ansible 配置空邮件客户端
21. 通过 ansible 部署打印机

# 重要配置信息

---

在练习期间，除了您就坐位置的台式机之外，还将使用多个虚拟系统。您不具有台式机系统的根访问权，但具有对虚拟系统的完全 root 访问权。

## 系统信息

---

系统	IP地址	角色	LAN1	LAN2
workstation	172.25.250.9	ansible 控制节点	Y	
bastion	172.25.250.254	网关	Y	
servera	172.25.250.10	CMD - server	Y	Y
serverb	172.25.250.11	CMD - client	Y	
serverc	172.25.250.12	ansbile 托管节点	Y	
serverd	172.25.250.13	ansible 托管节点	Y	
servere		dhcp client		Y

这些系统的IP地址采用静态设置。请勿更改这些设置。主机名称解析已配置为解析上方列出的完全限定主机名，同时也解析主机短名称。

## 帐户信息

- 所有系统的root密码是 `redhat`。请勿更改root密码
- 除非另有指定，否则这将是用于访问其他系统和服务的密码。
- 除非另有指定，否则此密码也应用于您创建的所有帐户或者任何需要设置密码的服务。
- 为方便起见，所有系统上已预装了SSH密钥，允许在不输入密码的前提下通过SSH进行root访问。请勿对系统上的root SSH配置文件进行任何修改。
- **Ansible控制节点上已创建了用户帐户 `devops`**。此帐户预装了SSH密钥，允许在Ansible控制节点和各个Ansible受管节点之间进行SSH登录。请勿对系统上的student SSH配置文件进行任何修改。您可以从root帐户使用su访问此用户帐户。

## 其他信息

- 一些练习项目可能需要修改Ansible主机清单。您要负责确保所有以前的清单组和项目保留下来，与任何其他更改共存。您还要有确保清单中所有默认的组和主机保留您进行的任何更改。
- 所有节点，yum存储库已正确配置。
- 一些项目需要额外的文件，这些文件已在以下位置提供：<http://materials.example.com/classroom/ansible/>
- 产品文档可从以下位置找到：<https://docs.ansible.com/ansible/2.9/>
- 其他资源也进行了配置，供您在练习期间使用。关于这些资源的具体信息将在需要这些资源的项目中提供。

## 虚拟系统管理

练习期间，您可以随时关闭或重新引导虚拟机系统。您可以从虚拟系统本身进行这项操作，也可以从物理系统控制虚拟系统。要从物理系统访问或控制练习系统，单击桌面上VM控制台图标。这会显示一个表格，包含每个虚拟机系统的对应按钮，单击特定虚拟机系统的按钮将弹出一个菜单，包含用来控制该系统选项：

- 启动节点VM-如果指定的虚拟系统未在运行，该选项将启动指定系统。如果系统已经在运行-则该选项无任何作用。
- 重新引导节点VM-正常关闭练习虚拟系统，然后重启。
- 关闭节点VM-正常关闭指定虚拟系统。
- 关闭节点VM电源-立即关闭指定虚拟系统。
- VM控制台节点-这将打开一个窗口，用于连接到指定虚拟系统的控制台。请注意，如果将焦点移动到此窗口，控制台将抓住您的鼠标。要恢复鼠标，同时键入Ctrl+Alt。
- 重建节点VM-将当前VM还原为原始状态。系统将弹出一个单独的窗口，要求您确认操作。警告!!! 您在VM上完成的所有操作都将丢失。仅当系统无法使用时才应使用这个功能。在使用这个功能之前，确保关闭VM。

## 重要评测信息

请注意，在评分之前，您的 Ansible 托管节点系统 将重置为练习开始时的初始状态，您编写的 Ansible playbook 将通过以 **student** 用户身份在控制节点上运行来加以应用。在 playbook 运行后，系统会重新启动您的托管节点，然后进行评估，以判断它们是否按照规定进行了配置。

请注意，在评分之前，您的 Ansible 托管节点系统 将重置为练习开始时的初始状态，您创建的 Ansible Tower 作业将通过以指定的用户身份运行来加以应用。在作业运行后，系统会重新启动 Ansible Tower 托管节点，然后进行评估，以判断它们是否按照规定进行了配置。

## 练习要求

### 1. 配置 IPV6 地址

在您的练习系统上配置接口 `eth0` 使用下列IPv6地址：

- ☐ servera 上的地址应该是 `fddb:fe2a:ab1e::c0a8:64/64`
- ☐ serverb 上的地址应该是 `fddb:fe2a:ab1e::c0a8:65/64`
- ☐ 两个系统必须能与网络 `fddb:fe2a:ab1e::c0a8:fe` 内的系统通信
- ☐ 地址必须在重启后依旧生效
- ☐ 两个系统必须保持当前的IPv4地址并能通信

### 2. 配置 dhcp 服务器

Configure a DHCP server for IPv4 address assignment and provide fixed IP addresses to selected systems.

- ☐ you deploy a DHCP server on `servera`
- ☐ the second interface `eth1`
- ☐ The DHCP server manages the `192.168.0.0/24` subnet
- ☐ delivers IP addresses in the `192.168.0.200` to `192.168.0.254` range

- ☐ gateway 192.168.0.1
- ☐ domain-name-servers 172.25.254.254
- ☐ domain-search example.net
- ☐ default-lease-time 800
- ☐ associates the 192.168.0.100 IP address to the 52:54:00:01:fa:0b MAC address
- ☐ associates the 192.168.0.101 IP address to the 52:54:00:01:fa:0c MAC address

### 3. 配置防火墙

---

在 `servera` 和 `serverb` 上分别设置，针对SSH

- ☐ 允许 172.25.250.0/24 的域对 `servera` 和 `serverb` 进行 SSH
- ☐ 禁止 172.24.250.0/24 的域对 `servera` 和 `serverb` 进行 SSH

### 4. 完成主 DNS 配置

---

- ☐ 当前我们已经配置好了DNS服务，要求
  - ☐ 在 `servera` 配置主DNS，域名为 `lab.example.com`
  - ☐ 配置正向解析 `servera`, `serverb`
  - ☐ 配置反向解析 172.25.250.10, 172.25.250.11

### 5. 准备 samba 共享

---

在 `servera` 上准备 samba 共享

- ☐ 创建共享文件夹 `/common`
- ☐ 用户 `rob` 验证的密码是 `compede`
- ☐ 用户 `brian` 验证的密码是 `postroll`

### 6. 使用多用户访问 samba 共享目录

---

在 `servera` 上配置SMB服务

- ☐ 您的SMB服务器必须是 `STAFF` 工作组的一个成员
- ☐ 共享 `/common` 目录共享名必须为 `common`
- ☐ 只有 `example.com` 域内的客户端可以访问 `common` 共享
- ☐ `common` 必须是可以浏览的
- ☐ 用户 `rob` 必须能够读取共享中的内容

- ☐ 要求 `rob` 用户以只读的方式访问该目录，`brian` 可以用读写的方式来访问该目录

在 `serverb` 上，要求通过 `smb` 多用户的方式将共享目录 `common` 挂载到 `/mnt/private` 上

- ☐ 要求在对该共享目录挂载时，以 `rob` 的身份进行操作
- ☐ 要求每次开机该共享目录可以自动挂载

## 7. 配置 NFS 服务

在 `servera` 配置 NFS 服务，要求如下：

- ☐ 以只读的方式共享目录 `/public` 同时只能被 `example.com` 域中的系统访问
- ☐ 以读写的方式共享目录 `/protected` 能被 `example.com` 域中的系统访问
- ☐ 目录 `/protected` 应该包含名为 `project` 拥有人为 `student` 的子目录
- ☐ 用户 `student` 能以读写方式访问 `/protected/project`

## 8. 挂载一个 NFS 共享

在 `serverb` 上挂载一个来自 `servera` 的 NFS 共享，并符合下列要求：

- ☐ `/public` 挂载在下面的目录上 `/mnt/nfsmount`
- ☐ `/protected` 挂载在下面的目录上 `/mnt/nfssecure`
- ☐ 用户 `student` 能够在 `/mnt/nfssecure/project` 上创建文件
- ☐ 这些文件系统在系统启动时自动挂载

## 9. 配置 iSCSI 服务端

配置 `servera` 提供一个 iSCSI 服务，磁盘名为 `iqn.2014-11.com.example:servera`，并符合下列要求：

- ☐ 服务端口为 `3260`
- ☐ 使用 `iscsi_store` 作其后端卷 其大小为 `3G`
- ☐ 此服务只能被 `serverb.lab.example.com` 访问
- ☐ 后端卷为 `LVM` 形式

## 10. 配置 iSCSI 的客户端

配置 `serverb` 使其能连接 在 `servera` 上提供的 `iqn.2014-11.com.example:servera` 并符合以下要求：

- ☐ iSCSI 设备在系统启动的期间自动加载
- ☐ 块设备 iSCSI 上包含一个大小为 `2100MiB` 的分区，并格式化为 `ext4`
- ☐ 此分区挂载在 `/mnt/data` 上，同时在系统启动的期间自动挂载

## 11. 搭建 MariaDB

在 `servera` 上配置一个数据库服务器，然后执行下述步骤：

- ☐ 仅 `localhost` 登录。使用帐户 `root`。密码 `redhat`
- ☐ 将<http://materials/classroom/database-working/inventory.dump>文件下载，并恢复 `contacts` 库
- ☐ 按以下要求设置数据库访问用户  
用户名 `mary`，密码 `mary_password`，对 `contacts` 数据库所有数据有 `选择` 权限

## 12. 数据查询填空1

完成以下要求的查询并将结果填入相应的框格中。

- ☐ 查询 `RT-AC68U` 产品的供应商名称为\_\_\_\_\_

## 13. 数据查询填空2

完成以下要求的查询并将结果填入相应的框格中。

- ☐ 查询类型是 `Servers`，且供应商是 `Lenovo` 的产品有多少\_\_\_\_\_种

## 14. 实现一个 web 服务器

在 `servera` 上配置一个站点<http://www0.lab.example.com>然后执行下述步骤：

- ☐ 从<http://materials/www0.html>下载文件
- ☐ 并且将文件重命名为 `index.html` 不要修改此文件的内容
- ☐ 将文件 `index.html` 拷贝到您的web服务器的 `DocumentRoot` 目录下
- ☐ 来自于 `lab.example.com` 域的客户端可以访问此web服务
- ☐ 来自于 `lab.example.org` 域的客户端拒绝访问此Web服务

## 15. 配置安全 web 服务

站点<http://www0.lab.example.com>配置TLS加密

- ☐ 一个已签名证书从<http://materials/www0.lab.example.com.crt>获取
- ☐ 此证书的密钥从<http://materials/www0.lab.example.com.key>获取
- ☐ 此证书的签名授权信息从<http://materials/example-ca.crt>获取

## 16. 配置虚拟主机

在 `servera` 上扩展您的web服务器，

为站点<http://webapp0.lab.example.com>创建一个虚拟主机，然后执行下述步骤：

- ☐ 设置DocumentRoot为 `/var/www/virtual`
- ☐ 从<http://materials/webapp0.html>下载文件
- ☐ 并重命名为 `index.html` 不要对文件index.html的内容做任何修改
- ☐ 将文件index.html放到虚拟机的DocumentRoot目录下，确保 `floyd` 用户能够在/var/www/virtual目录下创建文件

注意：原始站点<http://www0.lab.example.com>必须仍然能够访问，  
名称服务器 `bastion.lab.example.com` 提供对主机名 `webapp0.lab.exmple.com` 的域名解析

## 17. 配置web内容的访问

在您的 `servera` 上的 web 服务器的 DocumentRoot 目录下创建一个名为 `private` 的目录，要求如下：

- ☐ 从<http://materials/permission.html>下载一个文件副本到这个目录，并且重命名为 `index.html`
- ☐ 不要对这个文件的内容做任何修改
- ☐ 从 `servera` 上，任何人都可以浏览 `private` 的内容，但是从其它系统不能访问这个目录的内容

## 18. 通过 ansible 布署 Nginx

在 `serverc` 和 `serverd` 上配置一个站点，然后执行下述步骤：

- ☐ 在 `playbooks` 目录下，创建剧本 `nginx.yml`
- ☐ 从<http://foundation0.ilt.example.com/nginx.conf.j2>下载jinja模板文件
- ☐ 从<http://materials/nginx.html>下载文件，并且将文件重命名为 `index.html` 不要修改此文件的内容
- ☐ 将文件 `index.html` 拷贝到您的 web 服务器的 DocumentRoot 目录下 `/www/src/html`

## 19. 通过 ansible 配置 firewall

在 `serverc` 和 `serverd` 上分别设置，针对SSH

- ☐ 在 `playbooks` 目录下，创建剧本 `firewall.yml`
- ☐ 允许 `172.25.250.0/24` 的域对 `serverc` 和 `serverd` 进行 `SSH`
- ☐ 禁止 `172.24.250.0/24` 的域对 `serverc` 和 `serverd` 进行 `SSH`

## 20. 通过 ansible 配置空邮件客户端

在系统 `serverc` 和 `serverd` 上配置邮件服务，满足以下要求：

- ☐ 在 `playbooks` 目录下，创建剧本 `nullclients.yml`
- ☐ 这些系统不能接收外部发送来的邮件
- ☐ 在这些系统上本地发送的任何邮件都会自动路由到 `smtp.lab.example.com`
- ☐ 从这些系统上发送的邮件显示来自于 `lab.example.com`
- ☐ 您可以通过发送邮件到本地用户 `student` 来测试您的配置，系统 `smtp.lab.example.com` 已经配置
- ☐ 可以通过如下网址测试 `http://bastion/mail`

## 21. 通过 ansible 部署打印机

---

在系统 `serverc` 和 `serverd` 上配置打印机，满足以下要求：

- ☐ 在 `playbooks` 目录下，创建剧本 `printer-create.yml`
- ☐ 安装打印机为默认打印机
- ☐ printer queue `new-printer`
- ☐ URI地址 `ipp://serverc:631/printers/rht-printer`