



一、系统管理部分

环境说明 ——

真机（无 root 权限）：room9pc13.tedu.cn

资源服务器-虚拟机（提供 DNS/YUM/认证/素材...）：classroom.example.com

虚拟机（有 root 权限）：server0.example.com

#####

准备工作：

00a、将系统的 root 账号密码设置为 **redhat**。

00b、配置您的虚拟机系统使用下述静态网络配置。

- ☐ Hostname: **server0.example.com**
- ☐ IP address: **172.25.0.11**
- ☐ Netmask: **255.255.255.0**
- ☐ Gateway: **172.25.0.254**
- ☐ Name server: **172.25.254.254**

#####

01. 为您的系统指定一个默认的软件仓库

YUM 的软件库源为 http://content.example.com/rhel7.0/x86_64/dvd, 将此配置为您的系统的默认软件仓库。

02. 配置一个用户帐户

创建一个名为 athena 的用户，用户 ID 是 3456。密码是 tomato

03. 管理用户账号、组账号

创建下列用户、组以及和组的成员关系：

- ☐ 一个名为 teachers 的组
- ☐ 一个名为 jerry 的用户，其属于 teachers，这个组是该用户的从属组
- ☐ 一个名为 tom 的用户，属于 teachers，这个组是该用户的从属组
- ☐ 一个名为 huloo 的用户，其在系统中没有可交互 shell，并且不属于 teachers 组
- ☐ jerry、tom、和 huloo 的密码都要设置为 tomato

04. 复制文件并配置文件权限

拷贝文件/etc/fstab 到/var/tmp/fstab，配置文件/var/tmp/fstab 的权限：

- ☐ 文件/var/tmp/fstab 的拥有者是 root 用户
- ☐ 文件/var/tmp/fstab 属于 root 组
- ☐ 文件/var/tmp/fstab 对任何人都不可执行
- ☐ 用户 jerry 能够对文件/var/tmp/fstab 执行读和写操作
- ☐ 用户 tom 对文件/var/tmp/fstab 既不能读，也不能写
- ☐ 所有其他用户（当前的和将来的）能够对文件/var/tmp/fstab 进行读操作



05. 创建共用目录

创建一个共用目录 `/home/rhcedir`，特性如下：

- ☐ `/home/rhcedir` 目录的组所有权是 `teachers`
- ☐ `root` 用户和 `teachers` 组的成员对此目录有读写和执行的权限，除此之外的其他所有用户没有任何权限
- ☐ 在 `/home/rhcedir` 目录中创建的文件，其组所有权会自动设置为属于 `teachers` 组

06. 配置 cron 计划任务

为用户 `jerry` 配置一个定时任务，每天在本地时间 10:30 时执行以下命令：

```
/bin/echo haha > /tmp/jerry.log
```

07. 升级 Linux 系统内核

新版内核可从 http://classroom/content/rhel7.0/x86_64/errata/Packages/ 获取。

升级你的系统内核，同时要满足下列要求：

- ☐ 当系统重新启动之后升级的内核要作为默认的内核
- ☐ 原来的内核要保留，并且仍然可以正常启动

08. 绑定到 LDAP 验证服务

配置您的系统使用服务器 `classroom.example.com` 提供的 LDAP 验证服务。

- ☐ 验证服务器的基本 DN 是：`dc=example,dc=com`
- ☐ 帐户信息和验证信息都由 LDAP 提供
- ☐ 连接要使用证书进行加密，证书可以在下面的链接中下载：
<http://classroom.example.com/pub/example-ca.crt>
- ☐ 当正确完成配置后，用户 `ldapuser0` 应该能够登录到您的系统，当您完成 `autofs` 的题目之后，此用户才能使用主目录
- ☐ `ldapuser0` 用户的密码是 `password`（已预先配好）

09. 配置 autofs 按需挂载

按照下述要求配置 `autofs` 用来自动挂载 LDAP 用户的主目录：

- ☐ 服务器 `classroom.example.com` 通过 NFS 输出 `/home/guests` 目录到您的系统，这个文件系统已预先配好包含用户 `ldapuser0` 的主目录
- ☐ `ldapuser0` 用户的主目录是 `classroom.example.com:/home/guests/ldapuser0`
- ☐ `ldapuser0` 的主目录应该挂载到本地的 `/home/guests/ldapuser0` 目录下
- ☐ 用户对其主目录必须是可写的
- ☐ `ldapuser0` 用户的密码是 `password`（已预先配好）

10. 配置 NTP 网络时间客户端

配置您的系统，让其作为一个 `classroom.example.com` 的 NTP 客户端



11. 查找文件

找出所有用户 student 拥有的文件，并且把它们拷贝到 /root/results 目录中

12. 查找文本内容

在文件 /usr/share/dict/words 中查找到所有包含字符串 tasia 的行：

- ☐ 将找出的行按照原文的先后顺序拷贝到 /root/wlist 文件中
- ☐ /root/wlist 文件中不要包含空行

13. 创建一个归档

创建一个名为 /root/backup.tar.bz2 的归档文件，其中包含 /usr/local 目录中的内容，tar 归档必须使用 bzip2 进行压缩

14. 创建一个逻辑卷

根据下面的要求创建一个新的逻辑卷：

- ☐ 逻辑卷命名为 database，属于 datastore 卷组，并且逻辑卷的大小为 50 个物理扩展单元 (physical extent)
- ☐ 在 datastore 卷组中的逻辑卷，物理扩展单元 (physical extent) 大小应为 16 MiB
- ☐ 使用 ext3 文件系统对新的逻辑卷进行格式化，此逻辑卷应该在系统启动的时候自动挂载在 /mnt/database 目录下

15. 逻辑卷扩容

将逻辑卷 vo 和其文件系统大小调整到 300 MiB。要确保文件系统中的内容保持完整。

16. 添加新的 swap 分区

在您的系统中添加一个大小为 512 MiB 的 swap 分区：

- ☐ 当您的系统启动时，swap 分区应该可以自动挂载

二、综合应用部分

环境说明 ——

真机（无 root 权限）：room9pc13.tedu.cn

资源服务器-虚拟机（提供 DNS/YUM/认证/素材...）：**classroom.example.com**

虚拟机 1（有 root 权限）：**server0.example.com**

虚拟机 2（有 root 权限）：**desktop0.example.com**

#####

01. 配置 SELinux

确保您的两个系统的 SELinux 处于强制启用模式。

02. 配置 SSH 访问控制

按以下要求配置 SSH 访问：

- ☐ 用户能够从域 **example.com** 内的客户端 SSH 远程访问您的两个虚拟机系统
- ☐ 在域 **unknown.org** 内的客户端不能访问您的两个虚拟机系统

03. 自定义用户环境（别名设置）

在系统 server0 和 desktop0 上创建自定义命令为 **qstat**，此自定义命令将执行以下命令：
/bin/ps -Ao pid,tt,user,fname,rsz
此命令对系统中所有用户有效。

04. 配置防火墙端口转发

在系统 server0 配置端口转发，要求如下：

- ☐ 在 172.25.0.0/24 网络中的客户机，访问 server0 的本地端口 5423 将被转发到 80
- ☐ 此设置必须永久有效

05. 配置链路聚合

在您的两个系统之间配置一个聚合链路 team0：

- ☐ 此链路使用接口 eth1 和 eth2（预先提供或自行添加接口）
- ☐ 此链路在一个接口失效时仍然能工作；
- ☐ 此链路在 server0 使用地址 **172.16.3.20/255.255.255.0**
- ☐ 此链路在 desktop0 使用地址 **172.16.3.25/255.255.255.0**
- ☐ 此链路在系统重启之后依然保持正常状态

06. 配置 IPv6 地址

在您的考试系统上配置接口 eth0 使用下列 IPv6 地址：

- ☐ server0 上的地址应该是 2003:ac18::305/64



- ☐ desktop0 上的地址应该是 2003:ac18::306/64
- ☐ 两个系统必须能与网络 2003:ac18/64 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

07. 配置本地邮件服务

在系统 server0 上配置邮件服务，满足以下要求：

- ☐ 这些系统不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 `smtp0.example.com`
- ☐ 从这些系统上发送的邮件显示来自于 `desktop0.example.com`

您可以通过在 server0 上发送邮件到本地用户 student 来测试您的配置，系统 `desktop0.example.com` 上的用户 student 将会收到这封邮件。

08. 配置默认 web 站点

为 `http://server0.example.com` 配置 Web 服务器：

- ☐ 从 `http://classroom.example.com/pub/materials/station.html` 下载一个主页文件，并将该文件重命名为 `index.html`
- ☐ 将文件 `index.html` 拷贝到您的 web 服务器的 DocumentRoot 目录下
- ☐ 不要对文件 `index.html` 的内容进行任何修改

09. 配置虚拟主机

在 server0 上扩展您的 web 服务器，为站点 `http://www0.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://classroom.example.com/pub/materials/www.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` 放到虚拟主机的 DocumentRoot 目录下
- ☐ 确保 `student` 用户能够在 `/var/www/virtual` 目录下创建文件

注意：原始站点 `http://server0.example.com` 必须仍然能够访问，名称服务器 `classroom.example.com` 提供对主机名 `www0.example.com` 的域名解析。

10. 配置安全 web 服务

为站点 `http://server0.example.com` 配置 TLS 加密：

- ☐ 已签名证书从 `http://classroom.example.com/pub/tls/certs/server0.crt` 获取
- ☐ 证书的密钥从 `http://classroom.example.com/pub/tls/private/server0.key` 获取
- ☐ 证书的签名授权信息从 `http://classroom.example.com/pub/example-ca.crt` 获取

11. 配置 web 内容的访问

在您的 server0 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://classroom.example.com/pub/materials/private.html> 下载一个文件副本到这个目录，并且得命名为 index.html
- ☐ 不要对这个文件的内容做任何修改
- ☐ 从 server0 上，任何人都可以浏览 private 的内容，但是从其他系统不能访问这个目录的内容

12. 实现动态 WEB 内容

在 server0 上配置提供动态 Web 内容，要求如下：

- ☐ 动态内容由名为 webapp0.example.com 的虚拟主机提供
- ☐ 虚拟主机侦听在端口 8909
- ☐ 从 <http://classroom.example.com/pub/materials/webinfo.wsgi> 下载一个脚本，然后放在适当的位置，无论如何不要修改此文件的内容
- ☐ 客户端访问 <http://webapp0.example.com:8909> 可接收到动态生成的 Web 页
- ☐ 此 <http://webapp0.example.com:8909> 必须能被 example.com 域内的所有系统访问

13. 通过 Samba 发布共享目录

在 server0 上通过 SMB 共享 /common 目录：

- ☐ 您的 SMB 服务器必须是 STAFF 工作组的一个成员
- ☐ 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 harry 必须能够读取共享中的内容，如果需要的话，验证的密码是 migwhisk

14. 配置多用户 Samba 挂载

在 server0 通过 SMB 共享目录/devops，并满足以下要求：

- ☐ 共享名为 devops
- ☐ 共享目录 devops 只能被 example.com 域中的客户端使用
- ☐ 共享目录 devops 必须可以被浏览
- ☐ 用户 kenji 必须能以读的方式访问此共享，该密码是 atenorth
- ☐ 用户 chihiro 必须能以读写的方式访问此共享，访问密码是 atenorth
- ☐ 此共享永久挂载在 desktop0.example.com 上的 /mnt/dev 目录，并使用用户 kenji 作为认证，任何用户可以通过用户 chihiro 来临时获取写的权限

15. 配置 NFS 共享服务

在 server0 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
- ☐ 访问/protected 需要通过 Kerberos 安全加密，您可以使用下面 URL 提供的密钥：
<http://classroom.example.com/pub/keytabs/server0.keytab>
- ☐ 目录/protected 应该包含名为 project 拥有人为 ldapuser0 的子目录
- ☐ 用户 ldapuser0 能以读写方式访问/protected/project



16. 挂载 NFS 共享

在 desktop0 上挂载一个来自 server0.example.com 的共享，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 并使用安全的方式,密钥下载 URL:
<http://classroom.example.com/pub/keytabs/desktop0.keytab>
- ☐ 用户 ldapuser0 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

17. 配置 iSCSI 服务端

配置 server0 提供 iSCSI 服务，磁盘名为 iqn.2016-02.com.example:server0，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 3GiB
- ☐ 此服务只能被 desktop0.example.com 访问

18. 配置 iSCSI 客户端

配置 desktop0 使其能连接 server0 上提供的 iqn.2016-02.com.example:server0，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 文件系统
- ☐ 此分区挂载在 /mnt/data 上，同时在系统启动的期间自动挂载

19. 编写简单脚本

在 server0 上创建一个名为 /root/foo.sh 的脚本，让其提供下列特性：

- ☐ 当运行 /root/foo.sh redhat，输出为 fedora
- ☐ 当运行 /root/foo.sh fedora，输出为 redhat
- ☐ 当没有任何参数或者参数不是 redhat 或者 fedora 时，其错误输出产生以下的信息：
/root/foo.sh redhat|fedora

20. 创建批量添加用户的脚本

在 server0 上创建一个脚本，名为 /root/batchusers，此脚本能实现为系统 server0 创建本地用户，并且这些用户的用户名来自一个包含用户名的文件，同时满足下列要求：

- ☐ 此脚本要求提供一个参数，此参数就是包含用户名列表的文件
- ☐ 如果没有提供参数，此脚本应该给出下面的提示信息 Usage: /root/batchusers <userfile> 然后退出并返回相应的值
- ☐ 如果提供一个不存在的文件名，此脚本应该给出下面的提示信息 Input file not found 然后退出并返回相应的值
- ☐ 创建的用户登陆 Shell 为 /bin/false，此脚本不需要为用户设置密码
- ☐ 您可以从下面的 URL 获取用户名列表作为测试用：
<http://classroom.example.com/pub/materials/userlist>



21. 配置一个数据库

在 server0 上创建一个 MariaDB 数据库，名为 Contacts，并符合以下条件：

- ☐ 数据库应该包含来自数据库复制的内容，复制文件的 URL 为：
<http://classroom.example.com/pub/materials/users.sql>
- ☐ 数据库只能被 localhost 访问
- ☐ 除了 root 用户，此数据库只能被用户 Raikon 查询，此用户密码为 atenorth
- ☐ root 用户的密码为 atenorth，同时不允许空密码登陆。

22. 数据库查询（填空）

在系统 server0 上使用数据库 Contacts，并使用相应的 SQL 查询以回答下列问题：

- ☐ 密码是 solicitous 的人的名字？
- ☐ 有多少人的姓名是 Barbara 同时居住在 Sunnyvale？