2022 年全国职业院校技能大赛

网络系统管理赛项

模块 C：Linux 部署

卷 II

ChinaSkills

目 录

一、竞赛说明

1. **竞赛环境确认：**选手入场后请根据竞赛所提供的《竞赛环境确认单》，依次检查所列的硬件设备、软件、材料、U 盘内竞赛答题卡等是否齐全，软硬件设备是否能正常使用，检查完毕后在《竞赛环境确认单》上签字并上交。
2. **试卷确认：**竞赛分发试题后请检查试题名称是否与当前考核模块相符，试题内容无缺页、模糊问题。
3. **安全操作：**竞赛过程安全操作，注意赛位电源线位置，操作时不要碰到，及时进行设备配置保存，以防误碰电缆导致设备断电配置丢失情况。
4. **竞赛成果物提交确认：**评分将以各参赛队提交的竞赛提交物为主要评分依据。请按照 U 盘中答题卡要求创建和编辑竞赛成果物，确保答题卡截图信息清晰完整，并在竞赛结束时提交，所有提交的内容必须按照“竞赛成果物提交要求”进行命名并签署《竞赛成果提交确认单》。
5. **离场要求：**竞赛结束时，所有设备保持运行状态，不要拆掉网络连接。禁止将竞赛用的所有物品（包括试卷和草纸）带离赛场。
6. **竞赛成果提交物：**请在 U 盘根目录建立“竞赛成果物”文件夹，文件夹中包含以下内容：
   - Linux 部署答题卡.pdf

二、初始化环境

（一）默认账号及默认密码

Username: root

Password: ChinaSkill!

Username: skills

Password: ChinaSkill!

注：若非特别指定，所有账号的密码均为 ChinaSkill!

（二）操作系统配置

所处区域：CST + 8

系统环境语言：English US (UTF-8)

键盘：English US

注意：当任务是配置 TLS，请把根证书或者自签名证书添加到受信任区。

控制台登陆后不管是网络登录还是本地登录 ，都按下方欢迎信息内容显示。

****

ChinaSkills 2022 - CSK

Module C Linux

>>hostname<<

>>OS Version<<

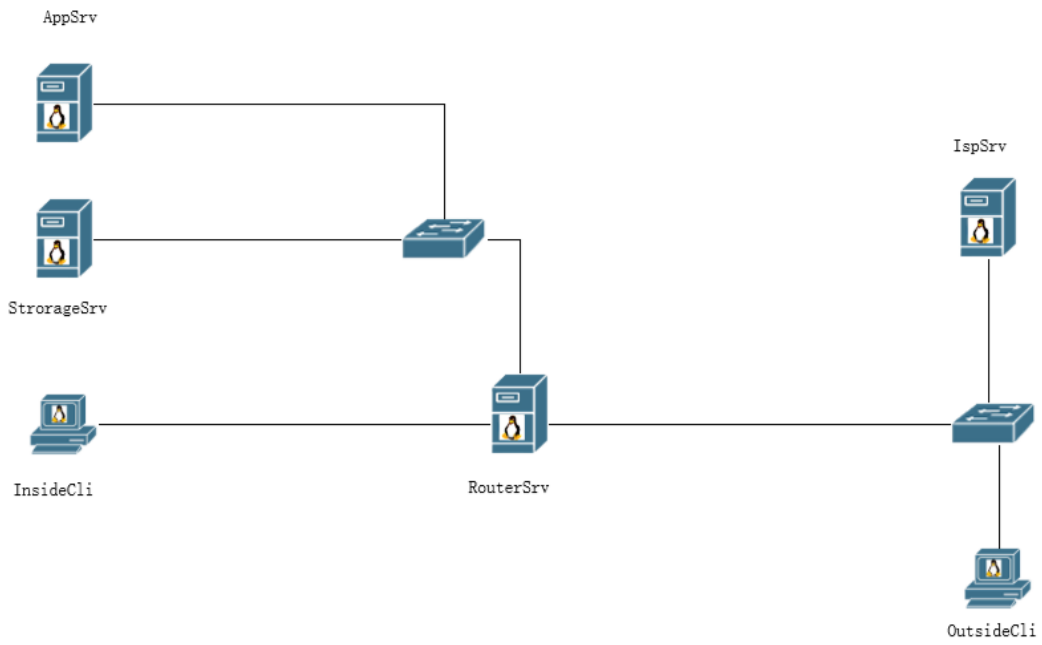
>> TIME <<

****

三、项目任务描述

你作为一个 Linux 的技术工程师，被指派去构建一个公司的内部网络，要为员工提供便捷、安全稳定内外网络服务。你必须在规定的时间内完成要求的任务，并进行充分的测试，确保设备和应用正常运行。任务所有规划都基于 Linux 操作系统，请根据网络拓扑、基本配置信息和服务需求完成网络服务安装与测试。网络拓扑图和基本配置信息如下：

（一）拓扑图



（二）网络地址规划

服务器和客户端基本配置如下表，各虚拟机已预装系统。

Device	System	FQDN	IP/Mask/Gateway
IspSrv	UOS	ispsrv	81.6.63.100/24/无
OutsideCli	UOS	outsidecli.chinaskills.cn	81.6.63.110/24/无
AppSrv	Centos	appsrv.chinaskills.cn	192.168.100.100/24/192.168.100.254
StorageSrv	Centos	storagesrv.chinaskills.cn	192.168.100.200/24/192.168.100.254

RouterSrv	Centos	routersrv.chinaskills.cn	192.168.100.254/24/无、 192.168.0.254/24/无、 81.6.63.254/24/无
InsideCli	Centos	insidecli.chinaskills.cn	DHCP From AppSrv

四、项目任务清单

（一）服务器 IspSrv 工作任务

1.DNS

- 配置为 DNS 根域服务器；
- 其他未知域名解析,统一解析为该本机 IP；
- 创建正向区域“chinaskills.cn”；
  - 类型为 Slave；
  - 主服务器为“AppSrv”；
- 启用 chroot 功能，限制 bind9 在/var/named/chroot/下运行；隐藏 bind 版本号，版本显示为“unknow”。

2.WEB 服务

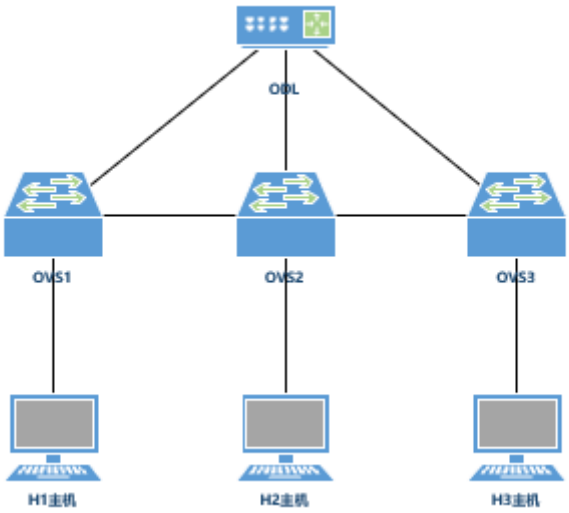
- 安装 nginx 软件包；
- 配置文件名为 ispweb.conf，放置在/etc/nginx/conf.d/目录下；
- 网站根目录为/mut/crypt（目录不存在需创建）；
- 启用 FastCGI 功能，让 nginx 能够解析 php 请求；
- index.php 内容使用 Welcome to 2022 Computer Network Application contest!

3.SDN

- 在 IspSrv 上导入 OpenDayLight 软件包；
- 启动 OpenDayLight 的 karaf 程序，并安装如下组件：

```
feature:install odl-restconf
feature:install odl-l2switch-switch-ui
feature:install odl-mdsal-apidocs
feature:install odl-dluxapps-applications
```

- 使用 Mininet 和 OpenVswitch 构建拓扑，连接 ODL 的 6653 端口如下拓扑结构：



- 在浏览器上可以访问 ODL 管理页面查看网元拓扑结构；
- 通过 OVS 给 S2 下发流表，使得 H2 与 H1、H3 无法互通；
- H1 启动 HTTP-Server 功能，WEB 端口为 8080，H3 作为 HTTP-Client，获取 H1 的 html 网页配置文件。

（二）服务器 RouterSrv 上的工作任务

1. DHCP RELAY

- 安装 DHCP 中继；
- 允许客户端通过中继服务获取网络地址。

2. ROUTING

- 根据题目要求，开启路由转发，为当前实验环境提供路由功能。

3. SSH

- 工作端口为 2021；
- 只允许用户 user01，登录到 routersrv。其他用户（包括 root）不能登录；
- 通过 ssh 尝试登录到 RouterSrv，一分钟内最多尝试登录的次数为 3 次，超过后禁止该客户端网络地址访问 ssh 服务；
- 记录用户登录的日志到/var/log/ssh.log，日志内容要包含：源地址，目标地址，协议，源端口，目标端口。

4.IPTABLES

- 添加必要的网络地址转换规则，使外部客户端能够访问到内部服务器上的 dns、mail、web 和 ftp 服务；
- INPUT、OUTPUT 和 FOREARD 链默认拒绝（DROP）所有流量通行；
- 配置源地址转换允许内部客户端能够访问互联网区域。

5.Web Proxy

- 安装 Nginx 组件；
  - 配置文件名为 proxy.conf，放置在/etc/nginx/conf.d/目录下；
  - 为 www.chinaskills.cn 配置代理前端，通过 HTTPS 的访问后端 Web 服务器；
  - 后端服务器日志内容需要记录真实客户端的 IP 地址；
  - 缓存后端 Web 服务器上的静态页面；
- 创建服务监控脚本：/shells/chkWeb.sh；
  - 编写脚本监控公司的网站运行情况；
  - 脚本可以在后台持续运行；
  - 每隔 3S 检查一次网站的运行状态，如果发现异常尝试 3 次；
  - 如果确定网站无法访问，则返回用户“The site is being maintained”。

6.OPENVPN

- 要求服务器日志记录客户端登录时间、用户名，格式如“2022-08-10:08:10:30 Successful authentication: username=″vpnuser1″”；日志文件存放至/var/log/openvpn.log 中；
- 创建用户 vpnuser1,密码为 123456，使用用户名密码认证，要求只能与 InsideCli 客户端网段通信，允许访问 StorageSrv 主机上的 SAMBA 服务；
- VPN 地址范围为 172.16.0.0/24，OPENVPN 使用 tcp 1194 端口号进行工作。

（三）服务器 AppSrv 上的工作任务

1.SSH

- 安装 SSH，工作端口监听在 2101；

- 仅允许 InsideCli 客户端进行 ssh 访问，其余所有主机的请求都应该拒绝；
- 在 cskadmin 用户环境下可以免秘钥登录，并且拥有 root 控制权限。
- 将 SSH 跟 SFTP 进行分离，要求 SFTP 监听端口为 54321，并且通过服务的方式进行启动或停止。

2.DHCP

- 为 InsideCli 客户端网络分配地址，地址池范围：192.168.0.110-192.168.0.190/24；
- 域名解析服务器：按照实际需求配置 DNS 服务器地址选项；
- 网关：按照实际需求配置网关地址选项；
- 为 InsideCli 分配固定地址为 192.168.0.190/24；
- 设置默认租约时间为 0.5 天，最大租约时间为 3 天；
- 将 DHCP 服务的日志信息从系统的日志服务中分离，通过 rsyslog 自定义消息处理，将日志信息保存至/var/log/dhcpd.log 中。

3.DNS

- 为 chinaskills.cn 域提供域名解析；
- 为 www.chinaskills.cn、download.chinaskills.cn 和 mail.chinaskills.cn 提供解析；
- 启用内外网解析功能，当内网客户端请求解析的时候，解析到对应的内部服务器地址，当外部客户端请求解析的时候，请把解析结果解析到提供服务的公有地址；
- 请将 IspSrv 作为上游 DNS 服务器，所有未知查询都由该服务器处理。

4.web 服务

- 安装 WEB 服务；
  - 服务以用户 webuser 系统用户运行；
  - 限制 web 服务只能使用系统 500M 物理内存；
  - 全站点启用 TLS 访问，使用本机上的“CSK Global Root CA”颁发机构颁发，网站证书信息如下：

    C = CN
    ST = China
    L = BeiJing
    O = skills
    OU = Operations Departments
    CN = *.chinaskills.cn
  - 客户端访问 https 时应无浏览器（含终端）安全警告信息；
  - 当用户使用 http 访问时自动跳转到 https 安全连接；

- 搭建 www.chinaskills.cn 站点；
  - 网页文件放在 StorgeSrv 服务器上；
  - 在 StorageSrv 上安装 MriaDB,在本机上安装 PHP,发布 WordPress 网站；
  - MariaDB 数据库管理员信息：User: root/ Password: Chinaskill21!
- 创建网站 download.chinaskills.cn 站点；
  - 仅允许 ldsgp 用户组访问；
  - 网页文件存放在 StorageSrv 服务器上；
  - 在该站点的根目录下创建以下文件“test.mp3, test.mp4, test.pdf”，其中 test.mp4 文件的大小为 100M，页面访问成功后能够列出目录所有文件；
  - 安全加固，在任何页面不会出现系统和 WEB 服务器版本信息。

5.Mariadb Backup Script

- 脚本文件：/shells/mysqlbk.sh；
- 备份数据到/root/mysqlbackup 目录；
- 备份脚本每隔 30 分钟实现自动备份；
- 导出的文件名为 all-databases-20210213102333,其中 20210213102333 为运行备份脚本的当前时间，精确到秒。

6.MAIL

- 安装配置 postfix 和 dovecot，启用 imaps 和 smtps，禁止使用不安全的 smtp 和 imap 发送和接收邮件；
- 安装配置 postfixadmin；
- 创建虚拟域 chinaskills.cn 以及 99 个邮件用户 mailuser1～mailuser99.虚拟用户映射至本地用户 vmail 和用户组 vmail，UID 和 GID 均为 2000；
- 使用 mailuser1@chinaskills.cn 的邮箱向 mailuser2@chinaskills.cn 的邮箱发送一封测试邮件，邮件标题为“just test mail from mailuser1”，邮件内容为“hello , mailuser2”。
- 使用 mailuser2@chinaskills.cn 的邮箱向 mailuser1@chinaskills.cn 的邮箱发送一封测试邮件，邮件标题为“just test mail from mailuser2”，邮件内容为“hello , mailuser1”；
- 添加广播邮箱地址 all@chinaskills.cn，当该邮箱收到邮件时，mailuser1 和 mailuser2 用户都能在自己的邮箱中查看；使用

mailuser1@chinaskills.cn 向 all@chinaskills.cn 发送测试邮件，邮件标题为“test all”，邮件内容为“hello ,test all”；

- 使用 https://mail.chinaskills.cn 网站测试邮件发送与接收。

7.CA（证书颁发机构）

- CA 根证书路径/csk-rootca/csk-ca.pem；
- 签发数字证书，颁发者信息：(仅包含如下信息)

C = CN
ST = China
L = BeiJing
O = skills
OU = Operations Departments
CN = CSK Global Root CA

8.网桥 VXLAN 服务

- 在 appsrv 和 storagesrv 上搭建 vxlan。需求如下，
- 安装实验网桥
- 新建 vxlan 隧道，网桥名称为 br-vxlan,网桥的出口为 vxlan100，id 为 100.
- appsrv 的隧道地址为 172.16.1.1/24，storagesrv 的隧道地址为 172.16.1.2/24.
- 测试网桥之间二层的联通性。

（四）服务器 StorageSrv 上的工作任务

1.磁盘管理

- 在 storagesrv 上新加一块 10G 磁盘；
- 创建 vdo 磁盘，并开启 vdo 磁盘的重删和压缩；
- 名字为 vdodisk，大小为 150G，文件系统为 ext4；
- 并设置开机自动挂载。挂载到/vdodata。

2.SSH

- 安装 openssh 组件；
- 创建的 user01、user02 用户允许访问 ssh 服务；
- 服务器本地 root 用户不允许访问；
- 修改 SSH 服务默认端口，启用新端口 2022；

- 添加用户 user01、user02 到 sudo 组，用于远程接入，提权操作。

3.NFS

- 共享/webdata/目录；
- 用于存储 AppSrv 主机的 WEB 数据；
- 仅允许 AppSrv 主机访问该共享；
- 考虑安全，不论登入 NFS 的使用者身份为何，都将其设置为匿名用户访问。

4.VSFTPD

- 禁止使用不安全的 FTP，请使用“CSK Global Root CA”证书颁发机构，颁发的证书，启用 FTPS 服务；
- 创建虚拟用户 webuser，登录 ftp 服务器，根目录为/webdata，上传的文件映射为 webadmin；
- 登录后限制在自己的根目录；
- 允许 WEB 管理员上传和下载文件，但是禁止上传后缀名为.doc .docx .xlsx 的文件；
- 限制用户的下载最大速度为 100kb/s;最大同一 IP 在线人数为 2 人；
- 通过工具或者浏览器下载的最大速度不超过 100kb/s；
- 一个 IP 地址同时登陆的用户进程/人数不超过 2 人；
- 采用随机端口用户客户端跟服务器的数据传输,并限制传输端口为 40000-41000 之间。

5.SAMBA

- 创建 samba 共享，本地目录为/data/share1，要求：
  - 共享名为 share1；
  - 仅允许 zsuser 用户能上传文件；
- 创建 samba 共享，本地目录为/data/public，要求：
  - 共享名为 public。
  - 允许匿名访问。
  - 所有用户都能上传文件。

6.LDAP

- 安装 slapd,为 samba 服务提供账户认证；
- 创建 chinaskills.cn 目录服务，创建 users 组织单元，并创建用户组 ldsgp ,将 zsuser、lsusr、wuusr 加入 ldsgp 组。

7.ShellScript

- 编写添加用户的脚本,存储在/shells/userAdd.sh 目录；
- 当有新员工入职时，管理员运行脚本为其创建公司账号；
- 自动分配客户端账号、公司邮箱、samba 目录及权限、网站账号等；
- 以 userAdd lifei 的方式运行脚本，lifei 为举例的员工姓名。

8.Cockpit

- 安装 cockpit 来监测 ispsrv 服务器的状态。

9.系统优化

- 系统资源限制设置：设置所有用户的硬件跟软件的最大进程数、最大文件打开数为 65535；
- 开启 IPV4 恶意 icmp 错误消息保护；
- 开启 SYN 洪水攻击保护；
- 允许系统打开的端口范围为 1024-65000。

10.磁盘快照

- 新增 15G 的磁盘，并将其做成 LVM 卷，VG 名称为 snapvg，LV 名称为 snaplv 大小为 5G，挂载至/snapdata 目录下；
- 写入文本的文件数据至/snapdata 目录下，名称为 cs.txt，内容为“this is test！”；
- 对 LV 卷进行快照，要求创建的逻辑卷快照为只读，快照名称为 snapsrc；
- 删除 cs.txt 文件，将快照挂载至/snap 目录下，进行文件数据的恢复。

（五）客户端 OutsideCli 和 InsideCli 工作任务

1.OutsideCli

- 作为 DNS 服务器域名解析测试的客户端，安装 nslookup、dig 命令行工具；
- 作为网站访问测试的客户端，安装 firefox 浏览器，curl 命令行测试工具；
- 作为 SSH 远程登录测试客户端，安装 ssh 命令行测试工具；
- 作为 SAMBA 测试的客户端，使用图形界面文件浏览器测试,并安装 smbclient 工具；

- 作为 FTP 测试的客户端，安装 lftp 命令行工具；
- 作为防火墙规则效果测试客户端，安装 ping 命令行工具；
- 截图的时候请使用上述提到的工具进行功能测试。

2.InsideCli

- 作为 DNS 服务器域名解析测试的客户端，安装 nslookup、dig 命令行工具；
- 作为网站访问测试的客户端，安装 firefox 浏览器，curl 命令行测试工具；
- 作为 SSH 远程登录测试客户端，安装 ssh 命令行测试工具；
- 作为 SAMBA 测试的客户端，使用图形界面文件浏览器测试,并安装 smbclient 工具；
- 作为 FTP 测试的客户端，安装 lftp 命令行工具；
- 作为防火墙规则效果测试客户端，安装 ping 命令行工具；
- 截图的时候请使用上述提到的工具进行功能测试。