**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

（样题8）



**目录**

[一、 初始化环境 4](#_Toc15758)

[1.默认账号及默认密码 4](#_Toc22002)

[2.操作系统配置 4](#_Toc15469)

[二、 项目任务描述 4](#_Toc30712)

[1.拓扑图 5](#_Toc16021)

[2.网络地址规划 5](#_Toc27768)

[三、 项目任务清单 6](#_Toc21839)

[服务器IspSrv工作任务 6](#_Toc7221)

[1. DHCP 6](#_Toc30834)

[2. DNS 6](#_Toc29025)

[3. WEB服务 7](#_Toc15436)

[服务器RouterSrv上的工作任务 7](#_Toc24148)

[1. DHCP RELAY 7](#_Toc17431)

[2. ROUTING 7](#_Toc29359)

[3. SSH 7](#_Toc15602)

[4. IPTABLES 7](#_Toc15094)

[5. Web Proxy 8](#_Toc19887)

[服务器AppSrv上的工作任务 8](#_Toc17835)

[1. SSH 8](#_Toc2545)

[2. DHCP 8](#_Toc16994)

[3. DNS 8](#_Toc11127)

[4. WEB服务 9](#_Toc4721)

[5. Mariadb Backup Script 10](#_Toc10887)

[6. MAIL 10](#_Toc8231)

[7. CA（证书颁发机构） 10](#_Toc22223)

[服务器StorageSrv上的工作任务 11](#_Toc14510)

[1. SSH 11](#_Toc23611)

[2. DISK 11](#_Toc17923)

[3. NFS 11](#_Toc15249)

[4. VSFTPD 11](#_Toc29097)

[5. SAMBA 11](#_Toc15566)

[6. LDAP 12](#_Toc15876)

[7. ShellScript 12](#_Toc20897)

[客户端OutsideCli和InsideCli工作任务 12](#_Toc21376)

[1. OutsideCli 12](#_Toc20591)

[2. InsideCli 12](#_Toc26605)

# **初始化环境**

## **1.默认账号及默认密码**

Username: root

Password: ChinaSkill22!

Username: skills

Password: ChinaSkill22!

注：若非特别指定，所有账号的密码均为 ChinaSkill22!

## **2.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<<

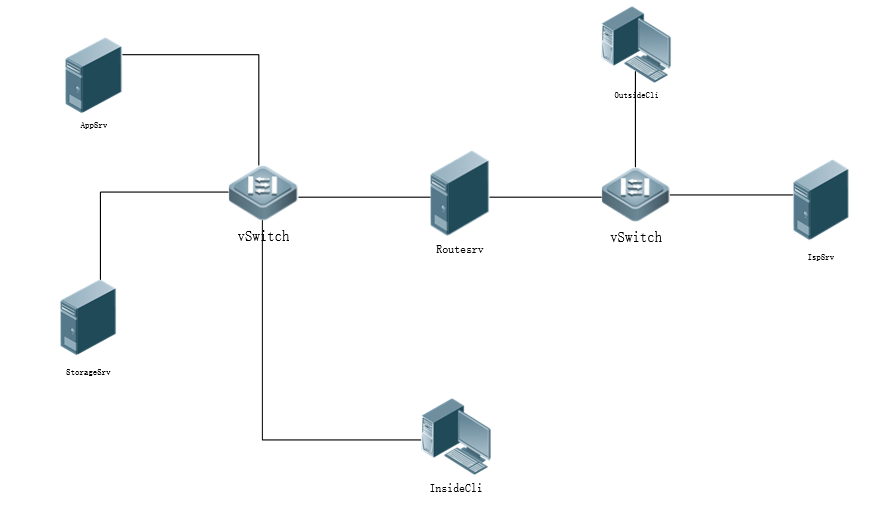
>> TIME <<

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

# **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：

## **1.拓扑图**



## **2.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。

**ISPSRV（UOS）**

* + - * 完全限定域名：ispsrv
      * 普通用户/登录密码：skills/ChinaSkill22
      * 超级管理员/登录密码：root/ChinaSkill22
      * 网络地址/掩码/网关：81.6.63.100/24/无

**AppSrv(Centos)**

* + - * 完全限定域名：appsrv.chinaskills.cn
      * 普通用户/登录密码：skills/ChinaSkill22
      * 超级管理员/登录密码：root/ChinaSkill22
      * 网络地址/掩码/网关：192.168.100.100/24/192.168.100.254

**STORAGESRV(Centos)**

* + - * 完全限定域名：storagesrv.chinaskills.cn
      * 普通用户/登录密码：skills/ChinaSkill22
      * 超级管理员/登录密码：root/ChinaSkill22
      * 网络地址/掩码/网关：192.168.100.200/24/192.168.100.254

**ROUTERSRV(Centos)**

* + - * 完全限定域名：routersrv.chinaskills.cn
      * 普通用户/登录密码：skills/ChinaSkill22
      * 超级管理员/登录密码：root/ChinaSkill22
      * 网络地址/掩码/网关： 192.168.100.254/24/无、192.168.0.254/24/无、81.6.63.254/24/无

**INSIDECLI(Centos)**

* + - * 完全限定域名：insidecli.chinaskills.cn
      * 普通用户/登录密码：skills/ChinaSkill22
      * 超级管理员/登录密码：root/ChinaSkill22
      * 网络地址/掩码/网关：DHCP From AppSrv

**OUTSIDECLI（UOS）**

* + - * 完全限定域名：outsidecli.chinaskills.cn
      * 普通用户/登录密码：skills/ChinaSkill22
      * 超级管理员/登录密码：root/ChinaSkill22
      * 网络地址/掩码/网关：DHCP From IspSrv

# **项目任务清单**

## **服务器IspSrv工作任务**

1. **DHCP**
   * + - 为OutsideCli客户端网络分配地址，地址池范围：81.6.63.110-81.6.63.190/24；
       - 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；
2. **DNS**
   * + - 安装BIND9；
       - 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”；
3. **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!

## **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**
   * + - 开启路由转发，为当前实验环境提供路由功能。
       - 根据题目要求，配置单臂路由实现内部客户端和服务器之间的通信。
3. **SSH**
   * + - 工作端口为2021；
       - 只允许用户user01，密码ChinaSkill21登录到router。其他用户（包括root）不能登录，创建一个新用户，新用户可以从本地登录，但不能从ssh远程登录。
       - 通过ssh登录尝试登录到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“网站正在维护中，请您稍后再试”的页面。

## **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。
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。
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.co](http://www.skbt.cn)m

* + - * + 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。
        + 作安全加固，在任何页面不会出现系统和WEB服务器版本信息。

1. **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。
2. **MAIL**
   * + - 安装配置postfix和dovecot，启用imaps和smtps，并创建测试用户mailuser1和mailuser2。
       - 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，所有用户都能在自己的邮箱中查看。
       - 使用https://mail.chinaskills.cn网站测试邮件发送与接收。
3. **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

## **服务器StorageSrv上的工作任务**

1. **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 3358；
       - 添加用户user01 user02 到sudo组；用于远程接入，提权操作。
2. **DISK**
   * + - 添加大小均为10G的虚拟磁盘，配置raid-5磁盘。
       - 创建LVM命名为/dev/vg01/lv01，大小为100G，格式化为ext4，挂在到本地目录/webdata，在分区内建立测试空文件disk.txt。
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。
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；
       - 用户webadmin，登录ftp服务器，根目录为/webdata/；
       - 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；
         * 用于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。
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，并创建用户组ldsgp ,将zsuser、lsusr、wuusr。
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。

## **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。