**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1）



**目录**

[一、 初始化环境 3](#_Toc11958)

[1.默认账号及默认密码 3](#_Toc19297)

[2.操作系统配置 3](#_Toc7854)

[二、 项目任务描述 3](#_Toc12749)

[1.拓扑图 4](#_Toc30346)

[2.基本配置 5](#_Toc32374)

[3.任务需求 5](#_Toc13048)

*[CLIENT TASK](#_Toc1173)* [6](#_Toc1173)

*[RSERVER TASK](#_Toc1667)* [6](#_Toc1667)

*[SERVER01 TASK](#_Toc4055)* [7](#_Toc4055)

*[SERVER02 TASK](#_Toc11314)* [9](#_Toc11314)

*[SERVER03 TASK](#_Toc15627)* [10](#_Toc15627)

[SERVER04 TASK 11](#_Toc27632)

# **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<<

>>Linux Version<<

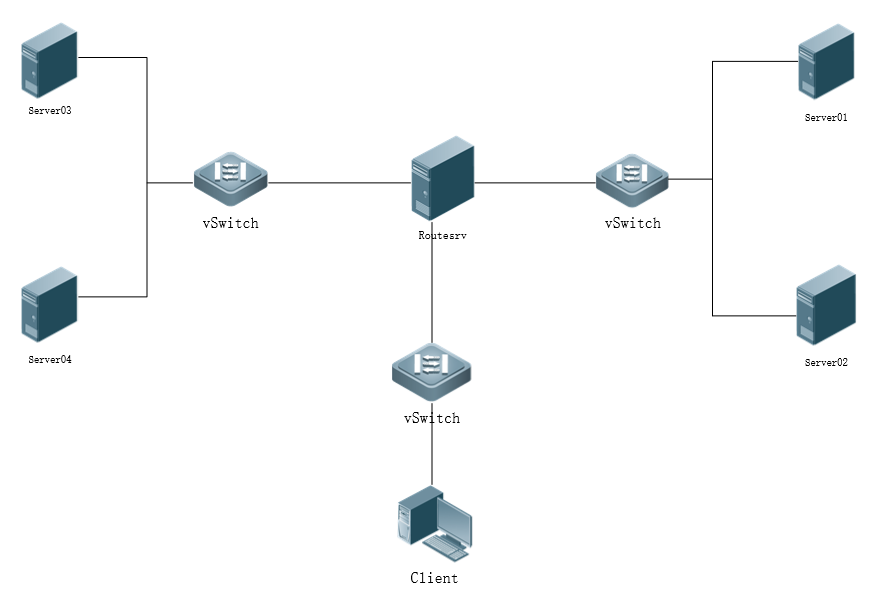
>> TIME <<

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

# **项目任务描述**

某公司要为员工提供便捷、安全稳定内外网络服务，你作为一个公司网络系统管理员，负责公司网络系统管理，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.基本配置**

服务器和客户端基本配置如下表，各虚拟机已预装系统。

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Device | Hostname | **System** | FQDN | IP Address | Service |
| Server01 | Server01 | Centos | Server01.sdskills.com | 172.16.100.201 | RAID5  NFS  DNS  Webserver  SSH  DBMS  SDN |
| Server02 | Server02 | Centos | Server02.sdskills.com | 172.16.100.202 | Ftp  Mail  SSH |
| Server03 | Server03 | UOS | Server03.skills.com | 192.168.10.3 | Ntp,  SSH |
| Server04 | Server04 | UOS | Server04.skills.com | 192.168.10.X | DNS  Webserver  SSH  LDAP |
| Rserver | Rserver | Centos | Rserver.skills.com  Rserver.sdskills.com | 172.16.100.254  192.168.10.2  10.10.100.254 | proxy  firewall  dhcp  SSH  CA |
| Client | Client | Centos |  | 10.10.100.x | none |

网络

|  |  |
| --- | --- |
| Network | CIDR |
| office | 10.10.100.0/24 |
| service | 172.16.100.128/25 |
| internet | 192.168.10.0/28 |

## **3.任务需求**

任务设备：Client,Rserver,servr01,server02,server03,server04。

注意：若题目中未明确规定，请使用默认配置。

### *CLIENT TASK*

**1.Client相关任务，具体要求如下：**

* 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。

### *RSERVER TASK*

**1.NETWORK**

* 请根据基本配置信息配置服务器的主机名，网卡IP地址配置、域名等。

**2.squid**

* 安装squid服务，开启路由转发，为当前实验环境提供路由功能；

**3.Iptables**

* 默认阻挡所有流量
* 添加必要的NAT规则和流量放行规则，正常情况下Internet网络不能访问office网络，满足使所有要求中的服务正常提供工作。

**4.DHCP**

* 为客户端分配IP范围是10.10.100.1-10.10.100.50；
* DNS：按照实际需求配置DNS服务器地址选项；
* GATEWAY：按照实际需求配置网关地址选项。

**5.SSH**

安装SSH

仅允许client客户端进行ssh访问，其余所有主机的请求都应该拒绝；

配置client只能在Chinaskill22用户环境下可以免秘钥登录，端口号为2022，并且拥有root控制权限。

**6.CA**

* CA根证书路径/CA/cacert.pem；
* 签发数字证书，颁发者信息：

国家 = CN

单位 = Inc

组织机构 = www.skills.com

公用名 = Skill Global Root CA

* 创建用户组ldsgp ,将zsuser、lsusr、wuusr添加到组内。

**7. 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。

### *SERVER01 TASK*

**1.NETWORK**

* + 请根据基本配置信息配置服务器的主机名，网卡IP地址配置、域名服务器、网关等。

**2.DISK(RAID5)**

* + - 在虚拟机上添加 4 个 1G 的硬盘；
      * 创建 raid5，其中一个作为热备盘, 设备名为md0;
      * 将 md0 设置为 LVM，设备为/dev/vg01/lv01；
        + 格式化为 ext4 文件系统;
        + 开机自动挂载到/data 目录。

**3.NFS**

* 共享/data/share目录；
* 用于存储server01主机的web数据；
* 仅允许service01主机访问该共享。

**4.DNS**

* + - 安装DNS服务相关软件包；
    - 建立sd[skills.com](http://www.skbt.cn)域，为所有除Internet区域的主机或服务器建立正\反的域名解析;
    - 当出现无法解析的域名时，向域[skills.com](http://www.mhls.com)申请更高层次的解析。

**5.Webserver**

* + - 安装web服务相关软件包；
    - 由Server01提供www.sdskills.com
    - skills公司的门户网站；
    - 使用apache服务；
    - 网页文件放在/data/share/htdocs/skills；
    - 服务以用户webuser运行；
    - 首页内容为“This is the front page of sdskills's website.”;
    - /htdocs/skills/staff.html内容为“Staff Information”；
    - 该页面需要员工的账号认证才能访问；
    - 员工账号存储在ldap中，账号为zsuser、lsus
  + 网站使用https协议；
    - SSL使用RServer颁发的证书, 颁发给:

C = CN

ST = China

L = ShangDong

O = skills

OU = Operations Departments

CN = [\*.skills.co](http://www.skbt.cn)m

* + - Sever01的CA证书路径：/CA/cacert.pem
    - 签发数字证书，颁发者：

C = CN;

O = Inc

OU = www.skills.com

CN = skill Global Root CA

* + - 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；
    - 当用户使用sdskills.com或any.sdskills.com（any代表任意网址前缀）访问时，自动跳转到[www.sdskills.co](http://www.skbt.cn)m。

**6.SSH**

* 安装SSH
* 仅允许client客户端进行ssh访问，其余所有主机的请求都应该拒绝；
* 配置client只能在Chinaskill22用户环境下可以免秘钥登录，端口号为3033，并且拥有root控制权限；

**7.DBMS**

* 在Server01上完成MariaDB数据库的安装，添加数据库root用户密码为Chinaskill22!
* 安装MariaDB 数据库服务器组件;
* MariaDB数据库管理员信息：User: root/ Password: Chinaskill20!；
* 安装MariaDB WEB 管理面板 “phpMyAdmin”，通过apache 进行发布
* 安装phpMyAdmin ，MariaDB 的web管理面板组件；
* 安装apache，配置php环境，用于发布phpMyAdmin；

**8.SDN服务**

* 安装opendaylight、mininet、Ovs软件平台。。
* 启动OpenDayLight的karaf程序，安装如下组件：odl-restconf、odl-l2switch-switch-ui、odl-mdsal-apidocs、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手工下发流表，H1可以ping通H3，H1、H3无法ping通H2。
* 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。

### *SERVER02 TASK*

**1.NETWORK**

* 请根据基本配置信息配置服务器的主机名，网卡IP地址配置、域名服务器、网关等。

**2.Ftp**

* 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。

**3.MAIL**

* Postfix
* sdskill.com 的邮件发送服务器
  + 支持smtps(465)协议连接，使用Rserver颁发的证书,证书路径/CA/cacert.pem
  + 创建邮箱账户“user1~user99”（共99个用户），密码为Chinaskill20!；
* **Dovecot**
  + sdskill.com 的邮件接收服务器；
  + 支持imaps（993）协议连接，使用Rserver颁发的证书，证书路径/CA/cacert.pem；
  + 请保留至少两个用户已成功登录并能正常收发邮件，以方便测试.

**4.SSH**

* 安装SSH
* 仅允许client客户端进行ssh访问，其余所有主机的请求都应该拒绝；
* 配置client只能在Chinaskill22用户环境下可以免秘钥登录，端口号为4044，并且拥有root控制权限；

### *SERVER03 TASK*

**1.NETWORK**

* 请根据基本配置信息配置服务器的主机名，网卡IP地址配置、域名服务器、网关等。

**2.chrony**

* chrony为全网提供时间同步服务器；
* Server01、Server02、Server04、Client和Rserver应定期与其校正时间；
* 每隔1分钟自动校正一次时间。

**3.SSH**

* 安装SSH
* 仅允许client客户端进行ssh访问，其余所有主机的请求都应该拒绝；
* 配置client只能在Chinaskill20用户环境下可以免秘钥登录，端口号为2233，并且拥有root控制权限；

### SERVER04 TASK

**1.NETWORK**

* + 请根据基本配置信息配置服务器的主机名，网卡IP地址配置、域名服务器、网关等。

**2.DNS**

* + 安装DNS相关服务软件包；
  + 为域[skills.com](http://www.skbt.cn)提供必要的域名解析
  + 当非[skills.com](http://www.skbt.cn)域的解析时，统一解析到Rserver连接Internet网段的IP地址或Rserver.[skills.com](http://www.skbt.cn)

**3.Webserver**

* + - 提供www.skills.com
    - skills公司的门户网站；
    - 使用apache服务；
    - 网页文件放在/htdocs/skills；
    - 服务以用户webuser运行；
    - 首页内容为“This is the front page of skills's website.”;
    - /htdocs/sdskills/staff.html内容为“Staff Information”；
    - 该页面需要员工的账号认证才能访问；
    - 员工账号存储在ldap中，账号为zsuser、lsus
    - 网站使用https协议；
    - SSL使用RServer颁发的证书, 颁发给:

C = CN

ST = China

L = ShangDong

O = skills

OU = Operations Departments

CN = [\*.skills.cn](http://www.skbt.cn)

* + - Rserver的CA证书路径：/CA/cacert.pem
    - 签发数字证书，颁发者：

C = CN;

O = Inc

OU = www.skills.com

CN = skill Global Root CA

* + - 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；
    - 当用户使用skills.cn或any.skills.cn（any代表任意网址前缀）访问时，自动跳转到[www.skills.co](http://www.skbt.cn)m。

**4.SSH**

* + 安装SSH
  + 仅允许client客户端进行ssh访问，其余所有主机的请求都应该拒绝；
  + 配置client只能在Chinaskill22用户环境下可以免秘钥登录，端口号为3344，并且拥有root控制权限；

**5.LDAP**

* + 安装openldap,为apache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。