2020年全国职业院校技能大赛

改革试点赛

网络系统管理（样题五）

模块A：Linux环境



**全国职业院校技能大赛执委会.技术专家组**

**2020年09月**

目录

[一、竞赛介绍 3](#_Toc31688)

[1.登录 3](#_Toc1519)

[2.系统配置 3](#_Toc15312)

[3.竞赛环境 3](#_Toc23967)

[二、竞赛时间 3](#_Toc11410)

[三、竞赛注意事项 4](#_Toc26246)

[四、竞赛结果文件的提交 4](#_Toc14446)

[五、项目任务描述 5](#_Toc9952)

[1.拓扑图 5](#_Toc17596)

[2.基本配置 6](#_Toc11903)

[3.任务需求 7](#_Toc27232)

*[CLIENT TASK](#_Toc16812)* [7](#_Toc16812)

*[RSERVER TASK](#_Toc30635)* [7](#_Toc30635)

*[SERVER01 TASK](#_Toc19450)* [9](#_Toc19450)

*[SERVER02 TASK](#_Toc11868)* [11](#_Toc11868)

*[SERVER03 TASK](#_Toc25269)* [12](#_Toc25269)

*[SERVER04 TASK](#_Toc1751)* [13](#_Toc1751)

# **一、竞赛介绍**

比赛规定开始时间和结束时间，请合理分配您的时间。

请仔细阅读以下要求！

比赛时间结束时，请将您工作站保持运行状态，评分会在您保持的运行状态进行。不允许重新启动，关机的机器不会再启动。

以下信息请用于所有服务器和客户端：

## **1.登录**

Username: root

Password: ChinaSkill20!

Username: Chinaskill20

Password: Chinaskill20!

注：若非特别指定，所有账号的密码均为 Chinaskill20!

## **2.系统配置**

Region: China

Locale: English US (UTF-8)

Key Map: English US

当任务是配置SSL或者TLS，如要求隐藏所有警告，请小心执行。

## **3.竞赛环境**

物理机 (HOST)：

文件夹路径：

虚拟机:[datastore1]（VMware ESXI）

ISO 镜像：[DATA]ISO/（VMware ESXI）

软件： D:\软件 (Host)

# **二、竞赛时间**

竞赛时间为4小时。

# **三、竞赛注意事项**

1. 竞赛所需的硬件、软件和辅助工具由组委会统一布置，选手不得私自携带任何软件、移动存储、辅助工具、移动通信等进入赛场。

2. 请根据大赛所提供的比赛环境，检查所列的硬件设备、软件清单、材料清单是否齐全，计算机设备是否能正常使用。

3. 操作过程中，需要及时保存设备配置。比赛结束后，所有设备保持运行状态，不要拆动硬件连接。

4. 比赛完成后，比赛设备、软件和赛题请保留在座位上，禁止将比赛所用的所有物品（包括试卷和草纸）带离赛场。

5. 裁判以各参赛队提交的竞赛结果文档为主要评分依据。所有提交的文档必须按照赛题所规定的命名规则命名，不得以任何形式体现参赛院校、工位号等信息。

# **四、竞赛结果文件的提交**

按照题目要求，提交符合模板的WORD文件以及对应的PDF文件（利用Office Word另存为pdf文件方式生成pdf文件），所有截图建议除了配置文件截图外，还需要截功能测试的图，能在终端client上测试的就一定要在终端上测试并截图，否则功能测试部分不得分。

# **五、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**



**Server01**

**Server02**

**Server03**

**Server04**

**Client**

**Rserver**

## **2.基本配置**

服务器和客户端基本配置如下表：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Device | Hostname | System | FQDN | IP Address | Service |
| Server01 | Server01 | Linux serve（预装） | Server01.sdskills.gov | 172.16.100.201 | RAID5  NFS  DNS（bind）  Webserver(apache)  SSH  DBMS |
| Server02 | Server02 | Linux serve（待安装） | Server02.sdskills.gov | 172.16.100.202 | Ftp(vsftpd)  Mail(postfix,dovecot)  Samba |
| Server03 | Server03 | Linux server（预装） | Server03.skills.gov | 192.168.10.3 | Ntp(chrony)  SSH  Vpn(openvpn) |
| Server04 | Server04 | Linux server（待安装） | Server04.skills.gov | 192.168.10.X | DNS（bind）  Webserver(apache)  SSH |
| Rserver | Rserver | Linux server（预装） | Rserver.skills.gov  Rserver.sdskills.gov | 172.16.100.254  192.168.10.2  10.10.100.254 | Proxy(squid)  Firewall(iptables)  DHCP  SSH  CA  Shellscript(bash) |
| Client | Client | Linux Desktop（预装） |  | 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：**已预装简易Debian，具体要求如下：

* 要求能访问所有服务器，用于测试应用服务。
* 请为该主机安装支持GNOME桌面环境。
* 调整显示分辨率至1280x768；
* 测试DHCP，该主机网卡IPv4地址为自动获取；
* 测试dns，安装dnsutils、dig 命令行工具；
* 测试web，安装firefox 浏览器, curl 命令行测试工具，在任何时候进行访问测试时不允许弹出安全警告信息；
* 测试ssh，安装ssh 命令行工具；
* 测试VPN，安装VPN客户端工具软件；
* 测试ftp，安装ftp命令行客户端工具；
* 测试文件共享，安装Samba命令行客户端工具；
* 测试mail，安装thunderbird，并能正常进行邮件收发；
* 其他设定均采用默认设定。

### *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Chinaskill20用户环境下可以免秘钥登录，端口号为2222，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.gov

公用名 = Skill Global Root CA

**7.Shellscript(bash)**

* 安装bash;
* 服务监控脚本：/shells/chkWeb.sh;
  + 在Rserver上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.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service网段访问该共享。

**4.DNS(bind)**

* + - 安装bind服务；
    - 建立sd[skills.gov](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.gov](http://www.mhls.com)申请更高层次的解析。

**5.Webserver(apache)**

* + - 安装apache服务；
    - 由Server01提供www.sdskills.gov
    - 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.shills.gov

CN = shill 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.gov或any.sdskills.gov（any代表任意网址前缀）访问时，自动跳转到[www.sdskills.gov](http://www.skbt.cn)。

**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Chinaskill20用户环境下可以免秘钥登录，端口号为3333，并且拥有root控制权限；

**7.DBMS(MariaDB)**

* 在Server01上完成MariaDB数据库的安装，添加数据库root用户密码为Chinaskill20!
* 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。

### *SERVER02 TASK*

**1.System install**

* 完成系统的安装，桥接网卡，把网卡桥接到service网段的虚拟交换机上。

**2.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。

**3.Ftp(vsftpd）**

* 使用ftp服务上传网页代码。
  + 使用vsftpd服务；
  + ftp的上传文件根目录即为web服务器的网站根目录；
  + ftp登录的用户为ftpuser；
  + 通过ftp上传的文件用户为webuser, 文件权限为644，目录权限为755。

**4.MAIL**

* **Postfix**
  + sdskill.gov 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.gov 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。

**5.Samba**

* 安装与配置Samba共享服务；
* 创建目录为/share/public的共享目录；
  + 共享名为public；
  + 仅支持匿名用户的只读访问（请在该目录内存放一个文件名为file.txt，文件内容为“Test File”以便于测试）；
* 创建目录为/share/files的共享目录；
  + 共享名为files；
  + 创建zhangsan，wangwu两个用户，密码均为Skills39，并且都能从client客户端登录访问到该共享目录并上传文件；
  + zhangsan用户可以查看和删除所有人的文件；
  + wangwu用户只能查看和删除自己的文件，不能查看和删除别人的文件。

### *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。

**4.Openvpn**

* 安装Openvpn服务;
* Client的客户端可以通过VPN拨号连接到SERVER03。
* VPN客户端拨号使用命令systemctl start openvpn@SERVER03；
* 比赛结束时请保持客户端VPN是未连接的状态。

### *SERVER04 TASK*

**1.System install**

* 完成系统的安装，桥接网卡，把网卡桥接到Internet网段的虚拟交换机上。

**2.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。

**3.DNS(bind)**

* + - 安装bind服务；
    - 为域[skills.gov](http://www.skbt.cn)提供必要的域名解析;
    - 当非[skills.gov](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.gov](http://www.skbt.cn)。

**4.Webserver(apache2)**

* + 提供www.skills.gov
    - 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.shills.gov

CN = shill 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。

**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Chinaskill20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。