测试项目 - 样题

***山东省职业技能大赛***

***网络系统管理项目模块A-Linux环境***

目 录

[《测试项目》简介 3](#_Toc1711)

[介绍 3](#_Toc17885)

[项目和任务的描述 3](#_Toc22449)

[登录所有虚拟机和设备： 3](#_Toc15951)

[系统环境要求： 4](#_Toc22422)

[选手须知 5](#_Toc8)

[网络结构 5](#_Toc22224)

[连接信息 5](#_Toc6993)

[基本信息 5](#_Toc1966)

[安全配置 5](#_Toc6053)

[任务需求 6](#_Toc8330)

[外部网络提供的服务 6](#_Toc29616)

[DMZ区域提供的服务 7](#_Toc10283)

[内部网络提供的服务 9](#_Toc23210)

[客户端测试 10](#_Toc1612)

[内部客户端测试 10](#_Toc24886)

[外部客户端测试 11](#_Toc377)

[所需的设备、机械、装置和材料 12](#_Toc28253)

[网络表 12](#_Toc23702)

[网络（逻辑）图 13](#_Toc22894)

[网络（物理）图 14](#_Toc6600)

# 《测试项目》简介

以下是提交的所有《测试项目》提案中必须包含的章节或信息清单。

* 目录，包括组成《测试项目》的所有文件、图纸和照片的清单
* 介绍/概述
* 项目和任务的简短描述
* 选手须知
* 完成《测试项目》所需的设备、机械、装置和材料
* 《评分方案》（包括评估标准）
* 其他

# 介绍

此《测试项目》由以下文档/文件组成：

* 山东省职业技能大赛网络系统管理项目-模块A-Linux-样题.docx
* users.csv

随着业务的不断增长，保障应用系统持续稳定性一直是信息技术的挑战。当事情变得复杂，现有系统的架构无法满足高性能、可扩展以及安全可靠的需求。Delix 公司决定处理这个问题，并雇佣你来对他们的基础设施进行现代化改造，强化和拓展。

# 项目和任务的描述

所有的虚拟机都已经预安装了Debian Linux操作系统。你可以使用这些虚拟机来开发及测试你的工作。

### 登录所有虚拟机和设备：

用户名 : root / skills

密码: GDSkills-2023

如果以下未特别说明，账号的密码均为“GDSkills-2023”（不含引号）。

### 系统环境要求：

Region: China

Locale: English US (UTF-8)

Key Map: English US

当任务需要配置SSL或者TLS时，应该要隐藏所有客户端警告。

出于测试目的，所有主机都应该装以下测试工具：curl, wget, lynx, nslookup, dig, ftp, lftp, showmount, smbclient, ssh, telnet, traceroute, ntpdate, lsof, nmap, mail

# 选手须知

## 网络结构

### 连接信息

* 外部网络:SERVER01,SERVER02,CLIENT01
* DMZ区域：SERVER03,SERVER04,SERVER05
* 内部网络：SERVER06,SERVER07,SERVER08,CLIENT02
* ROUTER01负责连接外部网络和内部网络
* ROUTER02负责连接内部网络和DMZ区域
* SWITCH01负责DMZ区域中的设备连接
* SWITCH02负责内部网络中的设备连接

### 基本信息

* 所有主机按照网络表完成初始化设置
* 所有应用的用户信息均来自于users.csv

### 安全配置

* 在ROUTER01上开启路由功能，配置防火墙(iptables)规则
  + 外部网络通过DNAT访问DMZ区域对外提供的服务
  + 内部网络，DMZ区域通过SNAT访问外部网络
  + 使用icmp-host-prohibited响应禁用其他所有INPUT和FORWARD数据流量
* 在ROUTER02上开启路由功能，配置防火墙(iptables)规则
  + 内部网络可以访问DMZ区域对内提供的服务
  + DMZ区域可以访问内部网络提供的存储服务
  + 使用icmp-host-prohibited响应禁用其他所有INPUT和FORWARD数据流量

## 任务需求

### 外部网络提供的服务

* **NTP服务**
  + 在SERVER01安装和配置chrony作为ntp服务器
  + 所有设备都应与其进行时间同步
* **CA服务**
  + 在SERVER02提供权威证书签名颁发服务
    - CA证书及其私钥应位于/ca-inf目录下
    - CA证书cacert.pem，CA私钥cakey.pem
    - common name为“GDSkills CA”
    - 本测试项目中所有应用所需的证书均由此CA颁发
* **DNS服务**
  + 在SERVER02安装和配置bind9作为DNS服务器
  + 为gdisp.cn和appsrv.com配置域名解析
  + 查询非法域名应答状态为“NXDOMAIN”
    - 非法域名如下：
      * virus01.net -- virus99.net(01至99连续)
      * www.xvsex.com, xvsex.com, \*.xvsex.com
      * soso4972.fun, soso4972.cc, soso4972.live, soso4972.art
  + 查询其他域名应CNAME到www.gdisp.cn
* **Web服务**
  + 在SERVER01安装和配置Nginx作为Web服务器
    - 全站启用https
    - 使用http访问会自动跳转(301)到https
    - 证书信息：
      * 公用名(CN): gdisp.cn
      * 组织(O): GDISP Corporation
      * 组织单位(OU): GDISP Technology
      * 有效期：730天
    - 禁止通过IP地址或其他域名访问
    - 不暴露服务器系统和应用的版本信息
  + [www.gdisp.cn](http://www.gdisp.cn)
    - 网站根目录/htdocs/gdisp/www
    - 支持PHP，开启OPCache缓存
    - 首页为测试页面index.php,显示<?php phpinfo(); ?>输出信息
    - 访问gdisp.cn自动跳转(301)到www.gdisp.cn
  + repos.gdisp.cn
    - 提供Debian 11系统镜像的网络源
    - 启用apt源URL为https://repos.gdisp.cn/
    - 能够通过浏览器访问到目录下的软件包列表
* **CDN服务**
  + 在SERVER02安装和配置Squid作为CDN服务器
  + 为https://www.gdisp.cn提供静态资源缓存加速

### DMZ区域提供的服务

* **Web服务**
  + 在SERVER04上安装和配置Nginx作为web服务器
  + 在SERVER05上安装和配置Apache作为Web服务器
  + 在SERVER03上安装和配置HAProxy作为负载均衡器
  + Nginx负责处理静态文件的请求
  + Apache负责处理动态文件的请求
  + HAProxy负责处理请求分发
  + 全站启用https
  + 使用http访问会自动跳转(301)到https
  + 证书信息：
    - 公用名(CN): appsrv.com
    - 组织(O): APPSRV Corporation
    - 组织单位(OU): APPSRV Technology
    - 有效期：730天
  + 禁止通过IP地址或其他域名访问
  + 不暴露服务器系统和应用的版本信息
  + [a](http://www.gdisp.cn)ppsrv.com
    - 网站根目录/htdocs/appsrv/www
    - 网站数据应存放在内部网络提供的存储服务中
    - 支持PHP，开启OPCache缓存
    - 测试页面test.php,显示<?php phpinfo(); ?>输出信息
    - 访问www.appsrv.com自动跳转(301)到appsrv.com
    - 安装部署wordpress
      * 开启伪静态
      * 支持用户注册
      * 发布一篇名“山东省职业技能大赛”为文章
        + 文章链接:https://appsrv.com/3rd-gdskills/
        + 文章内容：上传一张分辨率不小于400x400的png格式的图片
  + api.appsrv.com
    - 使用Django框架安装并配置一个REST API服务器
    - 配置API服务器与SERVER07的数据库服务进行通信
  + mail.appsrv.com
    - 采用Roundcube
* **邮件服务**
  + 在SERVER04上安装和配置Postfix,Dovecot作为邮件服务器
  + appsrv.com后缀的邮箱
  + 启用SSL/TLS
    - 仅支持SMTPS和IMAPS
    - 使用与Web服务相同的证书
  + 启用邮件群发功能
    - 向各部门邮箱发送邮件，其部门成员都能收到
    - 向all@appsrv.com邮箱发送邮件，所有人都能收到

### 内部网络提供的服务

* **存储服务**
  + 在SERVER07上安装和配置Mariadb作为数据库服务器
    - 存储appsrv.com的数据
    - 数据库root用户仅能凭密码从本地登录
    - 仅dbadmin用户凭密码可从DMZ区域登录
  + 在SERVER08上安装和配置NFS作为数据存储共享服务器
    - 存储appsrv.com的文件
    - 共享/share/website目录
      * 只允许DMZ区域访问
      * 自动挂载到网站根目录
* **代理服务**
  + 在SERVER06上安装和配置Squid作为代理服务器
    - 内部网络访问外部网站时需要使用该代理
    - 只允许CLIENT02使用
    - 禁止访问外部网络中的非法域名
* **DHCP服务**
  + 在SERVER06上安装和配置dhcpd作为DHCP服务器
    - 为内部网络客户端提供DHCP服务
    - IP地址范围192.168.1.201 - 192.168.1.250
    - 分配置正确的网关
    - 分配置正确的DNS服务器地址
* **DNS服务**
  + 在SERVER06上安装和配置bind作为DNS服务器
    - 为appsrv.com提供域名解析服务
    - 其他域名请求应转发到SERVER02上的DNS服务器
    - 仅允许内部网络访问
* **VPN服务**
  + 在SERVER06上安装和配置OpenVPN作为VPN服务器
    - 外网客户端可通过VPN连接访问到内部网络
    - 使用客户端证书进行身份验证

## 客户端测试

### 内部客户端测试

* **DHCP服务**
  + 自动获取IP地址及其他网络信息
* **NTP服务**
  + 自动与NTP服务器同步时间
* **DNS服务**
  + 解析DMZ区域服务域名
  + 解析外部网络服务域名
* **Web服务**
  + 访问DMZ区域Web应用
* **代理服务**
  + 使用代理访问外部网络Web服务
* **邮件服务**
  + 使用evolution客户端
  + 配置为ID号为6的用户的邮箱
  + 其他用户可通过Webmail登录邮箱

### 外部客户端测试

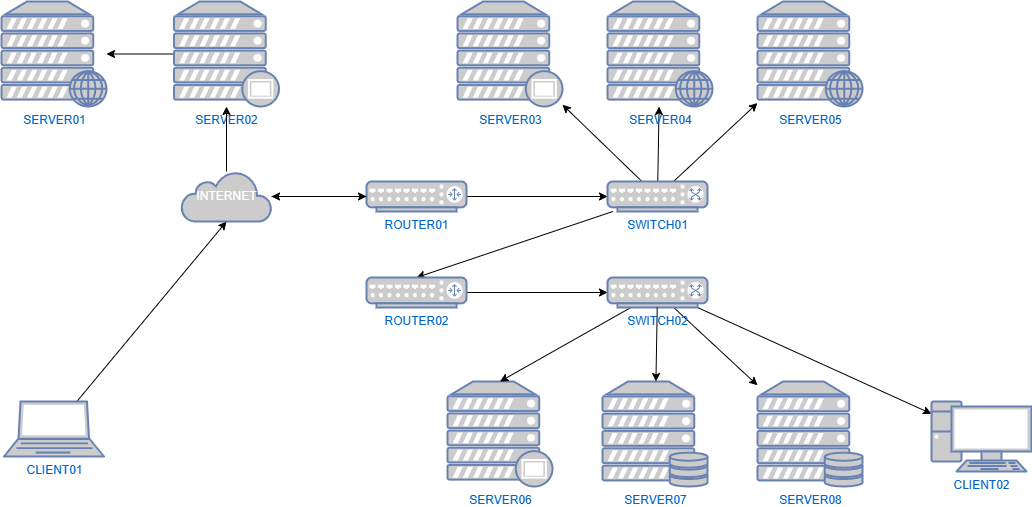
* **NTP服务**
  + 自动与NTP服务器同步时间
* **DNS服务**
  + 解析DMZ区域服务域名
  + 解析外部网络服务域名
* **Web服务**
  + 访问DMZ区域Web应用
  + 访问外部网络Web应用
* **Repo服务**
  + 配置apt源为SERVER01提供的https源
* **邮件服务**
  + 使用evolution客户端
  + 配置为ID号为14的用户的邮箱
  + 其他用户可通过Webmail登录邮箱
* **VPN服务**
  + 使用Gnome的NetworkManager连接VPN

# 所需的设备、机械、装置和材料

## 网络表

|  |  |  |  |
| --- | --- | --- | --- |
| **ID** | **HOSTNAME** | **IP ADDRESS** | **DESCRIPTION** |
| CLIENT01 | outsideclt | 47.119.161.24/28 | 外网客户端 |
| SERVER01 | isp | 47.119.161.25/28 | 互联网服务提供者 |
| SERVER02 | cdn | 47.119.161.26/28 | 内容分发网络服务器 |
| ROUTER01 | outsidertr | 每个与它相连的网络的最后一个IP。 | 边界路由/网关 |
| ROUTER02 | insidertr | 192.168.1.254/24 | 内部路由 |
| SERVER03 | proxy01 | 172.16.0.101/20 | 应用代理服务器 |
| SERVER04 | app01 | 172.16.0.102/20 | 对外应用服务器 |
| SERVER05 | app02 | 172.16.0.102/20 | 对外应用服务器 |
| SERVER06 | proxy02 | 192.168.1.101/24 | 内网代理服务器 |
| SERVER07 | storage01 | 192.168.1.102/24 | 内网存储服务器 |
| SERVER08 | storage02 | 192.168.1.103/24 | 内网存储服务器 |
| CLIENT02 | insideclt | 192.168.1.x/24 | 内网客户端 |

## 网络（逻辑）图



## 网络（物理）图

