2021 年全国职业院校技能大赛

网络系统管理（A-1）

模块 A：Linux 环境

ChinaSkills

全国职业院校技能大赛执委会.技术专家组

2021 年 06 月

目录

一、 竞赛简介

1. 请认真阅读以下指引！
2. 比赛共 4 个小时，你必须自行决定如何分配你的时间。
3. 当比赛结束时，离开时请不要关机您的虚拟机。
4. 如果没有明确要求，请使用“Chinaskill21”作为默认密码。
5. 本模块所有的系统为已经安装的最基本的系统状态，客户端带桌面。

二、 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。

三、 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。

四、 初始化环境

1.默认账号及默认密码

Username: root

Password: ChinaSkill21

Username: skills

Password: ChinaSkill21

注：若非特别指定，所有账号的密码均为 ChinaSkill21

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 2021 - CSK

Module A Linux

>>hostname<<

>>Debian Version<<

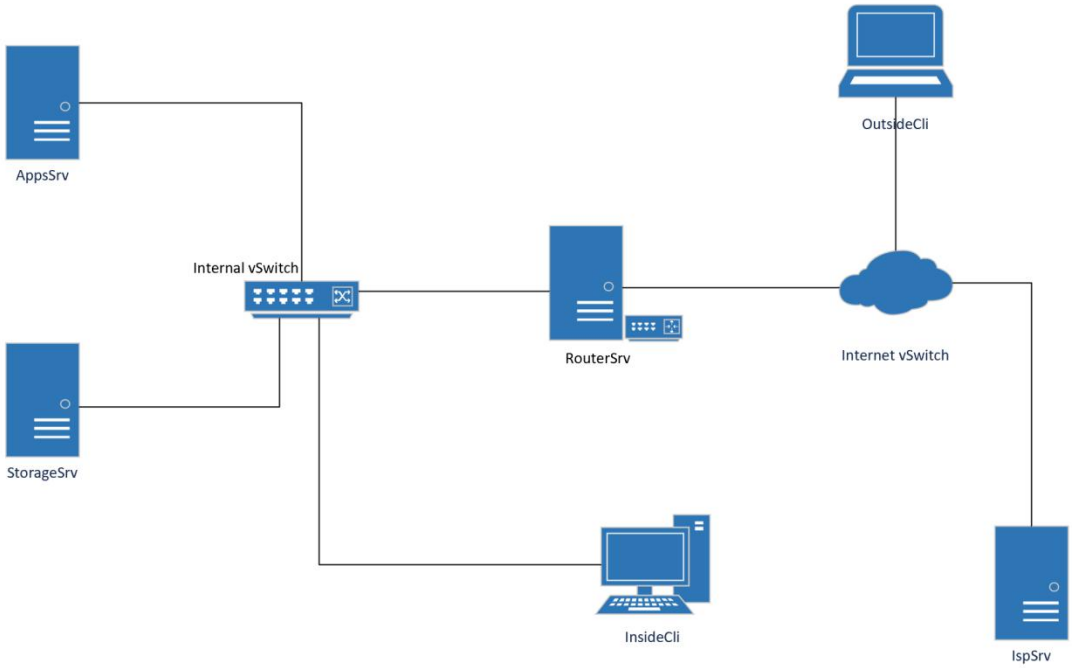
>> TIME <<

****

五、 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：

ISPSRV

- 全限定域名：ispsrv
- 普通用户/登录密码：skills/ChinaSkill21
- 超级管理员/登录密码：root/ChinaSkill21
- 网络地址/掩码/网关：81.6.63.100/24/无

AppSrv

- 全限定域名：appsrv.chinaskills.cn
- 普通用户/登录密码：skills/ChinaSkill21
- 超级管理员/登录密码：root/ChinaSkill21
- 网络地址/掩码/网关：192.168.100.100/24/192.168.100.254

STORAGESRV

- 全限定域名：storagesrv.chinaskills.cn
- 普通用户/登录密码：skills/ChinaSkill21
- 超级管理员/登录密码：root/ChinaSkill21
- 网络地址/掩码/网关：192.168.100.200/24/192.168.100.254

ROUTERSRV

- 全限定域名：routersrv.chinaskills.cn
- 普通用户/登录密码：skills/ChinaSkill21
- 超级管理员/登录密码：root/ChinaSkill21
- 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

- 全限定域名：insidecli.chinaskills.cn
- 普通用户/登录密码：skills/ChinaSkill21
- 超级管理员/登录密码：root/ChinaSkill21
- 网络地址/掩码/网关：DHCP From AppSrv

OUTSIDECLI

- 全限定域名：outsidecli.chinaskills.cn
- 普通用户/登录密码：skills/ChinaSkill21
- 超级管理员/登录密码：root/ChinaSkill21
- 网络地址/掩码/网关：DHCP From IspSrv

六、 项目任务清单

服务器 IspSrv 工作任务

1. IPTABLES

- 修改 INPUT 和 FORWARD 链默认规则为 DROP，添加必要的放行规则，在确保安全的前提下，最小限度放行流量通信；
- 放行 ICMP 流量。

2. DHCP

- 安装 isc-dhcp-server；
- 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。

3. DNS

- 安装 bind9；
- 启用 chroot 功能，限制 bind9 在/var/named 下运行（没有运行在/var/named 目录下，本题全部不得分。）；
- 配置为 DNS 根域服务器；
- 其他未知域名解析，统一解析为本机 IP；
- 创建正向区域“chinaskills.cn”；
  - 类型为 Slave；
  - 主服务器为“AppSrv”。

4. NTP

- 安装 ntp（使用其他 ntp 软件，以下功能均不得分）；
- 在 AppSrv 和 StorageSrv 上创建 CRON 计划任务；
- 使用 ntpdate 指令，每隔五分钟进行一次时间同步。

5. WEB 服务

- 安装 lighttpd（使用其他 web 平台，以下功能均不得分）；
- 启用 fastcgi-php 模块；
- index.php 网页内容显示当前服务器的日期和时间（刷新页面时间自动更新）。

服务器 RouterSrv 上的工作任务

1. DHCP RELAY

- 安装 isc-dhcp-server;
- 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；

3. SSH

- 安装 ssh，监听端口设置为 2021；
- 只允许用户 user01，密码 ChinaSkill21 登录到 RouterSrv。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. OPENVPN

- VPN 客户端只能与 InsideCli 客户端网段通信，允许访问 StorageSrv 主机上的 SAMBA 服务，允许访问 AppSrv 上的 dns 服务；
- VPN 客户端可使用的地址范围是 ：172.16.0.100-172.16.0.120/24；
- 在 OutsideCli 上创建连接服务“openvpn@csk.services”。

5. IPTABLES

- 添加必要的网络地址转换规则，使内部客户端能够访问外部网络；
- 添加必要的网络地址转换规则，使内部 DNS、MAIL、WEB、FTP 能对外提供服务；
- 修改 INPUT 和 FORWARD 链默认规则为 DROP，添加必要的放行规则，在确保安全的前提下，最小限度放行流量通信。

服务器 AppSrv 上的工作任务

1. IPTABLES

- 修改 INPUT 和 FORWARD 链默认规则为 DROP，添加必要的放行规则，在确保安全的前提下，最小限度放行流量通信；
- 放行 ICMP 流量。

2. SSH

- 安装 SSH，工作端口监听在 19210；
- 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(InsideCli)下可以使用秘钥免密码登录，并且拥有超级管理员权限。

3. 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。

4. DNS（BIND）

- 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；
- 添加邮件 MX 记录；
- 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。

5. APACHE2

- 安装 apache2 服务；
- 服务以 webuser 系统用户运行；
- 限制单个 IP 地址最大连接数为 50；
- 全站点启用 TLS 访问，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；
  - 使用/var/www/csk/wwwroot 作为网站根目录；
  - 安装 MriaDB 和 PHP，发布 WordPress 网站；
- 创建网站 download.chinaskills.cn 站点；
  - 使用/var/www/csk/download 作为网站根目录；

- 仅允许 ldsgp 用户组访问；
- 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。

6. Cacti

- 安装 cacti；
- 在 storagesrv 上配置 snmp，用于监控服务器接口流量情况；

7. MAIL（POSTFIX-SMTPS & DOVECOT-IMAPS）

- 安装配置 postfix 和 dovecot，启用 imaps 和 smtps；
- 创建 unix 用户 mail1~mail100，用户邮件均存储到用户家目录下的 Maildir 中；
- 禁止使用不安全的 smtp 和 imap 发送和接收邮件。

8. 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

O = skills

OU = Operations Departments

CN = CSK Global Root CA

服务器 StorageSrv 上的工作任务

1. IPTABLES

- 修改 INPUT 和 FORWARD 链默认规则为 DROP，添加必要的放行规则，在确保安全的前提下，最小限度放行流量通信；
- 放行 ICMP 流量。

2. DISK（RAID & LVM）

- 添加四张虚拟磁盘，大小均为 10G 的虚拟磁盘，配置 raid-5 磁盘，其中一张磁盘为热备磁盘；
- 创建 LVM 磁盘，路径为/dev/iscsivg/iscsistore。

3. Crypt-disk

- 创建一块新的磁盘，启用磁盘加密，解锁密码为“CSK2021!”；
- 映射到/dev/mapper/crypt 分区，并挂载到/mut/crypt 目录。

4. PURE-FTPD

- 安装 pure-ftpd（使用其他 ftp 软件，以下功能均不得分）；
- 仅允许使用 FTPES 协议访问，安全证书来自“CSK Global Root CA”颁发机构；
- 用户 ftpuser，登录 ftp 服务器，根目录为/mut/crypt/ftproot；
- 登录后限制在自己的根目录；
- 允许 ftpuser 上传和下载文件，但是不允许用户修改文件名称；
- ftpuser 用户仅允许登录一个会话窗口；
- 上传的文件所有者均设置为 ftpadmin。

5. LDAP

- 安装 slapd；
- 创建 chinaskills.cn 目录服务，并创建用户组 ldsgp ，用户 zsuser、lsusr、wuusr。

6. SAMBA

- 创建 samba 共享目录为/var/skills，共享名为 csk-share；
- 仅允许 ldsgp 组用户访问共享（使用 ldap 进行身份验证）；
- 用户登录后，能够上传和下载文件。

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 和 nmap 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 和 nmap 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。