2023 年四川省职业院校技能大赛

网络系统管理赛项(样题)

“网络构建”A 模块

一．说明

本模块比赛时间为 3 小时。请合理分配竞赛时间。请仔细阅读以下要求。

1. 比赛时间结束时，请将工作站保持运行状态，评分过程需要在运行状态进行，不允许重启。由于重启造成配置丢失由考生个人负责。

2. 为了方便测试，全网允许 ICMP 流量通行，请将操作系统的防火墙配置为允许 Ping 状态。

3．默认密码：XXXXXX。

4．软件&工具:见“2023 年“中银杯”四川省职业院校技能大赛网络系统管理赛项规程”。

目　录

任务清单

（一）基础配置

1.根据附录 1、附录 2，配置设备接口信息。
2.所有交换机和无线控制器开启 SSH 服务，基于用户名和密码认证，用户名密码分别为 admin、Test123456，授权用户角色为管理员角色。Console 口/AUX 口密码配置为 Test123456。密码均为明文类型。
3.总部所有设备配置 SNMP 功能，向主机 192.1.100.100 发送 Trap 消息版本采用 V2C，读写的 Community 为“Test”，只读的 Community 为“Public”，开启 Trap 消息，发送 Trap 的团体名为 Public。

（二）有线网络配置

1.在全网 Trunk 链路上做 VLAN 修剪。
2.为隔离部分终端用户间的二层互访，在交换机 S1 的 Gi0/1-Gi0/10 端口启用端口保护。
3.为规避网络末端接入设备上出现环路影响全网，要求在总部接入设备 S1 进行防环处理。具体要求如下：连接 vlan10、20、30 用户的终端的接口开启 BPDU 保护功能，配合 STP 边缘端口功能实现终端快速接入网络的同时需要避免终端接口私接设备造成的边缘端口失效的问题。连接 vlan40 的用户的终端的接口不需要配置为边缘端口，但是需要配置环路保护功能，检测到环路之后，触发 shutdown 接口的动作。为了避免接口在 shutdown 之后频繁的 up/down 的情况，需要在全局下将接口恢复时间修改为 300 秒。
4.在交换机 S3、S4 上配置 DHCP 中继，对 VLAN10 内的用户进行中继，使得总部 PC1 用户使用 DHCP Relay 方式获取 IP 地址。
5.DHCP 服务器搭建于 EG1 上，地址池命名为 Pool_VLAN10，DHCP 对外服务使用 loopback 0 地址。
6.为了防御动态环境局域网伪 DHCP 服务欺骗，在 S1 交换机部署 DHCP Snooping 功能。
7.在总部交换机 S1、S3、S4 上配置 MSTP 防止二层环路；要求 VLAN10、VLAN20、VLAN50、VLAN60、VLAN100 数据流经过 S3 转发，S3 失效时经过 S4 转发；VLAN30、VLAN40 数据流经过 S4 转发，S4 失效时经过 S3 转发。所配置的参数要求如下：region-name 为 test；revision 版本为 1；S3 作为实例 1 的主根、实例 2 的从根，S4 作为实例 2 的主根、实例 2 的从根；生成树优先级可设置为 4096、8192 或保持默认值；在 S3 和 S4 上配置 VRRP，实现主机的网关冗余，所配置的参数要求如下表；S3、S4 各 VRRP 组中高优先级设置为 150，低优先级设置为 120。

表 1 S3 和 S4 的 VRRP 参数表

VLAN	VRRP 备份组号（VRID）	VRRP 虚拟 IP
VLAN10	10	192.1.10.254
VLAN20	20	192.1.20.254
VLAN30	30	192.1.30.254
VLAN40	40	192.1.40.254

VLAN	VRRP 备份组号（VRID）	VRRP 虚拟 IP
VLAN50	50	192.1.50.254
VLAN60	60	192.1.60.254
VLAN100(交换机间)	100	192.1.100.254

9.总部与分部内网均使用 OSPF 协议组网，总部、分部与互联网间使用静态路由协议。具体要求如下：总部 S3、S4、EG1 间运行 OSPF，进程号为 10，规划单区域 0；分部 S7、EG2 间运行 OSPF，进程号为 20，规划单区域 0；服务器区使用静态路由组网；重发布路由进 OSPF 中使用类型 1。

10.总部与分部部署 IPv6 网络实现总分机构内网 IPv6 终端可通过无状态自动从网关处获取地址。IPv6 地址规划如下：

表 2 IPv6 地址规划表

设备	接口	IPv6 地址	VRRP 组号	虚拟 IP
S3	VLAN10	2001:192:10::252/64	10	2001:192:10::254/64
	VLAN20	2001:192:20::252/64	20	2001:192:20::254/64
	VLAN30	2001:192:30::252/64	30	2001:192:30::254/64
	VLAN40	2001:192:40::252/64	40	2001:192:40::254/64
	VLAN60	2001:192:60::252/64	60	2001:192:60::254/64
	VLAN100	2001:192:100::252/64	100	2001:192:100::254/64
S4	VLAN10	2001:192:10::253/64	10	2001:192:10::254/64
	VLAN20	2001:192:20::253/64	20	2001:192:20::254/64
	VLAN30	2001:192:30::253/64	30	2001:192:30::254/64
	VLAN40	2001:192:40::253/64	40	2001:192:40::254/64
	VLAN60	2001:192:60::253/64	60	2001:192:60::254/64
	VLAN100	2001:192:100::253/64	100	2001:192:100::254/64
S7	VLAN10	2001:193:10::254/64		
	VLAN20	2001:193:20::254/64		
	VLAN60	2001:193:60::254/64		

11.在 S3 和 S4 上配置 VRRP for IPv6，实现主机的 IPv6 网关冗余；在 S3 和 S4 上 VRRP 与 MSTP 的主备状态与 IPV4 网络一致。

12.R1、R2、R3 部署 IGP 中 OSPF 动态路由实现直连网段互联互通。

13.R1、R2、R3 间部署 IBGP，AS 号为 100，使用 Loopback 接口建立 Peer。

14.运营商通告 EG1、EG2 专线至服务器区，R1、R2 均以汇总 B 段静态路由的方式进行发布。服务器区通过 R3 将 AC1、AC2 通告到 BGP 中。

15.可通过修改 OSPF 路由 COST 达到分流的目的，且其值必须为 5 或 10。

16.总部财务、销售 IPv4 用户与互联网互通主路径规划为：S3-EG1。

17.总部研发、市场 IPv4 用户与互联网互通主路径规划为：S4-EG1。

18.主链路故障可无缝切换到多条备用链路上。

（三）无线网络配置

1.使用 S3、S4 作为总部无线用户和无线 AP 的 DHCP 服务器，使用 S6/S7 作为分部无线用户和无线 AP 的 DHCP 服务器。
2.创建总部内网 SSID 为 test-ZB_XX(XX 现场提供)，WLAN ID 为 1，AP-Group 为 ZB，总部内网无线用户关联 SSID 后可自动获取地址，启用 WEB 认证方。
3.创建分部内网 SSID 为 test-FB_XX(XX 现场提供)，WLAN ID 为 2，AP-Group 为 FB，总部内网无线用户关联 SSID 后可自动获取地址，启用 802.1X 认证方式。
4.认证服务器（IP：194.1.100.100）建立总部认证用户 user1，user2，分部认证用户 user3，user4 分别对应 WEB、DOT1X 认证；
5.AC1 为主用，AC2 为备用。AP 与 AC1、AC2 均建立隧道，当 AP 与 AC1 失去连接时能无缝切换至 AC2 并提供服务。
6.要求总部分部内网无线网络启用本地转发模式。
10.为了保障每个用户的无线体验，针对 WLAN ID2 下的每个用户的下行平均速率为 800KB/s ，突发速率为 1600KB/s。
7.总部每 AP 最大带点人数为 30 人。
8.分部通过时间调度，要求每周一至周五的 21:00 至 23:30 期间关闭无线服务。
9.总部设置 AP 信号发送强度为 30。
10.总部关闭低速率（11b/g 1M、2M、5M，11a 6M、9M）应用接入。

（四）出口网络配置

1. 出口网关配置 NAPT 技术，实现总部无线用户和总部有线用户可以访问 Internet 的需求，ACL 编号为 3000，同时实现分部无线用户和有线用户可以访问 Internet 的需求，ACL 编号为 3000。
2.在总部 EG1 上配置，使总部核心交换 S4（11.1.0.34）设备的 SSH 服务可以通过互联网被访问，将其地址映射至联通线路上，映射地址为 20.1.0.1。
3. 在总部出口和分部出口上配置安全域,将连接内部的接口划入到 trust 区域(包含 loopback 接口），将连接外部的接口划入到 untrust 区域。
4.在总部出口和分部出口上配置安全策略，策略为 ip 和 ipv6，对源安全域为 trust、untrust、local，目的安全域为 untrust、trust、local，放通 IPv4 的流量和 IPv6 的业务流量，规则 ID 为 0，name0。
5.分部 EG2 针对访问外网 WEB 流量限速每 IP 1000Kbps，内网 WEB 总流量不超过 50Mbps。
6.要求使用 ipsec 隧道主模式，安全协议采用 esp 协议，加密算法采用 3des，认证算法采用 md5，以 IKE 方式建立 ipsec SA。在 EG1 和 EG2 上所配置的参数要求如下：ipsec 加密转换集名称为 myset；预共享密钥为明文 123456；静态的 ipsec 加密图 mymap。ACL 编号为 3100。

（五）网络运维配置

1.完成整网连通后，进入网络监控运维阶段，运维软件已安装在 PC1 的虚拟机 OPMSrv 中(访问

运维平台的 URL 为 http://192.1.100.100)，通过运维平台监控广州总部内所有设备（具体设备：S1、S3、S4、EG1）。

2.通过运维平台将广州总部的被监控设备纳入监控范围；通过拓扑配置功能，将广州总部的网络拓扑配置到平台中；

3.将广州总部 S3、S4 和 EG1 的两条链路作为重点监测链路，纳入链路监控；

4.自定义监控大屏（名称：Chinaskills_network），将网络拓扑、设备运行状态（CPU 使用率）、链路运行状态实时显示在大屏中。

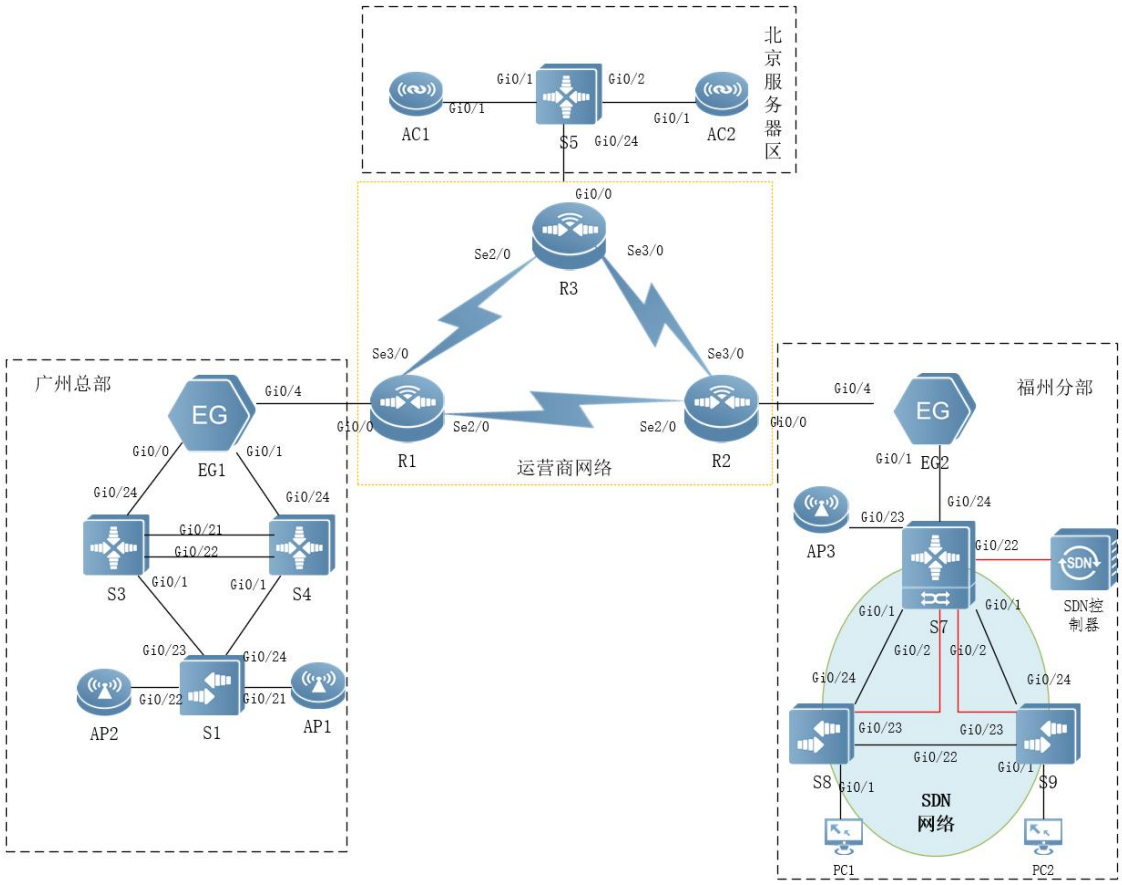
（六）SDN 网络配置

1.SDN 控制器登录地址：192.168.1.2/24，默认用户密码为 admin/test@123。

2.使用 S7/S8/S9 构建 SDN 网络，S8/S9 连接 SDN 控制器的 6653 端口。

3.通过 SDN 控制器手工给 S8 下发一条流表项名称为 drop 的流表，执行动作为丢弃，并在交换机上查看流表，测试普通 PC 禁止 ping 通高性能 PC。

附录 1：拓扑图



附录 2：地址规划表

设备	接口或 VLAN	VLAN 名称	二层或三层规划	说明
S1	VLAN10	CAIWU	Gi0/1 至 Gi0/4	财务部
	VLAN20	XIAOSHOU	Gi0/5 至 Gi0/8	销售部
	VLAN30	YANFA	Gi0/9 至 Gi0/12	研发部
	VLAN40	SHICHANG	Gi0/13 至 Gi0/16	市场部
	VLAN50	AP	Gi0/20 至 Gi0/21	无线 AP 管理
	VLAN100	Manage	192.1.100.1/24	设备管理 VLAN
S3	VLAN10	CAIWU	192.1.10.252/24	财务部
	VLAN20	XIAOSHOU	192.1.20.252/24	销售部
	VLAN30	YANFA	192.1.30.252/24	研发部
	VLAN40	SHICHANG	192.1.40.252/24	市场部
	VLAN50	AP	192.1.50.252/24	AP
	VLAN60	Wireless	192.1.60.252/24	无线用户
	VLAN100	Manage	192.1.100.252/24	设备管理 VLAN
	Gi0/24		10.1.0.1/30	
	LoopBack 0		11.1.0.33/32	
S4	VLAN10	CAIWU	192.1.10.253/24	财务部
	VLAN20	XIAOSHOU	192.1.20.253/24	销售部
	VLAN30	YANFA	192.1.30.253/24	研发部
	VLAN40	SHICHANG	192.1.40.253/24	市场部
	VLAN50	AP	192.1.50.253/24	AP
	VLAN60	Wireless	192.1.60.253/24	无线用户
	VLAN100	Manage	192.1.100.253/24	设备管理 VLAN
	Gi0/24		10.1.0.5/30	
	LoopBack 0		11.1.0.34/32	
AC1	LoopBack 0		11.1.0.204/32	
	Vlan100	Manage	194.1.100.2/24	管理与互联 VLAN
AC2	LoopBack 0		11.1.0.205/32	
	Vlan100	Manage	194.1.100.3/24	管理与互联 VLAN
S5	Gi0/24		40.1.0.1/30	
	VLAN100	Manage	194.1.100.254/24	管理与互联 VLAN
	LoopBack 0		11.1.0.5/32	
EG1	GI0/0		10.1.0.2/30	
	GI0/1		10.1.0.6/30	
	GI0/4		20.1.0.1/30	
	LoopBack 0		11.1.0.11/32	
EG2	GI0/0		10.1.0.14/30	

设备	接口或 VLAN	VLAN 名称	二层或三层规划	说明
	GI0/1		10.1.0.18/30	
	GI0/4		30.1.0.1/30	
	LoopBack 0		11.1.0.12/32	
R1	Gi0/0		20.1.0.2/30	
	Gi0/1		12.1.0.1/28	
	Gi0/2		13.1.0.1/28	
	LoopBack 0		11.1.0.1/32	
R2	Gi0/0		30.1.0.2/30	
	Gi0/1		12.1.0.2/28	
	Gi0/2		23.1.0.2/28	
	LoopBack 0		11.1.0.2/32	
R3	Gi0/0		40.1.0.2/30	
	Gi0/1		13.1.0.3/28	
	Gi0/2		23.1.0.3/28	
	LoopBack 0		11.1.0.3/32	
S2	VLAN10	CAIWU		财务部
	VLAN20	XIAOSHOU		销售部
	VLAN50	AP	Gi0/1 至 Gi0/20	无线 AP 管理
	VLAN100	Manage	193.1.100.2/24	设备管理 VLAN
S7	VLAN10	CAIWU	193.1.10.254/24	财务部
	VLAN20	XIAOSHOU	193.1.20.254/24	销售部
	VLAN50	AP	193.1.50.254/24	无线 AP 管理
	VLAN60	Wireless	193.1.60.254/24	无线用户
	VLAN100	Manage	193.1.100.254/24	设备管理 VLAN
	Gi0/24		10.1.0.17/30	
	LoopBack 0		11.1.0.67/32	
S8	VLAN10	CAIWU	Gi0/1 至 Gi0/4	财务部
	VLAN20	XIAOSHOU	Gi0/5 至 Gi0/8	销售部
	Gi0/23	SDN-Manage	192.168.1.3	SDN 管理网段
S9	VLAN10	CAIWU	Gi0/1 至 Gi0/4	财务部
	VLAN20	XIAOSHOU	Gi0/5 至 Gi0/8	销售部
	Gi0/23	SDN-Manage	192.168.1.4	SDN 管理网段

2023 年四川省职业院校技能大赛

网络系统管理赛项(样题)

“服务部署”B 模块

目　录

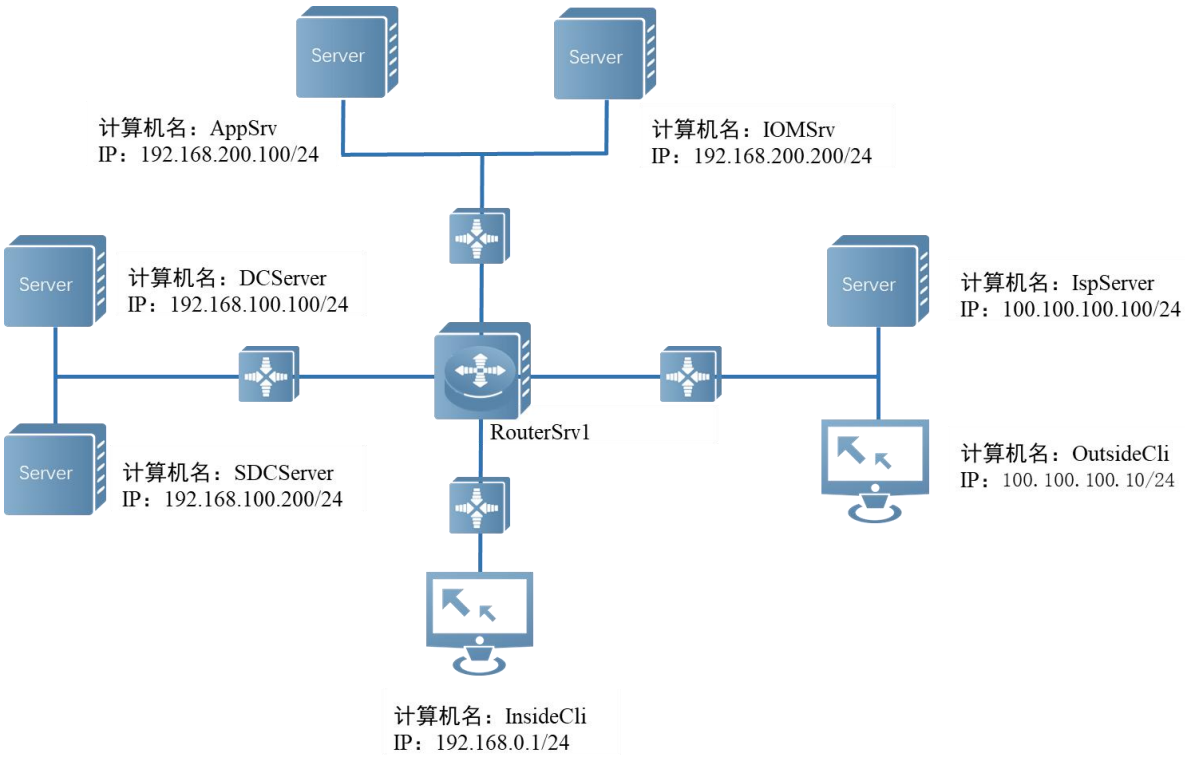
一、Windows 初始化环境

默认账号及默认密码
Username: Administrator
Password: ChinaSkill23@!
Username: demo
Password: ChinaSkill23@!
注：若非特别指定，所有账号的密码均为 ChinaSkill23@!

二、Windows 项目任务描述

你作为一个技术工程师，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 Windows 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：

（一）拓扑图



（二）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。

DCServer	chinaskills.com	192.168.100.100/24	127.0.0.1	192.168.100.254
SDCSserv	chinaskills.com	192.168.100.200/24	127.0.0.1	192.168.100.254

er				
AppSrv	chinaskills.com	192.168.200.100/24	192.168.100.100 192.168.100.200	192.168.200.254
IOMSrv	chinaskills.com	192.168.200.200/24	192.168.100.100 192.168.100.200	192.168.200.254
RouterSrv1	chinaskills.com	192.168.100.254/24 192.168.0.254/24 192.168.200.254/24 100.100.100.251/24	192.168.100.100	100.100.100.254
IspSrv	保持工作组状态	100.100.100.100/24	127.0.0.1	无
InsideCli	chinaskills.com	192.168.0.0/24(dhcp)	192.168.100.100 192.168.100.200	192.168.0.254
OutsideCli	保持工作组状态	100.100.100.10/24	100.100.100.100	100.100.100.254

三、Windows 项目任务清单

（一）服务器 IspSrv 上的工作任务

1. 互联网访问检测服务器

- 为了模拟 Internet 访问测试，请搭建网卡互联网检测服务。

2. DNS（域名解析服务）

- 拓扑中所有主机的 DNS 查询请求都应由 IspSrv 进行解析。
- 把当前机器作为互联网根域服务器，创建 test1.com~test100.com，并在所有正向区域中创建一条 A 记录，解析到本机地址。

（二）服务器 RouterSrv1 上的工作任务

1. 路由功能

- 安装 Remote Access 服务开启路由转发，为当前实验环境提供路由功能。
- 启用网络地址转换功能，实现内部客户端访问互联网资源。
- 配置网络地址转换，允许互联网区域客户端访问 AppSrv 上的 HTTP 资源。

2. **动态地址分配中继服务**
   - 安装和配置 dhcp relay 服务，为办公区域网络提供地址上网。
   - DHCP 服务器位于 AppSrv 服务器上。
3. **虚拟专用网络**
   - 设置 L2TP/IPSec，IKE 通道采用证书进行验证。
   - L2TP 通道使用 chinaskills.com 域内用户进行身份验证，仅允许 manager 组内用户通过身份证验证。
   - 对于 vpn 客户端，请使用范围 192.168.1.200-192.168.1.220/24。
4. **RDS**
   - 在 RouterSrv1 安装和配置 RDS 服务，用户通过“https://app.chinaskills.com/rdweb”进行访问。
   - 该页面无证书警告。
   - 用户可以获取以下应用：
   - Notepad

（三）服务器 AppSrv 上的工作任务

1. **万维网服务**
   - 在 RouterSrv1 上搭建网站服务器。
   - 将访问 http://www.chinaskills.com 的 http 的请求重定向到 https://www.chinaskills.com 站点。
   - 网站内容设置为“该页面为 www.chinaskills.com 测试页！”。
   - 将当前 web 根目录的设置为 d:\wwwroot 目录。
   - 启用 windows 身份验证，只有通过身份验证的用户才能访问到该站点，manager 用户组成员使用 IE 浏览器打开不提示认证，直接访问。
   - 设置“http://www.chinaskills.com/”网站的最大连接数为 1000，网站连接超时为 60sl；
   - 使用 W3C 记录日志；每天创建一个新的日志文件，文件名格式:
   - 日志只允许记录日期、时间、客户端 IP 地址、用户名、服务器 IP 地址、服务器端口号；
   - 日志文件存储到“C:\WWWLogFile”目录中；
   - 配置 IIS 配套 FTP 服务：
   - 匿名用户上传的文件都将映射为 ftp2 用户
   - ftp 在登录前显示 Banner 消息：
   - “Hello, unauthorized login is prohibited!”
2. **动态地址分配服务**
   - 安装和配置 dhcp 服务，为办公区域网络提供地址上网。
   - 地址池范围：192.168.0.100-192.168.0.200。

3. **DFS**
   - 在 ppSrv 上安装及配置 DFS 服务。
   - 目录设置在 F：\DFSsharedir。
   - 配置 DFS 复制，使用 DC1 作为次要服务器，复制方式配置为交错拓扑。
   - 在 F：\DFSsharedir 文件夹内新建所有部门的文件夹。
   - 所有部门的用户之可以访问部门内的文件，不可以跨部门访问别的部门文件夹内容。
   - Management 用户组用户可以访问全局的文件夹。
4. **磁盘管理**
   - 安装及配置软 RAID5。
   - 在安装好的 **AppSrv** 虚拟机中添加三块 10 G 虚拟磁盘。
   - 组成 RAID5，磁盘分区命名为卷标 F 盘：Raid5。
   - 手动测试破坏一块磁盘，做 RAID 磁盘修复；确认 RAID5 配置完毕。
5. **DNS**
   - 安装 DNS 服务器，根据题目创建必要的 DNS 解析。
   - 把当前机器作为互联网根域服务器。
6. **WSUS 更新服务**
   - 安装 WSUS 更新服务，更新补丁目录设置为“c:\wsusbackup”。
   - 创建更新组名称为“CHINASKILLS-WSUS”。
   - 每天凌晨 03:00 下发自动更新。
   - 更新服务器地址为“http://wsus.chinaskills.cn:8530”。

（四）服务器 DCSERVER&SDCSERVER 上的工作任务

1. **活动目录域服务**
   - 在 DCSERVER 和 SDCSERVER 服务器上安装活动目录域服务，DCSERVER 作为主域控，SDCSERVER 作为备份域控，活动目录域名为：chinaskills.com。
   - 域用户能够使用[username]@csk.cn 进行登录。
   - 创建一个名为“CSK”的 OU，并新建以下域用户和组：
     sa01-sa20，请将该用户添加到 sales 用户组。
     it01-it20，请将该用户添加到 IT 用户组。
     ma01-ma10，请将该用户添加到 manager 用户组。
     许除 manager 组和 IT 组，所有用户隐藏 C 盘。
     除 manager 组和 IT 组，所有普通给用户禁止使用 cmd。
   - 所有用户的 IE 浏览器首页设置为“https://www.chinaskills.com”。
   - 所有用户都应该收到登录提示信息：标题“登录安全提示：”，内容“禁止非法用户登录使用本计算机。”。

- 设置所有主机的登录 Banner：
  标题为“CHINASKILLS-DOMAIN”；
  内容为“Hello, unauthorized login is prohibited!”。
- 域内的所有计算机（除 dc 外），当 dc 服务器不可用时，禁止使用缓存登录。

2. 证书颁发机构

- 在 DCSERVER 服务器上安装证书办法机构。
- 定义名称：CSK2023-ROOTCA。
- 证书颁发机构有效期：3 years。
- 为 chinaskills.com 域内的 web 站点颁发 web 证书。
- 当前拓扑内所有机器必须信任该证书颁发机构。
- 所域内所有计算机自动颁发一张计算机证书。

3. 磁盘管理

- 在 DC2 上安装及配置软 RAID5。
- 在安装好的 DC2 虚拟机中添加三块 10G 虚拟磁盘。
- 组成 RAID5，磁盘分区命名为卷标 H 盘：Raid5。
- 手动测试破坏一块磁盘，做 RAID 磁盘修复，确认 RAID5 配置完毕。

（五）服务器 IOMSrv 上的工作任务

- 图形界面登陆 IOMSrv 运维平台，登陆地址 http://192.168.200.200；
- 通过 Windows 代理模板，添加 DCServer、SDCSserver、AppSrv 操作系统监控对象，查看运行状态。
- 通过中间件 IIS 模板，添加 IIS 监控对象，查看运行状态。
- 通过新增 WEB 探测对象，监控门户网站 http://www.chinaskills.com，查看运行状态。
- 基在运维概况完成应用监控，应用拓扑添加并在大屏上呈现

（六）客户端 InsideCli 上的工作任务

- 按照要求将该主机加入到对应区域的域。
- 设置电源配置，以便客户端在通电的情况下，永不进入睡眠。
- 该客户端用于测试用户登录，Profiles，文件共享，安全策略和 RDS 等功能。

（七）客户端 OutsideCli 上的工作任务

- 该主机不允许加入域。
- 添加一个名为 Connect-CSK 的 VPN 拨号器，用于连接到 chinaskills.com 域网络，不记录用户名称密码信息。
- 设置电源配置，以便客户端在通电的情况下，永不进入睡眠。

- 该客户端用于测试用户登录，Profiles，文件共享，安全策略和 RDS 等功能。

四、Linux 初始化环境

（一）默认账号及默认密码

Username: root
Password: ChinaSkill23@!
Username: skills
Password: ChinaSkill23@!
注：若非特别指定，所有账号的密码均为 ChinaSkill23@!

（二）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

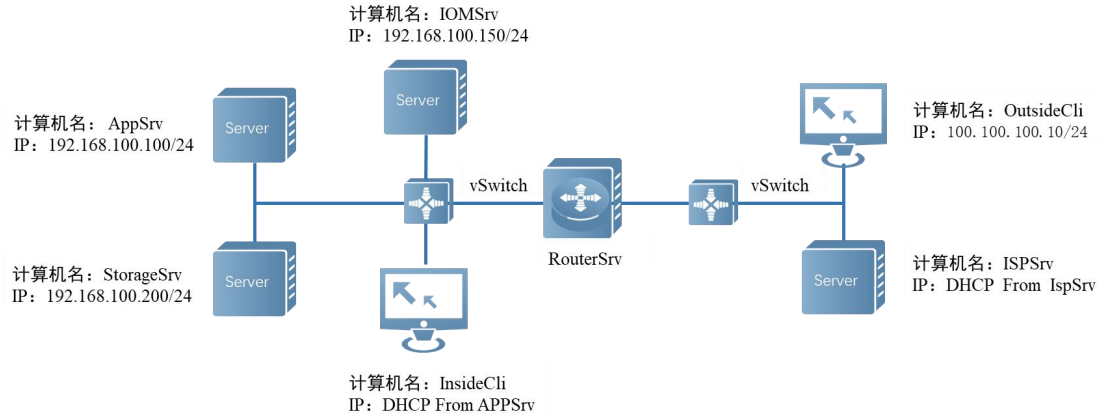
****
ChinaSkills 2023‐CSK
Module C Linux

>>hostname<<
>>System Version<<
>> TIME <<
****

五、Linux 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：

（一）拓扑图



（二）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/ChinaSkill23
- 超级管理员/登录密码：root/ChinaSkill23
- 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
- 超级管理员/登录密码：root/ChinaSkill23
- 网络地址/掩码/网关：192.168.100.100/24/192.168.100.254

IOMSrv(Centos)

- 网络地址/掩码/网关：192.168.100.150/24/192.168.100.254

STORAGESRV(Centos)

- 完全限定域名：storagesrv.chinaskills.cn
- 超级管理员/登录密码：root/ChinaSkill23
- 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/ChinaSkill23
- 超级管理员/登录密码：root/ChinaSkill23
- 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/ChinaSkill23
- 超级管理员/登录密码：root/ChinaSkill23

- 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/ChinaSkill23
- 超级管理员/登录密码：root/ChinaSkill23
- 网络地址/掩码/网关：DHCP From IspSrv

六、Linux 项目任务清单

（一）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

- 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 2023 Computer Network Application contest!

（二）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 2023；

- 只允许用户 user01，密码 ChinaSkill23 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。

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。

（三）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.com
- 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: ChinaSkill23@!。
- 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。

5. DBMS

- 在 Server01 上完成 MariaDB 数据库的安装，添加数据库 root 用户密码为 ChinaSkill23@!
- 安装 MariaDB 数据库服务器组件;

- MariaDB 数据库管理员信息：User: root/ Password: ChinaSkill23@!；
- 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；

6. 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。

7. 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

（四）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. 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。

5. 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。

（五）服务器 IOMSrv 工作任务

- 图形界面登陆 IOMSrv 运维平台，登陆地址 http://172.16.100.150；
- 通过 Linux 代理模板，添加 StorageSrv、AppSrv 操作系统监控对象，查看运行状态；
- 通过中间件 Nginx 模板，添加 Nginx 监控对象，查看运行状态；
- 通过中间件 MySQL 数据库 Agent 模板，添加 Mariadb 监控对象，查看运行状态；
- 通过新增 WEB 探测对象，监控门户网站 www.chinaskills.cn，查看运行状态；
- 在运维概况完成应用监控，应用拓扑添加并在大屏上呈现

（六）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。