2023 年湖南省“楚怡杯”职业院校技能竞赛

赛项规程

一、赛项名称

1. 赛项名称：网络搭建与应用

2. 赛项组别：中职组

3. 赛项归属：计算机类/电子与信息大类

二、竞赛内容

1. 竞赛主要内容

竞赛包含职业规范与素养、网络布线与基础连接、交换配置与调试、路由配置与调试、无线网络配置、安全策略配置、云平台网络连接与部署、Windows 服务配置和 Linux 服务配置，共九个模块。各模块有机结合，最终实现典型网络架构与部署整体实施。比赛过程中，要求团队选手合理的安排工作流程、按照题目要求规划网络实施方案，完成设备连接、配置与测试网络设备、设置虚拟化环境，配置云主机、配置操作系统、部署安全策略等，完成网络搭建与应用赛项整体竞赛任务。

2. 重点考查技能

重点考查参赛选手的网络实战能力，具体包括：

（1）能够根据竞赛要求，读懂文档需求，理解业务架构，实现项目应用。

（2）能够完成线缆制作、合理划分网络地址，配置路由器、交换机、无线控制器、无线 AP 和防火墙等网络设备，实现网络的正常运行。

（3）能够根据业务需求和应用环境，安装部署各类服务器、数据库、存储等相关服务；并根据网络业务需求配置各种策略，以达到网络互联互通，实现云平台和网络资源适应业务需求。

（4）能够预判网络运行中所面临的安全威胁，防范并解决网络恶意攻击行为；考查选手防御不良信息及病毒、构建和维护绿色网络的实战能力。

三、竞赛方式

2 人团体赛。

四、竞赛时量

竞赛时量为 240 分钟。

五、名次确定办法

按照竞赛成绩从高到低排序确定名次，不设并列名次。总分相同时，以“网络搭建及安全部署”成绩高者名次列前。

六、评分标准与评分细则

本赛项总分为 100 分，其中职业素养为 5 分，网络搭建及安全部署为 50 分，

服务器配置及应用为 45 分。评分标准和细则如下表所示。

1. 评分标准

序号	分类		评分标准
1	职业规范与素养		能整理赛位环境，工具设备归位，保持工作区整洁；科学专业施工，正确选择器具，未造成不应该损坏；团队合作默契，工时安排合理，有序规范开展竞赛；做好个人防护，注重安全健康，全程执行防控要求；恢复调试现场，符合交付要求，确保网络系统安全
2	网络搭建及安全部署	网络综合布线安装和施工	能按照竞赛要求完成设备连接，符合布线规范，保证线路通畅
3		IP 地址划分实施	能完成子网划分、IP 规划并实施
4		网络调试	能完成指定的交换、路由、广域网和无线的配置，实现网络联通
5		网络配置优化	能完成各种网络优化及策略配置
6		网络安全配置	通过防火墙等网络设备配置安全策略，能完成安全防护
7	服务器配置及应用	云平台部署及云主机创建	能按照项目要求连接和配置网络设备，连接云平台，保证系统服务正常运行；完成使用云平台规划和分配资源、配置已生成实例接入网络工作；完成 Windows/Linux 虚拟云主机的创建与基本设置
8		操作系统配置常用服务（Windows 与 Linux）	能完成各类服务器系统配置与管理，数据库安装调试、存储配置与管理、网站等各项服务搭建调试和安全策略配置等
9		操作系统安全技术	能完成操作系统的安全配置

2. 评分细则

序号	分类		评分细则	分值
1	职业规范与素养		整理赛位环境，科学专业施工,团队合作默契，做好个人防护，恢复调试现场，确保网络系统安全	5
2	网络搭建及安全部署	网络综合布线安装和施工	按照竞赛要求完成设备连接，符合布线规范，保证和测试物理路连通性	5
3		IP 地址划分实施	完成子网划分、IP 规划并实施	5
4		网络调试	完成指定的交换、路由、防火墙和无线的配置	20
5		网络配置优化	完成各种网络优化及策略配置	15
6		网络安全配置	完成网络安全策略配置	5
7	服务器配置及应用	云平台部署及云主机创建	完成连接云平台；完成使用云平台规划和分配资源、配置已生成实例接入网络工作；完成 Windows/Linux 虚拟云主机的创建与基本设置	20

8		操作系统配置常用服务（Windows 与 Linux）	完成安装配置各类应用服务和数据库安装调试、服务器集群及虚拟化等	20
9		操作系统安全技术	完成操作系统的安全配置	5
合计				100 分

七、赛项相关设施设备技术参数

1.硬件平台

序号	设备名称	数量	品牌	备注
1	路由器 DCR-2855	2	神州数码	含 CR-V35MT-V35FC
2	三层交换机 CS6200-28X-Pro	3	神州数码	含虚拟化连接套件 DAC-SFPX-3M
3	多核防火墙 DCFW-1800E-N3002-Pro	2	神州数码	含特征库升级许可
4	无线交换机 DCWS-6028-Pro	1	神州数码	
5	无线接入点 WL8200-I2(R2)	1	神州数码	含 POE 模块
6	云实训平台 DCC-CRL1000（R2.0）	1	神州数码	
7	PC 机 （CPU:主频>=3.5GHZ, >=四核心八线程,内存>=8G 硬盘>=1T,网卡>=1Gb 支持硬件虚拟化, 显示器：20 寸及以上）	2	承办校提供	
8	网络设备机柜和综合布线工具、耗材（含网线钳，测网仪，配置线、网线、水晶头等）	1 套	承办校提供	

2.软件技术平台

Windows 系统平台主要由服务器版和桌面版组成，桌面版主要采用 Windows 11(中文版)，服务器版主要采用 Windows Server 2022(中文版)；Linux 系统平台主要采用 Rocky 9；办公软件的版本为 WPS Office。

每赛位具体软件参数如下所示:

序号	软件参数	备注
1	Windows 11 中文专业版	承办校电脑自带
2	Rocky 9	云实训平台镜像
3	Windows Server 2022 中文数据中心版	云实训平台镜像
4	WPS Pro 2022 专业试用版	赛场提供
5	Secure CRT-SecureFX9 及以上	赛场提供

6	Kubernetes rpm 包及镜像	
7	Tomcat rpm 包	赛场提供
8	Oracle jdk-17 及以上	赛场提供
9	VLC media player 播放器	赛场提供

八、选手须知

1.选手自带工（量）具及材料清单

竞赛所需的硬件、软件和辅助工具、材料等都由赛点统一提供，参赛队不需自带任何工具、设备和软件进入赛场。

2.主要技术规范及要求

（1）教学标准

中等职业学校专业教学标准——信息技术类。

（2）行业标准

序号	标准号	中文标准名称
1	GB50311-2016	《综合布线系统工程设计规范》
2	GB50312-2016	《综合布线系统工程验收规范》
3	GB50174-2017	《电子信息系统机房设计规范》
4	GB21671-2018	《基于以太网技术的局域网系统验收测评规范》
5	GB50348-2018	《安全防范工程技术标准》
6	GB/T18729-2011	《基于网络的企业信息集成规范》
7	GB/T22239-2018	《信息系统安全等级保护基本要求》

（3）职业技术标准

网络设备调试达到并超过行业内各知名厂商 NA/NE（网络工程师）级别，接近 NP（高级网络工程师）级别；WINDOWS 服务器调试达到微软 MCSE（系统工程师）级别；Linux 服务器调试达到并超过 RHCSA（系统管理员）级别，接近 RHCE（系统工程师）级别。

全面对接“下一代互联网(IPv6)搭建与运维”与“网络系统软件应用与维护”1+X 证书，一二三等奖选手知识技能掌握及应用水平分别对应职业技能等级证书初中高级。

（4）主要竞赛知识点和技能点

序号	内容模块	具体内容	说明
1	网络搭建及安全部署	网络综合布线安装和施工	综合布线基础：网络布线、设备连接、端口标识、电源接入；物理连通性检测、链路质量（基于 GB50312-2016）检测、端口检测等
2		IP 地址划分并实施	VLSM、CIDR 等地址划分并实施网络配置

序号	内容模块	具体内容	说明
2		交换基本配置	LAN、STP、RSTP、MSTP、802.1X、ARP、交换机虚拟化、交换安全、端口聚合、端口镜像、VRRP、VRRPV3、IPV6、PBR、IPV6PBR、ACL、DHCPV6、DHCPSnooping、QOS、BFD、Keepalivegateway、基于流的重定向等
3		广域网和路由配置	E1 链路捆绑、PPP 或者 HDLC 协议、静态、RIP、RIPng、OSPF、OSPFV3、BGP、MBGP4+、ISIS 等单播路由协议、PIM、IGMP 等组播协议、NTP、DHCP、TELNET、策略路由、IPV6、NAT、QOS 等
4		无线配置	AP 到 AC 二、三层注册，AP 配置管理、AC 射频管理、无线认证和接入配置，QOS 配置、安全配置，限时策略、强制漫游、负载均衡配置等
5		安全配置	配置 GRE 隧道、IPSEC 隧道，安全域、接口、地址与服务，安全策略、NAT、安全控制、网络行为控制、攻击防护、日志配置、SecureConnectVPN、L2TPVPN 和或 MPLS_VPN 等
6	服务器配置及应用	云平台部署	在云平台创建实例规格、创建网络、创建卷、创建虚拟机等
7		操作系统安装 Windows 与 Linux	虚拟主机的创建与基本设置
8		配置常用服务 Windows 与 Linux	能够根据企业的应用需求，熟练安装和配置 AD、DNS、WEB、E-MAIL、DHCP、DFS、NTP、NIS、19/74 序号内容模块具体内容说明 KDC、MariaDB、Apache、Nginx、NFS、Samba、Tomcat、iSCSI、文件共享、NLB、故障转移、多路径、BitLocker、打印服务、PowerShell 脚本、LinuxShell 脚本、python3 脚本、Redis、PostgreSQL、PXE、WDS、FTPd、VPN、Ansible、Kubernetes、Containerd、RAID、磁盘加密、WordPress 等常用服务和数据库配置与管理、Docker 技术应用，并能实际运用。能够熟练掌握 vSphere 和 VMware 等常用虚拟化技术完成特定环境配置;使用服务器群集技术来实现网络的负载均衡、故障转移、群集管理等
9		操作系统安全技术	域安全配置、文件系统安全配置、权限管理、配置 CA 服务、系统防火墙防护等

3.选手注意事项

（1）参赛选手自觉遵守竞赛纪律，服从指挥，听从安排，文明参赛。

（2）参赛选手不得携带电子设备、通讯设备及其他资料与用品进入赛场。

（3）参赛选手应按照规定时间抵达赛场，凭参赛证、身份证件检录，按要求入场，不得迟到早退，遵守比赛纪律。参赛选手的服饰不得体现学校信息和选手信息。若有违反，暂停比赛，交由赛点组委会处理。

（4）参赛选手入场后，应与赛场工作人员共同确认操作设备的运行状况和工具、材料的配备情况，并签字确认。

（5）参赛选手应按有关要求在指定位置就坐，确认抽签工位号。在比赛开始前 10 分钟，认真阅读《比赛任务书》，须在确认竞赛内容和现场设备等无误后在裁判长宣布比赛开始后参与竞赛。如果违规先行做诸如打开显示器、制作线缆等任何操作，经裁判提示注意后仍无效，将酌情扣分，情节严重报经裁判长批准

取消参赛资格。

（6）参赛选手必须在指定区域，按规范要求操作竞赛设备，严格遵守比赛纪律。如果违反，经裁判提示注意后仍无效，将酌情扣分，情节严重的终止其比赛。一旦出现严重的安全事故，报经裁判长批准取消参赛资格。

（7）参赛选手应严格遵守赛场规章、操作规程和工艺准则，保证人身及设备安全，接受裁判员的监督和警示。

（8）竞赛期间，选手饮水等由赛场统一提供，不得自带。选手休息、饮食或如厕时间均计算在比赛时间内。

（9）在竞赛过程中，参赛选手如有不服从裁判判决、扰乱赛场秩序、舞弊等不文明行为的，由裁判长按照规定扣减相应分数，情节严重的取消比赛资格，比赛成绩记 0 分。

（10）在竞赛过程中，确因软件或硬件故障，导致操作无法继续的，经赛项裁判长确认，予以启用备用设备，由此耽误的比赛时间将予以补时。经现场技术人员、裁判和裁判长确认，如因个人操作导致设备系统故障，不予以补时处理。

（11）竞赛时间终了，选手应全体起立，结束操作。将资料和工具整齐摆放在操作平台上，经签字确认，工作人员清点后方可离开赛场，离开赛场时不得带走任何资料。

（12）在竞赛期间，未经执委会批准，参赛选手不得接受其他单位和个人进行的与竞赛内容相关的采访。参赛选手不得将竞赛的相关信息私自公布。

（13）所有选手在赛后必须参加闭幕式，如有特殊情况确实无法参加，应向领队说明情况，由领队向赛点学校提出书面申请，并报竞赛组委会办公室备案。

4. 竞赛直播

1. 赛点提供全程无盲点录像。
2. 不提供现场观摩。

九、竞赛任务书

2023 年湖南省“楚怡杯”职业院校技能竞赛

中职组 网络搭建与应用 赛项

[时量：240 分钟，试卷号：]

（样卷）

竞赛任务书

场次号：_____ 机位号（工位号）：____

（一）竞赛内容

“网络搭建与应用”竞赛共分三个部分，其中：

第一部分：职业规范与素养　　（5分）

第二部分：网络搭建及安全部署项目　（50分）

第三部分：服务器配置及应用项目　　（45分）

（二）竞赛注意事项

1.禁止携带和使用移动存储设备、计算器、通信工具及参考资料。

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

3.请参赛选手仔细阅读赛卷，按照要求完成各项操作。

4.操作过程中，需要及时保存配置命令。

5.比赛结束后，所有设备保持运行状态，评判以最后的硬件连接和提交文档为最终结果。

6.比赛完成后，禁止将比赛所用的所有物品（包括赛卷）带离赛场。

7.禁止在纸质资料、比赛设备和电脑桌上作任何与竞赛无关的标记，如违反规定，可视为0分。

8.与比赛相关的软件和《网络搭建及安全部署竞赛结果提交指南》、《服务器配置及应用竞赛结果提交指南》存放在物理机的D:\soft文件夹中。

9.请在物理机PC1桌面上新建“XXX”文件夹作为“选手目录”，用以保存按照《网络搭建及安全部署竞赛结果提交指南》、《服务器配置及应用竞赛结果提交指南》要求生成的全部结果文档。（XXX为赛位号。举例：1号赛位，文件夹名称为“001”）重要提示：选手目录如缺少文档，相应分值计为0分。

（三）竞赛说明

1.请根据物理机“D:\soft\网络搭建及安全部署竞赛结果提交指南、服务器配置及应用竞赛结果提交指南”的要求生成文档，将生成文档复制到选手目录。

2.收集防火墙信息时，需要先调整SecureCRT软件字符编号为：UTF-8（提示：默认是UTF-8），否则收集的命令行中文信息会显示乱码。

网络搭建及安全部署

项目简介：

某集团公司原在北京建立了总公司，后在成都建立了分公司，又在广东设立了一个办事处。集团设有营销、产品、法务、财务、人力5个部门，统一进行IP及业务资源的规划和分配，全网采用RIP、ISIS、OSPF和BGP路由协议进行互联互通。2022年在党的坚强领导下，全年公司规模保持快速增长，业务数据量和公司访问量增长巨大，不断开创新局面，向着全面建成社会主义现代化强国的第二个百年奋斗目标迈进。

为了更好管理数据，提供服务，集团决定在北京建立两个数据中心，在贵州建立异地灾备数据中心，以达到快速、可靠交换数据，增强业务部署弹性的目的，完成向两地三中心整体战略架构演进，更好的服务于公司客户。

集团、成都分公司及广东办事处的网络结构详见拓扑图。SW1和SW2分别作为集团北京两个DC的核心交换机；SW3作为灾备DC的核心交换机；两台防火墙FW1和FW2分别作为集团互联网出口、广东办事处的防火墙；RT1作为集团的核心路由器；RT2作为分公司的路由器；AC1作为分公司的有线无线智能一体化控制器，通过与高性能企业级AP配合实现分公司无线覆盖。

请注意：在此典型互联网应用网络架构中，作为 IT 网络运维人员，请根据拓扑构建完整的系统环境，使整体网络架构具有良好的稳定性、安全性、可扩展性。请完成所有服务配置后，从客户端进行测试，确保能正常访问到相应应用。

网络拓扑：

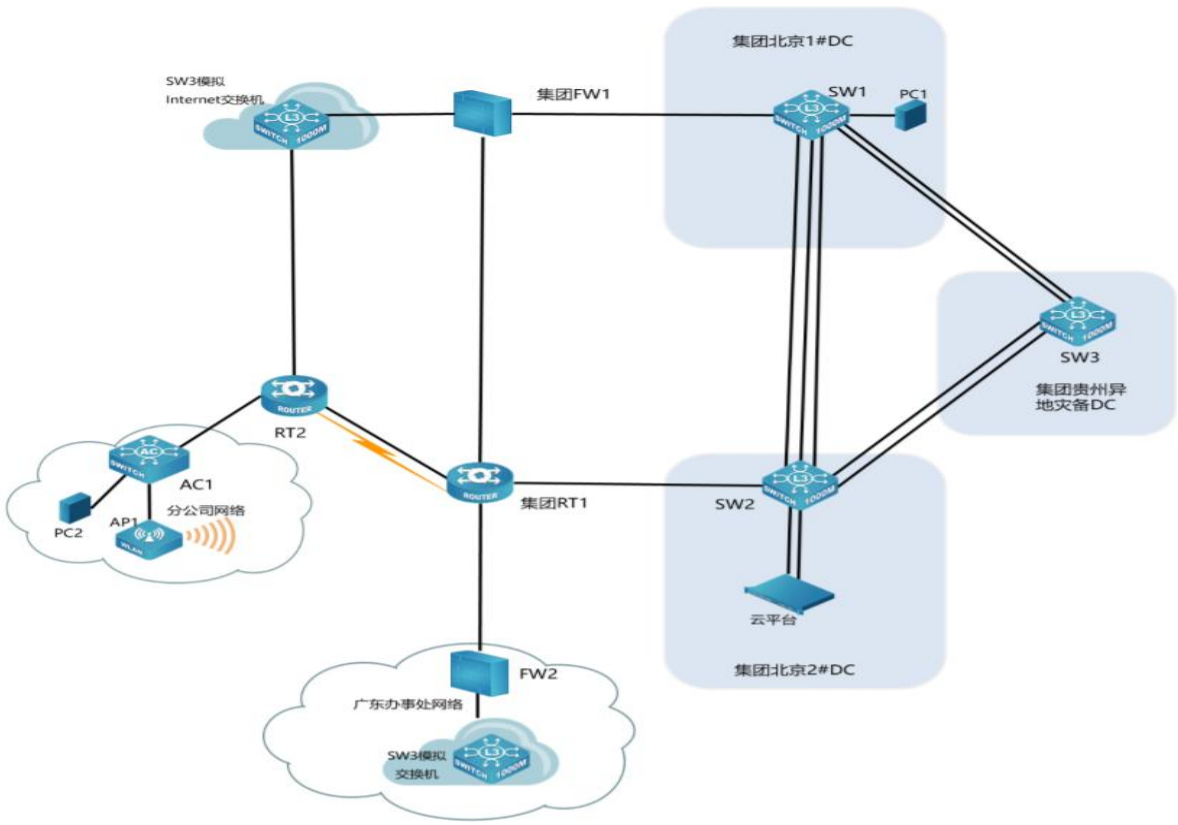

表 1-网络设备连接表

A 设备连接至 B 设备			
设备名称	接口	设备名称	接口
RT1	G0/0	RT2	G0/0
RT1	S1/0	RT2	S1/1
RT1	S1/1	RT2	S1/0
RT1	G0/1	SW2	E1/0/21
RT1	G0/2	FW1	E0/2
RT1	G0/3	FW2	E0/2
RT2	G0/1	AC1	E1/0/1
RT2	G0/3	SW3 模拟 Internet 交换机	E1/0/18
FW1	E0/3	SW3 模拟 Internet 交换机	E1/0/17
FW1	E0/1	SW1	E1/0/21
FW2	E0/1	SW3 模拟 办事处交换机	E1/0/15
SW1	E1/0/26(实现三层 IP 业务承载)	SW2	E1/0/26(实现三层 IP 业务承载)
SW1	E1/0/27(实现 VPN 业务承载)	SW2	E1/0/27(实现 VPN 业务承载)
SW1	E1/0/28(实现二层业务承载)	SW2	E1/0/28(实现二层业务承载)
SW1	E1/0/22	SW3	E1/0/21
SW1	E1/0/23（二层）	SW3	E1/0/23（二层）
SW2	E1/0/22	SW3	E1/0/22
SW2	E1/0/23（二层）	SW3	E1/0/24（二层）
SW1	E1/0/1	PC1	NIC
SW2	E1/0/11	云平台	Eth1
SW2	E1/0/12	云平台	Eth2
AC1	E1/0/3	AP1	ETH
AC1	E1/0/4 vlan210	PC2	NIC
SW3 模拟办事处	E1/0/11	模拟产品 PC	
SW3 模拟办事处	E1/0/12	模拟营销 PC	

表二网络设备 IP 地址分配表

设备名称	设备接口	IP 地址
SW1	Loopback1 OSPFv2 OSPFv3 BGP	10.10.1.1/32 2001:10:10:1::1/128
	Loopback2	10.10.1.2/32 2001:10:10:1::2/128
	vlan11	10.10.11.1/24 2001:10:10:11::1/64
	vlan12	10.10.12.1/24 2001:10:10:12::1/64
	vlan13	10.10.13.1/24 2001:10:10:13::1/64
	vlan14	10.10.14.1/24 2001:10:10:14::1/64
	vlan15	10.10.15.1/24 2001:10:10:15::1/64
	vlan60	10.10.60.1/24 2001:10:10:60::1/64
	vlan70	10.10.70.1/24 2001:10:10:70::1/64
	vlan80	10.10.80.1/24 2001:10:10:80::1/64
	vlan90	10.10.90.1/24 2001:10:10:90::1/64
	vlan1021	10.10.255.14/30
	vlan1022	10.10.255.5/30
	vlan1026	10.10.255.1/30
	vlan1027 VPN	10.10.255.1/30
SW2	Loopback1 OSPFv2 OSPFv3 BGP	10.10.2.1/32 2001:10:10:2::1/128
	Loopback2	10.10.2.2/32 2001:10:10:2::2/128
	vlan21	10.10.21.1/24 2001:10:10:21::1/64
	vlan22	10.10.22.1/24 2001:10:10:22::1/64
	vlan23	10.10.23.1/24 2001:10:10:23::1/64
	vlan24	10.10.24.1/24 2001:10:10:24::1/64
	vlan25	10.10.25.1/24 2001:10:10:25::1/64
	vlan60	10.10.60.2/24

设备名称	设备接口	IP 地址
		2001:10:10:60::2/64
	vlan70	10.10.70.2/24 2001:10:10:70::2/64
	vlan80	10.10.80.2/24 2001:10:10:80::2/64
	vlan90	10.10.90.2/24 2001:10:10:90::2/64
	vlan1021	10.10.255.22/30
	vlan1022	10.10.255.9/30
	vlan1026	10.10.255.2/30
	vlan1027 VPN	10.10.255.2/30
SW3	Loopback1 OSPFv2 OSPFv3 BGP	10.10.3.1/32 2001:10:10:3::1/128
	vlan31	10.10.31.1/24 2001:10:10:31::1/64
	vlan32	10.10.32.1/24 2001:10:10:32::1/64
	vlan33	10.10.33.1/24 2001:10:10:33::1/64
	vlan35	10.10.35.1/24 2001:10:10:35::1/64
	vlan60	10.10.60.3/24 2001:10:10:60::3/64
	vlan70	10.10.70.3/24 2001:10:10:70::3/64
	vlan80	10.10.80.3/24 2001:10:10:80::3/64
	vlan90	10.10.90.3/24 2001:10:10:90::3/64
	vlan1021	10.10.255.6/30
	vlan1022	10.10.255.10/30
SW3 模拟办事处	Loopback2	10.10.3.2/32 2001:10:10:3::2/128
	vlan230	10.10.230.1/24 2001:10:10:230::1/64
	vlan240	10.10.240.1/24 2001:10:10:240::1/64
	vlan1015	10.10.255.46/30
SW3 模拟 Internet	Loopback3	200.200.3.3/32 2001:200:200:3::3/128
	vlan1017	200.200.200.1/30
	vlan1018	200.200.200.5/30

设备名称	设备接口	IP 地址
AC1	Loopback1 OSPFv2 OSPFv3	10.10.4.1/32 2001:10:10:4::1/128
	Loopback2 RIP RIPng	10.10.4.2/32 2001:10:10:4::2/128
	Loopback3	10.10.4.3/32 2001:10:10:4::3/128
	vlan200 无线管理	10.10.200.1/24 2001:10:10:200::1/64
	vlan210 无线 2.4G 产品	10.10.210.1/24 2001:10:10:210::1/64
	vlan220 无线 5G 营销	10.10.220.1/24 2001:10:10:220::1/64
	vlan1001	10.10.255.42/30
RT1	Loopback1 OSPFv2 OSPFv3 BGP MPLS	10.10.5.1/32 2001:10:10:5::1/128
	Loopback2 RIP RIPng	10.10.5.2/32 2001:10:10:5::2/128
	Loopback3 ISIS	10.10.5.3/32 2001:10:10:5::3/128
	Loopback4 集团与办事处互联	10.10.5.4/32 2001:10:10:5::4/128
	Loopback5 VPN 财务	10.10.5.5/32 2001:10:10:5::5/128
	G0/0	10.10.255.29/30
	G0/1	10.10.255.21/30
	G0/2	10.10.255.18/30
	G0/3	10.10.255.25/30
	S1/0	10.10.255.33/30
	S1/1	10.10.255.37/30
RT2	Loopback1 OSPFv2 OSPFv3 BGP MPLS	10.10.6.1/32 2001:10:10:6::1/128
	Loopback2 RIP RIPng	10.10.6.2/32 2001:10:10:6::2/128
	Loopback3 ISIS	10.10.6.3/32 2001:10:10:6::3/128
	Loopback4 IPSecVPN	10.10.6.4/32 2001:10:10:6::4/128
	tunnel4 IPSecVPN	10.10.255.50/30
	Loopback5 VPN 财务	10.10.5.5/32 2001:10:10:5::5/128
	G0/0	10.10.255.30/30
	G0/1	10.10.255.41/30

设备名称	设备接口	IP 地址
	G0/3	200.200.200.6/30
	S1/0	10.10.255.38/30
	S1/1	10.10.255.34/30
FW1	Loopback1 OSPFv2 OSPFv3 trust	10.10.7.1/32 2001:10:10:7::1/128
	Loopback2 RIP RIPng trust	10.10.7.2/32 2001:10:10:7::2/128
	Loopback4 IPSecVPN trust	10.10.7.4/32 2001:10:10:7::4/128
	tunnel4 IPSecVPN VPNHUB	10.10.255.49/30
	E0/1 trust	10.10.255.13/30
	E0/2 trust	10.10.255.17/30
	E0/3 untrust	200.200.200.2/30
FW2	Loopback1 OSPFv2 OSPFv3 trust	10.10.8.1/32 2001:10:10:8::1/128
	E0/1 trust	10.10.255.45/30
	E0/2 dmz	10.10.255.26/30

一、职业规范与素养

1.整理赛位，工具、设备归位，保持赛后整洁有序。

2.无因选手原因导致设备损坏。

3.恢复调试现场，保证网络和系统安全运行。

二、网络布线与基础连接

1.截取适当长度的双绞线，端接水晶头，制作网络跳线，所有网络跳线要求按 568B 标准制作。

2.根据网络拓扑要求,将跳线插入相应设备的相关端口上；实现 PC、设备之间的连通；（提示：可交换机设备进行通断测试）。

三、交换配置

1.配置 vlan，SW1、SW2、SW3、AC1 的二层链路只允许相应 vlan 通过。

设备	vlan 编号	端口	说明
SW1	vlan11	E1/0/1	产品 1 段
	vlan12	E1/0/2	营销 1 段
	vlan13	E1/0/3	法务 1 段
	vlan14	E1/0/4	财务 1 段
	vlan15	E1/0/5	人力 1 段
	vlan60	E1/0/6	产品管理
	vlan70	E1/0/7	产品研发
	vlan80	E1/0/8	产品生产
	vlan90	E1/0/9	产品支持
SW2	vlan21	E1/0/1	产品 2 段
	vlan22	E1/0/2	营销 2 段
	vlan23	E1/0/3	法务 2 段
	vlan24	E1/0/4	财务 2 段
	vlan25	E1/0/5	人力 2 段
	vlan60	E1/0/6	产品管理
	vlan70	E1/0/7	产品研发
	vlan80	E1/0/8	产品生产
	vlan90	E1/0/9	产品支持
SW3	vlan31	E1/0/1	产品 3 段
	vlan32	E1/0/2	营销 3 段
	vlan33	E1/0/3	法务 3 段
	vlan35	E1/0/5	人力 3 段
	vlan60	E1/0/6	产品管理
	vlan70	E1/0/7	产品研发
	vlan80	E1/0/8	产品生产
	vlan90	E1/0/9	产品支持

2.SW1、SW2、SW3 启用 MSTP，实现网络 L2(二层)负载均衡和冗余备份，创建实例 Instance10 和 Instance20，名称为 skills，修订版本为 1，其中 Instance10 关联 vlan60 和 vlan70，Instance20 关联 vlan80 和 vlan90。SW1 为 Instance0 和 Instance10 的根交换机，为 Instance20 备份根交换机；SW2 为 Instance20 根交换机，为 Instance0 和 Instance10 的备份根交换机；根交换机 STP 优先级为 0，备份根交换机 STP 优先级为 4096。关闭交换机之间 L3(三层)互联接口的 STP。

3.SW1 和 SW2 之间利用三条裸光缆实现互通，其中一条裸光缆承载三层 IP 业务、一条裸光缆承载 VPN 业务、一条裸光缆承载二层业务。用相关技术分别实现财务 1 段、财务 2 段业务路由表与其它业务路由表隔离，财务业务 VPN 实例名称为 CW。

4.将 SW3 模拟为 Internet 交换机，实现与集团其它业务路由表隔离，Internet 路由表 VPN 实例名称为 Internet。将 SW3 模拟办事处交换机，实现与集团其它业务路由表隔离，办事处路由表 VPN 实例名称为 Guangdong。

5.SW1 和 SW2 所有端口启用链路层发现协议，更新报文发送时间间隔为 20s，老化时间乘法器值为 5，Trap 报文发送间隔为 10s，配置三条裸光缆端口使能 Trap 功能。

四、路由配置

1.启用所有设备的 ssh 服务，防火墙用户名 admin，明文密码 Pass-1234，其余设备用户名和明文密码均为 admin。

2.配置所有设备的时区为 GMT+08:00，调整 SW1 时间为实际时间，SW1 配置为 ntp server，其他设备用 SW1 Loopback1 IPv4 地址作为 ntp server 地址，ntp client 请求报文时间间隔 1 分钟。

3.配置接口 IPv4 地址和 IPv6 地址，互联接口 IPv6 地址用本地链路地址。

4.利用 VRRPv2 和 VRRPv3 技术实现 vlan60、vlan70、vlan80、vlan90 网关冗余备份，VRRP ID 与 vlan ID 相同。VRRPv2 VIP 为 10.10.vlanID.9（如 vlan60 的 VRRPv2 VIP 为 10.10.60.9），VRRPv3 VIP 为 FE80:vlanID::9（如 vlan60 的 VRRPv3 VIP 为 FE80:60::9）。配置 SW1 为 vlan60、vlan70 的 Master，SW2 为 vlan80、vlan90 的 Master。要求 VRRP 组中高优先级为 120，低优先级为默认值，抢占模式为默认值，VRRPv2 和 VRRPv3 发送通告报文时间间隔为默认值。当 SW1 或 SW2 上联链路发生故障，Master 优先级降低 30。

5.SW2 配置 DHCPv4 和 DHCPv6，分别为 SW1 产品 1 段网络 vlan11、SW2 产品 1 段网络 vlan21、分公司网络 vlan200&vlan210&vlan220 分配地址；IPv4 地址池名称分别为 POOLv4-vlan11、POOLv4-vlan21、POOLv4-vlan200、POOLv4-vlan210、POOLv4-vlan220，排除网关,DNS 为 10.10.110.101 和 10.10.120.101。IPv6 地址池名称分别为 POOLv6-vlan11、POOLv6-vlan21、POOLv6-vlan200、POOLv6-vlan210、POOLv6-vlan220，IPv6 地址池用网络前缀表示，排除网关，DNS 为 2400:3200::1；为 PC1 保留地址 10.10.11.9 和 2001:10:10:11::9，为 AP1 保留地址 10.10.200.9 和 2001:10:10:200::9。SW1

和 AC1 中继地址为 SW2 Loopback1 地址。SW1 启用 DHCPv4 和 DHCPv6 snooping，如果 E1/0/1 连接 DHCPv4 服务器，则关闭该端口，恢复时间为 10 分钟。

6.SW1、SW2、SW3、RT1 以太链路、RT2 以太链路、FW1、FW2、AC1 之间运行 OSPFv2 和 OSPFv3 协议（路由模式发布网络用接口地址，BGP 协议除外）。

(1)SW1、SW2、SW3、RT1、RT2、FW1 之间 OSPFv2 和 OSPFv3 协议，进程 1，区域 0，分别发布 Loopback1 地址路由和产品路由，FW1 通告 type1 默认路由。

(2)RT2 与 AC1 之间运行 OSPFv2 协议，进程 1，nssa no-summary 区域 1；AC1 发布 Loopback1 地址路由、产品和营销路由，用 prefix-list 重发布 Loopback3。

(3)RT2 与 AC1 之间运行 OSPFv3 协议，进程 1，stub no-summary 区域 1；AC1 发布 Loopback1 地址路由、产品和营销。

(4)SW3 模拟办事处产品和营销接口配置为 Loopback，模拟接口 up。SW3 模拟办事处与 FW2 之间运行 OSPFv2 协议，进程 2，区域 2，SW3 模拟办事处发布 Loopback2、产品和营销。SW3 模拟办事处配置 IPv6 默认路由；FW2 分别配置到 SW3 模拟办事处 Loopback2、产品和营销的 IPv6 明细静态路由，FW2 重发布静态路由到 OSPFv3 协议。

(5)RT1、FW2 之间 OSPFv2 和 OSPFv3 协议，进程 2，区域 2；RT1 发布 Loopback4 路由，向该区域通告 type1 默认路由；FW2 发布 Loopback1 路由，FW2 禁止学习到集团和分公司的所有路由。RT1 用 prefix-list 匹配 FW2 Loopback1 路由、SW3 模拟办事处 Loopback2 和产品路由、RT1 与 FW2 直连 IPv4 路由，将这些路由重发布到区域 0。

(6)修改 OSPF cost 为 100，实现 SW1 分别与 RT2、FW2 之间 IPv4 和 IPv6 互访流量优先通过 SW1_SW2_RT1 链路转发，SW2 访问 Internet IPv4 和 IPv6 流量优先通过 SW2_SW1_FW1 链路转发。

7.RT1 串行链路、RT2 串行链路、FW1、AC1 之间分别运行 RIP 和 RIPng 协议，FW1、RT1、RT2 的 RIP 和 RIPng 发布 Loopback2 地址路由，AC1 RIP 发布 Loopback2 地址路由，AC1 RIPng 采用 route-map 匹配 prefix-list 重发布 Loopback2 地址路由。RT1 配置 offset 值为 3 的路由策略，实现 RT1-S1/0_RT2-S1/1 为主链路，RT1-S1/1_RT2-S1/0 为备份链路，IPv4 的 ACL 名称为 ACLv4，IPv6 的 ACL 名称为 ACLv6。RT1 的 S1/0 与 RT2 的 S1/1 之间采用 chap 双向认证，用户名为对端设备名称，密码为 Pass-1234。

8.RT1 以太链路、RT2 以太链路之间运行 ISIS 协议，进程 1，分别实现 Loopback3 之间 IPv4 互通和 IPv6 互通。RT1、RT2 的 NET 分别为 10.0000.0000.0001.00、10.0000.0000.0002.00，路由器类型是 Level-2，接口网络类型为点到点。配置域 md5 认证和接口 md5 认证，密码均为 Pass-1234。

9.RT2 配置 IPv4 nat，实现 AC1 IPv4 产品用 RT2 外网接口 IPv4 地址访问 Internet。RT2 配置 nat64，实现 AC1 IPv6 产品用 RT2 外网接口 IPv4 地址访问 Internet，IPv4 地址转 IPv6 地址前缀为 64:ff9b::/96。

10.SW1、SW2、SW3、RT1、RT2 之间运行 BGP 协议，SW1、SW2、RT1 AS 号 65001、RT2 AS 号 65002、SW3 AS 号 65003。

11.SW1、SW2、SW3、RT1、RT2 之间通过 Loopback1 建立 IPv4 和 IPv6 BGP 邻居。SW1 和 SW2 之间财务通过 Loopback2 建立 IPv4 BGP 邻居，SW1 和 SW2 的 Loopback2 互通采用静态路由。

12.SW1、SW2、SW3、RT2 分别只发布营销、法务、财务、人力等 IPv4 和 IPv6 路由；RT1 发布办事处营销 IPv4 和 IPv6 路由到 BGP。

13.SW3 营销分别与 SW1 和 SW2 营销 IPv4 和 IPv6 互访优先在 SW3_SW1 链路转发；SW3 法务及人力分别与 SW1 和 SW2 法务及人力 IPv4 和 IPv6 互访优先在 SW3_SW2 链路转发，主备链路相互备份；用 prefix-list、route-map 和 BGP 路径属性进行选路，新增 AS 65000。

14.利用 BGP MPLS VPN 技术，RT1 与 RT2 以太链路间运行多协议标签交换、标签分发协议。RT1 与 RT2 间创建财务 VPN 实例，名称为 Finance，RT1 的 RD 值为 1:1，export rt 值为 1:2，import rt 值为 2:1；RT2 的 RD 值为 2:2。通过两端 Loopback1 建立 VPN 邻居，分别实现两端 Loopback5 IPv4 互通和 IPv6 互通。

五、无线配置

1.AC1 Loopback1 IPv4 和 IPv6 地址分别作为 AC1 的 IPv4 和 IPv6 管理地址。AP 二层自动注册，AP 采用 MAC 地址认证。

2.配置 2 个 SSID，分别为 skills-2.4G 和 skills-5G。skills-2.4G 对应 vlan210，用 network 210 和 radio1（模式为 n-only-g）,用户接入无线网络时需要采用基于 WPA-personal 加密方式，密码为 Pass-1234。skills-5G 对应 vlan220,用 network 220 和 radio2(模式为 n-only-a),不需要认证,隐藏 SSID，skills-5G 用倒数第一个可用 VAP 发送 5G 信号。

3.防止多 AP 和 AC 相连时过多的安全认证连接而消耗 CPU 资源，检测到 AP 与 AC10 分钟内建立连接 5 次就不再允许继续连接，2 小时后恢复正常。

六、安全配置

说明：ip 地址按照题目给定的顺序用“ip/mask”表示，IPv4 any 地址用 0.0.0.0/0，IPv6 any 地址用::/0，禁止用地址条目，否则按零分处理。

1. FW1 配置 IPv4 nat，实现集团产品 1 段 IPv4 访问 Internet IPv4，转换 ip/mask 为 200.200.200.16/28,保证每一个源 ip 产生的所有会话将被映射到同一个固定的 IP 地址。

2. FW1 配置 nat64，实现集团产品 1 段 IPv6 访问 Internet IPv4，转换为出接口 IP，IPv4 转 IPv6 地址前缀为 64:ff9b::/96。

3. FW1 和 FW2 策略默认动作为拒绝，FW1 允许集团产品 1 段 IPv4&IPv6 访问 Internet 任意服务。

4. FW2 允许办事处产品 IPv4&IPv6 访问集团产品 1 段 https 服务，允许集团产品 1 段 IPv4&IPv6 和分公司产品 IPv4&IPv6 访问办事处产品、FW2 Loopback1、SW3 模拟办事处 Loopback2。

5. FW1 与 RT2 之间用 Internet 互联地址建立 GRE Over IPSec VPN，实现 Loopback4 之间的加密访问。

服务器配置及应用

赛项说明：

1.请根据物理机“D:\soft\服务器配置及应用竞赛结果提交指南.docx”的要求生成文档，将生成的文档复制到“选手目录”。

2.云平台 web 网址 http://192.168.100.100/dncloud，登录管理员为 admin，密码为 dncloud。

3.Windows/Linux 虚拟机中 Administrator/root 用户密码为 Pass-1234，题目中所有未指定的密码均用该密码。

4.虚拟主机的 IP 地址必须手动设置为该虚拟机自动获取的 IP 地址（提示：先新建固定 IP 地址的端口，为了测试的需要，关闭端口安全；然后创建实例并指定端口）。

5.所有 windows 虚拟机都启用了远程桌面连接，所有 linux 虚拟机都启用了 ssh。

6.所有服务器要求虚拟机系统重新启动后，均能正常启动和使用。

7.使用完全合格域名访问网络资源。

一、云平台连接和配置

1.根据拓扑图连接交换机和云平台，并进行相关配置.

2.网络信息表

网络名称	VlanID	子网名称	网络地址	网关	IPv4 地址池
Network110	110	Subnet110	10.10.110.0/24	10.10.110.254	10.10.110.100-10.10.110.200
Network120	120	Subnet120	10.10.120.0/24	10.10.120.254	10.10.120.100-10.10.120.200

3.实例类型信息表

名称	VCPU	内存(MB)	磁盘(GB)	实例名称	镜像模板
Skills	4	4096	40	windows1 至 windows7	windows2022
skills	4	4096	40	linux1 至 linux7	rocky8.6

4.实例信息表

实例名称	IPv4 地址	完全合格域名
windows1	10.10.110.101	windows1.skills.com
windows2	10.10.110.102	windows2.skills.com
windows3	10.10.110.103	windows3.skills.com
windows4	10.10.110.104	windows4.skills.com
windows5	10.10.110.105	windows5.skills.com
windows6	10.10.110.106	windows6.skills.com
windows7	10.10.110.107	windows7.skills.com
linux1	10.10.120.101	linux1.skills.com
linux2	10.10.120.102	linux2.skills.com
linux3	10.10.120.103	linux3.skills.com
linux4	10.10.120.104	linux4.skills.com
linux5	10.10.120.105	linux5.skills.com
linux6	10.10.120.106	linux6.skills.com
linux7	10.10.120.107	linux7.skills.com

二、Windows 服务配置

（一）域服务

1.配置 windows1 为域控制器，域名为 skills.com；安装 DNS 服务，为所有的 Windows 服务器提供正反向解析;配置 windows2 为额外域控制器和第二台 DNS 服务器。

2.配置 windows1 为证书服务器,设置为企业根,CA 有效期 10 年,为 windows 服务器颁发证书，证书颁发机构的公用名为 windows1.skills.com。复制“计算机”模板证书，名称为“计算机副本”，根据该模板申请并颁发一张供 windows 服务器使用的证书,证书友好名称为 skills,(将证书导入到需要证书的 windows 服务器),证书信息:证书有效期=5 年,公用名=skills.com,国家=CN,省=Beijing,城市=Beijing,组织=skills,组织单位=system,使用者可选名称=*.skills.com 和 skills.com。浏览器访问 https 网站时，不出现证书警告信息。

3.配置 windows2 为从属证书服务，证书颁发机构的公用名为 windows2.skills.com。

4.把所有的 Windows 主机加入到域。

5.新建名称为 manager、dev、sale 的 3 个组织单元；每个组织单元内新建与组织单元同名的全局安全组;每个组内新建 20 个用户:manager00-manager19、sale00-sale19、dev00-dev19。

6. 新建 C:\sharedoc 共享文件夹，共享名称为 ShareDoc；在 AD DS 中发布该共享。

7. 新建 C:\documents 共享文件夹，共享名同文件夹名；所有用户到域计算机登录，“文档”文件夹重定向到\\windows1\documents。

（二）文件共享服务

1.在 windows1 的 C 分区划分 2GB 的空间，创建 NTFS 分区，驱动器号为 d;创建用户主目录共享文件夹：本地目录为 D:\share\home，共享名为 home，允许所有域用户完全控制。在本目录下为所有用户添加一个以用户名命名的文件夹，该文件夹将设置为所有域用户的 home 目录，用户登录计算机成功后，自动映射挂载到 h 卷。禁止用户在该共享文件中创建“*.exe”文件，文件组名和模板名为 my。

2.创建目录 D:\share\work,共享名为 work,仅 manager 组和 Administrator 组有完全控制的安全权限和共享权限,其他认证用户有读取执行的安全权限和共享权限。在 AD DS 中发布该共享。

（三）Web 服务配置

1.把 windows3 配置为 ASP 网站，安装 ASP.NET 4.8，站点名称为 asp。

2.http 和 https 绑定本机与外部通信的 IP 地址,仅允许使用域名访问,http 自动跳转到 https。

3.网站目录为 C:\iis\contents，默认文档 index.aspx 内容为"HelloASP"

4.新建虚拟目录 dev，对应物理目录 C:\development，该虚拟目录仅启用 windows 身份验证，默认文档 index.html 内容为"development"。

（四）打印服务配置

1.在 windows4 上安装打印机，驱动程序为“Ms Publisher Color Printer”，名称和共享名称均为“ skillsprinter”；在域中发布共享；使用组策略部署在"Default Domain Policy"的计算机。

2.网站名称为 skillssite，http 和 https 绑定主机 IP 地址，仅允许使用域名访问，启用 hsts，实现 http 访问自动跳转到 https（使用“计算机副本”证书模板）。

3.用浏览器访问打印机虚拟目录 printers 时，启用匿名身份认证，匿名用户为 manager00。

4.新建虚拟目录 dev，对应物理目录 C:\development，该虚拟目录启用 windows 身份验证，默认文档 index.html 内容为"development"。

（五）DFS 服务配置

1.在 windows5、windows6、windows7 的 C 分区各划分 2GB 的空间，创建 NTFS 主分区，驱动器号为 D，分别新建文件夹 D:\web，设置该文件夹共享，共享名称为 web。

2.配置 windows5 为 DFS 服务器，命名空间为 dfsroot，文件夹为 web，存储在 D:\web；实现\\WINDOWS6\web 和\\WINDOWS7\web 同步。

三、Linux 服务

（一） CA 服务配置

1.启用所有 Linux 服务器的防火墙，防火墙区域为 public，在防火墙中放行对应服务端口。

2.配置服务后，该服务开机自启动。

3.配置 linux1 为主要 DNS 服务器，linux2 为辅助 DNS 服务器，为所有 linux 服务器提供正反向解析。

4.所有 linux 主机 root 用户使用完全合格域名免密码 ssh 登录到其他 linux 主机。

5.linux1 安装 chrony，为所有 Linux 服务器提供时间同步。

6.配置 linux1 为 CA 服务器，为 linux 服务颁发证书。证书颁发机构有效期 10 年，公用名为 linux1.skills.com。申请并颁发一张供 linux 服务器使用的证书，证书信息：有效期=5 年，公用名=skills.com，国家=CN，省=Beijing，城市=Beijing，组织=skills，组织单位=system，使用者可选名称=*.skills.com 和 skills.com。将证书 skills.crt 和私钥 skills.key 复制到需要证书的 linux 服务器/etc/ssl 目录。浏览器访问 https 网站时，不出现证书警告信息。

（二）Web 服务配置

1.配置 linux2 为 web 服务器，安装 apache2，网站根目录为/https，默认文档 index.html 的内容为“Apache”；仅允许使用域名访问，http 访问自动跳转到 https。

（三）Tomcat 服务配置

1.配置 linux3 为 Tomcat 服务器，主页文件内容为“TomcatSkills”，仅允许域名访问，配置端口转发，http 80 端口转发到 8080，https 443 端口转发到 8443 端口，http 访问自动跳转到 https 端口；证书路径为/etc/ssl/skills.pfx。

（四）nginx 服务配置

1.配置 linux5 为 web 服务器，安装 nginx，默认文档 index.html 的内容为“Nginx”；仅允许使用域名访问，http 访问自动跳转到 https。

（五）NFS 服务配置

1.配置 linux1 为 KDC 服务器，负责 linux3 和 linux4 的验证。

2.在 linux3 上，创建用户，用户名为 tom，uid=2222，gid=2222，家目录为/home/tomdir。

3.配置 linux3 为 nfs 服务器，按下面要求新建共享：

共享目录	共享要求
/var/nfs1	10.10.120.0/24 网络用户具有读写权限，所有用户映射为 tom。kdc 加密方式为 krb5p;
/var/nfs2	所有人都可以读写，都不改变身份，但不可删除别人的文件。kdc 加密方式为 krb5p;

4.在 linux4 上，设置用户的密码长度最少为 6 位，普通用户的最小 id 为 2000。

5.配置 linux4 为 nfs 客户端，利用 autofs 按需挂载 linux3 上的/var/nfs1 到/nfs1，挂载 linux3 上的/var/nfs2 到/nfs2，挂载成功后创建/nfs1/test1 目录和/nfs2/test2 目录。

（六）mariadb 服务配置

1.配置 linux3 为 mariadb 服务器，创建数据库用户 xiao，在任意机器上对所有数据库有完全权限。

2.配置 linux4 为 mariadb 客户端，创建数据库 userdb；在库中创建表 userinfo，表结构如下：

字段名	数据类型	主键	自增
id	int	是	是
name	varchar(10)	否	否
birthday	datetime	否	否
sex	varchar(5)	否	否
password	varchar(200)	否	否

3.在表中插入 2 条记录，分别为(1,user1，1999-07-01，男)，(2,user2，1999-07-02,女),password 与 name 相同,password 字段用 password 函数加密。

4.修改表 userinfo 的结构，在 name 字段后添加新字段 height(数据类型为 float)，更新 user1 和 user2 的 height 字段内容为 1.61 和 1.62。

5.新建/var/databak/userinfo.txt 文件，文件内容如下，然后将文件内容导入到 userinfo 表中，password 字段用 password 函数加密。

3,user3,1.63,1999-07-03,女,user3
4,user4,1.64,1999-07-04,男,user4
5,user5,1.65,1999-07-05,男,user5
6,user6,1.66,1999-07-06,女,user6
7,user7,1.67,1999-07-07,女,user7
8,user8,1.68,1999-07-08,男,user8
9,user9,1.69,1999-07-09,女,user9

6.将表 userinfo 中的记录导出，并存放到/var/databak/mysql.sql，字段之间用','分隔。

7.每周五凌晨 1:00 以 root 用户身份备份数据库 userdb 到/var/databak/userdb.sql(含创建数据库命令)。

（七）虚拟化服务

1.分别在 linux6 和 linux7 上安装 containerd 和 kubernetes，linux6 作为 master node，linux7 作为 work node；containerd 的 namespace 为 k8s.io，使用 containerd.sock 作为容器 runtime-endpoint 和 image-endpoint。

2.master 节点配置 calico，作为网络组件。