

2020 年全国职业院校技能大赛

改革试点赛

网络搭建与应用竞赛

正式赛卷

(三)

技能要求

(总分 1000 分)

ZZ-2020004 网络搭建与应用赛项执委会及专家组

2020 年 11 月 26 日

竞赛说明

一、竞赛内容分布

“网络搭建与应用”竞赛共分三个部分，其中：

第一部分：网络搭建及安全部署项目（500 分）

第二部分：服务器配置及应用项目（480 分）

第三部分：职业规范与素养（20 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、软件清单、材料清单是否齐全，计算机设备是否能正常使用。
3. 请选手仔细阅读比赛试卷，按照试卷要求完成各项操作。
4. 操作过程中，需要及时保存设备配置。
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配置为最终结果。
6. 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。
7. 禁止在各类纸质资料、比赛设备、比赛报告上填写任何与竞赛无关的标记，如违反规定，可视为 0 分。
8. 与比赛相关的工具软件、设备手册和竞赛报告放置在每台主机的 D 盘 soft 文件夹中。

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 OSPF 和 BGP 路由协议进行互联互通。

2020 年突如其来的新冠肺炎疫情，给公司上半年业务发展带来巨大影响。在党及集团高层坚强领导下，下半年公司规模依然保持快速发展，业务数据量和公司访问量增长巨大。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及业务服务平台，以达到快速、可靠交换数据，以及增强业务部署弹性的目的，为后续向两地三中心整体战略架构逐步演进，更好的服务于公司客户。

集团、分公司及广东办事处的网络结构详见“主要网络环境”拓扑图。

其中一台 S4600 交换机编号为 SW-3，用于实现分公司业务终端高速接入；两台 CS6200 交换机作为集团的核心交换机；两台 DCFW-1800 分别作为集团、广东办事处的防火墙；一台 DCR-2655 路由器编号为 RT-1，作为集团的核心路由器；另一台 DCR-2655 路由器编号为 RT-2，作为分公司的路由器；一台 DCWS-6028 作为分公司的有线无线智能一体化控制器，编号为 DCWS，通过与 WL8200-I2 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 网络系统管理及运维人员，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。

网络搭建及安全部署项目

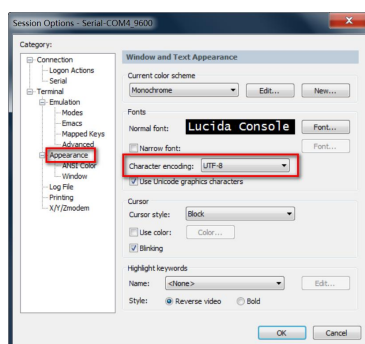
(500 分)

【说明】

1. 请将 PC1 上 D:\soft 文件夹中的《网络搭建及安全部署竞赛报告单》复制到 PC1 桌面上选手自建的“XX_网络比赛报告”(XX 为赛位号)文件夹中,并按照截图注意事项的要求填写完整;裁判以各参赛队提交的“XX_网络比赛报告”文档为主要评分依据。
2. 设备配置完毕后,保存最新的设备配置,按照以下命名规则保存文档,放置在 PC1 桌面的“XX_网络比赛报告”(XX 为赛位号)文件夹中:

设备配置文档命名规则如下:

- 交换机、路由器、AC 要把 show running-config 的配置、防火墙要把 show configuration 的设备配置文档命名规则为:设备名称.txt。例如:RT-1 路由器文件命名为:RT-1.txt;
- 提示:无论通过 SSH、telnet、Console 登录防火墙进行 show configuration 配置收集,需要先调整 CRT 软件字符编号为:UTF-8,否则收集的命令行中文信息会显示乱码。CRT 软件调整字符编号配置如图:



一、网络布线与基础连接 (50 分)

右侧布线面板立面示意图



左侧布线面板立面示意图



【说明】

1. 机柜左侧布线面板编号 101；机柜右侧布线面板编号 102。
2. 面对信息底盒方向左侧为 1 端口、右侧为 2 端口。所有配线架、模块按照 568B 标准端接。
3. 主配线区配线点与工作区配线点连线对应关系如下表所示。

PC1、PC2 配线点连线对应关系表

序号	信息点编号	配线架编号	底盒编号	信息点编号	配线架端口编号
1	W1-02-101-1	W1	101	1	02
2	W1-06-102-1	W1	102	1	06

(一)、铺设线缆并端接

1. 截取 2 根适当长度的双绞线，两端制作标签，穿过 PVC 线槽或线管。双绞线在机柜内部进行合理布线，并且通过扎带合理固定；
2. 将 2 根双绞线的一端，根据“PC1、PC2 配线点连线对应关系表”的要求，端接在配线架的相应端口上；
3. 将 2 根双绞线的另一端，根据“PC1、PC2 配线点连线对应关系表”的要求，端接上 RJ45 模块，并且安装上信息点面板，并标注标签。

(二)、跳线制作与测试

1. 再截取 2 根当长度的双绞线，两端制作标签，根据“PC1、PC2 配线点连线对应关系表”的要求，链接网络信息点和相应计算机，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，截取适当长度和数量的双绞线，端接水晶头，制作网络跳线，根据题目要求，插入相应设备的相关端口上；(包括设备与设备之间、设备与配线架之间)；
3. 实现 PC、信息点面板、配线架、设备之间的连通；(提示：可利用机柜上自带的设备进行通断测试)；
4. PC1 连接 102 底盒 1 端口、PC2 连接 101 底盒 1 端口。

二、交换配置与调试(141 分)

(一)、为了减少广播，需要根据题目要求规划并配置 VLAN。要求配置合理，所有链路上不允许不必要 VLAN 的数据流通过。根据下述信息及表，在交换机上完成 VLAN 配置和端口分配(13 分)。

设备	VLAN 编号	端口	说明
SW-1	VLAN10	E1/0/1-4	营销 1 段
	VLAN20	E1/0/5-7	产品 1 段
	VLAN30	E1/0/8-10	法务 1 段
	VLAN40	E1/0/11-12	财务 1 段
	VLAN50	E1/0/13-14	人力 1 段
SW-2	VLAN10	E1/0/1-4	营销 2 段
	VLAN20	E1/0/5-7	产品 2 段
	VLAN30	E1/0/8-10	法务 2 段
	VLAN40	E1/0/11-12	财务 2 段
	VLAN50	E1/0/13-14	人力 2 段
SW-3	VLAN20	E1/0/1-6	产品 3 段
	VLAN30	E1/0/7-11	法务 3 段
	VLAN50	E1/0/12-15	人力 3 段

(二)、集团核心交换机 SW-1 和 SW-2 开启 telnet 登录功能, 配置使用 telnet 方式登录终端界面前显示如下授权信息: “WARNING!!! Authorised access only, all of your done will be recorded! Disconnected IMMEDIATELY if you are not an authorised user! Otherwise, we retain the right to pursue the legal responsibility” (10 分)。

(三)、集团核心交换机 SW-1 和 SW-2 间租用运营商三条裸光缆通道实现两个 DC 之间互通, 一条裸光缆通道实现三层 IP 业务承载、一条裸光缆通道实现 VPN 业务承载、一条裸光缆通道实现二层业务承载。具体要求如下(32 分):

1. 为了节约集团成本, 设计实现 VPN 业务承载的裸光缆通道带宽只有 10Mbps, 后续再根据业务使用情况考虑是否扩容; 使用相关技术分别实现集团财务 1 段、财务 2 段业务路由表与集团其它业务网段路由表隔离, 财务业务位于 VPN 实例名称 CW 内(18 分);
2. 配置实现三层 IP 业务承载的裸光缆通道最大传输单元为 1600Bytes, 满足后续集团双 DC VXLAN 等新技术应用(6 分);
3. 目前设计实现二层业务承载的只有一条裸光缆通道, 随着集团 1#DC 服务器数量快速扩容, 预计未来 2-3 年集团 DC 间服务器大二层流量会呈现爆发式增长, 配置相关技术, 方便后续链路扩容与冗余备份(8 分)。

(四)、集团核心交换机 SW-1 和 SW-2 配置简单网络管理协议, 计划启用 V3 版本, V3 版本在安全性方面做了极大的扩充。创建认证用户为 DCN2020, 采用 3des 算法进行加密, 密钥为: Dcn20202020, 哈希算法为 MD5, 密钥为: DCn20202020; 加入组 DCN, 采用最高安全级别; 配置组的读、写视图分别为: Dcn2020_R、DCn2020_W; 当设备有异常时, 需要发送 Trap 消息至集团网管服务器 10.40.50.120、2001:10:40:50::121, 采用最高安全级别 (20 分)。

(五)、配置集团核心交换机 SW-1 和 SW-2 法务业务内部启用环路检测,存在环路与不存在环路时检测时间间隔都为 30s,发现环路以后物理关闭此接口(36 分)。

(六)、SW-1 既作为集团核心交换机,同时又使用相关技术将 SW-1 模拟为 Internet 交换机,实现与集团其它业务网段路由表隔离,Internet 路由表位于 VPN 实例名称 Internet 内(12 分)。

(七)、配置相关功能,使集团核心交换机 SW-1 和 SW-2 设备能够在网络中相互发现并交互各自的系统及配置信息,以供管理员查询两端接口对应关系及判断链路的通信状况;配置所有使能此功能的端口发送更新报文所携带的老化时间为五分钟 (18 分)。

三、路由配置与调试(160 分)

(一)、规划集团内、集团与广东办事处使用 OSPF 协议,集团内使用进程号为 1,集团与广东办事处间使用进程号为 2,具体要求如下(45 分):

1. 集团路由器与集团核心交换机之间、集团路由器与集团防火墙之间、集团核心交换机与集团核心交换机之间、集团核心交换机与集团防火墙之间均属于骨干区域,集团路由器与广东办事处防火墙之间属于普通区域,区域号为 20 (15 分);
2. 集团路由器、集团核心交换机、集团防火墙分别发布自己的环回地址路由;集团核心交换机只允许发布营销网段业务路由(10 分);
3. 集团防火墙和集团核心交换机 OSPF 进程 1 的路由表中只允许学习到分公司无线业务网段路由、集团路由器与广东办事处防火墙互联地址、广东办事处防火墙环回地址、与营销业务网段路由;由于广东办事处防火墙路由条目支持数量有限,禁止学习到集团、分公司的所有互联地址与业务路由(20 分)。

(二)、规划集团核心交换机与集团核心交换机之间使用 OSPFv3 协议,通过两端三层 IP 业务承载的裸光缆通道进行互联互通,要求只能发布两端相应环回地址(14 分)。

(三)、为了方便业务灵活调度,同时还规划集团与分公司使用 BGP 协议,集团使用的 AS 号为 62020、分公司使用的 AS 号为 62021,具体要求如下(86 分):

1. 集团路由器与集团核心交换机之间通过环回地址建立 IBGP 邻居、集团路由器与分公司路由器之间通过互联地址建立 EBGP 邻居 (20 分);
2. 集团核心交换机 SW-1 和 SW-2 间使用 BGP 协议实现 DC 间 IPV6 业务、DC 间财务业务互联互通,满足集团 DC 间 IPV6 及财务业务发展的需要,其中要求集团核心交换机 SW-1 和 SW-2 间实现 DC 间 IPV6 业务互联互通需使用环回地址建立 IBGP 邻居(30 分);
3. 要求集团核心交换机、分公司路由器禁止发布除产品、法务、财务、人力、无线业务网段外的其它路由;集团核心交换机 BGP 路由表中只允许学习到集团 DC 间产品&法务&人力业务网段、广东办事处产品业务网段路由、分公司产品&法务&人力&无线业务网段路由,利用 BGP 最通用相关功能特性,实现集团与分公司间产品、法务、人力业务互通(30 分);
4. 利用 BGP 相关功能特性,减少网络不稳定带来的过多的路由更新,抑制这些不稳定的路由信息,不允许这类路由参与路由选择(6 分)。

(四)、为了合理分配集团内业务流向,保证来回路径一致,业务选路具体要求如下(15 分):

1. 集团内部实现核心交换机 SW-1 与分公司路由器、广东办事处互访流量优先通过 SW-1_SW-2_RT-1 间链路转发,SW-1_RT-1、SW-1_FW-1_RT-1 间链路作为备用链路;集团内部实现核心交换机 SW-2 与分公司路由器、广东办事处互访流量优先通过 SW-2_RT-1 间链路转发,SW-2_SW-1_RT-1、SW-2_SW-1_FW-1_RT-1 间链路作为备用链路(10 分);
2. 集团内部实现核心交换机 SW-1 与 Internet 互访流量优先通过 SW-1_FW-1 间

链路转发, SW-1_RT-1_FW-1、SW-1_SW-2_RT-1_FW1 间链路作为备用链路; 集团内部实现核心交换机 SW-2 与 Internet 互访流量优先通过 SW-2_SW-1_FW-1 间链路转发, SW-2_FW-1、SW-2_RT-1_FW-1 间链路作为备用链路(5 分)。

四、无线配置(40 分)

(一)、分公司无线控制器 DCWS 与分公司路由器互连, 无线业务网关位于分公司路由器上, 配置 VLAN100 为 AP 管理 VLAN, VLAN101 为业务 VLAN, DCWS 不允许使用 DHCP 进行 AP 地址分配, 使用第一个可用地址作为 AC 管理地址、第二个可用地址作为 AP 管理地址, AP 二层手工注册(21 分)。

(二)、配置一个 SSID DCNXX: DCNXX 中的 XX 为赛位号, 访问 Internet 业务, 采用 WPA-PSK 认证方式, 加密方式为 WPA 个人版, 配置密钥为 Dcn20202020(10 分)。

(三)、配置当 AP 上线, 如果 AC 中储存的 Image 版本和 AP 的 Image 版本号不同时, 会触发 AP 自动升级; 配置 AP 失败状态超时时间及探测到的客户端状态超时时间都为 2 小时(9 分)。

五、安全策略配置(50 分)

(一)、根据题目要求配置集团防火墙、广东办事处防火墙相应的业务安全域、业务接口; 限制集团防火墙只允许集团营销业务、分公司无线业务、广东办事处营销业务访问 Internet 业务; 在广东办事处防火墙上限制广东办事处产品业务网段只可以访问集团产品网段 https、mysql 数据库类型业务 (16 分)。

(二)、集团防火墙与广东办事处防火墙之间使用互联地址建立 IPSEC 隧道, 集团防火墙侧使用 E0/3 侧接口地址, 实现广东办事处营销业务终端 172.40.11.100/32 与托管在运营商机房 172.40.254.254/32 业务通过逻辑隧道进行转发(20 分)。

(三)、在集团防火墙配置网络地址转换, 公网 NAT 地址池为: 202.40.21.0/28; 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, 当有流量匹配本地址转换规则时产生日志信息, 将匹配的日志发送至 10.40.10.120 的 UDP 2000 端口 (14 分)。

六、广域网业务选路 (59 分)

(一)、考虑到从集团到分公司共有三条链路, 且其带宽不一样, 集团法务业务网段与分公司法务业务网段互访优先在集团路由器 S0/1 与分公司路由器 S0/2 专线间转发; 集团人力业务网段与分公司人力业务网段互访优先在集团路由器 S0/2 与分公司路由器 S0/1 专线间转发; 集团产品业务网段与分公司产品业务网段互访、分公司 SSID DCNXX 与 Internet 业务互访只允许在集团路由器与分公司路由器以太网专线间转发, 同时以太网专线链路还作为集团法务业务网段与分公司法务业务网段互访。根据以上需求, 在路由器上进行合理的业务选路配置。具体要求如下(59 分):

1. 使用 IP 前缀列表匹配上述业务数据流;
2. 使用 LP 属性进行业务选路, 只允许使用 route-map 来改变 LP 属性、实现路由控制, LP 属性可配置参数数值为: 200。

服务器配置及应用项目

(480 分)

说明:

1. 云服务实训平台相关说明:

- (1) 云服务实训平台管理 IP 地址默认为 192.168.100.100, 访问地址 <http://192.168.100.100/dashboard>, 考生禁止修改云服务实训平台账号密码及管理 ip 地址, 否则服务器配置及应用项目部分计 0 分;
- (2) 云服务实训平台中提供镜像环境, 镜像的默认用户名密码以及镜像信息, 参考《云服务实训平台用户操作手册(国赛版)》;

名称	用户名	密码	ssh	rdp
WindowsServer2016	administrator	Qwer1234	否	是
Centos7-mini-V2	root	dcncloud	是	否

- (3) 所有 windows 主机实例在创建之后都直接可以通过远程桌面连接操作, linux 可以通过 CRT 软件连接进行操作, 所有 linux 主机都默认开启了 ssh 功能, Linux 系统软件镜像位于 “/opt” 目录下;
- (4) 要求在云服务实训平台中保留竞赛生成的所有虚拟主机。
2. 虚拟主机管理员密码以及题目中所有未指明的密码均为 Password-1234, 若未按照要求设置, 涉及到该操作的所有分值记为 0 分;
3. 虚拟主机的 IP 地址、主机名称请按照《主要网络环境》的要求设定, 若未按照要求设置, 涉及到该操作的所有分值记为 0 分;
4. 赛题所需的软件均存放在每台主机的 D:\soft 文件夹中;

5. 请将PC2的D:\soft文件夹中《服务器配置及应用报告单》复制到PC2桌面上的“XX_系统报告”(XX为赛位号)文件夹,并按照截图注意事项的要求填写完整;
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,否则会扣除该服务功能一定分数;如报告单存放位置错误,涉及到的所有操作分值记为0分。

一、云实训平台设置（150 分）

- (一) 按照《主要网络环境》要求新建网络。
- (二) 按照《主要网络环境》要求新建云主机类型。
- (三) 按照《主要网络环境》要求新建虚拟主机；

所有虚拟主机 IP 地址与《主要网络环境》中的一致，且手动设置为该虚拟机自动获取的 IP 地址。

- (四) 按照下述题目相关要求新建硬盘，并连接到虚拟主机。

二、Windows 服务配置（165 分）

(一) 域服务配置（43 分）

【任务描述】

为实现高效管理，请采用域控制器，提升企业网络安全程度，整合局域网内基于网络的资源。

1. 配置 Windows-1 为域控制器，域名为 skills.com；安装 DNS 服务，为所有的 Windows 服务器和 Linux 服务器提供正反向解析。
2. 配置 Windows-1 为证书服务器，设置为企业根，CA 证书有效期 20 年，CA 颁发证书有效期 10 年；证书的通用名称均用主机的完全合格域名，证书的其他信息：
 - (1) 国家=“CN”。
 - (2) 省=“Beijing”。
 - (3) 市/县=“Beijing”。
 - (4) 组织=“skills”。

(5) 组织单位= “system”。

3. 把所有的 Windows 主机加入到域。
4. 新建名称为 hr、fin、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：人力部(hr101~hr120)、营销部(sale101~sale120)、财务部 (fin101~fin120)，所有用户不能修改其口令，密码永不过期，并且只能每天 8:00~18:00 可以登录。
5. 新建 C:\share 共享文件夹，共享名称为 ShareDoc；在 AD DS 中发布该共享；复制 PC 机的 D:\soft\MicrosoftEdgeEnterpriseX64.msi 到 C:\share 中，运用适当的方法，进行软件部署。
6. 所有用户到任何一台域计算机登录，“文档”文件夹重定向到域控制器的 C:\Documents 文件夹。
7. 配置用户 hr120 可远程登录到域控制器。
8. 用户 sale120 使用漫游用户配置文件，配置文件存储在 Windows-1 的 C:\Profiles 文件夹。

(二) 辅助域服务配置 (15 分)

【任务描述】

为提供域服务和 DNS 服务的冗余性，在网络中提供第二台域控制器和 DNS 服务器。

1. 配置 Windows-2 为额外域控制器；
2. 配置 Windows-2 为第二台 DNS 服务器；
3. 配置 Windows-2 为从属 CA 服务器。

(三) NLB 服务配置 (24 分)

【任务描述】

为提升网络并发数据处理能力、优化网络性能，请采用 NLB，以保证网络服务的灵活性和可用性。

1. 配置 Windows-3 和 Windows-4 为 NLB 服务器，10.10.70.0 网络为负载均衡网络，10.10.80.0 网络为心跳网络。
2. 群集 IPv4 地址为 10.10.70.60/24，Windows-3 群集优先级为 1，Windows-4 群集优先级为 2，群集名称为 www.skills.com，采用多播方式。
3. 配置 Windows-3 为 web 服务器，站点名称为 www.skills.com，网站的最大连接数为 1000，网站连接超时为 60s，网站的带宽为 2Mbps。
4. 共享网页文件、共享网站配置文件和网站日志文件分别存储到 Windows-1 的 D:\FilesWeb\Contents、D:\FilesWeb\Configs 和 D:\FilesWeb\Logs。
5. 使用 W3C 记录日志，每天创建一个新的日志文件，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。
6. 网站只允许使用域名 SSL 加密访问，证书由 Windows-1 颁发，证书通用名称为 www.skills.com，证书路径为 Windows-1 的 D:\FilesWeb\Configs\www.cer。
7. 配置 Windows-4 为 web 服务器，要求采用共享 windows-3 配置的方式；导入 Windows-3 证书，证书路径为 Windows-1 的 D:\FilesWeb\Configs\www.pfx。

(四) DFS 服务配置 (17 分)

【任务描述】

为建立一个高效率的存储架构，请采用 DFS，实现集中管理共享文件。

1. 在 Windows-2 的 C 分区划分 2GB 的空间，创建 NTFS 分区，驱动器号为 D。
2. 配置 Windows-2 为 DFS 服务器，命名空间为 DFSROOT，文件夹为 Pictures；实现 Windows-3 的 D:\Pics 和 Windows-4 的 D:\Images 同步。
3. 配置 Windows-3 和 Windows-4 之间的“连接安全规则”，要求入站和出站都要求使用“CA 计算机证书”身份验证，完整性算法采用 SHA-256，加密算法采用 AES-CBC192。
4. 配置 Windows-3 的 DFS IPv4 使用 34567 端口；限制所有服务的 IPv4 动态 RPC 端口从 8000 开始，共 1000 个端口号。

(五) Web 服务配置 (30 分)

【任务描述】

为客户获取公司产品信息和企业宣传的需要，创建安全动态网站，采用 IIS 搭建 Web 服务。

1. 把 Windows-5 配置为 web 站点，仅允许使用域名访问，http 访问自动跳转到 https，证书由 Linux-1 颁发，证书路径为 C:\IIS\Configs\iis.crt。
2. web 站点同时支持 dotnet CLR v2.0 和 dotnet CLR v4.0。
3. web 站点目录为 C:\IIS\Contents，主页文档 index.aspx 的内容为<%=now()%>.

(六) 故障转移群集配置 (36 分)

【任务描述】

为提供一个高可用性应用程序或服务的网络环境，请采用 iSCSI SAN 文件服务器故障转

移群集。

1. 在 Windows-5 上添加 4 块硬盘，每块硬盘大小为 5G，配置为 Raid10，驱动器号为 D 盘。
2. 在 Windows-5 上安装 iSCSI 目标服务器和存储多路径，并新建 iSCSI 虚拟磁盘，存储位置为 D:\；虚拟磁盘名称分别为 Quorum 和 Files，大小分别为 512MB 和 5GB，访问服务器为 Windows-6 和 Windows-7，实行 CHAP 双向认证，Target 认证用户名和密码分别为 IncomingUser 和 IncomingPass，Initiator 认证用户名和密码分别为 OutgoingUser 和 OutgoingPass。
3. 在 Windows-6 和 Windows-7 上连接 Windows-5 的虚拟磁盘 Quorum 和 Files，创建卷，驱动器号分别为 M 和 N。
4. 配置 Windows-6 和 Windows-7 为故障转移群集；10.10.70.0 和 10.10.80.0 网络为 MPIO 网络，10.10.90.0 网络为心跳网络。
5. 在 Windows-6 上创建名称为 WinCluster 的群集，其 IP 地址为 10.10.70.70。
6. 在 Windows-7 上配置文件服务器角色，名称为 WinClusterFiles，其 IP 地址为 10.10.70.80；为 WinClusterFiles 添加共享文件夹，共享协议采用“SMB”，共享名称为 WinClusterShare，存储位置为 N:\，NTFS 权限采用域管理员具有完全控制权限，域其他用户具有修改权限；共享权限采用管理员具有完全控制权限，域其他用户具有更改权限。

三、Linux 服务配置（165 分）

(一) Linux CA 服务配置（12 分）

【任务描述】

为保障企业提供的网络服务具有加密功能，提供证书服务，配置 CA 服务器。

1. 启用所有 Linux 服务器的防火墙。
2. 配置服务后，该服务开机自启动。
3. 所有 Linux 服务器的时区设为“上海”。
4. Linux-1 安装 chrony，为所有 Linux 服务器提供时间同步。
5. 把 Linux-1 配置为 CA 服务器，证书通用名称均为主机的完全合格域名，CA 证书有效期 20 年，CA 颁发证书有效期 10 年，证书其他信息：
 - (1) 国家=“CN”。
 - (2) 省=“Beijing”。
 - (3) 市/县=“Beijing”。
 - (4) 组织=“skills”。
 - (5) 组织单位=“system”。

(二) Web 服务配置 (29 分)

【任务描述】

为了搭建快速、可靠的网页服务，请采用 Apache 配置 Web 服务，实现对企业网站的安全有效访问。

1. 从光盘复制安装 apache 需要的软件包到 Linux-2 的 /ApachePackages 目录，创建名称为 apache.repo 的软件仓库，该仓库的 id 为 www，并通过该软件仓库安装 apache。
2. 配置 Linux-2 为 web 服务器，网站根目录为 /https，默认文档 index.html 的内容为“Apache 加密访问!”；仅允许使用域名访问，http 访问自动跳转到 https，证书由

Windows-1 颁发,证书路径为/etc/pki/www.crt, 私钥路径为/etc/pki/www.key, 网站虚拟主机配置文件路径为/etc/httpd/conf.d/vhost.conf。

(三) samba 服务配置 (8 分)

【任务描述】

为在 Linux 和 Windows 之间实现共享文件和打印机的安全访问, 请采用 samba, 实现 Windows 操作系统和 Linux 操作系统的资源共享。

1. 在 Linux-2 上创建 user101~user120 等 20 个用户; user101 和 user102 属于 hr 组, user103 属于 sale 组, user104 属于 fin 组;
2. 配置 Linux-2 为 Samba 服务器, 建立共享目录 /share/hr_share, /share/sale_share, /share/public_share, 共享名与目录名相同;
3. hr 组用户对 hr_share 和 public_share 有共享读写权限, sale 组用户对 sale_share 和 public_share 有共享读写权限, fin 组对所有共享均有读写权限; 用户对自己新建的文件有完全权限, 对其他用户的文件只有读权限, 且不能删除别人的文件。

(四) Linux 链路聚合 (6 分)

【任务描述】

采用链路聚合, 提供链路的冗余性。

1. 利用 Linux-3 和 Linux-4 的 10.10.80.0/24 的两个网络创建聚合端口组, 组名为 team1, 聚合模式为 activebackup, 聚合接口 IP 地址为 10.10.80.0 网络的第一张网卡获取的 IP 地址。

(五) NIS 服务配置 (15 分)

【任务描述】

为实现 Linux 主机之间资源共享, 加强企业 Linux 账户的集中管理, 请采用 NIS 实现该需求。

1. 配置 Linux-1 为 KDC 服务器, 负责 Linux-3 和 Linux-4 的验证。
2. 在 Linux-3 上, 创建用户, 用户名为 tom, uid=222, gid=222, 家目录为/home/tomdir。
3. 配置 Linux-3 为 nfs 服务器, 按下面要求新建共享:

共享目录	共享要求
/srv/share	10.10.70.0/24 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;
/srv/tmp	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 Linux-4 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 Linux-4 为 nfs 客户端，新建 /mnt/share 和 /mnt/tmp 目录，分别挂载 Linux-3 上的 /srv/share 和 /srv/tmp。
6. 配置 Linux-3 为 NIS 服务器，ypserv 服务监听端口为 1020；新建 user1 和 user2 用户，用户目录分别为 /home/user1 和 /home/user2。
7. 配置 Linux-4 为 NIS 客户端，按需自动挂载 Linux-3 上的 user1 和 user2 用户目录到 /home。

(六) Mariadb 服务配置 (17 分)

【任务描述】

为按数据结构来存储和管理数据，请采用 Mariadb，实现方便、严密、有效的数据组织、数据维护、数据控制和数据运用。

1. 配置 Linux-3 为 Mariadb 服务器，创建数据库用户 jack，在任意机器上对所有数据库有完全权限。

2. 配置 Linux-4 为 Mariadb 客户端, 创建数据库 userdb; 在库中创建表 userinfo, 在表中插入 2 条记录, 分别为(1,user1, 1995-7-1, 男), (2,user2, 1995-9-1, 女), 口令与用户名相同, password 字段用 password 函数加密, 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	char(5)	否	否
password	char(200)	否	否

3. 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。
4. 把物理机 d:\soft\mysql.txt 中的内容导入到 userinfo 表中, password 字段用 password 函数加密。
5. 将表 userinfo 中的记录导出, 并存放到/var/databak/mysql.sql 文件中。
6. 每周五凌晨 1:00 备份数据库 userdb 到/var/databak/userdb.sql。

(七) Tomcat 服务配置 (28 分)

【任务描述】

为了 JSP 程序的开发和调试, 请采用 Tomcat, 实现基于 Java 平台 web 应用服务。

1. 配置 Linux-3 为 Tomcat 服务器, tomcat 安装目录为 /usr/local/tomcat。将 D:\soft\jndsjjs 中全部微网站应用程序, 复制到 tomcat 的相关目录, 仅允许使用域名正常访问且页面信息正确无误, http 访问自动跳转到 https, 通过修改配置文件的方法, 使用 443 端口; 证书由 Linux-1 颁发, 证书路径为 <安装目录>/conf/tomcat.pfx, 证书格式为 pfx。

2. 利用 systemd 实现 tomcat 开机自启动，服务名称为 tomcat.service。

(八) 高可靠性配置 (50 分)

【任务描述】

为准确地表达的集群资源之间的关系，请采用 packmarker，实现 web 服务的高可用。

1. 为 Linux-5 添加 4 块硬盘，每块硬盘大小为 5G，组成 Raid10，设备名称为/dev/md10，保证服务器开机,Raid 能正常工作。使用/dev/md10 配置为 iSCSI 目标服务器,为 Linux-6 和 Linux-7 提供 iSCSI 服务。iSCSI 目标端的 wwn 为 iqn.2020-11.com.skills:server, iSCSI 发起端的 wwn 为 iqn.2020-11.com.skills:client.
2. 配置 Linux-6 和 Linux7 为 iSCSI 客户端，实现 discovery chap 和 session chap 双向认证，Target 认证用户名为 IncomingUser，密码为 IncomingPass；Initiator 认证用户名为 OutgoingUser，密码为 OutgoingPass。实现多路径访问，路径别名为 mp，选择方式为轮询。
3. 在 Linux-6 中使用 iscsi 全部空间创建 lvm 卷，卷组名称为 vg1，逻辑卷名称为 lv1，格式化为 ext4 格式。
4. 配置 Linux-6 和 Linux-7 的 root 用户用域名免密码 ssh 登录。
5. 配置 Linux-6 和 Linux-7 为 packmarker 集群，集群名称为 lincluster，Linux-6 为主服务器，Linux-7 为备份服务器。提供 http 服务，域名为 www3.skills.com，网站目录 /var/www/html，网站主页 index.html 的内容为“Linux 集群网站”。IP 资源名称为 vip，虚拟 IP 为 10.10.70.90；站点文件系统资源名称为 site，物理目录为 lv1；监视资源名称为 webstatus，配置文件为/etc/httpd/conf/httpd.conf。

职业规范与素养

(20 分)

- 一、 整理赛位，工具、设备归位，保持赛后整洁有序；
- 二、 无因选手原因导致设备损坏；
- 三、 恢复调试现场，保证网络和系统安全运行。