2021年全国职业院校技能大赛

网络搭建与应用赛项

正式赛卷

技能要求

（总分1000分）

ZZ-2021030 网络搭建与应用赛项执委会及专家组

2021年05月20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需要完成的报告单在物理机的D:\soft文件夹中。

9.请在物理机PC1桌面上新建“XX”（XX为赛位号）文件夹，作为选手提交竞赛结果的目录，保存选手生成的所有文档。**全部自动生成的结果性文件和项目实施总结报告的保存位置必须正确，否则涉及到的所有操作分值记为0分。**

项目简介：

某集团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。

春回大地，万象更新，站在“两个一百年”历史的交汇点，上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，努力开创新局面，以高质量业绩向党献礼。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、在贵州建立异地灾备数据中心，以达到快速、可靠交换数据，以及增强业务部署弹性的目的，初步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、分公司及广东办事处的网络结构详见“网络环境”拓扑图。

两台交换机分别作为集团北京两个 DC 的核心交换机编号分别为 SW-1 和 SW-2；又新采购一台交换机编号为 SW-3，作为集团灾备 DC 的核心交换机；两台防火墙 FW-1 和 FW-2 分别作为集团、广东办事处的防火墙；一台路由器编号为 RT-1，作为集团的核心路由器；另一台路由器编号为 RT-2，作为分公司的路由器；一台有线无线智能一体化控制器作为分公司的 AC，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.请根据物理机“D:\soft\网络搭建及安全部署竞赛报告单.docx”的要求生成文档，将生成的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，否则收集的命令行中文信息会显示乱码。

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	2	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.按照“PC1、PC2 配线点连线对应关系表”连接机柜两侧底盒端口。

二、交换配置与调试(100 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。核心交换机 SW-1 和核心交换机 SW-2 之间实现二层业务承载的裸光缆通道目前暂时只允许 VLAN10、VLAN20、VLAN30、VLAN40、VLAN50 通过，禁止配置 VLAN 及接口的描述信息。根据下述信息及表，在交换机上完成 VLAN 配置和端口分配。

设备	VLAN 编号	端口	说明（非 VLAN 描述信息）
SW-1	VLAN10	E1/0/1-2	营销 1 段
	VLAN20	E1/0/3-4	产品 1 段
	VLAN30	E1/0/5-6	法务 1 段
	VLAN40	E1/0/7-8	财务 1 段
	VLAN50	E1/0/9-10	人力 1 段

设备	VLAN 编号	端口	说明（非 VLAN 描述信息）
SW-2	VLAN10	E1/0/1-2	营销 2 段
	VLAN20	E1/0/3-4	产品 2 段
	VLAN30	E1/0/5-6	法务 2 段
	VLAN40	E1/0/7-8	财务 2 段
	VLAN50	E1/0/9-10	人力 2 段
SW-3	VLAN10	E1/0/1-2	营销 3 段
	VLAN20	E1/0/3-4	产品 3 段
	VLAN30	E1/0/5-6	法务 3 段
	VLAN50	E1/0/9-10	人力 3 段

(二)核心交换机 SW-1 和核心交换机 SW-2 之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。核心交换机 SW-1 与核心交换机 SW-3 之间、核心交换机 SW-2 与核心交换机 SW-3 之间租用运营商 OTN 波分链路实现互通。具体要求如下：

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。

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 1700Bytes，满足后续集团双 DC VXLAN、EVPN 等新技术应用。

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 1#DC 与 2#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，编号为 1。

4.配置核心交换机 SW-1、SW-2、SW-3 采用源、目的 IP 进行实现流量负载分担。

5.核心交换机 SW-3 针对每个业务 VLAN 的第一个接口配置 Loopback 命令，模拟接口 UP，方便后续业务验证与测试。

(三)核心交换机 SW-1 和核心交换机 SW-2 针对营销业务网段的每个物理接

口限制收、发数据占用的带宽分别为 100Mbps、90Mbps；针对产品业务网段的每个物理接口限制所有报文最大收包速率为 100packets/s，如果超过了设置交换机端口的报文最大收包速率则关闭此端口，10 分钟后再恢复此端口，来保证交换机对其他业务的正常处理。

(四)要求禁止配置访问控制列表，实现核心交换机 SW-3 法务业务对应的物理端口间二层流量无法互通；针对 SW-3 人力业务配置相关特性，每个端口只允许的最大安全 MAC 地址数为 1，当超过设定 MAC 地址数量的最大值，不学习新的 MAC、丢弃数据包、发 snmp trap、同时在 syslog 日志中记录，端口的老化定时器到期后，在老化周期中没有流量的部分表项老化，有流量的部分依旧保留；配置相关特性实现报文上送设备 CPU 的前端整体上对攻击报文进行拦截，开启日志记录功能，采样周期 10s 一次，恢复周期为 2 分钟，从而保障 CPU 稳定运行。

(五)核心交换机 SW-1、SW-2、SW-3 分别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。配置引擎号分别为 62001、62002、62003;创建认证用户为 DCN2021,采用 3des 算法进行加密,密钥为:Dcn20212021，哈希算法为 SHA，密钥为：Dcn20212021；加入组 DCN，采用最高安全级别；配置组的读、写视图分别为：Dcn2021_R、Dcn2021_W；当设备有异常时，需要使用本地的环回地址 Loopback2 发送 Trap 消息至集团网管服务器 10.50.15.120、2001:10:50:15::120，采用最高安全级别；当人力部门对应的用户接口发生 UP/DOWN 事件时禁止发送 trap 消息至上述集团网管服务器。

(六)使用相关技术将核心交换机 SW-1、核心交换机 SW-3 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。

(七)配置相关功能，使核心交换机 SW-1、核心交换机 SW-2、核心交换机 SW-3 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的时间间隔为 1 分钟、更新报文所携带的老化时间为 5 分钟，配置租用运

营商三条裸光缆通道相关端口使能 Trap 功能，Trap 报文发送间隔为 1 分钟。

三、路由配置与调试(160 分)

(一)规划集团内部、集团与广东办事处之间使用 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：

1.核心交换机 SW-1 与 FW-1 之间、核心路由器 RT-1 与 FW-1 之间、核心路由器 RT-1 与 SW-2 之间、SW-1 与 SW-2 之间、SW-1 与 SW-3、SW-2 与 SW-3 均属于骨干区域；RT-1 与 FW-2 之间属于普通区域，区域号为 20。

2.调整 OSPF 进程号 1 所有接口发送 Hello 包的时间间隔为 5 秒，如果接口在 3 倍时间内都没有收到对方的 Hello 报文，则认为对端邻居失效。

3.RT-1、SW-1、SW-2、SW-3、FW-1、FW-2 分别发布自己的环回地址路由；SW-1、SW-2、SW-3 只允许发布营销网段业务路由；FW-2 分别发布自身营销、产品网段业务路由。

4.核心交换机 SW-1、SW-2、SW-3 OSPF 进程 1 的路由表中业务网段路由只允许学习到 FW-1 通告的 TYPE1 类型的缺省路由、集团营销业务网段路由、FW-2 环回地址与营销业务网段路由；由于 FW-2 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。

(二)规划核心交换机 SW-1 与 SW-2 之间、SW-1 与 SW-3 之间、SW-2 与 SW-3、SW-2 与 RT-1 之间使用 OSPFv3 协议，均属于骨干区域，发布相应环回地址，禁止发布业务路由；SW-1 与 SW-2 之间通过两端三层 IP 业务承载的裸光缆通道进行互联互通。

(三)为了方便业务灵活调度,同时还规划集团北京两个 DC 与集团灾备 DC 之间、集团与分公司之间使用 BGP 协议，集团北京两个 DC 使用的 AS 号为 62021、集团灾备 DC 使用的 AS 号为 62022、分公司使用的 AS 号为 62023，具体要求如下：

1.核心交换机 SW-1 与 SW-2 之间、SW-1 与 RT-1 之间、SW-2 与 RT-1 之间通

过OSPFv2环回地址建立IBGP邻居，SW-1与SW-3之间、SW-2与SW-3之间、核心路由器RT-1与分公司路由器RT-2之间通过互联地址建立EBGP邻居。

2.使用BGP协议实现集团DC之间IPV6业务、集团与分公司之间IPV6业务、北京DC之间财务业务互联互通，满足集团DC之间、集团与分公司之间IPV6及北京DC之间财务业务发展的需要；其中要求SW-1、SW-2、SW-3之间实现DC间IPV6业务互联互通需使用环回地址建立BGP邻居；集团与分公司之间IPV6业务互联互通要求SW-1、SW-2与RT-1使用环回地址建立BGP邻居、核心路由器RT-1与分公司路由器RT-2采用互联地址建立BGP邻居。

3.要求集团北京两个DC与集团灾备DC、分公司路由器RT-2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；SW-1、SW-2、SW-3 BGP公网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、分公司无线业务业务网段路由。

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。

(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：

1.实现核心交换机SW-1与分公司路由器RT-2、广东办事处IPV4互访流量优先通过SW-1_SW-2_RT-1之间链路转发，SW-1_FW-1_RT-1之间链路作为备用链路；实现核心交换机SW-2与分公司路由器RT-2、广东办事处IPV4互访流量优先通过SW-2_RT-1之间链路转发，SW-2_SW-1_FW-1_RT-1之间链路作为备用链路。

2.实现核心交换机SW-1与Internet互访流量优先通过SW-1_FW-1之间链路转发，SW-1_SW-2_RT-1_FW-1之间链路作为备用链路；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之间链路转发，SW-2_RT-1_FW-1之间链路作为备用链路。

3.核心交换机SW-3与SW-1、SW-2 IPv4营销业务互访流量优先通过SW-

3_SW-2 之间链路转发，SW-3_SW-1 之间链路作为备用链路；实现 SW-3 与 SW-1、SW-2 DC 间 IPV6 业务互访流量优先通过 SW-3_SW-1 之间链路转发，SW-3_SW-2 之间链路作为备用链路。

四、无线配置(40 分)

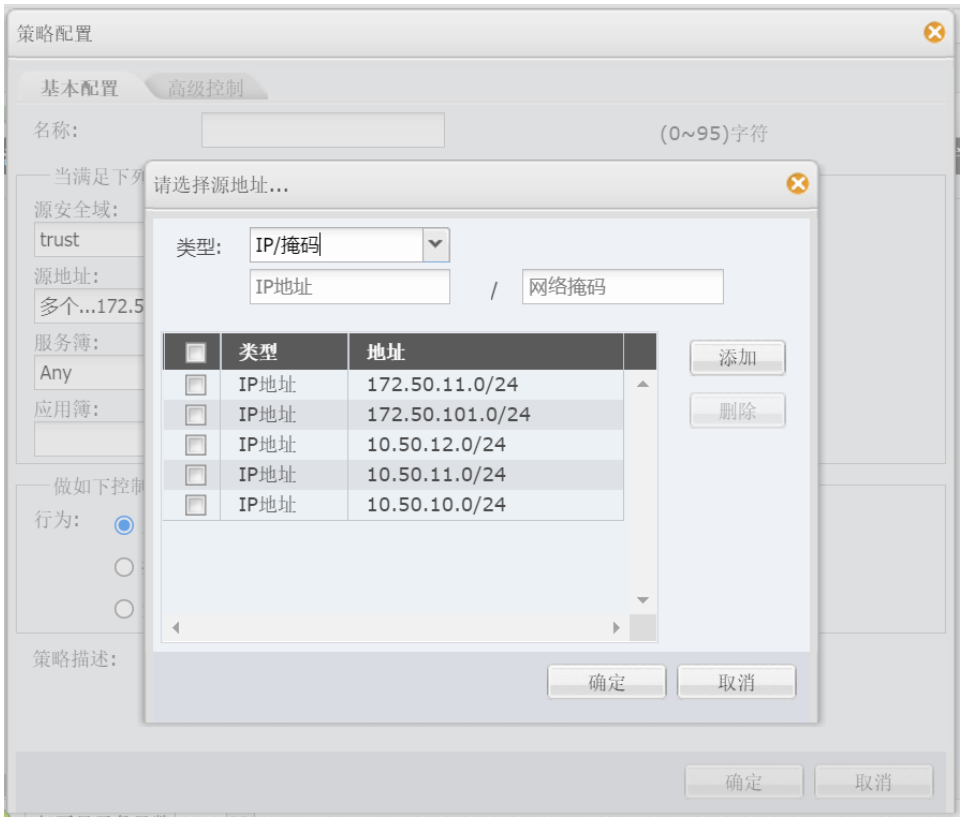
(一)分公司无线控制器 AC 与 RT-2 互连，无线业务网关位于 RT-2 上，配置 VLAN100 为 AP 管理 VLAN，VLAN200 为业务 VLAN；AC 提供无线管理与业务的 DHCP 服务，动态分配 IP 地址和网关；分别使用第一个可用地址作为 AC 管理地址和无线业务管理地址；AP 二层自动注册，AP 采用 MAC 地址认证。

(二)配置一个 SSID DCN2021，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 Dcn20212021。

(三)配置所有无线接入用户相互隔离，Network 模式下限制 SSID DCN2021 每天早上 0 点到 4 点禁止终端接入，开启 SSID DCN2021 ARP 抑制功能；配置当无线终端支持 5GHz 网络时，优先引导接入 5GHz 网络，从而获得更大的吞吐量，提高无线体验。

五、安全策略配置(50 分)

说明：为了统一结果，要求源地址和目的地址均使用“IP/掩码”表示，禁止使用地址薄或地址条目表示，否则按零分处理。举例截图如下：



(一)根据题目要求配置 FW-1、FW-2 相应的业务安全域、业务接口；2021 年护网行动开展在即，调整全网防火墙安全策略缺省规则为拒绝；限制 FW-1 只允许集团营销业务、分公司无线 IPV4 业务、广东办事处营销业务访问 Internet 业务；在 FW-2 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，集团营销网段可以访问广东办事处营销业务网段任何端口。

(二)为了避免集团内部业务直接映射至 Internet 成为攻击“靶心”，不断提升集团网络安全体系建设，在 FW-1 配置 L2TP VPN，满足远程办公用户通过拨号登陆访问集团营销业务，创建隧道接口为 tunnel 1、并加入 trust 安全域，地址池名称为 AddressPool，LNS 地址池为 10.50.253.1/24-10.50.253.100/24，网关为最大可用地址，认证账号 dcn2021001,密码 dcn2021。

(三)在 FW-1 配置网络地址转换,NAT 地址转换条件中源、目的 IP 均为 any，公网 NAT 地址池为：202.50.21.0/28；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 10.50.11.120 的 UDP 514 端口；开启相关特性，实现扩展 NAT 转换后的网络地址端口资源。

(四)在 FW-2 开启安全网关的 TCP SYN 包检查功能，只有检查收到的包为 TCP SYN 包后，才建立连接；配置所有的 TCP 数据包每次能够传输的最大数据分段为 1460、尽力减少网络分片；配置对 TCP 三次握手建立的时间进行检查，如果在 1 分钟内未完成三次握手，则断掉该连接。

六、业务选路与组播配置（50 分）

(一)考虑到从集团北京两个 DC 与集团灾备 DC 之间共有两条链路，集团灾备 DC 产品业务网段与集团北京两个 DC 产品业务网段 IPV4 协议栈互访优先在 SW-3 与 SW-1 之间链路转发；集团灾备 DC 法务&人力网段与集团北京两个 DC 法务&人力网段 IPV4 协议栈互访优先在 SW-3 与 SW-2 之间链路转发，主备链路相互备份。根据以上需求，在交换机上进行合理的业务选路配置。具体要求如下：

1.使用 IP 前缀列表匹配上述业务数据流。

2.使用 BGP 自治系统路径属性进行业务选路，允许新增的变量为 AS 62000，只允许使用 route-map 来改变路径属性、路由控制。

(二)前年集团内部完成视频会议系统组播功能的测试与上线，获得了良好演示效果与集团高层领导高度认可。为了更加方便集团与分公司多业务部门横向沟通、交流，提升工作效率，计划在集团营销与分公司无线业务部门间启用组播协议进行测试，具体要求如下：

1.在 SW-1 与 SW-2 之间、核心路由器 RT-1 与 SW-2 之间、核心路由器 RT-1 与 RT-2 之间运行协议独立组播—密集模式协议、因特网组管理协议第二版本。

2.SW-1 营销业务部门内部终端启用组播，此终端 IP 地址为：10.50.11.234/24，使用 VLC 工具串流播放视频文件“大赛宣传片.mp4”，模拟组播源，设置此视频循环播放，组地址 228.50.50.50，端口：2021，实现分公司无线业务部门内部终端可以通过组播查看视频播放。

七、IP 地址规划(50 分)

为了不断壮大集团业务经营范围，集团计划在上海成立办事处。通过调研，计划在上海办事处设立与 Internet 连接的 4 个业务部门，每个业务部门的最大所需主机数如下表所示,要求从 172.16.32.0/19 网络第一个网段开始进行 IP 地址规划，IP 地址按照下表依次往后顺延规划，网关地址取每个网段最后一个可用地址，请完成下表 IP 地址规划。

部门名称	最大所需主机数	网络地址 （表示形式 X.X.X.X/N）	网关地址 （表示形式 X.X.X.X）
营销	110		
产品	600		
法务	126		
财务	14		

服务器配置及应用项目（480 分）

【说明】

1.请根据物理机“D:\soft\服务器配置及应用竞赛报告单.docx”的要求生成文档，将生成的文档复制到选手目录。**注意：如果在生成报告后，又在虚拟机上修改了配置，则必须重新执行报告单中该虚拟机的 powershell 脚本，并重新复制生成的文件到选手目录。**

2.虚拟主机的 IP 地址、主机名称必须与《网络环境》的要求一致，且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，**为了输出结果文档时测试的需要，一定要关闭端口安全**，然后创建实例时，不指定网络，而指定端口）。

3.云平台访问网址 http://192.168.100.100/dcncloud，登录管理员用户名为 admin，密码为 dcncloud。

4.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。

5.镜像 win2019-gui 中用户 Administrator 的密码默认为 Qwer1234，镜像 centos8-cli 中用户 root 的密码为 dcncloud。

6.修改 Windows 虚拟机管理员 Administrator 的密码为 Admin-12345，Windows 题目中所有未指明的密码均为管理员 Administrator 的密码。不能修改 Linux 虚拟机管理员 root 的密码，Linux 题目中所有未指明的密码均为管理员 root 的密码。

7.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。

8.openstack 实例仅供导出云平台配置使用，不需要配置服务。

一、云平台配置（150分）

1.按照《网络环境》要求新建网络。

2.按照《网络环境》要求新建实例类型（删除云平台中已有实例类型）。

3.按照《网络环境》要求新建实例，实例IP地址必须与《网络环境》中的一致。

4.按照《网络环境》要求新建卷，并连接到实例。

二、Windows服务配置（165分）

(一)域服务配置

【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skills.com域服务和DNS服务，DNS正反向区域在Active Directory中存储，为skills.com域中主机提供正反向解析。把其他Windows主机加入到skills.com域。

2.配置Windows-1为企业根证书服务器，为所有Windows主机颁发证书。CA证书有效期20年，CA颁发证书有效期均为10年，证书的通用名称均用主机的完全合格域名,证书信息:国家=“CN”,省=“Beijing”,市/县=“Beijing”,组织=“skills”，组织单位=“system”。

3.把skills.com域服务迁移到Windows-2；安装DNS服务，DNS正反向区域在Active Directory中存储;为Windows主机提供冗余的域服务和DNS服务。

4.在Windows-2上新建名称为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），所有用户只能每天8:00-18:00可以登录，不能修改其口令，密码永不过期；为fin

用户组新建名称为 FinPasswordPolicy 的密码策略，优先级为 1，密码必须符合复杂性要求、强制最短密码长度为 8 字符、强制密码历史记录为 12 次，强制最短密码期限为 2 天、强制最长密码期限为 30 天、允许失败登录尝试的次数为 3 次、5 分钟后重置失败登录尝试计数、账户锁定持续时间为 10 分钟。

5.在 Windows-2 上设置组策略，所有域用户到任何一台域计算机登录，“文档”文件夹重定向到 Windows-2 的 C:\Documents 文件夹，在根目录路径下为每一用户创建一个文件夹。

6.在 Windows-2 上设置组策略，所有域用户使用漫游用户配置文件，配置文件存储在 Windows-2 的 C:\Profiles 文件夹，为每个用户提供单独的配置文件文件夹。

7.在 Windows-2 上设置组策略，客户端自动申请计算机证书；让域中主机之间通信采用 IPSec 安全连接，但域控制器和网关除外，采用计算机证书验证。

(二)Web 服务配置

【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-2 配置为 web 网站，站点名称为 ws2.skills.com，网站绑定 IP 地址 10.10.60.102，仅允许使用域名访问，利用物理机提供的"D:\soft\rewrite_amd64_zh-CN.msi"软件，实现 http 访问自动跳转到 https，证书路径为 C:\IIS\Configs\iis.cer。

2.web 网站同时支持 dotnet CLR v2.0 和 dotnet CLR v4.0。

3.ws2.skills.com 网站目录为 C:\IIS\Contents，主页文档 index.aspx 的内容为"HelloAspx"。

4.修改 openstack 主机的 DNS，openstack 信任 Windows-1 的 CA 证书。

(三)DFS 服务配置

【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的DFS IPv4使用34567端口；限制所有服务的IPv4动态RPC端口从10000开始，共20000个端口号。

(四)WDS服务

【任务描述】 由于企业新购一批服务器，需要安装Windows Server 2019操作系统，请采用WDS服务实现需求。

1.配置Windows-3和Windows-4为DHCP服务器，两台DHCP服务器实现故障转移,故障转移关系名称为ws3-ws4,最长客户端提前期为2小时,模式为“负载平衡”，负载平衡比例各为50%，状态切换间隔60分钟，启用消息验证，共享机密为Admin-12345。

2.DHCP IPv4的作用域名称为skills，地址范围为10.10.60.10-10.10.60.19，网关为10.10.60.254，DNS为10.10.60.101和10.10.60.102，DNS域名为skills.com,租约期3小时,DHCP服务只绑定10.10.60.0/24接口。

3.在Windows-3上安装WDS，部署安装Windows Server 2019 Datacenter Core。

(五)NLB服务配置

【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，10.10.60.0网络为负载均衡网络，10.10.80.0网络为心跳网络。

2.Windows-3群集优先级为3，Windows-4群集优先级为5，群集IPv4地址为10.10.60.60/24，群集名称为www1.skills.com，采用多播方式。

3.配置Windows-3为web服务器，站点名称为www1.skills.com，网站的最大连接数为10000，网站连接超时为60s，网站的带宽为100Mbps。

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-2的D:\FilesWeb\Contents、D:\FilesWeb\Configs和D:\FilesWeb\Logs。网站主页index.html内容为"HelloNLB"，index.html文件编码为ANSI。

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.网站仅绑定https，IP地址为群集地址，仅允许使用域名加密访问，证书通用名称为www1.skills.com，证书路径为Windows-2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-2的D:\FilesWeb\Configs\www.pfx。

(六)故障转移群集配置

【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，初始化为GPT磁盘，配置为Raid5，驱动器号为D盘。

2.在Windows-5上安装iSCSI目标服务器，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，目标名称为win，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上安装多路径I/O,10.10.60.0和10.10.80.0网络为MPIO网络，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；10.10.90.0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10.10.60.70.

6.在Windows-7上配置文件服务器角色，名称为WinClusterFiles，其IP地址为10.10.60.80。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权限为仅域管理员和本地管理员组具有完全控制权限,域其他用户具有修改权限;共享权限为仅域管理员具有完全控制权限，域其他用户具有更改权限。

(七)虚拟化

【任务描述】 随着虚拟化技术的发展，企业把测试环境迁移到docker容器中。

1.在windows-2安装docker，导入NanoServer镜像。软件包和镜像存放在物理机D:\soft\DockerWindows。

2.创建名称为web的容器,映射Windows-2的8080端口到容器的80端口，容器启动后运行cmd命令，保持容器处于运行状态。

三、Linux服务配置（165分）

(一)DNS服务和CA服务配置

【任务描述】 创建DNS服务器，实现企业域名访问。

1.设置所有Linux服务器的时区设为“上海”，本地时间调整为实际时间。

2.启动所有Linux服务器的防火墙，并添加相应端口（不允许添加服务）放行相关服务。

3.利用chrony配置Linux-1为其他Linux主机提供时间同步服务。

4.利用bind9软件，配置Linux-1为主DNS服务器，采用rndc技术提供不间断的DNS服务；配置Linux-2为备用DNS服务器。为所有Linux主机提供冗余DNS正反向解析服务。

5.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。

(1)配置Linux-1为CA服务器,为所有Linux主机颁发证书，不允许修改/etc/pki/tls/openssl.conf。CA证书有效期20年，CA颁发证书有效期均为10年，证书的通用名称均用主机的完全合格域名，证书信息：国家=“CN”，省=“Beijing”，市/县=“Beijing”，组织=“skills”，组织单位=“system”。

(二)mail服务配置

【任务描述】为构建一个企业级邮件服务器,请采用postfix和dovecot，实现更快、更容易管理、更安全的邮件服务。

1.配置Linux-2为mail服务器，安装postfix和dovecot。

2.仅支持smtps和pop3s连接，证书路径为/etc/ssl/mail.crt，私钥路径为/etc/ssl/mail.key。

3.创建用户mail1和mail2，向all@skills.com发送的邮件，每个用户都会收到。

4.root用户使用mail工具向all@skills.com发送一封邮件，邮件主题为“Hello”，内容为“Welcome”。

(三)PXE服务配置

【任务描述】由于企业新购一批服务器,需要安装CentOS 8.3 操作系统，

请采用DHCP+TFTP+vsftpd服务实现需求。

1.配置Linux-2为DHCP服务器，为PXE客户端提供IP，地址范围为10.10.70.20-10.10.70.29，网关为10.10.70.254，DNS为10.10.70.101和10.10.70.102，域名为skills.com。

2.配置Linux-2为TFTP服务器，为PXE客户端提供启动服务，TFTP目录为默认值。

3.配置Linux-2为ftp服务器，为PXE客户端提供软件包；复制CentOS8.3光盘内文件到/var/ftp/centos；复制物理机D:\soft\kickstart.cfg到/var/ftp，并对该文件进行必要的修改，实现完全自动化部署。

(四)samba服务和NIS服务配置

【任务描述】 采用samba和NIS实现的安全共享访问。

1.在Linux-2上创建user101-user120等20个用户；user101和user102添加到hr组，user103添加到sale组，user104添加到fin组。

2.配置Linux-2为Samba服务器，建立共享目录/share/ShareHr，/share/ShareSale，/share/SharePublic，共享名与目录名相同。

3.hr组用户对ShareHr和SharePublic有共享读写权限，sale组用户对ShareSale和SharePublic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。

4.把用户user101-user104添加到samba用户。

5.配置Linux-2为KDC服务器，负责Linux-3和Linux-4的验证。

6.在Linux-3上，创建用户，用户名为tom，uid=222，gid=222，家目录为/home/tomdir。

7.配置Linux-3为NFS服务器，目录/srv/share的共享要求为：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。目录/srv/tmp 的共享要求为：所有人都可以读写，都（含 root 用户）不改变身份；kdc 加密方式为 krb5p。

8.配置 Linux-4 为 NFS 客户端，新建/opt/share 和/opt/tmp 目录，分别挂载 Linux-3 上的/srv/share 和/srv/tmp。

9.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。

10.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。

(五)LNMT 服务配置

【任务描述】根据企业需要搭建 Linux 动态网站,采用 LNMT 实现该需求。

2.配置 Linux-3 为 Mariadb 服务器，安装 Mariadb-server，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；允许 root 远程登陆。

3.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

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.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。

6.将表 userinfo 中的记录导出，并存放到/var/databak/mysql.sql 文件中。

7.根据物理机 D:\soft\Tomcat 提供的软件，配置 Linux-3 和 Linux-4 为 Tomcat 服务器，安装目录均为/usr/local/tomcat，网站默认首页内容分别为“TomcatOne”和“TomcatTwo”,使用80端口访问http和443端口访问https;证书路径均为/etc/ssl/tomcat.pfx，证书密码dcncloud，格式为pkcs12。信任Linux CA证书。

8.配置Linux-1为nginx服务器，安装nginx，网站根目录为默认值，默认文档index.html的内容为“HelloNginx”;仅允许使用域名访问，http访问自动跳转到https，证书路径为/etc/ssl/nginx.crt，私钥路径为/etc/ssl/nginx.key。信任Linux CA证书。

9.利用nginx反向代理，客户端通过https://tomcat.skills.com加密访问Tomcat，实现Linux-3和Linux-4的两个Tomcat负载均衡，http访问通过301自动跳转到https。

(六)高可靠性配置

【任务描述】 为准确地表达的集群资源之间的关系，请采用pacemarker+CoroSync，实现web服务的高可用。

10.为Linux-5添加4块硬盘，每块硬盘大小为5G，创建lvm卷，卷组名称为 vg1，逻辑卷名称为 lv1，容量为全部空间，格式化为 ext4 格式。使用/dev/vg1/lv1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.2021-05.com.skills:server, iSCSI发起端的wwn为iqn.2021-05.com.skills:client.

11.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。

12.利用多路径实现负载均衡，多路径别名为 mp。

13.配置 Linux-6 和 Linux-7 为集群服务器，根据物理机 D:\soft\HighAvailability.tar.gz 安装 pcs，集群名称为 LinCluster，Linux-6 为主服务器，Linux-7 为备份服务器。提供 apache 服务，域名为 www2.skills.com，网站目录/var/www/html，网站主页 index.html 内容为“HelloLinuxCluster”。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 website，物理目录为 mp；监视资源名称为 webstatus，配置文件为/etc/httpd/conf/httpd.conf。仅允许使用域名访问，http 访问自动跳转到 https，证书路径为/etc/ssl/www.crt，私钥路径为/etc/ssl/www.key，信任 CA 根证书。

(七)虚拟化

【任务描述】 随着虚拟化技术的发展，企业把测试环境迁移到 docker 容器中。

1.在 Linux-2 上安装 docker-ce，导入 centos 镜像。软件包和镜像存放在物理机 D:\soft\DockerLinux。

2.创建名称为 skills 的容器，映射 Linux-2 的 80 端口到容器的 80 端口，在容器内安装 apache2，默认网页内容为“HelloContainer”。

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。

四、撰写项目实施总结报告。

请参考物理机“D:\soft\项目实施总结报告模板.docx”，撰写完成后将文件存放到PC1桌面的“XX\项目实施总结报告.docx”（XX为赛位号）文件夹中。