**2021年度湖南省职业院校技能竞赛**

**中职组信息技术类网络搭建与应用赛项**

**[时量：180分钟，试卷号：A]**

**竞**

**赛**

**任**

**务**

**书**

**场次号： 机位号（工位号）： 。**

**2020年12月**

竞赛说明

一、竞赛任务概述

本赛项包括网络搭建及安全部署、服务器配置及应用、职业规范与素养三个竞赛任务（部分），各任务（部分）分值分别为50、48、2分，本赛项满分为100分。

二、注意事项

1.竞赛任务书总共19页。

2.职业规范与素养要求：整理赛位，保持整洁有序，无因选手原因导致设备损坏。

3.禁止携带移动存储设备、计算器、通信工具及参考资料。

3.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。

4.请选手仔细阅读比赛试卷，按照试卷要求完成各项操作。

5.操作过程中，需要及时保存设备配置。

6.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。

7.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。

8.禁止在纸质资料、比赛设备、上填写任何与竞赛无关的标记，如违反规定，可视为0分。

9.与比赛相关的工具软件放置在每台主机的D盘soft文件夹中。

10.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；所有需要提交的文档均放置在U盘的“比赛文档\_AM\_X”或者“比赛文档\_PM\_X”（X为赛位号）文件夹中。

项目简介

某重点大学拥有南、北、东三大校区和一个大型产教融合基地。具体网络拓扑如下图所示。

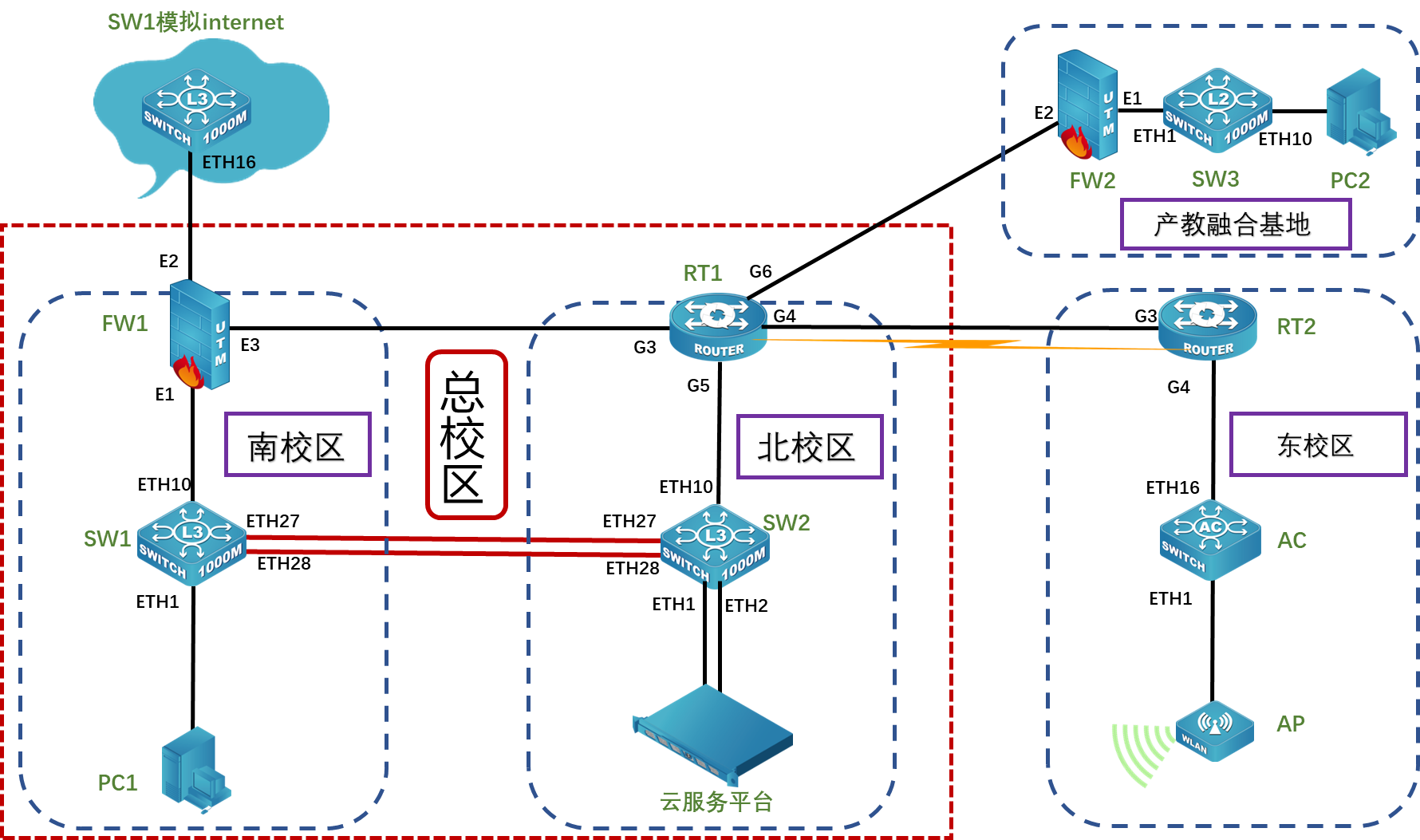


表1.网络设备连接表

**A设备连接至B设备**

|  |  |  |  |
| --- | --- | --- | --- |
| **设备名称** | **接口** | **设备名称** | **接口** |
| FW1 | E0/1 | SW1 | E1/0/10 |
| FW1 | E0/2 | SW1 VRF Internet | E1/0/16 |
| FW1 | E0/3 | RT1 | G0/3 |
| RT1 | G0/4 | RT2 | G0/3 |
| RT1 | G0/5 | SW2 | E1/0/10 |
| RT1 | G0/6 | FW2 | E0/2 |
| RT2 | G0/4 | AC | E1/0/16 |
| AP | - | AC | E1/0/1 |
| FW2 | E0/1 | SW3 | E1/0/1 |
| SW3 | E1/0/10 | PC2 | - |
| SW1 | E1/0/27 | SW2 | E1/0/27  （实现三层IP业务承载） |
| SW1 | E1/0/28 | SW2 | E1/0/28  （实现二层业务承载） |
| SW1 | E1/0/1 | PC1 | - |
| SW2 | E1/0/1 | 云服务平台 | - |
| SW2 | E1/0/2 | 云服务平台 | - |

**表2.网络设备IP地址分配表**

| **设备** | **设备名称** | **设备接口** | **IP地址** |
| --- | --- | --- | --- |
| 路由器 | RT-1 | Loopback1 | 10.16.255.4/32  (北校区内使用) |
| Loopback2 | 10.16.255.5/32  (北校区与基地  互联使用) |
| G0/3 | 10.16.254.17/30 |
| G0/4 | 10.16.254.25/30 |
| G0/5 | 10.16.254.13/30 |
| G0/6 | 10.16.254.9/30 |
| S0/1 | 10.16.254.29/30 |
| S0/2 | 10.16.254.33/30 |
| RT-2 | G0/4.20 | 172.17.20.254/24 |
| G0/4.30 | 172.17.30.254/24 |
| G0/4.50 | 172.17.50.254/24 |
| G0/4.100 | 172.17.100.254/24 |
| G0/4.101 | 172.17.101.254/24 |
| G0/3 | 10.16.254.26/30 |
| S0/2 | 10.16.254.30/30 |
| S0/1 | 10.16.254.34/30 |
| 三层交换机 | SW-1 | Loopback 1  (ospfv2使用) | 10.16.255.1/32 |
| Loopback 2  (ospfv3使用) | 10.16.255.7/32  2001:10:16:255::7/128 |
| VLAN10 SVI | 10.16.10.254/24 |
| VLAN20 SVI | 10.16.20.254/24  2001:10:16:20::254/64 |
| VLAN30 SVI | 10.16.30.254/24  2001:10:16:30::254/64 |
| VLAN40 SVI | 10.16.40.254/24 |
| VLAN50 SVI | 10.16.50.254/24  2001:10:16:50::254/64 |
| VLAN1000 SVI | 10.16.254.2/30 |
| VLAN4094 SVI | 10.16.254.41/30  2001:10:16:254::21/64 |
| SW-1模拟Internet交换机 | VLAN4000 SVI | 113.218.100.2/30 |
| Loopback100 | 113.218.20.20/32  172.17.254.254/32 |
| SW-2 | Loopback 1  (ospfv2使用) | 10.16.255.2/32  10.16.255.7/32  2001:10:16:255::2/128 |
| Loopback 2  (ospfv3使用) | 10.16.255.8/32  2001:10:16:255::8/128 |
| VLAN10 SVI | 10.16.11.254/24 |
| VLAN20 SVI | 10.16.21.254/24  2001:10:16:21::254/64 |
| VLAN30 SVI | 10.16.31.254/24  2001:10:16:31::254/64 |
| VLAN40 SVI | 10.16.41.254/24 |
| VLAN50 SVI | 10.16.51.254/24  2001:10:16:51::254/64 |
| VLAN1001 SVI | 10.16.254.14/30 |
| VLAN4094 SVI | 10.16.254.42/30  2001:10:16:254::22/64 |
| 防火墙 | FW-1 | Loopback1 | 10.16.255.3/32 |
| E0/1 | 10.16.254.1/30  （trust安全域） |
| E0/2 | 113.218.100.1/30  （untrust安全域） |
| E0/3 | 10.16.254.18/30  （trust安全域） |
| FW-2 | Loopback1 | 10.16.255.6/32 |
| E0/2 | 10.16.254.10/30  （dmz安全域） |
| E0/1.10 | 172.18.10.254/24（trust安全域） |
| E0/1.20 | 172.18.20.254/24  （trust安全域） |
| E0/1.30 | 172.18.30.254/24  （trust安全域） |
| E0/1.50 | 172.18.50.254/24  （trust安全域） |
| Tunnul 1 | 172.18.100.254/24  （trust安全域） |
| Tunnul 2 | 172.18.101.254/24  （trust安全域） |

任务一、网络搭建及安全部署项目

（50分）

【说明】

1.设备console线有不同两条。交换机、AC、防火墙使用同一条console线，路由器使用另外一条console线。

2.U盘中含有《网络搭建及安全部署竞赛报告单》模板，请按照要求进行过程和结果展示截图，将报告单填写完整。

3.裁判以各参赛队提交的竞赛结果文档为主要评分依据。所有需要提交的文档均放置在U盘的“比赛文档\_AM\_X”或者“比赛文档\_PM\_X”（X为赛位号）文件夹中。

**一、网络布线与基础连接（5分）**

（一）按照网络拓扑图连接设备，并保持网络连接美观。（1分）

（二）自行制作4根网络跳线，要求符合T568A和T568B的标准，长度适中。（2分）

（三）根据网络设备IP地址分配表，为设备接口配置正确的地址。（2分）

**二、交换配置与优化（12分）**

（一）根据网络拓扑图，修改交换机主机名。（1分）

（二）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，包括VLAN 1。根据下述信息及表，在交换机上完成VLAN配置和端口分配。（3分）

|  |  |  |  |
| --- | --- | --- | --- |
| **设备** | **VLAN编号** | **端口** | **说明** |
| SW-1 | VLAN10 | E1/0/1-4 | 招生1段 |
| VLAN20 | E1/0/5-7 | 教务1段 |
| VLAN30 | E1/0/8-9 | 法务1段 |
| VLAN40 | E1/0/11-12 | 财务1段 |
| VLAN50 | E1/0/13-14 | 生产1段 |
| SW-2 | VLAN10 | E1/0/3-4 | 招生2段 |
| VLAN20 | E1/0/5-7 | 教务2段 |
| VLAN30 | E1/0/8-9 | 法务2段 |
| VLAN40 | E1/0/11-12 | 财务2段 |
| VLAN50 | E1/0/13-14 | 生产2段 |
| SW-3 | VLAN20 | E1/0/2-6 | 教务3段 |
| VLAN30 | E1/0/7-11 | 法务3段 |
| VLAN50 | E1/0/12-15 | 生产3段 |
| AC | VLAN20 | E1/0/2-3 | 教务4段 |
| VLAN30 | E1/0/4-5 | 法务4段 |
| VLAN50 | E1/0/6-7 | 生产4段 |

（一）南校区核心SW1和北校区核心SW2间租用运营商两条裸光缆通道实现两个核心之间互通，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二层业务承载。具体要求如下：

1. 为了节约成本，设计实现三层业务承载的裸光缆通道带宽只有100Mbps；（1分）

2. 目前设计实现二层业务承载的只有一条裸光缆通道，随着学校升一本成功，预计未来2-3年南北校区核心交换机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。（1分）

（二）SW1既作为南校区核心交换机，同时又使用相关技术将SW1模拟为Internet交换机，实现与其它业务网段路由表隔离。（1分）

（三）配置相关功能，使核心交换机SW1和SW2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。（1分）

（四） 因产教融合基地实习人员较多、同时也为了节约成本，计划在交换机SW3的14、15端口下挂两个8口交换机实现实习人员的生产业务接入，学校信息中心为实习人员生产业务分配IP主机位为10-30，在交换机上使用相关特性实现只允许上述IP数据包进行转发，对IP不在上述范围内的用户发来的数据包，交换机不能转发，直接丢弃, 要求禁止采用访问控制列表实现。（1分）

（五）产教融合基地的生产网段发现有ARP网关欺骗攻击，请配置相应的安全防护策略。（1分）

（六）产教融合基地的法务业务非常重要，不允许远程传输数据及远程配置电脑，在交换机配置相关命令，实现禁止使用文件传输协议（包含FTP、TFTP等）及远程桌面协议等数据通过。（1分）

（七）核心交换机SW1和SW2开启telnet登录功能，配置实现使用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”。（1分）

**三、路由配置与优化（14分）**

(一) 根据网络拓扑图修改路由器主机名。（1分）

(二)规划南北校区及产教融合基地使用OSPF协议，南北校区使用进程号为1，北校区与产教融合基地间使用进程号为2，具体要求如下：

1. 南校区核心、南校区出口防火墙、北校区核心及北校区路由器之间均属于骨干区域，北校区路由器与产教融合基地之间属于普通区域，区域号为20。（2分）

2. 北校区路由器、南北校区核心交换机、南校区防火墙分别发布自己的环回地址路由；南北校区核心交换机只允许发布生产网段业务路由。（2分）

3. 南校区防火墙和南、北校区核心交换机OSPF进程1中只允许学习到产教融合基地防火墙环回地址与生产业务网段路由，三本学院无线业务网段路由。（2分）

(三) 规划南校区核心交换机与北校区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。（2分）

(四) 为了方便业务灵活调度，同时还规划南北校区及分公司使用BGP协议，进程号为65225，具体要求如下：

1. 北校区路由器与北校区核心交换机之间通过环回地址建立IBGP邻居、北校区路由器与三本学院路由器之间通过互联地址建立IBGP邻居。（1分）

2. 核心交换机SW1和SW2间使用BGP协议实现南北校区间IPV6业务互联互通，满足南北校区间IPV6业务发展的需要。（1分）

3. 要求南北校区的核心交换机、三本学院路由器禁止发布除教务、法务、生产、无线业务网段外的其它路由。（1分）

4. 使用BGP最通用相关功能特性，实现南、北主校区与三本学院间教务、法务、生产业务互通。（1分）

5. 使用BGP相关功能特性，实现BGP配置的路由策略有变化时、可以自动进行策略刷新，无需手工清除BGP会话；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。（1分）

**四、无线配置（5分）**

(一) 根据网络拓扑图修改无线控制器主机名。（1分）

(二) 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。（1分）

(三) 配置一个SSID DCNXX：DCNXX中的XX为赛位号，访问总部及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DCN12345678。（1分）

(四) 开启Radio的自动信道调整，每天上午7:00触发信道调整功能；开启AP逃离策略，防止总部无线控制器异常影响营业网点正常业务。（1分）

(五) 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发送向无线终端表明AP存在的帧时间间隔为1秒；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。（1分）

**五、网络安全配置（9分）**

(一) 根据网络拓扑图修改防火墙的主机名。（1分）

(二) 根据题目要求配置南校区总出口防火墙、产教融合基地防火墙相应的业务安全域、业务接口；设置南校区总出口防火墙只允许南、北校区生产业务、三本学院无线业务、产教融合基地生产业务访问Internet业务；设置产教融合基地防火墙，限制基地的生产业务网段只可以访问Internet业务、教务网段只可以与主校区教务网段https、mysql数据库类型业务间互访；南北主校区所有业务网段均可以与产教融合基地业务网段双向互ping，方便网络连通性测试与排障。（2分）

(三) 在总出口防火墙配置网络地址转换，公网NAT地址池为：113.208.10.0/28，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10.16.10.120。（2分）

(四) 南校区总出口防火墙只有1000M Internet出口，需要进行带宽限速，总出口防火墙上限制教务业务网段每个IP上下行最多4MB/s,其他所有业务网段每个IP上下行最多8Mb/s；对Internet出口http流量整形到10Mbps，从而实现流量精细化控制，保障其它关键应用和服务的带宽。（1分）

(五) 产教融合基地为了便于远程处理业务，计划在防火墙FW2上开启SSLvpn服务，配置两条SSLvpn加密隧道，一条采用端口5551，一个采用端口6662，方便不同权限的管理员在外可通过登录VPN访问内部的不同资源。隧道接口地址详见地址分配表，每个VPN的地址池从第10个可用地址开始共100个地址，均创建2个用户（VPN1：user1至user2；VPN2：user4至user5）。VPN1仅可访问地址段为：172.18.50.25-172.18.50.60，VPN2仅可访问可访问地址段为：172.18.50.66-172.18.50.100。（3分）

**六、 路由选路优化（5分）**

考虑到从南北总校区到三本学院共有三条链路，且其带宽不一样，总校区法务业务网段与三本学院法务业务网段互访只允许在总校区路由器S0/1与三本学院路由器S0/2专线间转发；总校区教务业务网段与三本学院教务业务网段互访只允许在总校区路由器S0/2与三本学院路由器S0/1专线间转发；总校区生产业务网段与三本学院生产业务网段互访、三本学院SSID DCNXX与Internet业务互访只允许在总校区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总校区法务业务网段与三本学院法务业务网段互访、总校区教务业务网段与三本学院教务业务网段互访备用链路。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：

1.使用IP前缀列表匹配上述业务数据流。（2分）

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属性可配置的参数数值为：200。（3分）

任务2、服务器配置及应用项目

（48分）

**【竞赛技术平台说明】**

**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默认域、账号、密码为default\admin\dcncloud，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。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 名称 | 用户名 | 密码 | ssh | rdp |
| Windows10 | administrator | Qwer1234 | 否 | 是 |
| WindowsServer2012 | 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，centos主机实例可以通过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.云服务实训平台和服务器PC1和PC2相关服务说明:**

（1）题目中所有未指明的密码均为“2021Netw@rk（注意区分大小写）”，若未按照要求设置密码，涉及到该操作的所有分值记为0分。

（2）虚拟主机的IP属性设置请按照“拓扑结构图”以及“服务器IP地址分配表”的要求设定。

（3）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。

#### **服务器IP地址分配表**

| **宿主机** | **虚拟主机名称** | **域名信息** | **服务角色** | **系统及**  **版本信息** | **IPv4**  **地址信息** |
| --- | --- | --- | --- | --- | --- |
| **云**  **实**  **训**  **平**  **台** | 云主机1 | ad.netskills.net | 域控制器  DNS服务器  DHCP服务器 | Windows Server 2012 R2 | 10.16.11.xx/24 |
| 云主机2 | ca.netskills.net | 主CA服务器  辅助域控制器 | Windows Server 2012 R2 | 10.16.11.xx/24 |
| 云主机3 | www.netskills.net | WEB服务器  FTP服务器 | Windows Server 2012 R2 | 10.16.11.xx/24 |
| 云主机4 | iscsi.netskills.net | 存储服务器  更新服务器  ISCSI服务器 | Windows Server 2016 R2 | 10.16.11.xx/24 |
| 云主机5 | ftp.chinaskills.net | DNS服务器  FTP服务器 | Centos 7.4 | 10.16.21.xx/24 |
| 云主机6 | nat.chinaskills.net | NAT服务器  DHCP服务器 | Centos 7.4 | 10.16.21.xx/24  10.17.30.254/24 |
| 云主机7 | mail.chinaskills.net | 邮箱服务器 | Centos 7.4 | 10.16.21.xx/24 |
| 云主机8 | www.chinaskills.net | WEB服务器 | Centos 7.4 | 10.16.21.xx/24 |
| 云主机9 | sql.chinaskills.net | 数据库服务器 | Centos 7.4 | 10.16.21.xx/24 |
| 客户端 | win10.netskills.net | Client | Windows 10 | 10.16.21.xx/24 |

#### **云平台网络信息表**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **网络**  **名称** | **Vlan号** | **外部**  **网络** | **子网**  **名称** | **子网网络地址** | **网关IP** | **激活DHCP** | **地址池范围** |
| Vlan10 | 10 | 是 | Vlan10-subnet | 10.16.11.xx\24 | 10.16.11.254\24 | 是 | 10.16.11.100,  10.16.11.200 |
| Vlan20 | 20 | 是 | Vlan20-subnet | 10.16.21.xx\24 | 10.16.21.254\24 | 是 | 10.16.21.100,  10.16.21.200 |

#### **虚拟主机信息表**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **虚拟主机名称** | **镜像模板 (源)** | **VCPU 数量** | **内存、硬盘信息** | **网络名称** | **备注** |
| 云主机1 | WindowsServer2012 | 1 | 2G、40G | Vlan10 | 域控 |
| 云主机2 | WindowsServer2012 | 1 | 2G、40G | Vlan10 | 加入域 |
| 云主机3 | WindowsServer2012 | 1 | 2G、40G | Vlan10 | 加入域 |
| 云主机4 | WindowsServer2016 | 1 | 2G、40G | Vlan10 | 连接卷hd1-hd5 |
| 云主机5 | Centos7-mini-V2 | 1 | 1G、30G | Vlan20 | \ |
| 云主机6 | Centos7-mini-V2 | 1 | 1G、30G | Vlan20 | \ |
| 云主机7 | Centos7-mini-V2 | 1 | 1G、30G | Vlan20 | \ |
| 云主机8 | Centos7-mini-V2 | 1 | 1G、30G | Vlan20 | \ |
| 云主机9 | Centos7-mini-V2 | 1 | 1G、30G | Vlan20 | \ |
| 云主机10 | windows10 | 1 | 2G、40G | Vlan20 | 加入域 |

### 云实训平台安装与运用

**一、云平台基础设置**

1.按照“云平台网络信息表”要求创建两个外部网络，这些外部网络所使用的 VLAN均为总部业务VLAN，详细操作过程请参照“云服务实训平台用户操作手册”。

2.创建5块云硬盘，卷命名为hd1-hd5，其中hd1-hd5大小为10G；将所有的云硬盘连接至云主机4。

注意:必须通过“项目”栏中的“计算”子栏中的“卷”功能来创建云硬盘；不能使用“管理员”，“系统”栏下的“卷”功能，该功能使用不当会造成云硬盘创建失败，界面卡死。

在云平台中可以创建多个云硬盘，所有云硬盘容量的总大小不能超过 100G，否则将创建失败。一个实例可以同时连接多个云硬盘，但一个云硬盘同时只能给一个实例作为扩展硬盘使用。

在分离卷之前一定要保证使用该卷的linux 主机中，已经不存在该卷的任何挂载点。如果使用该卷的主机是windows 实例，必须保证该卷在主机的“磁盘管理”项目中处于脱机状态，否则会造成分离失败，或是一直显示“分离中”状态。

**二、创建虚拟主机**

1.按照“虚拟主机信息表”所示，按要求生成虚拟主机，详细操作过程请参照“云服务实训平台用户操作手册”。

2.云平台中所有虚拟机的IP地址，要求手动设置为该虚拟机DHCP获取的地址。

### Windows操作系统（15分）

**一、AD-域控服务器（4分）**

1.将云主机1的服务器配置成域控制器，域名为netskills.net，设置域和林的功能级别为Windows Server 2012。（0.5分）

2.启用Active Directory的回收站功能；将此服务器配置为主DNS服务器:正确配置netskills.net区域的正向及反向解析区域；创建对应服务器主机记录，正确解析netskills.com域中的所有服务器。（0.5分）

3.关闭网络掩码排序功能；配置DNS的SOA为netskills.net，NS为netskills.net，负责人Tech，刷新间隔20分钟；DNS日志大小上限为17984KB，覆盖超过7天的事件，设置转发器8.8.8.8，清理过时记录，刷新间隔5天。（0.5分）

4.对netskills.net区域中的所有主机记录提供完整性验证，来保证数据在传输的过程中不被篡改。（0.5分）

5.创建3个组织单位、采用对应部门名称的中文全拼命名，每个部门创建2个用户，行政部用户:adm1~adm2、营销部用户:sale1~sale2、技术部用户:sys1~sys2，所有用户第一次登陆必须修改密码，账号设置“使用可逆加密存储密码”，并要求用户只能在上班时间可以登录（每周一至周五9:00~17:00）。（0.5分）

6.配置域中技术部的所有员工必须启用密码复杂度要求、密码长度最小为8位、密码最长存留34天、允许失败登录尝试的次数为4次、重置失败登录尝试计数（分钟）为5分钟、直至管理员手动解锁帐户。（0.5分）

7.配置相关策略，实现所有技术部的用户登录域后自动去除“计算机”的上下文菜单中的“属性”。（1分）

**二、AD、CA-额外域控、证书服务器**（3分）

1.创建云主机2加入域后，安装CA服务，配置CA服务器的私钥加密为MD5加密方式。（0.5分）

2.安装证书服务，为企业内部手动回复证书申请；设置为企业根，此证书颁发机构生成的证书有效期为2年。（0.5分）

3.配置CA服务器后，要求证书申请者只能通过ssl加密通道访问证书申请页面；去除证书申请页面的访问限制，要求证书申请者无需登录即可访问证书申请页面。（0.5分）

4.将云主机2的服务器配置成“skillschina.com”额外域控制器。（0.5分）

5.添加辅助DNS区域，云主机2成为云主机1的辅助DNS，备份所有条目，备份成功后查看DNS正反向查找区域。（1分）

**三、WEB、SAMBA、FTP-网站、共享、文件服务器**（6分）

1.创建云主机3加入域后安装IIS组件，创建www.netskills.net站点，将网站的根目录设置为C:\www文件夹下，网站内容为:“欢迎访问网站页面”。（0.5分）

2.设置网站的最大连接数为1100，网站连接超时为70s，网站的带宽为1100KB\S，日志文件存储到“C:\WWWLogFile”目录中。（0.5分）

3.将云主机3中的证书申请文件导出，访问云主机2证书申请页面申请web证书后，申请到证书后将证书文件存储到C:\ssl\文件夹下；将服务器配置成CA服务器，证书必需信息为：（0.5分）

|  |  |
| --- | --- |
| 通用名称 | www.netskills.net |
| 组织 | netskills |
| 组织单位 | sales |
| 城市\地点 | ChangSha |
| 省\市\自治区 | HuNan |
| 国家\地区 | CN |

4.设置https网站根目录为C:\www-ssl\，设置https网站默认端口为4433，将证书文件导入到云主机3中，要求访问者能够使用ssl加密访问网站，网站内容为“欢迎访问SSL网站”。（0.5分）

5.备份该网站用于解密ssl网站私钥文件，将私钥文件命名成private.txt，并且将私钥文件放置到C:\ssl\文件夹内，以文本方式打开查看。（0.5分）

6.在C:\下面新建SAMBA文件夹，将其设置为共享文件夹，开放共享文件夹的权限给sys1用户，要求sys1只允许下载该文件夹内的文件，不允许上传，开放共享文件夹的权限给sys2用户，要求sys2允许上传下载该文件夹的文件。（0.5分）

7.新建FTP服务，将默认端口修成2121，启动虚拟主机名:ftp.netskills.net，使用C:\ssl\文件夹下的证书文件，搭建ftps服务，ftps的根目录为C:\ftps，要求技术部员工可以上传下载，其他部门的员工只拥有上传功能。（1分）

8.配置“连接安全规则”，配置其他的云主机的安全规则和云主机4一致，入站和出站都要求身份验证，完整性算法采用SHA-1，加密算法采用AES-CBC 128，预共享的密钥为chinaskills。（2分）

**四、Windows server、ISCSI-更新服务器**（2分）

1.创建云主机4并且加入到域中，连接云平台上的五块硬盘，将新增的硬盘制作成RAID5磁盘列阵，加入到存储池中，并且将创建的磁盘名修改成“E:\”盘。（0.5分）

2.安装iscsi服务，在E创建四个虚拟磁盘，每个磁盘6G；分别取名为:LINUX1-4。（0.5分）

3.将更新文件存储服务安装在此服务器上，为内网主机提供更新，从Microsoft更新中同步，更新包括SQL SERVER，每天晚上12点自动同步，每周8点送状态报告到123@qq.com，下载快速安装文件。（0.5分）

4.配置“连接安全规则”，配置其他的云主机的安全规则和云主机3一致，入站和出站都要求身份验证，完整性算法采用SHA-1，加密算法采用AES-CBC 128，预共享的密钥为chinaskills。（0.5分）

### Linux操作系统部分（15分）

**一、存储服务器（3分）**

1.安装云主机5后，在云主机5安装iSCSI客户端后，连接云主机4的iSCSI磁盘，并且将该磁盘挂载至\ima上，并且设置成开机自动连接自动挂载。（0.5分）

2.在此服务器上安装VSFTP，要求新建虚拟用户，账号密码一致为:ftpuser1-3，宿主根目录为\ima，在\ima路径下分别新建宿主目录为ftpuser1-3。（0.5分）

3.FTP的虚拟用户ftpuser1拥有上传下载创建文件的权限，虚拟用户ftpuser2权限为:上传下载创建删除重命名权限；ftpuser3只拥有读取文件的权限。（0.5分）

4.在FTP服务器上开启Ascii上传与下载、将所有用户的用户目录限定在自己的家目录内；关闭匿名者登陆，开启被动数据传输模式，端口范围3000-3100、设置最大连接数为100，每个IP连接数2个，空闲5分钟断开。（0.5分）

5.给VSFTP主配置文件加上不可更改属性，在锁定文件的情况下，任何用户（包括root）也不能更改该文件。（0.5分）

6.服务器配置防火墙策略，要求默认禁止所有的连接，只开放该服务器上安装的服务端口，保证该服务器上所有的服务均能正常使用。（0.5分）

**二、NAT、DHCP、DNS服务器（3分）**

1.安装云主机6后，在云主机6上多新增一张网卡2以用作NAT地址转发，设置此网卡2地址为: 10.17.30.254/24。

2.在此服务器上安装DHCP服务，网段为此服务器网卡2的地址段，地址池为220-225。指定DNS服务器为云主机6的地址以及网关的IP地址信息，设置租约时间43200s，最大租约时间为86400s。

3.修改网卡接口区域，将第一张网卡设置为public区域，将网卡2设置为external区域，设置地址伪装，要求将10.17.30.0/24网段的地址伪装成网卡1的地址进行数据转发。

4.将你所作的NAT配置永久保存，防止开机启动后失效。

5.在此服务器中安装配置DNS服务，负责区域”chinaskills.com”内主机解析，，做好正反向DNS服务解析。

6.服务器配置防火墙策略，要求默认禁止所有的连接，只开放该服务器上安装的服务端口，保证该服务器上所有的服务均能正常使用。

**三、MAIL-邮箱服务器（3分）**

1.安装云主机7后，连接云主机4的iSCSI磁盘，并且将该磁盘挂载至\imail上，并且设置成开机自动连接自动挂载。

2.在此服务器上安装配置邮件服务，要求创建三个邮箱用户mail4，mail5，mail6，用户密码为123，不允许命令行登陆。

3.设置用户邮箱存放的目录为\imail下，每个用户新建一个文件夹，文件夹命名为邮箱用户名。

4.邮件服务器的域名后缀为chinaskills.com，邮件服务器要在所有IP地址上进行侦听；拒绝垃圾邮件，设置邮件服务器的黑名单，拒绝接收用户mail6的邮件。

5.配置邮件服务器的SSL连接，具体要求，设置仅支持pop3s协议连接，证书需要向云主机2申请证书，并且保存在\root\ca下。

6.测试邮箱的可使用性，使用mail4发送测试给mail5，查看收件邮件。

**四、WEB-网站服务器（3分）**

1.安装云主机8，连接云主机4的iSCSI磁盘，并且将该磁盘挂载至\iweb上，并且设置成开机自动连接自动挂载；

2.在此服务器中安装Apachehe+php服务，建立虚拟主机站点www.chinaskills.com，其网站主目录为\iweb\www\html\www1，新建主页存放该主目录中，主页名称为index.php，内容为“<?php phpinfo();?>”。

3.配置访问日志路径和名称为为\iweb\log\httpd\www1.netdj.net-access\_log，日志记录格式为普通型。

4.新建一个用来存储上传文件的文件夹，\iweb\www\html\www1\upload，使用相关方法，禁止此文件夹执行php脚本，但是需要保证能够正常存储其他文件。

5.隐藏apache和php版本号、禁止apache显示目录结构，通过访问http:\\ www.chinaskills.net\ss查看访问结果。

6.生成证书生成文件，要求向云主机2申请CA证书，获得证书批准后,新建一个新站点，要求网站根目录为\iweb\www\html\www2，主页名称为index.php，内容为<?php system(”whoami”);?>。

7.将apache使用的证书文件的私钥导出\root\ca文件夹下，以用作备份。

**五、SQL-数据库服务器（3分）**

1.安装云主机9，连接云主机4的iSCSI磁盘，并且将该磁盘挂载至\isql上，并且设置成开机自动连接自动挂载。（0.5分）

2.安装数据库服务，并且修改数据库存放数据的位置为\isql\，更改数据库登陆账号为root\123456，数据库的远程登陆账号为:root\654321。（0.5分）

3.创建数据库Campus，创建表information,后创建数据库用户为:user1，要求user1用户具有远程连接数据库的权限，要求该用户连接数据库后只能看到Campus数据库。（0.5分）

4.创建数据库表，表结构如下：

|  |  |  |  |
| --- | --- | --- | --- |
| **字段名** | **数据类型** | **主键** | **注释** |
| ID | Int | 是 | 序号 |
| Name | varchar(10) | 否 | 名字 |
| Sex | varchar(4) | 否 | 性别 |
| age | varchar(3) | 否 | 年龄 |
| Birthday | Datetime | 否 | 出生日期 |
| Phone | varchar(11) | 否 | 电话 |

5.创建文本xx.txt并输入两行记录（1,wws1,male,21,1999-8-20,15611112222）（2,wws2,female,24,1995-9-15,15822221111）将内容导入至information表中。（0.5分）

6.服务器配置防火墙策略，要求默认禁止所有的连接，只开放该服务器上安装的服务端口，保证该服务器上所有的服务均能正常使用。（1分）

### 测试排障部分（8分）

**测试结果**

1.安装Windows 10操作系统后，使用技术部账号加入云主机1域中，右击桌面上的“计算机”后进行截图。（0.5分）

2.访问云主机2的证书申请页面，申请用户证书后进行截图。（0.5分）

3.访问云主机3的http://www.netskills.net、https://www.netskills.net:4433，将访问结果进行截图。（0.5分）

4.测试云主机3的FTP功能，使用技术部员工的账号密码进行登陆，测试其上传下载功能；分别截图。（0.5分）

5.访问云主机3的SAMBA文件夹、分别使用sys1、sys2上传下载功能，分别截图。（1分）

6.访问云主机5的FTP功能，使用虚拟账号登陆FTP服务器，使用账号ftpuser1-3分别登陆，测试其服务器的上传下载功能，分别截图。（1分）

7.测试云主机6的DNS功能，修改网卡的DNS后，使用命令“nslookup”，将“chinaskills.net”的所有主机域名进行测试并且分别截图。（1分）

8.使用Windows自带的邮箱登陆客户端，使用账号“mail4”登陆邮箱后给mail5发送邮件，标题“test”，内容“test mail”；发送成功后截图。（1分）

9.访问云主机8的web功能，通过浏览器访问http://www.chinaskills.net、https://www.chinaskills.net，分别截图。（1分）

10.访问云主机9的数据库功能，使用cmd窗口，输入命令“telnet （云主机9IP） 3389”，后将窗口截图。（1分）

任务三、职业规范与素养

（2分）

一、整理赛位，工具、设备归位，保持赛后整洁有序。（1分）

二、无因选手原因导致设备损坏。（1分）