**2019年全国职业院校技能大赛**

**赛项申报方案**

一、赛项名称

（一）赛项名称

网络搭建与应用

（二）压题彩照



（三）赛项归属产业类型

第三产业-信息传输、计算机服务和软件业

（四）赛项归属专业大类/类

|  |  |  |  |
| --- | --- | --- | --- |
| **组别** | **专业类** | **专业代码** | **专业名称** |
| 中职 | 09信息技术类 | 090500 | 计算机网络技术 |
| 中职 | 09信息技术类 | 090100 | 计算机应用 |
| 中职 | 09信息技术类 | 090600 | 网站建设与管理 |

1. 赛项申报专家组

三、赛项目的

通过竞赛，引导中职院校关注绿色、安全、共享、智慧的计算机网络技术发展趋势和产业应用方向，引导行业、企业、院校促进产教融合、校企合作，引领中职信息技术类专业建设紧密对接新一代信息技术产业链、创新链的专业体系，提升学生专业能力素质与企业用人标准的吻合度，以适应新一轮科技革命和产业变革及新经济发展，为在新形势下全面提高信息技术类专业教学质量、扩大就业创业、推进经济转型升级、培育经济发展新动能做出新贡献。

赛项涉及了计算机网络技术专业中网络布线设计与施工、网络设备安装与调试、无线网络测试与维护、网络系统管理与维护、网络技术支持与服务、网络安全配置与管理等专业（技能）方向，涵盖了在交换路由、无线网络、虚拟网络、信息安全、系统管理、云服务等六大领域的知识点和技能点，重点检验了参赛选手网络拓扑的理解能力、IP地址的规划能力、网络设备的调试能力、网络安全的防范能力、系统服务器的配置能力、网络故障的排除能力、应用服务的管理能力、技术文档的阅读能力、现场问题的解决能力、团队组织的协调能力和质量成本的控制意识。

赛项作为全国职业院校技能大赛的成熟赛项，已经成功举办十一年。为参赛选手提供了网络技术方面自我实践能力的展示平台，成就了大量的高素质技能人才；提升了专业教师实践技能，培养了大批网络领域优秀师资；拓展了职业学校的专业视野，使之明确了企业社会对人才需求的要求和标准；充分展现了职教改革成果及师生良好精神面貌，扩大了职业教育社会影响力，促进了职业教育在全社会弘扬工匠精神。

四、赛项设计原则

（一）公开、公平、公正。

为保证竞赛公平、公开、公正，本赛项成功举办十一年来汇集大量国赛及各省市赛的样题、赛题。每年比赛来源于以专家组、国家示范校、行业专家、企业专家为班底成立赛题开发团队，参照行业规范，工作内容，设计比赛试题。

大赛设计与国际接轨，在竞赛前发布竞赛设备、设备技术文档，竞赛网络环境和赛题相关信息，参赛选手可以有充分的时间思考网络架构、查找网络资料、针对性训练，技能水平得以迅速提高；在实际竞赛中，基于已经发布的网络环境和赛题要求，选手可对竞赛任务书中具体的技术问题借助设备技术文档进行设计和解决；在竞赛后，再次发布抽中正式比赛赛题和与之对应的评判标准，帮助参赛学校提高整体专业水平。整个竞赛过程，力求通过科学细致的评分标准、开放的形式、工作团队严谨认真的态度，与真实工作实践相符合竞赛内容、充分考察学生解决网络工程实践能力和整体知识技能运用能力，同时也最大限度保障竞赛的公平、公开、公正性。

（二）赛项关联专业人才需求量大或行业人才紧缺或职业院校开设专业点多，服务国家重点战略。

赛项符合习近平同志在中央网络安全和信息化领导小组第一次会议上指出：“建设网络强国，要有自己的技术，有过硬的技术”的要求。目前大多数中职学校都开办了计算机及网络相关专业，赛项覆盖地区、学校、专业点、学生众多，随着国家对网络技术要求日益提升，各地对高素质网络技术技能型人才需求量长年高居不下。赛项通过对计算机网络和集成企业进行调研和分析，根据行业企业业务背景进行网络业务需求分析、技术应用环境分析，理解实际的工程应用与业务架构分析，结合国家专业教学标准，确定了中职计算机网络毕业生主要从事系统集成、系统应用、网络工程、网络安全及售后技术支持等五个岗位。

竞赛设计适应国家“新一代信息技术产业”的需要，聚焦计算机网络领域岗位的主要技能，与国产知名网络厂商合作，以实际工作项目为基础，针对计算机网络专业学生的“能力短板”，围绕计算机网络领域的先进技术、主流产品，力求突出工作实践；以赛促教，以赛促改，引领计算机网络专业的教育教学改革；通过竞赛提升中职计算机网络专业学生的信息安全意识、设备配置和系统管理能力，使之具备适应岗位工作的全面能力；通过竞赛展示中职计算机网络专业学生的工作实践能力，促进社会对网络强国、网络技术的重视，充分提高中职计算机网络专业的社会认可度，着重提高学生的就业质量和就业水平，服务于国家重点战略落地。

（三）竞赛内容对应相关职业岗位或岗位群、体现专业核心能力与核心知识、涵盖丰富的专业知识与专业技能点。

竞赛内容就是岗位的主要工作内容，主要分为三部分：

1. 网络组建：利用赛项提供的计算机、网络等设备完成设备连接、链路质量检测、端口检测；IP地址规划与实施；交换机、路由器和无线等网络设备的设置与调试，局域网、广域网、虚拟云的相关配置。

2. 服务器配置及应用：安装服务器操作系统(Windows/Linux)并配置DNS、Web、FTP、E-mail、DHCP等各种系统服务(Windows/Linux)、数据库安装配置、系统管理、云服务部署，集群技术。

3. 网络设备安全配置与防护：部署防火墙保证网络安全，包括实现路由、NAT转换、防DDoS攻击、包过滤、URL过滤、P2P流量控制、入侵检测、病毒攻击、缓冲区溢出攻击、端口攻击等、利用VPN技术实现远程安全接入和站点到站点的IPsec VPN；配置无线网络WEP加密、MAC认证接入控制。

最终达到在安全的网络环境下，实现服务器、存储、网络无缝对接，云部署、系统服务与网络设备协同工作，并合理实现信息应用。

（四）竞赛平台成熟。根据行业特点，赛项选择相对先进、通用性强、社会保有量高的设备与软件。

赛项覆盖全国各地区、各学校、及各专业点学生众多，参与群体数量广，形成成熟的校赛、省(地、市)赛、国赛的三级大赛机制。赛项从2008年企业网搭建、园区网应用赛项开始，至今已经顺利举行十一年，每年都要经历全国30余个省赛（全国近100场的市赛），竞赛平台的技术成熟。

2019年赛项设计中在保证原有主要比赛设备不变的基础上，针对业内出现的新技术、新功能，并考虑其实际工作应用成熟度，适时提升Centos免费系统软件版本，以保证赛项的技术引领性。

赛项各方无论在赛事组织、技术支持、赛项实施、安全保障都具备丰富经验；网络设备合作企业为行业知名企业，连续支持赛项多年，社会及院校保有量高，系统软件为免费或者试用版，参赛学校无软件费用负担。

五、赛项方案的特色与创新点

1. 竞赛内容选择贴近行业，关注新技术和新产业需求。

近些年，在新技术、新业务的强力带动下，宽带网络、移动互联网、云计算、虚拟化等新业态的发展不断推动信息技术行业加速前行。特别是信息通信技术的创新与扩展，与传统产业生产组织和制造业的深度融合，加快推动了以数字化、网络化、智能化、服务化为核心的新型产业变革，随之带来了各地对精通交换机、掌握网络服务、虚拟化和云计算技术的高素质技能型人才需求量长年高居不下。

竞赛内容来源与实际应用的网络业务需求，依据行业客户真实案例，竞赛时间内在网络架构的不同功能区域，合理部署RIP、OSPF、BGP等多种路由协议，以及NTP和DHCP服务等常见协议的应用，实现了综合性网络架构的部署；通过防火墙的安全策略的部署及路由交换上QOS、策略、IPSEC VPN等安全策略的使用，有效的实现了多部门、多业务及多应用的优化及部署，并实现了广域网链路加速，广域网链路加密，无线安全，流量过滤与优化等；在云服务实训平台部分上实现了多种业务及应用系统的基础平台的搭建，并完成了域控制器迁移、存储和故障转移群集等应用的部署工作，实现云与传统网络的对接。

赛项的考查选手配置网络互联互通、管理系统运行服务、防范网络安全威胁、实现设备虚拟化，部署云平台应用等技术技能，既考虑到传统网络运维，又充分关注了新技术和新产业需求，体现赛项内容的与时俱进。

（二）竞赛过程安排合理、赛项成熟稳定。

竞赛设计符合行业通用规范与标准，使用的竞赛技术平台和设备为行业内主流企业的通用产品，支持国赛十余年，中职学校拥有率高、技术性能可靠性强。竞赛过程无论从赛项设计、规程制定、赛项说明、赛题公开、培训评判、正式比赛、结果评判、技术点评，还是从场地准备、平台测试、生活保障、电力备份、医疗应急等各方面均呈现了优质、高效、周到、细致工作。特别是近些年严格按照大赛制度要求，“热情办赛、精彩办赛、依规办赛、安全办赛”，每年都高标准、出色的完成赛事工作，赛项成熟稳定。

（三）竞赛公开、公平、公正，赛项多年零投诉。

赛项严格遵照《全国职业院校技能大赛制度》设计赛项，认真落实、遵照实施，竞赛过程供参赛学校现场观摩、多机位视频直播，保证了实时、全方位、无死角、完整展示参赛选手的操作过程和工作成果，全部客观性结果评判，赛后合理方式公布成绩，成绩结果呈正态分布。赛事效果长期良好，制度颁布五年来，赛项年年零投诉，得到参赛院学校的一致高度认可，充分彰显了竞赛的公平、公正、公开。

（四）竞赛资源转化，内容丰富实用。

“以赛促教、以赛促改、以赛促学”是全国职业院校技能大赛的重要目的。将竞赛内容成功转化为教学资源无疑是实现这一目的的重要保障。企业专家和院校专家校企合作，共同形成中等职业计算机网络技术专业教学资源包，系统梳理计算机网络技术专业的培养目标、岗位需求、课程体系、核心知识点及历年竞赛考核内容与评分要点，并结合技术发展趋势对未来的竞赛内容设置进行了权威预测；开发了一套融入大赛思想的，体现“新设备、新技术、新标准”的实用型系列教材。

六、竞赛内容简介（须附英文对照简介）

赛项简介：团体赛。根据赛场软、硬件环境和网络建设要求，遵照工作规范，团队合作完成网络架构及应用平台的搭建，并保障网络应用的安全性和可靠性。

竞赛内容即岗位主要工作内容，分为三部分：

1. 网络组建：利用本届大赛执委会提供的计算机、网络等设备完成设备连接、链路质量检测、端口检测；IP地址规划与实施；交换机及交换机虚拟化、路由器和无线等网络设备的设置与调试，局域网和广域网的相关配置。

2. 服务器与云服务实训平台配置及应用：使用云服务实训平台配置DNS、Web、FTP、E-mail、DHCP服务(Windows/Linux)、数据库配置、服务器系统管理、虚拟化技术，服务器集群技术，JDK安装部署、Tomcat安装及部署移动WEB应用，并访问。

3. 网络设备安全配置与防护：部署防火墙，包括实现路由、NAT转换、防DDoS攻击、包过滤、URL过滤、P2P流量控制、病毒攻击、缓冲区溢出攻击、端口攻击等、利用VPN技术实现远程安全接入和站点到站点的IPsec VPN；配置无线网络WEP加密、MAC认证接入控制等竞赛内容。

Brief introduction to the competition: team competition. According to the software and hardware environments and the requirements for establishing the network, In accordance with the norms, Team work to establish the framework of the network, set up the application platform and ensure the safety and reliability network application.

The content of competition is the main content of the jobs, is divided into three parts:

1.setup the network: Completing the network connections, Link quality and port detection, implementing the IP address planning，Setting and debugging the equipment including the switches and VSF, the routers, the wireless equipment and network security equipment，with the computers and equipment those was provided by Competition Commission. Aiming at the problems of complex network configuration, low operation efficiency and slow fault switching in traditional park network, the new technology of virtual switch is added.

2.Server and Cloud training platform configuration and application: use Cloud training platform configure DNS, Web, FTP, E-mail, DHCP services (Windows/Linux), install the database, according to the requirements of the use of virtualization technology, the server cluster technology to realize network high availability and load balancing.

3.Network security and protection configuration: The deployment of firewall network security, including Implementation of routing, NAT conversion, the anti DDoS attack, packet filtering, URL filtering, P2P flow control, virus attacks, buffer overflow attacks, port attack, using VPN technology to realize remote secure access and site to site IPsec VPN, Configure your wireless network WEP encryption, MAC authentication and access control.

Requirements of teaming: two contestants and at most two instructors for each team.

七、竞赛方式（含组队要求、是否邀请境外代表队参赛）

（一）竞赛方式：团体赛

（二）组队要求：省、自治区、直辖市、计划单列市、新疆生产建设兵团可组织报名参加比赛，每支参赛队由2名选手组成，不得跨校组队，其中队长1名，可配2名指导教师。

（三）参赛说明：凡在往届全国职业院校技能大赛中获一等奖的选手，不能再参加同一项目同一组别的比赛。

（四）本赛项正在与国际参赛队接洽，同时欢迎国内外团队及选手到场观赛。

八、竞赛时间安排与流程

（一）竞赛时间

本赛项竞赛时间3小时

（二）日程安排

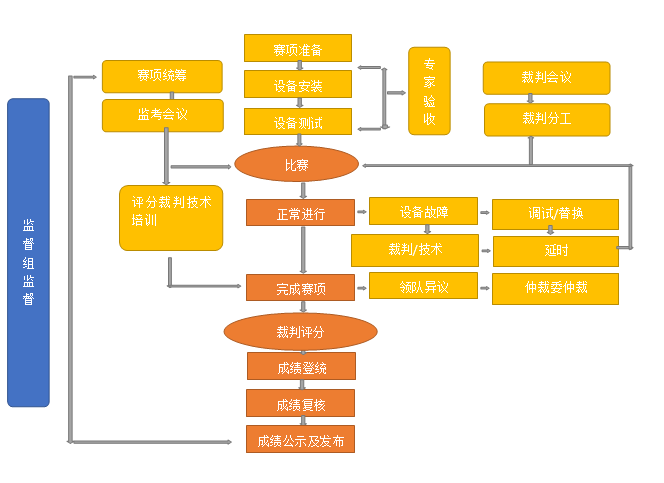
具体安排分配如下：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **日期** | **时间** | **事项** | **参加人员** | **地点** |
| 竞赛前2日 | 20:00前 | 裁判、仲裁、监督报到 | 工作人员 | 住宿酒店 |
| 竞赛前1日 | 09:00-12:00 | 参赛队报到，安排住宿，领取资料 | 工作人员、参赛队 | 住宿酒店 |
| 09:00-12:00 | 裁判工作会议 | 裁判长、裁判员、监督组 | 会议室 |
| 13:00-14:30 | 领队会 | 各参赛队领队、裁判长 | 会议室 |
| 15:00-16:00 | 参观赛场 | 各参赛队领队 | 竞赛场地 |
| 16:00 | 检查封闭赛场 | 裁判长、监督组 | 竞赛场地 |
| 16:00 | 返回酒店 | 参赛领队 | 竞赛场地 |
| 竞赛  当天 | 07:30 | 参赛队到达竞赛场地前集合 | 各参赛队、工作人员 | 竞赛场地前 |
| 07:30-07:40 | 大赛检录 | 参赛选手，检录工作人员 | 竞赛场地前 |
| 07:40-08:00 | 第一次抽签加密（抽序号） | 参赛选手、第一次加密裁判、监督 | 一次抽签区域 |
| 08:00-08:20 | 第二次抽签加密（抽工位号） | 参赛选手、第二次加密裁判、监督 | 二次抽签区域 |
| 08: 00 | 依次进入赛场 | 现场裁判、裁判长、监督 | 竞赛场地 |
| 08:20-08:30 | 就位并领取比赛任务 | 参赛队 | 竞赛场地 |
| 08:20 | 比赛选手就位，裁判员宣读竞赛须知 | 参赛选手、现场裁判、裁判长、监督 | 竞赛场地 |
| 08:30-11:30 | 正式比赛 | 参赛选手、现场裁判、裁判长、监督 | 竞赛场地 |
| 08:30-11:30 | 评分裁判培训会议 | 裁判、监督、专家组 | 会议室 |
| 11:30-12:30 | 午餐 | 参赛选手、裁判、仲裁、监督、专家组、指导教师、领队 | 承办校安排 |
| 12:30 | 回酒店 | 参赛选手、指导教师、领队 | 住宿酒店 |
| 12:30-评判完毕 | 评判（含晚餐、夜宵） | 评分裁判、裁判长、专家、监督 | 竞赛场地 |
| 评判完毕后 | 成绩汇总报送，成绩公示 | 评分裁判、裁判长、专家、监督 | 竞赛场地  和参赛队住宿酒店 |
| 竞赛  后1日 | 13:00-14:00 | 专家讲评 | 领导、嘉宾、裁判组、各参赛队、专家组、监督组 | 礼堂 |
| 闭赛式 |

（三）比赛流程

赛前准备：选手抽签加密入场，参赛队就位并领取比赛任务，完成比赛设备、线缆和工具检查等准备工作。

正式比赛：参赛选手需按题目要求规划IP地址，配置网络设备、安装调试操作系统，配置安全策略等，完成企业级网络搭建及应用项目实施，操作顺序和分工，由参赛队自行商定。



九、竞赛试题

（一）赛项执委会下设的专家工作组负责本赛项命题工作。

（二）本赛项建有赛题库，赛题库含10套竞赛赛卷。

（三）正式比赛公开方式为赛卷和主要网络环境公开。比赛完成后，赛卷进行封闭回收。

（三）具体内容将于开赛1个月前，在大赛信息发布平台上(<http://www.chinaskills-jsw.org>)发布。

样题详见附件1：2019年全国职业院校技能大赛网络搭建与应用竞赛样题

十、评分标准制定原则、评分方法、评分细则

（一）评分标准的制定原则

竞赛评分严格按照公平、公正、公开的原则，评分标准注重考察参赛选手以下三个方面的能力和水平：

1. 网络系统的安装组建、配置管理、安全防护的正确性、规范性和合理性；

2. 相关文档的准确性与规范性；

3. 竞赛要求遵守、团队风貌、团队协作与沟通、组织与管理能力；

（二）评分方法：结果性评分

1. 参赛队成绩由赛项裁判组统一评定；

2. 评分流程按照《全国职业院校技能大赛制度汇编》成绩管理办法中结果性评分统一要求执行，100%为客观性评分。

（三）评分细则

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **具体内容** | | **分值及评分细则** |
| 1 | 综合布线  5% | 网络综合布线安装和施工 | 完成配线架安装调试，设备连接，保证和测试物理连通性 |
| 2 | 网络配置  45% | IP地址划分实施 | 完成子网划分、IP规划实施 |
| 3 | 网络调试 | 完成指定的交换路由、广域网和无线的配置 |
| 4 | 硬件防火墙配置 | 完成企业网的相关策略配置 |
| 5 | 网络配置优化 | 完成网络优化配置,交换虚拟化配置 |
| 6 | 无线网络安全技术 | 完成无线网络安全配置 |
| 7 | 系统配置管理  50% | 云服务实训平台安装与应用 | 完成云服务实训平台搭建及传统服务的部署，保证云服务实训平台及其上层服务与网络设备协同工作 |
| 8 | 操作系统安装(Windows/Linux) | 完成操作系统的安装和配置 |
| 9 | 配置常用服务(Windows/Linux) | 能够熟练安装配置各类应用服务、系统管理和数据库安装调试  在服务器、数据库、网络部署完成后，安装部署真实的移动web应用，并达到最终访问测试 |
| 10 | 服务器虚拟化  服务器集群 | 掌握虚拟化技术，使用服务器集群技术 |
| 11 | 操作系统安全技术 | 掌握操作系统方面安全技术配置 |

基于竞赛保密性的考虑，竞赛详细评分细则结合竞赛试题由竞赛执委会和命题专家共同制定。

附：主要竞赛知识点和技能点

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **内容模块** | **具体内容** | **说明** |
| 1 | 网络基本配置 | 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GB50312-2007）检测、端口检测等 |
| 2 | IP地址划分实施 | VLSM、CIDR等 |
| 3 | 交换基本配置 | VLAN、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等 |
| 4 | 路由基本配置 | 静态、RIP、OSPF、BGP等路由协议、NTP、DHCP、TELNET、策略路由等 |
| 5 | 无线配置 | 设置、分配、接入、开通等 |
| 6 | 广域网配置 | PPP、NAT、NAPT等 |
| 7 | 服务器配置与管理 | 操作系统安装(Windows/Linux) | 能够熟练安装操作系统，并能对操作系统进行安全配置和应用管理 |
| 8 | 配置常用服务(Windows/Linux) | 能够根据企业的应用需求，熟练安装和配置AD、DNS、WEB、FTP、E-MAIL、DHCP、代理等常用服务并进行数据库配置与管理，并能实际运用。能够熟练掌握虚拟化技术完成特定环境配置；使用服务器集群技术来实现网络的负载均衡 |
| 9 | 云服务实训平台部署 | 在云服务实训平台配置资源模板、创建网络、创建卷、利用平台内置系统生成实例，使运行后实例可以接入网络工作 |
| 10 | 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 |
| 11 | 网络安全与网络优化 | 防火墙 | 能够在企业网络中部署防火墙，使用防火墙规则保护内网服务安全，在防火墙上实现路由、NAT转换、防DDOS攻击；实现包过滤、URL过滤、P2P流量控制等 |
| 12 | 网络优化 | 利用ACL、QOS、交换机虚拟化等配置，实现网络优化 |
| 13 | VPN技术 | 利用VPN实现远程安全接入和站点到站点的IPSEC VPN等 |
| 14 | 无线网络 | 配置无线网络WEP加密、MAC认证接入控制等；配置二层漫游、三层漫游、无线桥接（点对点)、负载均衡、无线桥接（点对多点），信道自动调整等 |

十一、奖项设置

（一）参赛选手奖励

赛项设参赛选手团体一、二、三等奖。以赛项实际参赛队（团体赛）总数为基数，一、二、三等奖获奖比例分别为10%、20%、30%（小数点后四舍五入）。

（二）指导教师奖励

各赛项获得一等奖的参赛队（团体赛）指导教师获“优秀指导教师奖”。

十二、技术规范

1. 教育教学标准

1. 职业素养

（1）具备计算机基础知识，能使用常用软件

（2）能安装与维护计算机系统

（3）具备网络相关知识，了解网络技术发展动态

（4）具备良好的人际交往、团队合作能力和服务意识

2. 专业知识和技能

（1）能使用网络施工常用设备和工具

（2）能进行网络布线施工

（3）能够组建局域网络

（4）能安装、配置桌面和服务器操作系统

（5）能管理和维护网络软、硬件

（6）会使用与维护数据库

（7）具有网络安全维护的能力

（8）能够建立与维护网站

1. 行业标准

|  |  |  |
| --- | --- | --- |
| **序号** | **标准号** | **中文标准名称** |
| 1 | GB50311-2007 | 综合布线系统工程设计规范 |
| 2 | GB50312-2007 | 综合布线系统工程验收规范 |
| 3 | GB50174-2008 | 电子信息系统机房设计规范 |
| 4 | GB21671-2008 | 基于以太网技术的局域网系统验收测评规范 |
| 5 | GB/T22239-2008 | 信息系统安全等级保护基本要求 |
| 6 | IEEE 802.11 | 无线局域网的介质访问控制协议CSMA/CA及其物理层技术规范 |

1. 职业技术标准

达到并超过中级计算机网络技术人员（国家职业资格四级）），接近高级计算机网络技术人员（国家职业资格三级）。

十三、建议使用的比赛器材、技术平台和场地要求

（一）网络设备竞赛器材

本次比赛使用各网络厂商通用网络设备竞赛器材，建议优先选择满足竞赛功能需要，且为业界先进、成熟、往届使用的设备。如以下网络设备代表为示例。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **设备名称** | **参数** | **数量** | **备注** |
| 1 | 路由器 | 4个10/100/1000Base-TX路由口，1个10/100Base-TX路由口，2个高速同/异步串口，4个接口卡插槽， 1个网络模块插槽，1个配置口，1个备份口 | 2 | 沿用往届设备 |
| 2 | 路由器线缆 | DB60(针)—1×DB34 DCE(孔)+1×DB34DTE(针)，V.35 1拖2混合型线缆 | 2 | 沿用往届设备 |
| 3 | 三层虚拟化交换机 | 24个千兆以太网电口+4个复用千兆SFP光口+4个10G SFP+光口  每台标配：  DAC-SFPX-3M VSF虚拟化连接套件 | 2 | 沿用往届设备 |
| 4 | 二层交换机 | 千兆以太网交换机，（24个千兆以太网电口+4个千兆SFP光口） | 1 | 沿用往届设备 |
| 5 | 多核防火墙 | 9个10/100/1000M以太网电口；1U标准机箱  每台标配：  USG-N3002-LIC 特征库升级许可 | 2 | 沿用往届设备 |
| 6 | 无线交换机 | 有线无线一体化智能控制器，4个千兆SFP光口，24个千兆PoE电口，全部电口支持最大30W （802.3at标准）供电，最大PoE供电功率370W | 1 | 沿用往届设备 |
| 7 | 无线接入点 | 室内802.11ac放装式无线AP，内置天线，2.4G/5G双频，整机4条空间流，整机最大速率1.167Gbps，支持802.11a/n/ac和802.11b/g/n同时工作，1个千兆口，支持USB 2.0口 | 1 | 沿用往届设备 |
| 8 | POE模块 | 10/100/1000Mbps单端口802.3at PoE模块，最高输出功率为30W | 1 | 沿用往届设备 |
| 9 | 云服务实训平台 | 软件提供统一的WEB管理界面，可以提供稳定，高速的云环境 | 1 | 沿用往届设备 |
| 10 | 网络布线工具 | 工具包含综合布线常用工具，压线钳，打线钳，测线仪，美工刀等等 | 1 | 沿用往届设备 |

2.竞赛用PC机

|  |  |  |  |
| --- | --- | --- | --- |
| **设备名称** | **设备需求描述** | **数量** | **备注** |
| PC机 | CPU 主频>=3.5GHZ, >=四核心 八线程  内存>=8G硬盘>=1T  支持硬件虚拟化 | 2 | 承办校提供 |

（二）软件技术平台

具体软件参数如下所示:

1. 微软 Windows 7 (64位中文版) 试用版；
2. 微软 Windows 10 (64位中文版) 试用版；
3. Centos 7.0（64位）；
4. WINRAR 5.21(中文版) 试用版；
5. 微软 Microsoft Office 2010(中文版) 试用版；
6. 微软 Windows Server 2008 R2(中文版) 试用版；
7. 微软 Windows Server 2012 R2(中文版) 试用版；
8. VMware workstation 12免费版；
9. SecureCRT；
10. Apache Tomcat 7.0.27；
11. JDK（Java Development Kit）1.7及以上；
12. 谷歌浏览器(Google Chrome)官方正式版。

（三）赛场环境要求

竞赛现场设置场内竞赛区、现场裁判工作区、技术支持区、场外互动区等。

竞赛工位内设有操作平台，每工位配备220V电源（带漏电保护装置），工位内的电缆线应符合安全要求。每个竞赛工位面积8-12m2，确保参赛队之间互不干扰，具备至少安排100支参赛队的竞赛场地。竞赛工位标明工位号和参赛设备号，并配备竞赛平台和技术工作要求的软、硬件。环境标准要求保证赛场采光(大于500lux)、照明通风良好、温度湿度适宜；为每支参赛队提供一套网络布线工具、5类非屏蔽双绞线20米、5类水晶头40个和一个垃圾箱，留有赛场观摩通道。

十四、安全保障

赛事安全是全国职业院校技能大赛一切工作顺利开展的先决条件，是本赛项筹备和运行工作必须考虑的核心问题。

（一）组织机构

赛项执委会组织专门机构负责赛区内赛项的安全工作，建立公安、消防、司法行政、交通、卫生、食品、质检等相关部门协调机制保证比赛安全，制定应急预案，及时处置突发事件。制定相应安全管理的规范、流程和突发事件应急预案，全过程保证比赛筹备和实施工作安全。

（二）赛项设计

1. 比赛内容涉及的器材、设备应符合国家有关安全规定。赛项专家组应充分考虑比赛内容和所用器材、耗材可能存在的危险因素，通过完善设计规避风险，采取有效防范措施保证选手备赛和比赛安全。危险提示和防范措施应在赛项技术文件中加以明确。

2. 赛项技术文件应包含国家（或行业）有关职业岗位安全的规范、条例和资格证书要求等内容。

3. 赛项执委会须在赛前对本赛项全体裁判员进行裁判培训和安全培训，对服务人员进行安全培训。源于实际生产过程的赛项，须根据《中华人民共和国劳动法》等法律法规，建立完善的安全事故防范制度，并在赛前对选手进行培训，避免发生人身伤害事故。

4. 赛项执委会须制定专门方案保证比赛命题、赛题保管和评判过程的安全。

（三）比赛环境

1. 环境安全保障

赛场组织与管理员应制定安保须知、安全隐患规避方法及突发事件预案，设立紧急疏散路线及通道等，确保比赛期间所有进入竞赛地点的车辆、人员需凭证入内；严禁携带易燃易爆物、管制刀具等危险品及比赛严令禁止的其他物品进入场地；对于紧急发生的拥挤、踩踏、地震、火灾等进行紧急有效的处置。

2. 信息安全保障

安装UPS：采用UPS防止现场因突然断电导致的系统数据丢失，额定功率：3KVA，后备时间：2小时，电池类型：输出电压：230V±5%V；市电采用双路供电。

3. 操作安全保障

赛前要对选手进行计算机、网络设备、工具等操作的安全培训，进行安全操作的宣讲，确保每个队员能够安全操作设备后方可进行比赛。裁判员在比赛前，宣读安全注意事项，强调用火、用电安全规则。

整个大赛过程邀请当地公安系统、卫生系统和保险系统协助支持。

参赛队：由各省市负责参赛选手旅途及竞赛过程中的安全保障。

4. 赛项执委会须在赛前组织专人对比赛现场、住宿场所和交通保障进行考察，并对安全工作提出明确要求。赛场的布置，赛场内的器材、设备，应符合国家有关安全规定。如有必要，也可进行赛场仿真模拟测试，以发现可能出现的问题。承办单位赛前须按照赛项执委会要求排除安全隐患。

5. 赛场周围要设立警戒线，防止无关人员进入发生意外事件。比赛现场内应参照相关职业岗位的要求为选手提供必要的劳动保护。在具有危险性的操作环节，裁判员要严防选手出现错误操作。

6. 承办单位应提供保证应急预案实施的条件。对于比赛内容涉及高空作业、可能有坠物、大用电量、易发生火灾等情况的赛项，必须明确制度和预案，并配备急救人员与设施。

7. 赛项执委会须会同承办单位制定开放赛场和体验区的人员疏导方案。赛场环境中存在人员密集、车流人流交错的区域，除了设置齐全的指示标志外，须增加引导人员，并开辟备用通道。

8. 大赛期间，赛项承办单位须在赛场管理的关键岗位，增加力量，建立安全管理日志。

9. 参赛选手进入赛位、赛事裁判工作人员进入工作场所，严禁携带通讯、照相摄录设备，禁止携带记录用具。如确有需要，由赛场统一配置、统一管理。赛项可根据需要配置安检设备对进入赛场重要部位的人员进行安检。

（四）生活条件

1. 比赛期间，原则上由赛事承办单位统一安排参赛选手和指导教师食宿。承办单位须尊重少数民族的信仰及文化，根据国家相关的民族政策，安排好少数民族选手和教师的饮食起居。

2. 比赛期间安排的住宿地应具有宾馆/住宿经营许可资质。以学校宿舍作为住宿地的，大赛期间的住宿、卫生、饮食安全等由赛项执委会和提供宿舍的学校共同负责。

3. 大赛期间有组织的参观和观摩活动的交通安全由赛区组委会负责。赛项执委会和承办单位须保证比赛期间选手、指导教师和裁判员、工作人员的交通安全。

4. 各赛项的安全管理，除了可以采取必要的安全隔离措施外，应严格遵守国家相关法律法规，保护个人隐私和人身自由。

（五）组队责任

1. 各省、自治区、直辖市和计划单列市在组织参赛队时，须安排为参赛选手购买大赛期间的人身意外伤害保险。

2. 各省、自治区、直辖市和计划单列市参赛队组成后，须制定相关管理制度，并对所有选手、指导教师进行安全教育。

3. 各参赛队领队须加强参赛人员的安全管理，实现与赛场安全管理的对接。

（六）应急处理

比赛期间发生意外事故，发现者应第一时间报告赛项执委会，同时采取措施避免事态扩大。赛项执委会应立即启动预案予以解决并向赛区执委会报告。出现重大安全问题的赛项可以停赛，是否停赛由赛区组委会决定。事后，赛区执委会应向大赛执委会报告详细情况。

（七）处罚措施

1. 赛项出现重大安全事故的，停止承办单位的赛项承办资格。

2. 因参赛队伍原因造成重大安全事故的，取消其参赛资格。

3. 参赛队伍有发生重大安全事故隐患，经赛场工作人员提示、警告无效的，可取消其继续比赛的资格。

4. 赛事工作人员违规的，按照相应的制度追究责任。情节恶劣并造成重大安全事故的，由司法机关追究相应法律责任。

十五、经费概算

具体包括五部分：

（一）设备支持

提供2019年中职组“网络搭建与应用”赛项的赛项主要专业器材，包括交换机、路由器、防火墙、无线交换机、接入点、云服务实训平台等竞赛设备的使用权。

（二）环境支持

提供达到赛项比赛要求所需的PC机、网络布线工具及辅助耗材，按照竞赛要求部署比赛环境。

（三）经费支持

用于大赛宣传、培训、交通、食宿、场地租赁、命题、专家指导、裁判、资源转化等相关费用支出。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **项目阶段** | **资金用途** | | **费用（万）** |
| 1 | 方案和比赛规程论证 | 调研费、论证会议、差旅、专家费 | | 6 |
| 2 | 赛前准备 | 模拟题和试题开发专家费  （10名） | | 5 |
| 赛项说明  及培训 | 现场1次 | 2 |
| 网络直播 | 2 |
| 3 | 比赛现场 | 场内活动 | 比赛用辅助耗材 | 1 |
| 设备运输  安装调试 | 13 |
| 工作人员服务保障 | 3 |
| 出题，监考和裁判 | 9 |
| 获奖选手奖品 | 6 |
| 场外活动 | 技术展示体验 | 2 |
| 教师学生论坛 |
| 赛事宣传报道 | 3 |
| 4 | 比赛总结  资源转化费 | 总结及资源转化研讨  形成成果推广 | | 6 |
| 5 | 机动费用 | 临时突发事件 | | 2 |
| 小计(单位：万元) | | | | 60 |

（四）技术支持

提供一系列比赛器材技术和培训支持，为赛项的调研、研讨、论证工作提供技术支持，负责比赛设备现场安装调试、比赛现场临时突发事件处理等技术支持，及赛前比赛器材培训支持等一系列相关工作。

（五）其他支持

根据大赛执委会的工作安排，承接一些力所能及的公益工作。

十六、比赛组织与管理

（一）赛项组织机构。

参照《全国职业院校技能大赛组织机构与职能分工》完成赛项组织机构的组织工作。赛项组织机构主要由赛项牵头单位、赛项执委会、赛项专家组、赛项承办单位、赛项合作企业等组成。

1．赛项牵头单位。

中国职业技术教育学会信息化工作委员会，主要负责筹备赛项、主持成立赛项执委会，并按照大赛执委会的要求，维护专家库、裁判库；负责试题库的更新和维护；负责成立赛项执委会完成赛项的组织设计、赛题设计、赛项执行等活动。

2．赛项执委会。

赛项执行委员会全面负责本赛项的筹备与实施工作，接受大赛执委会领导，接受赛项所在分赛区执委会的协调和指导。

赛项执委会的主要职责包括：领导、组织和协调赛项专家工作组和组织保障工作组的工作，编制赛项经费预算，管理赛项经费使用，选荐赛项专家组人员及裁判与仲裁人员，牵头负责赛项资源转化、安全保障等工作。

3．赛项专家组。

全国职业院校技能大赛赛项专家工作组在赛项执委会领导下开展工作，负责本赛项技术文件编撰、赛题设计、赛场设计、设备拟定、赛事咨询、竞赛成绩分析和技术点评、赛事成果转化、赛项裁判人员培训、赛项说明会组织等竞赛技术工作；同时负责赛项展示体验及宣传方案设计。

4．赛项保障工作组。

主要由赛项承办院校担任。在赛项执委会领导下，负责承办赛项的具体保障实施工作，主要职责包括：按照赛项技术方案落实比赛场地及基础设施，做好赛项宣传，组织开展同期活动，接待参赛人员，负责比赛过程文件存档，做好赛务人员及服务志愿者的组织，赛场秩序维持及安全保障，赛后搜集整理大赛影像文字资料上报大赛执委会等工作。参与赛项经费预算，管理赛项经费账户，执行赛项预算支出，委托会计师事务所进行赛项审计。

5．赛项合作企业。

由赛项合作企业负责设备支持、资金支持和技术保障等，按照《全国职业院校技能大赛企业合作管理办法》规范自身的赛项保障和服务活动，不得从事任何有损大赛形象的行为。

（二）赛场管理。

参照《全国职业院校技能大赛赛项设备与设施管理办法》完成赛场环境的部署和管理工作。

1．赛场条件。

（1）赛场布置，贯彻赛场集中，赛位独立的原则。选手竞赛单元相对独立，确保选手独立开展比赛，不受外界影响；赛位集中布置，保证竞赛氛围。

（2）卫生间、医疗、维修服务、生活补给站和垃圾分类回收点都在警戒线范围内，以确保大赛在相对安全的环境内进行。

（3）设置安全通道和警戒线，确保进入赛场的大赛参观、采访、视察的人员限定在安全区域内活动，以保证大赛安全有序进行。

2．赛项保障。

（1）建立完善的赛项保障组织管理机制，做到各竞赛单元均有专人负责指挥和协调，确保大赛有序进行。

（2）设置生活保障组，为竞赛选手与裁判提供相应的生活服务和后勤保障。

（3）设置技术保障组，为竞赛设备、软件与竞赛设施提供保养、维修等服务，保障设备的完好性和正常使用，保障设备配件与操作工具的及时供应。

（4）设置医疗保障服务站，提供可能发生的急救、伤口处理等应急服务。

（5）设置外围安保组，对赛场核心区域的外围进行警戒与引导服务。

3．赛场布置。

（1）赛场应进行周密设计，绘制满足赛事管理、引导、指示要求的平面图。竞赛举行期间，应在竞赛场所、人员密集的地方张贴。

（2）赛场平面图上应标明安全出口、消防通道、警戒区、紧急事件发生时的疏散通道。

（3） 赛场的标注、标识应进行统一设计，按规定使用大赛的标注、标识。赛场各功能区域、赛位等应具有清晰的标注与标识。

（4）赛位上应张贴各种设备的安全文明生产操作规程。

4．参赛院校选手和教师的管理。

赛事承办院校统一安排参赛选手和指导教师食宿。承办院校须尊重少数民族参赛人员的宗教信仰及文化习俗，根据国家相关的民族、宗教政策安排好少数民族参赛选手和教师的饮食起居。

（三）赛项监督与仲裁管理

参照《全国职业院校技能大赛赛项监督与仲裁管理办法》的规定，完成赛项监督与仲裁管理管理工作。

1. 赛项监督。

（1）监督组在大赛执委会领导下，对指定赛区、赛项执委会的竞赛筹备与组织工作实施全程现场监督。监督工作实行组长负责制。

（2）监督组的监督内容包括赛项竞赛场地和设施的部署、廉洁办赛、选手抽签加密、裁判培训、竞赛组织、成绩评判及成绩复核与发布、申诉仲裁等。

（3）监督组不参与具体赛事组织活动及裁判工作。

（4）监督组在工作期间应严格履行监督工作职责。

（5）对竞赛过程中违规现象，应及时向赛项执委会提出改正建议，同时留取监督过程资料。赛事结束后，认真填写《监督工作手册》并直接递交大赛执委会办公室存档。

2.申诉与仲裁。

（1）各参赛队对不符合大赛和赛项规程规定的仪器、设备、工装、材料、物件、计算机软硬件、竞赛使用工具、用品，竞赛执裁、赛场管理、竞赛成绩，以及工作人员的不规范行为等，可向赛项仲裁组提出申诉。申诉主体为参赛队领队。

（2）仲裁人员的姓名、联系方式应该在竞赛期间向参赛队和工作人员公示，确保信息畅通并同时接受大众监督。

（3）申诉启动时，参赛队向赛项仲裁工作组递交领队亲笔签字同意的书面报告。书面报告应对申诉事件的现象、发生时间、涉及人员、申诉依据等进行充分、实事求是的叙述。非书面申诉不予受理。

（4）提出申诉的时间应在比赛结束后（选手赛场比赛内容全部完成）2小时内。超过时效不予受理。

（5）赛项仲裁工作组在接到申诉报告后的2小时内组织复议，并及时将复议结果以书面形式告知申诉方。申诉方对复议结果仍有异议，可由省（市）领队向赛区仲裁委员会提出申诉。赛区仲裁委员会的仲裁结果为最终结果。

（6）申诉方不得以任何理由拒绝接收仲裁结果，不得以任何理由采取过激行为扰乱赛场秩序。仲裁结果由申诉人签收，不能代收，如在约定时间和地点申诉人离开，视为自行放弃申诉。

（7）申诉方可随时提出放弃申诉。

十七、教学资源转化建设方案

依照《全国职业院校技能大赛赛项资源转化工作办法》的有关要求，赛项资源转方案按要求与规程同时公布；于赛后30日内向大赛执委会办公室提交资源转化实施方案，作为十一年的老赛项会在三个月完成新资源的补充与完善，半年内完成全部资源的转化工作。

（一）竞赛过程中获得的主要资源

1．竞赛样题、试题库；

2．竞赛赛题的评分标准；

3．考核环境描述；

4．竞赛过程音视频记录；

5、评委、裁判、专家点评和技术分析报告；

6．优秀选手、指导教师访谈。

（二）资源转化基本方案与呈现形式

资源转化成果按照行业标准、契合课程标准、突出技能特色、展现竞赛优势，形成满足职业教育教学需求、体现先进教学模式、反映职业教育先进水平的共享性职业教育教学资源。资源转化成果包含基本资源和拓展资源，充分体现本赛项技能考核特点：

资源转化成果应包含基本资源和拓展资源。

1. 基本资源

基本资源按照风采展示、技能概要、教学资源三大模块设置。

（1）风采展示。赛后即时制作时长15分钟左右的赛项宣传片，以及时长10分钟左右的获奖代表队（选手）的风采展示片。供专业媒体进行宣传播放。

（2）技能概要。包括技能介绍、技能操作要点、评价指标等。

（3）教学资源。教学资源充分涵盖赛项内容。包括教学方案、训练 指导、作业/任务、实验/实训/实习资源等，其呈现形式主要是演示文稿、图片、操作流程演示视频、动画及相关微课程、微资源等。

2. 拓展资源

拓展资源是指反映技能特色、可应用于各教学与训练环节、支持技能教学和学习过程的较为成熟的多样性辅助资源。

（三）资源的技术标准

资源转化成果以文本文档、演示文稿、视频文件、Flash文件、图形/图像素材和网页型资源等，技术标准符合《全国职业院校技能大赛资源转化工作办法》的要求。

（四）资源的提交方式与版权

赛项资源转化成果的版权由技能大赛执委会和赛项执委会共享。

（五）资源的使用与管理

资源转化成果的使用与管理由大赛执委会统一使用与管理，会同赛项承办单位、赛项有关专家，联系出版社编辑出版有关赛项试题库、岗位典型操作流程等精品资源。

（六）资源转化项目工作进程表

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **资源名称** | | | **表现形式** | **资源数量** | **资源要求** | **完成时间** | **实施人员** |
| 基 本 资 源 | 风采 展示 | 赛项宣传片 | 视频 | 1 | 15 分钟  以上 | 赛后5日 | 承办校 |
| 风采展示片 | 视频 | 1 | 10 分钟  以上 | 赛后5日 | 承办校 |
| 技能 概要 | 技能介绍 | 文本 | 1 | 补充完善 | 赛后60日 | 专家组 |
| 训练大纲 | 文本 | 1 | 补充完善 | 赛后60日 | 专家组 |
| 评价指标 | 文本 | 1 | 补充完善 | 赛后60日 | 专家组 |
| 教学 资源 | 专业教材 | 教材 | 1本以上 | 电子教材  补充完善  定期再版 | 赛后90日 | 专家组  技术支持单位 |
| 技能训练  指导书 | 教材 | 1本以上 | 电子教材  补充完善  定期再版 | 赛后90日 | 专家组  技术支持单位 |
| 认证培训  网络工程师  高级网络工程师 | 课程 | 各1套 | 教材、文档、图片、视频等，  补充完善 | 赛后90日 | 技术支持单位 |
| 拓 展 资 源 | 案例集 | | 文本 | 1套 | 教材、文档、图片、视频等，  补充完善 | 赛后90日 | 专家组  技术支持单位 |
| 仿真微课 | | 资源库 | 1套 | 云微课平台  补充完善 | 赛后90日 | 专家组  技术支持单位 |
| 优秀选手访谈 | | 视频 | 1 | 结合19年比赛补充完善 | 赛后90日 | 承办校 |

（七）资源转化说明

1.计算机网络技术专业系列教材。依托大赛，开发一套融入大赛思想的，体现“新设备、新技术、新标准”的实用型系列教材。

2.计算机网络技能训练指导书。系统梳理计算机网络技术专业的岗位需求、核心知识点和能力点及历年竞赛考核内容与评分要点。

3. 认证培训

网络工程师

适用于需要了解网络产品及应用解决方案的人员、中小型企业的网络管理员、网络项目规划设计人员、工程技术人员。

高级网络工程师

适用于需要从事大中型网络项目规划、实施和维护的工程技术人员、需要进一步提升多层交换技术以适应当前园区网高速数据吞吐率和稳定性技术的工程师、需要进一步提升路由技术以适应当前企业级广域网要求的工程师。

4.计算机网络应用赛项案例集。将2010年—2018年国赛及各省赛的竞赛内容进行分析汇总，形成行业应用案例，从而使赛题中的行业应用成为日常教学内容的载体。

5.仿真实训微课的制作。在2014年研发搭建的“云微课平台”和 “在线交互式仿真实训课件”的基础上补充完善新资源。

十八、筹备工作进度时间表

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **筹备阶段** | **内　容** | **时间安排** |
| 1 | 申报、立项 | 赛项设计专家研讨会，完成赛项申报方案 | 2018年8月 |
| 确定赛项后，成立赛项执委会、专家组 | 2018年11月 |
| 2 | 赛前准备 | 赛项专家会议3-5轮次会议，确定赛项规程、样题、赛项技术方案、赛场方案、体验环节设计方案、开放方案、宣传方案、教学资源转化方案、赛事安全规章、突发事件应急预案等 | 2018年11月  ～2019年1月 |
| 确定分赛区及承办校 | 2019年2月 |
| 全国赛项说明会 | 2019年4月 |
| 命题专家组会议，赛题开发、确定竞赛题库 | 2019年4月 |
| 赛项预报名及报名完成 | 2019年4月 |
| 3 | 比赛阶段 | 比赛设备安装、调试，赛场布置、同期技术展示、体验和活动现场布置；赛项指南印刷、选手服装制作 | 2019年5月 |
| 专家组题库审核，确定评分标准及抽题 |
| 成立裁判组、仲裁组、监督组；培训并验收赛场 |
| 正式比赛、同期技术展示、体验和活动举办；竞赛成绩提交、竞赛过程文档提交、教学资源转化成果与赛项总结 |

十九、裁判人员建议

赛项所需现场裁判和评分裁判在能遵守《全国职业院校技能大赛专家和裁判工作管理办法》的前提下，参照有关要求，竞赛裁判组由裁判长、检录裁判、加密裁判、现场裁判、评分裁判组成。其中，裁判长由赛项执委会推荐、赛区执委会确认；加密裁判、检录裁判由赛项承办校邀请校外专业教师担任；赛前在赛项裁判员库中随机抽取既定数量的现场裁判和评分裁判。

赛项所需现场裁判和评分裁判的具体要求如下：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **专业技术方向** | **知识能力要求** | **执裁、教学、工作经历** | **专业技术职称**  **（职业资格等级）** | **人数** |
| 1 | 网络设备调试与管理 | 熟悉综合布线和机房；  熟悉交换、路由方面的知识，如VLAN、ACL、VRRP、STP、OSPF等网络配置，具备分析、故障排错的能力；  有知名网络厂商认证资质优先。 | 具有相关专业教学经验或者工作经验、且具有电子信息类省级执裁经验 | 中级及以上职称 | 12 |
| 2 | 网络系统管理 | 具有虚拟化  平台下的工作经验；  熟悉windows 2003 server、windows 2008 server、windows 2012 server、linux系统；  能完成存储实施、管理和运维；  有相关厂商认证资质优先。 | 具有相关专业教学经验或者工作经验、且具有电子信息类省级执裁经验 | 中级及以上职称 | 13 |
| 3 | 网络安全 | 熟悉安全服务工作，包括漏洞扫描、渗透测试、风险评估、安全评估、安全培训、代码审计、应急响应等；  熟悉各种网络安全产品；  熟悉数据库、操作系统，有数据库、操作系统。 | 2 |
| 4 | 云计算 | 能掌握云平台系统的基本架构；掌握云产品与服务的特点；能创建ECS并部署网站与应用，能使用OSS存储文件，能使用RDS进行数据库操作，会配置SLB、云盾及云监控。 | 具有相关专业教学经验或者工作经验、且具有电子信息类省级执裁经验 | 中级及以上职称 | 2 |
| 裁判总人数 | 29 | | | | |  |  |

二十、赛题公开承诺

承诺保证于开赛1个月前在大赛网络信息发布平台上（www.chinaskills-jsw.org)公开全部赛题。

二十一、其他

（二）同期活动

可同期举办包括针对学生、带队教师的活动、校企合作论坛、新技术展示、媒体宣传等。

（三）往年赛项回顾

2015年赛项回顾



2016年赛项回顾



2017年赛项回顾



2018年赛项回顾

****

**附件1**

**2019年全国职业院校技能大赛**

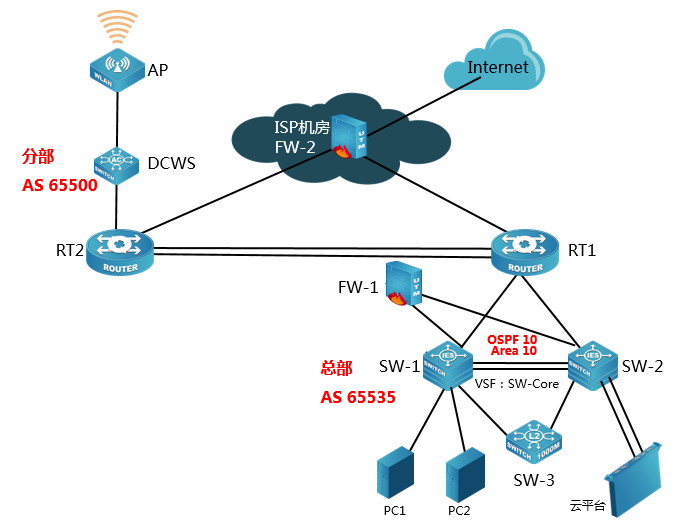
**网络搭建与应用竞赛**

**（总分1000分）（样题）**

|  |
| --- |
|  |

**《主要网络环境》**

### 拓扑结构图

****

### 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 | G0/5 | FW-2 | E0/6 |
| RT1 | S0/1 | RT2 | S0/2 |
| RT1 | S0/2 | RT2 | S0/1 |
| SW-1 | E1/0/26 | SW-2 | E1/0/27 |
| SW-1 | E1/0/28 | SW-2 | E1/0/25 |
| SW-1 | E1/0/23 | SW-3 | E1/0/23 |
| SW-2 | E1/0/23 | SW-3 | E1/0/24 |
| SW-1 | E1/0/22 | FW-1 | E0/5 |
| SW-2 | E1/0/22 | FW-1 | E0/3 |
| SW-1 | E1/0/21 | RT1 | G0/3 |
| SW-2 | E1/0/21 | RT1 | G0/4 |
| FW-2 | E0/4 | Internet |  |
| RT2 | G0/5 | FW-2 | E0/1 |
| RT2 | G0/3 | DCWS | E1/0/10 |
| DCWS | E1/0/6 | AP |  |
| SW-1 | E1/0/5 | PC1 | NIC |
| SW-1 | E1/0/6 | PC2 | NIC |
| SW-2 | E1/0/5 | 云服务实训平台 | 管理口 |
| SW-2 | E1/0/6 | 云服务实训平台 | 业务口 |

### 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 | RT1 | Loopback1 | 10.80.254.2/32 |
| G 0/3 | 10.80.255.10/30 |
| G 0/4 | 10.80.255.14/30 |
| G 0/5 | 10.80.255.25/30 |
| S 0/1-2 | 10.80.255.21/30 |
| Tunnel 1 | 10.80.255.17/30 |
| RT2 | G 0/5 | 10.80.255.30/30 |
| G0/3.10（VLAN10） | 172.17.10.254/24 |
| G0/3.20（VLAN20） | 172.17.20.254/24 |
| G0/3.100（VLAN100） | 172.17.101.254/23 |
| S 0/1-2 | 10.80.255.22/30 |
| Tunnel 1 | 10.80.255.18/30 |
| 三层交换机 | SW-Core | Loopback 1 | 10.80.254.1/32 |
| VLAN10 SVI | 10.80.10.254/24 |
| VLAN20 SVI | 10.80.20.254/24 |
| VLAN30 SVI | 10.80.30.254/24 |
| VLAN40 SVI | 10.80.40.254/24 |
| VLAN50 SVI | 10.80.50.254/24 |
| VLAN60 SVI | 10.80.60.254/24 |
| VLAN70 SVI | 10.80.70.254/24 |
| VLAN80 SVI | 10.80.80.254/24 |
| VLAN90 SVI | 10.80.90.254/24 |
| VLAN100 SVI | 192.168.100.1/24 |
| VLAN200 SVI | 10.80.200.254/24 |
| VLAN1000 SVI | 10.80.255.1/30 |
| VLAN1001 SVI | 10.80.255.5/30 |
| VLAN1002 SVI | 10.80.255.9/30 |
| VLAN1003 SVI | 10.80.255.13/30 |
| 防火墙1 | FW-1 | Eth0/5、3 | 10.80.255.2/30（trust安全域） |
| Eth0/5、3 | 10.80.255.6/30（untrust安全域） |
| 防火墙2 | FW-2 | Eth0/6 | 10.80.255.26/30（trust安全域） |
| Eth0/1 | 10.80.255.29/30（DMZ安全域） |
| Eth0/4 | 202.99.192.1/28（untrust安全域），对端地址：202.99.192.12/28 |
| 二层交换机 | SW-3 | VLAN200 SVI | 10.80.200.1/24 |

### 表3.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**  **服**  **务**  **实**  **训**  **平**  **台** | 云主机1 | dc.skillschina.com | 域控制器  DNS服务器  CA证书服务器 | Windows Server 2012 R2 | 10.80.60.xx/24 |
| 云主机2 | dfs.skillschina.com | 存储服务器NFS服务器  DFS服务器 | Windows Server 2012 R2 | 10.80.60.xx/24  10.80.70.xx/24 |
| 云主机3 | bacp.skillschina.com | 辅助DNS服务器 | Windows Server 2012 R2 | 10.80.60.xx/24 |
| 云主机4 | www1.skillschina.com | WEB服务器  故障转移集群服务 | Windows Server 2008 R2 | 10.80.60.xx/24  10.80.70.xx/24  10.80.80.xx/24 |
| 云主机5 | www2.skillschina.com | WEB服务器  故障转移集群服务 | Windows Server 2008 R2 | 10.80.60.xx/24  10.80.70.xx/24  10.80.80.xx/24 |
| 云主机6 | ftp.skillschina.com | FTPS服务器  DFS服务器 | Windows Server 2008 R2 | 10.80.60.xx/24 |
| 云主机7 | win7.skillschina.com | Client | Windows 7 | 10.80.60.xx/24 |
| 云主机8 | mail.netdj.net | MAIL服务器  NIS服务器 | Centos 6.5 | 10.80.90.xx/24 |
| 云主机9 | ftp.netdj.net | FTPS服务器  SAMBA服务器 | Centos 6.5 | 10.80.90.xx/24 |
| 云主机10 | dns.netdj.net | 域名服务器  代理服务器 | Centos 6.5 | 10.80.90.xx/24 |
| 云主机11 | www.netdj.net | WEB服务器  数据库服务器 | Centos 6.5 | 10.80.90.xx/24 |
| **PC1**  （IP为10.80.60.0/24网段） | 服务器1 | dcro.skillschina.com | RODC服务器 | Windows Server 2008 R2 | 10.80.60.221/24 |
| 服务器2 | Server2.bj.skillschina.com | 子域控制器  卷影副本 | Windows Server 2008 R2 | 10.80.60.222/24 |
| 服务器3 | Server3 | DHCP服务器  WDS服务器 | Windows Server 2012 R2 | 10.80.60.223/24 |
| 服务器4 | core.skillschina.com | CORE系统 | Windows Server Core 2012 R2 | 10.80.60.224/24 |
| **PC2**  （IP为10.80.60.0/24网段） | 服务器5 | pxe.netskills.net | PXE服务器 | Centos 6.5 | 10.80.60.225/24 |
| 服务器6 | tcat.netskills.net | Tomcat服务器 | Centos 6.5 | 10.80.60.226/24 |
| 服务器7 | mail.netskills.net | 数据库服务器  MAIL服务器 | Centos 7.0 | 10.80.60.227/24 |
| 服务器8 | www.netskills.net | DNS服务器  WEB服务器 | Centos 7.0 | 10.80.60.228/24 |

**表4.云服务实训平台网络信息表**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 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 |
| Vlan60 | 60 | 是 | Vlan60-subnet | 10.80.60.0/24 | 10.80.60.254 | 是 | 10.80.60.100,10.80.60.200 |
| Vlan70 | 70 | 是 | Vlan70-subnet | 10.80.70.0/24 | 10.80.70.254 | 是 | 10.80.70.100,10.80.70.200 |
| Vlan80 | 80 | 是 | Vlan80-subnet | 10.80.80.0/24 | 10.80.80.254 | 是 | 10.80.80.100,10.80.80.200 |
| Vlan90 | 90 | 是 | Vlan90-subnet | 10.80.90.0/24 | 10.80.90.254 | 是 | 10.80.90.100,10.80.90.200 |

**表5.虚拟主机信息表**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **虚拟主机名称** | **镜像模板 (源)** | **云主机类型(flavor)** | **VCPU 数量** | **内存、硬盘信息** | **网络名称** | **备注** |
| 云主机1 | win2012 | window-470 | 2 | 4G、70G | Vlan60 |  |
| 云主机2 | win2012 | window-270 | 2 | 2G、70G | Vlan60 Vlan70 | 连接卷hd1-hd3 |
| 云主机3 | win2012 | window-470 | 2 | 4G、70G | Vlan60 | 加入域 |
| 云主机4 | win2008 | window-455 | 2 | 4G、55G | Vlan60 Vlan70 Vlan80 | 加入域 |
| 云主机5 | win2008 | window-280 | 2 | 2G、80G | Vlan60 Vlan70 Vlan80 | 加入域 |
| 云主机6 | win2008 | window-245 | 2 | 2G、45G | Vlan60 | 加入域，连接卷hd4-hd5 |
| 云主机7 | win7 | window7-165 | 2 | 1G、65G | Vlan60 | 加入域 |
| 云主机8 | centos6.5-mini | linux-160 | 1 | 1G、60G | Vlan90 |  |
| 云主机9 | centos6.5-mini | linux-175 | 1 | 1G、75G | Vlan90 |  |
| 云主机10 | centos6.5-mini | linux-145 | 1 | 1G、45G | Vlan90 |  |
| 云主机11 | centos6.5-mini | linux-145 | 1 | 1G、45G | Vlan90 |  |

**表6.云主机和服务器密码表**

|  |  |
| --- | --- |
| 云主机和服务器密码 | 2018NeTw@rk（注意区分大小写） |

注：需把云主机的默认密码改为表6.云主机和服务器密码表要求的密码

**技能要求**

一、竞赛内容分布

“网络搭建与应用”竞赛共分二个部分，其中：

第一部分：网络搭建及安全部署项目

第二部分：服务器配置及应用项目

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）本试卷共有两个部分。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。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。

（5）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。

（6）禁止在纸质资料上填写与竞赛无关的标记，如违反规定，可视为0分。

（7）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。

## 项目简介:

某集团公司原在北京建立了总部，后在深圳建立了分部。总部设有研发、行政、营销、财务、信息技术 5个部门，统一进行IP及业务资源的规划和分配，网络采用RIP、OSPF、BGP多种路由协议。

公司规模在2018年快速发展，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，集团决定建立自己的小型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。

集团总部及深圳分部的网络结构如不同网络环境图拓扑所示。

其中一台S4600交换机编号为SW-3，用于实现终端高速接入；两台CS6200交换机VSF虚拟化后编号为SW-Core，作为总部的核心交换机；一台DCFW-1800作为总部的内网防火墙；另一台DCFW-1800作为总部&分部的外网防火墙，存放于ISP机房；一台DCR-2655路由器编号为RT1，作为总部的核心路由器；另一台DCR-2655路由器编号为RT2，作为分部路由器；一台DCWS-6028作为分部机构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配合实现分部无线覆盖。

### 网络搭建及安全部署项目

（500分）

【说明】

1. 设备console线有两条。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. 设备配置完毕后，保存最新的设备配置。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，截图有截图的简要说明，否则按无效内容处理；所有需要提交的文档均放置在PC1桌面的“比赛文档\_X”（X为组号）文件夹中。

保存文档方式分为两种：

* 交换机和路由器要把show running-config的配置保存在PC1桌面的相应文档中，文档命名规则为：设备名称.docx,例如：RT1路由器文件命名为：RT1.docx，然后放入到PC1桌面上“比赛文档\_X”文件夹中；
* 防火墙等截图方式的设备，把截图的图片放到同一word文档中，文档命名规则为：设备名称.docx,例如：防火墙FW-1文件命名为：FW-1.docx, 保存后放入到PC1桌面上“比赛文档\_X”文件夹中。

1. **网络布线与基础配置**

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，机柜上已经安装好的信息点底盒代表为总公司数据中心水平配线区配线点101；机柜右侧布线面板，机柜上已经安装好的信息点底盒代表为总公司数据中心水平配线区配线点102。

（2） 机柜上配线架（1-12号端口）模拟代表总部数据中心主配线区配线点；机柜上配线架（13-24号端口）模拟代表分公司二数据中心主配线区配线点。

（3） 数据中心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。

数据中心主配线区配线点与工作区配线点连线对应关系表

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **信息点编号** | **计算机编号** | **底盒编号** | **信息点编号** | **配线架端口编号** |
| 1 | PC1-101-1 | PC1 | 101 | 1 | 01 |
| 2 | PC2-102-1 | PC2 | 102 | 1 | 02 |

1. 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“数据中心主配线区配线点与工作区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“数据中心主配线区配线点与工作区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。

2. 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“数据中心主配线区配线点与工作区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）。

1. **交换配置与调试**
2. 总部两台核心交换机通过VSF物理端口连接起来形成一台虚拟的逻辑设备，用户对这台虚拟设备进行管理，来实现对虚拟设备中所有物理设备的管理。两台设备之间建立一个vsf port-group，vsf port-group编号都为1，每个vsf port-group绑定两个千兆光端口，SW-1的成员编号为1，SW-2的成员编号为2，正常情况下SW-2负责管理整个VSF，采用LACP MAD分裂检测，配置快速检测模式为short，配置VSF链路down延迟上报时间为2s、VSF分裂后桥MAC地址保留时间为6分钟；
3. 为了减少广播，需要根据题目要求规划并配置VLAN。具体要求如下：
4. 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；
5. 尽可能加大总部接入交换机与核心交换机之间的带宽。

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** | **VLAN名称** | **端口** | **说明** |
| SW-3 | VLAN10 | YF | E1/0/6至E1/0/7 | 研发 |
| VLAN20 | XZ | E1/0/8至E1/0/9 | 行政 |
| VLAN30 | YX | E1/0/10至E1/0/12 | 营销 |
| VLAN40 | CW | E1/0/13至E1/0/15 | 财务 |
| VLAN50 | XXJS | E1/0/16至E1/0/18 | 信息技术 |
| VLAN200 | GL |  | 网络管理 |

1. SW-3上实现营销、财务各自部门业务内部终端相互二层隔离，行政、信息技术各自部门业务内部启用环路检测，环路检测的时间间隔为10s，发现环路以后阻塞该端口，恢复时间为30分钟；
2. 营销、行政、财务各自部门业务内部终端、采用自动获取IP地址，总部RT1作为DHCP服务器进行IP地址分配，地址池主机位范围为100-200；为了防止营销、行政部门用户私设DHCP服务器，使用相应技术进行安全防范，当检测到私设DHCP服务器时，自动关闭该端口；
3. 要求尽可能加大总部核心交换机SW-Core与FW-1之间的带宽，采用PBR方式实现总部与分部互访业务都经过FW-1进行安全防护；
4. 2017年勒索蠕虫病毒席卷全球，爆发了堪称史上最大规模的网络攻击，通过对总部核心交换机SW-Core 所有业务VLAN下配置访问控制策略实现双向安全防护；
5. 总部部署了一套网管系统实现对核心交换机SW-Core所有交换机进行管理，网管系统IP为：10.XX.200.50（XX根据赛卷地址变化而变化），读团体值为：2018Net\_R，版本为V2C，交换机SW-Core Trap信息实时上报网管，当MAC地址发生变化时，也要立即通知网管发生的变化，每35s发送一次。
6. **路由配置与调试**

因历史原因，总部使用RIP、OSPF、BGP多协议组网。RT1、SW-Core之间规划使用OSPF协议; RT1、FW-2、RT2之间规划使用RIP协议；RT1、RT2之间规划使用BGP协议。

1. 总部RT1、SW-Core之间规划使用OSPF协议，进程号为10，Area10，NSSA区域，启用区域MD5验证，验证密钥为：Net2018，调整接口的网络类型加快邻居关系收敛，为了管理方便，需要发布Loopback地址，并尽量在OSPF域中发布；
2. 总部RT1、ISP机房FW-2、分部RT2之间规划使用RIP协议，版本号为RIP-2，取消自动聚合，在分部RT2上通告SSID FenZhiXX-Internet业务路由；
3. RT1、RT2之间使用与FW-2的接口互联地址建立GRE隧道，再使用IPSEC技术对GRE隧道进行保护，使用IKE协商IPSec安全联盟、交换IPSec密钥，两端加密访问列表名称都为ipsecacl，这样有了IPSec，数据在通过运营商网络传输时，就不用担心被监视、篡改和伪造；
4. 总部RT1、分部RT2之间规划使用BGP协议，通过接口互联地址建立两对E-BGP邻居关系，其中一对邻居关系建立采用GRE Tunnel IP地址，同时在分部RT2上通告SSID FenZhiXX-IN业务路由；
5. 总部RT1配置路由重分布、路由控制策略，实现如下要求：
6. 将BGP协议与OSPF协议相互引入；
7. 借助黑洞路由，使RIP学习到总部业务的路由；
8. 要求分部RT2禁止学习到总部研发的明细路由信息。
9. **广域网配置**
10. 总部RT1与分部RT2间、总部RT1、分部RT2与ISP机房FW-2间都属于租用运营商专线链路，其中总部RT1-分部RT2间所租用串行链路默认通过S0/1接口转发数据，在RT1上实现当S0/1接口的实际流量超过70%，S0/2接口才会进入到工作状态，当S0/1接口的实际流量减小至40%，S0/2接口进入关闭状态，当S0/1接口故障6S后，S0/2接口才会进入到工作状态，避免主接口频繁up/down，造成网络震荡；
11. 为了提高带宽利用率，采用MPPC压缩协议对总部RT1-分部RT2间所租用串行链路数据进行压缩传输。
12. **无线配置**
13. 无线控制器DCWS二层与分部RT2互通，所有业务网关位于分部RT2上， DCWS配置VLAN100为AP管理VLAN，VLAN10、20为业务VLAN，不允许使用DHCP进行地址分配，使用第一个地址作为AC管理地址、第二个地址作为AP管理地址，本地转发，AP二层手工注册，启用密码认证，验证密钥为： Net\_2018 ；
14. 设置两个SSID FenZhiXX-IN、FenZhiXX-Internet，其中FenZhiXX中的XX为组号，具体要求如下：
15. SSID FenZhiXX-IN：访问总部业务，VLAN10，采用WAPI预共享密钥鉴别方式，配置密钥为Net12345678,信号隐藏；
16. SSIDFenZhiXX-Internet：访问Internet，VLAN20，采用开放接入；
17. 配置所有无线接入用户相互隔离，Network模式下限制SSID FenZhiXX-IN每天早上0点到6点禁止终端接入，开启SSID FenZhiXX-Internet ARP抑制功能。
18. **安全策略配置**
19. FW-1采用静态路由协议，根据题目要求配置相应的安全域、基于明细网段的安全访问策略；FW-2采用RIP协议，根据题目要求配置相应的安全域，配置安全策略禁止总部所有业务与分部SSID FenZhiXX-Internet业务双向访问；
20. 针对FW-1、FW-2 untrust区域开启所有攻击防护，发现攻击时丢弃；
21. 总部与分部统一通过ISP机房FW-2访问外网，配置PAT，实现总部行政与信息技术业务、分部SSID FenZhiXX-Internet业务访问外网；
22. FW-2实现对公司所有用户访问网址中含有“游戏”、“购物”关键字网站的过滤，对试图访问及搜索的行为进行记录；阻止在社区论坛、社会生活类网站发布含有关键字“舆论”的信息，并记录日志；并将上述日志发送至网管系统方便统一管理、审计。
23. **业务选路配置**

考虑到从分部到总部有两条广域网链路，且其带宽不一样，所以规划正常情况下总部RT1-ISP机房FW-2-分部RT2间专线为主链路，总部RT1与分部RT2间Serial专线为备链路；分部访问总部行政、财务业务优先走主链路，分部访问总部营销、信息技术业务优先走备链路，只有分部访问总部行政、财务、营销业务主备链路相互备份、信息技术业务无备份链路。根据以上需求，在分部RT2进行合理的业务选路配置。具体要求如下：

1. 使用IP前缀列表匹配业务数据流；
2. 使用BGP路由权值属性进行业务选路，只允许使用route-map来改变路由权值属性、路由控制，且路由权值必须为100或200。

### 服务器配置及应用项目

（500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默认账号密码为admin/dcncloud，ssh默认账号密码为root/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，参考《云服务实训平台用户操作手册》；

（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，centos6.5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“参见表6”，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“表3：服务器IP地址分配表”的要求设定；

（3）除非作特殊说明，在PC1和PC2上需要安装相同操作系统版本的虚拟机时，可采用VMwareWorkstation软件自带的克隆系统功能实现。

（5）PC1和PC2上所有系统镜像文件及赛题所需的其它软件均存放在每台主机的D:\soft文件夹中， 请在PC1桌面上，选手自己建立BACKUP\_X （X为组号）文件夹，并在该文件夹中建立PC1相对应的虚拟机名称的文件夹；在PC2桌面上，选手自己建立BACKUP\_X （X为组号）文件夹，并在该文件夹中建立PC2和云服务实训平台相对应的虚拟机名称的文件夹；将竞赛题目要求的截图和内容以.png和.docx的格式存放于“相对应表3虚拟主机名称的文件夹中；虚拟机文件名、扩展名和存放位置错误，涉及到的所有操作分值记为0分；

（6）PC1和PC2要求的虚拟机均安装于每台在D盘根目录下自建的名为virtualPC文件夹中，即路径为D：\virtualPC\虚拟主机名称。

**云服务实训平台安装与运用**

**一、在云服务实训平台上完成如下操作：**

**（一）云服务实训平台基础设置**

1、按照“表4：云服务实训平台网络信息表”要求创建四个外部网络，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、设置5块卷，卷命名为hd1-hd5，其中hd1-hd3大小为10G，hd4-hd5大小为5G；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。

注意：在云服务实训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“表5：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、云服务实训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**

**一、在云服务实训平台上完成如下操作:**

**（一）完成虚拟主机的创建**

将按照“表5：虚拟主机信息表”生成的虚拟主机加入到skillschina.com域环境；

**（二）在云主机1和云主机2完成域控制器的滚动升级**

1、将标识为“服务器1”的服务器启动，对其进行滚动升级，将原来skillschina.com域的域控制器“服务器1”升级到新安装的Windows Server 2012 R2服务器“云主机1“，在迁移域控制器的时候如果出现错误提示，请查找原因并进行排错，最终完成升级（如果无法解决问题，可直接将云主机1作为域控制器）；

2、将云主机2的服务器升级成skillschina.com域的的辅助域控制器；

**（三）在云主机1中完成域控制器及CA服务器的部署**

1、安装证书服务，设置为企业根，有效期为5年，为企业内部自动回复证书申请；

2、创建3个用户组，组名采用对应部门名称的中文全拼命名，每个部门都创建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，所有用户不能修改其用户口令，并要求用户只能在上班时间可以登录（每周一至周五9:00~18:00）；

**（四）在云主机2中完成存储池及iSCSI存储的部署**

1、添加三块SCSI虚拟硬盘，其每块硬盘的大小为10G，将三块硬盘配置为跨区卷，对应磁盘盘符为E:\ ，在E盘开启数据删除重复功能，排除扩展名为.xlsx,.txt的文件；

2、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E:\；虚拟磁盘名称分别为Quorum和Files，大小分别为512M和5G，访问服务器为云主机4和云主机5；

**（五）在云主机2中完成NFS服务和DFS服务的部署**

1、安装NFS服务，共享目录为E:\nfsroot，配置用户名映射，将云主机10的root用户映射为administrator的权限，可以完全访问NFS共享目录；

2、配置DFS服务，实现两个服务器的内容保持同步，空间名称为DFSROOT，文件夹为E:\DFSroot，复制组为ftp-backup，设置复制在周六和周日带宽为完整，周一至周五带宽为64M；

**（六）在云主机4中完成故障转移群集服务器的部署**

1、添加安装三块网卡，第一块网卡和第二块网卡为提供MPIO网卡，第三块网卡为心跳线网卡；

2、安装故障转移群集功能、文件服务器功能和存储多路径功能，在存储多路径功能的属性中，添加对iSCSI设备的支持；

3、使用iSCSI发起程序连接云主机2的iSCSI虚拟磁盘Quorum和Files，实现对iSCSI虚拟磁盘Quorum和Files的存储多路径功能，并能正常访问。

**（七）在云主机4中完成WEB服务器1的部署**

1、安装IIS组件，创建www.skillschina.com站点，在N:\MyShare文件夹内中创建名称为skillschina.asp的主页，主页显示内容“全国职业院校技能大赛网络搭建及比赛项目时间为：<%=now()%>”，同时只允许使用域名通过SSL加密访问；

2、设置网站的最大连接数为1000，网站连接超时为60s，网站的带宽为1000KB/S；使用W3C记录日志，每天创建一个新的日志文件，使用当地时间作为日志文件名；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、服务器端口号和方法；

**（八）在云主机5中完成故障转移群集服务器的部署**

1、添加安装三块网卡，第一块网卡和第二块网卡为提供MPIO网卡，第三块网卡为心跳线网卡；

2、安装故障转移群集功能和存储多路径功能，在存储多路径功能的属性中，添加对iSCSI设备的支持；

3、使用iSCSI发起程序连接云主机2的iSCSI虚拟磁盘Quorum和Files，实现对iSCSI虚拟磁盘Quorum和Files的存储多路径功能，并对Quorum和Files进行初始化和创建卷，设置驱动器号分别为M和N，完成格式化操作；

4、在故障转移群集功能中，添加云主机4和云主机5服务器，并生成故障转移群集验证报告验证结果；

5、创建故障转移群集，群集名称为：webcluster，IP网段为表3此云主机的第一个网段，地址为55;

6、添加文件服务器功能和配置文件服务器角色，名称为：MyClusterFiles，IP地址最后一位为56，为MyClusterFiles添加共享文件夹，共享协议采用“SMB”，共享名称为MyShare，存储位置为N:\，共享权限采用管理员具有完全控制权限，其他用户具有读写权限，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；

7、访问[www.skillschina.com](http://www.skillschina.com)站点，对<http://www.skillschina.com>；http://webcluster的IP；对[https://www.skillschina.com](http://www.skillschina.com)；https://webcluster的IP进行测试；

**（九）在云主机5中完成WEB服务器2的部署**

1、安装IIS组件，创建www.skillschina.com站点，在N:\MyShare文件夹内中创建名称为skillschina.asp的主页，主页显示内容“全国职业院校技能大赛网络搭建及比赛项目时间为：<%=now()%>”，同时只允许使用域名通过SSL加密访问；

2、设置网站的最大连接数为1000，网站连接超时为60s，网站的带宽为1000KB/S；使用W3C记录日志，每天创建一个新的日志文件，使用当地时间作为日志文件名；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、服务器端口号和方法；

**（十）在云主机6中完成磁盘阵列的部署**

1、添加二块SCSI虚拟硬盘，其每块硬盘的大小为5G；并创建镜像卷盘符为E盘；

2、在E盘上新建共享文件夹ftproot，只有技术部的员工具有完全控制权限；

**（十一）在云主机6中完成FTPS服务和DFS服务的部署**

1、安装FTP服务，新建一个FTP站点：名称为：MyFTP，主目录为E:\ftproot，不允许匿名登录，FTP站点欢迎消息为：“欢迎访问网络搭建FTP服务器！”，并且用命令浏览文件时使用UNIX方式显示，日志文件记录到E:\ftproot\LogFiles目录下；

2、通过适当技术实现域中的技术部员工sys1与sys2在登录MyFTP站点时，只能访问自己的子文件夹，并且是通过SSL进行安全的访问；

3、配置DFS服务，实现两个服务器的内容保持同步，空间名称为DFSROOT，文件夹为E:\DFSroot，复制组为ftp-backup，拓扑采用交错方式，设置复制在周六和周日带宽为完整，周一至周五带宽为64M；

**（十二）在云主机3中完成辅助DNS服务的部署**

安装DNS服务，将云主机3服务器配置成skillschina.com的辅助DNS服务器；

**（十三）在云主机7中完成相关测试功能**

1、访问云主机11的http://[www.netdj.net](http://www.netdj.net)；http://云主机11服务器IP；https:// [www.netdj.net；https:// 云主机11服务器IP](http://www.netdj.net；https://192.168.100.160) 的网站；

2、对服务器8的[www.netskills.net](http://www.netskills.net)站点进行测试；

3、使用FileZilla（可从云主机1上复制）软件对云主机6服务器的ftps服务进行验证；

4、使用FileZilla（可从云主机1上复制）软件对云主机9的ftps服务进行验证；

**二、在PC1上完成如下操作:**

**（一）完成虚拟主机的创建**

1、安装虚拟机“服务器3”，其内存为2G，硬盘40G；

2、安装虚拟机“服务器4”, 其内存为768MB，硬盘40G，通过“服务器3”的WDS服务进行网络引导和安装，安装完成后停止“服务器3”中DHCP中服务器网段的作用域；

**（二）在主机“服务器3”中完成DHCP和WDS服务的部署**

1、安装DHCP服务，为服务器网段部分主机动态分配IPv4地址，建立作用域，作用域的名称为dhcpserver，网段参照表3的本机ip地址段设置，地址池范围195-199；

2、安装WDS服务，目的是通过网络引导的方式来安装Windows server 2012 R2 CORE操作系统，运用适当技术手段，让“服务器4”只获取到对应WDS服务器端DHCP下发的IP地址。

**（三）在主机“服务器2”中完成DHCP服务和DNS服务迁移的部署**

1、将标识为“服务器2”的服务器上的DHCP服务和DNS服务迁移到“云主机1”服务器上；

2、将“服务器2”的服务器，升级为子域bj.skillschina.com；

3、在 “服务器2”中添加三块SCSI虚拟硬盘，其每块硬盘的大小为2G。将三块硬盘配置为RAID5，对应磁盘盘符为e:\；同时需要在e:\启用卷影副本功能，设置每周工作日的下午19:30创建卷影副本，将副本存储于c:\；

**（四）在主机“服务器1”中完成独立服务器和RODC服务器的部署**

1、将标识为“服务器1”的服务器从skillschina.com降级为独立服务器；

2、将“服务器1”服务器作为RODC服务器，重新加入到skillschina.com域中;

3、将域控制器中技术部的员工增加到缓存组，允许该账户的密码复制到本服务器中；

**（五）在主机“服务器4”中完成Core服务器的部署**

1、使用命令修改计算机的主机名为Core，修改服务器4的IP地址为表3中要求的地址，并按照题目要求设置默认网关；

2、将其“服务器4”的服务器加入AD DS域skillschina中；

3、关闭“服务器4”服务器的防火墙，开启远程桌面功能；

**Linux操作系统部分**

**一、在云服务实训平台上完成如下操作:**

**（一）在云主机8中完成E-MAIL服务器的部署**

1、在此服务器上安装配置postfix邮件服务，创建两个用户mail1,mail2；每个用户的邮箱空间为20MB，限定用户发邮件时，单封邮件最大为5MB；

2、为mail1和mail2两员工创建邮箱账户，实现不同用户之间的正常通讯，用户密码为321，邮件服务器的域名后缀为netdj.net，邮件服务器要在所有IP地址上进行侦听；

3、开启SMTP的SASL验证,允许通过身份验证的用户转发邮件；

4、在云主机7上安装office outlook 2013软件发送邮件；mail1用户发给mail2用户，主题为“你好”，内容为“欢迎大家”；

**（二）在云主机8中完成NIS服务的部署**

1、在此服务器上安装配置NIS服务，域名为netdj.net，建立验证数据库；

2、只为本机IP网段主机提供user1和user2的用户身份验证(密码与用户名相同) ；

**（三）在云主机8中完成NFS服务的部署**

1、配置NFS服务，按下表要求共享目录：

|  |  |
| --- | --- |
| **共享目录** | **共享要求** |
| /home | 本服务器网段的用户具有读写权限，其它只读 |
| /var/tmp | 所有人都可以存取，root写入的文件还具有root的权限 |

**（四）在云主机9中完成FTPS服务器的部署**

1、配置FTP服务，创设FTP服务站点，域名为ftp.netdj.net，站点主目录为 /var/ftpsite，不允许匿名用户访问，开启ftp支持被动数据传输模式；

2、建立虚拟用户ftpuser1及ftpuser2，密码和用户相同，用户的宿主目录为/home/vsftpd，用户的权限配置文件目录为/etc/vsftpd\_user\_conf，实现ftpuser1和ftpuser2用户通过SSL进行安全的访问；

**（五）在云主机9中完成Samba服务器的部署**

1、此服务器中安装配置Samba服务，创建三个用户user4, user5, user6；

2、建立共享目录/opt/finance\_share，要求共享名为archive，user4, user5, user6用户都能通过输入用户名和密码登录并上传文件；

3、实现user4能够查看和删除所有人的文件，user5能够查看所有人的文件，但不能删除别人的文件，user6只能查看和删除自己的文件，不能查看和删除别人的文件；

**（六）在云主机10中完成NIS客户端的部署**

1、安装NIS服务，设置NIS域名为netdj.net，指定通过NIS进行身份认证；

2、使用user1登录后，发现无法找到用户主目录，通过使用NFS的功能将其实现，并实现开机自启动；

3、使用命令进行验证，实现在/wnfs目录下，可以成功访问云主机2的NFS服务，并实现开机自动启动；

**（七）在云主机10中完成BIND域名服务器及代理服务器的部署**

1、在此服务器中安装配置bind服务，负责区域“netdj.net”内主机解析，四台主机分别为mail.netdj.net、dns.netdj.net 、[www.netdj.net](http://www.jnds.net)、ftp.netdj.net,做好正反向DNS服务解析，禁止172.16.10.0/24网段的主机访问此DNS服务器；

2、安装并完成代理服务器squid的初始配置，使用8090作为代理服务端口，指定DNS服务器IP地址信息，使得squid服务器能够解析域名；

3、设置squid代理服务器采用ufs缓存机制，缓存目录设置为/cache,目录容量为5GB，L1及L2级目录数量分别为16及256，定义高速缓存值为512MB，并将缓存日志存放于/var/squid/cache.log中；

4、设置禁止访问.mp3、.flv 扩展名后缀的资源；

5、设置需要身份认证的代理方式，认证方式为基础认证，认证程序的进程为5个，账户为proxy\_user，账户存储在/squid/squid\_user，密码为user\_proxy；

**（八）在云主机11中完成Apache服务器及MySQL数据库服务器的部署**

1、在此服务器中安装httpd服务，建立虚拟主机站点[www.netdj.net](http://www.jnds.net)，其网站主目录为/www/netdj，主页名字为netdj.html，首页内容为“Welcome netdj’s website”；

2、使用openssl申请证书，创建自签名证书server.crt和私钥server.key，要求只允许使用域名通过SSL加密访问；

3、将此服务器配置为MySQL服务器，创建数据库为myschool，在库中创建表为mystudent，在表中创建2个用户，分别为（1，myuser1，1996-7-1，male），（2，myuser2，1997-9-1，female），口令与用户名相同，口令使用PASSWORD方式认证，需要对登录网站的用户进行身份验证，表结构如下；

|  |  |  |
| --- | --- | --- |
| **字段名** | **数据类型** | **主键** |
| ID | Int | 是 |
| Name | varchar(10) | 否 |
| Birthday | Datetime | 否 |
| Sex | char(8) | 否 |
| Password | char（128） | 否 |

4、创建文本文件mysql.txt，并输入两行记录（3，myuser3,1999-7-1,male,myuser3）和(4，myuser4,1999-12-10,male,myuser4)将mysql.txt中的内容导入到mystudent表中；

**（九）在云主机11中完成iptables服务器的部署**

1、开启服务器的路由转发功能；

2、配置系统防火墙，关闭除提供系统服务以外的端口，并使用命令将其保存到/etc/iptables文件中。

**二、在PC2上完成如下操作：**

**（一）完成虚拟主机的创建**

1、安装虚拟机“**服务器7**”,具体要求为内存1G，硬盘20GB；

2、安装虚拟机“**服务器8**”,具体要求为内存1G，硬盘20GB；

3、通过“**服务器5**”的PXE服务器网络安装“**服务器6**”虚拟机，具体要求为内存512MB，硬盘20GB，运用适当技术，让此PXE的客户端，只获取到对应PXE服务器端DHCP下发的IP地址；

**（二）在主机“服务器5”中完成PXE服务器的部署**

1、管理员小明将标识为PC2服务器上的已有虚拟机“服务器5”启动，发现“服务器5”无法正常使用，系统启动时提示为“grub>”，请您帮忙解决，**将其解决方案主要步骤截图保存在名字为grub.docx的文档中**（如无法排除故障，可重新安装虚拟机“服务器5”）；在此服务器上以YUM方式安装DHCP服务，创建超级作用域，名称为：mydhcpdomain，网段为此服务器ip地址段，地址池为200-210。指定DNS服务域名为dns.netskills.net，指定DNS服务器以及网关的IP地址信息，设置租约时间172800s，最大租约时间为259200s，指明下一跳TFTP服务器IP信息，同时设置自动安装脚本文件;

2、在此服务器上以YUM方式安装TFTP服务，并将服务根目录设置为/tftpboot；

3、在此服务器上以YUM方式安装FTP服务，并将比赛提供的CentOS光盘内容完整拷贝至FTP公共目录下，开启FTP服务的匿名上传及写入权限；

4、配置PXE服务器，目的是通过网络引导的方式来安装Centos6.5操作系统，安装完成后，停止PXE服务器的DHCP服务；

**（三）在主机“服务器6”中完成磁盘管理的部署**

1、在“服务器6”中手动添加四块SCSI硬盘，前三块容量均为2G，第四块容量为4G，将前三块硬盘设置为一个主分区，第四块硬盘设置为两个逻辑分区（分别2G容量），并完成磁盘阵列RAID10的操作；

2、将RAID10的/dev/md10分区，分出一个大小为1G的空间，格式化为swap分区，设为开机生效；

3、将RAID10的/dev/md10分区上剩余的空间创建二个大小相同的分区，建立LVM为/dev/vg1/lv0和/dev/vg1/lv1，格式化为ext3文件系统，开机自动挂载到/lvm0和/lvm1目录；

4、针对现有的逻辑卷/dev/vg1/lv0实现在线扩容，将/dev/sde6分区加入到已有的逻辑卷vg1中，实现目录/lvm0在线扩容2G容量，总容量达到3.5G；

5、将逻辑卷lv0上的文件系统动态地减少200M，将逻辑卷lv1上的文件系统动态地增加200M，重新挂载这两个文件系统；

**（四）在主机“服务器6”中完成JSP+Tomcat运行环境的部署**

1、安装jdk和jre，安装完成后，配置JAVA环境变量；

2、安装tomcat服务并启动，在浏览器输入http://本服务器IP:8080；

3、将D:\soft\jndsjs中全部微网站应用程序，复制到tomcat的相关目录下，通过适当配置，可以实现通过http:// tcat.netskills.net显示指定的网页内容；

**（五）在主机“服务器7”中完成数据库服务器的部署**

1、将此服务器配置为数据库服务器，创建数据库为myuserdatabase，在库中创建表为username，在表中创建2个用户，分别为（myuser1，1998-4-2，female），（myuser2，1999-10-8，male），口令与用户名相同，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(8) | 否 | 否 |
| Password | char（128） | 否 | 否 |

2、在username表格中，查询性别为male男的用户记录，修改用户myuser1的出生日期为1999-10-25；

**（六）在主机“服务器7”中完成E-MAIL服务器的部署**

1、在此服务器上安装配置Sendmail邮件服务，创建两个用户mail3，mail4；限定用户发邮件时，附件最大为5MB；

2、为mail3和mail4两员工创建邮箱账户，实现不同用户之间的正常通讯，用户密码为321，邮件服务器的域名后缀为netskills.net，邮件服务器要在所有IP地址上进行侦听；

3、创建名称为everyone的邮件列表，发给everyone@ netskills.net的邮件，每个员工均可收到；

4、开启SMTP的SASL验证,允许通过身份验证的用户转发邮件；

5、在Server2上使用office outlook 2013软件发送邮件，mail3用户发给mail4用户，主题为“你好”，内容为“欢迎大家”；

**（七）在主机“服务器8”中完成域名服务器和Apache服务器的部署**

1、在此服务器中安装配置unbound服务，负责区域“netskills.net”内主机解析，四台主机分别为pxe.netskills.net、tcat.netskills.net、mail.netskills.net 、[www.netskills.net](http://www.jnds.net)、,做好正反向DNS服务解析；

2、在此服务器中安装配置WEB服务，建立web站点为[www.netskills.net](http://www.jnds.net)，其网站主目录为/share/www，主页名字为netskills.html，首页内容为“Welcome netskills’s website”;

3、配置apache服务器，实现网站状态监控；

4、对apache服务的日志文件进行保护，只允许往文件里添加数据，不能删除数据；

**（八）在主机“服务器8”中完成磁盘配额的部署**

1、在“Centos7-C2”中手动添加一块SCSI硬盘，大小为2G，挂载到/sdb1目录下；

2、使用xfs\_quota磁盘配额命令，将该/sdb1目录对普通用户user1设置开机自动启用磁盘配额管理，bsoft和bhard的限制大小分别为300M和500M；

3、在user1用户登录下，使用dd命令在目录/sdb1内创建一个510M的ds2018.txt文件，检查soft的警告值500M是否生效；

**（九）在主机“服务器8”中完成firewall服务器的部署**

1、配置系统防火墙firewall，关闭除提供系统服务以外的端口；