# 项目概况

## 项目名称

全国一体化先进算力服务平台（四川）（以下简称“算力服务平台”）

## 建设单位

四川算力服务科技有限公司（以下简称“合资公司”）

## 建设地点

算力服务平台计划部署于成都市简阳市空天产业园四川能投天府云数据产业基地。

## 项目定位

算力服务平台定位为四川省省级数字基础战略性项目、能投数产公司战略性投资项目、四川省算力服务的第一平台和第一门户。以政府引导下的企业市场化方式建设运营，使其既能对内统筹全省富余算力资源，又能对外开展节点间的算力资源供需对接和调度交易，降低用户使用门槛、提高算力应用水平。通过以算引数、以数育产，极大提高算力资源的利用效率和节能环保水平，助力区域协调发展和数字经济创新，同时有利于提高数据基础设施的使用效率。

## 建设目标

到2024年底，初步建成算力服务平台，实现对天府数据中心集群内超算中心、智算中心和部分数据中心的统一调度，接入雅安、达州等部分基础较好的城市内部数据中心，初步形成全省一体化算力调度标准体系，成为全省算力交易服务市场的首选平台。到2026年，全面建成四川省算力服务平台，完成全省所有大型、超大型数据中心接入，实现算力“三跨四互联”（“三跨”是指跨资源池、跨不同算力厂商以及跨算力架构。“四互联”即该平台架构,实现了通用算力、智算、超算和网络的互相联动。”）的一体化调度，打造成为具有全国影响力的算力服务平台。

## 建设任务

项目分3年进行建设，在2024年一季度内实现基本交易功能建成上线运营，并在2026年底前逐步完善算力服务平台建设。统筹盘活全省各类富余算力资源，丰富以先进算力为中心的应用场景，为算力需求方提供高效、便捷的算力调度、交易、技术咨询等服务。

## 建设内容

本项目建设内容包括1个底座、3个平台、3个体系以及N个算力资源接入。

1个底座：建设平台软件部署所需的计算、存储、网络等系统。安全相关的软硬件由“全国一体化大数据中心体系云安全能力平台（四川）”提供能力。

3个平台：包括算力服务平台、综合监测平台和一体化安全保障平台；其中一体化安全保障平台由“全国一体化大数据中心体系云安全能力平台（四川）”提供能力。

3个体系：包括标准规范体系、安全保障体系和运维保障体系；

N个算力资源接入：包括成都超算、成都智算、天府云、雅安智算、达州智算以及各类数据中心通过专线网络接入算力服务平台。

## 建设工期

本项目计划按照3年周期进行建设，其中2024年一季度内实现基本交易功能建成上线运营。

## 建设模式

由四川省数字产业有限责任公司（以下简称“能投数产公司”）牵头成立合资公司，并由合资公司出资，按照设计+施工总承包（D-B）模式推进建设工作。

## 主要结论及建议

### 结论

通过对项目投资以及组建合资公司的初步可行性研究，得出以下基本结论：

本项目符合国家、地方政府相关要求，契合“东数西算”发展战略，满足结构合理、供需匹配、绿色安全的数据中心一体化发展格局要求。项目建成后社会效益突出，经济效益可预期，且对企业战略发展具有重大意义，项目整体可行。

### 建议

本项目到2024年一季度需建成并运营，时间紧，任务重，建议加快审批，尽快成立合资公司，推动项目设计、建设和运营。

# 编制依据

## 政策文件

1. 《“十四五”数字经济发展规划》；
2. 《数字中国建设整体布局规划》；
3. 《新型数据中心发展三年行动计划（2021-2023 年）》;
4. 《关于加快构建全国一体化大数据中心协同创新体系的指导意见》；
5. 《全国一体化大数据中心协同创新体系算力枢纽实施方案》；
6. [《四川省数字化转型促进中心建设的政策措施》](https://www.baidu.com/link?url=IVRUPZpi8LX1WN-XHaNFsfqoo0jllT9qb-sYoFElvmNNoCYIoIs9sXqyXL5Yzc-S&wd=&eqid=8ad772ed0002c2ad0000000664c1e880)；
7. 《关于同意成渝启动建设全国一体化算力网络国家枢纽节点的复函》；
8. 《全国一体化算力网络成渝国家枢纽节点（四川）实施方案》；
9. 《2023年四川省政府工作报告》；
10. 《中共四川省委关于深入推进新型工业化加快建设现代化产业体系的决定》。

## 计算机信息系统类标准

1. 《云计算服务协议参考框架》（YDB 144-2014）；
2. 《信息技术开放系统互连 网络层安全协议》（GB/T 17963-2000）；
3. 《信息安全技术操作系统安全技术要求》（GB/T 20272-2019）；
4. 《信息安全技术数据库管理系统安全技术要求》（GB/T 20273-2019）。

## 软件类规范

1. 《信息技术软件工程术语》（GB/T 11457-2006）；
2. 《软件工程软件生存周期过程用于项目管理的指南》（GB/Z 20156-2006）；
3. 《信息技术软件维护》（GB/T 20157-2006）；
4. 《信息技术软件生存周期过程配置管理》（GB/T 20158-2006）；
5. 《信息技术软件生存周期过程》（GB/T 8566-2007）；
6. 《系统与软件工程 系统与软件质量要求和评价（SQuaRE） 第10部分：系统与软件质量模型》（GB/T 25000.51-2016）。

## 信息安全类规范

1. 《中华人民共和国网络安全法》（中华人民共和国主席令第五十三号）；
2. 《信息安全技术 网络安全等级保护测评要求》（GB/T 28448-2019）；
3. 《信息安全技术 网络安全等级保护安全设计技术要求》（GB/T 25070-2019）；
4. 《信息安全技术 网络安全等级保护测评过程指南》（GB/T 28449-2018）；
5. 《信息安全技术 网络安全等级保护测试评估技术指南》（GB/T 36627-2018）；
6. 《信息安全技术网络安全等级保护定级指南》（GB/T 22240-2020）；
7. 《信息安全技术网络安全等级保护基本要求》（GB/T22239-2019）；
8. 《信息安全技术办公信息系统安全管理要求》（GB/T 37094-2018）；
9. 《信息安全技术操作系统安全技术要求》（GB/T 20272-2019）；
10. 《信息安全技术移动通信智能终端操作系统安全技术要求》（GB/T 30284-2020）；
11. 《信息安全技术数据库管理系统安全技术要求》（GB/T 20273-2019）；
12. 《安全防范工程技术标准》（GB 50348-2018）；
13. 《信息安全等级保护管理办法》；
14. 《信息系统安全等级保护定级指南》；
15. 《信息系统安全等级保护基本要求》；
16. 《信息系统安全等级保护实施指南》。

## 造价编制依据

1. 《基本建设项目建设成本管理规定》（财建[2016]504号）；
2. 《工程勘察设计收费管理规定》（计价格[2002]10号）；
3. 《建设工程监理与相关服务收费管理规定》发改价格[2007]670；
4. 《招标代理服务收费管理暂行办法》（计价格[2002]1980号）；
5. GB/T 36964-2018《软件工程 软件开发成本度量规范》；
6. 《2022年中国软件行业基准数据》。

## 其他规范

1. 中华人民共和国国家标准GB 50314-2015《智能建筑设计标准》；
2. 中华人民共和国国家标准GB50052-2009《供配电系统设计规范》；
3. 中华人民共和国国家标准GB50343-2012《建筑物电子信息系统防雷技术规范》；
4. 中华人民共和国国家标准GB50057-2010《建筑物防雷设计规范》；
5. 中华人民共和国国家标准GB50217-2018《电力工程电缆设计标准》；
6. 中华人民共和国国家标准GB50016-2014《建筑设计防火规范》；
7. 2006年7月信息产业部发布的YD 5059-2005《电信设备安装抗震设计规范》；
8. GB 50371-2006 厅堂扩声系统建设规范；
9. GB 50311-2016 综合布线系统工程设计规范；
10. YD/T 1095-2018 通信用交流不间断电源（UPS）。

# 需求分析

## 监管需求分析

监管需求主要是政府需要对算力进行资源监测、安全监管和安全认证。一是需要实时监测平台接入的算力资源使用情况，包括计算、存储和网络等资源，及时了解算力资源和能源的消耗情况，结合算力需求进行资源的合理布局和调配，并制定算力建设规划，提高资源利用率、数据基础设施的使用效率和能源效率；二是需要对全省算力资源进行安全监管，可以及时发现异常行为和不安全因素，采取相应的安全措施来保障算力资源的安全稳定运行，确保算力的可信交易；三是在安全监管的基础上对全省算力资源进行安全准入评估认证和信创认证，提升算力产品的公信力，确保用户得到认证的产品。

## 需方需求分析

在政府侧，算力需求主要涉及科研、卫生、安全、基础设施等多个领域，发挥四大方面的作用。一是数据分析和决策支持，利用算力来分析社会经济数据，预测未来趋势，制定相应的政策和计划；二是社会管理和安全预警，利用算力可以分析城市运行和社交媒体等数据，提前发现和预防潜在的社会安全问题；三是提升公共服务质量和效率，利用算力对公共服务进行优化规划并提高政府机构和公共服务平台信息化水平，提供高质量的便民服务；四是进行网络安全监测和防护，利用算力防范网络攻击和数据泄露，保护公民个人信息隐私。

在企业侧，算力主要应用在业务创新、数字化转型、客户服务优化、运营效率提升等领域，发挥五大方面的作用。一是实现基础设施和资源管理，利用算力来管理和优化其基础设施和资源，提高资源利用效率和降低成本；二是数据分析和业务决策，利用高性能的算力处理和分析大量的数据，挖掘数据的潜在价值，指导业务决策。三是训练优化模型，利用算力强化人工智能和机器学习能力，提高人工智能系统预测、决策的准确性。四是大规模计算和仿真，利用高性能算力对产品的设计和工艺进行仿真优化，提高产品质量和生产效率。五是云计算和分布式处理，利用云计算平台来部署和管理大规模的数据存储和处理任务，实现弹性扩展和高可用性。

在科研院所侧，算力主要应用在科研项目和学术研究领域，发挥三大方面的作用，一是大规模数据处理和分析，利用高性能算力处理、分析、挖掘大量实验数据、学术数据和各种复杂数据集，发现新的科学现象、验证理论模型或探索未知的规律。二是实现仿真和模拟实验，利用算力对物理学、生物学、天文学等学科领域复杂的科学模型进行大规模的计算和仿真，加速仿真和模拟过程，提高计算效率和准确性。三是模型训练，广泛应用人工智能和机器学习技术进行数据分析、模式识别和预测建模，利用算力训练复杂的神经网络模型，提高模型的准确性和性能，应用于基因组学、天文学、材料科学等领域研究。

在个人或团体侧，算力主要应用在工作和生活中，主要发挥三方面的作用，一是游戏娱乐，利用强大的算力运行各种高质量的游戏和娱乐应用，支持更流畅的游戏画面和更逼真的虚拟现实体验；二是媒体影音处理，利用算力进行视频编辑、音频处理和图像处理等多媒体处理，可以加速处理过程，提高处理效率和质量；三是虚拟化和云计算，利用云计算服务来存储和备份大量的文件、实施远程桌面服务等，扩展计算能力和存储容量，无需购买昂贵的硬件设备；四是支持软件开发、产品设计，利用高性能算力处理复杂的三维渲染任务、编译大型代码库和进行软件开发和测试。

## 供方需求分析

对于算力资源服务商来说，目前四川省整体算力资源呈现供大于求的趋势，线下供需对接比较难，闲置算力资源较多，难以得到有效利用；算力用户取决于自身生态的建立情况，很多用户因地域、距离以及考虑到算力资源安全和算力产品质量问题等因素流失；对用户的订单确认、服务响应时间长，线下交易流程缓慢、复杂。针对以上问题，迫切需要一个省级算力服务平台进行资源整合和并利用高效的服务面向全省甚至全国提供算力服务。

# 平台建设建议

为保障平台建成之后能满足算力资源服务商、政府、企业、科研院所、个人或团体、合资公司等“供、需、管”三方实际需求，参考全国市场已有算力相关平台的服务能力以及运营机制，结合四川实际情况，为本算力服务平台的服务能力和运营机制建设提出以下建议。

## 平台服务能力建议

### 调度服务能力

算力服务平台应具备“三跨四互联”的资源接入能力，实现超算、智算、通用算力和网络的联动，能对资源进行封装、加工，实现通用算力多云纳管，能屏蔽底层异构资源架构，进行跨资源池、跨厂商、跨架构调度，对外提供算网一体、云网融合的多样化算力服务。同时能将用户的应用和环境打包成可移植的格式进行算力解构和部署。具备为客户提供算力、存力、云安全等服务的能力。

### 应用服务能力

算力服务平台建成后应具备算力和应用加工能力，能基于基础算力提供应用服务，能为用户提供芯片和软件的适配能力，能快速针对不同行业用户的创新软件应用或定制化算力需求提供国产芯片适配或通用芯片适配服务，形成跨数据中心、跨算力类型的专用算力产品，满足不同行业、不同用户的算力增值服务需求。能通过专用算力服务，带动算力资源的利用，为算力建设规划、布局提供数据支撑，指导各类数据中心建设。

### 交易运营能力

算力服务平台能够通过算力服务门户面向用户提供安全、便捷、稳定的交易服务，能提供基础算力、应用软件、专用算力、机柜资源、云安全和算力服务等产品服务能力，能根据不同使用需求进行差异化计费，并具备在线交易和在线结算能力，能快速完成算力服务订单确认，产品试用、在线支付，并能与供应商按照约定支付比例进行在线结算。

### 综合监测能力

平台能对数据中心和接入的算力算效、网络质量、能源状态等进行实时监测，全面掌握算力资源、能源利用情况和运行趋势，实现全省数据中心算力资源、网络资源、能源利用效率等动态监测管理，支撑算力一体化调度能力实现。

### 安全保障能力

平台能从主机、应用、网络、数据、终端 5个方面，对数据中心和接入的算力进行扫描、监测和采集，提供国家信息安全等级保护三级保障能力，实现各数据中心节点的统一安全态势感知和安全防护能力，支撑算力相关数据的可信传输。

### 安全认证能力

可以将本项目安全建设作为标准，制定四川算力安全认证机制。通过政府出台算力准入规则，与高校或科技机构成立联合实验室或由第三方独立专业机构对全省智能算力、超算算力、通用算力资源进行安全评估、认证和信创产品认证，提升算力产品的公信力，确保用户得到认证的产品，实现算力资源的可信交易。

### 运行保障能力

（1）高可用性：平台应具备高可用性，保证在各种场景下都能稳定运行，出现问题后能够及时修复，提供不间断的服务。系统可用性（=MTBF（平均无故障工作时间）/（MTBF+MTTR（平均维修时间）））不低于99.99%。

（2）可扩展性：考虑到未来可能的业务增长，平台应具备良好的可扩展性，能够随着业务规模的扩大而自动地进行扩展。

（3）高性能：对于大规模数据处理和计算，平台需要具备高性能，可以快速处理各种交易和请求。按照全国1000个用户同时访问，确保tps≥1000+；系统查询响应时间设置为≤5秒；硬件设备需支持连续7×24小时不间断地工作，支持主要配件如电源模块、磁盘等的热拔；硬件设备的CPU忙时峰值利用率平均不超过70%，内存忙时利用率平均不超过70%，带宽利用率忙时不超过70%；应用系统需支持连续7×24小时不间断地正常工作，应用软件中的任一模块更新、加载时不影响业务运转和服务；系统支持全国注册和使用，设计充分考虑容量扩展性和性能平衡，可支持未来10年用户注册和使用的容量增长，单日5万人次访问量。业务正常运行期间，核心业务用户正常访问相应延时＜1秒。

（4）安全性：平台应具备强大的安全机制，保障算力交易过程的安全性和交易各方的隐私。具备故障守护恢复机制，即当发生一般性软件和硬件障碍时，系统具有自我恢复能力，15分钟切换完毕，30分钟恢复正常。

（5）灵活性：平台应能够灵活地支持不同的算力需求和交易模式，满足不同的业务需求。

（6）易用性：对于普通用户，平台应具备友好的界面和简单的操作流程，方便其进行算力购买和使用。

## 运营机制建议

### 市场化选聘技术支撑方

算力服务平台的重点是如何有效地利用和管理算力资源，为客户提供高效、可靠、定制化的服务。算力服务平台的建设和运营期间，需要选择可靠的技术支撑方参与方案制定、建设和运营管理。单一厂商很难全部满足平台运营需求。首先需要调研多家潜在技术支撑方，通过市场化方式从建设方案和经验、运营方案、服务报价等多个方面进行打分，公平公正遴选技术支撑方。

建设方案和经验。要求候选人提供建设方案和工程报价并提供相关领域的经验和能力证明，包括过去实施的项目、使用的技术和工具以及实施效果等。评估其方案的契合度、可行性和报价合理性以及经验能力。

运营方案。要求候选人提供与本项目匹配的运营方案，包括平台软硬件运营、用户画像和市场推广等内容，评估候选人提供的运营方案是否匹配本项目需求，是否具有可行性。并要求其提供免费支撑年限、利益绑定机制、能够带来的生态资源、渠道等，评估其合作方式是否满足期望，是否能保障算力服务平台的正常高效运行，是否能提升市场能力和盈利能力。

服务报价。要求候选人进行服务报价，并对各个候选人的报价进行评估打分。

### 利益绑定机制

算力服务平台建成后，将不同利益方之间的利益诉求和目标进行有机融合，通过一定的契约、合同或其他形式，建立一个相对稳定和互利共赢的合作模式。在这个机制下，合资公司与技术或运营服务商需明确自己的权利和义务，追求共同的利益目标，进行联合运营。技术或运营服务商通过引入生态合作伙伴，扩展算力服务平台营销渠道，同时合资公司制定合理的激励机制，提高各方参与积极性，实现互利共赢和长期合作的良好生态。

### 生态能力建设

算力服务平台建设和运营需要从平台上游、下游等多个层面进行生态能力建设，逐步开拓算力服务市场，提高市场占有率，增强平台盈利能力。

**政策支持能力。**从政府侧，争取出台相关政策，鼓励和支持企业和科研院所等机构加大产品研发和科技创新力度，推动算力服务平台的资源利用和发展。同时争取让政府通过算力服务平台发放算力券，引导和促进有算力需求的用户在算力服务平台进行消费抵扣。

**算力整合能力。**算力服务平台需与省内主要算力中心进行合作，将分布在不同地区、不同架构的富余算力资源进行整合，同时与各类设备厂商、算力服务平台达成合作，形成一个丰富的、统一的、高效的算力资源池，满足不同用户的需求。

**建立合作伙伴网络。**与各类企业、机构等建立合作伙伴关系，形成一个广泛的生态系统。与IT厂商、电信运营商、独立软件开发商、算法提供商等打造朋友圈，建立合作伙伴之间的合作机制，包括合作方式、利益分配、风险控制等，共同提供算力服务，实现共赢。同时建立良好的沟通渠道，以便能够及时交流信息和分享经验，共同解决问题和探讨发展方向。

**拓展客户群体。**通过举办竞赛、发布课题、培训等方式，并提供活动基金，吸引潜在客户群体参与使用算力服务平台，同时提供技术支持，协助合作伙伴解决技术难题，提高业务效率和品质，在提高其专业能力的同时，培养其使用习惯，逐步进行订单转化。

# 总体建设方案

## 总体建设要求

### 科技引领，技术赋能

坚持探索创新，推动物联网、大数据、云计算、人工智能等现代信息技术广泛应用于算力服务平台，提高平台的性能和效率，提供丰富、精准的数据分析和人工智能应用。同时参考国内先进经验，采用成熟技术，着力打破算力调度“三跨四互联”壁垒，推动不同算力资源的整合、利用。

### 科学布局，适度超前

在建设算力服务平台时，坚持以整合富余算力和市场需求为导向，聚焦算力行业的痛点堵点，同时考虑算力中心地理位置、能源供应、政策支持、市场需求等，保证接入的数据中心资源能满足当前的业务需求。同时要有预见性和前瞻性，考虑到未来的技术发展、市场需求和政策变化，在建设过程中预留一定的扩展空间，能适应未来的发展变化，避免频繁的改建或扩建。

### 政府引导，市场主体

在算力服务平台的建设和运营过程中，平衡政府和市场之间的关系。政府的角色是引导和支持，通过制定相关的政策、法规和标准，引导服务商、企业和机构等投入到这一领域。同时需要充分发挥市场的作用，企业、科研机构、院所等是创新的主体，也是推动平台发展的主要力量，要鼓励其在市场竞争中不断创新，推动算力服务平台的多元化发展，以满足市场的不同需求。

### 绿色低碳，安全发展

在算力服务平台的建设过程中，需要积极推动绿色低碳的发展，采用高效节能的技术和设备，优化数据中心的能源利用效率，减少碳排放。同时，需要确保平台在运行过程中的安全性，包括数据安全、网络安全、系统安全等，建立完善的安全管理体系，包括严格的安全管理制度、高效的安全管理团队、完备的安全防范措施等。另外，加强相关人员的安全培训，提高安全意识，确保平台的安全稳定运行。

## 总体建设原则

### 系统性原则

必须坚持系统性原则，采取有力的组织措施和严格的制度保障，统筹规划、统一设计，保证整个系统的统一和数据的一致。

### 先进性原则

应充分考虑信息化社会迅猛发展的趋势，在技术上适度超前，采用国际或国内目前的先进技术，并考虑到今后将会出现的新技术，设计具有一定的前瞻性。

### 成熟性和实用性原则

应采用被实践证明为成熟和实用的技术和设备，最大限度地满足现在和未来发展的需求，确保耐久使用。

### 安全性和可靠性原则

系统选用的技术或配套设备采用“主流”技术和产品，所谓的“主流”技术和产品是指工程项目应采用在实际工程广泛应用的成熟可靠的先进技术或产品，以保证系统的长期正常运行。

### 标准化和模块化原则

各子系统必须标准化、模块化，应体现系统的整体性、相关性、联动性。集成管理平台接口开发兼容性强，界面标准化、规范化，对于各种标准接口（OPC、BACnet、ODBC、RS485/422/232等）和非标准化接口，都能够实现各应用系统信息（运行数据和命令）的转换和实时传递；子系统需提供独立的硬件接口，及基于此接口的标准通讯协议，并开放其数据库。项目建成后，后续新增设备接口需满足本次设定的标准接口要求，需开放软件接口协议，接入到现有系统平台。

### 开放性和可扩展性原则

应考虑到项目后期的扩展需要，使系统与未来发展的设备具有互联性与互操作性。系统结构要按照开放性和可扩展性原则设计。一方面，采用开放性、标准化的设计以尽可能地利用已有的设备、软件及信息资源。另一方面，对于未来可能增添的新的子系统、新的数据库、新的功能、新的用户都要留有接口和二次开发 API，并符合信息化建设相关技术标准.可以随形势的发展而不断成长扩大。同时软件供应商应提供一定权限的源代码，保证用户能够自己成立开发团队进行代码维护和系统升级。

### 经济性原则

本项目建设应当充分利用已有资源，避免重复工作，力求减少浪费。

### 完整性原则

除了针对本期项目系统功能需求外，还要充分考虑非功能需求和项目全程监管，包含：

（1）加强领导、统一协调；

（2）坚持项目法人责任制和招投标制；

（3）性能设计、安全保密设计、集成与运行环境要求、备份恢复要求等内容的相关设计方案、数据准备、设备购置与人员培训、组织机构调整同时进行；

（4）在项目建设的全过程实施质量控制，及时发现、解决建设中的问题；

（5）吸收国内外先进经验，从建设开始就实施现代项目管理，对项目的建设管理、项目实施、人员培训等项目建设的诸多环节进行初步规划和设计，确保涵盖建设的全部需求。

## 总体系统架构



总体系统架构图

全国一体化先进算力服务平台（四川）总体按照“133N”架构体系进行建设，包括1个底座，3个平台、3个体系和N个算力资源接入，面向政府、企业、科研院所等提供仿真、渲染、AI训练、科学计算、存储备份等算力服务。

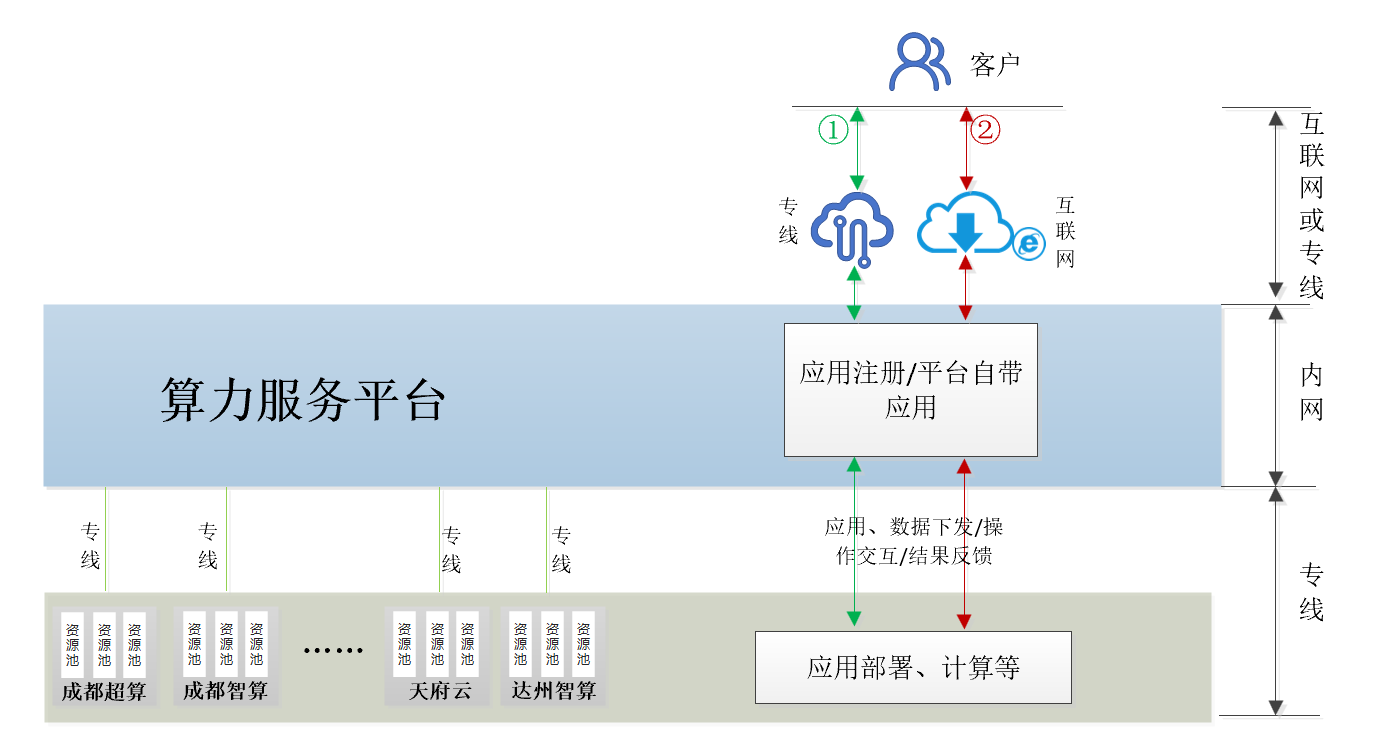
1个底座：建设平台软件部署所需的计算、存储、网络等系统。安全相关的软硬件由“全国一体化大数据中心体系云安全能力平台（四川）”提供能力。

3个平台：包括算力服务平台、综合监测平台和一体化安全保障平台；其中一体化安全保障平台由“全国一体化大数据中心体系云安全能力平台（四川）”提供能力。

3个体系：包括标准规范体系、安全保障体系和运维保障体系；

N个算力资源接入：包括成都超算、成都智算、天府云、雅安智算、达州智算以及各类数据中心通过专线网络接入算力服务平台。

## 用户访问示意图



用户访问示意图

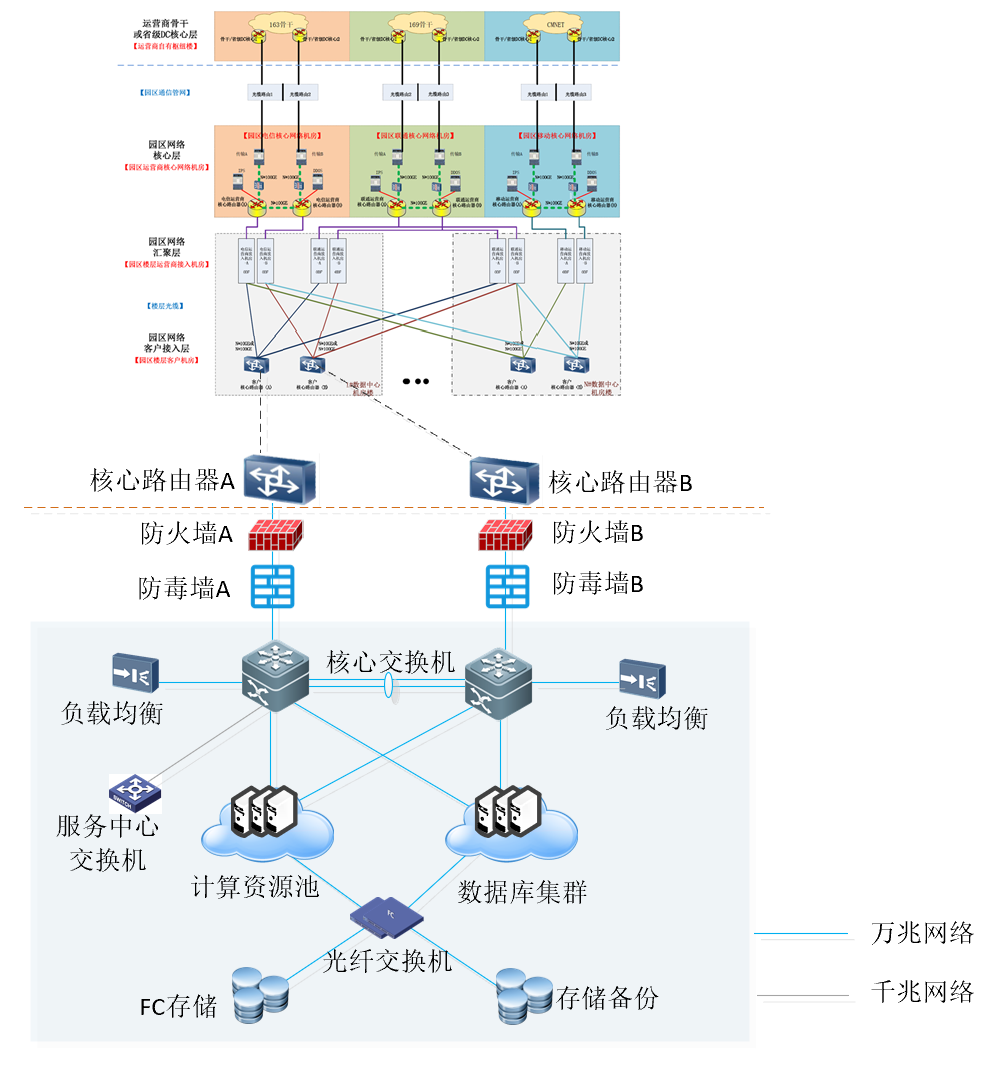
本项目网络分为算力服务平台中心网络、客户侧网络和算力供应方侧网络。用户可通过互联网或专线进行访问和操作，所有操作均通过算力服务平台进行，所有数据通过算力服务平台进行中转。当用户自己提供软件时，需要在算力服务平台进行注册并下发应用；当平台自带软件时，则直接使用或根据实际情况进行应用下发。

（1）算力服务平台内部新建网络系统，接入能投天府云基地内客户核心路由器，再进行内外网地址转换，实现内外网互联互通；

（2）客户侧利用互联网或专线访问和控制算力服务平台，专线带宽需求通常为200Mbps以上，算力服务平台出口互联网带宽需求1Gbps以上，根据业务量的变化可进行网络扩容；

（3）算力服务平台与各个算力中心之间通过专线进行互联互通，专线接入能投天府云边界网络，通过客户核心路由器与平台内网进行互联互通，专线带宽需求200Mbps以上。该专线由算力中心负责打通。

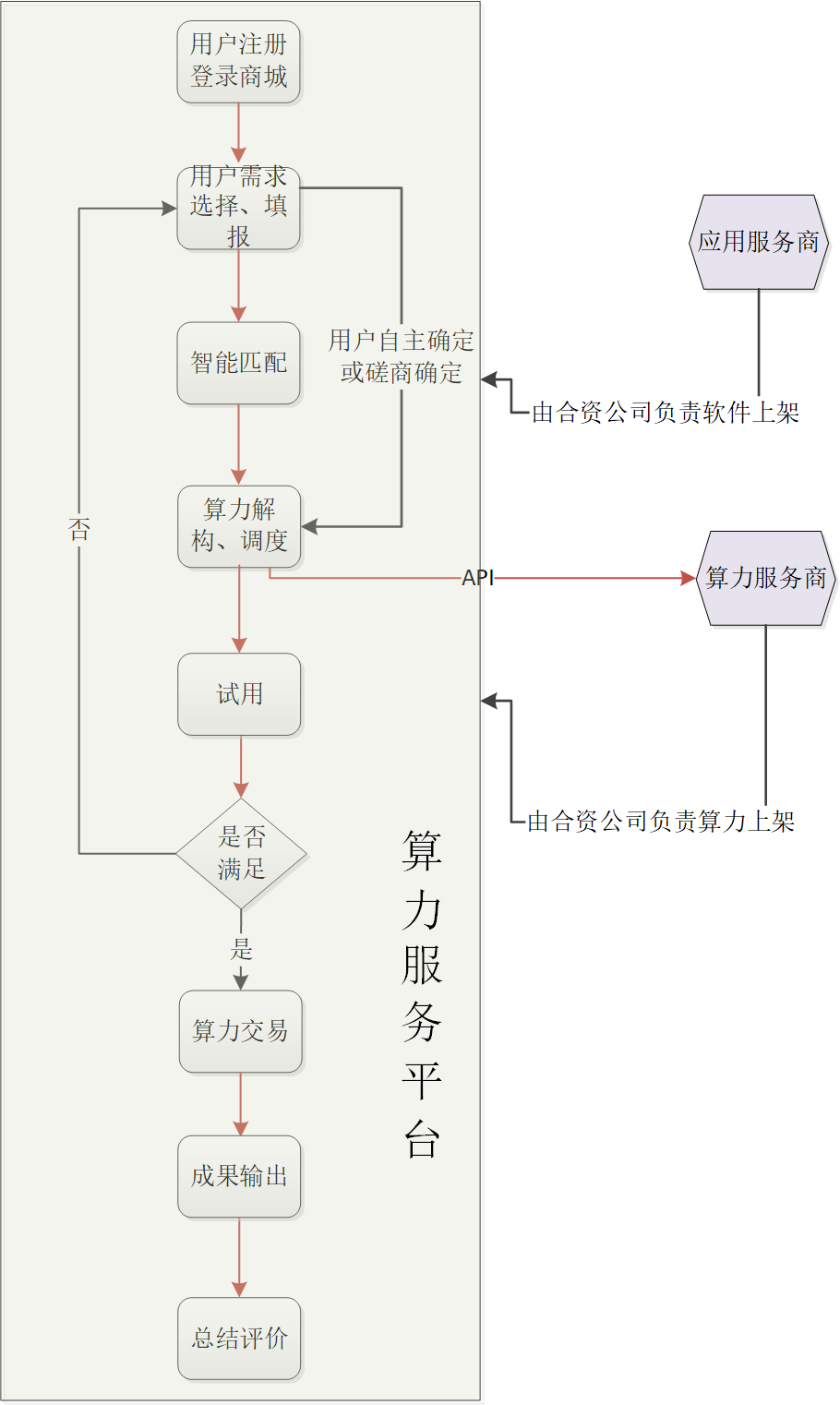
## 总体网络架构



总体网络架构图

本项目新增设备均部署在能投天府云数据中心内，包括网络和计算、存储设备，安全平台及安全相关的设备由“全国一体化大数据中心体系云安全能力平台（四川）”提供能力。网络系统主要包括核心网、业务网、管理网、存储网。以核心交换机为中心，北向与外部核心路由器相连，并接入外部互联网和专线，南向接入计算存储设备、安全设备和服务中心的设备。

## 总体业务流程



总体业务流程图

各类算力资源和应用资源需由合资公司负责在算力服务平台进行上架。用户在商城进行注册，选择、填报需求，系统可进行智能匹配算力资源，也可由用户直接确定或与运营人员磋商确定，平台根据确定的需求进行算力解构和算力调度。用户根据确定的算力资源进行试用，如果试用不满足需求则重新进行选择和匹配，如果满足需求则在线进行算力交易，在交易完成后用户可进行总结评价，助力平台进一步完善。

# 详细建设方案

## 软件平台

本项目软件建设包括算力服务平台、综合监测平台和一体化安全保障平台3个平台。

### 算力服务平台

算力服务平台建设整体包括可信数据、算网编排和交易运营以及统一门户四个部分。可信数据主要是平台运行所产生的数据存储管理；算网编排主要是算力资源的接入与调度、资源封装、算力解构等；交易运营主要指面向用户、服务商以及管理者的算力门户/商城及运营管理和社区服务；统一门户则通过认证、鉴权等方式实现一站式登录管理。

#### 可信数据

算力服务平台运行过程中会产生大量用户数据、交易数据、计算数据、运营数据、监测数据、日志数据等，为保障数据安全和可信交易，需采用国产数据库软件进行管理，并结合分布式存储系统进行数据分布式存储。

#### 算网编排

算网编排服务作为算力服务平台的支撑层，是算力服务的核心能力，建设能力包括资源接入与调度、资源封装、智能匹配和算力解构。

##### 资源接入与调度

###### 资源接入

根据具体算力服务的业务场景，支持三种接入方式，包括资源层接入、平台能力层接入和用户服务层接入。

（1）资源层接入

在资源层接入，指对算力中心计算、存储等资源进行直接纳管。需在算力中心部署资源管理平台、调度系统以及调度服务相应的应用、工具和数据，实现对资源的直接纳管。

（2）平台能力层接入

平台能力层接入，指使用完全权限打通或使用代理服务的方式，与算力中心内部平台打通认证与资源调度权限。

* 完全权限打通

当算力中心已具备资源层划分、算力调度能力并能够开放足够的调度和业务权限，如用户登录、认证、调度等服务，能够提供算力调度所需应用缓存、计算、存储等能力和资源，算力服务平台能够将用户需求打包封装并在算力中心进行远程部署，由算力服务平台和算力中心相关平台打通接口，实现算力服务平台在云端直接调度算力中心资源。

* 代理服务

当算力中心不愿意开放足够的调度和业务权限，仅提供登录认证、查看等权限，不能实现算力调度时，则需在算力中心部署代理服务，即轻量级算力管理平台，包括Nginx、Redis服务、应用仓库、数据库、数据转发服务等。

在使用代理服务时，不考虑在算力中心部署服务器，由算力中心提供代理服务部署所需的计算存储等资源进行部署。算力服务平台应能提供代理服务部署所需的软件、工具等，在需要进行部署时，在各个算力中心进行部署、调试。

（3）用户服务层接入

针对用户服务层级的接入，指通过API接口方式与算力中心相关平台进行应用级对接，实现对算力中心的算力和应用调度。

**根据调研情况，本项目拟主要采用平台能力层接入，根据算力中心权限开放情况，进行完全权限打通或使用代理服务，同时制定接口标准接入算力中心资源。**

###### 资源调度

建立或打通各算力中心资源池，为方便管理及调度，根据算力特性进行一致性管理和属性标注，将单资源池定义为同构资源。根据任务的优先级、业务特征和资源池特点等因素进行任务分配和调度，动态地将任务分配给可用资源，并优化任务的执行顺序和并发性，以最大程度地提高计算效率。

采用Slurm、K8S等资源调度工具，统一协调高性能计算作业与智能计算作业分发与管理，结合综合监测平台能力，针对不同类型资源池进行监测以及任务的分配与执行，能够根据算力需求进行指令发布，包括资源的申请、分配、释放等功能。从环境感知、调度策略、数据分布、资源池规模等方面进行协同，满足作业分发路由清晰、计算资源可靠、运行稳定、任务可容错的要求。利用平台负载均衡能力，将需求合理进行分配，支持屏蔽异构资源差异，统一抽象定义资源特征，实现多个域之间的资源共享和协同，以及跨域的任务调度和执行。

##### 资源封装

###### 资源池封装

对不同算力中心的计算、存储、网络等资源进行封装，聚合异构资源形成一个资源池；面向用户时，不体现算力资源来源，有算力需求时，能够按照资源调度策略进行智能分配和调度。

###### 算力加工

对封装形成的算力资源池进行划分，匹配智算或超算应用软件，结合四川行业特性和实际需求，将算力资源和应用进行深度绑定，形成定制化的算力产品，即面向行业应用的专用算力，此部分算力资源则固定为对应的产品提供服务。项目前期主要面向特定用户需求时，进行临时的算力加工。

在本项目，拟面向智慧交通、智慧城管、智慧园区、气象环保、生物医药等领域提供专用算力，详见下表：

专用算力应用领域

| **序号** | **行业类别** | **专用算力属性** |
| --- | --- | --- |
| 1 | 智慧交通 | 通过将智慧交通领域相关的AI等软件与算力进行加工绑定，实时监测基础设施状态、各类交通事件、人车流量等关键数据，动态分配路权，智能诱导交通，为城市交通规划、政策制定、建设施工、设施运维、源头监管等工作提供有力支撑 |
| 2 | 智慧城管 | 通过将智慧城管领域相关的AI等软件与算力进行加工绑定，以城市级计算服务数据中心为基础，搭载合作伙伴的智能AI算法与应用，统一在云端完成视频资源汇聚、解析，支撑业务应用闭环，实现城市管理可视化、日常监控网络化、技术应用智能化。 |
| 3 | 智慧园区 | 基于算力服务平台的强大计算资源，搭载智能软件，实现园区综合安防、便捷通行、资产管理、设施管理、能效管理、环境空间管理等智慧化应用，为客户打造可视、可管、可控的园区。 |
| 4 | 气象环保 | 通过将气象专业软件与算力结合，解决环保应用中常用模式如WRF、NAQPMS的计算特征分析为高核心、高内存带宽、低延迟网络通信及大容量存储资源需求。丰富的算力资源，助力产业升级、科研创新、政务服务和信息技术应用创新。 |
| 5 | 生物医药 | 通过将生物医药领域相关的专业软件与算力进行加工绑定，应用于医学检测、医学成像、大分子建模和计算机药物辅助设计等方方面面，可为生命科学相关领域研究提供全栈算力及云存储基础设施解决方案。 |
| 6 | 科研教育 | 通过将科研教育领域相关的专业软件与算力进行加工绑定，在物理、化学、材料、生物等相关学科中，利用高性能计算可以观察到比实验现象更细致的层次，对目前比较昂贵或无法实现的实验进行理论模拟，从而帮助解释实验结果，理解自然规律，进一步指导实验过程。 |
| 7 | 游戏行业 | 通过将游戏领域相关的专业软件与算力进行加工绑定，提供游戏服、游戏运营、云游戏等服务。 |
| 8 | 汽车行业 | 通过将汽车领域相关的专业软件与算力进行加工绑定，利用智能系统自动驾驶辅助企业数字化运营操作系统、自动驾驶云计算、虚拟化数据存储车联网、一体化调度云计算等。 |
| 9 | 人工智能 | 通过将AI应用与算力进行加工，生成虚拟主播、数字分身等，为新媒体销售提供虚拟客服服务，同时通过图像识别、人脸识别等技术衍生新型智慧应用场景。 |

###### 对外接口服务（2026）

支持能力封装和能力鉴权，将封装后的资源池进行整体打包输出，对外构建一致化API调用能力，与用户自有云资源一起提供算力支撑服务，实现混合云的服务模式。

##### 多云纳管

通过平台API接口对接，接入各个IDC云平台，进行多云纳管，使用单一的界面或工具来监控和管理多个云平台，并将IDC算力资源与超算和智算资源进行统一封装。

##### 算网感知

算力网络调度能力进行多要素智能编排与一体化运维，需要提供对业务与算网资源状态实时捕捉、理解以及预测的感知能力，因此感知是算网编排管理层实现智能编排调度、算网自智、数字孪生的重要基础能力。

通过算力注册、使用量监测、过往算力需求情况等数据，感知当前并预测未来一段时间内的算网使用情况。算网感知应具备动态的感知能力，对算网全领域环境进行感知，包括资源、性能数据的采集和分析，既包括静态环境数据的收集，也涵盖动态环境数据的感知，感知的数据包括对已注入的算力资源总量、已用量、未用量、资源负载、性能负载、网络质量、时延质量等实时数据进行统计。基于算网动态感知的能力，可以统计和展示算力任务的运行总量、任务运行状态、算力资源的分布、调度策略等能力，并具备自适应、自弹性、自愈的能力。同时，通过多云纳管，提供跨云平台的资源视图，了解其资源利用情况。

集中管理：对多资源池告警、性能、日志、容量和资源配置等进行集中监测管理。

统一呈现：采用拓扑、大屏、仪表盘等方式，实现资源可视化、运维可视化。

自动化巡检：支持自定义巡检脚本，能够输出巡检报告。

##### 算网质量

平台提供算网质量控制模块，能够根据算网感知的数据进行质量监测和故障处理，包括时延质量、网络质量和算力硬件质量等，确保用户使用的算网资源稳定可靠。

算网质量控制的目的就是为了提升用户的算网业务体验，提供高质量、高可靠、有保障的算网业务服务。当出现算网业务服务质量的下降和中断时，需要具备自动的调整和调度能力使故障自动恢复。

算网质量保障首先具备业务质量和故障的感知和预测能力，能够对算网业务的状态和业务质量进行持续的监控，及时发现故障或质量下降。同时，需要能够对未来可能出现的故障或业务质量下降进行预测，提前发现问题。其次算网质量保障需要具备自动决策、自动执行的能力，根据感知到的故障，根据决策模板能够自动、快速的给出分析结果和给出解决措施，转换为对南向专业域的调度或配置。

##### 智能匹配（2025）

根据平台上各类资源运行信息、作业排队信息、应用部署等情况，基于机器学习或深度学习的算法，智能匹配用户的任务需求以及资源优先级等因素，动态调配最优或最具性价比资源，提升资源调配效率，提升用户满意度。

同时采用基于业务的意图识别，用户通过主动输入算网资源需求，平台根据输入的需求对业务、需求、场景、网络的输入进行意图识别，将自然语言转化为具体策略。对于用户需求，意图识别模块需要将用户所要表达的意图准确识别出来，也可以通过平台预先定义的标准进行精准匹配，从而为后续的对话反馈提供重要的意图标签信息。

##### 算力度量

统一的算力度量标准是实现灵活调度多元异构算力资源的前提,但算力与水力、电力等能源不同，算力资源的复杂性决定了难以通过单一维度来量化算力算力资源的复杂性主要体现在三个方面。第一，由CPU、GPU等多种计算单元组成的异构处理体系难以进行标准化的统一；第二，除了计算单元，算力资源还包括网络、存储等多维资源，需要从多个维度进行算力资源的建模和评估；第三，不同行业、不同企业、不同场景对算力资源类型和需求量的要求存在较大差异，用户很难精准把握需要多少算力。因此，需建立统一的标准将算力业务需求量化，以提供更好的服务。

从业务场景维度出发，将总体的算力资源统一表达为包含计算、网络、存储等多维度资源在内的综合模型。通过模型分析，结合用户位置、业务需求等关键信息，对外生成面向用户的算力资源视图,对内生成算力资源清单和初始配置策略。

##### 应用注册

用户对应用的访问，都需经过算力服务平台，用户只能访问在算力服务平台上已注册的应用。通过应用注册，用户进行应用上传，部署客户端或登录界面，明确路径、地址、权限等内容。当用户自己提供应用时，需要在算力服务平台进行注册并下发应用；当平台自带软件时，则直接使用或根据实际情况进行应用下发。

##### 算力解构

针对用户的算力需求，将应用软件和中间件、数据等进行封装，将用户的应用和环境打包成可移植的格式，使业务可以分布式地在不同的平台和设备上部署和运行，实现多设备并行计算，克服单设备资源能力有限的瓶颈，同时支持同构和异构算力的解构和分发。

#### 交易运营

##### 算力门户/商城

建设算力门户并提供商城服务，可实现平台介绍、政策推送、广告投放、产品交易等功能。

###### 产品目录

产品目录分为基础算力、应用软件、专用算力、云安全服务和算力服务等产品。根据不同的硬件类型或性能指标进行分类，显示网络时延、单价等信息。

基础算力

通过算力接入、多云纳管等方式，提供智能算力、超算算力、通用算力三种产品能力，涵盖计算、存储等算力资源（CPU、GPU、DCU、内存、存储等），推荐多种业务场景资源配置，也可以手动选择计费模式、算力架构、算力规格、算力数量、带宽、购买时长等需求。

应用软件

提供应用仓库，部署并向用户提供科学计算、人工智能、智能制造等所需的各类应用软件，支持不同类型应用的快速接入，实现应用发布、订阅、交易、部署、服务等多种能力。本项目初期拟通过合作模式引入并上架文献管理软件、办公软件、国产替代等应用软件。

具体应用软件规模，由合资公司与技术或运营服务商签订服务协议确定引入生态合作伙伴，进而明确应用软件类型及规模。

专用算力

针对客户的特定需求，将应用软件和算力进行封装，提供用户所需的定制化算力产品；同时按电子信息、生物医药、教育、人工智能等行业领域进行划分，提供行业属性专用算力产品。

云安全服务

与能投天府云云安全平台进行对接，将云安全平台进行能力封装，并在算力服务平台进行应用上架，对外提供云安全服务，包括云防火墙、云上网行为管理、云漏洞扫描、云Web应用防火墙、云流量分析、云日志审计、云堡垒机、云主机安全防护、云防毒墙、云数据库审计、云高级威胁检测、云入侵防御、云态势感知等服务。

算力服务（2026）

* 裸金属服务

为用户提供裸金属物理服务器并提供裸金属管理服务，适合运行高性能、高安全性或高定制化的应用程序。

* 容器服务

为用户提供计算所需的容器管理服务，如微服务架构应用、AI应用部署等，可对算力资源进行容器化管理，并能对客户直接输出容器资源。

* 云主机服务

提供在虚拟化环境中运行的主机服务，可以快速部署、扩展和管理，适合运行标准化、低成本或易变化的应用程序。

* 灾备/双活服务

通过整合通用算力，为用户提供灾备/双活服务，同时也响应东数西存的战略要求。

灾备：按照一定备份策略对用户数据进行存储，提供本地或异地灾备服务，确保重要信息系统的数据安全和关键业务可以持续服务，提高抵御灾难的能力，减少灾难造成的损失。

双活：备份双活指的是主备数据中心之间的一种备份方式，主备两个数据中心互为备份，并且进行实时备份。

备份双活通过将业务分类，部分业务以数据中心A为主，数据中心B为热备，而部分业务则以数据中心B为主，数据中心A为热备，以达到近似双活的效果。

###### 服务估价

制定定价策略，基于资源性能、市场竞争等因素制定价格，可针对不同用户的优惠措施进行调整。平台计费系统根据不同类型和规模的计算任务，采用不同的计费模式和标准，能够按小时计费、按天计费、包月包年计费等。用户可在线定向选择产品需求进行估价，也可根据智能匹配结果进行价格估算。

###### 服务申请

用户可根据确定的资源和价格，提交服务申请审批，审批通过后进行资源释放和调度。

###### 产品试用

具备产品试用功能，可根据初步确定的算力资源供给，为用户提供限时的试用服务。

###### 在线交易

根据服务申请审批结果生成订单，对接第三方支付平台，支持微信、支付宝、银联等多种支付方式，提供在线交易支付服务。同时支持使用算力券、积分兑付等进行抵扣。

###### 服务结算（2025）

通过打通成本、收入、分成等关键数据，提供结算申请、审批、支付等服务。

###### 用户控制台

为用户提供会员权益查询、订单管理、算力资源管理、运行监控、资源扩容、续费、投诉、评价等服务。

###### 服务商控制台

向算力和应用服务商提供入驻与清退、资源管理、订单管理、分成结算等服务。其中资源管理可提供算力资源新建、重置和删除等功能。

##### 运营管理

###### 运营分析

提供可视化服务功能，对经营数据进行实时分析，生成图形报表，并进行趋势决策分析，包括产品销售数据分析、营销活动效果分析、客户满意度调查分析、成本控制与盈利分析、平台稳定性与性能分析和用户留存与流失分析。

* 产品销售数据分析

统计各类产品的销售额、销量、库存等数据，分析各产品的市场表现，找出热销产品和潜在爆款，以便调整产品结构和定价策略。

* 营销活动效果分析

对各种营销活动效果进行数据分析，评估活动对销售额、用户增长、品牌知名度等方面的影响，以便优化营销策略。

* 客户满意度调查分析

通过问卷调查、用户评价等方式收集用户对算力商城的满意度反馈，了解用户在使用过程中遇到的问题和建议，以便改进产品和服务。

* 成本控制与盈利分析

通过对运营成本和利润进行分析，评估盈利能力，以便调整经营策略和提高盈利水平。

* 用户留存与流失分析

通过分析用户的活跃度、成交率、复购率等数据，了解用户的忠诚度和流失情况，以便采取措施提高用户留存率和降低流失率。

###### 后台管理

面向运营管理者提供用户管理、权限管理、服务商管理、内容发布、审批管理、资源管理（包括产品发布、产品下架等）、订单管理、资金管理、调度管理、告警管理、定价管理等服务。

用户管理

平台用户管理功能主要提供用户注册、登录、查看、移除账号等功能。用户管理功能是平台的基础功能，为其他功能提供用户身份认证和授权服务。用户管理支持普通用户、团队等多种用户管理，平台接入多域算力资源后，满足平台用户的统一登录，多域资源使用的场景。

用户均有所属团队，团队设置团队管理员，支持团队管理员新增或邀请用户，实现团队级的用户添加和移除管理。平台管理员可以设置团队的有效期，管控用户资源使用。

用户登录功能允许已注册的用户在平台上登录，以便使用平台的其他功能。

权限管理

平台支持角色管理和菜单权限管理，实现平台级的用户权限灵活管理。初始角色可分为普通用户、运营管理员、运维管理员、超级管理员等。

普通用户主要进行作业提交、服务申请、账号注册等功能；

运营管理员负责管理资源、资源审批，管理系统中所有计算资源和作业信息；

运维管理员负责系统基础环境、作业调度环境、业务环境运维，进行相关环境健康检查；

超级管理员可以管理角色和菜单权限，支持给各个角色分配菜单权限。

服务商管理

平台可以统计算力资源服务商和应用服务商的基础信息，并能统计分析每个服务商的上架情况和交易服务情况，可以清晰掌握各个服务商的活跃度和服务质量等。

内容发布

运营管理员可通过平台进行政策、活动等内容发布，支持线上网页和短信同步推送。

审批管理

平台可设置审批环节和相关责任人，对服务申请、资源上下架、内容发布等进行审批。

资源管理

提供资源管理模块，管理者可清晰掌握已上架资源的来源、种类、规模、单价以及使用情况，支持报表导出。

订单管理

管理者通过订单管理，能够按周期统计订单数量、金额等交易信息，支持报表导出。

资金管理

管理者能够通过平台按周期统计交易额、营业收入、支出等情况，支持报表导出。

调度管理

能够根据用户需求，进行算力调度任务指令下发。

告警管理

通过告警管理模块，能够对平台自身运行情况进行监测预警，同时对算力资源使用情况进行监测，当资源使用达到阈值，进行告警。

定价管理

定价管理模块提供相关资源的定价标准设置，实现对上架的资源进行统一定价。

##### 社区服务（2025）

建设社区服务板块，发布服务场景案例、行业知识、常见问题及解答等内容，开设培训课程，聚焦专业领域合作伙伴，邀请行业专家入驻，用户可发布问题或需求，由管理者或专家提供咨询服务，以论坛形式帮助用户增长知识、解决问题。通过答疑解惑，提升用户参与度，同时助力用户精确匹配需求，促进科技成果转化，实现社区服务反哺算力服务平台。

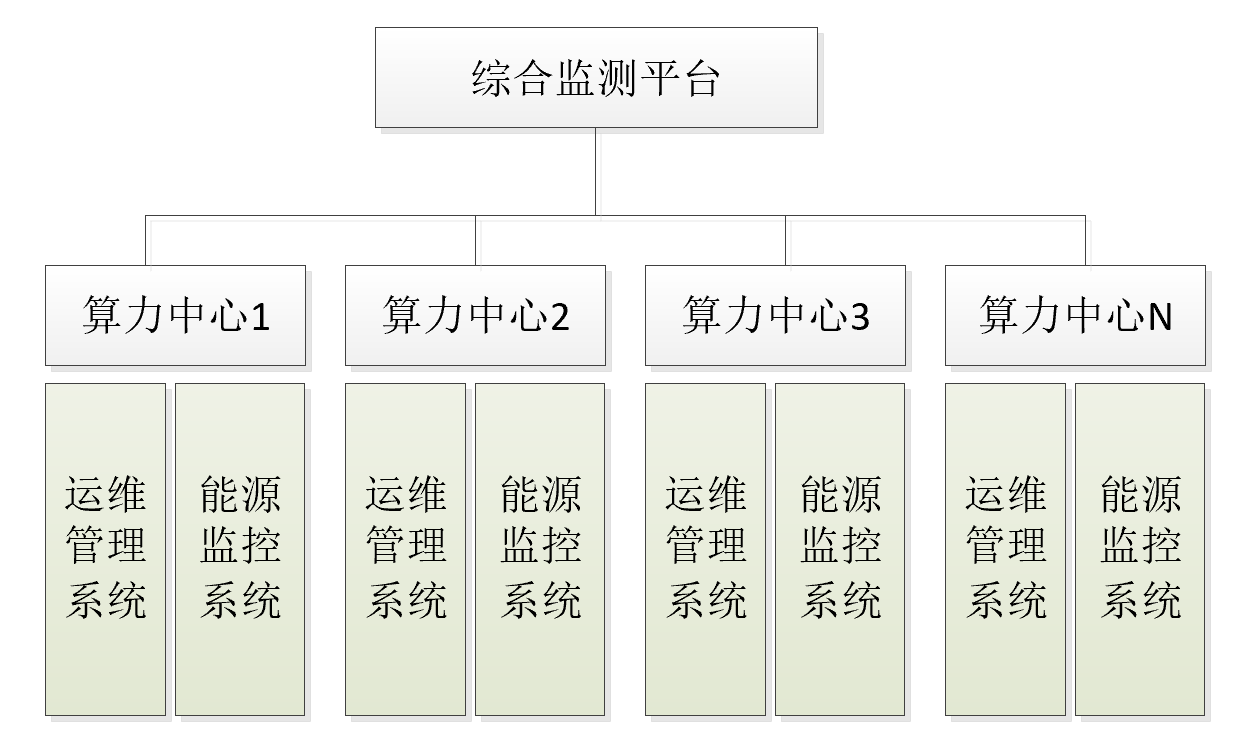
#### 统一门户

平台提供提供系统集成、统一认证和统一鉴权服务。系统集成。建设本项目平台的统一门户，页面集成各业务系统，实现单点登录。账号登录后，点击各个业务系统，可直接进入各业务系统的界面，进行系统操作。统一认证。实现用户登录管理，提供统一token，进入各业务系统时传递token到各业务系统。各业务系统解析token，获取平台的用户id，对应各自系统中的账号。统一鉴权。提供统一的鉴权接口，供各业务系统调用；业务系统传递token，校验登录状态，接口返回正常、异常状态。

| **序号** | **对接系统** |
| --- | --- |
| 1 | 综合监测平台（运维监测、能源监测） |
| 2 | 一体化安全保障平台 |
| 3 | 政府算力券、科技创新券相关管理平台 |
| 4 | 各算力中心算网资源相关平台 |

### 综合监测平台

#### 系统架构



综合监测平台架构

建设综合监测平台，平台与各个算力中心的运维管理系统和能源监控系统（动环监控系统）进行接口适配，通过一定权限，获取对应系统的相关数据，进行汇总、分析、展示和预警，实时掌握各个算力中心接入的IT设备运行情况以及算力中心整体的能源使用等情况。

#### IT设备运维监测

本项目拟对能投天府云因本次工程新增的IT资源进行监管，针对其他算力中心则通过接口方式获取接入资源相关的运维监测数据。

通过平台对接和直接监测等方式对算力中心IT资源进行实时监控，主要涵盖网络设备、安全设备、服务器、存储、虚拟化（虚拟主机和子机）、数据库、中间件等。系统需具备数据分析与挖掘能力，实现故障预判与工单推送、匹配智能知识库；能够全面直观展示各资源运行状态；能够结合各类型日志、流量、进程、端口等数据，精准定位，分析及预防故障，保障资源稳定运行。

统计和展示算力服务平台任务的运行总量、任务运行状态、任务资源分布等数据。实时监测任务运行对应的算力资源运行情况，反映任务运行健康度（对应的服务器、网络、安全等运行是否正常，对多个运行设备进行综合评价）和繁忙度（对相应设备的线程数、端口流量等信息进行综合评价）。

##### 网络管理

支持对符合SNMP协议的网络设备进行监测和远程重启等操作，包含设备的名称、ip地址、mac地址、厂商、运行时间、描述信息、ICMP、内存利用率、CPU利用率等基本信息。能够自动发现设备的网络接口，自动过滤虚拟接口，能够监测到接口的状态、类型、索引、名称、输入输出流量、输入输出速率、输入输出利用率等信息。能够自动发现设备之间的连接关系。支持自定义方式扩展其它指标项。能够自由配置设备背板，可根据设备物理接口数量，自动生成设备背板。

##### 安全管理

对符合SNMP协议的安全设备进行监测，包含设备的名称、ip地址、运行时间、描述信息、Ping时延、内存利用率、CPU利用率等基本信息。能够自动发现安全设备的接口，能够监测到接口的状态、名称、输入输出流量、输入输出速率等信息。

##### 服务器管理

对支持snmp协议服务器的监控，监控多种主流操作系统以及远程重启等操作。支持服务器的名称、ip地址、mac地址、系统类型、运行时间、描述等基础信息。服务器的运行指标包括存储使用情况、ICMP、物理内存、虚拟内存、CPU、进程、接口指标运行服务等指标使用情况。CPU包括多个CPU中每个CPU的实时负载情况；磁盘包括逻辑分区的分区容量、使用率等。系统能够支持通过自定义SNMP OID 脚本，采集特殊的服务器特殊指标项。

##### 硬件管理

基于IPMI、ILO等标准协议实现对服务器硬件监测功能，包含电源状态、磁盘状态、内存状态、CPU状态、风扇状态、温度等指标项的监测。

##### 应用支撑管理

支持对数据库、中间件、容器进行监测管理。

##### 存储管理

通过SMI-S、SNMP协议、接口等多种方式，对存储设备进行集中式管理。包含存储名称、设备IP、容量、使用率、控制器状态、磁盘组状 态等信息的监控，通过在策略中调整阈值大小，能够对受监控设备当发现异常性能数据超过设定阈值时，能够进行主动报警。

##### 虚拟化管理

对接虚拟化管理平台，采用一站式登录访问控制虚拟化管理平台的方式来控制虚拟机。包含对主机资源池情况的监测，包含主机cpu、存储、内存等资源的分配情况。同时可查询到子机系统名称、IP地址、mac地址，包含状态、资源使用率、操作系统性能指标。

##### 业务应用管理

支持以列表形式查看整体业务的运行时间、健康度、繁忙度和设备数量。

根据用户需求和模型灵活定制业务展示，可快速地看清楚整个业务的基础架构逻辑架构图，清楚的反应业务中各个节点资源的工作状态，可通过颜色可直观反应资源与链路性能负载的分布情况，同时终端线路、网络、主机、数据库、存储、应用在一张图上体现。

对业务服务应用进行监控，包括Tomcat、JAVA应用程序后台服务、业务服务应用状态的实时监测，判断是否正常运行（是否启动、是否掉线等），如有异常自动预警。

##### IP地址管理

系统支持自动对全网进行发现，并发现全网终端设备。实现将IP地址、MAC地址、上联设备的IP地址和端口一一对应，通过查看IP-MAC-PORT 3者之间的绑定关系，包括 IP 地址与MAC 地址的关系，MAC 地域与交换机端口的关系，同时还能由 IP 地址查找到该 IP 的 MAC地域及该 IP 所连接的交换机端口。可以查看基准表信息、实时表信息、实时表与基准表信息比较后的差异信息、差异处理信息等，并显示上下行流量，终端的采集时间，方便运维人员快速定位到终端的位置，并快速处理故障，并能对终端进行快速拓扑定位。

系统支持地址分配，用户可自定义名称、描述信息、所属VLAN、地址段，并对该地址段内地址进行分配，分配时可记录使用人、部门等信息。自动计算地址容量、分配率等信息。支持以图形化的方式直观展现地址段的分配情况，鼠标移动可提示该地址的使用人、上联IP等信息。同时支持对IPV6地址进行管理，能够对IPV6地址和拓扑管理等具备与IPV4同样的管理能力。

##### 系统管理

提供日志管理、故障管理、工单管理、资产管理、值班管理、报表管理、巡检管理等内容。

##### 告警管理

对算网资源和IT设备运行进行监测，根据资源使用情况和设备运行情况，设定阈值，当超过设定值时进行自动告警并短信推送。按周期类别对告警数据进行实时统计分析，全面掌握算力算效运行情况。

#### 能源效率监测

##### 能耗数据接入

对接各个算力中心能源监控系统或动环监控系统，获取算力中心能耗相关指标。结合大数据分析和AI算法技术，实现能耗数据的实时采集、分析，提供能耗监控、用能分析、用能告警、成本分析及能耗数据上送至政府在线监管平台等功能。

使用大数据分析技术实现能源数据可视化、用能计量器具在线实时监测。对周期综合能耗、耗电总量进行统计，可实时了解能源能耗指标。支持地图定位展示、实时告警数量、当月累积告警数、累计已处理告警、告警情况统计、采集环境整体运行管理指标分析、计量器具在线情况汇总等功能，准确掌握算力中心能耗实时情况。

##### 能耗监测分析

算力中心能源利用效率指标是衡量算力中心能效的量化标准，可以反映算力中心运行过程中的电能利用情况，可作为算力中心设计和运维优化改进的重要依据和衡量指标。通过全面掌握各个算力中心的能耗状况，合理调配能源，建立能源使用预警机制，持续优化能源利用。

对算力中心总功率、负载率、不间断电源功率、PDU功率、空调和照明等功率进行监测，生成曲线图，实时展示监测数据，并与历史数据以及不同算力中心之间进行对比分析。

###### PUE分析

根据获取的各个算力中心能耗数据，对各个算力中心PUE值进行实时计算，可按年、月、日统计展示PUE值变化曲线。

###### 能源分析

能源分析是对数中心能源系统、能源消耗、能源安全进行深入的监视分析，分析的维度包括平衡维度、质量维度、安全维度、用能成本维度等。

能源成本及用量分析

支持开展总能耗分析及分项明细分析，总能耗分析可按年、月、日等时间段统计分析数据中心总能耗数据，分项明细分析支持。

按设备、设施分析对水、电、油等用能分别进行多维度能耗分析展示；

按能源类别进行分析展示，主要包括综合能耗占比以及主、辅、附、外供各分项的去年及今年的分项综合能耗曲线展示；

按能源种类进行展示，主要包括能源类别占比以及电、柴油、水分项的去年及今年的分项综合能耗曲线展示；

按设备维度进行展示，主要包括各主要用能设备的能耗占比以及各设备分项的去年及今年的综合能耗曲线展示。

通过能耗数据采集及建立符合特性的用能模型，实现能耗统计功能，支持按照年、月、日查询按整体（包括电、油、水等）或能源类别（如：电）的能耗统计数据，支持采用能源类别方式查询如主要生产、辅助生产、附属生产等年、月、日查询的生产用能的统计。

能源平衡分析

根据算力中心计量拓扑中各仪表的用量来统计上下级的用量差异率，通过差异率的异常来判断识别是否存在异常线损或者跑冒滴漏等情况，挖掘节能空间。

能源安全分析

对设备报警的统计，评价能源系统以及用能设备的整体健康度，提前识别安全隐患，减少安全事故。 查看报警信息详情，包括报警设备名称、报警设备类型、报警参数、报警类型、报警时间、报警等级、报警状态、恢复时间、确认时间、持续时间、负责人、报警阈值以及报警参数的曲线；查询周期内的报警信息根据报警等级进行数量统计，持续时间分布分析等。

电能质量分析

对每一条有计量监测的线路进行电能质量综合评价打分，对电压合格率、频率合格率、谐波畸变率合格率、三相不平衡合格率、功率因数合格率进行统计。

###### 能源报表

对算力中心的能源消耗量、产量等进行分析及管理。以报表形式呈现各类能源数据，并支持报表导出。解放手抄报表的人工成本，提高核算精度。报表服务包括用能报表、工况报表、安全报表及计划报表。

###### 碳管理服务

在双碳政策下，对碳指标的管理将成为重要的一个部分，包括碳核查、碳排放量的计算、碳指标的管理、碳排放权交易等。通过设备的自动采集、人工录入等多种方式采集数据中心能源碳排放数据，进行能源用量数据汇总并生成碳排量报表，按阶段（日、月、年）查询能源碳排量消耗，可根据每阶段的碳排消耗报表进行统计、汇总上报。

##### 告警管理

对各个算力中心能耗进行监测，根据能耗使用情况，设定阈值，当超过设定值时进行自动告警并短信推送。按周期类别对告警数据进行实时统计分析，全面掌握能源利用率。

### 建设计划

该项目分3年，按照2024年搭框架，2025年功能完善，2026年全面形成服务能力的路径进行建设。

#### 2024年建设计划

2024年底前，完成平台的基础架构和主体建设并上线运行，为整个项目提供坚实基础，接入成都超算中心、智算中心、能投天府云数据中心以及达州、雅安等5个算力中心的算力资源，并引入一批应用服务商，初步形成算力调度、交易等服务能力；同时初步建成综合监测平台，对算网和能源进行实时监测和趋势研判；另外由“全国一体化大数据中心体系云安全能力平台（四川）”提供安全保障服务。

2024年计划建设清单表

| **序号** | **一级功能** | **二级功能** | **三级功能** | **四级功能** |
| --- | --- | --- | --- | --- |
| 1 | 可信数据 | / | / | / |
| 2 | 算力编排 | 资源接入与调度 | 资源接入 | / |
| 3 | 资源调度 | / |
| 4 | 资源封装 | 资源池封装 | / |
| 5 | 算力加工 | / |
| 6 | 多云纳管 | / | / |
| 7 | 算网感知 | / | / |
| 8 | 算网质量 | / | / |
| 9 | 算力度量 | / | / |
| 10 | 应用注册 | / | / |
| 11 | 算力解构 | / | / |
| 12 | 交易运营 | 算力门户/商城 | 产品目录 | 基础算力 |
| 13 | 应用软件 |
| 14 | 专用算力 |
| 15 | 机架资源 |
| 16 | 云安全服务 |
| 17 | 服务估价 | / |
| 18 | 服务申请 | / |
| 19 | 产品试用 | / |
| 20 | 在线交易 | / |
| 21 | 用户控制台 | / |
| 22 | 服务商控制台 | / |
| 23 | 运营管理 | 运营分析 | / |
| 24 | 后台管理 | / |
| 25 | 统一门户 | / | / | / |

#### 2025年建设计划

2025年，进一步丰富资源、功能和应用支持类型，以满足用户差异化的算力需求，能够实现用户需求智能匹配服务能力，并结合社区服务功能加强客户引流，同时计划新增接入8个算力中心资源和一批次应用资源。

2025年计划建设清单表

| **序号** | **建设平台** | **一级功能** | **二级功能** | **三级功能** | **四级功能** |
| --- | --- | --- | --- | --- | --- |
| 1 | 算力服务平台 | 算力调度 | 资源接入与调度 | 资源接入（增加8个算力资源接入） | / |
| 2 | 智能匹配 | / | / |
| 3 | 算力门户/商城 | 服务结算 | / |
| 4 | 社区服务 | / | / |
| 5 | 综合监测平台 | 平台整体功能优化 | | | |
| 6 | 增加8个算力中心监测接入，进一步优化平台功能。 | | | |

#### 2026年建设计划

2026年，全面建成平台功能，继续新增算力中心资源接入和一批次应用资源，优化资源供给能力，将资源进行深度融合并对外形成统一接口服务，提供混合云服务能力；持续跟踪用户使用情况，发现用户使用过程中的痛点，跟踪与分析系统数据，发现用户新增需求，根据问题及需求，持续迭代平台系统。

2026年计划建设清单表

| **序号** | **建设平台** | **一级功能** | **二级功能** | **三级功能** | **四级功能** |
| --- | --- | --- | --- | --- | --- |
| 1 | 算力服务平台 | 算力调度 | 资源接入与调度 | 资源接入（增加8个算力资源接入） | / |
| 2 | 资源封装 | 对外接口服务 | / |
| 3 | 交易运营 | 算力门户/商城 | 产品目录 | 算力服务 |
| 4 | 平台整体功能优化 | | | |
| 5 | 综合监测平台 | 增加8个算力中心监测接入，进一步优化平台功能。 | | | |

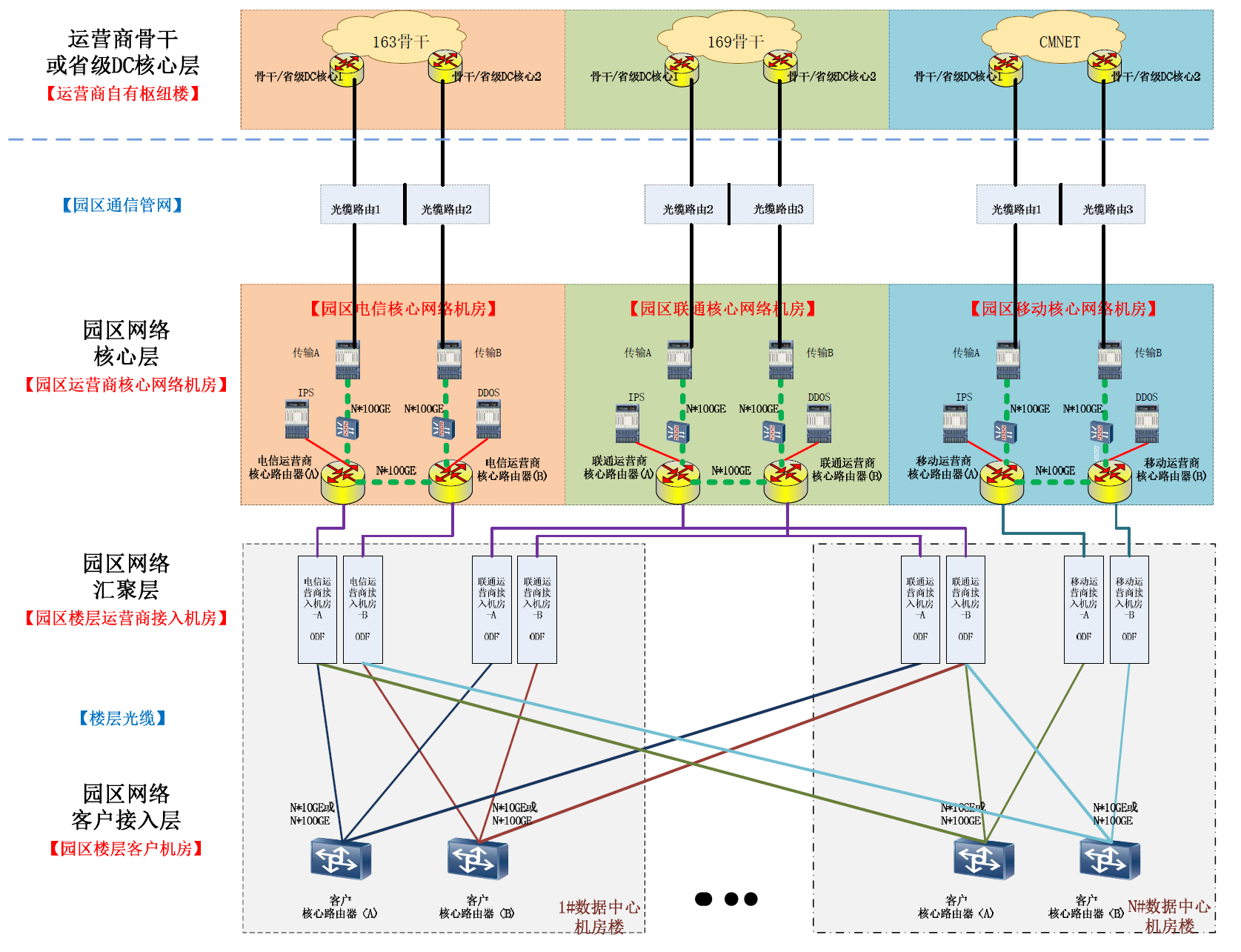
## 底座

### 机房环境

本项目部署于四川能投天府云数据产业基地，天府云项目已获取建设项目环境影响批复（简环评审[2022]27号）。四川能投天府云数据产业基地（一期）项目已完成建筑、安装、内装等关键节点的建设，目前已具备客户接入条件。

数据中心内将为算力服务平台建设提供机房物理环境，包括机柜、配电、暖通、消防、综合布线等基础设施条件，在安全保障方面提供等保2.0三级标准的安全系统以及一体化安全保障平台服务。具体在机房内需部署防火墙、WAF、流量监测，以及运维管理需要的数据库审计、日志审计、堡垒机、漏洞扫描等专用安全设备，同时为保障平台与各个数据中心之间的数据安全，部署包括CA、协同签名网关、密码机和密钥系统等密码服务的专用设备。

数据中心目前有3条骨干专线接入，包括1条移动、1条电信、1条联通。在每个机房楼配置有2台核心路由器，本项目新增设备就近接入2台核心路由器。



能投天府云网络现状架构图

本项目在能投天府云中心内部署设备，需租赁IT机柜，相应需求如下：

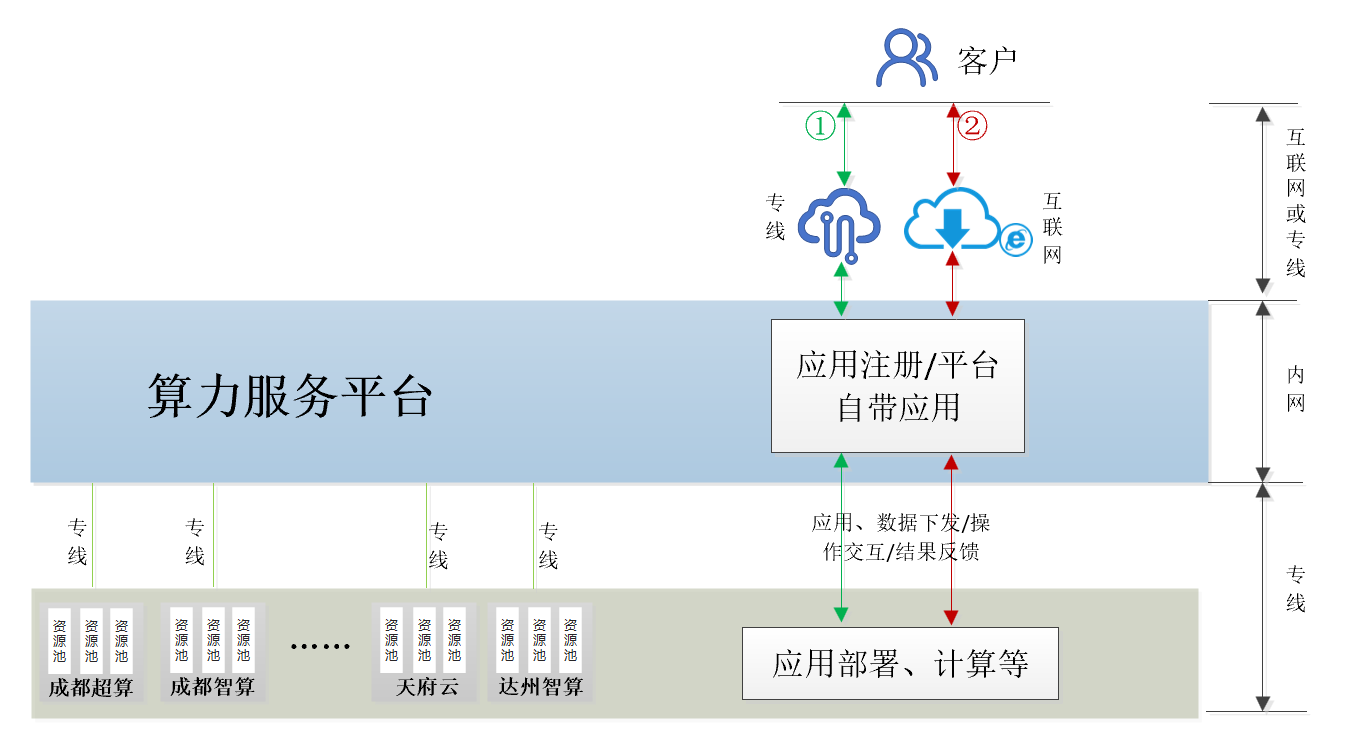
机柜空间需求表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **设备名称** | **空间需求/台** | **数量** | **空间需求** |
| 1 | 核心交换机 | 8U | 2 | 16U |
| 2 | 业务交换机 | 1U | 2 | 2U |
| 3 | 管理交换机 | 1U | 2 | 2U |
| 4 | 存储交换机 | 1U | 2 | 2U |
| 5 | 带外交换机 | 1U | 1 | 2U |
| 6 | 负载均衡 | 2U | 2 | 4U |
| 7 | 云管理节点服务器 | 2U | 2 | 4U |
| 8 | 虚拟化服务器 | 2U | 23 | 46U |
| 9 | 存储服务器 | 2U | 7 | 14U |
|  | 合计 |  |  | 92U |

根据设备存储空间预估，共需92U高度的机柜空间，按照一个机柜42U测算，考虑空间散热，一个机柜摆放20U，故机柜数量=92U/20≈5个。

### 网络系统

#### 网络带宽



用户访问示意图

（1）客户侧利用互联网或专线访问和控制算力服务平台，算力服务平台出口互联网带宽需求1Gbps以上，专线带宽需求200Mbps以上；

互联网带宽需求：本项目网络出口带宽按1000个客户同时访问平台测算，单次访问数据量按100KB，则业务访问所需带宽：1000\*100K\*8=800000Kbps≈800Mbps；预留200Mbps带宽作为扩容；则本项目所需带宽为1Gbps。本项目所需互联网带宽需向能投天府云数据产业基地申请带宽流量。

专线带宽需求：用户利用专线网络进行大量数据传输，且需要低时延特性，为保障客户使用效果，建议采用200Mbps以上带宽。该网络仅在用户有专线需求时进行建设。

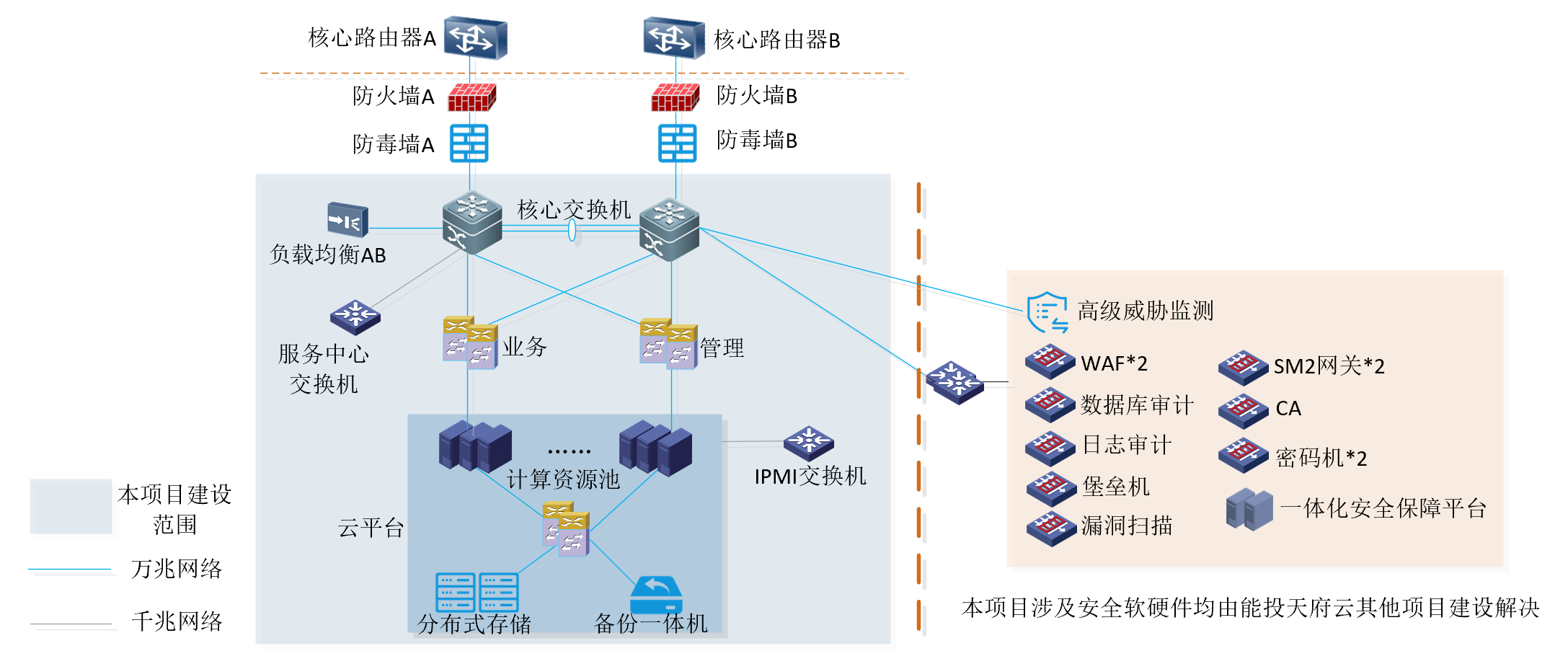
（2）算力服务平台与各个算力中心之间通过专线进行互联互通，按照200个客户同时访问一个算力中心进行测算，所需带宽：200\*100K\*8=160000Kbps≈160Mbps以上，为保障平台和算力中心之间的偶发性的大数据并行传输和低时延性，专线带宽建议200Mbps以上。经调研，该专线由算力中心负责打通。

#### 平台内部网络架构

本项目在能投天府云数据机房内新建IT设备，配套网络系统主要包括核心网、业务网、管理网、存储网。

新建2台核心交换机，上行就近接入原有核心路由器，下行接入本项目新增服务器、存储等设备；新建2台业务交换机和2台管理交换机用于云平台业务和管理数据交换；新建2台存储用交换机，用于存储设备接入；新建1台IPMI交换机用于对服务器进行运维管理；新建1台接入交换机用于接入服务中心内大屏相关设备。

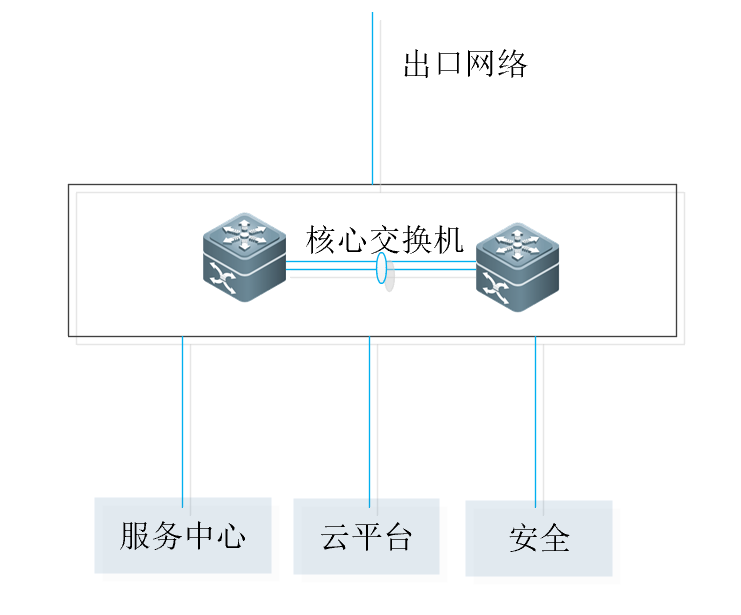
配置2台负载均衡通过服务器、链路、全局负载技术，提供业务分配、SSL加速、压缩功能及保障业务应用稳定可靠，提高业务体验。



网络系统架构图

备注：涉及安全接入的交换机由其他项目解决。

#### 核心网



核心网架构

核心交换机作为本项目网络架构的中心，新建2台核心交换机，下行接入服务中心、云平台和安全网络，上行实现网络出口与路由器相连，按照堆叠和主备等策略进行配置。提供外网与内网数据的高速交换、安全路由策略快速下发、高性能IPv4/IPv6业务能力、面向云数据中心化技术，控制、管理、转发三平面安全保障机制。

新建1台千兆服务中心用交换机，用于接入服务中心内大屏相关设备。

#### 业务网

为了以后私有云扩展方便，新建2台业务交换机，用于接入私有云服务器，考虑到市场打开后业务数据量较大，且运行效率要求高等因素，汇聚交换机配置为万兆光口交换机。

#### 管理网

##### 带内管理

新建2台管理交换机，用于云管平台对云平台设备进行管理。用户通过管理交换机能够访问管理界面，向计算节点发送管控指令等管理操作。

##### 带外管理

新建1台千兆IPMI（带外管理）交换机，用于对服务器和交换机进行统一管理和监控，包括配置管理、故障排除、安全监控等功能。

#### 存储网

为接入分布式存储设备，需配置2台存储交换机，互为主备，以IP方式连接私有云宿主机和存储设备，实现存储数据的传输和交换。

#### 负载均衡

新建2台负载均衡器，使用光纤连接至核心交换机，通过服务器、链路、全局负载技术，将请求分发到多个计算和存储节点上，避免单个节点过载，从而提高整个系统的处理能力和吞吐量。确保每个节点都能够高效地处理请求，减少用户等待时间。

#### 网络设备配置

网络设备配置需求详见下表：

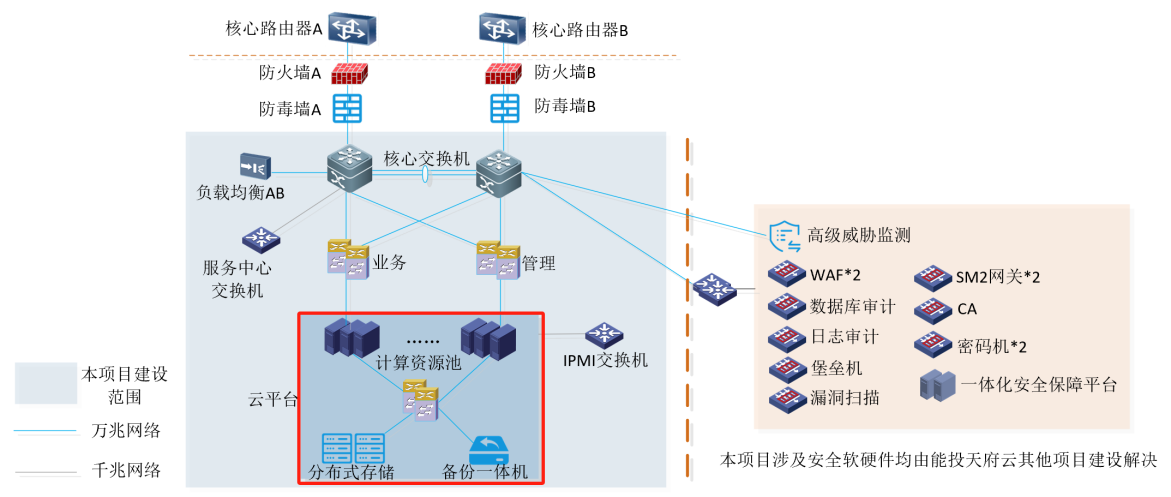
网络设备配置表

| **序号** | **名称** | **单位** | **数量** |
| --- | --- | --- | --- |
| 1 | 核心交换机 | 台 | 2 |
| 2 | 业务交换机 | 台 | 2 |
| 3 | 管理交换机 | 台 | 2 |
| 4 | 存储交换机 | 台 | 2 |
| 5 | IPMI交换机 | 台 | 1 |
| 6 | 服务中心交换机 | 台 | 1 |
| 7 | 负载均衡 | 台 | 2 |

### 计算存储

#### 系统架构

根据本次平台资源需求分析，采用私有云部署，服务器与存储设备各自独立，由计算资源池、分布式存储和备份一体机组成。适应本项目业务发展需求。

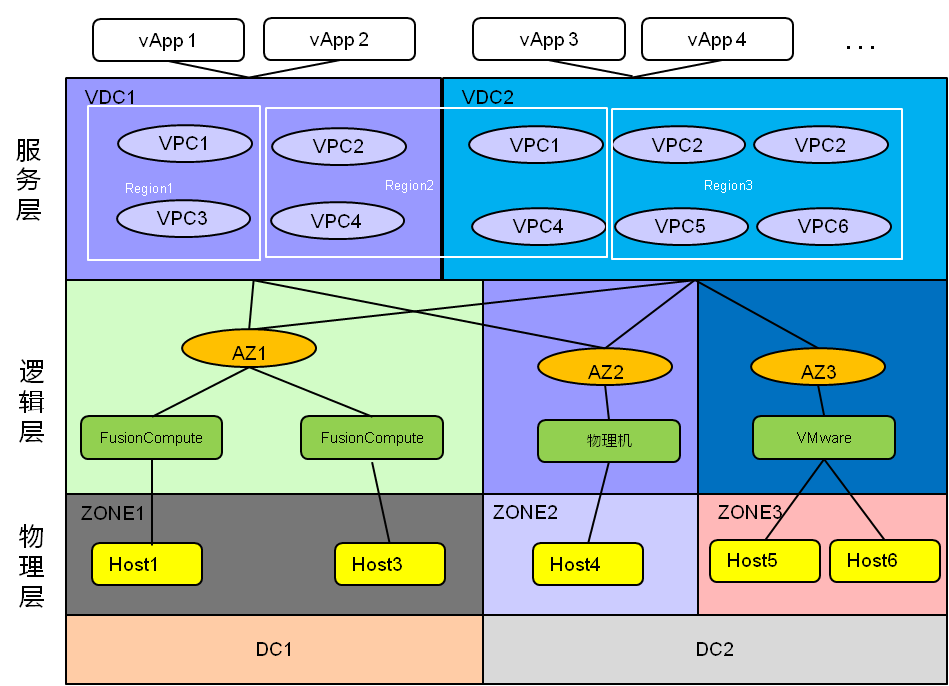


计算存储系统架构图

#### 计算资源池

##### 虚拟化平台

搭建计算资源池的核心是虚拟化软件，是运行在基础设施层和上层客户操作系统之间的虚拟化内核软件。针对上层客户操作系统对底层硬件资源的访问，虚拟化软件用于屏蔽底层异构硬件之间的差异性，消除上层客户操作系统对硬件设备以及驱动的依赖，同时增强虚拟化运行环境中的硬件兼容性、高可靠性、高可用性、可扩展性、性能优化等功能。通过将基础架构资源（包括计算、存储和网络）及其相关策略整合成虚拟数据中心资源池，按需消费这些资源。通过虚拟化管理软件的部署可以实现计算资源虚拟化，并对计算、网络、存储资源进行调度管理。



云计算资源池系统架构

云平台管理软件需具有以下功能特点：

（1）通过虚拟机HA、虚机热迁移、存储热迁移功能，能够有效减少设备故障时间，确保核心业务的连续性，避免传统IT，单点故障导致的业务不可用；

（2）易实现物理设备、虚拟设备、应用系统的集中监控、管理维护自动化与动态化；

（3）便于业务的快速发放，缩短业务上线周期，高度灵活性与平滑可扩展性，提高管理维护效率；

（4）利用云计算虚拟化技术可自动化并简化资源调配，实现分布式动态资源优化，智能地根据应用负载进行资源的弹性伸缩，从而大幅提升系统的运作效率，使 IT 资源与业务优先事务能够更好地协调；

（5）项目所采用的云计算虚拟化软件必须是成熟稳定且业界主流技术的软件系统，能够实现各子系统的计算资源和存储资源的动态伸缩和分配管理，便于按上层业务应用系统需求灵活分配资源。

虚拟化平台软件配置表

| 序号 | 名称 | 设备配置 | 单位 | 数量 |
| --- | --- | --- | --- | --- |
| 1 | 云平台软件授权 | 实现虚拟计算、虚拟网络、虚拟存储、高可用性（HA）、动态资源调度（DRS），46个CPU授权，云数据库服务授权，容器服务授权，云专家现场实施服务 | 套 | 1 |

##### 宿主机

根据对潜在平台供应商进行调研，算力服务平台和综合监测平台的计算需求如下：

计算资源需求表

| **序号** | **软件平台** | **虚拟机数量** | **Vcpu（核）/台** | **内存（GB）/台** | **总Vcpu（核）** | **总内存（GB）** |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | 算力服务平台 | 32 | 64 | 256 | 2048 | 8192 |
| 2 | 综合监测平台 | 6 | 64 | 256 | 384 | 1536 |
| 合计 |  |  |  |  | 2432 | 9728 |

共需要2432Vcpu和9728GB内存。

虚拟化宿主机建议采购计算型定制化服务器，结合本次主机服务器计算模型（如下表），得出本期新增建设的服务器规模，计算过程如下：

宿主机服务器计算模型

|  |  |
| --- | --- |
| CPU超配比建议值 | 2 |
| 预留处理能力比例（系统消耗+冗余） | 20% |
| 资源池单台PC服务器物理CPU数（颗） | 2 |

物理CPU核总需求=vCPU需求数/超配比\*（1+预留处理能力比例）=2432/2/1\*1.2≈1460核。

资源池虚拟化部分所需物理服务器数量=物理CPU核总数/单台物理服务器（单台物理服务器CPU按64核），所需物理服务器数量=1460/64≈23台。

单台物理服务器内存=总内存需求/服务器数量=9728/23≈423GB，内存配置512GB/台。

根据以上模型计算出计算服务器配置需求，同时设计4台服务器用于云管平台部署和管理，具体配置需求如下：

服务器配置表

| **序号** | **名称** | **设备配置** | **单位** | **数量** |
| --- | --- | --- | --- | --- |
| 1 | 云管理节点服务器 | 1、国产CPU：2颗，单颗核心数≥32；  2、内存：≥256GB；  3、配置相应端口和必要存储；  4、含操作系统。 | 台 | 4 |
| 2 | 虚拟化服务器 | 1、国产CPU：2颗，单颗核心数≥32；  2、内存：≥512GB；  3、配置相应端口和必要存储；  4、含操作系统。 | 台 | 23 |

#### 分布式存储

云资源池存储资源根据部署模式和提供方式不同可分为集中式存储和分布式存储两大类：

集中式存储：基于集中式部署的磁盘阵列提供存储，可提供块、文件存储，主流技术包括FC-SAN、IP-SAN、NAS等，通过硬件保障性能和可靠性，一般以Raid5方式实现冗余，安全性较高、响应速度快，但是存在单节点隐患；

分布式存储：基于通用/定制化服务器提供存储，可提供对象、文件和块存储，具备低成本、灵活扩容、高并发访问等优势，通过软件保障性能和可靠性，一般以保存3份数据实现冗余，可满足数据归档备份、大数据存储等需求，安全性很高，是目前云计算架构的主要存储资源提供方式。

本项目考虑到数据存储量安全性，采用分布式存储方式，按照3份副本进行保存。

##### 分布式管理系统

分布式存储需要分布式管理系统进行管理，实现数据的分布式存储，将数据分散到多个节点上，增强数据的安全性和可靠性。支持数据的自动备份和恢复。具有高效的查询和检索功能，可以快速地定位和获取存储在系统中的数据。

在分布式存储管理系统中，数据被存储在多个节点上，每个节点都有自己的存储空间。这些节点通过网络互联，形成一个整体。当一个节点发生故障时，其他节点可以自动接替它的工作，保证系统的可用性和稳定性。同时系统可用性是最重要的指标之一，需要保证在机器发生故障时，系统可用性不受影响，数据需要保存多个副本，并且多个副本要分布在不同的机器上，多个副本的数据是一致的，在机器故障引起某些副本失效时，其它副本仍然能提供服务。

分布式存储管理系统还采用了数据一致性技术，以避免数据在多个节点上出现不一致的情况，保证每个节点都能访问到最新、最准确的数据，从而保障系统的性能和可靠性。采用负载均衡技术，以实现数据在不同节点之间的均衡分配，避免单个节点的负载过大。

##### 存储服务器

根据对潜在平台供应商进行调研，算力服务平台和综合监测平台的存储需求包括系统部署和数据的存储需求，系统上线后初始存储按20TB计算，运行后存储数据包括访问数据、交易数据、用户上传数据等，按照日增50GB，前三年一定比例递增，每年数据量同比上一年增长20%，即：第二年对比第一年系数1.2，第三年对比第一年系数1.44，第四年开始稳定。按3年存储周期进行设计，预计存储空间：20TB+50GB/天\*365天\*（1+1.2+1.44）/1024≈85TB。考虑到用户特殊需求，可能有长期存储和临时大文件存储，按1.5系数测算，则总体存储需求为85T\*1.5≈128TB。

采用分布式存储，按照3份副本进行保存，则存储配置为128\*3=384TB。按市场通用配置，单块存储7.68T，每台服务器配置12块，则存储服务器需要384/（12\*7.68）≈5台，即采用5个分布式存储节点。

存储配置表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **名称** | **设备配置** | **单位** | **数量** |
| 1 | 分布式存储（含分布式管理系统） | 1.存储≥12块 7.68TB SSD；  2. 国产CPU：2颗，核心数≥32；  3.内存：≥512GB。 | 节点 | 5 |

#### 备份

本项目分布式的存储架构即使有多副本等手段保证数据的实时完整性，却无法保证数据的错误和损坏，比如人为删除，勒索病毒等问题带来的数据错误。为了防止整个分布式存储系统的宕机或出现重要数据丢失，需要建设备份系统，备份的意义在于使用与存储完全隔离的故障域来保护数据，分离的存储操作系统，不同的物理设备，不同的物理区域，以防止物理故障、逻辑故障等问题再次发生。保障系统运行安全，避免数据丢失，在机房内设置备份系统，按周期对重要数据进行备份，相关需求如下：

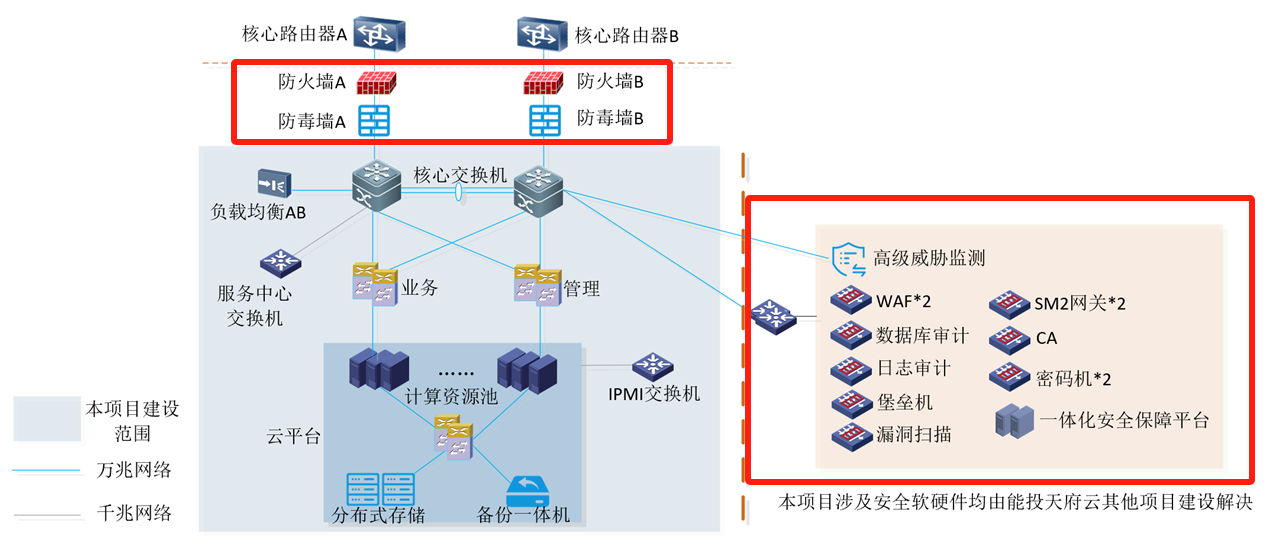
存储备份需求表

| **序号** | **备份系统** | **数据内容** | **每次备份量（GB）** | **备份频率** | **备份存储时长** | **备份存储容量（TB）** |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | 算力服务平台 | 应用和数据 | 200 | 1天/次 | 365天 | 71.29 |
| 2 | 综合监测平台 | 数据 | 10 | 1天/次 | 365天 | 3.56 |
|  | 合计 |  |  |  |  | 74.85 |

根据需求，配置备份一体机1台，容量不低于74.85TB，采用独立备份系统，支持本地存储、物理带库、VTL、SAN、NAS等存储；支持定时备份、副本数据管理、实时数据保护。

### 安全系统

#### 系统架构



安全系统架构图

由能投天府云数据中心提供安全相关的软硬件支撑服务，包括等保三级所需的硬件、软件以及国密SM相关的密码机、CA、签名网关等设备。防火墙和防毒墙用于边界网络串联接入，高级威胁监测系统通过核心交换机进行旁挂部署，其他安全设备通过配置交换机接入2台核心交换机进行部署。

#### 防火墙

在平台边界部署下一代防火墙，用于对内外网边界进行安全防护。

访问控制能力：集成防入侵、病毒过滤检测、失陷主机过滤检测、防泄密等应用层安全功能，通过单次解析引擎对进出IT资源接入区及安防、音视频区的所有流量进行深度威胁检测，在保证检测效率的同时确保访问流量的合法性。

漏洞防护功能：内置丰富的漏洞特征库与漏洞检测引擎，快速识别匹配主流的服务器安全漏洞和最新爆发的安全漏洞，例如攻击者常利用服务器高威漏洞RDP、SSH、SMB发起对业务的攻击，有效应对各类利用应用漏洞发起的网络攻击行为。

加密流量检测：具备精准的检测能力，及时发现IT资源接入区及安防、音视频区存在的僵尸主机，抑制网络中木马蠕虫等恶意软件的传播。通过漏洞安全防护功能，不仅将漏洞引发的安全风险拦截在业务区外部，而且有效解决安全漏洞难以及时修复的困境。

0day漏洞处置：威胁检测引擎应用行为分析检测能力，利用攻击泛化技术应对0day漏洞，对于新发现的漏洞通过规则库升级和虚拟补丁的形式在网络层对漏洞进行加固，防止漏洞被利用。

#### 防毒墙

在平台边界部署防毒墙，提供检测、防护、阻止恶意代码攻击的行为，包括蠕虫、病毒、勒索等攻击，以防止各类病毒的攻击造成系统瘫痪。

#### WAF

在服务器部署区内部署WAF防护，为WEB应用提供针对HTTP、HTTPS协议的安全检查，以保护WEB系统受到的应用层攻击。

#### 高级威胁监测

高级威胁监测系统，是利用海量的原始数据审计分析精准识别网络威胁，对内部的服务器进行自动识别，并且还能自动识别服务器上开放端口和存在的漏洞，弱密码等风险，0day漏洞处置，对于病毒、蠕虫、木马后门、拒绝服务攻击、各种服务器攻击、终端攻击、扫描攻击、SQL注入、XSS、缓冲区溢出、欺骗劫持等攻击行为以及网络资源滥用行为（如P2P上传/下载、CGI访问攻击、IIS服务器攻击、网络游戏、视频/音频、网络炒股）等威胁具有高精度的检测能力。同时，高级威胁监测系统的自定义应用识别规则库模块，可以通过参数的灵活设定，把关注的特殊事件作为自定义策略下发给引擎进行检测。对于网络流量的异常情况具有非常准确、有效的发现能力。

#### 数据库审计

SQL解析模块和数据库审计模块：主要实现对数据库服务器的数据流量的采集，提取用户对数据库操作的SQL语句。

安全规则模块：主要完成对安全规则的匹配，检测当前SQL语句是否存在风险操作。利用每一个插件，进行具体的规则匹配，得到相应的规则ID，最后，对全部匹配中的规则ID进行汇总。

策略模块：主要收集安全规则的匹配结果，并根据安全规则的匹配结果，进行动作。如记录日志、发送告警、拒绝连接等。

#### 日志审计

日志审计系统作为一个统一日志监控与审计平台，能够实时不间断地将来自不同厂商的安全设备、网络设备、主机、操作系统、数据库系统、用户业务系统的日志、警报等信息汇集到审计中心，实现全网综合安全审计。

可将日志审计系统放置在运维管理区，对被审计对象进行必要的配置，使得他们的日志信息能够发送到日志审计系统。管理员通过浏览器可以从统一认证与授权管理登录日志审计系统，进行各项操作。

#### 堡垒机

针对运维工作，提供集中提供账号管理、身份认证、访问控制、行为审计功能，解决在运维管理中出现的账号管理混乱、身份账号共用、授权控制不明确、操作行为不规范、事件责任无法定位等问题。

#### 漏洞扫描

对空间资产探测、系统漏洞扫描、Web 漏洞扫描、网站安全监测、数据库漏洞扫描、基线配置核查、工控漏洞扫描、大数据漏洞扫描、Docker 漏洞扫描、系统渗透测试、网络流量分析、源代码安全审计、离线弱口令扫描、木马病毒扫描、漏洞工单管理、视频监控安全检测、WIFI 安全检测、APP 漏洞扫描、Windows 安全加固、等保合规关联等。

#### SM网关

针对平台和各个算力中心以及用户之间的各类数据通信，提供对链路的通信加密改造，集成身份认证、访问控制和资源管理等功能。支持商用密码算法SM2、SM3、SM4，支持国密SSL规范GM/T 0024-2014。

#### CA

CA系统以硬件服务器形式提供，设计容量为 1 万张证书。它也是完整的 CA 系统，在系统结构上和大型 CA 完全一致，包括有证书注册模块、证书签发模块、证书发布模块、密钥管理模块等四个部分，提供完备的证书管理功能：

用户信息注册/签发；

用户信息更新；

证书恢复；

证书废除；

证书重发；

微软智能卡证书/计算机证书/域控制器证书签发；

证书注销列表（CRL）与 CA 证书下载；

内置 LDAP 服务；

同时，具备完备的产品管理功能，如系统备份/恢复、系统在线升级、系统日志查询、License 在线升级、管理员管理、网络配置等。

#### 密钥系统（密码机）

密钥管理系统用于管理加密数字证书的密钥对，对密钥对的整个生存周期进行全过程管理，包括密钥的生成、存储、分发、备份、销毁、归档、恢复以及司法密钥恢复等，支持 RSA、SM2 两种格式的非对称密钥。

密钥管理服务器从 CA 接收的密钥获取请求，密钥注销和密钥更新和密钥恢复请求，同时以 B/S 的模式对密钥管理系统管理员开放密钥管理服务：

当接收到密钥获取请求时，密钥管理子系统首先从备用库获取得到所需密钥对，送到加密机解密得到公私钥对，使用数字信封加密的方式加密后送还给 CA，然后将此密钥对从备用库中删除，放到在用库中。

当接收到密钥恢复请时，密钥管理子系统会从当前库查询得到所需密钥对，送到加密机解密得到公私钥对，使用数字信封加密的方式加密后送还给 CA。

当接收到密钥更新请求时，密钥管理子系统查询当前库得到当前使用密钥对，对其设置撤销标志，然后按照密钥获取流程获取新的密钥对送还给 CA。

当接收到密钥撤销请求时，密钥管理子系统查询当前库得到当前使用密钥对，对其设置撤销标志。

密钥管理子系统主要提供密钥恢复审核，密钥查询，手动密钥归档， 司法取 证恢复等密钥服务功能。

密钥查询功能可以查询某一用户的当前密钥情况和历史密钥状态。

密钥恢复审核是当用户从 RA 经过 CA 提出用户密钥恢复请求后，由密钥管理系统操作员进行审核，同意或拒绝。同意后，用户从 RA 执行密钥恢复动作，经 CA 向密钥管理系统提交请求后，密钥恢复模块恢复用户密钥，经 CA 向 RA 直至传送到客户端，安装到用户证书载体中。

手动密钥归档，指当还未到自动定时归档时间前，可以手动将已经撤销的密钥 归档到密钥历史库中。

司法取证密钥恢复指司法取证人员在密钥管理系统中申请，经审核后，由密钥恢复模块恢复所需要的密钥并记录于特定载体。

#### 配置清单

推荐部署内容如下：

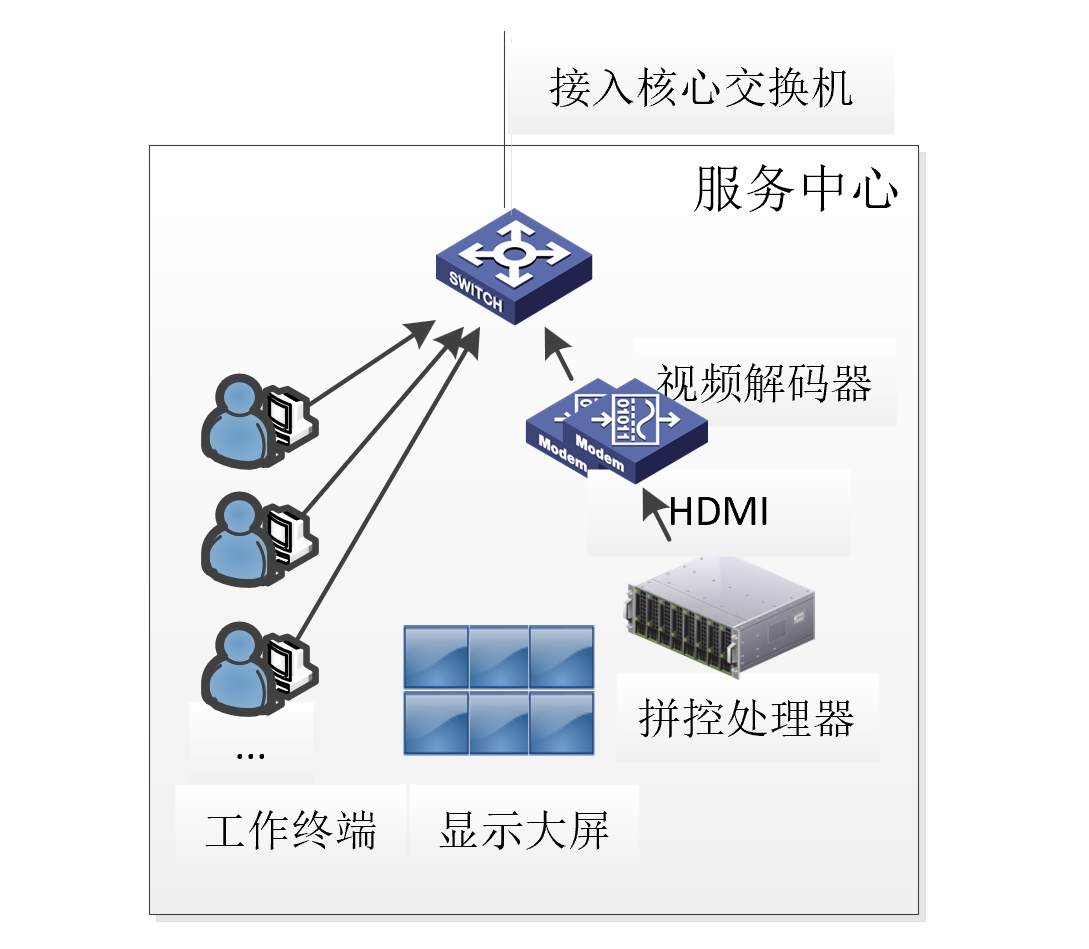
安全系统推荐配置表

| **序号** | **产品名称** | **功能** | **单位** | **数量** |
| --- | --- | --- | --- | --- |
| 1 | 防火墙 | 提供边界防护，对跨越边界的流量依据源地址、目的地址、源端口、目的端口、应用协议和应用内容进行控制 | 台 | 2 |
| 2 | 防毒墙 | 在网络关键节点提供检测、防护、阻止恶意代码攻击的行为，包括蠕虫、病毒、勒索等攻击。 | 台 | 2 |
| 3 | WAF | 为WEB应用提供针对HTTP、HTTPS协议的安全检查，以保护WEB系统受到的应用层攻击 | 台 | 2 |
| 4 | 高级威胁监测 | 针对高级持续威胁攻击（APT）行为以及勒索软件攻击行为进行全面检测，发现未知威胁。 | 台 | 1 |
| 5 | 数据库审计 | 对对数据库的各类操作行为、访问路径进行监视并记录，审计到操作人、操作时间、操作地点、操作内容及操作结果 | 台 | 1 |
| 6 | 日志审计 | 对安全设备、网络设备、服务器以及应用系统所生成的日志进行采集，实现安全数据的多条件组合查询，集中日志存储和审计功能 | 台 | 1 |
| 7 | 堡垒机 | 针对运维工作，提供集中提供账号管理、身份认证、访问控制、行为审计功能，解决在运维管理中出现的账号管理混乱、身份账号共用、授权控制不明确、操作行为不规范、事件责任无法定位等问题 | 台 | 1 |
| 8 | 漏洞扫描 | 对空间资产探测、系统漏洞扫描、Web 漏洞扫描、网站安全监测、数据库漏洞扫描、基线配置核查、工控漏洞扫描、大数据漏洞扫描、Docker 漏洞扫描、系统渗透测试、网络流量分析、源代码安全审计、离线弱口令扫描、木马病毒扫描、漏洞工单管理、视频监控安全检测、WIFI 安全检测、APP 漏洞扫描、Windows 安全加固、等保合规关联等 | 台 | 1 |
| 9 | SM网关 | 提供对链路的通信加密改造，集成了身份认证、访问控制和资源管理等功能。支持商用密码算法SM2、SM3、SM4，支持国密SSL规范GM/T 0024-2014。 | 台 | 2 |
| 10 | CA | 第三方CA机构签发的站点证书和个人证书 | 套 | 1 |
| 11 | 密钥系统（密码机） | 提供SM1、SM4、SM7、AES、3DES算法的ECB/CBC/CTR/GCM等模式的数据加密和解密运算。对密钥进行管理，包括对称密钥管理，非对称密钥管理，支持密钥生成、存储、导入、导出、使用、备份、恢复、销毁等全生命周期管理。 | 套 | 2 |
| 12 | 一体化安全保障平台（含服务器） | 包含数据采集、网络安全态势可视化、安全监管三个子系统。 | 套 | 1 |
| 13 | 交换机 | 用于接入安全设备及安全设备管理端口 | 台 | 2 |

### 服务中心

#### 系统架构

在能投天府云数字产业基地内建设服务中心，包括大屏、座席、扩声设备、工作终端以及装修、空调、配电等，相关设备通过1台交换机接入2台核心交换机。



服务中心系统架构

#### 大屏显示系统

大屏显示系统承担各类信息的显示，是一个综合多业务（视频、网络、计算机）信号的综合显示平台。通过显示系统能够直观、完整、准确、清晰、灵活的显示视频监控画面、各类管理图表和多媒体宣传等内容，便于及时作出判断和处理，实现实时监控和集中控制、监管指挥调度的目的。在功能上系统应支持单屏、多屏、整屏显示和跨屏显示，支持图像窗口缩放、移动和漫游等功能，支持多路数字画面和视频画面的完全实时显示。

##### 显示系统类型

室内各显示技术对比表

| 显示屏类型 | 液晶拼接（LCD） | 等离子拼接（PDP） | DLP拼接 | 投影融合 | 小间距LED显示屏 |
| --- | --- | --- | --- | --- | --- |
| 原理 | 背光源投射 | 自发光 | 光源投射 | 光源投射 | 自发光 |
| 物理拼缝 | 3.9mm | 1.8mm | 0.5mm-1.0mm | 无缝隙，有融合带 | 整屏无拼缝 |
| 均匀性与一致性 | 长期使用，单元间亮度与色彩衰减不一致，不可恢复。 | | 长期使用，单元间亮度与色彩衰减不一致，需专业人员重新调试。 | | 亮度、色度逐点可调，整屏均匀一致。 |
| 亮度 | 450-700cd/m² | 450-1700cd/m² | 200-400cd/m² | 投影机亮度&投影尺寸 | 50-2000cd/m² |
| 色温调节 | 5000K-10000K | 5000K-10000K | 5000K-9300K | 5000K-9300K | 2500K-10000K |
| 可视角（H/V） | 178°/178° | 179°/179° | 120°/80° | 依屏幕而不同 | 170°/160° |
| 刷新频率 | ≤120Hz | ≤120Hz | ≤120Hz | ≤120Hz | 960Hz-3840Hz |
| 声噪 | 25-30dB(A) | 25-30dB(A) | 30-40dB(A) | 依投影机而不同 | 无风扇，静音 |
| 7\*24小时工作 | 不建议 | | 支持 | 不支持 | 支持 |
| 平均功耗 | 170W-200W | 240W-450W | 140W-350W | 依投影机而不同 | 110W-230W |
| 光源寿命（不小于） | 6万小时 | 6万小时 | 6000-6万小时 | 依光源类型而不同 | 10万小时 |

通过上表，各显示系统主要技术指标比对如下：

（1）亮度：对于亮度而言，大厅面积较大，高清晰小间距数字LED显示系统幕前亮度可高达2000cd/m²流明，较其他屏接具备明显优势。

（2）受环境光线影响：由于高清晰小间距数字LED显示系统具有自发光的特性，屏幕表面没有加装玻璃体镜面，受环境光线的影响较小。

（3）物理拼缝：高密度LED显示系统和激光显示系统可做到没有可视物理拼接缝隙，虽然其他类型的拼接最小能做到0.5mm的物理拼缝，但在整屏显示时还是明显可见。

（4）可靠性：小间距LED相对具有寿命长，易维护的特点。

综上所述，小间距LED大屏整屏完全无缝，逐点可调、可校正。支持7\*24h不间断工作。本项目中选用小间距LED作为显示系统。

##### 系统组成



大屏显示系统图

LED显示系统组成主要由三大子系统构成：信号源子系统，中央控制子系统、LED显示屏子系统。

（1）信号源子系统

为整个系统提供播放所需的视频、动画及数码图像等各类信息素材，本项目输入设备包括：视频会议摄像机、视频解码设备、PC计算机/视频工作站等。

（2）中央控制子系统

作为整个系统的中央控制部分，视频处理器把不同的信号源数字化后，并对信号进行广播级的高品质图像处理，最后由信号线传送至LED显示屏（各厂商协议不同，具体的信号由建设厂商深化设计）。视频处理器可由一台装有视频显示系统控制软件的PC进行控制或移动平板电脑控制LED显示屏。

（3）LED显示屏子系统

各种输入视频源信号，通过中央控制系统处理后，传输到LED箱体上进行显示，同时LED箱体要安装在特定的钢结构上。

##### 系统功能

###### 信号显示

（1）网络信号显示

具有多网络连接功能，大屏幕上打开的网络窗口无限制。支持TCP/IP协议。图形可单屏显示，也可跨屏拼接或全屏显示，画面无延时，无抖动，刷新速度≥30帧/秒。工作站经网络将数据输入控制器后，无论计算机运行软件是何种分辨率，都会自动适应，并以同等分辨率显示，与原有工作站的显示屏幕及大屏幕的分辨率无关。

网络上的所有工作站均可在授权情况下利用所提供的控制软件对大屏幕进行信号切换、开窗等操作。

（2）计算机信号显示

通过RGB开窗方式，大屏上显示的内容同工作站上的内容完全一致。在大屏上能进行用户应用程序的操作，保证在大屏幕上对应窗口、图形操作等同于在工作站显示器的全部操作。

兼容任何分辨率的计算图形，图像光滑、无像素感，可兼容视频信号、数字信号和RGB模拟信号。

支持各种信号源输入的汉字在大屏幕上的正确显示，包括点阵汉字，矢量汉字，特殊符号等的屏间拼缝不会产生图形和文字错位现象。

（3）视频信号显示

全制式视频信号接收。

对于输入的视频信号具有局部放大功能。

采用视频图像增强技术使图像对比度、色彩度、层次感更高。

支持多种视频信号的同时显示。

对于多屏拼接控制器接收到的视频信号任一路可以任意大小显示，没有物理边界的限制，可以放大到整个屏幕墙，整个屏幕墙画面的刷新的速率小于1秒，速度可达30帧/秒。

（4）数字信号显示

作为高性能及高品质的图像显示产品，大屏幕显示系统在传输的过程中使用的是纯数字化的传输方式，支持以DVI、SDI的数字传输方式，避免了在A/D-D/A的过程中采用的量化、采样及编码的繁琐过程，保证了信号的完全输入，做到图像不失真、无杂波等，避免了一切影响图像质量的因素，做到图像清晰、完整的显示。

（5）信号综合处理

整个拼接屏作为一个没有分隔的虚拟屏，对所开的窗口不受物理拼缝的限制。可对多路输入信号（包括计算机、网络和视频）的画面进行任意进行灵活开窗显示，既可整屏显示，也可分屏显示，并能自定义显示画面的尺寸，完成多画面、多层次叠加，任意缩放、移动和漫游等功能，不受物理拼缝限制，实现分区或分屏显示时的多个窗口的联动的功能。

采用多通道的处理方式，使系统整体性能更加可靠。具有视频信号和计算机信号的直通显示功能。

系统对网络、视频及RGB信号具有相同的拼接能力，达到无缝拼接，并且拼接的图形比例正确，画面无延时，无抖动。

通过控制器显示的视频图像窗口、RGB窗口和网络窗口都可以同时显示，并能任意缩放、同屏、多路分屏、分区、整屏和跨屏混合显示，这些窗口之间可以覆盖，相互不受影响，完全动态实时，无延迟、无丢帧、无白窗。

在完成各类图像信号显示的同时还具有屏幕滚动字幕显示功能。

输入的网络画面信号均可放大到整个屏幕墙。

（6）显示效果及图像拼接

投影屏幕亮度均匀、显示清晰、图像失真小，单屏周边无眩光，色彩还原真实，具有高分辨率、可调亮度和对比度范围，在室内正常办公环境下能显示清晰明亮的图形、图像效果。

系统采用软件拼接技术保证分辨率叠加，使高分辨率、大容量图形能在整屏上清晰显示，并且当网络画面以最高分辨率整屏显示的实时画面刷新速率小于1秒。

支持多屏图像拼接，用户可在任意位置开启多个窗口显示网络画面，窗口画面可自由缩放、跨屏移动、不受物理拼缝限制，显示的窗口数量不受限制，并有足够的控制速度。所有类型的显示画面能从单屏显示按相应比例无级放大到全屏，图形不变形。整个屏幕亮度均匀，无暗角或亮角现象，画面稳定无闪烁。系统采用软件控制窗口的拼接与分割，屏与屏之间的拼缝不影响字符和图形的正确显示。

###### LED大屏控制器

LED拼接处理器是特别针对LED大屏的不规则拼接方式以及每个拼接显示单元的有效显示区等特性进行了独特的设计，大大简化了操作步骤，并使得显示效果显著提高。

拼接处理器集高清视频信号采集、实时高分辨率数字图像处理、三维高阶数字滤波等高端图像处理功能于一身，具有强大的信号处理能力。本款产品采用大容量高速FPGA阵列和CrossPoint数字多总线数据路由交换的处理机制，从根本上保证对所有输入信号源进行全实时处理和数据一致性，图像无延迟、无离散化、不丢帧，实现了图像的完美呈现。

处理器支持多种信号源输入模式，包括复合视频（DVD或摄像头信号）、电脑信号（VGA或DVI信号）、高清数字信号（HDMI或高分辨率DVI、DP、HDMI1.4信号）、网络IP信号等。对计算机视频信号，能兼容支持各种常见分辨率，并可实现自定义非常规分辨率。

拼接控制器可输出DVI-I信号、HDMI、SDI、HDMI1.4DVI双链、光纤或双绞线数字信号，支持RGB（模拟）/DVI（数字）同时输出，这意味着可以在大屏幕正常显示的同时，将信号备份输出至另一组大屏幕，部分型号还支持双DVI-I通道备份。

###### 软件功能

屏幕显示图像色彩柔和逼真，层次感和立体感强，采用单点亮度、颜色校正技术，亮度色彩显示均匀一致，实现真正色彩还原，达到广播级1024级灰度，即使屏体后期衰减也可通过现场校正再次还原，达到接近新屏的显示效果。

◆亮度与色彩校正

控制系统软件具有色彩校正功能，可以实现对整个显示屏幕的颜色和亮度的校正、同时也能对显示系统中多个屏幕中的某一个屏幕进行亮度和颜色的校正，或者对屏幕中某一个显示单元进行亮度和颜色校正。

在出厂时，所有的显示单元都经过了专业设备进行单点颜色的校正检测，并将检测数据存储在箱体内的记忆芯片中。在更换新箱体或颜色匹配不正确的时候，可以通过控制软件自动调整亮度、颜色设置，在整个使用寿命期间内都保持极佳的亮度和颜色的均匀性。

◆基于人眼非线性和TV非线性的γ变换和色空间变换

为满足不同环境及不同用户需求的显示效果，系统内置有20条γ曲线，并可分别调节三基色。γ系统可由最小1.5调整到最大3.0；由于人们习惯了多年来电视信号的色还原度，为使LED显示屏再现与阴极管同样的色调，系统内置了可编程的颜色校正算法，通过矩阵系统之间的关系实现颜色真实再现。

◆亮度

为提高屏幕的亮度，除了选择优质LED灯外，减小行扫消隐周期及场扫消隐周期，并采用恒流源驱动，最大限度地避免由于加大LED灯驱动电流带来的害处（寿命、功耗、发热）。

◆对比度

对比度是人工重显图像的关键技术指标，如果对比度达不到要求，图像重现的层次感和颜色感无从谈起。屏幕图像对比度至少要保证不小于200，才能获得较为满意的视觉效果。为了获得较高的对比度，我们采取了下面两种方法，使对比度达到了高等级。

提高显示屏亮度，这也是提高对比度最主要的方法

降低屏幕表面的光反射系数。对于屏幕表面光反射系数的控制，采用乌光黑色材料和黑色胶水封装像素，并且采用乌光黑色模组。

◆白平衡

同一块屏上所用的LED灯是同一厂家，同一亮度等级，同一色度等级。

箱体结构设计保证所有模块之平整度一致。

选择高等级的LED，一致性好。

由恒流源器件调整使每个模块亮度一致。

◆运动补偿和静态网络

在对视频图像处理上，我们使用了运动补偿技术以确保消除高速图像时所产生的拉毛、锯齿边现象。而静态网络技术更使得静态图像被网络准确捕获，更稳定地输出。这两项技术的采用使输出图像在专业级的概念上超过了电视显示的效果。

◆高速扫描

由于采用分布的控制，使系统的高速扫描成为可能。在我们最大限度地提高扫描频率的情况下，使我们的显示屏用人眼即使是专业的摄像机亦无法捕捉到帧闪烁，并且可根据用户要求采用逐点检测技术，以实现对显示屏状态的完全监控。

◆恒流源驱动技术

恒流源：顾名思义是一种恒定电流输出的驱动器件，它的交流等效电阻很大，直流压降却不大，其等效的数字模型是VCCS（电压控制的电流源），工作于开关状态，其电流输出一旦通过调节电阻设定后，仅受控于输入的逻辑状态0或者1，输入信号有效时，其输出电流保持为某个给定时间常数的函数，不会因它所连接的外电路不同而变化，输入信号无效时，其输出电流关断。

LED是一种电流驱动的双端口器件，其发光特性仅与流过的电流大小相对应，普通的驱动器件不具备恒流特性，其输出电流亦会随输入电压变化。而我们知道，TTL电路的电压是一阈值，一点微小的变化虽不影响逻辑状态，但会影响到输出电流的大小，而直接反映到LED的发光，解决这一问题的唯一途径即是采用如上所提到的恒流源。

另外，恒流源驱动器件的选用，保证了输出电流的大小恒定，也就可以去掉变通驱动器件必须有的串联限流电阻，大大降低了消耗在电阻上的功率，降低了系统的发热，恒流源驱动器件的输出电流可以通过调节电阻很方便的调校，这样对于系统最终的白平衡定位提供了最大程度上的方便。

本系统的LED显示屏采用恒流源驱动集成电路，对显示发光单元LED（发光二极管）进行直接驱动，从而保证了每一个发光二极管的发光显示效果的一致性。显示屏显示的画面图像效果亮度均匀，过渡平滑，纹理细腻，真实动人。如果电路中不采用恒流源驱动技术，由于每个发光二极管的显示效果不一致，有的偏亮、有的偏暗，图像画面上将会存在少数零星分布的亮点和暗点，图像画面粗糙，过渡生硬。

恒流源驱动电路是采用多路恒流源集成芯片驱动发光二极管，使通过二极管的电流恒定一致。

非恒流源电路采用电阻PNP三极管驱动发光二极管发光，由于电阻阻值的不一致，PNP三极管的饱和特性不一致，发光二极管的发光亮度互相之间存在细微的差别。

#### 音频扩声系统

##### 声学标准

音频扩声系统对整个指挥大厅起着至关重要的作用，应确保其音响效果达到GB50731-2006《厅堂扩声系统设计规范》中规定的会议类扩声系统声学一级标准。

会议类扩声系统声学一级标准要求

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **等级** | **最大声压级（dB）** | **传输频率特性** | **传声增益（dB）** | **声场不均匀度（dB）** | **系统总噪声** |
| 会议类扩声系统一级 | 额定通带内，大于或等于98dB | 以125~4000Hz的平均声压级为0dB，在此频带内允许范围：-6dB~+4dB；63~125Hz和4000~8000Hz的允许范围见国家标准《厅堂扩声系统设计规范》GB50371-2006 | 125Hz~  4000Hz传声增益的平均值大于或等于-10dB | 1000Hz小于等于8dB，4000Hz小于等于8dB | NR-20 |

##### 系统组成

系统组成应包括：会议系统主机、手拉手话筒、数字音频矩阵、功率放大器、音箱、相关音源及相应安装辅助设备，并由时序电源供电。

##### 系统功能

（1）能接收、发送远端音频信号；

（2）能对音频信号进行还原、放大，并且不会产生回音和啸叫；

（3）扩声时，以主扬声器为主，其他扬声器则配合以达到单点声源的效果；

（4）系统保证了声场的均匀度指标；

（5）系统应能平衡主扬声器和辅助扬声器在音质和声压级上的差别；

（6）数字化调音台信噪比高、失真小，带哑音编组且带有多路输出。保证了调音台背景噪声最小，且有足够的音频信号输出通道提供电视会议及音频录制端口等。

（7）为了提高系统的可靠性，功放具有可靠性最高的智能化电路控制设计；

（8）前置反馈抑制、选用强指向话筒及无线话筒采用内置反馈抑制剂限幅。话筒在不同位置时均有良好的传声增益，不致引起扬声器啸叫；

（9）可播放会议、摄像、录像等输出的音频（说明：摄像、录像功能本项目预留接口，本次不作建设）；

（10）使每一位与会人员都能听到清晰的声音；

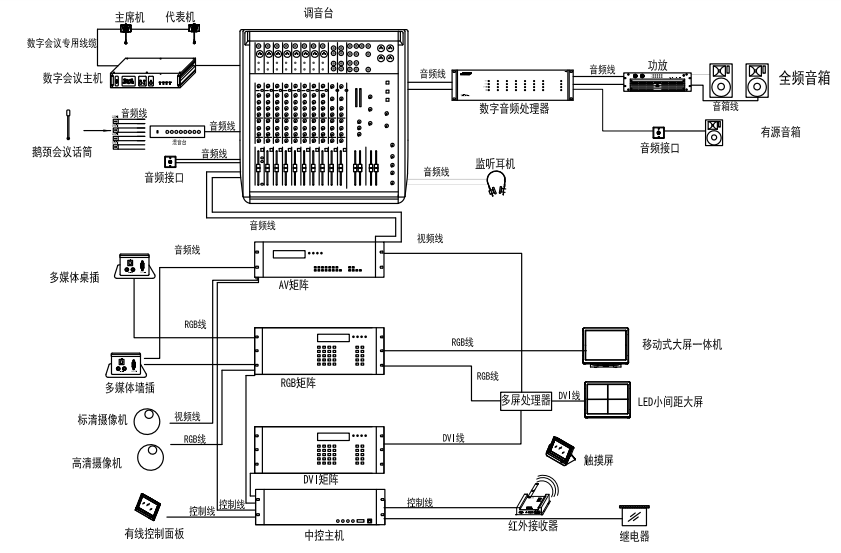
（11）必须具备电视电话会议功能所需的接口；

（12）扩声系统达到国家有关语言一级标准；

（13）能通过接口与集中控制系统连接。

#### 集中控制系统

为实现指挥大厅设置集中控制系统，可实现设备统一、集中、便捷化管理，本次工程配置1套集中控制系统，实现服务中心大屏幕显示系统（含视频综合管理平台、图像拼接控制器等）、音频扩声系统（数字音频处理器等）及电源控制器集中控制。



集中控制系统示意图

针对本场所设计要求各系统均能以集中控制系统统一管理；

多媒体显示方面要求显示输入、输出设备各信号通过各矩阵管理，实现信号同步、灵活切换并通过触摸屏控制设备；

实现对指挥中心灯光的明暗和开关控制；

系统要实现无线触摸屏控制。

#### 操作台及工作终端

在服务中心内配置操作台、桌椅以及相应的工作终端。

#### 装修

对服务中心内吊顶、墙面、地面、灯具等进行装饰装修。设计风格以科技风为主格调，打造简约、清爽的服务中心。同时重视环境设计，包括自然光源环境设计和人造光源设计，以及相应的避光、隔声和吸音措施。利用自然采光、通风，采用合理有效的措施，尽量降低能源消耗，体现生态思想和节能理念。

#### 其他

在服务中心内进行综合布线、空调、配电等部署，以支撑服务中心内相关系统正常运行。

#### 服务中心设备配置

相关配置需求如下：

服务中心设备配置表

| **序号** | **产品名称** | **技术参数/功能指标要求** | **单位** | **数量** |
| --- | --- | --- | --- | --- |
| 1 | 大屏显示系统 | 包括LED大屏显示单元（点间距：=<1.27mm）、发送卡、接收卡、拼控处理器和相关配套设备. | 项 | 1 |
| 2 | 操作台及工作终端 | 包括指挥座席、座椅、工作站等 | 项 | 1 |
| 3 | 装修工程 | 包括吊顶、墙面、地面、灯具等装饰装修 | 项 | 1 |
| 4 | 集中控制系统 | 包括电源控制、灯光控制、窗帘控制、矩阵、平板等 | 项 | 1 |
| 5 | 其他 | 空调、配电、综合布线等 | 项 | 1 |

## 算力资源接入

### 四川算力规模

综合全省目前已投产IDC机架数量、在建及规划数量，上架率，参考增速等各方面因素，预计未来5年全省数据中心市场需求在40万架左右。

四川区域数据中心规模统计表（架）

| **IDC主体** | | **地点** | **已投产** | **在建** | **规划新增** |
| --- | --- | --- | --- | --- | --- |
| 运营商类 | 电信 | 成都双流 | 17000 | 5000 | 10000 |
| 移动 | 成都双流 | 18000 | 10000 | 10000 |
| 联通 | 成都双流 | 5000 | 2300 | 5000 |
| 政府和运营商  合建类（政府主导） | 成都超算 | 成都天府新区 | 5000 |  |  |
| 华为智算 | 成都郫都 | 7000 |  |  |
| 天府热线 |  | 4000 |  |  |
| 雅安 | 雅安 | 20000 |  |  |
| 大数据产业园 |
| 川发展（雅安数据湖） | 雅安 | 5000 |  | 10000 |
| 宜宾 | 宜宾 | 6000 | 2500 |  |
| 长江上游区域大数据中心 |
| 达州 | 达州 | 2000 |  | 2000 |
| 德阳云上天府 | 德阳 | 2000 | 1500 | 10000 |
| 乐山 | 乐山 | 2000 |  |  |
| 泸州华为大数据中心 | 泸州 | 2000 |  |  |
| 眉山华为大数据中心 | 眉山 | 2000 |  |  |
| 能投数产简阳基地 | 成都简阳 | 10000 |  |  |
| 绵阳军民融合国安启祥 | 绵阳 | 1500 |  |  |
| 民营企业 | 万国数据 | 成都郫都 | 10000 |  |  |
| 世纪互联 |  | 10000 |  |  |
| 立昂 | 成都简阳 | 2000 |  |  |
| 珉田 | 大邑 | 2500 |  |  |
| 远洋 | 成都简阳 | 4000 | 5000 |  |
| 温江 |
| 网新积微云一期 | 成都简阳 | 1500 |  |  |
| 金茂 | 成都 | 3000 |  |  |
| 中立数据温江IDC中心（鹏博士） | 成都温江 | 1500 |  |  |

### 算力接入规模

本项目初期可接入算力资源包括成都超算、成都智算、能投天府云、雅安智算、达州智算。

初期算力接入规模

| **序号** | **区域** | **算力中心名称** | **资源类型** | **资源规模** |
| --- | --- | --- | --- | --- |
| 1 | 成都 | 国家超算成都中心 | 超算 | 170P |
| 2 | 成都 | 成都智算中心 | 智算 | 300P |
| 3 | 成都 | 四川能投天府云数据产业基地 | 智算 | 300P |
| 4 | 达州 | 万达开先进计算中心 | 智算 | 100P |
| 5 | 雅安 | 雅安智算 | 智算 | 500P |

具体接入算力规模及规格（如FP64、FP32或FP16），由后续协商结果为准。

## 主要软硬件选型原则

### 软件选型原则

#### 可移植性

应用软件应满足平滑移植，即应用软件与硬件平台相对分离，应用软件可以自由运行在主流硬件平台的主流操作系统上。当硬件平台发生变更时，可不用重新研发或购买相同功能的应用软件。

#### 灵活性

应用软件应尽可能采用参数化、可配置的设计开发原则，保证在系统相关指标（如有效期）和业务流程、管理流程发生变化时，能够通过参数修改或程序配置灵活适应新的要求。

#### 模块化设计

要求软件采用分层的模块化结构，模块之间的通信应按规定接口进行。任何一层的任何一个模块的维护和更新以及新模块的追加都不应影响其他模块，应用系统可以处理由于业务功能和用户量不断增加而带来的压力，保证系统正常运行。在硬件扩容之后，仅在原系统基础上简单地增加模块和修改参数，就能完成新功能的增加或整体扩容。

#### 可扩展性

系统功能、设备必须具有扩展能力，并且系统具有开放的业务开发接口。系统的扩展能力包括设备容量的扩展能力，端口密度的扩展能力、带宽的扩展、网络规模的扩展能力和系统功能的扩展等。

### 硬件选型原则

#### 安全性

系统软硬件的选型必须充分考虑其安全性，在确保信息系统安全的前提下进行系统软硬件的选型。对于核心、关键系统及软硬件优先采用自主可控产品。

#### 实用性、成熟性、先进性

遵循性能为主、兼顾价格以降低投资的原则，选择与该项目相适应的成熟的产品，兼顾产品的实用性与先进性，保证产品具有一定的超前性，不会在短期内被淘汰，代表着主流技术。

#### 通用性

选择具有通用性的产品，在存在标准的情况下，严格遵循国际和国家标准协议以及标准接口，保证产品的相互兼容，以实现不同网络的互联和数据交换。

#### 信创

在保证平台性能的前提下，新增服务器应尽量采用信创设备，以满足数据交互可信要求。本项目涉及的所有服务器按国产芯片的设备进行建设，并采用国产数据库进行管理，后期可以逐步对操作系统等进行国产化替代，这样既可以逐步完成国产化，同时也不会造成投资过大。

# 保障体系

## 标准规范体系

为保障本项目的正常开展，应制定相应的接口标准、算力度量标准和定价标准，在国家层面出台相关标准后再进一步修订完善。

### 接口标准

包括命名规范、接口协议、返回值格式等内容。平台接口统一后可要求资源供应方按照标准的接口进行开发和接入，同时也便于与各方进行适配。

算力中心已具备资源层划分、算力调度能力的情况下，算力中心应开放足够的调度和业务权限，如用户登录、认证、调度等服务，能够提供算力调度所需应用缓存、计算、存储等能力和资源，算力服务平台能够将用户需求打包封装并在算力中心进行远程部署，由算力服务平台和算力中心相关平台打通接口，实现算力服务平台在云端直接调度算力中心资源。

### 算力度量标准

需要制定统一的算力度量标准，实现灵活调度多元异构算力资源。包括由CPU、GPU、现场可编程逻辑门阵列（FPGA）等多种计算单元组成的异构处理体系的统一；从多个维度进行算力资源的建模和评估：不同行业、不同企业、不同场景对算力资源类型和需求量的评估。支持屏蔽异构资源差异，统一抽象定义资源特征，实现多个域之间的资源共享和协同，以及跨域的任务调度和执行。

### 定价标准

制定定价的相关标准，针对不同算力、不同时延等资源特征以及应用、工具的叠加服务等因素，进行综合定价。

## 安全保障体系

### 网络安全需求分析

本项目将来承载着全省重要算力资源，并传输和存储着大量敏感信息，面对来自信息系统内外部的各种安全威胁，以及新技术新安全形势的发展，需要按照本项目信息系统安全定级结果，根据等保2.0安全防护的具体要求，从多层级、多维度建设整体的、符合系统安全保护等级要求的安全防御体系。

#### 安全物理环境需求

安全物理环境是信息系统安全运行的基础和前提，是系统安全建设的重要组成部分。在等级保护基本要求中将物理安全划分为技术要求的第一部分，从物理位置选择、物理访问控制、防盗窃防破坏、防雷击、防火、防水和防潮、防静电、温湿度控制、电力供应、电磁防护等方面对信息系统的物理环境进行了规范。

物理层考虑因素包括机房环境、机柜、电源、服务器、网络设备和其他设备的物理环境。该层定级的功能室为上层提供一个生成、处理、存储和传输数据的物理媒体。物理环境安全需求主要考虑：物理位置选择、物理访问控制、防盗窃和防破坏、防雷击、防火、防水和防潮、防静电、温湿度控制、电力供应、电磁防护。

#### 安全通信网络需求

安全通信网络是在安全计算环境之间进行信息传输及实施安全策略的软硬件设备，是本项目平台建设的重要基础设施，也是保证数据安全传输和业务可靠运行的关键，更是实现数据内部纵向交互、对外提供服务、与其他单位横向交流的重要保证。

通信网络进行的各类传输活动的安全都应得到关注。现有的大部分攻击行为，包括病毒、蠕虫、远程溢出、口令猜测、未知威胁等攻击行为，都可以通过网络实现。安全通信网络需求主要考虑：网络架构、通信传输、可信验证。

#### 安全区域边界需求

安全区域边界安全对安全计算环境边界，以及安全计算环境与安全通信网络之间实现连接并实施安全策略的相关软硬件设备。区域边界安全防护是实现各安全域边界隔离和计算环境之间安全保障的重要手段，是实现纵深防御的重要防护措施。

通过边界防护、访问控制、入侵防范、恶意代码和垃圾邮件防范、安全审计、可信验证，实现保护环境的区域边界安全。

安全区域边界安全需求主要考虑：边界防护、访问控制、入侵防范、恶意代码和垃圾邮件防范、安全审计、可信验证。

#### 安全计算环境需求

安全计算环境是对系统的信息进行存储、处理及实施安全策略的相关软硬件设备，包括各类计算服务资源和操作系统层面的安全风险。本项目用于信息存储、传输、应用处理的计算服务资源，其自身安全性涉及到承载业务的方方面面，任何一个节点安全隐患都有可能威胁到整个网络的安全。

计算环境作为本项目平台的业务数据和信息的主要载体，这些业务数据和信息是信息资产的重要组成；另一方面，其是系统各项支撑业务的起点和终点，病毒、木马等安全威胁也容易通过网络渗透到后台各种业务应用和服务主机中，从而对系统的整体安全带来危害。

计算环境面临的安全风险主要来自多方面，对系统的不安全使用、配置和管理、未进行有效的入侵防范、没有进行安全审计和资源控制，这导致业务系统存在被黑客入侵或暴发高级安全威胁的可能。安全计算环境需求主要考虑：身份鉴别、访问控制、安全审计、入侵防范、恶意代码防范、可信验证、数据完整性、数据保密性、数据备份恢复、剩余信息保护、个人信息保护。

#### 安全管理中心需求

安全管理中心是等级保护安全应用环境提供集中安全管理功能的技术管控中枢，是安全应用系统安全策略部署和控制的中心，对安全策略和安全计算环境、安全区域边界和安全通信网络上的安全机制实施统一管理，安管中心为各级系统管理员、安全管理员和安全审计员提供身份鉴别和权限管理的集成平台，实施系统管理、安全管理、审计管理和集中管控。

安全管理中心针对整个系统提出了安全管理方面的技术控制要求，通过技术手段实现集中管理，安全管理中心需求主要考虑：系统管理、审计管理、安全管理、集中管控。

#### 安全管理需求

除了采用网络安全技术措施控制安全威胁外，安全管理措施也是必不可少的手段，所谓“三分技术，七分管理”更加凸显了安全管理的重要性，健全的安全管理体系是各种安全防范措施得以有效实施、网络系统安全实现和维系的保证，安全技术措施和安全管理措施可以相互补充，共同构建完整、有效的网络安全保障体系。管理需求主要考虑安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理等。

很显然，本项目的安全建设需要考虑以上各个层次的安全管理要求，同时还需要结合国际国内成熟的安全体系建设经验，并通过借助成熟的安全产品、安全服务和安全管理措施不断进行持续改进，最终建立符合业务工作的安全保障体系。

### 安全防护原则

#### 分区分域防护原则

任何安全措施都不是绝对安全可靠的，为保障攻破一层或一类保护的攻击行为而不会破坏整个网络，以达到纵深防御的安全目标，需要合理划分安全域，综合采用多种有效安全保护措施，实施多层、多重保护。

#### 均衡性保护原则

对任何类型网络，绝对安全难以达到，也不一定是必须的，需正确处理安全需求、安全风险与安全保护代价的关系。因此，结合适度防护实现分等级安全保护，做到安全性与可用性平衡，达到技术上可实现、经济上可执行。

#### 技管并重原则

网络安全涉及人、技术、操作等方面要素，单靠技术或单靠管理都不可能实现。因此在考虑网络安全时，必须将各种安全技术与运行管理机制、人员思想教育、技术培训、安全规章制度建设相结合，坚持管理与技术并重，从而保障网络安全。

#### 动态调整原则

由于网络安全需求会不断变化，以及环境、条件、时间的限制，安全防护一步到位、一劳永逸地解决网络安全问题是不现实的。网络安全保障建设可先保证基本的、必需的安全保护，后续再根据应用和网络安全技术的发展，不断调整安全保护措施，加大安全防护力度，以适应新的网络安全环境，满足新的网络安全需求。当安全保护等级需要变更时，应当根据等级保护的管理规范和技术标准的要求，重新确定网络安全保护等级，根据调整情况重新实施安全保护。

#### 三同步原则

网络运营者在网络新建、改建、扩建时应当同步规划、同步建设、同步运行网络安全保护、保密和密码保护措施，确保其具有支持业务稳定、持续运行性能的同时，保证安全技术措施能够保障网络安全与信息化建设相适应。在全过程中推行安全同步开展，强化安全工作前移，降低运维阶段的服务压力。

### 安全风险分析

#### 安全技术风险分析

##### 传统安全风险分析

本项目私有化部署平台作为一个物理与虚拟化环境并存的信息化体系，自然也面临大量传统类型的安全风险，具体包括以下内容：

###### 物理安全风险

物理环境安全主要影响因素包括机房环境、机柜、电源、通信线缆和其他设备的物理环境。该层面为基础设施和业务应用系统提供了一个生成、处理、存储和传输数据的物理环境。具体安全需求如下：

* 由于机房容易遭受雷击、地震和台风和暴雨等自然灾难威胁，需要考虑机房场地位置的选择，以及采取防雷击措施等来解决雷击、地震和台风等威胁带来的问题；
* 由于机房容易遭受水患和火灾等灾害威胁，需要采取防水、防潮、防火措施来解决水患和火灾等威胁带来的安全威胁；
* 由于机房容易遭受高温、低温、多雨等原因引起温度、湿度异常，应采取温湿度控制措施来解决因高温、低温和多雨带来的安全威胁；
* 由于机房电压波动影响，需要合理设计电力供应系统来解决因电压波动带来的安全威胁；
* 针对机房供电系统故障，需要合理设计电力供应系统，如：部署UPS系统、建立备用发电机机房、铺设双电力供电电缆来保障电力的供应等措施，来解决因供电系统故障带来的安全威胁；
* 针对机房容易遭受静电和线缆电磁干扰，需要采取防静电和电磁防护措施来解决静电和线缆电磁干扰带来的安全威胁；并对关键设备采取电磁屏蔽措施；
* 针对利用非法手段进入机房内部盗窃、破坏等安全威胁，需要通过采取物理区域访问控制及监控报警装置等控制措施，来解决非法手段进入机房内部盗窃、破坏等带来的安全问题；
* 针对利用工具捕捉电磁泄漏的信号，导致信息泄露的安全威胁，需要通过采取防电磁措施，来解决电磁泄漏带来的安全问题。

###### 计算环境安全风险

计算环境的安全主要指主机以及应用层面的安全风险与需求分析，包括：身份鉴别、访问控制、系统审计、入侵防范、恶意代码防范、软件容错、数据完整性与合法性、备份与恢复、资源合理控制、剩余信息保护、抗抵赖等方面。

###### 区域边界安全风险

区域边界的安全主要包括：边界访问控制、边界完整性检测、边界入侵防范以及边界安全审计等方面。

###### 通信网络安全风险

数据中心通信网络的安全主要包括：网络结构安全、网络安全审计、网络设备防护、通信完整性与机密性等方面。

（1）网络结构

网络结构是否合理直接影响着是否能够有效地承载业务需要。因此网络结构需要具备一定的冗余性；带宽能够满足业务高峰时期数据交换需求；并合理地划分网段和VLAN。

（2）网络安全审计

由于用户的计算机相关的知识水平参差不齐，一旦某些安全意识薄弱的管理用户误操作，将给信息系统带来致命的破坏。没有相应的审计记录将给事后追查带来困难。有必要进行基于网络行为的审计。从而威慑那些心存侥幸、有恶意企图的少部分用户，以利于规范正常的网络应用行为。

（3）网络设备防护

由于数据中心在建网络系统将会使用大量的网络设备和安全设备，如交换机、防火墙、入侵检测设备等。这些设备的自身安全性也会直接关系到各种网络应用的正常运行。如果发生网络设备被不法分子攻击，将导致设备不能正常运行。更加严重情况是设备设置被篡改，不法分子轻松获得网络设备的控制权，通过网络设备作为跳板攻击服务器，将会造成无法想象的后果。例如，交换机口令泄漏、防火墙规则被篡改、入侵检测设备失灵等都将成为威胁网络系统正常运行的风险因素。

（4）通信完整性与机密性

由于网络协议及文件格式均具有标准、开发、公开的特征，因此数据在网上存储和传输过程中，不仅仅面临信息丢失、信息重复或信息传送的自身错误，而且会遭遇信息攻击或欺诈行为，导致最终信息收发的差异性。因此，在信息传输和存储过程中，必须要确保信息内容在发送、接收及保存的一致性；并在信息遭受篡改攻击的情况下，应提供有效的察觉与发现机制，实现通信的完整性。

而数据在传输过程中，为能够抵御不良企图者采取的各种攻击，防止遭到窃取，应采用加密措施保证数据的机密性。

###### 应用层安全威胁

1）威胁来源与安全防护的核心资源

威胁来源：安全威胁主要来自外部攻击、内部人员的错误和有意破坏。

核心资源：环境中受保护的核心资源包括：各级服务器、服务器上所承载的业务。

2）应用层主要安全威胁：

当前的视频监控网主要是通过Web应用系统提供服务，主要体现如下的安全风险。

A恶意的应用服务器信息扫描和收集

威胁1：扫描应用服务器配置开放的信息

威胁来源：内部攻击源

受攻击面：应用服务器

攻击行为：有时Web应用服务器除业务端口外还会开放一些默认端口（如Jboss开放的8083），这些默认端口对最终用户是不需要开放的，而且也不会用于维护，容易被攻击。

产生的后果：服务器获取是后续攻击的前提。

主要原因：应用服务器配置失误等。

威胁2：扫描应用服务器开放的目录

威胁来源：内部攻击源

受攻击面：应用服务器

攻击行为：网站目录查找是进行攻击的必备知识，只有知道了目录信息才能确定攻击的目标，进行目录查找是测试的首要阶段，一般扫描工具进行扫描前首先要进行目录查找。其次对于某些隐藏的管理接口（目录或文件），虽然没有对外有明显的链接，但是通过一系列有特定含义的枚举是可以访问的。

产生的后果：服务器获取是后续攻击的前提。

主要原因：应用服务器配置失误等。

B应用服务器输入校验漏洞导致恶意攻击

威胁3：通过各种注入攻击执行恶意脚本或者命令

威胁来源：内部攻击源

受攻击面：应用服务器

攻击行为：注入攻击漏洞，例如SQL、OS命令以及向XML注入。这些攻击发生在当不可信的数据作为命令或者查询语句的一部分，被发送给解释器的时候。攻击者发送的恶意数据可以欺骗解释器，以执行计划外的命令或者访问未被授权的数据。

产生的后果：服务器的信息窃取、篡改、增加恶意账户等

主要原因：应用服务器安全漏洞，服务器端没有对输入数据的合法性进行再次校验。

威胁4：通过跨栈脚本XSS执行恶意脚本或者命令

威胁来源：内部攻击源

受攻击面：应用服务器

攻击行为：当后台应用程序收到含有不可信的数据，在没有进行适当的验证和转义的情况下，就将它发送给一个网页浏览器，这就会产生跨站脚本攻击（简称XSS）。XSS允许攻击者在受害者的浏览器上执行恶意脚本。

产生的后果：访问该应用的一般用户受到攻击，跨站脚本会导致会话被劫持、敏感信息泄漏、账户被盗，严重时甚至造成数据修改、删除，从而导致业务中断。

主要原因：应用服务器安全漏洞，服务器端没有对输入数据的合法性进行再次校验。

C失效的身份认证和会话管理

威胁5：用户登录会话管理不善导致恶意攻击

威胁来源：内部攻击源

受攻击面：应用服务器

攻击行为：用户注销后会话信息没有清除或者浏览器超时一定时间而没有重新登录认证机制，导致用户在点击注销按钮之后还能继续访问注销之前（也就是登录之后）或者超时才能访问的页面。

产生的后果：用户身份冒用导致各种后果等

主要原因：用户注销后会话信息没有清除，或者浏览器超时一定时间而没有重新登录认证机制。

威胁6：通过无效输入参数恶意绕过认证机制

威胁来源：内部攻击源

受攻击面：应用服务器

产生的后果：无效的认证机制，黑客可以为所欲为。

主要原因：应用服务器安全漏洞，服务器端没有对输入数据的合法性进行再次校验。

##### 高级可持续性威胁

目前互联网APT攻击泛滥，政府、大型企事业单位的信息化系统极易成为不法分子进行APT攻击的目标。为此，做好网络安全运营监测和态势感知、威胁预警和分析处置方面的工作，是本项目网络安全防护的重要工作。

##### 虚拟化带来的威胁

目前云环境中安全威胁主要有以下几点：

（1）虚拟化软件漏洞

（2）定向攻击性的病毒木马

（3）虚拟化环境成为病毒木马、网络攻击的重灾区

（4）利用不安全接口的攻击

（5）利用共享技术漏洞进行的攻击

（6）越权、滥用与误操作

（7）安全防护能力的高要求和虚拟化追求性能稳定理念相背离

总体上讲，在虚拟化环境中上，建设虚拟化安全能力，安全防护能力是首要考虑的指标，另外如何平衡防护能力和资源消耗成为衡量虚拟化中安全解决方案的重要指标。

##### 数据安全风险

业务上云后将用户的数据分散存储，用户失去了对数据的直接监管，导致对数据安全风险控制能力也相应减弱，这些风险主要包括数据传输风险、数据存储风险和数据隔离风险。

（1）数据传输风险：是指用户与云就算环境进行数据交互的过程中，如不能对传输数据进行有效的加密等措施进行保护时，导致数据在传输的过程中丢失、篡改。

（2）数据存储风险：是指数据被存储在云计算环境中，如不能对存储数据进行有效地保护，导致数据在云计算环境中丢失、滥用或泄漏的风险。

（3）数据隔离风险：“多租户”架构是云计算的典型特征。在“多租户”下，大量用户的敏感数据可能存储在同样的云服务器上，如果没有有效的数据隔离机制，其他“租户”或者恶意攻击者就能够轻易地获取用户的敏感数据，并对数据进行篡改、窃取等操作。

#### 安全运维风险分析

安全运维管理涉及环境管理、资产管理、系统安全运行维护管理、配置与变更管理、安全事件处置及应急响应管理等方面。其安全需求如下：

* 需要保证机房具有良好的运行环境；
* 需要建立机房安全管理制度来规范物理访问、物品进出和环境安全；
* 需要对信息资产进行分类标识、规范化管理；
* 需要对各种软硬件设备的选型、采购、使用和保管等过程进行控制；
* 需要各种网络设备、服务器正确使用和维护；
* 需要采取措施对安全漏洞和隐患进行识别，并及时修补；
* 需要对网络、操作系统、数据库系统和应用系统进行安全管理；
* 需要定期地对通信线路进行检查和维护；
* 需要对恶意代码防范有效性进行验证；
* 需要对运维工具的使用和远程运维的权限进行管理控制；
* 需要硬件设备、存储介质存放环境安全，对其使用进行控制和保护；
* 需要对支撑设施、硬件设备、存储介质进行日常维护和管理；
* 需要对系统使用手册、维护指南等工具文档进行管理；
* 需要规范配置管理和变更管理流程；
* 需要在事件发生后能采取积极、有效的应急策略和措施；
* 需要建立应急响应机制来应对突发事件，做好应急预案并进行演练；
* 需要与符合国家有关规定的外包运维服务商签订相关协议，并明确运维服务能力要求。

#### 安全管理风险分析

“三分技术、七分管理”更加突出的是管理层面在安全体系中的重要性。除了技术管理措施外，安全管理是保障安全技术手段发挥具体作用的最有效手段。建立健全安全管理体系不但是信息安全保障的要求，也是安全体系不可或缺的重要组成部分。

安全管理体系依赖于国家相关标准、行业规范、国际安全标准等规范和标准来指导，形成可操作的体系。

#### 安全合规风险分析

安全合规工作是安全体系的重要一环。导致合规保护需要解决的问题如下：

（1）缺少后合规时代的风险处置能力

主要表现在安全合规工作完成后，没有对风险进行有效地抑制，导致安全问题一旦发生，就没有办法有效应对。

（2）新技术带来的风险

新技术带来了业务、应用等方面的便利性，但同时也带来了旧标准中无法覆盖的风险控制，导致类似移动应用、APT攻击、边界失守的问题比较严重。

（3）安全管理覆盖度低

新技术加大了安全管理层面的难度，使管理成本提升，人员队伍建设无法与时俱进，导致管理上的空白。

（4）缺少有效的动态安全监控

传统安全管理体系中，监控技术各自为战，标准无法统一，新业务、系统上线又缺乏持续有效的监控，导致动态安全监控能力的缺失。

（5）合规形式化、风险成本增加，有些系统为了合规而合规，等风险发生时，再临时应对，导致拆东墙补西墙，风险应对的成本不断增加。

### 安全等级保护测评合规性分析

#### 技术层面（安全通用要求）

技术通用合规性

| **类别** | **序号** | **基本要求** | **安全整改措施及解决方案** |
| --- | --- | --- | --- |
| 安全  物理环境 | 1 | 物理位置选择 | 机房场地设计及选址 |
| 2 | 物理访问控制 | 安装电子门禁系统 |
| 3 | 防盗窃和防破坏 | 设备设置标签；安装防盗报警系统 |
| 4 | 防雷击 | 安装防雷保安器，或过压保护装置 |
| 5 | 防火 | 安装火灾自动消防系统；耐火材料；防火隔离布局 |
| 6 | 防水和防潮 | 采取防水防渗措施；安装防水检测和报警装置 |
| 7 | 防静电 | 防静电地板，采用静电消除器、佩戴防静电手环等 |
| 8 | 温湿度控制 | 安装机房空调（温湿度调节） |
| 9 | 电力供应 | 稳压设计、过电保护；UPS电源；冗余电力线路供电 |
| 10 | 电磁防护 | 电源线和通信线缆隔离铺设；关键设备采取电磁屏蔽（屏蔽柜、屏蔽室） |
| 安全  通信网络 | 1 | 网络架构 | 网络架构设计、关键设备冗余部署、安全域划分，部署抗DDoS设备、负载均衡设备 |
| 2 | 通信传输 | VPN安全网关 |
| 3 | 可信验证 |  |
| 安全  区域边界 | 1 | 边界防护 | 终端安全管理、安全准入控制 |
| 2 | 访问控制 | 下一代防火墙 |
| 3 | 入侵防范 | 部署IDS、IPS、APT检测系统 |
| 4 | 恶意代码和垃圾邮件防范 | 部署防病毒网关、IPS/UTM/下一代防火墙开启防病毒模块、防垃圾邮件系统 |
| 5 | 安全审计 | 部署数据库审计、综合日志审计 |
| 6 | 可信验证 | 部署基于可信芯片的安全网络设备 |
| 安全  计算环境 | 1 | 身份鉴别 | 部署统一认证与授权管理、Ukey或数字证书登录；通过VPN安全网关与统一认证与授权管理联动远程安全登录；部署4A管理平台或应用系统开发 |
| 2 | 访问控制 | 部署统一认证与授权管理实现帐号权限分配；部署配置核查系统实现帐号检查与管理；在服务器部署主机加固系统实现安全标记访问；部署4A管理平台实现帐号权限管理、帐号检测管理；通过应用系统定制开发实现基于安全标记访问控制 |
| 3 | 安全审计 | 部署数据库审计系统 |
| 4 | 入侵防范 | 部署终端安全管理实现终端安全基线检查、补丁管理；部署IDS、IPS实现入侵行为检测、阻断；部署漏洞扫描系统 |
| 5 | 恶意代码防范 | 部署网络防病毒软件系统、Web应用安全防护、网页防篡改 |
| 6 | 可信验证 | 部署基于可信芯片的服务器、终端 |
| 7 | 数据完整性 | 部署VPN安全网关，及应用系统开发 |
| 8 | 数据保密性 | 部署VPN安全网关，及应用系统开发 |
| 9 | 数据备份恢复 | 保证重要节点设备冗余、部件冗余；部署数据备份与恢复系统、构建异地灾备中心 |
| 10 | 剩余信息保护 | 部署剩余信息清除工具，或应用系统开发 |
| 11 | 个人信息保护 | 应用系统开发 |
| 安全  管理中心 | 1 | 系统管理 | 部署统一认证与授权管理（运维审计） |
| 2 | 审计管理 | 部署统一认证与授权管理（运维审计） |
| 3 | 安全管理 | 部署统一认证与授权管理（运维审计） |
| 4 | 集中管控 | 部署安全管理平台SOC |

#### 技术层面（云计算安全扩展要求）

云计算安全扩展合规性

| **类别** | **序号** | **基本要求** | **安全整改措施及解决方案** |
| --- | --- | --- | --- |
| 安全物理环境 | 1 | 基础设施位置 | 参考通用要求 |
| 安全通信网络 | 1 | 网络架构 | 参考通用要求 |
| 安全区域边界 | 1 | 访问控制 | 流量清洗、抗DDoS攻击、防火墙、UTM、VPN、WEB应用防护、网络入侵防御IPS等 |
| 2 | 入侵防范 |
| 3 | 安全审计 |
| 安全计算环境 | 1 | 身份鉴别 | 入侵检测IDS或XDS、漏洞扫描、安全配置核查、数据库审计、Web应用审计、安全域流量监控、网络行为分析、安全运维（统一认证与授权管理）等 |
| 2 | 访问控制 |
| 3 | 入侵防范 |
| 4 | 镜像和快照保护 |
| 5 | 数据完整性和保密性 |
| 6 | 数据备份恢复 |
| 7 | 剩余信息保护 |
| 安全管理中心 | 1 | 集中管控 | 综合安全管理（云SOC） |

#### 管理层面

管理层面合规性

| **类别** | **序号** | **基本要求** | **安全整改措施及解决方案** |
| --- | --- | --- | --- |
| 安全管理制度 | 1 | 安全策略 | 相关管理制度的编制及宣贯落实 |
| 2 | 管理制度 | 相关管理制度的编制及宣贯落实 |
| 3 | 制定和发布 | 相关管理制度的编制及宣贯落实 |
| 4 | 评审和修订 | 相关管理制度的编制及宣贯落实 |
| 安全管理机构 | 1 | 岗位设置 | 相关管理制度的编制及宣贯落实 |
| 2 | 人员配备 | 相关管理制度的编制及宣贯落实 |
| 3 | 授权和审批 | 相关管理制度的编制及宣贯落实 |
| 4 | 沟通和合作 | 相关管理制度的编制及宣贯落实 |
| 5 | 审核和检查 | 相关管理制度的编制及宣贯落实 |
| 安全管理人员 | 1 | 人员录用 | 相关管理制度的编制及宣贯落实 |
| 2 | 人员离岗 | 相关管理制度的编制及宣贯落实 |
| 3 | 安全意识教育和培训 | 相关管理制度的编制及宣贯落实 |
| 4 | 外部人员访问管理 | 相关管理制度的编制及宣贯落实 |
| 安全建设管理 | 1 | 定级和备案 | 相关管理制度的编制及宣贯落实 |
| 2 | 安全方案设计 | 相关管理制度的编制及宣贯落实 |
| 3 | 产品采购和使用 | 相关管理制度的编制及宣贯落实 |
| 4 | 自行软件开发 | 相关管理制度的编制及宣贯落实 |
| 5 | 外包软件开发 | 相关管理制度的编制及宣贯落实 |
| 6 | 工程实施 | 相关管理制度的编制及宣贯落实 |
| 7 | 测试验收 | 相关管理制度的编制及宣贯落实 |
| 8 | 系统交付 | 相关管理制度的编制及宣贯落实 |
| 9 | 等级测评 | 相关管理制度的编制及宣贯落实 |
| 10 | 服务供应商选择 | 相关管理制度的编制及宣贯落实 |
| 安全运维管理 | 1 | 环境管理 | 相关管理制度的编制及宣贯落实 |
| 2 | 资产管理 | 相关管理制度的编制及宣贯落实 |
| 3 | 介质管理 | 相关管理制度的编制及宣贯落实 |
| 4 | 设备维护管理 | 相关管理制度的编制及宣贯落实 |
| 5 | 漏洞和风险管理 | 相关管理制度的编制及宣贯落实 |
| 6 | 网络和系统安全管理 | 相关管理制度的编制及宣贯落实 |
| 7 | 恶意代码防范管理 | 相关管理制度的编制及宣贯落实 |
| 8 | 配置管理 | 相关管理制度的编制及宣贯落实 |
| 9 | 密码管理 | 相关管理制度的编制及宣贯落实 |
| 10 | 变更管理 | 相关管理制度的编制及宣贯落实 |
| 11 | 备份与恢复管理 | 相关管理制度的编制及宣贯落实 |
| 12 | 安全事件处置 | 相关管理制度的编制及宣贯落实 |
| 13 | 应急预案管理 | 相关管理制度的编制及宣贯落实 |
| 14 | 外包运维管理 | 相关管理制度的编制及宣贯落实 |

### 安全保障服务

在建设后由第三方提供长期的安全保障服务，包括安全评估、安全配置检查、脆弱性识别、渗透测试、应急预案编制及演练、供应链审查、网络安全培训、安全应急响应等服务。

#### 网络安全及数据安全纲领文件编写

提供组织机构建设，建设信息安全团队，并提供信息安全和数据安全战略方向，编写主要的一级纲领性文件和确定主体责任。

#### 脆弱性识别服务

采用漏洞扫描工具对城运平台各种软硬件设备进行网络层、系统层、数据库、应用层面的扫描与分析，扫描设备检测规则库及知识库应涵盖 CVE、 CNCVE、 CNVD、 CNNVD 等标准。扫描完成后并人工验证所发现的操作系统漏洞、数据库漏洞、弱口令、信息泄露及配置不当等脆弱性问题。提供准确有效的扫描报告，并针对漏洞扫描中出现的问题，提供解决方案。

#### 应急预案编制及演练服务

根据相关规章和标准，结合近年网络安全行业发生的安全事件和面临的安全风险，编制网络安全应急预案。制定符合客户自身组织架构的网络安全应急预案，明确各个部门的责任，准备措施以及应对突发事件的配合机制，配合单位组织应急演练工作。

#### 供应链审查服务

分别从供应链安全管理组织机构、供应链安全管理流程与政策、供应商安全管理、供应链人员管理、产品安全审查、供应链统一安全管理等方面开展供应链安全风险排查，全面发现供应链安全风险，及时进行相关风险处理。

#### 网络安全培训服务

针对领导、运维人员、系统开发人员和系统保障人员开展网络安全培训，通过网络安全培训，全面提升参会人员安全意识水平，降低网络攻击事件的概率。培训内容包括但不限于：网络安全防护要点、网络安全意识、社会工程学防护、安全技术、安全管理等。

#### 协助加固服务

根据整体评估测试结果，针对所发现的安全漏洞及安全风险，提出可操作性强、效果佳的整改建议，并协助完成安全整改。

#### 安全通告服务

根据目前的信息安全形势，收集和整理最新安全漏洞、安全事件、安全资讯等信息，定期发送安全预警通告，遇紧急高危漏洞或重大信息安全事件即时通告。

#### 应急响应服务

在服务期内，当信息系统遇到突发的安全问题如：发生网络入侵事件、大规模病毒暴发、遭受拒绝服务攻击等，无法及时对该事件进行处理或解决时，在收到单位的应急响应服务请求信息后，以远程或现场的方式协助相关人员查明安全事件原因，确定安全事件的威胁和破坏的严重程度，并根据对事件的分析及原因提供相应的解决方案。

#### 外包管理制度编写

制定服务外包公司安全管理要求，对服务外包公司提供精细化管理，防止因为外包团队的管理不当，导致数据中心出现网络安全事件。

### 算力资信认证标准制定

制定算力资信认证标准可以确保算力服务提供者所提供的资源符合安全性要求，同时帮助用户判断其安全性。

建立标准：在制定算力资信认证标准前，先确定算力服务的基本定义和分类，包括智能算力、超算算力、通用算力。然后针对每一种算力服务制定具体的安全性要求和认证标准。

安全性和可靠性：算力服务必须具备一定的安全性和可靠性，这包括数据安全、隐私保护、系统稳定性等方面。制定认证标准时，需要针对这些方面制定具体的测试和评估方法，以及相应的指标要求。

认证机构和测试机构：为确保算力资信认证的权威性和可靠性，需要指定专门的认证机构和测试机构来进行测试和认证。这些机构需要具备相应的专业资质和技术实力，以保证测试和认证工作的科学性和公正性。

认证流程：制定详细的认证流程，包括申请认证、资料审核、现场考察、测试、审核、认证决定等环节。同时，需要明确每一步骤的具体要求和时间节点，以保证认证流程的可操作性和规范性。

认证标志和证书：为方便用户判断算力服务的安全性，需要设计相应的认证标志和证书。认证标志和证书上应包含相应的认证级别、认证标准、认证时间等信息，以便用户进行判断和选择。

# 报价表

报价总表

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **项目或费用名称** | **2024年** | **2025年** | **2026年** | **合计(万元)** |
| 1 | 算力服务平台 |  |  |  |  |
| 2 | 综合监测平台 |  |  |  |  |
| 3 | 网络系统 |  |  |  |  |
| 4 | 计算存储 |  |  |  |  |
| 5 | 服务中心（大屏) |  |  |  |  |

算力服务平台报价表

| **序号** | **一级功能** | **二级功能** | **三级功能** | **四级功能** | **单价（万元）** | **单位** | **数量** | **合计（万元）** | **备注** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **2024年建设** | | | | | | | | |  |
| 1 | 可信数据 | / | / | / |  | 项 | 1 |  |  |
| 2 | 算力编排 | 资源接入与调度 | 资源接入 | / |  | 项 | 1 |  | 5个算力中心接入，含接口适配对接费用 |
| 3 | 资源调度 | / |  | 项 | 1 |  |  |
| 4 | 资源封装 | 资源池封装 | / |  | 项 | 1 |  |  |
| 5 | 算力加工 | / |  | 项 | 1 |  |  |
| 6 | 多云纳管 | / | / |  | 项 | 1 |  |  |
| 7 | 算网感知 | / | / |  | 项 | 1 |  |  |
| 8 | 算网质量 | / | / |  | 项 | 1 |  |  |
| 9 | 算力度量 | / | / |  | 项 | 1 |  |  |
| 10 | 应用注册 | / | / |  | 项 | 1 |  |  |
| 11 | 算力解构 | / | / |  | 项 | 1 |  |  |
| 12 | 交易运营 | 算力门户/商城 | 产品目录 | 基础算力 |  | 项 | 1 |  |  |
| 13 | 应用软件 |  | 项 | 1 |  |  |
| 14 | 专用算力 |  | 项 | 1 |  |  |
| 15 | 机架资源 |  | 项 | 1 |  |  |
| 16 | 云安全服务 |  | 项 | 1 |  |  |
| 17 | 服务估价 | / |  | 项 | 1 |  |  |
| 18 | 服务申请 | / |  | 项 | 1 |  |  |
| 19 | 产品试用 | / |  | 项 | 1 |  |  |
| 20 | 在线交易 | / |  | 项 | 1 |  |  |
| 21 | 用户控制台 | / |  | 项 | 1 |  |  |
| 22 | 服务商控制台 | / |  | 项 | 1 |  |  |
| 23 | 运营管理 | 运营分析 | / |  | 项 | 1 |  |  |
| 24 | 后台管理 | / |  | 项 | 1 |  |  |
| 25 | 统一门户 | / | / | / |  | 项 | 1 |  |  |
| **合计** |  |  |  |  |  |  |  |  |  |
| **2025年建设** | | | | | | | | |  |
| 1 | 算力调度 | 资源接入与调度 | 资源接入 | / |  | 项 | 1 |  | 增加8个算力中心接入，含接口适配对接费用 |
| 2 | 智能匹配 | / | / |  | 项 | 1 |  |  |
| 3 | 交易运营 | 算力门户/商城 | 服务结算 | / |  | 项 | 1 |  |  |
| 4 | 社区服务 | / | / |  | 项 | 1 |  |  |
| 5 | 平台整体功能优化 |  |  |  |  | 项 | 1 |  |  |
| **合计** |  |  |  |  |  |  |  |  |  |
| **2026年建设** | | | | | | | | |  |
| 1 | 算力调度 | 资源接入与调度 | 资源接入 | / |  | 项 | 1 |  | 增加8个算力中心接入，含接口适配对接费用 |
| 2 | 资源封装 | 对外接口服务 | / |  | 项 | 1 |  |  |
| 3 | 交易运营 | 算力门户/商城 | 产品目录 | 算力服务 |  | 项 | 1 |  |  |
| 4 | 平台整体功能优化 |  |  |  |  | 项 | 1 |  |  |
| **合计** |  |  |  |  |  |  |  |  |  |
| **总计** |  |  |  |  |  |  |  |  |  |

综合监测平台报价表

| **序号** | **系统名称** | **一级功能** | **功能描述** | **单价（万元）** | **单位** | **数量** | **合计（万元）** | **备注** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **2024年建设** | | | | | | | |  |
| 2 | IT设备运维监测 | / | 本项目拟对能投天府云因本次工程新增的IT资源进行监管，针对其他算力中心则通过接口方式获取接入资源相关的运维监测数据。 通过平台对接和直接监测等方式对算力中心IT资源进行实时监控，主要涵盖网络设备、安全设备、服务器、存储、虚拟化（虚拟主机和子机）、数据库、中间件等。系统需具备数据分析与挖掘能力，实现故障预判与工单推送、匹配智能知识库；能够全面直观展示各资源运行状态；能够结合各类型日志、流量、进程、端口等数据，精准定位，分析及预防故障，保障资源稳定运行。 统计和展示算力服务平台任务的运行总量、任务运行状态、任务资源分布等数据。实时监测任务运行对应的算力资源运行情况，反映任务运行健康度（对应的服务器、网络、安全等运行是否正常，对多个运行设备进行综合评价）和繁忙度（对相应设备的线程数、端口流量等信息进行综合评价）。 |  | 项 | 1 |  |  |
| 4 | 能源效率监测 | / | 包括能源数据接入和分析等，详见建设方案 |  | 项 | 1 |  | 含接口适配对接费用 |
| **合计** |  |  |  |  |  |  |  |  |
| **2025年建设** | | | | | | | |  |
| 1 | IT设备运维监测 | / | 增加8个算力中心监测接入，进一步优化平台功能 |  | 项 | 1 |  | 含接口适配对接费用 |
| 2 | 能源效率监测 | / |  | 项 | 1 |  | 含接口适配对接费用 |
| **合计** |  |  |  |  |  |  |  |  |
| **2026年建设** | | | | | | | |  |
| 1 | IT设备运维监测 | / | 增加8个算力中心监测接入，进一步优化平台功能 |  | 项 | 1 |  | 含接口适配对接费用 |
| 2 | 能源效率监测 | / |  | 项 | 1 |  | 含接口适配对接费用 |
| **合计** |  |  |  |  |  |  |  |  |
| **总计** |  |  |  |  |  |  |  |  |

网络系统报价表

| **序号** | **产品名称** | **技术参数/功能指标要求** | **单价（万元）** | **单位** | **数量** | **合计（万元）** | **备注** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 核心交换机 | 框式 4 槽以上满足 10G/40G/100G 板卡，不少于以下配置 1\*48端口10GE以太网光接口板(FD-G,SFP+)；10G-多模模块(850nm,0.3km,LC)\*48 2\*18端口100GE以太网光接口板（QSFP28），满配光模块 |  | 台 | 2 |  | 供应商应根据设计方案进行配置 |
| 2 | 业务交换机 | 不低于2个40G端口，48个10GB 端口，含双电源，双风扇模块（端口侧出风），满配光模块 |  | 台 | 2 |  |
| 3 | 管理交换机 | 不低于2个40G端口，48个10GB 端口，含双电源，双风扇模块（端口侧出风），满配光模块 |  | 台 | 2 |  |
| 4 | 存储交换机 | 不低于2个40G端口，48个10GB 端口，含双电源，双风扇模块（端口侧出风），满配光模块 |  | 台 | 2 |  |
| 5 | 带外交换机 | 不低于48个千兆电端口，4个万兆光接口，满配光模块 |  | 台 | 1 |  |
| 6 | 服务中心交换机 | 不低于48个千兆电端口，4个万兆光接口，满配光模块 |  | 台 | 1 |  |
| 7 | 负载均衡 | 1、独立硬件应用交付设备，而非通过添加功能模块的方式实现；机架高度≥2U；千兆电口≥6个；千兆光口≥4个，万兆光口≥2个；包含千兆SFP多模光纤模块4个； 2、四层吞吐量≥20Gbps,并发连接数≥900万，四层每秒新建≥40万；冗余电源； |  | 台 | 2 |  |
|  | **合计** |  |  |  |  | **0.00** |  |

计算存储报价表

| **序号** | **产品名称** | **技术参数/功能指标要求** | **单价（万元）** | **单位** | **数量** | **合计（万元）** |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | 云管理节点服务器 | 1、国产CPU：2颗，单颗核心数≥32；2、内存：≥256GB； 3、配置相应端口和必要存储； 4、含操作系统。含操作系统 |  | 台 | 4 |  |
| 2 | 云平台计算节点 | 1、国产CPU：2颗，单颗核心数≥32；2、内存：≥512GB；3、配置相应端口和必要存储；4、含操作系统。 |  | 台 | 23 |  |
| 3 | 云平台软件授权 | 实现虚拟计算、虚拟网络、虚拟存储、高可用性（HA）、动态资源调度（DRS），46个CPU授权，1套云数据库服务授权，1套容器服务授权，云专家现场实施服务 |  | 套 | 1 |  |
| 4 | 分布式存储（含分布式管理系统） | 1、本次存储系统含1套分布式存储管理软件和5个存储节点； 2、每个节点配置如下：CPU：2颗，核心数≥32；内存：≥512GB，硬盘≥12块 7.68TB SSD，4个万兆光纤网口和4个千兆网口； |  | 套 | 1 |  |
| 5 | 备份一体机 | 备份容量不低于74.85TB，含备份系统，支持本地存储、物理带库、VTL、SAN、NAS等存储；支持定时备份、副本数据管理、实时数据保护 |  | 套 | 1 |  |
|  | **合计** |  |  |  |  |  |

服务中心（大屏）报价表

| **序号** | **产品名称** | **技术参数/功能指标要求** | **单价（万元）** | **单位** | **数量** | **合计（万元）** | **备注** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 大屏显示系统 | 包括LED大屏显示单元（点间距：=<1.27mm）、发送卡、接收卡、拼控处理器和相关配套设备. |  | 项 | 1 |  | 预估25-30个平方 |
| 2 | 操作台及工作终端 | 包括指挥座席、座椅、工作站等 |  | 项 | 1 |  |  |
| 3 | 装修工程 | 包括吊顶、墙面、地面、灯具等装饰装修 |  | 项 | 1 |  |  |
| 4 | 集中控制系统 | 包括电源控制、灯光控制、窗帘控制、矩阵、平板等 |  | 项 | 1 |  |  |
| 5 | 其他 | 空调、配电、综合布线等 |  | 项 | 1 |  |  |
|  | **合计** |  |  |  |  |  |  |

备注：以上报价单位均为人民币：万元，需填写单价和合计等内容。