融讯光通
RONG XUN GUANG TONG

数据中心建设方案

（政务央企）

北京融讯光通科技有限公司

2023 年 11 月

目　录

一、建设背景

当前，我国数字政府建设已全面进入快车道。数字政府建设的一项重要目标是推动政务服务高效化和利企便民最大化，在不见面的互联网空间中，要实现各项政务服务的在线和远程办理，其关键和首要是解决电子政务系统中的身份认证的问题。

在数字时代，数字政府是政府高效透明地为民服务，推进国家治理体系和治理能力现代化的重要支撑。通过政府数字化、智能化的运行和服务，可以让人民生活的安全感、获得感和幸福感得到明显提升。

随着数据量的不断增长和对大数据分析的需求，数据中心在特种行业中变得越来越重要。它为企业、组织和个人提供了高效、安全和可靠的数据服务，推动着数字化时代的发展。数据中心是一个集中存储、管理和处理大量数据的设施，其建设的重要性和必要性体现在如下方面：

1. **数据存储和备份：** 数据中心提供了安全可靠的存储空间，可以保存大量的数据。在数字化时代，企业和组织生成的数据数量快速增长，这些数据是企业重要的资产。数据中心的建设使得数据可以被集中存储和备份，避免了数据丢失和损坏的风险。

2. **数据安全与隐私：** 数据中心采用了严格的物理和网络安全措施，保护数据免受未经授权的访问、恶意攻击和数据泄露的风险。数据中心的建设提供了一种安全可靠的环境，确保敏感数据得到妥善保护，符合法规的隐私要求。

3. **数据处理和分析：** 数据中心配备了高性能的服务器和数据处理设备，可以支持大规模数据的处理和分析。通过数据中心，企业和组织能够利用先进的数据分析技术，从海量数据中提取有价值的信息和洞察，帮助决策者做出准确的决策，并提供更好的产品和服务。

二、建设目标

数据中心的建设目标是确保数据安全和可靠性、提供高性能和可扩展性的计算和存储能力、保证业务连续性和灾备能力、关注能源效率和环保可持续发展以及实现成本效益和资源共享。这些目标旨在满足日益增长的数据需求，提供可靠的数据服务和支持业务的发展。

1. **数据安全和可靠性：** 数据中心的建设目标之一是提供安全可靠的环境，确保数据的完整性、保密性和可用性。通过采用物理安全措施、网络安全技术和数据备份策略，防止未经授权的访问、数据丢失和外部攻击。

2. **高性能和可扩展性：** 数据中心被要求提供高性能的计算和存储能力。建设目标是构建高效的硬件设施、网络架构和软件系统，以满足大规模数据的处理、高速数据传输和快速

响应的需求。同时，数据中心还需要具备可扩展性，随着业务的增长可以灵活扩展资源。

3. 业务连续性和灾备能力： 数据中心的目标之一是确保业务的连续性和可靠性。通过采用冗余系统、备份设施和灾备计划，保证在意外事故、硬件故障或自然灾害发生时，能够及时切换到备份设备并恢复业务的正常运行。

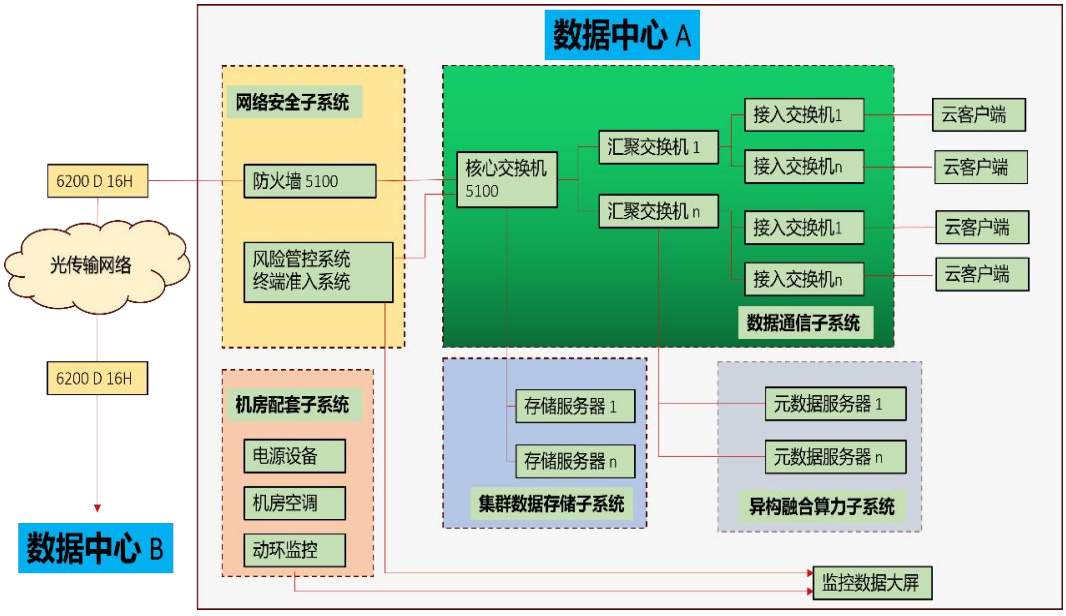
4. 能源效率和环保可持续发展： 数据中心的目标还包括节能环保和可持续发展。通过采用高效的能源管理技术、热回收和冷却方案，降低能源消耗和碳排放，减少对环境的影响。同时，数据中心也应当关注资源的合理利用和回收利用。

5. 成本效益和资源共享： 数据中心建设的目标之一是实现成本效益和资源共享。通过合理规划和配置硬件设施、网络资源和人力资源，降低建设和运营成本。同时，多个企业和组织可以共享一处设施，实现资源的共享和利用，提高资源利用效率。

三、总体方案

数据中心是一个专门用于存储、管理和处理大量数据的设施。它由服务器、网络设备、存储设备、电源设备和冷却系统等组成的一个集中化的运行环境。数据中心的建设和管理需要考虑多个方面，包括选址、硬件设备的选择和配置、网络架构设计、安全措施、能源管理、监控系统以及运维管理等。它不仅提供了数据存储和处理的基础设施，还提供了高可用性、灾备能力和安全保障，以保护数据的完整性、可靠性和安全性。

如下图所示，数据中心可分为网络安全子系统、数据通信子系统、存算融合平台（数据存储子系统+算力子系统）、数据中心互联传输子系统。



1、 网络安全子系统

网络安全子系统由防火墙、风险管控系统和终端准入系统组成。基于网络攻防技术融合云计算、大数据、人工智能等技术，将网络安全被动防御模式转变为主动防御模式。以自动化运行方式，完成资产巡检、风险发现、风险识别、渗透验证与风险评估，实现事前主动发现安全风险、主动验证风险可利用性、主动修复风险等，从而构建起网络空间安全风险管控体系。

子系统提供与外部资源和其他子系统进行接口交互，最终实现对中心网络安全防护、网络攻防、网络风险评估业务的支撑。

1.1 多合一防火墙

T 比特级 7 层防火墙以保障用户应用安全为目标，立足于高性能的矢量操作系统和一体化引擎，通过 L2-L7 层全面威胁防御及强大应用安全管控技术，为用户提供超高性能的网络安全解决方案。

1.2 风险管控系统

以主动防御为目标，基于网络攻防融合云计算、大数据、人工智能等技术，将网络安全被动防御模式转变为主动防御模式，实现信息化资产的发现、监控，整体网络安全态势的实时呈现和动态预警。

自动化运行方式，完成快速部署，操作简易，维护便捷，双引擎漏扫实现事前主动发现安全风险、主动验证风险可利用性、主动修复风险等，从而构建起网络安全主动防御风险体系。

1.3 终端准入控制系统

零信任泛终端安全网关，也称为终端准入控制系统，属于全终端接入管控、安全防护设备，基于流量，来真正解决物联网时代，海量物联网终端接入安全防护以及内网安全防护的难点和痛点问题。

终端准入控制系统，是一种网关类单机产品，具备资产探测、资产防冒用检测、资产行为分析、防火墙、轻量 IPS 功能。该产品最初面向的需求为哑终端设备的入网安全检查及防护，主要解决哑终端入网审核和网络访问控制问题，防止非法入网。所谓哑终端即具备单一功能的网络终端，主要为有线终端。这类终端具有分布广、数量多、种类杂、功能单一、无人值守的特点。

产品支持旁路模式或者透明串式部署，一般旁路或串接网络域的网关前汇聚后，通常部署于二层网络域，也可以作为防火墙网关和部署于三层网关处。

2、 数据通信子系统

数据通信子系统用于将多个网元设备或终端连接起来，通过数据传输实现信息的交流和共享的系统。从而实现快速、可靠、安全地传输和交换信息。

3、存算融合平台

随着信息技术的不断发展，信息化建设已经成为政府和企业发展战略的重要组成部分，是提升政务央企行业单位竞争力的有效手段。随着信息化建设的不断深入，信息系统的安全性已经成为业必须面对的一个重要问题。

大型超大型云平台，承载着很多重大的行业战略战术意义。存/算融合平台由集群数据存储子系统和异构融合算力子系统构成，本方案提供如下三种组网方案，用户可根据自身的业务需求和预算情况灵活选择：

选项一（区、县级系统--数据单元）：采用海光节点建设区、县级终极融合环境，可以实现区、县级业务超融合部署在一台设备上，拥有虚拟化超融合系统、安全存储系统和加密通讯网盘系统。

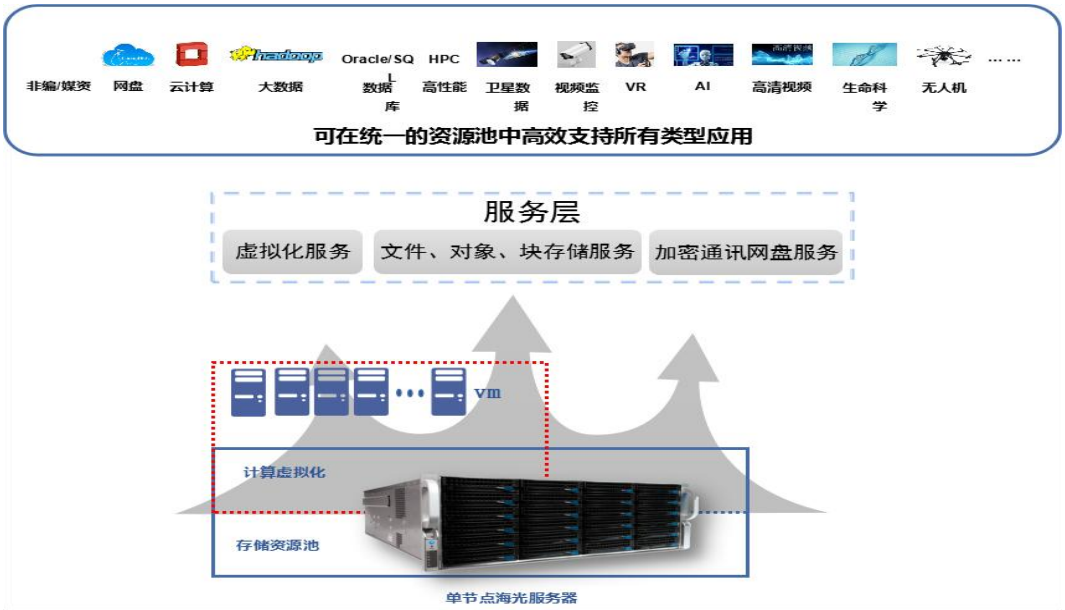
选项二（市级系统--数据节点）：采用海光节点+申威节点建设市级终极融合环境，可以实现存算分离，架构独立的高效率虚拟化节点，访问安全存储系统空间及加密通讯网盘系统。

选项三（省级系统--数据中心）：采用海光节点+申威节点+x86 GPU 节点建设省级终极融合环境，实现模块化架构的终极融合平台，可以实现海光、申威、x86 芯片平台异构混合

部署统一资源池。

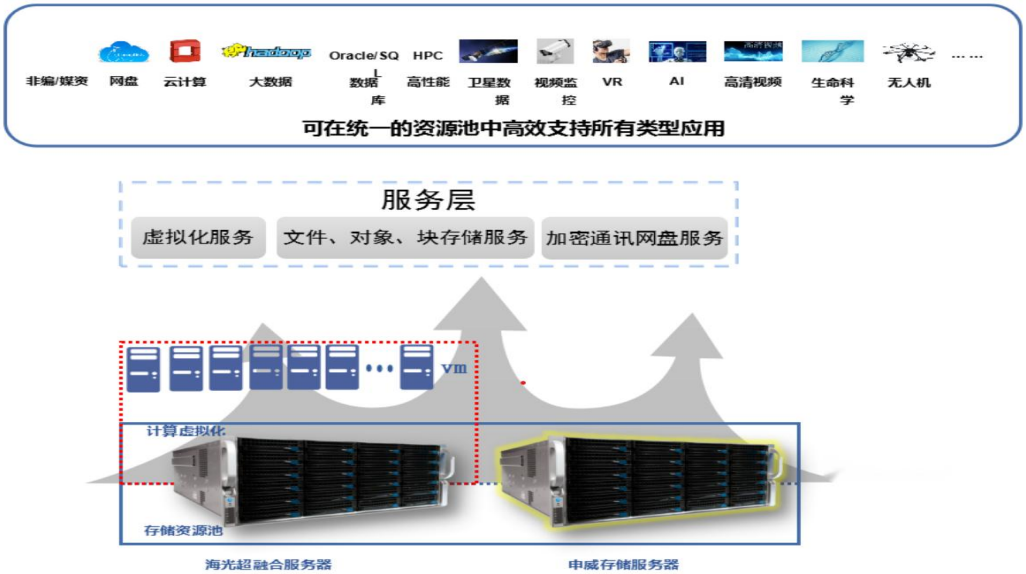
3.1 架构说明

区、县级数据单元架构图如下：



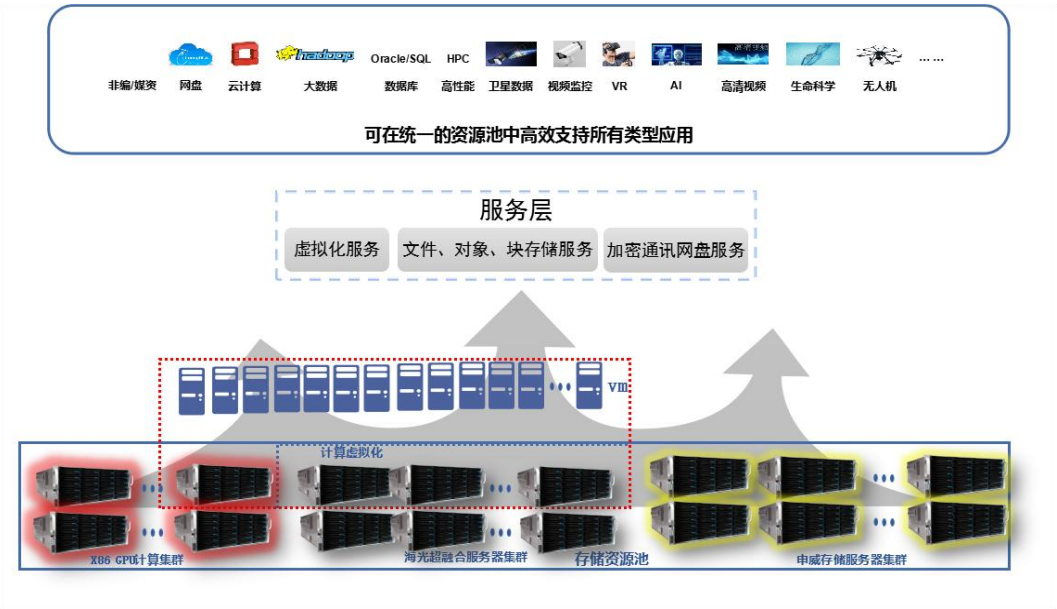
区、县级系统采用单台海光节点提供虚拟化，存储+加密通讯网盘服务，主要为区、县级单位提供小规模共享、虚拟化资源提供支持，并且可以支持内网加密通讯网盘，实现区、县级内部交流互通，数据安全存储的目的。

市级数据节点架构图如下：



市级架构图可得知，为保障数据安全可靠的同时，还需提供更高效的虚拟化资源，采用1台海光节点+1台申威节点组成集群。由海光节点提供计算虚拟化服务，由海光和申威节点异构混合构建统一存储池，共同为上层业务提供存储服务，满足虚拟化服务的存储需求，也保障数据安全可靠。

省级数据中心架构图如下：



省级系统采用海光服务器集群提供虚拟化服务，x86 GPU集群提供GPU计算资源，整合海光集群、申威集群、x86集群上的硬盘资源构建统一存储资源池，为虚拟化服务及GPU计算资源提供高安全、高性能的存储服务。

3.2 方案优势

1、军用级稳定性、成熟性、可靠性

目前，国内规模最大压力最大系统背后均由该方案在支撑，可靠性能够远超行业水平地实现到99.9999%级以上。在雷击、磁爆、灾害等极端情况下依然能够保障系统可恢复、数据可恢复。

2、数据的红线兜底安全

传统安全体系已不可持续，数据层数据本身的安全已是退无可退的红线。在系统被攻陷等极端情况下，依然能确保数据不被偷、不被篡改、不被摧毁等非法操作。

3、彻底国产自主可控

历史原因，软件代码100%自主。硬件方面，能够支持所有通用X86设备和所有国产设备（包含但不限于鲲鹏、海光、龙芯、申威、飞腾等）的同时异构混合部署。能最大化降低全球供应链不确定性给用户平台长期建设发展带来的系统性风险。

4、吞吐性能卓越且无瓶颈

同等硬件环境和配置下，性能跨代翻倍高于其他方案，且无任何扩展提升瓶颈。能够最大化释放计算资源能力，能最充分最优地满足用户即时级业务响应需求。

5、极简运维

无论多大规模，仅需1人即可实施和运维。为用户腾出更多人力专注于深耕前端业务。

3.3.6 终极融合服务

1. 具有国产自主知识产权，非进口或OEM产品，非在Lustre、Ceph、gluster等开源软件基础上更改。
2. 单套系统存储节点可支持10000台以上，容量可支持在线扩展至1000PB以上
3. 支持POSIX/NFS/CIFS/HDFS/S3/Swift等多种访问协议访问同一文件，避免因访问协议不同造成的数据拷贝，支持多协议同时读写，无明显语义损失，支持文件修改写、对象多段上传等常用语义，无需配置独立的网关节点。
4. 集群内任意一台存储节点均可同时提供文件级、块级、对象级接口，且使用任意一种上述接口写入数据时，集群内所有硬盘均有数据增长。。
5. 支持异构部署，支持海光、申威、x86设备异构部署为统一存储池，数据统一共享。
6. 存储自带客户端以及用户访问权限机制，可设置客户端以及存储私有用户对存储系统中任意数据的读、写、删、列表、链接、重命名、追加写权限，以上权限支持自由组合使用，此权限机制为系统自带功能，不允许借助第三方软件实现且任何超级管理员用户均无法逾越此权限机制，以保证数据的安全性。
7. 同时提供文件/块/对象/大数据快照功能，快照须采用增量快照，不允许复制完整数据进行快照。单存储池快照数量不少于100000个。
8. 支持对目录、用户、用户组设置容量、目录数、文件数配额，配额对所有访问接口有效，并可在线设定、更改和取消，配额实时性为秒级，支持配额嵌套，并提供配额预警功能。
9. 支持应用超融合及虚拟化超融合两种架构。满足存储节点与应用节点复用，同一节点既

做存储又做应用，可在存储节点上运行应用业务系统软件；支持服务器虚拟化平台。

10. 同时提供文件/块/对象/大数据克隆功能，无需在应用服务器之间耗时复制，即可在存储系统内部秒级完成数据快速克隆，且克隆后无额外空间增长。
11. 系统能够准确的体现具体某个文件的数据写入客户端 ID、写入时间、数据删除客户端 ID、删除时间的详细记录。
12. 通过设置周期性数据扫描预知磁盘是否损坏以及进行数据自动恢复，防止磁盘静默错误导致数据丢失。
13. 存储，虚拟化，加密通讯网盘服务为同一厂商提供。
14. 即时通讯功能，要求能在云盘中进行聊天，默认包含部门聊天组，用户能自主创建聊天群组，可自定义添加成员进群组，聊天共享文件可转存至云盘个人空间中。
15. 文件恢复功能，将已删除的文件恢复到个人存储中，通过该功能可以使得用户找回某天删除的文件可恢复设置时间段误删除数据。
16. 支持文件过滤功能，支持对文件类型进行自动识别，拒绝指定类别的数据类型的存放，拒绝数据类型可以在线设置并即刻生效。
17. 文件保险箱的多级密码防护机制防止用户数据被盗窃和被篡改，保险箱密码支持文件列表，只读，读写等多种权限。
18. 文件独占编辑功能，支持用户对文件加锁和解锁，加锁后可以独占编辑，防止多个用户同时编辑同一个文件造成数据破坏。
19. 个人共享管理功能，实现用户一对一、一对多进行文件共享，同时能够控制共享权限，包含只读、读写等多种权限；对于同一个目录，共享名只有一个，共享给不同的好友可以设置不同的权限。
20. 部门共享管理功能，支持在管理端对每个用户访问部门目录的权限进行在线动态配置，并即可生效，部门目录的权限支持无法访问、只读、读写（无法删除和改名）、完全控制（可以读写，删除和改名）等多种模式。
21. 可选择在线映射的方式或同步盘两种模式登录访问云盘用户数据。
22. 支持虚拟机热迁移，须满足将运行在一台物理机中的虚拟机迁移到另一台物理机上继续运行，而不影响虚拟机内应用的正常运行。
23. 支持动态调整虚拟机内存，在虚拟机正常运行时，可以对虚拟机内存使用量进行动态的增加或减少。
24. 提供三级用户的使用权限，三级租户分别为：云服务管理员、租户管理员和普通用户。

25. 须支持虚拟机镜像管理，虚拟机可以通过镜像安装来快速构建具有特定系统环境的虚拟机。
26. 虚拟机快速启动，满足 100 个虚拟机 30s 内快速启动，不会造成启动风暴。
27. 系统支持虚拟机快照，可针对虚拟机在某个时间点运行状态进行快照。当恢复虚拟机快照时，会恢复到保存快照时刻虚拟机的运行状态。

4、 数据中心互联设备

RT-06200-D16H 是针对数据中心互联应用而定制的可堆叠超 100G 波分传输平台。该产品传输容量超大、体积小且完全符合数据中心机房的要求，功耗低，运维便捷，既适用于数据中心间短距离业务互联，又适用于数据中心间骨干网长距离业务传输。

RT-06200-D16H 支持 16 个 100G 客户侧接口和 8 个 200G 系统侧接口，以开放软件架构为基础，提供各种开放接口，DCI 用户可以进行二次开发，使其管理方式能便捷的和数据中心设备管理系统实现融合，减轻了设备日常维护的难度，为快速增长的数据中心业务提供了有力的保障。

物 理 特 性：

特性	描述
机框尺寸(mm)（高*宽*深）	44mm*442mm*340mm
可插放机柜	19 英寸机柜
电源	1+1 电源备份 AC 输入：100～240V，47～63Hz DC 输入：-40V～-72V
散热	前进风， 后出风
工作环境	工作温度：0°C～45°C 存储温度：-40°C～70°C 相对湿度：10%～90%，无冷凝
最大功耗	360W

5、 机房配套子系统

机房配套子系统采用一体化集成方案，主要具备一体化集成，安全可靠，节省机房占地面积，节约能源，安装省时、省力、省心，架构兼容，部署快速灵活和监控完善等特点，是新一代智能微模块数据中心产品。方案整体采用 All-In-Room 建设模式，一体化集成了机柜

系统、供配电系统、制冷系统、监控系统和综合布线系统。采用单、双排密封冷通道部署方式。

机房配套设备，按区、县级，市级，省级三级考虑，推荐的设备组成如下，具体设备数量可根据机房实际情况调整：

1）区、县级：10 平米，配一个综合电源柜，里面放 1 个 6K UPS 机架式+锂电池包，及配电分配；

2）市级：100-150 平米，配机柜及综合配电柜，综合配电柜内放 20KW 机架式 UPS+锂电池包，30A 综合直流柜；

3）省级：200-300 平，配综合配电柜内放 20KW 机架式 UPS+锂电池包+封闭冷通道，加 90A 综合直流柜。

智能模块化数据中心效果图

本方案采用封闭冷通道建设方式，建设 3 个封闭通道模块，每个模块内包括温控系统、机柜系统、监控系统，配电系统。