附件：

**景德镇市第一人民医院新区医院**

**双活数据中心建设项目技术要求**

**目 录**

[1 项目概述 3](#_Toc129110728)

[1.1 项目名称 3](#_Toc129110729)

[1.2 项目建设背景 3](#_Toc129110730)

[1.3 建设目标 3](#_Toc129110731)

[1.4 建设方案及思路 4](#_Toc129110732)

[1.4.1 业务运行级别 4](#_Toc129110733)

[1.4.2 业务特点 4](#_Toc129110734)

[1.4.3 数据中心解决方案架构 4](#_Toc129110735)

[1.4.4 业务分布规划 5](#_Toc129110736)

[1.4.5 业务平台建设 5](#_Toc129110737)

[1.4.6 核心业务双活平台 6](#_Toc129110738)

[1.4.7 重要业务平台 6](#_Toc129110739)

[1.4.8 影像系统及数字化病理数据存储 6](#_Toc129110740)

[1.4.9 虚拟桌面平台 7](#_Toc129110741)

[1.4.10 外网业务平台 7](#_Toc129110742)

[1.4.11 容灾备份系统 7](#_Toc129110743)

[1.4.12 网络安全建设 7](#_Toc129110744)

[1.4.13 虚拟化安全设计 8](#_Toc129110745)

[2 工期要求 9](#_Toc129110746)

[3 质保要求 9](#_Toc129110747)

[4 总体技术要求 9](#_Toc129110748)

[4.1 标准要求 9](#_Toc129110749)

[4.2 技术路线 10](#_Toc129110750)

[5 采购清单 10](#_Toc129110751)

[5.1 软件 10](#_Toc129110752)

[5.2 硬件 11](#_Toc129110753)

[6 软件参数要求 12](#_Toc129110754)

[6.1 智能化消化内镜网络信息系统 12](#_Toc129110755)

[6.1.1 消化内镜网络服务端模块 12](#_Toc129110756)

[6.1.2 预约登记工作站 13](#_Toc129110757)

[6.1.3 消化内镜图文报告工作站 14](#_Toc129110758)

[6.1.4 智能化质控 15](#_Toc129110759)

[6.1.5 主任审核工作站 16](#_Toc129110760)

[6.1.6 信息化集成 16](#_Toc129110761)

[6.2 产科信息管理系统 17](#_Toc129110762)

[7 硬件参数要求 25](#_Toc129110763)

[8 服务要求 80](#_Toc129110764)

[9 培训要求 80](#_Toc129110765)

# 1 项目概述

## 项目名称

景德镇市第一人民医院新区医院双活数据中心建设项目

## 项目建设背景

2021年6月4日，国务院办公厅印发了《关于推动公立医院高质量发展的意见》，提出加强公立医院在我国医疗服务体系中的主体地位，力争通过5年努力，公立医院发展方式从规模扩张转向提质增效，运行模式从粗放管理转向精细化管理，资源配置从注重物质要素转向更加注重人才技术要素，为更好提供优质高效医疗卫生服务、防范化解重大疫情和突发公共卫生风险、建设健康中国提供有力支撑的目标。

《关于推动公立医院高质量发展的意见》中也明确了引领公立医院高质量发展的新趋势，除加强临床专科建设、推进医学技术创新和推进医疗服务模式创新外，最重要的就是强化信息化支撑作用。推动云计算、大数据、物联网、区块链、第五代移动通信（5G）等新一代信息技术与医疗服务深度融合。推进电子病历、智慧服务、智慧管理“三位一体”的智慧医院建设和医院信息标准化建设。大力发展远程医疗和互联网诊疗。

景德镇市第一人民医院是全市成立最早的公立医院，始建于1950年，市一院几代人坚持砥砺前行，不忘初心，秉承“博学、精医、仁术、诚信”的院训，以凤凰涅槃的姿态，绽放出光彩。现已发展成为集医疗、教学、科研、 预防、保健和急救服务为一体的大型综合性三级甲等医院。本次新院区建设规划，总体投资约15亿元，30多万平方使用面积，拟规划建设床位1300张。

## 建设目标

景德镇市第一人民医院新院数据中心规划以满足医院业务实际需要和响应国家公立医院高质量发展为总体目标，在满足本院医疗业务需求，保障业务连续运行能力和数据安全的前提下，同时考虑对《电子病历系统应用水平分级评价》、《医院信息互联互通标准化成熟度评测》、《医院智慧服务分级评估标准体系》和《医院智慧管理分级评估标准体系》等主要医疗评测相关业务的承载能力，在此原则上对双活数据中心内计算、存储、网络、安全等资源池进行总体规划。

## 建设方案及思路

### 业务运行级别

在业务部署规划中，按照业务系统重要性及业务系统特征，对不同业务采取不同的承载和数据存储、保护方式。

首先按照业务重要程度，将所有业务分为两类：

1、与患者就医流程相关的业务及部分特殊业务；

2、与患者就医流程无关或关联度非常小的业务。

针对与就医流程相关的业务，必须保障其业务连续性及数据安全性，同时采用业务高可用方案及多种手段的数据保护方案对其进行保障，保证这一类业务的安全、稳定运行。

针对与患者就医流程无关的业务，主要依靠其本身的系统、集群的能力来保障其业务连续性，并根据数据特点采用不同的数据保护方案。

### 业务特点

部分医疗业务有非常鲜明的业务特点：

1、如HIS、EMR等业务，其核心数据库要求具备高性能、高并发的能力应对前端系统的访问压力；

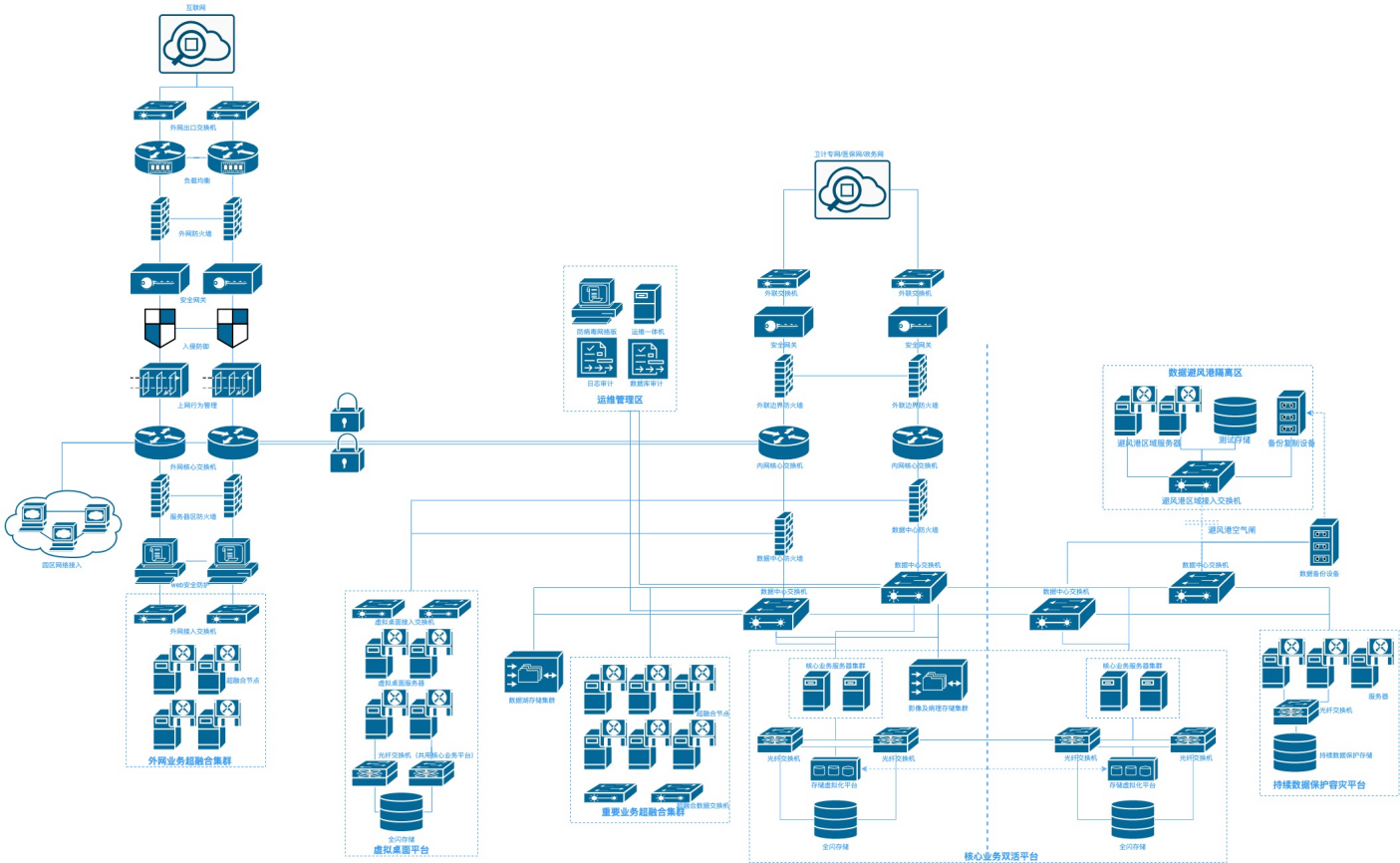
2、如集成平台/CDR等业务，则需要具备高并发的即时消息处理能力和数据仓库的OLAP（在线数据分析）能力。

3、如影像类、数字病理类业务，其特点是有非常大的非结构化数据的存储需求，并且随着影像设备的更新，其需求量会越来越大。

针对以上不同的医疗业务的特点，对即时性、并发性要求较高的业务采用全闪存的方案进行承载；对大数据量的非结构化数据采用分布式文件存储的方式进行承载，并同时需要考虑大量影像文件的访问和存储效率问题。

### 数据中心解决方案架构

因本次项目为医院的整体迁建，老院区不再保留，故而所有数据中心生产系统均部署于新院区内，新院区规划建设两个数据中心，建设方案以“双数据中心双活+远程数据容灾”为主要框架，采取不同的架构、介质对不同类型的业务进行有针对性的部署。



### 业务分布规划



**各区域业务规划分布**

### 业务平台建设

医疗信息化业务日趋复杂，发展也极为快速，从原有仅包含部分患者就诊流程逐渐发展到对院前、院中、院后的全流程覆盖，以及对医疗临床业务、医院管理决策的全面精细化支撑。而新型的大数据、5G和人工智能等技术的实践也对医疗科研、智慧医院的建设提供了强大支撑。所以医疗业务平台建设的首要目标就是能够支撑重要系统的连续运行，保障患者就医；其次是对大数据、互联网等业务的支持，帮助医院提升患者就医体验、辅助医院决策；第三就是对医院科研能力的支撑，以新型信息化技术助力科研。

### 核心业务双活平台

医院业务中与患者就诊流程相关的业务是最重要的，这部分业务改动相对较少，为保障稳定性和响应能力，一般以传统的数据库方式承载，即以一个主数据库为核心（如HIS、EMR等业务的数据），前端不同业务根据需求从数据库中读写数据，而不同的业务模块之间，则主要采取消息系统进行通信。

无论是数据库还是消息系统，均对底层硬件有很高的稳定性和响应能力的要求，为提高患者体验，这部分业务规划采取双活架构及全闪存存储进行承载，最大化业务的连续运行能力及快速响应能力。在架构规划上采用偏传统的服务器、光纤交换机、全闪存储三层架构方式部署。

基于医院的业务发展情况，并考虑未来3～5年的发展，业务平台计算层采用四台四路服务器，并部署虚拟化。底层存储则通过存储虚拟化平台加两台高性能全闪存储搭建核心存储系统，核心业务数据基于存储虚拟化平台进行双活镜像，保障业务安全；同时在存储技术上引入最新的NVMe等技术提高存储系统的整体性能，并且全闪存系统可以提供较高的数据去重效率，通过这些新型技术可以进一步提升存储系统的运行效能。

### 重要业务平台

在医疗业务中，与患者就医流程无关的业务也占了很大一部分，这部分业务对连续运行的要求比上述业务要低，并且需求不确定性较高，同时其部分数据安全也需要一定的保证。

考虑到其业务特性和需求的不确定性，这部分业务可以采用超融合的方式来承载，超融合技术以分布式计算技术为基础，将计算与存储融为一体，实现计算、存储资源的模块化横向扩展，具有极强的灵活性和扩展性。

规划重要业务平台初始采用六个超融合节点，充分利用超融合方案的敏捷性，在初期以小规模建设，随业务增长进行快速扩展，仅单边运行，不参与双活，同时对其中较为重要的数据部署持续数据保护进行容灾。

### 影像系统及数字化病理数据存储

影像和数字化病理是目前医疗业务中对存储容量需求最高的两个业务，其本身数据特性也与一般的医疗业务有所不同，其数据以快速增长的文件类数据为主，需要较大的出口带宽以及较强的空间扩展能力。同时考虑到目前检验检测类业务对医院整体收入的影响逐渐增高，其业务连续性也越来越重要，需要保障较高的连续运行能力。

影像和数字化病理业务的数据库建议作为核心业务系统运行在双活架构上保障生产业务连续性，而图片数据则考虑存放在分布式文件存储中，以保障其访问效率和扩展性。

### 虚拟桌面平台

桌面系统的管理和安全一直是医疗信息化领域的痛点和难点，以新院区数据中心建设为契机，引入新型的虚拟桌面技术，通过统一的部署以及集中的管理，能够有效提升桌面系统的管理便捷性和安全性。

在本次项目中虚拟桌面区域按照使用规模，结合虚拟桌面软件、虚拟化安全软件和桌面防病毒软件等建立统一的虚拟桌面系统，覆盖全院的办公类电脑使用场景。

### 外网业务平台

由于目前医院的外网业务开展的越来越多，很多系统都采取了数据库->业务系统->外网前置的部署方式，特别像预约、支付类的业务用户也越来越多，这些业务本身具备一定的互联网业务特性，需要有高度的灵活性和扩展性，以适应医院初期建设和互联网业务爆发后的快速扩展需求。

并且从安全角度考虑，外网业务区作为单独的业务区域进行独立部署变得非常有必要。

因此，在本次新院区外网业务平台的设计上，建议使用具有互联网基因的超融合技术来解决外网业务的需求。

### 容灾备份系统

为提升医院业务的持续运行能力和数据安全，并应对医疗评测对信息化建设的要求，建议采用多层次、多手段的方式对不同级别、类型的业务和数据进行保护。

对核心数据（数据库、重要的文件、日志数据等）采用持续数据保护方式复制到容灾平台上，基于存储的持续数据保护系统，能够从落盘的I/O级别对所有写入操作进行时间戳标记，并根据这些时间戳进行数据恢复。区别于一般的快照方式，I/O的方式对系统的消耗影响更小，恢复的时间点更加的密集，有更强的数据保护能力。

同时采用备份方案作为所有数据安全的兜底，对全院所有业务数据，以“应备尽备”为原则，全部进行数据备份；备份系统采用具备高去重率的备份体系，实现数据去重率高、兼容性好和备份效率高的特点，能够以较小的实际容量实现较大数据量的备份。

### 网络安全建设

本次方案将根据业务类型及安全需求将整个网络划分为多个安全区域，现分别阐述如下：

* **内网数据中心区**

数据中心主要运行医院信息化的生产业务系统，存储重要医疗数据，是整个信息系统的核心数据资产。

在数据中心边界处部署数据中心防火墙，承担对数据中心区的边界防护、访问控制功能。防火墙采用双机热备部署形式，确保网络结构的高可靠性。

* **数据备份恢复区**

作为数据中心的延伸部分，部署数据保护系统和数据恢复环境。通过软件边界防火墙与数据中心区域做虚拟机层面隔离。

* **运维管理区**

该区域主要整合全网的管理及运营维护功能，实际部署与内网数据中心一同部署。

在区域内部署漏洞扫描、运维审计、安全审计、综合日志审计及未知威胁分析，监控和记录各种入侵行为、威胁事件等，并进行可视化展示。

* **专线互联**

专线互联区主要承载专线对接的业务，如专线对接卫计委进行业务信息的上报等工作、和银行对接实现财务往来业务、和医保局对接进行人口健康上报等。

在边界处部署冗余下一代防火墙，承担对外联接入区的边界防护、访问控制、入侵防御等功能。

* **数据中心外网**

主要承载外网数据中心部署相关的应用系统，这些应用以虚拟化的方式部署在超融合平台之上。

在内外网边界部署双机隔离网闸，实现内外网访问隔离。

* **互联网外联**

该区域直接与互联网相连，主要承载着医院需要通过互联网完成的业务需求，如内部人员访问互联网、外部人员通过互联网对医院内部业务系统进行访问、远程运维人员通过互联网对医院信息系统的运维操作以及为广大患者群众提供的互联网+医疗服务。

在边界处部署下一代防火墙，通过自身的入侵防御模块，承担对互联网接入区的边界防护、访问控制功能，并提供对网络攻击的监控，阻断入侵行为。提供病毒过滤，防止病毒侵入扩散，与网络防病毒组成多层次深度防御

外网数据中心边界部署WEB应用防护系统，针对WEB应用进行防护。

在外网接入处部署上网行为管理，提供行为审计、流量控制功能，根据应用类型进行识别控制，限制用户的应用流量，为关键应用提供流量保证。

### 虚拟化安全设计

在虚拟化环境安全保障中，传统的防护手段所起到的作用是不能忽视的，但虚拟化环境的全面安全防护还是应该采用传统安全技术手段和虚拟化技术结合的方法。

在不同物理实体之间（服务器与服务器、主数据中心与备数据中心）采用传统的技术手段与虚拟化的技术手段进行防护。而对于同一物理实体之上的虚拟化应用则应采取有针对性的虚拟化技术手段进行防护。

为了应对虚拟化平台可能面临的威胁，建议在虚拟化平台安全方面通过软件定义网络技术和虚拟化安全技术相结合，达到快速的进行安全虚拟化和业务自定义。

为了加强数据中心内部的安全，对工作人员的访问权限进行认证和监控，防止非受权人员对信息资源的非法访问和抵御黑客的袭击，防止内网外联等非法网络使用行为，以保证系统内的数据不被损坏、丢失。同时防止病毒对计算机系统的破坏，保证用户终端的防病毒软件安装使用符合企业安全管理策略。虚拟化安全防护体系建议由分布式防火墙、虚拟化防病毒、入侵防御等构成，采用统一的、集中的安全策略管理，实现整个网络的全面防护。具体为：

1、在虚拟化平台上部署分布式防火墙对数据中心虚拟机与虚拟机之间的东西向流量数据交互进行防护，配合边界处的安全设备为整个数据中心提供东西南北棋盘式全维度的防护。

2、部署虚拟化云安全系统，实现虚拟机层面的DOOS、访问控制、入侵防御、病毒过滤功能。

# 工期要求

工期6个月，其中3个月建设，3个月完善。

# 质保要求

软件：1年

硬件：3年

# 总体技术要求

## 标准要求

本项目建设遵循以下标准（包含但不限于）：

国家卫健委《三级医院评审标准（2020年版）》

国家卫健委《医院信息互联互通标准化成熟度测评方案（2020年版）》

国家卫健委《医院智慧管理分级评估标准体系（试行）》

国家卫健委《医院智慧服务分级评估标准体系（试行）》

国家卫健委《全国医院信息化建设标准与规范》

国家卫健委《医院信息系统基本功能规范》

国家卫健委《卫生系统电子认证服务管理办法（试行）》

《信息安全等级保护管理办法》

《国卫办医发关于印发电子病历应用管理规范（试行）的通知》

## 技术路线

本项目建设软硬件应具备标准化、先进性、实用性、可维护性、安全性、整合性与扩展性、高性能等特点。

（1）标准化

必须按照国家卫健委发布的《医院信息管理系统规范》的要求以及国家信息管理的标准，能够满足硬件设备设计标准以及医院对于网络传输的需求，应当严格按照有关法定法规进行标准化设计，比如《电子计算机机房设计规范》《计算机站场地技术条件》等国家及行业标准。

（2）实用性和先进性

实用性和先进性采用先进成熟的技术和设备，尽可能采用先进的技术、设备和材料，以适应高速的数据处理与业务需要。

（3）可维护性

需要进行定期的维护，此外运行的方式需要满足简单，方便日后的维修，有效降低其标准成本。

（4）安全性

系统应满足实现系统7×24H连续安全运行，性能可靠，易于维护。保证设备安全的运营基础之上，更要保证子系统之间能够互相协调，支持其他管理系统、网络通信设备的应用，能够高效实现设备之间的数据传输，减少数据传输的等待时间。

（5）整合性与扩展性

所谓的系统拓展，即是指在保证原有系统能够进行安全操作运行基础之上，能够在设备以及技术上得到一定的拓展功能，以此来方便日后设备的升级，满足数据的存储空间。

（6）高性能

系统应充分考虑医院业务环境中运行的效率，防止死锁和并发操作。系统应支持自动任务管理，可以把比较大的，时实性不强的业务放到晚上执行，整个过程无须人工干涉以合理分配医院服务器的资源，提高医院服务器的利用率。

# 采购清单

## 软件

|  |  |  |
| --- | --- | --- |
| **序号** | **分类** | **子系统** |
| 1 | 智能化消化内镜网络信息系统 | 内镜服务端系统 |
| 预约登记系统 |
| 胃肠图文报告系统 |
| 智能化质控系统 |
| 主任审核工作站 |
| 信息化接口对接 |
| 2 | 产科信息管理系统 | 孕妇手机端 |
| 门诊护士工作站 |
| 门诊专科病历（医生端） |
| 住院部病历 |
| 数据上报 |
| 系统管理 |

## 硬件

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **分类** | **设备名称** | **数量** | **单位** |
| 1 | 网络安全设备及服务 | 互联网区域业务出口防火墙 | 2 | 台 |
| 2 | 互联网区域防火墙 | 2 | 台 |
| 3 | 互联网区域上网行为管理 | 1 | 台 |
| 4 | 互联网区域web防毒 | 1 | 台 |
| 5 | 互联网区域SSL vpn | 1 | 台 |
| 6 | 网闸 | 1 | 台 |
| 7 | 内网区域防火墙 | 2 | 台 |
| 8 | 内网区域日志审计 | 1 | 台 |
| 9 | 内网区域数据库审计 | 1 | 台 |
| 10 | 堡垒机 | 1 | 台 |
| 11 | 安全感知平台 | 1 | 台 |
| 12 | 业务专线防火墙 | 2 | 台 |
| 13 | 服务器安全 | 1 | 套 |
| 14 | 终端安全软件 | 1 | 套 |
| 1 | 数据安全设备及服务 | 数据资产测绘系统 | 1 | 套 |
| 2 | 数据接口风险监测系统 | 1 | 套 |
| 3 | 流量复制汇聚设备 | 1 | 台 |
| 4 | 数据防泄密系统 | 1 | 套 |
| 5 | 数据安全管控平台 | 1 | 套 |
| 1 | 桌面云终端 | 云服务器 | 1 | 台 |
| 2 | 云计算平台 | 2 | 套 |
| 3 | 云盘软件 | 1 | 套 |
| 4 | 云桌面控制器 | 1 | 套 |
| 5 | 胖云终端（含授权） | 50 | 点 |
| 6 | 显示器 | 50 | 台 |
| 7 | 键盘鼠标 | 50 | 套 |
| 8 | 数据中心交换机 | 1 | 台 |
| 9 | 万兆多模光模块 | 4 | 块 |
| 10 | 网络切换器 | 50 | 台 |
| 11 | 瘦云终端 | 50 | 台 |
| 12 | 瘦云终端授权 | 50 | 套 |
| 1 | 双活数据中心建设硬件及服务 | 业务外网超融合服务器 | 3 | 台 |
| 2 | 服务器虚拟化软件 | 6 | 套 |
| 3 | 虚拟化云安全 | 6 | 套 |
| 4 | 内网核心业务服务器 | 4 | 台 |
| 5 | 光纤交换机 | 4 | 台 |
| 6 | 存储虚拟化平台 | 2 | 套 |
| 7 | 核心全闪存存储 | 2 | 台 |
| 8 | 现有核心存储扩容硬盘 | 1 | 批 |
| 9 | 内网超融合设备 | 4 | 台 |
| 10 | 影像存储 | 4 | 台 |
| 11 | 备份软件 | 1 | 套 |
| 12 | 备份设备 | 1 | 台 |
| 13 | 容灾服务器 | 2 | 台 |
| 14 | 容灾光交 | 1 | 台 |
| 15 | 容灾存储 | 1 | 台 |
| 16 | 可持续性数据保护软件 | 1 | 套 |
| 17 | 避风港接入交换机 | 1 | 台 |
| 18 | 避风港区域备份 | 1 | 套 |
| 19 | 备份复制设备 | 1 | 台 |
| 20 | 数据避风港软件 | 1 | 套 |
| 21 | 避风港区域服务器 | 1 | 台 |
| 22 | 内网端服务器虚拟化软件 | 30 | 套 |
| 23 | 内网端虚拟化管理中心 | 3 | 套 |
| 24 | 配套辅材及线材 | 1 | 批 |
| 25 | 系统集成服务 | 1 | 套 |

# 软件参数要求

## 智能化消化内镜网络信息系统

### 消化内镜网络服务端模块

* 基于当前主流操作系统和数据库设计。
* 整套系统采用平台化、一体化的设计，平台上各个系统采用同源同构的设计，相互之间可以实现无缝集成。
* 客户端支持WIN 7/WIN 10（32位或64位）操作系统。
* 系统提供7×24小时运行。
* 系统在生产环境部署，项目实施工作不能影响医院现有工作。
* 完整的权限控制，合法用户方可使用。
* 新购设备能顺畅接入系统。
* 系统遵循DICOM3.0、HL7、IHE国际标准。
* 支持DICOM 3.0 Storage SCP（影像存储）、SCU（影像发送）、Query/Retrieve（查询获取）。
* 支持DICOM 3.0压缩服务和存储验证服务。
* 为杜绝形成信息孤岛，系统需符合IHE（Integrating the Healthcare Enterprise）医疗信息系统集成规范。
* 支持HL7标准,WebService或中间件方式的集成方式。
* ★提供IHE-C基础PACS标准规定整体通过合格证书。
* ★消化内镜系统可支持与省/国家消化内镜质控平台对接（提供软件截图）。

### 预约登记工作站

* 可根据HIS提供的信息，将病人基本资料及临床检查信息自动获取模块。
* 提供患者登记功能，产生患者排队队列。
* 对不同申请类型的病人显示不同的颜色和优先级。
* 可直观显示各个检查室的患者分配情况。
* 提供数据检索功能，可以通过各种条件检索预约登记的患者信息。
* 支持可视化的排队安排界面，护士可快速对病人进行预约排队安排。
* 预约签到：对于已预约病人，根据预约信息签到并安排检查。并可补充登记检查信息。
* 分诊调整：对因故不能立即检查的病人，可人工调整其分诊排队顺序。对急诊病人，也可提前排队顺序。
* 语音叫号：分诊台可播放语音叫号。语音信息需能读出病人中文姓名等各种信息。可由用户自行设定。
* 分诊大屏：分诊信息可以显示在病人集中候诊处的大屏幕显示器上。
* 绿色通道病人处理：对于因各种紧急或特殊情况未正常挂号、登记、收费的病人提供特别处理流程。非特殊病人必须先收费后检查。
* 医生操作终端具有顺序呼叫、重复呼叫、选择呼叫功能。

### 消化内镜图文报告工作站

* 候诊队列可根据房间、检查类型进行过滤显示。
* 可通过患者预约信息条码快速定位病人，并进行检查前的二次确认。
* 支持各种内镜视频接口，包括DVI、SDI、RGB/YUV、S-VIDEO、复合视频。
* 支持内镜、超声高清信号采集，分辨率最大可1920\*1080。
* DICOM3.0标准：全面符合DICOM影像标准, 标准化图像采集与归档。
* 支持图像的自动裁剪，报告打印时系统可将黑边剪切掉。
* 提供脚踏开关控制采集图片操作。
* 可将图像导出成BMP、JPG、DCM计算机通用格式。
* 采集的动态视频可进行二次提取。
* 静态影像与动态影像采集可同时进行，互不影响。
* 采集的图像转换为标准DICOM格式统一存储。
* 支持内镜标清，高清信号动态采集（录像）。采集帧数大于等于25帧/秒。采集段数不受限制，采集时间大于30分钟。
* 支持超声内镜标清，高清信号动态采集（录像）。采集帧数大于等于25帧/秒。采集段数不受限制，采集时间大于30分钟。
* 支持X光信号的动态采集（录像）。采集帧率大于等于25帧/秒。采集段数不受限制，采集时间大于30分钟。
* ★ERCP工作站同时支持放射线、内镜2路视频信号的同录同播。（提供软件截图）
* ★超声内镜工作站同时支持超声、内镜两路视频信号的同录同播。（提供软件截图）
* 多线程操作：允许在编辑上一病人报告同时采集其他病人的图像。
* 报告书写时，患者列表可根据科室需求自定义类别分类显示。
* 报告模板：根据患者的诊断部位调用已定义的典型报告模板，模板调入后可加以编辑，快速生成影像诊断报告。
* 支持病例“阳性”标记，可以统计阳性率。
* 可以将病例标记为“典型病例”。
* 以供科研和教学使用。医生可以建立个人病例收藏夹。
* 支持多条件组合模糊查询。具有快速检索、高级检索多种方式。
* 报告的打印格式支持客户化定制，打印输出时，支持根据用户选择图像的数量智能选取报告格式。
* 图像描述：支持报告中对图像性质的描述，其文字内容由诊断医生输入，并在报告上打印出来。
* 具有开放的解剖示意图库功能。可对各个部位的解剖示意图进行编辑，连同报告一起打印出。
* 具备自动患者匹配功能，如该患者以前在本科室有过检查历史，则自动将多次检查归入同一患者名下。
* 根据图像数量，自动选择报告格式。
* 可与病理系统集成，实现病理申请及结果的互联互通。（需与病理系统做接口）

### 智能化质控

* 质控模块深度嵌入当前消化内镜系统界面，非第三方外挂系统。UI设计规范和操作规范与当前系统一致。
* 所有图文报告工作站（带有采集卡的）均具有人工智能智能识别功能。
* ★基于图像分析技术对工作站所采集的静态图片进行自动识别，可分析上消化道部位，达盲率，退镜时长，胃镜检查时长。
* AI计算服务端，提供面向所有内镜工作站所采集的图片智能化识别。I7,16G内存，3080显卡，1TB SSD硬盘，支持6个终端工作站。
* ★系统可支持与国家消化内镜质控平台对接，支持国家消化内镜质控指标的自动汇总、自动计算、自动上传。（需支持内外网互联）
* 科室运营数据实时显示，显示包括：患者平均等待时间，已报到患者数量，已预约患者数量，各操作间检查数量等。
* 科室质控数据实时显示，按照国家消化内镜中心中心要求的质控指标数据显示。

### 主任审核工作站

* 支持按用户类别或者组类别赋予使用权限。
* 系统的所有用户由系统管理员统一创建，并根据该用户在业务流程中担任的角色设置用户权限，还可根据用户需求设置初始密码。可按用户或者组类别赋予使用权限，支持对个别用户或者用户组，分配使用或者变更系统资源及数据的使用控制功能。
* 每个用户必须使用各自的ID和密码登录系统，访问系统中的数据。
* 支持特殊疾病的统计和查询。
* 支持阳性率统计。
* 支持将检查信息导出到Excel。
* 支持登记员工作量统计，检查技师工作量统计。
* 支持按时间段工作量统计。
* 支持检查项目明细统计。
* 支持申请科室明细统计。
* 支持报告医生、审核医生工作量统计。
* 可根据科室的工作需要，设计定制化的统计报表，报表可导出电子表格，或者直接进行打印。
* 可根据科室管理的需要，设计定制化的绩效统计报表。报表可导出电子表格，或者直接进行打印。

### 信息化集成

* 实现电子申请单的获取，申请单状态回传。
* 在内镜系统中调取门诊和住院电子病历，电子病历提供EXE/WEB方式显示调阅，电子病历引用内镜报告。
* 内镜报告以PDF的格式进行整体归档。
* 提供web方式嵌入到电子病历系统中，临床通过web进行内镜报告调阅。

## 产科信息管理系统

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **模块** | **功能** | | **功能要求** |
|  | 产科门诊 | 孕妇手机端 | 自助建档 | 基本信息、本孕信息、孕产史等孕册信息。 |
|  | 产检提醒 | 孕期常规产检提醒包括产检孕周、产检内容、产检注意事项。 |
|  | 产检复诊，根据预约日期提前发送复诊提醒，当天未复诊发送超时提醒。 |
|  | 孕妇学校 | 支持图文并茂的宣教文章，支持点赞、收藏。 |
|  | 支持视频宣教内容，点赞、收藏。 |
|  | 支持查阅护士端发布的课程，进行线上预约、现场扫码签到/出示二维码签到。 |
|  | 产科随访闭环 | ★支持移动端接收PGDM依从性、线下课程学习情况、线下课程满意度、心理评估表、科室满意度等类型问卷，进行问卷填写，提交等。 |
|  | 支持在线填写、提交、及根据问卷得分情况提示注意事项。 |
|  | 电子产检本 | 提供PDF格式的标准版产检本模板；支持建档、首诊、复诊、居家监护、孕期曲线等产检记录生成电子产检本，支持检验检查内容合并查看，支持转发、打印。 |
|  | 个人健康记录 | 包括体重、血压、血糖、体温、胎动记录的居家监护数据。 |
|  | ★支持手动录入，系统自动在线判断和解析居家监测数据，并给出风险分类提示；数据同步医生工作站。 |
|  | 围产码 | ★支持根据建档信息自动生成电子围产码；支持用户扫码进行自助体检、胎心监护产检报到等。 |
|  | 出生证预约办理 | 自动同步住院产妇、新生儿信息，支持在线预约办理出生证时间。 |
|  | 业务集成 | 支持通过安全授权方式集成到医院公众号或小程序或APP；支持统一的推送集成。 |
|  | 护士工作站 | 护士首页 | 自动统计护士工作量（建档、宣教、随访），待处理事件（待审核、待上报、随访任务等），复诊到诊量，孕妇学校情况等。 |
|  | 建档与结案 | 支持护士在线建档；支持输入身份证、手机号等方式进行搜索建档用户；支持护士端进行结案管理。 |
|  | ★支持在线审核，支持对接硬件实现认证合一，支持身份证读卡器、扫码枪扫二维码方式查询用户；支持一键审核建档，孕册锁定。 |
|  | 体征管理 | 支持孕妇手机录入，支持对接设备测量血压，数据同步移动端、护士端、医生专科病历中，测量设备支持国内主流品牌，血压测试支持多次记录。 |
|  | 支持孕妇手机录入，支持对接设备测量体重，数据同步移动端、护士端、医生专科病历中。 |
|  | 外院报告&知情同意书管理 | 支持高拍仪录入外院检验检查和知情同意书；支持知情同意书模版配置。 |
|  | 支持单标记外院报告类型及信息，支持同步到检验报告、影像报告列表中；支持病人病例页上传或集中上传两种方式。 |
|  | 健康宣教 | 支持知识库管理，包括图文内容、视频等。 |
|  | ★支持自定义宣教流程，包括组合条件自定义用户类型、自定义发送时间及频率的设定。 |
|  | 系统需内置常规产检提醒；支持多种知识库内容管理；支持生成宣教记录，发送异常记录。 |
|  | 孕妇学校 | 支持课程排班设置，支持编辑开课介绍、主讲人、目标用户、开课时间等信息，支持对课程发布。 |
|  | 发布的课程内容，支持目标对象移动端结束开课提醒，支持在线预约。 |
|  | 支持统计预约人数，支持孕产妇现场 扫码/出示二维码签到，支持课中、课后发送问卷；支持统计开课情况，孕产妇个人听课情况管理。 |
|  | 随访管理 | ★支持问卷模版配置，支持添加单选、多选、填空题、支持建立题型关联的问卷；支持自定义随访流程，自定义用户类型，随访频率，支持设定推送时间和周期自动生成随访任务、自动统计工作量，自动形成问卷测评报告。 |
|  | 支持电话随访，记录随访结果，支持对接电话设备，在线拨打随访并记录随访结果；支持推送问卷随访，同步孕产妇填写详情。 |
|  | 支持统计随访情况，查阅随访记录，随访详情，及导出随访结果。 |
|  | 转诊管理 | 支持转入登记、转出登记；支持越级转诊提醒配置。 |
|  | 支持统计转入转出患者追踪管理；支持转诊单打印及归档。 |
|  | 门诊统计报表 | 1. 建档统计：系统自动统计建档孕妇信息，包括：建档日期、孕妇姓名、孕妇电话、建档编号、末次月经等信息，并生成统计报表，支持导出功能，便于数据上报。 2. 高危统计：支持根据评定高危的用户自动统计，支持筛选各类高危等级，支持根据评定日期、居住地址等筛选用户，支持显示用户当前高危因素及历次高危评定记录。 3. 追访统计：对系统建档的孕妇进行追访，记录复诊提醒统计、超时复诊提醒统计、电话随访统计等信息进行统计。 4. 唐氏筛查统计：自动统计唐氏筛查情况、筛查孕妇的基本信息、筛查结果、NIPT、产前诊断结果、分娩结局等。 5. 待分娩统计表：对孕晚期（孕37周及以上）孕妇进行自动统计，便于统计即将分娩的孕妇情况。 6. 艾梅乙检测统计。 7. 医生工作量统计：支持根据科室医生在系统接诊的工作量情况，包括总数，首诊、复诊、产后各人数，孕产妇高危分布情况等。 8. 护士工作量统计：支持根据科室护士在系统建档、审核、宣教、随访、开课等情况进行统计。 9. 科室就诊统计：依据日期统计科室每日接诊的数量，包括首诊、复诊、产后复诊、孕产妇高危分布情况，转诊数量；支持查看每天接诊患者详情。 |
|  | 出生证预约管理 | 支持同步移动端预约信息，支持打印及签发，形成签领记录。支持补发、变更管理。 |
|  | 门诊专科 病历（医生端） | 单点登录&电子病例集成 | ★以安全授权网页方式内嵌在HIS、电子病历系统或门诊医生工作站，支持在HIS、电子病历系统或门诊医生工作站一键打开产科信息系统；支持同步电子病历到门诊病历系统；支持ICD10~11诊断库模板，支持自定义模板。 |
|  | 医生首页 | 自动生成医生首页，包括工作量情况，预约人数，患者分布情况等。 |
|  | 首诊管理 | 包括病史、孕产史、月经史、体格检查、专科检查、实验室必查、诊断处理等电子首检病历信息管理，支持异常值提醒，自动导入手机端/护士端保存的建档信息。 |
|  | ★支持自动解析本院报告结果，支持报告结果直接引用，支持异常报告红色预警。 |
|  | 复诊管理 | 支持添加复诊记录、提供诊断、处理等模板，支持记录下次复诊时间并给孕妇推送产检提醒。支持查看历次诊断记录、历次复诊记录。 |
|  | 诊断、主诉、处理模板 | 支持ICD-10诊断库，支持全院、科室、个人模板维护。 |
|  | 实验室检验报告 | ★支持查看实验室报告，异常提示；支持报告结构化解析。 |
|  | 影像检查报告 | ★支持查看影像报告，支持报告结构化解析。 |
|  | 高危管理 | ★根据孕妇病史、诊断，智能定位预判对应的高危因素细项，提示医生标记，支持在提示框一键标记高危因素，支持病情变化时提示动态标记，支持色卡管理和高危专案闭环管理等。支持自动根据解析异常结果触发弹框漏诊提醒功能。 |
|  | 高危快讯 | ★集中提醒孕妇近期的检验检查缺漏、专案跟踪异常的情况，包括检验检查的缺漏、最近检验检查异常、专案监测异常等。该查看功能支持展开、收起查看详细信息。 |
|  | 自动孕期曲线 | ★自动解析产检信息、影像数据，自动生成孕期曲线，包括BMI、妊娠图、胎儿生长曲线等，其中胎儿生长曲线支持配置中国南方人群与NICHD亚裔人群版本。 |
|  | 产前必查检验清单 | 门诊必查清单，支持手动录入报告结果，根据报告日期自动生成时间轴。 |
|  | ★支持自动解析报告结果，缺漏和异常提示。 |
|  | 专病风险评估 | 支持瘢痕子宫、深静脉血栓、子痫前期等风险评估。 |
|  | ★深静脉血栓、子痫前期评估表支持自动解析病历判断高风险因素弹出评估表。 |
|  | 专案管理 | 根据指南、专家共识的病种，形成专案病历、风险评估、产检指导等，如GDM/PGDM、甲减、子痫前期、梅毒、瘢痕子宫、深静脉血栓、双（多）胎、ICP、心血管系统疾病、前置胎盘、巨大儿、羊水过多、羊水过少、胎儿生长缓慢（受限）等。 |
|  | ★糖尿病专案管理  建立糖尿病高危专案，管理糖尿病高危专病，可在接诊页查看血糖监测情况，复诊自动关联血糖、血红蛋白、胰岛素监测指标；支持根据专案自动生成处理措施建议。 |
|  | ★高血压专案管理  建立高血压高危专案，管理高血压高危专病，复诊自动关联尿蛋白定量、24h尿蛋白等监测指标，更集中地关注到专案病情变化；支持根据专案自动生成处理措施建议。 |
|  | ★ICP专案管理  建立ICP高危专案，管理ICP高危专病，复诊自动关联胆汁酸、肝功等监测指标，更集中地关注到专案病情变化；支持根据专案自动生成处理措施建议。 |
|  | ★双胎多胎妊娠专案管理  建立双胎、多胎高危专案，管理双胎多胎高危专病，复诊自动关联胎儿估重、羊水等超声监测指标，支持录入多胎的胎心、先露等产检指标；支持根据专案自动生成处理措施建议。 |
|  | 产检计划 | ★针对指南或专家共识中未涵盖的，科室形成规范流程的支持自定义产检计划。 |
|  | 居家监护 | 同步孕妇居家监护的数据，包括血糖、血压、胎动等，异常标红。 |
|  | 产检报告打印 | 支持单页病历和完整电子产检本，支持病例归档。 |
|  | 产科住院 | 住院部病历 | 护理白版 | ★护理白板区分待分娩和已分娩分别监测孕产妇关键指标，待分娩白板显示高危因素、胎儿监护信息、宫口扩张情况、孕妇生命体征等信息，已分娩白板显示孕妇体征、新生儿情况、24小时阴道流血量、高危等级、高危因素、重要事件等信息，支持投屏显示。 |
|  | 电子病历 | 住院病历支持整个住院生产的全程病历记录。 |
|  | ★支持门诊全景病历，支持文书化和结构化显示。 |
|  | ★支持产时、产后高危管理。 |
|  | 支持自动产程图绘制。 |
|  | ★支持三网监测、艾梅乙等报卡管理。 |
|  | 支持解析护理记录、分娩记录、新生儿记录等结构化导入。 |
|  | 文书管理 | 护理纸质表单全部实现电子化，支持打印。 |
|  | 知情同意书归档闭环 | ★支持知情同意书、申请单在线编辑打印，支持高拍仪导入签名知情同意书，支持同意书归档管理；支持文书编辑设置，可以自定义编辑文书。 |
|  | 住院报表 | 1. 接生登记本统计：根据孕妇建档信息、分娩信息、新生儿信息生成接生登记本，生成统计图表，支持预览、打印、导出功能。 2. 分娩信息上报统计：根据建档信息、分娩信息、新生儿信息生成分娩信息上报记录，若市平台/省平台接口支持，自动完成建档信息、首诊信息、复诊信息、分娩信息的上报。 3. 筛查登记本统计：根据新生儿记录生成筛查计划，根据筛查清单对新生儿疾病筛查登记本进行数据采集及完善，并支持打印采血卡等。 4. 门诊住院率统计：统计孕妇从门诊建档到最后在最终分娩的人数，自动统计出门诊住院率以及产妇流失率。 5. 出血量统计：对住院产妇出血量进行统计，可以筛选出血范围统计，支持导出。 6. 新生儿听力筛查：根据新生儿记录生成需要听力筛查的儿童记录，支持筛查结果进行登记，打印。 7. 围产儿年报表：依据产妇年龄段、性别和城乡分别统计出围产儿的人数，并形成年度报表，支持预览、打印、导出excel。 8. 孕产妇死亡登记卡：登记死亡孕产妇姓名、年龄、死亡日期、死亡原因、死因分类、死亡地点、ICD-10死亡诊断等信息，形成统计报表，支持导出、预览、打印。 9. 围产儿死亡登记卡：登记死亡围产儿的性别、出生日期、出生体重、孕周、死因分类等信息，形成统计报表，支持导出、预览、打印。 10. 围产儿缺陷登记卡：登记缺陷围产儿的性别、出生日期、缺陷类别等信息，形成统计报表，支持预览和打印。 11. 产科医疗质量指标统计：系统自动生成本院建档孕产妇及新生儿的剖宫产率、初产妇剖宫产率、阴道分娩椎管内麻醉使用率、早产率、早期早产率、巨大儿发生率、严重产后出血发生率、严重产后出血患者输血率、孕产妇死亡活产比、妊娠相关子宫切除率、产后或术后非计划再次手术率、足月新生儿 5 分钟 Apgar 评分＜7 分发生率。 |
|  | 数据上报 | 数据上报 | 建档信息 | 支持建档信息自动上报区域平台，异常提示。 |
|  | 首诊信息 | 支持首诊信息自动上报区域平台，异常提示。 |
|  | 复诊信息 | 支持复诊信息自动上报区域平台，异常提示。 |
|  | 分娩记录 | 支持分娩信息自动上报区域平台，异常提示。 |
|  | 系统基础配置 | 系统管理 | 用户账号管理 | 支持添加、删除、编辑用户账号及关联角色。 |
|  | 用户角色管理 | 支持添加、删除、编辑角色及匹配权限。 |
|  | 操作审计记录 | 生成病历所有修改记录。 |
|  | 任务设置 | 支持新增、启动、关闭等任务管理。 |
|  | 表单配置 | 支持自定义移动端、护士端、医生端首诊、复诊产后复诊等表单的配置。 |
|  | 打印模板配置 | 支持定制化打印模板变量，支持配置打印的样式等。 |
|  | 质控驾驶舱 | 高危孕产妇管理：包括高危等级分布、支持显示高危病种分布。 |
|  | 门诊复诊管理，包括按时复诊率、超时复诊率、超时追回成功率。 |
|  | 分娩管理，支持统计各种分娩方式人数，支持统计小于37周、38~40周、41~42周、42周以上。 |
|  | 科室门诊转诊情况，支持统计科室转入转出人数。 |
|  | 科室工作量情况：支持统计建档、宣教、随访、医生工作量情况等。 |
|  | 产科质量指标，依据全国质量指标需要的数据，自动统计数据。 |
|  | 病历情况分析：支持多胎、初产妇、瘢痕子宫等。 |
|  | 系统引导 | 支持在线文档和系统引导，方便系统学习和使用； |
|  | 支持专科知识库管理方便查阅指南、专家共识等内容。 |
|  | 病例模版配置 | 支持备查清单、诊疗计划、高危专案（GDM、妊娠高血压）等配置，快速支持临床需求变更等。 |
|  | 系统风格、主题 | 系统包括多种主题样式；医生工作站支持集中首诊病历风格、TAB导航等风格。 |
|  | 接口管理 | 第三方数据接口 | 第三方数据接口（包括但不限于HIS系统、LIS系统、PACS系统、区域妇幼平台/省级妇幼平台、系统集成平台等） | 1. HIS系统第三方数据采集：HIS系统开放接口，需达到与院内信息管理系统互联互通,包括但不限于获取病人信息、挂号信息、门诊普通病历信息。 2. LIS系统第三方数据采集， LIS系统开放接口，需达到与院内检验科信息系统信息互联互通,获取用户的检验结果，包括但不限于患者的血常规、尿常规。 3. PACS系统第三方数据采集， PACS系统开放接口，需达到与院内影像系统信息互联互通，获取病人影像报告结果信息，包括但不限于患者每次来院检查的超声报告。 4. 系统需要与区域妇幼平台/省级妇幼平台做到数据自动上报。 5. 支持与医院其他系统对接。 |

# 硬件参数要求

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **设备名称** | **参数** | **数量** | **单位** |
| **桌面云终端** | | | | |
| 1 | 云服务器 | 1、服务器要求为19英寸工业标准2U机架式服务器，提供4个USB接口，其中USB 3.0≥3个  2、CPU：配置2颗Intel处理器，每颗CPU≥16核心32线程，主频≥2.9Ghz  3、内存：服务器提供≥24个内存插槽，配置≥384G内存；为保证后续服务器扩容性，在配置384G内存后，需具备≥12根内存的扩容能力  4、具备≥12个前置硬盘盘位，配置≥3\*8T 3.5寸 HDD硬盘，配置≥1\*240G SSD硬盘，配置≥1\*480G SSD硬盘  5、网口：提供≥2个千兆电口，≥2个万兆光口，≥1个千兆管理口  6、电源：提供2个电源模块，支持1+1电源冗余 | 1 | 台 |
| 2 | 云计算平台 | 1、要求采用超融合架构，在同一管理平台内至少包含计算资源、存储资源、网络资源等功能管理模块。  2、管理平台为B/S架构，中文界面，同一管理界面中可实现对计算、存储、网络等功能的配置操作。  3、支持向导式添加主机节点，为降低部署难度，支持精简纳管主机节点，仅需输入主机节点名称、主机IP地址即可完成主机节点添加。  4、支持查询主机节点名称、管理IP、连接状态、描述、创建时间、CPU、内存、硬盘、网卡、主机心跳等信息  5、支持主机性能状态监控，能以小时、天、周、月、季度、半年、一年维度，对主机CPU使用率、内存使用率、磁盘速率、磁盘IOPS、网卡错误数、丢包率、网卡带宽进行性能监控记录  6、支持将服务器主机节点添加为计算集群，为上层业务平台提供统一的计算、存储、网络资源调度，形成基础计算平台支撑  7、支持查询集群名称、节点个数、CPU总数、内存总数、已使用计算性能等信息  8、单套授权软件能提供1颗物理CPU激活码 | 2 | 套 |
| 3 | 云盘软件 | 1、可以与云桌面实现联动，在用户登录云桌面时自动登录，不需二次身份认证。  2、提供个人存储空间，实现个人云盘文件的存储、分享等功能  3、可根据实际情况建立不同的分组，分组由群主进行管理，可删除文件，群组成员可在组内进行资源上传、查看、下载等操作。文件内容可支持文本、图片、PPT、WORD、EXCEL、音频等种文件格式。  4、可通过配置支持通过互联网访问内网云盘数据，实现云盘的互联网访问 | 1 | 套 |
| 4 | 云桌面控制器 | 提供云桌面管理、镜像管理、用户管理、终端管理、策略管理等功能模块 | 1 | 套 |
| 5 | 胖云终端（含授权） | 1、软硬件一体化设备，内置虚拟化系统和软件。  2、配置≥Intel第十代i5（处理器主频≥2.4GHz）；内存≥8GB，显卡≥Intel UHD 630；本地存储≥256 GB SSD；802.11ac无线网卡  3、USB接口≥8个（包含≥4个USB 3.0接口），≥1个千兆网口，≥1个VGA接口，≥1个HDMI接口，≥1对音频输入输出接口，且支持4段式耳机音频输入及输出  4、配置≥1个内存扩展槽，配置≥1个硬盘扩展槽  5、为了降低部署难度，终端首次上电后支持终端配置向导，无需管理员账号即可实现终端配置，降低配置难度。  6、为了适用不同的业务应用场景，终端支持多种模式切换，包含但不限于个人桌面使用的个性化模式、公共桌面使用的还原模式、公共查询端使用的无账号公用模式。  7、为了便于终端部署在办公桌面底部，终端需提供外延电源开关接口，方便开关机。  8、终端支持终端自身及虚拟桌面IP地址设置，为了便于管理，能够通过web管理端进行IP地址修改与维护。  9、支持上电自启动功能，并能够根据实际使用情况选择关闭或开启。  10、保障业务连续性，在网络中断的情况下，依然支持离线使用虚拟云桌面。 | 50 | 点 |
| 6 | 显示器 | 1、屏幕尺寸: ≥21.5英寸  2、屏幕分辨率: ≥1920x1080像素  3、屏幕比例: 16:9  4、接口类型：HDMI  5、提供三年质保 | 50 | 套 |
| 7 | 键盘鼠标 | USB键盘鼠标套装 | 50 | 套 |
| 8 | 数据中心交换机 | 1、交换容量≥4Tbps，转发性能≥1900Mpps  2、固化10G SFP+光端口≥48个，40G/100G QSFP28端口≥8个  3、工作温度0°~45°  4、支持虚拟化技术，将多台设备虚拟为一台使用  5、支持Telnet、Console、SSH、SNMP v1/v2/v3等管理方式  6、支持静态路由、RIP、RIPng、OSPF、OSPFv3、BGP、BGP4+、ISIS、ISISv6  7、支持VXLAN网桥、支持VXLAN网关，支持EVPN VxLAN | 1 | 台 |
| 9 | 万兆多模光模块 | 原厂光纤模块，支持标准的万兆SFP+接口，适用于SFP+多模接口，850nm，传输距离300M | 4 | 块 |
| 10 | 网络切换器 | RJ45网络切换器1进2出，含配套网络跳线 | 50 | 台 |
| 11 | 瘦云终端 | 1、为保证软件运行的兼容稳定，需采用X86架构的云终端  2、处理器不得低于四核，处理器主频不得低于1.44GHz,睿频可达1.92G Hz，内存容量不低于2GB；提供不少于8GB的内置存储空间  3、接口不少于5个USB 2.0接口、1个USB3.0口、1个GE口、1对音频输入输出接口、1个VGA接口、1个HDMI口  4、具备防盗设计的显示器背挂架  5、支持主流办公软件，如Office,flash等，保障办公业务平稳开展  6、支持锁屏功能，用户可以通过锁屏键从虚拟桌面退回到登陆界面，防止用户离开座位时系统被他人误操作  7、支持桌面抢占功能，用户在A处登陆虚拟桌面后，若在B处再登陆同一账户，则可以登陆成功并且A处会自动退出 | 50 | 台 |
| 12 | 瘦云终端授权 | 包含1个VDI桌面授权，按桌面并发数授权 | 50 | 套 |
| **网络安全设备及服务** | | | | |
| 1 | 互联网区域业务出口防火墙 | 1. 网络处理能力≥10G，并发连接≥260万，每秒新建连接≥18万/秒， 标准2U机箱，冗余电源，配置≥6个10/100/1000M自适应电口，≥4个SFP插槽，≥2个SFP+万兆光口，支持两个扩展槽，1个Console口，支持液晶屏。含三年病毒库和三年入侵防御特征库升级服务、三年硬件维保服务。利旧1台。 2. 支持VTEP（VxLan Tunnel EndPoint）模式接入VxLAN网络，并可作为VXLAN二层、三层网关实现VxLan网络与传统以太网的相同子网内、跨子网间互联互通；支持通过绑定VLAN、VNI（VXLAN Network Identifier）、远程VTEP，手动管理VxLan网络；支持MAC、VNI、VTEP静态绑定。 3. 支持支持静态路由、策略路由及动态路由。策略路由支持用户自定义其优先级，动态路由应至少支持RIP v1/v2/ng， OSPFv2/v3，BGP4/4+协议；必须支持静态和动态多播路由，动态多播路由必须支持PIM-SM（稀疏模式）。 4. 支持NAT64，NAT66、NAT-PT等种IPv4/v6过渡技术，支持针对ICMPv6以及IPv6扩展头防护功能。 5. 支持在虚系统内独立配置病毒防护、漏洞利用防护、间谍软件防护、URL过滤、文件过滤、内容过滤、邮件过滤、行为管控等安全功能。并可支持对本虚系统内产生的日志进行独立审计。 6. 支持对最多6级的压缩文件进行解压查杀。 7. 产品的漏洞防护特征库及间谍软件库包含高危漏洞攻击特征，至少包括“永恒之蓝”、“震网三代”、“暗云3”、“Struts”、“Struts2”、“Xshell后门代码”以及对应的攻击的名称、CVEID、CNNVDID、CWEID、严重性、影响的平台、类型、描述、解决方案建议等（CVEID、CNNDID、CWEID等信息在漏洞攻击特征中体现）详细信息。 8. 能够对HTTP/FTP/POP3/SMTP/IMAP/SMB六种协议进行病毒查杀；本地病毒库规模大于3000万。 9. 支持基于主机或威胁情报视图，统计网络中确认被入侵、攻破的主机数量，至少可查看被入侵、攻破的时间、威胁类别、情报来源、威胁简介、被入侵、攻破的主机IP、用户名、资产等信息；并对威胁情报发现的恶意主机执行自动阻断。 10. 支持自定义基于TCP、UDP、HTTP协议的间谍软件特征。间谍软件特征可通过多个字段以文本或正则表达式的形式进行有序和无序匹配；并可自定义间谍软件的源、目的端口范围。   为保障应急响应能力，要求制造厂商为网络安全应急服务支撑单位（国家级）、国家信息安全漏洞库（CNNVD）技术支撑单位（一级）；（投标时须提供相关证书复印件加盖公章佐证）。 | 2 | 台 |
| 2 | 互联网区域防火墙 | 1. 网络层吞吐量≥20G，并发连接≥350万，每秒新建连接数≥25万，标准2U机箱，冗余电源，标准配置1个Console口 、1个HA接口，1个MGT接口，≥6个千兆以太网电口，≥4个SFP插槽，≥2个SFP+插槽，≥2个接口板卡扩展插槽，支持液晶屏，三年硬件维保服务。病毒防护特征库、入侵防御特征库升级服务，另外利旧两台。 2. 支持VTEP（VxLan Tunnel EndPoint）模式接入VxLAN网络，并可作为VXLAN二层、三层网关实现VxLan网络与传统以太网的相同子网内、跨子网间互联互通；支持通过绑定VLAN、VNI（VXLAN Network Identifier）、远程VTEP，手动管理VxLan网络；支持MAC、VNI、VTEP静态绑定。 3. 支持支持静态路由、策略路由及动态路由。策略路由支持用户自定义其优先级，动态路由应至少支持RIP v1/v2/ng， OSPFv2/v3，BGP4/4+协议；必须支持静态和动态多播路由，动态多播路由必须支持PIM-SM（稀疏模式）。 4. 支持NAT64，NAT66、NAT-PT等种IPv4/v6过渡技术，支持针对ICMPv6以及IPv6扩展头防护功能。 5. 支持在虚系统内独立配置病毒防护、漏洞利用防护、间谍软件防护、URL过滤、文件过滤、内容过滤、邮件过滤、行为管控等安全功能。并可支持对本虚系统内产生的日志进行独立审计。 6. 支持对最多6级的压缩文件进行解压查杀。 7. 产品的漏洞防护特征库及间谍软件库包含高危漏洞攻击特征，至少包括“永恒之蓝”、“震网三代”、“暗云3”、“Struts”、“Struts2”、“Xshell后门代码”以及对应的攻击的名称、CVEID、CNNVDID、CWEID、严重性、影响的平台、类型、描述、解决方案建议等（CVEID、CNNDID、CWEID等信息在漏洞攻击特征中体现）详细信息。 8. 能够对HTTP/FTP/POP3/SMTP/IMAP/SMB六种协议进行病毒查杀；本地病毒库规模大于3000万。 9. 支持基于主机或威胁情报视图，统计网络中确认被入侵、攻破的主机数量，至少可查看被入侵、攻破的时间、威胁类别、情报来源、威胁简介、被入侵、攻破的主机IP、用户名、资产等信息；并对威胁情报发现的恶意主机执行自动阻断。 10. 支持自定义基于TCP、UDP、HTTP协议的间谍软件特征。间谍软件特征可通过多个字段以文本或正则表达式的形式进行有序和无序匹配；并可自定义间谍软件的源、目的端口范围。   11、为保障应急响应能力，要求制造厂商为网络安全应急服务支撑单位（国家级）、国家信息安全漏洞库（CNNVD）技术支撑单位（一级）；（投标时须提供相关证书复印件加盖公章佐证） | 2 | 台 |
| 3 | 互联网区域上网行为管理 | 1. 带宽≥500M网络环境使用；最大并发连接数≥60万;最大新建连接数≥35000个/秒；2U硬件;配置≥6个千兆电接口（其中含1个管理接口和1个HA接口）;≥2个扩展槽（可选配扩展网卡）;≥1T硬盘;冗余交流电源。含三年软件版本升级服务;提供新版本功能优化与性能提升价值。 URL库、应用协议库定期更新;保持对网络应用识别与管理的有效性；三年硬件质保服务。 2. 设备必须提供物理硬件bypass按钮，便于设备巡检、设备故障时管理员无需重启、关机、断电即可恢复网络通畅。 3. 设备在部署时支持模式选择，可设置为Portal模式，实现Portal服务器功能。 4. 可集中呈现上网行为风险等级和状态。行为风险等级包括安全等级、效率等级、合规等级和管控等级。行为状态包括管控效果、运行状态、安全状态、泄密风险状态、合规状态和应用使用状态。 5. 支持与云端杀毒平台联动，对网络中传输的文件进行特征比对，以便减少对本地计算资源的消耗。 6. 支持通过恶意软件特征检测方式识别失陷主机并记录日志。 7. 为覆盖工作无关应用，移动应用不少于1000种，即时消息应不低于150种，虚拟货币交易平台不低于40种。 8. 设备内置常用应用标签，分类至少包含内容外发风险、期货行业合规、证券行业合规、高安全风险、影响工作效率、消耗带宽6大类； 9. 根据URL库及URL关键字进行网址访问管理，一条策略实现阻断、记录、告警，方便维护。 10. 当用户的网页访问被网页浏览策略封堵时，用户如果发现分类错误能够在页面中向管理员进行反馈；管理员可查看用户反馈的分类错误，并可以选择向服务器反馈。   11、其它要求：为方便管理要求与防火墙统一品牌。 | 1 | 台 |
| 4 | 互联网区域web防毒 | 1. 网络吞吐量≥1Gbps，应用层处理能力≥500Mbps，网络并发连接数≥65万，HTTP并发≥24万，HTTP新建连接数≥5000/s。有液晶面板，1TB硬盘，单电源，2个扩展插槽。配置≥6个10/100/1000M自适应电口，2组bypass，1个Console口，2个USB口.Web安全保护16个站点。包含三年WAF软件特征库服务，三年硬件维修服务。 2. 具备旁路部署对镜像流量分析的同时实现阻断功能，产品具备专门的阻断接口设置和对端MAC地址设置功能。 3. 产品具备对HTTP、HTTPS协议的代理网关功能，支持透明代理、反向代理、负载均衡等模式。 4. 产品具备SQL注入、XSS跨站攻击防御策略，支持特征检测与语义算法检测。 5. 产品具备Web业务控制防御功能，提供针对爬虫、黑链、内网代理以及盗链的防护功能。 6. 产品具备Web业务加固防御功能，提供人机识别、弱密码检测、会话安全、CGI安全、跨站请求伪造以及业务流程控制的防御功能。 7. 产品具备虚拟补丁功能，支持导入Appscan和SecVSS scan扫描器的扫描结果生成WAF的规则，对此类网站漏洞直接防护。 8. 产品具备机器学习引擎，针对业务建模，可通过学习URL、host等信息展示网站结构树形图，并支持对URL的访问量和响应健康度进行图形化统计。 9. 产品具备检测并抵御IP，TCP，UDP，ICMP，DNS，HTTP协议的20多种DDoS攻击类型。 10. 产品具备HTTP访问控制，可根据实际网络状况自定义请求方法等参数的访问控制规则，支持设置HTTP 0.9/1.0/1.1/2.0版本和10多种http访问控制方法。   11、其它要求：为方便管理要求与防火墙统一品牌。 | 1 | 台 |
| 5 | 互联网区域SSL vpn | 1. VPN专用硬件平台,配置≥6个10/100/1000电口，，操作系统及VPN软件，默认带300个SSL/Ipsec共用收取和300个ID授权，最大支持300用户，产品软硬件三年质保。 2. 支持旁路或串接部署到用户网络，支持多链路接入、支持策略路由、支持链路聚合。 3. 支持配置向导功能，用户能够按照配置向导一步一步的操作，向导结束用户能够完成账号建立、服务发布、正常访问。 4. 支持B/S和C/S的应用支持单点登录（SSO），并提供加密认证功能。访问多个应用，只须输入一次密码，支持针对不同的访问资源设定不同的SSO用户名和密码。 5. 支持建立256个虚拟站点，每个站点可指定管理员，管理员可以关联和管理相应的用户。根据虚拟站点不同，可配置相应应用和应用组、服务控制策略以及认证策略等。 6. 可单独对每个应用发布业务进行负载均衡，具有轮询、加权轮询、最少连接数、静态就近性、动态就近性等算法来实现。 7. 支持自动跳转功能，用户登录后自动弹出默认的应用界面。可自定义应用图标，可自行设置智能终端应用图标、PC端应用图标。 8. 支持终端使用Win7、win7 64位、win8、win10、Mac、Linux等操作系统登录，保证登录后能够正常访问SSL VPN发布的服务。 9. 支持动态令牌APP根据网关配置的安全策略，进行Root、越狱检测，若不通过，禁止登录和绑定。 10. 支持动态令牌APP根据网关配置的安全策略，实现一人一机绑定，用户账号与手机DEVID进行绑定，DEVID需收集收集硬件信息经过HASH算法而来，达到硬件token的安全要求。 | 1 | 台 |
| 6 | 网闸 | 1. 网系统吞吐量≥450Mbps ；硬件配置：2U机箱，支持液晶面板，内网接口≥6个10/100/1000Base-T端口，≥2个SFP插槽，1个Console口，2个USB口；外网接口≥6个10/100/1000Base-T端口，≥2个SFP插槽，1个Console口，2个USB口。 2. 功能模块：数据库同步、文件交换、数据库访问、邮件访问、安全浏览、安全FTP、定制模块、工控访问等；质保年限：默认包含三年维保。 3. 文件交换：文件交换可灵活设置文件传输方向，同时工作模式支持源端移动、源端删除、增量更新、完全复制、延迟删除等多种模式。 4. 文件交换：具备文件断点续传，同时支持文件并发数量设置，大幅度提升文件传输性能，充分利用硬件资源。 5. 数据库同步：支持MySQL、ORACLE、ORACLE\_RAC、SQLServer、DB2、SYBASE、POSTGRESQL等常见数据库，支持神通、达梦、人大金仓、南大通用等国产数据库同步。 6. 数据库访问：数据库库名控制、数据库表控制，可以根据用户与数据库表对应关系，进行相应数据库操作过滤。 7. 安全浏览：安全浏览支持域名控制、源端控制、URL过滤、命令过滤、文件大小限制、用户认证。 8. TCP/UDP访问：支持TCP、UDP定制服务；支持源地址绑定、网络接口地址绑定功能。 9. TCP/UDP访问：支持源地址、源端口、目的地址、目的端口过滤功能、任务运行时间控制。 10. 病毒防护：支持异构双引擎病毒模块，可根据用户需求选择需要的病毒引擎，支持云查杀模式，可联动云端文件鉴定中心，预判文件安全风险，防止恶意文件通过网闸进入内网，提供高中低不同级别阻断策略。 | 1 | 台 |
| 7 | 内网区域防火墙 | 1. 网络层吞吐量≥20G，并发连接≥350万，每秒新建连接数≥25万，标准2U机箱，冗余电源，配置1个Console口 、1个HA接口，1个MGT接口，配置≥6个千兆以太网电口，≥4个SFP插槽，≥4个SFP+插槽，≥2个接口板卡扩展插槽，支持液晶屏，三年硬件维保服务。病毒防护特征库、入侵防御特征库升级服务。 2. 支持VTEP（VxLan Tunnel EndPoint）模式接入VxLAN网络，并可作为VXLAN二层、三层网关实现VxLan网络与传统以太网的相同子网内、跨子网间互联互通；支持通过绑定VLAN、VNI（VXLAN Network Identifier）、远程VTEP，手动管理VxLan网络；支持MAC、VNI、VTEP静态绑定。 3. 支持支持静态路由、策略路由及动态路由。策略路由支持用户自定义其优先级，动态路由应至少支持RIP v1/v2/ng， OSPFv2/v3，BGP4/4+协议；必须支持静态和动态多播路由，动态多播路由必须支持PIM-SM（稀疏模式）。 4. 支持NAT64，NAT66、NAT-PT等种IPv4/v6过渡技术，支持针对ICMPv6以及IPv6扩展头防护功能。 5. 支持在虚系统内独立配置病毒防护、漏洞利用防护、间谍软件防护、URL过滤、文件过滤、内容过滤、邮件过滤、行为管控等安全功能。并可支持对本虚系统内产生的日志进行独立审计。 6. 支持对最多6级的压缩文件进行解压查杀。 7. 产品的漏洞防护特征库及间谍软件库包含高危漏洞攻击特征，至少包括“永恒之蓝”、“震网三代”、“暗云3”、“Struts”、“Struts2”、“Xshell后门代码”以及对应的攻击的名称、CVEID、CNNVDID、CWEID、严重性、影响的平台、类型、描述、解决方案建议等（CVEID、CNNDID、CWEID等信息在漏洞攻击特征中体现）详细信息。 8. 能够对HTTP/FTP/POP3/SMTP/IMAP/SMB六种协议进行病毒查杀；本地病毒库规模大于3000万。 9. 支持基于主机或威胁情报视图，统计网络中确认被入侵、攻破的主机数量，至少可查看被入侵、攻破的时间、威胁类别、情报来源、威胁简介、被入侵、攻破的主机IP、用户名、资产等信息；并对威胁情报发现的恶意主机执行自动阻断。 10. 支持自定义基于TCP、UDP、HTTP协议的间谍软件特征。间谍软件特征可通过多个字段以文本或正则表达式的形式进行有序和无序匹配；并可自定义间谍软件的源、目的端口范围。   11、为保障应急响应能力，要求制造厂商为网络安全应急服务支撑单位（国家级）、国家信息安全漏洞库（CNNVD）技术支撑单位（一级）；（投标时须提供相关证书复印件加盖公章佐证）。 | 2 | 台 |
| 8 | 内网区域日志审计 | 1. 包括日志采集、分析、集中存储和展示等功能。事件综合处理性能最高≥3000EPS。硬件规格≥6个千兆电口，≥2个扩展插槽（可选2万兆光、4千兆电、4千兆光），4T硬盘，1个Console接口，220V交流冗余电源。标配≥100个日志源授权，三年硬件维保服务。 2. 能够对组织的IT资源中构成业务信息系统的各种网络设备、安全设备、安全系统、主机操作系统、虚拟化、云计算、数据库、中间件以及各种应用系统的日志、事件、告警等安全信息进行全面的审计。 3. 支持通过Syslog、Syslog-NG、SNMP Trap、Netflow V5、JDBC、Agent代理、WMI、(S)FTP、NetBIOS、文件\文件夹读取、Kafka等多种方式完成各种日志的收集功能，支持多行日志采集合并为一行。 4. 支持对资产日志进行过滤，设置允许接收和拒绝接收日志，并可以对资产设置一定时间范围内未收到事件后进行主动告警。 5. 系统提供页面可视化编辑归一化策略，对页面查看的日志编辑归一化策略，所见即所得，也支持通过归一化文件的导入来支持归一化,不需修改系统程序。 6. 日志解析字段内置130个字段，属性字段可扩展，用户可根据审计需要自行创建字段，字段类型包括IP、字符串、整型等6种，可设定字段长度、选择字段操作符集，选择映射函数等。内置及新增的所有字段均可参与查询、关联分析和报表统计。 7. 针对匹配的多条范化策略，系统支持用户手工设置策略匹配优先级，保证最佳范化策略匹配。 8. 系统提供即席查询功能，支持归一化字段及关键字搜索，从海量事件原始信息中获取与关键字匹配或部分匹配的所有事件。系统支持基于正则表达式的检索功能，用户可在搜索栏内输入正则表达式，系统可搜索出原始信息中与正则表达式相匹配的所有事件。 9. 可以以图形化的方式展示日志属性之间的聚合关系，并支持手动选择日志属性，显示多维事件分析图；属性可增加或减少，且支持图片大小调整。 10. 持柱状图、饼图、折线图、面积图、堆积图、环状图、数值图、地图、3D地球等形式的统计信息可视化展示，并可将统计结果保存为仪表板和报表等。图表数据支持数据下钻。 | 1 | 台 |
| 9 | 内网区域数据库审计 | 1. 事件处理≥25000条/秒，内置≥4TB磁盘存储空间。标准2U机箱，双电源；标配≥6个千兆自适应电口，≥2个SFP+万兆光口，1个Console口，≥支持两个扩展槽位，支持液晶屏。包含三年软件升级和硬件维修服务。 2. 可通过端口镜像（SPAN）或者分流器（TAP）模式旁路部署或Agent插件方式部署，并支持通过Agent审计回环地址的流量。 3. 支持的数据库：Oracle、SQL-Server、DB2、Informix、Sybase、MySQL、PostgreSQL、达梦、人大金仓、南大通用Gbase、神舟通用、Caché等。 4. 支持旁路阻断功能（非串联方式），阻断两种模式，宽松模式：对单一会话危险操作阻断；严格模式：源IP操作的所有请求直接阻断。 5. 支持全文检索数据库solr的审计，可审计到solr的查询、插入行为的操作信息。 6. 支持重复操作的统计审计规则，可根据在一定的时间内，重复某项操作达到设定的统计次数进行规则审计告警。 7. 支持C/S架构COM、COM+、DCOM组件的审计，可提取应用层工号（账号）的身份信息，精确定位到人。 8. 系统能自动发现网络中存在的数据库（支持发现数据库地址、端口、数据库类型等内容），并自动添加成保护对象进行审计，简化操作，避免用户因模糊记忆引起的配置故障。 9. 内置疑似SQL注入、跨站脚本攻击、字段猜测、代码更改、等近500种风险审计规则库，无需单独配置，直接调用。 10. 系统支持全库检索、条件检索和关键字检索，检索效率达到1亿条数据二十秒内检索出结果，快速定位相应的审计会话内容。 | 1 | 台 |
| 10 | 堡垒机 | 1. 标准≥6个千兆电口；支持2个接口扩展槽位；内置4TB硬盘；支持液晶屏；最大支持150路图形会话或400路字符会话并发；提供≥200授权许可。含三年标准售后服务。。 2. 物理旁路，逻辑串联模式，不影响原有网络架构； 3. 支持SSH、RDP、VNC、Telnet、FTP、SCP、SFTP、DB2、MySQL、Oracle、SQL Server、Rlogin等协议； 4. 通过应用发布实现对MySQL、SQL Server、Oracle、IE、Firefox、Chrome、VNC Client、SecBrowser、VSphere Client、Radmin、dbisql等应用程序/客户端的扩展支持； 5. 支持运维过程中会话协同，可邀请其他用户参与、协助操作；会话协同过程中，参与者可以控制会话，创建者强制获取控制权； 6. 持动态令牌、USBKEY、手机令牌、手机短信等多因子认证； 7. 支持按用户、账户组设置多对多的资源访问授权，用户组和账户组内的新增成员自动继承授权关系； 8. 页面直观展示操作指令，包括原始操作命令，命令输出、并可以通过操作的命令关键字定位播放会话视频，视频回放，支持播放速度调整、拖动、暂停、停止、跳过空闲、重新播放等操作，会话录像可离线下载播放； 9. 系统内置多种运维、系统报表模板，支持按日、周、月为周期，自动生成Word、Excel等格式报表。 | 1 | 台 |
| 11 | 安全感知平台 | 1. 由全流量威胁发现模块、威胁分析模块两个节点组成。 2. 全流量威胁发现模块：≥4个GE管理电口；≥4\*USB接口；1\*DB9 Console接口；冗余电源；≥960G SSD ，≥12\*4TB SATA 存储硬盘。威胁分析模快：≥2个GE流量监听电口；≥2个10GE流量监听光口；≥2个GE管理电口；4\*USB接口；≥1\*DB9 Console接口；冗余电源；≥4TB SATA存储硬盘。三年原厂硬件保修服务。三年威胁情报更新授权与规则升级授权 3. 支持常见协议识别并还原网络流量，用于取证分析、威胁发现，支持：http、dns、smtp、pop3、imap、webmail、DB2、Oracle、MySQL、sql server、Sybase、SMB、FTP、SNMP、telnet、nfs等。 4. 支持其他类型的WEB攻击，如目录遍历、弱口令、权限绕过、信息泄露、文件包含、文件写入攻击等检测。 5. 支持基于流量实时IOC匹配功能，设备具备主流的IOC，情报总量50+万条。 6. 支持基于工具特征的WEBSHELL检测，能通过系统调用、系统配置、文件的操作来及时发现威胁；如：中国菜刀、小马上传工具、小马生成器等。 7. 支持基于网络请求的语义分析检测，能够将网络请求拆分后从请求头、响应头、请求体、响应体四方面详细展示请求内容，并能提升对未知威胁检测能力。 8. 以攻击者的维度进行分析，对攻击者进行画像，画像内容包括地理位置信息、国家信息、所属组织、使用的攻击手段、攻击的所有资产。 9. 支持从威胁情报、应用安全、系统安全和设备安全的业务场景维度对告警进行攻击带外分析。 10. 支持异常登录行为检测，检测内容包括：源ip、账号、登录资产IP、使用协议、登录结果等信息，且能进行异常时间配置。 11. 支持对任意线索的自定义拓线及溯源取证分析，支持以可视化分析画布形式展示拓线过程并支持结果快照导出；支持对于给定线索的溯源结果展示，包括但不限于攻击溯源、失陷主机分析、暴力破解分析、弱口令分析等。 12. 支持大屏可视化展示，包括外部威胁态势、威胁事件态势、资产风险态势、访问态势等多种态势展示。   ★要求安全感知平台与本次采购清单中各个区域防火墙、服务器安全、终端安全软件、上网行为管理等全套产品为同一品牌，各产品支持与安全态势感知平台协同联动，构成安全事件自动化响应处置闭环体系。 | 1 | 台 |
| 12 | 业务专线防火墙 | 1. 网络处理能力≥10G，并发连接≥260万，每秒新建连接≥18万/秒， 标准2U机箱，冗余电源，配置≥6个10/100/1000M自适应电口，≥4个SFP插槽，支持两个扩展槽，1个Console口，支持液晶屏。含三年病毒库和三年入侵防御特征库升级服务、三年硬件维保服务。 2. 支持VTEP（VxLan Tunnel EndPoint）模式接入VxLAN网络，并可作为VXLAN二层、三层网关实现VxLan网络与传统以太网的相同子网内、跨子网间互联互通；支持通过绑定VLAN、VNI（VXLAN Network Identifier）、远程VTEP，手动管理VxLan网络；支持MAC、VNI、VTEP静态绑定。 3. 支持支持静态路由、策略路由及动态路由。策略路由支持用户自定义其优先级，动态路由应至少支持RIP v1/v2/ng， OSPFv2/v3，BGP4/4+协议；必须支持静态和动态多播路由，动态多播路由必须支持PIM-SM（稀疏模式）。 4. 支持NAT64，NAT66、NAT-PT等种IPv4/v6过渡技术，支持针对ICMPv6以及IPv6扩展头防护功能。 5. 支持在虚系统内独立配置病毒防护、漏洞利用防护、间谍软件防护、URL过滤、文件过滤、内容过滤、邮件过滤、行为管控等安全功能。并可支持对本虚系统内产生的日志进行独立审计。 6. 支持对最多6级的压缩文件进行解压查杀。 7. 产品的漏洞防护特征库及间谍软件库包含高危漏洞攻击特征，至少包括“永恒之蓝”、“震网三代”、“暗云3”、“Struts”、“Struts2”、“Xshell后门代码”以及对应的攻击的名称、CVEID、CNNVDID、CWEID、严重性、影响的平台、类型、描述、解决方案建议等（CVEID、CNNDID、CWEID等信息在漏洞攻击特征中体现）详细信息。 8. 能够对HTTP/FTP/POP3/SMTP/IMAP/SMB六种协议进行病毒查杀；本地病毒库规模大于3000万。 9. 支持基于主机或威胁情报视图，统计网络中确认被入侵、攻破的主机数量，至少可查看被入侵、攻破的时间、威胁类别、情报来源、威胁简介、被入侵、攻破的主机IP、用户名、资产等信息；并对威胁情报发现的恶意主机执行自动阻断。支持自定义基于TCP、UDP、HTTP协议的间谍软件特征。间谍软件特征可通过多个字段以文本或正则表达式的形式进行有序和无序匹配；并可自定义间谍软件的源、目的端口范围。 | 2 | 台 |
| 13 | 服务器安全 | 1. 提供≥100个主机授权的服务器安全功能授权，提供完整的系统加固和防护能力，包括资产梳理、风险发现、病毒扫描、安全基线等基础检测能力，提供防病毒+防火墙+入侵防御+防暴力破解功能等高级防护能力。含三年特征库升级服务和原厂维护。 2. 系统需支持无代理部署模式及有代理部署模式，以便结合管理需求选择相应部署模式。 3. 支持windows/linux主流操作系统（不限于下）：Windows Server 2003、2008、2012、2016、2019、Windows 7、Windows 8、Windows 10、Windows Vista、RedHat Enterprise Linux 6.0-7.7、CentOS6.0-8.4、Ubuntu 10.04-20.04、SUSE 11、12、15 、中兴新支点NewStart、BC-linux、Oracle Serve、Deepin、RE-DCOS、NeoKylin Linux等操作系统。。 4. 采用主动的方式进行自动化病毒查杀，支持多引擎联动防护Bitdefender、QOWL、云查杀、支持灵活开启或停用引擎；支持病毒文件自动隔离、自动删除、修复、监控多种处理方式。支持病毒查杀的结果生成报告。提供防护策略控制可避免启动风暴和查杀风暴。 5. 系统支持快速扫描、全盘扫描；支持个性化扫描，可以提供不同路径、不同文件类型、时间等进行自定义病毒扫描查杀。针对压缩文件处理，支持压缩文件数量、压缩层级、压缩包大小进行精确扫描，系统除文件、文件夹例外，还需支持单独的病毒黑白名单的管理运维。 6. 系统应支持入侵防御功能，可针对出入虚拟机的流量进行检测识别，防御网络攻击及入侵行为，通过真实漏洞利用流量的特征来检测或阻止漏洞利用(虚拟补丁防护能力)。 7. 提供防火墙功能，支持虚拟机/终端系统的双向控制。可提供对威胁情报实时分析网络流量功能，检测出失陷主机并提供监控及阻止失陷主机与恶意域名的连接功能。系统需支持对DDoS等异常流量进行拦截和清洗能力。 8. 产品预置入侵防御规则应不少于8000条次（不包含自定义规则），需覆盖系统、数据库、应用漏洞、防勒索、防挖矿等多种类型防御规则，防御规则支持严格、高、中三种预定义级别，针入侵威胁，提供检测和阻止模式，可以自动捕获违反规则的网络包，供验证和分析使用。 9. 支持对全流量或指定流量进行采集转发。支持VXLAN和GRE转发协议，且可以限制转发速率。 10. 产品应支持对应用协议的内容进行解析和识别，包括应预置应用分类协议库，针对分类配置阻断、允许策略；应用分类协议库不少于2300种，包含主流应用及协议。   11、其它要求：为方便管理要求与防火墙统一品牌。 | 1 | 套 |
| 14 | 终端安全软件 | 1. 提供≥1000点终端含防病毒（不含第三方扩展引擎）、补丁管理、主机防火墙、终端管控功能。智能全网管理，远程客户端信息管理，漏洞管理。支持Windows XP/7停服系统加固功能。原厂三年升级服务和标准维保。 2. 操作系统支持：Windows XP\_SP3及以上/Windows Vista/Windows 7/Windows 8/Windows 10；Windows Server 2008/Windows Server 2012/Windows Server 2016/Windows Server 2019。 3. 终端管控：支持根据分组、计算机名称、IP地址、操作系统、在线状态等条件的组合筛选出符合条件的终端进行管理。 4. 病毒防护概况：终端基础信息、病毒库版本、发现病毒数、未处理病毒数、最后查杀时间、文件防护状态、引擎使用状态、扩展病毒库版本。 5. 病毒扫描支持扫描所有文件和仅扫描程序及文档文件设置，支持对压缩包文件设置最大扫描层数和大小，当发现压缩包内存在病毒时，还需继续扫描压缩包内其他文件。 6. 支持不少于三个杀毒引擎混合使用，提高病毒检出率。 7. 支持针对Windows XP/Windows 7系统可带来安全隐患的设计机制进行加固性修复，支持远程漏洞攻击防护、本地钓鱼攻击防护和浏览器漏洞攻击防护。 8. 支持对Windows操作系统、IE、.NET Framework、Office、Adobe Flash Player、Adobe Acrobat和Adobe Acrobat Reader DC、硬件驱动更新等软件进行补丁修复。 9. 支持管理员预先设置好灰度发布批次和漏洞修复策略（分时间段、按级别、排除有兼容性问题的补丁等），每当控制台更新补丁库，自动化编排完成漏洞修复——将全网终端划分为由小到大的多个批次，根据企业环境，自动先推送给第一个小批次分组，如无问题自动推送给下一个批次，直到推送给全网。如有问题，只需将有问题的补丁添加到排除列表和卸载已安装的终端即可。整个推送安装过程自动化编排，无需管理员过多参与，只需在有问题时添加排除列表和下发卸载补丁任务。 10. 支持对终端各种外设（USB存储、硬盘、存储卡、光驱、打印机、扫描仪、摄像头、手机、平板等）、接口（USB口、串口、并口、1394、PCMIA）设置使用权限，并支持生效时间设置。   11、其它要求：为方便管理、联动要求与防火墙统一品牌。 | 1 | 套 |
| **数据安全设备及服务** | | | | |
| 1 | 数据资产测绘系统 | 一、功能要求  1.支持创建数据源时，根据IP地址、端口号进行对原始库、资源库、主题库等数据库进行测试，同时可配置账号密码、Keberos等方式的认证配置。  2.支持创建数据源时，进行部门、业务系统等维度的标记，并支持根据部门、业务系统信息进行快速数据源列表筛选。  3.支持数据源以列表方式进行呈现，至少包括：应用名、应用类型、IP、端口、访问账号、部门、业务系统等信息，并支持列表上直接展开呈现数据源下的实例清单。  4.支持对发现的数据源进行自动状态标记，允许对未确认的数据源进行快速录入数据源操作，生成新的数据源。  5.支持数据分类列表呈现，至少包括：数据分类、备注、数据权重、数据等级、规则状态等信息，并支持列表上直接展开呈现子集数据分类信息。  6.支持添加检测规则时，关联对应的分类分级信息，同时可对目标范围、命中率、识别方式、识别内容、识别长度等进行精细化配置，并支持自定义对应的防护建议，为数据分类分级的落实提供支撑。  7.支持数据资产检测任务列表呈现，至少包括：任务名称、目标应用、执行方式、创建时间、最近结束时间、部门、业务系统、采用数量等信息，同时支持列表上直接展开呈现对应的实例清单，至少包括：实例名称、当前状态、最近检测、检测开始、检测结束等信息。  8.支持列维度的数据资产清单呈现，支持通过应用、实例进行快速列资产筛选操作，列资产清单至少包括：列名、数据权重、列描述、命中特征、数据等级、数据分类、表名等信息，支持快速查看列所属应用详细信息。  9.支持资产概览分析，分析维度至少包括：资产总览、数据资产分析、数据分类统计、数据资产清单、文件资产分析、文件分类统计、文件资产清单等。  10.为能够将数据资产进行统一的展示和分析，以及方便运维人员统一管理，需与数据安全管控平台同一品牌，制造商提供参数确认函加盖制造商公章佐证。  二、硬件要求  1.CPU≥4核心4线程  2.网卡：千兆电口≥6个；  3.内存：≥32G；  4.硬盘：≥1T；  5.电源：双电源  6.扩展：网卡扩展槽≥2个。 | 1 | 套 |
| 2 | 数据接口风险监测系统 | 一、功能要求  1.支持主动和被动方式对重点系统数据请求监测，包含患者个人信息查询、健康状况数据查询、医疗支付数据查询、医疗应用数据查询、卫生资源数据查询、公共卫生数据查询等数据接口进行画像分析，包括访问接口热度、风险走势、访问账号热度、访问源热度等维度。  2.支持数据接口台帐管理，支持以接口资产清单或文件的方式进行导入，支持汇总统计应用、接口等，支持接口台帐导出操作。  3.支持按照层次递进的方式进行数据接口资产呈现，包括组织机构、应用、接口等维度。  4.支持对数据接口识别规则的独立管理，并支持手动或自动方式的将人员的个人身份信息、健康状况信息、医疗支付信息、医疗应用信息数据等同步到流量分析组件。  5.支持数据接口威胁维度的风险发现，包括大并发量的访问搜患者信息、搜处方信息、实时挂号数据、健康状况信息等，非业务时间访问医院信息系统，下载过量患者信息、医疗应用信息及医疗支付数据等风险。  6.支持账号行为维度的风险发现，包括账号特权使用、弱口令、暴力破解、操作时间异常、账号访问超频、一账号多人用、一人用多账号等。  7.实现数据接口访问的全流量审计，支持通过接口资产名称、IP、时间段、账号等多维度的检索。  8.支持对接医院信息系统应用日志，进行用户异常分析，包括失效用户行为异常、权限超限异常、特权账号窃取、异常时空登录、登录凭证滥用、登录行为异常、登录时间异常、登录地点异常等。  9.为精准采集现网全部流量，以及对现网数据接口访问进行分析，必须与流量复制汇聚设备同一品牌，制造商提供参数确认函加盖制造商公章佐证。  10.为方便运维人员进行统一管理，必须与数据安全管控平台同一品牌，实现设备统一管理和策略下发，制造商提供参数确认函加盖制造商公章佐证。  二、硬件要求  1.CPU：≥（8核心8线程）×2  2.内存：≥64G  3.网卡：千兆电口≥4个，万兆光口≥2个  4.硬盘：硬盘≥4T，SSD≥480G  5.电源：双电源  6.扩展：硬盘扩展槽≥7个，网卡扩展槽≥5个。 | 1 | 套 |
| 3 | 流量复制汇聚设备 | 1.硬件指标：≥4个千兆光口，≥20个千兆电口。  2.性能指标：支持流量复制汇聚线速采集转发，可支持60Gbps以上汇聚能力。  3.流量镜像汇聚：支持多接口双向汇聚。  4.端口聚合：支持多端口聚合输出输入。  5.标签识别：支持对流量的VLAN等标签进行识别并替换或解除，实现多种流量采集的设备兼容。  6.流量QOS定义：支持QOS流量自定义镜像汇聚采集，可针对某种业务端口或协议进行定制流量汇聚采集。  7.为实现现网全流量的采集和分析，数据接口风险监测系统必须和流量复制汇聚设备同一品牌，制造商提供参数确认函加盖制造商公章佐证。  8.★支持“肉鸡”防护、防蠕虫病毒传播等功能（提供CNAS认可的国家权威机构出具的测试报告复印件并加盖制造商公章佐证）。  9.★支持IP扫描防护、UDP扫描防护、TCP扫描防护等功能（提供CNAS认可的国家权威机构出具的测试报告复印件并加盖制造商公章佐证）。  10.★支持终端类型识别、仿冒终端识别、终端安全防护等功能，只允许特定类型的设备接入网络（提供CNAS认可的国家权威机构出具的测试报告复印件并加盖制造商公章佐证）。 | 1 | 台 |
| 4 | 数据防泄密系统 | 一、功能要求  1.能对图片、文档等多种数据形式进行识别、具备多种协议监控能力，并能够完整地进行恢复流量中传输的内容。  2.支持点滴式泄露规则，可监测一定时间内的累计泄露情况审计和分析用户风险行为  3.支持发现终端数据资产、分类数据及风险数据，支持配置不同的扫描路径，支持全盘扫描、关键目录扫描、指定目录扫描，支持即时扫描和周期扫描方式，周期扫描可支持按天、周、月的定时扫描，支持终端实时扫描、闲时扫描模式  4.支持监控文件打开行为，支持监控文件内容拷贝粘贴行为，支持监控USB拷贝行为  5.支持监控网络发送行为，支持终端网络外发疑似目的地关联分析，支持监控网络共享行为，支持监控IM附件粘贴行为，支持监控文件打印行为，支持文件打印加水印，可自定义水印内容，支持监控ADB操作行为，支持监控截屏拷屏行为  6.支持对终端屏幕设置水印，对于截屏、拍照等泄露方式可追溯查找泄露源；支持设置文字、二维码、点状、折线等水印类型；支持设置水印大小、颜色、透明度、间距、形状大小等参数；支持不可见水印还原，水印颜色可自适应不同背景色  7.支持终端“提醒告警、用户填写原因、阻断、审批”的系统响应方式  8.支持根据预设的策略标准对违规事件的严重等级进行划分支持根据预设的策略标准对违规事件的严重等级进行划分，支持通过修改事件状态和指定责任人完成事件的处理跟踪，支持添加事件批注和修改严重度  9.支持基于管理角色对事件的访问进行限制，并可以对违规内容进行访问控制，可以定义不同的管理员角色来对事件进行管理。仅安全管理员及内容管理员有对风险事件具备访问权限。其它人员无法访问仅内容管理员有下载风险文件权限，其他人员无权下载风险文件  10.具备趋势分析的能力，可按机构，部门或用户来报告事件和趋势。报告通过图形化方式显示事件趋势及分析统计结果，支持报表统计维度多层钻取  11.支持组合报表定制功能、可导出定制生成的PDF报告报表页。  12.为能够将现网数据泄露风险事件实现自动化闭环处置，数据防泄密系统必须与数据安全管控平台同一品牌，制造商提供参数确认函加盖制造商公章佐证。  二、硬件要求  1.CPU：≥10核心20线程  2.内存：≥32G  3.网卡：千兆电口≥4个  4.硬盘：4T  5.电源：双电源  6.扩展：硬盘扩展槽≥7个，网卡扩展槽≥4个。 | 1 | 套 |
| 5 | 数据安全管控平台 | 一、功能要求  1.支持接口风险、应用风险、账号风险、资产等维度的风险态势大屏可视化，并支持数据下钻。  2.支持以地图方式进行资产分布可视化呈现，并支持数据下钻。  3.支持数据资产测绘，通过网络互联中的数据交互情况，寻找数据安全隐患问题。  4.基于数据载体的访问威胁监测，包含数据污染、数据越权、数据窃取、数据截断、数据违规下载等。  5.基于数据流动的实时监测分析，包含接口数据分类分级标记、数据级别高亮、敏感数据外泄、数据出境评估。  6.基于数据流动的行为监测分析，自动构建数据切面的访问基线，数据行为异常告警发现，支持数据溯源分析，人物画像溯源分析，基于数据切面的风险溯源分析。  7.基于访问实体的威胁监测分析，包含高权限访问发现，认证脆弱性。  8.数据运维监测分析，包含权限监测，数据运维可视化，数据日志聚合分析。  9.内置多种基于场景化的数据安全模型、支持基于行业业务属性、特殊系统自定义数据安全建模。  10.数据资产自动分类分级打标，包括静态、动态、边缘数据资产；持续数据资产状态监控。  11.丰富的内置敏感数据特征匹配规则，同时支持敏感数据特征匹配规则的自定义。  12.支持统一管控敏感数据发现系统的敏感扫描特征和全流量数据发现系统的流量检测特征。  13.支持对数据安全防护设备进行统一管控，支持自定义重点账号、自定义弱口令字典。  14.支持管控敏感数据发现系统的数据资源发现任务和敏感数据扫描任务。  15.支持应用接口资产实时监控功能、接口风险事件溯源及取证功能、账号风险事件溯源及取证功能。  16.支持数据资产主动扫描功能、敏感数据定位功能、数据价值挖掘分析功能。  17.具备灵活的报表功能：1）支持以每天、每周、每月的周期自动导出报表；2）支持自定义报表导出周期；3）支持自定义报表模板，可从接口风险分析、账号风险分析、敏感检测结果等几个维度配置报表内容。  18.为实现设备的统一管理，数据安全管控平台和数据接口风险监测系统、数据资产测绘系统和数据防泄密系统必须为同一品牌，制造商提供参数确认函加盖制造商公章佐证。  19.★支持资产画像功能，支持显示外连访问、内部访问、外部访问的流量统计信息、访问的源 IP、目的 IP、访问方式和流量趋势（提供CNAS认可的国家权威机构出具的测试报告复印件并加盖制造商公章佐证）。  20.★支持全包存储流量，以及远程调取、查看和下载功能（提供CNAS认可的国家权威机构出具的测试报告复印件并加盖制造商公章佐证）。  21.★支持AI自动处置功能，处置信息可显示处置目标、所属机构、数据来源、威胁等级、威胁资产数量、事件类型、处置来源、处置手段、处置时间、生效日期和备注信息（提供CNAS认可的国家权威机构出具的测试报告复印件并加盖制造商公章佐证）。  二、硬件要求  1.CPU：≥（10核心20线程）×2  2.内存：≥128G  3.网卡：千兆电口≥4个，万兆光口≥2个  4.硬盘：硬盘≥ 8T，SSD≥480G  5.电源：双电源  6.扩展：硬盘扩展槽≥7个，网卡扩展槽≥5个，支持RAID卡。 | 1 | 套 |
| **双活数据中心建设硬件及服务** | | | | |
| 1 | 业务外网超融合服务器 | 超融合相关软件出厂预安装，硬件采用模块化架构，每套包括两个节点，节点及配件均支持热插拔，单节点配置如下。  CPU：2颗Intel® Xeon® 4216 CPU处理器  内存：256G 2933MHz DDR4 。  硬盘：系统盘：2\*480GB SATA SSD，缓存盘：1\*960GB NVMe SSD，数据盘：4\*8TB 7.2K SATA HDD  网络：配置万兆光接口:4个、GE接口:2个、4个万兆模块。  电源：800W冗余电源  通过超融合管理平台上即可实现对计算、存储、网络、安全等资源的统一管理运维。配置一键秒级创建虚机、扩容节点自动发现、可视化实时监控中心（对硬件可靠性、超融合系统可靠性、服务可靠性三大层面进行实时监控和分层监控）、一键切换展示大屏、一键健康巡检、一键存储清理、一键资源导出、一键虚机还原、一键僵尸虚机管理、支持纳管VMware、全运行态业务（支持容器）、动态资源扩展（DRX）、应用HA、SRM站点容灾、跨集群迁移（云彩虹）、双活、硬件SR-IOV、DPDK、分布式防火墙、集成在线p2v、v2v迁移工具、AI资源容量预测，应用监控APM、集成虚拟网络安全功能，提供公网IP地址池、虚拟防火墙、虚拟负载均衡、虚拟路由器、虚拟网络设备的连通性探测、网络拓扑所画即所得等功能  存储虚拟化软件，采用软件定义存储架构，把所有服务器硬盘组织成一个虚拟存储资源池，支持在同一节点同时提供分布式块、对象、NAS存储服务，同一硬盘池支持配置不同冗余策略、支持2~5副本数用户自定义、支持故障域和保护域设置、支持厚/精简配置、块存储支持快照功能、数据落盘的时候就自动平衡、存储集群规模支持>=256个节点，数据重构速率快于30min/T，本次配置分布式块功能许可 | 3 | 台 |
| 2 | 服务器虚拟化软件 | 计算虚拟化：通过虚拟化技术将物理服务器虚拟化为一个逻辑计算资源池。虚拟机可以实现物理机的全部功能，具有自己的资源（内存、CPU、网卡、存储），可以指定单独的IP地址、MAC地址等，支持现有市场上主要国内外操作系统，配置虚拟机快照、集群HA（高可用），DRS（动态资源调度）、虚拟机回收站、虚拟机桌面预览、虚拟机模板在线克隆、批量修改虚拟机的配置参数、硬件SR-IOV、GPU直通、vGPU、跨集群迁移等功能。含三年软件版本升级服务和远程技术支持服务 | 6 | 套 |
| 3 | 虚拟化云安全 | 管理控制中心支持主流虚拟化平台；能够与虚拟化平台无缝对接，支持适配主流虚拟化平台，并能够实现同一个控制中心管理，配置安全防护管理平台 1 套，6个CPU授权。  管 控 平 台 提 供 图 形 化 安 装 界 面 ， 并 可 支 持Windows、Linux 两种  安装包，满足不同类型环境需求；具备集中控管的功能，能够统一的管理和配置系统安全防护策略，并且安全威胁日志能够统一的在集中管控平台上呈现。  防病毒功能需支持本地扫描和云安全扫描，具备本地病毒码和云端病毒码，支持实时扫描，预设扫描和、手动扫描和快速扫描。  支持入侵防御功能，在已知漏洞修复之前，屏蔽漏洞以免遭受无限制的入侵；产品支持推荐扫描，可以根据不同计算机的扫描结果自动下发对应的入侵防御规则，入侵防御规则包含 Web 应用程序防护、可疑网络活动、漏洞和利用等防护规则。  支持可集中控管的防火墙策略，策略定制可以针对IP,Mac地址或通讯端口，可保护所有基于IP通讯协议（TCP、 UDP、 ICMP 等）和所有框架类型（IP、ARP 等）。 提供三年原厂维保服务、三年原厂软件升级维护 | 6 | 套 |
| 4 | 内网核心业务服务器 | 配置≥4颗Intel Xeon Gold 6230或以上处理器 配置≥1024GB DDR4 3200MHz服务器内存 配置≥2块企业级600GB SAS热插拔硬盘 配置Raid卡，支持RAID 0、1、5、6、10、50、60，配置≥2GB缓存（可支持扩展到8G缓存卡） 配置≥2个32Gbps HBA存储连接端口 配置≥4个万兆光口（含多模光模块） 配置≥2个千兆电口 配置≥2个热插拔冗余电源 配置原装滑动导轨 制造商三年7×24小时质保服务; | 4 | 台 |
| 5 | 光纤交换机 | 48端口或以上光纤交换机 至少配置24端口激活，配置≥24个32G光模块 含级联许可 制造商三年7×24小时质保服务; | 4 | 台 |
| 6 | 存储虚拟化平台 | 为了保障售后服务统一及产品兼容性，本次所供产品要求与本项目的核心全闪存存储为同一品牌 全冗余模块化体系结构  支持控制器的横向的扩展  采用分布式缓存一致性架构 本次配置≥2个虚拟化控制器，每个控制器配置≥128GB缓存；  单集群支持最大缓存≥1024GB，单集群支持扩展≥8个虚拟化控制器  多控制器构成集群时，控制器间通讯通过额外的FC或IB端口进行，不占用用于连接主机和存储阵列的FC端口  配置在逻辑设备上封装建立类RAID 0的逻辑卷功能，通过跨LUN进行I/O条带以提升性能；  配置在逻辑设备上封装建立类RAID 1的逻辑卷功能，通过跨分布在不同阵列的LUN进行镜像以提供后端阵列的高可用性；  配置在逻辑设备上的封装拼接逻辑卷功能，提供一种通过组合两个或多个较小设备来创建较大设备的功能  支持实现数据中心多台存储系统之间的双活。任何一台存储发生硬件故障，另一台存储仍然继续对外提供服务，业务无中断。采用LUN直接映射方式，将原有存储整合时，不能摧毁原有存储上的数据 本次要求配置跨数据中心双活，通过FC或IP链路实现两个数据中心的存储设备的双活，任何一个数据中心的存储设备发生故障，仍然能够通过另一个数据中心的存储设备进行访问，无需任何人工干预下存储数据访问零中断。  支持使用UNMAP为精简配置回收空间 支持XCOPY功能，提升数据移动效率 本次配置≥16个16Gb/s光纤接口  单集群支持不低于11000个LUN；  配置最大主机连接数≥1600个  实现自动在多个虚拟化引擎的控制器之间执行存储域的共享、平衡和故障切换。实现存储私有云功能  跨阵列移动生产卷而不会造成主机中断或宕机  冗余集群设计，无单点故障，能够进行无中断硬件和软件升级  系统还附带 FAST Cache，可提高 IO 和  FAST VP 性能，实现自动分层效率。高密度存储模块仅仅在三个机架单元中便支持 80 个  闪存驱动器，进一步提升了空间利用效率。 制造商三年7×24小时质保服务; 提供制造商盖章的投标产品技术参数确认函和制造商盖章的服务承诺函。 | 2 | 套 |
| 7 | 核心全闪存存储 | 企业级NVMe全闪存存储，存储操作系统为全闪存架构优化，不支持使用机械磁盘； 一体化统一存储架构，同时提供NAS、IP SAN和FC SAN访问模式； 配置LUN、VVOLs及NAS服务方式，同时提供数据块和文件访问服务； 存储系统支持控制器的横向扩展，可扩展≥8个控制器； 最大可扩展缓存≥8000GB 最大可扩展处理器核心数≥368核 最大可扩展前端FC端口数≥64，支持32Gb端口配置 最大可扩展前端10GbE端口数≥96，支持25Gb端口配置 本次配置≥2个SAN+NAS融合控制器，每个控制器配置≥2颗12核Intel Xeon 2.1GHz或以上处理器，两控制器总核数≥48核，且控制器采用Active-Active架构; 每控制器缓存配置≥384GB，两控制器总缓存配置≥768GB，缓存配置非SSD模拟、闪存扩展卡，NVMe卡，SCM卡，NAS缓存等其他扩展方式 配置≥8个32Gbps的前端FC光纤通道端口 配置≥4个10Gb/s的前端NAS和iSCSI一体化端口 配置≥10块3.84TB企业级NVMe全闪存固态硬盘 固态硬盘单盘每块最大可支持15.36TB 双控制器下支持≥21块NVMe SCM磁盘作为可读写的用户数据存储空间 同时支持NVMe和SAS协议的固态硬盘 全冗余模块化架构，数据路径、电源、驱动器连接和存储处理器，任何部件具备无中断现场更换能力和故障自动切换能力，具有完全在线、无需停机的扩充能力，包括系统微码升级、系统处理能力的升级或扩充、存储容量的扩充等； 配置全容量许可的存储管理与性能监控功能 配置全容量在线重复数据删除和压缩功能 配置全容量数据复制功能 配置服务质量管理功能，通过优化磁盘阵列中的应用程序IO队列，实现对应用程序的IOPS、带宽和响应时间的控制优化； 支持并配置存储机器学习和智能预测软件，可以基于存储的系统健康状态，资源使用情况等作出趋势分析预测以及智能的资源负载均衡告警提醒，促使业务数据存储卷空间更加智能的均衡分布和运行。 支持并配置快照及克隆功能，快照克隆要求基于ROW Redirect on Write技术，不影响生产卷性能，快照克隆要求支持重复数据删除和数据压缩 配置≥2块8GB专有高速卡用于重复数据删除和数据压缩，不占用控制器性能 具备DevOps能力，能够与主要管理和编排框架集成，简化应用程序开发并自动执行存储工作流。至少支持VMware的vRO、Kubernetes的CSI Driver和Ansible的Ansible Module三种主流或开源框架 配置应用感知的数据副本管理软件，支持Oracle, SQL Server, Exchange等主流应用环境，实现副本自动化创建与挂接，刷新等操作，应用管理员可直接对应用使用的数据卷进行快照克隆日程定制化，并可在主机挂载用于数据分析，备份恢复和测试开发等用途 支持虚拟化集成功能，支持在存储设备控制器上直接部署应用程序虚拟机，并与虚拟机管理程序集成，统一管理和运维 支持并配置图形化管理界面，支持并配置Rest API管理功能，支持并配置命令行管理功能 支持不同型号的控制器混合使用  针对物理、虚拟和基于容器的应用和数据库采用单一体系结构。专为实现99.9999% 的可用性而设计 满配情况下最大功耗不超过1650伏安 满配情况下最大散热量不超过6000000焦耳/小时 每个电源至少配置单线20安或以上保险丝 制造商三年7×24小时质保服务; 提供制造商盖章的投标产品技术参数确认函和制造商盖章的服务承诺函。 | 2 | 台 |
| 8 | 现有核心存储扩容硬盘 | 现有全闪存储扩容原装NVMe固态硬盘 扩容11块1.92TB企业级NVMe全闪存固态硬盘 扩容存储容量及功能软件许可 存储制造商专业扩容实施服务 | 1 | 批 |
| 9 | 内网超融合设备 | 产品采用标准x86服务器架构，横向扩展架构，由多节点组成集群并行工作，并且互为冗余； 分布式架构，存储为分布式存储，支持多台独立服务器本地SSD和/或HDD盘组成一个可以共享的存储资源池； 每个节点都同时提供计算与存储能力，任何一个CPU都同时支持计算和存储； 采用横向扩展架构，集群支持≥64个节点； 节点磁盘无需做RAID，通过副本镜像方式保证数据可靠性，可选择1副本、2副本、3副本、4副本；也可以通过纠删码方式保证数据可靠性 2U高架装式机箱，可支持冗余电源，前面板和后面板的每个节点配有独立的电源控件； 每个节点至少配置2块480GB 固态硬盘作镜像，安装虚拟化系统盘使用，保证可靠性； 每个节点配置不少于2颗CPU，CPU规格不低于Intel® Xeon® 5320 26核心 2.2GHz处理器 每个节点支持32DIMM插槽， 最大支持4TB内存，本次配置不少于1536GB内存； 每个节点不少于16个硬盘槽位； 本次至少配置2块800GB企业级固态盘作为读写缓存空间; 不接受SATA固态盘作为读写缓存空间； 本次至少配置12块4TB 7.2Krpm磁盘作为存储容量空间； 具有预防误拔功能，可以智能区分盘体故障和物理拔除，触发自我修复的时间阀值可以修改； 每个节点本次配置至少8个万兆以太网光口（每个端口含多模光模块）； 每个节点配置至少1个千兆以太网络作为管理使用； 配置软硬件设备统一管理平台授权 每节点至少配置2颗CPU的存储管理软件授权； 配置软件分布式交换机功能 超融合产品所有管理界面均要求有中文支持。 初次配置全Web单一界面向导，简单易用快速完成全自动化部署，无需人工干预自动安装服务器虚拟化底层软件和自动完成虚拟化分布式存储安装和配置，自动配置网络。 一键式诊断集群系统健康状况，包括组件连通状况，硬件组件健康状况等；并可一键式生成集群系统日志包。 支持在线对厂商后台提交服务请求，与售后服务人员在线沟通 具备安全远程服务主动支持。具备无人值守维护功能，能提供24x7规格的安全远程监视、诊断与修复、提供信号检测功能，以确保持续监视、通知和远程故障排除、能够在潜在问题影响业务之前进行快速的远程诊断和修复无缝地自动接收支持更新； 支持超融合设备在线和先将系统镜像下载离线式，同时升级超融合系统、服务器虚拟化和虚拟化分布式存储软件组件的一键升级。 支持应用商店方式在线或离线选择并安装或升级超融合设备上的扩展组件应用，比如虚拟机连续性数据保护软件，公有云扩展软件等。 可以以波形图方式查看集群一段时间内的性能状况，包括：集群存储IOPS的当前值和高峰值，存储的总容量/已用用量/空闲量/已置备用量，CPU的总Hz数和空闲Hz数以及当前利用率，内容的总量和空闲总量以及当前利用率， 可以查看节点中每个容量磁盘、缓存磁盘、系统磁盘和网卡的健康状况，以及每个网卡的当前流量。 可以以前后面板指示灯形式查看超融合设备物理组件的工作状况，包括：每块磁盘指示灯，每个节点的电源指示灯，每个网卡指示灯，电源和风扇指示灯等。 可以在管理界面里自动发现添加的新节点，并完成向集群内添加节点过程。 可以在管理界面里自动发现发生问题的磁盘，并向导式完成磁盘更换过程，同时自动完成数据再平衡过程。 可以在界面中，一键关掉整个集群节点。在关机过程中，节点轮流下电，节点上的虚拟机也会轮流关机，不会影响整个集群业务。 支持Web界面方式进行管理，可在同一界面管理计算和存储资源，既可以完成虚拟机例如创建/快照/开关机/删除功能，虚拟化集群创建/虚拟交换机配置,分布式存储定义策略/管理磁盘组，并监控详细的性能与容量； 存储以单一Datastore方式提供给虚拟化平台使用，无需再通过划分卷或LUN映射给虚拟化层； 提供基于存储策略的管理机制，如： 每个对象保存镜像份数 每个对象的条带宽度 每个对象预留读写缓存空间 每个对象IOPS服务限制QoS 每个对象是否强制置备 每个对象空间预留 每个对象是否校验和等， 并可以通过变更存储策略可在线动态调整业务应用正在使用的存储资源。 根据业务应用的需求，可以以每一个虚拟机磁盘VMDK粒度定义存储策略，而不是只能以datastore或卷粒度。 针对每个虚拟机或每个虚拟磁盘可以灵活设置1/2/3/4个副本，对于同一个虚拟机，可以为不同VMDK虚拟磁盘配置不同副本份数 采用SSD作为高速读/写缓存，并且提供可以动态调整的虚拟机级别的读写缓存预留，确保重要应用的读写性能。 配置支持基于存储的IOPS服务质量控制（QoS）功能 无缝集成虚拟化平台的HA、虚拟机在线迁移、存储在线迁移、自动化资源调度等功能，无需额外安装软件 支持iSCSI、NFS、SMB、HTTP协议对外提供存储空间 支持HDFS文件协议 支持OpenStack Swift文件协议 支持MS WSFC集群技术，支持Oracle RAC集群技术，支持Splunk  可以实现 99.9999% 的高可用性 虚拟化管理平台提供API、SDK等接口，可以与第三方管理软件结合或二次开发 为了保证产品的可靠性和稳定性及兼容性，超融合所有软硬件产品须为同一厂商提供 配置并支持虚拟机持续数据保护功能，实现多集群间虚拟机秒级IO记录和恢复级别，实现虚拟机逻辑性灾备；可进行生产虚拟机与备份虚拟机的切换，可进行备份虚拟机的多副本验证。 支持备份立即验证功能，可以将备份的虚拟机文件立即在备份设备上启动验证备份正确性，无需先将备份虚拟机文件先恢复再验证； 提供一个基于GUI的直观界面,易于运行交互式搜索和深度分析查询,以获得快速、切实可行的深入见解 支持多种图形统计视图，包括但不限于柱状图、线图、堆栈图、多种颜色类别的综合示意图 支持多个关键词的聚合查询，即根据关键字逐渐缩小查询范围 制造商三年7×24小时质保服务; 提供制造商盖章的投标产品技术参数确认函和制造商盖章的服务承诺函。 | 4 | 台 |
| 10 | 影像存储 | 全冗余架构，企业级分布式NAS存储； 为保障兼容性及售后服务统一，本次招标产品要求与本项目核心全闪存存储同一品牌； 采用横向扩展集群存储架构；不接受纵向扩展架构和共享式非对称集群架构。全Active并行集群模式，集群内所有节点成员功能一致、地位均等、数据均衡分布。没有单独的元数据（索引和管理等）服务节点，无单独管理节点； 节点数量可以在线动态扩展，容量与性能随着扩展同步增加； 每个节点配置缓存≥96GB，系统支持全局缓存，提高存储访问效率； 存储节点之间支持采用InfiniBand交换机或25GbE网络交换机互连，本次每节点配置2个25GbE后端网络接口，全集群配置2台25GbE交换机用于后端数据交换； 每节点配置≥2个25GbE前端接口（含多模SFP模块）； 每节点配置≥1块800GB企业级固态盘，用于元数据和缓存加速； 每节点配置≥15块2TB 6Gbps 7200rpm企业级硬盘； 存储集群提供单一文件系统, 单一卷，最大可扩展到17PB以上； 存储系统要求支持多副本及跨节点RAID技术，要求全局数据灵活多级别冗余设置数据保护，最大可达N+4保护级别或8倍副本镜像保护。可以根据数据重要性对存储系统中的不同目录(存储系统中的任意目录)灵活调节冗余度等功能； 允许在线更改文件目录保护机制，不影响应用使用； 支持Telnet/SSH管理，提供基于Web浏览器的管理界面，管理界面简单易用； 配置针对目录、子目录和用户、用户组的配额管理功能； 配置客户端连接管理软件，要求支持针对节点轮询的负载均衡策略，无需客户端安装任何Agent或者其他调度管理的角色服务器； 配置针对小文件的压缩打包功能，提高存储效率； 配置性能监控和文件系统监控工具，可定期将监控数据生成可视化报告； 支持第三方文件系统审计，用来提高存储基础架构的安全和控制并满足重要的法规和法规遵从性要求。使用此审计功能，管理员可追溯用户的访问行为，可以确定哪些用户正在访问特定的文件，并更加有效地控制和管理文件访问权限； 存储设备提供数据安全检测接口，供第三方杀毒软件直接进行数据的集中病毒检测和杀毒； 支持并配置标准的ICAP防病毒协议，并且与主流的杀毒软件卡巴斯基、诺顿等兼容； 为了保证文件共享的安全性，存储系统的NFS和CIFS协议支持特定类型文件的扩展名过滤策略，如禁止写入exe扩展名的文件； 支持通过频繁的、用户可恢复的文件备份来提供简单的时间点数据保护和恢复。支持自动化根据需要不断备份数据，以满足RPO。 支持NDMP协议，可将存储集群中的数据备份到带库中；支持提供专用的备份性能加速模块，加快大数据的备份速度； 支持引擎加速功能。可配置加速引擎，用于提升存储整体性能； 存储配置VMware系统集成功能，支持VMware API，包括VAAI VASA等集成； 为了方便管理，集群至少支持WEB，CLI，REST API以及液晶面板方式实现扩容，可以实现存储节点液晶面板直接操作完成存储扩容，可通过存储节点的液晶面板进行管理，液晶面板功能包括显示状态和告警信息等； 为保证存储设备的安全访问，存储需要支持多租户功能，即可以将一套物理集群在逻辑上划分为多套“独立”集群，拥有独立的网络、域控、共享点等； 在整个NAS范围内支持文件级别数据重删功能； 支持WORM(一写多读)功能； 防止关键数据意外、过早或恶意更改或删除，同时满足严格合规性要求和管理要求。 支持基于角色的访问控制（RBAC），细粒度设置权限和角色； 支持同一节点对外提供多种访问接口，同时支持并配置NFS、SMB、FTP、HTTP，HDFS，ICAP、SWIFT和S3等协议。用户可通过以上任意协议同时访问一份数据，要求在任何情况下都无需在客户端主机增加任何软件或驱动程序； 存储支持与应用系统Hadoop模块集成，Hadoop模块需通过原生HDFS方式，无需将HDFS协议的文件访问请求转换为NFS协议请求（非NFS方式）读写存储，实现数据存储服务；且Hadoop节点与客户端无需额外安装插件； 集群存储支持云分层功能，存储可将数据分层至公有云和私有云存储中，如亚马逊S3、微软Azure中。该功能对应用透明，不改变客户业务系统； 允许单个文件系统中存在多个存储层，以在单个存储池中聚合和合并应用程序。通过单个管理点实现工作流隔离、更高的利用率和独立的可扩展性。 通过文件级粒度和自动策略控制,能够业务无感知地调整性能和数据布局、存储层一致性和保护设置。 通过优化的数据放置，确定最佳数据放置位置，其策略触发条件包括：文件时效、大小、类型、所有者、位置或日期字段等 制造商三年7×24小时质保服务; 提供制造商盖章的投标产品技术参数确认函和制造商盖章的服务承诺函。 | 4 | 台 |
| 11 | 备份软件 | 为保障兼容性及售后服务统一，本次招标产品要求与本项目核心全闪存存储同一品牌； 支持多种网络环境备份:支持TCP/IP网络环境的数据备份，可以升级到SAN环境下的LANFree备份，并支持升级到ServerFree备份。 支持多种数据库系统备份:支持各种数据库平台（包括DB2、SQL Server、Oracle、Informix、Sybase等）的在线备份。 支持多种存储备份设备:支持各种类型的磁盘阵列（SAN，iSCSI，NAS等）、磁带机和磁带库，支持冗余的备份设备。 支持可视化人机界面:支持以图形或WEB方式进行管理，包括在管理范围内设备的状态和性能信息、各种数据保护参数、各种备份作业的设置信息、各种备份/恢复作业的执行状态统计信息、各种备份业务数据的相关信息等. 备份管理平台:备份管理平台可支持自由选择安装，可以部署在虚拟机、桌面机、台式机、移动终端（如平板电脑、智能手机等），采用独立的APP，而不是Web版本进行管理和控制。 支持用户审计管理:支持对备份系统的用户的分级管理，如：系统管理员、维护员、操作员等不同的角色，并且可以纪录所有的用户的操作情况。 云备份文档管理组件:支持基于共有云、私有云、混合云的备份解决方案，可以自由选择将备份数据备份到云端，必要时可以从云端将数据进行恢复。 支持桌面机备份:支持通过局域网或VPN进行桌面机备份，个人用户实现自助式文件备份和恢复。 全面支持VMware虚拟化备份:  a、可以通过新的VADP方式，配合高性能的磁盘备份设备，提供对VMware的高效备份；  b、能自动发现VMware拓扑结构，方便管理；  c、支持源端消重方式备份VMware；  d、支持与vSphere web client界面集成，即可以在vSphere web client中直接操作备份恢复；  e、支持在VM中自助恢复丢失的单个文件；  f、支持Instant Access功能，无需恢复，直接访问备份的VM；  g、支持对单个VMDK文件的备份/恢复；  h、当vCenter完全损坏的时候可以快速恢复虚拟机，而不需要重新部署vCenter；  i、软件能够安装在VMWARE环境中。 磁盘阵列快照集成:支持与磁盘阵列的快照集成，通过备份软件控制存储的快照产生/快照删除，并支持把指定快照备份到指定介质中。 支持client push:支持向导方式对备份客户端软件的批量推送升级。 支持虚拟合成全备份:支持把一个全备份和多个增量备份合成一个新的全备份，且合成过程在备份设备底层完成，不占用介质服务器的资源。 支持高密度文件系统快照备份:通过快照提高对大量小文件系统的备份性能，如WEB Server。同时支持文件级别的恢复。 支持开放磁带格式:支持在各个操作系统平台使用相同的纪录磁带格式，保证磁带介质在各种平台之间的交换和共享；保证备份内容的安全性，任何人拿到单独的备份介质，无法使用通用的tar之类的指令读出数据，截取信息。 备份过程中提供非活动文件报告:支持在备份过程直接记录“非活动文件”使用报告，备份完毕后进行报表显示，为数据归档提供依据。 数据切分比对技术:备份方案需采用高效率的重复数据删除技术，能够对不同的文件采用变长而非定长的数据段进行分割。无论文件更改了那部分都能够智能的找到未发生变化的部分，而不会增加需要传输的备份数据量。 备份服务器间的数据冗灾:备份系统要支持对备份后数据的远程复制功能，可以创建备份后数据的副本，并且能够支持基于广域网的低带宽传输。使用内置的数据复制功能，将已经备份的数据按照增量的方式定时传送到远程站点上进行备份后数据的容灾。 高效的恢复能力:恢复数据时不需采用全备份叠加增量备份来恢复至指定的时间点，而是采用任意时间点恢复的方式直接恢复到客户所要求时间点的数据。 备份源重复数据删除技术:备份方案要支持在数据源进行的重复数据的删除功能，避免大量数据通过网络传输时带来的带宽的占用和过长的备份窗口，将客户端上需要备份的数据中的重复部分在传输之前就进行甄别和筛选，只将唯一的数据段备份到终端存储上。 备份服务端全局数据删除技术:备份数据经过备份客户端的重复删除之后被传送到备份服务端，服务端可自动对这些来自多个客户端的数据作全局性的重复数据再删除，以最小化重复数据的可能性。 备份方式:采用永久全备份的方式。 监控软件类型:对整个数据灾备流程和系统进行监控/报告/告警/预测/分析，支持客户现有存储及网络环境，支持多操作系统，支持主流的数据保护系统及备份系统，支持对连续性数据复制的监控和报告。能够提供清晰、详细的图示和报表，清晰显示生产端到容灾段数据保护逻辑。 支持监控的操作系统:IBM AIX， HPUX，Windows，SUN Solaris，Linux等操作系统。 支持复制系统及软件类型的监控:Symantec NetBackup/PureDisk  EMC Avamar/ NetWorker/ Recoverpoint/ SRDF  HP Data Protector  IBM TSM  Backup Exec  CommVault Galaxy  CA ARCserve  Oracle RMAN  Sun/STK ACSLS Manager 等。 支持监控类型:支持IP和SAN网络监控，支持物理机和虚拟机(VMware)的监控，基于Real-time和事务的监控。 容量分析预警功能:支持对容量的全面监控和预测，通过预警功能更好的计划购买或部署新的容量，防止容量耗尽影响应用程序。 监控平台统一管理:整合跨多个系统和域收集的信息，通过单一窗口实现监控，分析和报告。 支持备份统计功能:支持对于所有备份/恢复作业内容的统计并形成文本或图形方式的报告。 分析功能:当对本地生产端和远程端的数据保护进行监控时，可以监控到以下内容：远程站点的配置信息，包括服务器和存储拓扑关系，数据复制映射关系，数据复制带宽。 监控功能:对远程端被复制的数据进行可恢复性分析，比对主机，存储，数据库结构等信息，给出分析诊断结论或报表以确定远端数据是否可恢复，支持对数据库关联结构进行分析。 告警功能:对数据保护过程进行全程实时监控可以通过e-mail, SNMP, or external scripts来实现告警功能。 支持SLA目标监控.支持用户指定的SLA，即服务级别目标监控，即当用户指定数据保护在一定的时间或其他条件内没有完成，系统给于自动告警和分析。 支持多种操作系统备份:Server端需支持所有主流Windows、Linux、UNIX平台（HP-UX、SUN Solaris、IBM AIX等）；Client端需支持通用操作系统平台，包括：AIX、HP-UX、Solaris， Window2019/2012/2008、Linux等等。 配置不限制备份客户端授权； 配置不限制数据库备份数量授权； 配置不限制虚拟机备份数量授权。 制造商三年7×24小时质保服务; 提供制造商盖章的投标产品技术参数确认函和制造商盖章的服务承诺函。 | 1 | 套 |
| 12 | 备份设备 | 具备高去重特性的备份存储设备，配置在线重复数据消除技术，对于用户生产环境的数据，全局重复数据消除比率不低于1：20。重复数据消除过程是在备份任务执行过程中并行进行，而不依赖于某种备份软件的格式； 为保障兼容性及售后服务统一，本次招标产品要求与本项目核心全闪存存储同一品牌； 配置线内可变长字段的备份重复数据删除技术,使设备设备内不存在伪重复数据； 配置基于CPU的重复数据删除技术,重删时减少对磁盘性能的损耗,最长时间的保护磁盘使用寿命； 支持主流备份软件：DellEMC NetWorker，Symantec NBU/BE，IBM TSM, HP DP, Commvault等； 配置≥2颗Intel Xeon 10核心处理器 配置≥192GB高速缓存 配置≥2个16Gbps FC接口 配置≥4个10Gbps网络接口 配置≥1块1.92TB企业级固态盘作为高速缓存 配置≥16GB NVRAM压缩加速卡 配置≥32TB可用备份空间 配置CIFS/NFS/VTL协议 配置备份增强软件，提高数据备份效率，并提供高级负载均衡和故障切换功能，增强复制功能，实现单点管理所有备份拷贝 配置数据复制软件，支持两台设备间实现去重后的数据复制 配置虚拟化版本软件 配置不限制备份节点数量 支持OST备份，采用介质服务器端和目标端协同重复数据删除实现带宽优化的OST备份，以显著提高性能，简化灾难恢复过程，并为备份应用程序与备份存储系统之间的其他集成奠定基础； 提供LAN-FREE备份和LAN备份方式； 不限制磁带库和驱动器数量，方便备份环境扩展； 含热备件、冗余电源、冗余冷却系统、热插拔驱动器、电源和风扇。无单点故障风险； 配置相应的热备磁盘保护； 具备多种技术以保障数据从CACHE到写入硬盘以及整个数据保留周期时间内的完整性和安全性，本次配置的备份设备需要提供并结合最少4种保护机制并建立连续的防线来防御所有的错误源,确保数据可完整恢复； 提供端到端的验证所有文件系统数据和元数据可恢复,可在备份数据写入备份设备后自动将备份数据与发送到备份设备的原始数据相比较,以验证备份数据是否可完整恢复； 制造商三年7×24小时质保服务; 提供制造商盖章的投标产品技术参数确认函和制造商盖章的服务承诺函。 | 1 | 台 |
| 13 | 容灾服务器 | 配置≥2颗Intel Xeon Gold 5320或以上处理器 配置≥1024GB DDR4 3200MHz服务器内存 配置≥2块企业级600GB SAS热插拔硬盘 配置Raid卡，支持RAID 0、1、5、6、10、50、60，配置2GB缓存（可支持扩展到8G缓存卡） 配置≥2个16Gbps HBA存储连接端口 配置≥4个万兆光口（含多模光模块） 配置≥2个千兆电口 配置≥2个热插拔冗余电源 配置原装滑动导轨 制造商三年7×24小时质保服务; | 2 | 台 |
| 14 | 容灾光交 | 24端口或以上光纤交换机 至少8端口激活，配置≥8个16G光模块 含级联许可 制造商三年7×24小时质保服务; | 1 | 台 |
| 15 | 容灾存储 | 为保障兼容性及售后服务统一，本次招标产品要求与本项目核心全闪存存储同一品牌； 一体化统一存储架构，同时提供NAS、IP SAN和FC SAN访问模式；全冗余模块化体系结构 配置两个SAN+NAS融合控制器,每控制器配置2颗Intel 8核心, 1.8GHz处理器 每个控制器缓存配置96GB,每台存储总缓存配置192GB 配置≥8个16Gbps的前端FC光纤通道端口 配置≥25块1.8TB企业级SAS硬盘 存储双控后端板载4通道嵌入式12Gbps SAS I/O端口4个，后端总带宽为192Gbps 提供图形化存储管理软件，集成在线支持体系 配置存储性能在线分析功能 提供存储集中管理功能 配置本地存储数据保护套件（内含快照和克隆等功能） 配置精简资源调配功能 配置固态硬盘扩展存储二级缓存功能 配置存储远程数据保护套件（包含远程同步/异步数据复制） 配置在线重复数据删除和压缩 配置服务质量管理QOS功能 配置内部数据迁移功能 配置异构阵列数据迁移功能 具备全冗余数据路径、电源、驱动器连接和存储处理器，任何部件具备无中断现场更换能力和故障自动切换能力，具有完全在线、无需停机的扩充能力，包括系统微码升级、系统处理能力的扩充、存储容量的扩充等； 免费提供利用存储端负载创建与数据库等应用一致性快照管理的图形化软件，应用管理员可直接进行快照日程定制化，并可在主机挂载用于数据分析，备份恢复和测试开发等用途 制造商三年7×24小时质保服务; 提供制造商盖章的投标产品技术参数确认函和制造商盖章的服务承诺函。 | 1 | 台 |
| 16 | 持续数据保护软件 | 为保障兼容性及售后服务统一，本次招标产品要求与本项目核心全闪存存储同一品牌； 对基于SAN/Server SAN/NAS/DAS等存储的虚拟机提供本地连续数据保护功能; 能够在存储上保存过去一段时间内应用数据的连续历史状态； 在主中心和容灾中心之间提供通过IP网络的数据连续历史状态复制功能; 能够在备份中心的存储上保存过去一段时间内应用数据的连续历史状态； 提供良好的架构扩展能力，满足今后扩展成更多站点的容灾需求； 必须捕获并记录虚拟机每一个写I/O操作，当虚拟机需要恢复时，用户可从任意时间点中选择，使虚拟机能够基于以前的事务快速地从任一时间点恢复； 必须从虚拟主机上直接捕获对需要保护虚拟机的写I/O数据，非通过快照方式实现持续数据保护； 可将对虚拟机任意时间点恢复，并且当虚拟化服务故障时，可直接在本地或灾备站点直接使用被保护的虚机，无需长时间数据恢复； 实现对物理和数据逻辑故障的恢复，逻辑故障包括：逻辑错误、人为误操作和病毒等引起的数据库数据丢失、人为或病毒引起的数据库崩溃等故障； 提供一致性组功能，可以将有一致性管理的所有虚拟机，绑定到一个一致性组中，以确保事务向以前时间点的回滚同时进行，从而确保应用程序及虚拟机的一致恢复； 可以由应用程序和系统自动生成事件书签，也可以由用户向系统输入自己的书签，通过书签，将系统范围的事件（端口故障、系统错误等）与潜在的损坏事件关联起来，管理员可以通过选择书签来恢复数据，从而确保恢复的数据是正确的； 对于捕获的写I/O，既支持同步复制到本地站点，也支持异步复制到远程容灾站点。以上两种方式可以配合使用，提供对同一台虚拟机的并行本地和远程保护； 提供快照整合功能，可以让用户能够决定将捕获的每一个写I/O操作保留多久，在哪一时间点将数据更改整合成一个每日、每周或每月恢复点，从而让用户能够以一致性组为单位优化使用的日志空间，这样只使用其一部分就可以跟踪每一个写操作；余下的空间可用于保存每日、每周或每月映像； 能够灵活进行主、备站点切换，在进行切换时不需要对现有系统重新配置； 能够不断测量两个站点间的带宽，并根据优先级、压缩及其他参数以动态方式，满足RPO的要求； 支持在执行故障切换之前装载复制的映像以处理和检查一致性的能力； 提供线性扩展能力，可以通过添加更多应用装置，实现性能的线性扩展和高可用性(HA)； 支持各种主流操作系统，包括支持Unix/Windows/RedHat Linux/ SUSE Linux /CentOS Linux/ Ubuntu等版本虚拟机； 支持按照秒级间隔将数据恢复到任意时间点； 持续数据保护软件要求集成针对虚拟机的持续性数据保护功能,实现虚拟机的远程容灾和任意时间点的一键式恢复功能； 本次招标要求总共配置不少于60台虚拟机的本地和远程的持续数据保护许可。 制造商三年7×24小时质保服务; 提供制造商盖章的投标产品技术参数确认函和制造商盖章的服务承诺函。 | 1 | 套 |
| 17 | 避风港接入交换机 | ≥28个万兆端口，配置≥28个万兆多模光模块 制造商三年7×24小时质保服务; | 1 | 台 |
| 18 | 避风港区域备份软件 | 为保障兼容性及售后服务统一，本次招标产品要求与本项目核心全闪存存储同一品牌； 支持多种网络环境备份:支持TCP/IP网络环境的数据备份，可以升级到SAN环境下的LANFree备份，并支持升级到ServerFree备份。 支持多种数据库系统备份:支持各种数据库平台（包括DB2、SQL Server、Oracle、Informix、Sybase等）的在线备份。 支持多种存储备份设备:支持各种类型的磁盘阵列（SAN，iSCSI，NAS等）、磁带机和磁带库，支持冗余的备份设备。 支持可视化人机界面:支持以图形或WEB方式进行管理，包括在管理范围内设备的状态和性能信息、各种数据保护参数、各种备份作业的设置信息、各种备份/恢复作业的执行状态统计信息、各种备份业务数据的相关信息等. 备份管理平台:备份管理平台可支持自由选择安装，可以部署在虚拟机、桌面机、台式机、移动终端（如平板电脑、智能手机等），采用独立的APP，而不是Web版本进行管理和控制。 支持用户审计管理:支持对备份系统的用户的分级管理，如：系统管理员、维护员、操作员等不同的角色，并且可以纪录所有的用户的操作情况。 云备份文档管理组件:支持基于共有云、私有云、混合云的备份解决方案，可以自由选择将备份数据备份到云端，必要时可以从云端将数据进行恢复。 支持桌面机备份:支持通过局域网或VPN进行桌面机备份，个人用户实现自助式文件备份和恢复。 全面支持VMware虚拟化备份:  a、可以通过新的VADP方式，配合高性能的磁盘备份设备，提供对VMware的高效备份；  b、能自动发现VMware拓扑结构，方便管理；  c、支持源端消重方式备份VMware；  d、支持与vSphere web client界面集成，即可以在vSphere web client中直接操作备份恢复；  e、支持在VM中自助恢复丢失的单个文件；  f、支持Instant Access功能，无需恢复，直接访问备份的VM；  g、支持对单个VMDK文件的备份/恢复；  h、当vCenter完全损坏的时候可以快速恢复虚拟机，而不需要重新部署vCenter；  i、软件能够安装在VMWARE环境中。 磁盘阵列快照集成:支持与磁盘阵列的快照集成，通过备份软件控制存储的快照产生/快照删除，并支持把指定快照备份到指定介质中。 支持client push:支持向导方式对备份客户端软件的批量推送升级。 支持虚拟合成全备份:支持把一个全备份和多个增量备份合成一个新的全备份，且合成过程在备份设备底层完成，不占用介质服务器的资源。 支持高密度文件系统快照备份:通过快照提高对大量小文件系统的备份性能，如WEB Server。同时支持文件级别的恢复。 支持开放磁带格式:支持在各个操作系统平台使用相同的纪录磁带格式，保证磁带介质在各种平台之间的交换和共享；保证备份内容的安全性，任何人拿到单独的备份介质，无法使用通用的tar之类的指令读出数据，截取信息。 备份过程中提供非活动文件报告:支持在备份过程直接记录“非活动文件”使用报告，备份完毕后进行报表显示，为数据归档提供依据。 数据切分比对技术:备份方案需采用高效率的重复数据删除技术，能够对不同的文件采用变长而非定长的数据段进行分割。无论文件更改了那部分都能够智能的找到未发生变化的部分，而不会增加需要传输的备份数据量。 备份服务器间的数据冗灾:备份系统要支持对备份后数据的远程复制功能，可以创建备份后数据的副本，并且能够支持基于广域网的低带宽传输。使用内置的数据复制功能，将已经备份的数据按照增量的方式定时传送到远程站点上进行备份后数据的容灾。 高效的恢复能力:恢复数据时不需采用全备份叠加增量备份来恢复至指定的时间点，而是采用任意时间点恢复的方式直接恢复到客户所要求时间点的数据。 备份源重复数据删除技术:备份方案要支持在数据源进行的重复数据的删除功能，避免大量数据通过网络传输时带来的带宽的占用和过长的备份窗口，将客户端上需要备份的数据中的重复部分在传输之前就进行甄别和筛选，只将唯一的数据段备份到终端存储上。 备份服务端全局数据删除技术:备份数据经过备份客户端的重复删除之后被传送到备份服务端，服务端可自动对这些来自多个客户端的数据作全局性的重复数据再删除，以最小化重复数据的可能性。 备份方式:采用永久全备份的方式。 监控软件类型:对整个数据灾备流程和系统进行监控/报告/告警/预测/分析，支持客户现有存储及网络环境，支持多操作系统，支持主流的数据保护系统及备份系统，支持对连续性数据复制的监控和报告。能够提供清晰、详细的图示和报表，清晰显示生产端到容灾段数据保护逻辑。 支持监控的操作系统:IBM AIX， HPUX，Windows，SUN Solaris，Linux等操作系统。 支持复制系统及软件类型的监控:Symantec NetBackup/PureDisk  EMC Avamar/ NetWorker/ Recoverpoint/ SRDF  HP Data Protector  IBM TSM  Backup Exec  CommVault Galaxy  CA ARCserve  Oracle RMAN  Sun/STK ACSLS Manager 等。 支持监控类型:支持IP和SAN网络监控，支持物理机和虚拟机(VMware)的监控，基于Real-time和事务的监控。 容量分析预警功能:支持对容量的全面监控和预测，通过预警功能更好的计划购买或部署新的容量，防止容量耗尽影响应用程序。 监控平台统一管理:整合跨多个系统和域收集的信息，通过单一窗口实现监控，分析和报告。 支持备份统计功能:支持对于所有备份/恢复作业内容的统计并形成文本或图形方式的报告。 分析功能:当对本地生产端和远程端的数据保护进行监控时，可以监控到以下内容：远程站点的配置信息，包括服务器和存储拓扑关系，数据复制映射关系，数据复制带宽。 监控功能:对远程端被复制的数据进行可恢复性分析，比对主机，存储，数据库结构等信息，给出分析诊断结论或报表以确定远端数据是否可恢复，支持对数据库关联结构进行分析。 告警功能:对数据保护过程进行全程实时监控可以通过e-mail, SNMP, or external scripts来实现告警功能。 支持SLA目标监控.支持用户指定的SLA，即服务级别目标监控，即当用户指定数据保护在一定的时间或其他条件内没有完成，系统给于自动告警和分析。 支持多种操作系统备份:Server端需支持所有主流Windows、Linux、UNIX平台（HP-UX、SUN Solaris、IBM AIX等）；Client端需支持通用操作系统平台，包括：AIX、HP-UX、Solaris， Window2019/2012/2008、Linux等等。 配置不限制备份客户端授权； 配置不限制数据库备份数量授权； 配置不限制虚拟机备份数量授权。 制造商三年7×24小时质保服务; 提供制造商盖章的投标产品技术参数确认函和制造商盖章的服务承诺函。 | 1 | 套 |
| 19 | 备份复制设备 | 具备高去重特性的备份存储设备，配置在线重复数据消除技术，对于用户生产环境的数据，全局重复数据消除比率不低于1：20。重复数据消除过程是在备份任务执行过程中并行进行，而不依赖于某种备份软件的格式； 为保障兼容性及售后服务统一，本次招标产品要求与本项目核心全闪存存储同一品牌； 配置线内可变长字段的备份重复数据删除技术,使设备设备内不存在伪重复数据； 配置基于CPU的重复数据删除技术,重删时减少对磁盘性能的损耗,最长时间的保护磁盘使用寿命； 支持主流备份软件：DellEMC NetWorker，Symantec NBU/BE，IBM TSM, HP DP, Commvault等； 配置≥2颗Intel Xeon 10核心处理器 配置≥192GB高速缓存 配置≥2个16Gbps FC接口 配置≥4个10Gbps网络接口 配置≥1块1.92TB企业级固态盘作为高速缓存 配置≥16GB NVRAM压缩加速卡 配置≥32TB可用备份空间 配置CIFS/NFS/VTL协议 配置备份增强软件，提高数据备份效率，并提供高级负载均衡和故障切换功能，增强复制功能，实现单点管理所有备份拷贝 配置数据复制软件，支持两台设备间实现去重后的数据复制 配置虚拟化版本软件 配置不限制备份节点数量 支持OST备份，采用介质服务器端和目标端协同重复数据删除实现带宽优化的OST备份，以显著提高性能，简化灾难恢复过程，并为备份应用程序与备份存储系统之间的其他集成奠定基础； 提供LAN-FREE备份和LAN备份方式； 不限制磁带库和驱动器数量，方便备份环境扩展； 含热备件、冗余电源、冗余冷却系统、热插拔驱动器、电源和风扇。无单点故障风险； 配置相应的热备磁盘保护； 具备多种技术以保障数据从CACHE到写入硬盘以及整个数据保留周期时间内的完整性和安全性，本次配置的备份设备需要提供并结合最少4种保护机制并建立连续的防线来防御所有的错误源,确保数据可完整恢复； 提供端到端的验证所有文件系统数据和元数据可恢复,可在备份数据写入备份设备后自动将备份数据与发送到备份设备的原始数据相比较,以验证备份数据是否可完整恢复； 制造商三年7×24小时质保服务; 提供制造商盖章的投标产品技术参数确认函和制造商盖章的服务承诺函。 | 1 | 台 |
| 20 | 数据避风港软件 | 为保障兼容性及售后服务统一，数据“避风港”软件产品要求与本项目备份设备同一品牌； 负责编排同步，管理和锁定存储在CR存储区中的备份系统上的多个副本，并编排恢复。 控制对存储在CR存储区中备份系统上的数据执行分析的可选过程。 订阅数据分析检测套件，检测被篡改的备份数据 本次配置分析检测套件3年软件订阅 制造商三年7×24小时质保服务; | 1 | 套 |
| 21 | 避风港区域服务器 | 配置≥2颗Intel Xeon Gold 5320处理器 配置≥512GB DDR4 3200MHz服务器内存 配置≥2块企业级600GB SAS热插拔硬盘 配置Raid卡，支持RAID 0、1、5、6、10、50、60，配置2GB缓存（可支持扩展到8G缓存卡） 配置≥2个16Gbps HBA存储连接端口 配置≥4个万兆光口（含多模光模块） 配置≥2个千兆电口 配置≥2个热插拔冗余电源 配置原装滑动导轨 制造商三年7×24小时质保服务; | 1 | 台 |
| 22 | 内网端服务器虚拟化软件 | 采用裸金属架构，无需绑定操作系统即可搭建虚拟化平台。 虚拟机之间可以做到隔离保护，其中每一个虚拟机发生故障都不会影响同一个物理机上的其它虚拟机运行，每个虚拟机上的用户权限只限于本虚拟机之内，以保障系统平台的安全性。 虚拟机可以实现物理机的全部功能，如具有自己的资源（内存、CPU、网卡、存储），可以指定单独的IP地址、MAC地址等。 能够提供性能监控功能，可以对资源中的CPU、网络、磁盘使用率等指标进行实时统计，并能反映目前物理机、虚拟机的资源瓶颈。 支持现有市场上的主流x86服务器，具有双方认可的官方服务器硬件兼容性列表，包括IBM、HP、DELL、Cisco、NEC以及国内自主品牌服务器等。 兼容现有市场上主流的存储阵列产品，具有双方认可的官方存储阵列兼容性列表，存储阵列类型包括SAN、NAS和iSCSI等，存储阵列品牌包括EMC、IBM、HP、HDS、NetApp、Dell等。 兼容现有市场上主流厂商的多款不同型号的服务器配件、网卡和HBA卡产品。 兼容现有市场上x86服务器上能够运行的主流操作系统，具有双方认可的官方客户操作系统兼容性列表， 尤其包括以下操作系统：Windows XP、Windows Vista、Windows 2000、Windows 2003、Windows 2008、Windows 8、Redhat Linux、Suse linux、Solaris x86、FreeBSD、Ubuntu、Debian、Mac OS等，虚拟机上的操作系统不进行任何修改即可运行。 vGPU技术可以支持NVIDIA、AMD和Intel硬件厂商的GPU卡。Linux虚拟机和Windows虚拟机都可以支持vGPU技术。 提供HA功能，当集群中的主机硬件或虚拟化软件发生故障时，该主机上的虚拟机可以在集群之内的其它主机上自动重启。当虚拟机的客户操作系统出现故障时，可以自动重启该虚拟机客户操作系统，保障业务连续性。 提供应用级别的HA功能，可以自动检测并修复虚拟机内运行的应用故障，保障应用的持续可用。 提供容错机制，可以保证运行虚拟机的主机发生故障时，虚拟机会自动触发透明故障切换，同时不会引起任何数据丢失或停机，保障所有应用持续可用。 支持虚拟机的在线迁移功能，无论有无共享存储，都可以在不中断用户使用和不丢失服务的情况下在服务器之间实时迁移虚拟机，保障业务连续性。 可以实现基于LAN或WAN的、独立于磁盘阵列的虚拟机级别的复制，可以对虚拟机数据进行基于多个时间点的复制。 提供虚拟机的备份功能，能够利用重复数据删除技术对整个虚拟机或虚拟机单个磁盘快速进行无代理备份(全备份或增量备份)和恢复。同时提供备份接口，能够与第三方备份软件无缝兼容对虚拟机进行集中备份。 虚拟机支持多路虚拟CPU（vSMP）技术，以满足高负载应用环境的要求。 提供将多台物理主机组成集群的能力，同时支持动态资源分配功能，可为整个集群中的虚拟机提供独立于硬件的动态负载平衡和资源分配，增强业务系统的服务质量。 具有智能的电源管理功能，可以持续地优化每个集群中的服务器功耗，根据集群内服务器的负载状况对物理主机自行下电和加电，更好地支持绿色环保节能减排的政策。 支持可靠内存技术，可以将关键的组件（如Hypervisor）放置在受支持硬件上已被确定为“可靠”的内存区域中，避免其受到无法纠正的内存错误的影响，提高系统稳定性。 可以为虚拟机创建一个或多个快照来保存虚拟机的基于时间点的运行状况和数据。 提供专用的P2V工具，实现在线物理机至虚拟机的无间断平滑转换。 虚拟机支持USB 3.0设备，支持3D显示卡虚拟化功能。虚拟机支持3D图形加速功能，可以根据需要启用或停用。 提供分布式虚拟交换机功能，实现虚拟机之间或虚拟机与物理机之间的网络调度，通过分布式虚拟交换机可以在单一界面中对虚拟化集群环境进行统一的网络管理。同时提供网络接口，支持第三方虚拟网络交换机。 提供防病毒和防恶意软件解决方案，可以与第三方杀毒软件或安全软件融合，无需在虚拟机内安装代理即可保护虚拟机，实现虚拟化环境下的安全防范。 支持物理主机级别的无状态防火墙，无需使用IPTABLES，管理员可以用命令行和图形化界面配置防火墙。 虚拟机支持直接访问裸设备，将虚拟机数据直接存储在LUN上。 具有存储精简配置能力，可以超额分配存储容量，提高存储的利用率，减少存储容量的需求。 可以利用服务器的本地闪存，提供一个可大幅缩短应用延迟的高性能分布式读缓存层，提高虚拟机的性能。 提供虚拟机的存储在线迁移功能，无需中断或停机即可将正在运行的虚拟机从一个存储位置实时迁移到另一个存储位置。支持跨不同存储类型以及不同厂商存储产品之间进行在线迁移。 提供热添加CPU，磁盘和内存的功能，无需中断或停机即可根据需要向虚拟机添加CPU，磁盘和内存。 提供具有存储识别功能的API，使第三方存储厂商可以将存储软件与虚拟化平台更好的整合，使虚拟化平台能够识别特定磁盘阵列的功能特性以及状态信息。 提供基于存储的API，以利用基于磁盘阵列的高效操作和第三方存储供应商的多路径软件功能，进而改进性能，可靠性和可扩展性。支持对现有市场上主流的存储厂商的存储进行虚拟化加速功能。 提供虚拟机存储的动态负载平衡功能，通过存储特征来确定虚拟机数据在创建和使用时的最佳驻留位置，可根据存储卷性能及容量情况进行无中断自动迁移，消除存储隐患。 支持存储与网络的I/O控制功能，可以根据虚拟机的服务质量优先级别，对存储I/O或网络I/O进行流量控制，确保虚拟机对存储资源或网络资源的访问。 支持单根I/O虚拟化功能(SR-IOV)，以实现低延迟和高I/O工作负载，实现对复杂应用的性能优化。 支持无需停机即可在正在运行的物理主机上热插拔PCIe SSD驱动器（添加/删除）的功能。 通过按用户自定义的策略对存储进行分组，确保应用服务级别与可用存储相匹配，减少存储资源管理的复杂度。 支持跨多个LUN的共享数据文件系统，可以聚合至少32个异构逻辑卷（LUN），支持在线实时添加LUN以实现集群卷容量动态增长，可支持至少64TB容量集群卷。虚拟机文件系统也支持主流存储厂商的存储自动分层功能。 提供集中式自动管理物理主机和虚拟机补丁程序的功能。 提供自动化部署能力，服务器无需安装虚拟化软件，即可实现主机的虚拟化软件运行，并通过虚拟化管理平台统一管理。 提供可以被多台物理主机共享的主机配置文件，以缩短配置新主机所需的时间，并将相同的配置更改应用到多个主机，简化主机部署及满足合规性要求。 制造商三年7×24小时质保服务; | 30 | 套 |
| 23 | 内网端虚拟化管理中心 | 支持单点管理，可以从单个控制台对所有虚拟机的配置情况、负载情况进行集中监控，并根据实际需要实时进行资源调整。 每个控制台可管理至少1000台物理服务器、10000台已打开电源的虚拟机，15000台已注册的虚拟机，并可以通过链接至少10个控制台实例，跨10个实例管理30000个已打开电源的虚拟机和50000个已注册的虚拟机。 提供统一的图形界面管理软件，可以在一个地点完成所有虚拟机的日常管理工作，包括控制管理、CPU内存管理、用户管理、存储管理、网络管理、日志收集、性能分析、故障诊断、权限管理、在线维护等工作。同时能够直接配置、管理存储阵列，具有对存储阵列的多路径管理功能。支持QoS能力，支持基于应用程序的服务级别自动管理功能。 可以支持Web Client和命令行管理功能。 支持单点登录，用户只需登录一次，无需进一步的身份验证即可访问控制台并对集群进行监控与管理。 支持自定义角色和权限，可以限制用户对资源的访问，实现分级管理并增强安全性和灵活性。 支持AD域整合，域用户可以访问控制台，由AD来处理用户身份验证。 管理软件可实现多管理软件级别互通功能，支持多管理中心架构，并可实现分布式管理。 可以记录重大配置更改以及发起这些更改的管理员的记录，可以导出报告以进行事件跟踪。 控制台可选支持双节点高可用管理方式，以减少单点故障影响。 提供自动报警功能，能够提供物理服务器或虚拟机的CPU、网络、磁盘使用率等指标的实时数据统计，并能反映目前各物理服务器、虚拟机的资源瓶颈。 制造商三年7×24小时质保服务; | 3 | 套 |
| 24 | 配套辅材及线材 | 网线、光纤跳线、PDU电源线等辅材 | 1 | 批 |
| 25 | 系统集成服务 | 产品安装到采购人指定地点和位置，并完成具体的系统安装、调试、优化直至系统稳定运行，数据中心总体集成、 实施方案、项目实施计划，项目数据中心设备的总体规划和实施部署集成服务；老院区机房生产系统设备摸排、搬迁，协调制定业务迁移及设备搬迁总体计划，协调及配合软件商进行业务迁移的实施，保障业务迁移和设备搬迁过程中的数据安全，尽量减少业务停机时间 | 1 | 套 |

# 服务要求

项目交付和免费服务期间，提供原厂工程师驻场服务。

驻场人员要求：免费服务期的驻场人员具有系统集成经验；在三甲医院做过项目实施或维护工作；业务熟练；要求驻场人员固定，如需变动须经医院同意，人员辞职或生病等其他特殊情况除外。

服务范围：本项目所包含硬件软件系统的故障分析处理、补丁升级及日常维护服务。

服务响应：7\*24小时响应。

# 9 培训要求

软件系统上线前，针对管理人员、各科室信息联络员、临床操作人员提供针对性的培训，并提供包含系统截图的操作手册。

硬件设备上线后，为医院信息技术人员系统后台配置、维护等技术培训。